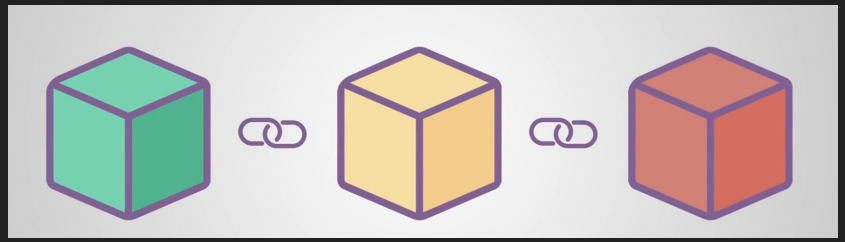
Blokķēdes tehnoloģija; principi un lietojumi



Ronalds Rundāns
Latvijas Universitāte 2024

Prezentācijas saturs

Kā radās blokķēdes?

Kas ir blokķēdes?

Kādi ir tās darbības principi?

Kas ir viedlīgumi?

Kā darbojas viedlīgumi?

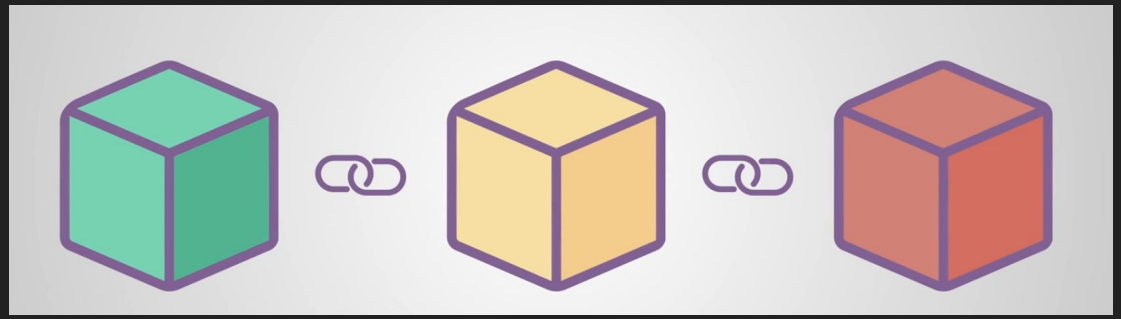
Kādi ir šo tehnoloģiju trūkumi?

1991.gads

Kriptogrāfiski ķedes bloki ar laika zīmogiem

(Digital timestamps kā notāra zīmogs)

Neļaut sagrozīt esošos datus



2008.gads

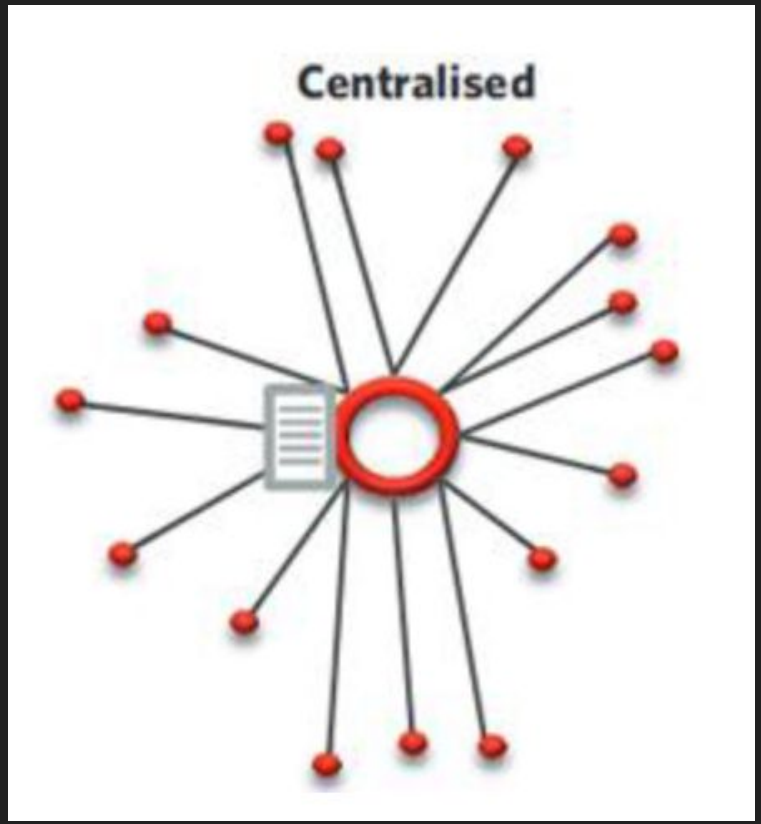
Bitcoin

“Satoshi Nakamoto”

Hash funkcijas laika zīmogu vietā

Nav viena organizācija, kas uztur blokķēdi

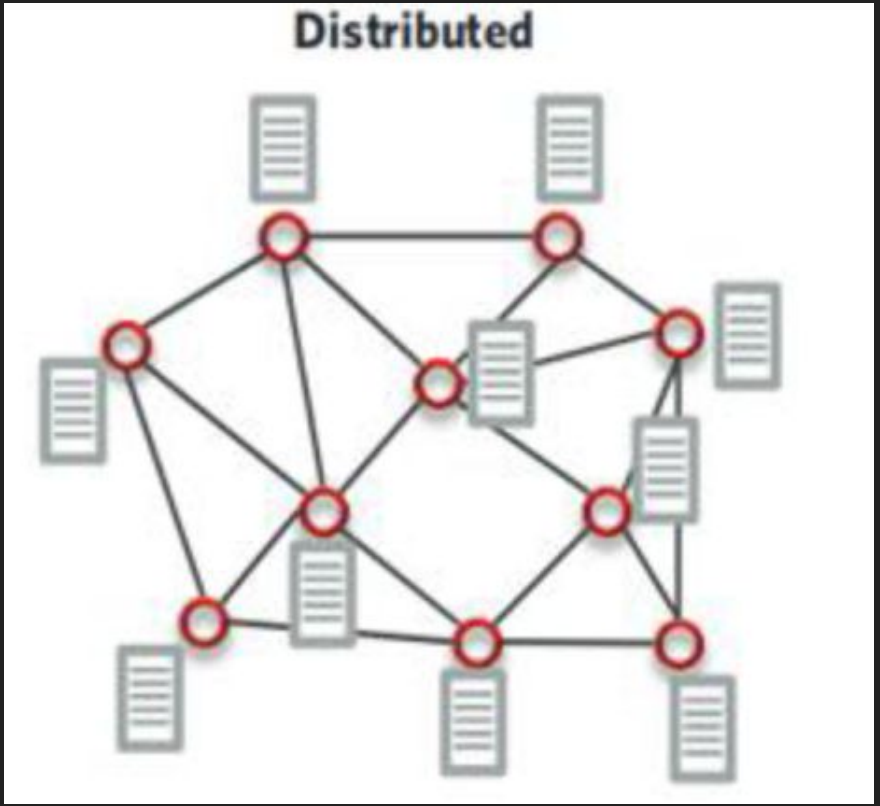
Tradicionāla banka un tās klienti



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)

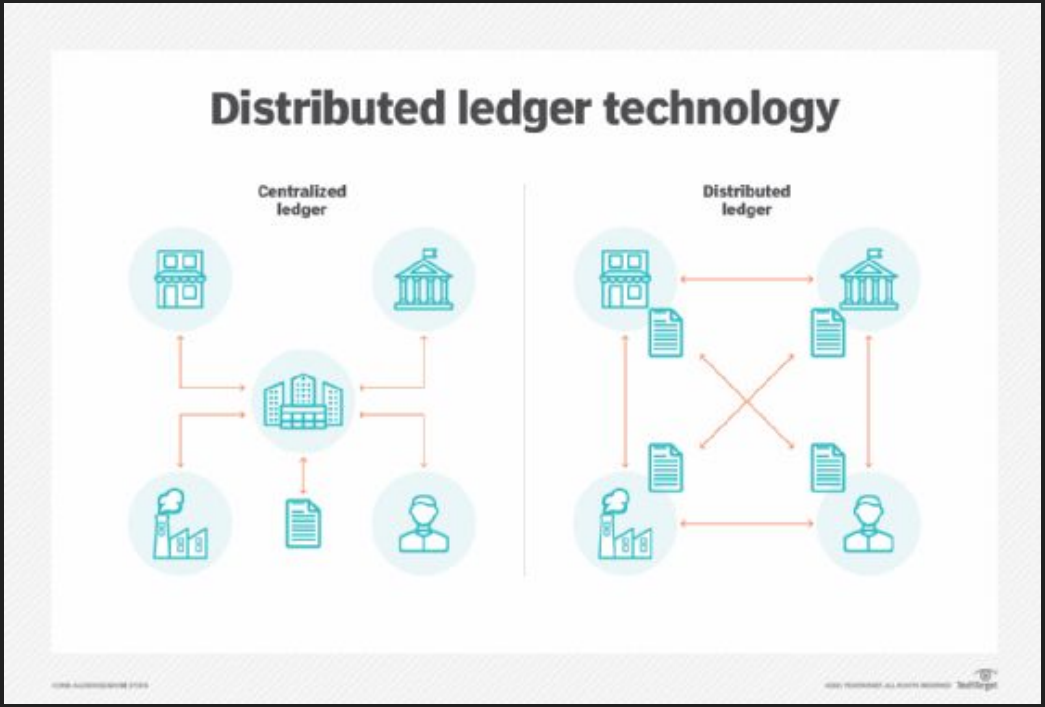
Ar algoritmiem apstiprina veiktos darījumus

