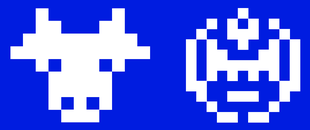


Sibilla Merlo

Fondamenti tecnici di Bitcoin

BitPolito — Politecnico di Torino

Bitcoin è uno strumento di libertà ed emancipazione

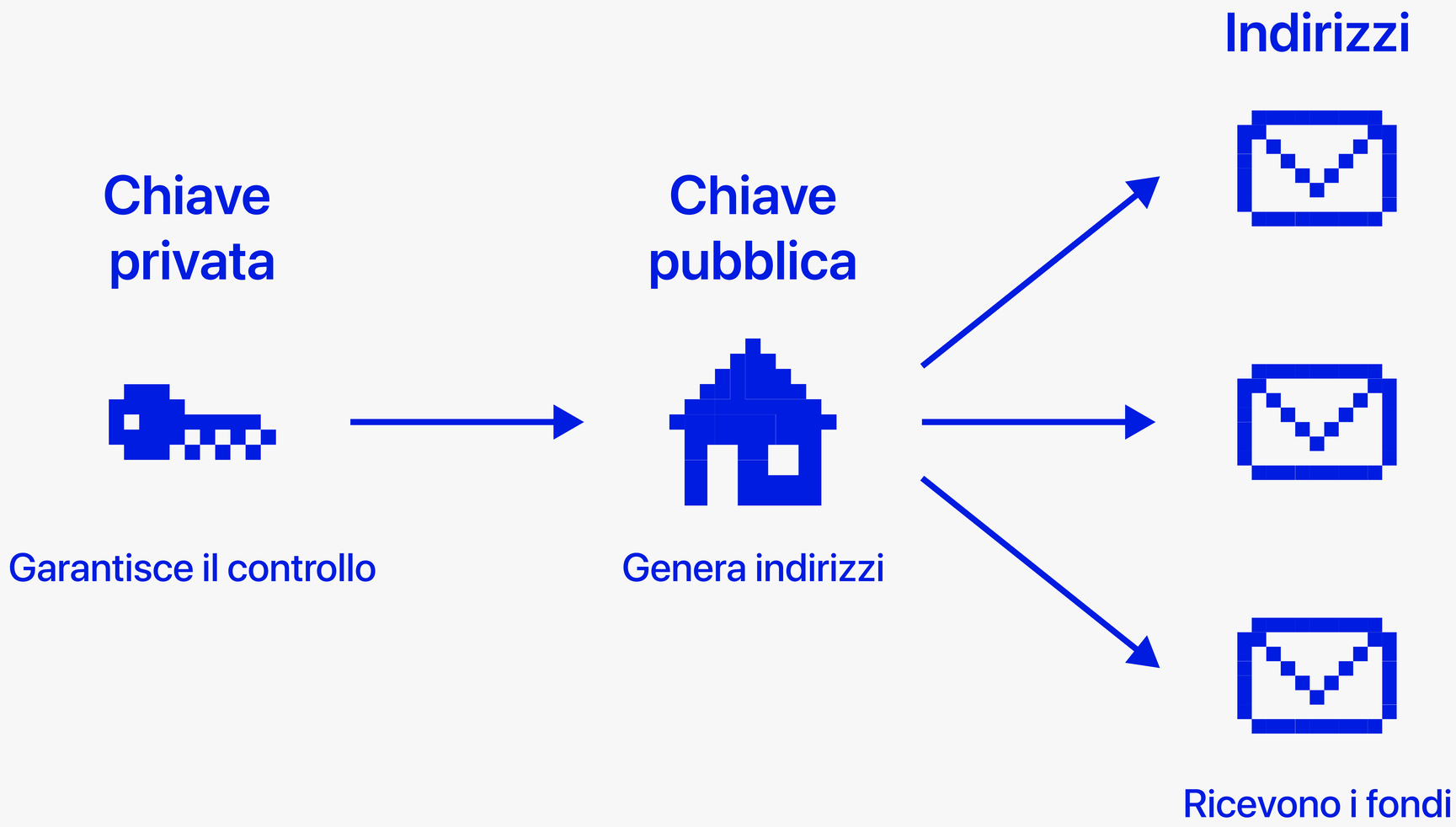
Tasselli fondamentali

Crittografia

Blockchain

Consenso

Mining


Indirizzi
Chiave privata
Chiave pubblica
Garantisce il controllo
Genera indirizzi
Ricevono i fondi

