Prelude

Smals
ICT for society

Blockchain
Meer dan een hype

Frank Robben

frank.robben@ksz.fgov.be

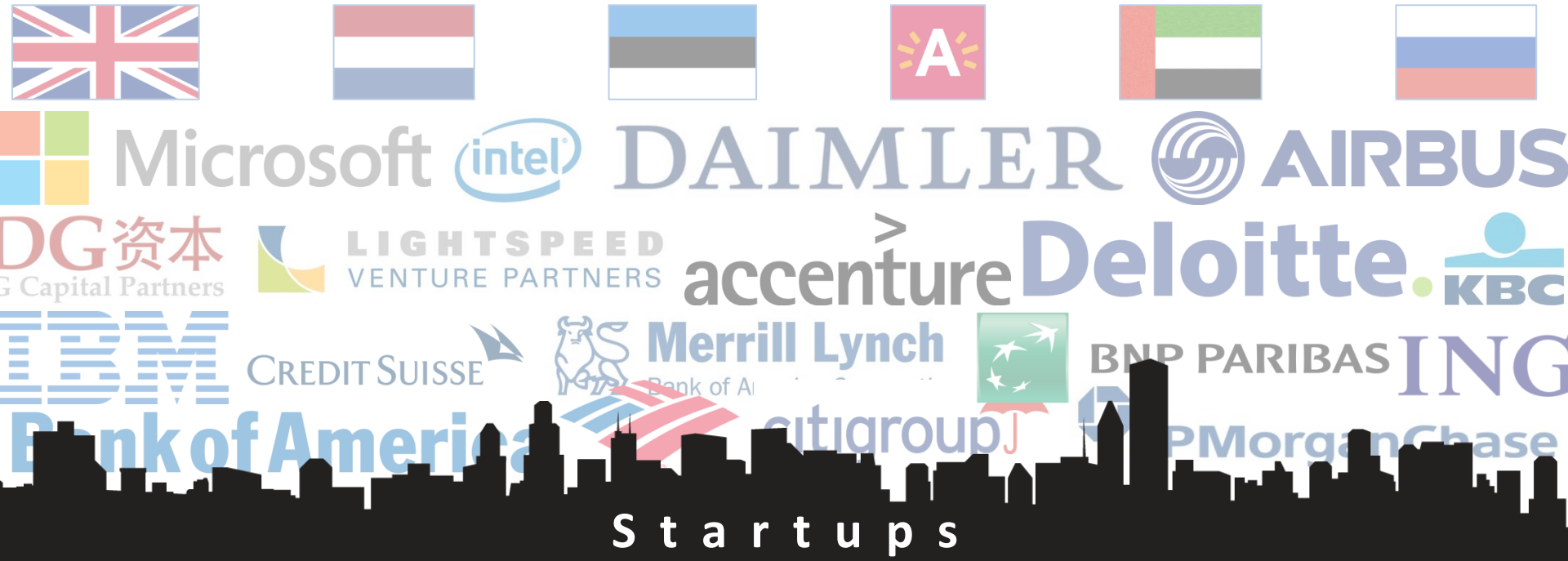
@FrRobben

https://www.ksz.fgov.be
https://www.ehealth.fgov.be
https://www.frankrobben.be

Blockchain Investeringen

Totaal 2016: **$ 2,5 miljard**

Verwachte groei tot 2022: **35% per jaar**



Gedistribueerd vertrouwen

Stelling uit de cryptografie
Alles wat gedaan kan worden met een vertrouwde autoriteit kan ook gedaan worden zonder

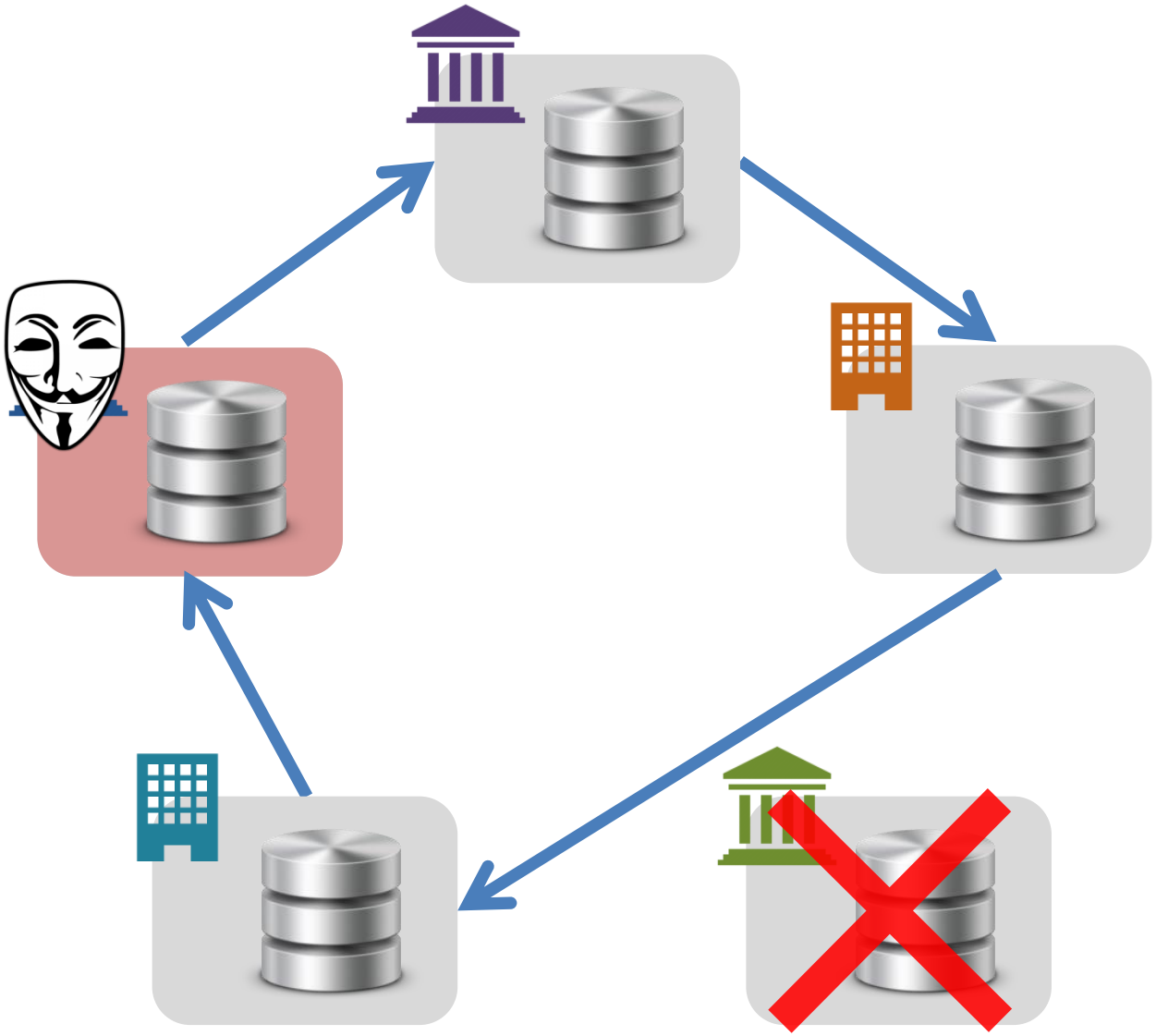
Dan Boneh,
Professor Stanford University
Crypto expert

Wel overhead wat betreft rekenkracht, opslag en communicatie

Blockchain niet enige technologie voor gedistribueerd vertrouwen

→ Blockchain trigger voor algemenere vraag:
Efficiëntere overheid d.m.v. gedistribueerd vertrouwen?

