Politie Oost Nederland, Deventer 30 oktober 2019

Masterclass Blockchain
Dag 2

Arthur Janse

Chhay Lin Lim

Christa Barkel

Jan Veuger

Ronald Kramer

SAXION HOGESCHOOL



AGENDA DAG 2 – 13 November

Diepere achtergrond, gevolgen Blockchain, praktische cybercrime voorbeelden.

09.00 Recap dag 1
09.30 De praktijk met tools door Eljo Haspels CEO Cointell.
11.30 Verdieping blockchain en bouwstenen.

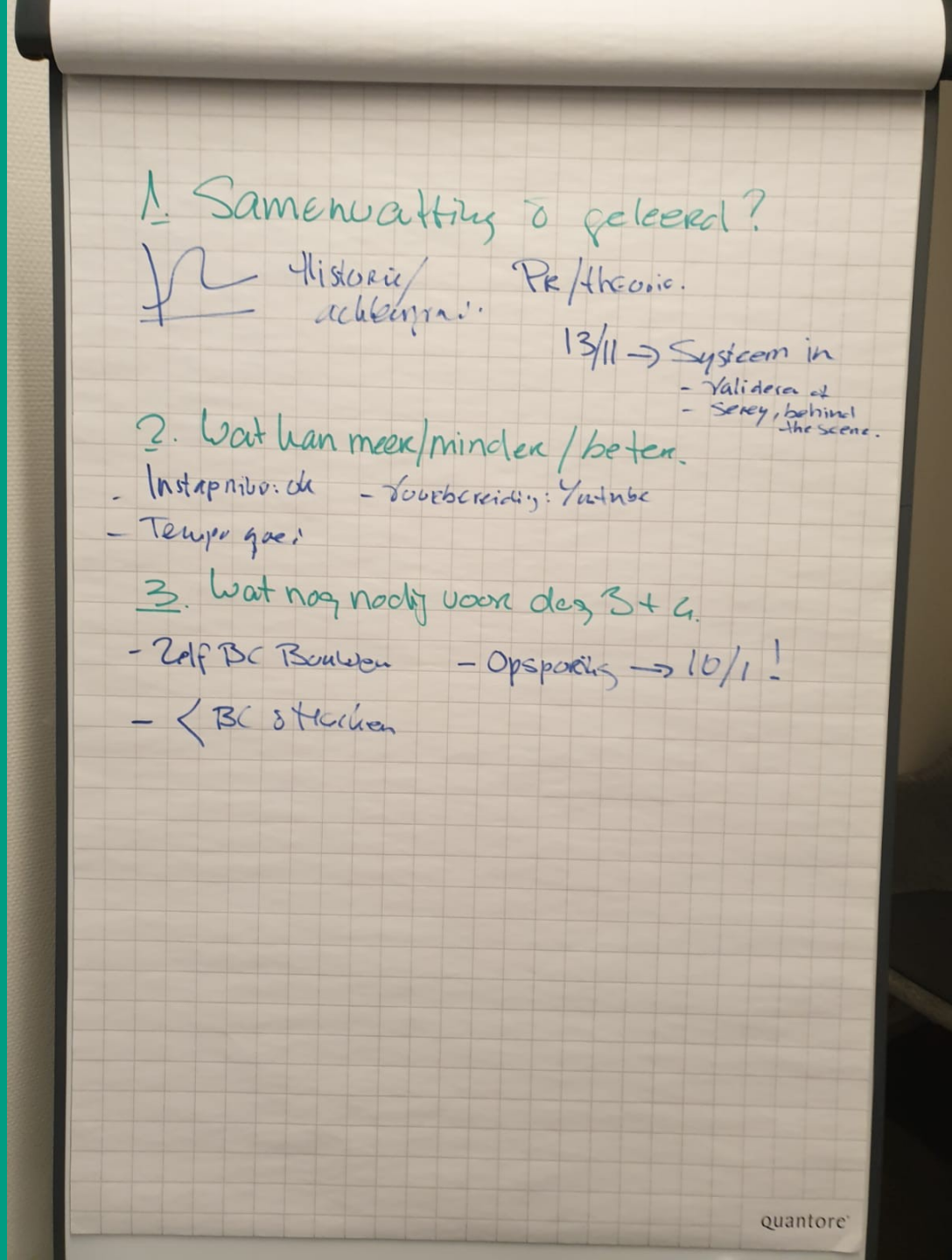
12.30 Lunch

13.15 Verdieping Blockchain en bouwstenen.
14.15 Consensusprotocollen en public, private, consortium.
15.45 Serey. Waar moet je aan denken als je een blockchain project opzet?
15.30 De casus
16.50 Afsluiting en reflectie.

SAXION HOGESCHOOL



Verwachtingen?



Waar staan we ?



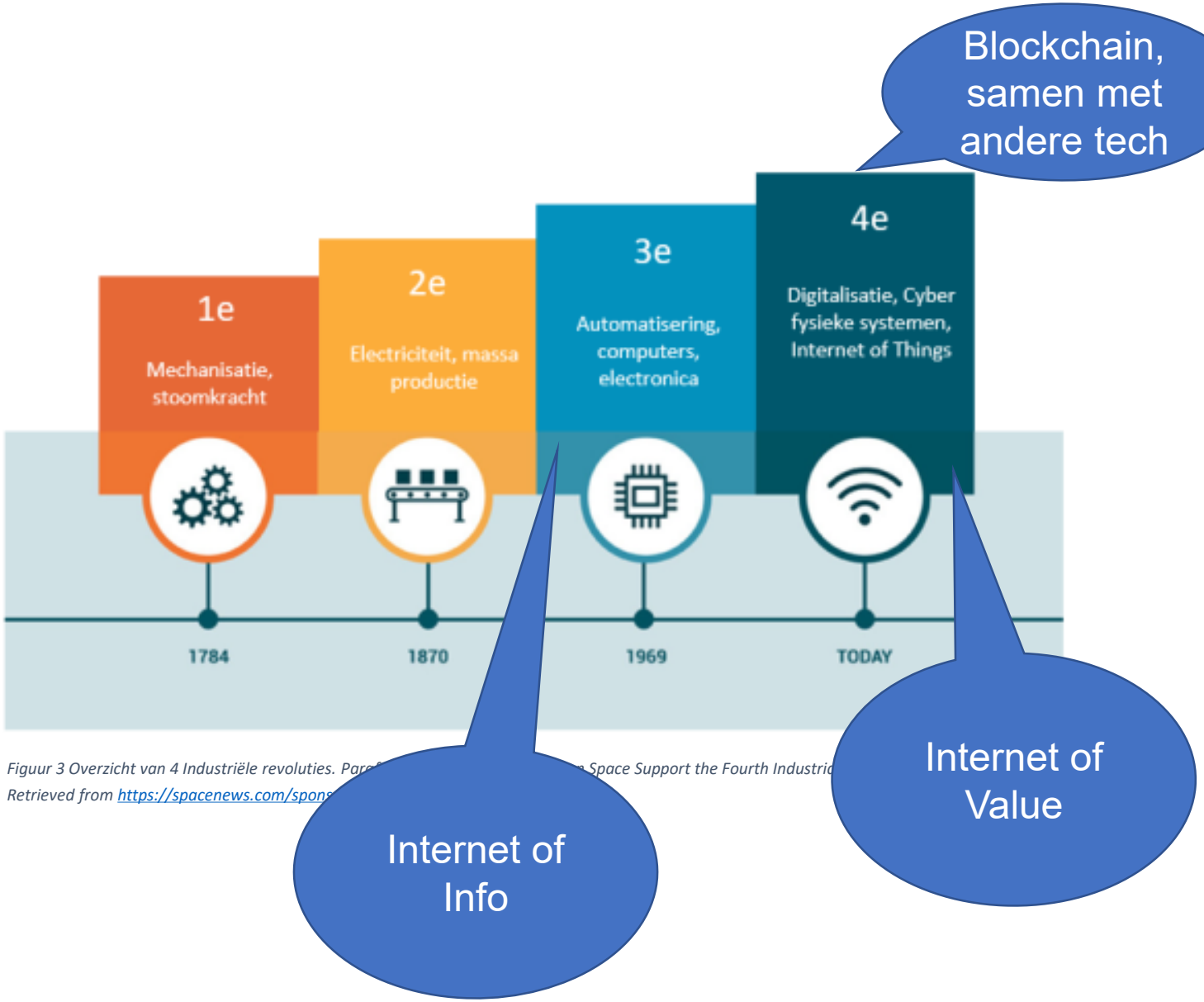

Recap dag 1

Welke kennis is aanwezig van dag 1?

SAXION HOGESCHOOL

Industriële revoluties

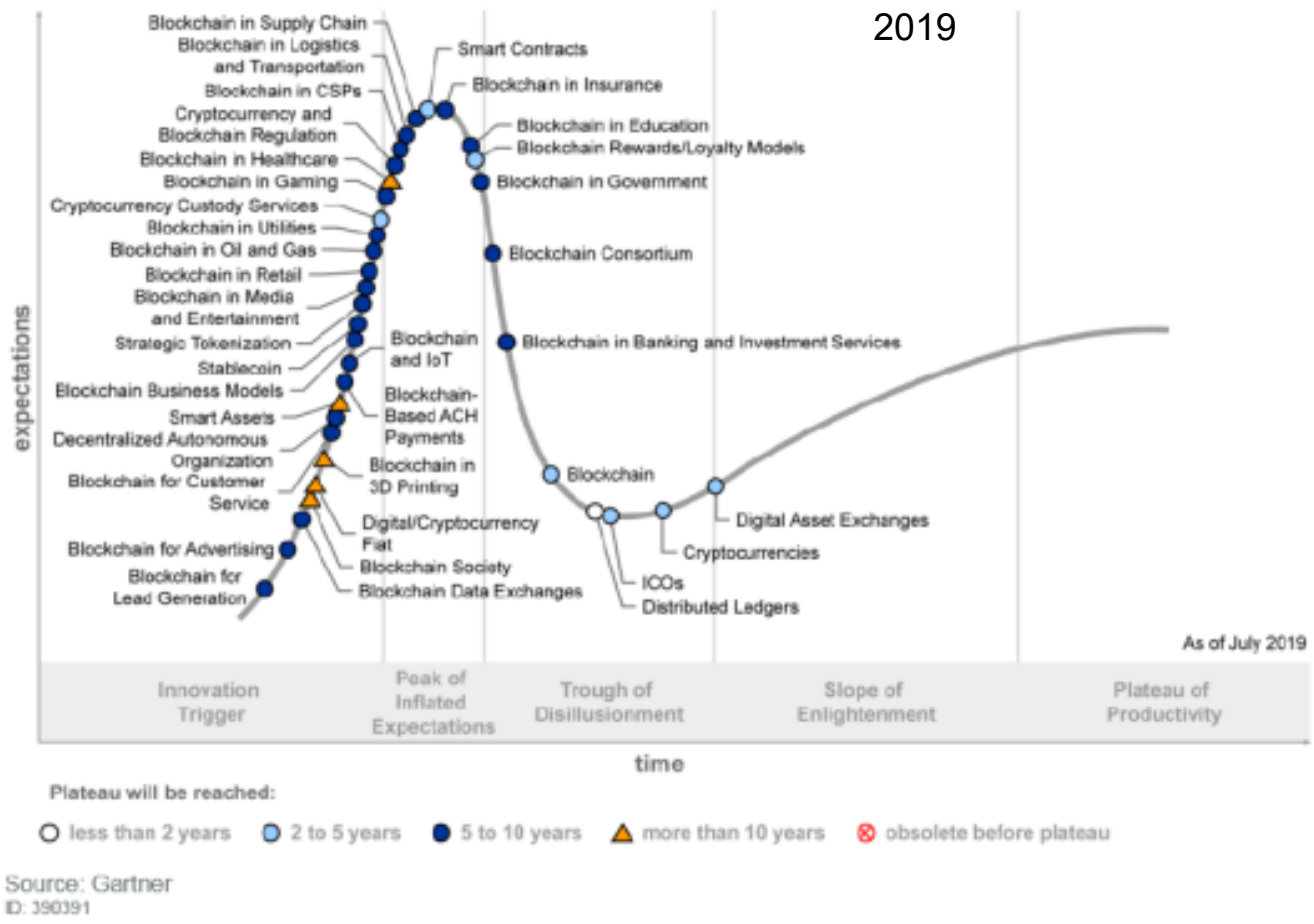
Vier perioden van technologische innovatie



Figuur 3 Overzicht van 4 Industriële revoluties. Par… Space Support the Fourth Industri…
Retrieved from https://spacenews.com/spons…

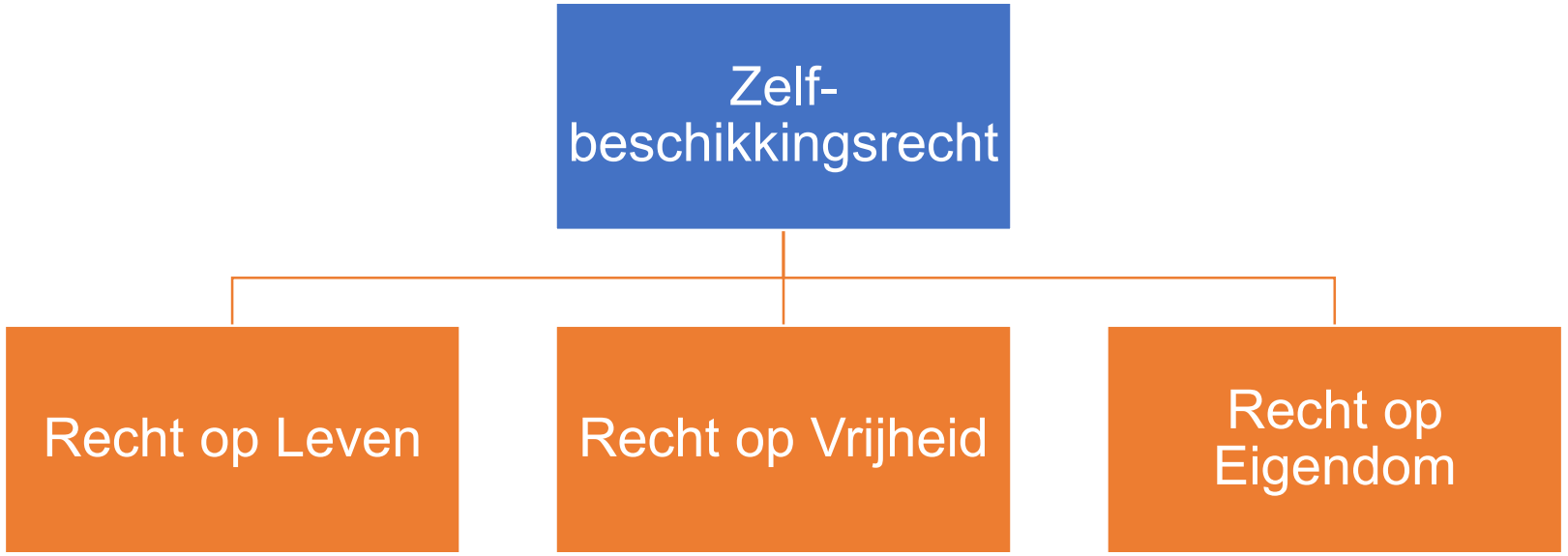
Flink in ontwikkeling

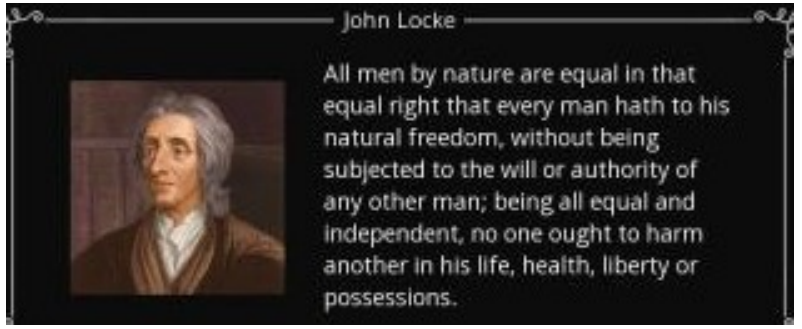
Hype cycle for blockchain business

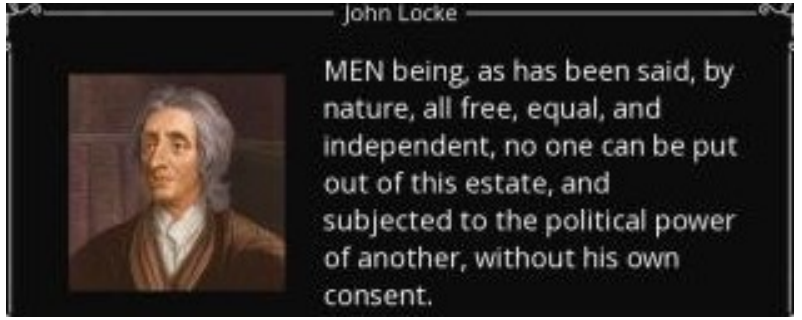


Bron; https://www.gartner.com/en/newsroom/press-releases/2019-09-12-gartner-2019-hype-cycle-for-blockchain-business-shows

Libertarisme: Zelf-soevereiniteit

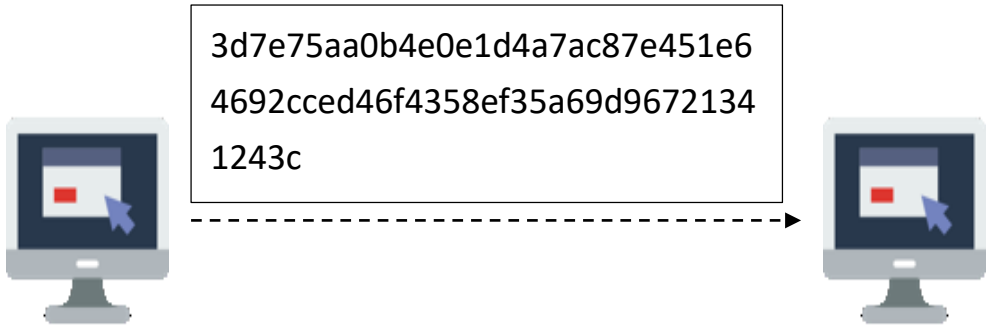




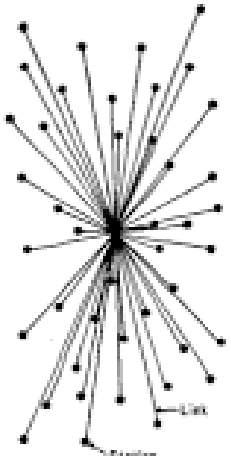


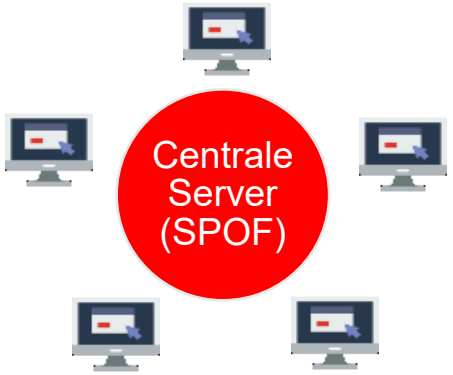
Filosofisch perspectief

- Als wij de praktische en sociale implicaties van Blockchain willen begrijpen, dienen we ook de filosofie die het heeft voortgebracht te begrijpen
- Blockchain is een sociale, politieke en economische revolutie
- Blockchain komt voort uit Libertarisch Anarchisme, Crypto-Anarchisme en Cypherpunk
  - Filosofie die de bescherming nastreeft van
    - Privacy
    - Politieke vrijheid
    - Economische vrjiheid
    - door gebruik van cryptografie



