

POLITECNICO DI TORINO

Laurea Magistrale in Ingegneria Matematica



Tesi di Laurea Magistrale

Blockchain e Decentralized Autonomous Organization per la Sostenibilità delle Comunità Energetiche

Relatori

Prof. Danilo BAZZANELLA

Dr. Alfredo FAVENZA

Dr. Silvio MENEGUZZO

Candidata

Rachele PIERRI

Matricola 305728

Anno Accademico 2023/2024

Abstract

Le Decentralized Autonomous Organization (DAO) rappresentano una forma innovativa di governance, differenziandosi radicalmente dalle strutture organizzative tradizionali. Il loro funzionamento si basa sulla tecnologia blockchain, che ne costituisce il fondamento. Accanto a questa, gli smart contract e i meccanismi di voto svolgono un ruolo cruciale all'interno delle DAO, poichè garantiscono decentralizzazione e trasparenza nei processi decisionali.

L'obiettivo della tesi, svolta presso Links Foundation, è analizzare l'innovazione introdotta dalle DAO rispetto ai modelli organizzativi tradizionali, soffermandosi su come la blockchain e gli smart contract eliminino intermediari e automatizzino i processi decisionali. L'analisi delle DAO esistenti è stata condotta utilizzando Key Performance Indicator (KPI) ideati specificamente per questa ricerca, attraverso i quali è emersa una problematica significativa: la bassa partecipazione degli utenti alle attività di governance.

Per affrontare questo problema di partecipazione, è stato elaborato un modello basato sulla teoria dei giochi, con l'intento di incentivare una maggiore partecipazione degli utenti al processo decisionale. Il modello prevede meccanismi di ricompensa, penalità e reputazione per stimolare il coinvolgimento attivo nel voto.

Infine, il modello proposto è stato applicato ad una comunità energetica basata su una DAO, simulando diversi parametri per identificare la configurazione ottimale in grado di garantire la stabilità e la longevità della comunità nel lungo periodo. I risultati della tesi dimostrano come l'integrazione di incentivi mirati e un meccanismo di reputazione adeguato possano migliorare il livello di partecipazione e assicurare la sostenibilità delle DAO in contesti pratici, come quello delle comunità energetiche.

Indice

Elenco delle tabelle	VII
Elenco delle figure	VIII
Elenco dei codici	IX
Acronimi	X
Introduzione	1
1 Blockchain	3
1.1 Definizione e caratteristiche	3
1.2 Protocolli di consenso	6
1.3 Ethereum e smart contract	8
1.4 Sicurezza	9
2 Decentralized Autonomous Organization	11
2.1 Economia Blockchain - verso le DAO	11
2.2 Definizione e storia	11
2.3 Caratteristiche e confronto	15
2.3.1 Lancio del progetto e ciclo di vita	15
2.3.2 Proprietà	16
2.3.3 Governance	18
2.3.4 Tesoreria	18
2.3.5 Confronto con le organizzazioni tradizionali	19
2.4 Problematiche	19
2.4.1 Sicurezza	19
2.4.2 Privacy	21
2.4.3 Stato giuridico	21
2.4.4 Limitazioni tecniche	22
2.4.5 Corporate governance	22
2.5 Architettura	23
2.5.1 Livello tecnologico di base	23
2.5.2 Livello esecutivo	24
2.5.3 Livello di coordinamento	25
2.5.4 Livello organizzativo	25
2.5.5 Livello applicativo	26

2.6	Meccanismi di coordinamento	26
2.6.1	Meccanismo di incentivazione	27
2.6.2	Meccanismo di voto	27
2.7	Procedura e potere di voto	30
2.7.1	Rilevanza della correttezza nei sistema di voto	30
2.7.2	Potere di voto	31
2.7.3	Procedura di voto	32
2.7.4	Confronto con la struttura tradizionale	34
2.8	Key Performance Indicator	35
2.9	DAO popolari	42
2.9.1	MakerDAO	42
2.9.2	Aragon e la sua architettura	44
2.9.3	DAOstack e Holographic Consensus	46
2.9.4	Compound, Uniswap e ENS	47
2.9.5	Commenti	51
2.10	Applicazioni	52
2.10.1	Swarm City	53
2.10.2	E-government	53
2.10.3	LikeStarter	54
2.10.4	Veicoli elettrici	54
3	Comunità energetiche	57
3.1	Introduzione alle comunità energetiche	57
3.1.1	Definizione di comunità energetica	58
3.2	Blockchain nelle comunità energetiche	59
3.2.1	Vantaggi	60
3.2.2	Svantaggi	61
3.3	DAO nella comunità energetica	62
3.3.1	DAEO	62
3.3.2	Confronto con il tradizionale	64
3.4	Sistemi proposti in letteratura	64
3.4.1	Mercato transattivo P2P	64
3.4.2	Local Energy Market	66
3.4.3	EnergyDAO	67
4	Teoria dei giochi e modello proposto	69
4.1	Introduzione alla teoria dei giochi	69
4.2	Modello proposto	70
4.2.1	Definizioni base e parametri	70
4.2.2	Reward, utility ed equilibri di Nash sotto la soglia μ	75
4.2.3	Reward, utility ed equilibri di Nash superata la soglia μ	77

4.3	Adattamento alle comunità energetiche	87
4.3.1	Simulazione dei parametri	90
4.3.2	Plot della simulazione	100
4.3.3	Commenti finali	103
	Conclusione e sviluppi futuri	109
	Bibliografia	111

Elenco delle tabelle

2.1	Confronto tra DAO e organizzazioni tradizionali	20
2.2	Confronto tra voto all'interno di una DAO e tradizionale	35
2.3	KPI e suddivisione in livelli	39
2.4	Variante KPI Efficienza del meccanismo di voto	41
2.5	Analisi KPI MakerDAO	43
2.6	Analisi KPI Aragon	45
2.7	Analisi KPI DAOstack	46
2.8	Coefficienti di Gini e di Nakamoto per Compound, Uniswap e ENS	48
2.9	Analisi KPI Compound, Uniswap e ENS	49
3.1	Confronto tra comunità basata su DAEO e tradizionale	65
4.1	Reward nel caso in cui la soglia μ non sia superata	75
4.2	Utility nel caso in cui la soglia μ non sia superata	76
4.3	Reward nel caso in cui si superi la soglia μ - idea 1	78
4.4	Utility nel caso in cui si superi la soglia μ - idea 1	78
4.5	Reward nel caso in cui si superi la soglia μ - idea 2	84
4.6	Utility nel caso in cui si superi la soglia μ - idea 2	84
4.7	Parametri e rispettivi valori della simulazione	91
4.8	Altri parametri e rispettivi valori della simulazione	92

Elenco delle figure

1.1	Struttura della blockchain	4
2.1	Struttura a triangolo della DAO	13
2.2	Linea temporale della storia delle DAO	13
2.3	Ciclo di vita di una DAO	16
2.4	Architettura di una DAO	23
2.5	Procedura di voto all'interno di una DAO	33
2.6	Suddivisione in livelli dei KPI	40
2.7	Variante KPI Efficienza del meccanismo di voto	41
2.8	Livelli KPI per punteggio finale	51
3.1	Struttura ICES	59
3.2	Struttura DAEO	63
4.1	Esempio di simulazione del modello	74
4.2	Evoluzione della reputazione degli utenti nel tempo	100
4.3	Numero di contributori nel tempo	101
4.4	Totale di astensioni per utente	101
4.5	Evoluzione delle astensioni negli anni	102
4.6	Tempo trascorso come non contributore	103
4.7	Evoluzione della reputazione degli utenti aumentando ΔR_{voto} e $\Delta R_{astenuto}$	104
4.8	Evoluzione della reputazione degli utenti diminuendo ΔR_{voto} e $\Delta R_{astenuto}$	105
4.9	Evoluzione della reputazione degli utenti aumentando ρ	106
4.10	Evoluzione della reputazione degli utenti diminuendo ρ	106

Elenco dei codici

4.1	Funzione per inizializzare la reputazione di nuovi membri	93
4.2	Funzione per aggiornare le reputazioni degli utenti dopo la votazione	94
4.3	Funzione per fare un redeem casuale per un utente non contributore	94
4.4	Funzione per l'aggiunta di impianti rinnovabili	95
4.5	Funzione per simulare la selezione degli utenti	96
4.6	Funzione per calcolare il tempo necessario per diventare non contributore	96
4.7	Funzione per calcolare il tempo trascorso come non contributore . .	97
4.8	Simulazione completa	97

Acronimi

1P1V

Una Persona Un Voto

1T1V

Un Token Un Voto

AGP

Aragon Governance Proposal

AI

Intelligenza Artificiale

BoT

Blockchain of Things

DAEO

Decentralized Autonomous Energy Organization

DAO

Decentralized Autonomous Organization o Distributed Autonomous Organization

dApp

Applicazioni decentralizzate

DER

Distributed Energy Resources

DLT

Distributed Ledger Technology

DoS

Denial of Service

ENS

Ethereum Name Service

ETH

Ether

EVM

Ethereum Virtual Machine

FER

Fonti di Energia Rinnovabili

GSE

Gestore dei Servizi Energetici

HC

Holographic Consensus

ICES

Integrated Community Energy System

IoT

Internet of Things

KPI

Key Performance Indicator

LEM

Local Energy Market

MRA

Maggioranza Relativa Autorizzata

NFT

Non-Fungible Token

P2P

Peer-to-Peer

PoA

Proof of Authority

PoS

Proof of Stake

PoW

Proof of Work

SHEMS

Smart Home Management System

TBQ

Token-Based Quorum

Introduzione

Le Decentralized Autonomous Organization (DAO) rappresentano una nuova frontiera nel campo della governance, ridefinendo i modelli organizzativi tradizionali grazie all'uso della tecnologia blockchain. Le DAO sono organizzazioni decentralizzate, in cui le decisioni vengono prese collettivamente dagli utenti attraverso meccanismi di voto e smart contract, senza la necessità di un'autorità centrale o intermediari. Questa struttura innovativa si basa su principi come la decentralizzazione, la trasparenza e l'automazione dei processi decisionali, caratteristiche che le rendono particolarmente interessanti per l'applicazione in contesti come le comunità energetiche e altri sistemi partecipativi.

Nonostante il loro potenziale, uno dei principali ostacoli delle DAO attuali è la scarsa partecipazione degli utenti alle attività di governance. Questo fenomeno può minare l'efficacia e la sostenibilità di queste organizzazioni. In un modello decentralizzato, dove le azioni dei singoli possono influenzare significativamente l'esito delle decisioni, la partecipazione attiva degli utenti riveste un ruolo cruciale per il corretto funzionamento dell'organizzazione nel lungo periodo. Senza un coinvolgimento adeguato, le DAO rischiano di non raggiungere pienamente i loro obiettivi di decentralizzazione ed efficienza.

Le motivazioni alla base di questo lavoro derivano dalla volontà di affrontare questa problematica, esplorando soluzioni che possano incentivare una maggiore partecipazione degli utenti e migliorare il funzionamento delle DAO. Inoltre, il progetto è motivato dal crescente interesse verso l'applicazione delle DAO in ambiti come le comunità energetiche, dove l'automazione e la trasparenza nei processi decisionali possono giocare un ruolo cruciale.

L'obiettivo principale di questa tesi è analizzare il contributo innovativo delle DAO rispetto ai modelli organizzativi tradizionali, concentrandosi sui meccanismi che regolano la partecipazione e la governance decentralizzata. In particolare, il lavoro vuole esaminare come la tecnologia blockchain e gli smart contract possano automatizzare i processi decisionali e ridurre la necessità di intermediari, promuovendo

trasparenza e efficienza. Inoltre, l'analisi delle DAO esistenti, condotta tramite specifici Key Performance Indicator (KPI), mira ad individuare le criticità legate soprattutto alla partecipazione.

A partire da queste premesse, viene elaborato un modello basato sulla teoria dei giochi, con l'obiettivo di incentivare una partecipazione più attiva e consapevole degli utenti. Infine, il modello proposto viene applicato ad un caso studio di una comunità energetica basata su DAO, simulando diverse configurazioni per identificare la soluzione ottimale in grado di garantire la sostenibilità a lungo termine.

Nella prima fase della ricerca viene condotta una revisione della letteratura su blockchain (capitolo 1) e DAO (capitolo 2), con l'obiettivo di individuare le caratteristiche principali e le sfide legate a queste tecnologie. Il secondo capitolo, in particolare, approfondisce le caratteristiche e l'architettura delle DAO. Successivamente, viene selezionato un set di KPI specifici per valutare le DAO esistenti e identificare le problematiche più critiche. Il capitolo 3 esplora il caso d'uso delle comunità energetiche e i sistemi proposti in letteratura. Infine, il capitolo 4 presenta un modello basato sulla teoria dei giochi, ideato per incentivare una partecipazione attiva tramite meccanismi di ricompensa, penalità e reputazione, applicato ad una simulazione di una comunità energetica basata su DAO, con l'obiettivo di garantirne la sostenibilità nel tempo.

I risultati della tesi dimostrano che l'integrazione di meccanismi di incentivazione mirati e un sistema di reputazione adeguato possono migliorare significativamente la partecipazione degli utenti nelle DAO. L'applicazione del modello ad una comunità energetica ha evidenziato come questi incentivi possano non solo incrementare il coinvolgimento degli utenti, ma anche contribuire alla stabilità e longevità della DAO nel lungo periodo. Tali conclusioni indicano che le DAO, se ben progettate, possono essere uno strumento efficace per la gestione decentralizzata e partecipativa di risorse fornendo un modello di governance più democratico e automatizzato.

Capitolo 1

Blockchain

1.1 Definizione e caratteristiche

La blockchain può essere descritta come una tecnologia di database distribuita, noto anche come Distributed Ledger Technology (DLT), che non può essere modificato da singoli utenti o gruppi di utenti. Più nello specifico, la DLT è una tecnologia che consente di registrare transazioni e dati in modo decentralizzato attraverso una rete di nodi distribuiti, eliminando la necessità di un'autorità centrale che controlla il registro.

In una generica DLT si possono effettuare quattro diverse operazioni: Create (creazione), Retrieve (recupero), Update (modifica) e Delete (eliminazione). La blockchain rappresenta un tipo specifico di DLT, che consente solo due operazioni: Create e Retrieve. Non è quindi possibile modificare o cancellare alcun dato una volta inserito.

La struttura di questa tecnologia è a blocchi ed è organizzata nel seguente modo: ogni blocco contiene una sequenza di transazioni, un timestamp ed una funzione hash che lo collega al blocco precedente, fino al blocco di genesi iniziale. Un nuovo blocco viene inserito nella catena grazie al lavoro del miner e viene convalidato tramite un protocollo di consenso, che analizzeremo in seguito. Grazie a questa struttura, ogni nodo all'interno della rete detiene una copia del registro completo, favorendo così la decentralizzazione e l'affidabilità della tecnologia blockchain.

Per capire meglio la struttura della blockchain, introduciamo la nozione di Merkle tree. Nei Merkle tree, le transazioni sono sottoposte ad operazioni di hashing, accoppiate e rielaborate finché non rimane un unico hash finale, noto come Merkle

root. Ogni blocco successivo salva la Merkle root del blocco precedente, formando così una catena di dati collegata e protetta tramite crittografia.

Nella figura sottostante possiamo vedere nel dettaglio la struttura appena descritta.

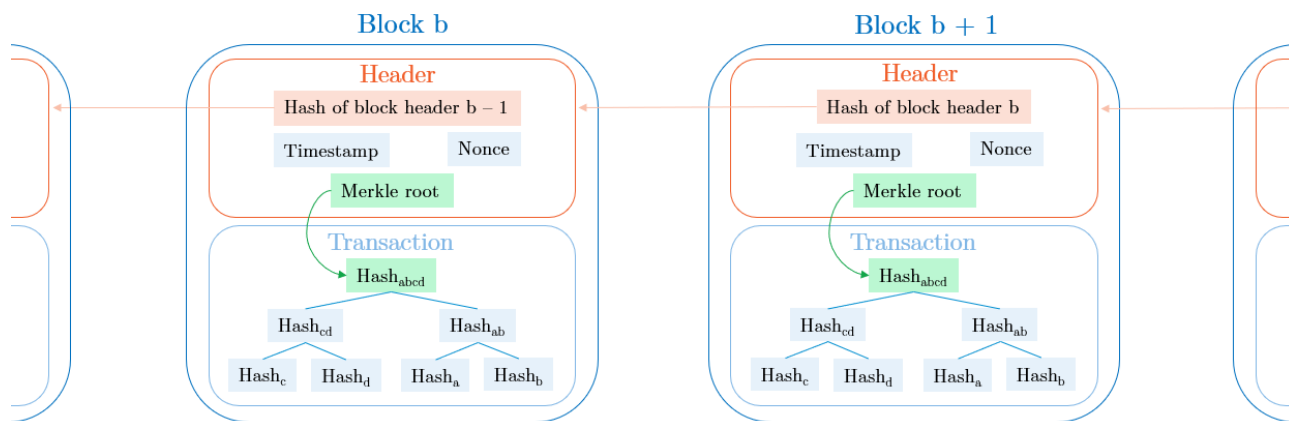


Figura 1.1: Struttura della blockchain

Abbiamo nominato alcuni elementi crittografici su cui si basa la sicurezza della blockchain, più nel dettaglio [1]:

Funzioni di hash: Questa funzione mappa una stringa di lunghezza arbitraria in una a dimensione fissa. Una proprietà dell'hash è la resistenza alla pre-immagine, ovvero, dato l'output hash, è computazionalmente impossibile risalire all'input. Inoltre, è impossibile dal punto di vista computazionale trovare due input distinti che producono lo stesso output hash. Con queste caratteristiche, la funzione hash collega i blocchi nella catena in modo immutabile, sicuro ed affidabile. Infatti, se un blocco, o un'informazione contenuta in esso, viene modificato, l'hash sarà diverso e i vari collegamenti tra i blocchi saranno interrotti.

Crittografia a chiave pubblica: La chiave privata, conservata in un wallet digitale o in un dispositivo hardware dedicato, è utilizzata dall'utente per firmare un messaggio, generando così una firma digitale unica. La chiave pubblica, invece, viene usata per dimostrare la provenienza del messaggio. La firma viene poi trasmessa insieme ai dettagli della transazione alla blockchain. Quando un miner riceve questi dati, sfrutta la chiave pubblica dell'utente per decrittare la firma digitale e ottiene l'hash associato. L'hashing dei dati della transazione ricevuti produce un altro valore hash. Il miner quindi confronta i due valori hash: se corrispondono, la transazione è considerata valida. Poiché solo il

proprietario della chiave privata può generare la firma corrispondente, la firma digitale costituisce una prova inequivocabile della legittimità della transazione. La coppia di chiavi (pubblica e privata) è fondamentale per il funzionamento della blockchain, utilizzata sia per firmare che per verificare le transazioni.

Zero-Knowledge Proof: Questo principio è utilizzato in alcuni contesti crittografici delle blockchain per preservare la privacy degli utenti. Un esempio chiaro è il processo di validazione di transazioni di denaro tra utenti. La blockchain, infatti, non ha bisogno di conoscere l'identità o la quantità di denaro del mittente per sapere se una transazione può essere effettuata. In questo modo, si garantisce la sicurezza e la validità delle transazioni senza compromettere la riservatezza dei dati personali o finanziari degli utenti.

Questa tecnologia supporta quindi in modo efficiente ed efficace transazioni peer-to-peer (P2P) dirette tra nodi della rete, eliminando la necessità di intermediari e garantendo l'integrità e la sicurezza dell'intera catena di blocchi. Attraverso l'uso di algoritmi crittografici avanzati, ogni transazione è registrata in maniera permanente e verificabile, assicurando che i dati non possano essere alterati o manipolati senza consenso, aumentando così la fiducia tra i partecipanti alla rete.

In sintesi, la blockchain rappresenta una tecnologia innovativa che offre un registro distribuito, immutabile e trasparente per le transazioni. Grazie all'uso combinato di crittografia avanzata e meccanismi di consenso distribuito, garantisce livelli elevati di sicurezza e affidabilità, riducendo rischi di frode e di manipolazione dei dati, senza dipendere da un'autorità centrale, promuovendo così un ecosistema decentralizzato.

Dopo aver dato una definizione esaustiva, descriviamo le caratteristiche principali e le tipologie di blockchain più rilevanti.

- **Decentralizzazione:** La caratteristica chiave della blockchain è la sua natura decentralizzata. Questo significa che il registro digitale, o database, non è controllato da un'unica autorità centrale, ma è distribuito tra i numerosi nodi della rete. Questo modello rende la blockchain resistente alla censura e alle manipolazioni, poiché non è soggetta al controllo di un singolo ente o organizzazione.
- **Immutabilità:** Un'altra proprietà fondamentale della blockchain è l'immutabilità dei dati. Una volta che una transazione è stata registrata sulla blockchain e inserita all'interno di un blocco, essa diventa permanente e non può essere modificata o eliminata senza il consenso della maggioranza dei partecipanti della rete. Questo garantisce l'integrità e l'affidabilità delle informazioni archiviate sulla blockchain.

- **Sicurezza e anonimato:** La crittografia svolge un ruolo cruciale nella blockchain, garantendo la sicurezza e l'anonimato dei dati. Le transazioni sono crittografate e i partecipanti della rete sono identificati da indirizzi pseudonimi, preservando così la privacy e l'anonimato degli utenti.
- **Verificabilità e trasparenza:** La blockchain offre un alto livello di verificabilità e trasparenza. Tutte le transazioni sono accessibili pubblicamente e registrate in modo permanente sin dal primo blocco, noto come blocco genesis. Questo significa che chiunque può esaminare l'intero storico delle transazioni e verificare l'autenticità e l'integrità dei dati senza doversi affidare ad un intermediario di fiducia.

Si può fare una distinzione delle blockchain in base all'accesso ai dati e alle transazioni. Possiamo individuare tre categorie di strutture:

1. **Blockchain pubblica:** In questa tipologia di blockchain tutti i nodi della rete hanno la possibilità di leggere i dati e convalidare le transazioni, essendo aperta pubblicamente. È quindi una blockchain permissionless e completamente decentralizzata, ovvero non è presente un'autorità centrale. Le blockchain di Bitcoin ed Ethereum sono esempi di blockchain pubbliche.
2. **Blockchain privata:** Al contrario della precedente, la blockchain privata è completamente centralizzata e il permesso di scrittura è concesso solo a nodi preregistrati da un'autorità centrale. Per questo motivo, questa tipologia di struttura si adatta più facilmente a società o organizzazioni private. Un vantaggio risiede nella riduzione del tempo di consenso, favorendo così una portata delle transazioni elevata ed una bassa latenza. Un difetto invece è che vi è solo un punto di guasto, ciò significa che un unico nodo che fallisce influisce sull'intera rete.
3. **Blockchain consortium:** Quest'ultima tipologia è un ibrido delle due precedenti. In questa struttura la convalida delle transazioni è controllata solo da un gruppo di nodi della rete. La blockchain consortium è quindi solo parzialmente decentralizzata, ma è più veloce e sicura.

1.2 Protocolli di consenso

Un aspetto cruciale che ogni blockchain deve affrontare è il processo di consenso per l'inserimento dei nuovi blocchi nel database condiviso. Grazie alla sua natura distribuita e alla sua struttura di hash, le transazioni già inserite nella blockchain

sono molto difficili da modificare fraudolentemente. Il punto più problematico riguarda l’inserimento di nuovi blocchi.

Questo processo è fondamentale per garantire l’integrità e la sicurezza delle transazioni registrate sulla blockchain. Infatti, se un attore malintenzionato potesse inserire transazioni fraudolente nella blockchain, comprometterebbe l’affidabilità e l’utilità del sistema. Anche l’anonimato, caratteristica molto ricercata nelle blockchain, solleva interrogativi sulla fiducia e l’integrità delle transazioni.

Per questi motivi, il sistema blockchain richiede la convalida di ogni transazione da parte dei partecipanti della rete attraverso protocolli di consenso. I protocolli di consenso sono algoritmi complessi che consentono a partecipanti sconosciuti e non fidati di concordare su quali blocchi siano validi per essere aggiunti alla blockchain. In particolare, gli algoritmi di consenso definiscono regole che tutti i nodi della rete devono seguire e sfruttano l’interesse comune dei partecipanti per mantenere la catena di blocchi onesta e affidabile. Questo è particolarmente importante in una rete decentralizzata come la blockchain, dove non esiste una terza parte che possa arbitrare le transazioni o risolvere dispute.

Ci sono vari requisiti che devono essere soddisfatti da un protocollo di consenso, tra cui la sicurezza, la tolleranza ai guasti, l’efficienza energetica e la gestione dei ritardi di rete. Sono stati sviluppati diversi algoritmi di consenso per affrontare queste sfide e consentire alle reti blockchain di prendere decisioni in modo affidabile e distribuito. Vediamo i principali [1], [12]:

- **Proof of Work (PoW):** Questo protocollo prevede una “prova di lavoro”, ovvero richiede di risolvere un problema computazionalmente complesso, ma veloce da verificare. Il problema che i miner devono risolvere è trovare un valore nonce che, quando combinato con i dati del blocco, produca un output hash che soddisfi determinati criteri di difficoltà. Ad esempio, l’hash risultante potrebbe dover iniziare con un certo numero di zeri. Poiché non c’è modo di prevedere quale valore nonce porterà alla soluzione del problema, i miner devono eseguire molte iterazioni, ciascuna con un calcolo di hash, fino a trovare la soluzione corretta. Il primo che trova il valore nonce corretto può propagare il nuovo blocco attraverso la rete. Gli altri nodi della rete verificano che il blocco sia stato validato correttamente, principalmente controllando che l’hash del blocco soddisfi i criteri di difficoltà. Una volta che il blocco è accettato e aggiunto alla blockchain, il miner viene ricompensato, spesso con una criptovaluta. Per attaccare il sistema PoW, è necessario disporre del 51% della potenza di calcolo della rete. Sebbene la PoW sia un metodo efficace per garantire la sicurezza e l’integrità della blockchain, ha alcuni svantaggi significativi. Il più evidente è il suo consumo energetico elevato. Poiché i miner devono eseguire un gran numero di calcoli per trovare soluzioni valide,

questo richiede un'enorme quantità di potenza di calcolo, che a sua volta si traduce in un consumo significativo di elettricità.

- **Proof of Stake (PoS):** Con il protocollo PoS, i nodi validator bloccano una quantità di criptovaluta o di token (stake). I validator vengono scelti in base alla quantità bloccata, piuttosto che sulla potenza computazionale come avviene nella PoW. Quindi, la PoS mira a raggiungere un consenso distribuito basato sulle puntate dei nodi anziché sulla potenza di calcolo. Quando un nodo viene scelto per convalidare un blocco, riceve le commissioni di transazione associate a quel blocco. Tuttavia, se il nodo selezionato tenta di inserire un blocco non valido, perde la sua puntata. La PoS offre diversi vantaggi rispetto alla PoW, tra cui una minore necessità di calcolo e consumo energetico.
- **Proof of Authority (PoA):** Nella PoA non è la valuta ad essere messa in gioco, come nella PoS, bensì la reputazione. Nel contesto della PoA, i validator devono rendere pubblica la propria identità per partecipare. L'approccio prevede la preselezione di nodi affidabili ai quali viene delegata l'autorità di inserire nuovi blocchi, diventando quindi validator. Di solito, nei sistemi PoA vengono imposti dei limiti al numero di blocchi che ogni singolo validator può inserire, ad esempio impedendo l'inserimento di blocchi consecutivi. Questo modello opera con un numero limitato di validator, il che lo rende estremamente scalabile. Infatti, la PoA offre alta scalabilità e riduzione del consumo energetico, ma è caratterizzata da una decentralizzazione limitata. Un potenziale svantaggio è che, essendo i validatori in numero limitato e conosciuti, un attaccante potrebbe cercare di corromperli per compromettere il sistema dall'interno. La PoA trova particolare utilità nelle blockchain private o consortium, dove è più semplice garantire l'affidabilità degli utenti.

I protocolli di consenso appena descritti sono tra i più diffusi nelle diverse blockchain, ma ne esistono molti altri, come la Proof of Burn (PoB), la Proof of Importance (PoI) e il Practical Byzantine Fault Tolerance (PBFT), solo per citarne alcuni.

Si vuole sottolineare ancora una volta quanto questi protocolli di consenso siano essenziali per il funzionamento delle blockchain, poiché permettono ai nodi della rete di raggiungere un accordo sulla validità delle transazioni senza affidarsi ad un'autorità centrale.

1.3 Ethereum e smart contract

In questa sezione aggiungiamo un altro concetto che facilita l'automazione all'interno della blockchain, ovvero gli smart contract. Ma per far ciò, bisogna introdurre

Ethereum, sistema fondato nel 2014 da Vitalik Buterin.

Non si tratta soltanto di una nuova criptovaluta, ma rappresenta un cambiamento radicale nel paradigma delle blockchain. È una piattaforma globale open source basata su una blockchain, su cui possono essere eseguite applicazioni decentralizzate (dApp), chiamate smart contract. Infatti, Ethereum è stata la prima blockchain ad integrare un linguaggio Turing completo, permettendo così lo sviluppo di codice.

La piattaforma Ethereum include una macchina virtuale decentralizzata chiamata Ethereum Virtual Machine (EVM), che esegue script tramite una rete di nodi pubblici. Come altre blockchain, possiede la sua criptovaluta (ether - ETH), ma il suo obiettivo principale è quello di creare un ambiente decentralizzato in cui possono girare applicazioni con scopi diversi.

Per prevenire il blocco della rete dovuto all'esecuzione di cicli infiniti, Ethereum ha introdotto il "gas": uno smart contract può essere eseguito fintanto che dispone di gas, acquistato con gli ETH. La quantità massima di gas disponibile per lo smart contract deve essere definita e fissata in precedenza all'interno del contratto stesso.

Il lancio di questa piattaforma ha dimostrato la possibilità di programmare blockchain per supportare una vasta gamma di logiche transazionali attraverso smart contract, che eseguono parti di software predefiniti sulla blockchain quando specifiche condizioni sono soddisfatte [20].

Dopo il rilascio di Ethereum nel 2014, con smart contract ci si riferisce a programmi eseguiti sui nodi validatori di una blockchain. Più nel dettaglio, lo smart contract è codice che gestisce processi in modo preciso e non soggettivo, in risposta ad eventi specifici e senza coinvolgere terze parti. Possono gestire diversi tipi di transazioni, non solo trasferimenti di criptovalute. In particolare, possono definire regole, come un normale contratto, ed applicarle in modo automatico tramite il codice.

Gli smart contract offrono sicurezza e velocità superiori rispetto alla contrattualistica tradizionale, riducendo i costi di transazione e garantendo autonomia ed efficienza. Nonostante superino molte sfide legate a fiducia, sicurezza e riservatezza, gli smart contract presentano ancora problematiche legali da affrontare.

1.4 Sicurezza

La sicurezza della blockchain costituisce uno degli elementi fondamentali per il successo delle applicazioni blockchain nel contesto aziendale.

Guo e Yu [1] e Liu et al. [6] hanno sottolineato che i principali rischi associati alla

blockchain includono:

- **Attacchi di rete:** Un esempio di attacco informatico è il Denial-of-Service (DoS), in cui l'attaccante sfrutta un programma per inondare la rete di transazioni, superando la capacità massima della blockchain e rendendo il sistema non disponibile. Questi attacchi sovraccaricano la rete rendendola temporaneamente inoperabile e compromettendone la fiducia.
- **Sicurezza degli endpoint:** Gli endpoint rappresentano i punti di accesso alla rete blockchain. Questi, per definizione, sono molto eterogenei, e perciò ci possono essere più opzioni per sfruttarne le vulnerabilità e compromettere l'intera rete.
- **Uso improprio intenzionale:** Un singolo o un gruppo di attaccanti possono controllare il 51% del potere computazionale della rete blockchain, favorendo attacchi di maggioranza. Questo tipo di controllo rende il sistema vulnerabile e mina la fiducia dei singoli utenti.
- **Vulnerabilità del codice:** Data la loro definizione, chiunque può scrivere gli smart contract. Questo però può portare a vulnerabilità ed errori legati al codice che, a causa della rete distribuita, hanno un impatto di vasta portata.
- **Smart contract fraudolenti:** Per lo stesso motivo del punto precedente, gli smart contract possono potenzialmente essere progettati con l'intenzione di ingannare o danneggiare altri utenti.
- **Negligenza umana:** Il rischio umano è un punto debole per qualsiasi sistema. In particolare, potrebbero esserci gestione negligente delle credenziali, registrazione e monitoraggio insufficienti, oppure una configurazione errata della sicurezza. Questi errori consentono agli attaccanti di compromettere la rete.
- **Perdita di privacy:** Con sempre più dati da archiviare sulla blockchain, è crescente la preoccupazione per la perdita di privacy degli utenti. Infatti, le informazioni registrate sulla blockchain sono permanenti e accessibili pubblicamente. Per mitigare questo rischio, si possono adottare alcune soluzioni, tra cui tecniche di offuscamento del codice, crittografia omomorfa, piattaforme affidabili e smart contract orientati alla tutela della privacy.

Un ultimo punto da sottolineare è la mancanza di regolamentazione delle blockchain. La definizione di regole è ancora più importante se si considera l'aumento delle applicazioni blockchain a livello internazionale. La regolamentazione è essenziale per garantire sicurezza, affidabilità e interoperabilità dei sistemi blockchain. Di conseguenza, la definizione di regole e standard rappresenterà una delle principali sfide per la piena implementazione dei sistemi blockchain su vasta scala.