SHA 256

Dati

Funzione di Hash

Hash/Fingerprint

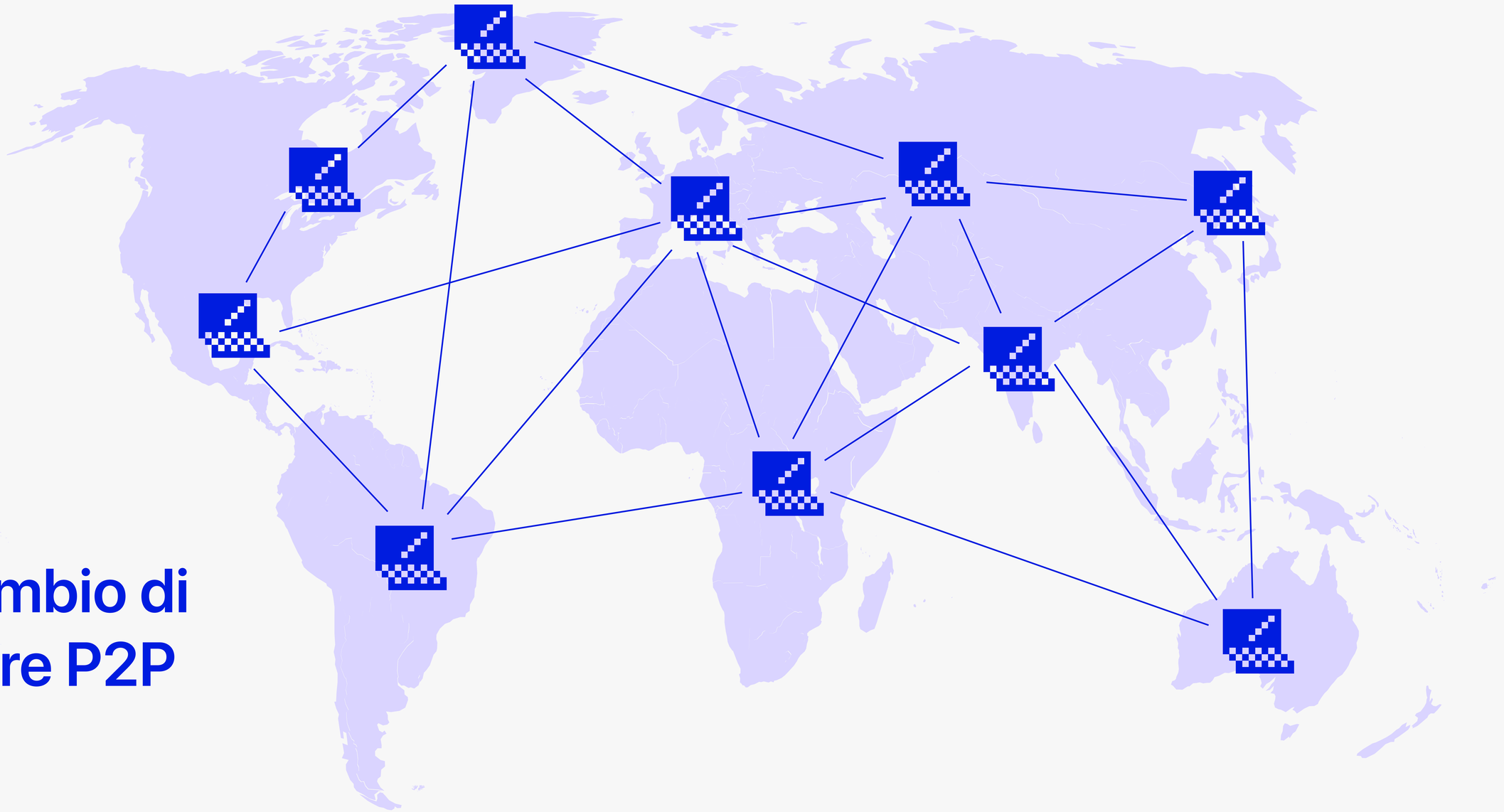
Bitpolito

b0ebdc32452d1faa6a20ccf9f0f22d49af
74f2e0340f4f6981542a56 4b7685c1

BitPolito

62da87333e7742a47efc8ee8f03e0f1b8
0d92cea56cb7021ca537a ba80804b16

