Internet 2.0: De blockchain

Morrison Toussaint
Blockchain Specialist & Security Consultant, Cyber4Z

Blockchain

Cyber4z heeft ervaring in het ontwerpen en implementeren van blockchain in uw organisatie. Wij hebben ontwikkelaars in dienst die perfect maatwerk leveren.

Neem gerust contact op met Morrison Toussaint om te bekijken wat wij voor u en uw organisatie kunnen betekenen.

+31 6 280 35 691

morrison.toussaint@cyber4z.com

Programma

- Introductie
- Wat is blockchain
  - Geschiedenis & achtergrond
  - Technologie
  - Nadelen
- Smart contract
- Toepassingen blockchain
  - Implementatie in het dagelijkse leven
- Vragen

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", *The Times* has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed gurantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

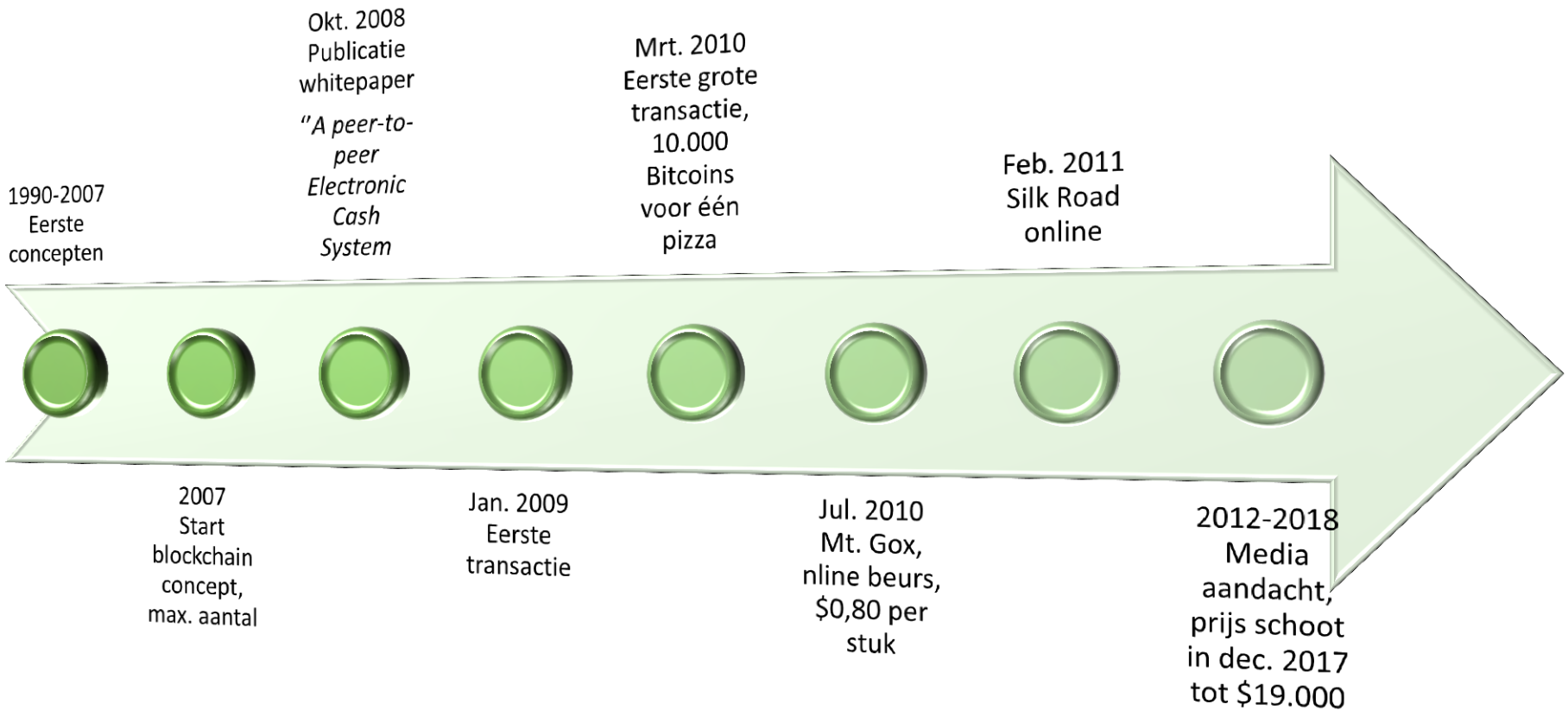
Pub chain cuts the price of a pint from £1.69 to 1989 levels
Business, page 47

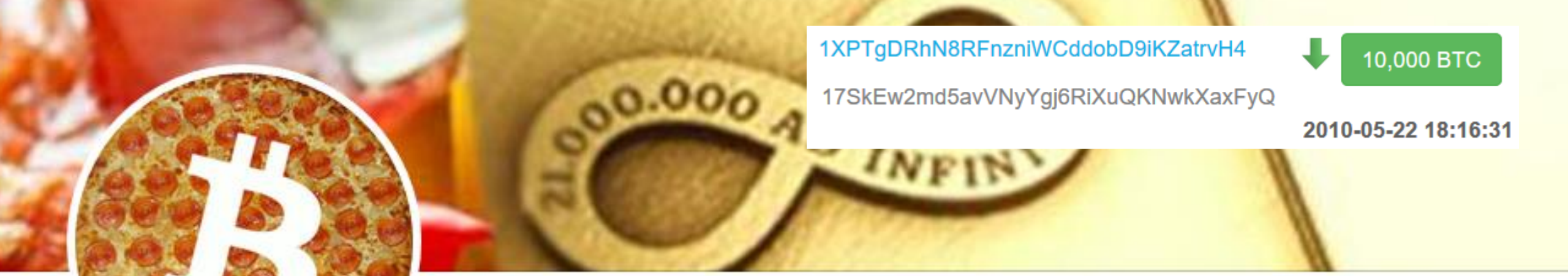
KIVI Engineering Society

IMF INTERNATIONAL MANAGEMENT FORUM

CYBER

Geschiedenis





Tweets 1,410 | Following 3 | Followers 7,416 | Likes 222

Bitcoin Pizza

@bitcoin_pizza

On 22nd May 2010, Laszlo Hanyecz bought a pizza for 10,000 bitcoins. This is the current USD value of that pizza. #bitcoin

Joined January 2015

Tweets Tweets & replies

Bitcoin Pizza @bitcoin_pizza · 13h
The #Bitcoin pizza is worth $63,961,650 today. (+0.42% from yesterday)
1 3

Bitcoin Pizza @bitcoin_pizza · Nov 10
The #Bitcoin pizza is worth $63,695,850 today. (+0.13% from yesterday)
1 2

Bitcoin Pizza @bitcoin_pizza · Nov 9
The #Bitcoin pizza is worth $63,614,725 today. (-0.93% from yesterday)

