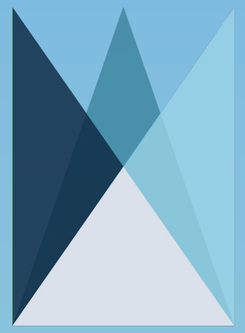
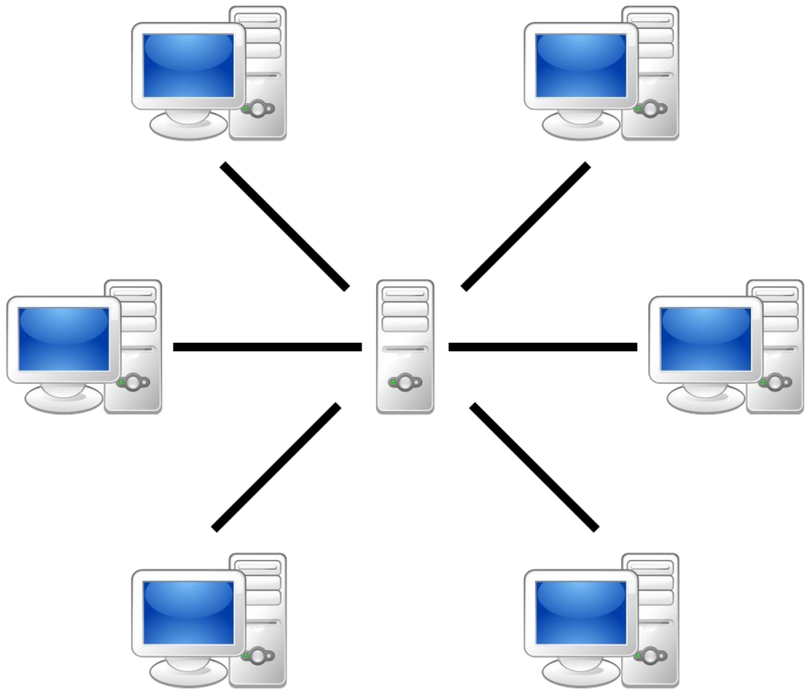
BLOCKCHAINS AND CRYPTOCURRENCIES



BLOCKCHAIN
@ COLUMBIA

Problems of Centralized Data



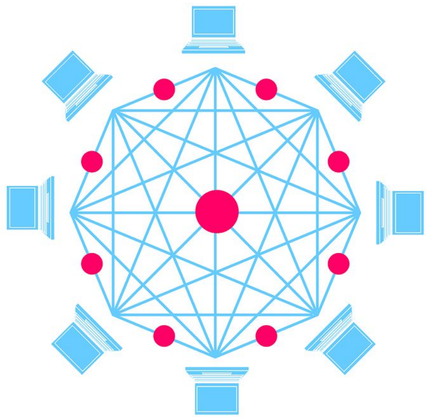
Distributed Ledger Technology

Blockchain as a Digital Ledger

	Ledger Book	Blockchain
Components	Pages	Blocks
Content	Text	Data (transactions)
Metadata	Title, Chapter, Page numbers	Technical info: link to previous block, unique block ID
Ordering	By page number	Time
Control	Central Authority	Everyone

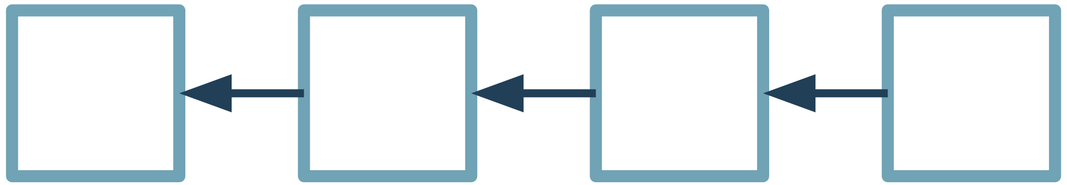
Distributed Ledger

- All data is recorded on ***a distributed public ledger*** that is maintained by multiple nodes (servers) connected to the network
- Everyone in the network has a copy of the ledger
- Anyone can participate on the network by becoming a node in the network

