GENNAIO 2023

ETHEREUM 2.0: L'INNOVAZIONE DELLA BLOCKCHAIN

#CRYPTOS

INDICE

Autori

Minari Alessandro

Vagge Andrea

INTRODUZIONE

Nel seguente elaborato verrà ripercorsa la storia di *Ethereum* (ETH), una delle più innovative e rivoluzionarie piattaforme di scambio di *criptocurrencies* affermatasi nell'ultimo decennio come principale competitor di *"Re Bitcoin"*. Per comprendere a fondo come tale criptovaluta, *Ether*, e la relativa piattaforma abbiano acquisito sempre maggiore diffusione e successo, è necessario analizzare e comprendere quali sono stati gli step fondamentali che hanno portato il suo geniale creatore, Vitalik Buterin, ad elaborare un progetto di tale complessità e grandiosità. Di seguito, verranno illustrate le principali peculiarità della piattaforma Ethereum, soffermandosi con particolare attenzione sull'analisi di una delle più grandi innovazioni tecnologiche implementate nell'ambito della *blockchain*: il passaggio da *Proof to Stake a Proof to Work*.

IL GENIO DIETRO ETHEREUM

Prima di presentare Vitalik Buterin, è necessario fare un passo indietro introducendo la *blockchain* e il *Bitcoin*. La criptovaluta creata da Satoshi Nakatomo si regge su un sistema di *blockchain* ossia un sistema per trasmettere informazioni nel modo più sicuro e trasparente possibile. Prevede un controllo di *disclosure* quasi infallibile. Per comprenderne il funzionamento si potrebbe immaginare di osservare le banconote all'interno del nostro portafoglio e poter sapere per che cosa sono state usate fino a quel momento, dal momento della stampa fino a quando sono arrivate nelle nostre mani. Tali informazioni sono disponibili a tutti quelli che si scambiano la banconota e tutti possono constatare che non si tratta di una banconota falsa. Tuttavia, ciò che caratterizza la *blockchain* è il fatto che può essere usata per qualsiasi altro oggetto o bene. Ciò che ha reso famoso a livello globale tale meccanismo è senz'altro *Bitcoin*, il primo e più diffuso mezzo di pagamento digitale. Questa nuova forma di moneta ha spinto sempre più persone a informarsi circa il funzionamento del denaro e dell'emissione di moneta.

Qui entra in gioco Vitalik Buterin, il quale comprende che le *criptovalute* non sono altro che una delle tante applicazioni della *blockchain*. Infatti, la *blockchain* può essere usata praticamente per tutto: ritirare denaro, depositarlo, investire e addirittura votare *online*. È in tale contesto che Vitalik Buterin ha portato il sistema *blockchain* ad un livello superiore a soli diciannove anni.

Vitalik nasce nel 1994 a Kolomna, vicino Mosca, e dopo, pochi anni la famiglia si trasferisce in Canada, a Toronto. Fin da piccolo spicca per le sue doti matematiche. Il padre, Dimitry Buterin, era programmatore e gli parla di *Bitcoin* all'età di diciassette anni. Vitalik da subito inizia ad informarsi circa *criptovalute* e *blockchain*. Scopre e inizia a far parte della *community* dei "*Criptolover*" senza però partecipare attivamente poiché non ha risorse né per acquistare *Bitcoin* né un computer abbastanza potente per effettuare il *mining*. Inizia a scrivere articoli per un blog venendo pagato cinque *Bitcoin* per elaborato,

