Politecnico di Torino

Politecnico di Torino

Corso di Laurea Magistrale
Ingegneria del Cinema e dei Mezzi di Comunicazione
A.a. 2020/2021
Sessione di Laurea Ottobre 2021

Blockchain, NFT e Crypto Art

Stato dell'arte di una nuova tecnologia, approccio e sviluppi

Relatore:
Prof. Riccardo Antonino

Candidato:
Antonello Campo

Blockchain, NFT e Crypto Art

Stato dell'arte di una nuova tecnologia, approccio e sviluppi

1. Introduzione

L'anno di nascita della tecnologia Blockchain può essere fatta convenzionalmente coincidere con la pubblicazione nell'ottobre 2008 dell'articolo "Bitcoin: A Peer to Peer Electronic Cash System", autore Satoshi Nakamoto [1], quasi sicuramente uno pseudonimo di cui non si conosce l'effettiva identità, così come se si tratti di una persona o di un gruppo.

Questo atto di nascita ha in qualche modo indotto a identificare la tecnologia con la sua applicazione alle cripto valute, di cui il BTC, bitcoin, è stato ed è la cripto valuta più importante e diffusa.

Questa innovativa tecnologia si presta invece ad applicazioni nei settori più vari. Per dare un'idea di queste applicazioni, prendendo semplicemente come riferimento tesi di laurea già svolte presso il Politecnico di Torino, si trovano esempi volti all'applicazione della Blockchain alla filiera alimentare [2], all'aerospazio [3] ed all'automobile [4], ovvero i settori tradizionali che caratterizzano la vocazione produttiva del Piemonte. E' giusto anche menzionare il progetto europeo DECODE [5], volto a garantire ed accrescere, attraverso questa nuova tecnologia, la sovranità dei cittadini, che vede la partecipazione del Politecnico, tramite Nexa Center for Internet & Society.

L'intento del presente lavoro è di fare il punto sull'applicazione della tecnologia Blockchain al settore dell'arte, nella modalità intesa come Crypto Art. Provando ad andare oltre il clamore mediatico suscitato dalla recente asta presso Christies's, di un'opera digitale, intitolata "Everydays - The First 5000 Days" di Mike Winkelmann , noto come Beeple, battuta per 69,3 milioni di dollari [6].

L'opera è un collage di 5000 immagini create giorno per giorno, a partire dal 1 maggio 2007, e poi postate su Instagram, che comprende disegni di diversa ispirazione: satira politica, Donald Trump e Hillary Clinton i politici più presenti; personaggi dei cartoni; eventi di risonanza globale, come il tributo al movimento Black Lives Matter dopo la morte di George Floyd [7].

La Blockchain potrebbe aver segnato l'inizio di una rivoluzione nel "mestiere dell'artista", oggetto di considerazioni da parte di esperti di vari settori, che nel presente lavoro è trattato prevalentemente sotto l'aspetto tecnologico. La Crypto Art trova infatti la sua base/possibilità nell'evoluzione della tecnologia delineata da Satoshi Nakamoto nel 2009. Precisamente nel lavoro di Vitalik Buterin "A next generation smart contract & decentralized application platform" [8]. Questo lavoro ha introdotto la piattaforma Ethereum, che gestisce una cripto valuta specifica denominata ETH (ether), ma che si presta anche a gestire oggetti diversi e tra questi le opere d'arte digitali, con riferimento a diritti d'autore, esposizione, tracciamento delle compravendite.

Come per altre tecnologie si è soliti usare dei numeri d'ordine per schematizzare l'evoluzione dello stato dell'arte, così la tecnologia Blockchain, che sta alla base della piattaforma Ethereum e quindi della Crypto Art, viene designata come Blockchain 2.0.

Nel capitolo 2 è illustrata la tecnologia Blockchain di base, evidenziando i maggiori elementi / ingredienti che combinati danno luogo a una realizzazione così complessa.

Nel capitolo 3 è trattata la differenza tra Blockchain 1.0 e Blockchain 2.0.

Il capitolo 4 è dedicato interamente alla Crypto Art, alle sue caratteristiche costitutive, alla sua genesi, affermazione e diffusione.

Le caratteristiche costitutive sono considerate tanto quelle strettamente tecniche quanto quelle prevalentemente attribuibili a un movimento artistico omonimo.

La genesi della Crypto Art è trattata con riferimento a eventi, in buona parte concentrati a inizio 2018, che possono essere assunti come tappe e traguardi fondamentali, sebbene la loro selezione non possa che essere necessariamente soggettiva.

Infine notizie su affermazione e diffusione della Crypto sono fornite in una panoramica di gallerie e artisti, seguendo un ordine di importanza necessariamente stabilito sulla base dei riscontri di mercato registrati.

Il capitolo 5 è dedicato a valutazioni dello stato dell'arte ed ai suoi possibili sviluppi, avendo ben presente la complessità dell'argomento, essendo la Crypto Art intersezione e sovrapposizione di mondi regolati da leggi e storie diverse.

Limitandosi ad un approccio cartesiano riduzionista, sono formulate semplici considerazioni su tre voci: la tecnologia, il mercato, l'artista. Si è poi ritenuto opportuno aggiungere notizie e considerazioni sugli spin-off della Crypto Art. Spin-off intesi come sviluppi secondari e separati dell'applicazione della tecnologia Blockchain al settore dell'arte.

Per ultimo ma non meno importante in termini pratici, in Appendice è riportata una guida alla creazione di un NFT – Crypto Art, che ripercorre l'esperienza diretta acquisita nell'ambito del lavoro di tesi.

2. La tecnologia Blockchain

2.1 Concetto base

Il concetto base della tecnologia Blockchain [9], letteralmente catena di blocchi, è di avere un libro mastro digitale, ovvero un registro contabile nel quale si raccolgono tutti i conti di un dato sistema di transazioni, condiviso tra tutti gli utenti della rete.

L'architettura logica di rete peer-to-peer, ovvero paritaria / paritetica, esclude la gerarchizzazione o centralizzazione delle responsabilità. Ogni nodo / computer connesso alla rete Blockchain ha il compito di convalidare e inoltrare le transazioni ed ha sempre il libro mastro aggiornato.

In altre parole l'essenza della tecnologia è il registro (ledger in inglese) distribuito, Distributed Ledger Technology (DLT), infrastruttura che consente lo sviluppo di applicazioni decentralizzate, senza alcuna autorità centrale che presieda registrazione, condivisione e sincronizzazione delle transazioni [10].

L'illustrazione di fig.2.1, tratta da un documento dell'OCSE [11], Organizzazione per la Cooperazione e lo Sviluppo Economico, rappresenta in modo semplice ed efficace l'infrastruttura tecnologica di base.

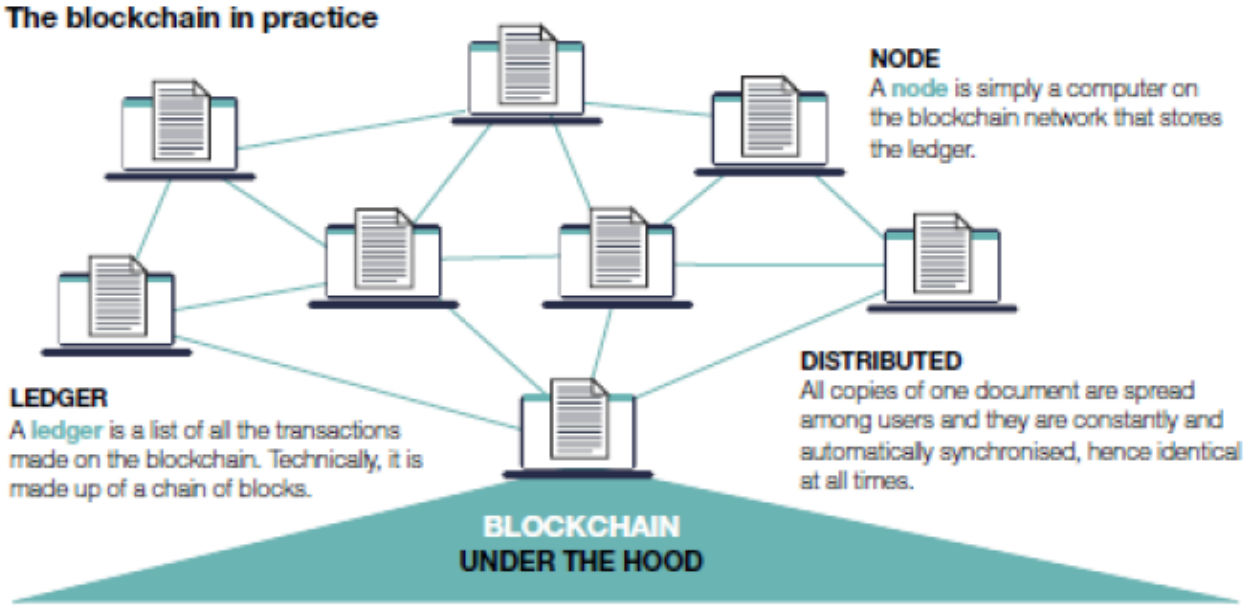


Fig. 2.1, Schematizzazione della Blockchain come DLT [11]

L'ambito di applicazione della tecnologia DLT richiede la distinzione tra "reti permissionless", praticamente reti pubbliche alle quali tutti possono collegarsi liberamente in modo paritario, e "reti permissioned", praticamente reti private sviluppate ad esempio per le aziende, per collegare dipendenti, fornitori e clienti, ma con ruoli e prerogative definite da un'autorità centrale. Nel seguito si farà praticamente esclusivo riferimento a reti pubbliche, ma la crescente applicazione della tecnologia ai settori più svariati ha richiesto questa distinzione.

In un libro mastro contabile su carta, le pagine devono essere necessariamente numerate, in modo che non possano esserci pagine aggiunte e/o pagine strappate; parimenti non deve esserci spazio

nelle pagine per aggiungere transazioni a posteriori. Questi fondamentali requisiti sono garantiti nel DLT della Blockchain, dove il blocco è un insieme di transazioni equivalente ad una pagina del registro cartaceo. Il blocco deve essere opportunamente sigillato affinché non intervengano alterazioni; inoltre blocchi creati in successione cronologica devono essere concatenati in modo che, a posteriori, non possano esserci aggiunte o cancellazioni. La concatenazione è ottenuta dall'accorgimento di riportare in ogni blocco il riferimento che individua il blocco precedente. Per una data piattaforma la catena di blocchi non può essere mai interrotta.

La semplicità del concetto base, racchiuso nell'acronimo DLT e nell'analogia con il vecchio libro mastro contabile, nulla toglie alla complessità della tecnologia che per gli aspetti più salienti sarà accennata nei paragrafi successivi.

2.2 Crittografia

La complessità della tecnologia Blockchain è determinata dal fatto di essere il frutto della coalescenza di tanti sviluppi dell'informatica teorica e applicata. Una componente importante è data dalla crittografia [12].

Schematicamente si può dire che la crittografia simmetrica costituisce una scienza antica, mentre gli sviluppi recenti, legati alla sicurezza informatica, sono riconducibili all'invenzione della crittografia asimmetrica.

La simmetria si verifica nel fatto che la stessa chiave viene utilizzata per criptare e decifrare il messaggio, e la sicurezza basata sul segreto della chiave condiviso solo da chi invia e chi riceve il messaggio. L'esempio più semplice di codifica/decodifica simmetrica può essere dato dal nome del supercomputer HAL, nel famoso film di Stanley Kubrick "2001: Odissea nello spazio".

Infatti è interpretazione diffusa, sebbene non confermata dall'autore, che HAL fosse la semplice riscrittura di IBM, al tempo la più importante azienda produttrice di computer, sostituendo ciascuna lettera con la lettera che nell'alfabeto la precede.

Nell'ambito Blockchain hanno rilevanza fondamentale le funzioni crittografiche di HASH [13], in inglese letteralmente "frittata di carne e patate fatte a pezzettini"

$$y = H(x)$$

caratterizzate dalle seguenti proprietà:

- x è un input digitale di qualsiasi dimensione;
- y è una stringa di dimensione prefissata denominata *digest*
- la funzione non è invertibile, ovvero dato y non può essere calcolato x
- se $x_1 \neq x_2$ ne consegue che $y_1 \neq y_2$, proprietà che viene indicata come resistenza alla collisione
- se $y_1 \neq y_2$ significa che $x_1 \neq x_2$.

Esistono 3 generazioni di funzioni HASH, che vengono indicate come SHA-1, SHA-2 e SHA-3.

SHA è l'acronimo di Secure Hash Algorithm.

Nell'ambito della seconda generazione la funzione più nota ed usata è la HASH-256, così definita perche il suo digest è di 256 bit, corrispondenti a 64 cifre esadecimali.

Nella tabella si riportano esempi di input ed output della funzione SHA-256 [14]. E' possibile osservare come una minima variazione nell'input produce un output completamente diverso, così come l'input può essere di qualsiasi lunghezza e il corrispondente digest è sempre di 64 cifre.

input	***digest***
Antonello Campo	351d3718b19325a7409aac45ad1b34319bd72e8eb06b9a9b6d1e894db35e71a3
AntonelloCampo	94ac9c1a22e06c0a7ec1d69642d0af4d470ef676e0a4b2a6a310f50ee1d27f82
Antonello CAMPO	fe0ef89be522aee2aa6bd84db6952aabe92e2d3a0b3c55d2d0821a16ae90fe8c
It's not time to make a change Just relax, take it easy You're still young, that's your fault There's so much you have to know Find a girl, settle down If you want you can marry Look at me, I am old, but I'm happy	a7c69facc2ef23b0eab5505ccfc6cb06f41c6560a8ca76af931b2002c59b0b41

Nella tabella il terzo esempio di 213 caratteri, spazi inclusi, corrisponde alla prima strofa della canzone di Cat Stevens "Father and Son". L'output sarebbe stato della stessa lunghezza anche se si fosse considerato come input il testo completo o addirittura l'intero repertorio del cantante.

La funzione HASH viene comunemente intesa come l'impronta digitale di un oggetto che ammette una rappresentazione digitale univoca. L'uso massiccio delle funzioni HASH, nella tecnologia Blockchain, oltre a garantire la sicurezza/privacy degli utenti serve ad assicurare l'integrità dei dati e la formazione del consenso della rete.

I digest HASH hanno un ruolo importante nella definizione ed identificazione (anonima) di mittenti e destinatari delle transazioni nella rete Blockchain. Infatti ciascun utente possiede una chiave privata d'accesso ed una chiave pubblica, tale che dalla prima si possa derivare la seconda, ma non viceversa. L'indirizzo dell'utente è ottenuto a partire dalla chiave pubblica, utilizzando delle funzioni di HASH. Nel caso della rete Bitcoin il passaggio è ottenuto applicando alla chiave pubblica prima la funzione SHA-256 e poi la funzione RIPEMD160, ovvero una doppia funzione HASH che fornisce un digest di 160 bit, che per comodità viene codificato con base 58.

Per completezza è opportuno trattare il legame tra chiave privata e chiave pubblica. La chiave privata è un numero k scelto liberamente dall'utente: non mancano consigli e mezzi sul modo di definirlo e custodirlo. Può essere un numero qualsiasi, grande fino a 10^{77}, teoricamente definibile giocando a testa o croce e lanciando la moneta 256 volte.

La chiave pubblica K è derivata ricorrendo alla crittografia a curve ellittiche, in accordo allo standard secp256k1 [15].

Le curve ellittiche sono delle curve di terzo grado (cubiche), analiticamente espresse dall'equazione

$$y^2 = \alpha \cdot x^3 + \beta \cdot x^2 + \gamma \cdot x + \delta$$

che godono di un'importante proprietà schematizzata in fig. 2.2: dati due punti A e B appartenenti ad una curva ellittica, essi determinano una retta che avrà un terzo punto C in comune con la curva; il punto simmetrico a C, rispetto all'asse x, è definibile come la somma A+B, perché è una composizione che gode delle proprietà dell'addizione.

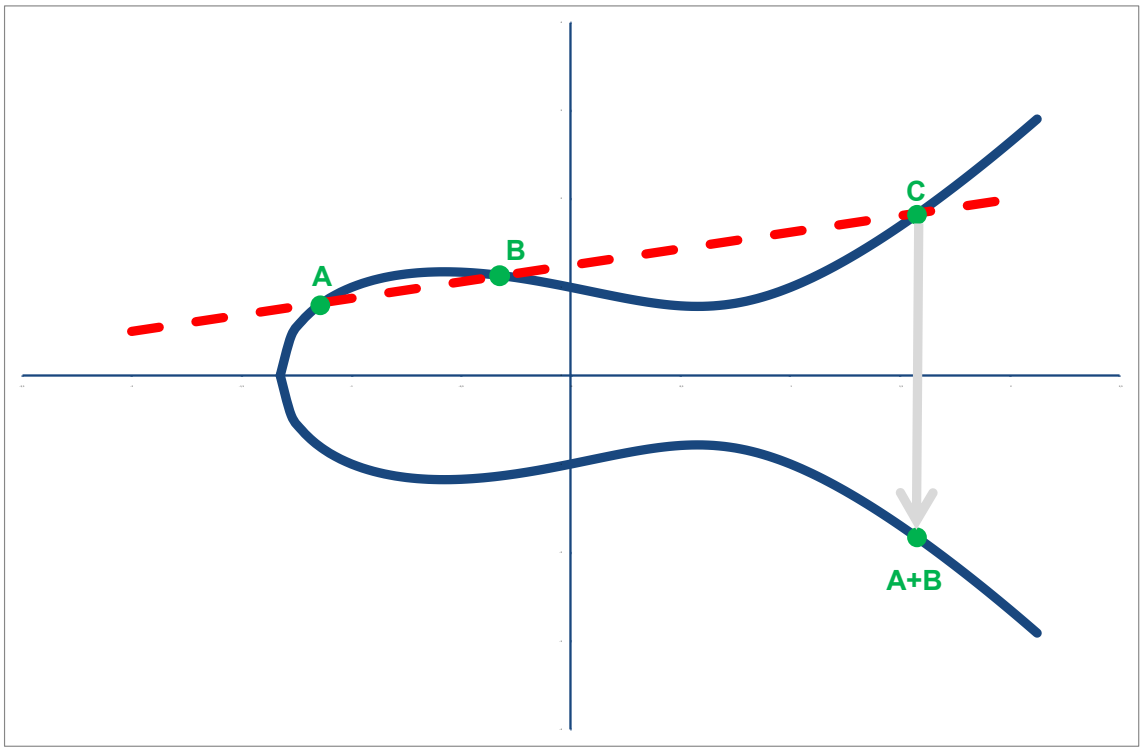


Fig. 2.2, Curva ellittica e composizione/addizione di due punti

Se A e B coincidono, ovvero la retta risulta tangente alla curva, la composizione determina il punto A+A = 2A, un prodotto scalare, che attraverso ripetute composizioni consente di moltiplicare A per un numero intero qualsiasi.

