Unit I - Introduction to Blockchain Technology

Text Book:

Mastering Blockchain

Unlocking the Power of Cryptocurrencies and Smart Contracts

Authors

Lorne Lantz & Daniel Cawrey

Electronic Systems and Trust

- Initially, in 1960, the internet was a simple, relatively small network
- It was primarily used as a tool for university researchers and the US government to share information digitally
- With time TCP/IP model and other protocols came into existence such as HTTP and SMTP
- Thus, electronic systems evolved
- However, using online services and products require use of **Trusted Third Parties – TTP** (intermediaries)
  - These TTPs act as ***trusted gatekeepers***
- In general, electronics systems require **two types** of trust
  - **Intermediary Trust:** A third party is relied on to make rational and fair decisions
  - **Issuance Trust:** A third party is relied on to ensure the safety and security of any value.

Centralized – Decentralized – Distributed

- Internet today is mix of centralized and distributed applications
- Internetworks were designed as distributed system initially with the goal that
  - ***if one part of the system were attacked, remaining part would still be able to operate***
- In the recent times, companies such as Google, Facebook, Apple, and Amazon have **dominated** and turned the internet into more centralized system

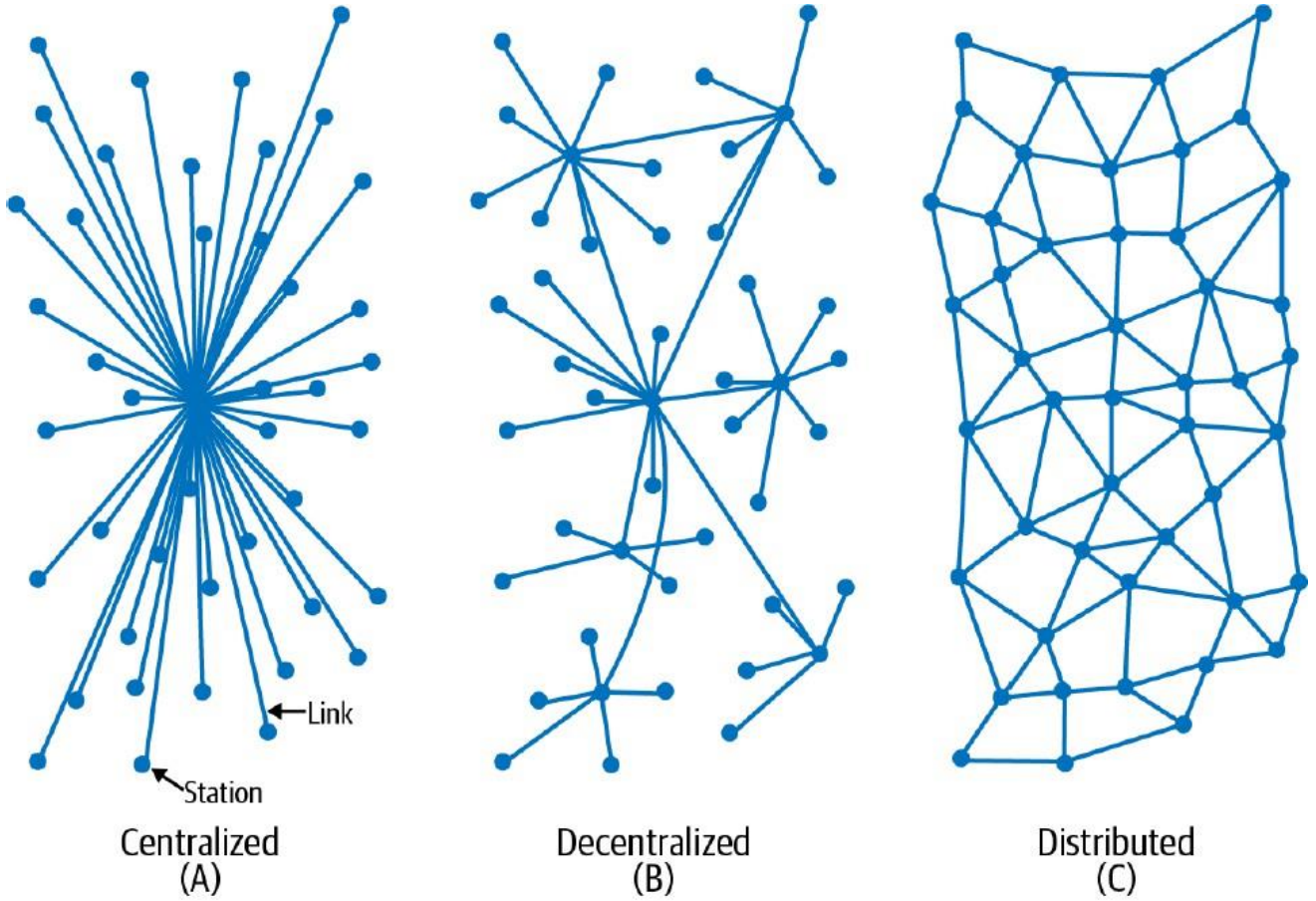


Figure 1-2. Centralized, decentralized, and distributed network designs

Centralized System

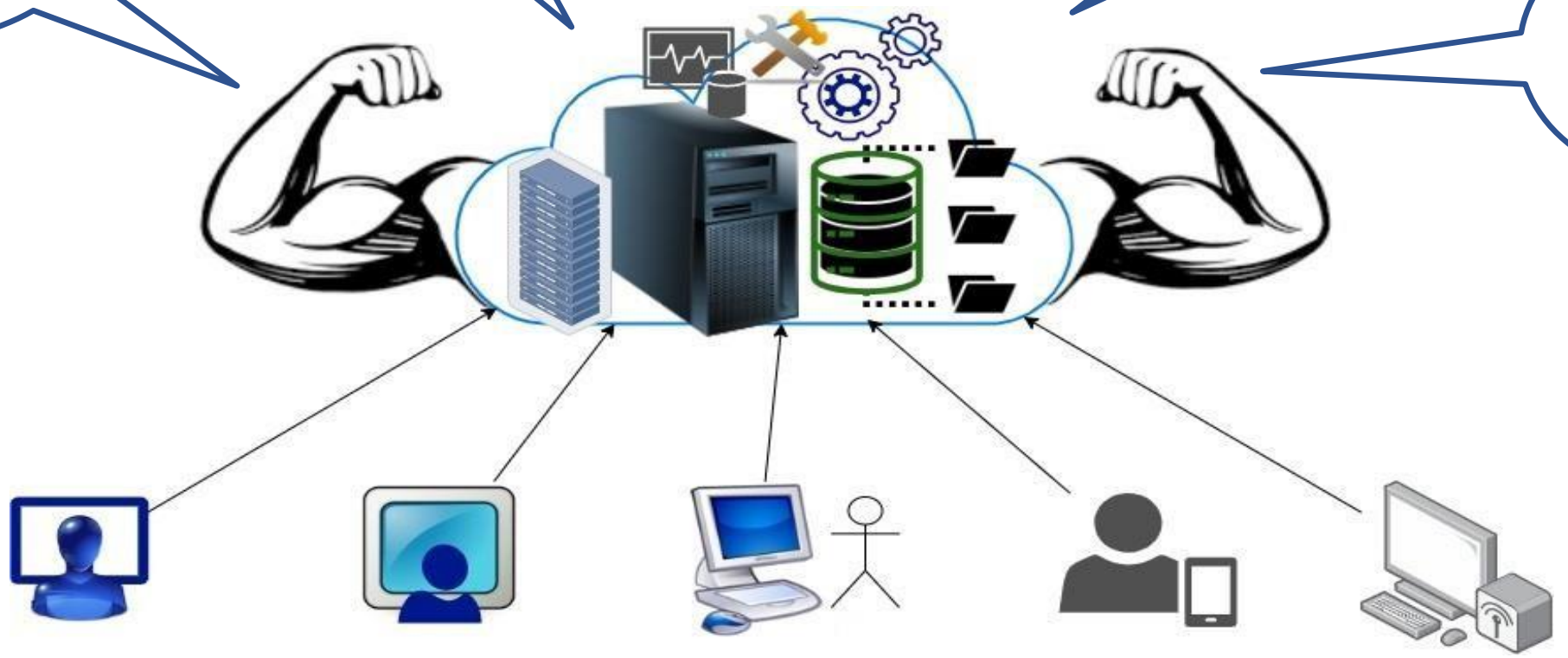
High physical security since housed at fixed locations

No need for multiple infrastructure facility

Easy monitoring, maintenance, and controllability

Established legal frameworks for auditing and compliance

Supports closed markets and businesses



Issues with Centralized Systems and Database

Centralized in Nature

- Loss of ownership
- Single point-of-failure
- Not open and limited access
- Availability issue due to down time

Third Party Invocation

- Authoritative entities
- Processing delay
- Fee
- Privacy Issue

Centralized System – An Example

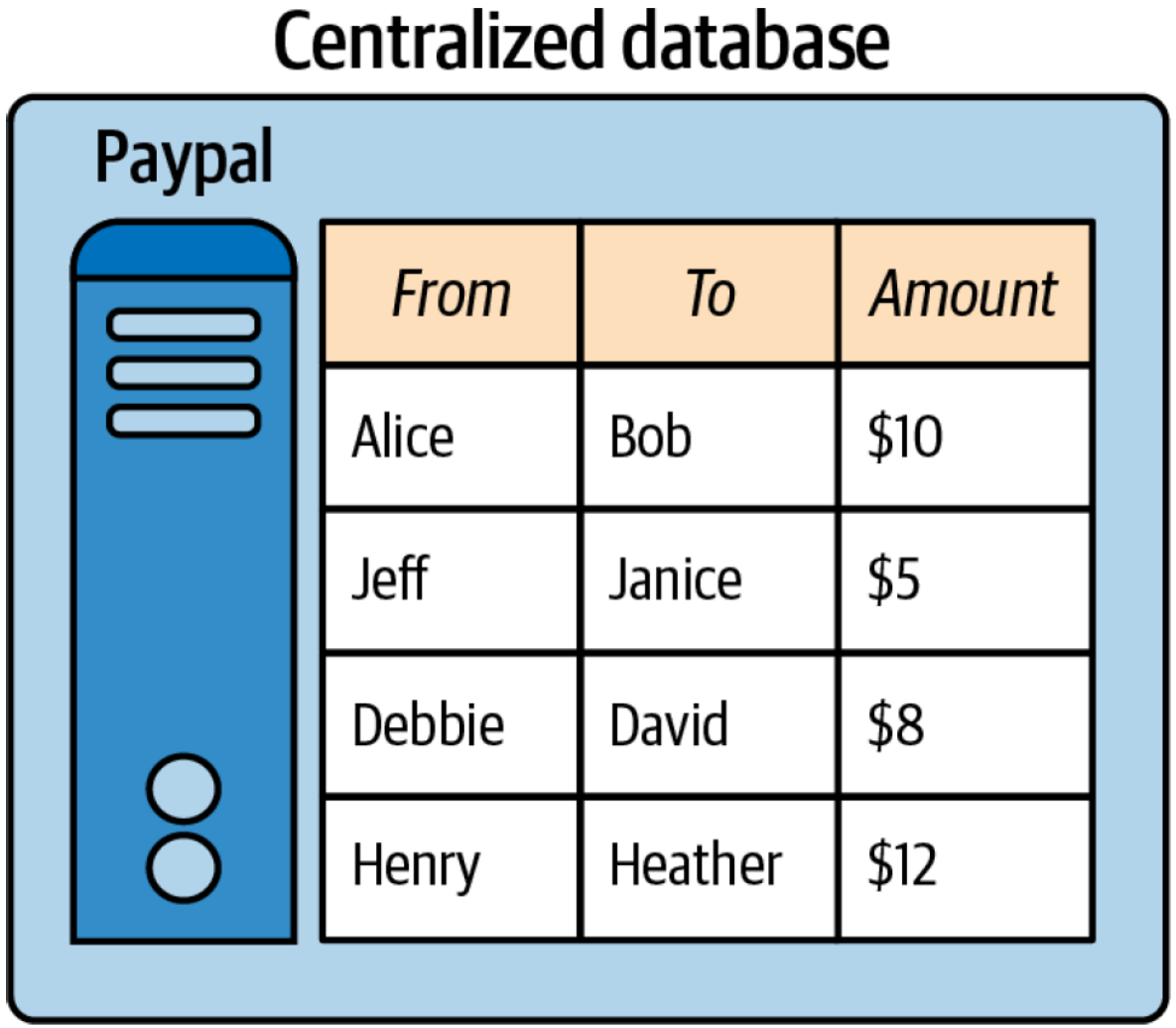
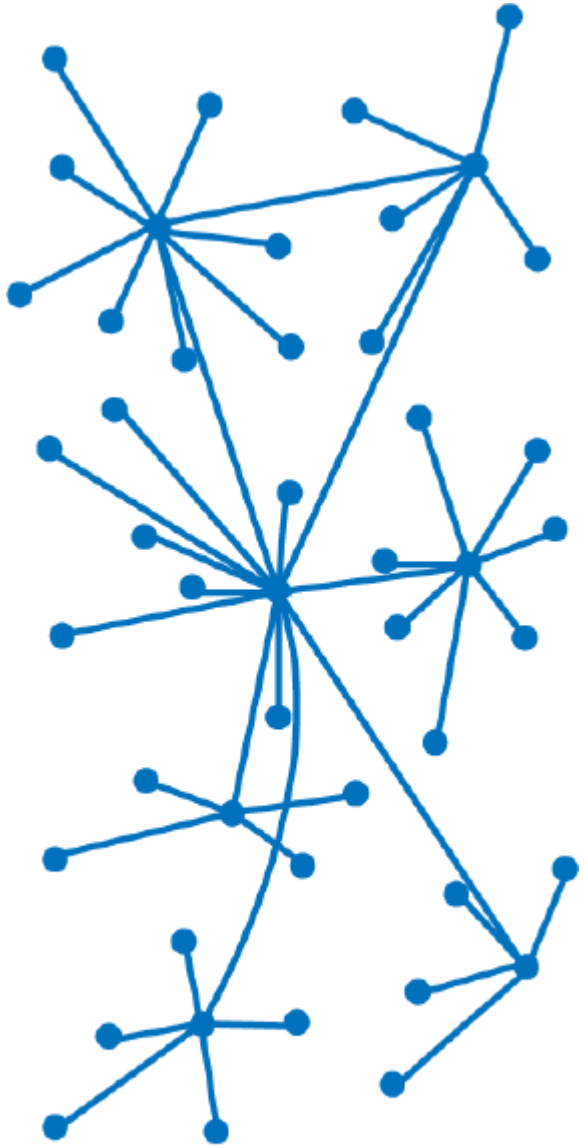


