

Tecnologia Blockchain e Criptovalute



Andrea Lisi

Università di Pisa - Informatica
Centro Nazionale delle Ricerche - IIT

Crittografia 2021
Pisa



Scaletta



Parte 1

- Cosa sono le criptovalute?
- Come funziona Bitcoin? Una spiegazione gentile

Parte 2

- Come funziona Bitcoin? Entriamo nei dettagli

Parte 3

- Altri progetti e campi applicativi

Domande frequenti

The background features a network diagram with light blue circular nodes containing white padlock icons. These nodes are interconnected by thin grey lines. Some nodes are larger than others, and the connections form a complex web. The overall aesthetic is clean and modern, with a light blue and white color palette.

PARTE 1



**Che cosa sono le
criptovalute?**



Che cosa sono le criptovalute?

Contesto storico, siamo nel 2009





Che cosa sono le criptovalute?



Contesto storico, siamo nel 2009

Viene pubblicato online un articolo
intitolato

“*Bitcoin: A Peer-to-Peer Electronic Cash System*”

firmato da

Satoshi Nakamoto

[Bitcoin]

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.



Che cosa sono le criptovalute?

Che cosa è una **valuta digitale**?

- È una valuta che esiste **SOLTANTO** in forma digitale, e quindi utilizzabile soltanto da computers^[Investopedia]

Che cosa è una **criptovaluta**?

- È una valuta digitale resa sicura grazie a tecniche di crittografia che rendono quasi impossibile spendere due volte la stessa moneta^[Investopedia]





Che cosa sono le criptovalute?

Bitcoin è il primo esempio concreto di criptovaluta

- Ma non la prima concezione di valuta digitale (1983)

Ma come si differenzia da un pagamento con Mastercard?

- Un pagamento online in Euro è un processo digitale di trasferimento, transazione, di una moneta fisica tra conti correnti (o altro)



The background features a network diagram with nodes and connections, overlaid with a grid of padlock icons. The padlocks are arranged in a pattern that suggests a secure network or blockchain structure. The text is centered in the middle of the image.

Come funziona Bitcoin? Una spiegazione gentile



Come funziona Bitcoin?



Per capire il funzionamento di Bitcoin servono due concetti fondamentali

- Transazione
- Registro, o libro contabile

CONTO CORRENTE

DATA	DESCRIZIONE	IMPORTO	
		DARE	AVERE
23-2-19	Banq. N. 10918	1296	
21-4-19	Asseque Banca	15000	
21-5-19	"	10000	
9-6-19	"	10000	
30-6-19	"	10000	
25-8-19	"	5000	
1-9-19	"	1000	
1-1-20	Asseque Banca	10000	
31-1-20	Asseque Banca	200	
	- Poste sul prelev.		
	- in natura, 4/30/20	1299	
	- Poste sul'acceden		
	ca. n. 100, 2/3/20	110	
	- Ricavo su banca		
	sul mio prelev. in		
	natura, 4/30/20		360
	- Liquidazione		
	del mio prelev.		
	del 1/1/20		4500
	- Saldo		88
		75449	75449

- a mano a pag. 6



Come funziona Bitcoin?



Pagamento in contanti

- Transazione: il passaggio di banconote o monete
- Libro contabile: un documento personale

Pagamento bancario

- Transazione: un movimento tra conti correnti
- Libro contabile: conto corrente della banca

CONTO CORRENTE			
DATA	DESCRIZIONE	IMPORTO	
		DARE	AVERE
23.2.17	Banq. Vita H? 10917	1296	
21.4.17	assegno Banca Vita	15000	
21.5.17	" " " "	10000	
9-6-17	" " " "	15000	
30.6.17	" " " "	10000	
25-8-17	" " " "	5000	
12.9.17	" " " "	1000	
11.10.17	assegno Banca Vita	13200	
31.12.17	assegno Vita H?	200	
	- Poste Vita H?		
	- in natura, 4/30/2017	1299	
	- Poste Vita H?		
	- in natura, 30.12.17	110	
	- Poste Vita H?		
	- in natura, 4/30/2017		360
	- Poste Vita H?		
	- in natura, 12/17		4500
	- Poste Vita H?		
	- Soldo		75449
	- a mano a pag. 6	75449	



Come funziona Bitcoin?

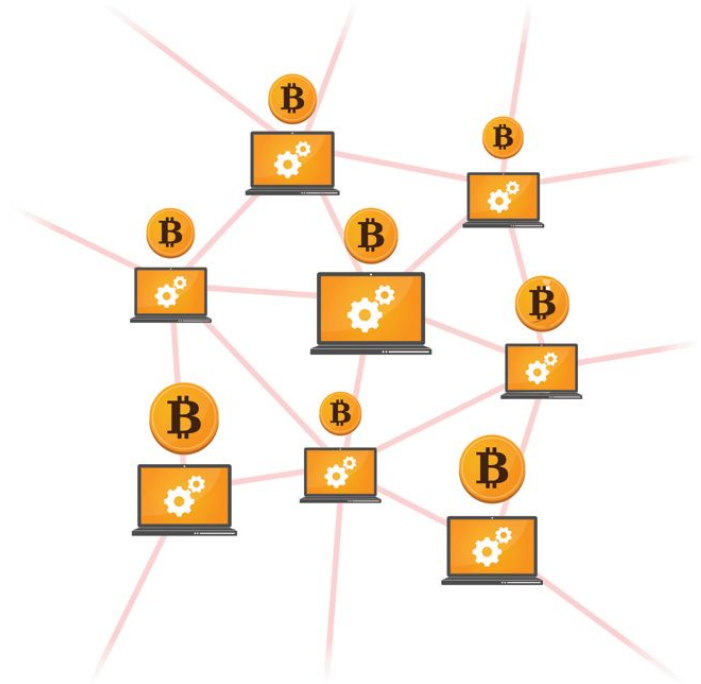


Bitcoin è formata da una rete P2P di nodi che eseguono il software Bitcoin

E.g. Bitcoin core^[BitcoinCore]

Ogni nodo è autorizzato ad eseguire una transazione

Ogni nodo memorizza il libro contabile dell'intera rete
Bitcoin





Come funziona Bitcoin?



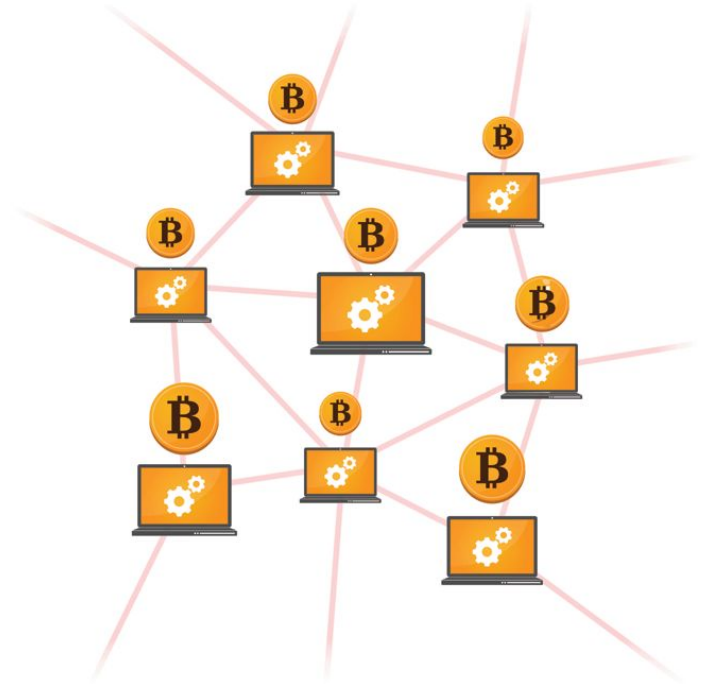
Bitcoin è formata da una rete di computer connessi tra di loro grazie ad un software

Ogni nodo è autorizzato ad eseguire una transazione

Ogni nodo memorizza il libro contabile dell'intera rete
Bitcoin

Problema

Se ogni nodo ha il libro contabile, come viene aggiornato?





Come funziona Bitcoin?

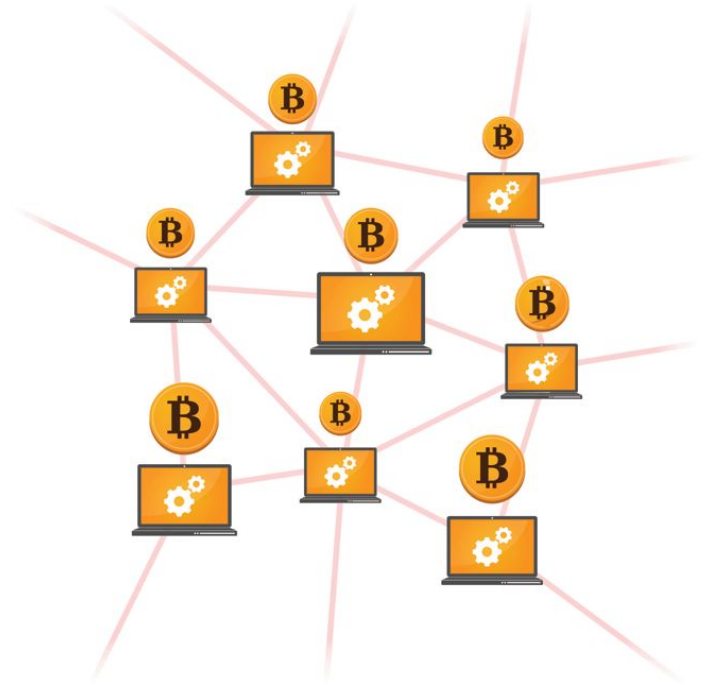


Tutti i nodi devono essere d'accordo

- Ovvero, inserendo le stesse transazioni nello stesso ordine

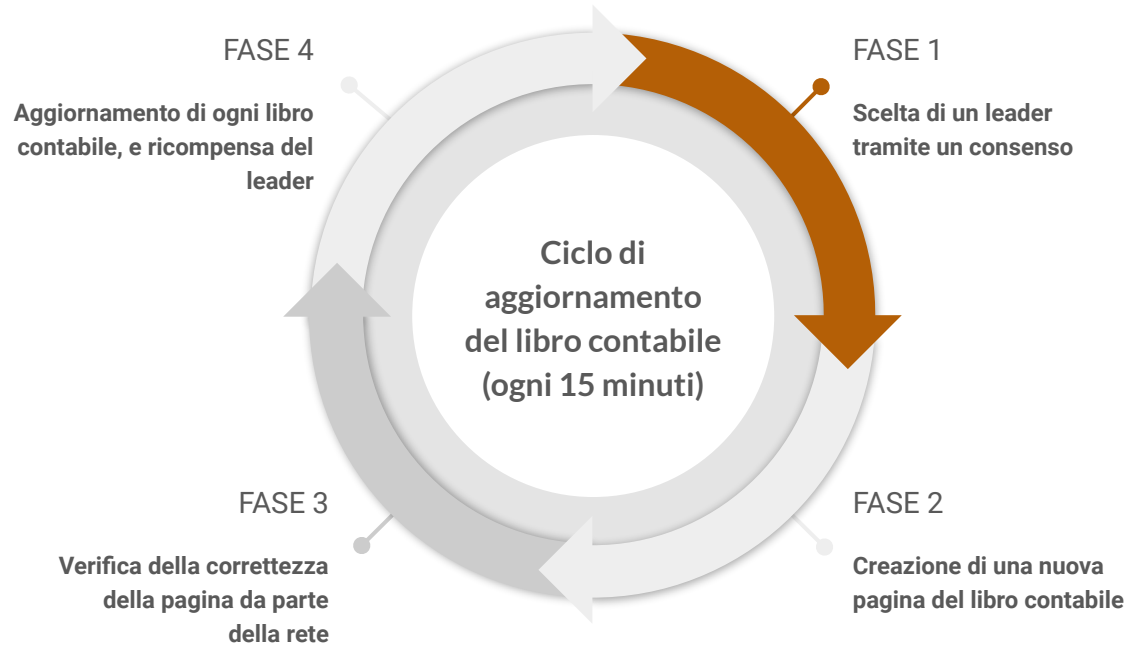
Una nuova pagina viene prodotta ad intervalli

- Circa 15 minuti





Come funziona Bitcoin?





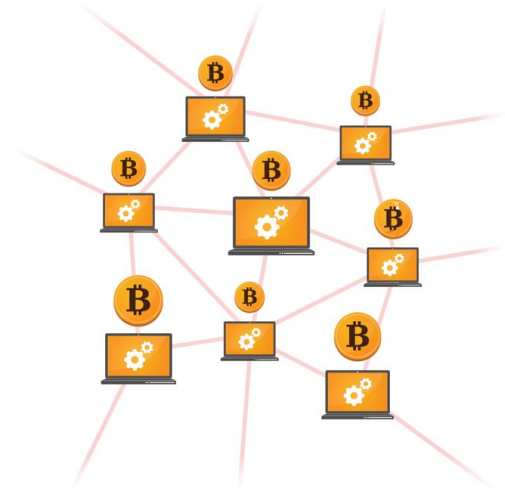
Come funziona Bitcoin?



