Chain Verse

Understanding Blockchain Architecture & Web3

(Session - 1 : Theory)

Mrs. Lifna C S

Assistant Professor

Department of Computer Engineering

Vivekanand Education Society's Institute of Technology, Mumbai

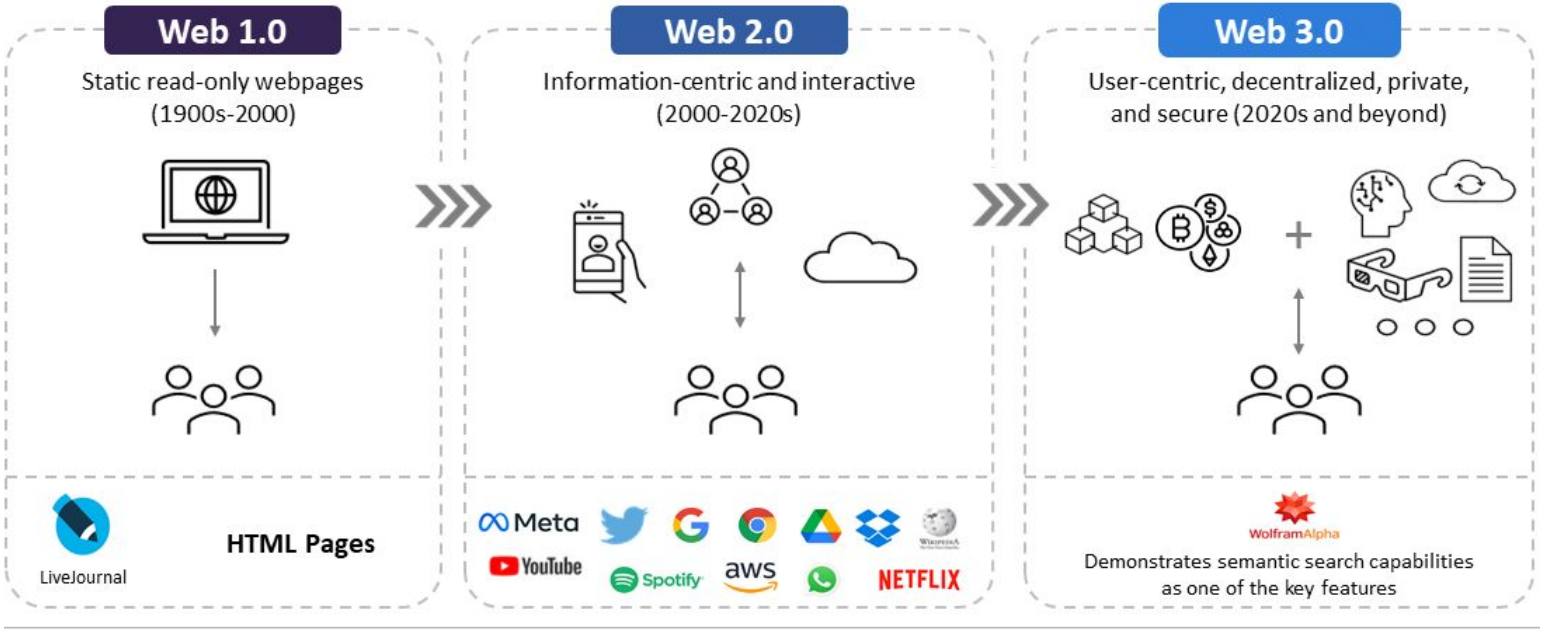
Dated : 26th Feb 2026

Topics to be covered

1. **Introduction to Blockchain**
2. Blockchain Fundamentals
3. Cryptocurrency Basics
4. Introduction to Solidity Programming

Evolution of Web

Web 3.0 is the evolution of the internet towards user-centric intelligent services



1. Introduction to Blockchain

Why to learn Blockchain ?

Current Scenario

- Internet is owned by Technical Giants
- Huge Transaction fees by 3rd Parties
- Time to complete Transactions..
- Ownership for Content Creators
- Lack of Transparency

Blockchain Offers …

- Decentralized with P2P Network
- Trust in a Trustless Network
- Immutable
- Security through Cryptography
- Transparency

1. Introduction to Blockchain

What is Web3?

- Decentralized version of the internet
- Powered by blockchain and smart contracts
- User-owned data and digital assets

Benefits of Web3

- User ownership and control
- Censorship resistance
- Trustless transactions
- Global accessibility

Key Components of Web3

- Blockchain platforms (Ethereum, Polygon)
- Smart Contracts
- Decentralized Storage (IPFS)
- Tokens and Cryptography

Real-World Use Cases

- Decentralized Finance (DeFi)
- NFTs and Digital Ownership
- DAOs and Governance
- Supply Chain & Healthcare

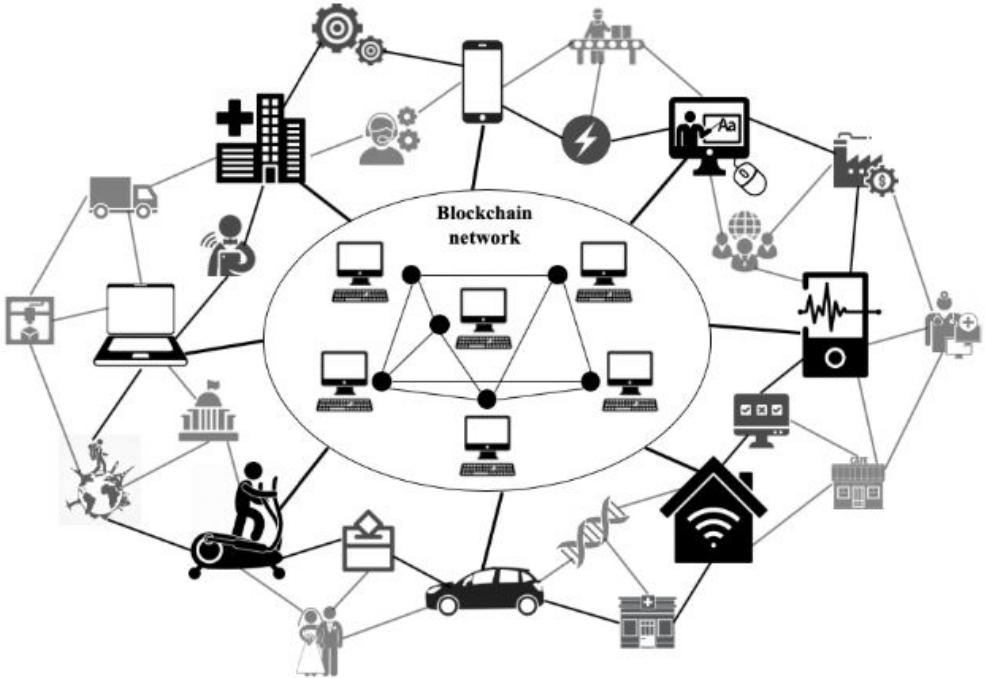
1. Introduction to Blockchain

What is Decentralization?

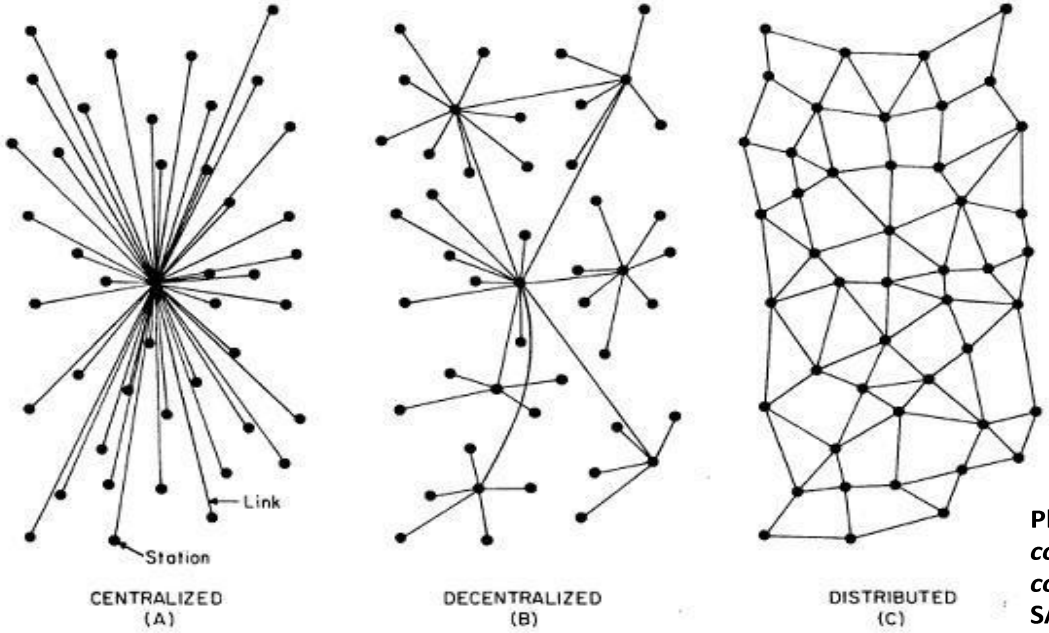
- No single controlling authority
- Distributed nodes and governance
- Improved resilience and transparency

Backbone of Blockchain

- Distributed ledger technology
- Consensus-based validation
- Immutable and transparent records



Centralized vs Decentralized vs Distributed



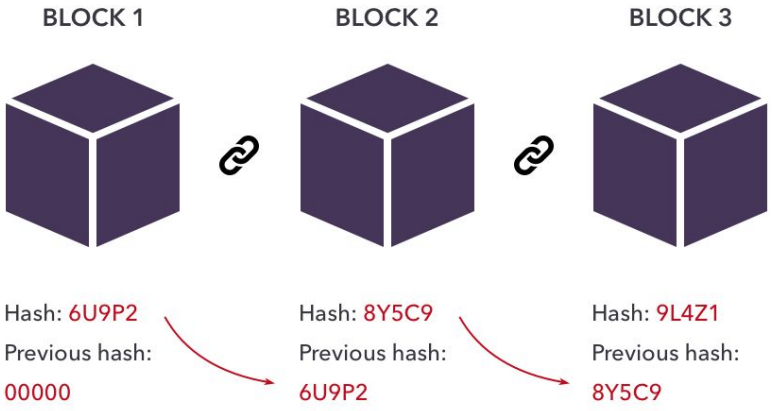
Complete reliance on single point (centralized) is not safe

- **Decentralized: Multiple points of coordination**
- **Distributed: Everyone collectively execute the job**

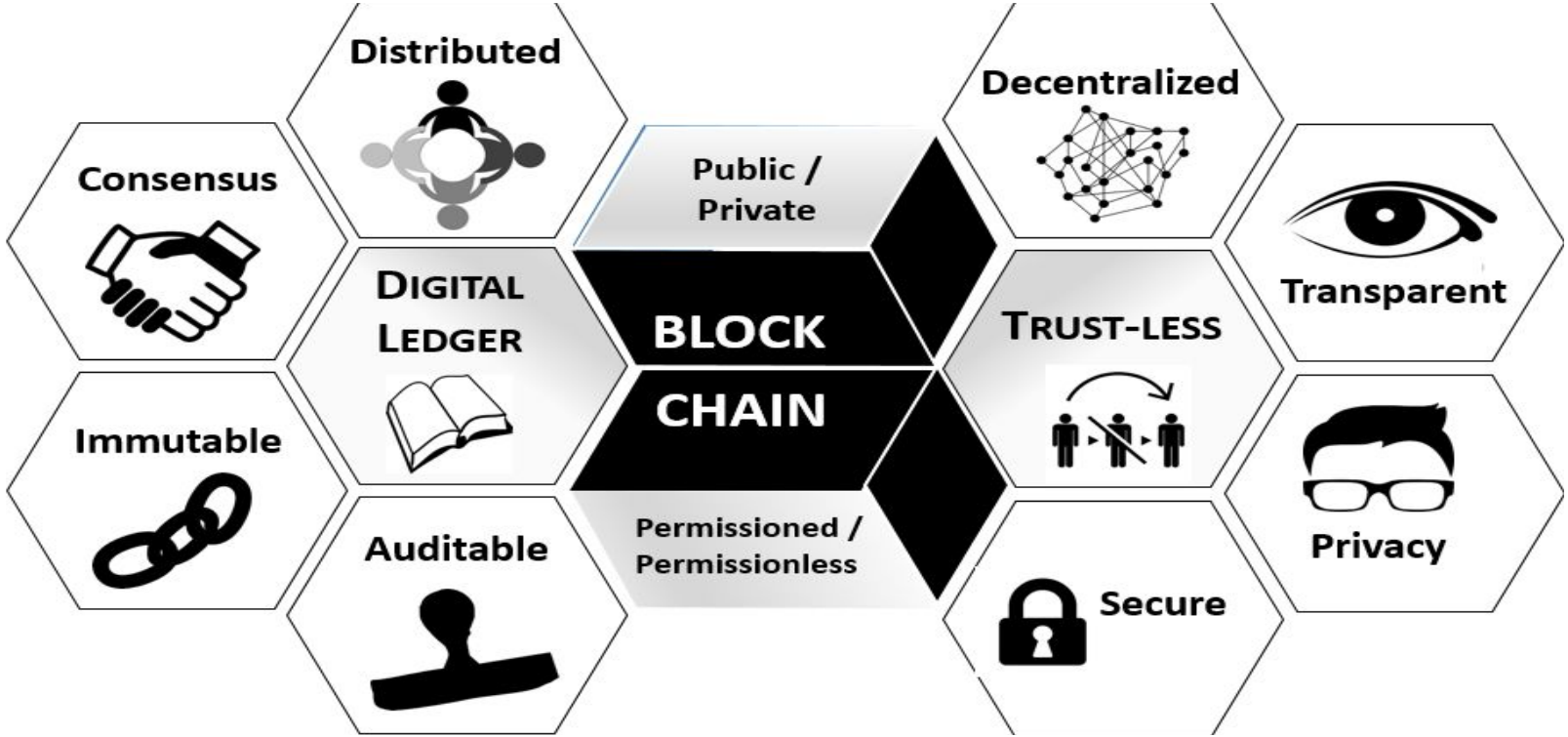
Photo courtesy: Baran, Paul. *On distributed communications: I. Introduction to distributed communications networks.* No. RM3420PR. RAND CORP SANTA MONICA CALIF, 1964.

1. Introduction to Blockchain

- ✔ Blockchain is a **digital public ledger** that records **online transactions**.
- ✔ Blockchain ensures **confidentiality, integrity and privacy**.
- ✔ When a **new block** is added to a blockchain, it is **linked to the previous block** using a **cryptographic hash**.
- ✔ This ensures the **chain is never broken** and that **each block is permanently recorded.**
- ✔ It is also **intentionally difficult** to alter past transactions in blockchain since **all the subsequent blocks must be altered first**.

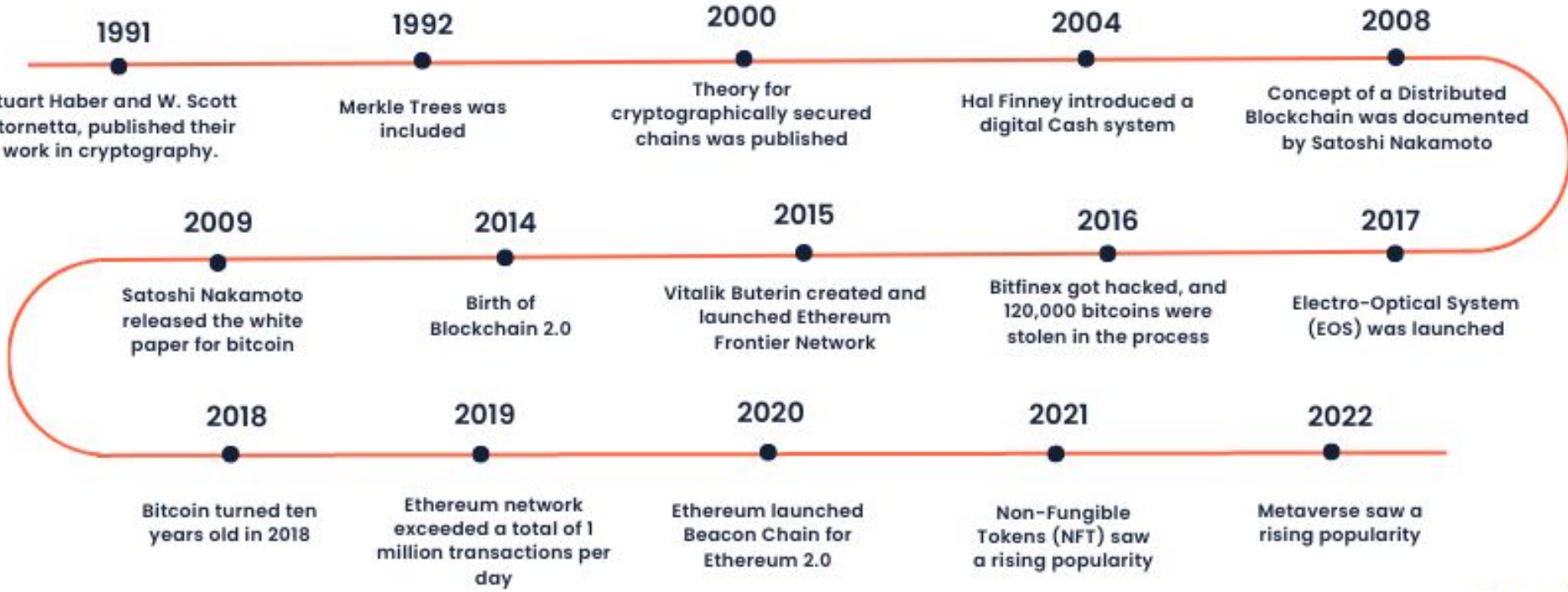


Characteristics of Blockchain

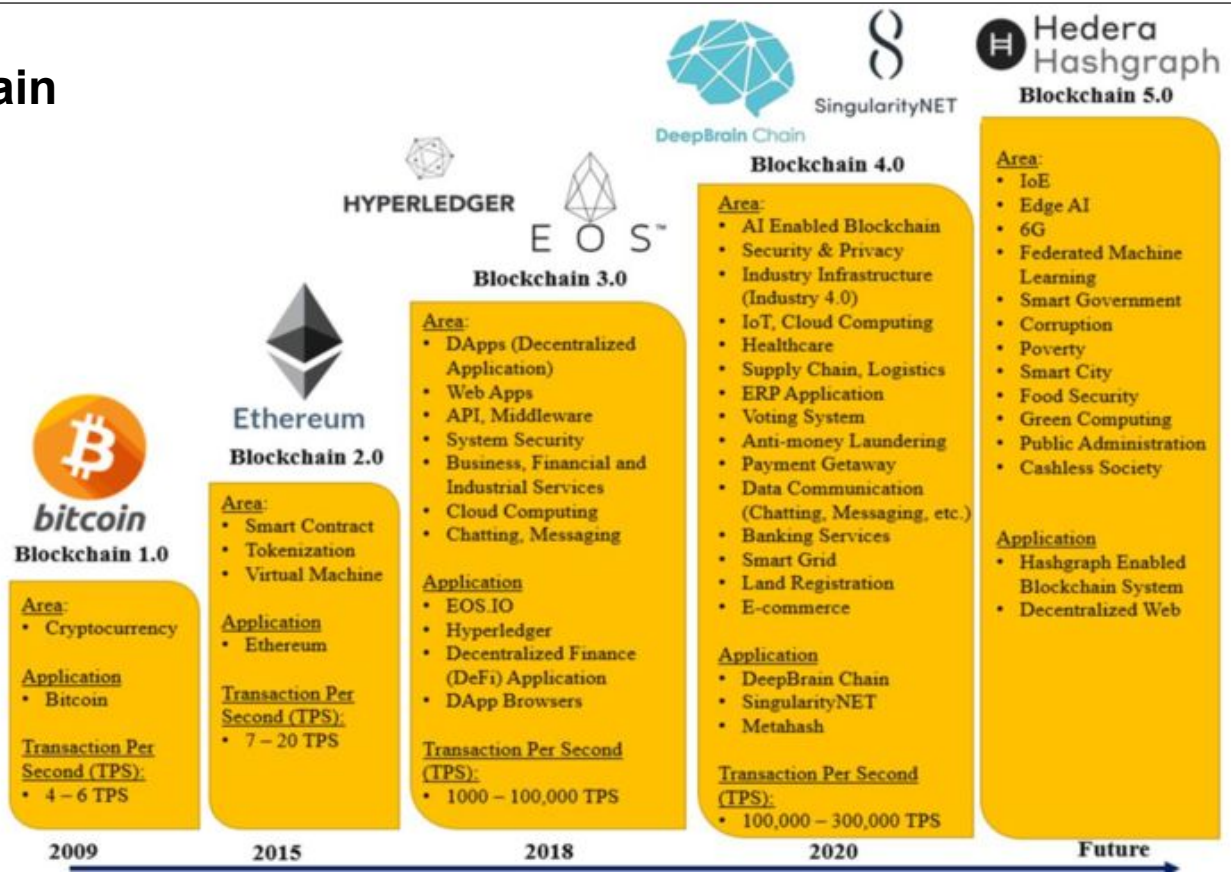


1. Introduction to Blockchain

Blockchain History Timeline



Generations of Blockchain

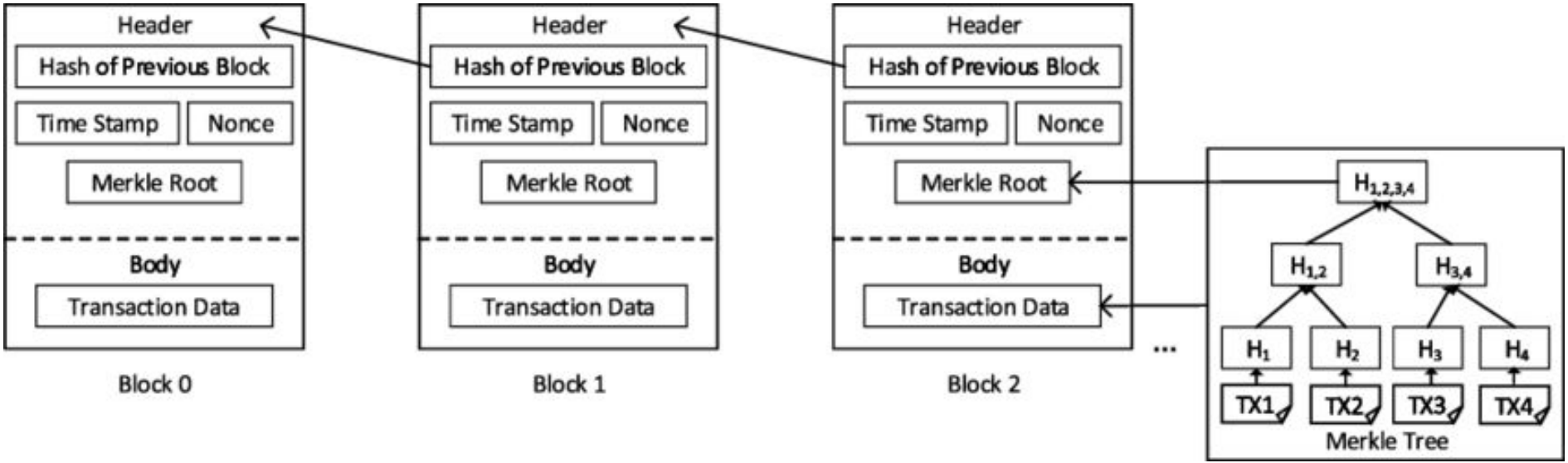


Courtesy : Research Gate

Topics to be covered

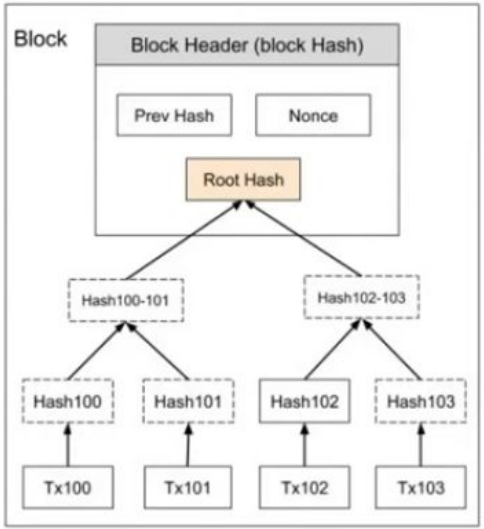
1. Introduction to Blockchain
2. **Blockchain Fundamentals**
3. Cryptocurrency Basics
4. Introduction to Solidity Programming

