National Telecommunications Institute

For Policy Research, Innovation & Training

“Introduction to Blockchain Technology”

Ravi Kumar Mathur
ADG, NTIPRIT

Blockchain $\neq Bitcoin$

- **The technology behind cryptocurrencies.**
- **Analogous to the internet**

When we have internet

Why BlockChain?

Problems which Internet failed to solve??

Trust

Intermediary

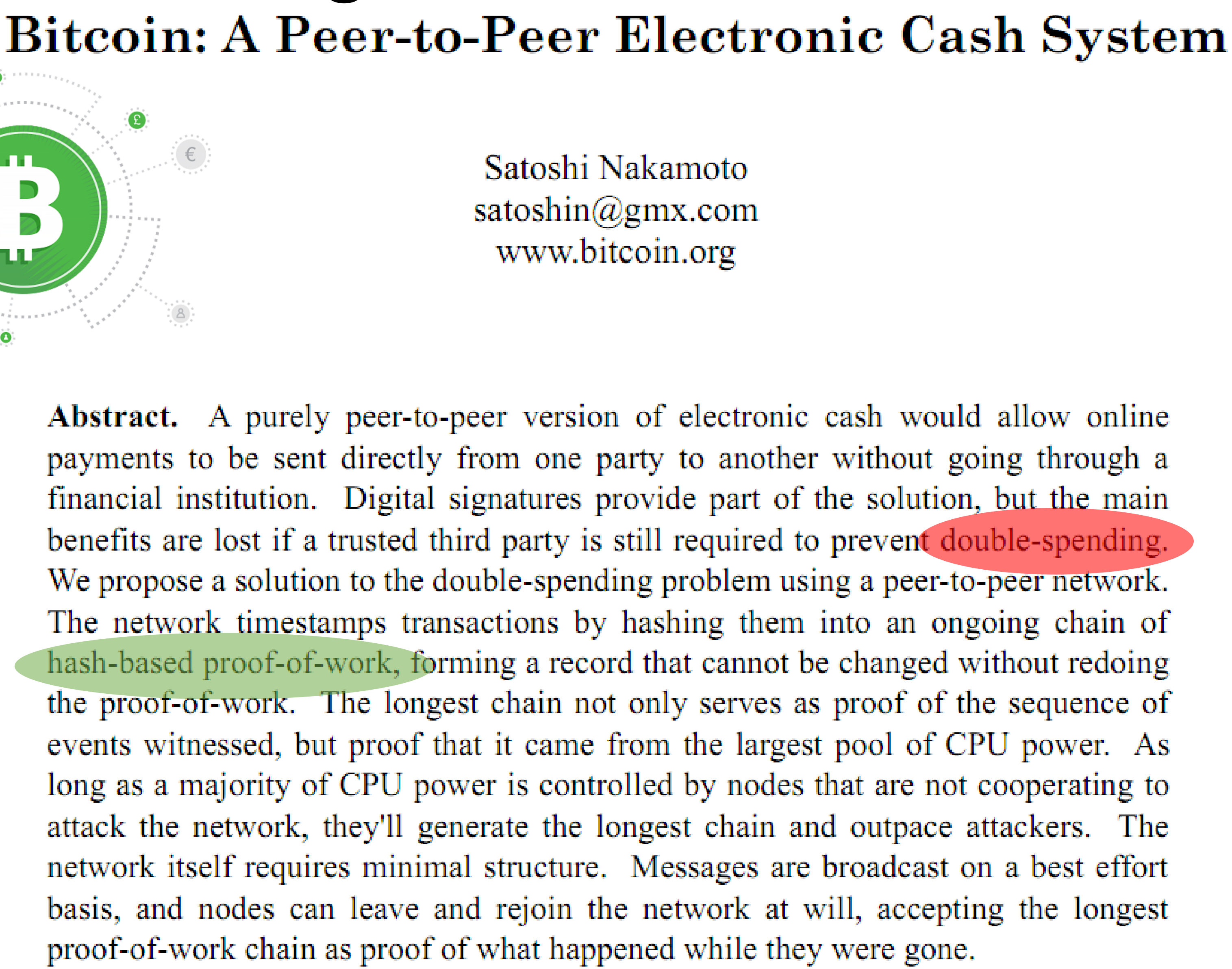
Origin of Blockchain

Short comings of current transaction system:

- Cash is useful only in local transactions and in relatively small amounts.
- The time between transaction and settlement can be long.
- Duplication of effort and the need for third-party validation and/or the presence of intermediaries add to the inefficiencies.
- Fraud, cyberattacks, and even simple mistakes add to the cost and complexity of doing business, and they expose all participants in the network to risk if a central system, such as a bank, is compromised.
- Many people in the world don’t have access to a bank account and have had to develop parallel payment systems to conduct transactions.

And transaction volumes will explode with the rise of Internet of Things (IoT)

Emergence of BitCoin

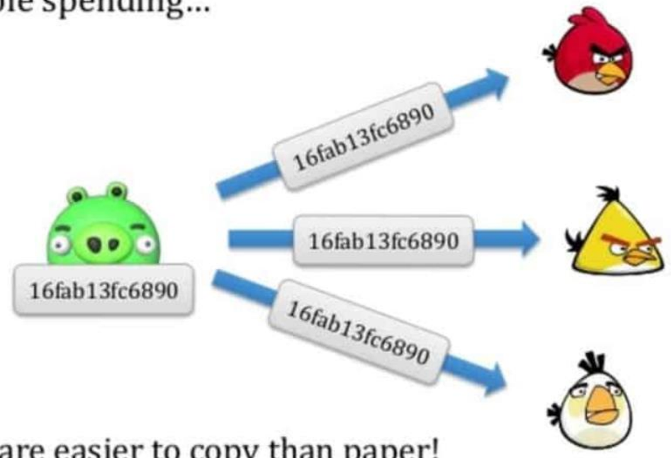


Bitcoin: A Peer-to-Peer Electronic Cash System

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.

Double spending...



Bits are easier to copy than paper!

Emergence of BitCoin

BITCOIN- A digital currency to address the complexities, vulnerabilities, inefficiencies, and costs of current transaction systems.

Advantages:

» Cost-effective: Bitcoin eliminates the need for intermediaries.

» Efficient: Transaction information is recorded once and is available to all parties through the distributed network.

» Safe and secure: The underlying ledger is tamper evident. A transaction can't be changed; it can only be reversed with another transaction, in which case both transactions are visible