circa 4 dollari al tempo, ma l'equivalente di duecentomila dollari oggi. All'età di diciotto anni fonda "*Bitcoin Magazine*", in poco tempo la rivista *online* diventa un punto di riferimento del settore. Dopodiché lascia l'università e inizia a girare il mondo incontrando imprenditori che lavorano a nuove versioni di blockchain. In Israele scopre "*Master Coin*", un progetto *blockchain* che offre servizi finanziari, ossia registra e archivia contratti finanziari sulla *blockchain* creando un modo per stipulare contratti in automatico, i cosiddetti "*Smart Contacts*". È proprio da qui che nasce l'idea di *Ethereum*, mentre la *blockchain* di *Bitcoin* è concepita solo come sistema di pagamento *"Peer to Peer"*, Vitalik ha saputo integrare gli *Smart Contracts* nel design di *Ethereum*. Abbozza il *white paper* di *Ethereum* nel 2013 e con un *team* di sviluppatori di fiducia si trasferisce in Svizzera nel Canton Zugo, la cosiddetta *Criptovalley*. Per finanziare il progetto vengono creati nel 2014 gli *Ether*, una nuova *criptovaluta*, per far sì che gli investitori trovassero appetibile la piattaforma. Nello stesso anno Vitalik vince il "*World Technology Award*" grazie al suo progetto. Vengono fatte partire *diverse ICO (Initial Coin Offering)*, un modo per raccogliere capitali offrendo in cambio *Ether*. *Ethereum* vende 2000 *ether* al prezzo di 1 *bitcoin*, raccogliendo in tutto trentuno mila *bitcoin* per un valore che supera i 18 milioni di dollari, la terza ICO per raccolta nella storia. Nel 2015 viene lanciata la prima beta della piattaforma chiamata "*Olympic*", ma il lancio finale di *Ethereum* avviene nel 2016. In un'intervista al Corriere della Sera, Vitalik afferma: *"Per costruire la piattaforma ho messo insieme tutto ciò che mi interessa. Matematica, criptografia, economia e politica"*. Vitalik è uno dei primi programmatori esperti di economia, le prime *criptovalute* infatti mancavano di molte peculiarità dal punto di vista economico come, per esempio, la registrazione di contratti di vario genere. Ha capito che la vera potenzialità delle *criptovalute* stava proprio nella *blockchain*. Nella creazione di Ethereum si è ispirato a *Bitcoin* e *BitTorrent*, uno dei primi *network* di condivisione di file decentralizzato. Ciò che distingue *Ethereum* da *Bitcoin*, pur essendo entrambi basati su un sistema di *blockchain* pubblico, è che possiamo vedere il secondo come una semplice *app* che usa la tecnologia della *blockchain*, *Ethereum* invece è come se fosse un "*app store*" che permette agli utenti di creare nuove applicazioni. È proprio questa la svolta di *Ethereum*, prima creare applicazioni sulla *blockchain* richiedeva grandi capacità di programmazione, ora *Ethereum* fornisce ai suoi utenti strumenti per creare facilmente applicazioni decentralizzate e per farlo utilizza una sola *blockchain*, mentre prima ad ogni

blockchain corrispondeva una sola app. *Ethereum* può essere usata per creare applicazioni finanziarie affidabili e trasparenti, sistemi di sicurezza crittografati e per gestire proprietà e contratti, ma anche per amministrare nuovi *social network*, big data e voti online. L'obiettivo finale di Vitalik è di sostituire tutto con la *blockchain*. Ad agosto 2021 con l'aggiornamento *London* viene implementato un meccanismo "*mangia Ether*" per cui in ogni istante vengono bruciati un certo numero di *Ether*, processo necessario per controllare l'andamento della criptovaluta, deflazionandola e rendendola più stabile.

In ragione di tali peculiarità che rendono unico *Ethereum*, si riporta il grafico relativo all'oscillazione di prezzo nel tempo in cui è evidente come tale piattaforma di scambio di criptovalute abbia risentito molto meno di altre del calo generalizzato dei prezzi dovuto ad un *outlook* economico pessimista e *hawkish*.

Fonte: Bloomberg

Vitalik Buterin, diventato a 27 anni il più giovane *cripto* miliardario del mondo, potrebbe essere davvero l'antieroe che tutti volevano nell'imprenditoria, la nemesi dei *banker* di *Wall Street*.

