Contenuto

I. Riassunto

Epic Cash è il punto finale del viaggio verso il vero e proprio P2P per cash, la pietra angolare di un sistema finanziario privato. La moneta Epic mira a diventare la forma di denaro digitale più efficace al mondo per la protezione della privacy. Per raggiungere questo obiettivo, soddisfa le tre funzioni principali del denaro:

1. **Riserva di valore** – possono essere salvati, recuperati e scambiati in un secondo momento, e hanno un valore prevedibile quando vengono richiamati;
2. **Mezzo di scambio** – qualsiasi cosa accettata come standard di valore e scambiabile con beni o servizi;
3. **Unitá di conto** – l'unità con cui il valore di una cosa è contabilizzato e confrontato.

	$ USD	BTC	EPIC
Riserva di valore	✗	✓	✓
Mezzo di scambio	✓	✗	✓
Unitá di conto	✓	✗	✓

Nel 2009 Bitcoin è emersa come la prima valuta digitale basata su blockchain e con essa tre caratteristiche che definiscono le altre criptomonete:

- **Trustlessness** – nessuno è tenuto a fidarsi di un'entità o controparte centralizzata per il funzionamento della rete;
- **Immutabilitá** – le transazioni non possono disfarsi;
  a. altamente improbabile o difficile riscrivere la storia;
  b. solo il proprietario di una chiave privata, puó spostare fondi associati a quella chiave privata;
  c. Tutte le transazioni sono registrate nella catena a blocchi.
- **Decentralizzazione** – "Le catene di blocchi sono politicamente decentralizzate (nessuno le controlla) e architettonicamente decentralizzate (nessun punto di fallimento infrastrutturale)..."[1].

Bitcoin ha aperto nuove strade tecnologiche, aderendo nel contempo a fondamentali collaudati nella struttura della sua politica monetaria. Il successo di Bitcoin è fortemente legato alla sua limitata offerta combinata con una catena di blocchi senza fiducia, immutabile e decentralizzata. Epic Cash emula la politica monetaria di Bitcoin, che consiste nel ridurre l'inflazione e l'offerta limitata per garantire che la moneta Epic possa servire come efficace riserva di valore.

Nonostante il successo di Bitcoin, alcune carenze sono state rivelate sin dalla sua nascita 10 anni fa. Altri progetti hanno cercato di superare queste carenze e noi abbiamo studiato il meglio di questi da utilizzare come punto di partenza. Abbiamo deciso di utilizzare il codice Grin e l'eccellente lavoro di molti altri progetti per aiutarci a perfezionare i risultati ottenuti a fatica e scoprire i difetti dei predecessori di Epic Cash. Epic Cash possiede le qualità chiave per essere una valuta ideale:

- **Fungibilitá** – Il valore di un'unità di Epic deve essere sempre uguale ad un'altra unità di Epic, così come uno Yen o Yuan è sempre uguale e sostituibile con un altro Yen o Yuan. Il raggiungimento della fungibilità in gran parte dipende dalla privacy.
- **Scalabilitá** – Epic Cash mantiene una catena di blocchi efficiente in termini di spazio, sulla quale è possibile stabilire facilmente nuovi nodi senza bisogno di grandi quantità di risorse. La catena di blocchi Epic Cash è in grado di raggiungere un throughput almeno doppio rispetto a Bitcoin.
- **Privacy** – La catena di blocco Epic Cash salvaguarda l'anonimato dei titolari e degli utenti Epic proteggendo i dettagli delle transazioni da parte di terzi, ed è progettata per essere allo stesso tempo non rintracciabile e invisibile alla sorveglianza.
- **Velocitá** – Le transazioni Epic Cash sono fluide, continue e vengono eseguite molto più velocemente rispetto alle precedenti generazioni di tecnologia a catena di blocco. Mentre Bitcoin richiede sei blocchi da 10 minuti per ottenere una conferma completa della transazione, le transazioni Epic vengono confermate all'interno di un singolo blocco non appena viene estratto un blocco da 1 minuto.

[1] Buterin, Vitalik, ***The Meaning of Decentralization***, 6 February, 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II. Privacy

L'uso moderno del denaro può essere inteso come il trasferimento collettivo di unità di tra persone e istituzioni. Il paesaggio del denaro in qualsiasi momento può essere tracciato rispondendo alle seguenti domande:

1. *Chi lo tiene in mano, e quanto tiene in mano?*
2. *Chi sta trattando con chi, e per quanto?*

Per le valute fiat tradizionali, e anche per Bitcoin, possiamo rispondere a queste domande. In questo modo, molto può essere rivelato sulla vita delle persone, come i modelli di consumo, la proprietà e le controparti transazionali. Si possono trarre conclusioni abbastanza accurate sugli interessi e le intenzioni di un individuo, tracciando i trasferimenti di valore. Senza privacy, i dati delle transazioni possono essere informazioni pericolose nelle mani di terzi.

L'uso delle crittomonete nell'ultimo decennio mostra un continuum di "privacy" in varie implementazioni a catena di blocco. La scala della privacy, se si considera una di esse, va da quella aperta e nota da un lato all'anonimato dall'altro. Quando la privacy viene meno, una pietra angolare essenziale delle crittomonete, la mancanza di fiducia, si degrada. Come evidenziato dal successo dei servizi di analisi del blockchain di Bitcoin, Bitcoin si trova più verso il lato trasparente. Gli utenti devono sempre più spesso adottare misure per assicurarsi di non effettuare inavvertitamente transazioni in Bitcoin contaminato. La soluzione Epic Cash fa oscillare l'ago verso l'anonimato e ripristina questa proprietà essenziale garantendo che sia la privacy dell'individuo che la privacy delle transazioni siano ingegnerizzate nel sistema a un livello fondamentale.