Lo standard secp256k1 adotta l'equazione

$$y^2 = x^3 + 7$$

che ha nel campo dei numeri reali la rappresentazione di fig. 2.3, ma che viene applicata in un campo di numeri finito delimitato dal numero primo 2^{256}-2^{32}-977.

Per dare conto di analogie e differenze tra insieme dei reali e campo finito, in fig. 2.4 è riportata la rappresentazione dell'equazione $y^2 = x^3 + 7$ nel campo finito delimitato da p = 23.

La chiave pubblica K è ottenuta come prodotto scalare di un punto G, definito dallo standard secp256k1, per un fattore uguale alla chiave privata k: K=k•G. L'operazione risulta praticamente a senso unico, perché dato K non è possibile calcolare k, in virtù del fatto che è avvenuta in un campo di numeri finito caratterizzato da un numero primo molto grande.

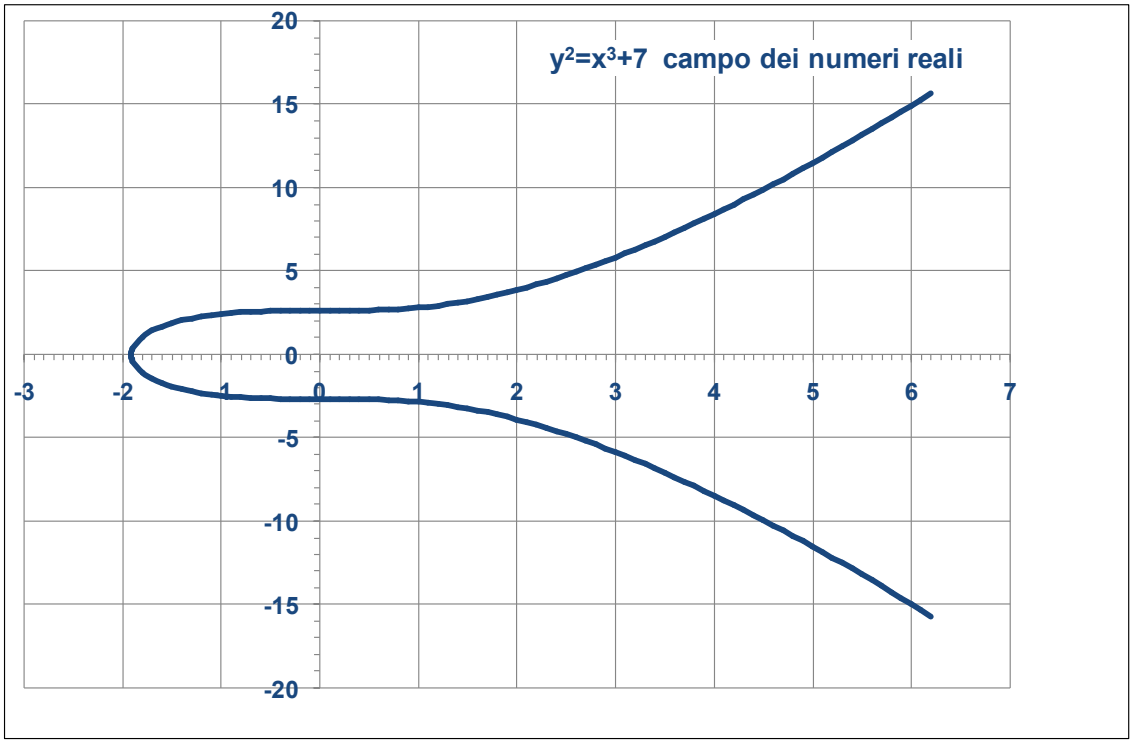


Fig. 2.3, Curva ellittica secp256k1 nel campo dei numeri reali

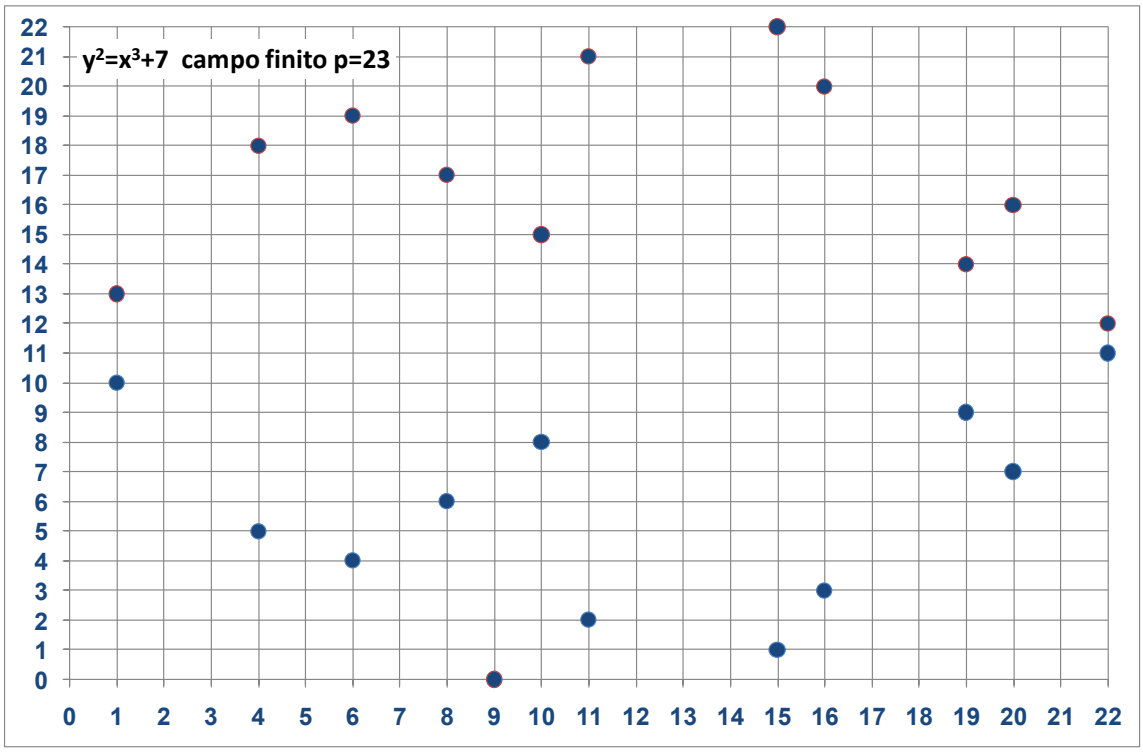


Fig. 2.4, Curva ellittica secp256k1 in un campo di numeri finito

2.3 Contenuto di un blocco

Per semplicità si continua ad assumere come riferimento la prima e più importante delle piattaforme Blockchain, quella della cripto valuta bitcoin lanciata da Satoshi Nakamoto [1].

Ogni blocco può contenere da una a un migliaio di transazioni (TX). Ciascuna TX può muovere una quantità di cripto valuta bitcoin con un minimo 10^{-8} BTC, sottomultiplo che prende il nome di satoshi.

Mittente della valuta e destinatario della stessa sono individuati dai loro indirizzi, codici alfanumerici corrispondenti ai loro rispettivi account (portafogli) e derivati con il metodo presentato nel paragrafo precedente.

La stessa transazione può contenere più input e più output. Gli oggetti in input devono necessariamente corrispondere a oggetti ricevuti e non spesi, con lo stesso numero di BTC/satoshi, ovvero devono essere degli UTXO, acronimo di unspent transaction output. L'unica eccezione è costituita dalla prima transazione di ogni blocco, che riporta la dicitura COINBASE (Newly generated coins), che corrisponde ai BTC di nuovo conio assegnati a chi ha confezionato con successo il blocco.

La somma degli input deve essere maggiore o uguale alla somma degli output più una commissione (fee in inglese), dove la commissione va ragionevolmente commisurata all'estensione in byte della transazione stessa.

Nel caso specifico in cui la taglia degli UTXO spendibili non consenta di mettere assieme una somma di input esattamente uguale alla somma degli output più la commissione voluta, il mittente predispone il movimento del resto a sua favore, con un ulteriore output a beneficio del suo stesso codice alfanumerico.

Poiché nel sistema bitcoin il pagamento di una commissione per transazione è libero ed implicito (differenza tra sommatoria di input e sommatoria di output, senza una voce esplicita), se per errore o dimenticanza il movimento del resto a favore del mittente non viene espresso, il resto viene inteso dal sistema come commissione da accreditare al validatore / minatore del blocco.

Per garantire sicurezza e integrità, all'intero testo della transazione è applicata la funzione SHA-256, pertanto un codice HASH di 64 cifre esadecimale è ad essa associato.

Oltre ai dati di input, output e relativi indirizzi la transazione deve riportare la firma digitale (signature) del mittente, apposta usando la sua chiave privata, senza che quest'ultima sia comunicata ai destinatari, che potranno comunque verificarne l'autenticità disponendo della corrispondente chiave pubblica.

Tutte le transazioni comprese in un blocco, vengono poi associate a due a due, in modo da formare un albero di Merkle, così come mostrato nella figura 2.5 tratta dal paper di Nakamoto [1].

Il contenuto di un blocco in termini di numero di TX dipende principalmente dalla memoria occupata, che deve essere, approssimativamente, di 1MB.

L'HASH associato alle transazioni contenute nel blocco corrisponde alla radice dell'albero di Merkle.

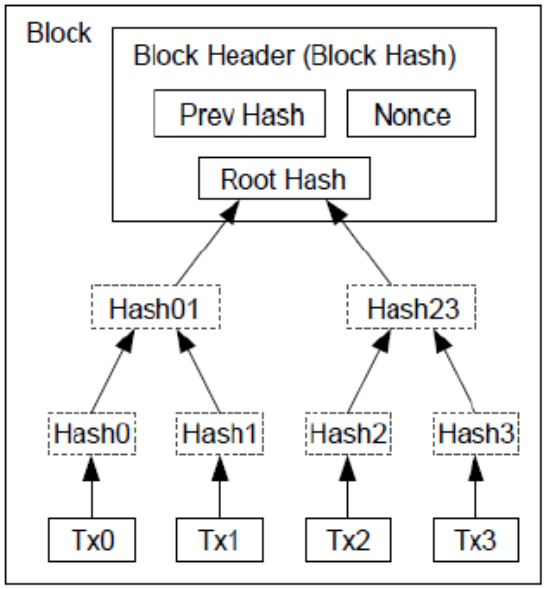


Fig. 2.5, Schematizzazione di un blocco [1]

2.4 Consenso (Proof-of-Work)

La Proof-of-Work ha un ruolo essenziale nella gestione della Blockchain. I nodi della rete con le transazioni ricevute possono comporre un blocco e cimentarsi per chiuderlo, mediante una gara che richiede enormi capacità di calcolo. Infatti la gara consiste nel trovare la funzione di HASH (SHA-256) di un argomento composto da 3 elementi: l'HASH del blocco precedente (y_{n-1}), l'HASH della radice dell'albero di Merkle composto da tutte le transazioni del blocco in esame (x_n), un numero chiamato NONCE, da definire in modo tale che l'HASH risultante soddisfi ad una determinata condizione.

$$y = HASH(y_{n-1}\ \ x_n\ \ nonce) \leq y_0$$

La difficoltà dell'esercizio è funzione inversa del valore dato ad y_0, che prende il nome di target.

In ambito bitcoin la difficoltà ha anche una definizione numerica, data dal rapporto tra il valore y_0 imposto come target da Satoshi Nakamoto nella creazione del primo blocco, inteso da tutti come blocco genesi, ed il target imposto al blocco in esame.

Grado di difficoltà /target è aggiornato ogni 2016 blocchi, con l'obiettivo di ottenere un tempo medio di 10 minuti per trovare la NONCE da associare al blocco.

Il primo nodo/computer che trova la soluzione la comunica alla rete; quando oltre metà della rete l'avrà verificata il blocco viene chiuso e sigillato e si passa all'esame del blocco successivo (fig. 2.6). E' da precisare che i calcoli di verifica sono alquanto semplici.

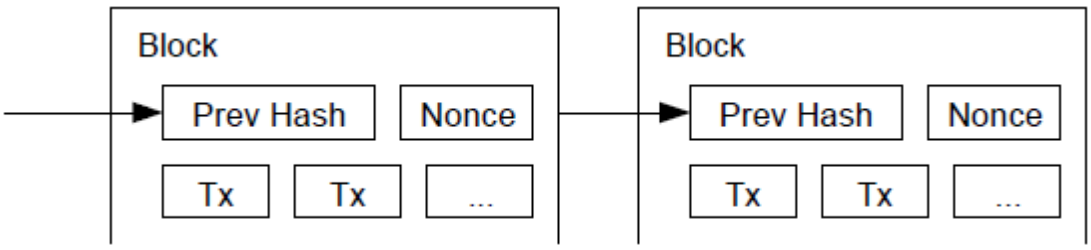


Fig. 2.6, Concatenazione dei blocchi [1]

Questo apparente gioco determina partecipazione, condivisione e controllo di pressoché l'intera rete nella gestione del libro mastro digitale. Per tornare all'analogia del paragrafo 2.1, completata una pagina/blocco del registro, la PoW è la verifica fatta dalla rete prima di voltare pagina ovvero passare ad un nuovo blocco.

Poiché il PoW consente di garantire il corretto funzionamento della Blockchain, la partecipazione dei nodi al PoW è favorita dall'incentivo destinato al primo che trova e mette in rete la soluzione.

Si tratta di un enorme impegno collettivo, che può forse essere inteso meglio riportando come esempio alcuni dati del blocco n° 686800, comprendente 2527 transazioni, chiuso in data 8 giugno 2021.

Dati leggibili sui così detti Blockchain explorer, interfacce web progettate per permettere agli utenti di controllare il funzionamento della Blockchain, come ad esempio Blockchain.com [16], btc.com [17], blockchair.com [18].

HASH 686800 => 00000000000000000001c2a333c5418a3c9b7ccbbcc2c347145df713feccc570
Marca temporale (timestamp) => 2021-06-08 15:25
HASH 686799 => 00000000000000000000ce0d38bd2e839534607d81531f5c94b38d2ad5bfd3b9c
Hash radice Merkle => d06002592450f89fcdefe2fa4e82824872037812dfb320ae22fa6eec35d32d60
TARGET (Bit) => 386752379
Grado di difficoltà => 21047730572452
NONCE => 716674682
Numero nodi => 8500 circa
HASH rate => 150 EH/s
Solutore => SlushPool
Tempo impiegato => 16 minuti
Compenso per SlushPool => 6,25 + 0,74016073 BCT

Occasionalmente in una rete pubblica come Bitcoin può capitare che il tempo di latenza della rete provochi dei conflitti, ad esempio che due nodi propongano due blocchi contenenti insiemi di transizioni non coincidenti al 100%. Questo anche in virtù del fatto che esiste una "mempool" di transazioni in attesa di essere processate, tanto che i minatori hanno discrezionalità nella selezione delle transazioni da includere nel blocco, privilegiando ovviamente le transazioni che pagano le commissioni più alte.

Se al blocco n -1 seguono due diversi blocchi n_A ed n_B, il dilemma su quale debba essere considerato blocco legittimo si risolve in modo pressoché spontaneo. La biforcazione determinerebbe due catene, due rami ai quali agganciare i blocchi successivi. La regola da seguire è semplice: il ramo legittimo è quello che diventa più lungo.

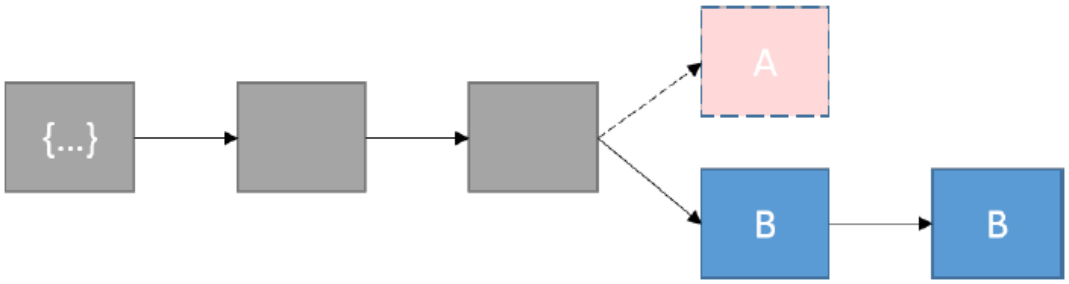


Fig. 2.7, Esempio di biforcazione di una Blockchain

Nell'esempio riportato in figura 2.7 la catena deve prosegue con il ramo B ed il blocco della catena A va eliminato.

