Social Farming 3

Inclusione sociale nella filiera agrumicola siciliana

Nozioni Base 1/4

15 aprile 2020

Marco Vitale
Marco Crotta

Blockchain Experts

Modulo 1:

Storia della blockchain
Decentralizatione e doppia spesa
Bitcoin: il primo protocollo
Blocchi, hash, transazioni
Consensus e mining
Immutabilità dei dati

Bitcoin

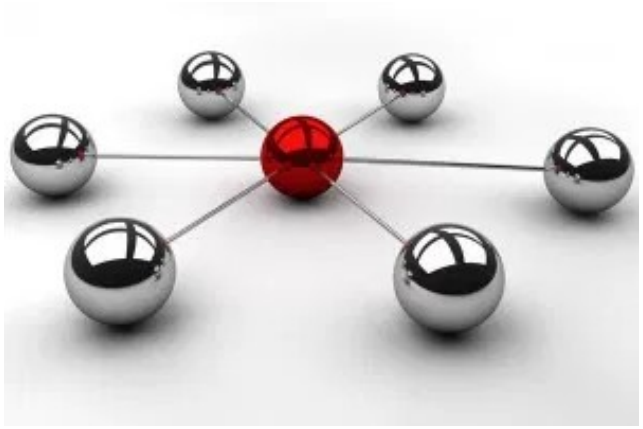
Bitcoin: A Peer-to-Peer Electronic Cash System

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

Decentralizzazione

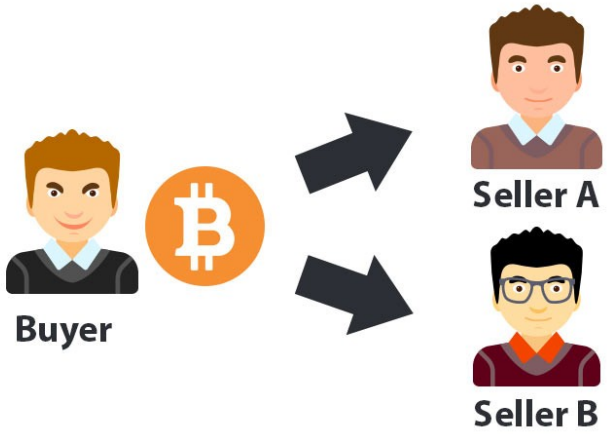
- Singolo punto critico
- Censura / Controllo
- Fiducia (accezione negativa)



Storia della blockchain

Doppia spesa

- Copia-incolla del valore
- Inflazione
- Frodi, inaffidabilità



Il primo annuncio

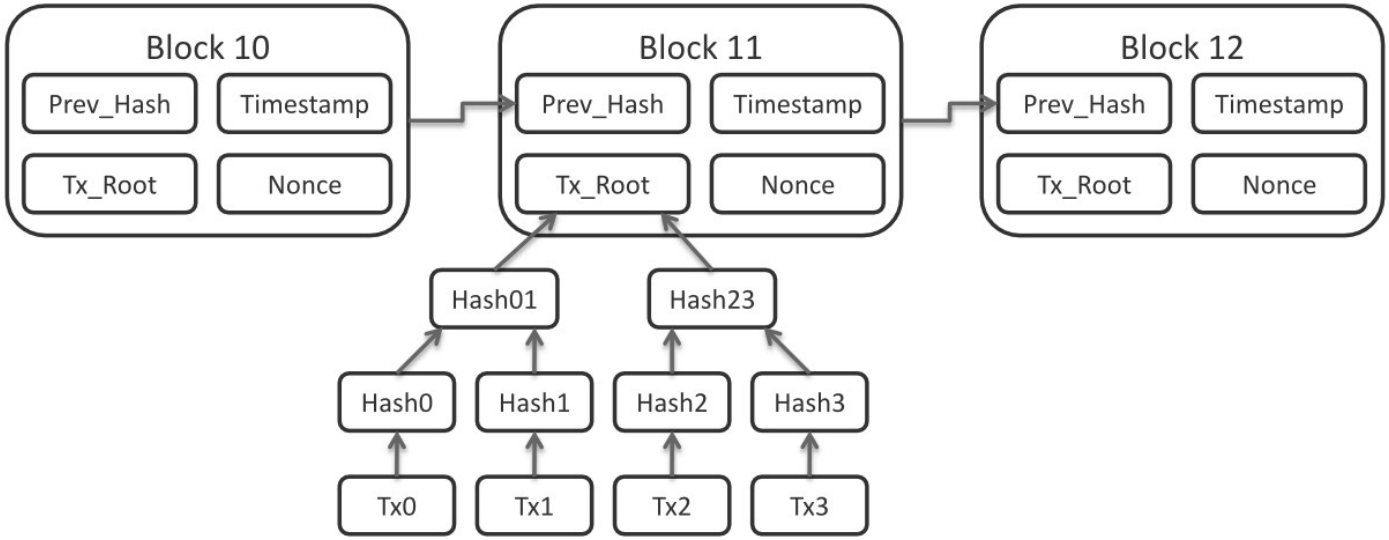
"Ho sviluppato un sistema di moneta digitale open source p2p chiamato Bitcoin. E' completamente decentralizzato, senza server centrali o parti fiduciarie, perché tutto è basato su prove crittografiche al posto della fiducia. Provatelo o date un'occhiata agli screenshots e docuentazione di progetto..."