Privacy dell' Identitá

Privacy delle Transazioni

Privacy dell'identitá

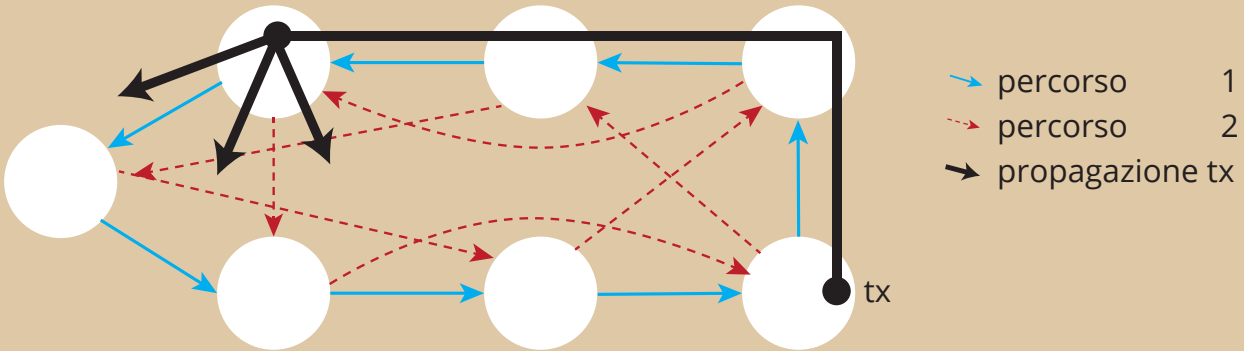
La maggior parte delle crittomonete come Bitcoin sono conservate in portafogli i cui indirizzi si riferiscono a chiavi pubbliche derivate dalle chiavi private di un portafoglio. Questi indirizzi diventano quindi localizzatori della propria cassaforte privata nel mondo digitale. La blockchain Epic Cash elimina completamente gli indirizzi e applica invece una grande firma multipla da cui tutte le chiavi pubbliche e private sono generate su base monouso.

Poiché gli indirizzi dei portafogli Bitcoin sono il localizzatore di un caveau nel mondo digitale, quel portafoglio può essere ricondotto all'indirizzo IP (Internet Protocol) di un proprietario, e quindi al propietario stesso in un luogo unico in un dato momento. Spiegato in modo semplice: quando avviene una transazione Bitcoin, la transazione viene trasmessa da un hub di comunicazione chiamato 'nodo' e poi propagata ad altri nodi chiamati 'peers'. Queste informazioni si diffondono rapidamente a ciascuno di questi nodi in modo consecutivo su tutta la rete. Questo processo è giustamente chiamato "Gossip Protocol". Molto semplicemente, ogni Bitcoin ha una posizione online visibile e una posizione fisica dove può essere trovato, o meglio il proprietario del Bitcoin. Come ha notato la giornalista Grace Caffyn, Bitcoin non è "più segreto di una ricerca di Google da una connessione internet domestica."[2]

Oltre ad eliminare gli indirizzi dei portafogli, la catena di blocchi Epic Cash assicura la privacy dell'identità assicurando che gli indirizzi IP non possano essere rintracciati. Lo fa attraverso l'integrazione del protocollo Dandelion++. Migliorando rispetto al suo predecessore, il protocollo originale Dandelion, il protocollo Dandelion++ è il risultato del lavoro continuo di sette ricercatori per combattere gli attacchi di deanonimizzazione alla catena di blocchi. Attraverso Dandelion++, le transazioni vengono passate su percorsi casuali intrecciati, o 'cavi', e poi improvvisamente diffuse in una grande rete di nodi, come i baccelli di un fiore di dente di leone quando soffiato dal loro stelo (Figura 1). Questo rende quasi impossibile risalire alle transazioni fino alla loro origine, e quindi ai loro indirizzi IP di origine.

Figura 1: Anonimizzazione delle transazioni con il *protocollo Dandelion++.*

Dandelion++ inoltra i messaggi su uno dei due percorsi intrecciati su un grafico a 4 righe, quindi li trasmette utilizzando la diffusione. Nella figura, la transazione si propaga sul percorso azzurro[3]. Questo processo rende estremamente difficile risalire alla fonte delle transazioni, preservando così la privacy.



[2] F2Caffyn, Grace, ***Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network,*** 14 March, 2015, https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network

[3] Fanti, G, Venkatakrishnan, S B, Bakshi, S, Denby, B, Bhargava, S, Miller, A & Viswanath, P 2018, 'Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees', ***Proc. ACM Meas. Anal. Comput. Sys.***, Vol. 2, Article 29, pg. 8, https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

Privacy delle transazioni

La blockchain Epic Cash assicura la privacy delle transazioni oscurando gli importi e il rapporto mittente-ricevitore di una transazione. Ciò si ottiene attraverso l'applicazione di ***Confidential Transactions (CT)***[4] e ***CoinJoin***[5], metodi sviluppati principalmente da Gregory Maxwell ((sviluppatore di Bitcoin Core, co-fondatore e CTO di Blockstream).

CT, originariamente creato da Adam Back e successivamente perfezionato da Maxwell, funziona suddividendo le transazioni in parti più piccole attraverso la crittografia omomorfa, un metodo per eseguire calcoli su informazioni crittografate senza decrittografarle prima per preservare la privacy. Una volta divisi, gli osservatori non possono vedere l'ammontare effettivo delle transazioni a causa di fattori accecanti, un sistema che getta numeri casuali nel mix di frammenti di transazione per nascondere i valori di quei frammenti. In definitiva, solo le parti che effettuano la transazione conoscono il valore di uno scambio, mentre la transazione viene verificata dalla rete attraverso la conferma che la somma dei valori in uscita è uguale alla somma dei valori in ingresso, e la somma dei fattori di accecamento in uscita è uguale alla somma dei fattori di accecamento in ingresso.

Per complicare ulteriormente il compito di occhi indiscreti, tutte le transazioni di Epic Cash sono mascherate con CT e poi mescolate insieme per nascondere le connessioni tra le parti che effettuano le transazioni. Questo viene fatto attraverso il secondo concetto di Maxwell, CoinJoin.

Per illustrare CoinJoin in modo semplice, immaginate che A, B e C stiano inviando Epic rispettivamente a X, Y e Z. Inviato attraverso il mezzo CoinJoin, tutto ciò che è noto è che A, B e C stanno inviando e X, Y e Z stanno ricevendo, mentre gli importi delle transazioni rimangono invisibili. Il sistema CoinJoin è fondamentale per Epic Cash attraverso le One-Way Aggregate Signatures (OWAS), che combinano tutte le transazioni all'interno di un blocco in un'unica transazione.