Twee typen netwerken

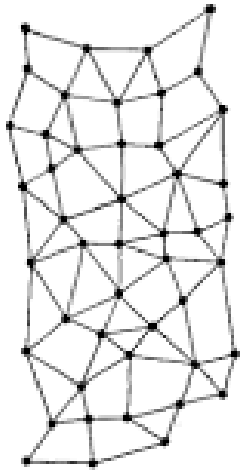




- **Gecentraliseerd**
- Via een gecentraliseerde server
- Wel Single Point of Failure (SPOF)
- Wel Trusted Third Party (tussenpersoon)
- Vaak niet anoniem
- Historie kan worden overschreven
- Schaalbaar en snel
- **Permissioned**







- **Gedistribueerd/gedecentraliseerd**
- Peer-2-Peer
- Geen Single Point Of Failure
- Geen Trusted Third Party (tussenpersoon)
- 100% transparent of volledig anoniem
- Onveranderbaar, alleen read/write
- Consensus, verificatie, gedistribueerd, lastig te implementeren
- **Permissioned of permissionless**

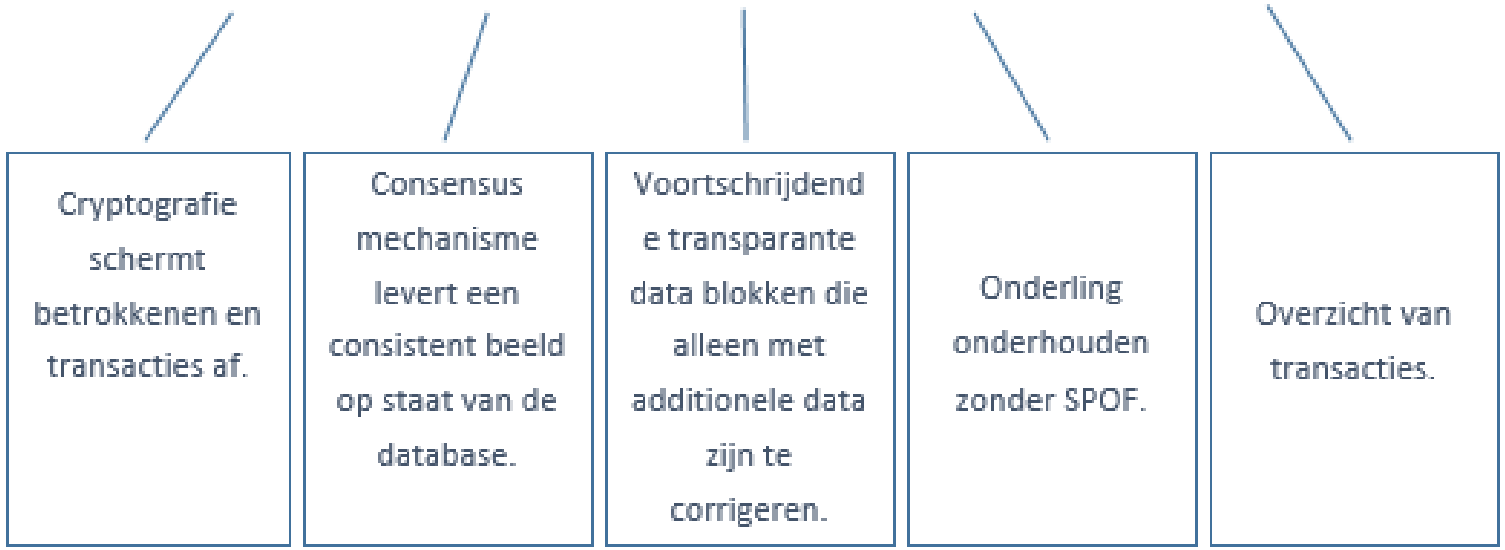


Blockchain 1.0: Bitcoin

Bouwstenen

Blockchain is in de basis een..

versleutelde overeengekomen gelinkte gedistribueerde database.

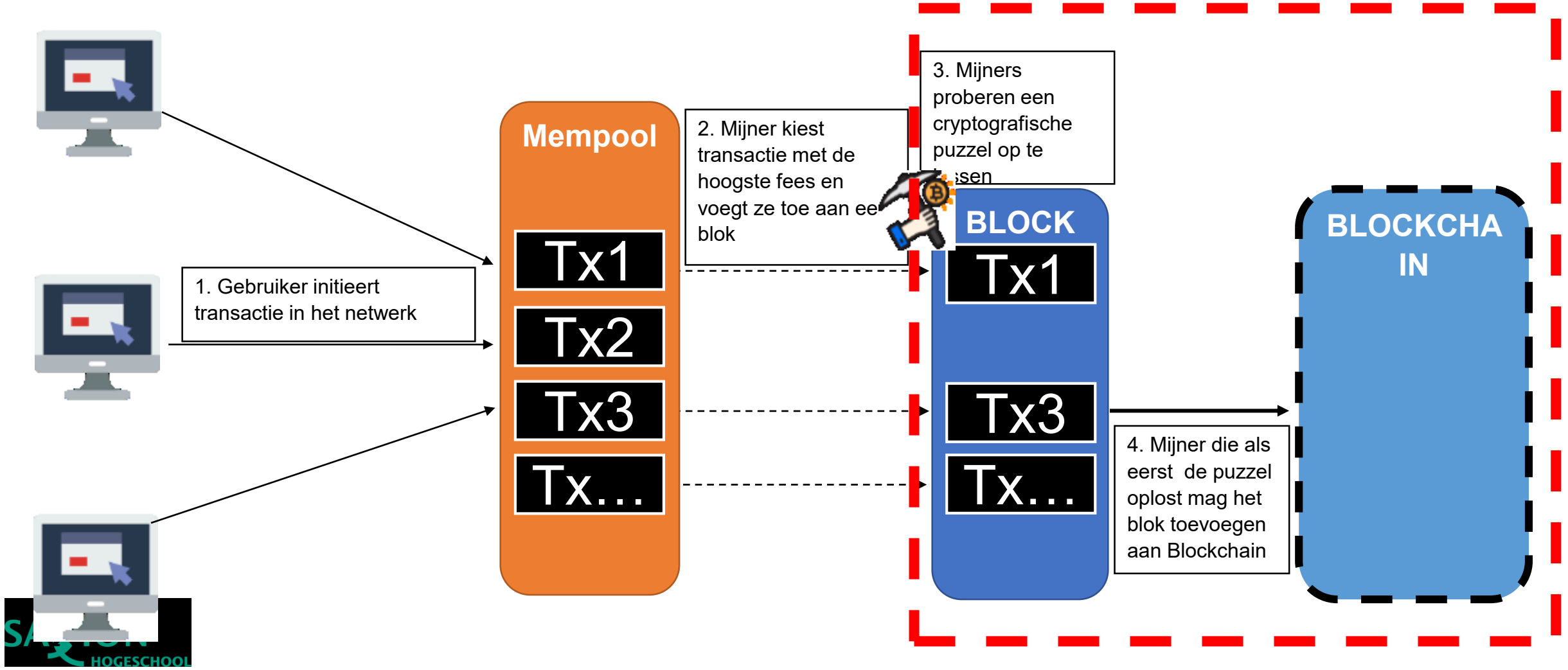


Deze bouwstenen kun je gelang je behoefte gebruiken en veranderen

SAXION HOGESCHOOL

bitcoin

Hoe een Bitcoin transactie werkt

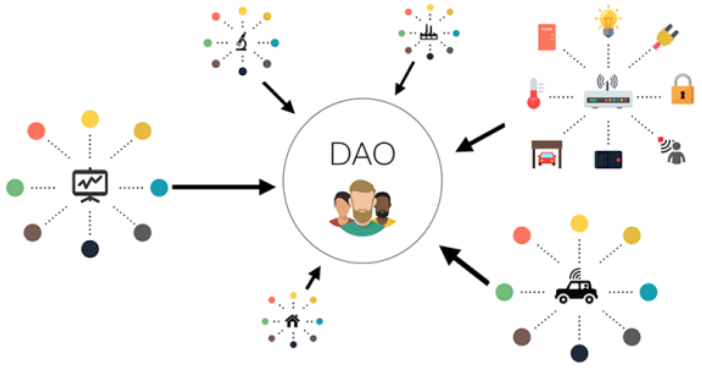


Blockchain 2.0.: Ethereum

Bouwstenen

BLOCKCHAIN Bouwstenen 2.0

- Smart contracts
- dApps
- Tokenization
  - Cryptocurrency
  - Asset
  - Fractionalisering
- Autonome organisatievorm (DAO)
- Self Sovereign Identity
- Open source



ethereum

SAXION HOGESCHOOL

AGENDA DAG 2 – 13 November

Diepere achtergrond, gevolgen Blockchain, praktische cybercrime voorbeelden.

09.00 Recap dag 1
09.30 De praktijk met tools door Eljo Haspels CEO Cointell.
11.30 Verdieping blockchain en bouwstenen.

12.30 Lunch

13.15 Verdieping Blockchain en bouwstenen.
14.15 Consensusprotocollen en public, private, consortium.
14.45 Serey. Waar moet je aan denken als je een blockchain project opzet?
15.30 De casus
16.50 Afsluiting en reflectie.

SAXION HOGESCHOOL




De praktijk met tools
door Eljo Haspels CEO
Cointell.

AGENDA DAG 2 – 13 November

Diepere achtergrond, gevolgen Blockchain, praktische cybercrime voorbeelden.

09.00 Recap dag 1
09.30 De praktijk met tools door Eljo Haspels CEO Cointell.
11.30 Verdieping blockchain en bouwstenen.

12.30 Lunch

13.15 Verdieping Blockchain en bouwstenen.
14.15 Consensusprotocollen en public, private, consortium.
15.45 Serey. Waar moet je aan denken als je een blockchain project opzet?
15.30 De casus
16.50 Afsluiting en reflectie.

SAXION HOGESCHOOL



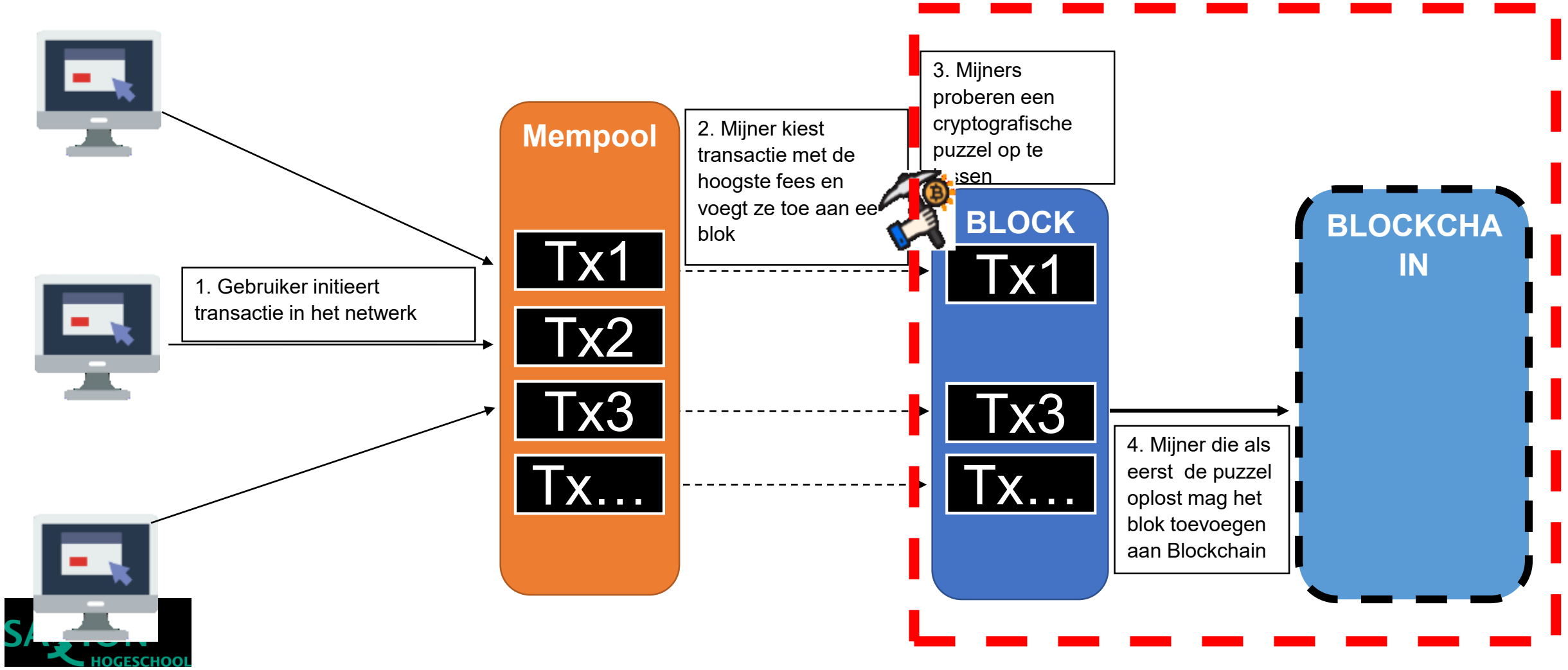

Verdieping blockchain en bouwstenen

Introductie in de Bitcoin Blockchain

- Proof of Work (consensus mechanisme)
- Peer-2-peer
- 100% transparant
- Data is onwijzigbaar
- Cryptografie
- Open-source

SAXION HOGESCHOOL

Hoe een Bitcoin transactie werkt



Bitcoin maakt gebruik van Proof of Work consensus mechanisme

- Oorspronkelijk een manier om e-mail spam te voorkomen
  - Als je een e-mail wil versturen moet je computer eerst een kleine cryptografische puzzel oplossen. Wanneer deze is opgelost, dan wordt je mail verstuurd
- Bitcoin Blockchain gebruikt Proof of Work om het netwerk te helpen beveiligen
- Mijners moeten een cryptografische puzzel oplossen
- Dat kost veel rekenkracht
- De mijner die het eerst de puzzel oplost mag een blok toevoegen aan de Blockchain en krijgt een beloning: 12,5 BTC + transactie fees

SAXION HOGESCHOOL

Wie mag een nieuw blok produceren bij Proof-of-Work?

- Kans om een blok te mogen aanmaken is gebaseerd op de rekenkracht die de mijner levert aan het netwerk
- Verbruikt veel energie





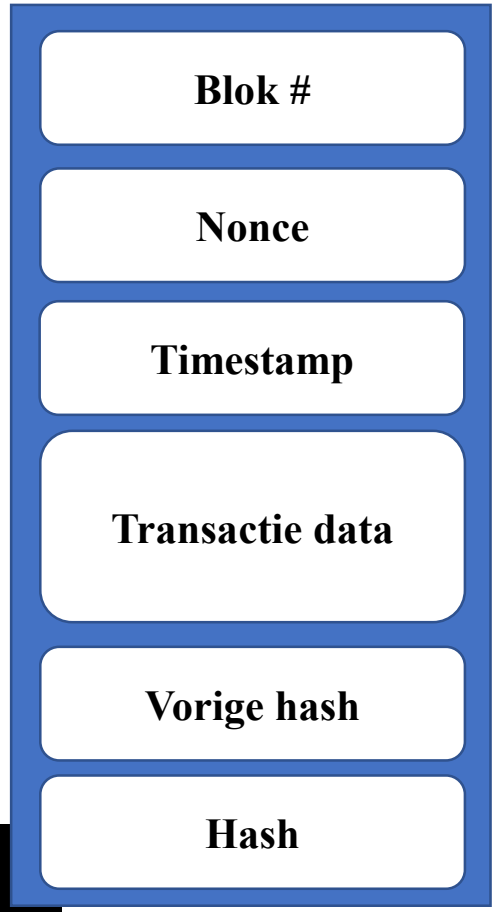
Wat is Hash cryptografie?

- Een manier om plaintext middels wiskundig algoritme om te zetten in iets onleesbaar
- Bitcoin maakt gebruik van SHA-256 (Secure Hash Algorithm)
  - 64 karakters lang
  - Elk karakter is een hexadecimaal (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F)
  - Elk karakter is 4 bits groot. De hash is dus 64 * 4 = 256 bits lang

- Eigenschappen van een betrouwbaar hash algoritme:
  - Deterministisch: zelfde input leidt altijd tot dezelfde output
  - Reverse engineering onmogelijk: je kan de input niet achterhalen als je de output weet
  - Omzetten van data in een hash-waarde moet snel kunnen
  - Als de input wijzigt, verandert de output compleet

SAXION HOGESCHOOL

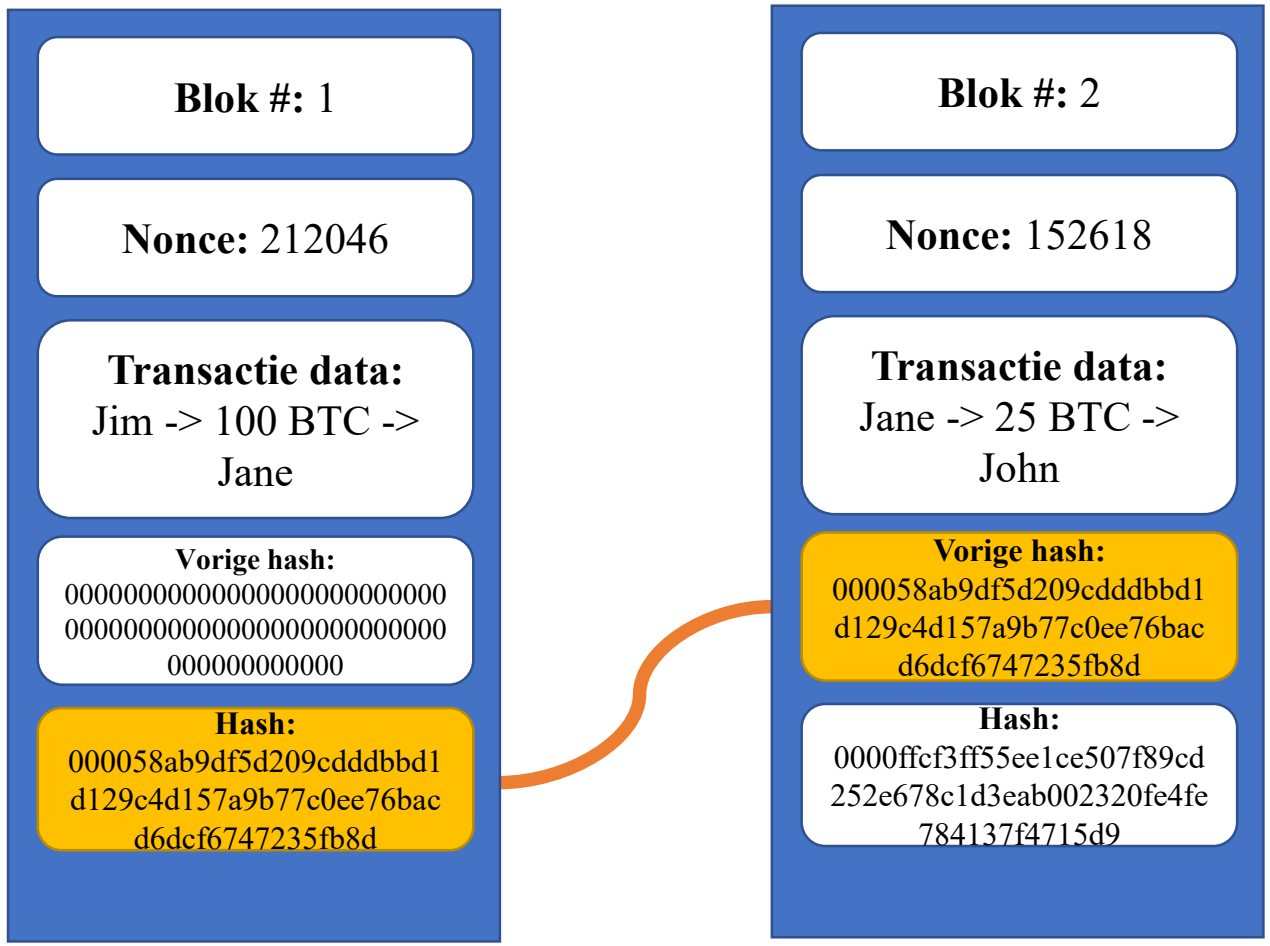
Welke Data zit er in een Blok?



