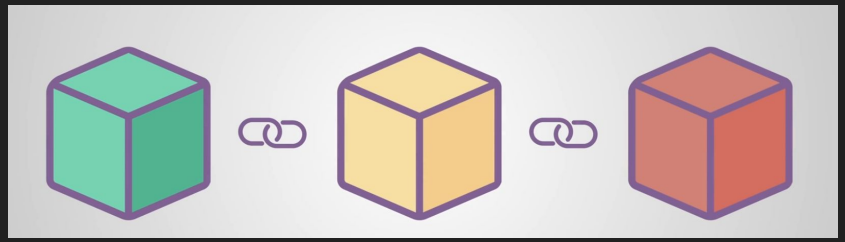
Blokķēdes tehnoloģija; principi un lietojumi



Ronalds Rundāns
Latvijas Universitāte 2024

Prezentācijas saturs

Kā radās blokķēdes?

Kas ir blokķēdes?

Kādi ir tās darbības principi?

Kas ir viedlīgumi?

Kā darbojas viedlīgumi?

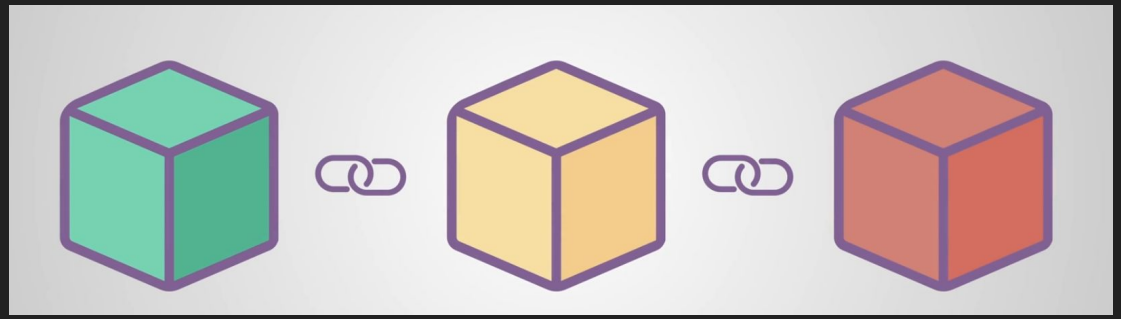
Kādi ir šo tehnoloģiju trūkumi?

1991.gads

Kriptogrāfiski ķedes bloki ar laika zīmogiem

(Digital timestamps kā notāra zīmogs)

Neļaut sagrozīt esošos datus



2008.gads

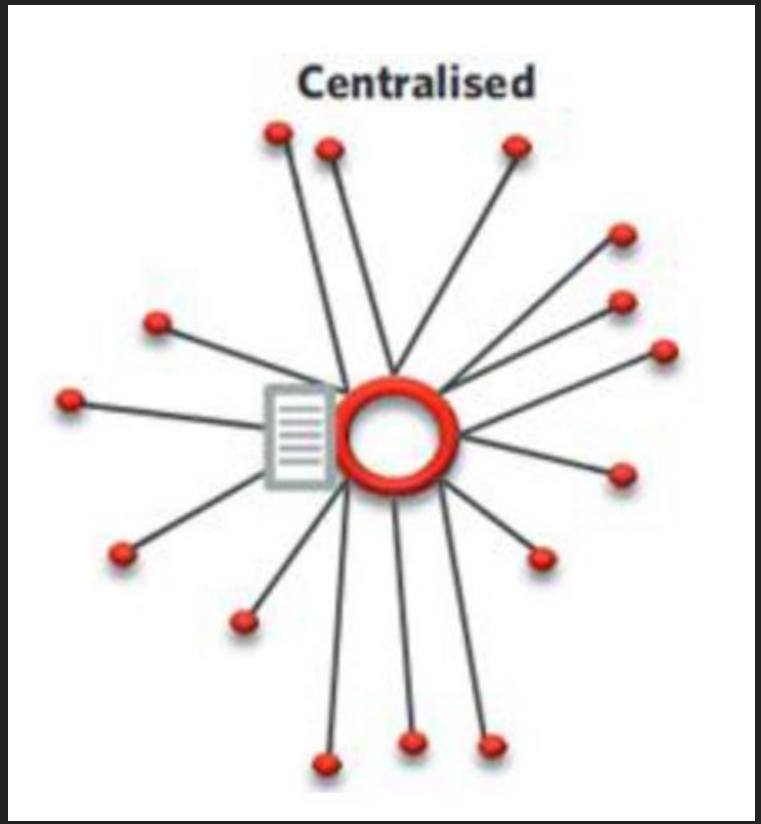
Bitcoin

“Satoshi Nakamoto”

Hash funkcijas laika zīmogu vietā

Nav viena organizācija, kas uztur blokķēdi

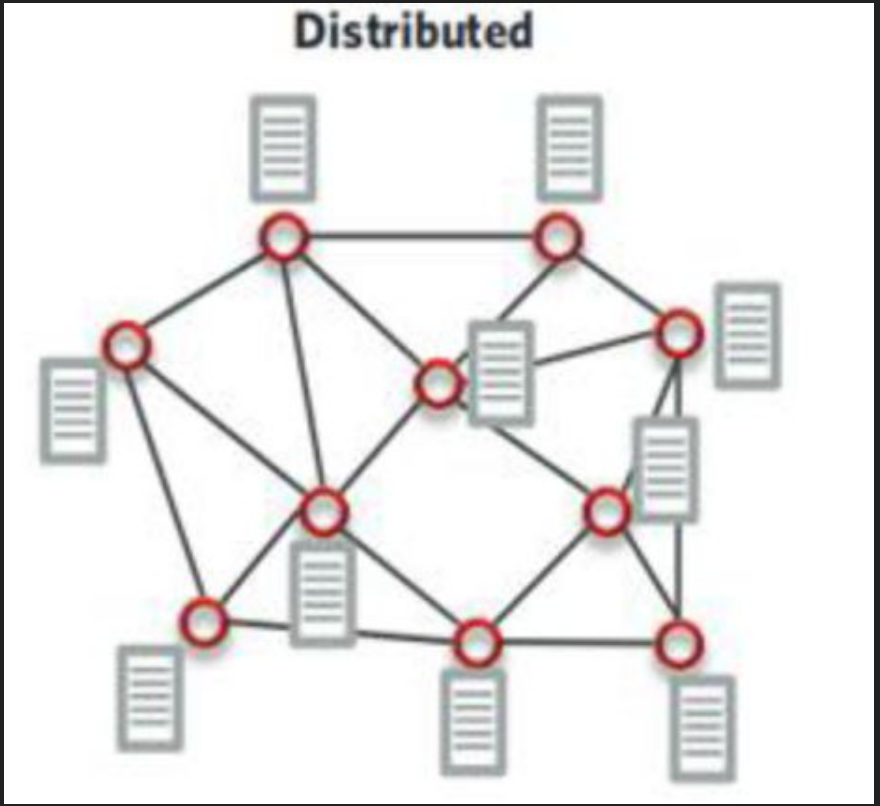
Tradicionāla banka un tās klienti



Bitcoin un tā lietotāji

Visu transakciju vēsture

>200 GB (2020.gadā)



Blokķēdes definīcija

Definīcija: Tehnoloģija, kas ļauj pārbaudāmā un pastāvīgā veidā kopīgot informāciju un reģistrēt darījumus starp divām pusēm.

EuroVoc tēzaurs v4.12 © Eiropas Savienība, 2020

Ieraksti var pārstāvēt gandrīz jebkādu darījumu

Blokķēdes galvenās īpašības un pazīmes

Blokķēdes galvenās īpašības un pazīmes

Virsgrāmata (kā grāmatvedība)

Kopīgots

Izplatīts

Drošs

Izplatītā virsgrāmata (Distributed ledger)

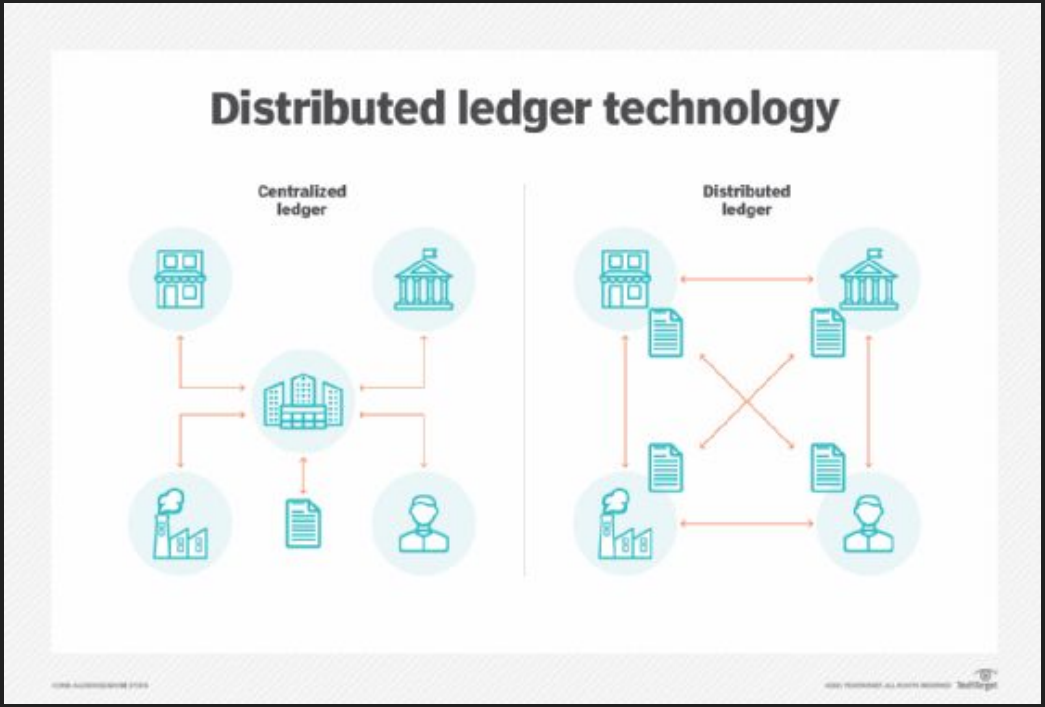
Ar algoritmiem apstiprina veiktos darījumus

Virsgrāmatas definīcija: Grāmatvedības dokuments:

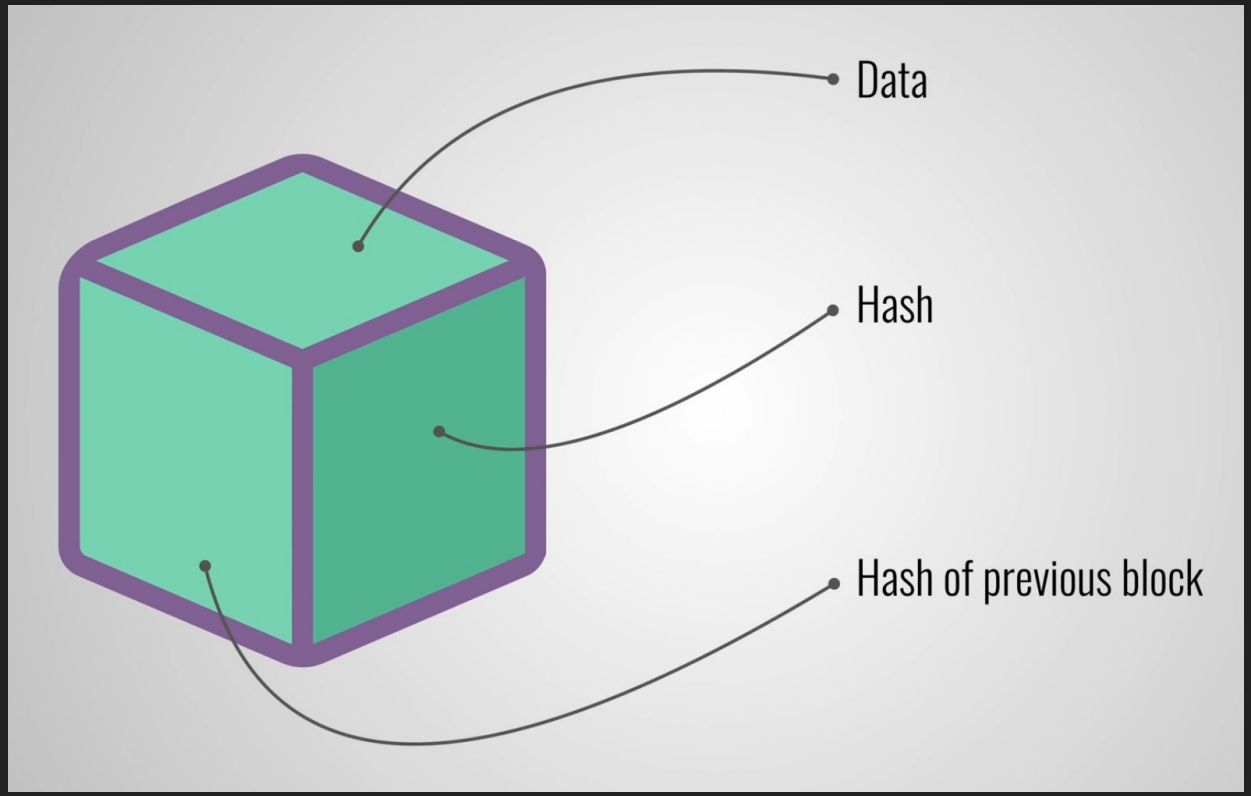
bilances kontu apkopojums, kas sakārtots

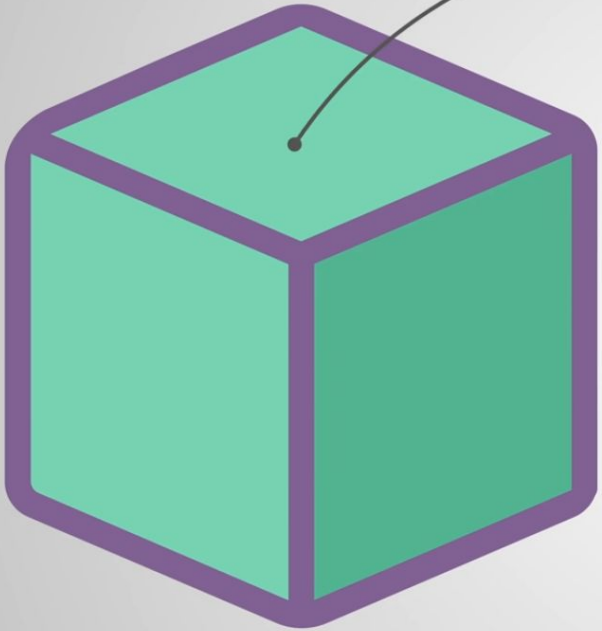
pēc noteikta plāna.