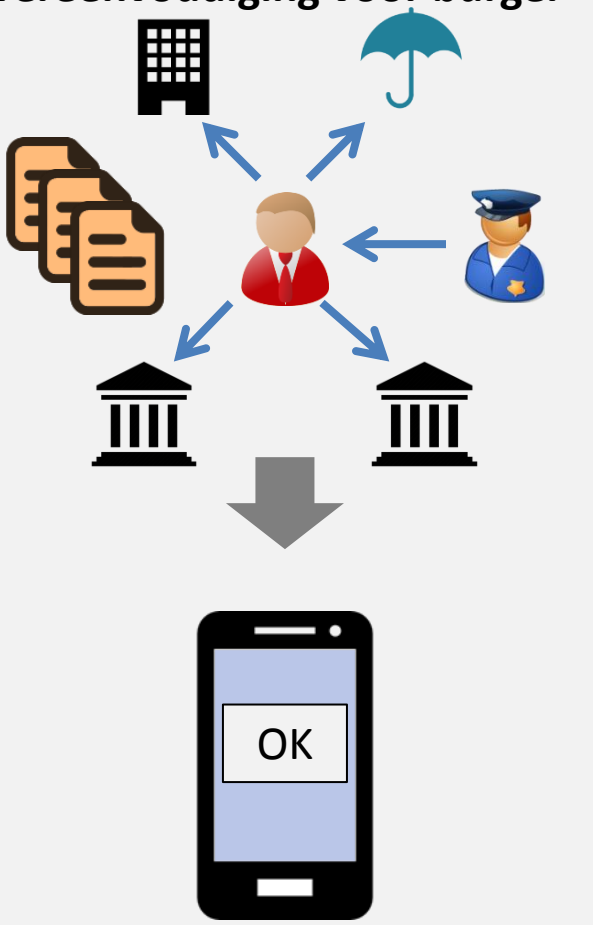
Concept



- Gedistribueerd
- Append-only
- Robuust
- Schaalbaar

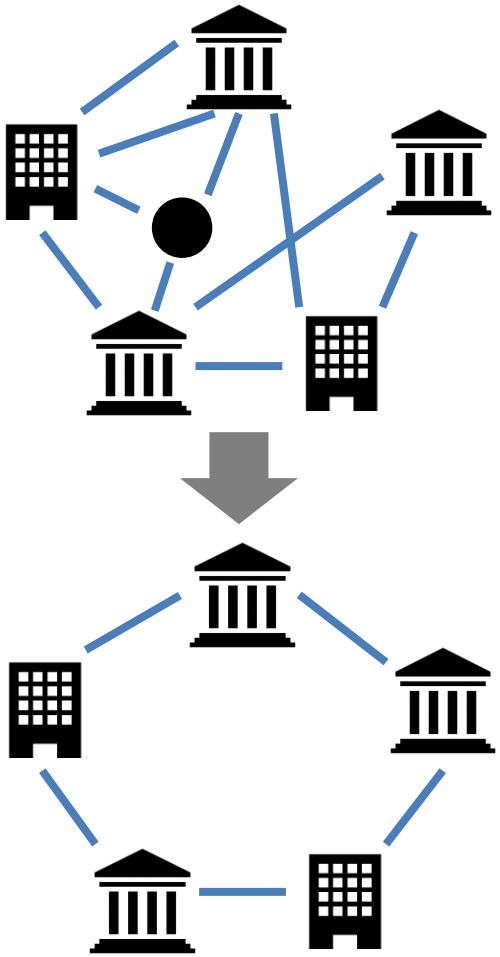
Beter bestuur

Vereenvoudiging voor burger



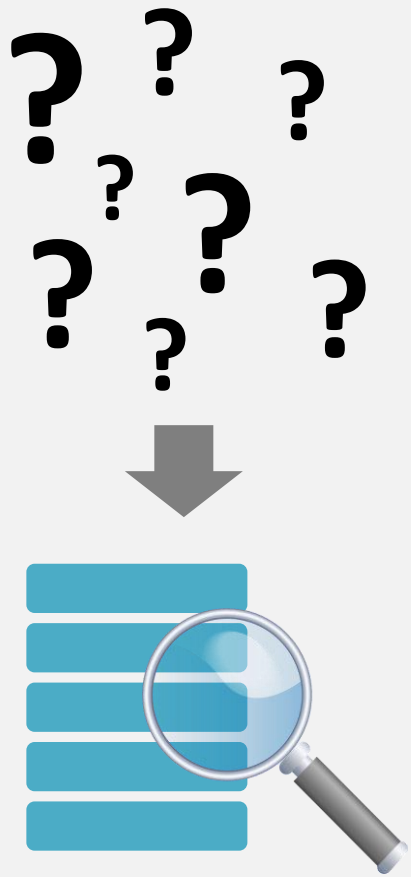
Levensloop

Gestroomlijnde processen



Schuldafhandeling

Transparantie



Voedselveiligheid

Blockchain veelbelovende technologie

Blockchain & overheid

Silo 2.0
Gevaar data verspreid in diverse geïsoleerde blockchains

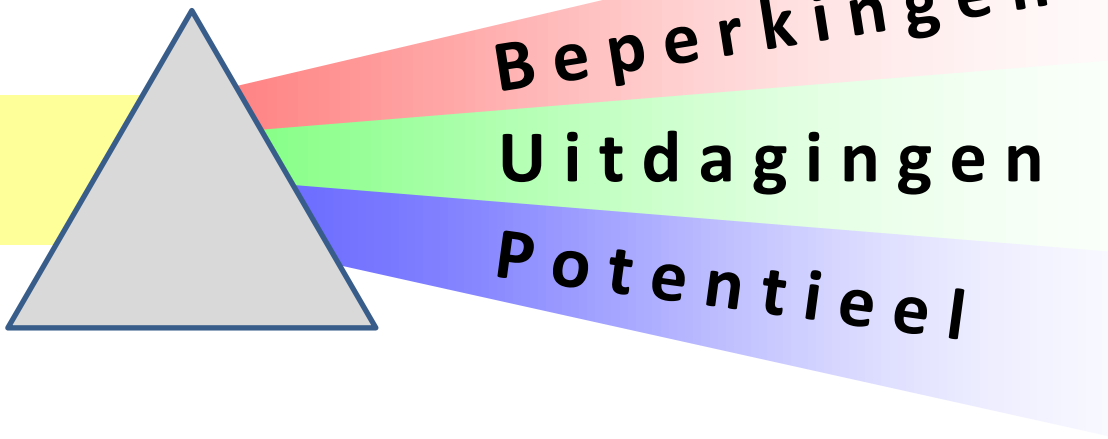
Gecoördineerde aanpak noodzakelijk om te komen tot blockchain ecosystemen over instellingen heen

