UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea triennale in Economia e Commercio

L'EVOLUZIONE DELLE CRYPTOCURRENCIES: DAL BITCOIN A CHIA LA MONETA ECOSOSTENIBILE

.....

THE EVOLUTION OF CRYPTOCURRENCIES: FROM BITCOIN TO CHIA THE ECO-SUSTAINABLE CURRENCY

Relatore:
Prof.ssa Camilla Mazzoli

Rapporto Finale di:
Giacomo Borini

Anno Accademico 2021/2022

INTRODUZIONE

Questa tesi è incentrata sul tema delle cryptocurrencies, in particolare sulla loro evoluzione nel tempo, analizzando le principali caratteristiche, le funzioni applicative e l'impatto che questa tecnologia sta avendo nel nostro mondo.

Nel primo capitolo verrà approfondita la nascita di questa tecnologia e i suoi concetti principali, verrà inoltre analizzato l'impatto ambientale dovuto al consumo elettrico di Bitcoin. Nei capitoli successivi verrano analizzati i successivi tentativi di innovazione con l'analisi di Ethreum e Chia, due alternative che si sono posto l'obbiettivo di abbatrere il consumo energetico tipico delle cryptocurrencies.

Saranno presenti degli approfondimenti riguardanti gli Smart Contract, strumenti in grado di cambiare radicalmente le intereazzioni economiche e non fra diversi soggetti, la blockchain, il principo su cui si basa la sicurezza e il funzionamento delle cryptocurrencies, e l'impatto ambientale legato al metodo di convalida.

Ho deciso di trattare questo argomento perchè ritengo che questo campo sia ancora ai primi stadi di sviluppo e che in futuro le applicazione pratiche di questa tecnologia troverranno una larga diffusione.

L'obbiettivo di questa tesi è di analizzare le soluzioni proposte dalle cryptocurrencies di recente creazione per abbatere i consumi elettrici senza intaccare la sicurezza e il corretto funzionamento della Blockchain.

Indice

CAPITOLO 1

Cryptocurrencies: definizione e Blockchains

1.1 Definizione di Cryptocurrencies

Cryptovaluta: Strumento digitale impiegato per effettuare acquisti e vendite attraverso la crittografia, al fine di rendere sicure le transazioni, verificarle e controllare la creazione di nuova valuta; denaro, moneta virtuale.

Questa è la definizione che si può trovare nel sito della Treccani se si cerca di capire cosa sono le *cryptocurrencies* ma per capire davvero cosa sono e cosa rappresentano bisogna analizzare la sua storia e la tecnologia che la caratterizza.

Nel corso della nostra storia i mercati finanziari e gli strumenti a esso legati si sono evoluti per far fronte a nuove esigenze e per facilitare gli scambi commerciali. Il principale strumento utilizzato per intermediare lo scambio di beni è la moneta. Per ogni periodo storico c'è stata un'evoluzione tecnologica che ha permesso nuove tipologie di pagamento di contribuire in quanto a velocità e sicurezza nella transazione sui mercati. Le *cryptocurrencies* rappresentano uno degli strumenti più recenti che più hanno influenzato il modo di concepire la moneta e le transazioni ad essa legata.

Le *cryptocurrencies* sono da considerarsi a tutti gli effetti come una moneta digitale che nasce dall'esigenza del mercato di trovare un nuovo strumento completamente digitale che sia allo stesso tempo sicuro e facile da utilizzare, infatti oltre ad essere impossibile da contraffare essa può essere scambiata liberamente da qualsiasi luogo ad un altro senza nessun tipo di limitazione. (Bunjaku et al, 2017)

La principale caratteristica che accomuna le monete digitali è la Blockchain che garantisce la sicurezza e il funzionamento della stessa, tutte le altre caratteristiche sono definite alla nascita della moneta e possono differenziarsi notevolmente fra le tante che sono al momento in circolazione.

1.2 Definizione di Blockchain

Il termine *Blockchain* è stato introdotto per la prima volta dal w*hite paper* di Bitcoin, si utilizza per identificare in modo generico qualsiasi forma di tecnologia DLT (Distributed Ledger Technology). Una definizione di questo meccanismo viene data anche dal legislatore che con la legge di conversione n.12, 11 febbraio 2019 in riferimento al decreto 14 dicembre 2018 definiscono come "tecnologie basate su registri distribuiti":

" tecnologie e protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato

su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili."

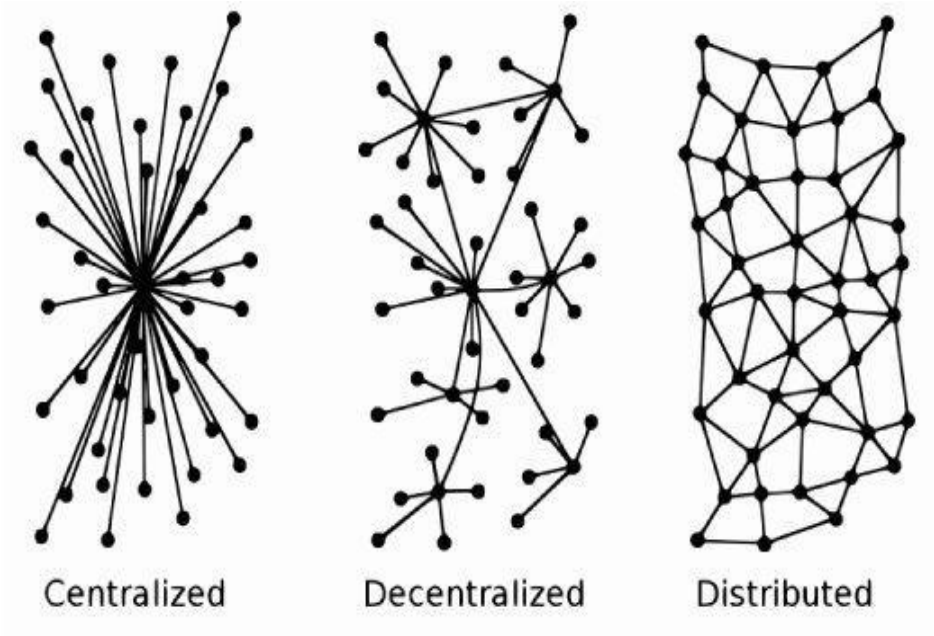
La tecnologia *Blockchain* viene considerata da molti come un'innovazione tecnologica *disruptive,* che rivoluzionerà la nostra società. (The Economist, 2015)

La teoria dietro alla *Blockchain* nasce dalla volontà di creare un sistema che non necessiti di interventi da parte di terzi e possa basarsi interamente sullo scambio diretto fra i singoli utilizzatori della *cryptocurrencies.*

Si può quindi definire il concetto di Blockchain come un database distribuito e decentralizzato contenente blocchi sequenziali, collegati tra loro attraverso la crittografia, questo database contiene al suo interno tutte le informazioni inerenti agli scambi del sistema e vengono successivamente condivise fra tutti gli utilizzatori del sistema.

Il sistema viene quindi definito come distribuito in quanto il registro degli scambi è pubblico, verificabile e presente contemporaneamente su più di un computer, in questo modo il sistema viene decentralizzato e si formano dei Nodi che contribuiscono alla stabilità e sicurezza del sistema.

