

POLITECNICO DI TORINO

Facoltà di Ingegneria
Corso di Laurea in Ingegneria matematica

Tesi di Laurea Magistrale

Analisi on-chain della governance decentralizzata: uno studio comparativo su un campione di 50 DAO



Relatore

prof. Danilo Bazzanella

Correlatori

dot. Silvio Meneguzzo

dot. Alfredo Favenza

Candidata

Beatrice Sara

Anno Accademico 2025-2026

Marzo 2026

Indice

Indice	I
Elenco delle figure	VIII
Elenco delle tabelle	XIII
Introduzione	1
1 Blockchain	4
1.1 Introduzione alla crittografia asimmetrica	4
1.2 La tecnologia blockchain	7
1.2.1 Caratteristiche di una blockchain	7
1.2.2 Struttura della blockchain	8
1.2.3 Protocolli di consenso	12
1.2.4 Classificazione delle blockchain	15
2 Decentralized Autonomous Organization (DAO)	16
2.1 Storia delle DAO	16
2.2 Definizione e caratteristiche	17
2.2.1 Confronto con le Organizzazioni tradizionali	19
2.2.2 Architettura di governance	20
2.2.3 Governance	22
2.2.4 Tesoreria	22
2.3 Meccanismi di voto	23
2.3.1 Tipologie di meccanismi di voto	26
2.4 Classificazione dei token	28
2.5 Implementazione della Governance	31
2.6 Classificazione delle DAO	35

3	Analisi di 50 DAO	38
3.1	Introduzione	38
3.1.1	Criteri di selezione	38
3.1.2	Struttura dell'analisi	39
3.1.3	Fonti dei dati	40
3.1.4	Limitazioni	41
3.2	Uniswap	42
3.2.1	Token UNI	44
3.2.2	Processo di governance e analisi dei contratti	45
3.3	Arbitrum	50
3.3.1	Token ARB	51
3.3.2	Processo di governance e analisi dei contratti	52
3.4	Aave	57
3.4.1	Tokens AAVE e GHO	59
3.4.2	Processo di Governance e meccanismi di voto	61
3.4.3	Analisi dei contratti di governance	62
3.5	Sky	65
3.5.1	Token di governance e Stablecoin	67
3.5.2	Processo di governance e meccanismo di voto	68
3.5.3	Analisi dei contratti di governance	71
3.6	Curve DAO	72
3.6.1	Token CRV	73
3.6.2	Processo di governance e analisi dei contratti	75
3.7	Lido DAO	79
3.7.1	Token LDO	81
3.7.2	Processo di governance e analisi dei contratti	81
3.8	Ethereum Name Service	87
3.8.1	Token ENS	88
3.8.2	Processo di governance e analisi dei contratti	89
3.9	DeXe	93
3.9.1	DEXE Token	94
3.9.2	Processo di governance e meccanismo di voto	95

3.9.3	Analisi dei contratti di governance	97
3.10	Compound	100
3.10.1	Token COMP	102
3.10.2	Processo di governance e analisi dei contratti	102
3.11	Maple Finance	105
3.11.1	Token SYRUP	106
3.11.2	Processo di governance e analisi dei contratti	108
3.12	Wormhole	110
3.12.1	Token W	111
3.12.2	Processo di governance e analisi dei contratti	112
3.13	Diva Staking	116
3.13.1	Token DIVA	117
3.13.2	Processo di governance e analisi dei contratti	119
3.14	Braintrust	123
3.14.1	Token BTRST	123
3.14.2	Processo di governance e analisi dei contratti	124
3.15	UMA	128
3.15.1	Token UMA	129
3.15.2	Processo di governance e analisi dei contratti	130
3.16	POOH	135
3.16.1	POOH Crew NFT DAO	136
3.16.2	\$POOH DAO	139
3.17	Adventure Gold	141
3.17.1	Token AGLD	143
3.17.2	Processo di governance e analisi dei contratti	144
3.18	Degen Dogs	146
3.18.1	Token BSC ed NFT Degen Dog	148
3.18.2	Processo di governance e analisi dei contratti	149
3.19	Dope Wars	151
3.19.1	Processo di governance e analisi dei contratti	154
3.20	Hop	155
3.20.1	Token HOP	156

3.20.2	Processo di governance e analisi dei contratti di governance . .	157
3.21	onchainaustria	159
3.21.1	Tokens: OCA e BOCK	160
3.21.2	Processo di governance e meccanismo di voto	162
3.21.3	Analisi dei contratti di governance	164
3.22	Rarible	166
3.22.1	Token RARI	168
3.22.2	Processo di governance e analisi dei contratti	169
3.23	Inverse	172
3.23.1	Tokens DOLA e INV	174
3.23.2	Processo di governance e analisi dei contratti	176
3.24	Public Nouns	178
3.24.1	NFT e processo d'aste	179
3.24.2	Processo di governance e analisi dei contratti	181
3.25	Unlock	183
3.25.1	Token UP o UDT	184
3.25.2	Processo di governance e analisi dei contratti	185
3.26	Hifi	188
3.26.1	Token HIFI	189
3.26.2	Processo di governance e analisi dei contratti	190
3.27	Fluence	191
3.27.1	Token FLT	193
3.27.2	Processo di governance e analisi dei contratti	194
3.28	Gitcoin	196
3.28.1	Token GTC	198
3.28.2	Processo di governance e analisi dei contratti	199
3.29	GMX	201
3.29.1	Token GMX e GMX_DAO	202
3.29.2	Processo di governance e analisi dei contratti	203
3.30	Tornado Cash	206
3.30.1	Token TORN	207
3.30.2	Processo di governance e analisi dei contratti	208

3.31	KyberSwap	211
3.31.1	Token KNC	212
3.31.2	Processo di governance e analisi dei contratti	213
3.32	Audius	216
3.32.1	Token AUDIO	217
3.32.2	Processo di governance e analisi dei contratti	218
3.33	Ampleforth	221
3.33.1	Token AMPL e FORTH	221
3.33.2	Processo di governance e analisi dei contratti	223
3.34	Radworks	226
3.34.1	Token RAD	226
3.34.2	Processo di governance e analisi dei contratti	227
3.35	Idle	231
3.35.1	Token IDLE	232
3.35.2	Processo di governance e analisi dei contratti	233
3.36	HAI	236
3.36.1	Token HAI e KITE	237
3.36.2	Processo di governance e analisi dei contatti	238
3.37	Union	241
3.37.1	Token UNION	242
3.37.2	Processo di governance ed analisi dei contratti	243
3.38	OpenDollar	245
3.38.1	Token ODG	246
3.38.2	Processo di governance e analisi contratti	247
3.39	Cryptex	249
3.39.1	Token CTX	250
3.39.2	Processo di governance e analisi dei contatti	250
3.40	Threshold Network	252
3.40.1	Token T	253
3.40.2	Processo di governance e analisi dei contratti	254
3.41	Anvil	256
3.41.1	Token ANVL	257

3.41.2	Processo di governance ed analisi dei contratti	257
3.42	TrueFi	260
3.42.1	Token TRU	261
3.42.2	Processo di governance e analisi dei contratti	262
3.43	PoolTogether	265
3.43.1	Token POOL	266
3.43.2	Processo di governance e analisi dei contratti	267
3.44	Seamless	269
3.44.1	Token SEAM	270
3.44.2	Processo di governance e analisi dei contratti	271
3.45	Antfarm	276
3.45.1	Token ATF ed AGT	276
3.45.2	Processo di governance ed analisi dei contratti	278
3.46	Summer.fi	280
3.46.1	Token SUMR	281
3.46.2	Processo di governance e analisi dei contratti	283
3.47	RealToken	284
3.47.1	Token REG	285
3.47.2	Processo di governance e analisi dei contratti	286
3.48	Fame Lady Society	288
3.48.1	Token FAME e gSOCIETY	289
3.48.2	Processo di governance e analisi dei contratti	290
3.49	RigoBlock	292
3.49.1	Token GRG	292
3.49.2	Processo di governance e analisi contratti	293
3.50	Lisk	295
3.50.1	Token LSK	296
3.50.2	Processo di governance e analisi dei contratti	297
3.51	Comparazione finale	299
4	Risultati	305
4.1	Statistiche descrittive	305

4.1.1	Distribuzione per categoria	305
4.1.2	Distribuzione per Blockchain	306
4.1.3	Distribuzione per token standard	307
4.2	Analisi parametri di governance	308
4.2.1	Statistiche sull'intero campione	308
4.2.2	Confronto statistiche tra categorie diverse	309
4.3	Pattern tecnologici	315
5	Discussione	316
5.1	Confronto con la letteratura	316
5.2	Implicazioni pratiche	318
5.3	Limitazioni	319
	Conclusioni	320
	Bibliografia	322

Elenco delle figure

1.1	Crittografia simmetrica.	5
1.2	Crittografia asimmetrica.	6
1.3	Struttura dei blocchi in una blockchain.	11
2.1	Architettura di governance di una DAO	21
2.2	Schema di decentralizzazione a cinque livelli	25
3.1	Uniswap Logo	43
3.2	Token UNI	44
3.3	Differenze tra le prime due versioni della governance di Uniswap	47
3.4	Arbitrum Logo	50
3.5	ARB Token	51
3.6	Ritardi di esecuzione nelle proposte di Arbitrum	54
3.7	AAVE Logo	58
3.8	AAVE Token	59
3.9	GHO Token.	60
3.10	SKY Logo	65
3.11	SKY e MKR Tokens	67
3.12	USDS e DAI Stablecoins	68
3.13	Curve Logo	73
3.14	CRV Token	74
3.15	Variazione del potere di voto in Curve	76
3.16	Processo di governance di Curve	76
3.17	Lido Logo	80

3.18 LDO Token	81
3.19 Processo di governance di Lido	83
3.20 ENS DAO Logo	87
3.21 ENS Token	88
3.22 ENS - Fase 3	91
3.23 DeXe DAO Logo	93
3.24 DeXe Token	94
3.25 DeXe: Interazione tra i contratti di governance	99
3.26 Compound Logo	100
3.27 COMP Token	102
3.28 Maple Finance Logo	105
3.29 SYRUP Token	107
3.30 stSYRUP Token	108
3.31 Wormhole Logo	111
3.32 W Token	112
3.33 Processo di governance di Wormhole	114
3.34 Diva Staking Logo	116
3.35 Stakers and Operators	117
3.36 DIVA Token	118
3.37 Processo di governance di Diva Staking	119
3.38 Braintrust Logo	123
3.39 Braintrust Logo	123
3.40 Fasi della governance di Braintrust	125
3.41 UMA logo	128
3.42 Token UMA	129
3.43 Processo di governance di UMA	131
3.44 POOH Logo	135
3.45 NFTs POOH	136
3.46 POOH Token	139
3.47 Adventure Gold	141
3.48 AGLD Token	143
3.49 Degen Dog NFTs	146

3.50 Dope Wars Logo	152
3.51 Esempio di hustler equipaggiato	153
3.52 Token PAPER	153
3.53 Hop Logo	156
3.54 Token HOP	156
3.55 onchainaustria Logo	159
3.56 Token OCA	160
3.57 Token BOCK	161
3.58 Processo di governance di onchainaustria	163
3.59 Rarible Logo	166
3.60 Token RARI	168
3.61 Inverse Finance Logo	173
3.62 Token INV	174
3.63 Token DOLA	175
3.64 Public Nouns Logo	179
3.65 Examples of $\textcircled{P}$ NOUN NFTs	180
3.66 Unlock Logo	184
3.67 UP e UDT Token	185
3.68 Hifi Finance Logo	188
3.69 HIFI Token	189
3.70 Fluence Network Logo	192
3.71 FLT Token	193
3.72 Gitcoin Logo	197
3.73 GTC Token	198
3.74 GMX Logo	201
3.75 GMX Token	202
3.76 Tornado Cash Logo	206
3.77 TORN Token	208
3.78 Kyber Network Logo	211
3.79 KNC Token	212
3.80 Audius Logo	216
3.81 Token AUDIO	217

3.82 Ampleforth Logo	221
3.83 Token AMPL	222
3.84 Token FORTH	223
3.85 Radworks Logo	226
3.86 Token RAD	227
3.87 Idle Logo	231
3.88 Token IDLE	232
3.89 HAI Logo	237
3.90 Token HAI	237
3.91 Token KITE	238
3.92 Union Logo	241
3.93 Token UNION	242
3.94 OpenDollar Logo	245
3.95 Token OD	245
3.96 Token ODG	246
3.97 Cryptex Logo	249
3.98 TCAP Token	249
3.99 Token CTX	250
3.100Threshold Network Logo	252
3.101Token T	253
3.102Anvil Logo	256
3.103Token ANVL	257
3.104Processo di governance di Anvil	258
3.105TrueFi Logo	260
3.106Token TRU	261
3.107Processo di governance di TrueFi	263
3.108PoolTogether Logo	265
3.109TokenPOOL	266
3.110Seamless Logo	270
3.111SEAM Token	271
3.112Antfarm Logo	276
3.113Token ATF	277

3.114Token AGT	277
3.115Logo Summer.fi	280
3.116Token SUMR	281
3.117RealToken Ecosystem Logo	285
3.118Token REG	285
3.119Fame Lady Society Logo	288
3.120Token FAME	289
3.121Examples of NFTs gSOCIETY	290
3.122RigoBlock Logo	292
3.123Token GRG	292
3.124Lisk Logo	295
3.125Token LSK	296
4.1 Distribuzione per categoria	306
4.2 Distribuzione per blockchain\layer	307
4.3 Distribuzione per categoria del Threshold	310
4.4 Distribuzione per categoria del Quorum	311
4.5 Distribuzione per categoria del Voting Delay	312
4.6 Distribuzione per categoria del Voting Period	313
4.7 Distribuzione per categoria del Timelock Delay	314

Elenco delle tabelle

1.1	Struttura dell'header di un blocco	9
2.1	Confronto tra DAO e Organizzazioni tradizionali	19
2.2	Meccanismi di voto nelle DAO e nelle organizzazioni convenzionali . .	23
2.3	Principali differenze tra gli standard ERC-20 ed ERC-721	30
3.1	Tabella delle variabili estratte	40
3.2	Lista degli indirizzi dei contratti di governor di Uniswap nel tempo .	48
3.3	Parametri di governance di Uniswap	49
3.4	Lista indirizzi dei contratti di Uniswap attualmente in uso	49
3.5	Lista indirizzi dei contratti su Arbitrum One ChainID:42161	55
3.6	Parametri usati nel processo di governance di Arbitrum DAO	57
3.7	Lista indirizzi dei contratti di Aave attualmente in uso.	64
3.8	Parametri del processo di governance di Aave	65
3.9	Parametri di governance dei contratti di Sky	72
3.10	Lista indirizzi dei contratti coinvolti nel protocollo di Sky	72
3.11	Parametri proposte e votazioni di Curve DAO	78
3.12	Lista indirizzi dei contratti coinvolti nel protocollo di Curve DAO . .	79
3.13	Parametri proposte e votazioni on-chain di Lido DAO	85
3.14	Parametri della dual governance di Lido DAO	85
3.15	Lista indirizzi dei contratti coinvolti nel protocollo di Lido DAO . . .	86
3.16	Parametri di governance di ENS DAO	92
3.17	Lista indirizzi dei contratti di ENS DAO	92
3.18	Parametri proposte di DeXe DAO	99

3.19	Lista indirizzi dei contratti di DeXe DAO	100
3.20	Attuali parametri di governance di Compound	104
3.21	Lista indirizzi dei contratti di Compound	105
3.22	Parametri di governance di Maple Finance	109
3.23	Lista indirizzi dei contratti in uso di Maple Finance	110
3.24	Parametri di governance di Wormhole	115
3.25	Lista indirizzi dei contratti in uso di Wormhole	115
3.26	Parametri considerati per la governance di Diva Staking	122
3.27	Lista indirizzi dei contratti di Diva Staking	122
3.28	Parametri considerati per la governance di Braintrust	127
3.29	Lista indirizzi dei contratti di Braintrust	127
3.30	Parametri considerati per la governance di UMA	134
3.31	Lista indirizzi dei contratti attualmente in uso di UMA	135
3.32	Parametri della governance e delle aste di PoohCrew DAO	138
3.33	Lista indirizzi dei contratti di PoohCrew DAO	139
3.34	Parametri relativi al processo di governance di POOH	140
3.35	Lista indirizzi dei contratti della DAO primaria di POOH	141
3.36	Parametri relativi al processo di governance di Adventure Gold	145
3.37	Lista indirizzi dei contratti coinvolti nella governance di AGLD	145
3.38	Regole Streamonomics di Degen Dogs DAO	147
3.39	Parametri del processo di governance di Degen Dogs DAO	150
3.40	Lista indirizzi dei principali contratti di Degen Dogs	151
3.41	Parametri per la gestione della governance di Dope Wars	155
3.42	Lista indirizzi dei principali contratti di Dope Wars	155
3.43	Parametri principali del processo di governance di Hop	158
3.44	Lista indirizzi dei principali contratti di Hop	158
3.45	Parametri principali del processo di governance di onchainaustria	165
3.46	Lista indirizzi dei principali contratti di onchainaustria	165
3.47	Parametri principali del processo di governance di RARI DAO	172
3.48	Lista indirizzi dei principali contratti di RARI DAO su RARI Chain	172
3.49	Parametri principali del processo di governance di Inverse Finance	178
3.50	Lista indirizzi degli attuali contratti di governance di Inverse Finance	178

3.51	Parametri regolamentanti le aste di Public Nouns	181
3.52	Parametri principali del processo di governance di Public Nouns . . .	182
3.53	Lista indirizzi principali che gestiscono Public Nouns DAO	183
3.54	Parametri principali della governance di Unlock	186
3.55	Lista indirizzi contratti di governance di Unlock DAO su Base	188
3.56	Parametri principali del processo di governance di Hifi Finance	190
3.57	Lista indirizzi contratti di governance di Hifi Finance	191
3.58	Parametri usati nel processo di governance di Fluence DAO	195
3.59	Lista indirizzi contratti di governance di Hifi Finance	196
3.60	Parametri usati nel processo di governance di Gitcoin	201
3.61	Lista indirizzi contratti di governance di Gitcoin	201
3.62	Parametri usati nel processo di governance di GMX	204
3.63	Lista indirizzi contratti di governance della GMX.DAO	205
3.64	Parametri usati nel processo di governance di Tornado.Cash	210
3.65	Indirizzi degli attuali contratti di governance di Tornado.Cash	210
3.66	Parametri usati per l'esecuzione delle proposte di KyberDAO	215
3.67	Indirizzi degli attuali contratti di governance di KyberDAO	215
3.68	Parametri usati nel processo di governance di Audius	220
3.69	Indirizzi degli attuali contratti di governance di Audius	220
3.70	Parametri usati nel processo di governance di Ampleforth	225
3.71	Indirizzi degli contratti di governance di Ampleforth	225
3.72	Parametri usati nel processo di governance di Radworks	231
3.73	Indirizzi degli contratti di governance di Radworks attualmente in uso	231
3.74	Parametri usati nel processo di governance di Idle	235
3.75	Indirizzi degli contratti di governance di Idle DAO	236
3.76	Parametri usati nel processo di governance di HAI	240
3.77	Indirizzi degli contratti di governance di HAI DAO	241
3.78	Parametri usati nel processo di governance di Union	244
3.79	Indirizzi degli contratti di governance di Union	245
3.80	Parametri usati nel processo di governance di OpenDollar	248
3.81	Indirizzi degli contratti di governance di OpenDollar	248
3.82	Indirizzi degli contratti di governance di Cryptex	251

3.83 Parametri usati nel processo di governance di Cryptex	252
3.84 Indirizzi degli contratti di governance di Threshold Network	255
3.85 Parametri di governance di Threshold Network	256
3.86 Parametri di governance di Anvil	259
3.87 Indirizzi degli contratti di governance di Anvil	259
3.88 Parametri di governance di TrueFi	264
3.89 Indirizzi degli contratti di governance di TrueFi	264
3.90 Parametri del processo di governance di PoolTogether	269
3.91 Indirizzi degli contratti di governance di PoolTogether	269
3.92 Indirizzi degli contratti di governance di Seamless	274
3.93 Parametri del processo di governance di Seamless	275
3.94 Indirizzi degli contratti di governance di Antfarm	279
3.95 Parametri del processo di governance di Antfarm	280
3.96 Parametri del processo di governance di Lazy Summer	284
3.97 Indirizzi degli contratti di governance di Lazy Summer	284
3.98 Parametri del processo di governance di RealToken Ecosystem	287
3.99 Indirizzi degli contratti di governance di RealToken Ecosystem	288
3.100 Parametri del processo di governance di FAMEus DAO	291
3.101 Indirizzi degli contratti di governance di FAMEus DAO	291
3.102 Parametri del processo di governance di RigoBlock	294
3.103 Indirizzi degli contratti di governance di RigoBlock	295
3.104 Parametri del processo di governance di Lisk	298
3.105 Indirizzi degli contratti di governance di Lisk	298
3.106 Identificazione delle 50 DAO: Da 1 a 25	299
3.107 Identificazione delle 50 DAO: Da 26 a 50	300
3.108 Parametri di governance delle 50 DAO: Da 1 a 25	301
3.109 Parametri di governance delle 50 DAO: Da 26 a 50	302
3.110 Gestione finanziaria e contratti delle 50 DAO: Da 1 a 25	303
3.111 Gestione finanziaria e contratti delle 50 DAO: Da 26 a 50	304
4.1 Distribuzione per categoria	305
4.2 Distribuzione per categoria	306

4.3	Distribuzione token standard	308
4.4	Statistiche descrittive parametri di governance	308
4.5	Medie parametri per categorie	309
4.6	Mediane parametri per categorie	310
4.7	Distribuzione governor proxy pattern	315
4.8	Distribuzione aggiornabilità del contratto governor	315

Introduzione

L'avvento della tecnologia blockchain e la maturazione degli ecosistemi decentralizzati hanno dato origine a nuovi paradigmi che sfidano la concezione tradizionale di organizzazione. Al centro di questa evoluzione si collocano le Decentralized Autonomous Organizations (DAO), sistemi che mirano a sostituire le strutture decisionali centralizzate con protocolli di governance codificati in smart contract e registrati su registri distribuiti. In un contesto in cui la fiducia non è più riposta in un autorità centrale, ma nella verificabilità del codice, le DAO rappresentano il tentativo più ambizioso di realizzare un'autogestione collettiva, trasparente e resistente alla censura. Il presente lavoro di tesi si pone l'obiettivo di analizzare criticamente l'architettura di governance e le dinamiche operative di queste organizzazioni (seguendo il metodo proposto in [39]), cercando di colmare il divario tra la teoria riportata nella documentazione e l'implementazione on-chain dei processi decisionali attraverso un rigoroso studio dei codici che definiscono gli smart contracts.

Il percorso di ricerca si articola in tre fasi fondamentali, tra loro strettamente interconnesse. La prima parte è dedicata a una disamina teorica dei pilastri fondanti delle DAO, analizzando gli aspetti che ne definiscono l'identità giuridica e tecnologica: dalla natura degli smart contract ai meccanismi di consenso e di votazione. Questa base teorica è essenziale per inquadrare il primo interrogativo della ricerca, volto a indagare in che misura i modelli di governance implementati on-chain riflettano effettivamente i principi di decentralizzazione dichiarati nelle documentazioni ufficiali oppure se, al contrario, tenda a riprodurre vecchie dinamiche di potere in una nuova veste digitale.

La seconda parte del lavoro consiste nell'analisi di un campione selezionato di 50 DAO finalizzata alla creazione di un dataset organico che, attraverso un processo di normalizzazione dei dati, sia in grado di tradurre in metriche comuni e confrontabili le informazioni eterogenee estratte da architetture blockchain distinte. Tale operazione risulta essenziale per superare la frammentazione informativa e l'assenza di standard metodologici che attualmente precludono una comparazione sistematica tra i diversi modelli di governance decentralizzata.

Infine, l'ultima sezione della tesi è dedicata all'analisi statistica dei dati raccolti. Superando la fase puramente descrittiva, le informazioni estratte dalla blockchain vengono normalizzate ed elaborate per identificare pattern ricorrenti e modelli comportamentali. Questa analisi quantitativa permette di rispondere all'ultimo quesito della ricerca, ovvero quali siano i principali schemi decisionali che emergono dall'evidenza dei dati e in che modo questi influenzino l'operatività dell'organizzazione e la gestione del patrimonio delle DAO analizzate.

In conclusione, questo approccio multidimensionale non intende solo mappare lo stato dell'arte delle DAO, ma fornire una base oggettiva e verificabile per valutare se i modelli di autogoverno siano pronti a sostenere la prossima fase di evoluzione del Web3, contribuendo alla letteratura esistente con un approccio basato sull'evidenza quantitativa dei dati.

Capitolo 1

Blockchain

1.1 Introduzione alla crittografia asimmetrica

La crittografia (dal greco *kryptòs* = nascosto e *graphè* = scrittura) è costituita da un insieme di procedure ideate allo scopo di nascondere ad utenti esterni il significato di un messaggio scambiato tra un mittente ed un destinatario. Essa costituisce la base della protezione dei dati ed il miglior modo per evitare che le informazioni vengano intercettate o rubate da qualcuno non autorizzato.

La crittografia si divide in due categorie principali:

- la *crittografia simmetrica* o *crittografia a chiave privata*,
- la *crittografia asimmetrica* o *crittografia a chiave pubblica*.

Andiamo quindi ad analizzare le caratteristiche di queste due categorie, evidenziandone in particolare le principali differenze [1].

Iniziamo descrivendo la crittografia a chiave privata che fino a pochi decenni fa era l'unico metodo crittografico esistente. Come si evince dalla Figura 1.1 la caratteristica principale di questa tecnica è l'utilizzo delle medesime chiavi crittografiche sia per codificare il testo in chiaro, sia per decodificare il testo cifrato. Tale aspetto rende gli algoritmi di codifica a chiave privata molto performanti e semplici da implementare.

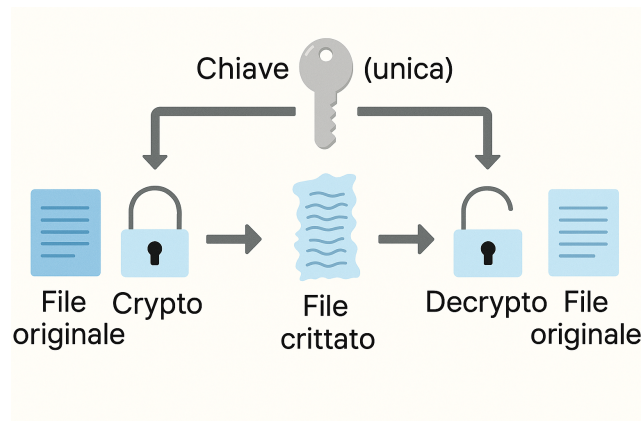


Figura 1.1: Crittografia simmetrica.

Le chiavi possono essere identiche, oppure può essere necessaria una semplice trasformazione per passare da una chiave all'altra. Le chiavi di cui dispongono le due parti rappresentano sostanzialmente un segreto condiviso che può essere utilizzato per mantenere un collegamento privato tra mittente e destinatario.

I problemi principali di questo tipo di crittografia sono due:

- la prima questione è lo *scambio delle chiavi*: ad un certo punto infatti la chiave comune deve essere scambiata tra le due parti, quindi esisterà almeno un momento in cui una terza parte potrebbe impossessarsene. L'intercettazione permetterebbe a quest'ultimo non solo di decodificare i messaggi cifrati ma anche di generare falsi messaggi o alterare gli originali senza che il destinatario possa scoprirlo.
- il secondo problema è legato al fatto che il numero di chiavi necessarie aumenta con il numero di utenti che partecipano allo scambio di informazioni, ad esempio se si considera una rete con n interlocutori, le chiavi necessarie sono $\frac{n(n-1)}{2}$. In generale per n grande, il numero di chiavi sarà $\approx n^2$.

Per risolvere tali problemi nasce la crittografia a chiave pubblica. In tale metodo, come evidenziato nella Figura 1.2, ad ogni utente coinvolto nella comunicazione è associata una coppia di chiavi:

- la chiave pubblica, che viene distribuita;
- la chiave privata, che resta personale e segreta.

Se la prima chiave viene utilizzata per la codifica del messaggio, allora quest'ultimo potrà essere decodificato soltanto con la seconda o viceversa.

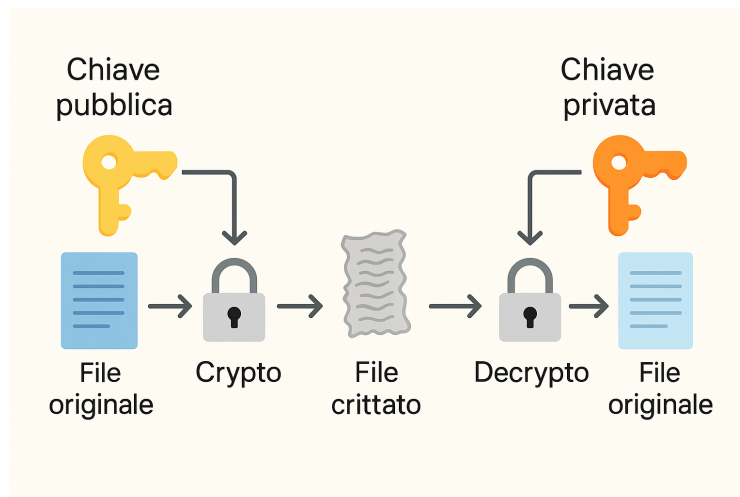


Figura 1.2: Crittografia asimmetrica.

La sicurezza di questo tipo di sistema crittografico risiede quindi nella segretezza della chiave privata, mentre la chiave pubblica può essere condivisa senza compromettere in alcun modo la comunicazione; con tale approccio si evita quindi qualunque problema connesso alla necessità di scambiare le chiavi mediante un canale sicuro.

I sistemi crittografici a chiave pubblica si basano su una categoria di problemi matematici per i quali non risulta noto alcun algoritmo in grado di risolverli in maniera efficiente.

Tra i più usati ricordiamo il problema della fattorizzazione in numeri primi e il problema del logaritmo discreto. Di fatto anche utilizzando i più potenti sistemi di calcolo oggi a disposizione la risoluzione di questi problemi potrebbe richiedere migliaia di anni.

1.2 La tecnologia blockchain

La blockchain (letteralmente "catena di blocchi") è una tecnologia decentralizzata basata su una DLT (Distributed Ledger Technology) che consente di registrare dati e transazioni in modo sicuro, immutabile e trasparente, senza la necessità di un'autorità centrale o intermediari. Una blockchain lavora su una rete peer-to-peer in cui ogni nodo della rete ha la stessa copia del registro della blockchain [2].

Si tratta dunque di una struttura dati che consiste in una serie di blocchi concatenati, ognuno dei quali contiene un insieme di transazioni o informazioni, un timestamp (marcatura temporale), e un riferimento crittografico al blocco precedente. E' sempre solo possibile aggiungere nuovi blocchi mentre non è possibile modificare o eliminare blocchi precedentemente inseriti.

Questa architettura rende la blockchain resistente alla manomissione e particolarmente adatta alla gestione di dati sensibili o alla certificazione di eventi.

In ambito blockchain al fine di garantire la sicurezza e la privacy della rete e degli utenti viene utilizzata principalmente la crittografia a chiave pubblica sia per collegare tra loro i blocchi della catena, sia per generare e firmare le transazioni in essi contenuti.

1.2.1 Caratteristiche di una blockchain

Ora che abbiamo introdotto il concetto di blockchain ed abbiamo fornito una descrizione generale di questa innovativa tecnologia andiamo a delinearne le caratteristiche chiave [4]:

Decentralizzazione Le transazioni nelle blockchain vengono elaborate e validate tramite il consenso dei nodi della rete, con metodi diversi a seconda del protocollo di consenso associato alla rete specifica. Tali transazioni e le informazioni relative alla rete vengono poi registrate e replicate in ognuno dei nodi andando a generare un registro di tipo distribuito. Questo elimina la necessità di un'autorità centrale che permetta di condividere e gestire i dati delle transazioni.

Immutabilità Le transazioni all'interno di una blockchain sono archiviate in blocchi. Ogni blocco nella catena è collegato al precedente tramite una funzione di hash crittografica. Qualsiasi tentativo di modifica del contenuto di un blocco influenzerà i blocchi successivi nella catena. Di conseguenza se un attaccante malevolo dovrebbe modificare tutti i blocchi successivi per alterare un blocco specifico, cosa computazionalmente molto difficile poiché i blocchi concatenati sono replicati su più nodi per via della struttura a registro distribuito. Possiamo quindi concludere che nel momento in cui una transazione è stata registrata sulla blockchain attraverso l'inserimento in un blocco, essa diventa permanente e non può essere modificata o eliminata. Questo garantisce l'integrità e l'affidabilità delle informazioni archiviate.

Trasparenza Il registro viene aggiornato solo nel momento in cui viene raggiunto il consenso. Quando l'aggiornamento viene apportato, i cambiamenti nella rete possono essere scaricati da ogni nodo e risultano quindi visibili pubblicamente da ogni utente, garantendo trasparenza e sicurezza.

Tracciabilità La natura distribuita e trasparente della blockchain rende possibile tracciare l'intero storico di ogni transazione. Ogni aggiornamento dello stato di un bene o di ogni transazione può quindi essere rintracciato fino alla sua origine. Questo contribuisce a rendere la rete più sicura, efficiente e trasparente.

Anonimato e sicurezza La sicurezza e l'anonimato nel contesto blockchain sono garantiti dal fatto che le transazioni sono crittografate così come le identità dei partecipanti della rete. Le transazioni quindi avvengono tra parti sconosciute che non si fidano reciprocamente ed è la struttura a registro distribuito unita all'uso dei protocolli di consenso a garantire la validità delle transazioni in un ambiente privo di fiducia.

1.2.2 Struttura della blockchain

La struttura di ogni blockchain come detto è costituita da una catena di blocchi, i quali contengono una lista di transazioni più diverse informazioni aggiuntive che

vengono utilizzate per caratterizzare univocamente il blocco che sono contenute nell'header Tabella 1.1.

Campo	Descrizione
Nonce	Numero casuale o pseudocasuale che viene utilizzato per generare un hash del blocco.
Hash blocco precedente	Un riferimento all'hash del blocco precedente.
Hash del Merkle Root	Hash della radice del Merkle Tree delle transazioni del blocco corrente.
Timestamp	Ora approssimativa di creazione del blocco corrente.

Tabella 1.1: Struttura dell'header di un blocco

L'header di ogni blocco della catena in particolare contiene un riferimento al blocco precedente realizzato tramite l'applicazione di una funzione hash, che rende sempre possibile risalire ai blocchi precedenti fino ad arrivare se necessario al blocco genesi ovvero il primo blocco, quello da cui è partita l'intera struttura.

Andiamo ora a definire con più precisione cosa sono le funzioni hash e come vengono utilizzate nel contesto delle blockchain per la creazione di merkle tree per crittografare transazioni ed identità degli utenti [5].

Funzioni hash

Definizione 1.1. *Una funzione hash è una funzione $h : D \rightarrow R$, con dominio $D = \{0, 1\}^*$ e codominio $R = \{0, 1\}^n$ per qualche $n \geq 1$. [6]*

Sono dunque definite come funzioni che comprimono una stringa in input arbitraria generando in output una stringa di lunghezza fissa. Inoltre se tali funzioni soddisfano anche alcuni requisiti aggiuntivi tali funzioni hash possono essere utilizzate

per applicazioni crittografiche e prendere il nome di "funzioni hash crittografiche". Le caratteristiche aggiuntive che rendono una funzione hash applicabile in ambito crittografico sono le seguenti:

- Data h ed x (un qualsiasi input) risulti semplice calcolarne la hash $h(x)$.
- Dati h ed $h(x)$ è computazionalmente impossibile trovare x .
- Dati h ed $h(x)$ è computazionalmente impossibile trovare una collisione, ovvero trovare x ed x' tali che $h(x) = h(x')$.

In ogni blocco infatti abbiamo già visto che compaiono la hash del blocco precedente, più precisamente dell'header e la hash del merkle root del merkle tree delle transazioni del blocco precedente, come riportato in Figura 1.3; l'uso delle funzioni hash quindi permette di garantire la validità e l'integrità dei dati all'interno del sistema, questo perché ogni modifica dei dati in un blocco genererebbe una modifica di tutte le hash dei blocchi successivi spezzando dunque l'intera catena e rendendo la modifica visibile da tutti i nodi nel sistema.

Merkle tree Sfruttando le funzioni hash è possibile costruire una struttura dati chiamata Merkle tree [5].

I Merkle Tree servono per rappresentare un blocco di dati, ad esempio l'insieme delle transazioni contenute in un blocco, sotto forma di albero, in cui ogni nodo contiene la hash del suo nodo figlio eccetto per i nodi foglia che contengono i dati originali che sono stati inseriti nel blocco.

Ogni utente dunque per verificare un blocco deve solamente verificare la hash contenuta nel Merkle Root (nodo radice del Merkle Tree) poiché anche la minima variazione in una singola transazione (nodo foglia) porterebbe a variazioni a cascata nelle hash successive producendo un valore nel Merkle Root completamente differente. L'integrità dei dati dunque può essere efficientemente verificata calcolando la hash e verificando che questa coincida con quella fornita.

Tramite l'uso delle funzioni hash e delle strutture Merkle tree nell'header di ogni blocco abbiamo un collegamento al blocco precedente della catena ed anche un collegamento ai dati contenuti nel corpo del blocco stesso.

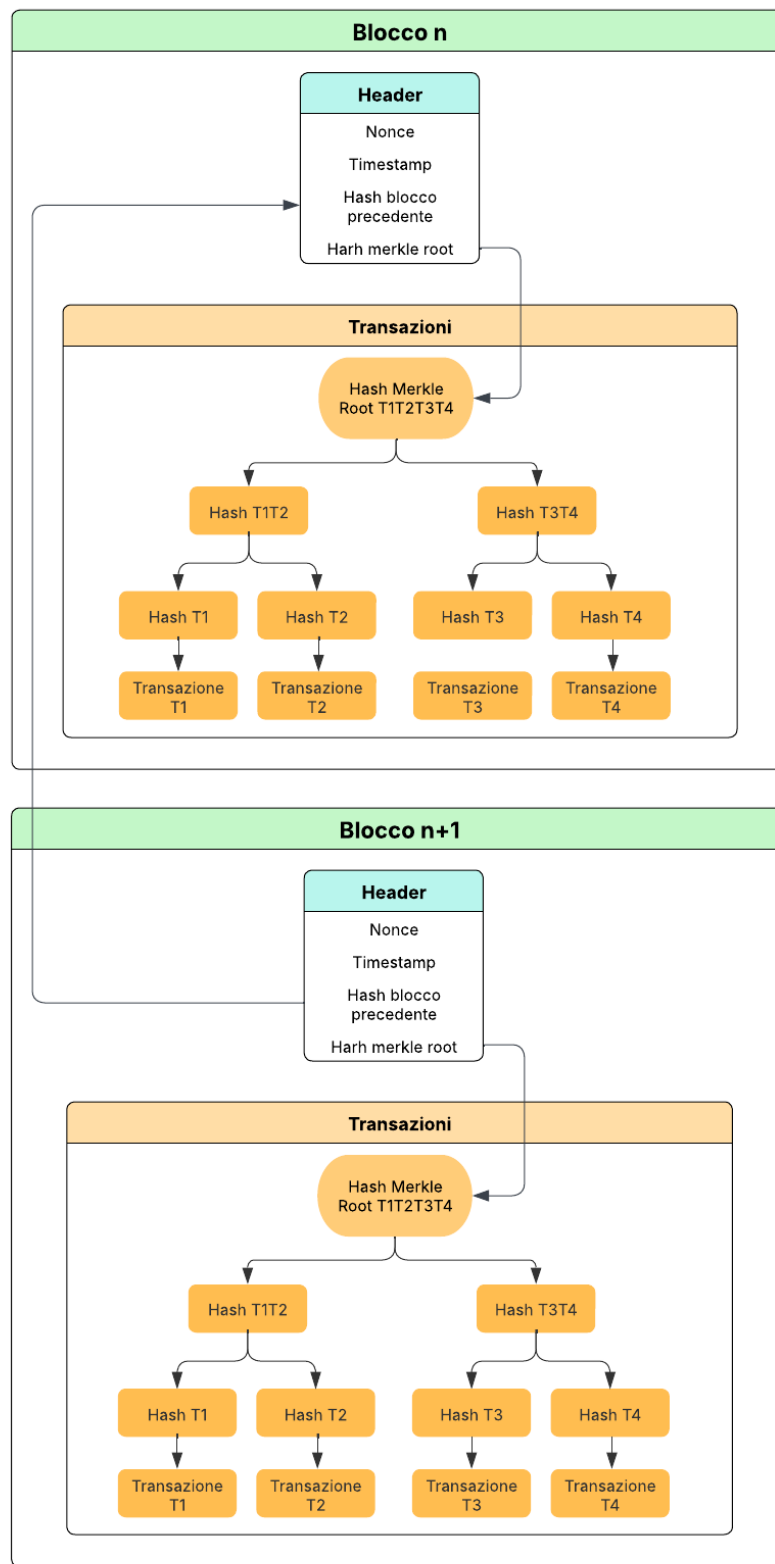


Figura 1.3: Struttura dei blocchi in una blockchain.

1.2.3 Protocolli di consenso

Gli algoritmi di consenso possono essere considerati il cuore di tutte le transazioni delle blockchain [7], infatti, in un sistema blockchain gli algoritmi di consenso sono usati per creare fiducia tra i membri e memorizzare correttamente le transazioni sui blocchi.

Un protocollo di consenso è essenzialmente un insieme di regole che ogni partecipante deve seguire. Essendo una tecnologia distribuita, priva di fiducia universale, la blockchain necessita di un meccanismo di consenso distribuito affinché tutti i partecipanti concordino sullo stato attuale della blockchain.

Tra gli algoritmi di consenso più comuni utilizzati nelle principali blockchain presentiamo i seguenti.

Proof-of-Work (PoW) La PoW seleziona un problema che può essere risolto solo per tentativi. Ad esempio, quando è il momento di creare e convalidare un blocco, il problema consiste nell'indovinare un valore del nonce in modo tale che, utilizzando i dati della transazione e il valore del nonce come input per una funzione hash, il suo output debba rientrare nel range previsto della difficoltà, ad esempio iniziando con quattro zeri iniziali. Le funzioni di hash dunque assumono un ruolo chiave nell'implementazione dell'algoritmo della PoW; la rete Bitcoin ad esempio adotta la funzione di hash crittografica SHA-256 [8].

Con la PoW ogni nodo (chiamato anche nodo di mining) sulla rete ora effettua diversi tentativi in modo casuale al fine di indovinare il nonce corretto, tale processo procede in modo parallelo su tutti i nodi che cercano di minare il blocco finché uno di questi non trova per primo il valore del nonce che corrisponde alla difficoltà prevista. Ogni nodo di mining dunque va a investire molte risorse computazionali (da qui il termine "lavoro") al fine di risolvere il problema più velocemente degli altri e quindi validare il blocco da collegare alla Blockchain e ottenere una ricompensa, che spesso consiste in un certo quantitativo di criptovaluta. Due esempi di Blockchain pubbliche che usano la PoW come algoritmo di consenso sono quelle di Bitcoin ed Ethereum.

Un grosso problema con il processo di consenso PoW è che richiede molto tempo ed elettricità per essere completato.

Proof of Stake (PoS) La PoS è il secondo algoritmo di consenso più diffuso.

La PoS risolve i problemi di tempo e consumo di elettricità della PoW in cui il fabbisogno di elettricità è associato alla ricerca di un nonce da parte dei miner il che come detto processo un investimento in termini di risorse e tempo. Nella PoS invece i nodi per validare un nuovo blocco devono bloccare in stake una certa quantità di criptovaluta per essere scelti e poter inserire il nuovo blocco.

Quando un blocco viene selezionato per l'inserimento, il creatore riceverà le commissioni delle transazioni presenti nel blocco. Se il vincitore per l'inserimento del blocco tenta di inserirne uno non valido, perderà la sua puntata, ovvero la criptovaluta che aveva bloccato in stake.

Un esempio di utilizzo della PoS lo troviamo in seguito alla prima fase di aggiornamento a Ethereum 2.0, in cui i "computer mondiali" della blockchain passano dall'algoritmo di consenso PoW a quello PoS.

Delegated Proof-of-Stake (DPoS) Nella DPoS, tutti i possessori di token possono votare un certo numero di delegati, i quali possono anche delegare ad altri utenti il loro potere di voto partecipando quindi alla scelta di quelli che saranno i validatori dei blocchi. Maggiore è il numero di token posseduti da un utente, maggiore sarà il suo potere di voto. I delegati sono quindi responsabili della convalida delle transazioni e dei blocchi al fine di proteggere la rete.

A differenza della maggiore potenza di calcolo della PoW o del maggior numero di token della PoS, nella DPoS a decretare i validatori dei blocchi sono è il potere di voto acquisito dal possesso dei propri token e dalle deleghe acquisite dagli altri utenti. Un esempio di utilizzo della DPoS lo possiamo riscontrare in EOS.

Wisdom of the crowd Il meccanismo di consenso della "saggezza della folla" (wisdom of the crowd) si basa sull'idea che la media delle opinioni di un gruppo numeroso e diversificato di individui possa essere più accurata di quella di un singolo esperto. Per funzionare correttamente, questo meccanismo richiede che si considerino persone con prospettive e conoscenze diverse che prendano decisioni in modo indipendente. L'intelligenza collettiva emerge dalla sintesi delle decisioni prese dai singoli individui.

Proof of Elapsed Time (PoET) Intel Corporation ha sviluppato PoET al fine di definire un nuovo metodo per determinare un vincitore per l'estrazione di un blocco. Nella PoET, ad ogni potenziale nodo di convalida viene richiesto di attendere per un tempo di attesa casuale che viene generato da una piattaforma di elaborazione affidabile, ad esempio SGX di Intel. Il primo nodo che raggiunge il completamento del tempo di attesa è il vincitore della convalida ed è in grado quindi di aggiungere il nuovo blocco. Utilizzando una piattaforma di elaborazione affidabile viene garantito che ogni nodo abbia la possibilità di essere il vincitore.

Practical Byzantine Fault Tolerant (PBFT) La tolleranza ai guasti bizantina (BFT) serve a risolvere il noto problema dei generali bizantini i quali devono raggiungere un accordo per decidere quale politica seguire tenendo in considerazione che nell'insieme dei generali ne sono presenti alcuni disonesti. Il PBFT è un algoritmo di consenso che ottimizza il BFT. Nel PBFT, finché i nodi dannosi o ostili siano meno di un terzo di tutti i nodi nel sistema blockchain. Più nodi ci sono nel sistema blockchain, più sicura risulterà essere la blockchain.

Un esempio di utilizzo del PBFT è Hyperledger Fabric.

Grafo aciclico diretto (DAG) I DAG sono grafi costituiti da vertici e archi orientati in quanto puntano in una specifica direzione e sono aciclici perché i vertici non possono in alcun modo ricollegarsi a se stessi.

Ogni vertice nella struttura rappresenta una transazione. Non esiste il concetto di blocco e non è necessario il mining per aggiungere transazioni, infatti invece di raccogliere le transazioni in blocchi, ogni transazione viene costruita l'una sopra un'altra. Tuttavia, viene eseguita una piccola operazione PoW quando un nodo invia una transazione. Questo garantisce che e convalida non vengano inserite transazioni non valide nella rete e permettono anche la validazione delle transazioni precedenti.

IOTA è un esempio di utilizzo dei DAG come protocollo di consenso.

Quelli presentati non sono gli unici protocolli di consenso, ne esistono ancora molti altri come ad esempio PoA (Proof-of-Authority), in cui ad essere messa a confronto è la reputazione dei vari nodi oppure la PoB (Proof-of-Burn) in cui invece si va

a considerare la quantità di criptovaluta bruciata dai vari nodi oppure ancora PoI (Proof-of-Importance) in cui si valutano i punteggi di importanza dei vari nodi.

1.2.4 Classificazione delle blockchain

Nel progettare una struttura di governance efficace per una blockchain, è fondamentale tenere conto della configurazione del registro. A seconda degli obiettivi del sistema, il registro può essere amministrato da un'entità centrale oppure può funzionare in modo decentralizzato, seguendo regole condivise e rispettate da tutti i partecipanti alla rete.

La governance definisce i meccanismi per la gestione delle autorizzazioni e delle policy di controllo, stabilendo chi può accedere o utilizzare determinate risorse all'interno della blockchain. Si tratta di un insieme di normative che regolano i permessi degli utenti, dei nodi e del sistema stesso, con particolare attenzione alla sicurezza.

Le blockchain possono differenziarsi in base ai livelli di accesso e controllo sui dati, ed è secondo questi criteri che possiamo andare a suddividerle nelle seguenti tre categorie [3]:

- *Pubbliche (permissionless)*: Sono delle reti a cui chiunque può accedere senza dover chiedere il permesso di partecipare a nessuno. E' decentralizzata, non c'è quindi nessuna autorità centrale che controlla la rete. Tutti i nodi sono dotati dei medesimi diritti e poteri, chiunque può quindi effettuare verifiche su qualunque transazione.
- *Private (permissioned)*: Queste reti sono gestite da un'individuo o da un gruppo di individui che ne costituiscono l'autorità, i quali decidono chi può partecipare alla rete e che tipo di apporto può applicare. Sono gli utenti dotati dell'autorità ad avere la responsabilità sulla sicurezza dei nodi esistenti e che verificano i nuovi nodi.
- *A consorzio*: Sono reti prive della necessità di un'autorizzazione per l'accesso e sono decentralizzate ma solo ad una parte preselezionata dei nodi è consentito di partecipare al processo gestionale.

Capitolo 2

Decentralized Autonomous Organization (DAO)

2.1 Storia delle DAO

La teoria sulle organizzazioni ha una vasta letteratura relativa a quelle decentralizzate, tuttavia, i primi riferimenti a vere e proprie Decentralized Autonomous Organization (DAO) emersero solo negli anni '90 per descrivere sistemi multi-agente in un ambiente di Internet-of-Things (IoT).

Il significato moderno di DAO in realtà può essere fatto risalire al concetto precedente di Decentralized Autonomous Corporation (DAC), coniato alcuni anni dopo l'apparizione di Bitcoin (2008) [9]. Le DAC erano descritte come una nuova forma di governance aziendale, che utilizzava azioni tokenizzate e commerciabili come mezzo per fornire dividendi agli azionisti. Tali corporazioni erano descritte come “incorruttabili”, in quanto operavano “senza alcun coinvolgimento umano” e con “statuti pubblicamente consultabili” come “software open source distribuito sui computer dei loro stakeholder”. Secondo questa definizione, qualunque utente poteva diventare un stakeholder in una DAC semplicemente comprando azioni della società e venendo ricompensato per il servizio fornito alla comunità. Di conseguenza, i proprietari delle azioni di una DAC avrebbero diritto a “una parte dei suoi profitti, partecipazione alla sua crescita e/o su come viene gestita”.

Anche se alcuni sostengono che la rete Bitcoin sia la prima DAO mai esistita, dato che la rete si sviluppa tramite accordo comunitario e che i partecipanti siano distribuiti a livello globale, il termine DAO è oggi inteso come riferito non a una rete blockchain in sé, ma piuttosto a organizzazioni implementate come smart contracts sopra una rete blockchain esistente e Bitcoin non ha un meccanismo di governance organizzato e quindi non può essere considerata una DAO secondo gli standard odierni.

La prima DAO in assoluto, secondo la maggioranza fu "The DAO" creata nel 2016 da un'azienda chiamata Slock.it sulla blockchain di Ethereum [10], [11]. Questa azienda puntava originariamente a fornire un servizio che permettesse alle persone di affittare, vendere o condividere le proprie proprietà senza intermediari utilizzando la tecnologia blockchain. Per il loro scopo hanno quindi creato una DAO simile a una piattaforma di raccolta fondi come Kickstarter o GoFundMe, ma con una differenza fondamentale: hanno concesso a tutti gli investitori/membri il diritto di voto sul modo in cui spendere il capitale raccolto, istituendo così un nuovo modello di governance. "The DAO" arrivò a raccogliere oltre 150 milioni di dollari in ether da 11.000 membri, detenendo all'epoca circa il 14% di tutti gli ether in circolazione, ma nel giugno 2016 subì un attacco informatico, che portò ad una perdita di circa 3,6 milioni di ether (circa 50 milioni di dollari all'epoca). Per limitare l'impatto di questo hack, la comunità decise di fare un hard fork della blockchain generando quindi due blockchain separate: Ethereum ed Ethereum Classic

2.2 Definizione e caratteristiche

Come prima cosa andiamo a fornire una definizione di DAO secondo [9].

Definizione 2.1. *Una DAO è un sistema basato su blockchain che consente alle persone di coordinarsi e governarsi in modo autonomo, mediato da un insieme di regole autoesecutive implementate su una blockchain pubblica, e la cui governance è decentralizzata (cioè, indipendente dal controllo centrale).*

Le proprietà principali che caratterizzano le DAO [10], [14], [13] sono le seguenti:

- **Decentralizzazione:** Essendo tutto basato su una rete decentralizzata e distribuita, non vi è più un'autorità centrale e l'organizzazione è completamente gestita dai nodi della rete.
- **Automazione:** Le regole dell'organizzazione vengono implementate tramite l'uso di programmi informatici auto-esecutivi (smart contract) attraverso i quali è anche possibile controllare le attività dell'organizzazione senza la necessità di interazioni umane.
- **Trasparenza e Persistenza:** Il codice che esegue una DAO è open source e può essere verificato da chiunque. È anche possibile consultare la cronologia per vedere come sono state prese le decisioni fin dalla nascita dell'organizzazione, infatti una volta che una transazione è stata inserita in un registro, non può essere eliminata o modificata (rollback).
- **Anonimato:** Dato che le DAO sono generalmente costruite su blockchain pubbliche si basano sulla crittografia asimmetrica e sull'hashing crittografico dei dati della blockchain rendendo anonime le operazioni.
- **Verificabilità:** I dati della blockchain possono essere accessibili e tracciati per verificare e rintracciare tutte le transazioni precedenti sempre grazie agli strumenti di crittografia asimmetrica utilizzati per la loro generazione.
- **Resistenza alla Censura:** Nessuna autorità, compresi i governi, può chiudere o interferire con una DAO poiché gestita da una rete decentralizzata di nodi i quali operano essi stessi come gestori e autorità sull'organizzazione.
- **Democrazia:** Chiunque, ovunque nel mondo, può entrare a far parte di una DAO e contribuire ad essa nel modo che preferisce. Qualsiasi investitore o membro di una DAO può inoltre fare proposte o partecipare a votazioni al fine di determinare il futuro dell'organizzazione.

Alcune di queste caratteristiche sono più aspirazionali che realisticamente realizzabili; nella pratica infatti molte DAO non rispecchiano perfettamente tutte le caratteristiche ideali delineate in questo elenco, ognuna di esse può dare priorità a determinati

aspetti rispetto ad altri, risultando così in strutture che possono incarnare solo alcune di queste caratteristiche.

2.2.1 Confronto con le Organizzazioni tradizionali

Considerando le principali proprietà presentate nel paragrafo precedente andiamo a confrontare le DAO e le organizzazioni di tipo tradizionale (Tabella 2.1), [10] e [13].

DAO	Organizzazioni tradizionali
Completamente democratizzata.	Presenza di una gerarchia e di una qualche forma di autorità centrale.
Prima di essere attuare qualsiasi modifica e/o prendere qualsiasi decisione, viene effettuata una votazione che coinvolge i membri.	Le modifiche possono essere richieste da una singola parte senza coinvolgere gli altri membri oppure possono essere decise votazione.
Le votazioni che vengono svolte sono automatizzate di conseguenza il conteggio dei voti e implementazione del risultato può essere svolto senza la presenza di una terza parte responsabile.	Qualora una decisione venisse presa a seguito di una votazione, i voti verrebbero conteggiati internamente rendendo necessaria la presenza di una terza parte responsabile dell'integrità degli esiti della votazione.
I servizi forniti sono gestiti automaticamente e in modo decentralizzato.	E' necessaria una gestione umana.
Le attività sono trasparenti e completamente pubbliche.	Le attività sono private e limitate al pubblico.
Completamente globali.	Non sono necessariamente globali.

Tabella 2.1: Confronto tra DAO e Organizzazioni tradizionali

2.2.2 Architettura di governance

Prima di poter descrivere l'architettura di governance di una DAO, è opportuno introdurre le definizioni dei tre elementi cardine di quest strutture. Per prima cosa definiamo il concetto di registro distribuito o DLT.

Definizione 2.2. *La DLT, o Distributed Ledger Technology, è un sistema di registro elettronico condiviso, distribuito e sincronizzato tra più partecipanti di una rete, che non ha un'autorità centrale. Ogni nodo possiede una copia del registro e le modifiche vengono convalidate tramite algoritmi di consenso e crittografia, garantendo sicurezza, trasparenza e immutabilità dei dati.*

La tecnologia blockchain come abbiamo già spiegato nel capitolo precedente è una forma particolare di registro distribuito, ma non è l'unica, esistono anche altre forme di implementazione per queste strutture di dati.

Ora definiamo formalmente anche il concetto di smart contract secondo [15].

Definizione 2.3. *Uno smart contract è un codice immutabile che gestisce processi in modo preciso e non soggettivo, che opera in modo predefinito ed automatico in risposta ad eventi specifici, senza la necessità di coinvolgere terze parti per l'esecuzione.*

Gli smart contract possono gestire diversi tipi di transazioni, non solo trasferimenti di tipo monetario e quindi traferimenti di criptovalute, infatti possono anche in particolare definire delle regole, come fossero dei contratti, ed applicarle in modo automatico tramite il codice. In questo modo gli smart contract offrono sicurezza e velocità superiori rispetto alla contrattualistica tradizionale, riducendo i costi di transazione e garantendo autonomia ed efficienza.

Infine formiamo una definizione generale di cosa sia un meccanismo di voto (tale concetto, verrà poi approfondito più nel dettaglio nel paragrafo successivo).

Definizione 2.4. *Un meccanismo di votazione di una DAO è un sistema basato su smart contract che definisce le regole per proporre e votare su decisioni all'interno di un'organizzazione decentralizzata.*

Ora che abbiamo fornito queste definizioni possiamo andare a descrivere l'architettura di governance delle DAO. Secondo [12] tale struttura può essere rappresentata come un triangolo tra registro distribuito, smart contracts e meccanismi di voto. La loro relazione è mostrata in Figura 2.1.

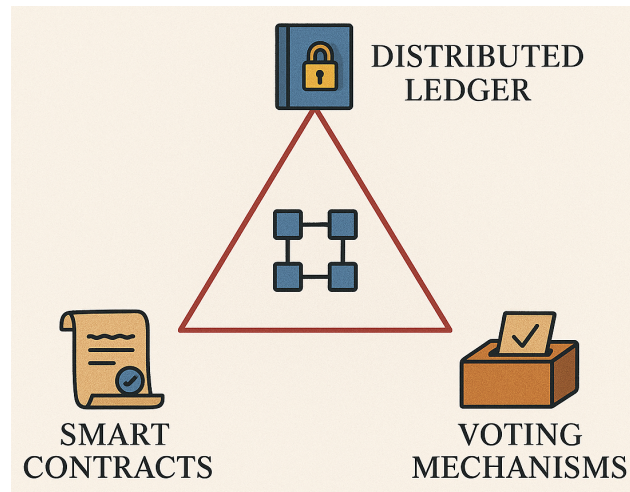


Figura 2.1: Architettura di governance di una DAO

Gli smart contracts sono responsabili della supervisione e dell'implementazione di tutte le regole e contratti nelle DAO, che ovviamente includono anche le regole e le procedure nei meccanismi di voto. Allo stesso tempo, il voto è l'unico modo formale per cambiare le regole definite dagli smart contracts e/o crearne di nuovi. Gli smart contracts e i meccanismi di voto non solo congiuntamente consentono un'armoniosa gestione delle DAO, ma si covincolano a vicenda, rappresentando i punti cardine per il sano funzionamento delle DAO. Il ruolo del registro distribuito è infine quello di registrare le attività critiche svolte dai meccanismi di voto e dagli smart contract, in questo modo il registro distribuito è allineato non solo con i requisiti di decentralizzazione, ma fornisce anche registrazioni coerenti e immutabili.

Le interazioni e i vincoli che si sviluppano tra registro distribuito, smart contracts e meccanismi di voto formano un sistema di governance stabile per le DAO.

2.2.3 Governance

La governance di una DAO è definita come un insieme di regole implementate in smart contracts basati su blockchain, utilizzate per gestire e coordinare strategie e operazioni di un'organizzazione senza la necessità di un'autorità centrale [16]. Ai membri di una DAO sono concessi diritti di voto tramite token di governance per decidere collettivamente a proposito di cambiamenti o aggiornamenti dell'organizzazione stessa. Le votazioni possono riguardare qualsiasi aspetto della governance o delle attività dell'organizzazione, a patto che tali proposte rimangano in accordo con ciò che è consentito dalla DAO [14].

I problemi che la governance di una DAO potrebbe dover affrontare sono i seguenti:

- La necessità di indire votazioni per poter prendere qualsiasi tipo di decisione può rallentare e rendere meno efficiente l'intero processo decisionale.
- Il rischio di un eccessivo accentramento di token di governance nelle mani di pochi individui potrebbe minare il principio di decentralizzazione su cui tali organizzazioni si fondano.
- Non sempre la partecipazione dei membri dell'organizzazione risulta essere sufficiente per poter prendere decisioni che accontentino la maggioranza.

2.2.4 Tesoreria

La tesoreria di una DAO rappresenta il nucleo finanziario dell'organizzazione e viene gestito in maniera decentralizzata ed automatica. Per mezzo della tesoreria una DAO è in grado di raccogliere fondi dagli investitori, generare entrate dall'attività dell'organizzazione, pagare i membri che contribuiscono al funzionamento della stessa e fornisce un ritorno agli investitori. Come per ogni altro aspetto anche la tesoreria deve mantenere valide le proprietà chiave della DAO di conseguenza nessun membro può prendere decisioni sugli investimenti della DAO senza aver prima sottoposto la proposta al voto di tutti i membri [17].

2.3 Meccanismi di voto

Il terzo elemento dell'architettura di una DAO è il meccanismo di voto che essendo il principale metodo decisionale delle DAO, influisce profondamente sulla solidità dell'intera rete. [12].

I meccanismi di voto delle DAO possono apprendere dai metodi di voto convenzionali, ma non possono semplicemente copiarli. Le differenze chiave dei meccanismi di voto che vengono utilizzati nelle DAO rispetto a quelli utilizzati convenzionalmente sono presentate nella Tabella 2.2.

Voto nelle DAO	Voto convenzionale
Posizioni uguali per ogni membro.	Posizioni gerarchiche.
Generalmente, le proposte possono essere avviate da qualunque membro e possono riguardare qualunque aspetto della DAO.	Le proposte riguardano solo specifiche tematiche e la gran parte dei membri non ha idiritti di avviare una proposta.
Solitamente tutti i membri hanno diritto di voto.	Le votazioni non sono aperte a tutti i membri dell'organizzazione.
I processi di votazione sono automatizzati tramite smart contracts. Di conseguenza i processi sono completamente trasparenti.	I processi di votazione solitamente richiedono un intervento umano, il che richiede fiducia interna tra i membri della comunità poichè il processo stesso non è accessibile a ogni tutti.
Il potere di voto è solitamente basato su token e distribuito demograticamente.	Il potere di voto è pesantemente influenzato dallo status e dalla ricchezza.

Tabella 2.2: Meccanismi di voto nelle DAO e nelle organizzazioni convenzionali

La decentralizzazione, interpretata come la caratteristica più significativa che distingue il voto nelle DAO rispetto al voto convenzionale, deve essere attentamente

considerata nella progettazione di questi particolari meccanismi di voto. Fortunatamente, il voto nelle DAO ha una base naturalmente ben decentralizzata. Il voto nelle DAO mira a prendere una decisione collettiva normalmente aperta a ogni membro, e il processo decisionale non richiede la partecipazione di membri specifici.

Ogni partecipante al voto della DAO è fortemente indipendente, e il sistema di voto può resistere, in larga misura, all'assenza di qualsiasi partecipante. Tuttavia, questo fornisce solo una base decentralizzata per il voto delle DAO; entità come l'allocazione del potere di voto e le condizioni del processo di voto possono contenere la minaccia di centralizzazione.

In [12] viene inoltre proposto uno schema di decentralizzazione a cinque livelli nel voto delle DAO, suddividendo le esigenze di decentralizzazione in cinque entità nel sistema di voto delle DAO come rappresentato in Figura 2.2.

1. **Fiducia:** Il voto è un metodo decisionale che coinvolge più parti, il che richiede fiducia per mantenere la stabilità e il funzionamento efficiente dei meccanismi di voto. Il voto DAO trasferisce la fiducia basata sull'autorità centralizzata del meccanismo di voto convenzionale al funzionamento degli smart contract.
2. **Appartenenza:** L'appartenenza nelle DAO è generalmente aperta e non gerarchica. Possedere i token nativi della DAO significa diventare membro nella maggior parte dei casi. La decentralizzazione dell'appartenenza mira a una posizione relativamente uguale tra i membri creando relazioni che siano cooperative piuttosto che governative.
3. **Diritti di Voto:** I diritti di voto qui si riferiscono ai diritti di proporre proposte e di votare. Nelle DAO, i diritti di voto sono accessibili a tutti i loro membri, il che rappresenta una decentralizzazione dei diritti di voto. Tuttavia, poiché la membership della maggior parte delle DAO è permissionless e aperta, non è difficile ottenere i diritti di voto nelle DAO. Pertanto, alcune DAO hanno aumentato i requisiti.
4. **Potere di Voto:** Il potere di voto è il peso dei voti di un membro su una proposta, e l'allocazione di questo potere varia da un'organizzazione all'altra. Nella maggior parte delle DAO attuali, l'allocazione del voto è basata su token,

il che significa che l'allocazione del potere di voto dipende in gran parte dal numero di token detenuti da un votante. Gli schemi che distribuiscono il potere di voto sono vari, i più comuni sono:

- Un token un voto (1T1V): implica che un token può essere convertito in una unità di potere di voto.
- Una persona un voto (1P1V): assegna poteri di voto uguali a ciascun votante.

5. **Processo di Voto:** Normalmente, il processo di voto inizia con una proposta. Dopo che la proposta è stata presentata con successo, viene aperta per il voto fino a raggiungere la soglia di potere di voto o il limite di tempo. Il risultato finale del voto sarà generato automaticamente secondo i criteri di approvazione della proposta scritti nello smart contract.



Figura 2.2: Schema di decentralizzazione a cinque livelli

La decentralizzazione di una DAO può essere studiata mediante l'uso di differenti metriche, tra queste in particolare in [11] vengono considerate le seguenti.

- **Entropia:** Può essere generalmente utilizzata per valutare il grado di casualità e libertà di un dato sistema. Un alto valore di entropia, implica un alto grado di casualità e libertà, il che è correlato a un elevato livello di decentralizzazione.
- **Coefficiente di Gini:** Viene utilizzato per misurare l'ineguaglianza di ricchezza, può essere applicato per valutare l'ineguaglianza del potere di voto tra gli elettori nella nostra analisi. Un coefficiente di Gini di 0 significa perfetta uguaglianza, mentre 1 indica piena concentrazione di potere.
- **Coefficiente di Nakamoto:** Riflette il numero minimo di entità necessarie per sovvertire il sistema, evidenziando l'importanza di evitare una significativa concentrazione di potere per una vera democrazia DAO.

2.3.1 Tipologie di meccanismi di voto

Concludiamo ora l'analisi sui meccanismi di voto andando ad elencare quelli più comunemente utilizzati [12].

Maggioranza Relativa Permessa (PRM) PRM è il meccanismo di voto più semplice e ampiamente utilizzato. Il meccanismo prevede una soglia di passaggio del voto pari al 50% di tutto il potere di voto speso nella votazione.

Il meccanismo può però essere facilmente manipolato quando le proposte non ricevono sufficiente attenzione dai membri.

Meccanismo di Quorum Basato su Token (TBQ) La regola fondamentale è la stessa di PRM, che consiste nell'ascoltare la maggioranza, ma richiede un livello più elevato di partecipazione da parte dell'organizzazione.

Il requisito di partecipazione riduce notevolmente la minaccia delle proposte approvate senza attenzione o con poca partecipazione, aumentando la sicurezza del voto.

Come contro si allunga il tempo necessario per raccogliere un'attenzione sufficiente, e il tasso di approvazione delle proposte potrebbe essere ridotto a causa delle condizioni di approvazione più rigorose.

Voto Quadratico Il voto quadratico è uno schema di allocazione del potere di voto che bilancia 1T1V e 1P1V con un design di aumento del costo marginale. Nello specifico il costo marginale aumenta man mano che un utente vota ripetutamente sulla stessa opzione di conseguenza il numero di voti di ciascun utente è uguale alla radice quadrata dei token pagati. Questo metodo permette di mitigare i problemi legati allo schema 1T1V che condensa un potere di voto schiacciante di un piccolo numero di enormi detentori di token, allo stesso tempo, è più ragionevole e flessibile rispetto a 1P1V.

Democrazia Liquida Nello schema della Democrazia Liquida, agli elettori è consentito votare direttamente o delegare i loro diritti di voto a un rappresentante, che è di solito un esperto della comunità. La delega è consentita in modo multilivello, il che significa che i rappresentanti possono a loro volta delegare ad altri rappresentanti tutti i voti che hanno ricevuto in delega. Con questo metodo l'efficienza del voto sarà notevolmente migliorata grazie all'elaborazione rapida di un gran numero di voti delegati, tuttavia, la delega può causare un arresto della decentralizzazione poiché una struttura di voto delegato tenderà ad essere gerarchica e centralizzata.

Voto Ponderato Il Voto Ponderato aggiunge un peso extra al calcolo dell'utilità del potere di voto di ciascun membro. Solitamente per definire questo peso vengono utilizzate la reputazione e la conoscenza sulla DAO. Fondamentalmente, il Voto Ponderato tende ad allocare più potere di voto a membri esperti, aumentando la possibilità di prendere decisioni informate. Pertanto, l'efficacia del voto è notevolmente migliorata.

Rage Quitting Con il metodo di rage quitting, una proposta approvata rimarrà in un periodo di grazia prima che i risultati del voto vengano eseguiti. In questo periodo

di grazia, i membri che sono insoddisfatti del risultato possono ritirarsi dall'organizzazione. In questo metodo i membri non sono vincolati da una scelta collettiva, ed è difficile per un proprietario con un potere di voto schiacciante controllare gli asset degli altri, il che aumenta la decentralizzazione. Tuttavia, il periodo di grazia rallenta il processo di voto, il che ha un impatto negativo sull'efficienza del voto.

Consenso Olografico Introduce un mercato di scommesse sulle proposte, dove i membri possono scommettere sull'esito di votazioni. Le proposte con scommesse sufficienti possono essere approvate con una maggioranza relativa, mentre quelle senza rimangono in coda e richiedono una maggioranza assoluta.

Voto Conviction Si basa sulla durata dello staking dei token, dove il potere di voto aumenta in base al tempo dedicato a una proposta. Questo incoraggia una riflessione più attenta sulle scelte.

2.4 Classificazione dei token

Il termine “criptovaluta” si riferisce in generale al concetto di denaro virtuale, il che è fuorviante o almeno riduttivo. A seconda delle loro funzioni e peculiarità tecnologiche infatti le criptovalute possono differire significativamente l'una dall'altra [23].

Solitamente vengono distinte nelle seguenti categorie a seconda della loro funzione:

- token di pagamento (criptovaluta o moneta): un token creato per essere utilizzato come strumento di pagamento accettato da una specifica comunità oppure da un insieme di comunità.
- token di utilità (utility tokens): un token necessario per accedere a una piattaforma o per utilizzare i servizi offerti da una piattaforma.
- token di investimento (security tokens): token equivalenti a strumenti finanziari o di investimento in quanto rappresentano delle azioni di una determinata organizzazione.

Le distinzioni che è possibile operare tra i diversi tipi di token non si esauriscono in una classificazione per funzionalità; un ulteriore criterio di differenziazione riguarda lo standard adottato per la loro definizione. Gli standard impiegati, noti come Ethereum Request for Comments (ERC), saranno di seguito presentati e analizzati nei loro aspetti principali.

ERC-20 Il primo standard ad essere stato introdotto è stato l'ERC20 nel 2015 da Fabian Vogelsteller e Vitalik Buterin ed è lo standard definito per i *Fungibile token* ovvero per token hanno una proprietà che li rende esattamente uguali (per tipo e valore) a un altro token ¹ rendendoli intercambiabili e privi di un proprietario specifico.

Lo standard definisce delle interfacce comuni ai contratti che implementano i token in modo tale che, definendo comportamenti comuni, possano essere usati tutti nello stesso modo [24]. L'interfaccia comprende diverse funzioni che rappresentano una base da implementare presente per ogni token ERC20 al quale poi ogni sviluppatore può aggiungere attributi o funzioni aggiuntive. Nello specifico lo standard ERC-20 è composto dalla seguente serie di caratteristiche e funzioni [23]:

- nome del token;
- simbolo del token;
- numero di decimali che il token utilizza;
- numero totale dei token;
- saldo del numero dei token nel wallet di un utente;
- trasferibilità del token tra utenti;
- prelievo dei token da un wallet;

¹<https://ethereum.org/it/developers/docs/standards/tokens/erc-20/>

ERC-721 Lo standard ERC-721 viene utilizzato per i *Non-fungibile token* anche chiamati semplicemente *NFT* [22].

Solitamente, il termine NFT viene associato all'arte digitale; in realtà, il concetto di NFT trae origine da uno standard di Ethereum ideato con l'obiettivo di distinguere ogni token in modo univoco attraverso l'uso di identificatori specifici. Questa caratteristica consente di associare tale tipologia di token al concetto di proprietà digitale, poiché ciascun NFT è definito da un'identificazione unica. Di conseguenza, le proprietà digitali rappresentate dagli NFT possono essere liberamente scambiate, con valori che variano in base a diversi fattori, spesso legati all'opera stessa.

Le principali differenze questi standard sono mostrate in Tabella 2.3.

ERC-20	ERC-721
Token Fungibili: Privi di una individualità specifica.	Token non fungibili: Ognuno è originale e diverso dagli altri.
Può essere sostituito e/o scambiato.	Non può essere sostituito con un altro bene dello stesso tipo, perché ciascuno ha un valore e delle caratteristiche uniche.
Può essere diviso in parti più piccole ed ognuna di esse può essere venduta liberamente.	Non può essere diviso in parti più piccole e vendute separatamente.