Technologische revolutie

Internet of Things

Social media

Robotica

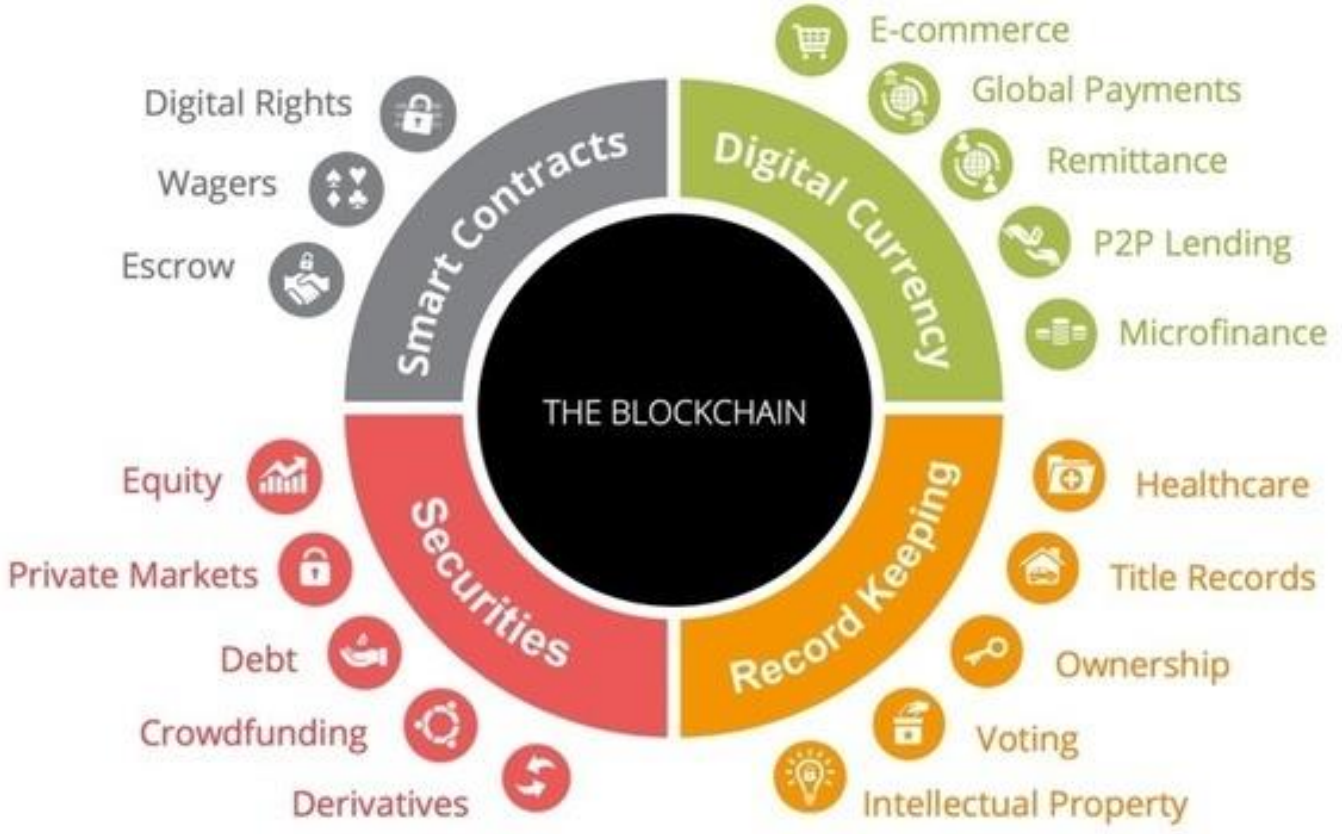
Machine learning

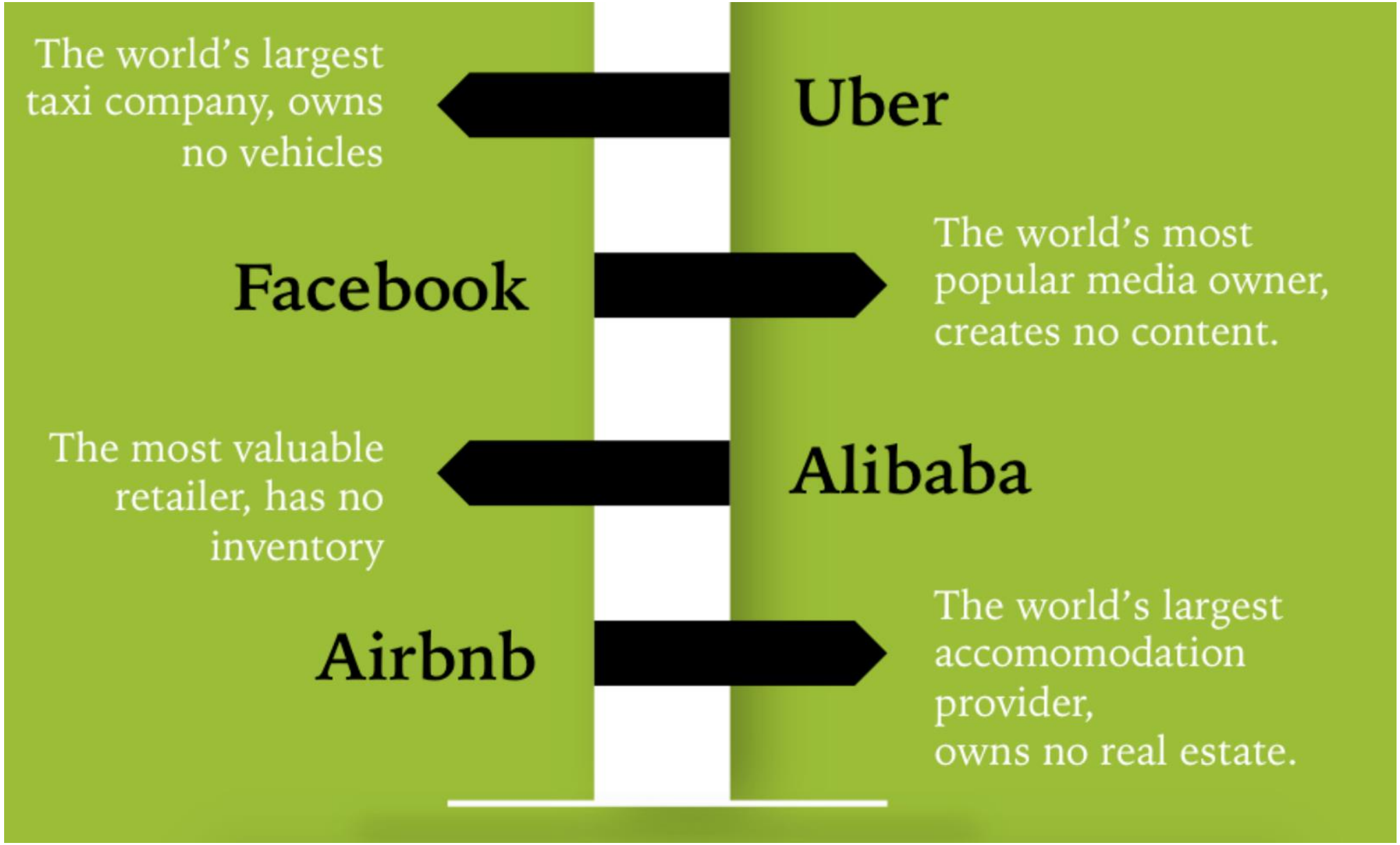
Big data

Drones

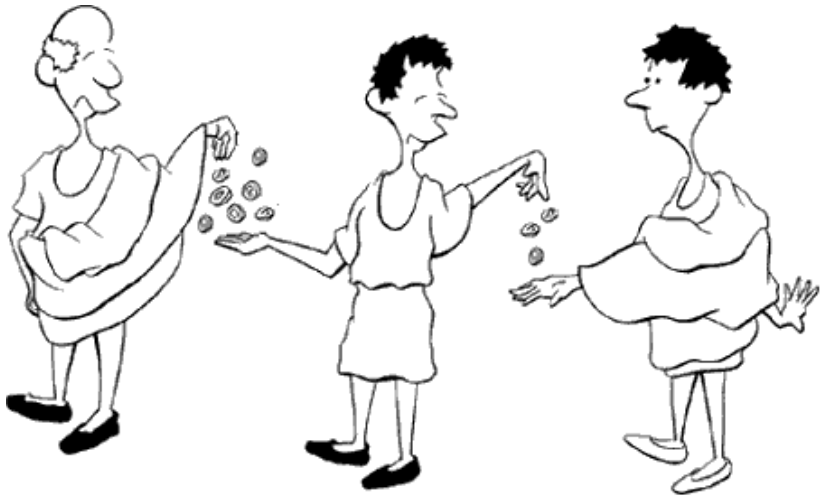
The cloud

Internet 2.0 – Blockchain: Informatie en waarde



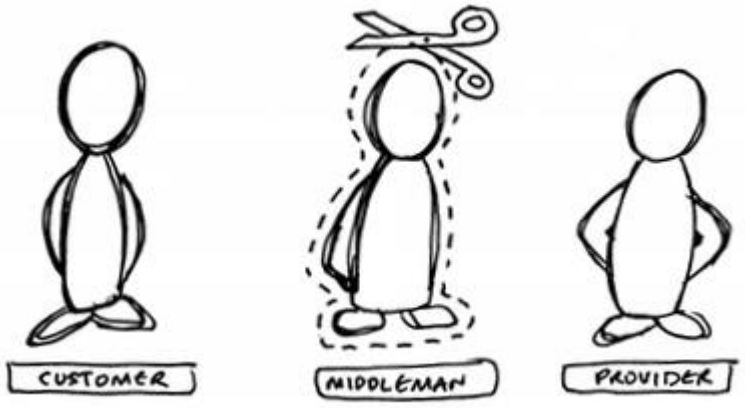

The world's largest taxi company, owns no vehicles
Uber
Facebook
The world's most popular media owner, creates no content.
The most valuable retailer, has no inventory
Alibaba
Airbnb
The world's largest accomomodation provider, owns no real estate.

Intermediair



Old School

New School



Gecentraliseerde tussenpartij - Bank

Autoriteit	→	Alleenrecht
Uitsluiting	→	2.5 miljard
Doelwit	→	DDoS
Technologie	→	Oud, Swift

Decentraal uitgangspunt - Bitcoin

Autoriteit	→	Geen
Uitsluiting	→	Geen
Doelwit	→	51%
Technologie	→	State-of-the-art

Blockchain

- Blockchain is een decentraal gedistribueerd systeem met de taak om iedere vorm van transacties vast te leggen op een wijze waardoor gemaakte transacties niet manipuleerbaar zijn.

- Beste vergelijking: een grootboek met de transactiegeschiedenis, maar nu zonder mogelijkheid om de 'geschiedenis' te veranderen.

Centrale autoriteit

- Bank
- Kickstarter
- Spotify

Decentrale autoriteit

- Franchise
- Open source software

Decentraal gedistribueerd

(•) Anoniem

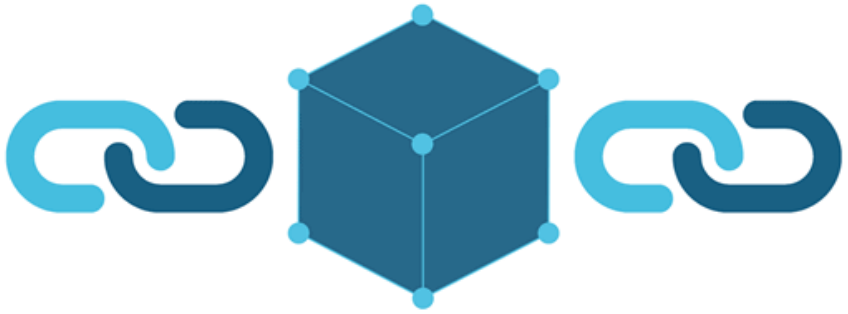
- Publieke blockchain
- Bitcoin

(•) Niet anoniem

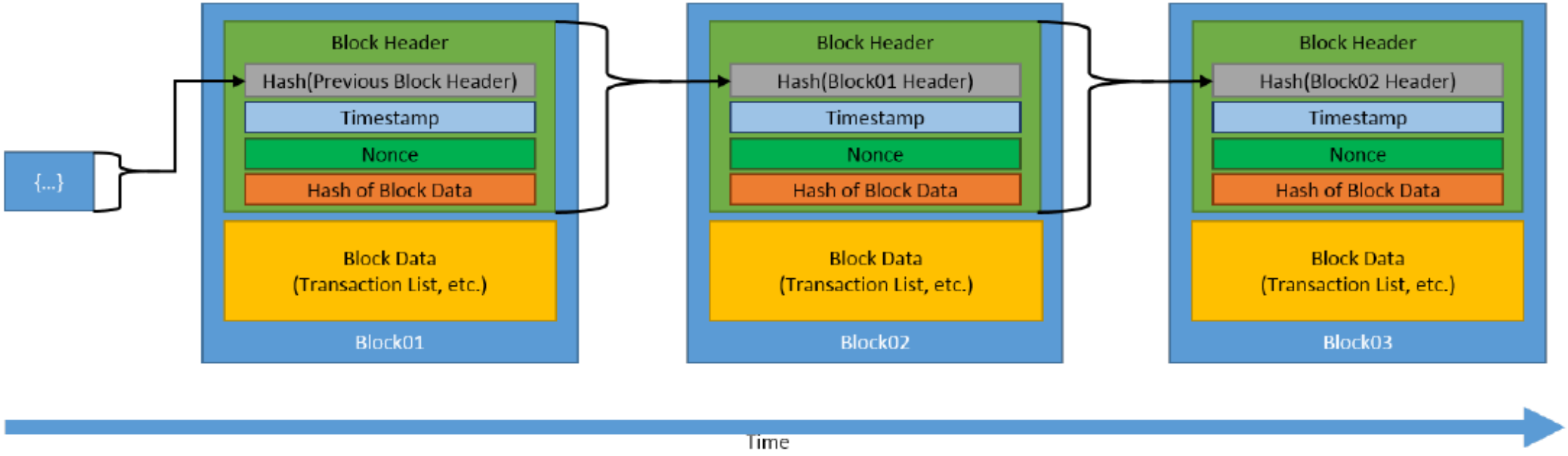
- Private blockchain
- Bedrijfsoplossingen

Opbouw blockchain

- Transacties, bestanden, rechten of andere gegevens worden in een block gestopt
- Block: onveranderlijke, opeenvolgende reeks records
- Transacties worden aan elkaar geketend d.m.v. cryptografie

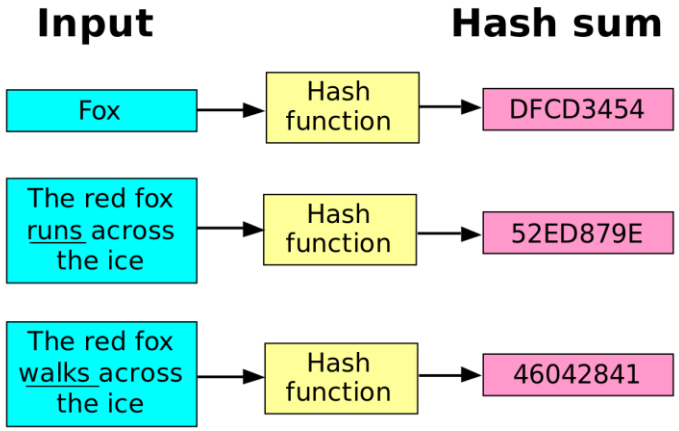


Opbouw blockchain - componenten



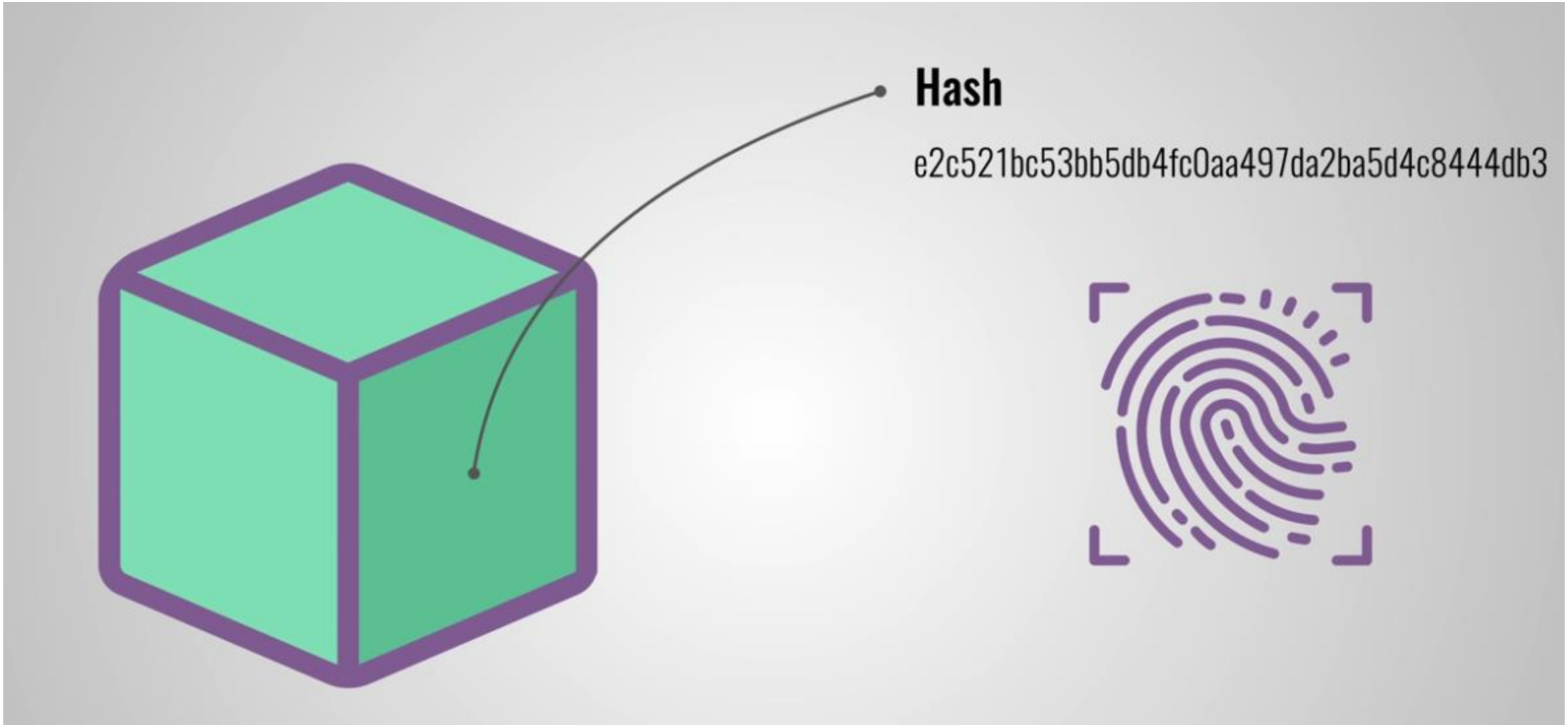
Wat maakt een blockchain onveranderlijk?