Ogni nodo presente nel sistema porta dentro di sé una copia completa del registro degli scambi, anche se un nodo dovesse fallire (*single point of failure*) il sistema rimarrebbe invariato visto la moltitudine di nodi presenti nel sistema. (Sultan, Ruhi e Lakhani, 2018)



Fonte: Ehmke C., Blum F. e Gruhn V. (2019)

Tutte le transazioni presenti nella Blockchain, vengono registrate in un Ledger, ovvero un registro che verifica l'effettiva proprietà e la possibilità di trasferire tale proprietà.
Questo registro è di tipo open-source, ossia è disponibile per tutti e può essere modificato o consultato semplicemente scaricando l'apposito software dedicato.
Ogni utente che scarica una copia del registro diventa anche un nodo della rete e contribuisce alla decentralizzazione e alla distribuzione della stessa, ciò comporta la mancanza di un registro ufficiale e ogni singolo nodo ha lo stesso livello di credibilità degli altri.
Un problema che potrebbe affliggere questo tipo di sistema è il Double-spending ovvero la possibilità che vengano spesi in contemporanea gli stessi asset in più transazioni. Quando queste transazioni raggiungono la Blockchain solo una verrà validata, infatti il sistema funziona attraverso il meccanismo della maggioranza ovvero la transazione che riceverà per prima la maggioranza delle registrazioni diverrà parte della Blockchain mentre le altre verranno considerate invalide o semplicemente non verranno riconosciute.
In conclusione, la Blockchain funziona esattamente come una catena che ad ogni transazione o scambio aggiunge un anello alla catena e grazie alla condivisione della stessa tra più nodi è possibile garantire la sicurezza e rendere vano qualsiasi tipo di manipolazione. (Sultan, Ruhi e Lakhani, 2018)

1.3 La Prima crypto: Il Bitcoin

Il nome Bitcoin compare per la prima volte nel 2008 con la registrazione del dominio Bitcoin.org, nasce dall'unione di due progetti: B-money che rappresentava un sistema decentralizzato di pagamenti e Bit-gold una cryptocurrencies che sfruttava dei meccanismi molti simili a Bitcoin. Nell'ottobre del 2008 venne pubblicato il paper "*Bitcoin A peer-to-peer electronic cash system*" a cura Satoshi Nakamoto, uno pseudonimo di un programmatore anonimo, successivamente a questa pubblicazione viene lanciata la moneta vera e propria nel 2009 con la creazione del primo blocco di monete del valore di 50 BTC, denominato Genesis block. (Surda, 2014)
Il nome Bitcoin con la prima lettera maiuscola viene utilizzato per indicare la rete che gestisce la Blockchain mentre il bitcoin è la moneta vera e propria, nonostante il nome sia lo stesso questa distinzione serve per definire meglio l'oggetto trattato.
Il sistema dei bitcoin utilizza una rete peer-to-peer con una tecnologia simili a quella del protocollo Torrent, questa rete non ha una gerarchia o una linea di trasmissione dei dati unica bensì ogni nodo può operare come client o come server, in sostanza si tratta di un sistema in cui tutti possono ricevere dati e trasmetterli. Questi nodi possono essere smartphone, computer, server o qualsiasi sistema sia in grado di far funzionare il software su cui opera il Bitcoin. Questa rete non ha quindi

un sostegno fisico, i bitcoin possono essere conservati in appositi wallet elettronici installati nei dispositivi oppure digitali e disponibili solo online da alcune piattaforme che offrono questo tipo di servizio. (Gervis, 2014)

Il Bitcoin sfrutta tre fattori per poter funzionare: la Blockchain per tenere un registro delle transazioni, la criptografia per la gestione di tutti gli aspetti funzionali e il mining per creare nuova moneta e verificare le transazioni.

Nel capitolo precedente abbiamo trattato il problema del double spending, ovvero il problema derivato dall'ipotetica possibilità di inviare due volte lo stesso asset, per questo motivo ogni scambio deve essere prima convalidato dal sistema (Karame,2012). Gli utenti che sono dentro la rete mettono a disposizione la potenza di calcolo dei loro computer per convalidare le transazioni. Questi utenti sono detti anche miner, si occupano di organizzare le transazioni in blocchi e di convalidare. Ogni volta che un miner convalida un blocco, questo viene trasmesso alla rete in modo che possa essere aggiunto alla fine della Blockchain; in cambio il miner ottiene una ricompensa in bitcoin di nuova emissione. L'ammontare di questa ricompensa viene stabilito dal protocollo ed è stato programmato per dimezzare le ricompense ricevute ogni quattro anni, proprio per evitare che i bitcoin in circolazione superino i 21 milioni in circolazione. Il protocollo in questione è noto anche come Proof of Work (PoW), esso rende la convalida delle transazioni come una lotteria, più la potenza computazionale dell'utente è elevata più saranno le possibilità per quest'ultimo di vincere la ricompensa per la convalida della transazione.

Inoltre, il software che sta alla base del sistema Bitcoin è definito come Open Source, ovvero è privo di copyright, qualsiasi persona è libera di analizzarlo e modificarlo per contribuire al suo sviluppo. (guttmann, 2014)

1.4 Il costo del Mining: il Prof of Work

Come scritto già in precedenza la maggior parte delle Cryptocurrencies non hanno un'autorità centrale, ma sono dei sistemi decentralizzati e distribuiti, di cui fa parte anche il Bitcoin, pertanto necessità di un sistema particolare per funzionare. Le transazioni non possono considerarsi sicure finché non vengono confermate e aggiunte nella Blockchain, una volta che questo processo viene confermato diventa impossibile per chiunque modificarle. (O'Dwyer e Malone, 2014)

La combinazione del mining e del Proof of Work permette il corretto funzionamento della rete e attraverso dei soggetti detti anche "miner" avviene un processo di verifica delle transazioni. Questo processo viene eseguito attraverso la risoluzione di un processo di risoluzione di un problema matematico la cui difficoltà aumenta progressivamente. Per ogni transazione nasce un nuovo problema e tutti i miner entrano in competizione tra loro per riuscire a risolverlo: maggiore è la

potenza computazionale a disposizione maggiori sono le probabilità di vincere la ricompensa. (Wu, Pandey e Dba, 2014)

Per ogni problema risolto viene aggiunto un nuovo blocco alla Blockchain e il premio per l'aggiunta di questo blocco si divide in due parti: la prima consiste in una data quantità di bitcoin di nuova emissione, la seconda invece è composta dalle commissioni corrisposte dall'utente che ha richiesto la verifica della transazione. (Taylor, 2017)

Il problema matematico consiste in una prova criptografica che richiede un grosso dispendio di potenza computazionale e di conseguenza anche di energie elettrica. La difficoltà del problema viene deciso ogni 2016 blocchi, l'algoritmo aumenta la difficoltà ogni volta che questi 2016 blocchi vengono processati in meno di 10 minuti. Nella pratica ogni qual volta si riesca a completare un ciclo in meno di 2 settimane il protocollo aumenta la difficoltà dei problemi.

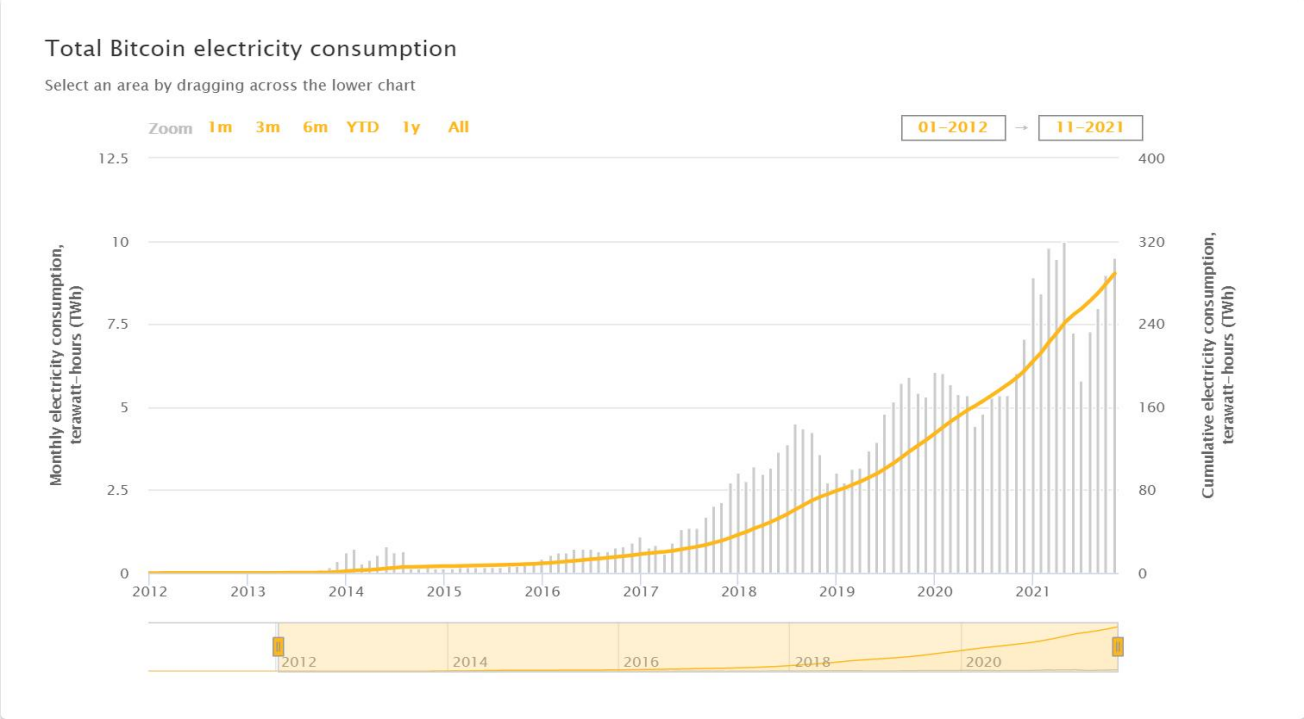
Una volta che il miner pensa di aver trovato la soluzione la comunica la soluzione e se la risposta data è corretta riceva la ricompensa che risulta decrescente nel tempo. Infatti la ricompensa è stata programmata per dimezzarsi ogni qual volta vengano raggiunti i 210.000 blocchi finché non si esauriranno completamente una volta raggiunti i 21 milioni di unità. Sorpassato questo limite le ricompense saranno così infinitesimali da risultare inesistenti e i miner verranno ricompensati solo con le commissioni. (Ma, Gans e Tourky, 2018)