The Birth of Blockchain

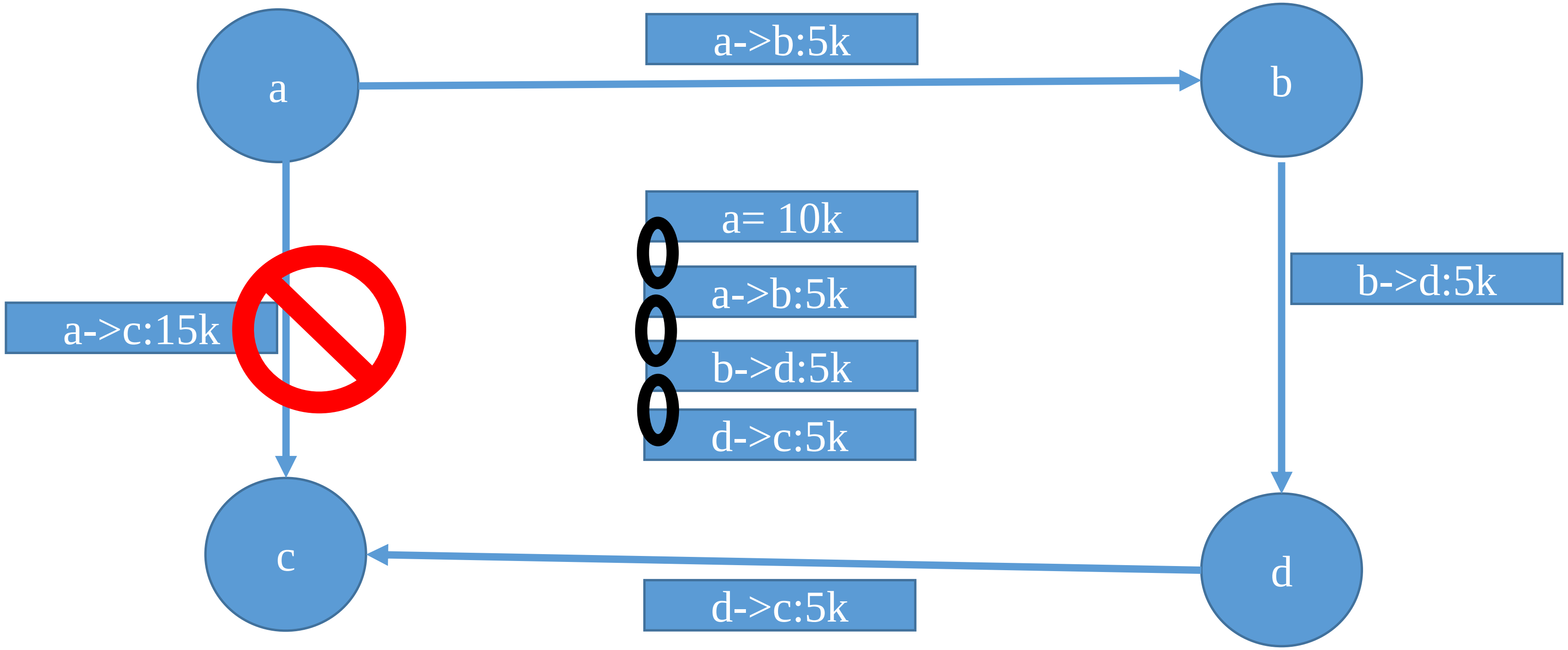
- Bitcoin is actually built on the foundation of blockchain, which serves as bitcoin’s shared ledger.

- This shared ledger can be used to record any transaction and track the movement of any asset whether tangible, intangible, or digital

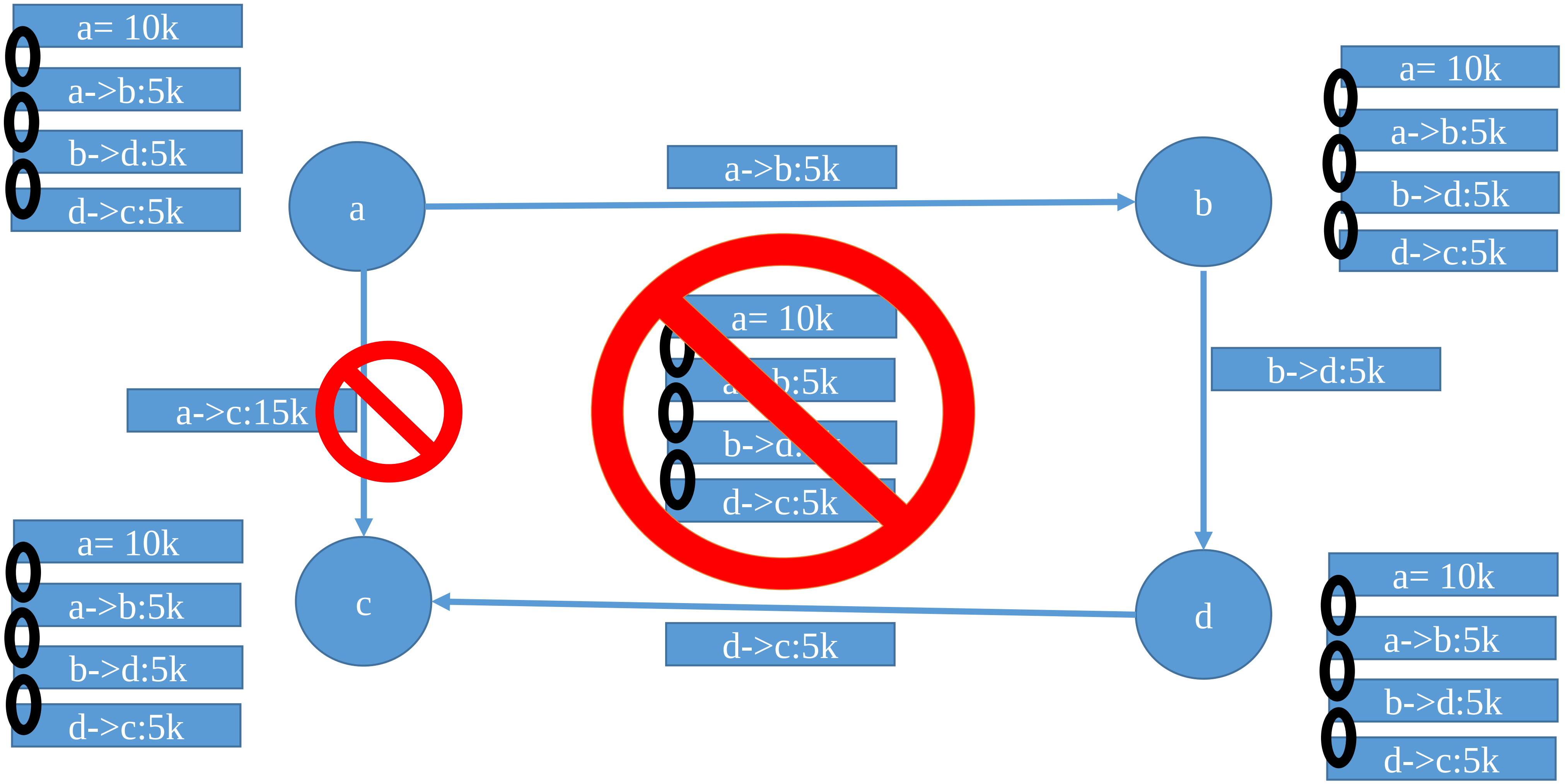
Bitcoin and blockchain are not the same. Blockchain provides the means to record and store bitcoin transactions, but blockchain has many uses beyond bitcoin. Bitcoin is only the first use case for blockchain

- Blockchains are Distributed Ledgers
  - Ledgers are historically centralized and private
  - Blockchains are Decentralized or Distributed