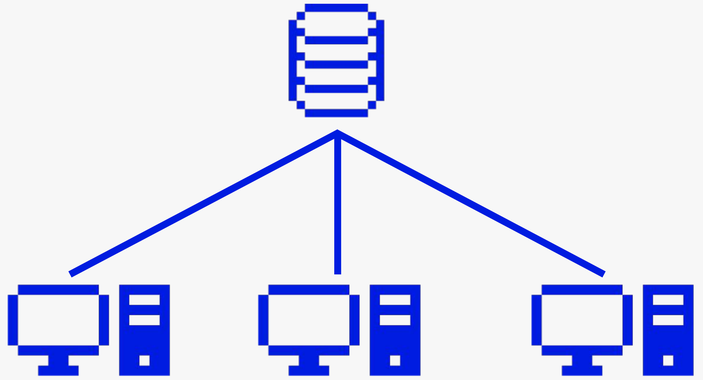
Scambio di valore P2P



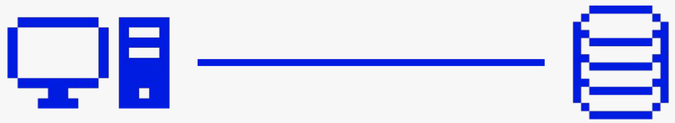
Architetture informatiche

Standalone

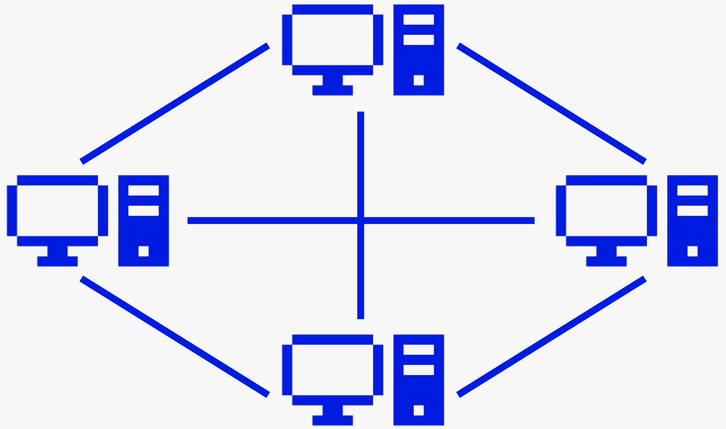
Mainframe



Client-server