Figure 1-3. In a centralized database, like PayPal, all nodes connect to a single, central node that is controlled by one entity

Decentralized System

- In a fully decentralized system, a given node **does not** necessarily **collaborate** with every other node to achieve its objective
- In fact, **every node** makes its **own decision** and hence, has different clocks that they run and follow
- The **final behavior** of the system is **driven by the consensus** established among the *majority of the nodes*
- There is **no single entity** that receives and responds to the request
- Nodes are connected using Peer-to-Peer (P2P) architecture



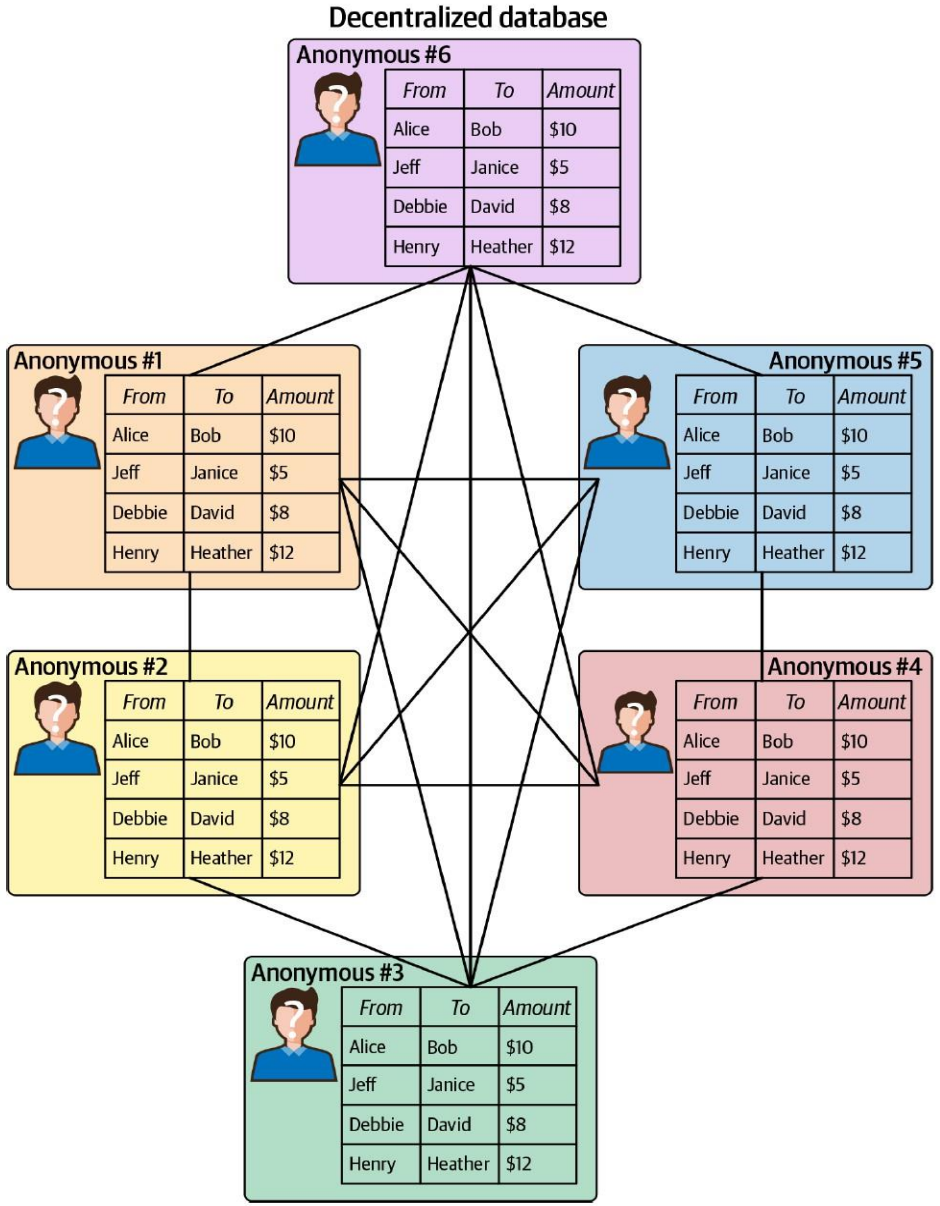
Decentralized
(B)

Decentralized System

Advantages

- **High Availability** – Always there are some nodes which are available/online for work, leading to high availability
- **Improved Fault Tolerance**: Decentralized systems are designed to be fault tolerant, meaning that if one or more nodes fail, the system can still continue to function
- **Increased Transparency:** Decentralized systems often have a transparent and open structure, which allows for greater accountability and trust
- **Higher Autonomy and Control over Resources** – As each node controls its own behavior, it has better autonomy leading to more control over resources.

Decentralized System – An Example

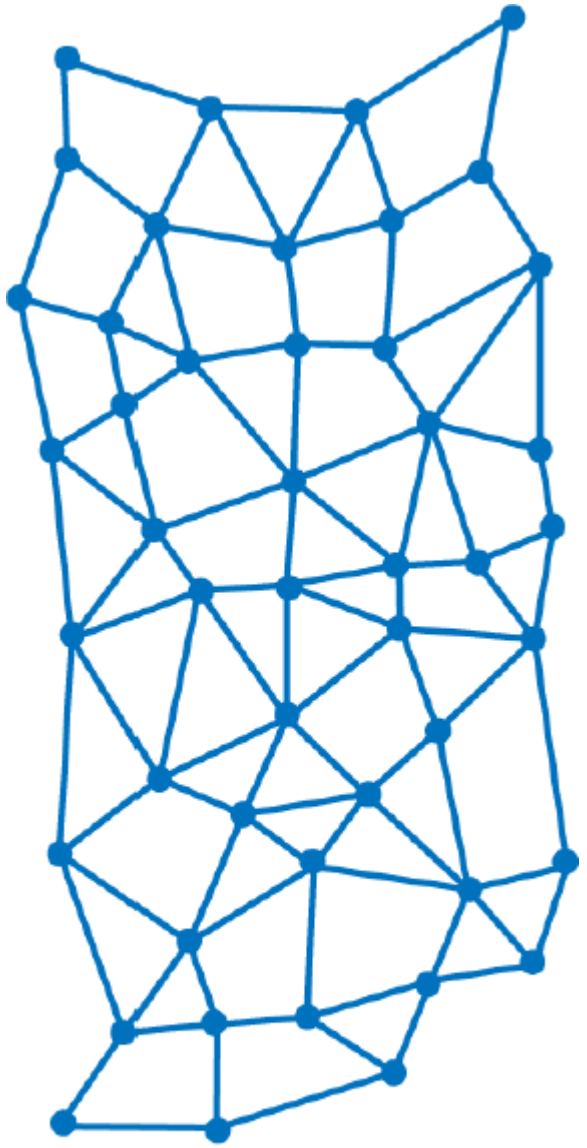


In a decentralized database, like Bitcoin's Blockchain,

- each node can maintain a **replicated** copy of the same data,
- each node may **not** know the identity of other nodes (i.e. **anonymous**), and
- all nodes are ***controlled*** by different entities which are anonymous

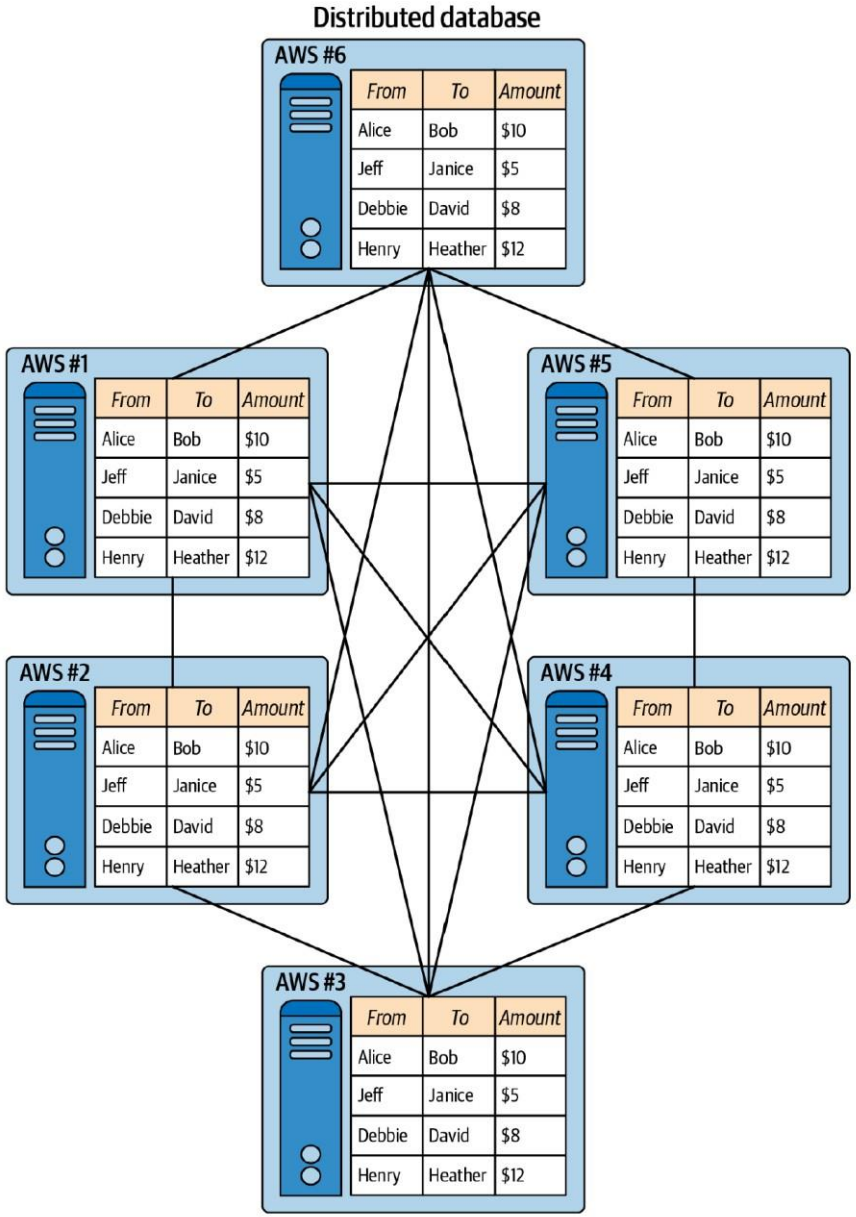
Distributed System

- In the field of computing, a distributed system is one where **computation** is ***shared across*** a number of computing resources
- The **common goal** is to use processing power to collectively accomplish a task by distributing responsibility across many computers
- These systems communicate with one another using some form of ***messaging***
- Synchronization issues: Data consistency and synchronization across all nodes can be a challenge
- Distributed systems require a **complex network infrastructure** to operate, which can be difficult to set up and maintain



Distributed
(C)

Distributed System – An Example



In a distributed database, like multiple databases hosted on Amazon Web Services (AWS),

- each node can maintain a replicated copy of the same data,
- each node **knows** the identity of other nodes (thus not anonymous), and
- all nodes are controlled by **one entity**

Bitcoin Predecessors

DigiCash

- DigiCash company founded by **David Chaum** in 1989
- It facilitated **anonymous online** digital payments
- Chaum is the inventor of **blind signature technology**, which proposed using cryptography to protect the privacy of payments online
- The DigiCash platform had its own currency, known as **cyberbucks**
- At the time of signup users would receive $100 in cyberbucks, which were often referred to as tokens or coins
- The ***company pioneered secure microchipped smart cards***, similar to the system used in most credit cards today
- It was also an early innovator in terms of the concept of a digital wallet for storing value—in this case, cyberbucks.

DigiCash

- Many privacy-conscious users did begin using cyberbucks
- However, it was never able to achieve traction due to lack of merchants, though, and DigiCash ultimately filed for bankruptcy in 1998.

E-Gold

- E-gold was a digital store of value established in 1996, and the digital value was backed by real units of precious metal.
- E-gold was operated by a company called Gold & Silver Reserve
- Everything on the E-gold platform was denominated in units of gold or other precious metals.
- E-gold enabled instant transfers between its users on the internet.
- With denominations as small as **one ten-thousandth of a gram of gold**, the platform was the first to introduce the concept of making micropayments, on the internet.
- Innovative for the time, E-gold also offered **developers** an **API** that allowed others to **create additional services** on top of the platform.
- Merchants accepted E-gold as a form of payment alongside credit cards in online shopping carts.

E-Gold

- By 2006 there were over 3.5 million E-gold accounts. At that time, the company was processing $5.9 million in daily volume.
- As a centralized system, E-gold had no mechanism to tie accounts to anyone's identity.
- The platform was being used for nefarious purposes, facilitating money laundering, online scams, and other illegal activity.
- The US government shut down E-gold in 2008, seizing its assets and establishing a system of redemption for account holders.

Hashcash

- Hashcash was invented by Adam Back in 1997
- It was designed to mitigate the problem of Email spam and denial-of-service attack
- Hashcash is a cryptographic hash-based proof-of-work algorithm that requires sender to produce some kind of verifiable computational output
- However, it takes for receiver negligible effort to verify the work of the sender
- Before sending an email, hashcash stamp is added to the header of an email to prove the sender has expended a modest amount of CPU time calculating the stamp
- The receiver can, at negligible computational cost, verify that the stamp is valid.