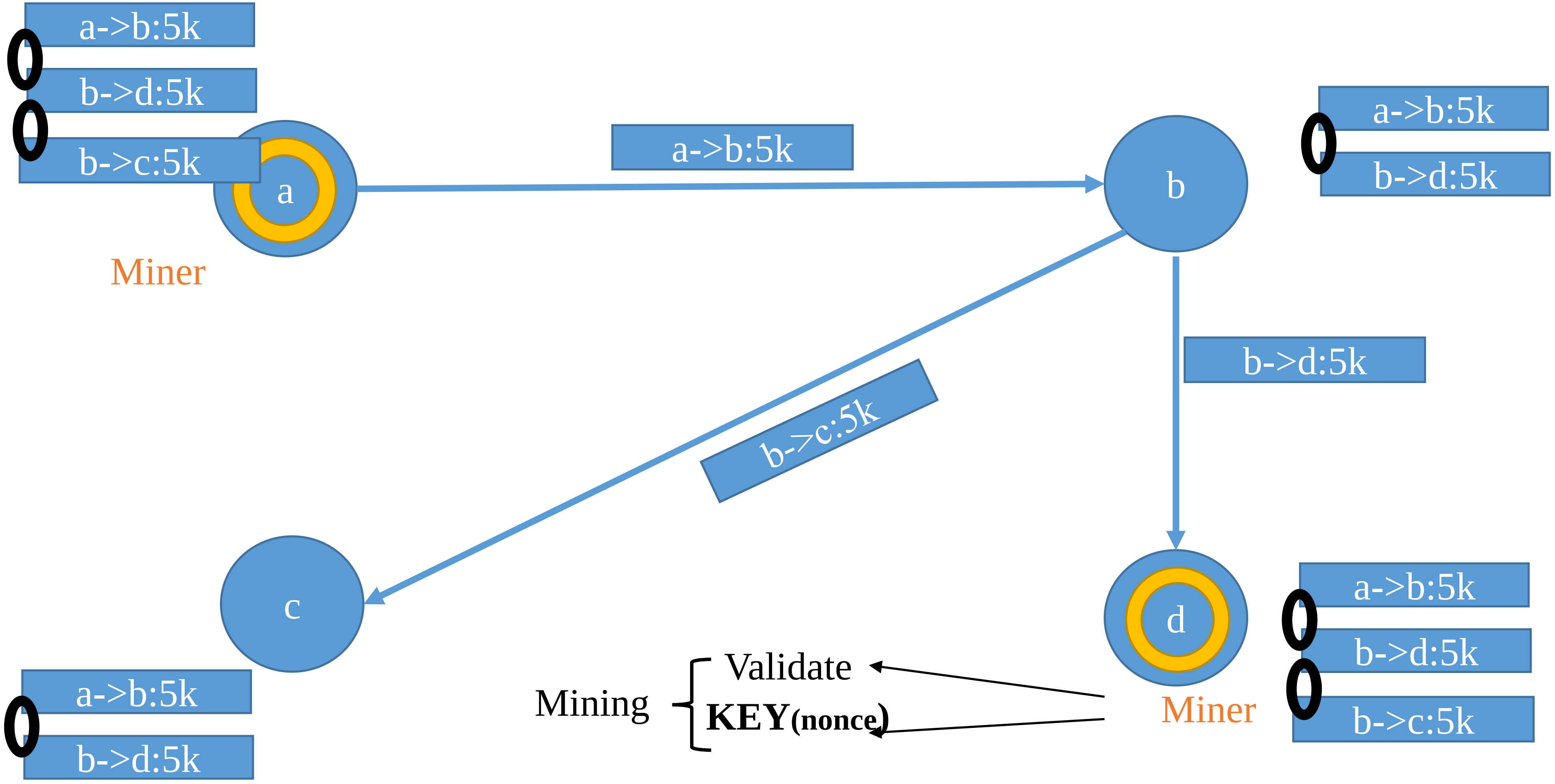
Open Ledger



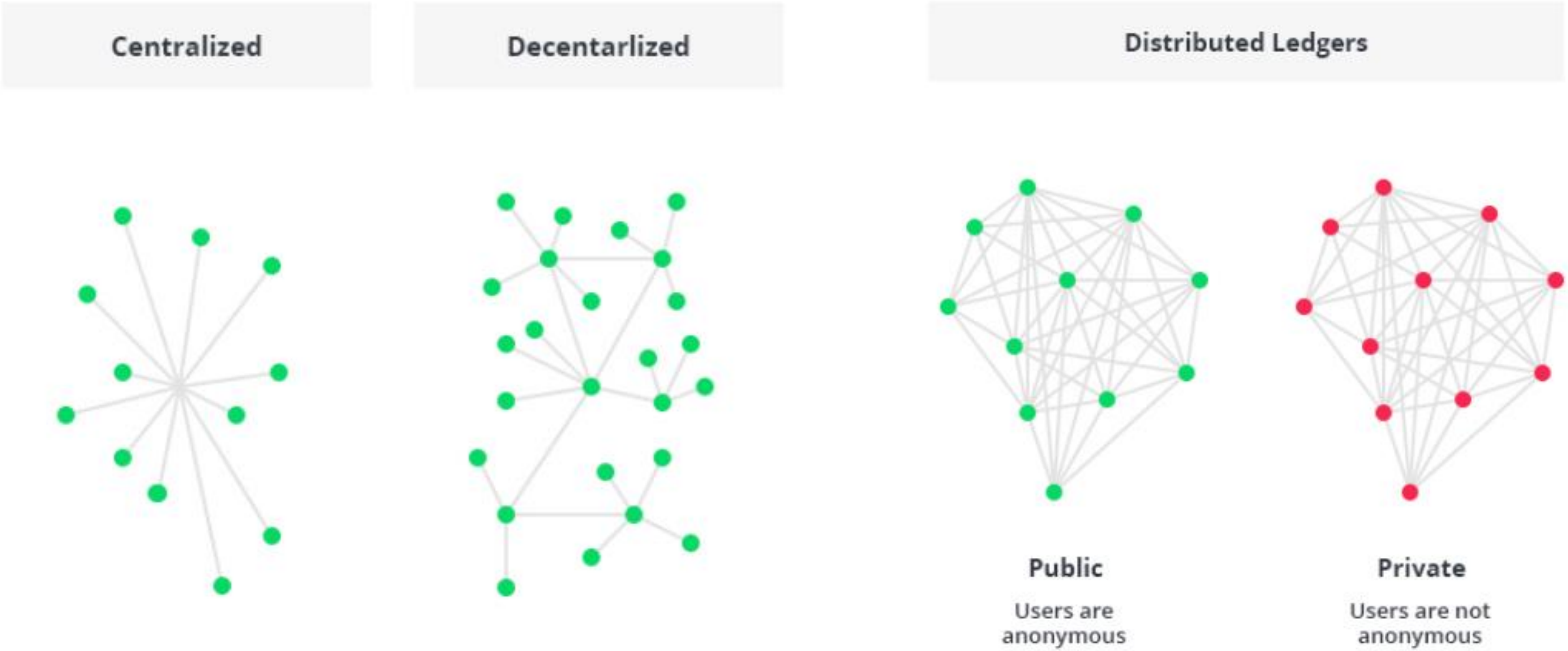
Distributed Ledger



Synchronising Distributed Ledger



Blockchain Architecture



Centralized

Decentarlized

Distributed Ledgers

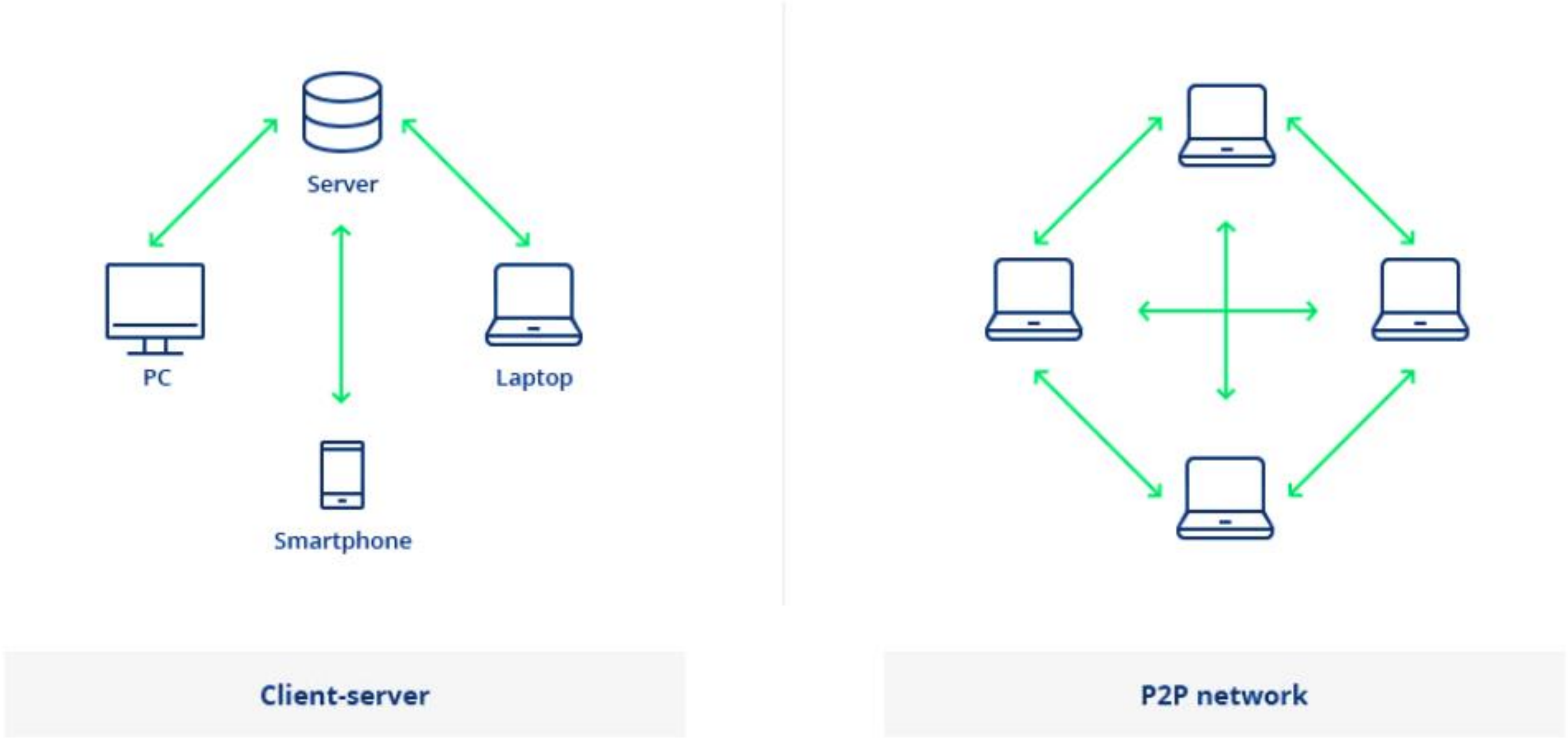
Public

Users are anonymous

Private

Users are not anonymous