Virsgrāmatas definīcija: Grāmatvedības dokuments:

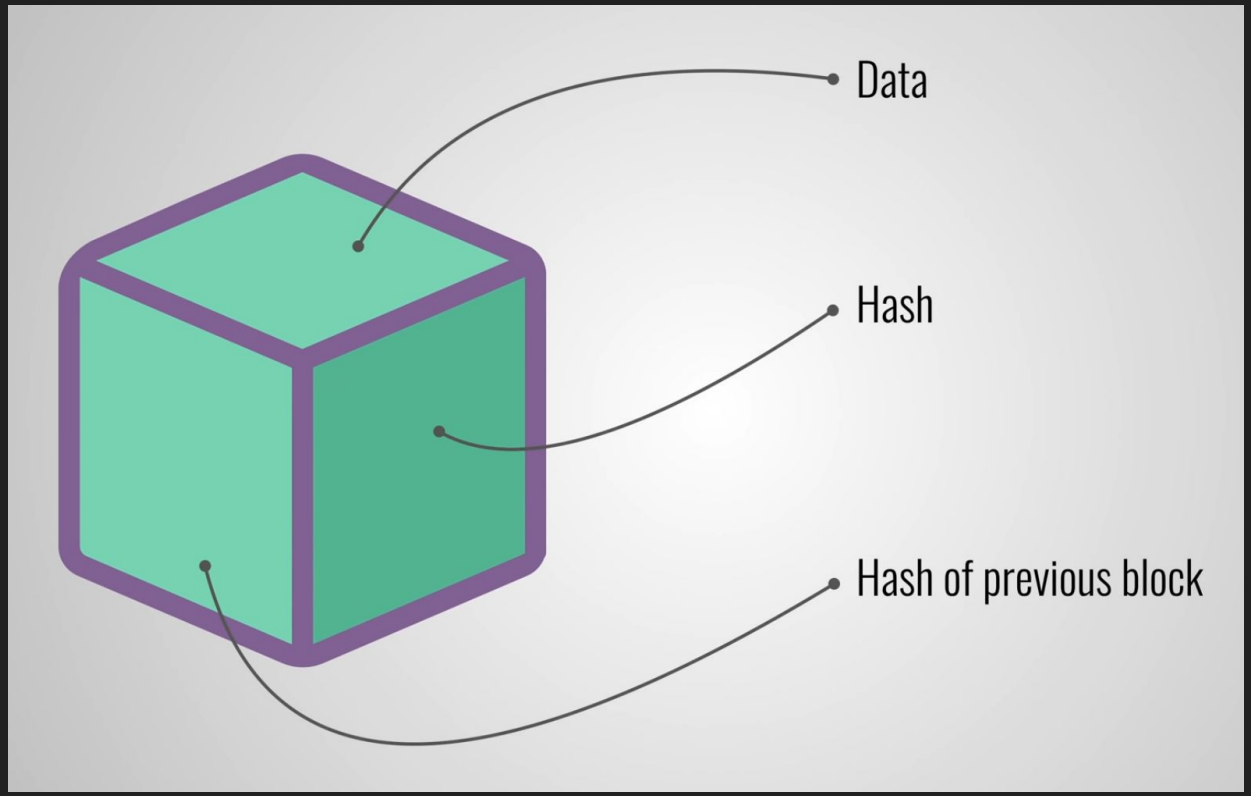
bilances kontu apkopojums, kas sakārtots

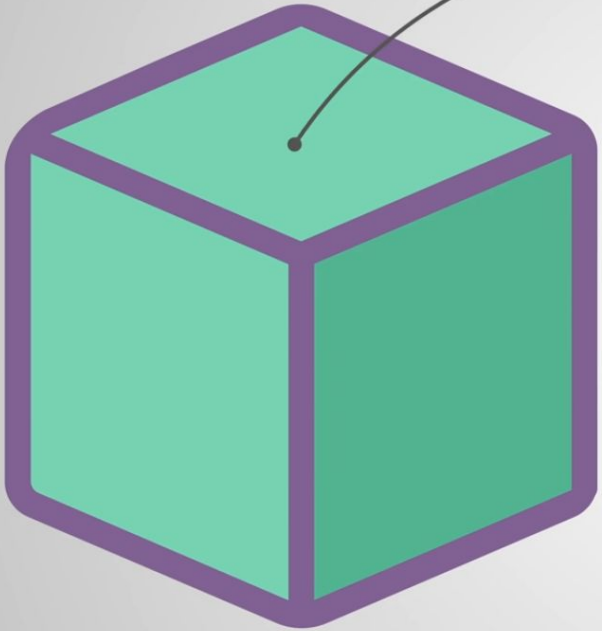
pēc noteikta plāna.

