Blockchain: concetti fondamentali e applicazioni

Blockchain – Storia

- **1990**: Stuart Haber e W. Scott Stornetta (Bell Communications Research) pubblicano «How to time-stamp a digital document»*

"The prospect of a world in which all text, audio, picture, and video documents are in digital form on easily modifiable media raises the issue of how to certify when a document was created or last changed. The problem is to time-stamp the data, not the medium. We propose computationally practical procedures for digital time-stamping of such documents so that it is infeasible for a user either to back-date or to forward-date his document, even with the collusion of a time-stamping service."

*Haber, S., & Stornetta, W. S. (1990, August). How to time-stamp a digital document. In *Conference on the Theory and Application of Cryptography* (pp. 437-455). Springer, Berlin, Heidelberg. (https://link.springer.com/content/pdf/10.1007/3-540-38424-3_32.pdf)

Blockchain – Storia

Haber e Stornetta evidenziano i limiti del ricorrere ad un ente «certificatore» (TTS – Time Stamping Service):

- Privacy
- Banda richiesta per la trasmissione e spazio di storage
- Incompetenza
- Fiducia (trust)

Introducono quindi l'uso di crittografia, firma digitale e catene di blocchi per la marcatura temporale di documenti digitali

*Haber, S., & Stornetta, W. S. (1990, August). How to time-stamp a digital document. In *Conference on the Theory and Application of Cryptography* (pp. 437-455). Springer, Berlin, Heidelberg. (https://link.springer.com/content/pdf/10.1007/3-540-38424-3_32.pdf)

Blockchain – Storia

- **1992**: Cynthia Dwork e Moni Naor pubblicano «Pricing via Processing or Combatting Junk Mail»*

"We present a computational technique for combatting junk mail in particular and controlling access to a shared resource in general. The main idea is to require a user to compute a moderately hard, but not intractable, function in order to gain access to the resource, thus preventing frivolous use."

Dwork e Naor introducono una forma di «Proof of Work – PoW», meccanismo alla base di alcune blockchain (es. Bitcoin)

*Dwork, C., & Naor, M. (1992, August). Pricing via processing or combatting junk mail. In Annual international cryptology conference (pp. 139-147). Springer, Berlin, Heidelberg. (https://link.springer.com/content/pdf/10.1007/3-540-48071-4_10.pdf)

Blockchain – Storia

- **2008**: Satoshi Nakamoto (pseudonimo usato dal creatore o dai creatori di Bitcoin) pubblica il whitepaper «Bitcoin: A Peer-to-Peer Electronic Cash System»*

Vengono definiti aspetti centrali (hashing, marcatura temporale, proof of work, …) di una delle più note blockchain: Bitcoin

Bitcoin non è l'unica blockchain!

*https://bitcoin.org/bitcoin.pdf

Blockchain – Storia

- **2013**: Nasce Ethereum
- **2014-22**: Il ledger di bitcoin passa da 20 GB (2014) 100 GB (2017) agli attuali 400 GB (2022)*
- **2020-22**: Guadagna popolarità il termine “Web3” (originariamente proposto dai creatori di Ethereum**)

	Caratteristiche	**Periodo**
Web 1.0	Pagine web statiche, utenti «consumatori»	1991-2004
Web 2.0	Web come piattaforma, utenti produttori di contenuti (blog, social media,…)	2004-oggi
Web 3.0 (Web3)	Ecosistema decentralizzato, economia basata su blockchain (criptovalute, NFTs, …)	2021-?

*https://www.blockchain.com/explorer/charts/blocks-size
**https://www.wired.com/story/web3-gavin-wood-interview/

Blockchain

Criptovaluta ≠ Specifica Blockchain ≠ Blockchain in generale

Blockchain

Con il termine «Blockchain» si indica una tecnologia che:

- Permette di raccogliere e registrare transazioni in blocchi
- Permette accesso distribuito e decentralizzato da più nodi di una rete al registro (ledger – libro mastro) così creato
- Incatena i blocchi in ordine logico garantendone l'integrità sfruttando la crittografia

Blockchain

Blockchain: è un registro (*ledger*) digitale distribuito in grado di memorizzare transazioni in modo sicuro, verificabile e permanente.

Si basa su:

1. Decentralizzazione
2. Immutabilità
3. Trasparenza
4. Consenso
5. Sicurezza
6. Programmabilità

Blockchain

Decentralizzazione: non esiste un'autorità centrale che svolga funzioni di controllo e che possa autorizzare la legittimità di una operazione

Immutabilità: una volta inserite le transazioni in blocchi i dati non possono più essere modificati. Se così non fosse, ne risulterebbe invalidata tutta la catena successiva.

Trasparenza e consenso: ogni nodo della rete ha la propria copia della blockchain, non ne esiste una centrale. Per aggiungere un blocco alla catena occorre un meccanismo di consenso noto tra i nodi della rete

Blockchain

Sicurezza: l'aggiunta di blocchi, la loro concatenazione e la loro verifica si basa su algoritmi crittografici

Programmabilità: le blockchain offrono la possibilità di programma determinate azioni da eseguire al verificarsi di specifiche condizioni (*smart contracts*).

Blockchain – Definizioni

Nodi: partecipanti alla blockchain connessi in rete (sono fisicamente i server di ciascun partecipante)

Transazione: dati da memorizzare nella blockchain e che devono essere sottoposti a processo di verifica, approvazione (consenso) e archiviazione

Blocco: insieme di transazioni raggruppate per la verifica, l'approvazione e l'archiviazione da parte dei partecipanti alla blockchain

Blockchain – Definizioni

Timestamp: marcatore temporale che viene assegnato ad ogni transazione

Ledger: il registro pubblico nel quale vengono «annotate» in maniera trasparente e immutabile le transazioni. E' composto dai blocchi concatenati tra loro tramite una funzione di «hash»

Funzione di hash: funzione che mappa dei dati in una stringa univoca di dimensione fissa. E' non invertibile (dall'hash non si risale al dato originale).

Blockchain

L’obiettivo di una blockchain è quello di essere un sistema di database decentralizzato (in questo senso, la blockchain è una Decentralized Ledger Technology – DLT).

Può essere immagazzinato ed archiviato in modo permanente un qualunque dato:

- Messaggi
- Voti istituzionali
- Pagamenti
- …

Blockchain

Ma quando usare una blockchain piuttosto che un semplice qualunque altro tipo di database digitale?