2.5 La metafora della miniera

Nell'esempio precedente sono circa 8500 i nodi della rete che hanno lavorato in competizione per comporre il blocco numero 686800 e trovare sulla base di notevoli calcoli il così detto NONCE del blocco.

Considerata la potenza di calcolo della rete ed il tempo trascorso si può dedurre che per trovare la soluzione la funzione HASH è stata calcolata oltre 10^{23} volte. In media i calcoli effettuati da ciascun nodo sono stati circa 10^{19}.

Questo lavoro è denominato con gergo specialistico mining [19], ovvero come il lavoro di estrazione da una miniera, denominazione che nasce da una doppia analogia.

L'analogia più appropriata è che i minatori cercano, ed uno di essi lo troverà, il numero NONCE che soddisfa il requisito e che consentirà, con la condivisione degli altri minatori/nodi, di validare e sigillare il blocco.

L'altra analogia, meno appropriata ma suggestiva perché richiama la febbre dell'oro in America nell'ottocento, nasce dal fatto che il minatore che trova la soluzione si aggiudica un premio che nel caso del blocco assunto come esempio è di 6,99016073 BTC, corrispondente a ben 228553 dollari USA (8 Giugno 2021)

Ricompensa significativa se si pensa al fatto che trattasi di una ricerca che nel caso specifico è durata 16 minuti, ma che mediamente è prevista durare solo 10 minuti. Questo incentivo induce molti a entrare nella rete Bitcoin ed a organizzarsi/attrezzarsi adeguatamente per risultare competitivi.

Per accrescere la velocità di calcolo oltre che alle CPU (Central Processing Unit) ci si affida alla potenza di elaborazione delle schede grafiche, le GPU (Graphics Processing Unit). L'algoritimo HASH-265 può essere ancora più velocemente calcolato tramite dispositivi ASIC (Application Specific Integrated Circuits), appositamente creati per il mining.

Inoltre molti "minatori" aderiscono a consorzi (pool) e/o dipendono da consorzi, attualmente i più importanti, con un HASH rate complessivo di circa il 50% del totale, sono nell'ordine F2 Pool, Ant Pool, Poolin, Via BTC, seguono con circa il 25% BTC com, Binance, HUOBI, BTC Pool, Slush Pool [dati desunti dai riferimenti 15,16,17 e 18].

Tornando al premio c'è da riferire un altro aspetto importante dell'architettura definita da Satoshi Nakamoto. La parte più consistente del premio (6,25 BTC) non deriva dal pagamento del servizio di trasferimento delle cripto monete richiesto dai clienti, bensì è moneta fresca coniata per ogni blocco che si chiude, ovvero "newly generated coins", come riportato nel paragrafo 2.3.

Tenendo conto della crescente potenza di calcolo dei computer, Nakamoto ha previsto che questo premio si dimezzasse ogni 4 anni circa, a partire da un premio iniziale di 50 BTC. Più precisamente il dimezzamento è previsto dopo il concatenamento di 210000 blocchi. Questa è la sequenza dei dimezzamenti già applicati [20]: il primo è avvenuto il 28 novembre 2012 (da 50 a 25 BTC), il secondo il 9 luglio 2016 (da 25 a 12,5 BTC), il terzo l'11 maggio 2020 (da 12,5 a 6,25 BTC). Questo consente di calcolare facilmente che con l'erogazione del premio riservato al minatore del blocco numero 686800 del paragrafo precedente, il totale dei bitcoin creati ammonta a 18730 milioni di BTC.

Poiché la progressione dei BTC emessi può essere espressa come sommatoria di una serie geometrica

$$\sum_{1}^{\infty} \left(\frac{1}{2}\right)^{n} = 1$$

ne consegue che il limite è dato da

$$2 \cdot 210000 \cdot 50 = 21000000\ BTC$$

Limite asintotico che di fatto potrà essere considerato approssimativamente raggiunto nell'anno 2140.

3 Tecnologia Blockchain 2.0

3.1 Ethereum

Quanto illustrato nel capitolo precedente, con particolare riferimento alla rete Bitcoin, può essere catalogato come Blockchain 1.0. In essa le transazioni possibili di criptovaluta sono movimenti da un indirizzo (account /wallet) a un altro detto-fatto, ovvero sono ordini esecutivi.

Si deve a Nick Szabo l'introduzione del concetto di smart contract (contratto intelligente), come transazioni che avvengono se e quando sono verificate determinate condizioni, che nella logica di programmazione possano esprimersi con istruzioni del tipo IF, WHEN, THEN, ELSE, … [21].

In sostanza si tratta di un programma/software che esegue obbligazioni contrattuali, al verificarsi di eventi predefiniti ed eventualmente incorporare rimedi nel caso gli eventi non si verifichino.

La Blockchain Ethereum, sviluppata principalmente da Vitalik Buterin nel 2014 [8], è in grado di eseguire smart contract, pertanto viene solitamente indicata come tecnologia Blockchain 2.0.

Prima di approfondire ulteriormente i vantaggi della tecnologia 2.0, rispetto al livello precedente, conviene riportare i dati salienti sul funzionamento di Ethereum relativamente a creazione e scambio di cripto moneta. Per semplicità è riportato il confronto con il sistema Bitcoin.

	ETHEREUM	*BITCOIN*
Fondatore	Vitalik Buterin	Satoshi Nakamoto
Cripto valuta	ETH ether	BTC
Sottomultiplo	Gwei	satoshi
Rapporto valuta sottomultiplo	1E+09	1E+08
Dimensione Blocco	50 kB	1 MB
Codice	Solidity et al,	Script
Tipo di codice	Turing equivalente	non Turing
Transazioni per blocco	~ 100	~ 1000
Data blocco genesi (1°blocco)	30/07/2015	03/01/2009
N° blocchi (11/07/2021)	12807900	690600
Circolante (11/07/2021)	*116,7 milioni ETH*	18,8 milioni BTC
Circolante limite	*N/A*	21 milioni BTC
PoW, funzione HASH	ETHASH	SHA-256
H/W mining	→ GPU	→ ASIC
Tempo tra due blocchi	14 sec	10 minuti
*Compenso iniziale per blocco**	3 ETH	50 BTC
*Compenso attuale**	2 ETH	6,25 BTC
Commissione per transazione	obbligatoria	base volontaria

* premio non comprensivo delle commissioni

Il confronto tra i due sistemi si presta ad alcune immediate considerazioni: le transazioni di Ehereum hanno mediamente dimensione di memoria inferiore e vengono elaborate più velocemente. E' comunque indispensabile precisare che le transazioni in Ethereum non avvengono unicamente da un portafoglio EOA (acronimo di externally owned account) a un altro, usando i rispettivi indirizzi derivati dalla chiave pubblica. La creazione di uno smart contract determina

l'assegnazione di un indirizzo CA (contract accounts) al contratto stesso, non derivato dalle chiavi del portafoglio che lo ha generato. Le transazioni possibili sono quindi da EOA a EOA, ma anche da EOA a CA e viceversa. In ogni caso deve essere una transazione da EOA che innesca una transazione da CA, così come deve essere una transazione da EOA a creare uno smart contract.

In Ethereum le transazioni che hanno ber oggetto una valuta non sono basate sugli UTXO (unspent transaction output) bensì sul saldo del conto di provenienza, questo conferisce importanza al numero d'ordine di emissione della transazione da EOA (denominato nonce) che evita duplicazioni e determina l'ordine di esecuzione della transazione. Qualora nella sequenza di nonce ci fosse una discontinuità, le transazioni successive alla discontinuità non verrebbero eseguite fino a quando i numeri ordinali mancanti non venissero utilizzati.

Ethereum usa una funzione HASH denominata Keccak-256, che può essere considerata del tipo SHA-3, sebbene questa classificazione non è del tutto conforme a quanto formalmente pubblicato dal NIST, National Institute of Standards and Technology degli Stati Uniti [13].

Per dare una panoramica completa delle due cripto valute, le fig. 3.1 e 3.2 riportano le loro rispettive serie storiche rapportate al dollaro USA.
C'è da osservare che sono le due cripto valute più importanti, perché dopo la creazione del bitcoin c'è stata una proliferazione di nuove valute ed attualmente il loro numero complessivo è dell'ordine delle migliaia.

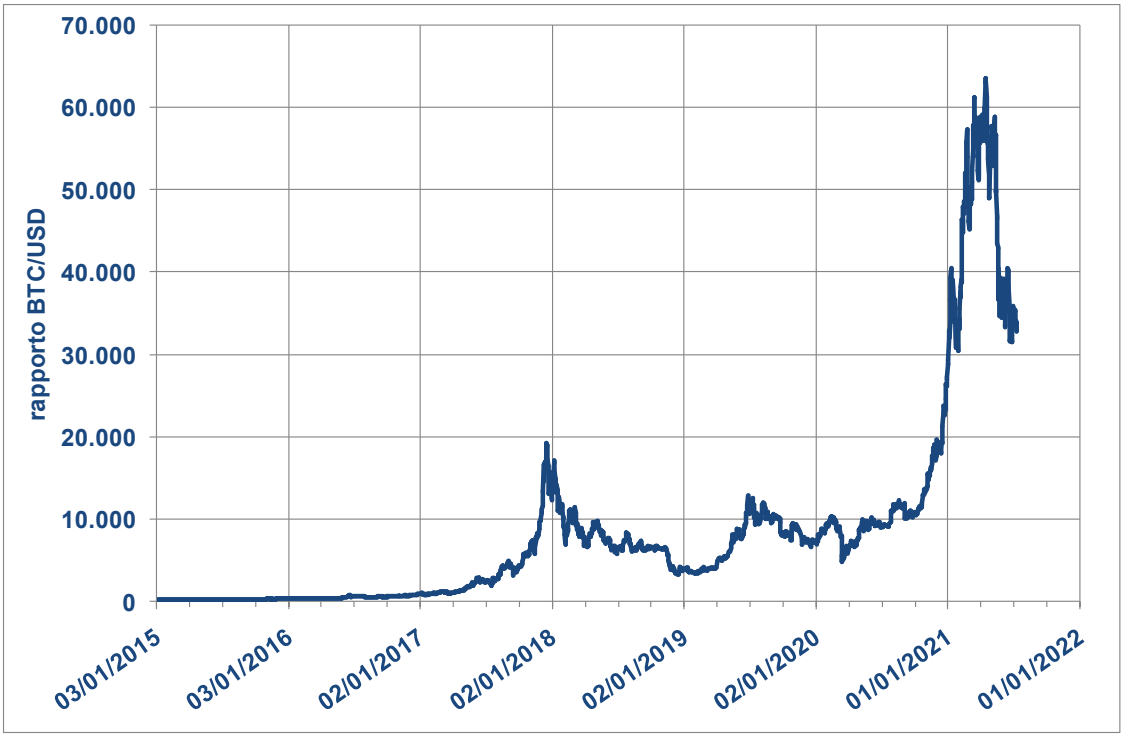


Fig. 3.1, Cambio bitcoin (BTC) dollaro USA

Fig. 3.2, Cambio ether (ETH) dollaro USA

3.2 EVM

Alla base della visione dei fondatori di Ethereum non c'era una Blockchain con una criptovaluta alternativa al bitcoin, c'era bensì una sorta di computer globale [21,22,23].

Un'infrastruttura decentralizzata, open source, in grado di eseguire programmi indicati come smart contract, dove la Blockchain servisse per sincronizzare e memorizzare i cambiamenti di stato del sistema. La principale ragion d'essere della cripto valuta, l'ether, era semplicemente legata a regolare l'uso dell'infrastruttura condiviso.

Il nome dato all'infrastruttura così realizzata è EVM, acronimo di Ethereum Virtual Machine. L'accresciuta potenzialità della Blockchain dalla prima alla seconda generazione è riconducibile all'EVM: cosi la creazione di programmi intelligenti e la loro esecuzione. L'EVM è un grande computer distribuito su tutta la rete, dove codici e dati di ogni singolo contratto, indicati rispettivamente come codici e variabili di stato, sono condivisi da tutti i nodi . Per raggiungere questo obiettivo, i contratti intelligenti non possono di regola operare su dati al di fuori del loro contesto. In caso contrario bisogna individuare un "oracle", ovvero una fonte esterna di autorità indiscussa dalla quale attingere i dati aggiuntivi.

Si spiega con l'azione dell'EVM la più elementare differenza tra Bitcoin ed Ethereum. Mentre in Bitcoin le transazioni si basano sulle precedenti UTXO, ovvero transazioni ricevute e non ancora spese, più o meno come partire da un estratto conto per effettuare un nuovo pagamento, nel caso di Ethereum il sistema parte dal saldo dell'estratto conto. Di conseguenza, come schematizzato nella fig. 3.3, la validazione di un nuovo blocco Ethereum determina l'aggiornamento di tutte le variabili di stato e tra questi il saldo di tutti gli *account.*

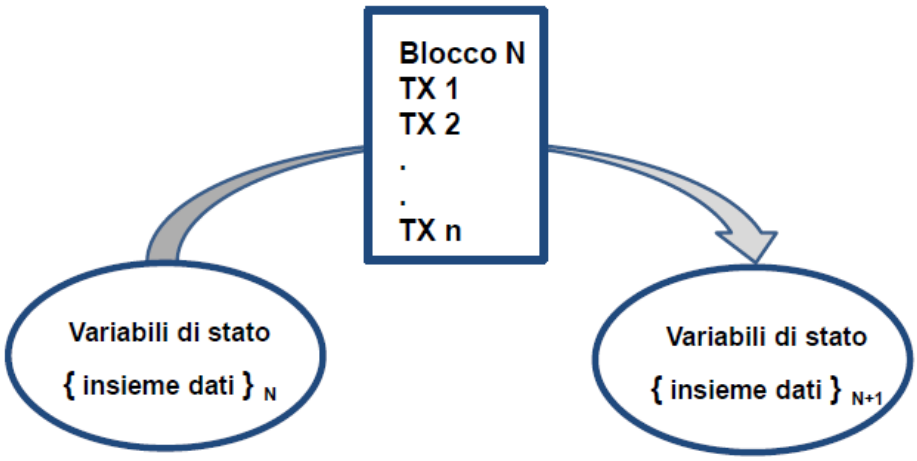


Fig. 3.3, Azione dell'EVM in conseguenza di un nuovo blocco

L'ultima ma non meno importante delle differenze salienti tra Ethereum e Bitcoin è facilmente osservabile usando ad esempio uno degli explorer elencati in bibliografia [16,17,18]. Le transazioni in Bitcoin sono sempre trasferimenti di valuta da un conto all'altro, con relativo valore in BTC; molte delle transazioni in Ethereum non hanno per oggetto trasferimenti di valuta, questo perché evidentemente la transazione è regolata da uno smart contract che non prevede trasferimenti di ETH oppure, in alternativa, i pagamenti in ETH sono differiti, condizionati da variabili / eventi dipendenti dal tempo. In questo caso la transazione veicola dati e non criptovaluta.

In ogni caso per comunicare con la Blockchain l'utente deve disporre di un'interfaccia denominata wallet, parola inglese che significa portafoglio, che pertanto si presta a più significati pur nell'ambito ristretto della tecnologia Blockchain. Infatti il wallet è un'applicazione, che non contiene cripto valute e/o smart contract, dati che risiedono nella Blockchain, bensì è un mezzo che consente di gestire il proprio account ed effettuare transazioni.

Gli unici dati effettivamente contenuti nel wallet sono le chiavi di accesso alla Blockchain. Nel caso di Ethereum il wallet più consigliato o richiesto, è Metamask. Esso è un'estensione di browser diffusi come Chrome e Firefox, liberamente scaricabile dal sito https://metamask.io [22].

3.3 Gas

Le commissioni sulla Blockchain Ethereum sono pagate in Ether, ma sono definite in un'unità specifica chiamata gas che misura l'impegno di tutto il sistema (EVM) nell'esecuzione della transazione [22].

Ogni smart contract è un programma con un certo numero di istruzioni /operazioni, a ciascuna di esse corrisponde una quantità di gas come riportato nel Libro Giallo [23].

All'utente è richiesto per ogni transazione/smart contract di prevedere una quantità di gas, che deve essere maggiore o uguale a quella che poi effettivamente sarà consumata. La doppia stima, gas preventivato e gas consumato, serve a proteggere il sistema da attacchi informatici, infatti l'esecuzione di qualsiasi programma si arresta una volta che il gas consumato raggiunge la quantità di gas prevista dall'utente.

Questa vulnerabilità deriva dal fatto che il codice di programmazione dell'EVM è Turing equivalente, altrimenti detto Turing completo, che ha il pregio di eseguire qualsiasi programma, ma anche il rischio che esegua istruzioni che intenzionalmente o accidentalmente provochino un loop infinito. L'esaurimento del gas preventivato arresta l'esecuzione e riporta tutte le variabili di stato ai valori precedenti alla transazione interrotta.

L'utente deve inoltre fissare, regolandosi sulla quantità di transazioni in attesa e sull'importanza/urgenza della propria transazione, il prezzo in Ether disposto a pagare per ogni unità di gas. Questa scelta determina la priorità che viene attribuita alle singole transazioni nella composizione di un nuovo blocco. Poiché i nodi / minatori lavorano con l'intento di massimizzare il loro guadagno, scelte eccessivamente economiche comportano il rischio che la transazione resti ferma per lungo tempo nella Mempool, viceversa una scelta onerosa serve ad ottenere la precedenza alla propria transazione.