- Blok # (index nummer)
- Nonce: arbitrair nummer, gebruikt door mijner om een geldige hash te verkrijgen
- Timestamp: data dat certificeert wanneer het blok is gecreëerd
- Transactiedata: alle data mbt Bitcoin transacties
- Vorige hash: hash-waarde van het vorige blok
- (Block Header) Hash: hash-waarde van het huidige blok

De hash is een “vingerafdruk” van het blok. Als er data verandert in het blok, verandert de hash en ziet het hele netwerk dat er is gesjoemeld met data

Hoe worden Blokken aan elkaar gelinkt?



- Elk blok heeft een “vorige hash” die gelijk is aan de hash van het vorige blok

Waarom is het zo moeilijk om een geldig Blok te maken?

- Waarom wil je niet dat er té veel geldige blokken worden gevonden?
- Hoe wordt dat voorkomen?

- Een blok is alleen geldig met een geldige hash
- Een hash is alleen geldig als het kleiner of gelijk is aan een “target hash”
- De target hash reguleert de “mining difficulty”

SAXION HOGESCHOOL

Wat is de Target Hash?



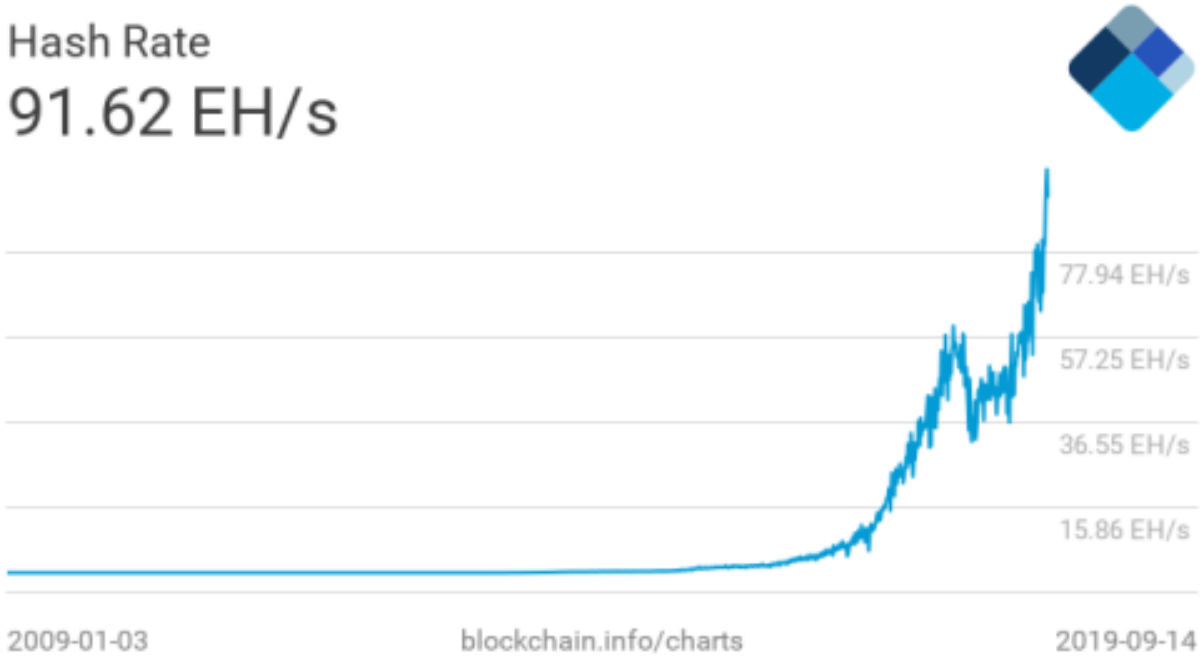
- Door de nonce te veranderen, verandert de hash-waarde
- Alle hash-waarden boven de target hash zijn ongeldig, dus wordt het blok niet opgenomen in de Blockchain
- Alle hash-waarden onder de target hash zijn geldig, dus wordt het blok opgenomen in de Blockchain

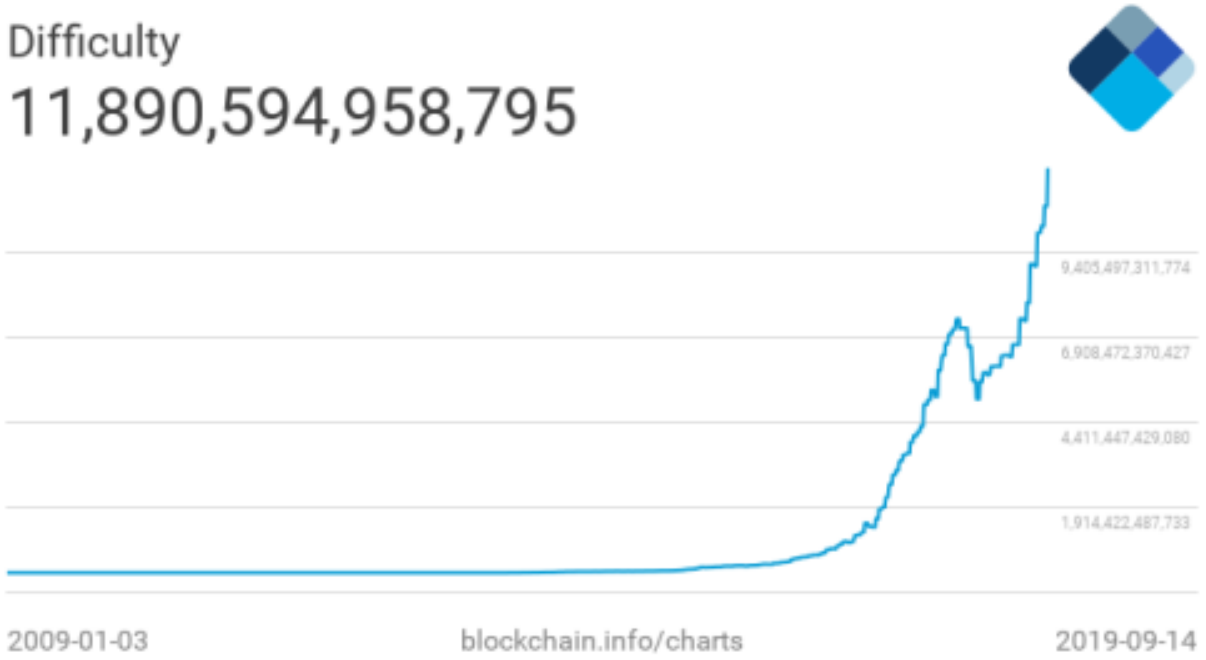
Wat is de rol van de Target Hash?

- Target hash bepaalt de “mining difficulty”. Hoe hoger de Target hash, hoe makkelijker het is om een geldige hash te vinden
- Hoe meer hashing power (computerkracht) er is om hashes te genereren, hoe sneller geldige hashes kunnen worden gevonden, hoe meer blokken er worden aangemaakt
- Om ervoor te zorgen dat er ongeveer 1 blok in de 10 minuten wordt aangemaakt, wordt de Target hash automatisch aangepast om de 2,016 blokken
- Bij meer hashing power, gaat de Target hash omlaag zodat de mining difficulty hoger wordt

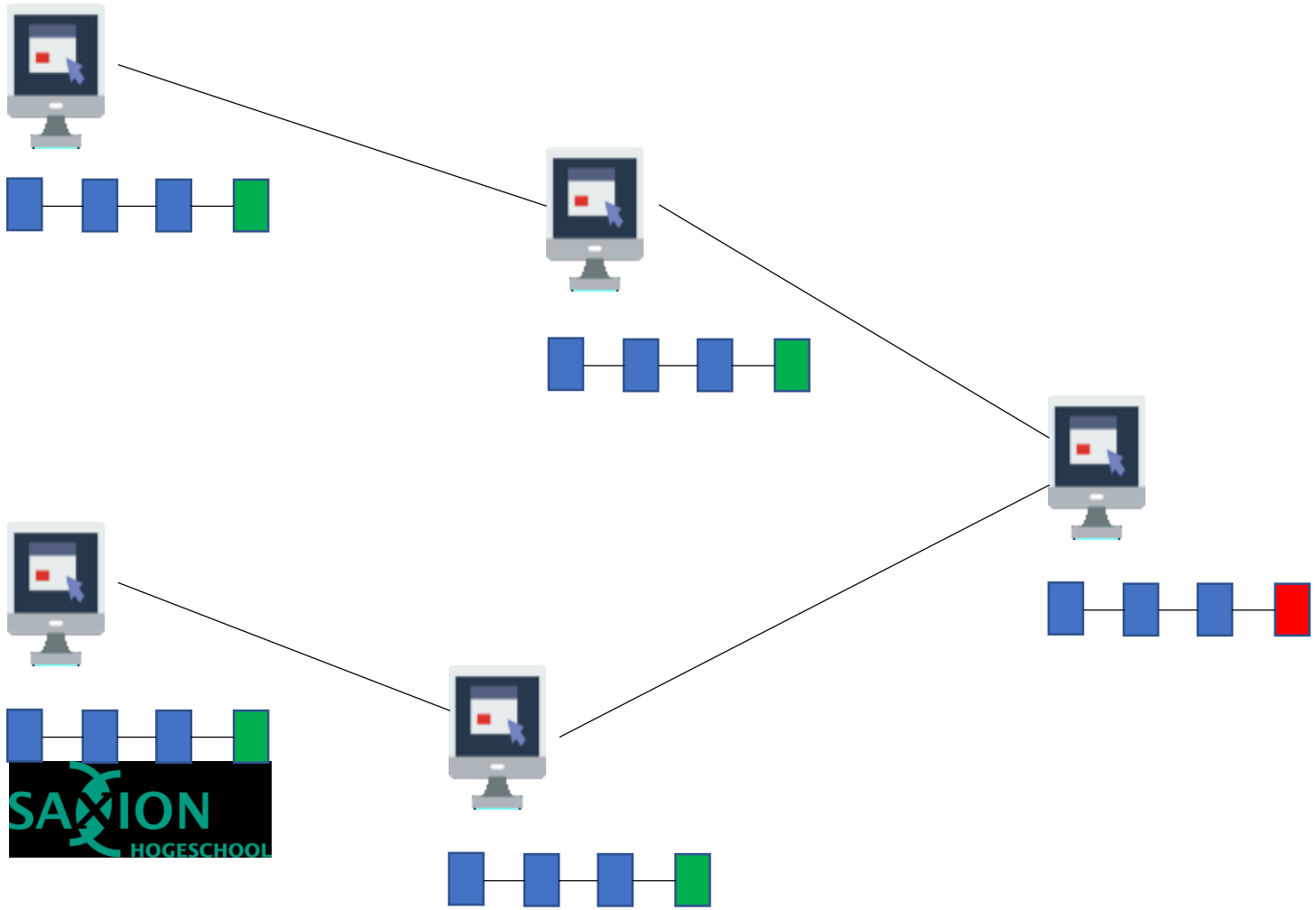
SAXION HOGESCHOOL

Dus een hogere Hash Rate leidt tot een grotere Mining Difficulty



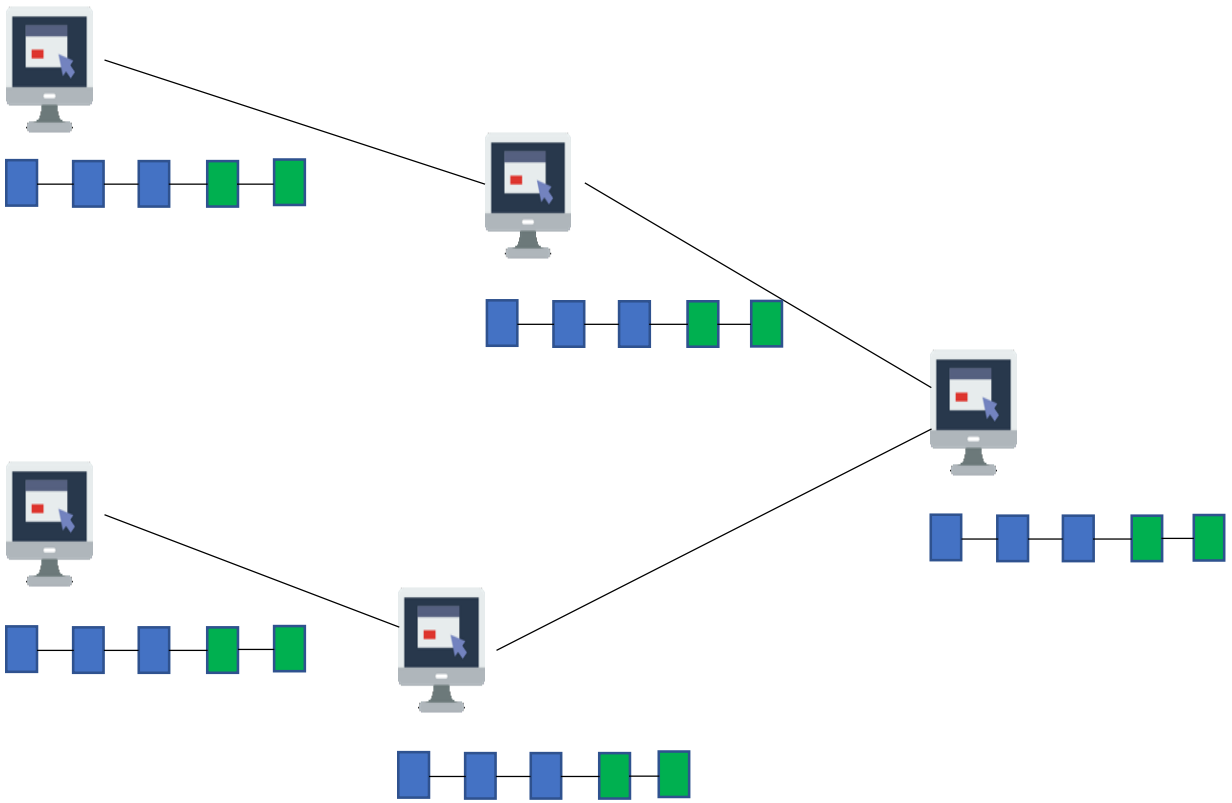


Wat gebeurt er wanneer twee mijners rond dezelfde tijd een geldig blok genereren? (1)



- Mijner met groene blok heeft íéts eerder groen blok aangemaakt en gedeeld met anderen. Andere mijner heeft voordat hij het blok kreeg ook één aangemaakt: het rode blok
- **Het netwerk neemt altijd de langste blockchain aan als waar**
- Als meer mijners met groene blok meer rekenkracht hebben, kunnen zij sneller blokken maken

Wat gebeurt er wanneer twee mijners rond dezelfde tijd een geldig blok genereren? (2)



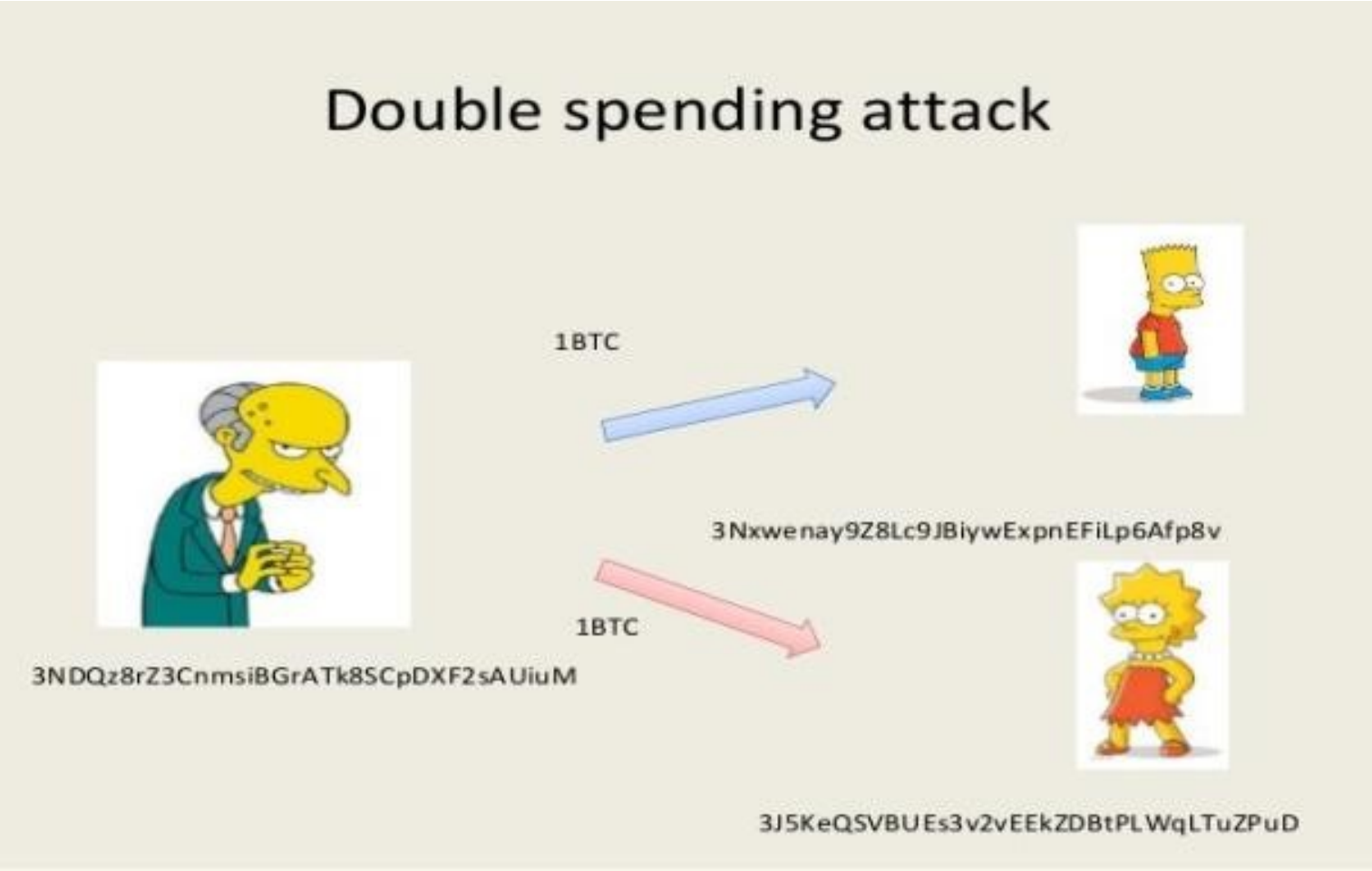
- Mijners met gezamenlijk meer computerkracht, kunnen gezamenlijk sneller geldige blokken vinden
- Naarmate de tijd verstrekt, wordt hun blockchain dus langer en als waar aangenomen
- De rest van het netwerk sluit automatisch over op de langste Blockchain (groen)

Als de langste chain altijd de ware chain is, hoe kun je dan een Proof-of-Work Blockchain hacken?

- Als je meer computerkracht hebt dan de rest samen
- Want dan kun je sneller blokken genereren en de langste chain maken
- Een dergelijke aanval wordt een 51%-aanval genoemd

SAXION HOGESCHOOL

Wat kun je doen als je een 51%-aanval hebt uigevoerd?