Gemeenschappelijk platform

Gemeenschappelijke visie

Doelstelling sessie

HYPE

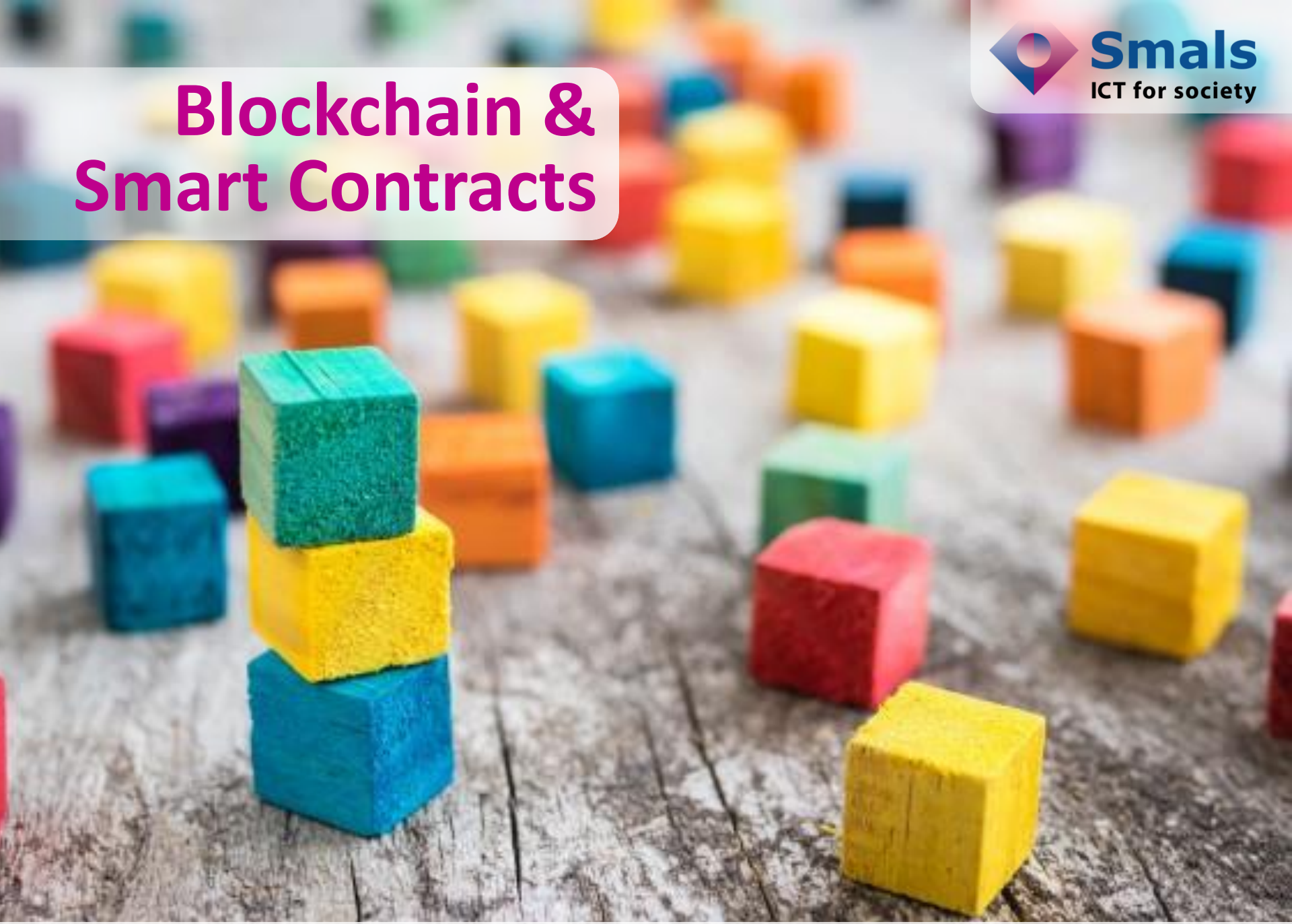


Opportuniteiten

Risico's

A.d.h.v. **achterliggende principes**
en **mogelijke toepassingen**

Blockchain & Smart Contracts



Smals
ICT for society

Kristof Verslype, Smals Research

Agenda

Smals
ICT for society

Blockchain 1.0

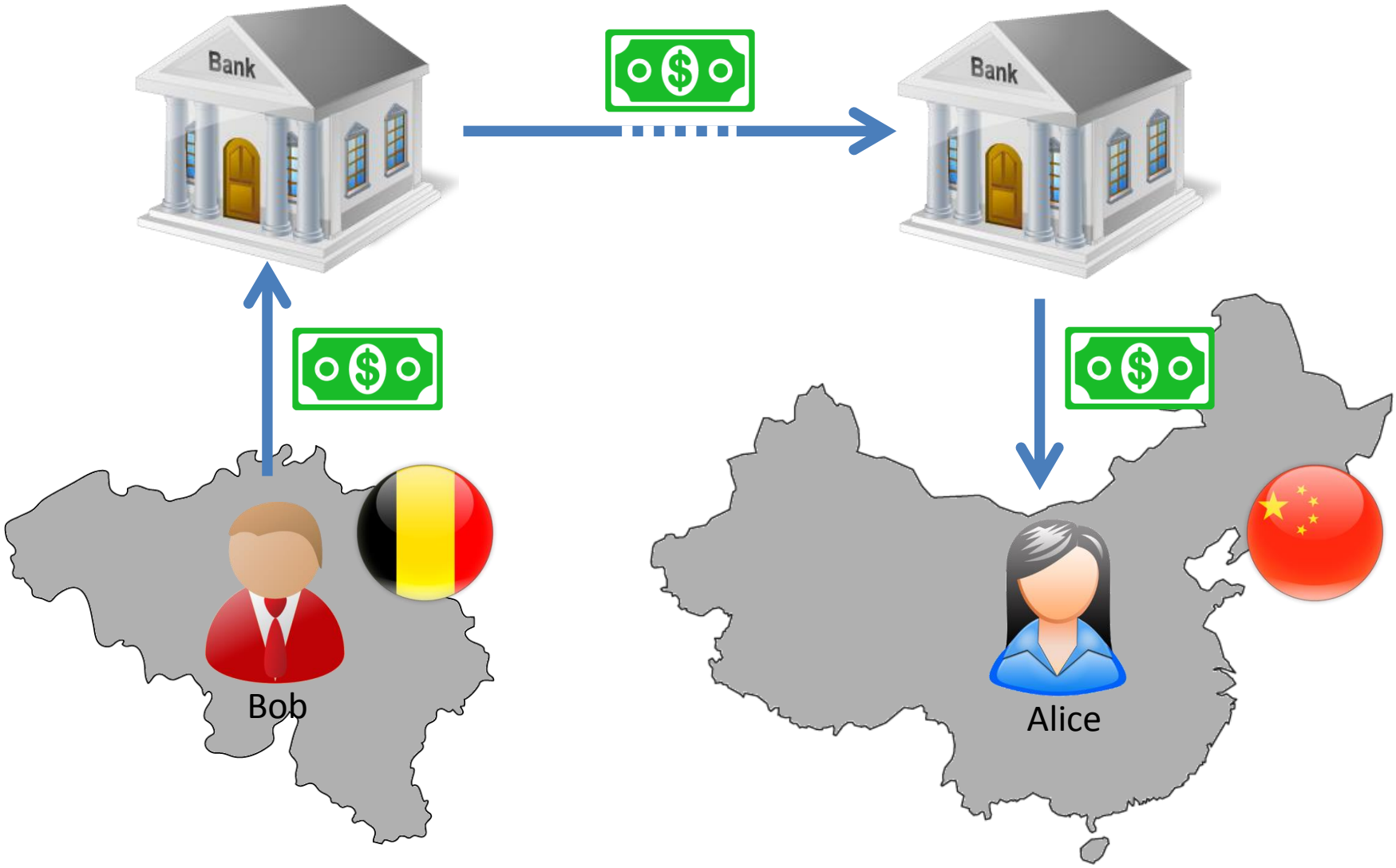
Pauze

Blockchain 2.0

Bitcoin Blockchain

Smals
ICT for society

Traditionele Internationale Transactie



Traditionele Internationale Transactie

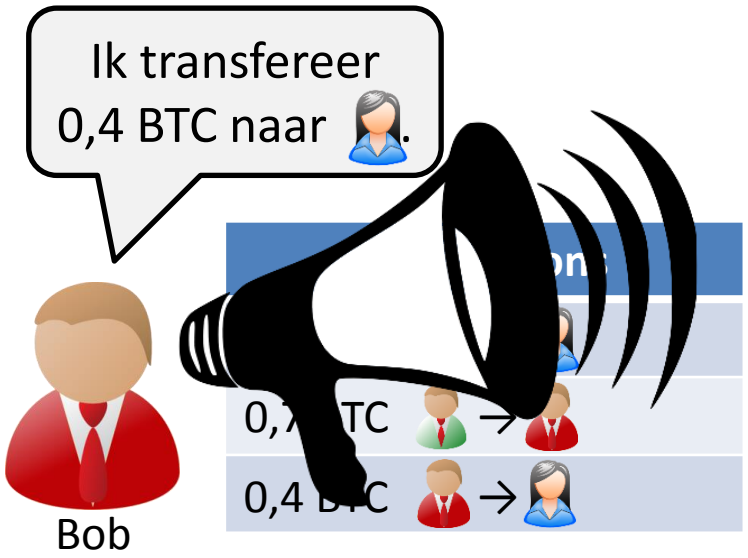
Kan dit zonder vertrouwde partijen?

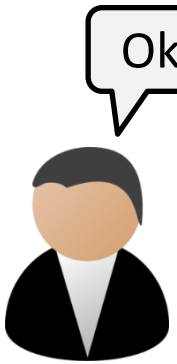
1e **gedistribueerde** cryptomunt (2009)

Schok doorheen de financiële wereld

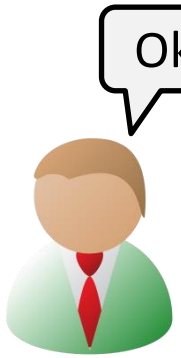
Financiële wereld veel aandacht voor Bitcoin/Blockchain

Idee



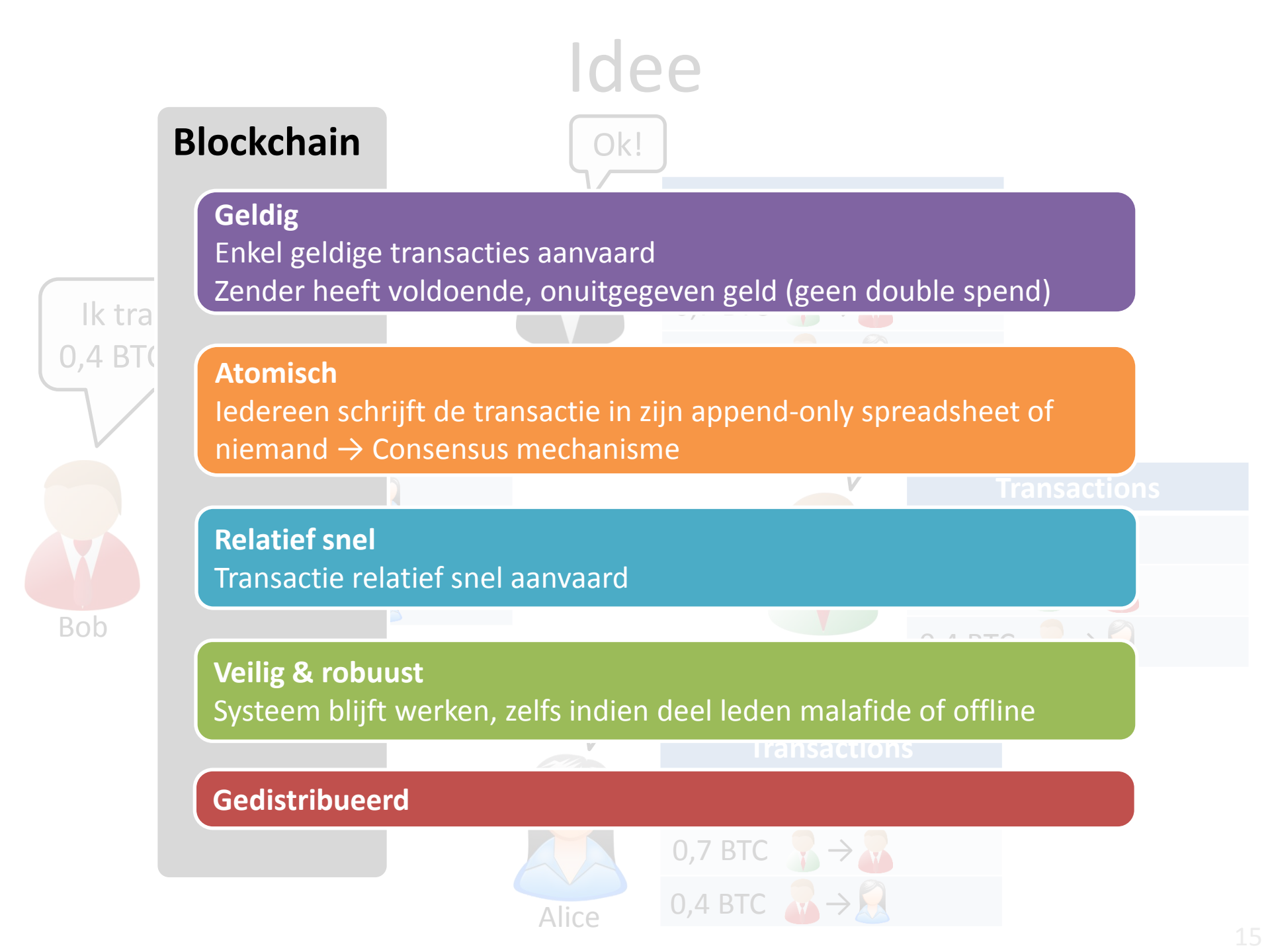


Transactions
5,1 BTC →
0,7 BTC →
0,4 BTC →



Transactions
5,1 BTC →
0,7 BTC →
0,4 BTC →

Transactions
5,1 BTC →
0,7 BTC →
0,4 BTC →



Blockchain

Geldig
Enkel geldige transacties aanvaard
Zender heeft voldoende, onuitgegeven geld (geen double spend)

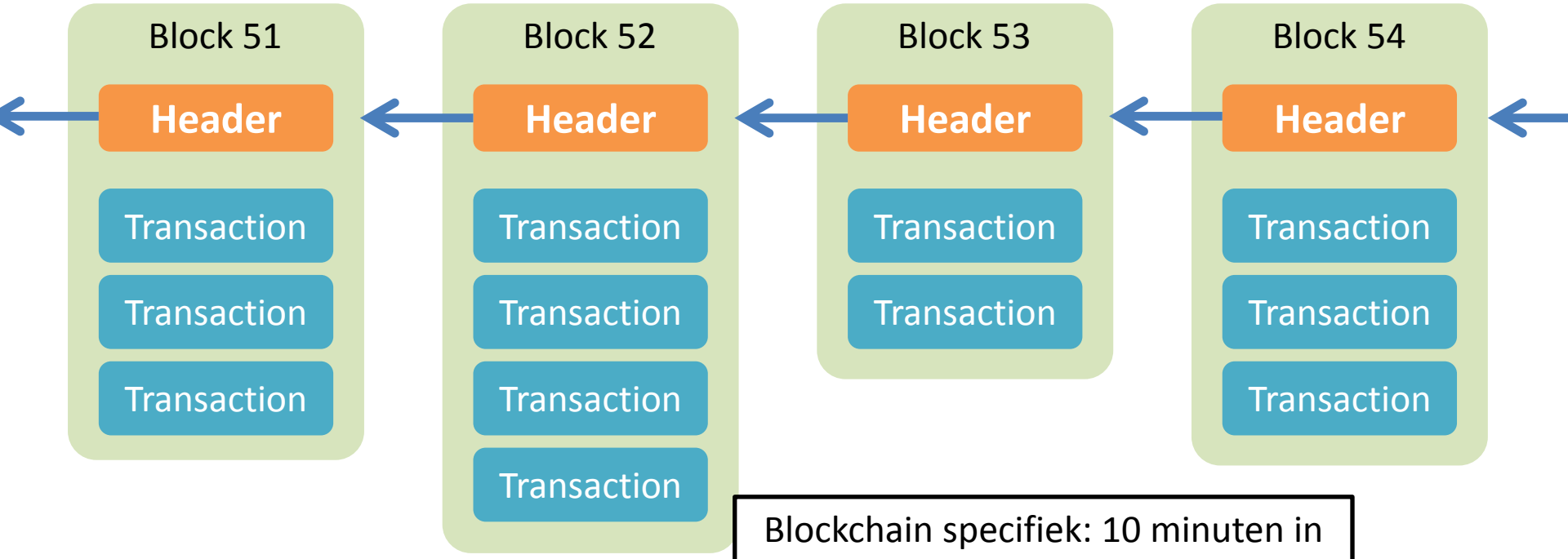
Atomisch
Iedereen schrijft de transactie in zijn append-only spreadsheet of niemand → Consensus mechanisme

Relatief snel
Transactie relatief snel aanvaard

Veilig & robuust
Systeem blijft werken, zelfs indien deel leden malafide of offline