FASE 1: Scelta di un leader tramite un consenso

Il leader proporrà la nuova pagina del libro contabile con le transazioni

- Competizione tra i computer della rete





Come funziona Bitcoin?



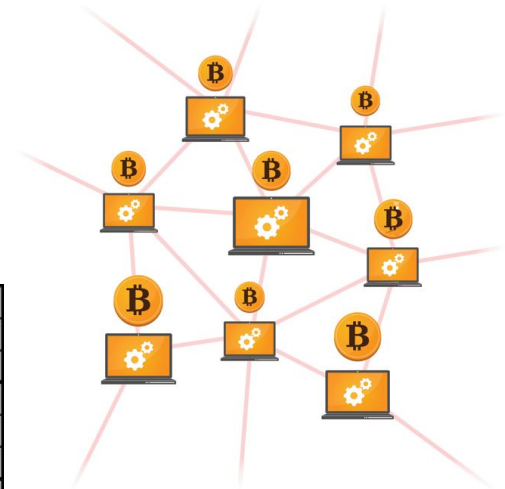
FASE 1: Scelta di un leader tramite un consenso

Il leader eletto sarà colui che per primo risolverà un puzzle

- Un puzzle è difficile da risolvere, ma una volta risolto è facile vedere se è risolto bene
- Il sudoku funziona con lo stesso principio



5	3		7				
6			1	9	5		
	9	8				6	
8			6				3
4			8	3			1
7			2				6
	6				2	8	
			4	1	9		5
			8			7	9





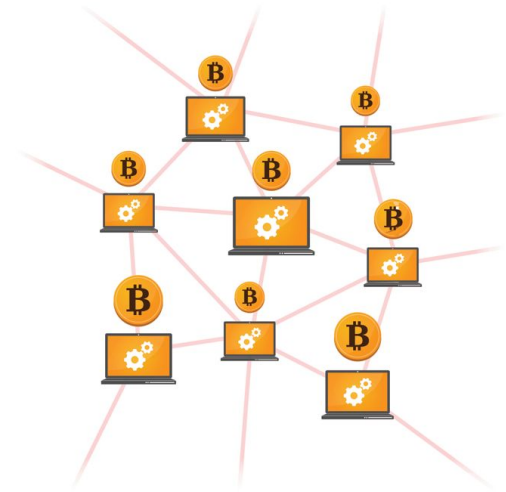
Come funziona Bitcoin?



FASE 1: Scelta di un leader tramite un consenso

In Bitcoin il puzzle è crittografico, la cui difficoltà viene bilanciata nel tempo così che la risoluzione impieghi circa 15 minuti di tempo

- Un po' come aumentare o diminuire le tessere “cielo blu” in un puzzle
- Se è troppo facile, la rete diventa inconsistente
- Se è troppo difficile, nessuno partecipa





Come funziona Bitcoin?





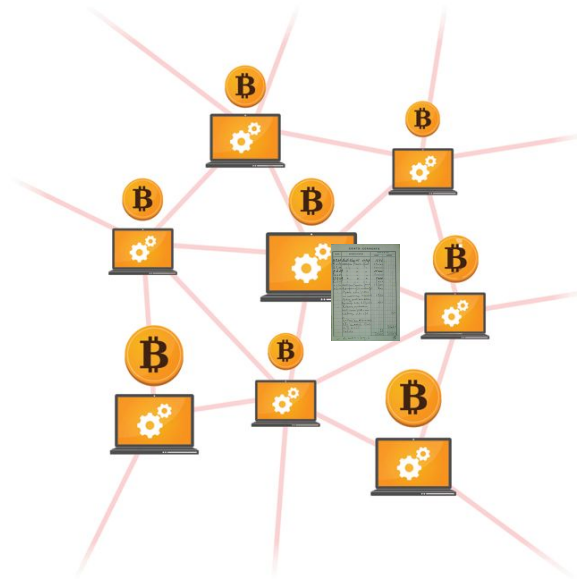
Come funziona Bitcoin?



FASE 2: Creazione di una nuova pagina del libro contabile

Il computer vincitore, il leader, è in carica di collezionare una porzione delle transazioni richieste dalla rete, e compilare così la nuova pagina del libro contabile

Il leader comunica a tutta la rete la nuova pagina





Come funziona Bitcoin?



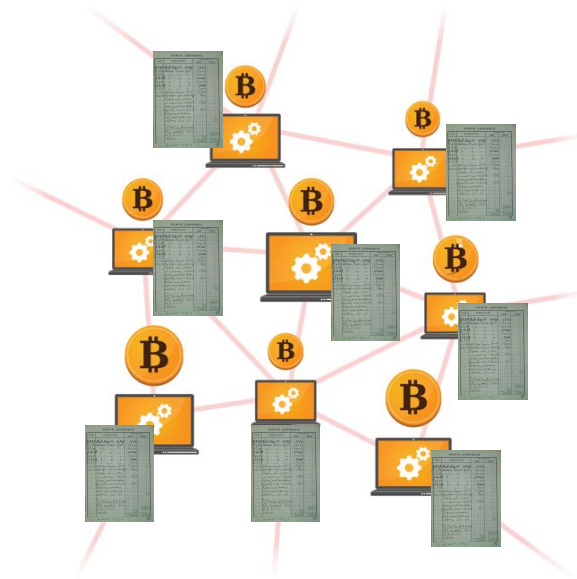


Come funziona Bitcoin?



FASE 3 Verifica della correttezza della pagina da parte della rete

Tutti i computer della rete ricevono la pagina e, basandosi sulla propria copia del libro contabile, controllano che le transazioni inserite siano corrette





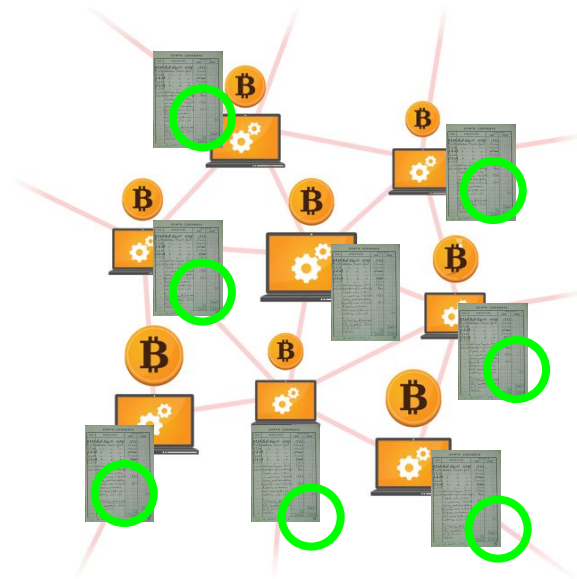
Come funziona Bitcoin?



FASE 3 Verifica della correttezza della pagina da parte della rete

Tutti i computer della rete ricevono la pagina e, basandosi sulla propria copia del libro contabile, controllano che le transazioni inserite siano corrette

- Se lo sono, accettano la pagina





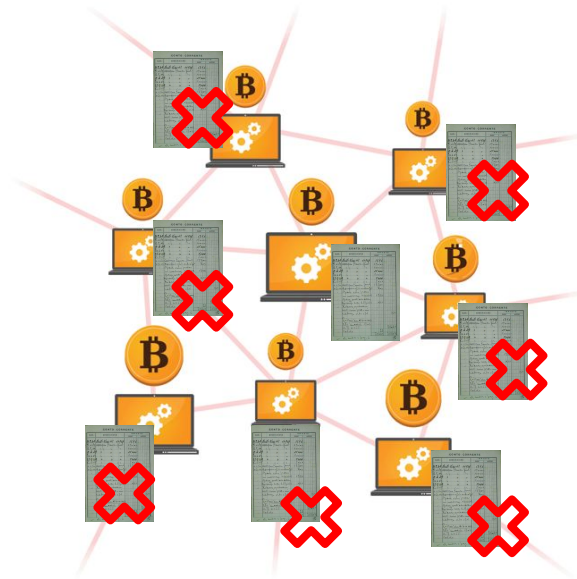
Come funziona Bitcoin?



FASE 3 Verifica della correttezza della pagina da parte della rete

Tutti i computer della rete ricevono la pagina e, basandosi sulla propria copia del libro contabile, controllano che le transazioni inserite siano corrette

- Se lo sono, accettano la pagina
- **Altrimenti la rifiutano**





Come funziona Bitcoin?





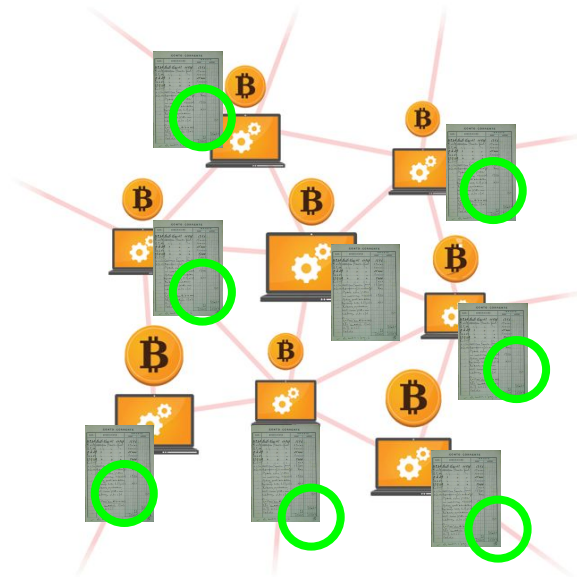
Come funziona Bitcoin?



FASE 4 Aggiornamento di ogni libro contabile, e ricompensa de leader

Ogni computer aggiorna il proprio libro contabile con la nuova pagina

La nuova pagina conterrà una transazione speciale che ricompensa il leader con una quantità fissa di Bitcoin come prei per aver vinto la competizione





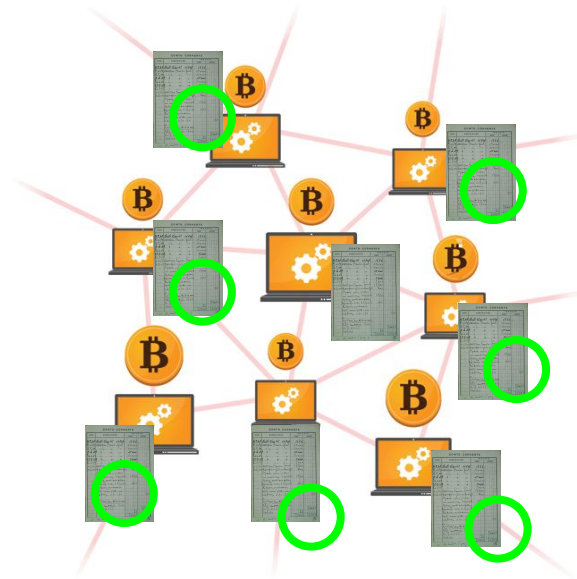
Come funziona Bitcoin?



La ricompensa è la motivazione principale per la quale i computer competono

- Risolvere il puzzle crittografico richiede una grande quantità di energia elettrica

Inoltre, il leader trattiene una piccola commissione da ogni transazione





Come funziona Bitcoin?




Bitcoin vive grazie agli incentivi

- I partecipanti sono intenzionati a giocare secondo le regole per poter guadagnare
- Se giocare sporco fa scappare gli utenti, il valore di Bitcoin crollerebbe e non ci sarebbe nessun guadagno



The background features a network diagram with light blue circular nodes connected by thin grey lines. Each node contains a white padlock icon. The nodes vary in size, with some being significantly larger than others. The overall aesthetic is clean and modern, with a light blue and white color palette.