Capitolo 2

Decentralized Autonomous Organization

2.1 Economia Blockchain - verso le DAO

La blockchain e gli smart contract possono essere alla base di un nuovo sistema economico, che Beck et al. [10] hanno chiamato “economia blockchain”. Questo concetto si distingue dall’economia digitale in quanto le transazioni seguono le regole stabilite negli smart contract, quindi possono essere eseguite in modo autonomo e senza la necessità di terze parti per l’approvazione.

Questa concezione si basa su una forma innovativa di governance, che può trovare espressione nelle organizzazioni autonome decentralizzate (Decentralized Autonomous Organization - DAO), rappresentando un’innovazione dal tradizionale modello di governance organizzativa. In particolare, a differenza dell’economia digitale, la governance nell’economia blockchain sarà caratterizzata da una decentralizzazione maggiore del potere decisionale.

2.2 Definizione e storia

Le DAO (Decentralized Autonomous Organization o Distributed Autonomous Organization) rappresentano una forma avanzata di organizzazione che sfrutta la tecnologia blockchain e gli smart contract per automatizzare e gestire le proprie attività e processi decisionali. Questo modello emergente di organizzazione elimina

la necessità di una struttura gerarchica tradizionale, affidandosi invece a regole e protocolli codificati su una rete blockchain per coordinare e governare le attività dell'organizzazione.

Gli interessi dei membri della DAO sono allineati attraverso meccanismi economici e di incentivazione basati su token, che consentono ai partecipanti di presentare e votare proposte all'interno dell'organizzazione.

Le blockchain fungono da fondamentali tecniche per le DAO, garantendo la sicurezza, la trasparenza e l'immutabilità delle transazioni e delle decisioni prese all'interno dell'organizzazione. Infatti, queste decisioni possono essere valutate pubblicamente da parte di tutti i membri, che possono anche verificare crittograficamente i risultati delle votazioni, chi ha votato e come è avvenuto il voto. Inoltre, grazie alla decentralizzazione, le DAO eliminano la necessità di una figura centrale di controllo, consentendo ai nodi della rete di contribuire e partecipare in modo autonomo e trasparente.

L'appartenenza ad una DAO può essere ottenuta o assegnata tramite l'acquisizione di token o attraverso contributi e partecipazione attiva. I membri della DAO hanno diritti specifici all'interno dell'organizzazione, che possono includere il diritto di partecipare al processo decisionale, di ricevere ricompense o benefici, o di accedere a risorse e servizi controllati dalla DAO stessa.

Fan et al. [17] hanno fornito un'immagine molto rappresentativa della governance delle DAO (figura 2.1). È stata infatti descritta come un triangolo tra registro distribuito, smart contract e meccanismi di voto. Il primo elemento è quindi la blockchain stessa, che sta alla base di questa struttura organizzativa. Gli smart contract definiscono e implementano le regole e gli accordi nella DAO. Il voto invece è lo strumento cardine che serve per prendere decisioni e modificare le regole esistenti. Questi tre pilastri lavorano insieme per garantire il funzionamento fluido e trasparente delle DAO.

Secondo i dati di DeepDAO [25] (maggio 2024), le DAO hanno accumulato un tesoro di oltre 32 miliardi di dollari, dimostrando il crescente interesse e coinvolgimento nella governance decentralizzata. Con oltre 3.1 milioni di elettori attivi, le DAO stanno emergendo come una forma alternativa e promettente di organizzazione, capace di rivoluzionare il tradizionale modello di gestione aziendale e ridurre i costi associati alla comunicazione, alla gestione e alla collaborazione all'interno delle organizzazioni.

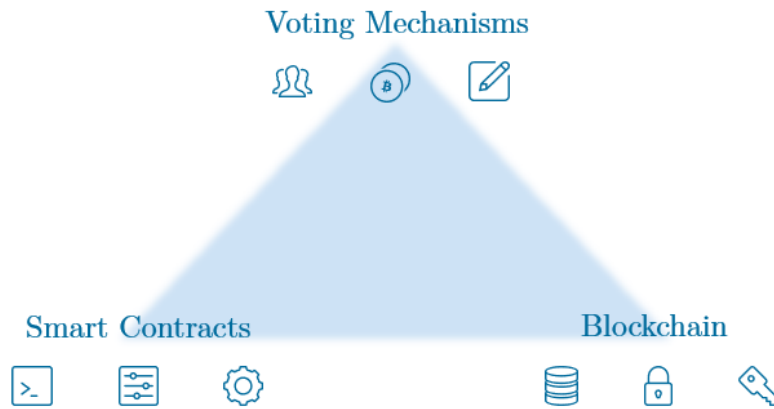


Figura 2.1: Struttura a triangolo della DAO

Ripercorriamo la storia di queste organizzazioni decentralizzate:

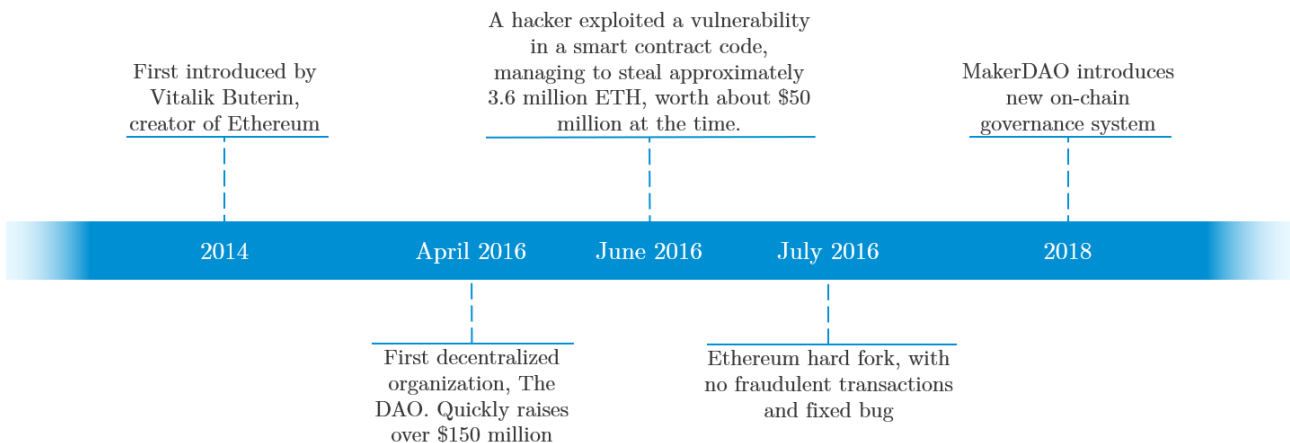


Figura 2.2: Linea temporale della storia delle DAO

La DAO è un'applicazione software presentata per la prima volta nel 2014 da Vitalik Buterin [20], il creatore di Ethereum. Come spiegato nel capitolo 1.3, Ethereum è diventata la prima piattaforma blockchain pubblica a supportare gli smart contract tramite la sua macchina virtuale Turing completa, EVM. Questa opportunità ha portato all'idea di codificare le regole gestionali ed operative delle organizzazioni

su blockchain tramite smart contract, permettendo all'organizzazione di operare autonomamente secondo logiche di business predefinite senza l'intervento di terze parti.

Due anni più tardi, ad Aprile 2016, The DAO è stata lanciata come prima organizzazione decentralizzata [3]. Anche se la maggior parte delle DAO sono state sviluppate su Ethereum, considerata infatti la pioniera delle reti DAO, altre piattaforme hanno adottato l'implementazione delle DAO, come Polygon, Solana, Substrate e Cardano.

In un breve periodo, The DAO ha raccolto ETH per un valore di più di 150 milioni di dollari, diventando il più grande progetto di raccolta fondi al mondo fino a quel momento [4]. Da allora, sono state proposte diverse DAO, alcune delle quali vedremo in seguito.

Qualche mese dopo la sua creazione, un hacker ha sfruttato una vulnerabilità del codice di uno smart contract per raccogliere ETH dalle vendite di token di The DAO. Questo è stato possibile a causa di una funzione mal implementata della piattaforma. L'attaccante è riuscito a rubare circa 3.6 milioni di ETH, all'epoca del valore di circa 50 milioni di dollari, facendo scendere il prezzo della moneta da oltre 20 dollari a meno di 13 dollari e causando perdite di circa 70 milioni di dollari [6].

In risposta a ciò, il fondatore di Ethereum ha inizialmente suggerito una soft fork, cioè una modifica software, con l'obiettivo di impedire all'hacker di spostare i fondi rubati e di offrire agli investitori un modo per recuperare i propri fondi. Questa proposta ha generato un acceso dibattito sulla moralità e sulla filosofia dell'accaduto, poiché la modifica unilaterale della storia della blockchain solleva questioni sulla resistenza alla censura e sulla non reversibilità, suscitando dubbi sul grado di controllo effettivo di Ethereum. Alla fine, la maggior parte degli investitori coinvolti nell'organizzazione ha concordato nell'implementare una modifica più incisiva, ovvero una hard fork, per restituire i fondi. Questa modifica ha portato molti utenti a modificare la loro versione della blockchain in cui l'attacco non si era mai verificato, creando così una blockchain parallela senza transazioni fraudolente e con il bug risolto [6].

Questo evento ha rappresentato un punto di svolta nella storia delle DAO. Tuttavia, ha anche evidenziato la natura controversa dell'autorità implicita nel codice blockchain. È importante sottolineare l'opinione dell'hacker, il quale sosteneva di aver agito conformemente ai termini dello smart contract. In una lettera anonima, l'hacker ha dichiarato di aver utilizzato una funzionalità specifica del contratto, sostenendo che la sua azione fosse legittima e legale secondo il contratto e la legislazione degli Stati Uniti. È stato quindi sottolineando il fatto che chiunque sfrutti il codice del contratto, eticamente o meno, sta solo esercitando i suoi diritti

[21].

Questo incidente ha sollevato domande importanti sulla responsabilità e sull'affidabilità dei sistemi decentralizzati come The DAO. Ha messo in discussione uno dei concetti alla base della blockchain, ovvero il non richiedere di doversi fidare degli altri nodi per poter eseguire le transazioni correttamente. Inoltre, ha evidenziato le sfide legate alla governance, alla legalità e all'eticità delle organizzazioni autonome decentralizzate.

Dopo questo incidente, sono trascorsi alcuni anni prima che l'interesse per le DAO tornasse a crescere. Nel 2018, il protocollo di stablecoin MakerDAO ha introdotto un sistema di governance on-chain, diventando uno tra i pionieri delle applicazioni basate su blockchain. Successivamente, nel 2020, è emersa una nuova ondata di DAO. Da allora, sempre più progetti basati su blockchain hanno adottato sistemi di governance on-chain, compresi molti protocolli di finanza decentralizzata. Vedremo qualche esempio di DAO esistente e delle loro applicazioni in seguito.

2.3 Caratteristiche e confronto

2.3.1 Lancio del progetto e ciclo di vita

Essendo gli smart contract uno dei pilastri delle organizzazioni decentralizzate, le DAO assorbono le proprietà di trasparenza, automazione e tracciabilità nel loro intero ciclo di vita. Maxim di Savaljev [26] ha analizzato le quattro fasi principali del ciclo di vita di una DAO:

1. **Pre DAO:** Questa prima fase comprende il lancio del progetto, avendo modellato e sviluppato una comunità. Si devono trattare diverse configurazioni e meccanismi, tra cui obiettivi, governance, economia dei token, piattaforma, processo decisionale e altro.
2. **Flat DAO:** Il nome di questa fase deriva dal fatto che, una volta lanciata, la DAO assume una struttura piatta, dato che ogni membro ha lo stesso ruolo senza alcun tipo di gerarchia. A questo punto, i membri della comunità più motivati contribuiscono alla DAO. Mentre la comunità cresce, nasce il bisogno di maggiore organizzazione e iniziano a sorgere le Sub-DAO, dipartimenti interni alla DAO che aiutano le interazioni sempre più complesse.
3. **DAO:** Le Sub-DAO iniziano a completare le attività interne alla DAO, assumendo sempre più indipendenza al di fuori dell'organizzazione stessa. In questa fase, la DAO è completa e funzionante.

4. **Post DAO:** Quest'ultima fase vede l'organizzazione stabilita e alcune Sub-DAO possono staccarsi dalla DAO principale e divenirne completamente indipendenti.

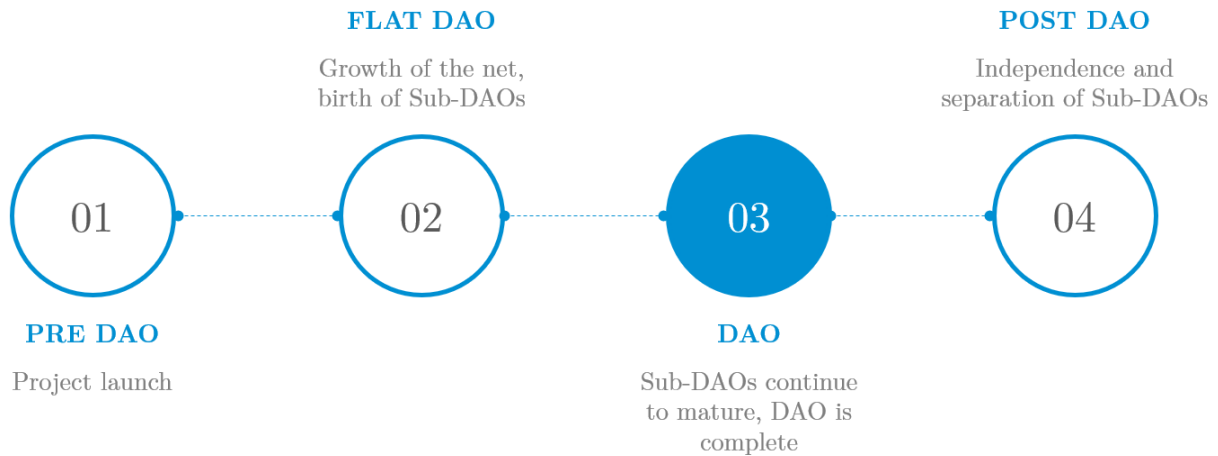


Figura 2.3: Ciclo di vita di una DAO

Dopo questo ciclo, la DAO funziona a pieno regime e si iniziano ad avanzare proposte che i membri possono votare. È importante sottolineare che le proposte presentate devono essere finalizzate a scopi specifici e nei tempi stabiliti, ma analizzeremo nel dettaglio questi meccanismi.

2.3.2 Proprietà

Partendo dall'acronimo DAO, possiamo delinearne le prime caratteristiche [2], [4], [8]:

Decentralizzazione: È il fattore chiave per questo tipo di struttura, dove è 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. Anche nel meccanismo di voto, il singolo membro della DAO non può decidere in modo unilaterale, a meno che non sia l'unico partecipante della rete.

Automazione: Idealmente, nella DAO il codice è legge. La gestione stessa si allontana dal sistema burocratico tradizionale, trovando invece fondamento nell'autonomia della comunità. Una DAO funziona seguendo regolamentazioni e modelli di collaborazione definiti da tutte le parti coinvolte. Ciò favorisce

il consenso e l'affidabilità all'interno della comunità, contribuendo a ridurre notevolmente i costi associati alla fiducia, alla comunicazione e alle transazioni.

Organizzazione: Utilizzando gli smart contract come base, le regole operative della DAO sono trasparenti e aperte. Si delineano, quindi, chiaramente la responsabilità e l'autorità dei partecipanti, nonché i termini relativi a ricompense e penali. Coloro che contribuiscono finanziariamente, partecipano attivamente e si assumono responsabilità associate a corrispondenti poteri e benefici. Questo approccio unisce potere, responsabilità e interessi in modo coerente, garantendo un funzionamento coordinato e ordinato dell'organizzazione.

Dopo questa prima panoramica, elenchiamo altre importanti proprietà di una DAO [2], [4], [8]:

- Nel contesto di una DAO, tutte le transazioni e le decisioni sono completamente trasparenti e immutabili. Si promuove così la fiducia tra i membri e le parti coinvolte, nonostante i membri non si conoscano a vicenda. Le DAO utilizzano una blockchain per registrare e gestire i voti, garantendo procedure di voto altamente trasparenti che eliminano rischi di contestazioni nelle decisioni, frodi o errori accidentali.
- Un'altra caratteristica chiave è la loro capacità di garantire che le parti coinvolte non possano manipolare o censurare le transazioni. Infatti, le DAO implementano smart contract e meccanismi di voto che riducono il rischio di comportamenti egoistici da parte dei singoli membri, proteggendo così l'integrità delle transazioni e degli interessi collettivi.
- L'interoperabilità è una funzionalità che consente alle DAO di interagire e collaborare tra loro in maniera fluida. Ciò significa che possono avvenire scambi di dati e risorse in modo diretto e autonomo, favorendo un sistema decentralizzato.
- Per coinvolgere attivamente la comunità e garantire un contributo continuo, si implementano incentivi basati su token. I membri possono ottenerli partecipando all'organizzazione o impegnandoli per sostenere dei progetti specifici. I diritti economici, di partecipazione, di governance e di utilità possono essere associati a token. Questo tipo di incentivo favoriscono la crescita e il coinvolgimento attivo della comunità della DAO.
- Infine, come conseguenza di un processo decisionale più trasparente ed autonomo, si ottiene un'organizzazione più reattiva. In questo modo infatti, le DAO possono garantire una maggiore efficienza operativa e capacità di innovazione, adattandosi rapidamente alle diverse condizioni ed esigenze della comunità.

2.3.3 Governance

Uno spazio molto importante che bisogna dedicare quando si tratta di DAO, è quello della governance. Per governance della DAO ci si riferisce al processo attraverso il quale vengono prese decisioni e gestite le attività all'interno dell'organizzazione.

Le attuali esperienze con il voto nei progetti DAO evidenziano la decentralizzazione e la democrazia delle comunità DAO, ma presentano sfide nel raggiungere il consenso, mostrando un'efficacia inferiore rispetto ai metodi tradizionali di voto [2]. La tecnologia blockchain può migliorare i processi democratici riducendo i costi, ma il voto diretto richiede un impegno continuo.

Standardizzare la governance blockchain è essenziale per migliorarne l'affidabilità ed efficienza, rispettando le normative e le responsabilità. La governance blockchain coinvolge autorità decisionali, incentivi e meccanismi di responsabilità per guidare il comportamento nell'uso di risorse scarse. Tuttavia, non esiste un quadro universale per comprendere la governance blockchain, e molti modelli teorici non sono completamente realizzabili on-chain [3].

Alcune DAO stanno esplorando meccanismi come la delega del voto, il voto quadratico e i mercati di previsione per migliorare l'efficienza decisionale e ridurre l'apatia degli elettori. Alcuni di questi esempi saranno approfonditi in seguito.

2.3.4 Tesoreria

La tesoreria è il cuore finanziario dell'organizzazione, gestito in maniera decentralizzata ed automatica. Tramite questa, la DAO raccoglie fondi dagli investitori, genera entrate dall'attività principale dell'organizzazione, paga i contribuenti e fornisce un ritorno agli investitori [48].

Anche questo aspetto deve seguire le caratteristiche della DAO. In particolare, tutte le decisioni di investimento si sottopongono al voto dei partecipanti e nessun singolo membro può accedere ai fondi accumulati, a meno che non sia l'unico utente dell'organizzazione [8].

Esistono diverse tipologie di fondi con cui la DAO può gestire la tesoreria: possono essere custoditi token di governance, stablecoin o altri token (come Bitcoin o Ether) [48], [49]. Per quanto riguarda i token di governance, questi sono emessi direttamente dalla DAO e rappresentano la partecipazione del membro all'interno dell'organizzazione. Infatti, tramite questi si ottengono diritti di voto sulle decisioni interne, inclusa la gestione della stessa tesoreria.

In generale, i fondi sono controllati attraverso un wallet multisig o tramite uno smart contract che richiede approvazioni multiple. Questo aumenta la sicurezza nella gestione e la trasparenza di tutte le operazioni.

2.3.5 Confronto con le organizzazioni tradizionali

Abbiamo sottolineato più volte la diversità della natura delle DAO rispetto a quella convenzionale. La tabella 2.1, nella pagina seguente, riassume le principali caratteristiche di queste organizzazioni decentralizzate messe a confronto con quelle delle organizzazioni tradizionali [3], [8], [11].

Le DAO offrono diversi vantaggi, tra cui una notevole diminuzione dei costi associati alle transazioni, compresi i costi relativi alla gestione e al mantenimento dei sistemi di controllo [11]. Ciò è dovuto all'utilizzo degli smart contract, che unificano e automatizzano le varie procedure di coordinamento, conferma, verifica, approvazione e attuazione delle decisioni gestionali.

Inoltre, poiché le DAO seguono regole e modelli di collaborazione concordati da tutte le parti coinvolte, dovrebbe essere più facile ottenere consenso e fiducia all'interno di un'organizzazione decentralizzata. Questo si traduce in una significativa riduzione dei costi legati alla fiducia e alla comunicazione [11].

2.4 Problematiche

Essendo la DAO un progetto implementato solo negli ultimi anni, non si è ancora arrivati alla sua forma definitiva e deve quindi affrontare diverse sfide. Nelle sezioni che seguono elenchiamo le problematiche relative alla sicurezza, alla privacy, allo stato giuridico, alle limitazioni tecniche e alla governance.

2.4.1 Sicurezza

Data la sua struttura, la DAO eredita i problemi della blockchain, primo tra tutti quello legato alla sicurezza [6]. Le sfide legate alla gestione del rischio che derivano dalle strutture decentralizzate e automatizzate sono significative. La tecnologia blockchain, grazie alla sua natura a prova di manomissione, rende estremamente difficile apportare modifiche ad una DAO o agli smart contract che la governano dopo che sono stati implementati.

DAO		Organizzazione tradizionale	
Democratizzata	Il sistema di una DAO si basa su un piano di parità, in modo meno gerarchico e più democratico, gestito dal consenso distribuito	Gerarchica	Il sistema tradizionale si affida ad un rapporto fiduciario dei membri, imponendo una gerarchia interna
Sistema di votazione per le modifiche	Tutte le eventuali modifiche da adottare devono essere votate dai membri dell'organizzazione	Modifiche proposte da un solo gruppo	Alcune modifiche possono essere richieste anche da solo un partito dell'organizzazione, non per forza dall'intera struttura
Conteggio automatizzato dei voti	Il conteggio e il risultato delle votazioni è completamente automatizzato e non necessita di una terza parte	Conteggio interno dei voti	Se vi è una votazione, il conteggio avviene all'interno e i risultati si contano manualmente
Sistemi automatici e decentralizzati	Attraverso l'utilizzo degli smart contract, i servizi forniti sono interamente automatizzati e decentralizzati	Centralizzato e con trattamento umano	L'organizzazione tradizionale necessita dell'intervento umano e centralizzato per fornire i diversi servizi
Attività trasparente e pubblica	Grazie alla tecnologia blockchain, tutte le attività sono svolte in maniera trasparente e pubblica	Attività private e limitate	Le attività svolte sono principalmente private o comunque limitate al pubblico
Il codice è legge	Le DAO sono governate secondo le regole rigide scritte negli smart contract, consentendo all'organizzazione di essere deterministica	Sistema legale del paese	La struttura tradizionale segue le normative e i contratti legali applicati secondo il sistema legale del paese

Tabella 2.1: Confronto tra DAO e organizzazioni tradizionali

Questa caratteristica può essere sfruttata dagli attaccanti per trarre profitto da eventuali falle negli smart contract. È stato proprio questo il problema alla base dell'attacco a The DAO del 2016, di cui abbiamo parlato nella sezione 2.2. Tali questioni di sicurezza hanno notevolmente limitato lo sviluppo delle DAO [4].

Quindi, la robustezza delle DAO dipende fortemente dall'integrità dei loro smart contract, che si può rafforzare investendo nella sicurezza e nell'analisi approfondita dei rischi durante la progettazione e l'implementazione delle DAO e dei relativi smart contract.

2.4.2 Privacy

Il mancato rispetto degli attributi di sicurezza, come l'anonimato, può compromettere gravemente le DAO. Come sottolineano Liu et al. [6], il vero pericolo non risiede solo nelle singole vulnerabilità, ma piuttosto nella combinazione di un attacco al software con un attacco alla struttura economica sottostante. Questo introduce un secondo problema, che riguarda la privacy degli utenti.

L'autenticazione dell'utente è importante se si parla di responsabilità, ma al contempo solleva gravi questioni legate alla privacy. Basta pensare alla struttura della blockchain per capire questa problematica: ogni transazione è visibile chiaramente per quanto riguarda mittente e destinatario, quindi un'analisi dei cluster può rivelare le associazioni tra i diversi nodi. Senza pensare all'accesso con le chiavi private, che potrebbero essere divulgate, sia intenzionalmente che accidentalmente, e gli attaccanti potrebbero sfruttare tali informazioni per intercettare gli utenti [10].

Questi problemi di privacy si aggravano particolarmente quando viene stabilito un legame diretto tra identità e transazioni. Infatti, se consideriamo l'implementazione del voto sulle DAO, si presuppone che ogni voto sia affiancabile all'identità dell'elettore, rendendo molto difficile l'anonimato della votazione.

2.4.3 Stato giuridico

Un'altra incognita che insorge trattando di blockchain e DAO riguarda l'aspetto giuridico poco chiaro. Attualmente, le DAO non hanno una definizione legale chiara a livello globale.

Poiché le DAO presentano caratteristiche come decentralizzazione e anonimato, possono sorgere problemi legali durante il loro funzionamento che comportano difficoltà di responsabilità. Come spiegato da Wang et al. [4], alcune persone le associano ad una società in nome collettivo (S.n.c.) insieme ai loro investitori. Questo implica che ogni stakeholder, investitore o possessore di token di una DAO sia responsabile dei debiti o delle azioni legali che l'organizzazione potrebbe dover affrontare. Al contrario, altri le considerano più simili a contratti di investimento o titoli.

Uno dei vantaggi tradizionali di un'entità legale, come una società per azioni (S.p.a.) o una società a responsabilità limitata (S.r.l.), è la protezione dei beni personali dei proprietari dai creditori. Le DAO non godono di questi vantaggi perché il sistema legale non le riconosce come entità giuridiche con responsabilità limitata. A causa di queste limitazioni, grandi aziende, investitori e altre entità

regolamentate potrebbero esitare ad investire e supportare le DAO per timore che i membri possano esporre altri asset a rischi [8].

Al momento, alcuni stati stanno lavorando per adattare le entità commerciali tradizionali alle DAO. Ad esempio, nel Vermont nel 2018 è stato approvato un emendamento allo statuto delle società a responsabilità limitata per consentire la creazione di “S.r.l. basata su blockchain” [27]. Leggi simili sono state adottate in Wyoming nel 2021 [28], nelle Isole Marshall nel 2022 [29] e nello Utah nel 2023 [30], riconoscendo legalmente le DAO come società a responsabilità limitata (S.r.l.).

Nel corso del tempo, si confida nel fatto che la necessità di ricerche approfondite sulla blockchain e sulle DAO diventi più accettata e meno soggetta a controversie, contribuendo così a consolidare il ruolo di questa tecnologia nel panorama digitale futuro.

2.4.4 Limitazioni tecniche

La DAO aspira a far sì che il codice sia la legge, ma incontrare questa aspirazione nella pratica è problematico [4], [8]. Questo è dovuto ad un significativo divario semantico tra le norme legali e quelle codificate negli smart contract. Infatti gli smart contract sono rigorosi e scritti dettagliatamente per consentire una corretta esecuzione, a differenza delle norme legali che spesso hanno l’obiettivo di garantire maggiore versatilità sfruttando quindi un linguaggio più ambiguo e flessibile [4].

Inoltre, l’utilizzo di testi legali per descrivere le logiche degli smart contract può creare spazio ad ambiguità o errori di interpretazione sul funzionamento effettivo degli smart contract di una DAO. Questo potrebbe compromettere l’efficacia e la convenienza dei contratti [8].

2.4.5 Corporate governance

Un’ultima problematica è legata alla governance. Essendo la DAO un’applicazione della blockchain nella governance, vengono sollevate questioni aggiuntive rispetto alla blockchain convenzionale [6]. Sebbene gli smart contract possano migliorare l’efficienza operativa, non riescono ad eliminare le complessità sociali e politiche della governance [8].

Tra questi, potrebbero esserci rischi di monopolio dovuti all’accumulo di token da parte di pochi o, al contrario, alcuni nodi potrebbero non avere abbastanza

coinvolgimento nelle attività della DAO. La dipendenza dai token per la governance può favorire gruppi di partecipanti attivi che accumulano potere di voto, compromettendo così la decentralizzazione.

2.5 Architettura

Finora abbiamo fornito una panoramica dettagliata sulle DAO; ora passiamo ad esaminarne l'architettura. Per descrivere l'architettura di una DAO, abbiamo unito le strutture a cinque livelli esposte da Wang et al. [4] e Qin et al. [5] (vedi figura 2.4). Nelle prossime sezioni saranno analizzati i livelli tecnologico di base, esecutivo, di coordinamento, organizzativo e applicativo, riprendendo quanto descritto da queste fonti.

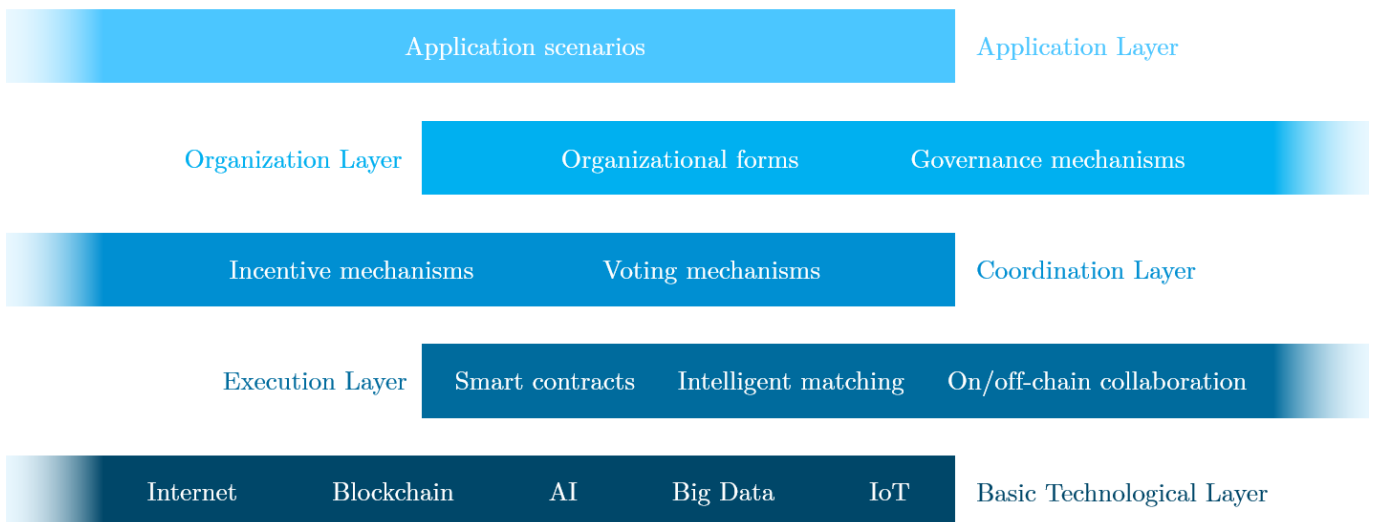


Figura 2.4: Architettura di una DAO

2.5.1 Livello tecnologico di base

Il primo livello costituisce l'infrastruttura fondamentale che supporta la DAO e le applicazioni che ne derivano.

- **Protocollo Internet:** La DAO si basa su una rete P2P per incentivare la partecipazione di nodi distribuiti globalmente.

- **Blockchain:** La caratteristica distintiva della DAO è la decentralizzazione e l'autonomia, per cui la tecnologia blockchain è essenziale.
- **Intelligenza Artificiale:** Con l'avanzamento della tecnologia dell'Intelligenza Artificiale (AI), ogni nodo di una DAO può diventare un agente autonomo.
- **Big Data:** La tecnologia dei Big Data può essere impiegata per raccogliere in tempo reale varie tipologie di dati all'interno di una DAO, fornendo così informazioni cruciali per comprendere lo sviluppo di una DAO.
- **Internet of Things:** La blockchain può essere integrata con l'Internet of Things (IoT) per formare la Blockchain of Things (BoT), per digitalizzare ed integrare dispositivi intelligenti e asset fisici nella DAO.

2.5.2 Livello esecutivo

Questo secondo livello comprende le tecnologie esecutive relative al consenso e alla gestione dei problemi.

- **Smart contract:** Le organizzazioni si basano su contratti per regolare le relazioni e garantire i diritti delle parti coinvolte. Nel caso delle DAO, ci si affida a smart contract, che portano a queste organizzazioni sicurezza, trasparenza ed equità.
- **Algoritmi smart:** Le DAO si affidano alla digitalizzazione per la loro governance. Gli algoritmi smart, a differenza degli smart contract, hanno grandi capacità di analisi dati e ragionamento decisionale, migliorando l'attività di coordinamento delle DAO.
- **Abbinamento intelligente:** Le DAO utilizzano spesso tecnologie AI per facilitare l'interconnessione di individui, organizzazioni e servizi su reti decentralizzate. Questo approccio riduce i costi di comunicazione e migliora l'efficienza complessiva della DAO.
- **Collaborazione on-chain e off-chain:** A differenza della gestione centralizzata, le DAO adottano un approccio collaborativo sia on-chain che off-chain. La governance on-chain è utilizzata per gestire il consenso e le decisioni tramite smart contract, garantendo equità e trasparenza. Allo stesso tempo, la governance off-chain consiste in misure adottate per stabilire e mantenere il consenso, spesso limitata dalla tecnologia attuale.