Privacy: Riassunto

La blockchain Epic Cash protegge la privacy degli individui e le loro transazioni:

- **Eliminazione degli indirizzi dei portafogli – Non ci sono identificatori di posizione nei caveau digitali all'interno della catena di blocchi. Le transazioni sono costruite direttamente da persona a persona su base portafoglio a portafoglio;**
- ***Con idential Transactions* – divide le transazioni in più pezzi e introduce fattori accecanti nella raccolta di questi pezzi, in modo che i valori dei pezzi e altri parametri di transazione non possono essere conosciuti;**
- ***Protocollo Dandelion++* – oscura i percorsi digitali di una transazione dall'indirizzo IP del mittente della transazione;**
- ***CoinJoin* – combina le transazioni in pacchetti per mascherare le relazioni tra le parti coinvolte nelle transazioni.**

[4] Maxwell, Gregory, ***Confidential Transactions,*** Technical Report (2015), https://people.xiph.org/~greg/confidential_values.txt

[5] Maxwell, Gregory, ***CoinJoin: Bitcoin Privacy for the Real World***, 22 August, 2013, post on Bitcoin Forum, https://bitcointalk.org/index.php?topic=279249.0

III. Fungibilitá

Charlie Lee, il creatore di Litecoin, ha dichiarato che la fungibilità era l'unica proprietà del denaro mancante a Bitcoin e Litecoin, ammettendo che la privacy e la fungibilità erano i prossimi campi di battaglia per quelle monete[6]. Andreas Antonopoulos, uno dei maggiori esperti mondiali di blockchain, ha affermato che "....le monete contaminate sono distruttive. Se si rompe la fungibilità e la privacy, si rompe la moneta."[7]

La fungibilità è la proprietà di un insieme di beni che assicura che le singole unità di tale insieme siano di pari valore e intercambiabili. È ciò che differenzia le prime forme di moneta dai loro precedenti sistemi di baratto. Senza fiducia nella fungibilità del denaro, questo denaro perde rapidamente la sua utilità. Come verrà illustrato di seguito, la fungibilità della maggior parte delle crittomonete è incerta, mentre l'architettura di privacy di Epic Cash assicura che sia impermeabile alle stesse minacce.

La maggior parte delle crittomonete simili a Bitcoin, per la natura delle catene di blocchi trasparenti su cui esistono, possono essere rintracciate in modo verificabile attraverso ogni portafoglio in cui sono state tenute. Terzi privati e governi controllano la catena di blocchi Bitcoin con mezzi sempre più sofisticati per identificare rapidamente le monete utilizzate nelle attività precedenti. Ciò porta naturalmente a temere che le monete contaminate possano un giorno essere vietate dalle transazioni, lasciando in perdita i loro successivi detentori in buona fede.

Il 19 Marzo 2018 lo U.S. Office of Foreign Asset Control (OFAC) ha annunciato che stava valutando la possibilità di includere gli indirizzi di valuta digitale nell'elenco degli Specially Designated Nationals (SDNs), che sono entità con cui le persone o le imprese statunitensi non possono effettuare transazioni. Ancora più preoccupante è il fatto che l'OFAC non ha escluso l'inclusione nella lista SDN di indirizzi attualmente in possesso di monete contaminate, che di fatto metterebbe i proprietari innocenti di crittomonete contaminate in una lista nera criminale a causa dell'affiliazione delle monete contaminate di proprietà. Questo ha portato il professore di diritto della New York University, Andrew Hinkes, a "baciare l'addio alla fungibilità", e che il pubblico dovrebbe aspettarsi "un premio sulle monete appena coniate, o sulle monete pulite tracciate..."[8].

Con questi sviluppi in mente, non è difficile immaginare uno sconvolgimento del mercato della crittografia e la crisi, o addirittura l'estinzione, di molte crittomonete. Tuttavia, Epic è una delle poche crittomonete che evita questo problema interamente a causa delle forti caratteristiche di privacy precedentemente descritte in questo articolo. Eliminando il legame tra identità e proprietà, e il rapporto tra le parti della transazione, Epic non può mai essere affiliata a una persona o a un'attività. Come tale, il valore di Epic rimane indipendente dai suoi utenti e fornisce elevati livelli di privacy e sicurezza che non possono essere facilmente manipolati da attori malintenzionati in ambito criminale, finanziario o politico.

> **“....LE MONETE CONTAMINATE SONO DISTRUTTIVE. SE SI ROMPE LA FUNGIBILITÀ E LA PRIVACY, SI ROMPE LA MONETA.”**
>
> **ANDREAS ANTONOPOULOS**

[6] Njui, John P, ***Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility***, 29 January, 2019, https://ethereumworldnews.com/charlie-lee-litecoin-ltc-to-soon-have-confidential-transactions-for-fungibility/

[7] Carl T, ***Andreas Antonopoulos Says If Fungibility Is Not Fixed Bitcoin Could Be Attacked,*** 9 April, 2019, https://bitcoinexchangeguide.com/andreas-antonopoulos-says-if-fungibility-is-not-fixed-bitcoin-could-be-attacked/

[8] Hinkes, Andrew, Ciccolo, Joe, ***OFAC's Crypto Blacklist Could Change Crypto***, 24 March, 2018, https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

IV. Scalabilitá

Epic Cash è un'implementazione della blockchain MimbleWimble che produce progressi nella scalabilità grazie a una progettazione efficiente in termini di spazio che elimina i dati delle transazioni ridondanti. La funzionalità Cut-Through, che ne è responsabile, assicura che la blockchain aumenti l'efficienza dello spazio nel tempo, a differenza della maggior parte delle crittomonete, compreso Bitcoin, e che i nuovi nodi possano essere creati con investimenti minimi in memoria e potenza di calcolo. Rimanendo efficiente in termini di spazio, consente la capacità di una rete ampiamente dispersa e favorisce il decentramento. Inoltre, mentre ogni nodo Bitcoin deve memorizzare l'intera catena, i nodi Epic Cash sono in grado di contribuire alla sicurezza della rete sulla base di un piccolo sottoinsieme di blocchi.La maggior parte delle crittomonete richiede la memorizzazione a tempo indeterminato di tutti i dati delle transazioni sulle loro catene di blocchi. La catena Bitcoin attualmente aumenta di 0,1353 GB di memoria ogni giorno, mentre la catena di Ethereum aumenta ad un tasso ancora più veloce di 0,2719 GB al giorno. Se la catena di Bitcoin continua a crescere al suo ritmo attuale, alla fine raggiungerà una dimensione di circa 6 TB nel momento in cui il suo ultimo blocco ricompensa verrá estratto nell'anno 2140. Ethereum supererà i 10 TB entro tale data[9]. Nella maggior parte delle catene di blocchi senza MimbleWimble, le transazioni devono essere verificate da nodi in tutto il mondo. Con l'aumento dei dati, aumenta anche l'onere per ciascun nodo. Anche a soli 200 GB (la dimensione approssimativa dell'attuale catena Bitcoin), la sincronizzazione dei dati richiede una rete stabile e una capacità di lettura e scrittura su disco ad alta velocità.