PARTE 2



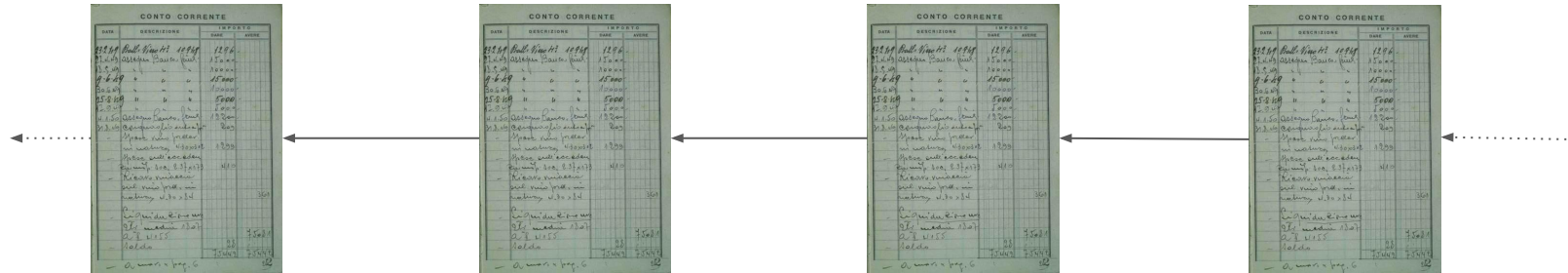
**Come funziona Bitcoin?
Entriamo nei dettagli**



Struttura dati



Ogni nuova pagina del libro contabile è collegata a quella precedente



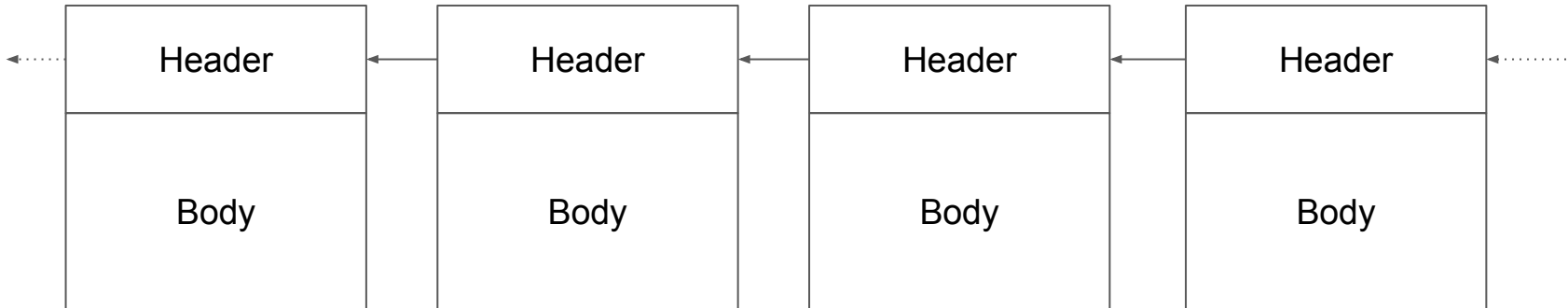
Si crea così una catena di pagine



Struttura dati



The image shows four identical handwritten ledger pages, each titled "CONTO CORRENTE". Each page is a table with columns for "DATA", "DESCRIZIONE", "DEBITO", and "CREDITO". The data is handwritten in ink on a grid background. The entries include various transactions such as "Rendita", "Riscossione", "Pagamento", and "Saldo". The final entry on each page is "Saldo" with a value of 25000. The pages are connected by arrows pointing from right to left, indicating a sequence of records.



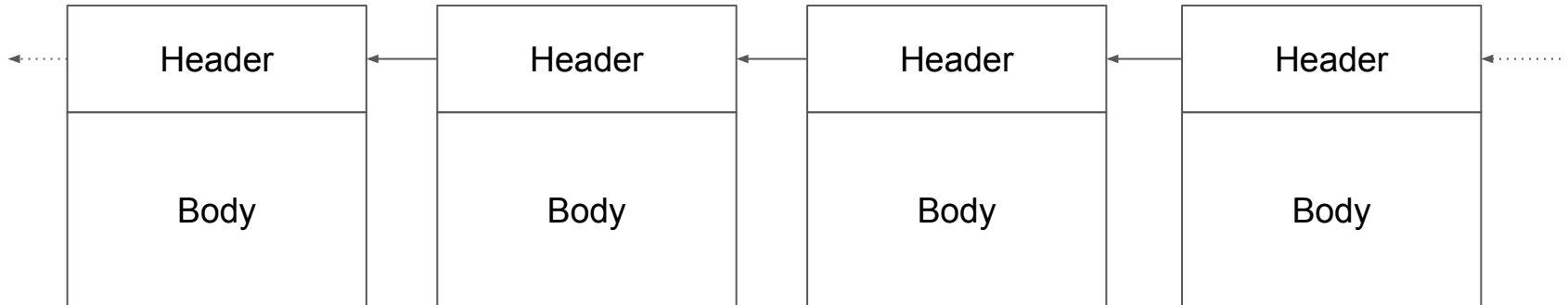


Blockchain



Il libro contabile è conosciuto come Blockchain. Ogni blocco è composto da

- Header: metadati e linking information
- Body: lista di transazioni

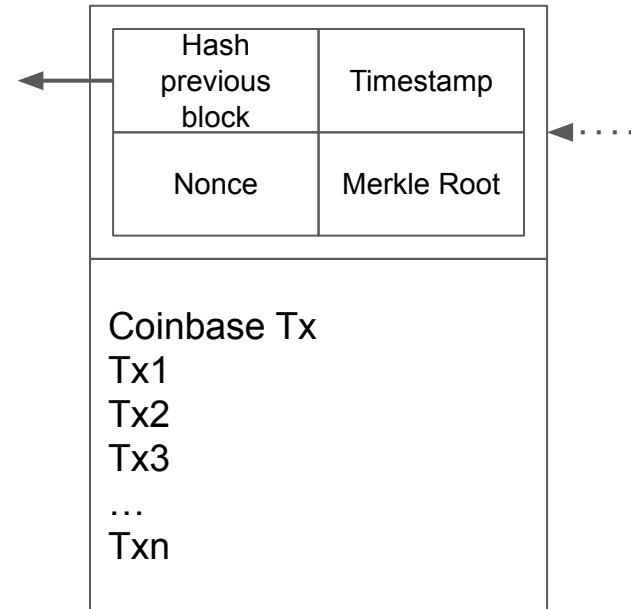




Into the block



Informazioni nell'header:



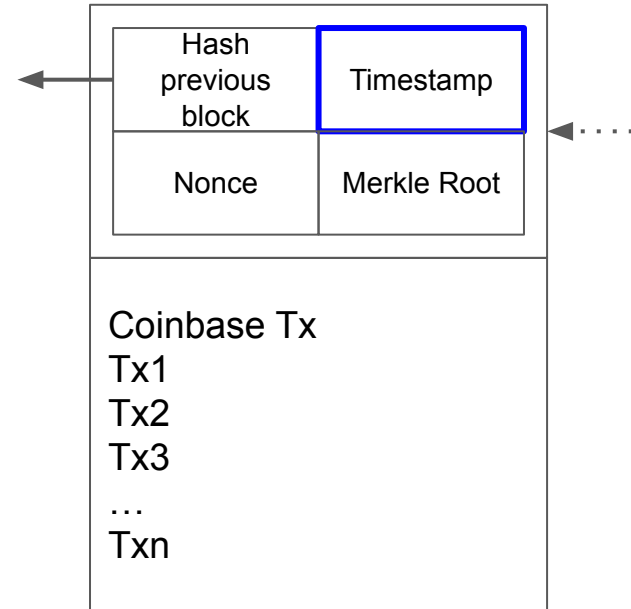


Into the block



Informazioni nell'header:

- **Timestamp**



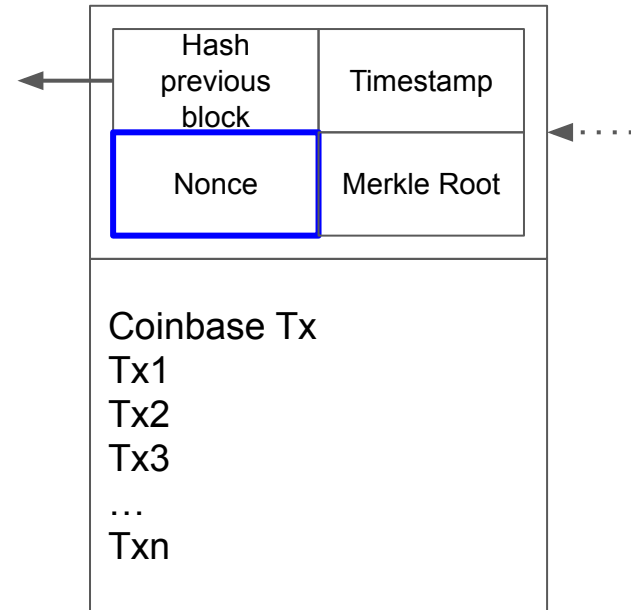


Into the block



Informazioni nell'header:

- Timestamp
- Nonce





Nota: Funzioni hash

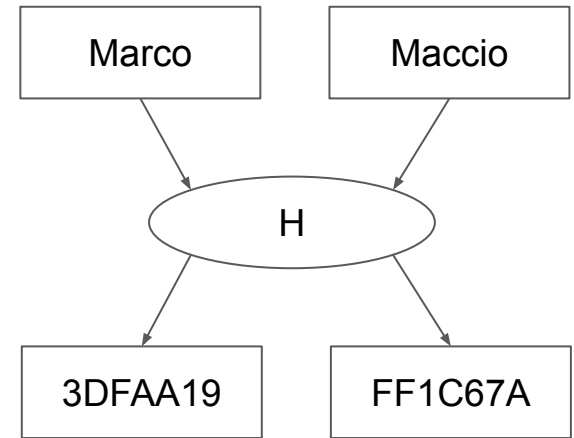


Funzione hash $H(): X \rightarrow Y$

- Grandezza di X: arbitrariamente grande
- Grandezza di Y: fissa
- Ridurre la probabilità di collisioni

Funzione hash crittografica

- **Pre-image resistance:**
 - Dato y , difficile calcolare x tale che $H(x) == y$
- **Second pre-image resistance:**
 - Difficile trovare $x1 \neq x2$ tale che $H(x1) == H(x2)$



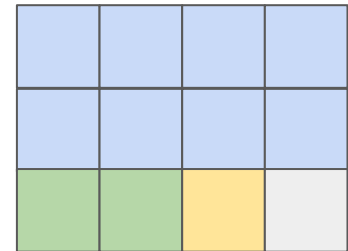
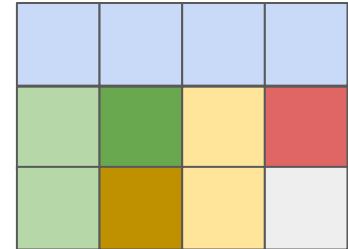


Il puzzle crittografico: Proof of Work



Trovare un valore **nonce** tale che

- $\text{Sha256}(\text{block_header}, \text{nonce}) < \text{value}_{\text{difficulty_target}}$
 - Maggiore il $\text{difficulty_target}^{\text{[Difficulty]}}$
 - Minore il $\text{value}_{\text{difficulty_target}}$
 - Maggiori i tentativi
- Unico approccio: forza bruta su nonce



Esempio:

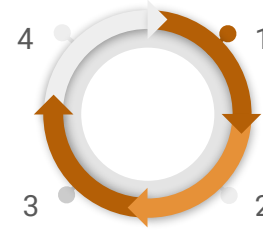
$\text{Sha256}(\text{block_header}, \text{nonce1}) = 00\text{AA}23..1$ NO

$\text{Sha256}(\text{block_header}, \text{nonce2}) = 0\text{FAA}23..1$ NO

...