Ekonomikas skaidrojošā vārdnīca. — R., Zinātne, 2000



Bitcoin bloks





Data

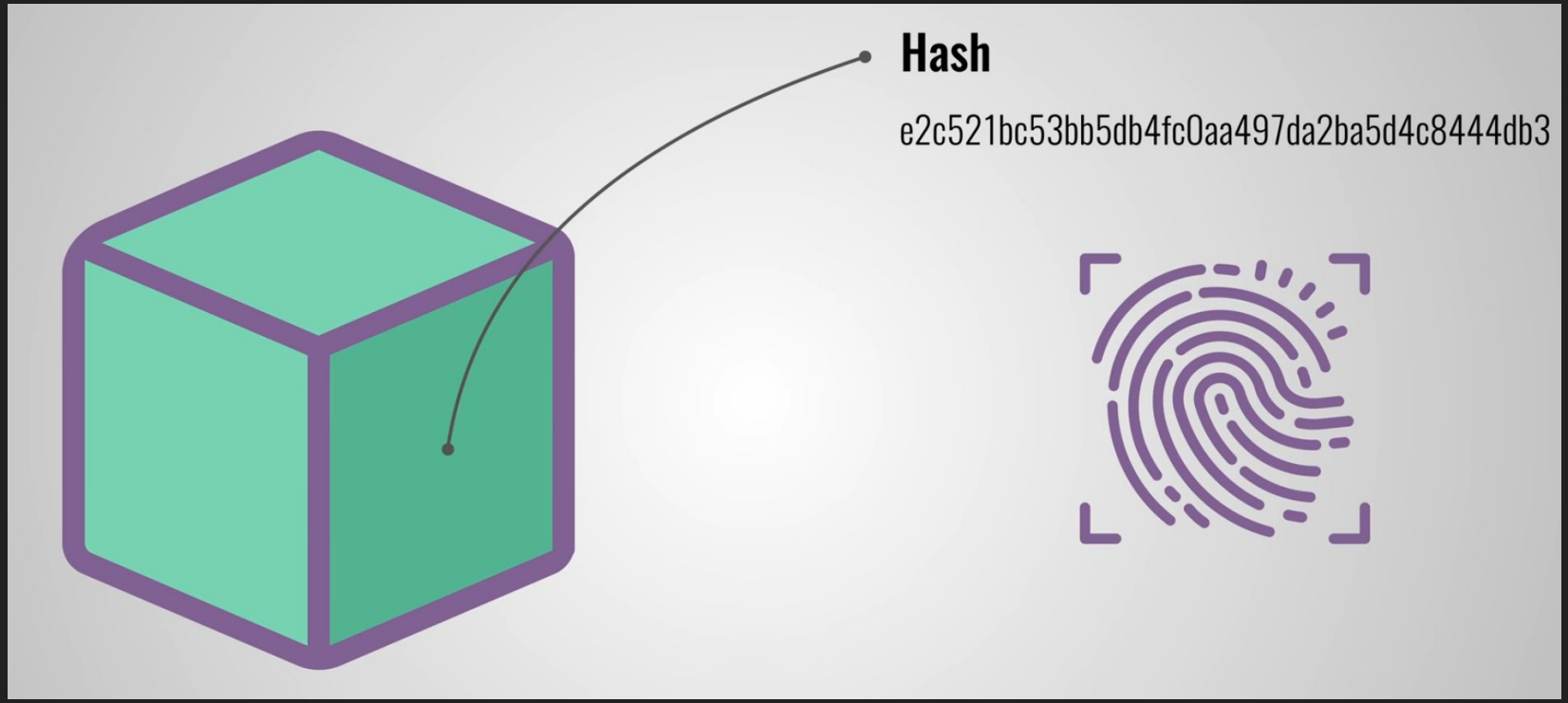
From: 👩

To: 👨

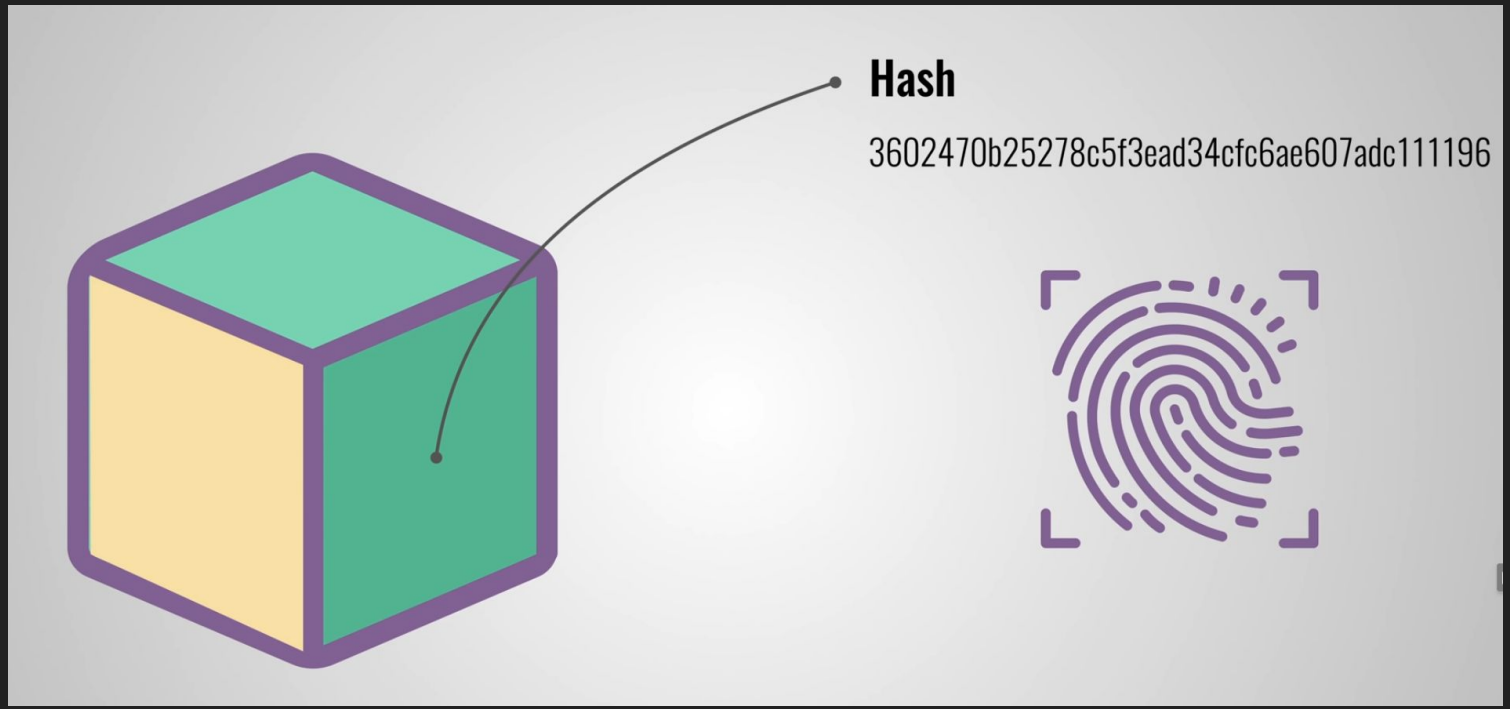
Amount: 💵

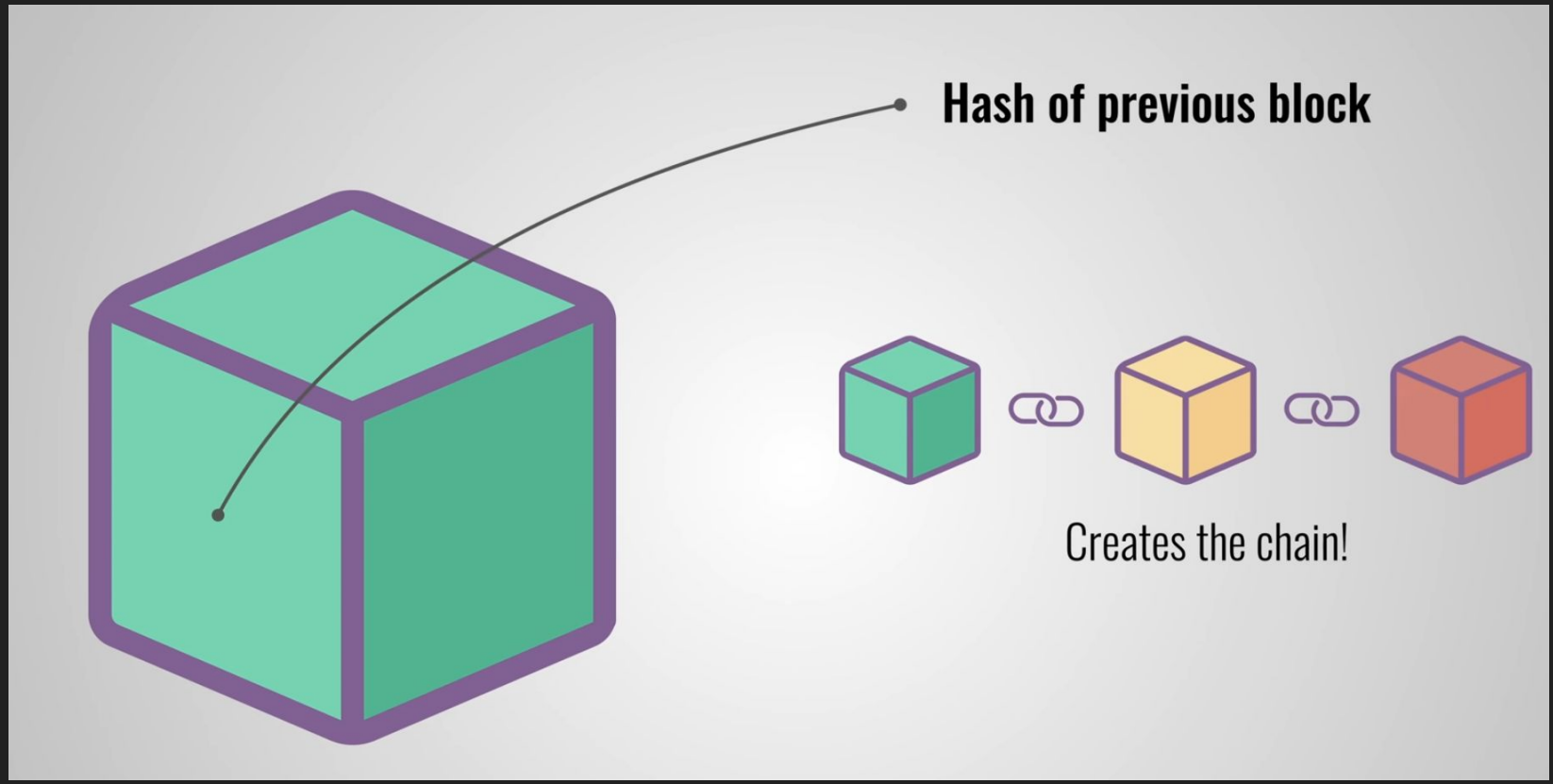
Bitcoin block example

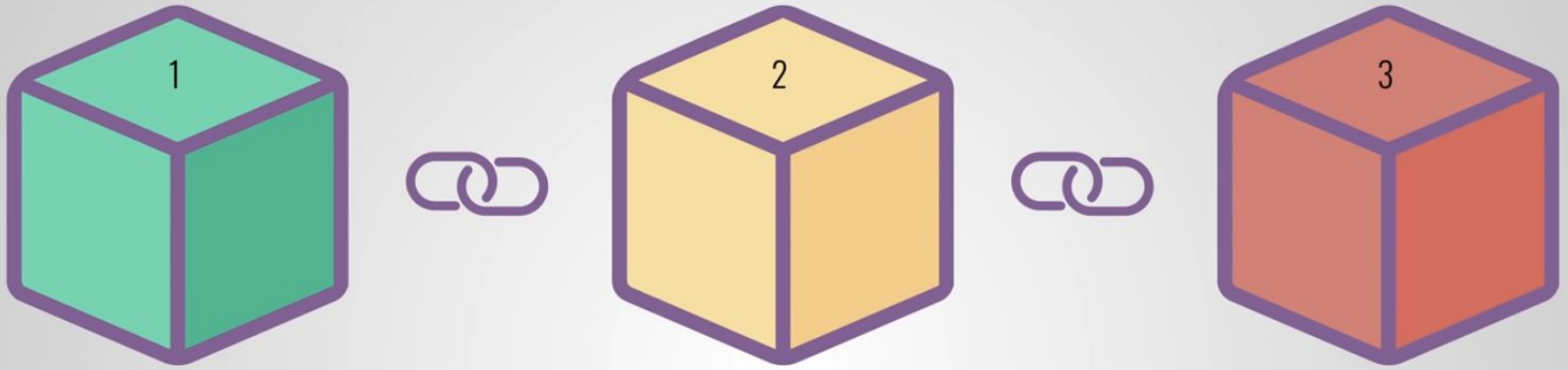
Hash



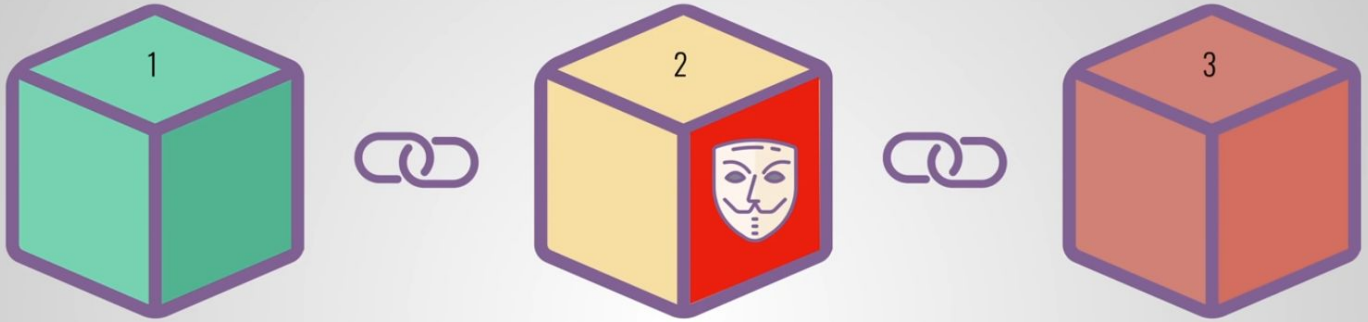
Ja maina datus mainās Hash vērtība




Hash of previous block
Creates the chain!