Di conseguenza, l'estrazione mineraria è diventata sempre più centralizzata tra i grandi bacini che sfruttano le costose risorse informatiche. Se l'intera storia della catena di blocchi di Bitcoin dovesse invece essere memorizzata nella catena di blocchi di Epic Cash, si troverebbe in quasi il 90% di spazio in meno. Più piccolo è più veloce perché ogni transazione richiede meno tempo per la trasmissione e la sicurezza.

MimbleWimble risolve questo dilemma dello storage con un metodo innovativo di potatura a blocchi, denominato 'Cut-Through'. Per capire come funziona il Cut-Through, è meglio guardare prima di tutto come le transazioni e i blocchi sono composti all'interno di una catena di blocchi MimbleWimble.

Inputs:

Riferimenti a vecchi outputs;

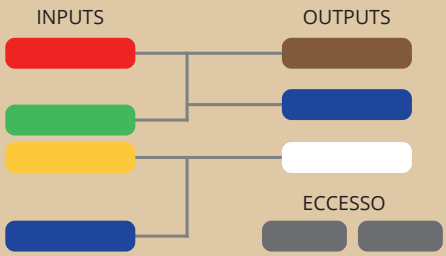
Outputs:

Con idential Transaction outputs e **rangeproofs**;

Eccesso

Differenza tra outputs e inputs, piú le **firme** (per autenticare e dimostrare la non-inflazione

Figura 2:
Elementi delle transazioni MimbleWimble.



[9] Li, Crypto, ***Blockchain's Big Data Problem,*** 27 January, 2019, https://www.longhash.com/news/blockchains-big-data-problem

Tutti i blocchi Epic Cash blocks contengono:

Merkle Trees degli inputs delle transazioni;

Merkle trees degli outputs delle transazioni e rangeproofs;

Lista dei valori in eccesso e le firme.

Nelle figure 2 e 3, adattate dalle presentazioni di Andrew Poelstra[10], Nelle figure 2 e 3, adattate dalle presentazioni di Andrew Poelstra10 , si mostra un Epic appena estratto rappresentato come le celle di input bianche. Le celle identiche colorate rappresentano le uscite con i corrispondenti inputs spesi. Con il processo Cut-Through, gli input e output spesi corrispondenti vengono rimossi per liberare spazio all'interno del blocco, riducendo così la quantità di dati che devono essere memorizzati nella catena di blocchi. Mentre le transazioni vengono omesse dal libro mastro, i kernels in eccesso (solo 100 byte) documentano in modo permanente che le transazioni sono state effettuate. Mentre i blocchi continuano ad essere creati, MimbleWimble applica il Cut-Through attraverso i blocchi, in modo che nel lungo periodo tutto ciò che rimane sono le intestazioni dei blocchi (circa 250 byte), le transazioni non spese e i kernel delle transazioni (circa 100 byte). Grin, la seconda implementazione MimbleWimble ad essere lanciata, ha dimostrato che una catena MimbleWimble con un numero di transazioni simile a quello della catena Bitcoin sarebbe quasi il 10% delle dimensioni della catena Bitcoin[11]. Inoltre, la dimensione di un nodo sarà di poche centinaia di megabyte invece dei pochi GB per una catena come quella di Bitcoin."[12]

Questo è in netto contrasto con Bitcoin, dove l'intera catena di blocchi deve essere memorizzata da ciascun nodo. Nel tempo, man mano che l'efficienza spaziale della blockchain di Epic Cash cresce rispetto alla blockchain di Bitcoin, crescerà anche l'efficienza dei costi relativi alla partecipazione dei nodi alla rete di Epic Cash. L'abbassamento delle barriere alla partecipazione contribuisce a garantire una resilienza cruciale a livello del nodo di progettazione della rete. Attraverso la sua implementazione di MimbleWimble e l'applicazione della potatura a catena con il processo Cut-Through, la catena di blocco Epic Cash offre scalabilità in un modo spesso trascurato dalla comunità delle crittomonete. Si ottiene quindi l'essenza di progeti come Bitcoin: la decentralizzazione. Indipendentemente da quante transazioni al secondo una moneta potrebbe essere in grado di elaborare, a che cosa serve se non può essere sostenuta da una rete ampia e diversificata? Se i requisiti di memoria sono tali che la validazione gravita alla fine verso forti conglomerati minerari, allora tutti gli sforzi della comunità della moneta criptata per creare un ecosistema decentralizzato sono vanificati. Per fornire un throughput aggiuntivo, l'implementazione di un livello 2 in stile Lightning è pianificata come obiettivo a breve termine nella roadmap di sviluppo di Epic Cash.

Figura 3: transazioni MimbleWimble transactions prima e dopo Cut-Through.

[10] SF Bitcoin Developers, ***MimbleWimble with Andrew Poelstra,*** 24 November, 2016, https://www.youtube.com/watch?v=aHTRlbCaUyM&t=940s

[11] Grin Forum, ***Grin Blockchain Size,*** December, 2018, https://www.grin-forum.org/t/grin-blockchain-size/1334

[12] GandalfThePink, ***Introduction to Mimblewimble and Grin,*** 28 March, 2019, https://github.com/mimblewimble/grin/blob/master/doc/intro.md

V. Politica monetaria

Le politiche monetarie di Epic Cash e Bitcoin sono molto simili. L'offerta circolante di Epic Cash prima si espande rapidamente e poi si sincronizza con l'offerta circolante di Bitcoin nel 2028. Aumenta successivamente ad un tasso decrescente fino a raggiungere un'offerta massima di 21 milioni di Epic nel 2140. Epic Cash ha le qualità per diventare un deposito sicuro di valore a lungo termine perché la fornitura in circolazione è nota in qualsiasi punto del programma di emissione e culmina in una fornitura massima fissa. La politica monetaria di Epic Cash è caratterizzata dalle seguenti quattro caratteristiche:

- Emissioni rapide nei primi nove anni di vita, durante i quali devono essere estratti 20.343.750 Epic (96,875% della fornitura totale). I tassi di emissione esatti sono delineati nella sezione Programma di emissione del presente documento;
- Una fornitura massima di 21 milioni di Epic sarà raggiunta nell'anno 2140, all'incirca nello stesso momento in cui Bitcoin raggiunge una fornitura massima di 21 milioni di unità;
- La fornitura e il tasso di emissione di Epic in circolazione si sincronizzano con quelli di Bitcoin sulla Epic Singularity intorno al 24 maggio 2028. In seguito alla Singolarità, il tasso di emissione diminuisce ad un ritmo crescente, mentre l'offerta in circolazione cresce ad un ritmo decrescente;
- Epic ha una struttura di divisibilità a 8 decimali, tale che: 1 Epic è pari a 100.000.000.000 freeman (così come 1 Bitcoin è pari a 100.000.000.000 satoshi).