Scritto da Satoshi Nakamoto l'11 febbraio 2009 alle 22:27

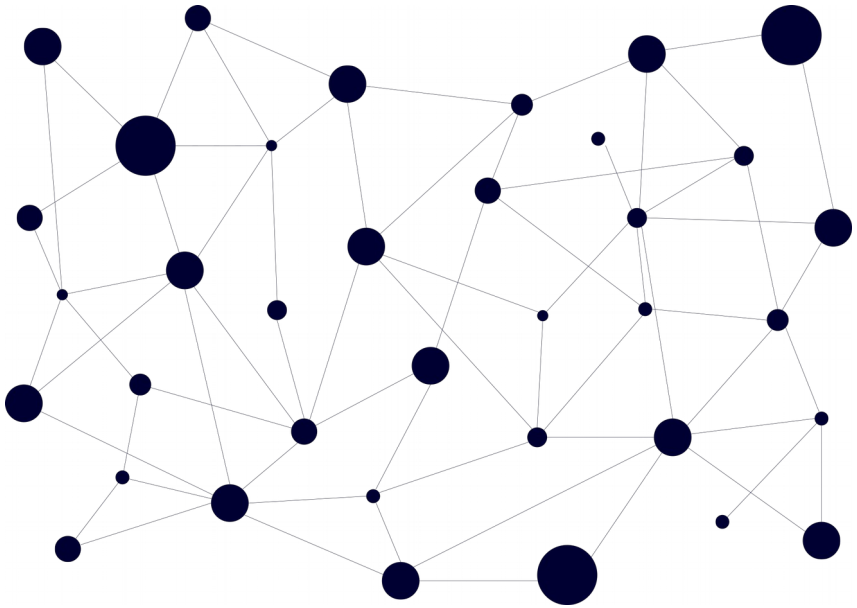
Timestamping (data certa)

Ordinamento di eventi
Unixtime
Data e ora certe

Blocchi & Catene



Rete Peer to Peer (da pari a pari)



No server centrali
No server speciali
Resiliente
Ridondata

Esempi storici:
Napster, Gnutella,
Kademlia...

Procollo Blockchain

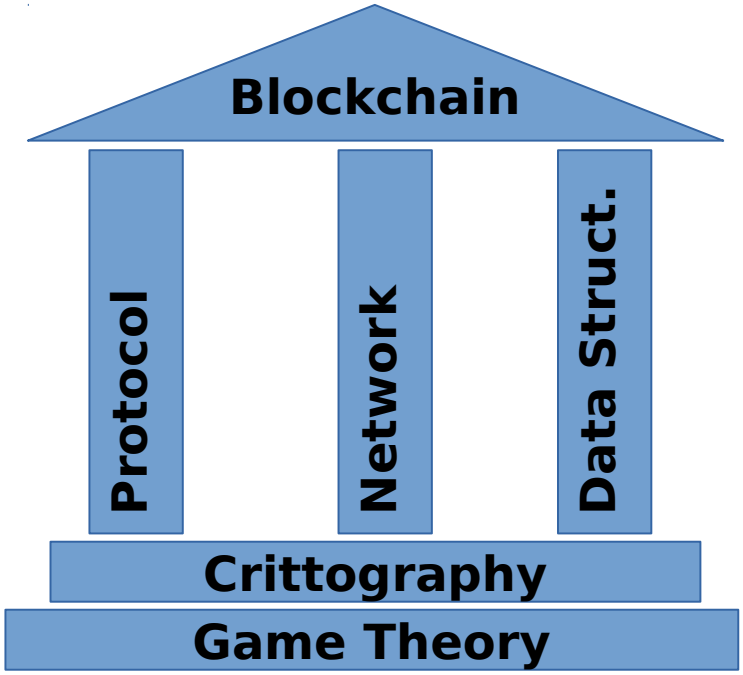
Transparenza
Informazioni Aperte
Controlli Indipendenti

Competizione e
Cooperazione

Blockchain Elementi fondanti

Rete +
Protocollo +
Struttura dati +
Crittografia +
Teoria dei Giochi =

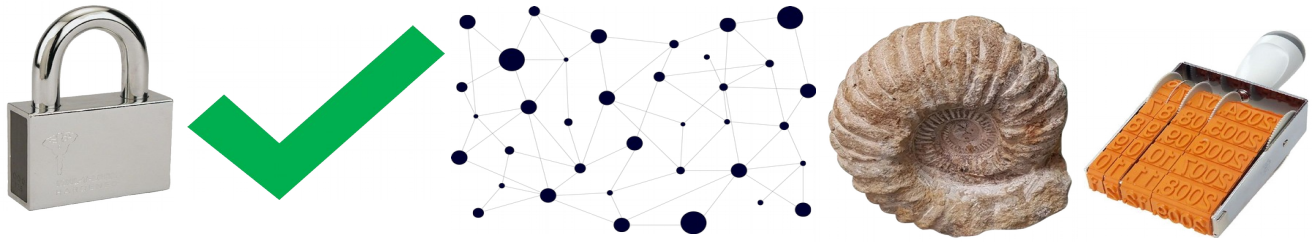
Blockchain



Benefici della Blockchain

Transparenza
Verificabilità
Responsabilità
Sicurezza

Timestamping
Immutabilità
Resilienza
Indipendenza



Applicazioni della Blockchain

Finanza
Assicurazioni
Media & Sport
Salute
Identità digitale
Amministrazione
Pagamenti

Filiera