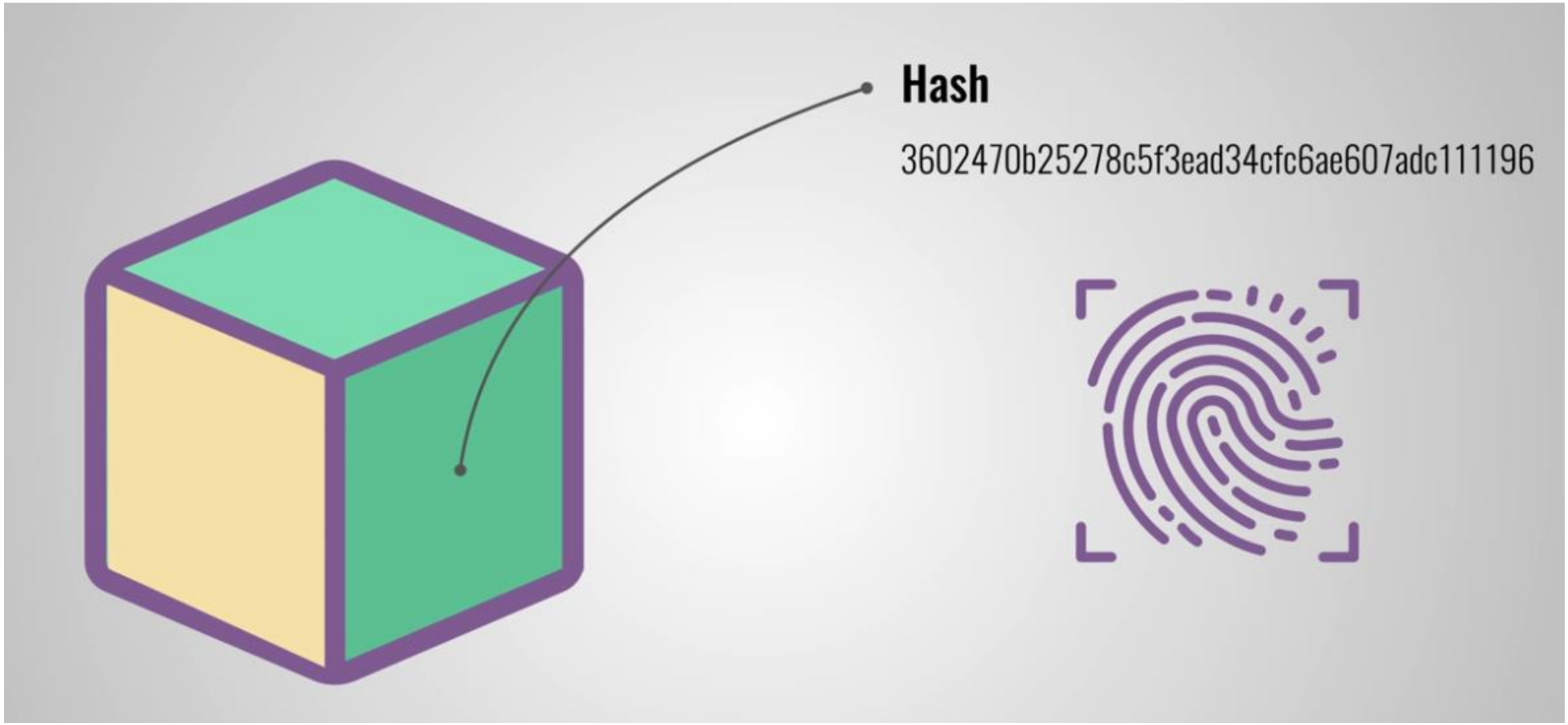
De hash

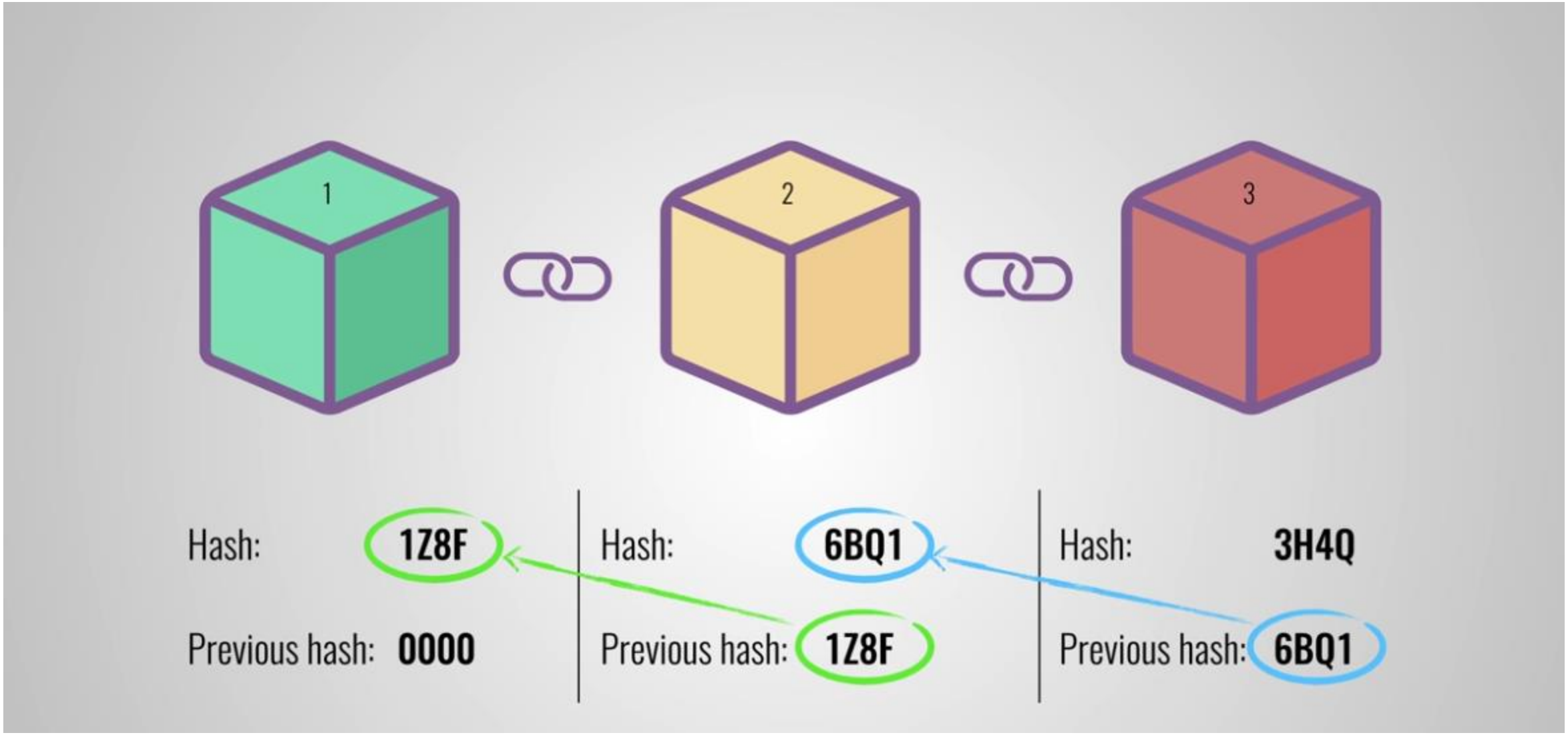


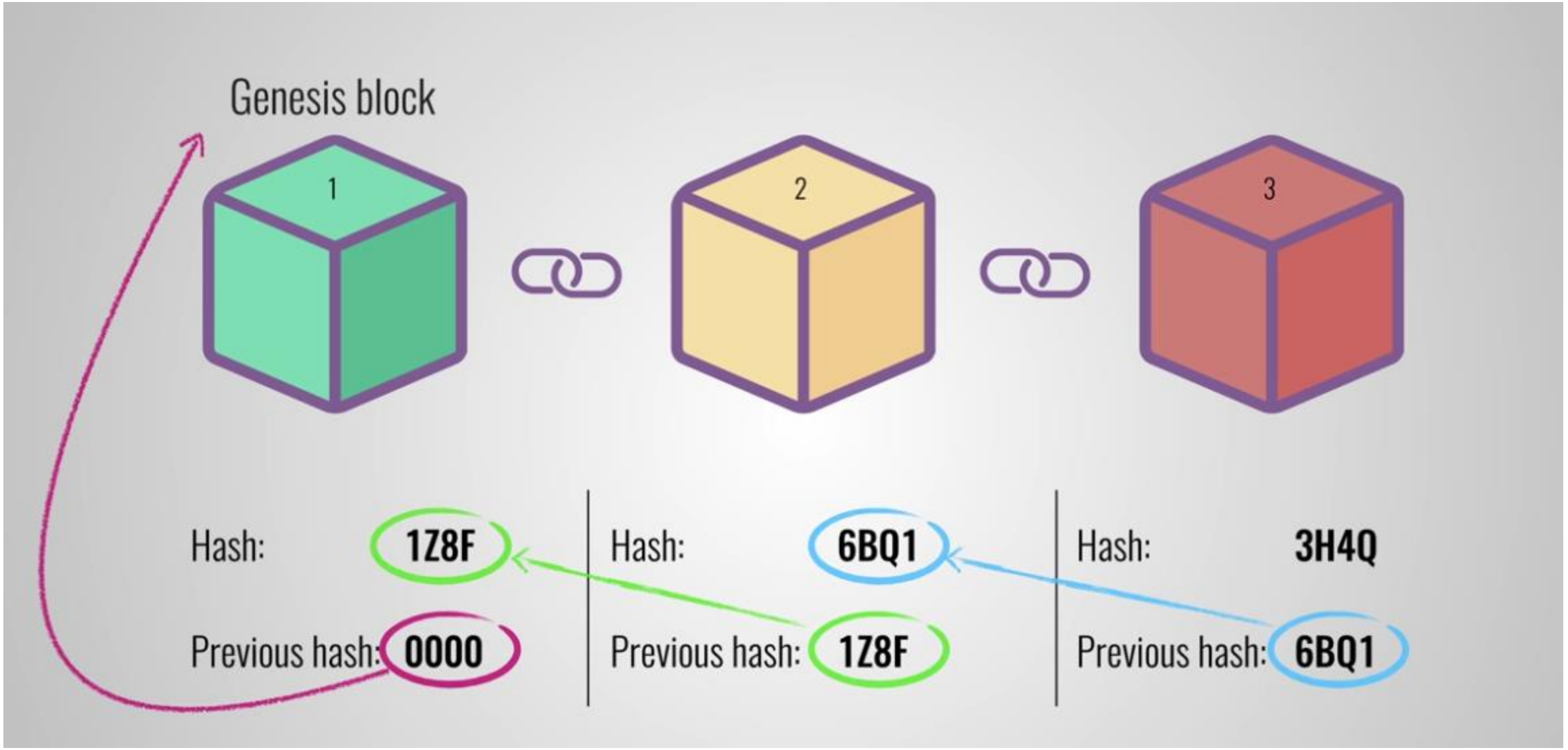
Proof of Work

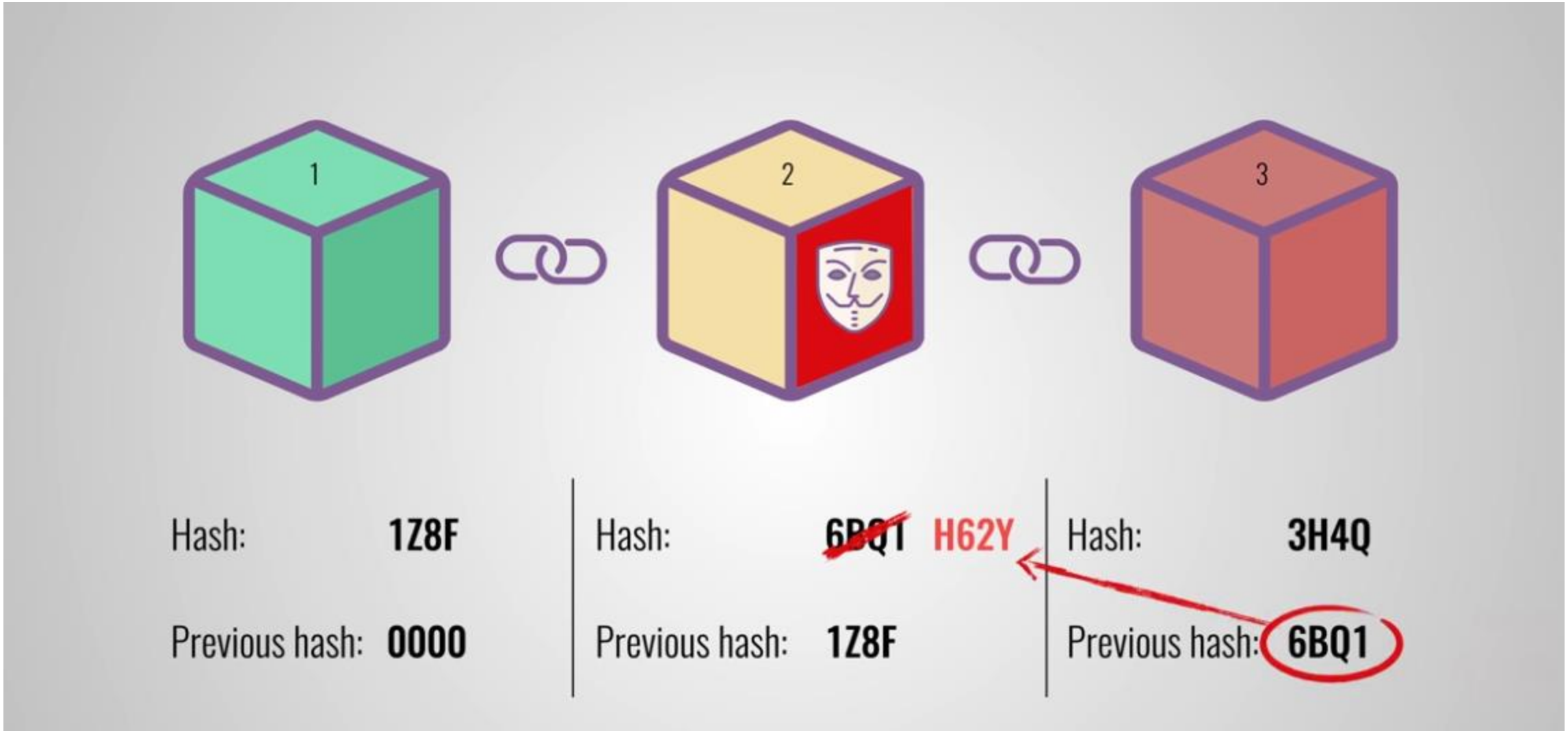
Peer-to-peer


Hash
e2c521bc53bb5db4fc0aa497da2ba5d4c8444db3

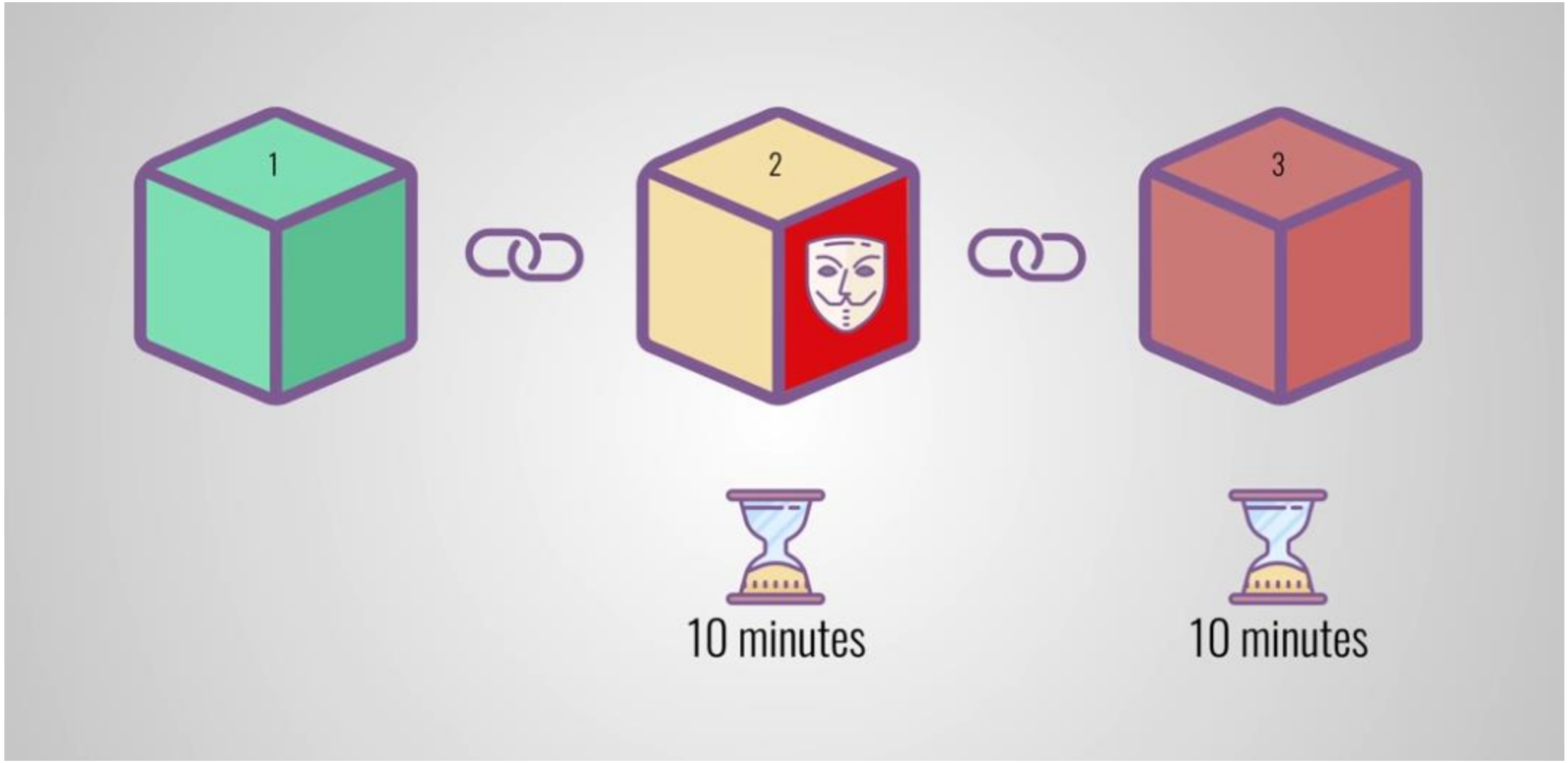

Hash
3602470b25278c5f3ead34cfc6ae607adc111196


1
2
3
Hash:
1Z8F
Previous hash:
0000
Hash:
6BQ1
Previous hash:
1Z8F
Hash:
3H4Q
Previous hash:
6BQ1

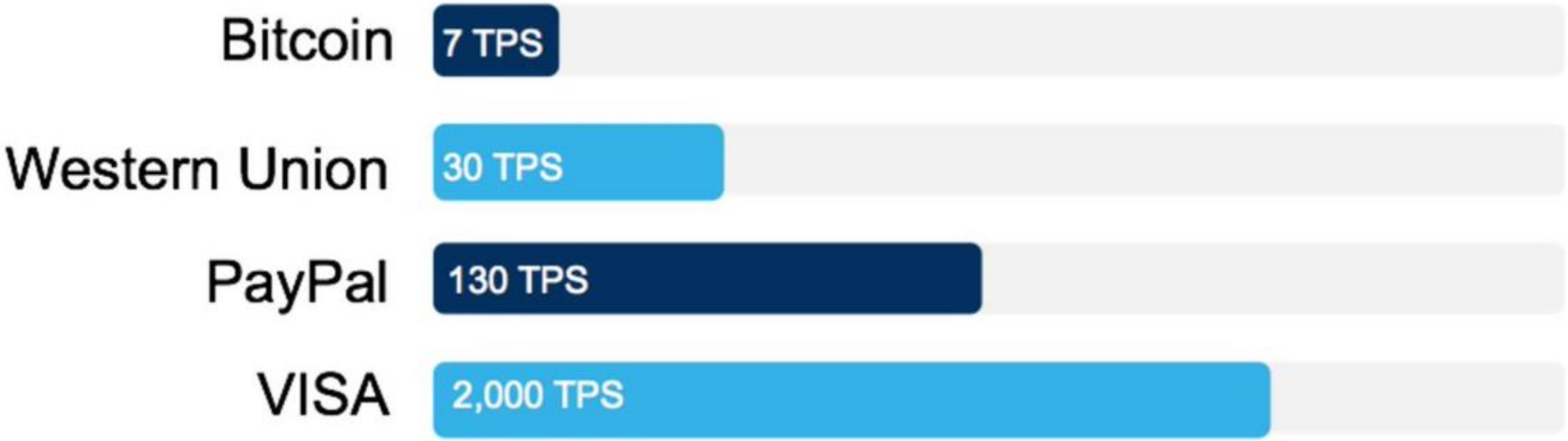

Genesis block
1
2
3
Hash:
1Z8F
Previous hash:
0000
Hash:
6BQ1
Previous hash:
1Z8F
Hash:
3H4Q
Previous hash:
6BQ1


1
2
3
Hash: 1Z8F
Previous hash: 0000
Hash: 6BQ1 H62Y
Previous hash: 1Z8F
Hash: 3H4Q
Previous hash: 6BQ1

Slow and steady...


1
2
3
10 minutes
10 minutes

Blockchain proof of work - schaalbaarheid