MECCANISMI DI CONSENSO: POS E POW

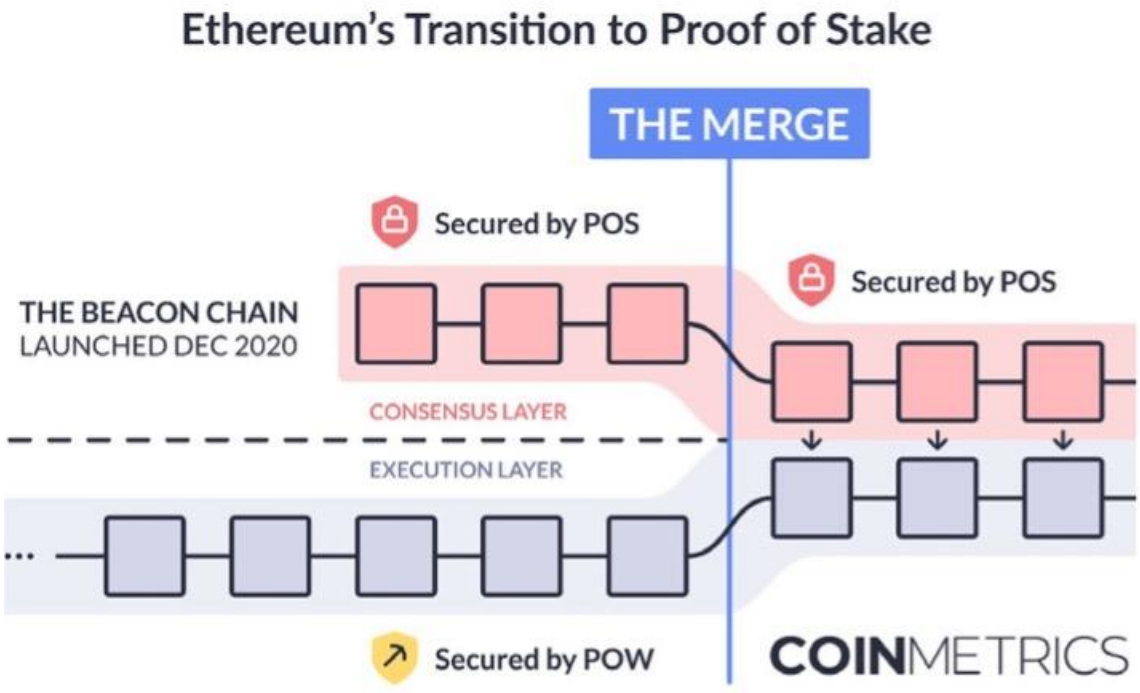
Con "il *Merge*" il mining *Proof-of-Work* (*PoW*) su *Ethereum* è stato sostituito a favore di un meccanismo di consenso alternativo chiamato *Proof-of-Stake (PoW)*. Il meccanismo *Proof-of-Stake* è gestito da validatori che vincolano il loro capitali in Ether (ETH) per garantire la sicurezza della rete e ricevere ricompense. Questo sarà il cambiamento più significativo di *Ethereum* dal suo lancio nel 2014 e avrà profonde implicazioni per la sicurezza, l'economia e, soprattutto, l'energia globale della rete. Il passaggio a *Proof-of-Stake* permette di abbassare drasticamente il consumo di energia elettrica. Mentre i *miners* convalidano le transazioni e rendono sicura la rete in base alla loro potenza di calcolo, i *validators* su *Ethereum* 2.0 (*Consensus Layer*) andranno a convalidare le transazioni grazie all'offerta che hanno vincolato nel network. La *Proof-of-Stake,* per chi possiede grosse quantità di Ether, avrà maggior controllo sul protocollo *Ethereum* (per esempio fondi istituzionali e JP Morgan). Il *Proof-of-Work* è un protocollo di consenso che permette ai vari nodi di concordare lo stato dell'EVM quindi l'assetto canonico di *Ethereum*. In pratica si tratta di un algoritmo che imposta le difficoltà a cui si devono sottoporre i *miner* per creare dei blocchi validi. Una sorta di rompicapo matematico, un "*cripto-puzzle*", che viene risolto da uno dei *miner* in competizione, che ottiene, in premio, degli ETH appena coniati e la creazione del nuovo blocco**.** La seconda criptovaluta più grande, *Ethereum*, è passata a un nuovo processo di mining che non si basa più su magazzini di GPU (Graphics Processing Units) che consumano energia. Il PoS consuma il 99,95% di energia in meno rispetto al passato, secondo quanto riportato da ethereum.org, il principale sito sostenuto dalla *Ethereum* Foundation. Una volta completato, il processo sposterà la blockchain *ETH* da *Proof-of-work* a *Proof-of-stake* . Invece di utilizzare le famose schede GPU per verificare le transazioni sulla *blockchain*, si utilizzerà il consenso di coloro che possiedono una quantità di *ETH*. *Ethereum* consuma circa 83,80 TWh all'anno - circa quanto la Finlandia - con il suo sistema attuale. Questo numero è salito negli ultimi mesi dopo un forte calo a giugno. Secondo Digiconomist, *Bitcoin* ha attualmente un consumo energetico stimato di 128,31 TWh all'anno. Si tratta di un minimo storico per il 2022 ed è pari alla quantità di energia consumata dalla Norvegia.