Ekonomikas skaidrojošā vārdnīca. — R., Zinātne, 2000



Bitcoin bloks





Data

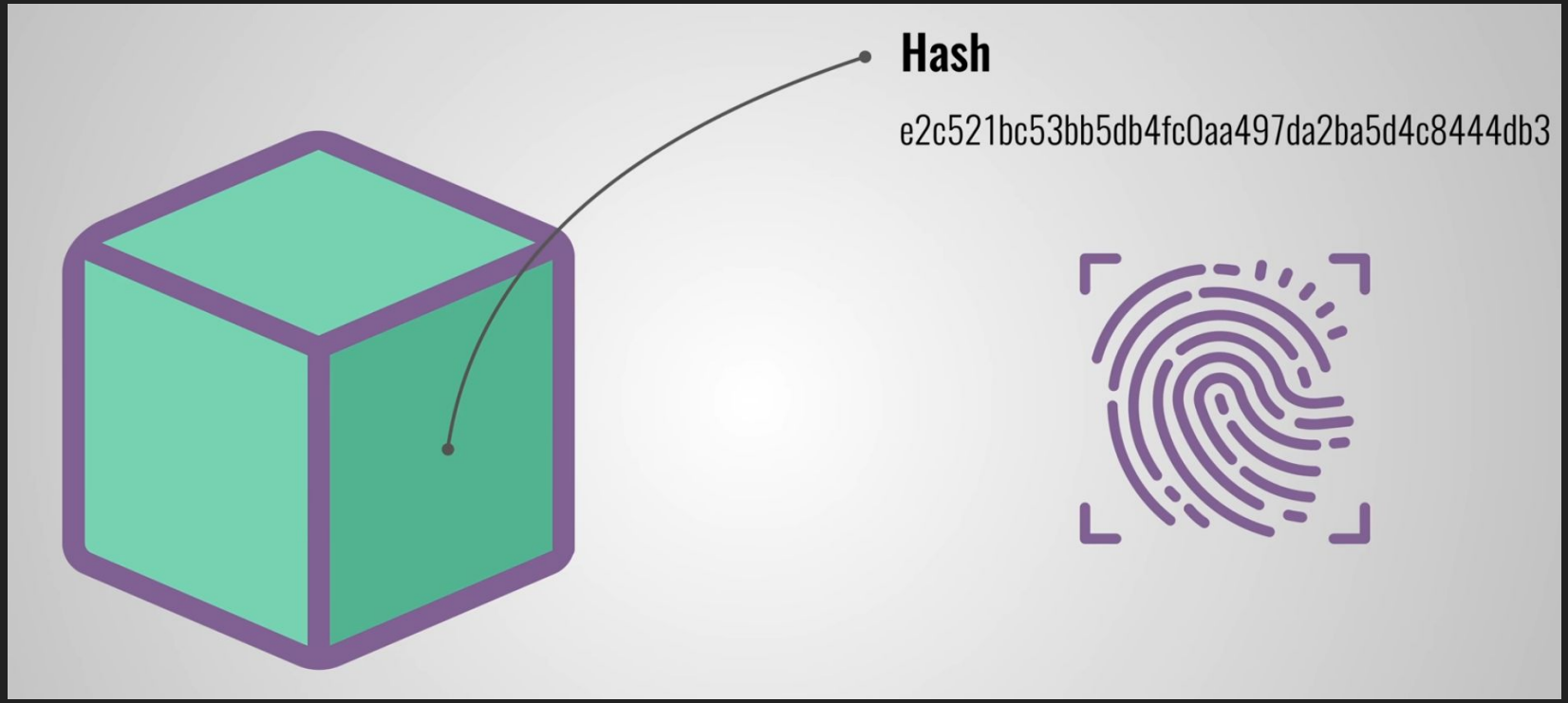
From: 👩

To: 👨

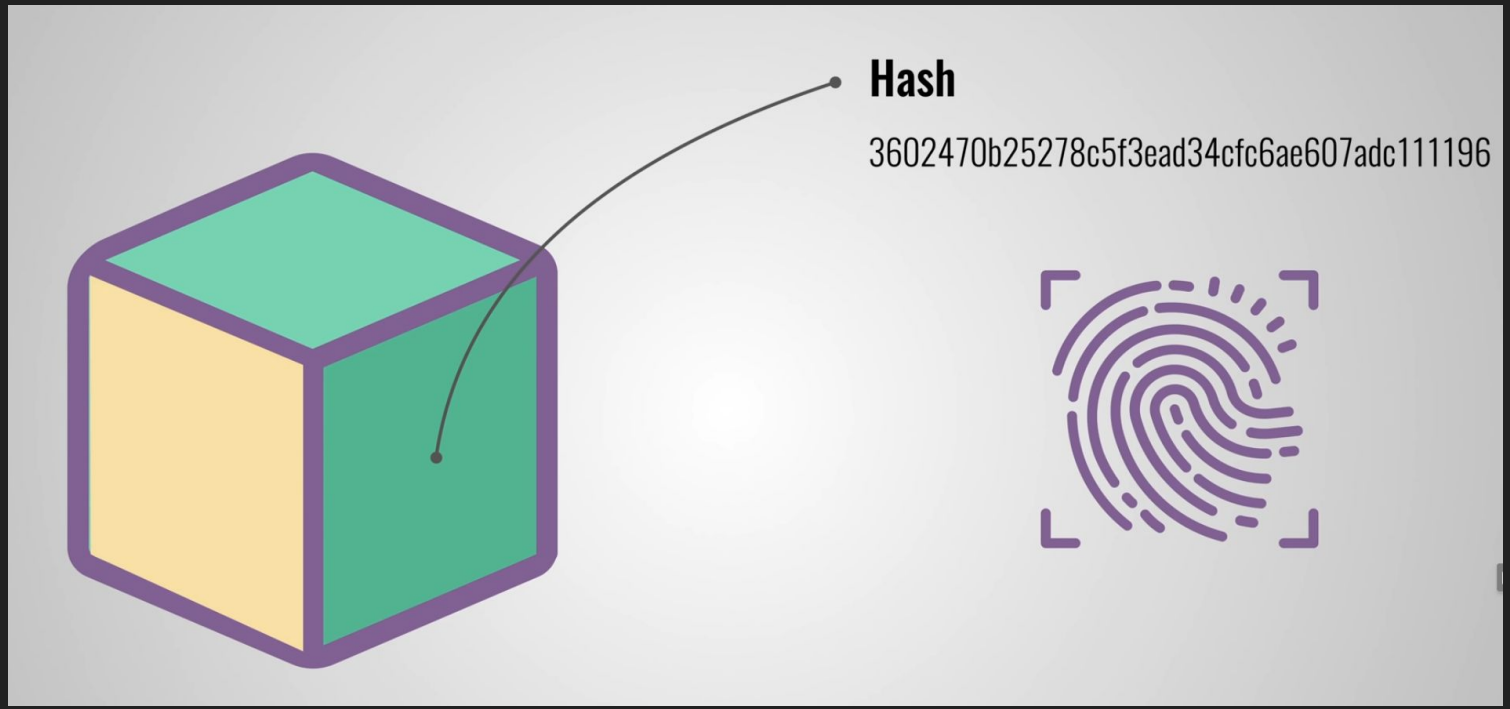
Amount: 💵

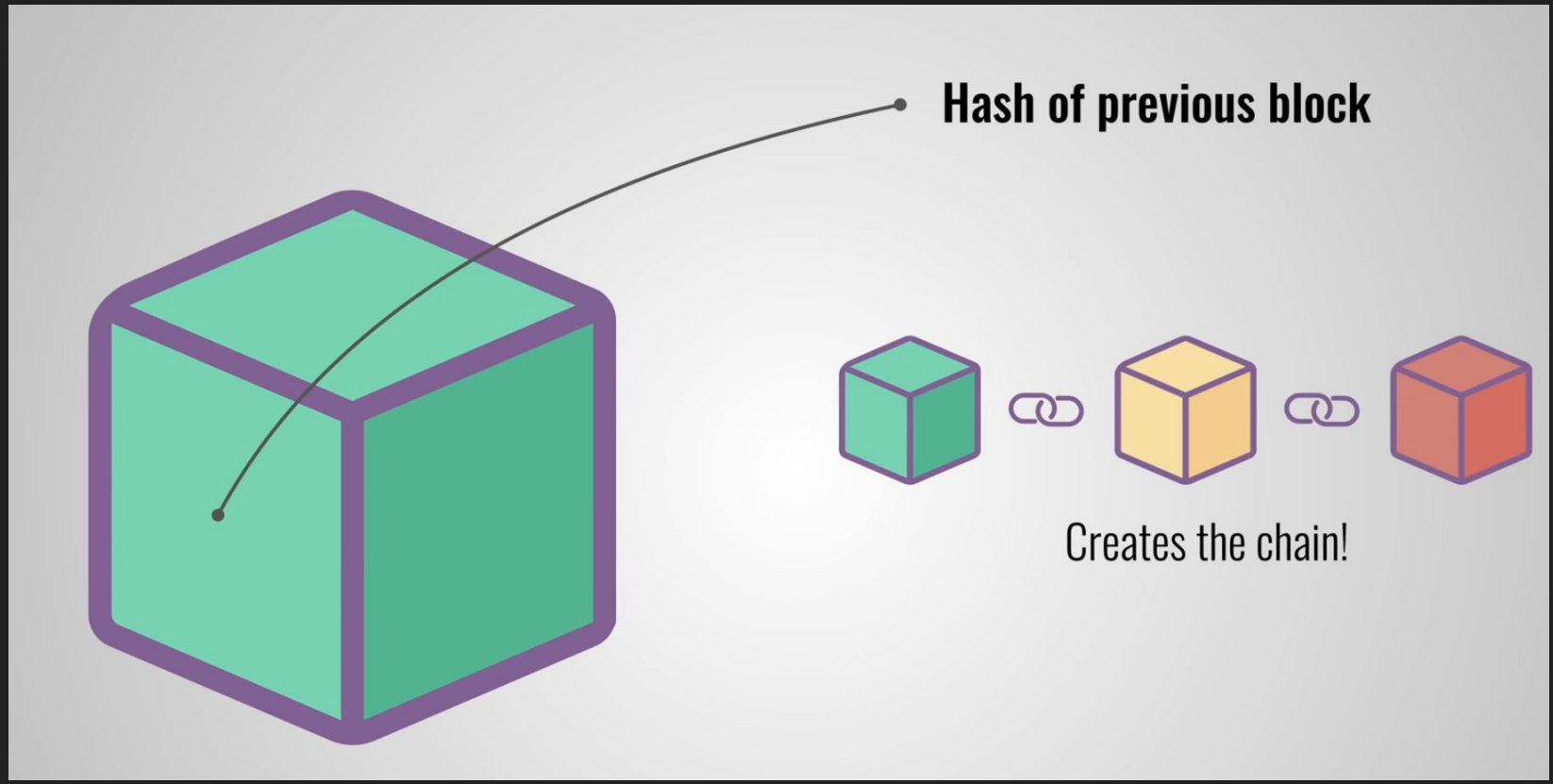
Bitcoin block example

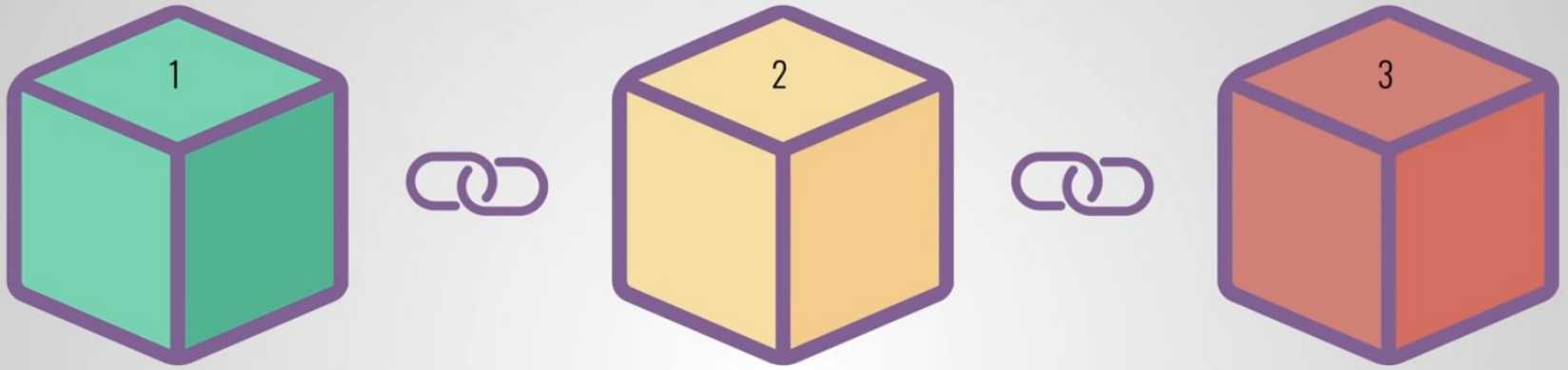
Hash



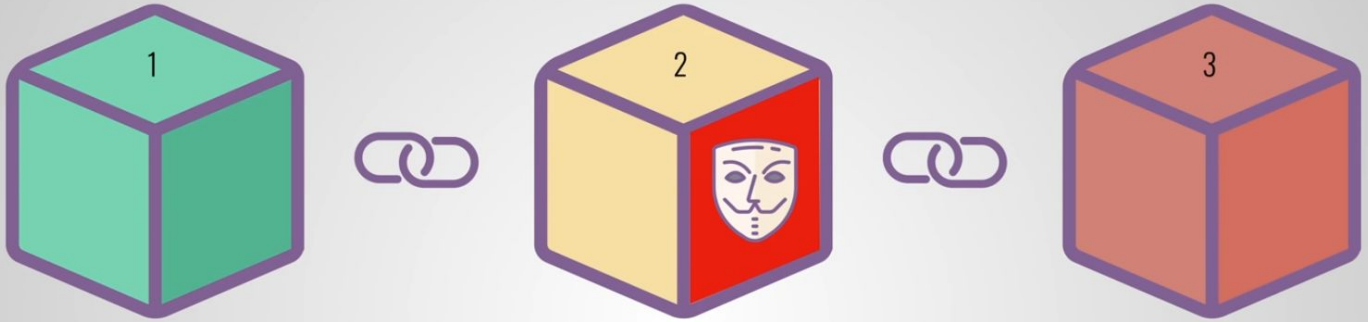
Ja maina datus mainās Hash vērtība




Hash of previous block
Creates the chain!