Minen rendabel?

Weer op voorraad (beperkte aanbieding)

Radiant

Goud

Starter

$255.00

1 TH/s

Waarom wordt er nog gemined?

- Verificatie transacties
- Maken van nieuwe blocks en deze ketenen
- Grote miningpools zijn nog steeds winst-gevend (China en IJsland)
- Staan achter principe

Weer op voorraad (beperkte aanbieding)

Radiant

Platina

Beste koop

$1,250.00

5 TH/s

	Coins	Dollars	Dollars
per Day	0.00003766 BTC	$0.24	$0.22
per Week	0.00026360 BTC	$1.69	$1.57
per Month	0.00114620 BTC	$7.33	$6.81

	Coins	Dollars	Dollars
per Day	0.00018829 BTC	$1.20	$1.12
per Week	0.00131801 BTC	$8.43	$7.83
per Month	0.00573101 BTC	$36.63	$34.05

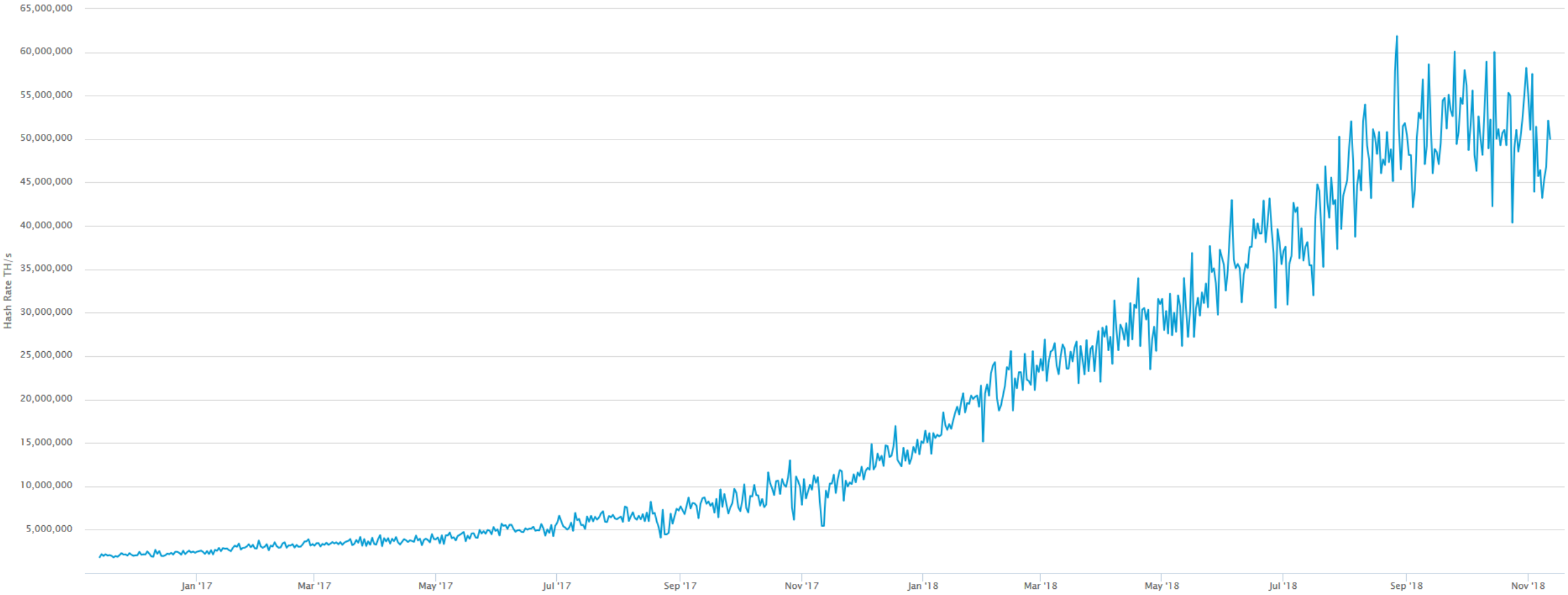
Proof of work

- Minen vindt plaats door een cryptografische puzzel op te lossen
- Miljoenen berekeningen per seconde

