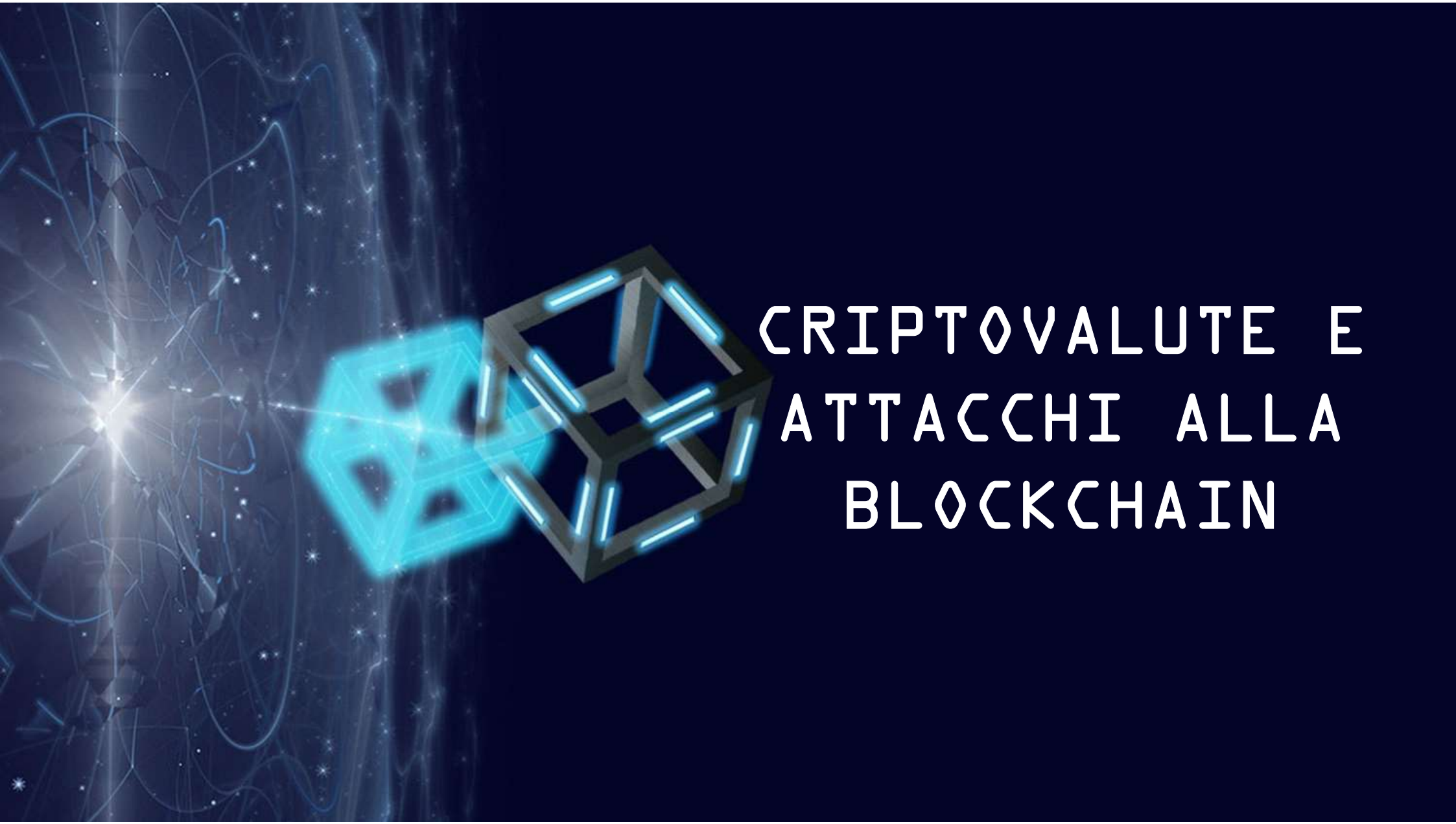
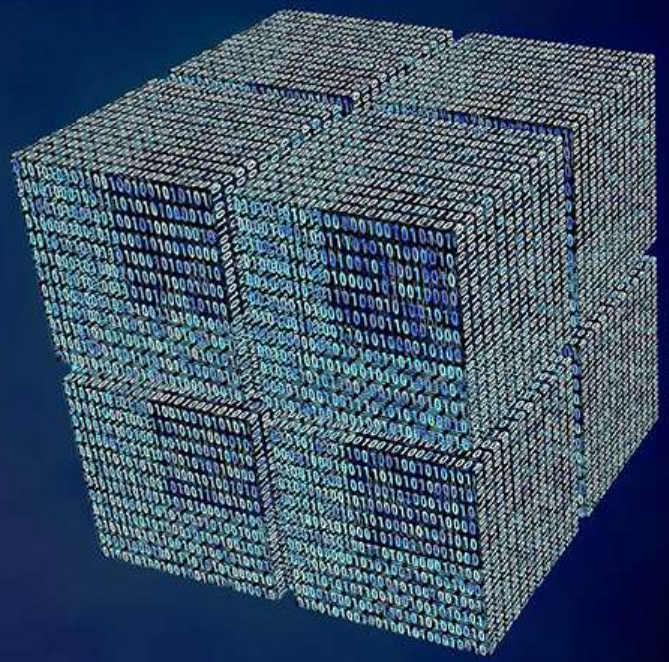
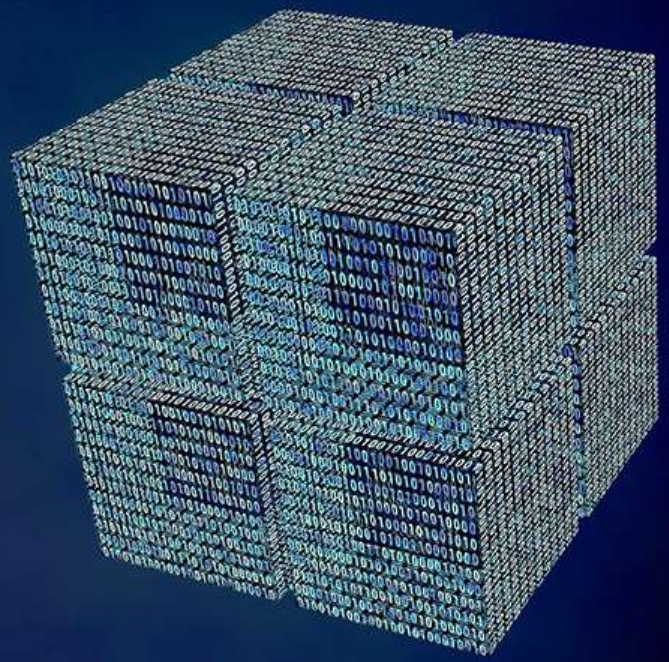

