Module 1: Blockchain Foundations

Aron Kondoro & Anthony Kigombola

UDSM

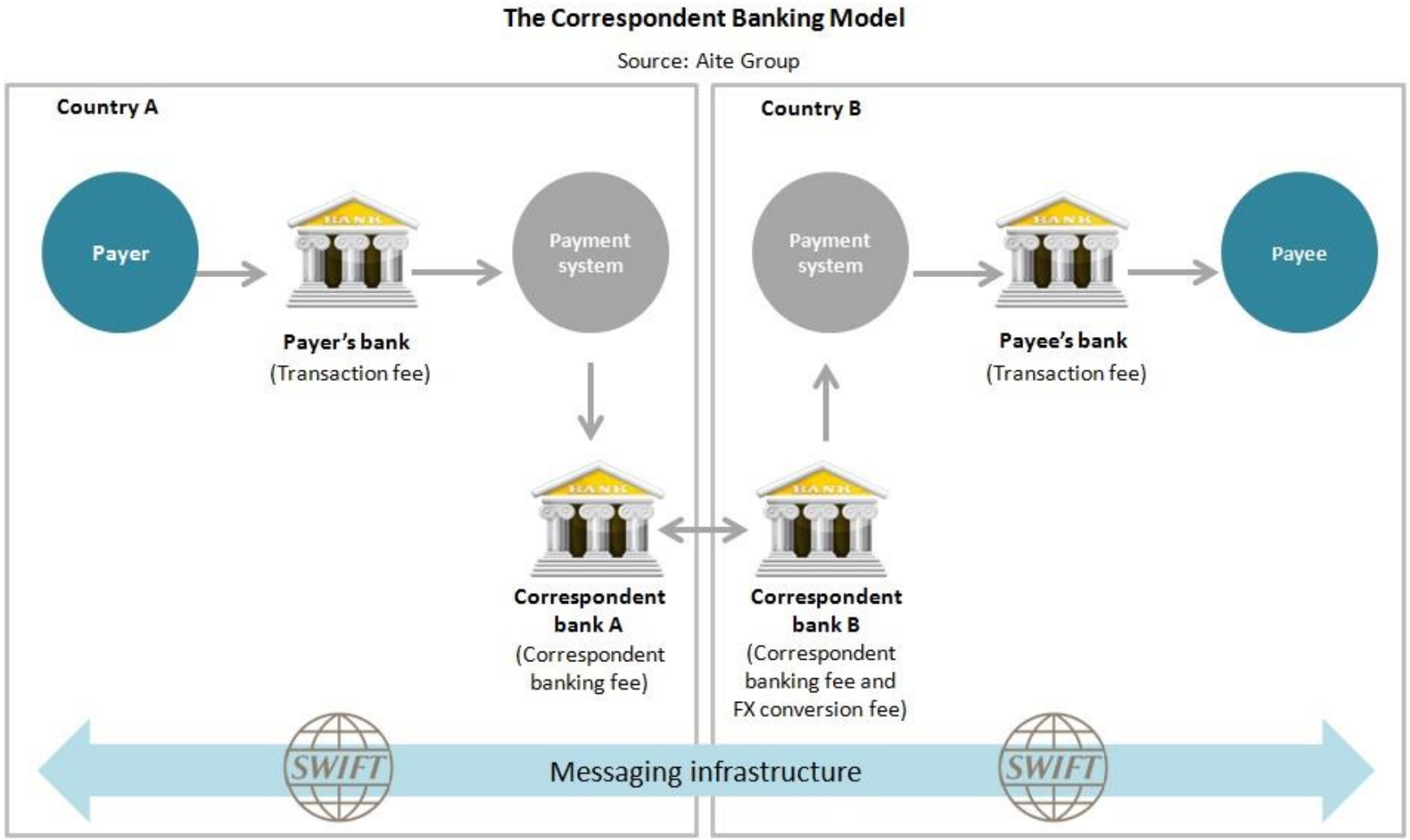
Contents

- Background
- What is a Blockchain?
- Blockchain Concepts
- Types of Blockchain
- Advantages of Blockchain
- Applications of Blockchain
- Hands-on: Setting up a Blockchain environment

Background

- Problems with centralized money/payment
  - Trust Based
  - Indirect
  - Inefficiencies
  - Transaction Fees
  - Privacy

Example: Cross Border Payment



Background

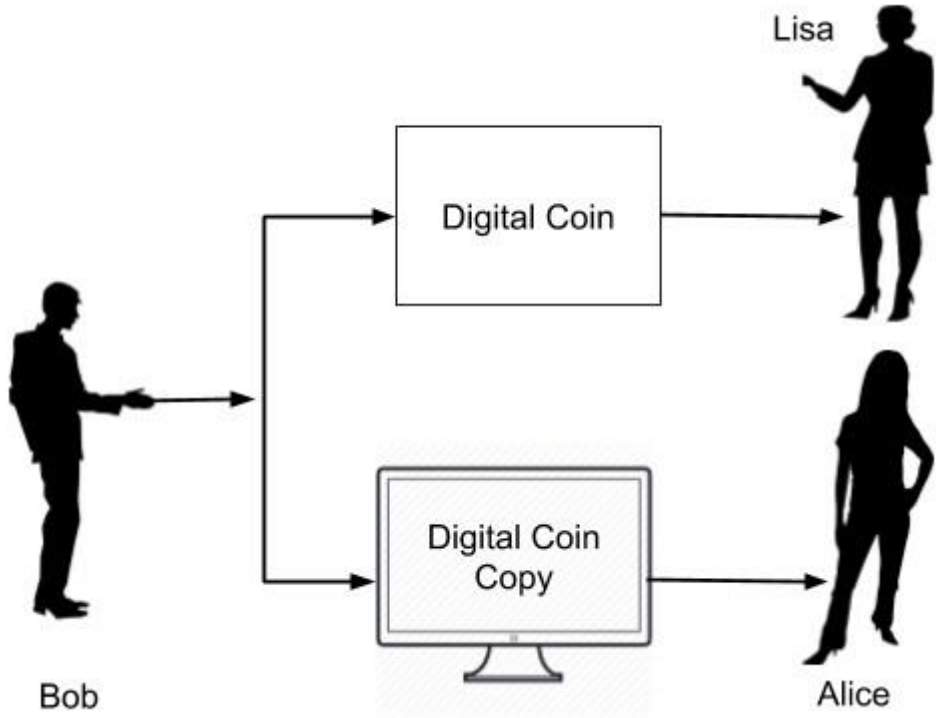
- What if this can be achieved in a decentralized way without middlemen?
- Would revolutionize payments
- This new system would need to
  - Serve as a medium of exchange to facilitate transactions
  - Store value (i.e., hold its value over time)
  - Contain a unit of account (i.e., a measure to use for value accounting or comparison)

Previous digital money attempts

- **1982 – Digi Cash**
  - One of the earliest electronic money solutions by David Chaum
  - Used cryptography to anonymize payments
- **1997 – HashCash**
  - Proof of work system originally for fighting spam and DDoS
  - Require the sender of an email to use a small amount of CPU power to solve a puzzle before sending the email out
- **1998 – B Money**
  - Anonymous, distributed electronic cash system by Wei Dai
  - Proof of Work, distributed ledger
- **2005 – Bit Gold**
  - By blockchain pioneer Nick Szaboa
  - When you solve puzzle it creates money

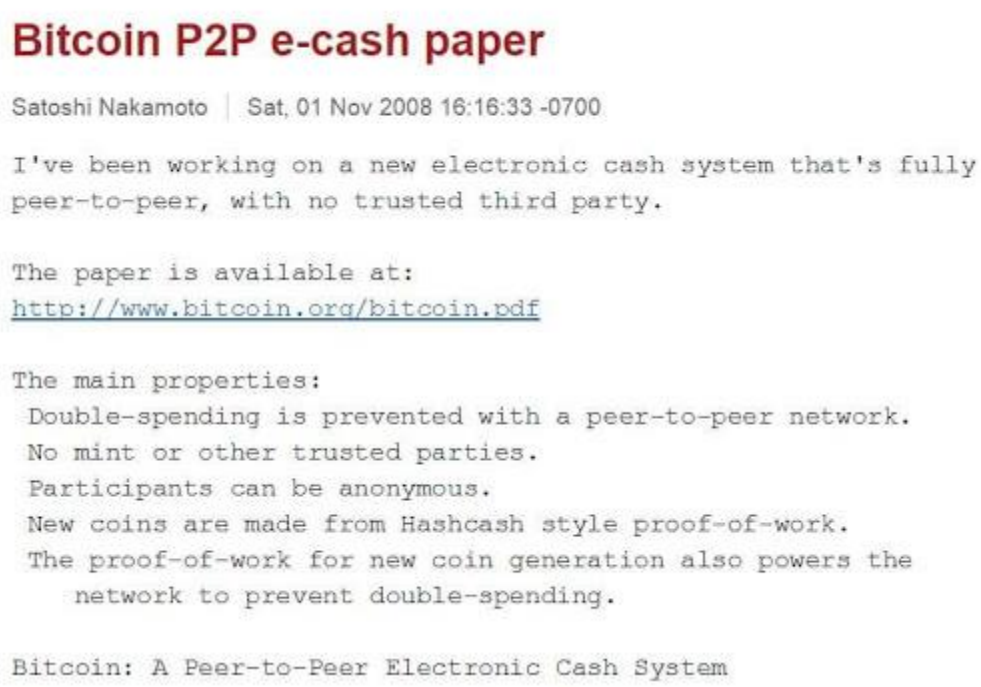
Double Spending Problem

- An instance of the problem of maintaining data consistency in distributed peer-to-peer systems
  - Digital data can be copied multiple times
  - Changes take time to propagate to all peers



Invention of Bitcoin

- Decentralized digital currency
- Invented in 2008 by “Satoshi Nakamoto”
- Solves the **double spending problem**
- Relies on **proof** instead of **trust**



Bitcoin P2P e-cash paper

Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

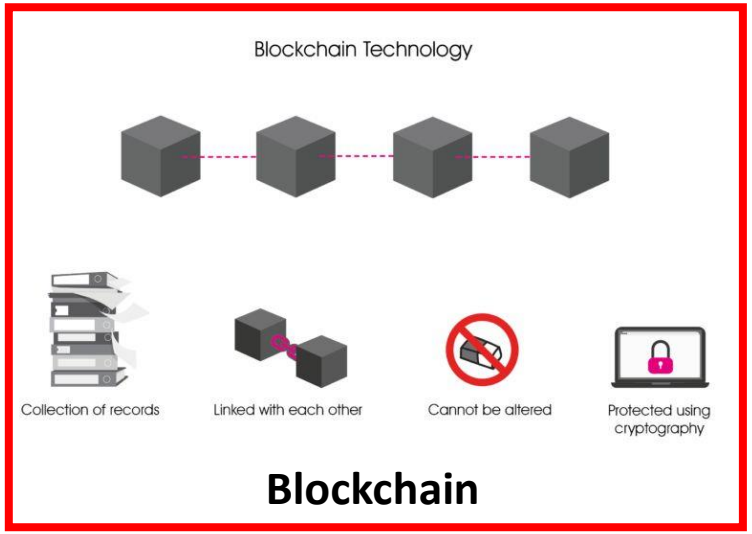
The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