Tabella 2.3: Principali differenze tra gli standard ERC-20 ed ERC-721

ERC-777 E' lo standard utilizzato per i token definiti *Token standard* e si tratta di uno standard compatibile con ERC-20 e migliorativo dello stesso in quanto permette di inviare token per conto di un altro utente e offre agli emittenti un maggiore controllo sui token emessi.

ERC-1155 Lo standard ERC-1155, noto anche come *Multi Token Standard*, introduce la possibilità di gestire più tipologie di token attraverso un unico smart contract. A differenza dell'ERC-20, che prevede il dispiegamento di contratti separati per ciascun tipo di token, e dell'ERC-721, che consente la gestione di una singola collezione di NFT con impostazioni uniformi, l'ERC-1155 permette di definire token configurabili individualmente, ciascuno con propri metadati, quantità e ulteriori attributi distintivi.

2.5 Implementazione della Governance

La questione centrale di questo paragrafo è la seguente: se gli smart contract sono per loro natura immutabili, in che modo possono essere aggiornati analogamente a un software tradizionale? [25]

Occorre innanzitutto considerare che un contratto o un opcode già distribuito sulla blockchain non può essere modificato. È tuttavia possibile implementare tramite l'uso di smart contract aggiornabili un sistema di mappatura della memoria che collega il nuovo contratto a quello originario, consentendo così di mantenere lo stato e i dati pur aggiornando la logica del programma affrontando dunque le limitazioni derivanti dalla loro immutabilità.

Analizziamo i modelli più utilizzati di smart contract aggiornabili, per farlo andiamo innanzitutto a dividerli in due categorie principali:

- Modelli di segregazione dei dati (data segregation).
- Modelli basati su proxy (proxy patterns).

Modelli di segregazione dei dati In questa sezione trattiamo i modelli di segregazione dei dati [25]. L'idea fondamentale dietro questo approccio è separare i dati dalla logica del contratto. In questo modo, un contratto viene scritto come due sottocontratti distinti:

- un data contract, che contiene le variabili di stato e conserva i dati sulla blockchain;
- un logic contract (o business contract), che contiene le funzioni operative e manipola i dati tramite interfacce fornite dal contratto dati.

Questo tipo di modello consente di aggiornare o ridistribuire il contratto logico mantenendo inalterato il contratto dati, uno svantaggio di questo modello dunque è dato dal fatto che il contratto dati rimane non aggiornabile.

Attualmente, esistono tre varianti principali di questo modello:

- Basic Data Segregation (Segregazione di base): Il contratto originale viene diviso in due sottocontratti: uno per i dati e uno per la logica.
- Satellite Pattern (Contratto Satellitare): Anch'esso utilizza un singolo contratto dati, ma introduce uno o più contratti satelliti, ognuno dedicato a una singola funzionalità consentendo una maggiore modulabilità rispetto al caso precedente.
- Register Contract Pattern (Contratto Registro): Aggiunge un contratto di registro per aggiornare l'indirizzo del contratto logico a cui il contratto dati fa riferimento. Tuttavia, non consente di importare i dati esistenti nel nuovo contratto logico; quindi, deve essere combinato con altri modelli come la segregazione di base o quella satellitare.

Modelli basati su proxy Un'altra categoria di modelli aggiornabili è quella dei proxy contracts, introdotti da OpenZeppelin per la piattaforma Ethereum [25].

Tutti i contratti di questo tipo condividono lo stesso principio di base: il contratto proxy prende il controllo di tutti gli stati e gestisce ogni chiamata al contratto originale utilizzando l'istruzione *delegatecall* dell'EVM.

Questo modelli mantengono invariato l'indirizzo del mittente originario, ma inoltra la chiamata attraverso il proxy verso l'indirizzo di memoria del contratto originale

correntemente in uso. A livello pratico quello che accade è che tutte le chiamate verso il contratto vengono intercettate dal proxy, che le inoltra al contratto effettivo tramite `delegatecall`, consentendo così di aggiornare la logica del contratto mantenendo invariato lo stato e l'indirizzo sulla blockchain.

Con questa tecnica, il proxy ha pieno controllo sulla memoria e sugli stati del contratto, poiché `delegatecall` esegue il codice del contratto logico nel contesto del contratto chiamante (il proxy).

È importante notare che con questi modelli non è necessario separare il contratto dati dal contratto logico, poiché il proxy stesso gestisce lo storage e garantisce l'aggiornabilità del codice senza modificare gli indirizzi o gli stati esistenti.

Di modelli basati su proxy ne esistono molteplici, tra i più utilizzati possiamo considerare [27]:

- **Inherited Storage (Archiviazione Ereditata):** Sia il contratto proxy che quello logico ereditano la stessa struttura di archiviazione per garantire che entrambi rispettino le variabili di stato necessarie del proxy.
- **Eternal Storage (Archiviazione Eterna):** I contratti proxy e di implementazione non dichiarano mai proprie variabili, ma le archiviano in una mappatura, facendo sì che Solidity le salvi in posizioni arbitrarie di memoria basate sui loro nomi.
- **Unstructured Storage (EIP-1967):** Questo pattern imita il modo in cui Solidity gestisce mapping e array di dimensione dinamica per evitare conflitti di memoria tra proxy: memorizza l'indirizzo dell'implementazione in uno slot arbitrario della memoria.
- **EIP-1822 – Universal Upgradeable Proxy Standard (UUPS):** Questo standard sposta la logica di aggiornamento nel contratto di implementazione anziché nel proxy stesso. I contratti di implementazione estendono un contratto base

“proxiable”. L’indirizzo dell’implementazione è salvato in uno slot determinato da keccak256(“PROXIABLE”).

- Transparent Proxy (EIP-1967 solo Admin): Estensione dell’Unstructured Storage in cui solo l’amministratore può chiamare le funzioni di gestione degli aggiornamenti, mentre tutti gli altri utenti possono solo interagire con le funzioni del contratto di implementazione.
- EIP-1538 – Transparent Proxy (versione precedente): In questa versione, invece di salvare un singolo indirizzo di implementazione, il proxy conserva una mappatura tra il selettore della funzione e l’indirizzo dell’implementazione.
- EIP-2535 – Diamonds Proxy: Sostituisce EIP-1538. Anche qui il proxy memorizza una mappatura da selettore di funzione a indirizzo di implementazione. Prende il nome di Diamonds Proxy poichè utilizza la terminologia del settore dei diamanti.
- Beacons Proxy: I beacon permettono di avere più proxy per la stessa implementazione, con la possibilità di aggiornarli tutti contemporaneamente. Ogni proxy conserva l’indirizzo di un beacon, che a sua volta memorizza l’indirizzo dell’implementazione.
- Registry Proxy: Simile al Beacon Proxy, ma interroga un contratto Registry per ottenere l’indirizzo dell’implementazione. Il registro associa un numero di versione a un indirizzo di implementazione.
- EIP-1167 – Minimal Proxy: Riduce i costi di distribuzione quando sono necessarie più istanze dello stesso contratto. Invece di distribuire molte copie costose in gas, viene distribuita una singola implementazione e molteplici proxy che la puntano. Questi proxy sono semplici, non aggiornabili e non necessitano di storage o funzioni di gestione.
- EIP-897 – DelegateProxy: Propone un insieme di interfacce per i proxy, per segnalare come funzionano e qual è la loro implementazione principale.

Concludiamo l'analisi sugli smart contract aggiornabili osservando che ad essi sono però associati anche dei rischi [26]. I due rischi principali che possono essere riscontrati sono i seguenti:

- Aumento della complessità del sistema, implementare contratti aggiornabili rende l'architettura più complessa e può introdurre nuovi bug.
- Mancanza di fiducia nell'aggiornamento, spesso, infatti, solo i distributori del contratto detengono il potere centralizzato di controllare il processo di aggiornamento.

2.6 Classificazione delle DAO

In quest'ultimo paragrafo andremo a fornire una panoramica su una possibile categorizzazione delle DAO in funzione della loro funzione secondo [10] e [28]:

DAO di protocollo Si occupano di gestire e governare un protocollo web3 come una comunità coesa e collaborativa. I membri di queste DAO possiedono una piccola quota del progetto e sono coinvolti nel successo del protocollo tramite l'andamento del prezzo del token, senza essere tenuti a fornire finanziamenti o risorse aggiuntive. Tali organizzazioni in particolare possono raggiungere dimensioni considerevoli, con ampie tesorerie e molti membri i quali possono proporre e votare modifiche relative al protocollo sfruttando i diritti acquisiti con il possesso di token.

Alcuni esempi di DAO appartenenti a questa categoria sono:

- Uniswap: Il più popolare exchange decentralizzato su Ethereum, che ha lanciato il proprio token di governance, UNI, a settembre 2020.
- Aave: Un organizzazione che consente di prestare e prendere in prestito asset su internet in un contesto di assenza di fiducia reciproca tra gli utenti.
- Maker: Il protocollo di governance per la stablecoin algoritmica più popolare, DAI, considerata la DAO originaria nell'ecosistema DeFi.

DAO di Investimento Queste DAO sono simili ai fondi di investimento di venture capital tradizionali, che raccolgono capitale da più fonti e lo destinano a startup in fase iniziale. La differenza è che, invece di un numero limitato di persone selezionate a decidere dove investire, tutti i membri della DAO possono votare su come investire il capitale dell'organizzazione.

Un esempio di DAO appartenente a questa categoria è:

- MetaCartel Ventures: Una delle prime DAO a scopo di lucro, investe in applicazioni decentralizzate (DApp) in fase iniziale.

DAO di Sovvenzioni Queste DAO sono progettate per finanziare nuove imprese, hackathon e sviluppi di protocolli. Solitamente strutturati come un ramo separato di un ecosistema più grande, ma possono anche esistere in modo indipendente.

Un esempio di DAO appartenente a questa categoria è:

- Bitcoin: Una piattaforma per sviluppatori di applicazioni open-source, in questa DAO i donatori possono scegliere a quali progetti contribuire tramite opportune votazioni.

DAO Collezionisti Questo tipo di DAO raccoglie fondi per acquistare oggetti da collezione, sia reali (asset fisici) che virtuali (NFT). L'obiettivo è possedere, curare e monetizzare questi pezzi unici di arte e cultura a beneficio della comunità. In generale queste DAO sono molto simili a quelle di investimento, solo che gli investimenti si concentrano esclusivamente sulla raccolta e cura di opere d'arte e non in progetti o nella creazione di prodotti e servizi;

L'esempio di DAO appartenente a questa categoria più noto è certamente:

- PleasrDAO: Una DAO incentrata sull'acquisto di opere d'arte e oggetti da collezione.

DAO Sociali Le DAO sociali consentono l'accesso a comunità di nicchia a cui si può accedere solo se si possiede un certo token ottenibile pagando una quota associativa. La cerchia sociale della comunità è specifica per la DAO e può includere appassionati d'arte, club del libro e molto altro.

Alcuni esempi di DAO appartenenti a questa categoria sono:

- **Friends with Benefits:** Questo club sociale esclusivo è composto da artisti, operatori ed entusiasti del web3. Si può diventare membro solo possedendo un certo numero di token FWB, che danno accesso a eventi esclusivi e gallerie di aste di collezionabili digitali.
- **AssangeDAO:** E' un'organizzazione che nasce alla fine del 2021 con una missione ben precisa, «ispirare una potente rete di solidarietà al fine di lottare per la libertà di Julian Assange».

Capitolo 3

Analisi di 50 DAO

3.1 Introduzione

3.1.1 Criteri di selezione

La selezione del campione è stato circoscritto a 50 Decentralized Autonomous Organizations (DAO) per garantire un equilibrio ottimale tra significatività statistica e profondità di analisi qualitativa. Le DAO selezionate risiedono su rete Ethereum (Layer 1) e sulle chain del suo ecosistema allargato, includendo principalmente soluzioni Layer 2 (Arbitrum, Optimism, Base) ma anche network compatibili come Polygon, Gnosis, ecc. . . . Ciò ha permesso di eliminare le variabili di disturbo derivanti da differenze architettoniche tra blockchain diverse, focalizzando l'analisi comparativa principalmente sulle dinamiche di governance. La scelta di includere sia Ethereum Mainnet che i principali L2 ha inoltre consentito di esaminare un campione rappresentativo che spazia dalle DAO storiche ad alta capitalizzazione (spesso su L1) alle nuove organizzazioni caratterizzate da bassi costi di transazione (su L2), offrendo una panoramica completa su come l'accessibilità economica influenzi i processi decisionali. Il numero di 50 entità costituisce, in questo specifico perimetro tecnologico, un campione statisticamente significativo per osservare i trend dominanti.

La selezione del campione finale di 50 DAO è avvenuta attraverso un processo di

scrematura a più stadi volto a garantire sia la rappresentatività economica che la consistenza tecnica dei dati analizzati.

- **Criterio di rilevanza economica:** In prima istanza, la selezione si è orientata verso le organizzazioni a maggiore capitalizzazione di mercato, al fine di garantire l'inclusione dei protocolli con il maggior peso nell'ecosistema Crypto.
- **Criterio di omogeneità tecnologica:** Sono state escluse le DAO operanti su blockchain proprietarie non compatibili con la Ethereum Virtual Machine (EVM), per garantire la comparabilità tecnica dei meccanismi di voto e degli smart contract di governance.
- **Criterio di rilievo accademico:** Un sottoinsieme di DAO è stato individuato attingendo a un dataset¹ di riferimento condiviso dal relatore, al fine di includere casi studio di particolare interesse accademico e metodologico.
- **Criterio di vitalità:** Le ultime DAO scelte sono state selezionate cercando di evitare l'analisi di organizzazioni inattive o prive di reale operatività. Per considerare la DAO attiva, sono stati applicati due parametri congiunti. E' stato richiesto un volume storico minimo di 10 proposte, per garantire la presenza di processi decisionali consolidati ed è stato imposto che l'ultima votazione sia avvenuta entro il semestre antecedente la raccolta dati, al fine di garantire la contemporaneità delle dinamiche osservate.

3.1.2 Struttura dell'analisi

Al fine di garantire un'analisi rigorosa e comparabile tra le diverse Decentralized Autonomous Organizations (DAO) selezionate, è stato adottato un approccio metodologico standardizzato [40]. Ciascun caso studio è stato esaminato seguendo una struttura tripartita fissa: una descrizione del progetto e del suo scopo operativo, l'analisi delle caratteristiche del token di governance e l'approfondimento dei meccanismi di governance. In particolare, lo studio dei processi di governance è stato sviluppato su due aspetti complementari: un profilo teorico, volto a comprendere

¹<http://130.192.84.45:8080/>

le logiche e le regole dichiarate dall'organizzazione, e un profilo pratico, focalizzato sull'analisi tecnica dei contratti distribuiti sulla blockchain.

Per facilitare una sintesi comparativa e una lettura trasversale dei risultati, le informazioni chiave raccolte per ogni DAO sono state formalizzate nella **Tabella delle variabili estratte** (Tabella 3.1). Tale prospetto elenca in modo formale tutte le variabili raccolte per ogni organizzazione, specificando per ciascuna di esse una breve descrizione esplicativa e la fonte ufficiale da cui il dato è stato ottenuto.

Variabile	Descrizione	Fonte
Token Standard	ERC-20, ERC-721, ERC-1155	Token contract
Proxy Pattern	Transparent, UUPS, Diamond, Nessuno	Governor contract
Threshold	Soglia minima di token di cui disporre per poter avviare una proposta	Governor contract
Quorum	Percentuale o valore assoluto minimo necessario per il successo di una proposta	Governor contract
Voting Delay	Ritardo tra la pubblicazione e l'inizio della votazione	Governor contract
Voting Period	Durata della fase di votazione	Governor contract
Timelock Delay	Ritardo tra approvazione ed esecuzione	Timelock contract
Meccanismo tesoreria	Tipo di gestione della tesoreria	Treasury contract

Tabella 3.1: Tabella delle variabili estratte

3.1.3 Fonti dei dati

La raccolta dei dati è stata condotta adottando un approccio metodologico, volto a incrociare le fonti dichiarative con le evidenze tecniche immutabili registrate su blockchain.

La ricostruzione del funzionamento teorico dei protocolli e dei relativi processi decisionali si è basata sull'analisi della documentazione ufficiale (Whitepaper, Gitbook, Wiki) fornita dalle singole DAO. Questa fase preliminare è stata fondamentale per comprendere le funzionalità di ogni singolo protocollo e l'architettura di governance prevista per la relativa organizzazione.

Per l'acquisizione delle metriche quantitative legate alla tokenomics (come la circulating supply e la capitalizzazione di mercato), si è fatto riferimento ai principali aggregatori di dati del settore, quali **CoinMarketCap** e **CoinGecko**, scelti per la loro capacità di fornire dati finanziari standardizzati e storicizzati.

Per garantire la massima accuratezza tecnica, l'indagine non si è limitata ai dati aggregati. L'analisi degli Smart Contract è stata effettuata direttamente alla fonte attraverso l'uso dei block explorer nativi delle reti oggetto di studio (nello specifico **Etherscan**, **Basescan**, **Arbiscan**, ...).

Per quanto concerne lo studio della struttura patrimoniale, i dati relativi alla tesoreria e ai relativi meccanismi di gestione sono stati ottenuti previa identificazione dell'indirizzo del contratto di custodia (Treasury Contract). La composizione del portafoglio e il valore degli asset in gestione sono stati successivamente esaminati mediante l'ausilio di piattaforme di portfolio tracking e analisi finanziaria on-chain quali **DeBank** e **token terminal**. Mentre per le DAO la cui governance ne prevedesse l'uso, si è fatto ricorso alla piattaforma Tally ed al relativo tracciamento del volume di tesoreria.

Infine, per la mappatura puntuale dei parametri di governance (quali quorum, soglie di proposta e timelock), è stata applicata una triangolazione dei dati che ha permesso di confrontare le informazioni presenti nelle documentazioni ufficiali con le interfacce di voto (piattaforme come **Snapshot** e **Tally**) e successivamente validate in via definitiva estraendo i valori esatti (variabili di stato) direttamente dai contratti di governance on-chain. Questo passaggio ha permesso di verificare la corrispondenza tra quanto dichiarato nelle documentazioni e il codice distribuito in rete.

3.1.4 Limitazioni

È opportuno inoltre delineare i confini e le limitazioni metodologiche entro cui si è svolta la ricerca.

In primo luogo, l'analisi delle dinamiche di voto si è concentrata esclusivamente sulla governance on-chain, ovvero su quelle decisioni che comportano un'interazione diretta con gli Smart Contract (e il conseguente pagamento di gas fee). Sebbene piattaforme off-chain come Snapshot siano ampiamente utilizzate nel settore esse non hanno effetti vincolanti diretti sul protocollo di conseguenza sono state analizzate solo da un punto di vista teorico. La scelta di escludere i dati tecnici di queste piattaforme dall'analisi statistica è stata dettata dalla volontà di misurare la partecipazione "reale", ovvero quella in cui gli stakeholder si assumono la responsabilità economica e tecnica di modificare lo stato della blockchain. Di conseguenza, lo studio potrebbe non catturare a pieno il funzionamento delle fasi preliminari e informali del dibattito politico.

In secondo luogo, data l'estrema rapidità di evoluzione dell'ecosistema Web3, è necessario considerare la validità temporale dei dati. La raccolta delle informazioni e lo 'snapshot' delle metriche di governance (quali tesoreria, numero di proposte e parametri di voto) sono stati raccolti in un periodo compreso tra luglio 2025 e febbraio 2026 e finalizzati in data 10.02.2026. Eventuali modifiche ai protocolli, aggiornamenti dei contratti o variazioni significative nella partecipazione avvenute successivamente a tale data non sono incluse nel presente elaborato.

3.2 Uniswap

Uniswap è un sistema peer-to-peer progettato per lo scambio di criptovalute sulla blockchain di Ethereum tramite l'uso di un token ERC20 di pool chiamato UNI. Il protocollo è implementato come un insieme di smart contract permanenti e non aggiornabili². Per tale protocollo sono state sviluppate quattro diverse versioni.

- v1 lanciata nel novembre del 2018 e la v2 [18] (ormai in disuso) sono open source e con licenza GPL (o General Public License).
- v3 [19] è ancora open source ed introduce la liquidità concentrata, consentendo di allocare la liquidità all'interno di un intervallo di prezzo personalizzato

²<https://docs.uniswap.org/concepts/uniswap-protocol>

invece che distribuirla uniformemente lungo la curva dei prezzi come fatto in precedenza.

- v4 [20] eredita le modifiche di Uniswap v3, ma offre flessibilità tramite l'introduzione di un'architettura singleton (in cui tutti gli stati e le operazioni del pool sono gestiti da un unico contratto: `PoolManager.sol`), l'uso di hook (contratti che possono essere richiamati dal PoolManager per un'esecuzione senza autorizzazioni) e l'ottimizzazione delle gas-fee durante l'intero ciclo di vita.



Figura 3.1: Uniswap Logo

Per comprendere come tale protocollo differisca da un exchange tradizionale, è utile esaminare due aspetti chiave.

In primo luogo il protocollo Uniswap invece adotta un approccio diverso, utilizzando un Automated Market Maker (AMM), il quale sostituisce gli ordini di acquisto e vendita tipici di un mercato con order book con un pool di liquidità composto da due asset, entrambi valutati l'uno rispetto all'altro. Quando un asset viene scambiato con l'altro, i prezzi relativi dei due cambiano, determinando così un nuovo prezzo di mercato per entrambi. In questa dinamica, un acquirente o un venditore scambia direttamente con il pool, piuttosto che con ordini specifici lasciati da altre parti.

La seconda differenza rispetto ai mercati tradizionali è il design permissionless e immutabile del protocollo Uniswap, il che significa che i servizi del protocollo sono completamente aperti all'uso pubblico, senza alcuna possibilità di limitare selettivamente chi possa o non possa utilizzarli ed inoltre nessuna parte ha la possibilità di sospendere i contratti, annullare l'esecuzione di uno scambio o modificare in alcun modo il comportamento del protocollo.

3.2.1 Token UNI

Come abbiamo già detto il protocollo Uniswap si basa sull'uso di un token di governance ERC-20 chiamato UNI. Il suo contratto è registrato all'indirizzo:

0x1f9840a85d5aF5bf1D1762F925BDADdC4201F984



Figura 3.2: Token UNI

Tramite questi token i membri della comunità possono partecipare alle votazioni indicando il proprio appoggio o il loro dissenso relativo a specifiche proposte. Affinchè i token UNI possano essere utilizzati nelle votazioni però, il titolare deve prima passare attraverso il processo di delegazione che preceda il periodo di voto della proposta. Delegare UNI lega il potere di voto dei propri token a un indirizzo, così da poter essere utilizzati per votare. Tale indirizzo può essere il wallet del titolare, oppure quello di una parte di fiducia che si ritiene voterà nell'interesse della DAO.

Osservazione 3.1. *La delega è un evento registrato on-chain, quindi creare o aggiornare la delega comporta un costo in gas.*

Per Uniswap non è previsto un hard cap, di conseguenza non c'è un limite massimo di token UNI che possono essere creati. Per quanto riguarda l'offerta totale fino al 27 dicembre 2025 è stata di 1.000.000.000 UNI. Il 28 dicembre però Uniswap ha eseguito un'importante operazione di tesoreria, bruciando 100 milioni di token UNI tramite una transazione on-chain approvata tramite una proposta on-chain ed attualmente il valore è di 899.318.420,04 UNI mentre l'offerta effettivamente circolante è pari a 634.683.562,75 UNI³.

³02.02.2026, <https://coinmarketcap.com/currencies/uniswap/>

3.2.2 Processo di governance e analisi dei contratti

La governance di Uniswap è gestita tramite l'uso di diverse piattaforme, ognuna con uno scopo specifico⁴.

- **Governance Forum**⁵: Un forum per discussioni legate alla governance. I membri della comunità per poter interagire con i post presenti nel forum devono registrare un account mentre per poter pubblicare i propri contenuti devono prima aver letto almeno 4 discussioni e un totale di 15 post per almeno 10 minuti.
- **Snapshot**⁶: Un'interfaccia di voto semplice che consente agli utenti di esprimere il proprio orientamento off-chain. I voti su Snapshot sono ponderati in base al numero di UNI delegati all'indirizzo utilizzato per votare.
- **Uniswap Agora**⁷: La Uniswap Foundation supporta Uniswap Agora come interfaccia di voto e delega.

Andiamo dunque ad analizzare come si sviluppa il processo di governance e come le precenti piattaforme sono coinvolte.

Fase 1: Request for Comment (RFC) Questa prima fase prevede la pubblicazione da parte del proponente di un post sul Governance Forum in cui la proposta viene presentata alla comunità specificando su cosa si sta chiedendo ai delegati di votare e spiegando le ragioni per cui la ritiene una buona idea. Prima di passare alla Fase 2, vengono concessi almeno 7 giorni per leggere e commentare l'RFC.

Fase 2: Temperature Check Durante la seconda fase lo scopo è raccogliere il segnale sul sentimento della comunità riguardo a una proposta, prima di passare a un voto on-chain. Tale proposta prevede di pubblicare: un sondaggio su snapshot ed un post sul Governance forum che permetta ai membri di raggiungere il sondaggio e

⁴<https://docs.uniswap.org/concepts/governance/process>

⁵<https://gov.uniswap.org/>

⁶<https://snapshot.org/#/uniswap>

⁷<https://vote.uniswapfoundation.org/>

di esprimere la propria opinione con una votazione off-chain.

La durata del sondaggio viene impostata a 5 giorni alla fine dei quali, vince l'opzione con la maggioranza dei voti. Se la maggioranza vota per il "Sì" è necessario inoltre che tale opzione che abbia ricevuto almeno 10 milioni di UNI di voti. Se vince l'opzione "Nessun cambiamento", la proposta non avanzerà alla Fase 3.

Fase 3: Governance Proposal La fase 3 è l'ultimo passaggio del processo di governance e prevede la creazione della proposta tramite un'interfaccia (ad esempio Tally o Agora) oppure scrivendo direttamente il calldata per logiche di proposta più complesse. Se la proposta viene approvata, questo calldata verrà eseguito.

Per poter presentare una proposta è necessario che almeno 1 milione di UNI sia delegato all'indirizzo del proponente. Una volta presentata la proposta, inizierà un ritardo di voto di 2 giorni. Al termine di questo periodo, avrà inizio una fase di voto di circa 7 giorni. Se la maggioranza avrà votato a favore della proposta con un numero di voti superiori al quorum di 40 milioni essa passerà e dovrà trascorrere un timelock di 2 giorni prima che il codice proposto possa essere eseguito e quindi applicato on-chain⁸.

Osservazione 3.2. *Dopo aver superato ognuna delle fasi intermedie è utile integrare eventuali modifiche alla proposta sulla base dei feedback ricevuti dalla comunità al fine di aumentare le probabilità di successo della stessa.*

Il protocollo Uniswap è governato e aggiornato dai possessori di token UNI attraverso due contratti di governance fondamentali: il governor ed il timelock. Insieme, questi smart contract permettono alla community di proporre, votare e implementare modifiche al protocollo Uniswap.

Governor Per quanto riguarda il modulo di governance le prime due versioni⁹ sono chiamate *GovernorAlpha* (lanciato nel settembre 2020) e *GovernorAlphaV2* (lanciato

⁸<https://www.uniswapfoundation.org/governance>

⁹<https://docs.uniswap.org/contracts/v2/reference/Governance/governance-reference>

nel maggio 2021) e sono registrate rispettivamente agli indirizzi:

0x5e4be8Bc9637f0EAA1A755019e06A68ce081D58F

0xC4e172459f1E7939D522503B81AFAaC1014CE6F6

Tali versioni risultano essere quasi coincidenti se non per i pochi aspetti che vediamo evidenziati in Figura 3.3. La seconda versione del contratto nello specifico si limita a semplificare la configurazione, in quanto non richiede parametri nel deploy, ed ampliare la partecipazione abbassando il threshold per la pubblicazione di una proposta.

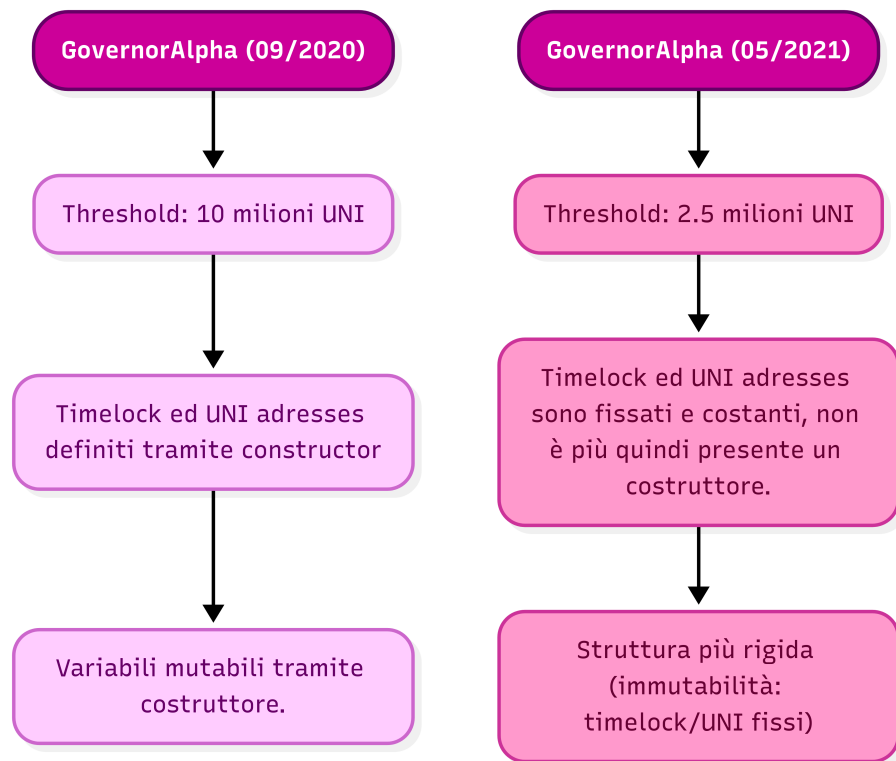


Figura 3.3: Differenze tra le prime due versioni della governance di Uniswap

Il contratto di governance attualmente in uso è invece chiamato *GovernorBravoDelegator* ed è registrato all'indirizzo:

0x408ED6354d4973f66138C91495F2f2FCbd8724C3

Tale versione aggiornata è un proxy (EIP-897 Delegate Proxy) il quale punta al contratto di implementazione *GovernorBravoDelegate* che è registrato all'indirizzo:

0x53a328F4086d7C0F1Fa19e594c9b842125263026

I codici che definiscono i contratti citati sono basati sullo standard definito da Compound e dalle relative evoluzioni avvenute nel corso del tempo.

Nella Tabella 3.2 sono raccolti gli indirizzi dei contratti di governor che si sono susseguiti nel corso del tempo per la gestione del processo di governance del protocollo.

<i>Nome</i>	<i>Indirizzo</i>
GovernorAlpha	0x5e4be8Bc9637f0EAA1A755019e06A68ce081D58F
GovernorAlpha v2	0xC4e172459f1E7939D522503B81AFAaC1014CE6F6
GovernorBravoDelegator	0x408ED6354d4973f66138C91495F2f2FCbd8724C3
GovernorBravoDelegate	0x53a328F4086d7C0F1Fa19e594c9b842125263026

Tabella 3.2: Lista degli indirizzi dei contratti di governor di Uniswap nel tempo

Timelock L'ultimo smart contract che partecipa al processo di governance è il contratto di *Timelock* registrato all'indirizzo:

0x1a9C8182C09F50C8318d769245beA52c32BE35BC

Tale contratto è costruito sul modello originale di Compound Finance, ma con un'importante citazione a OpenZeppelin per quanto riguarda la sicurezza matematica.

Il Timelock ha un ritardo minimo codificato per l'effettiva esecuzione di 2 giorni, che rappresenta il preavviso più breve possibile per un'azione di governance. Gli aggiornamenti principali, possono avere un ritardo fino a 30 giorni.

Tesoreria La tesoreria di Uniswap DAO è gestita principalmente dal contratto di timelock. Il volume attuale è di \$1.062.003.690 ¹⁰.

¹⁰02.02.2026, <https://debank.com/profile/0x1a9c8182c09f50c8318d769245bea52c32be35bc?chain=>

Nella Tabella 3.3 presentiamo una raccolta di i parametri usati per la gestione della governance facendo riferimento alla versione corrente del governor.

<i>Parametro</i>	<i>Valore</i>
proposalThreshold	1.000.000 UNI
MIN_PROPOSAL_THRESHOLD	1.000.000 UNI
MAX_PROPOSAL_THRESHOLD	10.000.000 UNI
quorum	40.000.000 UNI
maxOperations	10
votingDelay	13140 blocchi (15s) = 2 giorni e 6 ore
MIN_VOTING_DELAY	1 blocco ~ pochi secondi
MAX_VOTING_DELAY	40320 blocchi (15s) = 7 giorni
votingPeriod	40320 blocchi (15s) = 7 giorni
MIN_VOTING_PERIOD	5760 blocchi (15s) = 1 giorno
MAX_VOTING_PERIOD	80640 blocchi (15s) = 14 giorni
delay	172800s = 2 giorni
MINIMUM_DELAY	172800s = 2 giorni
MAXIMUM_DELAY	2592000s = 30 giorni
GRACE_PERIOD	1209600s = 14 giorni

Tabella 3.3: Parametri di governance di Uniswap

Concludiamo infine l'analisi della DAO di Uniswap raccogliendo in un unica Tabella 3.4 tutti gli indirizzi dei contratti attualmente in uso.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
Uni	0x1f9840a85d5aF5bf1D1762F925BDADdC4201F984	token
GovernorBravoDelegator	0x408ED6354d4973f66138C91495F2f2FCbd8724C3	governor proxy
GovernorBravoDelegate	0x53a328F4086d7C0F1Fa19e594c9b842125263026	governor implem.
Timelock	0x1a9C8182C09F50C8318d769245beA52c32BE35BC	timelock

Tabella 3.4: Lista indirizzi dei contratti di Uniswap attualmente in uso

3.3 Arbitrum

Arbitrum DAO è un'organizzazione autonoma decentralizzata (DAO) costruita sulla blockchain di Ethereum¹¹. Gli smart contracts di governance della DAO sono implementati sulla catena rollup Arbitrum One, che è una soluzione di scaling di Layer 2 per la blockchain di Ethereum. Questi contratti intelligenti includono il token di governance, ARB, il contratto di governor e di timelock ed il contratto della tesoreria.



Figura 3.4: Arbitrum Logo

Consiglio di Sicurezza L'Arbitrum DAO dispone anche di un meccanismo di sicurezza integrato chiamato Consiglio di Sicurezza¹² il quale è responsabile di garantire la sicurezza e l'integrità della DAO e delle sue catene. Il consiglio può bypassare il lento processo di votazione e agire rapidamente in caso di emergenza. Si compone di 12 membri ed è diviso in due gruppi. Ogni sei mesi si tengono delle elezioni per occupare per un mandato della durata di un anno i seggi in questi due gruppi.

Cosa è richiesto per diventare un candidato al Consiglio di Sicurezza?

- Essere un membro dell'Arbitrum DAO.
- Ottenere il sostegno di almeno lo 0.2% di tutti i token votabili.

Una volta scelti i candidati, tutti i membri dell'Arbitrum DAO votano per i candidati ed i 6 che ricevono il maggior numero di voti saranno eletti nel Consiglio di Sicurezza. Le regole per le elezioni del Consiglio di Sicurezza possono essere modificate

¹¹<https://docs.arbitrum.foundation/concepts/arbitrum-dao>

¹²<https://docs.arbitrum.foundation/concepts/security-council>

dai membri della DAO, ma queste modifiche non possono essere apportate durante un'elezione in corso.

I membri del Consiglio di Sicurezza possono anche essere rimossi dalla loro posizione prima della fine del loro mandato se almeno il 10% di tutti i token votabili partecipa a un voto di rimozione e almeno i 5/6 dei voti sono a favore della rimozione. Un membro può anche essere rimosso se almeno 9 su 12 dei membri del Consiglio di Sicurezza votano a favore della rimozione.

3.3.1 Token ARB

Il token ARB è un token di governance ERC-20 che consente ai suoi detentori di partecipare al protocollo di governance on-chain dell'Arbitrum DAO¹³.



Figura 3.5: ARB Token

I token ARB vengono utilizzati dai membri dell'organizzazione per votare le proposte on-chain segnalando il proprio supporto o la propria opposizione. Più token un membro possiede, maggiore sarà l'influenza del suo voto. Questo perché gli smart contract dell'Arbitrum DAO sono implementati in modo tale che il potere di un voto sia determinato precisamente dal numero di token che il portafoglio del votante rappresenta (1T1V). È importante anche notare che i token possono essere delegati tramite Tally ad altri portafogli. Ciò significa che si può votare utilizzando i propri ARB (quelli nel tuo portafoglio), oppure utilizzando i token di qualcun altro, a condizione che il proprietario di tali token ti abbia delegato il proprio potere di voto.

Lo smart contract che definisce il token di governance ARB è registrato come proxy

¹³<https://docs.arbitrum.foundation/concepts/arb-token>

(EIP-1967 Transparent Proxy) sulla rete Arbitrum One all'indirizzo:

0x912CE59144191C1204E64559FE8253a0e49E6548

mentre la sua implementazione è registrata all'indirizzo:

0xC4ed0A9Ea70d5bCC69f748547650d32cC219D882

Esistono inoltre gli indirizzi relativi al corrispettivo proxy di livello 1 del token ARB, ovvero il contratto depolyato sulla catena di Ethereum che è:

0xB50721BCf8d664c30412Cfbc6cf7a15145234ad1

ed il corrispondente contratto di implementazione con indirizzo:

0xAD0C361Ef902A7D9851Ca7DcC85535DA2d3C6Fc7

Il protocollo non prevede un hard cap fisso ma definisce un meccanismo di inflazione annuale secondo cui la quantità di token che può essere coniata in una singola operazione è limitata da un tasso massimo di inflazione del 2% dell'offerta totale corrente secondo la formula:

$$\text{amount} \leq \frac{\text{totalSupply}() \times \text{MINT_CAP_NUMERATOR}}{\text{MINT_CAP_DENOMINATOR}} = \frac{\text{totalSupply}() \times 200}{10000}.$$

In tempo minimo che deve passare tra due operazioni di conio è definito tramite il parametro `MIN_MINT_INTERVAL` = 365 giorni. Attualmente l'offerta totale è pari a 10.000.000.000 ARB di cui 5.826.785.045 ARB sono effettivamente in circolazione¹⁴.

3.3.2 Processo di governance e analisi dei contratti

Le proposte in Arbitrum vengono chiamate AIP o Proposte di Miglioramento Arbitrum e si distinguono in:

- **AIP Costituzionali:** Sono quelle che modificano il testo o le procedure della Costituzione o dell'AIP-1, installano o modificano software su qualsiasi catena, o intraprendono qualsiasi azione che richieda l'autorizzazione del `chain owner` su qualsiasi catena.

¹⁴03.02.2026, <https://coinmarketcap.com/it/currencies/arbitrum/>

- **AIP non Costituzionali:** Sono tutte le altre AIP, come quelle che richiedono fondi/sovvenzioni o che forniscono linee guida o informazioni generali alla comunità.

Il processo di governance della DAO di Arbitrum prevede i seguenti passaggi¹⁵.

Passaggio 1: Temperature check formale tramite sondaggio Snapshot

Come prima cosa si crea un nuovo post con la propria proposta sul forum di governance avviando così una discussione all'interno della comunità.

Dopodichè si procede con la creazione di un sondaggio su Snapshot che misurerà l'interesse della comunità per la proposta. Il sondaggio dura in genere una settimana e viene deciso a maggioranza semplice. Se la tua proposta supera la verifica preliminare, dopo aver modificato la proposta in base al feedback della comunità si può passare al secondo e ultimo passaggio: un voto on-chain facilitato da Tally.

Passaggio 2: Presentazione e votazione della proposta on-chain con Tally

Superato il primo step è necessario usare Tally per presentare la proposta on-chain e renderla eseguibile. Per farlo però è necessario che il portafoglio del proponente disponga di almeno 1.000.000 ARB. A seconda del tipo di proposta che si sta eseguendo è anche necessario selezionare a quale governor indirizzare la proposta:

- **Arbitrum Core:** Per Proposte Costituzionali.
- **Arbitrum Treasury:** Per Proposte non Costituzionali.

Una proposta viene approvata dopo un periodo di votazione della durata di 14 giorni (con possibilità di estensione di 2 giorni) se vengono soddisfatte due condizioni:

- Vengono espressi più voti a favore che contro (maggioranza semplice).
- Il numero totale di voti espressi a favore è almeno token votabili: 4.5% per un'AIP Costituzionale oppure 3% per un'AIP non Costituzionale.

¹⁵<https://docs.arbitrum.foundation/how-tos/create-submit-dao-proposal>

Le proposte costituzionali prima di essere effettivamente eseguite devono inoltre superare una serie di ritardi (Figura 3.6) per consentire ai membri contrari alla proposta di uscire dall'organizzazione prima che l'azione diventi definitiva¹⁶.



Figura 3.6: Ritardi di esecuzione nelle proposte di Arbitrum

- *Timelock di Arbitrum One – 3 giorni*: Dopo essere stata approvata, una proposta viene consegnata a un timelock su Arbitrum One. Lo scopo di questo ritardo è consentire agli utenti di avviare eventuali prelievi dalla catena.
- *Ritardo del Messaggio L2 → L1 – Circa 1 settimana*: Tutte le proposte devono essere inviate verso L1 prima di essere eseguite (anche se alla fine l'esecuzione avverrà nuovamente su un L2). Ciò garantisce che qualsiasi transazione effet-

¹⁶<https://github.com/ArbitrumFoundation/governance/blob/main/docs/overview.md>

tuata dagli utenti durante il ritardo precedente possa essere elaborata prima dell'aggiornamento.

- *Ritardo su Ethereum Mainnet L1 – 3 giorni*: La proposta di aggiornamento subisce un ulteriore ritardo dopo aver raggiunto L1, garantendo che tutti i prelievi avviati prima della proposta di aggiornamento siano idonei per l'esecuzione.

A questo punto le proposte di successo vengono automaticamente eseguite sul L2.

Passiamo ora ad analizzare tutti i contratti (riportati in Tabella 3.5) registrati su Arbitrum One che sono coinvolti nel processo di governance della DAO.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
Transparent UpgradeableProxy	0x912CE59144191C1204E64559FE8253a0e49E6548	token proxy
L2ArbitrumToken	0xC4ed0A9Ea70d5bCC69f748547650d32cC219D882	token implemen.
Transparent UpgradeableProxy	0xf07DeD9dC292157749B6Fd268E37DF6EA38395B9	governor proxy
Transparent UpgradeableProxy	0x789fC99093B09aD01C34DC7251D0C89ce743e5a4	treasury governor proxy
L2ArbitrumGovernor	0x065620d99E1785Cc56Fa95462d3012Eb844FDC9	governor implemen.
Transparent UpgradeableProxy	0x34d45e99f7D8c45ed05B5cA72D54bbD1fb3F98f0	timelock proxy
Transparent UpgradeableProxy	0xbFc1FECa8B09A5c5D3EFfE7429eBE24b9c09EF58	treasury timelock proxy
ArbitrumTimelock	0x41740588b86B4e0629b83A4e28786FF94361c3A3	timelock implemen.
Transparent UpgradeableProxy	0xF3FC178157fb3c87548bAA86F9d24BA38E649B58	treasury proxy
FixedDelegate Erc20Wallet	0x9F43ab02cACc8e709b05936a92dC85b76D1523c4	treasury implemen.

Tabella 3.5: Lista indirizzi dei contratti su Arbitrum One ChainID:42161

Governor Facendo riferimento a tale tabella come prima cosa possiamo osservare che i contratti di tipo governor nel caso di Arbitrum come abbiamo visto risultano essere due. Il **Core Governor** di indirizzo:

0xf07DeD9dC292157749B6Fd268E37DF6EA38395B9

ed il **Treasury Governor** di indirizzo:

0x789fC99093B09aD01C34DC7251D0C89ce743e5a4

Tali contratti sono entrambi definiti come proxy (EIP-1967 Transparent Proxy) i quali puntano entrambi alla medesima implementazione di indirizzo:

0x065620d99E1785Ccf56Fa95462d3012Eb844FDC9

Tale contratto è definito utilizzando la struttura modulare ottenibile usando le librerie di OpenZeppelin.

Timelock I contratti di timelock sono a loro volta due proxy (EIP-1967 Transparent Proxy), uno per ogni tipo di governor. Il **Core Timelock** ha indirizzo:

0x34d45e99f7D8c45ed05B5cA72D54bbD1fb3F98f0

mentre il **Treasury Timelock** ha indirizzo:

0xbFc1FECa8B09A5c5D3EFfE7429eBE24b9c09EF58

come nel caso del governor, entrambi puntano ad uno stesso contratto di implementazione **ArbitrumTimelock** definito all'indirizzo:

0x41740588b86B4e0629b83A4e28786FF94361c3A3

Tale contratto è basato sul **TimelockControllerUpgradeable** di OpenZeppelin, ma introduce modifiche per adattarsi all'architettura multi-chain di Arbitrum.

Tesoreria La tesoreria di Arbitrum è gestita quasi interamente da un contratto specifico. Come i precedenti contratti è anch'esso definito da un proxy (EIP-1967 Transparent Proxy) di indirizzo:

0xF3FC178157fb3c87548bAA86F9d24BA38E649B58

che punta all'implementazione distribuita all'indirizzo:

0x9F43ab02cACc8e709b05936a92dC85b76D1523c4

La caratteristica più importante di questo contratto è la gestione dei diritti di voto tramite **delega fissa**. Appena il contratto viene inizializzato, esso delega i diritti di voto di tutti i token ARB che detiene a un indirizzo specificato che non può essere più modificato. L'attuale volume della tesoreria di Arbitrum è 358.525.287\$ ed è costituito quasi interamente dagli asset detenuti in tale contratto.¹⁷.

Concludiamo la nostra analisi raccogliendo nella Tabella 3.6 tutti i parametri che partecipano alla definizione del processo di governance.

<i>Parametro</i>	<i>Valore</i>
proposalThreshold	1.000.000 ARB
$\text{quorum} = \frac{\text{quorumNumerator}}{\text{quorumDenominator}}$ (Core Governor)	4.5% della supply totale
$\text{quorum} = \frac{\text{quorumNumerator}}{\text{quorumDenominator}}$ (Treasury Governor)	3% della supply totale
lateQuorumVoteExtension	14400 blocchi (12s) = 2 giorni
votingPeriod	100800 blocchi (12s) = 14 giorni
votingDelay	21600 blocchi (12s) = 3 giorni
minDelay (Core Timelock)	691200s = 8 giorni
minDelay (Treasury Timelock)	259200s = 3 giorni

Tabella 3.6: Parametri usati nel processo di governance di Arbitrum DAO

Osservazione 3.3. *I parametri per cui non è specificato lo specifico contratto di appartenenza assumono il medesimo valore per entrambi i contratti di governor.*

Osservazione 3.4. *Nella tabella comparativa finale faremo riferimento al Treasury Governor e Timelock poichè le AIP Costituzionali sono le proposte più frequenti.*

3.4 Aave

Aave è un protocollo di liquidità decentralizzato e non custodiale, in cui gli utenti possono partecipare come fornitori o mutuatari. I fornitori offrono i propri asset

¹⁷03.02.2026, <https://www.tally.xyz/gov/arbitrum/treasury>

a pool di liquidità e guadagnano interessi, mentre i mutuatari possono prendere in prestito liquidità da tali pool fornendo garanzie (collaterale) di valore superiore all'importo preso in prestito mediante l'uso dei propri asset ¹⁸.



Figura 3.7: AAVE Logo

Una delle caratteristiche principali del protocollo di liquidità decentralizzato è la sua natura non custodiale, il che significa che gli utenti mantengono sempre il controllo sui propri asset. L'interazione con il protocollo avviene tramite wallet self-custodial, che consentono di fornire o prendere in prestito fondi direttamente, senza la necessità di intermediari¹⁹. In quanto piattaforma DeFi, Aave include inoltre una vasta gamma di funzionalità, dal proprio stablecoin nativo GHO ai contratti periferici che semplificano operazioni complesse come gli swap di asset e i rimborsi dei prestiti.

Il sistema di governance di AAVE²⁰ è suddiviso in tre componenti principali, ciascuna corrispondente ad una diversa fase del ciclo di vita di una proposta:

1. **Core Network:** Il ruolo di Core Network è assunto dalla Ethereum Mainnet ed agisce come livello di regolamento e sicurezza in cui risiede il potere di voto. Gestisce le validazioni di alto livello sulle proposte e i saldi dei token di governance.
2. **Voting Networks:** Raccoglie gli ambienti in cui avviene la votazione. Si tratta di reti con bassi costi di transazione, come Polygon POS e Avalanche

¹⁸<https://aave.com/docs>

¹⁹<https://aave.com/docs/developers/liquidity-protocol>

²⁰<https://aave.com/docs/developers/governance>

C-Chain, che permettono agli utenti di votare senza spostare fondi dalla rete principale.

3. **Execution Networks:** Riunisce le reti in cui vengono registrati ed eseguiti i payload delle proposte approvate su tutte le reti coinvolte — incluse le Voting Networks e la Core Network.

La comunicazione tra questi componenti è gestita dall'Aave Delivery Infrastructure (a.DI), che garantisce interazioni cross-chain sicure ed efficienti.

3.4.1 Tokens AAVE e GHO

AAVE Aave è governato dai detentori del token AAVE, i quali possono proporre, votare e implementare modifiche al protocollo, tra cui la regolazione dei tassi di interesse, la modifica dei requisiti di collaterale e di altri parametri chiave che possono influenzare sia i mutuatari che i fornitori. AAVE è quindi il token di governance nativo del protocollo, esso segue lo standard ERC-20 ed è distribuito sulla blockchain di Ethereum all'indirizzo:

0x7Fc66500c84A76Ad7e9c93437bFc5Ac33E2DDaE9

Esso però è accessibile tramite diverse exchange, sia centralizzate che decentralizzate.



Figura 3.8: AAVE Token

I token AAVE possono essere forniti ai pool di liquidità all'interno del protocollo Aave o a pool esterni, come quelli presenti sugli exchange decentralizzati (DEX), consentendo agli utenti di ottenere rendimenti. Gli utenti possono inoltre mettere in staking i propri token AAVE nel safety module, contribuendo alla sicurezza del siste-

ma fornendo una garanzia in caso di insolvenza e ricevendo ricompense in cambio²¹.

Il contratto di AAVE presentato sopra è un proxy (EIP-1967 Transparent Proxy) che punta al contratto di implementazione **AaveTokenV3** di indirizzo:

0x5D4Aa78B08Bc7C530e21f7447988b1Be7991322

La versione precedente **AaveTokenV2** è definita invece all'indirizzo:

0x96F68837877fd0414B55050c9e794AECdBcfCA59

Il contratto attuale è una modernizzazione e refactoring del precedente che migliora la struttura del codice in termini di modularità e implementa l'adozione delle nuove caratteristiche di sicurezza di Solidity.

Nel protocollo di AAVE non è previsto un hard cap massimo. E' possibile però conoscere l'offerta totale corrente che è pari a 16.000.000 AAVE di cui 15.323.112,5 AAVE sono effettivamente in circolazione²².

GHO GHO è un token ERC-20 distribuito su Ethereum all'indirizzo:

0x40D16FC0246aD3160Ccc09B8D0D3A2cD28aE6C2f

GHO è definito per mantenere il valore ancorato al dollaro statunitense (USD), esso è una stablecoin decentralizzata e sovra-collateralizzata, completamente sostenuta e nativa del protocollo.



Figura 3.9: GHO Token.

GHO funziona tramite un modello a facilitatori (facilitator model) che sono contratti

²¹<https://aave.com/docs/developers/aave>

²²04.02.2026, <https://coinmarketcap.com/currencies/aave/>

approvati dalla governance di Aave, con la capacità di emettere (mint) e bruciare (burn) token GHO, ciascuno entro un limite di conio definito dalla governance²³.

3.4.2 Processo di Governance e meccanismi di voto

Il ciclo di vita di una proposta è stato progettato con cura per consentire ai membri della comunità di presentare idee, votare ed implementare le modifiche approvate in maniera trasparente e ordinata.²⁴ Tale ciclo si compone di 6 fasi:

Fase 1: Governance Forum Il processo inizia con un'idea pubblicata nel Forum di Governance Aave²⁵, dove si svolgono le prime discussioni e si raccolgono i feedback della comunità. Con questa prima fase è possibile raffinare la proposta in funzione di quelli che sono stati i riscontri della comunità passare allo step successivo.

Fase 2: Temp Check (Votazione Snapshot) Dopo la discussione, la proposta passa alla fase di TEMP CHECK nella Snapshot Space di Aave²⁶. Si tratta di una votazione informale e non vincolante, che serve a misurare il sentimento della comunità e a capire se c'è sufficiente interesse a proseguire. Le proposte in questa fase non richiedono dettagli tecnici approfonditi.

Fase 3: ARFC (Aave Request for Final Comments) Se il TEMP CHECK ha esito positivo, la proposta passa allo stadio ARFC che si svolge ancora off-chain sulla piattaforma Snapshot, dove subisce un'analisi più approfondita. I service provider e i membri della comunità offrono feedback dettagliati su come la proposta influirebbe sul protocollo, preparando il terreno per la fase AIP.

Fase 4: AIP (Aave Improvement Proposal) Nella fase AIP, la proposta, che diventa una sottomissione on-chain formale, si compone di due parti: i metada-

²³<https://aave.com/docs/developers/gho>

²⁴<https://aave.com/docs/developers/governance>

²⁵<https://governance.aave.com/>

²⁶<https://snapshot.org/#/aave.eth>

ti (archiviati su IPFS) ed il payload del contratto. Entrambe vengono presentate attraverso i contratti di governance Aave, principalmente sulla Ethereum Mainnet.

Fase 5: Votazione Una volta inviata, la proposta entra nello stato PENDING, poi diventa ACTIVE per la votazione. La votazione avviene on-chain tramite opportune interfacce di governance tra cui Aave Labs²⁷. Una proposta ha successo se raggiunge i requisiti di quorum e differenziale di voto; in caso contrario, fallisce.

Fase 6: Esecuzione Le proposte approvate passano alla fase di esecuzione, attraverso l'infrastruttura di governance di Aave. A seconda del tipo di proposta, viene applicato un timelock (di 1 giorno o 7 giorni) prima della reale implementazione.

3.4.3 Analisi dei contratti di governance

Nel corso del tempo la governance di Aave ha subito delle evoluzioni, l'analisi dei contratti dunque farà riferimento ai principali moduli (governor e timelock) sia attualmente in uso sia quelle precedenti.

Governor La versione passata (ora in disuso) del contratto di governor **AaveGovernanceV2** ha indirizzo:

0xEC568fffba86c094cf06b22134B23074DFE2252c

tale contratto prende ispirazione dal modello di Compound ma lo evolve in una struttura più modulare e flessibile. Poi con la nascita di AAVE V3, l'ultima versione del protocollo (settembre 2021), il contratto è stato sostituito con il proxy (EIP-1967):

0x9AEE0B04504CeF83A65AC3f0e838D0593BCb2BC7

la cui implementazione è definita all'indirizzo:

0x58BcB647C4beFf253B4B6996c62F737B783f2cDd

Tale contratto è estremamente personalizzato e rappresenta lo stato dell'arte della governance Cross-Chain. Non segue nessuna delle strutture standard.

²⁷<https://app.aave.com/>

Timelock Aave come mostrato nella Figura 3.8 prevede due tipologie di votazioni differenti a cui sono associate differenti esecuzioni. Per questo motivo esistono due contratti di timelock distinti. Inizialmente esistevano **Short Executor** di indirizzo:

0xEE56e2B3D491590B5b31738cC34d5232F378a8D5

e **Long Executor** di indirizzo:

0x61910EcD7e8e942136CE7Fe7943f956cea1CC2f7

i quali seguiva fedelmente il pattern introdotto da Compound Finance. Dopodichè con lo sviluppo dell'aspetto multi-chain di Aave questi sono stati sostituiti da **Executor L1** per le esecuzioni sulla mainnet e **Executor L2** per le esecuzioni sulle altre chain. Tali esecutori rimandano poi ad un terzo contratto (il medesimo per entrambi) che è il vero responsabile delle esecuzioni delle decisioni. Esso è un proxy (EIP-1967 Transparent Proxy) di indirizzo:

0xdAbad81aF85554E9ae636395611C58F7eC1aAEc5

la cui implementazione ha indirizzo:

0x7222182cB9c5320587b5148BF03eeE107AD64578

Tale contratto non segue più il modello di timelock di Compound ma implementa standard moderni di interoperabilità permettendo l'esecuzione anche su altre chain.

Tesoreria La tesoreria (complessiva) di AAVE²⁸ si calcola considerando il valore totale in USD di tutti gli asset detenuti negli indirizzi delle tesorerie di Aave che sono distribuiti sulle varie reti blockchain. Nello specifico il calcolo aggrega i saldi dei token provenienti da indirizzi di tesoreria predefiniti su 13 diverse blockchain. Per quanto riguarda la mainnet di Ethereum gli indirizzi di tesoreria sono 8. Di questi consideriamo i due principali, il primo è un proxy (EIP-1967) di indirizzo:

0x25f2226b597e8f9514b3f68f00f494cf4f286491

con implementazione **AaveEcosystemReserveV2** distribuita all'indirizzo:

0x10c74b37Ad4541E394c607d78062e6d22D9ad632

²⁸<https://tokenterminal.com/explorer/projects/aave/metrics/treasury>

che può essere classificato come *Streaming-based Protocol Treasury* poichè introduce logiche finanziarie avanzate che lo rendono un sistema di gestione patrimoniale attivo. L'altro **CollectorWithCustomImpl** è anch'esso un proxy (EIP-1967) di indirizzo:

0x464C71f6c2F760DdA6093dCB91C24c39e5d6e18c

con implementazione:

0x83b7Ce402A0E756E901C4A9d1cAfa27cA9572afC

il quale funge da "raccolgitore" primario di tutte le commissioni generate dal protocollo. Possiamo quindi classificarlo come una *Revenue Collection Treasury*.

Il volume totale della tesoreria, calcolato secondo il metodo descritto è 150.900.000\$²⁹.

Concludiamo dunque l'analisi raccogliendo nella Tabella 3.7 gli indirizzi dei contratti di governance in uso attualmente e nella Tabella 3.8 i parametri di governance ad essi associati.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
InitializableAdmin UpgradeabilityProxy	0x7Fc66500c84A76Ad7e9c93437bFc5Ac33E2DDaE9	token proxy
AaveTokenV3	0x5D4Aa78B08Bc7C530e21f7447988b1Be7991322	token implem.
Transparent UpgradeableProxy	0x9AEE0B04504CeF83A65AC3f0e838D0593BCb2BC7	governor proxy
Governance	0x58BcB647C4beFf253B4B6996c62F737B783f2cDd	governor implem.
Executor	0x5300A1a15135EA4dc7aD5a167152C01EFc9b192A	executor L1
Executor	0x17Dd33Ed0e3dD2a80E37489B8A63063161BE6957	executor L2
Transparent UpgradeableProxy	0xdAbad81aF85554E9ae636395611C58F7eC1aAEc5	timelock proxy
PayloadsController	0x7222182cB9c5320587b5148BF03eeE107AD64578	timelock implem

Tabella 3.7: Lista indirizzi dei contratti di Aave attualmente in uso.

²⁹04.02.2026,<https://tokenterminal.com/explorer/projects/aave/metrics/treasury-net>

<i>Parametro</i>	<i>Valore</i>
proposalThreshold	80.000 AAVE
quorum	320.000 AAVE
votingPeriod	19200 blocchi (12s) $\simeq$ 3 giorni
votingDelay	7200 blocchi (12s) = 1 giorno
MIN_EXECUTION_DELAY	86400s = 1 giorno
MAX_EXECUTION_DELAY	864000s = 10 giorni
delay	86400s = 1 giorno
EXPIRATION_DELAY (of payloads)	3024000s = 35 giorni
GRACE_PERIOD	604800s = 7 giorni

Tabella 3.8: Parametri del processo di governance di Aave

3.5 Sky

Il Protocollo Sky è una piattaforma di finanza decentralizzata (DeFi) costruita su Ethereum e rappresenta l'evoluzione avanzata del precedente Protocollo MakerDAO, progettato in modo tale da essere più scalabile, modulare e accessibile agli utenti³⁰. Il suo obiettivo principale rimane lo stesso del suo predecessore: creare e gestire una stablecoin decentralizzata e collateralizzata.



Figura 3.10: SKY Logo

L'Ecosistema Sky è una rete guidata dalla community di progetti decentralizzati noti come **Sky Stars**. Questi progetti indipendenti favoriscono un'innovazione e una crescita rapida all'interno del framework più ampio di Sky. Ogni Sky Star può avere

³⁰<https://www.binance.com/it/academy/articles/what-is-sky-sky>

il proprio token di governance, la propria tesoreria e governance, allineandosi però agli obiettivi complessivi dell'ecosistema.

L'accesso all'ecosistema avviene tramite **Sky.money**³¹, un portale non-custodial che collega gli utenti a protocollo di Sky. Attraverso esso, gli utenti possono:

- Effettuare il trading tra token popolari ed i token dell'ecosistema (USDS, SKY).
- Accedere alle funzionalità di risparmio e ricompense della piattaforma.

Per garantire scalabilità ed economicità, viene introdotto **SkyLink** che funge da sistema di bridging che connette Sky con molteplici reti Layer 2. SkyLink quindi permette di spostare i token USDS e SKY tra le reti, consentendo agli utenti di utilizzare funzionalità come lo Sky Savings Rate senza pagare elevate commissioni gas o attendere a lungo per le transazioni.

Per far fruttare gli asset l'ecosistema fornisce ai membri della comunità differenti meccanismi:

- **Sky Savings Rate (SSR)**: L'SSR è un sistema automatizzato che consente di guadagnare USDS composti nel tempo. Quando si deposita USDS nel modulo SSR, si ricevono token sUSDS, che rappresentano la propria partecipazione e il valore guadagnato. I token USDS vengono aggiunti alla pool ogni pochi secondi in base all'attuale tasso SSR (deciso tramite votazioni di governance on-chain), facendo crescere il valore di sUSDS che possono essere riscattati in qualsiasi momento per ricevere gli USDS originali più eventuali ricompense accumulate.

Osservazione 3.5. *La conversione tra USDS e sUSDS è gestita automaticamente dagli smart contract.*

- **Sky Token Rewards (STR)**: I detentori di USDS possono partecipare al modulo STR per guadagnare SKY come ricompense che vengono distribuite in base alla quota detenuta da ciascun utente nella pool delle ricompense.

³¹<https://vote.sky.money/>

3.5.1 Token di governance e Stablecoin

Token di governance Il token di governance che regola il protocollo della DAO è il token ERC-20 SKY, registrato su ethereum all'indirizzo:

0x56072C95FAA701256059aa122697B133aDEd9279

esso risulta essere il sostituto del token ERC-20 MKR definito all'indirizzo:

0x9f8F72aA9304c8B593d555F12eF6589cC3A579A2

che rappresentava il token di governance di MakerDAO prima del rebranding.

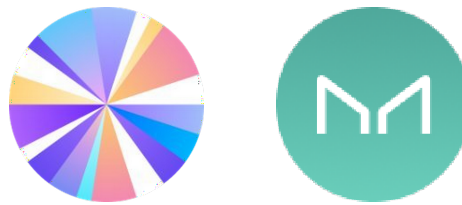


Figura 3.11: SKY e MKR Tokens

La conversione tra questi token avviene tramite uno specifico contratto chiamato convertitore MKR-SKY e definito all'indirizzo:

0xA1Ea1bA18E88C381C724a75F23a130420C403f9a

il quale abilita conversioni bidirezionali tra i token MKR e SKY, utilizzando le funzioni di mint e burn di entrambi i token. Il tasso di cambio è fisso a 1:24.000³².

Per SKY viene indicata un'offerta massima tecnica di 23.462.665.147 SKY che discende quasi automaticamente dal fattore di conversione ed il fatto che l'offerta massima originale di MKR era di 1.000.000 MKR. L'offerta totale di SKY attuale coincide con l'offerta massima mentre l'offerta circolante è 23.006.491.401,01 SKY³³.

Stablecoin USDS è un token conforme allo standard ERC-20 con supporto aggiuntivo per la funzionalità permit e la validazione delle firme per contratti intelligenti

³²<https://developers.sky.money/protocol/tokens/sky/>

³³03.02.2026,<https://coinmarketcap.com/it/currencies/sky/>

EIP-1271³⁴. Il contratto è un proxy distribuito all'indirizzo:

0xdC035D45d973E3EC169d2276DDab16f1e407384F

che punta al contratto di implementazione con indirizzo:

0x1923DfeE706A8E78157416C29cBCCFDe7cdF4102

Come SKY per MKR, USDS è il sostituto della stablecoin DAI associata a MakerDAO prima del rebranding registrata all'indirizzo:

0x6B175474E89094C44Da98b954EedeAC495271d0F



Figura 3.12: USDS e DAI Stablecoins

Il convertitore DAI-USDS (registrato al seguente indirizzo) facilita le conversioni 1:1 tra DAI e USDS, fornendo un modo semplice per scambiare i due token.

0x3225737a9Bbb6473CB4a45b7244ACa2BeFdB276A

3.5.2 Processo di governance e meccanismo di voto

Il processo di governance di SKY non ha subito variazioni strutturali rispetto a quello previsto da MakerDAO, infatti tutto ciò che riguarda il processo di governance ed i meccanismi di votazione definito nella documentazione di MakerDAO³⁵ è stato applicato e trasferito al rebranding SKY. Il ciclo di governance della DAO prevede specifiche fasi che si sviluppano a cadenza mensile e settimanale.

³⁴<https://developers.sky.money/protocol/tokens/usds/>

³⁵<https://manual.makerdao.com/>

Ciclo di governance mensile Il ciclo di governance mensile fornisce una cadenza prevedibile con cui vengono prese le decisioni di governance³⁶.

Il ciclo di governance mensile è utilizzato prevalentemente per l'introduzione di nuovi MIP (Maker Improvement Proposals) o subproposte MIP nel Protocollo Maker. Esempi di tali modifiche possono includere l'aggiunta di una nuova Core Unit (CU) al Protocollo, l'aggiustamento del budget operativo di una CU esistente, ecc. . .

- **Settimana 1**

- Da lunedì a mercoledì: Gli Autori dei MIP spostano le loro proposte in: *Formal Submission*. Questa fase dura 3 giorni.
- Giovedì: I Governance Facilitators eseguono la Revisione della Presentazione come parte della riunione settimanale di Governance e Rischio e comunicano quali dei MIP proposti sono in linea con le linee guida. Dopodiché devono raggiungere un consenso affinché le proposte procedano ad un Sondaggio di Ratifica altrimenti possono bloccarle se ritengono che questo possa influire negativamente sulla comunità. I MIP che soddisfano le linee guida e non sono ritenuti discutibili dai Facilitatori della Governance proseguiranno alla fase del Sondaggio di Ratifica.

- **Settimana 2**

- Lunedì: I Facilitators pubblicano l'insieme dei sondaggi di Ratifica su GitHub e vengono presentati on-chain in modo tale da farli apparire sul portale ufficiale di voto (per SKY: Sky.money). Tali sondaggi prevedono un periodo di votazione di 2 settimane.

- **Settimana 4**

- Lunedì: I sondaggi vengono chiusi ed ogni proposta viene contrassegnata come *Accettata* o *Rifiutata* dagli Editor dei MIP.
- Giovedì: I Facilitators effettuano una revisione del ciclo che si è svolto riassumendolo e discutendone con la comunità.

³⁶<https://manual.makerdao.com/governance-processes/governance-cycle/monthly-governance-cycle>

Ciclo di governance settimanale Il ciclo di governance settimanale lavora in congiunzione con il ciclo di governance mensile ma consente di prendere decisioni ricorrenti che richiedono un'azione più rapida di quella permessa dal ciclo mensile³⁷.

- **Sondaggio settimanale standard:** è un sondaggio di governance non vincolante che determina i contenuti del voto esecutivo settimanale. Essi non possono modificare i parametri di sistema in modo indipendente; dettano semplicemente ciò che sarà incluso nel successivo voto esecutivo.
- **Sondaggio settimanale non standard:** è un sondaggio non vincolante che contiene decisioni arbitrarie e urgenti (time-sensitive). Questi sondaggi devono essere accelerati attraverso il processo di governance Maker tramite un voto separato. L'uso di questi sondaggi è esclusivo dei Facilitators, dato che hanno già stabilito un alto livello di fiducia con la comunità.

La ripartizione del ciclo di governance settimanale standard si sviluppa come segue.

- **Settimana 1**

- Lunedì: Ogni lunedì, il ciclo settimanale inizia e include decisioni ricorrenti standard proposte sotto forma di un sondaggio settimanale che avrà una durata di tre giorni.
- Gli opportuni Facilitators confermeranno i contenuti del voto esecutivo e consegneranno la copia dello spell (codice di esecuzione) al Consiglio Consultivo il quale preparerà e revisionerà uno spell sulla testnet.

- **Settimana 2**

- Lunedì-Mercoledì: Il Consiglio Consultivo inizierà a scrivere lo spell per la mainnet che verrà poi dispiegato il martedì.
- Mercoledì: I Facilitators aggiungeranno il voto esecutivo al portale di voto (per SKY: Sky.money) e lo comunicheranno alla comunità. Il voto esecutivo settimanale ha una scadenza di trenta giorni.

³⁷<https://manual.makerdao.com/governance-processes/governance-cycle/weekly-governance-cycle>

Osservazione 3.6. *Dal punto di vista della governance off-chain non è strettamente richiesta, è però possibile svolgere discussioni sul forum³⁸, il quale consente anche la creazione di sondaggi per misurare il sentimento della comunità oppure su Discord³⁹.*

I detentori di token SKY per imporre il proprio voto (1T1V) possono affidare il loro potere di voto a uno o più delegati scelti, i quali voteranno a loro nome oppure votare autonomamente non appena il wallet per il voto è stato configurato.

3.5.3 Analisi dei contratti di governance

Governor Il governor è di tipo Approval Voting in cui a differenza dei sistemi di voto classici "una tantum", prevedono votazioni in uno stato persistente. Nel corso del tempo sono state implementate tre versioni del modulo di governor, a partire dalle versioni originali usate prima del rebranding. La prima versione del contratto è stata distribuita all'indirizzo:

0x8E2a84D6adE1E7ffFEe039A35EF5F19F13057152

La seconda versione invece ha indirizzo:

0x0a3f6849f78076aefaDf113F5BED87720274dDC0

e costituisce un'aggiornamento della precedente costruito migliorando il codice senza apportare modifiche in termini di logica di base. L'ultima versione invece di indirizzo:

0x929d9A1435662357F54AdcF64DcEE4d6b867a6f9

è quella attualmente in uso e presenta una differenza chiave nella gestione del token di governance. Con questo aggiornamento infatti non viene più utilizzato il token non votante IOU come token di voto. Gli utenti bloccano il token di governance SKY e lo sbloccano direttamente.

Timelock Il ruolo di timelock è gestito dal contratto **DSPause** di indirizzo:

0xbE286431454714F511008713973d3B053A2d38f3

³⁸<https://forum.sky.money/>

³⁹<https://discord.com/invite/skyecosystem>

Nella Tabella 3.9 sono riportati tutti i valori dei parametri coinvolti nel processo di governance di Sky che troviamo definiti nei precedenti contratti.

<i>Parametro</i>	<i>Valore</i>
launchThreshold (I avvio)	2.400.000.000 SKY
delay	86400s = 1 giorno

Tabella 3.9: Parametri di governance dei contratti di Sky

Tesoreria Il modulo centrale della tesoreria è rappresentato dal proxy di indirizzo:

0xBE8E3e3618f7474F8cB1d074A26afFef007E98FB

il quale punta all'indirizzo di implementazione:

0x3f8650250df9A3Ef830C72720B5BB30B425B92b0

Il volume attuale detenuto il tale contratto è pari a 148.244.171\$⁴⁰.

Concludiamo infine l'analisi di SKY raccogliendo tutti gli indirizzi che attualmente definiscono il processo di governance della DAO nella Tabella 3.10.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
Sky	0x56072C95FAA701256059aa122697B133aDEd9279	governance token
Chief	0x929d9A1435662357F54AdcF64DcEE4d6b867a6f9	governor
DSPause	0xbE286431454714F511008713973d3B053A2d38f3	timelock
DSPauseProxy	0xBE8E3e3618f7474F8cB1d074A26afFef007E98FB	treasury proxy
DssSpellAction	0x3f8650250df9A3Ef830C72720B5BB30B425B92b0	treasury implemen.

Tabella 3.10: Lista indirizzi dei contratti coinvolti nel protocollo di Sky

3.6 Curve DAO

Curve.fi è un exchange decentralizzato non-custodial che ha rivoluzionato il trading di stablecoin. Inizialmente il protocollo si limita a offrire tassi di cambio superiori

⁴⁰03.02.2026, <https://debank.com/profile/0xbe8e3e3618f7474f8cb1d074a26affef007e98fb>

per gli swap di stablecoin tramite liquidity pool, dove gli utenti ottengono un rendimento depositando i propri asset. Con l'evoluzione della piattaforma, iniziano a includere pool di asset volatili, accoppiando criptovalute come ETH con stablecoin come USDT. L'ultima innovazione del protocollo è **crvUSD**, una stablecoin nativa che gli utenti possono prendere in prestito fornendo come garanzia collaterali come ETH in liquid staking e BTC wrapped. Questo sviluppo ha portato alla creazione del più ampio sistema che supporta prestiti garantiti da una gamma più vasta di asset⁴¹.

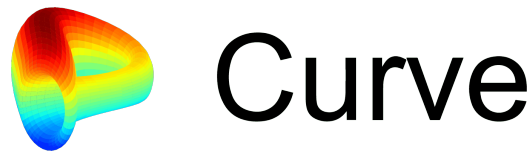


Figura 3.13: Curve Logo

Curve DAO è governata esclusivamente dai suoi membri. I membri ottengono diritti di governance bloccando CRV in token veCRV e hanno più diritti di voto quanto più a lungo li lasciano bloccati prima dello sblocco. Al fianco dei membri dell'organizzazione lavora anche l'EmergencyDAO ovvero un gruppo multisig 5/9 (5 firme su 9) autorizzato per interventi di sicurezza e gestito dal contratto GnosisSafe che ha proxy all'indirizzo⁴²:

`0x467947EE34aF926cF1DCac093870f613C96B1E0c`

ed implementazione definita all'indirizzo:

`0x34CfAC646f301356fAa8B21e94227e3583Fe3F5F`

3.6.1 Token CRV

Il token CRV è il token ERC-20 che governa l'intero ecosistema di Curve Finance. L'indirizzo a cui è registrato è:

`0xD533a949740bb3306d119CC777fa900bA034cd52`

⁴¹<https://resources.curve.finance/getting-started/>

⁴²https://docs.curve.finance/curve_dao/crv-token/

Ci sono 4 principali casi d'uso per il tokenCRV, la maggior parte dei quali richiede di bloccare CRV trasformandoli in veCRV:

- Incentivare i fornitori di liquidità a fornire liquidità a pool e mercati di prestito tramite ricompense in CRV.
- Consentire ai fornitori di liquidità di aumentare le proprie ricompense in CRV fino a 2,5 volte detenendo veCRV.
- Consentire agli utenti di partecipare e votare sulle proposte di governance.
- Raccogliere una parte delle commissioni derivanti dagli swap e dai prestiti che avvengono su Curve detenendo veCRV.

