Blockchain DLOC Sem VII

NMCPC62 : Cryptocurrency and Blockchain Development

Module - 1: Introduction to Cryptocurrency and Blockchain (7 Hours)

Instructors : Geocey Shejy, Lifna C S, Pradnya Raut

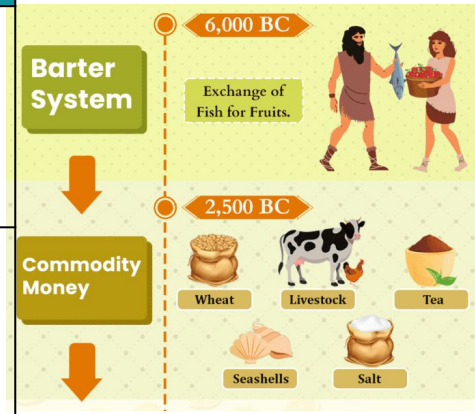
Department of Computer Engineering, VESIT, Mumbai

Topics to be covered

- History and Evolution of Money and Digital Currencies
- Understanding Cryptocurrencies : Concepts, Types, and Benefits
- Blockchain Technology Fundamentals:
  - Cryptography, Hashing,
  - Immutable Ledger
  - Distributed P2P Network - Challenges & Solution, Double Spending Problem, 51% Attack
  - Mining - Working, Mining Difficulty, Mining Pools, How do mempool works ?
  - Consensus Mechanisms - Proof of Work (PoW), Proof of Stake (PoS), Alternatives - Byzantines Generals Problem, Byzantine Fault Tolerance
- Applications of Blockchain Beyond Cryptocurrencies (Supply Chain, Healthcare, etc.)
- Blockchain's Role in Decentralization and the Future of Web3

History and Evolution of Money and Digital Currencies

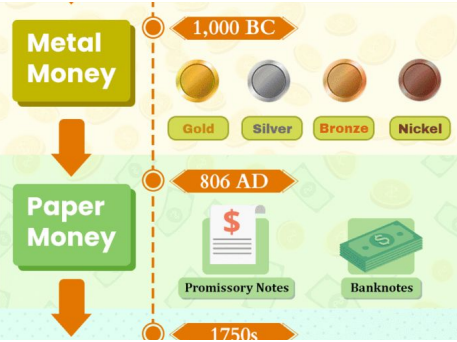
Evolution Stage	When, Where & Why Did It Start?	Examples
Barter System	**When?:** Around 6,000 BC **Where?:** Mesopotamia; later adopted by Phoenicians. **Why?:** In early societies, people often had more of some goods and less of others. To get what they needed, they traded their extra goods with others who had what they wanted.	Food, spices, weapons.
Commodity	**When?:** Around 2,500 BC **Where?:** Mesopotamia **Why?:** Issues were arising in the barter system. For instance, one person might have milk and need grains, but the person with grains doesn't need milk. It also became hard for businesses to get the resources they needed. So, people started using specific items as money.	Barley, wheat, livestock, cocoa beans, tea, tobacco, salt, seashells.



Courtesy :
https://www.educba.com/evolution-of-money/

History and Evolution of Money and Digital Currencies

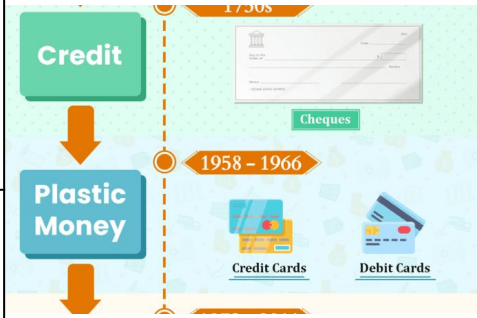
Evolution Stage	When, Where & Why Did It Start?	Examples
Metal Coins	**When?:** Around 1,000 BC **Where?:** China **Why?:** People found that commodities were hard to store & transport, perished quickly, and had different trade values. So, they started using metals like gold and silver to make coins. These coins were long-lasting and easier to carry and trade than commodities.	Electrum coins (gold-silver alloy), gold coins, silver coins, Bronze coins, Nickel coins.
Paper Money	**When?:** 806 AD **Where?:** China **Why?:** Trading large amounts of money with coins became a problem. So, during the Tang dynasty, people used paper bills (promissory notes) as a promise of the amount they would pay. True paper money didn't come in use until the 11th century, during the Song dynasty.	Promissory notes, Exchange certificates, Banknotes.



Courtesy :
https://www.educba.com/evolution-of-money/

History and Evolution of Money and Digital Currencies

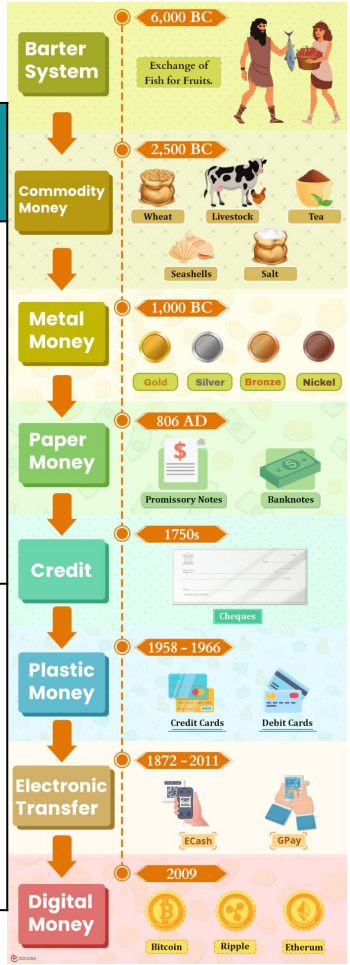
Evolution Stage	When, Where & Why Did It Start?	Examples
Credit	**When?:** Early 1750s **Where?:** England **Why?:** Working on the promissory note system, people started using checks, which were handwritten notes known as drawn notes. It was to streamline payment procedures and reduce risks.	DD, Cheques.
Plastic Money	**When?:** 1958 (Credit Card), 1966 (Debit Card) **Where?:** Fresno, California (Credit Card), Delaware (Debit Card) **Why?:** Instead of carrying paper money around, Bank of America introduced the first credit card, working on a similar concept of credit that had already been in use. Later, as an alternative to carrying cash or a checkbook, the Bank of Delaware started a pilot program for debit cards.	Credit cards, Debit cards.



Courtesy :
https://www.educba.com/evolution-of-money/

History and Evolution of Money and Digital Currencies

Evolution Stage	When, Where & Why Did It Start?	Examples
Electronic Transfer	**When?:** 1872 (Telegraph), 2011 (GPay) **Where?:** Denver, Colorado, by Western Union **Why?:** Western Union started the first telegraph transfer to make it easier to send money across borders or to distant places. It allowed people to send money using the telegraph. By the 1990s, banks introduced Internet banking, which let customers manage their accounts and transactions online with a computer. Then, in 1998, Peter Thiel, Max Levchin, Luke Nosek, Ken Howery, and Yu Pan started PayPal, making digital payments simpler.	Telegraph wire transfer, ecash, Paypal, Google Pay, PhonePe, Bhim.
Digital Money	**When?:** 2009 (Bitcoin) **Where?:** Unknown **Why?:** Satoshi Nakamoto, whose true identity is still unknown, created the first cryptocurrency, Bitcoin, in 2009. Seeing people frustrated with online transactions and worried about the global economy, Nakamoto wanted to give individuals more control over their money. Using a consensus-based approach, the idea was to create a system where no third party had exclusive control over money.	Bitcoin, Ripple, Ethereum, Dogecoin



Courtesy :
https://www.educba.com/evolution-of-money/

Understanding Cryptocurrencies : Concepts, Types, and Benefits

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.**

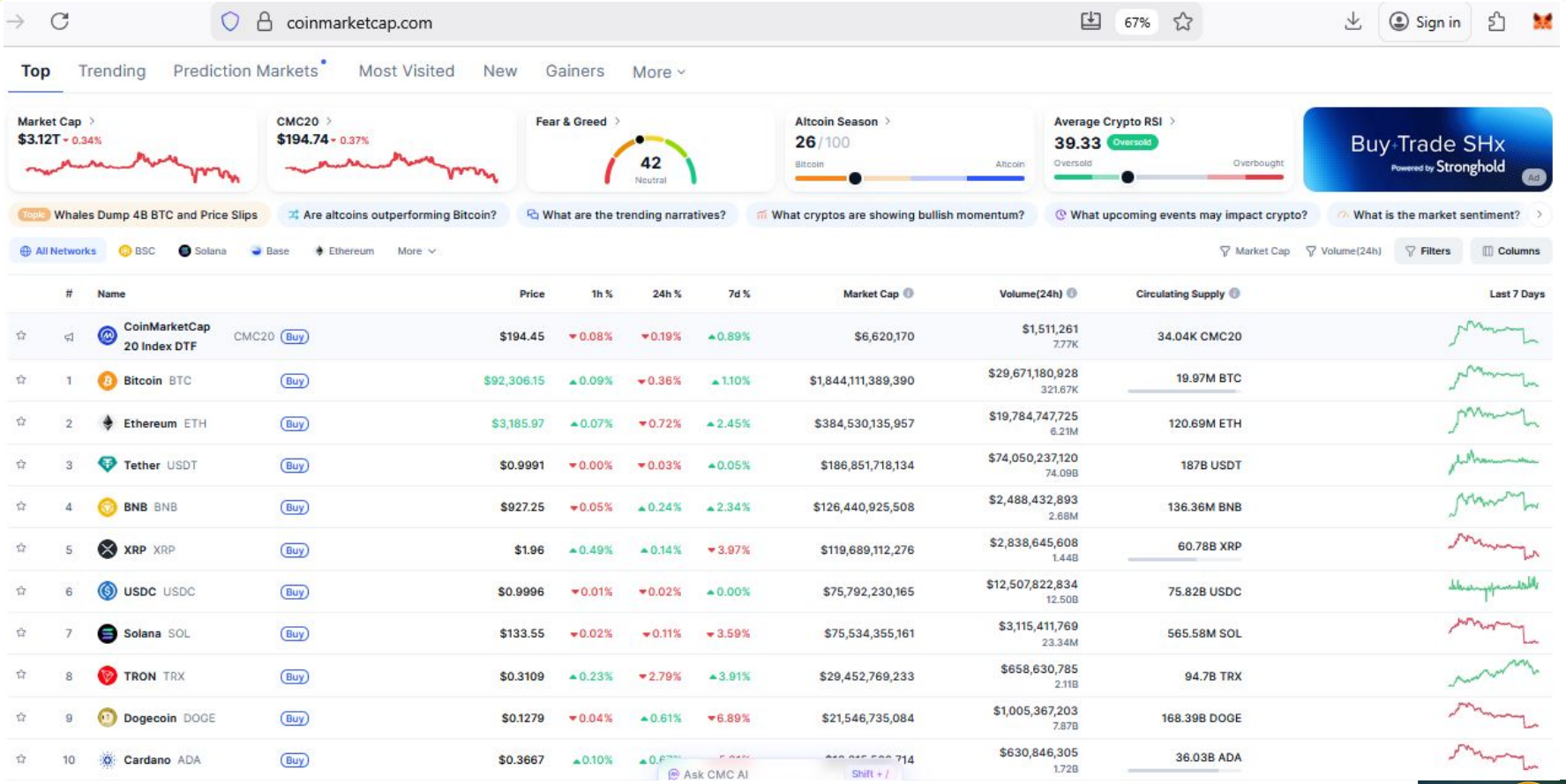
Understanding Cryptocurrencies : Concepts, Types, and Benefits

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

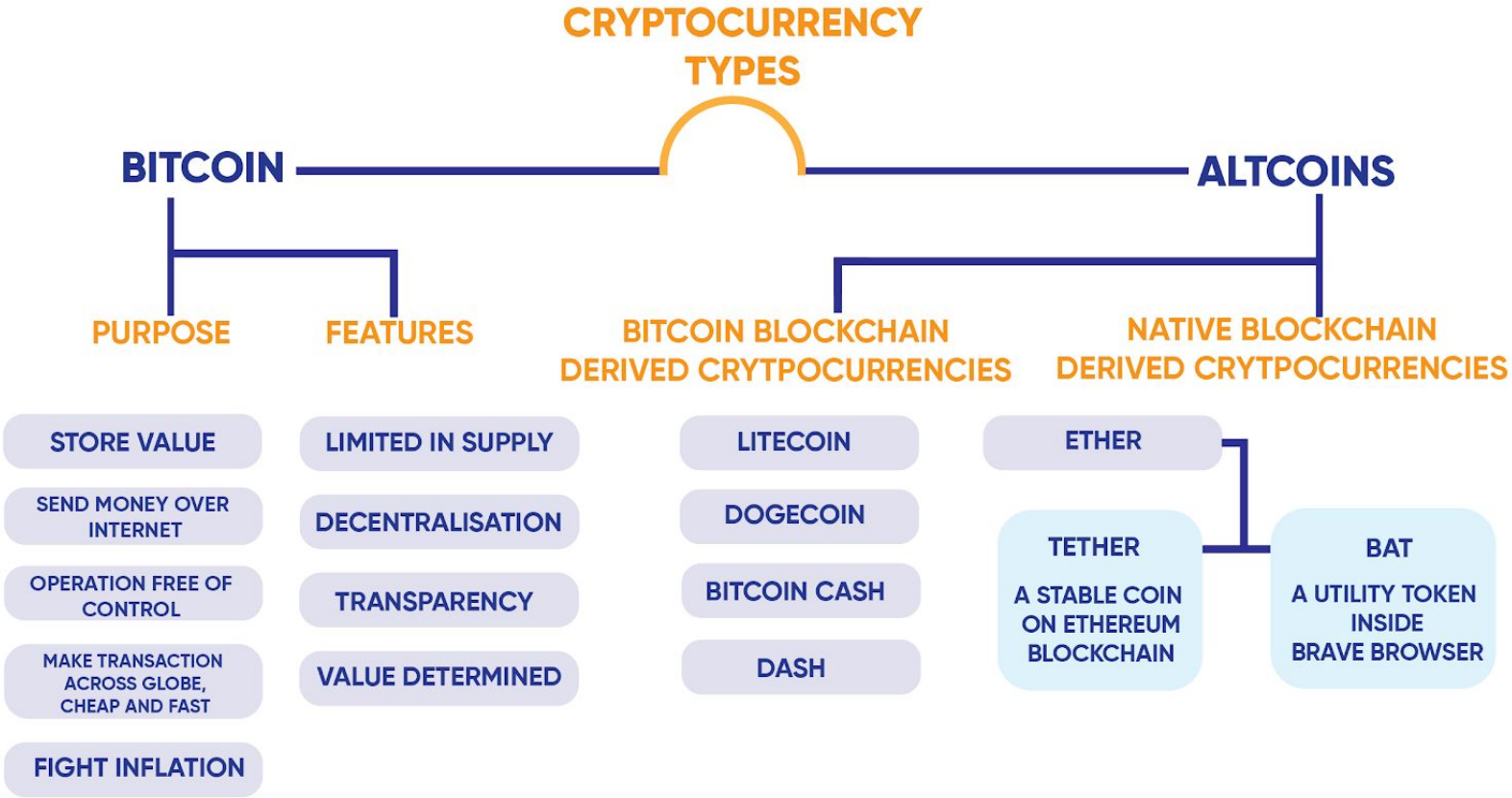
Courtesy :DevTechnoSys

Understanding Cryptocurrencies : Concepts, Types, and Benefits



Courtesy :Coin Market Cap

Understanding Cryptocurrencies : Concepts, Types, and Benefits



Understanding Cryptocurrencies : Concepts, Types, and Benefits

BitCoin

- Launched in **2009**
- **world's largest cryptocurrency** by market capitalization.
- Bitcoin is **created, distributed, traded, and stored using a decentralized ledger system (**Blockchain)
- Bitcoin and its ledger are **secured by proof-of-work (PoW) consensus,**
- Bitcoin can be **purchased via various cryptocurrency exchanges.**
- **first decentralized virtual currency**
- provides **secure global transactions quickly and without third-party manipulations**.
- **created to address the inefficiencies in global financial systems**.
- Bitcoin is **not issued by any government**, and **banks do not manage accounts or validate transactions.**
- It is **based on a cryptographic system** that uses certain codes and numbers to keep information safe and secure.
- **stored in digital wallets that allow users to manage and trade their coins.**
- **currently accepted as a means of payment for products sold or services provided.**
- **offers lower transaction fees compared to traditional online payment mechanisms.**
- However, **the value of Bitcoin has been extremely volatile over the past few years.**

Courtesy : JAKE FRANKENFIELD

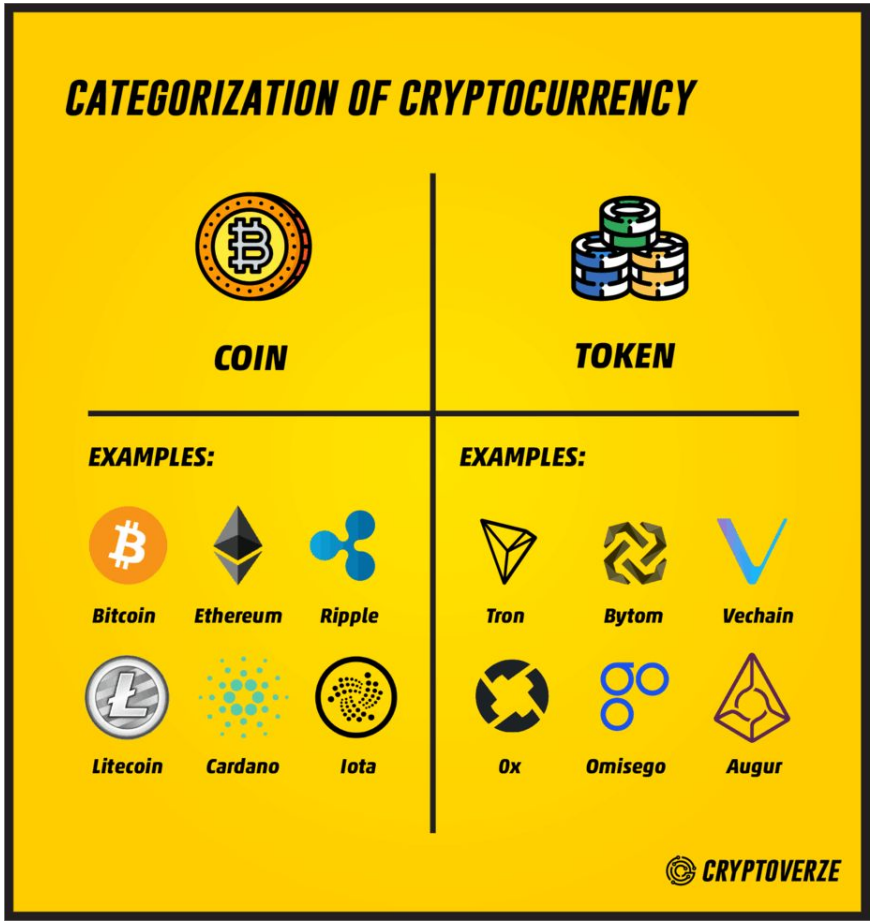
Understanding Cryptocurrencies : Concepts, Types, and Benefits

Altcoins or Alternative Coins

- **Describe all cryptocurrencies other than Bitcoin**.
- These coins also **use blockchain technology that allows secure peer-to-peer transactions**.
- Altcoins were built on the success of Bitcoin by **slightly changing the rules to appeal to different types of users**.
- They essentially **solve the inefficiencies of Bitcoin**.
  - **Litecoin** - *address issues related to scalability, higher transaction time & charges, and environmental concerns*
  - **Ether** - *created based on the idea that blockchain tech can be used to create applications that go beyond just enabling a digital currency.*
- There are **more than 10,000 altcoins** in existence today.
- Altcoins come in **several types based on what they were designed for.**

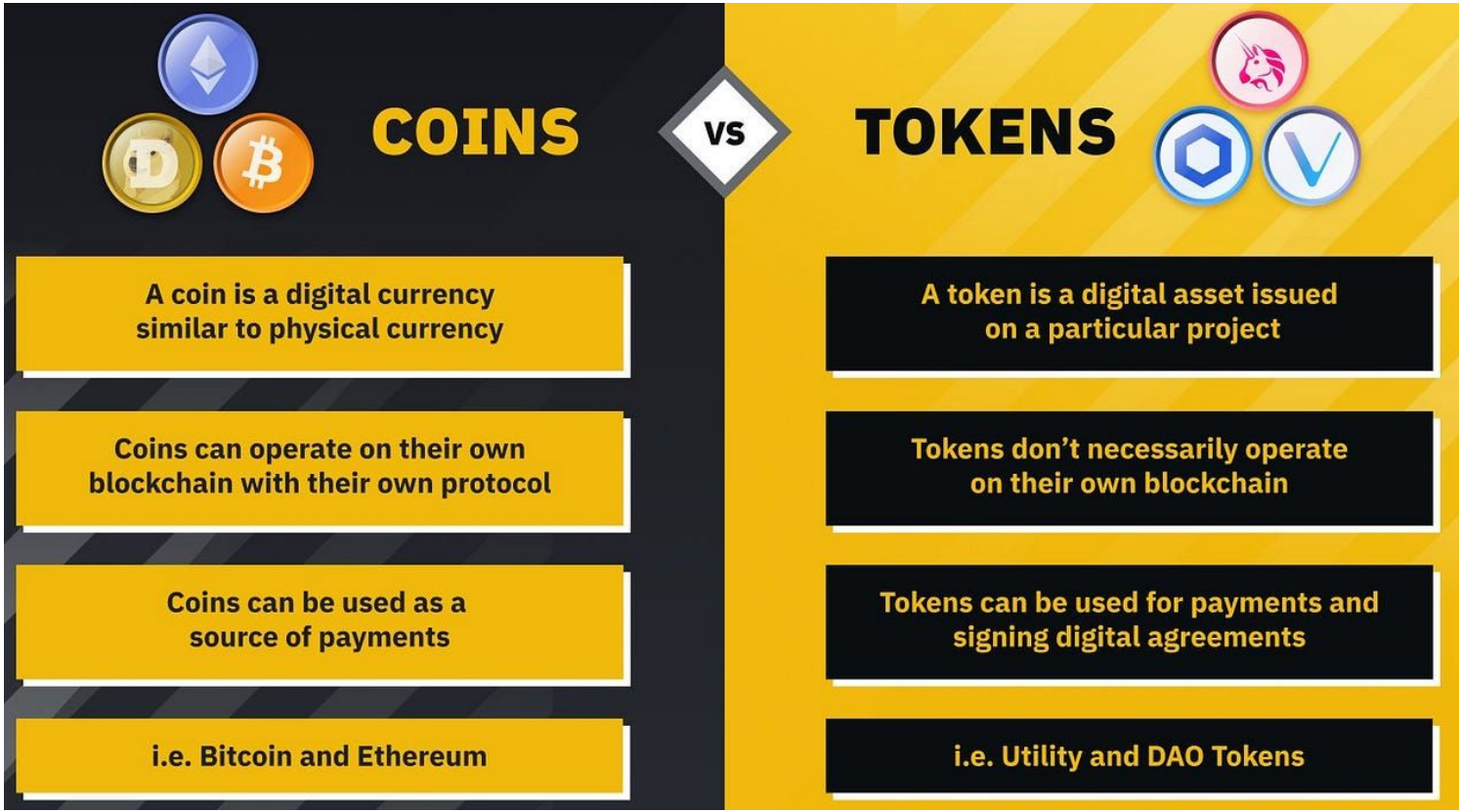
Courtesy : JAKE FRANKENFIELD
Cherian Varghese

Understanding Cryptocurrencies : Concepts, Types, and Benefits

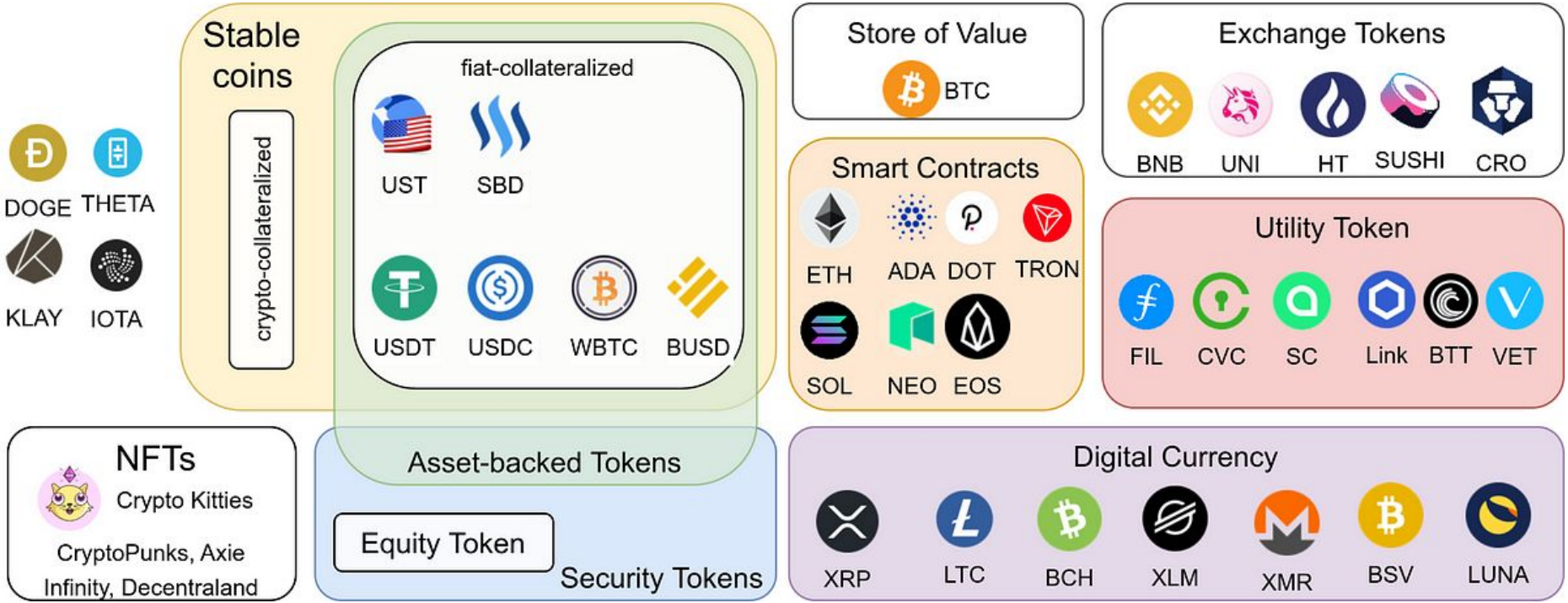


Courtesy : CoinCrunch - Medium

Understanding Cryptocurrencies : Concepts, Types, and Benefits



Understanding Cryptocurrencies : Concepts, Types, and Benefits



Courtesy : Martin Thoma

Understanding Cryptocurrencies : Concepts, Types, and Benefits

Stablecoins

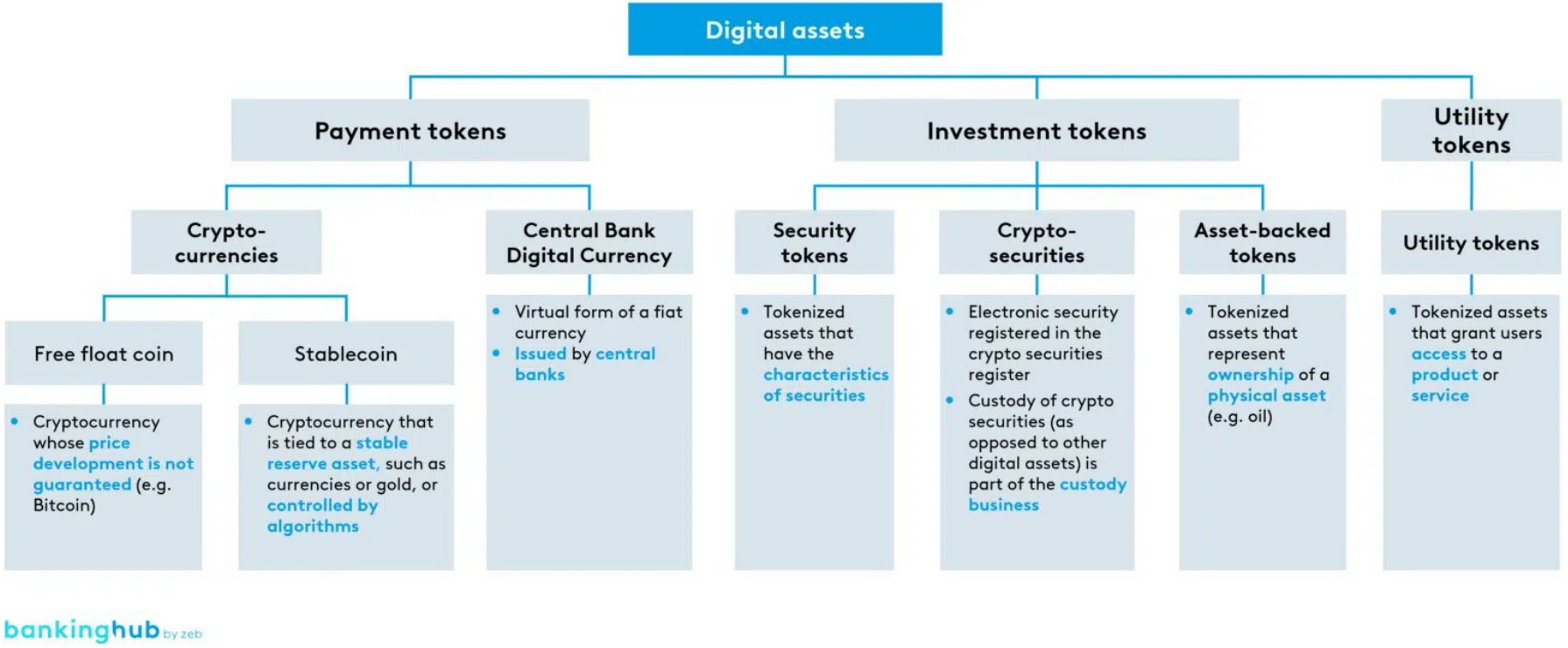
- **Class of cryptocurrencies backed by reserve assets** (cash or commodity).
- **offer price stability while ensuring all basic features or benefits of cryptocurrencies.**
- Provides **instant processing and security of payments.**
  - **1 Tether (USDT)** is pegged to (or **backed by) 1 US Dollar**, as fiat currencies are pegged to an underlying asset such as gold or foreign exchange reserves, **their valuations remain free from wild movements.**
  - **PAX Gold,** a digital token **backed by physical gold**. (currently, **1 PAXG is nearly 30 grams**)
- The basket is meant to act as a reserve to redeem holders if the cryptocurrency fails or faces problems. Price fluctuations for stablecoins are not meant to exceed a narrow range.

Courtesy : JAKE FRANKENFIELD
Cherian Varghese

Understanding Cryptocurrencies : Concepts, Types, and Benefits

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

Understanding Cryptocurrencies : Concepts, Types, and Benefits



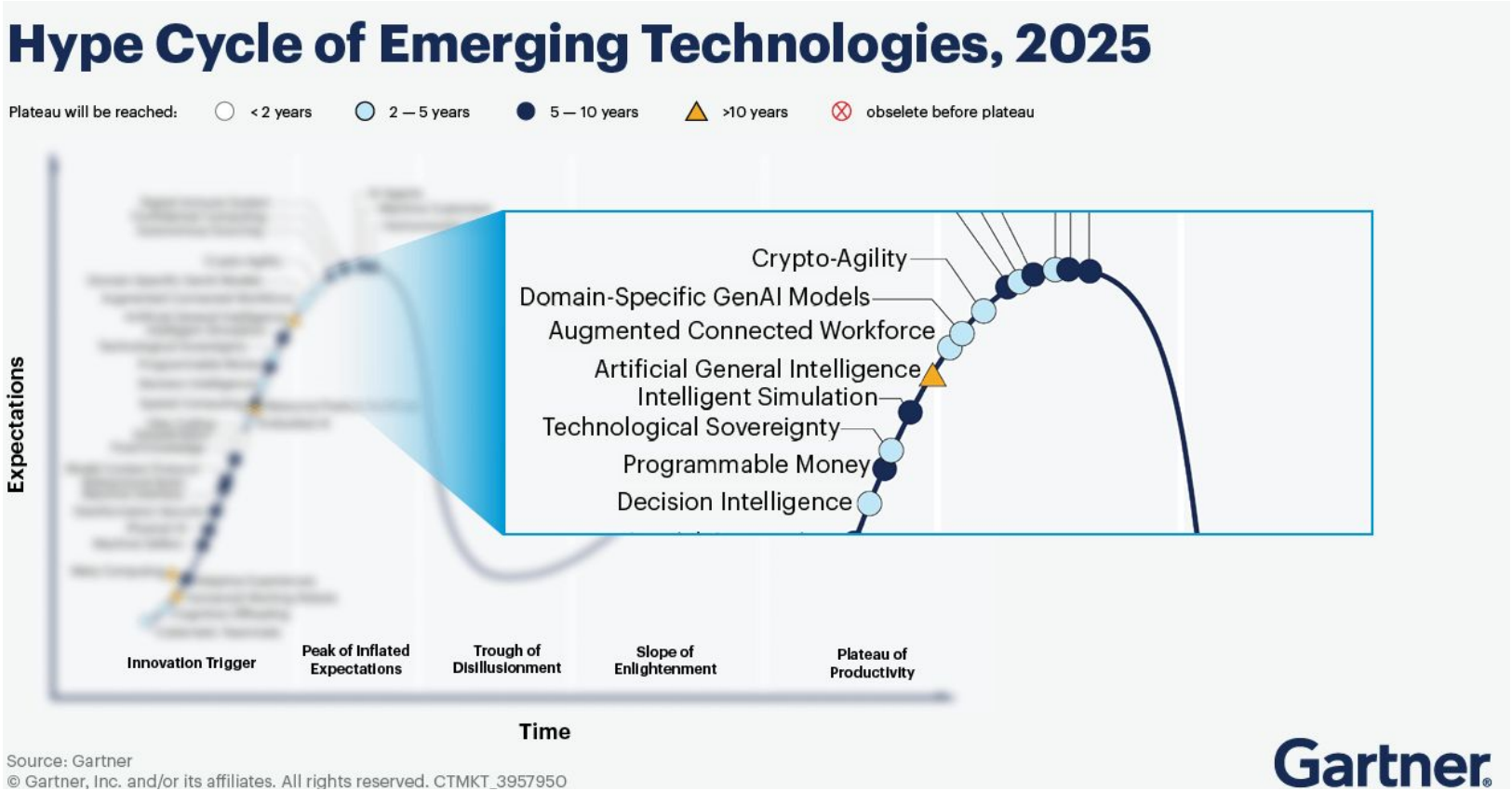
Courtesy : BankingHub

Understanding Cryptocurrencies : Concepts, Types, and Benefits

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

Courtesy : BankingHub



Courtesy : Gartner Hype Cycle

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

What is Blockchain ?

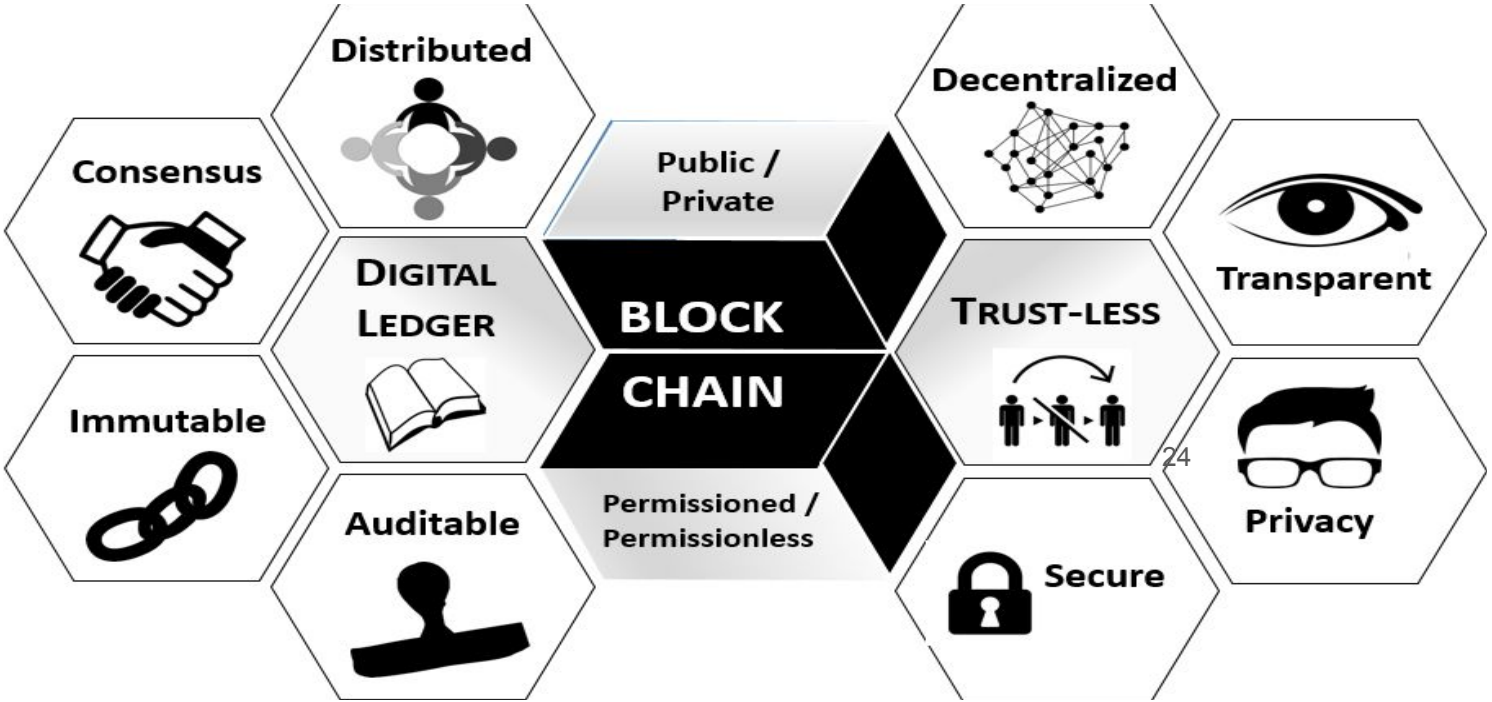
- A Blockchain is "an **open**, **distributed ledger** that can record transactions between two parties **efficiently** and in a **verifiable** and **permanent** way" (Iansiti, Lakhani 2017)

- The keywords: **Open** (accessible to all), **Distributed or Decentralized** (no single party control), **efficient** (fast and scalable), **verifiable** (everyone can check the validity of information), **permanent** (the information is persistent)

What is 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**.

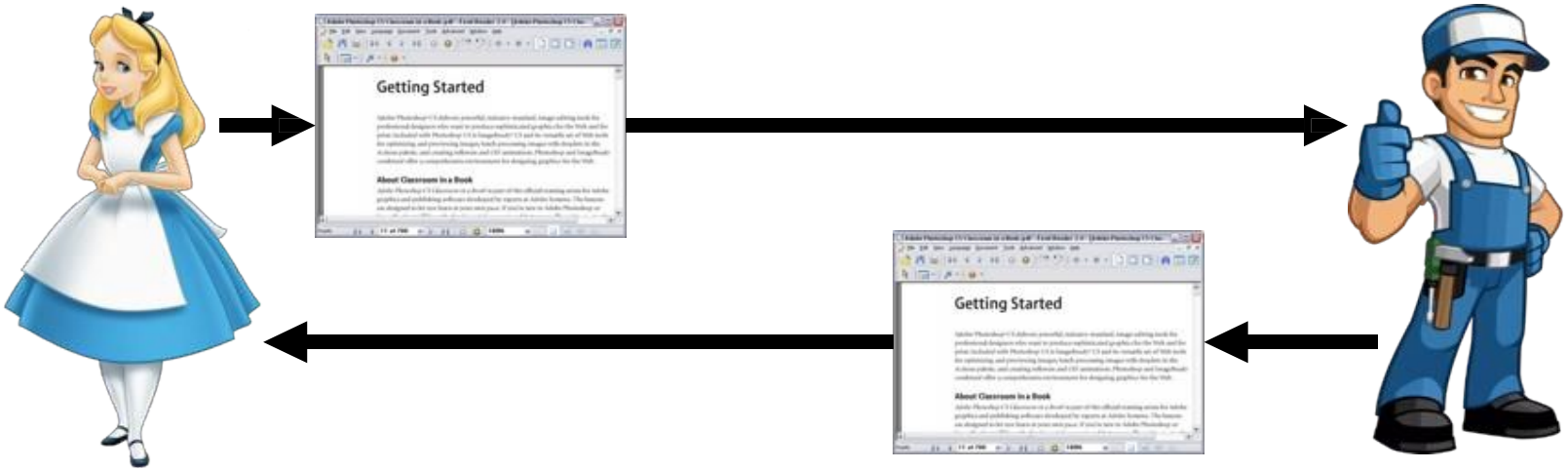
Characteristics of Blockchain



Courtesy : Chandramouli et.al

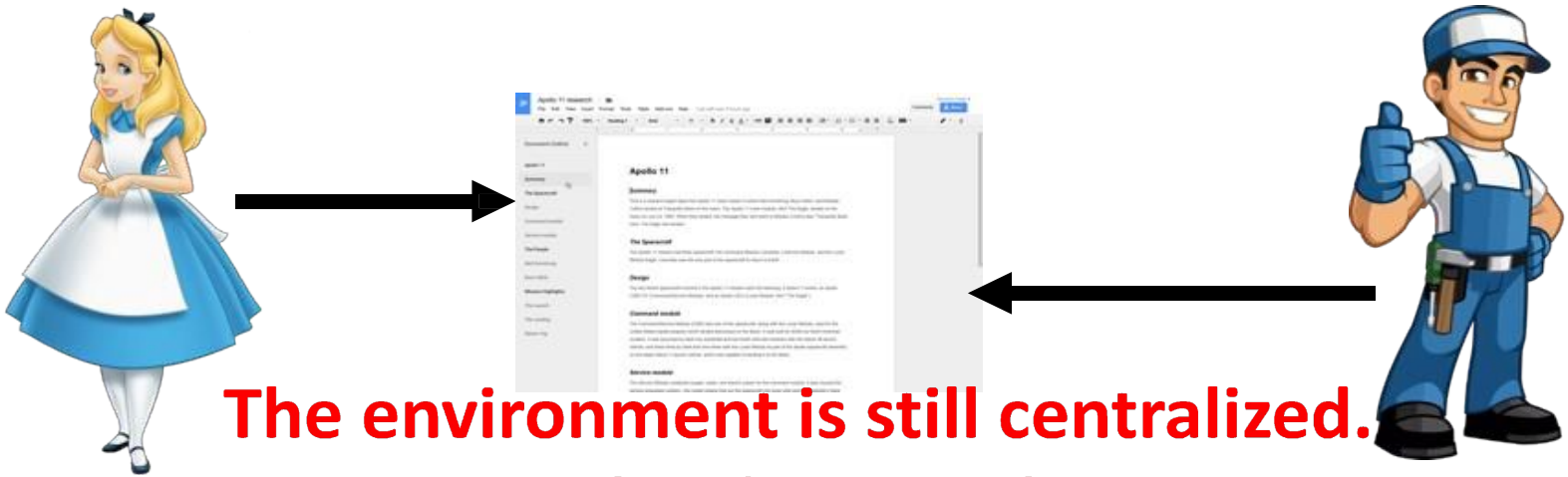
Example Scenario

Traditional way of sharing documents



Example Scenario

- Shared Google doc – both the users can edit simultaneously



The environment is still centralized.

Does centralized system harm?

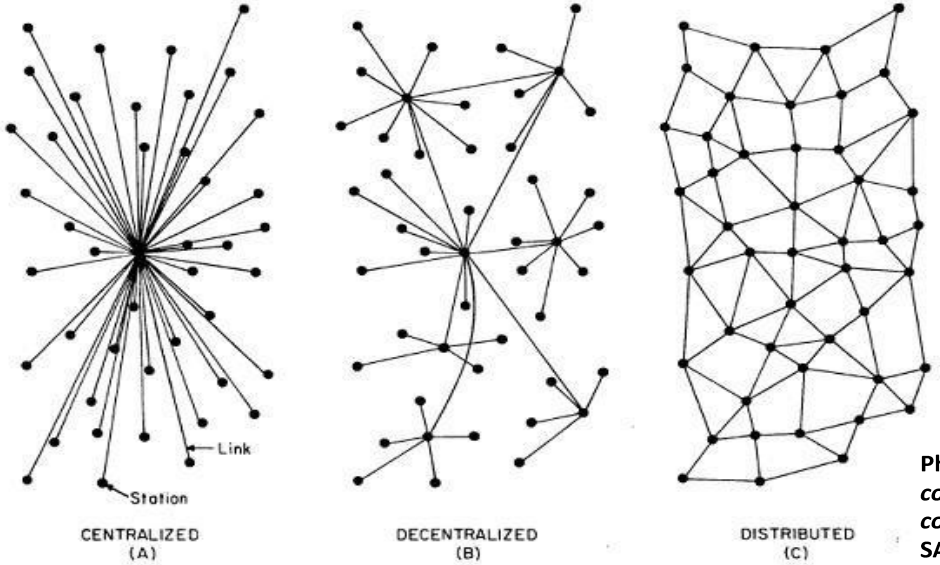
Example Scenario

Problems with a Centralized System

A single point of failure

- If you do not have sufficient bandwidth to load Google doc, you'll not be able to edit
- What if the server crashes?

Centralized vs Decentralized vs Distributed

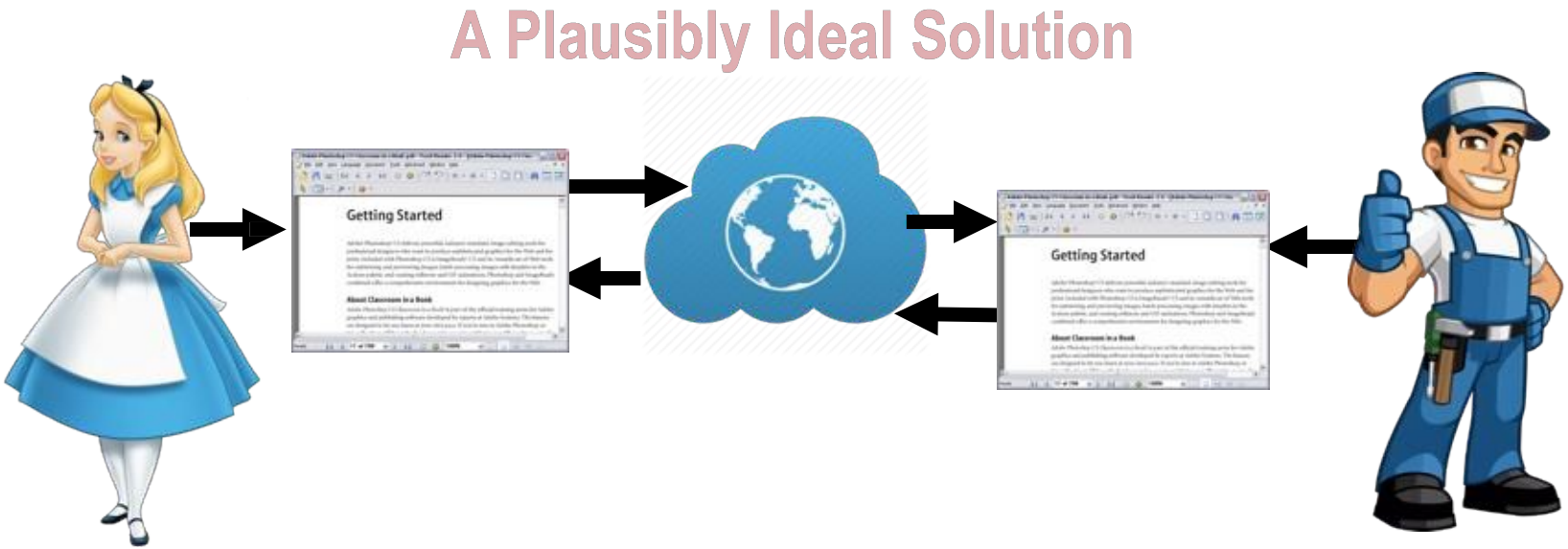


Complete reliance on single point (centralized) is not safe

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

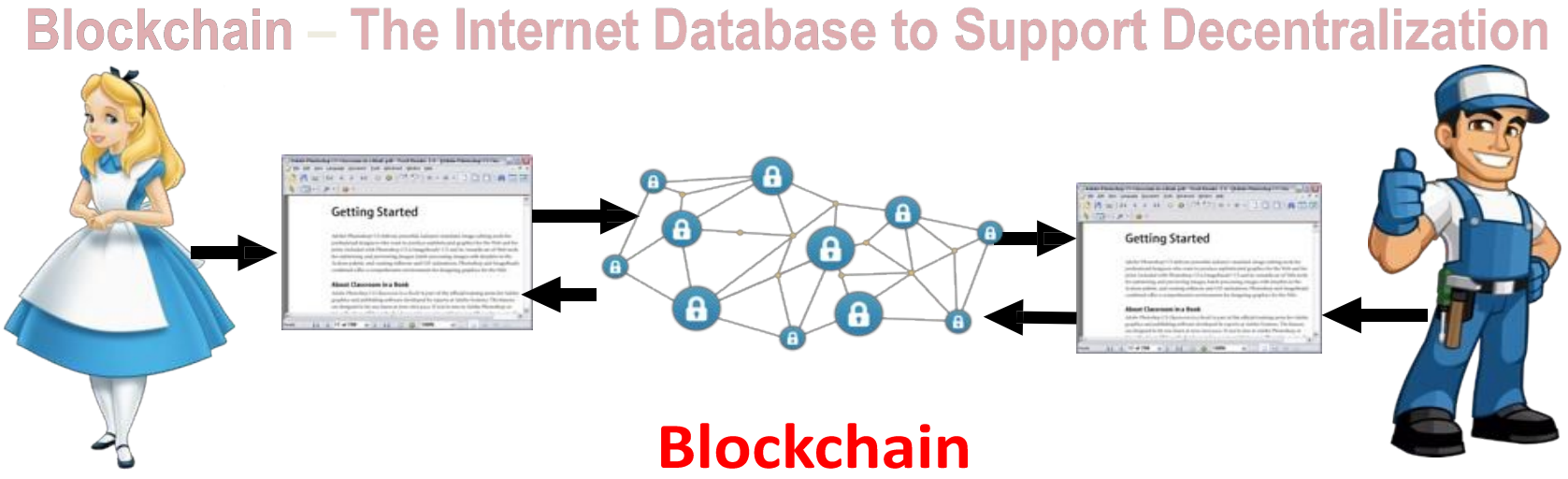
Photo courtesy: Baran, Paul. *On distributed communications: I. Introduction to distributed communications networks.* No. RM3420PR. RAND CORP SANTA MONICA CALIF, 1964.