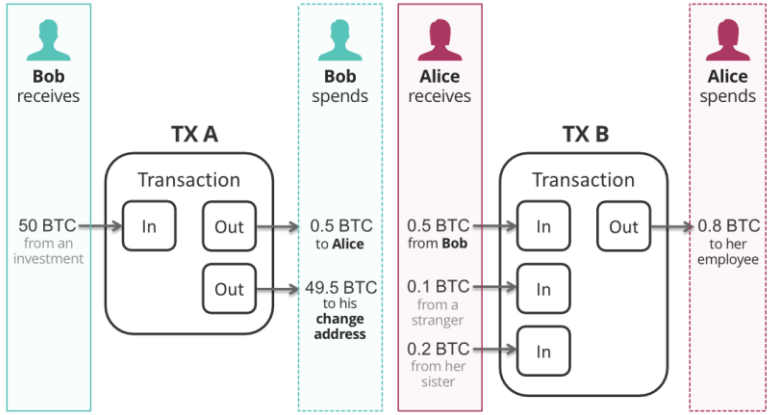
Bitcoin: A Peer-to-Peer Electronic Cash System

Bitcoin Design

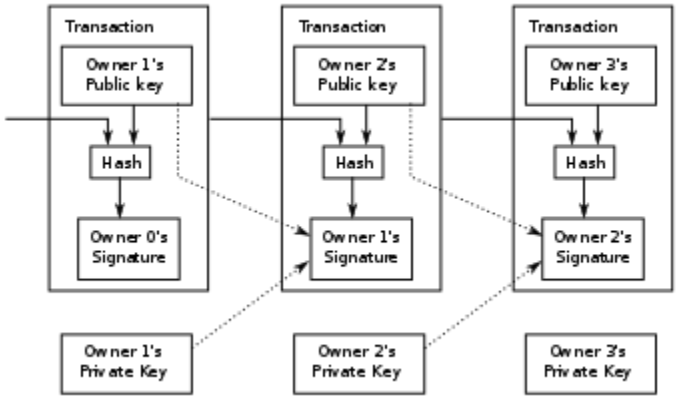
Currency/Token



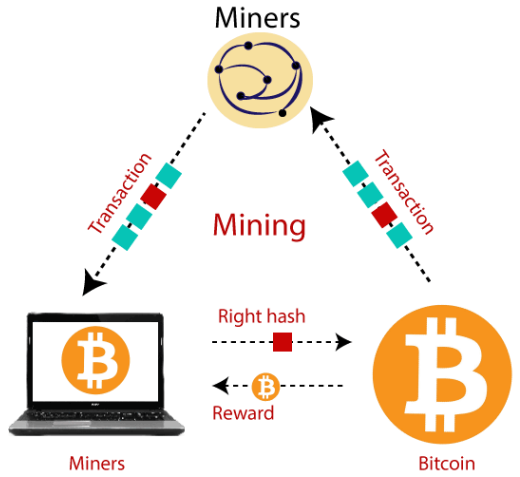
Blockchain



Transactions



Ownership



Mining

Core problem solved by Blockchain technology

Achieving and maintaining integrity in a purely distributed peer-to-peer system that consist of an unknown number of peers with unknown reliability and trustworthiness.

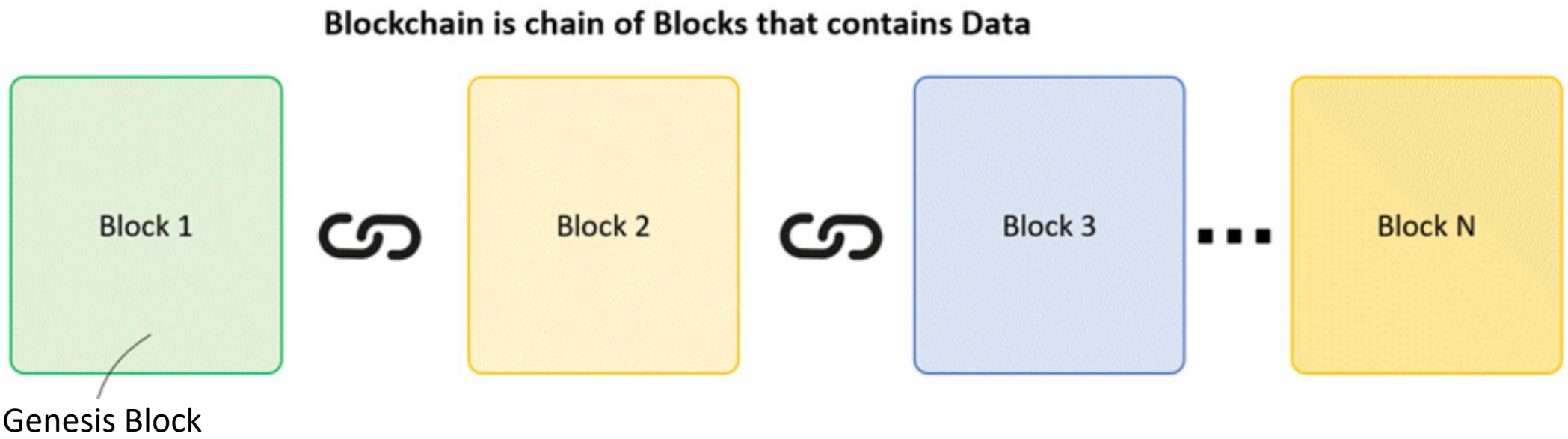
Blockchain vs Bitcoin

- Blockchain is not Bitcoin, but it is the technology behind Bitcoin
- Bitcoin is the digital token and blockchain is the ledger to keep track of who owns the digital tokens
- You can’t have Bitcoin without blockchain, but you can have blockchain without Bitcoin.

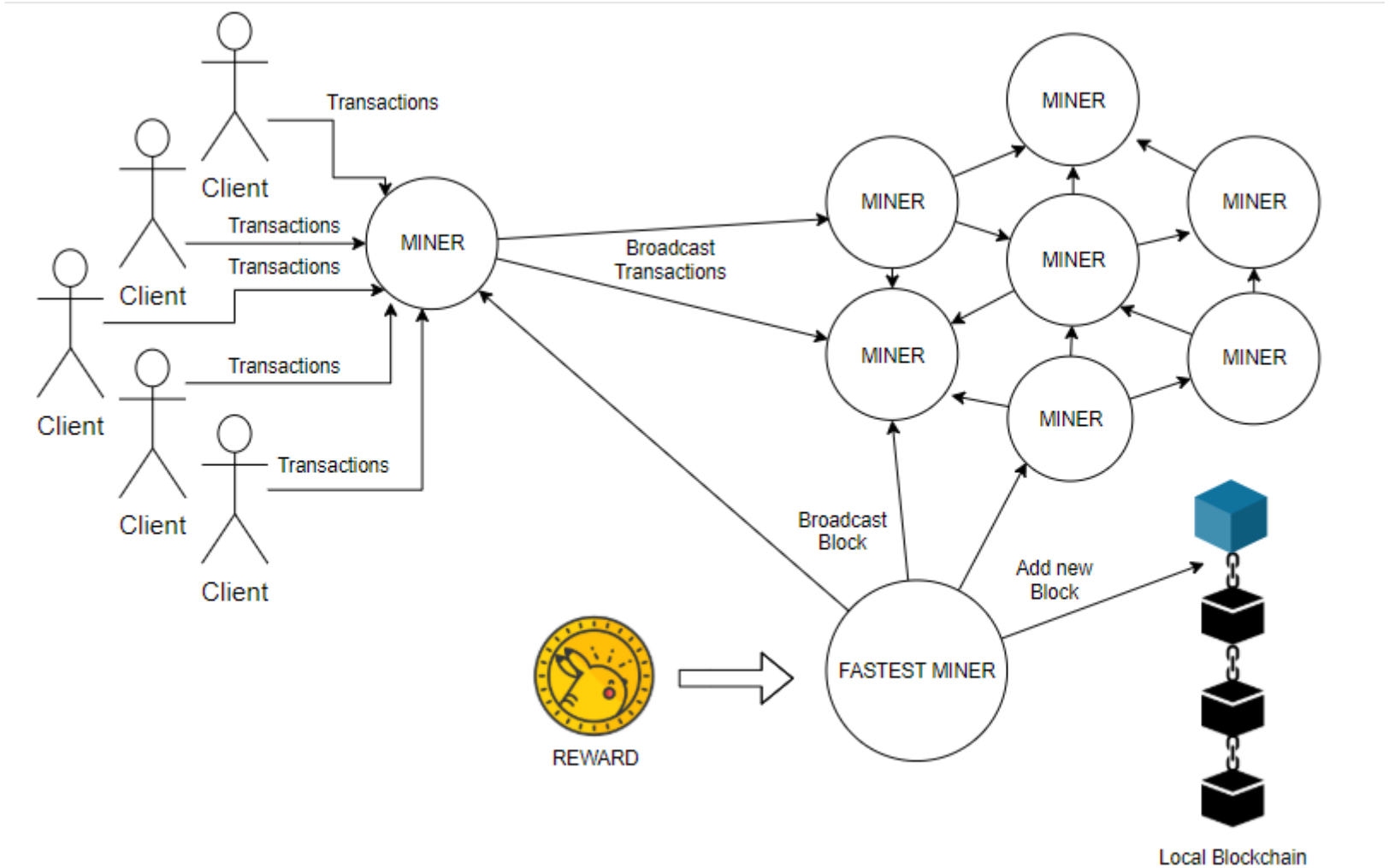
What is a blockchain?