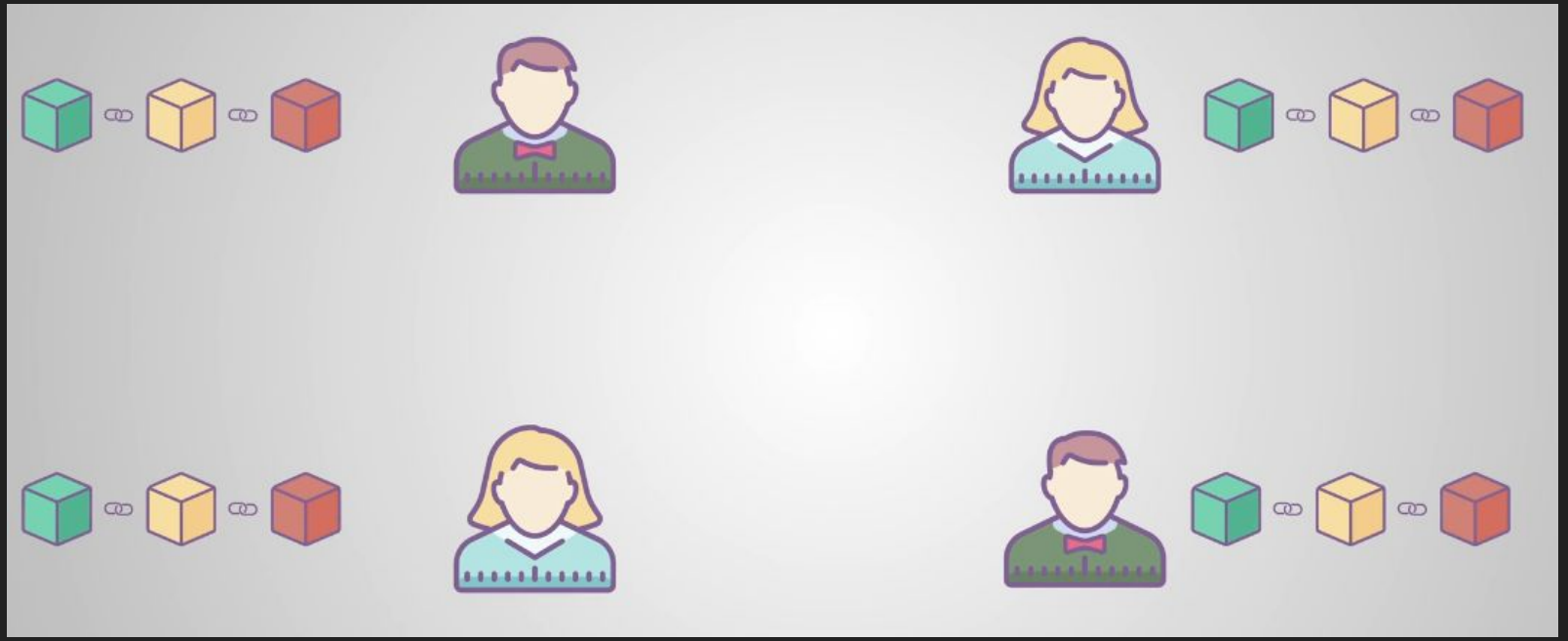
Hash: **1Z8F**	Hash: **6BQ1**	Hash: **3H4Q**
Previous hash: **0000**	Previous hash: **1Z8F**	Previous hash: **6BQ1**