Example Scenario



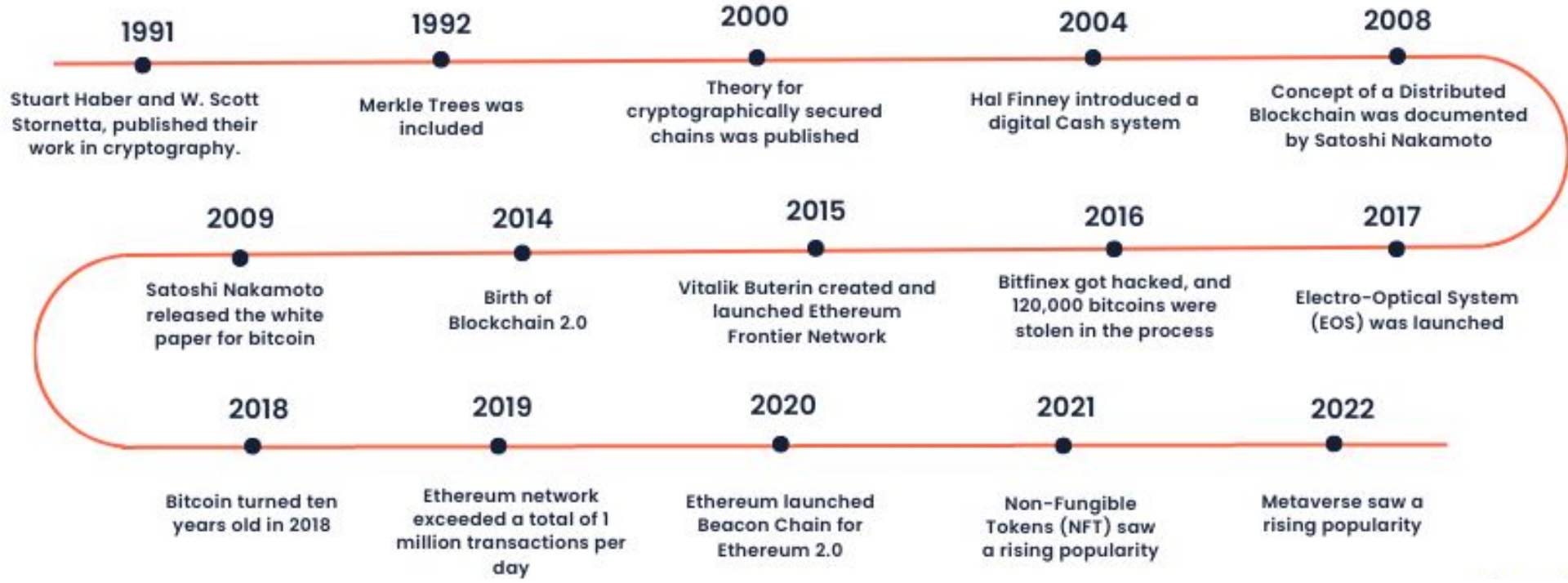
Everyone edits on their local copy of the document – the Internet takes care of ensuring consistency

Example Scenario



A decentralized database with strong consistency support

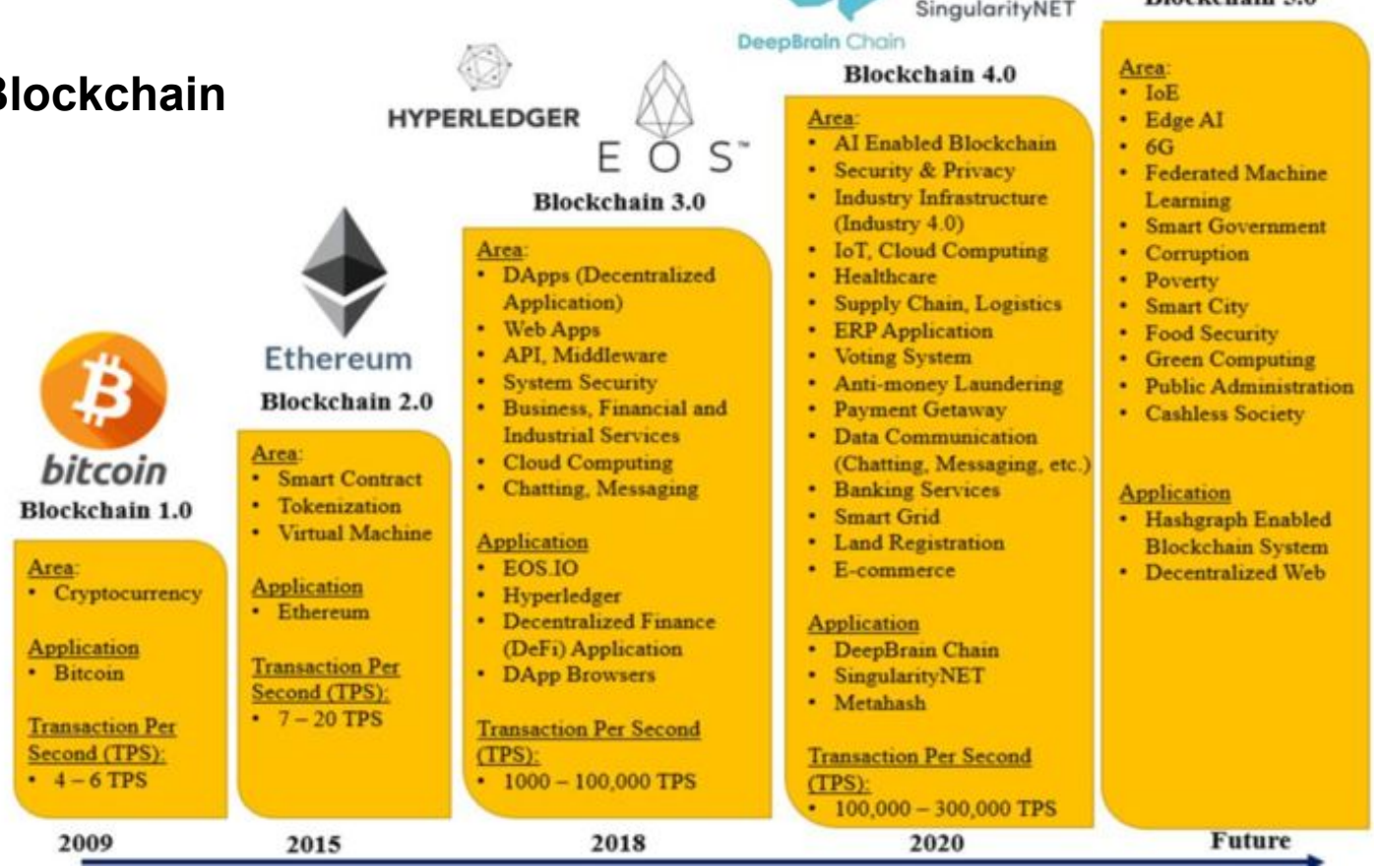
Blockchain History Timeline



Courtesy : Knowledge Academy

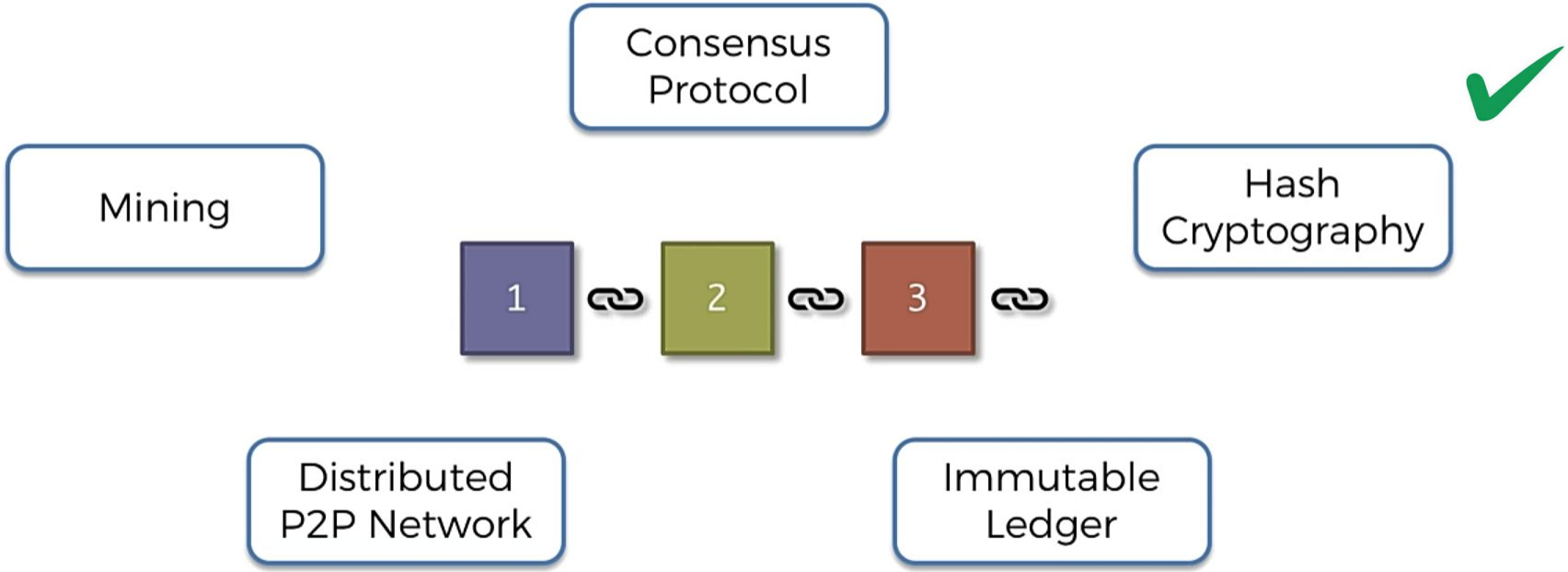
Blockchain Technology Fundamentals

Generations of Blockchain



Courtesy : Research Gate

Blockchain Technology Fundamentals

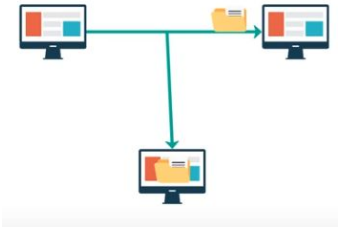


Blockchain Technology Fundamentals

P2P Network in Blockchain

Challenges

1. **Confidentiality**
2. **Integrity**
3. **Non-repudiation**
4. **Authentication**



Solution

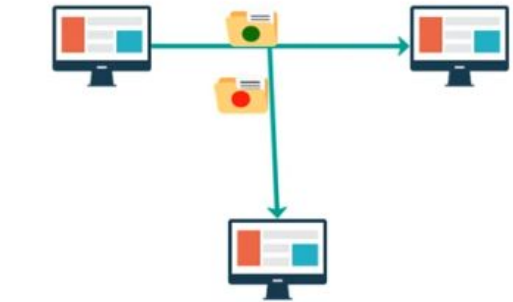
- **Cryptography**

Blockchain Technology Fundamentals

P2P Network in Blockchain

Challenges

1. Confidentiality
2. Integrity
3. Non-repudiation
4. Authentication

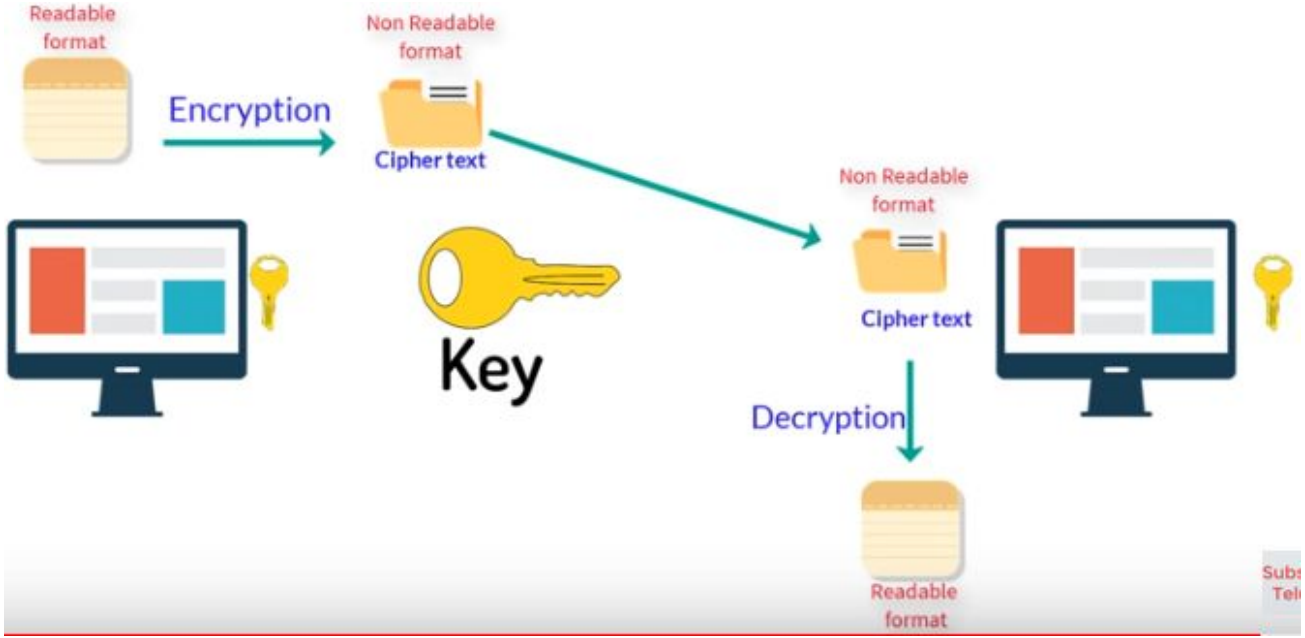


Solution

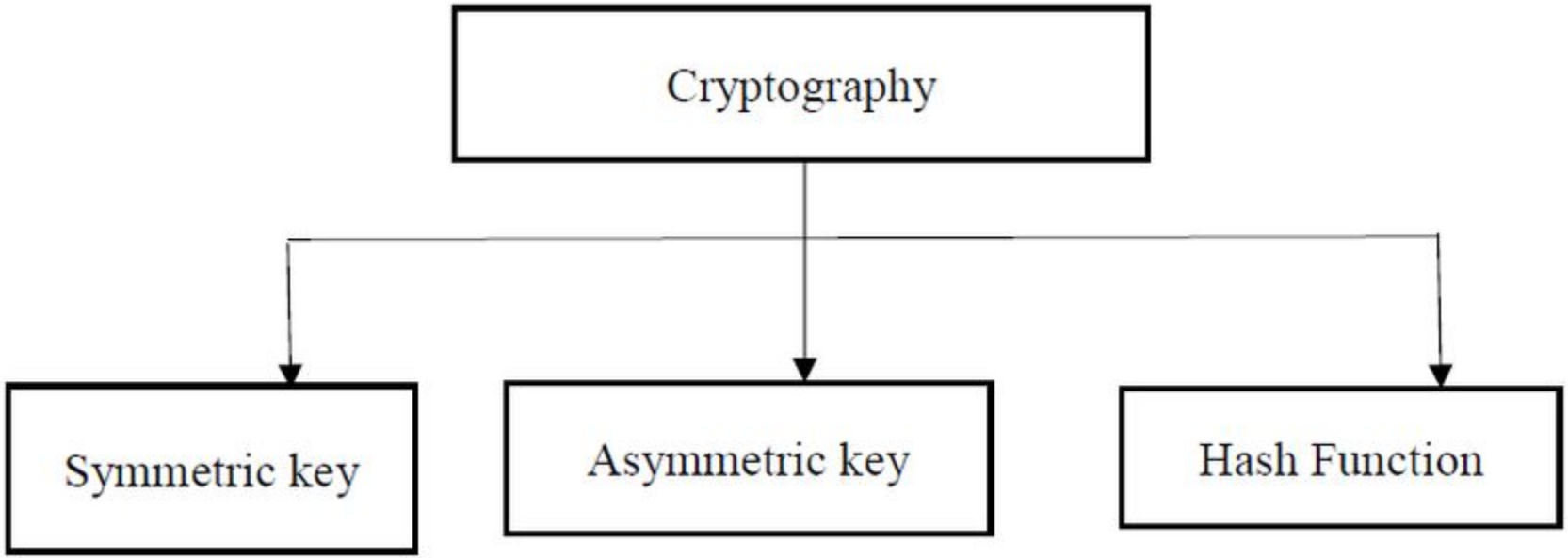
- Cryptography

Blockchain Technology Fundamentals

P2P Network in Blockchain → Cryptography



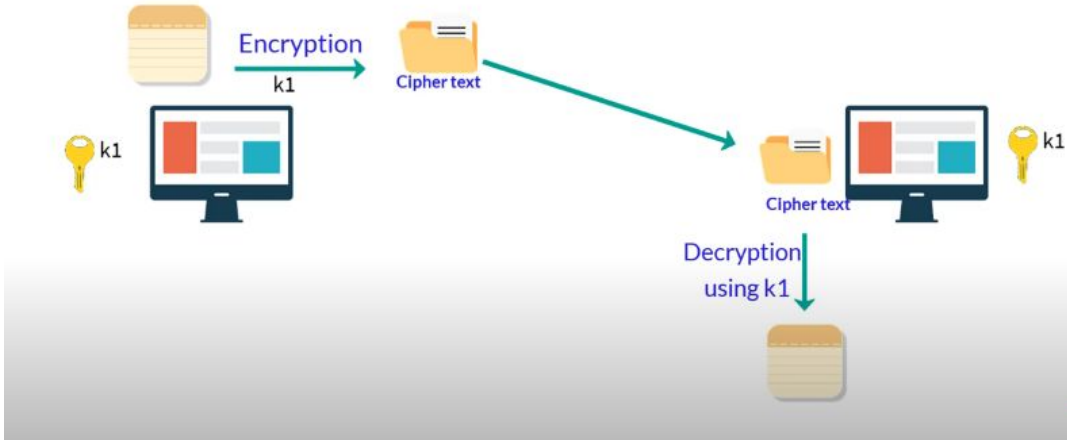
Cryptography - Types



Courtesy : Telusko - Digital Signature

Blockchain Technology Fundamentals

Symmetric Key Cryptography

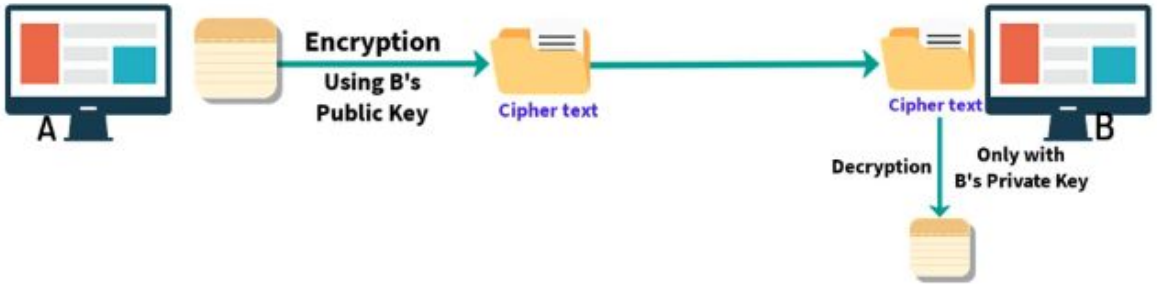


Challenges

- Key must be secure
- Need for Frequent Key changes
- Key Distribution Problem
- # Communication pairs

Blockchain Technology Fundamentals

Public Key or Asymmetric Key Cryptography

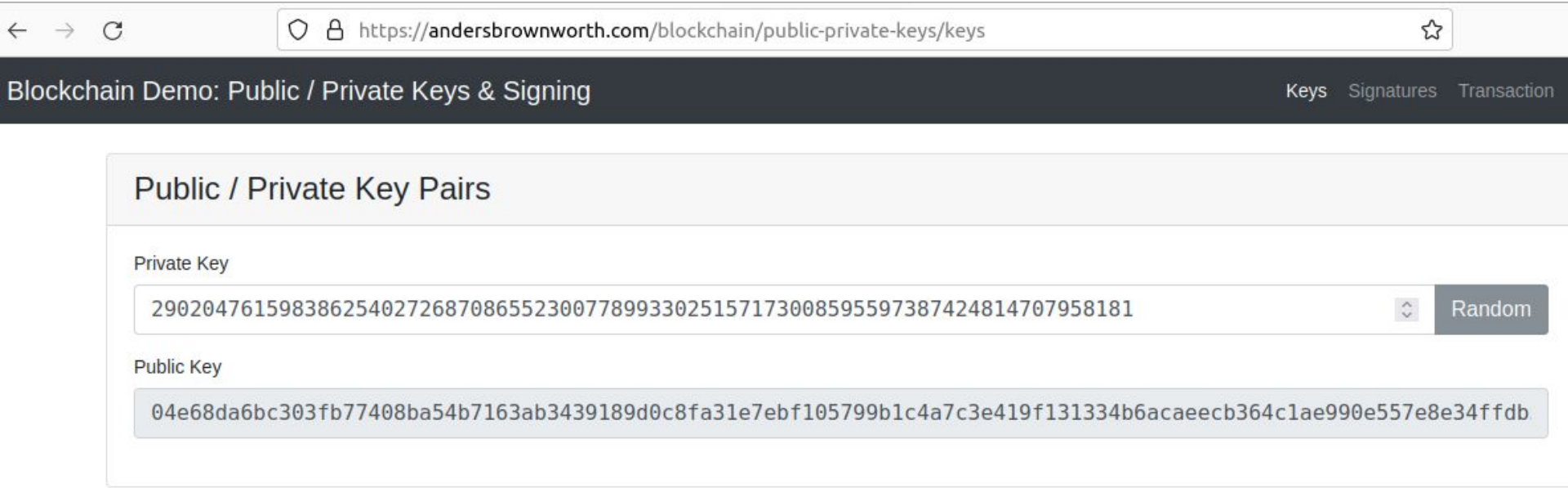


Challenges

- Require a pair of keys
- Expensive to generate
- Not efficient for long messages
- Require High Computational Power

Blockchain Technology Fundamentals

Asymmetric Key Generation - Demo

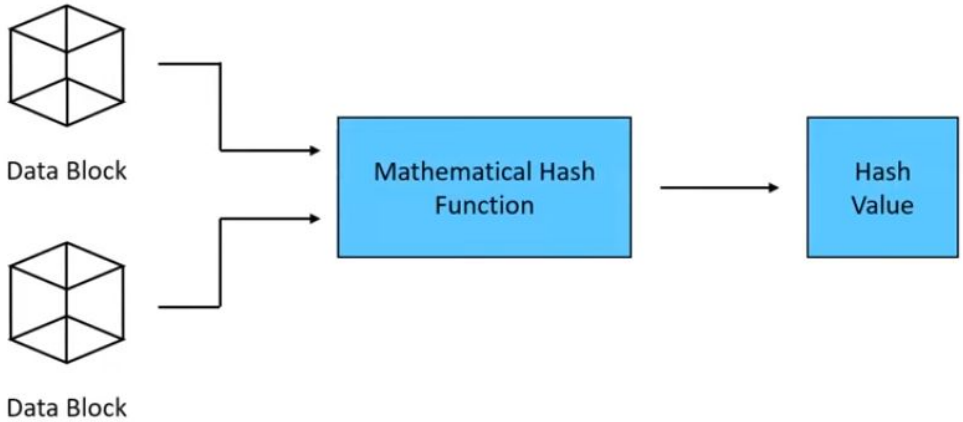


Blockchain Technology Fundamentals

Cryptographic Hash Functions

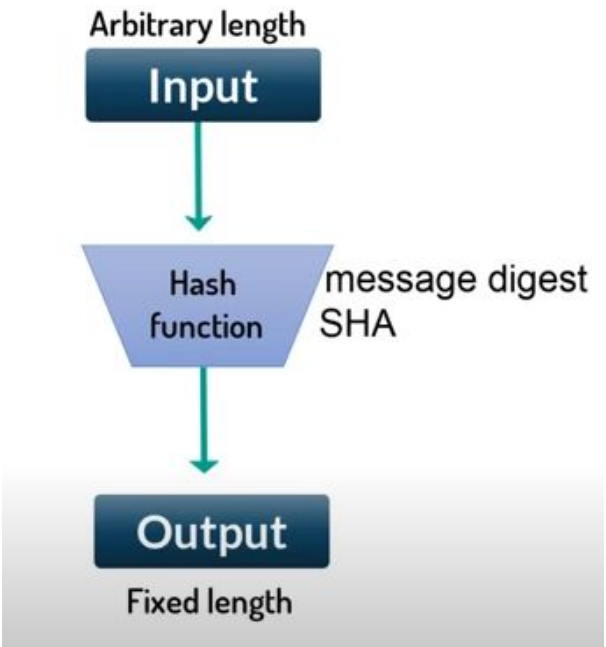
A hash function maps any type of arbitrary data of any length to a fixed-size output. They are efficient and are well-known for one property: they can't be reversed.

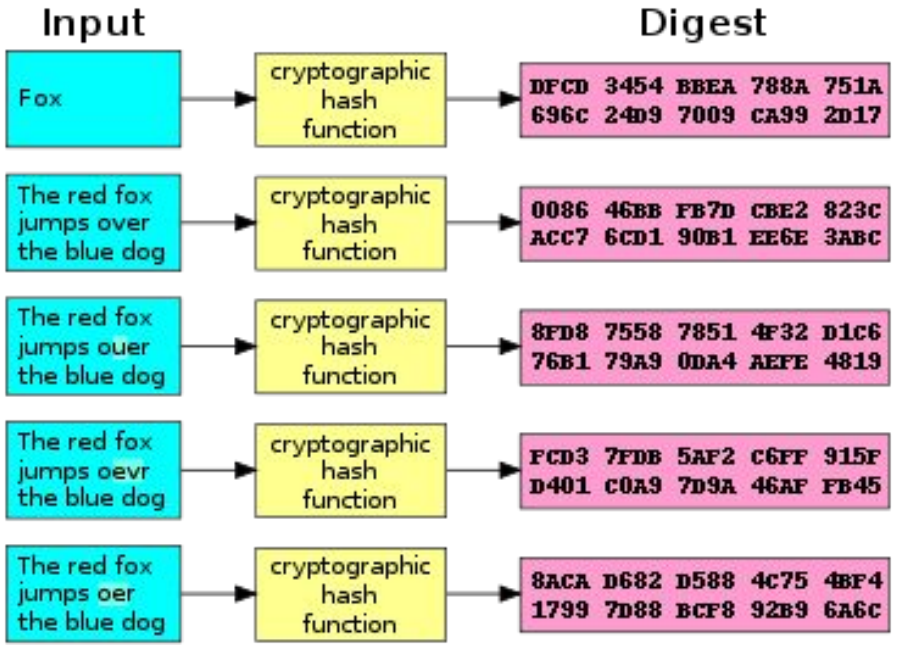
Hash Function for Blockchain



Blockchain Technology Fundamentals

Cryptographic Hash Functions



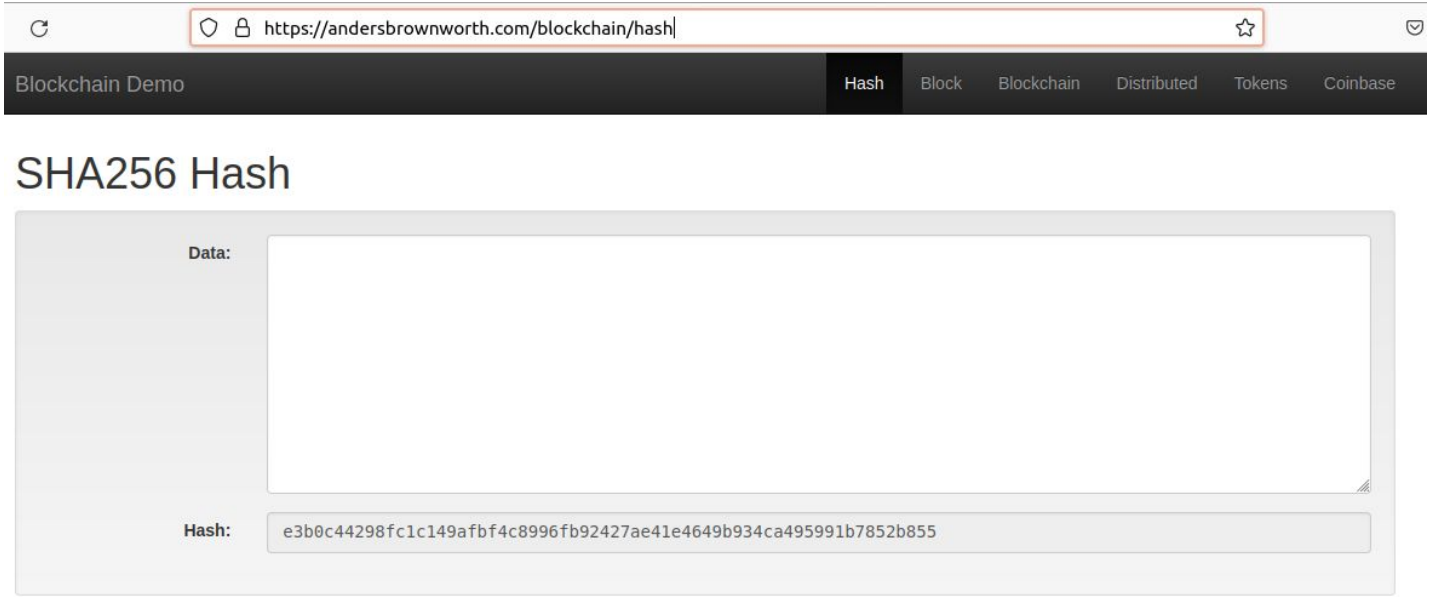


Blockchain Technology Fundamentals

Cryptographic Hash Functions - Eg.

Blockchain Technology Fundamentals

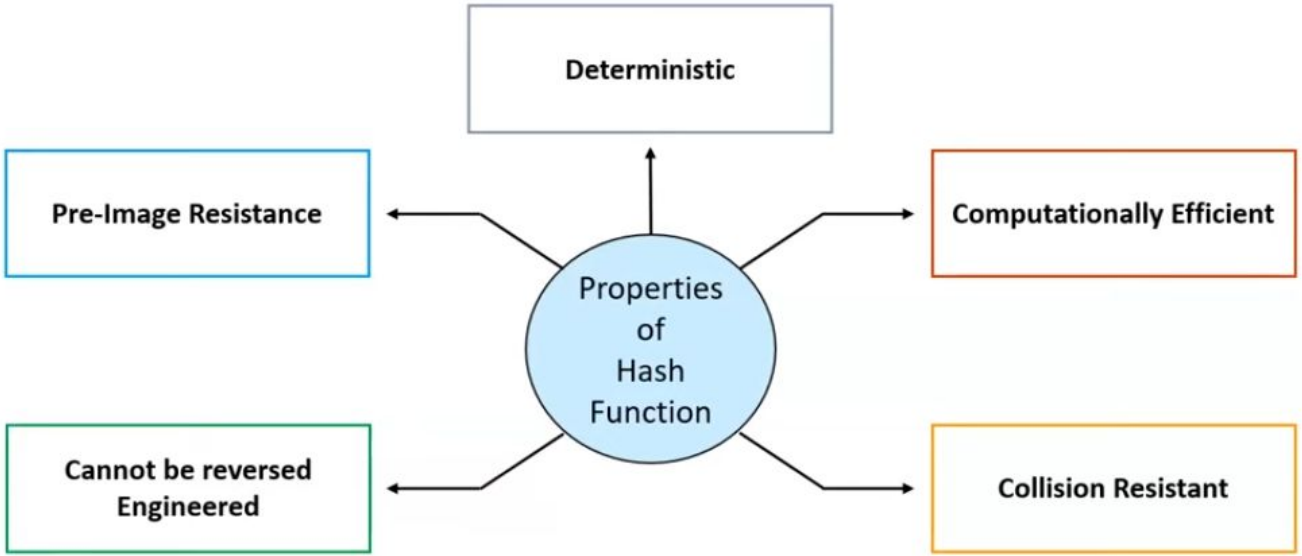
Cryptographic Hash Functions - Demo



Blockchain Technology Fundamentals

Cryptographic Hash Functions

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

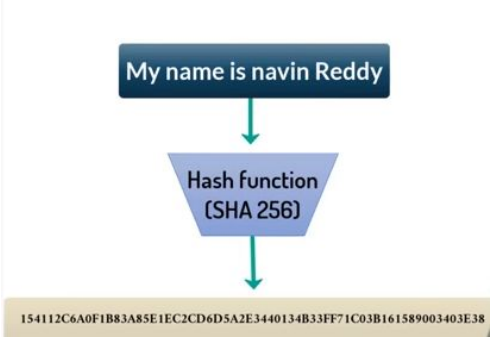


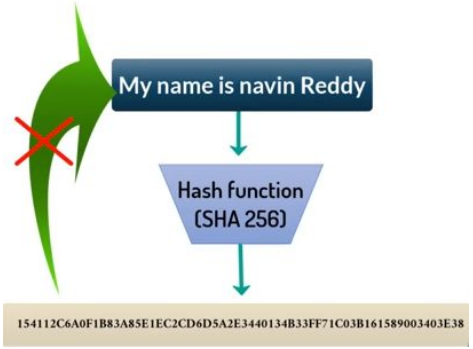
Courtesy : Simply Learn - Merkle Tree

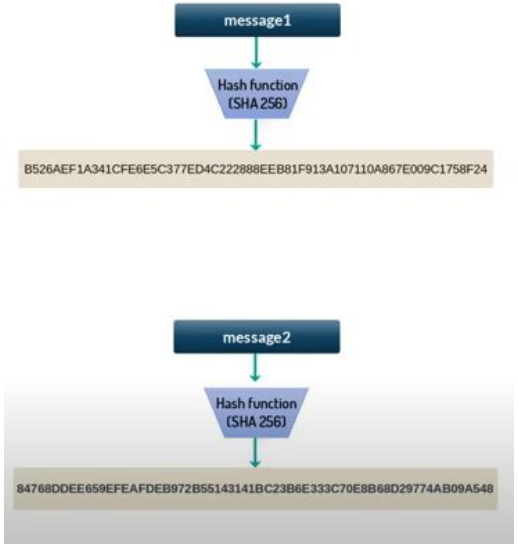
Blockchain Technology Fundamentals

Cryptographic Hash Functions

- Deterministic
- Cannot be reverse engineered
- Collision Resistant







Blockchain Technology Fundamentals

P2P Network in Blockchain

Challenges

1. Confidentiality
2. Integrity
3. Non-repudiation
4. Authentication

Solution

- Digital Signature

Blockchain Technology Fundamentals

P2P Network in Blockchain

Challenges

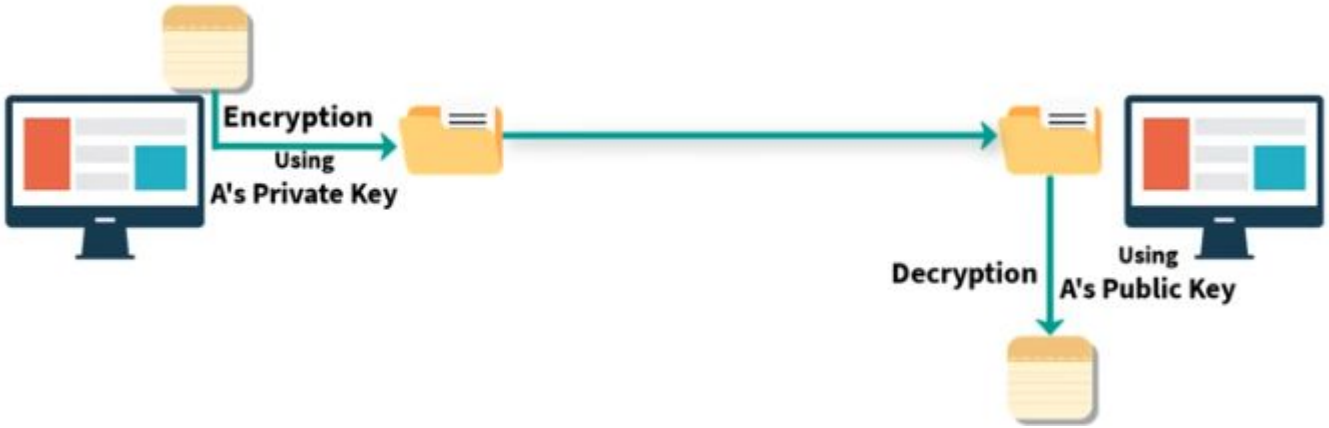
1. Confidentiality
2. Integrity
3. Non-repudiation
4. Authentication

Solution

- Digital Signature

Blockchain Technology Fundamentals

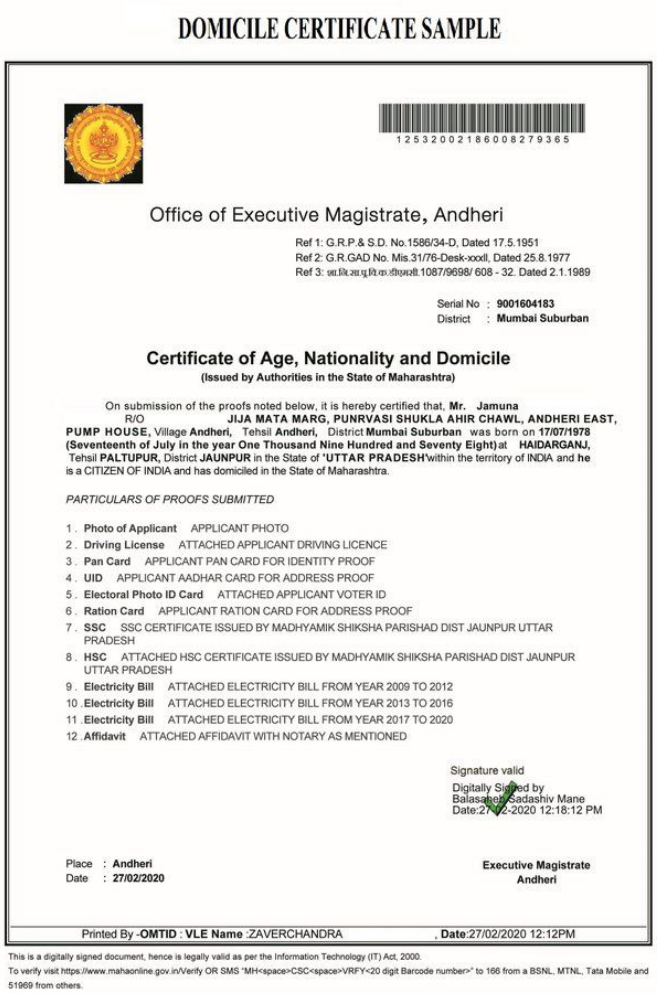
Digital Signature - Basic



Courtesy : Telusko - Digital Signature

Blockchain Technology Fundamentals

Digital Signature - Eg.



DOMICILE CERTIFICATE SAMPLE

12532002186008279365

Office of Executive Magistrate, Andheri

Ref 1: G.R.P.& S.D. No.1586/34-D, Dated 17.5.1951
Ref 2: G.R.GAD No. Mis.31/76-Desk-xxxII, Dated 25.8.1977
Ref 3: [illegible] 1087/9698/ 608 - 32. Dated 2.1.1989

Serial No : **9001604183**
District : **Mumbai Suburban**

Certificate of Age, Nationality and Domicile
(Issued by Authorities in the State of Maharashtra)

On submission of the proofs noted below, it is hereby certified that, **Mr. Jamuna** R/O **JIJA MATA MARG, PUNRVASI SHUKLA AHIR CHAWL, ANDHERI EAST, PUMP HOUSE,** Village **Andheri,** Tehsil **Andheri,** District **Mumbai Suburban** was born on **17/07/1978 (Seventeenth of July in the year One Thousand Nine Hundred and Seventy Eight)** at **HAIDARGANJ,** Tehsil **PALTUPUR,** District **JAUNPUR** in the State of **'UTTAR PRADESH'** within the territory of INDIA and **he** is a CITIZEN OF INDIA and has domiciled in the State of Maharashtra.

PARTICULARS OF PROOFS SUBMITTED

1. **Photo of Applicant** APPLICANT PHOTO
2. **Driving License** ATTACHED APPLICANT DRIVING LICENCE
3. **Pan Card** APPLICANT PAN CARD FOR IDENTITY PROOF
4. **UID** APPLICANT AADHAR CARD FOR ADDRESS PROOF
5. **Electoral Photo ID Card** ATTACHED APPLICANT VOTER ID
6. **Ration Card** APPLICANT RATION CARD FOR ADDRESS PROOF
7. **SSC** SSC CERTIFICATE ISSUED BY MADHYAMIK SHIKSHA PARISHAD DIST JAUNPUR UTTAR PRADESH
8. **HSC** ATTACHED HSC CERTIFICATE ISSUED BY MADHYAMIK SHIKSHA PARISHAD DIST JAUNPUR UTTAR PRADESH
9. **Electricity Bill** ATTACHED ELECTRICITY BILL FROM YEAR 2009 TO 2012
10. **Electricity Bill** ATTACHED ELECTRICITY BILL FROM YEAR 2013 TO 2016
11. **Electricity Bill** ATTACHED ELECTRICITY BILL FROM YEAR 2017 TO 2020
12. **Affidavit** ATTACHED AFFIDAVIT WITH NOTARY AS MENTIONED

Signature valid
Digitally Signed by Balasaheb Sadashiv Mane
Date:27-02-2020 12:18:12 PM

Place : **Andheri**
Date : **27/02/2020**

Executive Magistrate
Andheri

Printed By -**OMTID : VLE Name** :ZAVERCHANDRA , **Date**:27/02/2020 12:12PM

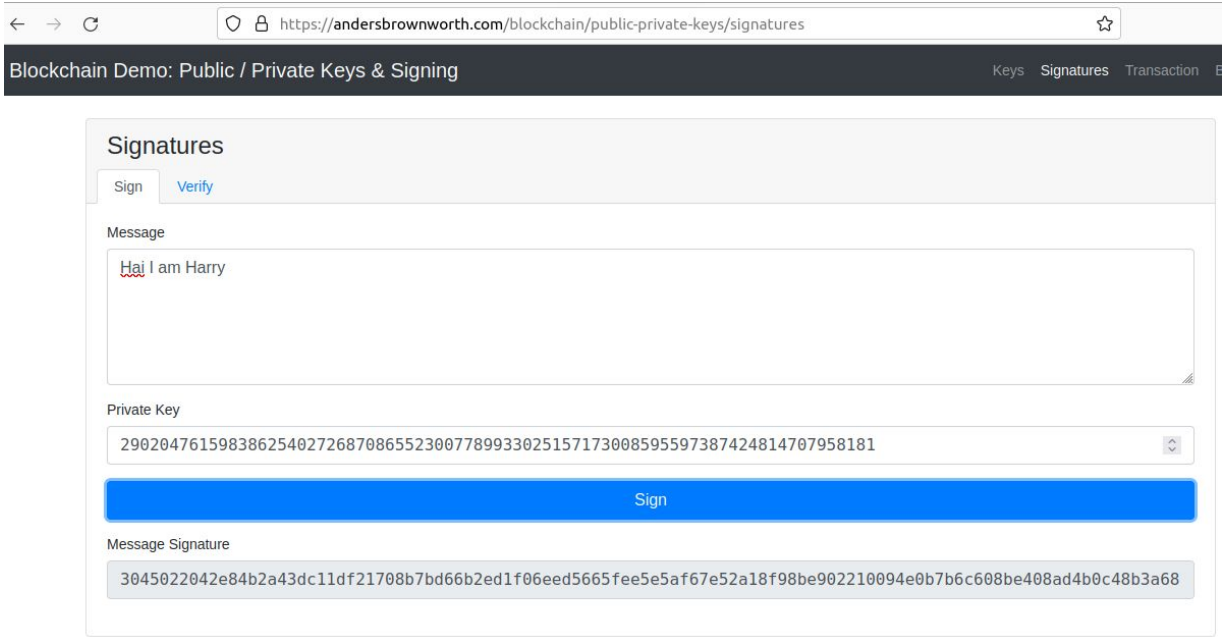
This is a digitally signed document, hence is legally valid as per the Information Technology (IT) Act, 2000.
To verify visit https://www.mahaonline.gov.in/Verify OR SMS "MH<space>CSC<space>VRFY<20 digit Barcode number>" to 166 from a BSNL, MTNL, Tata Mobile and 51969 from others.

Courtesy :

- https://www.digilocker.gov.in/
- https://github.com/jai-singhal/digiLocker

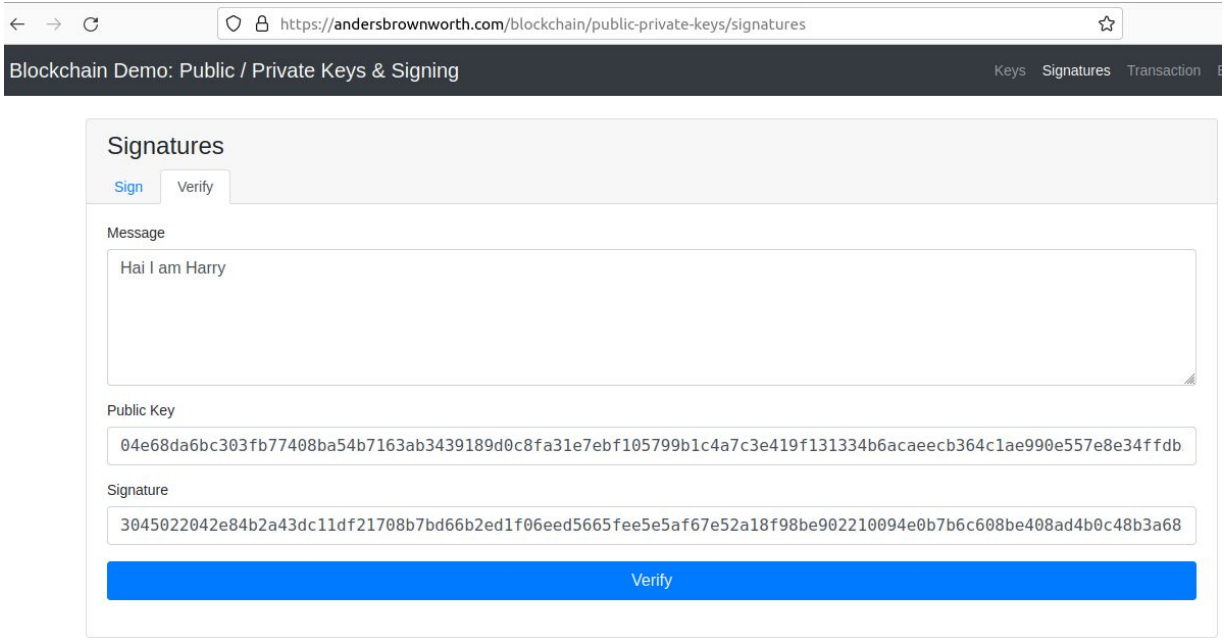
Blockchain Technology Fundamentals

Digital Signatures - Demo



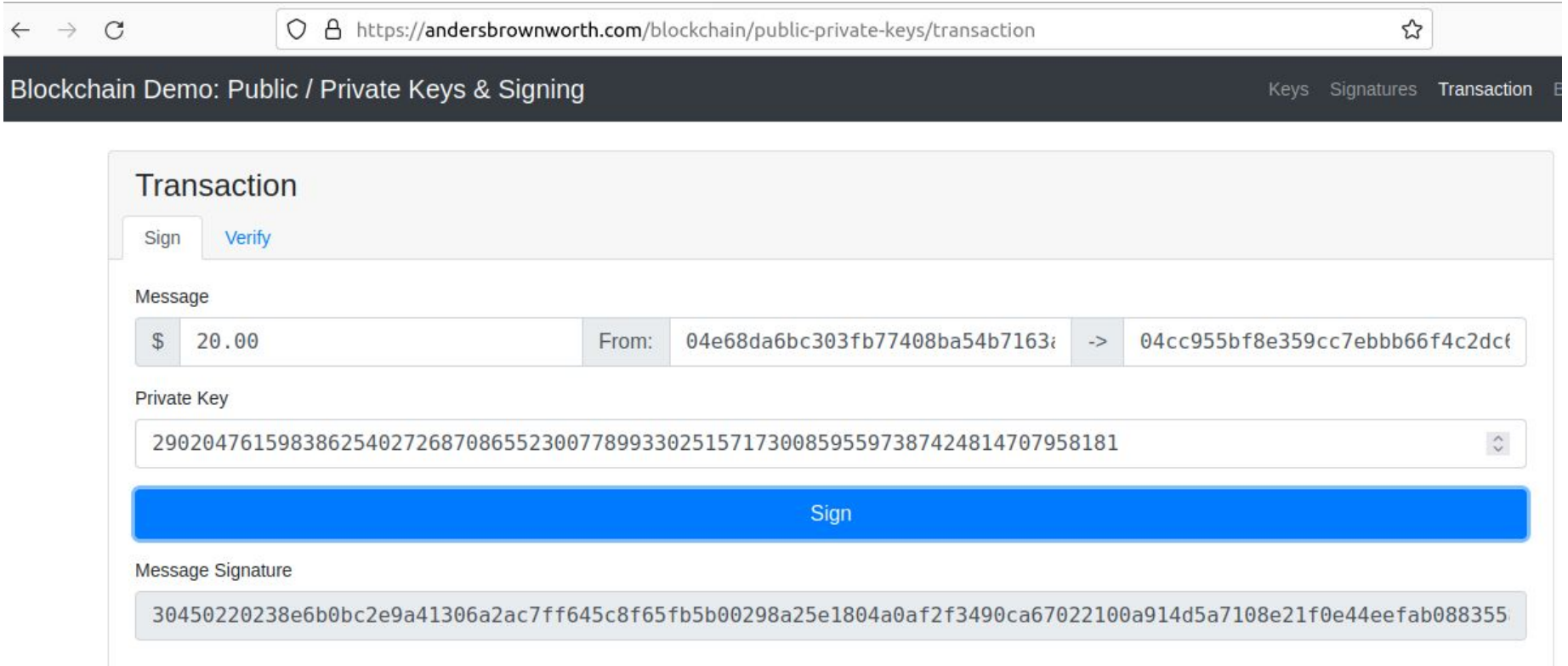
Blockchain Technology Fundamentals

Digital Signatures - Demo



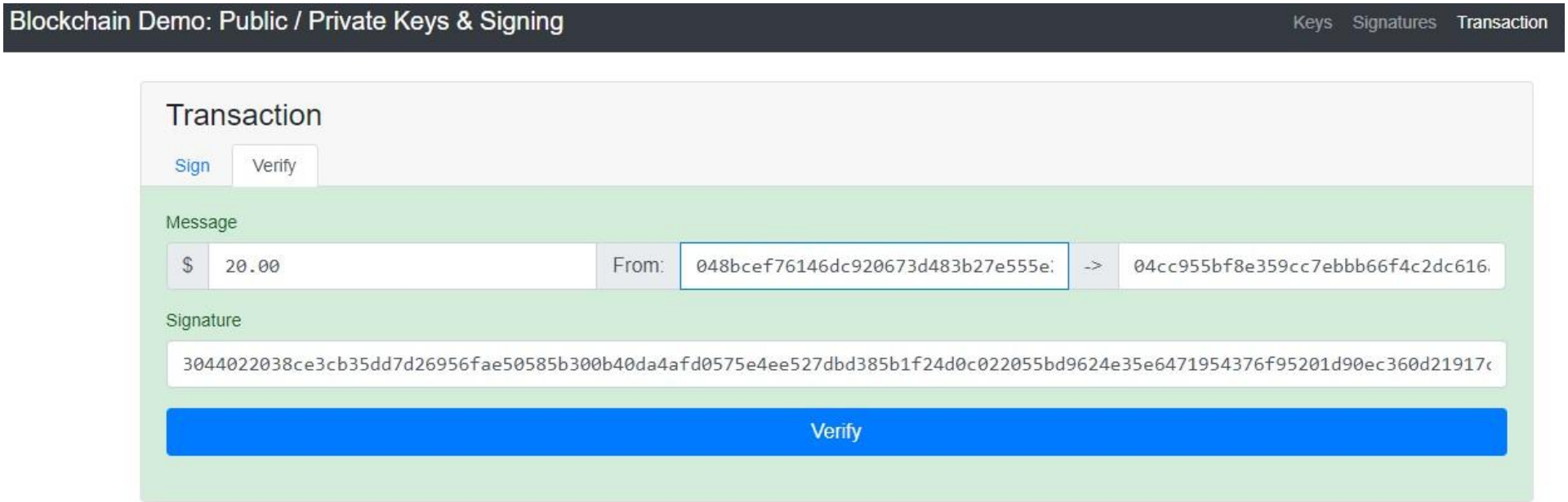
Blockchain Technology Fundamentals

Digitally Signed Transaction - Demo



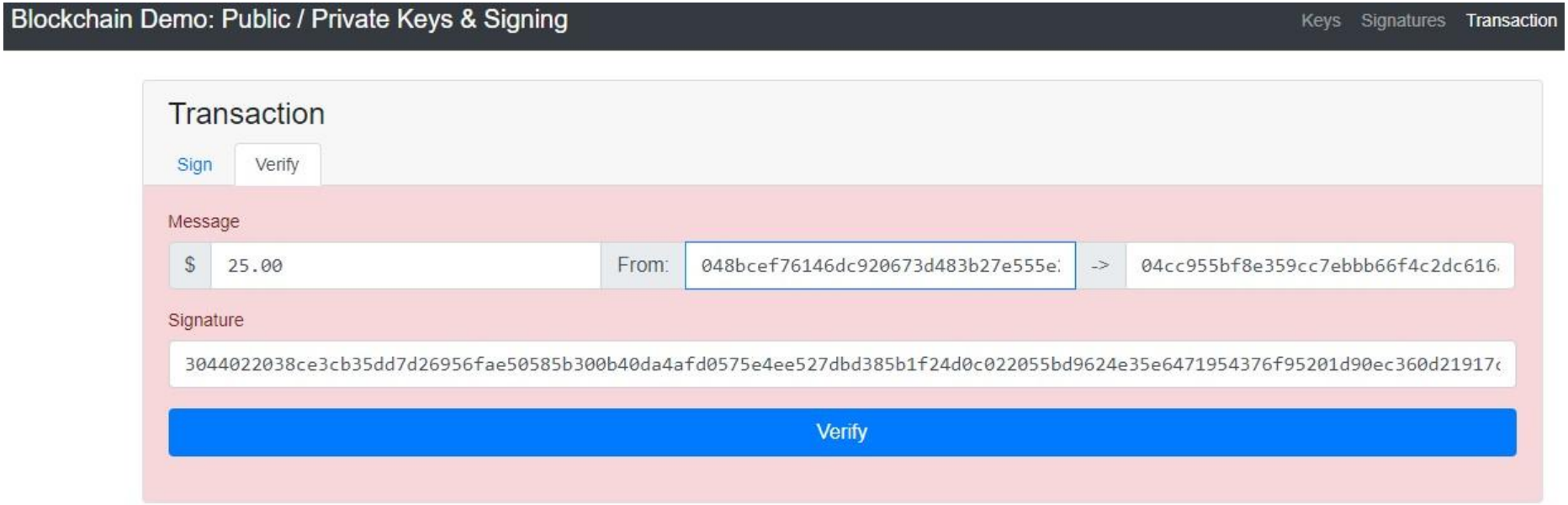
Blockchain Technology Fundamentals

Digitally Signed Transaction - Demo



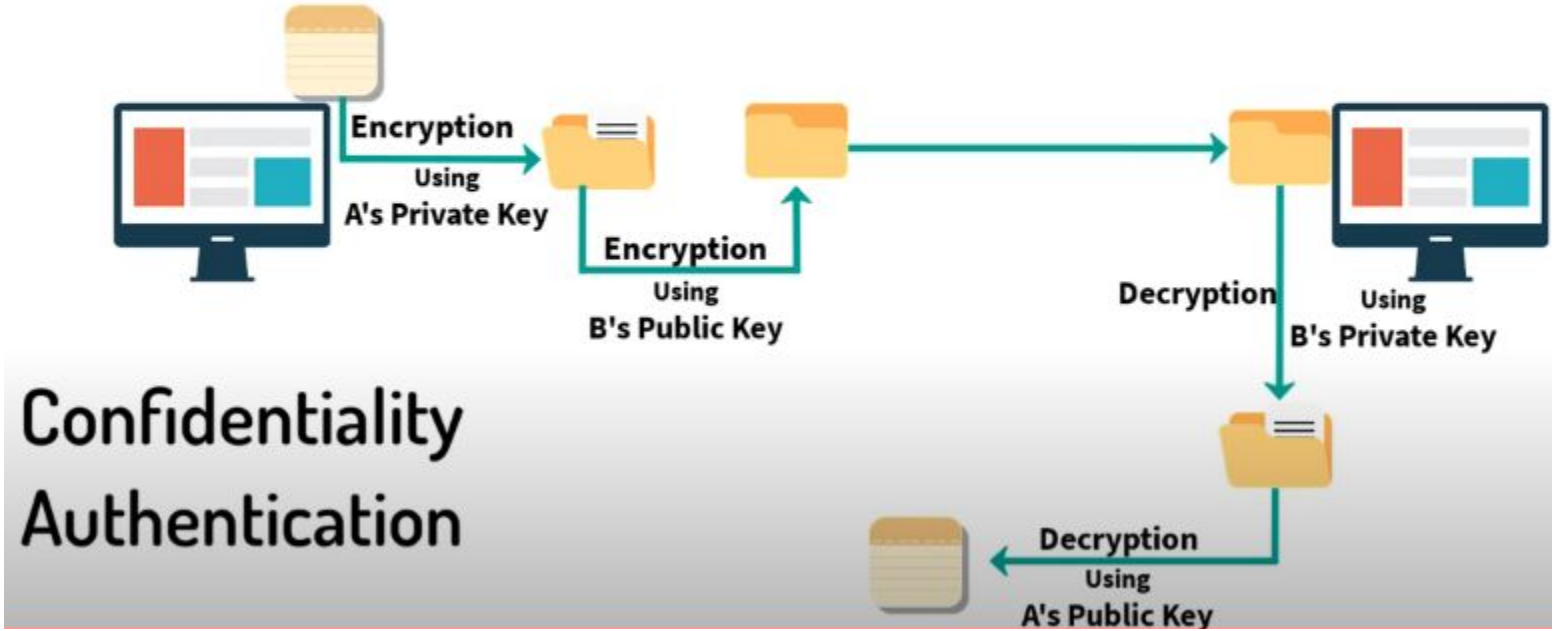
Blockchain Technology Fundamentals

Digitally Signed Transaction - Demo



Blockchain Technology Fundamentals

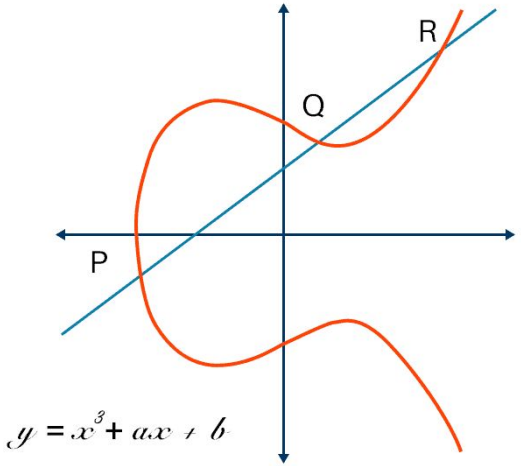
Digital Signature



Courtesy : Telusko - Digital Signature

Elliptical Curve Cryptography

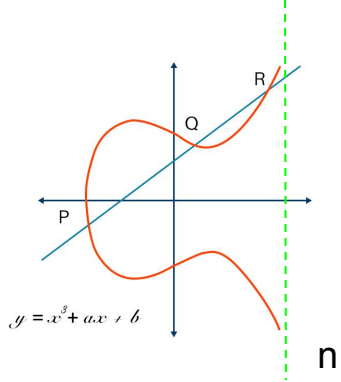
- Asymmetric Key Cryptography
- Provides **High Security with smaller key size** (compared to RSA) and **high security**
- Uses **Elliptical Curves**
  - defined using equations of degree 3
  - Symmetric to x-axis
  - Line drawn will intersect atmost 3 points.