2.5.3 Livello di coordinamento

Questo livello ha l'obiettivo di regolare il meccanismo di coordinamento all'interno di una specifica divisione del lavoro. Le DAO promuovono la creazione di un meccanismo autonomo e dinamico di coordinamento, automatizzato attraverso incentivi, e gestiscono il processo decisionale che si avvale del consenso collettivo in un ambiente senza fiducia.

- **Meccanismo di incentivazione:** Per coinvolgere a pieno i membri nella governance della DAO, migliorandone sicurezza e affidabilità, sono stati creati vari meccanismi di incentivazione. Questi includono la generazione e distribuzione di token, reputazione e poteri di governance. Combinando diversi incentivi, si possono soddisfare le esigenze dei membri della DAO, motivandoli a raggiungere gli obiettivi organizzativi attraverso il coordinamento. Ogni DAO ha la capacità di emettere il proprio token e definirne vari parametri come la circolazione, la modalità di distribuzione e altri aspetti del modello di token. L'obiettivo è promuovere l'allineamento degli incentivi tra i partecipanti, creando una situazione vantaggiosa per tutti i nodi coinvolti.
- **Meccanismo di voto:** Le decisioni cruciali riguardanti lo sviluppo delle DAO, come cambiamenti dei protocolli, questioni di governance e controllo dei fondi, vengono votate sulla blockchain da tutti i membri della DAO. La gestione quotidiana e il funzionamento delle DAO sono invece solitamente responsabilità di un comitato eletto dai membri. In caso di disaccordi o controversie tra membri, vengono generalmente utilizzati tribunali decentralizzati o meccanismi di "rage quitting" per la risoluzione.

Data l'importanza di questi meccanismi, la sezione 2.6 è interamente dedicata ad essi.

2.5.4 Livello organizzativo

Il livello organizzativo è focalizzato sull'impiego delle tecnologie per perseguire gli obiettivi complessivi dell'organizzazione a livello macro. Questa struttura costituisce il fondamento delle DAO, rappresentando un sistema di collaborazione con obiettivi strategici specifici e con il personale come elemento centrale.

Uno dei principali problemi gestionali riguarda la divisione del lavoro, ovvero l'assegnazione di compiti differenti. Le DAO gestiscono questo tema definendo poteri, responsabilità e allocazione delle risorse in modo distribuito e decentralizzato, costruendo così una struttura organizzativa di proprietà della comunità.

- **Forma organizzativa:** Le DAO possono essere classificate in tre tipologie in base al grado di decentralizzazione e distribuzione. Queste includono centri multipli distribuiti, centri interamente distribuiti e centri diseguali. Nei primi, il potere del nodo centrale tradizionale è suddiviso tra più piccoli nodi centrali, creando uno stato di coesistenza equilibrata. Nei centri interamente distribuiti, il potere è uniformemente distribuito a tutti i nodi; mentre nei centri di disuguaglianza, la distribuzione del potere è disuguale tra i nodi così che i membri abbiano diritti organizzativi differenti.
- **Meccanismo di governance:** Le DAO generalmente adottano tre meccanismi di governance. Questi includono la proposta off-chain (al di fuori della blockchain), la proposta on-chain (all'interno della blockchain) e una combinazione di queste due. Le proposte off-chain vengono presentate in un forum organizzato dalle DAO e votate al di fuori della blockchain, mentre le proposte on-chain sono avanzate e votate direttamente sulla blockchain. La combinazione di queste coinvolge la presentazione delle proposte nel forum organizzato prima dalle DAO e la pubblicazione sulla blockchain per farle votare dai membri.

2.5.5 Livello applicativo

La DAO assume una vasta gamma di forme e applicazioni, che risiedono in quest'ultimo livello dell'architettura. A seconda dei servizi forniti, può coinvolgere valute digitali come Bitcoin, piattaforme di sviluppo pubbliche come Ethereum, o persino dispositivi IoT interconnessi come sensori per il monitoraggio energetico. Inoltre, abbiamo già accennato alle differenze sul grado di decentralizzazione, parlando di DAO basate su blockchain pubbliche o consortium (sezione 1.1).

Tra le DAO che analizzeremo faremo un'analisi dettagliata sull'architettura di Aragon (sezione 2.9.2), seguendo la struttura appena descritta.

2.6 Meccanismi di coordinamento

In questa sezione analizziamo i meccanismi che sono stati accennati nel livello di coordinamento (2.5.3): il meccanismo di incentivazione e il meccanismo di voto.

2.6.1 Meccanismo di incentivazione

I meccanismi di incentivazione sono sfruttati dalle DAO per unire i membri che condividono benefici in un ambiente basato su blockchain, incoraggiandoli ad interagire e collaborare efficacemente per raggiungere obiettivi comuni. La progettazione e la ricerca dei meccanismi di incentivazione delle DAO devono tenere conto delle caratteristiche e delle esigenze dei diversi tipi di membri [5].

Gli incentivi nelle DAO possono essere distinti in due categorie: pecuniari e non pecuniari. I primi sono incentivi trasferibili che includono premi di contribuzione, profitti, remunerazioni e ricompense, spesso sotto forma di token fungibili o non fungibili (NFT). Gli incentivi non trasferibili comprendono la reputazione, la fiducia e il riconoscimento, non necessariamente di natura economica [5]. Beck et al. [10] sottolineano l'importanza degli incentivi perché “un sistema con incentivi allineati consente agli agenti di scegliere liberamente i propri comportamenti, ma utilizza gli incentivi per renderli inclini a scegliere azioni che coincidono con gli obiettivi del progetto del sistema”.

I meccanismi di incentivazione regolano l'acquisizione e l'utilizzo di questi incentivi, ponendo la sfida di progettare modelli che soddisfino le esigenze specifiche dei membri e gli obiettivi comuni delle DAO. L'efficacia di questi meccanismi dipende dalle esigenze e dagli obiettivi individuali, richiedendo misurabilità e personalizzazione nella progettazione degli incentivi [5].

2.6.2 Meccanismo di voto

Il voto è uno dei tre pilastri, oltre la blockchain e gli smart contract, che abbiamo nominato nella definizione di DAO (sezione 2.2). È quindi necessario conoscere le meccaniche del voto per comprendere a pieno la struttura dell'organizzazione autonoma decentralizzata.

Fan et al. [17] hanno analizzato sette tipi di meccanismi di voto che sono tipicamente utilizzati nelle DAO attuali:

1. **Maggioranza Relativa Autorizzata (MRA):** Questo è il metodo di voto più comune, dove il passaggio di una proposta richiede il sostegno di almeno il 50% del potere di voto impiegato in questa votazione. Tuttavia, può essere manipolato se ci sono proposte ingannevoli a cui i membri non prestano sufficiente attenzione. Questo tipo di proposta rischiosa è detta “slip-through” e rappresenta una minaccia alla sicurezza.

2. **Quorum Basato su Token (TBQ):** Simile all'MRA, ma richiede una partecipazione più elevata per approvare una proposta, riducendo il rischio di approvazione "slip-through" e aumentando la sicurezza della votazione. La maggior adesione si può ottenere inserendo una soglia di attenzione, che potrebbe aumentare la decentralizzazione coinvolgendo più nodi. Tuttavia, questo meccanismo richiede più tempo per raggiungere la partecipazione necessaria.
3. **Voto Quadratico:** Il voto quadratico rappresenta un sistema di distribuzione del potere di voto che coniuga gli aspetti di "un token, un voto" (1T1V) e "una persona, un voto" (1P1V). Questo concetto è stato originariamente proposto per applicazioni nella politica democratica ed è stato successivamente adottato anche nelle DAO. In questo sistema, il costo marginale aumenta quando un utente vota ripetutamente per la stessa opzione. Per esempio, il costo per un singolo voto è di 1 token, mentre per due voti sono necessari 4 token, per tre voti 9 token, e così via.
4. **Democrazia Liquida:** In questo sistema, i nodi possono votare direttamente o delegare il loro diritto di voto a rappresentanti esperti. Si migliora l'efficacia complessiva del voto perché il delegato è solitamente più attivo dei nodi ordinari, e ciò dovrebbe portare ad una più veloce elaborazione dei voti delegati. Questo meccanismo potrebbe minare il decentramento, tuttavia, la "liquidità" è concepita per poter direzionare la delega diversamente in qualsiasi momento, attenuando così la centralizzazione.
5. **Voto Ponderato:** I membri con più reputazione o conoscenza hanno più peso nel voto, incoraggiando decisioni informate ma potenzialmente limitando il potere decisionale decentralizzato. Un esempio è il Knowledge-Extractable Voting, un sistema che conferisce maggior potere di voto agli esperti di un determinato campo, basato sui loro token di conoscenza individuali. I token di conoscenza premiano gli utenti quando le loro scelte di voto si rivelano corrette rispetto al risultato vincente, mentre penalizzano gli utenti quando le loro scelte si discostano dal risultato vincente.
6. **Rage Quitting:** I membri possono ritirarsi dalla DAO e recuperare i loro fondi in token se non sono d'accordo con una decisione approvata, limitando il controllo da parte di pochi membri influenti. In questo contesto, tra l'approvazione di una proposta e l'esecuzione dei risultati del voto, ci sarà un "periodo di grazia". Durante questo intervallo di tempo, i membri hanno la possibilità di ritirarsi dall'organizzazione se sono insoddisfatti del risultato, agendo "in preda alla rabbia". Questa opzione offre ai membri una scelta più flessibile e riflette il principio del decentramento del voto. Tuttavia, è importante notare

che questo “periodo di grazia” rallenta il processo di voto, avendo un impatto negativo sull’efficienza complessiva del sistema decisionale.

7. **Holographic Consensus (HC):** Introduce un mercato di scommesse per le proposte, coinvolgendo i membri e il pubblico nel processo decisionale. HC è stato sviluppato da DAOstack, uno stack software open source per la creazione e l’esecuzione di DAO. HC è progettato per migliorare l’efficacia delle decisioni prese all’interno delle DAO attraverso l’uso di mercati di previsione e un token specifico per le scommesse chiamato GEN. Questo approccio consente ai membri della DAO e al pubblico di scommettere su proposte che credono passeranno o falliranno. Queste scommesse sono fatte attraverso l’utilizzo di GEN, con “up-staking” per il successo di una proposta e “down-staking” per il suo fallimento. Gli scommettitori che fanno previsioni accurate rispetto ai risultati delle votazioni vengono ricompensati con un aumento dei loro GEN. HC opera con due modalità per raggiungere un risultato di voto valido:

- (a) **Proposte Boosted:** Le proposte che raccolgono una quantità di GEN sopra una certa soglia diventano “boosted” e richiedono solo la maggioranza relativa (ovvero la semplice prevalenza numerica dei voti favorevoli) per essere approvate.
- (b) **Proposte in Coda:** Le proposte che non raccolgono abbastanza GEN rimangono in coda e richiedono la maggioranza assoluta di tutti i voti (corrispondente alla metà più uno degli aventi diritto al voto) per essere approvate.

L’uso dei GEN consente alle persone di manifestare le proprie opinioni sulle proposte, anche se non dispongono di un grande potere di voto all’interno della DAO. Tuttavia, HC non è immune da critiche. Ad esempio, coloro che scommettono sui risultati delle proposte hanno un maggiore incentivo a partecipare al voto, il che potrebbe influenzare i risultati e distorcere la vera volontà della comunità.

Un’altra fonte [31] ha nominato anche quest’ultimo meccanismo di voto:

8. **Voto Conviction:** Per determinare il peso di un voto, questo sistema si basa sia sulla preferenza aggregata che sul tempo. In questo contesto, i nodi della rete possono esprimere le proprie preferenze sulle proposte attraverso lo staking dei propri token per un periodo di tempo specifico. Il potere di voto di un membro è direttamente proporzionale alla durata del periodo di staking: più lungo è il periodo, maggiore è la “convinzione” che il membro ha nella propria votazione. Questo meccanismo mira ad incoraggiare una riflessione attenta sulle implicazioni a lungo termine delle proposte, scoraggiando il pensiero e la speculazione a breve termine.

Ding et al. [31] hanno comparato diversi meccanismi di voto, alcuni dei quali sono stati spiegati sopra, prendendo in considerazione parametri come efficienza, equità, scalabilità, robustezza e incentivazione. Da questa analisi, sono arrivati alla conclusione che nessuno schema è perfetto, ma ognuno presenta dei pro e dei contro. In particolare, un buon compromesso è quello di combinare meccanismi diversi e provare a modellarne uno migliore.

2.7 Procedura e potere di voto

Come già abbiamo sottolineato, il ruolo del voto all'interno di una DAO è significativo ed è caratterizzato da una forte automazione, trasparenza e parità. In questa sezione si analizza l'importanza della correttezza dei sistemi di voto, le metriche notevoli riguardanti il potere di voto, la procedura effettiva della votazione e, infine, la differenza con la struttura convenzionale.

2.7.1 Rilevanza della correttezza nei sistema di voto

Nella sezione 2.6.2 abbiamo elencato i principali meccanismi di voto attualmente impiegati nelle DAO, ma è fondamentale capire che la mancata attenzione nell'implementazione di questo processo può portare a diversi problemi.

Fan et al. [17] sottolineano alcune delle problematiche che potrebbero sorgere. In primo luogo, meccanismi di voto difettosi possono rendere vulnerabile il sistema a minacce per la sicurezza, come manipolazioni, permettendo agli attaccanti di danneggiare gli interessi dei nodi partecipanti. Un altro punto da analizzare è la distribuzione corretta del potere di voto, senza la quale si può arrivare a decisioni non efficaci e poco professionali, considerando che ogni nodo ha competenze e conoscenze limitate. Inoltre, bisogna ricordare che le regole negli smart contract possono essere modificate solo tramite le votazioni, quindi, se il meccanismo è difettoso o dannoso, questo può portare a modifiche imprudenti o addirittura a minacce significative per le DAO. Un'ultima preoccupazione riguarda il mantenimento della decentralizzazione delle DAO. Infatti, copiare i meccanismi di voto delle organizzazioni tradizionali centralizzate può condurre ad un processo decisionale centralizzato, contrariando lo scopo stesso delle DAO.

Quest'ultimo problema è stato sottolineato anche da Feichtinger et al. [7], che hanno esaminato i sistemi di governance di 21 organizzazioni autonome decentralizzate arrivando alla conclusione che “Sebbene si assista ad una leggera tendenza verso la decentralizzazione, il potere di voto è ancora altamente centralizzato nella

maggior parte delle DAO. Infatti, per 17 dei 21 sistemi di governance analizzati, la maggioranza del potere di voto, che è sufficiente per decidere qualsiasi voto, è controllata da meno di 10 partecipanti”.

2.7.2 Potere di voto

Introduciamo ora un nuovo concetto, che abbiamo citato più volte: il potere di voto. Quest’ultimo rappresenta il valore di voto di un membro su una proposta, e la sua distribuzione varia tra il voto convenzionale e quello all’interno di una DAO. Nella maggior parte delle DAO attuali, questo potere segue il principio “un token, un voto” (1T1V) ed è quindi determinato dalla quantità di token posseduti da ciascun elettore. Tuttavia, nonostante la sua apparente equità, questo schema può favorire un controllo plutocratico, voto tattico e altre pratiche che contrastano l’obiettivo di decentralizzazione delle DAO [17].

Al contrario, il modello “una persona, un voto” (1P1V) rappresenta la forma più decentralizzata di distribuzione del potere di voto, assegnando un peso di voto uguale a ciascun elettore. Tuttavia, questo approccio è poco utilizzato nelle DAO a causa delle sfide che presenta nel gestire proposte che richiedono grandi finanziamenti [17].

Pertanto, le DAO attuali tendono a bilanciare tra questi due estremi, cercando un modello di distribuzione del potere di voto che sia equo e allo stesso tempo pratico per il funzionamento e lo sviluppo della piattaforma.

Negli studi di Feichtinger et al. [7] e di Fritsch et al. [9] sono state trattate due misure della distribuzione del potere di voto:

- **Coefficiente di Gini:** Rappresenta una misura di disuguaglianza tra le più comunemente usate. I valori di questo coefficiente variano da 0.0 a 1.0 e rappresentano, rispettivamente, il livello di uguaglianza perfetta e livello in cui un solo nodo possiede tutto. Più nel dettaglio, questo fattore misura l’area tra la curva di Lorenz di una specifica distribuzione e la curva di perfetta uguaglianza.
- **Coefficiente di Nakamoto:** Misura il grado di decentralizzazione di un sistema, ovvero quante parti devono collaborare per ottenere il controllo totale. Nel contesto di una DAO, rappresenta il numero di address necessari per accumulare più del 50% del potere decisionale. Questo parametro è cruciale per valutare quanto il controllo sia distribuito o concentrato all’interno di una specifica piattaforma di governance decentralizzata.

Questi due coefficienti si possono adattare anche nel contesto di token delegati, nel caso di democrazia liquida per esempio. Sotto queste condizioni, oltre alla distribuzione tra i possessori di token, si deve tenere in considerazione anche la distribuzione del potere di voto tra i delegati [7], [9].

Dopo aver definito cosa si intende per “grandi delegati”, ovvero coloro che insieme detengono almeno il 90% dei diritti di voto, Fritsch et al. [9] sollevano una questione significativa: quanto spesso vincono contro la minoranza dei piccoli delegati? In quell’analisi, si arriva ad affermare che questo avviene solo in casi isolati. Infatti, nella governance di Compound “i grandi delegati hanno votato in modo diverso da quelli piccoli solo su 6 delle 84 proposte”. Anche per la governance di Uniswap la situazione era simile: “i delegati grandi e piccoli non erano d’accordo su una singola proposta, e di molto poco: sulla proposta 7, i delegati grandi erano a favore per il 50.5%, mentre i delegati piccoli si opponevano (il 34.5% era a favore)”.

Sempre nello studio citato, viene sottolineato che, in Compound e Uniswap, i partecipanti al voto sono meno del 10% dei token totali. Questo dimostra quanto i sistemi di governance delle DAO siano ancora centralizzati. Di quest’ultimo aspetto ne parleremo nella sezione dedicata alle DAO esistenti e porteremo come esempio proprio l’analisi di Fritsch et al. [9] su tre diversi modelli di DAO.

2.7.3 Procedura di voto

La struttura fondamentale di tutte le procedure di voto delle DAO comprende la presentazione di una proposta, la raccolta dei voti, la verifica di alcune condizioni e l’esecuzione dei risultati. Nella spiegazione dell’architettura abbiamo accennato ai diversi meccanismi di governance che possono esserci all’interno di una DAO (sezione 2.5.4). Quello proposto di seguito è l’ultimo dei tre elencati, ovvero quello in cui la proposta è presentata in un forum off-chain mentre la votazione avviene on-chain. La figura 2.5 rappresenta la procedura descritta di seguito.

Come spiegano Zhao et al. [19], questo processo ha inizio con la formulazione di una proposta. I nodi interessati al potenziamento della piattaforma sono invitati a condividere commenti, suggerimenti e proposte in un forum online dedicato. Queste possono riguardare sia aspetti operativi che strategici, come la modifica di parametri o l’introduzione di funzionalità aggiuntive. In questa fase, gli altri nodi discutono di queste proposte in varie modalità off-chain per valutare l’interesse generale. La scelta di includere una proposta per un voto formale on-chain è di norma presa dal team di base, che prepara la proposta ufficiale basandosi sulle idee che hanno ricevuto un ampio consenso. Dopo che la proposta è stata presentata correttamente, viene aperta alla votazione fino al raggiungimento di una soglia di

potere decisionale o di una scadenza temporale. Infine, il risultato del voto viene automaticamente determinato in base ai criteri di superamento stabiliti nello smart contract.

All'interno di questo procedimento, è possibile incorporare varie condizioni. Queste sono denominate da Fan et al. [17] “condizioni di approvazione”: affinché una proposta venga approvata, deve soddisfare tutte le condizioni di approvazione nel corso della votazione. Per garantire il mantenimento del decentramento, è fondamentale che una percentuale significativa dei membri partecipi al voto. Una decisione non può essere considerata decentralizzata se vi è una partecipazione limitata nel sistema di voto.

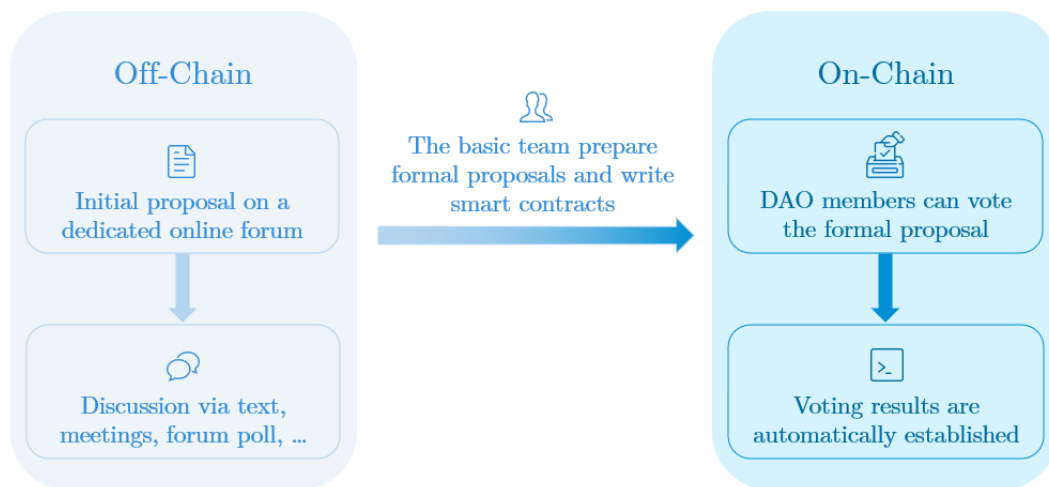


Figura 2.5: Procedura di voto all'interno di una DAO

Si ricorda che questo percorso all'interno della DAO è completamente trasparente, quindi i membri dell'organizzazione e altri utenti esterni possono accedere alle informazioni rilevanti, inclusi dettagli sulle votazioni, attraverso siti web della piattaforma o chain data explorer.

Esempi di DAO che integrano il sistema di voto completamente on-chain includono Aragon, DAOstack e Compound. In questa configurazione, a differenza dell'approccio precedentemente descritto, le proposte vengono presentate tramite una transazione sulla blockchain che contiene tutti i dettagli necessari. Successivamente, il processo di votazione procede come illustrato in precedenza.

Idealmente, la governance di una DAO dovrebbe essere completamente eseguita on-chain per garantire l'autenticità e la trasparenza del processo decisionale. Da

una parte, questa modalità di gestione basata interamente sulla blockchain offre diversi vantaggi, tra cui la trasparenza e l'immutabilità delle transazioni, nonché l'esecuzione automatica della proposta e una maggiore resistenza alla censura. Tuttavia, è importante notare che, sebbene questo sistema possa risultare più decentralizzato, potrebbe non essere facile gestire la discussione delle proposte della rete all'interno della blockchain [34].

Effettivamente, l'adozione di un sistema di voto completamente on-chain presenta svantaggi che derivano dalla necessità di interagire direttamente con la blockchain, determinando complessità tecnica, rallentamenti nelle comunicazioni e costi elevati associati alle transazioni [34].

Di conseguenza, molte DAO integrano una combinazione di sistemi sia on-chain che off-chain, come quello illustrato in precedenza. Si forniscono strumenti e canali per la condivisione e lo scambio di idee tra i membri della DAO, consentendo loro di elaborare proposte in modo collaborativo prima di procedere con il voto on-chain. Questo approccio ibrido aiuta a garantire un processo decisionale più maturo e informato, permettendo alle idee di essere discusse e raffinate prima di essere sottoposte alla votazione ufficiale sulla blockchain [19].

2.7.4 Confronto con la struttura tradizionale

Nella sezione 2.7.1 abbiamo sottolineato che, durante la realizzazione della DAO, non basta emulare i meccanismi di voto implementati nelle organizzazioni tradizionali. Infatti, bisogna tener conto della caratteristica più importante di queste nuove organizzazioni, ovvero la decentralizzazione. In caso contrario, come accennato, si potrebbe incorrere in alcuni problemi che minerebbero la sicurezza della DAO.

Nella tabella 2.2 sono descritte le principali differenze tra il voto all'interno di una DAO e la struttura di votazione tradizionale [17].

Da queste differenze, si sottolinea ancora di più lo scopo delle organizzazioni autonome decentralizzate, che mirano infatti ad una decisione collettiva aperta a tutti i membri e in cui il potere e la partecipazione al voto non sono limitate. Si evidenzia la forte indipendenza di ciascun nodo e la resilienza del processo di voto anche in assenza del contributo di singoli partecipanti.

Tuttavia, questa struttura offre soltanto un fondamento decentralizzato per il voto all'interno di una DAO. Allo stesso tempo, è importante considerare che l'assegnazione del potere di voto e le modalità operative del processo decisionale potrebbero costituire delle potenziali minacce alla decentralizzazione, introducendo rischi di centralizzazione all'interno del sistema [17].

DAO		Organizzazione tradizionale	
Democratizzata	Il sistema di una DAO mira ad una parità delle posizioni di voto tra i membri, garantendo così una struttura meno gerarchica	Gerarchica	Il sistema tradizionale impone delle posizioni gerarchiche, a partire dall'autorità centrale
Diritto di proposta democratico	Le proposte all'interno di una DAO possono essere avviate da qualsiasi nodo su qualunque argomento	Diritto di proposta elitario	Le proposte, solitamente, riguardano aspetti specifici e non tutti i membri hanno il diritto di presentarle
Diritto di voto democratico	Tutti i membri di una DAO hanno lo stesso diritto di voto	Possibilità di voto non aperto	Può accadere che il voto non sia aperto a tutti i membri
Potere di voto democratico	Il potere di voto è basato sui token e solitamente sono distribuiti in modo democratico	Potere di voto centralizzato	Il potere di voto è notevolmente influenzato dallo status dei membri
Processo di voto automatizzato	Basandosi su smart contract, il processo è completamente automatizzato	Processo di voto manuale	Solitamente, il processo prevede una gestione manuale
Procedure trasparenti	Grazie alle tecnologie alla base delle DAO, le procedure di voto sono interamente trasparenti e visibili a tutti	Procedure limitate al pubblico	Nelle strutture tradizionali, le procedure di voto sono limitate al pubblico

Tabella 2.2: Confronto tra voto all'interno di una DAO e tradizionale

Si vuole citare anche lo studio di Feichtinger et al. [7] sui costi legati alla governance on-chain. In questa ricerca, gli autori hanno analizzato due tipologie di costi: le spese delle transazioni di governance e le spese generali di trasferimento. Tuttavia, non ci sono dati sufficienti per un confronto efficace.

2.8 Key Performance Indicator

Dopo aver delineato i dettagli di una generica DAO, in questa sezione descriviamo i Key Performance Indicator (KPI) che prenderemo in considerazione nell'analisi delle organizzazioni. Data la struttura delle DAO, sappiamo che l'organizzazione aggiunge la sfera della governance e delle votazioni. Per questo motivo, una metrica

sarà sulla comunità e sulla partecipazione dei membri alle attività dell'organizzazione, un'altra sugli asset a disposizione e una terza sarà sul meccanismo di votazione adottato. Un ultimo indice riguarderà un aspetto cruciale delle DAO e della blockchain, ovvero la decentralizzazione.

Nel dettaglio, i KPI che valuteremo sono:

1. **Partecipazione della rete** [35]: È cruciale valutare attentamente l'attività e l'impegno della comunità all'interno della DAO, tenendo conto di diversi aspetti. Si considerano il numero di membri attivi e la frequenza con cui partecipano alle votazioni e alle discussioni.
2. **Fondi accumulati** [35]: Le DAO si distinguono per la caratteristica di permettere la gestione collettiva dei fondi tramite un sistema di contabilità aperta e trasparente. Questo indice, quindi, misura la quantità di attività economica all'interno della DAO. Questo può includere il totale degli asset a disposizione della DAO (tesoreria, di cui abbiamo parlato nella sezione 2.3.4), oltre che il numero di token detenuti dai partecipanti (token circolanti). Tutto ciò può essere utile per valutare l'adesione e l'interesse della community.
3. **Efficienza del meccanismo di voto**: Considera il tasso di approvazione delle proposte e la durata delle votazioni. Fan et al. [17] mettono in evidenza l'importanza di considerare la variabilità nella qualità delle proposte presentate nelle attuali DAO, rendendo irrealistico affidarsi esclusivamente ad un alto tasso di approvazione come indicatore di efficienza. Allo stesso tempo, un basso tasso di approvazione delle proposte può compromettere l'efficienza decisionale dell'organizzazione. Inoltre, una durata inadeguata delle votazioni può influenzare negativamente il tasso di approvazione delle proposte.
4. **Decentralizzazione**: Misura quanto la governance e le decisioni all'interno della DAO siano effettivamente decentralizzate. Secondo la ricerca condotta da Park et al. [36] "le DAO hanno tre dimensioni per misurare il decentramento: 'decentramento politico come impegno partecipativo', 'decentramento economico come distribuzione delle risorse' e 'decentramento amministrativo come esecuzione autonoma delle decisioni'". Per il parametro di 'impegno partecipativo', si terrà conto del primo KPI nominato.

Per valutare questi indici, abbiamo utilizzato i servizi web DeepDAO [25], Etherscan [38], DAO-analyzer [37], CoinMarketCap [39] e IntoTheBlock [40] (maggio 2024).

Per proseguire con l'analisi, bisogna definire dei livelli per questi KPI:

1. **Partecipazione della rete**: Abbiamo diviso in tre livelli (basso, medio e alto) in base alla percentuale dei membri attivi, rifacendoci ai dati di DeepDAO

[25] e DAO-analyzer [37] (maggio 2024). Il 10% e il 40% sono stati scelti come soglie perché le percentuali di partecipazione al voto nelle DAO sono molto basse e selezionare percentuali più alte avrebbe fatto abbassare notevolmente i livelli di questo indice. Pertanto, si è ritenuto che una DAO con il 41% dei membri attivi abbia un'alta partecipazione della rete.

2. **Fondi accumulati:** Da subito è stata presa in considerazione la tesoreria, per poi suddividere un livello medio in “medio-basso” e “medio-alto” sulla base della percentuale dei token circolanti. Per i livelli basso e alto, la selezione avviene esclusivamente in base alla tesoreria poiché questo criterio distingue chiaramente le fasce più estreme. Per le fasce intermedie, invece, consideriamo il 50% come soglia di separazione essendo il numero di token circolanti una metrica che ha un impatto significativo sui fondi di una DAO. I dati sono stati presi da DeepDAO [25], DAO-analyzer [37] e CoinMarketCap [39] (maggio 2024).
3. **Efficienza del meccanismo di voto:** Nonostante ciò che è stato citato sopra di Fan et al. [17], abbiamo notato che i periodi di votazione delle DAO sono molto simili tra loro (in media, variano tra i 5 e i 7 giorni). Per questo motivo, si è pensato di basarsi soprattutto sul tasso di approvazione delle proposte per dividere i tre livelli proposti (basso, medio e alto), nonostante la durata delle votazioni sia un criterio importante da considerare nella creazione di nuove DAO. Il 30% e il 70% sono stati selezionati come limiti poiché meno di un terzo delle proposte approvate significa che la struttura di voto non è abbastanza efficiente; mentre, se più di due terzi di ciò che si propone viene accettato, il meccanismo di voto ha un'efficienza elevata. Le fonti sono DeepDAO [25] e DAO-analyzer [37] (maggio 2024).
4. **Decentralizzazione:** Questa suddivisione in livelli è la più complessa. Il primo criterio di divisione è la percentuale di risorse possedute da un singolo token holder, ottenendo una partizione iniziale. Per suddividere ulteriormente il livello medio, sono stati presi in considerazione il livello dell'impegno partecipativo (ovvero, la partecipazione della rete nominata al punto 1) e se l'esecuzione delle decisioni fosse completamente automatizzata. Per quest'ultimo punto in particolare, si intende se il processo di voto sia interamente on-chain o meno. Le percentuali scelte per la suddivisione delle risorse sono 10%, 33%, 66%. In particolare, se un singolo utente possiede più di due terzi dei token totali, la rete è subito considerata poco decentralizzata, senza guardare gli altri parametri; se i token posseduti sono tra un terzo e due terzi, siamo ad un livello di decentralizzazione medio-bassa; il livello di decentralizzazione è considerato alto se le risorse possedute da un singolo membro sono meno di un decimo. Tra un decimo e un terzo, si distingue in base al livello di

partecipazione e automazione. I dati principali sono stati raccolti su Etherscan [38] e IntoTheBlock [40] (maggio 2024).

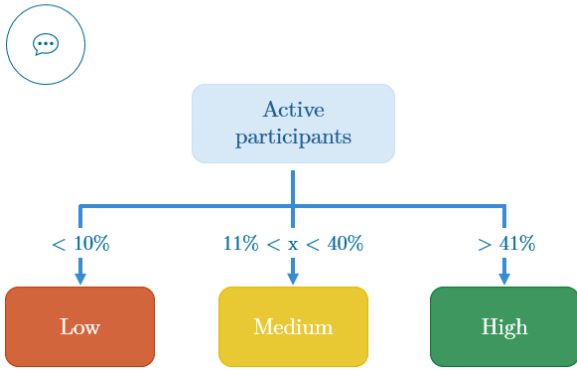
In tabella 2.3 sono riassunte le metriche e le rispettive suddivisioni in livelli. Oltre ad una breve descrizione, vi è un punteggio necessario per determinare gli output finali di questi KPI. Per far ciò, si è pensato di assegnare dei punteggi da 0 a 3 per ogni metrica, per un totale di 12 punti per la DAO ideale.