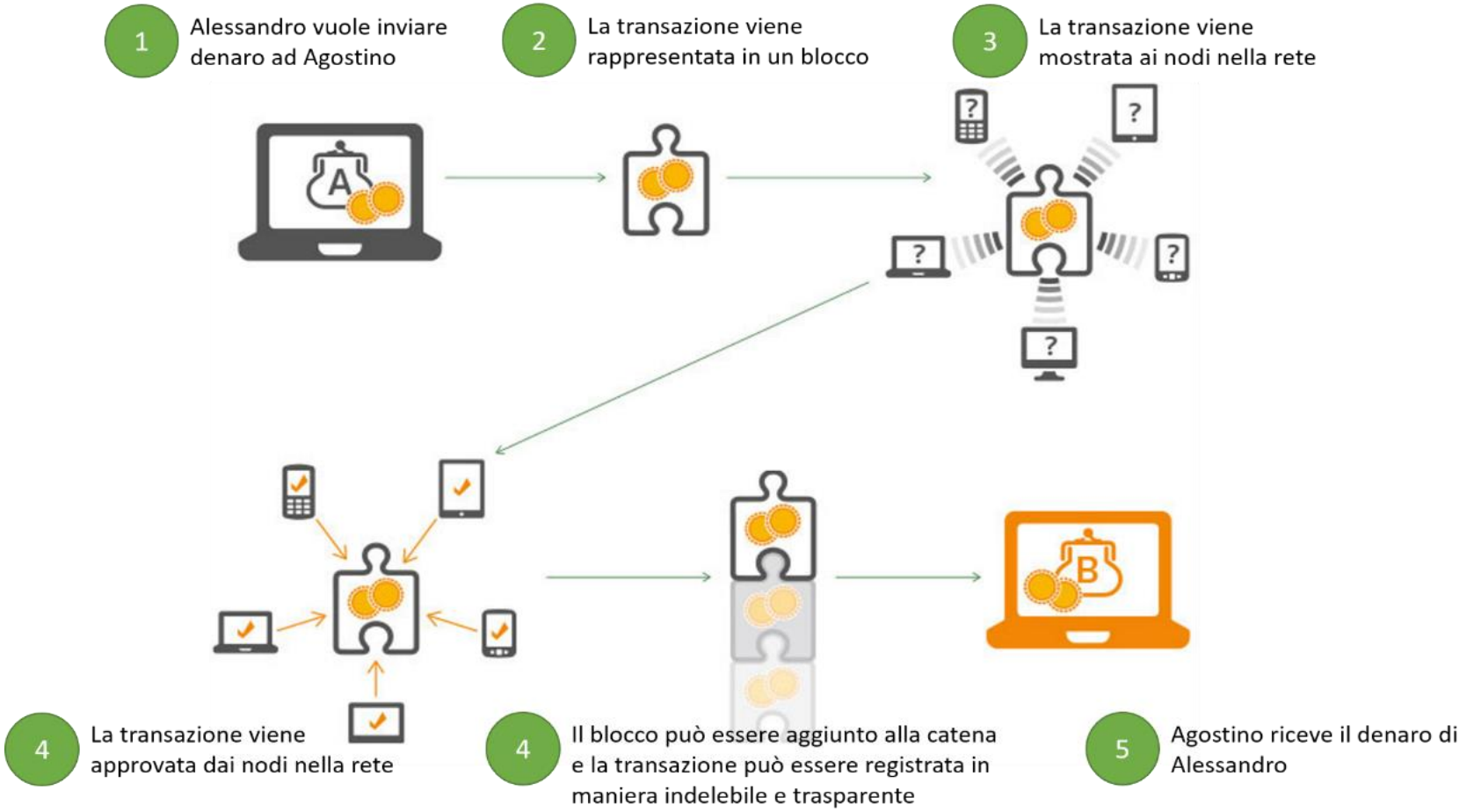
In tutti quei casi in cui si vogliono tutelare in modo imprescindibile due elementi:

- la sicurezza
- l'immutabilità

Senza l'intervento di un ente «certificatore terzo». Tutti i nodi della rete si trasmettono le modifiche apportate al registro e le validano. Non esiste una entità centralizzata che detiene i dati memorizzati e si occupa di informare gli altri nodi di eventuali modifiche.

Come funziona una blockchain?

Blockchain – Esempio di transazione



Transazione

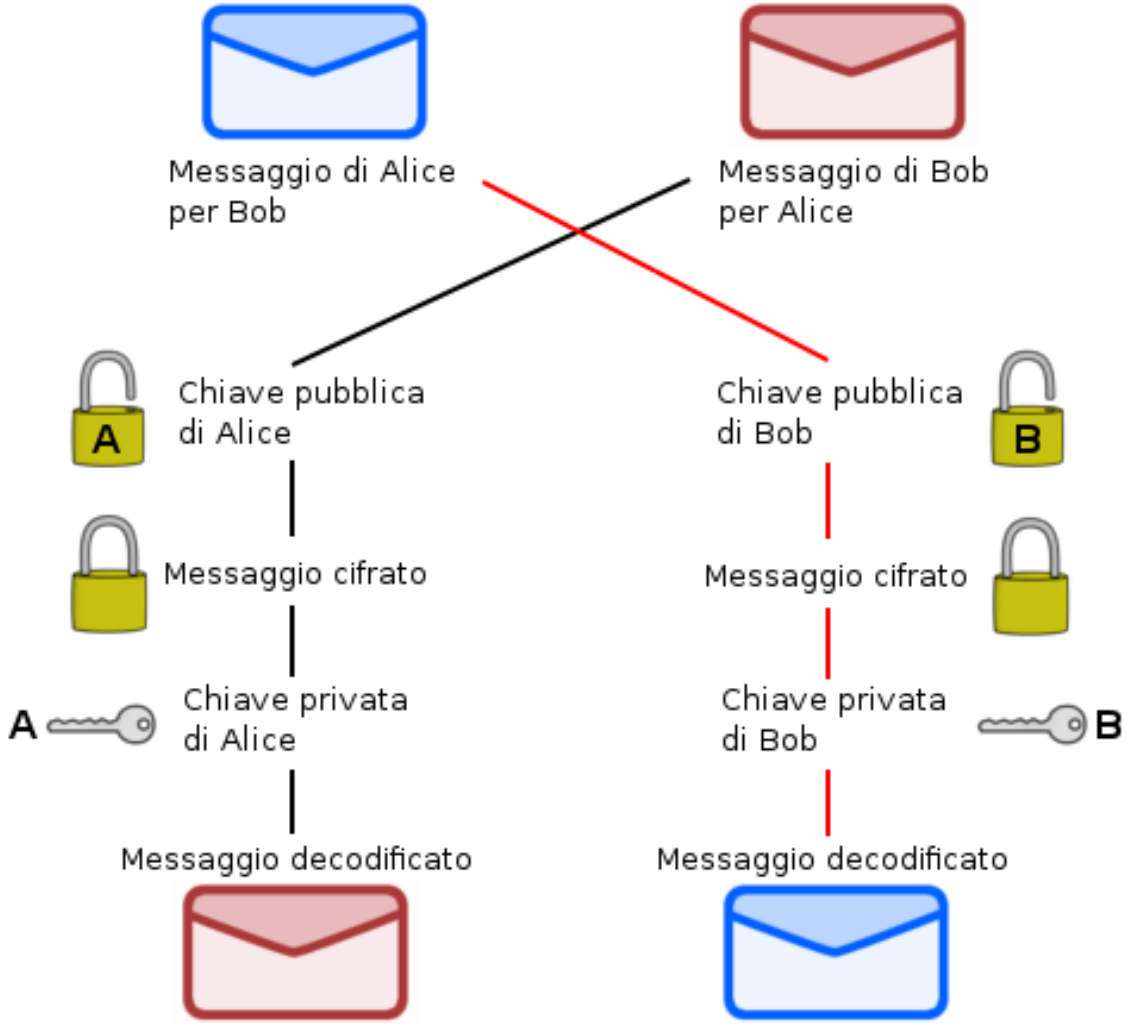
Qualunque transazione, ovvero i dati che la rappresentano, è sottoposta ad un meccanismo di firma a doppia chiave asimmetrica simile alla firma digitale.