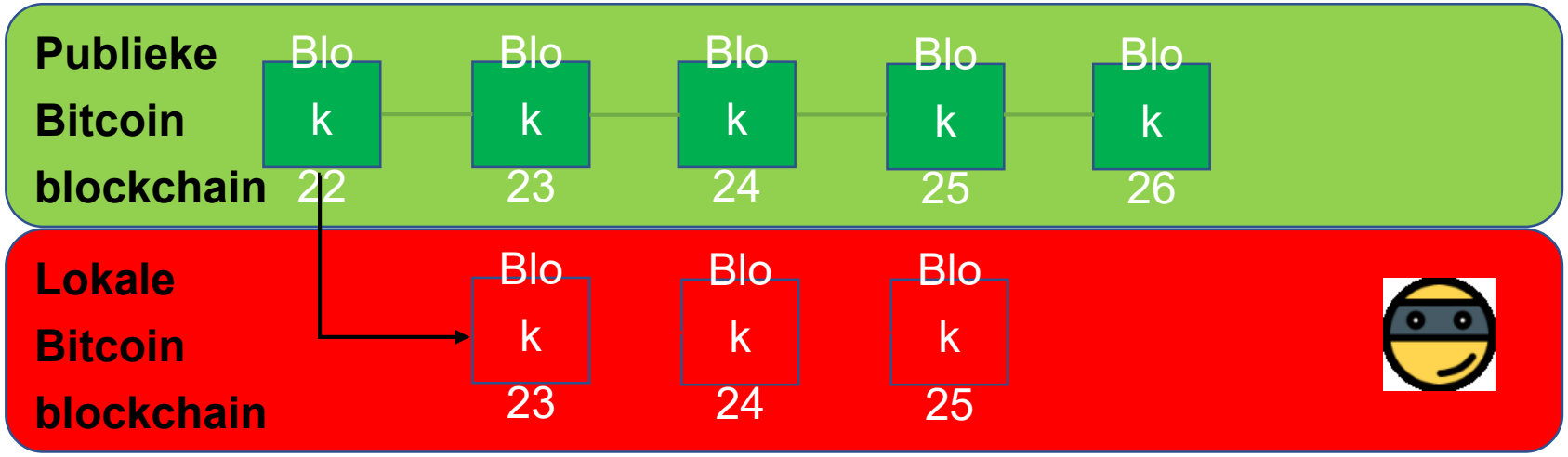
51%-Aanval

De ware blockchain is altijd de langste blockchain. Bij een 51%-aanval creëer je de langste blockchain zodat jouw blockchain als waar wordt gezien.

Deze aanval verloopt volgens 5 stappen.

51%-Aanval: Stap 1

Eerlijke mijners voegen blokken toe aan de publieke Bitcoin blockchain en zenden deze uit over het netwerk. Ondertussen voegt de malafide mijner blokken toe aan de Bitcoin blockchain die hij lokaal houdt op zijn eigen computer. Echter, zendt hij de blokken die hij toevoegt niet uit naar het netwerk voor validatie.



Stap 1 van een 51%-aanval op Proof-of-Work.

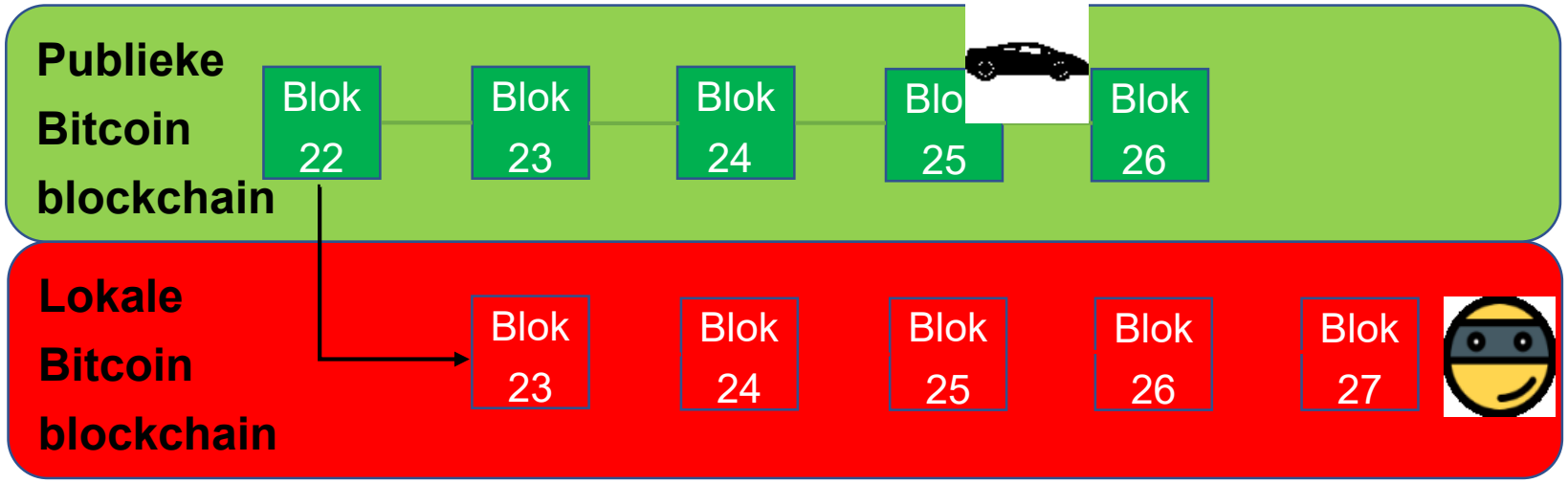
51%-Aanval: Stap 2

De malafide mijner spendeert zijn Bitcoin op de publieke blockchain in blok 25 – bijvoorbeeld voor de aankoop van een Lamborghini. De transactie wordt goedgekeurd door het netwerk en opgenomen in blok 26. De verkoper heeft niet door dat hij te maken heeft met een malafide mijner en geeft hem een Lamborghini mee. Ondertussen voegt de mijner deze transactie niet toe aan zijn lokale Bitcoin blockchain.

SAXION HOGESCHOOL

51%-Aanval: Stap 3

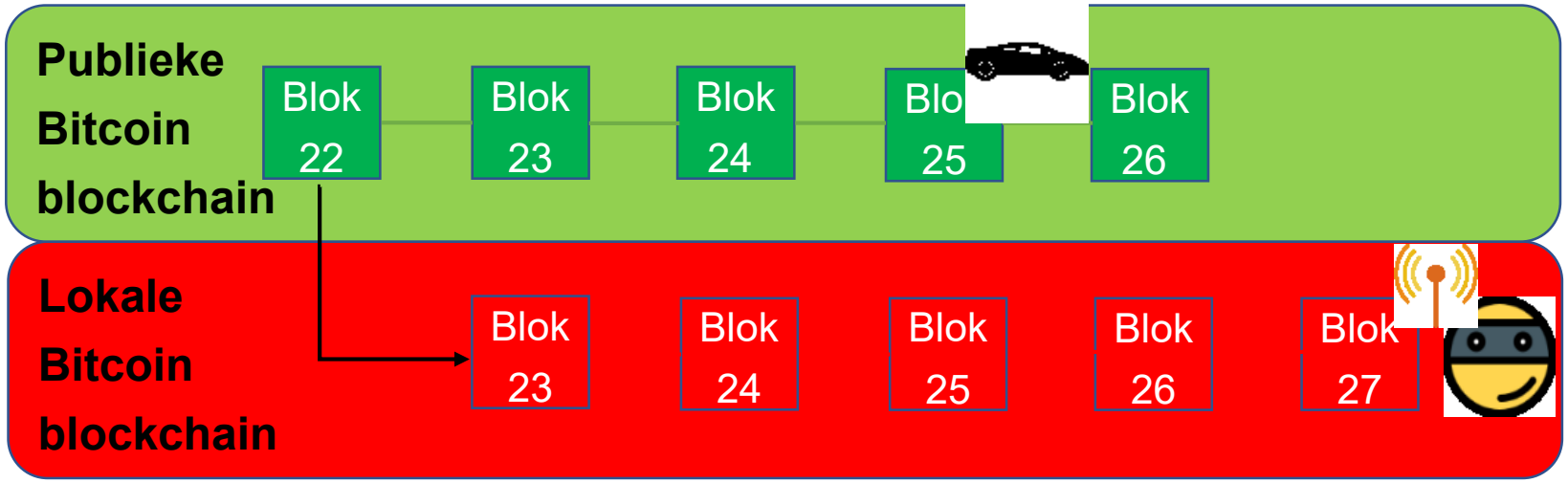
Eerlijke mijners blijven blokken toevoegen aan de publieke blockchain. Er wordt echter niet meer zo snel nieuwe blokken toegevoegd, omdat de malafide mijner zijn computerkracht heeft onttrokken van de publieke chain. Hij richt zijn computerkracht op het produceren van nieuwe blokken op zijn eigen lokale blockchain. Aangezien hij meer hashing power heeft dan alle eerlijke mijners op de publieke blockchain samen, kan hij sneller blokken aanmaken. Hij haalt de publieke blockchain in en heeft nu een langere blockchain.



Stappen 2 en 3 van een 51%-aanval op Proof-of-Work.

51%-Aanval: Stap 4

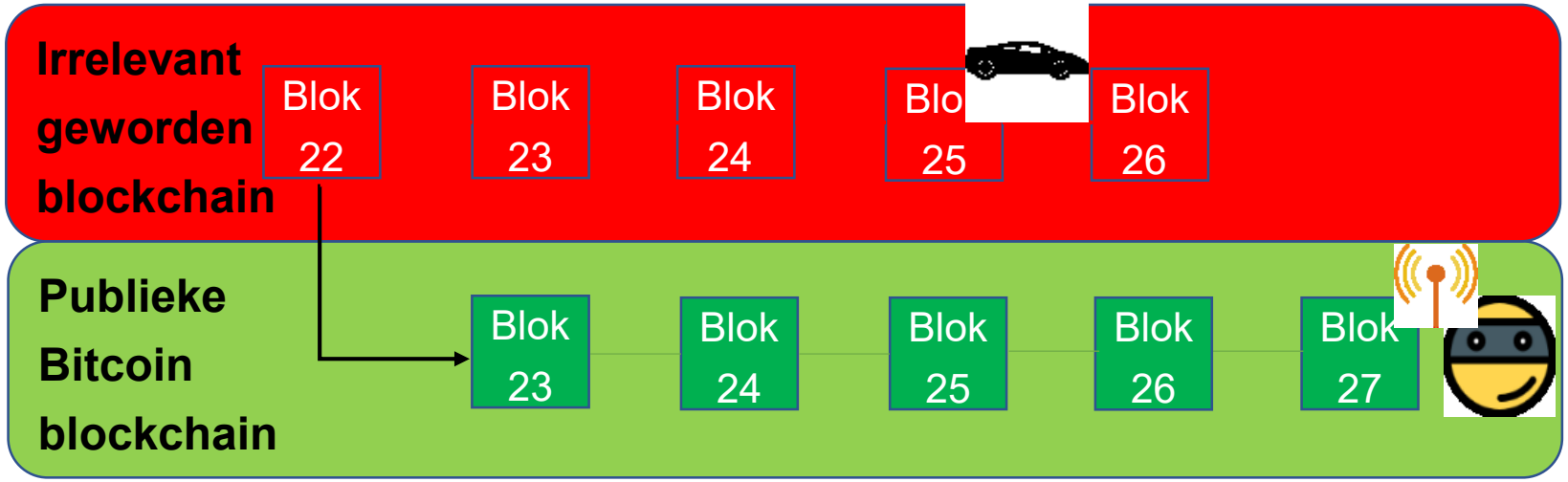
Eerlijke mijners volgen altijd het protocol en het protocol mandateert dat zij de langste versie van de blockchain moeten volgen. De malafide mijner zendt zijn langere versie van de blockchain uit naar de rest van het publieke netwerk. Dit zorgt ervoor dat de eerlijke mijners automatisch overgaan op de blockchain versie van de malafide mijner. Alle Bitcoin balansen en vorige transacties zullen in overeenstemming met de malafide blockchain worden geüpdate.



Stap 4 van een 51%-aanval op Proof-of-Work.

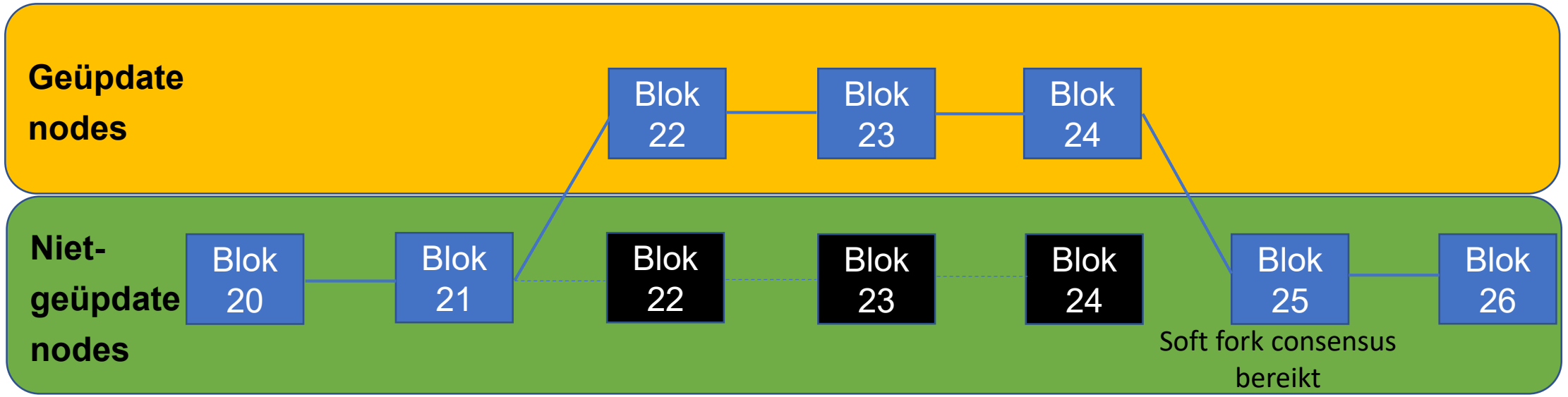
51%-Aanval: Stap 5

De oude publieke blockchain wordt verlaten, omdat deze korter is. Alle data binnen deze gehele blockchain is nu irrelevant geworden. Omdat de Bitcoins die hij op de publieke blockchain heeft uitgegeven aan een Lamborghini nooit is gespendeerd op zijn lokale blockchain, krijgt de malafide mijner weer de beschikking over deze Bitcoins en kan hij ze nogmaals spenderen. Met andere woorden, de malafide mijner kan zijn Bitcoins double spenden.



Stap 5 van een 51%-aanval op Proof-of-Work.

Soft Forks: tijdelijke divergentie met Blockchain protocol



- Soft-forked nodes volgen niet de originele regels, maar de geüpdate regels
- De geüpdate regel behoeft meerderheidsconsensus om te worden ingevoerd
- Software code schrijft voor dat x% van consensus nodig is bij een bepaald Blok #. Anders gaat de update niet door en keert iedereen terug op de oude software

een sucesvolle soft fork, worden geüpdate nodes herkend als degenen met de sterkste en ware chain

is backwards compatible

Voorbeeld: blokgrootte verkleinen van 1MB naar 300kb

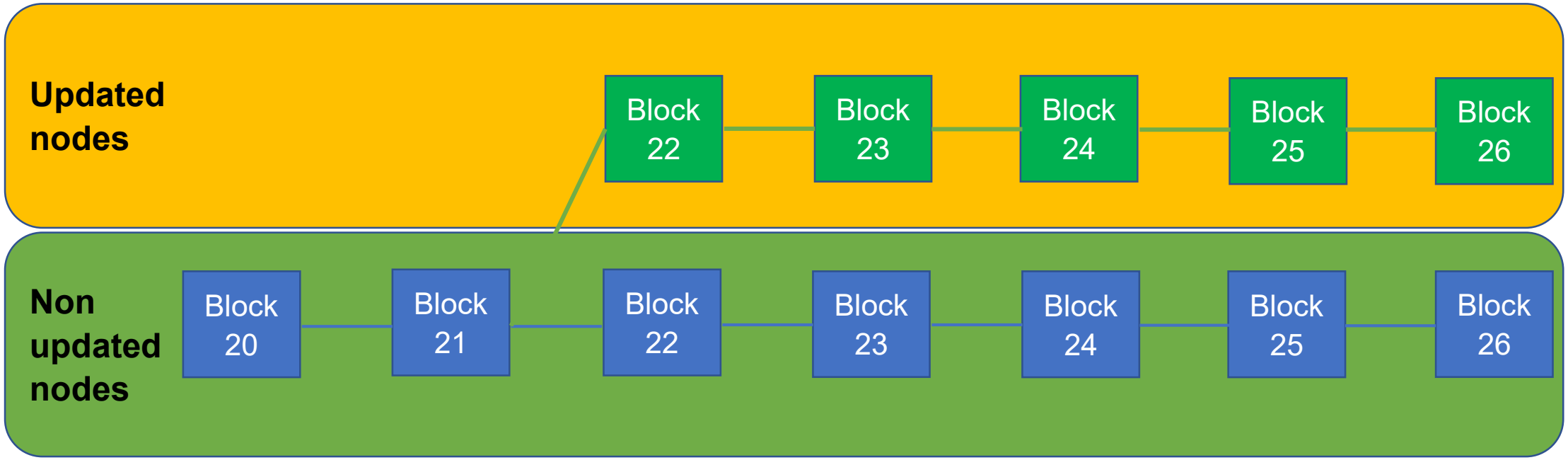
- Nieuwe regel om de blokgrootte te verkleinen van 1MB naar 300kb
- Oude nodes kunnen nog steeds kleinere blokken accepteren, want 300kb < 1MB
- 1MB blokken die wél door oude nodes kunnen worden geaccepteerd, kunnen niet door nieuwe nodes worden geaccepteerd
- Oude nodes die graag willen dat hun blokken worden geaccepteerd door iedereen, stappen over naar de nieuwe software

Voordeel: Tijdelijke splitsing van de blockchain, dus het netwerk verliest maar tijdelijk computerkracht

Nadeel: geen recht op vrijwillige associatie, iedereen wordt gedwongen gebruik te maken van dezelfde software versie

SAXION HOGESCHOOL

Hard Fork: permanente divergentie met Blockchain protocol



- Is niet backwards compatible
- Oude en nieuwe chains lopen parallel naast elkaar
- De coins op de ene chain zijn niet uitwisselbaar met de coins van de andere chain
- Elke chain heeft zijn eigen coins: Bitcoin / Bitcoin Cash

SAXION HOGESCHOOL

Voorbeeld: vergroting van blokgrootte van 1MB naar 2MB

- Niet compatible met oude nodes die nog de vorige software versie hebben
- Blokken die groter zijn dan 1MB worden niet geaccepteerd door nodes die een blokgrootte limiet van 1MB hebben
- M.a.w. de blokken op de nieuwe chain (2MB) zijn niet compatible met de oude chain (1MB)

Voordeel: vrijwillige associatie, het recht om je af te scheiden

Nadeel: computerkracht wordt verdeeld over twee chains. Dit maakt het netwerk minder veilig

SAXION HOGESCHOOL

De Ethereum DAO hack

Anti Hard Fork:

- "Code is law" - the original statement of The DAO terms and conditions should stand under any circumstances
- Things that happen on the blockchain are immutable and they should never change regardless of what the outcome is
- There is a slippery slope and once you modify/censor for one reason there is not a lot to keep you from doing it for other contracts
- The decision to return the money is short sighted and you might reduce the value of ETH down the line based on your decision to act
- This is a bailout

Pro Hard Fork:

- "Code is law" is too drastic of a statement at the current time and humans should have the final say through social consensus
- The hacker could not be allowed to profit from the exploit as it is ethically wrong and the community should intervene
- The slippery slope argument is not valid as the community is not beholden to past decisions, people can act rationally and fairly in each situation
- It would be problematic to leave such a big piece of the Ether supply in the hands of a malicious actor and it might harm the value of Ether down the line
- This is not a bailout as money isn't being taken from the community, it is just a return of funds to the original investors
- It would stop an ongoing war between the white-hat hackers and the hacker that would demoralize the community and possible continue for many years
- The exploit was big enough to take action and reverse it
- If the community acts now it will make people that are unethical think twice before using Ethereum as their platform of choice
- A hard-fork to return the funds would keep regulators and the legal system out of the debate: "our mess, we fixed it."

Een meerderheid van de mensen (89%) stemden voor een Hard-Fork wat plaats vond tijdens blok 1920000 (20 juli, 2016).



SAXION HOGESCHOOL

AGENDA DAG 2 – 13 November

Diepere achtergrond, gevolgen Blockchain, praktische cybercrime voorbeelden.