Gedistribueerd

Blockchain



Blockchain specifiek: 10 minuten in Bitcoin, 10 seconden in Ethereum,…

Blockchain = aaneenschakeling van blokken die transacties bevatten

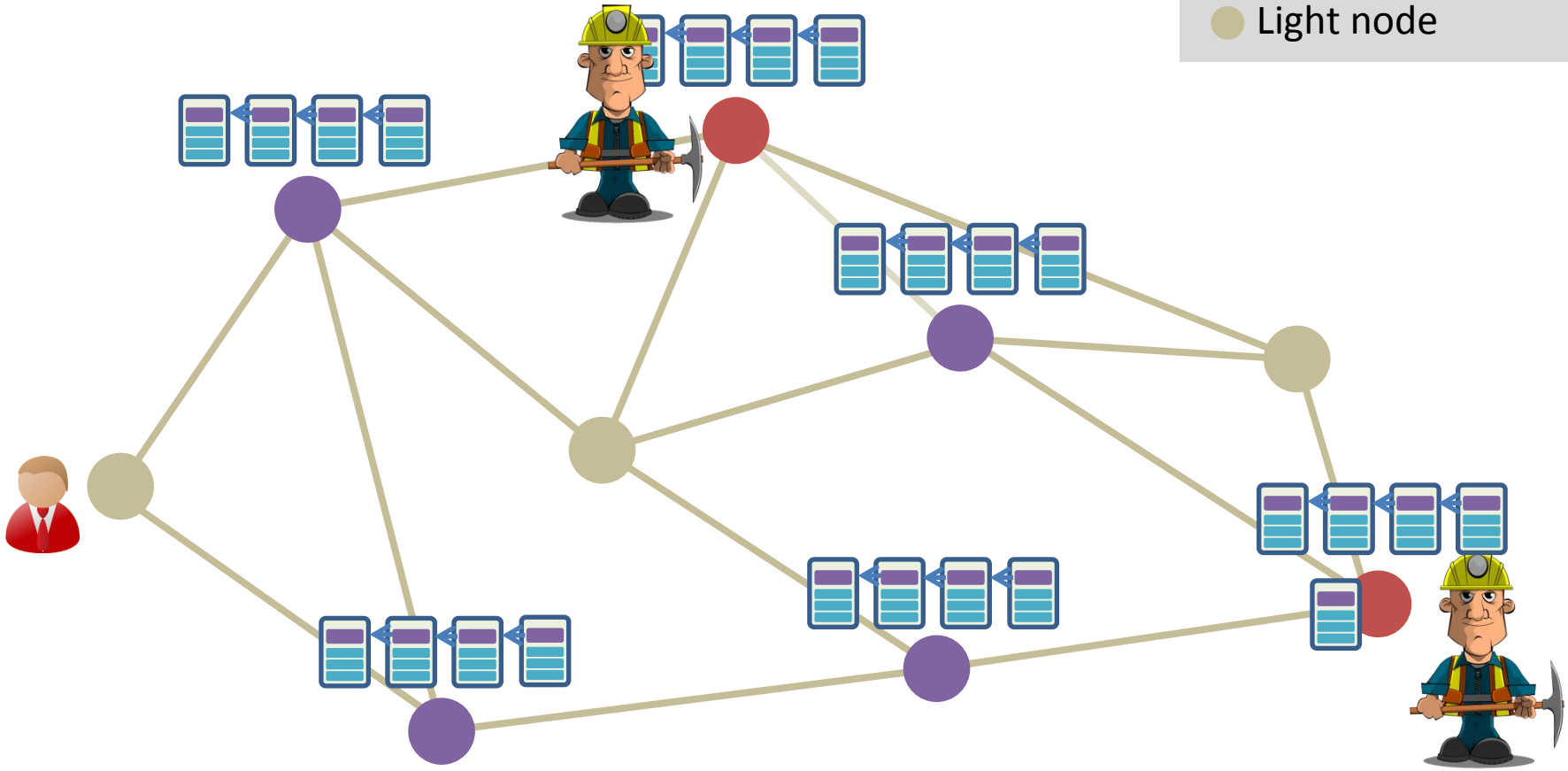
Elke 10 minuten (Bitcoin) nieuw blok met meest recente transacties achteraan toegevoegd

blockchain bevat ALLE transacties

Transactie in blockchain quasi onmogelijk te verwijderen

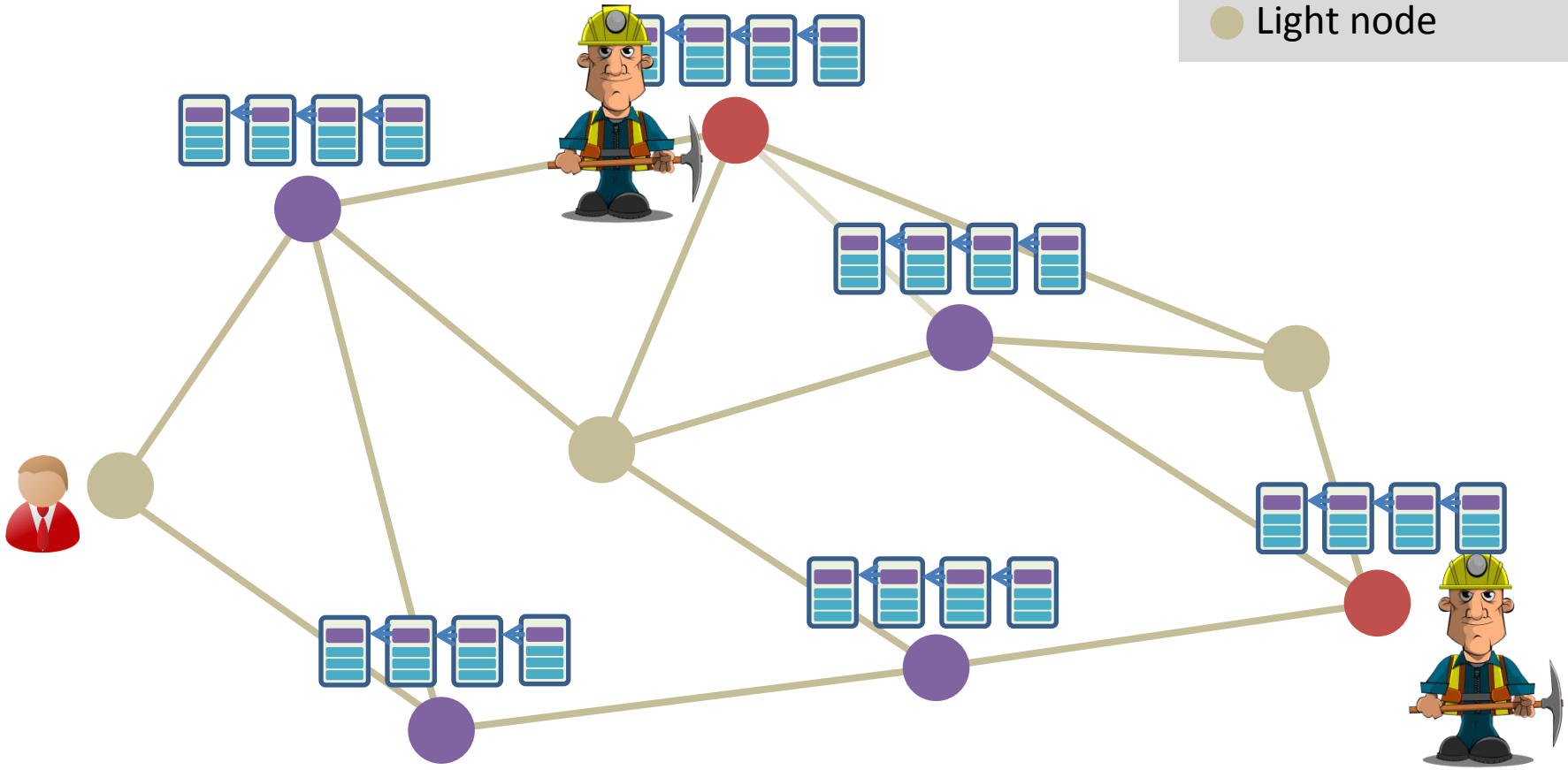
Vele entiteiten beschikken over dezelfde versie van de blockchain

Netwerk & Consensus



1. Node creëert transactie en stuurt het naar zijn buren.
2. Validating nodes verifiëren geldigheid transactie en forwarden het
3. Miners voegen de transactie toe aan het volgende blok dat ze trachten te creëren
4. De creatie blok vereist oplossen rekenintensieve, onvoorspelbare puzzel
5. Winnende miner verspreid nieuw blok in netwerk en ontvangt beloning (Bitcoins)
6. Validating nodes valideren blok en voegen het toe aan lokale blockchain kopie

Netwerk & Consensus



Consensusmechanisme

- Iedereen met identieke kopie van blockchain zal hetzelfde, nieuwe blok toevoegen aan die kopie
- Mechanisme voor omgaan met situatie waarbij twee miners ongeveer gelijktijdig blok creëren

bitcoin - Mining

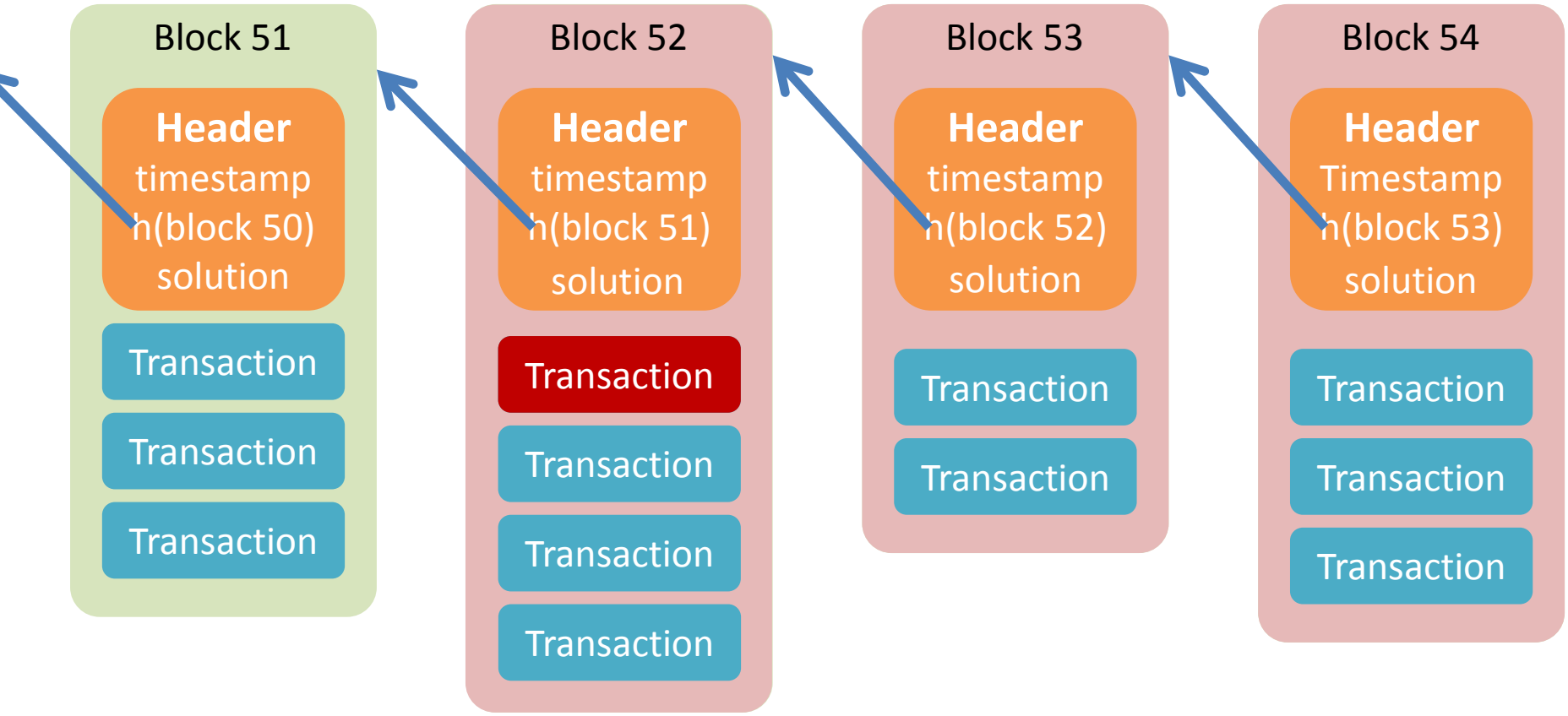
- Vereist enkel hashing (SHA256)
- Specifieke hardware (ASICs - application specific integrated circuit)
- 100.000x efficiënter dan standaard computer
- Grote datacenters (“60-70% in China”)