La politica monetaria di Epic Cash si ispira a quella di Bitcoin per i seguenti motivi:

- Accordo con i fondamenti economici di Bitcoin, vale a dire che la scarsità e la prevedibilità dell'offerta in circolazione sono alla base della sua forte riserva di proprietà di valore;
- Il pubblico conosce già il modello di Bitcoin e la sua tracciabilitá nel corso degli ultimi dieci anni dalla sua nascita. Sincronizzandosi approssimativamente con la fornitura circolante di Bitcoin e rispecchiando la struttura di massima fornitura e divisibilità di Bitcoin, Epic prende la strada della minima resistenza verso l'adozione di massa.

VI. Programma di Emissione

Epic Cash ha un totale di 33 fasi estrattive, ciascuna definita da diminuzioni delle ricompense di blocco, rispetto all'epoca precedente. La Epic Genesis, la data in cui viene estratto il primo blocco Epic, ha luogo il 1° agosto 2019. I blocchi vengono estratti ad uno al minuto. Le prime cinque fasi producono quasi il 97% dell'offerta massima di Epic, corrispondenti a 20 anni di emissioni di Bitcoin in circa nove anni. Questo può essere pensato come un'occasione per "far tornare indietro l'orologio" per coloro che hanno perso la spettacolare ascesa di Bitcoin.

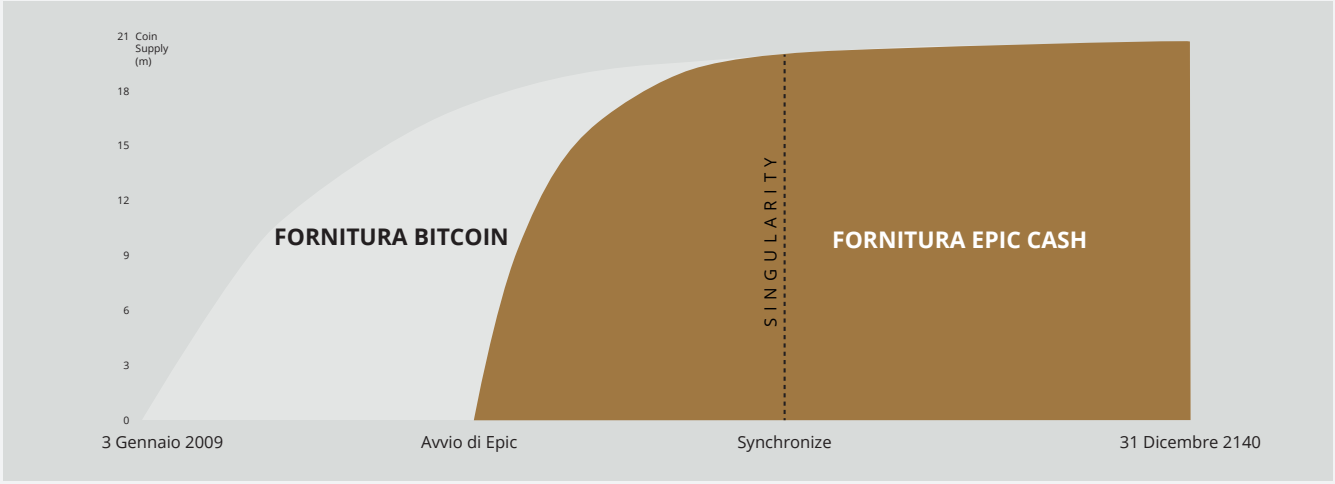
Il programma di emissione nella tabella 1 delinea le date di inizio e fine delle prime sette fasi minerarie, le corrispondenti ricompense dei blocchi e le conseguenti forniture in circolazione per ogni fase. Le fasi dalla 8 alla 33 non sono incluse nella tabella per brevità. Per quelle fasi, basti capire che ogni fase successiva avrà una ricompensa di blocco pari alla metà della ricompensa della fase precedente, esattamente come in Bitcoin. La quantità di Epic emessa durante ciascuna di queste fasi sarà la somma dei premi di blocco nella fase quadriennale (circa 1460 giorni).

All'Epic Singularity (2028), la fornitura circolante Epic interseca il numero di fornitura circolante di Bitcoin, a quel punto Epic Cash adotta la ricompensa del blocco Bitcoin e il halving, che vede le ricompense del blocco dimezzarsi ogni quattro anni. L'unica eccezione è che i blocchi di Epic continuano ad essere estratti al ritmo di un blocco ogni minuto, contro il ritmo di un blocco di Bitcoin ogni dieci minuti. In questo modo, l'offerta circolante Epic mantiene approssimativamente la parità con l'offerta circolante di Bitcoin per il resto della loro esistenza.

Tabella 1: Programma di emissioni per le prime sette fasi minerarie. Le date sono approssimazioni.

Fase	1	2	3	4	5	SINGULARITY	6	7
Ricompensa di blocco	16	8	4	2	1		0.15625	0.078125
Data inizio	Aug 1, 2019	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025		May 24, 2028	May 22, 2032
Data fine	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025	May 24, 2028		May 22, 2032	May 20, 2036
Durata (in giorni)	334	470	601	800	1019		1460	1460
Fornitura iniziale	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
Fornitura finale	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
% di fornitura massima	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

Figura 4: Programma di emissioni di Epic e Bitcoin.



VII. Mining

La catena di blocco Epic Cash cerca il decentramento accogliendo un'ampia varietà di hardware di calcolo. Il mining di Epic è inizialmente disponibile per CPUs, GPUs, e ASICs, utilizzando tre rispettivi algoritmi di hashing: RandomX, ProgPow, e CuckAToo31 +. Gli algoritmi possono essere scambiati senza compromettere l'integrità della catena.

1 RandomX e CPUs

RandomX é un algoritmo Proof-of-Work (PoW) ottimizzato per CPU di uso generale. Utilizza esecuzioni di programmi randomizzati con diverse tecniche memory-hard per raggiungere i seguenti obiettivi:

- Prevenzione dello sviluppo di ASIC a chip singolo;
- Ridurre al minimo il vantaggio di efficienza dell'hardware specializzato rispetto alle CPU di uso generale.