- Data structure?
- Algorithm?
- Suite of technologies?
- A group of purely distributed peer-to-peer systems with a common application area

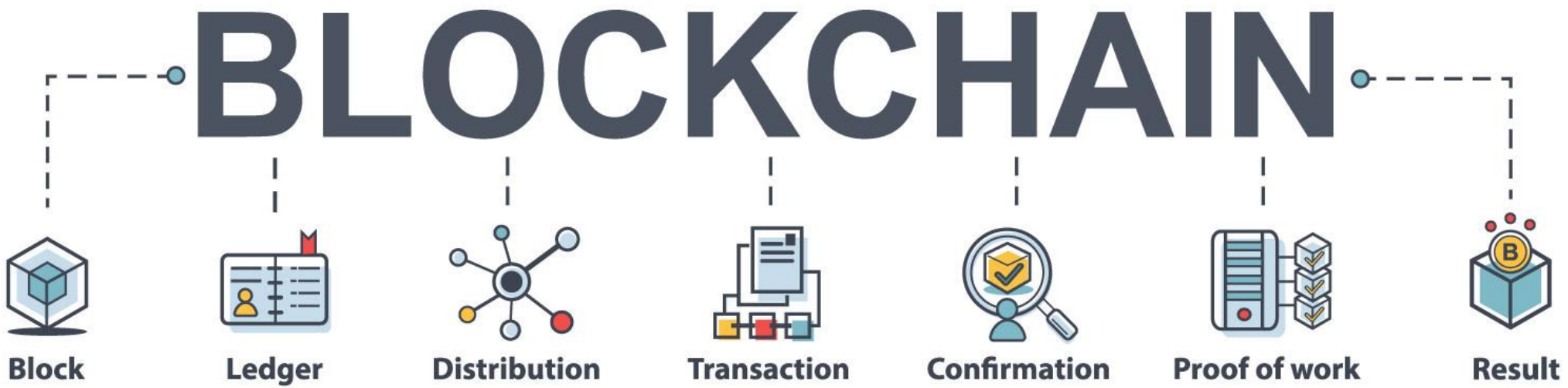
As a data structure



As an algorithm



As a suite of technologies



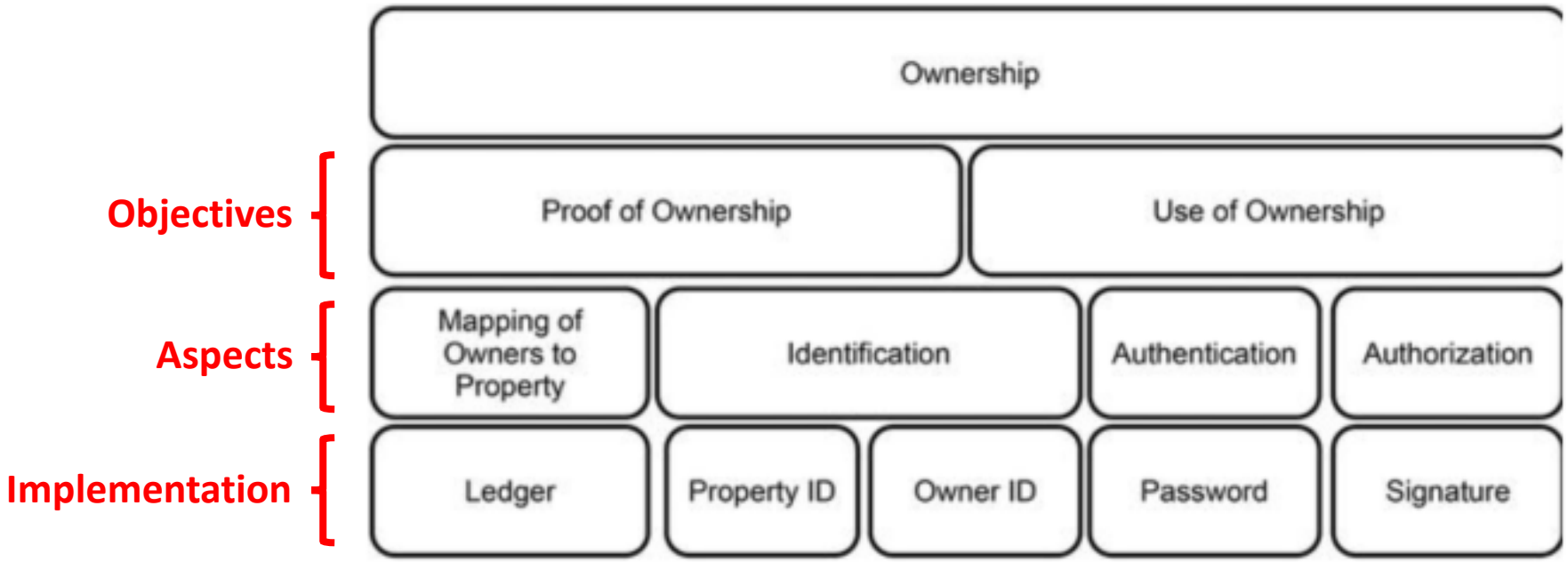
Definition of a blockchain

Purely distributed **peer-to-peer system of ledgers** that utilizes a software unit that consist of an **algorithm**, which negotiates the informational content of ordered and connected blocks of data together with cryptographic and security technologies in order to achieve and maintain its **integrity**.

Key Blockchain Elements

- **Goal**: Managing a distributed peer-to-peer systems of ledgers i.e. ownership of currency
- Distributed ledger i.e. public, immutable
- Consensus algorithm
- Currency/token

Blockchain Foundations

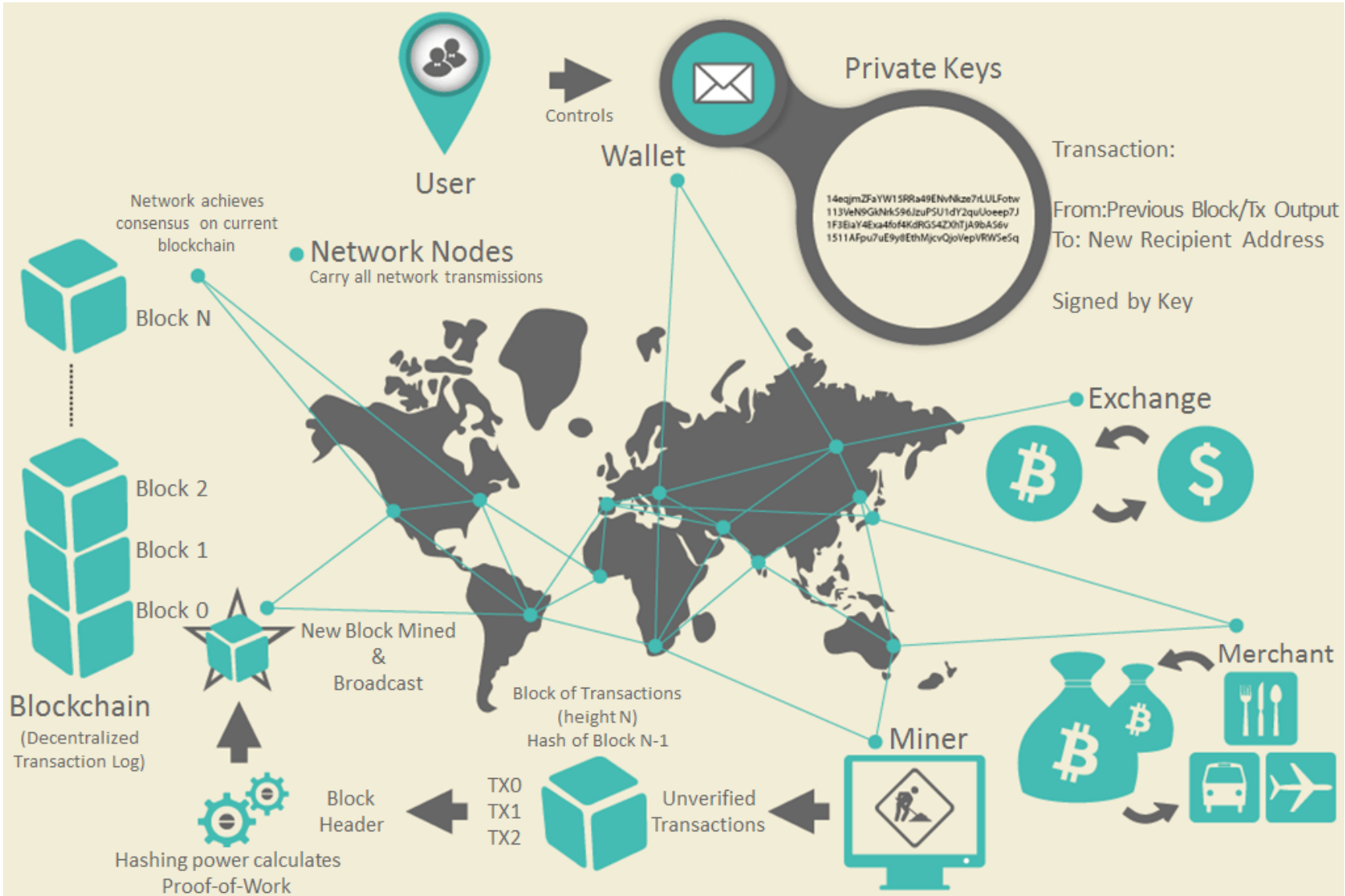


Blockchain Objectives

- Proof of Ownership => Blockchain as data structure
  - Ledger
- Change of ownership => Blockchain as algorithm
  - Consensus
  - Cryptography i.e. authentication, authorization

Assumptions

- Designing a piece of software for managing ownership in a purely distributed peer-to-peer system of ledgers that operates in completely open and untrustworthy environment
- Distributed peer-to-peer system
- Internet as the connecting network
- Nodes with unknown trustworthiness and reliability
- Management of ownership of a digital good


User
Controls
Wallet
Private Keys
14eqjmZFaYW15RRa49ENvNkze7rLULFotw
113VeN9GkNrkS96JzuPSU1dY2quUoeep7J
1F3EiaY4Exa4fof4KdRGS4ZXhTjA9bAS6v
1511AFpu7uE9y8EthMjcvQjoVepVRWSeSq
Transaction:
From:Previous Block/Tx Output
To: New Recipient Address
Signed by Key
Network achieves consensus on current blockchain
Network Nodes
Carry all network transmissions
Block N
Block 2
Block 1
Block 0
Blockchain
(Decentralized Transaction Log)
New Block Mined & Broadcast
Block of Transactions (height N) Hash of Block N-1
Exchange
Merchant
Miner
Block Header
TX0
TX1
TX2
Unverified Transactions
Hashing power calculates Proof-of-Work

Blockchain Tasks

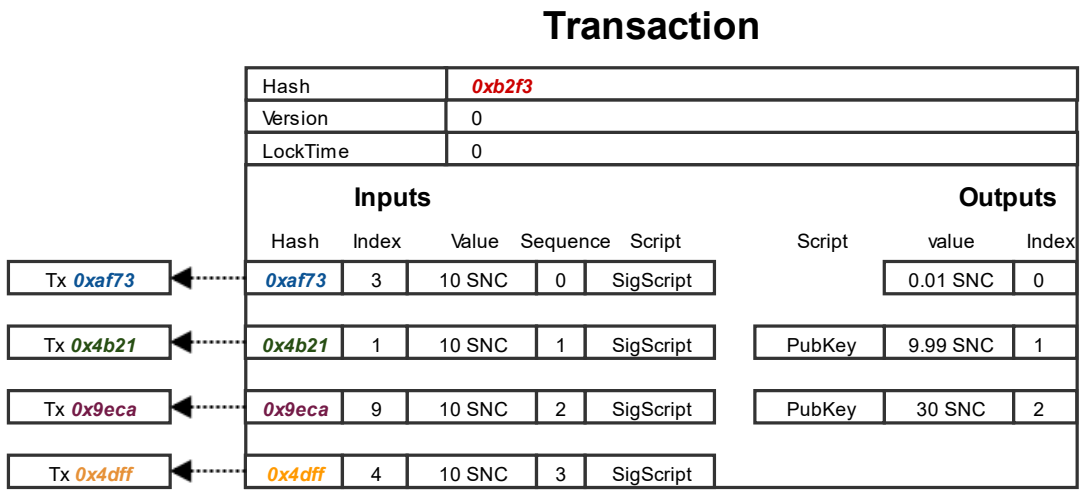
1. Ownership description
2. Ownership protection
3. Transaction data storage
4. Preparation of ledgers for distribution in an untrustworthy environment
5. Ledger distribution
6. Transaction addition to the ledgers
7. Decision of which ledgers to represent the truth