In un protocollo a doppia chiave asimmetrica ogni attore è dotato di:

- Una chiave pubblica (distribuita e nota)
- Una chiave privata (personale e segreta)

Un messaggio cifrato con una delle due chiavi può essere decodificato solo con l'altra

Crittografia a doppia chiave asimmetrica

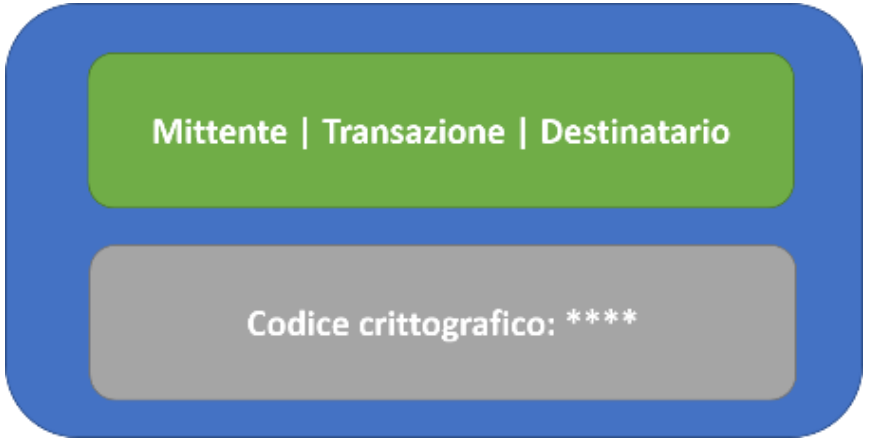


Crittografia a doppia chiave asimmetrica

- Chiunque con la chiave pubblica può usarla per cifrare un messaggio che può essere aperto solo dal detentore della chiave privata. Il messaggio resta segreto se la chiave privata rimane segreta.

- Un messaggio può essere cifrato con la chiave privata, come fosse una firma. Il messaggio può essere decifrato correttamente (cioè la firma può essere verificata) da chiunque con la chiave pubblica.

Transazione



Una transazione prevede un mittente, un destinatario e un processo oggetto della transazione. Il mittente codifica la transazione con la propria chiave privata.

Blocco di transazioni

La transazione entra a far parte di un blocco con altre transazioni non ancora validate dei partecipanti alla blockchain.

Blockchain

Una volta validato, il blocco viene inserito nella blockchain che, di fatto, è una sequenza di questi blocchi.

Blocco

Sul blocco (che è comunque una sequenza di 0 e 1…) viene calcolata una funzione di hash.

In particolare, si usa SHA 256 (Secure Hash Algorithm 256-bit), un algoritmo di hash che permette di convertire un testo alfanumerico di qualunque lunghezza in un codice output della lunghezza standard di 64 caratteri.

- Non è possibile risalire al testo di input facendo riferimento soltanto al codice criptato (l'hash).
- Lo stesso testo restituisce sempre lo stesso output.
- Due testi diversi non hanno lo stesso hash.

Blocco

L’hash, che

- identifica univocamente un blocco e
- dipende dal suo contenuto,

Viene inserito nell’*header* del blocco stesso. Quando viene formato, il blocco contiene anche l’hash del blocco che lo precede.

Una volta validato il contenuto del blocco non può essere modificato: cambierebbe l’hash risultante, invalidando tutti i blocchi successivi della catena!

Validazione di un blocco

Le blockchain funzionano in maniera decentralizzata: il compito di validare un blocco e tutte le transazioni in esso contenute per aggiungerla alla blockchain spetta ai nodi della rete.

- Il meccanismo di consenso tra i nodi della rete per accettare il blocco cambia da implementazione a implementazione
- Validare il blocco richiede la risoluzione di un puzzle crittografico complesso («mining»)
- Il nodo che effettua per primo il mining del nuovo blocco per aggiungerlo alla catena può essere ricompensato con la somma delle commissioni per le transazioni di quel blocco.

Aggiunta di un blocco

- Se la validazione va a buon fine e i partecipanti riconoscono la legittimità delle transazioni in esso contenute il blocco viene aggiunto alla blockchain
  - Ogni nodo ha una copia della blockchain
  - La validazione del blocco viene trasmessa ai nodi della rete, che aggiungono il blocco alla blockchain
  - Per quanto visto in precedenza, nessun partecipante può più modificare il blocco così aggiunto
- Se la validazione fallisce, tutti i nodi ne sono informati

Blockchain

Blockchain: è un registro (*ledger*) digitale distribuito in grado di memorizzare transazioni in modo sicuro, verificabile e permanente.

Validazione di un blocco e consenso

Proof of Work (PoW)

Sistema/protocollo/funzione (nata per impedire l'abuso di servizi online come lo spam) in cui al richiedente di un servizio viene imposto di eseguire un lavoro di computazione moderatamente complesso (ad esempio la risoluzione di un puzzle crittografico) facile da controllare e validare per il fornitore.

- Alcune blockchain (come Bitcoin) usano la PoW per la validazione dei blocchi e il raggiungimento del consenso dei nodi per aggiungere un blocco alla blockchain.

Validazione di un blocco e consenso

Proof of Work (PoW)

- I nodi competono per calcolare l'hash di un blocco.
- L'hash calcolato deve essere «minore» di un certo valore target (deve cioè iniziare con una sequenza di zeri)
- Per far questo si aggiunge all'intestazione del blocco un numero, il *nonce*.
- Il nodo che per primo riesce a trovare il *nonce* (con un approccio brute-force) per ottenere l'hash con la proprietà desiderata, può essere ricompensato con le commissioni sulla transazione (o con la criptovaluta appena coniata)
- Una volta calcolato l'hash, gli altri nodi posso facilmente verificarlo