09.00 Recap dag 1
09.30 De praktijk met tools door Eljo Haspels CEO Cointell.
11.30 Verdieping blockchain en bouwstenen.

12.30 Lunch

13.15 Verdieping Blockchain en bouwstenen.
14.15 Consensusprotocollen en public, private, consortium.
15.45 Serey. Waar moet je aan denken als je een blockchain project opzet?
15.30 De casus
16.50 Afsluiting en reflectie.

SAXION HOGESCHOOL




Lunch

AGENDA DAG 2 – 13 November

Diepere achtergrond, gevolgen Blockchain, praktische cybercrime voorbeelden.

09.00 Recap dag 1
09.30 De praktijk met tools door Eljo Haspels CEO Cointell.
11.30 Verdieping blockchain en bouwstenen.

12.30 Lunch

13.15 Verdieping Blockchain en bouwstenen.
14.15 Consensusprotocollen en public, private, consortium.
15.45 Serey. Waar moet je aan denken als je een blockchain project opzet?
15.30 De casus
16.50 Afsluiting en reflectie.

SAXION HOGESCHOOL




Verdieping Blockchain
en bouwstenen.

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply
1	Bitcoin	$71,700,857,000	$4,070.37	$9,442,289,532	17,615,300 BTC
2	Ethereum	$14,705,075,208	$139.48	$4,257,196,143	105,428,907 ETH
3	XRP	$12,909,564,535	$0.309533	$699,421,876	41,706,564,590 XRP *
4	EOS	$3,873,560,791	$4.27	$2,158,630,318	906,245,118 EOS *
5	Litecoin	$3,737,233,138	$61.17	$1,878,667,982	61,090,861 LTC
6	Bitcoin Cash	$3,012,967,984	$170.24	$580,721,340	17,697,938 BCH
7	Binance Coin	$2,367,403,855	$16.77	$192,554,810	141,175,490 BNB *
8	Stellar	$2,071,026,639	$0.107652	$216,446,430	19,238,133,492 XLM *
9	Tether	$2,052,184,429	$1.01	$8,258,098,498	2,028,143,500 USDT *
10	Cardano	$1,719,197,329	$0.066309	$80,282,096	25,927,070,538 ADA

Bouwstenen van Blockchain 2.0

Bitcoin is ideaal om waarde te versturen. Het is echter niet mogelijk om met Bitcoin condities en voorwaarden vast te leggen in transacties. Ethereum komt op als Blockchain 2.0 voor smart contracts en decentralized applications.

Om nieuwe coins uit te geven op de Bitcoin Blockchain werd “Colored Coins” geïntroduceerd.

1. dApps (decentralized applications)
2. Smart contracts
3. Distributed Autonomous Organization (DAO)
4. Tokenization van bedrijven en projecten

SAXION HOGESCHOOL

Blockchain 2.0: Decentralized Applications (dApps)

Applicatie die is gebouwd op een Blockchain en daardoor geniet van de voordelen van decentralisatie

Voorbeelden:

- Bitcoin (valuta applicatie) die is gebouwd op de Bitcoin Blockchain
- Steepshot is gebouwd op Steem Blockchain
- Serey is gebouwd op Serey Blockchain

SAXION HOGESCHOOL

Top Dapps

#	Name	Category	Protocol	Users 24h	Volume 24h
1	**PRA CandyBox**	Other	EOS	6.5k +7.65%	$0 0 —
2	**ENBank**	Other	EOS	6.4k -2.47%	$0 0 —
3	**EOS Knights**	Games	EOS	5.6k +1.19%	$1.7k 395.03 +2.12%
4	**TronBank**	High-Risk	TRON	4.5k +6.57%	$428.6k 18.4M +7.28%
5	**p3t.network**	High-Risk	TRON	3.2k +1.56%	$30.8k 1.3M -53.65%
6	**EOSBet**	Gambling	EOS	3.2k +9.81%	$1.2M 274.8k +23.25%
7	**DTH (Decentralized-Texas-...**	Gambling	EOS	3.1k +0.13%	$61.1k 14.2k +7.00%

Blockchain 2.0: Smart Contracts

ethereum

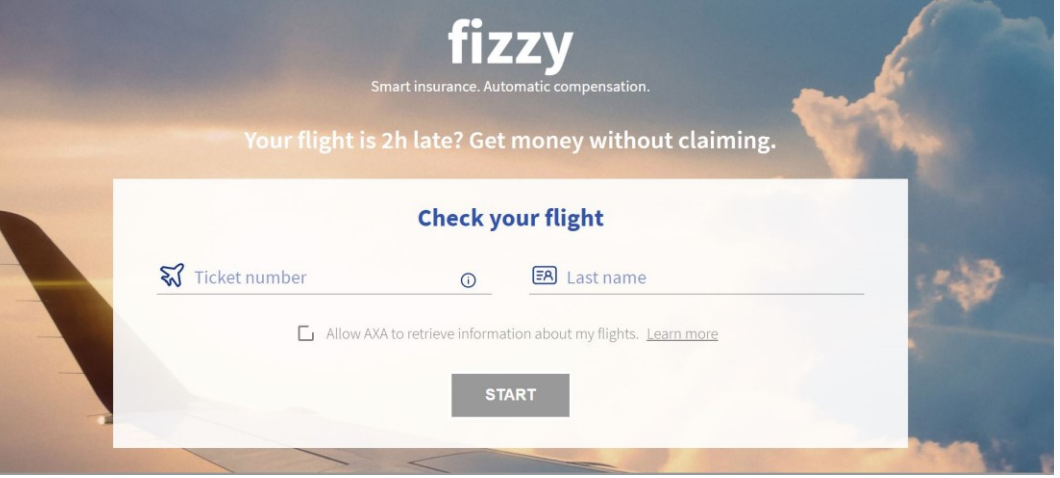
Wat als je contracten wil uitvoeren zonder tussenpartijen?

Smart Contracts
Contracten met condities en voorwaarden die in code zijn vastgelegd en zichzelf automatisch uitvoeren. Ze zijn traceerbaar op de blockchain en onomkeerbaar.

Simpel voorbeeld, AXA Verzekeringen:

1. Jij koopt een verzekering tegen vluchtvertraging en allerlei andere voorwaarden op Fizzy (https://fizzy.axa)
2. De aankoop wordt geregistreerd in een smart contract
3. Het smart contract is verbonden met global air traffic databases en zoekt of jouw vlucht vertraging heeft
4. Bij 2+ uur vertraging wordt het smart contract getriggered om jou automatisch te vergoeden
5. Afhandeling is dus volledig overgedragen aan een onafhankelijk netwerk. Er is geen [illegible]erwerk, geen aanvraag voor vergoeding en geen interpretatie van mensen die de aanvraag moeten goedkeuren

SAXION HOGESCHOOL



SIMULATION

I enter my flight details

COVERAGE

I personalize my coverage

IDENTITY

I fill in my personal information

PAYMENT

I subscribe

DELAY

In case of delay (2h+), my compensation is triggered

COMPENSATION

I receive my indemnity directly on my bank account

Wat zijn Orakels en wat is het Orakel probleem?

- Een ***orakel*** is een externe bron die het smart contract voedt met informatie die relevant is voor de contractuele overeenkomst
- Blockchains en smart contracts kunnen uit zichzelf geen data van buiten hun netwerk benaderen
- In het voorbeeld van Fizzy maakt het smart contract gebruik van data die afkomstig is van de databases van het globale luchtverkeer
- ***Orakel probleem*** is dat er vertrouwd moet worden op derde partijen om het smart contract te voeden met externe data

SAXION HOGESCHOOL

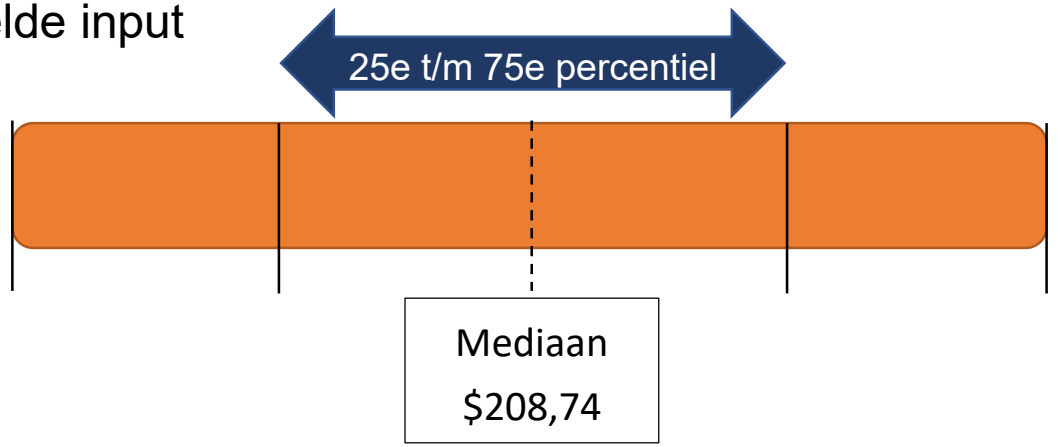
Wat zijn Orakels en wat is het Orakel probleem?

Orakel is een externe bron die het smart contract of dApp voedt met informatie van buiten de Blockchain.

Orakel probleem = je moet vertrouwen op orakels (3e partijen) dat ze juiste informatie doorspelen naar de blockchain.

Oplossingen:

1. Gebruik maken van meerdere databronnen voor gemiddelde input
2. Gebruik maken van Schelling points voor mediane input
3. Gebruik maken van beloningsysteem
4. …

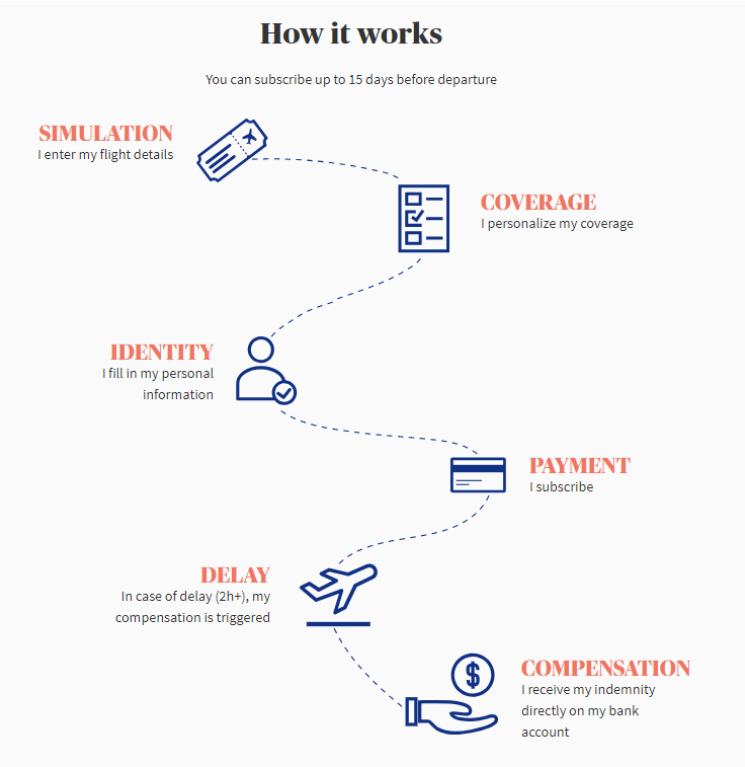


Twee typen Smart Contracts



1. **Deterministisch**: heeft geen data van een oracle nodig om een smart contract uit te kunnen voeren
   - Vb: Getallen loterij waarbij winnend getal wordt bepaald door de laatste drie cijfers van een hash
   - Hash: … 01ab2d8ce90adf27
   - Transparant en traceerbaar

2. **Non-deterministisch**: heeft wél data nodig van een oracle om een smart contract uit te kunnen voeren
   - Vb: Fizzy





Mankind made a huge leap forward regarding human organization when it implemented the Constitution. Man was no longer to be ruled by kings and despots, but by a document that stipulated the rule of law. Still, we had the issue of who was going to interpret these laws and who was allowed to add new rules.

Now, we have made another revolutionary leap forward in human organization. We don't need a third party – kings, governments, courts – to interpret the laws anymore if we have self-executing smart contracts that eliminate the need to trust these third parties. Trust is established through mass collaboration and clever code. On top of that, everyone is free to opt-in, to submit new rules, and to participate in a set of rules. No one is forced to participate. You can always opt out and secede. We have had many secessions in the blockchain space. Bitcoin Cash seceded from Bitcoin Core, Ethereum seceded from Ethereum Classic etc. It is therefore a peaceful means to organize human beings.

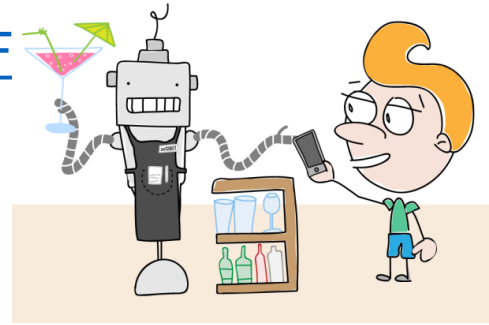
This is, in my opinion, the fundamental revolution of blockchain: a peaceful trust machine for social agreements and human organization.

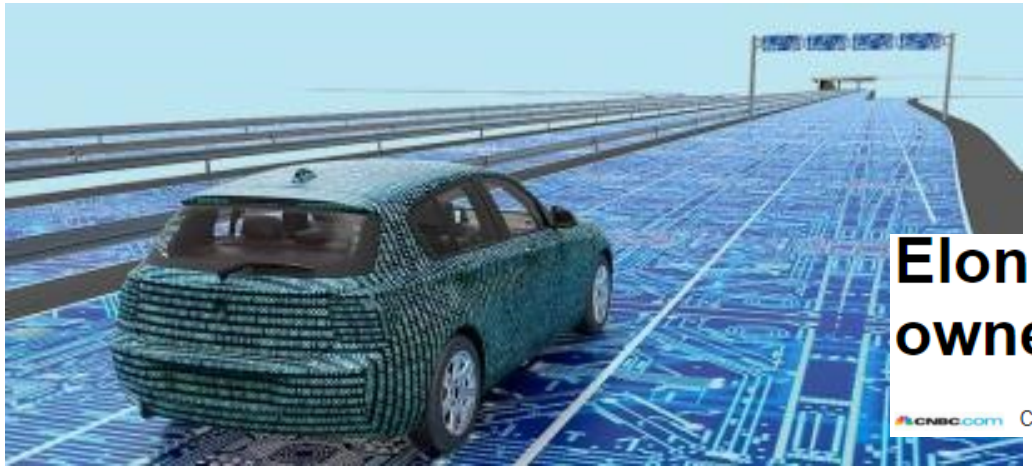
SAXION HOGESCHOOL

Distributed Autonomous Organization (DAO)

- Business model zonder een centraal beslissingspunt. Het is geen traditionele organisatie met werknemers (managers, board of directors, CEO etc.)
- **Consequenties**: autonome organisaties. DAOs zetten bedrijven (Uber, Facebook, Twitter etc.) “out of business”
- **Voorbeelden**: Autonome auto die wordt beheerd door een groep mensen en waarvan de winsten automatisch worden verstuurd naar de groep middels smart contracts

Lees ook: [Chhay Lin Lim - Machines that own themselves in SAF]





Elon Musk: Self-driving Teslas are going to make their owners money by competing with Uber, Lyft

CNBC.com CNBC • April 5, 2019


Co-founder
FRED EHRSAM
PARADIGM

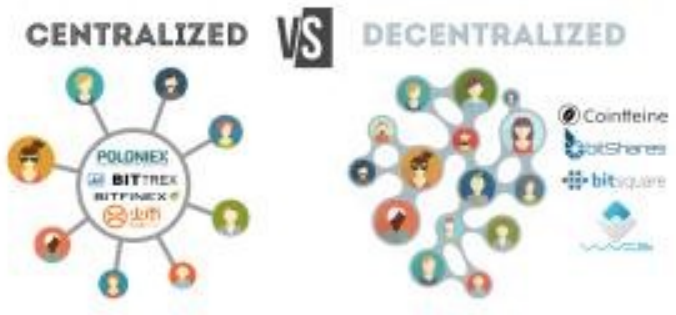
Praktische Opdracht:
BitShares - Decentralized Exchange en DAO

1. Registreer
2. Maak een eigen crypto token
3. Verhandel deze op de exchange

SAXION HOGESCHOOL

Gecentraliseerde VS Gedecentraliseerde Exchanges

Gecentraliseerd Exchange	Gedecentraliseerd Exchange (DEX)
Centrale server (SPOF)	Geen centrale server (P2P exchange)
Beheren jouw fondsen (en hebben jouw private key)	Gebruiker beheert zijn eigen fondsen en bezig zelf zijn eigen private key)
Niet anoniem, vaak moet je KYC doen	(Pseudo)anonym
Gevoelig voor hacks (single point of entry)	Minder gevoelig voor hacks (multiple points of entry)
Gevoelig voor server downtime	Minder gevoelig voor server downtime
Vaak grotere handelvolumes	Minder handelvolumes
Snel	Sommige zijn snel
Makkelijker te reguleren door overheidsinstanties	Moeilijker te reguleren door overheidsinstanties

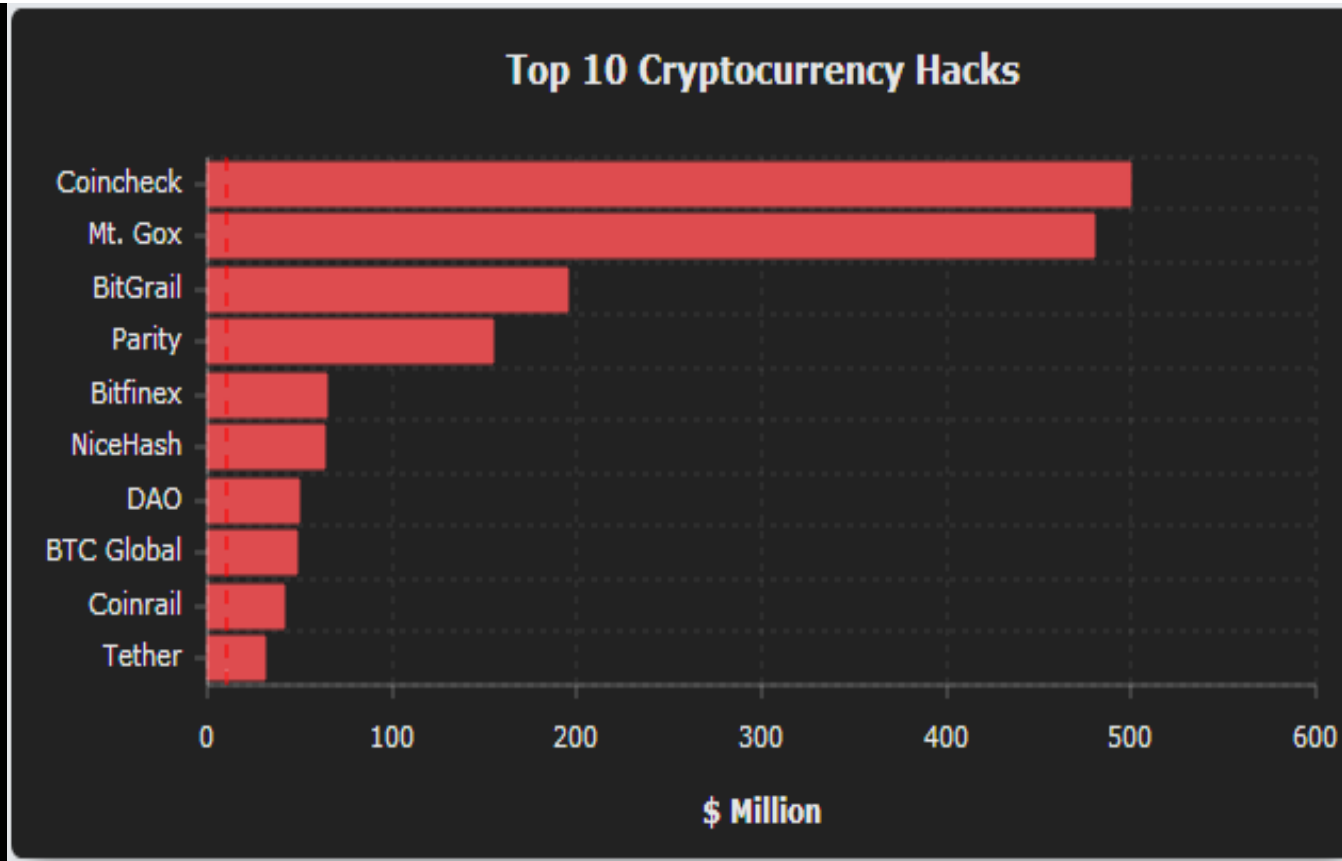


Gecentraliseerde Exchanges (omzet en hacks)

"I definitely hope **centralized exchanges** go burn in hell as much as possible."