Il mining di Epic con CPU richiede un'allocazione contigua di 2 GB di RAM fisica, 16 KB di cache L1, 256 KB di cache L2 e 2 MB di cache L3 per ogni thread di mining[13]. I dispositivi Windows 10 richiedono almeno 8 GB di RAM. Non è inconcepibile che un giorno, in un futuro non troppo lontano, i telefoni cellulari possano diventare dei validi nodi di estrazione mineraria. La precoce integrazione della CPU nella rete di estrazione di Epic Cash è un'ottima opportunità per molti, con mezzi informatici solo modesti, per guadagnare ricompense di blocco contribuendo a proteggere la rete di Epic Cash.

2 ProgPow e GPUs

Programmatic Proof-of-Work (ProgPow) è un algoritmo che dipende dalla larghezza di banda della memoria e dal calcolo del nucleo di sequenze matematiche randomizzate, che sfruttano molte delle caratteristiche di elaborazione di una GPU e quindi catturano in modo efficiente il costo energetico totale dell'hardware. Poiché ProgPow è specificamente progettato per trarre il massimo vantaggio dalle GPU di base, è difficile e costoso ottenere efficienze significativamente più elevate attraverso hardware specializzato. Come tale, l'algoritmo ProgPow riduce gli incentivi per i grandi pool ASIC a superare le GPU, come spesso si vede con molti altri algoritmi PoW, come lo SHA-256 di Bitcoin. Le GPU, anche se non così diffuse come le CPU, sono ancora comunemente disponibili. Con lo sviluppo tecnologico guidato da Nvidia e AMD, le GPU sono in grado di elaborare in parallelo molti multipli di soluzioni minerarie al di sopra delle CPU su base unitaria. È grazie a questa combinazione di ubiquità ed elevata potenza di elaborazione che le GPU forniranno la spina dorsale a gran parte dell'attività estrattiva durante le fasi iniziali, come indicato nella tabella 2.

3 CuckAToo+31 e ASICs

CuckAToo31+ è una permutazione ASIC friendly dell'algoritmo Cuckoo Cycle sviluppato dall'informatico olandese John Tromp. Simile al resistente CuckARoo29 , CuckAToo31+ genera grafici bipartiti casuali e presenta ai minatori il compito di trovare un ciclo di una data lunghezza 'N' che passa attraverso i vertici di quel grafico.

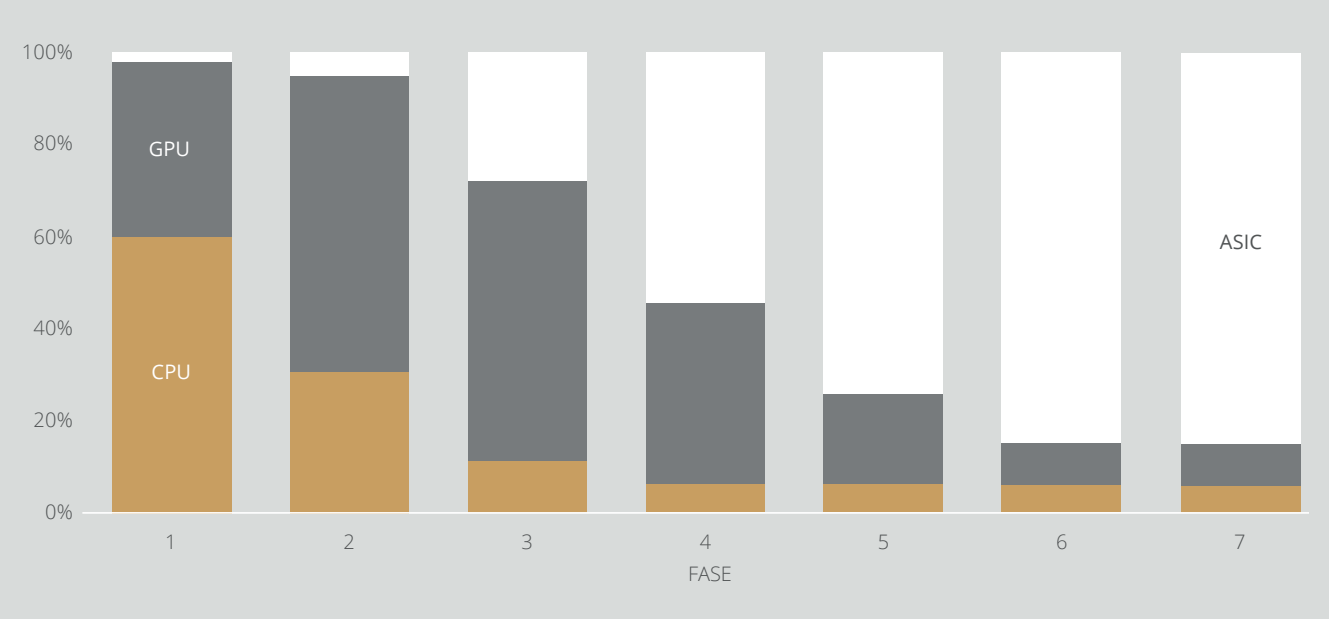
[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

Si tratta di un compito legato alla memoria, il che significa che il tempo della soluzione è vincolato dalla larghezza di banda della memoria piuttosto che dalla velocità del processore grezzo o della GPU. Di conseguenza, gli algoritmi del Cuckoo Cycle producono meno calore e consumano molta meno energia rispetto ai tradizionali algoritmi PoW. L'ASIC friendly CuckATOO31+ permette di migliorare l'efficienza rispetto alle GPU utilizzando centinaia di MB di SRAM, pur rimanendo vincolati dalla memoria I/O[14]. In definitiva, gli ASIC offrono le maggiori economie di scala potenziali delle tre opzioni di estrazione mineraria. Nell'interesse dell'inclusività, tuttavia, sebbene venga loro assegnata una piccola parte delle ricompense minerarie rispetto alle CPU e alle GPU, alla fine gli ASIC assumono una quota maggioritaria delle ricompense dei blocchi minerari, nell'ipotesi che ci sarà un ecosistema competitivo di produttori di dispositivi per CuckATOO31+.

Tabella 2: Assegnazioni dei premi minerari. Soggetto a revisione. Le assegnazioni saranno orientate alla massima decentralizzazione e coerenti con gli interessi a lungo termine della rete.