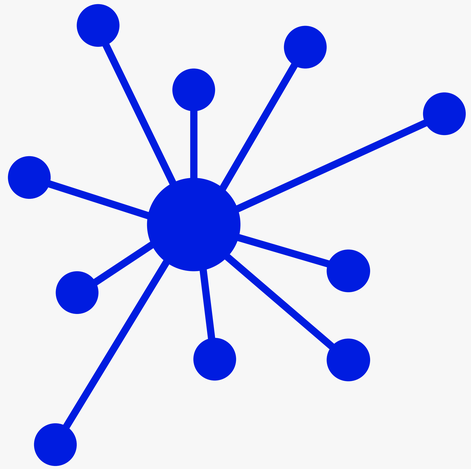
P2P




VISA
Alice
Banca Alice
PayPal
Banca Bob
Bob

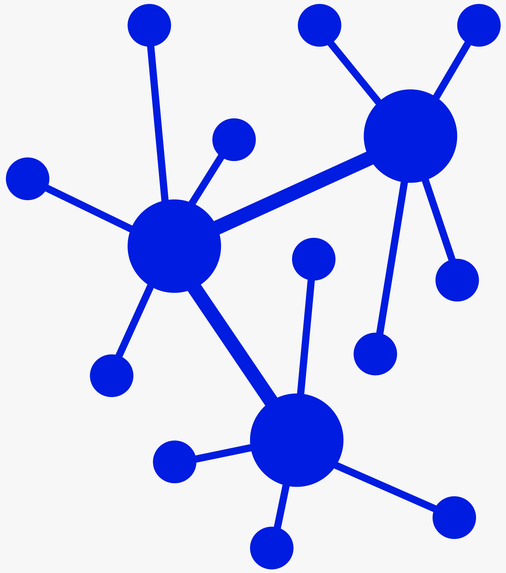

Alice
P2P Network
Bob

Tipologie di reti



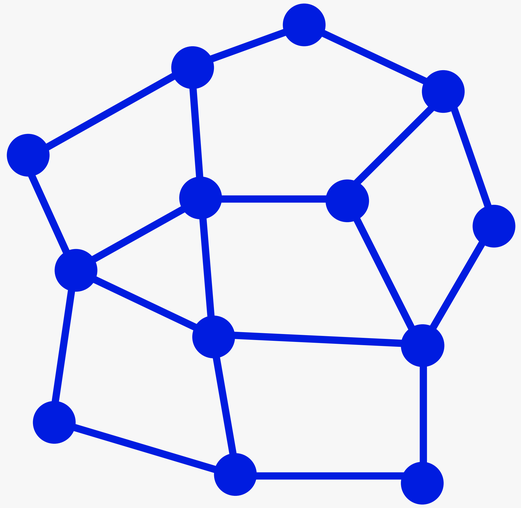
Sistema centralizzato

Monete Fiat