La scelta del termine gas è dovuta all'analogia con il carburante necessario per compiere un determinato percorso in auto. Tipo e lunghezza del percorso che si intende fare consentono una previsione della quantità necessaria di carburante, prima della partenza il rifornimento deve essere adeguato alla previsione. Un rifornimento insufficiente comporterebbe il mancato raggiungimento della meta, mentre un rifornimento sovrabbondante comporterebbe solo un residuo di carburante nel serbatoio.

Nel caso di Ethereum una stima eccessiva del gas necessario non comporta nessun inconveniente per l'utente, in quanto si paga il gas effettivamente consumato.

Il prezzo unitario del gas è espresso nel sottomultipli dell'ether chiamato gwei.

1gwei = 10^{-9} ether.

In un'istantanea relativa al giorno 12 luglio 2021 risultavano i seguenti dati statistici [24]:

- veloce (30 secondi) => 37 gwei
- media (3 minuti e 30 secondi) => 28 gwei
- lenta ($\geq$ 16 minuti) => 23 gwei.

Poiché un trasferimento standard di valuta ETH richiede una quantità limite di gas pari a 21000 unità, e considerato inoltre che il cambio cripto valuta / USD risulta nello stesso istante pari 2101 USD, un pagamento effettuato tramite cripto valuta ha un costo di commissione pari a poco più di un dollaro. Costo del tutto analogo a quello di un bonifico bancario, bisogna però non trascurare la dinamicità del sistema, che può comportare in certe situazioni commissioni più alte, anche oltre un ordine di grandezza, a meno di non attendere tempi molto lunghi.

3.4 Token, fungibili e non fungibili [25]

La parola inglese token ha lo stesso significato delle parole italiane gettone o buono, quest'ultima ovviamente come sostantivo.

Le criptovalute BTC e ETH possono essere classificate come token digitali. Si può anche dire che sono token nativi, perché legati alle funzionalità di base dei rispettivi sistemi Bitcoin ed Ethereum.

La tecnologia Blockchain 2.0 consente di creare/gestire ulteriori token come schematizzato nella stratificazione di fig. 3.4, ad esempio biglietti di ingresso per un dato evento, buoni pasto, miglia premio. Questi token pertanto esistono e sono gestiti all'interno di un contratto (smart contract) come una base dati indipendente, con una gestione distinta rispetto ai token nativi.

1	livello smart Blockchain	token
2	livello base Blockchain	consenso / registrazione
3	livello rete	collegamento peer-to-peer
4	livello fisico	utenti / computer / nodi

Fig. 3.4, Stratificazione della Blockchain 2.0

In ambiente Ethereum vengono generalmente designati come token ERC-20 quelli creati sulla base dello standard omonimo [8].

Una proprietà distintiva dei token nativi e dei token ERC-20 è la loro fungibilità, ovvero l'intercambiabilità, la capacità di sostituzione reciproca.

Si possono creare anche "non fungible token" ed a questa possibilità deve la sua nascita la Crypto Art. In termini informatici si può provare a dare la seguente definizione.

Un token non fungibile è un insieme di dati assegnato in modo univoco a un indirizzo Blockchain, con gestione del ciclo di vita programmabile. Il token costituisce una risorsa digitale unica. Può essere messo in circolazione e trasferito solo riassegnando l'account del proprietario. La Blockchain assicura che i token non fungibili non possano essere duplicati. Gli oggetti token possono essere accompagnati da metadati off-chain, la cui integrità può essere verificata tramite hash crittografici on-chain.

ERC-721 è uno standard Ethereum che consente di implementare un API (application programming interface) per NFT, quindi creare un NFT [8].

Dopo ERC-20 e ERC-721, Ethereum ha ideato e sviluppato il nuovo standard ERC-1155, che consente di creare un'interfaccia di contratto intelligente in grado di rappresentare e controllare tanto token fungibili quanto token non fungibili.

ERC è l'acronimo di Ethereum Request for Comments, un documento con il quale ha inizio un processo di miglioramento che si conclude formalmente con un EIP (Ethereum Improvement Proposal), che consente di usare il sistema nel modo più efficiente e sicuro. Non si tratta di prescrizioni, bensì di linee guida.

Lo standard ERC-20, introdotto dopo pochi mesi dal blocco genesi di Ethereum, consente di creare e gestire in modo ottimale token fungibili diversi dall'ETH. Lo smart contract comprende sei funzioni fondamentali e tre funzioni opzionali:

- *totalSupply* (quantità totale di token immessi nel sistema)
- *balanceOf* (saldo dei token di uno specifico indirizzo)
- *transfer* (invio di token)
- *transferFrom* (prelievo di token)
- *approve* (autorizzazione al prelievo)
- *allowance* (limite imposto al prelievo)
- *name* (nome del token creato, opzionale)
- *symbol* (simbolo del token creato, opzionale)
- *decimal* (la più piccola quantità trasferibile, opzionale).

Lo standard ERC-721, che crea e gestisce token non fungibili (NFT), alle funzioni relative allo standard ERC-20 aggiunge altre funzioni. Queste funzioni aggiuntive servono a definire l'unicità del token e definire/gestire il titolo di proprietà. Esse sono:

- *tokenMetadata* (identifica l'indirizzo URL, uniform resource locator, dell'oggetto digitale sottostante al titolo di proprietà dell'NFT)
- *ownerOf* (fornisce l'indirizzo proprietario di un determinato NFT)
- *takeOwnership* (trasferisce la proprietà di un NFT)
- *takeOwnershipByIndex* (è utilizzato nel caso di NFT con numero di edizioni ≠1, per tracciare le singole edizioni).

Può essere opportuno evidenziare come, nel caso di un'opera d'arte digitale, la creazione di un NFT per gestire il titolo di proprietà mediante Blockchain non significa che l'opera risieda nella Blockchain. La gestione è fatta con riferimento a metadata corrispondenti all'archiviazione del file, che generalmente avviene ricorrendo al protocollo IPFS (InterPlanetary File System) per l'archiviazione e la condivisione di dati in un sistema distribuito peer-to-peer.

3.5 Il prezzo del consenso

La gestione non centralizzata del registro / libro mastro di Bitcoin ed Ethereum, cosi come di altri sistemi analoghi, richiede la formazione del consenso attraverso l'attività di *mining* / *proof-of-work.*

Attività incentivata con un premio al nodo che per primo trova la soluzione che permette di chiudere / sigillare il blocco. L'attrazione data dall'incentivo ha determinato una crescita enorme della potenza di calcolo impegnata dalla rete, che ha richiesto inevitabilmente un aumento della potenza elettrica di alimentazione.

Alex de Vries ha creato nel 2014 la piattaforma Digiconomist [26] che prova a evidenziare le conseguenze non volute delle innovazioni digitali. Nel caso specifico i consumi annuali di Bitcoin ed Ethereum sono rispettivamente dell'ordine di 128 e 50 TWh, ovvero considerando entrambe 178 TWh.

Per avere un'idea della rilevanza di questo dato basta qualche confronto con le statistiche di Terna [28] nell'anno 2019, prima della pandemia da Covid-19:

- il consumo della piattaforma Bitcoin è pressoche uguale all'energia assorbita in Italia dell'intero settore industriale: 128,94 TWh;
- il dato di Bitcoin più Ethereum è leggermente superiore al consumo di energia, nel 2019, delle regioni settentrionali: Piemonte, Valle d'Aosta, Lombardia, Trentino alto Adige, Veneto, Friuli Venezia Giulia, Liguria, Emilia Romagna: 173,404 TWh;
- assumendo come metro di paragone il consumo complessivo della città metropolitana di Torino (agricoltura, industria, servizi, abitazioni), esso risulta soltanto 1/18 del consumo attribuibile a Bitcoin e Etheurum.

Come risposta al problema dell'enorme quantitativo di energia richiesto, le società di mining hanno localizzato le loro apparecchiature in regioni del mondo dove il costo dell'energia è relativamente basso.

Il sito web Cambridge Bitcoin Electricity Consumption Index [27] , dell'Università di Cambridge, fornisce la suddivisione della potenza di HASH rate nelle varie regioni del mondo, suddivisione che bene evidenzia la ricerca delle regioni con i costi più bassi dell'elettricità.

Paese	*% capacità mining bitcoin*
Cina	65,08
Stati Uniti	7,24
Russia	6,9
Kazakistan	6,17
Malaysia	4,33
Iran	3,82
Canada	0,82
Germania	0,56
Norvegia	0,48
Venezuela	0,42

E' forse opportuno precisare in questo paragrafo le differenze tra Bitcoin ed Ethereum, indicate nella tabella del paragrafo 3.1 relativamente a Proof-of-Work e hardware impiegato per il mining. Il metodo PoW di Ethereum, denominato Ethash, anche se in essenza analogo al metodo illustrato nel paragrafo 2.4, è volutamente più complicato del metodo PoW di Bitcoin. La complicazione è unicamente mirata a rendere impossibile l'utilizzo di dispositivi ASIC (Application Specific Integrated Circuits), pertanto a evitare l'eccessiva concentrazione dell'attività di mining in pochi gruppi.

Una risposta al problema dell'enorme consumo di energia è sta annunciata da Ethereum. Essa prevede l'abbandono del metodo proof-of-work a favore del metodo proof-of-stake (PoS), la sua implementazione in rete sarà possibile alla conclusione della sperimentazione in corso [21].

Con il nuovo metodo cesserebbe la gara tra i nodi / minatori per aggiudicarsi il premio, trovando per primi il numero NONCE che soddisfa il target per l'hash del blocco da chiudere.

Il prof-of-stake prevede che i nodi con più dote, in termini di cripto valuta, possano candidarsi ad essere i validatori di nuovi blocchi. La scelta avverrebbe con estrazione a sorte per ogni blocco, parte della dote del nodo validatore fungerebbe da garanzia in caso di errori, fermo restando l'erogazione del premio previa conferma della maggioranza dei nodi restanti.

La sperimentazione per la transizione di Ethereum da PoW a PoS ha avuto inizio il primo dicembre 2020, con un gruppo iniziale di 16384 validatori che hanno depositato ciascuno una cauzione, per un ammontare complessivo di 524288 ETH.

Il programma di sperimentazione è articolato in 4 fasi, include anche obiettivi aggiuntivi e/o complementari al PoS, quali la suddivisione (sharding) della rete ed il passaggio da EVM a EWASM (acronimo di Ethereum Web Assembly Machine).

E' stato già suggerito il nome da dare all'attività di validazione basato sul proof-of-stake: sempre attingendo dalla metallurgia, il suggerimento è di chiamare i validatori forgiatori. Quindi non più la metafora della produzione di monete a partire dall'estrazione del metallo in miniera, ma limitarsi all'ultima fase, quella di coniare/forgiare le monete.

4 Crypto Art

4.1 Definizione tecnica

Crypto Art o arte crittografica può essere semplicemente definita come un'opera d'arte per la quale una Blockchain contiene il corrispondente token, un NFT (non fungible token) che costituisce titolo di proprietà dell'opera, che consente di tracciarne tutti i passaggi e di garantirne l'autenticità [29].

L'aggettivo crittografico è quindi riferito al tipo di registrazione, ovvero alla crittografia usata nelle transazioni Blockchain e non assolutamente a materiali e/o processi /metodi usati nella realizzazione dell'opera.

E' solitamente un'opera digitale, ma non necessariamente digitale, perché in ogni caso la Blockchain non contiene il file dell'opera bensì la sua impronta digitale, ovvero i metadata del file prodotto dall'artista.

Assumendo come esempio il famoso collage di Beeple, "the first 5000 days", venduto per 69 milioni di dollari da Christie's, l'asta era stata così annunciata [30]:

Beeple (b. 1981)
EVERYDAYS: THE FIRST 5000 DAYS
token ID: 40913
wallet address: 0xc6b0562605D35eE710138402B878ffe6F2E23807
smart contract address: 0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756
non-fungible token (jpg)
21,069 x 21,069 pixels (319,168,313 bytes)
Minted on 16 February 2021. This work is unique.

Il file dell'opera, un jpg di 319 Mbyte, non risiede nella Blockchain, bensì il suo NFT, avente numero identificativo 40913, creato (minted / coniato) dall'indirizzo

0xc6b0562605D35eE710138402B878ffe6F2E23807,

sulla base delle regole dello smart contract

0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756.

Attraverso il codice pubblico del portafoglio è possibile vedere tutte le transazioni effettuate e tra queste la creazione (mint, ovvero conio) del token, identificata dall'hash

0x84760768c527794ede901f97973385bfc1bf2e297f7ed16f523f75412ae772b3.

L'oggetto dell'asta di Christie's è pertanto quanto creato da Beeple, definito dalle seguenti informazioni [31]:

creator : 0xc6b0562605d35ee710138402b878ffe6f2e23807

metadataPath : QmPAg1mjxcEQPPtqsLoEcauVedaeMH81WXDPvPx3VC5zUz

Dove il codice metadata consente di risalire al file dell'opera, mediante il protocollo IPFS (InterPlanetary File System) usato per l'archiviazione dei dati [32].

Schematizzando, gli step compiuti da Beeple precedenti l'asta da Christie's sono stati:

a) la creazione del collage digitale con i 5000 disegni
b) caricamento su IFPS e derivazione di metadata
c) il conio di un NFT su Ethereum che riporta i metadata.

E' da sottolineare che nella Blockchain non risiede l'opera digitale, bensì il suo digest o impronta digitale ottenuto con la funzione HASH-256.

Un'opera non digitale pertanto può essere oggetto di registrazione su Blockchain, basta creare/riconoscere un documento digitale legato bi-univocamente all'oggetto fisico da sottoporre ad HASH.

In sintesi, il primo passo di un'artista digitale per proporre in ambito Crypto Art una sua creazione artistica è il download e l'installazione di IPFS (fig.4.1), seguendo le istruzioni date per il proprio sistema operativo. Istallato IFPS si procede all'archiviazione del file che si intende lanciare sul mercato.

Il secondo passo è la disponibilità di un wallet che consenta di interfacciarsi con la Blockchain. Per Ethereum il wallet più raccomandato o prescritto è Metamask [33].

La disponibilità di Metamask (fig.4.2). è anche una pre-condizione per chi volesse acquistare Crypto Art. Dopo il download e l'installazione di Metamak, artisti e collezionisti devono entrambi registrarsi su una o più delle gallerie esistenti, dove ovviamente i collezionisti sono sempre i benvenuti mentre gli artisti devono esibire le loro referenze per essere accettati.

Infine non è da trascurare il fatto che disporre di Metamask è una condizione necessaria ma non sufficiente per interagire con la Blockchain. E' infatti necessario possedere cripto valuta per effettuare qualsiasi transazione, compresa quella del conio (minting) di una nuova opera, nel caso specifico ETH. Le operazioni di archiviazione e conio possono essere agevolate e/o effettuate dalla piattaforma che funge da Gallery (paragrafo 4.3), che comunque richiederà di regola il possedimento del wallet.

4.2 Definizione storica

La necessaria correlazione Crypto Art – NFT non è sufficiente a dar conto della crescente importanza che la Crypto Art sta assumendo negli ultimi anni. Forse non è azzardato definire la Crypto Art un movimento artistico e ad esso convenzionalmente assegnare come data di nascita il 13 gennaio 2018, quando a New York si è svolto il primo Rare Digital Art Festival,

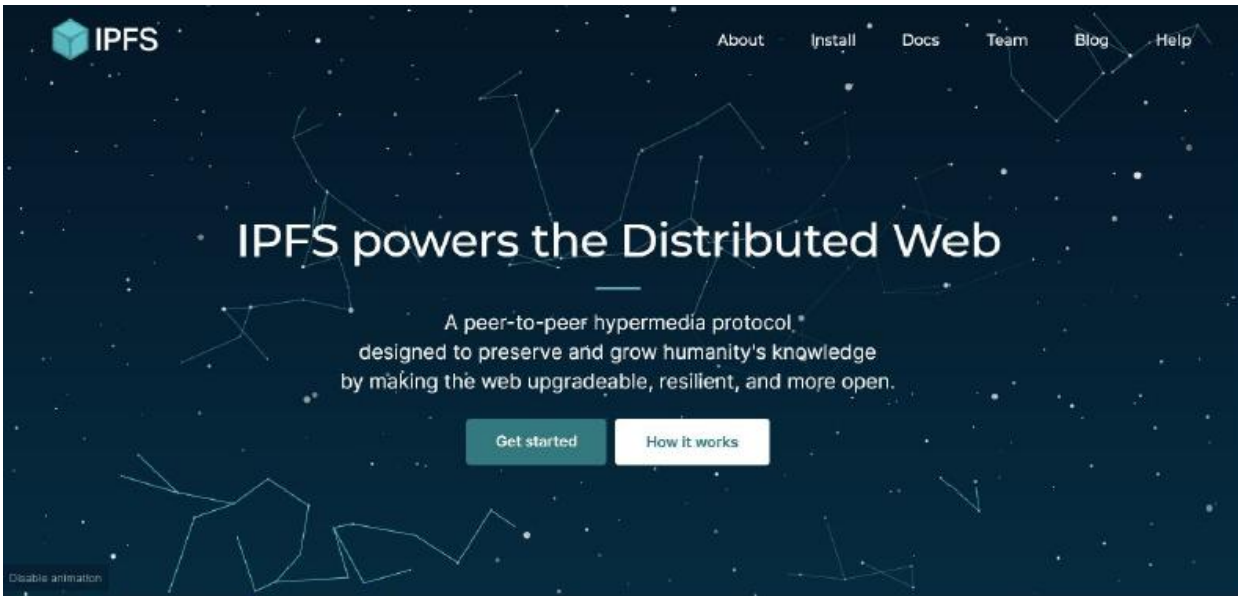


Fig. 4.1, Protocollo IPFS

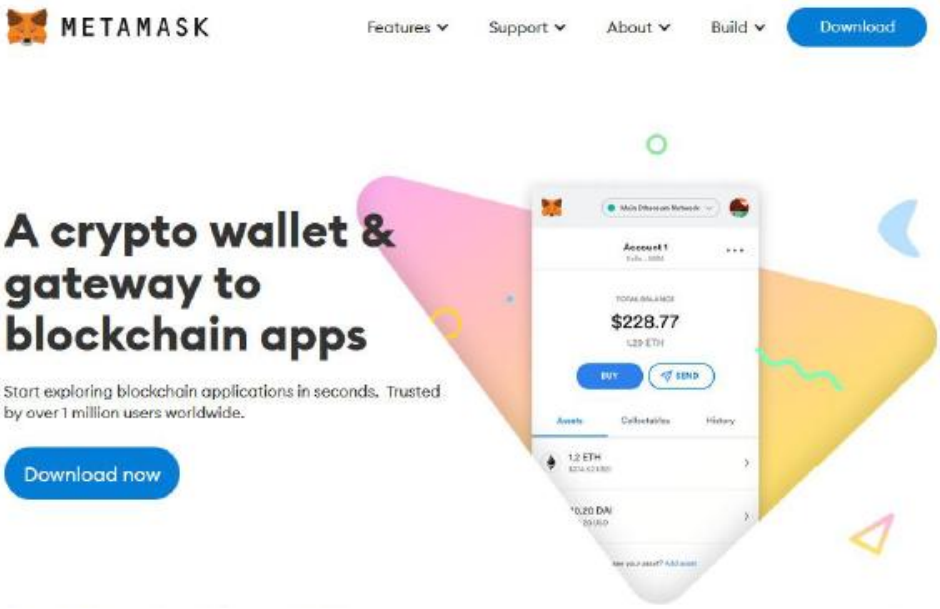


Fig. 4.2, Il wallet Metamask per Ethereum

Primo festival perché il successo è stato tale che l'appuntamento si è ripetuto negli anni successivi: il 18 maggio del 2019 (in fig 4.3 il logo), dal 14 al 17 maggio 2020 in modo virtuale a causa della pandemia Covid-19, l'appuntamento più recente il 15 maggio 2021.