CRIPTOVALUTE E
ATTACCHI ALLA
BLOCKCHAIN

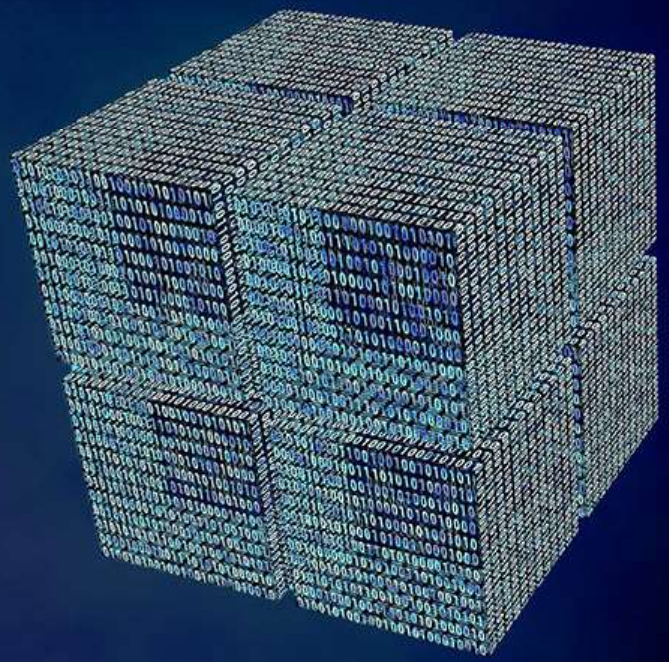
Indice:



Indice:



Indice:



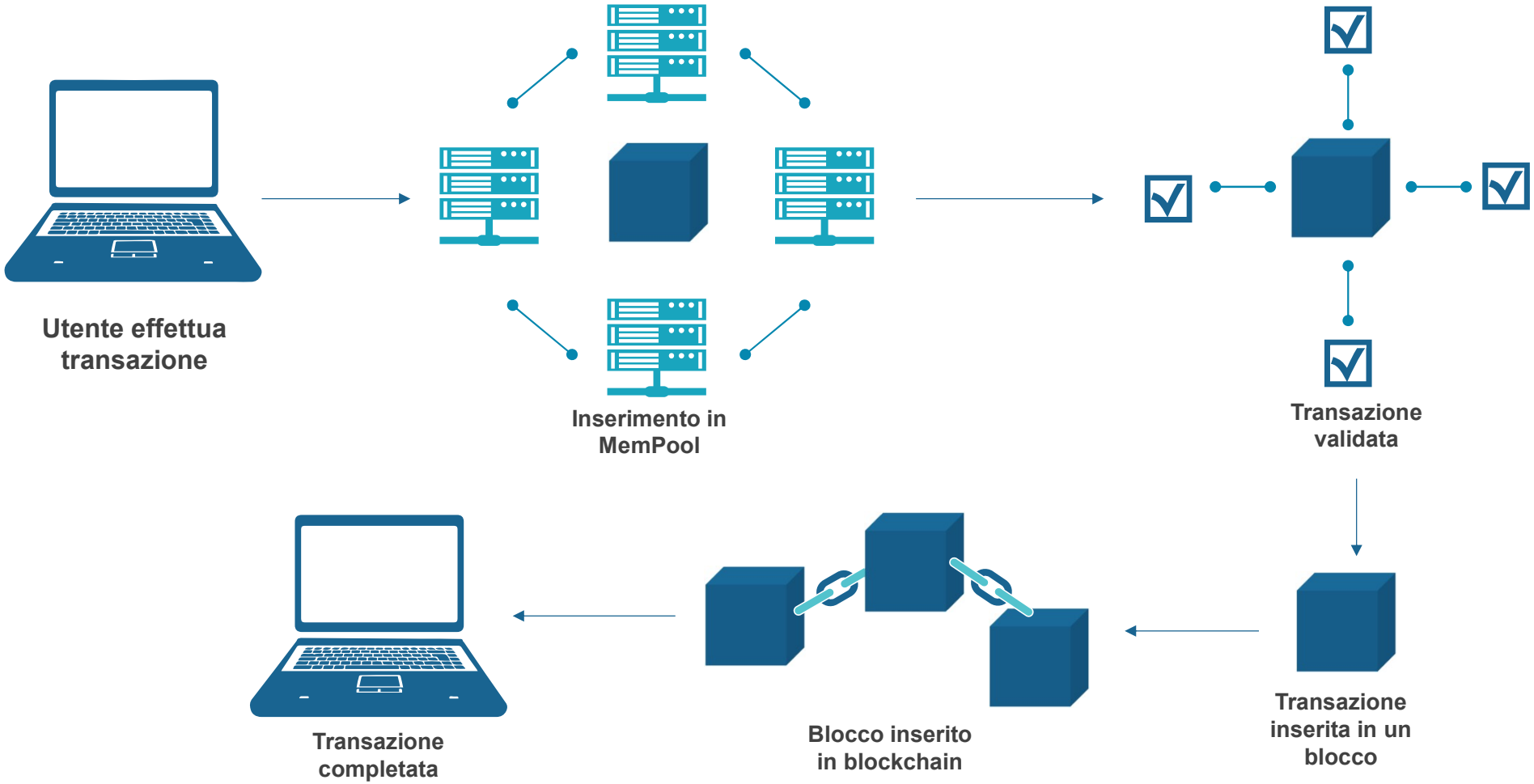
DEFINIZIONE

Bitcoin: A Peer-to-Peer Electronic Cash System

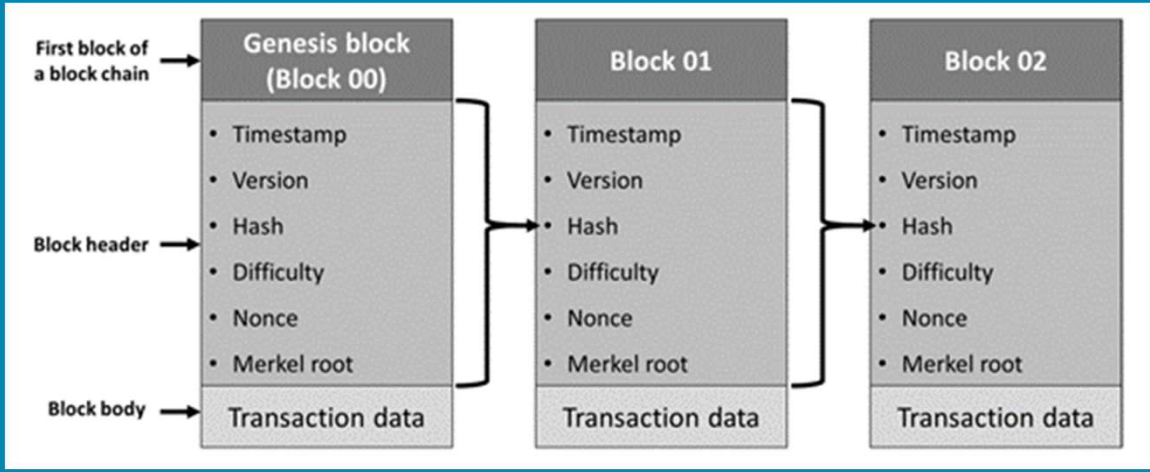
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

FUNZIONAMENTO



ANALISI DI UN BLOCCO



Composto da tre sezioni:

- Index
- Header
- Body

Index: codice univoco per identificare il blocco

Header: contiene i metadati come timestamp, nonce, Merkle root, nonce

Body: contiene tutte le transazioni che compongono il blocco

Tecniche crittografiche