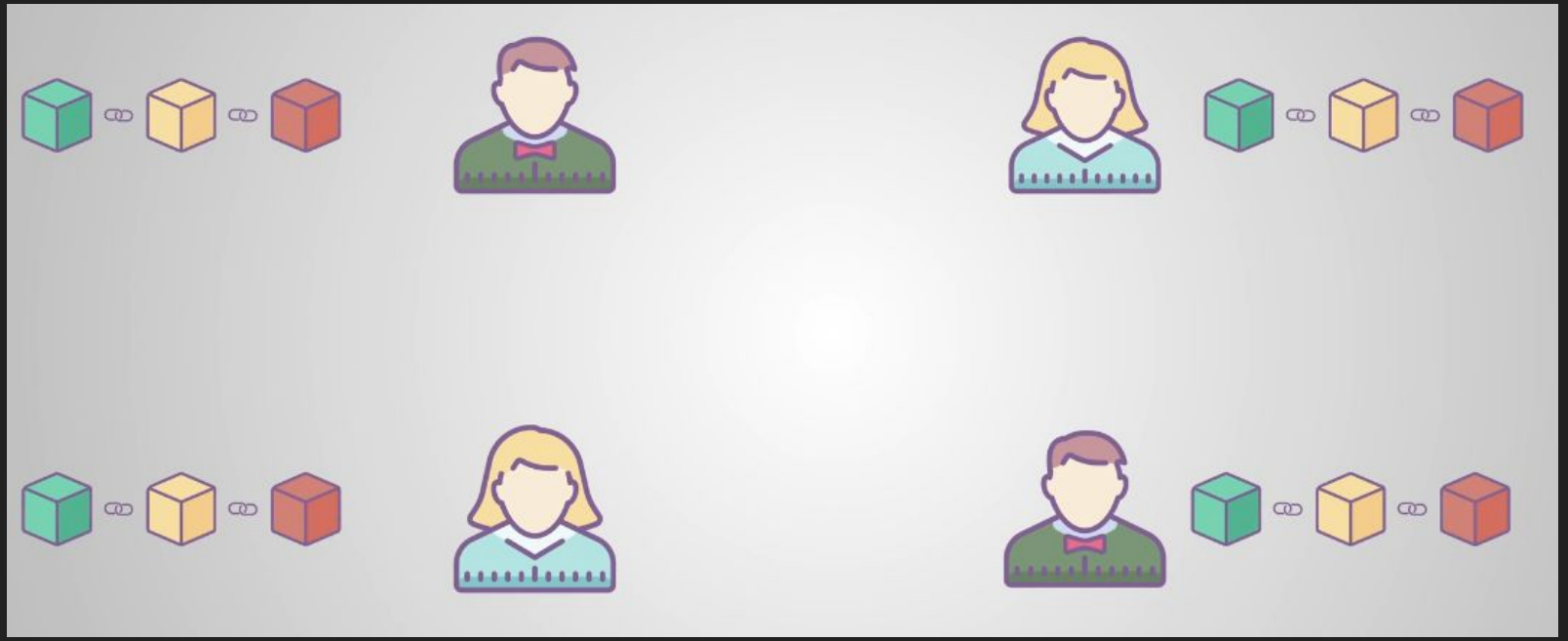
Hash: **1Z8F**	Hash: **6BQ1**	Hash: **3H4Q**
Previous hash: **0000**	Previous hash: **1Z8F**	Previous hash: **6BQ1**

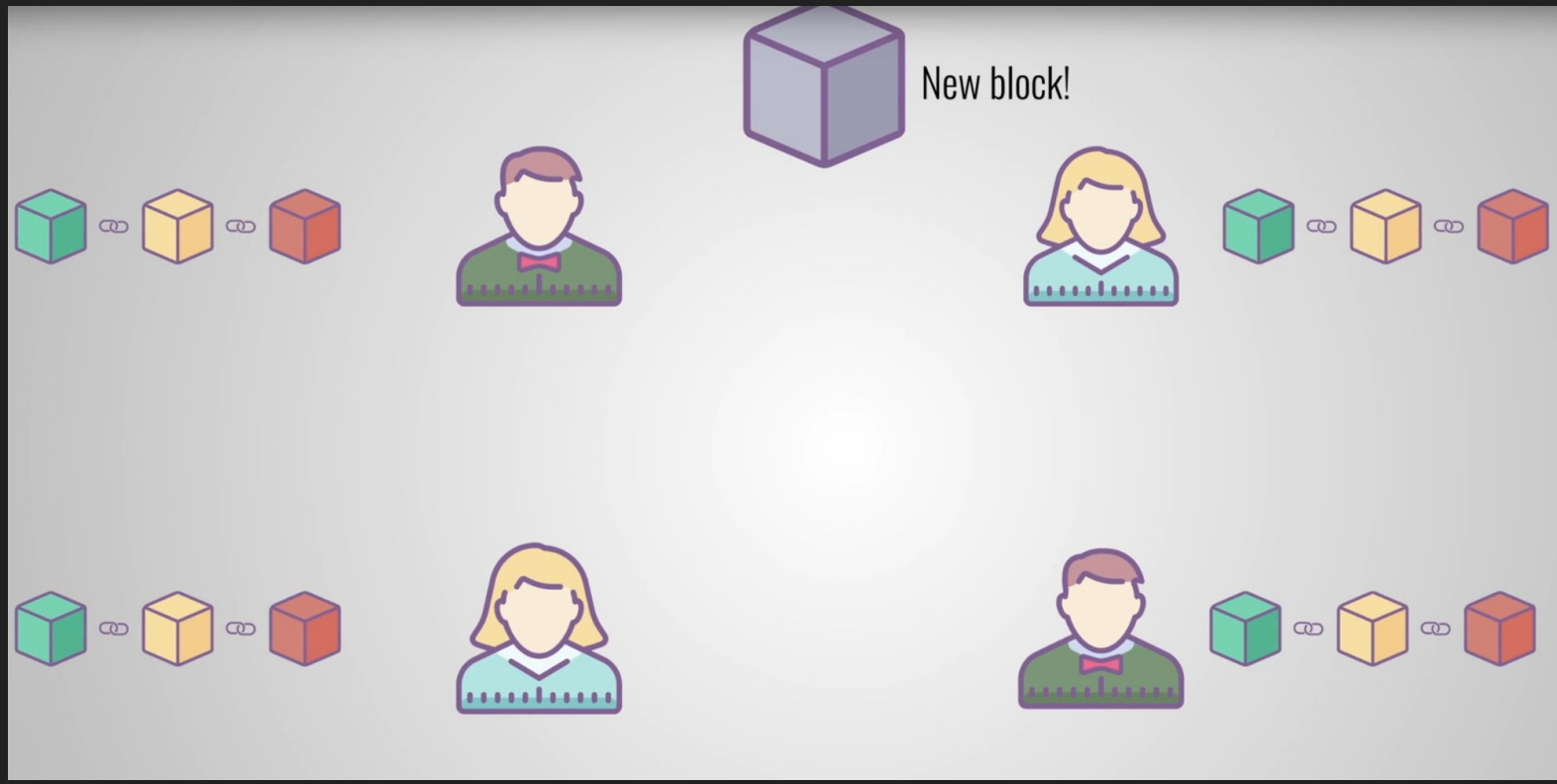


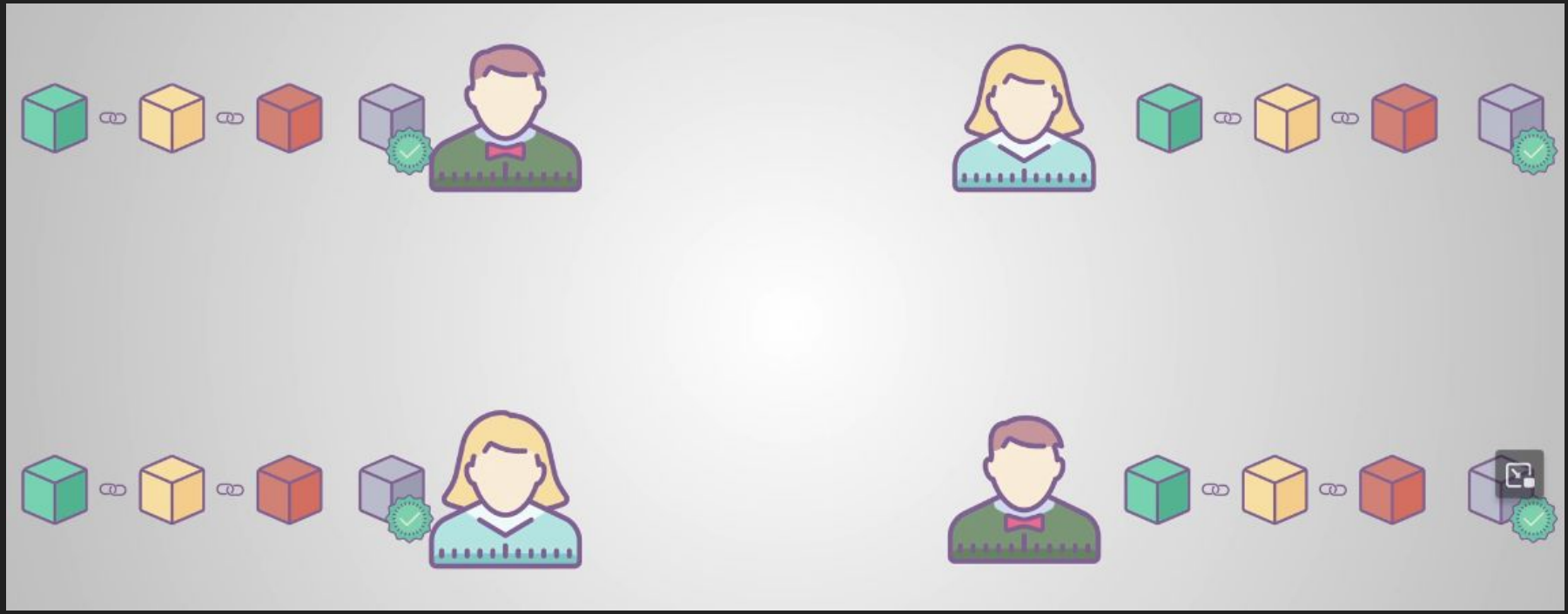
Hash: 1Z8F	Hash: ~~6BQ1~~ H62Y	Hash: 3H4Q
Previous hash: 0000	Previous hash: 1Z8F	Previous hash: 6BQ1

Uh thats not right??

P2P




New block!




Consensus!