Fig. 4.3, Secondo Rare Digital Art Festival

Un saggio di Jason Bailey dal titolo (What is crypto art ?) racconta del primo festival ed elenca le caratteristiche salienti che accomunano gli artisti [34]:

1. Digitally Native (la possibile completa digitalizzazione di creazione, edizione e compravendita dell'opera).
2. Geographically Agnostic (l'emancipazione data da internet, consente la partecipazione degli artisti di tutte le parti del mondo, rendendo il movimento della Crypto Art il primo movimento veramente globale).
3. Democratic/Permissionless (tutti possono partecipare a prescindere da abilità, formazione, classe, genere, razza, età, credo, etc).
4. Decentralized (strumenti e linee guida sono definiti per ridurre il potere di esperti e intermediari, conferendo così maggior autonomia agli artisti).
5. Anonymous (l'uso di pseudonimi permette agli artisti di lavorare e vendere restando anonimi, sottraendosi così al giudizio sociale).
6. Memetic (la Crypto Art spesso realizza meme, capaci di diffondersi rapidamente).
7. Self-Referential (autoreferenziali rispetto ad eventi e personalità importanti della cultura Blockchain e delle criptovalute).
8. Crypto Patrons (i collezionisti più important sono coloro che hanno investito creatività e/o denaro nella tecnologia Blockchain).
9. Pro-Artist (le piattaforme Blockchain spesso non fanno pagare alcuna commissione agli artisti, che vengono poi remunerati dalla vendite e ri-vendie successive della loro opera).
10. Dankness (la CryptoArt è aperta a tutti, non può essere giudicata ricorrendo a vecchi canoni, bensì giudicata per la sua creatività e potenza espressiva).

Jason Bailey continua il suo saggio con una serie di citazioni che toccano le piattaforme partecipanti al festival del 2018: CryptoKitties e CryptoPunks entrambe rivolte al mercato dei collezionisti,

riconoscendo la padronanza tecnica dei loro rispettivi artisti principali Guide Gaspar e John Watkinson, quindi del social Dada.nyc dove i partecipanti comunicano con i loro disegni e di Rare Pepes, dove tutti possono creare e pubblicare il loro meme della rana Pepe rispettando un minimo di prescrizioni: numero di pixel 400 x 560, dimensione minore o uguale a 1,5 MB, niente NSFW (not safe for work), etc.

Curioso l'auto-commento alla raccomandazione/prescrizione NSFW: cercate di essere leggeri, perché Pepe ha già tanta stampa cattiva. Il fatto è in una certa misura connesso all'uso di Pepe da parte dei movimenti americani di destra, in particolare ALT-RIGHT, movimento alternativo alla destra tradizionale. Uso che Jason Bailey assicura avvenire senza la minima adesione ideologica da parte della piattaforma.

Il riferimento all'articolo di Bailey, successivo al primo Rare Digital Art Festival, è stato un mezzo per fissare, arbitrariamente quanto si vuole, una data di inizio del movimento ed elencare le principali realtà allora esistenti: quelle degli oggetti da collezione (CryptoKitties e CryptoPunks) che in una certa misura anticipano e mostrano affinità con la Crypto Art, e quelle aperte di Rare Pepes e Dada che perfettamente aderiscono al decalogo prima riportato.

L'enfasi posta al 13 gennaio 2018, data di svolgimento del primo Rare Digital Art Festival, come data di nascita della Crypto Art, può risultare ancora più giustificata se si evidenzia come lo standard fondamentale per creare e gestire NFT, ERC-721, è stato emesso il 24 gennaio 2018.

Sono successivi al gennaio 2018 gli inizi delle attività delle piattaforme che fungono da mercati digitali per la Crypto Art, a cominciare dalla più importante SupeRare la cui data di lancio risulta il 2 aprile 2018.

4.3 Le gallerie

Per analogia con il mercato dell'arte tradizionale, le piattaforme che fungono da mercato digitale in ambiente Blockchain vengono solitamente chiamate gallerie. Il loro numero è in continua crescita, ad ulteriore conferma del successo della Crypto Art.

Nel seguito si fornirà una descrizione complessiva delle gallerie che nel 2020, come si vedrà nel paragrafo successivo, hanno guidato il mercato.

La prima è la galleria SuperRare [35]. E' molto selettiva nell'ammissione degli artisti che sono esaminati dopo aver inviato una serie di elementi: una breve presentazione video, il portfolio, da 3 a 5 opere con relativa storia/genesi, i motivi della scelta di SuperRare, la presenza sui social.

Gli artisti ammessi/invitati possono esporre le loro opere con la condizione che siano opere uniche, ovvero con un'unica edizione. Le modalità di vendita sono tre:

a) asta
b) prezzo fisso (buy now)
c) offerta

Per l'asta l'artista può scegliere tra due diverse modalità: asta con prezzo di riserva, importo minimo che l'artista è disposto ad accettare, oppure asta programmata a partire da un prezzo base. L'asta con prezzo di riserva termina 24 ore dopo che l'importo minimo è stato raggiunto; nel caso di asta programmata si fissa una scadenza temporale per la fine dell'asta.

Nel caso b) si tratta di una normale vendita a prezzo fisso, mentre nel caso c) si tratta di formulare un'offerta per qualsiasi opera catalogata nel sito purché non sia oggetto di un'asta in corso

L'artista per coniare l'NFT necessariamente dovrà possedere un portafoglio (wallet) Ethereum, consigliato MetaMask. Stesso consiglio per l'acquirente. I pagamenti avvengono nella cripto valuta ETH.

Nella sezione Market del sito si possono esplorare le opere presenti agendo eventualmente su varie opzioni: asta in corso, prossima asta, mercato secondario.

L'artista riceve 85% del prezzo di vendita diretta, avrà poi il 10% di royalty sulle compravendite che eventualmente si verificheranno nel mercato secondario.

L'acquirente/collezionista per operare su SuperRare dovrà già essere collegato; come per l'artista il requisito fondamentale è la disponibilità di un portafoglio Ethereum. La commissione per ogni acquisto è del 3%.

La galleria Makers Place [36] è stata lanciata un anno dopo SuperRare. Le due piattaforme hanno molte analogie nel funzionamento, pertanto conviene evidenziare le differenze.

Gli artisti devono essere ammessi per poter esporre, ma non sono date indicazioni strutturate sul modo per richiedere l'ammissione. L'unica indicazione puntuale è di connettersi tramite la piattaforma di messaggistica Discord.

Con Makers Place si possono avere copie numerate e limitate della stessa creazione.

L'acquirente può pagare anche con la carta di credito, ma in questo caso è richiesta una commissione aggiuntiva.

Nel caso di rivendita di un'opera Makers Place trattiene il 12,5%, destinando il 10% all'artista che ha coniato il token e prendendosi il resto come commissione per il servizio.

La galleria Known Origin [37] è sta lanciata nello stesso periodo di SuperRare, ha molte analogie con Makers Place. L'ammissione di nuovi artisti, nelle intenzioni strutturata, è di fatto attualmente bloccata per eccesso di domande.

La galleria Sync Art [38], lanciata ufficialmente a febbraio 2020, presenta delle caratteristiche che la differenziano rispetto alle precedenti. Prevede infatti opere d'arte digitali programmabili nei diversi elementi costitutivi, con un master che corrisponde all'assieme e dei layer che sono le parti come le tessere di un puzzle.

Un esempio delle possibilità può essere dato dalle composizioni di Fabiello, creativo italiano che propone immagini remixabili. L'ultima ha per titolo "the Remixable Reclining Nude" ed è stata lanciata su Sync Art (in gergo ha avuto il drop a maggio 2021). Il master della donna sdraiata è

composto da 4 layer: lo sfondo, la testa, il petto, i fianchi. Il mix è ottenuto attingendo dai capolavori di sei maestri della pittura:

- Giorgione - Venere dormiente
- Tiziano - Venere di Urbino
- Francisco Goya - Maja desnuda
- Gustave Courbet - Femme nue couchée
- Amedeo Modigliani - Nudo sdraiato
- Isaac Israëls - Reclining reading nude

La scomposizione in 4 layer e 6 diverse origini danno la possibilità di ottenere ben 6^4 =1296 mix/stati.

Il mercato della galleria Sync Art è fatto in modo che Master e singoli Layer vengano quotati e venduti separatamente.

Però non tutte le opere esposte da Sync Art sono costituite da layer. La maggior parte delle opere presenti sono con layer 0 ed autonome, ad esempio le immagini cambiano autonomamente in funzione del parametro impostato dall'artista.

Nell'elenco delle gallerie più importanti non può mancare Nifty Gateway [39], creata dai gemelli Foster e poi acquisita, nel 2019, dalla Gemini, dei gemelli Winkelvoss. Il motto della galleria è: "We will not rest until one billion people are collecting Nifties".

L'elenco potrebbe continuare e sarebbe comunque da aggiornare continuamente per la continua nascita di nuove gallerie.

Infine una citazione è dovuta alla piattaforma Open Sea [40], che anche se non propriamente una galleria, è molto popolare perché tratta tutti i generi di Non Fungible Token.

4.4 Il mercato

Fissata convenzionalmente a inizio 2018 la nascita della Crypto Art, è possibile raccogliere alcuni dati che si prestano a dare la misura del successo della Crypto Art nel triennio successivo.

Se assumiamo come riferimento i report redatti e ricevuti dal sito https://nonfungible.com:

- Non Fungible Art Report 2018-19 [41]
- Non Fungible Token Yearly Report 2018 [42]
- Non Fungible Token Yearly Report 2019 [43]
- Non Fungible Token Yearly Report 2020 [44]
- Non Fungible Token Quarterly Report Q1-2021 & Q2-2021[45]

si ricavano i seguenti dati di mercato

anno	mercato [USD]
2018	260.290
2019	559.403
2020	12.947.341
2021-Q1 & Q2	200.000.000 circa

Può essere utile aggiungere che i dati della tabella sono esclusivamente quelli relativi alla Crypto-Art. Infatti i report analizzati considerano il mercato degli NFT suddiviso in sei categorie, per le quali si è avuta nell'anno 2020 la seguente ripartizione.

	mercato [USD]	%
Metaverso	14.020.406	25,4
Arte	12.947.341	23,4
Giochi	12.907.165	23,3
Sport	7.143.501	12,9
Oggetti da collezione	6.168.973	11,2
Utilità	2.101.244	3,8
totale NFT	55.288.630	100,0

A dividersi il mercato della CryptoArt nel 2020 sono state le seguenti piattaforme principali:

	mercato [USD]	%
Super Rare	6.000.734	46,3
Makers Place	1.844.919	14,2
Async Art	991.917	7,7
Known Origin	784.523	6,1
Ava Stars	753.145	5,8
Autoglyphs	397.518	3,1
Nifty Gateway	340.529	2,6
altri	1.834.056	14,2
totale	12.947.341	100,0

Nel 2021 Super Rare e Makers Place sono state le principali protagoniste dell'ulteriore grande balzo del mercato, seguite da Async Art e Known Origin. Nel seguito i relativi volumi con riferimento al secondo trimestre (2021-Q2)

	mercato [USD]
Super Rare	84.540.280
Makers Place	20.208.551
Async Art	4.232.720
Known Origin	3.187.000

I dati relativi alle vendite di Crypto Art, notevolissimi per la dinamica di crescita, possono essere meglio apprezzati se confrontati con il settore nel suo complesso.

In accordo al report redatto da Clare McAndrew di Art Basel, The Art Market 2021 [46], negli ultimi 10 anni il mercato globale di arte ed antichità ha fatto registrare una media annua di 62 miliardi di US dollari con una deviazione standard di 5,6, la fetta di mercato relativa all'arte

prodotta dalla fine della seconda guerra mondiale ai giorni nostri ha totalizzato una media annua di 6,3 miliardi, con una deviazione standard di 0,8 miliardi di dollari. Questo riferimento al mercato tradizionale consente di stimare per la Crypto Art un target possibile di qualche miliardo di USD per anno, nell'ipotesi di invarianza di numero e disponibilità economica dei potenziali collezionisti.

4.5 Gli artisti

Il sito cryptoart.io fornisce un elenco di oltre 6500 artisti e per ciascuno di essi il numero di creazioni e i valori economici registrati in dollari [47]. E' un elenco ordinato, aggiornato continuamente pressoché in tempo reale, anche con riferimento al valore di mercato delle opere, con una differenza tra i valori monetari riconosciuti tra il primo e l'ultimo artista della lista di ben 5 ordini di grandezza. Per ogni artista è indicata inoltre l'opera di maggior successo commerciale. La tabella seguente riporta la classifica, così come registrata alla fine del primo semestre 2021, per le prime venti posizioni..

	artista	n° opere vendute	valore globale[USD]
1	Beeple	1342	139.118.850
2	Pak	7840	37.528.135
3	Trevorjonesart	5285	18.734.474
4	Maddogjones	1571	18.397.546
5	Fewocious	3180	18.218.898
6	Hackatao	1907	14.891.636
7	Xcopy	1908	13.952.510
8	Slime Sunday	6768	12.829.040
9	3Lau	6462	9.494.645
10	Jose Delbo	3067	9.084.611
11	Whisbe	1651	8.017.137
12	SSx3Lau	5804	7.947.458
13	Grimes	1122	7.221.015
14	Fvckrender	1831	5.793.871
15	Rtfktstudios	925	5.465.837
16	Bosslogic	1173	5.168.504
17	Snowden	1	4.984.273
18	Deadmau5	943	4.696.797
19	Micah_Johnson	2240	4.532.423
20	Steveaoki	1769	4.185.879

La classifica è guidata da Beeple [48], prima posizione consolidata nella famosa asta da Christie's, dell'11 marzo 2021, quando il collage "The first 5000 days" (fig. 4.4) è stato battuto per 69'346'250 dollari. Il suo vero nome è Mike Winkelmann, nato nel 1981 vive a Charleston, South Carolina. E' un graphic designer che adotta una certa varietà di tecnologie digitali incluse VJ loop, VR/AR. Ha lavorato per marchi importanti come Apple, Space X, Nike, Coca-Cola, Adobe, Pepsi, Samsung. Prima delle elezioni presidenziali americane ha venduto su Nifty Gateway una creazione dinamica, dal titolo "Cross Road" con tre differenti stati: prima del voto, vittoria di Trump, vittoria di Biden. L'acquirente avrebbe così conosciuto il contenuto dell'opera solo dopo l'esito elettorale.

Fig. 4.4, Prima e ultima opera del collage "The first 5000 days"

Al secondo posto Pak [49], altro pseudonimo di un artista, del quale in questo caso non si conosce la vera identità. Forse di origine turca, attivo da almeno venti anni, apprezzato da Elon Musk. La sua opera più valutata è "The switch" venduta in un'asta da Sotheby's lo scorso 12 -14 aprile. L'opera testimonia l'evoluzione dell'arte che si avvale delle tecnologie digitali, essa infatti è progettata per cambiare nel tempo in funzione di parametri decisi dall'artista. Pak è anche il creatore di Archillect [50], un algoritmo sviluppato per scoprire e condividere stimolanti contenuti visivi sui diversi social media. Le sue opere sono prevalentemente su Nifty Gateway.

Segue Trevor Jones [51], un canadese dal percorso molto interessante. Da giovane, nel 1996, si è trasferito in Scozia dove è stato impegnato per sette anni nella gestione di laboratori di arte terapia a favore di persone disabili. L'opera più valutata è "Genesis", venduta su Makers Place, un'animazione che fornisce la successione delle immagini relative alla realizzazione di un dipinto su tela raffigurante Batman. Raffigurazione che parte da un disegno ricevuto dal fumettista argentino Josè Delbo (fig. 4.5).