Sistema decentralizzato

Altcoins



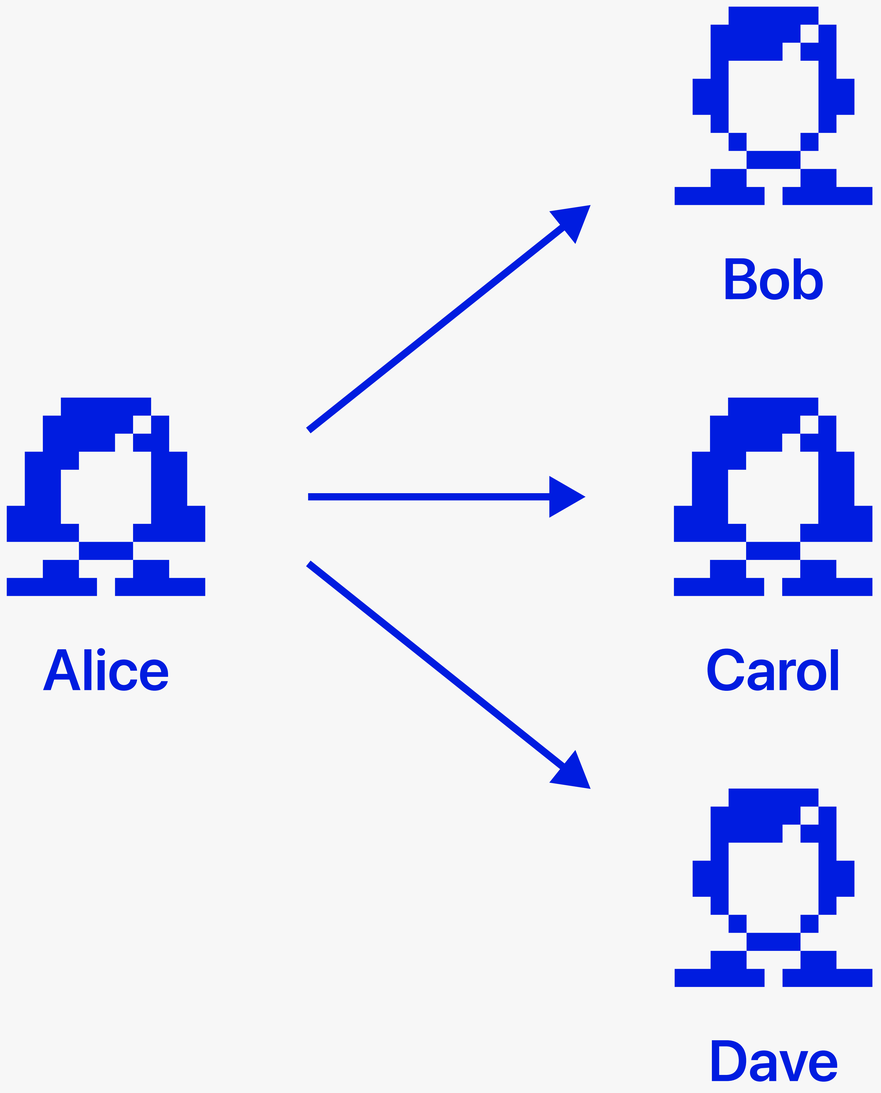
Sistema distribuito

Bitcoin

Sistemi distribuiti

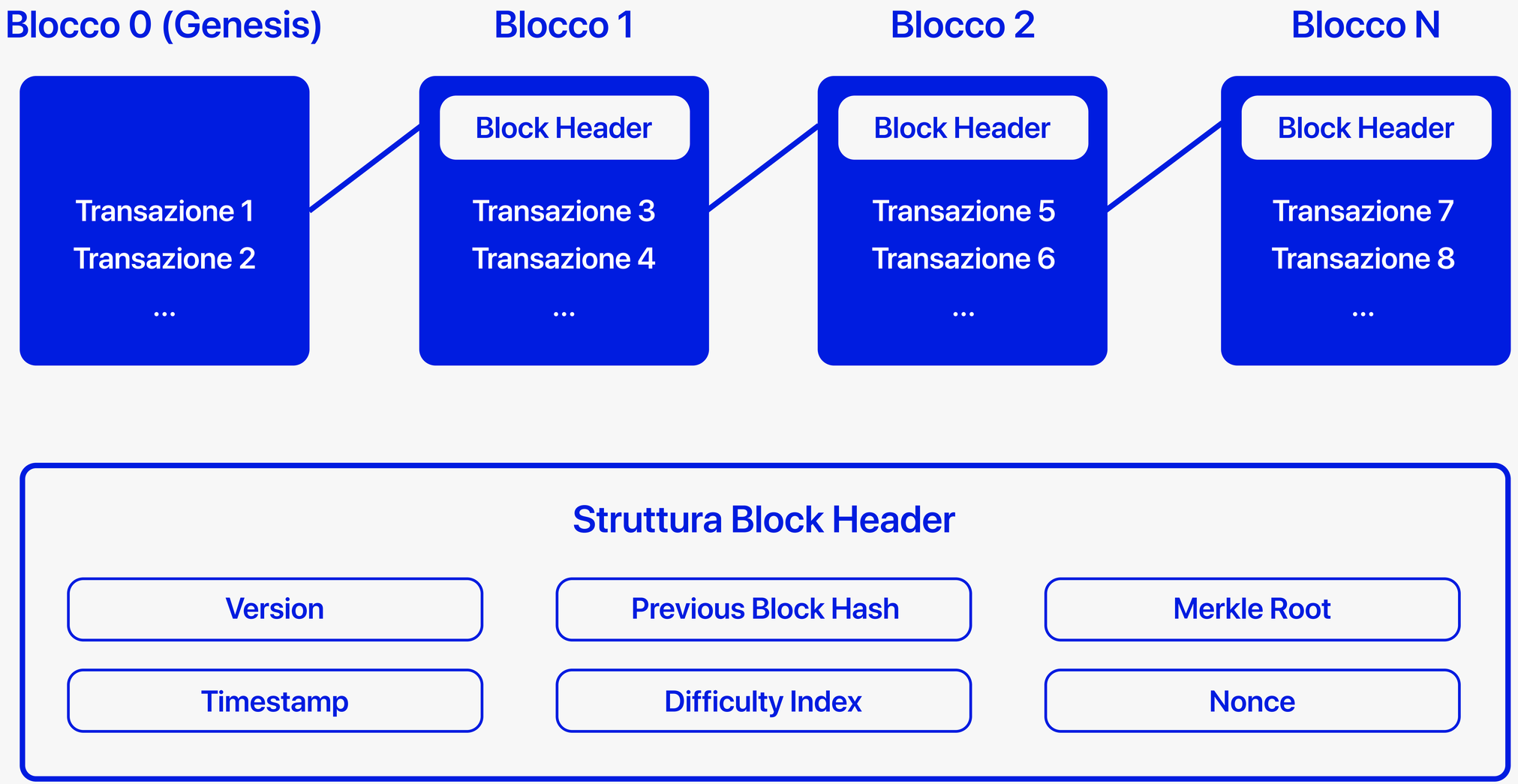
- Assenza coordinatore centrale
- Regole comuni
- Simmetria client-server