Il puzzle crittografico: Proof of Work



Difficile da risolvere, ma facile da verificare

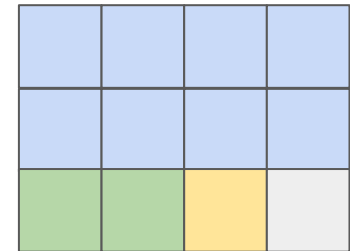
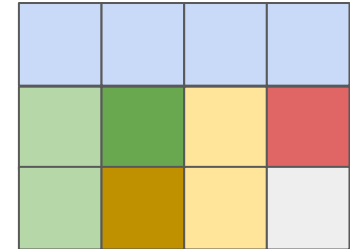
$\text{Sha256}(\text{block_header}, \text{nonce42}) = 0000000..00\text{FAA231}$ SI

Gli altri nodi ricevono il nuovo blocco, e controllano che

$\text{Sha256}(\text{block_header}, \text{nonce42}) < \text{value}_{\text{difficulty_target}}$

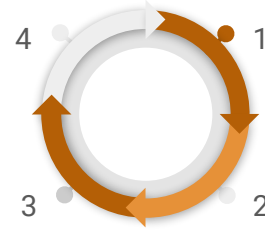
Noto come “che il risultato inizi per un minimo numero di “0” ”

- Sha256 pre-image resistance ci assicura che nonce42 sia difficile da trovare “a caso”





Il puzzle crittografico: Proof of Work



Difficile da risolvere, ma facile da verificare

$\text{Sha256}(\text{block_header}, \text{nonce42}) = 0000000..00\text{FAA231}$ SI

Gli altri nodi ricevono il nuovo blocco, e controllano che

$\text{Sha256}(\text{block_header}, \text{nonce42}) < \text{value}_{\text{difficulty_target}}$

Noto come “che il risultato inizi per un minimo numero di “0” ”

- Sha256 pre-image resistance ci assicura che nonce42 sia difficile da trovare “a caso”

0	0	0	0
A	E	4	1
4	2	0	F

0	0	0	0
0	0	0	0
F	F	4	1

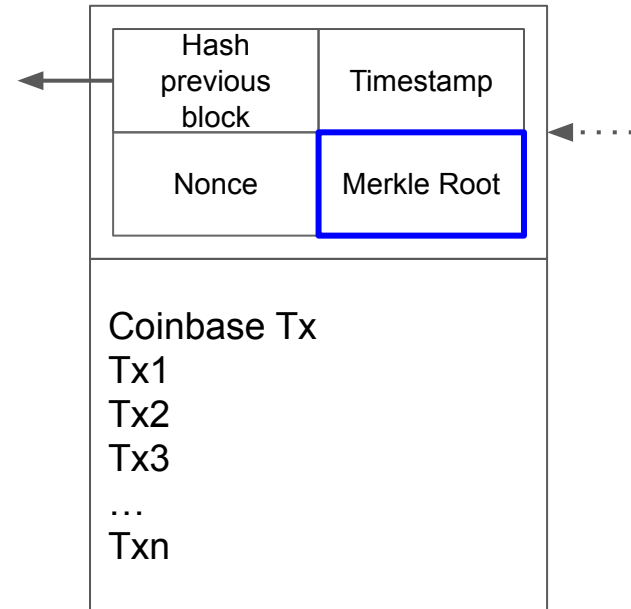


Into the block



Informazioni nell'header:

- Timestamp
- Nonce
- Merkle Root





Nota: Merkle tree



Alberi che permettono di verificare che un dato sia integro (non modificato)

Dato un insieme di dati, transazioni, costruire l'albero bottom-up calcolando l'hash dei figli

[MerkleTree]

Tx1

Tx2

Tx3

Tx4



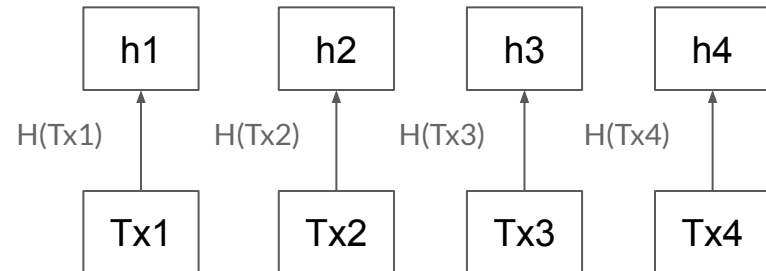
Nota: Merkle tree



Alberi che permettono di verificare che un dato sia integro (non modificato)

Dato un insieme di dati, transazioni, costruire l'albero bottom-up calcolando l'hash dei figli

[MerkleTree]





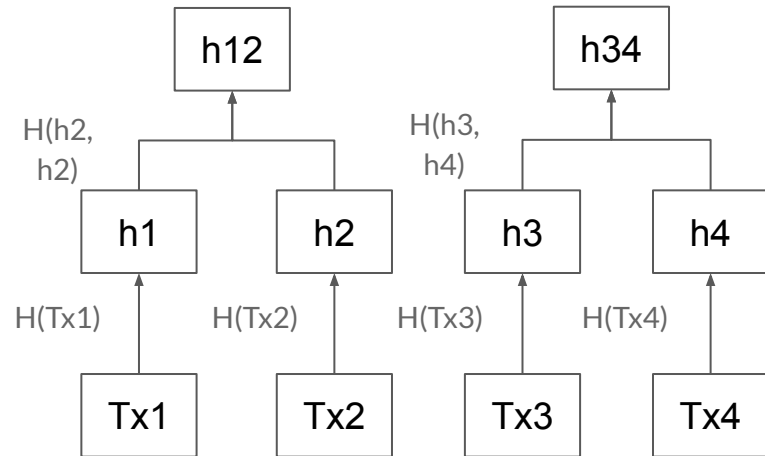
Nota: Merkle tree



Alberi che permettono di verificare che un dato sia integro (non modificato)

Dato un insieme di dati, transazioni, costruire l'albero bottom-up calcolando l'hash dei figli

[MerkleTree]





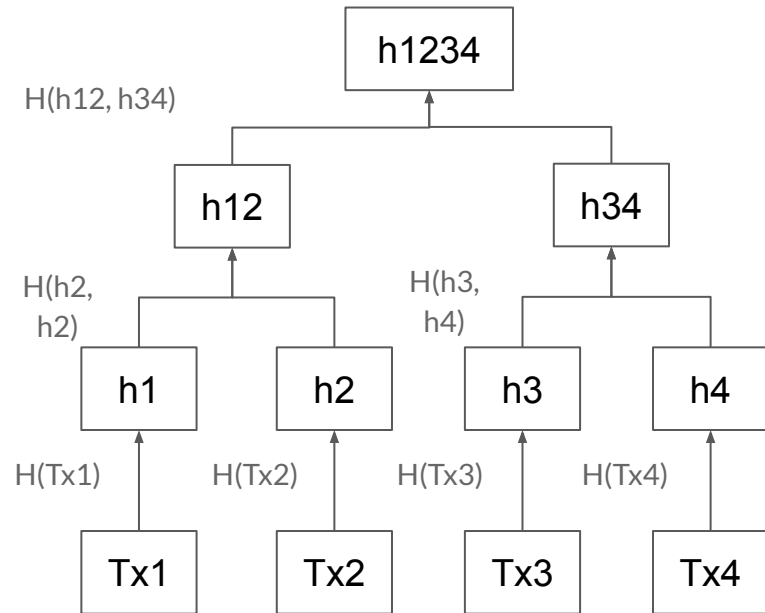
Nota: Merkle tree



Alberi che permettono di verificare che un dato sia integro (non modificato)

Dato un insieme di dati, transazioni, costruire l'albero bottom-up calcolando l'hash dei figli

[MerkleTree]





Nota: Merkle tree



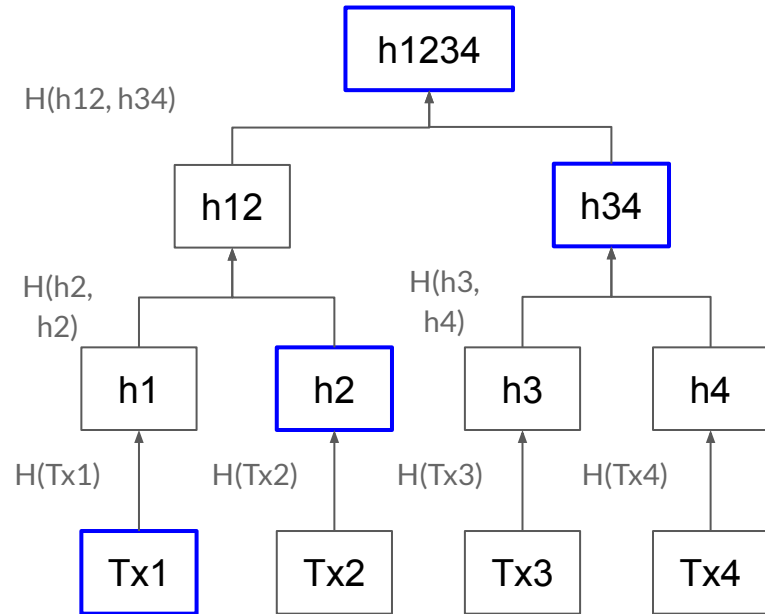
Voglio essere sicuro che Tx1 non sia stata modificata.
Conosco Tx1 e h1234. Chiedo h2 e h34.

Input: [Tx1, h2, h34, h1234]

Procedura:

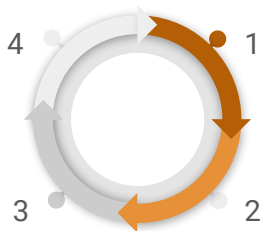
1. $H(H(H(Tx1), h2), h34) == h1234$

Sono sicuro che chi mi da h2 e h34 non ha modificato Tx1

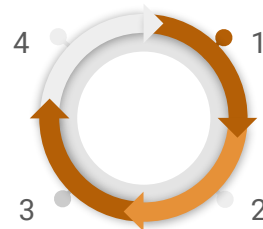




Creazione ed accettazione del blocco



Creazione (leader)
Esecuzione delle transazioni
Calcolo della radice del merkle tree



Accettazione (tutti gli altri)
Ri-Esecuzione delle transazioni
Ri-Calcolo della radice del merkle tree

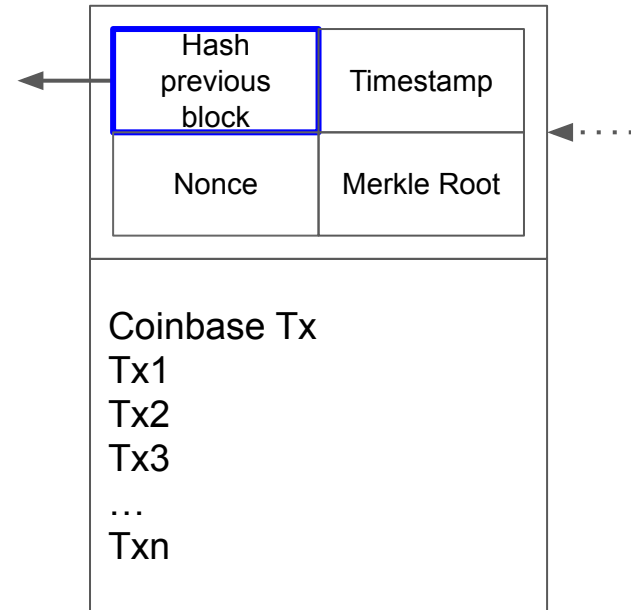


Into the block



Informazioni nell'header:

- Timestamp
- Nonce
- Merkle Root
- Hash Previous block



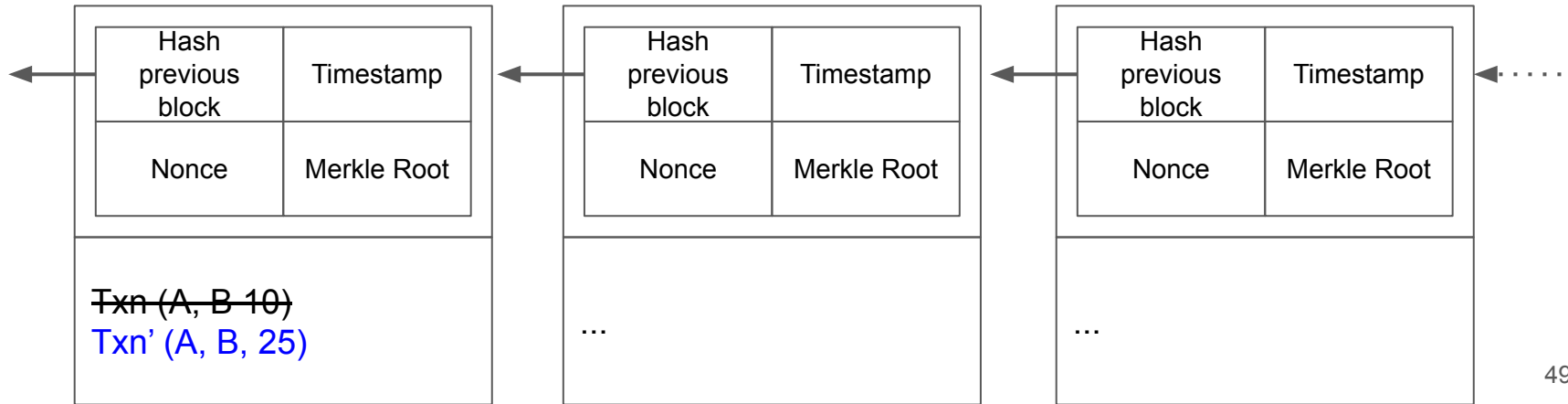


Tentativo di modifica



Un nodo cattivo A modifica una sua transazione nella sua copia locale della blockchain