Molteplici criticità sono emerse negli ultimi anni per quanto riguarda il mining di bitcoin, in particolare dovute all'ingente consumo elettrico della rete, che ha portato molti stati a valutare azioni per impedire o limitare questa moneta.

In particolare, la problematica è legata alla modalità di auto regolazione della moneta che ne aumenta la difficoltà andando così a spingere i miner a potenziare le loro attrezzature per rimanere al passo con la difficoltà, questo ha portato a una costante aumento dell'inquinamento legato alla rete Bitcoin

L'aspetto che viene maggiormente criticato di Bitcoin è proprio la sua necessità sempre maggiore di elettricità per funzionare: infatti, come sopra riportato, l'algoritmo è stato programmato per aumentare la difficoltà dei problemi man mano che la potenza di calcolo dei miner diventa maggiore. Risulta quindi che con l'aumentare dell'interesse del mondo della finanza in Bitcoin, quindi anche del suo valore, i miner abbiano optato per aumentare la loro capacità di estrarre moneta portando quindi ad una sorta di corsa all'oro digitale.

L'università di Cambridge ha creato il "" proprio per monitorare questo consumo, questo dato è ormai da diversi anni in aumento e sta raggiungendo livelli paragonabili ad interi settori industriali.



Fonte: https://ccaf.io/cbeci/index

Questi livelli sono stati raggiunti con l'innalzamento del valore dei bitcoin che ha comportato un maggior guadagno per i miner. Questo ha portato ad una maggiore competizione e ad un maggior dispendio energetico.

Fonte: https://www.google.com/finance/

Il valore di un bitcoin rimane direttamente collegato al consumo della rete fintanto che i miner verranno ricompensati sulla base della velocità e della potenza di calcolo.
Tutte le monete che utilizzano il Proof of Work condividono questa caratteristica e per tanto si possono considerare inefficienti man mano che il loro valore sale.

CAPITOLO 2

Evoluzione delle Cryptocurrencies

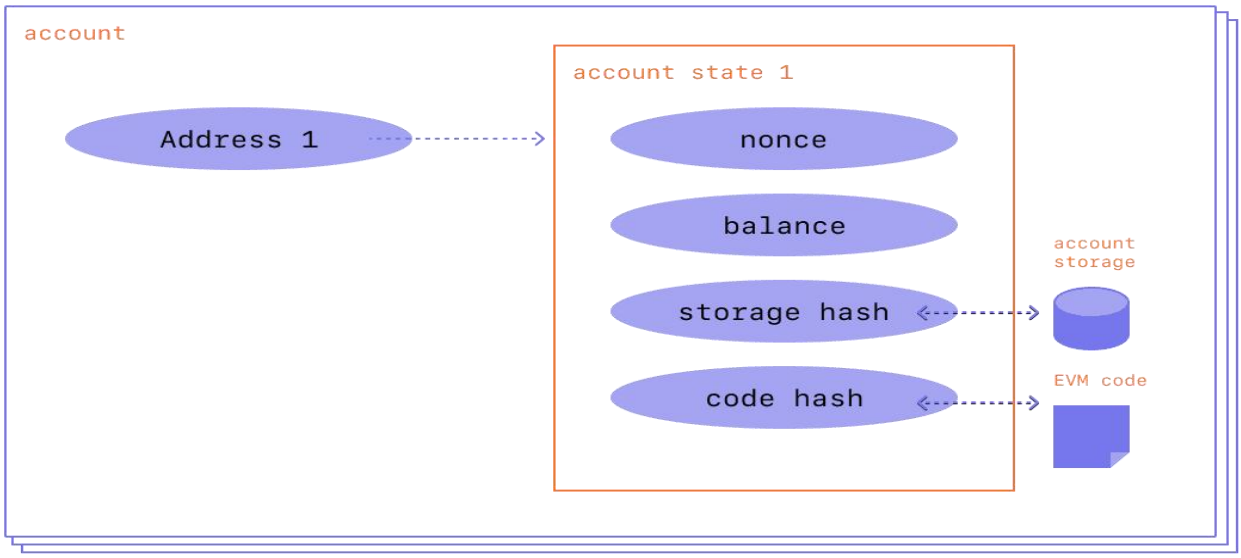
2.1 Ethereum

Ethereum è una piattaforma open source che permette la creazione di token e smart contract, ovvero applicazioni dove gli utenti possono interagire con diversi tipi di sistemi, tra cui: sistemi sociali, interfacce di gioco e sistemi finanziari in cui ogni partecipante contribuisce con il proprio nodo all'esecuzione in maniera peer to peer. Lo scopo di questa piattaforma è quello di facilitare lo sviluppo di Blockchain basate sullo stesso protocollo ma con regole diverse, infatti Ethereum è anche il nome del linguaggio Turing completo che serve pe programmare in tale piattaforma.

Il processo di creazione di Token e smart contract è alla base della piattaforma: si può dire infatti che Ethereum sia diventato il punto di partenza di molti progetti e che molti sviluppatori, incentivati dall'idea di creare una rete di cryptocurrencies, abbiano iniziato a sviluppare i loro progetti basandosi sulla rete Ethereum. (Buterin , Wood, Wilcke, & Altri, 2021)

Nella pratica, Ethereum è stata sviluppato partendo dalla stessa tecnologia del Bitcoin, la Blockchain, con il presupposto di renderla adattabile a qualsiasi altra applicazione, ognuna delle quali può essere modellata con regole arbitrarie, resa sicura e scambiata, garantendo lo stesso livello qualitativo. Esattamente come per il Bitcoin non è presente nessuna autorità centrale o banca a gestire la rete, ogni utente ha il pieno controllo delle proprie informazioni personali, della propria identità e dei propri capitali.

La piattaforma Ethereum è composta da "account, essi sono composti da un indirizzo delle dimensioni di 20 byte, le transazioni che intercorrono fra questi account sono principalmente trasferimenti diretti di valore e di informazioni. Gli account sono composti da quattro campi:



Fonte: Buterin V (2014)

1) Il Nonce: è un contatore che indica il numero di transazioni inviate dall'account, se ad assicurarsi che ogni transazione venga eseguita una sola volta.
2) Il Balance: il numero di ether posseduto dall'account.
3) Storage Hash: che rimane vuoto di default.
4) Code Hash: o Contract Code, è presente unicamente se la tipologia dell'indirizzo lo consente

Esistono due tipologie di account: account di contratto, sono account interni alla piattaforma che funzionano attraverso l'Ethereum virtual machine (EVM), e gli account esterni, controllati da chiavi private.

Gli account esterni non presentano il Code Hash, sono costituiti da due "chiavi", una pubblica e una privata, la prima serve a identificare l'account nella piattaforma per ricevere messaggi e la seconda serve invece come "password" e serve per mettere la convalida delle transazioni. Gli account di contratto sono invece completamente autonomi e liberi dal controllo esterno, infatti reagiscono unicamente a messaggi esterni, attivandosi e scrivendo nello storage interno limitandosi poi a spedire nuovi messaggi o crenando a sua volta nuovi contratti.