L'indirizzo del contratto che definisce il token veCRV è:

`0x5f3b5DfEb7B28CDbD7FABA78963EE202a494e2A2`

Nello specifico la quantità di token veCRV ottenuti a partire da una data quantità di token CRV bloccati è definita dalla relazione:

$$\text{veCRV} = \text{CRV bloccati} * (\text{locktime in anni}) / 4$$

La durata massima di blocco è pari a 4 anni, mentre la durata minima è 1 settimana.

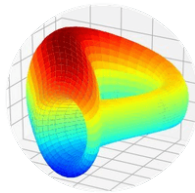


Figura 3.14: CRV Token

L'hard cap previsto dal protocollo è 3.030.303.030,29 CRV ed è distribuito così⁴³:

- 62% ai fornitori di liquidità della comunità;
- 30% agli azionisti (team e investitori) con periodo di maturazione di 2-4 anni;

⁴³<https://resources.curve.finance/crv-token/overview/>

- 5% alla riserva della community;
- 3% ai dipendenti con vesting di 2 anni.

L'offerta iniziale è stata di 1.303.030.303 CRV, i quali erano stati pre-coniati e inviati ai contratti di vesting, che li hanno sbloccati linearmente per 1-4 anni. I nuovi token CRV possono essere conati solo dal contratto minter il cui indirizzo è:

`0xd061D61a4d941c39E5453435B6345Dc261C2fcE0`

I parametri di mining vengono utilizzati per determinare le emissioni dei token, che si basano su epoche. Ad ogni epoca che passa, il tasso di conio verrà ridotto, diminuendo di conseguenza le emissioni complessive di CRV.

L'offerta totale attualmente è 2.348.641.387,14 CRV mentre quella circolante è di 1.461.787.979,62 CRV⁴⁴. I restanti CRV verranno conati lentamente e distribuiti alla community ogni settimana per oltre 200 anni⁴⁵.

3.6.2 Processo di governance e analisi dei contratti

Curve utilizza Aragon per la governance e il controllo della funzionalità di amministrazione del protocollo⁴⁶. Curve ha due diversi agenti di voto, uno per la proprietà e uno per i parametri. L'agente di proprietà viene utilizzato per modifiche critiche come la modifica dell'indirizzo di voto della DAO, mentre l'agente dei parametri è utilizzato principalmente per la modifica dei parametri delle pool.

I membri della comunità, per creare nuove proposte, hanno bisogno di almeno 2.500 veCRV ottenuti bloccando sufficienti token CRV per abbastanza tempo⁴⁷. Per votare su una proposta invece non è richiesta una quantità minima di veCRV è sufficiente che l'utente disponga di un qualunque saldo di veCRV prima che la votazione inizia⁴⁸. Quando si vota sulle proposte del DAO, il potere di voto di un utente su

⁴⁴04.02.2026, <https://coinmarketcap.com/it/currencies/curve-dao-token/>

⁴⁵<https://resources.curve.finance/crv-token/supply-distribution/>

⁴⁶<https://docs.curve.finance/governance/overview/>

⁴⁷<https://resources.curve.finance/governance/locking-crv/>

⁴⁸<https://resources.curve.finance/governance/proposals/>

una specifica proposta inizia a diminuire a metà del periodo di voto, come misura per proteggere dalla manipolazione all'ultimo minuto da parte dei grandi detentori. Nello specifico se per ogni proposta è previsto un periodo di votazione di 7 giorni, votare prima conferisce al tuo voto la massima influenza:

- Primi 3,5 giorni: Il tuo voto ha il pieno (100%) potere di voto.
- Ultimi 3,5 giorni: Il tuo potere di voto diminuisce linearmente fino allo 0% entro la fine del periodo di votazione.

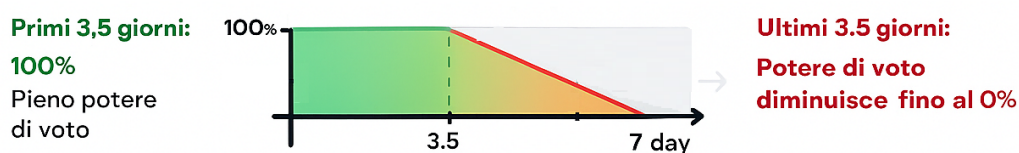


Figura 3.15: Variazione del potere di voto in Curve

Dopo che un voto ha raggiunto le soglie di supporto e quorum, può essere eseguito. L'esecuzione dei voti è completamente permissionless: chiunque può eseguire un voto, non è richiesto un minimo di veCRV, serve solo una piccola quantità di ETH per la gas fee. L'esecuzione può essere effettuata tramite l'interfaccia utente (UI) di Curve⁴⁹ o direttamente dal contratto di voto appropriato.

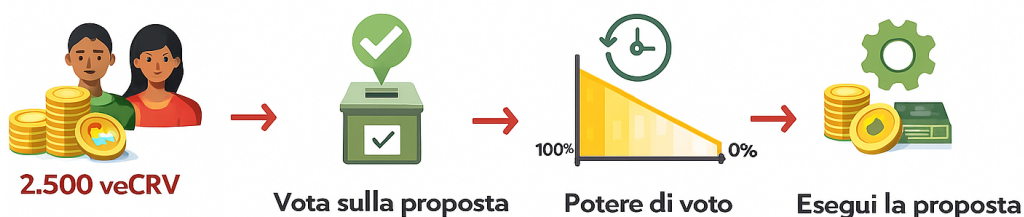


Figura 3.16: Processo di governance di Curve

E' inoltre importante osservare che al fine di poter gestire ed eseguire le attività di governance non solo su Ethereum, ma anche su altre reti come Arbitrum, Optimism, Base e molte altre, Curve ha sviluppato un sistema di governance cross-chain

⁴⁹<https://www.curve.finance/dao/ethereum/proposals>

denominato x-gov⁵⁰. Il voto per le proposte di governance viene condotto esclusivamente sulla mainnet di Ethereum. A seguito di una votazione andata a buon fine, le azioni da eseguire vengono trasmesse a un'altra rete L2 tramite uno specifico contratto **Broadcaster**, dopodichè il contratto **Relayer** riceve il messaggio e lo inoltra al contratto di **Agent** appropriato che compie l'esecuzione automatica delle azioni.

Essendo costruita tramite il framework di Aragon non sono presenti i classici contratti di governor e di timelock. Esiste il contratto **Voting** che interpreta il ruolo di governor ed il contratto **Agent** che invece ha il ruolo di eseguire le decisioni prese, senza però implementare un ritardo di esecuzione come il timelock.

Ownership voting Il contratto di governor di "proprietà" è registrato come proxy (EIP-897 DelegateProxy) all'indirizzo:

0xE478de485ad2fe566d49342Cbd03E49ed7DB3356

La cui implementazione in origine era registrata all'indirizzo:

0x5f990Ee41EB20ee3678B0254aBd128650983aD94

per poi essere sostituita dal contratto di indirizzo:

0xa4D1a2693589840BABb7f3A44D14Fdf41b3bF1Fe

Tale aggiornamento introduce la votazione continua, ovvero consente ai detentori di token di governance di dividere il proprio potere di voto tra le varie opzioni.

Parameter voting Il contratto di governor per i "parametri" è registrato a sua volta come proxy (EIP-897 DelegateProxy) all'indirizzo:

0xBCfF8B0b9419b9A88c44546519b1e909cF330399

La sua implementazione corrisponde al medesimo contratto di quella del governor di "proprietà" sia per la versione originale che per la versione attualmente in uso.

⁵⁰<https://docs.curve.finance/deployments/interactive-deployments/>

Nella Tabella 3.11 sono riportati i parametri chiave usati nel processo di governance.

<i>Parametro</i>	<i>Valore</i>
minTime (tra due votazioni di un utente)	43200s = 3600 blocchi (12s) = 12h
minTimeLowerLimit	43200s = 3600 blocchi (12s) = 12h
minTimeUpperLimit	1209600s = 100.800 blocchi (12s) = 14 giorni
voteTime	604800s = 50.400 blocchi (12s) = 7 giorni
supportRequiredPct	51%
minAcceptQuorumPct	30%
minBalanceLowerLimit	2500 veCRV
minBalanceUpperLimit	50000 veCRV
minBalance	2500 veCRV

Tabella 3.11: Parametri proposte e votazioni di Curve DAO

Agent Come per il governor abbiamo due contratti **Agent** che sono responsabili dell'esecuzione effettiva delle decisioni delle votazioni. In particolare esiste un contratto per le votazioni di "proprietà" e uno per le votazioni per i "parametri".

Il contratto del primo è registrato come proxy (EIP-897 DelegateProxy) all'indirizzo:

0x4EEb3bA4f221cA16ed4A0cC7254E2E32DF948c5f

mentre il secondo, è definito dallo stesso tipo di proxy ma è registrato all'indirizzo:

0x40907540d8a6C65c637785e8f8B742ae6b0b9968

L'implementazione è la stessa per entrambi i contratti ed è definita all'indirizzo:

0x3A93C17FC82CC33420d1809dDA9Fb715cc89dd37

Tesoreria Il contratto di riferimento usato per la tesoreria di Curve DAO ha il seguente indirizzo:

0xe3997288987E6297Ad550A69B31439504F513267

Ad esso è poi stato affiancato un ulteriore contratto di tesoreria il 27 giugno 2025 in cui sono stati allocati il 10% dei ricavi della DAO. Il suo indirizzo è:

0x6508ef65b0bd57eabd0f1d52685a70433b2d290b

L'attuale volume totale della tesoreria di Curve è 2.716.246\$⁵¹.

Concludiamo quindi l'analisi di Curve DAO raccogliendo nella Tabella 3.12 gli indirizzi dei contratti attualmente in uso tra quelli che abbiamo definito ed analizzato che definiscono il processo di governance di Curve DAO.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
Vyper_contract	0xD533a949740bb3306d119CC777fa900bA034cd52	protocol token
Vyper_contract	0x5f3b5DfEb7B28CDbD7FAba78963EE202a494e2A2	governance token
Minter	0xd061D61a4d941c39E5453435B6345Dc261C2fcE0	minter
AppProxyUpgradable	0xE478de485ad2fe566d49342Cbd03E49ed7DB3356	ownership governor
AppProxyUpgradable	0xBCfF8B0b9419b9A88c44546519b1e909cF330399	parameter governor
Voting	0xa4D1a2693589840BABb7f3A44D14Fdf41b3bF1Fe	governor implem.
AppProxyUpgradeable	0x40907540d8a6C65c637785e8f8B742ae6b0b9968	ownership agent
AppProxyUpgradeable	0x4EEb3bA4f221cA16ed4A0cC7254E2E32DF948c5f	parameter agent
Agent	0x3A93C17FC82CC33420d1809dDA9Fb715cc89dd37	agent implem
Vyper_contract	0xe3997288987E6297Ad550A69B31439504F513267	community fund
Treasury	0x6508eF65b0Bd57eaBD0f1D52685A70433B2d290B	treasury

Tabella 3.12: Lista indirizzi dei contratti coinvolti nel protocollo di Curve DAO

3.7 Lido DAO

Lido è la principale soluzione di liquid staking che fornisce un modo semplice per ottenere ricompense dai propri token digitali. Facendo staking con Lido, i token rimangono liquidi e possono essere usati in una gamma di applicazioni DeFi, ottenendo ricompense extra. Sulla base del protocollo di Lido nasce Lido DAO un

⁵¹04.02.2026,<https://debank.com/profile/0x6508ef65b0bd57eabd0f1d52685a70433b2d290b>

organizzazione che gestisce i protocolli di liquid staking scegliendo i parametri chiave tramite votazioni regolate dai detentori del token di governance LDO. Inoltre, la DAO accumulerà le commissioni di servizio e le destinerà alla ricerca, allo sviluppo, agli incentivi per il liquidity mining ed agli aggiornamenti del protocollo⁵².



Figura 3.17: Lido Logo

I membri della DAO governano Lido per garantirne l'efficienza e la stabilità, nello specifico si devono occupare di⁵³:

- Costruire, implementare, aggiornare e decidere i parametri chiave dei protocolli di liquid staking, approvare gli incentivi per le parti che contribuiscono agli obiettivi della DAO.
- Gestire gli operatori dei nodi.
- Approvare le sovvenzioni LEGO per supportare diverse ricerche e iniziative delle "protocol guilds".
- Pagare i collaboratori a tempo pieno e altri collaboratori che si occupano di specifici compiti operativi.
- Gestire l'accumulo delle commissioni di servizio da Lido, che possono essere convogliate nei fondi assicurativi e di sviluppo, distribuiti dalla DAO.

⁵²<https://docs.lido.fi/>

⁵³<https://docs.lido.fi/lido-dao>

3.7.1 Token LDO

LDO è un token conforme a ERC-20 per la governance di Lido, derivato dal MiniMe Token. La caratteristica principale e distintiva di questo tipo di struttura di token ERC-20, è la sua capacità di conservare la cronologia dei saldi di tutti i detentori. Pertanto, i saldi dei detentori di LDO sono interrogabili per un numero di blocco arbitrario, una caratteristica di sicurezza essenziale nel processo di voto di Lido⁵⁴.



Figura 3.18: LDO Token

L'indirizzo Ethereum a cui è registrato il contratto del token è:

`0x5A98FcBEA516Cf06857215779Fd812CA3beF1B32`

Nel protocollo non è previsto un hard cap per il token. La supply totale è 1.000.000.000 LDO mentre la supply effettivamente circolante è pari a 848.066.802,59 LDO⁵⁵.

3.7.2 Processo di governance e analisi dei contratti

La DAO di Lido è governata dai detentori di LDO attraverso un processo regolare che si basa su framework consolidati e piattaforme di voto approvate dalla comunità ed è salvaguardata dai detentori di stETH tramite il sistema di Dual Governance.

Fase 1: Discussione Il primo passo per avviare una proposta consiste nella raccolta di feedback della comunità tramite la pubblicazione di tale proposta sul forum della DAO⁵⁶. Il periodo di discussione dura almeno 7 giorni dopodichè in caso di riscontro positivo e dopo aver integrato i feedback della comunità è possibile passare alle fasi successive.

⁵⁴<https://docs.lido.fi/guides/lido-tokens-integration-guide/#lido>

⁵⁵05.02.2026, <https://coinmarketcap.com/it/currencies/lido-dao/>

⁵⁶<https://research.lido.fi/>

Fase 2: votazione off-chain Il secondo passo consiste in una votazione off-chain su Snapshot⁵⁷. I proponenti possono pubblicare autonomamente le proposte sulla piattaforma ma per farlo gli utenti devono possedere almeno 1.000 LDO al fine di evitare la pubblicazione di proposte spam. Gli utenti senza LDO sufficienti possono richiedere a DAO Ops di creare una proposta per loro conto.

Per essere approvata, dopo un periodo di votazione della durata di 7 giorni, una proposta richiede che l'opzione vincente riceva la maggioranza semplice di tutti i token partecipanti e che riceva un minimo del 5% della fornitura totale di token LDO.

Le votazioni su Snapshot si svolgono una volta al mese di conseguenza tutte le nuove proposte vengono raccolte e lanciate insieme.

Osservazione 3.7. *Se la proposta votata non necessita di azioni on-chain, il successo della votazione off-chain rappresenta già il passo finale, altrimenti si procede con la fase successiva.*

Fase 3: votazione on-chain Per le proposte che lo richiedono dopo il successo della votazione off-chain viene avviata anche una votazione on-chain utilizzando il framework Aragon per la governance⁵⁸.

Per essere approvata, una proposta richiede che l'opzione "Sì" riceva sia un minimo del 5% della fornitura totale di token LDO sia la maggioranza semplice di tutti i token partecipanti. Analogamente se più del 50% dei token votanti e almeno il 5% della fornitura totale di token è contrario, tale proposta sarà rigettata. Se nessuna delle due opzioni riceve almeno il 5% della fornitura totale di token in voti, non viene presa alcuna decisione e la proposta non sarà attuata. La proposta può essere riproposta se non ci sono obiezioni esplicite. Le votazioni on-chain iniziano il mercoledì alle 14:00 e durano 5 giorni articolati come segue:

- **Fase principale:** un periodo di 3 giorni di votazione convenzionale, in cui i partecipanti possono votare "Sì" o "No".

⁵⁷<https://snapshot.box/#/s:lido-snapshot.eth>

⁵⁸<https://vote.lido.fi/>

- **Fase di obiezione:** un periodo di 2 giorni in cui i partecipanti possono votare "No" o cambiare il proprio voto da "Sì" a "No".

Fase 4: Dual Governance Dopo aver superato il voto, le azioni on-chain che riguardano il protocollo Lido su Ethereum entrano in un sistema di Dual Governance in cui un timelock dinamico che consente ai detentori di stETH di estendere il ritardo di esecuzione in base al livello di opposizione⁵⁹. Ogni proposta affronta un ritardo minimo di 3 giorni, dando ai detentori di stETH il tempo di valutare le proposte, dopodichè possono verificarsi differenti situazioni:

- Se i detentori di stETH non sollevano obiezioni, la proposta viene programmata e diventa disponibile per l'esecuzione dopo 24 ore dalla fine dei 3 giorni.
- Se l'opposizione raggiunge una prima soglia dell'1% della fornitura totale di stETH. La proposta viene messa in pausa e il timelock viene prolungato in modo dinamico in proporzione al livello di opposizione.
- Se l'opposizione raggiunge la soglia di blocco del 10% della fornitura totale di stETH al termine del timelock, la proposta viene bloccata o congelata. In questo caso il protocollo entra nello stato di "Rage Quit". La governance e l'esecuzione delle proposte riprendono solo dopo un tempo sufficiente affinché gli staker dissenzienti completino il processo di ritiro dei propri ETH dal protocollo oppure la DAO annulla la proposta contestata.

Le varie fasi che abbiamo presentato sono schematizzate in Figura 3.19⁶⁰.

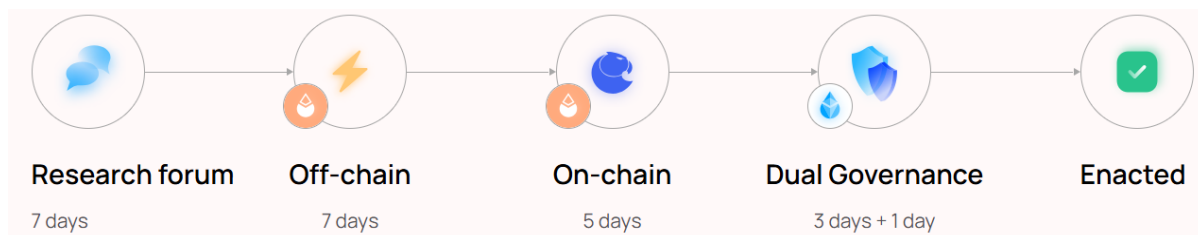


Figura 3.19: Processo di governance di Lido

⁵⁹<https://dg.lido.fi/>

⁶⁰<https://lido.fi/governance>

Delega Ai detentori di LDO è consentito assegnare il proprio potere di voto a delegati fidati per una partecipazione più coerente nella governance. Questa azione mappa l'indirizzo del detentore del token a un delegato, consentendo a quest'ultimo di votare per conto del detentore, mentre i token LDO rimangono completamente sotto il controllo del detentore per essere utilizzati in qualsiasi altro modo.

Osservazione 3.8. *Il detentore del token può annullare la decisione del delegato o revocare i diritti di delega in qualsiasi momento.*

Lido è stata costruita tramite il framework di Aragon. Di conseguenza andremo ad analizzare i contratti di **Voting** che interpreta il ruolo di governor, il contratto **DualGovernance** che interagendo con il contratto di **timelock** permette di introdurre un sistema di estensione della votazione in funzione del livello di opposizione integrando un ritardo tra approvazione ed esecuzione effettiva delle decisioni agendo dunque da timelock. Infine il contratto **Agent** che oltre ad essere l'esecutore finale in questo caso agisce anche da tesoreria della DAO.

Voting Le funzionalità del governor per la fase di votazione on-chain sono regolate dal contratto di **Voting** del framework di Aragon registrato come proxy (EIP-897 DelegateProxy) all'indirizzo:

0x2e59A20f205bB85a89C53f1936454680651E618e

Il cui contratto di implementazione ha una prima versione registrata all'indirizzo:

0x72fb5253AD16307B9E773d2A78CaC58E309d5Ba4

mentre la versione più recente ed in uso attualmente ha indirizzo:

0xf165148978Fa3cE74d76043f833463c340CFB704

La novità chiave che viene introdotta nella versione più recente del contratto è rappresentata dall'introduzione del meccanismo di delega del voto.

Nella Tabella 3.13 sono riportati i parametri chiave usati nelle votazioni on-chain.

<i>Parametro</i>	<i>Valore</i>
objectionPhaseTime	172800s = 14.400 blocchi (12s) = 2 giorni
voteTime	432000s = 36.000 blocchi (12s) = 5 giorni
supportRequiredPct	50%
minAcceptQuorumPct	5%

Tabella 3.13: Parametri proposte e votazioni on-chain di Lido DAO

Dual governance Il contratto che definisce la seconda fase della governance per le decisioni di protocollo è definito all'indirizzo:

0xC1db28B3301331277e307FDCfF8DE28242A4486E

Esso interagisce con il contratto **Timelock** che consente di eseguire automaticamente le decisioni prese dopo un ritardo prefinito. L'indirizzo corrispondente è:

0xCE0425301C85c5Ea2A0873A2dEe44d78E02D2316

Nella Tabella 3.14 sono riportati i parametri usati nel sistema di dual governance.

<i>Parametro</i>	<i>Valore</i>
afterScheduleDelay	86400s = 7.200 blocchi (12s) = 1 giorno
afterSubmitDelay	259200s = 3 giorni

Tabella 3.14: Parametri della dual governance di Lido DAO

Tesoreria - Agent Il contratto Agent è un componente fondamentale, progettato da AragonOS, per fungere da braccio operativo e tesoreria digitale di una DAO. Il contratto in questione è definito da un proxy (EIP-897 DelegateProxy) con indirizzo:

0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c

la cui implementazione è invece definita nel contratto di indirizzo:

0x3A93C17FC82CC33420d1809dDA9Fb715cc89dd37

L'aspetto più potente di tale contratto è la sua capacità di eseguire azioni esterne arbitrarie per conto della DAO.

- **Esecuzione Standard - execute:** Permette di inviare transazioni semplici.

- **Esecuzione Sicura - safeExecute:** Offre una modalità di esecuzione più cauta. Prima di eseguire un'azione, memorizza i saldi di una lista di token protetti. Dopo l'azione, verifica che i saldi di quei token non siano diminuiti.
- **Esecuzione di Script - forward:** Funge da interprete per gli Script EVM, definiti come sequenze di azioni concatenate.

Il ruolo di esecutore non è però l'unico interpretato da questo contratto, abbiamo infatti detto che esso funge anche da Vault o tesoreria multi-asset.

Il volume corrente della tesoreria in esso registrata è 136.468.142\$⁶¹.

Concludiamo l'analisi di Lido raccogliendo nella Tabella 3.15 gli indirizzi dei contratti attualmente in uso tra quelli che abbiamo analizzato.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
MiniMeToken	0x5A98FcBEA516Cf06857215779Fd812CA3beF1B32	token
AppProxyUpgradable	0x2e59A20f205bB85a89C53f1936454680651E618e	governor proxy
Voting	0xf165148978Fa3cE74d76043f833463c340CFB704	governor implem.
AppProxyUpgradeable	0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c	agent proxy
Agent	0x3A93C17FC82CC33420d1809dDA9Fb715cc89dd37	agent implem
DualGovernance	0xC1db28B3301331277e307FDCfF8DE28242A4486E	dual gov governor
EmergencyProtected Timelock	0xCE0425301C85c5Ea2A0873A2dEe44d78E02D2316	timelock

Tabella 3.15: Lista indirizzi dei contratti coinvolti nel protocollo di Lido DAO

⁶¹05.02.2026,<https://debank.com/profile/0x3e40d73eb977dc6a537af587d48316fee66e9c8c>

3.8 Ethereum Name Service

L'ENS DAO è l'organizzazione autonoma decentralizzata che governa il protocollo Ethereum Name Service (ENS). Tale protocollo rappresenta un sistema di denominazione open-source basato sulla blockchain di Ethereum⁶². Il suo scopo principale è quello di rendere l'ecosistema di Ethereum più facile da usare per le persone.



Figura 3.20: ENS DAO Logo

La ENS DAO è dotata di un'entità legale, l'ENS Foundation, un'organizzazione senza scopo di lucro che non ha azionisti e non può distribuire dividendi a direttori o membri⁶³. Il suo protocollo si fonda su una Costituzione definita dalla seguente serie di regole vincolanti che determinano quali azioni di governance sono legittime.

- La proprietà del nome non deve essere lesa.
- Le tariffe sono principalmente un meccanismo di incentivo mentre lo scopo secondario è quello di fornire entrate sufficienti per finanziare lo sviluppo e il miglioramento di ENS.
- I proventi finanziano ENS e altri beni pubblici qualora ci siano delle eccedenze.
- ENS si integra con lo spazio dei nomi globale definito dal sistema di denominazione DNS (Domain Name System) legacy, senza però sacrificare la decentralizzazione di ENS.
- Emendamenti a questa costituzione tramite voto a maggioranza dei due terzi e con quorum del 1% dei token totali.

⁶²<https://docs.ens.domains/learn/protocol>

⁶³<https://docs.ens.domains/dao/foundation>

3.8.1 Token ENS

Tutte le decisioni principali della governance della ENS DAO si basano sull'ENS Governance Token, che è stato distribuito ai proprietari ENS nel 2021⁶⁴. ENS è un token ERC-20, il cui contratto è registrato all'indirizzo:

0xC18360217D8F7Ab5e7c516566761Ea12Ce7F9D72



Figura 3.21: ENS Token

La DAO è governata attraverso un processo democratico in cui tutte le questioni principali sono decise tramite un voto aperto a tutti i detentori dei token di governance. Coloro che lo desiderano possono anche delegare il proprio potere di voto, affidando a qualcun altro il compito di seguire le ultime questioni della DAO. I delegati possono essere scelti o cambiati in qualsiasi momento, spesso senza costi, tramite Tally, Agora o altre applicazioni.

Per le questioni più quotidiane, ci sono gli **Stewards** che vengono eletti per un mandato di un anno. L'elezione avviene ogni anno il 10 dicembre e dura 5 giorni. Gli Stewards sono divisi in diversi gruppi di lavoro, ognuno dei quali riflette il proprio specifico focus: Meta-Governance, ENS Ecosystem e Public Goods⁶⁵.

Oltre agli stewards esiste anche il **Consiglio di Sicurezza** della ENS DAO è un multi-sig 4-di-8 con un mandato limitato: annullare le proposte malevole che minacciano la DAO, in particolare quelle che comprometterebbero la tesoreria⁶⁶.

⁶⁴<https://docs.ens.domains/dao/token>

⁶⁵<https://docs.ens.domains/dao/stewards>

⁶⁶<https://docs.ens.domains/dao/security-council>

Il protocollo prevede che si possano coniare tramite la funzione `mint` presente nel contratto ulteriori token a intervalli almeno di `minimumMintInterval = 31536000 s = 1 anno` tra una produzione e l'altra; la quantità massima di token che possono essere prodotti è definita da `mintCap` corrisponde al 2% annuale.

L'offerta totale di token attuale è pari a 100.000.000 ENS mentre l'offerta effettivamente circolante è 38.203.682,92 ENS⁶⁷.

3.8.2 Processo di governance e analisi dei contratti

Il processo di governance è regolato da circuiti di proposte e votazioni⁶⁸. Tali proposte possono appartenere a tre distinte categorie:

- **Proposta Eseguitibile:** Questa è una proposta relativa ad una serie di operazioni implementabili tramite smart contract che devono essere eseguite da account che la DAO controlla. Le proposte eseguibili hanno un requisito di quorum dell'1% e richiedono un'approvazione minima del 50% per passare.
- **Proposta Sociale:** Questa è una proposta che chiede l'accordo della DAO su qualcosa che non può essere fatto rispettare onchain. Le proposte sociali come quelle eseguibili hanno un requisito di quorum dell'1% e richiedono un'approvazione minima del 50% per passare.
- **Emendamento Costituzionale:** Questa è una proposta sociale che chiede alla DAO di emendare la costituzione. Le regole per emendare la costituzione sono stabilite nella costituzione stessa, e attualmente richiedono un quorum dell'1% e un'approvazione minima di due terzi per passare.

Per ognuna delle proposte il protocollo prevede l'attraversamento di tre fasi.

Fase 1: Temperature Check Lo scopo della prima fase è determinare se c'è sufficiente volontà per fare cambiamenti allo status quo. Come primo passo è quindi

⁶⁷05.06.2026, <https://coinmarketcap.com/it/currencies/ethereum-name-service/>

⁶⁸<https://docs.ens.domains/dao/proposals/submit>

richiesto di avviare una proposta off-chain sul forum⁶⁹. I temperature checks sono informali e opzionali; sta all'utente usare il feedback per decidere se vuoi procedere oltre con la tua proposta.

Fase 2: Draft Proposal Lo scopo della fase 2 è stabilire una discussione formale attorno a una potenziale proposta. Si crea dunque una nuova proposta di governance nel repository governance-docs su GitHub scegliendo l'opportuno template di partenza e si discute la proposta e sollecitando i delegati a fornire feedback su di essa. Una volta che la proposta si trova in uno stato stabile, si può procedere alla fase 3.

Fase 3: Proposta Attiva Il proponente usa GitHub per segnalare la proposta come *Pronta per la Revisione*. Un contributore a questo punto se la proposta soddisfa i requisiti programmerà la proposta per un voto su Snapshot.

A seconda della tipologia di proposta l'esito positivo della votazione produrrà risultati differenti e richiederà un numero di passaggi diversi.

- se la proposta è una Proposta Sociale o un Emendamento Costituzionale e se il voto snapshot passa, la proposta è passata e si conclude il processo.
- se la proposta è una Proposta Eseguitibile, dovrà essere inviata al contratto governor per la votazione onchain. Per avviare on chain una Proposta Eseguitibile è necessario che almeno 100k ENS siano delegati all'indirizzo del proponente o deve trovare un delegato che abbia abbastanza ENS delegati per soddisfare la soglia di proposta per proporre a proprio nome. Una volta che la votazione viene avviata ha inizio un periodo di votazione di 7 giorni. Se la proposta passa con successo, seguirà un timelock di 2 giorni prima che il codice proposto sia effettivamente eseguito.

Nella Figura 3.22 troviamo la schematizzazione della fase 3 del processo di governance appena descritta, la quale evidenzia le differenze tra le varie tipologie di proposte disponibili.

⁶⁹<https://discuss.ens.domains/>

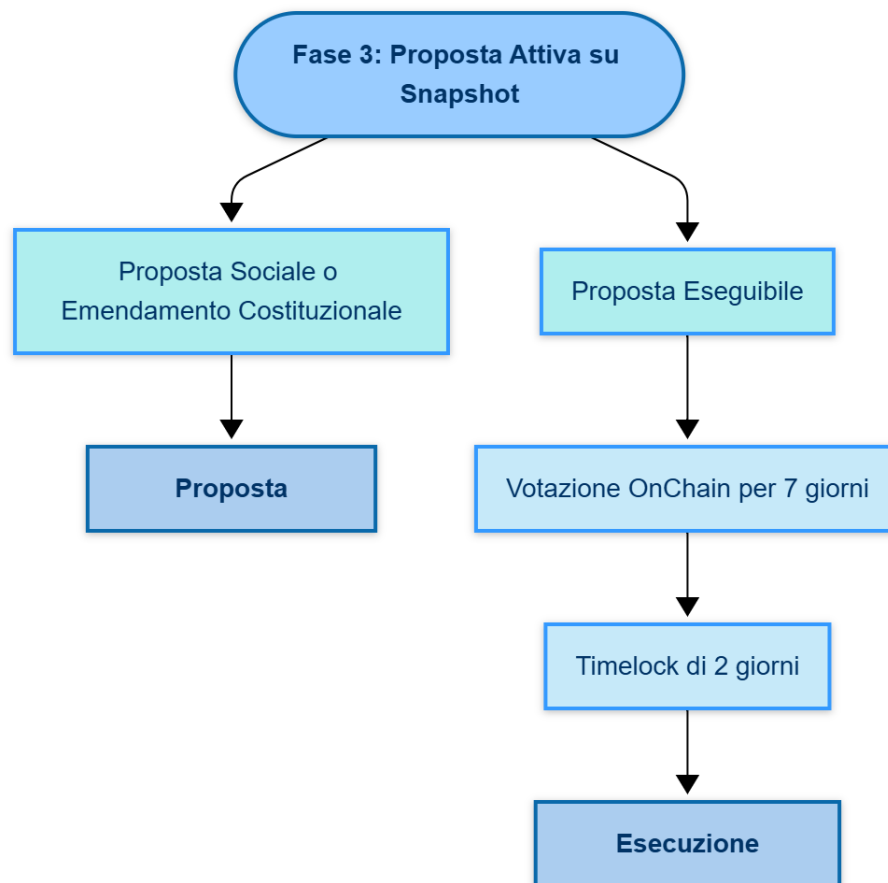


Figura 3.22: ENS - Fase 3

Governor Il contratto di Governor della ENS DAO è definito all'indirizzo:

0x323A76393544d5ecca80cd6ef2A560C6a395b7E3

L'implementazione di tale contratto ha una struttura standard basata sulle librerie in OpenZeppelin ovvero una libreria di codice Solidity open-source e ampiamente verificata, che fornisce implementazioni sicure, riutilizzabili e modulari di standard e componenti comuni per le blockchain.

Timelock Il contratto di Timelock di ENS, ovvero il responsabile dell'esecuzione automatica delle proposte che passano la fase di votazione è registrato all'indirizzo:

0xFE89cc7aBB2C4183683ab71653C4cdc9B02D44b7

Esso è definito dall'implementazione del Timelock standard di OneZeppelin.

Tesoreria La tesoreria di ENS DAO è individuata nel contratto di timelock ma non è interamente contenuta in esso. Il volume della tesoreria di ENS DAO è pari a 67.729.999,03\$⁷⁰.

Considerando dunque i dati definiti nei contratti analizzati e facendo riferimento alla documentazione ufficiale ⁷¹ possiamo raccogliere nella Tabella 3.16 una lista dei parametri che definiscono il protocollo di governance ed i valori ad essi associati.

<i>Parametro</i>	<i>Valore</i>
votingPeriod	45.818 blocchi $\approx$ 7 giorni
votingDelay	1 blocco
proposalThreshold	100.000 ENS
quorum	1% della fornitura totale = 1.000.000 ENS
minDelay	172800 s $\equiv$ 2 giorni

Tabella 3.16: Parametri di governance di ENS DAO

Concludiamo infine l'analisi di ENS DAO raccogliendo in Tabella 3.17 gli indirizzi di tutti i contratti responsabili del funzionamento del processo di governance.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
ENSToken	0xC18360217D8F7Ab5e7c516566761Ea12Ce7F9D72	token
ENSGovernor	0x323A76393544d5ecca80cd6ef2A560C6a395b7E3	governor
TimelockController	0xFE89cc7aBB2C4183683ab71653C4cdc9B02D44b7	timelock
TokenLock	0xd7A029Db2585553978190dB5E85eC724Aa4dF23f	vesting

Tabella 3.17: Lista indirizzi dei contratti di ENS DAO

⁷⁰05.02.2026, <https://www.tally.xyz/gov/ens/treasury>

⁷¹<https://www.tally.xyz/gov/ens>, <https://docs.ens.domains/dao/proposals/submit/>

3.9 DeXe

Il DeXe Protocol è un innovativo costruttore DAO open-source che presenta una libreria di oltre 50 smart contract in continuo sviluppo. La DAO del DeXe Protocol governa il Protocollo con l'obiettivo di creare e promuovere soluzioni all'avanguardia per lo sviluppo di DAO funzionali, trasparenti e decentralizzate e per la costruzione di meccanismi efficienti per la governance decentralizzata⁷².



Figura 3.23: DeXe DAO Logo

Ogni contratto del DeXe Protocol è open-source. Pertanto, sviluppatori indipendenti possono prendere qualsiasi parte del protocollo e implementarla a modo loro.

Alcuni esempi di ciò che può essere fatto con DeXe Protocol sono: creazione di DAO, creazione di utility token, invio ed esecuzione di proposte on-chain e off-chain, ecc. . .

Gli utenti della DAO DeXe Protocol e di ogni DAO che può essere costruita utilizzando tale costruttore possono essere classificati in maniere differenti⁷³.

Membro Chiunque detenga i token di governance di una DAO è un membro della stessa. I membri sono coinvolti nel voto, nelle discussioni e nella creazione di proposte; possono anche delegare i loro token ad altri membri o esperti.

Validatore I validatori sono un gruppo di utenti eletto dalla comunità che genera un secondo livello di sicurezza al di sopra e successivo al normale meccanismo di voto della DAO. In questo modo essi monitorano le attività dell'organizzazione e bloccano eventuali iniziative dannose. I validatori vengono eletti e destituiti tramite votazioni.

⁷²<https://whitepaper.dexe.network/>

⁷³<https://whitepaper.dexe.network/dexe-protocol-overview/user-roles>

Esperti Un esperto è una persona o una DAO fidata dalla comunità di un'altra DAO a cui viene concesso questo status (verificato dall'assegnazione di uno specifico NFT) attraverso un processo di proposta e votazione.

- **Esperto Locale:** È nominato all'interno di una DAO specifica e la sua autorità è limitata a quella DAO. A questi esperti possono essere delegati token dalla tesoreria della rispettiva DAO compresa la DAO del DeXe Protocol stessa.
- **Esperto Globale:** È nominato attraverso una proposta specifica nella DAO del DeXe Protocol. A questo tipo di esperto possono essere delegati token da qualsiasi DAO all'interno del Protocollo, poiché la DAO che governa il DeXe Protocol ne riconosce l'esperienza e lo status.

Lo status di esperto e i token delegati possono essere revocati tramite opportune votazioni. In tali proposte, l'esperto non può votare con i token delegati dalla DAO. Tuttavia, può comunque votare con i propri token o con quelli delegati dai saldi privati dei membri della DAO.

3.9.1 DEXE Token

Il token DEXE è il token di governance nativo per DeXe Protocol DAO⁷⁴. DEXE è un token ERC-20 con contratto registrato su Ethereum all'indirizzo:

0xde4EE8057785A7e8e800Db58F9784845A5C2Cbd6



Figura 3.24: DeXe Token

DEXE può essere utilizzato per gestire vari aspetti dell'organizzazione tra cui:

⁷⁴<https://whitepaper.dexe.network/dexe-protocol-dao/token-and-treasury>

- *Governance*: I detentori di DEXE gestiscono il DeXe rotocol, attraverso sequenze di proposte e votazioni.
- *Ricompense*: I contributori attivi della DAO riceveranno ricompense dalla Tesoreria per la loro partecipazione.
- *Grant/Sovvenzioni*: La Tesoreria, in base al consenso della comunità, può essere utilizzata per finanziare ricerca e sviluppo del protocollo o di altri progetti in ambito blockchain, ma anche per organizzare eventi e conferenze che diffondano informazioni del mondo blockchain o più nello specifico che promuovano la DAO DeXe Protocol.

La DAO consente anche di delegare DEXE continuando a mantenerne la proprietà. Nel momento in cui si delegano dei token essi vengono bloccati nello smart contract di delega fino a quando non li richiami.

L'offerta totale al momento è di 96.504.599,33 DEXE mentre l'offerta effettivamente circolante è 83.733.681,65 DEXE⁷⁵.

3.9.2 Processo di governance e meccanismo di voto

Il processo di governance di DeXe Protocol DAO prevede che qualunque decisione deve passare attraverso il "Circuito delle Proposte" articolato come segue⁷⁶:

Iniziazione Qualsiasi membro della DAO può presentare una proposta se dispone di un numero sufficiente di token di governance nel suo wallet.

Votazione Dopo la pubblicazione della proposta, i membri della DAO possono votarla. I membri devono votare una proposta prima di accedere ai risultati di votazione attuali per prevenire la preferenza nel processo decisionale. Affinché una proposta sia considerata approvata devono essere soddisfatte le seguenti condizioni:

⁷⁵05.02.2026,<https://coinmarketcap.com/it/currencies/dexe/>

⁷⁶<https://whitepaper.dexe.network/proposal-circuit>

- Deve essere raggiunto un quorum minimo.
- La maggioranza dei voti deve essere a favore.

Votazione dei validatori A seguito del primo round di votazione ne segue un secondo round in cui votano solo i validatori in carica.

Esecuzione Una volta terminate la fase di votazione principale e la votazione dei Validatori, e soddisfatte le condizioni per l'approvazione, la proposta può essere eseguita tramite il relativo contratto esecutore.

La DeXe Protocol DAO prevede un meccanismo di voto non lineare anche detto voto ponderato⁷⁷. Questo modello contiene una combinazione di misure che contrastano la concentrazione di potere in una singola parte, considerando l'esperienza nel conteggio dei voti e incoraggiando il coinvolgimento attivo tramite incentivi.

Al centro di questo sistema ci sono funzioni definite a tratti (piecewise-defined functions) che permettono un controllo preciso sul potere di voto, minimizzando il rischio di manipolazione. Per costruire queste dipendenze non lineari, il protocollo impiega due funzioni polinomiali a tratti di quarto e terzo grado⁷⁸.

La funzione per i membri ordinari della DAO è una dipendenza definita a tratti e composta da due intervalli: entro il 7% della fornitura totale (TS) di token viene utilizzata una funzione lineare standard, dove il potere di voto è uguale al numero di token, oltre il 7% viene utilizzato un polinomio di terzo grado che rallenta gradualmente la crescita del potere di voto.

$$V_m(x) = \begin{cases} x & \text{per } x < 7\% \text{ di } TS \\ k_m \left(7 \cdot TS \cdot \frac{1}{100} + a \left(\frac{100x}{TS} - 7 \right) + \right. \\ \quad \left. + b \left(\frac{100x}{TS} - 7 \right)^2 + c \left(\frac{100x}{TS} - 7 \right)^3 \right) \frac{TS}{100} & \text{altrimenti} \end{cases}$$

⁷⁷<https://whitepaper.dexe.network/voting-logic/voting-models>

⁷⁸<https://whitepaper.dexe.network/meritocratic-governance/mathematical-logic>

Dove: V_m = potere di voto, x = bilancio di token di un votante, k_m = fattore di pendenza settato di default $k_m = 0.97$ e $a = 1.041$, $b = -0.007211$ e $c = 0.00001994$.

Per quanto riguarda la funzione per gli esperti prevede che per ciascun esperto, venga definito uno specifico coefficiente di pendenza, k che dipende dalla provenienza dei token delegati. Se tutti i token sono delegati dalla Tesoreria della DAO, il coefficiente $k = k_{max} = 1.08$ (il valore massimo, k_{max}) mentre se tutti i token sono delegati da membri regolari o sono di proprietà dell'esperto, $k = k_{min} = 0.92$. Nei casi in cui un esperto abbia token delegati sia dalla Tesoreria che dai membri regolari, il coefficiente k viene calcolato in base al coefficiente R ($R = 1$ quando il 100% dei token proviene dalla Tesoreria e $R = 0$ quando il 100% proviene dai membri) come:

$$k = k_{min} \cdot R + k_{max} \cdot (1 - R)$$

La funzione per gli esperti è un polinomio di quarto grado definito a tratti:

$$V_{exp}(x) = \begin{cases} k \left(f \left(\frac{100x}{TS} \right)^4 + g \left(\frac{100x}{TS} \right)^3 + h \left(\frac{100x}{TS} \right)^2 + i \left(\frac{100x}{TS} \right) \right) \frac{TS}{100} & \text{per } x < 6.63\% \text{ di } TS \\ k \left(a + b \left(\frac{100x}{TS} - 6.63 \right) + c \left(\frac{100x}{TS} - 6.63 \right)^2 + \right. \\ \quad \left. + d \left(\frac{100x}{TS} - 6.63 \right)^3 + e \left(\frac{100x}{TS} - 6.63 \right)^4 \right) \frac{TS}{100} & \text{altrimenti} \end{cases}$$

Dove: $a = 8.83755895036092$, $b = 1.130$, $c = -0.006086$, $d = 0.00004147$, $e = -0.000000148$, $f = -0.001328$, $g = 0.023761$, $h = -0.169889$ e $i = 1.801894$.

3.9.3 Analisi dei contratti di governance

Governor Il corpo principale del protocollo di governance è gestito dal contratto di governor definito come proxy (EIP-1967 Beacon Proxy) con indirizzo:

0xB562127efDC97B417B3116efF2C23A29857C0F0B

con implementazione **GovPool** è registrata all'indirizzo:

0x1fb8cEC3A37B89E68d49e6CcB5927f0ecAA59673

Tale contratto non segue un modello standard come quello di Compound o quello costruito classico sulla base delle librerie OneZeppelin. Dexe ha costruito uno standard proprio, integrando alcune meccaniche molto avanzate pur mantenendo compatibilità con i pilastri del settore. Per integrare tale contratto viene inoltre definito il proxy (EIP-1967 Beacon Proxy) di indirizzo:

0x57CbF649aC9b87FF8d0c710842bc26b5d05be566

la cui implementazione **GovSettings** è definita all'indirizzo:

0xaD8c754B5a2115D7d159307032c8514Df48aaA0b

ed ha un unico scopo fondamentale: memorizzare e definire parametri e regole chiave per regolare il processo di governance.

Timelock Il contratto proxy (EIP-1967 Beacon Proxy):

0x6e290f6ae029006ABD5CEe8dAb7C4a552803E115

la cui implementazione **GovValidators** è definita all'indirizzo:

0x1c5575fc70d8c76bcce30a446fcc3c30ff5a6c9e

E' il contratto che regola le proposte interne dei validatori e che consente l'esecuzione delle proposte assumendo anche il ruolo di contratto di timelock del sistema.

Tesoreria La tesoreria della DAO è gestita tramite il contratto di governor stesso. Il volume in esso detenuto è pari a 107.437.788\$⁷⁹.

Un altro contratto di rilievo per la detenzione di fondi è il proxy:

0xbE8cB128fBCf13f7F7A362c3820f376b0971B7B2

a cui corrisponde l'implementazione definita in:

0x9e8885e5Fb417908E15757DB65Bd725E5d70C844

Questo contratto è in particolare responsabile della conservazione sicura dei fondi degli utenti utilizzati durante le votazioni.

⁷⁹05.02.2026,<https://debank.com/profile/0xb562127efdc97b417b3116eff2c23a29857c0f0b>

I parametri principali che possono essere estratti da tali contratto che usati nel processo di governance e di votazione ⁸⁰ sono quelli mostrati in Tabella 3.18.

<i>Parametro</i>	<i>Valore</i>
duration	432000 s = 36.000 blocchi (12s) = 5 giorni
durationValidators	432000 s = 36.000 blocchi (12s) = 5 giorni
executionDelay	1800 s = 30 min
quorum	51% della fornitura totale
quorumValidators	51% della fornitura dei validatori
minVotesForVoting	13 Votes
minVotesForCreating	10,000 Votes

Tabella 3.18: Parametri proposte di DeXe DAO

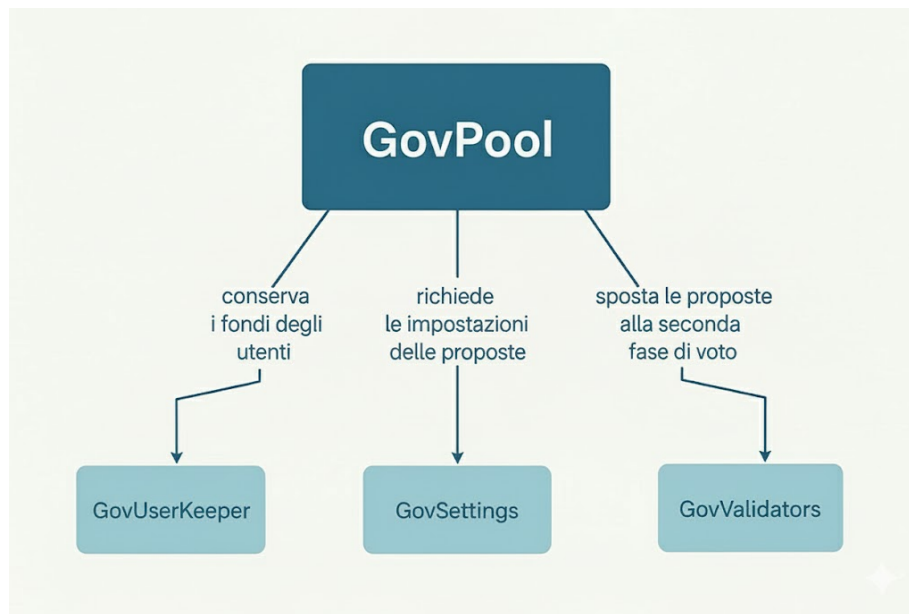


Figura 3.25: DeXe: Interazione tra i contratti di governance

Infine raccogliamo nella Tabella 3.19 gli indirizzi di governance della DAO.

⁸⁰<https://app.dexe.io/dao/0xb562127efdc97b417b3116eff2c23a29857c0f0b/voting-rules>

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
Dexe	0xde4EE8057785A7e8e800Db58F9784845A5C2Cbd6	token
ProtectedPublic BeaconProxy	0xB562127efDC97B417B3116efF2C23A29857C0F0B	governor proxy
GovPool	0x1fb8cEC3A37B89E68d49e6CcB5927f0ecAA59673	governor implement.
ProtectedPublic BeaconProxy	0x6e290f6ae029006ABD5CEe8dAb7C4a552803E115	validators proxy
GovValidators	0x1c5575fc70d8C76BcCE30A446fcC3c30Ff5A6c9e	validators implement.
ProtectedPublic BeaconProxy	0xbE8cB128fBCf13f7F7A362c3820f376b0971B7B2	treasury proxy
GovUserKeeper	0x9e8885e5Fb417908E15757DB65Bd725E5d70C844	treasury implement.
ProtectedPublic BeaconProxy	0x57CbF649aC9b87FF8d0c710842bc26b5d05be566	gov. setting proxy
GovSettings	0xaD8c754B5a2115D7d159307032c8514Df48aaA0b	gov. setting implement.

Tabella 3.19: Lista indirizzi dei contratti di DeXe DAO

3.10 Compound

Compound è un protocollo costruito sulla blockchain di Ethereum che stabilisce mercati monetari, ovvero pool di asset con tassi di interesse derivati algoritmicamente, basati sull'offerta e sulla domanda dell'asset. I fornitori (e i mutuatori) di un asset interagiscono direttamente con il protocollo, guadagnando (o pagando) un tasso di interesse variabile, senza dover negoziare termini come la scadenza, il tasso di interesse o la garanzia con un pari o una controparte [33].



Figura 3.26: Compound Logo

Modello dei tassi di interesse Gli utenti con un saldo positivo dell'asset di base guadagnano interessi, denominati nell'asset di base, in base al **supply rate model** mentre gli utenti con un saldo negativo pagano interessi in base a un **borrow rate model**. Questi modelli di tasso di interesse sono separati e vengono impostati dalla governance. I tassi di interesse di offerta e di prestito sono una funzione dell'**utilization rate** dell'asset di base. Ciascun modello include un "punto di flesso" (o kink): al di sopra di questo punto, il tasso di interesse aumenta più rapidamente. Gli interessi maturano ad ogni secondo utilizzando il timestamp del blocco.

Supply Rate Model: Restituisce il tasso di offerta al secondo come rappresentazione decimale di una percentuale scalata per 10^{18} .

- Se l'Utilizzo è inferiore o uguale al parametro Kink: $\mathbf{TO} = \mathbf{TB}_O + \mathbf{TPB}_O \times \mathbf{U}$
- Altrimenti: $\mathbf{TO} = \mathbf{TB}_O + \mathbf{TPB}_O \times \mathbf{K}_O + \mathbf{TPA}_O \times (\mathbf{U} - \mathbf{K}_O)$

Dove: $\mathbf{U} = \text{Tasso di Utilizzo} = \frac{\text{Prestiti Totali}}{\text{Offerta Totale}}$, $\mathbf{TO} = \text{Tasso di Offerta}$, $\mathbf{TB}_O = \text{Tasso Base Offerta}$, $\mathbf{TPB}_O = \text{Tasso Pendenza Bassa Offerta}$, $\mathbf{TPA}_O = \text{Tasso Pendenza Alta Offerta}$, $\mathbf{K}_O = \text{Kink Offerta}$.

Per calcolare **Tasso Percentuale Annuo Di Offerta** di Compound III in percentuale, si deve passare l'utilizzo corrente a questa funzione, dividere il risultato per 10^{18} e moltiplicare per il numero di secondi in un anno e scalare per 100.

Borrow Rate Model: Restituisce il tasso di prestito al secondo come rappresentazione decimale di una percentuale scalata per 10^{18} .

- Se l'Utilizzo è inferiore o uguale al parametro Kink: $\mathbf{TP} = \mathbf{TB}_P + \mathbf{TPB}_P \times \mathbf{U}$
- Altrimenti: $\mathbf{TP} = \mathbf{TB}_P + \mathbf{TPB}_P \times \mathbf{K}_P + \mathbf{TPA}_P \times (\mathbf{U} - \mathbf{K}_P)$

Con: $\mathbf{U} = \text{Tasso di Utilizzo}$, $\mathbf{TO} = \text{Tasso di Prestito}$, $\mathbf{K}_P = \text{Kink Prestito}$, $\mathbf{TB}_P = \text{Tasso Base Prestito}$, $\mathbf{TPB}_P = \text{Tasso Pendenza Bassa Prestito}$, $\mathbf{TPA}_P = \text{Tasso Pendenza Alta Prestito}$.

Per calcolare il **Tasso Percentuale Annuo Di Prestito** di Compound III in percentuale, si deve passare l'utilizzo corrente a questa funzione, dividere il risultato per 10^{18} e moltiplicare per il numero di secondi in un anno e scalare per 100.

3.10.1 Token COMP

COMP è un token ERC-20 che consente al proprietario di delegare i diritti di voto a qualsiasi indirizzo, incluso il proprio. Il suo indirizzo Ethereum è il seguente.

0xc00e94Cb662C3520282E6f5717214004A7f26888



Figura 3.27: COMP Token

Gli utenti possono delegare a un solo indirizzo alla volta, e il numero di voti aggiunti al conteggio dei voti del delegato è equivalente al saldo di COMP nel conto dell'utente. Le modifiche al saldo del token del proprietario adeguano automaticamente i diritti di voto del delegato. I voti sono delegati a partire dal blocco corrente e in avanti, fino a quando il mittente non delega nuovamente o non trasferisce i propri COMP.

Il protocollo di Compound non prevede un hard cap. L'offerta totale è di 10.000.000 COMP di cui 9.964.791,94 COMP sono attualmente in circolazione⁸¹.

3.10.2 Processo di governance e analisi dei contratti

Il protocollo Compound è governato e aggiornato dai possessori del token COMP, utilizzando tre componenti distinti: il token COMP, il contratto di governor ed il timelock. Insieme, questi smart contract consentono alla comunità di proporre, votare

⁸¹05.02.2026,<https://coinmarketcap.com/currencies/compound/>

e implementare cambiamenti. Le proposte di governance che regolano il protocollo possono: modificare i parametri di sistema, supportare nuovi mercati o aggiungere funzionalità interamente nuove al protocollo⁸².

Per poter creare una proposta esistono due strategie differenti:

- Se l'indirizzo del proponente dispone di almeno 25.000 COMP delegati può creare direttamente una **proposta di governance**.
- Se l'indirizzo del proponente non dispone di sufficienti token per creare direttamente una proposta di governance ma è in grado di bloccare 100 COMP può creare una **proposta autonoma** che diventerà una proposta di governance solo dopo aver ricevuto la delega di 25.000 COMP.

Dopo che una proposta di governance è stata creata, essa entra in un periodo di revisione di 2 giorni, dopodiché i pesi di voto vengono registrati e inizia la votazione. La votazione dura 3 giorni; se viene raggiunta la maggioranza (più del 50% a favore) e vengono espressi almeno 400.000 voti a favore della proposta, questa viene messa in coda nel timelock e può essere implementata automaticamente dopo un ritardo di 2 giorni. Qualsiasi modifica al protocollo richiede quindi almeno una settimana.

Governor Il contratto di governor di compound ha attraversato diverse variazioni nel corso del tempo. La prima versione del contratto di governor è un proxy (EIP-897 DelegateProxy) con indirizzo:

0xc0Da02939E1441F497fd74F78cE7Decb17B66529

che inizialmente puntava all'indirizzo di implementazione:

0xF3B6E9e13706A8F01fe98fdCf66335dc5CfdEED

la quale è stata poi sostituita dalla nuova implementazione:

0x6F6e4785c97885d26466945055d4Ae8931bE6f7a

⁸²<https://docs.compound.finance/governance/>, <https://docs.compound.finance/v2/governance/>

Attualmente la versione del contratto⁸³ di governor di riferimento è un proxy (EIP-1967 Transparent Proxy) registrato all'indirizzo:

0x309a862bbC1A00e45506cB8A802D1ff10004c8C0

la cui implementazione **GovernorCompound** invece ha indirizzo:

0x501Eb63A2120418C581B3bD31CF190b0a0616752

Con questa innovazione viene abbandonata la logica del **GovernorBravoDelegate** per adottare il modello modulare degli Standard OpenZeppelin di Governor. Tale contratto rappresenta un completo cambio di architettura e paradigma offrendo una maggiore modularità, sicurezza e introducendo funzionalità avanzate come il quorum flessibile e la prevenzione del quorum tardivo.

Timelock Il contratto di timelock è registrato all'indirizzo:

0x6d903f6003cca6255D85CcA4D3B5E5146dC33925

Esso implementa un solido meccanismo di sicurezza con cui le modifiche sono soggette a un ritardo forzato prima dell'esecuzione.

I parametri chiave coinvolti nell'attuale processo di governance definiti nei contratti **CompoundGovernor** e **Timelock** sono raccolti nella Tabella 3.20.

<i>Parametro</i>	<i>Valore</i>
proposalThreshold	25.000 COMP
lateQuorumVoteExtension	14400 $\equiv$ 2 giorni (blocchi da 12s)
votingDelay	13140 blocchi $\simeq$ 2 giorni (= 1,825 giorni)
votingPeriod	19710 blocchi $\simeq$ 3 giorni (= 2,737 giorni)
MAXIMUM_DELAY	2592000s = 30 giorni
MINIMUM_DELAY	172800s = 2 giorni
delay	172800s = 2 giorni
GRACE_PERIOD	1209600s = 14 giorni

Tabella 3.20: Attuali parametri di governance di Compound

⁸³<https://www.comp.xyz/t/governance-contracts-upgrade-and-proposal-moratorium-period/6220>

Tesoreria La tesoreria di Compound è gestita da vari contratti sulle diverse reti su cui è distribuito il protocollo. Il volume complessivo è pari a 104,072,902\$⁸⁴. Sulla mainnet di Ethereum in particolare il contratto di tesoreria principale è rappresentato dal contratto di timelock.

Concludiamo la nostra analisi raccogliendo nella tabella Tabella 3.21 tutti i contratti che gestiscono il protocollo di Compound.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
Comp	0xc00e94Cb662C3520282E6f5717214004A7f26888	token
Transparent UpgradeableProxy	0x309a862bbC1A00e45506cB8A802D1ff10004c8C0	governor proxy
CompoundGovernor	0x501Eb63A2120418C581B3bD31CF190b0a0616752	governor implem
Timelock	0x6d903f6003cca6255D85CcA4D3B5E5146dC33925	timelock

Tabella 3.21: Lista indirizzi dei contratti di Compound

3.11 Maple Finance

Maple finance fu fondata nel 2019 e guidata da un team di ex banchieri e professionisti degli investimenti creditizi che mirano a migliorare i mercati dei capitali tradizionali. Essa è una piattaforma di prestito di asset digitali leader, che ne potenzia l'economia con soluzioni di prestito sicure e innovative⁸⁵.



Figura 3.28: Maple Finance Logo

Il rendimento di Maple è generato da prestiti a tasso fisso e sovracollateralizzati a

⁸⁴05.02.2026,<https://www.tally.xyz/gov/compound/treasury>

⁸⁵<https://docs.maple.finance/>

mutuatari istituzionali. Per i Mutuatari, Maple offre un finanziamento trasparente ed efficiente, eseguito interamente on-chain⁸⁶.

- Le istituzioni possono prendere in prestito garantendo con collaterale, secondo termini definiti on-chain.
- I mutuatari accedono a pool di capitale gestiti da smart contract e collaborano con i Pool Delegate per completare in modo confidenziale le valutazioni dei prestiti.

Per i Liquidity Providers, Maple offre una fonte di rendimento sostenibile attraverso pool di prestito gestiti professionalmente.

- Esposizione diversificata su mutuatari di alto livello.
- Soluzione "imposta e dimentica" con la dovuta diligenza affidata in outsourcing ai Pool Delegate.
- Gli interessi maturano e vengono reinvestiti per consentire al capitale di crescere nel tempo.

Questa strategia ha una comprovata esperienza di sovraperformance del rendimento rispetto ai principali protocolli di prestito DeFi.

3.11.1 Token SYRUP

Al centro di Maple si trova il token SYRUP, che allinea gli stakeholder, guida la governance e incentiva la partecipazione⁸⁷. SYRUP è il token di governance dell'ecosistema Maple e alimenta due linee di prodotto complementari ma distinte:

- **Maple Permissioned** (Istituzionale): Collega il capitale istituzionale a opportunità di prestito di asset digitali di alta qualità.
- **Maple Open Access**: Un protocollo DeFi permissionless che democratizza l'accesso a rendimenti di livello istituzionale.

⁸⁶<https://docs.maple.finance/technical-resources/protocol-overview/background>

⁸⁷<https://docs.maple.finance/maple-for-token-holders/mpl-token>

Mettendo in staking SYRUP, i partecipanti possono contribuire attivamente al processo decisionale attraverso la governance, guadagnando al contempo ricompense, creando una comunità dinamica e coinvolta. Questo circolo virtuoso di crescita rafforza l'allineamento, accelera il progresso e aumenta l'influenza di Maple.

SYRUP è un token ERC-20 il cui proxy (EIP-1967 Transparent Proxy) è registrato su Ethereum all'indirizzo:

`0x643C4E15d7d62Ad0aBeC4a9BD4b001aA3Ef52d66`

mentre la corrispondente implementazione ha indirizzo:

`0x6eD767EBCfF51533E5181f7bf818F2b9bD767aec`



Figura 3.29: SYRUP Token

In passato Maple Finance era gestita da un token di governance differente chiamato MPL che era a sua volta un token ERC-20. Il suo contratto è registrato all'indirizzo:

`0x33349b282065b0284d756f0577fb39c158f935e6`

ma ad oggi è stato integralmente sostituito dal nuovo token SYRUP.

Il rapporto di conversione stabilito prevede che 1 MPL venga convertito in 100 SYRUP⁸⁸. La coniazione iniziale di SYRUP è così ripartita:

- 1.000.000.000 SYRUP: L'offerta convertita.
- 100.000.000 SYRUP: 10% iniziale previsto dal programma di inflazione.
- 54.930.000 SYRUP: L'equivalente dell'inflazione prevista fino a 1° ottobre 2024.

⁸⁸<https://docs.maple.finance/maple-for-token-holders/syrup-tokenomics>

In linea con il programma di inflazione dei token e l'emissione concordati, l'offerta prevista di token sarà di 1.267.875.000 SYRUP entro settembre 2026. Oggi l'offerta totale è di 1.216.127.147,99 SYRUP di cui 1.157.145.692,53 SYRUP circolanti⁸⁹.

3.11.2 Processo di governance e analisi dei contratti

Con l'approvazione della proposta MIP-019, sia SYRUP che stSYRUP sono idonei alla partecipazione al voto⁹⁰. Il contratto del token di staking stSYRUP ha indirizzo:

0xc7E8b36E0766D9B04c93De68A9D47dD11f260B45



Figura 3.30: stSYRUP Token

Le votazioni di governance includono decisioni sulla distribuzione dei token, la ricapitalizzazione del Tesoro di Maple, il lancio di nuovi prodotti e l'aggiornamento dell'infrastruttura degli smart contracts.

Il voto viene condotto collegando a Snapshot⁹¹ un wallet con un saldo sufficiente di SYRUP o stSYRUP. Le proposte di governance hanno una finestra di votazione di 4-7 giorni, durante la quale i wallet partecipanti possono votare una proposta. Una volta raggiunto il quorum del 5% dell'offerta totale e trascorsa la finestra di votazione, il voto è approvato. Se non viene raggiunto un quorum, o se ci sono più voti contro la proposta che a favore, il voto viene respinto.

Dopodichè le votazioni approvate attraverseranno un periodo di ritardo programma-

⁸⁹05.02.2026,<https://coinmarketcap.com/it/currencies/maple-finance/>

⁹⁰<https://docs.maple.finance/maple-for-token-holders/governance-and-voting>

⁹¹<https://snapshot.box/#/s:maple.eth>

to di 3 giorni implementato tramite il timelock prima di essere eseguite. Dopodichè l'esecuzione deve avvenire entro i 2 giorni successivi.

Governor Nel caso di Maple Finance non esiste un contratto di governor poichè il processo di governance come abbiamo visto non prevede una fase di votazioni on-chain. Una volta che una proposta supera il voto durante la governance off-chain è considerata approvata e dunque passa direttamente alla fase di esecuzione.

Timelock Il contratto che regola l'esecuzione ed il ritardo di esecuzione ad essa associato è definito all'indirizzo ethereum:

0x2eFFf88747EB5a3FF00d4d8d0f0800E306C0426b

Tale contratto non eredita direttamente dalle librerie di OpenZeppelin, ma ne ricalca la logica di Timelock.

Nella Tabella 3.22 riportiamo i principali parametri di governance che vengono definiti all'interno del contratto.

<i>Parametro</i>	<i>Valore</i>
delay (Standard)	259200s = 3 giorni
executionWindow (Standard)	172800s = 2 giorni
MIN_DELAY	86400s = 1 giorno
MIN_EXECUTION_WINDOW	86400s = 1 giorno

Tabella 3.22: Parametri di governance di Maple Finance

Tesoreria Il cuore della tesoreria della DAO di Maple Finance è rappresentato dal contratto proxy:

0xd6d4Bcde6c816F17889f1Dd3000aF0261B03a196

che punta al contratto di implementazione **GnosisSafe** registrato all'indirizzo:

0xd9Db270c1B5E3Bd161E8c8503c55cEABeE709552

Esso rappresenta lo standard di fatto e l'infrastruttura più utilizzata per la gestione della tesoreria delle DAO e dei grandi team in Web3.

Tale contratto non è però l'unico componente della tesoreria di Maple Finance. L'altro contratto che contribuisce alla tesoreria ha indirizzo:

0xa9466EaBd096449d650D5AEB0dD3dA6F52FD0B19

Il volume complessivo attuale di Maple Finance è pari a 10.431.558\$⁹².

Concludiamo dunque l'analisi di Maple Finance raccogliendo gli indirizzi dei contratti chiave per il processo di governance nella Tabella 3.23.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
MapleTokenProxy	0x643C4E15d7d62Ad0aBeC4a9BD4b001aA3Ef52d66	token proxy
MapleToken	0x6eD767EBCfF51533E5181f7bf818F2b9bD767aec	token implem
xMPL	0xc7E8b36E0766D9B04c93De68A9D47dD11f260B45	staked token
Proxy	0xd6d4Bcde6c816F17889f1Dd3000aF0261B03a196	DAO Multisig proxy
GnosisSafe	0xd9Db270c1B5E3Bd161E8c8503c55cEABeE709552	DAO Multisig implem
GovernorTimelock	0x2eFFf88747EB5a3FF00d4d8d0f0800E306C0426b	timelock
MapleTreasury	0xa9466EaBd096449d650D5AEB0dD3dA6F52FD0B19	treasury

Tabella 3.23: Lista indirizzi dei contratti in uso di Maple Finance

3.12 Wormhole

Wormhole è un protocollo di messaggistica cross-chain che connette applicazioni decentralizzate su più blockchain. Offre una suite di strumenti di interoperabilità, ognuno dei quali affronta diverse sfide multichain, e consente agli sviluppatori di

⁹²05.02.2026,<https://debank.com/profile/0xd6d4bcde6c816f17889f1dd3000af0261b03a196,0xa9466eabd096449d650d5aeb0dd3da6f52fd0b19>

combinare questi prodotti a seconda delle necessità⁹³.



Figura 3.31: Wormhole Logo

L'architettura di Wormhole è divisa in due componenti principali, una on-chain ed una off-chain. Le componenti on-chain sono rappresentate dagli smart contract, ognuno dei quali è implementato su ogni singola blockchain supportata da Wormhole. Le componenti off-chain invece sono le seguenti e fundono da "ponte" decentralizzato di validatori tra le catene.

- **Guardian Network:** È una rete decentralizzata di validatori che monitorano continuamente tutti i Core Contract su tutte le catene supportate. Per convalidare un messaggio, è necessaria una maggioranza qualificata dei Guardiani (tipicamente 13 su 19).
- **VAA (Verifiable Action Approval):** Dopo che la maggioranza dei Guardiani ha convalidato un messaggio, firmano un documento chiamato VAA che rappresenta la prova crittografica che l'evento/il messaggio è realmente accaduto sulla catena di origine ed è stato attestato dalla rete Wormhole.
- **Relayer:** Sono entità off-chain (chiunque può essere un relayer) che prendono il VAA firmato dai Guardiani e lo inviano alla Core Contract sulla blockchain di destinazione.

3.12.1 Token W

Il token di governance di Wormhole è un token ERC-20 inizialmente distribuito su Solana e successivamente su molte altre blockchain vista la natura multi-chain del

⁹³<https://wormhole.com/docs/protocol/introduction/>, <https://wormhole.com/docs/protocol/ecosystem/>

suo protocollo. Su ethereum il contratto è definito come proxy all'indirizzo:

0xB0fFa8000886e57F86dd5264b9582b2Ad87b2b91

e la cui implementazione ha indirizzo:

0x344518934533ec82b49eA533b196dce5cfA64411



Figura 3.32: W Token

Tra le principali funzionalità del token W abbiamo⁹⁴:

- lo staking per partecipare alla governance e, nel tempo, supportare la sicurezza del protocollo o i meccanismi economici;
- guadagnare una quota delle entrate del protocollo.

L'hard cap previsto per il protocollo di Decred è pari a 10.000.000.000 W che coincide con l'offerta totale. L'offerta circolante iniziale è stata di 1.800.000.000 W ad oggi è invece 5.329.786.197 W⁹⁵.

3.12.2 Processo di governance e analisi dei contratti

La governance di Wormhole definita come **MultiGov** è un sistema di governance multichain che consente un processo decisionale decentralizzato su più blockchain. Costruito sulla messaggistica Wormhole, permette alle DAO di gestire proposte, voti ed esecuzione da qualsiasi catena connessa, aggregando il potere di voto attraverso le catene e coordinando l'esecuzione sicura delle proposte⁹⁶.

⁹⁴<https://messari.io/report/understanding-wormhole-a-comprehensive-overview>

⁹⁵05.02.2026,<https://coinmarketcap.com/it/currencies/wormhole/>

⁹⁶<https://wormhole.com/docs/products/multigov/overview/>

I passi che una proposta segue durante il proprio ciclo sono i seguenti⁹⁷.

- **Creazione della proposta (Hub):** Il proponente, in genere un membro della DAO o uno smart contract, crea una proposta e la invia al contratto HubGovernor sulla catena hub. Questa proposta include i target, i calldata, i metadati, i payload e la tempistica di voto della proposta. Una volta inviata, diventa immutabile e viene trasmessa a tutte le catene spoke supportate.
- **Inizio del periodo di voto:** Quando la proposta è attiva, sia l'HubGovernor che ogni SpokeGovernor entrano in uno stato di voto. Su ogni catena, i partecipanti alla governance possono esaminare la proposta e prepararsi a esprimere i voti utilizzando il loro potere di voto locale.
- **Gli utenti votano sulle spoke:** I singoli votanti interagiscono con il loro modulo di voto spoke locale per esprimere un voto. I voti vengono convalidati e registrati sulla catena spoke e preparati come aggregato a livello spoke.
- **Voti trasferiti all'hub:** Le spoke inviano i loro aggregati all'hub utilizzando Wormhole. L'hub verifica ogni aggregato prima di includerlo nel conteggio.
- **Fine del periodo di voto:** Dopo la scadenza del periodo di voto, il contratto HubGovernor smette di accettare nuovi voti. Tutti i conteggi finali sono congelati fino alla finalizzazione del risultato.
- **Conteggio finale e proposta messa in coda:** L'HubGovernor valuta il totale dei voti, verifica le soglie di quorum e determina se la proposta è stata approvata o respinta. Se ha successo, contrassegna la proposta come pronta per l'esecuzione. Le proposte fallite vengono semplicemente archiviate.
- **Proposta eseguita:** L'HubGovernor esegue la proposta. Se il payload dell'azione è sulla catena hub, viene eseguito direttamente, altrimenti i messaggi vengono composti e inviati tramite Wormhole Messaging e consegnati da un relayer al contratto esecutore della catena spoke di destinazione.

⁹⁷<https://wormhole.com/docs/products/multigov/concepts/proposal-flow/>

Il flusso delle proposte appena descritto è rappresentato nella Figura 3.33.