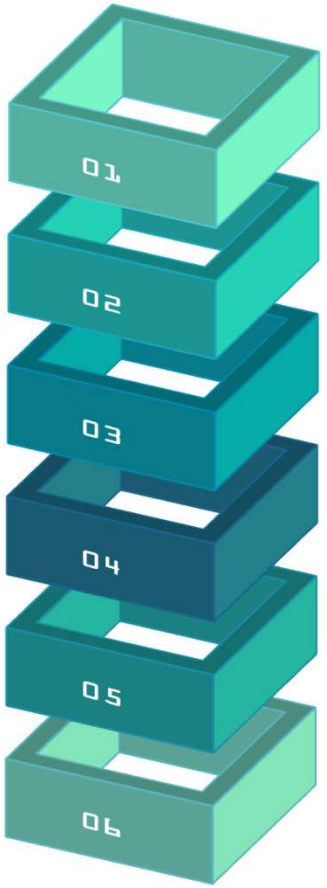
Le blockchain in generale utilizzano diverse tecniche crittografighe

Di seguito sono riportate le tecniche più utilizzate con una descrizione del loro utilizzo, e l'importanza che hanno nella blockchain

Public Key
Corrisponde all'address del wallet di un Utente, derivate dalla Private Key

SHA256
Utilizzato per hashare il blocco in se, il quale contiene: indice + header + transazione

Merkle Tree
Utilizzato per organizzare a struttura ad albero gli hash delle transazioni → Merkle Root