Ownership Description

- **Problem**: Proving ownership
- **Objective**: Tracking the transfer of ownership
- **Solution**: Transactions

Transaction

- Source identifier
- Destination identifier
- Amount of good
- Time
- Fee
- Proof of ownership



Transaction List

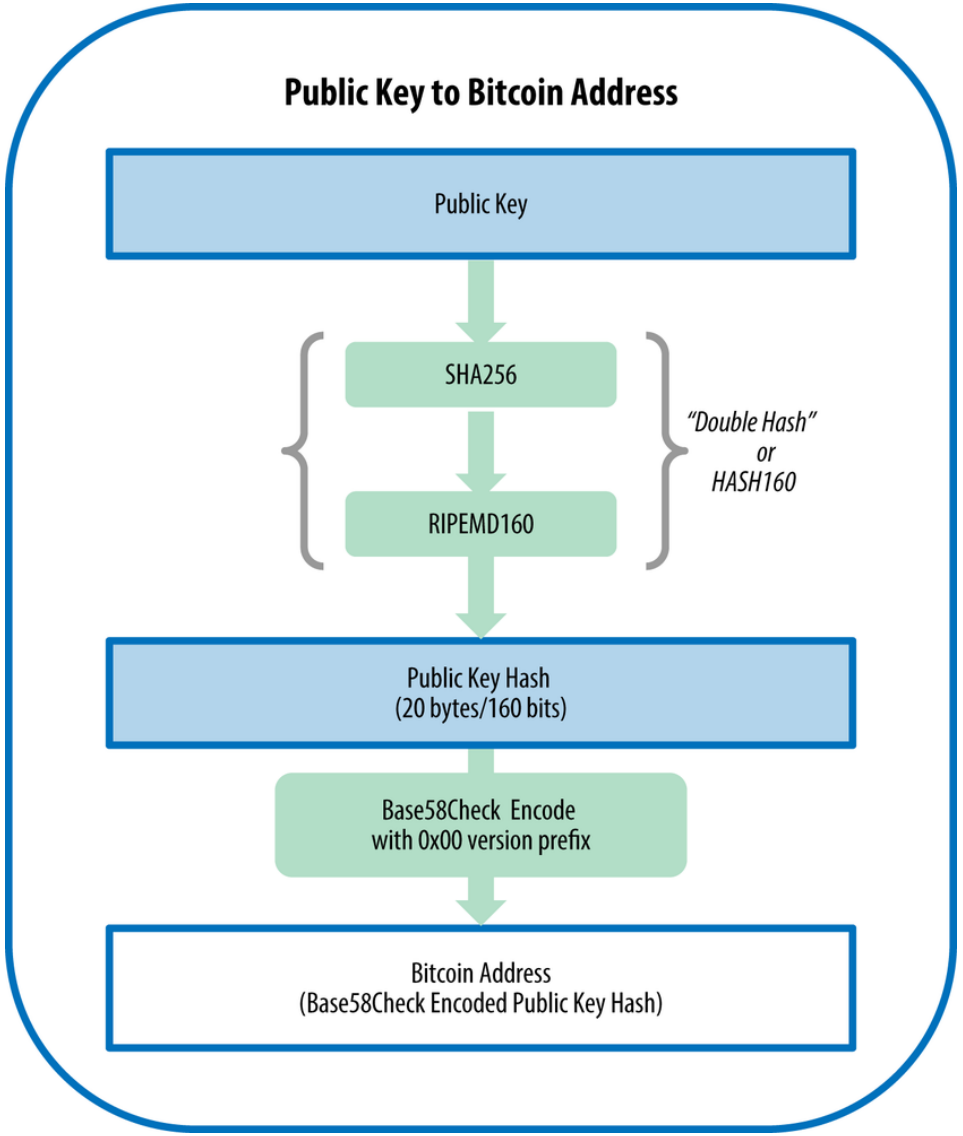
TxHash	Block	Age	From		To	Value	[TxFee]
0x2d055e4585ae2a...	5629306	16 secs ago	0x003e3655090890...		0x2bdc9191de5c1b...	0.004741591554641 Ether	0.000294
0xb4d37c791ff4cde...	5629306	16 secs ago	0x6c3b4faf413e0e4...		0xf14cb3acac7b230...	0.744767225 Ether	0.000294
0x9979410dcb5f4c...	5629306	16 secs ago	0x99bcd75abbac05...		0x2d42ee86390c59...	0.016294 Ether	0.000294
0x189c4d4aae09be...	5629306	16 secs ago	0x175cd602b2a1e7...		0xd39681bb0586fb...	0.01 Ether	0.000294
0xda0e9bbb11fb77...	5629306	16 secs ago	0x73a065367d111c...		0x01995786f14357...	0 Ether	0.00150007
0x6be498fafad9acb...	5629306	16 secs ago	0xa3eb206871124a...		0x8a91cac422e55e...	0.029594 Ether	0.000294

Protecting Ownership

- **Problem**: Anyone can change the ownership description
- **Objective**: Identify owners and property uniquely and to ensure that only the lawful owner can access his or her property
- **Solution**: Cryptography

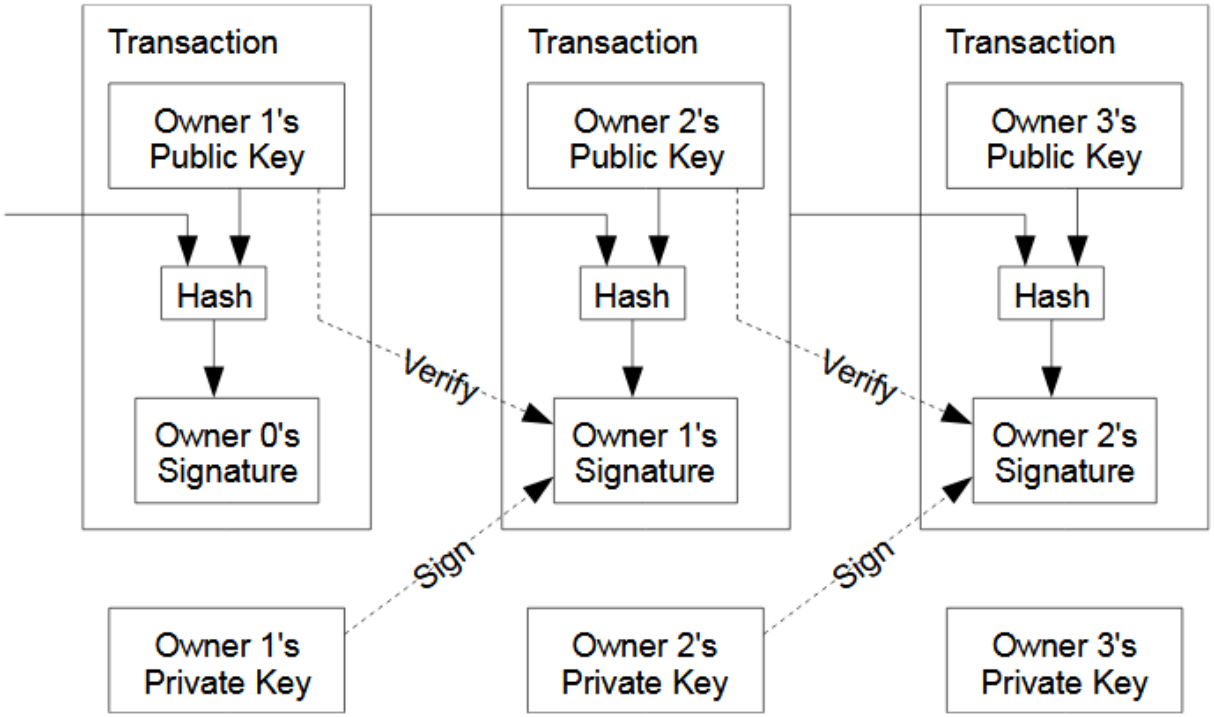
Asymmetric Cryptography

- Public keys as user accounts
  - Identify the author uniquely



Digital Signatures

- Authorize the transaction using signatures
- Only the owner can **sign** & execute transactions
- Peers need to **verify**

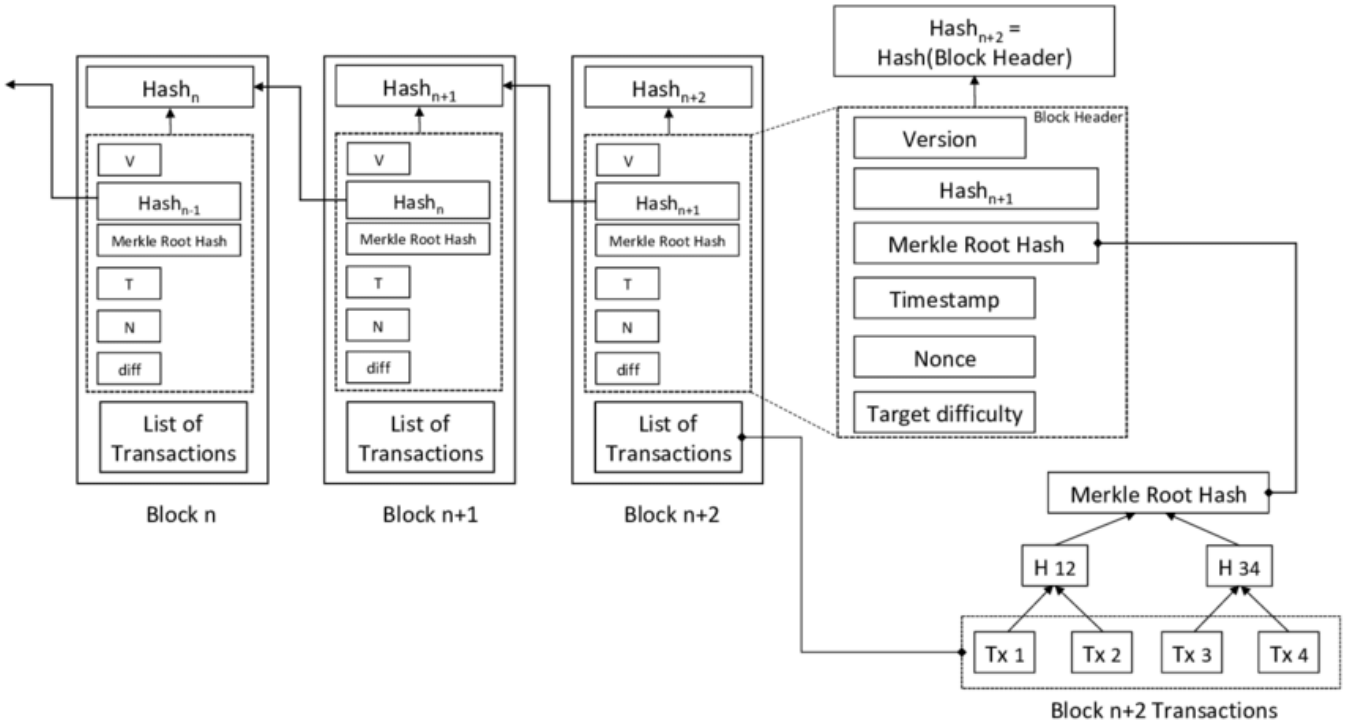


Transaction Data Storage

- **Problem**: Peers can manipulate order and history of transactions
- **Objective**: Maintain the whole history of transaction data in an orderly fashion
- **Solution**: Blockchain data structure