Le "transazioni" sulla piattaforma Ethereum vengono gestiste attraverso un sistema a consumi che sfrutta due variabili conosciute come "STARGAS" e "GASPRICE", questo sistema serve a prevenire la possibilità di loop infiniti o di spreco di capacità computazionale del sistema. Ogni account che intende eseguire una transazione deve decidere la quantità di gas limite a disposizione rappresentata dallo "STARGAS" e successivamente decidere che prezzo pagare per ogni unità di "gas" consumata ovvero il "GASPRICE". La combinazione dei due fattori determina la massima commissione che l'account è disposto a pagare per eseguire la transazione. Il "gas" utilizzato da Ethereum viene rappresentato dal token ETH e coincide con uno o più step computazionali necessari a risolvere la transazione, con questo sistema si spinge a pagare in modo proporzionale alle risorse consumate per lo scambio di dati fra gli account. Questo sistema lascia aperta la possibilità che il "gas" si esaurisca prima del completamento della transazione: se ciò accade la transazione verrà trattata come un'eccezione e la transazione sarà nulla e tutto il "gas" consumato però non verrà restituito al destinatario. Qualora il destinatario rimanga senza "gas" il mittente può decidere di usare il suo "gas" per gestire l'eccezione e completare la transazione. (Buterin V, 2014)

2.2 Gli Smart contract e i Token

Con il termine "Smart contract" si intende la trasposizione in codice di un contratto per automatizzare il processo di creazione e verifica dello stesso. Questi contratti hanno la capacità di auto-esecuzione, ovvero nel momento che le due parti concordano modalità e clausole il codice si auto-esegue per redigere in autonomia il contratto, e con l'approvazione delle parti coinvolte si ha la convalida del contratto. Questa nuova tipologia contrattuale si distingue per l'assenza dell'intervento umano, se non in fase di stesura del codice, quindi è privo di interpretabilità e per tanto deve essere basato su descrizione precise e inequivocabili.

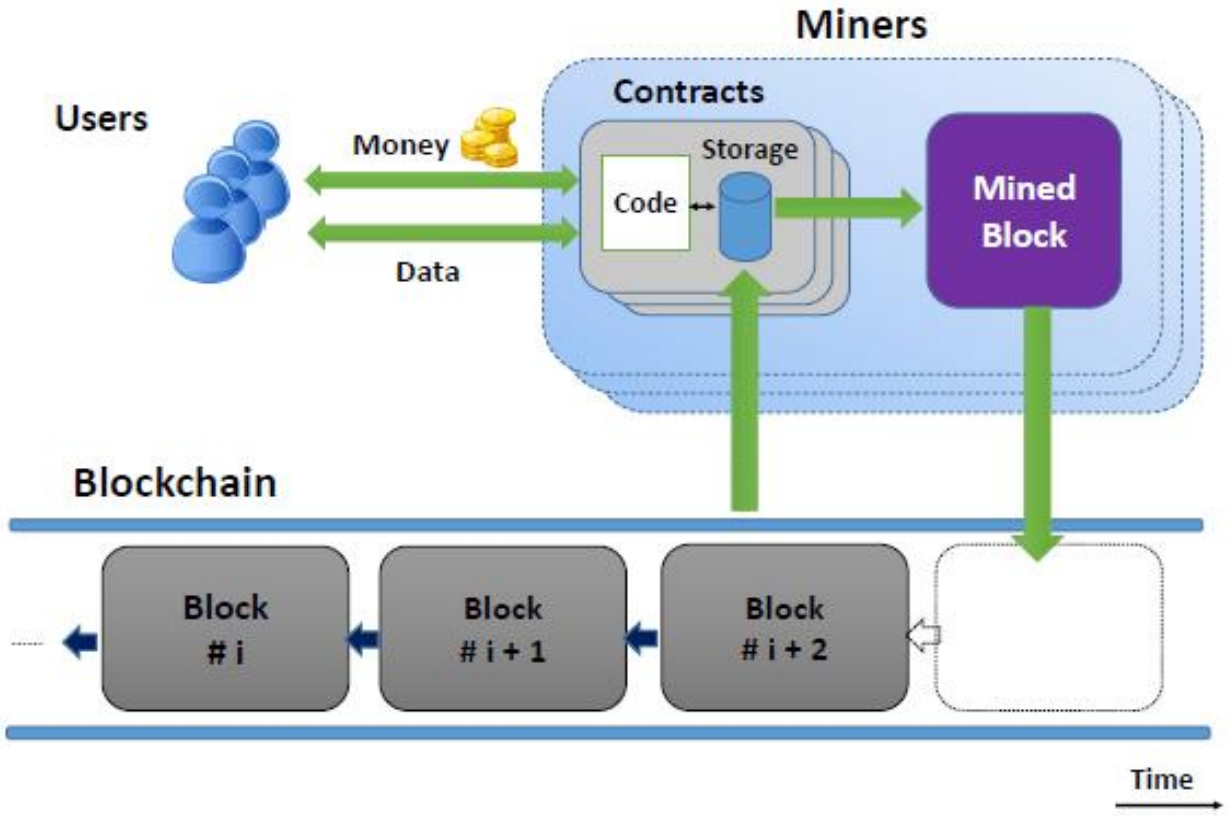
Nel quadro giuridico nazionale è stata emanata una legge (Legge n. 12/2019, G.U. 12/02/2019) che ha reso gli "Smart contract" al pari dei contratti scritti.

"Si definisce "Smart Contract" un programma per elaboratore che opera su Tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli Smart Contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia Digitale con linee guida da adottarsi entro 90 giorni dall'entrata in vigore della legge di conversione del decreto-legge"

https://www.gazzettaufficiale.it Art 8 ter

Gli Smart Contract sono stati teorizzati prima dell'avvento della Blockchain ma necessitavano di un sistema che potesse garantire la loro imparzialità ed immutabilità: hanno quindi trovato una reale applicazione soltanto negli ultimi anni. Questi contratti posso essere sviluppati su diverse piattaforme blockchain, al momento la più diffusa è Ethereum, ognuna offre diverse possibilità e limiti che vengo stabiliti dalla struttura della blockchain nella quale vengono programmati.

La piattaforma di Ethereum fa degli smart contract il suo obbiettivo primario sin dalla sua nascita, grazie al linguaggio di programmazione Solidity permette di creare istruzioni complesse come clausole ramificate, loop e limiti personalizzati. Tramite la piattaforma gli smart contract vengo creati come account indipendenti e distribuiti nella rete dando così la possibilità agli utenti di interagire con loro inviandogli transazioni che seguano la programmazione dello smart contract.



Fonte: Eze, Eziokwu, Okpara (2017)

Ogni transazione eseguita con un Contract account necessità di un evento che attivi il codice all'interno dell'account, solitamente un invio di fondi, per permettere la convalida del contratto e la sua registrazione nella blockchain. Questa tecnologia ha permesso la nascita di nuovi strumenti finanziari i più diffusi sono i Token, possono essere generati dagli smart contract in cui bisogna stabilire tutte le caratteristiche fondamentali, come ad esempio: il numero massimo dei token in circolazione, chi è autorizzato a scambiarli e le regole di accesso. (Buterin , Wood, Wilcke, & Altri, 2021)

I Token vengono utilizzati all'interno della blockchain per diversi scopi, possono essere utilizzati per scambiare denaro, quote di una società o asset in genarle. Si possono dividere in due principali categorie: i fungible Token in cui tutti token appartenenti alla stessa tipologia sono identici e rappresentano lo stesso valore come se fossero banconote o azione di una società, invece i non fungible-token (NFT) differiscono dai primi per il loro individualismo. Per quanto possano sembrare simili spesso contengono elementi molto precisi che differiscono in base al token.
Recentemente sono stati utilizzati per vendere opere d'arte digitalizzate come veri e propri certificati di proprietà ma vengo anche utilizzati per progetti di tracciabilità o per la gestione dell'identità digitale e il voto elettronico.