Alcuni *miners* passeranno a un'altra *coin* da minare, ma se si pensa che transiteranno a una *coin* come bitcoin, stiamo sbagliando, poiché questo movimento richiederebbe un nuovo investimento in impianti di mining ASIC personalizzati.

IL PASSAGGIO A ETHEREUM 2.0

La fase che prende il nome di "The *Merge*" è una fusione tra la *Beacon Chain* ed *Ethereum Chain*. La *Beacon Chain* è un modo "innovativo" per contribuire alla sicurezza di *Ethereum*. In pratica, occorre mettere in *staking* i propri ETH per attivare il software di convalida. I validatori elaborano transazioni e creano nuovi blocchi nella chain.

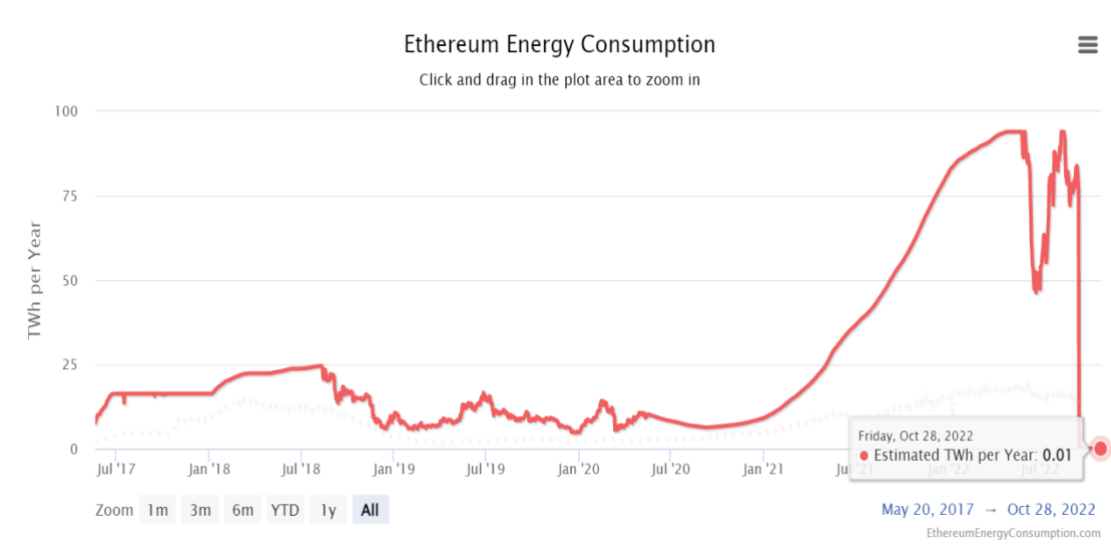
Dopo il Merge della rete principale con la *beacon* chain, il prossimo aggiornamento introdurrà le *shard chain* nella rete PoS. Questi "*shard*" dovrebbero andare a migliorare le capacità della rete e la velocità delle transazioni, estendendo la rete a 64 *blockchain*. La *beacon chain* è il primo passo importante per l'introduzione delle *shard chain*, poiché queste richiedono lo *staking* per adempiere alle loro funzionalità in totale sicurezza. Le *shard chain* potranno entrare in modo sicuro nell'ecosistema *Ethereum* solo ed esclusivamente quando sarà presente un meccanismo di consenso PoS operativo.