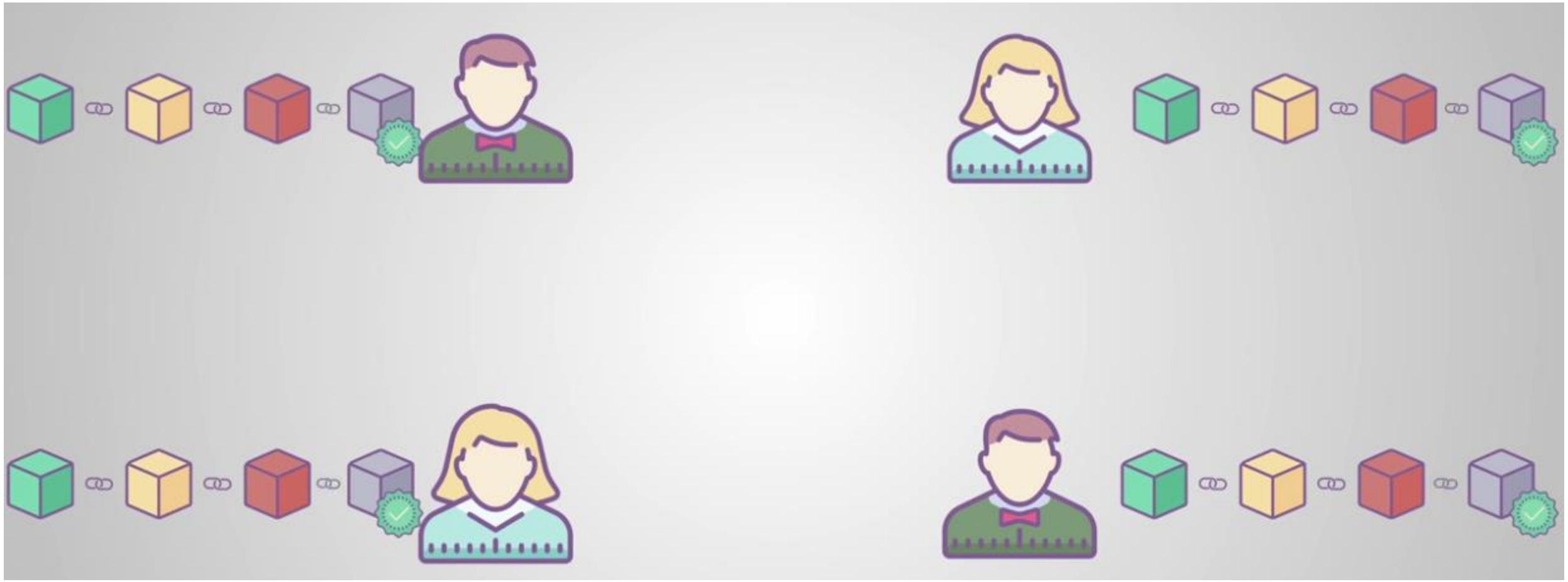
```
Challenge input: Cheesecake
Difficulty: Find a hash beginning with the letter "A"
Try 1: Cheesecake843053191528 - waJo9CULAjVMwVE4or1rpNUfi2mIasiEhL+XDHh+TKg=
Try 2: Cheesecake405291510419 - 4AYa82setWdp97Jd2qyXz0vw7StkcoWd+E51afqMyDw=
…
Try 15: Cheesecake513710455304 - A0SEQ/HRrRBtggh1igyxfkO4iZNkZZyrzjGZkN36oXw=
— A few milliseconds

Challenge input: Ice ice baby - too cold!
Difficulty: Find a hash beginning with the word "Hi"
Try 1: Ice ice baby - too cold!605794851640 - 6B7Pxk1rslm3CUmrZNNoU/YnNER6p5tmyqVeBwMkcwY=
Try 2: Ice ice baby - too cold!126995896088 - rpkMTHCqv9PEhmOJ7IRsSsURWNAeBwsfexkADoRnG94=
Try 3: Ice ice baby - too cold!91747106472 - bVqjtmhp/ESV97Tm7ukruOE6ALA8eI3PtpBo4BheAw4=
…
Try 1797: Ice ice baby - too cold!220662551486 - HiTFKtbBCvdQE52uLsORpHnYKig23Gl6HSZZ1b7Kfhw=
— Dozens of milliseconds

Challenge input: Who let them out?
Difficulty: Find a hash that begins with the word "Dog"
Try 1: Who let them out?302144717673 - oX4N6QkwBBUIlSCAc2zK8gqdtKFKGToOaaeisnqciq0=
Try 2: Who let them out?859453531286 - C8fAGy8asX4iykJYXIGZmLdsn9gykL7SCD9ox6ozrn8=
…
Try 773177: Who let them out?320123333599 - DogQ0XTBPKCFofXwxaUZidEsO326tW9sgqn0tQX0DUY=
— Many seconds
```

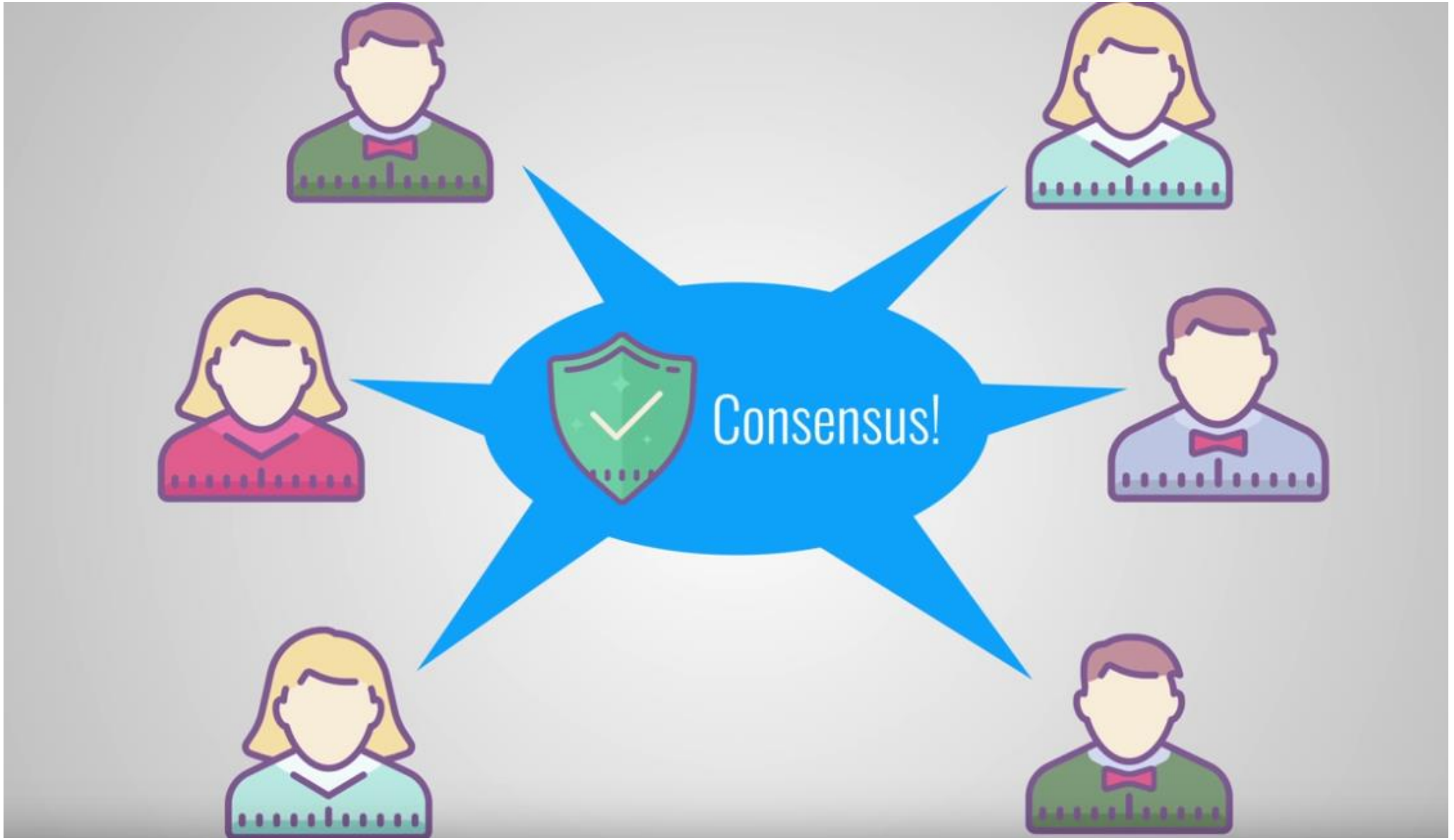
Hash Rate

The estimated number of tera hashes per second (trillions of hashes per second) the Bitcoin network is performing.



Consensus – Peer-to-Peer



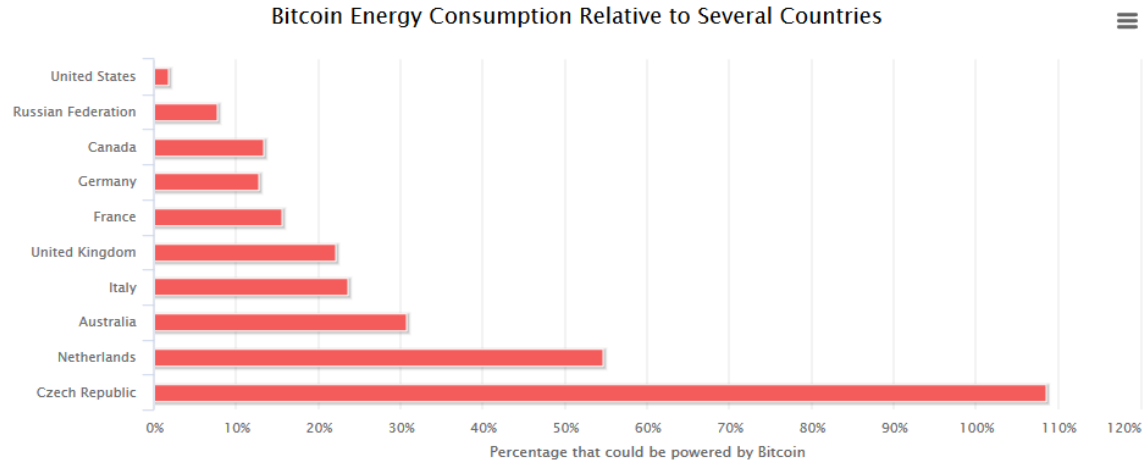

Consensus!