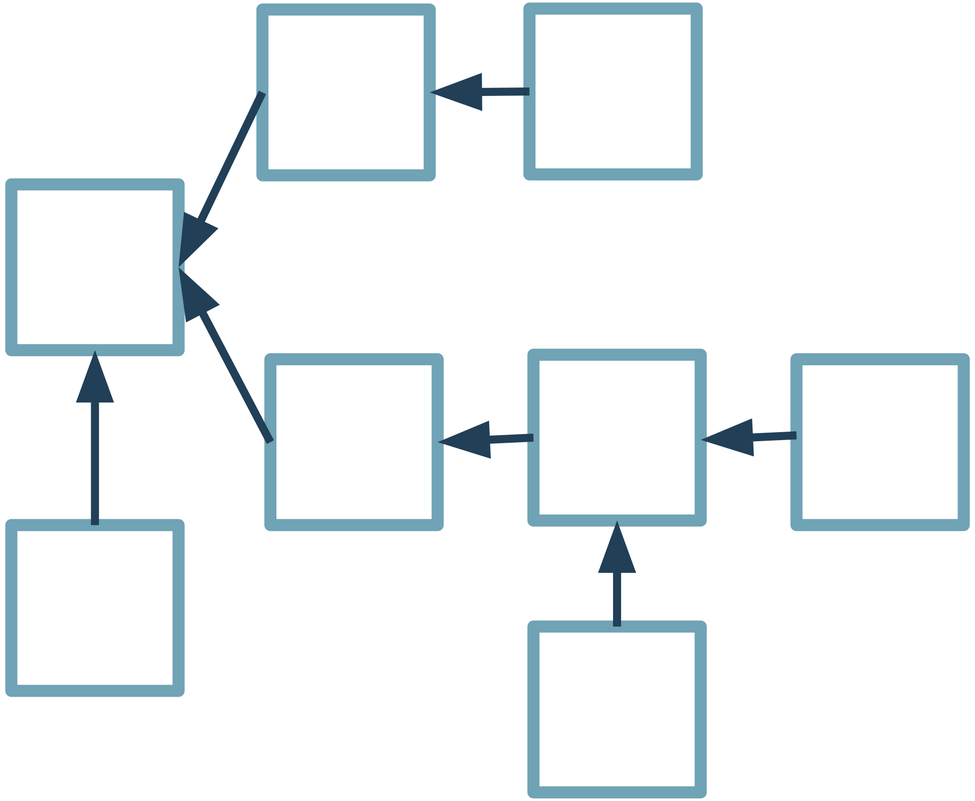


Implementations of DLT

Blockchain



Graph Architecture

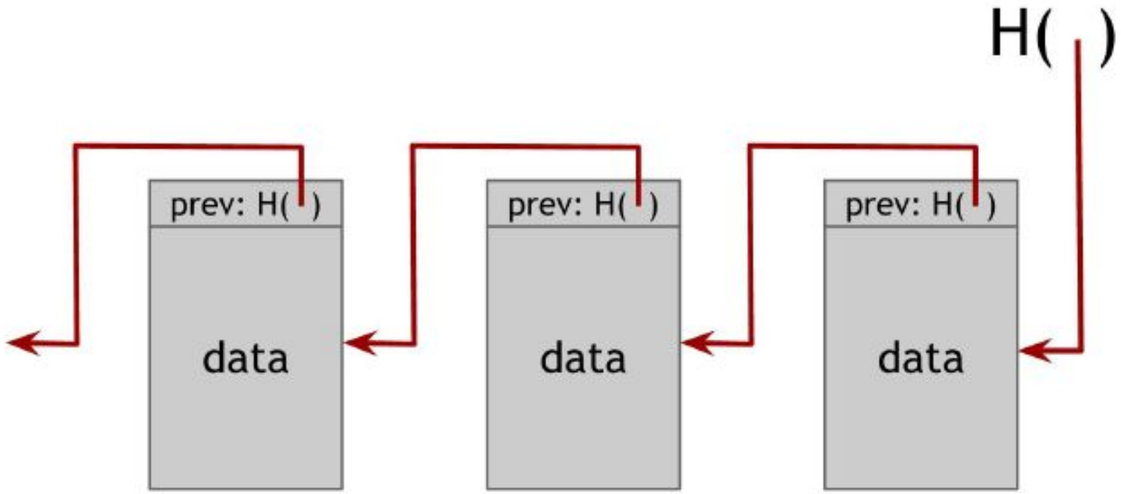


The “block” in Blockchain

- A **block** contains the data that has been sent into the network within a specific time interval
  - Consider it like a packet of new information that should be added to the chain
- Example of the Metadata (Bitcoin)
  - time stamp
  - nonce (will explain later)
  - unique id (hash) of previous block
  - coinbase transaction, the reward of producing a block