Fonte: Coinmetrics

MECCANISMI DI INCENTIVI

L'economia di *Ethereum* sta cambiando radicalmente. A differenza di quanto accade nel *Proof-of-Work,* la quantità di ETH emessi segue un programma dinamico, incrementato all'aumentare della quantità di ETH in *staking*. Al livello attuale (13M di ETH), l'emissione annuale è destinata a calare da 5M ETH a 600K ETH in regime PoS. Ciò porta a una riduzione di circa il 90% di emissione. Tenendo conto delle commissioni di transazione, è probabile che ETH vada a diventare un asset deflazionistico (in casi particolari) negli anni successivi al Merge. Lo *staking*, grazie al nuovo passaggio a POS, trasformerà ETH in un asset che genererà rendimento nel tempo; infatti, le ricompense previste per lo *staking* si muovono in maniera inversamente proporzionale al numero totale di validatori. Al tasso odierno, gli *stakers* hanno buone probabilità di guadagnare un aumento dell'rendimento all'anno solo grazie ai *rewards* derivati da *staking*. Il Merge sposta Ethereum da un meccanismo di consenso *Proof-of-work* a uno *Proof-of-stake*. Questa transazione avviene grazie all'unione di due livelli, da cui il termine "merge". Il Merge ha combinato il livello di esecuzione (che utilizza la *Proof-of-work*) con un nuovo livello di consenso chiamato *Beacon Chain*. La *blockchain* di *Ethereum* continuerà a funzionare come di consueto, ma attraverso PoS *Consensus*. *Ethereum* ha subito alcuni cambiamenti a seguito del merge: uno di questi riguarderà il modello di sicurezza della rete. *Ethereum*, con il passaggio alla *Proof*-of-*stake*, non è più protetto da *miners*, con potenti computer che risolvono calcoli, ma i partecipanti mettono in *staking* i *token* Ether (ETH) con i validatori per proteggere la rete. Il valore economico di ETH, messo in *staking*, funziona quindi parzialmente da indicatore di sicurezza per la *chain*. Con i *miners* fuori dai giochi, il carbon *footprint* di *Ethereum* dovrebbe ridursi. I validatori non avranno bisogno di utilizzare potenti computer che consumano molta energia; infatti, come si nota dal grafico, a partire dal 15 ottobre, il giorno del merge, i consumi del *network* sono scesi di oltre il 99,9%. Di conseguenza, l'attuale *carbon footprint* di *Ethereum* è di appena 0,1 milioni di tonnellate di CO2 (MtCO2) all'anno. In altre parole, una singola transazione su *Ethereum* consuma circa 0,03 kWh, con un carbon *footprint* di 0,01 kgCO2.



Fonte: EthereumEnergyConsumption.com

CONCLUSIONE

In conclusione, Ethereum sta attualmente attraversando un periodo di cambiamento radicale, con il passaggio dal meccanismo di proof-of-work a quello di proof-of-stake che sta portando significativi vantaggi in termini di efficienza energetica e decentralizzazione. La fusione della Beacon Chain con la main chain di Ethereum, nota come "The Merge", rappresenta un passo importante verso l'introduzione delle shard chains, che dovrebbero migliorare ulteriormente le capacità della rete e la velocità delle transazioni. Inoltre, la transizione verso il proof-of-stake sta trasformando ETH in un asset che genera rendimento nel tempo. In generale Ethereum sta cambiando il suo modello economico e sta diventando un asset deflazionistico, con emissioni in costante calo. In futuro, si prevede che Ethereum continuerà a evolversi e a espandersi, offrendo nuove opportunità per la creazione di applicazioni decentralizzate e soluzioni di contratti intelligenti.

BIBLIOGRAFIA E SITOGRAFIA:

Massimo Gaggi, Il Corriere della Sera: "*Vitalik Buterin, il guru che a 24 anni cambierà il web (e la politica)*", 06/04/2019;

Benjamin Snajder, CNBC: "*Meet Vitalik Buterin, the 23-year-old founder of bitcoin rival Ethereum*", 23/01/2017;

Alexis Benveniste, CNN: "*Ethereum's 27-year-old creator is now a billionaire*", 04/05/2021;

Arijit Sarkar, Cointelegraph: "*I consumi di Ethereum sono diminuiti del 99,9% dopo il Merge*", 29/10/2022;

Ethereum.org: "*La Beacon Chain*", 14/12/2022 ;

Digiconoist: "*New research highlights success of Ethereum's merge*", 10/12/2022;

Zhiyuan Sun, Cointelegraph: "*Vitalik Buterin svela quali sono i futuri sviluppi di Ethereum a cui è maggiormente interessato*", 06/12/2022;

Ethereum.org: "*Upgrading Ethereum to radical new heights*", 15/12/2022;

James Wo, Cointelegraph: "*Grazie ad Ethereum, 'altcoin' non è più un insulto*", 05/12/2022.