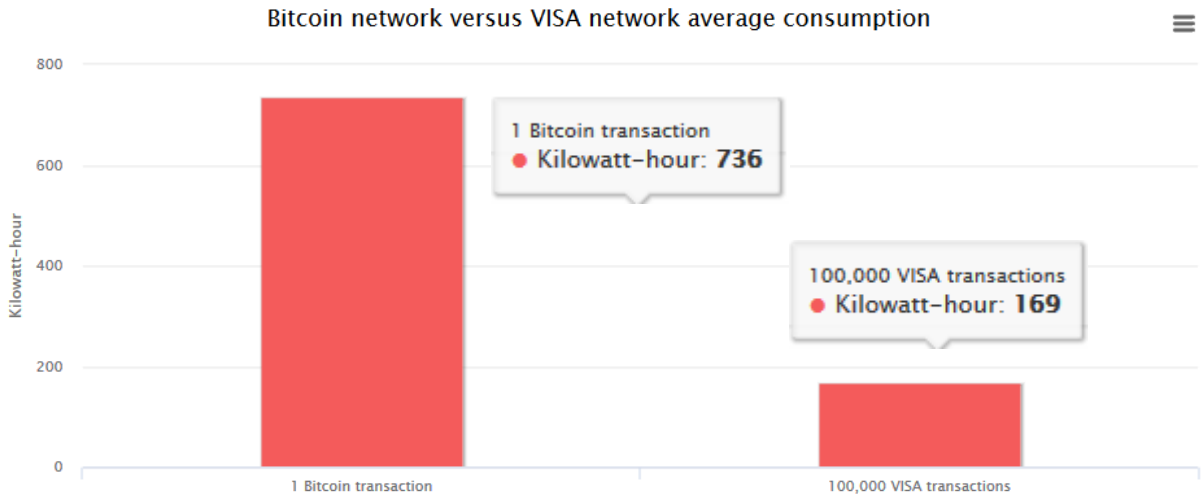
Blockchain - onveranderlijk

- Niet te veranderen:
  - Alleen geverifieerde transacties worden toegevoegd aan de blockchain
  - ‘Proof of work’ moet voor elk block opnieuw uitgevoerd worden
  - Meer dan 51% van alle nodes bezitten
- Reden om te minen:
  - Beloning voor het vinden van een nieuw block
  - Beloning voor het verifiëren en goedkeuren van transacties

Blockchain – Proof of work

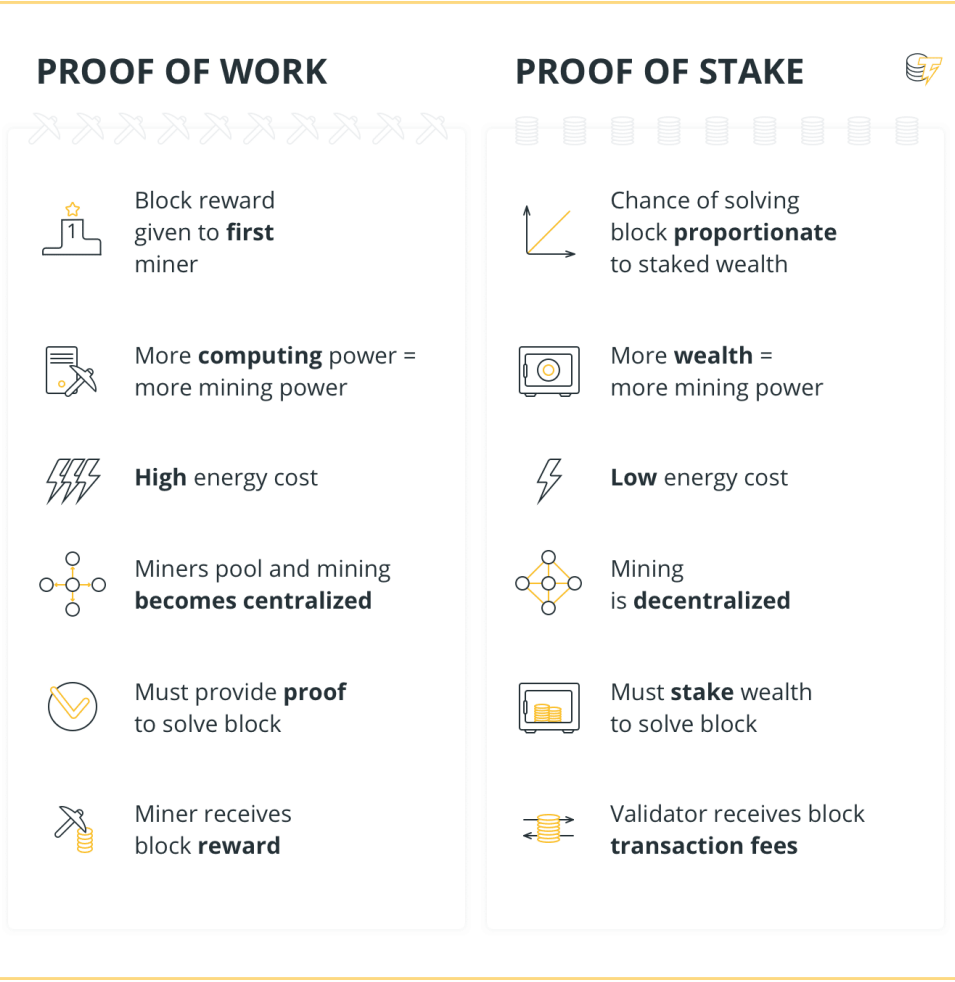
- Kost veel energie
- Centralisatie miningpool

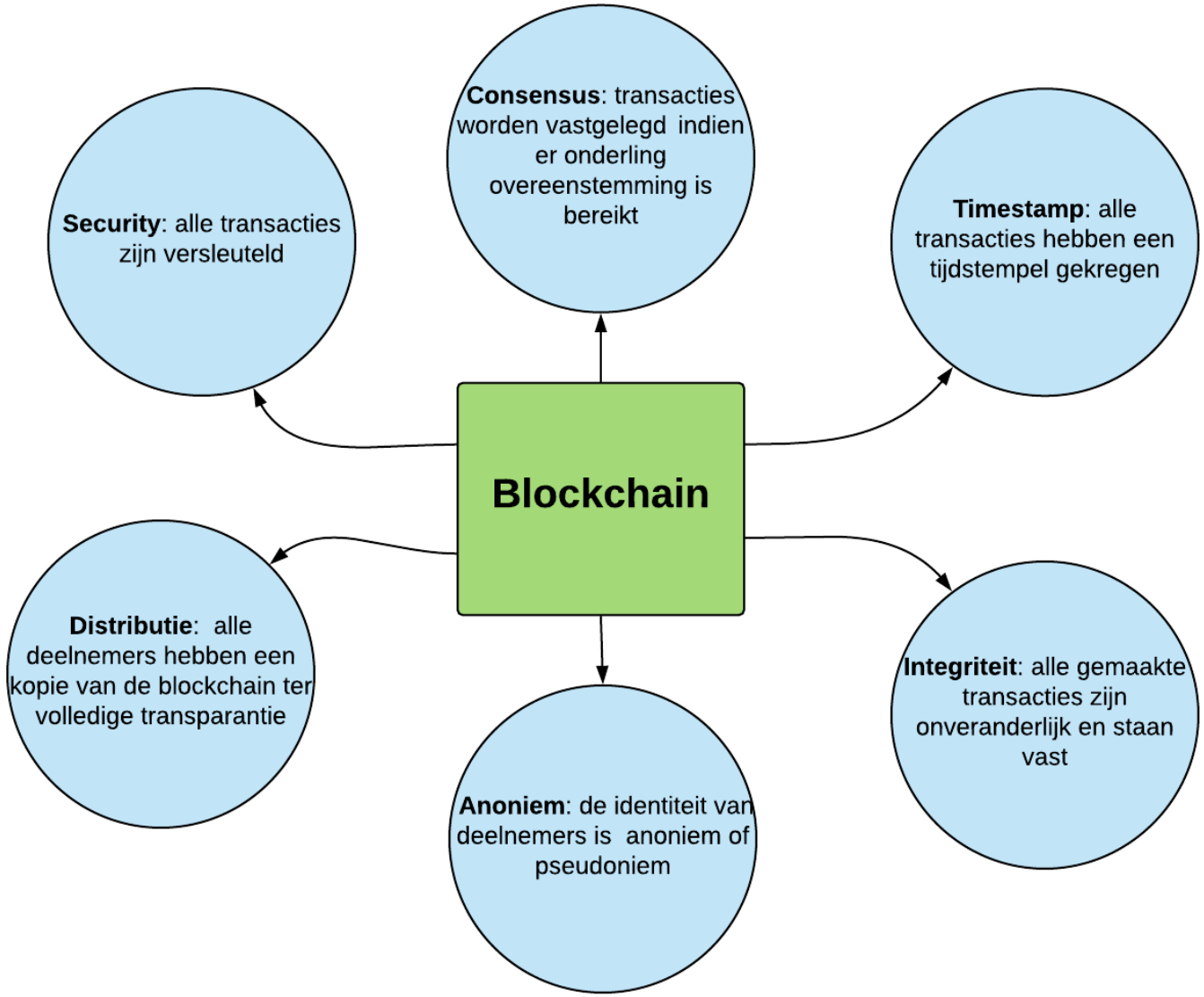




Blockchain – Proof of stake

- Computerkracht versus ‘recht van de sterkste’
  - Nog geen standaard
  - Nog geen algemeen geaccepteerde oplossing




Consensus: transacties worden vastgelegd indien er onderling overeenstemming is bereikt
Security: alle transacties zijn versleuteld
Timestamp: alle transacties hebben een tijdstempel gekregen
Blockchain
Distributie: alle deelnemers hebben een kopie van de blockchain ter volledige transparantie
Integriteit: alle gemaakte transacties zijn onveranderlijk en staan vast
Anoniem: de identiteit van deelnemers is anoniem of pseudoniem

Blockchain

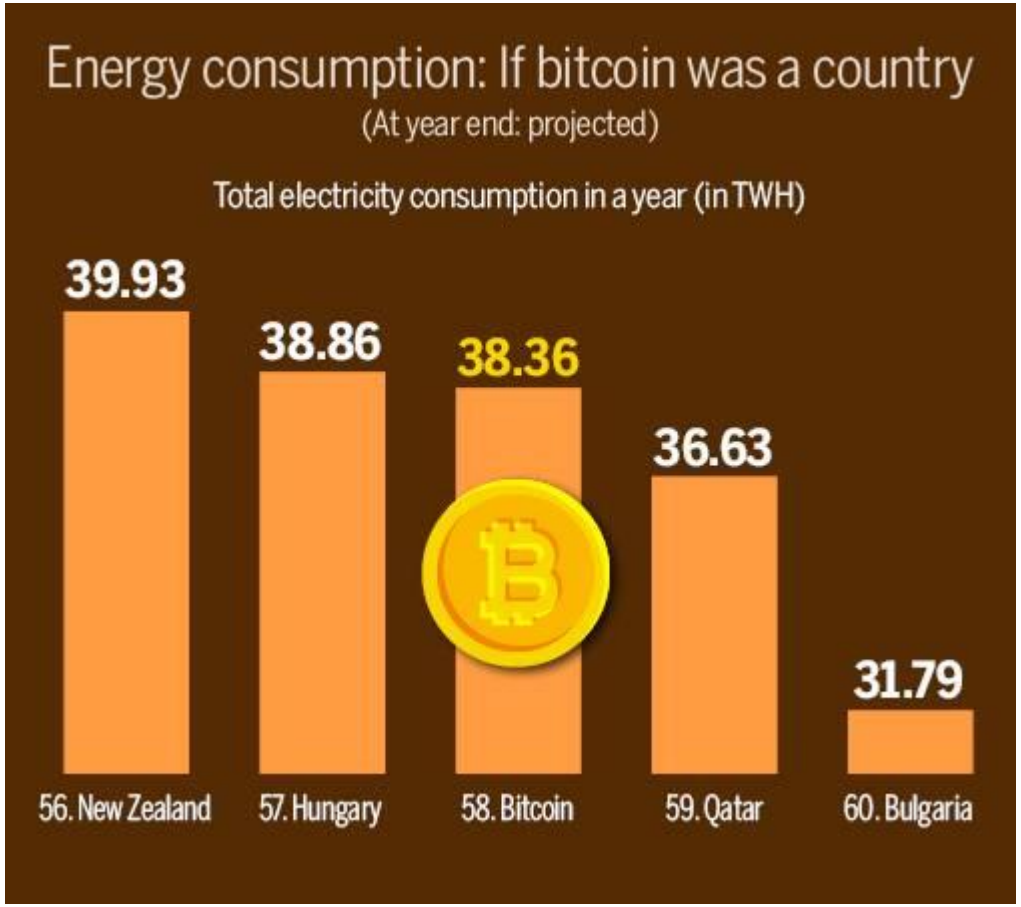
- Private
- Public

- Is een private blockchain nog wel typerend voor blockchain?