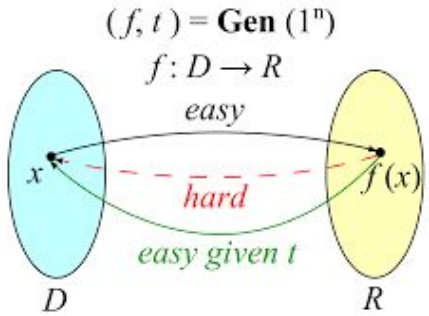
Courtesy : Elliptical Curve Cryptography

Blockchain Technology Fundamentals

Elliptical Curve Cryptography

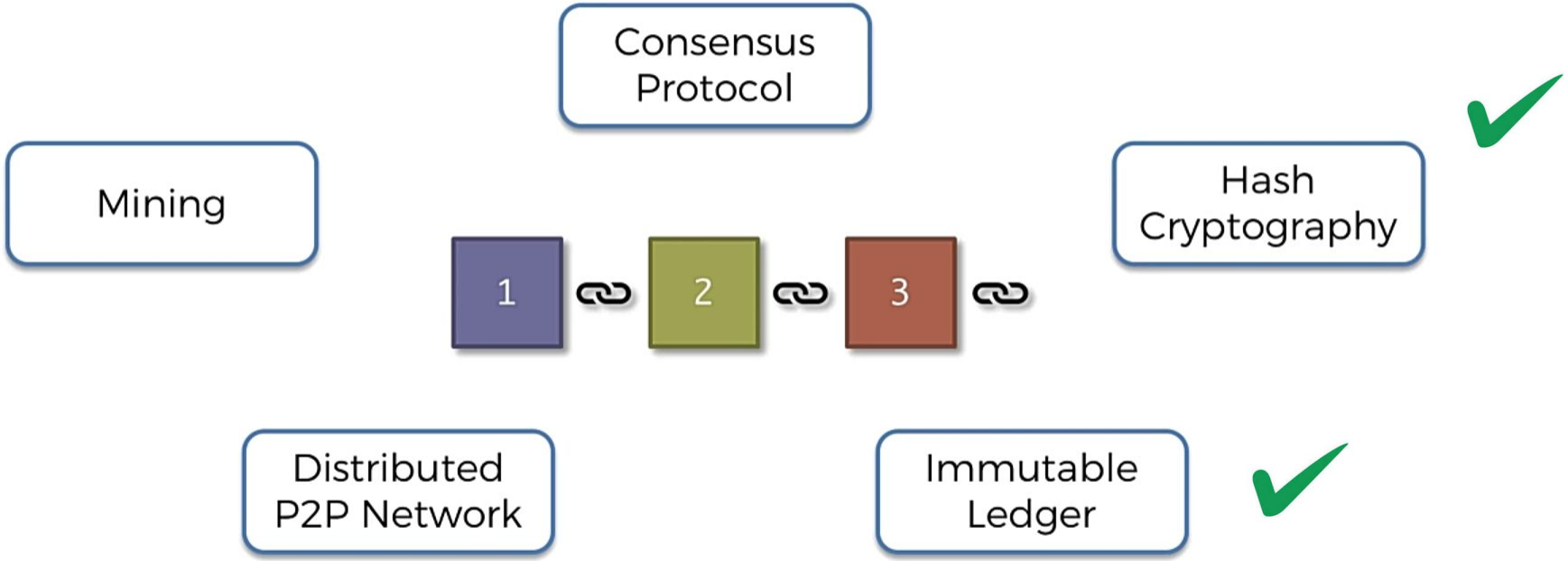


- **What makes ECC hard to crack ?**
  - **Discrete Logarithm Problem**
    - Let E_q (a,b) be the Elliptical Curve, consider the equation, Q = kP ; where Q & P are pts on curve and k < n
      - If k & P is given, its easy to find Q.
      - If P & Q is given, extremely difficult to find k
  - **Trapdoor Function**
    - Function which can be easily computed in one direction and difficult to computed in opposite direction.

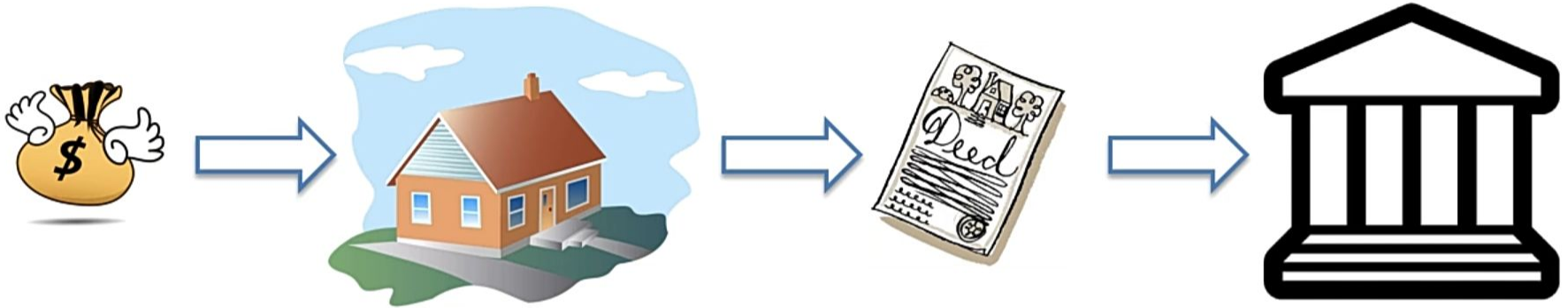


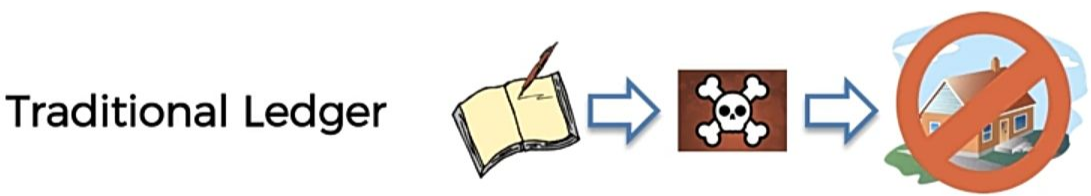
Courtesy : Trapdoor - wikipedia

Blockchain Technology Fundamentals



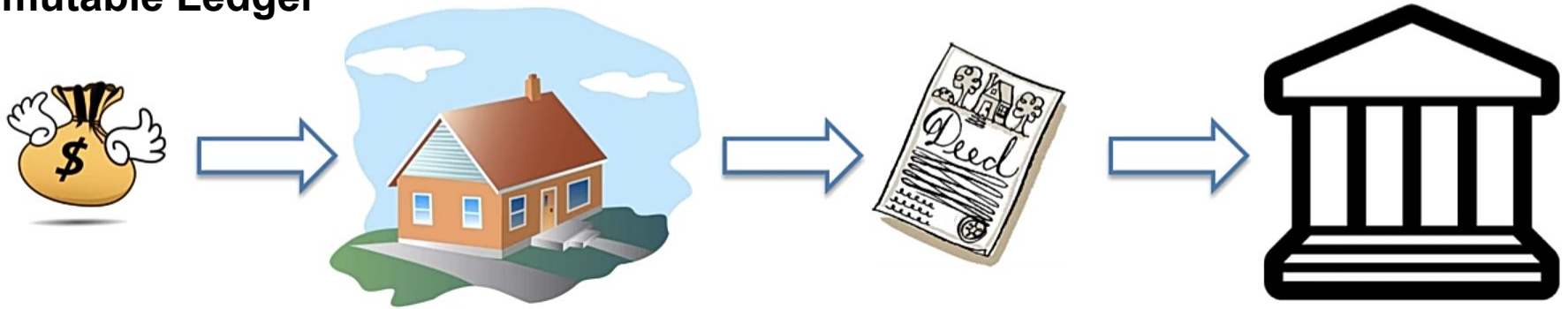
Immutable Ledger



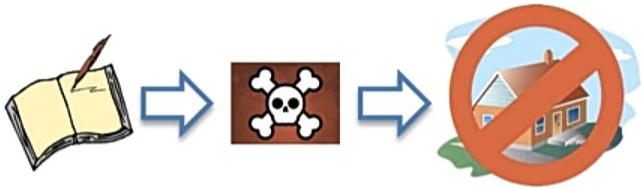


Blockchain Technology Fundamentals

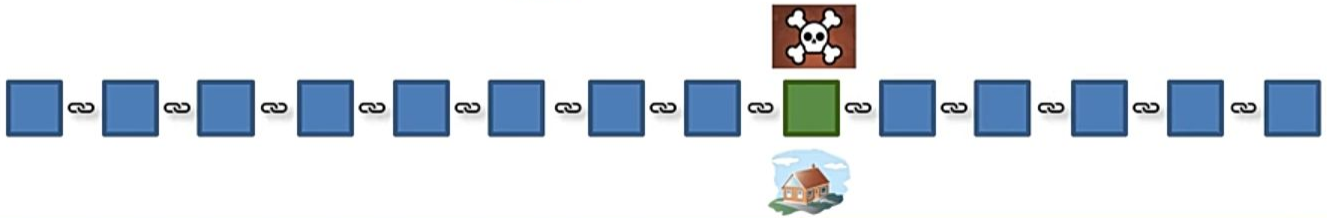
Immutable Ledger



Traditional Ledger

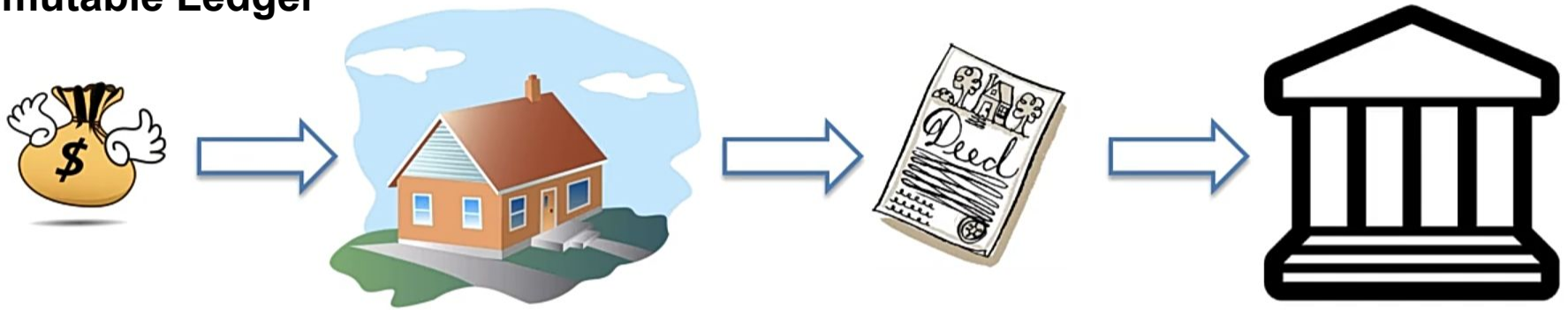


Blockchain

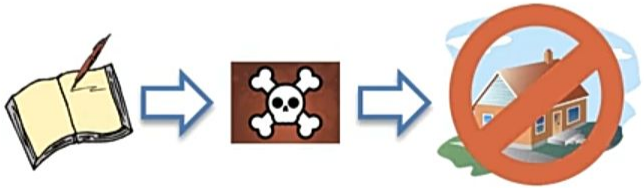


Blockchain Technology Fundamentals

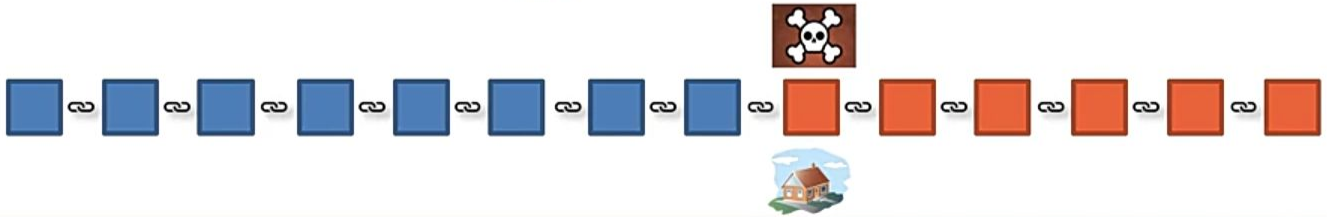
Immutable Ledger



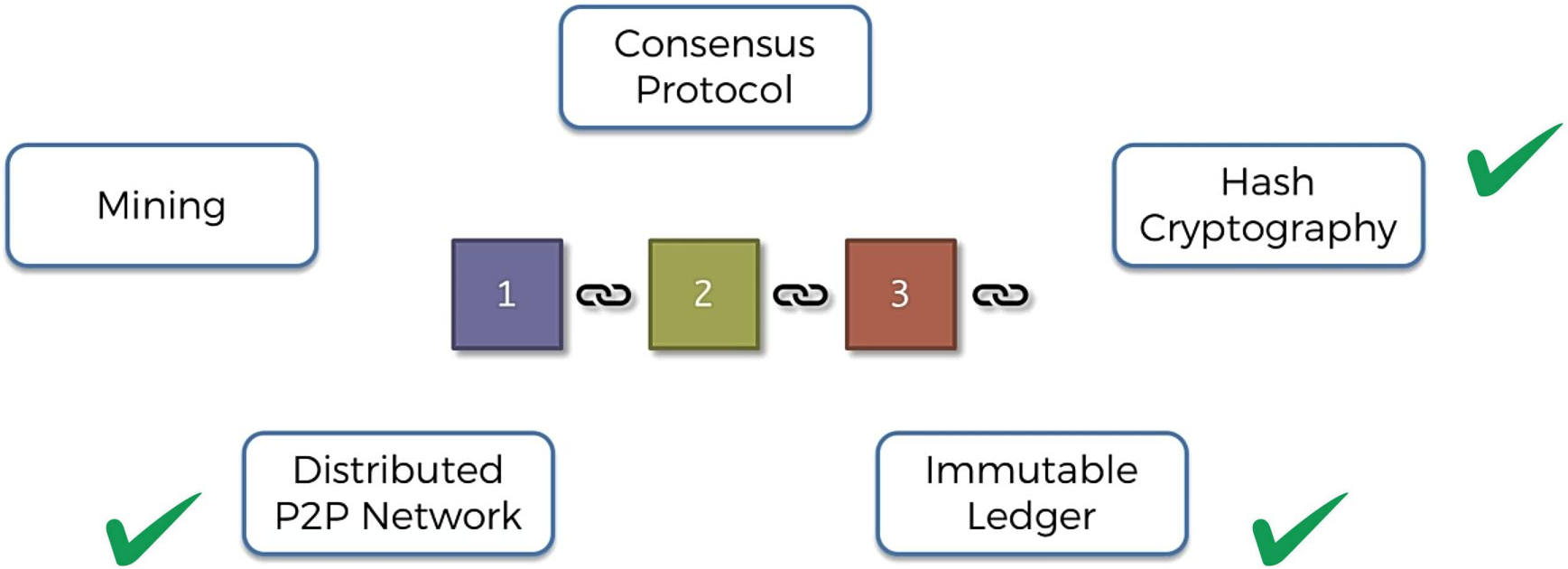
Traditional Ledger



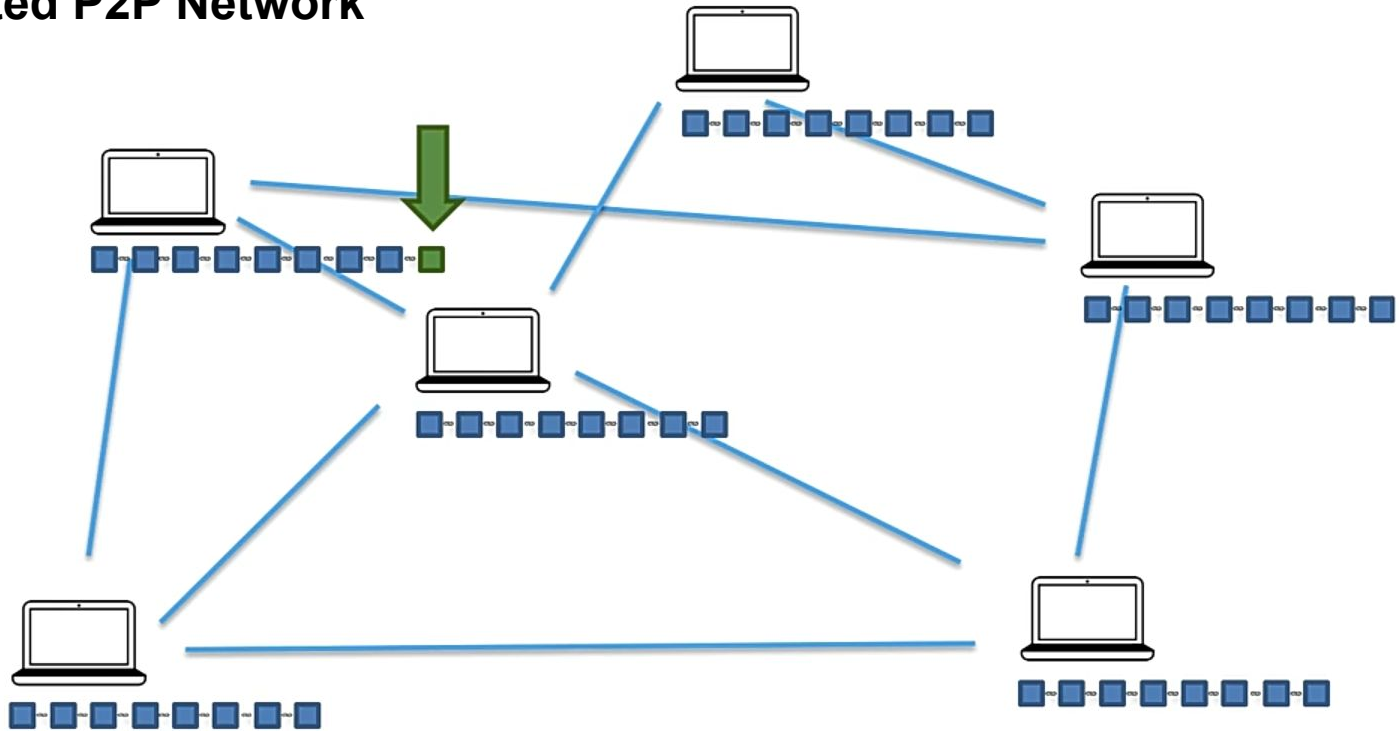
Blockchain



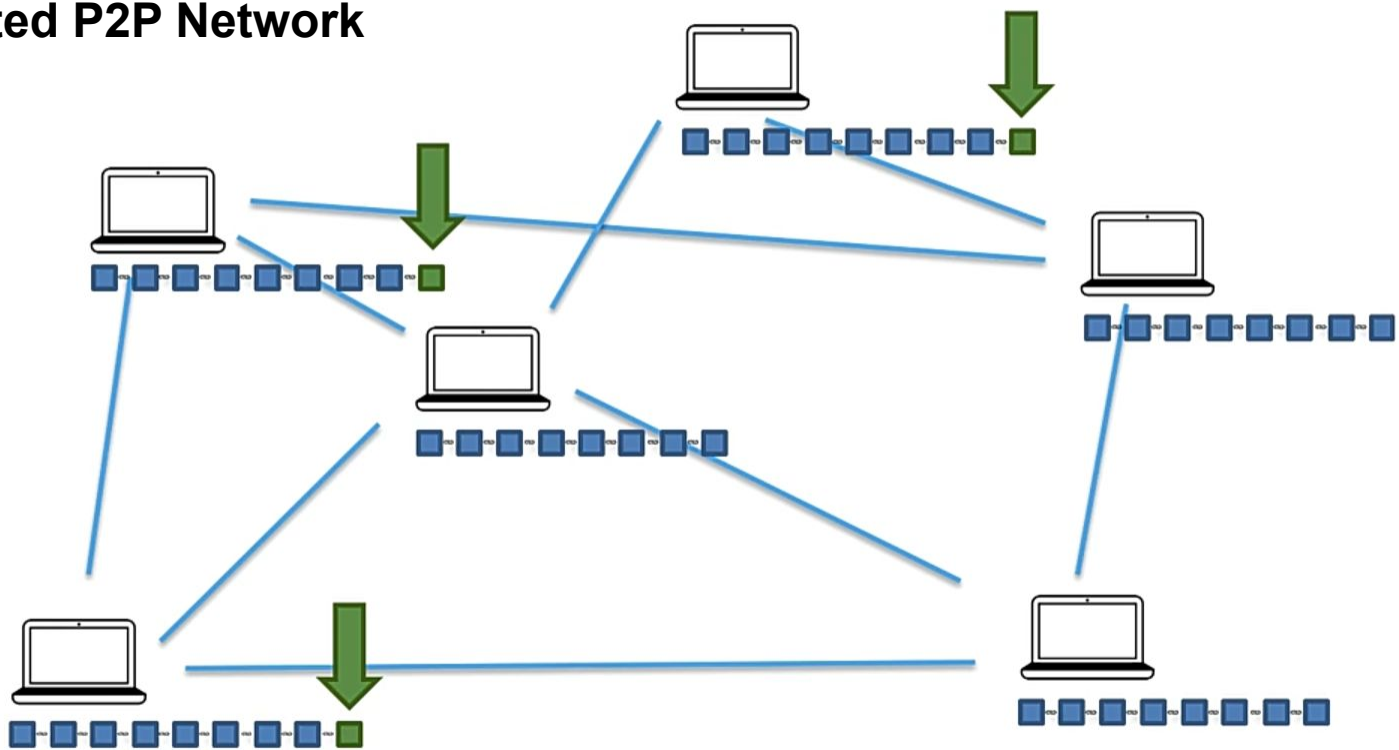
Blockchain Technology Fundamentals



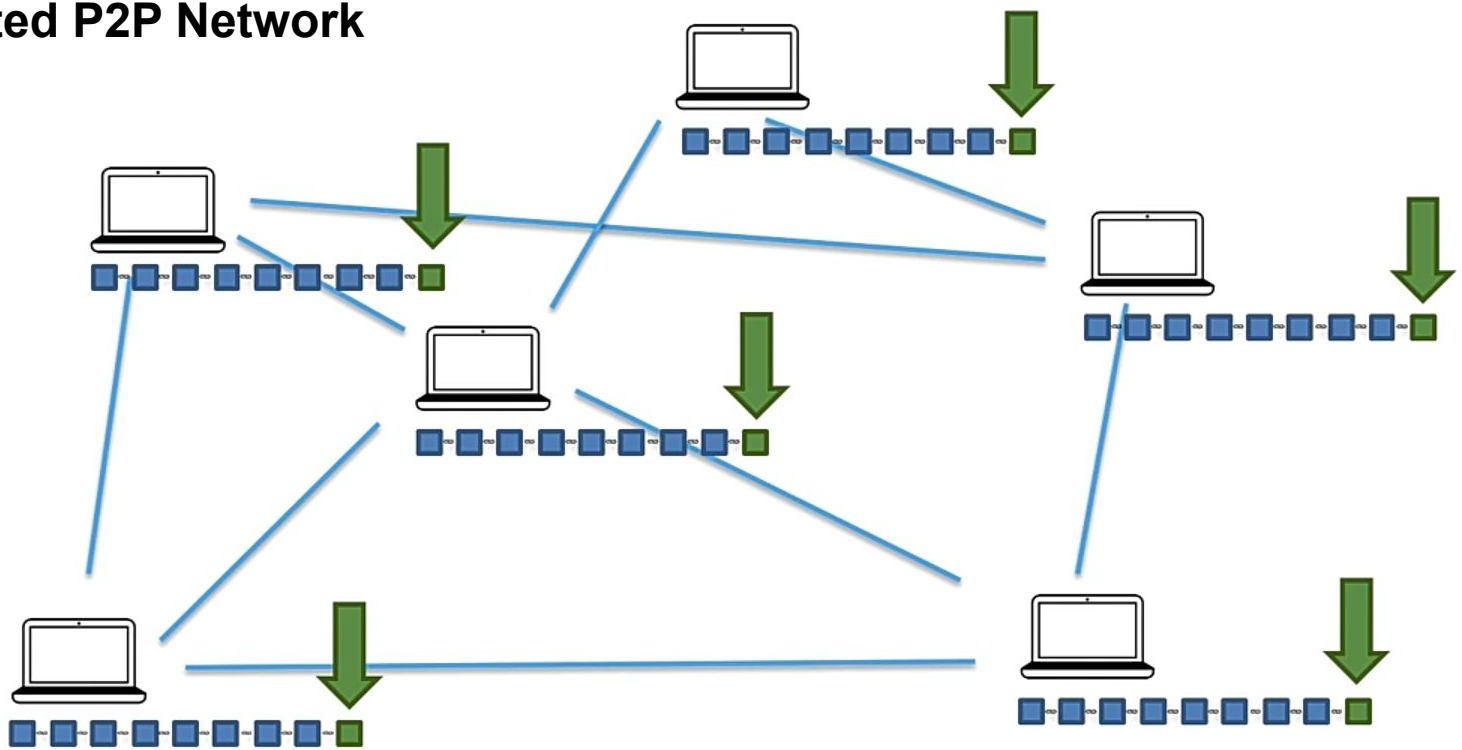
Distributed P2P Network



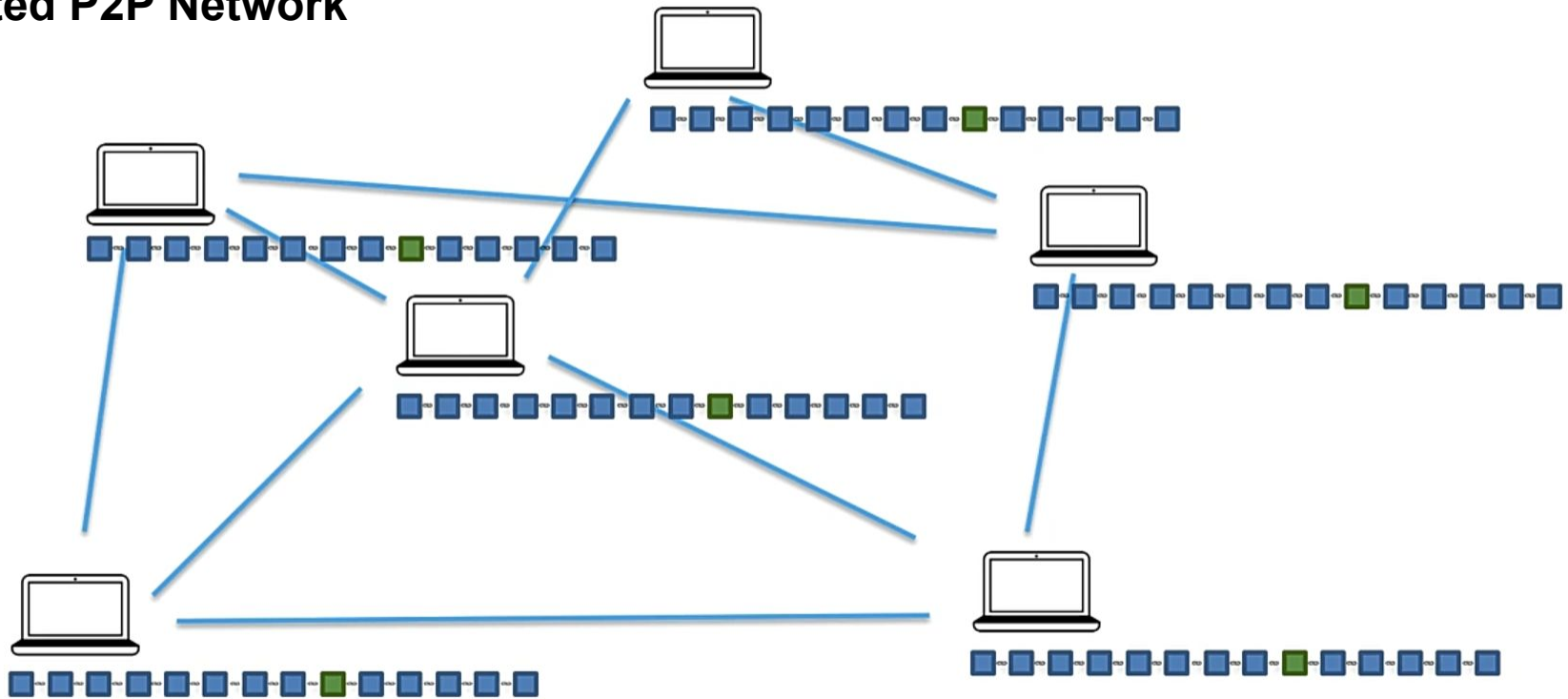
Distributed P2P Network



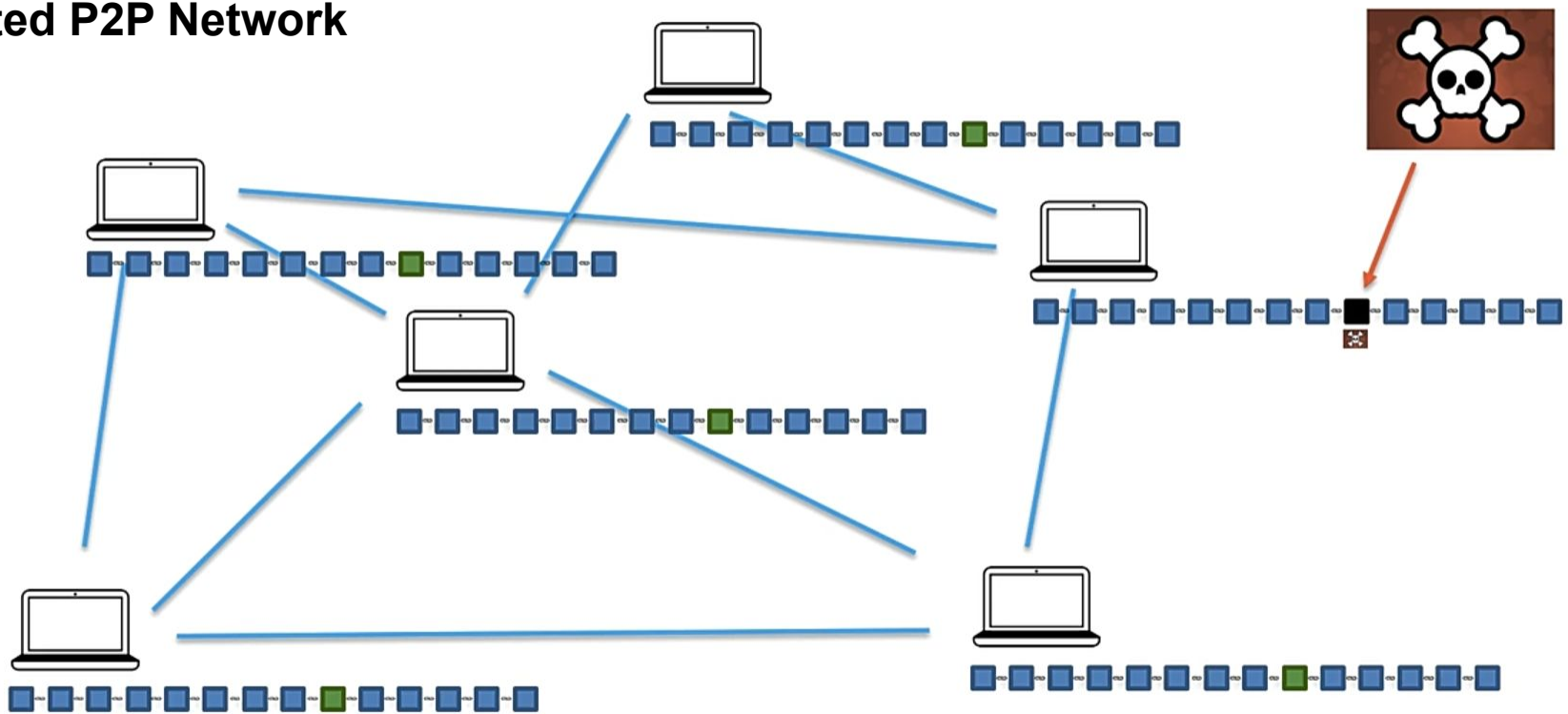
Distributed P2P Network



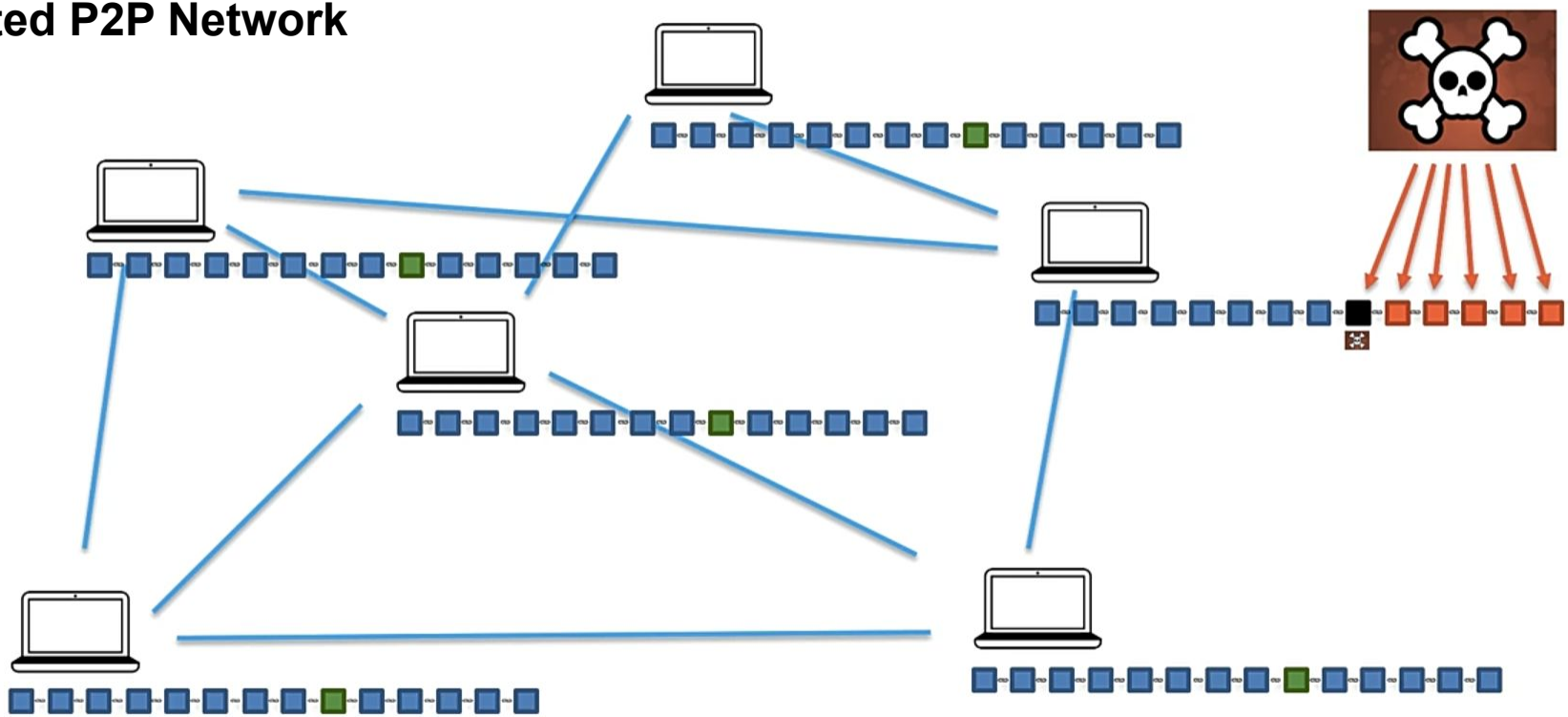
Distributed P2P Network



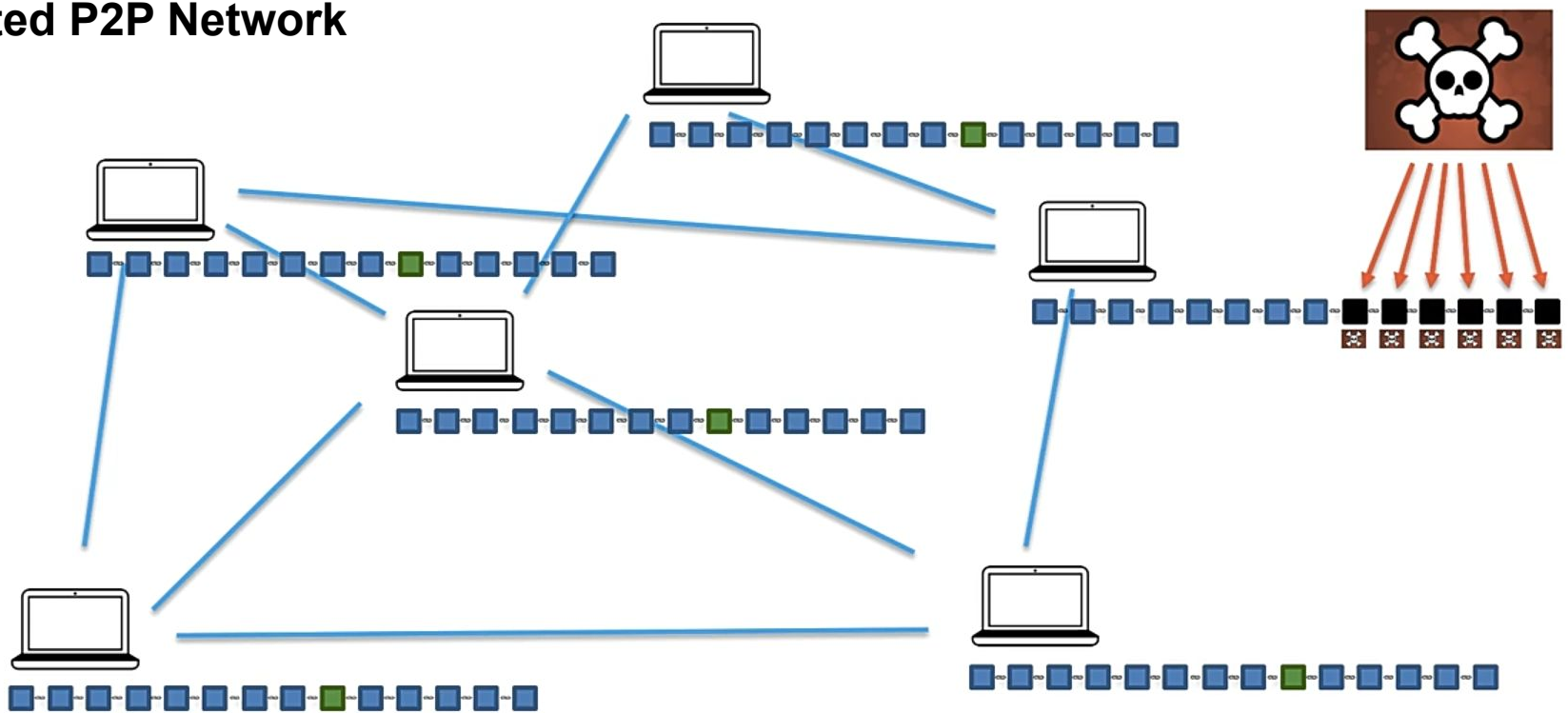
Distributed P2P Network



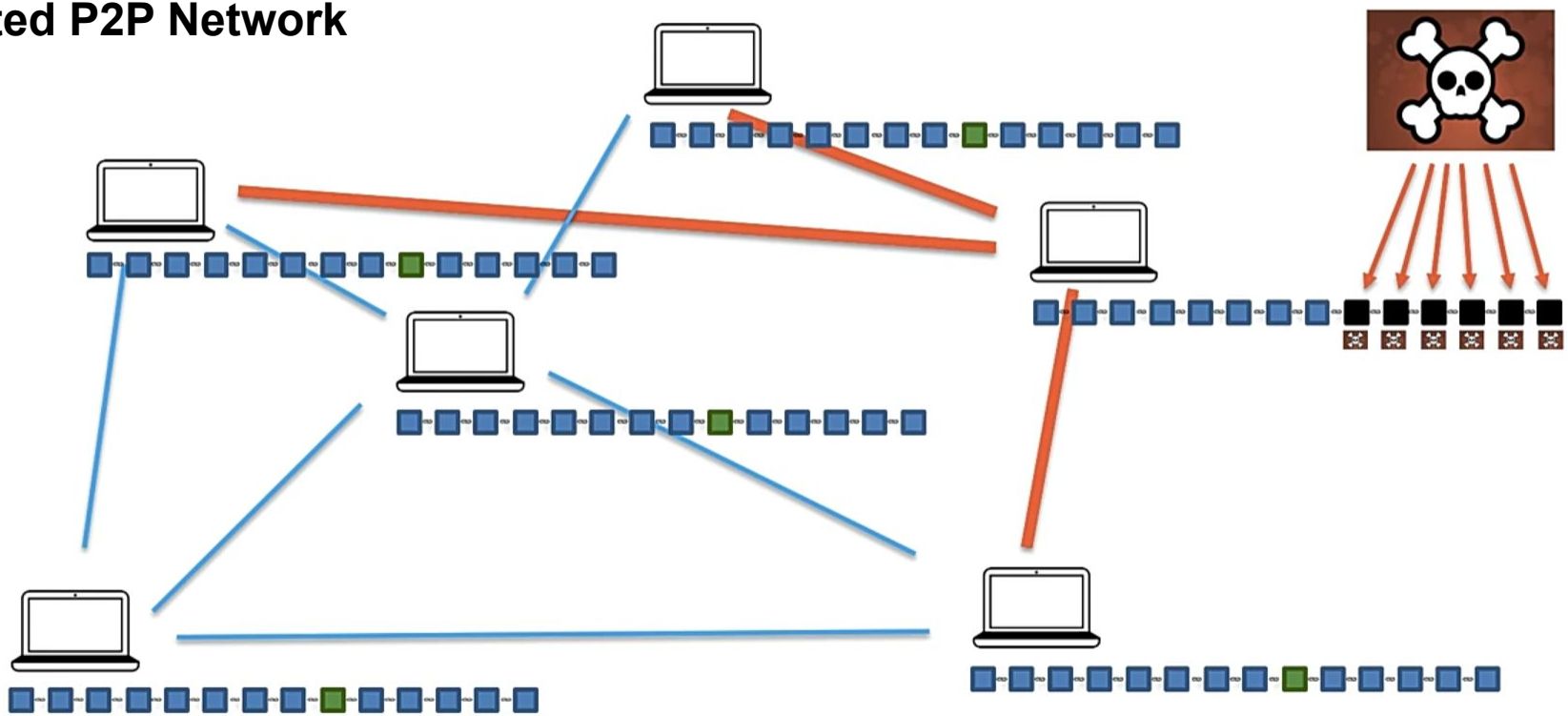
Distributed P2P Network



Distributed P2P Network

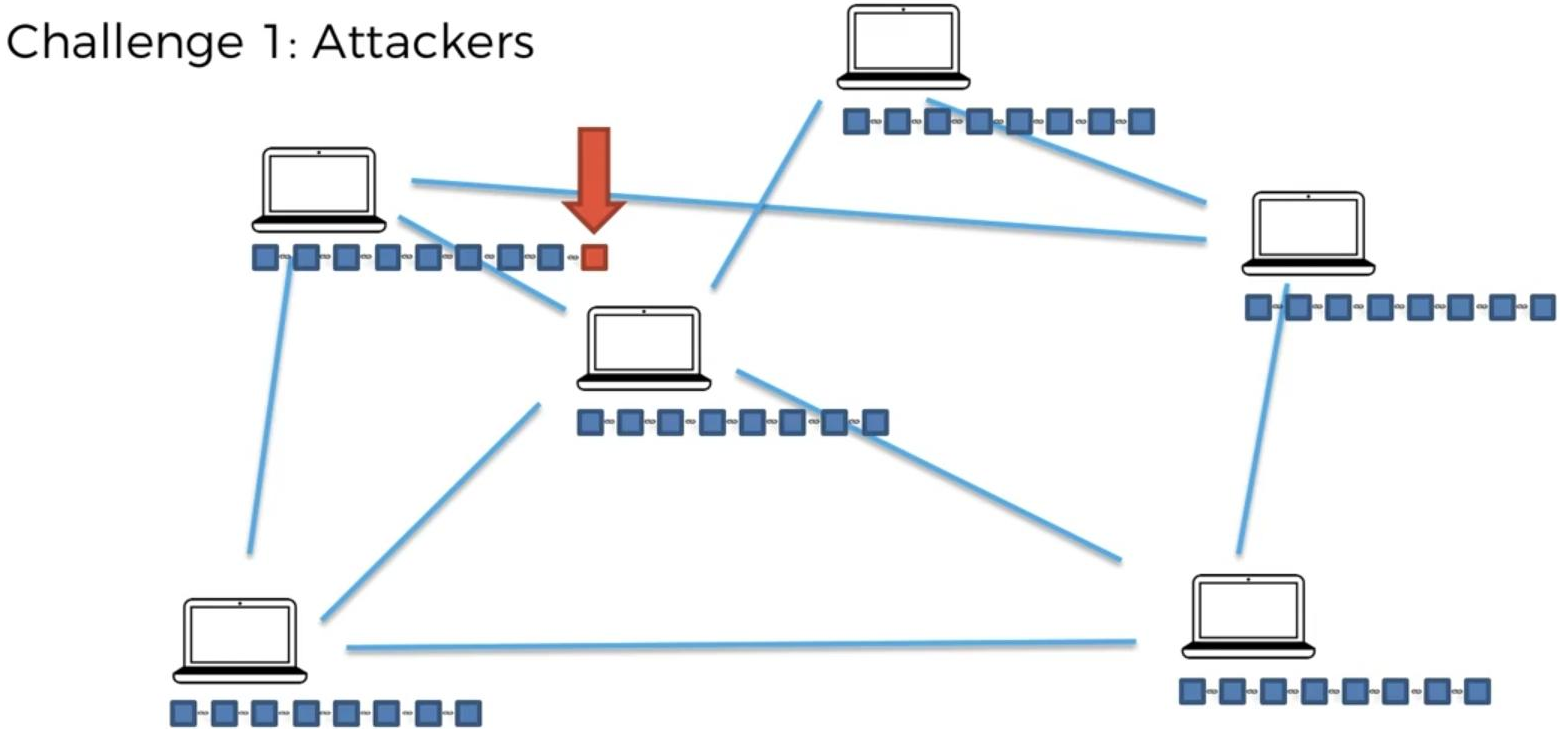


Distributed P2P Network



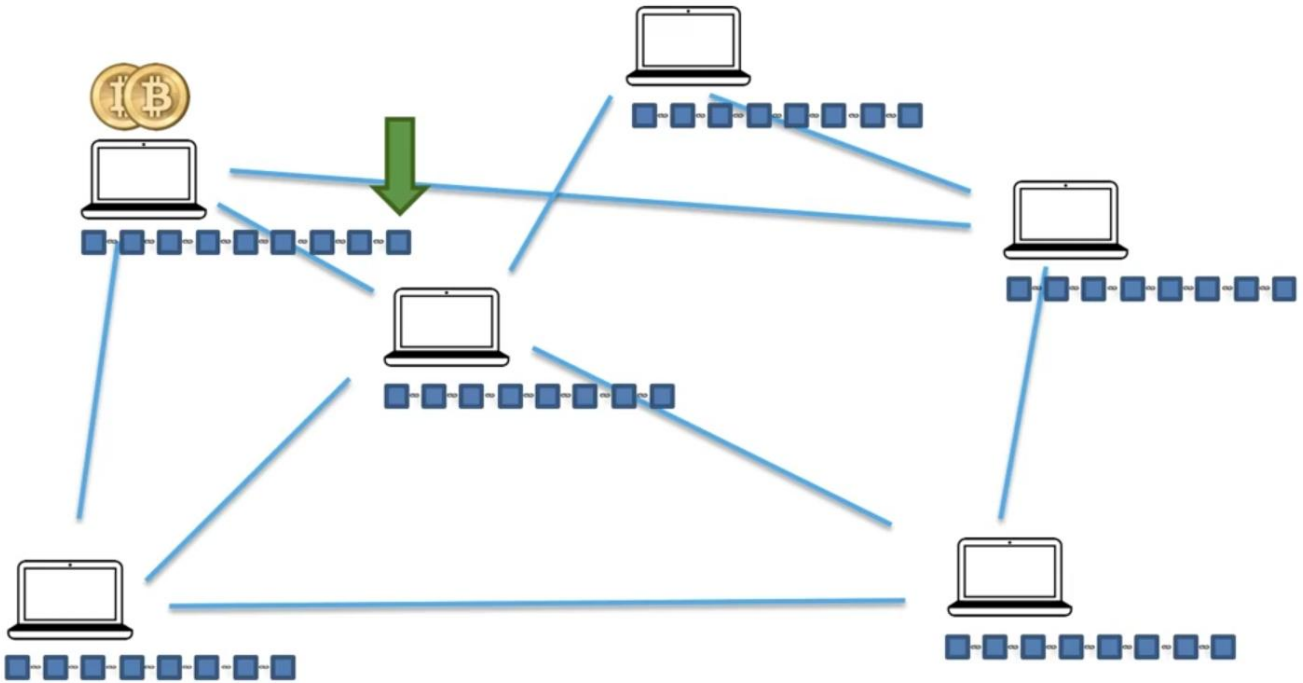
Blockchain Technology Fundamentals

Challenges in Distributed P2P Network



Blockchain Technology Fundamentals

Attackers Challenge in Distributed P2P Network addressed by Consensus

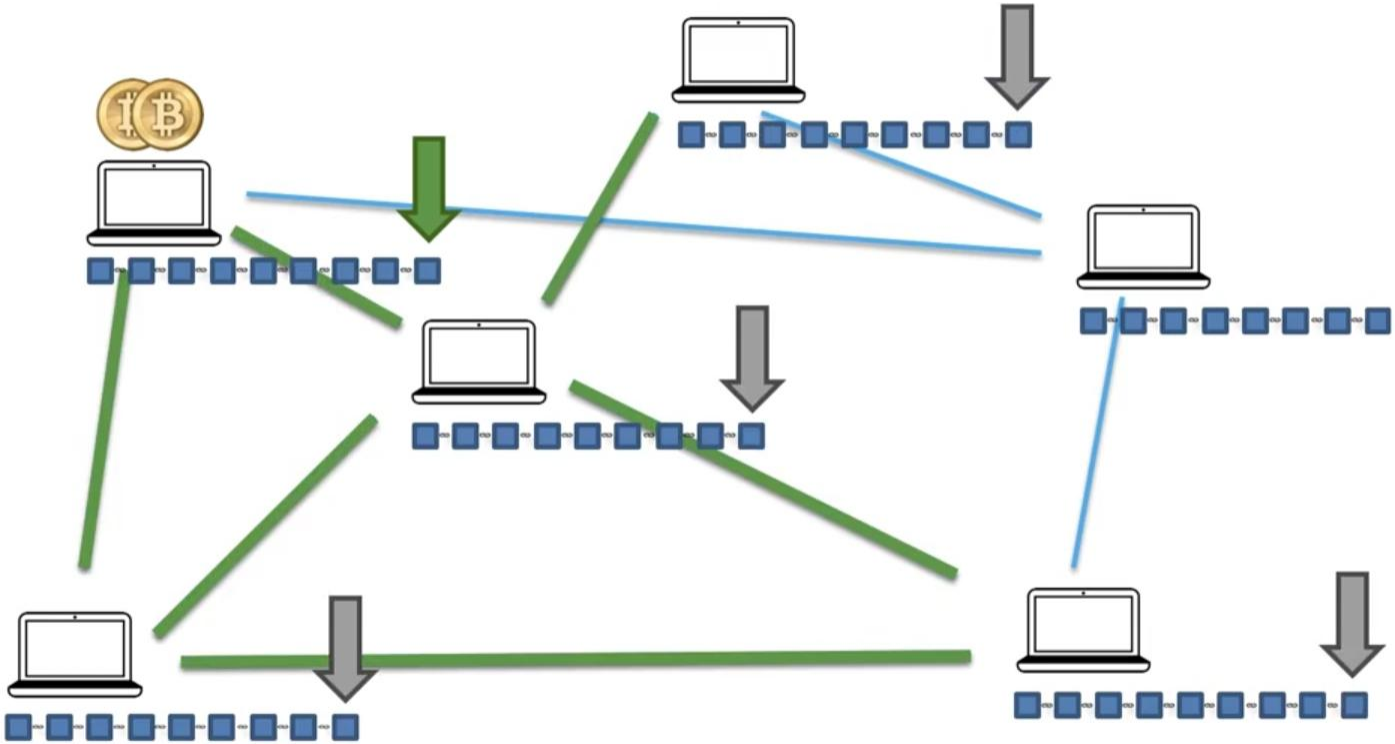


Miners get incentives for :