Blockchain Architecture

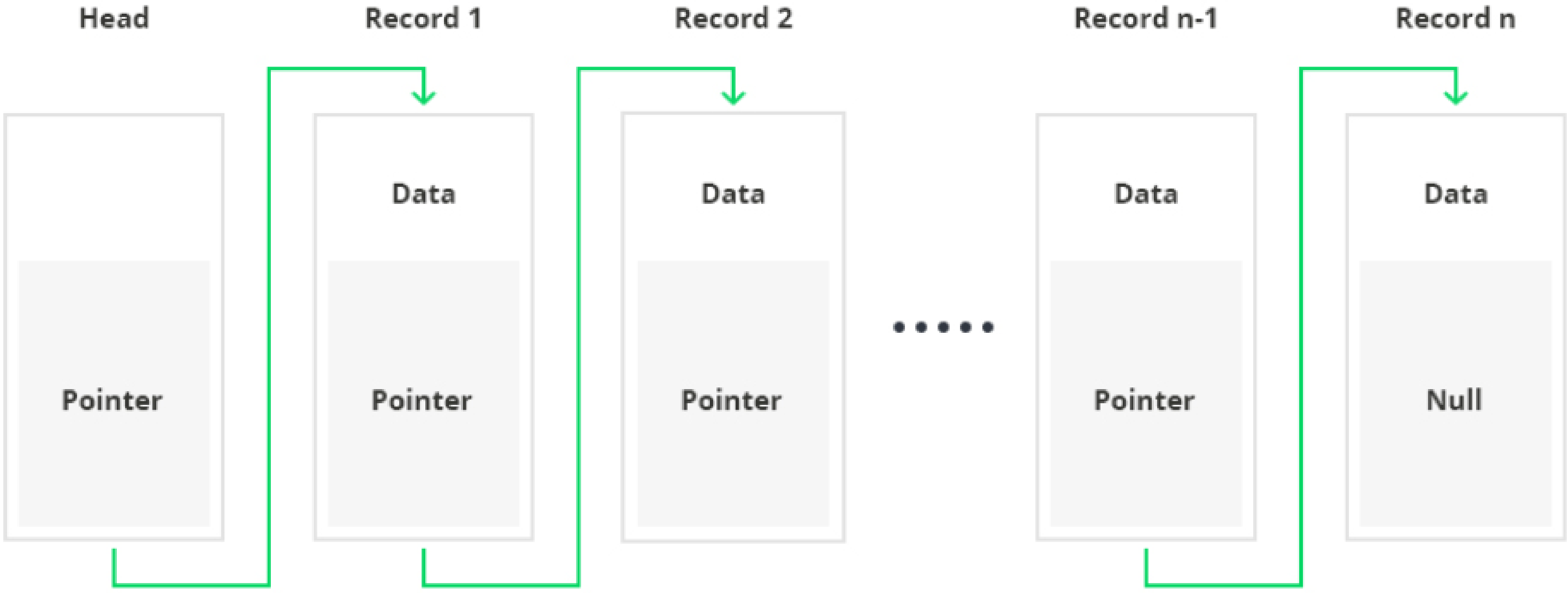


The blockchain is a decentralized, distributed ledger (public or private) of different kinds of transactions arranged into a P2P network. This network consists of many computers, but in a way that the data cannot be altered without the consensus of the whole network.