Blockchain Structure

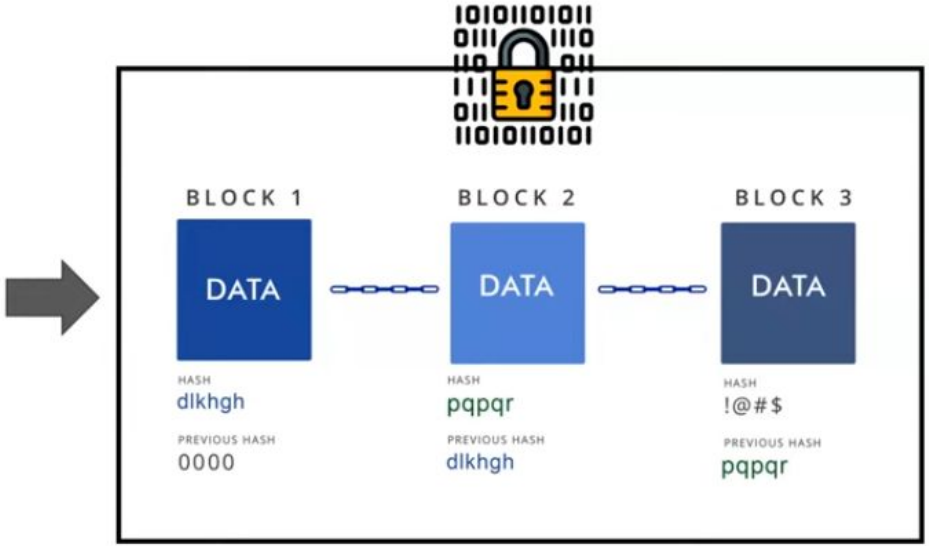


Merkle Tree

Merkle trees are a type of data structure commonly used in computer science. They are used to encrypt blockchain data more effectively and securely in bitcoin and other cryptocurrencies.



Merkle Tree

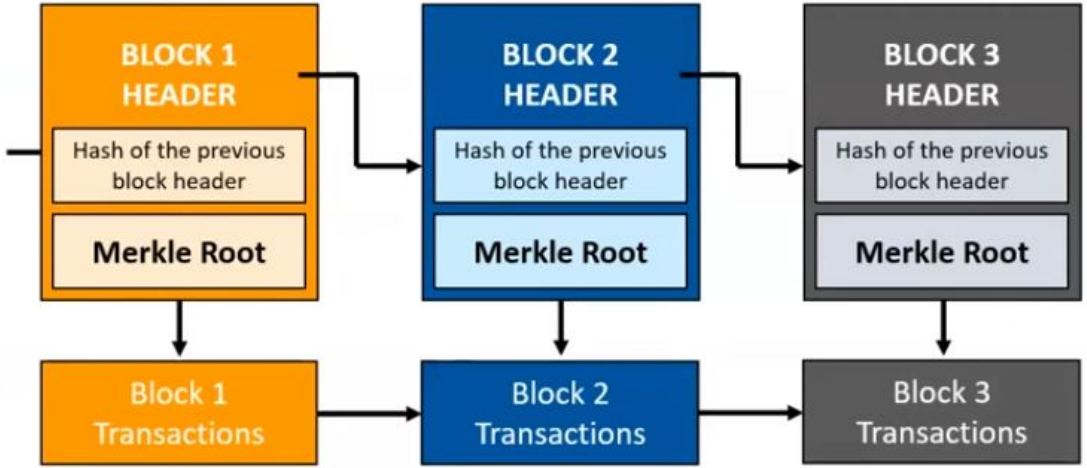


Blockchain Data encrypted Securely

2. Blockchain Fundamentals

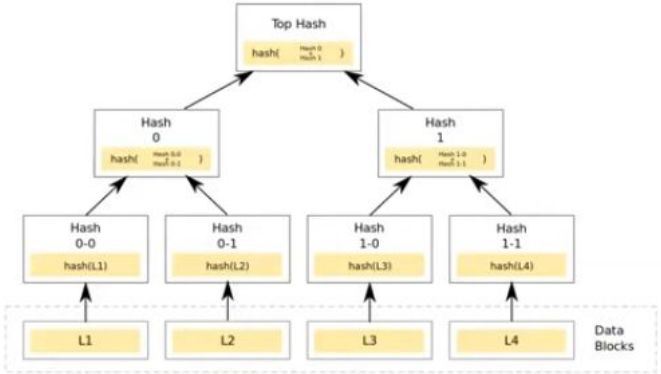
Why is it essential for Blockchain ?

Merkle Trees hash records in accounting, thereby separating the proof of data. Proving that given information across the network is all that is required for a transaction to be valid.



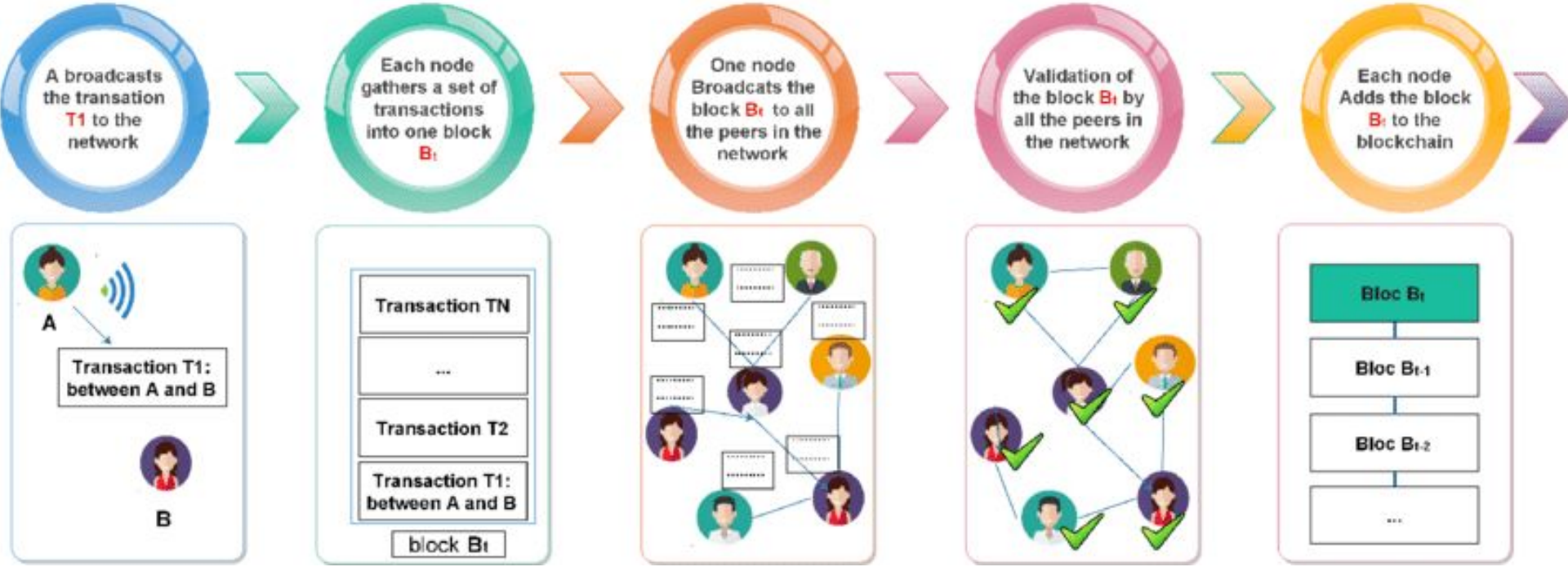
Merkle Tree breaking the data into tiny parts of information

Benefits of Merkle Tree



- Validate the data's integrity
- Takes little disk space
- Tiny information across networks
- Efficient Verification

Transactions in Blockchain - Example



2. Blockchain Fundamentals

WHAT ARE NODES?

Nodes are the electronic devices connected to the network and possessing an IP address. Generally, nodes are the communication endpoints which means that any user or application that wants to interact with the blockchain does so through nodes.

WHAT DOES A BLOCKCHAIN NODE DO?

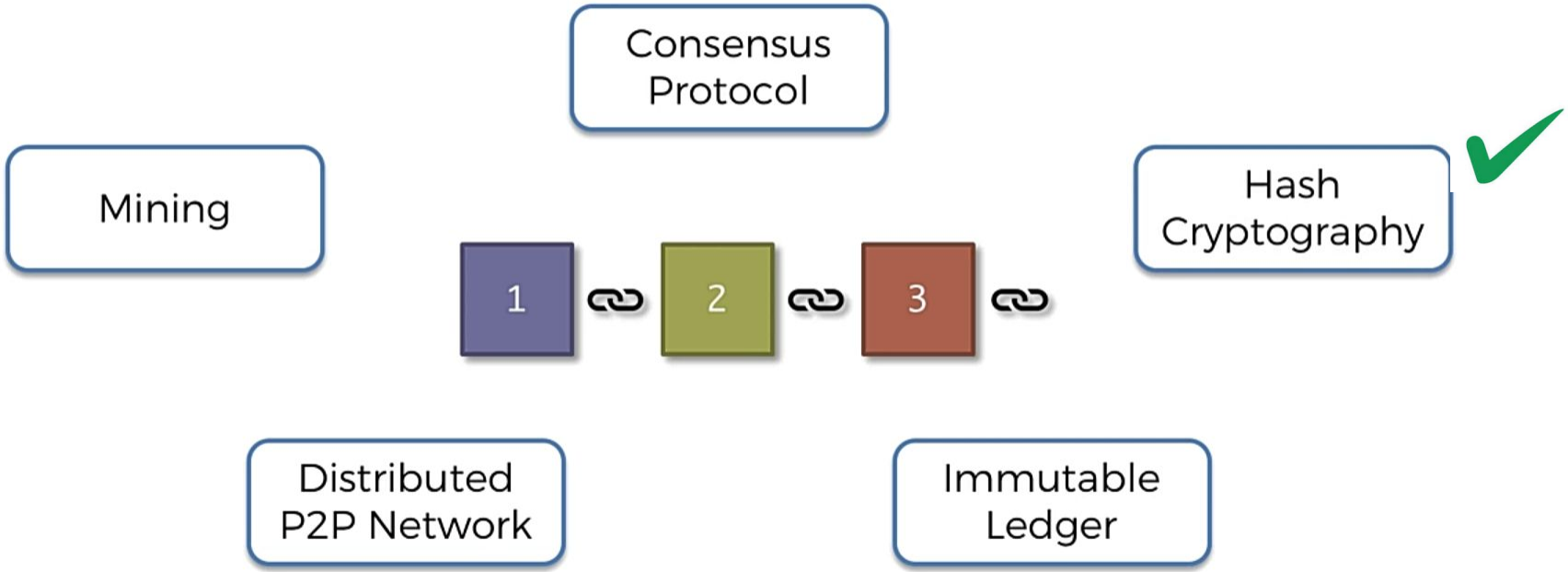
Processing A Transaction

Managing the transactions and their validity

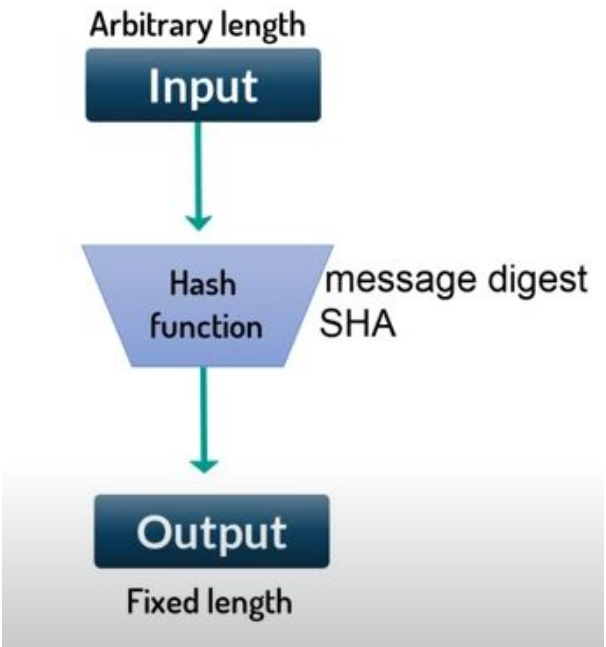
Storing the cryptographically linked blocks