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

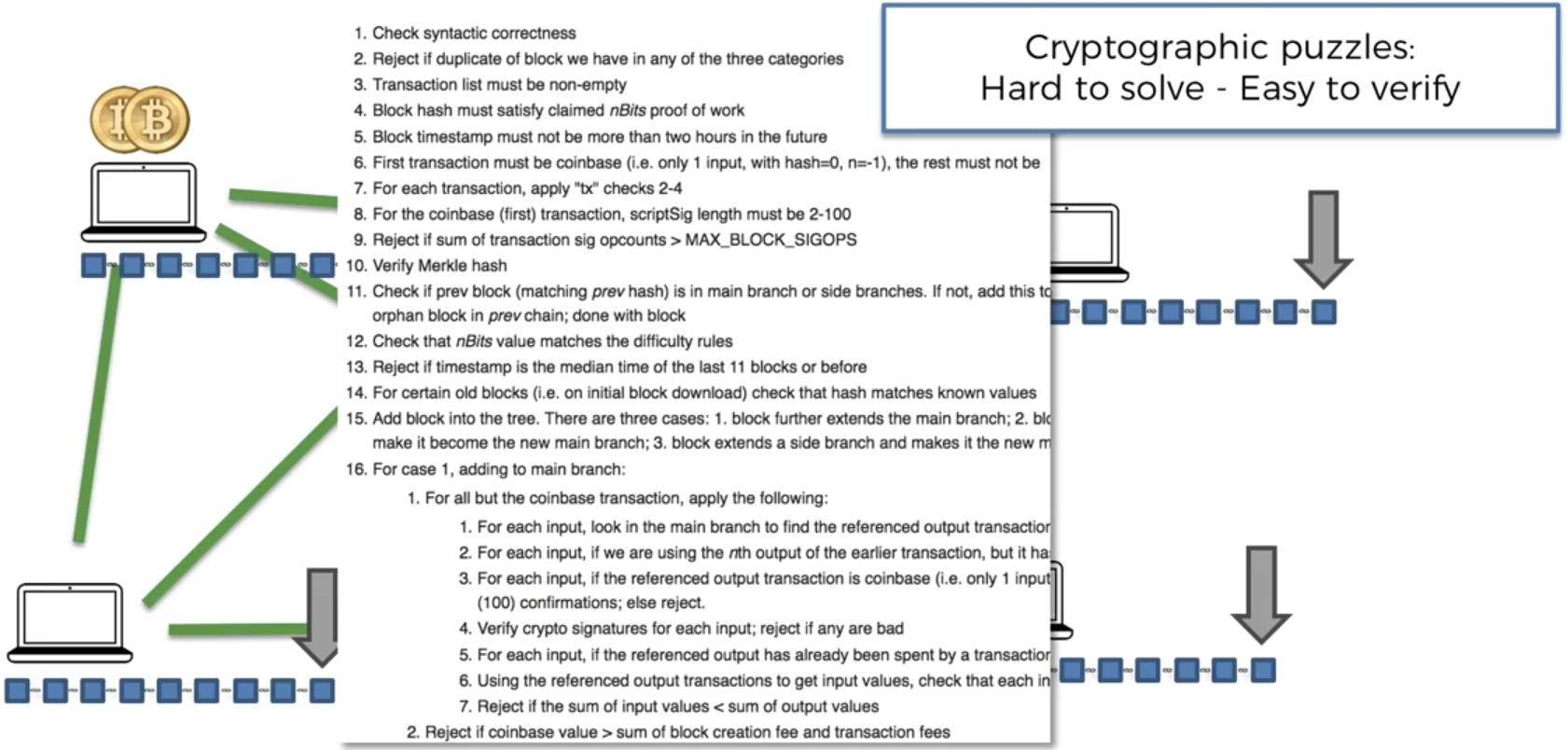
Blockchain Technology Fundamentals

Attackers Challenge in Distributed P2P Network addressed by Consensus



Blockchain Technology Fundamentals

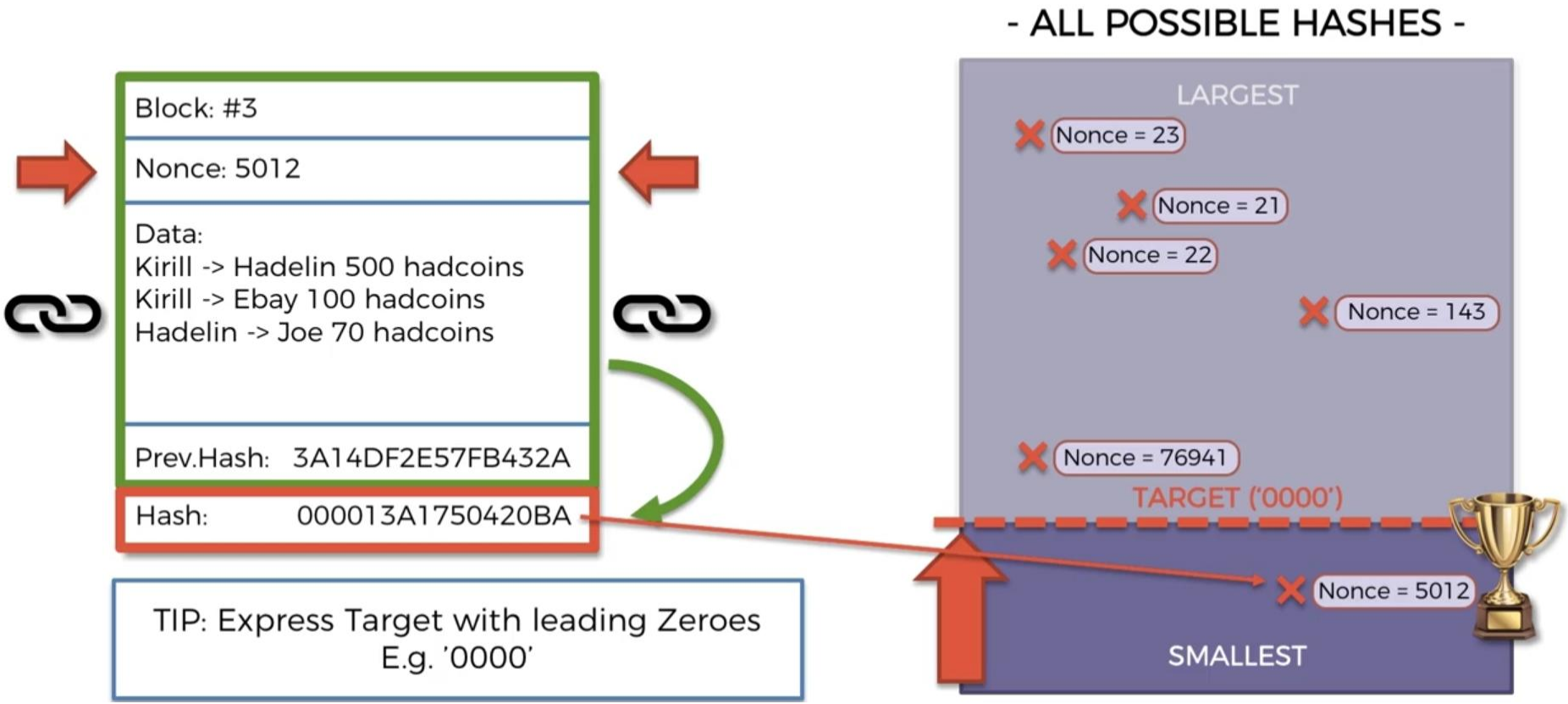
Attackers Challenge in Distributed P2P Network addressed by Consensus



Courtesy : Super Data Science

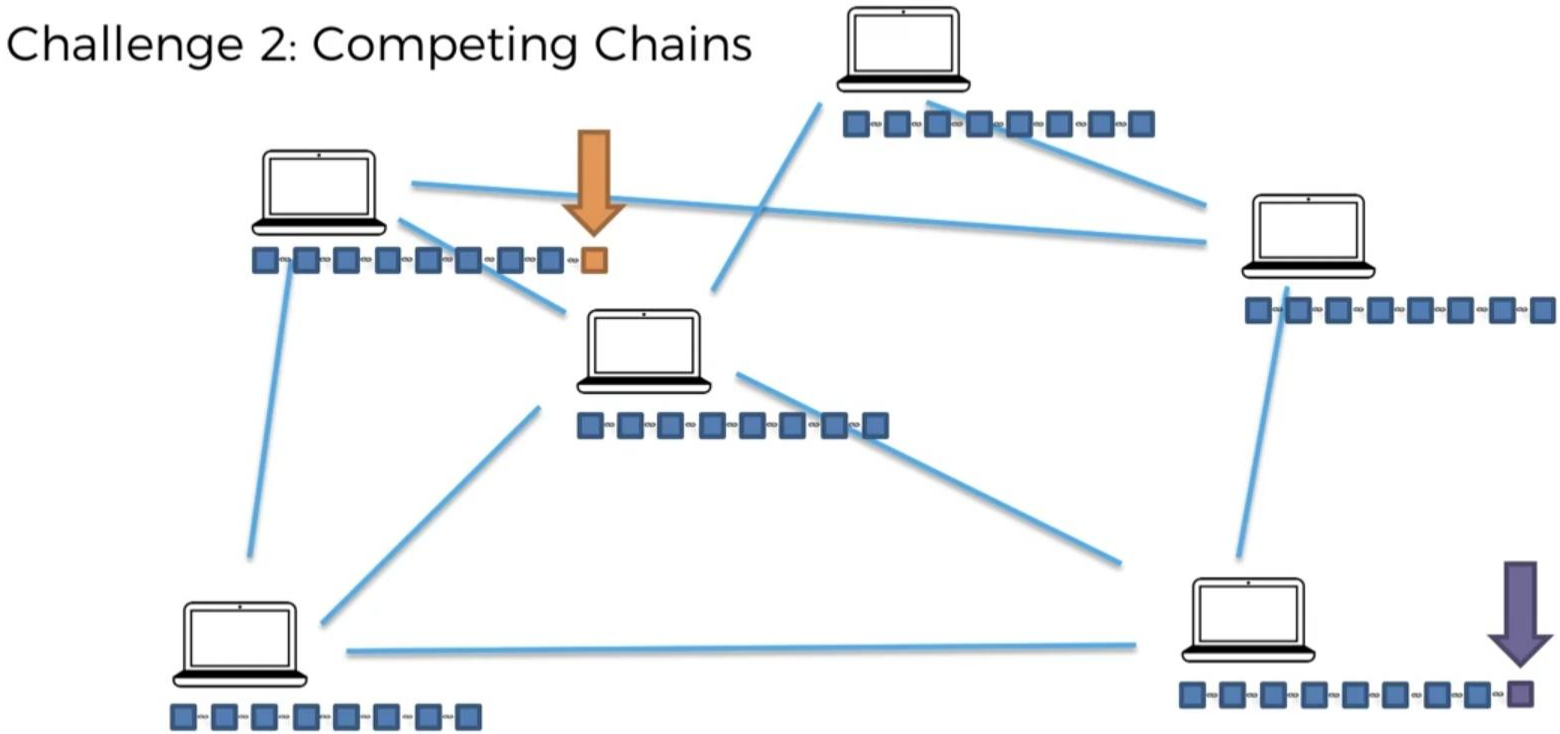
Blockchain Technology Fundamentals

Attackers Challenge in Distributed P2P Network addressed by Consensus



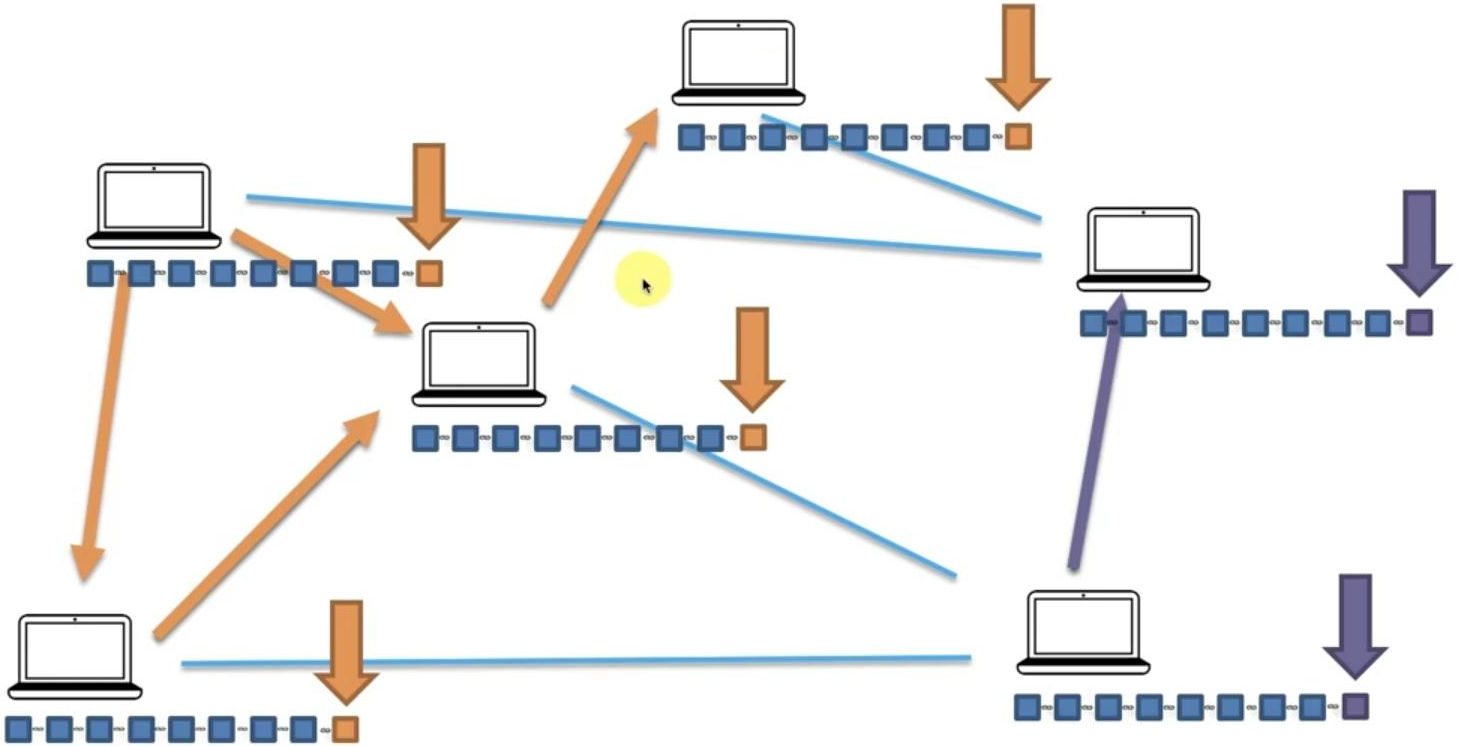
Blockchain Technology Fundamentals

Challenges in Distributed P2P Network



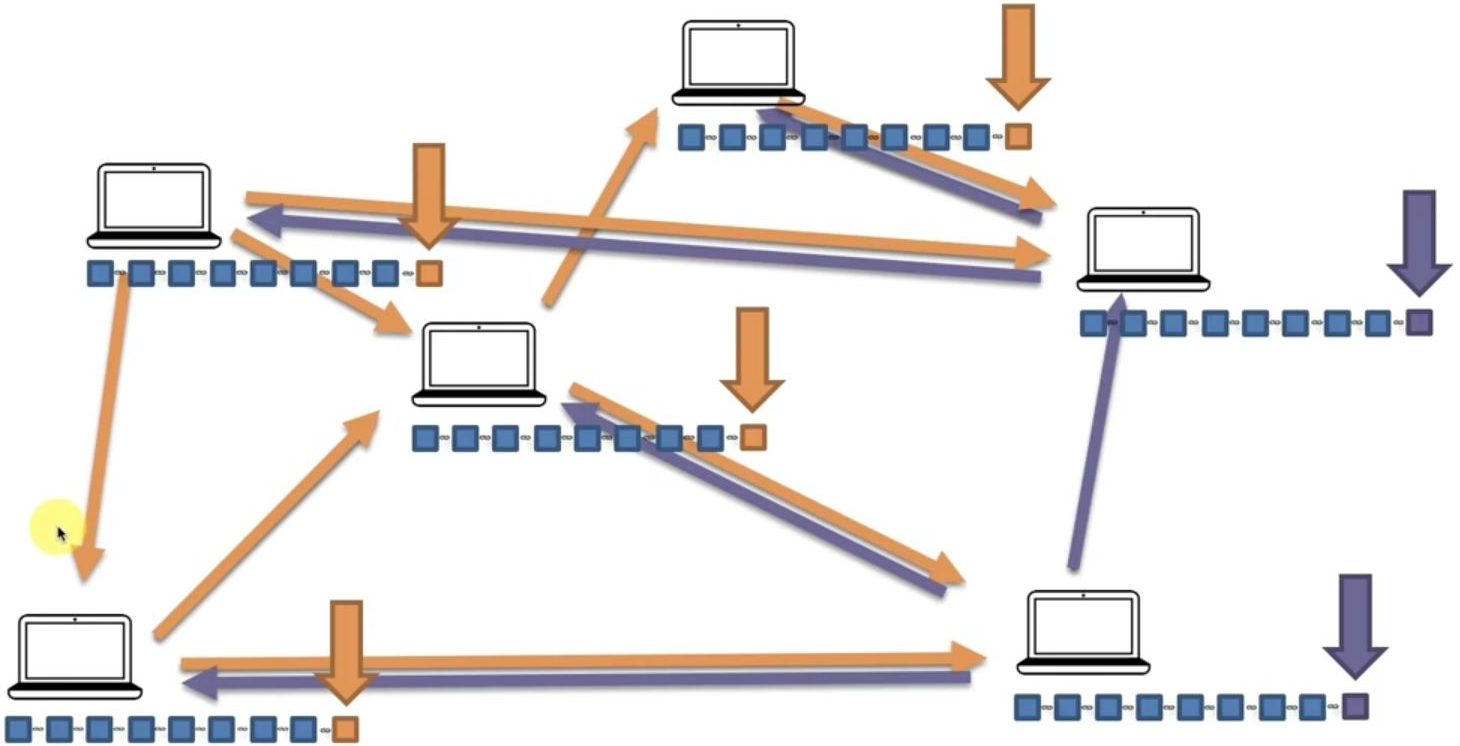
Blockchain Technology Fundamentals

Competing Chains in Distributed P2P Network addressed by Consensus



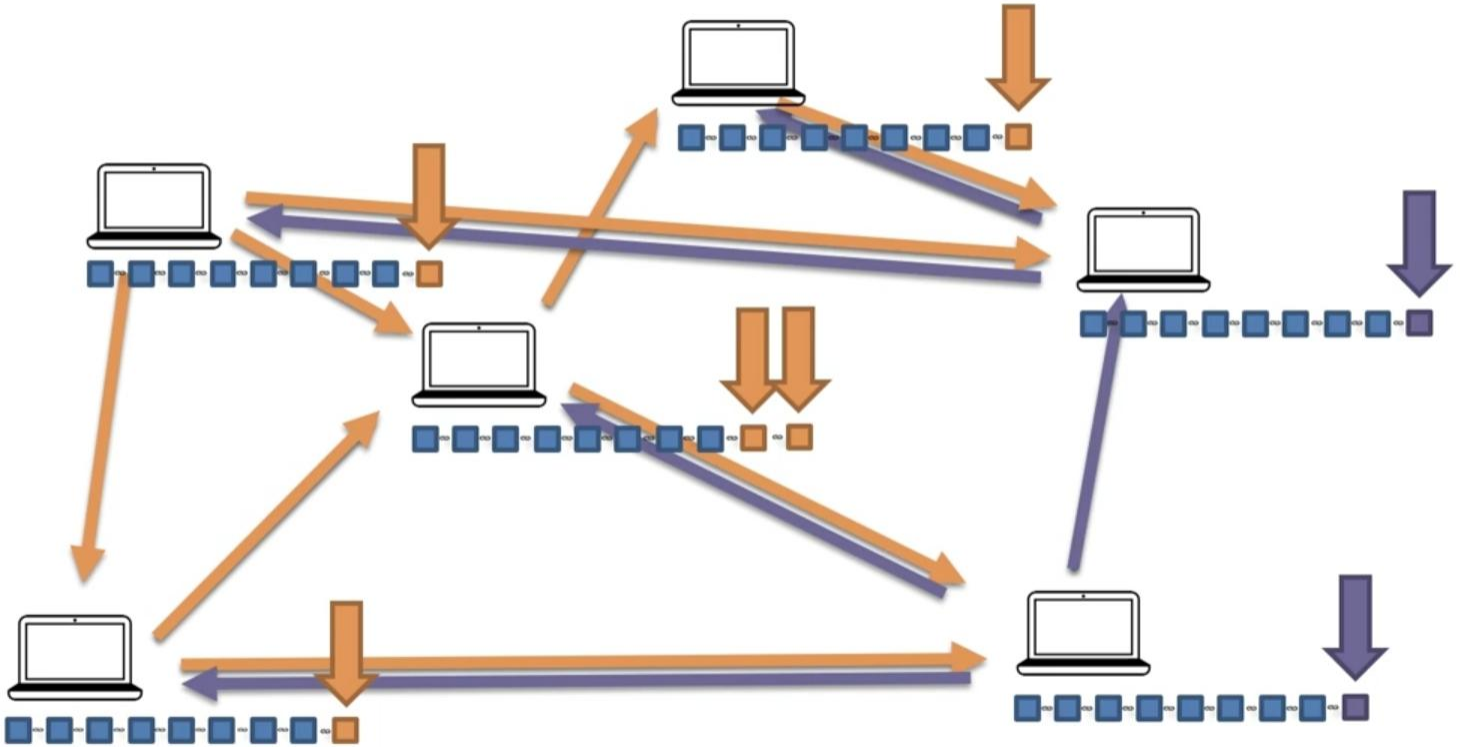
Blockchain Technology Fundamentals

Competing Chains in Distributed P2P Network addressed by Consensus



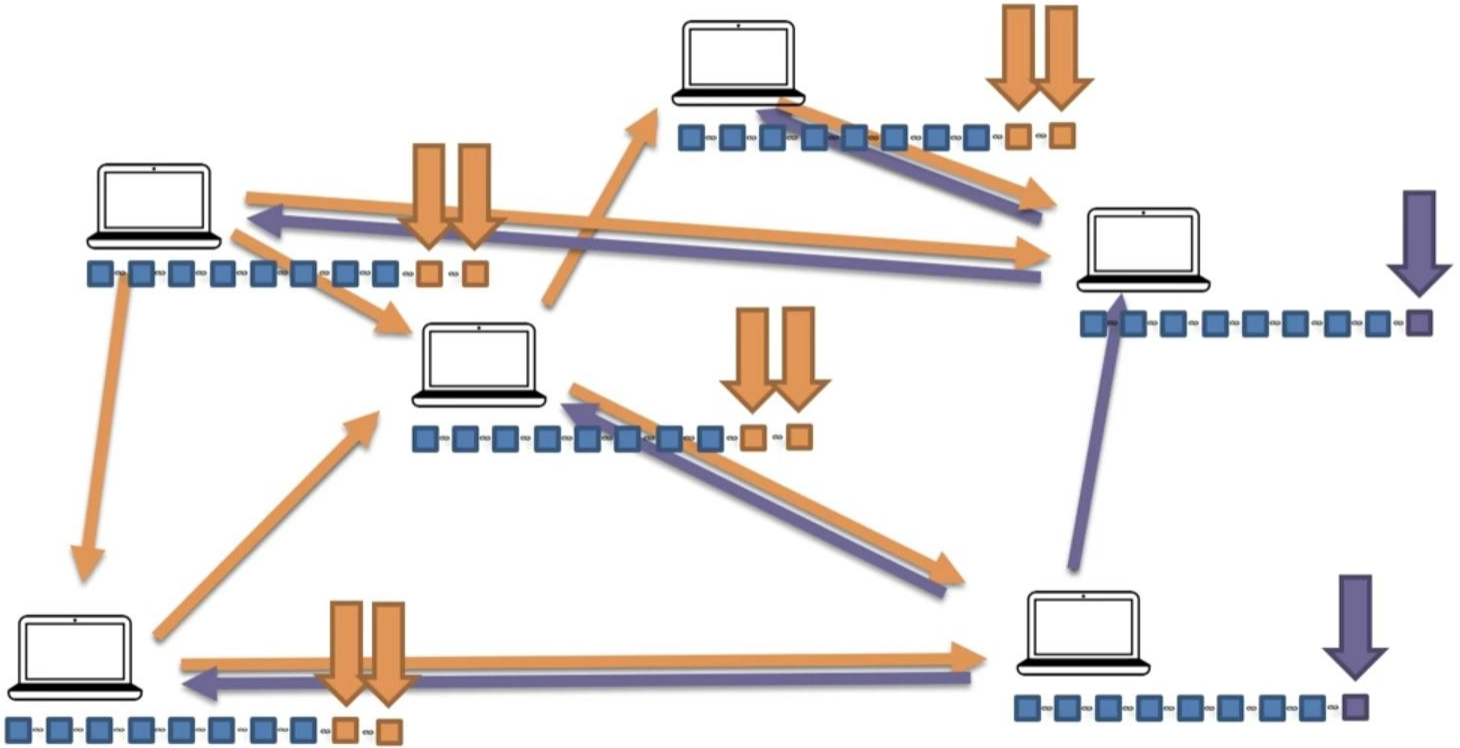
Blockchain Technology Fundamentals

Competing Chains in Distributed P2P Network addressed by Consensus



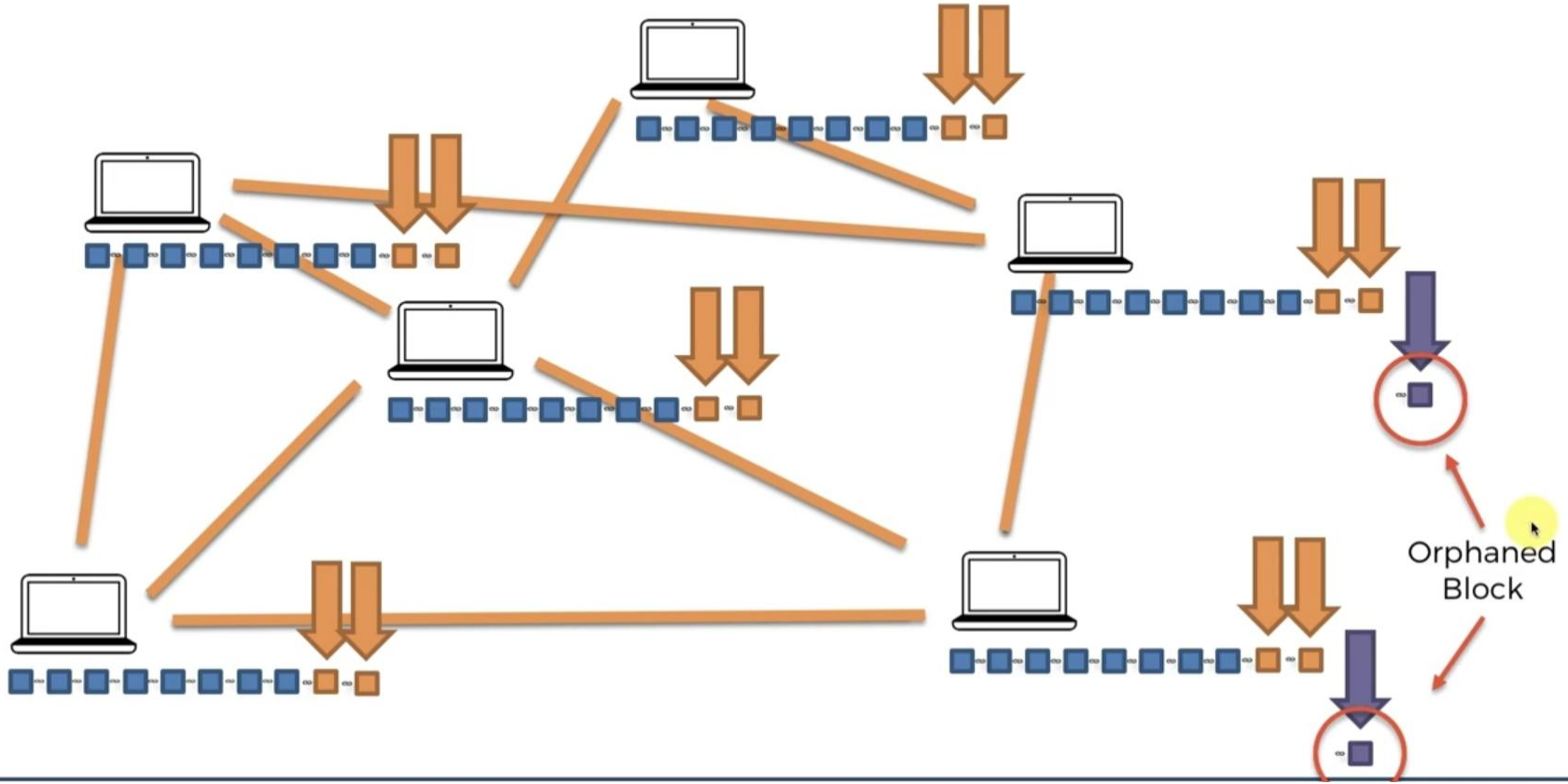
Blockchain Technology Fundamentals

Competing Chains in Distributed P2P Network addressed by Consensus



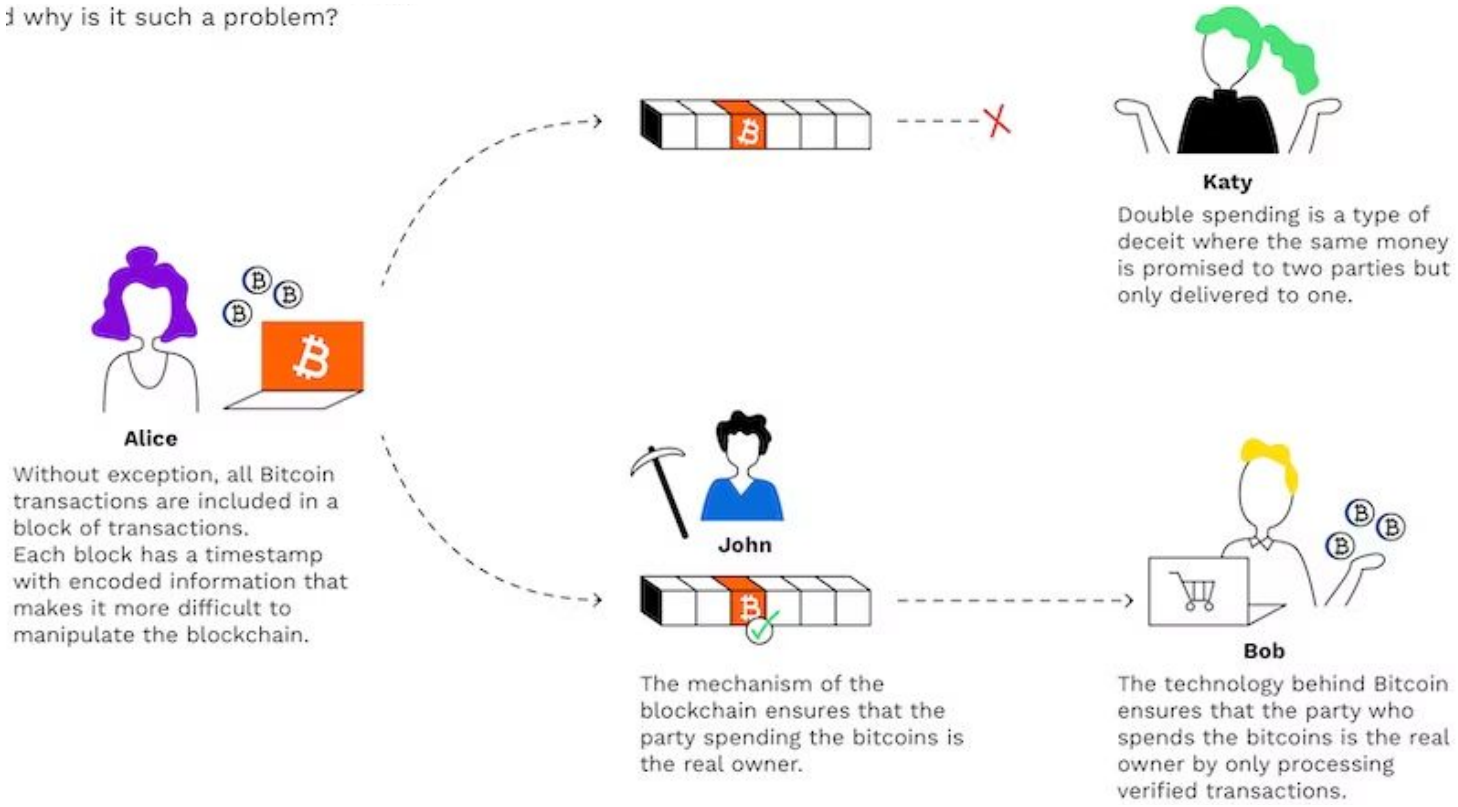
Blockchain Technology Fundamentals

Competing Chains in Distributed P2P Network addressed by Consensus



Blockchain Technology Fundamentals

Double Spending Problem



Courtesy : BitPanda

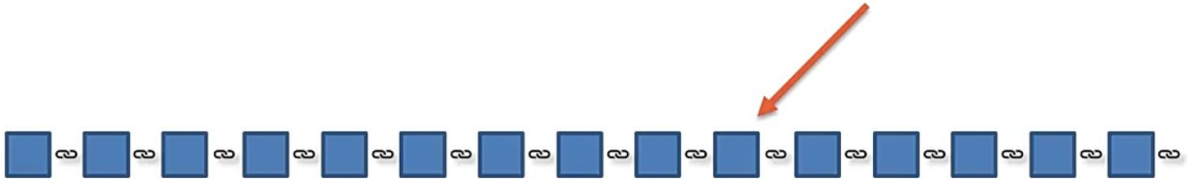
Double Spending Problem

- **Risk that a cryptocurrency can be used twice or more.**
- **Transaction information** within a blockchain **can be altered if specific conditions are met**.
  - The conditions allow modified blocks to enter the blockchain;
  - if this happens, the person that initiated the alteration can reclaim spent coins.
- occurs when someone alters a blockchain network and inserts a special one that allows them to reacquire a cryptocurrency.
- Double-spending can happen, but it is more likely that a cryptocurrency is stolen from a wallet that wasn't adequately protected and secured.
- Many variations of attacks could be used for double-spending—**51% is one of the most commonly cited attacks,** while the unconfirmed transaction attack is most commonly seen.

Courtesy : Investopedia

Blockchain Technology Fundamentals

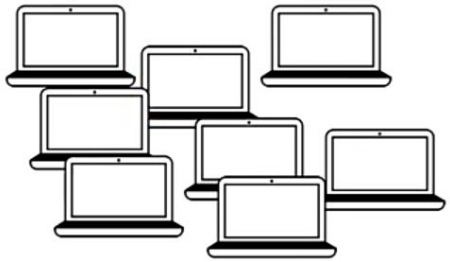
51% Attack



This is NOT the 51% attack

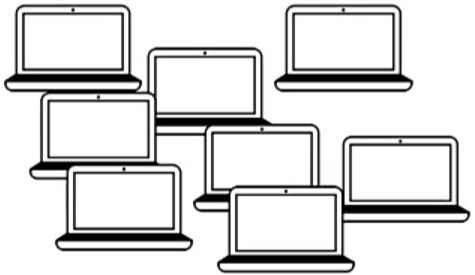
Blockchain Technology Fundamentals

51% Attack



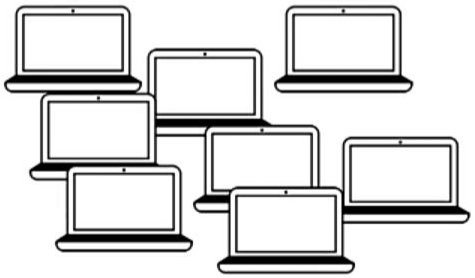
Blockchain Technology Fundamentals

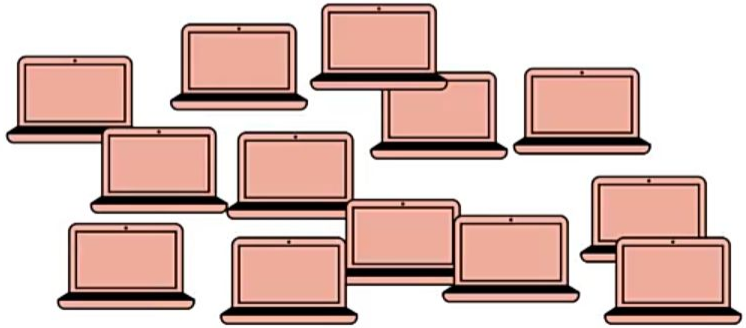
51% Attack



Blockchain Technology Fundamentals

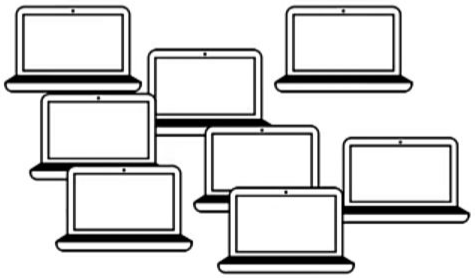
51% Attack

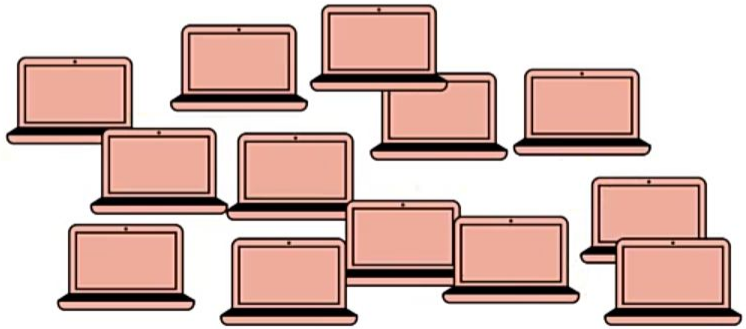




Blockchain Technology Fundamentals

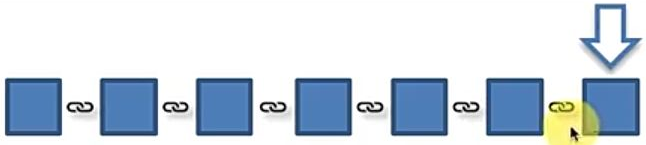
51% Attack

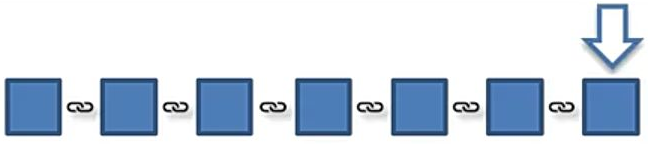


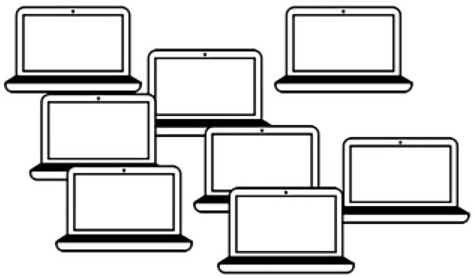


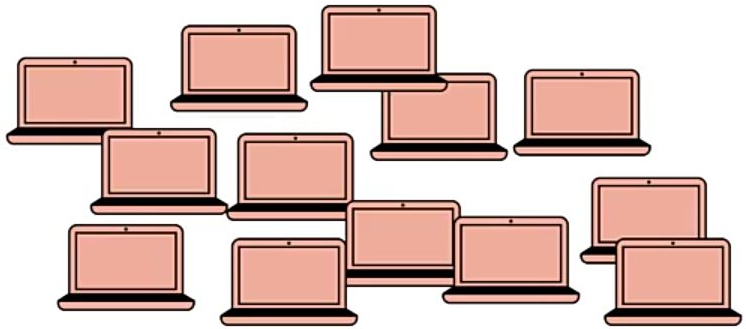
Blockchain Technology Fundamentals

51% Attack



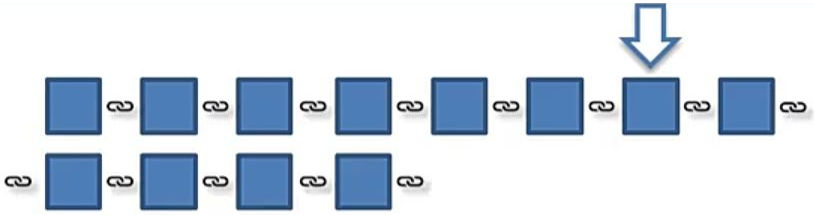


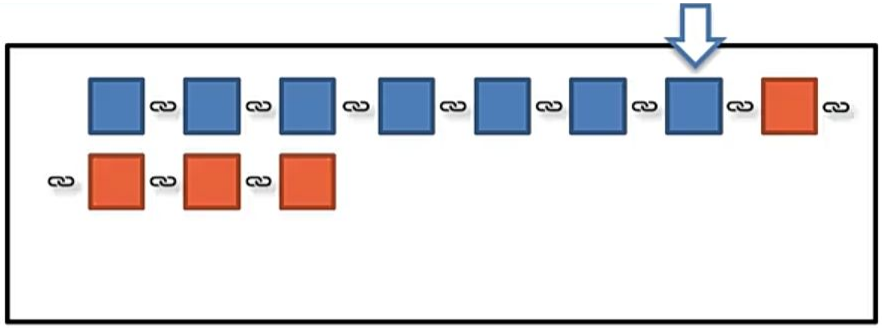


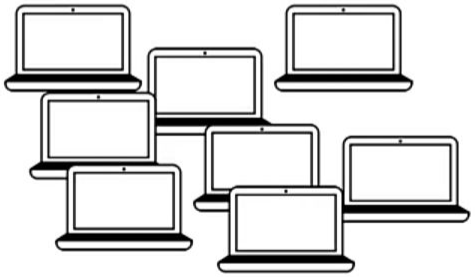


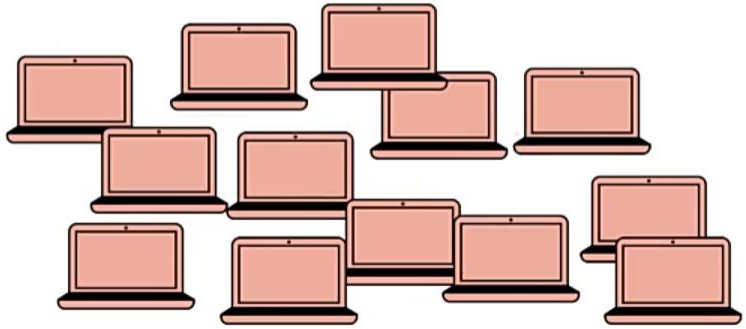
Blockchain Technology Fundamentals

51% Attack



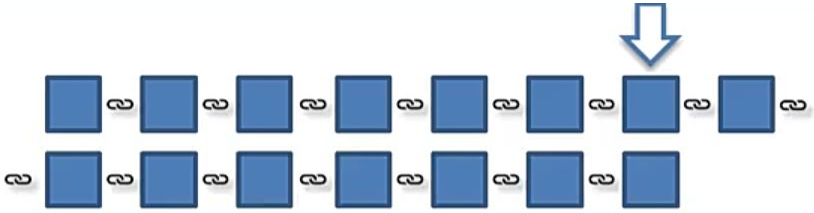


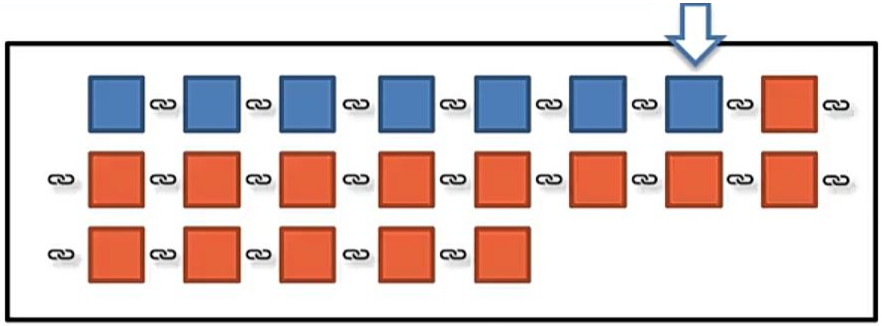


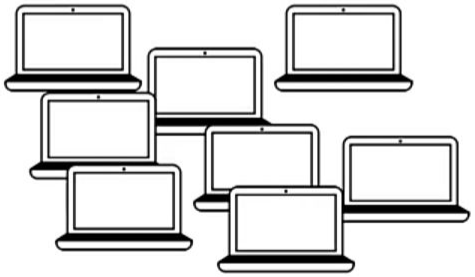


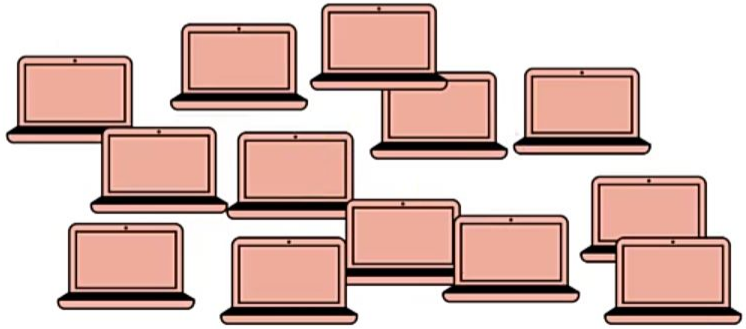
Blockchain Technology Fundamentals

51% Attack

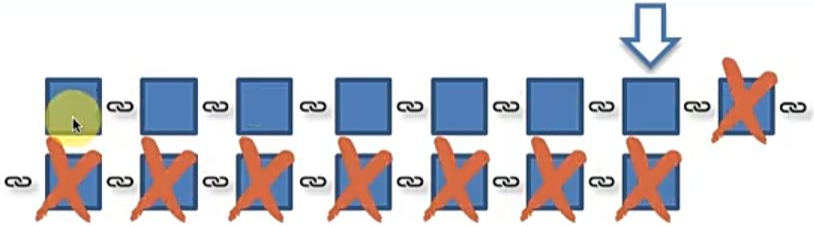


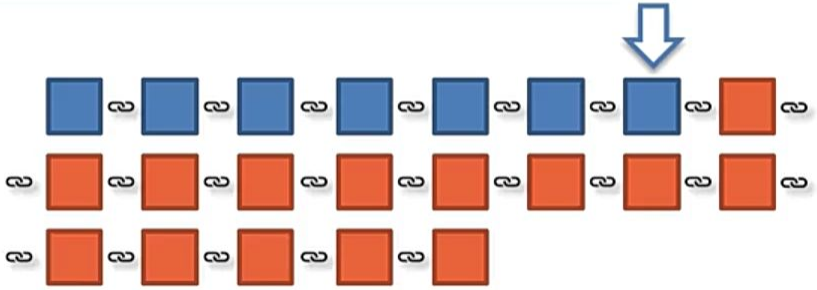


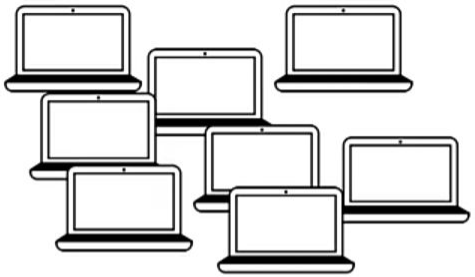


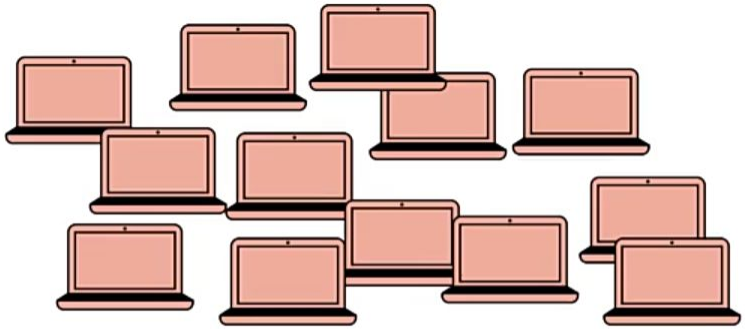


51% Attack

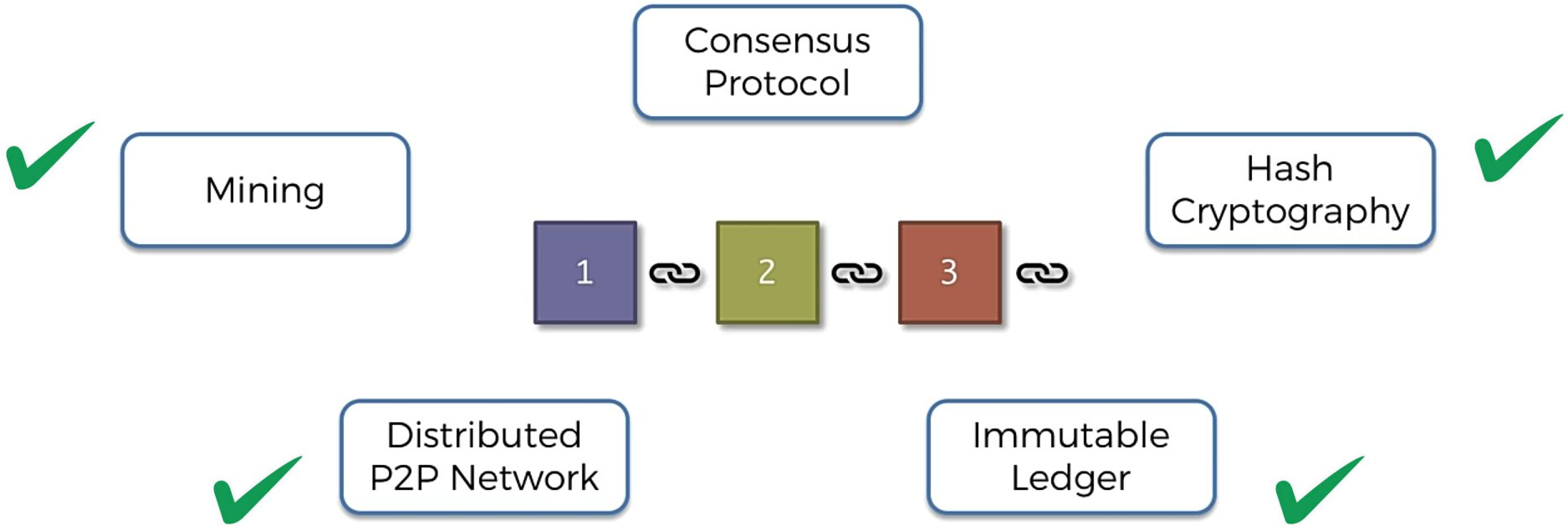




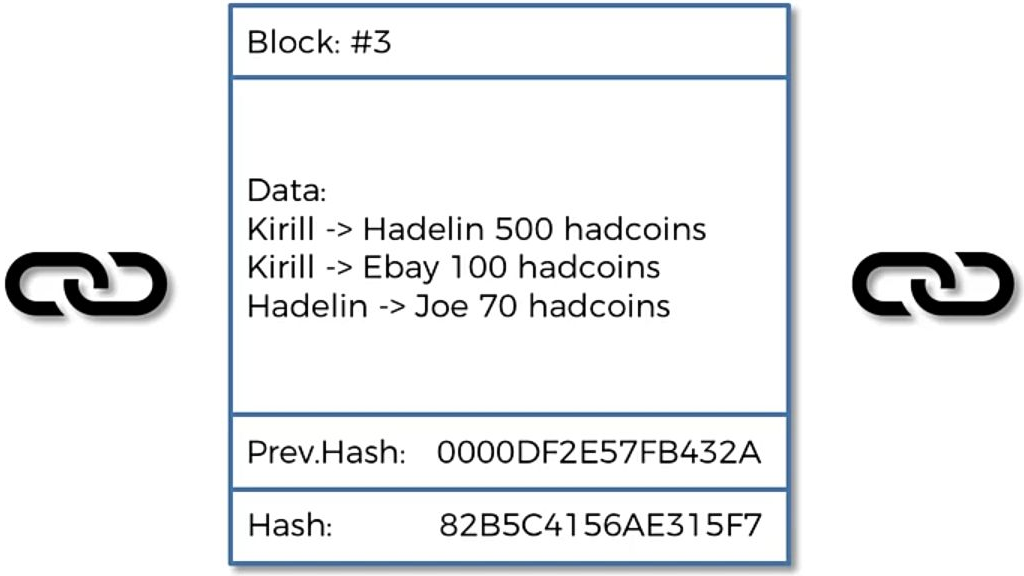




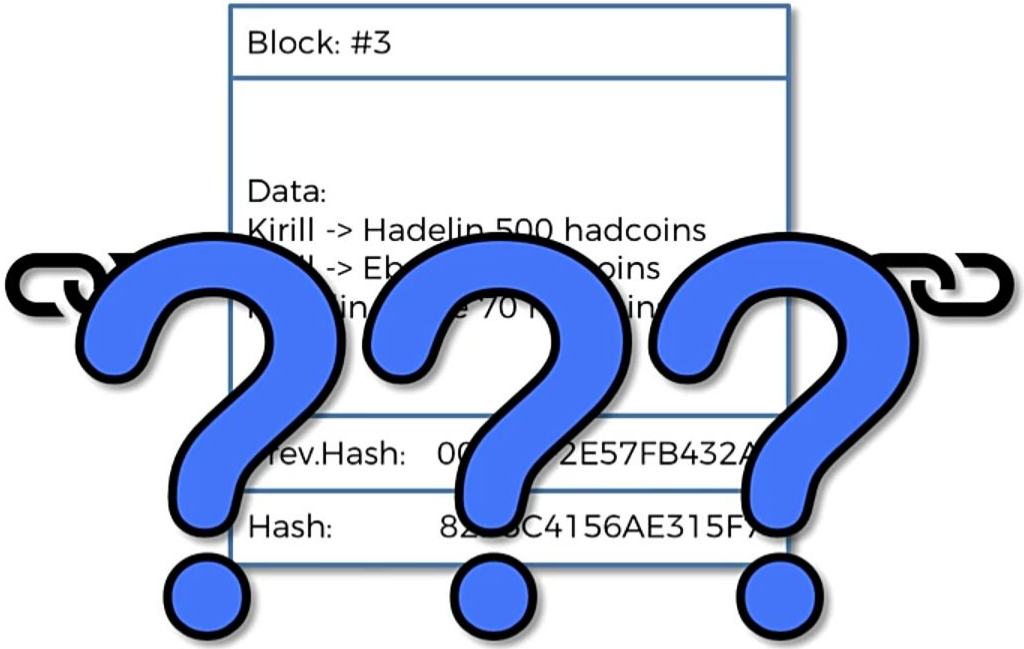
Blockchain Technology Fundamentals



How Mining Works ?

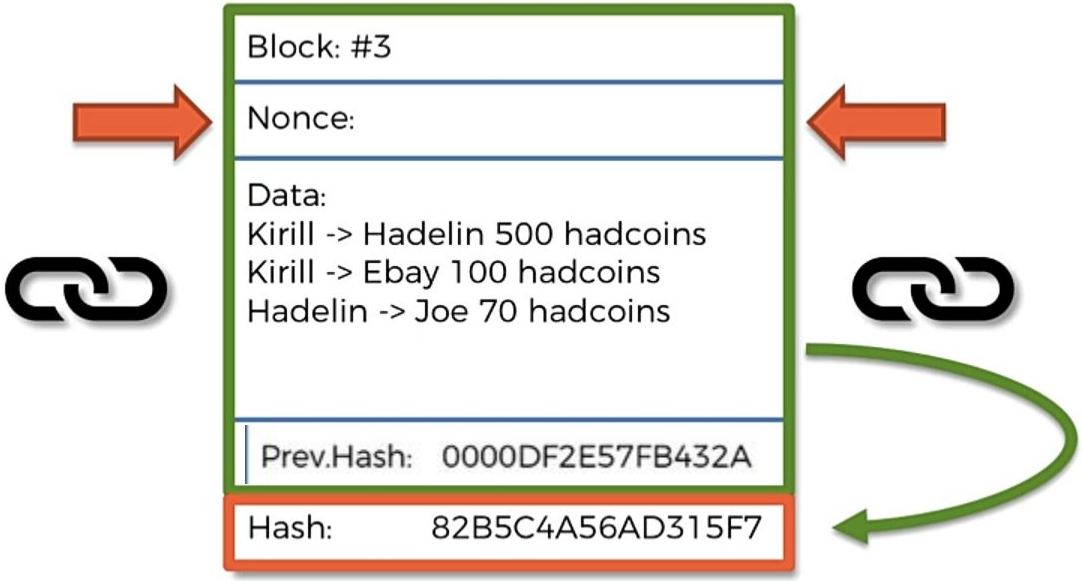


How Mining Works ?