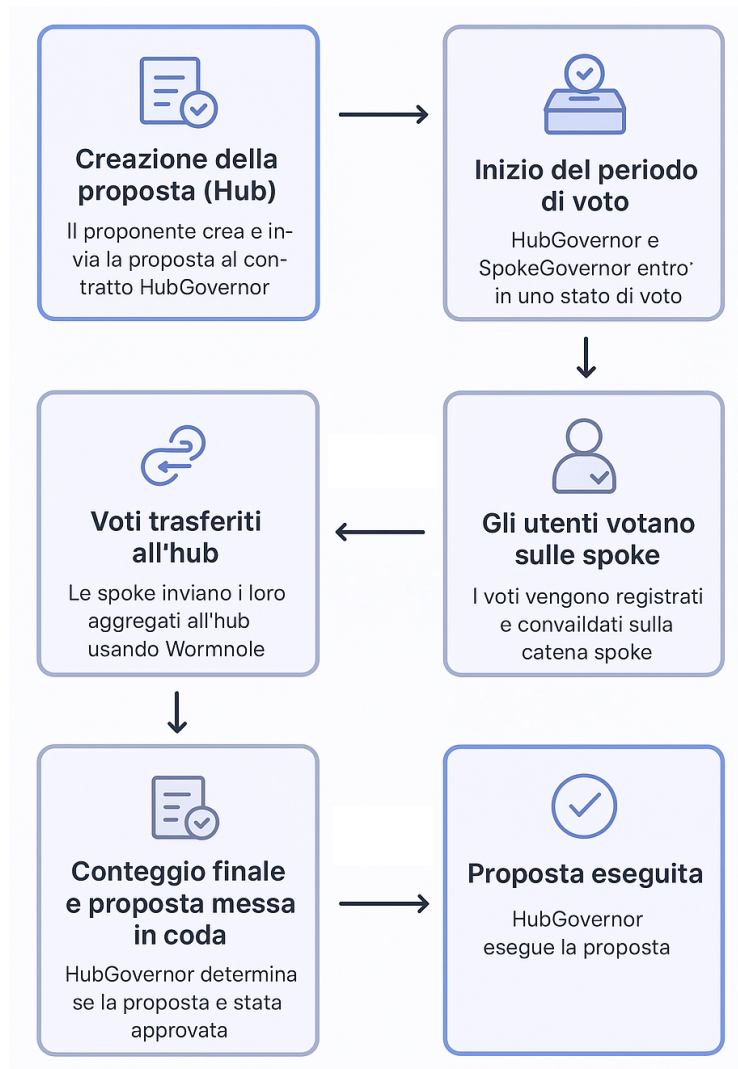


Figura 3.33: Processo di governance di Wormhole

Governor Il contratto che stiamo per analizzare implementa un sistema di governance decentralizzata, specificamente progettato per supportare meccanismi di governance multi-chain. Tale contratto è registrato all'indirizzo:

0x239B1F17E6Efa75662cB87781025538babF1Cf6b

Il contratto di governor di Wormhole estende molte funzionalità standard dalle librerie OpenZeppelin per aggiungere logiche specifiche per la gestione dei voti distribuiti.

Timelock Il contratto di timelock usato da Wormhole è definito all'indirizzo:

0xfBc580c0289121673EfB7375fF111bD2A4db4654

Esso è definito secondo lo standard di OneZeppelin senza modifiche di rilievo.

Tesoreria Nonostante il processo di governance on-chain sia gestito tramite Tally non è stato possibile reperire i dati relativi alla tesoreria della DAO poichè non indicato alcun valore nella sezione specifica⁹⁸ e l'analisi del contratto di rilievo della DAO non hanno a loro volta fornito i dati necessari.

Nella Tabella 3.24 riportiamo i principali parametri definiti nel contratto.

<i>Parametro</i>	<i>Valore</i>
quorum	350.000.000 W
proposalThreshold	1.000.000 W
votingDelay	172800s = 14.400 blocchi (12s) = 2 giorni
votingPeriod	432000s = 36.000 blocchi (12s) = 5 giorni
minDelay	345600s = 4 giorni

Tabella 3.24: Parametri di governance di Wormhole

Nella tabella Tabella 3.25 sono raccolti gli indirizzi dei contratti analizzati.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
ERC1967Proxy	0xB0fFa8000886e57F86dd5264b9582b2Ad87b2b91	token proxy
WToken	0x344518934533ec82b49eA533b196dce5cfA64411	token implem
HubGovernor	0x239B1F17E6Efa75662cB87781025538babF1Cf6b	governor
TimelockController	0xfBc580c0289121673EfB7375fF111bD2A4db4654	timelock

Tabella 3.25: Lista indirizzi dei contratti in uso di Wormhole

⁹⁸05.02.2026,<https://www.tally.xyz/gov/wormhole/treasury>

3.13 Diva Staking

Diva è un protocollo di Liquid Staking di Ethereum potenziato dalla tecnologia DVT (Distributed Validator Technology), ovvero una tecnologia che permette a un singolo Validatore di essere gestito non da un'unica entità o macchina, ma da un gruppo di nodi indipendenti che lavorano insieme in un "cluster"⁹⁹.



Figura 3.34: Diva Staking Logo

Tale protocollo estende il Proof of Stake di Ethereum fornendo nuove funzionalità per Staker e Operators:

- I **Liquid Stakers** ricevono divETH, un token di Liquid Staking che genera ricompense di staking di Ethereum. Con divETH, gli staker ottengono una flessibilità immediata, poiché il token è istantaneamente trasferibile e scambiabile, a differenza dei modelli di staking tradizionali in cui gli asset sono tipicamente bloccati¹⁰⁰.
- Gli **Operators** devono bloccare ETH, divETH o wdivETH come collaterale e gestire almeno un nodo di validazione distribuita per adempiere ai doveri di staking e guadagnare ulteriori ricompense specifiche per la categoria. Bloccare del collaterale permette loro di ottenere una quota della chiave privata del validatore chiamata "Key Shares". Il processo di validazione di Diva è interamente non-custodial, quindi gli operatori non hanno mai accesso ai fondi o alle chiavi private dei validatori. Il sistema si basa su un meccanismo di consenso 3/5, supportato dalla DVT di Diva e dalle firme a soglia BLS¹⁰¹.

⁹⁹<https://docs.divastaking.com/>

¹⁰⁰<https://docs.divastaking.net/diva/entities/high-level/stakers>

¹⁰¹<https://docs.divastaking.net/diva/entities/high-level/operators>

Le ricompense di staking di Ethereum sono distribuite tra i partecipanti alla rete Diva in base ai loro contributi, nello specifico divETH è un token di ricevuta e il suo saldo si aggiorna quotidianamente per riflettere il saldo di ETH depositato più le sue ricompense di staking di Ethereum.

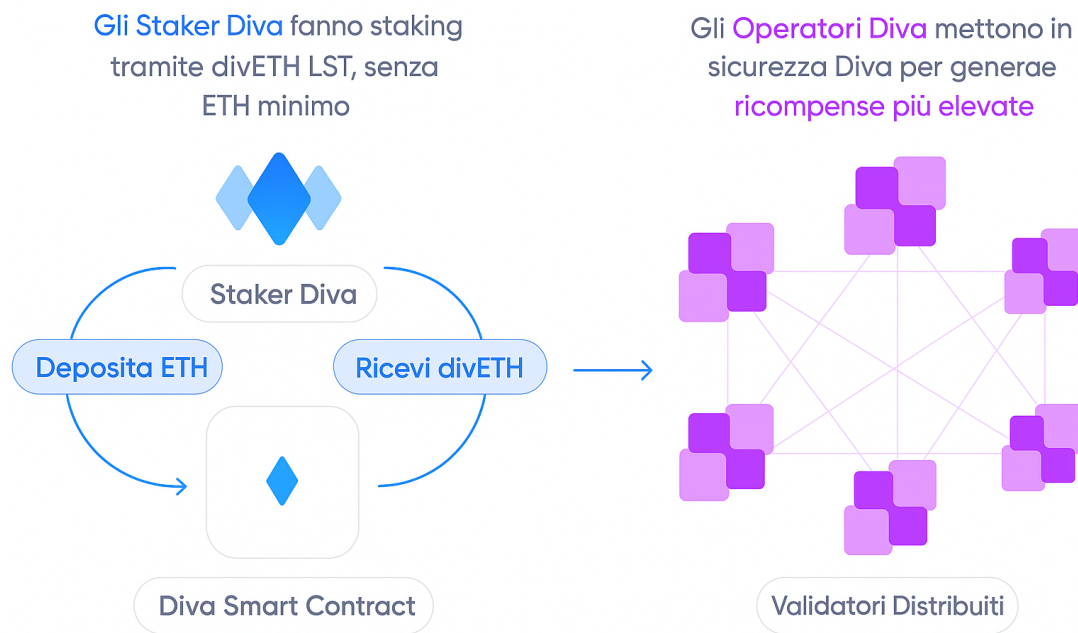


Figura 3.35: Stakers and Operators

Mentre altre soluzioni hanno alcune di queste funzionalità, Diva è la prima soluzione che integra completamente il Liquid Staking con la Validazione Distribuita, offrendo sia ai Liquid Staker che agli Operators la funzionalità più efficiente.

3.13.1 Token DIVA

Il token di governance della DAO Diva Staking è un token ERC-20 con indirizzo:

0xBFABdE619ed5C4311811cF422562709710DB587d

DIVA, al momento del lancio, fu caratterizzato come non trasferibile e privo di valore, il che ha permesso di eliminare qualsiasi interesse speculativo che avrebbe potuto influire negativamente sulla decentralizzazione e sull'equità della distribuzione¹⁰². All'inizio del progetto è stato proposto a circa 15.000 indirizzi di membri della comunità Ethereum di diventare partecipanti iniziali della DAO di Diva. Il processo di claim del token è terminato nell'agosto 2023. Lo scopo di questa distribuzione iniziale era coinvolgere i potenziali utenti di Diva nella progettazione del protocollo il prima possibile, costruendo un sistema che avesse la decentralizzazione al suo centro.



Figura 3.36: DIVA Token

Per partecipare alla governance di Diva Staking i detentori devono delegare i propri token DIVA¹⁰³. Tale delega prevede di selezionare un delegato che voti a proprio nome oppure di auto-delegarsi i token per votare direttamente.

Il token DIVA ha un'offerta fissa di 1.000.000.000 DIVA. L'attuale distribuzione è approssimativamente:

- 73M Distribuzione Iniziale sono stati riscossi, come dettagliato sopra.
- 115M Staking Foundation per ricerca, sviluppo e promozione (precisamente `FOUNDATION_SUPPLY = 115.850.000,00 DIVA`).
- 366M Riserve della DAO.
- 446M Distribuiti ai primi sostenitori del progetto.

¹⁰²<https://docs.divastaking.com/distribution>

¹⁰³<https://docs.divastaking.com/delegates>

Osservazione 3.9. *Non sono attualmente fornite indicazioni sulla precisa offerta attuale del token DIVA né della quantità di token in circolazione né del suo prezzo di mercato¹⁰⁴.*

3.13.2 Processo di governance e analisi dei contratti

Il processo di governance della DAO di Diva Staking è gestito tramite votazioni a proposte create dai membri della comunità rispettando i seguenti passaggi¹⁰⁵.

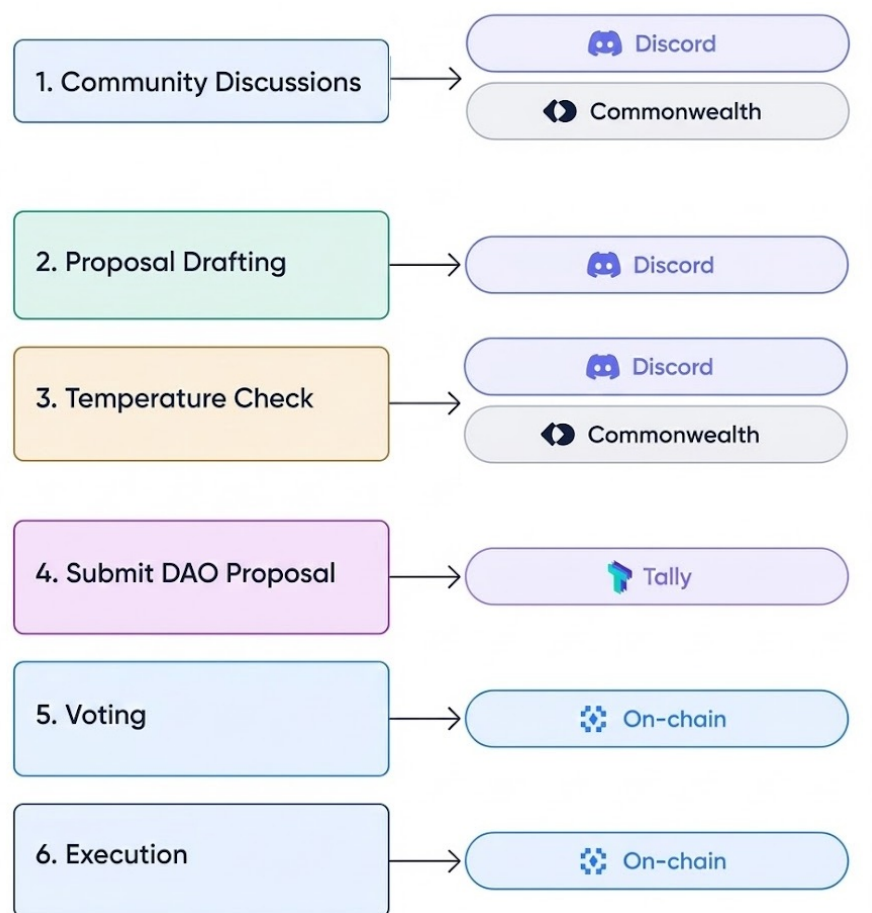


Figura 3.37: Processo di governance di Diva Staking

¹⁰⁴06.02.2026, <https://www.coingecko.com/it/monete/diva-staking>

¹⁰⁵<https://docs.divastaking.com/proposals>

Step 1: Discussioni nella comunità Prima che qualsiasi decisione venga sottoposta a votazione, si può avviare una discussione informale su qualsiasi pensiero/idea/domanda o sul forum ufficiale commonwealth¹⁰⁶ oppure sul canale discord¹⁰⁷. I membri della comunità sono incoraggiati a partecipare, seguendo le linee guida della comunità DAO. I forum sono aperti a tutti.

Step 2: Elaborazione della proposta Alcune discussioni sfoceranno in una proposta che potrà essere sottoposta a votazione. Le tipologie di proposte che possono essere avviate si distinguono a seconda del loro impatto e sono:

- **Basso impatto:** Intese a distribuire il potere di governance tra le comunità. Richiedono +50% di voti favorevoli per essere promulgate.
- **Medio impatto:** Volte ad adattare o modificare una funzionalità configurabile. Richiedono +66% di voti favorevoli per essere promulgate.
- **Alto impatto:** Proposte complesse volte ad aggiornare l'infrastruttura centrale del Protocollo Diva. Richiedono +75% di voti favorevoli per essere promulgate.

Step 3: RFC o Temperature Check Affinché una proposta sia formalmente considerata dalla comunità, deve essere seguito un processo di votazione ufficiale off-chain denominato "temperature check". L'obiettivo è valutare l'interesse per la proposta e il supporto della comunità prima di votare. Il temperature check viene effettuato tramite thread dedicati nei forum della comunità su Discord o Commonwealth.

Step 4: Invio della proposta alla DAO Le proposte, qualora richiedano l'implementazione di qualche operazione on-chain, vengono poi formalmente pubblicate tramite una transazione on-chain su Tally¹⁰⁸. Per inviare una proposta però è necessario che il membro della DAO abbia almeno 1M di DIVA delegati (D-DIVA).

¹⁰⁶<https://common.xyz/divastaking/discussions>

¹⁰⁷<https://discord.com/invite/diva>

¹⁰⁸<https://www.tally.xyz/gov/diva>

Step 5: Votazione Dopo la creazione on-chain, c'è un periodo di attesa di 2 giorni affinché qualsiasi detentore di token DIVA possa delegare i propri token per partecipare alla votazione. Dopodiché le proposte attraversano un periodo di votazione predeterminato di 5 giorni consentendo ai detentori di D-DIVA di votare a favore o contro. Se la proposta soddisfa un quorum valido (10M D-DIVA) e la soglia di votazione supera la percentuale richiesta per la specifica proposta, diventa una *Risoluzione DAO*.

Step 6: Esecuzione Dopo aver soddisfatto la soglia e i quorum, una transazione on-chain mette la *Risoluzione DAO* approvata in coda per l'esecuzione, avviando un periodo di cooldown. Una volta terminato il periodo di cooldown, chiunque può eseguire la transazione per implementare una Risoluzione DAO. I Periodi di Cooldown sono:

- 9 giorni per le proposte normali
- 14 giorni per le proposte critiche che influenzano la sicurezza del protocollo

Osservazione 3.10. *Le Risoluzioni DAO possono essere contestate per prevenire problemi di sicurezza come attacchi di governance o implementazioni di codice fraudolente. Una Proposta di Annullamento deve essere presentata da un membro della comunità con almeno 1M di D-DIVA e ha un Periodo di Cooldown di sole 2 ore.*

I contratti di governance principali che andremo ad analizzare sono i moduli di governor e di timelock il quale funge anche da tesoria dell'organizzazione.

Governor Il contratto **DivaGovernor** è il modulo di governor di Diva Staking basato sullo standard OpenZeppelin. L'indirizzo a cui è registrato è:

0xFb6B7C11a55C57767643F1FF65c34C8693a11A70

Timelock L'indirizzo Ethereum associato al contratto di timelock è:

0x4eBB20995B6264b4b1E25f4473a4636CDB6a9790

Come per il contratto di governor anche il timelock è definito secondo una struttura

modulare basata sullo standard OneZeppelin da cui eredita la gran parte delle funzioni e dei meccanismi logici di base.

Nella Tabella 3.26 troviamo i parametri principali che entrano in gioco della fase di governance di Diva Staking evidenziando quali di essi sono esplicitamente integrati nel codice dei contratti e quali sono noti dalla documentazione ufficiale.

<i>Parametro</i>	<i>Valore</i>
MIN_QUORUM	5.000.000 DIVA
quorum (standard)	10.000.000 DIVA
proposalThreshold	1.000.000 DIVA
votingDelay	14400 blocchi (12s) = 2 giorni
votingPeriod	36000 blocchi (12s) = 5 giorni
minDelay (proposte di annullamento)	600 blocchi = 2 ore
standard delay	9 giorni
long delay	14 giorni

Tabella 3.26: Parametri considerati per la governance di Diva Staking

Tesoreria La tesoreria è esplicitamente gestita attraverso il contratto di timelock ma nonostante tale informazione e nonostante il processo di governance on-chain sia gestito tramite Tally non è stato possibile reperire i dati relativi alla tesoreria della DAO poichè non indicato alcun valore nella sezione specifica¹⁰⁹.

Per concludere quindi la nostra analisi di Diva Staking riportiamo nella Tabella 3.27 l'elenco dei contratti usati per la gestione della sua DAO.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
DivaToken	0xBFAbdE619ed5C4311811cF422562709710DB587d	token
DivaGovernor	0xFb6B7C11a55C57767643F1FF65c34C8693a11A70	governor
DivaTimelockController	0x4eBB20995B6264b4b1E25f4473a4636CDB6a9790	timelock

Tabella 3.27: Lista indirizzi dei contratti di Diva Staking

¹⁰⁹05.02.2026,<https://www.tally.xyz/gov/wormhole/treasury>

3.14 Braintrust

Braintrust è il primo network di talenti decentralizzato al mondo [34]. Questo network mette in contatto i migliori talenti al mondo con lavori ben retribuiti, senza addebitare loro commissioni, offrendo al contempo opportunità di avanzamento di carriera e la proprietà del network su cui basano il proprio lavoro. La community che si affida a Braintrust per trovare lavoro è infatti composta dalle stesse persone che lo possiedono e lo costruiscono, garantendo che la rete serva sempre le esigenze dei suoi utenti, invece di quelle di una società controllata centralmente¹¹⁰.



Figura 3.38: Braintrust Logo

Braintrust consente ai talenti di mantenere il 100% dei propri guadagni e permette ai clienti di ottimizzare i propri budget eliminando gli intermediari superflui.

3.14.1 Token BTRST

Il token di governance della DAO di Braintrust è il token ERC-20 BTRST, il cui contratto è stato lanciato su Ethereum il 1° settembre 2021 con indirizzo:

0x799ebfABE77a6E34311eeEe9825190B9ECe32824

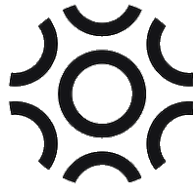


Figura 3.39: Braintrust Logo

¹¹⁰<https://docs.usebraintrust.com/communitydocs>, <https://docs.usebraintrust.com/communitydocs/welcome-to-braintrust>

I principali utilizzi del token BTRST sono¹¹¹:

- **Governance:** I possessori di token BTRST possono discutere idee per miglioramenti, proporre modifiche e votare sulle proposte di governance secondo il principio 1T1V.
- **Bid Staking:** In un mercato competitivo, i talenti possono mettere in staking i token per distinguersi, offrendo i propri token come garanzia i quali verrebbero persi in caso di mancato rispetto del contratto. Anche i clienti possono mettere in staking dei token, i quali vengono distribuiti ai candidati qualificati qualora il cliente decida di non procedere con il lavoro; questo incoraggia i talenti a candidarsi, sapendo che saranno compensati per il tempo speso a redigere una proposta.
- **Vantaggi di Carriera:** Si prevede che i token siano riscattabili per vantaggi speciali offerti da altri partecipanti in esclusiva per la community di Braintrust, inclusi software gratuiti o scontati, prodotti e risorse per la carriera. Gli utenti possono anche guadagnare token seguendo i corsi della Braintrust Academy, un'organizzazione indipendente gestita dalla community che insegna ai talenti competenze preziose per aiutarli a guadagnare di più sul network.

Braintrust prevede un'offerta fissa di 250.000.000 BTRST coincidente con l'offerta totale attuale di cui 241.347.782 BTRST sono in circolazione ¹¹².

3.14.2 Processo di governance e analisi dei contratti

Il processo di governance di Braintrust è composto da tre componenti chiave [34]:

- **Smart Contracts:** Tutto ciò che risiede on-chain può essere, in ultima analisi, soggetto a un processo di governance distribuita.
- **Processo di proposta multifase per gli stakeholder:** Derivato (tramite fork) e adattato dal protocollo Compound, questo funge da metodo ufficiale per

¹¹¹<https://www.usebraintrust.com/tokenomics>

¹¹²06.02.2026,<https://coinmarketcap.com/it/currencies/braintrust/>

la presentazione, la valutazione, la modifica e l'approvazione delle proposte. Le proposte vengono discusse dall'insieme degli stakeholder per poi, in ultima analisi, essere soggette a un voto formale on-chain.

- **Ambienti di Discussione off-chain:** Modellati sull'approccio di Uniswap al coinvolgimento della community, questi servono come canali non vincolanti per la discussione e il dibattito.

Andiamo quindi a vedere quali sono le fasi (Figura 3.40) che vengono attraversate esattamente durante il processo di governance.

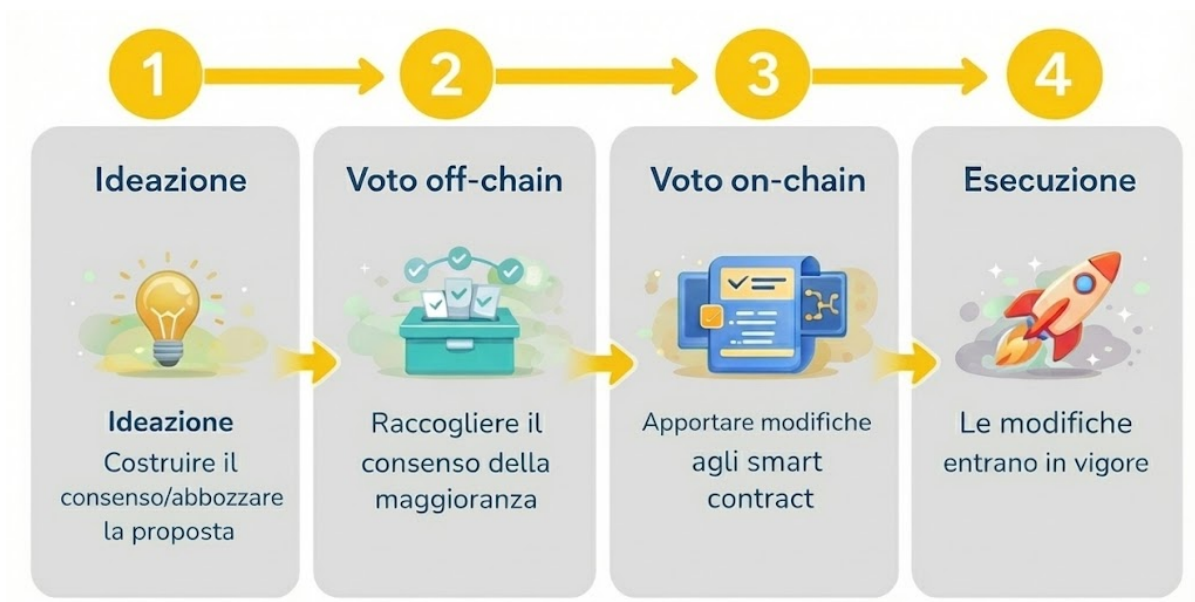


Figura 3.40: Fasi della governance di Braintrust

Fase 1: Ideazione Gli utenti forniscono idee, feedback e sponsorizzazione sul forum ufficiale¹¹³. Quando si sviluppa un certo consenso all'interno della comunità, le proposte vengono redatte e presentate per il voto off-chain.

¹¹³https://app.usebraintrust.com/auth/sign_up/

Fase 2: votazione off-chain In questa fase ci si occupa di ricercare il consenso della maggioranza con due votazioni off-chain tramite la piattaforma Snapshot¹¹⁴:

- **Temperature check:** un semplice sondaggio sì/no utilizzato per determinare se vi sia un sufficiente interesse iniziale da parte della community.
- **Consensus check:** un sondaggio sì/no o a risposta multipla utilizzato per stabilire una votazione formale in merito a una proposta che ha superato il Temperature check.

Le proposte che superano questi passaggi e richiedono modifiche agli smart contract passano poi al votazione on-chain altrimenti passano direttamente all'esecuzione.

Fase 3: votazione on-chain Lo scopo di questa ulteriore votazione è stabilire in maniera formale l'esito di una proposta e di eseguire in maniera automatica il codice in essa contenuto senza il bisogno di intervento esterno.

Fase 4: Esecuzione La fase finale del processo è rappresentata dall'esecuzione. Dopo il successo della fase 3 la proposta on-chain entra in un periodo di timelock di 7 giorni prima di poter essere ufficialmente eseguita.

Governor Il modulo di governor della DAO è un contratto definito all'indirizzo:

0x1a0D3d5a43e53510f80F16905Bc96e907A47dD01

Lo scopo principale di tale contratto è permettere ai detentori del token BTRST di proporre, votare ed eseguire modifiche al protocollo in modo decentralizzato. Il suo codice si basa modello di governance originariamente sviluppato da Compound.

Timelock Il modulo di timelock è invece definito dal contratto con indirizzo:

0xb6f1F016175588a049fDA12491cF3686De33990B

Anche in questo caso il codice si basa sullo standard definito da Compound.

¹¹⁴<https://snapshot.org/#/usebraintrust.eth/about>

Tesoreria La tesoreria della DAO di Braintrust risulta governata dal contratto di timelock. Il volume attuale è di 1.460.963,9\$¹¹⁵

Nella Tabella 3.28 sono raccolti tutti i parametri principali usati nel processo di governance definiti nei precedenti contratti.

<i>Parametro</i>	<i>Valore</i>
proposalMaxOperations	10
quorumVotes	100.000 BTRST
proposalThreshold	500 BTRST
votingDelay	1 blocco = pochi secondi
votingPeriod	17280 blocchi (15s) = 3 giorni
delay	604800s = 7 giorni
MINIMUM_DELAY	172800s = 2 giorni
MAXIMUM_DELAY	2592000s = 30 giorni
GRACE_PERIOD	1209600s = 14 giorni

Tabella 3.28: Parametri considerati per la governance di Braintrust

Come per le precedenti organizzazioni, concludiamo l'analisi della DAO Braintrust raccogliendo nella Tabella 3.29 gli indirizzi dei contratti principali utilizzati nel suo processo di governance.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
BTRST	0x799ebfABE77a6E34311eeEe9825190B9ECe32824	token
GovernorAlpha	0x1a0D3d5a43e53510f80F16905Bc96e907A47dD01	governor
Timelock	0xb6f1F016175588a049fDA12491cF3686De33990B	timelock

Tabella 3.29: Lista indirizzi dei contratti di Braintrust

¹¹⁵06.02.2026,<https://www.tally.xyz/gov/braintrust/treasury>

3.15 UMA

UMA è un Optimistic Oracol (OO) in grado di registrare qualsiasi dato verificabile su una blockchain¹¹⁶. Il sistema di oracoli di UMA fornisce dati on-chain verificati per progetti che includono:

- Mercati predittivi;
- Protocolli assicurativi;
- Derivati personalizzati.

L'Oracolo di UMA¹¹⁷ consente ai contratti di richiedere e ricevere rapidamente in maniera ottimistica nel senso che a differenza degli oracoli tradizionali che verificano ogni singolo dato prima di inserirlo nella blockchain (lento e costoso), UMA parte dal presupposto che i dati proposti siano corretti e vengono verificati solo se qualcuno contesta il dato. Se nessuno si oppone, il dato passa velocemente. Se qualcuno si oppone, si avvia una procedura di disputa tramite il sistema di Data Verification Mechanism (DVM), che generalmente si risolve entro pochi giorni, dopo che i detentori di token UMA hanno votato su quale avrebbe dovuto essere l'esito corretto.



Figura 3.41: UMA logo

L'OO rappresenta la prima parte del sistema e funziona come un gioco di incentivi tra due attori:

- **Asserter:** Colui che propone/invia un nuovo dato (es. "Il prezzo di ETH è 2000\$") e per farlo deposita una cauzione in denaro che gli verrà restituito qualora il dato non venga contestato.

¹¹⁶<https://docs.uma.xyz/>

¹¹⁷<https://oracle.uma.xyz/>

- **Disputer:** Colui che controlla i dati e in caso di problemi con i dati inseriti li contesta entro un periodo di tempo limitato e se ha ragione, guadagna parte della cauzione dell'Asserter.

La seconda parte che compone il sistema è il Data Verification Mechanism (DVM) che funge da "Corte Suprema" di UMA ed interviene solo se c'è una disputa tra Asserter e Disputer. Nel momento in cui entra in azione i detentori del token UMA votano per decidere quale sia la verità, in questo modo introduce il giudizio umano. Questo è fondamentale per risolvere situazioni ambigue o mercati manipolati che un codice automatico non capirebbe¹¹⁸.

Il DVM di UMA è progettato con una garanzia economica basata sul rapporto tra il costo necessario per corrompere l'oracolo e il profitto che se ne potrebbe ricavare. Se il valore del collaterale protetto da UMA sale, il protocollo agisce (tramite buyback o incentivi) per far sì che il valore di mercato del 65% dei token UMA superi sempre quel capitale, rendendo un attacco economicamente svantaggioso¹¹⁹.

3.15.1 Token UMA

UMA è l'omonimo token di utilità e di governance principale del protocollo. Tale token segue lo standard ERC-20 ed il suo contratto si trova all'indirizzo:

0x04Fa0d235C4abf4BcF4787aF4CF447DE572eF828



Figura 3.42: Token UMA

Tale token viene utilizzato per lo staking, per votare e per mettere in sicurezza l'o-

¹¹⁸<https://docs.uma.xyz/protocol-overview/how-does-umas-oracle-work>

¹¹⁹<https://docs.uma.xyz/community/governance>

racolo. I possessori del token contribuiscono a verificare i dati, risolvere le dispute e guidare la direzione del protocollo partecipando alla governance.

La fornitura di UMA non è fissa, al contrario è dinamica e governata dalla DAO. L'offerta totale è di 127.586.834,16 UMA di cui 89.860.607,21 UMA sono in circolazione¹²⁰. I token UMA vengono emessi in base all'`emissionRate`, a favore di coloro che mettono in stake i propri UMA e partecipano attivamente al sistema di votazione¹²¹.

3.15.2 Processo di governance e analisi dei contratti

Le UMIP vengono presentate ai possessori di token UMA per la votazione tramite la Voting dApp¹²² al fine di proporre nuove funzionalità, raccogliere pareri su un determinato tema e documentare, ecc...¹²³.

Fase 1: Pubblicazione su Discourse Il primo passo consiste nel pubblicare un post nel Discourse di UMA¹²⁴. Il post dovrebbe delineare le componenti chiave della proposta e dare alla comunità la possibilità di inviare feedback e suggerire modifiche.

Fase 2: Votazione su Snapshot Quando la proposta sembra pronta, il proponente può creare una votazione su Snapshot¹²⁵ con una durata di 5 giorni. Se alla fine dei 5 giorni riceve il sostegno della maggioranza, passerà a una votazione on-chain. Le proposte che richiedono lo spostamento di fondi dalla tesoreria necessitano del deposito di una cauzione (bond) di 4.000 UMA, che viene restituita se la proposta viene approvata con successo nel voto on-chain dai possessori di token.

Fase 3: Voto on-chain Dopo che una votazione su Snapshot è stata approvata con successo, si tiene un voto on-chain sulla Voting dApp. Se il voto ha esito posi-

¹²⁰06.06.2026<https://coinmarketcap.com/it/currencies/uma/>

¹²¹<https://docs.uma.xyz/faqs#governance>,<https://blog.uma.xyz/articles/uma-token-supply-disclosure>

¹²²<https://vote.uma.xyz/>

¹²³<https://docs.uma.xyz/community/governance/the-umip-process>

¹²⁴<https://discourse.uma.xyz/>

¹²⁵<https://snapshot.box/#/s:uma.eth>

tivo, vengono implementate le modifiche richieste ed eventualmente i fondi richiesti vengono trasferiti all'indirizzo del portafoglio del destinatario tramite oSnap¹²⁶ che è uno strumento costruito sfruttando l'Oracolo Ottimistico (OO) e viene utilizzato per eseguire le votazioni della DAO in modo trustless.

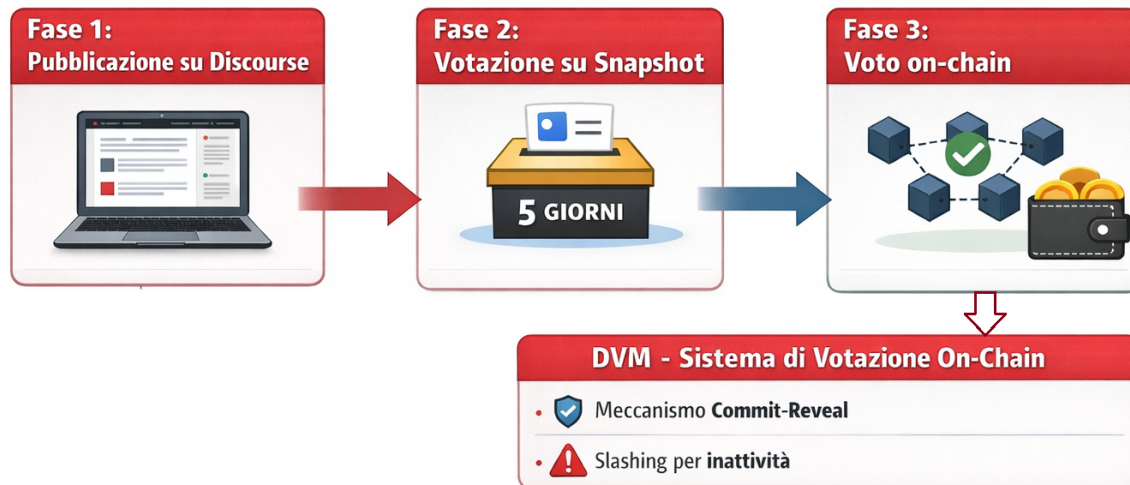


Figura 3.43: Processo di governance di UMA

Il DVM è la sede in cui avvengono tutte le votazioni on-chain di governance vincolanti. È lo stesso sistema di voto sicuro, basato sul meccanismo commit-reveal, utilizzato per risolvere le dispute dell'oracolo; tuttavia, invece di deliberare su proposte relative ai dati, viene utilizzato per approvare o respingere aggiornamenti del protocollo, modifiche ai parametri e decisioni di finanziamento. Il meccanismo commit-reveal prevede che i votanti effettuino il **commit** (impegno) e **reveal** (rivelazione) in due fasi distinte ognuna delle quali è aperta per 24 ore, quindi ogni periodo di votazione dura complessivamente 48 ore. Un'ulteriore differenza rispetto alla risoluzione delle dispute, consiste nel meccanismo di slashing (decurtazione dei token) subito dai votanti. Se votano contro il consenso nelle votazioni di governance non subiscono lo slashing (mentre lo subiscono nelle votazioni sulle dispute). Tuttavia, se un votante non invia alcun voto durante una sessione di governance, subisce una penalità¹²⁷.

¹²⁶<https://uma.xyz/osnap>

¹²⁷<https://docs.uma.xyz/faqs#governance>

I moduli principali che vengono utilizzati nel processo di governance di UMA sono tre: governor, oracle e voting.

Governor Il contratto di governor di UMA ha una prima versione di indirizzo:

0x592349F7DeDB2b75f9d4F194d4b7C16D82E507Dc

Il governor di UMA non descrive un sistema di voto standard, ma delega la decisione all'Oracolo di UMA. Esso in particolare permette di proporre modifiche amministrative o trasferimenti di fondi e di eseguirli automaticamente se i detentori dei token UMA approvano la proposta attraverso il meccanismo di voto del sistema, il DVM.

Il contratto originale è stato sostituito il 24 febbraio 2023 dal contratto di indirizzo:

0x7b292034084A41B9D441B71b6E3557Edd0463fa8

il quale mantiene la funzione principale di eseguire decisioni amministrative basate sul voto dei token holder UMA, ma agisce anche come "Guardiano" grazie a nuove funzionalità di sicurezza e ruoli di emergenza.

Oracle L'oracolo di UMA inizialmente definito tramite il contratto di indirizzo:

0xC43767F4592DF265B4a9F1a398B97fF24F38C6A6

il quale è stato sostituito l'08 giugno 2022 da una nuova versione che introduce maggiore flessibilità e lo rende utilizzabile per casi d'uso più complessi dei semplici feed di prezzo, il cui indirizzo:

0xA0Ae6609447e57a42c51B50EAe921D701823FFAe

Questo è un contratto di servizio che fornisce dati (prezzi, risultati di eventi, ecc.) a chiunque ne faccia richiesta. Il ciclo di vita dell'oracolo prevede che un utente (o uno smart contract) faccia una domanda all'oracolo ed offra una ricompensa (reward) per la risposta quindi un **proposer** fornisce una risposta depositando una cauzione come garanzia di onestà. A questo punto si apre una finestra temporale (Liveness) che di default dura 2 ore in cui possono verificarsi due distinti scenari:

- **Nessuna Disputa:** Nessuno contesta il prezzo o la risposta fornita. Passate le 2 ore, il prezzo diventa ufficiale. Il **proposer** riprende i suoi soldi + la ricompensa.
- **Disputa:** Un **disputer** crede che il **proposer** abbia mentito allora deposita a sua volta una cauzione e apre una contestazione. In questo caso entra in gioco il DVM in cui i detentori di token possono votare quale sia la verità per loro. Alla fine chi ha mentito perde la cauzione e chi ha detto la verità riprende la propria cauzione e la parte di quella del perdente che non viene bruciata.

Voting Il Data Verification Mechanism è implementato all'interno del contratto di voting la cui versione originale ha indirizzo:

0x8B1631ab830d11531aE83725fDa4D86012eCCd77

Tale contratto è poi stato sostituito insieme al contratto di governor il 24 febbraio del 2023. L'indirizzo della nuova versione è:

0x004395edb43EFca9885CEdad51EC9fAf93Bd34ac

Il contratto di voting gestisce il processo attraverso il quale i detentori di token UMA determinano il valore di verità di un dato (prezzo, evento, ecc.) sulla blockchain. Il sistema funziona a Round e utilizza lo schema Commit-Reveal.

- **Fase di commit:** I possessori di token decidono il prezzo segretamente off-chain. Generano un hash crittografico del loro voto + un "salt" (un numero casuale segreto). Inviano questo hash alla blockchain (**commitVote**). In questa fase, nessuno sa cosa hanno votato gli altri.
- **Snapshot:** Appena finisce la fase di Commit, viene scattata una "fotografia" dei saldi dei token UMA. Il peso del voto di ogni utente è determinato da quanti token possedeva in quel preciso istante. Comprare token dopo lo snapshot non aumenta il potere di voto per quel round.
- **Fase di Reveal:** I votanti inviano il prezzo in chiaro e il salt usato prima (**revealVote**). Il contratto verifica che l'hash corrisponda al commit. Se corrisponde, il voto viene contato altrimenti rifiutato.

Dopodichè il contratto aggrega i voti. Verifica il **GAT** (Global Acceptance Threshold) e controlla se la percentuale di token totali che hanno partecipato al voto supera una soglia minima. Chi ha votato come la maggioranza riceve nuovi token UMA mintati. Chi ha votato contro la maggioranza o non ha rivelato il voto, non riceve nulla.

Nella Tabella 3.30 sono riportati i parametri principali che venfono definiti nell'ultima versione contratti analizzati per gestire le votazioni e la governance della DAO.

<i>Parametro</i>	<i>Valore</i>
<code>defaultLiveness</code>	7200s = 2 ore
<code>gat</code>	5.000.000 UMA
<code>spat</code> (% minima di voti concordi)	65%
<code>emissionRate</code>	0.13 UMA/s
<code>votingTime</code>	86400s = 1 giorno
<code>maxRequestPerRound</code>	1000
<code>maxRolls</code>	4
<code>unstakeCoolDown</code>	604.800s = 7 giorni

Tabella 3.30: Parametri considerati per la governance di UMA

Tesoreria La tesoreria di UMA è gestita attraverso il contratto di governor corrente precedentemente analizzato. Il volume contenuto è pari a 17.757.162\$¹²⁸.

Concludiamo la nostra analisi di UMA raccogliendo nella Tabella 3.31 l'elenco dei contratti usati nel processo di governance attuale della DAO e descrivendo il flusso logico che collega i vari contratti. I passaggi chiave di tale flusso prevedono:

- **Presentare la proposta:** Un indirizzo con il ruolo di "Proposer" invia una lista di transazioni che vorrebbe far eseguire al contratto di governor (es. cambiare un parametro del sistema, inviare fondi, aggiornare un contratto).

¹²⁸06.02.2026,<https://debank.com/profile/0x7b292034084a41b9d441b71b6e3557edd0463fa8>,
<https://tokenterminal.com/explorer/projects/uma/metrics/treasury>

- **Richiesta all'Oracolo:** Invece di aprire una votazione interna, il contratto chiama l'oracolo per richiedere un prezzo o un'azione di governance.
- **Fase di votazione:** Se avviata i detentori di token UMA votano nel sistema DVM. Se la proposta passa, il sistema DVM risolve il "prezzo" dell'identificativo inviato ad un valore diverso da 0 (solitamente 1), altrimenti proposta viene rifiutata, il "prezzo" viene risolto a 0.
- **Esecuzione:** Una volta che l'Oracolo ha risolto il "prezzo" (il risultato del voto), chiunque può chiamare la funzione di esecuzione del governor.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
VotingToken	0x04Fa0d235C4abf4BcF4787aF4CF447DE572eF828	token
GovernorV2	0x7b292034084A41B9D441B71b6E3557Edd0463fa8	governor
OptimistiOracleV2	0xA0Ae6609447e57a42c51B50EAe921D701823FFAe	oracle
VotingV2	0x004395edb43EFca9885CEdad51EC9fAf93Bd34ac	voting

Tabella 3.31: Lista indirizzi dei contratti attualmente in uso di UMA

3.16 POOH

POOH, lanciato nell'aprile 2023, nasce con l'ambizione di essere molto più di una semplice memecoin speculativa. L'idea di fondo è quella di superare la volatilità tipica di questo mercato per costruire un vero e proprio ecosistema digitale, capace di reggersi sulle proprie gambe e di durare nel tempo.

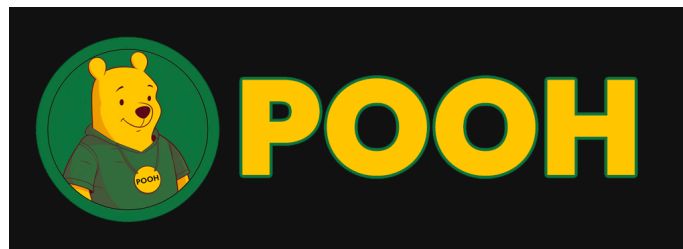


Figura 3.44: POOH Logo

Al centro del progetto c'è una filosofia puramente decentralizzata: POOH si definisce come un "movimento che fa sorridere", dove non esistono barriere all'ingresso. La gestione è affidata interamente alla comunità senza un'autorità centrale dove tutto si basa su trasparenza, distribuzione equa e partecipazione collettiva.

3.16.1 POOH Crew NFT DAO

Un utente che acquisisce un NFT della "POOH Crew", non sta semplicemente acquistando una PFP o un'opera d'arte di comprovata rarità. Sta acquistando l'accesso a una comunità incentrata sulla positività e sull'amicizia¹²⁹.



Figura 3.45: NFTs POOH

Il contratto che definisce tali NFT, che sono gli strumenti per avere accesso alla comunità, è registrato come proxy (EIP-1967 Transparent Proxy) all'indirizzo:

0x3D9F8E430Cd52DcE044b9D88a3574551ece31d1B

¹²⁹<https://pooch.money/nft/>

la cui implementazione ha invece indirizzo:

`0xAeD75D1e5c1821E2EC29D5d24b794b13C34c5d63`

Ogni giorno viene messo all'asta al 1 NFT fino al raggiungimento di 5.000 POOH conati. Ognuno di essi è creato tramite una combinazione specifica dei 66 tratti disponibili e contiene una firma digitale, rendendo ciascuno di essi speciale e unico. Gli NFT POOH sono sostenuti da una tesoreria di asset destinata a crescere nel tempo e controllata collettivamente dalla DAO. Ad oggi l'offerta di PHCR è di 405¹³⁰.

Governor Il modulo di governor che definisce il processo di governance di questa DAO è definito come proxy (EIP-1967 Transparent Proxy) all'indirizzo:

`0x7464012B6794EE8528d8c6b513Cca1C008802490`

la cui implementazione è definita dal contratto di indirizzo:

`0x46eA3fd17DEb7B291AeA60E67E5cB3a104FEa11D`

Tale contratto segue il modello standard OpenZeppelin Governor ed ha lo scopo di gestire la governance on-chain della DAO.

Timelock Il contratto di timelock della DAO è definito tramite il proxy (EIP-1967 Transparent Proxy) di indirizzo:

`0xe8A93664A164D302c83Bbc02CE97502563134aDA`

il quale punta all'indirizzo del contratto di implementazione seguente:

`0x3bdAFE0D299168F6ebB6e1B4E1e9702A30F6364D`

Tale contratto segue lo standard basato sul protocollo Nouns.

Tesoreria Il contratto che detiene i fondi della POOH Crew NFT DAO è il contratto di timelock. Non è stato però possibile risalire all'ammontare al suo volume.

¹³⁰06.02.2026,<https://etherscan.io/address/0x3D9F8E430Cd52DcE044b9D88a3574551ece31d1B#readProxyContract>

Auction Le aste giornaliere degli NFT avvengono tramite il contratto della casa d'asta che è definito dal proxy:

0x5dA573D9F6E5C1332773172131167E844782522a

dotato di implementazione definita al contratto:

0x785708d09b89C470aD7B5b3f8ac804cE72B6b282

Il modello si ispira al protocollo Nouns DAO. Il suo scopo fondamentale è la generazione continua di NFT e la gestione di un ciclo di aste continue e perpetue.

In Tabella 3.32 sono riportati i parametri implementati nei contratti analizzati.

<i>Parametro</i>	<i>Valore</i>
votingPeriod	345600s = 4 giorni
MIN_VOTING_PERIOD	600s = 10min
MAX_VOTING_PERIOD	14515200s = 6 mesi
votingDelay	86400s = 1 giorno
MIN_VOTING_DELAY	1s
MAX_VOTING_DELAY	14515200s = 6 mesi
quorumThresholdBps	10%
MIN_QUORUM_THRESHOLD_BPS	2%
MAX_QUORUM_THRESHOLD_BPS	20%
proposalThresholdBps	0.5%
MIN_PROPOSAL_THRESHOLD_BPS	0.01%
MAX_PROPOSAL_THRESHOLD_BPS	10%
delay	172800s = 2 giorni
gracePeriod	1209600s = 14 giorni
duration	86400s = 1 giorno
minBidIncrement	10%
reservePrice	0.01 ETH

Tabella 3.32: Parametri della governance e delle aste di PoohCrew DAO

Concludiamo raccogliendo nella Tabella 3.33 tutti gli indirizzi usati per la gestione del processo di governance della DAO di PoohCrew.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
ERC1967Proxy	0x3D9F8E430Cd52DcE044b9D88a3574551ece31d1B	token proxy
Token	0xAeD75D1e5c1821E2EC29D5d24b794b13C34c5d63	token implem
ERC1967Proxy	0x7464012B6794EE8528d8c6b513Cca1C008802490	governor proxy
Governor	0x46eA3fd17DEb7B291AeA60E67E5cB3a104FEa11D	governor implem
ERC1967Proxy	0xe8A93664A164D302c83Bbc02CE97502563134aDA	timelock proxy
Treasury	0x3bdAFE0D299168F6ebB6e1B4E1e9702A30F6364D	timelock implem

Tabella 3.33: Lista indirizzi dei contratti di PoohCrew DAO

3.16.2 \$POOH DAO

L'intero universo POOH è però regolato dai possessori di token POOH. Il 95% dei POOH è stato inviato alla pool di liquidità di Uniswap al momento del lancio mentre il 5% è stato allocato agli exchange centralizzati per il listing¹³¹.

Il contratto a cui è definito il token ERC-20 POOH è:

0xB69753c06BB5c366BE51E73bFc0cC2e3DC07E371



Figura 3.46: POOH Token

L'hard cap previsto dal protocollo coincide con l'offerta massima e circolante ed è pari a 420.690.000.000.000 POOH¹³².

¹³¹<https://pooh.money/>

¹³²06.02.2026,<https://coinmarketcap.com/it/currencies/pooh/>

Utilizzando strumenti come la piattaforma Tally¹³³, i membri della community partecipano a processi di voto on-chain trasparenti, consentendo loro di influenzare democraticamente la traiettoria del progetto. I detentori di token possono presentare proposte, partecipare alle discussioni e giungere collettivamente a decisioni che plasmano l’ecosistema POOH grazie ai seguenti smart contract¹³⁴.

Governor Il contratto di governor della DAO è definito all’indirizzo:

0xa5DbAae3daD2784D6B61ef56f934768EfE9d1336

Il contratto è assemblato usando diverse estensioni fornite da OpenZeppelin senza l’introduzione di particolari innovazioni.

Timelock Il timelock della DAO è distribuito all’indirizzo:

0xfefd45d6b7d04A9935C50Ef9226484A385071566

Esso è definito sulla base delle librerie di OpenZeppelin.

Tesoreria La tesoreria anche in questo caso è gestita tramite il contratto di timelock. Il suo volume è 22.280,27\$¹³⁵.

Nella Tabella 3.34 raccogliamo i principali parametri usati nella governance.

<i>Parametro</i>	<i>Valore</i>
proposalThreshold	420.690.000.000 POOH (0.1% della supply totale)
$\text{quorum} = \frac{\text{quorumNumerator}}{\text{quorumDenominator}}$	1.682.760.000.000 POOH (0.4% della supply totale)
votingDelay	1 blocco = pochi secondi
votingPeriod	50400 blocchi (12s) $\equiv$ 7 giorni
getMinDelay	259200s = 3 giorni

Tabella 3.34: Parametri relativi al processo di governance di POOH

¹³³<https://www.tally.xyz/gov/pooh>

¹³⁴<https://www.htx.com/en-in/tokens/pooh/>

¹³⁵06.02.2026, <https://www.tally.xyz/gov/pooh/treasury>

mentre nella Tabella 3.35 sono elencati tutti i contratti della DAO centrale di POOH.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
POOH	0xB69753c06BB5c366BE51E73bFc0cC2e3DC07E371	token
PoohGov	0xa5DbAae3daD2784D6B61ef56f934768EfE9d1336	governor
TimelockController	0xfefd45d6b7d04A9935C50Ef9226484A385071566	timelock

Tabella 3.35: Lista indirizzi dei contratti della DAO primaria di POOH

3.17 Adventure Gold

Loot lanciato da Dom Hofmann nell'agosto 2021 è una collezione di 8.000 NFT rappresentati semplici immagini a sfondo nero con solo testo bianco che elencava equipaggiamento fantasy¹³⁶. Il contratto in cui sono definiti tali NFT è:

0xFF9C1b15B16263C61d017ee9F65C50e4AE0113D7



Figura 3.47: Adventure Gold

Adventure Gold fornisce una gamma di moduli infrastrutturali preinstallati che gli

¹³⁶https://adventuregold.org/whitepaper/agld_whitepaper.pdf

sviluppatori possono personalizzare e utilizzare per implementare meccanismi di logica di gioco unici durante il deployment del loro smart layer. Questi moduli infrastrutturali sono costruiti interamente on-chain, sono open-source e interoperabili, garantendo che l'intero aggregatore di DApp formi un ecosistema di gioco aperto che consente agli sviluppatori di creare e caricare le proprie DApp del Lootverse. Questo ecosistema amplia i confini del game design e diversifica l'infrastruttura, creando maggiori opportunità per uno sviluppo di giochi innovativo.

Le infrastrutture essenziali per supportare le "Loot Adventures" nella creazione delle proprie catene di gioco personalizzate includono:

- **Dashboard di visualizzazione:** Questa interfaccia utente consente alle Loot Adventures di visualizzare facilmente le proprie Loot bags, le mappe di gioco e altri importanti grafici di analisi dati.
- **Marketplace:** Il marketplace fornisce una piattaforma per i giocatori per scambiare risorse e introduce nuovi incentivi per l'esplorazione da parte degli avventurieri.
- **Game engine:** Il motore di gioco è uno strumento cruciale per gli sviluppatori, fornendo un framework personalizzabile per progettare logiche di gioco interamente on-chain.
- **Identità decentralizzata (DID):** Il sistema DID registra la reputazione e le abilità dei singoli avventurieri attraverso i diversi livelli.
- **Smart bridge:** Un sincronizzatore cross-chain che consente ai giocatori di operare tra diverse Loot Chains.

L'ecosistema Adventure Gold è dunque un luogo in cui sviluppatori e giocatori possono unirsi per condividere idee, collaborare e spingere i confini di ciò che è possibile nel gaming on-chain.

3.17.1 Token AGLD

Adventure Gold (AGLD) è il token di incentivazione per il Lootverse.



Figura 3.48: AGLD Token

Il progetto ha assegnato 10.000 AGLD a ciascuno degli 8.000 NFT di Original Loot tramite un airdrop. Il contratto originario del token ERC-20 AGLD:

`0x32353A6C91143bfd6C7d363B546e62a9A2489A20`

Le applicazioni fondamentali che coinvolgono il Token AGLD sono:

- **Governance della comunità:** I detentori di AGLD votano sugli elementi di governance all'interno dell'ecosistema AGLD. Questo include parametri del protocollo (emissione e utilità di AGLD, ecc.), collaborazioni esterne (progetti dentro e fuori il Lootverse) e altro ancora!
- **Valuta In-game:** AGLD può essere utilizzato nei giochi che impiegano NFT del Lootverse che ricevono ricompense di staking in AGLD, per favorire una più rapida adozione da parte degli utenti.
- **Monetizzazione dell'attenzione:** AGLD fornisce un modo per monetizzare efficacemente e restituire valore alla comunità.
- **Commissioni del gas:** AGLD può essere utilizzato per le commissioni del gas dello smart layer e come token di incentivo per i validatori dei nodi.
- **Staking:** I detentori di Loot possono mettere in staking gli NFT per guadagnare ricompense in token AGLD.

L'hard cap previsto dal protocollo per il token è di 96.000.000 AGLD. La supply totale corrente è pari 92.810.001 AGLD mentre quella circolante è 86.610.001 AGLD¹³⁷.

Come anticipato il token AGLD è un token di incentivazione e non un vero e proprio token di governance, infatti per poter votare e partecipare al processo di governance è necessario convertire tali token in AGLDVOTES ovvero altri ERC-20 il cui contratto **AdventureGoldVotes** è un wrapped token definito all'indirizzo:

0x970C30646E5c95DC77A3D768C4362E113Ed92b5b

Attraverso l'uso di tale contratto i detentori di token AGLD li depositano e ricevono in cambio token Adventure Gold Votes per partecipare alla governance.

3.17.2 Processo di governance e analisi dei contratti

Il processo di governance regolato dai possessori di AGLD prevede tre fasi¹³⁸ :

- **Discussione Preliminare:** I membri della comunità avviano discussioni sulle proposte nel forum di governance dell'ecosistema Loot e sul canale Discord.
- **Votazione off-Chain:** Un round di votazione avrà inizio nello Snapshot¹³⁹ di Adventure Gold una volta che una proposta avrà superato la fase di discussione. Per avere successo, le proposte devono ricevere una maggioranza semplice di voti a favore.
- **Esecuzione:** Il core team, insieme ai membri della comunità, può implementare le proposte che sono state approvate.

Governor Il cuore della governance on-chain per il protocollo Adventure Gold è il modulo di governor che ha indirizzo:

0x7ae22bebF28366c328d5558E6Fad935487299DfE

Il contratto è costruito assemblando diversi moduli standard di OpenZeppelin.

¹³⁷06.02.2026, <https://coinmarketcap.com/currencies/adventure-gold/>

¹³⁸<https://messari.io/project/adventure-layer/governance/governance-process>

¹³⁹<https://snapshot.org/#/s:agld-dao.eth>

Timelock Il contratto di timelock è definito all'indirizzo:

0xE4f981249Dde7Cd3c295fc28CB934D4682d7ef9

Tale contratto è definito assemblando diversi moduli standard di OpenZeppelin senza l'introduzione di particolari innovazioni o differenze.

Tesoreria Il ruolo di tesoreria della DAO è assunto dal contratto di timelock. Il volume attuale ad esso associato è di 3.313.900 \$¹⁴⁰

Nella tabella Tabella 3.38 sono riportati i parametri di governance che troviamo definiti all'interno dei contratti esaminati.

<i>Parametro</i>	<i>Valore</i>
proposalThreshold	100 AGLDVOTES
supplyTotale	202.533,48 AGLDVOTES
$\text{quorum} = \frac{\text{quorumNumerator}}{\text{quorumDenominator}}$	20.253,348 (10% della supply totale di AGLDVOTES)
votingDelay	259200s = 21.600 blocchi (12s) = 3 giorni
votingPeriod	604800s = 50.400 blocchi (12s) = 7 giorni
supplyTotale	202.561,48 AGLDVOTES
getMinDelay	604800s = 7 giorni

Tabella 3.36: Parametri relativi al processo di governance di Adventure Gold

Nella Tabella 3.37 sono invece elencati tutti gli indirizzi i contratti principali coinvolti nel processo di governance della DAO.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
AdventureGold	0x32353A6C91143bfd6C7d363B546e62a9A2489A20	token
AdventureGoldVotes	0x970C30646E5c95DC77A3D768C4362E113Ed92b5b	voting token
AdventureGoldGovernor	0x7ae22bebF28366c328d5558E6Fad935487299DfE	governor
TimelockController	0xE4f981249Dde7Cd3c295fc28CB934D4682d7ef9	timelock

Tabella 3.37: Lista indirizzi dei contratti coinvolti nella governance di AGLD

¹⁴⁰06.02.2026, <https://debank.com/profile/0xed4f981249dde7cd3c295fc28cb934d4682d7ef9>

3.18 Degen Dogs

Degen Dogs è un progetto NFT incentrato su una storia di fantascienza distopica. Il "Planet Degen" sta morendo a causa del cambiamento climatico e dell'esaurimento delle risorse. I protagonisti sono 1.001 Degen Dogs, gli unici sopravvissuti, che devono rifugiarsi nel sottosuolo all'interno del CLUB (Canine Laboratory Underground Base) per pianificare la sopravvivenza della specie.



Figura 3.49: Degen Dog NFTs

Il progetto non è solo una collezione artistica, ma una vera e propria DAO il cui obiettivo è decidere come gestire le risorse limitate (i Dog Biscuits o BSCT) e scegliere se tentare di curare il pianeta oppure costruire astronavi per fuggire. A decidere sono i possessori di "Degen Dog" (NFT) che grazie al loro diritto di voto ("1 Dog = 1 Vote") decidono insieme il futuro del progetto¹⁴¹.

I Degen Dogs vengono venduti tramite asta, con un solo NFT all'asta in qualsiasi momento. Le aste si tengono su¹⁴² ma a livello pratico sono gestite dal contratto **DogsAuctionHouse** il cui indirizzo è:

0xC9F32Fc6aa9F4D3d734B1b3feC739d55c2f1C1A7

Le offerte per tali aste vengono presentate sulla rete Polygon in WETH.

¹⁴¹<https://docs.degendogs.club/degen-dogs-mission-1>

¹⁴²<https://degendogs.club/>

Al termine di ogni asta, questa viene finalizzata e l’NFT viene trasferito al miglior offerente. La cadenza dell’asta si riferisce alla sua durata e il protocollo prevede che le aste siano inizialmente piuttosto brevi per poi allungarsi, stabilizzandosi infine su un’asta ogni 24 ore dopo i primi 50 NFT venduti.

Ogni proprietario di un NFT Dog beneficia dei proventi delle aste future secondo il concetto di **Streamonomics** ovvero l’insieme di regole che determina come i flussi di token vengono distribuiti tra i proprietari dei Dog precedentemente conati. Nello specifico tali utenti ricevono in streaming il 50% dei proventi dell’asta con i saldi dei wallet che si aggiornano in tempo reale.

Ogni regola di Streamonomics ha 4 elementi:

- **percentage**: percentuale dei proventi da condividere secondo la regola.
- **start**: contando a ritroso dal Dog attuale, specifica il primo Dog a ricevere un flusso secondo la regola. Ad esempio, un valore di 1 si riferisce al Dog coniato precedentemente al Dog attuale.
- **step**: il prossimo Dog a ricevere un flusso secondo la regola, contando a ritroso.
- **limit**: il numero massimo di Dogs che ricevono flussi secondo la regola.

Le regole di Streamonomics previste nello specifico per la distribuzione del 50% dei proventi nel protocollo della Degen Dogs DAO sono le seguenti tre:

percentage	start	step	limit	Riepilogo
10%	1	1	1	10% al proprietario del Cane precedente.
30%	1	5	20	Una quota del 30% a ogni 5° Dog precedente, condivisa tra un massimo di 20 Dogs.
10%	10	1	1	10% al proprietario del Dog coniato 10 posizioni prima di quello attuale.

Tabella 3.38: Regole Streamonomics di Degen Dogs DAO

Attualmente Degen Dogs sta attraversando una fase di innovazione sull’onda della loro nuova missione che prevede che un totale di 201 Cani che si sono uniti al CLUB

sul Pianeta Degen (Polygon) si teletraportino su un nuovo pianeta Degen Chain una nuova blockchain Layer 3 che in quanto tale risulta essere estremamente specifica, economica e veloce¹⁴³.

3.18.1 Token BSC ed NFT Degen Dog

I token coinvolti nel processo di governance di Degen Dogs oltre ai WETH utilizzati nelle aste sono i Degen Dogs NFT e i Dog Biscuits tokens.

Dog Biscuits - BSCT I BSCT sono token ERC-20 il cui contratto ha indirizzo:

`0x600e5F4920f90132725b43412D47A76bC2219F92`

I token BSCT vengono emessi con un rapporto di 1000:1¹⁴⁴:

- basato sull'offerta presentata nel caso di emissione agli offerenti delle aste Degen Dog, sia vincenti sia perdenti.
- basato sull'offerta vincente nel caso di emissioni a chi invia le transazioni di finalizzazione dell'asta.

La `totalSupply` del token attualmente in circolazione è pari a circa 174.007 BSCT¹⁴⁵.

Degen Dogs NFT L'artwork dei Degen Dogs è ispirato alla pixel art dei Crypto-punks. L'arte "degenerativa" combina 12 tipologie di corpo canino con vari accessori come occhiali, cappelli, orecchini e altro. Alcuni tratti sono più rari di altri¹⁴⁶.

Il contratto che conia tali NFT è distribuito su Polygon all'indirizzo:

`0xA920464B46548930bEfECcA5467860B2b4C2B5b9`

¹⁴³<https://docs.degendogs.club/>

¹⁴⁴<https://docs.degendogs.club/degen-dogs-mission-1/basics/dog-biscuits-bsct>

¹⁴⁵06.02.2026,<https://polygonscan.com/address/0x600e5F4920f90132725b43412D47A76bC2219F92#readContract>

¹⁴⁶<https://docs.degendogs.club/degen-dogs-mission-1/nfts/artwork>

3.18.2 Processo di governance e analisi dei contratti

La governance di Degen Dogs si basa sulla governance di Nouns DAO, che a sua volta è basata sulla governance di Compound¹⁴⁷.

Per presentare una proposta un utente deve disporre in delega di almeno lo 0,25% dell'offerta totale di Degen Dogs. Tali proposte possono riguardare:

- finanziare progetti della community Degen Dogs;
- compensare i membri della DAO o terze parti per servizi a beneficio della DAO;
- investire i fondi della tesoreria;
- espandere il Degen Dogsverse;
- variazioni nelle soglie e i periodi di tempo.

Per inviare e votare le proposte di governance della DAO può essere utilizzato Tally che fornisce un'interfaccia utente (UI). Le proposte e i voti inviati tramite Tally vengono registrati on-chain sui contratti di governance della Degen DAO¹⁴⁸.

Governor Il governor è un proxy (EIP-897 DelegateProxy) definito all'indirizzo:

0x18288e01e2247166d7dF094743a5669BF7fDAaD2

Il corrispondente contratto di implementazione è invece registrato all'indirizzo:

0x9bf49265d8538BeD4dAAe7Fe304F2D41b8Cce265

Tale contratto si basa su una stirpe di contratti di governance ben noti. In particolare prende spunto dal governor della Nouns DAO con due principali innovazioni:

- **Parametri Dinamici (BPS):** Invece di usare numeri fissi di token per determinare il quorum ed il `proposalThreshold`, questo contratto usa i Basis Points (BPS). Questo perché l'offerta totale del token dogs può cambiare nel

¹⁴⁷<https://docs.degendogs.club/degen-dogs-mission-1/dao/governance>

¹⁴⁸<https://www.tally.xyz/gov/degen-dogs>

tempo, i requisiti si adattano automaticamente calcolando una percentuale sulla `totalSupply` al momento della creazione della proposta.

- **Potere di veto:** Esiste un ruolo specifico, il `vetoer`, che può annullare unilateralmente qualsiasi proposta non ancora eseguita.

Timelock/Treasury Il contratto di timelock di Degen Dogs DAO ha indirizzo:

`0xb6021d0b1e63596911f2cCeEF5c14f2db8f28Ce1`

La struttura logica è basata sul celebre `Timelock.sol` di Compound Finance ma è stato aggiornato sull'esempio di Nouns.

I parametri principali coinvolti nel processo di governance che compaiono nei codici dei contratti analizzati sono riportati nella Tabella 3.39.

<i>Parametro</i>	<i>Valore</i>
<code>votingPeriod</code>	152000s = 12667 blocchi (12s) ~ 2 giorni
<code>MIN_VOTING_PERIOD</code>	43200s = 12 ore
<code>MAX_VOTING_PERIOD</code>	604800s = 7 giorni
<code>votingDelay</code>	1s
<code>MIN_VOTING_DELAY</code>	1s
<code>MAX_VOTING_DELAY</code>	302400s = 3.5 giorni
<code>quorumVotesBPS</code>	20%
<code>MIN_QUORUM_VOTES_BPS</code>	2%
<code>MAX_QUORUM_VOTES_BPS</code>	20%
<code>proposalThresholdBPS</code>	0.25%
<code>MIN_PROPOSAL_THRESHOLD_BPS</code>	0.01%
<code>MAX_PROPOSAL_THRESHOLD_BPS</code>	10%
<code>delay</code>	86400s = 1 giorno
<code>MINIMUM_DELAY</code>	1s
<code>MAXIMUM_DELAY</code>	2592000s = 30 giorni
<code>GRACE_PERIOD</code>	1209600s = 14 giorni

Tabella 3.39: Parametri del processo di governance di Degen Dogs DAO

Tesoreria La tesoreria della DAO è gestita dal contratto di timelock analizzato sopra. Attualmente il volume vista la fase di transizione che la DAO sta attraversando è pari a soli 24,2\$¹⁴⁹.

Concludiamo infine l'analisi di Degen Dogs inserendo nella Tabella 3.40 i principali contratti utilizzati nel processo di governace tra quelli analizzati in precedenza.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
BidTokens	0x600e5F4920f90132725b43412D47A76bC2219F92	bid token
Dog	0xA920464B46548930bEfECcA5467860B2b4C2B5b9	token ERC-721
DegenDAOProxy	0x18288e01e2247166d7dF094743a5669BF7fDAaD2	governor proxy
DegenDAOLogicV1	0x9bf49265d8538BeD4dAAe7Fe304F2D41b8Cce265	governor implem
DegenDAOExecutor	0xb6021d0b1e63596911f2cCeEF5c14f2db8f28Ce1	timelock/ treasury
DogAuctionHouse	0xC9F32Fc6aa9F4D3d734B1b3feC739d55c2f1C1A7	auction

Tabella 3.40: Lista indirizzi dei principali contratti di Degen Dogs

3.19 Dope Wars

Dope Wars è un progetto videoludico interamente decentralizzato, permissionless e guidato dalla comunità – ispirato alla cultura hip-hop¹⁵⁰. Il mondo di Dope è ecosistema di gioco ma non solo! È un ambiente in cui giocatori, creatori e narratori danno vita alle idee. Esso viene modellato da ogni interazione, creazione e storia sviluppata dai membri della comunità¹⁵¹.

L'ecosistema di Dope Wars si compone di vari tasselli chiave che andremo ad esaminare ed analizzare di seguito.

¹⁴⁹06.02.2026,<https://www.tally.xyz/gov/degen-dogs/treasury>

¹⁵⁰<https://dopewars.gg/>

¹⁵¹<https://www.dopeworld.gg/>

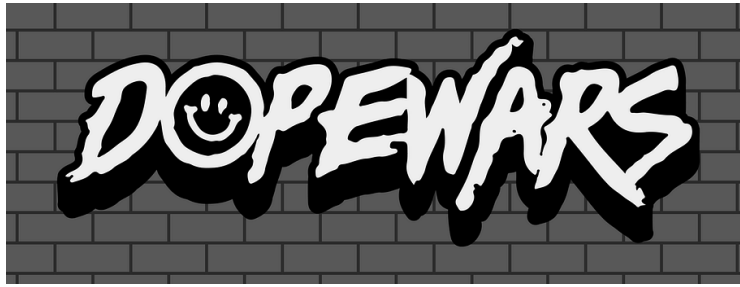


Figura 3.50: Dope Wars Logo

DOPE DOPE è il token di governance e primitiva di base del metaverso di Dope Wars. Tale token è un NFT il cui contratto è definito all'indirizzo:

`0x8707276DF042E89669d69A177d3DA7dC78bd8723`

Nel settembre 2021 sono stati rilasciati 8.000 bundle NFT in edizione limitata, generati casualmente e contenenti token PAPER e Gear, durante un mint in cui si pagava solo il costo del gas. Ogni DOPE fornisce un diritto di voto di Governance paritario sulle proposte della DAO.

Hustlers Gli Hustler sono personaggi di gioco all'avanguardia, completamente personalizzabili, creati riscattando il Gear da un DOPE originale e successivamente mintando un Hustler sulla rete Optimism.

Tutta la pixel art 2D degli Hustler è archiviata sulla blockchain e può essere modificata in qualsiasi momento utilizzando Swap Meet¹⁵².

Gear Sono pezzi di equipaggiamento intercambiabili che risiedono sulla blockchain L2 (Layer 2) Optimism come token ERC-1155. Per creare un gear è necessario riacquitarlo da un NFT DOPE originale usando token PAPER. Questo processo di riscatto produce 9 oggetti NFT separati che possono essere scambiati ed equipaggiati indipendentemente l'uno dall'altro su Optimism.

¹⁵²<https://app.dopewars.gg/swap-meet>



Figura 3.51: Esempio di hustler equipaggiato

PAPER: La valuta dell'ecosistema di Dope Wars, che può essere utilizzata per acquistare potenziamenti, per avanzare nel gioco, ecc... è rappresentata da un token ERC-20 chiamato PAPER il cui contratto è defito all'indirizzo:

0x7aE1D57b58fA6411F32948314BadD83583eE0e8C

Originariamente sono stati distribuiti come quantità riscattabile una tantum di 125.000 unità per ogni DOPE. Da protocollo dunque è prevista un offerta massima di 1.500.000.000 PAPER. Ad oggi è disponibile una supply totale di 1.419.875.000 PAPER di cui solo 901.785.709,9 PAPER effettivamente circolanti¹⁵³.



Figura 3.52: Token PAPER

¹⁵³<https://coinmarketcap.com/it/currencies/dope-wars-paper/>

3.19.1 Processo di governance e analisi dei contratti

Dope Wars è anche un esperimento di finanza di progetto decentralizzata e governata tramite una DAO. Non sono previsti finanziamenti da Venture Capital (VC), tutte le entrate della tesoreria della DAO derivano dalle royalty sulle vendite degli NFT¹⁵⁴.

Il processo di governance dell'organizzazione prevede cicli di proposte presentate off-chain sulla piattaforma Snapshot¹⁵⁵ che vengono poi eseguite on-chain su Tally¹⁵⁶ e quindi tramite opportuni gli smart contract. I contratti principali che vengono utilizzati per la governance sono **DopeDAO** e **Timelock**.

Governor Il cuore della governance della DAO è implementato all'interno del contratto di governor che risiede sulla rete Ethereum all'indirizzo:

0xDBd38F7e739709fe5bFaE6cc8eF67C3820830E0C

Il contratto è costruito secondo lo standard definito dalle librerie OpenZeppelin.

Timelock L'esecuzione delle proposte avviene solo dopo un periodo di timelock che viene gestito dal contratto con indirizzo:

0xB57Ab8767CAe33bE61fF15167134861865F7D22C

il quale a sua volta segue lo standard definito da OneZeppelin.

Tesoreria Il contratto che assume il ruolo di tesoreria principale dell'organizzazione anche in questo caso è il contratto di timelock. Il volume totale della tesoreria attualmente è pari a 19.125,89\$¹⁵⁷.

Nella Tabella 3.41 sono riportati i parametri che regolano il processo di governance che troviamo implementati nei contratti che abbiamo analizzato.