Konsenss

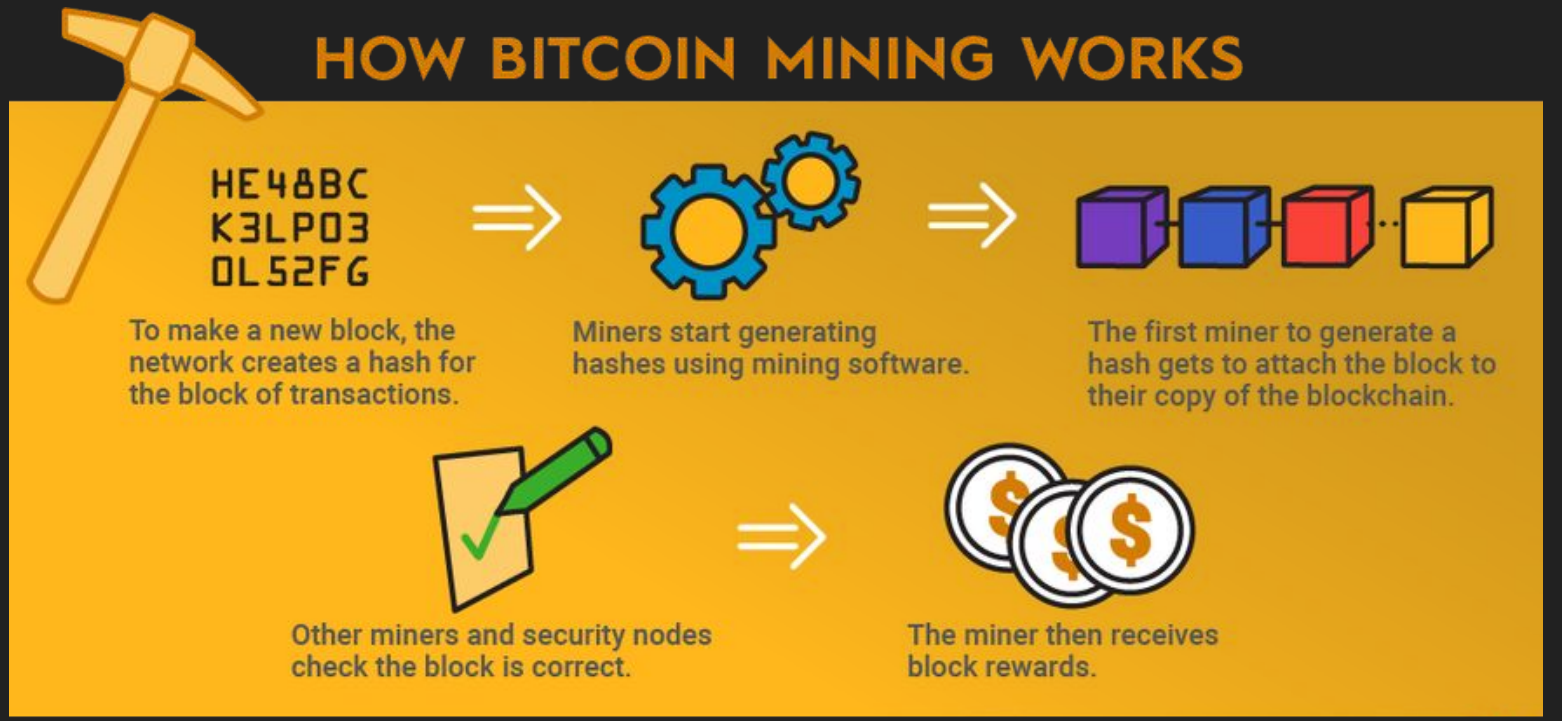
Darījumi tiek pārbaudīti ar konsensu –

dalībnieki savstarpēji apstiprina izmaiņas –

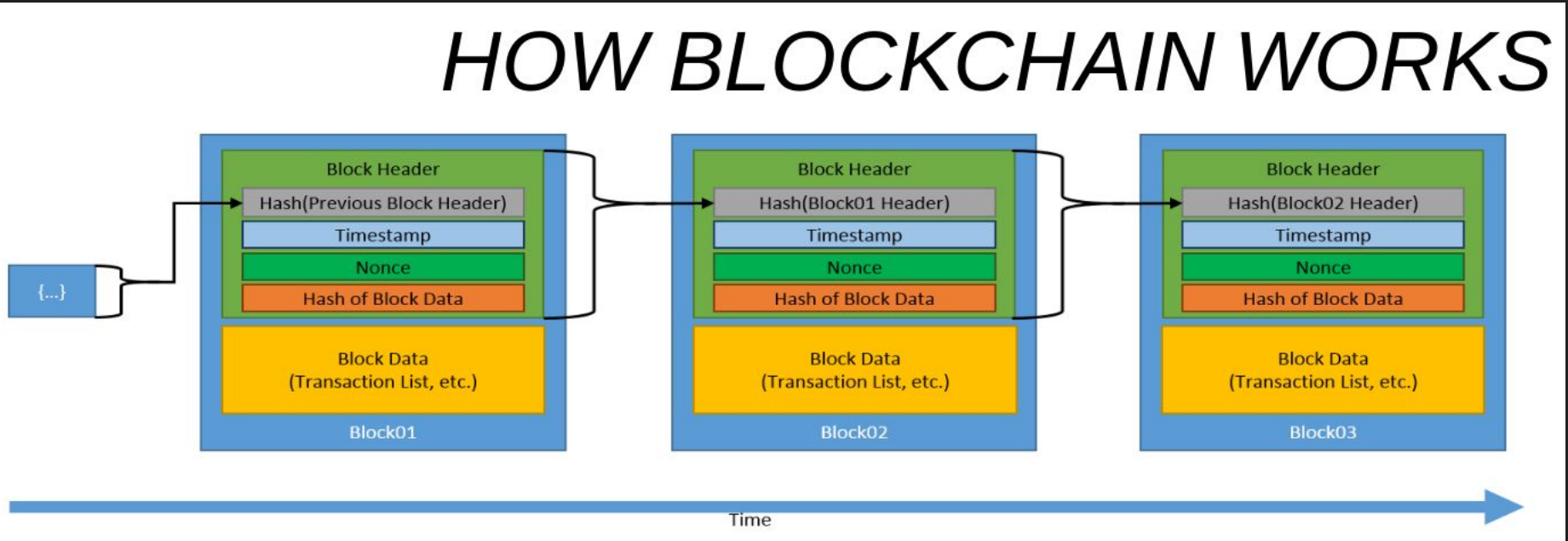
Kriptogrāfija nodrošina informācijas drošību.

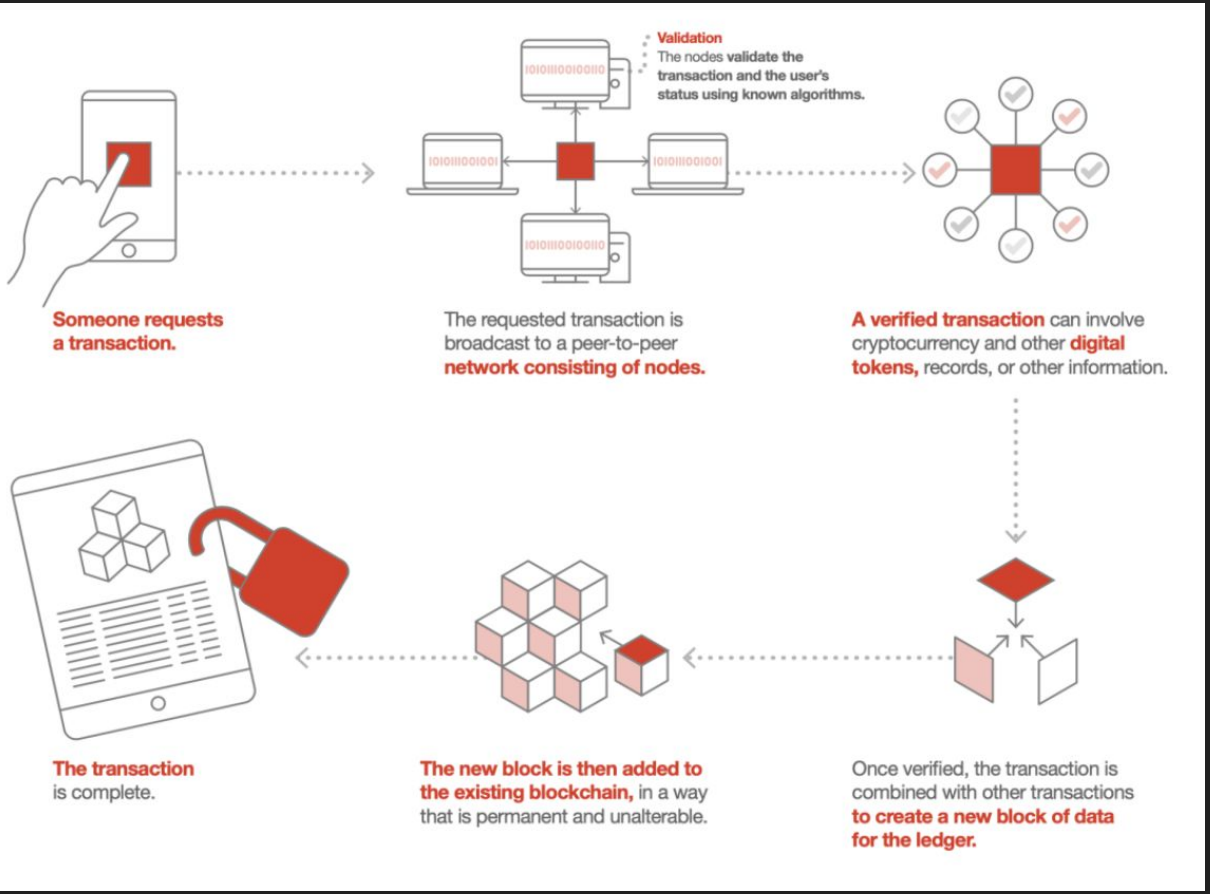
Tādējādi tiek novērsta nepieciešamība pēc centrālās sertifikācijas iestādes.

Bitcoin racēji

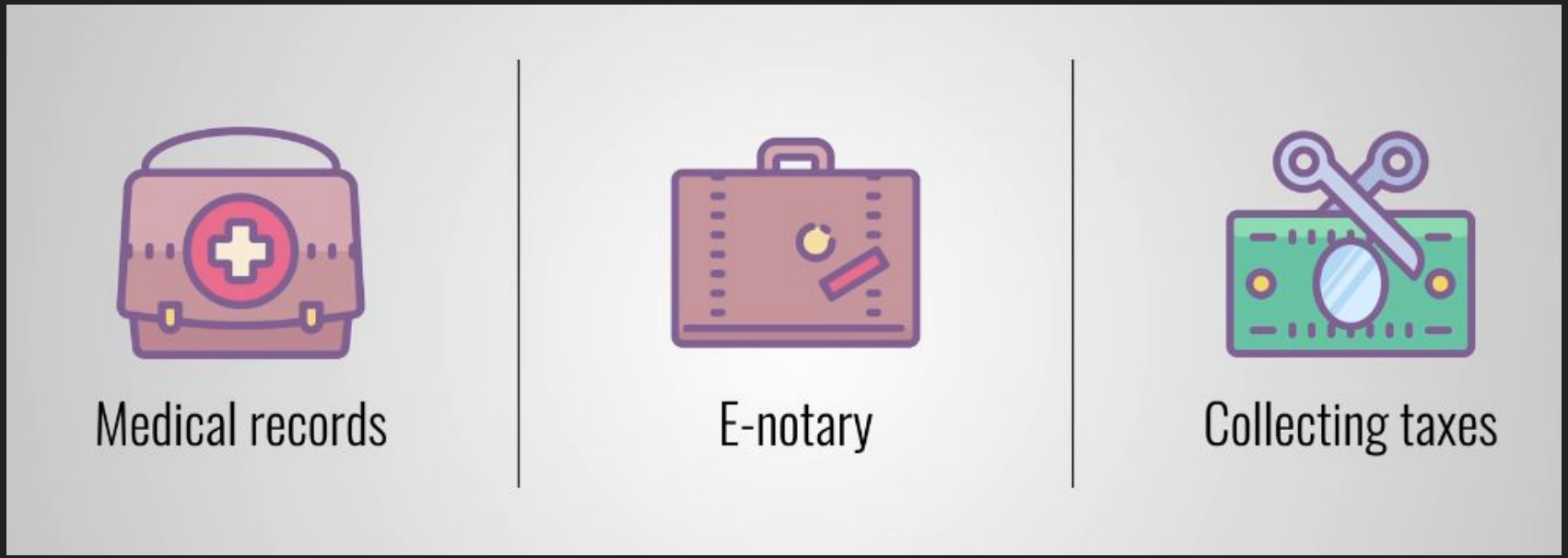


Kā darbojas blokķēde?