Nella piattaforma Ethereum è possibile creare dei token senza la necessità di creare una Blockchain dedicata dando così la possibilità di conservare i token in qualsiasi wallet compatibile con Ethereum; questa funzionalità ha portato alla creazione di configurazioni standard che contengono i valori e le finalità di un Token, gli Ethereum Request for Comment o in breve ERC.
A seconda dello scopo del Token si possono scegliere diversi standard ma i più popolari sono l'ERC-20, L'ERC-721 e l'ERC-777. Questi standard sono noti agli utenti che possono riconoscere le diverse tipologie e sapere in anticipo tutte le caratteristiche e le funzioni dei Token. (Buterin , Wood, Wilcke, & Altri, 2021)

- ERC-20: è lo standard più comune per quanto riguarda i Fungible Token oltre ad essere tutti identici permette di stabilire diversi parametri come il totale in circolazione o lo scopo, infine permette anche lo scambio degli stessi
- ERC.721: è un'interfaccia per la creazione dei non fungible token utilizzata principalmente per opere d'arte o diritti d'autore in generale.
- ERC 777: è uno standard di fungible token più avanzato che consente interazioni più complesse mirate a garantire uno sviluppo più trasparente e qualissimamente superiore agli standard più classici

2.3 Il costo del mining: il Proof of Stake

Il primo sistema di mining è stato il Proof of Work, che inizialmente è risultato un sistema efficiente che dava la possibilità a tutti, con il proprio computer, di partecipare e di contribuire al funzionamento della rete. Con il tempo questo sistema ha raggiunto i suoi limiti, la potenza computazionale richiesta per elaborare transazioni ha reso la pratica possibile solo attraverso la concentrazione di molte attrezzature e capitali andando così a minare lo scopo iniziale delle cryptocurrencies, ovvero una suddivisione del compito fra tutti gli utenti. In termini di consumo di risorse si è arrivati ad una situazione insostenibile, infatti tutte le cryptocurrencies più recenti hanno implementato diversi sistemi e superato a livello tecnologico il Proof of work.
Il Bitcoin ha provato in più occasioni a cambiare sistema di convalida delle transazioni ma senza riuscirci, in tutti questi casi si è trattato di Hard Fork, ovvero una presa di posizione di alcuni utenti per tentare di stabilire una nuova Blockchain con nuovi protocolli. La piattaforma Ethereum invece è stata creata per essere sempre aggiornata e aperta al cambiamento.
Con il passare del tempo si sono fatti evidenti diversi problemi, i principali sono il protocollo Proof of Work, da cui deriva anche il problema della scalabilità della Blockchain, e la privacy delle transazioni.

Ethereum per perseguire il suo scopo originale e mantenersi in linea con altre cryptocurrencies di più recente pubblicazione ha iniziato lo sviluppo di Ethreum 2.0, un progetto che mire attraverso diverse modifiche ad alleviare i problemi che affliggono la piattaforma: questo insieme di aggiornamenti prende il nome di "Serenity". (etherevolution.eu, 2019)

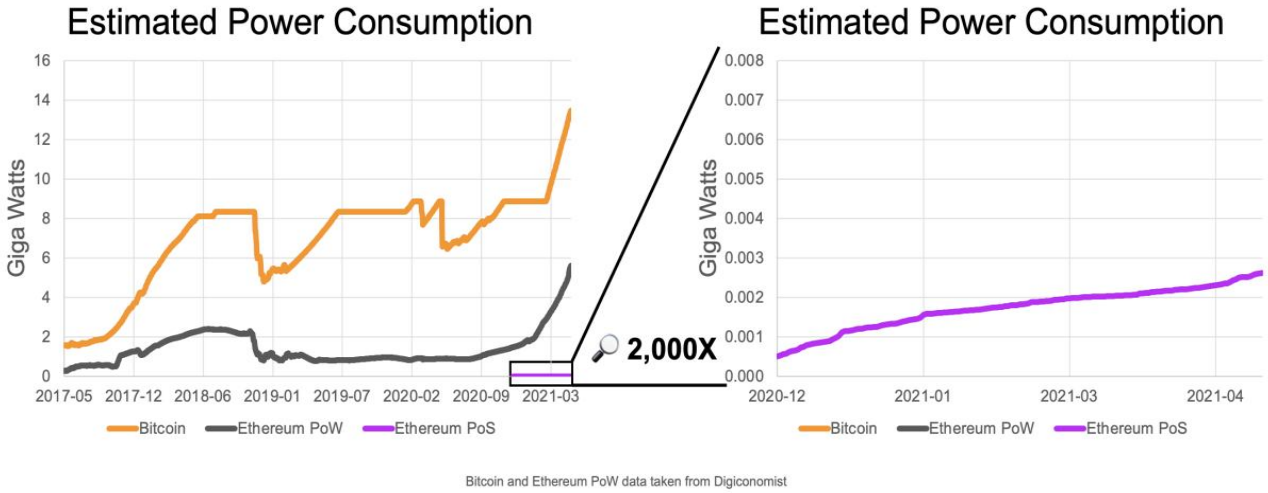
La piattaforma di Ethreum aveva pubblicato, nel 2019, una roadmap che riassumeva le 3 fasi per aggiornare e modernizzare la rete, queste fasi servivano per evitare uno shock fra gli utenti dovuto al drastico cambio all'interno della rete.

Fonte: https://etherevolution.eu/

Il piano originale prevedeva il completamento della transizione nell'anno 2022, ma a causa di diverse criticità la prima e la seconda fase sono state rimandate al 2023. Attualmente la piattaforma è ancora alla fase zero del programma, ovvero all'introduzione e allo sviluppo della Beacon Chain, una blockchain parallela che andrà a gestire e coordinare il registro dei validatori attraverso il protocollo Proof of stake.

Il Proof of Stake è un meccanismo già implementato in altre cryptocurrencies e ha già dato prova di essere un'alternativa valida in termini di sicurezza ed ecosostenibilità. La differenza principale che separa il Proof of work dal Proof of Stake risiede nel sistema di risoluzione dei blocchi; per il Poof of Work è necessaria la risoluzione di problemi matematici attraverso capacità di calcolo mentre per il Proof of Stake i blocchi vengono risolti dai cosiddetti "validatori". Il meccanismo del Proof of Staking si basa sull'attivazione dei validatori, ovvero utenti che eseguono uno staking di cryptocurrencies al fine di fornire una garanzia per il loro ruolo all'interno della rete. Ogni

validatore può essere scelto per creare o controllare e confermare i blocchi della blockchain, dunque maggiore sarà la dimensione dello staking, maggiore sarà la probabilità di essere scelti. Lo staking serve come strumento di controllo sui validatori: per esempio, qualora un validatore vada offline per non validare una transazione o vi sia qualsiasi tipo di operazione in malafede il validatore perderà parte o addiritura tutto il proprio stake. Questo tipo di protocollo nasce dall'esigenza di trovare metodi alternativi al Proof of work i cui costi, in temi di hardware e elettricità, creano un limite stesso alla funzionalità delle blockchain.



Fonte: https://blog.ethereum.org/

L'applicazione di questo protocollo porterà i consumi della rete a livelli neanche comparabili a quelli iniziali della piattaforma, inoltre contribuirà a rendere molti più utenti parti attivi nella rete creando così più nodi aumentandone la sicurezza.

Il Proof of Stake non solo risulta efficace in termini di costi ma apre le porte ad un'altra funzionalità chiamata Sharding, e si tratta di un sistema attraverso il quale sarà possibile aumentare la scalabilità, ovvero aumentare il numero di transazioni eseguite in un determinata unità di tempo. Ethreum ad oggi possiede una solo blockchain nella quale vengono inseriti i blocchi alla volta in una solo linea. Questo comporta la possibilità di un rallentamento nell'esecuzione di transazioni dovuto all'elevato numero di richieste e di smart contract che operano nella piattaforma. Lo sharding va a frammentare la blockchain principale in tante "sidechain" creando così tante linee che operano in simultanea, ognuna delle quali avrà una beacon chain che si occuperà di fornire in nodi validatori e di coordinarsi con la main chain, ovvero la blockchain principale. Ogni side chain risulterà allo stesso tempo indipendente e coordinata alle altre dando così la possibilità di elaborare un maggior numero

di transazioni in termini di costi. Inoltre, nella piattaforma di Ethreum è previsto l'inserimento di 64 side chain.