¹⁵⁴<https://dope-wars-033575f3e0ad5927a056d88610120.webflow.io/>

¹⁵⁵<https://snapshot.org/#/s:dopedao.eth/>

¹⁵⁶<https://www.tally.xyz/gov/dopeworld>

¹⁵⁷07.02.2026,<https://www.tally.xyz/gov/dopeworld/treasury>

<i>Parametro</i>	<i>Valore</i>
votingPeriod	45818 blocchi $\simeq$ 6,36 giorni (7 giorni)
votingDelay	13091 blocchi $\simeq$ 43,6 ore (2 giorni)
quorumVotes	500 DOPE
proposalThreshold	50 DOPE
MINIMUM_DELAY	1s
MAXIMUM_DELAY	2592000s = 30 giorni
delay	60s
GRACE_PERIOD	1209600s = 14 giorni

Tabella 3.41: Parametri per la gestione della governance di Dope Wars

Infine riportiamo in Tabella 3.42 gli indirizzi dei contratti coinvolti nel processo di governance della DAO.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
DopeWarsLoot	0x8707276DF042E89669d69A177d3DA7dC78bd8723	governance NFT
Paper	0x7aE1D57b58fA6411F32948314BadD83583eE0e8C	token ERC-20
DopeDAO	0xDBd38F7e739709fe5bFaE6cc8eF67C3820830E0C	governor
Timelock	0xB57Ab8767CAe33bE61fF15167134861865F7D22C	timelock

Tabella 3.42: Lista indirizzi dei principali contratti di Dope Wars

3.20 Hop

Hop Protocol è uno dei "bridge" più noti e utilizzati nell'ecosistema della finanza decentralizzata (DeFi) che serve principalmente a trasferire token in modo rapido e sicuro tra diverse reti combinando due approcci^{158 159}:

- Creare un bridge token inter-rete che possa essere spostato in modo rapido ed economico da un rollup all'altro, oppure riscattato sul Layer-1.

¹⁵⁸<https://hop.exchange/whitepaper.pdf>

¹⁵⁹<https://docs.hop.exchange/basics/a-short-explainer>

- Utilizzare degli Automated Market Maker (AMM) per scambiare ogni bridge token con i suoi corrispondenti Token Canonici su ciascun rollup, al fine di prezzare dinamicamente la liquidità e incentivarne il ribilanciamento.

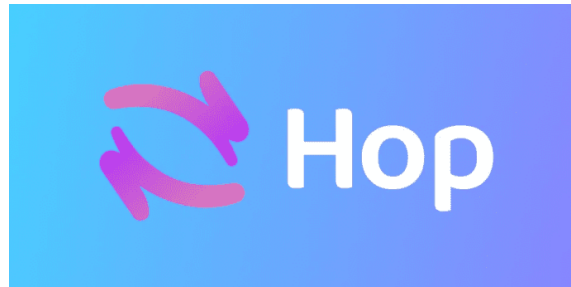


Figura 3.53: Hop Logo

Osservazione 3.11. *Il protocollo di Hop sta attualmente attraversando una fase di innovazione, tuttavia la versione v2 del protocollo è ancora in fase di sviluppo e i relativi contratti sono disponibili solo su testnet.*

3.20.1 Token HOP

Il token di governance della DAO di Hop Protocol è definito nel contratto di indirizzo:

0xc5102fE9359FD9a28f877a67E36B0F050d81a3CC



Figura 3.54: Token HOP

L'offerta iniziale del token ERC-20 al lancio della DAO era di 1.000.000.000 HOP:

- 8% distribuito tramite airdrop ai primi partecipanti della rete.
- 60,5% alla tesoreria della Hop DAO.

- 22,45% al team di sviluppo iniziale (vesting di 3 anni, cliff di 1 anno).
- 2,8% riservato ai futuri membri del team.
- 6,25% agli investitori (vesting di 3 anni, cliff di 1 anno).

Da allora, la DAO ha allocato token Hop dalla tesoreria per una serie di iniziative, come una campagna di liquidity mining per incentivare la liquidità negli AMM del bridge, la formazione di un grant committee, un programma di incentivazione per i delegati e molto altro¹⁶⁰.

Ad oggi la percentuale di offerta circolante nelle mani dei membri della community è pari a 64.107.570 HOP¹⁶¹.

3.20.2 Processo di governance e analisi dei contratti di governance

Per partecipare alla governance di Hop non è sufficiente disporre di token HOP è necessario autodelegare il potere di voto al proprio indirizzo se si vuole votare in prima persona oppure si può anche delegare il potere di voto a uno dei delegati esistenti. Una volta effettuata la delega, che è una transazione on-chain che quindi comporta un costo in gas, gli utenti saranno in grado di votare per la successiva proposta.

Le operazioni di delega e di votazione possono essere entrambe effettuate tramite il portale di Tally¹⁶² dopodichè l'esecuzione on-chain avviene tramite gli smart contract di governance che analizzeremo nel seguente paragrafo¹⁶³.

Governor Il contratto centrale che gestisce la governance della DAO è il contratto di governor definito all'indirizzo:

0xed8Bdb5895B8B7f9Fdb3C087628FD8410E853D48

¹⁶⁰<https://docs.hop.exchange/governance/token-distribution>

¹⁶¹07.02.2026,<https://www.coingecko.com/it/monete/hop-protocol>

¹⁶²<https://www.tally.xyz/gov/hop>

¹⁶³<https://docs.hop.exchange/governance/how-to-vote>

Il codice è costruito utilizzando le librerie standard di OpenZeppelin e ha lo scopo principale di gestire il processo decisionale on-chain del protocollo.

Timelock Il ruolo di timelock esecutivo della DAO è assunto dal contratto il cui indirizzo Ethereum è:

0xeeA8422a08258e73c139Fc32a25e10410c14bd7a

Tale contratto è anch'esso definito tramite le librerie OneZeppelin.

Tesoreria Il ruolo di tesoreria principale dell'organizzazione è assunto dal contratto di timelock. Il volume totale è di 392.566,58\$¹⁶⁴.

Nella Tabella 3.43 sono riportati i valori dei principali parametri coinvolti nel processo di governance.

<i>Parametro</i>	<i>Valore</i>
votingPeriod	45818 blocchi $\simeq$ 6,36 giorni (7 giorni)
votingDelay	1 blocco $\simeq$ pochi secondi
$\text{quorum} = \frac{\text{quorumNumerator}}{\text{quorumDenominator}}$	30% della supply totale (3.000.000 HOP)
proposalThreshold	1.000.000 HOP
minDelay	172800s = 2 giorni

Tabella 3.43: Parametri principali del processo di governance di Hop

Infine nella Tabella 3.44 sono raccolti i principali indirizzi dei contratti di governance coinvolti nel processo di governance della DAO.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
HOPToken	0xc5102fE9359FD9a28f877a67E36B0F050d81a3CC	token
HOPGovernor	0xed8Bdb5895B8B7f9Fdb3C087628FD8410E853D48	governor
TimelockController	0xeeA8422a08258e73c139Fc32a25e10410c14bd7a	timelock

Tabella 3.44: Lista indirizzi dei principali contratti di Hop

¹⁶⁴07.02.2026, <https://www.tally.xyz/gov/hop/treasury>

3.21 onchainaustria

onchainaustria è una comunità e piattaforma blockchain poliedrica, dedicata alla promozione dell'educazione, della decentralizzazione e dei servizi in ambito blockchain che mira a diventare la prima entità giuridica completamente gestita on-chain. onchainaustria è un'associazione austriaca senza scopo di lucro, legalmente registrata e gestita da una DAO come organo decisionale.

Essa si pone l'obiettivo e lo scopo di promuovere di riunire individui appassionati di tecnologia blockchain, fornendo risorse, servizi e opportunità per sostenere attivamente gli ecosistemi decentralizzati [35].



Figura 3.55: onchainaustria Logo

Il modello di governance della DAO è innovativo in quanto combina il processo decisionale basato sulla DAO con la conformità legale e fiscale. Alla base dell'organizzazione troviamo due differenti tokens, un token non speculativo (OCA) che funge da governance token ed un token di mercato (BOCK) che funge da incentivo; entrambi garantiscono in modo trasparente e senza affidamento sulla fiducia che lo

scopo dell'associazione possa essere raggiunto in modo sostenibile dal punto di vista amministrativo ed economico¹⁶⁵.

3.21.1 Tokens: OCA e BOCK

OCA Il token ERC-20 primario della DAO onchainaustria è OCA, un token rebase non trasferibile focalizzato sulla governance. Il suo contratto è definito sulla rete di Arbitrum da un proxy (EIP-1967 Transparent Proxy) di indirizzo:

`0x6BBd25ce17302A626EdF9cfeED6fb0B3ce2ffc47`

la cui implementazione è registrata invece all'indirizzo:

`0x418d2ae1b5bbA48dCABeeEd89B4fA6d21c4C6B47`



Figura 3.56: Token OCA

Da protocollo è prevista un'offerta massima pari a 100.000.000 OCA, con saldi adeguati tramite un meccanismo di rebase piuttosto che tramite la minting o burning di token. Nello specifico quando una nuova proposta viene approvata e comporta allocazioni di token, il meccanismo di rebase adegua proporzionalmente i saldi di tutti i detentori di token per accogliere la nuova allocazione preservando l'offerta totale senza effettuare reali trasferimenti essendo OCA è un token non trasferibile.

Il potere di voto dei membri della comunità si calcola secondo la relazione:

$$1 \text{ voto} = 10^{-18} \text{ OCA}$$

¹⁶⁵<https://onchainaustria.at/onchainaustria-dao/>

Dato che i saldi dei membri variano tramite il meccanismo di rebase varierà anche il potere di voto di ciascun membro, allineando l'influenza all'attività recente e al valore aggiunto.

BOCK Per fornire liquidità e accessibilità ai contributori e ai sostenitori della DAO, i detentori di OCA possono, a propria discrezione, utilizzare un contratto di wrapping che converte i token OCA in un token trasferibile a saldo fisso chiamato BOCK che può essere creato solo tramite tale processo di wrapping. Questo processo consente inoltre al token OCA di essere indirettamente trasferito tra i partecipanti, mantenendo la possibilità di effettuare l'unwrapping per tornare all'OCA originale.

Il contratto del token ERC-20 BOCK è a sua volta definito come un proxy, che segue il medesimo pattern di quello usato per OCA, il cui indirizzo è:

0x61328aaB4926D9ef1030DfC298340125b7EeFaB5

la cui implementazione risiede nel contratto di indirizzo:

0xBB3e61194eDB783c488dD3a367325d8fc34b4dCd



Figura 3.57: Token BOCK

A differenza di OCA, abbiamo detto che BOCK ha un saldo di token costante che non fluttua con gli aggiustamenti del rebase. Tuttavia, il valore sottostante di BOCK è legato alla quantità di OCA (adeguata dal rebase) che esso rappresenta, mantenendo un valore proporzionale senza alterare il conteggio dei token.

Il modello a doppio token si allinea con la missione di onchainaustria separando le funzioni di governance da quelle di liquidità. Mentre OCA è intrasferibile e garantisce

l'esclusività del diritto di voto, BOCK funge da strumento di scambio privo di potere decisionale. Questa separazione protegge la stabilità della governance dalle speculazioni di mercato, pur offrendo un incentivo economico tangibile per la partecipazione attiva ai membri della comunità.

3.21.2 Processo di governance e meccanismo di voto

La DAO di onchainaustria implementa un sistema di governance basato su cicli di proposte e votazioni[35]. Che si tratti di durate di voto dinamiche, finanziamenti scaglionati o creazione collaborativa di proposte, il sistema fornisce una solida base per una governance sostenibile e inclusiva. Le proposte su cui si fonda la governance della DAO sono accomunate da alcune caratteristiche chiave:

- **Formato unico:** La DAO prevede un unico formato di proposta in cui vengono specificati lo scopo, le risorse richieste e i risultati attesi. Questo approccio semplificato facilita la partecipazione, concentrandosi al contempo sull'avanzamento della missione dell'associazione.
- **Allocazione dell'indirizzo del destinatario:** Ogni proposta deve specificare uno o più indirizzi destinatari per l'allocazione di OCA. Non necessariamente tra questi deve esserci il creatore della proposta.
- **Determinazione dell'allocazione di OCA:** La quantità di OCA richiesta in una proposta è flessibile, consentendo ai proponenti di stabilire liberamente l'importo che ritengono equo per il loro contributo. Per aiutarli nel processo, è però disponibile uno strumento di calcolo off-chain come linea guida.
- **Costo per creare una proposta:** Per creare una proposta, i partecipanti devono detenere 10.000 OCA (0,01% della supply totale) nel proprio wallet.
- **Meccanismo di voto:** Le proposte sono soggette a un voto a maggioranza semplice ($> 50\%$) per essere approvate con quorum minimo impostato a 10.000.000 OCA (10% della supply totale). Le opzioni di voto sono tre: "Sì", "No" oppure "Astensione".

- **Delega del potere di voto:** Il potere di voto deve essere delegato per poterlo usare nelle decisioni. La delega può essere effettuata a se stessi o ad un altro indirizzo. La delega è "tutto o niente" compresi eventuali token acquisiti dopo l'inizio della votazione; non è possibile suddividere il potere di voto su più indirizzi.

Per quanto riguarda i passi effettivi che una proposta attraversa durante il processo di governance possiamo considerare 3 step principali schematizzati in Figura 3.58 ed analizzati di seguito.



Figura 3.58: Processo di governance di onchainaustria

Discussione Pre-Proposta All'inizio le proposte nascono come Pre-Proposte sul forum¹⁶⁶ di discussione off-chain della DAO. Questa prima fase consente ai contributori di condividere le proprie idee e di raccogliere i feedback della comunità. Durante questa fase è inoltre possibile suddividere la proposta originaria in due: una pre-approvazione del concetto con 0 OCA allocati seguita da un'approvazione finale per l'effettiva distribuzione di OCA dopo che i risultati sono stati raggiunti.

Invio della proposta on-chain I contributori possono inviare una proposta ufficiale on-chain una volta aggiunto un successo sufficiente durante la pre-discussione. I contributori sono incoraggiati a perfezionare le loro proposte in base agli input della comunità prima di pubblicare ufficialmente la proposta on-chain.

Votazione Il processo di voto include un ritardo di 1 giorno tra l'invio della proposta e l'inizio del periodo di votazione. Questo ritardo lascia tempo per la revisione e la discussione. Una volta iniziato, il periodo di votazione dura per un periodo fisso di 7 giorni, indipendentemente dall'importo di OCA richiesto.

Esecuzione I risultati del voto vengono poi eseguiti automaticamente tramite smart contract adeguando i saldi dei token OCA tramite il meccanismo di rebase.

3.21.3 Analisi dei contratti di governance

Governor Il contratto chiave che insieme ai contratti dei token precedentemente analizzati consente di gestire il processo di governance è il contratto di governor che è definito da un proxy (EIP-1967 Transparent Proxy) all'indirizzo:

0xc93DE629BF8f4Aa7051589F37d2AffdfCCe940cA

la cui implementazione invece risiede all'indirizzo:

0xbfDF915D7959a34BDdB7515306d39b88A03FBc73

Tale contratto è modulare in quanto eredita le funzionalità "standard" da OpenZeppelin e le configura in modo da rispettare il protocollo specifico della DAO.

¹⁶⁶<https://t.me/onchainaustriachat>

Nella Tabella 3.45 sono riportati i valori dei parametri definiti nel contratto.

<i>Parametro</i>	<i>Valore</i>
votingPeriod	604800s = 50.400 blocchi (12s) = 7 giorni
votingDelay (teorico)	1 giorno
votingDelay (codice)	10800s = 900 blocchi (12s) = 3 ore
quorum	10.000.000 OCA (10% supply totale)
proposalThreshold	10.000 OCA (0.01% supply totale)

Tabella 3.45: Parametri principali del processo di governance di onchainaustria

Timelock Il governor non eredita `GovernorTimelockControl.sol` però dalla libreria `OneZeppelin`, il che significa che non appena una proposta ha successo, può essere eseguita immediatamente quindi non troveremo un contratto di timelock.

Tesoreria Non è stato possibile individuare alcun contratto responsabile della tesoreria, di conseguenza non sono presenti dati sul relativo meccanismo e/o volume.

Concludiamo l'analisi della DAO riportando nella Tabella 3.46 i principali indirizzi dei contratti di governance coinvolti nel processo di governance della DAO.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
Transparent UpgradeableProxy	0x6BBd25ce17302A626EdF9cfeED6fb0B3ce2ffc47	governance token proxy
OCA	0x418d2ae1b5bbA48dCABeeEd89B4fA6d21c4C6B47	governance token impl
Transparent UpgradeableProxy	0x61328aaB4926D9ef1030DfC298340125b7EeFaB5	liquidity token proxy
BOCK	0xBB3e61194eDB783c488dD3a367325d8fc34b4dCd	liquidity token impl
Transparent UpgradeableProxy	0xc93DE629BF8f4Aa7051589F37d2AffdfCCe940cA	governor proxy
DAO	0xbfDF915D7959a34BDbe7515306d39b88A03FBc73	governor implem

Tabella 3.46: Lista indirizzi dei principali contratti di onchainaustria

3.22 Rarible

RARI DAO è un'organizzazione autonoma decentralizzata, governata dalla community, che promuove la crescita dell'ecosistema e plasma il futuro dei due principali livelli infrastrutturali:

- **Rarible Protocol:** infrastruttura open-source e gratuita per la creazione di app ed esperienze NFT, come marketplace, wallet, strumenti di analisi ecc. . .
- **RARI Chain:** una chain L3 su Ethereum, sicura ed economica, che garantisce il pagamento delle royalty attraverso l'applicazione diretta a livello di nodo¹⁶⁷.



Figura 3.59: Rarible Logo

In particolare RARI DAO si occupa dei seguenti aspetti:

- Tesoreria della RARI DAO (approvazione dei budget, programmi di incentivi, assegnazione di grant e altro).
- Crescita dell'ecosistema dei due prodotti nell'ecosistema RARI.

Questa visione viene realizzata attraverso una solida architettura di governance che permette a chiunque di essere coinvolto nel processo decisionale bloccando i propri token RARI per esercitare i diritti di voto¹⁶⁸. Tutti i membri della DAO hanno i diritti fondamentali di presentare proposte, votare ed eseguire le proposte approvate indipendentemente da qualsiasi parte centralizzata. Le nuove iniziative vengono

¹⁶⁷<https://rarichain.org/>

¹⁶⁸<https://rari-foundation.gitbook.io/rari-dao-knowledge-base/our-mission-and-values>

presentate alla community sotto forma di RRC (RARI Request for Comment).

Le primissime RRC che hanno segnato la creazione della RARI Foundation sono conosciute come "Costituzione". Mappano nel dettaglio il processo di governance e di voto completamente on-chain¹⁶⁹. Nello specifico:

- **RRC-0:** Ha proposto la costituzione di una RARI Foundation indipendente, interamente controllata e gestita dai detentori di RARI e veRARI. La RARI Foundation agisce come "Consiglio" della DAO, amministrando le proposte della DAO e servendo la visione della community. La RARI DAO può votare per nominare, incaricare e/o rimuovere i direttori della RARI Foundation.
- **RRC-1:** Questa proposta stabilisce l'infrastruttura di voto per permettere alla community di partecipare al processo decisionale della RARI DAO. Introduce il concetto di veRARI e il meccanismo di locking dei token RARI con un piano di rilascio specifico per ricevere potere di voto.
- **RRC-2:** In questa proposta è stato definito un programma di ricompense in RARI per incentivare gli utenti a listare NFT su Rarible e ad acquistare NFT dal marketplace aggregato di Rarible.

La governance di RARI DAO si sta attualmente evolvendo attraverso una transizione dalla DAO originale basata su Ethereum (v1) a una DAO appena lanciata sulla RARI Chain (v2).

- **v1 su Ethereum:** I token RARI vengono bloccati per ricevere veRARI. Per votare si può usare Tally¹⁷⁰ o delegare tramite il sito [rari.foundation](https://www.rari.foundation).
- **v2 su RARI Chain:** Si mettono in staking i token RARI e delegare il potere di voto tramite l'interfaccia di governance Tally¹⁷¹. Questo modello rimuove la necessità di scegliere tra partecipare alla governance e usare i token nella DeFi. Elimina inoltre le gas fee per il blocco e la delega, rendendo la partecipazione più accessibile e flessibile.

¹⁶⁹<https://rari-foundation.gitbook.io/rari-dao-knowledge-base/dao-constitution>

¹⁷⁰<https://www.tally.xyz/gov/rari-foundation>

¹⁷¹<https://www.tally.xyz/gov/rari-dao>

I membri della community sono invitati a partecipare a entrambe le DAO durante la transizione. La RARI Foundation continuerà a supportare e coordinare questa evoluzione verso una governance multichain unificata che alla fine governerà tutti gli aspetti del protocollo su tutte le chain¹⁷².

3.22.1 Token RARI

RARI è il token di governance dell'ecosistema Rarible Protocol, emesso nel 2020 con un'offerta massima di 25 milioni di RARI¹⁷³, ha attualmente un'offerta circolante di 19.488.927,79 RARI¹⁷⁴. La distribuzione iniziale del token è stata la seguente:

- 10% distribuito tramite airdrop ai detentori di NFT nella community.
- 60% accantonato per ricompensare gli utenti delle applicazioni costruite sul Rarible Protocol.
- Il restante 30% è stato distribuito agli investitori e al team di Rarible.

Il protocollo di voto per la RARI DAO si basa sui token RARI bloccati dai detentori, noti anche come veRARI (vote-escrowed RARI). veRARI rappresenta dunque il potere di voto non trasferibile che un detentore riceve bloccando i propri RARI in un contratto di voting-escrow per un periodo di tempo scelto.



Figura 3.60: Token RARI

Il contratto originale del token ERC-20 RARI risiede su Ethereum all'indirizzo:

0xFca59Cd816aB1eaD66534D82bc21E7515cE441CF

¹⁷²<https://rari-foundation.gitbook.io/rari-dao-knowledge-base/governance>

¹⁷³<https://rari-foundation.gitbook.io/rari-dao-knowledge-base/governance/usdrari>

¹⁷⁴08.02.2026,<https://coinmarketcap.com/currencies/rarible/>

mentre il contratto originale di veRARI è un proxy definito tramite EIP-1967 Transparent Proxy pattern con indirizzo:

0x096Bd9a7a2e703670088C05035e23c7a9F428496

la cui implementazione è definta all'indirizzo:

0x51c37534Ef4bB272caC10AB596ae843F786fD793

In seguito alla nascita di RARI Chain (chainID: 1380012617) per rendere possibile la transizione verso la nuova versione dell'organizzazione (v2) è stato creato il bridge token di RARI che risiede sulla nuova blockchain. Tale contratto è definito come proxy EIP-1967 all'indirizzo:

0xCf78572A8fE97b2B9a4B9709f6a7D9a863c1b8E0

il cui contratto di implementazione ha invece indirizzo:

0xBfA812cefAA83C355A8A231a1165773038BEb415

Per quanto riguarda invece il contratto di veRARI una volta completata la transizione verso RARI Chain, la v2 DAO diventerà l'unico organo di governo e il modello veRARI utilizzato nella v1 DAO verrà dismesso.

I contratti definiti sulla RARI Chain possono essere ricercati e analizzati usando l'explorer specifico¹⁷⁵.

3.22.2 Processo di governance e analisi dei contratti

Il processo di governance della RARI DAO consiste nelle seguenti fasi:

Fase 1: Ideazione La fase iniziale ha una durata di 7 giorni in cui gli autori della futura proposta ideano un'iniziativa, la condividono con la community e raccolgono ne raccolgono i feedback interagendo con loro sul forum.

Fase 2: Bozza della proposta Dopo aver raccolto gli input della community, viene redatta una proposta formale secondo la seguente struttura. Una volta che la

¹⁷⁵<https://mainnet.explorer.rarichain.org/>

proposta assume la sua forma di bozza definitiva, viene pubblicata sul forum ufficiale della RARI DAO, dove rimane per almeno 7 giorni affinché una community più ampia possa esaminarla. Successivamente, qualsiasi feedback aggiuntivo viene incorporato direttamente nella proposta inviata su Tally.

Fase 3: Invio e votazione on-chain La proposta a questo punto viene avviata per il voto on-chain su Tally, gli autori necessitano di 5.000 veRARI (v1) o dell'aiuto di un delegato con più di 5.000 voti che supporti l'idea (v2). Dal momento della pubblicazione la community ha 5 giorni per votare "a favore", "contro" o astenersi.

Fase 4: Periodo di Cooldown Nei 2 giorni successivi all'accettazione della proposta, il Consiglio ha il diritto di respingerne l'implementazione se risulta essere dannosa per la DAO. Questi poteri possono essere esercitati anche dal Security Council, che ha il potere di porre il veto su proposte che potrebbero essere di natura dannosa nei confronti della Tesoreria o del Protocollo.

Fase 5: Implementazione A questo punto chiunque può mettere in coda ed eseguire una proposta che se approvata si auto-eseguirà tramite smart contracts.

Analizziamo ora i principali contratti usati nel processo di governance di RARI DAO. Studieremo in particolare il governor ed il timelock definiti sia per v1 che per v2.

Governor Il contratto di governor definito per la blockchain di Ethereum è un proxy (EIP-1967 Transparent Proxy):

0x6552C8fb228f7776Fc0e4056AA217c139D4baDa1

a cui è associato il contratto di implementazione:

0x859E1C00ED6D4b4e649c7a38918E982653B2EdCA

Il contratto **RariGovernor** è costruito utilizzando lo standard di OpenZeppelin.

Il contratto di governor definito per la v2 su RARI chain non presenta particolari

differenze e quelle poche pesanti sono legate a miglioramenti nella pulizia del codice e non a livello strutturale. Tale contratto è definito come proxy all'indirizzo:

0x4086c6760B81B431624DD76f8c9EAB839Ea49beA

La corrispondente implementazione ha invece indirizzo:

0x401B9149459d489e7CB8bBadc86Fa2e5c8776A94

Timelock Il contratto di timelock della versione originale della DAO che risiede su Ethereum è un proxy (EIP-1967) che ha indirizzo:

0x7e9c956e3EFA81Ace71905Ff0dAEf1A71f42CBC5

Il contratto in cui è definita la corrispondente implementazione ha invece indirizzo:

0xF46e8e6fA0F048DdD76F8c6982eBD059796298B8

Il codice principale non contiene logica personalizzata complessa, si basa direttamente sulla libreria `OneZeppelin TimelockControllerUpgradeable.sol`.

Nella nuova versione v2 si fa riferimento al contratto proxy e alla corrispondente implementazione che risiedono su RARI Chain rispettivamente agli indirizzi:

0x90BeDbEf93120bf7E4AcDdd6171053c3A12903F0

0x12A142a3a311Cb176A788db9161Ff2367844326C

Tali contratti non presentano alcuna differenza rispetto alla v1.

Tesoreria In entrambe le versioni il timelock assume anche il ruolo di tesoreria della DAO. Il volume complessivo è pari a 12.071\$¹⁷⁶ ma tale valore è in continua evoluzione per via della fase di transizione che il progetto sta attraversando.

Riportiamo dunque nella tabella Tabella 3.47 i valori dei principali parametri coinvolti nel processo di governance di RARI DAO.

¹⁷⁶08.02.2026,<https://debank.com/profile/0x90bedbef93120bf7e4acddd6171053c3a12903f0>,<https://debank.com/profile/0x7e9c956e3efa81ace71905ff0daef1a71f42cbc5>

<i>Parametro</i>	<i>Valore v1</i>	<i>Valore v2</i>
votingPeriod	36000 blocchi (da 12s) = 5 giorni	36000 blocchi = 5 giorni
votingDelay	0	0
minDelay	172800s = 2 giorni	172800s = 2 giorni
$\text{quorum} = \frac{\text{quorumNumerator}}{\text{quorumDenominator}}$	15% della supply totale	10% della supply totale
proposalThreshold	5.000 RARI	5.000 RARI

Tabella 3.47: Parametri principali del processo di governance di RARI DAO

Per concludere infine l'analisi di Rari Capital raccogliamo nella Tabella 3.48 gli indirizzi dei contratti v2 che troviamo su RARI Chain e che diventeranno in futuro gli unici che si occuperanno di gestire la governance.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
EIP173Proxy	0xCf78572A8fE97b2B9a4B9709f6a7D9a863c1b8E0	token proxy
RariBridgeToken	0xBfA812cefAA83C355A8A231a1165773038BEb415	token implem
EIP713ProxyWithReceive	0x4086c6760B81B431624DD76f8c9EAB839Ea49beA	governor proxy
RariGovernor	0x401B9149459d489e7CB8bBadc86Fa2e5c8776A94	governor implem
EIP713ProxyWithReceive	0x90BeDbEf93120bf7E4AcDdd6171053c3A12903F0	timelock proxy
RariTimelockController	0x12A142a3a311Cb176A788db9161Ff2367844326C	timelock implem

Tabella 3.48: Lista indirizzi dei principali contratti di RARI DAO su RARI Chain

3.23 Inverse

Fondato originariamente da Nour Haridy alla fine del 2020, il protocollo è governato dalla Inverse Finance DAO, guidata dai detentori dei token di governance INV insieme ai collaboratori che lavorano a tempo pieno per la DAO. Questi collaboratori vantano complessivamente molti anni di esperienza nel settore delle criptovalute,

della DeFi e dello sviluppo blockchain¹⁷⁷.



Figura 3.61: Inverse Finance Logo

Inverse Finance è l'organizzazione autonoma decentralizzata che sviluppa e gestisce il protocollo di prestito a tasso fisso FiRM, DOLA (la sua stablecoin decentralizzata garantita da debito) e sDOLA (la versione di DOLA che genera rendimento).

La DAO delega certi poteri decisionali ai gruppi di lavoro, ai quali viene concessa un'autonomia limitata e un budget tramite il voto di governance della DAO. Le responsabilità di questi gruppi di lavoro sono determinate all'interno delle loro proposte, ma tutti i gruppi sono progettati per garantire che la DAO sia in grado di far fronte alle condizioni di mercato in rapida evoluzione, assicurare la continuità quotidiana dello sviluppo del prodotto, sollevare i singoli votanti (token holders) dal sovraccarico di governance e creare un ambiente comunitario affidabile e piacevole¹⁷⁸.

Gli attuali gruppi di lavoro includono:

- **Product Working Group (PWG)**: Il PWG è composto dai core contributors che guidano l'innovazione e la manutenzione del prodotto.
- **Growth Working Group (GWG)**: Il GWG guida lo sviluppo del business, il marketing, il design e le funzioni della community presso Inverse Finance.
- **Treasury Working Group (TWG)**: Il TWG è stato formato con l'obiettivo di ottimizzare la gestione degli asset della tesoreria per supportare l'ecosistema

¹⁷⁷<https://docs.inverse.finance/inverse-finance>

¹⁷⁸<https://docs.inverse.finance/inverse-finance/inverse-finance/introduction/organization>

DOLA. Il TWG consente inoltre alla gestione della liquidità di estendersi oltre la sola blockchain di Ethereum, come su Optimism, Base, Arbitrum e Polygon.

- **Risk Working Group (RWG):** Il RWG è stato formato per supportare tutte le funzioni di Inverse Finance, come l'espansione di DOLA, fornendo una solida analisi del rischio, la gestione del rischio, il monitoraggio continuo del rischio per i prodotti esistenti e il supporto agli sforzi degli altri gruppi di lavoro.
- **Analytics Working Group (AWG):** L'AWG ha l'obiettivo principale di consentire agli utenti di accedere senza problemi ai dati di cui hanno bisogno e utilizzarli nell'ambiente di loro scelta.

3.23.1 Tokens DOLA e INV

INV INV è il token di governance ERC-20 della DAO di Inverse Finance, il cui contratto è registrato all'indirizzo:

0x41D5D79431A913C4aE7d69a668ecdfE5fF9DFB68



Figura 3.62: Token INV

Tale token non si limita a consentire ai membri di partecipare a discussioni e votazioni, esso è infatti coinvolto in diversi aspetti della DAO¹⁷⁹.

- I detentori di INV che mettono in staking i loro INV su FiRM¹⁸⁰ ricevono due forme di ricompense di staking continue: ricompense anti-diluizione INV e ricompense in streaming DBR.

¹⁷⁹<https://docs.inverse.finance/inverse-finance/inverse-finance/product-guide/tokens/inv>

¹⁸⁰<https://docs.inverse.finance/inverse-finance/inverse-finance/product-guide/firm>

- Gli INV in staking possono essere utilizzati come collaterale per prestiti a tasso fisso a lungo termine sul mercato di prestito a tasso fisso della DAO, FiRM.
- INV fornisce ai detentori potere di voto nella Inverse Finance DAO.

L'offerta circolante di INV è soggetta a espansioni o emissioni periodiche utilizzate per finanziare varie iniziative della DAO. Per questo motivo il token INV non ha un'offerta massima. Attualmente l'offerta totale è di 727.000 INV la quale è quasi interamente circolante (725.586,02 INV)¹⁸¹.

DOLA DOLA è una stablecoin sintetica e decentralizzata ancorata al dollaro statunitense (USD). È progettata per essere valutata il più vicino possibile a 1\$ con una volatilità minima. Tale stablecoin esiste come token ERC-20 su diverse blockchain. In particolare il suo contratto sulla rete Ethereum ha indirizzo:

0x865377367054516e17014CcdED1e7d814EDC9ce4



Figura 3.63: Token DOLA

Due caratteristiche chiave che distinguono DOLA rispetto alle altre stablecoin sono¹⁸²:

- **Garantita da debito:** DOLA è interamente garantita da debito e non è una stablecoin algoritmica parzialmente collateralizzata.
- **Supportata dalle Fed di Liquidità DOLA:** Le Fed DOLA consentono a Inverse di distribuire rapidamente liquidità su catene diverse da Ethereum come Arbitrum, Optimism o Base e di utilizzare contemporaneamente le Fed DOLA per gestire l'ancoraggio USD di DOLA.

¹⁸¹08.02.2026,<https://coinmarketcap.com/currencies/inverse-finance/>

¹⁸²<https://docs.inverse.finance/inverse-finance/inverse-finance/product-guide/tokens/dola>

Essendo una stablecoin ancorata al dollaro, DOLA non ha un tetto massimo previsto da protocollo. La sua offerta totale coincide con quella circolante che ad oggi è pari a 183.814.118,24 DOLA¹⁸³.

3.23.2 Processo di governance e analisi dei contratti

I detentori di INV possiedono potere di voto nel nostro sistema di governance decentralizzato e on-chain, **Governor Mills**¹⁸⁴, dove un INV equivale a un voto¹⁸⁵. I passaggi che devono essere seguiti per lanciare una proposta di governance sono:

Fase 0: Discussione off-chain facoltativa Discussione della proposta con altri membri della community su Discord¹⁸⁶ nel canale Governance-General prima della pubblicazione ufficiale.

Fase 1: Pubblicazione proposta off-chain Creazione di un post sul forum¹⁸⁷ della DAO con la proposta descritta nella sua interezza ma senza il codice effettivo per le azioni on-chain

Fase 2: Creazione di una bozza Creazione di una bozza della proposta sul contratto di governor. E' in particolare richiesto da protocollo che una bozza sia visibile per almeno 24 ore prima che la votazione abbia inizio.

Fase 3: Votazione ed esecuzione Lancio della proposta per una votazione on-chain. Qualsiasi detentore di INV che possiede almeno 1900 INV delegati al proprio indirizzo o che è un membro della DAO in whitelist può inviare una proposta on-chain in Governor Mills. Le votazioni rimangono aperte per circa 60 ore, seguite da un periodo di attesa di 40 ore prima dell'esecuzione della proposta. Le proposte per

¹⁸³08.02.2026,<https://coinmarketcap.com/currencies/inverse-finance-dola-stablecoin/>

¹⁸⁴<https://www.inverse.finance/governance>

¹⁸⁵<https://docs.inverse.finance/inverse-finance/inverse-finance/introduction/governance>

¹⁸⁶<https://discord.com/invite/Q3pQ5WsXZ5>

¹⁸⁷<https://forum.inverse.finance/>

avere successo richiedono un minimo di 15500 voti "a favore" per superare il quorum e devono avere più voti "a favore" che "contro".

Osservazione 3.12. *Ogni utente per essere idoneo al voto, deve necessariamente delegare i propri voti a se stesso oppure ad un delegato preposto.*

Governor Inizialmente il processo di governance della DAO non era gestito tramite la piattaforma Governor Mills, che era ancora in fase di sviluppo, ma tramite Tally¹⁸⁸. Il contratto di governor che consentiva tale processo in tale fase era:

0x35d9f4953748b318f18c30634bA299b237eeDfff

Con la nascita della piattaforma Governor Mills si è reso necessario implementare un nuovo contratto di governor il cui indirizzo è:

0xBeCCB6bb0aa4ab551966A7E4B97cec74bb359Bf6

Il contratto **GovernorMills** rappresenta un'evoluzione significativa e "customizzata" rispetto allo standard **GovernorAlpha** precedente. Le principali differenze introdotte con tale contratto sono:

- Supporto di un'economia a doppio token consentendo anche ai possessori di xINV di votare le proposte introducendo la funzione `_getPriorVotes` che normalizza il valore di xINV in INV.
- Introduzione del ruolo di **Guardian** che consente al suo possessore di cancellare (`cancel`) qualsiasi proposta, anche se il proponente ha ancora i voti necessari se questa è considerata dannosa per l'organizzazione.
- Aumento di flessibilità e di customizzazione dei parametri.

Timelock Il contratto di timelock di Inverse Finance è invece unico fin dalla nascita della DAO ed è definito all'indirizzo:

0x926dF14a23BE491164dCF93f4c468A50ef659D5B

¹⁸⁸<https://www.tally.xyz/gov/inverse>

La logica del contratto non è un'innovazione specifica di Inverse Finance si tratta invece di una fork del Timelock di Compound Finance.

Tesoreria Il contratto di timelock gestisce anche la tesoreria della DAO. Il volume in esso contenuto è pari a 1.607.234\$¹⁸⁹.

I principali parametri che sono coinvolti nel processo di governance della DAO che vengono definiti all'interno dei precedenti contratti sono raccolti nella Tabella 3.49.

<i>Parametro</i>	<i>Valore GovernorAlpha</i>	<i>Valore GovernorMills</i>
votingPeriod	17280 blocchi (15s) = 3 giorni	17280 blocchi (15s) = 3 giorni
votingDelay	1 blocco $\simeq$ pochi secondi	1 blocco $\simeq$ pochi secondi
MAXIMUM_DELAY	2592000s = 30 giorni	2592000s = 30 giorni
MINIMUM_DELAY	172800s = 2 giorni	172800s = 2 giorni
GRACE_PERIOD	1209600s = 14 giorni	1209600s = 14 giorni
quorumVotes	4.000 INV	15.500 INV
proposalThreshold	1.000 INV	1.900 INV

Tabella 3.49: Parametri principali del processo di governance di Inverse Finance

Concludiamo l'analisi di Inverse Finance raccogliendo nella Tabella 3.50 gli indirizzi dei contratti principali coinvolti nel processo di governance attualmente in uso.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
INV	0x41D5D79431A913C4aE7d69a668ecdfE5fF9DFB68	token
ERC20	0x865377367054516e17014CcdED1e7d814EDC9ce4	stablecoin
GovernorMills	0xBeCCB6bb0aa4ab551966A7E4B97cec74bb359Bf6	governor
Timelock	0x926dF14a23BE491164dCF93f4c468A50ef659D5B	timelock

Tabella 3.50: Lista indirizzi degli attuali contratti di governance di Inverse Finance

3.24 Public Nouns

Public Nouns è un nuovo metodo sperimentale per sostenere i beni pubblici che nasce da una fork di Nouns in cui si considerano unicamente NFT ispirati a beni pubblici.

¹⁸⁹08.02.2026, <https://debank.com/profile/0x926df14a23be491164dcf93f4c468a50ef659d5b>

Tutti gli ETH provenienti dalle aste di Public Noun vanno direttamente alla Public Nouns DAO, dove un Public Noun equivale a un voto¹⁹⁰.

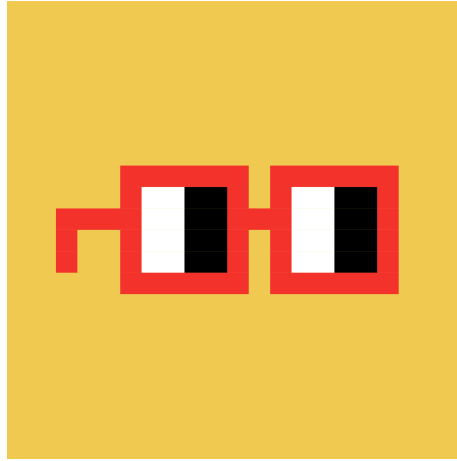


Figura 3.64: Public Nouns Logo

La missione della Public Nouns DAO è sostenere i beni pubblici:

- Sperimentando nuovi metodi di finanziamento dei beni pubblici, iniziando proprio con Public Nouns.
- Diffondendo la consapevolezza sui beni pubblici.
- Finanziando beni pubblici, creatori e meccanismi dedicati al bene comune.

3.24.1 NFT e processo d'aste

I token di governance che attribuiscono ai possessori il diritto e il potere di voto (1T=1V) sono gli NFT $\textcircled{P}$ NOUN. Il contratto che definisce tali token secondo lo standar ERC-721 è:

0x93ecac71499147627DFEc6d0E494d50fCFFf10EE

Il numero totale di NFT attualmente esistenti è definito in tale contratto tramite il parametro `totalSupply` ed è pari a 293¹⁹¹.

¹⁹⁰<https://publicnouns.wtf/>

¹⁹¹09.02.2026

Osservazione 3.13. *I voti dei Public Noun sono non trasferibili (vendendo $\textcircled{P}$ NOUN, il voto viene trasferito con esso). Tali voti sono però delegabili, ciò significa che si può assegnare il proprio voto a qualcun altro fintanto che si possiede l’NFT.*



Figura 3.65: Examples of $\textcircled{P}$ NOUN NFTs

Per generare $\textcircled{P}$ NOUN viene utilizzato il **Public Nouns Auction** contract che agisce come un meccanismo autosufficiente di generazione e distribuzione di Public Nouns, mettendone all’asta uno ogni 12 ore, per sempre. Tale contratto è definito come proxy (EIP-1967) all’indirizzo:

`0x5fd95a5af4E60B9B796Cca6FEB44273359929ea8`

la cui implementazione risiede all’indirizzo:

`0x5De4D6Fe756A9A1b0FBb2C3404411230d53Aa689`

Ogni volta che un’asta viene finalizzata, la transazione di chiusura determinerà anche il conio di un nuovo $\textcircled{P}$ NOUN e l’inizio di una nuova asta di 12 ore. Il 100% dei proventi dell’asta in ETH viene depositato automaticamente nella tesoreria della Public Nouns DAO.

I parametri che definiscono le regole su cui si basano le aste (definiti nel contratto) sono raccolti nella tabella Tabella 3.51.

<i>Parametro</i>	<i>Valore</i>
duration	43.200s = 12 ore
minBidIncrementPercentage	2%
reservePrice	0.33 ETH

Tabella 3.51: Parametri regolamentanti le aste di Public Nouns

3.24.2 Processo di governance e analisi dei contratti

I possessori di $\textcircled{P}$ NOUN partecipano alla governance della DAO tramite cicli di proposta che attraversano varie fasi¹⁹².

- **Discussione su Discord** (off-chain): Dopo aver verificato il proprio Public Noun su Discord per accedere ai canali di discussione è possibile avviare una discussione per raccogliere sostegno e idee per migliorare la propria proposta.
- **Proposta sul Forum** (off-chain): Dopo la prima fase di discussione su Discord ne viene avviata un'altra per una durata di circa una settimana dopo la pubblicazione della proposta sul forum.
- **Proposta alla DAO** (on-chain): Una proposta che ha riscontrato abbastanza supporto per raggiungere il quorum, può essere presentata on-chain alla DAO.

Passiamo ora ad analizzare nel dettaglio i codici che definiscono i principali contratti di governance di Public Nouns DAO.

Governor I principali aspetti legati al processo di governance e quindi ai cicli di proposte e votazioni sono regolate dal contratto di governor che nel caso di Public Nouns è definito come un proxy (EIP-897 Delegate) con indirizzo:

0x2BbEbFECA0fEbde8C70EF8501C991f3AB2095862

¹⁹²<https://docs.publicnouns.wtf/governance/proposal-flow>

la cui implementazione invece risiede all'indirizzo:

0x65519993deD435233d8E9EdE178d5604De6c6eb2

Il governor di Public Nouns DAO nasce come fork di Compound ma con una variazione fondamentale legata al fatto l'offerta di $\textcircled{P}$ NOUN aumenta di 1 ogni giorno per sempre e quindi non si possono usare numeri fissi per i quorum ma Basis Points.

Timelock Il timelock di Public Nouns DAO nasce anch'esso come fork del famoso contratto Timelock di Compound Finance. L'indirizzo del contratto in questione è:

0x553826Cb0D0Ee63155920F42b4E60aaE6607DFCB

Tesoreria La tesoreria della DAO è individuata nel contratto di timelock il quale attualmente detiene un volume pari a 21.936\$¹⁹³.

I parametri fondamentali del processo di governance descritti nei contratti di Tabella 3.53 sono elencati nella Tabella 3.52.

<i>Parametro</i>	<i>Valore</i>
MIN_PRRPROPOSAL_THRESHOLD_BPS	0.01%
MAX_PRRPROPOSAL_THRESHOLD_BPS	10%
proposalThresholdBPS	1%
MIN_QUORUM_VOTES_BPS	2%
MAX_QUORUM_VOTES_BPS	20%
quorumVotesBPS	10%
MIN_VOTING_DELAY - MAX_VOTING_DELAY	1 - 40320 blocchi (15s) $\simeq$ 0 - 7 giorni
votingDelay	19938 blocchi (15s) $\simeq$ 3 giorni
MIN_VOTING_PERIOD - MAX_VOTING_PERIOD	5760 - 80640 blocchi (15s) = 1 - 14 giorni
votingPeriod	26585 blocchi (15s) $\simeq$ 4 giorni
MINIMUM_DELAY - MAXIMUM_DELAY	172800s - 2592000s = 2 - 30 gioni
delay	172800s = 2 giorni
GRACE_PERIOD	1209600s = 14 giorni

Tabella 3.52: Parametri principali del processo di governance di Public Nouns

¹⁹³09.02.2026,<https://www.tally.xyz/gov/public-nouns/treasury>

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
NounsToken	0x93ecac71499147627DFEc6d0E494d50fCFFf10EE	NFT
NounsDAOProxy	0x2BbEbFECA0fEbde8C70EF8501C991f3AB2095862	governor proxy
NounsDAOLogicV1	0x65519993deD435233d8E9EdE178d5604De6c6eb2	governor implem.
NounsDAOExecutor	0x553826Cb0D0Ee63155920F42b4E60aaE6607DFCB	timelock
NounsAuctionHouseProxy	0x5fd95a5af4E60B9B796Cca6FEB44273359929ea8	auction proxy
NounsAuctionHouse	0x5De4D6Fe756A9A1b0FBb2C3404411230d53Aa689	auction implem.

Tabella 3.53: Lista indirizzi principali che gestiscono Public Nouns DAO

3.25 Unlock

Unlock è un sistema peer-to-peer open source, di proprietà collettiva e governato dalla comunità, che crea membership basate sul tempo¹⁹⁴. Le diverse componenti interdipendenti che costituiscono Unlock sono:

- **Unlock Protocol:** Una suite di smart contract aggiornabili che creano membership sotto forma di NFT.
- **L'Ecosistema Unlock:** Una comunità di creatori, distributori e consumatori che condividono la proprietà di Unlock Protocol attraverso i loro contributi utilizzando il protocollo.
- **Unlock DAO:** Un'organizzazione decentralizzata di detentori di token che governano e controllano Unlock Protocol.
- **Unlock Protocol Foundation:** Una fondazione delle Isole Cayman il cui scopo è agire al servizio dell'ecosistema Unlock e della DAO.

¹⁹⁴<https://docs.unlock-protocol.com/getting-started/what-is-unlock/>

- **Unlock Tools:** Applicazioni front-end di utilità create originariamente da Unlock Labs per favorire l'innovazione sostenibile su Unlock Protocol, e ora mantenute dai membri dell'Ecosistema Unlock.



Figura 3.66: Unlock Logo

L'obiettivo primario di Unlock è:

Rendere Unlock la primitiva di membership predefinita per ogni singola membership.

I fondatori di Unlock ritengono che il protocollo stesso non debba essere immutabile ma debba essere in grado di evolversi e sostenere l'educazione, la promozione e il marketing¹⁹⁵.

3.25.1 Token UP o UDT

I diritti di voto della Unlock DAO sono rappresentati dagli Unlock Protocol Governance Token un token ERC-20 che a seconda della blockchain a cui ci si riferisce viene indicato con il simbolo UP oppure UDT. I token UDT sono stati inizialmente creati su Ethereum mentre il token UP è nato a luglio 2024, quando la Unlock DAO ha approvato una migrazione verso la rete Base. La migrazione da UDT a UP è consentita tramite uno scambio il cui rapporto è 1 a 1000 come risultato delle diverse forniture dei due token: UP ha una fornitura di 1.000.000.000 mentre UDT aveva una fornitura di 1.000.000¹⁹⁶.

¹⁹⁵<https://docs.unlock-protocol.com/governance/>

¹⁹⁶<https://docs.unlock-protocol.com/governance/unlock-dao-tokens>

Sulla rete Base troviamo il contratto proxy di UP (EIP-1967 Transparent) definito all'indirizzo:

`0xaC27fa800955849d6D17cC8952Ba9dD6EAA66187`

la cui implementazione ha indirizzo:

`0xF52ce8bc8B9a1EC76C2c46008216a357812da67D`

Su Ethereum invece è definito il proxy (EIP-1967 Transparent) di UDT all'indirizzo:

`0x90DE74265a416e1393A450752175AED98fe11517`

con corrispondente contratto di implementazione all'indirizzo:

`0xcB22BD8b943879e83193F479Ec4E3c98B610B507`

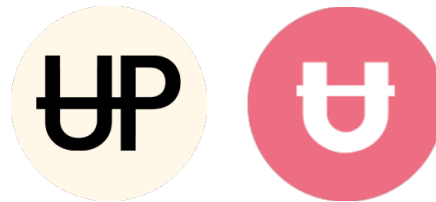


Figura 3.67: UP e UDT Token

L'offerta di UP in circolazione è di 279.008.436 UP¹⁹⁷.

3.25.2 Processo di governance e analisi dei contratti

La Unlock DAO prevede sia una fase di governance on-chain attraverso i contratti della DAO oppure tramite la piattaforma Tally¹⁹⁸, sia una fase off-chain tramite Snapshot¹⁹⁹ o altri canali di comunicazione ufficiali. Il processo di governance della DAO prevede in particolare di eseguire i seguenti passaggi per poter apportare qualche forma di modifica alla DAO tramite proposte ufficiali²⁰⁰.

¹⁹⁷09.02.2026,<https://www.coingecko.com/en/coins/unlockprotocoltoken>

¹⁹⁸<https://www.tally.xyz/gov/unlock-protocol>

¹⁹⁹<https://snapshot.box/#/s:unlock-dao.eth>

²⁰⁰<https://docs.unlock-protocol.com/governance/unlock-dao/>

Fase preparatoria off-chain Prima dell’invio ufficiale della proposta, è fondamentale la ricerca di feedback ed un’analisi del consenso della comunità. Questo può avvenire su Discord o in qualsiasi altro luogo dove ci si aspetta che i membri della comunità e i delegati possano fare domande e ottenere risposte.

Inoltre per effettuare una verifica tecnica si può inviare una Pull Request con i dettagli del codice che consente agli altri membri di testare il codice e verificare che faccia ciò che promette e utilizzare gli helper disponibili.

Fase di invio e votazione della proposta on-chain Dopo aver attraversato la fase di governance off-chain è possibile inviare la proposta on-chain. L’unica condizione richiesta è quella di avere delegati al proprio almeno 50.000 UP (`proposalThreshold`). Una volta che la proposta è stata pubblicata gli utenti a cui sono stati delegati token (da se stessi o da altri utenti) hanno diritto di voto. Il peso del voto di un utente dipende dal saldo dei token delegati al suo indirizzo al momento dell’invio della proposta.

I parametri chiave che consentono il funzionamento del processo di governance della DAO di Unlock dopo la transizione alla rete Base Tabella 3.54.

<i>Parametro</i>	<i>Valore rete Base</i>
<code>votingDelay</code>	345600s = 28.800 blocchi (12s) = 4 giorni
<code>votingPeriod</code>	518400s = 43.200 blocchi (12s) = 6 giorni
<code>proposalThreshold</code>	50.000 UP
$\text{quorum} = \frac{\text{quorumNumerator}}{\text{quorumDenominator}}$	0.3% della supply totale (3.000.000 UP)
<code>getMinDelay</code>	172800s = 2 giorni

Tabella 3.54: Parametri principali della governance di Unlock

Governor Il primo contratto di governor della DAO era definito all’indirizzo²⁰¹:

0x7757f7f21F5Fa9b1fd168642B79416051cd0BB94

Nel giugno 2023, è stato poi aggiornato in seguito ad una proposta della DAO che la

²⁰¹<https://basescan.org/>

comunità ha approvato. Questo aggiornamento è stato giustificato dal alcune vulnerabilità legate al precedente standard delle librerie di OpenZeppelin ed ha portato a definire il nuovo contratto di governor di tipo aggiornabile. Nello specifico il seguente contratto è stato definito come proxy (EIP-1967 Transparent) all'indirizzo:

0x440d9D4E66d39bb28FB58729Cb4D3ead2A595591

con implementazione definita all'indirizzo:

0x7E33dD3955b7B4a699CE75D507bfB2f044D5Df87

Nel settembre 2024 poi l'attuale contratto è stato istanziato come parte della migrazione a Base²⁰². L'indirizzo del proxy (EIP-1967 Transparent) è:

0x65bA0624403Fc5Ca2b20479e9F626eD4D78E0aD9

mentre la corrispondente implementazione è definita all'indirizzo:

0x6ac91d932B575E16c3d724Eb43FBc9CE7bF5F7f2

Tutti i contratti citati sono stati costruiti sulla base delle librerie OneZeppelin.

Timelock Il contratto di timelock originale (distribuito sulla rete Ethereum) è un contratto non aggiornabile il cui indirizzo è:

0x17EEDFb0a6E6e06E95B3A1F928dc4024240BC76B

Come per il governor anche il timelock è stato necessariamente sostituito da un nuovo contratto con la transizione a Base. L'innovazione principale apportata con l'aggiornamento è stata la scelta di rendere anche il timelock un contratto aggiornabile seguendo lo standard di OneZeppelin più recente. Il proxy (EIP-1967 Transparent) che lo definisce ha indirizzo è:

0xB34567C4cA697b39F72e1a8478f285329A98ed1b

e punta all'implementazione di indirizzo:

0x4473B159a3a7a14FC0F3F266a572d595B4906846

²⁰²<https://docs.unlock-protocol.com/governance/unlock-dao/>

Tesoreria La tesoreria di Unlock DAO è gestita dal contratto di timelock. Il volume attuale contenuto è pari a 101.483,85\$²⁰³.

L'indirizzo di tutti gli i contratti di governance nati con la transizione a Base e attualmente in uso sono riportati nella Tabella 3.55.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
Transparent UpgradeableProxy	0xaC27fa800955849d6D17cC8952Ba9dD6EAA66187	token proxy
UPToken	0xF52ce8bc8B9a1EC76C2c46008216a357812da67D	token implem
Transparent UpgradeableProxy	0x65bA0624403Fc5Ca2b20479e9F626eD4D78E0aD9	governor proxy
UPGovernor	0x6ac91d932B575E16c3d724Eb43FBc9CE7bF5F7f2	governor implem.
Transparent UpgradeableProxy	0xB34567C4cA697b39F72e1a8478f285329A98ed1b	timelock proxy
UPTimelock	0x4473B159a3a7a14FC0F3F266a572d595B4906846	timelock implem

Tabella 3.55: Lista indirizzi contratti di governance di Unlock DAO su Base

3.26 Hifi

Hifi è un protocollo di finanza decentralizzata che introduce prestiti a tasso fisso e a scadenza fissa su blockchain basate su Ethereum.



Figura 3.68: Hifi Finance Logo

La Hifi DAO è l'organizzazione che gestisce il protocollo di Hifi Finance. Essa ha

²⁰³09.02.2026,<https://www.tally.xyz/gov/unlock-protocol/treasury>

adottato una struttura legale ai sensi del Trustless Unincorporated Nonprofit Association Agreement (TUNAA). Questa struttura consente alla Hifi DAO di interagire con entità esterne e di rispettare efficacemente i requisiti legali e normativi. Il TUNAA, riconosciuto ai sensi del Delaware Uniform Unincorporated Nonprofit Association Act, stabilisce la Hifi DAO come associazione senza scopo di lucro, non intesa come partnership o società di investimento. Il TUNAA garantisce inoltre la responsabilità limitata per i membri e offre protezione per i loro asset²⁰⁴.

3.26.1 Token HIFI

HIFI è il token ERC-20 che consente al suo proprietario di assegnare, tramite delega, i diritti di voto a qualsiasi indirizzo, compreso il proprio. Le variazioni nel saldo dei token di un proprietario adeguano automaticamente i diritti di voto del delegato, garantendo un processo di governance dinamico, trasparente e reattivo per la DAO²⁰⁵.

Il contratto del token HIFI è definito all'indirizzo:

0x4b9278b94a1112cAD404048903b8d343a810B07e



Figura 3.69: HIFI Token

Da protocollo non è previsto un tetto massimo per l'offerta di HIFI che attualmente è pari 141.982.603,41 HIFI che risulta essere al momento interamente in circolazione²⁰⁶.

²⁰⁴<https://docs.hifi.finance/protocol/overview/hifi-dao>

²⁰⁵<https://docs.hifi.finance/protocol/technical-reference/governor-bravo/hifi>

²⁰⁶09.02.2026,<https://coinmarketcap.com/it/currencies/hifi-finance/>

3.26.2 Processo di governance e analisi dei contratti

Il protocollo di Hifi Finance è governato e aggiornato dalla sua community attraverso l'uso di tre componenti chiave: il token HIFI, il modulo di governance e il Timelock. Questi elementi agiscono in modo coeso per consentire alla community di proporre, votare e implementare modifiche al protocollo²⁰⁷.

Creazione e votazione della proposta Quando viene creata una proposta di governance, vengono registrati i pesi di voto e la fase di votazione inizia e dura cinque giorni. Affinché una proposta venga approvata, deve ricevere sia la maggioranza dei voti sia almeno il 2% dell'offerta di token HIFI espressi a suo favore.

Esecuzione Una volta approvata, la proposta viene messa in coda nel timelock e per poi essere eseguita dopo un periodo di attesa di due giorni.

I valori dei parametri che regolano tale processo di governance, tra cui quorum e il threshold citati sono raccolti nella Tabella 3.56.

<i>Parametro</i>	<i>Valore</i>
MIN_PROPOSAL_THRESHOLD	0.1% della supply totale
MAX_PROPOSAL_THRESHOLD	10% della supply totale
proposalThreshold	50.000 HIFI
quorumVotes	2% della supply totale
MIN_VOTING_DELAY - MAX_VOTING_DELAY	1 - 40320 blocchi (15s) = 0 - 7 giorni
votingDelay	13140 blocchi $\simeq$ 2 giorni
MIN_VOTING_PERIOD - MAX_VOTING_PERIOD	5760 - 80640 blocchi (15s) = 1 - 14 giorni
votingPeriod	36000 blocchi $\simeq$ 5 giorni
MINIMUM_DELAY - MAXIMUM_DELAY	172800s - 2592000s = 2 - 30 gioni
delay	172800s = 2 giorni
GRACE_PERIOD	1209600s = 14 giorni

Tabella 3.56: Parametri principali del processo di governance di Hifi Finance

²⁰⁷<https://docs.hifi.finance/protocol/technical-reference/governor-bravo/introduction>

Governor Il contratto di governor di Hifi deriva dalle fondamenta stabilite dal fork di Ampleforth della Governance di Compound²⁰⁸. Il contratto del proxy (EIP-897 Delegate) ha indirizzo:

0xef0A0421Ea43b602E5Be35e9018Dd3E34Bcee007

la sua implementazione è invece distribuita all'indirizzo:

0xdA161D0CFB4F836070e31fBf46Bd771FAE2F8E87

Timelock Il timelock di HIFI DAO ha indirizzo:

0xAC46Db50B44BBef8DC25f778359e1834248147F7

e segue lo standard originale di Compound Finance.

Tesoreria Non è stato possibile raccogliere informazioni relative alla tesoreria di Hifi nè da un punto di vista del meccanismo utilizzato nè in termini di volume totale.

Gli indirizzi di tali contratti sono raccolti nella Tabella 3.57.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
Hifi	0x4b9278b94a1112cAD404048903b8d343a810B07e	token
GovernorBravoDelegator	0xef0A0421Ea43b602E5Be35e9018Dd3E34Bcee007	governor proxy
GovernorBravoDelegate	0xdA161D0CFB4F836070e31fBf46Bd771FAE2F8E87	governor implem.
Timelock	0xAC46Db50B44BBef8DC25f778359e1834248147F7	timelock

Tabella 3.57: Lista indirizzi contratti di governance di Hifi Finance

3.27 Fluence

Fluence è una piattaforma di calcolo decentralizzato e cloudless costruita su un'infrastruttura di livello enterprise (per soddisfare le esigenze critiche delle grandi aziende), con una scalabilità e un'efficienza dei costi senza pari.²⁰⁹

²⁰⁸<https://docs.hifi.finance/protocol/overview/governance>

²⁰⁹<https://www.fluence.network/>

Il concetto di "cloudless" che contraddistingue il progetto di Fluence consiste nel fatto che a differenza dei cloud tradizionali, in cui i propri dati risiedono nei data center di un'unica entità che controlla tutto, Fluence crea un mercato aperto in cui chiunque può essere un provider, dai grandi data center professionali ai singoli utenti con potenti hardware. In questo modo se un provider alza i prezzi o ha problemi tecnici, ogni utente può spostare il proprio carico di lavoro su un altro provider della rete istantaneamente, senza dover riscrivere il codice (cosa molto difficile con AWS, Google Cloud o Azure)²¹⁰.



Figura 3.70: Fluence Network Logo

L'**Associazione Fluence** è dotata di tre organi costitutivi: la **DAO**, il **Comitato di Governance** e i membri dell'associazione stessa²¹¹. Le regole che definiscono le relazioni tra questi tre organi sono le seguenti:

- Per effettuare una modifica allo statuto dell'Associazione invece richiede l'approvazione di tutti e tre i gruppi.
- Qualsiasi possessore di FLT è un membro della DAO; la quale elegge i membri del Comitato di Governance ogni due anni tramite un voto on-chain e determina anche i criteri per diventare membri dell'associazione.
- Il Comitato di Governance è composto da un massimo di sette membri ed è a questo comitato che è attribuito il potere di veto sulle decisioni della DAO.

²¹⁰<https://fluence.dev/>

²¹¹<https://www.fluence.network/blog/the-fluence-dao-how-and-why/>

3.27.1 Token FLT

Il token di governance di Fluence DAO è il token ERC-20 FLT il cui contratto è un proxy (EIP-1967 Transparent Proxy) definito all'indirizzo:

0x236501327e701692a281934230AF0b6BE8Df3353

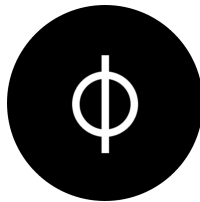


Figura 3.71: FLT Token

La rispettiva implementazione risiede invece all'indirizzo:

0xbDB50EFF425fb2B1B67fea21b8420eEB6D99CCCC0

Il protocollo prevede un hard cap di 1.000.000.000 FLT che sono stati distribuiti come segue²¹²:

- Offerta circolante iniziale: 50.000.000 FLT (5%)
- Anno 1: 50.000.000 FLT (5%) sono stati assegnati a un programma di ricompensa per sviluppatori iniziato il 27 febbraio 2024. I token sono bloccati per due mesi dalla data del riscatto e saranno rilasciati a partire dal 27 aprile 2024.
- ~ 45% dell'offerta totale di FLT assegnata al team e agli investitori è bloccata fino a febbraio 2025 e successivamente verrà sbloccata giornalmente fino a febbraio 2026.

L'offerta totale coincide con quella massima mentre l'offerta attualmente circolante è pari a 257.605.677,94 FLT²¹³.

²¹²<https://www.fluence.network/blog/fluence-tokenomics/>

²¹³09.02.2026,<https://coinmarketcap.com/currencies/fluence-network/>

3.27.2 Processo di governance e analisi dei contratti

Fluence rende possibile una nuova generazione di infrastrutture cloud di proprietà della comunità e da essa controllata²¹⁴. La DAO di Fluence è stata architettata per:

- Dare il controllo del voto alla DAO on-chain, sia per proposte dirette che per eleggere i membri del comitato di governance.
- Proteggere il progetto da voti dannosi e attacchi.
- Isolare i partecipanti della DAO dalla responsabilità legale.

Per raggiungere tali nostri obiettivi la DAO è stata strutturata come un'Associazione Svizzera, che fornisce un involucro legale protettivo²¹⁵.

Le Fluence Improvement Proposals (FLIP) sono documenti che descrivono gli standard per l'ecosistema Fluence e i processi attraverso i quali la comunità di Fluence introduce, migliora, raggiunge il consenso e implementa aggiornamenti su Fluence²¹⁶. Tali proposte possono essere utilizzate in particolare per:

- votare per la distribuzione della tesoreria della DAO verso attività di marketing, sviluppo o fornitura di liquidità.
- suggerire miglioramenti del protocollo, nuove funzionalità e partecipare all'ingegneria collettiva del token.”

Qualsiasi possessore di token sarà in grado di creare proposte, delegare e votare per le proposte. È richiesto l'1% dello stake per sottoporre una proposta al voto e l'approvazione di una proposta richiede la maggioranza dei voti espressi, con un minimo del 4% dell'offerta di token.

I parametri che regolano il processo di governance di Fluence DAO sono presentati nella Tabella 3.58.

²¹⁴<https://www.fluence.network/governance>

²¹⁵<https://www.fluence.network/blog/the-fluence-dao-how-and-why/>

²¹⁶<https://www.fluence.network/governance>

<i>Parametro</i>	<i>Valore</i>
proposalThreshold	10.000.000 FLT (1%)
$\text{quorum} = \frac{\text{quorumNumerator}}{\text{quorumDenominator}}$	4% della supply totale (40.000.000 FLT)
votingDelay	7200 blocchi (12s) = 1 giorno
votingPeriod	36000 blocchi (12s) = 5 giorni
detMinDelay	432000s = 5 giorni

Tabella 3.58: Parametri usati nel processo di governance di Fluence DAO

Tali parametri così come ogni altra funzione che consente il funzionamento automatizzato del processo sono definiti all'interno dei contratti di governor e timelock.

Governor Il governor di Fluence DAO è un proxy (EIP-1967 Transaparent) il cui indirizzo sulla rete Ethereum è:

0x674299Cc65CEFAac9057f7EB307f5f6bB861f8E0

la cui implementazione ha indirizzo:

0xfCF160acc5422d25a15abA6F3329Db588E6de28d

Tale contratto è costruito secondo un'implementazione modulare che segue lo standard OpenZeppelin Governor.

Timelock Il contratto di timelock è anch'esso definito tramite lo standard di Onezeppelin. Il proxy (EIP-1967 Transparent) ha indirizzo:

0xf5693Bbe961F166a2fE96094d25567f7517f27B7

e punta al contratto di implementazione di indirizzo:

0xD0229D0fD29898AAF11fEA34081eB6AF15145baC

Tesoreria La tesoreria di Fluence DAO è gestita da un differente contratto definito secondo lo standard GnosisSafe il cui proxy ha indirizzo:

0x7F629403fDCC02aD83aA5debd1D4B1548982afaC

mentre l'implementazione corrispondente ha indirizzo:

0xd9Db270c1B5E3Bd161E8c8503c55cEABeE709552

Il volume totale degli asset detenuti in tale tesoreria è pari a 3.926.174\$²¹⁷.

Gli indirizzi dei contratti che regolano il processo di governance sono tutti raccolti nella Tabella 3.59.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
ERC1967Proxy	0x236501327e701692a281934230AF0b6BE8Df3353	token proxy
FluenceToken	0xbDB50EFF425fb2B1B67fea21b8420eEB6D99CCC0	token implem
ERC1967Proxy	0x674299Cc65CEFAac9057f7EB307f5f6bB861f8E0	governor proxy
Governor	0xfCF160acc5422d25a15abA6F3329Db588E6de28d	governor implem.
ERC1967Proxy	0xf5693Bbe961F166a2fE96094d25567f7517f27B7	timelock proxy
Executor	0xD0229D0fD29898AAf11fEA34081eB6AF15145baC	timelock implem
GnosisSafeProxy	0x7F629403fDCC02ad83aA5debd1D4B1548982afaC	treasury proxy
GnosisSafe	0xd9Db270c1B5E3Bd161E8c8503c55cEABeE709552	treasury implem

Tabella 3.59: Lista indirizzi contratti di governance di Hifi Finance

3.28 Bitcoin

Bitcoin nasce nel 2009 guidato dalla missione di creare un mondo plasmato dal cambiamento positivo guidato dalla comunità dandole il potere di finanziare i propri bisogni condivisi. Nello specifico si occupa di creare tecnologie e opportunità che permettono alle comunità di costruire, finanziare e proteggere ciò che per loro conta²¹⁸. Per portare a termine la loro missione nel 2019 hanno lanciato il programma

²¹⁷09.02.2026,<https://debank.com/profile/0x7f629403fdcc02ad83aa5debd1d4b1548982afac>

²¹⁸<https://manual.gitcoin.co/introduction-and-overview/gitcoins-north-stars>

Gitcoin Grants con cui hanno incanalato oltre 59 milioni di dollari in beni pubblici.



Figura 3.72: Gitcoin Logo

Sebbene il primo e principale focus di Gitcoin sia risolvere il caso d'uso dei grant, hanno progettato uno stack di soluzioni modulari inteso per essere estensibile o ripetibile attraverso molti casi d'uso differenti²¹⁹. Lo stack consiste in tre livelli primari:

- **Livello Protocollo:** Allo Protocol (Capital Allocation Protocol) è progettato per essere un metodo di allocazione del capitale infinitamente flessibile ed estensibile, ma anche affidabile e preciso.
- **Livello Applicazione:** Grants Stack è una piattaforma no-code (una dApp) per gestire programmi di sovvenzione. L'app fornisce attualmente ai gestori dei grant la capacità di creare, gestire ed eseguire Quadratic Funding, Direct Grants e Retro PGF, con piani per estendersi a qualsiasi meccanismo di sovvenzione con forte domanda popolare.
- **Livello Programma:** Il programma Gitcoin Grants, è la parte più longeva e specifica di Gitcoin, esso è uno strumento potente per fare onboarding ed educare le comunità sul potere dei programmi di sovvenzione. Ha gestito 19 round di finanziamento fino ad oggi e distribuito oltre 59 milioni di dollari in finanziamenti all'ecosistema Ethereum.

²¹⁹<https://www.gitcoin.co/whitepaper/read>

3.28.1 Token GTC

Il token di governance di Gitcoin è il token ERC-20 con simbolo GTC, il cui indirizzo sulla rete Ethereum è:

0xDe30da39c46104798bB5aA3fe8B9e0e1F348163F

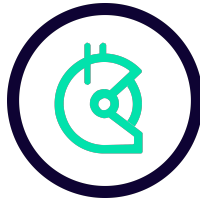


Figura 3.73: GTC Token

Tali token possono essere utilizzati all'interno dell'ecosistema di Gitcoin per due scopi principali²²⁰.

- **Governance:** Votare sui round di sovvenzioni (grant rounds), sulle allocazioni della tesoreria e sugli aggiornamenti del protocollo.
- **Staking:** Utilizzato da utenti web3 come prova della loro umanità (Proof of Humanity) su Gitcoin Passport.

La distribuzione dell'offerta totale di GTC che corrisponde a 100.000.000 GTC (87.491.501,9 GTC attualmente in circolazione²²¹) è articolata come segue²²²:

- Gitcoin DAO (50%): Per la governance della comunità, la gestione della tesoreria e la futura crescita dell'ecosistema.
- Stakeholder Esistenti (35%): Allocati al team iniziale, agli investitori e ai partner, soggetti a piani di vesting pluriennali.
- Airdrop Retroattivo (15%): Distribuito ai contributori e agli utenti passati della piattaforma Gitcoin.

²²⁰<https://www.gitcoin.co/gtc>

²²¹09.02.2026,<https://coinmarketcap.com/currencies/gitcoin/>

²²²<https://collectiveshift.io/gtc/>

3.28.2 Processo di governance e analisi dei contratti

La governance della DAO di Gitcoin è gestita da varie tipologie di utenti ognuna delle quali dotata di specifici poteri e caratteristiche²²³. Le principali tipologie sono:

- **Gitcoin Council:** Sono i decisori principali nel processo di governance di Gitcoin e si occupano sia di votare e approvare le proposte dei Community Round dei Gitcoin Grants, sia di ratificare la costituzione della DAO e di dirigere l'evoluzione della governance. I membri del consiglio sono tenuti a mantenere un tasso di partecipazione nelle votazioni del 90%.
- **Steward:** Sono i rappresentanti attivi della comunità che agiscono nell'interesse dei deleganti. Hanno poteri decisionali critici come il rilascio dei fondi della tesoreria o l'approvazione di modifiche alla governance. Gli Steward sono dunque tenuti a partecipare attivamente alle discussioni sul forum, commentare e votare le proposte off-chain.
- **Delegator:** Sono i detentori di token GTC che conferiscono il proprio "peso politico" agli Steward. Essi il compito si selezionare gli Steward più competenti e monitorare che agiscano nel loro interesse.

Il lavoro e la collaborazione di questi utenti consente il funzionamento del processo di governance di Gitcoin, il quale si compone di 3 fasi principali che prevedono una durata complessiva di minimo 21 giorni.

Discussione Le discussioni sulla governance avvengono sui forum ufficiali di Gitcoin²²⁴ e servono per richiedere/fornire feedback sulle nuove potenziali proposte. Le discussioni devono rimanere attive sul Forum di Governance per 5 giorni e avere un minimo di 5 commenti dagli Steward prima di poter passare alla fase successiva²²⁵.