- Cosa succede



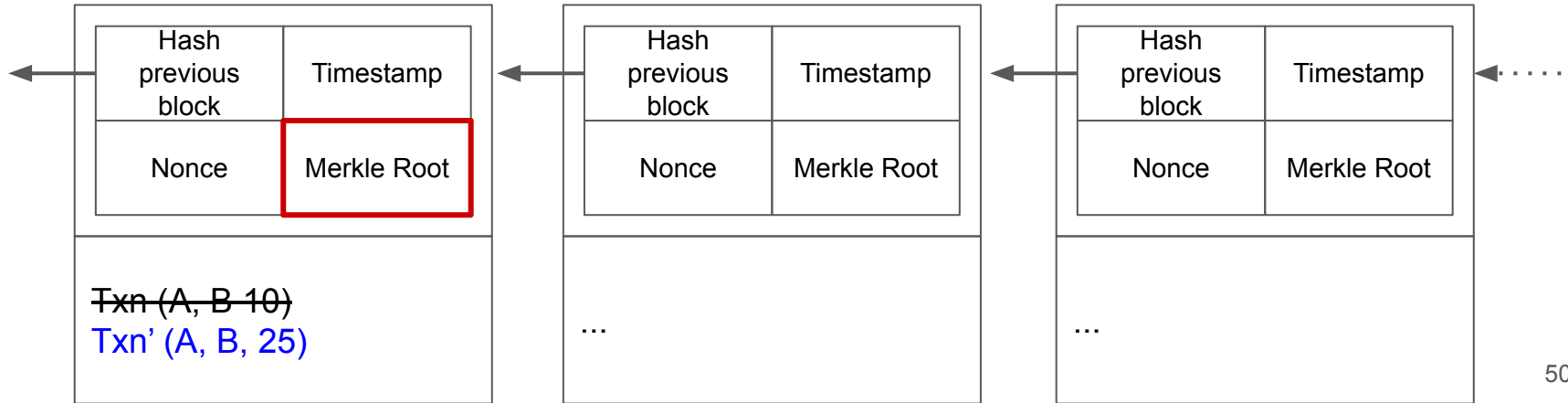


Tentativo di modifica



Un nodo cattivo A modifica una sua transazione nella sua copia locale della blockchain

- La radice del Merkle-tree è ora diversa



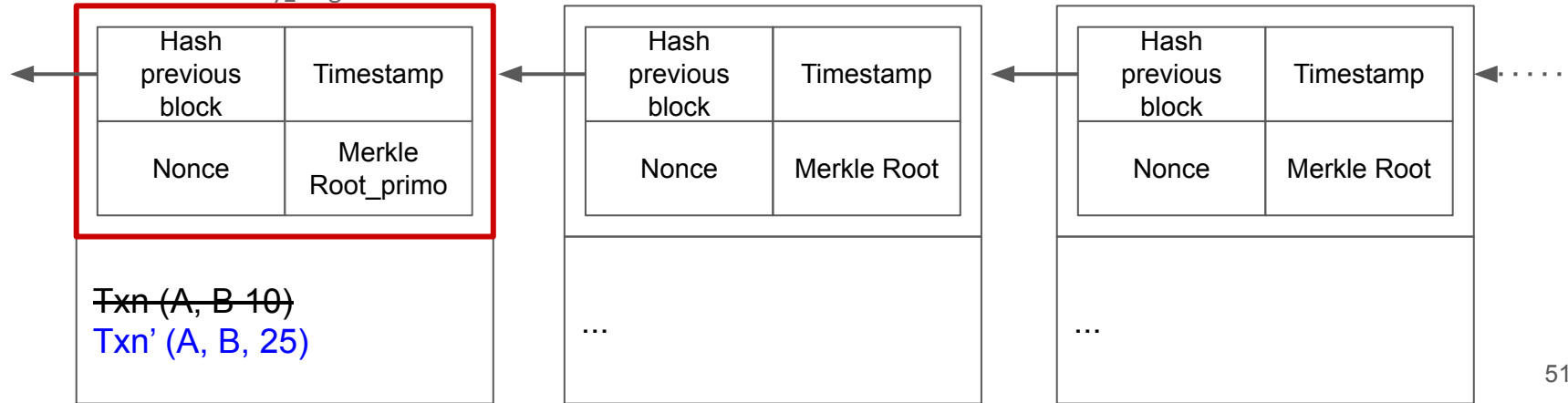


Tentativo di modifica



Il nodo cattivo A ricalcola Merkle Root_primo corretto

- Ma ora $\text{Sha256}(\text{block_header_primo}, \text{Nonce})$ è diverso da prima (forse $>$ $\text{value}_{\text{difficulty_target}}$)

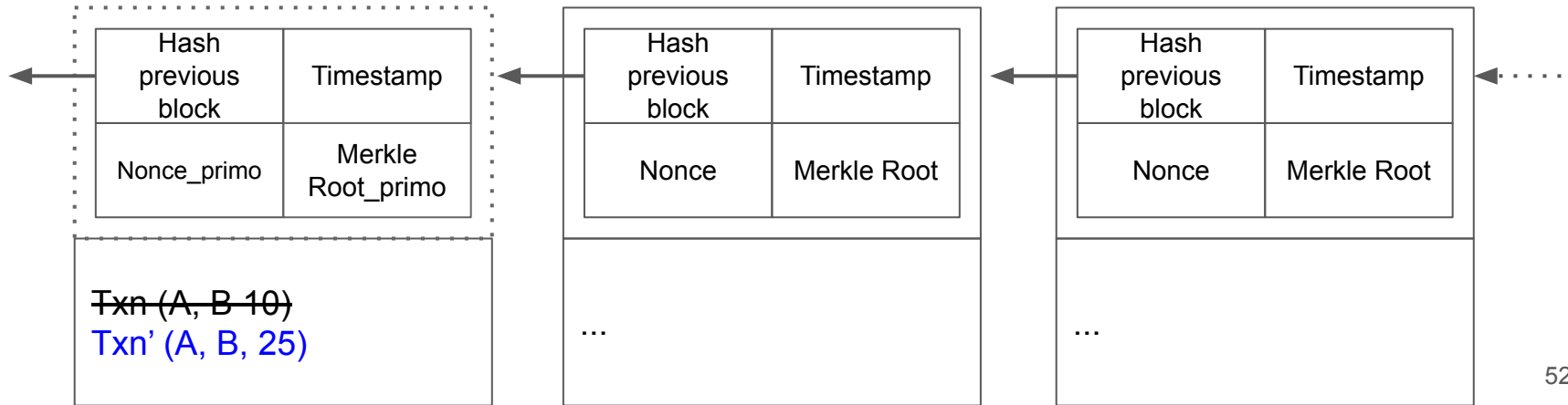




Tentativo di modifica



Il nodo cattivo A trova un nuovo Nonce_primo tale che $\text{Sha256}(\text{block_header_primo}, \text{Nonce_primo}) < \text{value}_{\text{difficulty_target}}$



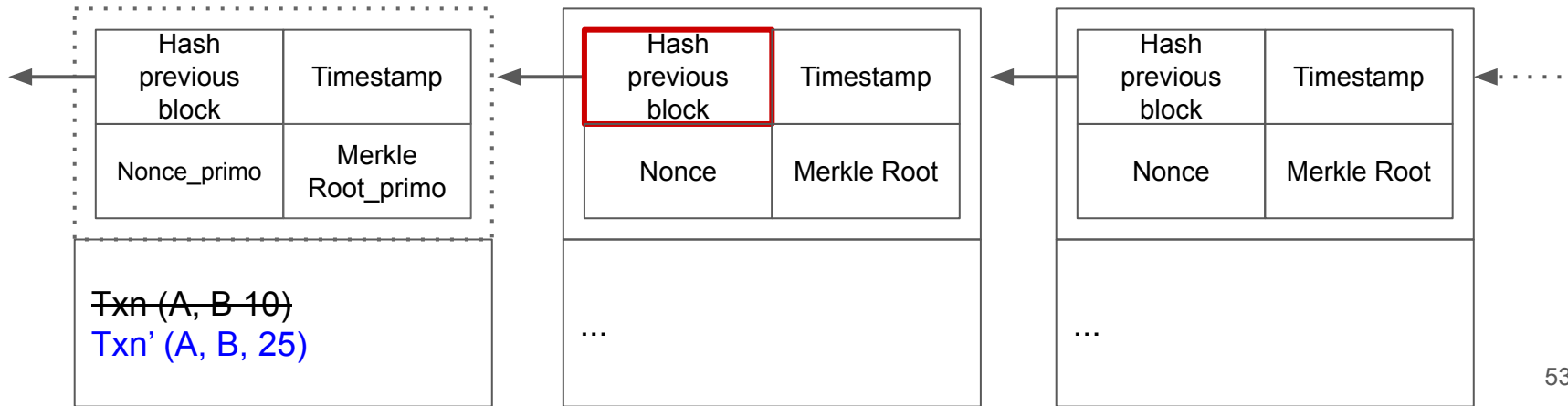


Tentativo di modifica



Il nodo cattivo A trova un nuovo Nonce_primo

- Però Hash previous block del blocco successivo è diverso ora è inconsistente



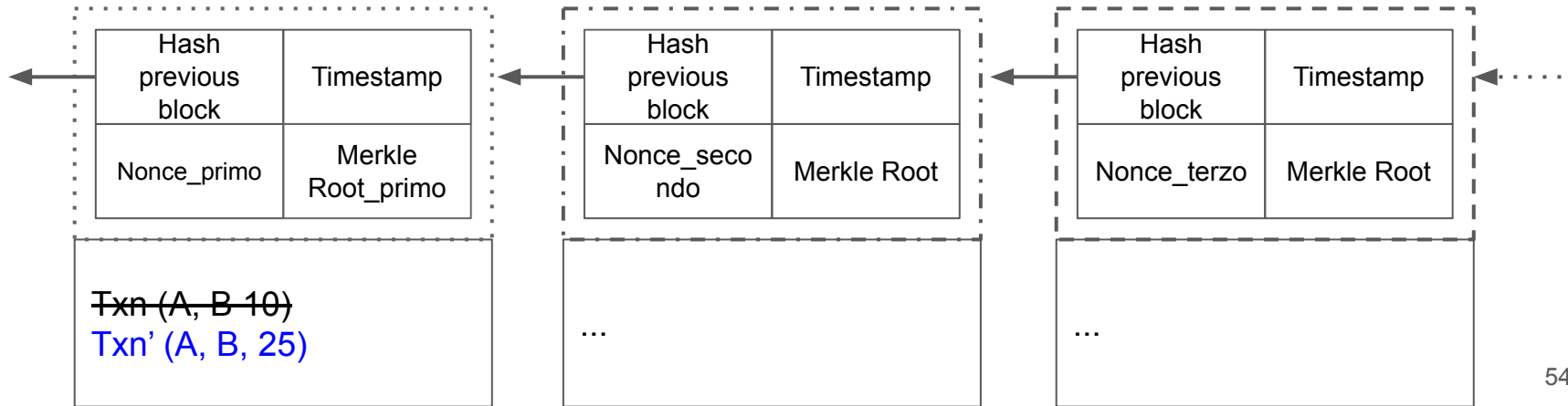


Tentativo di modifica



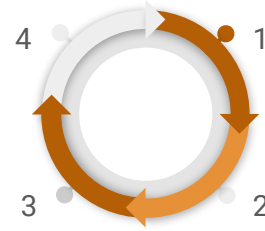
Modificare tutti i blocchi successivi della blockchain fino alla “cima”

- Ovvero ri-eseguire Proof of Work più e più volte prima degli altri





Tentativo di modifica



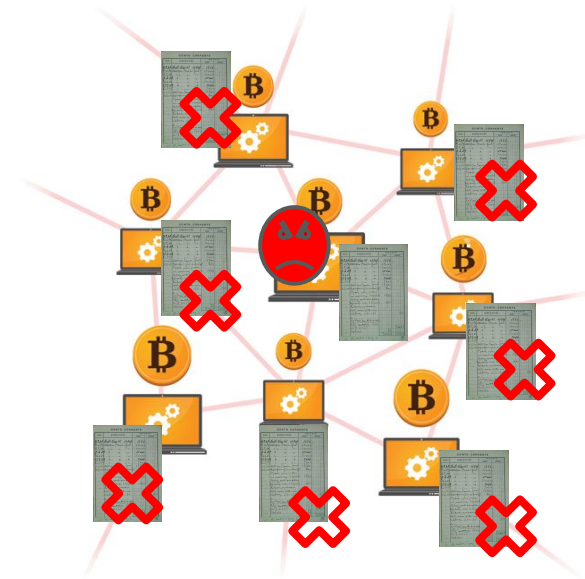
Non solo

Anche se un nodo riuscisse entro 15 minuti a fare N modifiche, gli altri nodi noteranno facilmente che

- $\text{Sha256}(\text{Blocco}_{n-1}) \neq \text{Blocco}_n.\text{Hash_previous_block}$

Dove Blocco_{n-1} è memorizzato da tutti gli altri nodi

Dove Blocco_n è il blocco ricevuto dal nodo cattivo





Attacco 51%

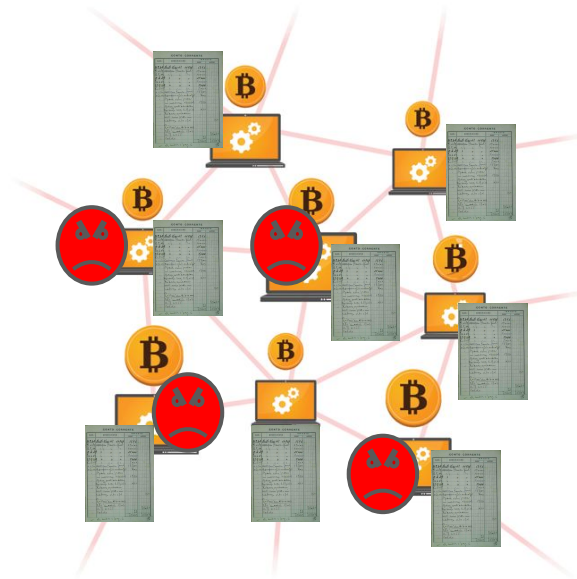


È possibile però scamparla?