Blockchain Architecture

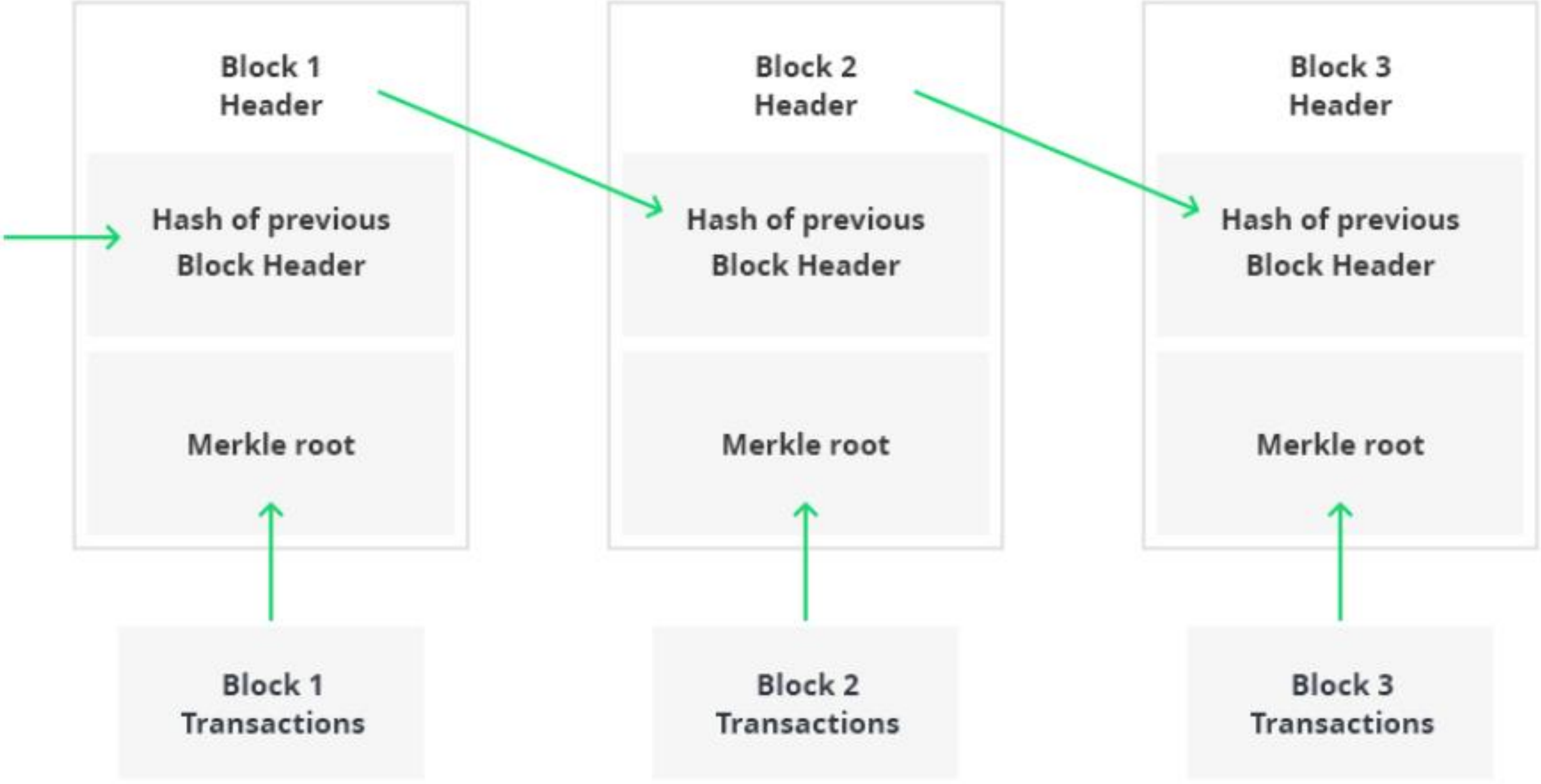
Data structures used in blockchain:

- **Pointers** - variables that keep information about the location of another variable. Specifically, this is pointing to the position of another variable.
- **Linked lists** - a sequence of blocks where each block has specific data and links to the following block with the help of a pointer.



Blockchain Architecture

Blockchain Structure:

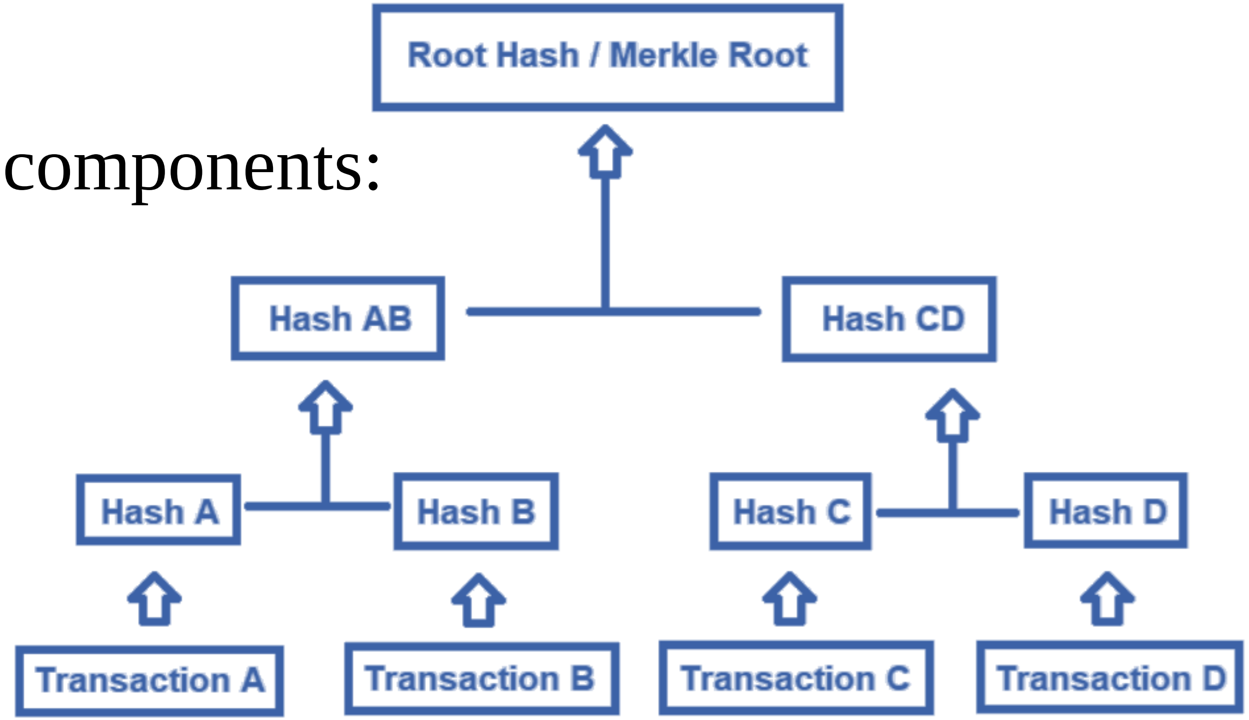


Blockchain Architecture

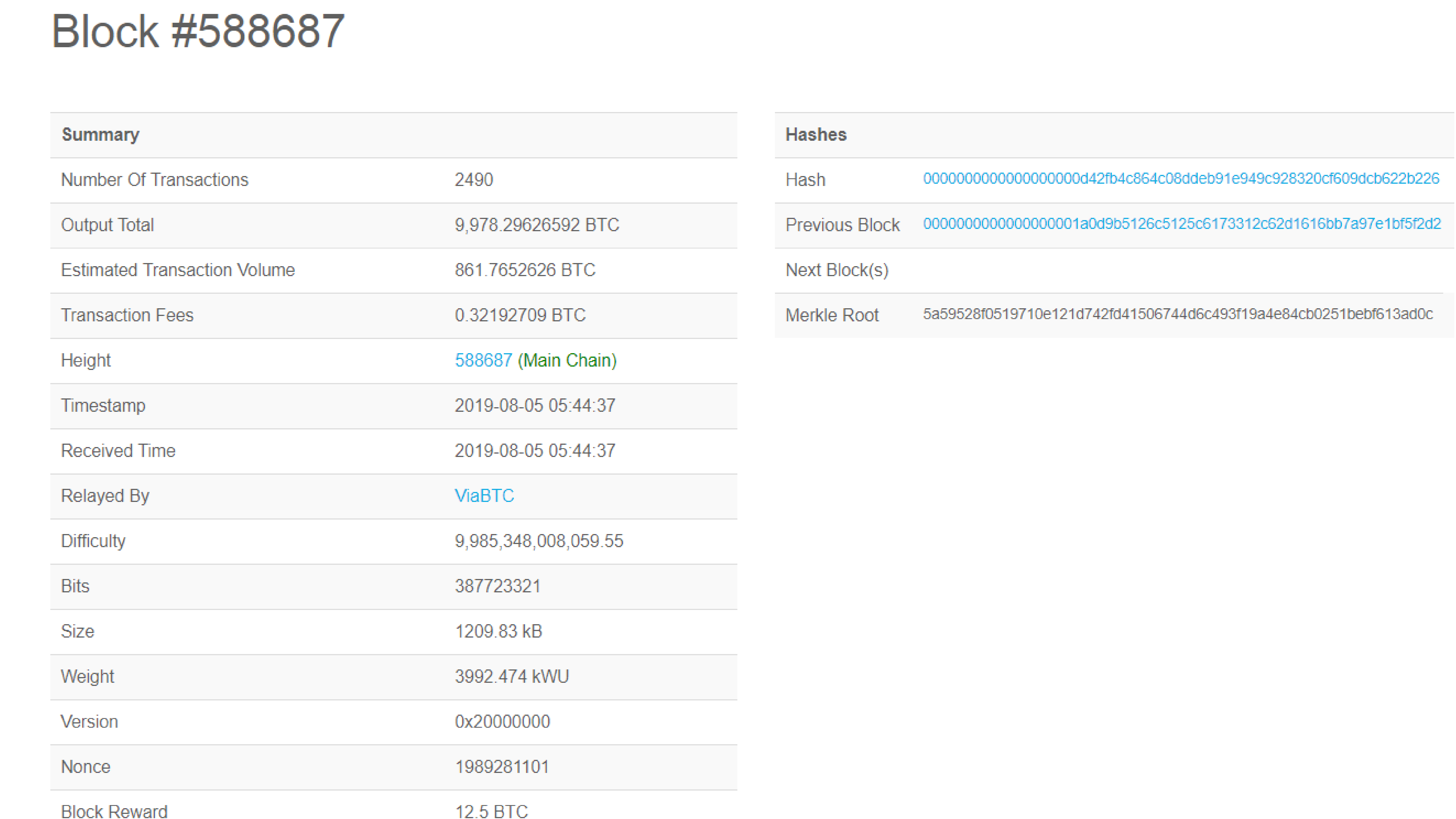
Block header

The head of the block have following components:

1. the hash of the previous block
2. the hash of the block
3. the root hash of the Merkle tree
4. the time in seconds
5. the goal of the current difficulty
6. the nonce



Block Hash = (Prev block Hash) Θ (Merkel Root) Θ Nonce



Block #588687

Summary	
Number Of Transactions	2490
Output Total	9,978.29626592 BTC
Estimated Transaction Volume	861.7652626 BTC
Transaction Fees	0.32192709 BTC
Height	588687 (Main Chain)
Timestamp	2019-08-05 05:44:37
Received Time	2019-08-05 05:44:37
Relayed By	ViaBTC
Difficulty	9,985,348,008,059.55
Bits	387723321
Size	1209.83 kB
Weight	3992.474 kWU
Version	0x20000000
Nonce	1989281101
Block Reward	12.5 BTC

Hashes	
Hash	0000000000000000000d42fb4c864c08ddeb91e949c928320cf609dcb622b226
Previous Block	0000000000000000001a0d9b5126c5125c6173312c62d1616bb7a97e1bf5f2d2
Next Block(s)	
Merkle Root	5a59528f0519710e121d742fd41506744d6c493f19a4e84cb0251bebf613ad0c

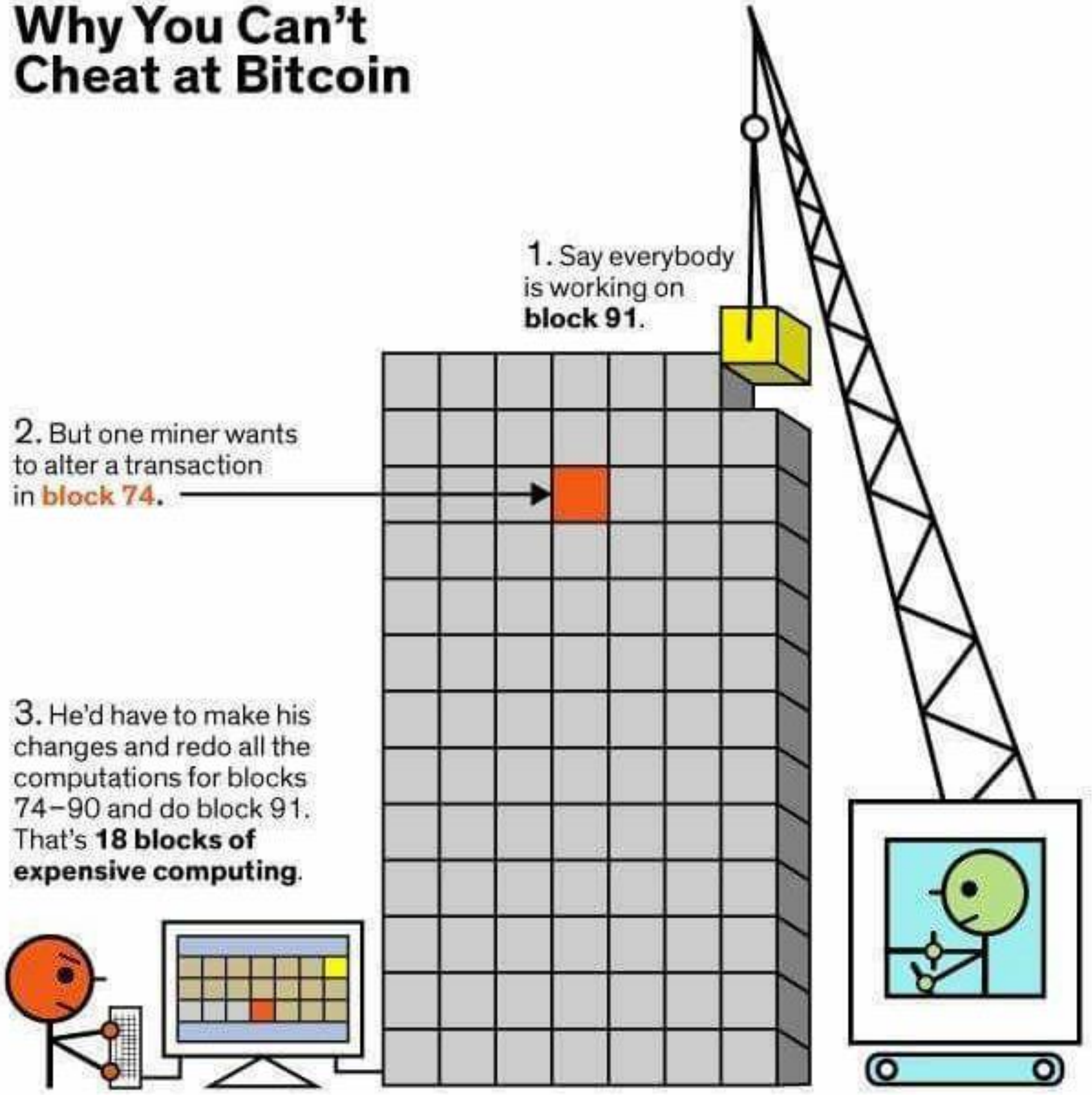
Proof of work

- A **proof of work** is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements.
- In order for a block to be accepted by network participants, miner must complete a proof of work which covers all of the data in the block.
- The difficulty of this work is adjusted so as to limit the rate at which new blocks can be generated by the network to one every 10 minutes.
- Due to the very low probability of successful generation, this makes it unpredictable which worker computer in the network will be able to generate the next block.