²²³<https://manual.gitcoin.co/governance-roles>

²²⁴<https://gov.gitcoin.co/>

²²⁵<https://manual.gitcoin.co/governance-processes/discussions>

Votazione off-chain Dopo aver superato la fase di discussione una proposta può essere ufficialmente pubblicata e avviata alla fase di votazione off-chain sulla piattaforma Snapshot²²⁶. Solo chi detiene GTC o chi ne riceve in delega può votare. Vince l'opzione di maggioranza se superato un quorum attualmente fissato a 2,5 milioni di token. Le proposte devono rimanere attive per sette giorni per poter essere prese in considerazione per la ratifica onchain²²⁷.

Votazione on-chain Il voto on-chain si svolge su Tally²²⁸ e viene utilizzato per ratificare le decisioni prese off-chain durante le votazioni su Snapshot che richiedono il prelievo di fondi dalla Tesoreria di Gitcoin. Se non è necessario prelevare fondi, non c'è bisogno di passare su Tally²²⁹.

Governor Il **GitcoinGovernor** è costruito facendo uso delle librerie standard di OpenZeppelin ed è distribuito all'indirizzo:

0x9D4C63565D5618310271bF3F3c01b2954C1D1639

Timelock Il **Timelock** è invece una fork del timelock di Compound. Il suo indirizzo sulla rete Ethereum è:

0x57a8865cfB1eCEf7253c27da6B4BC3dAEE5Be518

Tesoreria La tesoreria della DAO di Gitcoin è gestita dal suo contratto di timelock. Il volume degli asset in esso detenuta è attualmente pari a 1.758.677\$²³⁰.

Le durate delle votazioni, così come il quorum minimo e gli altri parametri fondamentali definiti nel codice dei contratti di governance sono raccolti nella Tabella 3.60 mentre la lista degli indirizzi dei contratti principali è presentata nella Tabella 3.61

²²⁶<https://snapshot.org/#/gitcoindao.eth>

²²⁷<https://manual.gitcoin.co/governance-processes/voting/off-chain-voting>

²²⁸<https://www.tally.xyz/gov/gitcoin>

²²⁹<https://manual.gitcoin.co/governance-processes/voting/onchain-voting>

²³⁰09.02.2026, 0x57a8865cfB1eCEf7253c27da6B4BC3dAEE5Be518

<i>Parametro</i>	<i>Valore</i>
votingDelay	13140 blocchi (15s) $\simeq$ 2 giorni
votingPeriod	40320 blocchi (15s) = 7 giorni
proposalThreshold	150.000 GTC
quorum	2.500.000 GTC
MINIMUM_DELAY - MAXIMUM_DELAY	172800s - 2592000s = 2 - 30 giorni
delay	172800s = 2 giorni
GRACE_PERIOD	1209600s = 14 giorni

Tabella 3.60: Parametri usati nel processo di governance di Bitcoin

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
GTC	0xDe30da39c46104798bB5aA3fe8B9e0e1F348163F	token
BitcoinGovernor	0x9D4C63565D5618310271bF3F3c01b2954C1D1639	governor
Timelock	0x57a8865cfB1eCEf7253c27da6B4BC3dAEE5Be518	timelock

Tabella 3.61: Lista indirizzi contratti di governance di Bitcoin

3.29 GMX

GMX è un exchange decentralizzato spot e perpetual che supporta il trading di contratti perpetui con un basso impatto sul prezzo (price impact), una leva finanziaria fino a 100x e commissioni di swap contenute.



Figura 3.74: GMX Logo

L'attività di trading è sostenuta da pool di asset unici, le GM Pool, che permettono ai fornitori di liquidità di guadagnare commissioni derivanti dalle operazioni perpetual, dalle liquidazioni e dagli swap.

GMX esegue ogni ordine attingendo alle GM Pool e quota l'indice di prezzo dell'oracolo, anziché affidarsi a un order book o a market maker esterni. Per garantire un pricing accurato ed evitare picchi di prezzo anomali, GMX utilizza gli oracoli Chainlink Data Stream, assicurando così che le liquidazioni avvengano esclusivamente a prezzi di mercato equi.

3.29.1 Token GMX e GMX_DAO

GMX è il token (ERC-20) di utilità e governance della piattaforma. Il suo contratto è definito sulla rete Arbitrum all'indirizzo:

0xfc5A1A6EB076a2C7aD06eD22C90d7E710E35ad0a



Figura 3.75: GMX Token

L'offerta massima prevista è di 13,25 milioni di token GMX. Di questi 10.385.273,16 GMX rappresentano l'offerta totale che coincide con quella attualmente circolante²³¹. Il minting oltre l'offerta massima avverrà solo se vi sarà una necessità. Tale necessità dovrà essere votata e approvata dalla governance di GMX prima di essere permessa²³². L'allocazione dell'offerta totale è stata distribuita come segue:

- 6 milioni GMX: Migrazione XVIX e Gambit. GMX è nato da una fusione delle community XVIX e Gambit.
- 2 milioni GMX: Appaiati con ETH per la liquidità su Uniswap.
- 2 milioni GMX: Riservati per il vesting dei token Escrowed GMX.

²³¹09.02.2026,<https://coinmarketcap.com/currencies/gmx/>

²³²<https://docs.gmx.io/docs/tokenomics/gmx-token>

- 2 milioni GMX: Per la tesoreria.
- 1 milione GMX: Da utilizzare per incentivi all'integrazione e per gli sviluppatori della community.
- 250.000 GMX: Distribuiti ai contributori linearmente nel corso di 2 anni.

La gestione della GMX DAO però non è consentita direttamente dal token GMX ma dal token GMX.DAO il cui indirizzo è:

`0x2A29D3a792000750807cc401806d6fd539928481`

Con questi token, gli utenti possono partecipare alla governance votando direttamente le proposte (dopo aver autodelegato al proprio indirizzo i token) o eleggendo un delegato che voti per conto loro. Per ottenerli è necessario mettere in stake token GMX ottenendo in cambio GMX.DAO secondo un rapporto 1:1²³³.

3.29.2 Processo di governance e analisi dei contratti

Per presentare una proposta alla GMX DAO è necessario seguire un processo strutturato, descritto in seguito²³⁴:

Fase 1: Ideazione In questa fase iniziale, l'autore cerca il feedback della community sulle proprie idee sul forum di governance di GMX²³⁵. Le proposte durante tale fase sono tipicamente anche oggetto di brainstorming informale in contesti come chat Discord o gruppi Telegram.

Fase 2: Richiesta di Commento (RFC) Una proposta che riceve l'approvazione della community passa alla fase 2 in cui gli autori possono richiedere formalmente l'input della community modellando la loro idea in una Richiesta di Commento (RFC) integrando i feedback ottenuti nella fase 1. Lo stato di "Bozza RFC" mira ad accumulare feedback e approvazione sufficienti per stabilire un consenso informale,

²³³<https://docs.gmx.io/docs/governance/voting-power>

²³⁴<https://docs.gmx.io/docs/governance/proposal-process/>

²³⁵<https://gov.gmx.io/>

consentendo così la progressione verso una proposta formale con un rischio ridotto di rifiuto immediato.

Fase 3: Voto su Snapshot Nel caso in cui la proposta raggiunga il consenso informale nella fase 2 essa viene presentata ufficialmente su Snapshot²³⁶ a patto che il proponente disponga almeno di 10.000 GMX delegati.

Il potere di voto per Snapshot si basa sul saldo dei token, il che consente la copertura di una percentuale maggiore della community GMX. Il meccanismo di voto usato prevede una maggioranza semplice ed il raggiungimento di un quorum di 50.000 GMX. La durata della votazione su Snapshot è di 5 giorni.

Fase 4: Tally In caso di successo della votazione su Snapshot e qualora la proposta richieda l'invio di una transazione o qualche modifica che deve essere implementata on-chain viene avviata una votazione su Tally²³⁷. L'utente che avvia la votazione deve disporre di almeno 30.000 GMX. Il meccanismo di voto previsto per questa fase è la maggioranza qualificata, è quindi richiesto 65% + 1 unità più piccola di un token. E' inoltre richiesto il raggiungimento di un quorum di 213.900.000 GMX. La votazione dura 5 giorni preceduti da un ritardo di voto di 24h e seguiti da un ritardo di esecuzione di 24h.

I parametri che governano tale processo citati nelle varie fasi e definiti negli opportuni contratti sono riportati nella Tabella 3.62.

<i>Parametro</i>	<i>Valore</i>
votingDelay	86400s = 7200 blocchi (12s) = 1 giorno
votingPeriod	432000s = 36000 blocchi (12s) = 5 giorni
proposalThreshold	30.000 GMX
$\text{quorum} = \frac{\text{quorumNumerator}}{\text{quorumDenominator}}$	3% della supply totale
quorumVotes	213.899,31 GMX
getMinDelay	86400s = 1 giorno

Tabella 3.62: Parametri usati nel processo di governance di GMX

²³⁶<https://snapshot.org/#/gmx.eth/>

²³⁷<https://www.tally.xyz/gov/gmx>

Governor Il **ProtocolGovernor** è il cuore della governance di GMX DAO. Attraverso tale contratto gli utenti possono partecipare alla governance pubblicando proposte e votando quelle presenti. Il suo contratto ha indirizzo:

0x03e8f708e9C85EDCEaa6AD7Cd06824CeB82A7E68

ed è definito sfruttando le librerie standard di OneZeppelin.

Timelock Il timelock usato dalla DAO è **GovTimelockController**, il quale è definito all'indirizzo:

0x4bd1cdAab4254fC43ef6424653cA2375b4C94C0E

secondo lo standard definito dalle librerie di OneZeppelin.

Gli indirizzi dei contratti analizzati sono riportati in Tabella 3.63.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
GMX	0xfc5A1A6EB076a2C7aD06eD22C90d7E710E35ad0a	token
GovToken	0x2A29D3a792000750807cc401806d6fd539928481	token
ProtocolGovernor	0x03e8f708e9C85EDCEaa6AD7Cd06824CeB82A7E68	governor
GovTimelockController	0x4bd1cdAab4254fC43ef6424653cA2375b4C94C0E	timelock

Tabella 3.63: Lista indirizzi contratti di governance della GMX.DAO

Tesoreria La tesoreria di GMX accumula fondi dalle seguenti fonti²³⁸:

- Commissioni dalla liquidità GMX/ETH di proprietà del protocollo.
- Fondi ricevuti tramite Bond Protocol.
- 10% delle commissioni di GMX V2.

Essa è distribuita su contratti multipli definiti ai seguenti indirizzi:

- **GmxTimelock**: 0x68863dDE14303BcED249cA8ec6AF85d4694dea6A
- **GmxTimelock**: 0x0339740d92fb8BAf73bAB0E9eb9494bc0Df1CaFD

²³⁸<https://docs.gmx.io/docs/tokenomics/gmx-token/>

- **GovTimelockController:** 0x4bd1cdAab4254fC43ef6424653cA2375b4C94C0E

Il volume complessivo detenuto dalla tesoreria, facendo riferimento ai contratti citati sopra è pari a 22.259.325\$²³⁹.

3.30 Tornado Cash

Tornado Cash è un protocollo non custodiale e completamente decentralizzato che consente transazioni private nello spazio delle criptovalute. In quanto protocollo non custodiale, gli utenti mantengono la custodia delle proprie criptovalute mentre operano su Tornado.Cash. Ciò significa che a ogni deposito viene fornita loro la chiave privata che abilita l'accesso ai fondi depositati, conferendo agli utenti il controllo completo sui propri asset²⁴⁰.



Figura 3.76: Tornado Cash Logo

Fin dalla sua nascita nel 2019, Tornado Cash opera sulla blockchain di Ethereum. Da giugno 2021, oltre alla blockchain di Ethereum, gli smart contract di Tornado Cash sono stati distribuiti anche su altre side-chain e blockchain. Queste implementazioni

²³⁹09.02.2026, <https://debank.com/profile/0x68863dde14303bced249ca8ec6af85d4694dea6a>,
<https://debank.com/profile/0x0339740d92fb8baf73bab0e9eb9494bc0df1cafd>, <https://debank.com/profile/0x4bd1cdaab4254fc43ef6424653ca2375b4c94c0e>

²⁴⁰<https://github.com/tornadocash/docs>

hanno permesso allo strumento di supportare nuovi token o di beneficiare dei vantaggi dei Layer-2, come transazioni più veloci ed economiche.

Tipologie di Pool Nelle **pool tradizionali** di Tornado Cash a importo fisso quando un utente versa fondi in una pool, viene generata una nota privata. Questa nota privata funge da chiave privata per l'utente per accedere a quei fondi in seguito. Grazie a tale chiave gli è inoltre consentito di utilizzare un indirizzo diverso da quello usato per il versamento per recuperare i propri fondi.

Con la nascita di **Tornado Cash Nova** nel dicembre 2021 gli utenti possono beneficiare dell'uso di una pool a importo arbitrario e trasferimenti schermati. In questo caso i fondi sono collegati direttamente a un determinato wallet per cui non c'è nessuna chiave privata. Gli utenti possono accedere ai propri fondi collegandosi alla pool con l'indirizzo appropriato. La custodia si acquisisce depositando token nella pool o registrandosi nella pool e ricevendo trasferimenti schermati da un altro indirizzo.

Osservazione 3.14. *Tornado.Cash utilizza lo Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) per verificare e consentire le transazioni.*

La forza del protocollo di Tornado.Cash è direttamente collegata al numero dei suoi utenti e alla dimensione della sua pool²⁴¹.

3.30.1 Token TORN

TORN è un token compatibile con lo standard ERC-20 con una fornitura fissa che governa Tornado.Cash. Il contratto del token è definito all'indirizzo:

0x77777FeDdddFfC19Ff86DB637967013e6C6A116C

TORN non è uno strumento di raccolta fondi né un'opportunità di investimento. Rimarrà non trasferibile finché la community non deciderà che sbloccare i trasferimenti tramite un voto di governance che sia conforme a tutte le leggi applicabili²⁴².

²⁴¹<https://github.com/tornadocash/docs/blob/en/general/how-does-tornado-cash-work.md>

²⁴²<https://tornado-cash.medium.com/tornado-cash-governance-proposal-a55c5c7d0703>



Figura 3.77: TORN Token

La distribuzione iniziale di TORN è suddivisa come segue²⁴³:

- 5% (500.000 TORN): Airdrop ai primi utenti delle pool ETH di Tornado.Cash.
- 10% (1.000.000 TORN): Anonymity mining per le pool ETH di Tornado.Cash, distribuito linearmente nel corso di 1 anno.
- 55% (5.500.000 TORN): Tesoreria della DAO, sarà sbloccata linearmente nell'arco di 5 anni con un cliff (periodo di attesa iniziale) di 3 mesi.
- 30% (3.000.000 TORN): Sviluppatori fondatori e primi sostenitori, sarà sbloccato linearmente nell'arco di 3 anni con un cliff di 1 anno.

Attualmente l'offerta totale è pari a 9.999.997,24 TORN a cui è associata un'offerta circolante pari a 5.260.163,43 TORN²⁴⁴.

3.30.2 Processo di governance e analisi dei contratti

Per partecipare alla governance di Tornado.Cash, gli utenti devono prima bloccare i propri token TORN nel contratto di governance. Se un utente vota o crea una proposta, i token non possono essere sbloccati prima che termini il periodo di esecuzione della proposta (8,25 giorni dalla creazione della proposta). I token bloccati possono essere delegati a se stessi oppure ad un altro indirizzo.

Per creare una proposta, un utente deve possedere almeno 1.000 TORN. Una proposta avrà successo se riceve la maggioranza semplice dei voti e se è stato raggiunto il quorum di 25.000 TORN durante il periodo di votazione di 5 giorni. Dopo che

²⁴³<https://docs.tornado.cash/general/torn>

²⁴⁴09.02.2026,<https://coinmarketcap.com/currencies/torn/>

una proposta ha successo, è soggetta a un timelock di 2 giorni dopodichè qualsiasi utente è in grado di eseguire la proposta. Se però la proposta non viene eseguita per i 3 giorni successivi, viene considerata scaduta e non può più essere eseguita²⁴⁵. Il processo di votazione appena descritto può essere attuato utilizzando l'opportuna piattaforma di governance²⁴⁶.

Governor e timelock Il principale contratto di governance della DAO di Tornado.Cash è uno solo ovvero il contratto di governor il quale integra anche le funzionalità di timelock. Tale contratto è definito come proxy (EIP-1967 Transparent) con indirizzo ethereum è:

`0x5efda50f22d34F262c29268506C5Fa42cB56A1Ce`

L'implementazione a cui tale contratto punta ha subito diverse modifiche nel corso del tempo di conseguenza ne esistono varie versioni. La versione originale è stata registrata sulla blockchain all'indirizzo:

`0xffbaC21a641Dcfe4552920138D90F3638B3c9fba`

Il codice è modulare e utilizza le librerie di OpenZeppelin per consentire il funzionamento della governance. Nella versione successiva del contratto di implementazione di indirizzo:

`0xBa178126C28F50Ee60322a82f5EbCd6b3711e101`

le differenze fondamentali non risiedono nella logica economica o di voto. La modifica chiave del contratto consiste nell'introduzione di un controllo di integrità del codice che serve la correttezza del contenuto della votazione. Infine per quanto riguarda invece l'ultima ed attuale versione di indirizzo:

`0xbf46f2222c0712cAF2f13B8590732DbD964ce395`

la differenza sostanziale risiede interamente all'interno della funzione **state** (già presente nelle precedenti versioni) che si occupa di caratterizzare lo stato di una specifica proposta. Nello specifico è stato cambiato l'ordine di priorità con cui il contratto

²⁴⁵<https://docs.tornado.cash/general/governance>

²⁴⁶<https://tornadocash.eth.link/governance/>

verifica se una proposta è "Eseguita" (**Executed**) o "Sconfitta" (**Defeated**).

I valori dei parametri di interesse sono riportati nella Tabella 3.64.

<i>Parametro</i>	<i>Valore precedente</i>	<i>Valore attuale</i>
VOTING_DELAY	75s $\simeq$ 1 minuto	75s $\simeq$ 6 blocchi (12s) $\simeq$ 1 minuto
VOTING_PERIOD	259200s = 3 giorni	432000s = 36000 blocchi (12s) = 5 giorni
PROPOSAL_THRESHOLD	1.000 TORN	1.000 TORN
QUORUM_VOTES	25.000 TORN	100.000 TORN
CLOSING_PERIOD	3600s = 1 ora	3600s = 1 ora
VOTE_EXTEND_TIME	21600s = 6 ore	21600s = 6 ore
EXECUTION_DELAY	172800s = 2 giorni	172800s = 2 giorni
EXECUTION_EXPIRATION	259200s = 3 giorni	259200s = 3 giorni

Tabella 3.64: Parametri usati nel processo di governance di Tornado.Cash

Tesoreria La tesoreria della DAO è gestita congiuntamente dal governor (fonte principale) e dal contratto **TornadoVault** definito all'indirizzo:

0x2F50508a8a3D323B91336FA3eA6ae50E55f32185

Il volume complessivo detenuto è attualmente pari a 60.203.020\$²⁴⁷.

Concludiamo ora l'analisi di Tornado Cash riportando nella Tabella 3.65 l'elenco dei principali contratti coinvolti nel processo di governance attuale della DAO.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
TORN	0x77777FeDdddFfC19Ff86DB637967013e6C6A116C	token
LoopbackProxy	0x5efda50f22d34F262c29268506C5Fa42cB56A1Ce	governor proxy
GovernanceProposal-StateUpgrade	0xbf46f2222c0712cAF2f13B8590732DbD964ce395	governor implem
TornadoVault	0x2F50508a8a3D323B91336FA3eA6ae50E55f32185	treasury

Tabella 3.65: Indirizzi degli attuali contratti di governance di Tornado.Cash

²⁴⁷09.02.2026, <https://debank.com/profile/0x2f50508a8a3d323b91336fa3ea6ae50e55f32185>,
<https://debank.com/profile/0x5efda50f22d34f262c29268506c5fa42cb56a1ce>

3.31 KyberSwap

Kyber Network sta costruendo un mondo in cui chiunque può scambiare i propri fondi liberamente, in modo affidabile e senza sforzo, alle proprie condizioni.



Figura 3.78: Kyber Network Logo

KyberSwap può essere definito come una suite completa di soluzioni per la finanza decentralizzata il cui centro è rappresentato dal **KyberSwap Aggregatore** che agisce come un potente motore di routing intelligente: scansiona l'intero mercato DeFi per trovare i percorsi di scambio più efficienti tra diverse piattaforme. Gli elementi e gli strumenti che contribuiscono a definire KyberSwap sono:

- **KyberSwap Interface:** L'applicazione web (dApp) offre un accesso comodo e aperto ad alcune delle migliori esperienze nella DeFi, inclusa la possibilità di sfruttare l'Aggregatore di KyberSwap per scambiare ai tassi migliori.
- **KyberSwap Widget:** Integra tassi superiori direttamente nella tua app con poche righe di codice (modalità plug-and-play). Il nostro widget personalizzabile consente agli integratori di fondere senza problemi i tassi migliori nelle loro dApp, con percorsi di trading, commissioni e temi configurabili.
- **KyberSwap Zap as a Service (ZaaS):** Introduzione dell'API Zap as a Service (ZaaS), che semplifica la fornitura di liquidità decentralizzata. Permette di aggiungere liquidità senza sforzo con un singolo token per un maggiore coinvolgimento nella DeFi, potenziato dall'Aggregatore DEX di KyberSwap per minimizzare l'impatto sul prezzo.

Infine, l'ecosistema comprendeva storicamente dei protocolli di liquidità proprietari come **KyberSwap Classic** ed **KyberSwap Elastic** (ora deprecati). A differenza dell'Aggregatore, questi erano sistemi di smart contract destinati alla gestione diretta dei fondi e delle pool di liquidità, rappresentando il "vecchio motore" di rendimento che è stato separato dalle attuali funzioni di scambio e aggregazione²⁴⁸.

3.31.1 Token KNC

Il Kyber Network Crystal token, o KNC in breve, è un token di utilità e governance ERC-20 che funge da fondamenta dell'ecosistema KyberSwap. Il contratto del token è registrato come proxy (EIP-1967 Transparent), il cui indirizzo è:

`0xdeFA4e8a7bcBA345F687a2f1456F5Edd9CE97202`

con corrispondente implementazione definita all'indirizzo:

`0xe5E8E834086F1a964f9A089eB6Ae11796862e4CE`

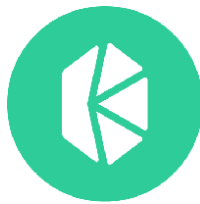


Figura 3.79: KNC Token

KNC è dinamico e può essere aggiornato o coniato dalla KyberDAO per supportare meglio la liquidità e la crescita. Detenere KNC significa avere una quota in tutte le importanti innovazioni e protocolli di liquidità creati per la DeFi. Tramite lo staking e il voto con KNC, gli utenti possono partecipare al processo di governance della KyberDAO e plasmare il futuro dell'ecosistema KyberSwap. In cambio della protezione del network Kyber, gli staker di KNC ottengono anche accesso a una serie di altri vantaggi, come rimborsi sulle spese del gas (gas refunds) o la distribuzione delle commissioni di trading del protocollo²⁴⁹.

²⁴⁸<https://docs.kyberswap.com/>

²⁴⁹<https://docs.kyberswap.com/governance/knc-token>

A settembre 2017 sono stati conati e distribuiti 226.000.000 KNC come segue:

- Investitori della comunità e partecipanti: 61,06% (137.995.600 KNC)
- Riserve operative dell'azienda: 19,47% (44.002.200 KNC)
- Fondatori, consulenti, primi investitori (vesting di 2 anni, lock-up di 1 anno): 19,47% (44.002.200 KNC)

Oggi l'offerta totale è pari a 240.892.876,38 KNC di cui 190.847.220,83 KNC in circolazione²⁵⁰.

3.31.2 Processo di governance e analisi dei contratti

Per partecipare alla KyberDAO è necessario disporre di un portafoglio Ethereum e di token KNC, dopodiché è sufficiente seguire i seguenti passi²⁵¹:

1. accedere alla piattaforma di governance²⁵²;
2. collegare il proprio wallet;
3. mettere in staking token KNC per ottenere potere di voto (oppure delega tale potere ad un altro utente);
4. attendi una nuova epoca di voto;
5. partecipa alle votazioni;
6. richiedi le tue ricompense nell'epoca successiva.

Osservazione 3.15. *Il potere di voto è determinato dalla quantità di KNC messi in staking, in proporzione alla quantità totale di KNC messa in staking nella KyberDAO e utilizzata per votare sulle proposte²⁵³.*

²⁵⁰09.02.2026,<https://coinmarketcap.com/currencies/kyber-network-crystal-v2/>

²⁵¹<https://docs.kyberswap.com/governance/kyberdao/user-guides/participating-in-kyberdao>

²⁵²<https://kyberswap.com/kyberdao/stake-knc>

²⁵³<https://docs.kyberswap.com/governance/kyberdao/user-guides/voting>

Governor Il cuore della governance di KyberDAO è rappresentato dal contratto di governance definito all'indirizzo:

0x7Ec8FcC26bE7e9E85B57E73083E5Fe0550d8A7fE

Tale contratto è costruito in maniera modulare senza però utilizzare come centro del codice le librerie OneZeppelin. Al fianco di **KyberGovernance** troviamo un altro contratto che si occupa di determinare chi ha diritto di voto e quanto pesa quel voto basandosi sui dati provenienti dal contratto di Staking. Il suo indirizzo è:

0xfbd73581af42b26295CF4B88B74A5AF71F209F8b

Tale contratto serve a collegare il sistema di Governance con il sistema di Staking.

Timelock/Executor I contratti responsabili dell'esecuzione on-chain delle decisioni prese sono gli executors. Esistono due tipologie di contratti di esecuzione: il **Long Executor**, di cui esistono due versioni, la prima (deprecata), ha indirizzo:

0x6758A66cD25fef7767A44895041678Fc4Ae9AfD0

la seconda, che presenta solo piccole differenze nei parametri, ha indirizzo:

0x7d4d05B1a1E5775a9C6ca248ABBE629B52C1D9D9

e lo **Short Executor** il cui indirizzo è:

0x41f5D722e6471c338392884088bD03340f50b3b5

Tesoreria La tesoreria di KyberDAO è principalmente identificata da due contratti, il primo, nonchè contribuente principale è un contratto che implementa un sistema multisig 5/9 ed è definito all'indirizzo:

0x91c9D4373B077eF8082F468C7c97f2c499e36F5b

Il secondo, **TreasuryPool**, è invece distribuito all'indirizzo:

0x0E590bB5F02A0c3888bFFb45DeE050b8fB60Bda

Il volume complessivo detenuto in tali contratti è attualmente pari a 364.902\$²⁵⁴.

²⁵⁴09.02.2026,<https://debank.com/profile/0x0e590bb5f02a0c3888bffb45dee050b8fb60bda>,<https://debank.com/profile/0x91c9d4373b077ef8082f468c7c97f2c499e36f5b>

I parametri legati al processo di governance sono definiti in Tabella 3.66 mentre in Tabella 3.67 sono raccolti tutti gli indirizzi dei contratti di governance analizzati.

<i>Parametro</i>	<i>Short Executor</i>	<i>Long Executor</i>
MAX_PROPOSAL_PER_EPOCH	10	10
getDelay	43200s = 12 ore	604800s = 7 giorni
MAXIMUM_DELAY	86400s = 1 giorno	1209600s = 14 giorni
MINIMUM_DELAY	3600s = 1 ora	86400s = 1 giorno
MIN_VOTING_DURATION	345600s = 4 giorni	604800s = 7 giorni
GRACE_PERIOD	345600s = 4 giorni	604800s = 7 giorni
MINIMUM_QUORUM	4% supply totale	15% → 20% (v2) supply totale
VOTE_DIFFERENTIAL	4% → 15% (v2)	0.01%

Tabella 3.66: Parametri usati per l'esecuzione delle proposte di KyberDAO

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
AdminUpgradeability Proxy	0xdeFA4e8a7bcBA345F687a2f1456F5Edd9CE97202	token proxy
KyberNetwork TokenV2	0xe5E8E834086F1a964f9A089eB6Ae11796862e4CE	token implem
KyberGovernance	0x7Ec8FcC26bE7e9E85B57E73083E5Fe0550d8A7fE	governance
EpochVotingPower Strategy	0xfbd73581af42b26295CF4B88B74A5AF71F209F8b	voting strategy
DefaultExecutor	0x41f5D722e6471c338392884088bD03340f50b3b5	short executor
DefaultExecutor	0x7d4d05B1a1E5775a9C6ca248ABBE629B52C1D9D9	long executor
MultiSigWallet WithDailyLimit	0x91c9D4373B077eF8082F468C7c97f2c499e36F5b	treasury multisig
TreasuryPool	0x0E590bB5F02A0c38888bFFb45DeE050b8fB60Bda	treasury

Tabella 3.67: Indirizzi degli attuali contratti di governance di KyberDAO

Osservazione 3.16. Nella tabella comparativa finale faremo riferimento ai valori legati allo short executor poichè caratterizzano il maggior numero delle proposte.

3.32 Audius

Originariamente introdotto nel Whitepaper [29] di Audius del 2020, l'Open Audio Protocol segna il capitolo successivo per un ecosistema musicale. Il protocollo combina blockchain, criptoeconomia e standard tecnologici dell'industria musicale per fornire nuovi strumenti di distribuzione, accesso e libertà di interazione diretta con i fan²⁵⁵. La missione del progetto Audius è dare a tutti la libertà di distribuire, monetizzare e trasmettere in streaming qualsiasi contenuto audio.



Figura 3.80: Audius Logo

Il protocollo unisce artisti, operatori di nodi e fan in modo che i loro incentivi siano allineati, permettendo a questi attori di fornire collettivamente un'esperienza di streaming audio di alta qualità, guidati dalle seguenti convinzioni fondamentali:

- Gli utenti dovrebbero essere compensati in proporzione a quanto valore creano per la rete.
- Gli artisti dovrebbero interagire e transare direttamente con i loro fan.
- Il potere di Governance dovrebbe essere guadagnato creando valore in Audius e condiviso costantemente tra i gruppi di utenti che contribuiscono al protocollo.
- Prezzi e guadagni per i partecipanti dovrebbero essere coerenti e trasparenti.
- L'accesso dovrebbe essere democratizzato; chiunque può contribuire ad Audius se segue le regole del protocollo, e tutte le informazioni sono accessibili pubblicamente.

²⁵⁵<https://docs.openaudio.org/>

- Gli intermediari dovrebbero essere rimossi ove possibile; quando necessari, dovrebbero essere algoritmici, trasparenti e verificabili.

Il protocollo Audius permette di fornire collettivamente un'esperienza di streaming musicale di alta qualità per l'utente finale senza un'infrastruttura centralizzata.

3.32.1 Token AUDIO

Il token di governance della DAO di Audius è il token ERC-20 AUDIO il quale è l'unità fondamentale di criptovaluta che alimenta le Artist Coin, le ricompense, lo staking, la governance e tutte le funzionalità derivate dell'Open Audio Protocol.



Figura 3.81: Token AUDIO

Il contratto del token è definito come proxy (EIP-1967) all'indirizzo:

```
0x18aAA7115705e8be94bfFEBDE57Af9BFc265B998
```

Il contratto di implementazione associato era inizialmente definito all'indirizzo:

```
0x22A9CCfdd10382D9cD18cA4437ff375bd7A87BBd
```

oggi però il proxy punta al contratto di implementazione aggiornato con indirizzo:

```
0x930C746a6e92ca8122682DF48CD5020bC1771b32
```

Attraverso la sua esistenza, AUDIO offre un modo agli attori indipendenti in una comunità distribuita di agire con incentivi allineati per difendere il catalogo aperto di musica che esiste nel database musicale globale. Insieme, i detentori e gli utenti di AUDIO alimentano un database musicale interamente ospitato dalla comunità. Chi possiede AUDIO possiede il protocollo.

Mettere in staking AUDIO conferisce agli utenti un peso di governance per influenzare il futuro del protocollo, dove ogni token in staking equivale a un voto. Gli AUDIO in staking generano inoltre un'emissione continua attraverso le ricompense previste con un tasso del 7% annuo che viene distribuito su base settimanale agli staker della rete, ma sono anche esposti a rischi di penalità tramite un meccanismo di slashing automatizzato²⁵⁶.

Lo staking di token AUDIO è consentito attraverso l'apposito contratto definito come proxy (EIP-1967) il cui indirizzo è:

`0xe6D97B2099F142513be7A2a068bE040656Ae4591`

l'implementazione corrispondente inizialmente è stata registrata all'indirizzo:

`0xEA10Fd3536FcE6A5d40d55c790b96df33B26702f`

la quale è stata poi sostituita ed è oggi registrata all'indirizzo:

`0xf26919F9b1CFF09c77E9300E971F6d2fEf761C33`

Il token è stato lanciato il 22 ottobre 2020 con una fornitura iniziale fissa di 1.000.000.000 AUDIO, ma ad oggi non è previsto un tetto massimo per il conio di token. L'offerta totale attuale coincide con quella circolante ed è pari a 1.394.975.804 AUDIO²⁵⁷.

3.32.2 Processo di governance e analisi dei contratti

La Governance è il processo attraverso il quale i detentori di token AUDIO attuano cambiamenti all'Open Audio Protocol tramite proposte on-chain. Tale processo prevede il susseguirsi di 6 distinte fasi: Post sul Forum → Proposta → Discussione → Votazione → Cooldown → Esecuzione.

Ogni proposta prevede un periodo di votazione di 72 ore alla fine del quale la proposta rimane inattiva per 24 ore prima di poter essere eseguita. Una volta terminato il cooldown di 24 ore, chiunque può eseguire la proposta.

²⁵⁶<https://docs.openaudio.org/concepts/audio/>

²⁵⁷10.02.2026,<https://coinmarketcap.com/currencies/audius/>

Il quorum di votazione è il 5%²⁵⁸ del totale di AUDIO in staking sulla rete, e le proposte passano con una maggioranza del 50%²⁵⁹.

Governor e timelock Il processo di governance è regolato dall'omonimo smart contract, il quale è un proxy (EIP-1967 Transparent) definito all'indirizzo:

0x4DEcA517D6817B6510798b7328F2314d3003AbAC

il cui contratto di implementazione associato fu originariamente definito all'indirizzo:

0x35dD16dFA4ea1522c29DdD087E8F076Cad0AE5E8

per poi essere sostituito da una nuova versione concettualmente e strutturalmente analoga il cui indirizzo è invece:

0x1c91aF03A390b4c619B444425b3119e553B5B44b

Gli scopi principali del contratto sono:

- **Gestione delle Proposte:** Permettere possessori di token AUDIO di proporre modifiche al protocollo. Le modifiche possono essere aggiornamenti del codice, cambiamenti dei parametri economici o nuove funzionalità.
- **Votazione Ponderata:** Gestire un sistema di voto in cui il peso del voto di un utente è proporzionale alla quantità di token che ha in staking (direttamente o tramite delega).
- **Esecuzione Automatica:** Se una proposta passa, il contratto esegue automaticamente la proposta. Non è quindi presente un contratto di timelock separato, il ruolo di timelock e tesoreria è gestito dal governor stesso.
- **Sicurezza:** Include un ruolo speciale chiamato "Guardian" che può porre il veto su proposte malevole o eseguire azioni di emergenza.

Nella tabella Tabella 3.68 sono riportati i valori esatti dei parametri di governance, così come sono stati implementati nel contratto di governance.

²⁵⁸Il valore specifico riportato in tabella è stato calcolato sulla base del valore del giorno 10.02.2026, <https://debank.com/profile/0xe6d97b2099f142513be7a2a068be040656ae4591>

²⁵⁹<https://docs.openaudio.org/concepts/governance>

<i>Parametro</i>	<i>Valore</i>
getVotingPeriod	21510 blocchi ($\sim 12s$) = 3 giorni
getVotingQuorumPercent	5% dello staking = 306.419 AUDIO
getExecutionDelay	7170 blocchi ($\sim 12s$) = 1 giorno
getMaxInProgressProposals	100

Tabella 3.68: Parametri usati nel processo di governance di Audius

Tesoreria Come anticipato il contratto che gestisce e detiene la tesoreria di Audius è il contratto di governance precedentemente analizzato. Il volume detenuto in tale contratto è pari a 4.619\$²⁶⁰. Il valore sia basso non implica un'inattività della DAO ma è invece una conseguenza di un attacco che il contratto ha subito nel luglio 2022, durante il quale l'hacker è riuscito a svuotare quasi interamente la "Community Treasury" portando via 18,5 milioni di token. La DAO invece di rifinanziare massicciamente quell'indirizzo specifico, ha deciso di mantenere il controllo dei fondi principali con altri strumenti che non vengono considerati nel calcolo della tesoreria.

Concludiamo dunque l'analisi di Audius raccogliendo gli indirizzi dei contratti principali usati attualmente per gestire il processo di governance Tabella 3.69.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
AudiusAdmin UpgradeabilityProxy	0x18aAA7115705e8be94bfFEBDE57Af9BFc265B998	token proxy
AudiusToken	0x930C746a6e92ca8122682DF48CD5020bC1771b32	token implem
AudiusAdmin UpgradeabilityProxy	0x4DEcA517D6817B6510798b7328F2314d3003AbAC	governance proxy
Governance	0x1c91aF03A390b4c619B444425b3119e553B5B44b	governance implem
AudiusAdmin UpgradeabilityProxy	0xe6D97B2099F142513be7A2a068bE040656Ae4591	staking proxy
Staking	0xf26919F9b1CFF09c77E9300E971F6d2fEf761C33	staking

Tabella 3.69: Indirizzi degli attuali contratti di governance di Audius

²⁶⁰10.02.2026,<https://debank.com/profile/0x4deca517d6817b6510798b7328f2314d3003abac>

3.33 Ampleforth

Il protocollo Ampleforth è definito da un insieme di istruzioni sulla blockchain di Ethereum che produce un'unità di conto decentralizzata chiamata AMPL. Il token AMPL è il componente primario dell'Ecosistema di Finanza Elastica di Ampleforth. Viene utilizzato per prestiti e crediti, per la creazione di derivati e come garanzia collaterale per una stablecoin decentralizzata.

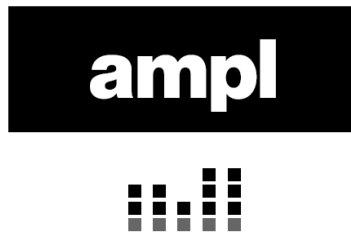


Figura 3.82: Ampleforth Logo

La Forth DAO è un'organizzazione autonoma decentralizzata dedicata esclusivamente alla crescita e all'adozione di AMPL. Può perseguire tale obiettivo attraverso iniziative come la liquidità di proprietà del protocollo (protocol owned liquidity), lo sviluppo dell'ecosistema, il marketing e altre attività al servizio del fine principale. Anche se AMPL è il token primario dell'organizzazione a gestire la DAO e come amministrare i fondi sono i detentori del token di governance FORTH.²⁶¹

3.33.1 Token AMPL e FORTH

AMPL Il token ERC-20 che funge da unità di conto. Il prezzo di AMPL ha come obiettivo il valore del dollaro USA del 2019 corretto per l'IPC (Indice dei Prezzi al Consumo), ma il numero di token AMPL nei portafogli degli utenti aumenta o diminuisce secondo una politica di **Offerta Elastica** che prevede:

²⁶¹<https://docs.ampleforth.org/learn/about-forth-dao>

- **Espansione:** Quando il tasso di cambio di AMPL è > 1 USD (2019), c'è più domanda che offerta. In risposta, il protocollo Ampleforth aumenta automaticamente e proporzionalmente la quantità di token nei portafogli degli utenti, portando gradualmente il prezzo verso il basso fino al suo obiettivo.
- **Contrazione:** Quando il tasso di cambio di AMPL è < 1 USD (2019), c'è più offerta che domanda. In risposta, il protocollo Ampleforth diminuisce automaticamente e proporzionalmente la quantità di token nei portafogli degli utenti, incrementandone il prezzo quanto necessario.

AMPL devierà dal suo obiettivo a seconda del mercato, ma il prezzo per singolo AMPL ritornerà sempre, al suo obiettivo di lungo periodo.

Il contratto Ethereum a cui è definito il token AMPL è un proxy che ha indirizzo:

0xD46bA6D942050d489DBd938a2C909A5d5039A161

la cui implementazione risiede all'indirizzo:

0xD0e3F82ab04B983C05263cF3BF52481FbAa435b1



Figura 3.83: Token AMPL

FORTH Il secondo token è quello di governance dell'ecosistema Ampleforth. FORTH è un token ERC-20 utilizzato per governare le modifiche ai parametri del protocollo, dirigere le emissioni di liquidity mining e indirizzare l'uso degli asset della tesoreria della DAO dedicati a stimolare le innovazioni nella finanza elastica.

Il contratto che definisce tale token è distribuito all'indirizzo:

0x77FbA179C79De5B7653F68b5039Af940AdA60ce0

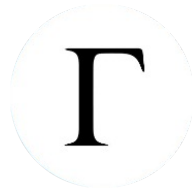


Figura 3.84: Token FORTH

L'offerta totale del token FORTH è al momento pari a 15.297.897,14 FORTH di cui 14.343.554,15 FORTH sono in circolazione²⁶².

3.33.2 Processo di governance e analisi dei contratti

Il protocollo Ampleforth è governato attraverso una serie di passaggi sequenziali dai detentori del token FORTH, ognuno dei quali rappresenta livelli crescenti di consenso da parte della community. La progressione verso un consenso sempre più vincolante è illustrata di seguito²⁶³.

- **Discussione:** Le discussioni di più alto livello possono far emergere idee in molti luoghi, inclusi il canale governance su Discord, il Governance Forum, i social media o le DAO della community. Quando sembra esserci un supporto sufficiente, un promotore può formalizzare l'idea inviando una Ampleforth Improvement Proposal (AIP) o una Configuration Change Proposal (ACCP).
- **Proposte (AIP/ACCP):** Le AIP e le ACCP²⁶⁴ sono documenti formali che descrivono la modifica proposta sul protocollo.
- **Discussione mirata:** Ogni proposta ha un argomento dedicato nel forum²⁶⁵ dove ha luogo una discussione orientata al risultato. L'obiettivo di questa fase è finalizzare eventuali questioni irrisolte e formalizzare il consenso off-chain.
- **Segnalazione off-chain:** Se la fase precedente non ha portato a un consenso evidente, il sentimento può essere raccolto in modo non vincolante tramite

²⁶²10.02.2026, <https://coinmarketcap.com/currencies/ampleforth-governance-token/>

²⁶³<https://docs.ampleforth.org/learn/about-forth-governance>

²⁶⁴<https://aips.ampleforth.org/>

²⁶⁵<https://forum.ampleforth.org/>

segnalazione off-chain su Snapshot²⁶⁶ da parte dei detentori di token. Sviluppo Tecnico I requisiti vengono implementati nel codice, lanciati su testnet e sottoposti a audit di sicurezza.

- **Voto Vincolante/Deployment:** Il passaggio finale è un voto vincolante che avviene on-chain. Il voto on-chain è "vincolante" perché il suo successo comporta l'esecuzione del codice, senza intermediari. I membri della community possono votare direttamente con i loro token FORTH o delegare a un altro indirizzo che può votare per loro conto. Puoi visualizzare le proposte, delegare e votare sulla dashboard di Tally²⁶⁷.

Governor Il contratto centale usato da Ampleforth per gestire il processo di governance della DAO è definito dal proxy (EIP-897 DelegateProxy) **GovernorBravoDelegator** con indirizzo Ethereum:

0x8a994C6F55Be1fD2B4d0dc3B8f8F7D4E3a2dA8F1

la cui implementazione, **GovernorBravoDelegate** è invece registrata con indirizzo:

0x444133fe9488cbec995Fd28601B3B1aD01b7fb9c

Tali contratti sono definiti sulla base di uno standard di governance originato da Compound Finance che permette ai possessori di token di proporre modifiche, votare e, se la votazione ha successo, eseguire automaticamente il codice sulla blockchain.

Timelock L'esecuzione però non avviene immediatamente ed è regolata da un contratto separato, il **Timelock**, il quale si occupa di imporre un ritardo tra l'approvazione di una proposta e la sua effettiva esecuzione. L'indirizzo di tale contratto sulla rete Ethereum è:

0x223592a191ECfC7FDC38a9256c3BD96E771539A9

Nella Tabella 3.70 sono raccolti tutti i parametri chiave del processo di governance con i corrispondenti valori.

²⁶⁶<https://snapshot.box/#/s:ampleforthorg.eth>

²⁶⁷<https://www.tally.xyz/gov/ampleforth>

<i>Parametro</i>	<i>Valore</i>
proposalMaxOperations	10
MIN_PROPOSAL_THRESHOLD/MAX_PROPOSAL_THRESHOLD	75.000/300.000 FORTH
proposalThreshold	75.000 FORTH
quorumVotes	600.000 FORTH
MIN_VOTING_DELAY/MAX_VOTING_DELAY	1/40320 blocchi = 12s/7 giorni
votingDelay	13140 blocchi = 2 giorni
MIN_VOTING_PERIOD/MAX_VOTING_PERIOD	5760/80640 blocchi = 1/14 giorni
votingPeriod	19710 blocchi = 3 giorni
MINIMUM_DELAY/MAXIMUM_DELAY	172800s/2592000s = 2/30 giorni
delay	172800s = 2 giorni
GRACE_PERIOD	1209600s = 14 giorni

Tabella 3.70: Parametri usati nel processo di governance di Ampleforth

Tesoreria Il timelock si occupa di gestire la tesoreria della Forth DAO attraverso un portafoglio controllato dal protocollo che detiene gli asset della DAO. Il volume degli asset detenuti è attualmente pari a 6.873.542\$²⁶⁸.

In Tabella 3.71 sono raccolti tutti gli indirizzi dei contratti di governance della DAO.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
Forth	0x77FbA179C79De5B7653F68b5039Af940AdA60ce0	governance token
GovernorBravo Delegator	0x8a994C6F55Be1fD2B4d0dc3B8f8F7D4E3a2dA8F1	governor proxy
GovernorBravo Delegate	0x444133fe9488cbec995Fd28601B3B1aD01b7fb9c	governor implem
Timelock	0x223592a191ECfC7FDC38a9256c3BD96E771539A9	timelock

Tabella 3.71: Indirizzi degli contratti di governance di Ampleforth

²⁶⁸10.02.2026,<https://debank.com/profile/0x223592a191ecfc7fdc38a9256c3bd96e771539a9>

3.34 Radworks

Radworks sta costruendo uno stack di sviluppo sovrano che consente agli sviluppatori di ospitare codice, collaborare e ricompensare i contributi open source in modo sicuro. Opera come una rete governata dalla community, che utilizza meccanismi di governance sia off-chain che on-chain per prendere decisioni collettive²⁶⁹.



Figura 3.85: Radworks Logo

Radworks si concentra in particolare sul finanziare e sostenere la creazione di tecnologie decentralizzate e resistenti alla censura, che forniscano a builder e creator gli strumenti necessari per collaborare. Attualmente in particolare si sta occupando di supportare lo sviluppo delle seguenti tecnologie:

- **Radicle:** Uno stack open source e peer-to-peer per la collaborazione sul codice, basato su Git.
- **Drips:** Il modo più semplice per finanziare l'open source nel tuo ecosistema.
- **Radworks App:** (In arrivo) Un launcher sicuro e local-first per frontend decentralizzati.

3.34.1 Token RAD

RAD è il token nativo della Rete Radworks, utilizzato come mezzo principale per coordinare tutti gli attori, governare la tesoreria e ricompensare i fornitori di infra-

²⁶⁹<https://docs.radworks.org/>

strutture della Rete Radicle²⁷⁰. Il token è definito, seguendo lo standard ERC-20, dal contratto Ethereum di indirizzo:

0x31c8EAcBFFdD875c74b94b077895Bd78CF1E64A3



Figura 3.86: Token RAD

Il protocollo di Radworks prevede un'offerta massima 99.999.620 RAD che è quasi stata raggiunta infatti al momento l'offerta totale è di 99.998.580 RAD di cui solo 59.075.978,89 RAD sono effettivamente in circolazione²⁷¹.

3.34.2 Processo di governance e analisi dei contratti

Radworks è governata da processi di governance on-chain e off-chain. Questi processi, insieme, costituiscono il sistema di governance di Radworks. I detentori del token di governance nativo di Radworks (RAD) possono partecipare alla governance creando, discutendo e votando le Radworks Governance Proposals (RGP)²⁷².

Governance on-chain La governance on-chain viene utilizzata per prendere decisioni su proposte che includono codice eseguibile. Questo include:

- Distribuzioni dalla Tesoreria di RAD, ETH e USDC.
- Aggiornamenti al sistema di governance on-chain.
- Modifiche ai parametri dei contratti governati dalla Tesoreria.

²⁷⁰<https://docs.radworks.org/rad-token/>

²⁷¹10.02.2026,<https://coinmarketcap.com/currencies/radworks/>

²⁷²<https://docs.radworks.org/governance/overview/>

Governance off-chain La governance off-chain viene utilizzata per ottenere il consenso della comunità sulle decisioni. Attualmente, il consenso è necessario per:

- Confermare che una proposta con codice eseguibile è pronta per essere inviata al voto on-chain (fase nota anche come Formal Review).
- Proposte che non includono codice eseguibile, ma che richiedono comunque il consenso della comunità (es. aggiornamenti al processo di governance).

Come conseguenza alla distinzione della tipologia di governance è necessario evidenziare anche le due tipologie di RGP che possono essere definite:

- **Eseguibile:** Azioni on-chain come distribuzioni della tesoreria, aggiornamenti ai parametri del contratto e upgrade del sistema di governance. (Passaggi previsti: Request for Comments → Formal Review → Submission).
- **Sociale:** Modifiche off-chain che non possono essere applicate dalla governance on-chain ma dovrebbero avere l'approvazione della comunità. (Passaggi previsti: Request for Comments → Formal Review).

Come possiamo intuire dunque il processo di governance prevede tre fasi: Request for Comments, Formal Review e Submission.

Fase 1: Request for Comments La fase di Request for Comments (RFC) ha luogo sul forum di governance²⁷³ e viene utilizzata per revisionare attivamente le bozze delle proposte che vengono presentate per essere prese in considerazione in un ciclo di proposte. Il feedback fornito durante questa fase consente agli autori di perfezionare e migliorare le loro proposte con il contributo della comunità. La durata della prima fase è di 14 giorni.

Fase 2: Formal Review La fase di Formal Review funge da passaggio finale di revisione nel processo di governance prima che le proposte vengano inviate on-chain. Le proposte in questa fase incorporano il feedback della fase RFC e sono

²⁷³<https://community.radworks.org/>

accompagnate da un sondaggio Snapshot²⁷⁴ off-chain per valutare il consenso. La durata di questa fase è di 7 giorni. Ogni sondaggio Snapshot deve avere tre opzioni di voto: Sì, No e Astensione.

Fase 3: Submission Inviare una proposta on-chain è il passo finale nel processo di governance. Una RGP può essere inviata alla governance on-chain da chiunque abbia una quantità di RAD maggiore o uguale all'1% dell'offerta totale di RAD delegata al proprio indirizzo (ovvero $\geq 1\text{M RAD}$). La durata della votazione on-chain (effettuata tramite la piattaforma di Tally²⁷⁵) è di 3 giorni seguiti da un ritardo di esecuzione di altri 2 giorni.

Una RGP è considerata approvata se la maggioranza dei voti è "a favore" e se il numero di voti "a favore" della proposta supera il quorum che è pari al 4% (4M di RAD) dell'offerta totale (100M). Il potere di voto considerato per gli utenti deriva direttamente dal numero di token secondo la regola 1T1V²⁷⁶.

E' importante osservare però che a differenza di molte altre DAO nel caso di Radworks le proposte vengono esaminate in cicli mensili descritti come segue:

- Settimana 1 - Primo lunedì del mese (Request for Comments): Inizio del prossimo ciclo di proposte e scadenza per pubblicare la proposta sul forum sotto Active Proposals.
- Settimana 2 - Secondo lunedì del mese (Request for Comments): Partecipa alla call mensile di Proposal Review per presentare e discutere la proposta.
- Settimana 3 - Terzo lunedì del mese (Formal Review): Apertura della proposta per la Formal Review a partire per una settimana.
- Settimana 4 - Quarto lunedì del mese (Submission): Invia la proposta on-chain.

²⁷⁴<https://snapshot.org/#/s:gov.radworks.eth>

²⁷⁵<https://www.tally.xyz/gov/radworks>

²⁷⁶<https://github.com/better-internet/radworks-governance/blob/main/manual.md#formal-review>

Per votare, sia off-chain sia on-chain, è necessario avere delegati al proprio indirizzo dei token RAD. La delega può essere eseguita su Tally scegliendo se delegare i token a se stessi oppure ad un altro utente, se si desidera che l'altro utente voti per proprio conto. La delega deve essere impostata solo una volta, dopodichè rimane valida a meno che non venga esplicitamente rimossa o cambiata.

Osservazione 3.17. *Per utilizzare il potere di voto delegato in una votazione, la delega deve avvenire prima che il voto diventi attivo.*

Governor Il **Governor** permette ai possessori del token di governance RAD, di proporre modifiche al protocollo, votarle e, se approvate, eseguirle automaticamente sulla blockchain. Il contratto originale è definito da un codice che è una fork dal celebre modello di governance di Compound. Il suo indirizzo è:

0x690e775361AD66D1c4A25d89da9fCd639F5198eD

In seguito il governor è stato sostituito da una nuova versione che implementa un codice moderno, modulare e basato sugli standard di OpenZeppelin con indirizzo:

0xD64D01D04498bFc60f04178e0B62a757C5048212

Timelock Il **Timelock** è il proprietario effettivo dei fondi e dei permessi del protocollo. L'indirizzo di tale contratto sulla rete Ethereum è:

0x8dA8f82d2BbDd896822de723F55D6EdF416130ba

Il suo codice è praticamente "byte-per-byte" identico a quello di Compound.

Tesoreria La gestione della tesoreria è affidata al contratto di timelock in cui è detenuto un volume complessivo di asset pari a 12.137.259\$²⁷⁷.

I parametri relativi al processo di governance di Radworks nello specifico sono definiti nella Tabella 3.72 mentre nella Tabella 3.73 sono riportati gli indirizzi dei contratti di governance attualmente in uso per la governance.

²⁷⁷10.02.2026,<https://debank.com/profile/0x8da8f82d2bbdd896822de723f55d6edf416130ba>

<i>Parametro</i>	<i>Valore</i>
proposalMaxOperations	10
poposalThreshold	1.000.000 RAD
quorumVotes	4.000.000 RAD
votingDelay	1 blocco $\sim$ pochi secondi $\rightarrow$ 7200 blocchi (12s) = 1 giorno
votingPeriod	17280 blocchi (15s) = 3 giorni
MINIMUM_DELAY	172800s = 2 giorni
MAXIMUM_DELAY	2592000s = 30 giorni
delay	172800s = 2 giorni
GRACE_PERIOD	1209600s = 14 giorni

Tabella 3.72: Parametri usati nel processo di governance di Radworks

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
RadicleToken	0x31c8EAcBFFdD875c74b94b077895Bd78CF1E64A3	token
RadworksGovernor	0xD64D01D04498bFc60f04178e0B62a757C5048212	governor
Timelock	0x8dA8f82d2BbDd896822de723F55D6EdF416130ba	timelock

Tabella 3.73: Indirizzi degli contratti di governance di Radworks attualmente in uso

3.35 Idle

Idle DAO è un collettivo decentralizzato che costruisce una serie di prodotti mirati a sbloccare il potenziale della finanza decentralizzata come fonte unica di rendimento. Permette agli utenti di ottimizzare algebricamente la propria allocazione di asset digitali attraverso i principali protocolli DeFi, sia che vogliano massimizzarla sia per monitorare il proprio profilo rischio-rendimento²⁷⁸.



Figura 3.87: Idle Logo

²⁷⁸<https://docs.idle.finance/>

L'offerta di prodotti è attualmente composta da²⁷⁹:

- **Best Yield:** Un aggregatore di prestiti che analizza automaticamente le funzioni dei tassi di offerta attraverso i protocolli integrati e i fondi totali nella pool per ribilanciare costantemente il capitale su un numero qualsiasi di protocolli, al fine di: "Guadagnare il tasso di interesse più alto possibile".
- **Yield Tranches:** Le YT sono pool di capitale che generano e suddividono in tranche automaticamente rendimenti e rischi basandosi su una gamma di strategie di rendimento neutrali rispetto al mercato, inclusi redditi da prestiti, commissioni di trading da AMM e farming di incentivi del protocollo.

3.35.1 Token IDLE

Il protocollo Idle è governato e aggiornato dai detentori di token IDLE. IDLE è un token ERC-20 definito dal contratto di indirizzo:

0x875773784Af8135eA0ef43b5a374AaD105c5D39e



Figura 3.88: Token IDLE

Oltre alla partecipazione alla governance della DAO, i token IDLE hanno due ulteriori casi d'uso²⁸⁰:

- **Lending, borrowing and collateral:** Grazie alla collaborazione con Paladin (protocollo di mercato di voti), i detentori di token IDLE possono prestare i propri token tramite Paladin in cambio di un rendimento e consentire a chi prende in prestito il token di votare nella Idle DAO per le proposte on-chain.

²⁷⁹<https://docs.idle.finance/products/introduction>

²⁸⁰<https://docs.idle.finance/governance/idle/use-cases>

- **Fornitura di liquidità sui DEX:** I detentori di IDLE possono fornire liquidità a una qualsiasi delle pool di trading decentralizzate in una coppia di trading come IDLE/ETH. Fornire liquidità sugli AMM richiede generalmente una pari quantità di ETH e IDLE.

Il protocollo prevede in generale un offerta massima (che coincide con l'offerta totale) di 13.000.000 IDLE di cui 8.914.214,36 IDLE attualmente in circolazione²⁸¹. I 13.000.000 IDLE sono stati distribuiti con il Token Generation Event e sono diventati totalmente disponibili nel corso dei successivi 3 anni secondo la seguente suddivisione²⁸²:

- **Ricompense Pubbliche:** il 60% dell'offerta totale di token con distribuzione su 2 anni: Fondo LPs (41%), Fondo Early LPs (4%), Ecosystem Fund (15%).
- **Team e Investitori:** il 40% dell'offerta totale di token con una distribuzione su 3 anni: Team Attuale e Futuro (22,7%), Investitori (17,3%).

3.35.2 Processo di governance e analisi dei contratti

La Idle DAO, composta dai detentori di token IDLE, consente ai partecipanti della community di guidare e contribuire ai futuri sviluppi del protocollo. Le modifiche al protocollo sono implementate tramite IIP (Idle Improvement Proposals) che prevedono il seguente processo²⁸³.

Fase 1: Discussione dell'idea I membri della community possono proporre idee in fase iniziale per ricevere feedback dagli alti utenti sul Forum di Governance²⁸⁴. La tempistica prevista per questa fase è di almeno 2 giorni.

Fase 2: Temperature Check Dopo una prima fase di successo, i membri della community possono creare il sondaggio off-chain su Snapshot²⁸⁵ per misurare

²⁸¹10.02.2026,<https://www.coingecko.com/en/coins/idle>

²⁸²<https://docs.idle.finance/governance/idle/distribution>, <https://iq.wiki/wiki/idle>

²⁸³<https://docs.idle.finance/governance/idle-dao/governance-process>

²⁸⁴<https://gov.pareto.credit/>

²⁸⁵<https://snapshot.org/#/idlefinance.eth>

il sentimento della community riguardo al potenziale cambiamento. Per il momento, i collaboratori devono aprire due sondaggi: uno per IDLE e uno per stkIDLE²⁸⁶. La somma dei pesi di voto espressi dai detentori di IDLE e stkIDLE rappresenta i risultati finali dello snapshot. Gli utenti devono detenere almeno 100 IDLE per aprire un sondaggio Snapshot. La tempistica prevista è di almeno 3 giorni.

Fase 3: Formalizzazione della proposta Dopo aver raggiunto un consenso nel Temperature Check, il proponente iniziale o un altro membro della community può sottoporre l'idea come IIP nella categoria Proposals nel forum di Governance. La tempistica prevista per questa fase è di almeno 2 giorni.

Fase 4: Proposta on-chain Superate tutte le fasi precedenti il proponente o altri membri della DAO possono distribuire on-chain la proposta ufficiale, che viene trasmessa come codice eseguibile. Una volta che la proposta on-chain è attiva, i detentori di token IDLE esprimono i loro voti.

Osservazione 3.18. *In caso di un sondaggio on-chain, anche i possessori di stkIDLE possono votare ma per rendere il sondaggio valido devono essere rispettate due soglie. Almeno il 20% degli stkIDLE circolanti votano e almeno il 70% di questi votano la stessa opzione.*

Qualsiasi indirizzo con almeno 130.000 IDLE (1% dell'offerta totale) delegati è in grado di proporre IIP on-chain. Se il quorum (4% dell'offerta totale di IDLE ovvero circa 520.000 IDLE) del sondaggio viene raggiunto, il multisig della Treasury, che detiene voti delegati, trasmetterà il risultato on-chain con l'intero saldo di voto.

La tempistica prevista per la votazione è di 3 giorni di votazione ed avviene tramite la piattaforma di Tally²⁸⁷. Se una proposta ha successo, può essere messa in coda per l'esecuzione e, dopo 2 giorni, può essere eseguita on-chain (timelock).

²⁸⁶<https://snapshot.org/#/s:staking.idlefinance.eth>

²⁸⁷<https://www.tally.xyz/gov/idle>

Governor La governance di Idle si basa sull'architettura di governance Governor Bravo di Compound con proxy (EIP-897 Delegate) definito all'indirizzo:

0x3D5Fc645320be0A085A32885F078F7121e5E5375

e corrispondente implementazione all'indirizzo:

0xe8707753C468238723887a4b7b47495a2D311F85

Timelock Il contratto di timelock, il cui indirizzo è il seguente:

0xD6dABBC2b275114a2366555d6C481EF08FDC2556

quando chiamato modificherà i parametri di sistema, la logica e i contratti in un modello di aggiornamento time-delayed. Il suo codice segue lo standard di Compound.

Nella Tabella 3.75 sono riportati i parametri, definiti in tali contratti, che caratterizzano il processo di governance della DAO.

<i>Parametro</i>	<i>Valore</i>
proposalMaxOperations	15
MIN_PROPOSAL_THRESHOLD	65.000 idle
MAX_PROPOSAL_THRESHOLD	130.000 IDLE
poposalThreshold	130.000 IDLE
quorumVotes	520.000 IDLE
MIN_VOTING_DELAY	1 blocco ~ pochi secondi
MAX_VOTING_DELAY	40320 blocchi = 7 giorni
votingDelay	100 blocchi ~ 20 minuti
MIN_VOTING_PERIOD	5760 blocchi = 1 giorno
MAX_VOTING_PERIOD	80640 blocchi = 14 giorni
votingPeriod	17280 blocchi (15s) = 3 giorni
MINIMUM_DELAY	172800s = 2 giorni
MAXIMUM_DELAY	2592000s = 30 giorni
delay	172800s = 2 giorni
GRACE_PERIOD	1209600s = 14 giorni

Tabella 3.74: Parametri usati nel processo di governance di Idle

Tesoreria La tesoreria di Idle DAO è gestita da un insieme di 9 distinti contratti, ognuno dei quali ha uno scopo ben definito. Il contratto principale che detiene la gran parte degli asset è il seguente proxy:

0xFb3bD022D5DAcF95eE28a6B07825D4Ff9C5b3814

a cui è associato un contratto di implementazione di tipo GnosisSafe di indirizzo:

0xd9Db270c1B5E3Bd161E8c8503c55cEABeE709552

Il volume complessivo detenuto nella tesoreria è attualmente di 102.900\$²⁸⁸.

Concludiamo infine lo studio di Idle raccogliendo tutti gli indirizzi dei contratti di governance nella Tabella 3.74.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
Idle	0x875773784Af8135eA0ef43b5a374AaD105c5D39e	token
GovernorBravoDelegator	0x3D5Fc645320be0A085A32885F078F7121e5E5375	governor proxy
GovernorBravoDelegate	0xe8707753C468238723887a4b7b47495a2D311F85	governor implem
Timelock	0xD6dABBC2b275114a2366555d6C481EF08FDC2556	timelock

Tabella 3.75: Indirizzi degli contratti di governance di Idle DAO

3.36 HAI

HAI è un protocollo di stablecoin a "peg controllato" lanciato su Optimism come fork multi-collaterale di RAI. Progettato per superare le limitazioni del suo predecessore, HAI permette agli utenti di coniare moneta depositando diverse tipologie di collaterale (ETH, OP, ...) riducendo i costi opportunità legati al blocco dei fondi.

Il cuore del protocollo risiede nel suo controller PI, un meccanismo algoritmico che

²⁸⁸10.02.2026, <https://tokenterminal.com/explorer/projects/idle-finance/metrics/treasury>

regola automaticamente il 'Prezzo di Riscatto' (Redemption Price). A differenza delle stablecoin classiche che hanno un valore fisso, HAI parte da un riferimento iniziale di 1\$, ma il suo valore reale fluttua nel tempo in risposta alla domanda di mercato per smorzare la volatilità. L'intero sistema è controllato da una governance decentralizzata tramite il token KITE, che permette agli utenti di votare sull'aggiunta di nuovi collateral e sui tetti di debito, con lo scopo strategico di portare le stablecoin a 'peg controllato' sulla rete veloce di Optimism.



Figura 3.89: HAI Logo

3.36.1 Token HAI e KITE

HAI La stablecoin HAI è definita come un token ER-20 su Optimism con indirizzo:

0x10398AbC267496E49106B07dd6BE13364D10dC71

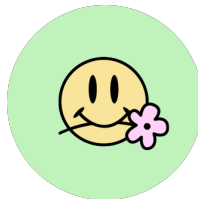


Figura 3.90: Token HAI

Da protocollo non è prevista una quantità massima di HAI che possono essere coniate. Attualmente l'offerta totale che coincide con quella circolante e pari a 504.392 HAI²⁸⁹.

²⁸⁹10.02.2026,<https://www.coingecko.com/it/monete/let-s-get-hai>

KITE Il token KITE è un token di governance ERC-20 che consente ai detentori di partecipare alla Governance di HAI. il relativo indirizzo su Optimism è:

0xf467C7d5a4A9C4687fFc7986aC6aD5A4c81E1404

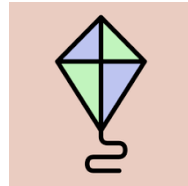


Figura 3.91: Token KITE

Se possiedi token KITE, puoi presentare e votare proposte che influenzano il funzionamento e l'evoluzione del protocollo HAI e delle sue tecnologie sottostanti. Il potere di voto dei tuoi token corrisponde direttamente alla loro quantità, poiché la Governance di HAI implementa un sistema di voto ponderato in base ai token. È importante notare che la Delega dei token KITE è necessaria per partecipare alla Governance di HAI ed è consentita attraverso la piattaforma Tally²⁹⁰.

Il protocollo prevede un hard cap per il token KITE di 1.000.000 KITE. L'offerta totale è di 854.764 KITE quasi interamente in circolazione (853.169 KITE)²⁹¹.

3.36.2 Processo di governance e analisi dei contatti

Le proposte che possono essere votate possono essere di due tipi diversi²⁹².

1. **HIP (HAI Improvement Proposals)** si occupano dell'aggiunta o rimozione di collaterali aggiuntivi all'ecosistema del protocollo HAI oppure della modifica di parametri di governance.
2. **Proposte RFS HIP** si occupano di modifiche al controllore PID.

²⁹⁰<https://www.tally.xyz/gov/hai>, <https://hai-9.gitbook.io/>

hai-governance-documentation/governance/intro-to-governance/kite-overview

²⁹¹<https://www.coingecko.com/it/monete/kite>

²⁹²<https://hai-9.gitbook.io/hai-governance-documentation/governance/governance-processes/proposal-types>

Osservazione 3.19. *Tutte le RFS HIP sono costituzionali, mentre le HIP possono essere sia costituzionali che non costituzionali.*

Il processo di Governance HAI per la presentazione di una proposta e la sua successiva votazione consiste in tre fasi: ideazione iniziale e segnalazione, sottomissione della proposta informale o Temperature Check (off-chain) e sottomissione della proposta formale (on-chain)²⁹³.

Fase Uno: Segnalazione Chiunque può proporre nuove idee per delle proposte non sono previsti requisiti o liminiti di durata per questa fase.

L'obiettivo della prima fase è informare la community di HAI sulle proprie idee e vedere se ottengono il consenso o il supporto da altri membri della community (su Discord). La Fase 1 è informale e opzionale il che significa che dipende dall'utente scegliere se effettuare o meno la segnalazione e nel momento in cui viene effettuata decidere se utilizzare o meno il feedback ricevuto per la tua proposta.

Fase Due: Proposta Informale o Temperature Check Chiunque può avviare una discussione per una nuova proposta sul Forum ufficiale di HAI al fine di valutare il potenziale di un'idea ed eseguire sondaggi non vincolanti. La durata minima di questa fase è di almeno una settimana, per garantire che le persone abbiano tempo sufficiente per esprimere la propria opinione.

Osservazione 3.20. *I risultati del voto off-chain su Discourse potrebbero non allinearsi accuratamente con i futuri risultati on-chain. Questa fase è progettata per identificare e risolvere eventuali problemi prima di procedere con un voto on-chain.*

Fase Tre: Proposta Formale Una proposta formale dovrebbe essere inviata e votata dalla community HAI tramite la piattaforma Tally solo se la proposta informale ha dimostrato il supporto della community.

²⁹³<https://hai-9.gitbook.io/hai-governance-documentation/governance/governance-processes/phases-of-hai-governance>

Governor Il contratto **HaiGovernor** di indirizzo:

0xe807f3282f3391d237BA8B9bECb0d8Ea3ba23777

è un modulo di governance standard e sicuro, basato sulle librerie di OpenZeppelin che serve a gestire le proposte, le votazioni e l'esecuzione di modifiche in una DAO ed progettato per essere modulare e includere protezioni contro gli attacchi più comuni.

Timelock Il **TimelockController** è il contratto standard OpenZeppelin (v5.0.0) definito all'indirizzo:

0xd68e7D20008a223dD48A6076AAf5EDd4fe80a899

È un componente critico per la sicurezza delle DAO. Agisce come un cuscinetto temporale tra la decisione di governance e l'esecuzione effettiva sulla blockchain.

All'interno dei contratti citati sono inoltre implementati i principali parametri che consentono di regolare e gestire il processo di governance. I valori specifici scelti per HAI DAO sono riportati nella Tabella 3.76.

<i>Parametro</i>	<i>Valore</i>
poposalThreshold	5.000 KITE
$\text{quorum} = \frac{\text{quorumNumerator}}{\text{quorumDenominator}}$	1% della supply totale
quorum (teorico per HIP)	3% della supply totale
quorum (teorico per RFS HIP)	25% della supply totale
votingDelay	43200s = 3.600 blocchi = 12h
votingPeriod	129600s = 10.800 blocchi = 36h (teorico 2 giorni)
votingPeriod (teorico)	17280 blocchi = 3 giorni
getMinDelay	86400s = 1 giorno
executionDelay (teorico)	172800s = 2 giorni

Tabella 3.76: Parametri usati nel processo di governance di HAI

Tesoreria La tesoreria è gestita da un contratto diverso rispetto a quelli analizzati ed è definita secondo lo standard GnosisSafe come proxy all'indirizzo:

0xDCb421Cc4Cbb7267F3b2cAcAb44Ec18AEbEd6724

con relativa implementazione definita di indirizzo:

0xfb1bffc9d739B8D520DaF37dF666da4C687191EA

Il volume degli asset detenuti in tale contratto è attualmente pari a 544.208,10\$²⁹⁴.

I contratti di governance principali di HAI DAO sono riportati nella Tabella 3.77.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
ProtocolToken	0xf467C7d5a4A9C4687fFc7986aC6aD5A4c81E1404	governance token
SystemCoin	0x10398AbC267496E49106B07dd6BE13364D10dC71	stablecoin
HaiGovernor	0xe807f3282f3391d237BA8B9bECb0d8Ea3ba23777	governor
TimelockController	0xd68e7D20008a223dD48A6076AAf5EDd4fe80a899	timelock
GnosisSafeProxy	0xDCb421Cc4Cbb7267F3b2cAcAb44Ec18AEbEd6724	treasury proxy
GnosisSafeL2	0xfb1bffc9d739B8D520DaF37dF666da4C687191EA	tresury implemen

Tabella 3.77: Indirizzi degli contratti di governance di HAI DAO

3.37 Union

Union è un protocollo di credito di proprietà dei membri costruito su Ethereum, dove i membri possono sottoscrivere linee di credito per gli indirizzi di altri membri.



Figura 3.92: Union Logo

Il Protocollo Union è una rete di credito che consente a qualsiasi indirizzo di accumulare una linea di credito on-chain in modo permissionless e crypto-native. Il

²⁹⁴10.02.2026,<https://www.tally.xyz/gov/hai/treasury>

protocollo stesso non è un sottoscrittore di rischio, ma piuttosto un meccanismo per ridurre il costo di coordinamento della fiducia in credito disponibile. Aggregando le linee di credito, i membri di Union possono reperire capitale a un costo inferiore rispetto a quanto potrebbe fare un singolo membro da solo. Ciò innesca un circolo virtuoso di maggiore credito disponibile, minori costi di indebitamento e maggiore attività di prestito²⁹⁵.

3.37.1 Token UNION

Il token UNION è un utility token ERC20, che nasce come token di governance per il protocollo, per poi assumere potenzialmente qualsiasi altra nuova funzione che la DAO potrebbe prevedere per esso. Il suo contratto è distribuito all'indirizzo:

0x5Dfe42eEA70a3e6f93EE54eD9C321aF07A85535C



Figura 3.93: Token UNION

La supply iniziale di UNION è 1.000.000.000 UNION, con la DAO che ha la capacità di coniare fino al 2% all'anno (a partire dal 22/12/2025). La distribuzione della supply iniziale è stata articolata come segue:

- 20% alla DAO della Community - 200.000.000 (+ 2%/anno di mint perpetuo);
- 46,78% al Team - 466.666.666: (1 anno di cliff + 4 anni di vesting);
- 33,22% agli Early Supporters - 332.166.667: (1 anno di lockup + 1 anno di vesting).

²⁹⁵<https://docs.union.finance/>

Al momento l'offerta totale ha raggiunto il tetto massimo previsto dal protocollo per un totale di 10.000.000.000 UNION di cui 1.919.050.000 UNION sono in circolazione²⁹⁶.

3.37.2 Processo di governance ed analisi dei contratti

Fase I: Temperature Check & Proposta (off-chain) Per determinare se c'è abbastanza richiesta per un cambiamento, si utilizza un Temperature Check ovvero un metodo di segnalazione soft usato per valutare il sentimento della community sulla proposta. Per avviare un Temperature Check, si pone una domanda generale e imparziale alla community nel Canale Governance del Discord di Union²⁹⁷.