In teoria sì. **Attacco 51%**, un nodo cattivo ha almeno il 51% della potenza di calcolo (hashrate)

- Il nodo cattivo vince sempre, quindi si può permettere di ignorare determinate transazioni
- Il nodo cattivo può fare “double spending”, ovvero spendere 2 volte i propri bitcoin

Una spiegazione dettagliata^[51%]





Transazioni: in dettaglio

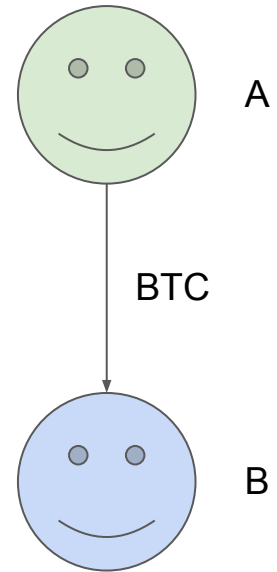


Una transazione è l'invio di BTC da A a B

- Tx(A, B, BTC)

In Bitcoin sono più complicate e fanno uso di firme digitali, che hanno le proprietà di

- Autenticazione
- Integrità
- Non-ripudio





Transazioni: in dettaglio



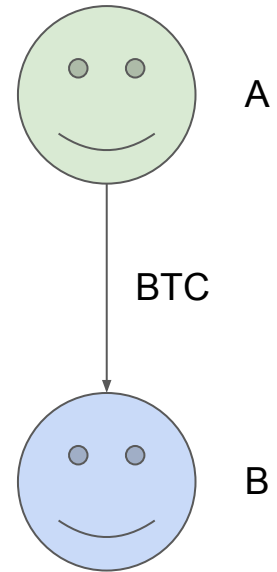
Siano A, B utenti e siano
SkA e SkB le loro chiavi private
PkA e PkB le loro chiavi pubbliche (derivate dalle chiavi private)
AddrA e AddrB i loro indirizzi (derivati dalle chiavi pubbliche)

A: $\text{Sign}(\text{Tx}(A, B, 50), \text{SkA}) :- \text{Msg}$

A: $\text{Send}(\text{Msg}, \text{AddrB})$

B: $\text{Verify}(\text{Msg}, \text{PkA}) :- \text{True}^{\text{[ScriptEsempio]}}$

Implementate in un linguaggio di scripting base: $\text{Script}^{\text{[Script]}}$





Transazioni: in dettaglio



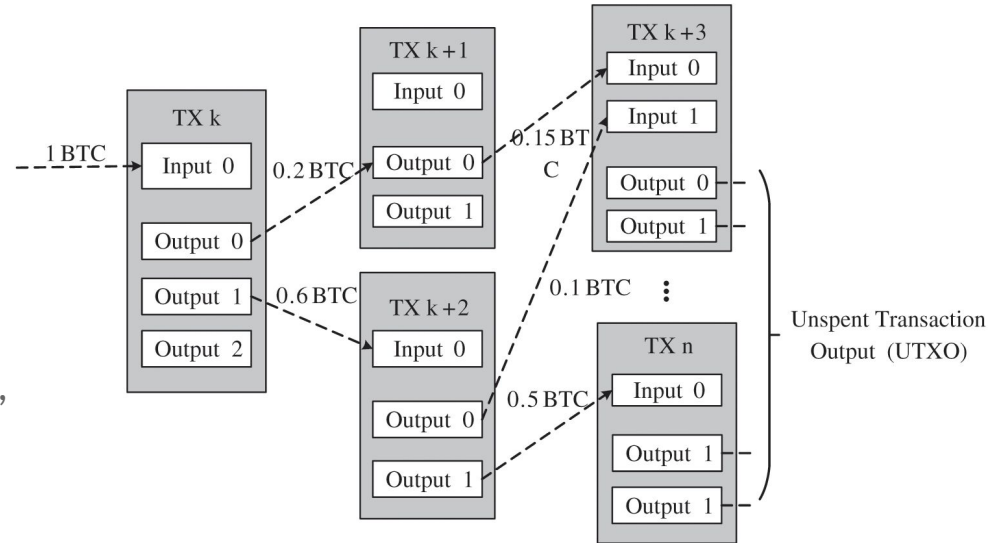
Input: BTC ricevuti

Output: BTC inviati

UTXO: Unspent Transaction Output, il “resto”

Output inviati ad una chiave pubblica, PkB, che è l'input di una chiave privata, SkB

Nessuno “possiede” BTC, ma ogni persona conosce una chiave privata per spenderli





PARTE 3

The background features a network diagram with light blue circular nodes containing white padlock icons. These nodes are interconnected by thin grey lines, forming a complex web. Some nodes are larger than others, and the overall aesthetic is clean and professional.

Altri progetti e campi applicativi



Ethereum



Nato nel 2014 circa, costruisce un sistema per l'esecuzione di applicazioni decentralizzate (DApp)

- Programmi chiamati Smart Contract
 - Programmabili in simil-Java (Solidity)
 - Eseguiti da tutti i nodi della rete Ethereum
- La criptovaluta ETH viene utilizzata per pagare le commissioni dell'esecuzione degli smart contract





DApp: Token



Token fungibili

- Token “interscambiabili”, tipo punti del benzinaio
 - Il valore è la quantità
- Spesso usati come coupon sconto o per svolgere operazioni in una DApp
 - Spesso distribuiti inizialmente tramite una ICO (Initial Coin Offering) come crowdfunding
 - Attenzione alle truffe! (SQUID)



Shiba INU



DApp: Token



Token non-fungibili (NFT)

- Token univoci, ognuno è diverso da un altro
- Tipicamente caratterizzati da un codice, e.g. hash
- Cryptokitties, la DApp Ethereum più popolare
 - Scambio di gattini
 - Ogni gattino è rappresentato da un NFT
 - L'uso intenso causò un rallentamento della rete Ethereum (2017)



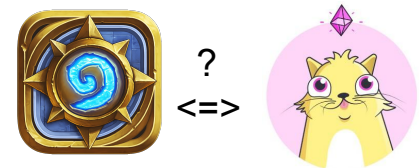
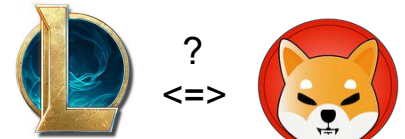


DApp: Token



Ma come sono diversi dal gold di League of Legends o dalle carte uniche di Heartstone?

- League of Legends / Heartstone
 - Applicazioni centralizzate dove la creazione, modifica, distruzione delle monete e carte sono a discrezione delle case produttrici (Riot Games / Blizzard)
 - Ogni “asset” del gioco quindi può essere replicato senza costi, questo lo priva di qualsiasi valore
 - Un PDF ha valore se basta fare copia/incolla per replicarlo?





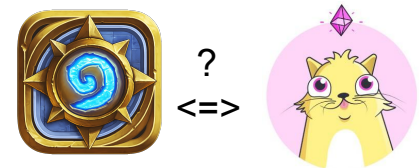
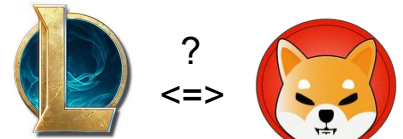
DApp: Token



Ma come sono diversi dalle monete d'oro di League of Legends o dalle carte uniche di Heartstone?

- DApp
 - Lo smart contract implementa le regole per la creazione, modifica, distruzione dei token
 - Queste regole non sono alterabili una volta che lo smart contract è presente (deployato) sulla blockchain
 - Queste regole sono visibili da tutti, quindi eventuali "exploit" sono visibili
 - Codice Solidity di Cryptokitties:

<https://etherscan.io/address/0x06012c8cf97bead5deae237070f9587f8e7a266d#code>



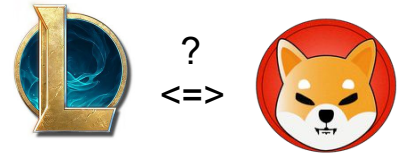


DApp: Proprietà



Non alterabilità e visibilità delle regole degli smart contract sono le proprietà per cui le DApp si distinguono dalle applicazioni “tradizionali client-server”

- Ovviamente valgono fintanto che la blockchain che ospita lo smart contract “vive”
- Essendo distribuita, la blockchain è resistente dal “single point of failure”
- La criptovaluta incentiva la partecipazione

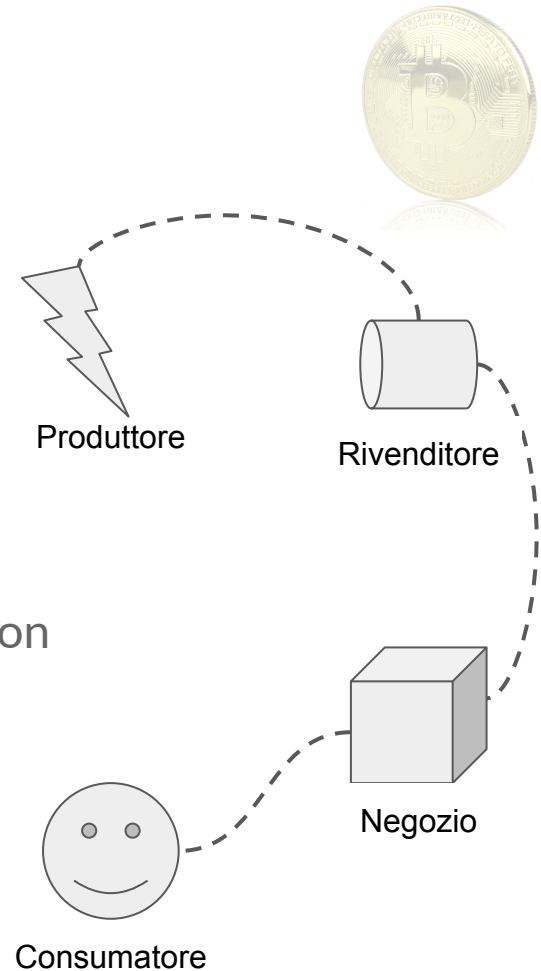




DApp: Filiera

Altro esempio popolare: la Filiera di un prodotto

- Vari attori: Produttore, Rivenditore, Negozio, Consumatore
- Chi gestisce i dati completi della filiera? Ogni attore non “si fida” degli altri

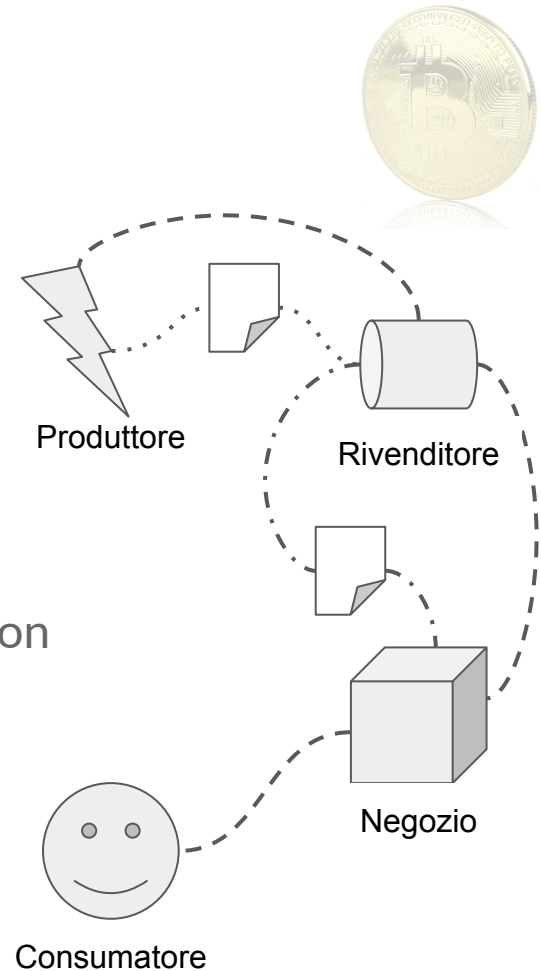




DApp: Filiera

Altro esempio popolare: la Filiera di un prodotto

- Vari attori: Produttore, Rivenditore, Negozio, Consumatore
- Chi gestisce i dati completi della filiera? Ogni attore non “si fida” degli altri
 - Fanno accordi (contratti)
 - Un sistema “opaco”