4.5, Batman disegnato da Jose Delbo e dipinto da Trevor Jonesart

Al quarto posto un altro canadese Mad Dog Jones [52], vero nome Michah Dowbak. Artista digitale che lo scorso aprile è stato protagonista della prima asta da Phillips di NFT, dove è stata venduta per 4'144'000 dollari la sua opera "Replicator" (fig. 4.6). Questi i dati:
Token ID: 1
Contract Address: 0xAe1fB0ccE66904b9fa2b60BeF2B8057CE2441538
Non-Fungible Token (ERC-721)
PNG: 16.5 MB (16,457,805 bytes), 4800x6000px
MP4: 64.2 MB (64,232,495 bytes), 4800x6000px, HD, 00:50, stereo
Minted on April 11, 2021, this work is unique.

Anche questa un'opera dinamica, la storia di una macchina fotocopiatrice attraverso il tempo, che ogni 28 giorni ha l'abilità di generare un nuovo unico NFT.

Infatti il token venduto all'asta da Phillips è programmato per riprodursi fino alla settima generazione, con una prolificità che diminuisce da una generazione all'altra e con un rischio significativo di inceppamenti e/o altri guasti che impediscono la riproduzione.
Il consuntivo alla fine di agosto 2021 è di 19 Replicator, compreso il capostipite coniato l'11 aprile 2021, di cui 7 oggetto di guasti.

4.6, Fotogramma di "Replicator" di Maddogjones

Segue FEWOCiOUS [53], transgender dichiarato, che a soli 18 anni ha già venduto 3180 NFT. Attualmente residente a Seattle, è cresciuto a Las Vegas dove all'età di 13 anni ha iniziato a dare forma artistica alle istantanee della sua memoria ed ai suoi sentimenti. L'opera meglio pagata, venduta dalla piattaforma Nifty Gateway, ha per titolo "The everlasting beautiful", opera digitale accompagnata anche da un dipinto su tela di dimensioni 30x30 pollici (fig. 4.7).

4.7, Un fotogramma di "The everlasting beautiful" di FEWOCiOUS

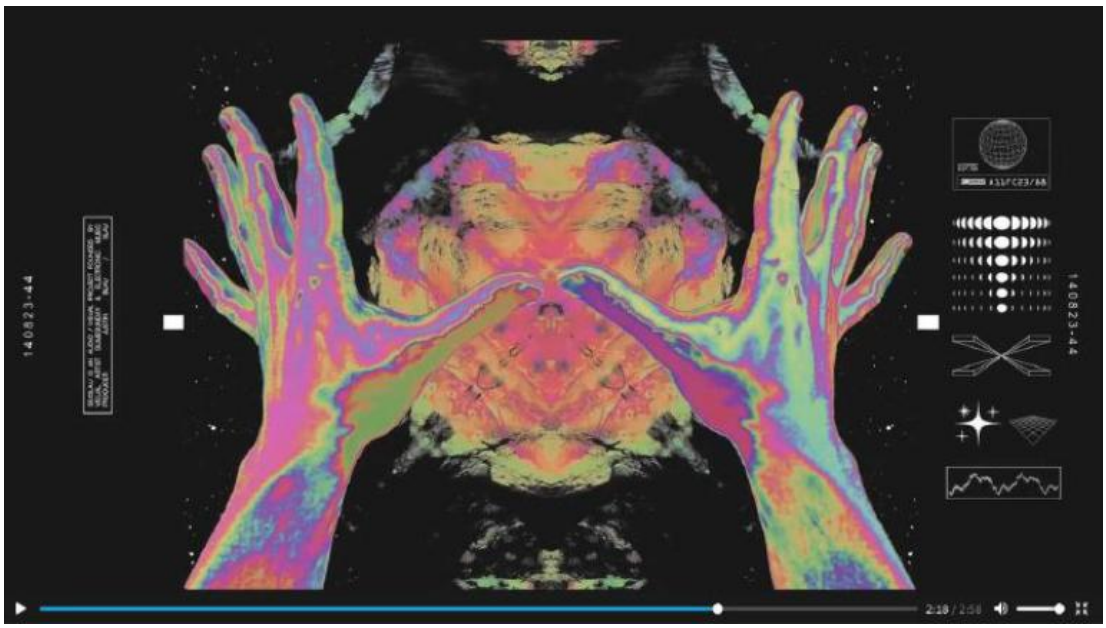
Anche il sesto posto è occupato da uno pseudonimo: Hackatao [54]. Ma in questo caso l'identità non è un segreto, è tutto scritto nell'omonimo sito internet. «Il dittico artistico Hackatao è nato nel 2007, è formato da Sergio Scalet e Nadia Squarci. Gli Hackatao vivono e lavorano un po' ovunque. Dopo anni vissuti in uno dei quartieri più creativi e artistici della psicotica Milano, Zona Isola, sono migrati nel piccolo borgo medioevale di Oltris (provincia di Udine). Tra le montagne della Carnia e una natura al limite del selvaggio danno il meglio della loro produzione artistica». La loro opera più quotata, venduta sulla piattaforma SuperRare, è di ispirazione politica ed ha per titolo "Kim Jong Un - Dead and Alive", di cui alcuni fotogrammi sono riportati in fig. 4.8.

4.8, Tre fotogrammi di "Kim Jong Un - Dead and Alive" degli Hackatao

Si torna in piena oscurità sulla vera identità passando al settimo posto, occupato da Xcopy [55]. Le uniche notizie sono: artista digitale da lungo tempo con base a Londra, entusiasta della Crypto Art. Costante ispirazione da morte, distopia ed apatia che traduce in immagini spettrali lampeggianti. Venduti 1908 NFT: il meglio pagato, per 2'241'130 dollari, "Death dip", sulla piattaforma SuperRare lo scorso marzo.

E' un millennial nato a Boston ad occupare l'ottavo posto: Slimesunday, vero nome Mike Parisiella [56]. Autore di molti NFT caricati su Nifty Gateway. Prevalentemente collage digitali di contenuto bizzarro e/o erotico, tendenti a spostare i limiti dell'accettabilità mainstream. Pertanto già oggetto di censure che forse ha trovato nella Crypto Art, in particolare tramite la piattaforma Nifty Gateway, maggiore libertà di espressione. E' direttore artistico del musicista 3Lau, con il quale condivide il progetto audiovisivo SSX3LAU che esplora l'intersezione tra arte digitale, dance music e tecnologia DLT.

Si scrive 3Lau, ma si pronunzia, Blau [57] l'artista che occupa il nono posto. 3Lau è la firma di Justin Blau, musicista nato nel 1991 nello stato di New York. Il token del video musicale di 2' 58" realizzato con Slimesunday, dal titolo Gunky's Uprising, è stato venduto a fine marzo 2021 per oltre un milione di dollari (fig. 4.9).



4.9, Un'immagine di "Gunky's Uprising"del duo SSX3LAU

Al numero 10 un artista nato nel 1933, Josè Delbo [58], impegnato da oltre settanta anni a disegnare fumetti, compreso Batman. Lo stesso che ha dato l'avvio all'opera Genesis, la più remunerativa di Trevor Jones. Di origine argentina ha disegnato cartoni prima con protagonisti cowboy, poi super eroi, quindi transformer, infine i cartoni con Captain Planet e i Planeteers di stampo ambientalista. Nel luglio 2020 ha coniato su Makers Place il suo primo NFT, con un fumetto originale di 43 pagine dal titolo poco scaramantico "Death".

5 Considerazioni

5.1 Approccio

La Crypto Art per sua natura è argomento complesso, intersezione e sovrapposizione di mondi regolati da leggi e tradizioni diverse. Un'analisi significativa e pregnante richiederebbe il concorso di più discipline, in un approccio di tipo olistico, che consentisse di esaminare lo stato dell'arte in tutta la sua complessità.

Analisi che non potrebbe ignorare, ad esempio, il famoso saggio di Walter Benjamin "L'opera d'arte nell'epoca della sua riproducibilità tecnica" [59]. In esso è proposto il concetto di aura, una qualità associata a unicità e originalità di un'opera d'arte, che «si atrofizza o deperisce» con la riproduzione dell'opera.

Potrebbe risultare molto interessante l'applicazione del concetto di aura all'arte digitale, per sviluppare il tema di quanto la Crypto Art possa restituire l'aurea dell'unicità, rarità, originalità, mediante il conio ed il possesso di un Non Fungible Token.

Tema interessante e affascinante, per più motivi non perseguibile nell'ambito del presente lavoro. Nel seguito ci si limiterà ad un approccio cartesiano riduzionista, formulando semplici considerazioni su tre voci della Crypto Art: la tecnologia, il mercato, l'artista. Riflessioni riportate rispettivamente nei tre paragrafi che seguono.

Infine, nell'ultimo paragrafo del capitolo, si è ritenuto opportuno aggiungere notizie e considerazioni sugli spin-off della Crypto Art. Intendendosi per spin-off gli sviluppi secondari e separati dell'applicazione della tecnologia Blockchain al settore dell'arte.

5.2 Tecnologia

Per la tecnologia sono da considerare due linee di sviluppo: l'arte mediale digitale e quella Blockchain. La prima, nell'uso anglosassone indicata come computer art o new media art, si colloca nella naturale evoluzione di materiali e tecniche usate nell'arte, basti pensare ad esempio all'introduzione della pittura ad olio o alla differenza tra scultura in legno, marmo o bronzo.

La creazione artistica digitale richiede competenze informatiche specifiche, tanto che gli artisti possono essere raggruppati in due categorie: gli esperti (tech-savvy) e gli autodidatti (self-trained). L'uso frequente di pseudonimi, per i quali spesso non si hanno informazioni sulla vera identità anagrafica, induce a pensare che sovente le opere digitali non siano il risultato del lavoro di un singolo ma di un team. Almeno due persone con talenti e competenze complementari che possano coniugare visione e realizzazione.

Uno dei S/W utilizzati è "Cinema 4D" per la modellazione 3D [60], il suo uso permette di gestire e realizzare lavori di design, animazione (motion graphics), VFX (effetti visivi), AR (realtà aumentata), VR (realtà virtuale), MR (realtà ibrida).

Se da un lato il mondo digitale mette a disposizione degli artisti nuovi mezzi espressivi, sempre più potenti ed efficienti, dall'altro lato li espone al rischio di plagio, in misura infinitamente maggiore rispetto al mondo fisico / materiale dell'arte tradizionale.

La tecnologia DLT, essenza della Blockchain, fornisce un utile mezzo per tutelare il diritto d'autore attraverso la corrispondenza tra opera creativa ed NFT.

I dubbi di natura tecnologica sul futuro della Crypto Art, così come espressi dai media, riguardano la sua compatibilità con la transizione ecologica, un obiettivo ormai considerato imprescindibile.

Per dare voce a questo dubbio è pertinente citare un articolo apparso sul Corriere della Sera, il 24 maggio 2021, di Vincenzo Trione [61]. L'autore oltre che collaboratore del giornale, è professore ordinario di Arte e media e di Storia dell'arte contemporanea. L'articolo è stato pubblicato con un titolo che efficacemente esprime i dubbi del professore: «Tutt'altro che sostenibile, la Crypto Art consuma energia quanto l'Argentina».

Il problema dell'eccessivo consumo di energia, richiesto dalle Blockchain pubbliche Bitcoin ed Ethereum, è stato già trattato nel capitolo 3. Considerato però che il conio di token non fungibili (NFT) viene generalmente effettuato sulla piattaforma Ethereum, in particolare con l'applicazione del protocolo ERC-721, il futuro della Crypto Art è in larga misura connesso all'evoluzione di Ethereum.

La sperimentazione in corso, iniziata a dicembre 2020, che ha come obiettivo la transizione dalla versione attuale alla versione Ethereum 2.0, determinerà una riduzione drastica del consumo di energia. Infatti il contestuale passaggio del meccanismo di consenso da PoW (proof of work) a PoS (proof of stake) ridurrà il consumo in una misura stimata del 99,95% [21].

5.3 Mercato

I dati di mercato, di quello che può essere considerato il primo triennio della Crypto Art, mostrano un successo così strepitoso da indurre molti osservatori a raffreddare gli entusiasmi.

Se il totale delle vendite del 2019 è risultato doppio rispetto al 2018, nel 2020 è stato addirittura moltiplicato per 20 rispetto all'anno precedente. I dati di primo e secondo trimestre 2021 mostrano che il tasso di crescita del 2020 dovrebbe essere ulteriormente migliorato nell'anno in corso.

Se considerassimo la CryptoArt semplicemente come un'innovazione potremmo applicare la curva di Rogers per rappresentare e prevedere la sua diffusione nel tempo [62]. Dato l'insieme degli attori protagonisti, artisti e/o collezionisti, i primi innovatori sono solo il 2,5%, questi sono seguiti da una percentuale del 13,5% di attori attenti alle novità (early adopter) , quindi la maggioranza iniziale del 34%, la maggioranza tardiva di un altro 34% ed infine il 16% dei ritardatari.

Se la curva di Rogers fosse applicabile dovremmo porci la domanda se la Crypto Art ha già toccato la maggioranza ed in che misura.

In verità l'innovazione ha toccato un mercato naturalmente in evoluzione, tanto sul lato della domanda quanto sul lato dell'offerta.

I collezionisti possono essere mossi da tre differenti driver:

- la genuina passione per l'arte accompagnata da personale gusto estetico
- il prestigio di possedere un'opera importante
- la scelta di investire in arte.

Una cosa è certa e documentata: la maggioranza dei collezionisti /acquirenti sono ormai della generazione così detta dei millennial [46], che sicuramente riescono meglio ad apprezzare la garanzia di autenticità della Crypto Art assicurata dalla Blockchain in maniera diretta. Così come i millennial sono sicuramente interessati alle opere digitali programmabili, ovvero all'arte generativa.

In quanto alle motivazioni sociali e psicologiche dei singoli collezionisti è da ritenere che queste sono forse gli ingredienti determinanti nella scelta della Crypto Art.
Perché possedere il token non è condizione indispensabile per avere una copia di un'opera digitale, è solo un titolo riconosciuto di esserne il legittimo proprietario.
In qualche modo una situazione analoga alla prima edizione di un libro con la firma dell'autore. Se di un libro di successo possono essere state vendute ed essere in circolazione centinaia di migliaia di copie, per un bibliofilo sono le copie autografate dall'autore che hanno valore ben aldilà dell'originale prezzo di vendita.

Il riferimento generazionale vale anche per gli artisti dove oltre che i millennial sono sempre più presenti artisti della generazione Z che trainati dai social, in primis Instagram e Twitter, con la Crypto Art si sono visti aprire le porte del mercato on-line.
Mercato on-line già in crescita, che la pandemia Covid-19 ha ulteriormente accelerata anche per il mercato dell'arte tradizionale [46].

5.4 Artisti

L'avvento della Crypto Art ha permesso a tanti giovani artisti digitali di affermarsi, evitando di ripercorrere lo stereotipo dell'artista come nella Bohème, sognatori senza quattrini con il culto dell'arte e avversione verso i valori mainstream.

Oltre al vantaggio di avere introdotto la copia unica, o in alternativa l'opera con numero di edizioni limitate, ponendo fine alla riproducibilità digitale senza limiti che comportava un grave pregiudizio verso i possibili guadagni, la Crypto Art garantisce la presenza dell'artista nel mercato secondario.

E' un'innovazione molto importante, che invano in passato si è tentata di introdurre nella legislazione di molti paesi per il mercato tradizionale. La situazione tipica era quella dell'artista giovane e non ancora conosciuto, che cedeva le sue opere per pochi soldi per potersi mantenere economicamente, opere che poi avrebbero assunto valori ben maggiori, ma di questa plusvalenza l'artista non avrebbe avuto alcuna parte.

La Blockchain mantiene costantemente traccia delle compravendite che hanno per oggetto un'opera, e riconosce ad ogni passaggio di proprietà una percentuale all'artista creatore.

Il mercato tradizionale è costituito da sei figure prominenti: l'artista, il gallerista, il critico d'arte, la casa d'aste, il collezionista, il curatore. Figure che nella vita di un'opera d'arte agiscono in momenti diversi, senza avere necessariamente interazioni / scambi con l'artista, se si esclude il gallerista, ruolo assimilabile a quello di primo acquirente. In altre parole nel mercato tradizionale l'artista partecipa solo al mercato primario, con un compenso che si stima essere circa il 50% del prezzo di vendita.

Con la Crypto Art l'artista ottiene un maggior remunerazione nel mercato primario, tutte le principali gallerie gli riconoscono l'85% del prezzo di vendita, inoltre ha un ruolo oltre il mercato primario, i diritti d'autore vengono registrati sulla Blockchain e con essa gestiti in tutti i possibili successivi scambi dell'opera che vengono puntualmente tracciati e remunerati con il 10% del prezzo di vendita.

In sintesi il cambio di paradigma determinato dalla Crypto Art avvantaggia soprattutto l'artista in termini di distribuzione dei compensi. Ma non bisogna sottovalutare come l'ecosistema Crypto Art possa esaltare l'estro creativo. In un mondo dove la digitalizzazione è un obiettivo primario di enti pubblici e privati, la realizzazione di questo obiettivo con tutte le trasformazioni conseguenti non può non influire sull'ispirazione artistica e sulle modalità espressive. Può essere considerato un esempio di questa accresciuta potenzialità la sigla SSX3LAU [57], associazione tra Slimesunday e 3Lau, che esplora l'intersezione tra arte digitale, dance music e la tecnologia DLT. Così come la galleria Sync.Art che promuove creazioni con le quali il collezionista può interagire.