- Vitalik Buterin (6 juli, 2018)





“Whereas most technologies tend to automate workers on the periphery doing menial tasks, **blockchains automate away the center**. Instead of putting the taxi driver out of a job, **Blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly**.”

- Vitalik Buterin (2015)

Tokenization

- Tokenization is het process waarbij rechten op assets worden gerepresenteerd door digitale tokens (coins) op een Blockchain
- Aandelen, onroerend goed, goud, airmiles etc. kunnen worden gedigitaliseerd in tokens en verhandeld op de Blockchain
- Handelen kan 24/7, onmiddellijk, tegen lage kosten, met meer transparantie en veiligheid
- Daarnaast kunnen projecten worden gefinancieerd door middel van coins (ICO)
- **Consequentie**: “Internet of value”

SAXION HOGESCHOOL

Internet of Value

1. Cryptocurrency: Bitcoin
2. Platform: Ethereum
3. Utility: Augur
4. Security: aandelen
5. Natural asset: goud, olie
6. Collectibles: unieke digitale assets als kunt en e-sports kaarten
7. Crypto-fiat/stable: bit.USD



AGENDA DAG 2 – 13 November

Diepere achtergrond, gevolgen Blockchain, praktische cybercrime voorbeelden.

09.00 Recap dag 1
09.30 De praktijk met tools door Eljo Haspels CEO Cointell.
11.30 Verdieping blockchain en bouwstenen.

12.30 Lunch

13.15 Verdieping Blockchain en bouwstenen.
14.15 Consensusprotocollen en public, private, consortium.
15.45 Serey. Waar moet je aan denken als je een blockchain project opzet?
15.30 De casus
16.50 Afsluiting en reflectie.

SAXION HOGESCHOOL

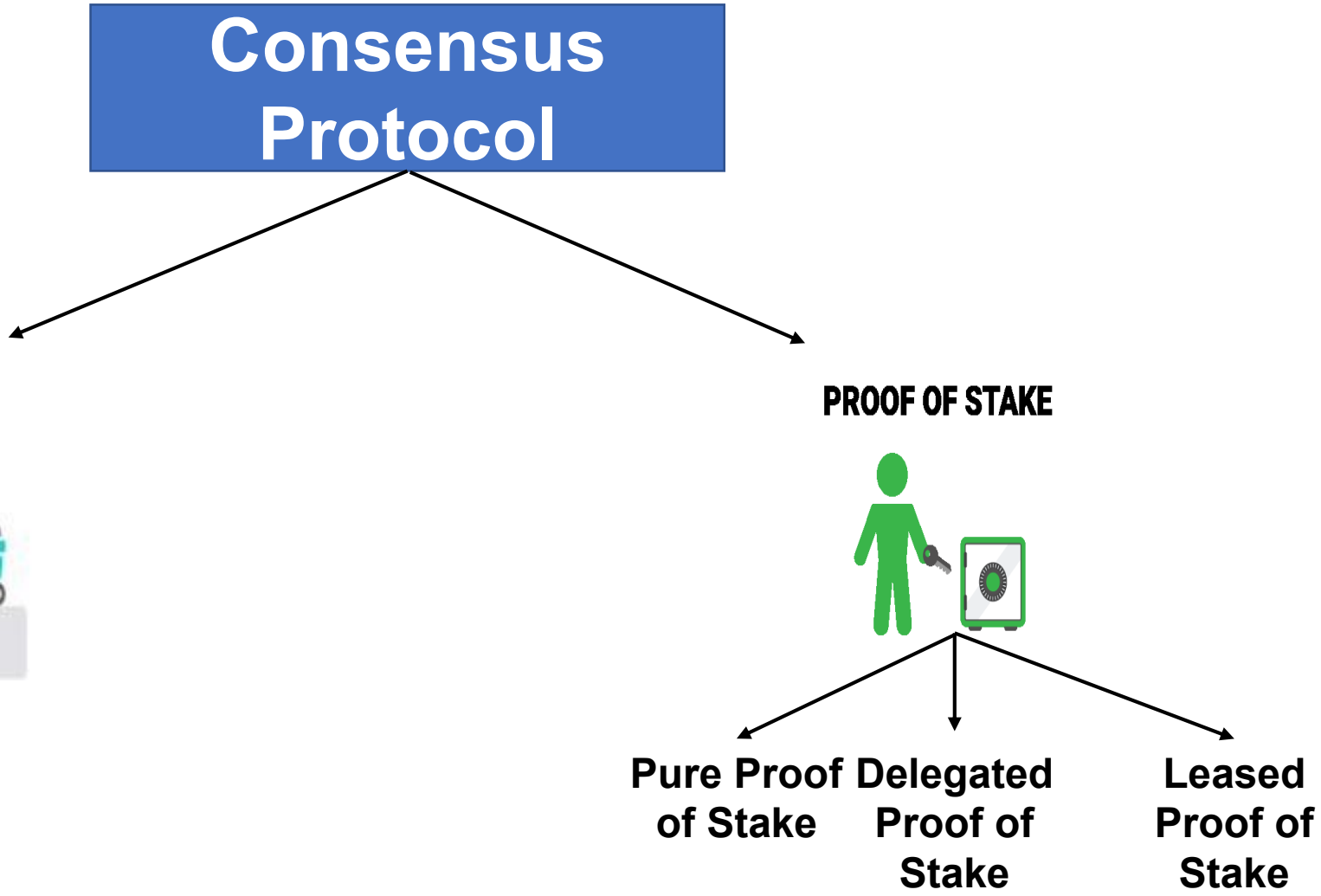



Consensusprotocollen
en public, private,
consortium.

Consensus

Het doel van **consensus** is om **double-spending** te voorkomen. Dit kan worden voorkomen als er overeenstemming is over de ware blockchain. Een goed consensus mechanisme beloont “goed” gedrag en straft “slecht” gedrag af.





Proof of Work vs Proof of Stake

1. Mijners zoeken naar een nonce, resulterend in een geldige hash om een blok te mogen toevoegen aan de blockchain
2. De kans om een blok te mogen toevoegen is gebaseerd op de rekenkracht (hashing power) die je levert aan het netwerk
3. Bewezen, goed werkend concept
4. Verbruikt veel energie
5. 51% aanval door meerderheid van computerkracht

Vb: Bitcoin



1. De kans om een blok te mogen toevoegen aan de blockchain is afhankelijk van je ‘stake’ in de blockchain. De blokproducent wordt een ‘forger’ genoemd
2. De stake is gebaseerd op het aantal coins dat je hebt
3. Stel je voor, je hebt 1% van alle SAX coins. Bij PoS, heb je dan ook 1% kans om een nieuw blok te mogen toevoegen en daar rewards voor te ontvangen
4. ‘Staken’ geeft je een passief inkomen
5. 51%-aanval door meerderheid van de coins te bezitten

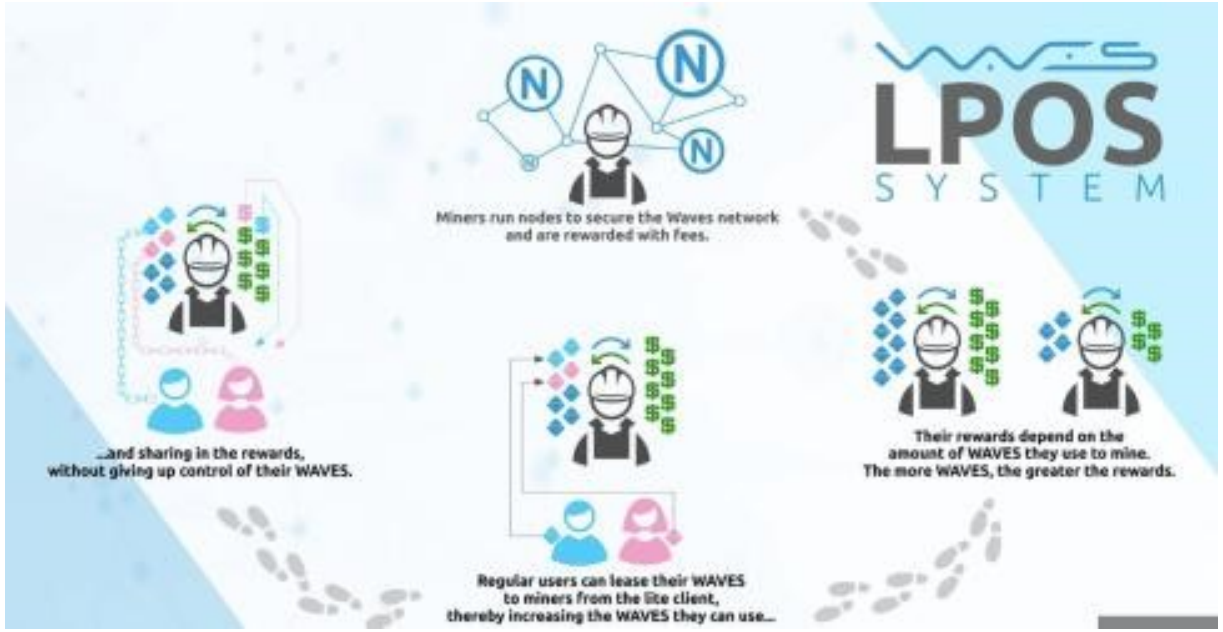
Vb: PiVX, NAVcoin, Reddcc





Leased Proof of Stake (LPoS)

1. Je kan je stake **leasen** aan een ander (pool) om samen meer kans te hebben een nieuw blok te mogen toevoegen
2. De pool krijgt een beloning voor de blokproductie
3. De pool keert jou een gedeelte van de winst uit



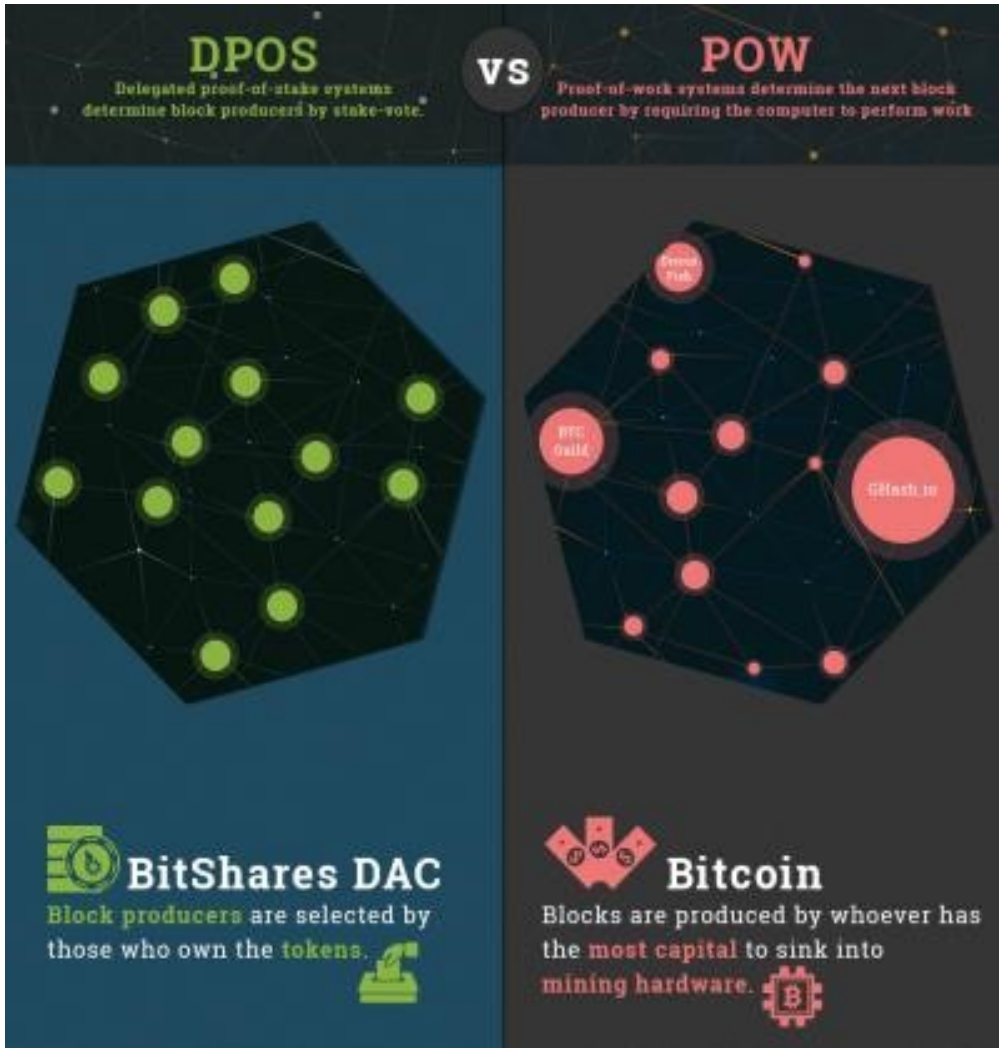
- Vb: WAVES

SAXION HOGESCHOOL

Delegated Proof of Stake (DPoS)

1. Er is direct en continue democratisch proces waarbij mensen met een **stake** kunnen stemmen op **gedelegeerden (witnesses)**
2. Er zijn een aantal actieve witnesses en reserved witnesses die blokken mogen toevoegen aan de blockchain
3. Énorm grote aantal trx/sec. BitShares kan 3,300 trx/sec verwerken

- Vb: BitShares, EOS, Serey, Lisk, Tron



Andere Consensusprotocollen

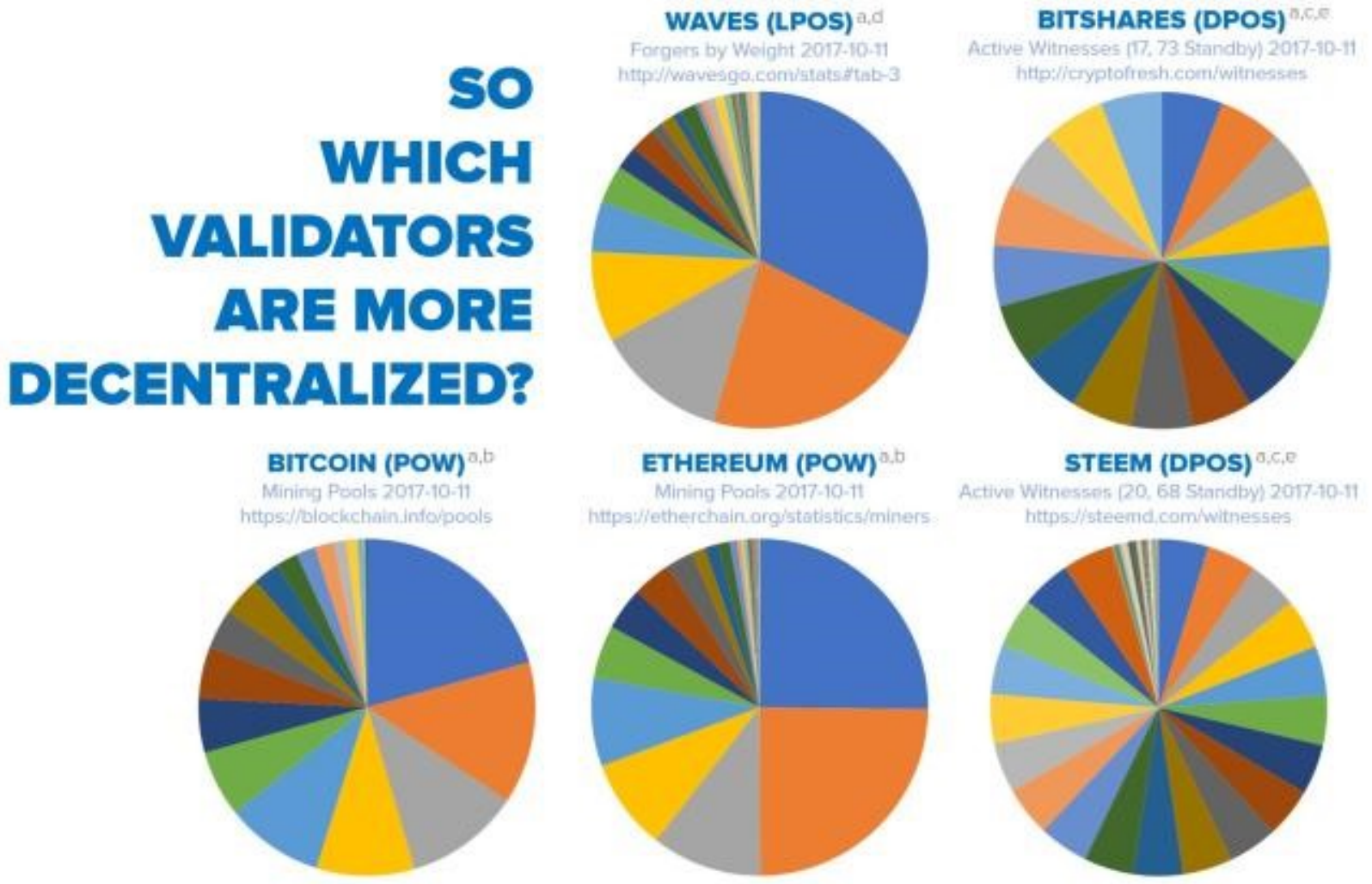


Hoe hebben PoS, LPoS en DPoS invloed op …

1. Beveiliging: 51% aanval
2. Decentralisatie
3. Energie-efficiëntie
4. Schaalbaarheid

SAXION HOGESCHOOL

Decentralisatieniveau



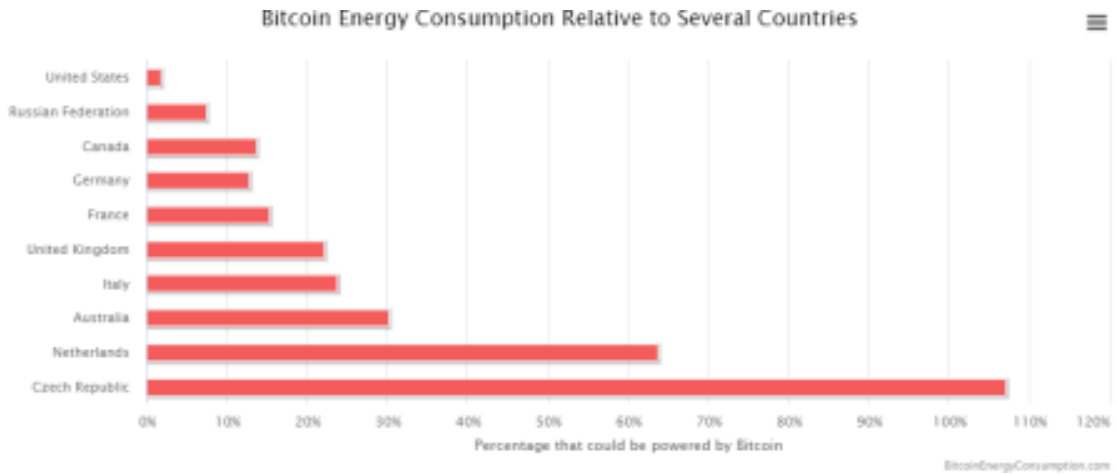
Bitcoin Energieconsumptie

Annualized Total Footprints

Carbon Footprint	Electrical Energy	Electronic Waste
34.73 Mt CO2	73.12 TWh	10.50 kt
Comparable to the carbon footprint of **Denmark**.	Comparable to the power consumption of **Austria**.	Comparable to the e-waste generation of **Luxembourg**.