Problema della doppia spesa

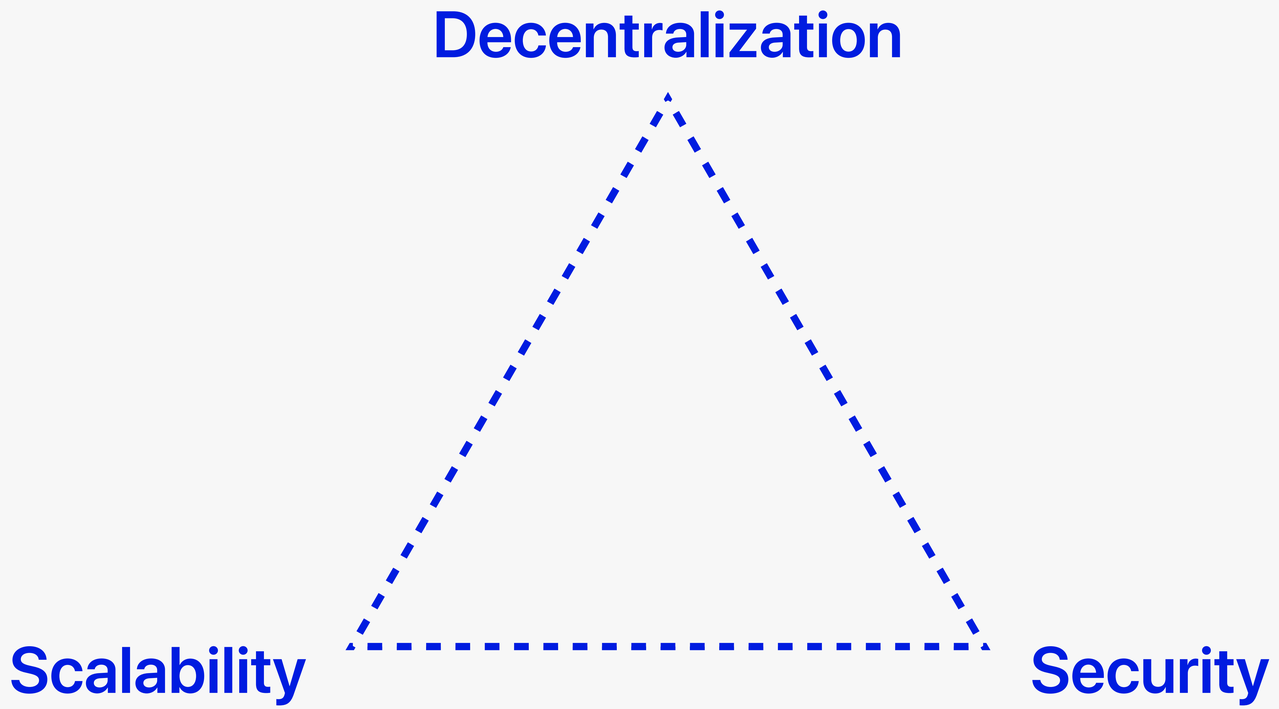


Blockchain

- Evita la doppia spesa
- Registro distribuito tra nodi
- Transazioni pubbliche e immutabili


Blocco 0 (Genesis)
Blocco 1
Blocco 2
Blocco N
Transazione 1
Transazione 2
...
Block Header
Transazione 3
Transazione 4
...
Block Header
Transazione 5
Transazione 6
...
Block Header
Transazione 7
Transazione 8
...
Struttura Block Header
Version
Previous Block Hash
Merkle Root
Timestamp
Difficulty Index
Nonce