Private Key
Utilizzata per firmare digitalmente le transazioni, create tramite Curve Ellittiche

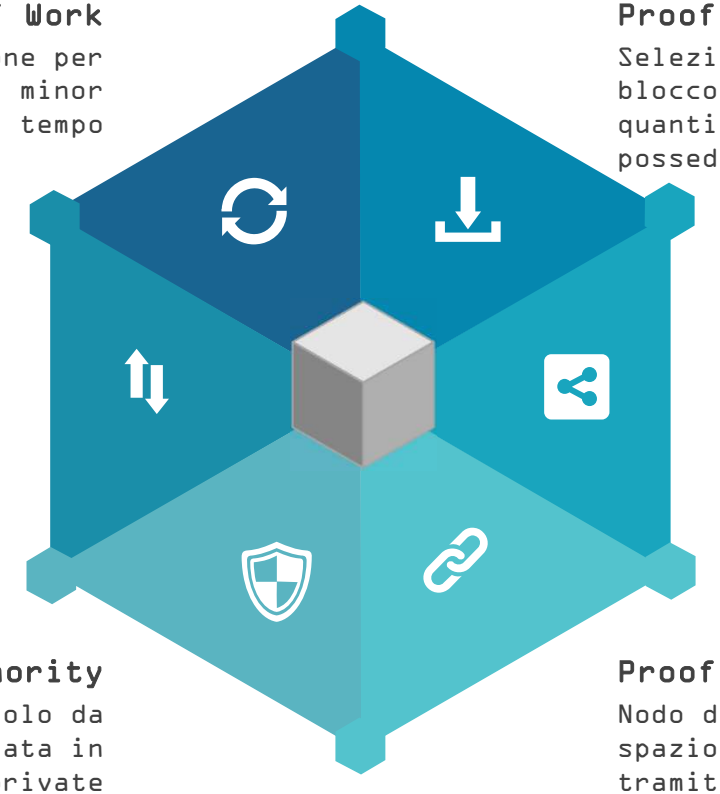
Hashing Transazioni
Informazioni della transazione hashati, la minima modifica cambierà l'hash

Nonce
Valore numerico che i miner devono trovare, se combinato con hash del blocco soddisfa condizioni dell'hash successivo

TIPOLOGIE DI CONVALIDAZIONE

Proof of Work
Miner in competizione per trovare il nonce nel minor tempo

Proof of Stake
Selezione per minare il blocco a partire dalla quantità di cryptovaluta posseduta



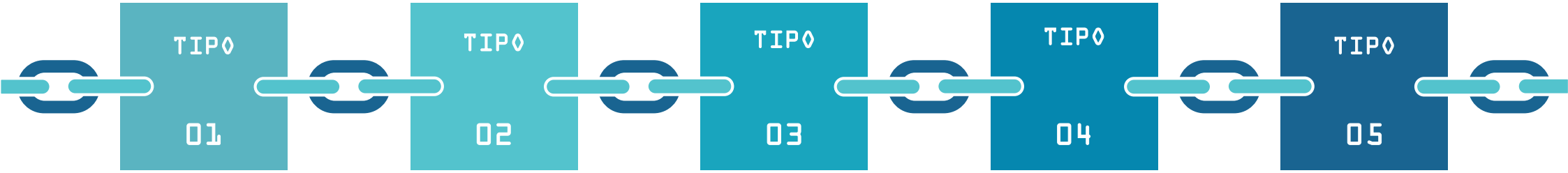
Proof of Burn
Nodo deve distruggere una quantità di criptovalute per dimostrare partecipazione

Delegated PoS
Unione di fondi piccoli eleggono un delegato che parteciperà all'estrazione

Proof of Authority
Blocchi convalidati solo da nodi autorizzati, usata in blockchain private

Proof of Space
Nodo dimostra il proprio spazio di archiviazione tramite prove di spazio

Tipologie di Blockchain



Pubblica / Privata

Pubblica permette accesso a chiunque, sia come nodo che utente.
Privata: consente accesso solo a nodi e utenti autorizzati, usate in ambito aziendale