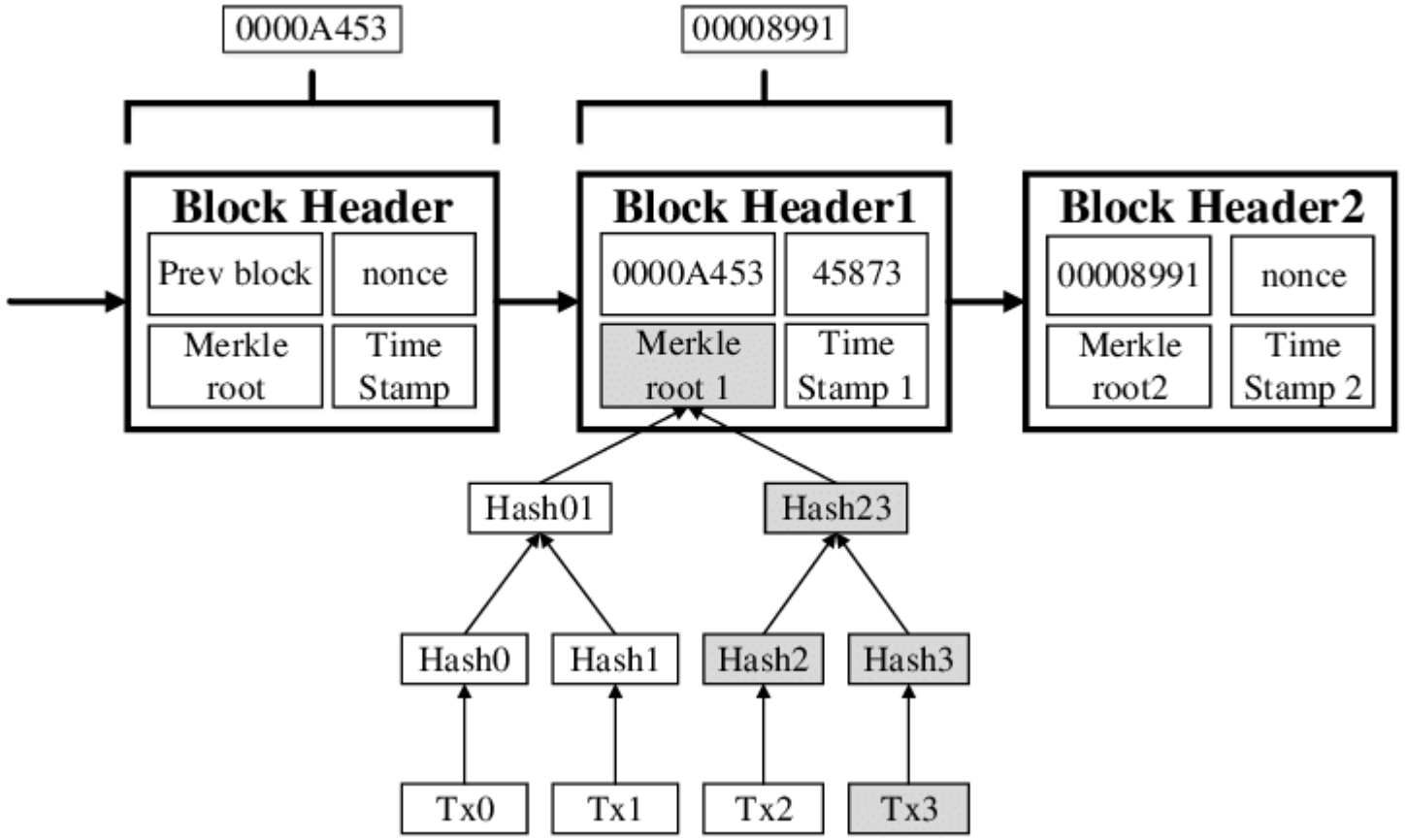
Blockchain Data Structure

- Ordered units called blocks
- Block: header + Merkle tree of transaction data
- Each block header references preceding header + application data

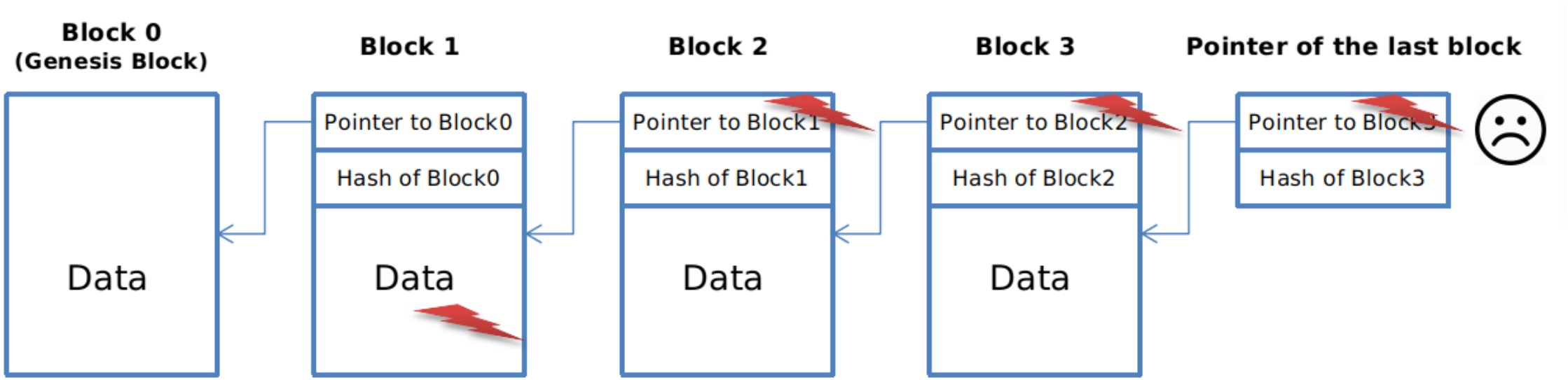


Blockchain data structure is tamper-proof

- Can detect
  - Changing tx data
  - Changing hash pointer in Merkle tree
  - Replacing tx
  - Changing Merkle root
  - Changing block header