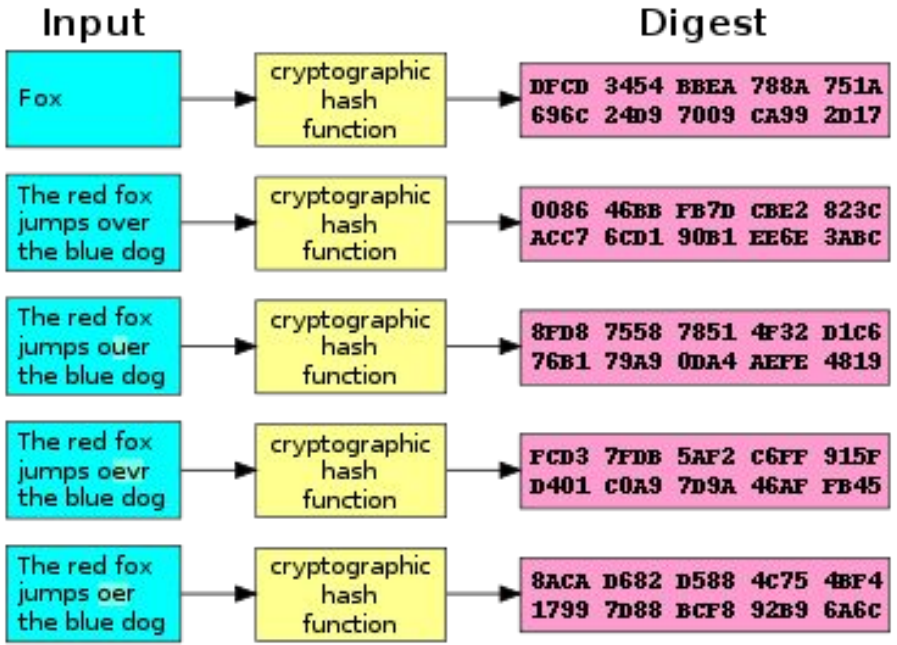
Acting as a point of communication

2. Blockchain Fundamentals

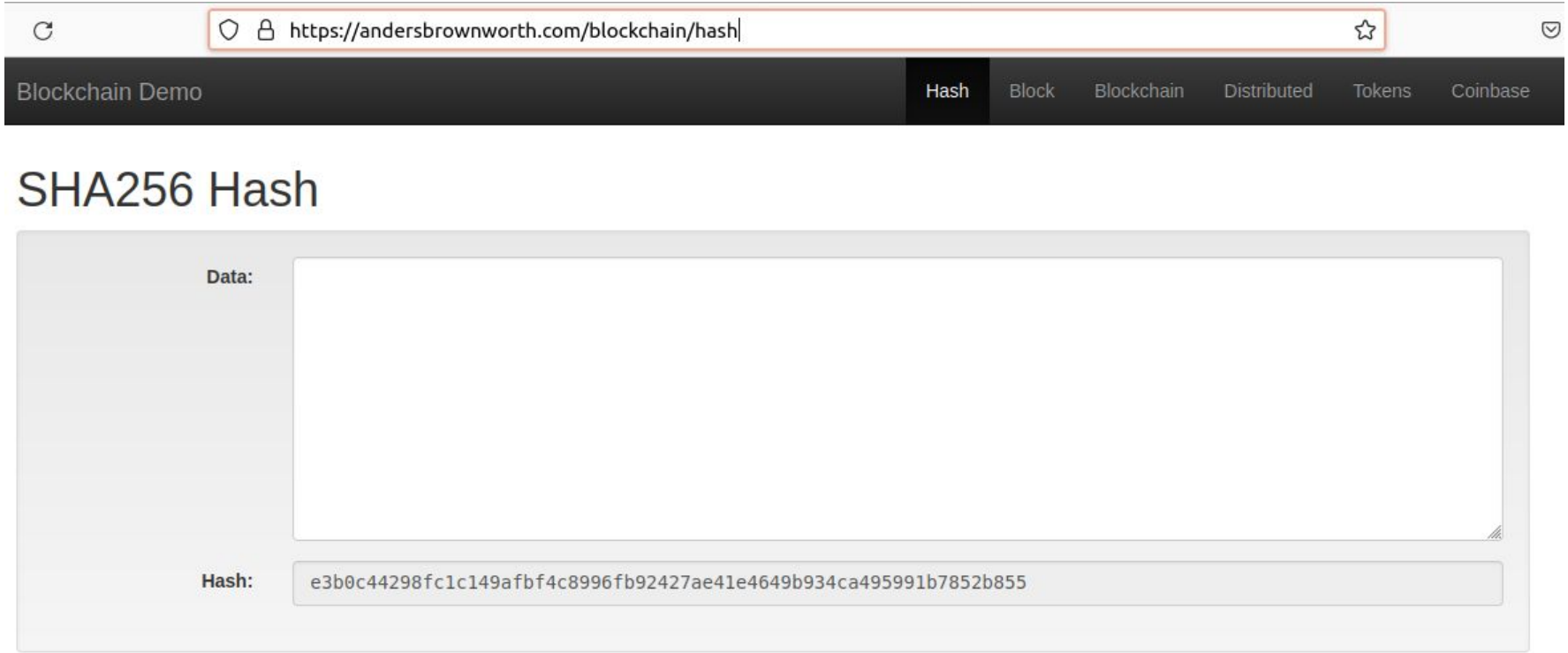


Cryptographic Hash Functions



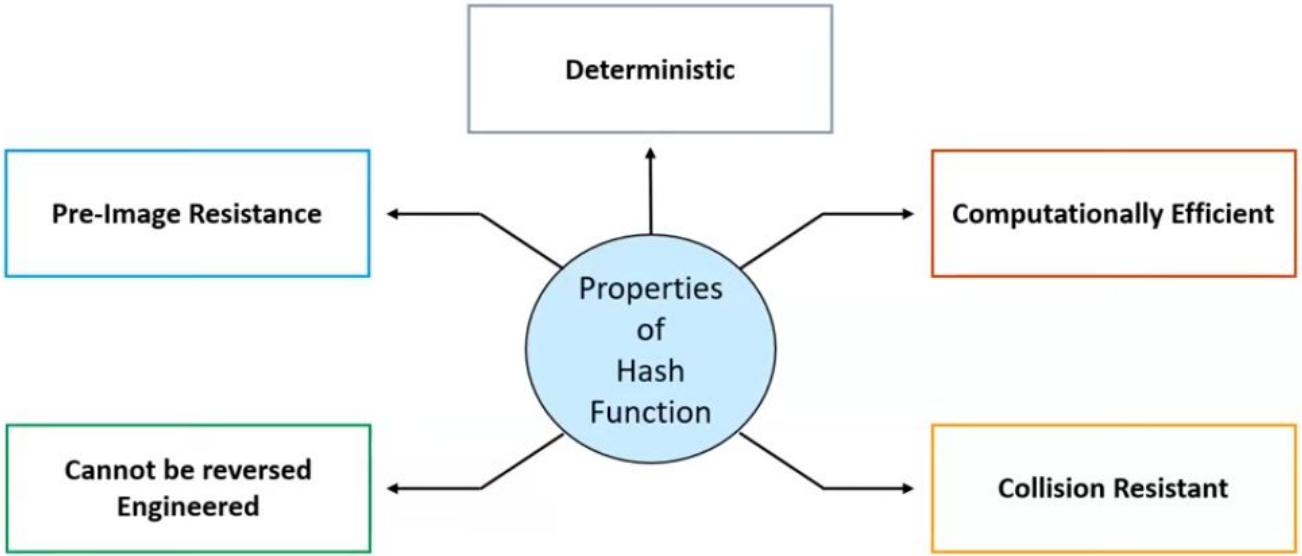


Cryptographic Hash Functions - Demo

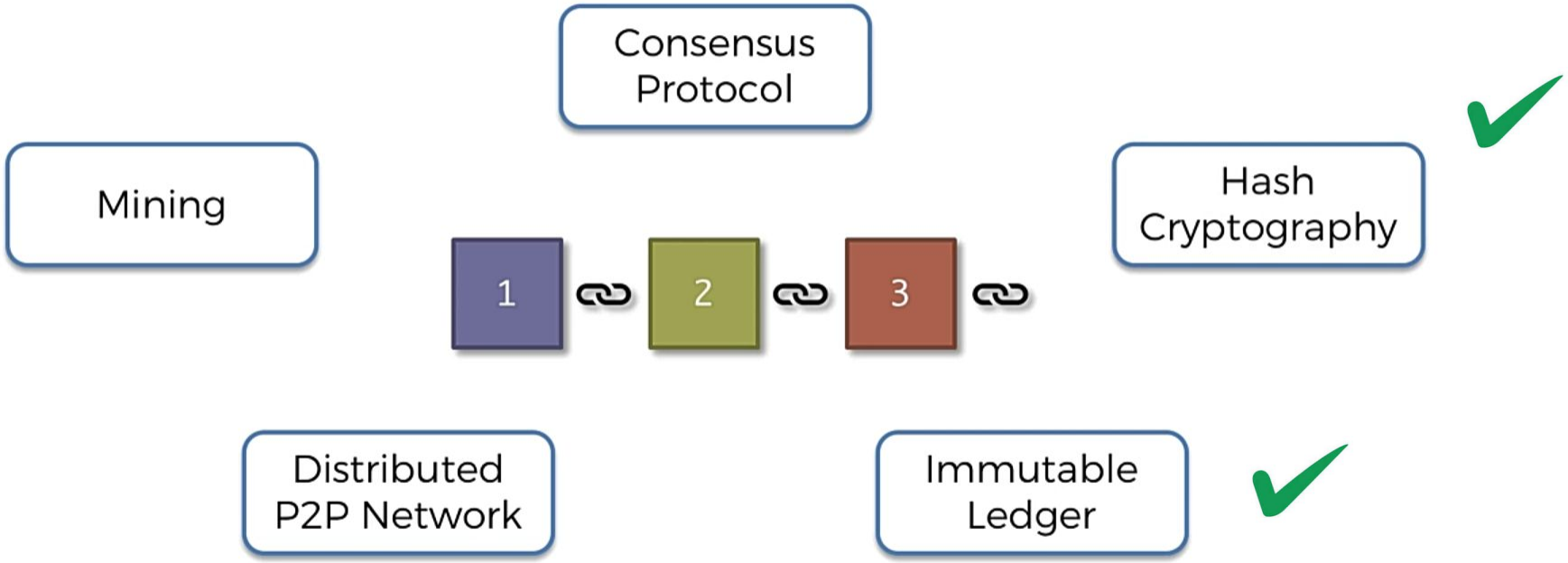


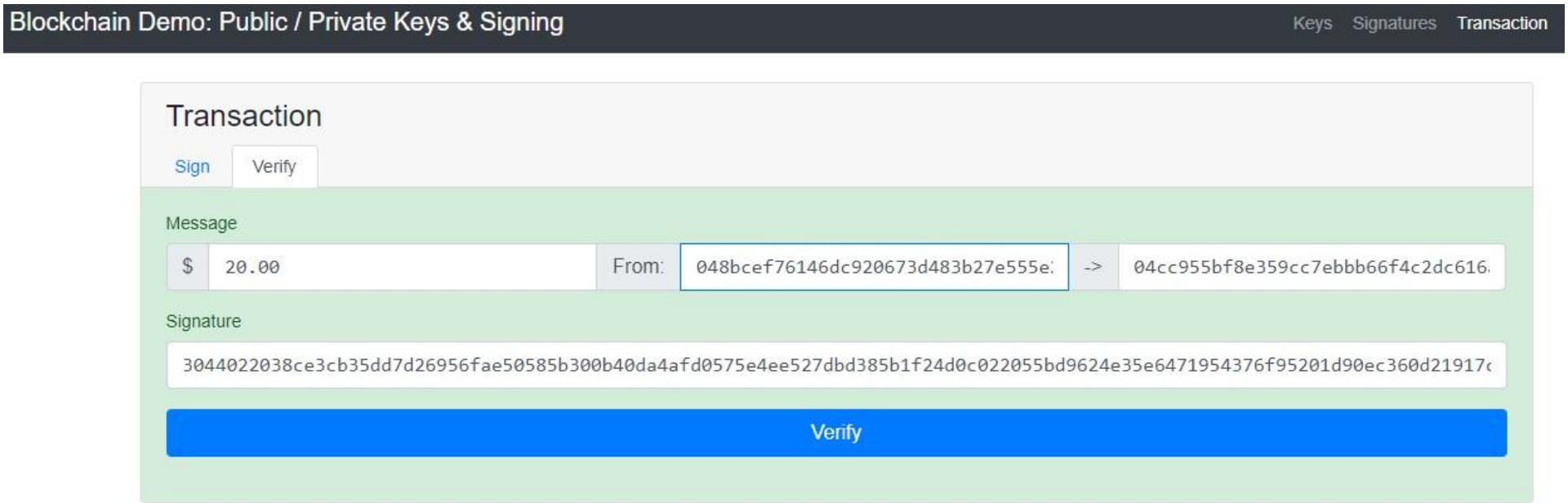
2. Blockchain Fundamentals

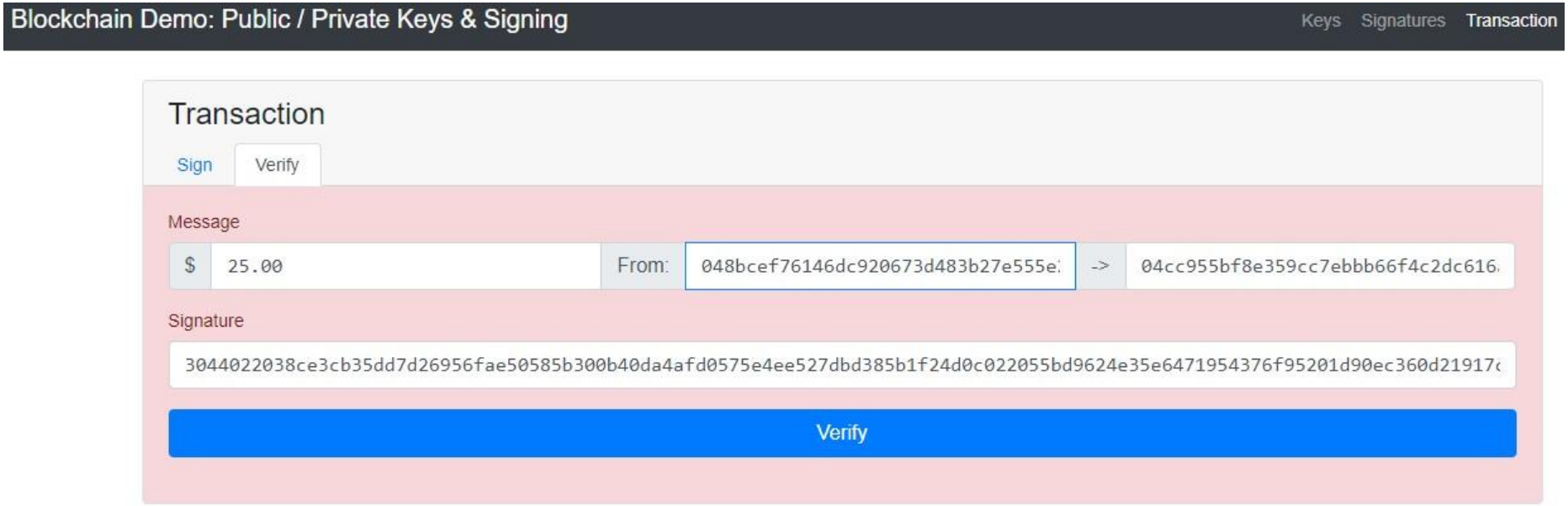
Let's take an example - If you use the SHA256 hash algorithm and pass 101Blockchains as input, you will get the following output:
fbffd63a60374a31aa9811cbc80b577e23925a5874e86a17f712bab874f33ac9



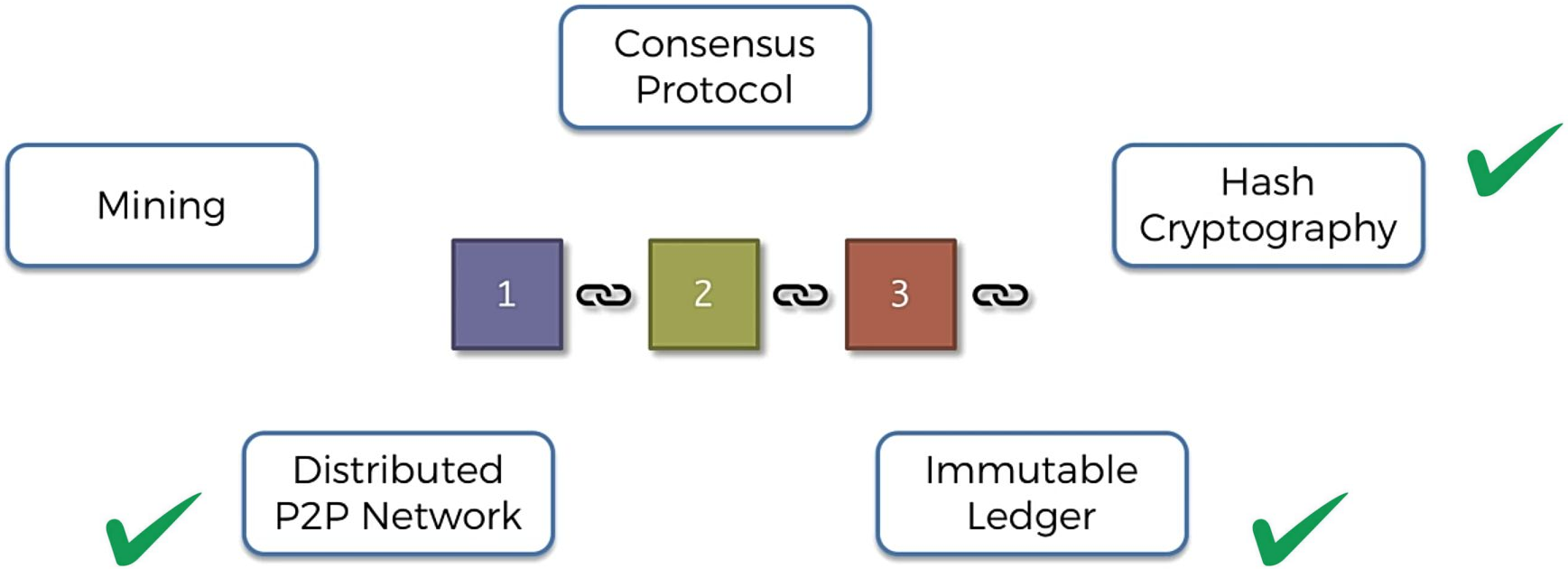
2. Blockchain Fundamentals



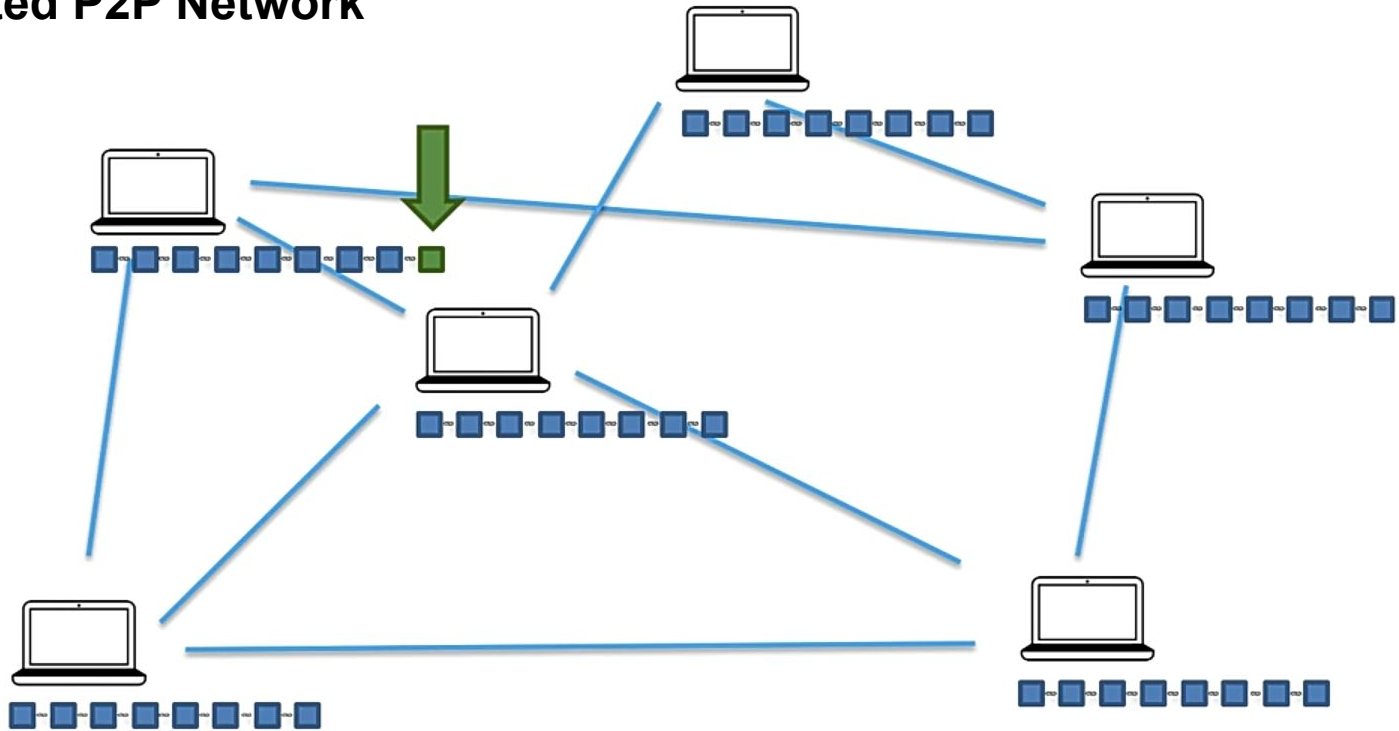

Blockchain Demo: Public / Private Keys & Signing
Keys
Signatures
Transaction
Transaction
Sign
Verify
Message
$
20.00
From:
048bcef76146dc920673d483b27e555e:
->
04cc955bf8e359cc7ebbb66f4c2dc616
Signature
3044022038ce3cb35dd7d26956fae50585b300b40da4afd0575e4ee527dbd385b1f24d0c022055bd9624e35e6471954376f95201d90ec360d21917
Verify


Blockchain Demo: Public / Private Keys & Signing
Keys
Signatures
Transaction
Transaction
Sign
Verify
Message
$
25.00
From:
048bcef76146dc920673d483b27e555e:
->
04cc955bf8e359cc7ebbb66f4c2dc616
Signature
3044022038ce3cb35dd7d26956fae50585b300b40da4afd0575e4ee527dbd385b1f24d0c022055bd9624e35e6471954376f95201d90ec360d21917
Verify