Ibrida

Unione di blockchain pubbliche e private, utilizzate per bilanciare la privacy e trasparenza

Consorziata

Anch'essa è un ibrido, in quanto solo un gruppo selezionato partecipa al consenso ma non è completamente centralizzata

NFT

Consentono la creazione di token unici, utilizzata maggiormente per rappresentare opera d'arte o beni di collezione

Smart Contract

Consentono la creazione di contratti intelligenti, ovvero programmi autoeseguibili per l'esecuzione di accordi tra parti

MINING

Ruolo

Ruolo di vitale importanza per il funzionamento della blockchain

Costi

Data la potenza di calcolo utilizzata, ha un costo molto elevato

Processo

Processo attraverso il quale nuovi blocchi vengono aggiunti alla blockchain

BLOCK CHAIN

MemPool

Pool nella quale finiscono le transazioni prima di essere approvate

Ricompensa

Assegnata al primo miner in grado di risolvere il problem o che viene estratto

Sicurezza

Meccanismo che consente la decentralizzazione della rete

HALVING

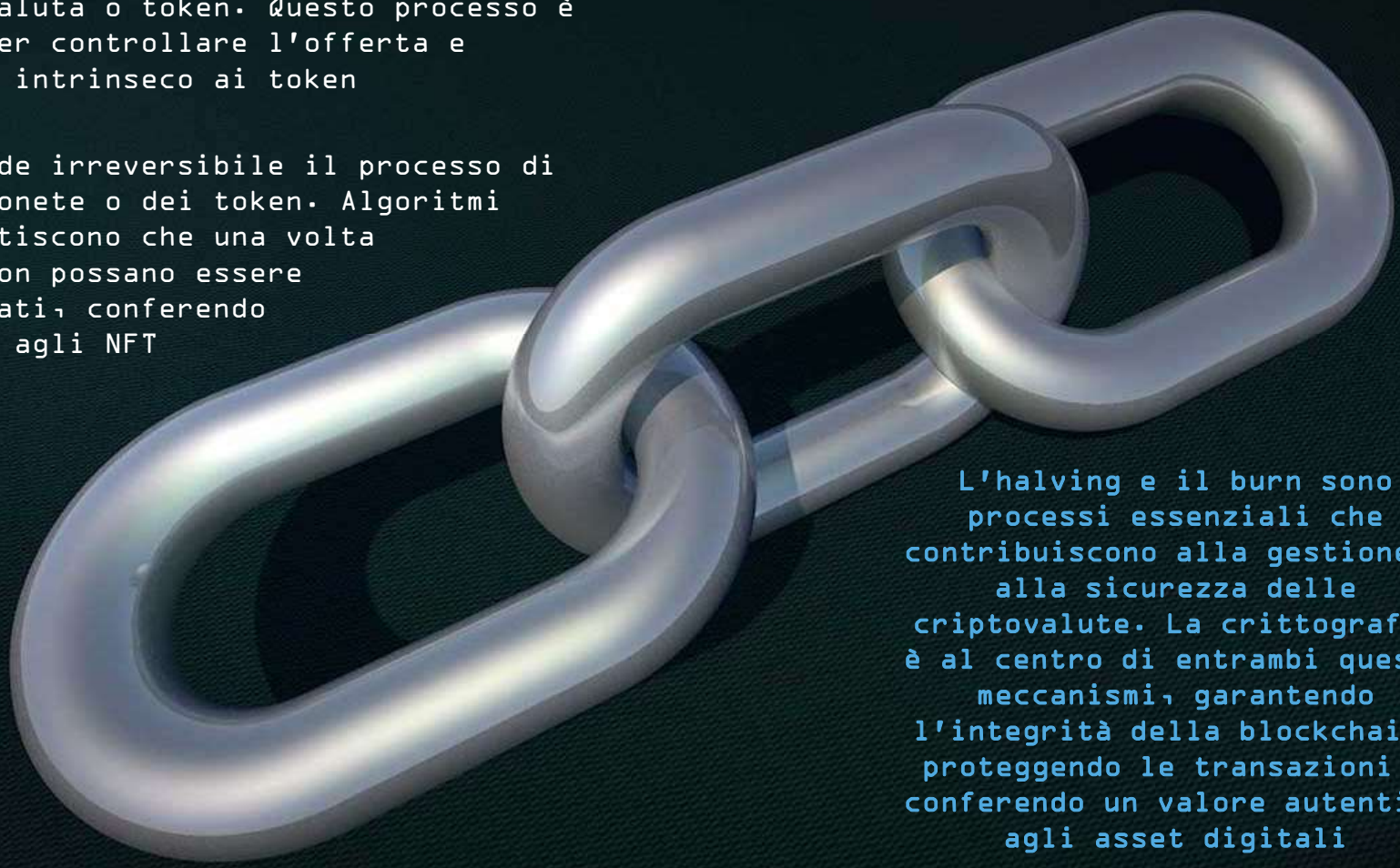
Meccanismo economico per il controllo dell'offerta, nel caso di Bitcoin avviene circa ogni 4 anni, ovvero 210.000 blocchi minati, il primo avvenne nel 2012, successivamente 2016, 2020, il prossimo sarà nel 2024 e ridurrà la ricompensa dei miner da 6,25 BTC a 3,125 BTC per blocco minato