Other Consensus Algorithm

- **Proof of Stake**
- **Proof of Burn**
- **Proof of Capacity**
- **Proof of elapsed time**

Why You Can't Cheat at Bitcoin



1. Say everybody is working on **block 91**.

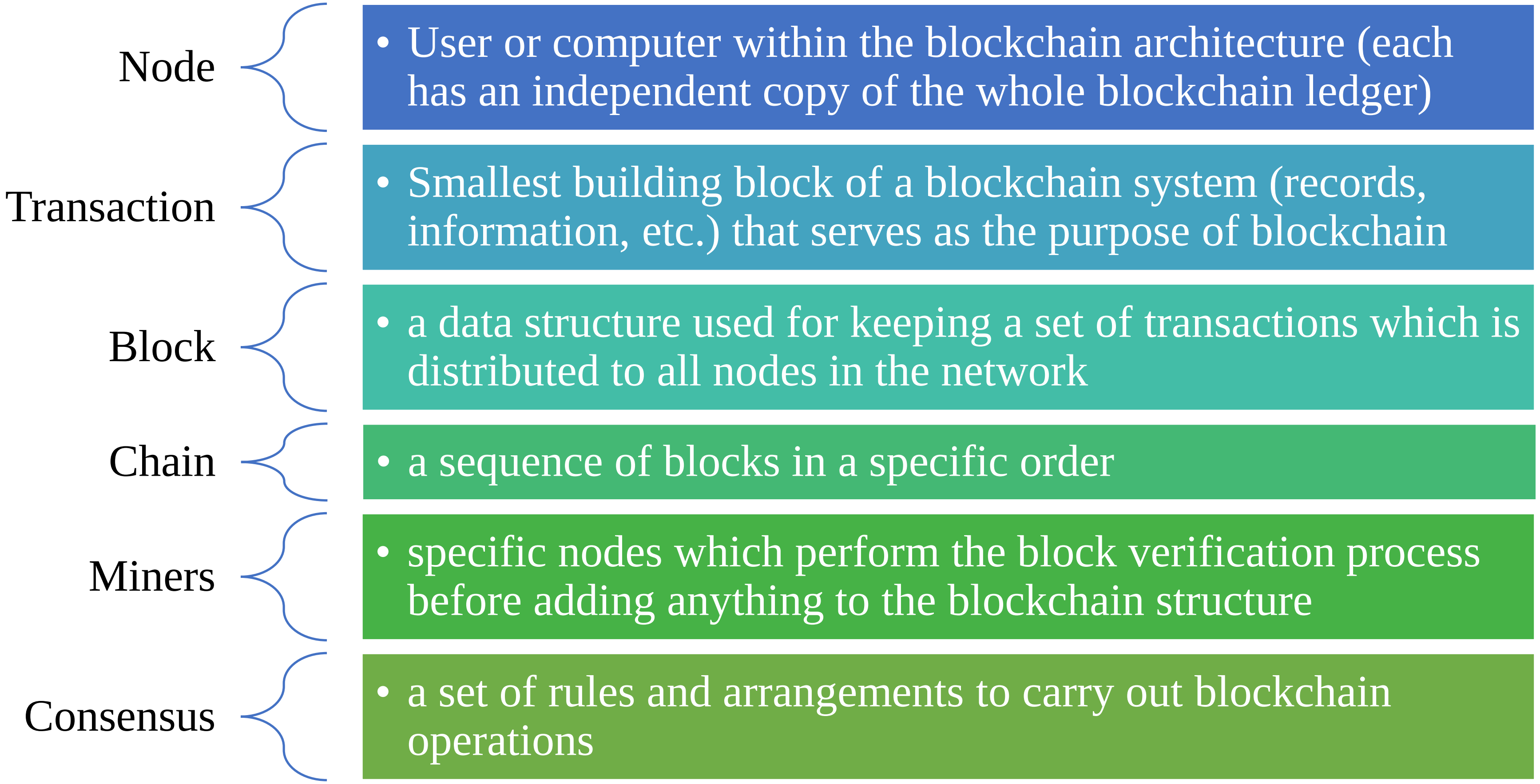
2. But one miner wants to alter a transaction in **block 74**.

3. He'd have to make his changes and redo all the computations for blocks 74–90 and do block 91. That's **18 blocks of expensive computing**.

4. What's worse, he'd have to do it all **before** everybody else in the Bitcoin network finished **just the one block (number 91)** that they're working on.

Click here for summary video

Core Blockchain component



Node

- User or computer within the blockchain architecture (each has an independent copy of the whole blockchain ledger)

Transaction

- Smallest building block of a blockchain system (records, information, etc.) that serves as the purpose of blockchain

Block

- a data structure used for keeping a set of transactions which is distributed to all nodes in the network

Chain

- a sequence of blocks in a specific order

Miners

- specific nodes which perform the block verification process before adding anything to the blockchain structure

Consensus

- a set of rules and arrangements to carry out blockchain operations

Types of Blockchain

Public

- A public blockchain architecture means that the data and access to the system is available to anyone who is willing to participate (e.g. Bitcoin, Ethereum, and Litecoin blockchain systems are public).

Private

- As opposed to public blockchain architecture, the private system is controlled only by users from a specific organization or authorized users who have an invitation for participation.

Consortium

- This blockchain structure can consist of a few organizations. In a consortium, procedures are set up and controlled by the preliminary assigned users.

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	Within one organization
Read permission	Public	Public or restricted	Public or restricted
Immutability level	Almost impossible to tamper	Could be tampered	Could be tampered
Efficiency (use of resources)	Low	High	High
Centralization	No	Partial	Yes
Consensus process	Permissionless	Needs permission	Needs permission

Ethereum

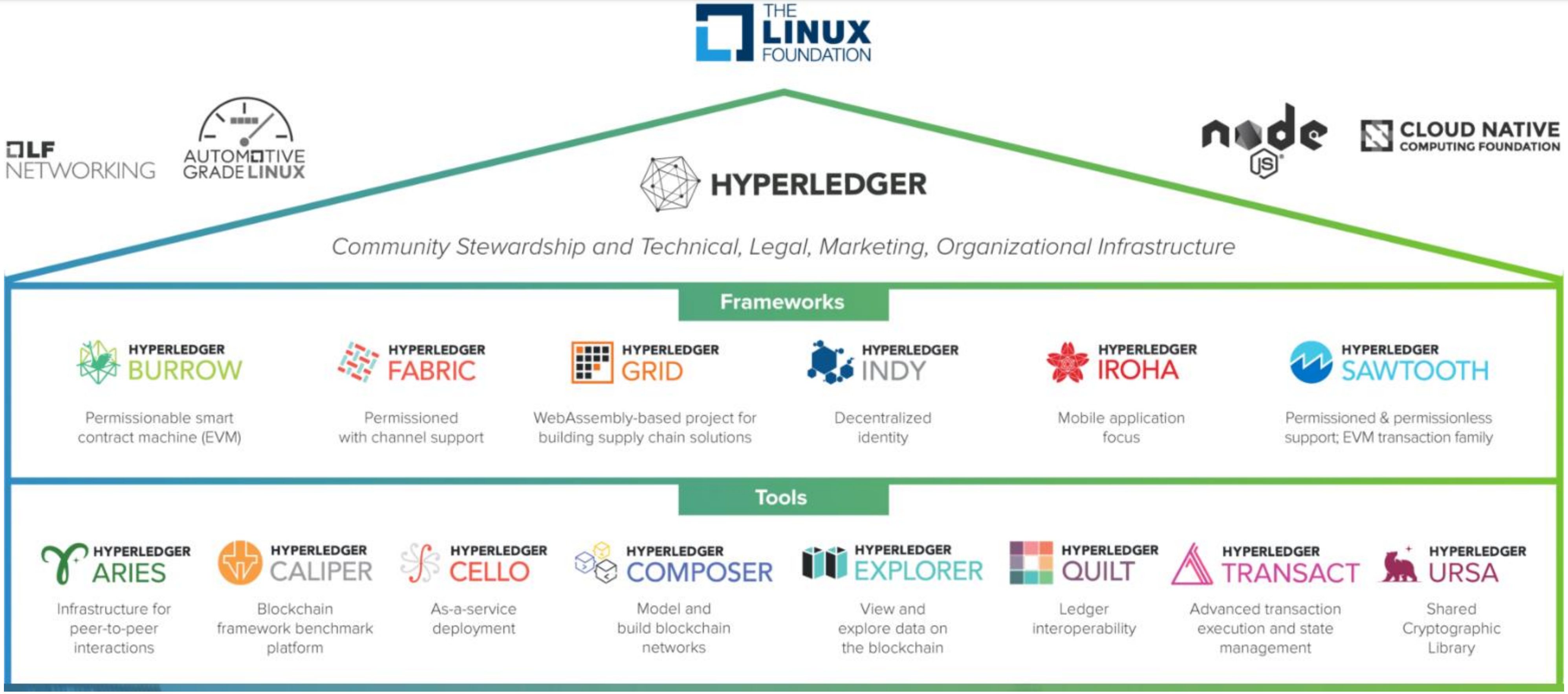
- Functions as a platform through which people can use tokens to create and run applications and create smart contracts
- Ethereum allows people to connect directly through powerful decentralized super computer
- Language- Solidity
- Currency- Ether
- Uses- POS