5.5 Spin-off

Esistono importanti esempi di applicazione della tecnologia Blockchain al settore dell'arte che, pur non essendo definibili propriamente Crypto Art, potrebbero rivelarsi in futuro anticipatori di nuove prassi o consuetudini.

Si tratta di esempi che hanno per protagonisti istituzioni storiche del settore e start-up intente ad introdurre le nuove tecnologie. In un ordine pressoché cronologico tre importanti start-up sono: Artory [63], Cinello [64], Vastari [65].

Artory è un database, introdotto nel 2018, dove i collezionisti possono registrare le opere d'arte possedute e le case d'asta registrare le transazioni. Un team di esperti vaglia le informazioni e garantisce autenticità e provenienza delle opere.

Sono rese pubbliche le informazioni relative a titolo dell'opera, descrizione, prezzo, etc, ma nello stesso tempo è garantito l'anonimato dei proprietari.

Christie's è un partner di Artory. Il sito comprende oltre trenta milioni di transazioni e oltre duecentomila artisti. Il database è alimentato soprattutto dalle aste, pertanto gli artisti più presenti sono artisti del novecento, nell'ordine : Picasso 1881-1973, Andy Warhol 1928-1987, Marc Chagall 1887-1985, Joan Mirò 1893-1983, tutti già con oltre diecimila transazioni. Tra gli old-masters sono nettamente primi Rembrandt 1606-1669 e Albrecht Dürer 1471-1528.

La Cinello ha brevettato un sistema denominato DAW® , acronimo di Digital Art Work, per la riproduzione digitale in scala 1-1 di opere importanti e la riproduzione fisica fedele della cornice

originale, accompagnate da registrazione su Blockchain. Di ciascuna opera vengono prodotte, e proposte al mercato, un numero di edizioni limitato, tutte accompagnate da certificato (fisico) di garanzia firmato dalla Cinello e dal responsabile del Museo che possiede l'opera e soprattutto il relativo NFT registrato su Blockchain..

Le cronache dei giornali hanno già riportato l'avvenuta vendita di un'opera di Michelangelo conservata presso la Galleria degli Uffizi [66], si tratta del così detto "Tondo Doni", un dipinto su tavola del diametro di 120 cm, con l'immagine della Sacra Famiglia commissionato dalla famiglia Doni. Si tratta della prima di nove edizioni, prodotte con il brevetto DAW®, venduta per € 140'000, somma da dividere in parti uguali tra Cinello e Uffizi.

L'accordo tra la start-up e il museo prevede di ripetere l'operazione con altri capolavori, secondo l'articolo già citato si tratta di tre opere di Raffaello, altrettante di Botticelli, due opere di Leonardo, poi ancora opere di Bronzino, Caravaggio, Tintoretto, Tiziano, Canaletto.

Un'operazione analoga a quella avviata dalla Galleria degli Uffizi è stata intrapresa dal museo Ermitage di San Pietroburgo [67]. Il sito del museo ha così titolato il 31 agosto 2021 un annuncio nella sezione News: «The State Hermitage announces the start of the sale of NFT tokens on the Binance NFT marketplace». Sono state messe all'asta le riproduzioni digitali di cinque capolavori di cinque autori: Leonardo da Vinci (Madonna Litta), Giorgione (Giuditta), Vincent van Gogh (Lillà), Wassily Kandinsky (Composizione VI) e Claude Monet (Il giardino degli Hoschedé a Montgeron).

In questo caso la vendita è avvenuta on-line, tramite la piattaforma Binance [68], dal giorno 31 agosto al 7 settembre 2021. Per ciascuna opera sono state previste 2 sole edizioni: quella oggetto dell'asta ed una seconda copia da conservare presso il museo.

Il museo Whitworth di Manchester [69], con la collaborazione di Vastari, ha lanciato un progetto denominato " The Ancient of days", proponendo un NFT con la riproduzione digitale multispettrale del famoso disegno di William Blake. Sono state realizzate 50 edizioni, un ulteriore NFT è stato creato per tracciare tutte le transazioni che avranno per oggetto le riproduzioni immesse sul mercato.

Il progetto Whitworth-Vastari presenta alcune caratteristiche degne di nota, oltre all'assonanza del titolo con quello dell'opera di Beeple andata all'asta da Christie's:

- Per manifestare sensibilità al problema ecologico legato al PoW, considerato che Ethereum non ha ancora completato la transizione da PoW a PoS, è stata scelta la piattaforma Tezos, che ha come cripto-valuta nativa XTZ.
- E' stata previsto il pagamento di una royalty del 20% per tutte le transazioni.
- Il Museo ha dichiarato la specifica destinazione del denaro ricavato da vendita degli NFT e successive transazioni.

Tutte le iniziative sopra riportate, per lo più apprese attraverso recentissime cronache dei giornali, inducono ad una semplice ulteriore considerazione. Se nella Crypto Art gli NFT sono il veicolo attraverso il quale le creazioni digitali vengono immesse sul mercato e scambiate (con la garanzia di originalità, unicità ed esclusività), gli stessi NFT possono essere per le tradizionali istituzioni dei Beni Culturali strumento di supporto alla ricerca (banche dati) e di raccolta fondi anche attraverso nuove proposte assimilabili ai tradizionali souvenir.

6 CONCLUSIONI

Crypto Art è un'opera d'arte digitale registrata criptograficamente su una Blockchain, come Non Fungible Token (NFT).

La principale Blockchain che rende possibile il conio si queste opere è Ethereum, in particolare la sua applicazione ERC-721.

Convenzionalmente si può fissare la data di nascita della Crypto Art il 13 gennaio del 2018, in coincidenza del primo Rare Digital Art Festival. Convenzione corroborata dalle date di due eventi successivi al Festival di poche settimane: l'emissione dello standard ERC-721 il 27 gennaio 2018 e il lancio della galleria SuperRare, ad oggi la più importante, il 2 aprile 2018.

Nei poco più di tre anni trascorsi la Crypto Art si è affermata prepotentemente. Ha dato spazio e visibilità a tanti giovani artisti, determinando un'emancipazione della loro figura.

Con la Crypto Art l'artista riacquista un ruolo oltre il mercato primario, i diritti d'autore vengono registrati sulla Blockchain e con essa gestiti in tutti i possibili successivi scambi dell'opera che vengono puntualmente tracciati.

La possibilità di riprodurre senza autorizzazione l'opera digitale può infatti essere bloccata e attraverso la Blockchain garantire autenticità, unicità, non riproducibilità. La Crypto Art accresce pertanto l'importanza e la nobiltà dell'arte digitale.

In un mondo dove la digitalizzazione è un obiettivo primario di enti pubblici e privati, la realizzazione di questo obiettivo con tutte le trasformazioni conseguenti non può non influire sull'ispirazione artistica e sulle modalità espressive: l'eco sistema Crypto Art potrebbe risultare determinante nell'esaltare l'estro creativo degli artisti.

Le riserve espresse nei confronti della Crypto Art, motivate dall'eccessivo consumo di energia elettrica della tecnologia Blockchain, hanno un valido fondamento se riferite al livello attuale di sviluppo. Giudizi negativi che non avranno motivo di esistere se avrà successo la sperimentazione in atto in ambiente Ethereum, che ha tra i suoi obiettivi la modifica del meccanismo di consenso che in accordo alle previsioni consentirà un risparmio di energia pari al 99,95%.

7. Bibliografia e sitografia

1. Satoshi Nakamoto: "Bitcoin : A Peer-to-Peer Electronic Cash System", https://bitcoin.org
2. Alessandro Pallante: "Blockchain per la filiera alimentare: un'applicazione decentralizzata per il tracciamento dei fondi Europei destinati al pascolo", tesi di laurea magistrale, Poltecnico di Torino, 2020.
3. Alberto Doglioli: "Industry 4.0 and Blockchain: On the use of distributed ledgers for supply chain management", master's degree thesis, Politecnico di Torino, 2019.
4. Laura Augugliaro: " Applicazione della Blockchain alla Supply Chain dell'Automotive: Analisi dello stato dell'arte e delle prospettive future", tesi di laurea magistrale, Poltecnico di Torino, 2020.
5. "Our Data, Our Future: Radical Tech for a Democratic Digital Society" DECODE Synposium 5-6 November 2019, La Centrale, Nuvola Lavazza, Torino.
6. Pierangelo Soldavini: "I token non fungibili - Christie's debutta nelle criptovalute: con 69,3 milioni di dollari è record per l'arte digitale" Il Sole 24 ore, Tecnologia / economia digitale, 12 marzo 2021.
7. https://www.beeple-crap.com
8. Vitalik Buterin: "Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform" Jan 23, 2014; https://ethereum.org
9. Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone: "Blockchain Trechnology Overview", National Institute of Standards and Technology (NIST) – US, NISTIR 8202, October 2018.
10. Claudia Antal , Tudor Cioara , Ionut Anghel, Marcel Antal and Ioan Salomie: "Distributed Ledger Technology Review and Decentralized Applications Development Guidelines. Future Internet 2021, 13, 62. https://doi.org/10.3390/613030062.
11. "The OECD Blockchain Primer", https://www.oecd.org/finance/Blockchain
12. Andreas M. Antonopoulos: "Mastering Bitcoin – Programming the open Blockchain", O'Reilly 2017.
13. "Secure Hash Standards (SHS)", National Institute of Standards and Technology (NIST) – US, FIPS-PUB 180-4, august 2015.
14. https://xorbin.com/tools/sha256-hash-calculator
15. Daniel R.L.Brown: "Recommended Elliptic Curve Domain Parameters", Standards for Efficient Cryptography (SEC), 2010.
16. https://www.Blockchain.com/
17. https://btc.com/
18. https://blockchair.com/
19. Antony Lewis: "A gentle introduction to bitcoin mining", https://bravenewcoin.com/insights/a-gentle-introduction-to-bitcoin-mining
20. "Bitcoin Halving, Explained" https://www.coindesk.com/bitcoin-halving-explainer
21. https://ethereum.org/it/
22. Andreas M. Antonopoulos, Gavin Wood :"Mastering Ethereum – Building Smart Contracts and DApps", O'Reilly 2018.
23. Gavin Wood: "Ethereum - A Secure Decentralised Transaction Ledger" [Yellow Paper versione 80085f7] dal sito https://ethereum.org/it/whitepaper/
24. https://etherscan.io/
25. Loïc Lesavre, Priam Varin, Dylan Yaga: "Blockchain Networks: Token Design and Management Overview", National Institute of Standards and Technology (NIST) – US, NISTIR 8301, february 2021.

26. https://digiconomist.net.
27. https://cbeci.org.
28. “Terna – Pubblicazioni Statistiche: Consumi 2019”, https://www.terna.it/it/sistema-elettrico/statistiche/pubblicazioni-statistiche.
29. Franceschet, Massimo, Giovanni Colavizza, T’ai Smith, Blake Finucane, Martin Lukas Ostachowski, Sergio Scalet, Jonathan Perkins, James Morgan, and Sebástian Hernández. 2020. “Crypto Art: A Decentralized View.” *Leonardo*. MIT Press. http://arxiv.org/abs/1906.03263.
30. https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924
31. Robert Graham: “Deconstructing that $69million NFT” https://securityboulevard.com/2021/03/deconstructing-that-69million-nft/
32. https://ipfs.io/
33. https://metamask.io/
34. Jason Bailey: “What is CryptoArt?” https://www.artnome.com/news/2018/1/14/what-is-cryptoart
35. https://superrare.com/
36. https://makersplace.com/
37. https://knownorigin.io/
38. https://async.art/
39. https://niftygateway.com/
40. https://opensea.io/
41. Maxime Laglasse: “Non-Fungible Art Report 2018-2019” https://nonfungible.com/
42. Daniel Kelly, Gauthier Zuffinger: “Non Fungible Tokens Yearly Report 2018” https://nonfungible.com/
43. Daniel Kelly, Gauthier Zuffinger: “Non-Fungible Tokens Yearly Report 2019” https://nonfungible.com/
44. Daniel Kelly, Gauthier Zuffinger, Maxime Laglasse, Jess Ford: “Non-Fungible Tokens Yearly Report 2020” https://nonfungible.com/
45. The Non Fungible Team: “Non-Fungible Tokens Quarterly Report Q1-2021” & “Non-Fungible Tokens Quarterly Report Q2-2021”https://nonfungible.com/
46. Clare McAndrew: “The Art Market 2021” An Art Basel & UBS Report
47. https://cryptoart.io/
48. https://www.beeple-crap.com/
49. https://pak.medium.com/
50. https://archillect.com/
51. https://www.trevorjonesart.com/
52. https://www.maddogjones.com/
53. https://fewocious.com/
54. https://hackatao.com/
55. https://xcopyart.com/
56. https://slimesunday.com/
57. https://3lau.com/
58. https://josedelbo.org/
59. Walter Benjamin: “ L’opera d’arte nell’epoca della sua riproducibilità tenica”, a cura di Giulio Schiavoni, BUR classici moderni, RCS libri, Milano 2013.
60. https://www.maxon.net/it/cinema-4d.
61. Vincenzo Trione: “Tutt’altro che sostenibile, la Crypto Art consuma energia quanto l’Argentina”, in “Pianeta 2021” periodico del Corriere della Sera, 24 maggio 2021.
62. Everett Rogers: “Diffusion of innovations”, sintesi del libro reperibile su Wikipedia e/o https://www.treccani.it/enciclopedia/everett-rogers(Lessico-del-XXI-Secolo).
63. https://www.artory.com.

64. https://www.cinello.com/it/
65. https://www.vastari.com/
66. Marilena Pirrelli: “Gli Uffizi sdoganano il Tondo Doni in versione NFT”, 24 Arteconomy, Il Sole24ore, 18 maggio 2021.
67. https://www.hermitagemuseum.org/wps/portal/hermitage/news/news-item/news/2021/news_188_21/?lng=it.
68. https://www.binance.com/en.
69. https://whitworth.vastari.com/theancientofdaysnft.

Appendice - **Guida alla creazione di un NFT-Crypto Art**

A.1 Creazione del Portafoglio

Il metodo più semplice per essere collegati alla rete Ethereum e poter quindi comprare e scambiare ETH, oltre che creare e collezionare NFT, è quello di utilizzare un'applicazione come MetaMask, un progetto Open Source (come tra l'altro Ethereum).

Metamask è un'estensione disponibile per i browser più utilizzati Firefox, Google Chrome, e altri. Questa estensione del browser permette facilmente l'interazione con siti internet e gallerie, dove la cryptovaluta è spendibile o acquistabile, oltre che poter confermare/firmare le operazioni direttamente dal browser. Procedimenti che sarebbero meno sicuri e più complessi nel caso di un software stand- alone.

In questo caso sarà utilizzato Firefox per la sua peculiarità di essere completamente Open Source (Chromium è la versione Open di Google Chrome).

Creare un portafoglio è un'operazione molto semplice per la quale servirà solo un indirizzo e-mail e una password, che a sua volta è accompagnata da una frase generata da MetaMask per un eventuale recupero password o per esportare/importare portafogli.

A questo punto la chiave pubblica sarà disponibile e si potrà comprare e ricevere ETH.

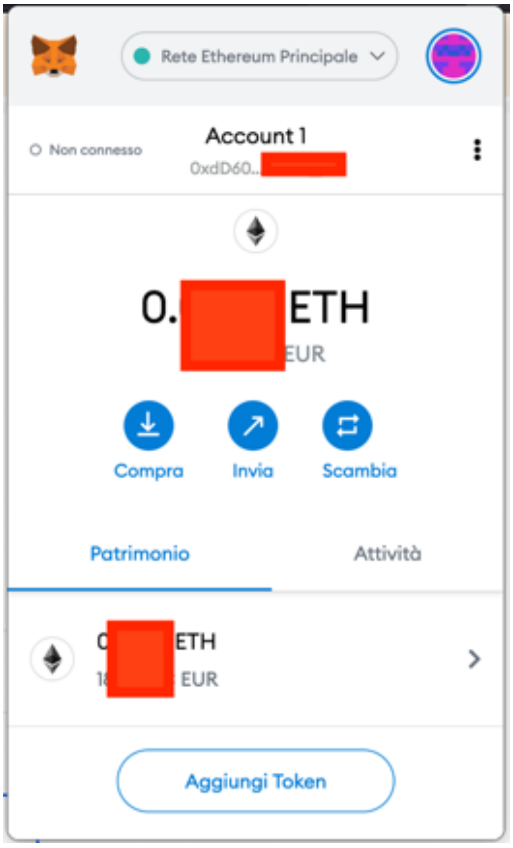


Fig A1, Interfaccia Metamask

A.2 Acquisto ETH

Una volta creato il portafoglio servirà quindi avere degli ETH disponibili, MetaMask offre due soluzioni, in questo caso sarà usato Wyre (dal sito sendwyre.com) per la sua velocità e semplicità d'uso, oltre all'integrazione con il portafoglio.