> Regola di protocollo che influenza l'economia della criptovaluta

BURN

Atto di distruggere in modo irreversibile una certa quantità di criptovaluta o token. Questo processo è spesso utilizzato per controllare l'offerta e conferire un valore intrinseco ai token

La crittografia rende irreversibile il processo di distruzione delle monete o dei token. Algoritmi crittografici garantiscono che una volta bruciati, i token non possano essere recuperati o duplicati, conferendo un valore autentico agli NFT



L'halving e il burn sono processi essenziali che contribuiscono alla gestione e alla sicurezza delle criptovalute. La crittografia è al centro di entrambi questi meccanismi, garantendo l'integrità della blockchain, proteggendo le transazioni e conferendo un valore autentico agli asset digitali

TIPOLOGIE DI ATTACCHI ALLA BLOCKCHAIN

Attacchi alla Rete

Hanno l'obiettivo di prendere il controllo della rete per manipolarla a proprio piacimento

Attacchi all'utente

Atti a rubare le credenziali al fine di rubare I fondi dell'utente

Attacchi al nodo

Maggiormente usati per isolare un nodo in modo tale da impedirgli di svolgere il suo funzionamento

Attacchi agli Smart Contract

Mirano a modificare il codice per sfruttare exploit o vulnerabilità del contratto per trarne profitto

TIPOLOGIE DI ATTACCO PER DOUBLE SPENDING

Obiettivo:

Sfruttare il breve periodo di tempo tra la conferma di una transazione e la sua registrazione permanente nella blockchain

Race attack:

Corsa di 10 minuti, nel quale si inviano due transazioni in rapida successione cercando di invalidare la prima tramite la seconda

Attacco al 51%:

Modifica delle transazioni hackerando almeno il 51% dei nodi che compongono l'Hash Rate di una blockchain

Finney attack:

Nodo prova ad effettuare il double spending, ma dovebbe essere sicuro di essere scelto per il mining del blocco successive, scoperto da Hal Finney

A SIMPLE BLOCKCHAIN

- ☑ Linguaggio utilizzato → Python e HTML
- ☑ Carattteristiche: firma, genesis block
- ☑ Funzionamento in localhost
- ☑ Librerie principali: Flask, json, rsa

BIBLIOGRAFIA

Di seguito la lista di tutte le risorse consultate:

- Wikipedia
- Blockchair.com
- Blockchain.com
- White Paper di Bitcoin
- Coindesk.com
- ChatGPT
- Binance
- Coinbase
- BitPanda Academy
- Prof. Carnabuci
- Youtube


GRAZIE
DELL'ATTENZIONE