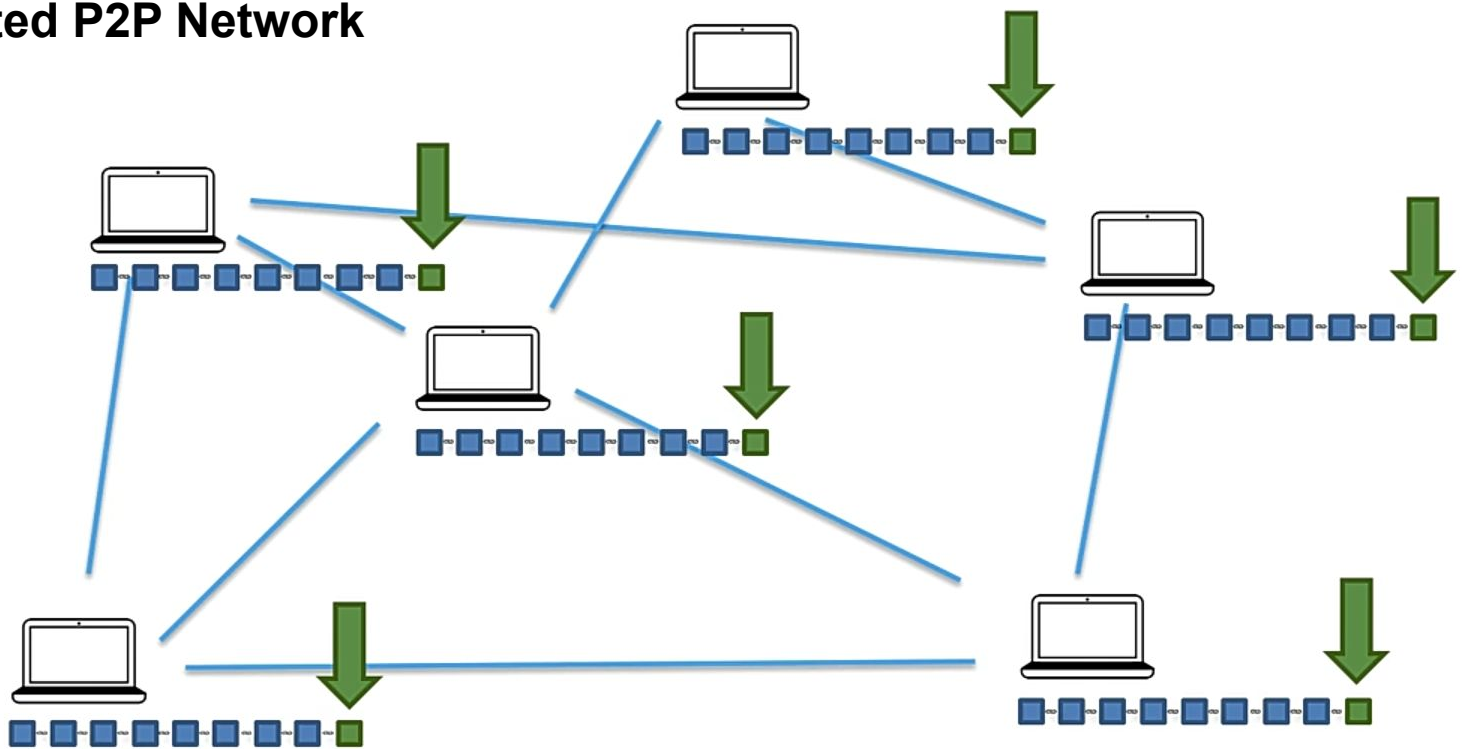
2. Blockchain Fundamentals



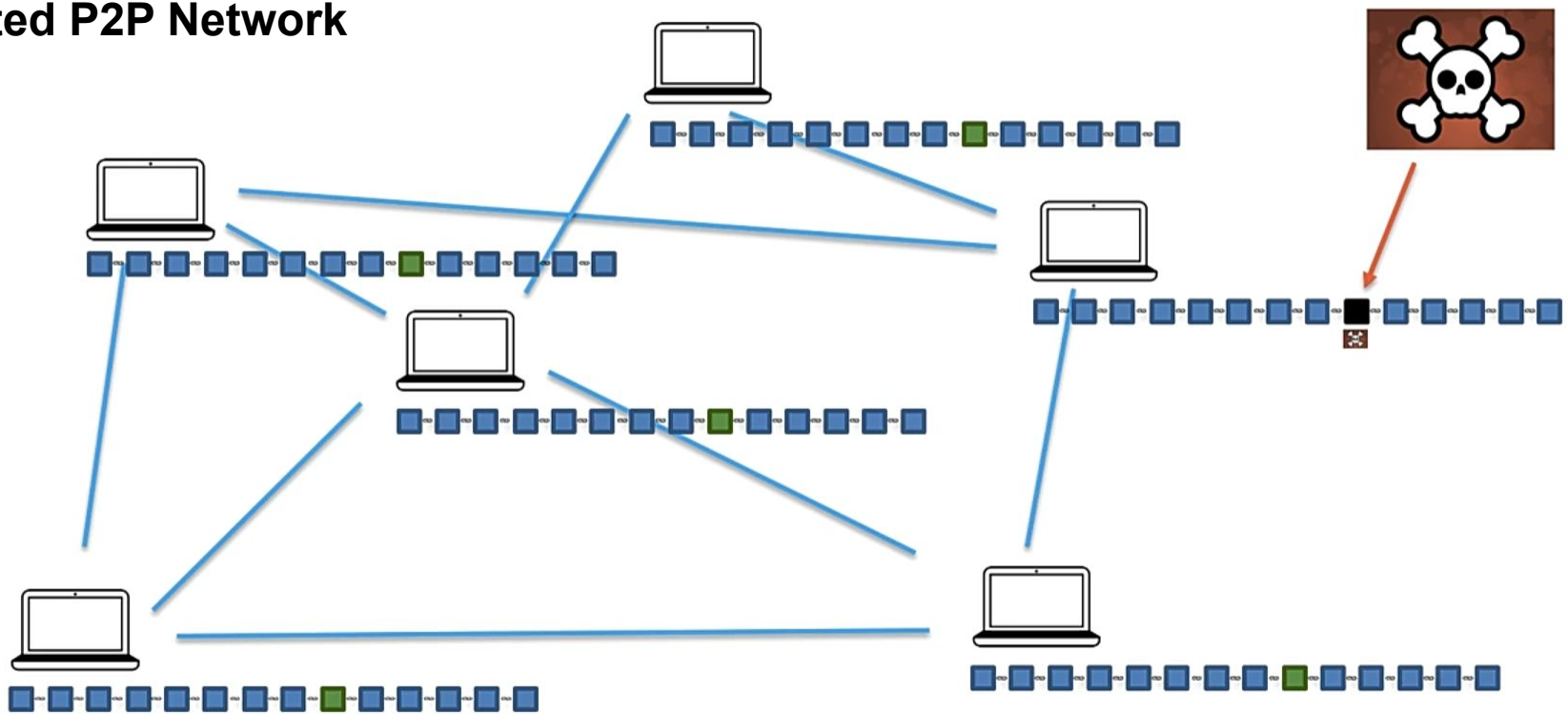
Distributed P2P Network



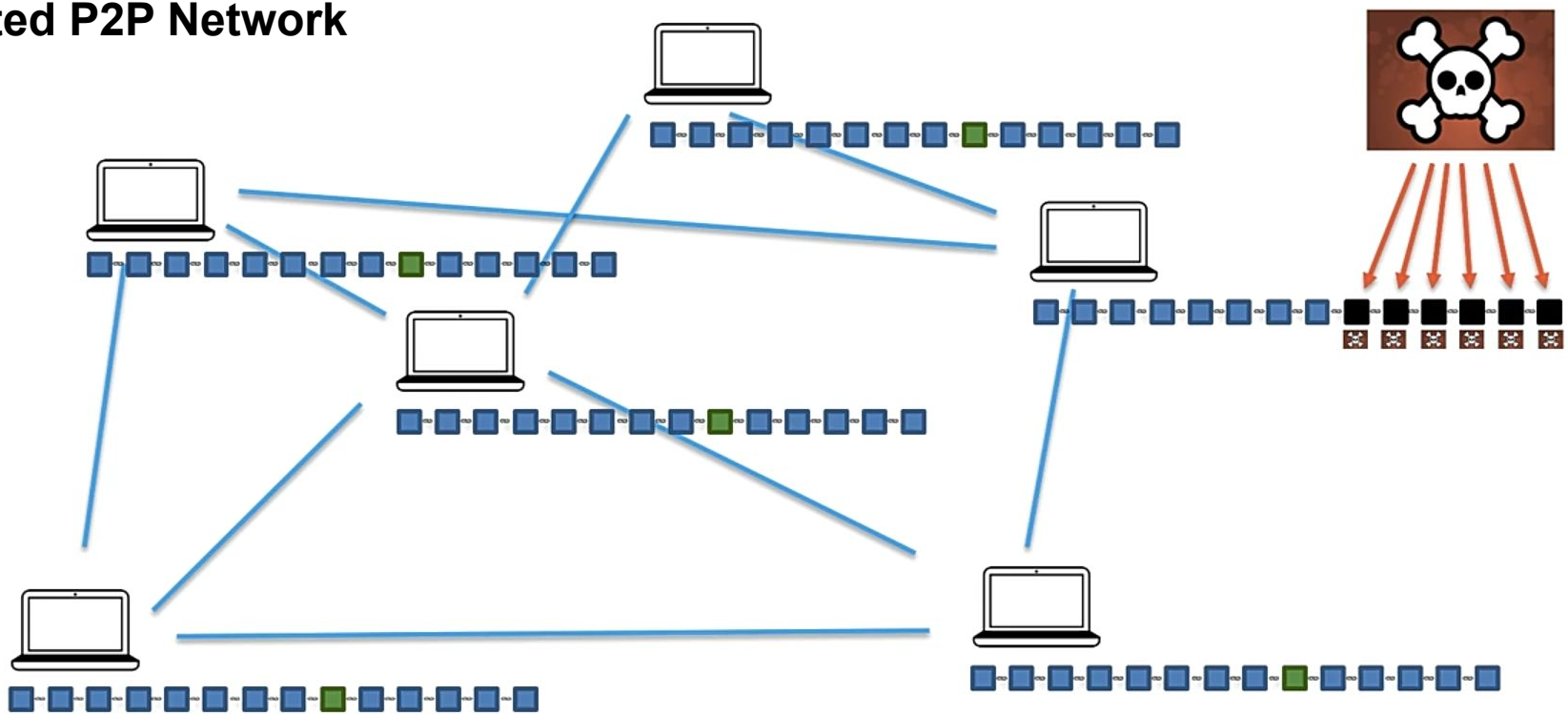
Distributed P2P Network



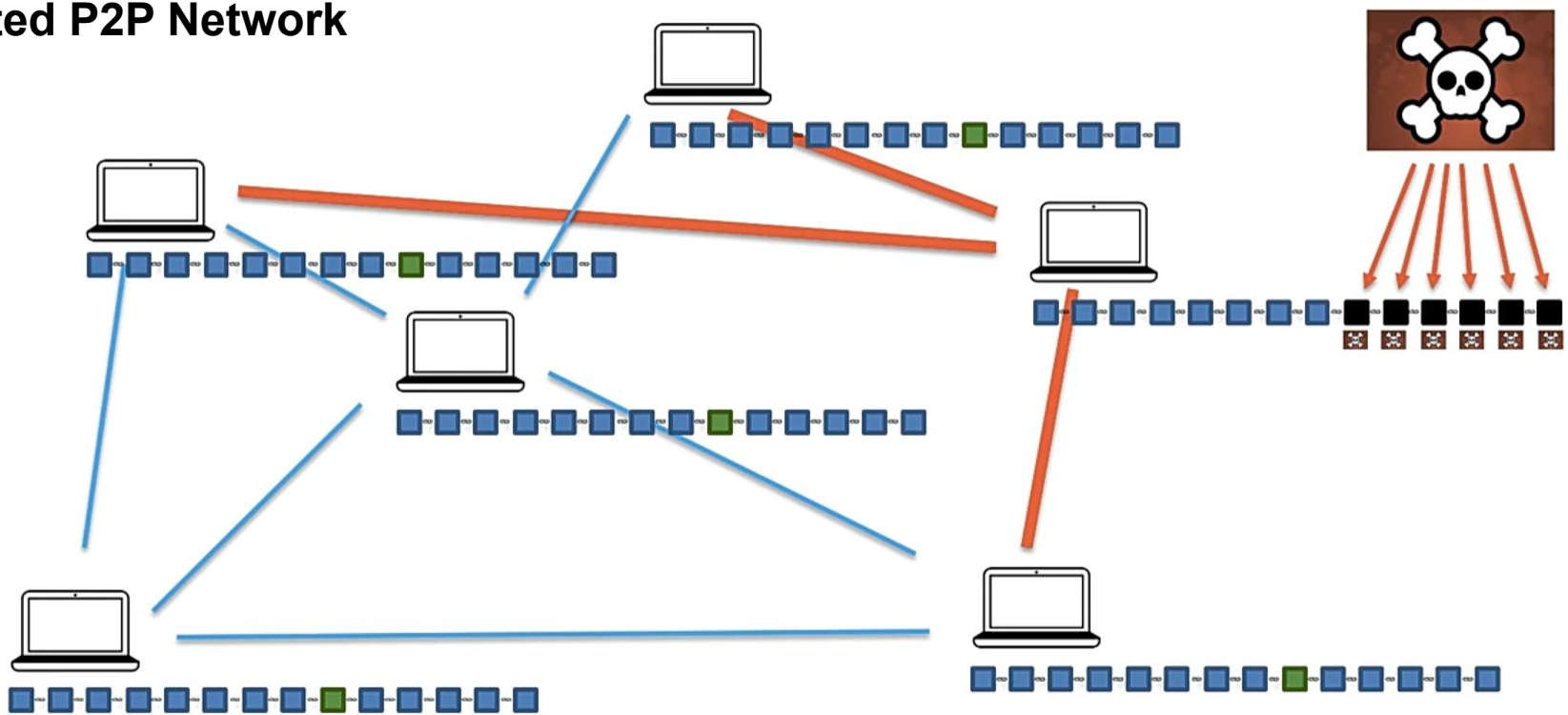
Distributed P2P Network



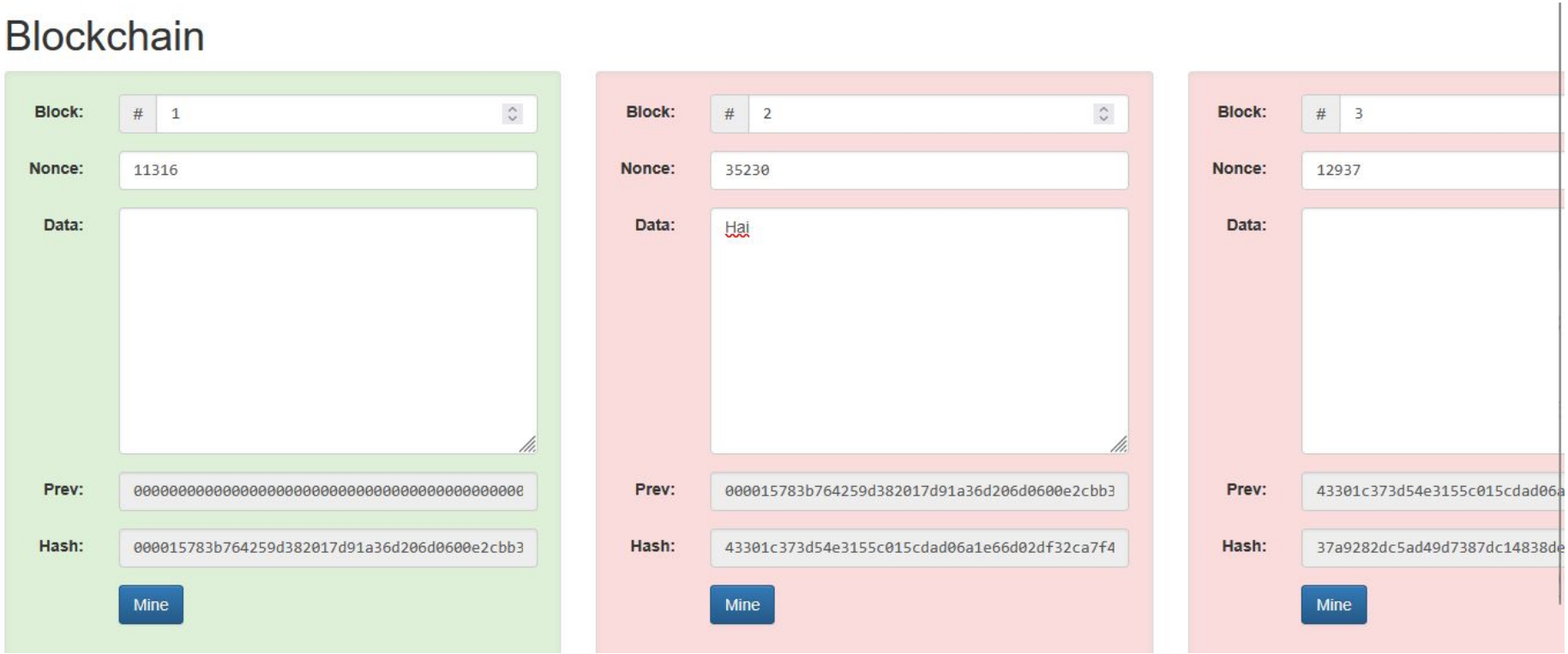
Distributed P2P Network



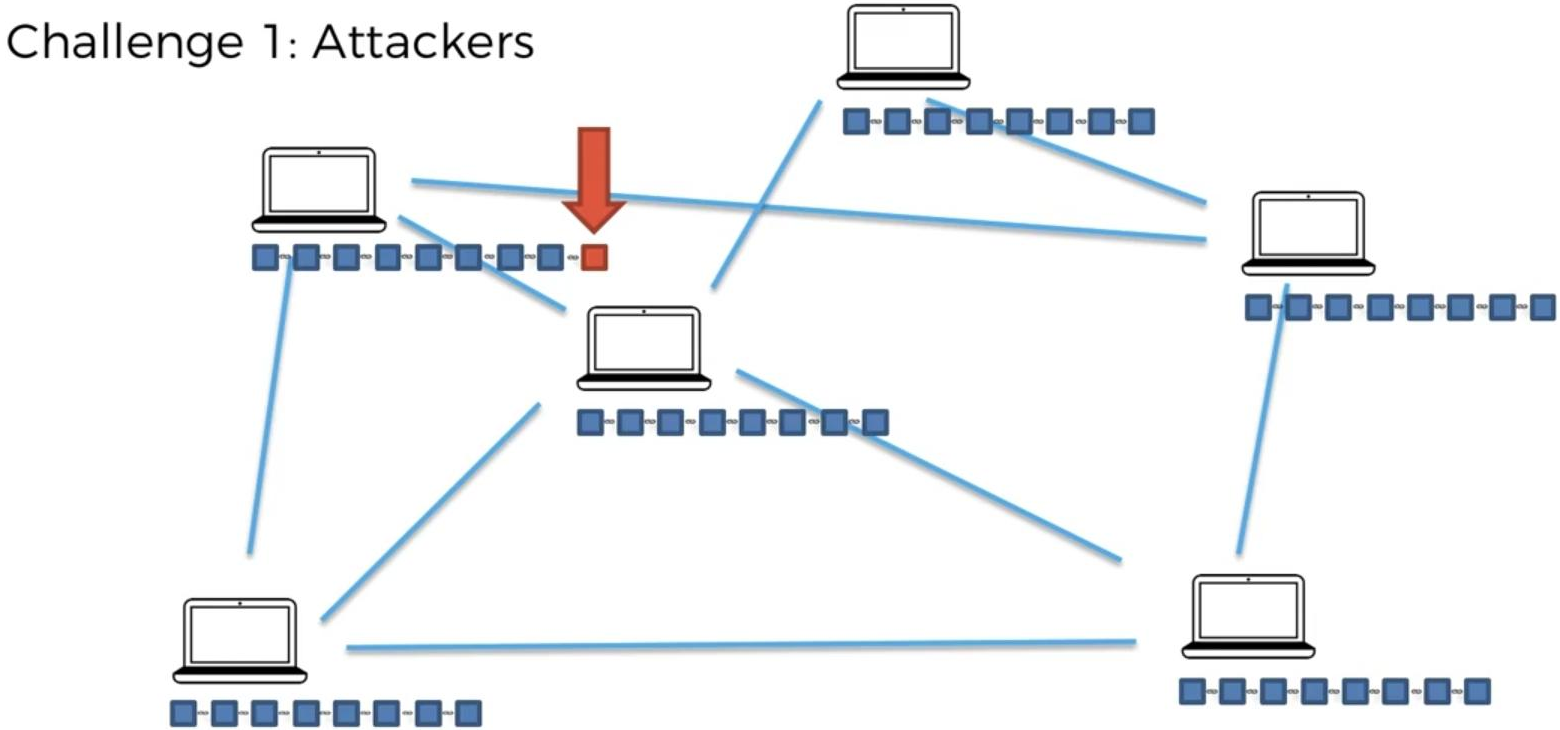
Distributed P2P Network



2. Blockchain Fundamentals

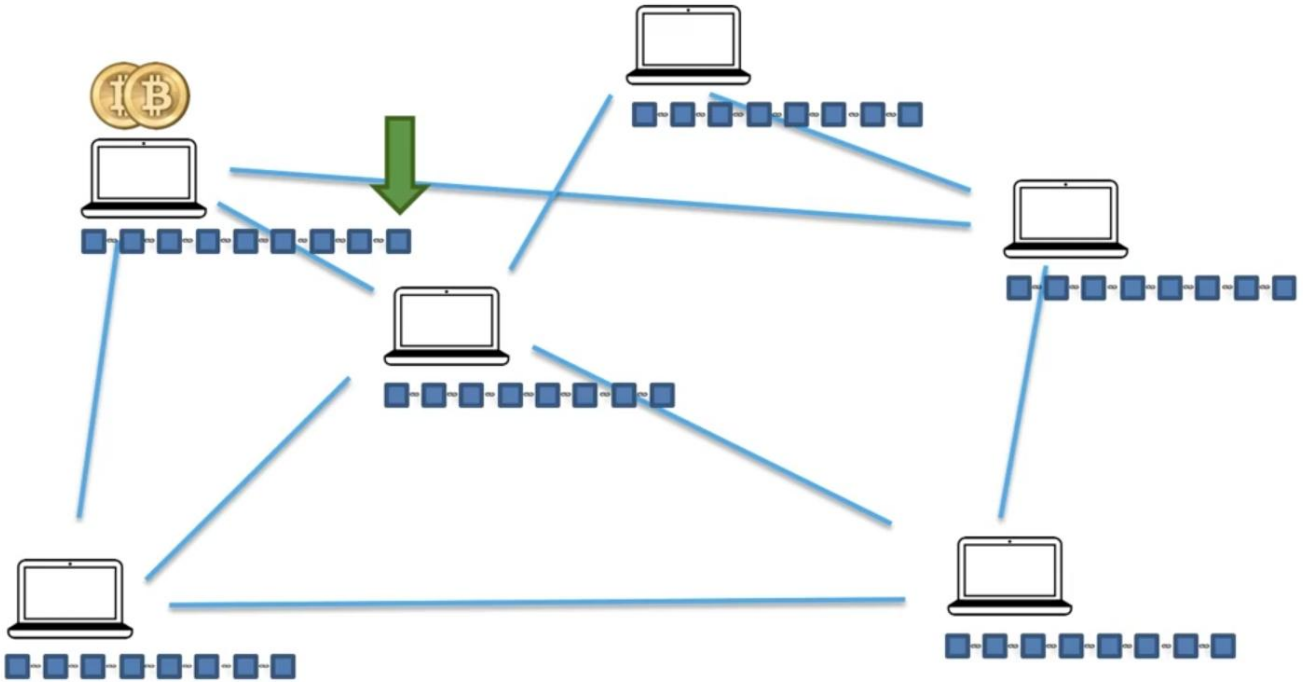


Challenges in Distributed P2P Network



2. Blockchain Fundamentals

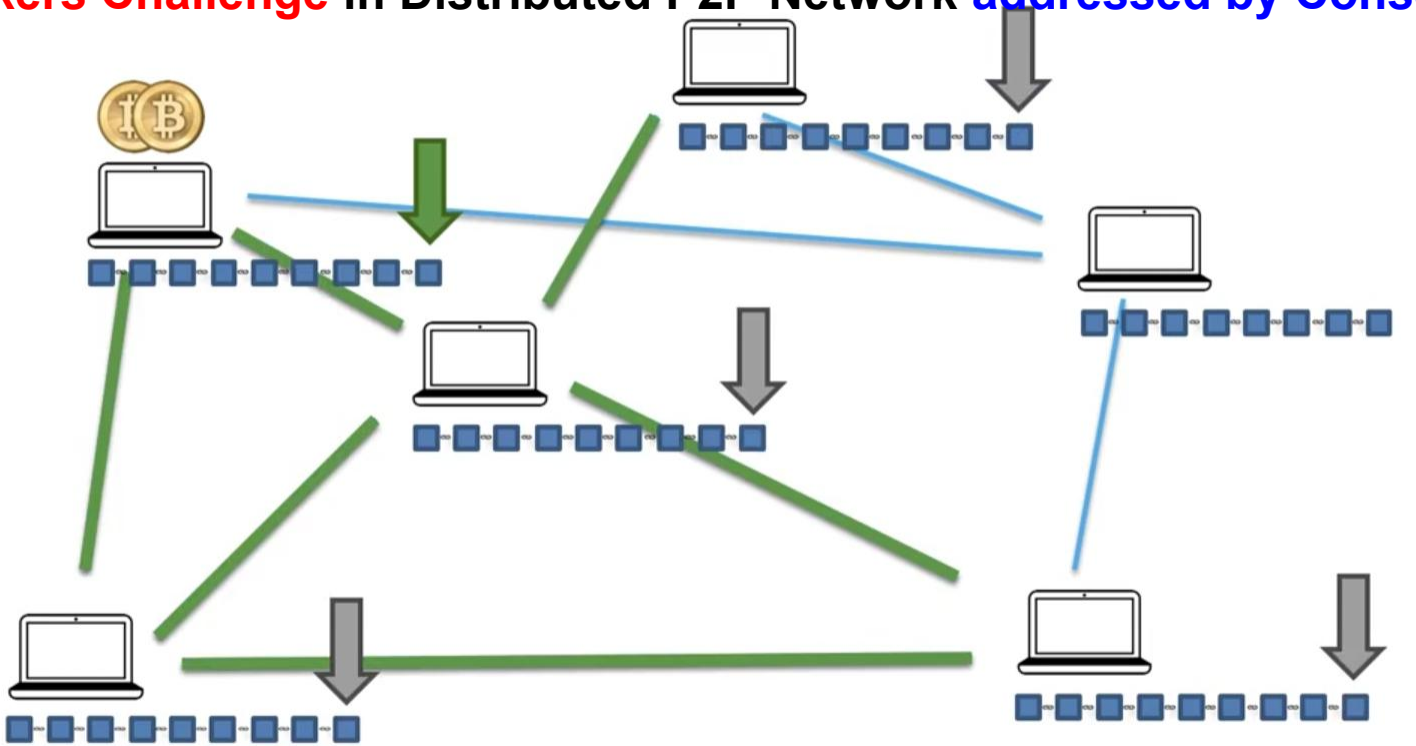
Attackers Challenge in Distributed P2P Network addressed by Consensus