Hashcash

- In general, the spammers want to send large numbers of emails with very little cost per email
- Now with hashcash if there is even a small cost for each spam they send then they will cease to be profitable
- Receivers can verify whether a sender made such an investment and use the results to help filter email.
- For hashing, Hashcash used SHA1 algorithm

B-Money

- B-Money was proposed by Wei Dai in 1998
- B-Money introduced the concept of using computer science to create money outside the governmental systems.
- B-Money advanced the idea of broadcasting transactions to a network.
  - For example, if one party wanted to pay another, a message would be sent to the network saying, “Person 1 will send $X to Person 2.”
  - The system would be enforceable via a system of digital contracts.
- This system would use cryptography instead of a centralized system for both payments and the enforcement of contractual issues,
  - enabling users of the network to be anonymous; no identity would be required.

B-Money

- There are many concepts put forward by B-Money
  - Idea of contracts to provide order to an anonymous and distributed system
  - The concept of using proof-of-work to create money
- B-Money was mostly just a theoretical exercise by Wei; it was not implemented

Bit Gold

- Bit gold was proposed in 2005 by computer scientist Nick Szabo
- Bit gold was never implemented, but has been called "***a direct precursor***" to the Bitcoin architecture
- Nick's idea came after the advent of E-gold, which used gold to back digital value.
- Szabo pointed out that materials such as gold have **value** and are "**unforgeable**," or very difficult to **counterfeit** due to their rarity and fixed costs such as mining and transportation.
- In bit gold, a **participant** would dedicate computer power for solving cryptographic puzzles
- In a bit gold network, solved puzzles would be sent to the **Byzantine fault-tolerant public registry** and assigned to the **public key of the solver**.
- Each solution would become part of the next challenge, creating a growing chain of new property.
- This provided a way for the **network** to **verify** and **time-stamp** new coins, because unless a majority of the parties agreed to accept new solutions, they couldn't start on the next puzzle

Bitcoin Experiment

Bitcoin Experiment

- By 2008, the world was already relying on the **internet** as a **distributed entity** for a **large number of services** such as Email, Skype, GPS, and WhatsApp
- In addition, e-commerce and m-commerce started in full swing
  - Buying and selling of goods online and with e-payments
- Then, the **2008 financial crisis** happened
  - This recession period was big shock because financial system was **still centralized** and thus lacks transparency
- On 18 August 2008 the domain bitcoin.org was registered
- Then, on 31 Oct 2008 the paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" was published by pseudonym pseudonym **Satoshi Nakamoto**
- The aim was to create a **digital currency** that could operate **without** any connection to a bank or central government

Bitcoin Experiment – Building by Taking Ideas From Predecessors

Bitcoin took number of ideas and techniques from its **predecessors**

- From **DigiCash** → Use of cryptography to secure transactions
- From **E-gold** → Ability to send small amounts of secured value
- From **B-Money** → The creation of money outside of governmental systems
- From **Hashcash** → Use of proof-of-work to verify validity of digital funds

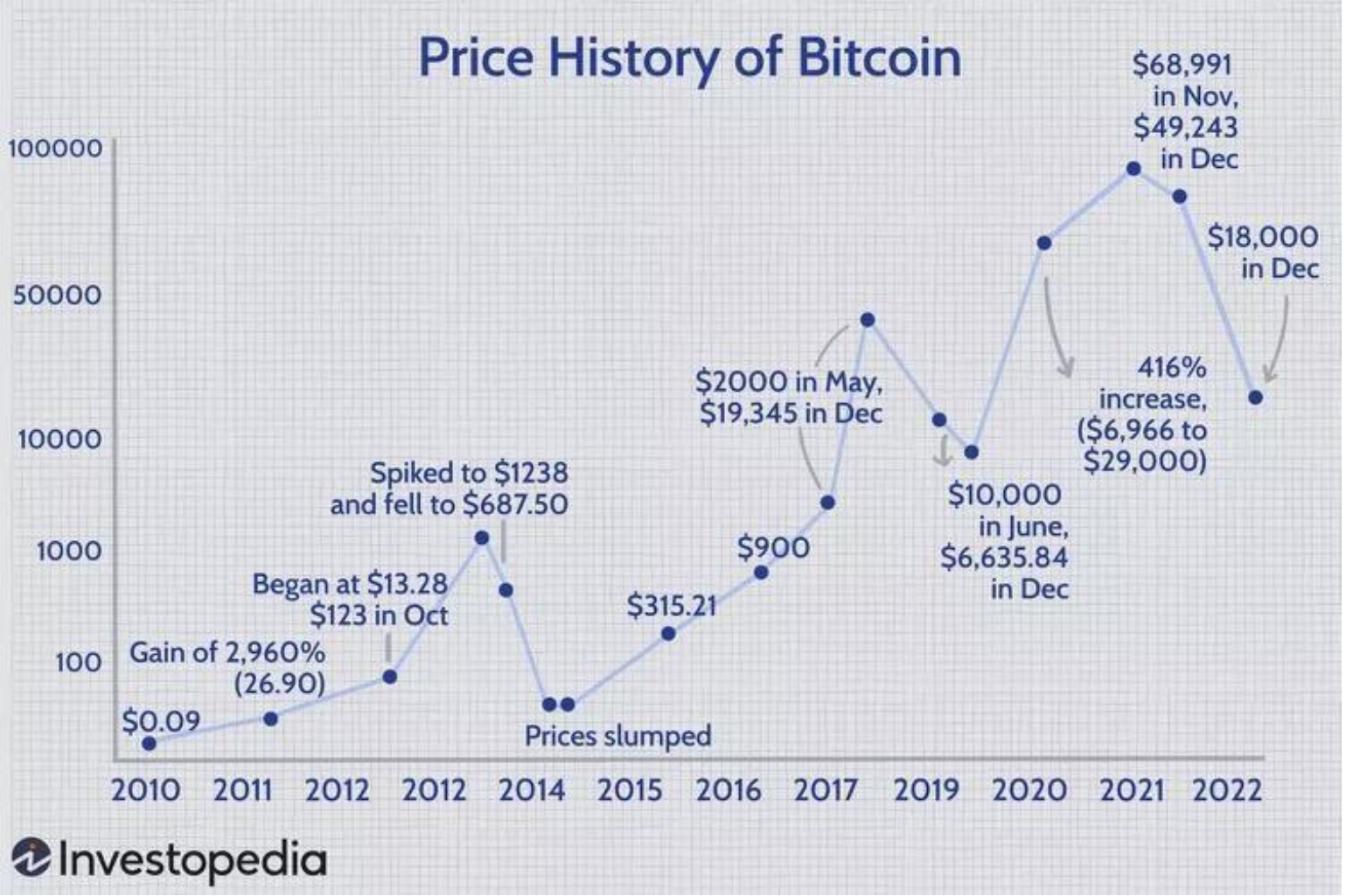
Bitcoin – The Cryptocurrency

- Bitcoin is first cryptocurrency (aka crypto)
- It is digital virtual currency with no central control of government
- Created by ***Satoshi Nakamoto*** in year 2008
- First bitcoin transaction took place in 2009 when ***Hal Finney*** received 10 BTC from Satoshi
- Its implementation is available as open source

Bitcoin – The First Commercial Transaction

- First retail transaction happened in 2010 when *two pizzas* were bought for ***10,000*** *BTC*
- Bought by ***Laszlo*** and paid to ***Jeremy*** who is reported to be 19 year old then
- This data is celebrated as **Bitcoin Pizza Day** by the Bitcoin community
- **Source**: Business Today News dated 17 June, 2022 https://www.businesstoday.in/crypto/story/two-pizzas-for-rs-2260-crores-12-years-of-the-bitcoin-pizza-day-334204-2022-05-19

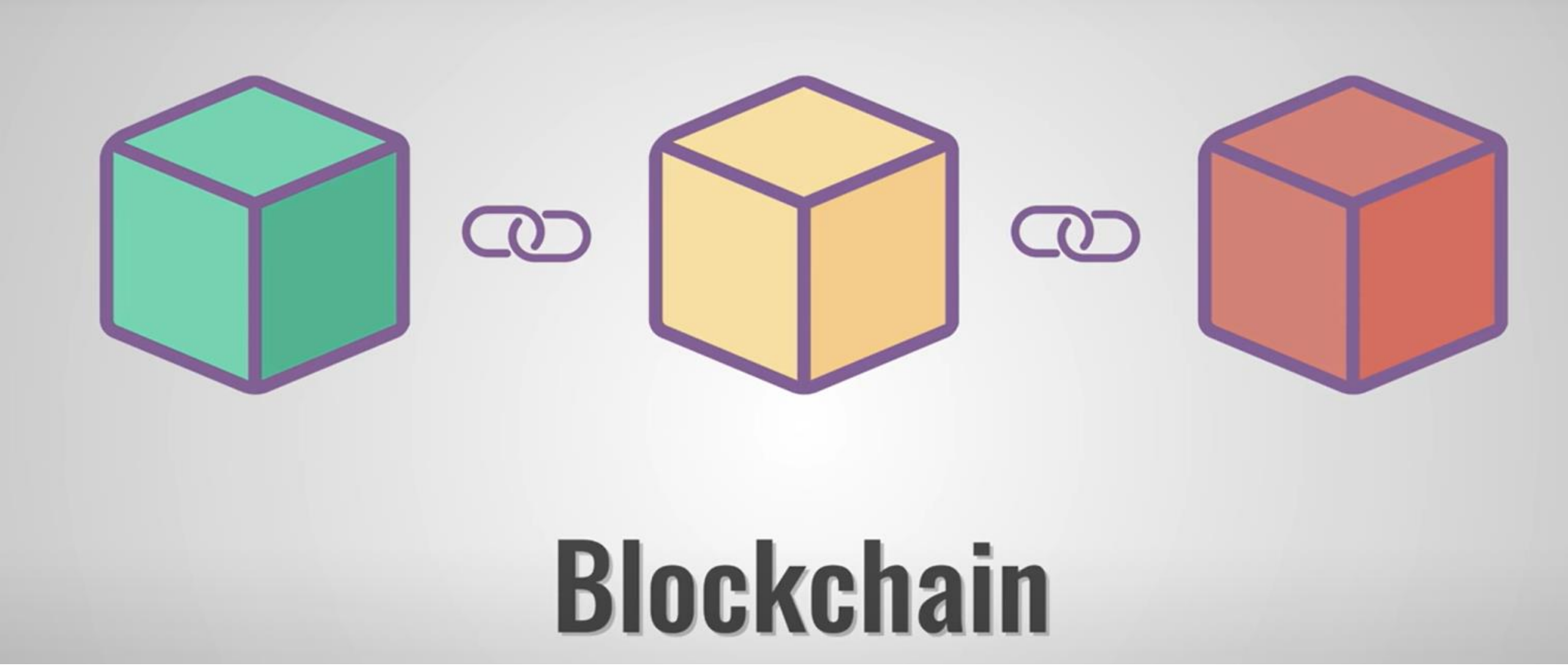
Bitcoin – The First Commercial Transaction



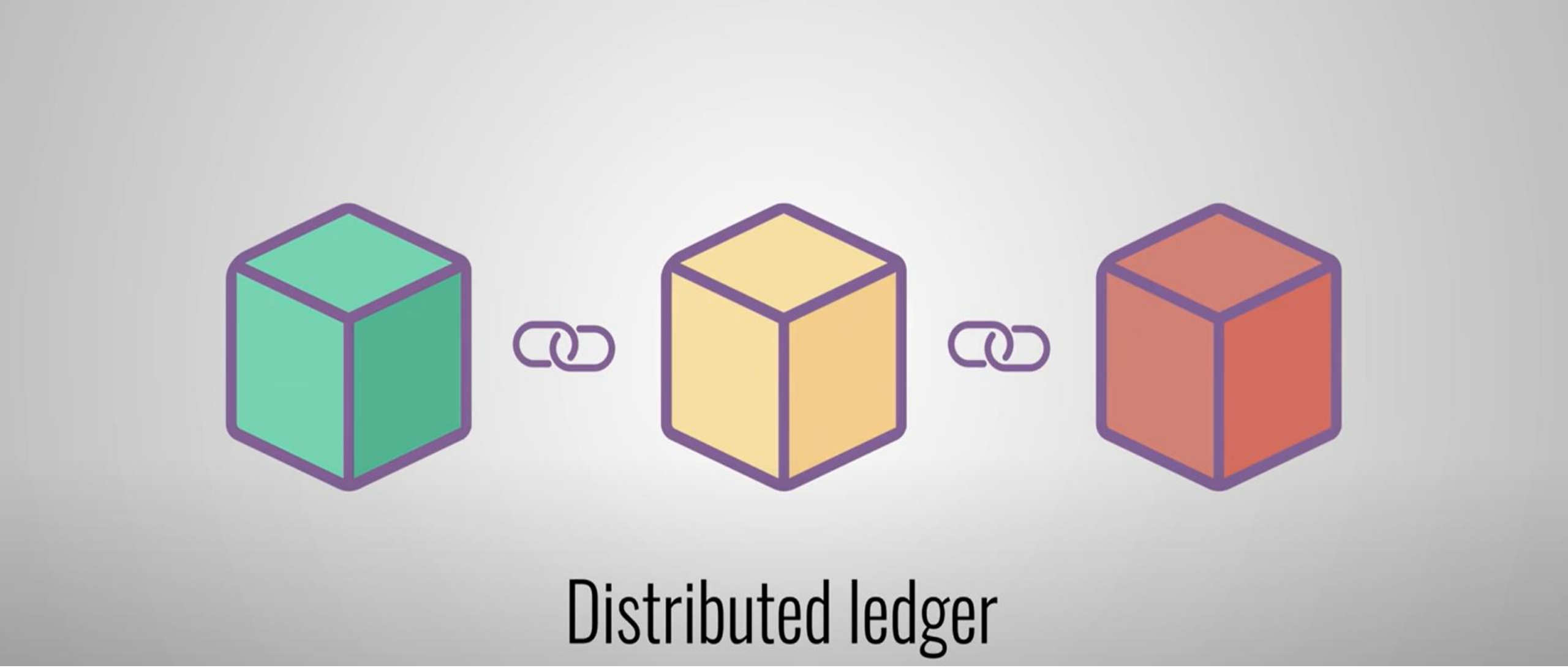
- **Source**: By John Edwards Updated April 05, 2023, Reviewed by Julius Mansa, Fact checked by Suzanne Kvilhaug, at Investopedia https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp

- Value as of today in INR is 23,71,554.99

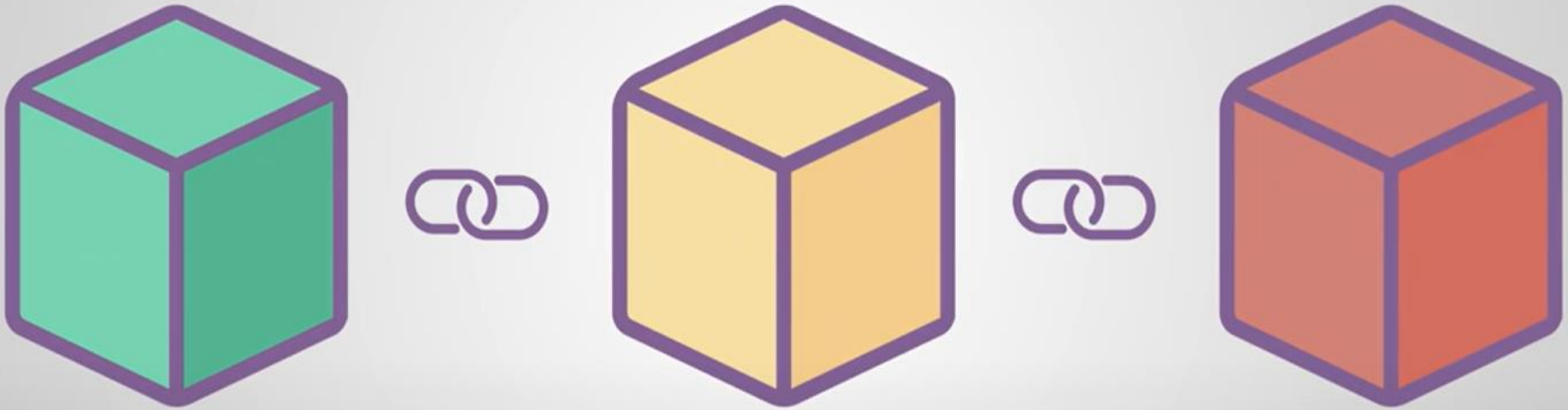
What is Blockchain?



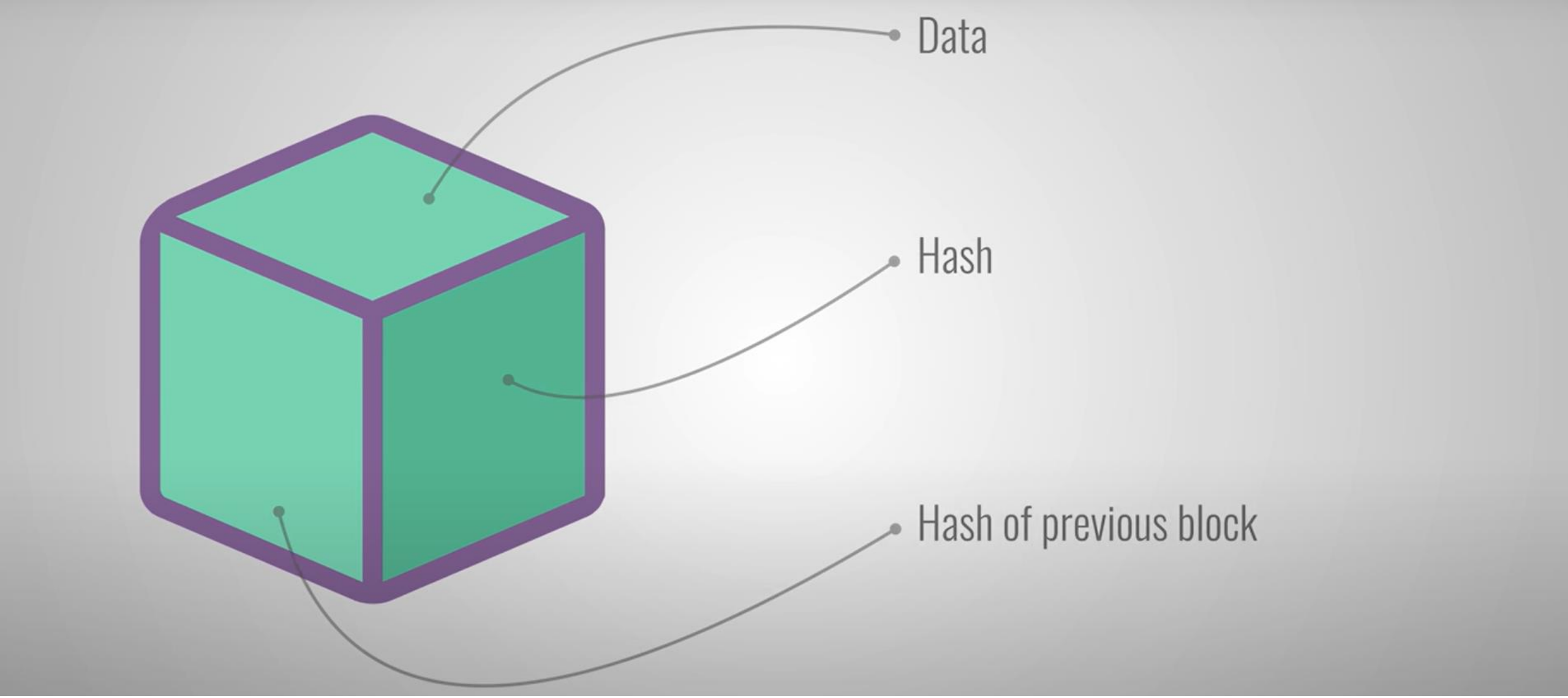
A **blockchain** is a chain of blocks that contains information.



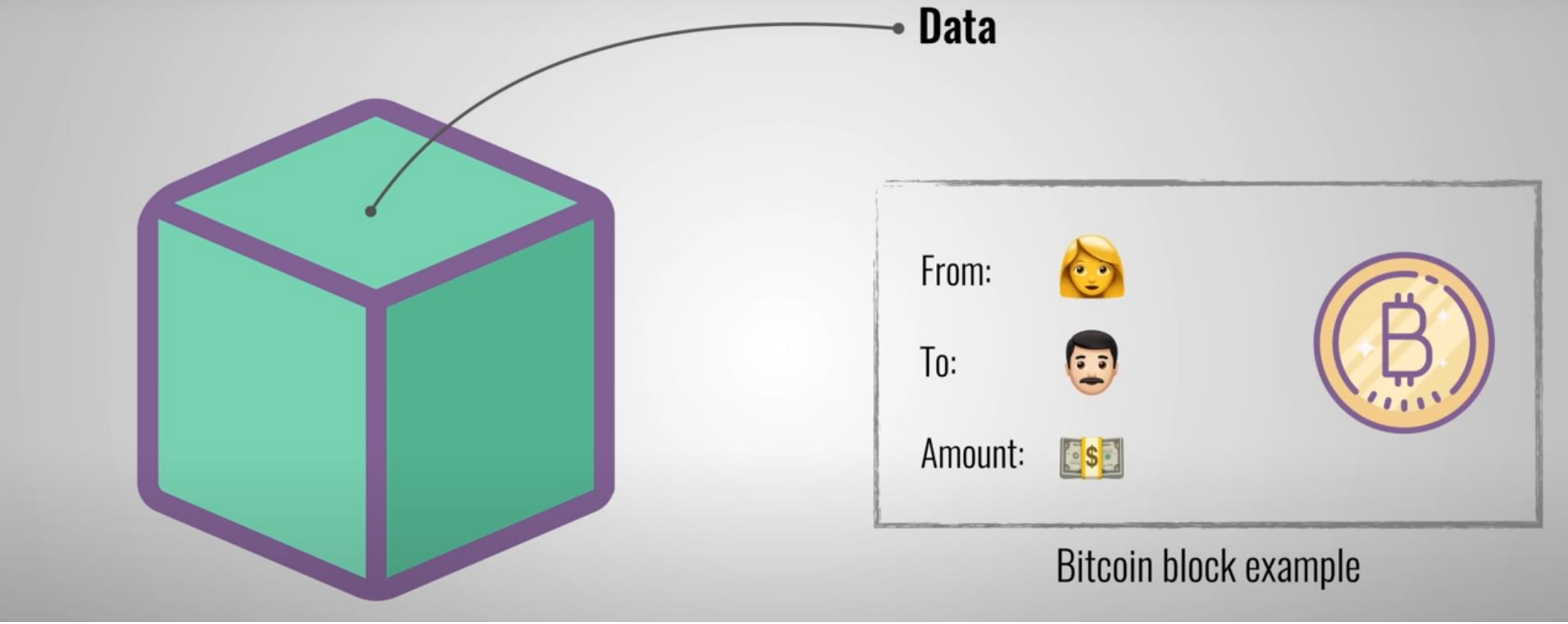
A **blockchain** is a distributed ledger that is completely open to everyone.



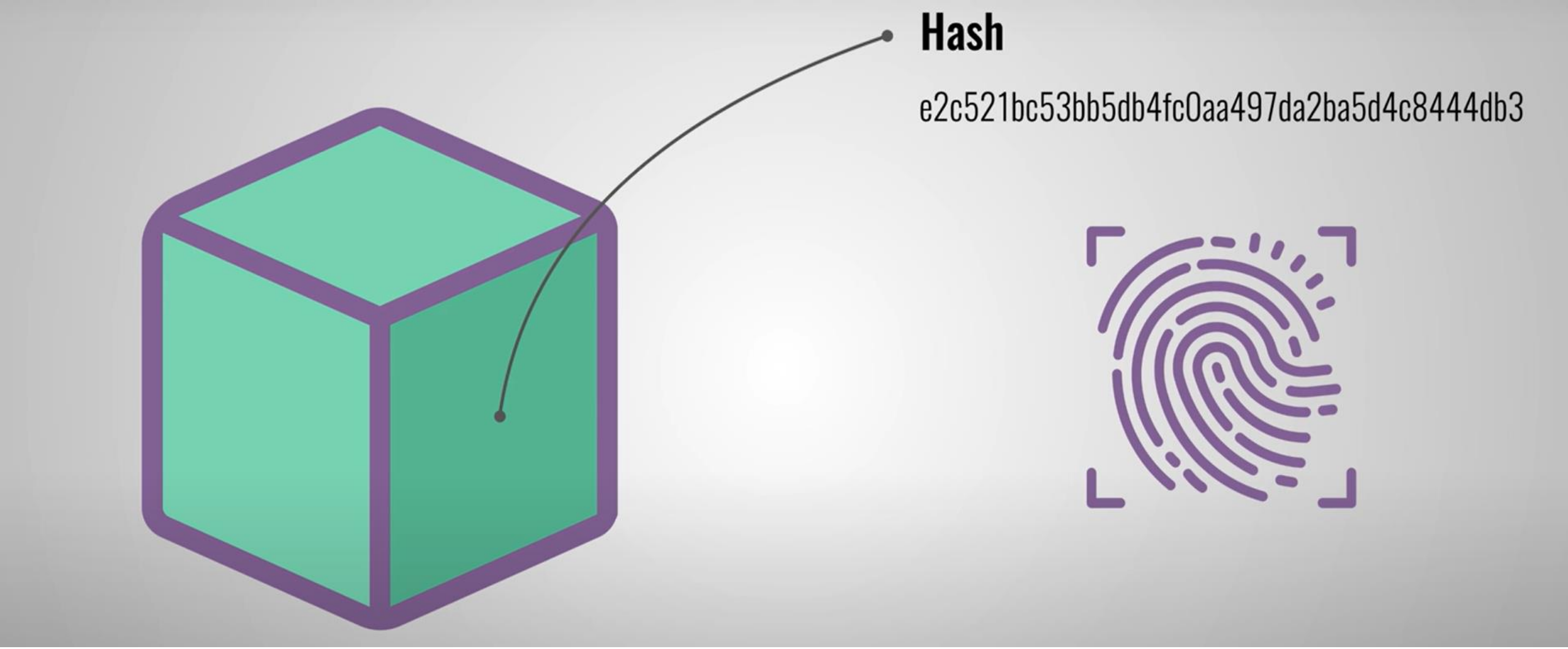
In distributed ledger once the data has been added/recorded inside the blockchain it becomes very difficult to change it.