Validazione di un blocco e consenso

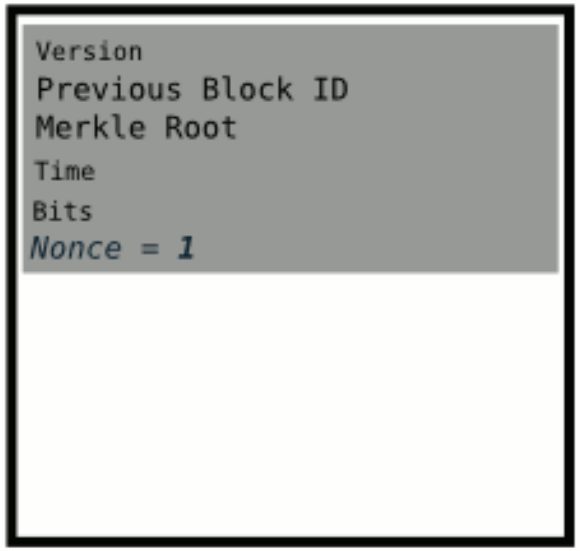


Immagine da: https://learnmeabitcoin.com/technical/nonce

Validazione di un blocco e consenso

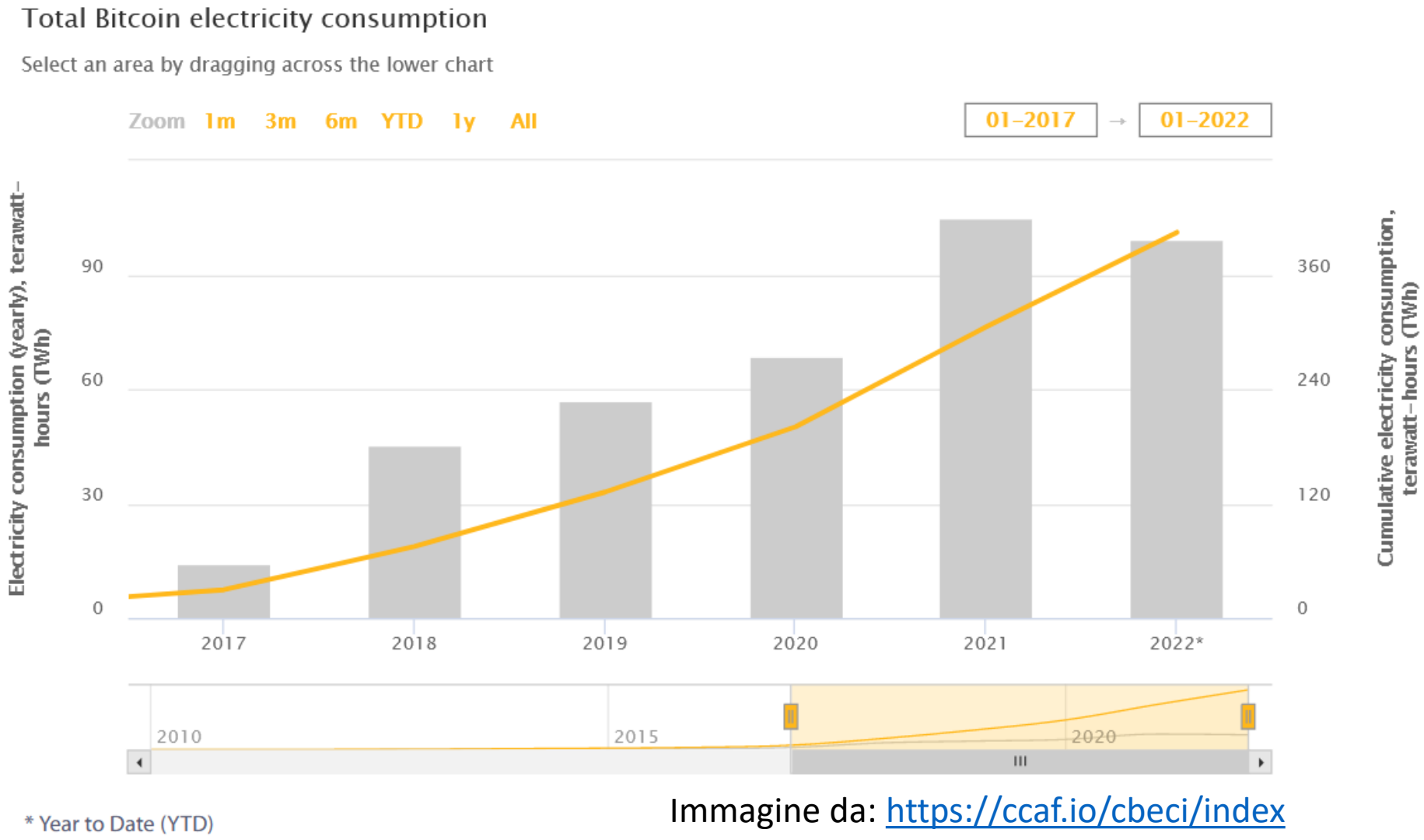


Immagine da: https://ccaf.io/cbeci/index

Validazione di un blocco e consenso

Proof of Stake (PoS)

Anziché vincolare la validazione di un blocco alla risoluzione, possono essere validatori solo i nodi che hanno una certa quantità di token associati alla blockchain.

- Permette di risparmiare computazione (e quindi energia)
- Prona ad alcuni problemi di sicurezza da gestire

Tipi di blockchain

Permissionless (*pubblica*): chiunque può partecipare alla blockchain (effettuare transazioni, validare blocchi)

Permissioned (*privata*): l'accesso è controllato dagli amministratori della blockchain (che più spesso è definita «Distributed Ledger»)

Applicazioni

Criptovalute

Criptovaluta: valuta digitale progettata come mezzo di scambio attraverso una rete di computer, senza essere coniata, gestita e sostenuta da un ente centrale.

- Puramente digitale, non esiste in forma «fisica»
- Controllo decentralizzato
- Sicurezza, immutabilità e integrità mantenute grazie ad una blockchain.

Es. Bitcoin

Criptovaluta e sistema di pagamento basato su blockchain.

La blockchain permettere di risolvere il problema della doppia spesa (double spending), cioè «duplicare» la stessa moneta digitale per usarla in più transazioni.

La validazione di un blocco mediante Proof-of-Work (PoW) evita il problema del double spending.