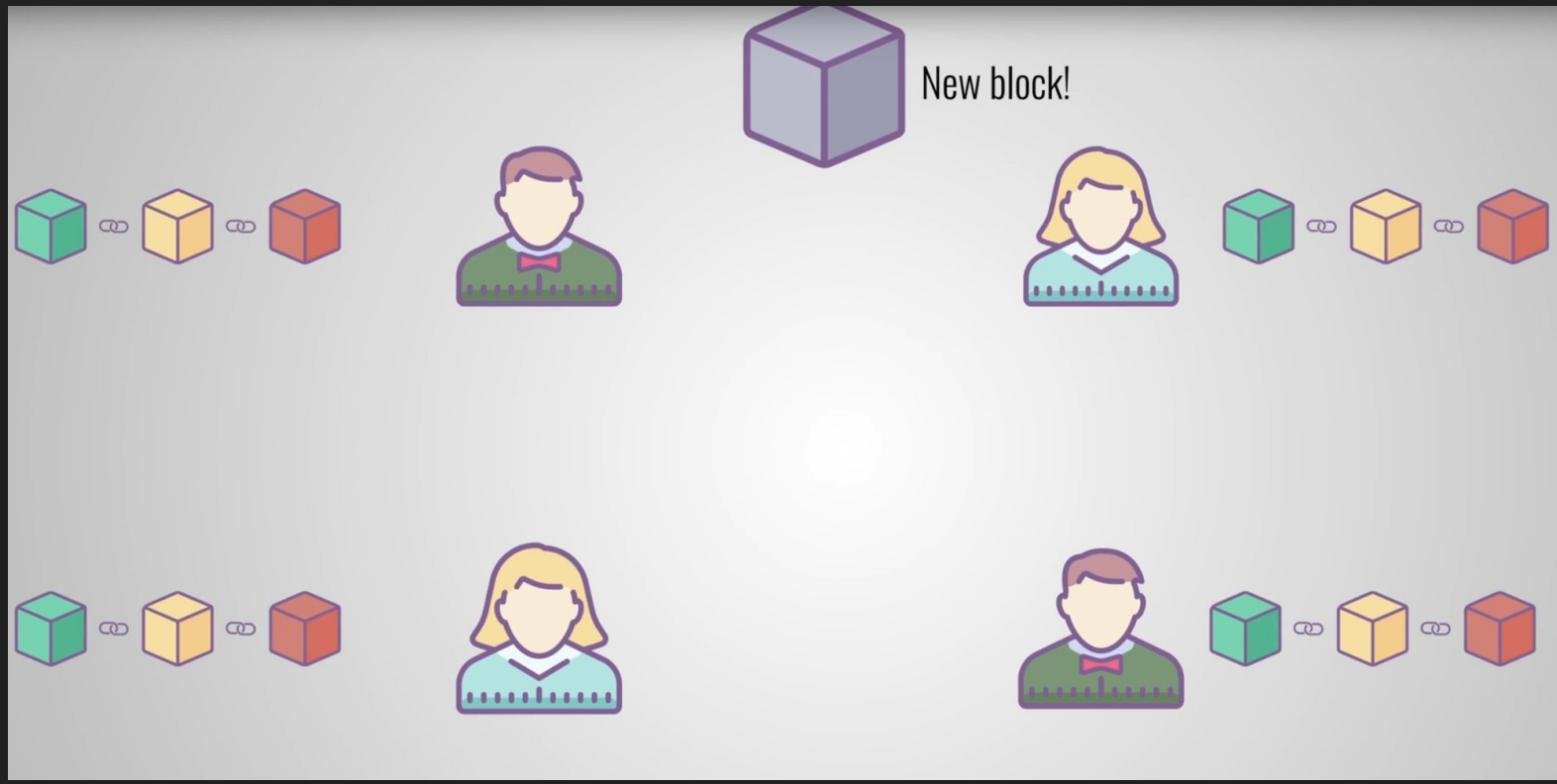


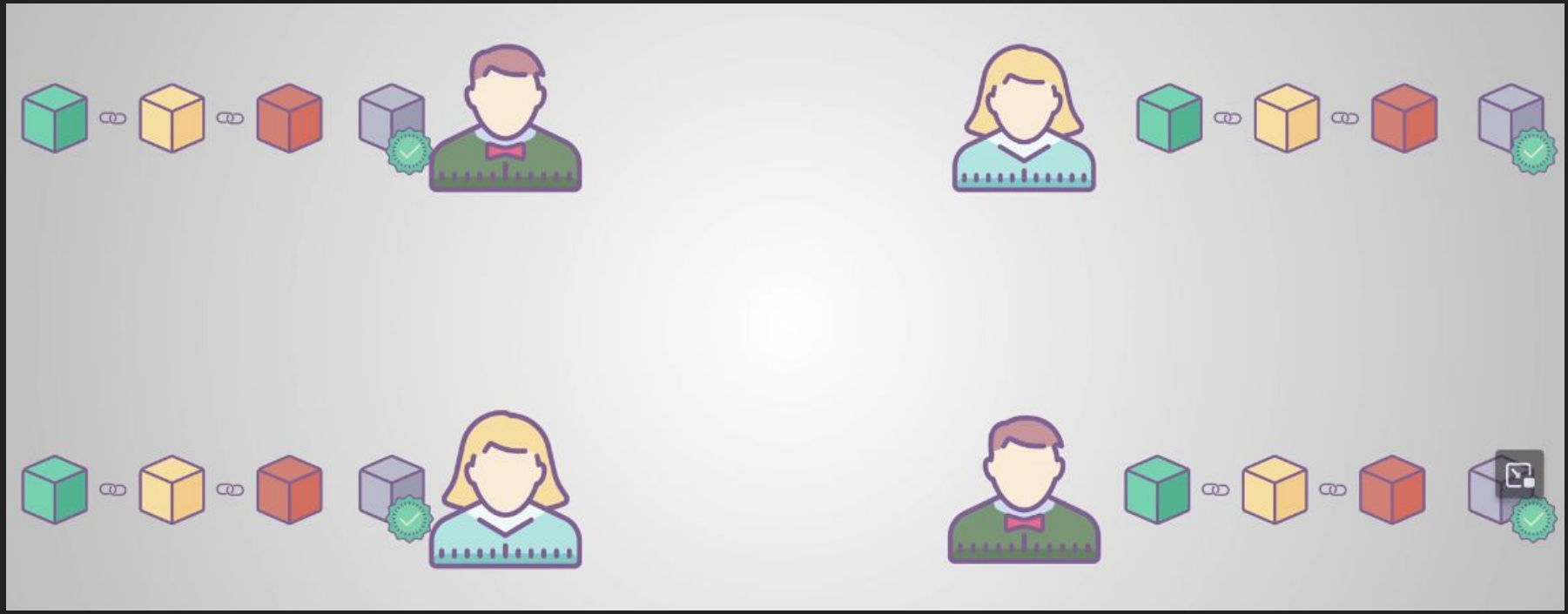
Hash: 1Z8F	Hash: ~~6BQ1~~ H62Y	Hash: 3H4Q
Previous hash: 0000	Previous hash: 1Z8F	Previous hash: 6BQ1

Uh thats not right??

P2P




New block!




Consensus!

Konsenss

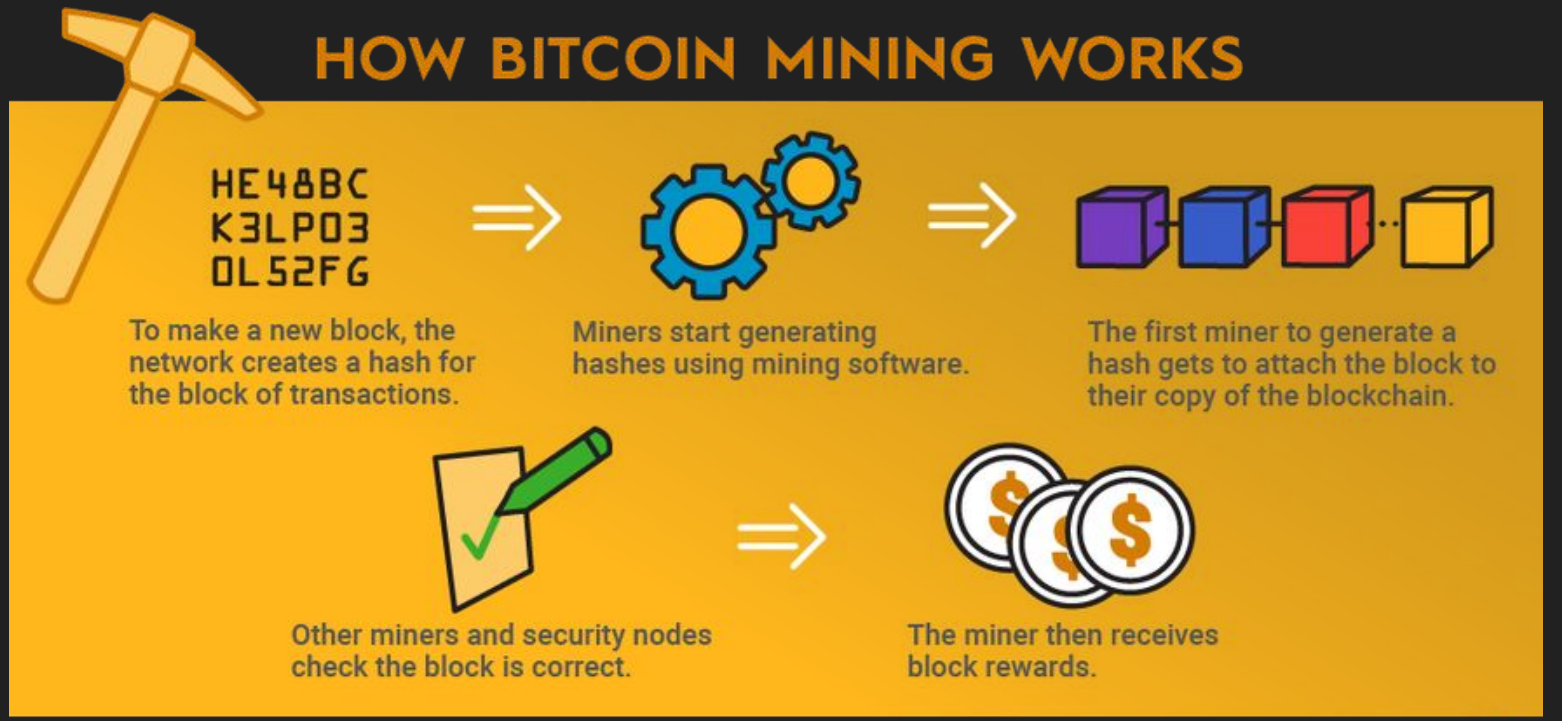
Darījumi tiek pārbaudīti ar konsensu –

dalībnieki savstarpēji apstiprina izmaiņas –

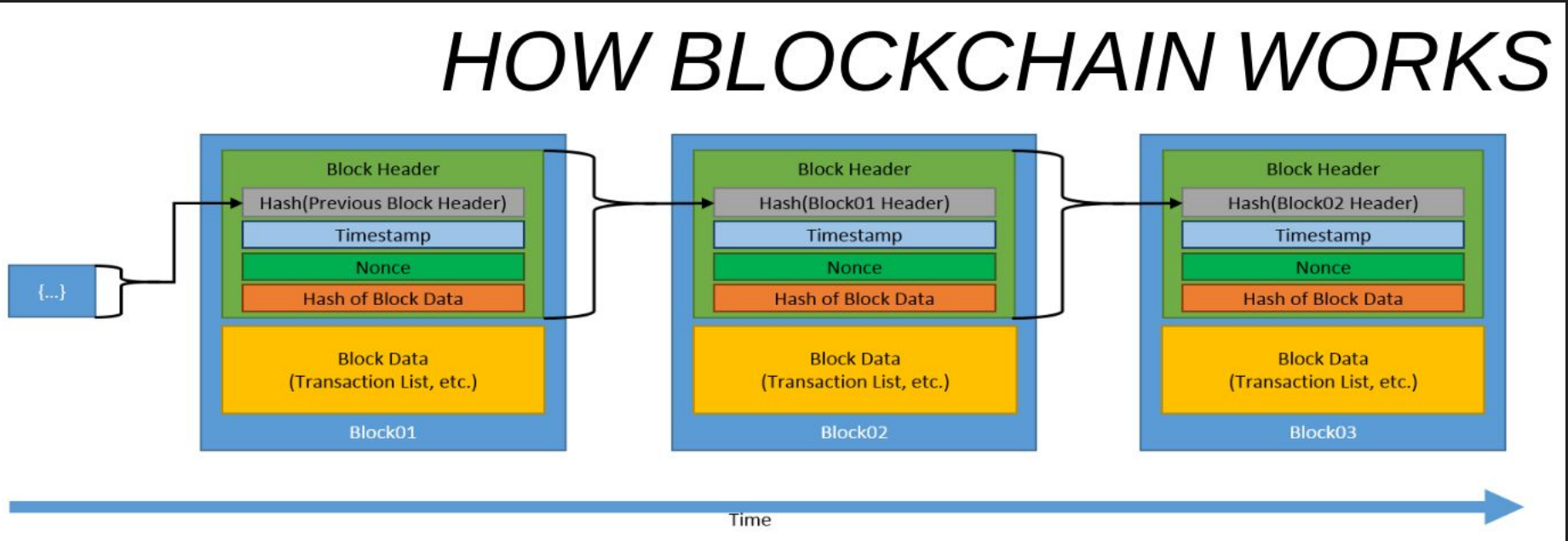
Kriptogrāfija nodrošina informācijas drošību.