Dopo aver analizzato i feedback della community è possibile creare una proposta nel repository Github di Union pubblico²⁹⁸. Lo scopo della Bozza di Proposta è generare discussione in seguito alla quale è necessario contattare gli Admin del Discord di Union per discutere la proposta in una Community Call o su uno Space di Twitter.

Fase II: Proposta Attiva (on-chain) Una volta che c'è un consenso generale sulla validità della proposta da parte della community e il codice necessario sia finalizzato e provato come eseguibile, la proposta può passare al voto on-chain inviandola al contratto governor. Per emanare una **Proposta Eseguitibile**, è necessario disporre di almeno 10.000.000 UNION delegati al proprio indirizzo oppure si cerca un delegato in grado di soddisfare la soglia minima.

Una volta chiamata la funzione `propose()`, la proposta viene messa in coda e la votazione inizierà in 24 ore. Il periodo di voto è di 3 giorni. Se la proposta ha successo, verrà attuato un timelock di 24 ore prima che il codice proposto venga eseguito. Per passare le proposte hanno un requisito di quorum del 4% e richiedono un minimo del 50% di voti favorevoli per passare.

²⁹⁶10.02.2026,<https://www.coingecko.com/it/monete/union>

²⁹⁷<https://discord.com/channels/714982388970684468/923268201486377010>

²⁹⁸<https://github.com/unioncredit/UIPs/issues>

Osservazione 3.21. *La delega, la visualizzazione delle proposte attive e le votazioni possono avvenire su Tally²⁹⁹ oppure sulla dApp di Union³⁰⁰.*

Governor Il contratto **UnionGovernor** è costruito sopra le librerie standard di OpenZeppelin, che sono lo standard di settore, ed è registrato all'indirizzo:

0xe1b3F07a9032F0d3deDf3E96c395A4Da74130f6e

Esso funge da "cervello" della DAO e permette ai detentori di token di creare proposte, votare e, se la proposta passa, eseguirla.

Timelock Il **TimelockController** è una copia esatta della libreria OpenZeppelin v4.4.0 ed è definito all'indirizzo:

0xBBD3321f377742c4b3fe458b270c2F271d3294D8

Nella Tabella 3.78 sono riportati i parametri del processo di governance della DAO.

<i>Parametro</i>	<i>Valore</i>
poposalThreshold	10.000.000 UNION
quorumVotes	40.000.000 UNION
votingDelay	7200 blocchi (12s) = 1 giorno
votingPeriod	21600 blocchi (12s) = 3 giorni
getMinDelay	86400s = 1 giorno

Tabella 3.78: Parametri usati nel processo di governance di Union

Tesoreria Il contratto responsabile della gestione della tesoreria ha indirizzo:

0x6DBDe0E7e563E34A53B1130D6B779ec8eD34B4B9

e detiene un volume attualmente pari a 355.993,06\$³⁰¹.

Nella Tabella 3.79 sono riportati gli indirizzi dei contratti responsabili della gestione del processo di governance della DAO.

²⁹⁹<https://www.tally.xyz/gov/union>

³⁰⁰<https://app.union.finance/governance>

³⁰¹10.02.2026,<https://etherscan.io/address/0x6DBDe0E7e563E34A53B1130D6B779ec8eD34B4B9#asset-multichain>

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
UnionToken	0x5Dfe42eEA70a3e6f93EE54eD9C321aF07A85535C	token
UnionGovernor	0xe1b3F07a9032F0d3deDf3E96c395A4Da74130f6e	governor
TimelockController	0xBBD3321f377742c4b3fe458b270c2F271d3294D8	timelock
Treasury	0x6DBDe0E7e563E34A53B1130D6B779ec8eD34B4B9	treasury

Tabella 3.79: Indirizzi degli contratti di governance di Union

3.38 OpenDollar

Open Dollar è un protocollo stablecoin costruito su Arbitrum, progettato per aiutare a generare rendimento e utilizzare la leva finanziaria sui propri asset in modo sicuro e prevedibile³⁰².



Figura 3.94: OpenDollar Logo

I Liquid Staking Token (LST) e altri asset nativi di Arbitrum possono essere depositati in Non-Fungible Vault (NFV) per prendere in prestito la stablecoin OD tramite prestiti a basso interesse, creare posizioni a leva e continuare a ottenere il 100% del rendimento dello staking. OD è sovracollateralizzata e ancorata agganciato al valore di \$1,00 tramite un sistema di incentivi dinamico. L'indirizzo del suo contratto è:

0x221A0f68770658C15B525d0F89F5da2baAB5f321



Figura 3.95: Token OD

³⁰²<https://docs.opendollar.com/>

Gli NFV di Open Dollar rappresentano un'alternativa più efficiente in termini di capitale rispetto ai CDP (Collateralized Debt Position) vincolati all'account, offrendo ai depositanti la libertà di scambiare le proprie posizioni o venderle ad arbitraggisti su qualsiasi piattaforma NFT senza dover rimborsare completamente i prestiti o incorrere in penalità di liquidazione³⁰³.

3.38.1 Token ODG

ODG è il token ERC-20 di governance del protocollo. Il suo contratto ha indirizzo:

0x000D636bD52BFc1B3a699165Ef5aa340BEA8939c

Esso conferisce ai detentori il diritto di partecipare al processo di governance, influenzando le decisioni chiave e la direzione strategica dell'ecosistema Open Dollar. La tesoreria del Protocollo è controllata dai detentori di token ODG attraverso una DAO. I detentori di ODG possono creare proposte, votare o delegare il proprio potere di voto a delegati di loro scelta per indirizzare la governance per loro conto.



Figura 3.96: Token ODG

La distribuzione iniziale del token è stata di 10.000.000 ODG. Nuovi token ODG non possono essere conati dalla DAO, dal team o da chiunque altro. Nuovi ODG possono essere conati esclusivamente dal protocollo stesso in modo autonomo in casi di emergenza, ovvero quando vi è un debito inesigibile che deve essere saldato³⁰⁴.

³⁰³<https://docs.opendollar.com/Open-Dollar-Protocol-Overview>

³⁰⁴<https://docs.opendollar.com/The-ODG-Token>

3.38.2 Processo di governance e analisi contratti

Il protocollo Open Dollar è progettato per garantire longevità e prevedibilità attraverso un approccio a governance minima che definiamo "Ungovernance". Diversamente dalla maggior parte degli altri protocolli DeFi governati da DAO, dove i detentori dei token possono alterare gran parte della piattaforma in modi drastici, talvolta a discapito degli utenti, il potere dei detentori di Open Dollar Governance (ODG) e della DAO è estremamente limitato. La DAO può votare per aggiungere nuove tipologie di collaterale, ma non può modificare gli aspetti principali del protocollo, come impostare nuovi tassi di stabilità per i vault esistenti, coniare nuovi token OD, modificare la distribuzione delle commissioni o aggiornare molti dei parametri pre-impostati o determinati dal mercato³⁰⁵.

Il processo di governance effettivo per la DAO di OpenDollar prevede³⁰⁶ una fase facoltativa (ma raccomandata) che avviene off-chain sul Forum della DAO³⁰⁷ ed una fase ufficiale on-chain che invece avviene sul portale costruito tramite Tally³⁰⁸.

- Il forum ufficiale è dedicato a discussioni, proposte, dibattiti e allo scambio di idee relative alla governance di Open Dollar. Condividendovi in anticipo tutte le proposte imminenti consente di fornire contesto ai votanti e ricevere feedback costruttivi che possano aiutare la DAO a raggiungere un consenso e ottenere i risultati desiderati.
- La dashboard di Tally invece permette ai detentori di token ODG di creare proposte, votare sulle proposte attive, diventare delegati e delegare i propri ODG ad altri membri della DAO.

Governor ODGovernor è il contratto centrale del processo di governance ed è definito sulla rete Arbitrum One all'indirizzo:

0xf704735CE81165261156b41D33AB18a08803B86F

³⁰⁵<https://docs.opendollar.com/Governance-introduction>

³⁰⁶<https://docs.opendollar.com/Proposals-and-Voting>

³⁰⁷<https://common.xyz/open-dollar-governance/discussions>

³⁰⁸<https://gov.opendollar.com/dao>

il suo codice non è scritto da zero, ma è un assemblaggio di moduli standard e sicuri forniti da OpenZeppelin.

Timelock Il timelock della DAO è definito all'indirizzo:

0x7A528eA3E06D85ED1C22219471Cf0b1851943903

attraverso il codice standard di OpenZeppelin **TimelockController**.

I parametri scelti dal protocollo di OpenDollar per il processo di governance della DAO sono raccolti in Tabella 3.80.

<i>Parametro</i>	<i>Valore</i>
poposalThreshold	5.000 ODG
$\text{quorum} = \frac{\text{quorumNumeratore}}{\text{quorumDenominator}}$	0.2% della supply totale
quorumVotes	20.000 ODG
votingDelay	3600 blocchi (12s) = 12h
votingPeriod	14400 blocchi (12s) = 2 giorni
getMinDelay	86400s = 1 giorno

Tabella 3.80: Parametri usati nel processo di governance di OpenDollar

Tesoreria La tesoreria della DAO è gestita dal contratto di timelock che detiene un volume di asset attualmente pari a 4.302.299,83\$³⁰⁹.

I contratti che definiscono il processo di governance sono riportati in Tabella 3.81.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
OpenDollar	0x221A0f68770658C15B525d0F89F5da2baAB5f321	stablecoin
ProtocolToken	0x000D636bD52BFc1B3a699165Ef5aa340BEA8939c	governance token
ODGovernor	0xf704735CE81165261156b41D33AB18a08803B86F	governor
TimelockController	0x7A528eA3E06D85ED1C22219471Cf0b1851943903	timelock

Tabella 3.81: Indirizzi degli contratti di governance di OpenDollar

³⁰⁹10.02.2026,<https://arbiscan.io/address/0x7A528eA3E06D85ED1C22219471Cf0b1851943903#asset-multichain>

3.39 Cryptex

Cryptex Finance è stata fondata da Joe Sticco, Preston Van Loon e Thomas Matzner. Si tratta di un protocollo blockchain che mira a fornire un'esposizione sicura al mercato delle criptovalute utilizzando strategie collaudate della finanza tradizionale applicate alla finanza decentralizzata.



Figura 3.97: Cryptex Logo

Dopo aver assistito al boom delle ICO del 2017 e ai conseguenti rug pull che hanno causato perdite agli investitori, il team ha iniziato a lavorare al progetto. Dopo 15 mesi di ricerca e sviluppo, la mainnet è stata lanciata su Ethereum il 6 aprile 2021.

Il protocollo Cryptex è una raccolta di smart contract che fornisce agli utenti esposizione alla crescita dell'intero settore delle criptovalute attraverso il suo token ERC20, TCAP (Total Crypto Market Cap) il cui contratto sulla rete Ethereum ha indirizzo:

0x16c52CeeCE2ed57dAd87319D91B5e3637d50aFa4



Figura 3.98: TCAP Token

TCAP è un derivato della capitalizzazione di mercato totale delle criptovalute, emesso e bruciato in base al mercato. I suoi dati di prezzo derivano da un meccanismo aggregato alimentato da Chainlink e sono garantiti dalla collateralizzazione di BTC, ETH o stablecoin per un prezzo equivalente al TCAP emesso.³¹⁰

³¹⁰<https://messari.io/project/cryptex-finance-2>

3.39.1 Token CTX

Il Protocollo Cryptex è governato e aggiornato dalla sua DAO che è gestita detentori del token CTX. L'indirizzo del contratto del token è:

0x321C2fE4446C7c963dc41Dd58879AF648838f98D



Figura 3.99: Token CTX

Da protocollo non è previsto un limite massimo di CTX. La sua offerta totale ad oggi è pari a 10.000.000 CTX di cui 8.203.919,45 CTX sono in circolazione³¹¹.

3.39.2 Processo di governance e analisi dei contatti

Le fasi in cui si articola il processo di governance della DAO sono le seguenti³¹²:

Fase 1: Discussione preliminare Qualsiasi membro della community può avviare una proposta iniziando una discussione sul Forum di Cryptex³¹³. La community discuterà l'idea e, se questa riuscirà a raccogliere un notevole supporto procederà alla fase successiva.

Fase 2: Creare una Cryptex Improvement Proposal (CIP) Una volta discussa un'idea, un membro della community può creare una Cryptex Improvement Proposal (CIP) sul medesimo Forum. La proposta per passare deve ottenere la maggioranza relativa dei voti nel sondaggio durante un periodo di quattro giorni.

³¹¹10.02.2026, <https://coinmarketcap.com/currencies/cryptex-finance/>

³¹²<https://messari.io/project/cryptex-finance-2/governance/governance-process>

³¹³<https://forum.cryptex.finance/>

Fase 3: Voto di degnalazione (off-chain) Una volta che la proposta raggiunge la Fase 3, il creatore può avviare una votazione su Cryptex Snapshot³¹⁴ e i detentori di CTX possono votare sulla proposta. Il voto su Snapshot richiede una maggioranza a favore della proposta.

Fase 4: Voto vincolante (on-chain) Se il voto su Snapshot ha esito positivo, qualsiasi detentore di token con oltre 100.000 CTX può creare una proposta direttamente sul modulo di governance di Cryptex o tramite la piattaforma Tally³¹⁵. Il voto on-chain deve ottenere la maggioranza dei voti a favore e raggiungere un quorum di 400.000 CTX per avere successo. Il periodo di voto dura 3 giorni.

Fase 5: Esecuzione Le proposte on-chain approvate vengono implementate dal modulo di Governance di Cryptex dopo un timelock di 2 giorni.

La fase on-chain di tale processo è gestito tramite tre componenti distinte: il token CTX, il modulo di governance e il Timelock (i cui indirizzi sono raccolti nella Tabella 3.82). Insieme, questi contratti consentono alla community di proporre, votare e implementare modifiche al protocollo Cryptex³¹⁶.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
TCAP	0x16c52CeeCE2ed57dAd87319D91B5e3637d50aFa4	token ERC-20
Ctx	0x321C2fE4446C7c963dc41Dd58879AF648838f98D	governance token
GovernorBeta	0x874C5D592AfC6803c3DD60d6442357879F196d5b	governor
Timelock	0xa54074b2cc0e96a43048d4a68472F7F046aC0DA8	timelock

Tabella 3.82: Indirizzi degli contratti di governance di Cryptex

Governor GovernorBeta è basato quasi interamente sull'omonimo modello di governance di Compound ed è registrato all'indirizzo:

0x874C5D592AfC6803c3DD60d6442357879F196d5b

³¹⁴<https://snapshot.org/#/s:cryptexdao.eth>

³¹⁵<https://www.tally.xyz/gov/cryptex>

³¹⁶<https://docs.cryptex.finance/governance/reference/>

Timelock Allo stesso modo il contratto di timelock è una copia quasi esatta del Timelock di Compound Finance ed è definito all'indirizzo:

0xa54074b2cc0e96a43048d4a68472F7F046aC0DA8

I parametri usati nel processo di governance sono raccolti nella Tabella 3.83.

<i>Parametro</i>	<i>Valore</i>
poposalMaxOperations	10
poposalThreshold	100.000 CTX
quorumVotes	400.000 CTX.
votingDelay	1 blocco $\sim$ pochi secondi
votingPeriod	17280 blocchi (15s) = 3 giorni
MAXIMUM_DELAY	2592000s = 30 giorni
MINIMUM_DELAY	172800s = 2 giorni
delay	259200s = 3 giorni
delay (teorico)	2 giorni
GRACE_PERIOD	1209600s = 14 giorni

Tabella 3.83: Parametri usati nel processo di governance di Cryptex

Tesoreria La tesoreria della DAO è gestita dal contratto di timelock che detiene un volume di asset pari a 740.084,87\$³¹⁷.

3.40 Threshold Network

Threshold Network alimenta tBTC, lo standard Bitcoin nella finanza, nonché il Bitcoin tokenizzato 1:1 più decentralizzato.



Figura 3.100: Threshold Network Logo

³¹⁷10.02.2026,<https://www.tally.xyz/gov/cryptex/treasury>

tBTC consente alla liquidità di Bitcoin di spostarsi fluidamente tra diverse chain senza compromettere la finalità del regolamento (settlement finality). Basato sulla crittografia a soglia e protetto da una rete a rotazione di operatori di nodi indipendenti, distribuisce il controllo dei Bitcoin in modo tale che nessuna singola entità possa agire autonomamente sui fondi. Il contratto di tBTC ha indirizzo:

`0x8dAEBADe922dF735c38C80C7eBD708Af50815fAa`

Questa struttura sostiene i principi fondamentali di Bitcoin, ovvero la minimizzazione della fiducia (trust-minimized), la natura permissionless e la resistenza alla censura, mantenendo al contempo un percorso diretto e verificabile verso il Bitcoin nativo³¹⁸.

3.40.1 Token T

Il token T è un token ERC-20 che alimenta tBTC e funge da asset di governance e di accumulo di valore della rete. Il contratto del token è distribuito all'indirizzo:

`0xCdF7028ceAB81fA0C6971208e83fa7872994beE5`



Figura 3.101: Token T

L'offerta iniziale è stata stabilita dalla DAO al momento del lancio a 10.000.000.000 T, con la seguente allocazione:

- 4,5 miliardi di T allocati ai detentori di token NU;
- 4,5 miliardi di T allocati ai detentori di token KEEP;
- 1 miliardo di T allocato alla tesoreria della Threshold DAO.

³¹⁸<https://docs.threshold.network/>

Ulteriori 1,155 miliardi di token sono stati conati durante la fase di bootstrap inflazionistico della rete come incentivi per gli staker e gli operatori dei nodi, portando a un'offerta totale finale di 11.155.000.000 token T³¹⁹ che coincide anche con l'offerta attualmente in circolazione³²⁰.

3.40.2 Processo di governance e analisi dei contratti

Il ciclo di vita attraversato dalle proposte nella DAO prevede le seguenti fasi³²¹.

Fase 1: Discussione sul forum Un membro della community di Threshold pubblica una potenziale proposta sui forum di governance di Threshold. Non è richiesta una soglia minima di token per creare una nuova proposta sui forum. I moderatori della community si riservano il diritto di moderare lo spam in questa fase eliminando le proposte non valide.

Fase 2: Temperature Check Una volta che una potenziale proposta ha ottenuto sufficiente trazione e discussione all'interno della community, può procedere a un "temperature check" tramite uno Snapshot off-chain³²². Se una proposta riceve il sostegno della maggioranza, è idonea a passare allo step successivo.

Fase 3: Creazione della proposta Un membro della community che detiene un peso di voto sufficiente (almeno lo 0,25% dell'offerta totale di T) sottomette la proposta on-chain. La proposta entra in un periodo di attesa di 2 giorni prima che il voto inizi ufficialmente.

Fase 4: Votazione La votazione della proposta rimane aperta per 10 giorni. Se la proposta passa con il quorum necessario (almeno l'1,5% dell'offerta totale di T), procede alla fase successiva; se fallisce, viene cancellata.

³¹⁹<https://docs.threshold.network/t-token>

³²⁰10.02.2026,<https://coinmarketcap.com/currencies/threshold/>

³²¹<https://docs.threshold.network/governance/governance-process>

³²²<https://snapshot.org/#/threshold.eth>

Fase 5: Periodo di timelock ed esecuzione Una volta approvata una proposta, gli smart contract Governor Bravo includono un ulteriore ritardo di timelock di 2 giorni. Dopo il ritardo del timelock, chiunque può eseguire una proposta approvata.

Tale ciclo però può subire alcune variazioni in casi particolari, ovvero:

- **Veto del Comitato:** Durante la fase on-chain, il Comitato può porre il veto su qualsiasi proposta proteggendo il sistema da eventuali proposte pericolose.
- **Prevenzione del quorum tardivo:** Il periodo di votazione di 10 giorni viene automaticamente esteso se il quorum viene raggiunto in ritardo. Nel caso in cui una proposta raggiunga il quorum a meno di 2 giorni dalla scadenza, la scadenza viene prorogata di ulteriori 2 giorni dal raggiungimento del quorum.
- **Proposte off-chain:** Alcune proposte non implicano alcuna azione on-chain. In questi casi, avviene una votazione su Snapshot che dura 5 giorni per le proposte regolari e 7 giorni per le elezioni.

I contratti che consentono tutte le procedure di votazione ed esecuzione on-chain delle proposte sono riportati nella Tabella 3.84 ed analizzati di seguito.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
T	0xCdF7028ceAB81fA0C6971208e83fa7872994beE5	governance token
TokenholderGovernor	0xd101f2B25bCBF992BdF55dB67c104FE7646F5447	governor
TimelockController	0x87F005317692D05BAA4193AB0c961c69e175f45f	timelock

Tabella 3.84: Indirizzi degli contratti di governance di Threshold Network

Governor e timelock Il **TokenholderGovernor** ha indirizzo:

0xd101f2B25bCBF992BdF55dB67c104FE7646F5447

ed il **TimelockController** di indirizzo:

0x87F005317692D05BAA4193AB0c961c69e175f45f

sono contratti con struttura modulare sfruttando le librerie standard di OneZeppelin.

Tesoreria La tesoreria della DAO è detenuta e gestita dal contratto di timelock, il quale detiene un volume di asset attualmente pari a 1.798.498,4\$³²³.

I parametri relativi al processo di governance sono riportati nella Tabella 3.85.

<i>Parametro</i>	<i>Valore</i>
poposalThreshold	0.25% della supply totale
quorum	1.5% della supply totale
votingDelay	13292 blocchi (13s) $\simeq$ 2 giorni
votingPeriod	50000 blocchi (13s) $\simeq$ 7 giorni
votingPeriod (teorico)	10 giorni
lateQuorumVoteExtension	13292 blocchi (13s) $\simeq$ 2 giorni
getMindelay	172800s = 2 giorni

Tabella 3.85: Parametri di governance di Threshold Network

3.41 Anvil

Anvil è un sistema di smart contract basati su Ethereum che gestisce il collaterale ed emette credito interamente garantito.



Figura 3.102: Anvil Logo

Anvil è un protocollo unificato per la fornitura di asset, progettato esplicitamente all'insegna della sicurezza, della semplicità e della componibilità come elemento costitutivo fondamentale per lo sviluppo di altre applicazioni³²⁴.

³²³10.02.2026,<https://www.tally.xyz/gov/threshold-network/treasury>

³²⁴<https://docs.anvilapplication.com/>

3.41.1 Token ANVL

ANVL è un token ERC-20 che governa tutti gli aggiornamenti e le operazioni del protocollo, oltre al supporto degli asset e alle approvazioni dei contratti esterni³²⁵. Il suo contratto fu originariamente distribuito all'indirizzo:

`0x2Ca9242c1810029Efed539F1c60D68B63AD01BFc`

Attualmente però il contratto è stato sostituito da una nuova versione più modulare ed aggiornata il cui indirizzo è:

`0xAEEAa594e7dc112D67b8547fe9767a02c15B5597`



Figura 3.103: Token ANVL

L'offerta totale è stata totalmente distribuita alla genesi, essa coincide con il suo tetto massimo ed è pari a 100.000.000.000 ANVL di cui 80.200.555.200 ANVL sono attualmente in circolazione³²⁶.

3.41.2 Processo di governance ed analisi dei contratti

Il protocollo Anvil è governato dalla community dei detentori di ANVL e dai delegati. La governance è un processo autonomo al 100% on-chain che consente alla community di proporre, votare e implementare modifiche ai parametri configurabili dei contratti del protocollo Anvil³²⁷.

L'intero processo si svolge nell'arco di due settimane come mostrato in Figura 3.103.

³²⁵<https://acronym-foundation.medium.com/introducing-the-anvil-protocol-and-anvl-6c0abf786b65>

³²⁶10.02.2026,<https://coinmarketcap.com/it/currencies/anvil/>

³²⁷<https://docs.anvilapplication.com/governance/governance>

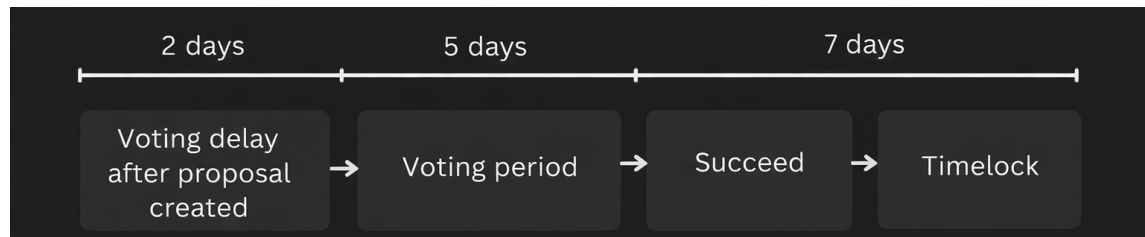


Figura 3.104: Processo di governance di Anvil

Per sottoporre una proposta on-chain sono necessari almeno 500.000.000 ANVL e richiedono almeno 5.000.000.000 di voti ANVL totali **for** o **abstain** per raggiungere il quorum. Alla fine del periodo di voto di 5 giorni, le proposte che non raggiungono il quorum, o che raggiungono il quorum ma ricevono più voti **against** rispetto ai voti **for**, non vengono eseguite mentre quelle che raggiungono il quorum e ricevono più voti **for** che **against** vengono approvata e quindi eseguite dopo un periodo di timelock di 7 giorni³²⁸.

Osservazione 3.22. *Per partecipare alla governance di Anvil, i detentori di token ANVL devono prima delegare i propri token per il voto.*

Governor Il governor, in questo caso, è definito dal proxy (EIP-1967 Transparent) **AnvilGovernorDelegator** di indirizzo:

0x00e83d0698FAf01BD080A4Dd2927e6aB7C4874c9

a cui è associato un contratto di implementazione **AnvilGovernorDelegate**, che attualmente risiede all'indirizzo:

0x123641B8A2063217A96EF88bF608931a43B49f49

ma che originariamente era distribuito all'indirizzo:

0xfe1118cE38818EA3C167929eacb6310CDc42a361

Entrambi i codici sono costruiti sulla base dello standard descritto dalle librerie di OneZeppelin. La loro struttura non presenta particolari differenze, infatti la ragione

³²⁸<https://docs.anvilapplication.com/governance/proposal-process>

principale per cui è stato creato il nuovo contratto è stata quella di permettere alla DAO di cambiare l'indirizzo del token che conferisce il diritto di voto.

Timelock Il contratto **AnvilTimelock** è definito all'indirizzo:

0x4eeB7c5BB75Fc0DBEa4826BF568FD577f62cad21

ha una struttura modulare ed è costruito sulla base delle librerie di OneZeppelin.

I parametri di governance della DAO e sono raccolti all'interno della Tabella 3.86.

<i>Parametro</i>	<i>Valore</i>
poposalThreshold	1.000.000.000 ANVL
poposalThreshold (teorico)	500.000.000 ANVL
$quorum = \frac{quorumNumerator}{quorumDenominator}$	10% della supply totale = 10.000.000.000 ANVL
quorum (teorico)	5% della supply totale = 5.000.000.000 ANVL
votingDelay	14400 blocchi (12s) = 2 giorni
votingPeriod	36000 blocchi (12s) = 5 giorni
getMindelay	604800s = 7 giorni

Tabella 3.86: Parametri di governance di Anvil

Gli indirizzi dei contratti che attualmente consentono il funzionamento del processo descritto sono raccolti nella Tabella 3.87.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
Anvil	0xAEEAa594e7dc112D67b8547fe9767a02c15B5597	governance token
AnvilGovernorDelegator	0x00e83d0698FAf01BD080A4Dd2927e6aB7C4874c9	governor proxy
AnvilGovernorDelegate	0x123641B8A2063217A96EF88bF608931a43B49f49	governor implem
AnvilTimelock	0x4eeB7c5BB75Fc0DBEa4826BF568FD577f62cad21	timelock
CollateralVault	0x5d2725fdE4d7Aa3388DA4519ac0449Cc031d675f	treasury

Tabella 3.87: Indirizzi degli contratti di governance di Anvil

Tesoreria La tesoreria è detenuta in un contratto differente definito all'indirizzo:

0x5d2725fdE4d7Aa3388DA4519ac0449Cc031d675f

Il volume degli asset in esso detenuti è pari a 39.738.879\$³²⁹.

3.42 TrueFi

TrueFi è un'infrastruttura modulare per il credito onchain che collega prestatori, mutuatari e gestori di portafoglio tramite smart contract governati dal token TRU³³⁰.



Figura 3.105: TrueFi Logo

L'obiettivo è aiutare i prestatori di criptovalute a godere di tassi di rendimento interessanti e sostenibili, offrendo al contempo ai mutuatari prestiti prevedibili che massimizzino il loro capitale circolante. TrueFi mira a creare un mercato dei prestiti in cui gli appassionati di DeFi possano mettere a disposizione fondi, garantiti o meno, come sicurezza per un prestito istantaneo con tassi di interesse molto bassi.

Tutte le funzioni su TrueFi sono completamente trasparenti per supportare prestatori e mutuatari nella gestione dei flussi di fondi durante l'utilizzo del progetto. Ecco come funziona il processo³³¹:

- **Fornitura di Liquidità:** Quando i prestatori aggiungono asset a una pool di prestito TrueFi, guadagnano interessi e TRU.

³²⁹10.02.2026,<https://debank.com/profile/0x5d2725fde4d7aa3388da4519ac0449cc031d675f>

³³⁰<https://docs.truefi.io/faq>

³³¹<https://coin98.net/what-is-truefi-tru>

- **Verifica del Mutuatario:** I mutuatari vengono quindi elaborati tramite una whitelist che esamina la loro situazione finanziaria, l'accordo firmato e l'approvazione della community.
- **Richiesta di Prestito:** Una volta completato il processo, la richiesta viene sottoposta ad approvazione, includendo il tasso di interesse, il limite di credito e il capitale concesso.
- **Votazione:** Il passaggio finale consiste nel sottoporre la domanda all'approvazione della community TRU, che voterà "Sì" o "No" sul prestito.
- **Accordo Legale:** Gli accordi di prestito sono contratti vincolanti tra prestatori e mutuatari. Il Mutuatario deve restituire il capitale concesso con gli interessi sul prestito. I termini di questi documenti stabiliscono cosa succede se una delle parti viola la propria parte dell'accordo; possono essere intraprese azioni legali per riscuotere il rimborso.

3.42.1 Token TRU

Il token nativo del sistema è TRU, un token ERC-20 il cui contratto è definito su Ethereum come proxy (EIP-897) all'indirizzo:

0x4C19596f5aAfF459fA38B0f7eD92F11AE6543784

mentre il contratto di implementazione corrispondente è definito all'indirizzo:

0x095527F5bEa113E9575B662c5ba01D990A280f2F



Figura 3.106: Token TRU

Il token nativo utilizzato in questo ecosistema alimenta tutte le transazioni all'interno del sistema "True Credit", che include ricompense per lo staking e diritti di

governance; questi ultimi permettono agli utenti di votare con i propri token sulle decisioni chiave che influenzano il futuro percorso di sviluppo del protocollo³³².

Il tetto massimo previsto dal protocollo per il token è di 1.450.000.000 TRU che coincide quasi perfettamente con l'offerta totale di 1.449.999.998,2 TRU. L'offerta circolante è invece pari a 1.435.338.064,34 TRU ³³³.

Per quanto riguarda il processo di governance on-chain però le decisioni effettive vengono prese mettendo in staking i propri token TRU ed ottenendo in cambio token StkTRU³³⁴. Il contratto corrispondente è definito come proxy (EIP-897) di indirizzo:

0x23696914Ca9737466D8553a2d619948f548Ee424

a cui corrisponde un contratto di implementazione con indirizzo:

0xBFE206c8eCd49751Bf7c9C8C1331738FC29F084d

Osservazione 3.23. *Il trasferimento di stkTRU modifica il potere di voto per le votazioni snapshot e on-chain esattamente della quantità di stkTRU trasferita.*³³⁵.

3.42.2 Processo di governance e analisi dei contratti

Il processo di governance di TruFi può essere schematizzato come in Figura 3.107³³⁶.

Le prime 3 fasi avvengono off-chain rispettivamente su: Discord³³⁷ (fase 1), Forum³³⁸ (Fase 2) e Snapshot³³⁹ (Fase 3). La fase 4 invece avviene on-chain interagendo direttamente con gli opportuni contratti di governance (i cui indirizzi e riferimenti sono riportati nella Tabella 3.89) e tramite l'appoggio della piattaforma Tally³⁴⁰.

³³²<https://coin98.net/what-is-truefi-tru>

³³³11.02.2026,<https://coinmarketcap.com/currencies/truefi-token/>

³³⁴<https://docs.truefi.io/faq/truefi-protocol/tru-token>

³³⁵<https://docs.truefi.io/faq/truefi-protocol/tru-token/stake>

³³⁶<https://truefi.io/>

³³⁷<https://discord.com/invite/3tMyMqyqDj>

³³⁸<https://forum.truefi.io/>

³³⁹<https://snapshot.org/#/truefi-dao.eth/>

³⁴⁰<https://www.tally.xyz/gov/truefi>

Governor Il contratto **DaoGovernor** è praticamente l'implementazione "da manuale" di un sistema di governance on-chain basato sulle librerie di OpenZeppelin ed è definito sulla rete Ethereum all'indirizzo:

0x585CcA060422ef1779Fb0Dd710A49e7C49A823C9

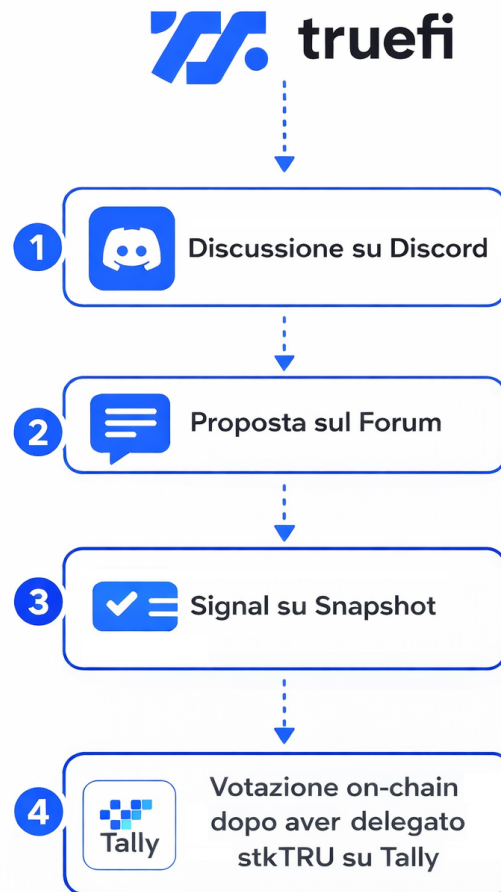


Figura 3.107: Processo di governance di TrueFi

Timelock Il **TimelockController** usato dalla DAO e definito all'indirizzo:

0x4f4AC7a7032A14243aEbDa98Ee04a5D7Fe293d07

contiene la copia esatta del file `TimelockController.sol` della libreria OpenZeppelin (versione 4.6.0).

All'interno di tali contratti vengono implementate le principali funzioni che consentono il processo descritto in precedenza e vengono inoltre definiti i principali parametri di governance che riportiamo in Tabella 3.88.

<i>Parametro</i>	<i>Valore</i>
poposalThreshold	100.000 stkTRU
$\text{quorum} = \frac{\text{quorumNumerator}}{\text{quorumDenominator}}$	15% della supply totale di stkTRU
votingDelay	13150 blocchi (13s circa) = 2 giorni
votingPeriod	19726 blocchi(13s circa) = 3 giorni
getMindelay	172800s = 2 giorni

Tabella 3.88: Parametri di governance di TrueFi

Tesoreria La tesoreria principale di TrueFi è individuata nel contratto di timelock già definito ma esiste anche un'ulteriore componente, che ha la funzione specifica di distributore di token. Complessivamente i due contratti detengono un volume di asset equivalente a 23.555\$³⁴¹.

Nella Tabella 3.89 sono riportati gli indirizzi dei principali contratti coinvolti nel processo di governance.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
Owned-UpgradeabilityProxy	0x23696914Ca9737466D8553a2d619948f548Ee424	governance token proxy
StkTruToken	0xBFE206c8eCd49751Bf7c9C8C1331738FC29F084d	governance token impl
TimeOwned-UpgradeabilityProxy	0x4C19596f5aAfF459fA38B0f7eD92F11AE6543784	system token proxy
TrueFi	0x095527F5bEa113E9575B662c5ba01D990A280f2F	system token impl
DaoGovernor	0x585CcA060422ef1779Fb0Dd710A49e7C49A823C9	governor
TimelockController	0x4f4AC7a7032A14243aEbDa98Ee04a5D7Fe293d07	timelock

Tabella 3.89: Indirizzi degli contratti di governance di TrueFi

³⁴¹11.02.2026<https://debank.com/profile/0x6151570934470214592aa051c28805cf4744bca7>,<https://debank.com/profile/0x4f4ac7a7032a14243aebda98ee04a5d7fe293d07>

3.43 PoolTogether

PoolTogether è un protocollo di risparmio a premi che permette di vincere semplicemente risparmiando. Ogni dollaro depositato offre una possibilità di vincere premi. Più risparmi, maggiori sono le probabilità di vittoria.



Figura 3.108: PoolTogether Logo

PoolTogether è una delle prime e più utilizzate applicazioni DeFi ed è attiva da oltre quattro anni. Dalla sua nascita, il protocollo ha distribuito oltre 10 milioni di dollari in premi ai depositanti. Il vincitore più fortunato finora ha depositato 74\$ vincendone oltre 40.000\$. Tutto questo è possibile perché i premi sono costituiti dagli interessi maturati su tutti i fondi depositati:

- Gli utenti depositano nella rete;
- Il rendimento matura su tutti i depositi;
- Il rendimento viene assegnato casualmente come premio agli utenti.

Il protocollo permette a chiunque di risparmiare. Offre condizioni di parità in cui ogni utente gode degli stessi termini.

Nessuno tranne il proprietario ha accesso ai fondi depositati. PoolTogether infatti è completamente non custodiale, il che significa che gli utenti possono riscattare il proprio denaro dalla pool in qualsiasi momento³⁴².

³⁴²<https://docs.pooltogether.com/>

3.43.1 Token POOL

Il token POOL controlla il protocollo PoolTogether per garantire la decentralizzazione e la proprietà comunitaria. I detentori dei token gestiscono i parametri del protocollo per promuoverne la crescita³⁴³. POOL è un token ERC-20 il cui contratto è definito sulla rete Ethereum all'indirizzo:

0x0cEC1A9154Ff802e7934Fc916Ed7Ca50bDE6844e



Figura 3.109: TokenPOOL

L'offerta totale di token POOL è di 10 milioni³⁴⁴.

- 4,8 milioni (48%) di questi token non sono stati distribuiti e sono controllati dalla governance.
- 5,2 milioni (52%) sono già stati distribuiti; i dettagli delle distribuzioni più significative sono i seguenti:
 - 1.500.000 POOL sono stati assegnati ai primi utenti del protocollo; di cui ~400.000 sono rimasti non reclamati nel contratto di distribuzione.
 - 1.200.000 POOL sono stati assegnati ai primi contributori del protocollo. Tali POOL sono soggetti a un blocco di un anno finito il 17 febbraio 2022.
 - 750.000 POOL sono stati assegnati agli investitori di PoolTogether Inc. Tali token sono soggetti a un blocco di un anno finito il 17 febbraio 2022.
 - 411.000 POOL sono stati distribuiti ai partecipanti alla diversificazione del protocollo. Questi token hanno un vesting di un anno con sblocco progressivo annuale iniziato a maggio 2022.

³⁴³<https://docs.pooltogether.com/pooltogether/pool-token>

³⁴⁴<https://docs.pooltogether.com/pooltogether/pool-token/pool-supply>

L'offerta totale di token al momento coincide con il tetto massimo previsto ed è 10.000.000 POOL. L'offerta attualmente in circolazione è invece pari a 6.768.510 POOL³⁴⁵.

3.43.2 Processo di governance e analisi dei contratti

Chiunque detenga o abbia delegato almeno 10.000 POOL può sottoporre una proposta alla governance di PoolTogether. Tutte le proposte devono essere presentate come uno dei tipi di proposta validi (PTIP - PoolTogether Improvement Proposal o PTBR - PoolTogether Budget Request) indicati di seguito e seguire il processo di proposta delineato di seguito³⁴⁶:

- Request for comments - RFC
- PTIP / PTBR
- Proposta on-chain

Request for comment (RFC) Tutte le discussioni principali dovrebbero iniziare sul forum di governance per essere esaminate da chiunque nella community di PoolTogether. Una volta inviata, la discussione sul forum dovrebbe rimanere aperta per il feedback della community per almeno 5 giorni. Se la proposta non ottiene un'approvazione esplicita, il proponente dovrebbe continuare a cercare feedback dalla community e presentare una proposta modificata. Se invece la proposta ha un forte sostegno, il proponente può creare il corrispondente PTIP/PTBR.

PTIP/PTBR Dopo aver applicato l'eventuale feedback della community alla proposta, il proponente crea una nuova discussione sul forum nella categoria appropriata dichiarando le modifiche apportate alla RFC iniziale nella proposta finale e lasciare l'argomento aperto per almeno 24 ore, prima di inviare la proposta on-chain.

³⁴⁵11.02.2026,<https://www.coingecko.com/en/coins/pooltogether>

³⁴⁶<https://docs.pooltogether.com/pooltogether/governance/proposal-process>

Proposta on-chain A questo punto il proponente deve creare una nuova proposta onchain, che corrisponda alle specifiche delineate nel post del forum. Dopo che una proposta è stata inviata on-chain, inizia un periodo di votazione³⁴⁷ di 5 giorni. Una proposta ha successo se, dopo cinque giorni:

- la maggioranza dei voti è a favore (soglia di approvazione del 51%)
- sono stati espressi almeno 100.000 voti a favore (quorum dell'1%).

Quando una proposta ha successo, il proponente (o qualsiasi altra persona) può metterla in coda, dopodichè c'è un timelock di due giorni prima che venga effettivamente implementata. Dopo la scadenza del timelock, la proposta può essere eseguita.

Osservazione 3.24. *Tutte le votazioni off-chain avvengono su Snapshot*³⁴⁸.

Governor Il governor inizialmente era definito dal contratto **GovernorAlpha** che è definito all'indirizzo:

0xB3a87172F555ae2a2AB79Be60B336D2F7D0187f0

il cui codice è uguale alla versione originale dello standard di governance introdotto da Compound Finance ed è stato adottato da PoolTogether nelle sue prime fasi. In seguito è stato sostituito dal **PoolTogetherGovernor** definito all'indirizzo:

0x8a907De47E00830a2b742db65e938a3ea1070A2E

il cui codice rappresenta un'evoluzione moderna e modulare del precedente basata sullo standard di OpenZeppelin.

Timelock Il contratto di timelock non ha invece subito variazioni ed è fin dall'inizio definito all'indirizzo:

0x42cd8312D2BCe04277dD5161832460e95b24262E

secondo lo standard di Compound Finance.

³⁴⁷<https://www.tally.xyz/gov/pooltogether>

³⁴⁸<https://snapshot.org/#/pooltogether.eth/>

I parametri relativi al processo di governance definiti nei precedenti contratti sono riportati nella Tabella 3.90.

<i>Parametro</i>	<i>Valore</i>
poposalThreshold	10.000 POOL
quorum	100.000 POOL
votingDelay	1 blocco $\sim$ pochi secondi $\rightarrow$ 7200 blocchi (15s) = 1 giorno
votingPeriod	28800 blocchi (15s) = 5 giorni
gracePeriod	1209600s = 14 giorni
minimumDelay	172800s = 2 giorni
maximumDelay	2592000s = 30 giorni
delay	172810s $\simeq$ 2 giorni
delay (teorico)	2 giorni

Tabella 3.90: Parametri del processo di governance di PoolTogether

Tesoreria La tesoreria è gestita dal contratto di timelock che detiene un volume di asset attualmente pari a 20.186\$³⁴⁹.

Gli indirizzi dei contratti analizzati sono raccolti in Tabella 3.91.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
Pool	0x0cEC1A9154Ff802e7934Fc916Ed7Ca50bDE6844e	token
PoolTogetherGovernor	0x8a907De47E00830a2b742db65e938a3ea1070A2E	governor
TimelockController	0x42cd8312D2BCe04277dD5161832460e95b24262E	timelock

Tabella 3.91: Indirizzi degli contratti di governance di PoolTogether

3.44 Seamless

Seamless Protocol è il primo protocollo di prestito decentralizzato e nativo su Base. Seamless pone le basi per la "Modern DeFi", concentrandosi su strategie di leva finanziaria automatizzate e una migliore esperienza utente per ispirare le masse.

³⁴⁹11.02.2026,<https://debank.com/profile/0x42cd8312d2bce04277dd5161832460e95b24262e>

Originariamente costruito su una fork di AAVE V3, Seamless ha optato per un "futuro senza piattaforma" migrando l'attività principale di prestito su Morpho. Seamless ha così eliminato i costi di gestione del proprio fork isolato e si è invece allineato con un livello base permissionless, modulare ed efficiente in termini di capitale.



Figura 3.110: Seamless Logo

Questo cambiamento consente al team di concentrarsi sulla costruzione di una nuova primitiva DeFi: i Leverage Token (LT). Gli LT prendono qualsiasi strategia DeFi e la "impacchettano" in un token ERC-20, consentendo agli utenti di accedere facilmente a strategie DeFi complesse semplicemente acquisendo un token. Gli LT rendono facile per gli utenti ottenere la leva finanziaria senza i problemi dell'intervento manuale e del monitoraggio continuo della posizione. Dietro le quinte, gli LT automatizzano transazioni che richiederebbero molto tempo ed eventi di ribilanciamento per mirare continuamente a un rapporto di leva stabilito³⁵⁰.

3.44.1 Token SEAM

Il token di governance e di utilità di Seamless Protocol è un token ERC-20 il cui contratto è un proxy distribuito sulla rete Base all'indirizzo:

0x1C7a460413dD4e964f96D8dFC56E7223cE88CD85

a cui corrisponden un implementazione definita all'indirizzo:

0x57b4b7f830244FC854cD1123ff14AFd4C1AEfd3F

³⁵⁰<https://docs.seamlessprotocol.com/>



Figura 3.111: SEAM Token

L'offerta totale di SEAM è di 100.000.000 di token di cui 46.346.837,77 SEAM sono attualmente in circolazione³⁵¹. La ripartizione generale è riportata di seguito³⁵²:

- Early Contributors 8%
- Early Advisors 3%
- Core Contributors & Advisors 11%
- Ecosystem Support & Foundation 20%
- Community - Incentives 13.5%
- Community - DAO - Liquidity Mining & Community Rewards 44.5%

3.44.2 Processo di governance e analisi dei contratti

Seamless protocol viene mantenuto, aggiornato e governato dalla community attraverso processi di governance sia offchain che onchain. Il token di governance nativo di Seamless Protocol, SEAM sulla rete Base, determina sia il potere di voto che i diritti di governance. Una volta delegati, questi token possono essere utilizzati per votare sulle proposte esistenti e per crearne di nuove relative a Seamless³⁵³. Il flusso del processo di proposta e voto prevede le seguenti fasi:

³⁵¹11.02.2026,<https://coinmarketcap.com/currencies/seamless/>

³⁵²<https://docs.seamlessprotocol.com/governance/seam-tokenomics>

³⁵³<https://docs.seamlessprotocol.com/governance/governance-overview>

Fase 1: Fase di ideazione Per inviare una proposta, si pubblica un post nel Seamless Governance Hub³⁵⁴. Prima dell'invio, cerca di condensare la tua proposta in un formato focalizzato e organizzato. Per rendere chiaro alla community quale tipo di proposta stai inviando, aggiungendo il prefisso opportuno al titolo della tua proposta tra: Protocol Changes Proposal (PCP), Governance Changes Proposal (GCP) o General Proposal (GP).

- Le Protocol Changes sono proposte relative a qualsiasi modifica dei parametri di rischio, l'aggiunta di nuovi mercati di asset, decisioni sul tasso di emissione dei token SEAM, ecc.
- Le Governance Changes riguardano le modifiche alle strutture di governance del protocollo più ampie, al formato, ai processi e alle soglie di quorum, e pertanto richiedono un margine più elevato di voti "A favore" per essere approvate.
- Le General Proposals sono utilizzate per varie iniziative offchain come ad esempio la nomina dei membri del comitato SCGP.

Dopo che una proposta è stata inviata al Seamless Governance Hub, i membri della community sono incoraggiati a commentare, discutere e porre domande. La durata predefinita per la fase di ideazione è di 5 giorni.

Osservazione 3.25. *Se il proponente lo ritiene necessario può richiedere un'estensione per una durata massima dell'estensione di ulteriori 5 giorni.*

Al termine della fase di ideazione, il proponente deve ripubblicare la proposta incorporando i feedback della comunità, quindi si aprirà una finestra temporale di 2 giorni (con possibilità di estensione) per una revisione finale della proposta e per affrontare eventuali contestazioni da parte della community.

Fase 2: Proposta inviata su Snapshot Labs (solo per le General Proposals)

Una volta pubblicata nel Seamless Governance Hub, se una proposta ottiene un interesse generale sufficiente, la proposta dovrebbe essere inviata tramite il portale

³⁵⁴<https://seamlessprotocol.discourse.group/c/newassets/8>

Snapshot Labs³⁵⁵ per ricevere una segnalazione precoce se le persone sono "A favore" (For) o "Contro" (Against) la modifica proposta. Le proposte su Snapshot hanno attualmente un periodo di voto aperto di 3 giorni. Il quorum è fissato a 1 milione di SEAM ed è richiesta una maggioranza semplice per essere considerata "approvata".

Fase 3: Fase di voto on-chain (SIP) Per le proposte che comportano modifiche agli smart contract (PCP o GCP), il passaggio successivo è inviare la proposta on-chain tramite l'interfaccia Tally³⁵⁶. Qualsiasi wallet con sufficiente potere di voto può creare una Seamless Improvement Proposal (SIP). L'attuale requisito di potere di voto per la Proposta è fissato allo 0,2% dell'offerta di token SEAM.

Fase 4: Fase del periodo di voto Il periodo di voto inizia dopo una finestra di 2 giorni e dura da 3 a 10 giorni a seconda della categoria della proposta:

- Protocol Changes - Periodo di voto di 3 giorni
- Governance Changes - Periodo di voto di 10 giorni

Durante il periodo di voto, solo i wallet con potere di voto delegato possono votare; questo include i wallet che hanno auto-delegato i propri token. Gli utenti che scelgono di delegare il loro potere di voto ad altri delegati non possono votare direttamente. Al termine del periodo di voto, una proposta ha successo se soddisfa le soglie:

- Protocol Changes: La proposta ha ricevuto un quorum di almeno 1.500.000 voti SEAM espressi ed un numero di voti a favore > numero di voti contro.
- Governance Changes: La proposta ha ricevuto un quorum di almeno 1.500.000 voti SEAM espressi ed un numero di voti a favore > 2x numero di voti contro.

Fase 5: Fase di Timelock Se il quorum viene raggiunto e il voto passa, il timelock esegue automaticamente il codice della proposta onchain. Il ritardo di esecuzione del timelock varia da 2 a 5 giorni a seconda della categoria della proposta:

³⁵⁵<https://snapshot.org/#/seamlessprotocol.eth>

³⁵⁶<https://www.tally.xyz/gov/seamless-protocol>

- Protocol Changes - Timelock di 2 giorni (48 ore)
- Governance Changes - Timelock di 5 giorni (120 ore)

Se il quorum non viene raggiunto o se il quorum viene raggiunto ma il voto non passa, la proposta inviata fallisce e il codice non viene eseguito.

Fase 6: Fase di esecuzione Dopo che la fase di Timelock è passata (2-5 giorni), qualsiasi utente sulla rete Base può eseguire la proposta. Questo attiverà l'esecuzione di tutto il codice eseguibile e le operazioni che erano contenute nella proposta.

Osservazione 3.26. *Nella tabella comparativa faremo riferimento alle proposte di tipo "protocol changes" poichè più comuni.*

I contratti di governance che attualmente consentono il funzionamento del seguente processo di governance sono riportati nella Tabella 3.92 e analizzati di seguito.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
ERC1967Proxy	0x1C7a460413dD4e964f96D8dFC56E7223cE88CD85	token proxy
Seam	0x57b4b7f830244FC854cD1123ff14AFd4C1AEfd3F	token implem
ERC1967Proxy	0x8768c789C6df8AF1a92d96dE823b4F80010Db294	governor proxy
SeamGovernorV2	0xC3A36d72bE57866EC4751D709b5bEF67efA9bAef	governor implem
ERC1967Proxy	0x639d2dD24304aC2e6A691d8c1cFf4a2665925fee	timelock proxy
SeamTimelockController	0x13F5B49217f330167D6350530F6185A75Ab35e6F	timelock proxy

Tabella 3.92: Indirizzi degli contratti di governance di Seamless

Governor Il contratto di governor è un proxy (EIP-1967 Transparent) di indirizzo:

0x8768c789C6df8AF1a92d96dE823b4F80010Db294

a cui inizialmente corrispondeva l'implementazione **SeamGovernor** di indirizzo:

0xC8A0E02878A4EF18fa260F0968cEcde8Eb607BFc

il cui codice estende lo standard Governor di OpenZeppelin, personalizzandolo per gestire la governance a doppio token (SEAM ed esSEAM). In seguito il contratto è stato sostituito dalla nuova versione **SeamGovernorV2** distribuita all'indirizzo:

0xC3A36d72bE57866EC4751D709b5bEF67efA9bAef

il cui codice è un aggiornamento diretto del contratto precedente la cui modifica principale è l'introduzione di un terzo asset nel calcolo del potere di voto stkSEAM.

Timelock Il **SeamTimelockController** è anch'esso un proxy (EIP-1967 Transparent) che ha indirizzo:

0x13F5B49217f330167D6350530F6185A75Ab35e6F

la cui implementazione di indirizzo:

0x639d2dD24304aC2e6A691d8c1cFf4a2665925fee

ed è fortemente basato sulle librerie OneZeppelin.

Nella Tabella 3.93 sono riportati i parametri di governance della DAO.

<i>Parametro</i>	<i>Valore</i>
poposalThreshold	200.000 SEAM
$\text{quorum} = \frac{\text{quorumNumerator}}{\text{quorumDenominator}}$	1,5% della supply totale
votingDelay	172800s = 2 giorni
votingPeriod PCP	259200s = 3 giorni
votingPeriod GCP	864000s = 10 giorni
getMinDelay	172800s = 2 giorni

Tabella 3.93: Parametri del processo di governance di Seamless

Tesoreria Il ruolo di tesoreria per Seamless DAO è affidato al contratto di timelock. All'interno di tale contratto è detenuto un valore di asset equivalente a 544.170,81\$³⁵⁷.

³⁵⁷11.02.2026, <https://www.tally.xyz/gov/seamless-protocol/treasury>

3.45 Antfarm

Antfarm è un protocollo di ribilanciamento on-chain costruito utilizzando l'architettura di un Exchange Decentralizzato (DEX), ma interamente dedicato ai Liquidity Provider (LP). Antfarm incarna lo spirito dell'innovazione decentralizzata, offrendo un approccio al ribilanciamento automatizzato (hands-off) che coltiva i tuoi investimenti per ottenere rendimenti costanti a lungo termine.



Figura 3.112: Antfarm Logo

Il protocollo, un fork perfezionato di Uniswap V2, si distingue per le sue commissioni distintamente elevate. Ciò permette ad Antfarm di funzionare come uno strumento di ribilanciamento automatico a tolleranza. Antfarm è costruito per fornire ai Liquidity Provider una compensazione equa per il rischio che si assumono³⁵⁸.

3.45.1 Token ATF ed AGT

ATF L'Antfarm Token (ATF) è un utility token ERC-20 utilizzato per pagare tutte le commissioni di scambio. Il suo contratto è definito all'indirizzo:

0x518b63Da813D46556FEa041A88b52e3CAa8C16a8

È stato introdotto per soddisfare le esigenze di tutti i diversi stakeholder dell'ecosistema grazie alla natura deflattiva (il 15% delle commissioni pagate viene bruciato dopo ogni swap) con cui il protocollo mira a proteggere i suoi possessori. Infatti con ogni "burn", il valore di ATF dovrebbe aumentare.

³⁵⁸<https://docs.antfarm.finance/>

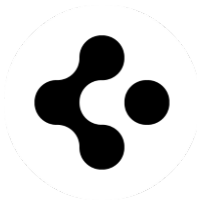


Figura 3.113: Token ATF

I Liquidity Provider (LP) possono riscattare le proprie commissioni in qualsiasi momento, senza alcun impatto sul valore o sul volume della pool, poiché tali commissioni sono pagate in token ATF³⁵⁹.

Il tetto massimo previsto dal protocollo per il token ATF è di 10.000.000 ATF. L'offerta totale è attualmente coincidente con quella in circolazione con un valore pari a 7.167.281 ATF³⁶⁰.

AGT L'AGT è invece il token di governance dell'ecosistema Antfarm; è un token ERC-20 il cui indirizzo sulla rete Ethereum è:

0x0BF43350076F95e0d16120b4D6bdfA1C9D50BDBD



Figura 3.114: Token AGT

Detenere AGT apre molte porte all'interno dell'ecosistema, inclusa la possibilità di far parte della DAO e di contribuire al miglioramento della piattaforma³⁶¹.

³⁵⁹<https://docs.antfarm.finance/strategy/antfarm-token-atf>

³⁶⁰11.02.2026, <https://www.coingecko.com/it/monete/antfarm-token>

³⁶¹<https://docs.antfarm.finance/dao/governance/antfarm-governance-token-agt>

L'allocazione dei 10.000.000 AGT (offerta massima prevista dal protocollo è stata gestita come segue:

- **Collaboratori principali:** Inizialmente deterranno il 40% dell'offerta totale. L'obiettivo a lungo termine sarà quello di distribuire questa porzione di AGT sul mercato per aumentare ulteriormente la decentralizzazione.
- **Programmi di incentivi:** Dal lancio, il 35% dell'offerta totale di AGT sarà suddiviso tra i fornitori di liquidità attraverso il programma di Liquidity Mining e gli staker di ATF attraverso il programma di ATF Staking. L'obiettivo di questi programmi di distribuzione è incentivare gli utenti a investire nell'ecosistema Antfarm, decentralizzando al contempo la DAO il più possibile.
- **Associazione legale:** L'entità legale che sostiene la DAO deterrà il 10% dell'offerta totale come tesoreria, per essere in grado di generare entrate e finanziare i servizi necessari (es. audit supplementari).
- **Riserva DAO:** Conserverà il 5% dell'offerta per creare le pool ATF/AGT.
- **Collaboratori e partner:** Coloro che collaborano con l'ecosistema Antfarm saranno ricompensati con i restanti per il loro lavoro, volto a migliorare l'esperienza complessiva e il prodotto.

Attualmente l'offerta totale coincide con l'offerta massima prevista dal protocollo ed è pari a 10.000.000 AGT mentre la porzione di token effettivamente in circolazione è pari a 4.200.000 AGT³⁶².

3.45.2 Processo di governance ed analisi dei contratti

La governance di Antfarm è il concetto centrale dell'intero ecosistema e la ragione d'essere della DAO. Essa è aperta a chiunque voglia contribuire all'ecosistema; è stata costruita per essere equa, trasparente e collaborativa. L'AGT, come anticipato, è il token che permette ai suoi titolari di far parte della DAO di Antfarm e di migliorare l'intero ecosistema.

³⁶²11.02.2026,<https://coinmarketcap.com/currencies/antfarm-governance-token/>

Per poter votare nella DAO di Antfarm, gli utenti devono mettere in staking e bloccare i propri token AGT in cambio di token veAGT il cui contratto è definito su Ethereum all'indirizzo:

0xDCd2B58585DF999DD145e529f09e8ACaFA6cd244

Ciò consentirà ai partecipanti di votare su tutte le proposte della DAO, dimostrando al contempo il proprio impegno a lungo termine per la crescita della piattaforma. I veAGT sono progettati per determinare il potere di voto di ogni partecipante all'interno della DAO e vengono concessi in un rapporto 1:1 per ogni AGT in staking.

La DAO di Antfarm utilizza Tally³⁶³ per le proposte e le votazioni³⁶⁴.

Osservazione 3.27. *Possedere AGT non è solo una questione di dovere, ma anche di ricompensa! Gli ATF accumulati dalla DAO vengono suddivisi tra i titolari di veAGT e la tesoreria della DAO per essere successivamente reinvestiti.*

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
AntfarmToken	0x518b63Da813D46556FEa041A88b52e3CAa8C16a8	utility token
AntfarmGovernanceToken	0x0BF43350076F95e0d16120b4D6bdfA1C9D50BDBD	token di governance
N\D	0xD63123527551F037fAAc74bf5fDA5B71569cf5af	governor
N\D	0x529C78Ee582e4293a20Ab60c848506eADd8723D8	timelock

Tabella 3.94: Indirizzi degli contratti di governance di Antfarm

Governor e timelock Gli indirizzi centrali che gestiscono il processo di governance della DAO sono due: il governor ed il timelock. I loro contratti sono stati distribuiti sulla rete Ethereum agli indirizzi riportati in Tabella 3.94, ma non è possibile al momento consultarne esplicitamente il codice di conseguenza i parametri di governance a cui faremo riferimento sono quelli riportati dalla piattaforma Tally. Tali parametri nello specifico sono riportati nella Tabella 3.95.

³⁶³<https://www.tally.xyz/gov/antfarm-dao>

³⁶⁴<https://docs.antfarm.finance/dao/governance>

<i>Parametro</i>	<i>Valore</i>
poposalThreshold	200.000 AGT
quorum	1.400.000 AGT
votingDelay	1 blocco ~ pochi secondi
votingPeriod	36.000 blocchi (12s) = 5 giorni

Tabella 3.95: Parametri del processo di governance di Antfarm

Tesoreria La gestione della tesoreria della DAO è affidata al contratto di timelock. Il volume degli asset detenuti è pari a 83.142\$³⁶⁵.

3.46 Summer.fi

Summer.fi è un'app progettata per semplificare e potenziare le interazioni degli utenti con il lending (prestito), il borrowing (accensione di prestiti) e la generazione di rendimento (yield generation). L'ecosistema è composto da entità separate e collaboratori che lavorano insieme per promuoverne la crescita e l'adozione³⁶⁶.



Figura 3.115: Logo Summer.fi

Per comprendere meglio Summer.fi, è importante distinguere tra le diverse aree e componenti della piattaforma. Queste distinzioni chiariscono come il protocollo operi, si evolva e interagisca con la sua community e la sua governance.

³⁶⁵[11.02.2026,https://debank.com/profile/0x529c78ee582e4293a20ab60c848506eadd8723d8](https://debank.com/profile/0x529c78ee582e4293a20ab60c848506eadd8723d8)

³⁶⁶<https://docs.summer.fi/>

Summer.fi è un frontend unificato che offre due prodotti distinti ma complementari:

- **Lazy Summer Protocol:** Un protocollo di lending passivo "hands-free" per un'ottimizzazione del rendimento senza sforzi.
- **Summer.fi Pro:** Un'app avanzata di lending, borrowing e earning per utenti DeFi più esperti.

3.46.1 Token SUMR

Il token SUMR è il token ERC-20 di governance del Summer Protocol. Il suo contratto ha indirizzo:

0x194f360D130F2393a5E9F3117A6a1B78aBEa1624



Figura 3.116: Token SUMR

I detentori di SUMR e i delegati costituiscono la Summer DAO, che supervisiona e governa il protocollo. La governance opera su un sistema di voto ponderato, in cui il numero di token SUMR posseduti determina il potere di voto. L'offerta totale che coincide con quella massima che è pari a 1.000.000.000 SUMR³⁶⁷ ed è stata distribuita come segue³⁶⁸:

- **Community (35%, 350M):** L'allocazione più consistente garantisce che la comunità rimanga la forza trainante di SUMR, premiando la partecipazione attiva e l'impegno.

³⁶⁷11.02.2026,<https://www.coingecko.com/it/monete/summer-2>

³⁶⁸<https://docs.summer.fi/lazy-summer-protocol/governance/usdsumr-token>

- Stakeholder Chiave e Partner Strategici (25%, 250M): Questi token sono riservati per rafforzare le collaborazioni e costruire un ecosistema resiliente attraverso partnership chiave.
- Core Contributors (20%, 200M): Dedicati agli sviluppatori, ai manutentori e ai collaboratori che alimentano l'evoluzione e l'innovazione del protocollo.
- Foundation (Sviluppo, Crescita dell'Ecosistema e Marketing) (20%, 200M): Riservati per finanziare lo sviluppo continuo, espandere l'ecosistema e guidare iniziative di crescita a lungo termine.

Con l'evolversi del protocollo è stato definito un nuovo contratto per il token di governance, ora rappresentato dai token SUMR messi in staking ovvero stkSUMR. L'indirizzo del contratto è:

`0x7cC488F2681cFC2A5E8A00184bfA94ea6d520D1c`

con questo contratto si consente ai detentori di SUMR di mettere in stake e, opzionalmente, bloccare (lock) le proprie posizioni per ricevere:

- Potere di governance (senza decadimento del potere di voto)
- Emissioni di SUMR (incentivi per la community)
- Ricompense dei vault denominate in USDC (provenienti dai ricavi del protocollo)

Chi effettua lo staking continua a partecipare alla governance attraverso il voto diretto o la delega. Lo Staking V2 unifica l'utilità del token attorno all'allineamento a lungo termine con il protocollo, a un potere di governance prevedibile e all'accesso alle ricompense a livello di protocollo³⁶⁹.

³⁶⁹<https://docs.summer.fi/lazy-summer-protocol/governance/usdsumr-token/staking>

3.46.2 Processo di governance e analisi dei contratti

Per partecipare alle decisioni di governance del Summer Protocol, si devono usare il forum³⁷⁰ ed la piattaforma di governance definita tramite la piattaforma Tally³⁷¹.

Affinché una proposta venga approvata, deve raggiungere un quorum. Il quorum per le proposte di governance è fissato al 15% della fornitura totale. Il periodo di votazione per le proposte generali dura 3 giorni, seguiti da un timelock di 24 ore per finalizzare la decisione e implementare le modifiche.

Sebbene non vi sia un periodo di attesa obbligatorio prima di avviare una votazione, i proponenti sono incoraggiati a discutere le proprie idee sul Forum di Governance.

Governor Come visto nel paragrafo sul token SUMR il protocollo di Lazy Summer sta sviluppando una nuova versione in cui è consentito usare stkSUMR come token di governance. Attualmente entrambi i contratti di governor sono attivi. Quello originale è definito all'indirizzo:

0xBE5A4DD68c3526F32B454fE28C9909cA0601e9Fa

mentre il governor **SummerGovernorV2** ha indirizzo:

0x4cEeE1b6289624d381383C1Bb42B118d5f2c3274.

Entrambi sono definiti in modo modulare secondo lo standard delle librerie di OneZeppelin. La principale differenza e la motivazione per cui è stato sviluppato il secondo contratto è consentire l'uso dei token in staking per le votazioni.

Timelock Il timelock della DAO è rimasto unico ed è implementato tramite lo standard delle librerie OneZeppelin all'indirizzo:

0x447BF9d1485ABDc4C1778025DfdfbE8b894C3796

³⁷⁰<https://forum.summer.fi/>

³⁷¹<https://www.tally.xyz/gov/lazy-summer-dao-official>,<https://www.tally.xyz/gov/lazy-summer-dao-official-v2>

Nella Tabella 3.96 riportiamo i parametri di governance definiti nei contratti precedenti (facendo in particolare riferimento al token SUMR).

<i>Parametro</i>	<i>Valore</i>
poposalThreshold	10.000 SUMR
$\text{quorum} = \frac{\text{quorumNumerator}}{\text{quorumDenominator}}$	15% della supply totale = 150.000.000 SUMR
votingDelay	86.400s = 7.200 blocchi (12s) = 1 giorno
votingPeriod	259.200s = 21.600 blocchi (12s) = 3 giorni
getMinDelay	86.400s = 1 giorni

Tabella 3.96: Parametri del processo di governance di Lazy Summer

Tesoreria La tesoreria della DAO è gestita dal contratto di timelock il quale detiene un volume di asset complessivo pari a 357.928,95\$³⁷².

Concludiamo infine l'analisi raccogliendo nella Tabella 3.97 tutti i contratti coinvolti nel processo di governance.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
SummerToken	0x194f360D130F2393a5E9F3117A6a1B78aBEa1624	token
SummerGovernor	0xBE5A4DD68c3526F32B454fE28C9909cA0601e9Fa	governor
StakedSummerToken	0x7cC488F2681cFC2A5E8A00184bfA94ea6d520D1c	staked token
SummerGovernorV2	0x4cEeE1b6289624d381383C1Bb42B118d5f2c3274	staked governor
SummerTimelockContoller	0x447BF9d1485ABDc4C1778025DfdfbE8b894C3796	timelock

Tabella 3.97: Indirizzi degli contratti di governance di Lazy Summer

3.47 RealToken

L'ecosistema RealToken è un'iniziativa comunitaria volta a innovare e sviluppare il settore dell'immobiliare tokenizzato, con RealT come attore principale. La missione è creare uno spazio collaborativo in cui idee, progetti e competenze si uniscano per plasmare il futuro del real estate tokenizzato.

³⁷²11.02.2026, <https://www.tally.xyz/gov/lazy-summer-dao-official/treasury>

La RealToken DAO mira a creare una comunità decentralizzata in cui i detentori di token REG possano partecipare a decisioni importanti riguardanti l'ecosistema di applicazioni decentralizzate (DApp) utilizzabili dai RealToken. L'idea è rendere l'investimento in asset del mondo reale il più accessibile, liquido e trasparente possibile, offrendo al contempo maggiori opportunità e casi d'uso agli investitori³⁷³.



Figura 3.117: RealToken Ecosystem Logo

Un utente può quindi partecipare alla governance della DAO possedendo REG, e investire acquistando RealToken. Le due attività sono indipendenti: non è necessario possedere RealToken per partecipare alla governance, così come non è necessario possedere REG per utilizzare i servizi della DAO³⁷⁴.

3.47.1 Token REG

Il token di governance REG è un token ERC-20 il cui scopo è unicamente legato alla partecipazione ai processi decisionali della governance.



Figura 3.118: Token REG

Il contratto del token è un proxy (EIP-1967 Transparent) con indirizzo su Gnosis:

`0x6382856a731Af535CA6aea8D364FCE67457da438`

la cui implementazione ha invece indirizzo:

³⁷³<https://wiki.realtoken.community/en/DAO>

³⁷⁴https://wiki.realtoken.community/en/DAO/DAO_RealToken

0xC6F2579D5D9D1697D86bc093a5328Eff03B3b010

I token di governance della DAO (RealToken Ecosystem Governance, REG) vengono creati in due fasi distinte³⁷⁵:

- Alla creazione della DAO (2024): per una quantità fissa di 500 milioni di token, suddivisi come segue³⁷⁶: il 86.5% sono stati distribuiti a varie porzioni dell'ecosistema; il 10% sono stati distribuiti al team ed il 3.5% sono stati utilizzati per il marketing.
- Durante la prima rivalutazione di un RealToken. In corrispondenza di tale evento un ammontare di USDREG (dollari convertibili in REG) viene assegnato ai detentori del RealToken rivalutato.

L'offerta totale attualmente è pari a 501.333.738 REG di cui solo 72.933.738 REG sono attualmente in circolazione³⁷⁷.

3.47.2 Processo di governance e analisi dei contratti

La RealToken DAO funziona come una comunità online dove i detentori di REG votano su decisioni importanti e propongono idee.

Gli step che si susseguono nel processo di governance della DAO sono i seguenti³⁷⁸:

- Sul forum³⁷⁹ della DAO, i membri possono proporre idee per migliorare la DAO e l'ecosistema;
- Viene avviato un dibattito sulle proposte per valutarne la fattibilità e l'interesse da parte della community;
- Se un'idea ottiene un consenso sufficiente, viene trasformata in una proposta formale e sottoposta al voto sulla piattaforma Tally³⁸⁰;

³⁷⁵<https://wiki.realtoken.community/en/DAO/Life/REG>

³⁷⁶<https://medium.com/realtplatform/token-economy-f0b935fe2777>

³⁷⁷11.02.2026,<https://coinmarketcap.com/currencies/realtoken-ecosystem-governance/>

³⁷⁸<https://wiki.realtoken.community/en/DAO/TechnicalOp>

³⁷⁹<https://forum.realtoken.community/>

³⁸⁰<https://www.tally.xyz/gov/realtoken-ecosystem-governance>

- I membri della DAO possono votare a favore o contro la proposta;
- Se la proposta viene approvata, viene eseguita dopo uno specifico ritardo.

I contratti utilizzati per gestire le fasi di tale processo on-chain sono i seguenti.

Governor Il contratto di governor di RealToken DAO è un proxy (EIP-1967 Transparent) di indirizzo:

0x4A5327347f077E72d2AaB19F68Ba8A7F12ec5d63

la cui implementazione ha indirizzo:

0x7B86888338D382D2aCD12a303F4224d217745FE0

Timelock Il timelock è a sua volta un proxy (EIP-1967 Transparent) di indirizzo:

0x3f2d192F64020dA31D44289d62DB82adE6ABee6c

la cui implementazione ha indirizzo:

0x431DD69503f5DAc4bD78be0Af215e184a8572f73

Entrambi i contratti sono definiti secondo lo standard delle librerie OneZeppelin.

Nella Tabella 3.98 riportiamo i parametri usati nel processo di governance implementati nei contratti precedenti i cui indirizzi sono tutti raccolti nella Tabella 3.99.

<i>Parametro</i>	<i>Valore</i>
proposalThreshold	100 REG
$\text{quorum} = \frac{\text{quorumNumerator}}{\text{quorumDenominator}}$	5% della supply bloccata = 167.050 REG
votingDelay	86.400s = 7.200 blocchi (12s) = 1 giorno
votingPeriod	604.800s = 50.400 blocchi (12s) = 7 giorni
getMinDelay	172.800s = 2 giorni

Tabella 3.98: Parametri del processo di governance di RealToken Ecosystem

Tesoreria Il contratto che gestisce la tesoreria della DAO è il contratto di timelock il quale detiene un volume pari a 3.307.027,70\$³⁸¹.