Es. Bitcoin

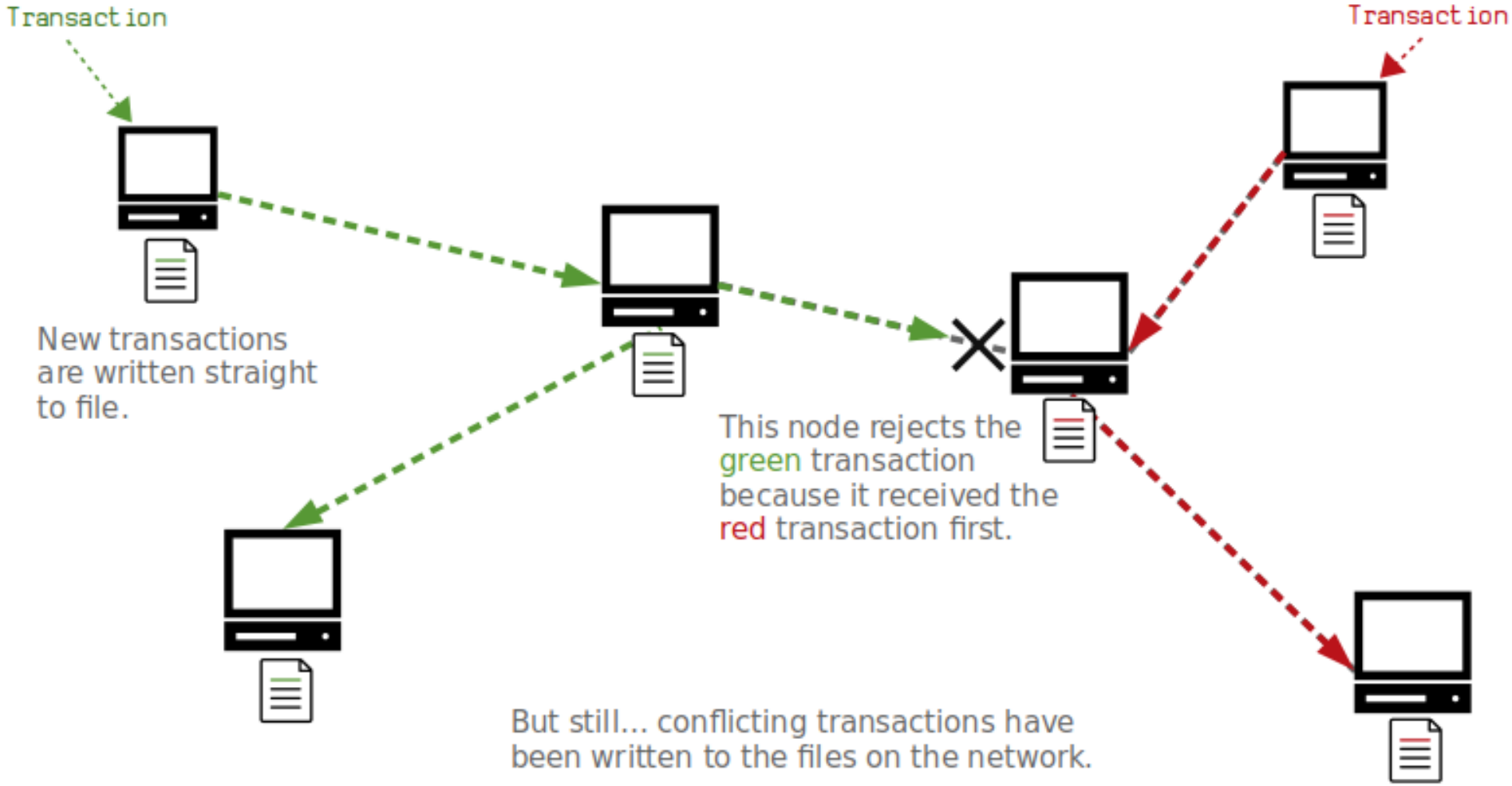


Immagine da: https://learnmeabitcoin.com

Es. Bitcoin

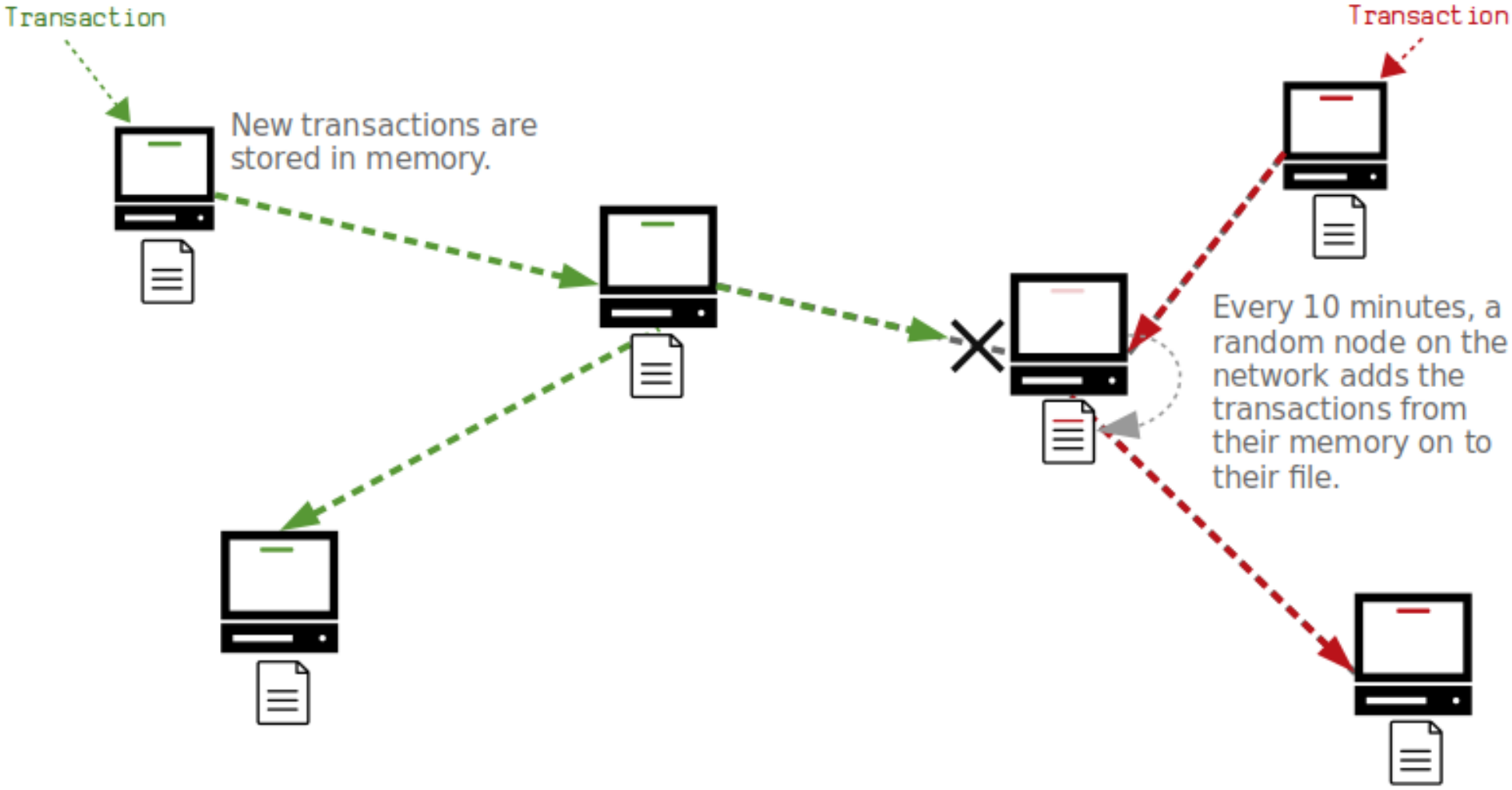


Immagine da: https://learnmeabitcoin.com

Es. Bitcoin

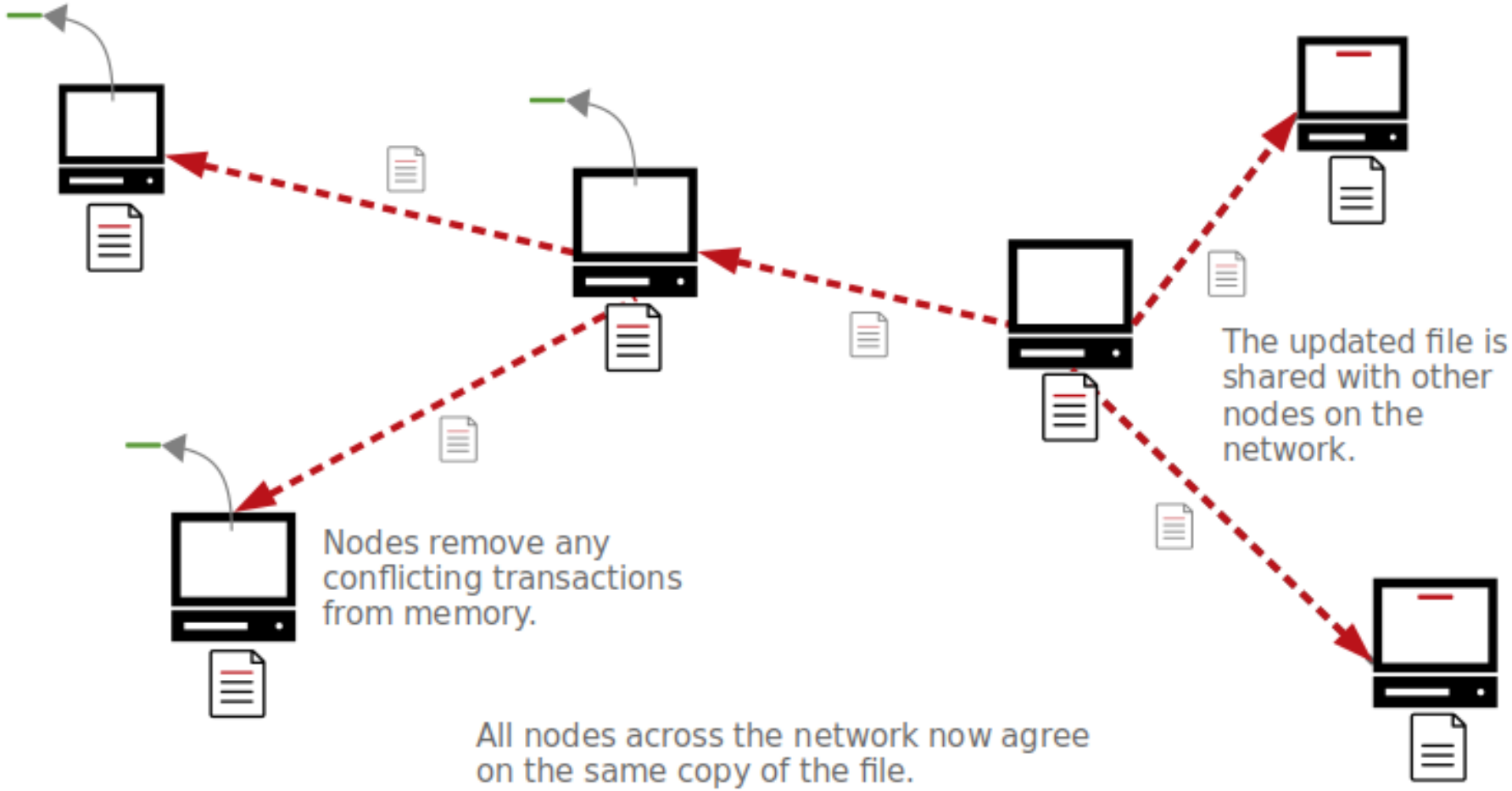


Immagine da: https://learnmeabitcoin.com

Es. Bitcoin – Funzionamento

Descritto nel white paper di Satoshi Nakamoto: «Bitcoin: A Peer-to-Peer Electronic Cash System»* (2008)

- La blockchain memorizza tutte le transazioni in bitcoin
- La validazione di un blocco, mediante PoW, viene premiata con un certo numero di nuovi bitcoin coniati
- Ogni 210.000 nuovi blocchi (~4 anni), la quantità di nuovi bitcoin coniati viene dimezzata (*bitcoin halving*)..

*https://bitcoin.org/bitcoin.pdf

Es. Bitcoin – Funzionamento

- Bitcoin halving, dai 50 iniziali (il primo blocco fu validato il 3 gennaio 2009) siamo a scesi a
  - 25 nuovi bitcoin per ogni blocco validato (2012)
  - 12,5 (2016)
  - 6,25 (2020)
  - Intorno al 2024, scenderemo a 3,125 nuovi bitcoin ogni nuovo blocco validato.
- Frazionamento minimo: 1 Satoshi = 0,00000001 BTC
- Questo impone un limite massimo al numero di Bitcoin: 21 milioni (che verrà raggiunto attorno al 2140)

Es. Bitcoin – Funzionamento

- Ogni 2016 nuovi blocchi aggiunti alla blockchain, il target per la PoW viene aggiustato cioè viene modifica la difficoltà della PoW, per far sì che (statisticamente) venga validato un nuovo blocco ogni 10 minuti
  - Se i 2016 blocchi sono stati generati più frequentemente di uno ogni 10 minuti, il target diminuisce, aumentando la difficoltà della PoW
  - Se i 2016 blocchi sono stati generati meno frequentemente di uno ogni 10 minuti, il target aumenta, diminuendo la difficoltà della PoW