	Public Blockchain	Private Blockchain	Federated/Consortium Blockchain
Access	• Anyone	• Single organization	• Multiple selected organizations
Participants	• Permissionless • Anonymous	• Permissioned • Known identities	• Permissioned • Known identities
Security	• Consensus mechanism • Proof of Work / Proof of Stake	• Pre-approved participants • Voting/multi-party consensus	• Pre-approved participants • Voting/multi-party consensus
Transaction Speed	• Slow	• Lighter and faster	• Lighter and faster

Blockchain - Nadelen

- Populair
  - Niet-bestaande problemen worden opgelost
- Geen one-size-fits-all oplossing
- Energieverbruik - exponentiële groei, in 2020 evenveel als wereldwijd energieverbruik

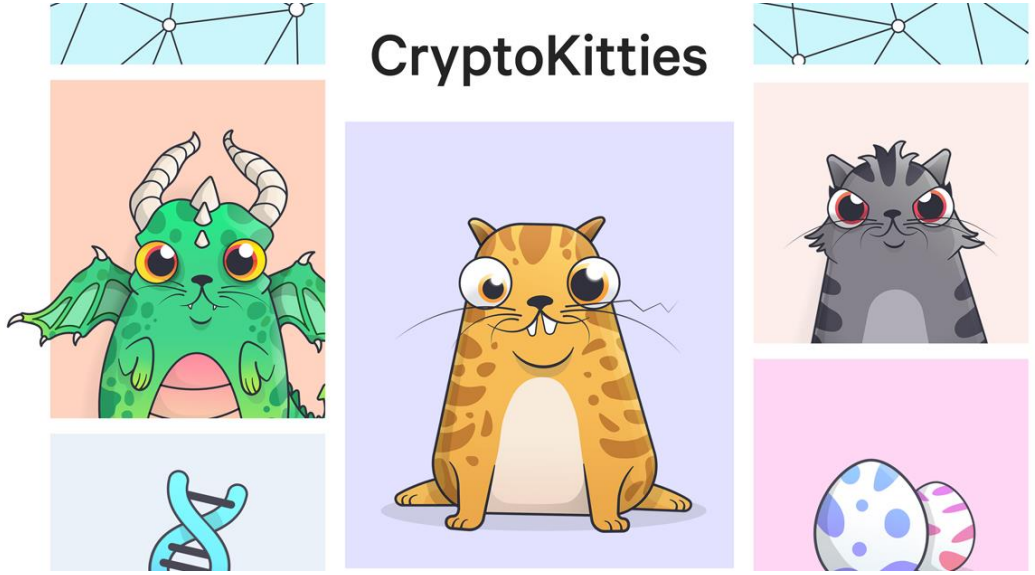


Blockchain - Nadelen

- Schaalbaarheid – transacties per seconde
  - Visa: 2.000 per seconde
  - Bitcoin: 7 per seconde
- Geen regulering en standaardisatie
  - Overheden zijn het niet eens
  - Manipulatie
  -
- Input door mensen, geen smartoplossing

Ethereum

- ‘Blockchain 2.0’
  - Sneller, zelfstandig en toegankelijkheid verhogen van crypto
- dApps
- ICO
- Smart contracten



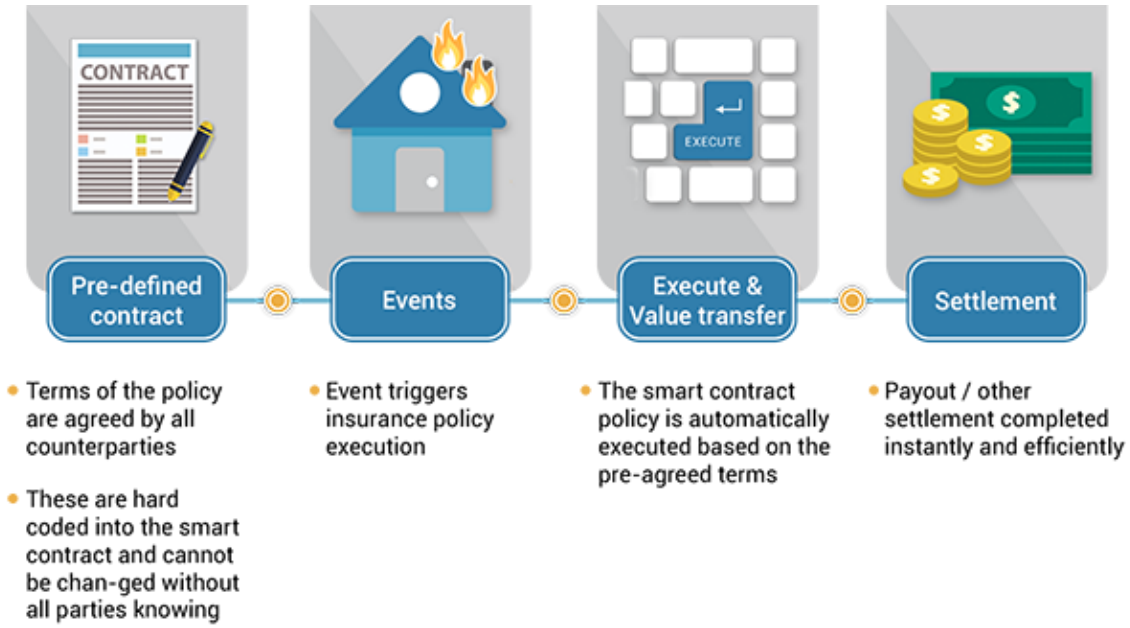
Smart contracten

- *"Een smart contract is een geprogrammeerd contract waarvan de afspraken in computercode staan vastgelegd op de blockchain. Het contract wordt automatisch uitgevoerd zonder dat hier (vertrouwen in) een tussenpartij voor nodig is. Deze afspraken zijn altijd in te zien, maar kunnen onmogelijk nog worden aangepast."*

- Geautomatiseerd transactieprotocol/ Deterministisch

Smart contracten

- Ethereum & NEO
- Voorbeelden
  - Kopen van huizen
  - Juridisch document
  - Weddenschap
  - Lease auto



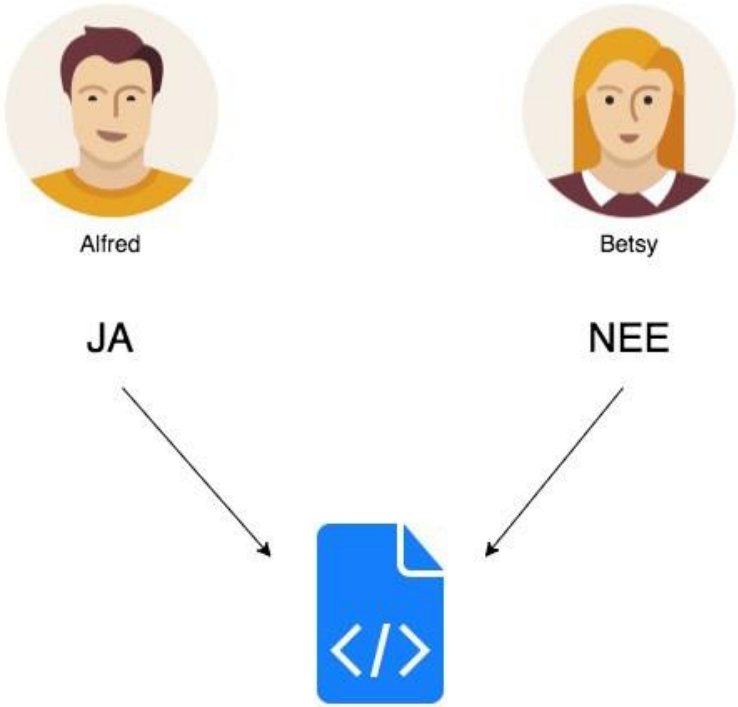
Smart contracten

- Voordelen:
  - Vertrouwen
  - Autonomie
  - Veiligheid
  - Snelheid
  - Back-up
  - Besparingen
  - Nauwkeurigheid

- Nadelen:
  - Menselijk input
  - Legale status
  - Kosten
  - Moet ‘foutloos’ opgesteld zijn
  - In theorie niet aanpasbaar, hacks mogelijk

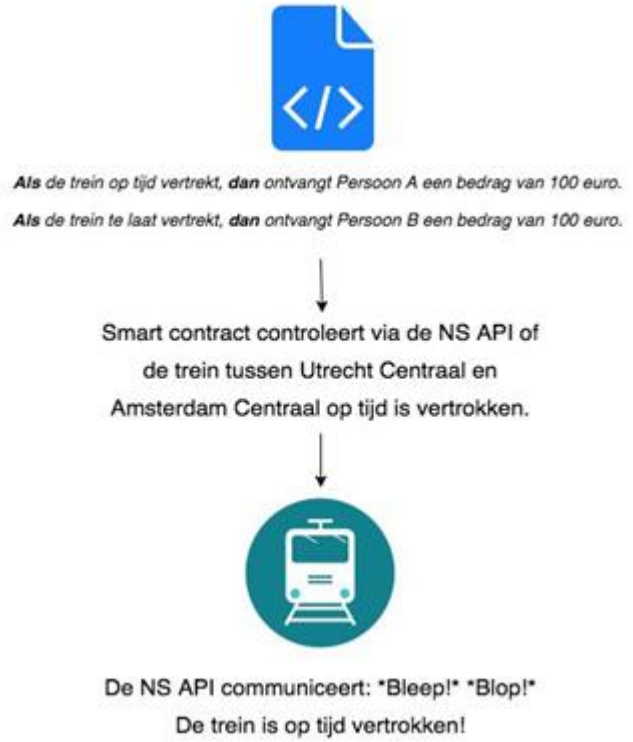
Smart contracten - voorbeeld

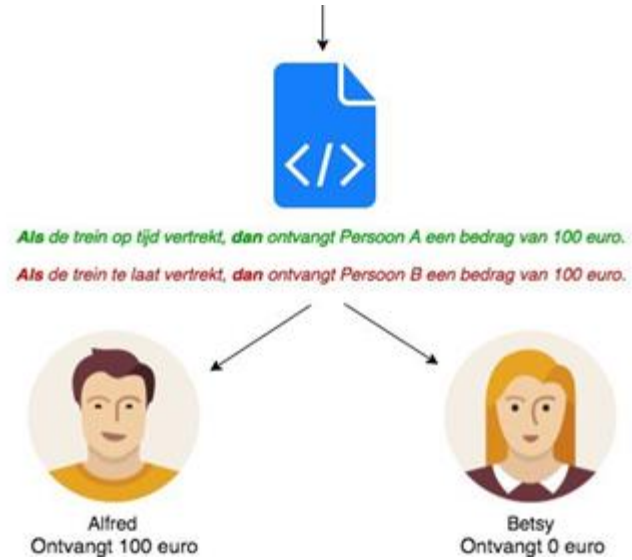
Vertrekt de trein van 09.00 tussen Utrecht Centraal en Amsterdam Centraal op tijd?



***Als** de trein op tijd vertrekt, **dan** ontvangt Persoon A een bedrag van 100 euro.*

***Als** de trein te laat vertrekt, **dan** ontvangt Persoon B een bedrag van 100 euro.*

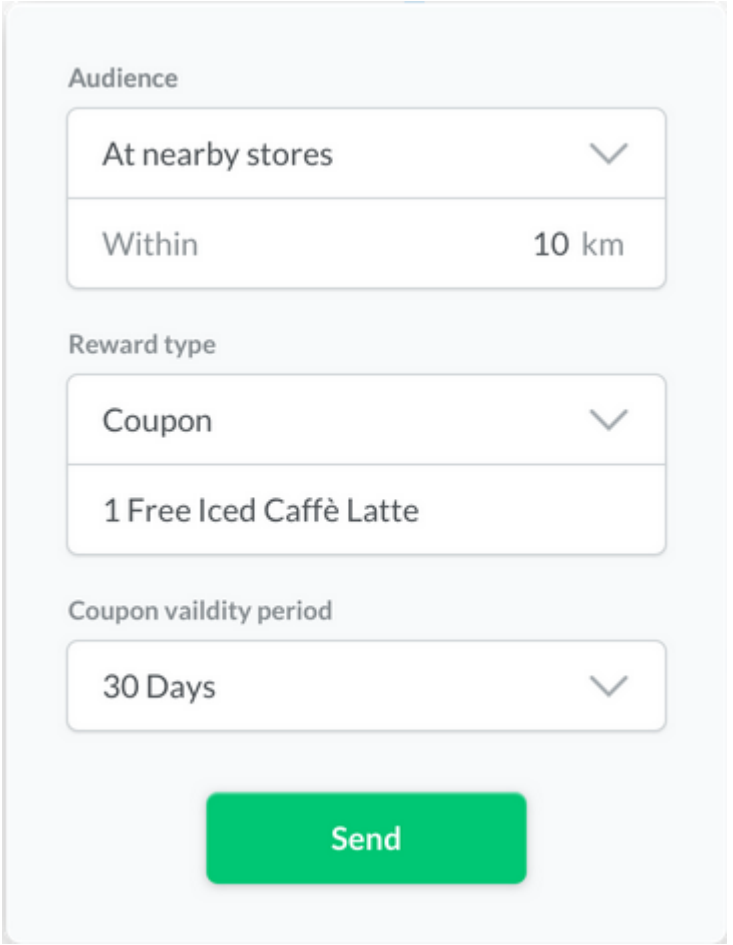




BLOCKCHAIN PROJECT ECOSYSTEM

Business models - Fintech

- Carry Protocol - Customer loyalty
  - Gebruiker beheert eigen data, winkel krijgt inzicht in gebruikersstromen