Fase	1	2	3	4	5	6	7
Giorni	334	470	601	800	1019	1460	1460
CPUs	60%	30%	10%	5%	5%	5%	5%
GPUs	38%	65%	62%	40%	20%	10%	10%
ASICs	2%	5%	28%	55%	75%	85%	85%

Figura 5: assegnazioni di premi minerari per ogni fase secondo la tabella 2. Soggetto a revisione.



[14] Le Sceller, Quentin, ***An Introduction to Grin Proof-of-Work,*** 16 November, 2018, https://blog.blockcypher.com/an-introduction-to-grin-proof-of-work-103aaa9f66ce

4 Contributi minerari

A partire dalla Epic Genesis (2019) e per finire alla Epic Singularity (2028), durante il processo estrattivo, c'è un'assegnazione di Epic che viene reindirizzata, come contributi minerari, verso la EPIC Blockchain Foundation.

La EPIC Blockchain Foundation è dedicata allo sviluppo tecnico e alla promozione della consapevolezza e dell'utilità del progetto Epic Cash durante i primi anni della sua nascita, creando attività di marketing e sviluppando partnership all'interno del settore delle tecnologie finanziarie.

Dopo la Singolarità, il ruolo della EPIC Foundation sarà assunto dalla EPIC Distributed Autonomous Corporation (EDAC), che sarà sviluppata dalla fondazione prima della consegna.

La EPIC Blockchain Foundation è finanziata da una percentuale di premi minerari, dedotti dai premi di blocco, secondo i seguenti tassi annuali:

Tabella 3: Tassi annuali dei contributi minerari alla Fondazione come percentuale delle ricompense minerarie.

Anno	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
% di Mining Rewards	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. Conclusioni

Epic mira ad essere riconosciuto come 'argento digitale decentralizzato', un mezzo di scambio controparte della posizione riconosciuta di Bitcoin come oro digitale decentralizzato. Reintroducendo la fungibilità perduta su una dorsale hardware molto più efficiente dal punto di vista energetico ed ecologico, Epic Cash inclina l'equilibrio energetico a favore dei singoli utenti, in netto contrasto con le recenti tendenze di centralizzazione. La combinazione dell'economia Bitcoin, della teoria dei giochi e della formula di prova del lavoro con il meglio della tecnologia contemporanea a catena di blocco si traduce in una moneta senza fiducia, immutabile e decentralizzata (Epic) che è scalabile, fungibile e che protegge la privacy dei suoi utenti. La catena di blocco Epic Cash è aperta, pubblica, senza confini e resistente alla censura. Preserva la privacy e la ricchezza dei suoi utenti e premia coloro che utilizzano il loro hardware a supporto della rete attraverso l'estrazione mineraria. Ogni Epic viene estratta per mezzo di prove di lavoro. La fornitura inizia da zero e la rete è considerata equa, con un testnet funzionale attualmente in funzione.

Fatti chiave di Epic Cash:

- **Il Mining inizia l'1 Agosto 2019.**

- **La blockchain di Epic Cash si basa su MimbleWimble.**

  Le caratteristiche che definiscono il protocollo sono:

  1. **Cut-Through** – la rimozione delle informazioni ridondanti dalla catena di blocco per promuovere l'efficienza spaziale, incoraggiare la partecipazione su larga scala alla convalida della rete e gestire il decentramento;
  2. ***CoinJoin*** – il raggruppamento di transazioni all'interno di un blocco per garantire la fungibilità di Epic;
  3. ***Protocollo Dandelion++*** – la propagazione delle transazioni comunicando attraverso canali interconnessi e diffondendo su un'ampia rete di nodi, interrompendo le connessioni tra le transazioni e la loro origine;
  4. **No Wallet Addresses** – l'uso di una grande firma multipla per generare chiavi private monouso per le parti della transazione, eliminando completamente la necessità di indirizzi di portafoglio.

- La politica monetaria di Epic Cash è stata progettata per sincronizzare l'offerta circolante di Epic con l'offerta circolante di Bitcoin in circa nove anni, e raggiungere la stessa fornitura massima di 21 milioni di unità contemporaneamente a Bitcoin, nell'anno 2140. Questa politica di inflazione decrescente garantisce trasparenza, prevedibilità dell'offerta e scarsità, favorendo la sicurezza dello stoccaggio del valore a lungo termine.

- Mining che incorpora CPU, GPU e ASIC tramite i corrispondenti algoritmi RandomX, ProgPow e CuckATOO31+, per facilitare l'adozione di massa e l'efficacia della rete.

IX. Specifiche tecniche

Nome del progetto: Epic Cash
Nome della moneta: Epic
Tempo del blocco: 60 secondi
Dimensione del blocco: 1 MB
Fornitura iniziale: 0
Fornitura finale: 21,000,000
Genesi del blocco: 1 Agosto 2019
Consensos: RandomX (CPUs), ProgPow (GPUs) and CuckAToo31+ (ASICs)

Links:

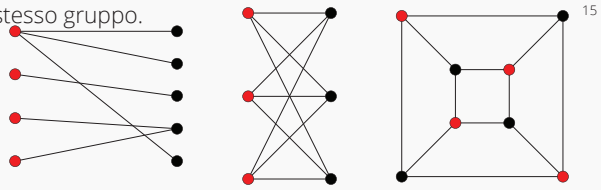
www.epic.tech

t.me/EpicCash – Telegram

X. Glossario

ASIC Circuiti integrati specifici per applicazioni; chip progettati per un unico scopo. Un insieme

Bipartite Graph di vertici del grafico scomposti in due gruppi in modo tale che non vi siano due vertici del grafico adiacenti all'interno dello stesso gruppo.



Blinding Factor un elemento casuale introdotto in un messaggio digitale per facilitare la cifratura; un segreto condiviso tra le due parti che codifica gli input e gli output di quella specifica transazione, nonché le chiavi pubbliche e private delle parti della transazione[16].

Block Reward nuova Epic distribuita dalla rete come ricompensa per i calcoli effettuati per verificare le transazioni all'interno di un nuovo blocco.

Cache un componente hardware o software che memorizza i dati in modo di velocizzare le future richieste di questi dati.

Circulating Supply la quantità di Epic esistente in un determinato periodo di tempo.

CPU Central Processing Unit: componente informatica responsabile per l'interpretazione e l'elaborazione dei dati eseguendo la maggior parte dei comandi del computer.

Cut-Through un processo della blockchain MimbleWimble in cui gli inputs e i corrispondenti outputs spesi vengono rimossi per liberare spazio all'interno del blocco, riducendo la quantità di dati da salvare nella catena di blocchi.