Questa tipologia di protocollo permetterà di aumentare l'efficienza in termini di costi-output e di sfruttare il maggior numero di "miner" che si verranno a creare con l'applicazione del Proof of Stake. (Buterin , Wood, Wilcke, & Altri, 2021)

CAPITOLO 3

Chia la Crypto ecosostenibile

3.1 Chia

Chia è una cryptocurrency e una piattaforma nata dall'esigenza di creare un alternativa ecologica e funzionale ai vecchi modelli di cryptocurrencies . Il progetto originale è stato sviluppato dalla Chia Company, fondata nel 2017 da Bram Cohen, il lancio effettivo della blockchain è avvenuto il 19 marzo del 2021. Nonostante Chia sia solo di recente creazione sono stati resi disponibili fin da subito due documenti fondamentali per la trasparenza del progetto, il Chia's business white paper che contiene tutte le informazioni inerenti alle politiche monetarie e come la compagnia intende garantire l'imparzialità della gestione e il Chia's Green Paper che contiene tutti i dettagli tecnici sul funzionamento del protocollo e della Blockchain.

Lo sviluppo di Chia è avvenuto in un contesto completamente Opensource, nella quale un gran numero di programmatori ha partecipato e contribuito, per tanto gran parte dei codici di programmazione della piattaforma è disponibile su Github, noto sito di condivisione fra programmatori.

Il modello di Chia si basa su quello del Bitcoin, a differenza di Ethreuma che sfrutta un sistema basato sugli account come una banca, un coin set model. L'utilizzo di questo modello è stato scelto per la sua semplicità che con le giuste modifiche lo ha reso un modello altamente sicuro e semplice per l'esecuzione di smart contract, a differenza dei sistemi che utilizzano il modello di account come Ethereum e il codice che crea le monete di Chia è fortemente sandbox. Ciò aumenta la sicurezza, riduce il valore massimo estraibile (MEV) e rende il codice completamente controllabile. (Bram Cohen & Krzysztof Pietrzak, 2019)

Le principali innovazioni che ha portato Chia sono:

- Proof of Space and Time
- BLS signature
- Verifiable Dalay Function
- Clas Groups Order

Queste funzioni sono state implementate per perseguire gli obbiettivi di questa cryptocurrencies, ovvero la creazione di una blockchain a basso impatto ambientale, funzionale ad ogni tipo di operazione di validazione dei dati e con una decentralizzazione dei nodi estremamente estesa.

3.2 Le differenze con la rete Ethereum

Le principali differenze tra Ethereum e Chia non risiede negli obbiettivi delle due Cryptocurrencies: infatti entrambe si sono poste come obbiettivo l'abbattimento dell'impatto ambientale, la decentralizzazione e la funzionalità della blockchain, ma allo stesso tempo, si sono differenziati nella diversità dei modelli utilizzati. Chia ha deciso di adottare un sistema Coin Set mentre Ethereum ha un sistema Account Model. Le principali differenze fra questi due modelli si basa su quale dato viene preso in considerazione dalla Blockchain, per gli Account model si tratta del saldo disponibile, mentre per il Coin model si tratta della moneta stessa. Questa differenza comporta un cambio radicale dietro il ragionamento delle transazioni, per gli account il funzionamento è simile a quello di una banca dove si sottrare da un conto per aggiungere ad un altro. Per i Coin invece l'oggetto della transazione è la moneta stessa, infatti ogni moneta può essere spesa solo da chi possiede la chiave privata associata alla moneta. Chia ha deciso di adottare uno Coin model per ovviare ai problemi che affliggevano Ethereum, a cui la piattaforma sta cercando soluzione con il progetto Ethreum 2.0, questo modello presenta una seri di vantaggi maggiori rispetto agli svantaggi.(Bram Cohen & Krzysztof Pietrzak, 2019)

VANTAGGI

Scalabilità: In un Coin Set model il sistema di verifica è incorporato nelle singole monete per tanto nel caso in cui la chiave privata necessaria per spendere la moneta vada smarrita la moneta diventa non spendibile. Tuttavia, il sistema non ne risente, al contrario degli account che, in caso di smarrimento della chiave privata, ogni Messaggio o codice non può essere processato rischiando di creare errori a cascata nell'intera rete. In sintesi, nel Coin set model essendo ogni moneta indipendente non si rischia nessun effetto a catena e per tanto è più facile inserire funzioni di Sharding.

Privacy: Il protocollo di Chia permette di creare con facilità in nuovi account e ogni funzione rimane legate alle monete ed esse possono essere diverse fra più account grazie ai bassi costi di transazione. Nelle piattaforme che utilizzano gli account tipicamente questo comportamento viene scoraggiato da alti costi di transazione, per tanto ogni utente dispone tipicamente di un solo account.

Determinismo: Nel coin set model le monete posso essere spese una sola volta, gli smart contract vengono eseguiti dagli Smart coin e pertanto ogni contratto viene eseguito indipendentemente dando sempre lo stesso risultato. Nelle piattaforme che sfruttano gli account gli smart contract vengono eseguiti da un account, se più utenti eseguono lo stesso codice in contemporanea c'è il rischio che l'ordine di esecuzione possa influire sul risultato riducendo il determinismo.

Sandboxing: Il valore delle monete è diviso tra molte monete, aumentando il sandboxing e quindi la sicurezza. Un programma non può chiamare o influenzare un altro. Se una moneta viene hackerata, solo il proprietario di quella moneta può farsi rubare del denaro. Nei sistemi con account il valore è memorizzato all'interno di un singolo account o contratto. Più persone possono eseguire lo stesso codice di smart contract. Se un contratto viene violato, tutti coloro che partecipano potrebbero subire il furto di denaro.

Dimensione del Database: Le funzioni programmabili non sono memorizzate direttamente sulla Blockchain. Invece, le monete usano l'hashing per consentire una verifica successiva del loro contenuto. Si prevede che il database di Chia aumenterà di circa 30 GB all'anno, che è più o meno la stessa velocità di Bitcoin. Con la dimensione odierna degli hard disk risulta molto facile archiviare l'intera blockchain anche con la crescita prevista. In piattaforme come Ethereum le informazioni sull'account utente, così come i dati sulle transazioni, sono piccole. Tuttavia, gli smart contract sono archiviati sulla Blockchain per questo motivo: il database di Ethereum crescerà proporzionalmente alla diffusione del suo utilizzo, probabilmente in modo più rapido di quello di Bitcoin o Chia

SVANTAGGI

Fungibilità Monetaria: Nel coi set model le monete non possono essere "mischiate" ovvero, possono essere identificate anche se combinate tra loro, ciò significa che alcune monete potrebbero essere visualizzate in modo diverso rispetto ad altre, anche se hanno lo stesso valore. Questo è già successo con Bitcoin: a causa del suo elevato consumo di energia, alcune persone si sono rifiutate di acquistare Bitcoin che possono essere ricondotti all'estrazione mineraria dei combustibili fossili. Ciò influisce sulla fungibilità di Bitcoin perché non tutte le monete sono visualizzate allo stesso modo. Negli Account set model esiste solo il saldo di un account, quindi è difficile stabilire che alcune monete debbano essere trattate in modo diverso rispetto ad altre. Il denaro è "misto" per impostazione predefinita.

Facilità di Programmazione: La programmazione su Coin set model risulte più difficile data la scarsa diffusione del modello per tanto, i programmatori che si affacciano a questo sistema impiegano un tempo maggiore per padroneggiare le regole che governano questi sistemi. Chia in particolare utilizza un nuovo tipo di linguaggio chiamato Chialisp che, per quanto possa essere più funzionale di Solidity, il linguaggio di Ethereum, rimane più difficile da utilizzare. Solidity condivide paradigmi simili nella programmazione allo sviluppo web, quindi esiste un ampio pool di programmatori che possono impararlo abbastanza rapidamente.