Single Transaction Footprints

Carbon Footprint	Electrical Energy	Electronic Waste
289.38 kgCO2	609.21 kWh	87.60 grams
Equivalent to the carbon footprint of **723,439** VISA transactions or **48,229** hours of watching Youtube.	Equivalent to the power consumption of an average U.S. household over **20.59** days.	Equivalent to the weight of **1.35** 'C'-size batteries or **1.91** golf balls.



Bron: https://www.digiconomist.net/bitcoin-energy-consumption

Schaalbaarheid en Consensusmechanisme

		Activity			Value	Index	
#	Name	Activity	Average (7d)	Record	Market Cap	AVI	CUI
1	EOS	47,008,658 Op	47,515,598 Op	89,240,619 Op	$2.7 B	3,007	
2	TRX	1,672,203 Op	1,729,427 Op	5,306,869 Op	$0.931 B	316	
3	STEEM	996,699 Op	996,699 Op	2,522,380 Op	$0.047 B	3,734	
4	KIN	879,513 Op	940,419 Op	5,258,216 Op	$0.006 B	23,939	
5	BTC	844,493 Op	806,433 Op	1,178,080 Op	$148 B	1.0	
6	BTS	689,629 Op	774,688 Op	6,112,075 Op	$0.077 B	1,579	
7	ETH	631,901 Op	650,433 Op	1,372,918 Op	$19 B	6	
8	IOST	365,369 Op	513,835 Op	874,225 Op	$0.057 B	1,122	
9	TFD	306,963 Op	306,226 Op	662,359 Op	$0.002 B	25,533	
10	MHC	295,466 Op	431,336 Op	1,256,700 Op	$0.006 B	8,844	
11	WAVES	284,593 Op	221,519 Op	6,141,108 Op	$0.083 B	599	

- Consensusmechanisme heeft impact op de schaalbaarheid
- Er is altijd een trade-off tussen decentralisatie en schaalbaarheid
  - Gecentraliseerde consensusmechanismen (DPoS) hebben grotere schaalbaarheid
- De Top 4 en Nr. 6 maken allemaal gebruik van DPoS en gebruiken slechts een fractie van hun max aantal trx/sec
- Bitcoin en Ethereum zitten regelmatig op hun max aantal trx/sec

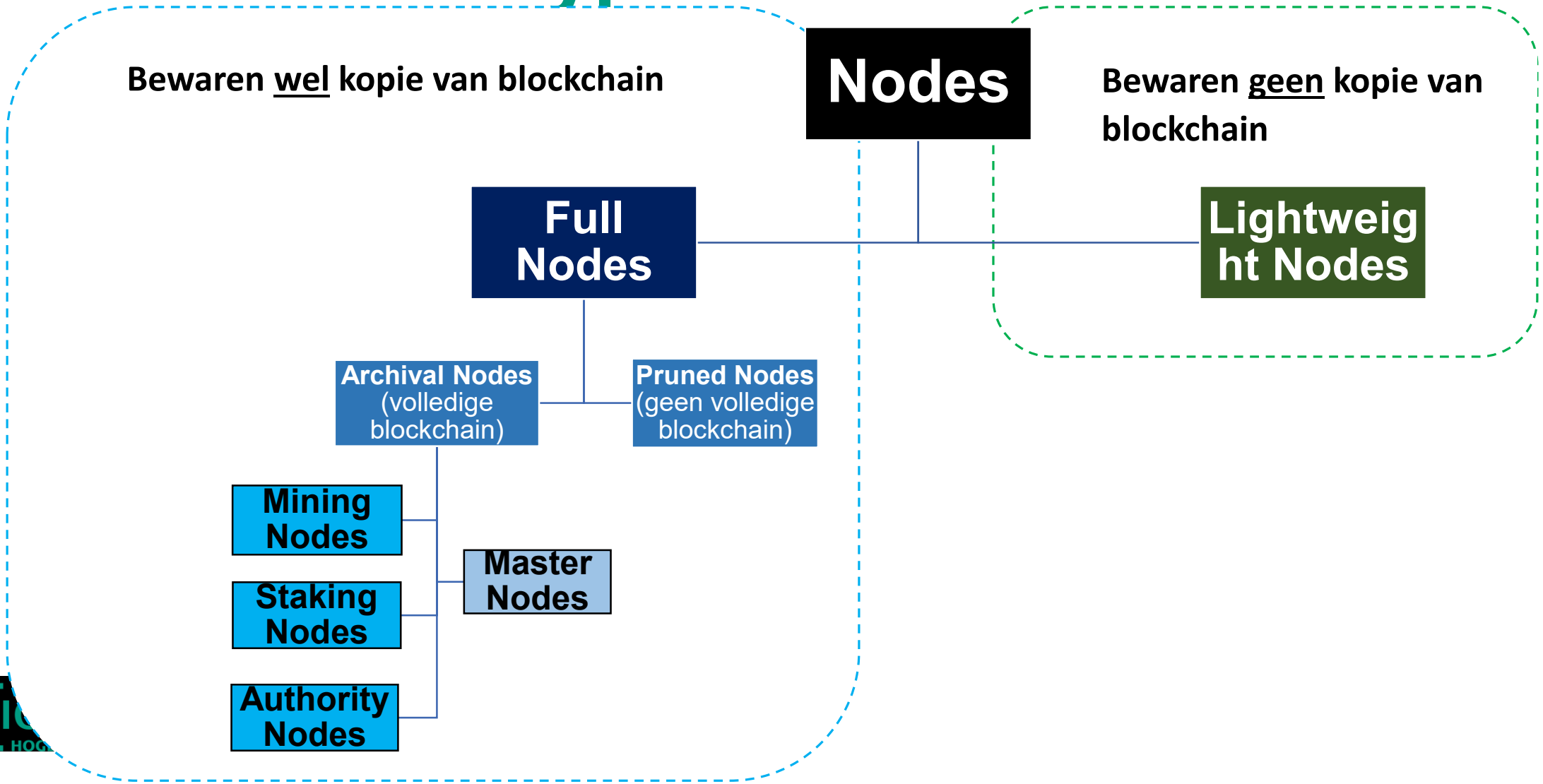
Hoeveel transacties zitten er in de Bitcoin mempool?

8547 Unconfirmed Transactions Live updating list of new bitcoin transactions

Summary	Status:Connected
Total Fees	29.89147943 BTC
Total Size	105812.533 (KB)
Transactions Per Second	6.74



Verschillende typen Nodes

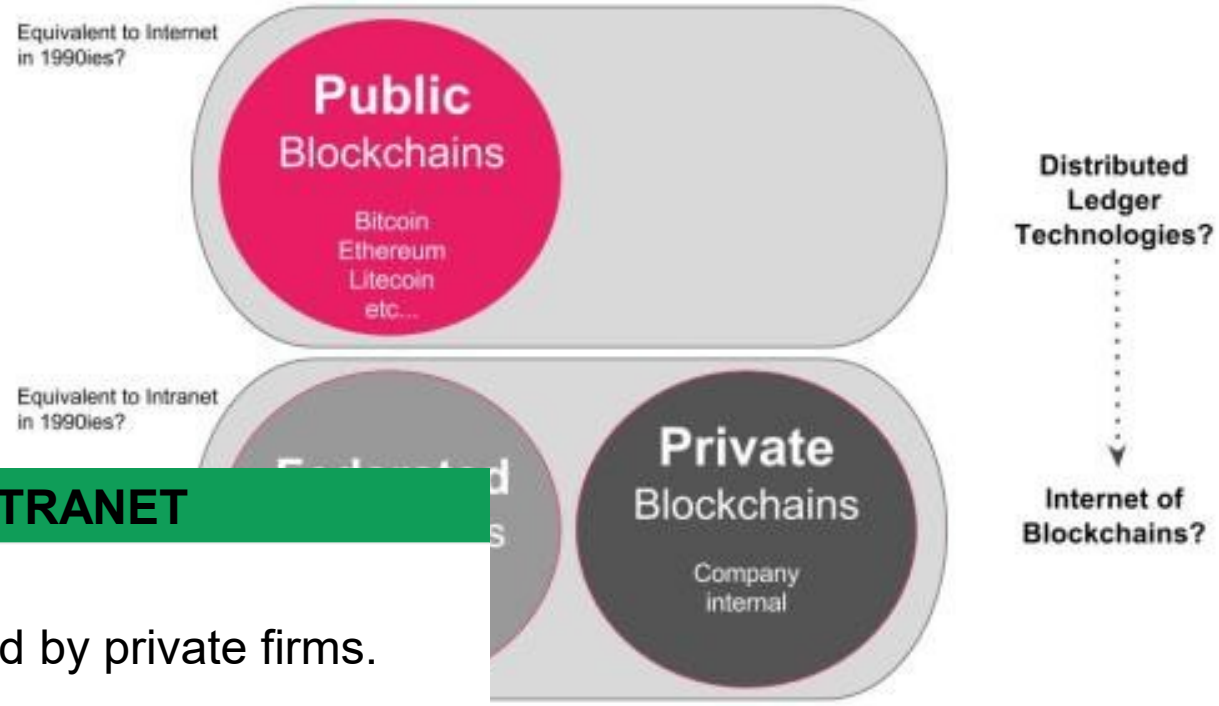


Verschillende typen Nodes (2)

1. **Full nodes**: hebben volledige blockchain en stemmen op proposals
   a) **Pruned Nodes**: heeft een limiet (bv. 500MB) voor volledige blockchain. Wanneer limiet is bereikt, verwijderen ze de oude blokken en bewaren ze daarvan alleen de header
   b) **Archival Nodes**: behouden altijd volledige versie van de blockchain
      i. **Mining nodes**: gebruiken computerkracht om een geldige blok te maken en toe te voegen
      ii. **Staking nodes**: houden coins in de wallet. De kans om een blok te mogen toevoegen is afhankelijk van hoeveel ‘stake’ je hebt
      iii. **Authority nodes**: een select groepje nodes die worden gekozen om blokken aan te mogen maken, toe te voegen en transacties te verifiëren
      iv. **Masternodes**: hebben extra gespecialiseerde functies. Ze moeten wel collateral hebben (bv. 1,000 Dash). Krijgen gegarandeerd inkomen
2. **Lightweight nodes**: hebben geen kopie van de blockchain. Zij zoeken naar de status van het laatste blok en leveren nieuwe transacties aan. Mobile wallets of lite wallets zijn lightweight nodes

SAXION HOGESCHOOL

Public vs Consortium vs Private Blockchains



S.NO	INTERNET	INTRANET
1.	Internet is used to connect different network of computers simultaneously.	Intranet is owned by private firms.
2.	In internet, there are multiple users.	In intranet, there are limited users.
3.	Internet is unsafe.	Intranet is safe.
4.	In internet, There are more number of visitors.	In intranet, There are less number of visitors.
5.	Internet is a public network.	Intranet is a private network.
6.	Anyone can access Internet.	In this, anyone can't access the Intranet.
7.	Internet provides unlimited information.	Intranet provides limited information.

chain	*Private blockchain*
les	One organisation
	Could be public or restricted
l	Could be tampered
	High
	Yes
	Permissioned

Libra: Consortium Blockchain



Network of partners

The Libra Association is governed by diverse businesses, nonprofit and multilateral organizations, and academic institutions. Organizations join the association by running a validator node on the network and serving in governance.

This initial group of organizations will work together to finalize the Libra Association's charter and will become the association's Founding Members upon its completion.

Zie ook [Chhay Lin Lim – Opheldering over Facebooks nieuwe Cryptomunt, de Libra]

Zie ook [Libra Hearing Day 1: Biggest Facepalm Moments]

SAXION HOGESCHOOL

Bekende Blockchain allianties



	Ethereum Enterprise Alliance	Hyperledger	R3 Corda
Industrie	Verschillend	Verschillend	Financieel
Governance	Ethereum	Linux Foundation	R3 consortium
Rollen als verifieerder en blokproducent	Permissionless en permissioned	Permissionless en permissioned	Permissioned
Token economie	Ether (ETH)	Geen-/-wel mogelijk	Geen/in toekomst mogelijk
Consensus mechanisme	PoW	Pluggable	Pluggable
Smart contracts	Ja	Ja	Ja

Permissionless: iedereen mag de blockchain helpen onderhouden

Permissioned: select aantal deelnemers mogen blockchain onderhouden

Bedrijven zien de limitaties van open blockchains en experimenteren met permissioned blockchains

Antonopoulos: Blockchain of Bullshit?

Volgens Andreas Antonopoulos dienen Blockchains de volgende eigenschappen te hebben. Anders zijn ze “Bullshit”.

1. Open
2. Grenzeloos
3. Neutraal: iedereen wordt gelijk behandeld door het network
4. Censuur resistent: data is niet te censureren door een derde partij
5. Publiekelijk: voor iedereen toegankelijk

Consortia zijn als een kartel en hebben te veel incentives om het consensusprotocol te veranderen of te riggen. Ze zullen de markt proberen te manipuleren. Daarnaast brengen ze veel security issues met zich mee: sleutels kunnen worden gelekt en zijn onmogelijk te beveiligen.

https://www.youtube.com/watch?v=Rv4nTMfAZo0

AGENDA DAG 2 – 13 November

Diepere achtergrond, gevolgen Blockchain, praktische cybercrime voorbeelden.

09.00 Recap dag 1
09.30 De praktijk met tools door Eljo Haspels CEO Cointell.
11.30 Verdieping blockchain en bouwstenen.

12.30 Lunch

13.15 Verdieping Blockchain en bouwstenen.
14.15 Consensusprotocollen en public, private, consortium.
15.45 Serey. Waar moet je aan denken als je een blockchain project opzet?
15.30 De casus
16.50 Afsluiting en reflectie.

SAXION HOGESCHOOL




Serey. Waar moet je aan denken als je een blockchain project opzet?

AGENDA DAG 2 – 13 November

Diepere achtergrond, gevolgen Blockchain, praktische cybercrime voorbeelden.

09.00 Recap dag 1
09.30 De praktijk met tools door Eljo Haspels CEO Cointell.
11.30 Verdieping blockchain en bouwstenen.

12.30 Lunch

13.15 Verdieping Blockchain en bouwstenen.
14.15 Consensusprotocollen en public, private, consortium.
15.45 Serey. Waar moet je aan denken als je een blockchain project opzet?
15.30 De casus
16.50 Afsluiting en reflectie.

SAXION HOGESCHOOL



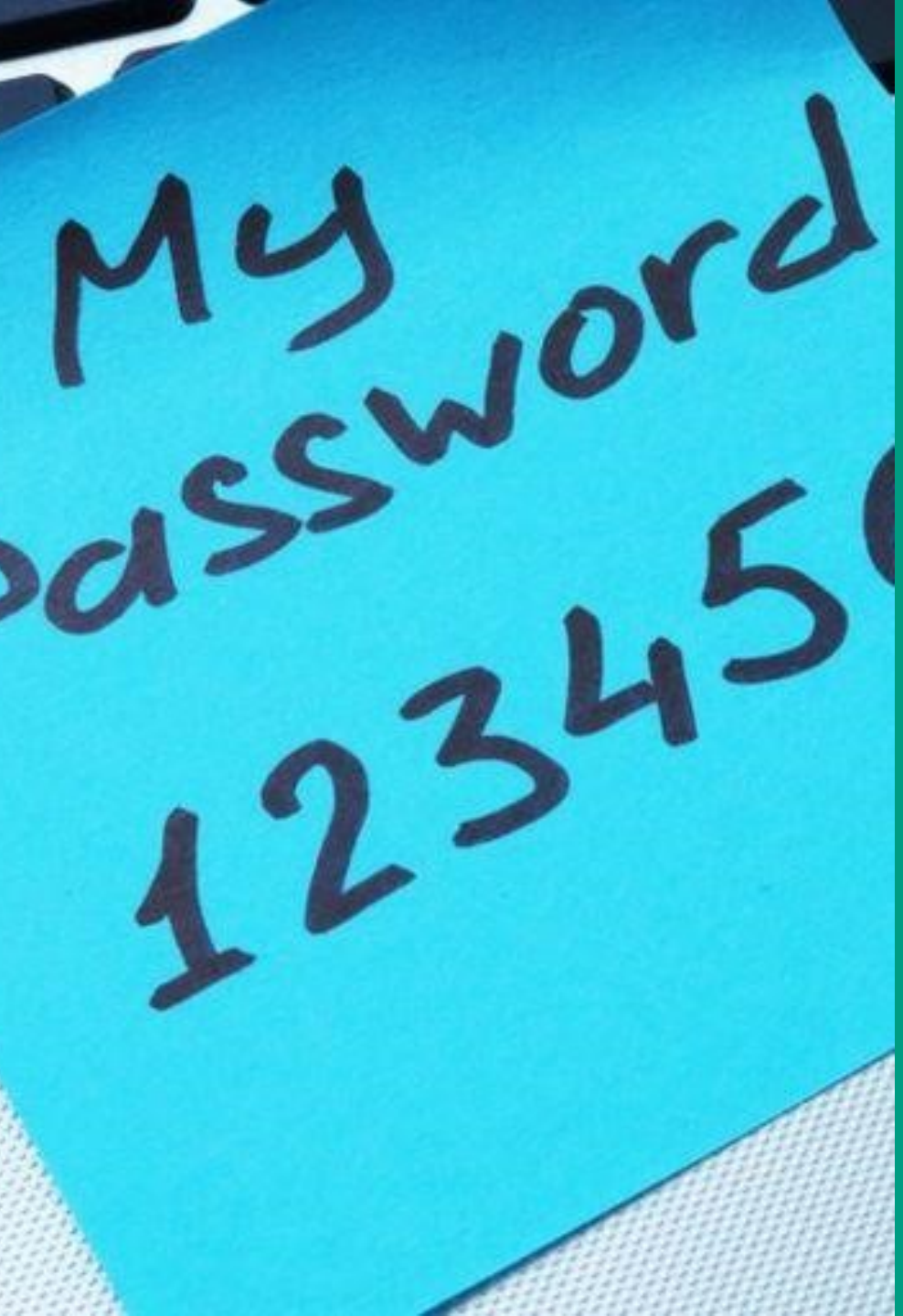

De casus



Thema

Iemand met een technische achtergrond

- Heeft altijd affiniteit gehad met cybercrime en een scheve schaats rijden.
- En hoort van de mogelijkheden van blockchain.
- Hoe zou hij/zij deze decentrale digitale innovatie in kunnen zetten voor eigen gewin?