Blockchain can detect changes

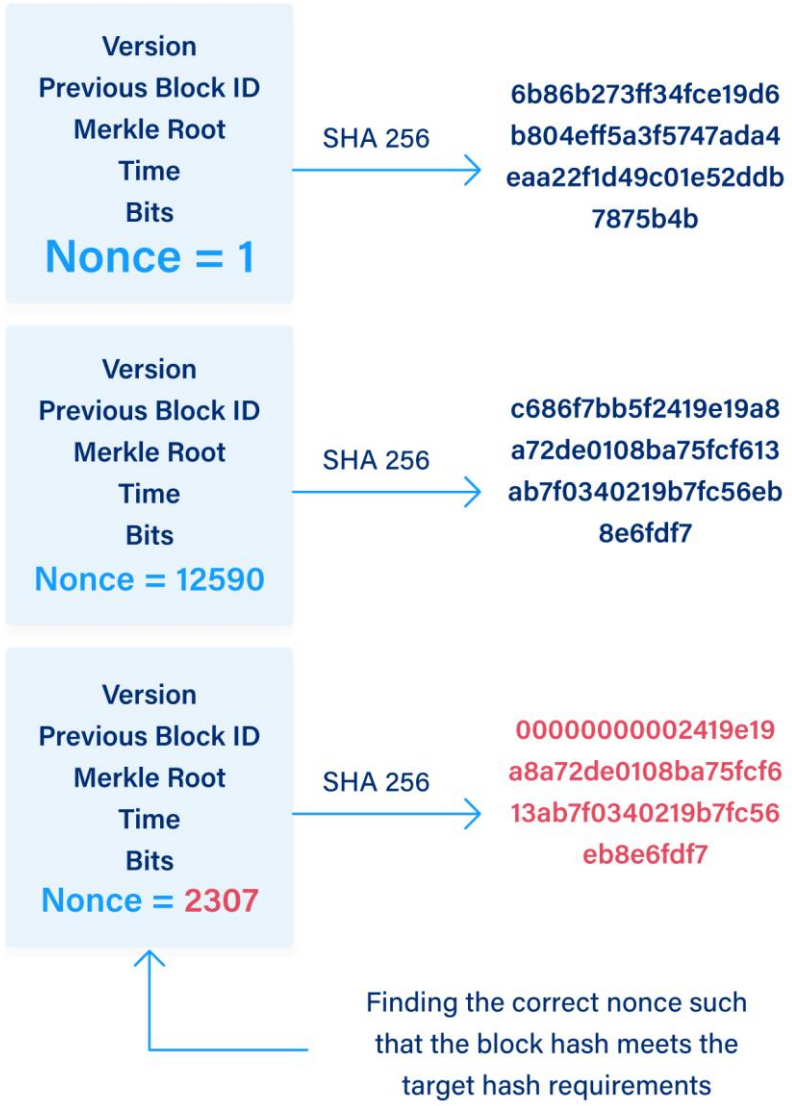


Preparation of ledgers for distribution

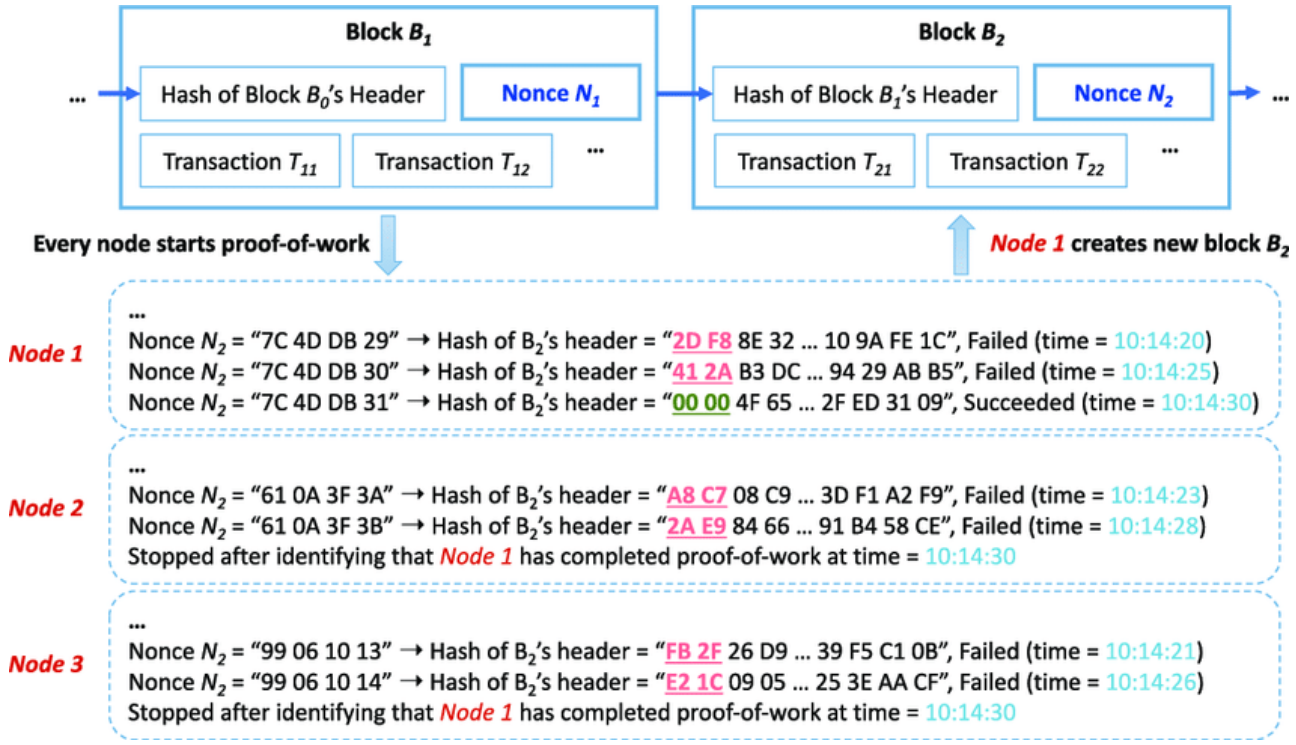
- **Problem**: Copies of ledger reside in untrustworthy nodes and network
- **Objective**: Prevent the ledger from being forged or manipulated
- **Solution**: Blockchain data structure that is append only

Proof of Work

- Make manipulation stand out
- Manipulations requiring huge changes
- Make changing transaction history prohibitively expensive



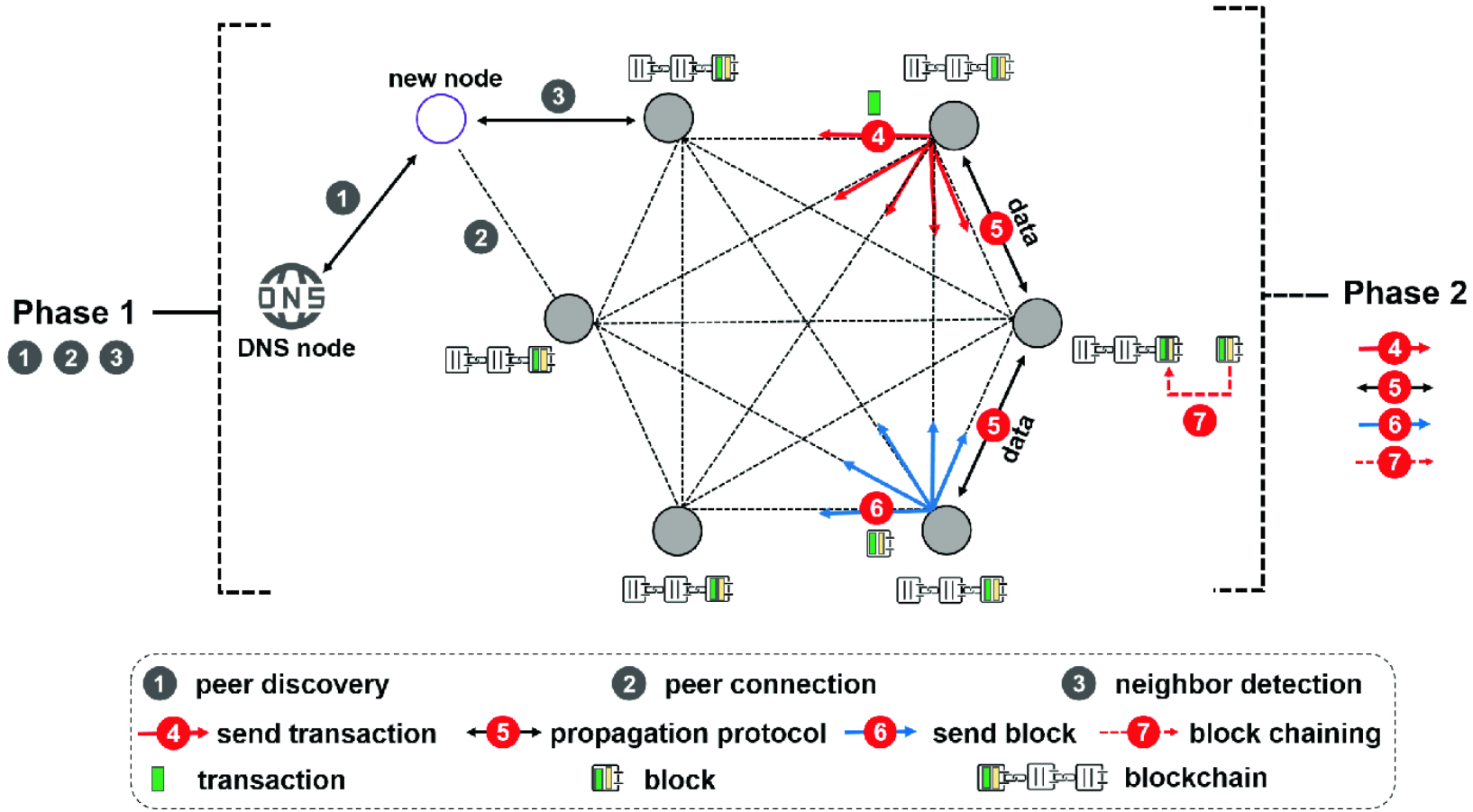
Mining


Block B_1
Hash of Block B_0's Header
Nonce N_1
Transaction T_{11}
Transaction T_{12}
Block B_2
Hash of Block B_1's Header
Nonce N_2
Transaction T_{21}
Transaction T_{22}
Every node starts proof-of-work
Node 1 creates new block B_2
Node 1
Nonce N_2 = "7C 4D DB 29" → Hash of B_2's header = "2D F8 8E 32 ... 10 9A FE 1C", Failed (time = 10:14:20)
Nonce N_2 = "7C 4D DB 30" → Hash of B_2's header = "41 2A B3 DC ... 94 29 AB B5", Failed (time = 10:14:25)
Nonce N_2 = "7C 4D DB 31" → Hash of B_2's header = "00 00 4F 65 ... 2F ED 31 09", Succeeded (time = 10:14:30)
Node 2
Nonce N_2 = "61 0A 3F 3A" → Hash of B_2's header = "A8 C7 08 C9 ... 3D F1 A2 F9", Failed (time = 10:14:23)
Nonce N_2 = "61 0A 3F 3B" → Hash of B_2's header = "2A E9 84 66 ... 91 B4 58 CE", Failed (time = 10:14:28)
Stopped after identifying that Node 1 has completed proof-of-work at time = 10:14:30
Node 3
Nonce N_2 = "99 06 10 13" → Hash of B_2's header = "FB 2F 26 D9 ... 39 F5 C1 0B", Failed (time = 10:14:21)
Nonce N_2 = "99 06 10 14" → Hash of B_2's header = "E2 1C 09 05 ... 25 3E AA CF", Failed (time = 10:14:26)
Stopped after identifying that Node 1 has completed proof-of-work at time = 10:14:30

Ledger Distribution

- **Problem**: No central point of coordination
- **Objective**: Ensure that peers get informed about transactions and are able to maintain their own history of transaction data
- **Solution**: Peer to peer communication

Peer to Peer Communication



Peer to Peer Communication

- Solution
  - Messages sent in a gossip style
  - Filtering of duplicates using hashes
  - Using timestamp for ordering
- Implementation
  - Keeping existing connections alive
    - ping/pong messages
  - Establishing new connections
  - Distributing new information
    - New transactions
    - New blocks

Distributing New Information

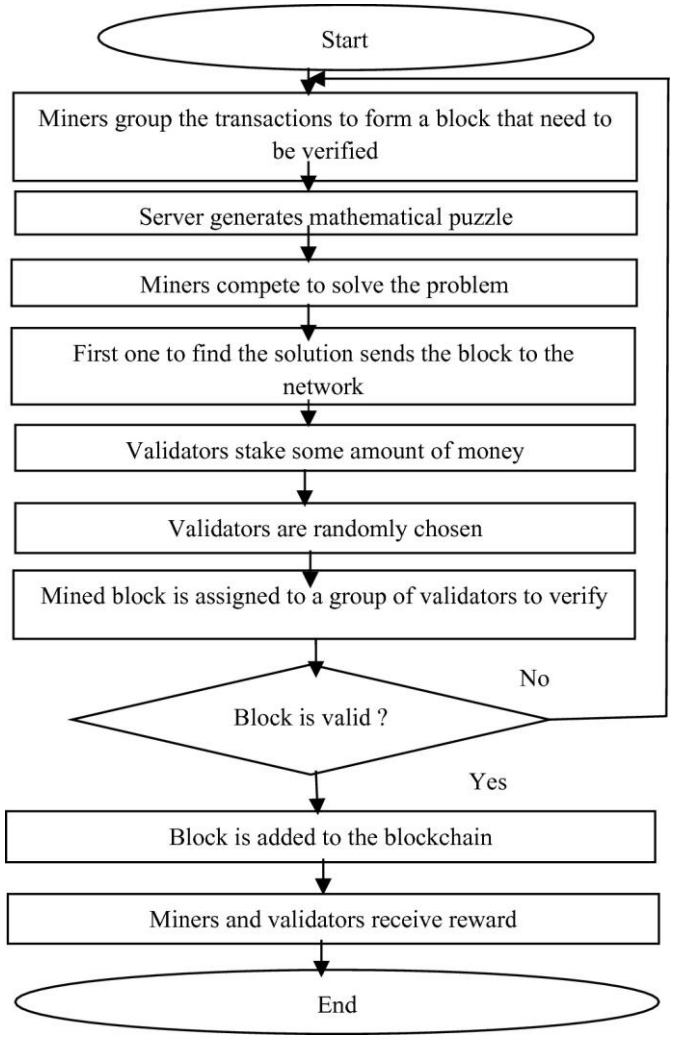
- In an ongoing fashion
  - New blocks and tx data
- As an update
  - When a node re-joins
- As part of the on-boarding process
  - When a new node joins

Adding transactions to the ledger

- **Problem**: Any node including untrustworthy ones can add to the ledger
- **Goal**: Ensuring only valid and authorized transactions are added
- **Solution**: Blockchain-algorithm

Blockchain Algorithm

- Incentivise peers to supervise and validate transactions
  - Any node can supervise
  - Nodes are rewarded for adding valid and authorized transactions
- Building Blocks
  - Validation rules
  - Reward
  - Punishment
  - Competition
  - Peer control