(Cohen B., Pietrzak K. e altri , 2021)

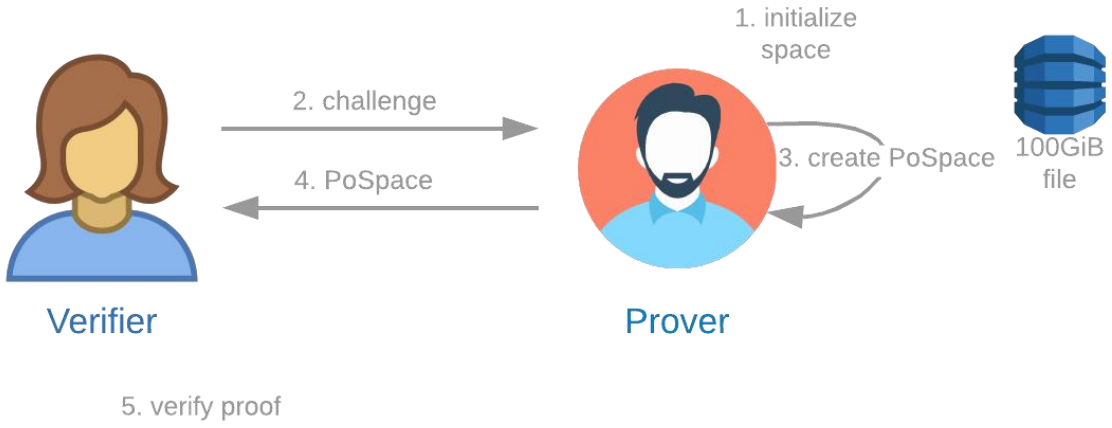
3.3 Il costo del Mining: Proof of Space and Time

Gli algoritmi di consenso decentralizzato richiedono l'utilizzo di una risorsa che sia crittograficamente verificabile e scarsa (non infinita). Nei precedenti sistemi blockchain sono state utilizzate due diverse risorse scarse: potenza di calcolo (Proof of Work) e staked money (Proof of Stake).

Il sistema di consenso Proof of Space and Time di Chia utilizza la capacità di archiviazione come risorsa scarsa. Questo è molto più vicino rispetto ai sistemi precedenti all'ideale originale di Satoshi, (il creatore anonimo di Bitcoin), ovvero di "una CPU, un voto", dove un voto si riferisce a una possibilità di vincere e convalidare un blocco, non un vero voto nella blockchain. Ad esempio, qualcuno che archivia 500 GiB ha 5 "voti" e qualcuno che archivia 100 GiB ha 1 "voto".

Un altro strumento crittografico viene utilizzato per proteggere il sistema di Chia: una funzione di ritardo verificabile (VDF), che è una prova crittografica che il tempo reale è passato.

Il primo elemento che compone il protocollo è il Proof of Space è quello che si occupa della convalida e della creazione di nuovi blocchi, è composto da tre componenti: Plotting, Proving/farming Verifyng. (Dan Boneh, Benedikt Bunz & Ben Fisch, 2018)



Fonte: Cohen B., Pietrzak K. e altri , (2021)

- PLOTTING:Il Plotting è il processo mediante il quale un prover, che chiamiamo "farmer", inizializza una certa quantità di spazio. Per diventare un farmer, è necessario disporre di almeno 101,4 GiB disponibili da prenotare sul proprio computer (la specifica minima è un Raspberry Pi 4). Non esiste un limite massimo per le dimensioni di una farm di Chia. Il risultato di questa

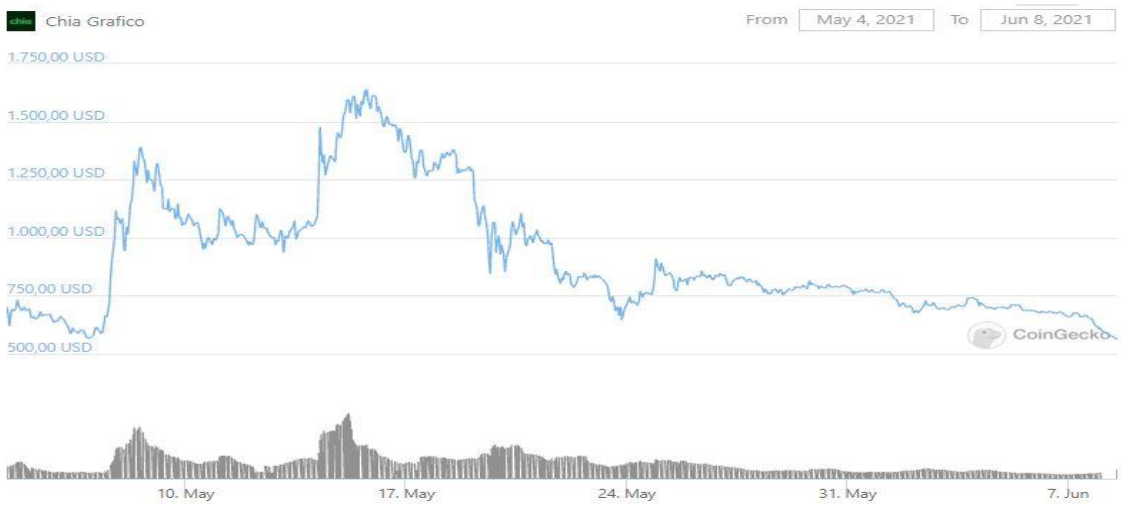
procedura è il “plot”, dove questo può essere paragonato a una lista di biglietti della lotteria. Ogni qual volta il sistema dovrà convalidare o creare un blocco estrae un biglietto, il plot che possiede il biglietto corrispondente vincerà la convalida e guadagnerà la ricompensa. I farmer dovranno iniziare con questa procedura per convertire il loro spazio disponibile in plot; questa procedura è quella che necessità del maggior volume di risorse sia hardware che energetiche. I plot devono essere creati partendo dalla chiave pubblica di un account, in questo modo tutte le ricompense guadagnate da quel plot verranno depositate nell’account del farmer.

- FARMING: Il farming è il processo attraverso il quale ogni farmer riceve una sfida dalla blockchain per dimostrare di aver legittimamente messo da parte una quantità definita di spazio di archiviazione. In risposta a ogni sfida, il farmer controlla i propri plot, genera una prova e invia tutte le prove vincenti alla rete per la verifica. Queste sfide richiedono la verifica dei “biglietti della lotteria”. Questi biglietti sono composti da 5000/10000 caratteri.

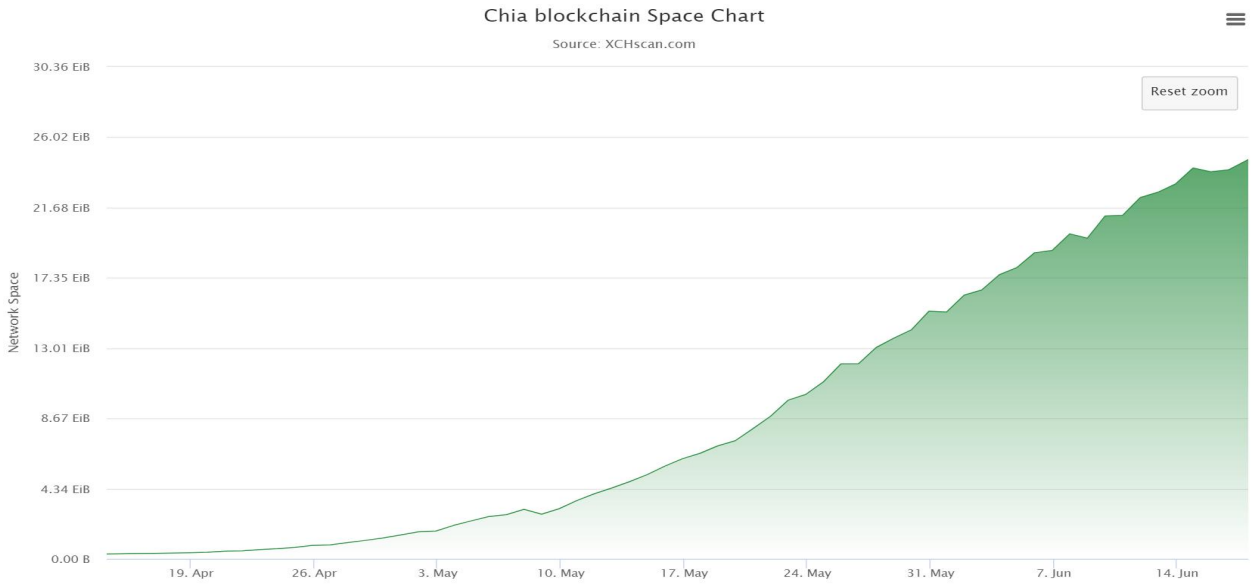
  Per velocizzare, il procedimento andrà a verificare solo una specifica sezione del codice: ogni volta che trova una corrispondenza esso seleziona il Plot per il processo di creazione della Proof of Space. Quando il codice riesce con successo a creare la Proof of Space, il farmer si aggiudica il blocco e la ricompensa.
- VERIFYNG: Dopo che il farmer ha creato con successo una Proof of Space, la prova può essere verificata eseguendo alcuni hash e confrontando i valori contenuti nel proprio plot con quelli richiesti, il peso complessivo di questo codice ammonta a 2048 bit, ed è quindi molto compatto. La verifica è molto veloce, ma non abbastanza veloce per essere verificata in Solidity su Ethereum (qualcosa che consentirebbe trasferimenti senza fiducia tra Blockchain).

