

# Origin Story:

The foundations for the modern Blockchain were outlined in Satoshi Nakamoto's white paper

## 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.

# Blockchain VS Bitcoin



**Bitcoin**

- The leading digital currency
- Numerous consumer/SME and financial service payment applications, particularly in developing economies
- A favourite for speculators given its volatility and liquidity, with high-frequency trading and hedge fund participation



**Blockchain**

- Distributed ledger with cryptographic integrity
- Potential replacement for middleware networks and clearing houses in financial transactions where 3<sup>rd</sup> party verification is required
- Applications extend to other networks where veracity is critical to performance

## Bitcoin:

“A digital coin as a chain of digital signatures” (Nakamoto)

- Basis of a digital currency
- Electronically created and held
- Commodity: 21 million can ever be “mined”
- Bitcoins are mined
- Divisible Units

## Blockchain:

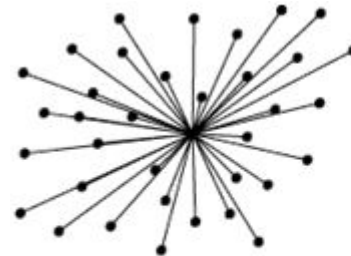
- Append only sequential data structure
- Hash pointer linked list of blocks
- Each block is a record of a transaction
- Used to build a ledger or record of transactions
- Copies of the blockchain are kept by everyone
- “Miners” append to it

# Decentralization

“What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.”-Nakamoto

Transactions between parties that require the trust provided by 3rd parties cost:

- i. Time
- ii. Money
- iii. Control



centralised



decentralised

# Fraud Protection

## 1. Reversible Transactions

- A fraction of traditional financial transactions are fraudulent.
- Computationally impossible to revert transaction

## 2. Byzantine Generals Problem

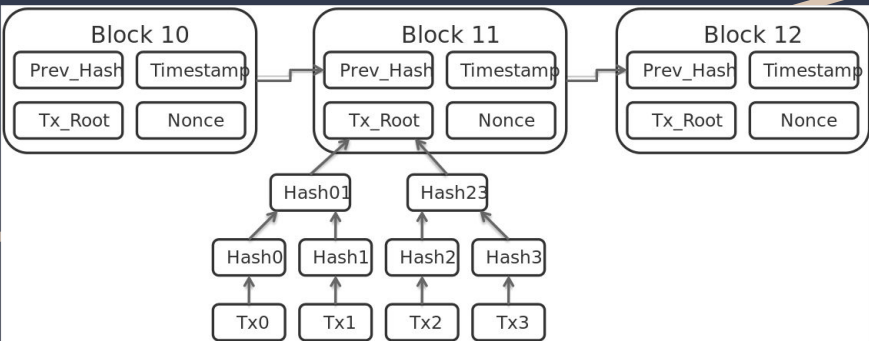
## 3. Double Spending

- The risk that a person could concurrently send a single unit of currency to two different sources.

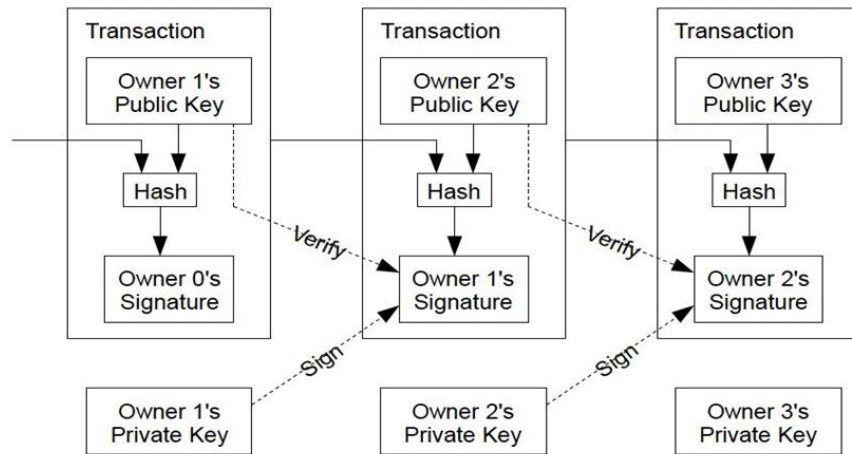
# What is the Blockchain?

A blockchain is a **ledger of facts**, replicated across several computers assembled in a peer-to-peer network.

- Facts can be anything from monetary transactions to content signature.
- All communication inside the network takes advantage of cryptography to securely identify the sender and the receiver.
- When a node wants to add a fact to the ledger, a consensus forms in the network to determine where this fact should appear in the ledger; this consensus is called a **block**.