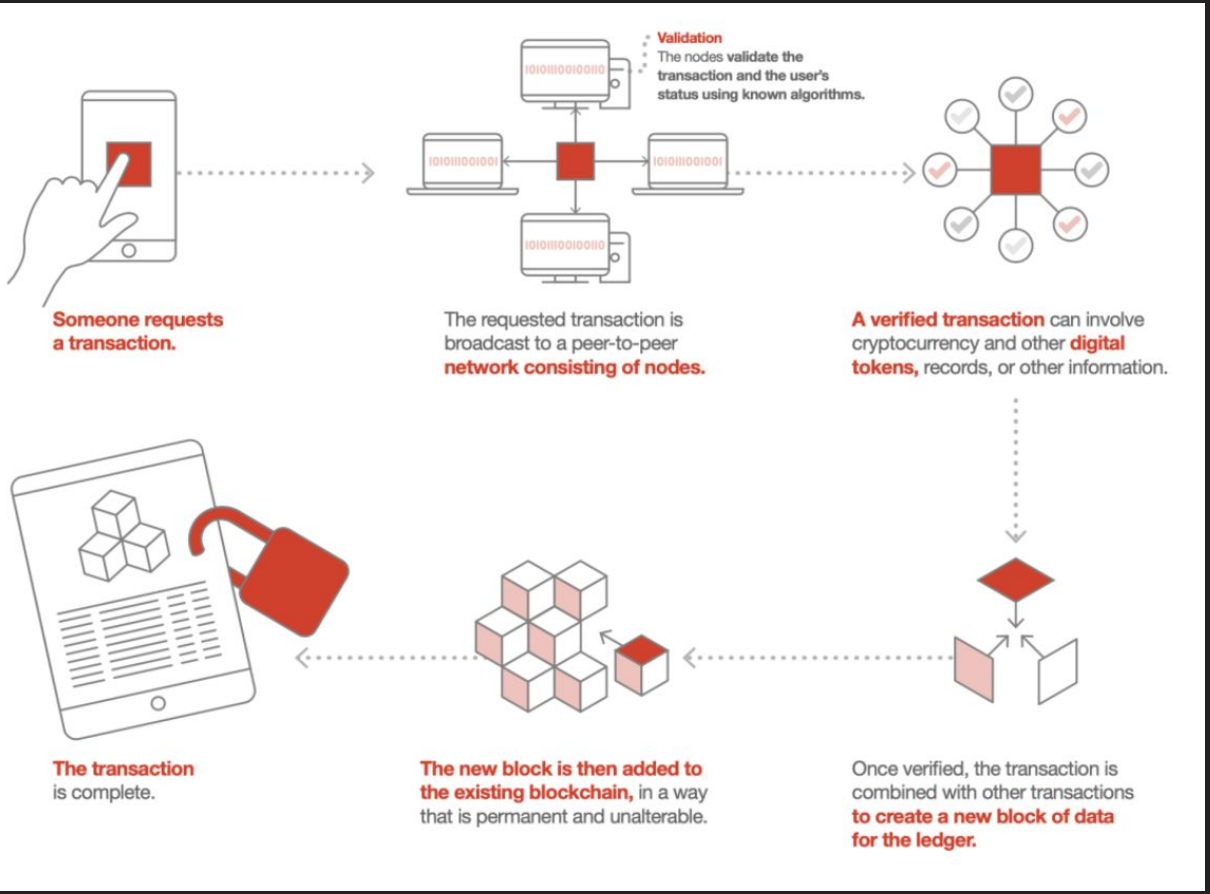
Tādējādi tiek novērsta nepieciešamība pēc centrālās sertifikācijas iestādes.

Bitcoin racēji

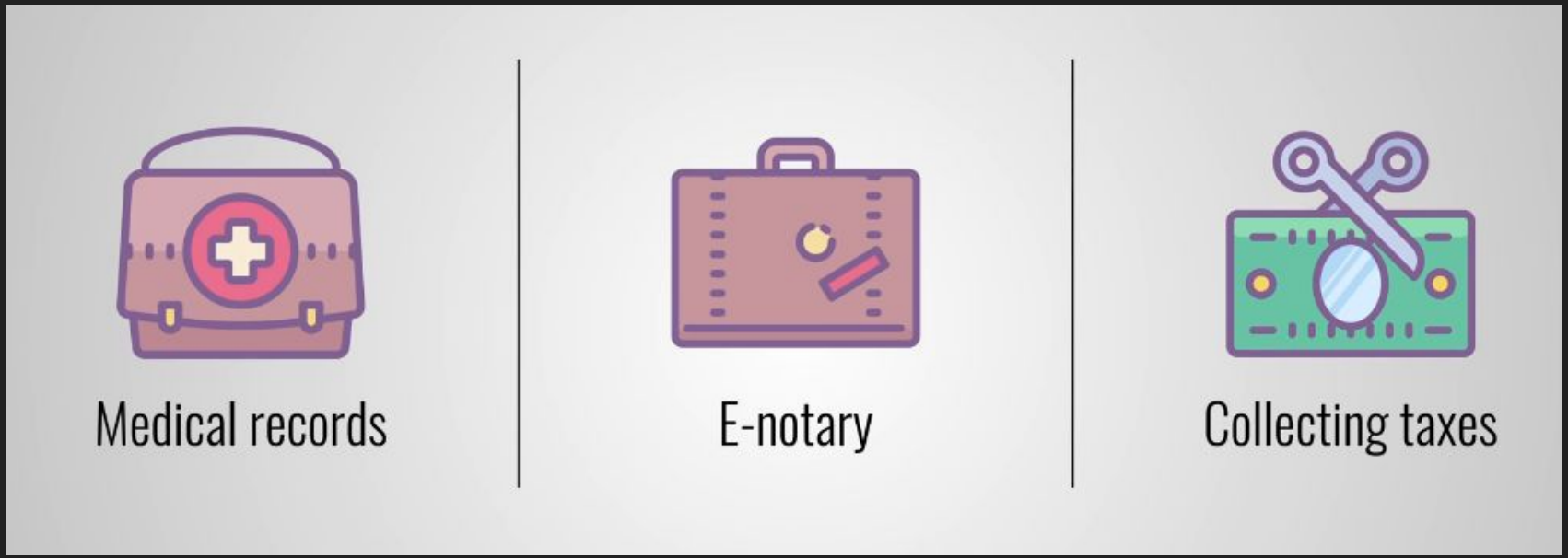


Kā darbojas blokķēde?