Decentralization lo stato di dispersione del funzionamento e della governance di una rete.

Emission la creazione di nuova Epic guadagnata dai minatori in block rewards. Epic è creato ogni 60 secondi quando le transazioni sono confermate nella catena.

Epic Singularity il punto in cui la fornitura circolante di Epic si sincronizza con la fornitura circolante di Bitcoin (maggio 2028).

Excess (MimbleWimble) la differenza tra outputs e inputs, più le firme (per l'autenticazione e per dimostrare la non inflazione).

Fungibility la proprietà di un bene o merce, per cui le singole unità sono essenzialmente intercambiabili, e ciascuna delle sue parti è indistinguibile da un'altra parte.

Genesis (Event) L'estrazione del primo blocco di Epic e l'inizio ufficiale della catena di blocchi.

GPU Graphics Processing Unit: Un'unità contenente un chip logico programmabile (processore) specializzato per le funzioni di visualizzazione. Le GPU si usano per il mining di crittomonete.

Halving (for Bitcoin) si verifica ogni 4 anni. Il tasso di fornitura diminuisce del 50% dopo ogni halving.

Hash valore calcolato a partire da un numero di input di base utilizzando una funzione di hashing.

Hashing Algorithm (function) algoritmo matematico che associa dati di dimensione arbitraria a un hash di dimensione fissa utilizzato per generare e verificare firme digitali, codici di autenticazione dei messaggi (MAC) e altre forme di autenticazione.

Homomorphic Encryption un metodo per eseguire calcoli su informazioni crittografate senza prima decrittografarle. (in programmazione) lo stato in cui un oggetto non può essere modificato dopo la sua creazione.

Immutability

Input (MimbleWimble) il componente di una transazione MimbleWimble che rappresenta la parte mittente della transazione; creato dagli output di transazioni precedenti.

I/O input/output; la comunicazione tra un sistema di elaborazione delle informazioni, come un computer, e il mondo esterno, eventualmente un sistema di elaborazione delle informazioni umano o di altro tipo.

[15] http://mathworld.wolfram.com/BipartiteGraph.html

[16] Macdonald, Andrew, ***Grin Coin and MimbleWimble: An Introductory Guide***, 18 October, 2018, https://cryptobriefing.com/grin-coin-mimblewimble-introduction/

Maximum Supply	la quantità di Epic da raggiungere e a quel punto l'offerta in circolazione non aumenterà successivamente (21.000.000Epic).
Memory-Hard	l'uso di molta RAM per impedire connessioni simultanee che eseguono tentativi in parallelo. Le funzioni memory-hard sono algoritmi i cui tempi di calcolo sono principalmente decisi dalla memoria disponibile per conservare i dati.
Merkle Tree	struttura di dati utilizzata nelle applicazioni informatiche. Nelle catene di blocchi, gli alberi Merkle consentono una verifica efficiente e sicura dei contenuti in grandi strutture di dati.
MimbleWimble	un protocollo messo in atto da un collaboratore sotto pseudonimo, Tom Elvis Jedusor, in una chatroom di sviluppatori Bitcoin.
Multisignature	uno schema di firma digitale che permette a un gruppo di utenti di firmare un singolo documento. Di solito, un algoritmo multifirma produce una firma congiunta che è più compatta di una raccolta di firme distinte di tutti gli utenti[17].
Node	un computer che si collega a una rete a catena di blocchi e si dirama verso altri nodi della rete per distribuire informazioni sulle transazioni e i blocchi, in modo peer-to-peer.
One Way Aggregate Signature (OWAS)	una firma di transazione composta da molte firme che viene criptata in modo tale che è molto difficile calcolare le singole firme che ne fanno parte.
Output (MimbleWimble)	la componente di un'operazione MimbleWimble che rappresenta la ricezione dell'operazione; utilizzata come input per le operazioni successive.
Pedersen Commitment Scheme	una primitiva crittografica che permette ad un prover di impegnarsi su un valore scelto senza rivelare alcuna informazione su di esso e senza che il prover sia in grado di recedere dall'impegno sul valore.
Private Key	una chiave privata è una piccola parte di codice che viene accoppiata ad una chiave pubblica per attivare algoritmi di cifratura e decifratura del testo. Viene creato come parte della crittografia a chiave pubblica durante la crittografia a chiave asimmetrica e utilizzato per decrittografare e trasformare un messaggio in un formato leggibile.
Proof of Work (PoW)	un pezzo di dati che è difficile (costoso e richiede tempo) da produrre, ma facile per altri da verificare e che soddisfa determinati requisiti. Le prove di lavoro sono spesso utilizzate nella generazione di blocchi di crittomonete.
Public Key	una chiave pubblica creata con algoritmi di crittografia a chiave asimmetrica. Le chiavi pubbliche sono utilizzate per convertire un messaggio in un formato illeggibile.
RAM (Random Access Memory)	chip di memorizzazione dei dati ad accesso rapido in un dispositivo informatico in cui sono conservati il sistema operativo (OS), le app e i dati in uso, in modo che possano essere rapidamente raggiunti dal processore del dispositivo.
Rangeproof	una validazione che verifica che la somma degli input di una transazione sia maggiore della somma degli output della transazione e che tutti i valori della transazione sono positivi. Le prove di intervallo assicurano che l'offerta monetaria non sia stata manomessa.
(Digital) Signature	parte standard di un protocollo blockchain, utilizzato principalmente per garantire la sicurezza delle transazioni e dei blocchi di transazioni, il trasferimento di informazioni, la gestione dei contratti e tutti gli altri casi in cui è importante rilevare e prevenire qualsiasi manomissione esterna. Essi offrono tre vantaggi della memorizzazione e del trasferimento di informazioni sulla catena a blocchi: • Rivelano se i dati inviati sono stati manomessi; • Verifica la partecipazione di una particolare parte alla transazione; • Può essere giuridicamente vincolante.
SRAM (Static Random Access Memory)	Random Access Memory (RAM) che conserva i bit di dati nella sua memoria finché c'è energia.
Throughput	la misura delle transazioni al secondo che può essere eseguita da un determinato protocollo di crittomonete.
Trustlessness	la qualità di una rete di crittomonete per aderire alle regole di un protocollo senza controllo di una parte centrale.

[17] Bellare, Mihir, Neven, Gregory, 2007, ***Identity-based Multi-signatures from RSA***, Lecture Notes in Computer Science vol. 4377, https://link.springer.com/chapter/10.1007%2F11967668_10

EPIC CASH

EPIC PRIVATE INTERNET CASH