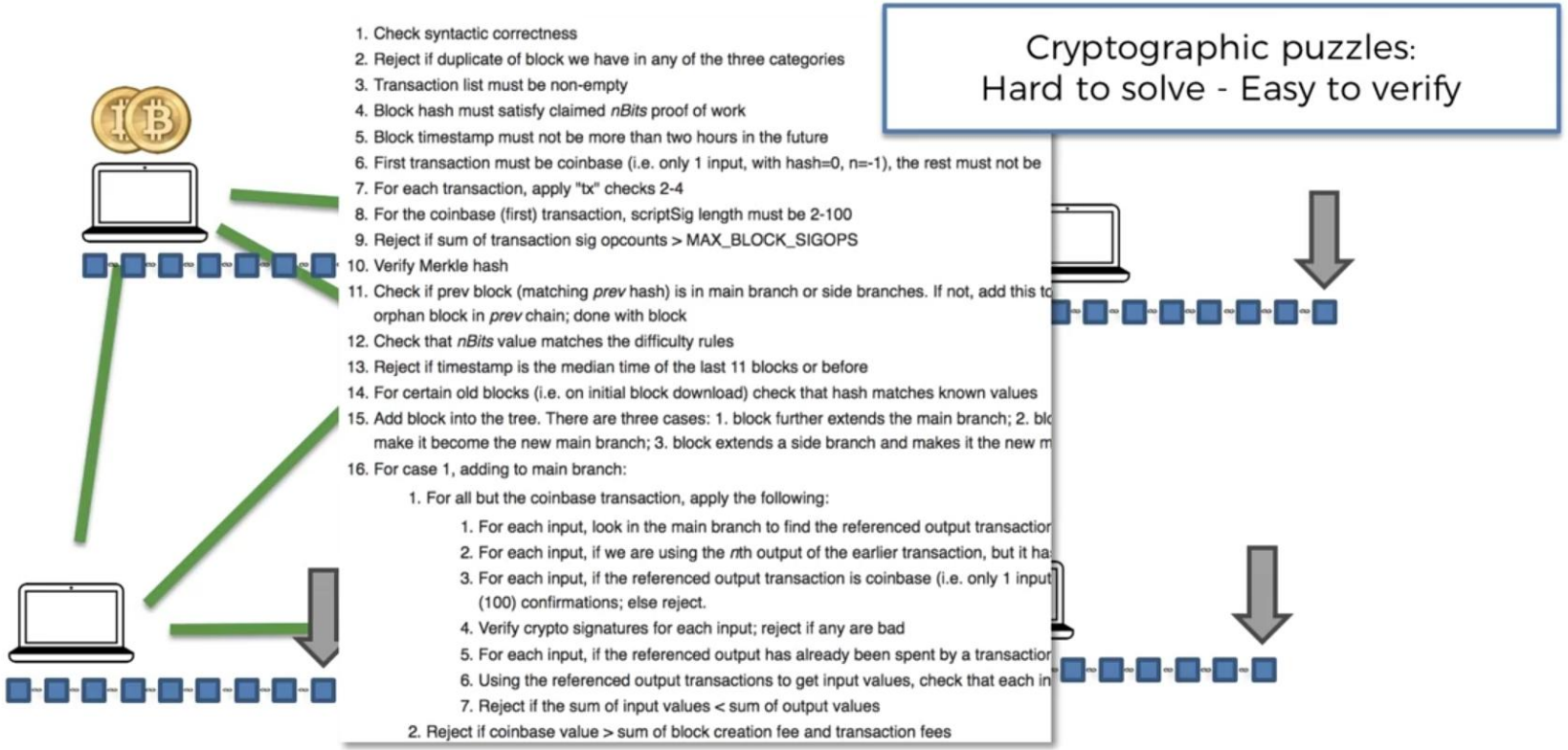
Miners get incentives for :

1. Adding a block
2. To play fair
3. From the transaction fees

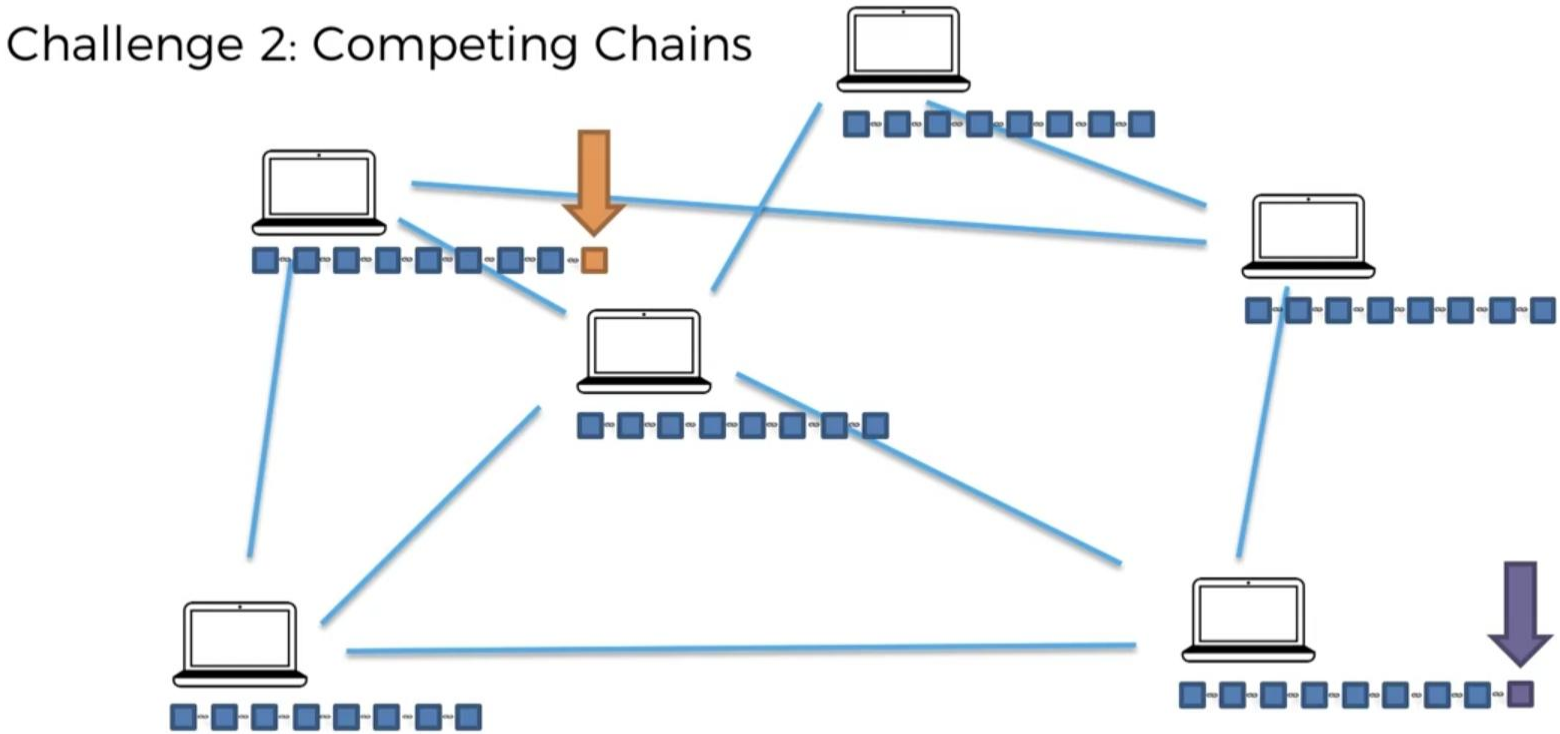
Attackers Challenge in Distributed P2P Network addressed by Consensus



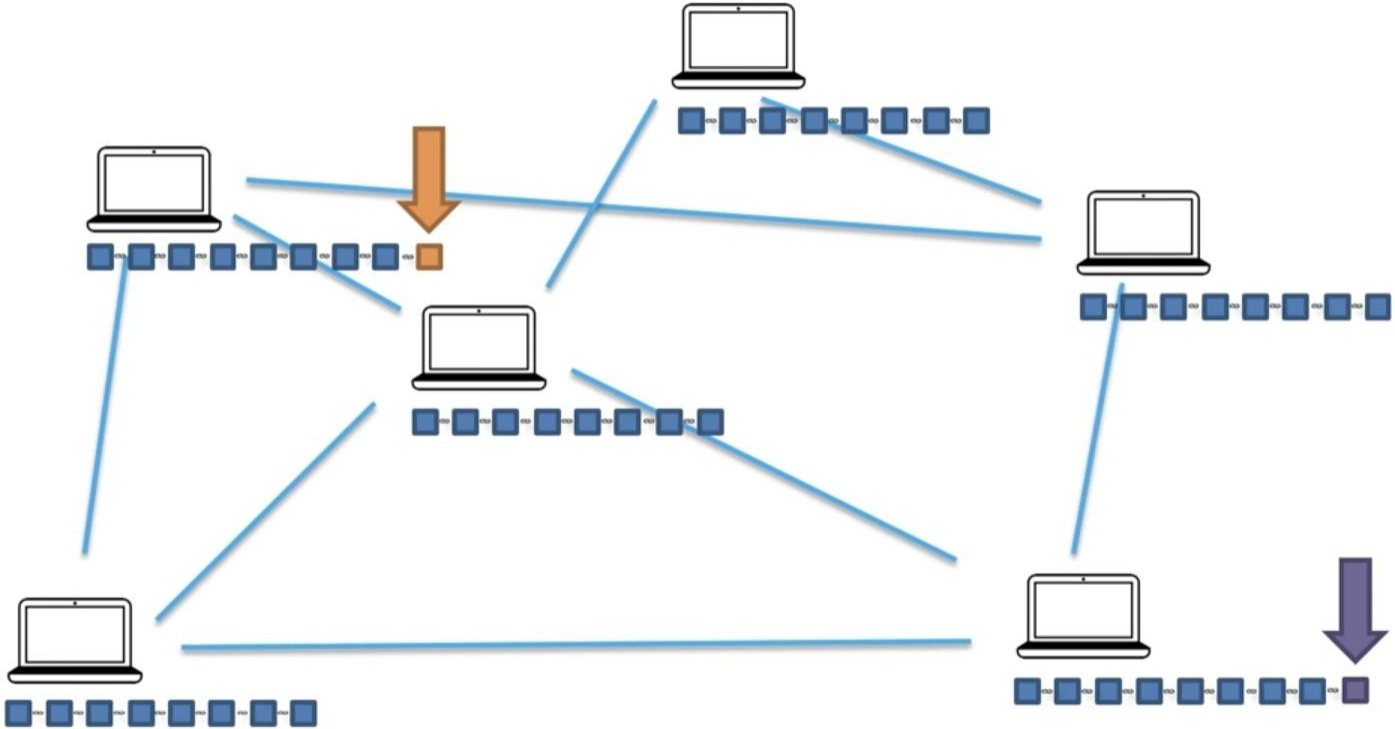
Attackers Challenge in Distributed P2P Network addressed by Consensus



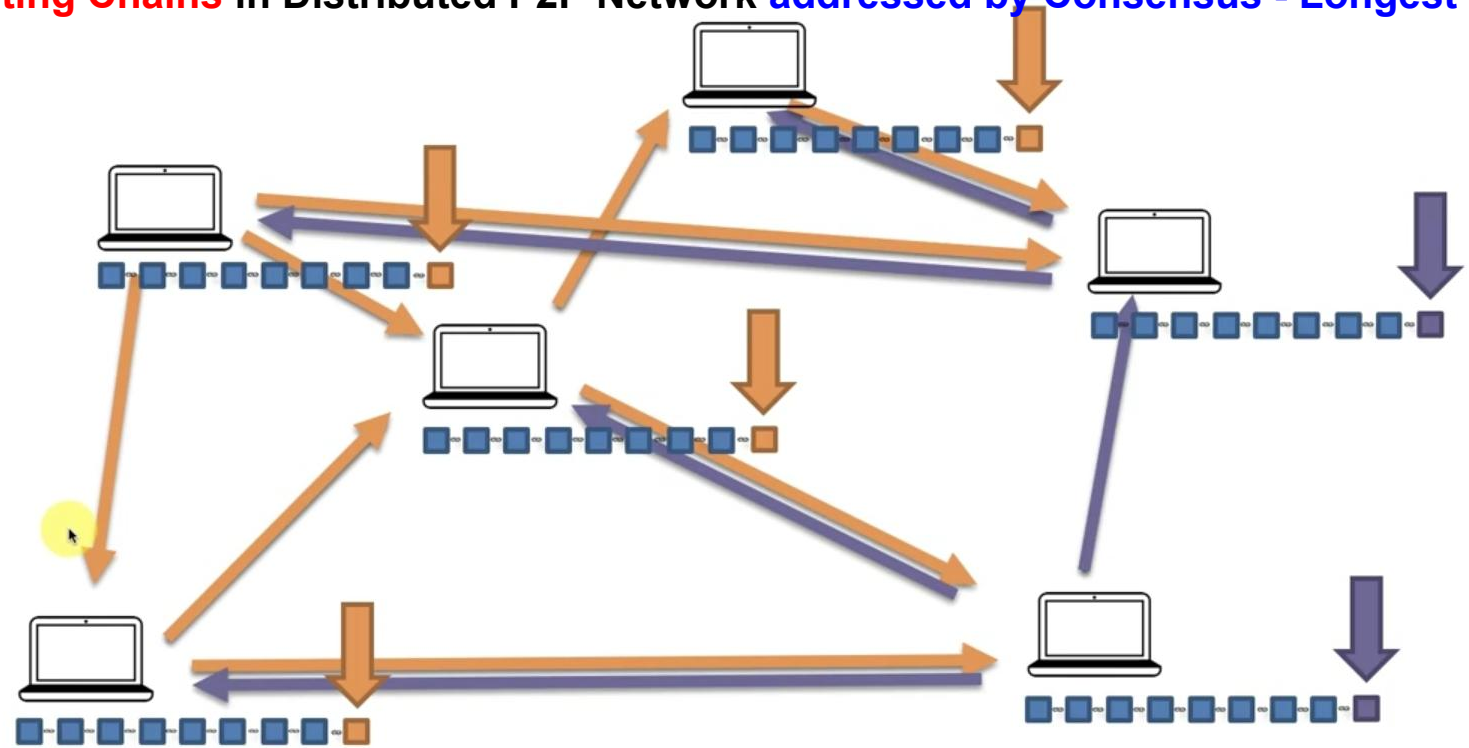
Challenges in Distributed P2P Network



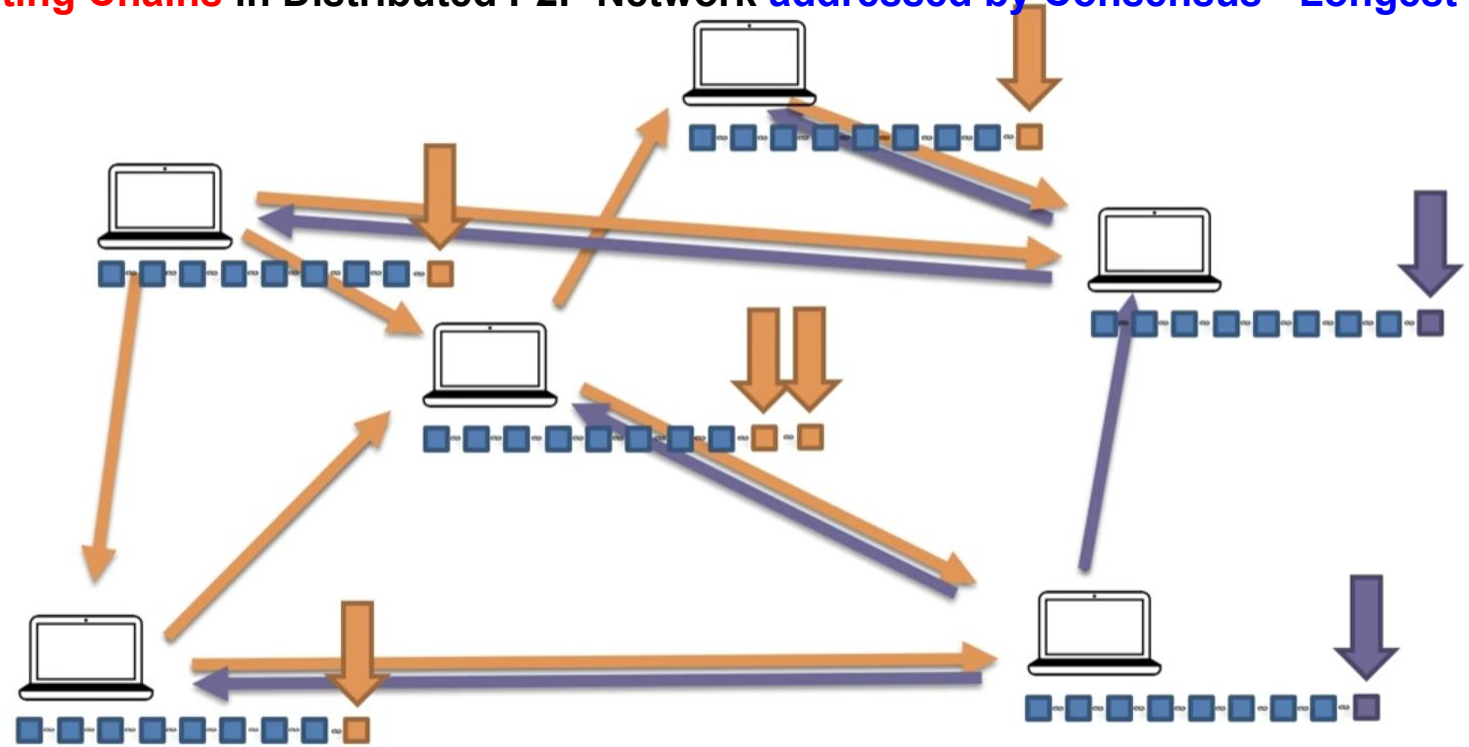
Competing Chains in Distributed P2P Network addressed by Consensus - Longest Chain



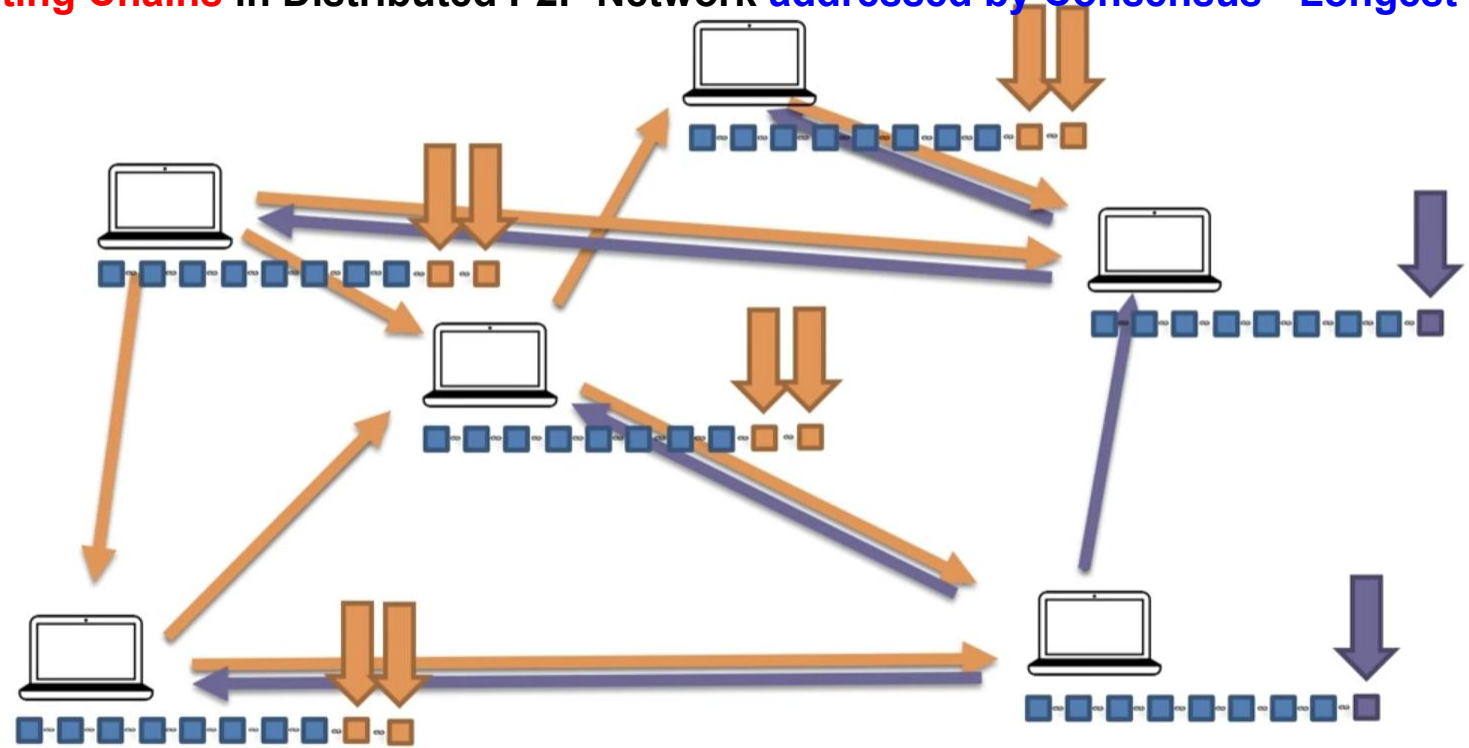
Competing Chains in Distributed P2P Network addressed by Consensus - Longest Chain