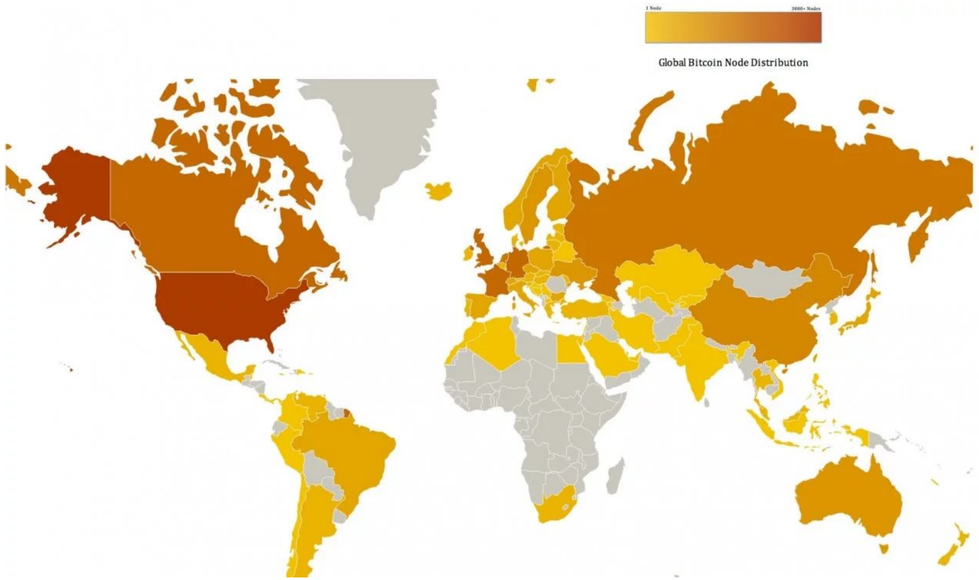
The “chain” in Block*chain*

- **Blocks are linked together to produce a tamper proof log of the entire history of data known as the *blockchain***
- **Each block contains a hash of the previous block**
  - Modifying the internal data of a block will produce a detectable change
  - **NOTE: block hashes uniquely identify a block and its content**



The Node

- A **node** is like a server or computer
- In order to maintain decentralization, cannot have centralized store of data
  - Many different sources, all with same ledger
  - Ensures immutability
  - Anyone can be a node