Smart Contracts

- A smart contract is an agreement or set of rules that govern a business transaction;
- It’s stored on the blockchain and is executed automatically as part of a transaction
- Their purpose is to provide security superior to traditional contract law while reducing the costs and delays associated with traditional contracts

Hyperledger

Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, Internet of Things, supply chains, manufacturing and Technology.


THE LINUX FOUNDATION
LF NETWORKING
AUTOMOTIVE GRADE LINUX
node JS
CLOUD NATIVE COMPUTING FOUNDATION
HYPERLEDGER
Community Stewardship and Technical, Legal, Marketing, Organizational Infrastructure
Frameworks
HYPERLEDGER BURROW
Permissionable smart contract machine (EVM)
HYPERLEDGER FABRIC
Permissioned with channel support
HYPERLEDGER GRID
WebAssembly-based project for building supply chain solutions
HYPERLEDGER INDY
Decentralized identity
HYPERLEDGER IROHA
Mobile application focus
HYPERLEDGER SAWTOOTH
Permissioned & permissionless support; EVM transaction family
Tools
HYPERLEDGER ARIES
Infrastructure for peer-to-peer interactions
HYPERLEDGER CALIPER
Blockchain framework benchmark platform
HYPERLEDGER CELLO
As-a-service deployment
HYPERLEDGER COMPOSER
Model and build blockchain networks
HYPERLEDGER EXPLORER
View and explore data on the blockchain
HYPERLEDGER QUILT
Ledger interoperability
HYPERLEDGER TRANSACT
Advanced transaction execution and state management
HYPERLEDGER URSA
Shared Cryptographic Library

Features/ Benefits Of using Blockchain

Information consensus Across Multiple Parties: Sophisticated cryptographic authorization and verification mechanisms enable trust in shared data across complex multi-party networks

Time Stamping: Timestamped events are agreed upon across multiple, possibly hostile or non-trusting entities

Security: Secure encryption and verification technologies enable untrusted participants to securely share trustable information with a third party.

Authenticity: Digital signatures provide authenticity and non-repudiation

B2B Ownership: End-to end asset lifecycles including ownership, custody and provenance can be tracked

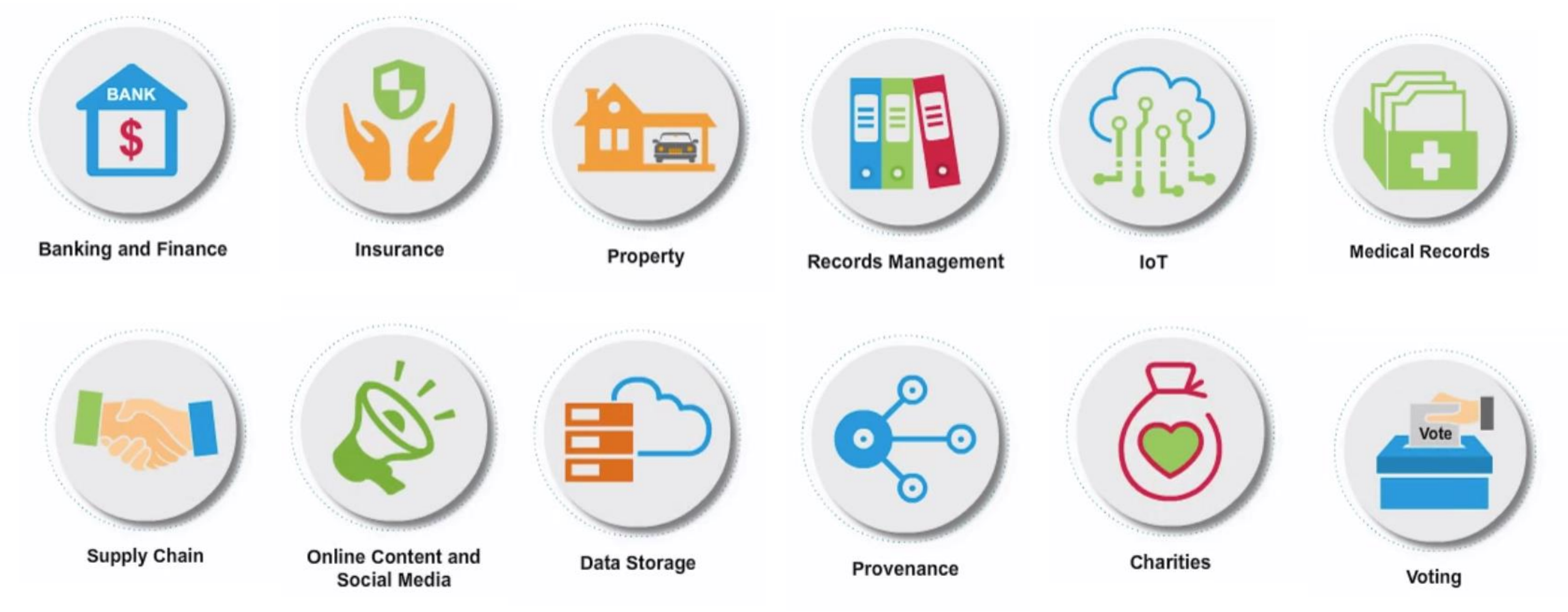
Data Loss Protection: Universal data loss becomes a lesser issue

Applications of Blockchain Technology

Cryptocurrencies

Blockchains for
everything else

Possible Verticals for blockchain technologies are practically endless, including



Thank You!

Ravi Kumar Mathur

ADG, NTIPRIT

adet.ict.ntiprit@gmail.com

String	Hash
ntiprit	6fef3bb73bc6c7b53c70d64ab1e6e5f8bb7278f68a0e7ad0d1e057ea6ede9af4
NTIPRIT	cafb724876f3b7d79ec22021c3f29d62e1cca70a0217625d51c1e0d34be17113
Ntiprit	578b5ebf1b0eaf70e72121fa158b3a3d58005730f9358e5aab074ada373c0bbf

☜