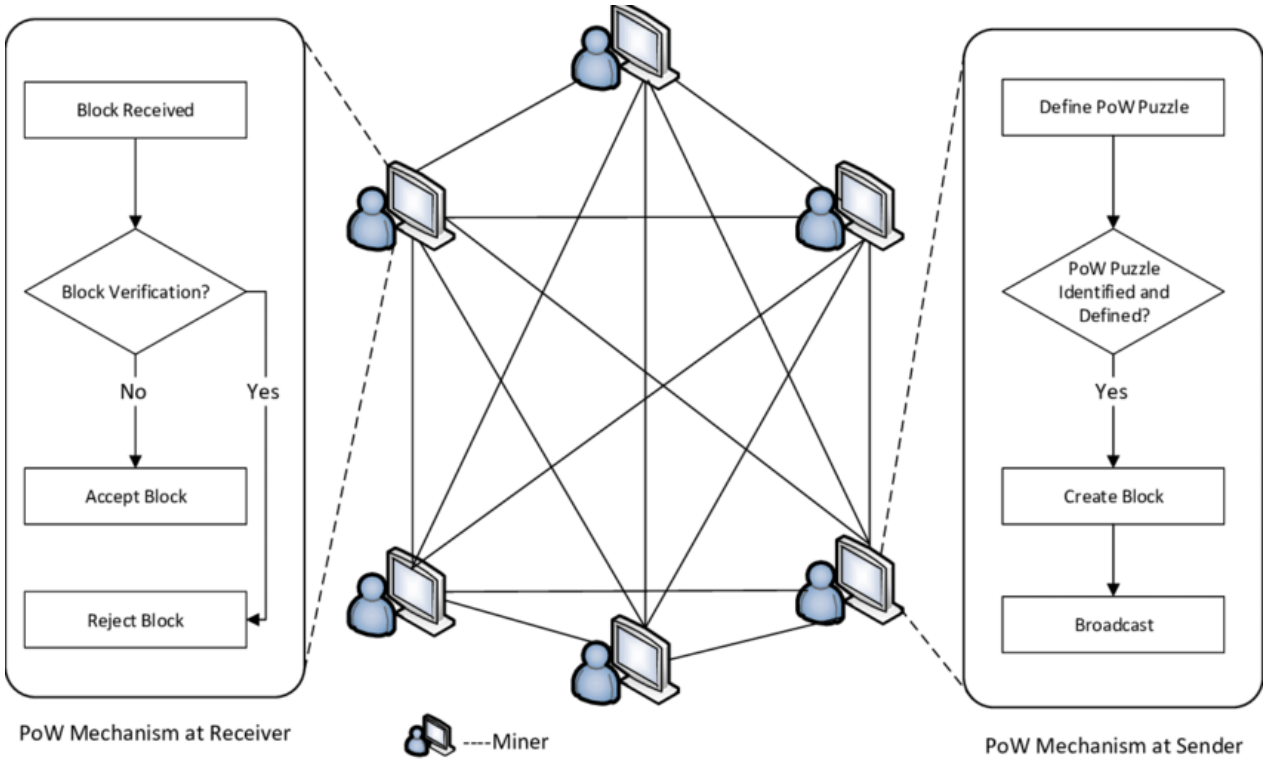


Deciding the source of truth

- **Problem**: Different peers may have different versions of the history
- **Goal**: Find a way to prevent emergence of different transaction histories or a way to decide which history is valid
- **Solution**: A mechanism where the majority wins

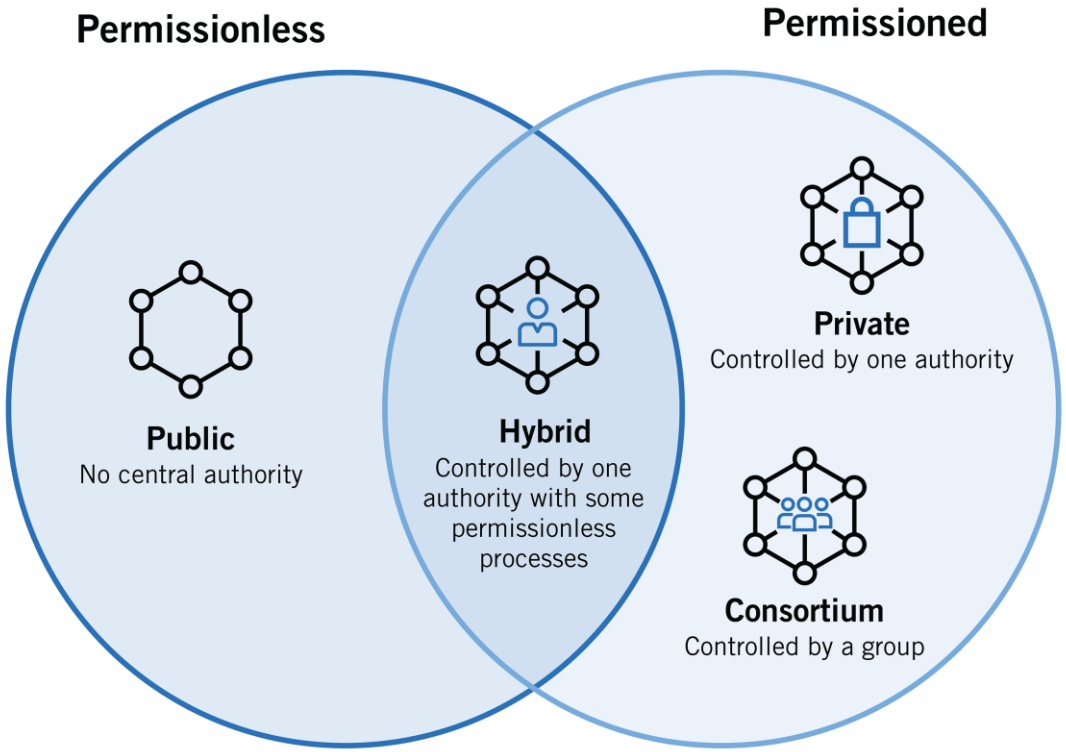
Distributed Consensus

- Longest chain criterion
- Heaviest chain criterion



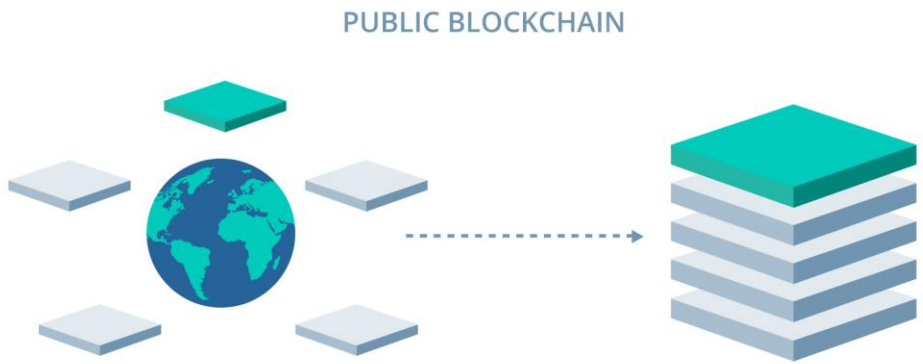
Types of Blockchain

1. Public (permissionless)
2. Private (permissioned)
3. Consortium



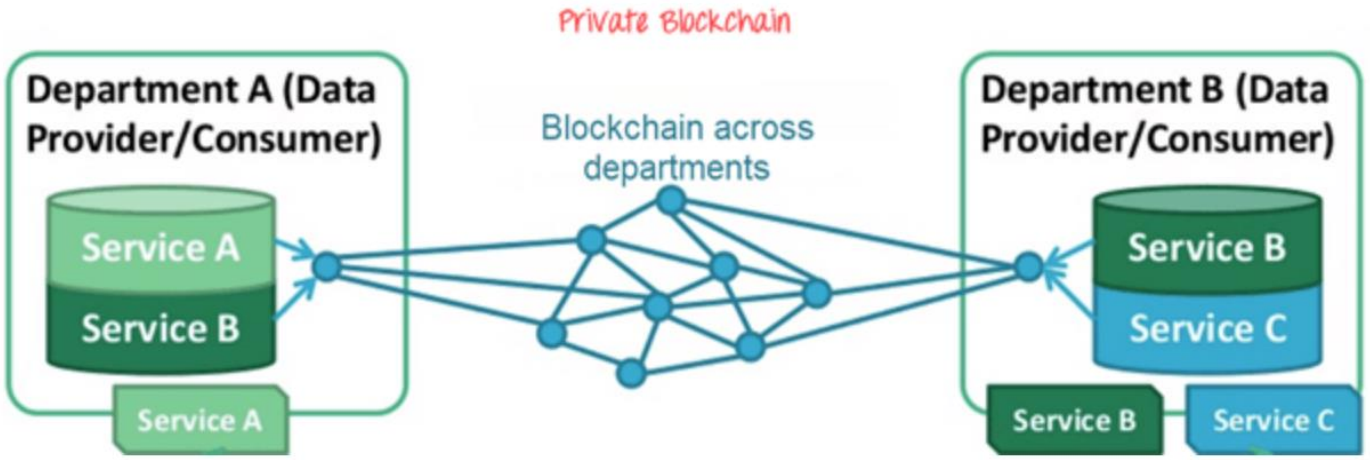
Public Blockchain

- Ledger are visible to everyone on the Internet
- Anyone can verify and add a block of transactions to the blockchain
- Need incentives to participate
- Disadvantages: Heavy power consumption, privacy
- Cryptocurrencies like Bitcoin, Ethereum etc



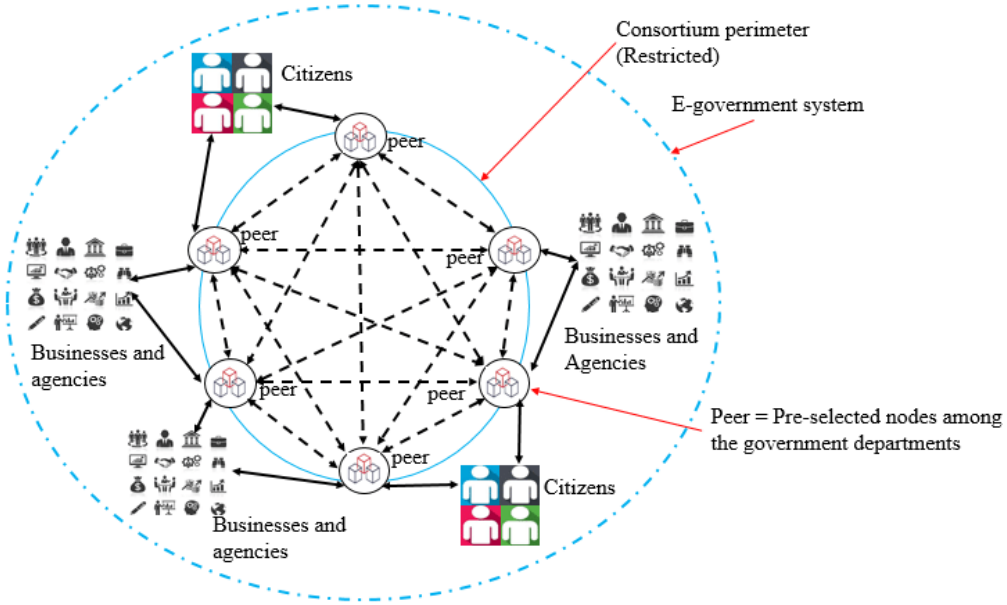
Private Blockchain

- Within a single organization
- Only specific people of the organization can verify and add transaction blocks
- Everyone on the internet is generally allowed to view
- Ripple, hyperledger