Es. Bitcoin – Funzionamento

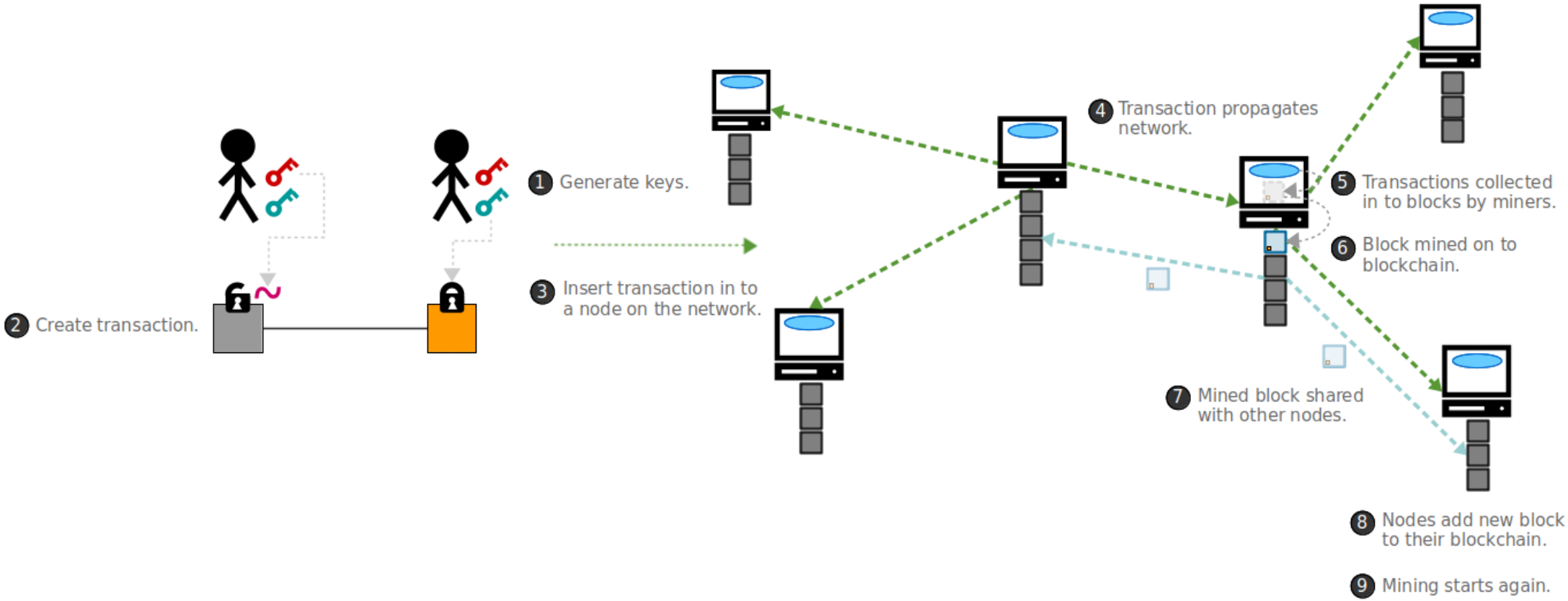


Immagine da: https://learnmeabitcoin.com

Smart contract

Smart contract: protocollo informatico per transazioni per eseguire, controllare o documentare automaticamente eventi e azioni secondo i termini di contratti o accordi.

- E' un programma che verificate alcune condizioni, esegue automaticamente delle transazioni (*if* `a` *then* `b`)
- Uno smart contract scritto nella blockchain è immutabile

Smart contract e blockchain

- La scrittura di uno smart contract nella blockchain avviene come qualsiasi altra transazione
  - La transazione includerà il codice dello smart contract
  - Dovrà essere inclusa in un blocco da validare
- Una volta validato il blocco, lo smart contract non può essere modificato e il suo stato iniziale dipende dal codice nello smart contract stesso
- Nel caso le condizioni dello smart contract dipendano da dati fuori dalla catena («off-chain»), servono applicazioni che recuperino questi dati e li scrivano sulla blockchain. Queste applicazioni sono dette oracoli.

Smart contract e blockchain

Funzionamento di un oracolo

- Tipicamente composto da componenti off-chain («oracle node») + smart contract
- Lo smart contract riceve richieste di dati da altri smart contract e passa le richieste alle componenti off-chain
- L'oracle node ottiene i dati e li passa allo smart contract per registrarli in altre transazioni

Smart contract e blockchain

Problemi

- Come verifichiamo che le informazioni provenienti dall'esterno siano corrette o non manomesse?
- Come ci assicuriamo che i dati siano sempre disponibili e aggiornati?

L'oracolo dovrebbe garantire:

- Autenticità e integrità
- Disponibilità del servizio offerto
- Attribuibilità e responsabilità

Smart contract – Applicazioni

- Pagamenti automatici. Es.: rimborso automatico di un biglietto del treno
  - 25% del biglietto per un ritardo tra i 60 e 120 minuti
  - 50% del biglietto per ritardo > 120 minuti

- Gestione della «supply chain»: smart contract possono essere usati per notificare alle parti problemi/violazioni
  - Tracciabilità dei prodotti e scambio di informazioni in real-time
  - Trasparenza nello scambio di informazioni tra le parti

Smart contract, blockchain e NFT

Contenuti digitali (immagini, video, testi, …) possono replicati «a costo zero» (o quasi)

Smart contract e blockchain possono essere combinate per introdurre «scarsità digitale»

Non-Fungible Tokens – NFTs

Smart contract, blockchain e NFT

Fungibilità: capacità di un certo bene (digitale o no) di essere scambiato equivalentemente con un altro bene dello stesso tipo

- Token fungibile: token (gettone) «interscambiabile». Es: 1 BTC può essere scambiato con qualunque BTC. Dopo lo scambio si è comunque in possesso di 1 BTC
- Token non-fungibile: token unico, indivisibile, non reciprocamente interscambiabile con altri NFT.

Smart contract, blockchain e NFT

- Un NFT ha un id univoco
- Tramite lo smart contract (un possibile standard: ERC-721) si regolano
  - La proprietà del token (ogni token ha un proprietario) e la verificabilità
  - Le modalità di cessione e utilizzo del token
- La blockchain garantisce l'immutabilità e l'integrità delle informazioni
- Ai «metadati» del token nello smart contract, può essere associato un qualunque oggetto digitale (un testo, una canzone, un video, un'immagine…)

Smart contract, blockchain e NFT

Artisti, creator, o chi ha la licenza relativamente ad un oggetto digitale (es. un'immagine) può creare un NFT e associare l'oggetto l'NFT

- Il processo si chiama «minting»
- Il proprietario dell'NFT è il proprietario dell'oggetto digitale associato