Il sistema di punteggio è stato progettato senza attribuire pesi differenti ai vari KPI, in quanto tutti e quattro sono considerati ugualmente importanti per valutare le DAO. Infatti, la rete e il meccanismo di voto rappresentano i pilastri di queste organizzazioni, la decentralizzazione è una delle caratteristiche distintive delle DAO, e la gestione trasparente dei fondi è altrettanto fondamentale. Per questi motivi, tutti i KPI sono stati valutati con punteggi da 0 a 3, senza differenziazione di peso.

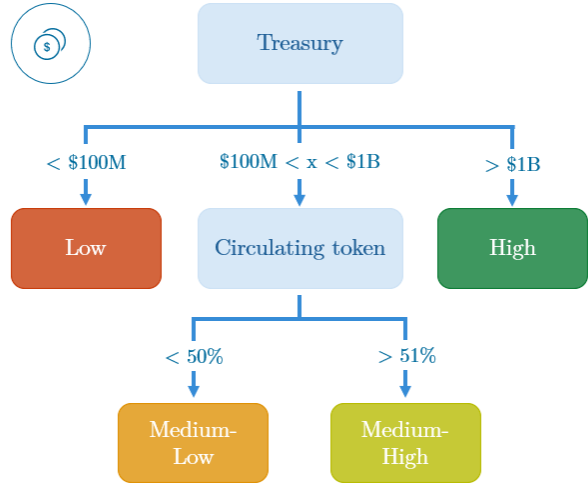
KPI	Livello	Descrizione	Punteggio
Partecipazione della rete	Basso	Se la percentuale dei membri attivi è minore del 10%	1
	Medio	Se la percentuale dei membri attivi è tra l'11% e il 40%	2
	Alto	Se la percentuale dei membri attivi è maggiore del 41%	3
Fondi accumulati	Basso	Se la tesoreria è minore di 100 milioni di dollari	0.75
	Medio-Basso	Se la tesoreria è tra i 100 milioni e 1 miliardo di dollari, e la percentuale di token circolanti è inferiore al 50%	1.5
	Medio-Alto	Se la tesoreria è tra i 100 milioni e 1 miliardo di dollari, e la percentuale di token circolanti è superiore al 51%	2.25
	Alto	Se la tesoreria è maggiore di 1 miliardo di dollari	3
Efficienza del meccanismo di voto	Basso	Se il tasso di approvazione delle proposte è minore del 30% e/o la durata delle votazioni è meno di 2 giorni	1
	Medio	Se il tasso di approvazione delle proposte è tra il 31% e il 70%, e la durata delle votazione tra i 3 e i 14 giorni	2
	Alto	Se il tasso di approvazione delle proposte è maggiore del 71%, e la durata delle votazione tra i 3 e i 14 giorni	3
Decentralizzazione	Basso	Se le risorse appartengono al 67% o più ad un singolo token holder	0.6
	Medio-Basso	Se un singolo token holder possiede tra il 34% e il 66% delle risorse, oppure se questa percentuale si trova tra l'11 e il 33% e l'impegno partecipativo è basso	1.2
	Medio	Se un singolo token holder possiede tra l'11% e il 33% delle risorse, l'impegno partecipativo è medio e l'esecuzione delle decisioni non è completamente automatizzata	1-8
	Medio-Alto	Se un singolo token holder possiede tra l'11% e il 33% delle risorse, l'impegno partecipativo è medio o alto e l'esecuzione delle decisioni è completamente automatizzata	2.4
	Alto	Se il token holder con la maggior percentuale di risorse ha meno del 10% dei token totali	3

Tabella 2.3: KPI e suddivisione in livelli

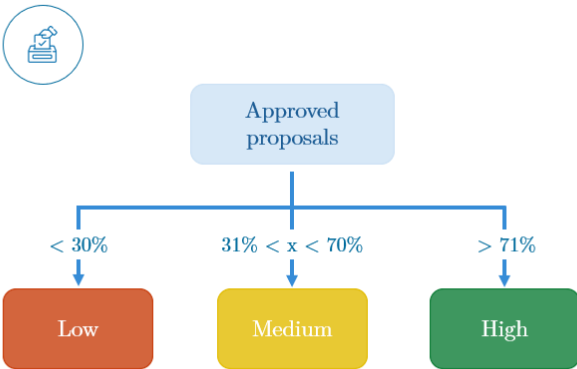
Rendiamo questa distinzione più chiara attraverso alcuni diagrammi ad albero:



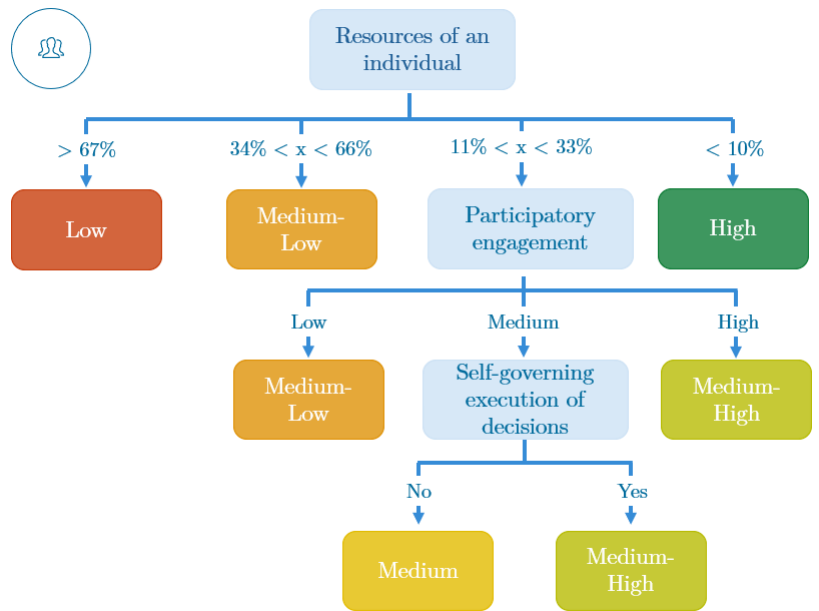
(a) Partecipazione della rete



(b) Fondi accumulati



(c) Efficienza del meccanismo di voto



(d) Decentralizzazione

Figura 2.6: Suddivisione in livelli dei KPI

Per quanto riguarda l'efficienza del meccanismo di voto, si propone di seguito una variante della suddivisione dei livelli precedentemente illustrata. In questa versione, oltre al rate di approvazione delle proposte, è stata presa in considerazione la decentralizzazione (l'ultimo indice nominato). I motivi di questa scelta sono dovuti al fatto che, se la rete è in mano a pochi e si ha un tasso di approvazione alto, non significa necessariamente che il meccanismo di voto utilizzato sia efficiente.

Per suddividere quindi i livelli di questa metrica è stato considerato il 50% come soglia di percentuale di approvazione: se le proposte approvate sono meno della metà di quelle totali, l'efficienza del meccanismo di voto è stato classificato direttamente come basso; mentre se supera la metà si tiene in considerazione anche la decentralizzazione. Si riporta la tabella e il diagramma ad albero (tabella 2.4, figura 2.7).

KPI	Livello	Descrizione	Punteggio
Efficienza del meccanismo di voto (variante)	Basso	Se il tasso di approvazione delle proposte è minore del 50% o supera il 50% ma la decentralizzazione è bassa	1
	Medio	Se il tasso di approvazione delle proposte è maggiore del 51% e la decentralizzazione è media o medio-bassa	2
	Alto	Se il tasso di approvazione delle proposte è maggiore del 51% e la decentralizzazione è alta o medio-alta	3

Tabella 2.4: Variante KPI Efficienza del meccanismo di voto

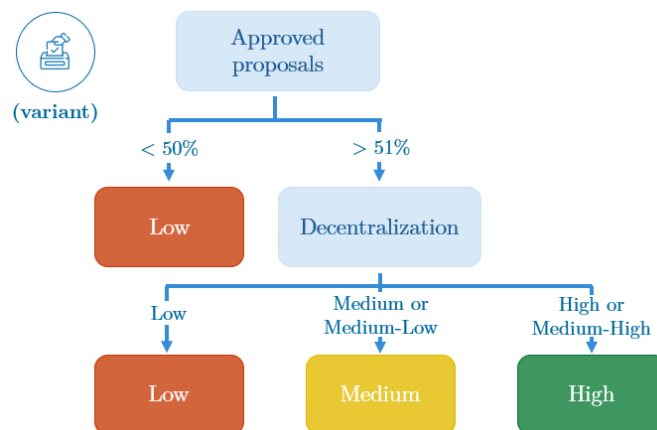


Figura 2.7: Variante KPI Efficienza del meccanismo di voto

Nonostante questa variante dia una rappresentazione più completa della metrica, è chiaro che sia meno stabile rispetto all'originale. Ciò è dovuto alla dipendenza da un'altra KPI, ma sono state presentate entrambe per far notare come l'indice cambi considerando anche la decentralizzazione.

I KPI definiti con questa modalità saranno utilizzati nella sezione 2.9 per attribuire i livelli in modo più chiaro, consentendo così un confronto più efficace tra diverse DAO, anche attraverso i punteggi finali.

2.9 DAO popolari

Dati i diversi meccanismi e modelli che possono essere scelti per l'implementazione di una DAO, si sono sviluppate varie piattaforme e di seguito ne trattiamo qualcuna tra le più rilevanti.

2.9.1 MakerDAO

Come primo esempio significativo portiamo MakerDAO, un'organizzazione autonoma decentralizzata formata sulla piattaforma Maker. L'analisi seguente, che riporta le parti più rilevanti per il nostro contesto, è basata sullo studio di Zhao et al. [19].

Maker è una delle piattaforme pionieristiche basate sulla blockchain di Ethereum. La piattaforma è nota per la creazione della stablecoin DAI, ancorata al dollaro. Gli utenti possono acquistare e vendere DAI sui mercati di trading, ma possono generare nuovi DAI solo attraverso un processo specifico offerto da Maker.

Quest'applicazione decentralizzata consente agli utenti di proteggere i loro cripto-asset in un caveau on-chain, scegliere i parametri del prestito e ricevere DAI sui loro account blockchain. Ciò permette agli utenti di ottenere liquidità dai loro asset crittografici, che possono poi convertire in dollari fiat attraverso i mercati di scambio di token. Quando gli utenti vogliono sbloccare i loro asset, possono rimborsare il prestito in DAI e le relative commissioni.

La piattaforma Maker è gestita da MakerDAO che emette il token di governance MKR. I detentori di MKR partecipano alla governance votando su questioni chiave come l'aggiunta o la rimozione di garanzie, o ancora la modifica di commissioni.

Per partecipare alle votazioni, i detentori di MKR devono congelare una quantità specifica di token negli smart contract di voto, aumentando così il peso del loro

voto. Tuttavia, la complessità delle attività di voto e i costi associati possono limitare la partecipazione. Meno del 15% dei possessori di MKR ha partecipato alle votazioni di Aprile 2024 [32], mentre molti detentori di MKR usano il token principalmente per investimento senza partecipare attivamente alle questioni di governance.

È importante notare che per essere considerati membri di MakerDAO e partecipare alle votazioni, i detentori di MKR devono possedere e trasferire MKR sul proprio address Ethereum, dimostrando così l'appartenenza e la possibilità di voto. Infatti, se un utente compra e mantiene i propri MKR in un account di mercato centralizzato, non è considerato membro di MakerDAO.

In sintesi, Maker è una piattaforma leader nel settore delle dApp che offre prodotti finanziari basati su blockchain, inclusa la stablecoin DAI. La governance è gestita attraverso MakerDAO e il token di governance MKR, i cui detentori partecipano alle decisioni riguardanti la piattaforma tramite votazioni on-chain.

Dopo aver descritto nel dettaglio questa particolare DAO, possiamo passare all'analisi dei KPI esposta nella tabella 2.5:

KPI	Livello	Descrizione	Punteggio
Partecipazione della rete	Medio	Circa il 15% dei possessori di MKR ha partecipato alle votazioni [32]	2
Fondi accumulati	Alto	La tesoreria di MakerDAO è \$ 2B e i token circolanti sono il 92.03% delle risorse totali [39]	3
Efficienza del meccanismo di voto	-	Non è stato possibile trovare dati sul tasso di approvazione delle proposte di MakerDAO	0
Decentralizzazione	Medio	Il token holder che possiede più risorse ha il 15% dei token totali [40], ma il processo di voto non avviene completamente on-chain	1.8
			6.8 / 12

Tabella 2.5: Analisi KPI MakerDAO



In questo caso è superfluo mettere a confronto le due versioni dell'efficienza del meccanismo di voto dato che non ci sono dati a riguardo.

2.9.2 Aragon e la sua architettura

Nella sezione 2.5 abbiamo delineato l'architettura di una generica DAO e ora ne vediamo un esempio pratico: Aragon.

Aragon è una piattaforma che consente agli utenti di creare e gestire diverse tipologie di DAO, ed è definito su un sistema di smart contract che si chiama aragonOS. Secondo il modello proposto da Wang et al. [4], vediamo gli elementi principali di Aragon.

Livello tecnologico di base: Le DAO di Aragon si sviluppano sulla blockchain Ethereum.

Livello esecutivo: Su Aragon è implementato Aragon Governance Proposal (AGP), che fornisce una proposta dettagliata di modifica riguardante la gestione, l'allocazione o l'utilizzo delle risorse condivise che sono di proprietà della rete Aragon o direttamente influenzate da essa. Tali risorse richiedono processi decisionali per concedere o negare l'accesso e le proposte di modifica. Per definire i criteri complessi che regolano le azioni eseguite all'interno dell'organizzazione, c'è la necessità di concatenare una serie di smart contract. Inoltre, Aragon dispone di un protocollo giudiziario per la risoluzione di controversie, che prevede l'attivazione di un processo e il coinvolgimento di una giuria di membri.

Livello di coordinamento: Il token utilizzato sulla rete Aragon è l'Aragon Network Token (ANT). I membri della DAO possono proporre modifiche ai regolamenti dell'organizzazione, e i detentori di token votano in proporzione alla quantità di token che possiedono. Coloro che hanno presentato una proposta devono depositare un certo numero di ANT come garanzia prima che la loro proposta possa essere sottoposta a votazione. Come meccanismo di voto, Aragon ne può sfruttare diversi, i principali sono l'MRA, il voto ponderato e quello conviction.

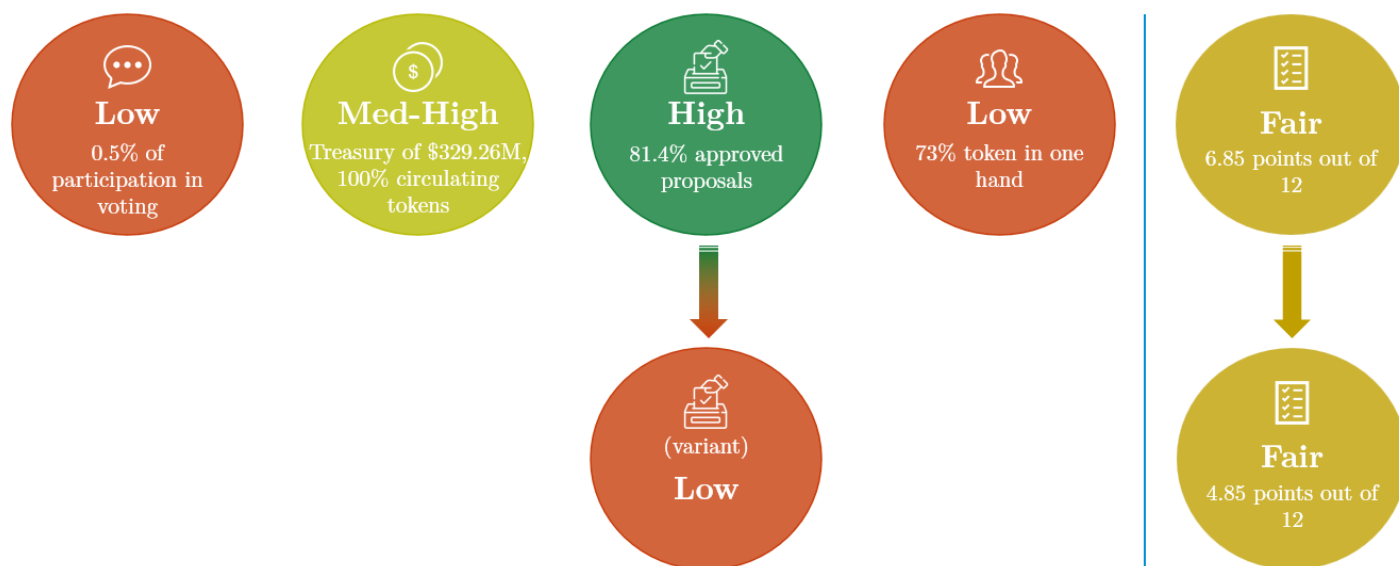
Livello organizzativo: L'obiettivo finale è quello di facilitare la creazione e la gestione di organizzazioni decentralizzate e rendere Aragon un'organizzazione autonoma, amministrata dai suoi membri per promuovere la decentralizzazione della comunità.

Livello applicativo: Lo scenario di applicazione è proprio il sistema di creazione e sviluppo di DAO pubbliche.

Per finire, esaminiamo le metriche per Aragon:

KPI	Livello	Livello con variante	Descrizione	Punteggio	Punteggio con variante
Partecipazione della rete	Basso		La percentuale di partecipazione al voto è molto bassa e arriva allo 0.5% [25]	1	
Fondi accumulati	Medio-Alto		La tesoreria di Aragon è \$ 329.26M e i token sono tutti in circolazione [39]	2.25	
Efficienza del meccanismo di voto	Alto	Basso	Si registra l'81.4% di successo delle proposte [25]	3	1
Decentralizzazione	Basso		Il 73% dei token totali sono posseduti da un singolo membro della rete [38]	0.6	
				6.85 / 12	4.85 / 12

Tabella 2.6: Analisi KPI Aragon



Notiamo come l'efficienza del meccanismo di voto sia scesa di due livelli (e quindi di due punti) considerando la variante con la decentralizzazione. Questo è certamente dovuto alla grande concentrazione di token posseduti da un singolo membro.

2.9.3 DAOstack e Holographic Consensus

DAOstack è un altro esempio di organizzazione autonoma decentralizzata, che offre la possibilità di creare applicazioni decentralizzate, DAO e strumenti DAO. Questa piattaforma, analizzata nel dettaglio da Dimitri [16], fornisce una procedura innovativa: Holographic Consensus (HC).

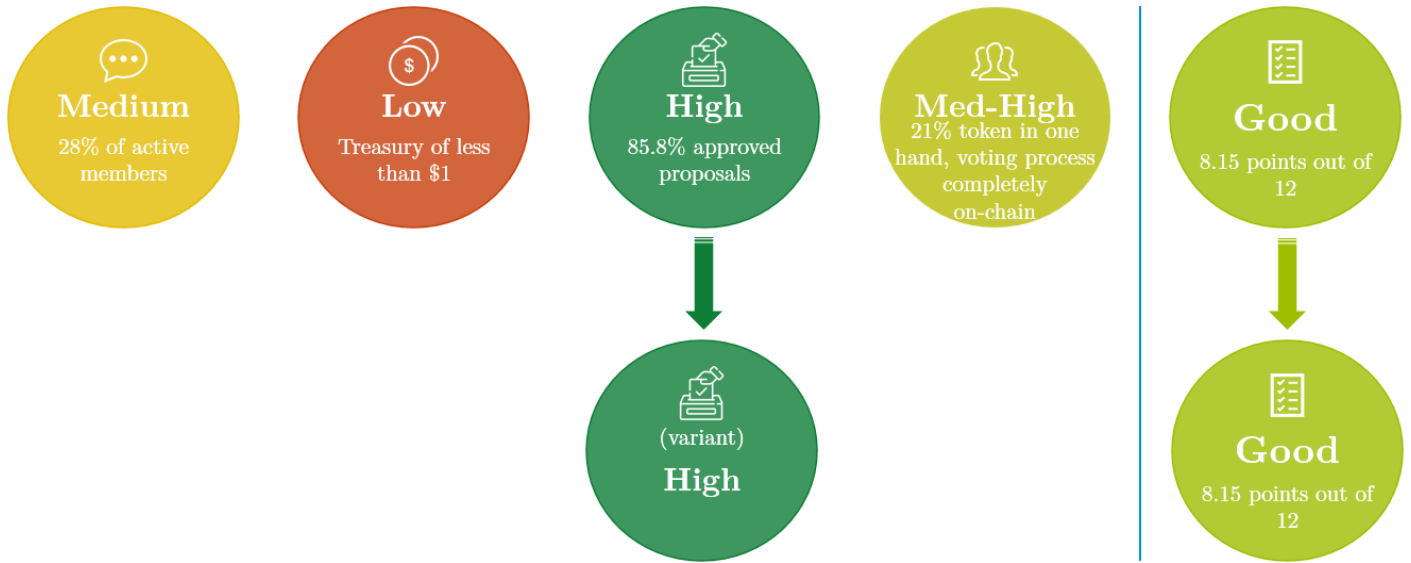
Abbiamo già esaminato il suo funzionamento nei meccanismi di voto (sezione 2.6.2), ma riprendiamone i concetti innovativi. HC è un metodo di consenso basato sul boosting, cioè votare su determinate questioni con una maggioranza relativa anziché con la tradizionale maggioranza assoluta del 51%, mediante scommesse degli stakeholder. L'azione di scommessa (stake) riflette la convinzione degli stakeholder sull'esito del voto: se l'esito è favorevole, gli stakeholder ricevono una ricompensa; al contrario, se l'esito è sfavorevole, possono perdere parte o tutto il loro stake. Questo modello si ispira ai mercati di previsione, dove le persone scommettono sull'esito di eventi, ricevendo una ricompensa se la loro previsione è corretta.

Il termine “olografico” in HC suggerisce che il risultato ottenuto con una maggioranza relativa dovrebbe essere rappresentativo di quello che verrebbe ottenuto con una maggioranza assoluta. Questo aiuta a risolvere problemi di scalabilità e di tempo di partecipazione, mantenendo comunque un'accurata rappresentazione delle opinioni complessive della DAO.

Passiamo ora all'analisi dei KPI:

KPI	Livello	Livello con variante	Descrizione	Punteggio	Punteggio con variante
Partecipazione della rete	Medio		Si registra il 28% di membri attivi [37]	2	
Fondi accumulati	Basso		La tesoreria ammonta a meno di \$ 1 [40]	0.75	
Efficienza del meccanismo di voto	Alto	Alto	L'85.8% delle proposte è stato approvato [37]	3	3
Decentralizzazione	Medio-Alto		Il token holder che possiede più risorse, dispone del 21% dei token totali [38] e l'esecuzione delle decisioni è interamente automatizzata	2.4	
				8.15 / 12	8.15 / 12

Tabella 2.7: Analisi KPI DAOstack



Questa DAO è l'unica che non ha subito modifiche nella considerazione della variante della terza metrica, dovuto al punteggio alto della decentralizzazione.

Concludiamo facendo notare che nel 2023 DAOstack ha deciso di chiudere e di concentrarsi su un altro progetto [41], per questo motivo la tesoreria risulta essere così bassa. Abbiamo comunque deciso che fosse rilevante per questo studio dato il suo innovativo meccanismo di voto.

2.9.4 Compound, Uniswap e ENS

Abbiamo già nominato l'analisi di Fritsch et al. [9], che mette a confronto tre modelli di DAO nel capitolo 2.7.2:

Compound è un protocollo di prestito decentralizzato e utilizza la democrazia liquida come meccanismo di voto.

Uniswap è uno dei più grandi progetti decentralizzati considerando la sua capitalizzazione; inoltre, richiede la delega dei propri token perché si attivi la possibilità di votare.

ENS (Ethereum Name Service) fa parte dell'infrastruttura Ethereum, e anche questa DAO sfrutta il meccanismo della democrazia liquida per il voto.

Queste tre DAO sono state comparate rispetto alla decentralizzazione del loro potere di voto, considerando il coefficiente di Gini e di Nakamoto.

Dal punto di vista della distribuzione del potere di voto, Fritsch et al. [9] hanno esaminato, a Marzo 2022, i due coefficienti e i risultati sono stati riassunti in tabella:

Coefficiente	Compound	Uniswap	ENS
Gini per i possessori di token	0.998	0.996	0.977
Gini per i delegati	0.987	0.995	0.908
Nakamoto per i delegati	8	11	18

Tabella 2.8: Coefficienti di Gini e di Nakamoto per Compound, Uniswap e ENS

Da questi dati, possiamo notare come la distribuzione per ENS risulti meno disomogenea rispetto alle altre due, essendo il coefficiente di Gini più basso. Tuttavia, questo coefficiente è molto alto in tutti e tre i casi, mostrando una forte centralizzazione del potere di voto. Spostandoci ora sul coefficiente di Nakamoto, nel caso di Compound il numero di delegati che possono prendere il controllo se collaborano è solo 8. Questo fattore cresce nel caso delle altre due DAO.

I risultati citati evidenziano ancora una volta quanto il potere di voto sia nelle mani di pochi individui, anche se esercitato raramente.

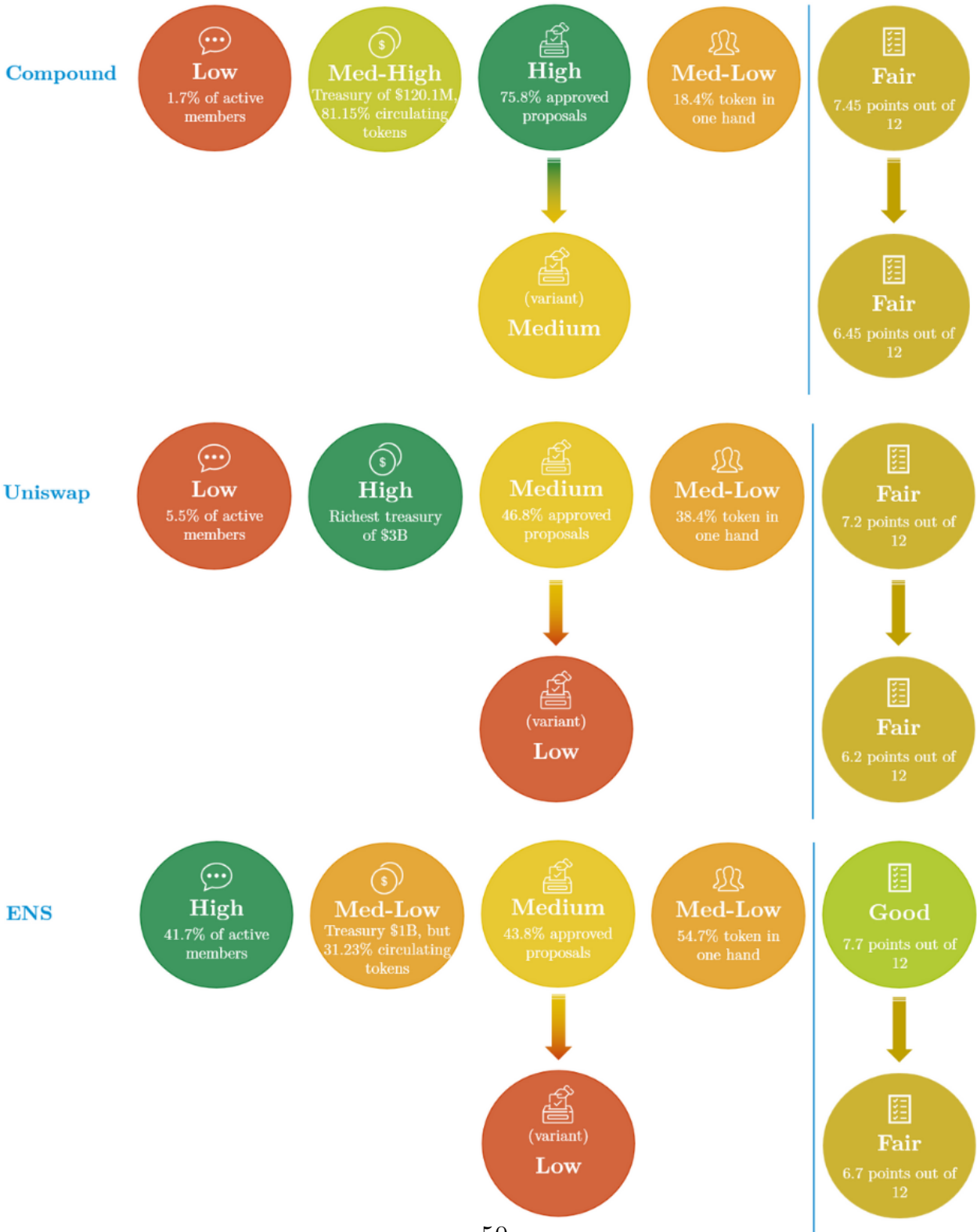
Queste considerazioni le possiamo rivedere anche nell'analisi dei KPI, nella tabella 2.9 riportata nella pagina successiva.

KPI	Livello Compound	Livello con variante	Descrizione	Punteggio	Punteggio con variante
Partecipazione della rete	Basso		Si riporta l'1.7% di membri attivi [25]	1	
Fondi accumulati	Medio-Alto		Compound possiede la tesoreria più bassa tra le tre, arrivando a \$ 120.1M secondo la stessa fonte citata sopra, e i token circolanti sono l'81.15% del totale [39]	2.25	
Efficienza del meccanismo di voto	Alto	Medio	Il 75.8% delle proposte è stato approvato [25]	3	2
Decentralizzazione	Medio-Basso		Il token holder più grande possiede il 18.4% delle risorse totali [25]	1.2	
				7.45 / 12	6.45 / 12

KPI	Livello Uniswap	Livello con variante	Descrizione	Punteggio	Punteggio con variante
Partecipazione della rete	Basso		Il 5.5% dei membri sono attivi [25]	1	
Fondi accumulati	Alto		Uniswap è tra le DAO con la tesoreria più ricca, che ammonta a \$ 3B [25]	3	
Efficienza del meccanismo di voto	Medio	Basso	Si registra il 46.8% come tasso di approvazione [25]	2	1
Decentralizzazione	Medio-Basso		Il token holder che possiede più risorse ha il 38.4% dei token totali [25]	1.2	
				7.2 / 12	6.2 / 12

KPI	Livello ENS	Livello con variante	Descrizione	Punteggio	Punteggio con variante
Partecipazione della rete	Alto		L'attività dei membri è alta, arrivando a 41.7% [25]	3	
Fondi accumulati	Medio-Basso		I fondi di ENS ammontano a circa \$ 1B [25], ma che i token circolanti sono il 31.23% del totale [39]	1.5	
Efficienza del meccanismo di voto	Medio	Basso	Similmente ad Uniswap, il tasso di approvazione è del 43.8% [25]	2	1
Decentralizzazione	Medio-Basso		Questa DAO è la meno decentralizzata delle tre, con il 54.7% dei token posseduti da un singolo [25]	1.2	
				7.7 / 12	6.7 / 12

Tabella 2.9: Analisi KPI Compound, Uniswap e ENS



Notiamo che il livello di decentralizzazione in tutti e tre i casi è medio-basso. Analizzando i coefficienti di Gini e di Nakamoto, eravamo arrivati alla conclusione che ENS, avendo un coefficiente di Gini più basso, avesse la miglior distribuzione del potere di voto, il che potenzialmente aumenta la decentralizzazione dell'organizzazione. Inoltre, ENS possedeva il più alto coefficiente di Nakamoto tra le tre, risultando quindi la più decentralizzata. Bisogna però notare che l'analisi di questi coefficienti e lo studio dei KPI sono avvenuti a due anni di distanza, quindi c'è una piccola discordanza riguardante la decentralizzazione. Rimane il fatto che l'approfondimento di Fritsch et al. [9] ribadisce che in tutti e tre i casi la centralizzazione era un fattore ancora forte.

Un'ultima osservazione riguarda la variante della suddivisione dell'efficienza del meccanismo di voto: in tutti e tre i casi ha subito un abbassamento di un livello (e quindi di un punto sul totale), dovuto alla forte centralizzazione che abbiamo appena evidenziato.

2.9.5 Commenti

Nelle scorse sezioni abbiamo analizzato diverse DAO e le abbiamo valutate attraverso i KPI precedentemente definiti. Gli output ottenuti ci indicano che nessuna di queste organizzazioni raggiunge un livello “eccellente”, definito tale se si ottiene un punteggio finale di 11 o 12 punti (vedi figura 2.8, con le dovute approssimazioni). Solo due delle sei esaminate rientrano nel livello “buono”: DAOstack con un punteggio di 8.15 ed ENS con 7.7 su un totale di 12. Le rimanenti rientrano in un livello “discreto”, avendo un punteggio inferiore a 7.5.