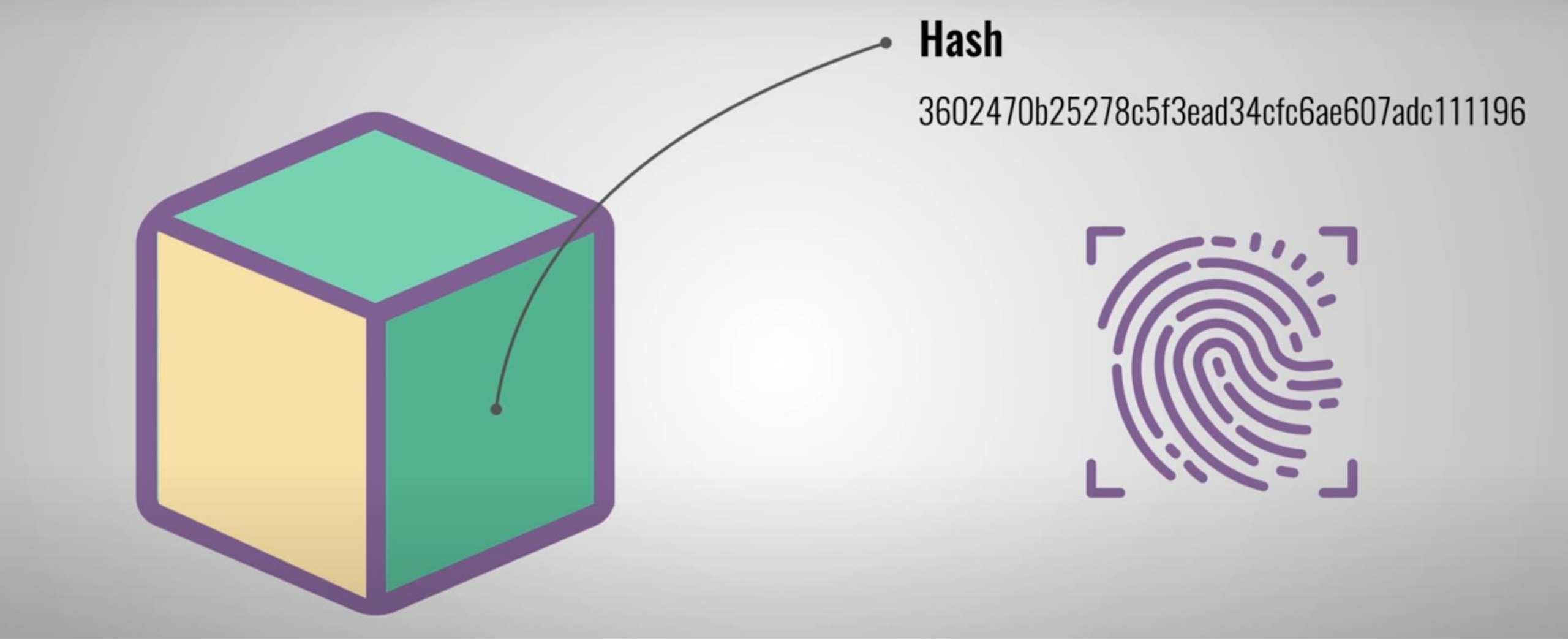
Block contains data, hash of the block and hash of the previous block



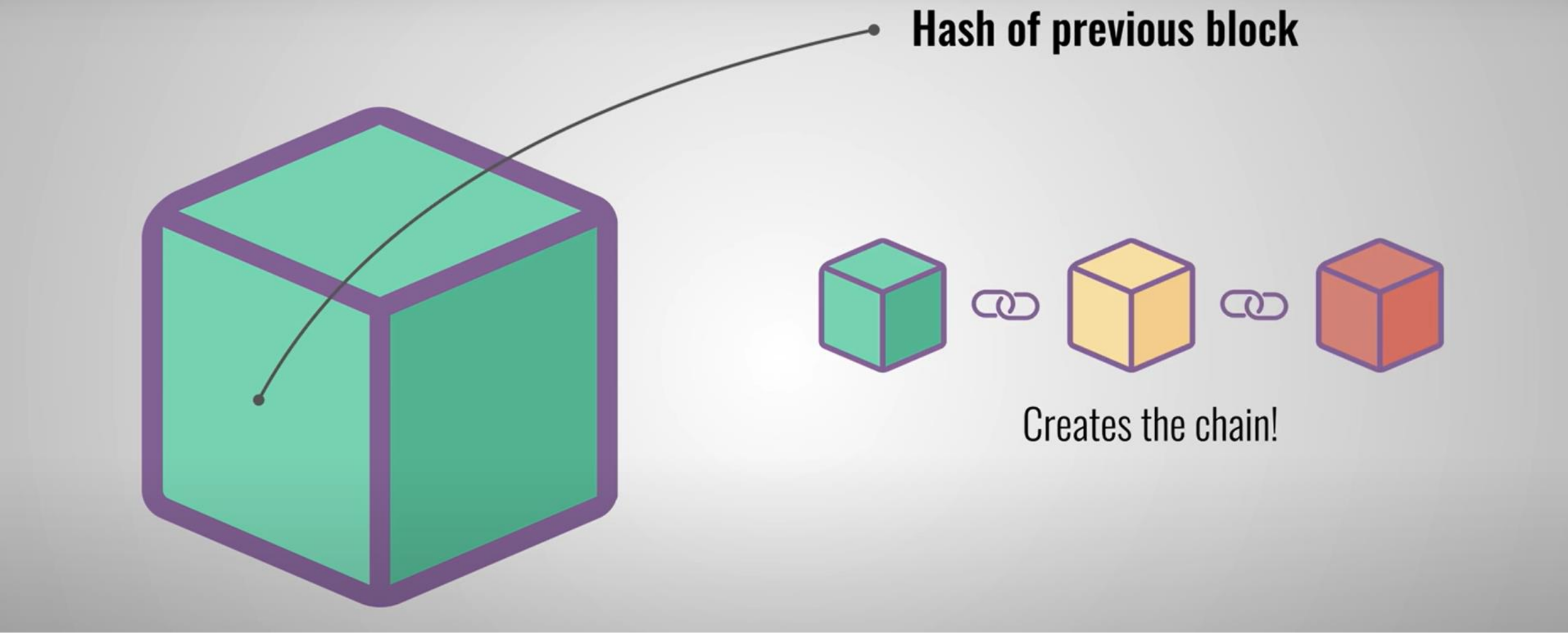
In a **bitcoin blockchain,** data stores the details like sender, receiver and amount of coins.



Once the block is created, the hash is being calculated.

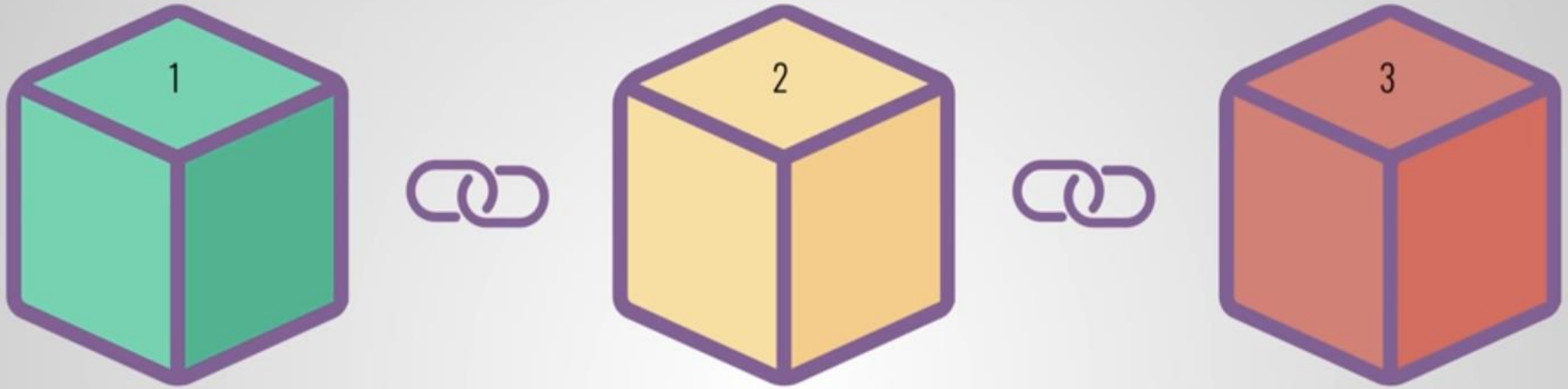


Once the block is created, the hash is being calculated.
Changing something inside the block will change the hash.
Hashes are important to detect changes to blocks.

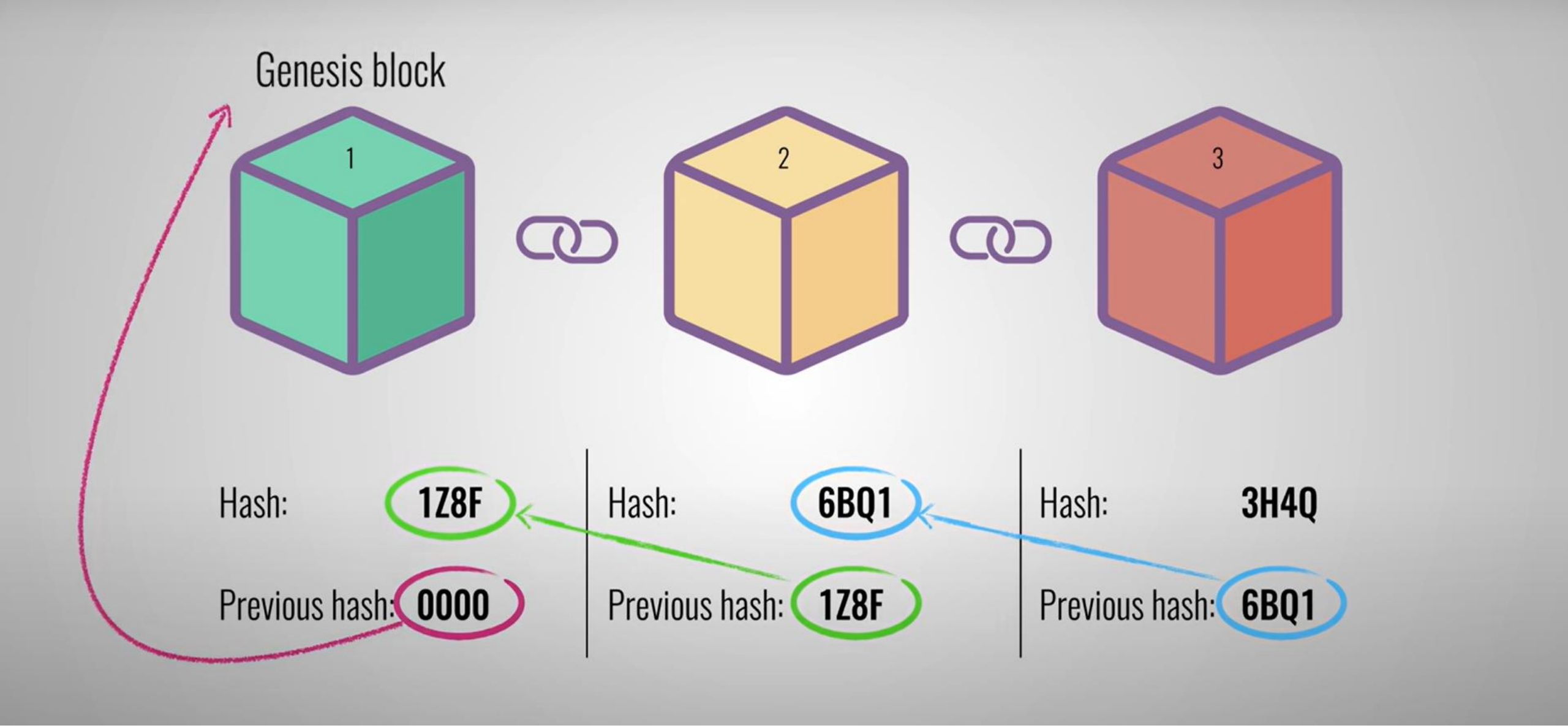


Hash of previous block in every block creates chain of blocks.

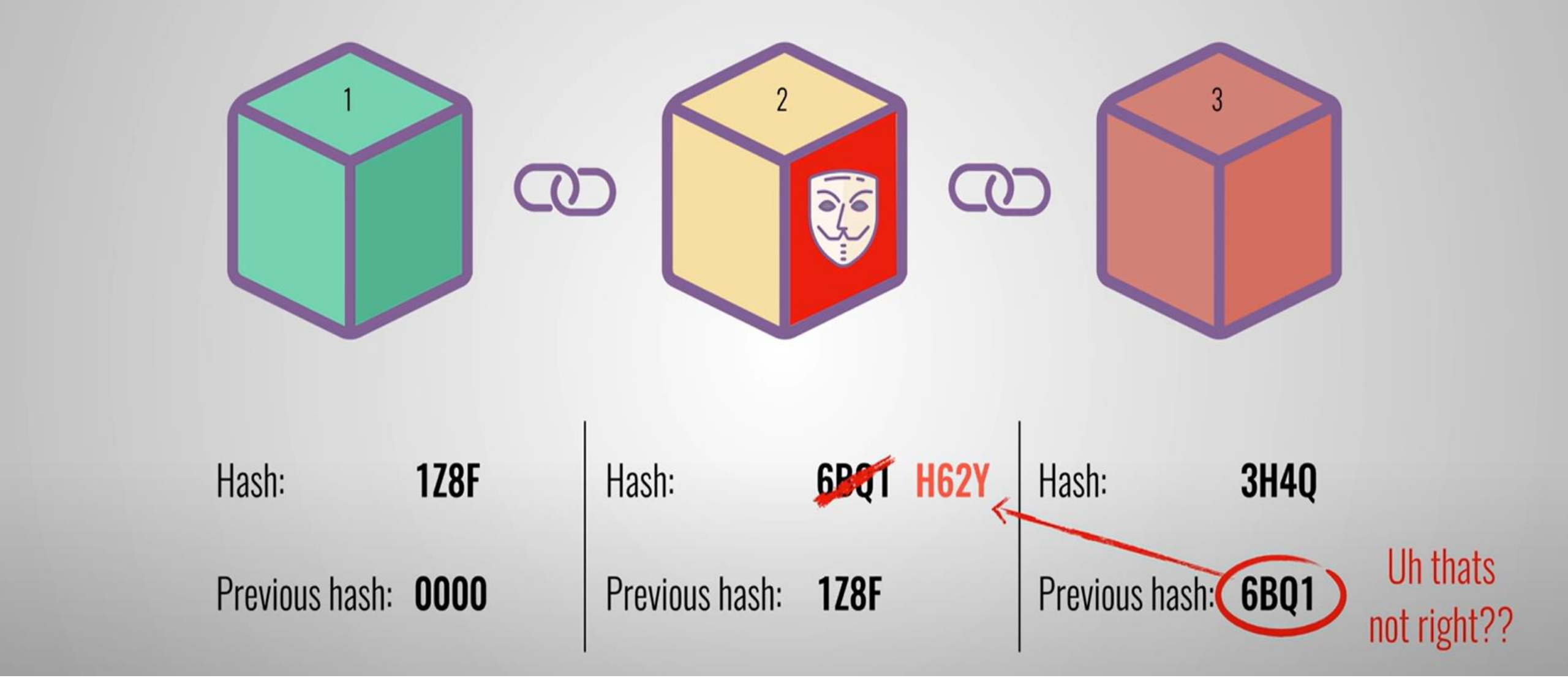
Is the Reason why blockchain is secure.