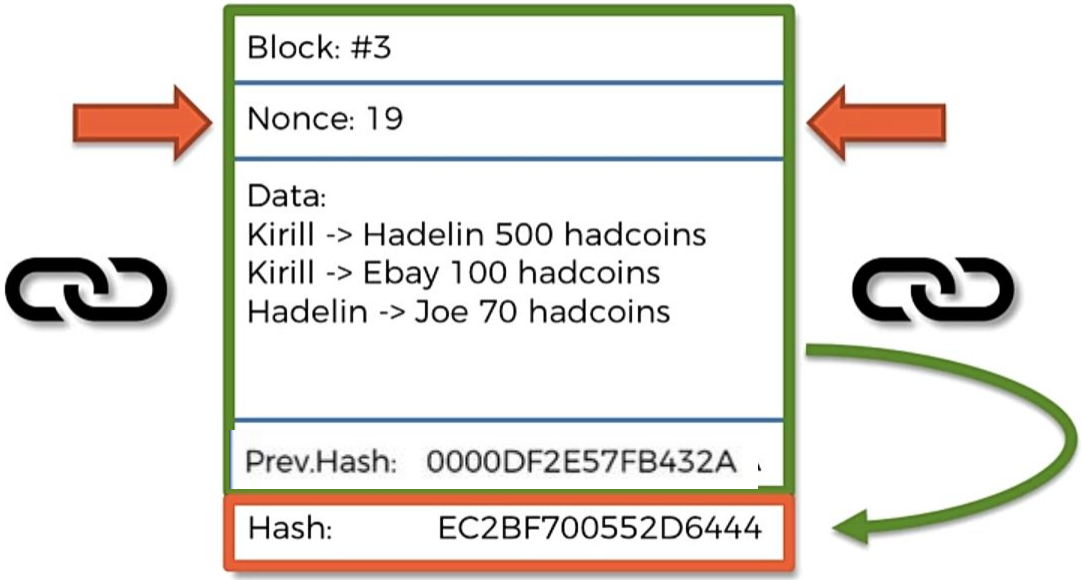


How Mining Works ?

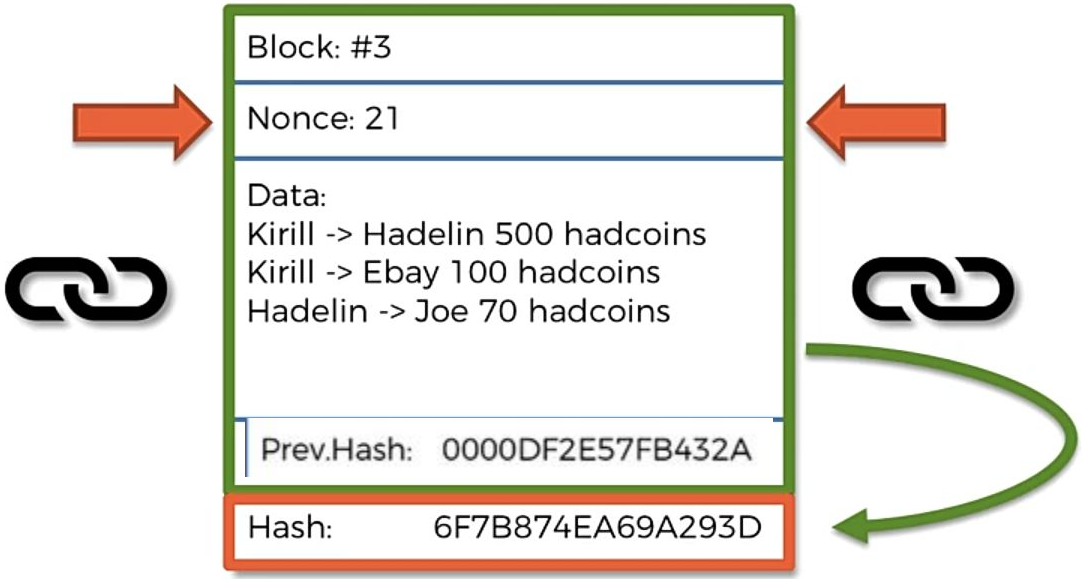
How Mining Works ?



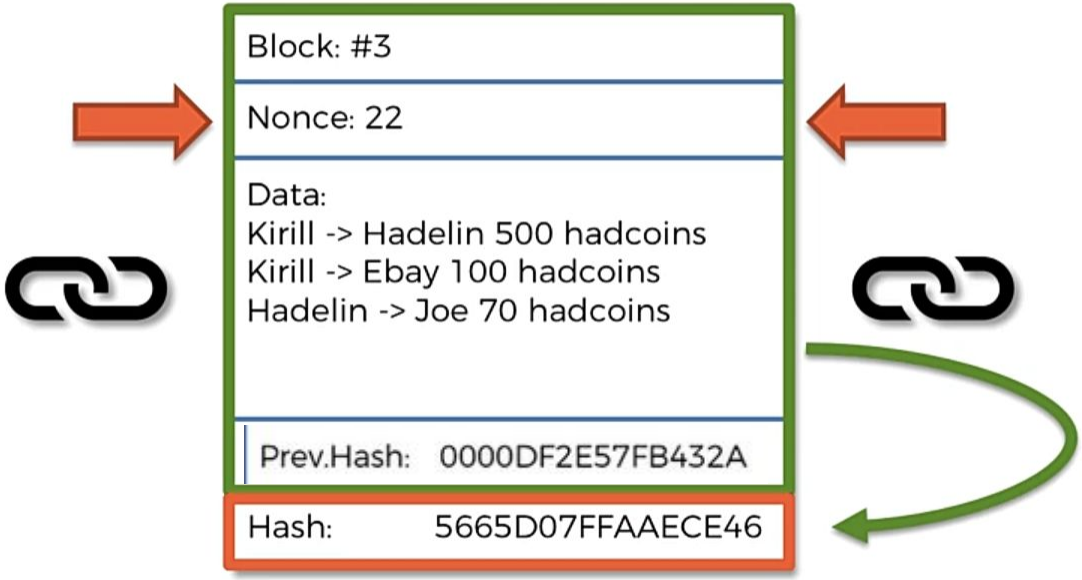
How Mining Works ?



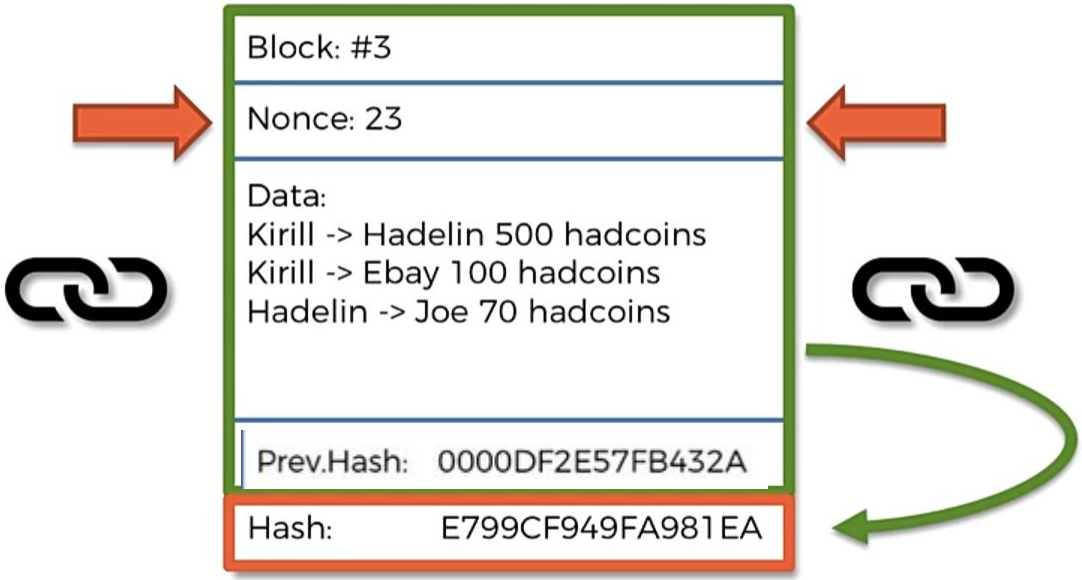
How Mining Works ?



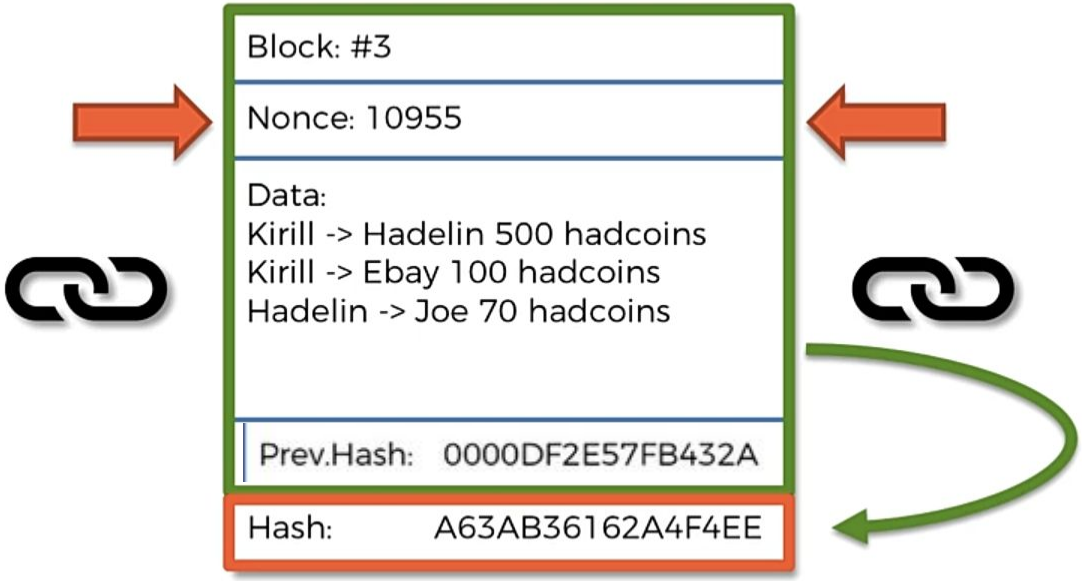
How Mining Works ?



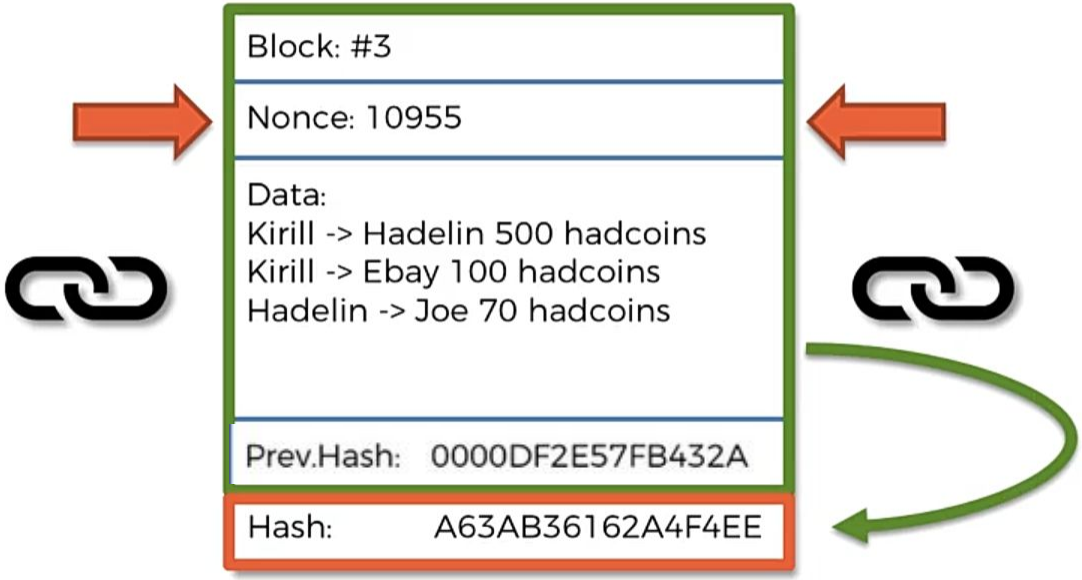
How Mining Works ?



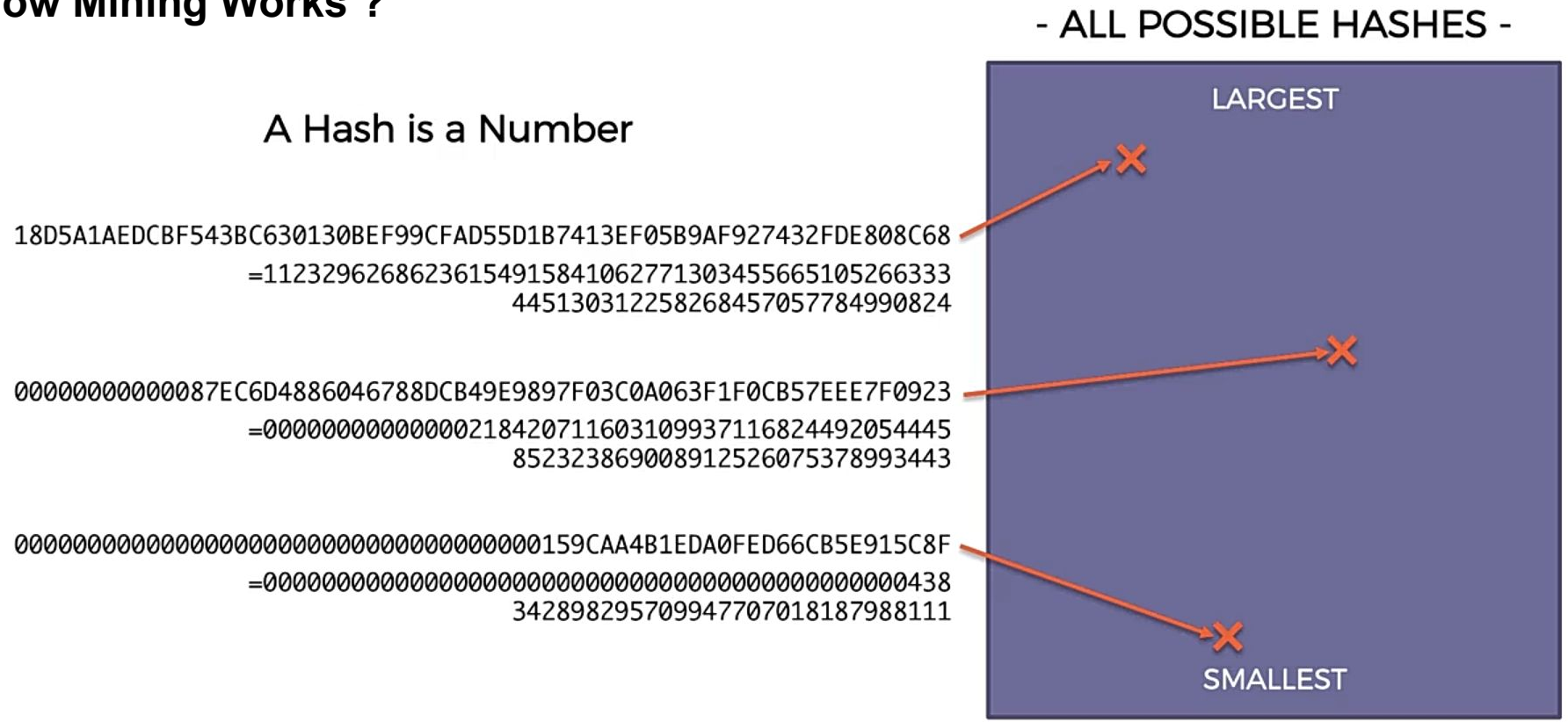
How Mining Works ?



How Mining Works ?



How Mining Works ?

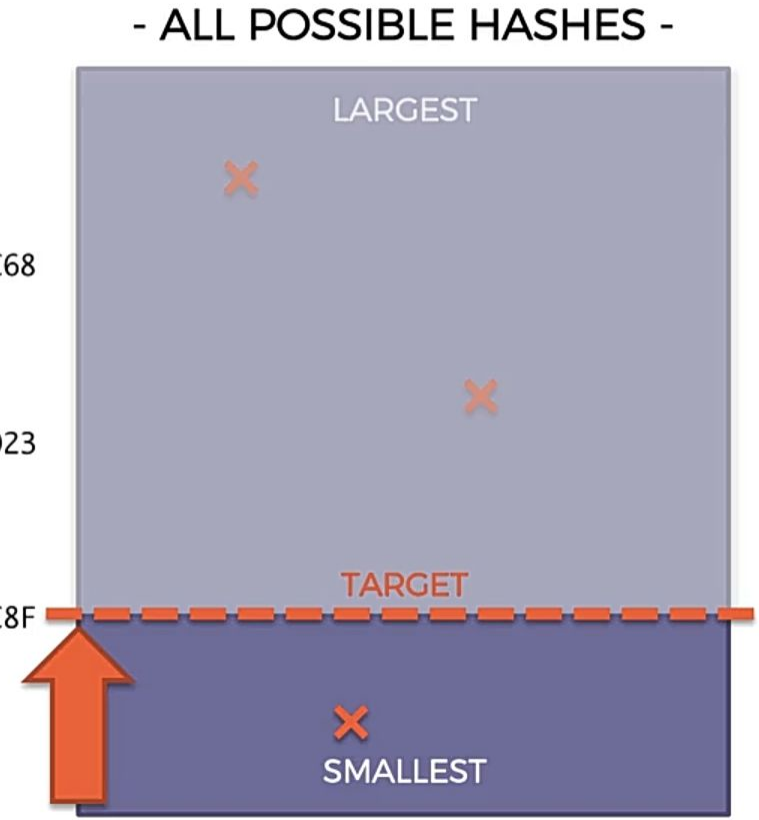


How Mining Works ?

18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68

00000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923

00000000000000000000000000000000000000159CAA4B1EDA0FED66CB5E915C8F



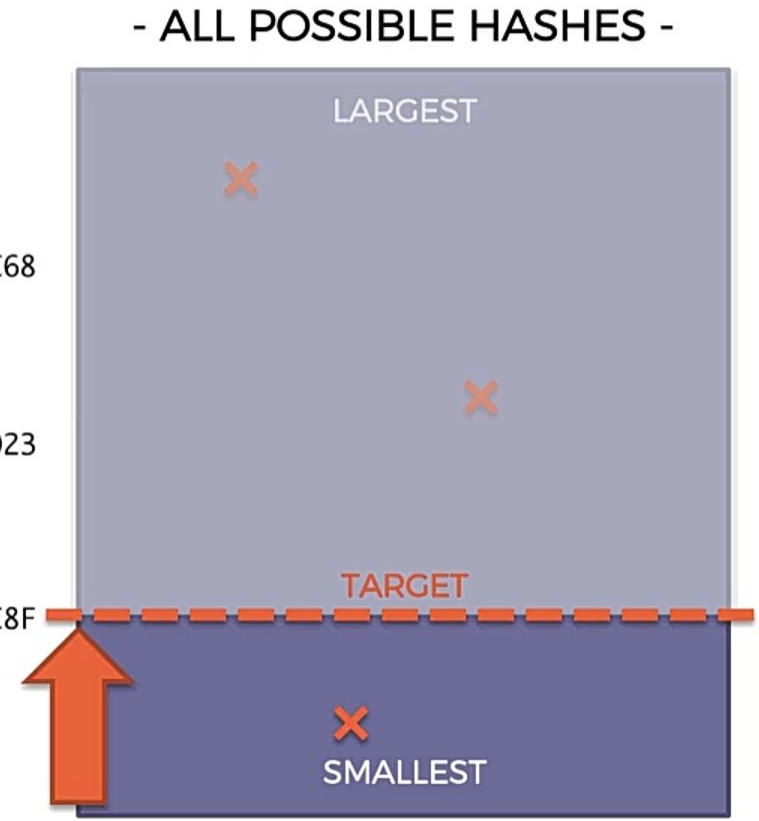
How Mining Works ?

18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68

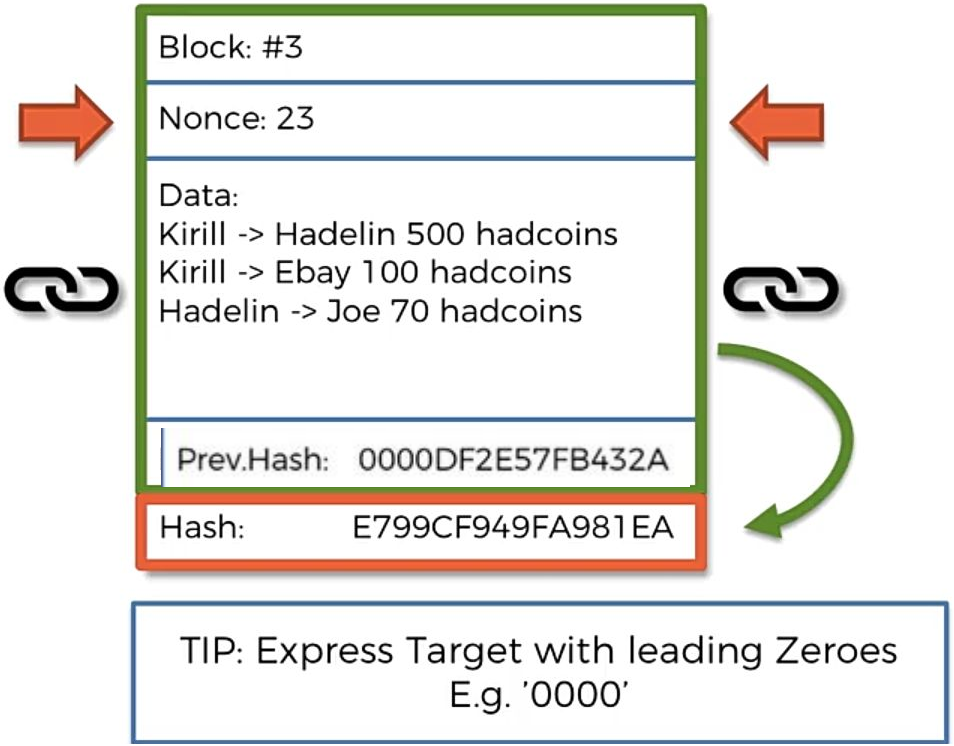
00000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923

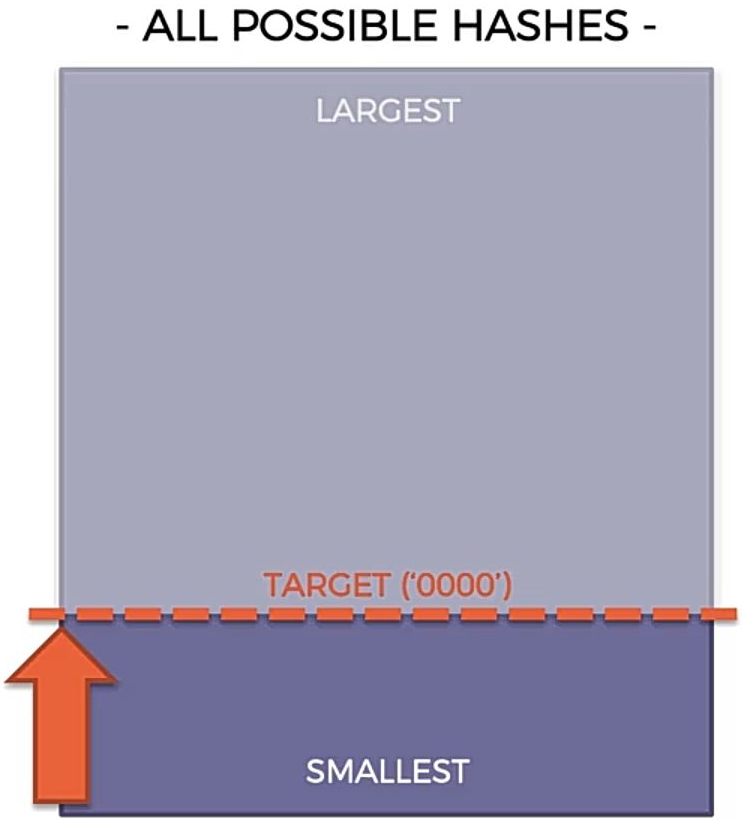
00000000000000000000000000000000000000159CAA4B1EDA0FED66CB5E915C8F

TIP: Express Target with leading Zeroes
E.g. '0000'

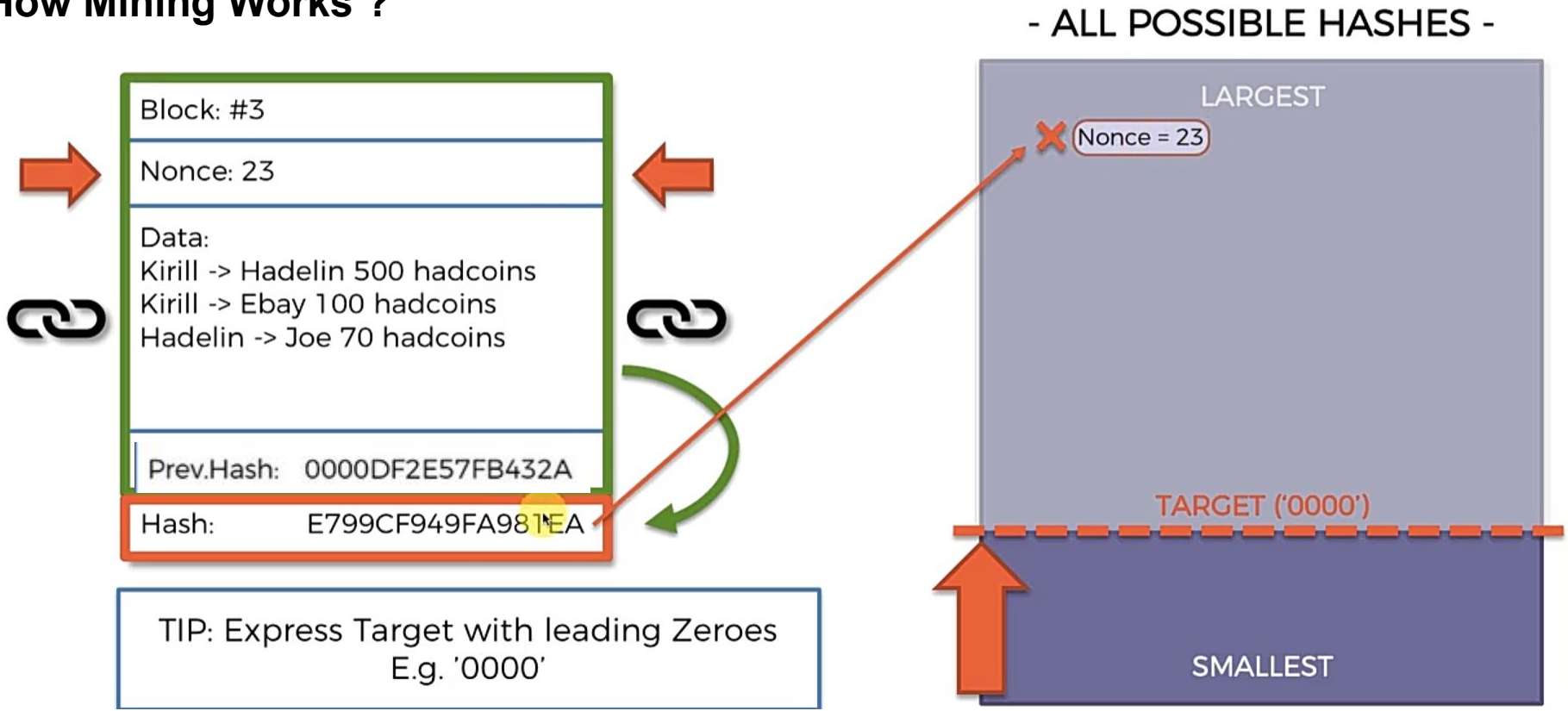


How Mining Works ?

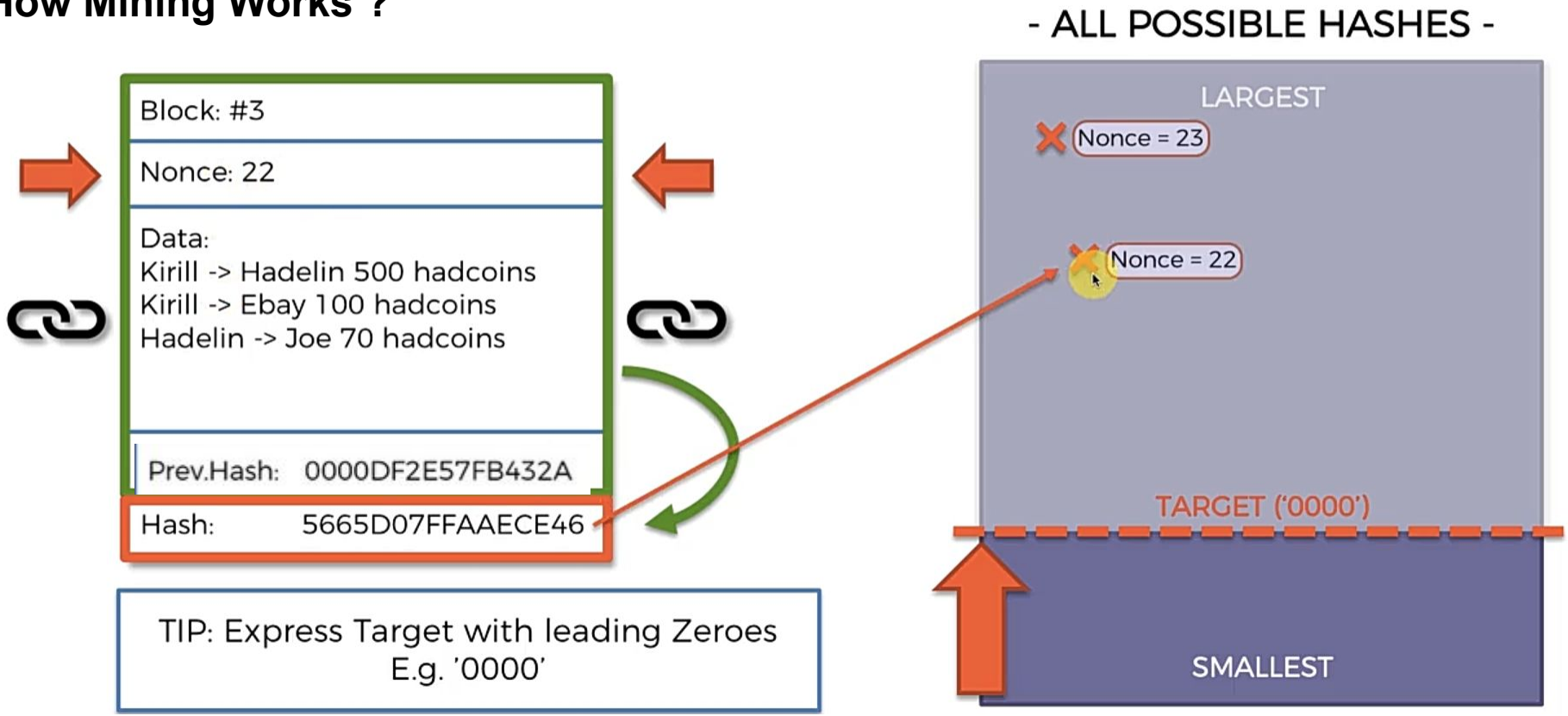




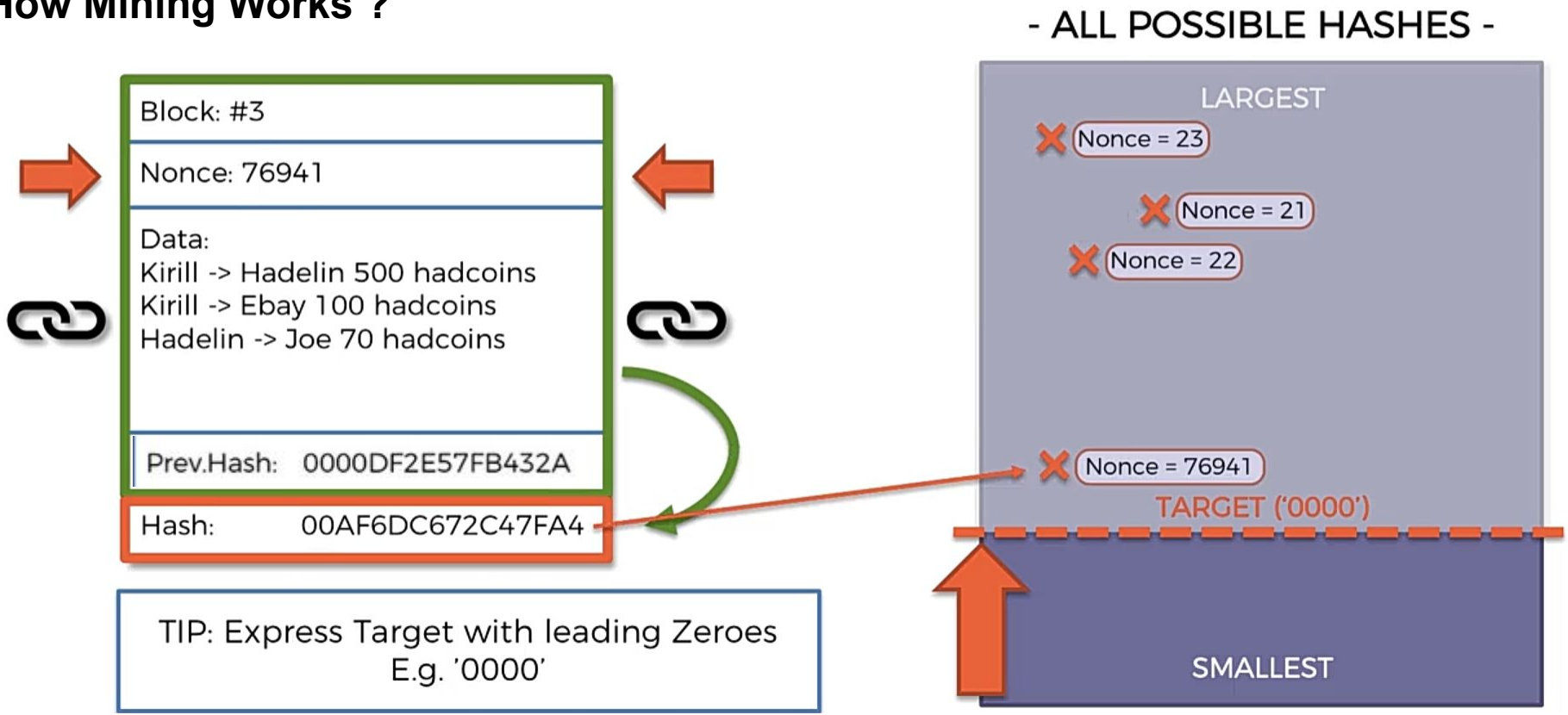
How Mining Works ?



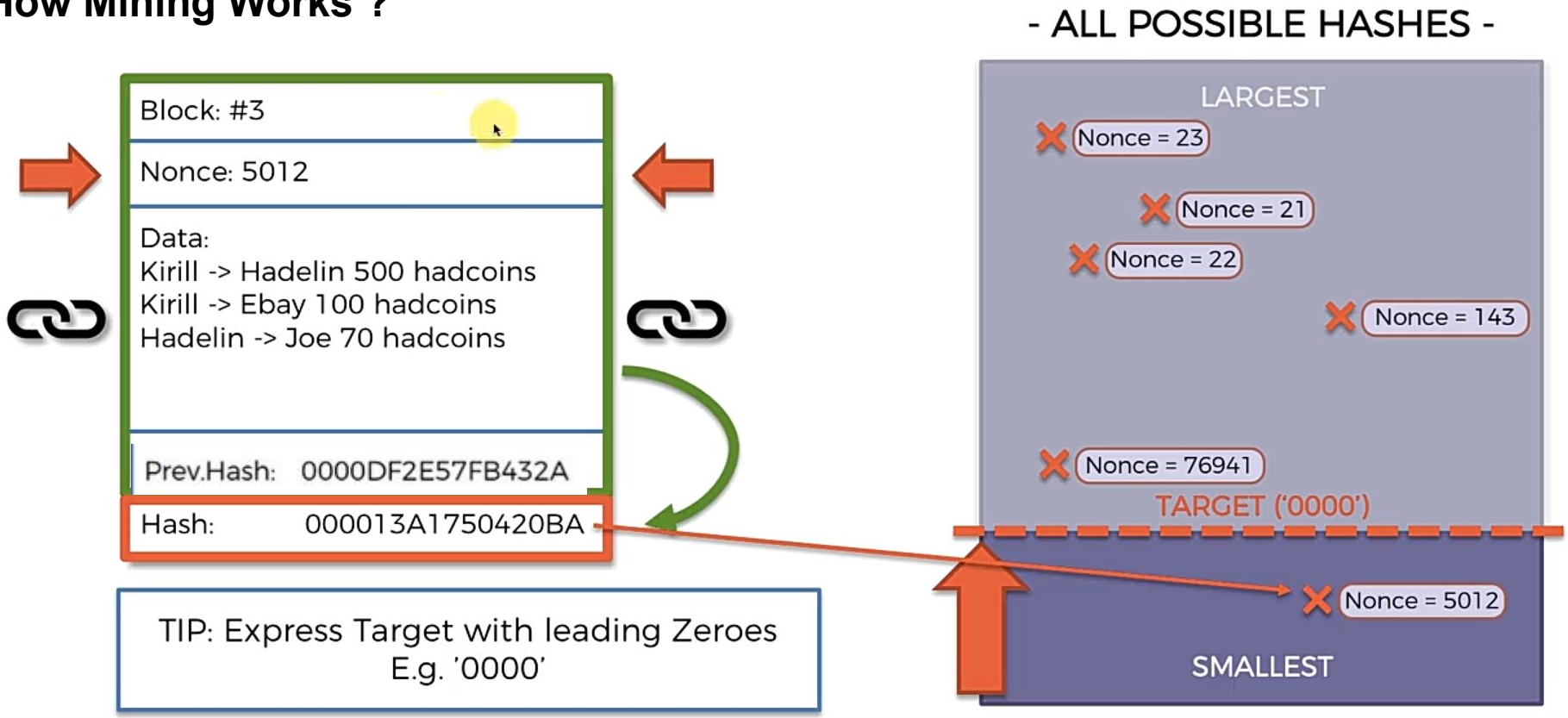
How Mining Works ?



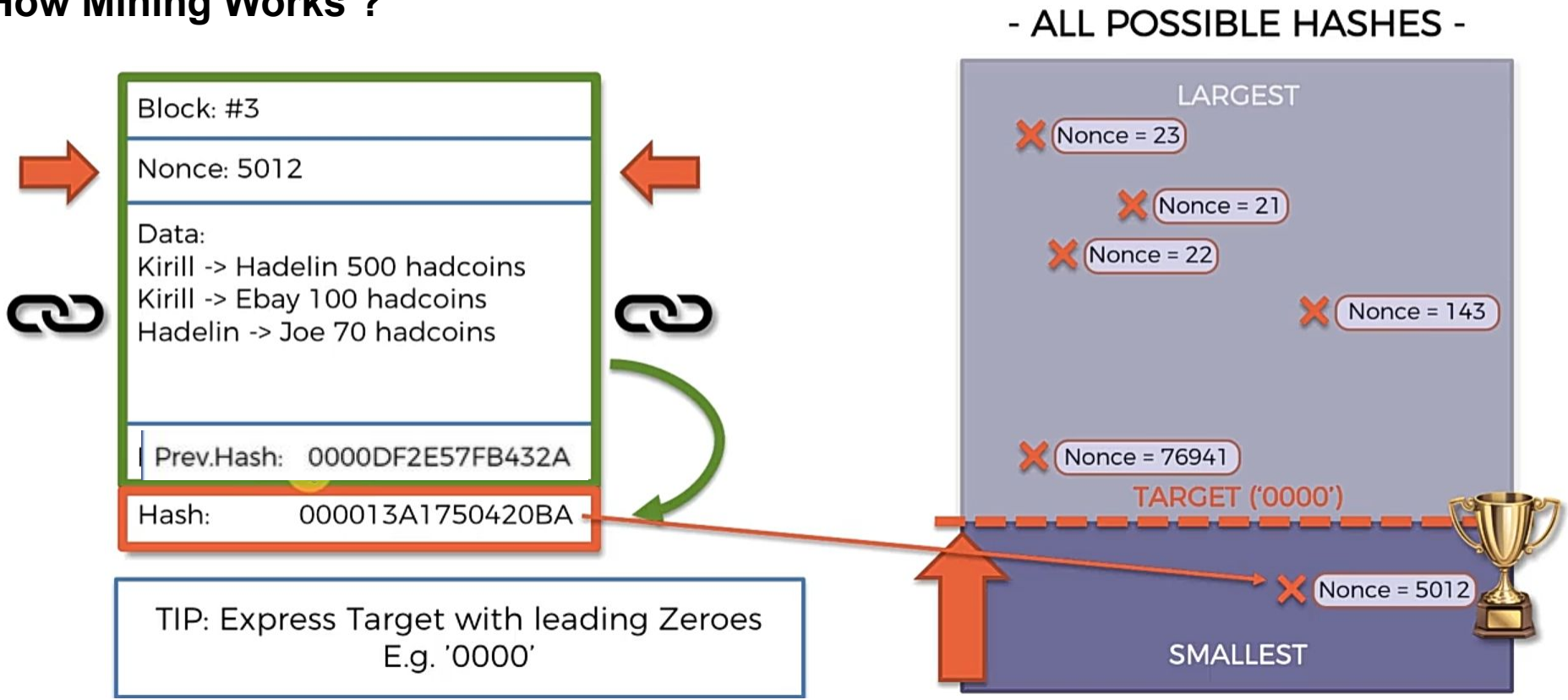
How Mining Works ?



How Mining Works ?



How Mining Works ?



Blockchain Technology Fundamentals

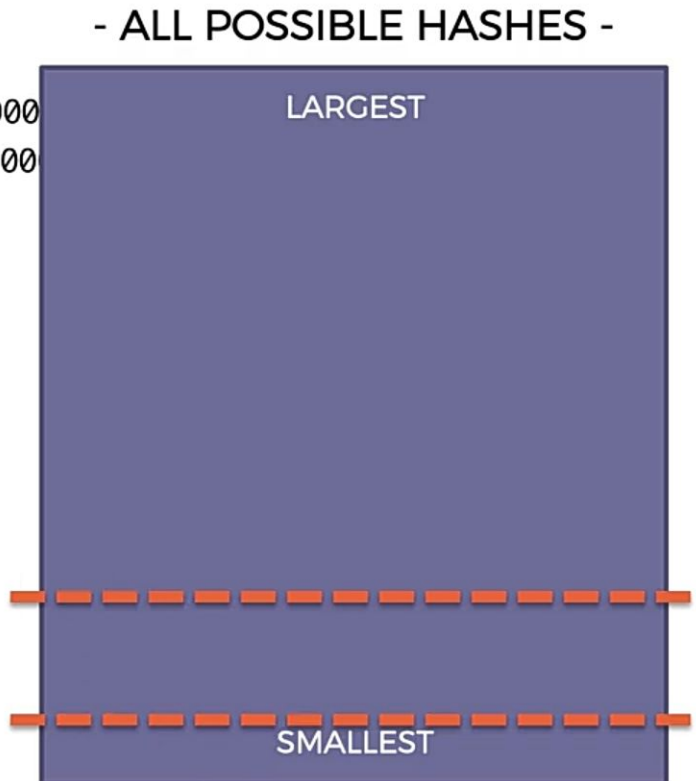
Understanding Mining Difficulty

Difficulty = current target / max target

Curr target = `00000000000000005d97dc0000000000000000000`

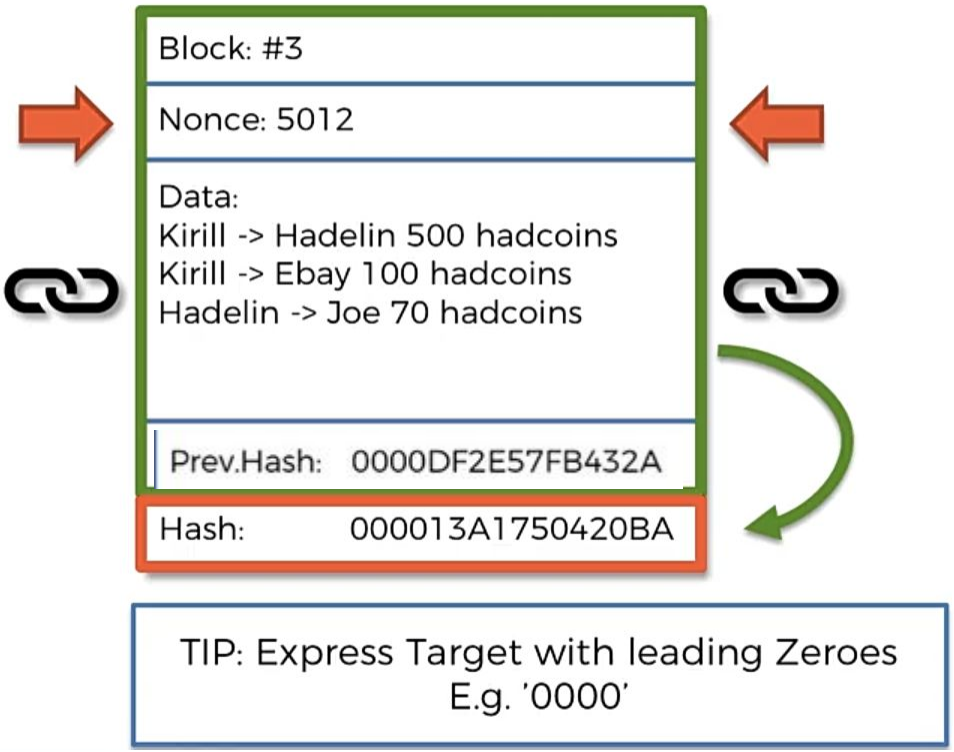
Max target = `00000000FFFF0000000000000000000000000000000`

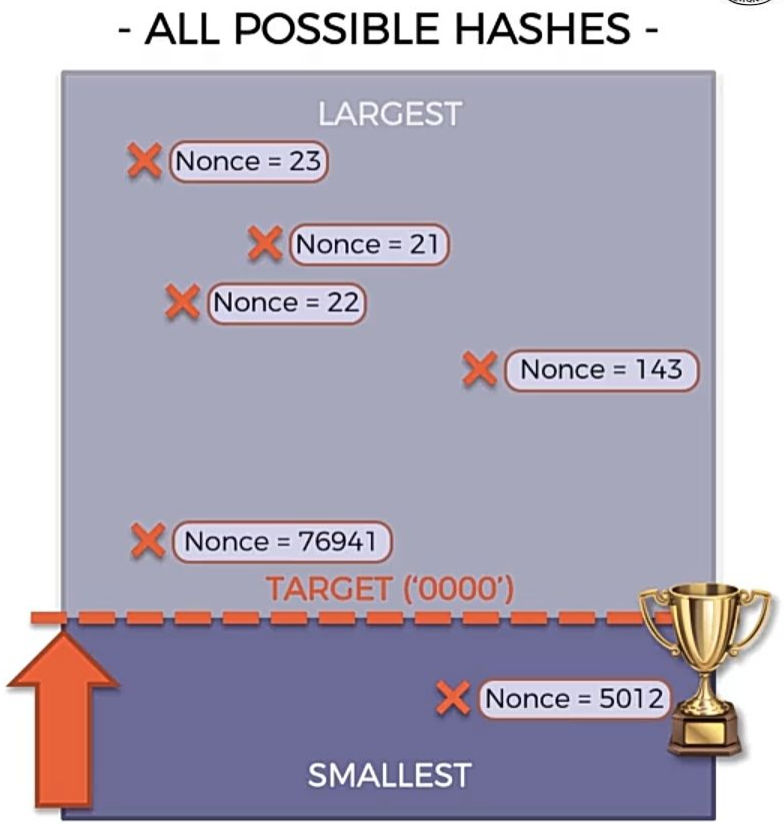
Difficulty is adjusted every 2016 blocks (2 weeks)



Blockchain Technology Fundamentals

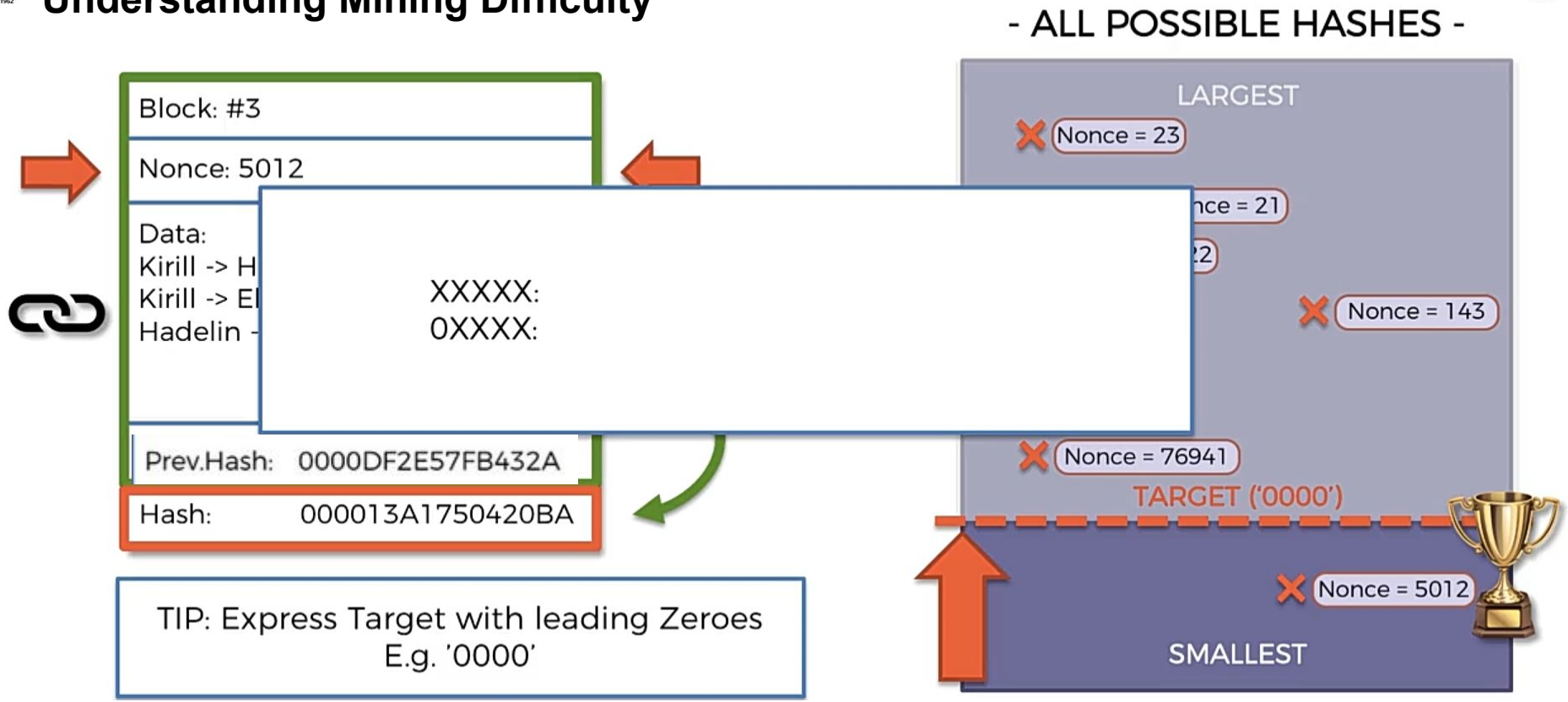
Understanding Mining Difficulty





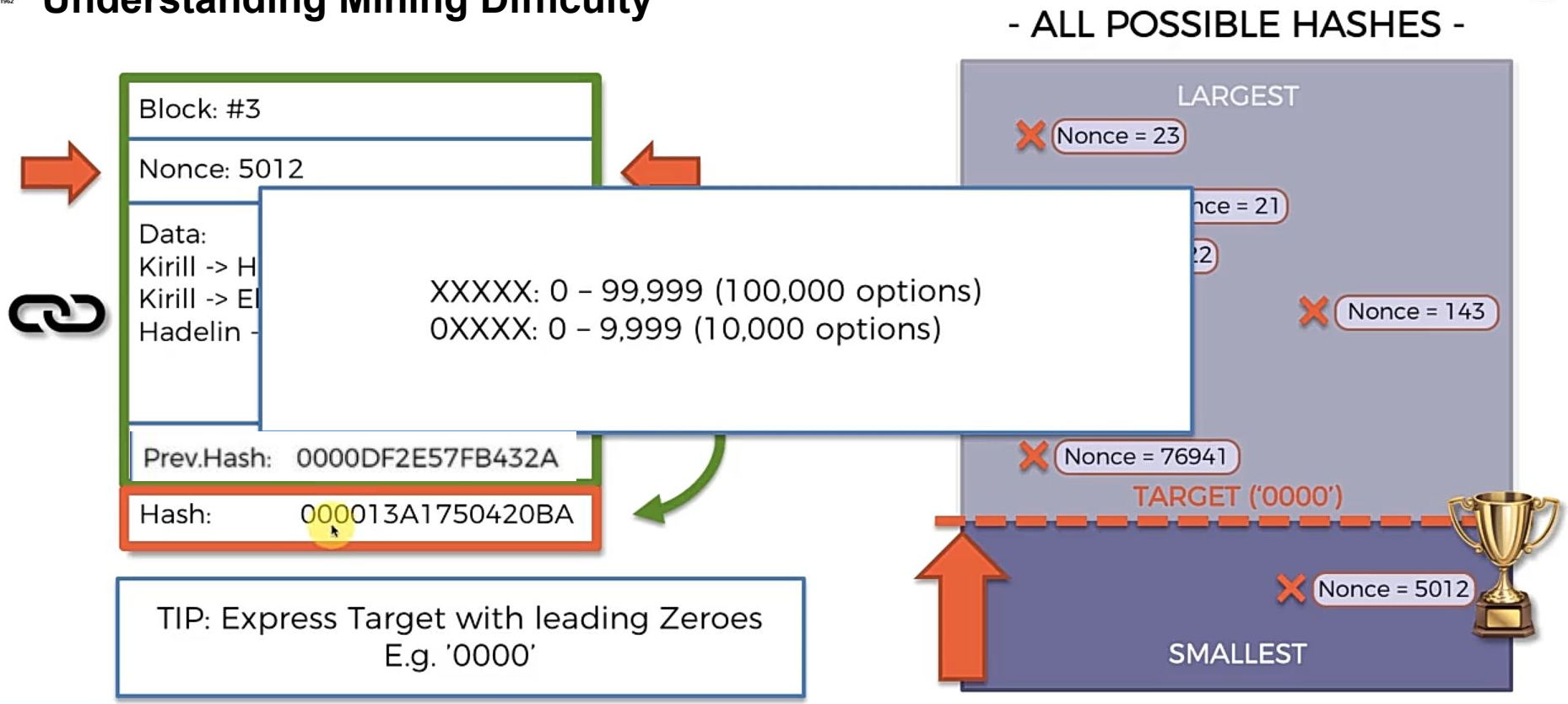
Blockchain Technology Fundamentals

Understanding Mining Difficulty



Blockchain Technology Fundamentals

Understanding Mining Difficulty



Understanding Mining Difficulty

Difficulty = current target / max target

Curr target = 0000000000000000005d97dc0000000000000000000000000000000000000000

Max target = 00000000FFFF0000000000000000000000000000000000000000000000000000

Difficulty is adjusted every 2016 blocks (2 weeks)