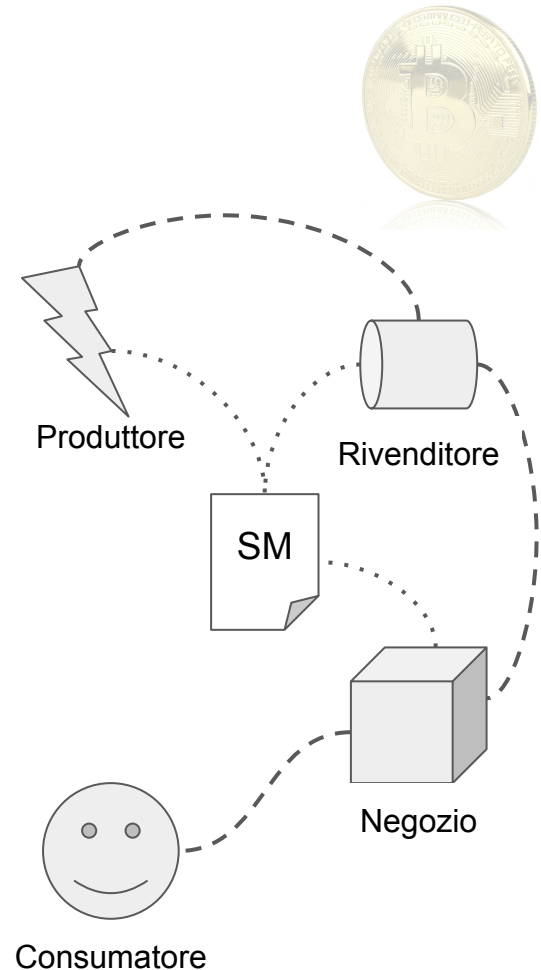




DApp: Filiera

Altro esempio popolare: la Filiera di un prodotto

- Vari attori: Produttore, Rivenditore, Negozio, Consumatore
- Delegare le regolamentazioni ad uno smart contract
 - Visibile a tutti
 - Non alterabile da nessuno
 - Non ripudiabile (transazioni firmate)

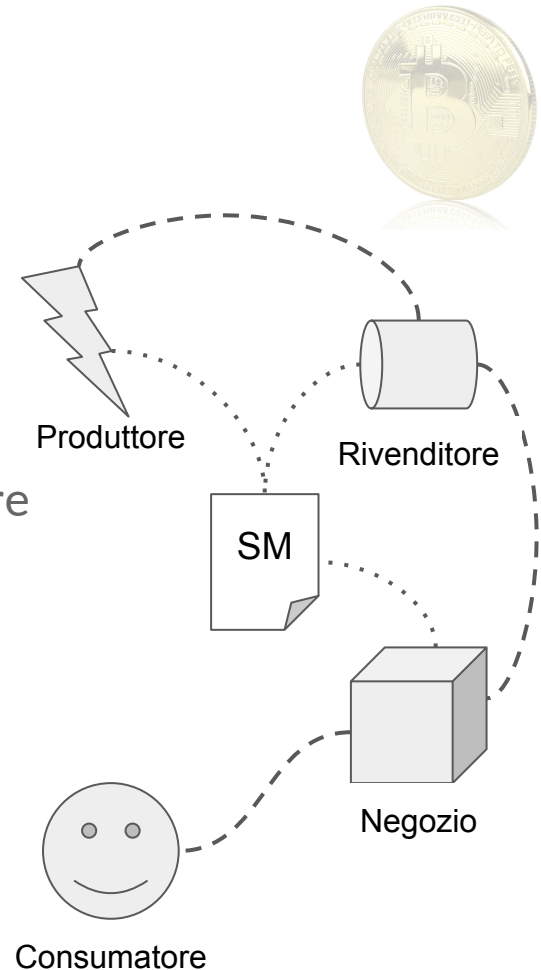




DApp: Svantaggi

Non è tutto oro quello che luccica

- Una transazione su blockchain (Ethereum) può essere molto costosa
 - “Highest average transaction fee of **\$68.72** on Tuesday, May 11, 2021”^[EthTx Fees]
 - Può essere molto più costosa di così
- Lentezza
- Completa visibilità contrasta con la privacy
 - E.g. GDPR





Blockchain private

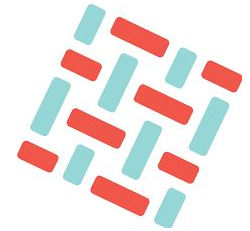


Bitcoin ed Ethereum sono esempi di blockchain “pubbliche”

- Tutti possono partecipare
- Ma hanno problemi (vedi slide precedente)

Questo ha fatto nascere framework per il setup di blockchain “private”

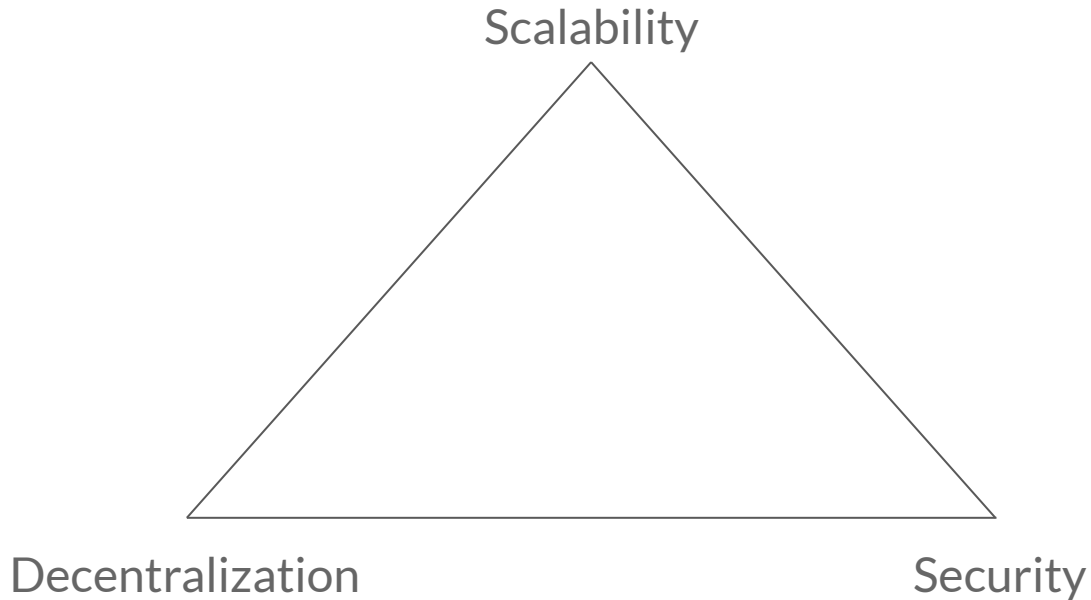
- Le proprietà di non alterabilità e visibilità limitate ad un insieme ristretto di partecipanti
- Sistema più “centralizzato” e vicino al sistema client-server



Hyperledger
Fabric



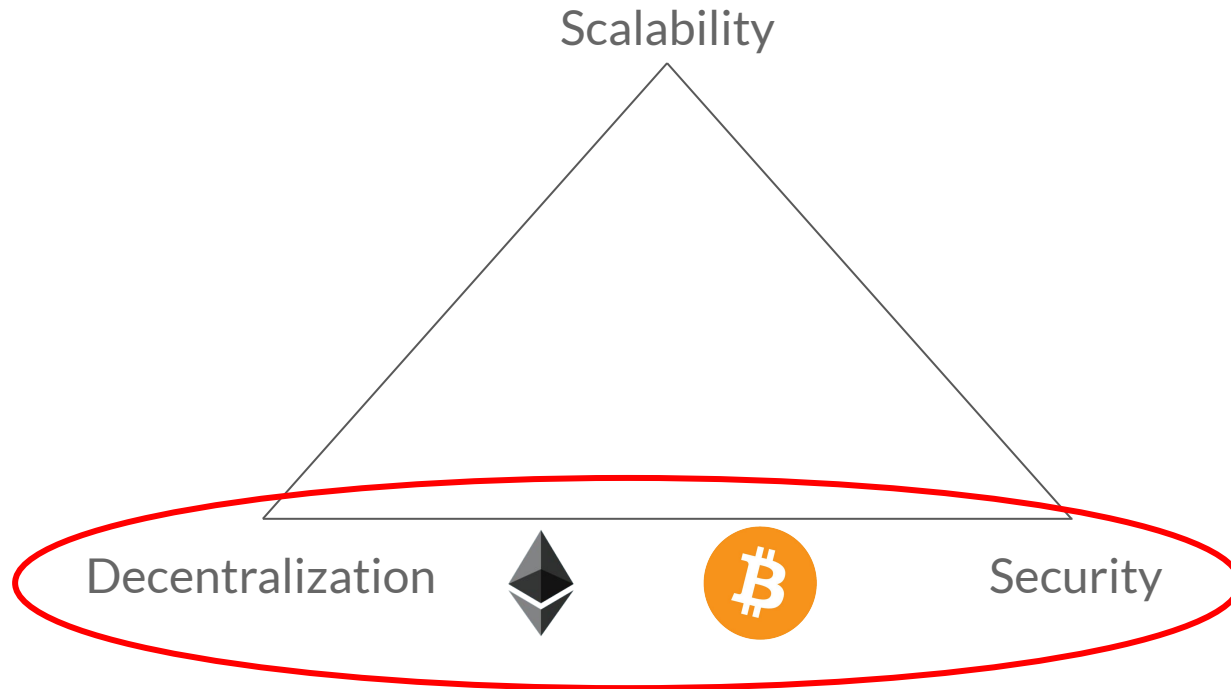
Blockchain trilemma



Trilemma
Max
2 proprietà
su queste 3



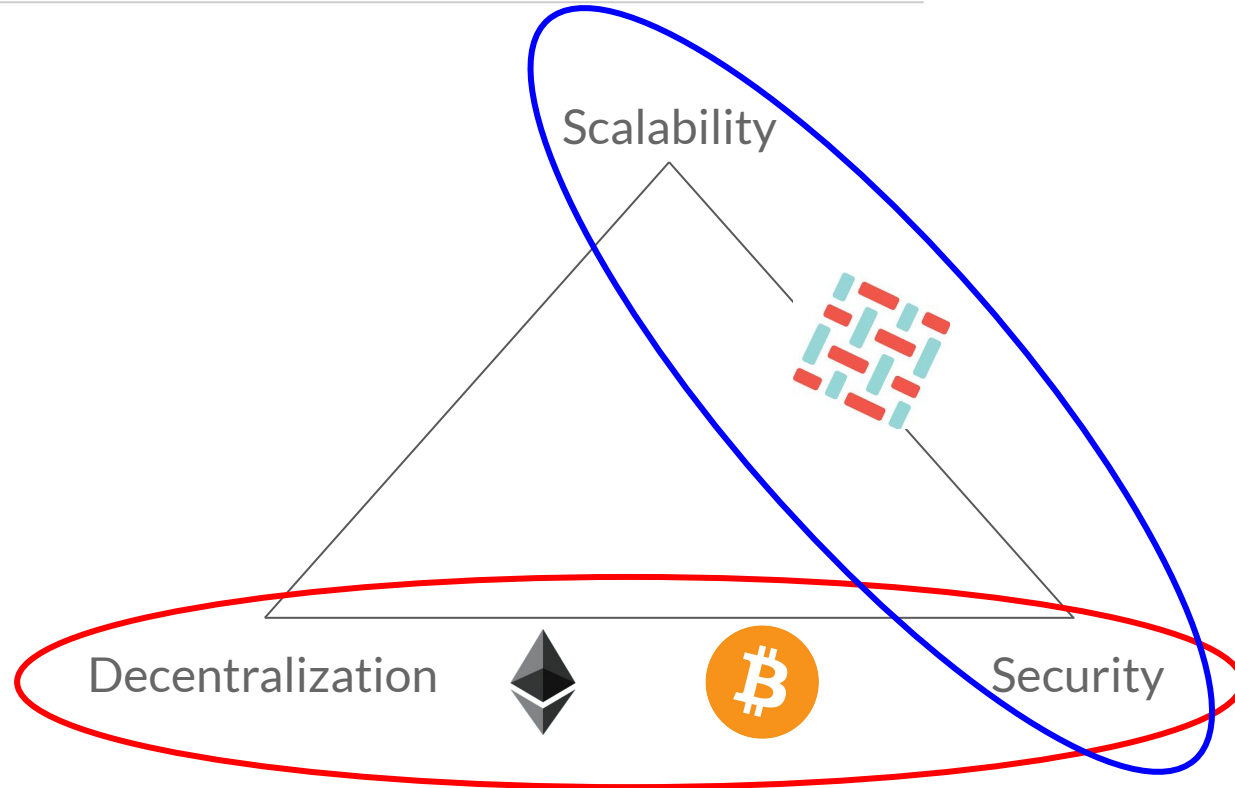
Blockchain trilemma



Trilemma
Max
2 proprietà
su queste 3



Blockchain trilemma



Trilemma
Max
2 proprietà
su queste 3

**Domande
frequenti**





Ma come ottengo Bitcoin?