Eén Bitcoin transactie verbruikt naar schatting evenveel elektriciteit als **14 382 VISA transacties**.
Bron: http://digiconomist.net/beci

Bitcoin is niet volledig gedistribueerd

Bitcoin is erg vervuilend

Veiligheid



Pas indien nieuwe blockchain langer dan originele -> aanvaard

=> Hoe ouder de transactie, hoe beter beschermd

Pseudoniemen

Fysieke wereld

Bitcoin netwerk

Bob

1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX

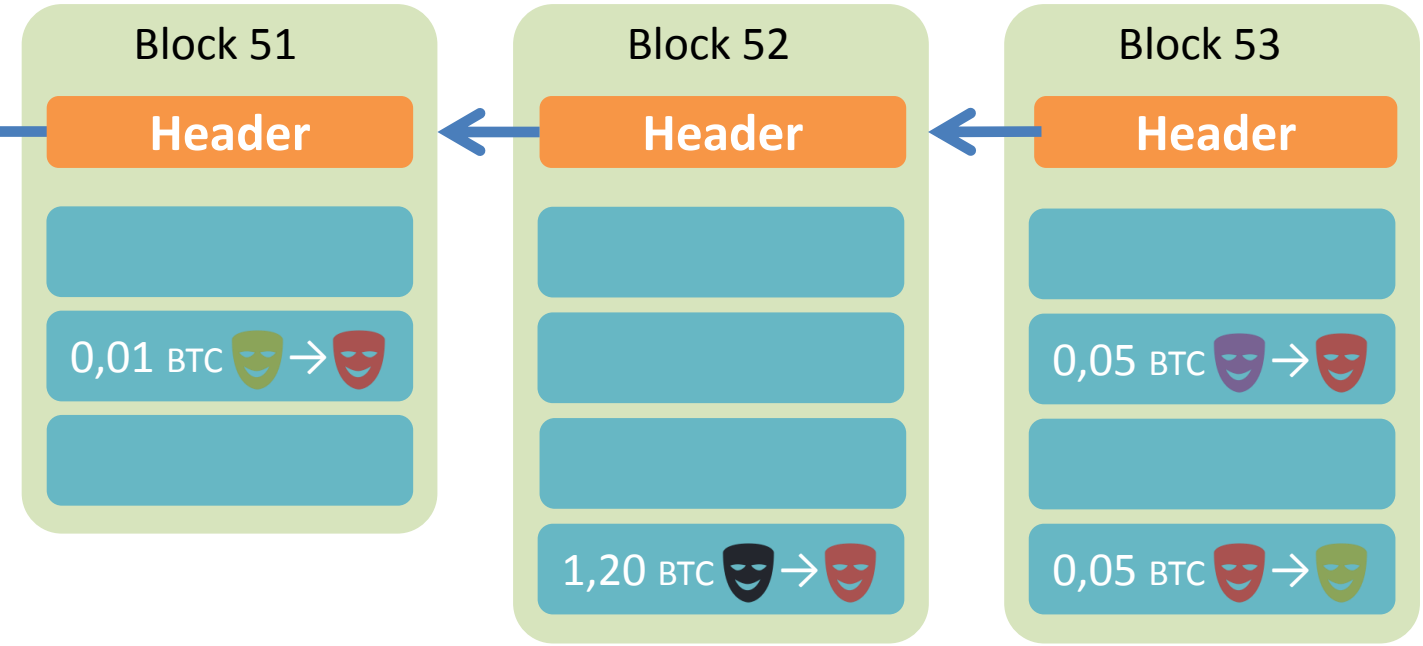
Alice

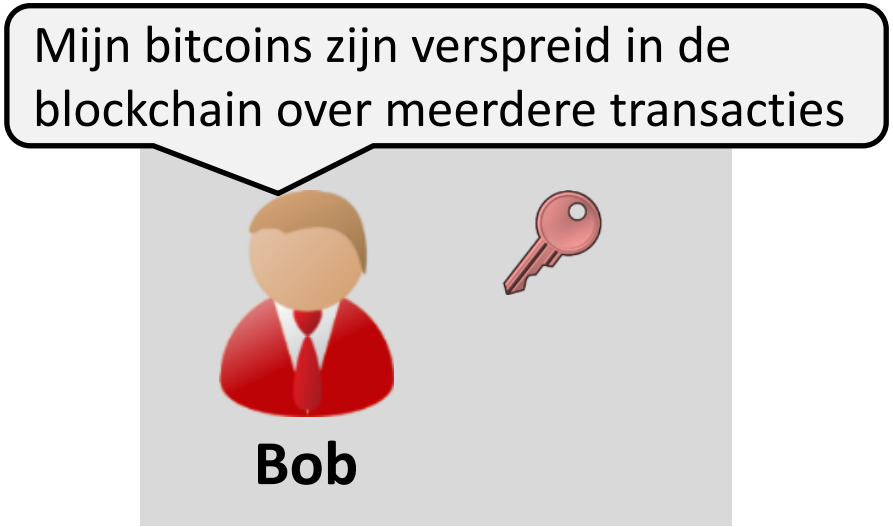
3BcMuv1VJqmwY5Wim8MPAzKAAiAKby9LcN

Charlie

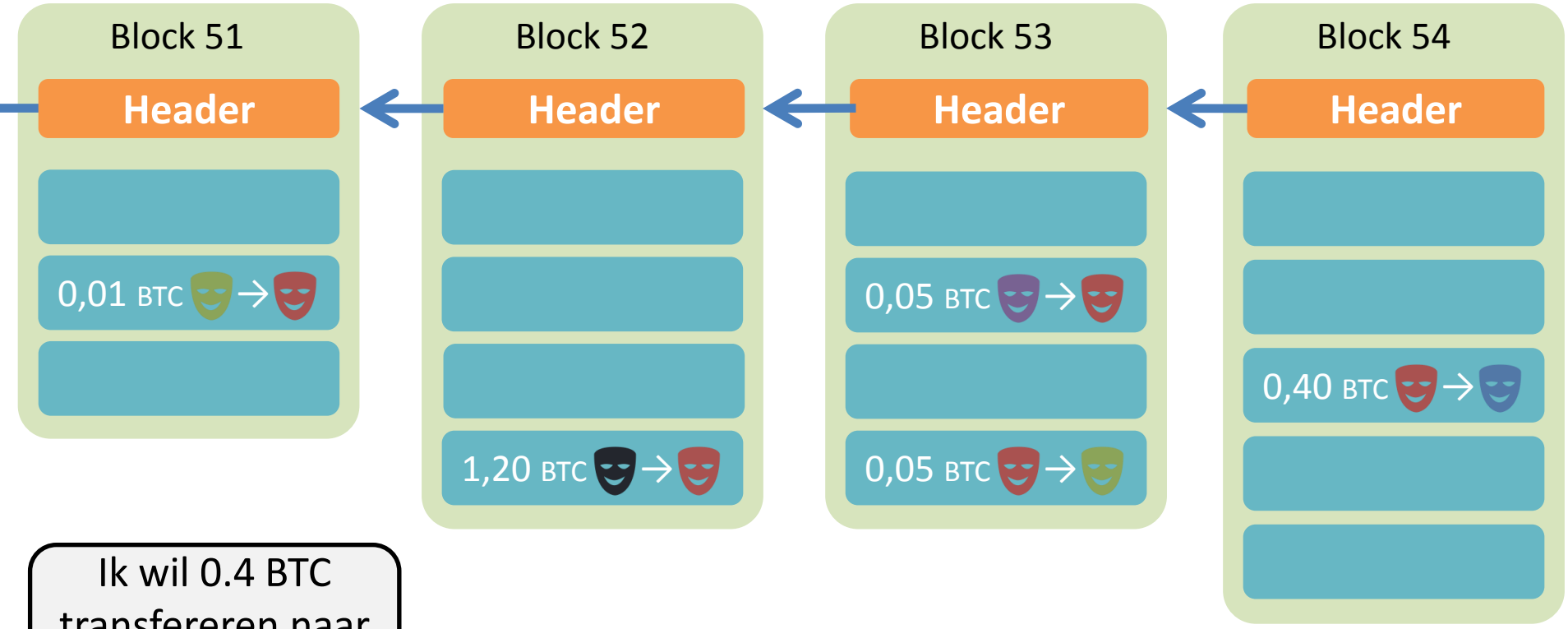
1Nf311Qb8rLDkWTHrhpmNewZzkcWFYptfc

Transacties (Vereenvoudigd)





Transacties (Vereenvoudigd)



Full nodes verifiëren op efficiënte manier of Bob wel over het nodige geld beschikt.

Pseudoniemen

Fysieke wereld

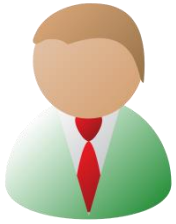
Bitcoin netwerk

Bob

1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX

Alice

3BcMuv1VJqmwY5Wim8MPAzKAAiAKby9LcN



Charlie

1Nf311Qb8rLDkWTHrhpmNewZzkcWFYptfc

Bitcoin & Anonimiteit

QR-code
- bevat pseudoniem
- Scan om te betalen

Alle transacties van en naar dit pseudoniem zijn publiek

Tweerichtings
Subway kan ook jouw bitcoin geschiedenis te weten komen

Bitcoin & Anonimiteit

Gebruikers onthullen hun pseudoniem

- Op het Internet
- Aan anderen bij een transactie

→ Linken aan persoon / nickname

Fleder, Michael, Michael S. Kester, and Sudeep Pillai. "Bitcoin transaction graph analysis." *arXiv preprint arXiv:1502.01657* (2015).