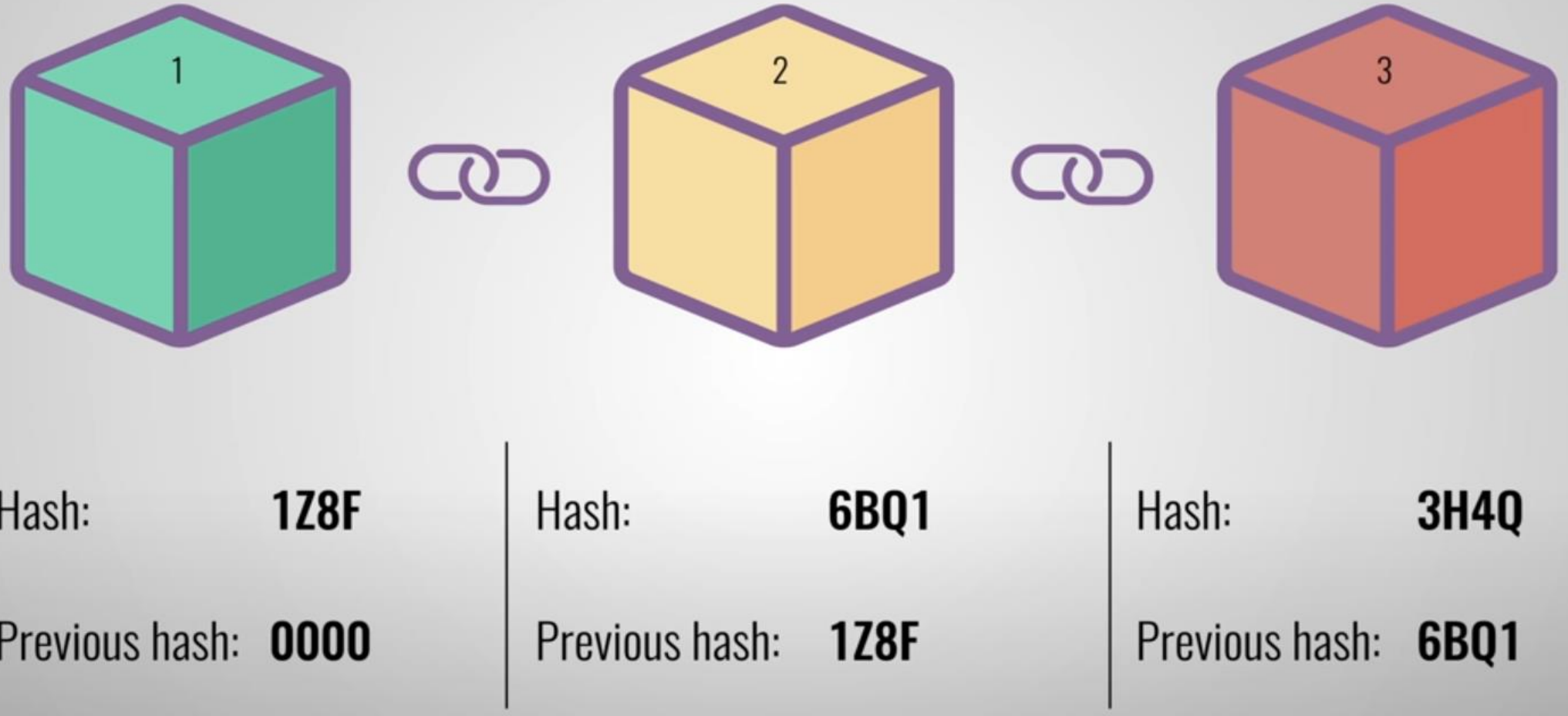
Hash:	**1Z8F**	Hash:	**6BQ1**	Hash:	**3H4Q**
Previous hash:	**0000**	Previous hash:	**1Z8F**	Previous hash:	**6BQ1**



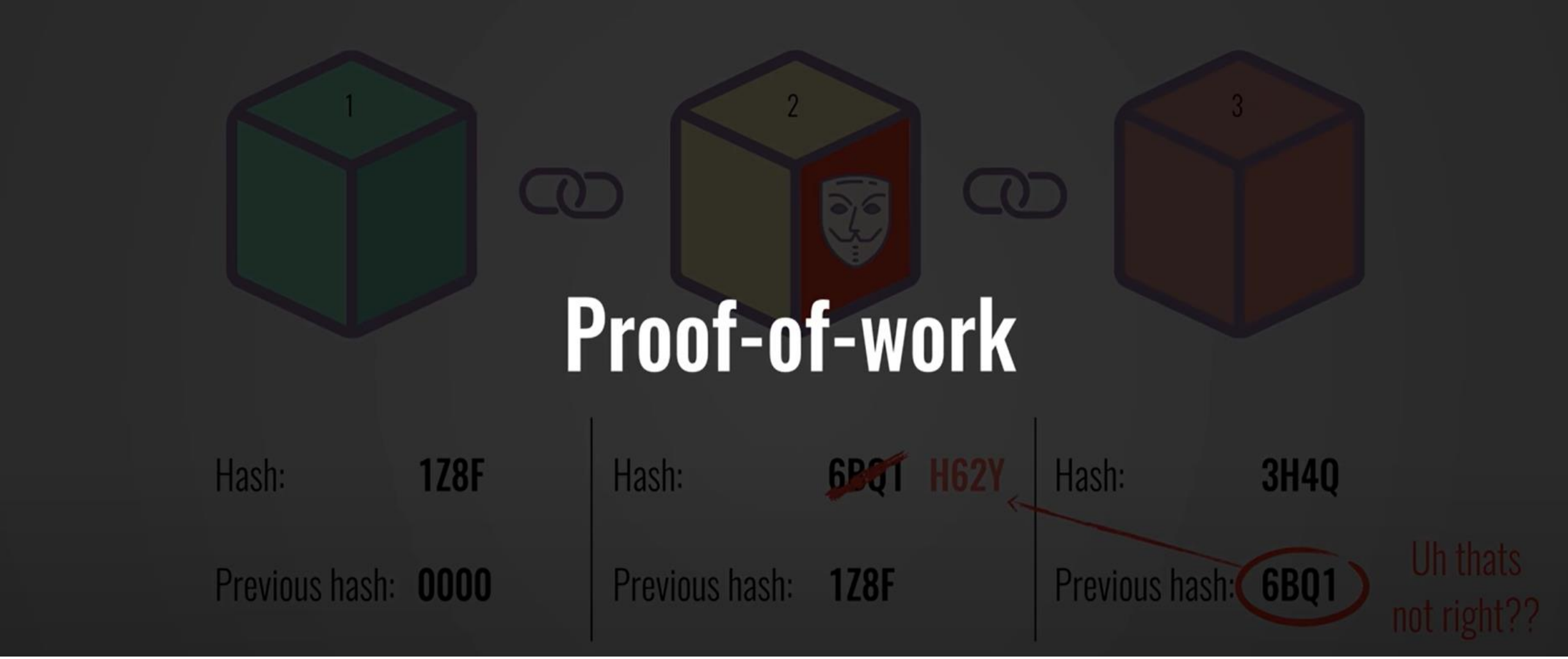
Genesis block is a first block of the blockchain.



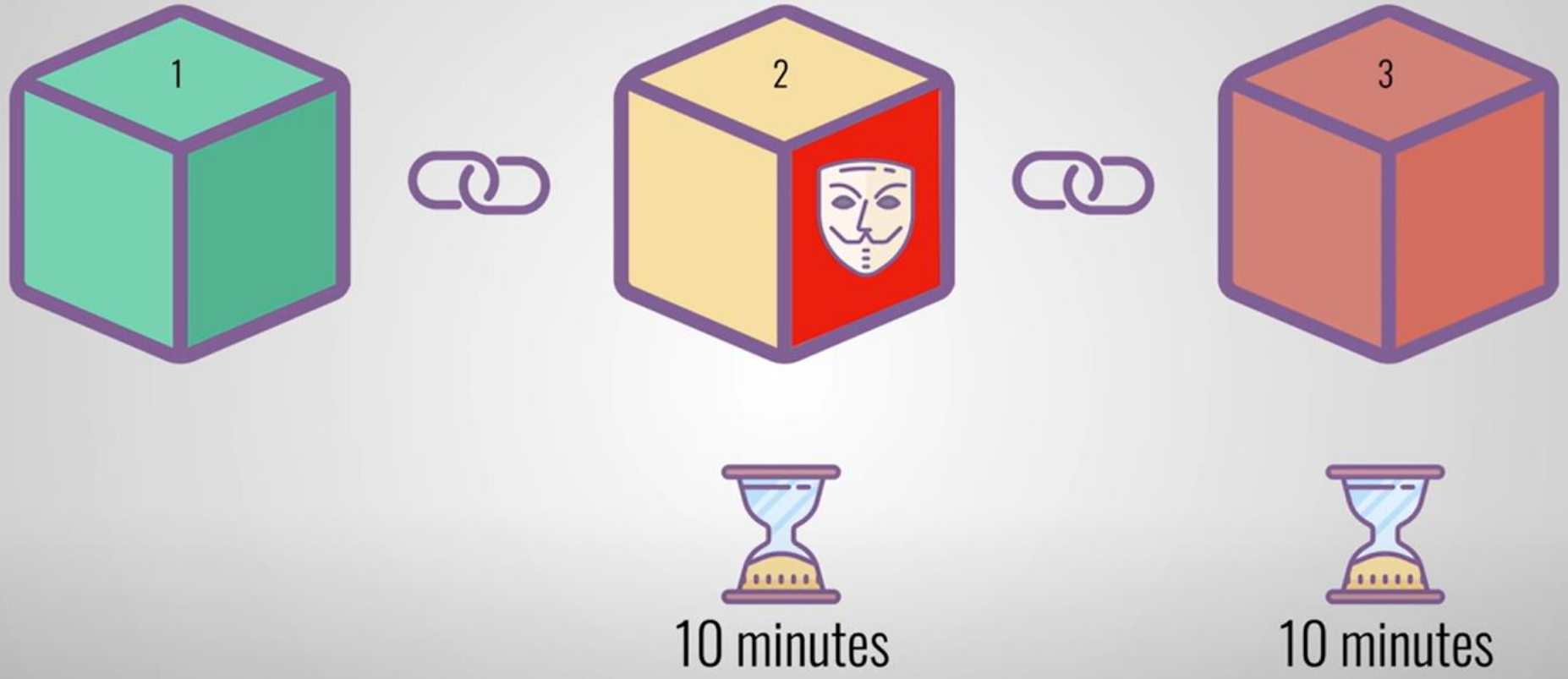
Changing a single block will make all its following blocks invalid.



Only hashes are not sufficient to secure blockchain. Computers now a days can calculate thousands of hashes per second may lead to a tempering of a block in blockchain.

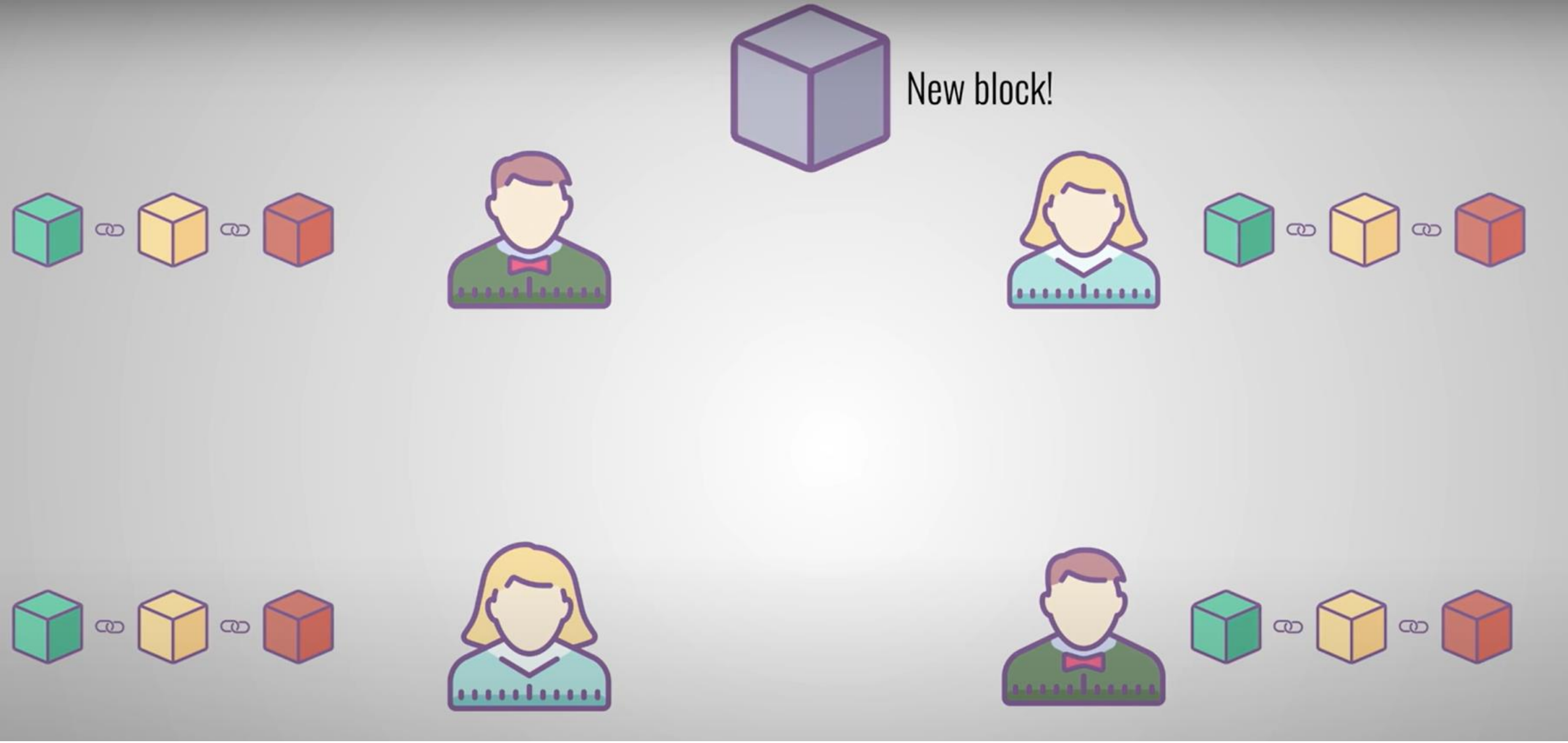


To prevent blockchain from such attacks, there is a concept of proof-of-work.