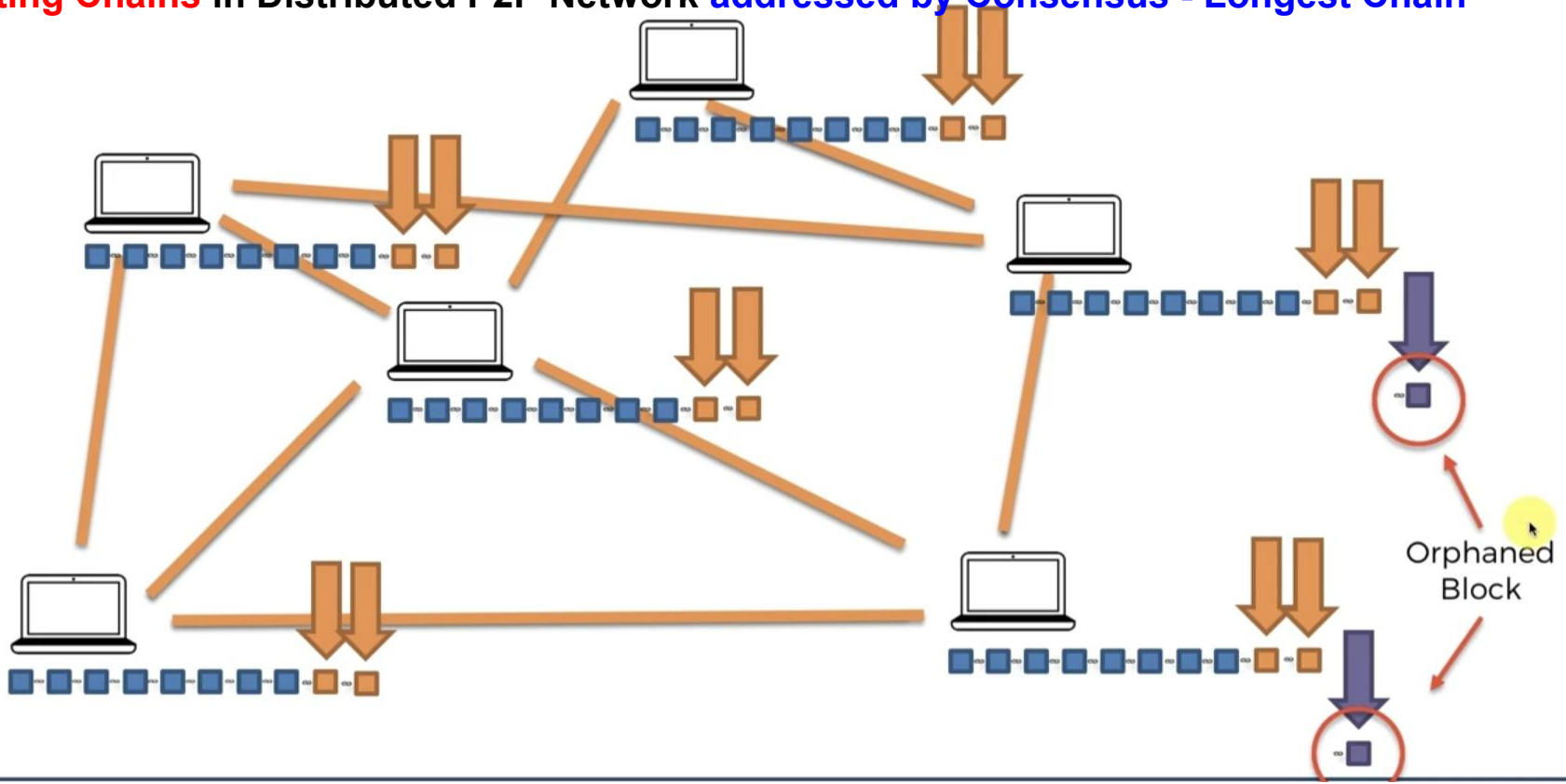
Competing Chains in Distributed P2P Network addressed by Consensus - Longest Chain



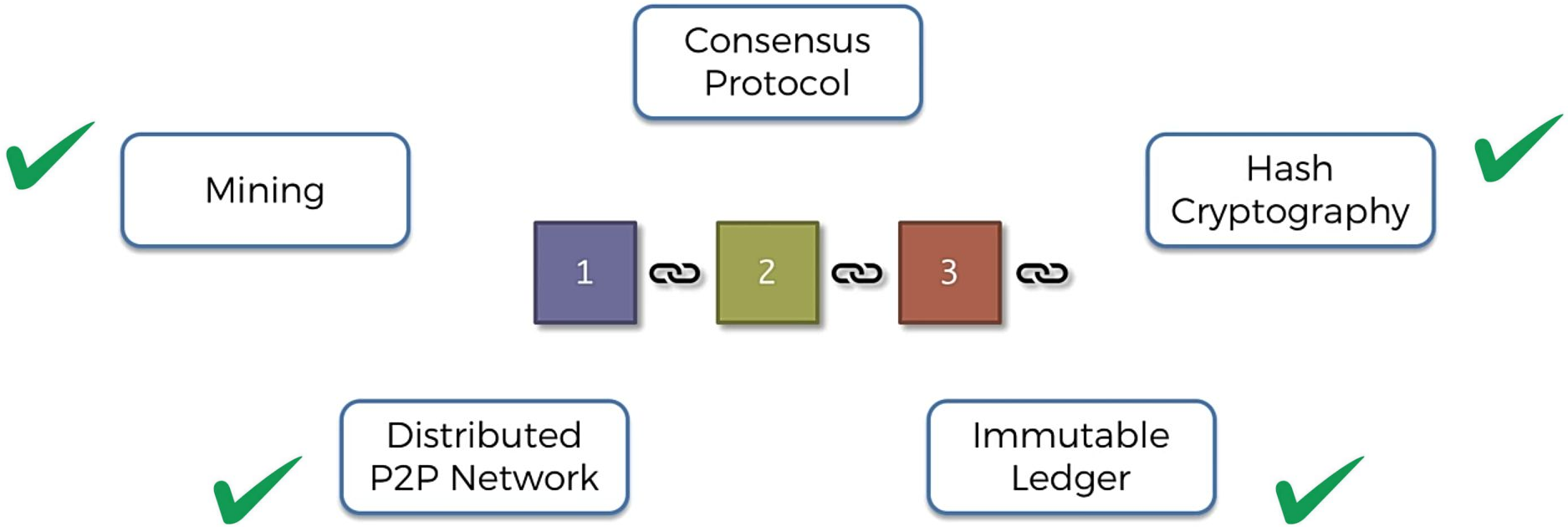
Competing Chains in Distributed P2P Network addressed by Consensus - Longest Chain



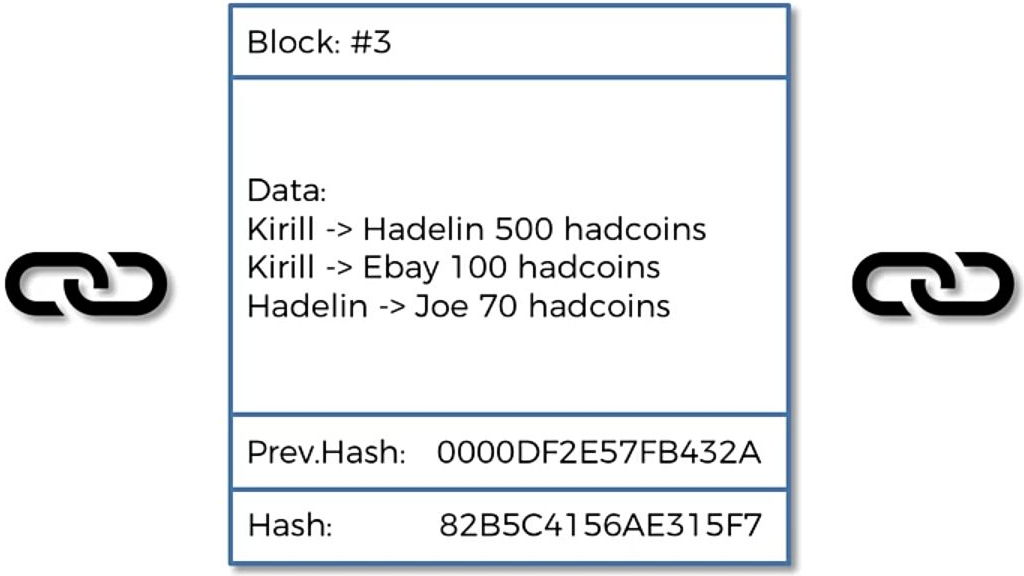
Competing Chains in Distributed P2P Network addressed by Consensus - Longest Chain



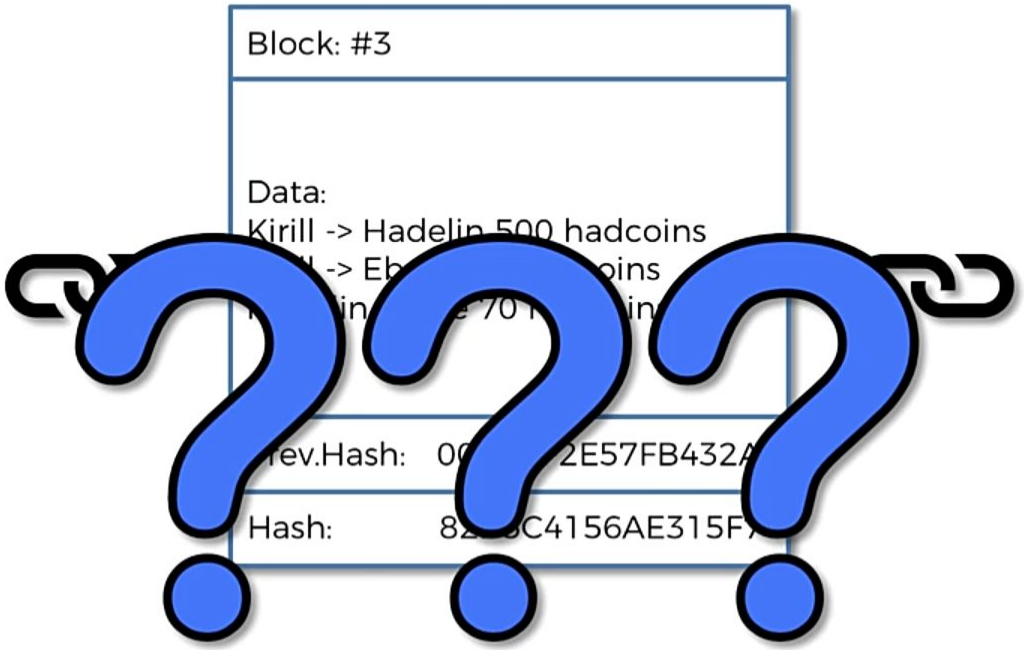
2. Blockchain Fundamentals



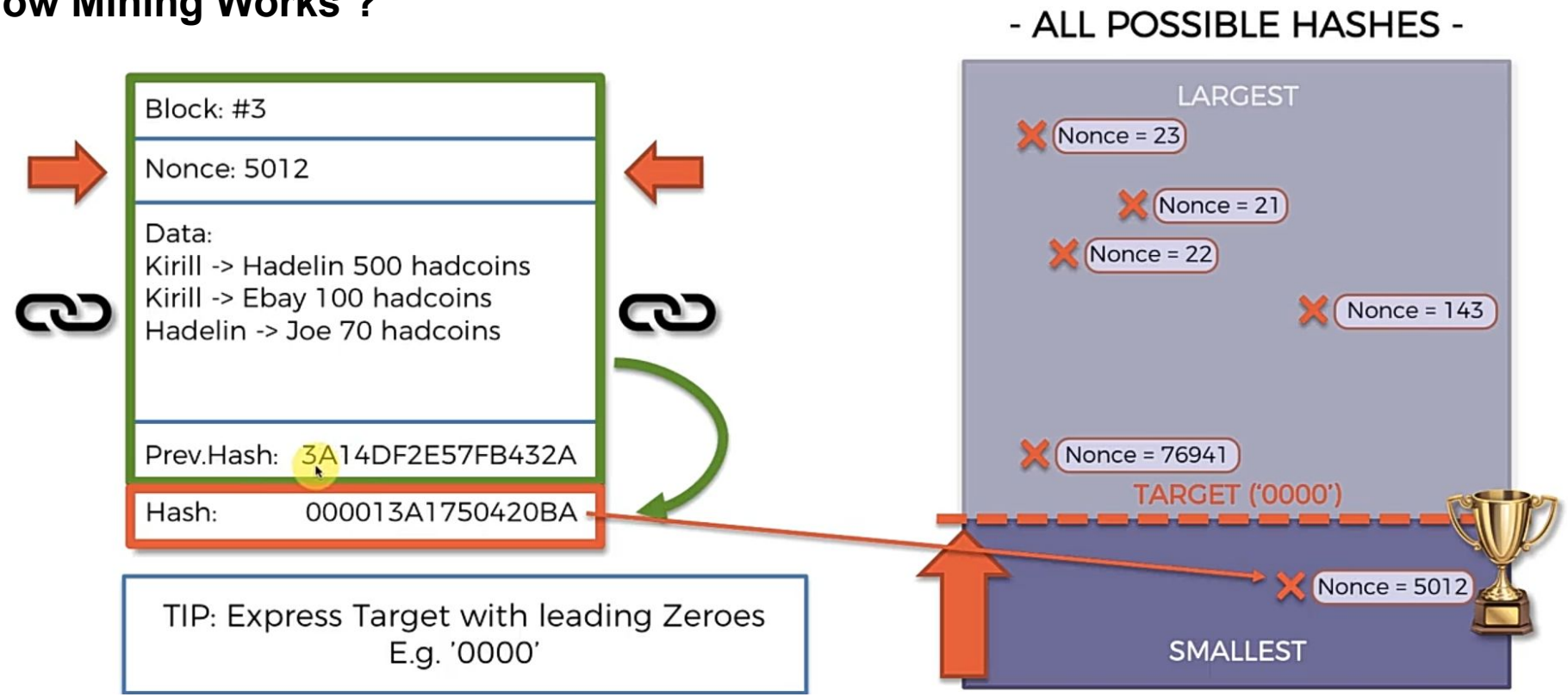
How Mining Works ?



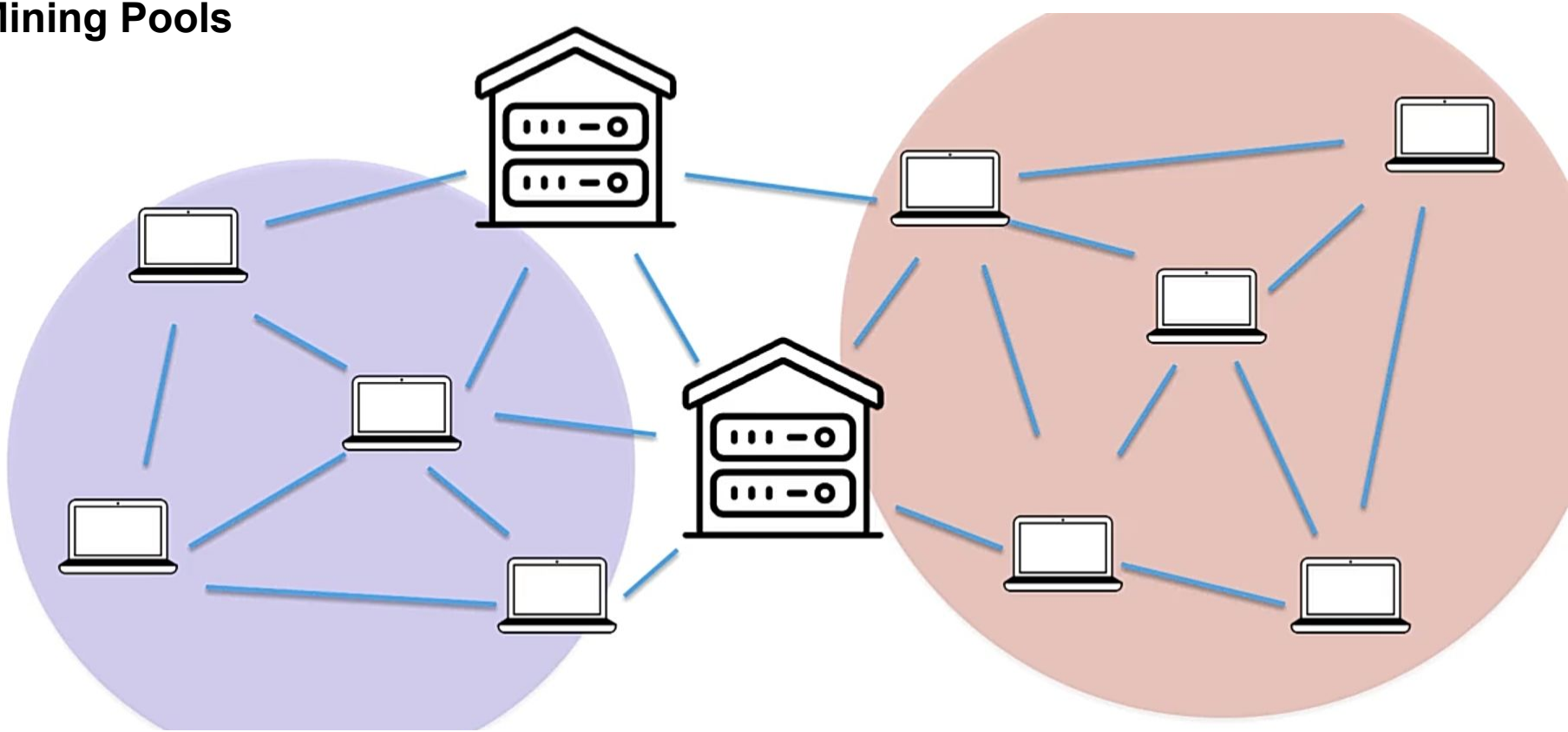
How Mining Works ?



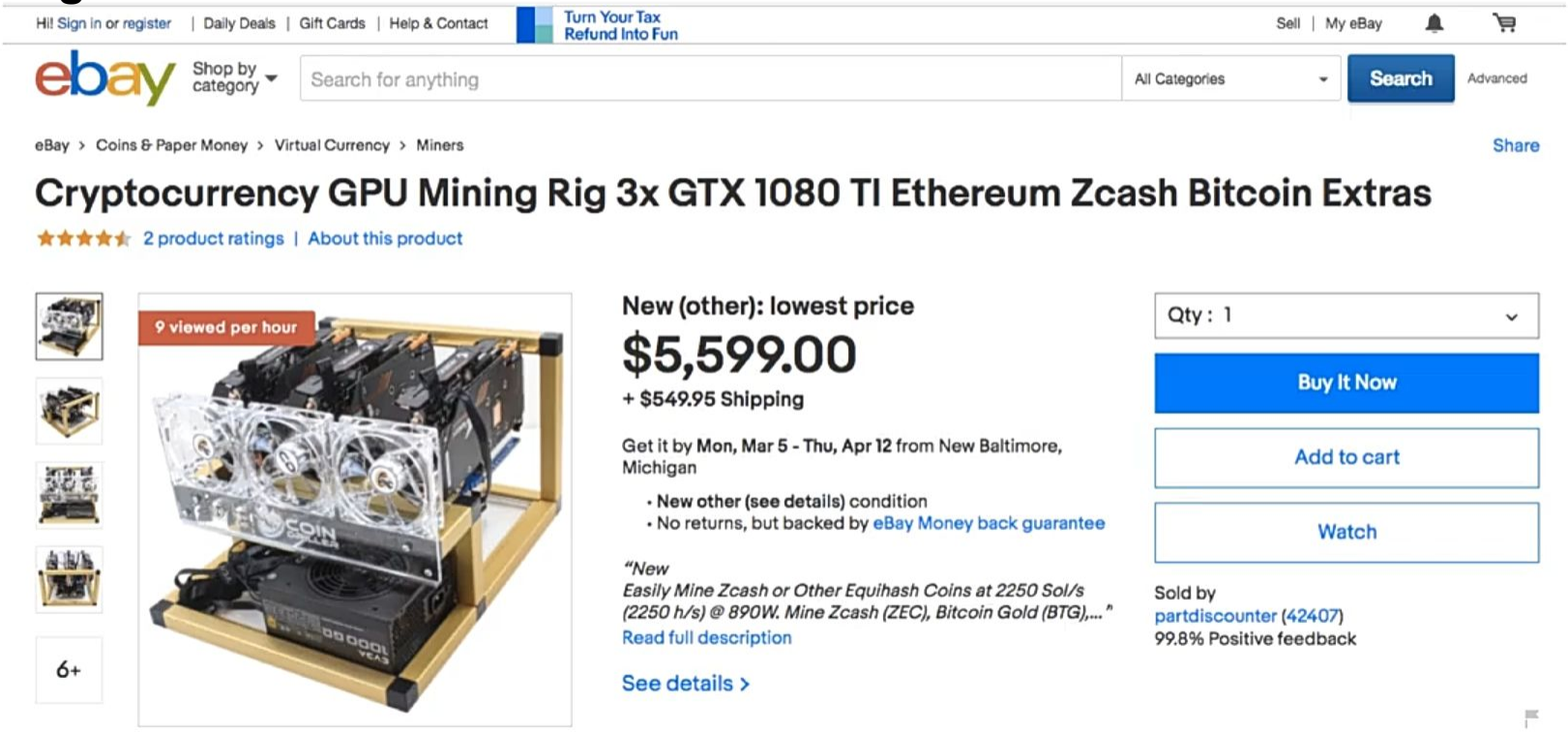
How Mining Works ?