One-Time Pseudoniemen

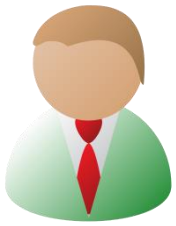
Betere privacy

Fysieke wereld

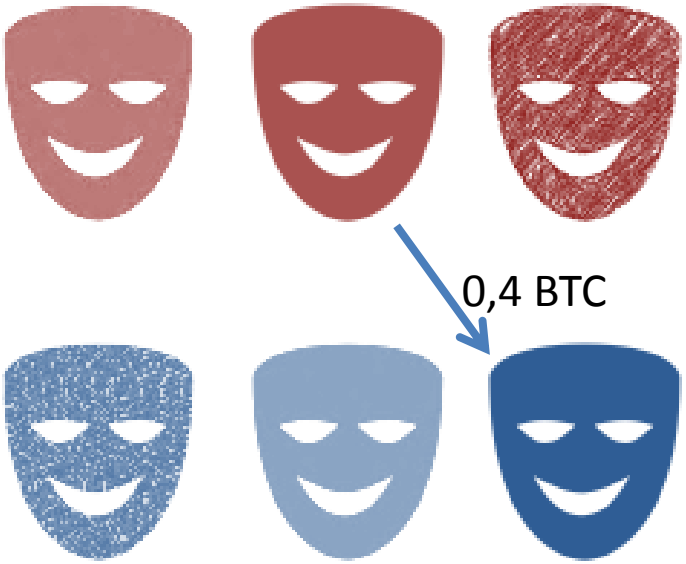
Bitcoin netwerk

Bob

Alice



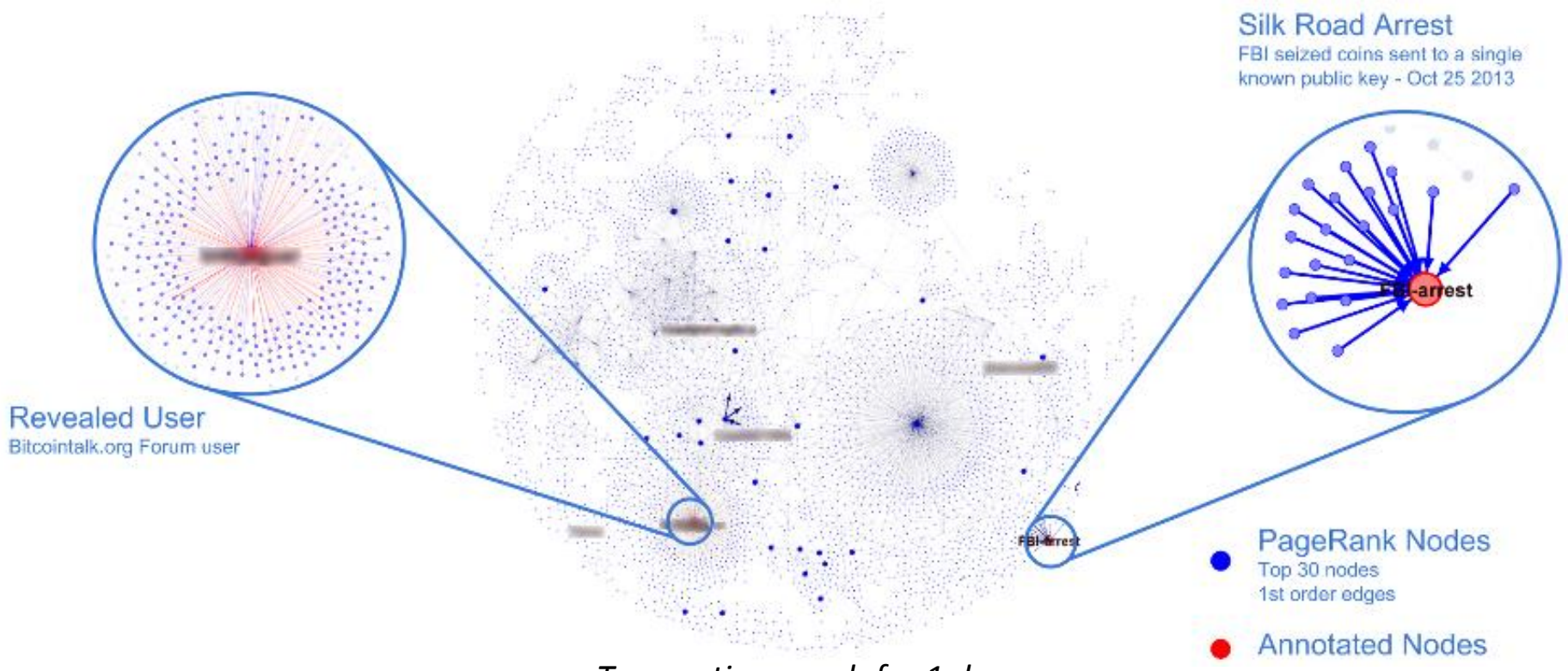
Charlie



0,4 BTC

Transaction
0,4 BTC →

Bitcoin Anonimiteit



Transaction graph for 1 day

'Geïdentificeerde' personen gelinkt aan
- Silk Road
- Wikileaks
- SatoshiDICE

Bitcoin beschermt slecht uw privacy

Fleder, Michael, Michael S. Kester, and Sudeep Pillai. MIT. "Bitcoin transaction graph analysis." *arXiv preprint arXiv:1502.01657* (2015).

Blockchain.info

Height	Time	Relayed By	Hash	Size (kB)
454964 (Main Chain)	2017-02-27 09:21:15	GoGreenLight	00000000000000000b20ef49806f854445f06a7708e78f30d3ffa01da9	927.97
454963 (Main Chain)	2017-02-27 09:09:25	BW.COM	00000000000000001e8c35fc00282e12b0a248c1957407e2cf4f2767fe	998.04
454962 (Main Chain)	2017-02-27 09:06:25	AntPool	00000000000000000178bf3ee6643f361ec341dc33ddd1959d0470e5c8	998.04
454961 (Main Chain)	2017-02-27 08:52:03	SlushPool	00000000000000000024a996b9be8a408fd8189029f5731300207ea92	966.64
454960 (Main Chain)	2017-02-27 08:50:45	AntPool	00000000000000000016e802c1c9e9d14b03fa463a52be714b0f714451	998.19
454959 (Main Chain)	2017-02-27 08:47:52	ViaBTC	00000000000000000bb1b9dcd6cee5d43e0b2b339d36aba4d8bc20a0	999.12
454958 (Main Chain)	2017-02-27 08:41:19	AntPool	00000000000000000a8c666c88a64d8207075e9234e1fac623feadcc2	998.19
454957 (Main Chain)	2017-02-27 08:39:27	Unknown	00000000000000000208d781c6c4d6d7a185aaa4dfebbc5c971388fb12	999.16
454956 (Main Chain)	2017-02-27 08:29:35	AntPool	00000000000000000bda8c59fc2d0e57a35f6728d4d7d730f164a7836	998.12
454955 (Main Chain)	2017-02-27 08:11:00	HaoBTC	00000000000000000c5dc465e585e2d6a14333e5a77b5758dcabb2c	0.2
454954 (Main Chain)	2017-02-27 08:10:57	AntPool	00000000000000001d0155f281523dd319b6a98a290723754abd5b91	998.21

Bitcoin zit aan maximumcapaciteit

Blockchain.info

Block #454961

Summary

Number Of Transactions	370
Output Total	2,802.2884713 BTC
Estimated Transaction Volume	365.84939391 BTC
Transaction Fees	0.28159014 BTC
Received Time	2017-02-27 08:52:03
Relayed By	SlushPool
Difficulty	440,779,902,286.59
Bits	402816659
Size	966.645 KB
Version	0x20000002
Block Reward	12.50 BTC

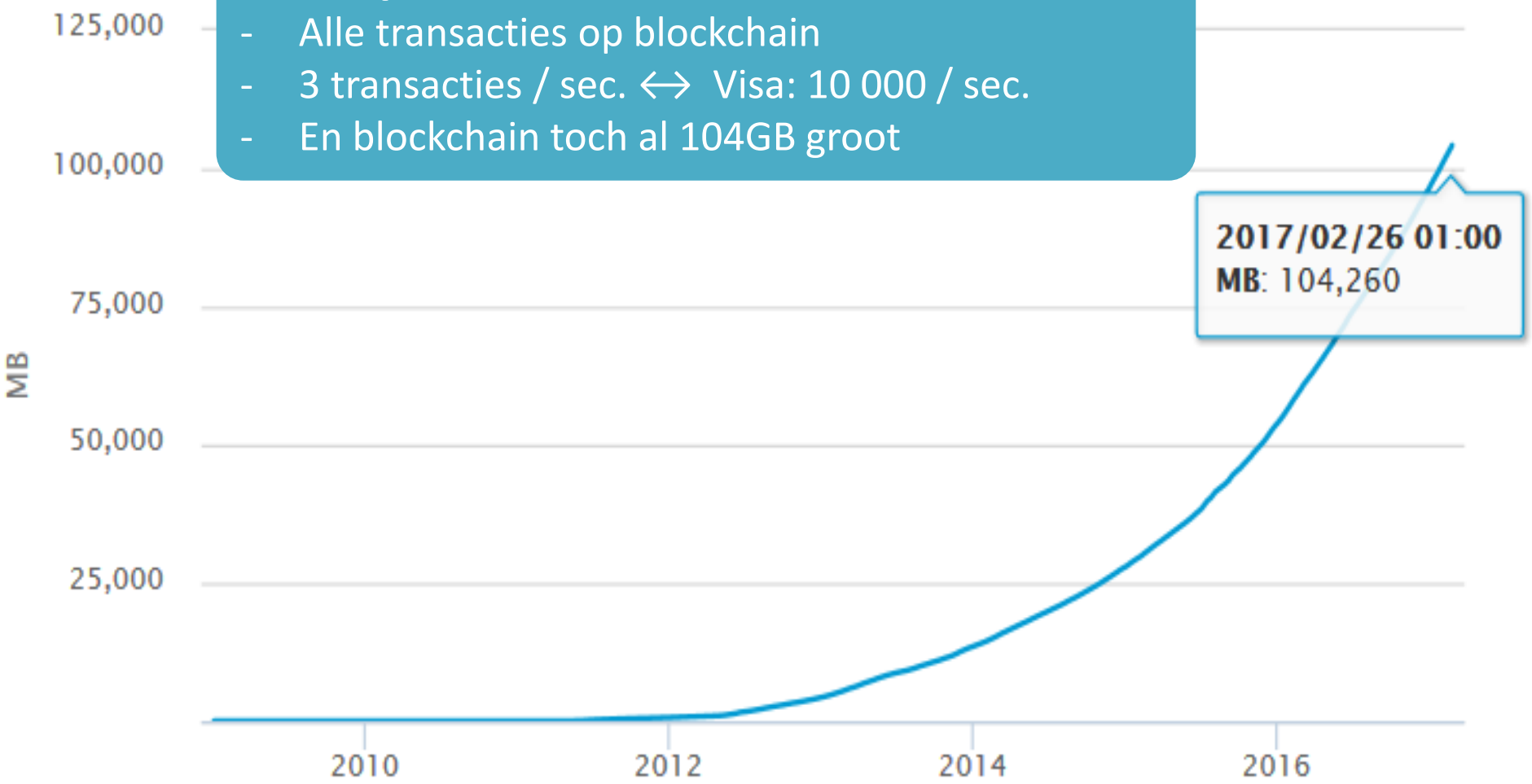
Hashes

Hash	00000000000000000024a996b9be8a408fd8189029f5731300207ea92cfcc372
Previous Block	00000000000000000016e802c1c9e9d14b03fa463a52be714b0f714451346bc66
	c0062a16ad514719b69addb3af290be4cc8b606335c73a128515c