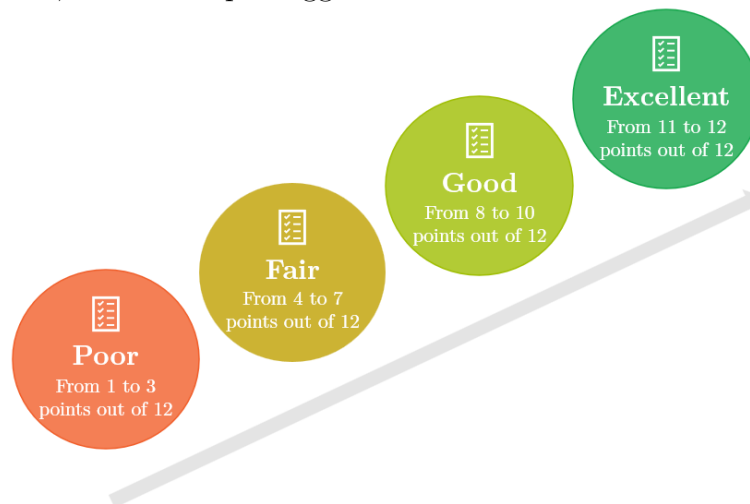


Figura 2.8: Livelli KPI per punteggio finale

Un commento è dedicato a MakerDAO, che ha ottenuto punteggi elevati ma è stata penalizzata dalla mancanza di fonti riguardanti l'efficienza del meccanismo di voto (che si vede quindi assegnati zero punti per questo KPI). A causa di ciò, ha raggiunto un totale di soli 6.8 punti su 12, classificandosi come la meno performante tra le DAO analizzate.

È utile accennare al fatto che i punteggi diminuiscano se si considera la variante del terzo KPI e, in particolare, questo porta all'abbassamento del livello di ENS che, avendo ora un punteggio di 6.7, si classifica come "discreto" e non più "buono". Segue quindi che, se consideriamo questa variante, DAOstack rimane l'unica ad un livello "buono" e Aragon toglie il titolo di meno performante a MakerDAO a causa di un abbassamento di due punti sul totale (arrivando a 4.85). Le altre DAO non subiscono cambiamenti riguardo a questo aspetto.

Un'osservazione che emerge chiaramente dalla suddivisione dei livelli dei KPI e dall'analisi dei punteggi ottenuti riguarda la bassa partecipazione della rete. Per evitare che i livelli scendessero troppo, è stato considerato alto un tasso di partecipazione del 41%. Tuttavia, in un contesto di votazioni convenzionali, ci aspetteremmo percentuali più elevate per considerare la partecipazione come alta. Nonostante questo, solo ENS ha raggiunto un alto livello di partecipazione della rete, mentre la maggior parte delle altre DAO ha una percentuale di membri attivi inferiore al 6%.

È importante sottolineare che 12/12 rappresenta un punteggio ideale, non raggiungibile dalle DAO attualmente esistenti. L'obiettivo è quello di modellare una DAO con un output ottimale, attraverso una combinazione potenzialmente ideale di fattori.

2.10 Applicazioni

Le DAO hanno dimostrato un potenziale significativo in una vasta gamma di settori, grazie alla loro capacità di eliminare intermediari e garantire processi decisionali trasparenti e sicuri. Queste organizzazioni stanno trasformando i modelli tradizionali, aprendo nuove opportunità per una gestione collettiva e automatizzata delle risorse. Vediamo alcune applicazioni nei prossimi paragrafi.

2.10.1 Swarm City

Lo use case di Swarm City è stato approfondito da Beck et al. [10], e riguarda una rete di ingegneri, fondata nel 2017, che supportano lo sviluppo di un'infrastruttura blockchain che ha come scopo il potenziamento delle applicazioni della sharing economy (o economia della condivisione). Questa struttura si basa su Ethereum e mira a trasformare le attuali piattaforme centralizzate, sostituendole con un sistema P2P che faciliti le transazioni dirette tra gli utenti. L'obiettivo è quindi quello di creare un ecosistema decentralizzato in cui i membri possano offrire e ricevere servizi senza la necessità di intermediari.

Nell'attuale panorama dell'economia della condivisione, le piattaforme centralizzate spesso traggono profitto attraverso commissioni di transazione, e sono criticate per pratiche di sfruttamento e per le loro tendenze al monopolio. Beck et al. [10] spiegano come Swarm City aspiri a creare un mercato competitivo basato su blockchain per l'economia della condivisione, dando agli utenti il controllo sui propri servizi e prezzi senza interventi di terze parti. Sebbene al momento la governance di Swarm City sia centralizzata per facilitare lo sviluppo iniziale, l'obiettivo a lungo termine è decentralizzare il controllo una volta che l'applicazione sarà consolidata.

Questo meccanismo di incentivazione per l'utilizzo di Swarm City è quindi basato su commissioni di transazione più basse e incentivi comportamentali, come la reputazione trasferibile tra piattaforme. Gli incentivi rivestono un ruolo chiave nel garantire il successo di Swarm City, assicurando il corretto funzionamento della blockchain Ethereum su cui si basa.

Il presidente dell'associazione Swarm City ha scritto: “nel 2019 abbiamo finalmente creato un'entità in Svizzera. L'Associazione Swarm City. Un'associazione è un'organizzazione gestita dai suoi membri. Ogni decisione presa si basa sul voto dei membri. Consideriamo questo un passo perfetto verso la creazione di una DAO, proteggendo già il marchio e le persone che gestiscono l'organizzazione” [33].

2.10.2 E-government

La maggior parte dei servizi di e-government attuali è centralizzata e basata su un'autorità individuale, rendendo le infrastrutture vulnerabili ad attacchi esterni e a minacce interne di utenti malevoli che potrebbero compromettere l'integrità dei dati.

Diallo et al. [22] hanno proposto l'utilizzo della tecnologia blockchain per potenziare i sistemi di e-government. In questo studio viene descritta l'architettura ad alto

livello della DAO, fornendo un sistema di e-government dettagliato.

Questo sistema ha mantenuto tutte le registrazioni di audit, riducendo le controversie tra le parti, accelerando l'assegnazione e l'applicazione dei contratti, garantendo trasparenza, responsabilità, immutabilità e una migliore gestione delle risorse.

L'implementazione di sistemi di e-government DAO, può aiutare i governi ad ottimizzare le risorse, gestire le attività governative in modo più efficace e mitigare il rischio di affidare contratti a imprese non idonee.

2.10.3 LikeStarter

Un'altra applicazione riguarda i social media, piattaforme che ormai rappresentano un mezzo cruciale per la diffusione globale delle informazioni.

Zichichi et al. [23] hanno introdotto LikeStarter, un innovativo social network in cui gli utenti possono raccogliere fondi per altri utenti attraverso un pulsante di "like". LikeStarter opera come una DAO sulla blockchain di Ethereum, facilitando il crowdfunding senza necessità di un ente centralizzato e sfrutta gli smart contract per gestire e controllare le transazioni finanziarie.

È un'importante applicazione della DAO perché sfrutta il sistema di voto per regolare il comportamento del crowdfunding e le attività del beneficiario. L'utilizzo di questa struttura porta a diversi vantaggi, tra cui la trasparenza delle azioni e dei meccanismi, l'immutabilità degli smart contract e l'equità dei membri dell'organizzazione.

2.10.4 Veicoli elettrici

Un'ultima applicazione tratta le fatturazioni per veicoli elettrici e stazioni di ricarica. Durante il processo di ricarica, è comune che i dati misurati all'interno del veicolo in carica possano differire dall'importo dichiarato dalla stazione di ricarica. Questa discrepanza può derivare dal fatto che veicoli e stazioni di ricarica utilizzano strumenti di misurazione interni per quantificare la carica elettrica. Inoltre, problemi tecnici o guasti ai dispositivi di misurazione possono compromettere l'integrità dei dati di fatturazione, portando ad errori o manipolazioni.

Per affrontare queste sfide, Jeong et al. [24] hanno proposto l'implementazione di un sistema di fatturazione basato su blockchain. Tale sistema prevede una mutua autenticazione tra veicoli e stazioni di ricarica, con entrambe le parti che registrano le informazioni di fatturazione su una blockchain. Trattandosi di una DAO, tutti i

partecipanti condividono lo stesso registro immutabile, impedendo così qualsiasi manipolazione dei dati di fatturazione.

Questo approccio introduce maggiore trasparenza, affidabilità e sicurezza nel processo di fatturazione per la ricarica dei veicoli elettrici, riducendo il rischio di frodi e controversie legate alle transazioni di ricarica.

Capitolo 3

Comunità energetiche

3.1 Introduzione alle comunità energetiche

La disponibilità di energia è fondamentale per la sicurezza e il benessere di qualsiasi società, ma la produzione energetica comporta costi. Per massimizzare la ricchezza e il benessere delle comunità, è importante promuovere il consumo locale dell'energia prodotta [18]. Attualmente, i combustibili fossili non rinnovabili come petrolio, gas naturale e carbone sono comunemente utilizzati nelle reti elettriche per generare energia, che viene poi distribuita e trasmessa tramite una rete centralizzata [12].

Per affrontare le sfide legate a questa struttura energetica centralizzata, si promuove la produzione decentralizzata di energia, in particolare da fonti di energia rinnovabili (FER), come l'energia solare ed eolica. Questa produzione avviene a livello locale e riduce le perdite di trasmissione grazie alla prossimità tra generazione e consumo. Inoltre, trasforma il mercato energetico da orientato al consumatore ad orientato al “prosumer” (produttore-consumatore). In questo contesto, si parla di evoluzione verso un mercato energetico distribuito, noto come mercato P2P [12], [13].

Le micro-reti rappresentano un'opportunità fondamentale per le FER distribuite su scala ridotta, consentendo lo scambio di energia localmente. Tuttavia, per far funzionare queste micro-reti in modo efficiente, è necessario un sistema sicuro e smart [12].

Quest'evoluzione dei mercati P2P è resa possibile anche dall'adozione di tecnologie innovative come i sistemi di gestione domestica intelligente (SHEMS). Questi sistemi permettono ai consumatori di diventare attivi nel mercato energetico, controllando la propria domanda di energia. Altri strumenti che facilitano l'automazione dei

mercati P2P sono le tecnologie di comunicazione e sensori come l'IoT, che consentono la programmazione automatica degli elettrodomestici dei consumatori [12].

È importante sottolineare ancora una volta che il protagonista centrale in questo nuovo sistema energetico è il prosumer, che non solo consuma energia ma la genera localmente. I prosumer possono scambiare l'eccesso di energia con altri partecipanti del mercato P2P, avvalendosi di risorse energetiche distribuite (DER).

In sintesi, il passaggio verso un mercato energetico P2P è un'evoluzione significativa che promuove l'efficienza energetica, l'uso delle fonti rinnovabili e l'attivismo dei consumatori, ponendo l'attenzione su uno scambio energetico locale.

3.1.1 Definizione di comunità energetica

In questa breve introduzione è stata evidenziata più volte l'importanza della produzione di energia a livello locale. Koirala et al. [42] hanno studiato nel dettaglio il concetto di sistemi energetici comunitari integrati (ICES), rappresentati come un approccio contemporaneo per la gestione dei sistemi energetici locali mirato ad integrare in modo efficiente le fonti energetiche distribuite e a coinvolgere attivamente le comunità locali.

Questo approccio intende trasformare i sistemi energetici attuali, rigidi e centralizzati, in sistemi più flessibili e decentralizzati. L'integrazione di fonti di energia distribuite a livello locale può creare un sistema energetico interconnesso, flessibile e robusto, con significativi vantaggi in termini di sicurezza energetica.

In questo scenario, si evidenzia il ruolo crescente dei consumatori che, da attori passivi, diventano prosumer attivi, ovvero consumatori e produttori di energia. Gli ICES sono progettati per soddisfare le esigenze energetiche locali, ottimizzando la sinergia tra diversi attori energetici. Lo scopo principale è quello di aumentare l'autoconsumo e bilanciare domanda e offerta a livello locale.

Le comunità locali sono particolarmente adatte ad identificare le necessità energetiche, prendere iniziative appropriate e collaborare per raggiungere obiettivi comuni come la riduzione dei costi energetici, delle emissioni di CO_2 e della dipendenza dalla rete nazionale. Attraverso questo sistema, si facilita la transizione verso un sistema energetico a basse emissioni di carbonio, rafforzando il coinvolgimento e la fiducia dei consumatori. L'autonomia energetica è cruciale per i sistemi energetici locali come gli ICES.

Un aspetto chiave sottolineato nello studio di Koirala et al. [42] sono i meccanismi di incentivazione. La gestione della domanda, infatti, può essere incoraggiata

attraverso politiche basate su incentivi. I sistemi di energia rinnovabile sono incentivati tramite contributi per i costi iniziali del capitale, oltre che attraverso la valorizzazione della produzione e dell'autoconsumo di energia rinnovabile. Tali incentivi sono fondamentali per incoraggiare i cittadini a investire nella produzione e nello stoccaggio di energia a livello locale, promuovendo la competizione e migliorando le prestazioni energetiche tra i vicini. Il coinvolgimento della comunità è quindi essenziale per avviare e sostenere gli ICES. L'identità collettiva e la ricerca di autonomia giocano un ruolo fondamentale nell'impegno della comunità verso i nuovi sistemi energetici. Nella figura 3.1, TSO e DSO rappresentano, rispettivamente, Transmission Operator System e il Distribution System Operator, incaricati di gestire e distribuire l'energia.

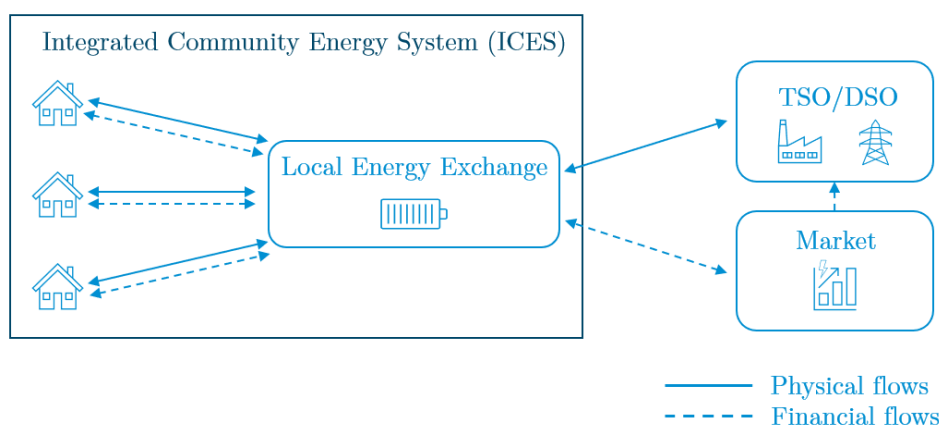


Figura 3.1: Struttura ICES

“Gli ICES sono spesso legati alla creazione di strutture decentrate e alla democratizzazione della produzione e dell’approvvigionamento di energia attraverso nuove forme organizzative” [42]. È proprio questa osservazione che ispira la creazione di una DAO energetica locale, su cui si concentra il nostro lavoro.

3.2 Blockchain nelle comunità energetiche

Nel contesto della decentralizzazione dei mercati P2P, la blockchain emerge come una tecnologia distribuita che offre nuove opportunità al settore energetico. Questa piattaforma innovativa fornisce applicazioni trasparenti e facili da usare, permettendo ai prosumer di partecipare al processo decisionale sul commercio locale di energia.

Come ribadito, stiamo assistendo ad una trasformazione nella produzione energetica: da centralizzata e basata su combustibili fossili a distribuita e dipendente dalle energie rinnovabili. Il controllo del sistema avviene a livello locale, riducendo la necessità di un controllo centrale. Grazie a questo approccio distribuito, un guasto in un singolo punto non mette in pericolo l'intero sistema. La blockchain ha il potenziale per decentralizzare l'archiviazione e la gestione dei dati, eliminando la necessità di intermediari nella società.

In particolare, questa tecnologia può essere impiegata per tracciare le transazioni energetiche sulla rete, sfruttando una robusta infrastruttura dati per permettere ai prosumer di accedere al registro distribuito. Inoltre, vengono utilizzati gli smart contract per eseguire e gestire i registri di transazione, abbinandoci una rete di misurazione avanzata.

Più nel dettaglio, Mylrea [15] spiega che: l'elettricità viene generata, il consumatore la acquista e infine i contatori smart aggiornano il registro distribuito, creando blocchi univoci con timestamp per la verifica nel registro. A livello di distribuzione, gli operatori di sistema possono utilizzare la blockchain per accedere ai dati delle transazioni energetiche e addebitare i costi netti ai consumatori.

Borges et al. [13] fanno notare che, attualmente, le funzionalità della blockchain sono in fase di sperimentazione e valutazione in applicazioni su scala ridotta, poiché la maggior parte degli esperti si concentra sugli aspetti tecnologici e sui possibili casi d'uso, piuttosto che sulla produzione di prodotti finali.

3.2.1 Vantaggi

La tecnologia blockchain offre diverse caratteristiche e aspetti che la rendono particolarmente adatta per rivoluzionare il sistema energetico di prossima generazione [12], [13], [15]:

- **Decentralizzazione:** La blockchain permette la creazione di comunità energetiche decentralizzate. Eliminando gli intermediari, si riducono i costi e si aumenta l'efficienza del commercio energetico locale, incoraggiando l'uso delle FER e riducendo le emissioni di carbonio.
- **Automazione:** Grazie alla blockchain, il sistema energetico può essere digitalizzato ed automatizzato. Contatori e sensori smart possono comunicare in tempo reale, consentendo un controllo più preciso e efficiente della rete elettrica. Questo migliora la gestione del sistema, riduce le perdite e ottimizza il consumo.

- **Interoperabilità:** La tecnologia blockchain favorisce l'interoperabilità tra i diversi attori del settore energetico. Questo facilita lo scambio di energia tra produttori e consumatori, agevolando la transizione verso un sistema più distribuito e resiliente.
- **Immutabilità:** Le transazioni sulla blockchain sono immutabili e sicure grazie alla crittografia. Ciò significa che una volta registrate, le transazioni non possono essere alterate o cancellate, aumentando la fiducia nel sistema e prevenendo frodi o manipolazioni.
- **Affidabilità:** Grazie alla crittografia e agli algoritmi di consenso alla base della blockchain, è possibile monitorare in modo affidabile e trasparente i flussi energetici e i dati associati. Ciò contribuisce a migliorare la fiducia e la sicurezza del sistema, riducendo i rischi e migliorando la resilienza complessiva della rete.
- **Gestione dei Big Data:** La blockchain permette la gestione efficiente e sicura dei big data nel settore energetico. I dati critici possono essere condivisi tra le varie parti in modo trasparente e controllato, consentendo un migliore utilizzo delle risorse e una maggiore trasparenza nel processo decisionale.

Quindi, la tecnologia blockchain offre un'infrastruttura innovativa e sicura per trasformare il settore energetico, consentendo una maggiore efficienza e favorendo la transizione verso un sistema energetico più sostenibile e resiliente.

3.2.2 Svantaggi

Tuttavia, ci sono diversi ostacoli nell'applicazione della tecnologia blockchain in questo settore di trading energetico P2P [12], [13], [15]:

- **Consumo energetico elevato:** La blockchain è fortemente criticata per il suo elevato consumo di energia.
- **Sfide legate all'immutabilità:** L'immutabilità dei dati può portare a difficoltà nel gestire contenuti indesiderati o illegali nella blockchain. Tuttavia, anche se i dati sono resistenti alla modifica, esistono scenari come le fork che richiedono interventi per modificare la blockchain.
- **Scalabilità:** La blockchain soffre di limiti di scalabilità con velocità di elaborazione delle transazioni inferiori rispetto a sistemi tradizionali. Le soluzioni come le blockchain consortium sono state proposte per migliorare le prestazioni mantenendo una decentralizzazione parziale.

- **Privacy:** Anche se gli utenti sono pseudonimi, attacchi di data mining possono mettere a rischio la privacy degli utenti.
- **Potenza di calcolo e archiviazione:** I requisiti elevati di potenza di calcolo e archiviazione rappresentano una sfida per l'implementazione della blockchain nei mercati energetici locali.
- **Mancanza di regolamentazione:** La mancanza di regolamentazione e standardizzazione rallenta l'introduzione di questa tecnologia nel settore energetico.

L'integrazione della blockchain nel settore energetico presenta sfide tecniche significative. Superare questi ostacoli è cruciale per sfruttare appieno il potenziale della blockchain nel trading energetico P2P e nelle comunità energetiche.

Concludiamo con alcune considerazioni di Mylrea [15]: Prima di implementare la blockchain per ottimizzare o proteggere l'infrastruttura, è cruciale valutare attentamente se la soluzione sia interoperabile, sicura e conveniente, con capacità di gestire le transazioni in modo efficiente. Inoltre, è essenziale determinare quale specifica piattaforma blockchain sarebbe più adatta per affrontare le diverse sfide. Alcune piattaforme potrebbero presentare sfide aggiuntive, come aumento dei costi o della vulnerabilità alla sicurezza, anziché generare miglioramenti. Le soluzioni blockchain dedicate alla gestione e protezione di grandi volumi di dati devono inoltre dimostrare efficienza energetica, economicità e compatibilità con l'infrastruttura tecnologica esistente, compresa la capacità di interoperare con altre blockchain.

3.3 DAO nella comunità energetica

3.3.1 DAEO

Le DAO costituiscono un potenziale strumento per migliorare la trasparenza della gestione dell'energia e la governance dell'organizzazione, consentendo la definizione di regole di base e l'automazione di processi decisionali efficienti e democratici [18].

La tecnologia blockchain offre l'opportunità di superare alcune delle sfide fondamentali per promuovere un maggior numero di quelle che Mylrea [15] chiama Organizzazioni Energetiche Autonome Distribuite (DAEO). Una DAEO può contribuire a risolvere diverse problematiche riguardanti il controllo e l'affidabilità di transazioni rapide, distribuite e complesse di DER.

Le DAO possono eliminare la necessità di interagire con terze parti, agevolando così l'adozione e la monetizzazione degli scambi di energia distribuita, sia in termini di flussi energetici che di transazioni finanziarie. Questo può contribuire a ridurre i costi delle transazioni energetiche e migliorare il controllo e la sicurezza dell'integrazione DER, spianando la strada verso una rete elettrica più decentralizzata e resiliente. In figura 3.2 la rappresentazione di una DAEO, come descritta da [15]:

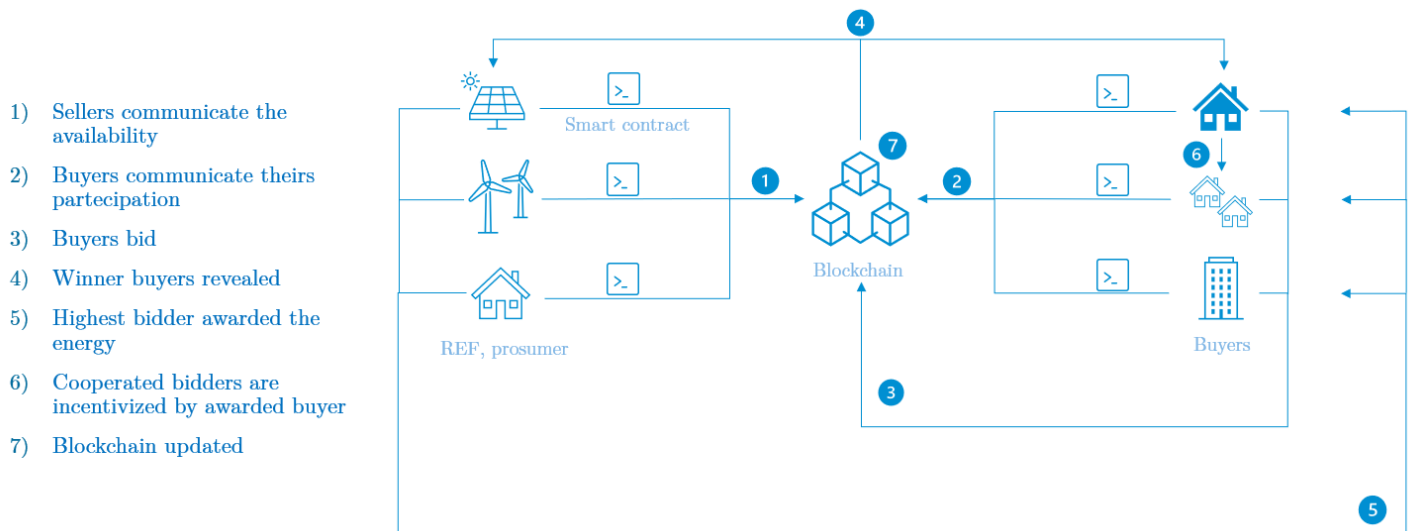


Figura 3.2: Struttura DAEO

Mylrea [15] illustra gli obiettivi che le DAEO possono contribuire a realizzare:

1. Trasformare radicalmente l'architettura del sistema di transazioni energetiche, passando dall'attuale processo di clearing house a sistemi autonomi basati su blockchain.
2. Offrire meccanismi e design di smart contract autonomi che soddisfino le esigenze dei consumatori di elettricità senza richiedere costi proibitivi per l'infrastruttura esistente.
3. Massimizzare l'utilizzo del sistema di distribuzione nazionale e delle architetture di sistema di transazioni al fine di ottimizzare l'efficienza del mercato.
4. Accelerare l'integrazione di FER, dei prosumer, della generazione distribuita e della gestione della domanda.

5. Proporre un design di mercato energetico orientato alle nuove architetture di comunicazione. Ciò consente agli smart contract di garantire la privacy dei partecipanti della comunità energetica, l'applicazione dei vincoli di capacità dell'alimentazione e la progettazione di meccanismi di mercato che massimizzino i volumi delle transazioni.

Le DAEO possono distribuire potere e leadership attraverso sistemi di voto, con l'obiettivo di diventare sempre più autonome, composte da appaltatori e investitori decentralizzati che hanno il potere di votare, investire e fornire servizi attraverso uno smart contract.

3.3.2 Confronto con il tradizionale

Dopo aver presentato queste comunità energetiche innovative e distribuite, è utile vederne le principali differenze con il tradizionale [12]. A tal proposito, si rimanda alla tabella 3.1 riportata nella pagina successiva.

Dal momento che questo mercato innovativo è basato sulle DAEO, eredita tutti i vantaggi che abbiamo analizzato per le DAO. In particolare, vanno sottolineate la fiducia e la sicurezza derivanti dall'utilizzo di smart contract e crittografia, oltre che decentralizzazione e automazione che si traducono in una maggior tolleranza ai guasti. Tutto ciò porta ad una notevole diminuzione dei costi di transazioni e, in generale, di gestione.

3.4 Sistemi proposti in letteratura

Dopo aver esplorato il concetto di comunità energetiche e di DAEO, illustriamo alcuni esempi di sistemi di mercato locale proposti in letteratura.

3.4.1 Mercato transattivo P2P

Afzal et al. [12] hanno esaminato un mercato di scambio di energia P2P implementato utilizzando la tecnologia blockchain di Ethereum, supportato anche da contatori smart.

Questo sistema consente agli individui produttori di energia rinnovabile di scambiare energia in eccesso con venditori e acquirenti all'interno della comunità energetica. L'interazione avviene in modo automatico attraverso uno smart contract eseguito

Comunità basata su DAEO		Comunità tradizionale	
Decentralizzata	Essendo basato su DAEO, sarà decentralizzata e distribuita	Centralizzata	La comunità tradizionale è più centralizzata
Interazione P2P	Il trading si basa sull'interazione peer-to-peer, fornendo un meccanismo di scambio efficiente	Interazione con terze parti	Il trading convenzionale necessita di interazioni con molte terze parti, rendendo il processo più complesso
Prosumer al centro	Dal punto precedente, i prosumer risultano essenziali in questo mercato diventando autonomi nel commercio di energia	Unidirezionale	Il commercio tra fornitore e consumatore è separato da quello tra fornitore e prosumer
Automatizzata	La comunità distribuita può essere supportata e facilitata da sensori e contatori smart, oltre che mediante la distribuzione automatica degli incentivi tramite smart contract	Non automatizzato	Nel tradizionale è più difficile gestire l'automazione e sensori IoT
Immutabile e trasparente	L'uso di smart contracts garantisce che le decisioni e le transazioni siano trasparenti e immutabili, migliorando la fiducia tra i membri della comunità	Non trasparente	Senza un registro distribuito con le transazioni visibili pubblicamente, il sistema non è trasparente e le decisioni potrebbero essere manipolate
Minor costi di transazione	La tecnologia alla base garantisce costi di transazione ridotti, in favore di un aumento dell'efficienza	Maggiori costi	I costi di gestione e di manutenzione risultano essere elevati, a causa delle varie interazioni, risultando meno efficiente da questo punto di vista

Tabella 3.1: Confronto tra comunità basata su DAEO e tradizionale

sulla blockchain Ethereum, che gestisce i dettagli delle transazioni. Di seguito sono elencati i passaggi chiave:

1. **Creazione di account e wallet:** Gli utenti creano un account utilizzando estensioni come Google Metamask e ottengono un portafoglio digitale. Questo consente loro di partecipare al trading di energia sulla rete blockchain, avviando o ricevendo transazioni.
2. **Produzione e scambio di energia:** I prosumer generano energia rinnovabile in eccesso, che viene quindi condivisa nella comunità per aumentare il loro

profitto. La blockchain facilita questo scambio in modo sicuro e trasparente tramite smart contract. I contatori smart aiutano in questo passaggio misurando con precisione la produzione e il consumo di energia.

3. **Offerte degli utenti:** Gli utenti possono fare offerte e tutte le transazioni sono memorizzate nella blockchain, accessibile a tutti e gestita tramite smart contract.
4. **Interfaccia:** Una dApp funge da interfaccia utente per consentire ai consumatori e ai fornitori di interagire con la comunità energetica.
5. **Esecuzione automatica degli smart contract:** Gli smart contract vengono eseguiti automaticamente sulla base delle condizioni specificate nel registro distribuito della blockchain. Questo facilita lo scambio automatico di energia senza la necessità di un'autorità centrale.

L'obiettivo di questo sistema è quindi quello di aumentare l'efficienza e ridurre i costi nelle comunità energetiche, consentendo ai partecipanti di trarre profitto dalla produzione e dalla condivisione di energia sostenibile.

3.4.2 Local Energy Market

Il Local Energy Market (LEM) è un sistema che permette ai prosumer di partecipare attivamente allo scambio locale di energia. La sua implementazione su blockchain è stata esaminata da Zade et al. [14] per valutare la sua efficacia e confrontarla con un sistema centralizzato. In particolare, si sono concentrati su una blockchain privata con meccanismo di consenso PoA, per ridurre significativamente i costi dell'energia.

Lo studio citato mette in risalto le principali sfide dell'implementazione di un LEM su blockchain: la sua complessità computazionale e i requisiti di sicurezza dei dati. Ma prima di riportare i risultati, vediamo la struttura:

- Prima di poter partecipare ad un LEM, un prosumer deve fornirsi di uno SHEMA e di un contatore smart per trasmettere le letture in modo affidabile.
- Ogni prosumer dispone inoltre delle etichette, ovvero varie informazioni riguardo l'origine dell'energia consumata, incoraggiando idealmente i consumatori a ridurre l'uso di combustibili fossili.
- Nella fase di registrazione di un utente, ciascun contatore per la misurazione dell'energia viene categorizzato secondo una specifica qualità energetica.

Quando i prosumer desiderano negoziare energia con il LEM, gli agenti di mercato inseriscono le richieste specificando le caratteristiche energetiche dei loro contatori.

- Dopo l'arrivo delle letture, si calcolano le energie di bilanciamento per ogni nodo, ovvero le discrepanze tra i risultati di mercato e la quantità effettivamente consumata o immessa di energia. Sulla base di queste si accreditano o addebitano i costi di ogni utente.

Le simulazioni eseguite da Zade et al. [14] mostrano che un LEM basato su blockchain riesce a calcolare risultati equivalenti ad un'implementazione centralizzata, ma richiede molto più tempo di calcolo. In particolare, “Il LEM centralizzato impiega 0.65 s per elaborare 50 offerte e 2.3 s per 550 offerte di mercato. Il LEM basato su blockchain elabora in media 50 offerte in 94 s e 550 offerte in 1343 s” [14].

Inoltre, la sicurezza dei dati è un aspetto critico. Sebbene la blockchain offra una maggiore immutabilità dei dati rispetto ad un sistema centralizzato, esistono rischi di privacy associati alla memorizzazione di informazioni non crittografate sulla blockchain. La crittografia potrebbe rallentare ulteriormente il processo e potrebbe non essere praticabile per tutte le applicazioni [14].

Un'altra considerazione importante riguarda la scalabilità. Mentre un LEM centralizzato può gestire un elevato numero di transazioni in tempi brevi (550 in meno di 3 secondi), un LEM blockchain è più limitato nella sua capacità di scalare efficacemente con l'aumento del carico di lavoro (400 offerte in circa 900 secondi).

Infine, la decentralizzazione effettiva di un LEM basato su blockchain è un argomento dibattuto perché ci sono comunque aspetti che richiedono un'organizzazione centralizzata o la fiducia in autorità centrali. Si potrebbe pensare che alcune funzionalità possano essere implementate negli smart contract, ma questo significherebbe aumentare ancora di più i tempi di calcolo.

Quindi, sebbene un LEM basato su blockchain offra vantaggi in termini di immutabilità dei dati e resistenza alla manipolazione, presenta ancora sfide significative in termini di complessità computazionale, sicurezza dei dati e scalabilità rispetto a un'implementazione centralizzata.

3.4.3 EnergyDAO

L'ultimo sistema che vediamo è stato proposto da Sharma et al. [18] e riguarda EnergyDAO.

Possiamo definire EnergyDAO come una collezione di smart contract progettati per gestire la tesoreria e le risorse energetiche rinnovabili all'interno di una comunità, offrendo una governance decentralizzata e trasparente. Questo approccio può coinvolgere sia membri locali di una comunità che investitori esterni interessati. La governance della community di EnergyDAO offre diversi vantaggi:

Meccanismi di governance comunitaria: EnergyDAO permette una governance affidabile e democratica, senza la necessità di leader centrali, consentendo decisioni collaborative e trasparenti.