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

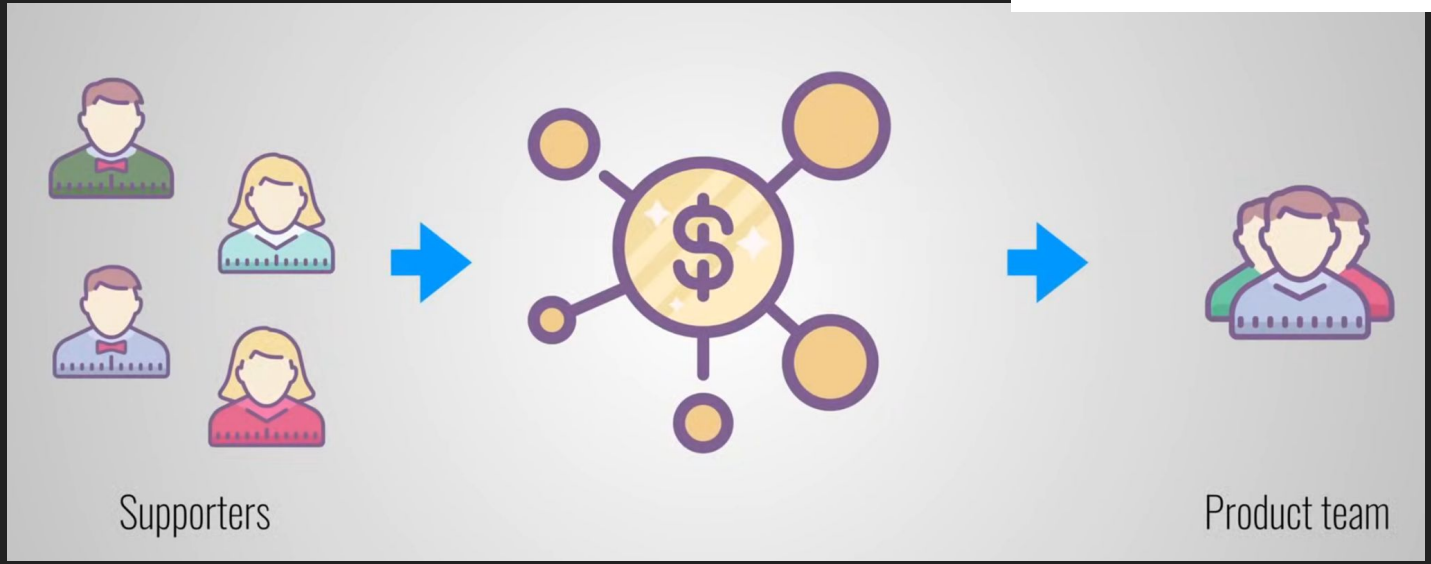


PUBLIC VS PRIVATE

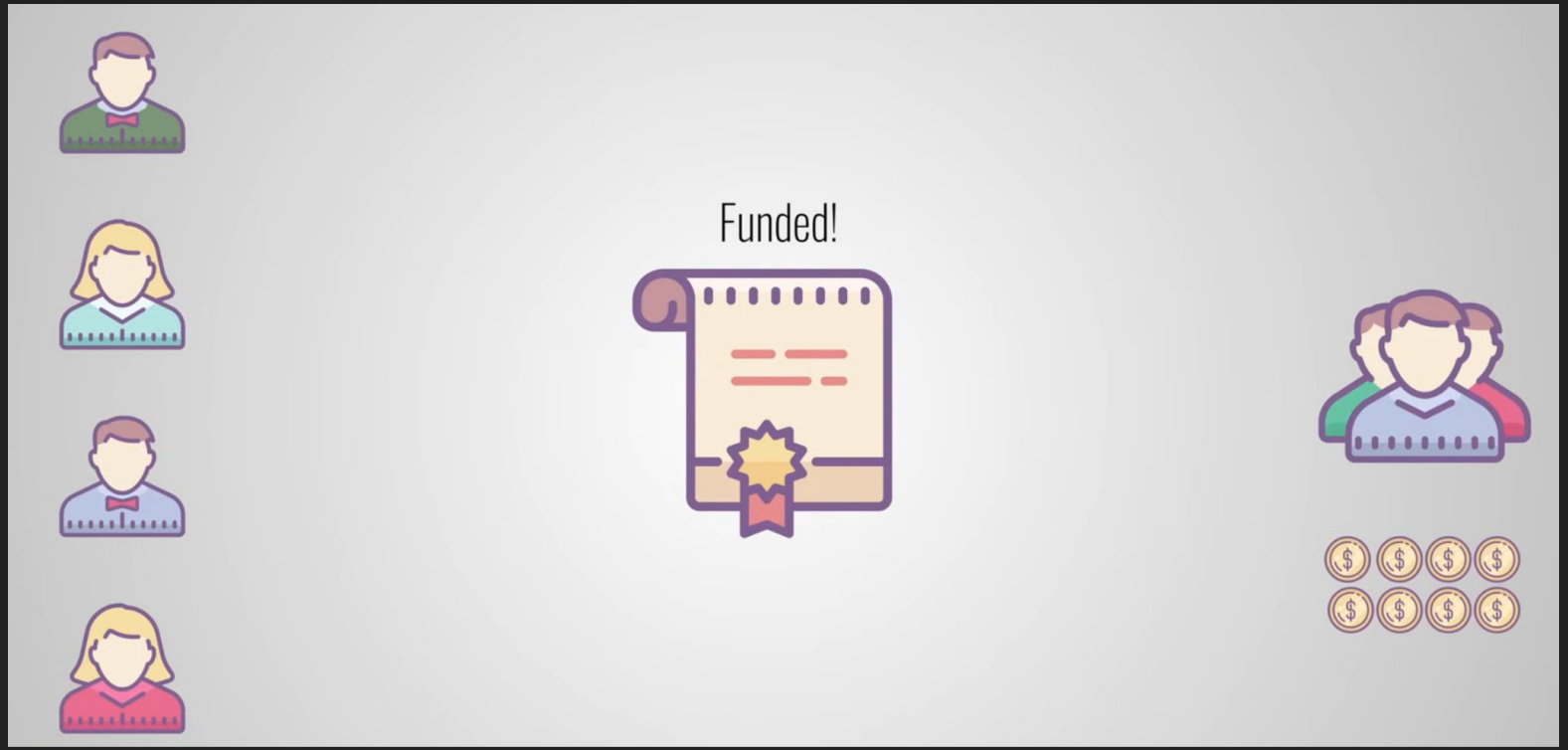
Viedlīgums (Smart contract)

1997.gadā Nick Szabo

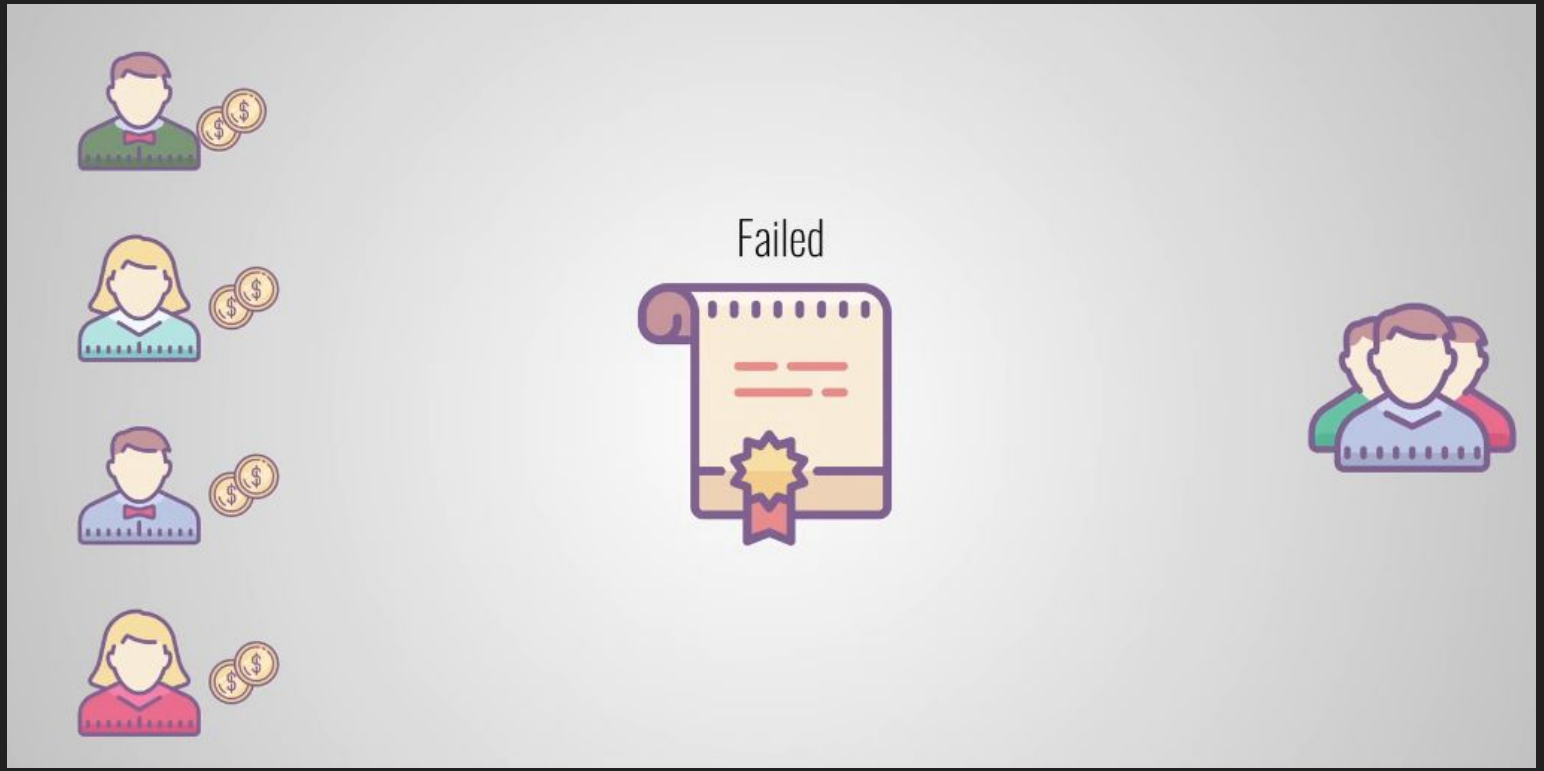
Līdzīgs kolektīvai finansēšanai (crowdfunding)