# What is a Bitcoin

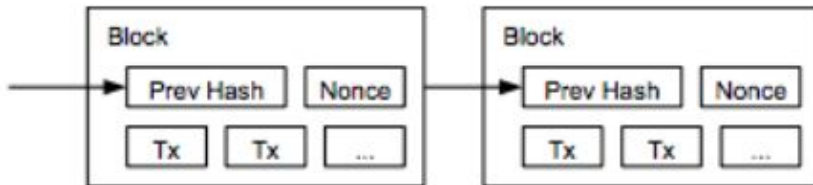


A coin owner transfers coins by digitally signing(via ECDSA) a hash digest of the previous transactions and the public key of the next owner. This signature is appended to the end of the coin

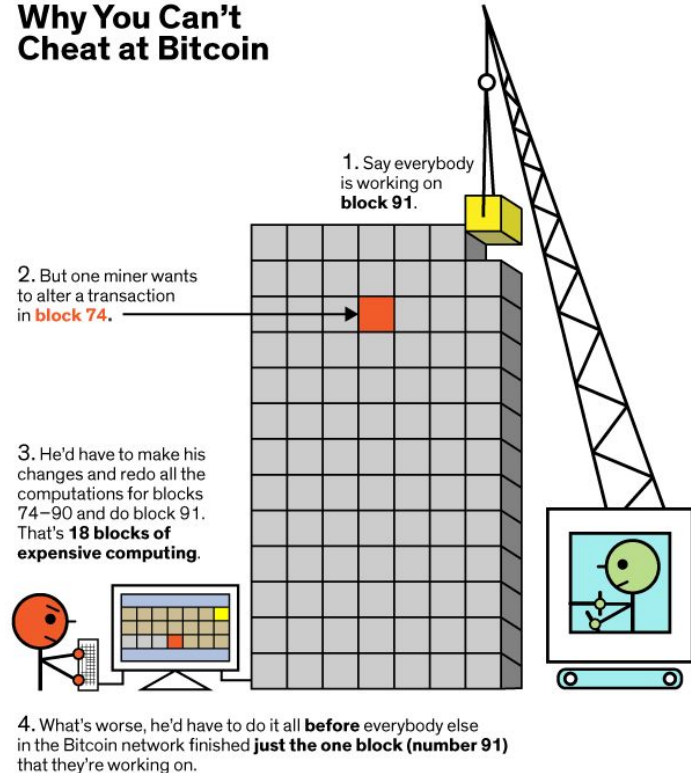
“electronic coin as a chain of digital signatures”  
- Nakamoto

# Proof-of-Work






















HashCash Algorithm used by trial and error to discover a "nonce" number that when included in the block yields a hash with a sufficient number of leading zero bits.



## Why You Can't Cheat at Bitcoin

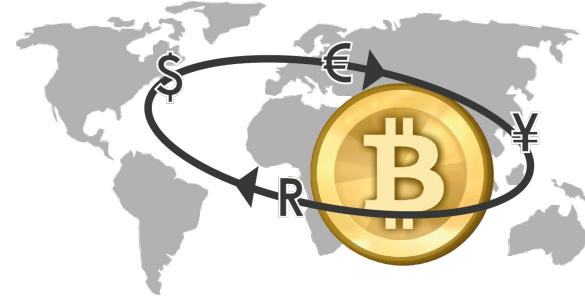


# Non - Financial Applications: Bitcoin & Blockchain

Non-Financial Use Cases					
Digital Content/Documents, Storage & Delivery	Authentication & Authorization		Digital Identity	Marketplace	
 BitProof, Blockcai, Ascribe, ArtPlus, Chainy.Link, Stampery, Blocktech (Alexandria), Bisantium, Blockparti, The Rudimental, BlockCDN	 The Real McCoy, Degree of Trust, Everpass, BlockVerify,		 Sho Card, Uniquid, Oname, Trustatom	 Providing premium rights & brand based coins: MyPowers	
Smart Contracts	Real Estate	Diamonds	Gold & Silver	Reviews/Endorsement	
 Otonomos, Mirror, Symbiont, New system Technologies	 Factom	 Everledger	 BitShares, Real Asset Co., DigitalTangible (Serica), Bit Reserve	 TRST.im, Asimov (recruitment services), The World Table	
Blockchain in IoT	App Development	Network Infrastructure & APIs	Other		
 Filament, Chimera-inc.io, ken Code – ePug	 Proof of ownership for modules in app development: Assembly	 Ethereum, Eris, Codius, NXT, Namecoin, Colored Coins, Hello Block, Counterparty, Mastercoin, Corona, Chromaway, BlockCypher	 <u>Prediction platform:</u> Augur  <u>Election Voting:</u> Follow My Vote  <u>Patient Records management:</u> BitHealth		
Financial Use Cases					
Currency Exchange & Remittance	P2P Transfers	Ride Sharing	Data Storage	Trading Platforms	Gaming
 Coinbase (Wallet), BitPesa, Billion, Ripple, Stellar, Kraken, Fundrs.org, MeXBT, CryptoSigma	 BTC Jam, Codius, BitBond, BitnPlay (Donation), DeBuNe (SME's B2B transactions)	 La'zooz	 Storj.io, Peernova	 equityBits, Spritzle, Secure Assets, Coins-e, DXMarkets, MUNA, Kraken, BitShares	 PlayCoin, Play(on DACx platform), Deckbound

# Financial Applications: Bitcoin & Blockchain

## 1) International Remittance



- 2) Creation of a modern economic system
- 3) Micropayments