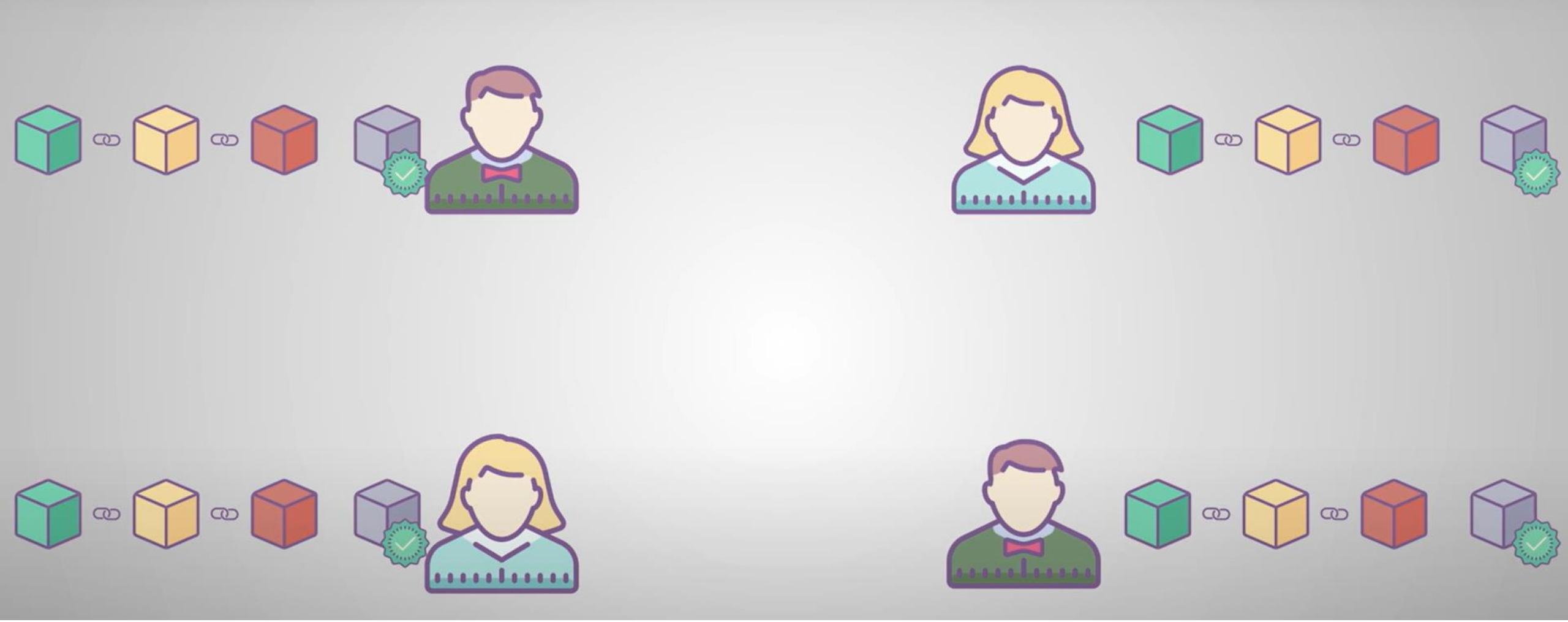


Proof of work (PoW) is a decentralized consensus mechanism that requires network members to expend effort in solving an encryption puzzle.

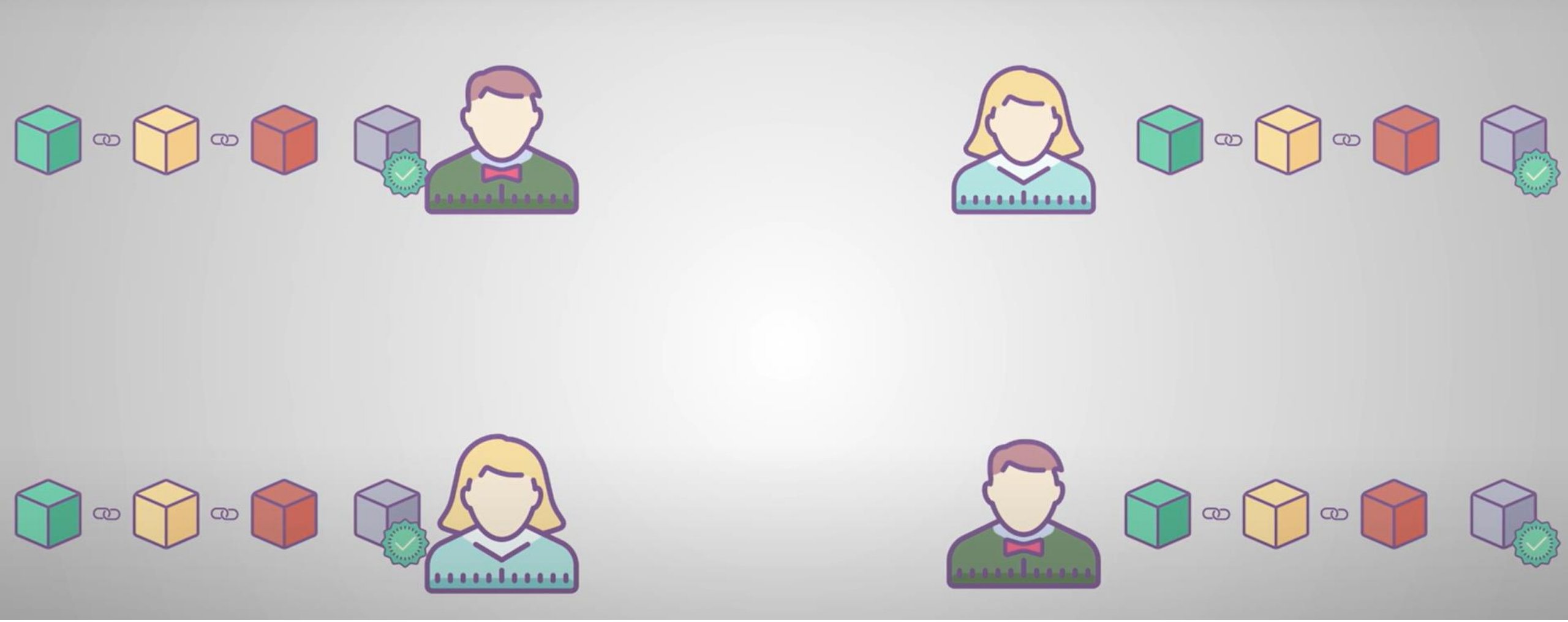
Proof of work is also called mining, in reference to receiving a reward for work done.



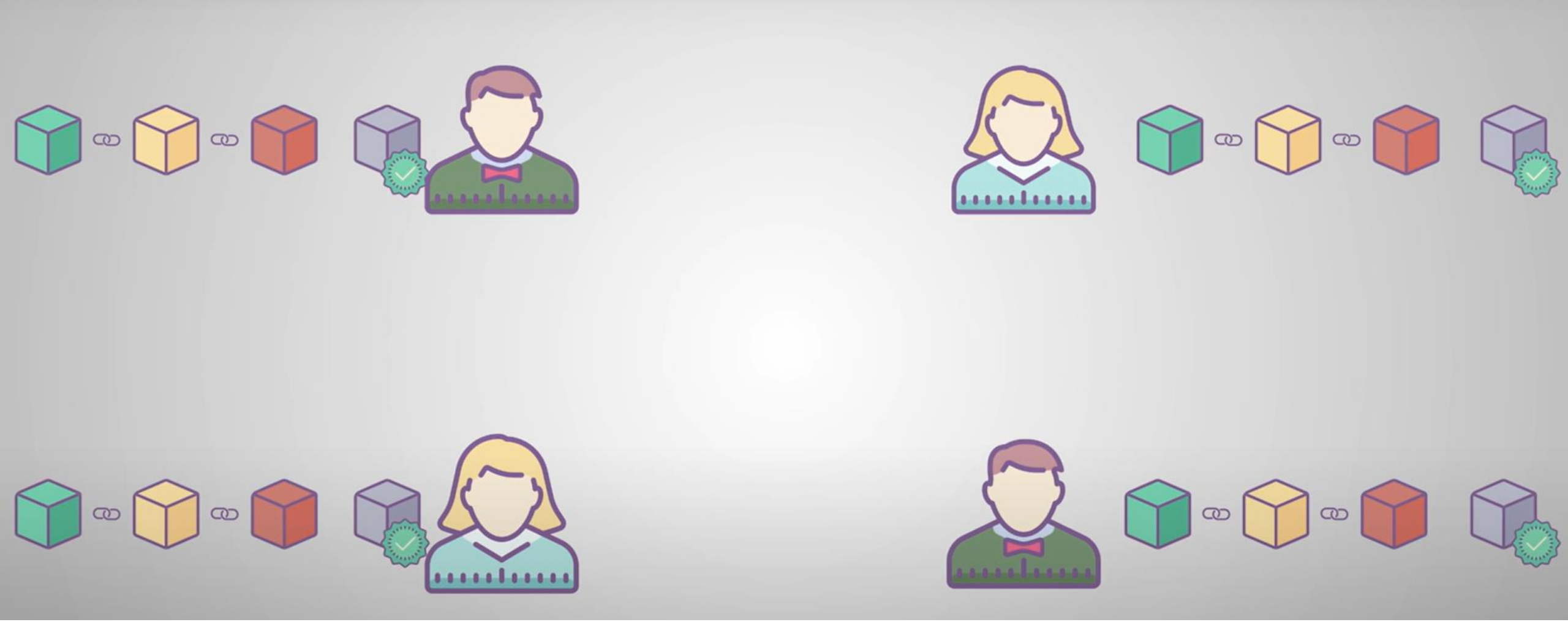
Peer-to-peer network



Each peer then verifies that new block, and after verification that new block been added to their blockchain.
This way consensus has been achieved in the network.



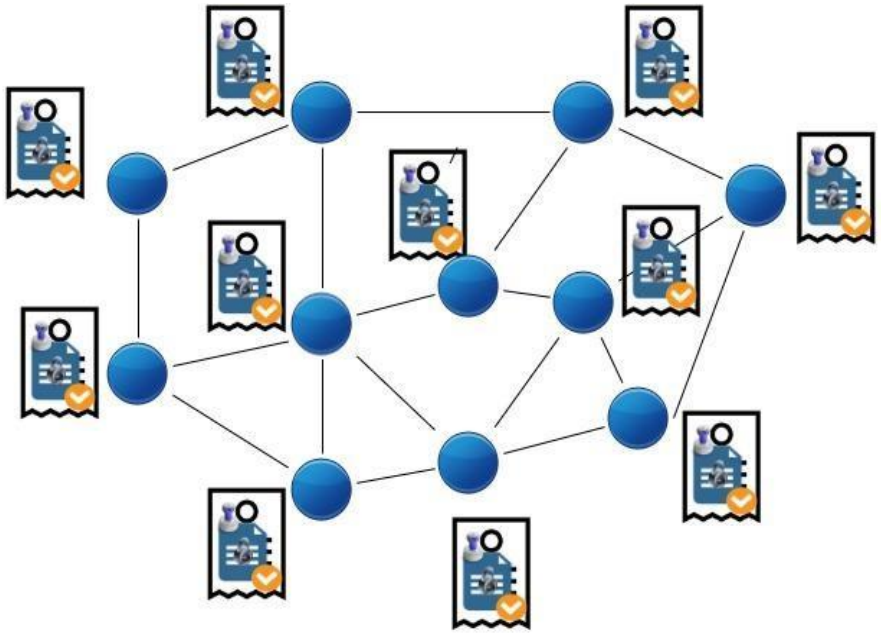
Through consensus they agreed that which blocks are valid. Blocks that are tempered will be rejected by other nodes in the network.



So to change a block one need to change all blocks on the chain, redo the proof-of-work for each block and take control of more than 50% peer-to-peer network.

Security of Blockchain

- ✓ Hash
- ✓ Proof-of-work
- ✓ Peer-to-peer network



Distributed Ledger Technology (DLT)

- Definition by **Financial Conduct Authority (FCA)**, UK:

  > "A set of technological solutions that enables a single, sequenced, standardised and cryptographically-secured record of activity to be safely distributed to, and acted upon by, a network of varied participants."

- Digital ledger that is distributed across all the nodes in a decentralized P2P network
- The ledger is
  - Immutable (unable to change)
  - Shared
  - Synchronized
  - Cryptographically sealed and secure

Source: Discussion Paper on Distributed Ledger Technology, 2017 https://www.fca.org.uk/publication/discussion/dp17-03.pdf

Terminologies:

- ✓ Hash: A variable-length input or data is converted to secure fixed-length output. (irreversible)
- ✓ Ledger: Ledger is a collection of all the transactions occurred in the past.
- ✓ Distributed Ledger Technology(DLT): Distributed ledger technology is a decentralized ledger network that uses the resources of many nodes to ensure data security and transparency.
- ✓ Block: A block containing set of valid transactions is created after every unit of time
- ✓ Proof-of-work: Proof of work (PoW) is a decentralized consensus mechanism that requires network members to expend effort in solving an encryption puzzle.

Terminologies:

- ✓ Peer-to-peer network: A peer-to-peer (P2P) network is based on the concept of decentralization, which allows the participants to conduct transactions without needing a central server.
- ✓ Consensus mechanism: A consensus mechanism is a protocol that brings all nodes of a distributed blockchain network into agreement on a single data set.