Scalabilità e replicazione rapida: Le comunità energetiche basate su micro-reti possono beneficiare di scalabilità orizzontale e di capacità di replica più efficiente.

Coinvolgimento dei membri: L'esperienza e il coinvolgimento dei membri della comunità sono potenziati.

Come ricompensa per il loro coinvolgimento, i membri della comunità ricevono token in base alla quantità del loro contributo alla tesoreria di EnergyDAO. Tramite l'utilizzo di token, i membri della comunità ottengono diritti di voto e possono proporre e approvare progetti di investimento nelle infrastrutture energetiche locali. Inoltre, gli autori Sharma et al. [18] consigliano l'utilizzo del voto ponderato imponendo un limite massimo al numero di token posseduti.

Per garantire la conformità legale e mitigare i rischi, EnergyDAO considera diverse configurazioni legali, tra cui:

- **DAO completamente decentralizzate:** Operano senza entità legale registrata, richiedendo pieno decentramento e una conformità alla legge.
- **S.r.l.:** Offrono flessibilità legale e consentono di avvicinarsi all'infrastruttura di una DAO.
- **DAO come fondazione:** Adatta a scale più grandi, ma meno utile per comunità più piccole.

In conclusione, EnergyDAO rappresenta un modello innovativo per la gestione e la governance delle risorse energetiche rinnovabili, combinando tecnologia blockchain, governance decentralizzata e coinvolgimento della comunità locale e degli investitori esterni per promuovere lo sviluppo sostenibile e l'efficienza energetica.

Capitolo 4

Teoria dei giochi e modello proposto

4.1 Introduzione alla teoria dei giochi

Un'osservazione su cui abbiamo già posto attenzione riguarda il tasso di partecipazione della rete (sezione 2.9.5): in base alle analisi fatte, è stato necessario considerare alto una partecipazione del 41%, nonostante, in un contesto di votazioni tradizionale, ci si aspettano percentuali più elevate. Infatti, tre DAO su sei esaminate presentano una partecipazione della rete bassa, mentre solo una ha un tasso di partecipazione superiore al 41%. Per questo motivo, abbiamo pensato di focalizzarci sui meccanismi di incentivazione con un approccio basato sulla teoria dei giochi.

La teoria dei giochi è lo studio di problemi decisionali in cui partecipano più individui. Questo campo della matematica applicata descrive e analizza situazioni decisionali interattive, dove ogni entità razionale cerca di ottimizzare la propria strategia basandosi sulle scelte degli altri, al fine di massimizzare il proprio beneficio. Dato che si focalizza su decisioni strategiche, la teoria dei giochi può essere applicata per esaminare i comportamenti e le interazioni tra i nodi di consenso in vari contesti [43]–[46].

Nel contesto delle DAO, la partecipazione attiva alle votazioni riveste un ruolo cruciale per il corretto funzionamento e la governance della comunità. Tuttavia, incentivare i membri a partecipare in maniera costante e informata non è sempre un compito facile. In questo capitolo, ci concentreremo su un modello di incentivazione

per la partecipazione alle votazioni all'interno di una DAO, attraverso l'utilizzo della teoria dei giochi.

L'importanza dell'incentivazione, come già accennato nella sezione 2.6.1, risiede nella sua capacità di bilanciare gli interessi individuali con quelli collettivi, promuovendo una maggiore partecipazione e migliorando la qualità delle decisioni. In un ambiente decentralizzato, dove le azioni dei singoli possono influenzare significativamente l'esito delle decisioni, è essenziale creare meccanismi che allineino i comportamenti dei partecipanti agli obiettivi dell'organizzazione.

La teoria dei giochi offre una struttura rigorosa per analizzare le interazioni strategiche tra i membri di una DAO. Attraverso l'applicazione di concetti come i reward, le utility e gli equilibri di Nash, è possibile progettare sistemi di incentivi che promuovano la partecipazione attiva e scoraggino comportamenti opportunistici.

L'obiettivo di questo capitolo è quindi quello di applicare un modello della teoria dei giochi per incentivare la partecipazione alle votazioni interne alle DAO. Dopo aver presentato tale modello che, idealmente, aumenta il rate di votanti all'interno dell'organizzazione, si procede con l'adattamento di questo al contesto delle comunità energetiche.

4.2 Modello proposto

Il modello proposto combina due approcci: un sistema di reputazione e un sistema basato sui prezzi. Nel sistema di reputazione, il comportamento dei singoli membri viene valutato in base alla loro reputazione. In particolare, attraverso una soglia di reputazione, sarà possibile distinguere tra nodi contributori e non contributori. Il sistema basato sui prezzi, invece, mira a incentivare la cooperazione dei membri tramite ricompense monetarie, come i token nel nostro caso. Così facendo, i membri egoisti, con una bassa reputazione, vengono identificati e gli incentivi vengono assegnati esclusivamente ai membri che contribuiscono.

Per quanto riguarda la struttura, ci siamo basati sul lavoro presentato da Chaidos et al. [47], integrandolo con un sistema di reputazione e di penalità. Nelle sezioni che seguono vengono proposte delle versioni di questo modello arricchito.

4.2.1 Definizioni base e parametri

Prima di approfondire il modello, in questa sezione vengono introdotte le definizioni fondamentali e i parametri che saranno utili nella sua costruzione.

Il gioco di partecipazione vede come scenario la votazione interna alla DAO, a cui l'utente può partecipare o meno. Sia $N = \{1, 2, \dots, n\}$ l'insieme di tutti i partecipanti, denoteremo con "epoca" ogniqualvolta ci sia una votazione e con "progresso" l'obiettivo da raggiungere in ogni epoca. Gli aspetti principali da considerare per il nostro modello sono:

Progresso

Il progresso della DAO è correlato alla partecipazione alla votazione, nel caso si arrivi ad una soglia minima di partecipazione. Si avrà un parametro pubblico k , in modo che il progresso sia compiuto se almeno k utenti hanno contribuito al voto.

Set di partecipanti alla DAO

1. C – contributori, i membri sono eleggibili e possono partecipare alle votazioni della DAO
2. NC – non contributori, gli utenti non sono eleggibili, quindi non possono partecipare alle votazioni e i contributi versati da loro sono bloccati

Inizialmente tutti i membri saranno considerati contributori. Una volta raggiunta la soglia minima di partecipanti μ , gli utenti con una reputazione inferiore ad una soglia ρ saranno classificati come non contributori e non potranno partecipare al progresso della DAO. Se un utente è considerato non contributore, il contributo iniziale versato al momento dell'ingresso nella DAO sarà bloccato e in questo periodo l'utente non riceverà bonus o malus. L'unico modo per tornare nel set dei contributori è effettuare un "redeem", ovvero pagare un contributo aggiuntivo alla tesoreria della DAO per ottenere una reputazione tale da rientrare tra gli eleggibili.

Randomizzazione

Esiste una probabilità q per selezionare i partecipanti al voto. Dato che non è pratico chiedere a tutti gli utenti di contribuire, a causa del throughput, ad ogni epoca si seleziona solo un sottoinsieme di utenti che possono contribuire e ricevere ricompense [47]. Inizialmente, questa probabilità non viene considerata, quindi tutti hanno la possibilità di partecipare alle votazioni della DAO. Dopo che si supera una soglia minima di partecipanti μ , l'eleggibilità di ogni utente segue una Bernoulli di parametro q : ovvero, ogni utente ha una probabilità q di essere selezionato per partecipare alle votazioni della DAO. Quindi, il processo di determinare se ciascun giocatore è eleggibile in ogni epoca è modellato come una serie di prove di Bernoulli indipendenti, una per ogni giocatore, tutte con la stessa probabilità q . Questo parametro può variare in base alla soglia μ e al numero di partecipanti n . Una scelta ragionevole

è impostarlo abbastanza alto da garantire un numero sufficiente di giocatori eleggibili in ogni epoca, così da raggiungere la soglia k [47].

Introduciamo ora i parametri del modello:

- $R_i^{(t)}$ – reputazione dell’ i -esimo membro all’epoca t . Questa varia a seconda della strategia scelta dall’utente nel seguente modo:

$$R_i^{(t+1)} = \begin{cases} \min \{ R_i^{(t)} + \Delta R_{voto}, R_{max} \} & \text{se } i \text{ è selezionato e partecipa al voto} \\ R_i^{(t)} & \text{se } i \text{ non è selezionato ma era intenzionato a} \\ & \text{partecipare, oppure si astiene meno di 3 volte} \\ \max \{ R_{min}, R_i^{(t)} - \Delta R_{astenuto} \} & \text{se } i \text{ è selezionato e si astiene per più di 3 volte} \end{cases}$$

Il numero di astensioni che comportano una penalità sulla reputazione viene inteso consecutivamente e può essere modificato e adattato al contesto. Per una generica DAO, con numero elevato di membri e proposte limitate, è stato considerato ragionevole impostare la soglia a 3.

- C_i – contributo iniziale del membro i alla tesoreria della DAO. Ogni membro contribuisce alla tesoreria dell’organizzazione con una quantità $C_i > 0$. Maggiore è il contributo, maggiore è la reputazione iniziale del membro:

$$R_i^{(0)} = R_{base} + \gamma C_i.$$

- γ – fattore di conversione per la reputazione iniziale.
- k – soglia minima di partecipazione al voto. Anche la scelta di questo valore dipende dal contesto e dal caso d’uso specifico. Abbiamo notato che nelle DAO attuali la partecipazione tende ad essere bassa. Per questo motivo, una soglia troppo elevata potrebbe essere difficile da raggiungere, ostacolando il progresso dell’organizzazione. D’altra parte, una soglia troppo bassa potrebbe portare a decisioni prese con una partecipazione limitata. Una soglia del 50% + 1 può essere considerata un buon compromesso, poiché le decisioni sono rappresentative di una parte significativa della comunità.
- μ – soglia minima di partecipanti, oltre la quale si considera la divisione tra contributori e non contributori.
- ρ – soglia minima di reputazione, sotto la quale un partecipante fa parte del set dei non contributori NC .
- g – guadagno intrinseco che un giocatore associa alla DAO se la partecipazione al voto supera una certa soglia k . Viene inteso come un reward indiretto dato dall’organizzazione che ha una reputazione maggiore perché progredisce.

- c – costo di partecipazione (costi di protocollo).
- r – premio monetario (token) dato ai partecipanti al voto in caso di progresso.
- p – penalità in caso di non partecipazione al voto.

Riportiamo un esempio di simulazione per chiarire meglio i parametri sopra elencati. Si fa riferimento alla figura 4.1 nella pagina successiva.

Per questo esempio, abbiamo supposto $\mu = 6, \rho = 3, R_{base} = R_{min} = 1, \gamma = 0.5, \Delta R_{voto} = 2, \Delta R_{astenuto} = 3, R_{max} = 15$. Analizziamo ogni periodo:

- **t=0**: entrano tre utenti con contributi C_i e rispettive reputazioni $R_i^{(0)} = R_{base} + \gamma C_i$.
- **t=1**: con s_i si indica la strategia del partecipante i . In questo caso, il secondo e il terzo utente votano mentre il primo si astiene. Le reputazioni sono aggiornate in base alle strategie scelte.
- **t=2**: dopo due “epoche” di votazioni, si aggiungono alla DAO due nuovi utenti.
- **t=3**: dopo un’altra votazione, si aggiornano le reputazioni. Non essendo ancora stata superata la soglia di partecipanti μ , tutti hanno la possibilità di votare.
- Tra la quinta e la sesta votazione, entra un altro membro all’interno della DAO e ora la soglia ora è superata.
- **t=6**: l’utente 3 è categorizzato come non contributore dato che la sua reputazione ($R_3^{(6)} = 1$) è inferiore alla soglia ρ . Questo utente non potrà partecipare alle attività della DAO.

È importante sottolineare che la soglia minima di reputazione ρ è nota sin dall’inizio a tutti i partecipanti; inoltre, all’entrata di un nuovo membro dovrà essere specificata la minima contribuzione da versare per essere considerato contributore.

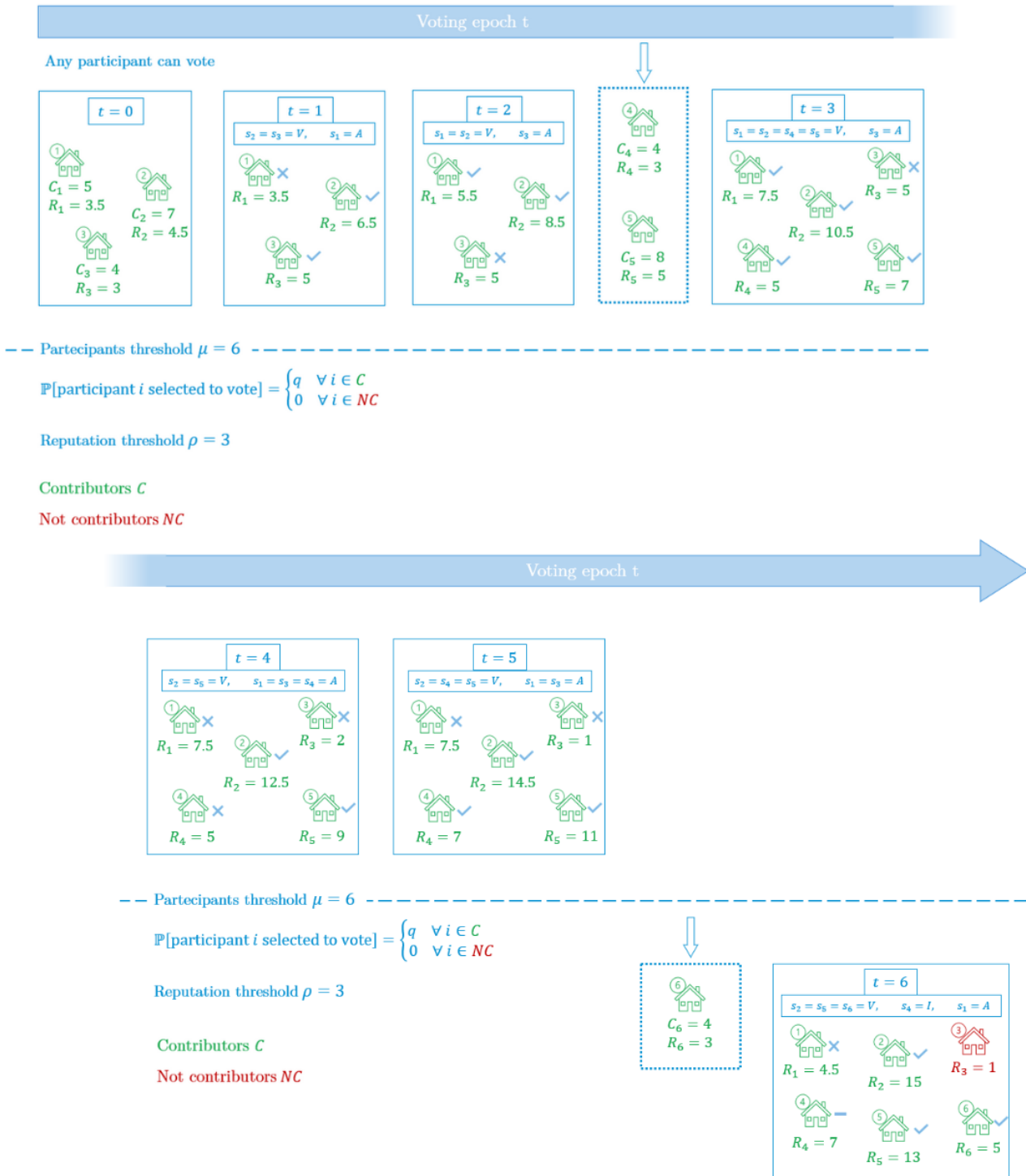


Figura 4.1: Esempio di simulazione del modello

Si procede ora con l'analisi degli equilibri di Nash, suddividendo il lavoro in due parti per riflettere ciò che avviene prima e dopo che il numero di utenti supera la soglia μ .

4.2.2 Reward, utility ed equilibri di Nash sotto la soglia μ

In questo scenario iniziale, tutti hanno la possibilità di votare all'interno della DAO.

Le strategie s_i del i -esimo membro al momento del voto sono:

V - partecipa al voto

A - si astiene dal voto

Per semplicità di notazione, la strategia del singolo utente e l'insieme di utenti che votano questa stessa strategia sarà denotata dalla stessa lettera. In particolare, V indicherà sia la strategia scelta da un utente, sia l'insieme di utenti che ha scelto di votare. Quindi, se diciamo che i è nel set V ($i \in V$), significa che questo utente partecipa al voto.

Di seguito è riportata la tabella 4.1 con i reward per le rispettive strategie, divisa in base al fatto che la DAO progredisca o meno.

	Partecipazione al voto sufficiente	Partecipazione al voto non sufficiente
V - vota	$g + r - c$	$-c$
A - astenuto	$g - p$	$-p$

Tabella 4.1: Reward nel caso in cui la soglia μ non sia superata

Denotiamo con $s = (s_1, s_2, \dots, s_n)$ la tupla che indica la strategia scelta da ogni partecipante e con s_{-i} intendiamo il profilo delle strategie scelte da tutti gli utenti eccetto i . Inoltre, introduciamo:

$\mathbb{P}(\text{progresso})$ - probabilità che ci sia progresso in una data epoca, senza tener conto di ciò che fa il giocatore i . Ovvero, è la probabilità che almeno k utenti votino.

$\mathbb{P}(\text{progresso} \mid i)$ - probabilità che si facciano progressi in una data epoca, dato che i partecipa al voto. Ovvero, è la probabilità che almeno $k - 1$ utenti votino, sapendo che i vota.

Segue la tabella 4.2 con le utility dell'utente i rispetto alla strategia scelta.

	Utility dell'utente i dato s_{-i}
V - vota	$\mathbb{P}(\text{progresso} \mid i)(g + r) - c$
A - astenuto	$\mathbb{P}(\text{progresso})g - p$

Tabella 4.2: Utility nel caso in cui la soglia μ non sia superata

Non disponendo di informazioni sulla probabilità individuale di contributo, abbiamo pensato che $\mathbb{P}(\text{progresso})$ e $\mathbb{P}(\text{progresso} \mid i)$ si possano stimare attraverso una simulazione Monte Carlo. Questo metodo permette di stimare la probabilità di progresso simulando numerose volte il processo decisionale dei partecipanti e osservando la frequenza con cui viene raggiunto il quorum k .

Proseguendo con l'analisi, una strategia $s = (s_1, s_2, \dots, s_n)$ è un equilibrio di Nash se e solo se

$$\begin{cases} u_i(s) \geq u_i(A) & \forall i \in V \\ u_i(s) \geq u_i(V) & \forall i \in A \end{cases} \quad (4.1)$$

Sostituendo e semplificando, otteniamo:

$$\begin{aligned} r\mathbb{P}(\text{progresso} \mid i \in V) + g[\mathbb{P}(\text{progresso} \mid i \in V) - \mathbb{P}(\text{progresso})] &\geq c - p \quad \forall i \in V \\ r\mathbb{P}(\text{progresso} \mid i \in V) + g[\mathbb{P}(\text{progresso} \mid i \in V) - \mathbb{P}(\text{progresso})] &\leq c - p \quad \forall i \in A \end{aligned} \quad (4.2)$$

Quindi, i giocatori saranno incentivati a votare quando il guadagno della partecipazione supera il costo (inclusa la penalità). In particolare, il premio r tale per cui sono incentivati è

$$r \geq \frac{c - p - g[\mathbb{P}(\text{progresso} \mid i \in V) - \mathbb{P}(\text{progresso})]}{\mathbb{P}(\text{progresso} \mid i \in V)}.$$

4.2.3 Reward, utility ed equilibri di Nash superata la soglia μ

Passiamo ora alla parte più interessante, in cui il numero di utenti è superiore alla soglia di partecipanti μ . In questo scenario, si introduce la distinzione tra contributori e non contributori, definita in base ad una soglia di reputazione ρ . Inoltre, gli utenti contributori sono selezionati per votare con una probabilità q .

Per questa fase dello studio degli equilibri, sono state sviluppate due idee. La prima idea si basa sul concetto presentato da Chaidos et al. [47], in cui si aggiunge una transazione che esprime l'intenzione di partecipare al progresso della DAO. Questa soluzione è più sicura, ma meno scalabile, poiché richiede di tenere traccia di tutte le transazioni. La seconda idea, invece, prevede un'interpretazione diversa di q e l'inserimento di uno stimatore, sfruttando un adattamento delle dimostrazioni fornite da Chaidos et al. [47]. Questa scelta è stata adottata per migliorare la scalabilità e adattarsi meglio a scenari di DAO più generici.

Per entrambe le opzioni, similmente a prima, si introducono due probabilità:

$\mathbb{P}(s_{-i})$ - probabilità che ci sia progresso in una data epoca, senza tener conto di ciò che fa il giocatore i . Ovvero, è la probabilità che siano selezionati almeno k utenti tra i contributori con il profilo s_{-i} .

$\mathbb{P}(s_{-i} | i)$ - probabilità che si facciano progressi in una data epoca, dato che i è selezionato e partecipa al voto. Ovvero, è la probabilità che almeno $k - 1$ utenti tra i restanti contributori, tranne i , siano selezionati per votare.

Idea 1 - con transazione

In questo caso si segue l'idea di Chaidos et al. [47], inserendo una transazione per registrare l'intenzione dei partecipanti. In questa ipotesi, q è la probabilità che un partecipante sia selezionato tra gli chi ha dato intenzione a votare (quindi non si può astenere). A causa dell'aggiunta della transazione, sono previsti degli ulteriori costi d . Con c denoteremo il costo della transazione per registrare l'intenzione, mentre con d il costo aggiuntivo per completare il voto.

Le strategie s_i dell' i -esimo membro al momento del voto sono:

V - dichiara di voler partecipare, è selezionato e partecipa al voto

I - dichiara di voler partecipare, ma non è selezionato

R - dichiara di voler partecipare, è selezionato ma ritratta (e non vota)

A - si astiene dal voto (non dichiara la partecipazione)

Anche in questo caso, per semplicità di notazione, verrà usata la stessa lettera per indicare strategia e insieme di utenti che usano quella strategia.

Si riportano reward e utility, rispettivamente tabella 4.3 e tabella 4.4, per ogni strategia scelta.

	Partecipazione al voto sufficiente	Partecipazione al voto non sufficiente
V - vota	$g + r - c - d$	$-c - d$
I - intenzionato	$g - c$	$-c$
R - ritratta	$g + r - c$	$-c$
A - astenuto	$g - p$	$-p$

Tabella 4.3: Reward nel caso in cui si superi la soglia μ - idea 1

	Utility dell'utente i dato s_{-i}
I-V - vota se selezionato	$(1 - q)\mathbb{P}(s_{-i})g + q[\mathbb{P}(s_{-i} i)(g + r) - d] - c$
I-R - ritratta se selezionato	$(1 - q)\mathbb{P}(s_{-i})g + q\mathbb{P}(s_{-i})(g + r) - c$
A - astenuto	$\mathbb{P}(s_{-i})g - p$

Tabella 4.4: Utility nel caso in cui si superi la soglia μ - idea 1

Per una questione di complessità e generalità, il premio r viene assegnato sulla base dell'intenzione a partecipare. Come già evidenziato, r rappresenta un incentivo economico destinato agli utenti che dimostrano l'intenzione di contribuire attivamente

alle attività dell'organizzazione. Questa metodologia permette di creare un sistema flessibile e adattabile a diversi casi d'uso, incentivando la partecipazione senza la necessità di un controllo dettagliato delle azioni effettivamente compiute. In questo modo, si riduce la complessità gestionale e si favorisce una maggiore generalità dei vari scenari di applicazione [47].

D'altro canto, in una DAO di dimensioni più ridotte, abbiamo pensato ad una penalizzazione della reputazione in caso di ritrattazione. Se un membro si ritrae più volte dalle proprie intenzioni dichiarate, subisce una diminuzione della reputazione. In questo modo, dopo un certo numero di ritrattazioni, entra a far parte del set di non contributori, diventando non eleggibile. Questo sistema scoraggia strategie opportunistiche di ritrattazione ripetuta, garantendo che solo coloro che mantengono un impegno costante e affidabile possano continuare a contribuire attivamente alla DAO. Tale meccanismo aiuta a mantenere l'integrità e la fiducia all'interno della comunità, rendendo non praticabile una strategia di ritrattazione nel lungo periodo.

Sotto queste condizioni, la reputazione si aggiorna nel seguente modo:

$$R_i^{(t+1)} = \begin{cases} \min \{ R_i^{(t)} + \Delta R_{voto}, R_{max} \} & \text{se } i \text{ è selezionato e partecipa al voto} \\ R_i^{(t)} & \text{se } i \text{ non è selezionato ma era intenzionato a} \\ & \text{partecipare, oppure si astiene meno di 3 volte} \\ \max \{ R_{min}, R_i^{(t)} - \Delta R_{ritratta} \} & \text{se } i \text{ è selezionato e ritratta} \\ \max \{ R_{min}, R_i^{(t)} - \Delta R_{astenuto} \} & \text{se } i \text{ è selezionato e si astiene per più di 3 volte} \end{cases}$$

Data questa riduzione di reputazione, la strategia di sola ritrattazione non è sostenibile poiché il partecipante entrerebbe nel set dei non eleggibili nel giro di poche votazioni. Infatti, dato l'utente i con reputazione massima $R_i^{(t)} = R_{max}$ all'epoca t , dopo una sola votazione la sua reputazione diventa:

$$R_i^{(t+1)} = R_{max} - q^{(t+1)} \Delta R_{ritratta}.$$

Ovvero, rimane R_{max} se non è selezionato ($q^{(t+1)} = 0$ ed è considerato intenzionato), mentre diminuisce se selezionato ($q^{(t+1)} = 1$). Si può facilmente vedere che, dopo un numero di epoche e in cui l'utente ha ritrattato se selezionato, la sua reputazione è ricalcolata come:

$$R_i^{(t+e)} = R_{max} - \sum_{j=1}^e q^{(t+j)} \Delta R_{ritratta}.$$

Cioè si accumula la penalità $\Delta R_{ritratta}$ ogni qualvolta l'utente viene selezionato.

A questo punto l'utente diventa non eleggibile se entra nel set dei non contributori, cioè se ha una reputazione minore della soglia, $R_i^{(t+e)} < \rho$. Questo si verifica se

$$\sum_{j=1}^e q^{(t+j)} > \frac{R_{max} - \rho}{\Delta R_{ritratta}}.$$

Se, per semplicità di notazione, consideriamo e il numero di epoche in cui l'utente ha effettivamente ritrattato (essendo quindi selezionato), otteniamo

$$e > \left\lfloor \frac{R_{max} - \rho}{\Delta R_{ritratta}} \right\rfloor.$$

In questo modo, e è il numero di volte in cui l'utente può ritrattare (anche se non consecutivamente selezionato) prima di diventare non eleggibile.

Inoltre, se si imposta una somma di redeem abbastanza alta, questa strategia di ritrattazione non è attuabile nel lungo periodo. In particolare, dovrebbe essere impostata con un valore superiore ai reward accumulati in questa fase, che ammontano a $e(g + r - c)$.

Passando ora al calcolo degli equilibri, una strategia $s = (s_1, s_2, \dots, s_n)$ è un equilibrio di Nash se e solo se sono soddisfatti i seguenti sistemi:

$$\begin{cases} u_i(s) \geq u_i(R) & \forall i \in V \\ u_i(s) \geq u_i(V) & \forall i \in R \end{cases} \quad \begin{cases} u_i(s) \geq u_i(A) & \forall i \in V \\ u_i(s) \geq u_i(V) & \forall i \in A \end{cases} \quad \begin{cases} u_i(s) \geq u_i(A) & \forall i \in R \\ u_i(s) \geq u_i(R) & \forall i \in A \end{cases} \quad (4.3)$$

Sostituendo le utility, otteniamo queste disequazioni con rispettive interpretazioni:

$$\begin{aligned} \mathbb{P}(s_{-i} | i) - \mathbb{P}(s_{-i}) &\geq \frac{d}{g+r} & \forall i \in V \\ \mathbb{P}(s_{-i} | i) - \mathbb{P}(s_{-i}) &\leq \frac{d}{g+r} & \forall i \in R \end{aligned} \quad (4.4)$$

Esiste un limite inferiore alla differenza tra le probabilità di successo: quella che si verifica quando i vota, e quella che si verifica grazie agli altri giocatori. Questo limite inferiore è indipendente da c , ma dipende da d .

$$\begin{aligned} q[\mathbb{P}(s_{-i} | i)(g+r) - \mathbb{P}(s_{-i})g] &\geq c + dq - p & \forall i \in V \\ q[\mathbb{P}(s_{-i} | i)(g+r) - \mathbb{P}(s_{-i})g] &\leq c + dq - p & \forall i \in A \end{aligned} \quad (4.5)$$

I giocatori sono incentivati a votare se il guadagno della partecipazione supera il costo (inclusa la penalità).

$$\begin{aligned} q\mathbb{P}(s_{-i})r &\geq c - p & \forall i \in R \\ q\mathbb{P}(s_{-i})r &\leq c - p & \forall i \in A \end{aligned} \tag{4.6}$$

Infine, il premio tale per cui i giocatori siano incentivati alla partecipazione dev'essere maggiore dei costi (inclusa la penalità).

Per semplicità, si considera il caso in cui $g = 0$. Chaidos et al. [47] dimostrano, inoltre, che per un equilibrio con un numero positivo di contributori, il profilo può essere caratterizzato da tutti votanti o includere alcuni ritrattanti, ma nessun astenuto. Pertanto, analizzeremo equilibri con soli votanti e ritrattanti. Date queste considerazioni, i vincoli risultano essere:

$$\begin{aligned} \mathbb{P}(s_{-i} | i) - \mathbb{P}(s_{-i}) &\geq \frac{d}{r} & \forall i \in V \\ \mathbb{P}(s_{-i} | i) - \mathbb{P}(s_{-i}) &\leq \frac{d}{r} & \forall i \in R \\ q\mathbb{P}(s_{-i} | i) &\geq \frac{c + dp - p}{r} & \forall i \in V \\ q\mathbb{P}(s_{-i}) &\geq \frac{c - p}{r} & \forall i \in R \end{aligned} \tag{4.7}$$

Definiamo $\lambda = |V|$ e consideriamo q la probabilità di selezionare un partecipante che ha dichiarato l'intenzione di votare, allora interpretiamo le probabilità di progresso come:

$$\begin{aligned} \mathbb{P}(s_{-i}) &= \sum_{j=k}^{\lambda} \binom{\lambda}{j} q^j (1 - q)^{\lambda - j} \\ \mathbb{P}(s_{-i} | i) &= \sum_{j=k-1}^{\lambda-1} \binom{\lambda-1}{j} q^j (1 - q)^{\lambda-1-j} \end{aligned} \tag{4.8}$$

Quindi i vincoli (4.7) diventano:

$$\begin{aligned}
 \binom{\lambda-1}{k-1} q^{k-1} (1-q)^{\lambda-k} &\geq \frac{d}{r} && \forall i \in V \\
 \binom{\lambda}{k-1} q^{k-1} (1-q)^{\lambda-k+1} &\leq \frac{d}{r} && \forall i \in R \\
 q \sum_{j=k-1}^{\lambda-1} \binom{\lambda-1}{j} q^j (1-q)^{\lambda-1-j} &\geq \frac{c+dq-p}{r} && \forall i \in V \\
 q \sum_{j=k}^{\lambda} \binom{\lambda}{j} q^j (1-q)^{\lambda-j} &\geq \frac{c-p}{r} && \forall i \in R
 \end{aligned} \tag{4.9}$$

Dalle prime due disequazioni, si può facilmente trovare un limite inferiore del numero di votanti:

$$\lambda \geq \frac{k-1}{q}.$$

Mentre, dalle ultime due si può trovare un bound per la quantità $\frac{c-p}{r}$:

$$\frac{c-p}{r} \leq q \min \left\{ \sum_{j=k-1}^{\lambda-1} \binom{\lambda-1}{j} q^j (1-q)^{\lambda-1-j} - \frac{d}{r}, \sum_{j=k}^{\lambda} \binom{\lambda}{j} q^j (1-q)^{\lambda-j} \right\}$$

Quindi, ci sarà un equilibrio con λ votanti e $n - \lambda$ ritrattanti se e solo se sono valgono:

- $\lambda \in \left[\frac{k-1}{q}, n-1 \right]$
- $\frac{d}{r} \in \left[\left(\binom{\lambda}{k-1} q^{k-1} (1-q)^{\lambda-k+1}, \binom{\lambda-1}{k-1} q^{k-1} (1-q)^{\lambda-k} \right) \right]$
- $\frac{c-p}{r} \in \left[0, q \min \left\{ \sum_{j=k-1}^{\lambda-1} \binom{\lambda-1}{j} q^j (1-q)^{\lambda-1-j} - \frac{d}{r}, \sum_{j=k}^{\lambda} \binom{\lambda}{j} q^j (1-q)^{\lambda-j} \right\} \right]$

Come ultima analisi ci si focalizza sull'equilibrio di soli votanti, ovvero $|V| = n$. Infatti, esiste un range per il premio r , dipendente dai costi c e d , tale per cui il caso in cui tutti votano è un equilibrio. In particolare,

$$\begin{aligned} \frac{d}{r} &\leq \binom{n-1}{k-1} q^{k-1} (1-q)^{n-k} && \forall i \in V \\ \frac{c-p}{r} &\leq q \sum_{j=k-1}^{n-1} \binom{n-1}{j} q^j (1-q)^{n-1-j} - \frac{dq}{r} && \forall i \in V \end{aligned} \quad (4.10)$$

Tutti gli equilibri hanno un numero relativamente alto di votanti, perciò la partecipazione può essere incentivata con l'uso di ricompense appropriate.