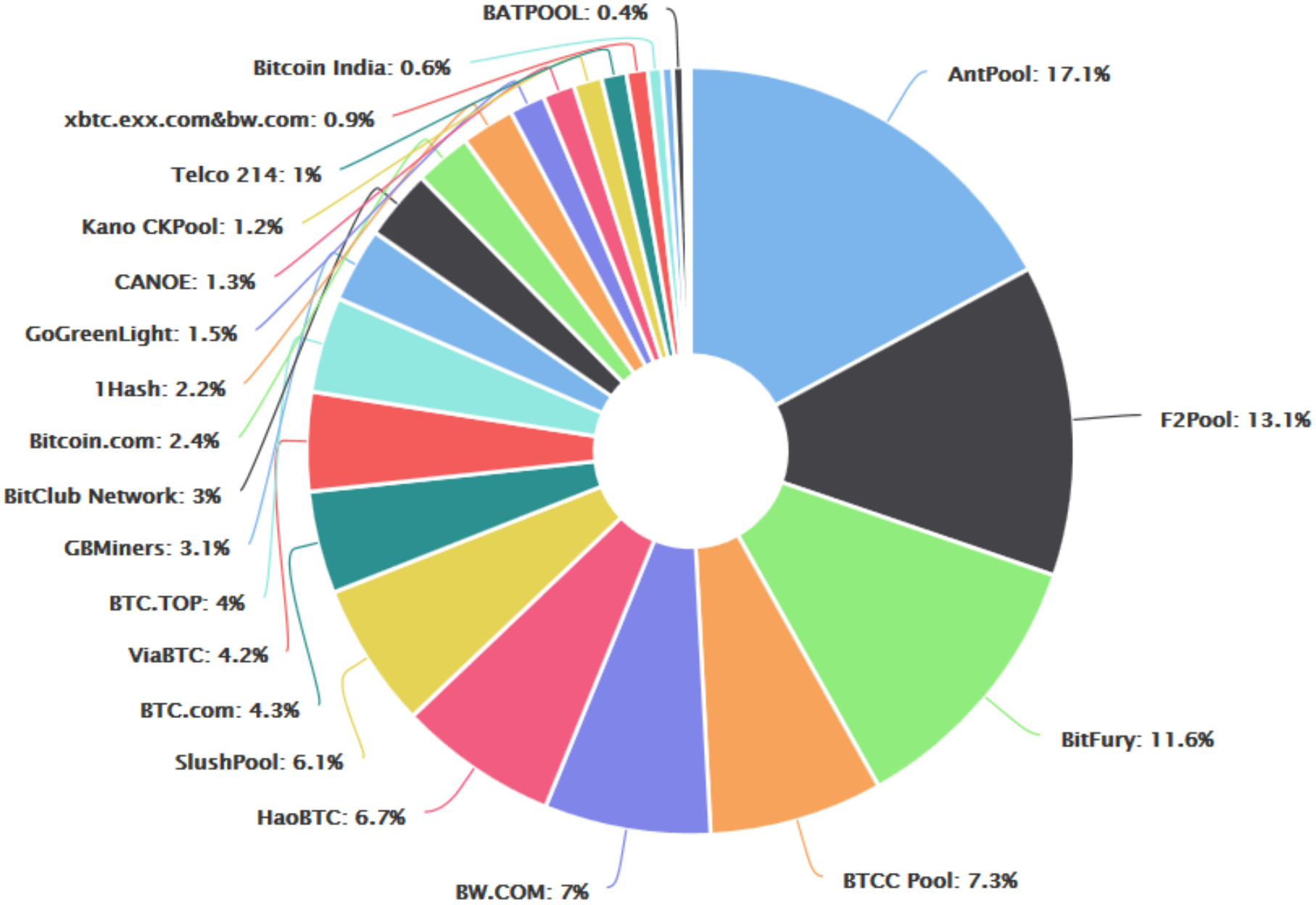
Network Propagation

Blockchain.info

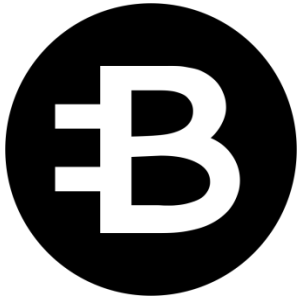
Schaalprobleem
- Alle transacties op blockchain
- 3 transacties / sec. ↔ Visa: 10 000 / sec.
- En blockchain toch al 104GB groot



Blockchain.info



Altcoins



Creëren van transacties op blockchain vereist een sleutel

Hardware Wallets

Sleutel fysiek beschermd in hardware


TREZOR
Confirm sending
0.0469 BTC
to
1Nuu2753n7h3ZnCQJ
CT2HVKTFfQjhpXhcw
Cancel
Confirm

Blockchain 1.0 Samengevat

Eigenschappen die elke blockchain bezit

Append-only
- Transacties niet verwijderbaar
- Bevat alle transacties (data)

Proces blokcreatie
- Bevat meest recente transacties
- Gemiddelde frequentie (vb. 10 min)

Consensus Mechanisme
- Full nodes hebben zelfde versie
- Gedistribueerd: Geen centrale partij

Robuust
- Wanneer deel deelnemers malafide
- Wanneer deel deelnemers offline

Gebruik
- Transactie vereist private sleutel
- Gebruikers gekend onder pseudoniemen

Eigenschappen die sommige blockchains bezitten

Inefficient / competitie

Gebruik cryptogeld

Open voor iedereen

Agenda

Smals
ICT for society

Blockchain 1.0

Pauze

Blockchain 2.0

Blockchain Toepassingen

Smals
ICT for society

Data in the Blockchain

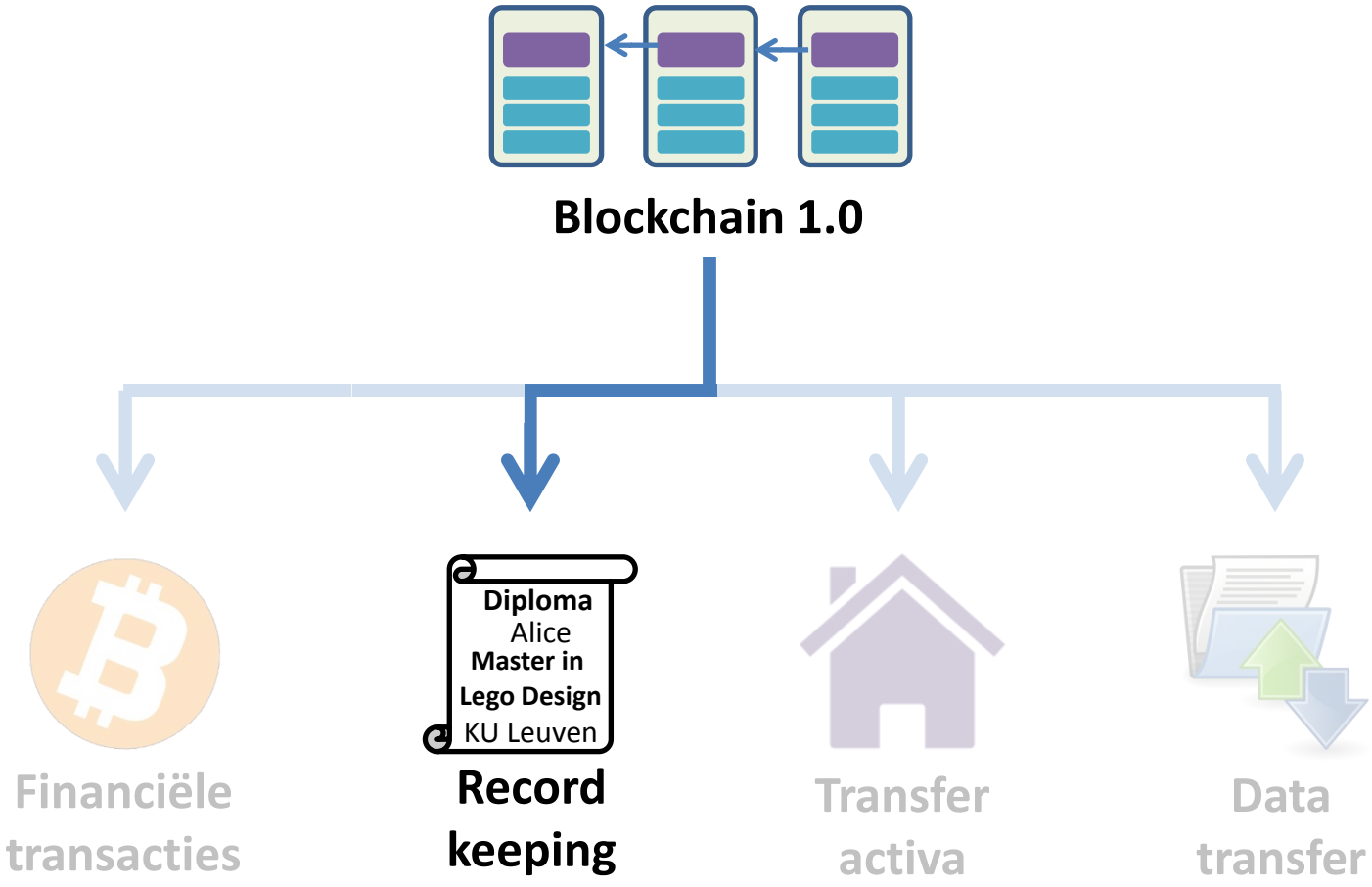
Eigenschappen data in blockchain

- **Onwijzigbaar (integriteit)**
- **Timestamped**
- **Onweerlegbaar / Verifieerbaar**

→ Applicaties die verschillen van cryptomunt.