Blockchain Trilemma



Meccanismo di consenso

Proof-of-work

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

Blocco: **10 minuti**

Halving: **4 anni**

Mining

19,8 M
BTC già minati

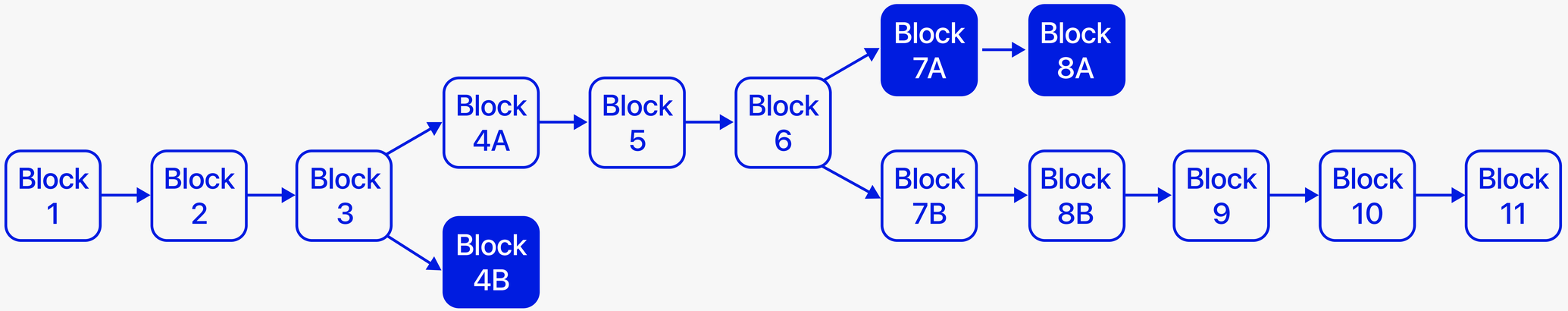
94,3%
BTC già minati

1,2 M
BTC da minare

450
BTC/giorno minati

- Emettere nuovi bitcoin
- Confermare nuove transazioni
- Proteggere la rete

Fork involontari

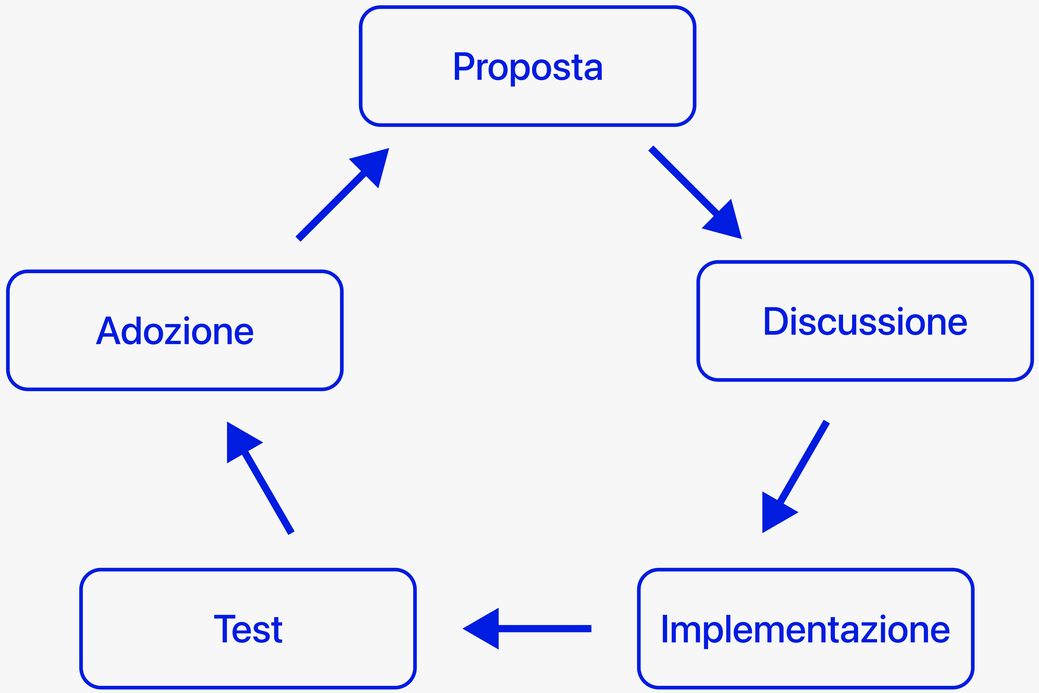


Delay nella propagazione delle informazioni all’interno della rete.

Due versioni della chain entrambe valide, poi si converge sulla versione “più lunga”

Bitcoin Development

BIP (Bitcoin Improvment Proposal)



Sviluppo Open Source

- Collaborazione tra sviluppatori
- Condivisione del codice sorgente
- Libertà nell’uso del codice

Soft Fork

- Variazione al sistema di consenso retrocompatibile
- Adozione per consenso del 95% dei miner

Hard Fork

- Variazione al sistema di consenso non retrocompatibile
- Biforcazione della chain con divisione della community

Est. 31/10/2008

BITCOIN

A PEER–TO–PEER ELECTRONIC CASH SYSTEM

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.*

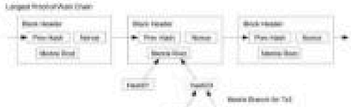
We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof 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.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for

The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest

Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late. The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction. The recipient waits until the transaction has been

@BitPolito