- ✓ Blockchain is a blend of the following technologies:

  Public key cryptography
  Hash algorithms
  Digital Signatures
  Merkle trees
  Peer-to-Peer networks
  Consensus mechanisms

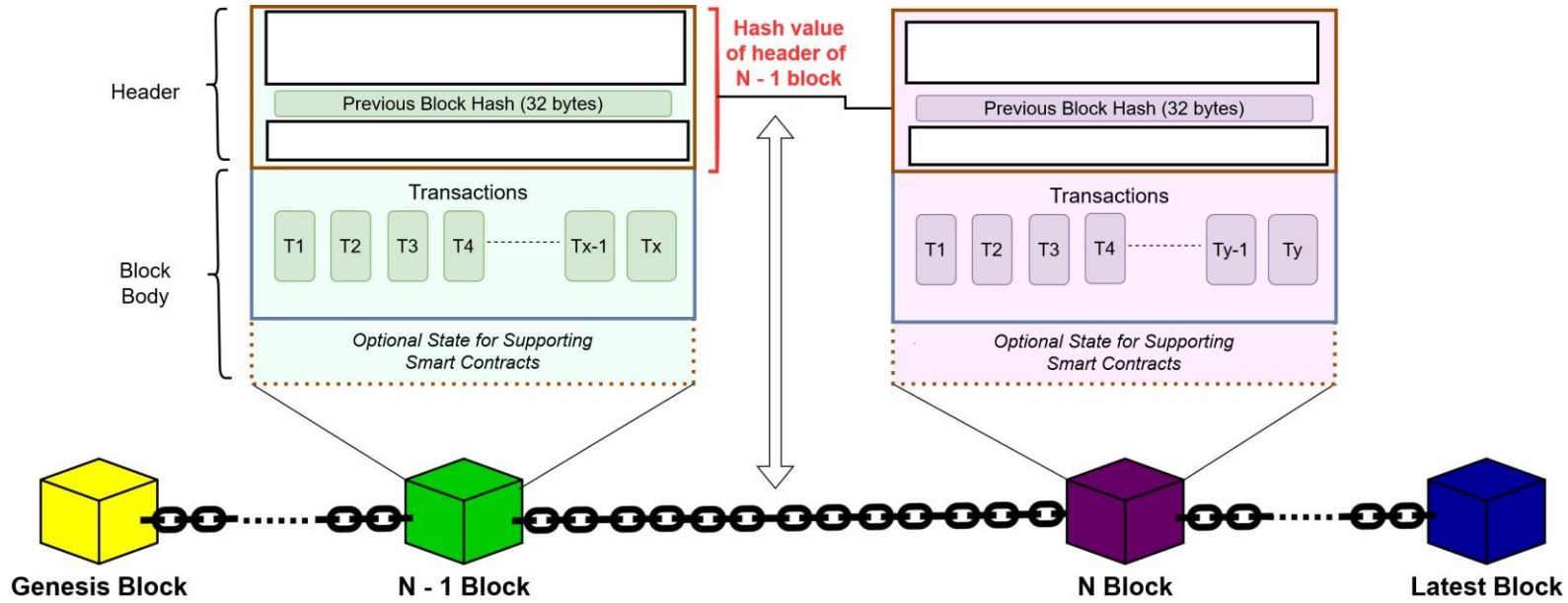
Storing Data In Chain of Blocks

- Bitcoin blockchain introduced the concept of **tracking transactions** using a **chain of cryptographic hashes**
- A **block** containing set of valid transactions is created after every unit of time (or time frame)
- A **newly created block** is logically connected with the most recent block using a cryptographic **hash-based chain**
- Thus, as the blocks are created with time, they are organized **in chronological order**
- The blockchain ledger (or database) is distributed among all the nodes in the blockchain network
- Thus, blockchain **does not** require any single entity to keep track of transactions
- Instead, the chain of blocks, or blockchain, uses cryptographic mathematical trust to keep track of transactions in a decentralized digital system

New Concepts & Terminologies

Block Hash

- A block hash is computed by **hashing** the **block header**
- Thus, it is a **unique identifier** of each block
- Every block stores the block hash value of previous block
- Thus, in Bitcoin block does not contain its own block hash, but it does contain the hash of the previous block it is building on
  - Hence the name blockchain → blocks are chained with a hash-based cryptographic chain
- The block hash is generated from input data that provides a **snapshot** of the **current state** of the blockchain within 256 bits of data.



New Concepts & Terminologies

Coinbase Transaction

- This is the first transaction of each new block mined on the network.
- It adds new bitcoin to the supply, which is given as a reward to the miner who adds the block to the chain

https://www.youtube.com/watch?v=MwyXYDXNvMY

Block Height Number

- This number identifies how many blocks there are between the current block and the first block in the chain (also known as the Genesis block).

Nonce

- Nonce is number used once.
- It is a random number which is used in conjunction with the other fields in the block header to compute the hash of block's header which matches the target range.

Block #170

Summary	
Number Of Transactions	2
Output Total	100 BTC
Estimated Transaction Volume	10 BTC
Transaction Fees	0.00 BTC
Height	170 (Main Chain)
Timestamp	2009-01-12 03:30:25
Received Time	2009-01-12 03:30:25
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.49 kB
Weight	1.716 kWU
Version	1
Nonce	1889418792
Block Reward	50 BTC

Hashes	
Hash	00000000d1145790a8694403d4063f323d499e655c83426834d4ce2f8dd4a2ee
Previous Block	000000002a22cfee1f2c846adbd12b3e183d4f97683f85dad08a79780a84bd55
Next Block(s)	00000000c9ec538cab7f38af9c67a95742f56ab07b0a37c5ba6b02808dbfb4e0
Merkle Root	7dac2c5666815c17a3b36427de37bb9d2e2c5ccec3f8633eb91a4205cb4c10ff

Transactions

b1fea52486ce0c62bb442b530a3f0132b826c74e473d1f2c220bfa78111c5082 **(Size: 134 bytes) 2009-01-12 03:30:25**

No Inputs (Newly Generated Coins)	1PSSGeFHDnKNxiEyFrD1wcEaHr9hrQDDWc - (Unspent)	50 BTC
		50 BTC

f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16 **(Fee: 0.00 BTC - Size: 275 bytes) 2009-01-12 03:30:25**

12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S (50 BTC - Output)	1Q2TWHE3GMdB6BZKafqwxXtWAWgFt5Jvm3 - (Spent)	10 BTC
	12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S - (Spent)	40 BTC
		50 BTC

New Concepts & Terminologies

Double Spending

- The risk that a unit of currency is spent more than once via falsified duplication.

Blockchain technology prevents double-spending through peer-to-peer file-sharing technology combined with public-key cryptography.

Merkle Root:

This is a hash that allows proof of the validity of the blockchain.

How transactions are verified in blockchain:

https://www.youtube.com/watch?v=6yIqXMaeEJ4

What is Double Spending

and why is it such a problem?

Alice

Without exception, all Bitcoin transactions are included in a block of transactions.
Each block has a timestamp with encoded information that makes it more difficult to manipulate the blockchain.

Katy

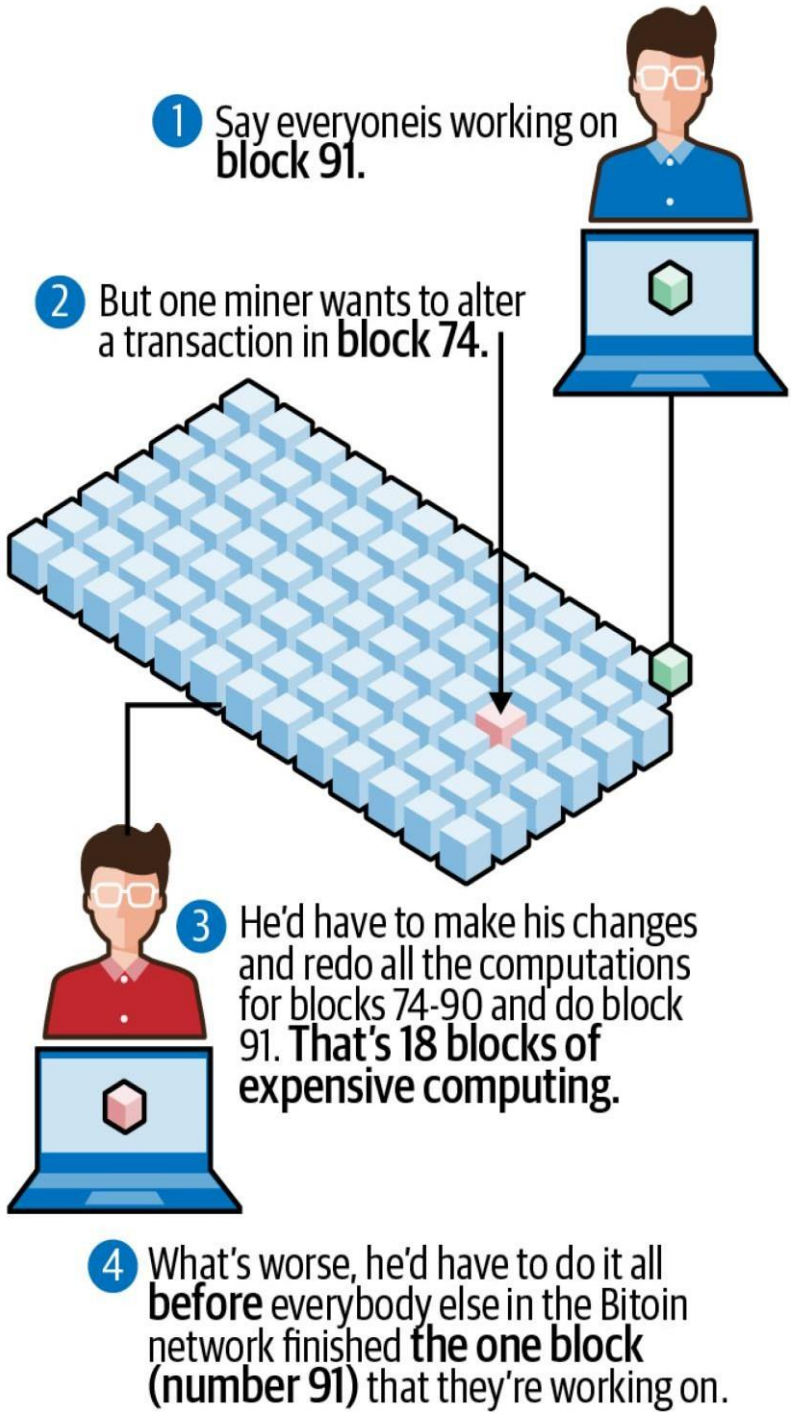
Double spending is a type of deceit where the same money is promised to two parties but only delivered to one.

John

The mechanism of the blockchain ensures that the party spending the bitcoins is the real owner.

Bob

The technology behind Bitcoin ensures that the party who spends the bitcoins is the real owner by only processing verified transactions.



Why and how it is difficult to alter a block or a transaction in blockchain?

Interesting Questions

Question 1

- Since anyone can participate in Bitcoin blockchain and participate in mining the system consists of multiple parties which are not knowing each other
- Then, How these multiple parties who do not know each other and do not trust each other can collaborate
- In other words, how such an anonymous and decentralized system can work fairly?

Question 2

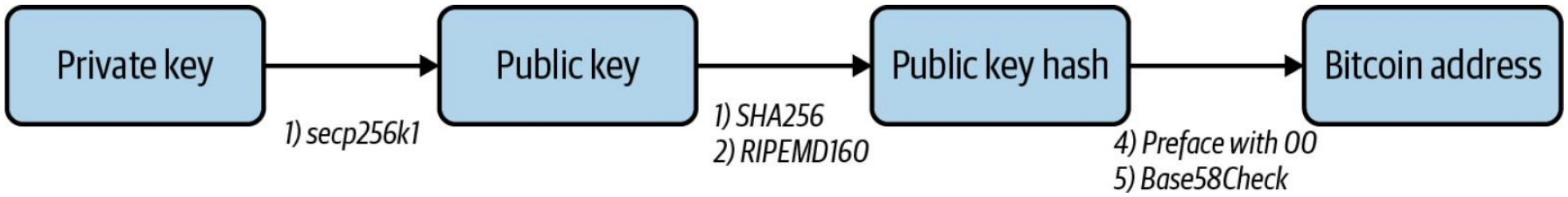
- How can bitcoin blockchain ledger which is acted upon by multiple parties is valid and accurate (remains in sync)?

Public/Private Key Cryptography

- Blockchain uses public/private key cryptography for its secure working
- **Private key** is used to digitally sign every transaction in blockchain
  - It is the way a user **proves** the *rightful ownership of an address* to the blockchain network
  - It kept **secret** with the user and not shared
- **Public Key** used to generate a public address
  - Public address is a compressed version of public key
  - Thus, public address (or compressed public key) can be shared with everyone

Generating Keys and Bitcoin Address

- A **private key** is usually 256-bit number and mostly shown in **hexadecimal** format
- Private key is chosen at random by using a function to generate a random number
- The corresponding **public key** can be generated by running the private key through an Elliptic Curve Digital Signature Algorithm (ECDSA) secp256k1 function
- The **double hash** of public key is then generated by running the public key through first SHA256 and then RIPEMD160 functions (output is 160 bits or 20 bytes)
- Prefix this hash with 00 and then run through Base58Check encoding
- The result is Base58Check Encoded Public Key Hash which is bitcoin address



Introduction to Transaction in Bitcoin

- Bitcoin transactions follow a unique type of accounting called **UTXO**, which stands for **unspent transaction output**
- A transaction is basically a list of inputs and a list of outputs
- Each **input** has
  - a Bitcoin address that is acting as the source of funds, plus
  - an unspent transaction that address has received in the past and
  - a digital signature which proves the ownership of the address
- Every **output** identifies
  - the Bitcoin address receiving the funds and
  - the amount that address will receive

Compelling Components of Bitcoin Blockchain

1. **Open Source**
   - No single entity or group has proprietary right of the software
   - Common users and developers have the **source code** of the Bitcoin
2. **Value**
   - A unit of account, called **bitcoin** (often denoted as BTC), is used to record transactions on the ledger
3. **Decentralization and Distributed**
   - From system point-of-view blockchain is decentralized system
   - From ledger point-of-view blockchain has distributed ledger
4. **Consensus**
   - It is a mechanism to establish the agreement among the nodes participating in the blockchain network about the current status of blockchain database (i.e., ledger).