Idea 2 - con stimatore

Questa seconda idea si basa su una diversa interpretazione della probabilità q e sull'inserimento di uno stimatore. Per rendere l'implementazione del modello più scalabile, q è intesa come la probabilità che un partecipante venga selezionato per contribuire. È importante sottolineare la natura differente di questo parametro rispetto alla sezione precedente. Prima, q rappresentava la probabilità che un contributore fosse eletto, ossia che l'utente selezionato contribuisca sicuramente (o ritratti, ma non si astiene). In questa seconda idea, invece, q rappresenta la probabilità che un partecipante venga selezionato per avere la possibilità di contribuire, potendo quindi potenzialmente astenersi.

Il concetto di base è lo stesso in entrambe le implementazioni, ma in quest'ultima non c'è una transazione che avviene prima del voto, rendendola così più adatta per DAO generiche.

Le strategie s_i dell' i -esimo membro al momento del voto sono:

V - è selezionato e partecipa al voto

I - intenzionato a partecipare (se, per esempio, ha partecipato al 50% delle votazioni passate), ma non è selezionato

A - si astiene dal voto, decide di non partecipare (che sia selezionato o meno)

Seguono reward e utility in tabella 4.5 e in tabella 4.6.

Una strategia $s = (s_1, s_2, \dots, s_n)$ è un equilibrio di Nash se e solo se è soddisfatto

$$\begin{cases} u_i(s) \geq u_i(A) & \forall i \in V \\ u_i(s) \geq u_i(V) & \forall i \in A \end{cases} \quad (4.11)$$

	Partecipazione al voto sufficiente	Partecipazione al voto non sufficiente
V - vota	$g + r - c$	$-c$
I - intenzionato	g	0
A - astenuto	$g - p$	$-p$

Tabella 4.5: Reward nel caso in cui si superi la soglia μ - idea 2

	Utility dell'utente i dato s_{-i}
I-V - vota se selezionato	$(1 - q)\mathbb{P}(s_{-i})g + q[\mathbb{P}(s_{-i} i)(g + r) - c]$
A - astenuto	$\mathbb{P}(s_{-i})g - p$

Tabella 4.6: Utility nel caso in cui si superi la soglia μ - idea 2

Sostituendo le utility in (4.11), otteniamo:

$$\begin{aligned}
 q[\mathbb{P}(s_{-i} | i)(g + r) - \mathbb{P}(s_{-i})g] &\geq cq - p \quad \forall i \in V \\
 q[\mathbb{P}(s_{-i} | i)(g + r) - \mathbb{P}(s_{-i})g] &\leq cq - p \quad \forall i \in A
 \end{aligned}
 \tag{4.12}$$

I giocatori sono incentivati a votare se il guadagno della partecipazione supera il costo (inclusa la penalità).

Sia $\lambda = |V|$ e $n - \lambda = |A|$, con $\lambda > 0$. Consideriamo q la probabilità di selezionare un partecipante e introduciamo la probabilità v che l'utente selezionato voti, allora

interpretiamo le probabilità di progresso come:

$$\begin{aligned}\mathbb{P}(s_{-i}) &= \sum_{j=k}^{\lambda} \binom{\lambda}{j} (qv)^j (1 - qv)^{\lambda-j} \\ \mathbb{P}(s_{-i} \mid i) &= \sum_{j=k-1}^{\lambda-1} \binom{\lambda-1}{j} (qv)^j (1 - qv)^{\lambda-1-j}\end{aligned}\tag{4.13}$$

Inizialmente si considera $g = 0$, quindi le condizioni (4.12) si riducono a:

$$\begin{aligned}q \sum_{j=k-1}^{\lambda-1} \binom{\lambda-1}{j} (qv)^j (1 - qv)^{\lambda-1-j} &\geq \frac{cq - p}{r} \quad \forall i \in V \\ q \sum_{j=k-1}^{\lambda} \binom{\lambda}{j} (qv)^j (1 - qv)^{\lambda-j} &\leq \frac{cq - p}{r} \quad \forall i \in A\end{aligned}\tag{4.14}$$

Da qui si può vedere come:

- Il profilo in cui nessuno vota è un equilibrio di Nash per $k > 1$ o se $k = 1$ e $r \leq c$.
- Il profilo in cui tutti votano è un equilibrio di Nash se e solo se

$$q \sum_{j=k-1}^{n-1} \binom{n-1}{j} (qv)^j (1 - qv)^{n-1-j} \geq \frac{cq - p}{r}.$$

- Non esistono altri equilibri.

Il profilo in cui nessuno partecipa è tecnicamente un equilibrio, ma viene considerato più come “un artefatto della definizione e lontano da ciò che avviene nella pratica” [47]. Sebbene esista questo equilibrio, si deve considerare che “questo scenario è difficile da mantenere nel tempo, poiché qualsiasi coalizione di almeno k utenti potrebbe deviare e ottenere maggiori guadagni” [47]. Questo aspetto è ancora più evidente se si considera che un utente che continua ad astenersi diventerà un non contribuente e vedrà le sue risorse interne alla DAO bloccate.

Per quanto riguarda, invece, la non esistenza di altri equilibri, si può facilmente vedere per contraddizione. Infatti, se supponiamo che esista un equilibrio tale che $\forall \lambda \in \mathbb{Z}$, $0 < \lambda < n$, allora si può scrivere

$$\begin{aligned}\sum_{j=k-1}^{\lambda} \binom{\lambda}{j} (qv)^j (1 - qv)^{\lambda-j} &= \sum_{j=k-1}^{\lambda-1} \binom{\lambda-1}{j} (qv)^j (1 - qv)^{\lambda-1-j} + \\ &+ \binom{\lambda-1}{k-2} (qv)^{k-1} (1 - qv)^{\lambda-k+1}\end{aligned}\tag{4.15}$$

Per essere un equilibrio, dovrebbe soddisfare entrambe le disequazioni (4.14).

Ma, imponendo il primo vincolo

$$\sum_{j=k-1}^{\lambda-1} \binom{\lambda-1}{j} (qv)^j (1-qv)^{\lambda-1-j} \geq \frac{cq-p}{rq}.$$

e unendolo all'equazione (4.15), si crea la contraddizione.

Passiamo ora al caso in cui $g > 0$. Sostituendo (4.13) a (4.12), le disequazioni da valutare diventano:

$$\begin{aligned} r \sum_{j=k-1}^{\lambda-1} \binom{\lambda-1}{j} (qv)^j (1-qv)^{\lambda-1-j} + g \binom{\lambda-1}{k-1} (qv)^{k-1} (1-qv)^{\lambda-k} &\geq c - \frac{p}{q} \quad \forall i \in V \\ r \sum_{j=k-1}^{\lambda} \binom{\lambda}{j} (qv)^j (1-qv)^{\lambda-j} + g \binom{\lambda}{k-1} (qv)^{k-1} (1-qv)^{\lambda-k+1} &\leq c - \frac{p}{q} \quad \forall i \in A \end{aligned} \quad (4.16)$$

Per semplicità, riscriviamolo introducendo A_j e B_j :

$$\begin{aligned} rA_1 + gB_1 &\geq c - \frac{p}{q} \quad \forall i \in V \\ rA_2 + gB_2 &\leq c - \frac{p}{q} \quad \forall i \in A \end{aligned} \quad (4.17)$$

Perché valgano entrambe le disequazioni, si richiede che

$$r(A_1 - A_2) \geq g(B_2 - B_1).$$

Per assurdo, poniamo

$$r(A_1 - A_2) < g(B_2 - B_1)$$

e in particolare $B_2 > B_1$, allora si ottiene

$$\lambda < \frac{k-1}{qv}.$$

Quindi all'equilibrio devono esserci almeno $\frac{k-1}{qv}$ partecipanti che votano.

Si può ottenere un risultato più forte se supponiamo $r \geq g$. In questo caso, l'assurdo diventa $A_1 - A_2 < B_2 - B_1$ e si ottiene

$$\lambda < (2 - qv) \frac{k-1}{qv}.$$

Quindi all'equilibrio devono esserci almeno $(2 - qv) \frac{k-1}{qv}$ partecipanti che votano.

Inoltre, esiste un intervallo per il premio r tale per cui il profilo in cui tutti giocatori votano è un equilibrio di Nash:

$$r \geq \frac{c - \frac{p}{q} - gB_1}{A_1}.$$

Si possono fare delle osservazioni su questo vincolo. Man mano che g si avvicina a 0, il vincolo diventa più forte per r . In particolare, quando g è strettamente positivo, abbiamo dimostrato che ci possono essere equilibri diversi dal profilo in cui tutti votano o tutti si astengono, con un numero sufficientemente alto di partecipanti.

4.3 Adattamento alle comunità energetiche

Per concretizzare l'implementazione del modello descritto, ci concentriamo su un caso d'uso all'interno del contesto delle comunità energetiche. Vediamo più nel dettaglio le caratteristiche del modello in quest'applicazione specifica:

Progresso

Il progresso della comunità energetica è definito attraverso il raggiungimento di obiettivi di produzione e consumo energetico sostenibile. Il parametro k sarà quindi un parametro pubblico, tale per cui la DAO progredisce se si scambia almeno una percentuale k di energia rinnovabile.

Set di partecipanti alla DAO

Si ha la stessa suddivisione del modello generico con i set di partecipanti contributori C e non contributori NC . La dinamica è la medesima: fino al raggiungimento della soglia di partecipanti μ , tutti i membri sono considerati contributori e possono partecipare alle votazioni della DAO. Dopo aver superato la soglia μ , gli utenti con una reputazione inferiore ad una soglia ρ sono identificati come non contributori, non potendo più partecipare al progresso della DAO. Inoltre, questi ultimi vedono il proprio contributo iniziale bloccato e non possono accedere ai bonus o malus. Per tornare nel set dei contributori si deve effettuare un "redeem", riottenendo una reputazione tale da rientrare tra gli eleggibili.

Randomizzazione

Come per il modello generico, dopo aver superato la soglia di partecipanti μ , si considera q come la probabilità di selezionare i partecipanti per votare.

Per creare un contesto il più democratico possibile, si mantiene la simmetria di q così che la probabilità di essere selezionati sia uguale per tutti. Rimane, inoltre, la modellazione dell'eleggibilità come una serie di prove di Bernoulli indipendenti.

Reputazione

Sia $R_i^{(t)}$ la reputazione dell' i -esimo membro all'epoca t . Il calcolo della reputazione iniziale coinvolge due fattori: l'uso di impianti sostenibili e il versamento di un contributo iniziale. In particolare, i membri che installano e mantengono impianti di energia rinnovabile aumentano la loro reputazione. Allora la reputazione iniziale è:

$$R_i^{(0)} = R_{base} + \gamma C_i,$$

dove R_{base} dipende dall'impianto installato (in base al tipo di impianto si attribuisce una reputazione diversa), γ è un fattore di conversione e $C_i > 0$ è un contributo obbligatorio per entrare nella DAO. Anche in questo adattamento, così come nel modello generale, la reputazione del singolo utente varia in base alla strategia scelta al momento delle votazioni:

$$R_i^{(t+1)} = \begin{cases} \min \{ R_i^{(t)} + \Delta R_{voto}, R_{max} \} & \text{se } i \text{ è selezionato e partecipa al voto} \\ R_i^{(t)} & \text{se } i \text{ non è selezionato ma era intenzionato a} \\ & \text{partecipare, oppure si astiene meno di * volte} \\ \max \{ R_{min}, R_i^{(t)} - \Delta R_{astenuto} \} & \text{se } i \text{ è selezionato e si astiene per più di * volte} \end{cases}$$

Si discuterà successivamente la questione del numero di astensioni consecutive che comportano una penalità sulla reputazione.

Ricordiamo che votare esprime la volontà di contribuire al progresso della DAO. Proprio per questo impegno nei meccanismi di scambio energetico sostenibile, la reputazione dell'utente che vota viene incrementata.

Configurazione esaminata

Secondo il rapporto semestrale del GSE [51], al 30 giugno 2023 risultano 35 Comunità Energetiche Rinnovabili in Italia. Di queste, quasi il 70% hanno impianti fino a 20 kW di potenza. Il numero medio di utenti è piuttosto moderato (circa 8). In particolare, 3 clienti circa per impianti tra 0 e 10 kW, 8 per impianti tra 10 e 20 kW.

Per la nostra simulazione si può quindi considerare una comunità energetica con potenza medio-bassa, tra i 10 e i 20 kW, con una media di 8 utenti circa. Data questa configurazione, si è pensato di seguire la seconda idea del modello che non implica una transazione aggiuntiva.

Scelta soglie e parametri

Per quanto riguarda la scelta delle soglie e dei parametri del modello, l'idea è effettuare delle simulazioni per individuare le combinazioni ottimali che permettono un progresso efficace della comunità. A tale proposito, possiamo fare alcune osservazioni: considerando la configurazione descritta sopra, una scelta iniziale ragionevole per la soglia di partecipanti potrebbe essere fissata a $\mu = 3$, dato che il totale degli utenti è pari a 8.

Anche se la DAO analizzata ha un numero ridotto di partecipanti rispetto al modello generico, l'obiettivo rimane quello di renderla longeva e sostenibile. Inoltre, poiché si tratta di una comunità energetica locale, risulta difficile integrare nuovi membri esterni. Per queste ragioni, il decadimento in caso di astensione sarà più lento. Per una valutazione iniziale, si è pensato di fissare a 6 il numero di astensioni massime prima di applicare la penalità sulla reputazione. Questa scelta è dovuta al fatto che, in questo modo, l'utente ha più opportunità di evitare di essere classificato come non contributore, essendo che la configurazione non favorisce l'ingresso di nuovi membri.

Inoltre, per la simulazione, sono stati assegnati dei valori alle reputazioni iniziali rispetto al tipo di impianto rinnovabile posseduto dall'utente. In particolare, sono stati presi in considerazione impianti di tipo solare, eolico, idroelettrico e un'ultima categoria denominata 'altro' che include le fonti rinnovabili minori come la geotermica e la bioenergia. Per determinare le reputazioni iniziali associate a ciascuna tipologia, è stato tenuto in considerazione il report della International Renewable Energy Agency datato Luglio 2024 [52]. Nelle statistiche qui riportate, si evidenzia che "nel 2022 l'energia idroelettrica è rimasta la principale fonte di energia elettrica rinnovabile" [52], generando il 51.3% dell'energia rinnovabile totale. Segue l'energia eolica con il 24.9% e la solare, definita come "la fonte di energia rinnovabile in più rapida crescita negli ultimi anni" [52], con il 15.3% della generazione rinnovabile. La bioenergia e la geotermica hanno contribuito rispettivamente per il 7.3% e il 1.2%.

Nell'ambito della simulazione, è logico supporre che un utente con un impianto rinnovabile parta con una reputazione almeno pari alla soglia minima di reputazione ρ . Considerando i valori iniziali attribuiti ai parametri (dove $\rho = 30$) e le percentuali sopra riportate, sono stati assegnati i seguenti valori agli impianti: 'solare': 35, 'eolico': 40, 'idroelettrico': 50, 'altro': 30. Questi valori possono essere modificati e adattati in base al caso d'uso specifico.

4.3.1 Simulazione dei parametri

L'idea della simulazione è quella di riprodurre il comportamento di una comunità energetica di 8 utenti basata su una DAO, su un periodo temporale di 10 anni.

L'obiettivo di questa simulazione è quello di identificare la combinazione ottimale dei parametri considerati nel modello proposto, al fine di assicurare la formazione e il mantenimento di una comunità energetica duratura e sostenibile nel tempo. Il processo di simulazione consente di testare diverse configurazioni e di individuare quelle che meglio rispondono al caso d'uso considerato, tenendo conto delle interazioni complesse tra i diversi fattori.

Nella tabella 4.7 riportiamo i parametri del modello generico, affiancati dal valore utilizzato nella simulazione.

Nella tabella 4.8 riportiamo, invece, altri parametri che ci sono stati utili per la simulazione, anche questi modificabili e adattabili per i diversi contesti. In particolare, durante la simulazione abbiamo supposto una media di una proposta a settimana (analizzando il numero di proposte della maggior parte delle DAO in DeepDAO [25]) e 7 giorni per la votazione di esse (come la media delle DAO attuali, sezione 2.8). Per lo scopo della simulazione, abbiamo stimato una probabilità di redeem e una probabilità v di votare se selezionati. Oltre a questo, per renderla più completa, abbiamo pensato ad un inserimento graduale degli utenti suddivisa in tre blocchi.

Parametro	Descrizione	Valore	Nota
μ	Soglia minima di partecipanti per distinguere tra contributori e non contributori	3	Come spiegato in “Scelta soglie e parametri”
ρ	Soglia minima di reputazione per essere considerato contributore	30	Vedi sezione 4.3.3
γ	Fattore di conversione per la reputazione iniziale	0.7	Per dare la giusta importanza al contributo iniziale C_i
ΔR_{voto}	Incremento di reputazione in caso di voto	10	Vedi sezione 4.3.3
$\Delta R_{astenuto}$	Penalità di reputazione in caso di astensione	15	Vedi sezione 4.3.3
R_{min}	Reputazione minima	1	Non si può considerare una reputazione negativa
R_{max}	Reputazione massima	100	Per semplicità di interpretazione e potersi esprimere in termini di percentuali più facilmente
$max\ astensioni$	Numero massimo di astensioni consecutive senza penalità	6	Come spiegato in “Scelta soglie e parametri”
q	Probabilità di essere selezionati per votare	0.7	Dev’essere abbastanza alta per permettere il progresso della DAO

Tabella 4.7: Parametri e rispettivi valori della simulazione

Parametro	Descrizione	Valore	Nota
<i>N anni</i>	Durata della simulazione (in anni)	10	Scelta per verificare la longevità di una comunità
<i>N utenti totali</i>	Numero totale dei partecipanti alla comunità energetica	8	Come spiegato in “Configurazione esaminata”
<i>proposte settimanali</i>	Numero di proposte settimanali all’interno della DAO	1	Considerando una media delle proposte settimanali attuali [25]
<i>durata votazione</i>	Durata di ogni votazione (in giorni)	7	Come nella media delle DAO attuali
<i>prob redeem</i>	Probabilità di effettuare il redeem essendo non contributore	0.5	L’utente non contributore, presumibilmente, ha comportamenti egoistici, quindi non sempre sceglierà di effettuare il redeem
<i>prob voto</i>	Probabilità di votare	Tra 0.4 e 0.9	Parametro variabile per considerare più tipologie di utenti
<i>utenti iniziali</i>	Primo blocco di utenti	3	Non si voleva superare la soglia μ fin dall’inizio della simulazione
<i>utenti secondo blocco</i>	Secondo blocco di utenti	2	Scelta per superare la soglia μ
<i>utenti terzo blocco</i>	Terzo blocco di utenti	3	Dalla differenza dei membri totali e gli altri blocchi

Tabella 4.8: Altri parametri e rispettivi valori della simulazione

Dopo aver definito i parametri, spieghiamo nel dettaglio cosa avviene all'interno della simulazione attraverso le funzioni implementate:

- ① Abbiamo definito una funzione che inizializza le reputazioni dei nuovi utenti, prendendo in input il tipo di impianto rinnovabile e la contribuzione iniziale obbligatoria.

```
def initialize_reputation(new_users, current_reputations):
    new_reputations = current_reputations.copy()

    for i in range(new_users):
        user_index = len(new_reputations) + 1
        plant = input(f"\nUser {user_index}, what type of renewable plant do you own? (
                    solar, wind, hydroelectric, other, none): ").strip().lower()
        R_base = plant_reputation.get(plant, 0)
        C_i = float(input(f"Enter your initial contribution for User {user_index}: "))

        while C_i <= 0:
            C_i = float(input("\nThe initial contribution must be greater than 0. Enter
                            again: "))

        R_i = R_base +  $\gamma$  * C_i

        # Alert and request for new contribution if reputation is less than  $\rho$  and number
        # of users exceeds  $\mu$ 
        if len(new_reputations) + 1 >=  $\mu$  and R_i <  $\rho$ :
            print(f"\nAlert: User {user_index}'s initial reputation is less than { $\rho$ }.")

            while R_i <  $\rho$ :
                C_i = float(input(f"\nPlease make a new contribution of at least {round( $\rho$ /
                     $\gamma$ ,2)} to reach the reputation threshold { $\rho$ }. Total
                    amount contributed: "))
                R_i = R_base +  $\gamma$  * C_i

        # Reputation must be between R_min and R_max
        R_i = min(R_max, max(R_min, R_i))

        new_reputations.append(R_i)
        print(f"\nUser {user_index}'s initial reputation: {round(R_i,2)} (Plant: {plant},
            Contribution: {C_i})")

    return new_reputations
```

Listing 4.1: Funzione per inizializzare la reputazione di nuovi membri

- ② La funzione successiva aggiorna le reputazioni degli utenti come abbiamo definito nel capitolo 4.3.

```
def update_reputation(reputations, selected, abstentions):
    new_reputations = reputations.copy()

    for i in range(len(reputations)):
        if i in selected:
            if random.random() < probab_vote[i]: # Generate a random number between 0 and
                                                    1, if it's less than the voting
                                                    probability, the user votes

                new_reputations[i] = min(reputations[i] + ΔR_vote, R_max)
                abstentions[i] = 0
            elif abstentions[i] < max_abstentions: # If the user abstains less than
                                                    max_abstentions consecutive times

                new_reputations[i] = reputations[i]
                abstentions[i] += 1
            else: # If the user abstains more than max_abstentions consecutive times

                new_reputations[i] = max(R_min, reputations[i] - ΔR_abstain)
                abstentions[i] += 1
        else: # If not selected

            new_reputations[i] = reputations[i]

    return new_reputations, abstentions
```

Listing 4.2: Funzione per aggiornare le reputazioni degli utenti dopo la votazione

- ③ Questa funzione effettua un redeem casuale per un utente non contributore, seguendo una distribuzione di Bernoulli. La contribuzione minima di redeem è quella che permette all'utente di rientrare con il minimo di reputazione per essere considerato contributore.

```
def redeem_user(user_index, reputations):
    # Check if the user is currently a non-contributor
    if reputations[user_index] < ρ:
        print(f"\nUser {user_index + 1} is a non-contributor.")

        # Determine if the user attempts the redeem based on a Bernoulli distribution
        if random.random() < probab_redeem:
            print(f"\nUser {user_index + 1} attempts a redeem.")

            # Request the contribution for the redeem
            C_i = float(input(f"\nUser {user_index + 1}: Enter the contribution for the
                               redeem (must be at least {round(ρ/γ, 2)}): "))

            # Check that the contribution is at least equal to ρ/γ
```

```

if C_i >= (ρ/γ):
    # Calculate the user's new reputation
    reputations[user_index] = min(R_max, reputations[user_index] + γ * C_i)

    print(f"\nThe redeem was successful. The new reputation of user
          {user_index + 1} is {round(reputations[user_index], 2)}.")
    return reputations, True
else:
    print(f"\nThe contribution is less than {round(ρ/γ, 2)}. The redeem was
          not completed.")
    return reputations, False
else:
    print(f"\nUser {user_index + 1} decided not to attempt a redeem.")
    return reputations, False
else:
    print(f"\nUser {user_index + 1} is already a contributor and does not need a
          redeem.")
    return reputations, False

```

Listing 4.3: Funzione per fare un redeem casuale per un utente non contributore

- ④ Per rendere la simulazione più completa, abbiamo pensato di dare la possibilità di aggiungere degli impianti rinnovabili durante il periodo temporale preso in esame. In questo caso, si aggiunge la reputazione corrispondente all'impianto alla reputazione attuale dell'utente.

```

def add_plant(user_index, reputations, plant_reputation):
    add = input(f"\nUser {user_index + 1}: Do you want to add a renewable plant? (y/n): ")
        .lower()

    if add == 'y':
        plant_type = input(f"\nUser {user_index + 1}: Enter the type of plant ('solar',
                              'wind', 'hydroelectric', 'other'): ").lower()

        # Default to "none" if an invalid type is entered
        if plant_type not in plant_reputation:
            print("\nInvalid plant type. No plant added.")
        else:
            # Add the plant's reputation value to the current one
            reputations[user_index] += plant_reputation[plant_type]

        if reputations[user_index] > R_max:
            reputations[user_index] = R_max

```

```

print(f"\nNew {plant_type} plant added. The new reputation of user {user_index
      + 1} is {round(reputations[user_index], 2)}.")

return reputations

```

Listing 4.4: Funzione per l'aggiunta di impianti rinnovabili

- ⑤ La funzione sottostante simula la selezione degli utenti che avranno la possibilità di votare, come una distribuzione Bernoulli.

```

def simulate_vote(reputations):
    # Check if the number of users is greater than  $\mu$  to consider the threshold  $\rho$ 
    if len(reputations) <  $\mu$ :
        contributors = list(range(len(reputations))) # Everyone is a contributor if the
                                                    # number of members is <  $\mu$ 
    else:
        contributors = [i for i in range(len(reputations)) if reputations[i] >=  $\rho$ ]

    selected = []

    for i in contributors:
        if len(reputations) <  $\mu$ :
            selected.append(i) # Everyone is selected if the number of members is <  $\mu$ 
        else:
            if random.random() < q: # Generate a random number between 0 and 1, if it's
                                    # less than q, the user is selected
                selected.append(i)

    return selected

```

Listing 4.5: Funzione per simulare la selezione degli utenti

- ⑥ Per regolare più facilmente i parametri, si teneva anche in considerazione il tempo necessario per diventare non contributore partendo dalla reputazione massima. Con i parametri impostati come nelle tabelle 4.7, 4.8, servono 11 epoche di voto per passare da R_{max} a $R_i < \rho$.

```

def calculate_time_to_become_non_contributor():
    reputation = R_max
    epochs_needed = 0
    consecutive_abstentions = 0

    while reputation >=  $\rho$ :
        if consecutive_abstentions >= max_abstentions: # The first max_abstentions-1 do
                                                        # not incur a penalty

```

```

        reputation = max(R_min, reputation - ΔR_abstain)

    consecutive_abstentions += 1
    epochs_needed += 1

return epochs_needed

```

Listing 4.6: Funzione per calcolare il tempo necessario per diventare non contributore

- ⑦ Infine, per costruire un plot significativo, si è calcolato il tempo che ogni utente ha trascorso come non contributore.

```

def calculate_non_contributor_time(reputation_history):
    non_contributor_time = [0] * N_total_users

    for i in range(N_total_users):
        for r in range(1, len(reputation_history), 2):
            # Participant threshold must be exceeded to consider non contributors
            if len(reputation_history[r]) >= μ and reputation_history[r][i] < ρ:
                non_contributor_time[i] += 1

    return non_contributor_time

```

Listing 4.7: Funzione per calcolare il tempo trascorso come non contributore

- ⑧ Successivamente, tutte le funzioni sono state integrate all'interno di una simulazione completa del processo di voto. In questa simulazione, anno per anno, si riproduce il ciclo completo, con l'aggiunta graduale degli utenti (rispettivamente dopo il primo e il secondo anno), la possibilità di redeem dopo 4 o 6 anni e l'opzione di aggiungere nuovi impianti ogni anno.

```

def simulation():
    # Initialize the first users
    reputations = initialize_reputation(initial_users, [])
    abstentions = [0] * N_total_users
    reputation_history = [reputations.copy()]
    selection_history = []
    abstention_history = [abstentions.copy()]
    simulation_days = N_years * 365
    num_proposals = weekly_proposals * 52 # Total number of proposals in 1 year
    voting_days = 0 # Counter to track voting days

    for day in range(simulation_days):
        if day % 365 == 0 and day != 0: # Every year

```

```

print(f"\n\nAfter {day // 365} years")

if day % (7 // weekly_proposals) == 0:      # Every time there is a proposal, a
                                             vote is simulated
    selected = simulate_vote(reputations)
    reputations, abstentions = update_reputation(reputations, selected,
                                                abstentions)

    voting_days = voting_duration
    reputation_history.append(reputations.copy())
    selection_history.append(selected)
    abstention_history.append(abstentions.copy())

if voting_days > 0:
    voting_days -= 1

# Gradual addition of users
if day == (1 * 365): # After 1 year
    reputations = initialize_reputation(second_block_users, reputations)
elif day == (2 * 365): # After 2 years
    reputations = initialize_reputation(third_block_users, reputations)
elif day == (4 * 365) or day == (6 * 365): # After 4 or 6 years, there is a
                                             possibility to redeem

    for i in range(N_total_users):
        if len(reputations) >=  $\mu$  and reputations[i] <  $\rho$ :
            reputations, success = redeem_user(i, reputations)
            if success:
                print(f"User {i + 1} has returned to being a contributor.")

if voting_days == 0:
    reputation_history.append(reputations.copy())
    selection_history.append([])
    abstention_history.append([])

# Addition of new plants once a year, but not for newly added users
if day % 365 == 0:
    if day == 365: # After 1 year, only for initial users
        for i in range(initial_users):
            reputations = add_plant(i, reputations, plant_reputation)
    if day == 2 * 365: # After 2 years, for the first and second blocks
        for i in range(initial_users + second_block_users):
            reputations = add_plant(i, reputations, plant_reputation)
    if day >= 3 * 365: # After 3 years, for all users
        for i in range(len(reputations)):
            if reputations[i] >=  $\rho$ : # Only contributors
                reputations = add_plant(i, reputations, plant_reputation)

```

```
print(f"\nAverage number of proposals analyzed in 1 years: {num_proposals}")  
return reputation_history, selection_history, abstention_history
```

Listing 4.8: Simulazione completa

4.3.2 Plot della simulazione

Una componente significativa della simulazione sono i grafici. In particolare, sono state sviluppate cinque diverse tipologie di plot. Infatti, questi grafici si sono rivelati fondamentali per individuare la configurazione ottimale dei parametri descritti in precedenza (all'inizio della sezione 4.3.1).

La figura 4.2 mostra l'andamento delle reputazioni di ogni utente nel periodo temporale specificato. Nello specifico, possiamo notare l'entrata di nuovi utenti (l'utente 4 e l'utente 5) al primo anno e successivamente il terzo blocco di utenti (l'utente 6, l'utente 7 e l'utente 8) al secondo anno. Un'altra osservazione da fare riguarda l'utente 2, che poco dopo l'inizio del quinto anno diventa non contributore perchè la sua reputazione è sotto la soglia $\rho = 30$. Questo utente effettua poi un redeem al sesto anno, tornando infatti tra i contributtori. In questa simulazione l'utente 2 aveva una probabilità di voto pari a 0.4, così come l'utente 6. Da notare che gli altri utenti (con *prob voto* tra 0.5 e 0.9) mantengono per quasi tutto il tempo una reputazione massima.

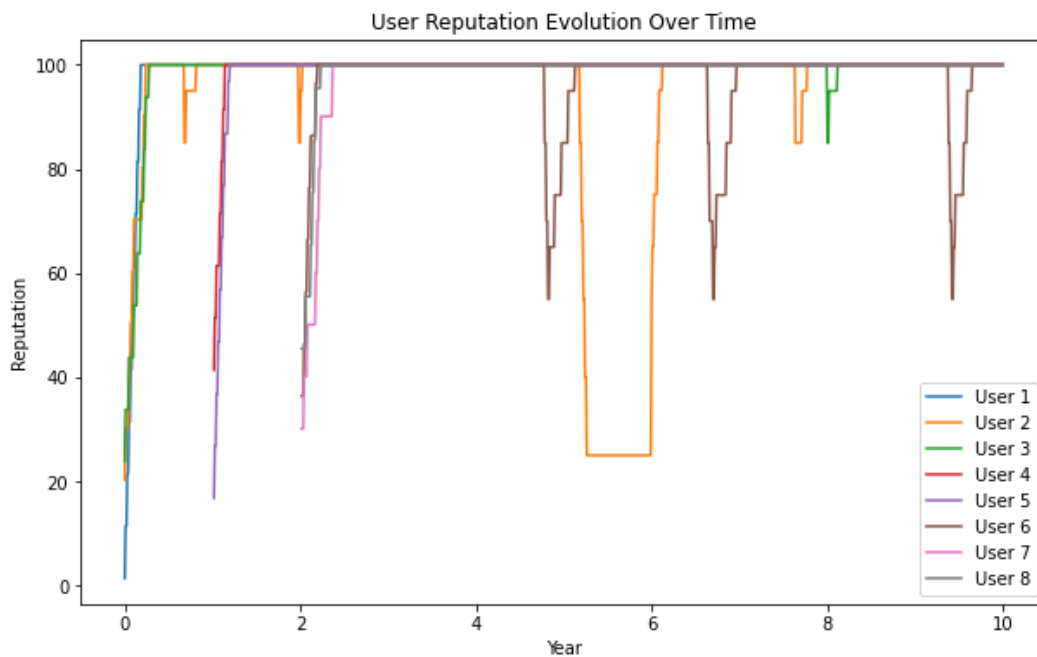


Figura 4.2: Evoluzione della reputazione degli utenti nel tempo

Un secondo grafico (figura 4.3) illustra il numero di contributtori al variare del tempo. Coerentemente con il plot precedente, tra il quinto e il sesto anno c'è un abbassamento del numero di contributtori, dovuto al fatto che l'utente 2 in questo periodo temporale aveva una reputazione troppo bassa. Questo grafico potrebbe

risultare più significativo nel contesto di una DAO con un numero elevato di utenti.