Esempio: il primo tweet della storia…

Primo tweet come NFT

POWER PLAYERS

Jack Dorsey sells his first tweet ever as an NFT for over $2.9 million

Published Mon, Mar 22 2021•3:07 PM EDT • Updated Wed, Mar 24 2021•2:10 PM EDT

Taylor Locke
@ITSTAYLORLOCKE

SHARE

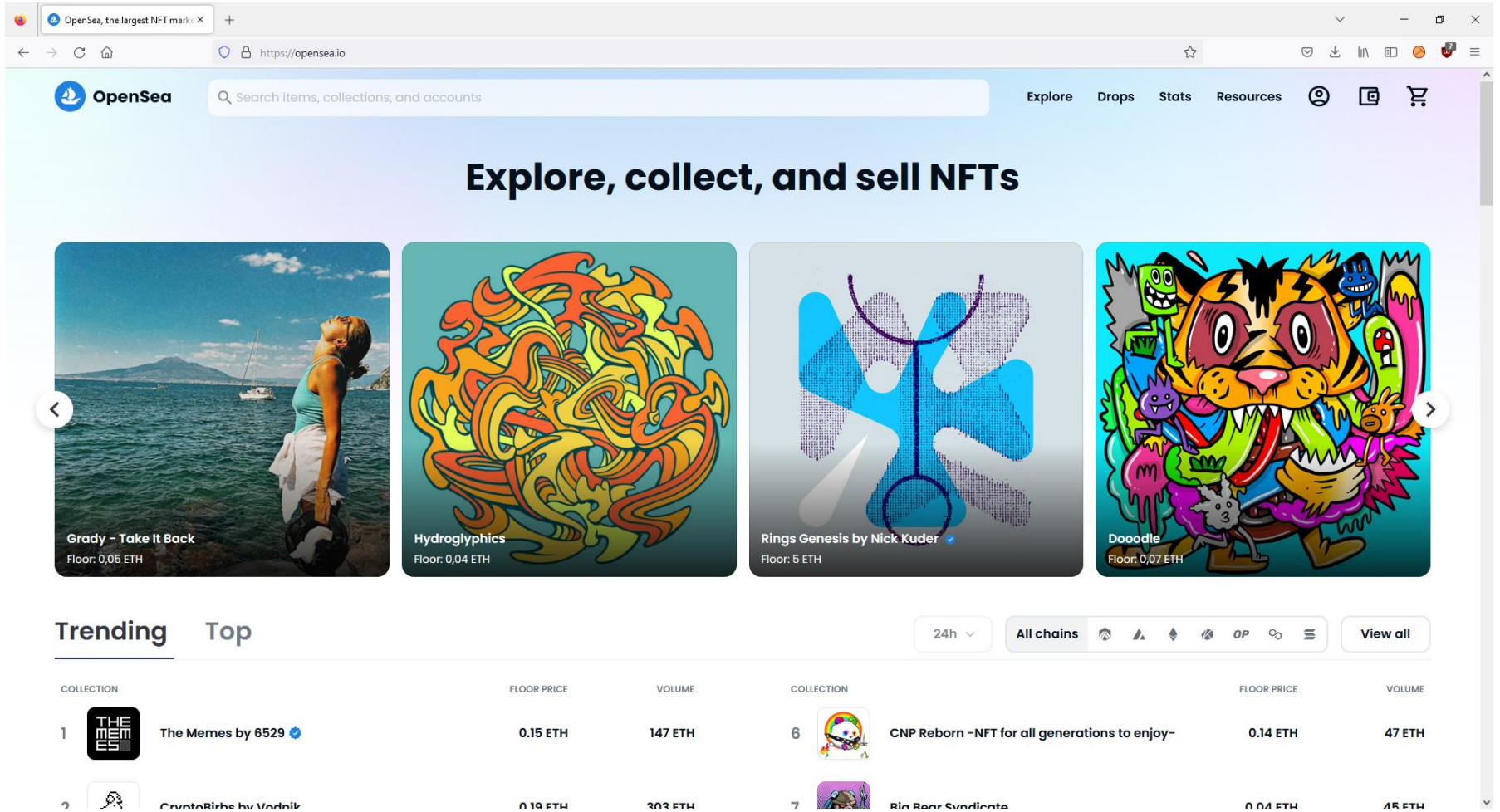
Prakash Singh | AFP | Getty Images

Trending Now

1. This 29-year-old super-saver earns $135,000 a year and plans to retire by 35
2. Parents of successful kids don't worry about screen time, expert says—they teach these 3 skills instead
3. My mom told me to read 'The Magic of Thinking Big': 5 quotes I'm using to help guide my career
4. Mark Cuban flew to Vegas to celebrate his company's $5.7

https://www.cnbc.com/2021/03/22/jack-dorsey-sells-his-first-tweet-ever-as-an-nft-for-over-2point9-million.html

Piattaforme per la vendita di NFT



https://opensea.io/

Smart contract, blockchain e NFT

Ma cosa possiede chi possiede un NFT associato ad un'opera digitale?

- Un token rappresenta un asset, un opera digitale ad esso associata, ma non è l'asset stesso
- Un file, in quanto tale, può essere duplicato
- L'NFT non può essere duplicato, ma altrettanto non vale l'immagine/video/audio/testo digitale ad esso associato

NFT = diritto a vantarsi?

Primo tweet come NFT

https://twitter.com/jack/status/20

Altre applicazioni degli NFT

- NFT per collezioni digitali
- NFT per ticket di eventi
- NFT per oggetti in-game (in-game items)
- NFT per gestione delle royalties
- …

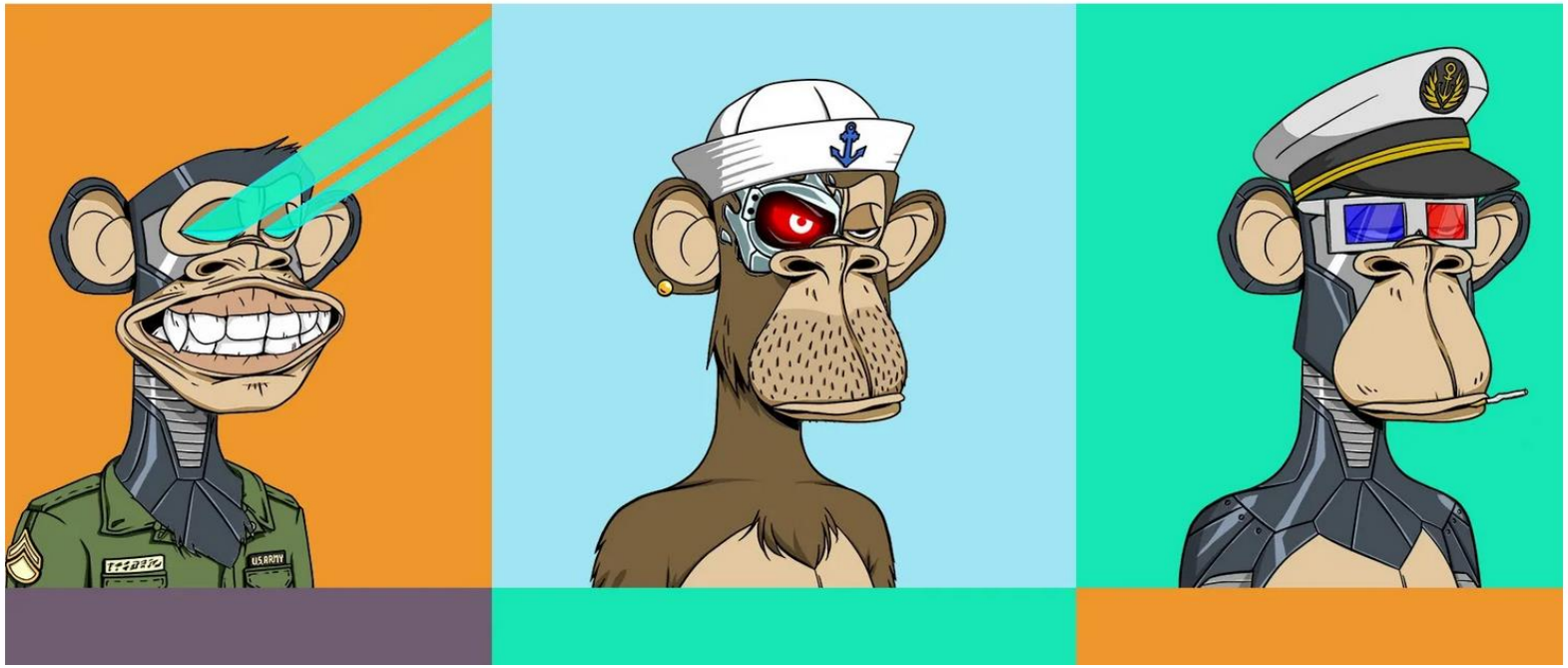
Sicurezza (e social engineering…)

WIRED SCIENZA ECONOMIA CULTURA GADGET SECURITY DIRITTI IDEE VIDEO PODCAST WIRED CONSIGLIA EVENTI NEWSLETTER MAGAZINE

TOMMASO MEO SECURITY 26.04.2022

Sono stati rubati alcuni nft Bored Ape che valgono milioni

I truffatori si sono introdotti nel profilo Instagram della famosa collezione e tramite un link fraudolento hanno rubato di un centinaio di token dai portafogli di alcuni utenti



https://www.wired.it/article/nft-bored-ape-rubati/