Una Verifiable Delay Function, denominata anche Proof of Time o VDF, è una prova che una funzione sequenziale è stata eseguita un certo numero di volte, questa funzione è il secondo elemento che compone questo protocollo. (Dan Boneh, Benedikt Bunz & Ben Fisch, 2018)
Ciò significa che dopo aver eseguito il calcolo (che richiede tempo), il farmer può creare una dimostrazione molto piccola in pochissimo tempo e il Verifier può verificare questa prova senza dover rifare l'intero calcolo. Questo serve a dimostrare che il farmer ha effettivamente impiegato una quantità di tempo reale (anche se non sappiamo esattamente quanto) per calcolare la funzione. Queste VDF accettano un input, chiamato challenge, e producono un output, insieme a una prova che certifica che la funzione è stata valutata correttamente. Il valore prodotto da questa procedura viene utilizzato in modo da avere una progressione lineare tra i blocchi, alternando Proof of Space a Proof of Time.

Il protocollo Proof of Space and Time è nato con lo scopo di evolvere il vecchio sistema del Proof of Work e si è posto fin da subito come alternativa ecologica. Con il lancio di Chia,17 marzo 2021, l'interesse verso questa tecnologia ha avuto un effetto esponenziale portando l'attenzione dei miner a questo nuovo mercato. Inizialmente il valore di Chia è stato fortemente gonfiato per via delle speculazioni dei marcati, pur trattandosi di una Cryptocurrencies acerba e solo ai primi stadi di sviluppo, questo ha portato diversi investitori a massicci investimenti.Nei primi mesi di vita, dopo il via libera allo scambio,4 maggio 2021, si è verificata una "corsa agli Hard Disk": molti miner attirati dai grossi margini di profitto hanno deciso di comprare un elevatissimo numero di hard disk e SSD, necessari per la fase di Plotting.

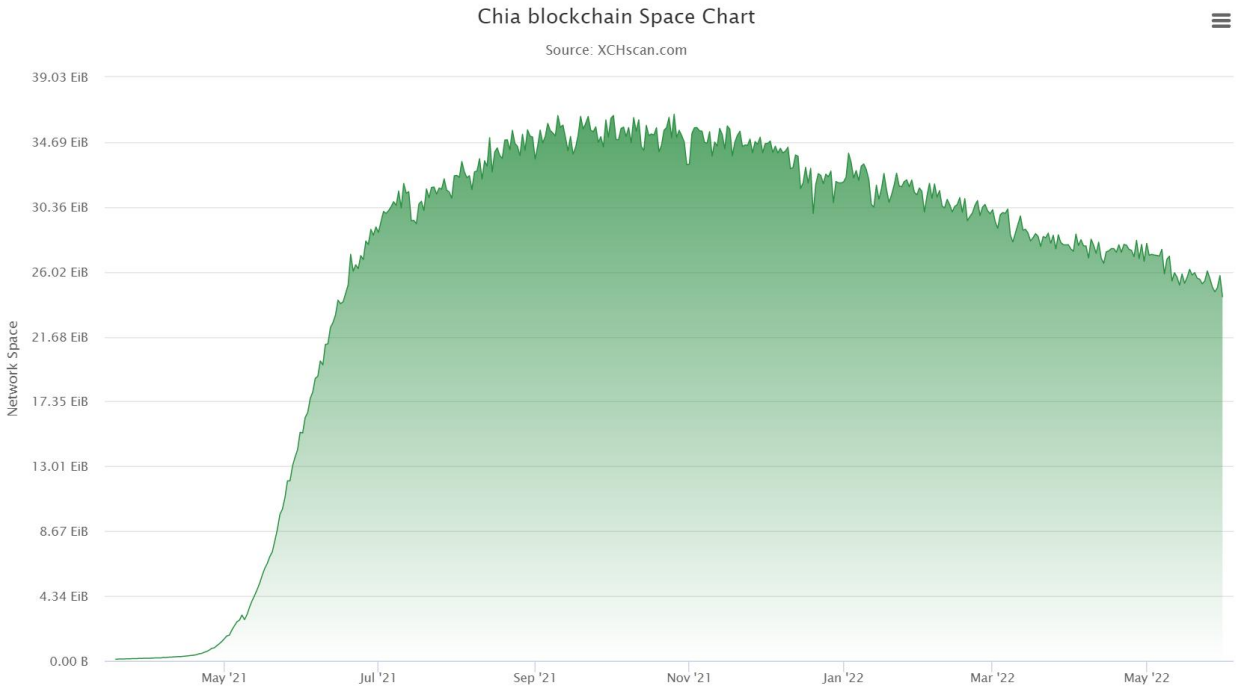


Fonte: https://www.finaria.it/



Fonte: https://www.chiaexplorer.com/

Lo spazio complessivo della rete Chia è cresciuto a ritmi insostenibili portando addirittura ad aumentare il valore in borsa dei principali produttori di Hard disk. In questa fase la rete ha consumato una quantità considerevole di energia ed è stata accusata dalle principali agenzie di stampa di non essere "green". Durante il 2022 con il cessare delle speculazioni iniziali Chia si è stabilizzato in egual maniera allo spazio totale e alla crescita della rete, dimostrando così la sua efficacia in termini di costi energetici.



Fonte: https://www.chiaexplorer.com/

FONTI BIBLIOGRAFICHE E SITOGRAFIA

Boneh D., Bunz B. e Fisch B., (2018). A Survey of Two Verifiable Delay Functions, *Lecture Notes in Computer Science vol. 10991.*

Buterin V., (2014). Ethereum Account, *Ethreum White Paper.*

Buterin V., Wood G., Wilcke J., & Altri, (2021) Documenti per lo sviluppo di Ethereum, Fonte internet: Raccolta di documentazione su https://ethereum.org/it/developers/docs/

Cohen B. e Pietrzak K., (2019). The Chia Network Blockchain.

Cohen B., Pietrzak K. e altri , (2021). Documenti per lo sviluppo di Chia, Fonte internet: racolta di documentazione su: https://docs.chia.net/docs/

Economist T.,The promise of the blockchain: The trust machin, The Economist, 2015

Ehmke C., Blum F. e Gruhn V., (2019).Properties of Decentralized Consensus Technology - Why not every Blockchain is a Blockchain, pp 22

Eze, P., Tochukwu, C., Okpara, R. (2017). A Triplicate Smart Contract Model using Blockchain Technology, *Circulation in Computer Science* (01), pp. 1-10.

Gervais A., Capkun S. e Karame G., (2014). Is Bitcoin a Decentralized Currency?, *IEEE Security and Privacy Magazine Maggio 2014*.

Gjorgie-Trajkovska O., Miteva-Kacarski E., (2017). Cryptocurrencies–advantages and disadvantages Vol. 2 No. 1, *Journal of Economics*.

Guttmann B., (2014). Alla scoperta del Bitcoin, *BITCOIN: Guida completa*.

Ma J., Gans J.S. e Tourky R., (2018). Market structure in bitcoin mining, *National Bureau of Economist Research.*

O'Dwyer J. K. e Malone D., (2014). Bitcoin mining and its energy footprint, *25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communities Technologies.*

Sultan K., Ruhi U. e Lakhani R., (2018). Conceptualizing blockchains: characteristics & applications, *11th IADIS International Conference Information Systems 2018*.

Surda P., (2014). The origin of Bitcoin, *The origin, classification and utility of Bitcoin*.

Taylor M., (2017). The evolution of bitcoin hardware, *Computer Vol. 50.*

Wu C., Pandey V. e Dba C., (2014). The value of Bitcoin in enhancing the efficiency of an investor's portfolio, *Journal of financial planning*.

Fonte internet: https://www.gazzettaufficiale.it Art 8 ter

Fonte internet: https://etherevolution.eu/

Fonte internet: https://ccaf.io/cbeci/index

Fonte internet: https://www.google.com/finance/

Fonte internet: https://blog.ethereum.org

Fonte internet: https://www.finaria.it/

Fonte internet: https://www.chiaexplorer.com/