Validation
The nodes validate the transaction and the user's status using known algorithms.
Someone requests a transaction.
The requested transaction is broadcast to a peer-to-peer network consisting of nodes.
A verified transaction can involve cryptocurrency and other digital tokens, records, or other information.
The transaction is complete.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.

Blokķēžu pielietojumi

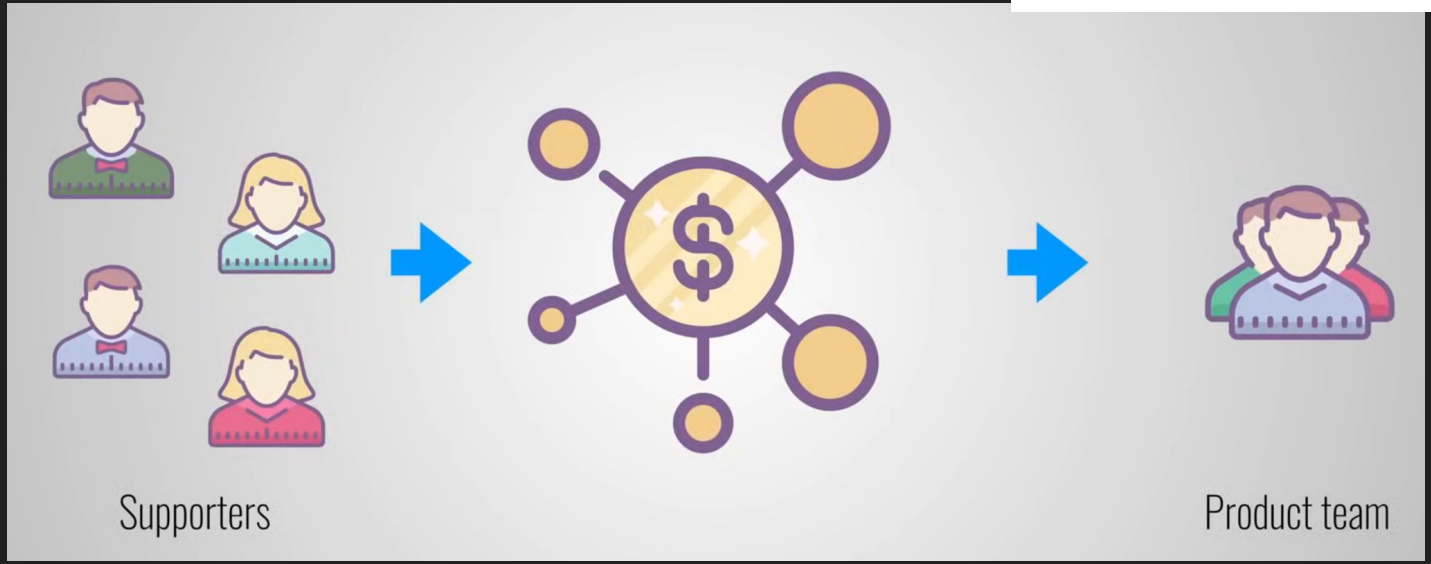


PUBLIC VS PRIVATE

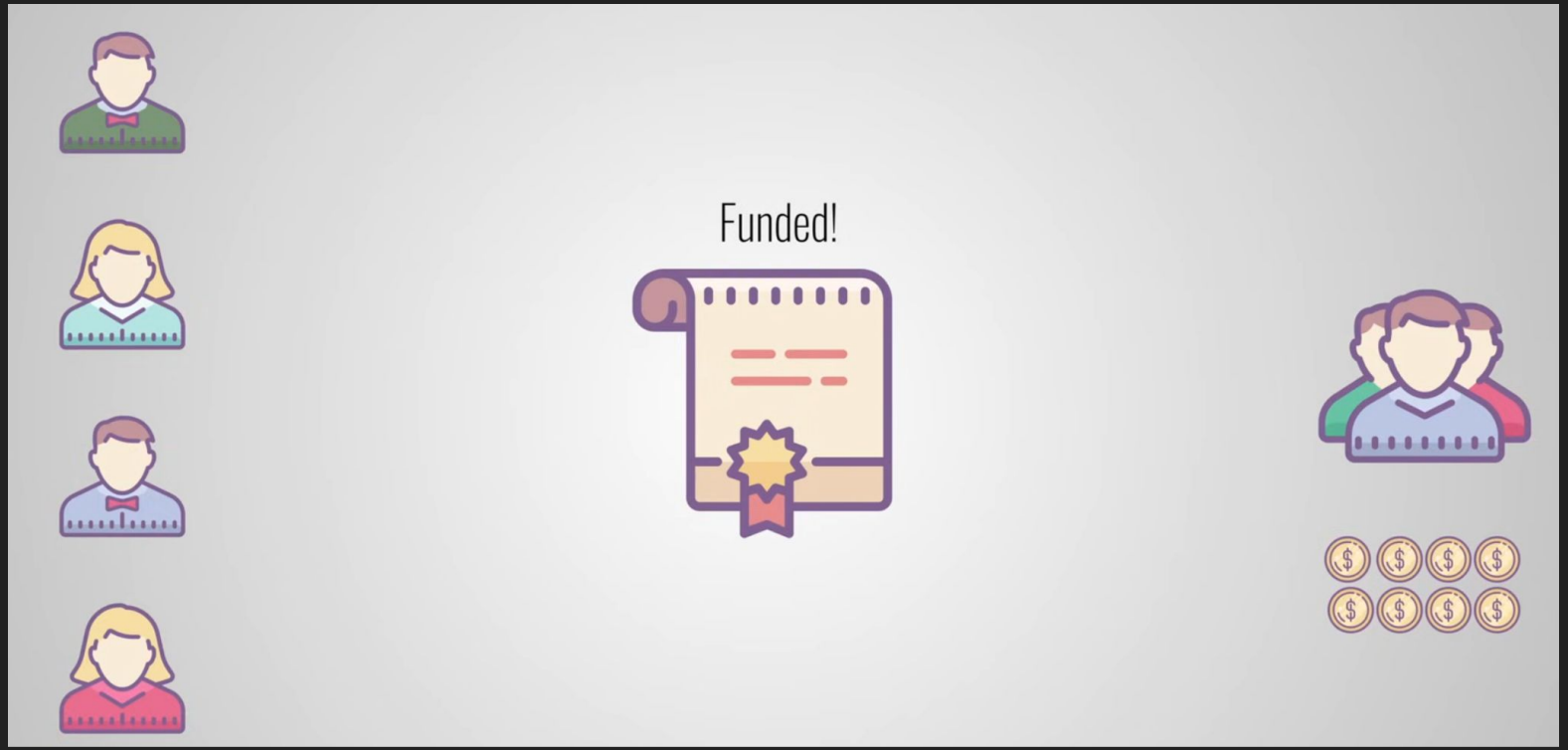
Viedlīgums (Smart contract)

1997.gadā Nick Szabo

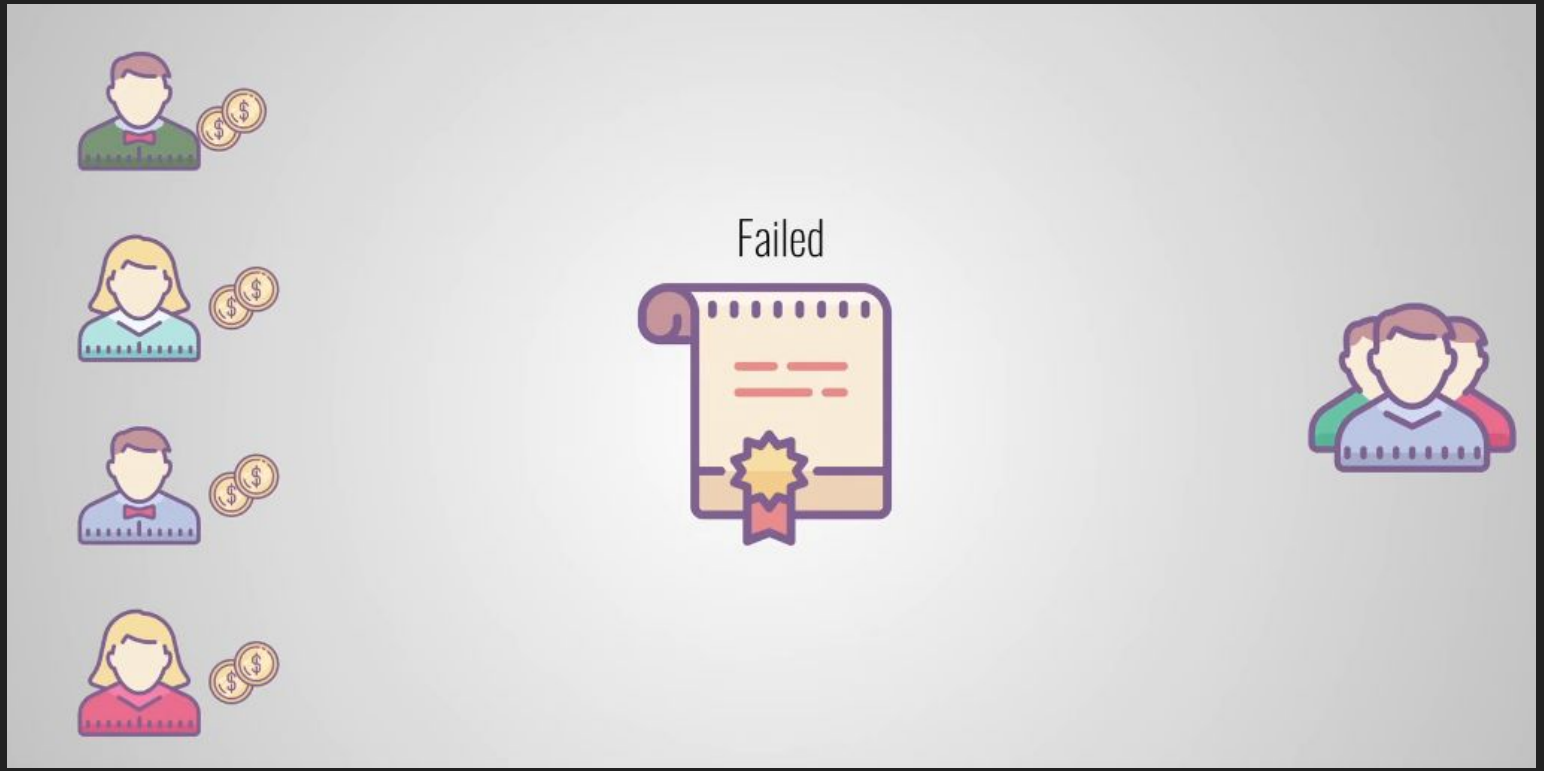
Līdzīgs kolektīvai finansēšanai (crowdfunding)