The Bitcoin Network

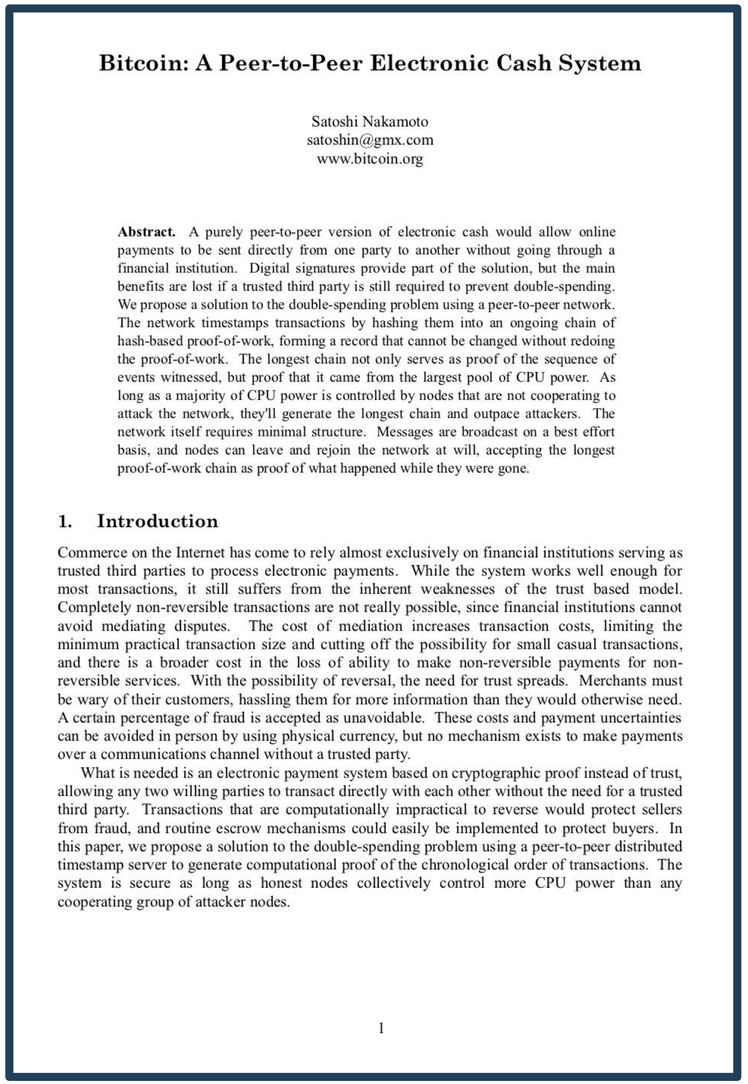
Blockchain is *not* Bitcoin

"[Blockchain] is to Bitcoin, what the internet is to email. A big electronic system, on top of which you can build applications. Currency is just one." —*Sally Davies, FT Technology Reporter*"

History of Bitcoin

- **Satoshi Nakamoto**
- **Bitcoin: A Peer-to-Peer Electronic Cash System**
- **October 2008**

The white-paper was published describing the cryptocurrency and later Satoshi launched the Bitcoin Network in 2009.



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.

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 non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

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. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1

Why Build a Digital Currency?

- **Centralized Regulation**
  - Counterparty risk and reversible transactions
  - Cost of mediation increases transaction costs
- **International Payments**
  - High transaction fees
  - Takes days to process (3-5 days on avg)
    - Quickest way to send 10k to London is to physically fly it there
- **Lack of financial inclusion**
  - 2B+ people don’t have bank account
  - Lack of support for small transfers
  - Requires registered identity

Wallets

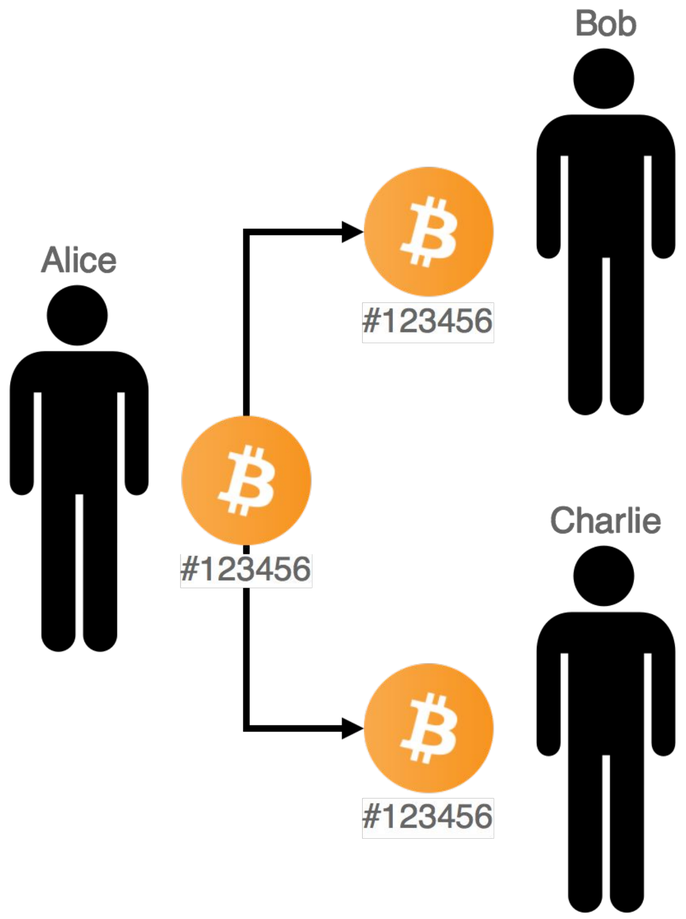
- Wallets are what store your digital tokens
- Tokens are owned by **public keys** which are publicly visible IDs
  - Think of it like a username to an online account
  - Example: asdf32cn234nosidfn0234lkjn12pi31..
- Each Wallet also contains a **private key** (password) to validate possession of the coin
  - Example: 0n12oi31028hmfasdofj123o4in2038..