Il modo più naturale è scaricare il software e metterlo in competizione per diventare leader

MA ...

- Il libro contabile di Bitcoin è grande circa 300 GB
- I partecipanti a Bitcoin al giorno d'oggi non sono portatili, ma interi palazzi di computer
- Servirebbe il computer in esecuzione 24 ore su 24 sempre
 - Poi chi la sente l'Enel?





Ma come ottengo Bitcoin?



Esistono dei broker di finanza che accettano Euro, Dollari etc in cambio di Bitcoin

- Vari siti web

Farseli dare da chi li possiede già

- Magari come pagamento di un servizio





Ma come utilizzo Bitcoin?



È possibile partecipare in maniera “light” tramite programmi “portafoglio” leggeri

Questi portafogli creano una speciale coppia di chiavi per poter ricevere ed inviare Bitcoin

- Una chiave **privata**, quindi da non comunicare a nessuno, permette di firmare una transazione ed inviare Bitcoin
- Una chiave **pubblica**, quindi nota a tutti, che permette di ricevere Bitcoin
 - Concetto della cassetta della posta





Ma come utilizzo Bitcoin?



Attenzione 1

Non esiste una banca! Ogni Bitcoin inviato per sbaglio non è rimborsabile

Attenzione 2

La perdita della chiave privata significa la perdita di tutti i Bitcoin associati, e non è recuperabile facilmente



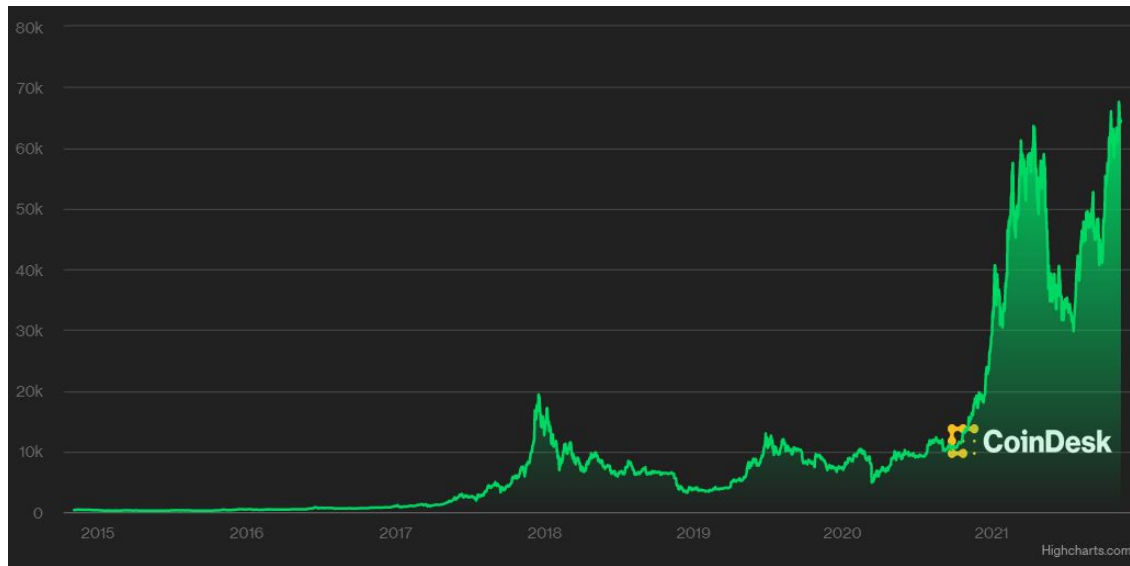


Ma quanto valgono i Bitcoin?

Oggi 1 bitcoin vale circa
55.000€

Circolano circa 18M BTC

[Coindesk, 14 Novembre
2021]

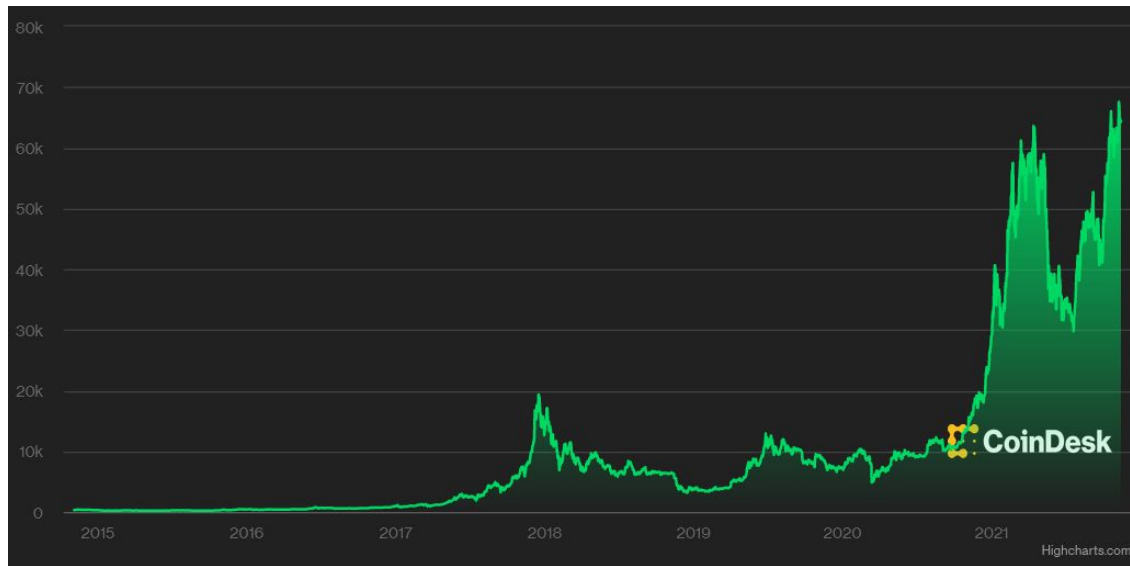




Chi decide il valore di Bitcoin?

Il mercato, pura
domanda / offerta

I bitcoin non sono legati
a nessun asset (tipo l'oro)





Quanti bitcoin ci saranno?



Come accennato, ci sono circa 18 Milioni di bitcoin a giro

- Ogni 15 minuti vengono “creati” nuovi, che sono quelli della ricompensa al leader

Massimale: 21 Milioni di bitcoin

- La ricompensa viene dimezzata ogni 4 anni
- È iniziata con 50 bitcoin, a Giugno 2020 c'è stato il terzo dimezzamento, ora è di 6.25 bitcoin
- 21 Milioni verranno raggiunti circa nel 2140





Quale è il futuro di Bitcoin?



Difficile prevederlo...





Quale è l'impatto di Bitcoin?



L'insieme di tecniche per l'aggiornamento del libro contabile hanno avuto un incredibile riscontro

- Sia nel mondo della ricerca universitaria
 - Migliorare Bitcoin, utilizzare i concetti su altri problemi
- Sia nel mondo dell'industria
 - Creare una rete di computer aziendali per migliorare i processi produttivi
 - Esempio: filiere alimentari





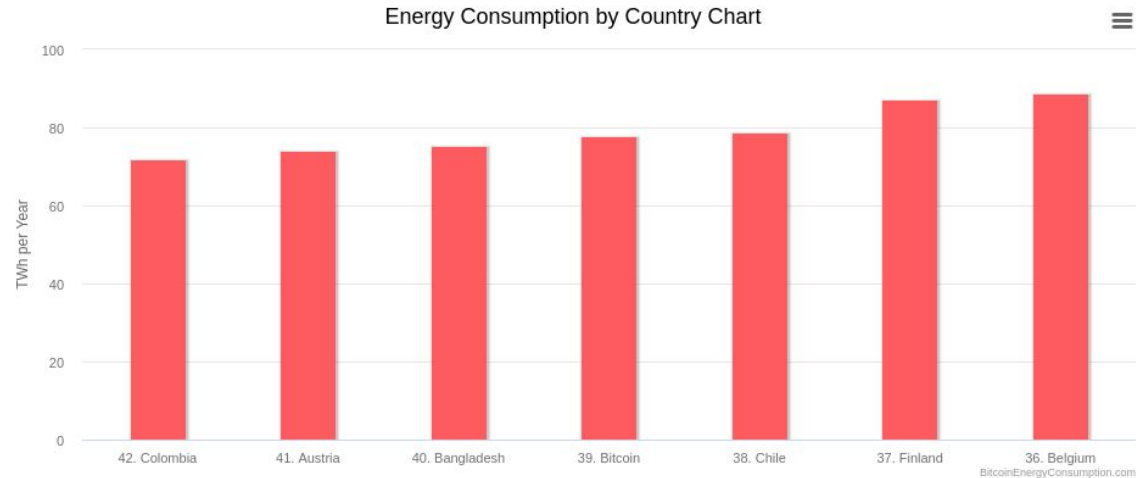
Quanto consuma Bitcoin?



Ad Agosto 2020, sottostima

Rete mondiale di Bitcoin
paragonabile a
Austria e Finlandia
[Digiconomist, 11 Novembre]

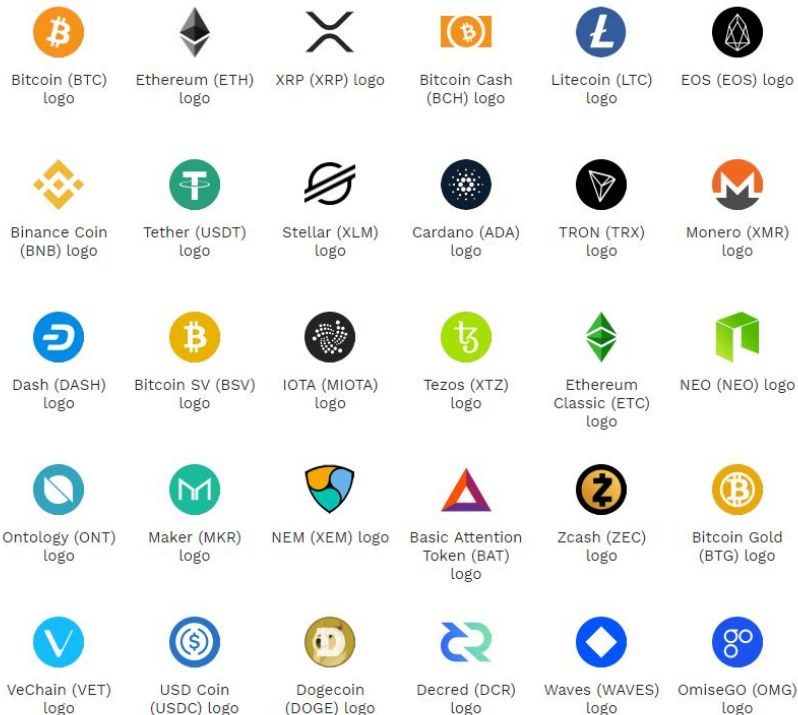
La ricerca sta studiando
alternative meno esose





Quante criptovalute esistono?

Troppe...



<https://cryptologos.cc/>

DOGE to the moon



Riferimenti



[Investopedia] <https://www.investopedia.com/terms/d/digital-currency.asp>

[Bitcoin] <https://bitcoin.org/bitcoin.pdf>

[BitcoinCore] <https://bitcoin.org/en/download>

[Difficulty] <https://en.bitcoin.it/wiki/Difficulty>

[MerkleTree] <https://medium.com/blockwhat/merkle-trees-ensuring-integrity-on-blockchains-508d6647d58e>

[51%] <https://www.youtube.com/watch?v=UxyGt58EPa4>

[Script] <https://en.bitcoin.it/wiki/Script>

[ScriptEsempio] [https://en.bitcoin.it/wiki/Script#Standard Transaction to Bitcoin address .28pay-to-pubkey-hash.29](https://en.bitcoin.it/wiki/Script#Standard_Transaction_to_Bitcoin_address_.28pay-to-pubkey-hash.29)

[EthTxFees] <https://etherscan.io/chart/avg-txfee-usd>

Grazie!

Per curiosità future
andrea.lisi@phd.unipi.it