³⁸¹11.02.2026, <https://www.tally.xyz/gov/realtoken-ecosystem-governance/treasury>

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
ERC1967Proxy	0x6382856a731Af535CA6aea8D364FCE67457da438	token proxy
REGVotingPowerRegistry	0xC6F2579D5D9D1697D86bc093a5328Eff03B3b010	token implem
ERC1967Proxy	0x4A5327347f077E72d2AaB19F68Ba8A7F12ec5d63	governor proxy
REGGovernor	0x7B86888338D382D2aCD12a303F4224d217745FE0	governor implem
ERC1967Proxy	0x3f2d192F64020dA31D44289d62DB82adE6ABee6c	timelock proxy
REGTreasuryDAO	0x431DD69503f5DAc4bD78be0Af215e184a8572f73	timelock implem

Tabella 3.99: Indirizzi degli contratti di governance di RealToken Ecosystem

3.48 Fame Lady Society

Fondata l'11 dicembre 2022 la Fame Lady Society è una vivace community di collezionisti e creatori di NFT dedicati agli NFT originali della Fame Lady Squad (FLS), il pionieristico progetto di PFP generativi interamente femminili su Ethereum³⁸².



Figura 3.119: Fame Lady Society Logo

Con un forte focus sulla trasparenza, la governance comunitaria, l'inclusività e l'emancipazione femminile, la FLSoc mira a trasformare il Web3 in "webWE", promuovendo un ambiente collaborativo e solidale in cui ogni membro abbia voce in ca-

³⁸²<https://www.fameladysociety.com/fame>

pitolo nel plasmare il futuro del progetto, promuovendo una reale decentralizzazione e sostenibilità a beneficio dell'intera comunità.

3.48.1 Token FAME e gSOCIETY

FAME, un progetto rivoluzionario basato sullo standard DN-404 che presenta 888 splendidi NFT femminili, con una liquidità garantita da 888 milioni FAME³⁸³. FAME è gestita sia un token ERC-20 chiamato FAME, sia un NFT ERC-721 chiamato Society. Il contratto associato al token ERC-20 FAME è definito all'indirizzo:

0xf307e242BfE1EC1fF01a4Cef2fdaa81b10A52418

mentre il contratto degli NFT ERC-721 gSOCIETY è definito all'indirizzo:

0x12cf4e3B1a07DDAC4046B18714D6bAb9063De852



Figura 3.120: Token FAME

1 milione di FAME = 1 Society NFT (gSOCIETY)

Nel momento in cui si acquista 1 milione di FAME una delle rare ed esclusive Society Ladies verrà coniata direttamente nel proprio wallet. Vendendo una qualsiasi parte di quel milione di FAME l'NFT scomparirà.

Gli NFT della Society sono pezzi d'arte unici 1/1 che rappresentano l'audace HER-story (storia al femminile) della Fame Lady Society³⁸⁴.

³⁸³<https://www.fameladysociety.com/>

³⁸⁴<https://www.fameladysociety.com/fame>



Figura 3.121: Examples of NFTs gSOCIETY

Osservazione 3.28. *DN-404 (Divisible NFT) è un'evoluzione dello standard ERC-404 che permette una "fusione" fluida tra token fungibili e NFT.*

La distribuzione dei token FAME al lancio nel marzo 2024 è stata la seguente:

- 50% Liquidità bloccata.
- 23.5% Claim gratuito per i possessori di Fame Lady Society.
- 1.5% Claim gratuito per i possessori di Hunnys, Mermaid Power e Metavixen.
- 20% Allocazione per la prevendita, destinata a coloro che forniscono la liquidità iniziale. Soggetta a un periodo di blocco di 2 settimane per il 10% e un periodo di maturazione lineare di 90 giorni per il restante 90%.
- 5% Donazione al multisig del consiglio della community.

3.48.2 Processo di governance e analisi dei contratti

L'obiettivo primario della DAO FAMEus è decidere come utilizzare i token FAME non riscattati. La DAO sarà controllata dai possessori degli NFT Society. Sebbene spetti in ultima analisi alla DAO decidere come impiegare i fondi, l'aspettativa è che questi vengano utilizzati per promuovere gli obiettivi di FAME e della Fame Lady Society come ad esempio il finanziamento di progetti comunitari o l'incentivazione della liquidità. La DAO sarà controllata da un vero contratto di governor e da un contratto di timelock ad esso associato che saranno accessibile tramite Tally³⁸⁵.

³⁸⁵<https://www.tally.xyz/gov/fameus-dao>

Governor Il **FAMEusGovernor** è definito sulla rete Base all'indirizzo:

0xbB2BD06084aB8AB66f14CE33fc713093E0f1d8D8

secondo lo standard descritto dalle librerie OneZeppelin.

Timelock Secondo il medesimo standard è definito anche **FAMEusTimelock-Controller**, il cui indirizzo è:

0x08f0194e4ca54ebDF4C28cD06273053e0eDc2Da0

Nella Tabella 3.100 sono riportati i valori dei parametri di governance, mentre in Tabella 3.101 sono riportati tutti i contratti di governance.

<i>Parametro</i>	<i>Valore</i>
poposalThreshold	8 gSOCIETY
$\text{quorum} = \frac{\text{quorumNumerator}}{\text{quorumDenominator}}$	12.5% della supply esistente = 18 gSOCIETY
votingDelay	86.400s = 7.200 blocchi (12s) = 1 giorno
votingPeriod	259.200s = 21.600 blocchi (12s) = 3 giorni
getMinDelay	86.400s = 1 giorno

Tabella 3.100: Parametri del processo di governance di FAMEus DAO

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
Fame	0xf307e242BfE1EC1ff01a4Cef2fdaa81b10A52418	token ERC-20
GovSociety	0x12cf4e3B1a07DDAC4046B18714D6bAb9063De852	NFT gover
FAMEusGovernor	0xbB2BD06084aB8AB66f14CE33fc713093E0f1d8D8	governor
FAMEus TimelockController	0x08f0194e4ca54ebDF4C28cD06273053e0eDc2Da0	timelock

Tabella 3.101: Indirizzi degli contratti di governance di FAMEus DAO

Tesoreria La tesoreria della FAMEus DAO è gestita dal contratto di timelock, il quale detiene un volume di attet pari a 36.848\$³⁸⁶.

³⁸⁶12.02.2026,<https://debank.com/profile/0x08f0194e4ca54ebdf4c28cd06273053e0edc2da0>

3.49 RigoBlock

Rigoblock è un protocollo blockchain che permette a chiunque di creare e gestire una pool di token digitali. Si tratta di un protocollo aperto che gli sviluppatori possono utilizzare per costruire le proprie applicazioni per la gestione dei token.



Figura 3.122: RigoBlock Logo

Essendo una componente del quadro più ampio dello scambio aperto di valore, Rigoblock è progettato per consentire alle persone di creare applicazioni con costi di avvio minimi e per attrarre un ecosistema di sviluppatori e marketplace, contribuendo ulteriormente all'evoluzione e all'adozione di massa del protocollo³⁸⁷.

3.49.1 Token GRG

Il token centrale dell'ecosistema è il token ERC-20 GRG il cui contratto è stato distribuito sulla rete Ethereum nel novembre del 2018 all'indirizzo:

0x4FbB350052Bca5417566f188eB2EBCE5b19BC964



Figura 3.123: Token GRG

Il token GRG serve a tre scopi distinti: l'accesso al portale, l'accesso al meccanismo di incentivi e la governance.

³⁸⁷<https://rigoblock.com/assets/downloads/blue-paper.pdf>

La distribuzione iniziale ha previsto che 3.000.000 GRG, su un totale di 10.000.000 GRG, sono stati allocati al pubblico durante un periodo di contribuzione. I token invenduti sono invece stati bruciati. L'emissione di nuovi token è autonoma, completamente trasparente e interamente distribuita ai contributori del network in base alla loro importanza relativa, come definito nel modulo Proof-of-Performance³⁸⁸.

Attualmente l'offerta totale ha raggiunto i 7.414.890,71 GRG di cui 2.701.063 GRG sono effettivamente in circolazione³⁸⁹.

3.49.2 Processo di governance e analisi contratti

Il processo di governance di Rigoblock è regolato dall'interazione direttamente con gli smart contract di riferimento.

Il periodo di votazione inizia all'avvio della successiva epoca di staking dei GRG e dura 7 giorni. Se durante la votazione la proposta raggiunge una maggioranza qualificata assoluta (ovvero, lo stato è definitivo e non può essere modificato da ulteriori voti contrari), lo stato della proposta viene aggiornato a "Qualificata" e la transazione può essere eseguita a partire dal blocco successivo.

Il potere di voto in Rigoblock è equivalente allo stake attivo di GRG di un wallet. Affinché una proposta sia valida e venga pubblicata on-chain, è richiesto un potere di voto di almeno 100.000 GRG sulla mainnet di Ethereum e 40.000 GRG sui Layer 2. Un votante può esprimersi a favore, contro o astenersi. Una proposta richiede un quorum di almeno 400.000 GRG su Ethereum mainnet e 200.000 GRG sui L2. Per l'approvazione di una proposta sono necessari i due terzi dei voti favorevoli. I voti astenuti vengono conteggiati, ma non sono computati nel quorum né nel calcolo dei favorevoli/contrari³⁹⁰.

³⁸⁸<https://docs.rigoblock.com/readme-1/grg-token>

³⁸⁹12.02.2026,<https://coinmarketcap.com/currencies/rigoblock/>

³⁹⁰<https://docs.rigoblock.com/governance/rigoblock-governance>

Governor Il governor è definito tramite un proxy (EIP-1967 Transparent) di governance leggero che viene distribuito all'indirizzo:

0x5F8607739c2D2d0b57a4292868C368AB1809767a

Questo proxy detiene lo stato della governance e delega l'esecuzione a un contratto di implementazione della governance canonico che contiene la logica principale ed è definito all'indirizzo:

0xE5D8204f8335e9786ea7Ce382771B865fE73a304

La sua natura deterministica garantisce indirizzi coerenti tra le diverse chain, semplificando le implementazioni e le interazioni multichain.

La logica di voto è però separata in un contratto di strategia di voto distinto, specifico per ogni progetto che nel caso della mainnet di Ethereum è definito all'indirizzo:

0x6e1423CB6B0b72316f051fbc3B6Bc54ed5e584Dc

Ciò consente a ciascun progetto di definire le proprie regole riutilizzando al contempo il proxy e il livello di governance principale.

Timelock Non è presente un contratto di timelock. Una volta approvate le decisioni vengono eseguite immediatamente dal contratto si governor.

Nella Tabella 3.102 sono riportati i valori dei parametri di governance.

<i>Parametro</i>	<i>Valore</i>
poposalThreshold	105.000 GRG
quorum	420.000 GRG
votingPeriod	604800s = 50.400 blocchi (12s) = 7 giorni

Tabella 3.102: Parametri del processo di governance di RigoBlock

Tesoreria La tesoreria della DAO è gestita dal contratto **GrgVault** di indirizzo:

0xfbd2588b170Ff776eBb1aBbB58C0fbE3ffFe1931

il quale detiene un volume di asset pari a 108.703\$³⁹¹.

³⁹¹12.02.2026,<https://debank.com/profile/0xfbd2588b170ff776ebb1abbb58c0fbe3fffe1931>

Concludiamo l'analisi riportando nella Tabella 3.103 gli indirizzi dei contratti chiave coinvolti nel processo di governance.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
RigoToken	0x4FbB350052Bca5417566f188eB2EBCE5b19BC964	token
RigoblockGovernance Proxy	0x5F8607739c2D2d0b57a4292868C368AB1809767a	governor proxy
RigoblockGovernance	0xE5D8204f8335e9786ea7Ce382771B865fE73a304	governor implem
RigoblockGovernance Strategy	0x6e1423CB6B0b72316f051fbc3B6Bc54ed5e584Dc	governor strategy
GrgVault	0xfbd2588b170Ff776eBb1aBbB58C0fbE3ffFe1931	treasury

Tabella 3.103: Indirizzi degli contratti di governance di RigoBlock

3.50 Lisk

Il protocollo Lisk oggi è una macchina di esecuzione ad alte prestazioni che delega la sicurezza a Ethereum e la governance alla sua DAO, con un focus verticale verso la tokenizzazione di asset del mondo reale.



Figura 3.124: Lisk Logo

Lisk offre una rete Layer 2 (L2) economica, veloce e scalabile basata su Optimism (OP) e protetta da Ethereum in questo modo partecipa alla costruzione del futuro in cui ha sempre creduto, ovvero sviluppare un livello di base interoperabile e senza soluzione di continuità che offra un'esperienza utente eccellente, liquidità condivisa e transazioni economiche per garantire che web3 rivoluzioni la vita delle persone proprio come ha fatto web2 .

La missione del protocollo è quella di fornire ai fondatori di Web3 più interessante possibile per creare progetti e prodotti concreti nei mercati di forte crescita. Per farlo combinano finanziamenti e infrastrutture consentendo ai fondatori in Africa, Sud-Est Asiatico e America Latina si espandersi oltre le proprie regioni e competere a livello globale.

3.50.1 Token LSK

LSK è il token di governance dell'ecosistema Lisk. Mettendoli in staking, i membri guadagnare ricompense e ottenere potere di voto nella Lisk DAO per influenzare il modo in cui la tesoreria viene utilizzata per supportare gli sviluppatori e la crescita di prodotti del mondo reale in regioni chiave. Il contratto del token ERC-20 LSK è un proxy (EIP-1967 Transparent) definito all'indirizzo:

0x2eE6Eca46d2406454708a1C80356a6E63b57D404

la cui implementazione è invece definita all'indirizzo:

0x99137F8880fB38e770EB7eF3d68038bC673D58EF



Figura 3.125: Token LSK

L'offerta totale del token è pari a 400.000.000 LSK di cui 226.557.616,68 LSK sono attualmente in circolazione³⁹².

³⁹²12.02.2026,<https://coinmarketcap.com/currencies/lisk/>

3.50.2 Processo di governance e analisi dei contratti

Il progetto Lisk è governato dalla Lisk DAO³⁹³ e dalla Onchain Foundation³⁹⁴. La Onchain Foundation definisce la visione e la strategia del progetto insieme al team di Lisk, ne finanzia lo sviluppo ed è uno stakeholder nella Lisk DAO attraverso il delegato del Team Lisk. La Lisk DAO permette a ogni detentore di token LSK che mette in staking i propri token di partecipare alla governance on-chain del progetto Lisk. La Lisk DAO decide come spendere i fondi della sua tesoreria e può approvare proposte generali riguardanti i parametri del protocollo o la direzione del progetto³⁹⁵.

Tali decisioni vengono prese attraverso sequenze di proposte e votazioni che possono essere effettuate sulla piattaforma Tally. Le proposte possono essere di tipo:

- **Funding:** Una proposta per ricevere una determinata quantità di fondi a un indirizzo specifico. Se approvata, il destinatario riceve l'importo indicato.
- **General:** Proposte generali riguardanti i parametri del protocollo o la direzione del progetto in generale. Possono essere seguite dalla Onchain Foundation oppure no, a seconda della fattibilità e dei costi.

Per creare una proposta, il potere di voto del proponente deve essere di almeno 300.000 vpLSK, ovvero il valore corrispondente a 100.000 LSK bloccati per 2 anni. Affinché una proposta venga approvata, la somma dei voti 'sì' e 'astensione' deve raggiungere almeno 24.000.000 vpLSK, ovvero il valore corrispondente a 8.000.000 LSK bloccati per 2 anni. Inoltre, i 'sì' devono essere tassativamente superiori ai 'no'.

Governor Il contratto di governor è un proxy (EIP-1967 Transparent) di indirizzo:

0x58a61b1807a7bDA541855DaAEAEe89b1DDA48568

la cui implementazione è definita all'indirizzo:

0x18a0b8c653c291D69F21A6Ef9a1000335F71618e

³⁹³<https://www.tally.xyz/gov/lisk>

³⁹⁴<https://onchain.org/>

³⁹⁵<https://docs.lisk.com/docs-user/governance/overview/#proposals>

Timelock Il contratto di timelock ha invece indirizzo:

0x2294A7f24187B84995A2A28112f82f07BE1BceAD

Entrambi i contratti principali di governance sono definiti entrambi secondo lo standard OneZeppelin.

I parametri che definiscono il processo sono riportati in Tabella 3.104.

<i>Parametro</i>	<i>Valore</i>
poposalThreshold	300.000 vpLSK
quorum	24.000.000 vpLSK
votingDelay	0s
votingPeriod	1.209.600s = 100.800 blocchi (12s) = 14 giorni
getMinDelay	0s

Tabella 3.104: Parametri del processo di governance di Lisk

Tesoreria La tesoreria è gestita dal contratto di timelock il quale detiene un attuale volume di asset pari a 2.773.445\$³⁹⁶.

Concludiamo infinite l'analisi raccogliendo in Tabella 3.105 gli indirizzi dei contratti di governance della DAO di Lisk.

<i>Nome</i>	<i>Indirizzo</i>	<i>Label</i>
ERC1967Proxy	0x2eE6Eca46d2406454708a1C80356a6E63b57D404	token proxy
L2VotingPower	0x99137F8880fB38e770EB7eF3d68038bC673D58EF	token implem
ERC1967Proxy	0x58a61b1807a7bDA541855DaAEAEe89b1DDA48568	governor proxy
L2Governor	0x18a0b8c653c291D69F21A6Ef9a1000335F71618e	governor implem
TimelockController	0x2294A7f24187B84995A2A28112f82f07BE1BceAD	timelock

Tabella 3.105: Indirizzi degli contratti di governance di Lisk

³⁹⁶12.02.2026,<https://debank.com/profile/0x2294a7f24187b84995a2a28112f82f07be1bcead>

3.51 Comparazione finale

Identità e asset Il primo set di tabelle (Tabella 3.106 per le prime 25 DAO e Tabella 3.107 per le restanti) delinea il profilo generale dei progetti, classificandoli per categoria e blockchain di appartenenza, con un focus sulle caratteristiche del token come lo standard e la fornitura totale.

<i>Nome</i>	<i>Categoria</i>	<i>Chain</i>	<i>Token</i>	<i>Std</i>	<i>Total Supply</i>
Uniswap	Protocol	Ethereum	UNI	ERC-20	899.318.420
Arbitrum	Protocol	Arbitrum	ARB	ERC-20	10.000.000.000
Aave	Protocol	Ethereum	AAVE	ERC-20	16.000.000
Sky	Protocol	Ethereum	SKY	ERC-20	23.462.665.147
Curve	Protocol	Ethereum	CRV	ERC-20	2.348.641.387
Lido	Protocol	Ethereum	LDO	ERC-20	1.000.000.000
ENS	Protocol	Ethereum	ENS	ERC-20	100.000.000
DeXe	Protocol	Ethereum	DEXE	ERC-20	96.504.599
Compound	Protocol	Ethereum	COMP	ERC-20	10.000.000
Maple	Protocol	Ethereum	SYRUP	ERC-20	1.216.127.148
Wormhole	Protocol	Ethereum	W	ERC-20	10.000.000.000
Diva Staking	Protocol	Ethereum	DIVA	ERC-20	1.000.000.000
Braintrust	Protocol	Ethereum	BTRST	ERC-20	250.000.000
UMA	Protocol	Ethereum	UMA	ERC-20	127.586.834
POOH	Social	Ethereum	POOH	ERC-20	420.690.000.000.000
PoohCrew	Social	Ethereum	PHCR	ERC-721	405
Adventure Gold	Social	Ethereum	AGLD	ERC-20	92.810.001
Degen Dogs	Investment	Polygon	DOG	ERC-721	201
Dope Wars	Grant	Ethereum	DOPE	ERC-721	8.000
Hop	Protocol	Ethereum	HOP	ERC-20	1.000.000.000
onchainaustria	Protocol	Arbitrum	OCA	ERC-20	100.000.000
Rarible	Protocol	Rari Chain	RARI	ERC-20	25.000.000
Inverse	Protocol	Ethereum	INV	ERC-20	727.000
Public Nouns	Grant	Ethereum	ⓅNOUN	ERC-721	293
Unlock	Protocol	Base	UP	ERC-20	1.000.000.000

Tabella 3.106: Identificazione delle 50 DAO: Da 1 a 25

<i>Nome</i>	<i>Categoria</i>	<i>Chain</i>	<i>Token</i>	<i>Std</i>	<i>Total Supply</i>
Hifi	Protocol	Ethereum	HIFI	ERC-20	141.982.603
Fluence	Protocol	Ethereum	FLT	ERC-20	1.000.000.000
Gitcoin	Grant	Ethereum	GTC	ERC-20	100.000.000
GMX	Grant	Arbitrum	GMX	ERC-20	10.385.273
Tornado Cash	Protocol	Ethereum	TORN	ERC-20	9.999.997
Kyber	Protocol	Ethereum	KNC	ERC-20	240.892.876
Audius	Protocol	Ethereum	AUDIO	ERC-20	1.394.975.804
Ampleforth	Protocol	Ethereum	FORTH	ERC-20	15.297.897
Radworks	Protocol	Ethereum	RAD	ERC-20	99.998.580
Idle	Protocol	Ethereum	IDLE	ERC-20	13.000.000
HAI	Protocol	Optimism	KITE	ERC-20	854.764
Union	Protocol	Ethereum	UNION	ERC-20	10.000.000.000
OpenDollar	Protocol	Arbitrum	ODG	ERC-20	10.000.000
Cryptex	Protocol	Ethereum	CTX	ERC-20	10.000.000
Threshold Network	Protocol	Ethereum	T	ERC-20	11.155.000.000
Anvil	Protocol	Ethereum	ANVL	ERC-20	100.000.000.000
TrueFi	Protocol	Ethereum	TRU	ERC-20	1.449.999.998
PoolTogether	Protocol	Ethereum	POOL	ERC-20	10.000.000
Seamless	Protocol	Base	SEAM	ERC-20	100.000.000
Antfarm	Protocol	Ethereum	AGT	ERC-20	7.167.281
Summer.fi	Investment	Base	SUMR	ERC-20	1.000.000.000
RealToken	Social	Gnosis	REG	ERC-20	501.333.738
FAMEus	Social	Base	gSOCIETY	ERC-721	144
RigoBlock	Investment	Ethereum	GRG	ERC-20	7.414.890,71
Lisk	Protocol	Lisk	LSK	ERC-20	400.000.000

Tabella 3.107: Identificazione delle 50 DAO: Da 26 a 50

Parametri di governance Il secondo set di tabelle (Tabella 3.108 per le DAO da 1 a 25 e Tabella 3.109 per le DAO da 26 a 50) entra nel dettaglio dei processi decisionali, confrontando le soglie di partecipazione e le tempistiche operative che regolano il voto e l'esecuzione delle proposte. Per garantire l'omogeneità dei dati, sono stati adottati i seguenti criteri:

- **Threshold e Quorum:** sono espressi in unità di token di governance. Nei casi in cui i valori originali fossero forniti in percentuale, è stato calcolato il

corrispondente valore assoluto per rendere i dati direttamente confrontabili.

- **Voting Delay (VD) e Voting Period (VP):** sono misurati in blocchi. Nei casi in cui il contratto di una DAO li definisse in secondi, è stata effettuata una conversione ipotizzando una durata media di 12 secondi per blocco.
- **Timelock Delay (Delay):** è indicato in secondi, in conformità con la convenzione standard di gestione dei ritardi di esecuzione.

<i>Nome</i>	<i>Threshold</i>	<i>Quorum</i>	<i>VD</i>	<i>VP</i>	<i>Delay</i>
Uniswap	1.000.000	40.000.000	13.140	40.320	172.800
Arbitrum	1.000.000	300.000.000	21.600	100.800	259.200
Aave	80.000	320.000	7.200	19.200	86.400
Sky	N\D	240.000.000	N\D	17.280	86.400
Curve	2.500	236.586.338	N\D	50.400	N\D
Lido	1.000	50.000.000	7.200	36.000	259.200
ENS	100.000	1.000.000	1	45.818	172.800
DeXe	10.000	49.217.345	N\D	36.000	1.800
Compound	25.000	400.000	13.140	19.710	172.800
Maple Finance	N\D	N\D	N\D	N\D	259.200
Wormhole	1.000.000	350.000.000	14.400	36.000	345.600
Diva Staking	1.000.000	10.000.000	14.400	36.000	777.600
Braintrust	500	100.000	1	17.280	604.800
UMA	4.000	5.000.000	N\D	7.200	7.200
POOH	420.690.000.000	1.682.760.000.000	1	50.400	259.200
PoohCrew	2,025	40.5	7.200	28.800	172.800
Adventure Gold	100	20.253,35	21.600	50.400	604.800
Degen Dogs	0,5025	40,2	1	12.667	86.400
Dope Wars	50	500	13.091	45.818	60
Hop	1.000.000	3.000.000	1	45.818	172.800
onchainaustria	10.000	10.000.000	900	50.400	N\D
Rarible	5.000	2.500.000	0	36.000	172.800
Inverse	1.900	15.500	1	17.280	172.800
Public Nouns	2,93	29,3	19.938	26.585	172.800
Unlock	50.000	3.000.000	28.800	43.200	172.800

Tabella 3.108: Parametri di governance delle 50 DAO: Da 1 a 25

<i>Nome</i>	<i>Threshold</i>	<i>Quorum</i>	<i>VD</i>	<i>VP</i>	<i>Delay</i>
Hifi	50.000	2.839.652	13.140	36.000	172.800
Fluence	10.000.000	40.000.000	7.200	36.000	432.000
Gitcoin	150.000	2.500.000	13.140	40.320	172.800
GMX	30.000	397.500	7.200	36.000	86.400
Tornado Cash	1.000	25.000	6	36.000	172.800
Kyber	N\D	9.635.715	N\D	28.800	43.200
Audius	N\D	306.419	N\D	21510	86.400
Ampleforth	75.000	600.000	13.140	19.710	172.800
Radworks	1.000.000	4.000.000	7.200	17.280	172.800
Idle	130.000	520.000	100	17.280	172.800
HAI	5.000	8.548	3.600	10.800	86.400
Union	10.000.000	40.000.000	7.200	21.600	86.400
OpenDollar	5.000	20.000	3.600	14.400	86.400
Cryptex	100.000	400.000	1	17.280	259.200
Threshold Network	2.887.500	17.325.000	13.292	50.000	172.800
Anvil	1.000.000.000	10.000.000.000	14.400	36.000	604.800
TrueFi	100.000	7.830.000	13.150	19.726	172.800
PoolTogether	10.000	100.000	7.200	28.800	172.800
Seamless	20.000	1.500.000	14.400	21.600	172.800
Antfarm	200.000	1.400.000	1	36.000	N\D
Summer.fi	10.000	150.000.000	7.200	21.600	86.400
RealToken	100	167.050	7.200	50.400	172.800
FAMEus	8	18	7.200	21.600	86.400
RigoBlock	105.000	420.000	N\D	50.400	N\D
Lisk	300.000	24.000.000	0	100.800	0

Tabella 3.109: Parametri di governance delle 50 DAO: Da 26 a 50

Gestione finanziaria e contratti L'ultimo set di tabelle (Tabella 3.110 per le prime 25 e Tabella 3.109 per le restanti) analizza la solidità economica e l'infrastruttura di controllo, riportando il volume della tesoreria (il cui valore è riportato in dollari), i meccanismi di gestione dei fondi e la tipologia di contratto di governator adottata.

<i>Nome</i>	<i>Tesoreria</i>	<i>Meccanismo</i>	<i>Governor Proxy</i>
Uniswap	1.062.003.690	Timelock	EIP-897 Delegate
Arbitrum	358.525.287	FixedDelegateWallet	EIP-1967 Transparent
Aave	150.900.000	Mixed	EIP-1967 Transparent
Sky	148.244.171	Spells	None
Curve	2.716.246	Vesting contract	EIP-897 Delegate
Lido	136.468.142	Agent	EIP-897 Delegate
ENS	67.729.999	Timelock	None
DeXe	107.437.788	Autonomous Treasury	EIP-1967 Beacon
Compound	104.072.902	Timelock	EIP-1967 Transparent
Maple Finance	10.431.558	GnosisSafe	N\D
Wormhole	N\D	N\D	None
Diva Staking	N\D	Timelock	None
Braintrust	1.460.963,90	Timelock	None
UMA	17.757.162	Governor	None
POOH	22.280,27	Timelock	None
PoohCrew	N\D	Timelock	EIP-1967 Transparent
Adventure Gold	3.313.900	Timelock	None
Degen Dogs	24,2	Timelock	EIP-897 Delegate
Dope Wars	19.125,89	Timelock	None
Hop	392.566,58	Timelock	None
onchainaustria	N\D	N\D	EIP-1967 Transparent
Rarible	12.071	Timelock	EIP-1967 Transparent
Inverse	1.607.234	Timelock	None
Public Nouns	21.936	Timelock	EIP-897 Delegate
Unlock	101.483,85	Timelock	EIP-1967 Transparent

Tabella 3.110: Gestione finanziaria e contratti delle 50 DAO: Da 1 a 25

<i>Nome</i>	<i>Tesoreria</i>	<i>Meccanismo</i>	<i>Governor Proxy</i>
Hifi	N\D	N\D	EIP-897 Delegate
Fluence	3.926.174	GnosisSafe	EIP-1967 Transparent
Gitcoin	1.758.677,00	Timelock	None
GMX	22.259.325	Timelock	None
Tornado Cash	60.203.020	Governor/Timelock	EIP-1967 Trasparent
Kyber	364.902	MultiSigWallet	None
Audius	4.619	Governor/Timelock	EIP-1967 Transparent
Ampleforth	6.873.542	Timelock	EIP-897 Delegate
Radworks	12.137.259	Timelock	None
Idle	102.900	GnosisSafe	EIP-897 Delegate
HAI	544.208,10	GnosisSafe	None
Union	355.993,06	Drip Treasury	None
OpenDollar	4.302.299,83	Timelock	None
Cryptex	740.084,87	Timelock	None
Threshold Network	1.798.498	Timelock	None
Anvil	39.738.879	Vault	EIP-1967 Transparent
TrueFi	23.555	Timelock	None
PoolTogether	20.186	Timelock	None
Seamless	544.170,81	Timelock	EIP-1967 Transparent
Antfarm	83.142	Timelock	N\D
Summer.fi	357.928,95	Timelock	None
RealToken	3.307.027,70	Timelock	EIP-1967 Transparent
FAMEus	4.116	Timelock	None
RigoBlock	108.703	Vault	EIP-1967 Transparent
Lisk	2.773.445	Timelock	EIP-1967 Transparent

Tabella 3.111: Gestione finanziaria e contratti delle 50 DAO: Da 26 a 50

Capitolo 4

Risultati

Il presente studio offre una panoramica quantitativa su un campione di 50 DAO, analizzandone la composizione strutturale e le scelte tecnologiche sottostanti.

4.1 Statistiche descrittive

Attraverso l'esame della distribuzione per categoria, blockchain di riferimento e standard dei token utilizzati, l'analisi mira a delineare i trend strutturali attuali nel settore della governance decentralizzata.

4.1.1 Distribuzione per categoria

La seguente tabella Tabella 4.3 e il relativo grafico Figura 4.1 illustrano la ripartizione numerica e percentuale delle DAO analizzate in base alla categoria di appartenenza.

<i>Categoria</i>	<i>Conteggio</i>	<i>Percentuale</i>
Protocol	39	78%
Social	5	10%
Grant	3	6%
Investment	3	6%

Tabella 4.1: Distribuzione per categoria

I dati raccolti mostrano che il campione di 50 DAO è composto per il 78% da progetti appartenenti alla categoria Protocol. Le restanti organizzazioni sono suddivise tra la categoria Social (10%), seguita da Investment (6%) e Grant (6%, 3 unità). La categoria Collector invece non presenta occorrenze nel dataset analizzato.

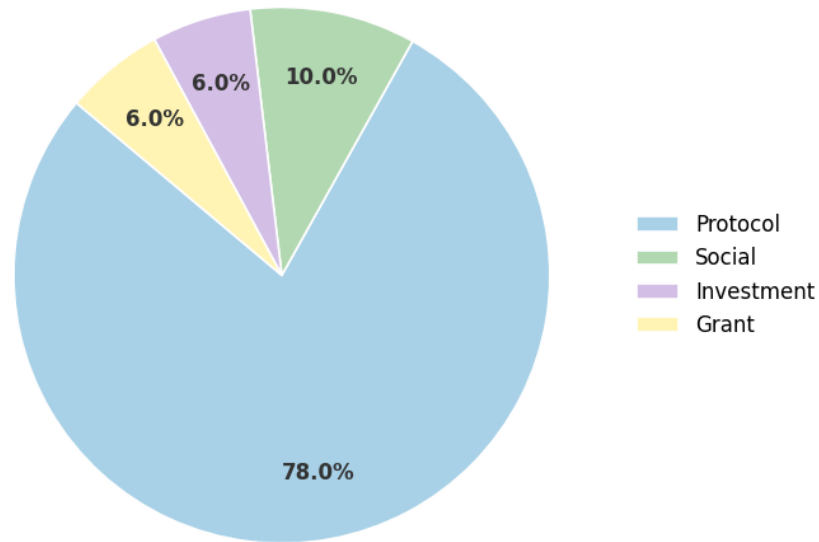


Figura 4.1: Distribuzione per categoria

4.1.2 Distribuzione per Blockchain

In questa sezione viene analizzata la distribuzione delle DAO sulle diverse infrastrutture blockchain, soluzioni Layer-2 e sidechain. Il grafico (Figura 4.2) permette di confrontare il numero di progetti ospitati su ciascuna rete del dataset (Tabella 4.2).

<i>Chain</i>	<i>Conteggio</i>	<i>Percentuale</i>
Ethereum	37	74%
Arbitrum One	4	8%
Base	4	8%
Polygon, Optimism, Lisk, Gnosis, RariChain	1	2% (ognuna)

Tabella 4.2: Distribuzione per categoria

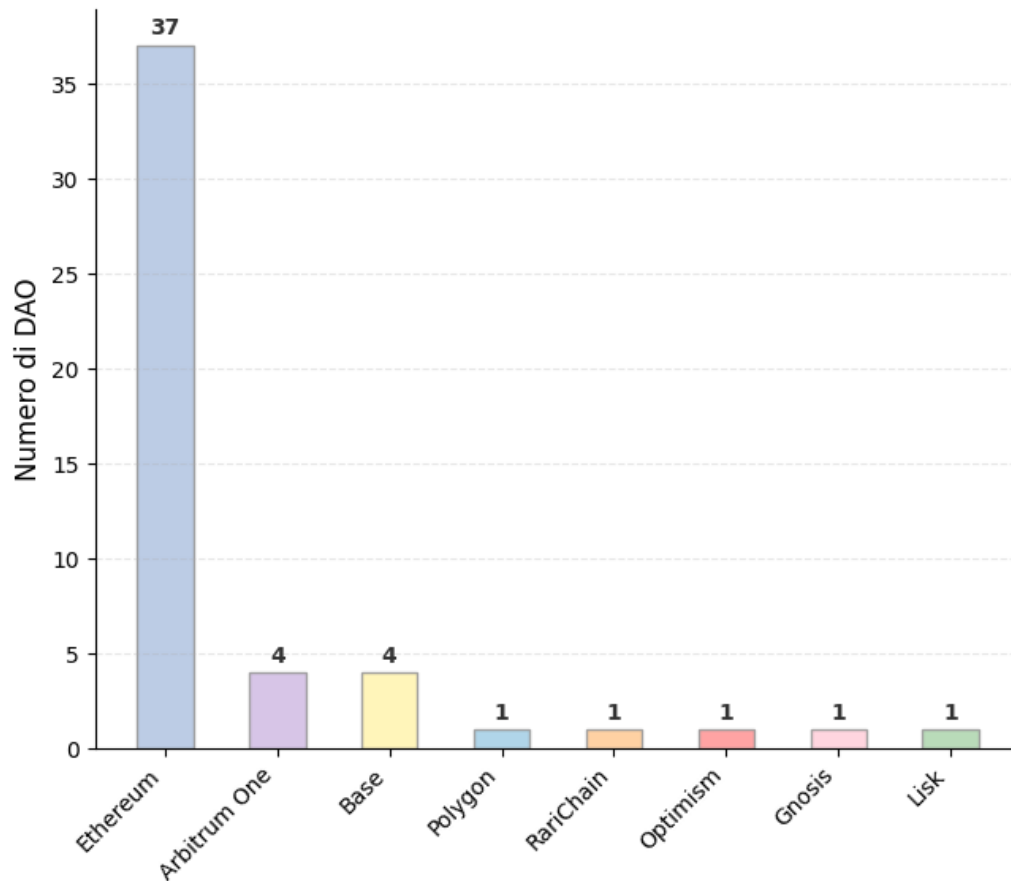


Figura 4.2: Distribuzione per blockchain\layer

L'analisi delle infrastrutture rivela che la maggior parte (74%) delle DAO opera sulla rete Ethereum. Il resto del campione è distribuito tra diverse soluzioni di secondo livello (Layer 2) e sidechain, tra cui si distinguono per frequenza Arbitrum One (8%) e Base (8%). Sono presenti anche occorrenze isolate su altre reti come Polygon, RariChain, Optimism, Gnosis e Lisk (2% ognuna).

4.1.3 Distribuzione per token standard

La tabella sottostante riporta la suddivisione delle DAO in base allo standard tecnico utilizzato per l'emissione dei propri token di governance. Il dato riflette le scelte

tecnologiche adottate per la gestione dei diritti di voto. In merito alle specifiche

<i>Token Standard</i>	<i>Conteggio</i>	<i>Percentuale</i>
ERC-20	45	90%
ERC-721	5	10%

Tabella 4.3: Distribuzione token standard

tecniche dei token di governance, il 90% del campione (45 DAO) utilizza lo standard ERC-20. Il restante 10% (5 DAO) adotta invece lo standard ERC-721. Non sono stati rilevati altri standard di token all'interno del dataset analizzato.

4.2 Analisi parametri di governance

Passiamo ora all'analisi dei parametri di governance. In questa sezione esamineremo le regole fondamentali che determinano come una proposta viene presentata, votata ed eseguita all'interno delle DAO. L'analisi si concentra su cinque metriche chiave: Threshold, Quorum, Voting Delay, Voting Period e Timelock Delay.

4.2.1 Statistiche sull'intero campione

Nella Tabella 4.4 sono riportate le statistiche descrittive per l'intero campione, escludendo per ogni parametro le DAO per cui l'informazione specifica non è disponibile.

<i>Parametro</i>	<i>Media</i>	<i>Mediana</i>	<i>Min</i>	<i>Max</i>	<i>Dev.Std</i>	<i>N.DAO</i>
Threshold	$9,17 \cdot 10^9$	40.000	0,5	$4,21 \cdot 10^{11}$	$6,20 \cdot 10^{10}$	46
Quorum	$3,46 \cdot 10^{10}$	2.500.000	18	$1,68 \cdot 10^{12}$	$2,40 \cdot 10^{11}$	49
Voting Delay	8.147,3	7.200	0	28.800	7.296,7	42
Voting Period	33.853,7	36.000	7.200	100.800	18.788,9	49
Timelock Delay	200.681,3	172.800	0	777.600	165.517,7	45

Tabella 4.4: Statistiche descrittive parametri di governance

Threshold e quorum L'aspetto più evidente è l'enorme divario tra la media e la mediana per Threshold e Quorum. La media infatti è pesantemente influenzata da pochi outlier presenti nel campione. La mediana (40.000 per il Threshold e 2.500.000 per il Quorum) rappresenta molto meglio un modello standard di DAO.

Voting Delay La mediana di 7.200 blocchi (circa 24 ore per blocchi della durata di 12s) indica una tendenza a lasciare un giorno di "riflessione" o di preparazione tecnica prima che la votazione diventi attiva.

Voting Period La media (33.853 blocchi) e la mediana (36.000 blocchi) sono molto vicine. Considerando che su Ethereum 36.000 blocchi corrispondono a circa 5 giorni, usando come convenzione la creazione di un blocco ogni 12s, emerge chiaramente come questo rappresenti lo standard più comune per dare ai votanti il tempo necessario di analizzare le proposte.

Timelock Delay Il Timelock Delay presenta una mediana di 172.800 secondi, che corrispondono esattamente a 48 ore. La deviazione standard elevata indica però che alcune DAO prolungano il ritardo fino a una settimana (max 777.600s), mentre altre (min 0) preferiscono l'esecuzione immediata, sacrificando la sicurezza per la rapidità.

4.2.2 Confronto statistiche tra categorie diverse

Le tabelle seguenti (Tabella 4.5, Tabella 4.6) riportano i parametri di governance suddividendo il campione per categoria, permettendo di identificare le diverse strategie gestionali adottate dai vari tipi di DAO.

<i>Categoria</i>	<i>Threshold</i>	<i>Quorum</i>	<i>Vot. Delay</i>	<i>Vot. Period</i>	<i>Timelock</i>
Protocol	$2,94 \cdot 10^7$	$3,01 \cdot 10^8$	7.675	33.153	206.177
Social	$8,41 \cdot 10^{10}$	$3,36 \cdot 10^{11}$	8.640	40.320	259.200
Grant	50.017	833.509	15.389	37.574	115.220
Investment	38.333	50.140.010	3.600	28.222	86.400

Tabella 4.5: Medie parametri per categorie

<i>Categoria</i>	<i>Threshold</i>	<i>Quorum</i>	<i>Vot. Delay</i>	<i>Vot. Period</i>	<i>Timelock</i>
Protocol	75.000	3.000.000	7.200	36.000	172.800
Social	100	20.253	7.200	50.400	172.800
Grant	50	500	13.140	40.320	172.800
Investment	10.000	420.000	3.600	21.600	86.400

Tabella 4.6: Mediane parametri per categorie

Per ciascun parametro di governance sono inoltre stati elaborati dei boxplot per che permettono di confrontare visivamente l'estensione dei valori all'interno delle diverse categorie, evidenziando non solo la tendenza centrale, ma anche la variabilità e gli outlier che caratterizzano i modelli di governance più estremi.

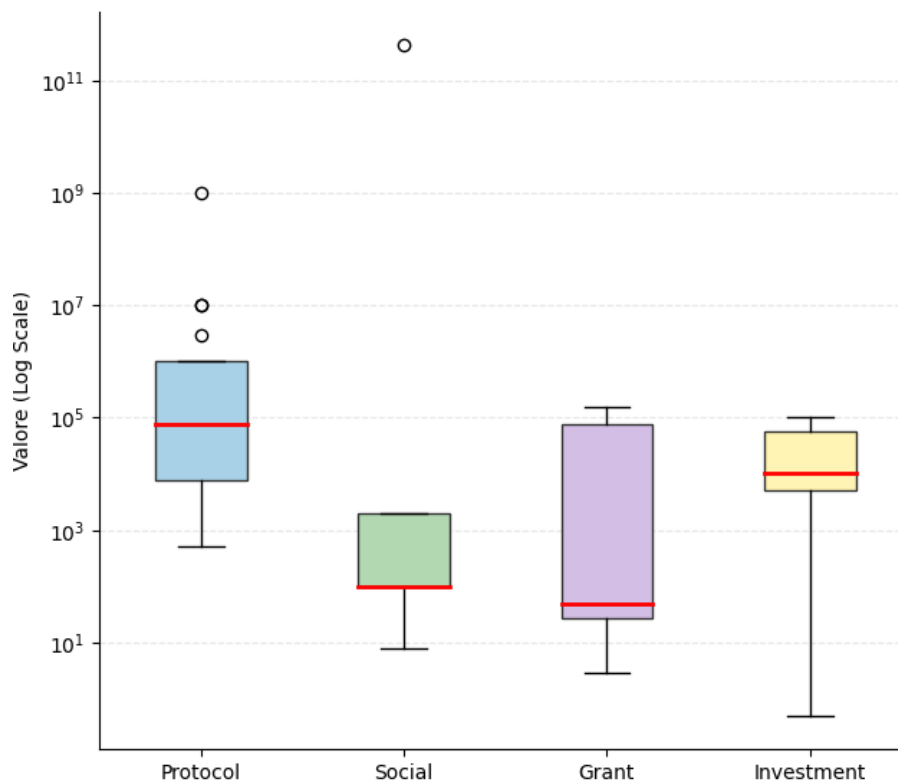
Threshold Figura 4.3

Figura 4.3: Distribuzione per categoria del Threshold

Confronto media e mediana: In tutte le categorie si osserva una marcata differenza tra media e mediana. In particolare, nella categoria Social, a fronte di una mediana di 100 unità, la media raggiunge $8,41 \cdot 10^{10}$, indicando una distribuzione fortemente asimmetrica verso destra con la presenza di outlier di magnitudo estrema.

Confronto tra le mediane delle categorie: La categoria Protocol presenta la mediana più elevata (75.000), seguita da Investment (10.000). Le categorie Grant (50) e Social (100) mostrano i valori mediani più bassi del campione.

Variabilità: Il boxplot (in scala logaritmica) evidenzia come la categoria Protocol presenti il range interquartile più ampio, segnalando una maggiore eterogeneità interna nei requisiti di accesso alla governance.

Quorum Figura 4.4

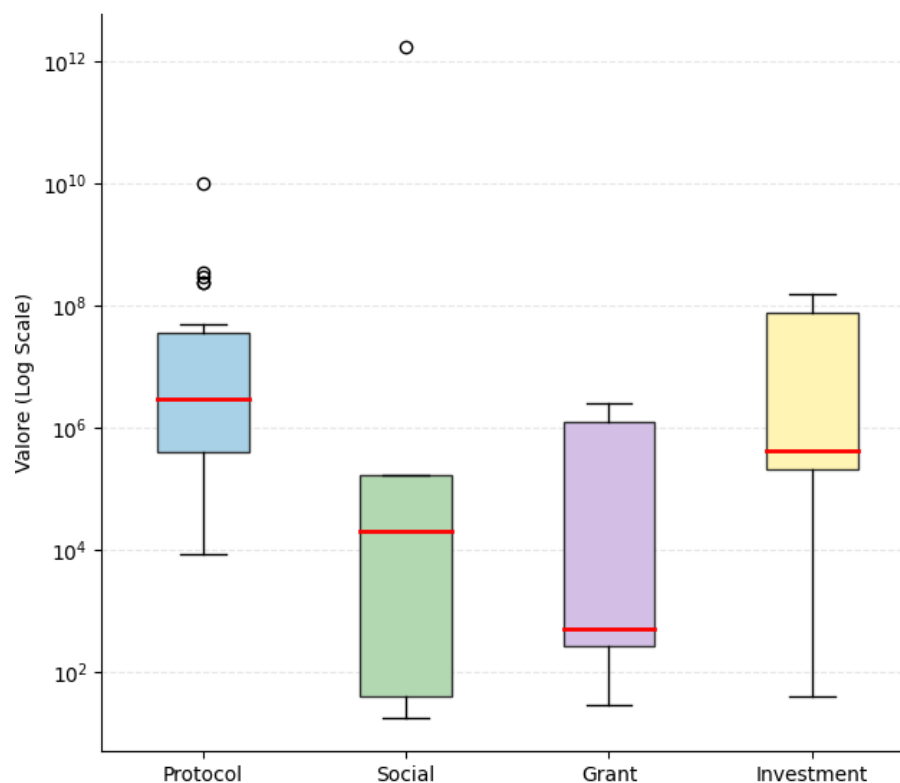


Figura 4.4: Distribuzione per categoria del Quorum

Confronto tra media e mediana: Analogamente al Threshold, la categoria Social registra il valore medio più alto ($3,36 \cdot 10^{11}$), mentre la mediana si attesta a 20.253.

Confronto tra mediane delle categorie: La categoria Protocol mantiene la mediana più alta anche per il quorum (3.000.000), distanziando significativamente tutte le altre categorie Investment (420.000), Social (20.253) e Grant (500).

Consistenza: I boxplot mostrano che la categoria Grant ha la distribuzione più compressa verso i valori minimi, con un quorum massimo che non supera le 833.509 unità come valore medio.

Voting Delay Figura 4.5

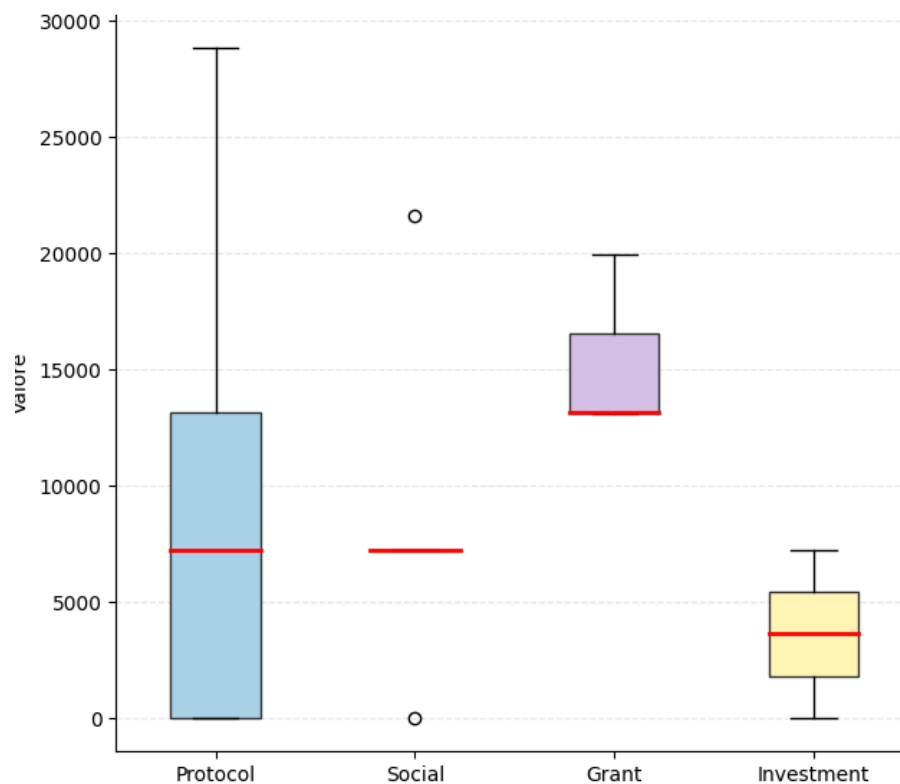


Figura 4.5: Distribuzione per categoria del Voting Delay

Le categorie Protocol e Social presentano una mediana identica di 7.200 blocchi, che

rappresenta il valore più frequente (standard) del campione complessivo.

La categoria Grant presenta i tempi di attesa pre-voto più lunghi, con una media di 15.389 blocchi e una mediana di 13.140 mentre la categoria Investment mostra i valori minimi sia medi che mediani (coincidenti e pari a 3.600 blocchi), indicando un intervallo tra proposta e voto ridotto rispetto alle altre classi.

Voting Period Figura 4.6

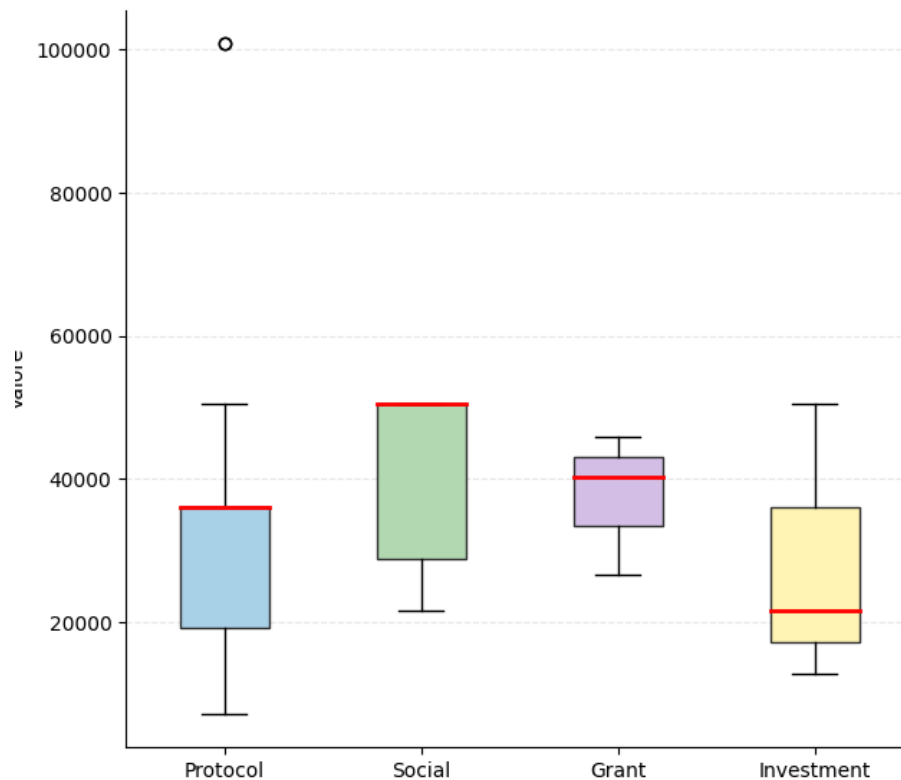


Figura 4.6: Distribuzione per categoria del Voting Period

La categoria Social registra la durata mediana più estesa (50.400) indicano che la maggior parte delle DAO in questa classe si attesta su durate superiori alla media globale (33.853). Al secondo posto troviamo Grant (40.320) seguita da Protocol

(36.000) ed infine la categoria Investment che riporta la finestra di voto più breve, con una mediana di 21.600 blocchi.

Timelock Delay Figura 4.7

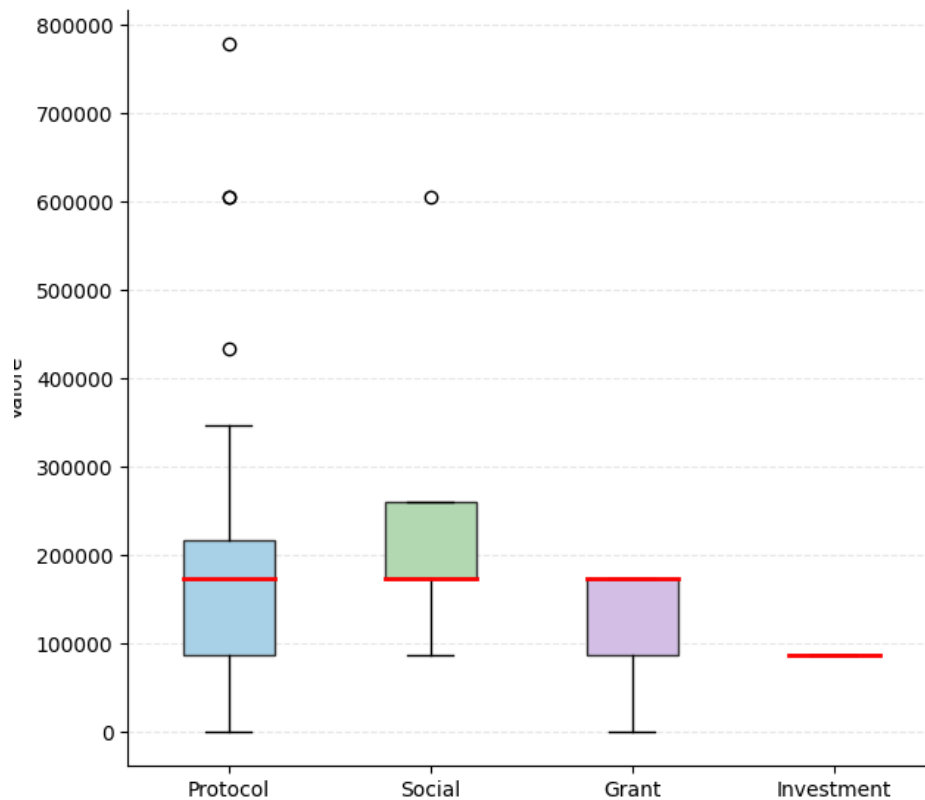


Figura 4.7: Distribuzione per categoria del Timelock Delay

Tre categorie su quattro (Protocol, Social e Grant) presentano una mediana identica di 172,800 secondi (corrispondenti a 48 ore) mentre la categoria Investment si discosta con una mediana di 86,400 secondi (24 ore).

Nonostante la convergenza delle mediane, la categoria Social ha la media più alta (259,200s), seguita da Protocol (206,177s), Grant (115,220s) ed infine Investment la cui media coincide con la mediana.

4.3 Pattern tecnologici

Concludiamo l'analisi con l'esame dell'architettura tecnica scelta per il contratto di governor, focalizzandoci sull'adozione di Proxy Pattern. La Tabella 4.7 seguente illustra la diffusione dei diversi pattern rilevati nel campione.

<i>Proxy Pattern</i>	<i>Conteggio</i>
EIP-1967 Transparent	15
ERC-1967 Beacon	1
ERC-897 Delegate	8
Nessun Proxy	24
Dato non disponibile	2

Tabella 4.7: Distribuzione governor proxy pattern

Sulla base della presenza o assenza di un proxy pattern, possiamo dividere inoltre il campione in due macro-categorie (Tabella 4.8):

- **Upgradable:** Contratti che utilizzano un proxy pattern per permettere modifiche al codice senza modificare l'indirizzo di riferimento.
- **Non-Upgradable:** Contratti definiti come "None", dove il codice della governance è immutabile.

<i>Stato contratto</i>	<i>Conteggio</i>	<i>Percentuale</i>
Upgradeable	24	50%
Non-Upgradeable	24	50%

Tabella 4.8: Distribuzione aggiornabilità del contratto governor

Escludendo i casi in cui l'informazione è mancante (N\D), l'analisi mostra un equilibrio perfetto tra le due strategie di implementazione.

Capitolo 5

Discussione

5.1 Confronto con la letteratura

Il panorama delle DAO che emerge dal confronto dell'analisi svolta con lo studio di Fritsch et al.[36] è quello di un ecosistema caratterizzato da una profonda asimmetria. I dati relativi ai parametri di threshold confermano lo scenario di estrema disuguaglianza descritto dai coefficienti di Gini da loro calcolati ($0.908 \leq G \leq 0.995$) i quali hanno evidenziato una concentrazione del potere di voto quasi assoluta. In molte delle organizzazioni analizzate, la barriera all'ingresso per la partecipazione politica è talmente alta che solo una piccola percentuale (inferiore all'1%) dei detentori di token ha effettivamente il potere di avviare una votazione. Questo crea un circolo vizioso in cui il quorum viene mantenuto proporzionalmente basso (generalmente al di sotto del 5%) per permettere al protocollo di progredire, ma ciò porta a consegnare le chiavi della governance ai pochissimi grandi detentori, validando le conclusioni di Fritsch, che evidenziano come la struttura di queste organizzazioni tenda a replicare dinamiche di potere di tipo oligarchico.

Passando alle criticità sollevate da Wang et al.[37], le analisi mostrano come i problemi di centralizzazione ed insostenibilità non siano solo teorici, ma strutturali. Il costo elevato delle transazioni sulle reti principali agisce come un filtro di partecipazione basato sul capitale: quando votare una proposta costa decine di dollari in

commissioni, la partecipazione diventa un lusso consentito solo a chi possiede capitali ingenti. Questo fenomeno svuota di significato la "tokenizzazione democratica" e rende il modello di partecipazione insostenibile per il piccolo utente. Dalle analisi emerge come molti protocolli, per contrastare l'apatia dei votanti, abbiano introdotto ricompense economiche per chi partecipa alla governance. Tuttavia, l'emissione continua di nuovi token per finanziare questi incentivi finisce per diluirne il valore, creando una pressione inflazionistica che erode il potere d'acquisto dei detentori nel lungo periodo. Tale evidenza supporta la tesi di Wang (2025), secondo cui la tokenizzazione utilizzata come unico motore della partecipazione crea sistemi fragili, destinati a collassare non appena l'incentivo economico non riesce più a compensare la svalutazione del token.

Infine, se proviamo a mappare queste realtà attraverso le tre dimensioni proposte da Park et al.[38], notiamo un profondo squilibrio evolutivo all'interno delle DAO analizzate. Se da un lato la dimensione amministrativa appare all'avanguardia, grazie a smart contract che garantiscono un'esecuzione dei voti automatica e priva di intermediari, le dimensioni politica ed economica rimangono ancorate a modelli molto tradizionali. Ne emerge un paradosso strutturale in cui le DAO analizzate si configurano come entità tecnicamente decentralizzate nel codice, ma politicamente accentrate nei fatti. La gestione della tesoreria è spesso affidata a gruppi ristretti e il potere decisionale segue la concentrazione della ricchezza, la decentralizzazione sembra oggi una proprietà intrinseca del software piuttosto che una reale conquista della comunità che lo utilizza.

In sintesi, i dati indicano che il traguardo di una governance equa e distribuita resta ancora lontano. La realtà empirica suggerisce che le DAO, anziché scardinare i vecchi paradigmi, tendano a riprodurre le asimmetrie di potere e le concentrazioni di capitale tipiche dei mercati finanziari convenzionali.

5.2 Implicazioni pratiche

Per chi si trova oggi a progettare una DAO, lo studio rivela che non esiste una configurazione universale, ma piuttosto un bilanciamento strategico tra accessibilità e sicurezza. Dalle analisi emerge che le configurazioni più robuste sono quelle che adottano modelli di "governance adattiva", capaci cioè di variare i quorum e le soglie di partecipazione, così come i periodi di votazione e di ritardo esecutivo, in base all'importanza o alla tipologia della proposta, evitando che un'unica barriera eccessivamente alta paralizzi l'attività o che una troppo bassa favorisca attacchi al sistema. Un ulteriore parametro che si rivela davvero critico per la partecipazione non è solo la quantità di token richiesti, ma il rapporto tra il costo del voto (le gas fee citate da Wang [37]) e l'impatto del voto sulla decisione finale. Per questo molte organizzazioni hanno spostato o sono in procinto di spostare la governance su layer secondari o a sovvenzionare i costi di transazione attribuendo tassi di coinvolgimento significativamente più alti ai propri utenti, suggerendo che per chi progetta una DAO, l'accessibilità economica sia il prerequisito fondamentale per evitare quella deriva verso l'estrema disuguaglianza descritta da Fritsch [36].

Al di là dell'aggiornabilità consentita da molti protocolli per i propri smart contract, i dati raccolti permettono di tracciare un profilo tecnico ricorrente tra le realtà più strutturate. Nello specifico, le configurazioni più robuste risultano essere quelle che prevedono un ritardo di votazione di 1 giorno (7.200 blocchi (12s)) seguito da un periodo 5 giorni (36.000 blocchi (12s)) in cui si svolge la votazione ed un Timelock di almeno 48 ore (172.800s). L'orientamento recente nella progettazione delle DAO sembra inoltre privilegiare la flessibilità delle architetture upgradable, introdotte per consentire la risoluzione di bug o l'ottimizzazione del codice nel tempo. Tuttavia, è interessante notare come l'analisi empirica condotta su questo campione evidenzi un quadro di equità assoluta tra l'adozione di smart contract aggiornabili e la scelta di modelli immutabili, segno che la flessibilità e l'adattabilità non hanno ancora eclissato il valore della persistenza deterministica del codice.

5.3 Limitazioni

L'analisi condotta presenta alcuni limiti strutturali che è necessario tenere in considerazione per una corretta interpretazione dei risultati:

- **Ampiezza del campione:** Lo studio si basa su un campione di 50 DAO. Sebbene queste rappresentino alcuni dei protocolli più rilevanti, l'insieme analizzato non è esaustivo dell'intero ecosistema, che conta migliaia di organizzazioni con logiche di governance molto eterogenee.
- **Esclusione dei dati off-chain:** Il focus è stato posto esclusivamente sui dati on-chain escludendo l'analisi di piattaforme off-chain come Snapshot, nonostante in diversi protocolli, tali piattaforme arrivano a gestire l'intero processo decisionale, riducendo la transazione on-chain a una mera esecuzione tecnica finale. Questa scelta comporta il rischio di sottostimare il reale coinvolgimento politico della community, in particolare dei piccoli detentori, che spesso ripiega su questi strumenti per la partecipazione evitando le elevate gas fee delle reti principali. Nei casi, tra quelli analizzati, in cui l'uso di tale piattaforme è previsto dal protocollo, queste architetture non sono state ignorate a priori, ma sono state oggetto di un'analisi limitata al piano teorico e procedurale: ne è stato studiato il funzionamento logico senza però procedere alla verifica dei dati effettivi o all'esame del processo dal punto di vista pratico e applicativo.
- **Natura dell'analisi (Snapshot temporale):** Il lavoro offre una fotografia istantanea della situazione attuale. Non essendo però un'analisi longitudinale, non permette di osservare come i parametri di governance si siano evoluti nel tempo in risposta a cambiamenti del mercato o aggiornamenti del protocollo.
- **Perimetro tecnologico:** La ricerca è stata limitata all'ecosistema Ethereum e reti EVM-compatibili escludendo modelli di governance nativi su altre architetture (es. Solana, Cosmos o Polkadot). Questi ultimi potrebbero presentare dinamiche di partecipazione e strutture di costo sensibilmente differenti, potenzialmente capaci di alterare il quadro fin qui delineato.

Conclusioni

La tesi ha esplorato la complessità delle Decentralized Autonomous Organizations (DAO), cercando di superare la narrazione teorica per ottenere un'analisi fondata sull'evidenza dei dati on-chain. Attraverso un percorso che ha coniugato l'analisi del codice degli smart contract con l'elaborazione statistica, si è cercato di mappare lo stato dell'arte della governance decentralizzata nel panorama Web3.

Sintesi dei contributi

Il contributo principale di questa ricerca risiede nella creazione di un framework metodologico capace di uniformare la frammentazione informativa tipica degli ecosistemi blockchain. Nello specifico, il lavoro si è svolto come un'analisi sistematica di un campione eterogeneo di 50 DAO, analizzandone l'architettura tecnica e i protocolli di governance sottostanti. Partendo dall'ispezione diretta degli smart contract, sono stati estratti parametri critici (quali quorum, soglie di proposta, periodi di votazione e ritardi di esecuzione). Tali dati, spesso codificati in modi differenti a seconda della chain o del framework utilizzato, sono stati normalizzati ottenendo metriche comuni e confrontabili. Il processo di normalizzazione ha permesso di superare il divario tra la documentazione e l'effettiva logica d'esecuzione "on-chain", fornendo una base di dati strutturata per un'analisi comparativa tra diverse categorie di DAO.

Risposta ai quesiti di ricerca

Sulla base dell'analisi quantitativa e qualitativa condotta, è possibile rispondere ai quesiti di ricerca formulati in fase introduttiva.

In che misura i modelli on-chain riflettono i principi di decentralizzazione dichiarati?

L'analisi dei dati evidenzia un paradosso: sebbene l'infrastruttura tecnica sia intrinsecamente decentralizzata e resistente alla censura, le dinamiche di potere tendono spesso a mostrare fenomeni di ricentralizzazione. La concentrazione dei token di governance e l'utilizzo di soglie di proposta elevate rendono, in molti casi, il processo decisionale riservato ad una ristretta cerchia di utenti. Pertanto, la decentralizzazione non risulta essere un obiettivo tecnologico pienamente raggiunto, ma una sfida politica ancora in fase di maturazione.

Quali sono i principali schemi decisionali e come influenzano l'operatività e il patrimonio?

Le DAO che adottano modelli di voto ponderato e deleghe attive mostrano una maggiore agilità operativa ma una minore partecipazione diretta dei piccoli utenti. Si è osservato inoltre che parametri di governance troppo rigidi possono portare a una paralisi decisionale, mentre parametri troppo permissivi espongono il patrimonio comune a rischi di attacchi o di centralizzazione decisionale. L'efficacia della gestione del patrimonio appare dunque direttamente proporzionale alla capacità dello smart contract di bilanciare l'accessibilità e la sicurezza.

Sviluppi futuri

I principali sviluppi della ricerca prevedono: l'estensione dell'analisi sul piano longitudinale per osservare il mutamento dei parametri nel tempo, l'estensione del dataset a chain non-EVM, il calcolo di metriche avanzate di decentralizzazione (come il coefficiente di Nakamoto o di Gini) per misurare l'impatto dei cambiamenti dei parametri sulla partecipazione effettiva della community ed infine l'estensione dell'analisi anche ai dati off-chain (Snapshot) al fine di completare il quadro della partecipazione.

Bibliografia

- [1] Elia, M., *An Introduction to Classic Cryptography. With an Exposition of the Mathematics of Private and Public Key Ciphers*, Arcane, 2018.
- [2] Mohamed Fartitchou, Hanaa El Marraki, Lamyae Lafkir, Anissa Azzouz, Khalid El Makkaoui, and Zakaria El Allali *Public-Key Cryptography behind Blockchain Security* 5th International Conference on Networking, Information Systems and Security: Envisage Intelligent Systems in 5g//6G-based Interconnected Digital Worlds (NISS), IEEE 2023.
- [3] Paolo Tasca and Claudio J. Tessone *Taxonomy of Blockchain Technologies. Principles of Identification and Classification* arXiv, 2018.
- [4] Ismail, Leila and Materwala, Huned *A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions*, Symmetry, 2019.
- [5] Ahmad, Sartaj and Arya, Shubham Kumar and Gupta, Shobhit and Singh, Puneeta and Dwivedi, Sanjeev Kumar *Study of Cryptographic Techniques Adopted in Blockchain*, 4th International Conference on Intelligent Engineering and Management (ICIEM), 2023.
- [6] Rajeev Sobti, G.Geetha *Cryptographic Hash Functions: A Review* IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, Marzo 2012.
- [7] Guo, Huaqun, Yu, Xingjie *A Survey on Blockchain Technology and its security* Blockchain: Research and Applications, Vol. 3, Febbraio 2022.

- [8] Satoshi Nakamoto *Bitcoin: A Peer-to-Peer Electronic Cash System* www.bitcoin.org page 3.
- [9] Samer Hassan, Primavera De Filippi *Decentralized Autonomous Organization* Internet Policy Review, Journal of internet regulation, 20 Aprile 2021.
- [10] Yves Longchamp, Chetan Kale, Sonali Gupta *Decentralised Autonomous Organisation (DAO)* The Bridge, Maggio 2022 – Seba Bank.
- [11] Tanusree Sharma, Yujin Potter, Kornrapat Pongmala, Henry Wang, Andrew Miller, Dawn Song, Yang Wang *Unpacking How Decentralized Autonomous Organizations (DAOs) Work in Practice* IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2024.
- [12] Yixuan Fan, Lei Zhang, Ruiyu Wang, and Muhammad Ali Imran *Insight Into Voting in DAOs: Conceptual Analysis and a Proposal for Evaluation Framework* Open Call Article, 5 Giugno 2023 IEEE Maggio/Giugno 2024.
- [13] Haya Altaieb, Zoltan Rajnai *Decentralized autonomous organizations review, importance, and applications* August 2022.
- [14] Law Commission of London (Joanna Otterburn, Stephanie Hack, Justice Fraser, Nick Hopkins, Sarah Green, Penney Lewis, Alison Young) *Decentralised autonomous organisations (DAOs) – Summary of scoping paper* Luglio 2024.
- [15] V. Buterin *A next-generation smart contract and decentralized application platform* Ethereum White Paper, 2014.
- [16] Ding Qinxua, Daniel Liebaub, Wang Zhiguo, Xu Weibiaoa *A Survey on Decentralized Autonomous Organizations (DAOs) and Their Governance* World Scientific Annual Review of Fintech Vol. 01, 2350001 (2023).
- [17] A. Wright *The rise of decentralized autonomous organizations: Opportunities and challenges* Stan. J. Blockchain L. & Pol’y, vol. 4, p. 1, 2020.
- [18] H. Adams, N. Zinsmeister, D. Robinson *Uniswap v2 Core* Marzo 2020

- [19] H. Adams, N. Zinsmeister, M. Salem, R. Keefer, D. Robinson *Uniswap v3 Core* Marzo 2021
- [20] H. Adams, M. Salem, N. Zinsmeister, S. Reynolds, A. Adams, W. Pote, M. Toda, A. Henshaw, E. Williams, D. Robinson *Uniswap v4 Core* Agosto 2014
- [21] Yuma Rao *Bittensor: A Peer-to-Peer Intelligence Market* www.bittensor.com
- [22] Qin Wang, Rujia Li, Qi Wang, Shiping Chen *Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges* ArXiv, Maggio 2021.
- [23] Raffaele Battaglini, Luigi Cantisani *Standard tecnici Ethereum e standardizzazione degli smart legal contract* MediaLaws, 29 mar 2022.
- [24] F. Vogelsteller, V. Buterin *EIP-20: Token Standard* Ethereum Improvement.
- [25] Van Cuong Bui, Sheng Wen, Jiangshan Yu, Xin Xia, Mohammad Sayad Haghghi, Yang Xiang *Evaluating Upgradable Smart Contract* IEEE International Conference on Blockchain (Blockchain), 2021.
- [26] Ye Liu, Shuo Li, Xiuheng Wu, Yi Li, Zhiyang Chen, David Lo *Demystifying the Characteristics for Smart Contract Upgrades* Conference'17, July 2017, Washington, DC, USA.
- [27] Sajad Meisami, William Edward Bodell III *A Comprehensive Survey of Upgradable Smart Contract Patterns* Illinois Institute of Technology, Department of Computer Science Poster session, 2023.
- [28] Amhaz Rabih, Bobenrieth Cédric, Marz Marlene *Impact of Decentralized Autonomous Organizations (DAO) on Society 5.0* 5th International Conference on Machine Learning, IOT and Blockchain, Febbraio 2024.
- [29] Roneil Rumburg Sid Sethi Hareesh Nagaraj *Audius: A Decentralized Protocol for Audio Content* 8 ottobre 2020.
- [30] *aelf Economic and Governance Whitepaper* V1.2.0 October 25th 2022.

- [31] *MANTRA DAO: Community Governed DeFi Platform* Whitepaper Version 1.0 June 2020.
- [32] *DeXe Protocol DAO Memorandum* <https://documents.dexe.network/DeXe-Protocol-DAO-Memorandum.pdf>.
- [33] *Compound: The Money Market Protocol* <https://compound.finance/documents/Compound.Whitepaper.pdf>.
- [34] The Braintrust Technology Foundation *Braintrust: The Decentralized Talent Network* July 2023.
- [35] Stephan Uracher *onchainaustria "First austrian DAO governed association"* 2024.
- [36] Robin Fritsch, Marino Müller, Roger Wattenhofer *Analyzing voting power in decentralized governance: Who controls DAOs?* 4 giugno 2024.
- [37] Qin Wang, Guangsheng Yu, Yilin Sai, Caijun Sun, Lam Duc Nguyen, Shiping Chen *Understanding DAOs: An Empirical Study on Governance Dynamics* IEEE Transactions on computational social system, vol. 12, no. 5, october 2025.
- [38] Hyejin Park, Ivan Ureta, Boyoung Kim *Developing Dimensions and Indicators to Measure Decentralization in Decentralized Autonomous Organizations* Administrative Sciences. 13. 241. 2023. <https://doi.org/10.3390/admsci13110241>
- [39] Silvio Meneguzzo, Claudio Schifanella, Valentina Gatteschi, Giuseppe Destefanis *Evaluating DAO Sustainability and Longevity Through On-Chain Governance Metrics* 2025, arXiv, <https://arxiv.org/abs/2504.11341>.
- [40] Silvio Meneguzzo, Claudio Schifanella, Valentina Gatteschi, Giuseppe Destefanis *Operationalising DAO Sustainability KPIs: A Multi-Chain Dashboard for Governance Analytics* 2026, arXiv, <https://arxiv.org/abs/2601.14927>.