Transactions as Data

- Each Wallet contains a decimal amount of Bitcoins
- To send Bitcoin you need to follow two steps:
  1. Provide another wallet address specifying where you want to send Bitcoin
  2. Use your **private key** to sign the transaction to validate possession of the coin
- Transactions are *pseudonymous* not anonymous
- Transactions are public and can be viewed using common block explorers

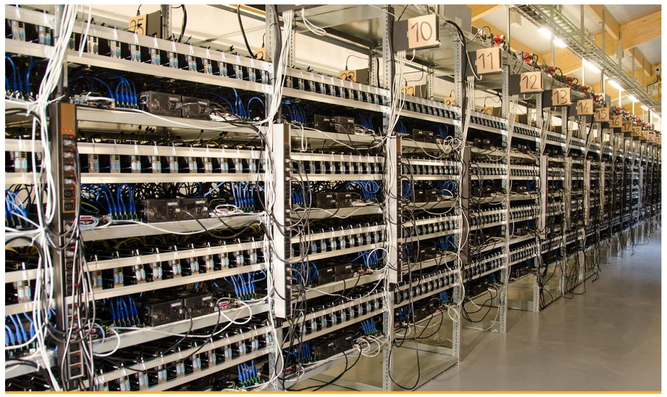
The Double Spending Problem

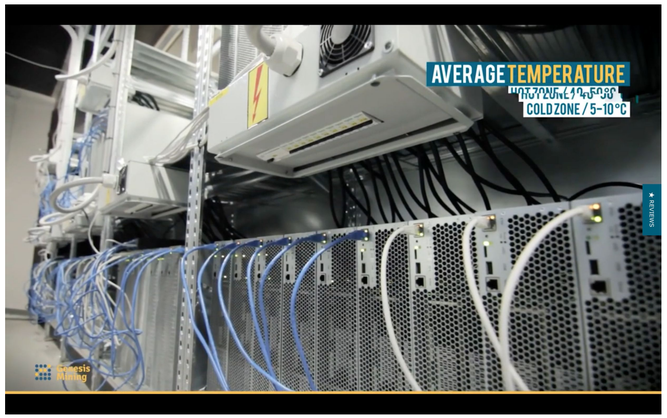
- **Double spending** involves spending the same unit of currency twice
- Very difficult problem to solve since information on the internet gets circulated through digital copies
  - e.g. sending copy of pdf or email



Who produces a block?

- Nodes who participate in the network must reach agreement on which new blocks and transactions are valid
- **Miners** follow certain consensus protocols to collect valid transactions into a block and add that block to the chain
- Mining Pools exist to increase the likelihood of receiving a reward





Consensus: Why it matters

- Trust
- Decentralization
- Security
- Efficiency

How is Consensus Reached?

- ***Consensus*** **occurs when all the nodes in the network agree on which block to produce next**
- **In centralized systems a single entity validates all incoming transactions**
- **In decentralized systems a consensus mechanism needs to ensure that no token is spent twice**
  - **Some examples include:**
    - Proof of Work [PoW] (e.g. Bitcoin, Ethereum)
    - Proof of Stake [PoS] (e.g. Nxt)
    - Delegated Proof of Stake [DPoS] (e.g. Steem)

Bitcoin Consensus

Steps for Bitcoin Consensus Algorithm

1. Every 10 seconds, a set of new transactions is broadcasted to all nodes
2. Each node collects new transactions into a block
3. In each round a “random” node gets selected to add a block
4. Nodes accept a block only if the transactions in it are valid
5. Nodes express acceptance by including its hash in the next block they create