Izpilda līguma nosacījumus



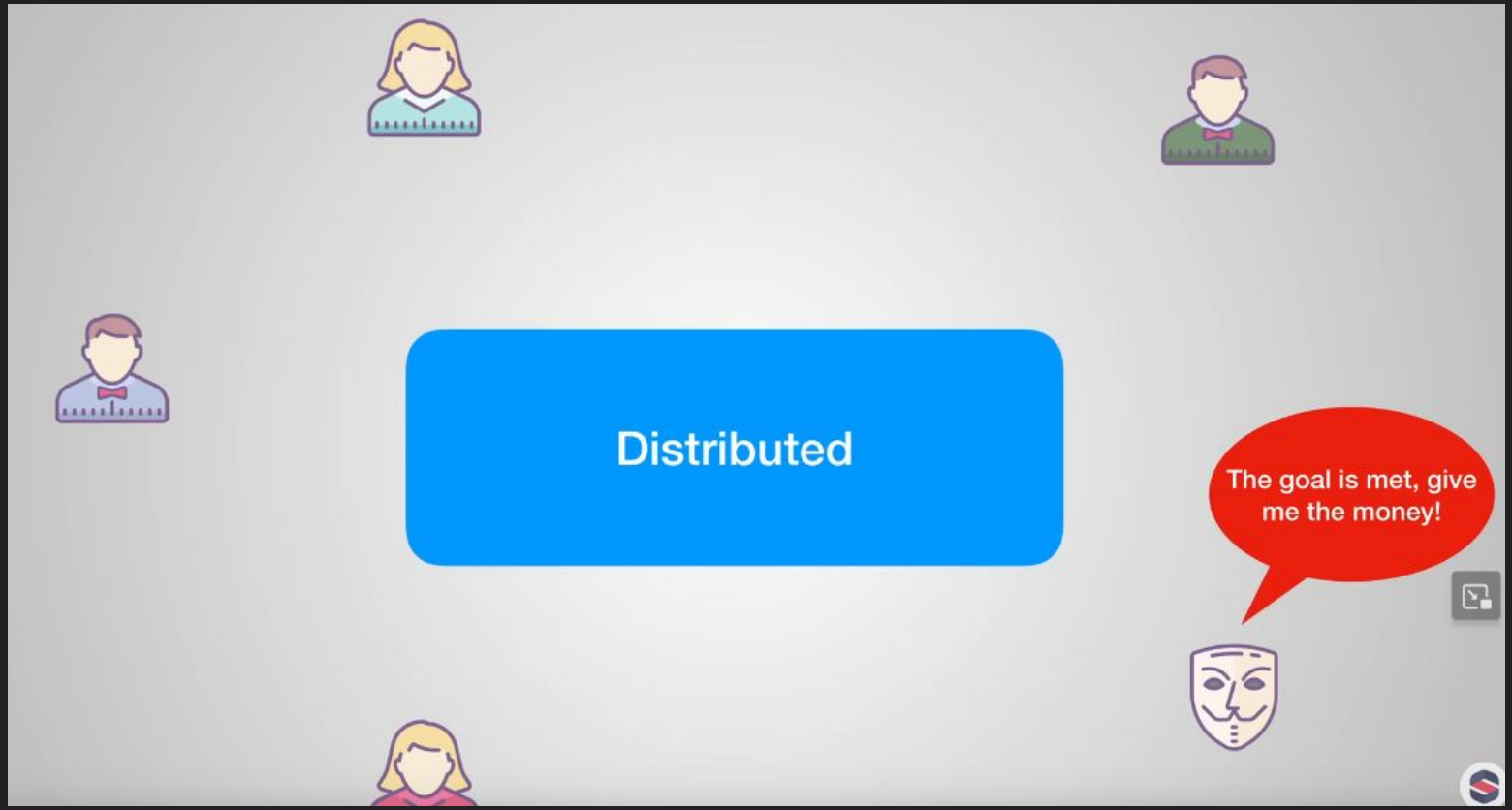
Neizpilda līguma nosacījumus



Viedlīgums (Smart contract)

Programmatūra, kas ir automātiski izpilda, kontrolē vai dokumentē nozīmīgus notikumus un rīcība saskaņā ar līguma noteikumiem vai vienošanos.

Viedlīgumi ļauj veikt automatizētus darījumus, pamatojoties uz iepriekš noteiktiem apstākļiem vai notikumiem.


Distributed
The goal is met, give me the money!


No, the goal isn't met!
We don't release the funds!