Blockchain Technology Fundamentals

Understanding Mining Difficulty

Current target = 00000000000000005d97dc0000000000000000000000000000000000000000

18 zeros

Let's do some estimations:

Probability:

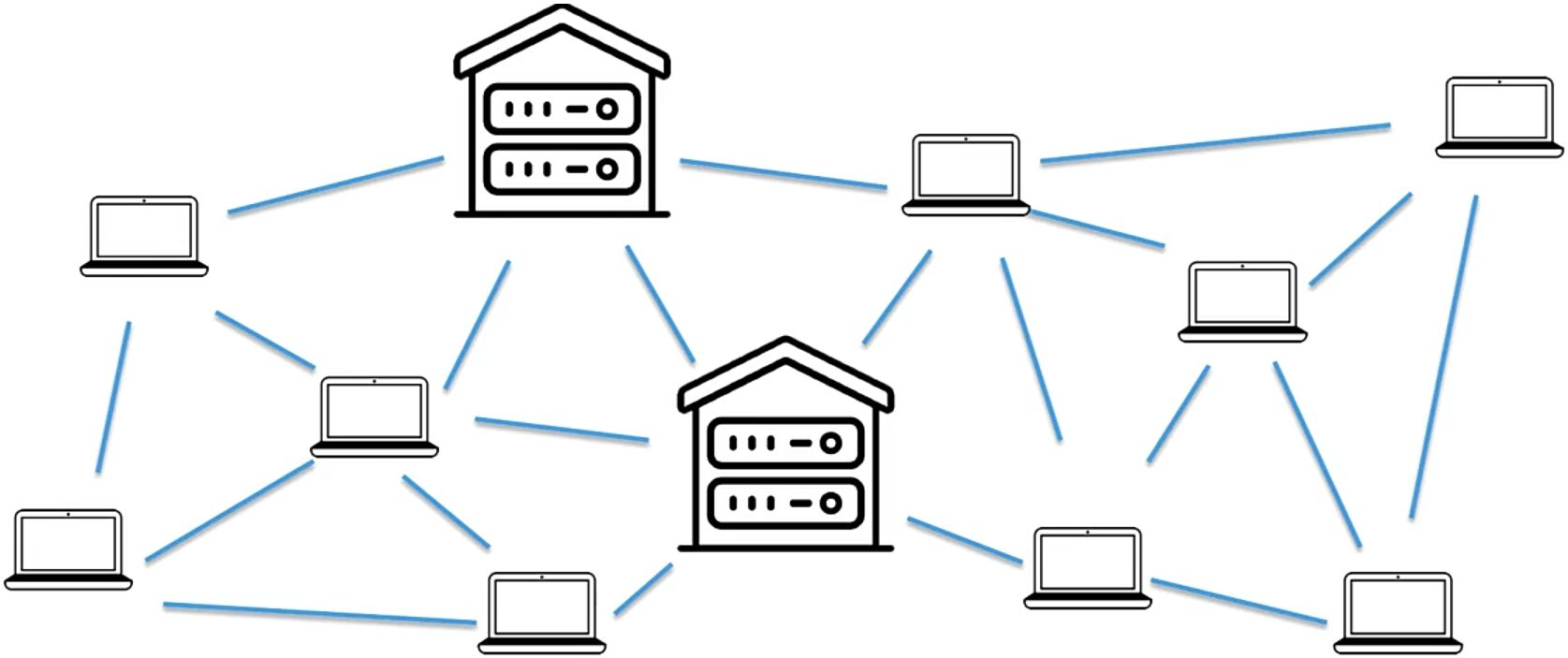
Total possible 64-digit hexadecimal numbers: $16 \times 16 \times \ldots \times 16 = 16^{64} \approx 1.1579 \times 10^{77} \approx 10^{77}$

Total valid hashes (with 18 leading zeros): $16 \times 16 \times \ldots \times 16 = 16^{64-18} \approx 2.4519 \times 10^{55} \approx 2 \times 10^{55}$

Probability that a Randomly picked hash is valid: $2 \times 10^{55} / 10^{77} = 2 \times 10^{-22} = 0.00000000000000000002\%$

Blockchain Technology Fundamentals

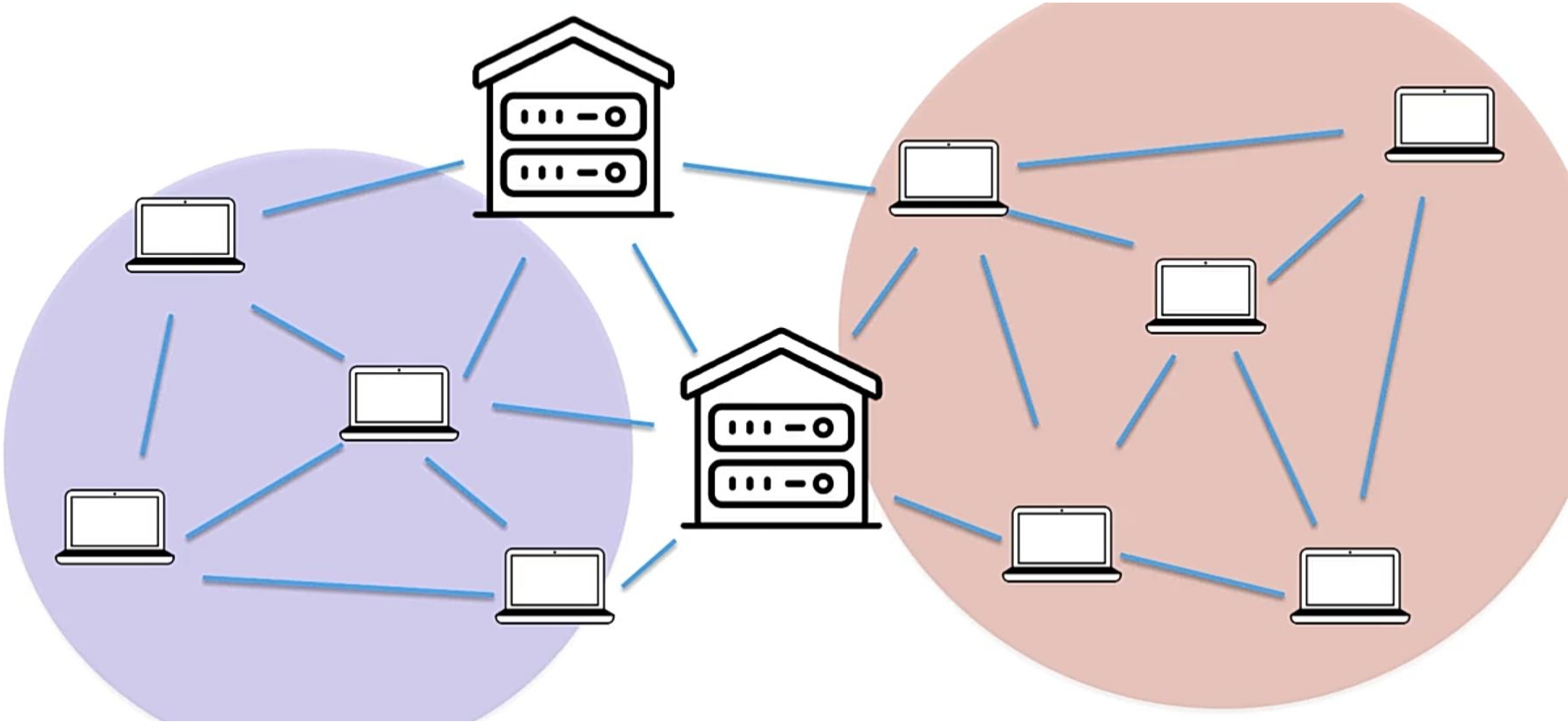
Mining Pools



Courtesy : Super Data Science

Blockchain Technology Fundamentals

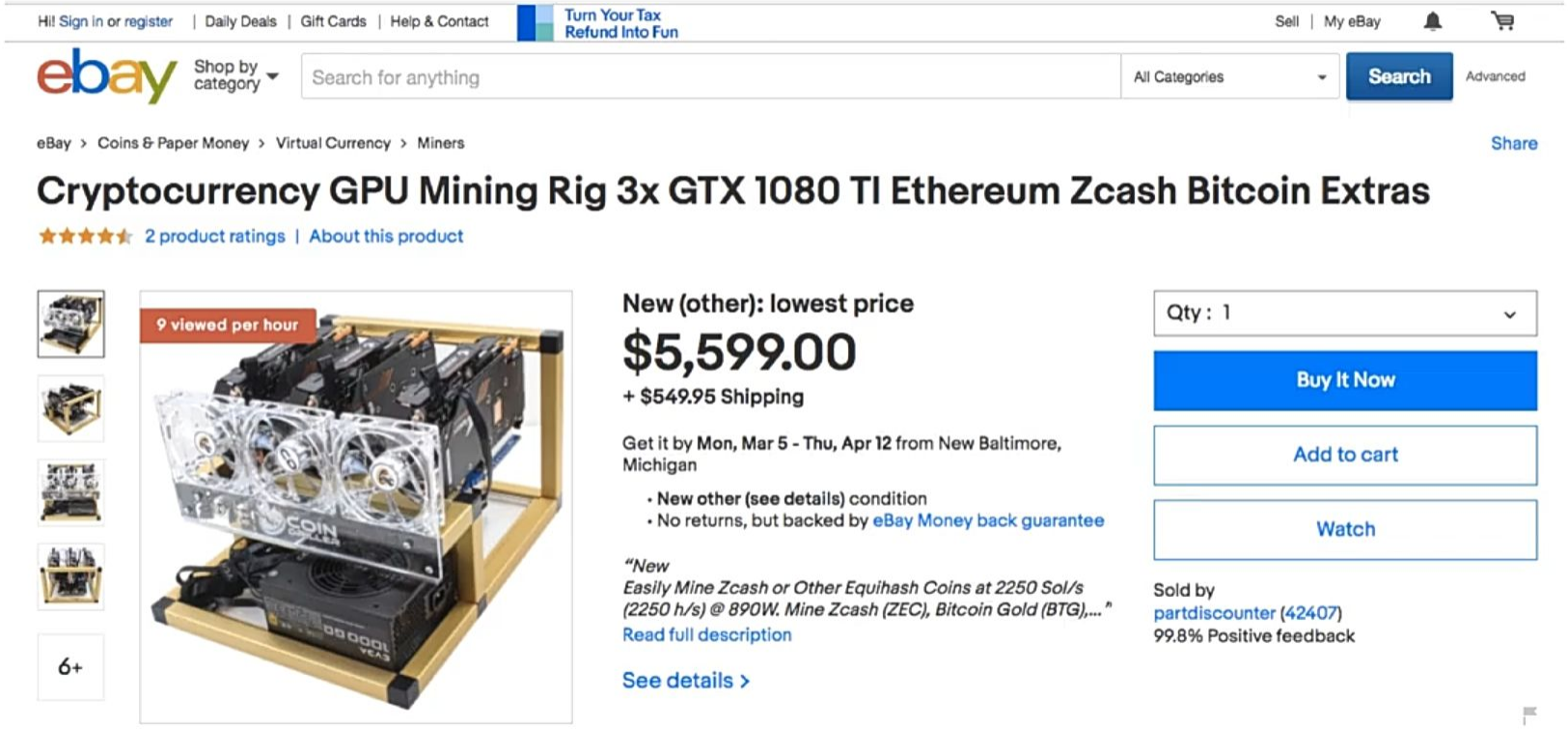
Mining Pools



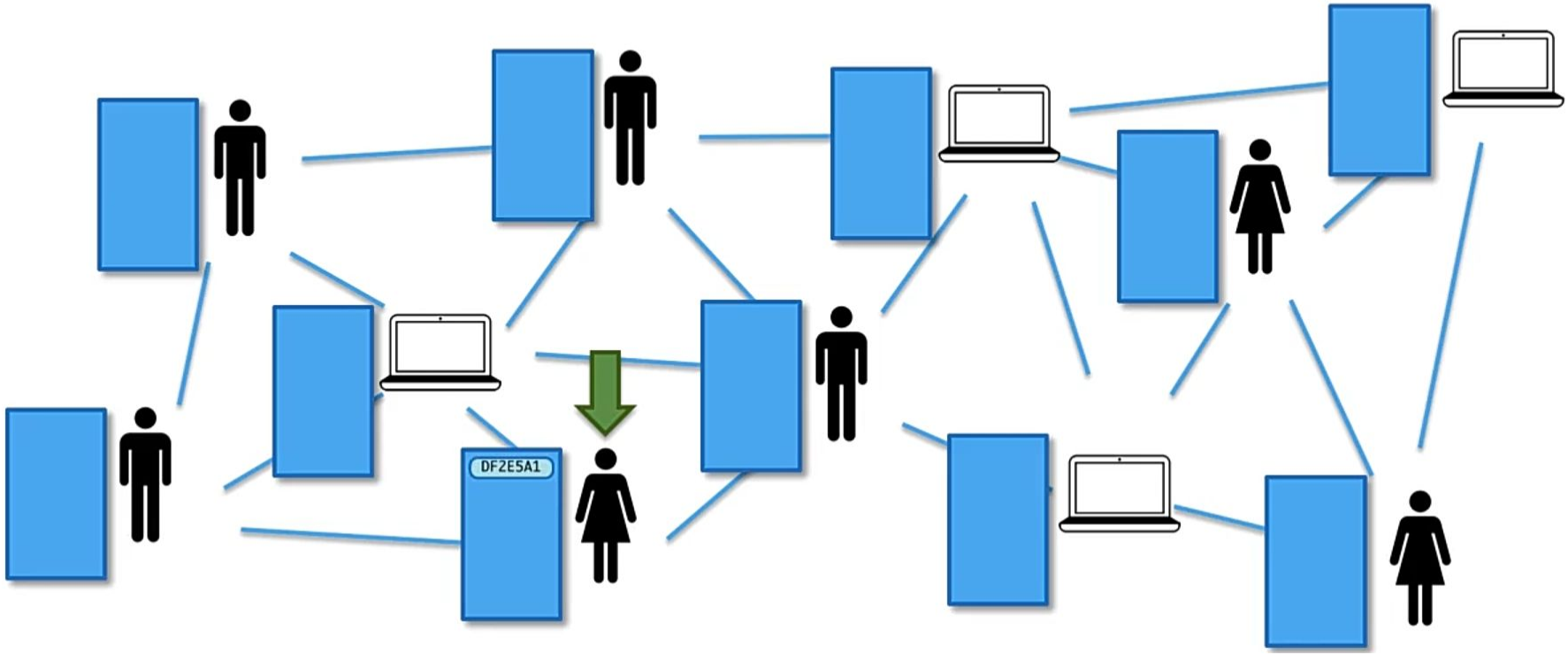
Courtesy : Super Data Science

Blockchain Technology Fundamentals

Mining Pools

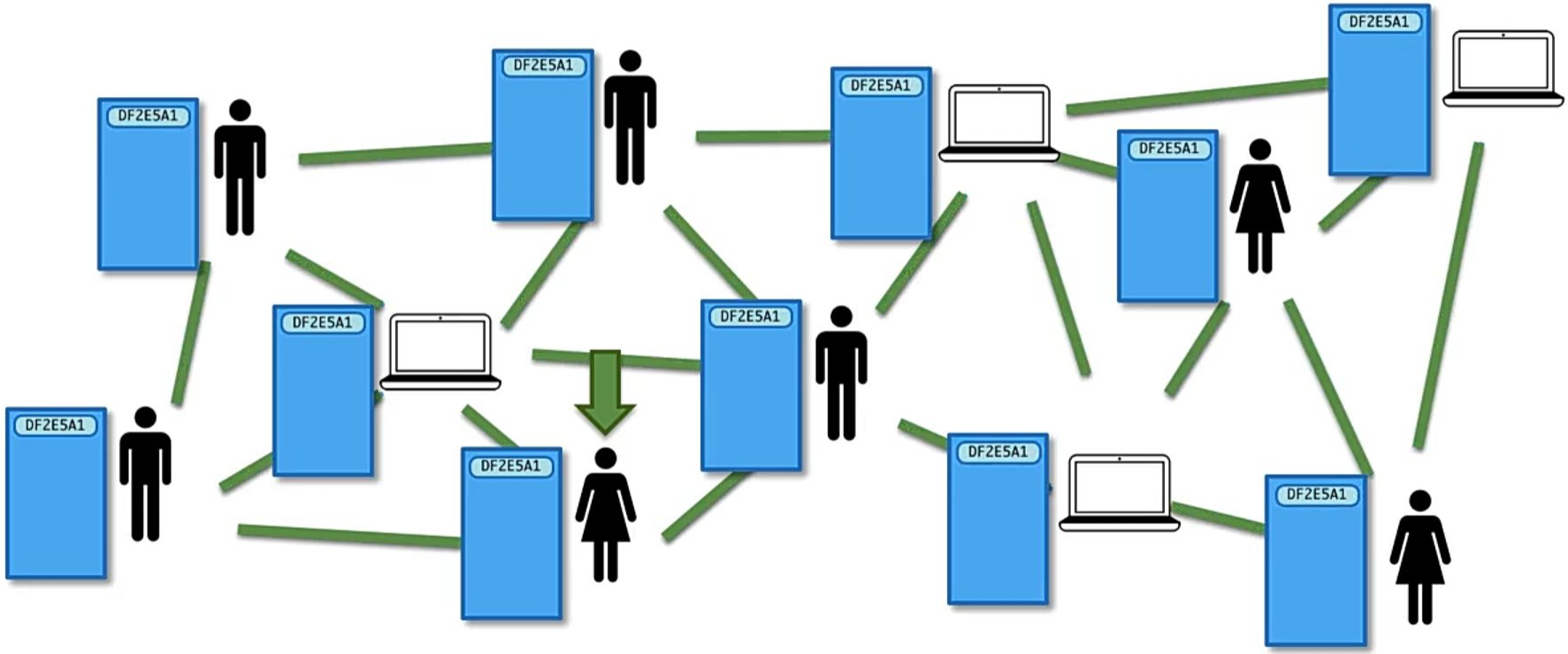


How do mempool works?



Courtesy : Super Data Science

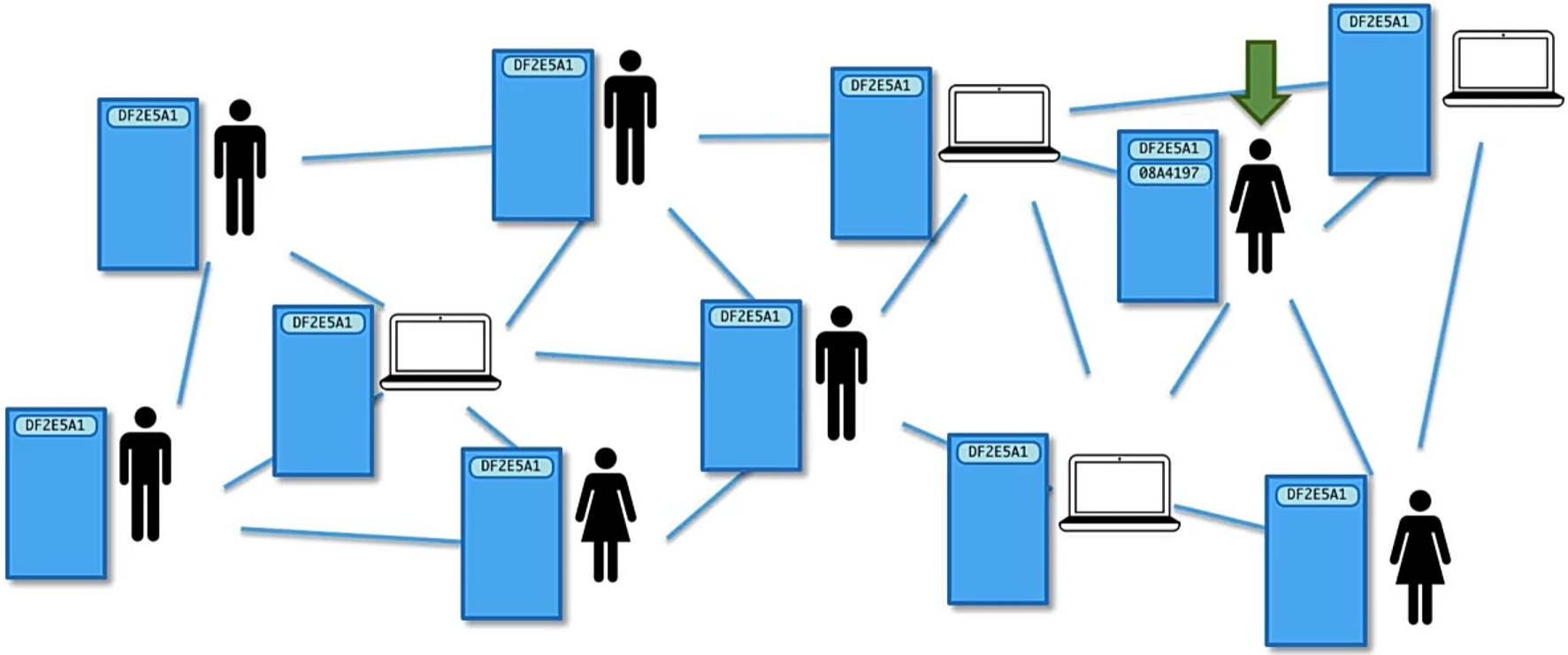
How do mempool works?



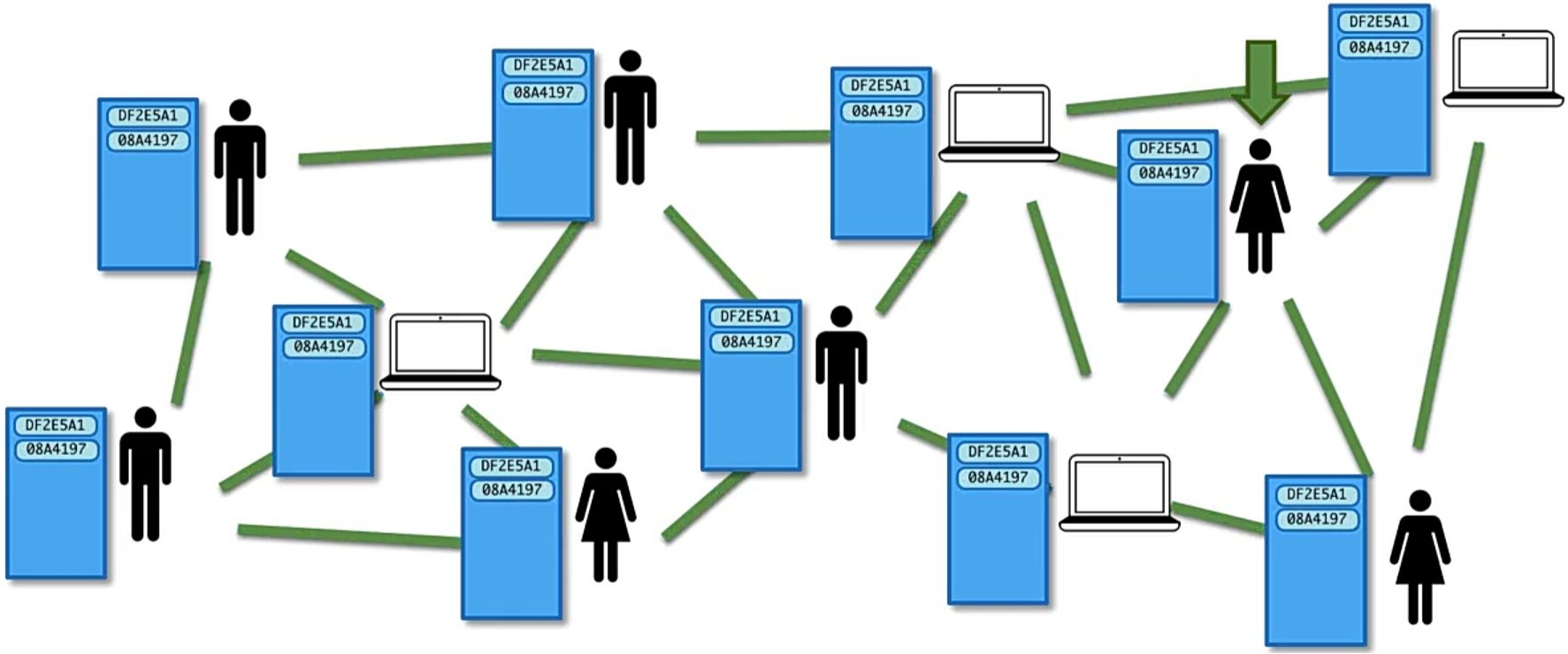
Courtesy : Super Data Science

Blockchain Technology Fundamentals

How do mempool works?



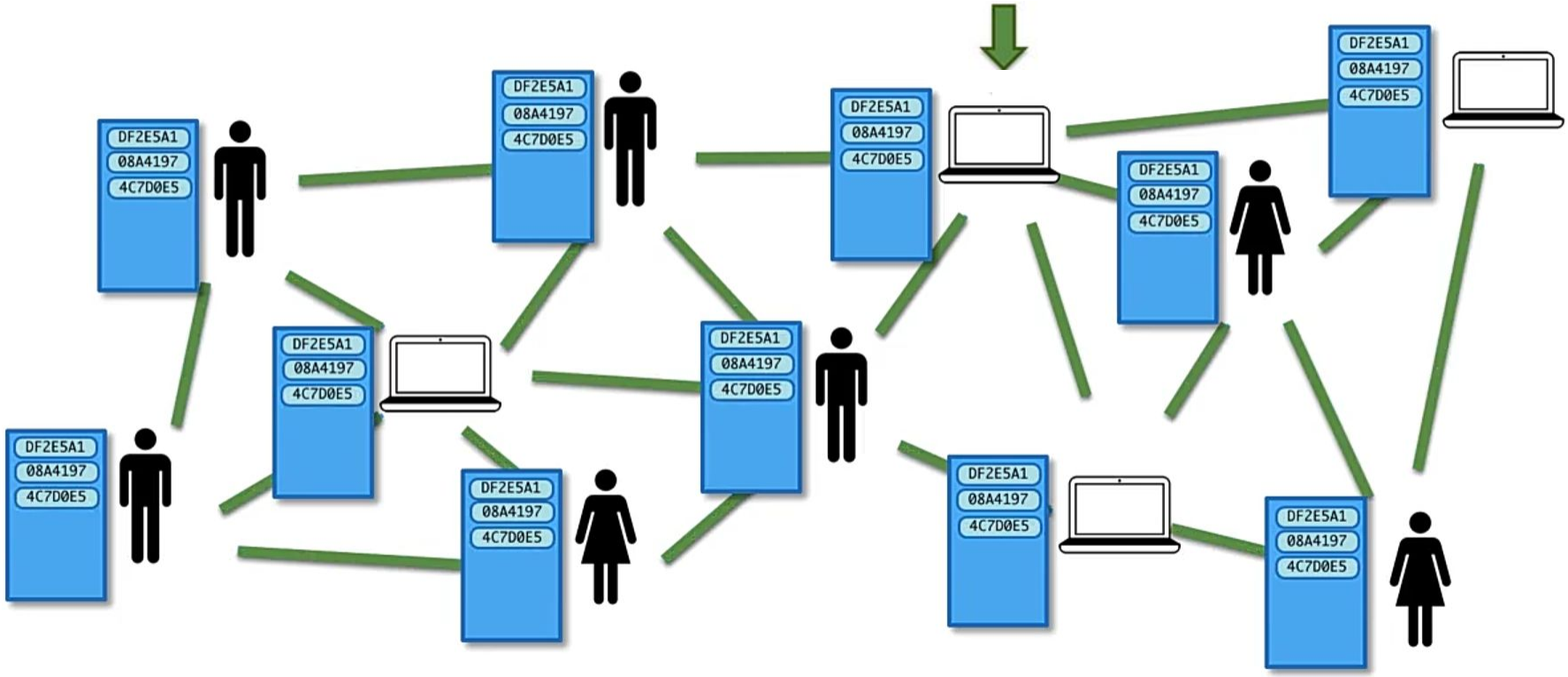
How do mempool works?



Courtesy : Super Data Science

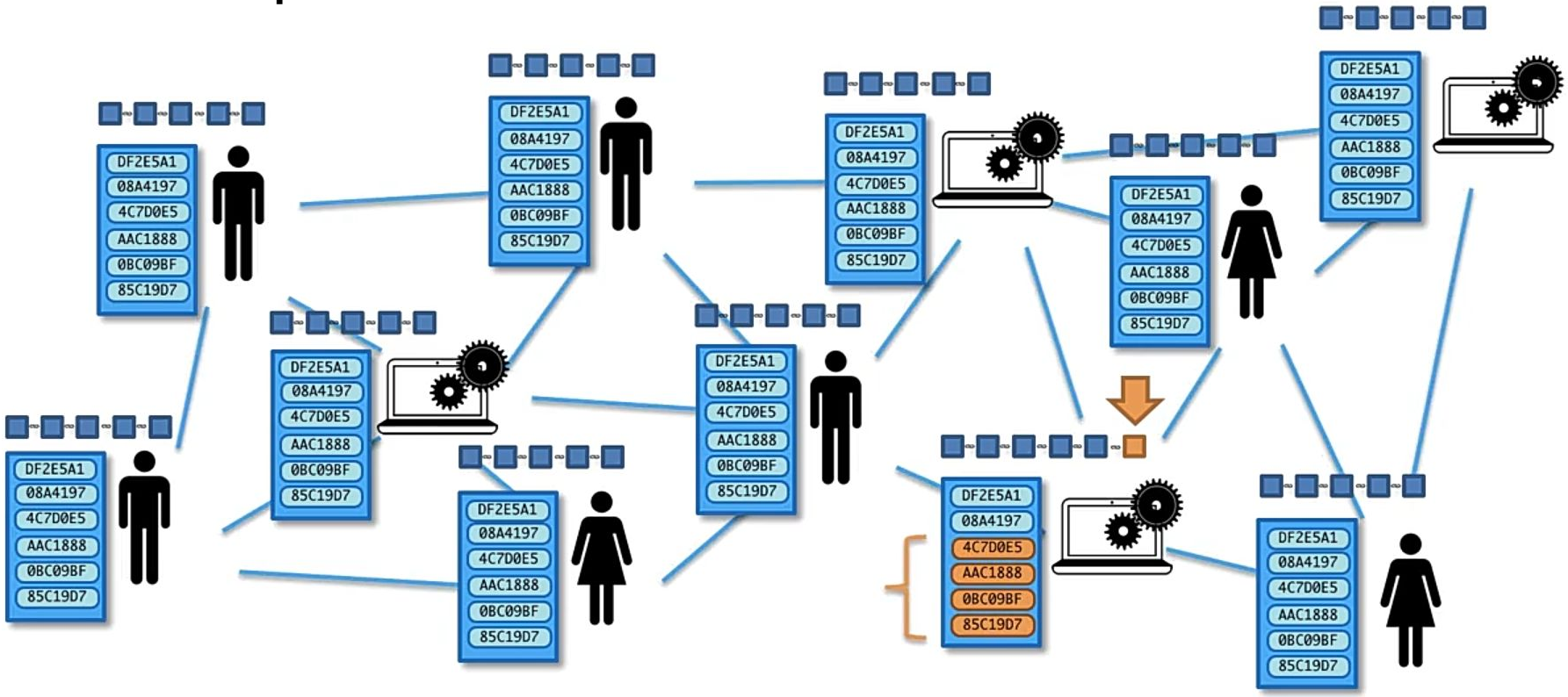
Blockchain Technology Fundamentals

How do mempool works?



Courtesy : Super Data Science

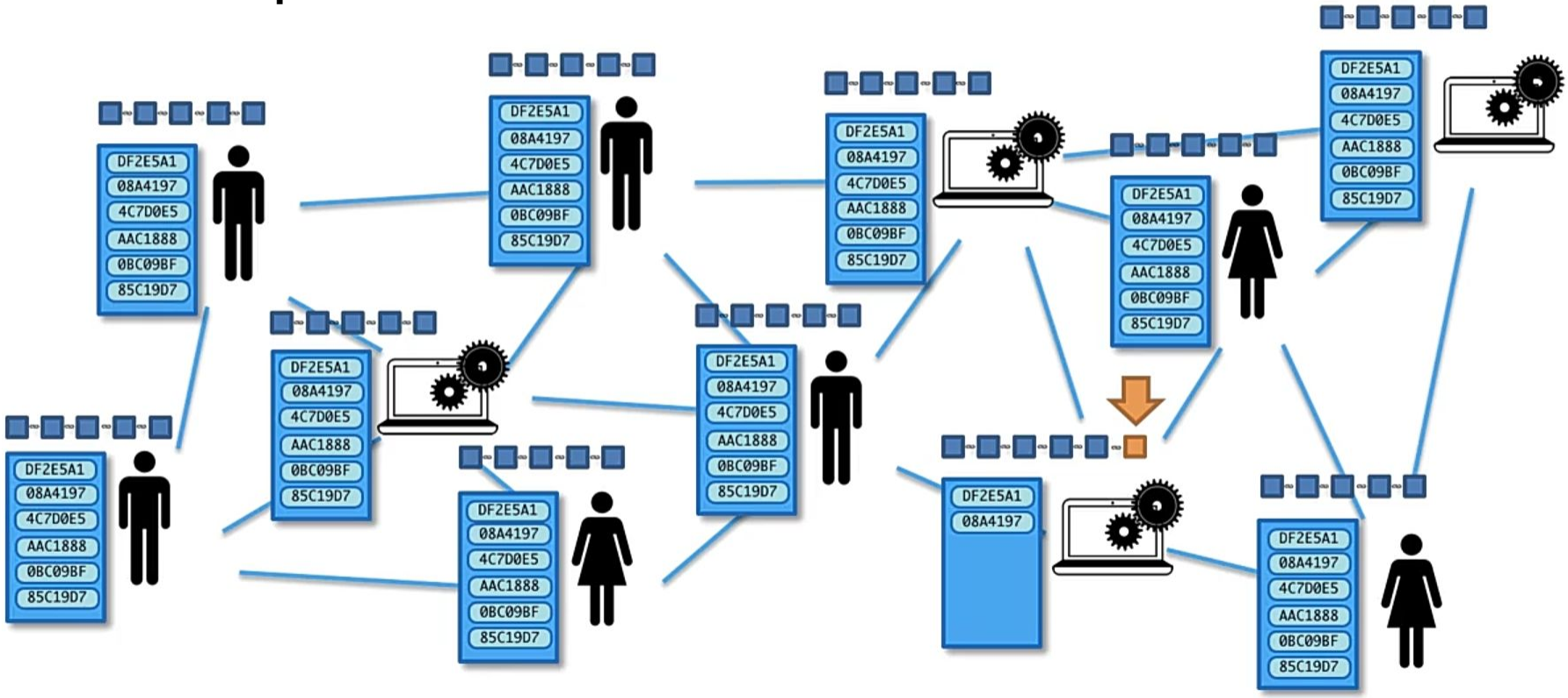
How do mempool works?



Courtesy : Super Data Science

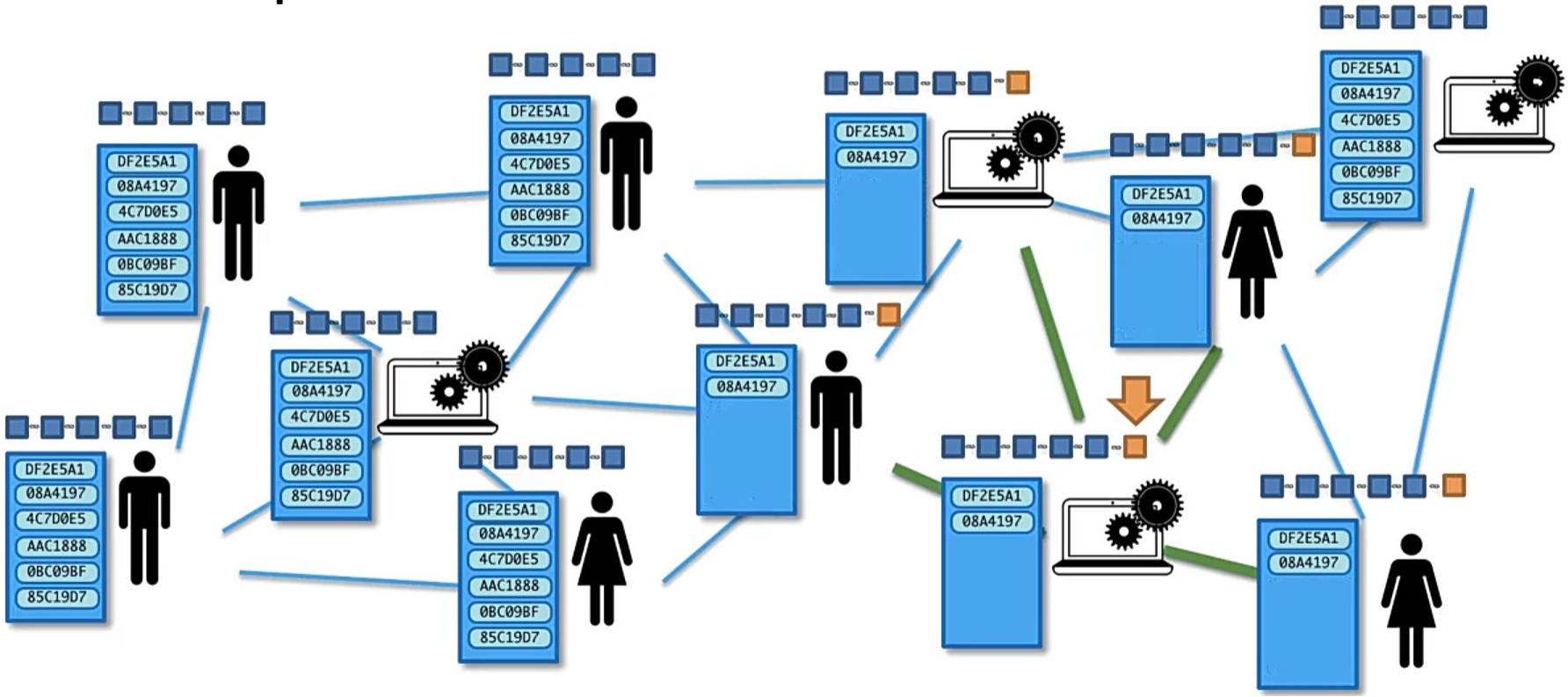
Blockchain Technology Fundamentals

How do mempool works?



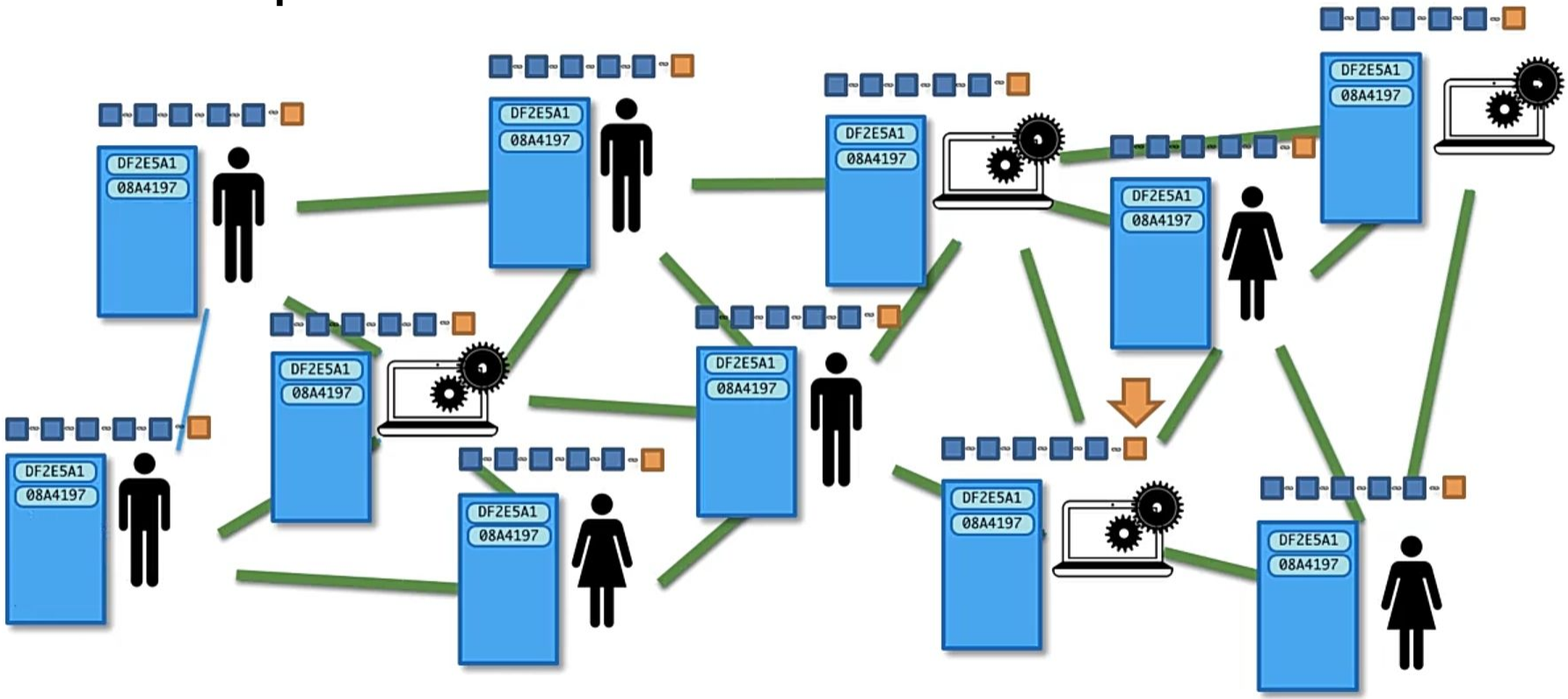
Blockchain Technology Fundamentals

How do mempool works?



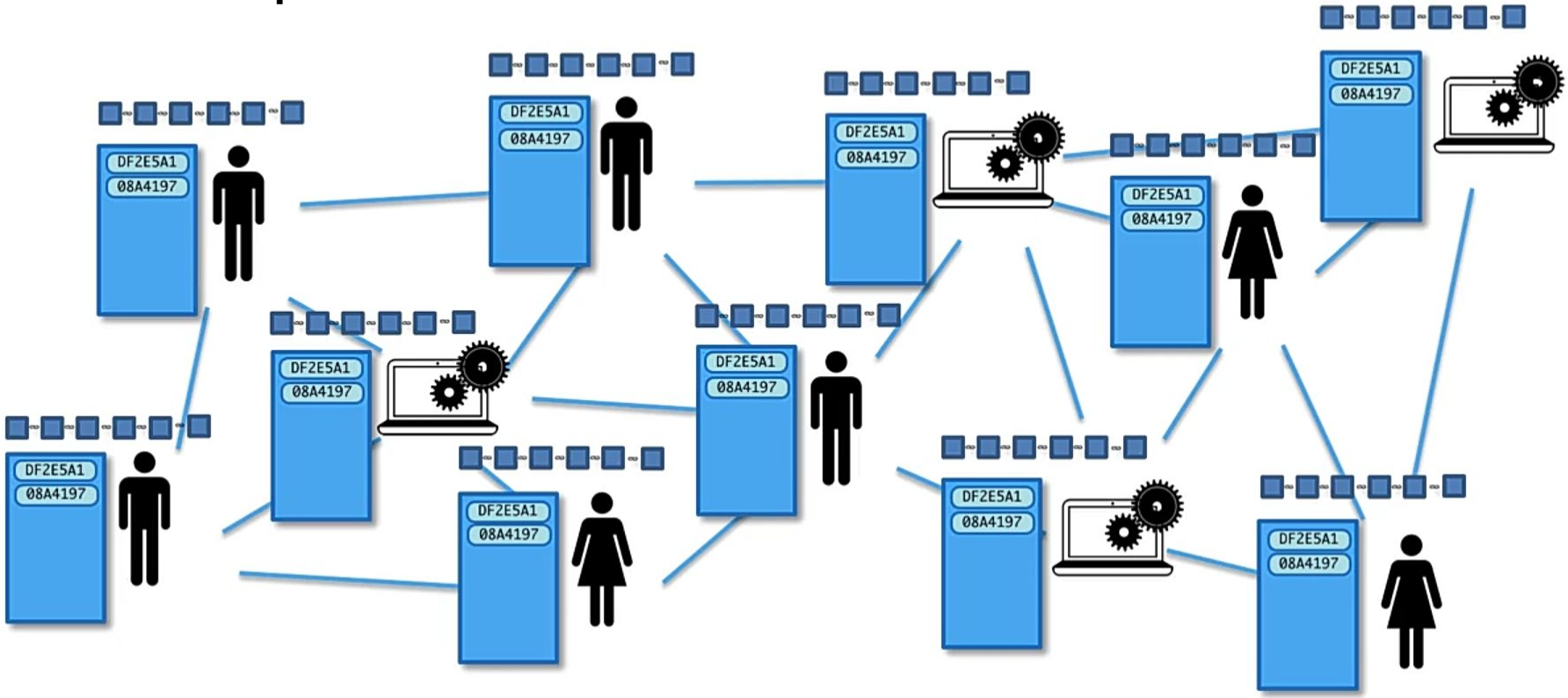
Courtesy : Super Data Science

How do mempool works?



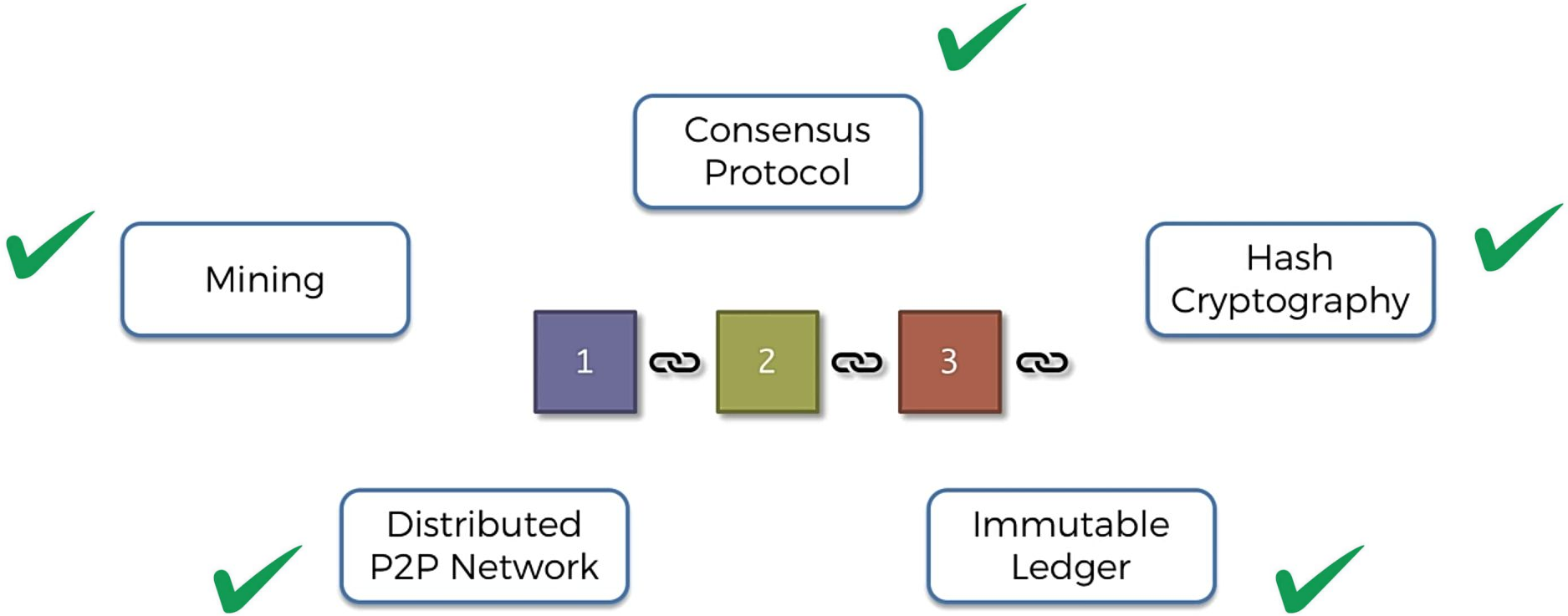
Courtesy : Super Data Science

How do mempool works?



Courtesy : Super Data Science

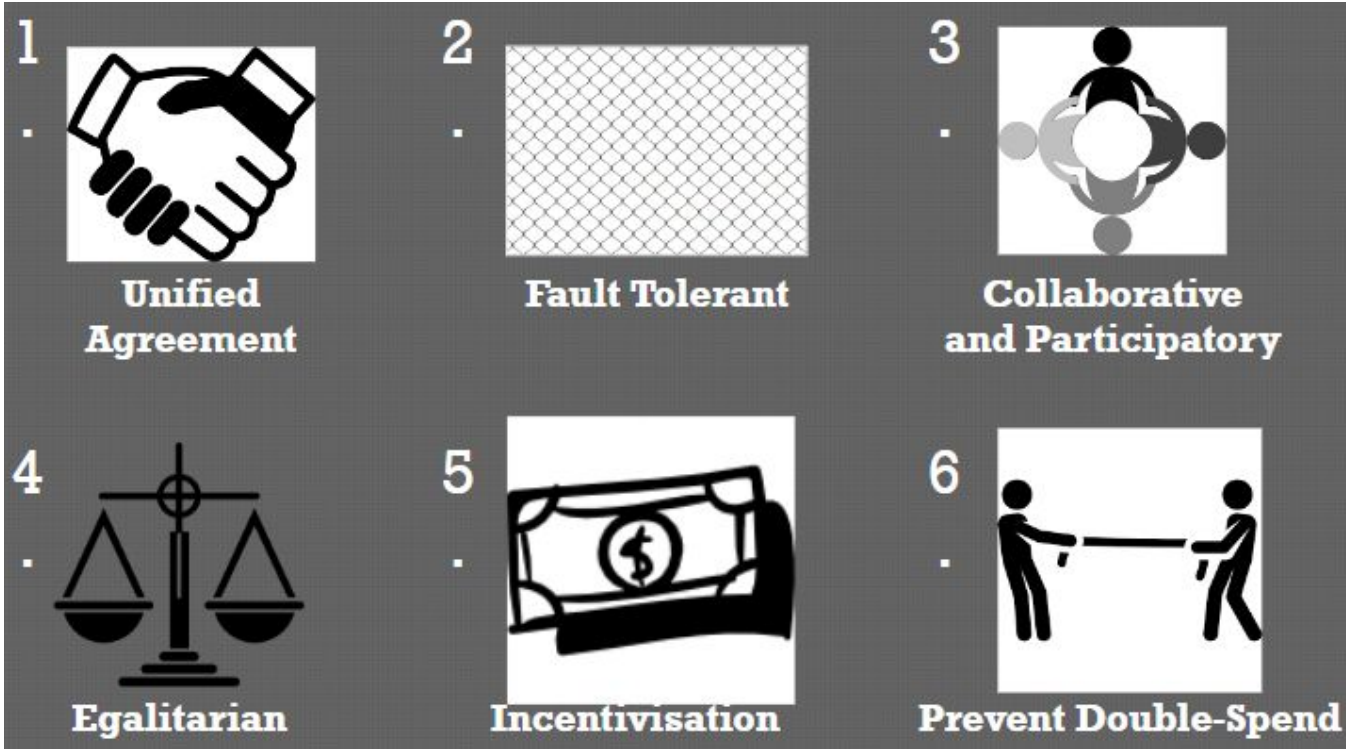
Blockchain Technology Fundamentals



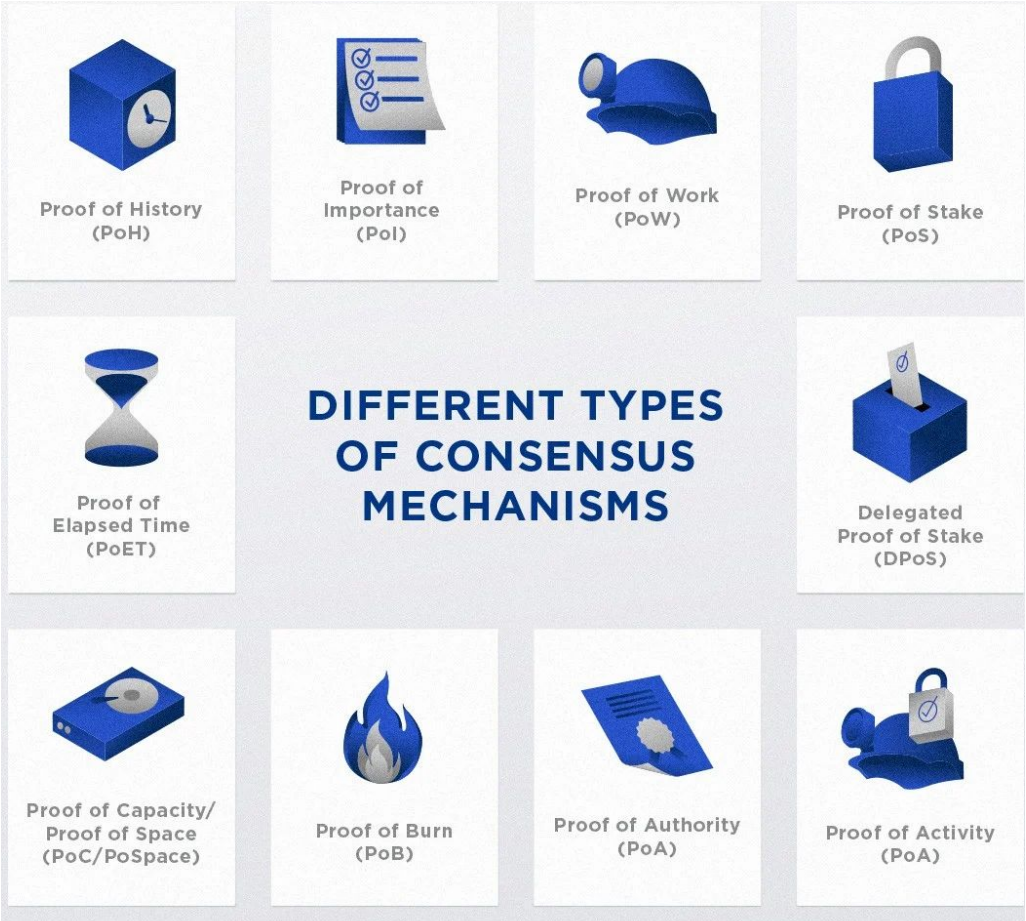
What is Consensus?