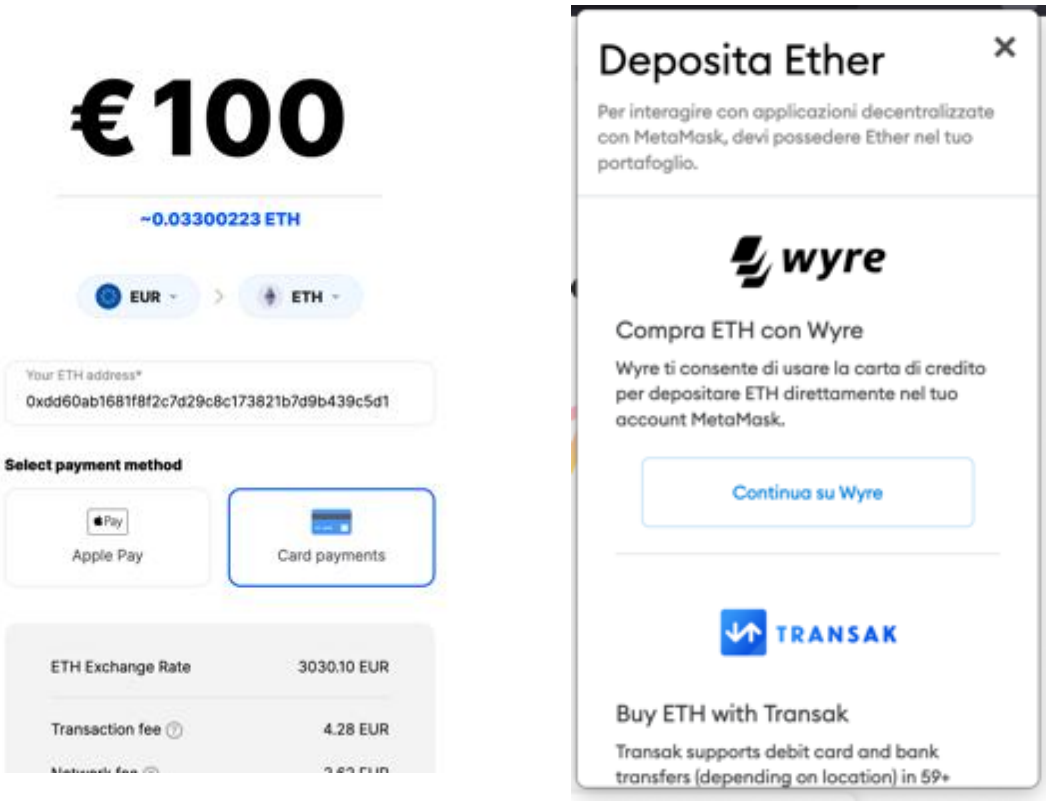


Fig A2, Acquisto ETH con Wyre.

A.3 Creazione di un Artwork

Un Artwork può essere un modello statico, 2D, 3D, una foto, una gif, un video, un audio, un'opera reale fatta a carta e penna o marmo e scalpello, ma anche una combinazione di più elementi. Ma la cosa più innovativa è l'arte generativa, in questo esempio si è utilizzato Processing, ma le possibilità sono ancora da esplorare, come un algoritmo GAN, o altri (es. The Switch e Replicator tra le opere più note).

Per questa appendice si è deciso di utilizzare un semplice generatore di linee astratte e casuali, ogni volta che verrà avviato, percorso e colore della traccia saranno generati in maniera casuale, riducendo al minimo la possibilità di generare due file identici. Il codice è riportato in allegato.

Per salvate l'opera basterà inserire nel *draw() saveFrame("output/image####.png");*e convertire in MP4/h.264 la sequenza di png con il semplice aiuto di ffmpeg:

```
ffmpeg -r 60 -f image2 -s 600x600 -i image%04d.png -vcodec libx264 -crf25  -pix_fmt yuv420p
output.mp4
```

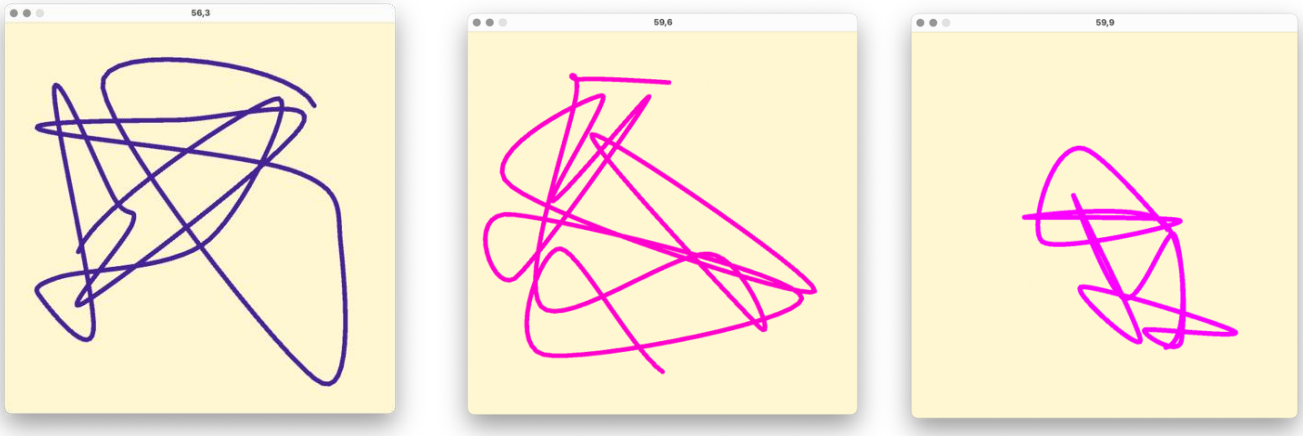


Fig. A3, Esempi di Output

A.4 Scelta Galleria

Diventare Collector di una galleria è molto semplice, basta registrarsi e collegare il proprio portafoglio, invece diventare Creator può essere tutt'altro che semplice.

Come già visto ci sono numerose gallerie, SuperRare è certamente la più pres tigiosama anche quella di più difficile accesso, poiché bisogna essere artisti riconosciuti di una certa fama e non è più neanche possibile mandare una richiesta di approvazione come Creator.

Makers Place offre ai suoi utenti di mandare un Portfolio e una breve presentazione di se stessi per diventare Creator, l'operazione non è lunga ma l'attesa può richiedere fino a 3 settimane.

La galleria di più facile accesso per pubblicare la propria opera è OpenSea. Questo sia per la semplicità, sia per la peculiarità di essere open source, così come le altre risorse utilizzate in questa guida. Come market ha molti punti a sfavore. Ad esempio l'enorme quantità di opere esposte comporta la difficoltà di emergere. Di contro Open Sea non mette limiti sulla pubblicazione di nuove opere e soprattutto non chiede documentazioni di nessun genere per essere un Creator.

Una volta registrati si è già pronti alla pubblicazione, i soli limiti sono dimensioni file e tipologia.

Si dovranno solo compilare i vari metadata, decidere come deve avvenire la vendita (asta, prezzo fisso), i numeri di copie in vendita, e la *fee* che si desidera ricevere sulle transizioni secondarie.

Maximum file size of 100MB (Image, video, audio, and 3D model file types are supported) **JPG, PNG, GIF, SVG, MP4, WEBM, MP3, WAV, OGG, GLB, GLTF**

Fig A4, Formato dei file di Artwork ammessi da Open Sea

A.5 Minting

Una volta completati tutti i passaggi non rimane che *coniare* la nostra opera.

Il processo è molto semplice ma ovviamente richiede un costo, quello del carburante (GAS). MetaMask offre già il prezzo consigliato, sulla base della mole di lavoro che la rete deve elaborare, e sul prezzo corrente di mercato dell'energia. Questo prezzo consigliato dovrebbe assicurarci che il Minting avvenga in meno di 30 secondi. Arbitrariamente si può scegliere di spendere di meno, ma senza la certezza delle tempistiche di inserimento del nostro NFT sulla rete.

L'NFT è pubblicato e disponibile allo scambio.

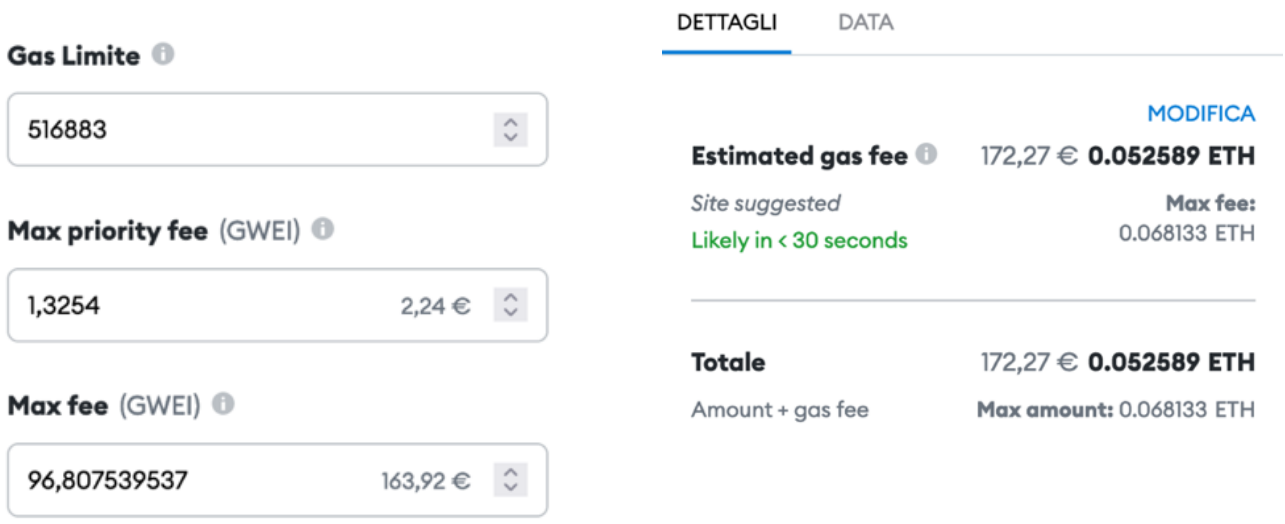


Fig A5, Screenshot UI Metamask per il pagamento del GAS e relative priorità

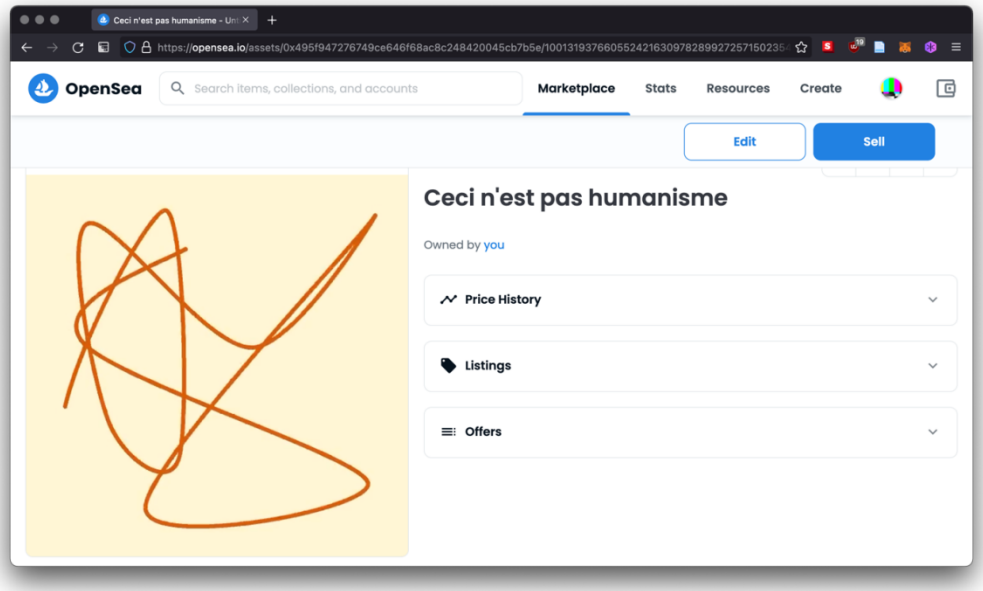


Fig.A6, L'Artwork dell'esempio su OpenSea

ALLEGATO: CODICE PROCESSING.

```
float margin = 50.0;
PMatrix3D crb = new PMatrix3D();
float curveTightness = 0.01;
int count = 20;
int draw = 250;
float animRate = 0.001;
PVector[] points;
PVector[] anim;
boolean closedLoop = true;
float rStrike = random(0,255);
float gStrike = random(0,255);
float bStrike = random(0,255);

void setup() {
  size(600, 600, P2D);
  strokeCap(ROUND);
  strokeJoin(ROUND);
  curveTightness(curveTightness);
  catmullBasis(curveTightness, crb);

  points = new PVector[count];
  for (int i = 0; i < count; ++i) {
    points[i] = new PVector();
  }

  anim = new PVector[draw];
  for (int i = 0; i < draw; ++i) {
   anim[i] = new PVector();

  }

  randomizePoints();
}

void mouseReleased() {
  if (mouseButton == LEFT) {
    randomizePoints();
     rStrike = random(0,255);
gStrike = random(0,255);
 bStrike = random(0,255);
  }
  if (mouseButton == RIGHT) {
    // closedLoop = !closedLoop;
    looping =  !looping;
  }
}

void draw() {

  surface.setTitle(nfs(frameRate, 1, 1));

  float t = (frameCount * animRate);
  t -= floor(t);

  background(#fff7d5);
  noFill();
  stroke(#fff7d5);
  strokeWeight(random(2.5,3.5));

  beginShape();
  for (PVector p : points) {
    curveVertex(p.x, p.y);
  }

  if (closedLoop) {
    curveVertex(points[0].x, points[0].y);
    curveVertex(points[1].x, points[1].y);
    curveVertex(points[2].x, points[2].y);
    endShape(CLOSE);
  } else {
    endShape(CLOSE);
  }

  strokeWeight(random(6.5,7.5));
  stroke(rStrike,gStrike,bStrike);

  PVector prev = points[1];
  for (int i = 0; i < draw; ++i) {
    float prc = i / (draw - 1.0);
    float sclprc = t * prc;
    PVector a = anim[i];
    curvePoints(crb, closedLoop, points, sclprc, a);
    line(prev.x, prev.y, a.x, a.y);
    prev = a;
  }
}


void randomizePoints() {
  for (PVector p : points) {
    p.set(
      random(margin, width - margin),
      random(margin, height - margin));
  }
}

PVector curvePoints(
  PMatrix3D cb,
  boolean closedLoop,
  PVector[] pts,
  float t,
  PVector target) {

  int len = pts.length;
  float tScaled = 0.0;
  int i = 0;

  PVector a;
  PVector b;
  PVector c;
  PVector d;

  if (closedLoop) {

    tScaled = (t - floor(t)) * len;
    i = (int) tScaled;
    a = pts[mod(i, len)];
    b = pts[mod(i + 1, len)];
    c = pts[mod(i + 2, len)];
    d = pts[mod(i + 3, len)];

  } else {

    if (t <= 0.0) {
      return target.set(pts[1]);
    }

    if (t >= 1.0) {
      return target.set(pts[len - 2]);
    }

    tScaled = t * (len - 3);
    i = (int) tScaled;
    a = pts[i];
    b = pts[i + 1];
    c = pts[i + 2];
    d = pts[i + 3];
  }

  return curvePoint(cb, a, b, c, d, tScaled - i, target);
}

PVector curvePoint(
  PMatrix3D cb,
  PVector a,
  PVector b,
  PVector c,
  PVector d,
  float t,
  PVector target) {

  if ( target == null ) {
     target = new PVector();
  }

  float tt = t * t;
  float ttt = tt * t;

  float acoeff = ttt * cb.m00 + tt * cb.m10 + t * cb.m20 + cb.m30;
  float bcoeff = ttt * cb.m01 + tt * cb.m11 + t * cb.m21 + cb.m31;
  float ccoeff = ttt * cb.m02 + tt * cb.m12 + t * cb.m22 + cb.m32;
  float dcoeff = ttt * cb.m03 + tt * cb.m13 + t * cb.m23 + cb.m33;

  return target.set(
    a.x * acoeff + b.x * bcoeff + c.x * ccoeff + d.x * dcoeff,
    a.y * acoeff + b.y * bcoeff + c.y * ccoeff + d.y * dcoeff,
    a.z * acoeff + b.z * bcoeff + c.z * ccoeff + d.z * dcoeff);
}

public PMatrix3D catmullBasis(float s, PMatrix3D target) {

  if ( target == null ) {
    target = new PMatrix3D();

  }

  float u = 1.0 - s;
  float th = (s - 1.0) * 0.5;
  float uh = u * 0.5;
  float v = (s + 3.0) * 0.5;

  target.set(
    th, v, -v, uh,
    u, ( -5.0 - s ) * 0.5, s + 2.0, th,
    th, 0.0, uh, 0.0,
    0.0, 1.0, 0.0, 0.0);

  return target;
}

int mod(int a, int b) {
  int result = a - b * ( a / b );
  return result < 0 ? result + b : result;
}
```

Ringraziamenti

Questo traguardo è stato frutto di un lungo e tortuoso percorso, molte persone volenti o nolenti hanno contribuito in qualche modo all'essere arrivato fino a qui, cosa non semplice e non scontata dati i miei innumerevoli incidenti di percorso. Quindi in ordine alfabetico ma non di importanza, senza distinzione tra chi ha dato supporto morale o produttivo, o anche solo chi mi ha fatto trovare nuove idee.:

Ángela G.
Angelo D.
Bartolomeo V.
Benedicta L.
Blu B.
Carlotta P.
Carlotta R.
Cecilia M.
Costanza S.
Edoardo A.
Edoardo R
Elena B.
Elena F.
Eli A.
Elisabetta O.
Emanuele P.
Emilia A.
Eugenio C.
FabriceM.
Gemma N
Giacomo B.
Giacomo R.
Gilles S.
Giovanni M.
Ilaria G
Jasmine J.
Joy S.
Laura B.
Lorenzo M.
Luca L.
Marco F.
Maria Vittoria V.
Marina P.
Marta D.
Martina S.
Matteo R.
Mattia M.
Michele R.
Monica M.
Monica S.
Nicolò C.
Ombra
Riccardo A.
Rocìo M.
Sara C.
Sarah R.
Silvia C.
Tommaso L.
Veronica C.
Virginia J.