Consumer advantages

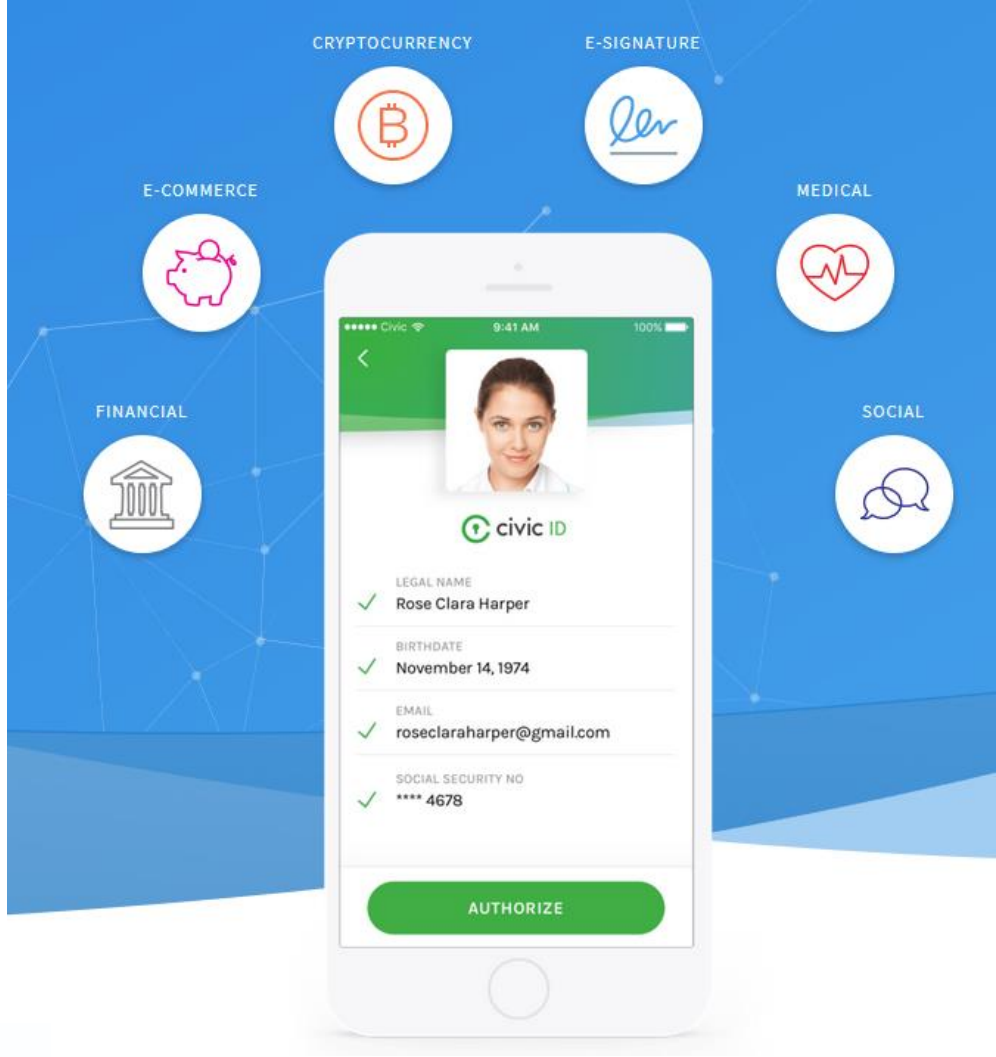
- Own their transaction data
- Anonymously monetize it
- Collect digital coupons and loyalty points

Merchant advantages

- Accept virtual currency in brick-and-mortar shops
- Process payments quickly
- Incentivize returning customers with digital coupons and custom Branded Tokens

Business models - Onafhankelijkheid

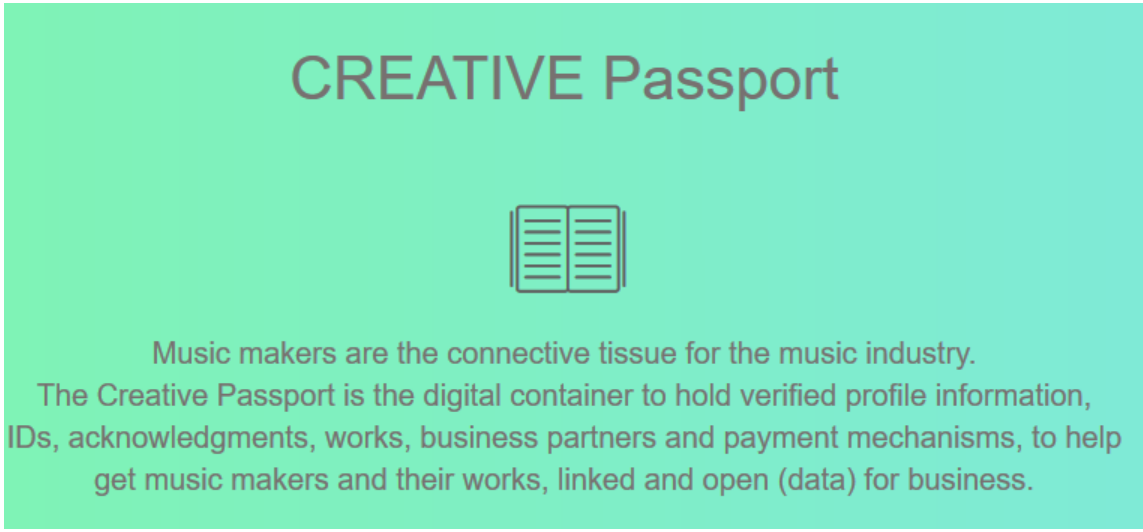
- Civic - ID & Access management
  - Gebruiker kiest zelf wat wel en niet gedeeld wordt



Civic's **Secure Identity Platform** (SIP) uses a verified identity for multi-factor authentication on web and mobile apps without the need for usernames or passwords.

Business models - Eigenaarschap

- Imogen Heap - Muziek royalties
  - Doorbreken van schakels en eigenaarschap teruggeven aan muzikanten en artiesten



Business models - Waardeoverdracht

- Filecoin – Opslag van data
  - Inzetten van ongebruikte dataruimte

EARN FILECOIN FOR HOSTING FILES

Put your unused storage to work by becoming a Filecoin miner. Use the Filecoin mining software to get paid for fulfilling storage requests on the Filecoin market.

RELIABLY STORE FILES AT HYPERCOMPETITIVE PRICES

Clients can tune their storage strategy to suit their needs, creating a custom balance between redundancy, speed of retrieval, and cost. The worldwide Filecoin storage and retrieval markets make vendors compete to give you flexible options at the best prices.

Business models - Identiteit

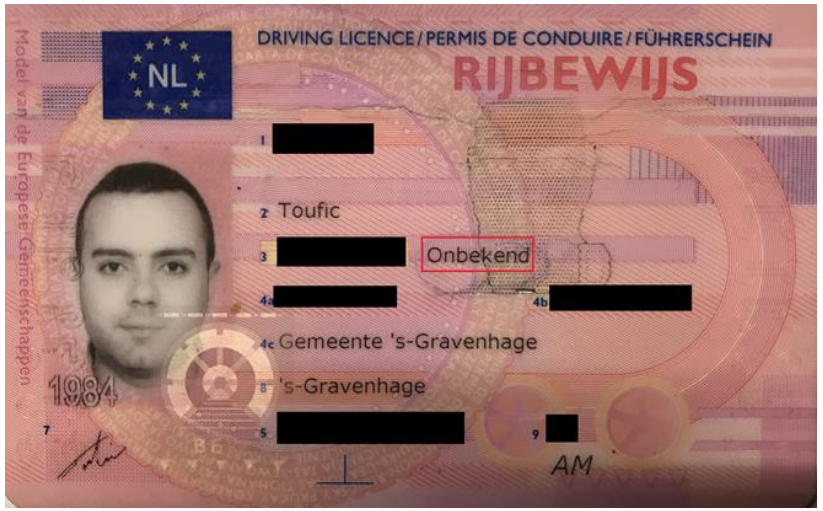
- Tykn - Registratie vluchtelingen
  - Het toekennen (teruggeven) van een identiteit

Beneficiary Identity Registration

Registration and verification of humanitarian aid beneficiaries through Ana, Tykn's distributed identification system built on Sovrin. To be launched in Q3 of 2018.

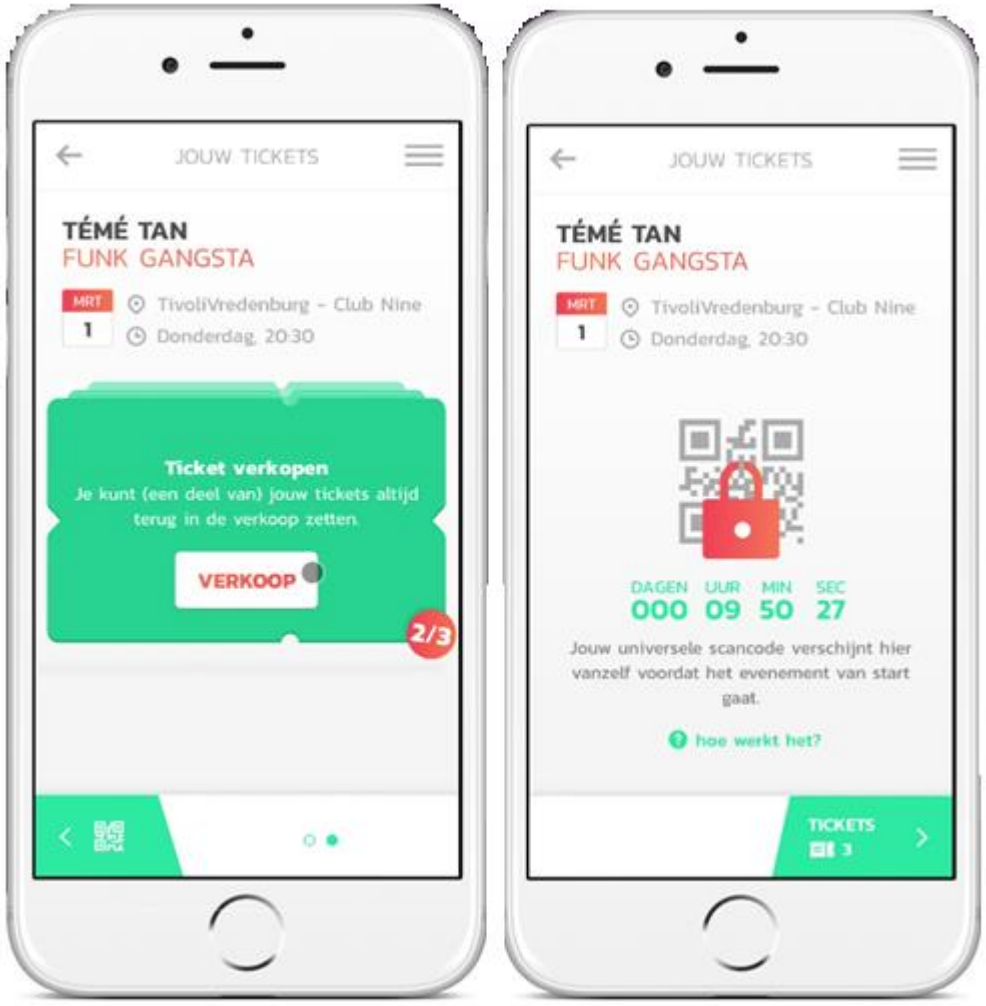
Blockchain as a Service (BaaS) Solutions

- Empowering NGOs and governments with tailor-made Blockchain-based identification tools.
- Building & designing systems for the registration and verification of persons via a distributed ledger.
- Reducing risk of fraud through systems of verifiable trust.



Business models – Authenticiteit

- Guts - Concertkaarten
  - Eerlijk en transparant verkoop van concertkaartjes



Vragen?

Cyber4Z
Ontwikkeling en implementatie van blockchain
Security consultancy

Morrison Toussaint, Blockchain Consultant
Tel (NL): +31 6 280 35 691
E-mail: morrison.toussaint@cyber4z.com
www.cyber4z.com