- 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**

Objectives of Consensus Protocol



Consensus Mechanisms



Courtesy : Crypto.com

Types of Consensus Mechanisms - Proof of Work (PoW)

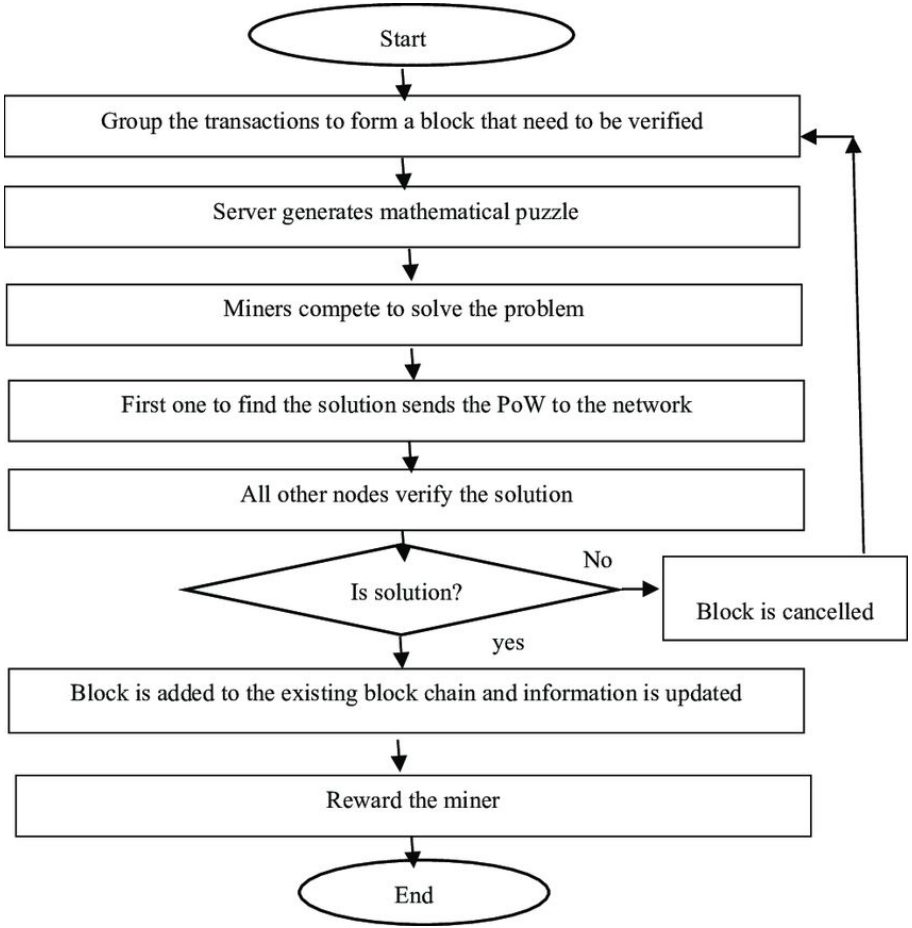
- Used by Bitcoin and many other public blockchains,
- very first consensus mechanism created.
- most reliable and secure of all the consensus mechanisms
- was first coined in the early 1990s,
- it was Bitcoin founder Satoshi Nakamoto who first applied the technology in the context of digital currencies.

Algorithm

- ‘miners’ essentially compete against one another to solve extremely complex computational puzzles using high-powered computers.
- The first to come up with the 64-digit hexadecimal number (‘hash’) earns the right to form the new block and confirm the transactions.
- The successful miner is also rewarded with a predetermined amount of crypto, known as a ‘block reward’.

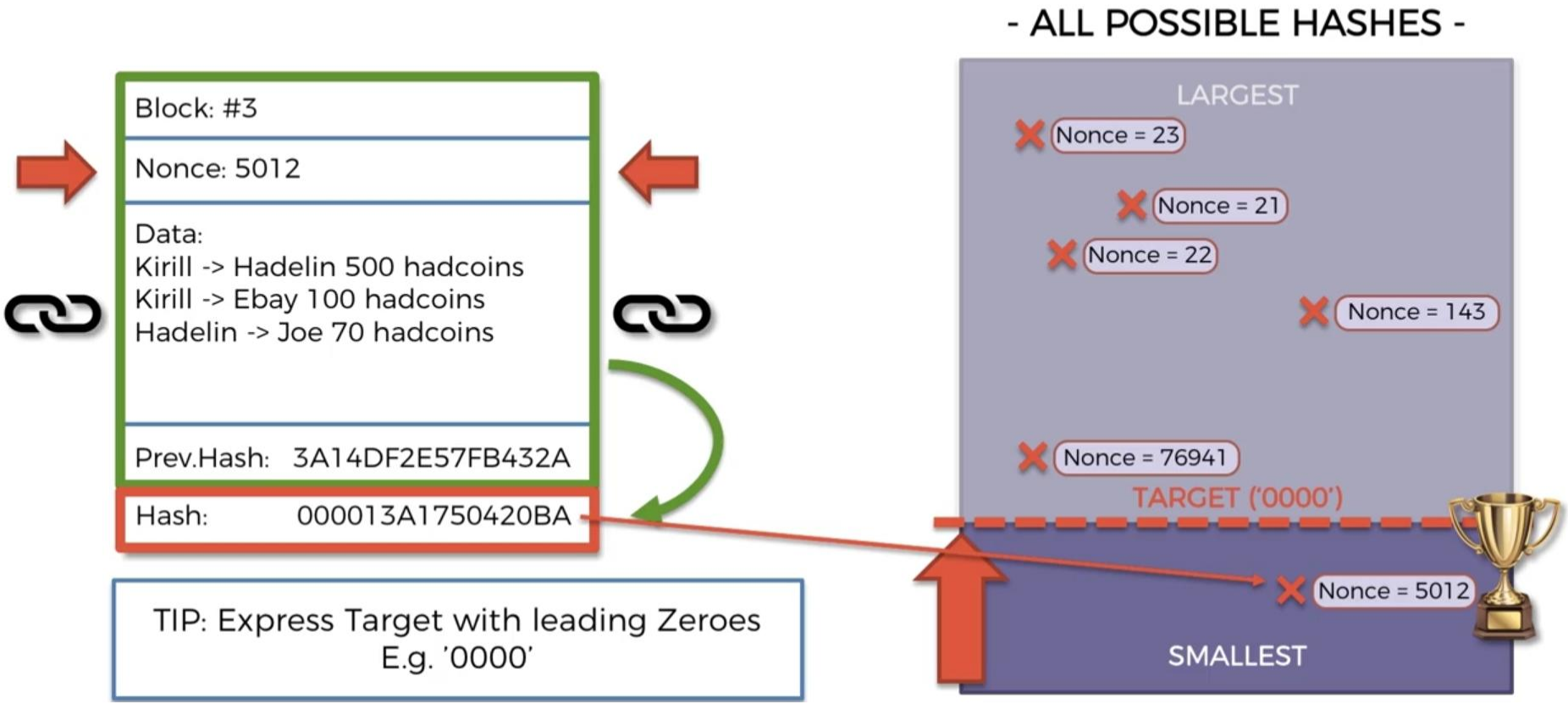
Courtesy : Crypto.com

Types of Consensus Mechanisms - Proof of Work (PoW)



Courtesy : Research Gate

Consensus Protocol - Cryptographic Challenge



Types of Consensus Mechanisms - Proof of Work (PoW)

Advantages of Proof-of-Work

- A **hard-to-find solution**. Still, easy verification.
- As an initial consensus mechanism, PoW **does not need initial stakes of coins before mining.** One can start with 0 coins and it will only be positive.
- Ease of implementation compared to other blockchain consensus mechanisms.
- It is **fault tolerant.** It means that the failure of one component will not shut down the entire blockchain network.
- **Give miners the opportunity to earn by adding a block.**
- PoW is the **oldest, most trusted, and most popular consensus protocol.**

Types of Consensus Mechanisms - Proof of Work (PoW)

Limitations of Proof-of-Work

- A **lot of energy is wasted** because only one miner can finally add their block.
- It requires a **lot of computing power** and, therefore, massive consumption of resources and energy.
- **51% risk of network attack**. A controlling person can get 51% to control the network.
- Spread environmental hazards with attachment machines.
- PoW is a **time and energy wipe-out process.**
- It required a lot of hardware costs.
- **Risk of Denial of Service Attacks by Intruders**.

Types of Consensus Mechanisms - Proof of Stake (PoS)

- Nodes in the network, **stake a certain amount of cryptocurrency to become candidates for validating a new block and receiving a fee**.
- The algorithm then selects a node from the pool of candidates to verify the new block.
- This selection **algorithm combines the amount of deposit** (amount of cryptocurrency) **with other factors (such as selection based on coin age, and randomization process)** to make the selection fair for everyone in the network.

Coin-age-based selection:

- The algorithm keeps **track of how long each candidate validator node remains a validator.**
- The older the node, the higher the chance of becoming a new validator.

Random Block selection:

- The validator is **selected by combining "lowest hash value" and "highest stake."**
- The **node that has the best-weighted combination of them becomes the new validator.**

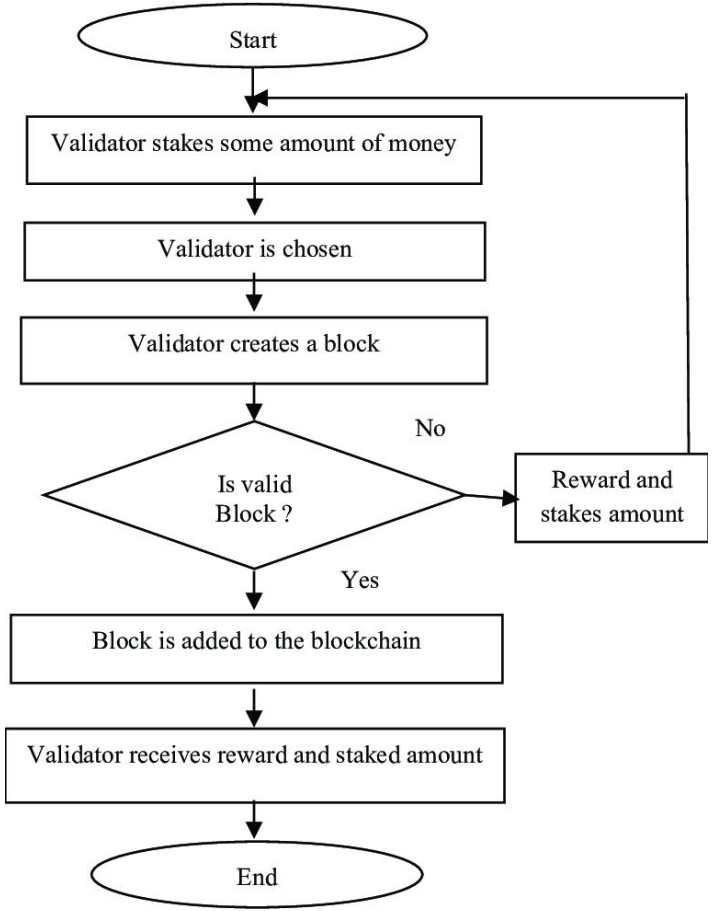
Types of Consensus Mechanisms - Proof of Stake (PoS)

Workflow of a PoS-based mechanism

1. Nodes perform transactions. The PoS algorithm puts all these transactions into a pool.
2. All nodes fighting to become validators for the next block **raise the stake**. This stake is combined with other factors such as “coin age” or “random block selection” to select a validator.
3. The validator verifies all transactions and publishes the block. His bet remains locked, and the forgery reward has also not yet been awarded. This is so that nodes in the network can “OK” a new block.
4. The **validator will get the stake back and the reward if the block is OK**. If the algorithm uses a mechanism based on coin age to select validators, the validator for the current block has its coinage reset to 0. This puts it in low priority for the next validator election.
5. **If other nodes in the network do not validate the block, the validator loses his stake and is marked as “bad” by the algorithm**. The process starts again from step 1 to create a new block.

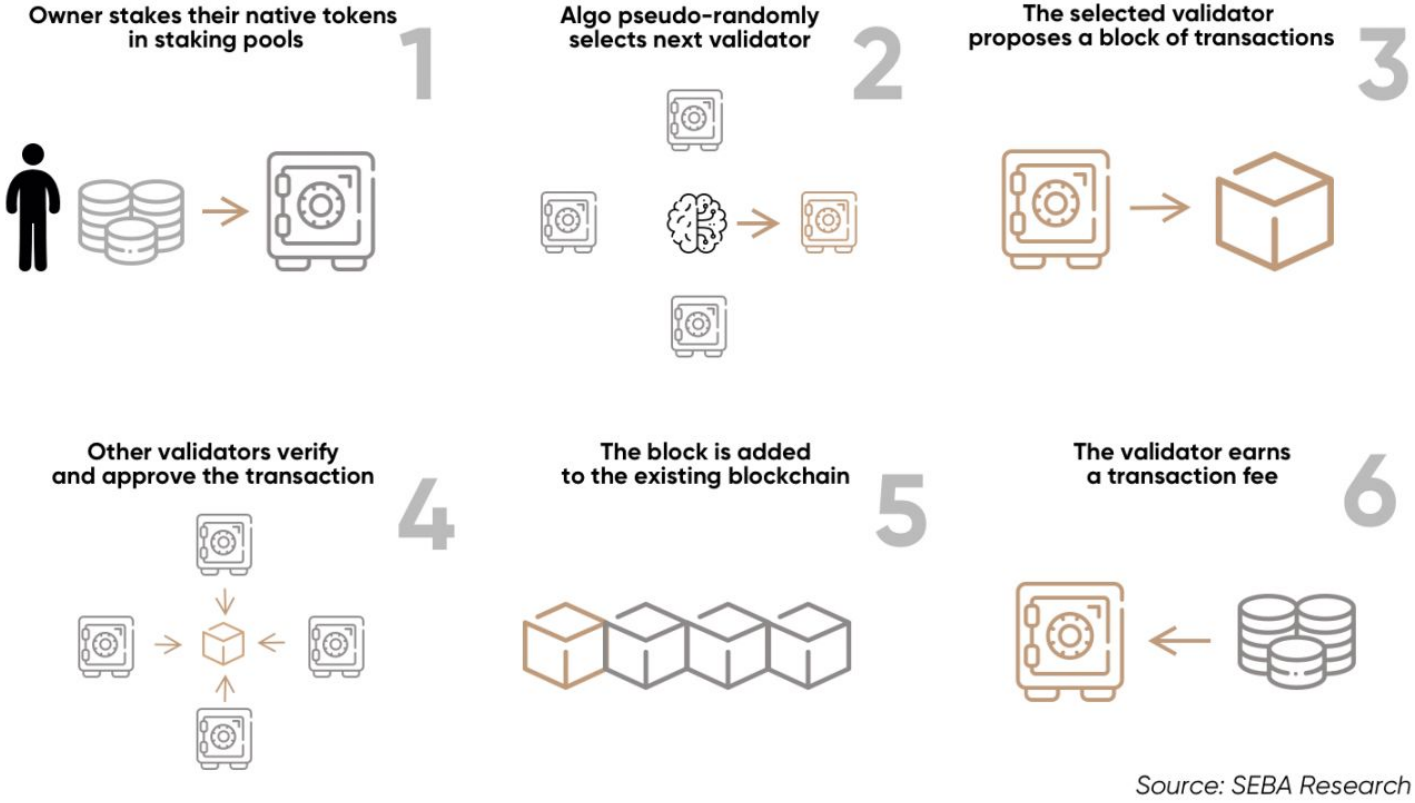
Courtesy : AnalyticsVidya

Types of Consensus Mechanisms - Proof of Stake (PoS)



Courtesy : ResearchGate

Types of Consensus Mechanisms - Proof of Stake (PoS)



Courtesy : AnalyticsVidya

Types of Consensus Mechanisms - Proof of Stake (PoS)

Advantages of PoS

- **Energy saving:**
  - Since all nodes are not competing to add a new block to the blockchain, energy is saved.
  - No problem needs to be solved (as in the case of a Proof-of-Work system), thus saving energy.
- **Decentralization:**
  - **PoW** :
    - to achieve distributed consensus, there is the added incentive of exponential rewards for joining a mining pool, leading to a more centralized nature of the blockchain.
  - **PoS** (such as Peercoin),
    - the r**ewards are proportional (linear) to the deposit amount.**
    - no additional benefits for joining a mining pool, thereby supporting decentralization.
- **Safety:**
  - A **person trying to attack the net must own 51% of the stakes (quite expensive).**
  - This **leads to a secure network.**

Types of Consensus Mechanisms - Proof of Stake (PoS)

Weakness of PoS mechanism

- **Big Bet Validators:**
  - If a group of validator candidates come together and own a significant share of the total cryptocurrency, they will have a better chance of becoming validators.
  - The increased odds lead to bigger withdrawals, leading to more rewards being earned, which leads to owning a huge share of the currency. This can be the reason for the n**etwork to come to be centralized over time.**
- **New technology:**
  - PoS is still relatively new.
  - Research is ongoing to find the flaws, fix them, and make them viable for a live network with real currency transactions.
- **The "Nothing at Stake" Problem:**
  - This problem describes little to no disadvantage for nodes if they support multiple blockchains, in the case of blockchain forking.
  - In the worst case, **each fork will lead to multiple blockchains, and validators will work, and the nodes in the network will never reach a consensus.**

Types of Consensus Mechanisms - Proof of Stake (PoS)

Goals of Proof-of-Stake

- Proof-of-stake is designed to reduce network congestion and environmental sustainability concerns associated with the proof-of-work (PoW) protocol.
- Bitcoin miners earn bitcoins by validating transactions and blocks. However, they pay their operating costs such as electricity and rent in fiat currency. What happens then is that miners exchange energy for cryptocurrency, which makes PoW mining consume as much energy as some small countries.
- The PoS mechanism seeks to solve these problems by **effectively replacing computing power with staking, where the ability of an individual to mine randomly is the network**. This means there should be a drastic reduction in power consumption, as miners can no longer rely on massive farms of single-purpose hardware to gain an edge.

Types of Consensus Mechanisms - Proof of Stake (PoS)

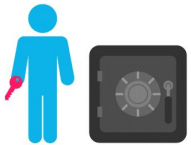
Proof-of-Stake security

- Long touted as a threat to crypto fans, the 51% attack is concerning when using PoS, but there are doubts that it will happen. In PoS, **a group or individual would have to own 51% of the staked cryptocurrency.**
- **Controlling 51% of the cryptocurrency staked is very expensive.** Under Ethereum's PoS, if a 51% attack were to occur, honest validators on the network could vote to ignore the altered blockchain and burn the offender's staked ETH. This incentivizes validators to act in good faith for the benefit of the cryptocurrency and the network.

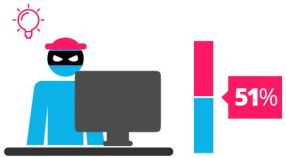
Consensus Mechanisms

Proof of Work vs Proof of Stake

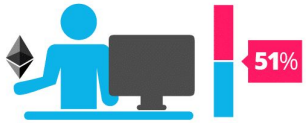
proof of work is a requirement to define an expensive computer calculation, also called mining



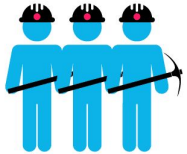
Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.



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.

Courtesy : Devopedia

Types of Consensus Mechanisms - Proof of Stake (PoET)

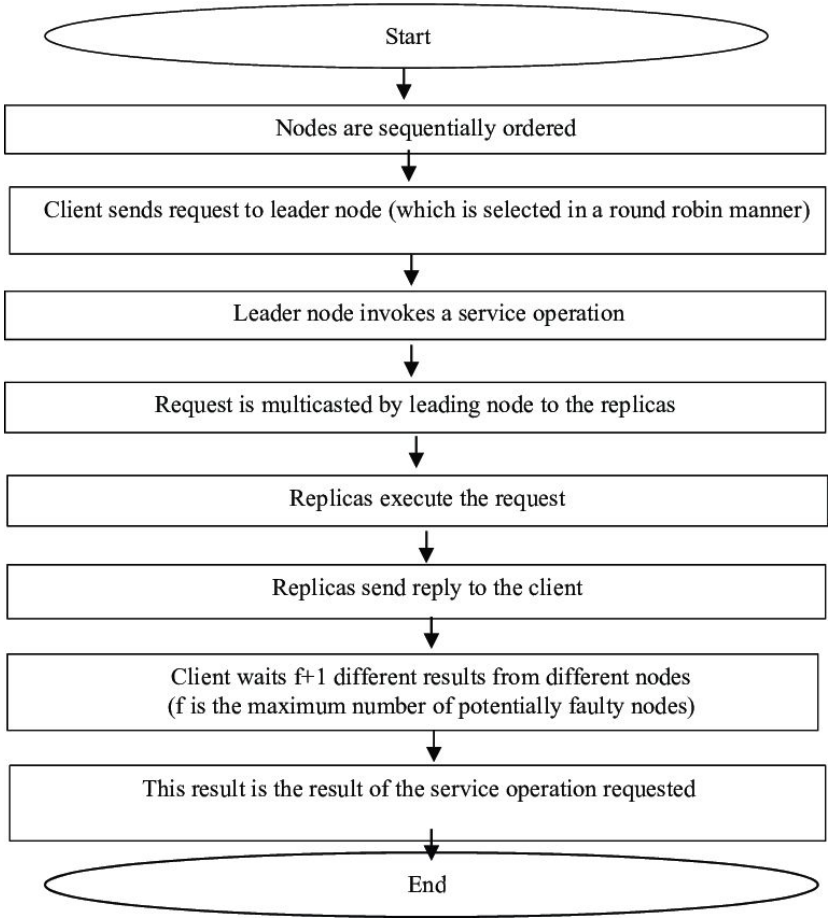
- used on permissioned blockchain networks,
- leverages trusted computing to enforce random waiting times for block construction.
- It was **developed by Intel** in early 2016,
- based on a special set of CPU instructions called **Intel Software Guard Extensions (SGXs).**
- **time-lottery-based consensus algorithm**

PoET Algorithm

1. randomly assigning different wait times to every node in the network.
2. During the waiting period, each of these nodes goes to 'sleep' for that specified duration.
3. The first to wake up (that is, the one with the shortest waiting time) is **awarded the mining rights.**

- This **randomisation guarantees that every participant is equally as likely to be the winner, ensuring fairness within the network.**
- highly efficient, less resource-intensive, and scalable.
- It has been implemented in **Hyperledger's Sawtooth.**

Types of Consensus Mechanisms - Proof of Stake (PoET)



Courtesy : Research Gate

Types of Consensus Mechanisms - Proof of Stake (PoB)

- more sustainable alternative to Bitcoin's PoW algorithm is Proof of Burn (PoB),
- miners gain the power to mine a block by 'burning' (destroying) a predetermined amount of tokens in a verifiable manner — namely, sending them to an 'eater address' where they cannot be recovered or spent.
- The **more coins a miner burns, the greater their chances of being randomly selected.**
- **burned coins are irretrievable**.
- This method of requiring **miners to sacrifice short-term wealth in order to gain the lifetime privilege** of creating new blocks helps to encourage long-term commitment from miners.
- The act of burning coins also leads to coin scarcity, limiting inflation and driving up demand.
- Eg : Slimcoin (SLM), Counterparty (XCP), and Factom (FCT).

Courtesy : Devopedia

Compare Consensus Mechanisms - PoW, PoS, PoET, PoB

Proof of work (PoW)	Proof of stake (PoS) [11]	Proof of Burn (PoB)	PoET
Used for industries working on financial level	Used for industries working on financial level	Used for industries working on financial level	Used for industries working on financial level
Using public key encryption (i.e. Bitcoin)	Using RSA algorithm for encryption	RSA algorithm for encryption	RSA algorithm for encryption
Miners having higher work done after investing higher power will have higher probability to mine the new block	It is some election type selection of miners for next block to be mined	PoB acquires some cryptocurrencies (wealth) to mine new block using virtual resource	Person spends some time and power to mine new block who finishes first the prior task will be the next miner
Power inefficient	Power efficient	Power efficient	Power efficient
Open environment	Open environment	Open environment	Open environment
Bitcoin script is used	Mostly Golong is used	Mostly Golong is used	