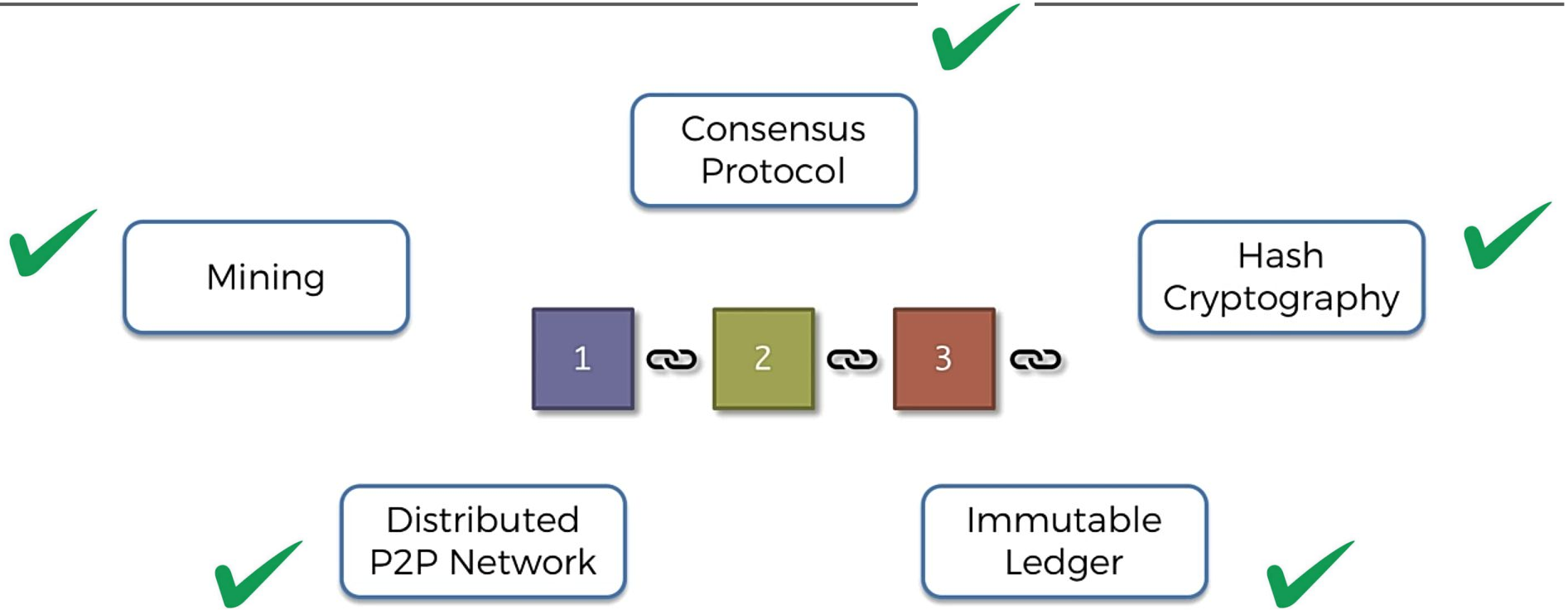
Mining Pools



Mining Pools



2. Blockchain Fundamentals

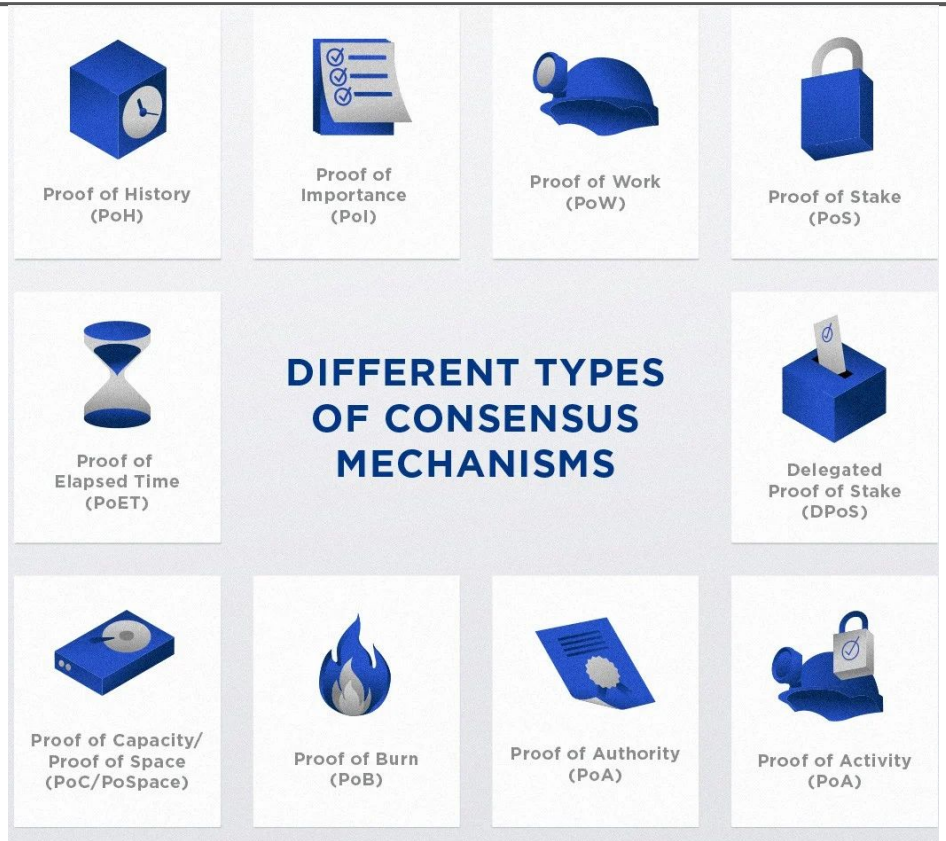


What is Consensus?

- As per Webster dictionary, a consensus is a **general agreement or opinion shared by all the people in a group**.
- A protocol is a **system of standard rules that are acceptable by all parties** to control the exchange of information in a network. Thus, a **consensus protocol** in Blockchain can be defined as **a set of rules and procedures for attaining a unified agreement (consensus) between the participating nodes** on the status of the network.
- The consensus protocol **aims to overcome the classic problem of a distributed computing system known as the Byzantine Generals Problem**

2. Blockchain Fundamentals

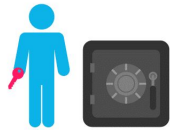
Different Consensus Mechanisms



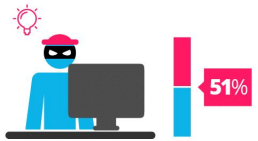
2. Blockchain Fundamentals

Proof of Work vs Proof of Stake

proof of work is a requirement to define an expensive computer calculation, also called mining

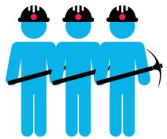


Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.



A reward is given to the first miner who solves each blocks problem.

The PoS system there is no block reward, so, the miners take the transaction fees.



Network miners compete to be the first to find a solution for the mathematical problem

Proof of Stake currencies can be several thousand times more cost effective.

2. Blockchain Fundamentals

	Public	Private	Hybrid	Consortium
Permissioned/ Permissionless	Permissionless	Permissioned	Permissioned & Permissionless	Permissioned
Control	No control by a central authority	Control by a central authority	Control by a central authority	Control by multiple central authorities
Main Advantages	✓ Independence ✓ Transparency	✓ Performance ✓ Scalability	✓ Performance ✓ Low Cost	✓ Performance ✓ Security
Main Disadvantages	✗ Performance ✗ Scalability Issues	✗ Security ✗ Trust	✗ Transparency ✗ Upgrading	✗ Transparency
Examples	Bitcoin Litecoin	Hyperledger Fabric	XRP token	Corda Quorum

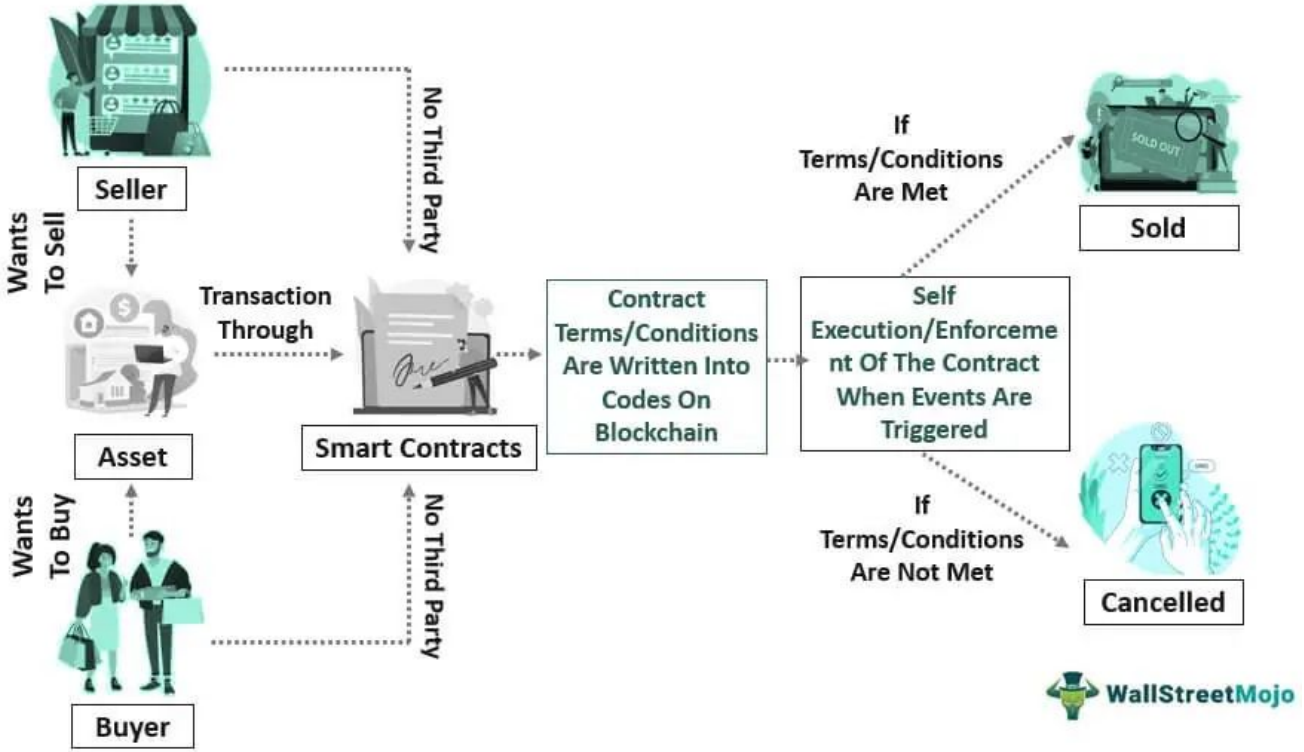
2. Blockchain Fundamentals

Feature	Bitcoin	Ethereum
Purpose	Digital currency	Smart contract platform
Launch	2009	2015
Founder	Satoshi Nakamoto	Vitalik Buterin
Consensus	Proof of Work	Proof of Stake
Supply	Fixed (21M)	No fixed cap

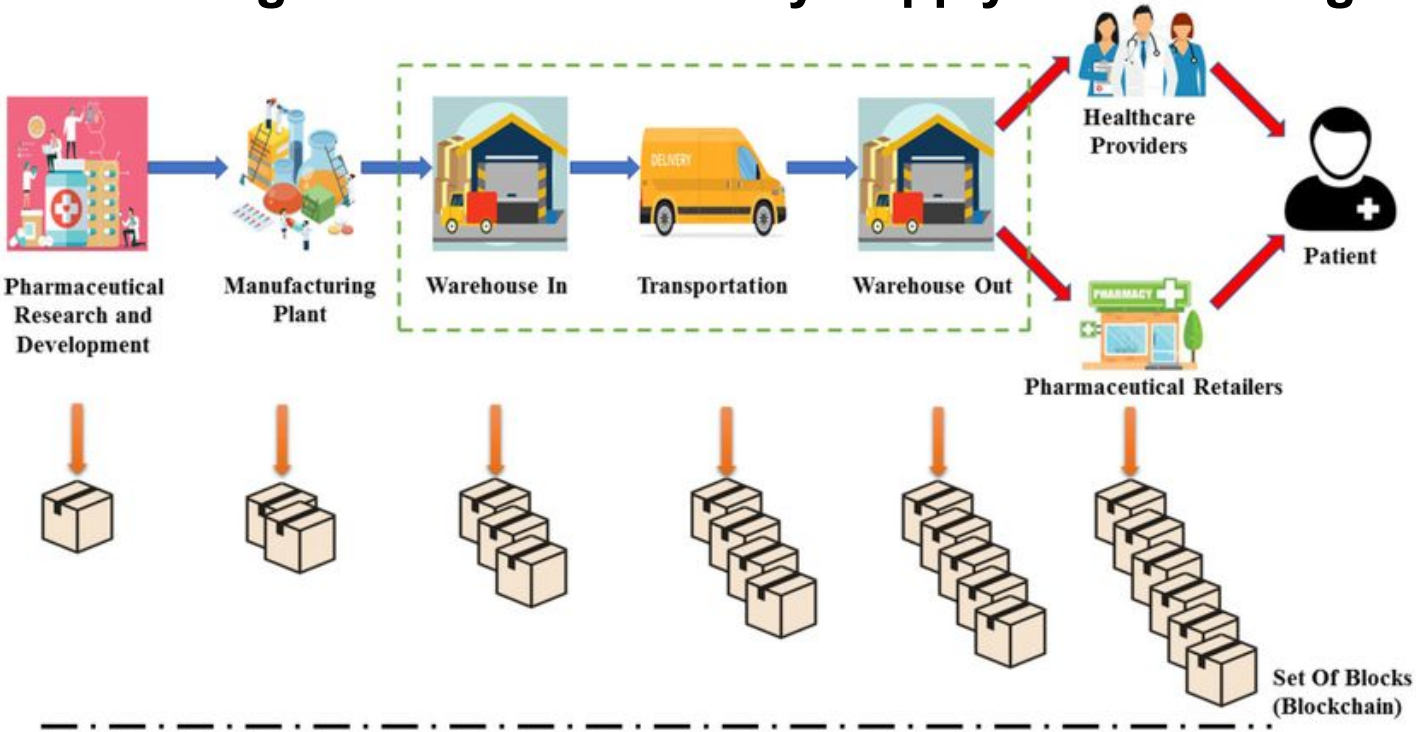
What is a Smart Contract ?

- A **self-executing program** that automates the actions required in an agreement or contract. Once completed, the transactions are trackable and irreversible.
- Smart contracts **permit trusted transactions and agreements to be carried out among disparate, anonymous parties** without the need for a central authority, legal system, or external enforcement mechanism.
- **do not contain legal language**, terms, or agreements
- **Only code that executes actions when specified conditions** are met.
- Nick Szabo, an American computer scientist
  - invented a virtual currency called "**Bit Gold**" in 1998,
  - defined smart contracts as computerized transaction protocols that execute the terms of a contract

Smart Contract Functioning



Blockchain Integration into Pharmacy Supply Chain Management



Topics to be covered

1. Introduction to Blockchain
2. Blockchain Fundamentals
3. **Cryptocurrency Basics**
4. Introduction to Solidity Programming

3. Cryptocurrency Basics

Cryptocurrency as a Form of Currency

- **Cryptos** - Eg. **Bitcoin, Litecoin, Shiba Inu, Dogecoin etc…**
- Various companies and even countries around the world accept some of these digital currencies for conducting transactions.
- However, the **high volatility of Bitcoin and other popular cryptocurrencies makes it unsuitable for everyday use by the public.**

Benefits:

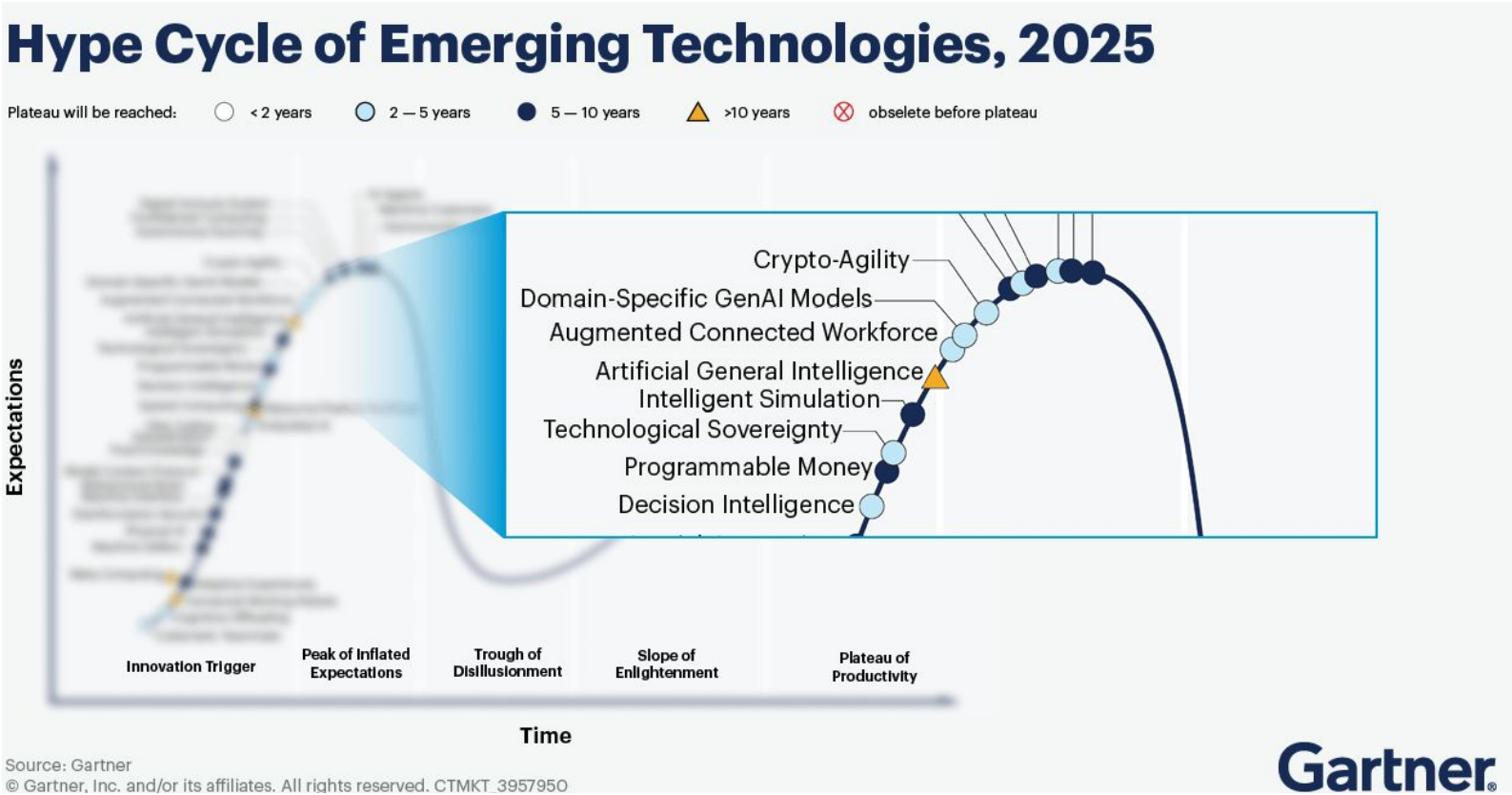
- Faster global transfers with reduced settlement times
- Lower transaction fees eliminating intermediaries
- Enhanced security through decentralization and cryptography
- Financial inclusion for unbanked populations
- Programmability enabling smart contracts and automation

3. Cryptocurrency Basics

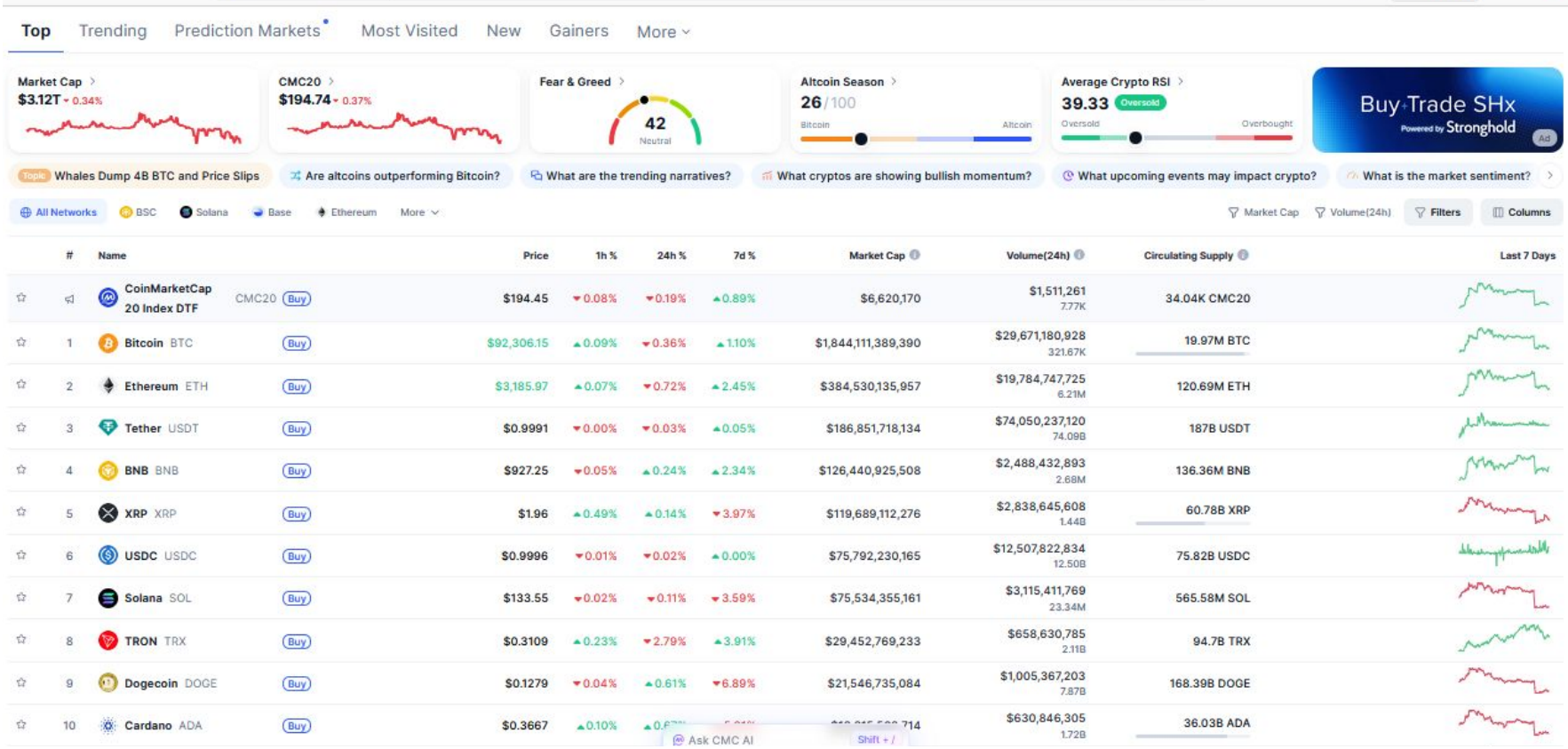
List of Latest Cryptocurrencies to Invest in 2025!