Izpilda līguma nosacījumus



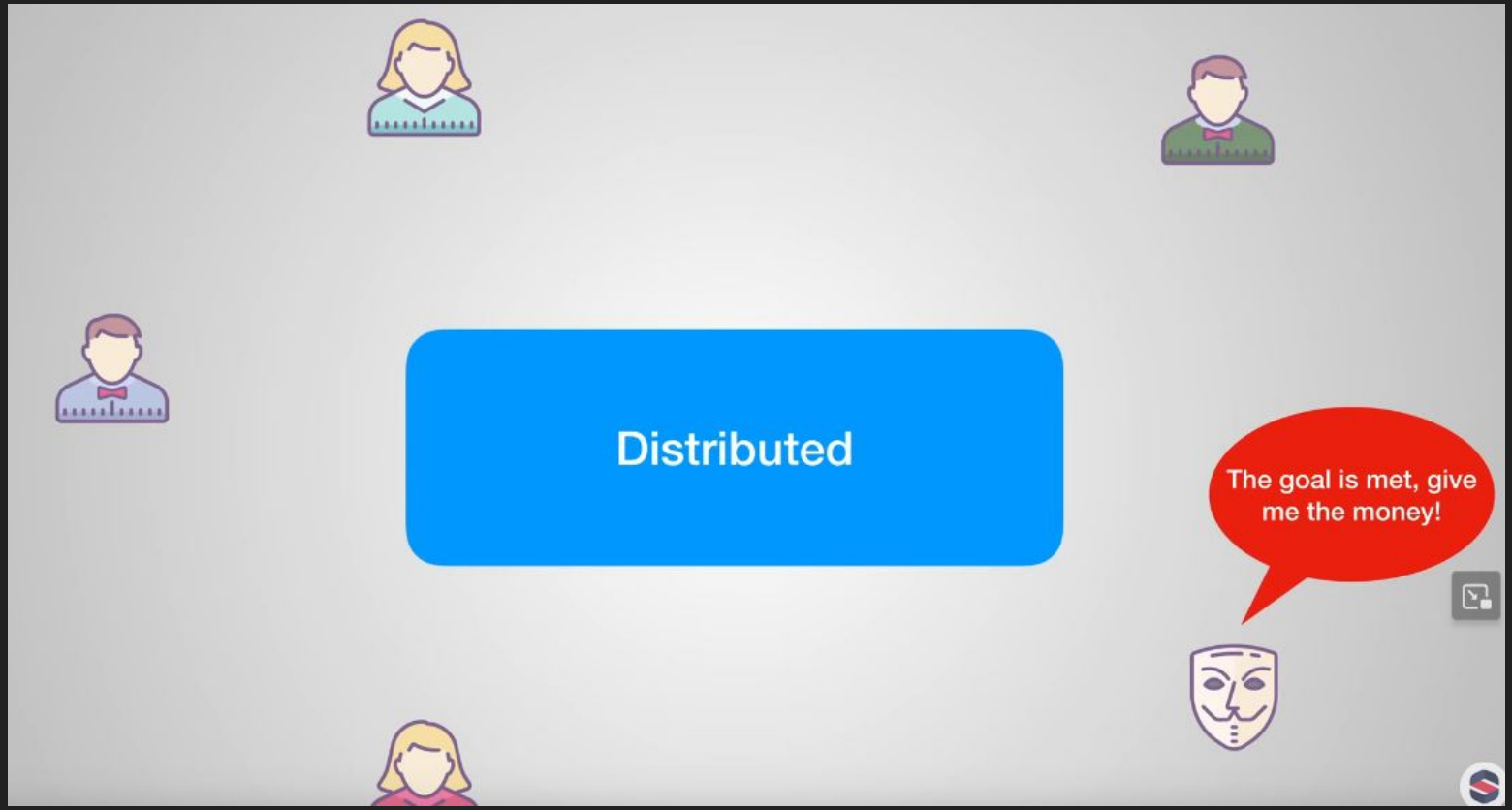
Neizpilda līguma nosacījumus



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

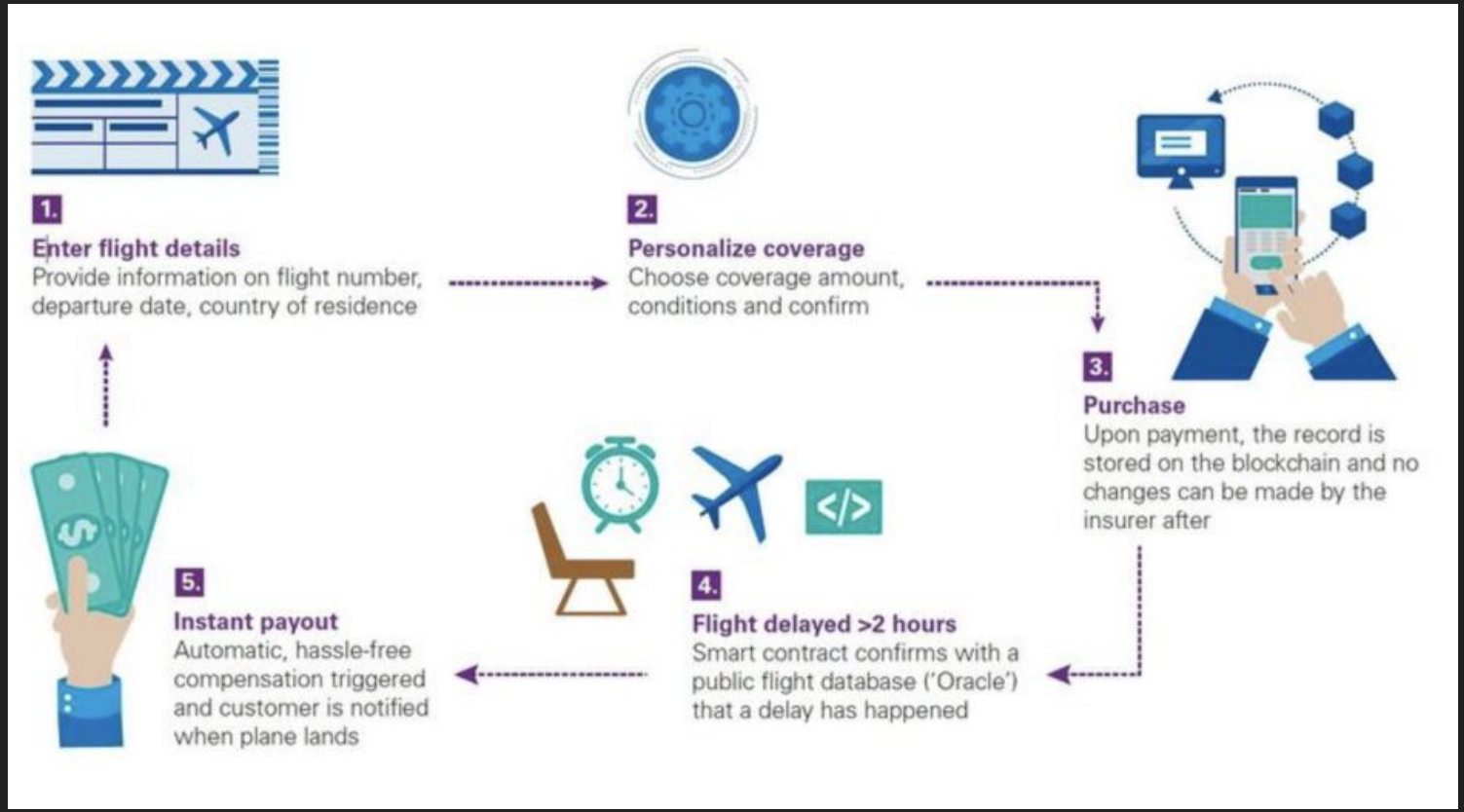
Postal

Payment on delivery

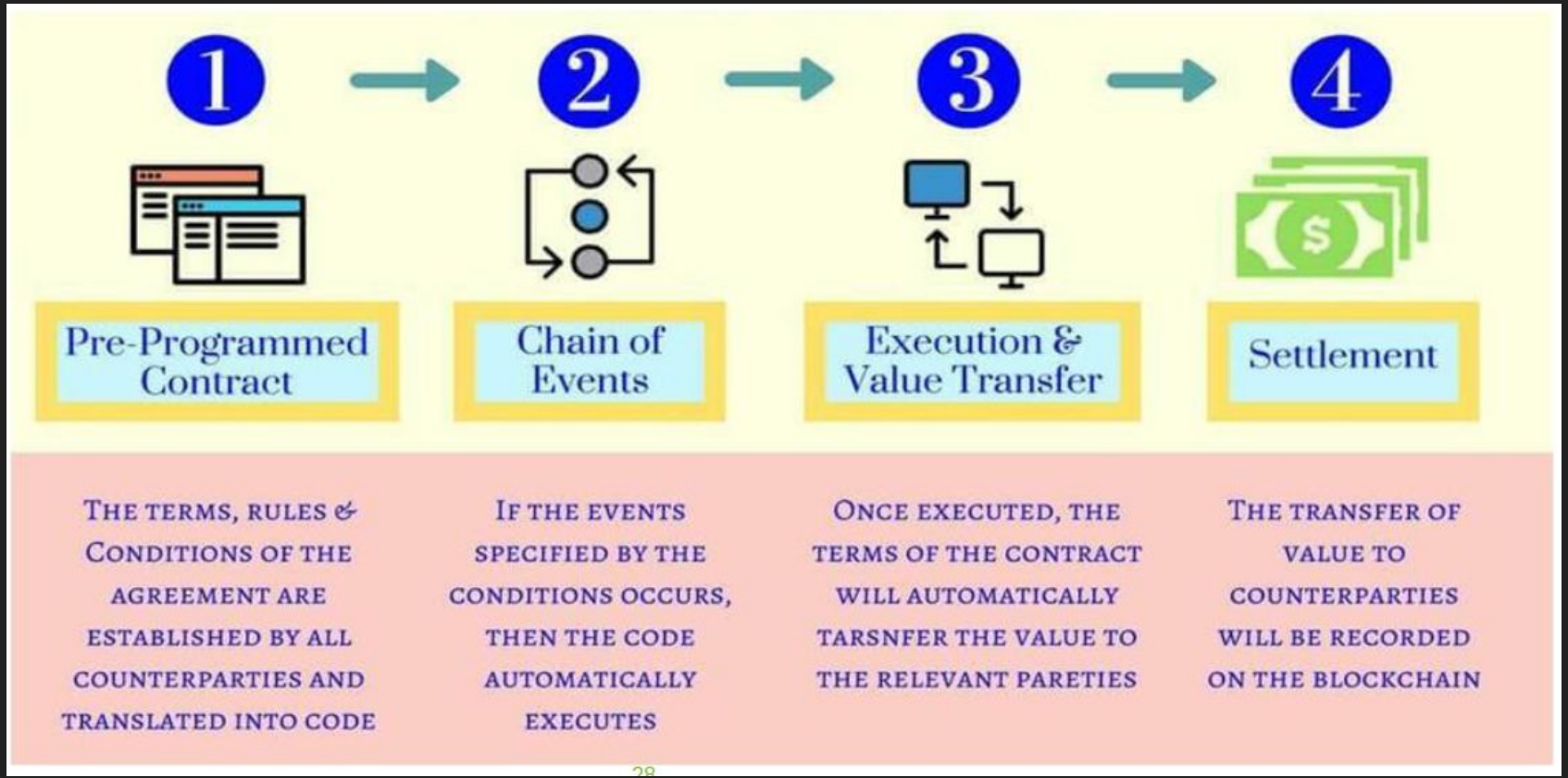
Ethereum

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?