De komende periode ontwikkelen we in tweetallen een blockchain case

Dag 1: bedenk een case rondom het thema ‘misdaad en blockchain’

Dag 2: business process, bouwstenen en impact

Dag 3: (D)BMC

Dag 4: Presentatie case voor een jury, beste case wint…

De case wordt constant aangescherpt naargelang de masterclass voortgaat

Blockchain case

bedenk een case rondom het thema misdaad en blockchain

Dag 1

Bedenk 2 alternatieve cases

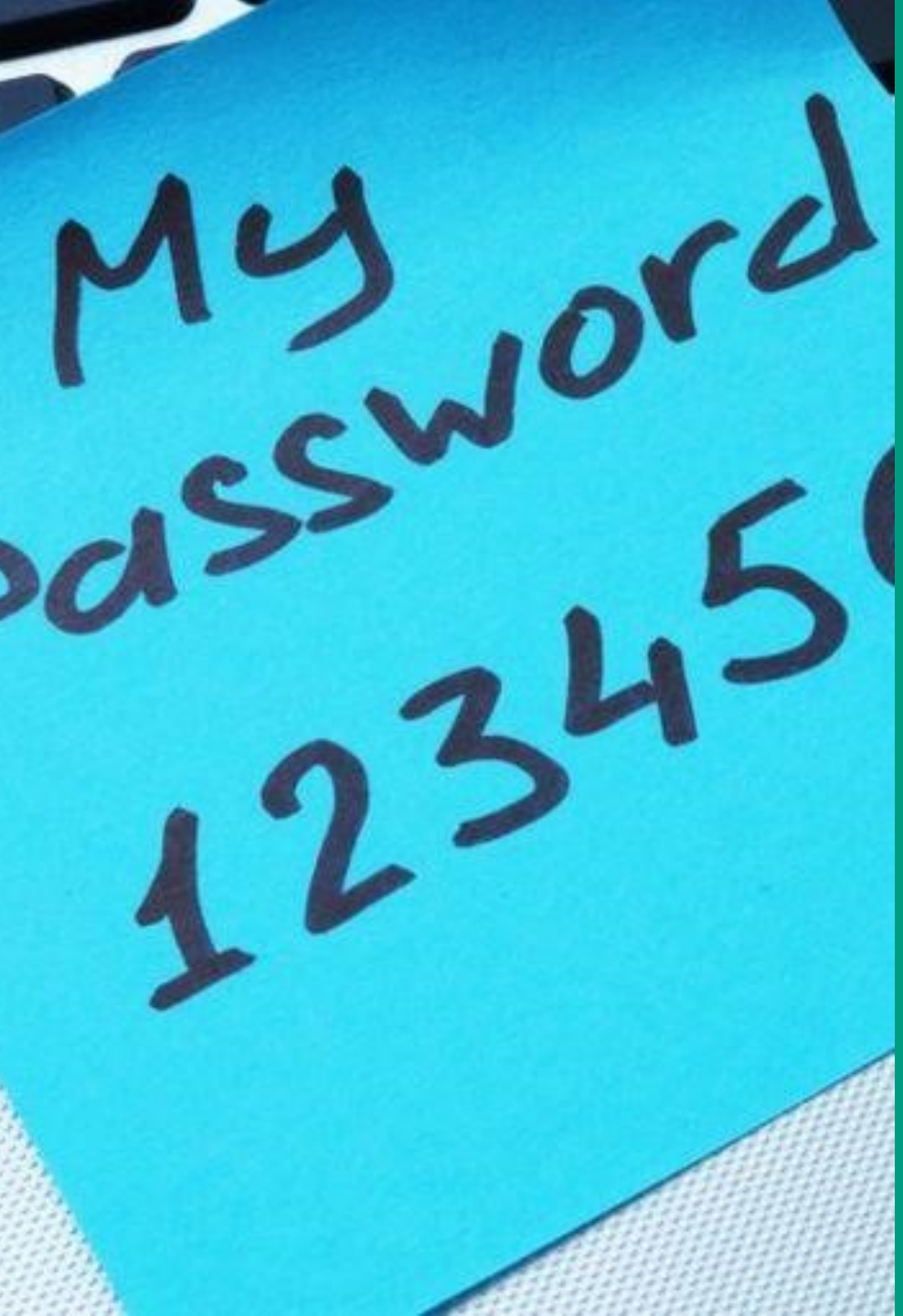
Vul PESTEL in

Maak een heatmap

Maak een ecosysteem

Kies de meest passende case

Welke case heb je waarom gekozen



Vandaag vullen we de basis van dag 1 verder in aan de hand van een voorbeeld van drugshandel

Dag 1: bedenk een case rondom het thema ‘misdaad en blockchain’

2: business process, bouwstenen en impact

Dag 3: (D)BMC

Dag 4: Presentatie case voor een jury, beste case wint…

Dag 2 Casus

agenda

- Business process
- Wat zijn de relevante externe ontwikkelingen
- Welke blockchain bouwstenen staan tot je beschikking
- Welk impact heeft het invoeren van blockchain

SAXION HOGESCHOOL

*het **proces** in 5 stappen*

Voel je vrij een model te ontwerpen waar nog geen process voor bestaat!

Voorbeeld business proces
drugshandel supply chain

1. Een koper en verkoper vinden elkaar en onderhandelen een prijs.
2. De koopovereenkomst wordt ondertekend door beiden.
3. De koper verricht een aanbetaling.
4. De partij wordt ontvangen, gewogen, getest, goedgekeurd.
5. De betaling wordt verricht.

Neem 5 minuten het proces te beschrijven

SAXION HOGESCHOOL

Karakteristieken

waar ligt de impact ligt voor het toepassen van blockchain

Voorbeeld drugshandel supply chain

- Het betreft overdrachten **van hoge waarde**.
- Typisch landsoverschrijdend en daarmee tussenpartijen die tijds-, fout- en fraude gevoelige en inefficiëne **papieren processen** gebruiken.
- **Wederzijdse afstemming van data** speelt een grote rol zoals kwaliteit van het product.
- Er is een hoge mate van **regelgeving** van en **controle** op de dienstverlening
- Er is een groot **wantrouwen** tussen partijen.
- De **identiteitscheck** van het product vindt manueel plaats, zo ook rapportage van ontvangst.

Neem 5 minuten de karakteristieken onderling te bevragen aan elkaar

SAXION HOGESCHOOL

Blockchain heeft vooral nut in situaties waar..

Hoe is dit toepasbaar op het drugshandel voorbeeld?

- Verschillende partijen **gegevens** delen
- **Partijen** bewerken deze gegevens
- Gegevens moeten worden geverifieerd
- **Verificatieproces** is complex en/of kostenverhogend
- Interacties zijn tijdsintensief
- Partijen zijn afhankelijk van elkaar
- Gegevens/transacties betreffen geldwaarde

Neem 10 minuten voor je eigen voorbeeld en benoem hoe welke data onderling wordt uitgewisseld en geverifieerd.

SAXION HOGESCHOOL

Dag 2 Casus

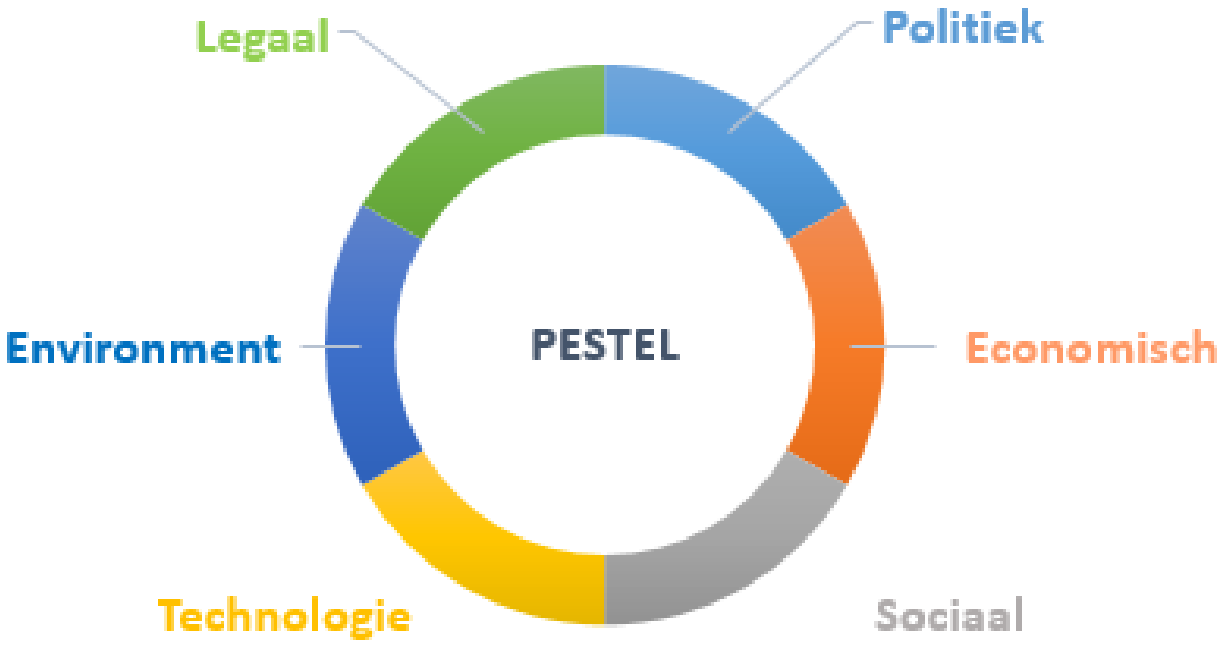
agenda

- Business process
- Wat zijn de **relevante externe ontwikkelingen**
- Welke blockchain bouwstenen staan tot je beschikking
- Welk impact heeft het invoeren van blockchain

SAXION HOGESCHOOL

Zijn hier nog vragen over?

Binnen welke omgeving werkt de crimineel?



Figuur 9 Het PESTEL model.

Rood	Uitdagende ontwikkeling met duidelijke invloed op het business model, actie nodig.
Oranje	Ontwikkeling met mogelijk een invloed op het business model, meer onderzoek nodig.
Groen	Kansrijke ontwikkeling met mogelijk positieve invloed op het business model, actie nodig.
Grijs	Ontwikkeling heeft geen invloed op het business model.

SAXION HOGESCHOOL

Dag 2 Casus

agenda

- Business process
- Wat zijn de relevante externe ontwikkelingen
- Welke **blockchain bouwstenen** staan tot je beschikking
- Welk impact heeft het invoeren van blockchain

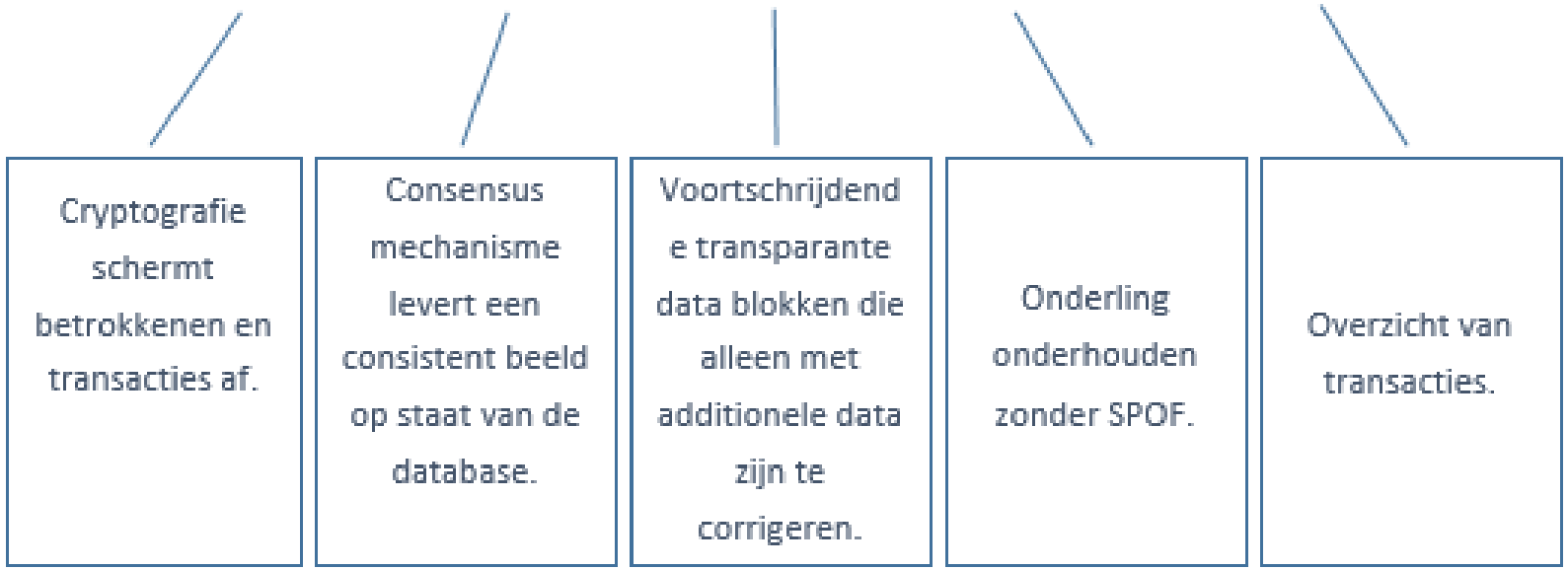
SAXION HOGESCHOOL

Blockchain bouwstenen

Waar is dit relevant voor een drugshandel supply chain?

Blockchain is in de basis een..

versleutelde overeengekomen gelinkte gedistribueerde database.



*** deze bouwstenen kun je gelang je behoefte gebruiken en veranderen**
*** open Source en makkelijk te kopiëren**
*** (pseudo) anonieme transacties**
*** public permissionless vs privaat permissioned**

SAXION HOGESCHOOL

Blockchain bouwstenen

- Wat als concurrenten nu gaan samenwerken in een DAO?
- Wat als participatie in die DAO als financier openstaat voor iedereen?
- Wat als de leverancier details van een keurmeester toevoegt?
- Wat als de rapportage van de levering door een 3e partij plaatsvindt of automatisch verloopt?
- Wat als je automatisch betaald of een schuld logt in een schaduwboekhouding?

SAXION HOGESCHOOL

Blockchain Bouwstenen 2.0.
Extra bouwstenen bovenop de basis

- Smart contracts
- dApps
- Tokens om
  - Deelnemers te belonen
  - Toegang te krijgen tot het platform
  - Als betalingsmiddel of aandeel
  - Als onderliggend bezit
  - Smart tokens & fractionalisering
- DAO - autonome organisatievorm zoals BitShares
- Self Sovereign Identity of digitale identiteit

Blockchain bouwstenen

Neem 10 minuten om te bedenken welke bouwstenen je minimaal nodig denkt te hebben

en hoe je deze invult

SAXION HOGESCHOOL

Dag 2 Casus

agenda

- Business process
- Wat zijn de relevante externe ontwikkelingen
- Welke blockchain bouwstenen staan tot je beschikking
- Welk **impact** heeft het invoeren van blockchain

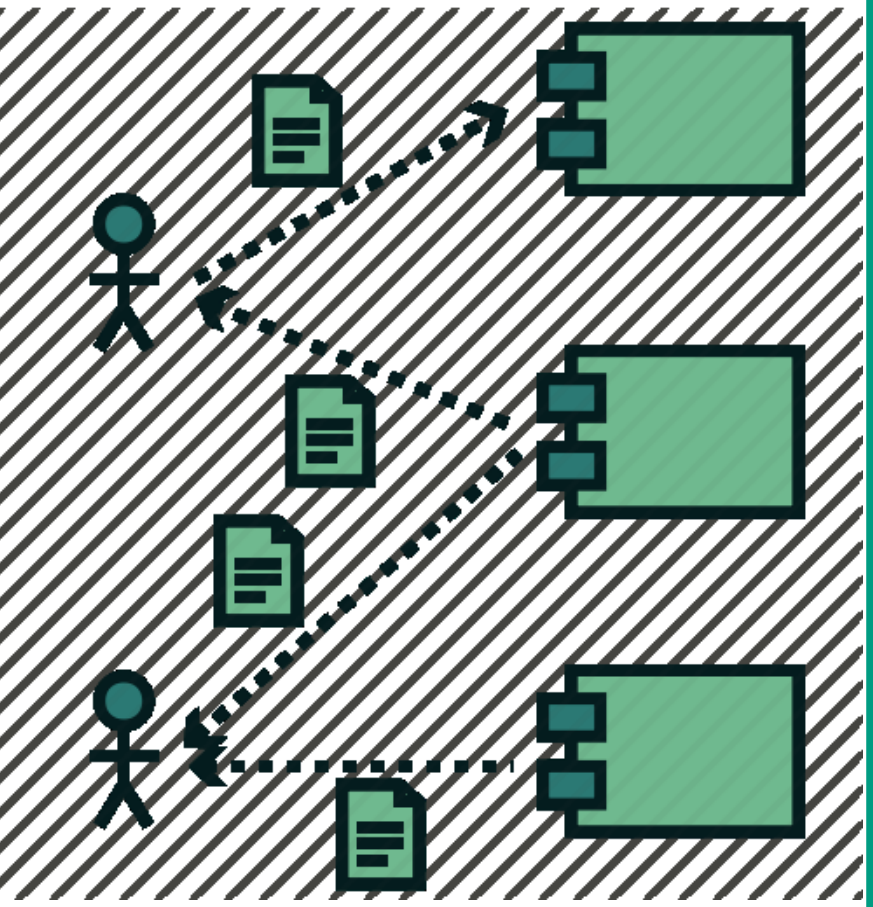
SAXION HOGESCHOOL

Blockchain impact

Neem 10 minuten om de impact te bediscussiëren

Omzet vermeerdering	opsplitsen markt, beter product met hogere marge.
Operationele efficiëntie	Tijdsreductie
Werkkapitaal	Tijdsbesparing leidt tot minder geld dat wordt vastgehouden in systeem..
Data kwaliteit	Verificatie van juiste data, weigering verifiëren onjuiste data, zekerheid van volledige data.
Risico vermindering	Één versie van het contract met eenduidige karakteristieken. Minder frauduleuze data.
Data integriteit	Transparantie in waardeketen en bezittingen.
Data beschikbaarheid	Inzicht in volledige keten t.o.v. eerder systeem.
Identiteitsmanagement	
Sterkere governance	Wellicht via DAO en smart contracts, open source software
Cryptocurrency voor betalingen	Mogelijkheid
Netwerk effect	Samenwerking binnen keten, betere en transparante afstemming
Gebruiksvriendelijkheid	
Valuta management	
Digitaal bezit	Digitaal product waar je automatische betaling aan kunt hangen.
Wettelijke compliance	
Veiligheid	Wellicht op publiek netwerk, anders privaat netwerk op eigen nodes draaien (PoS?)
Experimenteren met technologie	Verkregen kennis wordt gebruikt voor opschaling van diensten en ecosysteem inclusief internationale partijen.

SAXION HOGESCHOOL



Use case criteria

- Elke stap is **beargumenteerd**
- Het is **praktisch** uitvoerbaar.
- Er is een **implementatie** proces; hoe ga ik van het huidige system over naar een nieuw systeem of hoe kom ik tot een nieuw systeem
- Het gaat om het logisch kunnen beredeneren van blockchain, niet om het technisch bouwen.

SAXION HOGESCHOOL

AGENDA DAG 2 – 13 November

Diepere achtergrond, gevolgen Blockchain, praktische cybercrime voorbeelde

09.00 Recap dag 1
09.30 De praktijk met tools door Eljo Haspels CEO Cointell.
11.30 Verdieping blockchain en bouwstenen.

12.30 Lunch

13.15 Verdieping Blockchain en bouwstenen.
14.15 Consensusprotocollen en public, private, consortium.
15.45 Serey. Waar moet je aan denken als je een blockchain project opzet?
15.30 De casus
16.50 **Reflectie**
17.00 Afsluiting

SAXION HOGESCHOOL




Reflectie.

AGENDA DAG 3 – 3 December

09.00 Recap dag 1 & 2

09.15 Blockchain 2.0, het maken van een crypto token, Ethereum contracten en Coin Offerings.

10.15 Aan de slag met (de)centralized exchanges.
11.15 Interdisciplinaire samenwerking binnen politie m.b.t blockchain - Remco Spithoven / lector Maatschappelijke Veiligheid

12.45 Lunch

13.15 Aanvallen op blockchain en hoe je je kunt weren.
Self Sovereign Identity: over voor/nadelen van ingrepen overheid, KYC/AML, DigID als voorbeelden noemen
Hoe werken Bitcoin transacties en Block explorers.
Manieren om transacties te anonimiseren.

15.30 Casus
16.50 Reflectie
17.00 Afsluiting.

SAXION HOGESCHOOL



Dr. ing. Jan Veuger MRE FRICS

Professor Blockchain | Leading professor Saxion Institute for Blockchain

Saxion University of Applied Sciences

Schools of Finance & Accouting, Creative Technology and School of Governance, Law and Urban Development

Secretariaat: Ingrid Sinnema | T: 088-0196771 | i.k.sinnema@saxion.nl |

P.O. Box 70.000 | 7500 KB ENSCHEDE | Visiting adress: M.H. Tromplaan 28, Enschede | Handelskade 75, Deventer | The Netherlands |

M 06 22 99 53 12 | j.veuger@saxion.nl | www.saxion.nl |