Courtesy : Research Gate

Byzantine General Problem

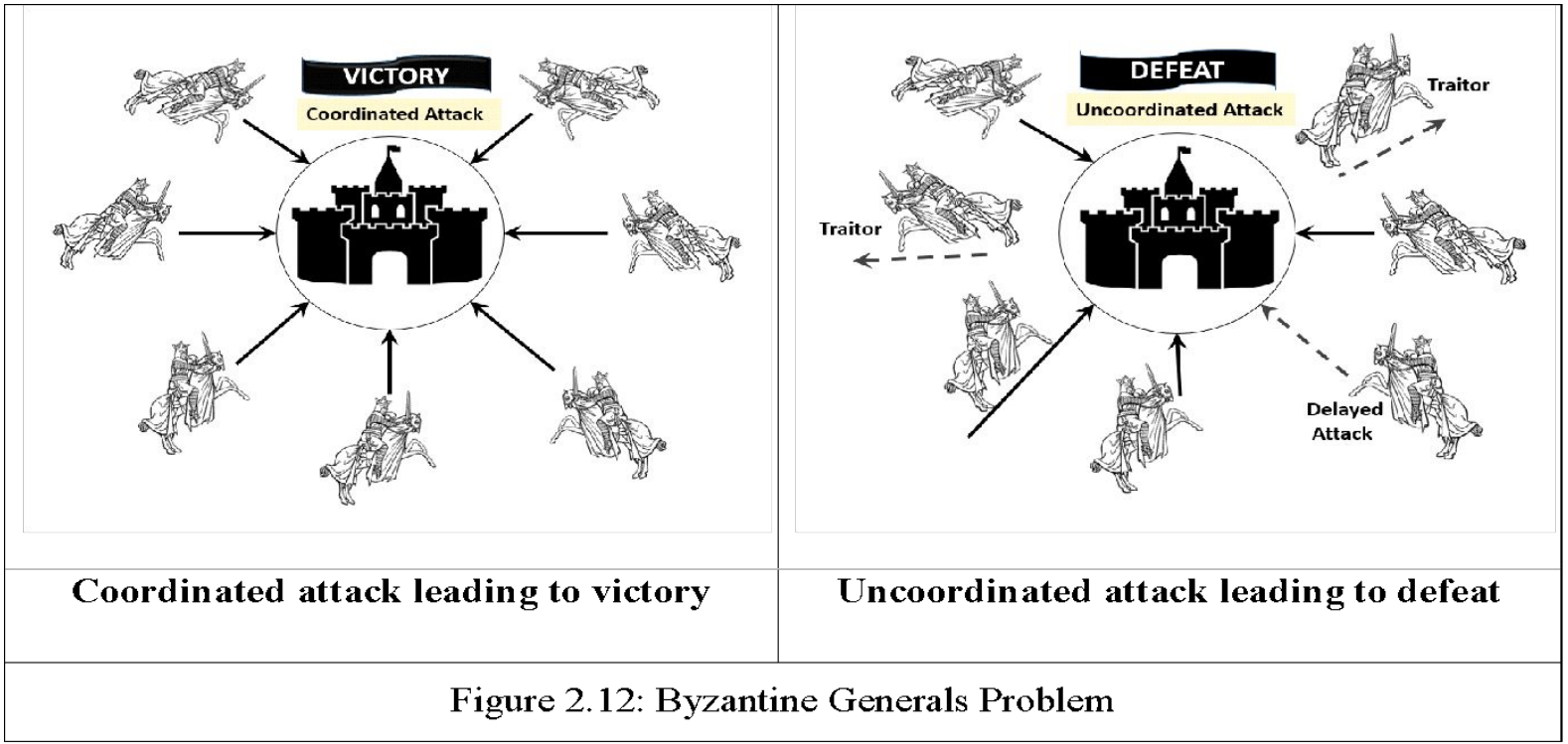


Figure 2.12: Byzantine Generals Problem

Byzantine Fault Tolerance

Blockchain Technology Fundamentals

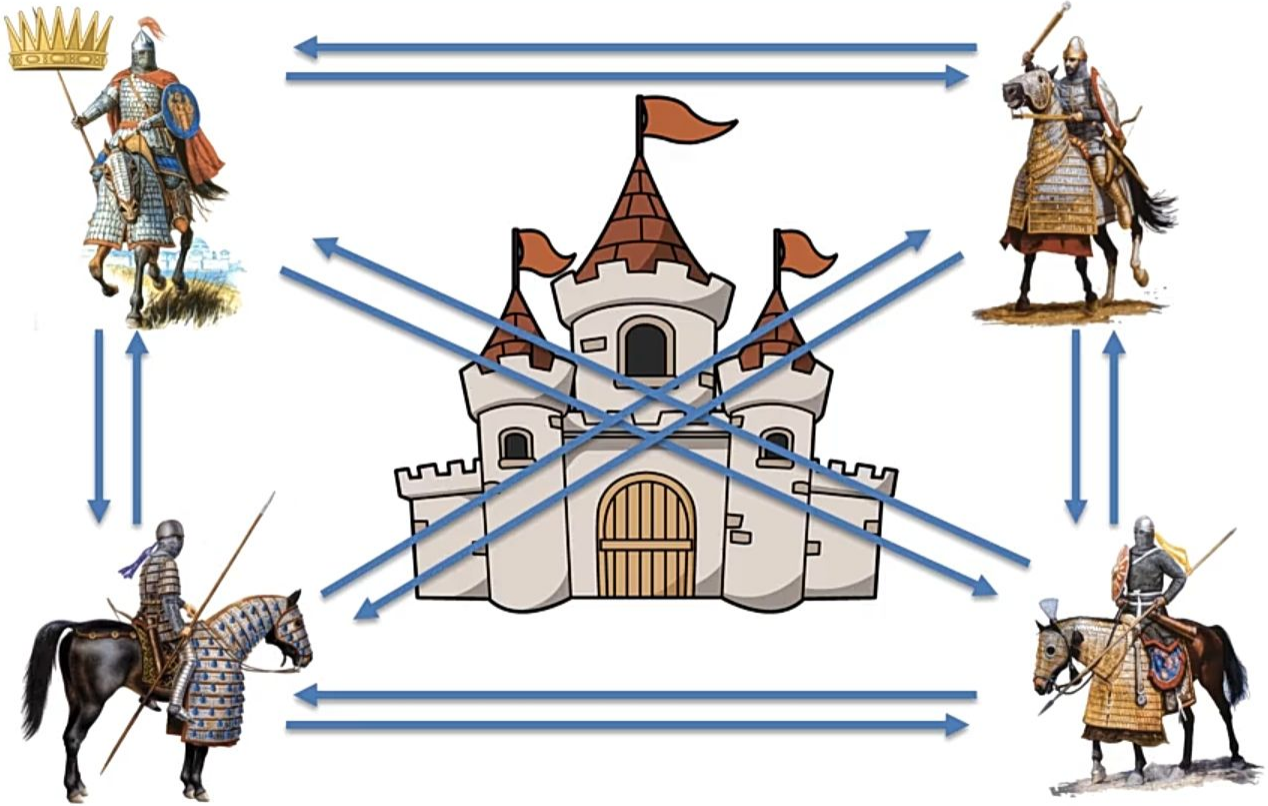
Byzantine Fault Tolerance

Blockchain Technology Fundamentals

Byzantine Fault Tolerance

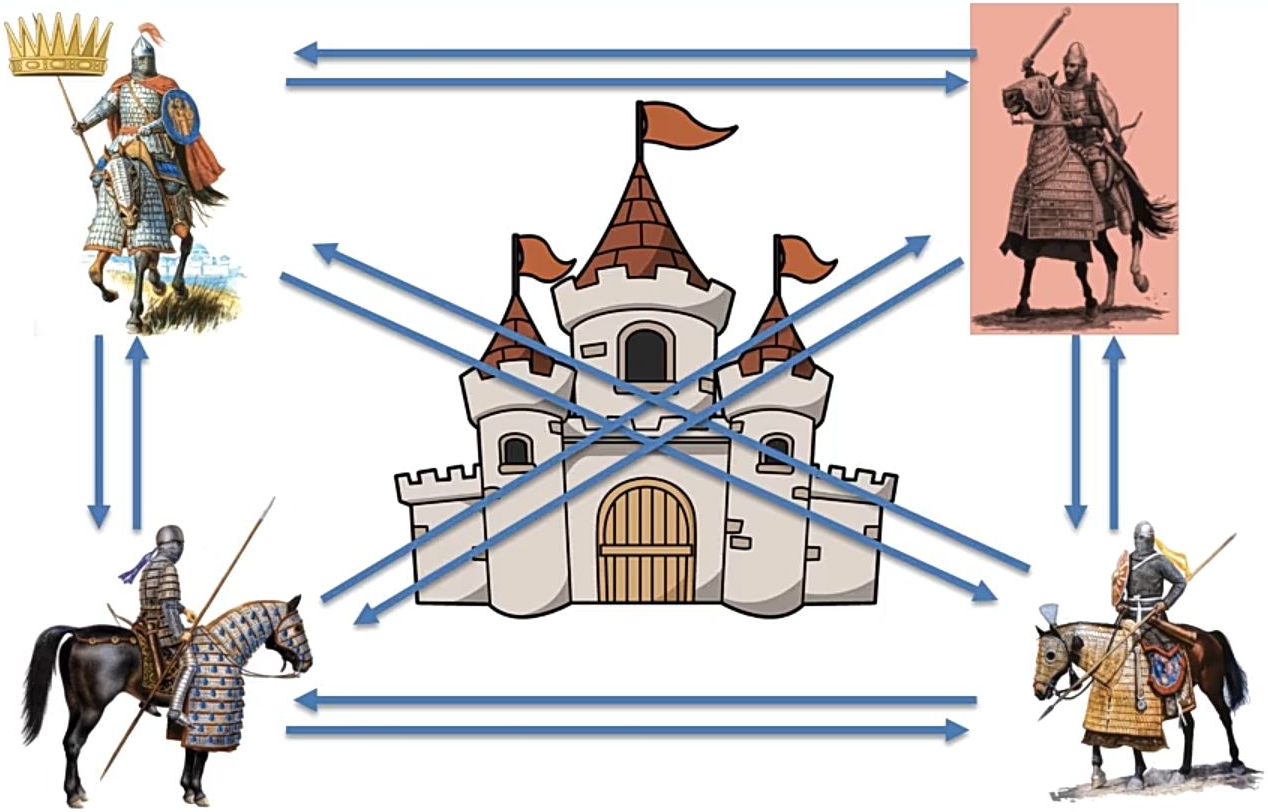
Blockchain Technology Fundamentals

Byzantine Fault Tolerance



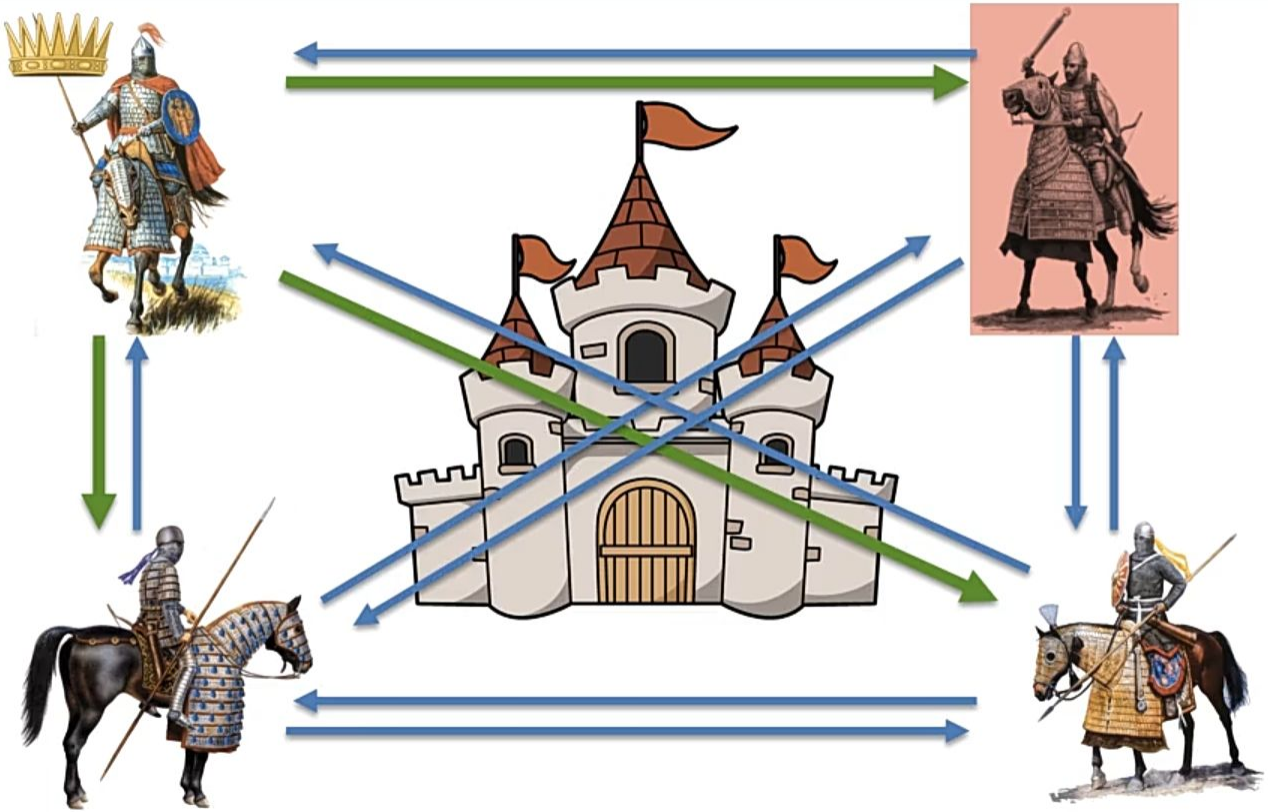
Blockchain Technology Fundamentals

Byzantine Fault Tolerance



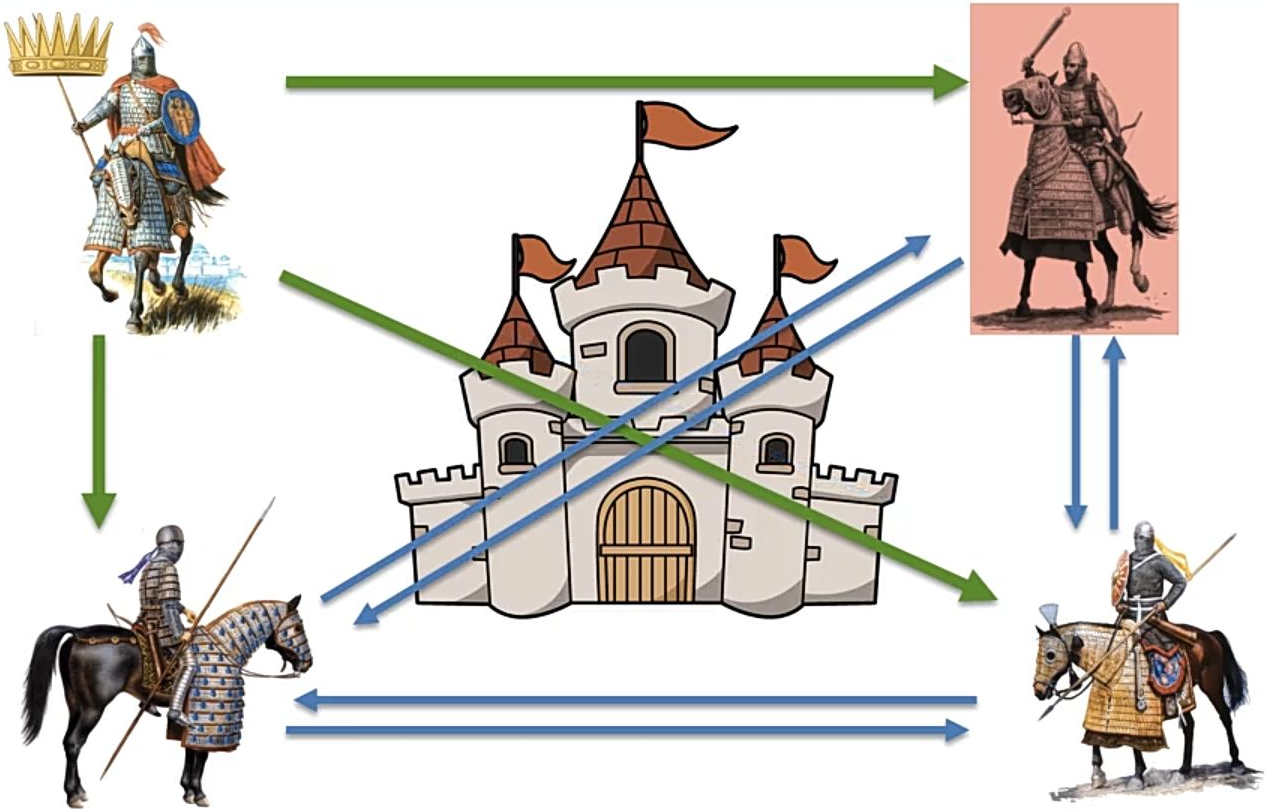
Blockchain Technology Fundamentals

Byzantine Fault Tolerance



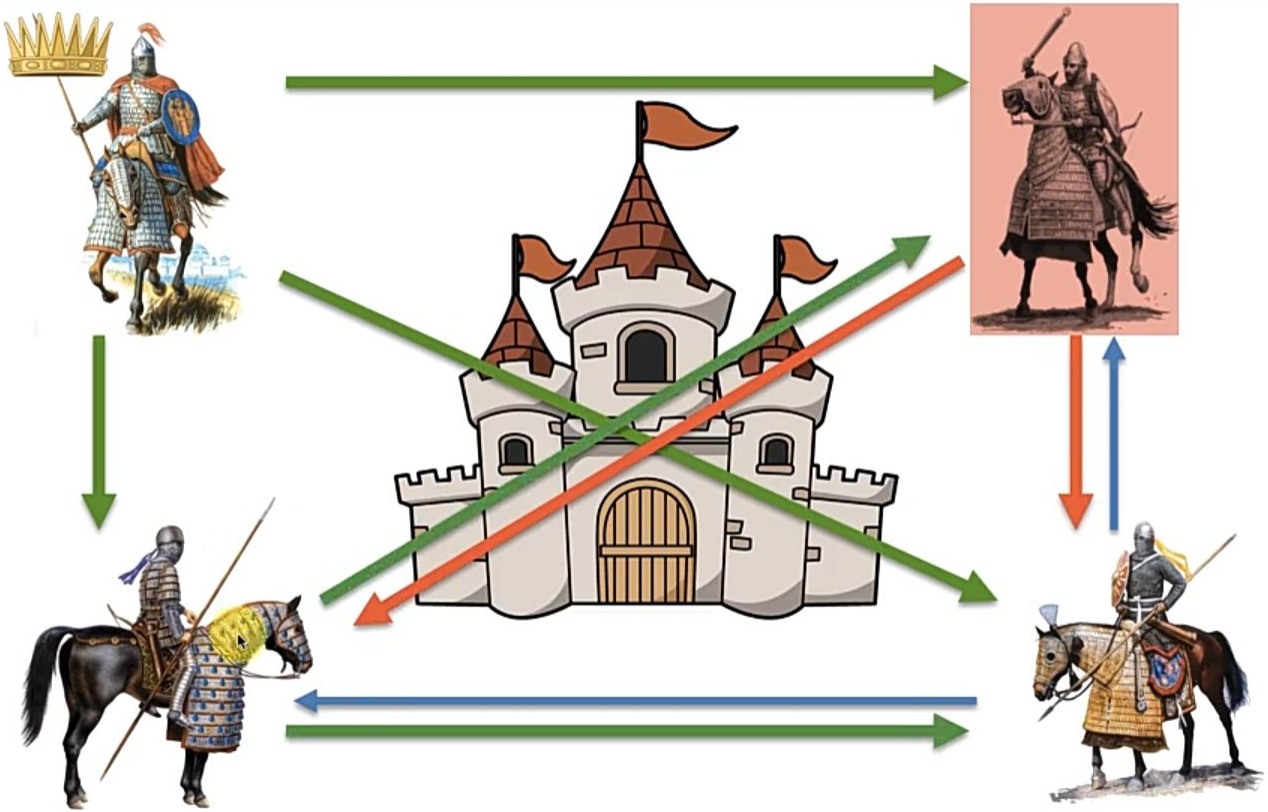
Blockchain Technology Fundamentals

Byzantine Fault Tolerance



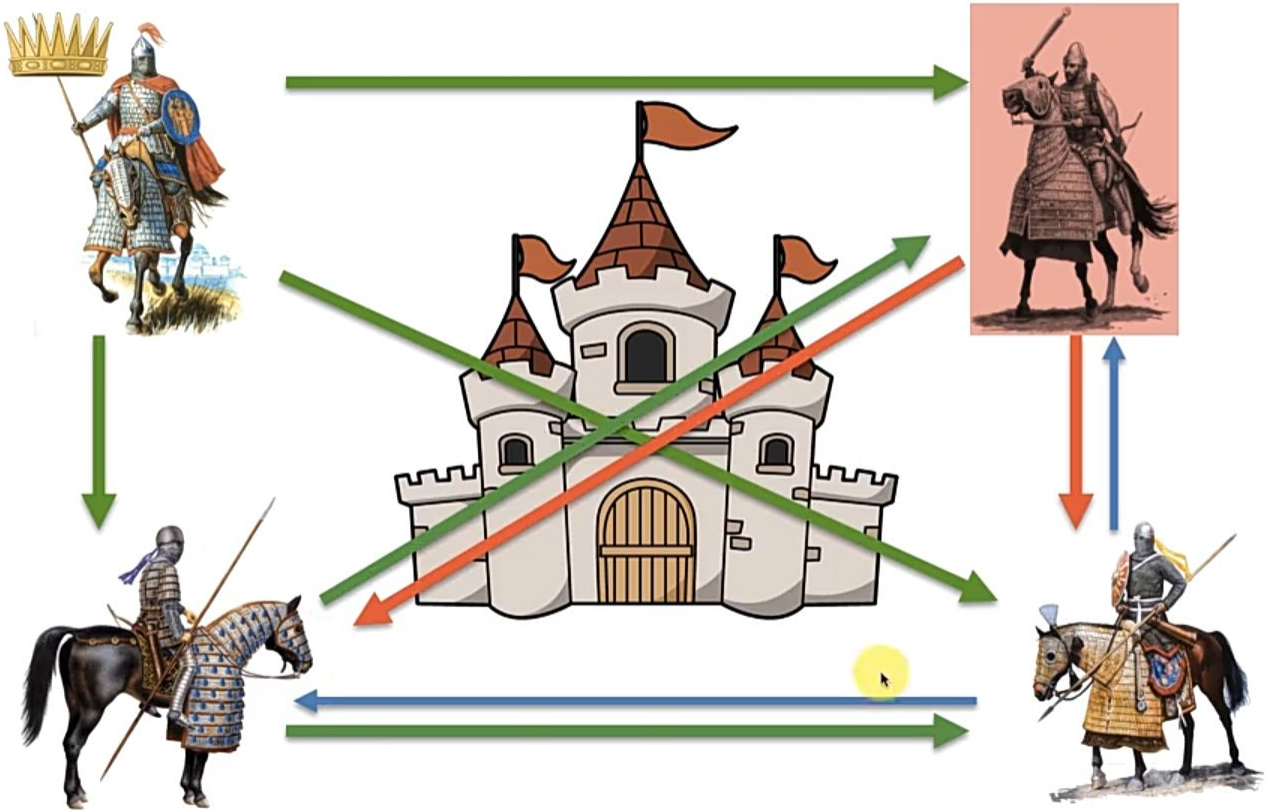
Blockchain Technology Fundamentals

Byzantine Fault Tolerance



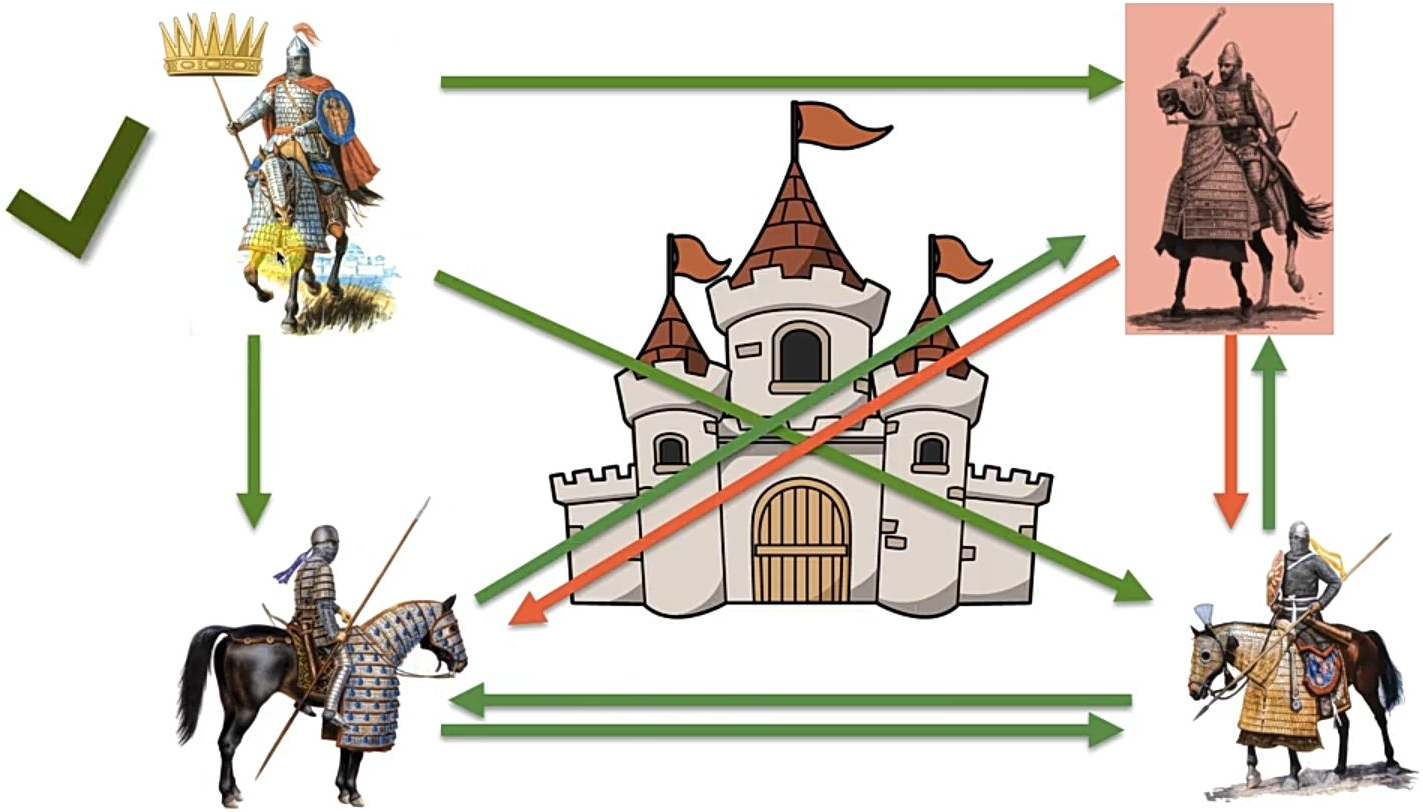
Blockchain Technology Fundamentals

Byzantine Fault Tolerance



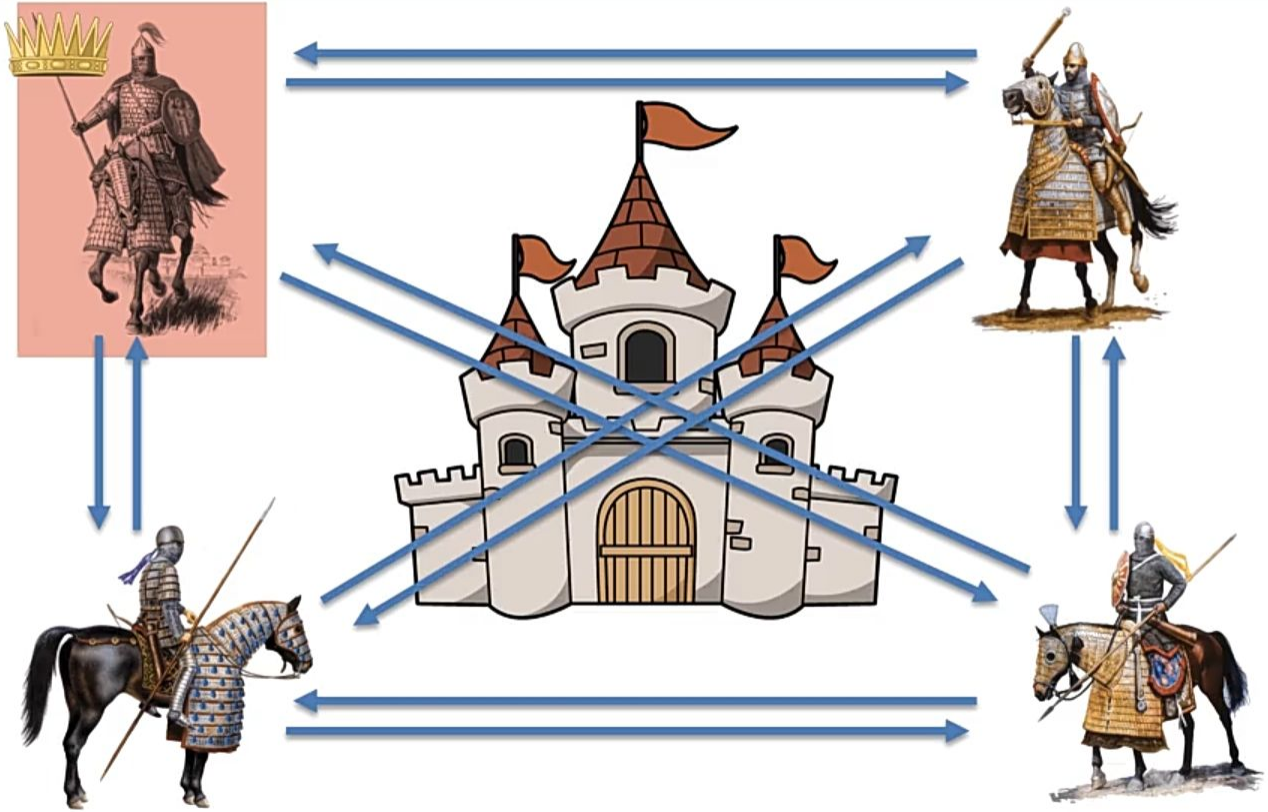
Blockchain Technology Fundamentals

Byzantine Fault Tolerance



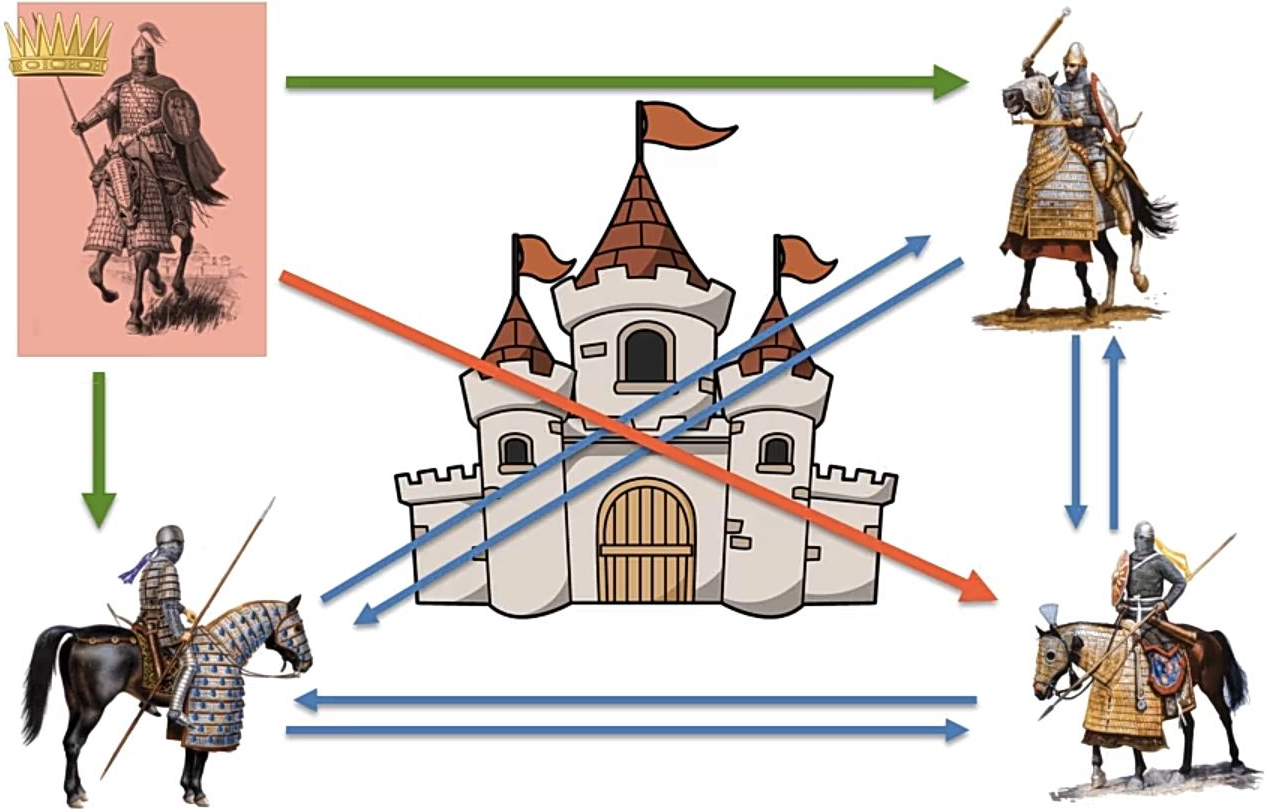
Blockchain Technology Fundamentals

Byzantine Fault Tolerance



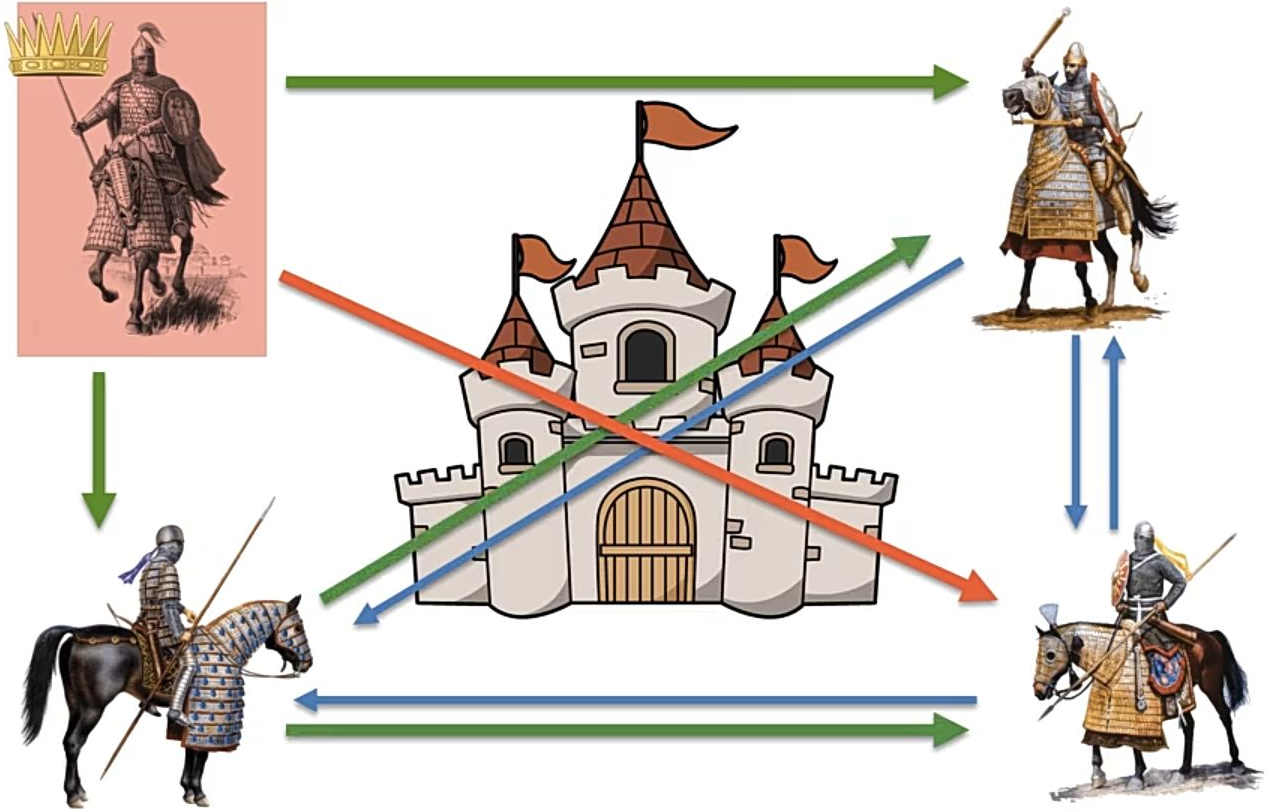
Blockchain Technology Fundamentals

Byzantine Fault Tolerance



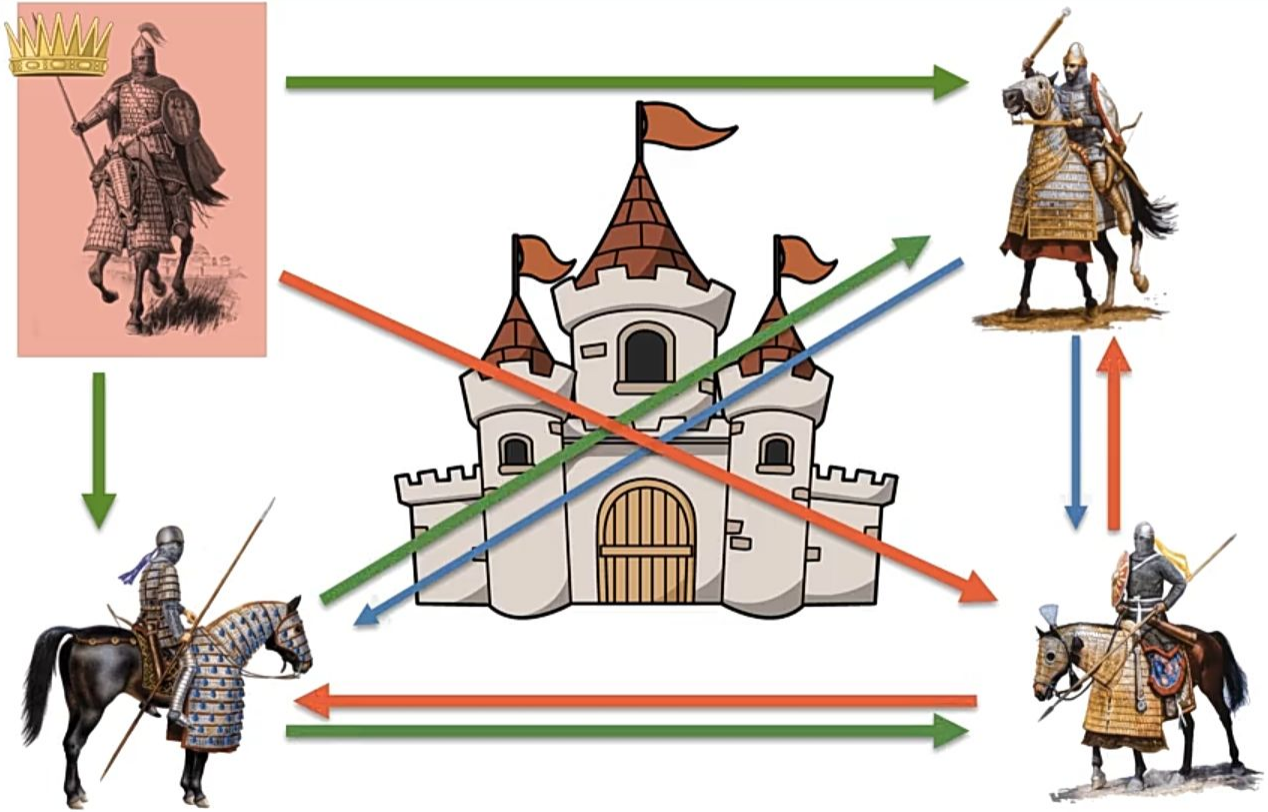
Blockchain Technology Fundamentals

Byzantine Fault Tolerance



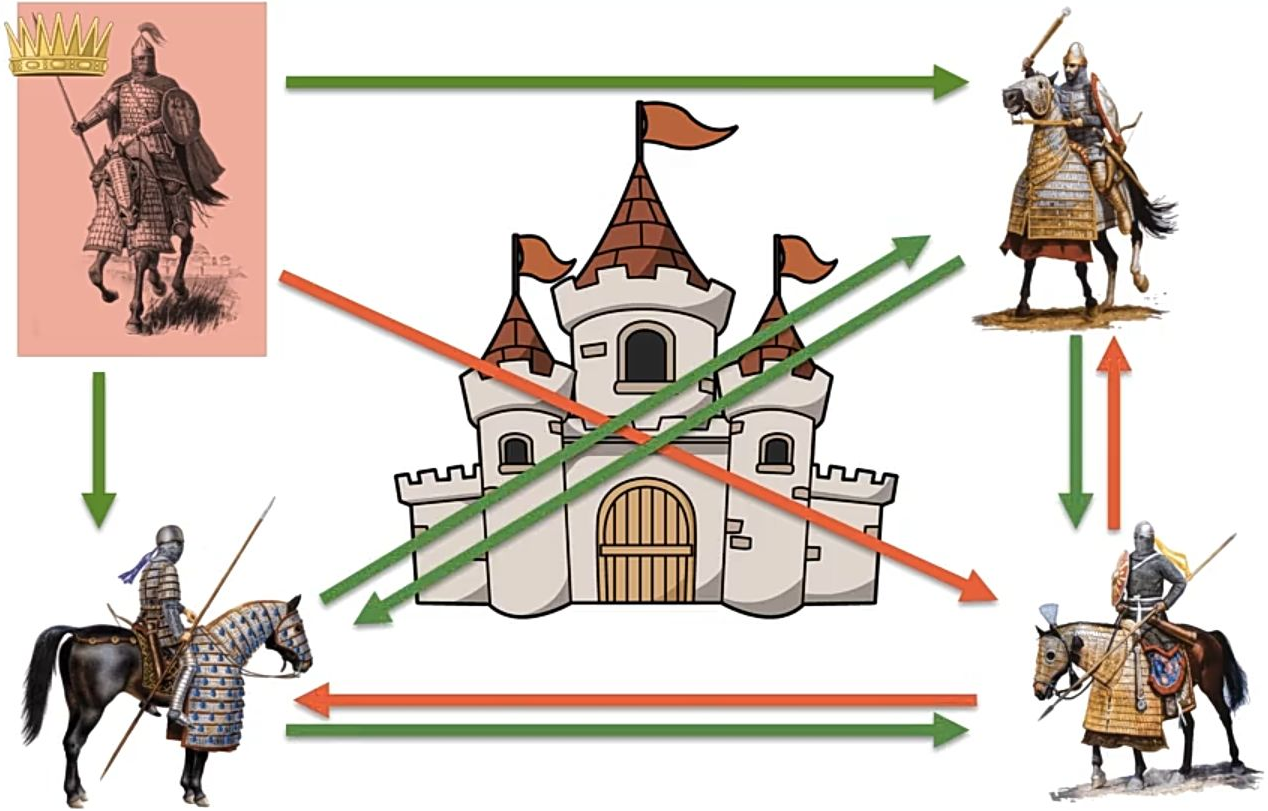
Blockchain Technology Fundamentals

Byzantine Fault Tolerance



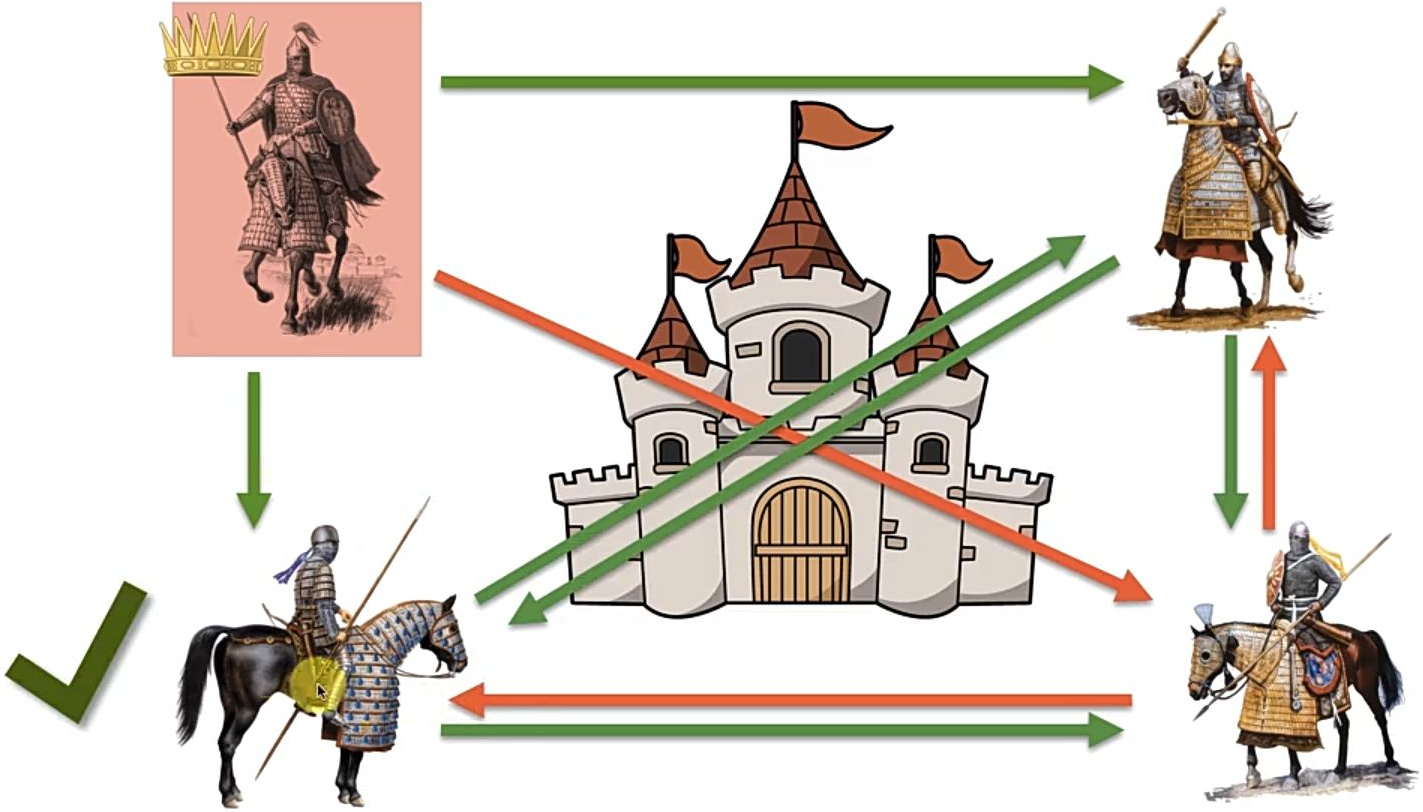
Blockchain Technology Fundamentals

Byzantine Fault Tolerance



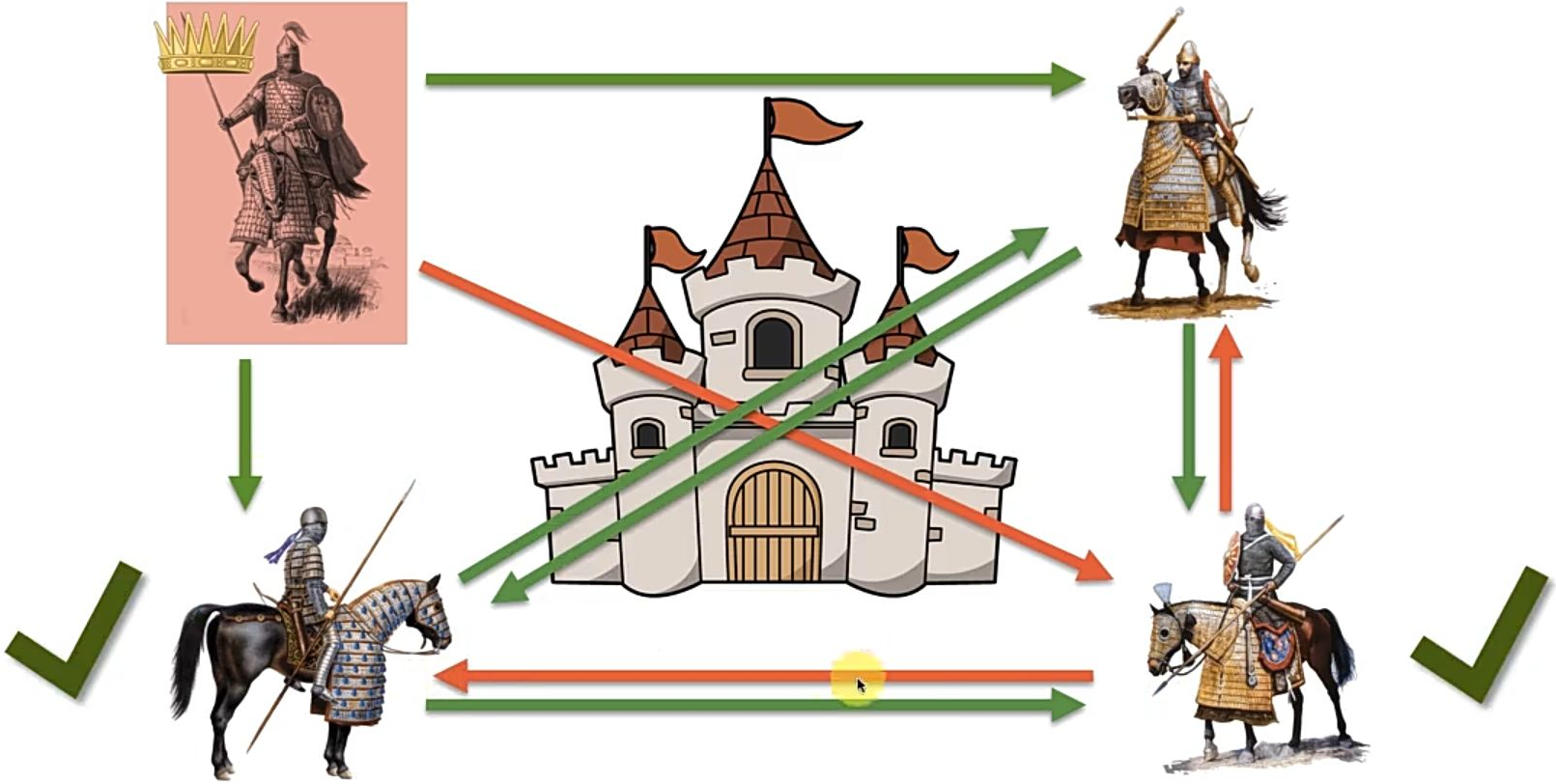
Blockchain Technology Fundamentals

Byzantine Fault Tolerance



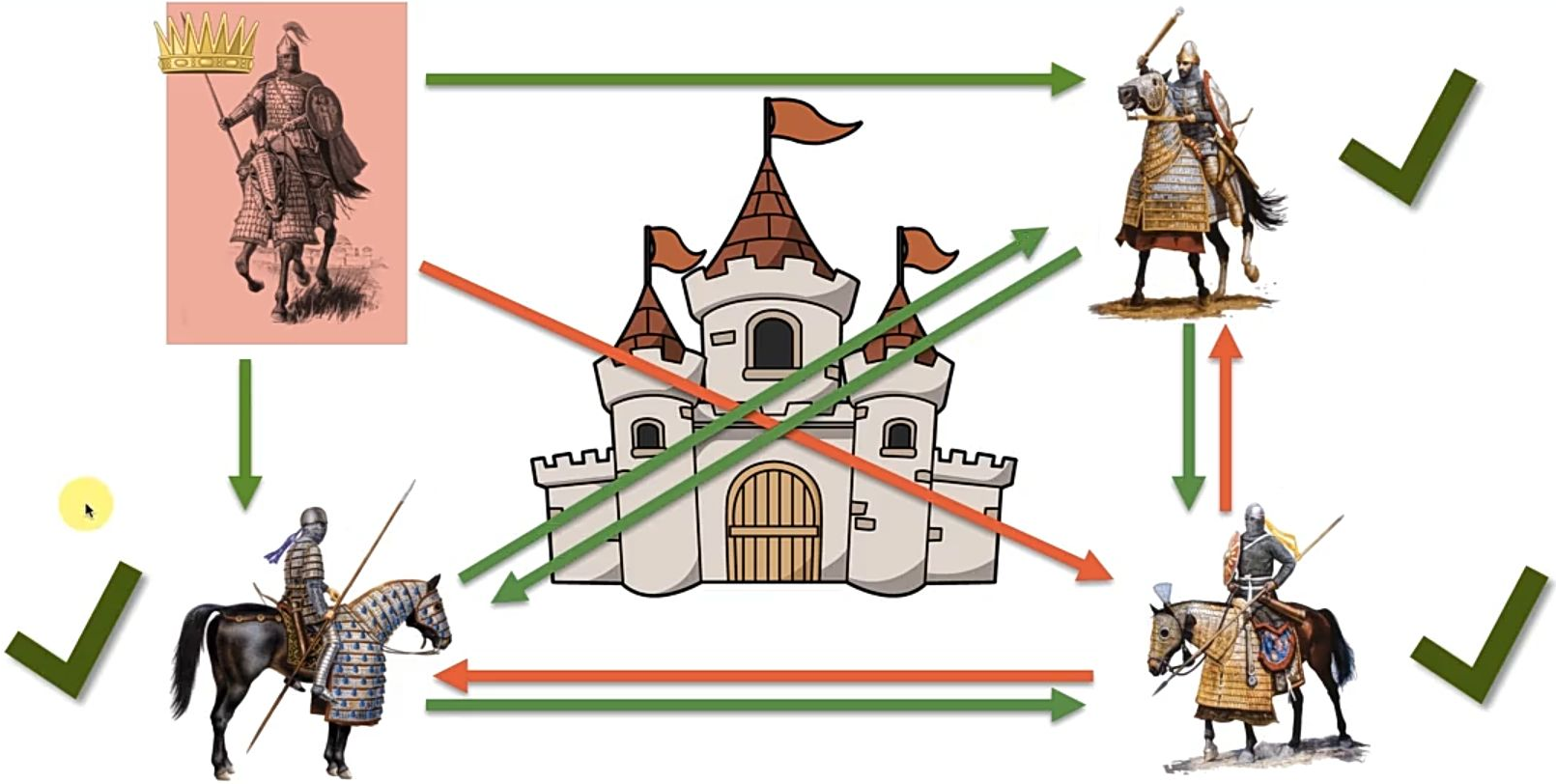
Blockchain Technology Fundamentals

Byzantine Fault Tolerance



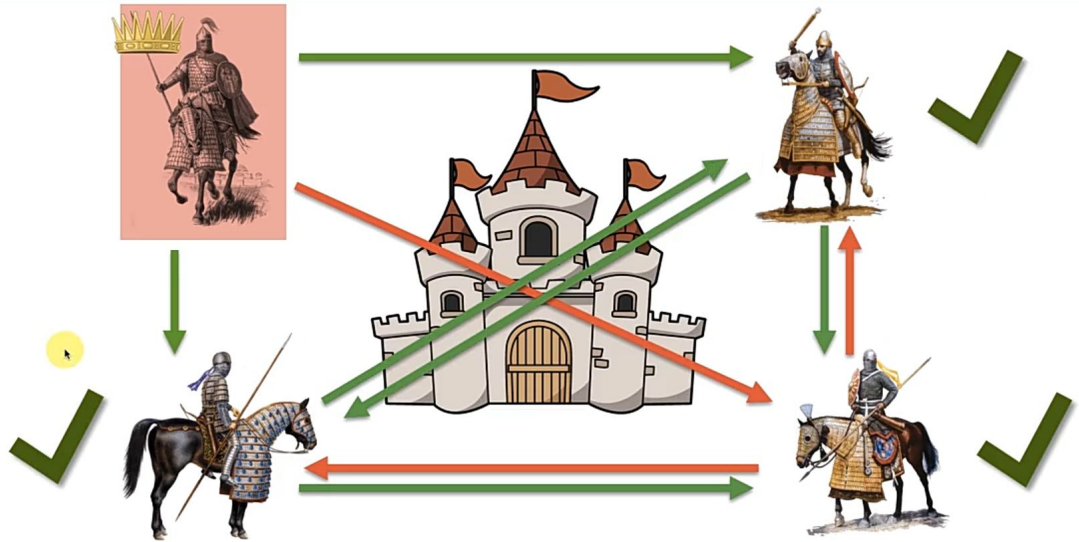
Blockchain Technology Fundamentals

Byzantine Fault Tolerance



Blockchain Technology Fundamentals

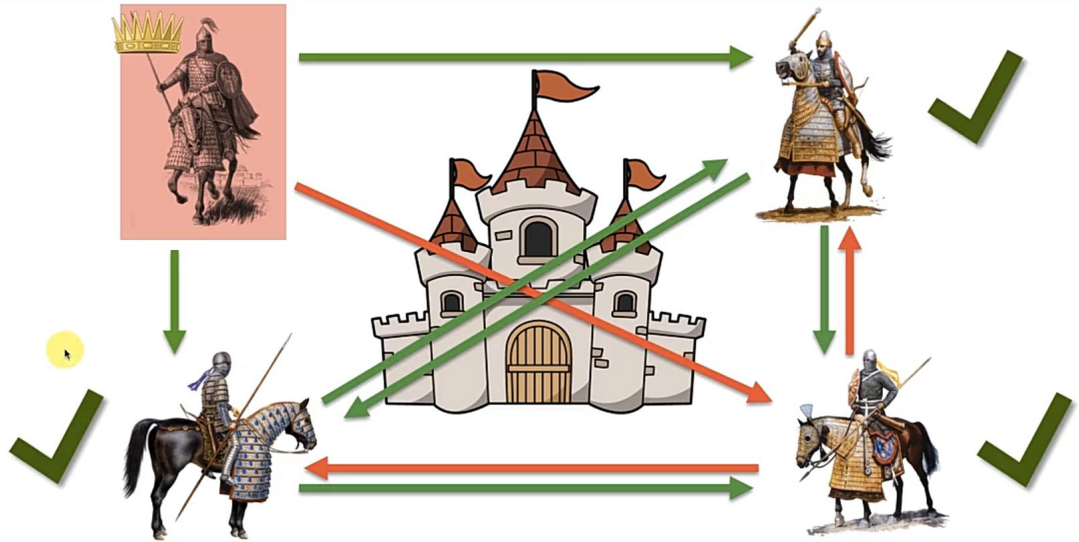
Byzantine Fault Tolerance



- What is the level of tolerance ?
- What if there are 2 traitors in this network ?

Blockchain Technology Fundamentals

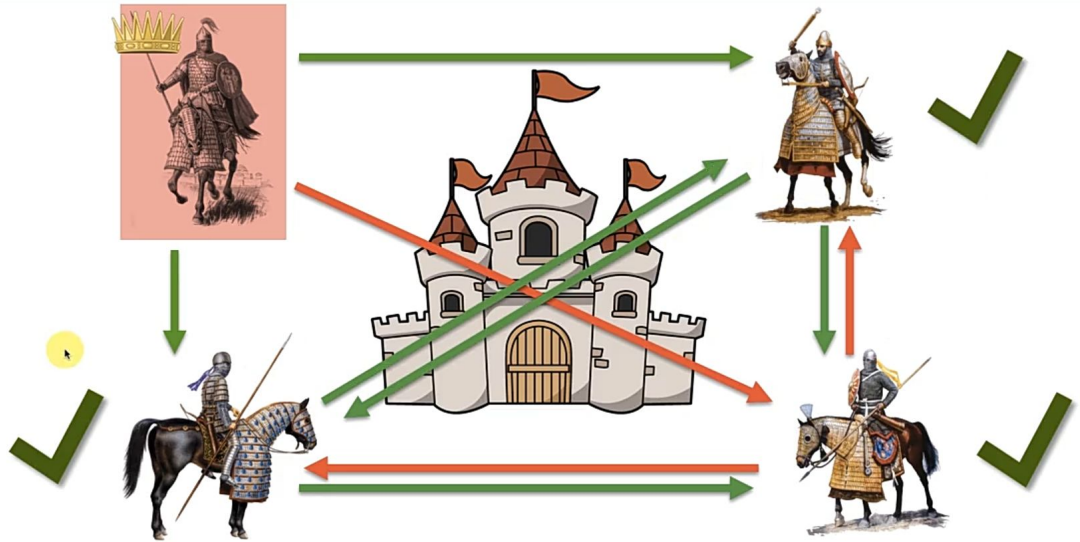
Byzantine Fault Tolerance



- What is the level of tolerance ?
- What if there are 2 traitors in this network ?
- **Not more than** ⅓ in the Army can be traitors.

Blockchain Technology Fundamentals

Byzantine Fault Tolerance



Applications of BFT

- Blockchain
- Aeroplane Circuits
- Nuclear Power Plants
- Rockets, etc …

Consensus Mechanisms

PROOF OF WORK (PoW)
- PoW lets miners add a new block to the network based on the computation done to find the correct block hash.

PROOF OF STAKE (PoS)
- PoS uses a staking mechanism where participants lock up some of their coins to get selected for block addition.

DELEGATED PROOF OF STAKE (DPoS)
- In DPoS mechanism, the block delegates' selection is based on voting. It's an additional layer to PoS.

PROOF OF IMPORTANCE (PoI)
- PoI rewards users with importance scores which eventually helps them to become block harvesters.

PROOF OF CAPACITY (PoC)
- PoC uses the storage capacity for mining a block in a decentralized network.

PROOF OF ELAPSED TIME (PoET)
- PoET uses a time-lottery-based consensus mechanism, distributing wait time to each participating node.

PROOF OF ACTIVITY (PoA)
- Proof of Activity (PoA) combines the capabilities of proof of work (PoW) and Proof of Stake (PoS) algorithms.

PROOF OF AUTHORITY (PoA)
- Proof of Authority (PoA) relies on the validator's reputation to make the blockchain work properly.

PROOF OF BURN (PoB)
- PoB allows miners to add their block by sending some of their coins to an unspendable account.

BYZANTINE FAULT TOLERANCE (BFT)
- BFT works on system to stay intact even if one of the nodes fails with constant communication among nodes.

Courtesy : Devopedia

Applications of Blockchain Beyond Cryptocurrencies

Why Blockchain Beyond Cryptocurrency?

- Trust without intermediaries
- Tamper-proof records
- Automation using smart contracts
- Improved transparency and traceability

Courtesy : EDUCBA

Applications of Blockchain Beyond Cryptocurrencies

Supply Chain Management

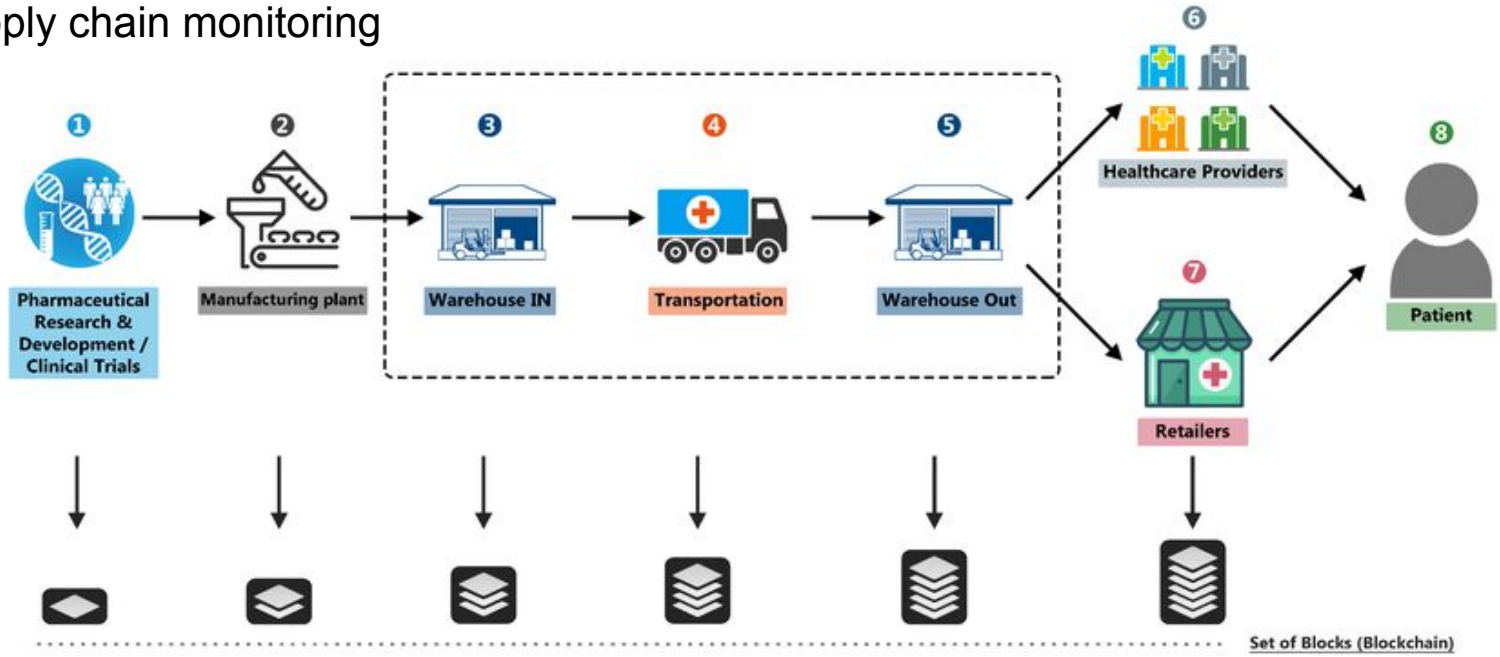
- End-to-end product traceability
- Prevention of counterfeit goods
- Real-time tracking of goods
- Eg: **Walmart** (for food traceability)

Courtesy : Walmart, LFDT

Applications of Blockchain Beyond Cryptocurrencies

Healthcare

- Secure patient health records
- Interoperability between hospitals
- Eg : Drug supply chain monitoring

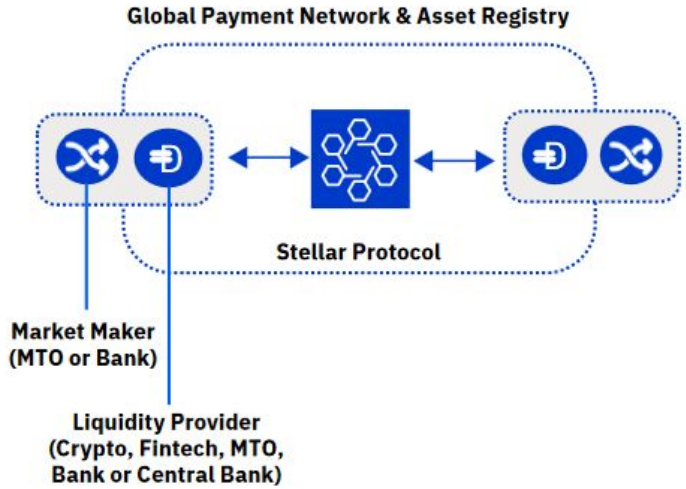


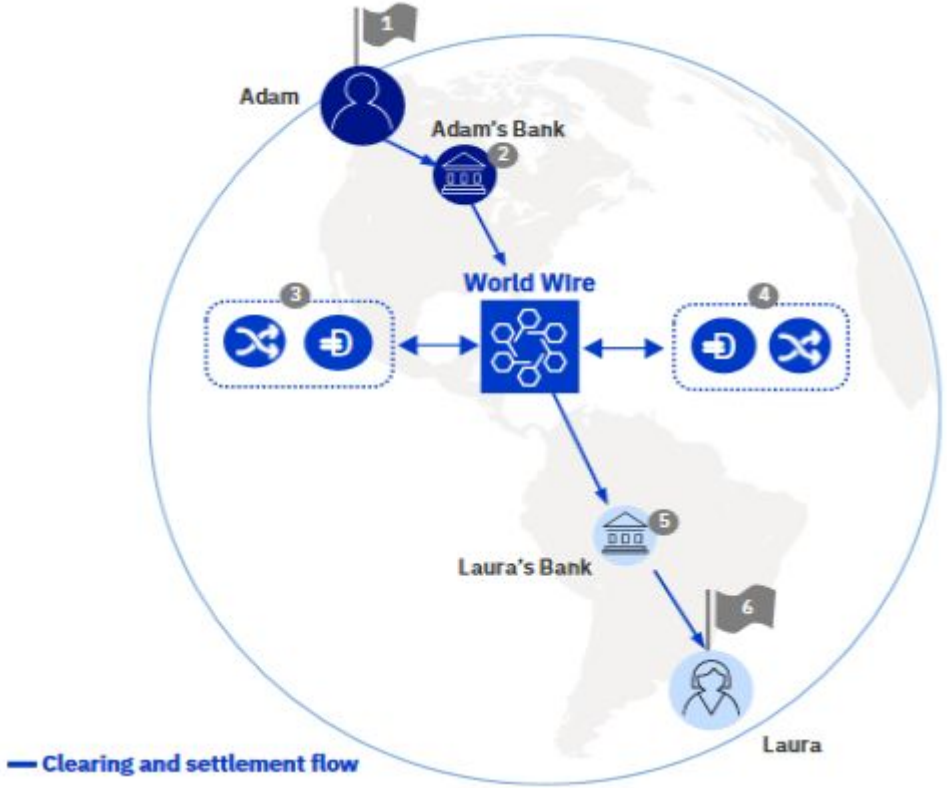
Courtesy : Drug Monitoring

Applications of Blockchain Beyond Cryptocurrencies

Finance & Banking (Beyond Crypto)

- Cross-border payments
- Trade finance
- Fraud reduction
- Example: IBM Blockchain World Wire



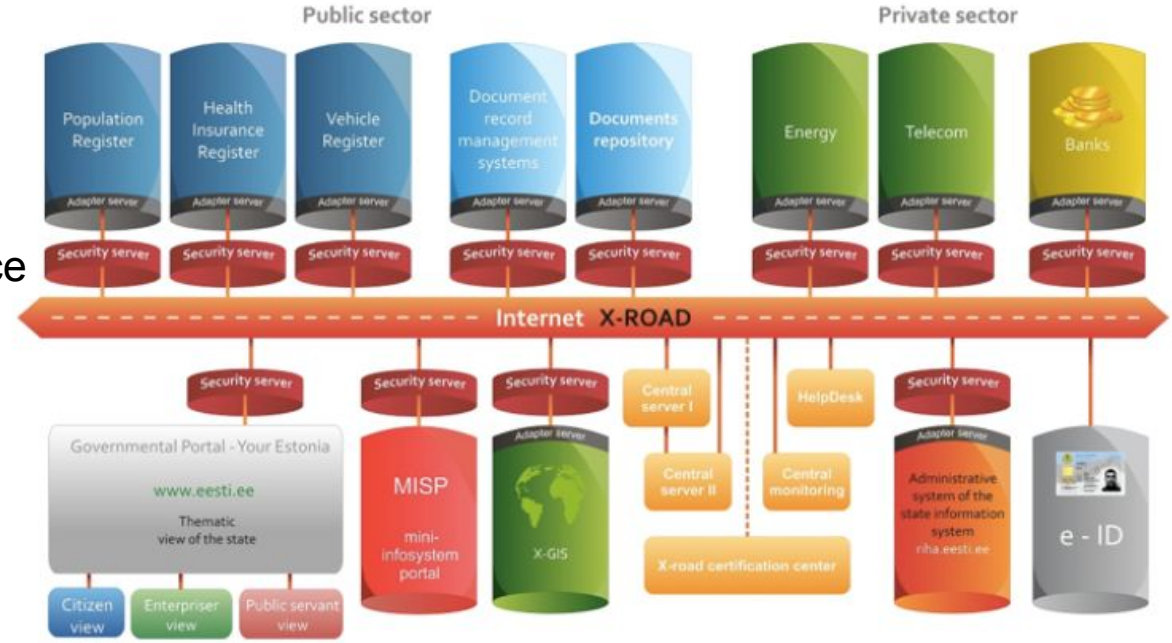


Courtesy : IBM World Wire

Applications of Blockchain Beyond Cryptocurrencies

Governance & Voting Systems

- Secure and transparent voting
- Reduced election fraud
- Improved trust in governance
- Example: Estonia e-Governance

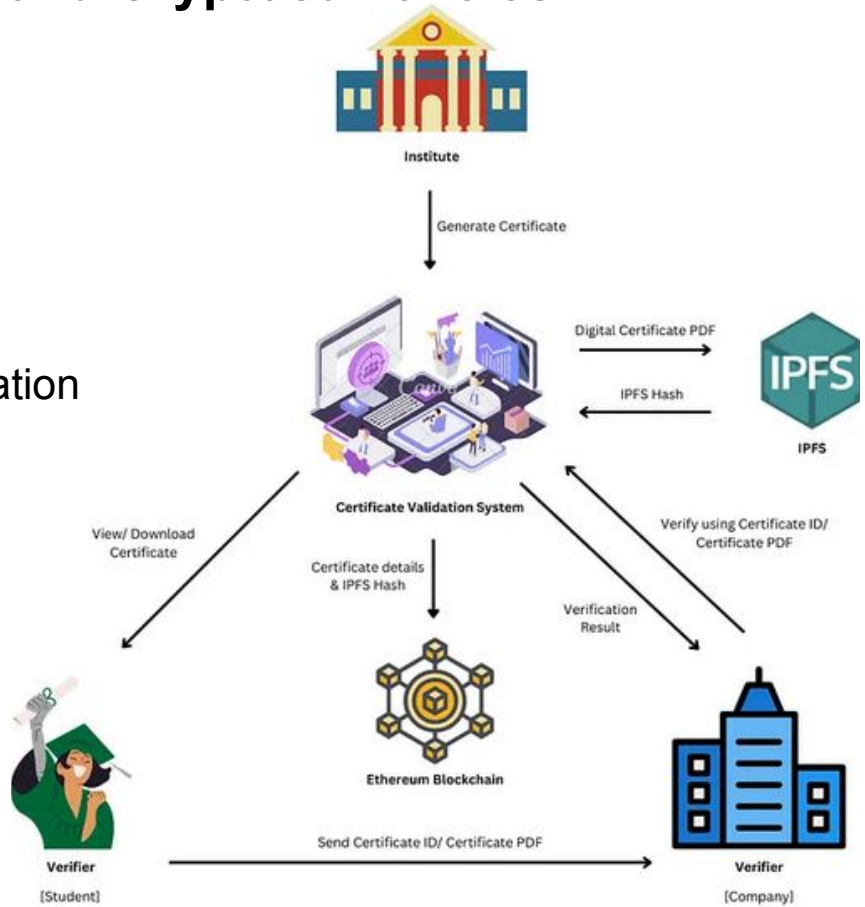


Source: e-estonia.com

Applications of Blockchain Beyond Cryptocurrencies

Education

- Tamper-proof academic certificates
- Verification of credentials
- Reduced certificate forgery
- Ex: Blockchain-based degree verification

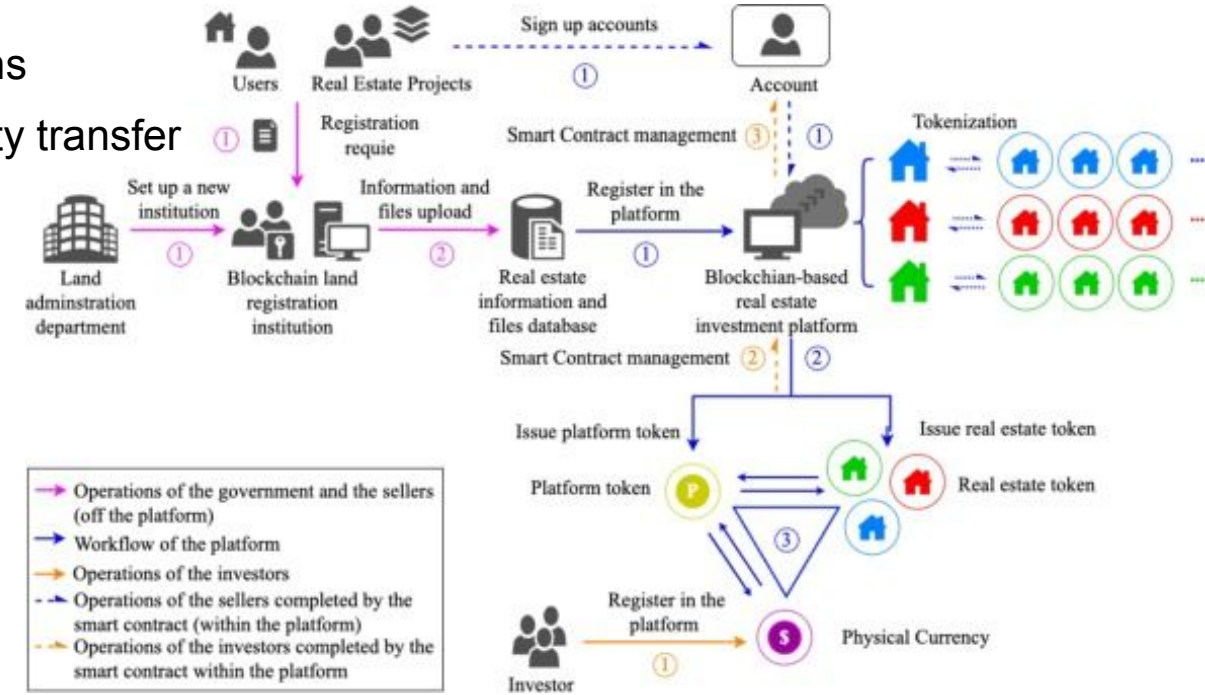


Courtesy : Medium - Certificate Verification

Applications of Blockchain Beyond Cryptocurrencies

Real Estate

- Property ownership records
- Fraud prevention
- Smart contracts for transactions
- Faster and transparent property transfer

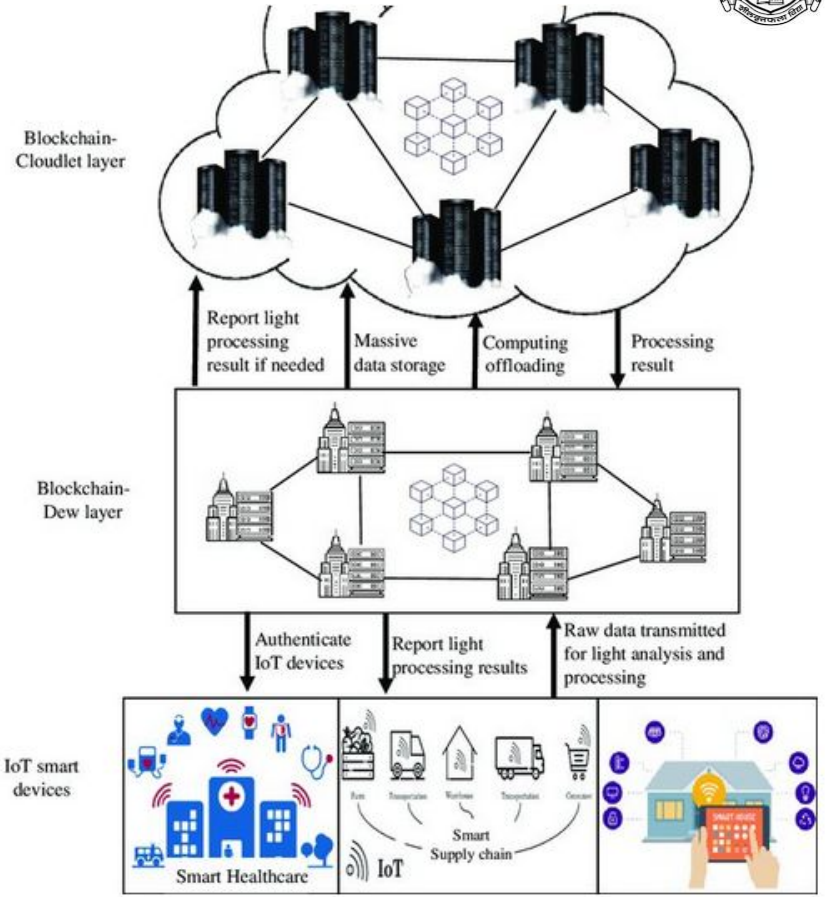


Courtesy : ScienceDirect - Land registry

Applications of Blockchain Beyond Cryptocurrencies

Internet of Things (IoT)

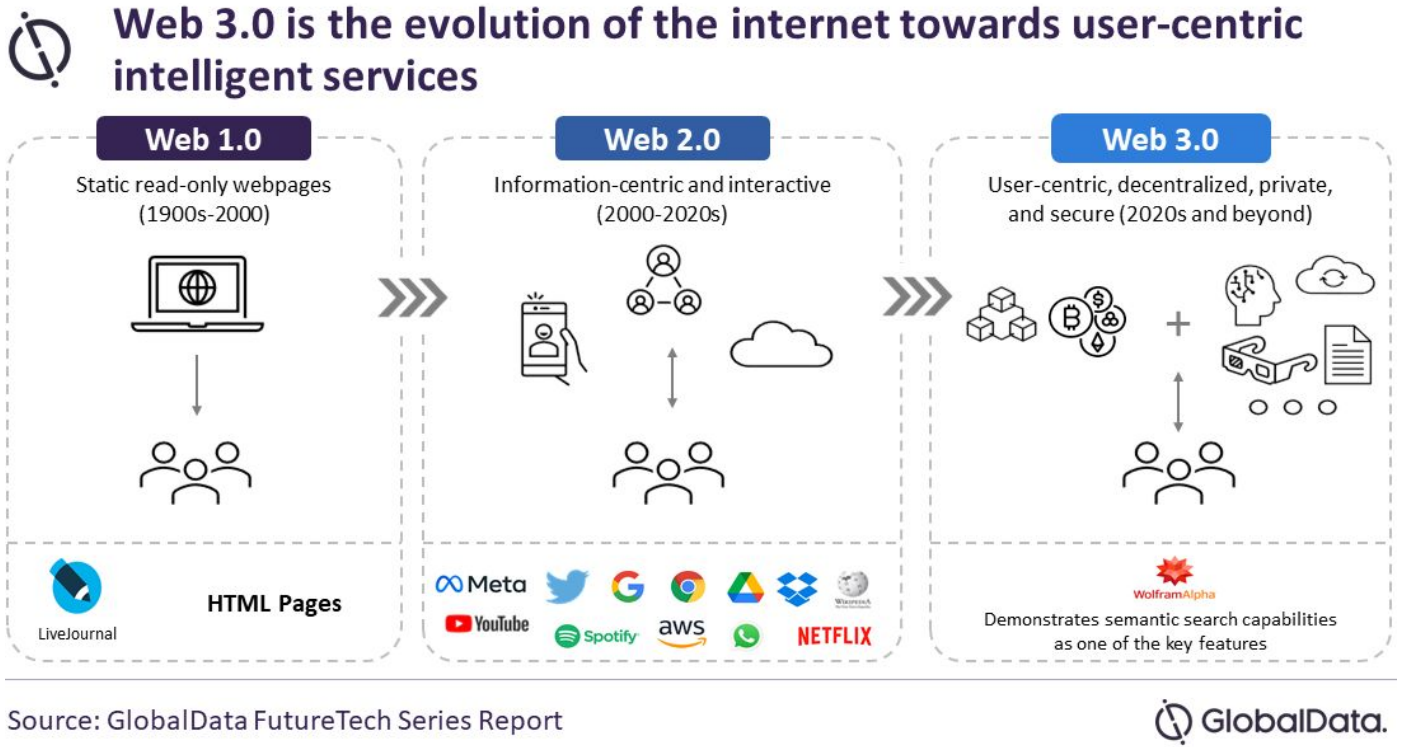
- Secure device communication
- Decentralized IoT networks
- Data integrity and authentication



Courtesy : ResearchGate - BIoT

Blockchain's Role in Decentralization and the Future of Web3

Evolution of Web



Courtesy : Global Data

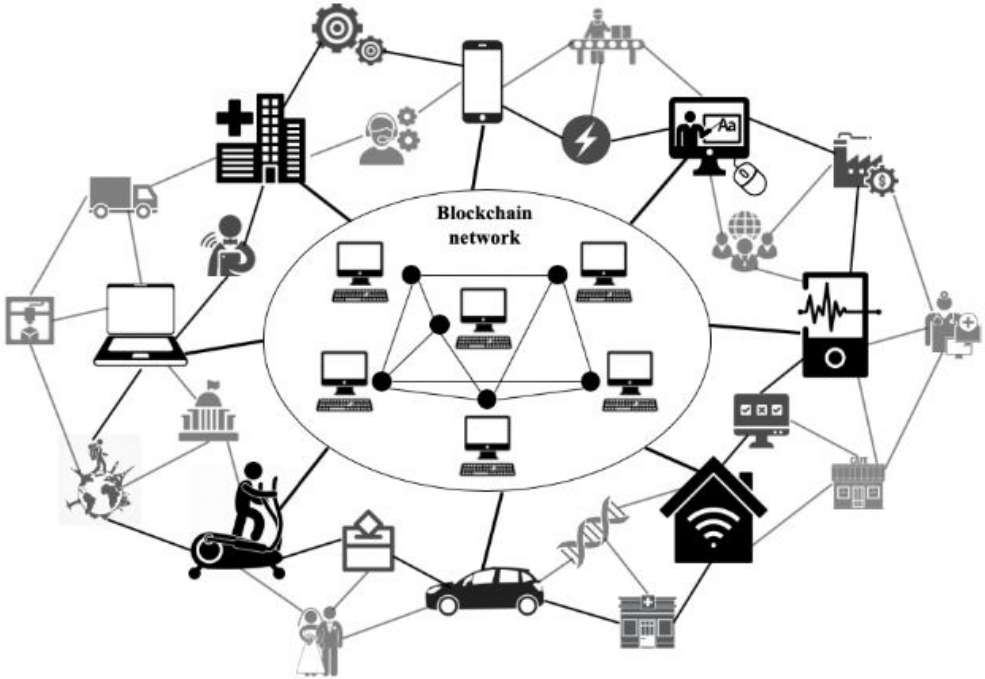
Blockchain's Role in Decentralization and the Future of Web3

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



Courtesy : ResearchGate

Blockchain's Role in Decentralization and the Future of Web3

What is Web3?

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

Key Components of Web3

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

Blockchain's Role in Decentralization and the Future of Web3

Real-World Use Cases

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

Benefits of Web3

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

Blockchain's Role in Decentralization and the Future of Web3

Challenges in Web3 Adoption

- Layer-2 scalability solutions
- Enterprise and government adoption
- Integration with AI and IoT

Future of Web3

- Scalability
- Regulatory uncertainty
- Security risks
- User experience

Courtesy : 101 Blockchains