Consortium Blockchain

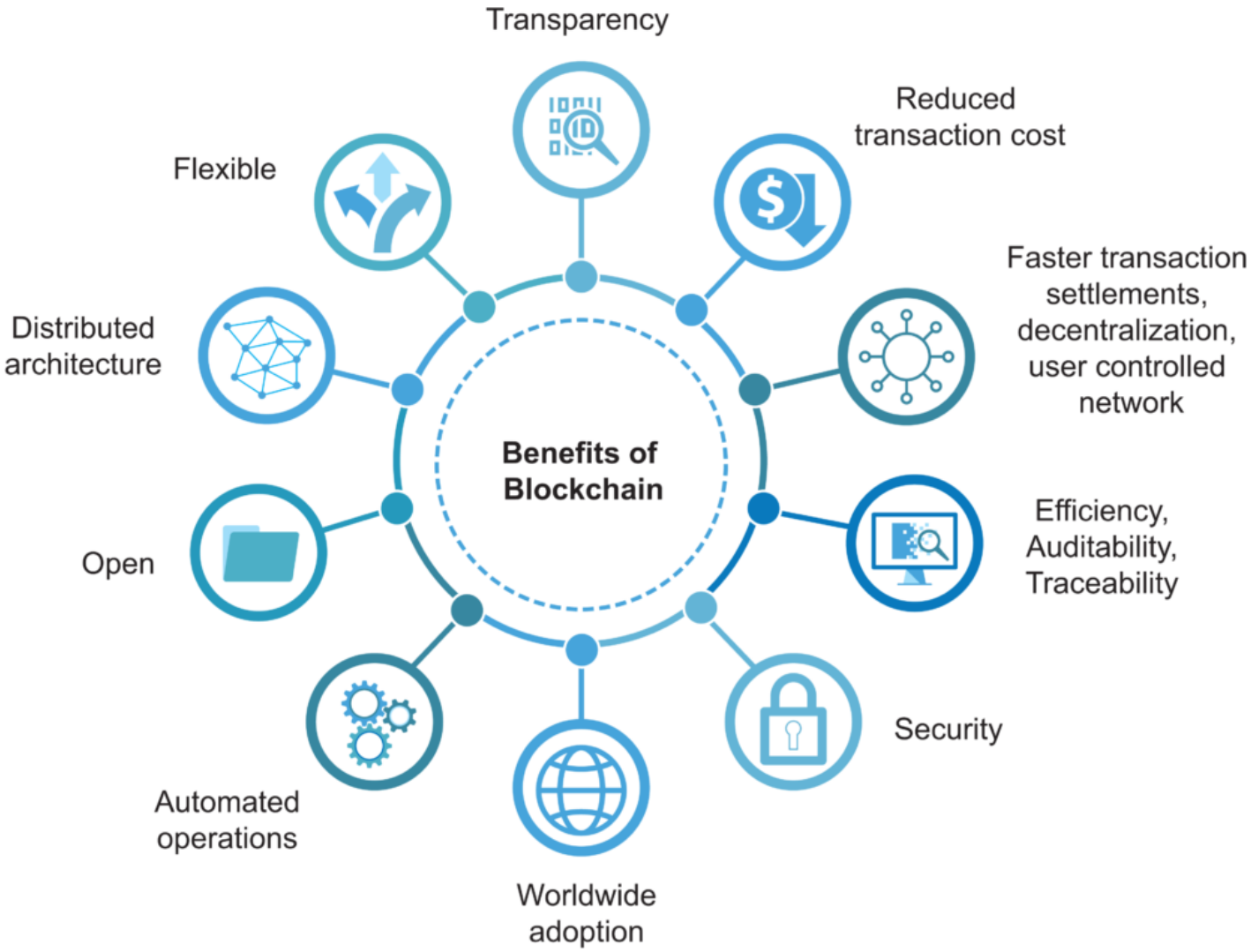
- Only a group of organizations can verify and add transactions
- The ledger can be open or restricted to select groups
- Controlled by pre-authorized nodes
- Ripple, hyperledger



Blockchain Versions

- Blockchain 1.0: Currency
  - Financial transactions based on Blockchain technology
  - Bitcoin is the most prominent example in this segment.
- Blockchain 2.0: Smart Contracts
  - Small computer programs that “live” in the blockchain.
  - Execute automatically, and check conditions defined earlier like facilitation, verification or enforcement
  - Replace traditional contracts
- Blockchain 3.0: Dapps
  - Backend code running on a decentralized peer-to-peer network
  - Frontend and user interfaces written in any language

Advantages of Blockchain



Applications of Blockchain

- Tracking of any kind of asset
- Infallible data management and identity tracking
- Trust less land registries
- Cross-border money transfers

50+ BLOCKCHAIN
REAL WORLD USES CASES

GOVERNMENT
Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government

essentia.one

IDENTIFICATION
Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by **Uport**.

uport

MOBILE PAYMENTS
The blockchain ledger that **Ripple** uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.

ripple

INSURANCE
A smart contract-based blockchain is being used by Insurer **American International Group Inc** as a means of saving costs and increasing transparency.

AIG

ENDANGERED SPECIES PROTECTION
The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.

CARBON OFFSETS
IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.

IBM HYPERLEDGER

ENTERPRISE
Ethereum's blockchain can be accessed as a cloud-based service courtesy of **Microsoft Azure.**

Microsoft Azure

BORDER CONTROL
Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.

essentia.one

SUPPLY CHAINS
IBM and **Walmart** have partnered in China to create a blockchain project that will monitor food safety.

IBM Walmart

HEALTHCARE
A number of healthcare systems that store data on the blockchain have been pioneered including **MedRec.**

MEDREC

SHIPPING
Shipping is a natural fit for blockchain, and **Maersk** have been trialling a blockchainbased project within the maritime logistics industry.

MÆRSK

REAL ESTATE
Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by **Propy**.

PROPY

ENERGY
Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.

essentia.one

LAND REGISTRY
Land registry titles are now being stored on the blockchain in Georgia in a project developed by the **National Agency of Public Registry**.

NATIONAL AGENCY of PUBLIC REGISTRY

COMPUTATION
Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.

DIGITAL CURRENCY GROUP

ADVERTISING
New York Interactive Advertising Exchange has been experimen- ting with blockchain as a means of providing an ads marketplace for publishers.

NYIAX

BORDER CONTROL
Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.

essentia.one

JOURNALISM
Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as **Civil** has shown.

CIVIL

WASTE MANAGEMENT
Waltonchain is using **RFID** technology to store waste management data on the blockchain in China.

ENERGY
Food importation is another industry where blockchain is proving its worth, with **Louis Dreyfus Co** trialling a soybean importation operation using this technology.

LDC. Louis Dreyfus Company

DIAMONDS
The **De Beers Group** is using blockchain to track the importation and sale of diamonds.

De Beers GROUP OF COMPANIES

FINE ART
By storing **certificates** of authenticity on the blockchain, it's possible to dramatically reduce art forgeries, as one blockchain project is proving.

NATIONAL SECURITY
For the past two years, the **US Department of Homeland Security** has been using blockchain to record and safely store data captured from its security cameras.

TOURISM
In a bid to boost its tourism economy, **Hawaii** is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.

TAXATION
In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by **Miaocai Network**.

ENERGY
Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.

CNE COMISIÓN NACIONAL DE ENERGÍA

RAILWAYS
Russian rail operator **Novotrans** is storing inventory data on a blockchain pertaining to repair requests and rolling stock

ГРУЗОВАЯ КОМПАНИЯ НОВОТРАНС

ENTERPRISE
Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by **Alphabet Inc**

Google Alphabet

MUSIC
Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.

arbit

FISHING
Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.

THE INTERNET OF BLOCKCHAIN FOUNDATION

Consortium Of 61 Japanese Banks To Release Instant Mobile Payment App Powered By Ripple

The 61-bank Japanese Bank Consortium has partnered with Ripple to release an instant domestic money transferring app this fall.

Using blockchain to make land registry more reliable in India

2 comments | 1 shares

Estimated reading time: 5 minutes

Kiva launches Africa's first national decentralized ID system with Hyperledger Indy

Kiva

- Global non-profit founded in 2005 in San Francisco
- Uses crowd-funding to finance micro-loans
- Has facilitated $1.5+ billion in loans in 90+ countries
- Loan repayment rate of 95.7%

Goals

- Make it easy for the unbanked to get digital ID
- Let the informal sector share credit history with banks
- Help the unbanked open bank accounts and get loans

Approach

1. Solve a two-sided problem: ID and data
2. Find the gaps in the process
3. Work with stakeholders to build a network
4. Choose a platform for fast, cheap and secure ID exchange
5. Involve local communities in a test project

Results

- Africa's first decentralized national ID system went live in 2019
- After Sierra Leone, will roll out to other countries
- eKYC can verify a customer ID in 5 seconds
- System requires only a thumbprint and national ID number

The National Bank of Cambodia boosts financial inclusion with Hyperledger Iroha

Bakong Project

- Sponsored by the National Bank of Cambodia, the country's central bank
- Co-developed with Soramitsu, the main contributor to Hyperledger Iroha
- The first retail payments system in the world using blockchain technology
- The first large-scale quasi-central bank digital currency (CBDC) in production

Goals

- To reach the unbanked population, especially in rural areas
- To promote use of the national currency instead of U.S. dollars
- To reduce the liquidity and compliance burdens on payment service providers that are not banks
- To modernize retail payments to deliver better services at lower cost

Approach

1. Acknowledge the country's banking challenges
2. Investigate distributed ledger technologies
3. Choose the best platform to use: Hyperledger Iroha
4. Design a modern, digital payments system
5. Build in strong security from the start
6. Test with a pilot program in the real world

Results

- During a pilot, a network of 16 banks supported 10,000+ users
- Retail throughput up to 2,000 transactions per second
- Interbank transfers improved from twice-daily batches to 5 seconds or less
- System to expand across the country in 2020

Blockchain Limitations

- **Higher costs**: Nodes seek higher rewards for completing Transactions in a business which work on the principle of Supply and Demand
- **Slower transactions**: Nodes prioritize transactions with higher rewards, backlogs of transactions build up
- **Smaller ledger**: It not possible to synchronize the full copy of the Blockchain (>300GB), potentially which can affect immutability, consensus, etc.
- **Scaling issues**: Max 7 transactions per second
- **Risk of error**: There is always a risk of error, as long as the human factor is involved. In case a blockchain serves as a database, all the incoming data has to be of high quality. However, human involvement can quickly resolve the error.
- **Wasteful**: Every node that runs the blockchain has to maintain consensus across the blockchain. This offers very low downtime and makes data stored on the blockchain forever unchangeable. However, all this is wasteful, because each node repeats a task to reach consensus.

Hands-on: Setting up a Blockchain Environment