RANK	APPS	RANK	APPS
1	Bitcoin	11	Litecoin
2	Ethereum	12	Chainlink
3	Ripple	13	Tron
4	Solana	14	Tether
5	Dogecoin	15	Dai
6	Binance Coin	16	SKALE
7	Cardano	17	PEPE
8	Avalanche	18	Uniswap
9	Polkadot	19	Bitcoin Cash
10	Stellar	20	Cosmos

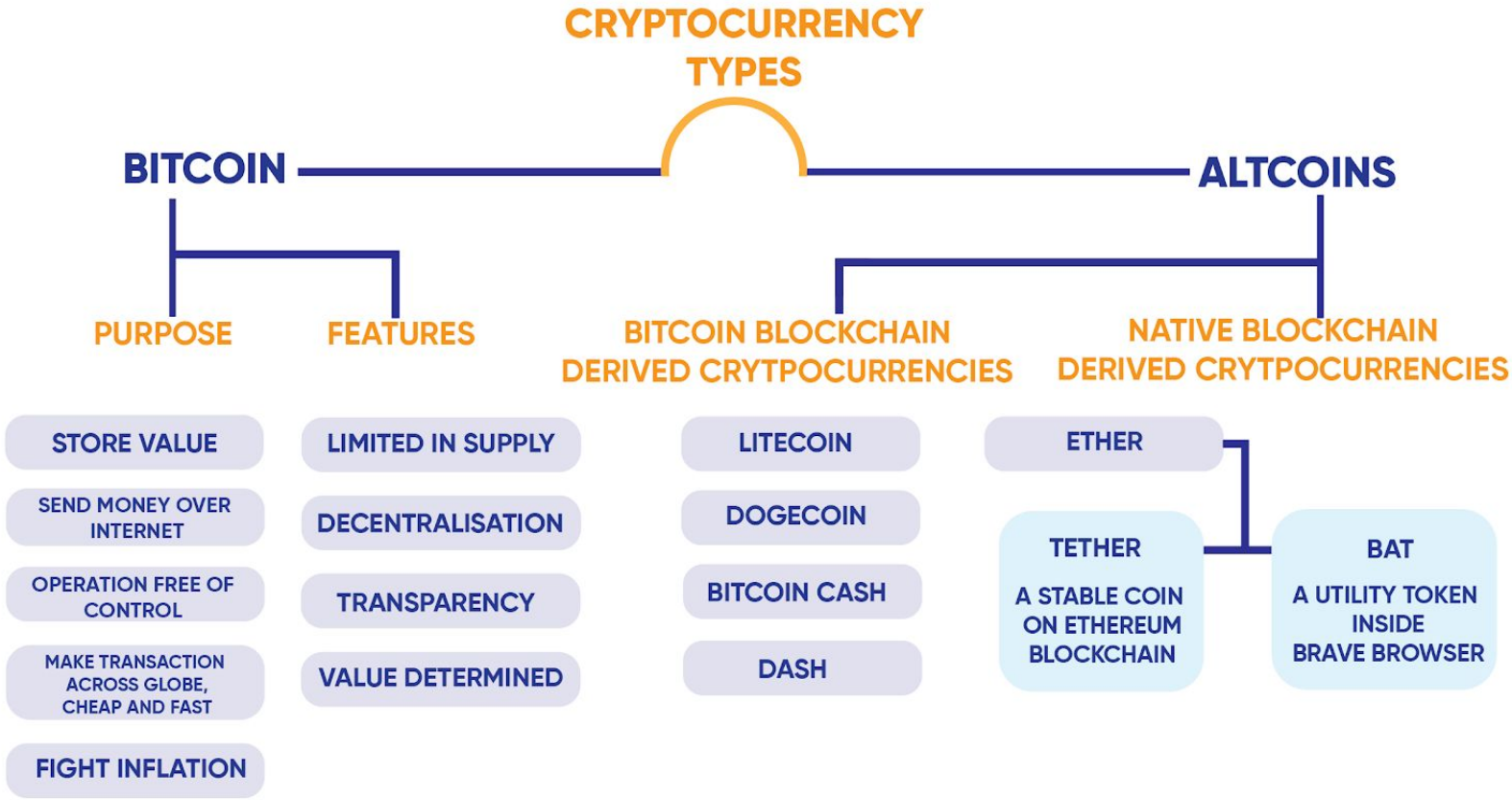
3. Cryptocurrency Basics



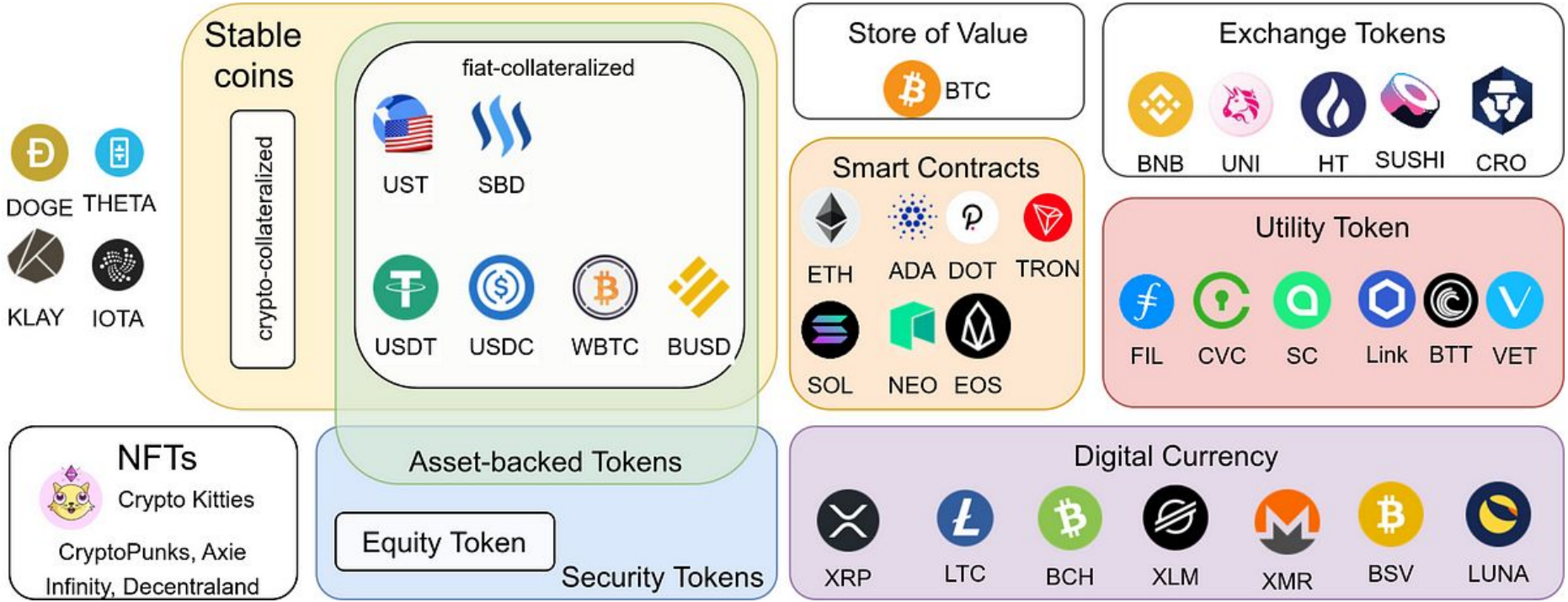
3. Cryptocurrency Basics



3. Cryptocurrency Basics

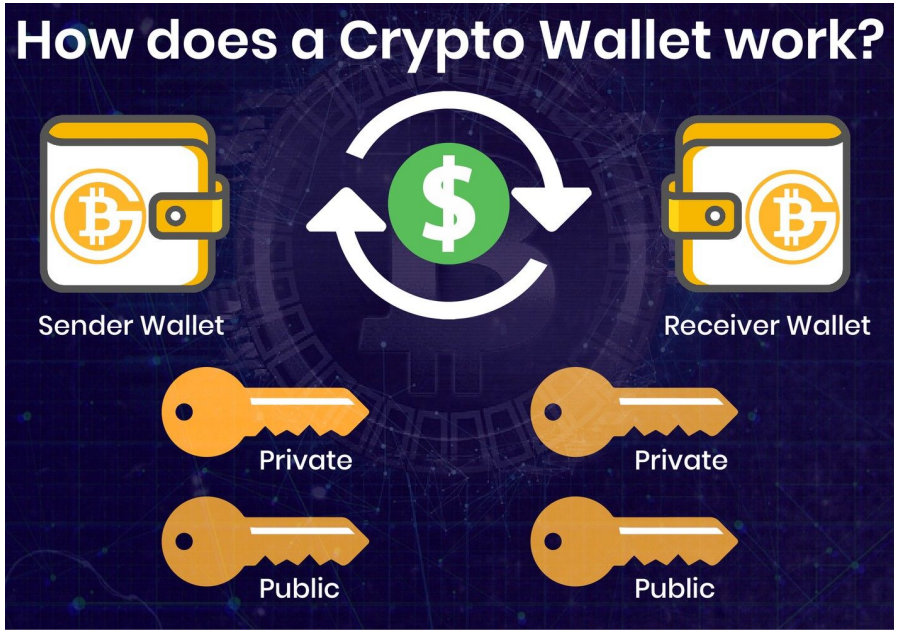


3. Cryptocurrency Basics



3. Cryptocurrency Basics

- **Cryptocurrency wallet** is a **software program that stores your digital money**.
- **store your private keys** - the passwords that give you access to your cryptocurrencies
- Keeps the **crypto safe and accessible.**
- **allow the user to send, receive, and spend cryptocurrencies** like Bitcoin and Ethereum.

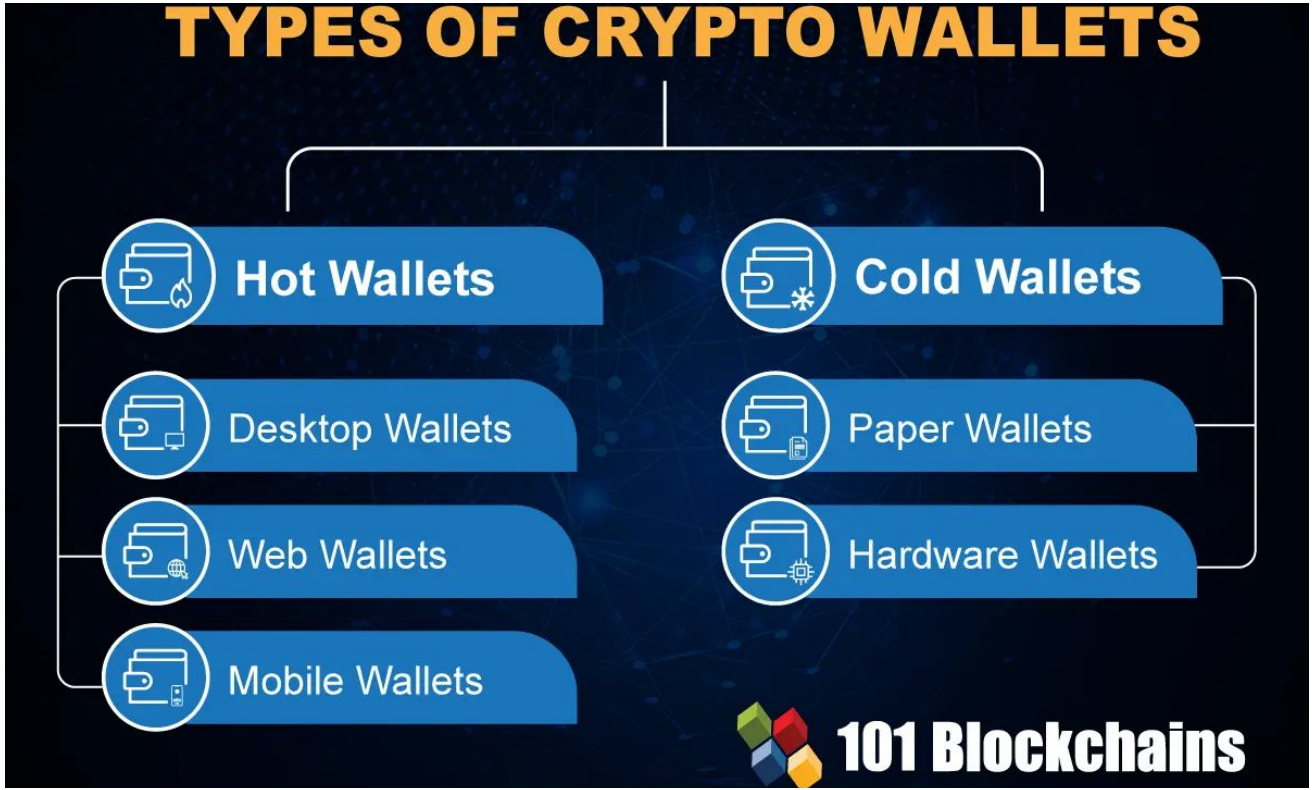


3. Cryptocurrency Basics

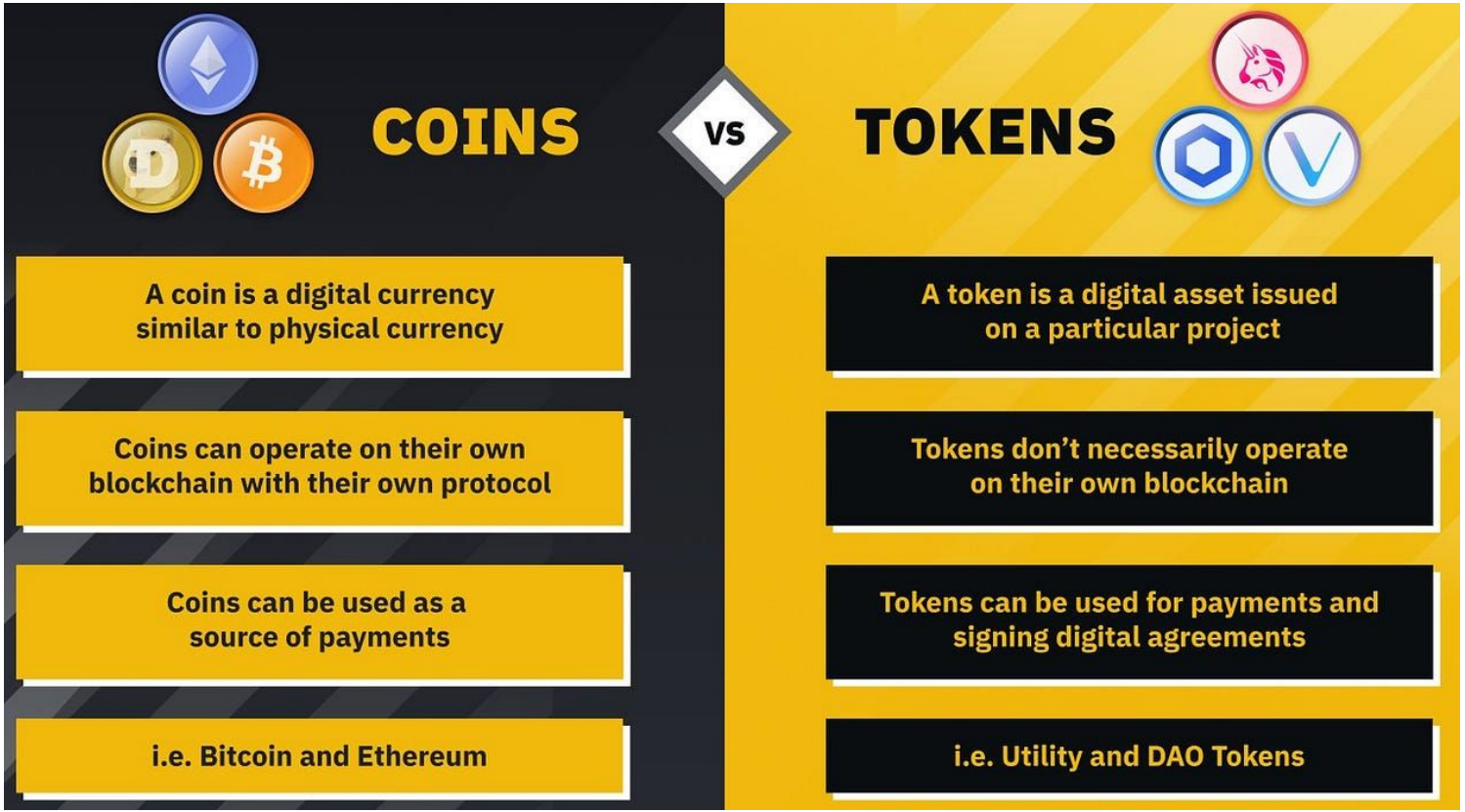
Why are crypto wallets important?

- Normal wallet - holds actual cash,
- Crypto wallets
  - **don't store your crypto** instead store **private keys**
    - used to access live holdings on the blockchain
    - prove the ownership of your digital money
    - Allows to perform transactions.
    - Losing private keys ⇒ losing access to your money.
  - That's why it's i**mportant to keep the hardware wallet safe, or use a trusted wallet provider like Coinbase.**

3. Cryptocurrency Basics



3. Cryptocurrency Basics



3. Cryptocurrency Basics

Aspect	Security Token	Utility Token	Asset Token	Government Token (CBDC)
Primary Purpose	Represents ownership in assets/securities like equity or debt	Provides access to platform services/products	Digitally represents real-world assets (e.g., real estate, commodities)	Central bank-issued digital fiat for payments and monetary policy
Regulation	Treated as securities; SEC/equivalent oversight, KYC/AML required	Often unregulated if not investment contracts; platform-specific rules	Varies; often security-like if fractionalized assets	Fully regulated by central banks/governments
Value Source	Tied to underlying asset performance/dividends	Derived from platform utility/demand	Pegged/mirrors physical asset value	Backed by government/fiat reserves
Transferability	Restricted; secondary markets with compliance	Freely tradable on exchanges	Tradable but may have lockups	Controlled by central bank; programmable limits
Examples	tZERO Polymath (security tokenized stocks)	ETH (network access), BNB (exchange fees)	RealT (property shares), PAXG (gold)	China's e-CNY, Digital Euro pilots
Risk Profile	Investment risk (market/issuer)	Platform adoption risk	Asset volatility + smart contract risk	Sovereign risk; low volatility

Topics to be covered

1. Introduction to Blockchain
2. Blockchain Fundamentals
3. Cryptocurrency Basics
4. **Introduction to Solidity Programming**

4. Introduction to Solidity Programming

- Variables - Local, Global, Variable, State Scope
- Data Types
- Operators - Arithmetic , Relational , Logical , Bitwise , Assignment , Conditional
- Functions
- Loops, if else
- Constructor, Visibility Modifier

4. Introduction to Solidity Programming

LearnETH Platform (RemixIDE) - Beginners Course