Viedlīgumu pielietojumi

Banks

Loans

Automatic payments

Insurance

Process claims

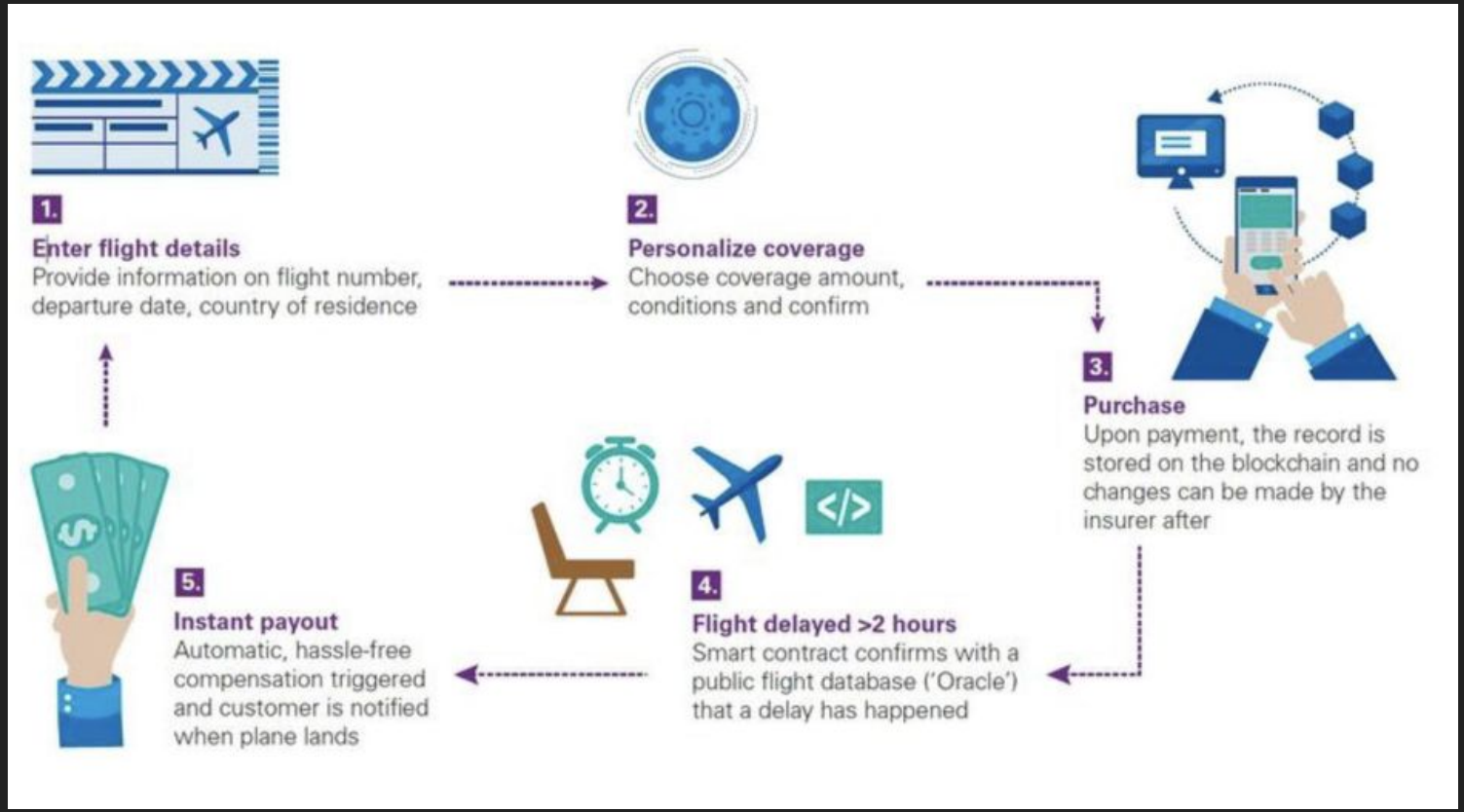
Postal

Payment on delivery

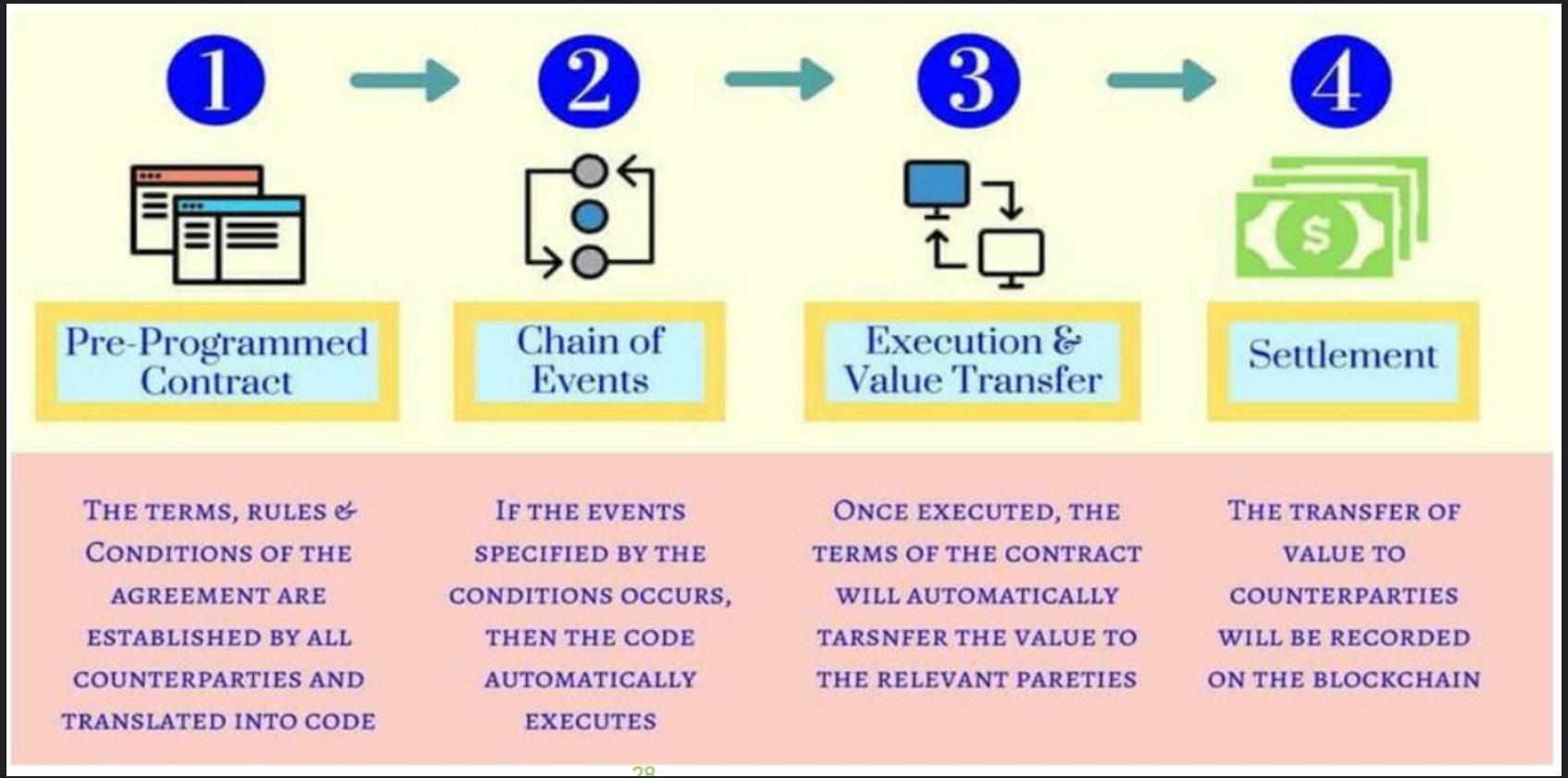
Ethereum

Solidity

AXA Fizzy (līdz 2020.gadam)



Kā darbojas viedlīgumi?



Benefits

Increased transparency and traceability

Faster transactions

Elimination of intermediaries

Lower costs

Barriers

Regulatory uncertainty

Complex technology

Collaboration challenges

Trust issues

Blokķēžu trūkumi

Decentralizācija ir dārga (konsenss)

Jo vairāk datoru darbina kodu, jo dārgāks produkts

Lieki aizņem atmiņu (visi nevis daži glabā blolkķēdi)

Kosavilkums

Kā radās blokķēdes?

Kas ir blokķēdes?

Kādi ir tās darbības principi?

Kas ir viedlīgumi?

Kā darbojas viedlīgumi?

Kādi ir šo tehnoloģiju trūkumi?

Jautājumi?

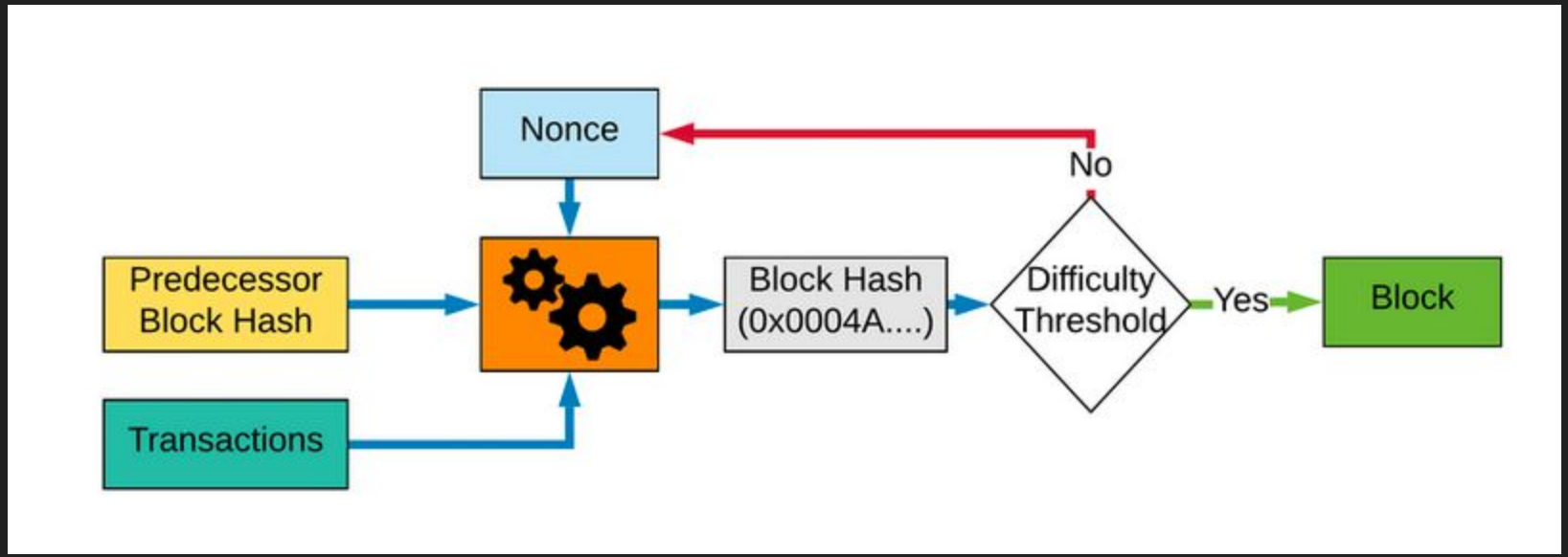
Konsensa iegūšana: ko darīt, ja vairākiem dalībniekiem ķēdes atšķiras?

Consensus Protocol says, whoever has the longest chain only that blockchain will consider as the valid blockchain and only that will be accepted by all the nodes, others will be discarded because it become an orphan block which is no longer needed and if there is the conflict between the two network having different set of blockchain with same numbers of blocks then that block will not be added until another block is mine by those networks, whoever adds the next block first ,and who's numbers of blocks will be more that networks blockchain will be accepted by all the nodes.

Piemērs

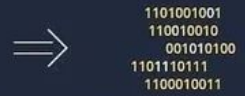
Lets assume there are 7 nodes in a network A,B,C,D,E,F,G and let miner A and G has mined a block at the same time, now we have 2 mined blocks,and both A and G will transfer their data in the network, and others will add blocks eg. B,C,D added A's Block and E,F has added G's block, so in this A's block will be accepted by all the nodes. because A's block is accepted by more nodes than by G's. now E,F,G have to discard their block and they also have to add A's block.

23. slaids: kāpēc "bitcoin mining" tērē tik daudz resursu?



HOW BITCOIN MINING WORKS:

Bitcoins are mined from blocks. Each block is part of the blockchain (a ledger of all the transactions made using Bitcoin).



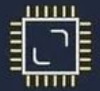
Blocks are where the complex mathematical code is stored

To mine Bitcoin users have to make a new block.

Blocks are linked together by hashcodes.

To make a new block, miners have to come up with a new hash which meets specific requirements, such as including the header of the block before and being above or belove the target value.

This can be a process of trial and error until miners find a hash which works.



Users must then solve the mathematical problem, known as a Proof of Work problem, using their computer CPU to run the problem solving software.

Each one is now worth 25 Bitcoins. It was previously 50 Bitcoins but the figure is halved every four years to reduce the rate at which they are mined.

Once the problem has been solved the Bitcoins are transferred to the miner's unique address.

They can then make transfers using Bitcoin via their Bitcoin wallet.

Kādas ir galvenās atšķirības starp publiskajām un privātajām blokķēdēm un kādos gadījumos tipiski izmanto katru veidu?

1. **Public Blockchains**: Open and permissionless; anyone can join and participate in transaction verification (e.g., Bitcoin, Ethereum).
2. **Private Blockchains**: Restricted and permissioned; control is held by select entities or organizations which dictate who may join (e.g., Hyperledger Fabric).
3. **Consortium Blockchains**: Also permissioned but control is shared among predetermined groups or organizations, balancing privacy with decentralization (e.g., R3 Corda).

Vai bez publiskajām un privātajām blokķēdēm ir vēl kādi blokķēžu tipi?

Other Prominent Blockchains

- **Tron**: Focusing on a decentralized internet and entertainment.
- **Ripple (XRP Ledger)**: Tailored for fast, cross-border payments.
- **Stellar**: Aiming to connect financial institutions for large transactions.
- **Solana**: Known for high throughput and fast transaction processing.
- **Polkadot**: Enables different blockchains to transfer messages and value in a trust-free fashion.

Ņemot vērā, ka viedlīgumi ir automatizēti, kā tie tiek galā ar neparedzētām situācijām vai kļūdām?

Testēšana

Kurās situācijās blokķēde nebūtu piemērota tehnoloģija?