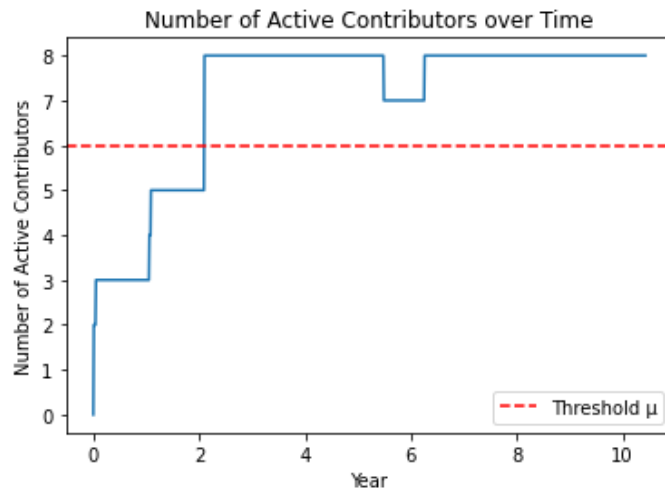


Figura 4.3: Numero di contributori nel tempo

In figura 4.4 si nota che l'utente con il maggior numero di astensioni è il numero 2, in maniera coerente con quanto osservato precedentemente. Un'altra osservazione da evidenziare riguarda l'utente 3: presenta un numero di astensioni paragonabile a quello dell'utente 6, ma, diversamente da quest'ultimo, la sua reputazione non è mai scesa drasticamente (vedi figura 4.2). Questo avviene perchè le astensioni dell'utente 3 non sono state consecutive e non hanno mai superato il numero massimo per cui sarebbe stata applicata una penalità alla reputazione.

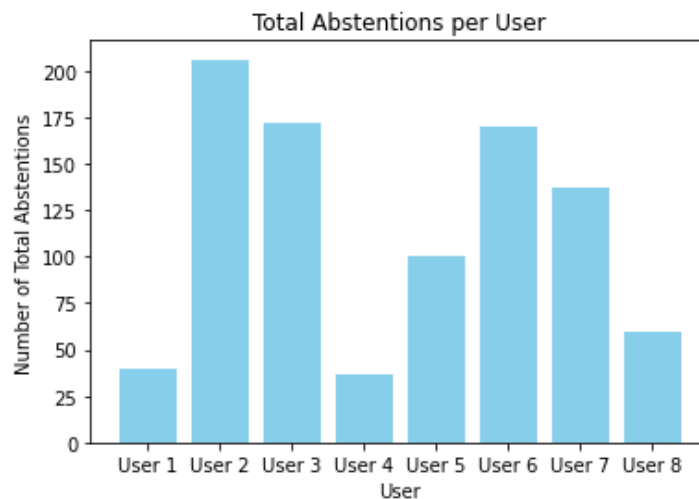


Figura 4.4: Totale di astensioni per utente

Il plot sottostante raffigura l'andamento delle astensioni nel periodo di tempo della simulazione. Le osservazioni precedenti continuano a valere: gli utenti 2 e 6 hanno un numero di astensioni alto per quasi ogni anno. Si può notare un abbassamento delle astensioni dell'utente 2 tra il quinto e il sesto anno, corrispondente al suo periodo di non contribuzione.

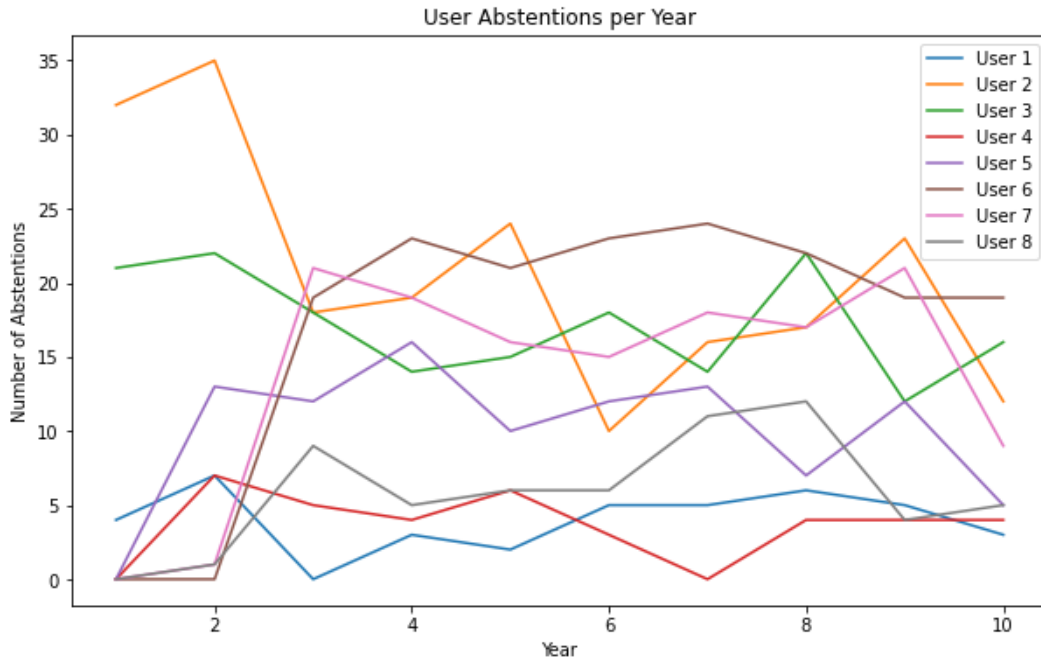


Figura 4.5: Evoluzione delle astensioni negli anni

L'ultimo grafico rappresenta il tempo trascorso da ciascun utente come non contributore. Poichè l'utente 2 è l'unico ad aver assunto quello status, anche se per un breve periodo, l'istogramma mostra una sola barra corrispondente a lui. Come già menzionato per la figura 4.3, questo grafico sarebbe più significativo con un numero maggiore di utenti, specialmente se alcuni di loro avessero attraversato periodi, anche brevi, come non contributori.

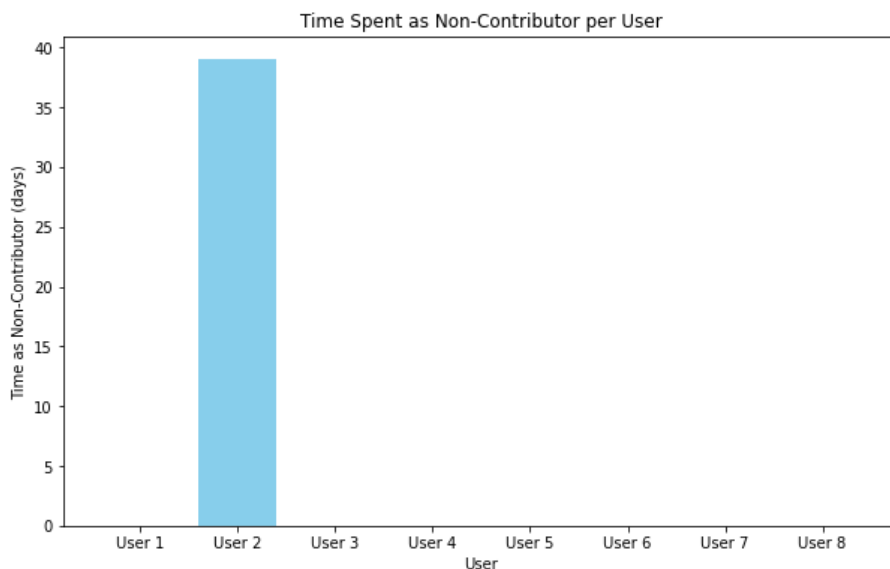


Figura 4.6: Tempo trascorso come non contributore

4.3.3 Commenti finali

In questa sezione, ci concentreremo sui parametri che sono stati modificati più frequentemente durante la simulazione: ρ , ΔR_{voto} e $\Delta R_{astenuto}$. Questi parametri sono fondamentali per l'andamento della reputazione di ogni utente, così come μ e $max\ astensioni$ che abbiamo già approfondito nella sezione “Scelta soglie e parametri”.

Consideriamo la stessa tipologia di grafico mostrata in 4.2, modificando però i parametri ΔR_{voto} e $\Delta R_{astenuto}$. In particolare, aumentiamo entrambi i valori di 10 unità e ne analizziamo le conseguenze. Un aspetto da sottolineare riguarda il tempo necessario per diventare non contributore (codice 4.6) che, con questi parametri, scende al di sotto delle 10 epoche di voto, equivalenti a meno di 70 giorni nel caso in cui l'utente venga selezionato ad ogni votazione. È importante notare che un periodo inferiore a 70 giorni, risulta piuttosto ridotto, compromettendo la possibilità di una partecipazione duratura. Inoltre, il grafico 4.7 evidenzia come i

cambiamenti di reputazione, sia in positivo che in negativo, diventino più bruschi. Per queste ragioni, si è deciso di non adottare i parametri $\Delta R_{voto}, \Delta R_{astenuto} \geq 20$.

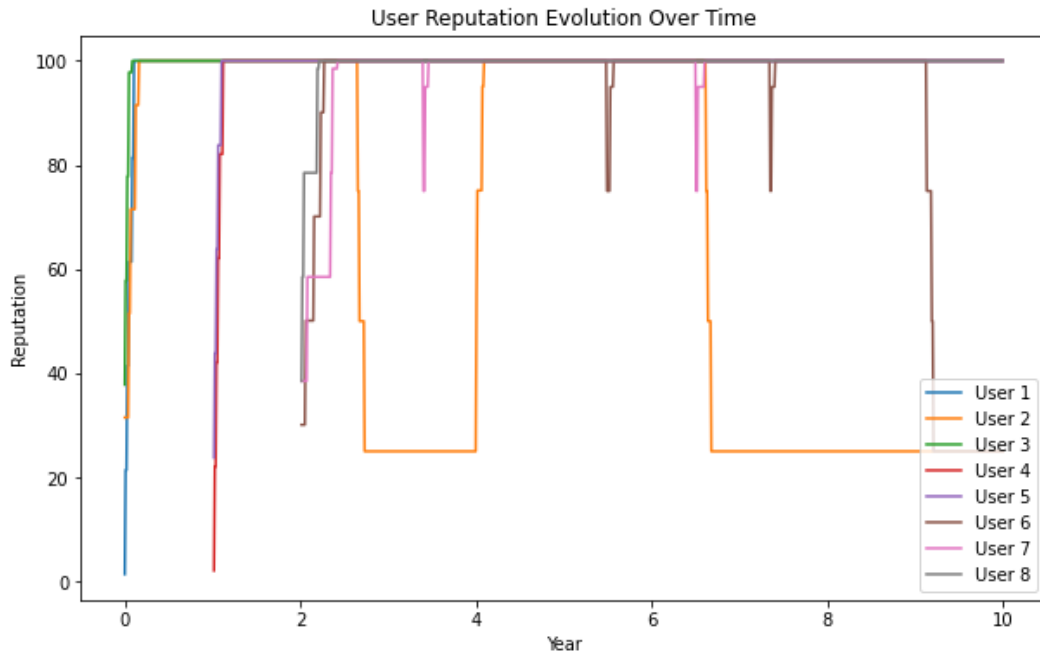


Figura 4.7: Evoluzione della reputazione degli utenti aumentando ΔR_{voto} e $\Delta R_{astenuto}$

D'altro canto, considerare delle soglie di ΔR_{voto} e $\Delta R_{astenuto}$ troppo basse, comporterebbe il rischio di non penalizzare i comportamenti scorretti adeguatamente e, d'altra parte, non incentivare sufficientemente quelli corretti. Impostando $\Delta R_{voto} = \Delta R_{astenuto} = 5$, abbiamo ottenuto la figura 4.8, da cui è evidente ciò che abbiamo appena affermato. Se volessimo adottare dei valori così ridotti, dovremmo modificare drasticamente anche gli altri parametri del modello, compromettendo la stabilità complessiva. Per questi motivi, i parametri scelti sono $\Delta R_{voto}, \Delta R_{astenuto} > 5$.

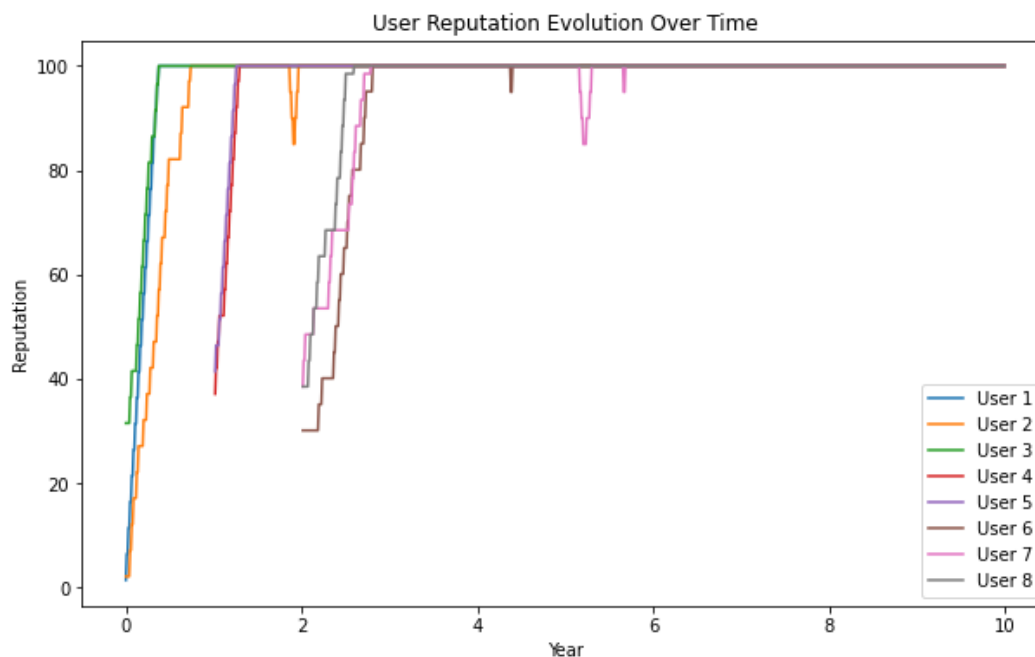


Figura 4.8: Evoluzione della reputazione degli utenti diminuendo ΔR_{voto} e $\Delta R_{astenuto}$

Ora fissiamo i valori di ΔR_{voto} e $\Delta R_{astenuto}$ come definiti in tabella 4.7 e concentriamoci su ρ .

Ricordiamo che ρ rappresenta la soglia minima di reputazione al di sotto della quale un utente non è più considerato contributore, perdendo così il diritto di partecipare alle attività della DAO. Di conseguenza, il contributo richiesto al momento dell'ingresso dell'utente nella comunità energetica dipenderà da questo parametro: all'aumentare di ρ , crescerà anche il contributo iniziale da versare. Tuttavia, un valore elevato di ρ potrebbe ridurre la flessibilità degli utenti, penalizzandoli in caso di eventuali periodi di inattività. Questo effetto è visibile nella figura 4.9.

Allo stesso tempo, non è possibile impostare un valore di ρ così basso da tollerare un comportamento non collaborativo per lunghi periodi. Nel grafico 4.10 vediamo che l'utente 2 e l'utente 6 non hanno contribuito in maniera adeguata al progresso della comunità energetica; tuttavia, nonostante ciò, non sono stati temporaneamente esclusi come contributori.

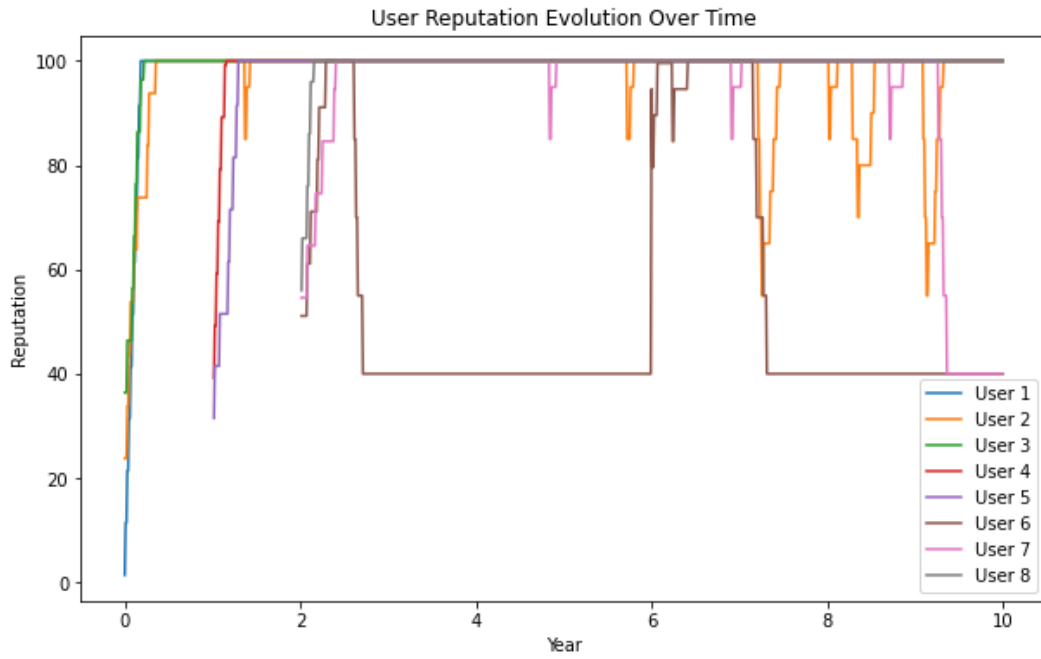


Figura 4.9: Evoluzione della reputazione degli utenti aumentando ρ

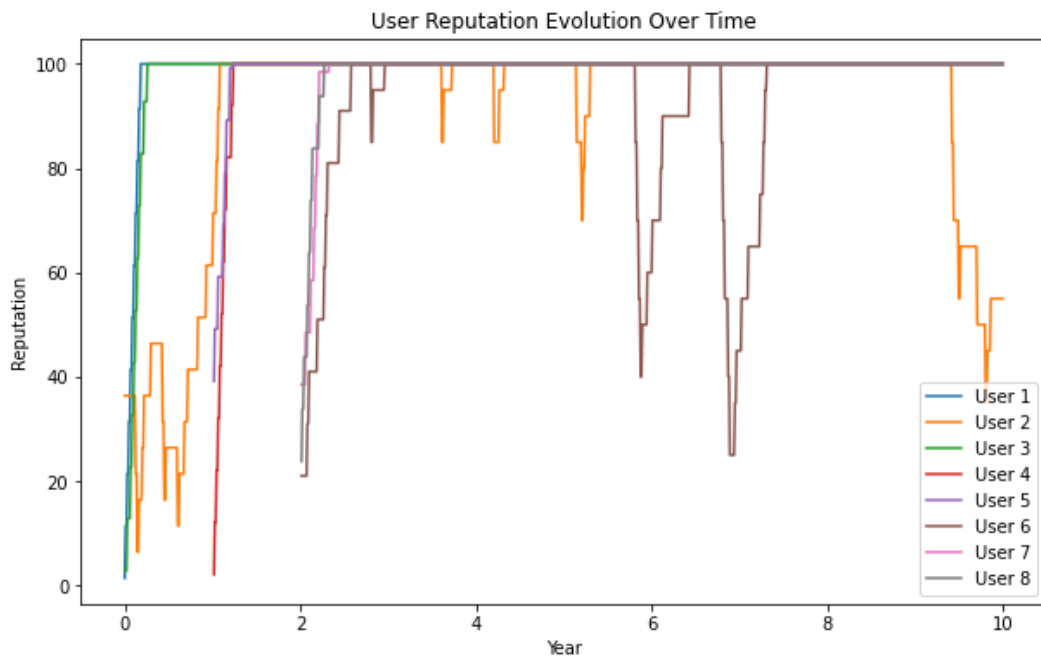


Figura 4.10: Evoluzione della reputazione degli utenti diminuendo ρ

Il sistema di reputazione studiato prevede un meccanismo in cui gli utenti possono acquisire o perdere reputazione gradualmente. Con una soglia $\rho = 30$, si offre agli utenti la possibilità di rendersi conto di essere in una “zona di rischio”, dando loro tempo sufficiente per correggere il loro comportamento prima di vedere i propri contributi bloccati. In generale, i parametri così impostati permettono di raggiungere un equilibrio tra la tolleranza verso comportamenti occasionalmente non collaborativi e la necessità di mantenere un sistema longevo e sostenibile nel tempo.

Conclusione e sviluppi futuri

Le Decentralized Autonomous Organization (DAO) rappresentano un'importante innovazione nel campo della governance, offrendo un modello decentralizzato che promette maggiore trasparenza, automazione ed efficienza rispetto alle strutture organizzative tradizionali. Attraverso l'uso della tecnologia blockchain e degli smart contract, le DAO permettono di eliminare intermediari, garantendo processi decisionali autonomi e sicuri. Tuttavia, come evidenziato dall'analisi dei KPI, uno dei principali ostacoli al successo delle DAO è la bassa partecipazione degli utenti alle attività di governance, problema che, se non affrontato, può minare la decentralizzazione stessa dell'organizzazione.

Per affrontare questa sfida, è stato sviluppato un modello basato sulla teoria dei giochi, progettato per incentivare una maggiore partecipazione attraverso meccanismi di ricompensa, penalità e reputazione. Applicando questo modello ad una comunità energetica basata su DAO, i risultati della simulazione hanno mostrato che un sistema di incentivazione ben strutturato può migliorare significativamente il coinvolgimento degli utenti, garantendo inoltre la stabilità e la sostenibilità a lungo termine della DAO. Infatti, come evidenziato dai grafici della simulazione, l'obiettivo è stato raggiunto: trovare la combinazione ottimale dei parametri del modello proposto per garantire la sostenibilità a lungo termine di una comunità energetica basata su una DAO.

Nonostante i risultati positivi, è importante sottolineare che sia la tecnologia blockchain sia le DAO sono ancora in fase di sviluppo. Una particolare attenzione dovrà essere posta nell'esplicitare le implicazioni legali e normative delle DAO, che ad oggi restano un'incognita. Nell'elaborato vengono discusse anche le principali problematiche che rendono difficile l'implementazione di una DAO in contesti reali, tra cui le sfide legate alla sicurezza e alla privacy. L'analisi dei KPI conferma che le DAO attuali sono ancora in una fase prematura per questo genere di applicazioni.

Questa tesi, inoltre, presenta alcuni limiti che aprono la strada a future ricerche. Innanzitutto, l'applicazione del modello è stata simulata in un contesto specifico,

ovvero quello delle comunità energetiche di soli otto utenti. Sebbene i principi possano essere generalizzati, è necessario verificare l'efficacia del modello in contesti più complessi e con dinamiche diverse. Inoltre, nella simulazione sono stati utilizzati stimatori per alcune probabilità e sono state considerate una serie limitata di variabili, non esplorando le complessità che possono emergere in ambienti reali, come la dinamica sociale tra i partecipanti o i conflitti di interesse. Sarà quindi necessario, in ricerche future, testare il modello in ambienti reali o su larga scala.

In conclusione, questa tesi ha dimostrato come l'implementazione di meccanismi di incentivazione possa migliorare la partecipazione nelle DAO e come queste organizzazioni possano offrire soluzioni promettenti per la governance di comunità complesse, come quelle energetiche. Tuttavia, rimangono molte sfide da affrontare per garantire il successo delle DAO in contesti più ampi e diversificati. La speranza è che i risultati di questa ricerca possano fungere da base per ulteriori studi e sperimentazioni, con l'obiettivo di rendere le DAO strumenti sempre più efficaci e sostenibili nel lungo periodo.

Bibliografia

- [1] H. Guo e X. Yu, «A survey on blockchain technology and its security,» *Blockchain: research and applications*, vol. 3, n. 2, p. 100 067, 2022.
- [2] Q. Wang, G. Yu, Y. Sai, C. Sun, L. D. Nguyen, X. Xu e S. Chen, «A First Look into Blockchain DAOs,» in *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, IEEE, 2023, pp. 1–3.
- [3] H. Altaieb e R. Zoltán, «Decentralized autonomous organizations review, importance, and applications,» in *2022 IEEE 26th International Conference on Intelligent Engineering Systems (INES)*, IEEE, 2022, pp. 121–126.
- [4] S. Wang, W. Ding, J. Li, Y. Yuan, L. Ouyang e F.-Y. Wang, «Decentralized autonomous organizations: Concept, model, and applications,» *IEEE Transactions on Computational Social Systems*, vol. 6, n. 5, pp. 870–878, 2019.
- [5] R. Qin, W. Ding, J. Li, S. Guan, G. Wang, Y. Ren e Z. Qu, «Web3-based decentralized autonomous organizations and operations: Architectures, models, and mechanisms,» *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 53, n. 4, pp. 2073–2082, 2022.
- [6] L. Liu, S. Zhou, H. Huang e Z. Zheng, «From technology to society: An overview of blockchain-based DAO,» *IEEE Open Journal of the Computer Society*, vol. 2, pp. 204–215, 2021.
- [7] R. Feichtinger, R. Fritsch, Y. Vonlanthen e R. Wattenhofer, «The hidden shortcomings of (d) aos—an empirical study of on-chain governance,» in *International Conference on Financial Cryptography and Data Security*, Springer, 2023, pp. 165–185.
- [8] A. Wright, «The rise of decentralized autonomous organizations: Opportunities and challenges,» *Stan. J. Blockchain L. & Pol’y*, vol. 4, p. 1, 2020.
- [9] R. Fritsch, M. Müller e R. Wattenhofer, «Analyzing voting power in decentralized governance: Who controls DAOs?» *Blockchain: Research and Applications*, p. 100 208, 2024.

-
- [10] R. Beck, C. Müller-Bloch e J. L. King, «Governance in the blockchain economy: A framework and research agenda,» *Journal of the association for information systems*, vol. 19, n. 10, p. 1, 2018.
- [11] E. Baninemeh, S. Farshidi e S. Jansen, «A decision model for decentralized autonomous organization platform selection: Three industry case studies,» *Blockchain: Research and Applications*, vol. 4, n. 2, p. 100–127, 2023.
- [12] M. Afzal, J. Li, W. Amin, Q. Huang, K. Umer, S. A. Ahmad, F. Ahmad e A. Raza, «Role of blockchain technology in transactive energy market: A review,» *Sustainable Energy Technologies and Assessments*, vol. 53, p. 102–146, 2022.
- [13] C. E. Borges, E. Kapassa, M. Touloupou, J. Legarda Macon e D. Casado-Mansilla, «Blockchain application in P2P energy markets: Social and legal aspects,» *Connection Science*, vol. 34, n. 1, pp. 1066–1088, 2022.
- [14] M. Zade, M. Feroce, A. Guridi, S. D. Lumpp e P. Tzscheutschler, «Evaluating the added value of blockchains to local energy markets—Comparing the performance of blockchain-based and centralised implementations,» *IET Smart Grid*, vol. 5, n. 4, pp. 234–245, 2022.
- [15] M. Mylrea, «Distributed autonomous energy organizations: Next-generation blockchain applications for energy infrastructure,» in *Artificial intelligence for the Internet of everything*, Elsevier, 2019, pp. 217–239.
- [16] N. Dimitri, «Voting in DAOs,» *Distributed Ledger Technologies: Research and Practice*, vol. 2, n. 4, pp. 1–12, 2023.
- [17] Y. Fan, L. Zhang, R. Wang e M. A. Imran, «Insight into voting in DAOs: conceptual analysis and a proposal for evaluation framework,» *IEEE Network*, vol. 38, n. 3, pp. 92–99, 2023.
- [18] D. Sharma, A. Thompson e K. Käsälä, «EnergyDAO-Decentralised Autonomous Organisation for energy community governance,» *EnergyDAO White Paper*, 2023.
- [19] X. Zhao, P. Ai, F. Lai, X. Luo e J. Benitez, «Task management in decentralized autonomous organization,» *Journal of Operations Management*, vol. 68, n. 6-7, pp. 649–674, 2022.
- [20] V. Buterin, «A next-generation smart contract and decentralized application platform,» *Ethereum White Paper*, 2014.
- [21] Anonimo, *An open letter*, Available online, 2016. indirizzo: <https://pastebin.com/CcGUBgDG>.

- [22] N. Diallo, W. Shi, L. Xu et al., «eGov-DAO: A better government using blockchain based decentralized autonomous organization,» in *2018 International Conference on eDemocracy & eGovernment (ICEDEG)*, IEEE, 2018, pp. 166–171.
- [23] M. Zichichi, M. Contu, S. Ferretti e G. D’Angelo, «LikeStarter: a Smart-contract based Social DAO for Crowdfunding,» in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, 2019, pp. 313–318.
- [24] S. Jeong, N.-N. Dao, Y. Lee, C. Lee e S. Cho, «Blockchain based billing system for electric vehicle and charging station,» in *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, IEEE, 2018, pp. 308–310.
- [25] «DeepDAO.» (2024), indirizzo: <https://deepdao.io/organizations>.
- [26] M. Savelyev. «Lifecycle and Structure of a DAO.» (2022), indirizzo: <https://blog.dex.guru/DAO-Structure>.
- [27] «The Vermont Statutes Online.» (2018), indirizzo: <https://legislature.vermont.gov/statutes/section/11/025/04173?ref=internetnative.org>.
- [28] «Wyoming DAO Jurisdictions.» (2023), indirizzo: <https://internetnative.org/wyoming-dao/>.
- [29] «Marshall Island DAO Jurisdictions.» (2023), indirizzo: <https://internetnative.org/marshall-islands-dao/>.
- [30] «Utah Passes Innovative DAO Legislation.» (2023), indirizzo: <https://natlawreview.com/article/utah-passes-innovative-dao-legislation>.
- [31] Q. Ding, W. Xu, Z. Wang e D. K. C. Lee, «Voting schemes in DAO governance,» *Forthcoming in Annual Review of Fintech*, 2023.
- [32] «Maker Governance Voting Portal.» (2024), indirizzo: <https://vote.makerdao.com/>.
- [33] «Swarm City Association.» (2020), indirizzo: <https://press.swarm.city/swarm-city-association-f097c0342e7e>.
- [34] UrbeTalks. «DAO Governance - Off-chain and On-chain proposals,» Youtube. (2023), indirizzo: <https://www.youtube.com/watch?v=jh1-0LvLeZk>.
- [35] Y. Faqir-Rhazoui, J. Arroyo e S. Hassan, «A comparative analysis of the platforms for decentralized autonomous organizations in the Ethereum blockchain,» *Journal of Internet Services and Applications*, vol. 12, pp. 1–20, 2021.

-
- [36] H. Park, I. Ureta e B. Kim, «Developing Dimensions and Indicators to Measure Decentralization in Decentralized Autonomous Organizations,» *Administrative Sciences*, vol. 13, n. 11, p. 241, 2023.
- [37] «DAO-Analyzer.» (2024), indirizzo: <https://dao-analyzer.science/>.
- [38] «Etherscan.» (2024), indirizzo: <https://etherscan.io/>.
- [39] «CoinMarketCap.» (2024), indirizzo: <https://coinmarketcap.com/it/>.
- [40] «IntoTheBlock.» (2024), indirizzo: <https://app.intotheblock.com/>.
- [41] «DAOstack end-of-road update.» (2023), indirizzo: <https://daostack.notion.site/DAOstack-end-of-road-update-and-the-Common-Open-Development-program-announcement-b808c3bf9e3a4b47bd42b7a67da707b4>.
- [42] B. P. Koirala, E. Koliou, J. Friege, R. A. Hakvoort e P. M. Herder, «Energetic communities for community energy: A review of key issues and trends shaping integrated community energy systems,» *Renewable and Sustainable Energy Reviews*, vol. 56, pp. 722–744, 2016.
- [43] R. Gibbons, *A primer in game theory*. Harvester Wheatsheaf New York, 1992.
- [44] R. Feng, S. Che, X. Wang e J. Wan, «An incentive mechanism based on game theory for trust management,» *Security and Communication Networks*, vol. 7, n. 12, pp. 2318–2325, 2014.
- [45] Z. Li e H. Shen, «Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks,» *IEEE Transactions on mobile computing*, vol. 11, n. 8, pp. 1287–1303, 2011.
- [46] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang e D. I. Kim, «A survey on applications of game theory in blockchain,» *arXiv preprint arXiv:1902.10865*, 2019.
- [47] P. Chaidos, A. Kiayias e E. Markakis, «Blockchain participation games,» in *International Conference on Web and Internet Economics*, Springer Nature Switzerland Cham, 2023, pp. 169–187.
- [48] Superdao. «DAO treasury explained | How DAOs store and spend money,» Youtube. (2022), indirizzo: <https://www.youtube.com/watch?v=mzDQi23WbvU>.
- [49] 3. Builders. «DAO TALK #3bis: Treasury Management,» Youtube. (2022), indirizzo: <https://www.youtube.com/live/uzf6-YyvZ5A>.

- [50] «Comunità energetiche rinnovabili - rapporto 2024,» GSE, Legambiente. (2024), indirizzo: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.legambiente.it/wp-content/uploads/2021/11/Comunita-energetice_report_2024.pdf&ved=2ahUKEwiJlZyBxM6HaxUUzQIHHbuEDksQFnoECCIQAQ&usg=A0vVaw2DIYShRvZZcaOUHUSI6F16.
- [51] «Energia e clima in Italia - rapporto periodico,» GSE. (2023), indirizzo: <https://www.gse.it/dati-e-scenari/rapporti>.
- [52] «Renewable energy statistics 2024,» IRENA. (2024), indirizzo: <https://www.irena.org/Publications/2024/Jul/Renewable-energy-statistics-2024>.