- **Bitcoin Blockchain (Colored coins)**
- **Andere Blockchain**

Blockchain Toepassingen



Verminderd vertrouwen vereist in centrale / intermediaire partijen

Record Keeping

Eigenschappen, certificaten, rechten, …

Medische records

Rijbewijs

huwelijk (-scontract)

Diploma

Vaccinatie

Identiteits-gegevens

Belastingen

Supply chain Tracking

Zo weinig mogelijk data op blockchain → Vaak slechts fingerprint (hash)

Applicaties / PoCs

Registratie huwelijken, geboortes, …

BITNATION
GOVERNANCE 2.0

Identiteit

ShoCard

Digitale handtekeningen

guardtime

Diploma

ESILV
LÉONARD DE VINCI
ÉCOLE D'INGÉNIEURS
PARIS-LA DÉFENSE

Interne verkiezingen

Deense
LIBERAL
ALLIANCE

Diploma

HOLBERTON
school()

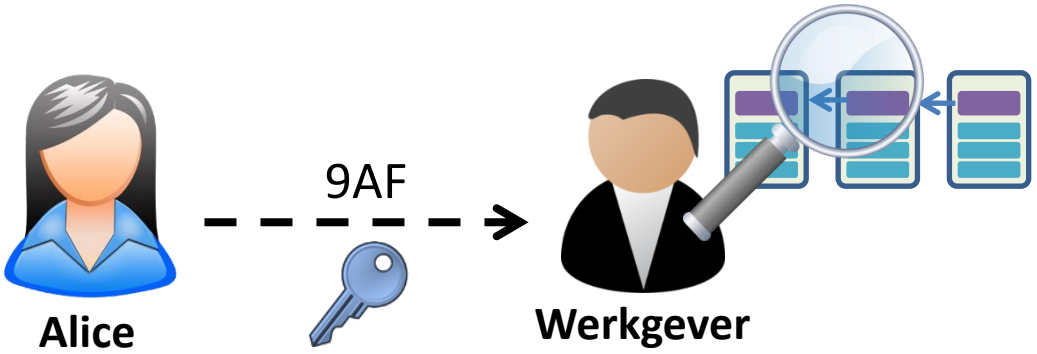
Integriteit & timestamping EHR

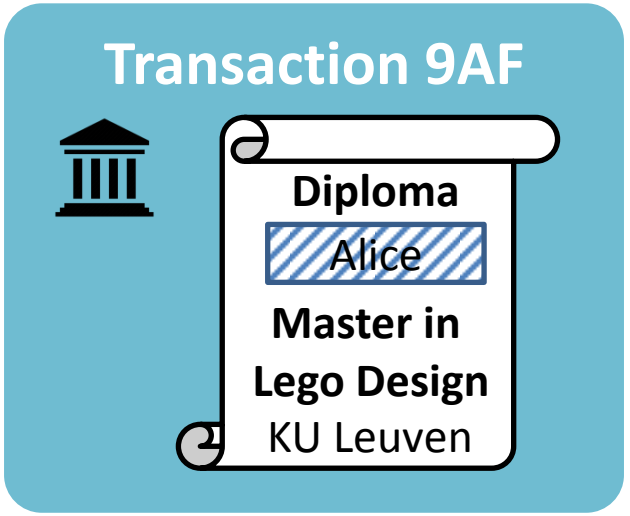
HealthNautica.com
+ factom

Uitgaven mensen met uitkering

Department for Work & Pensions

Record Keeping (Vereenvoudigd)





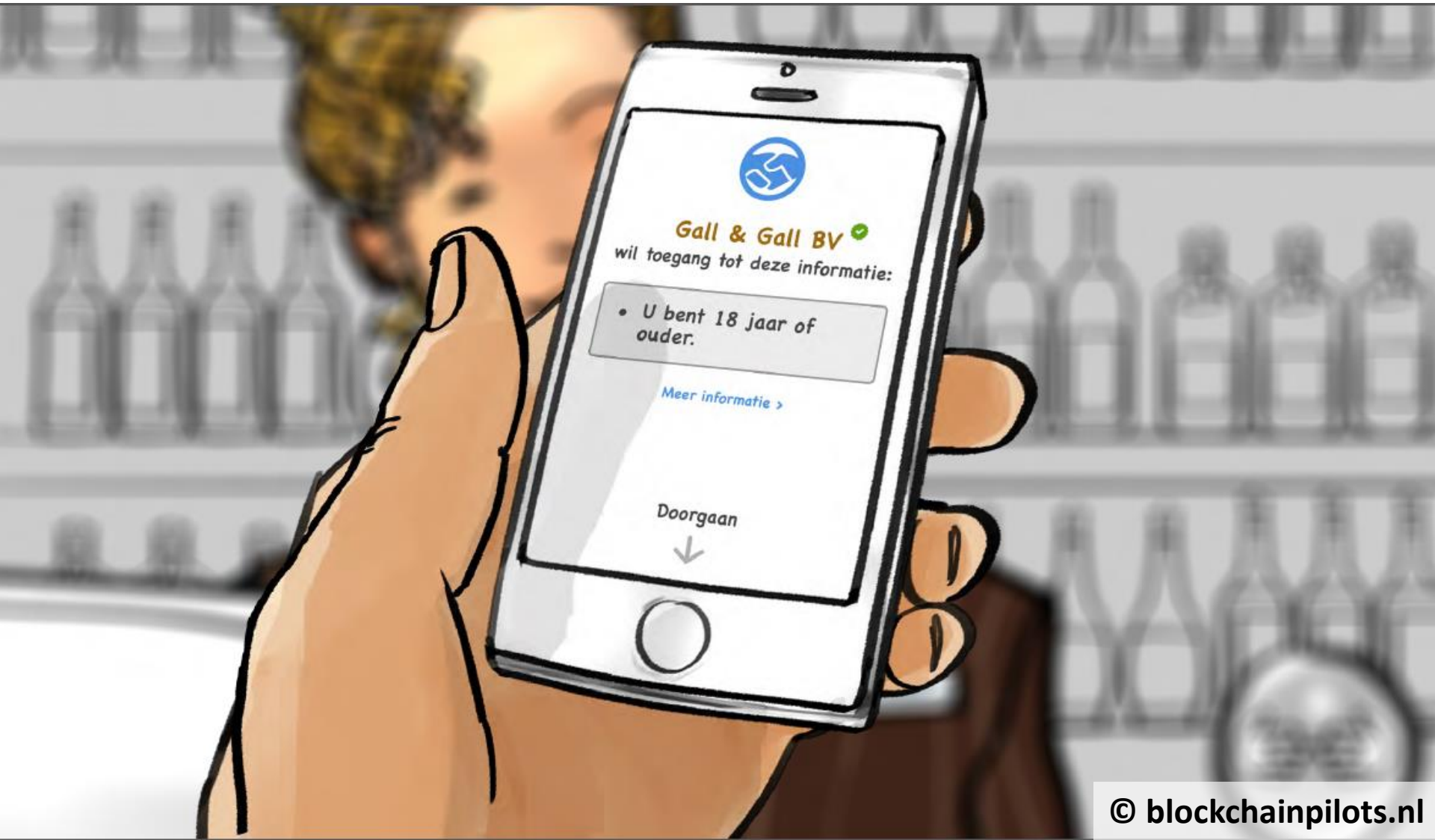
Alice zelf hoeft geen blockchain account of kopie te hebben

In werkelijkheid vaak extra crypto (hashing, encryptie, pseudoniemen)

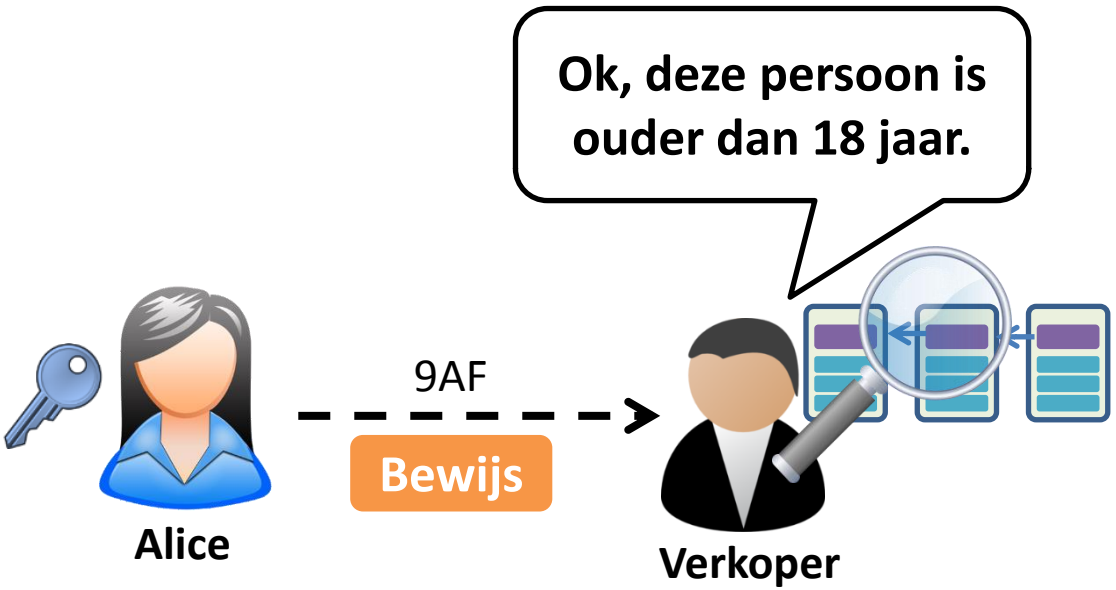
Gelijkaardig aan digitale handtekening, maar meer mogelijkheden

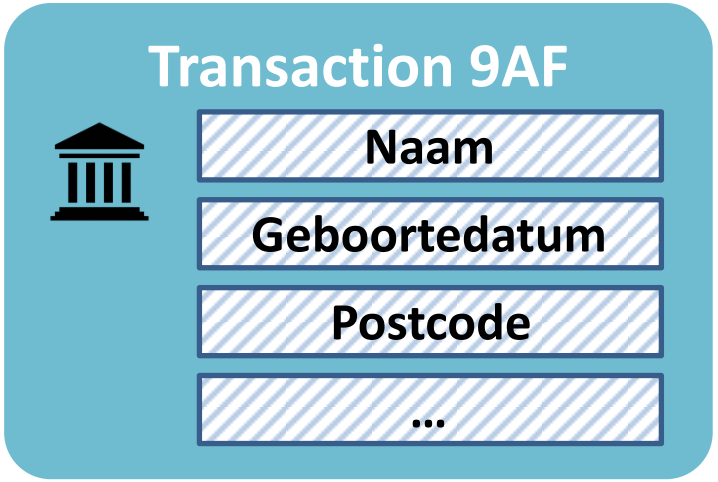
Identeitsgegevens

Identeitsgegevens



Identeitsgegevens





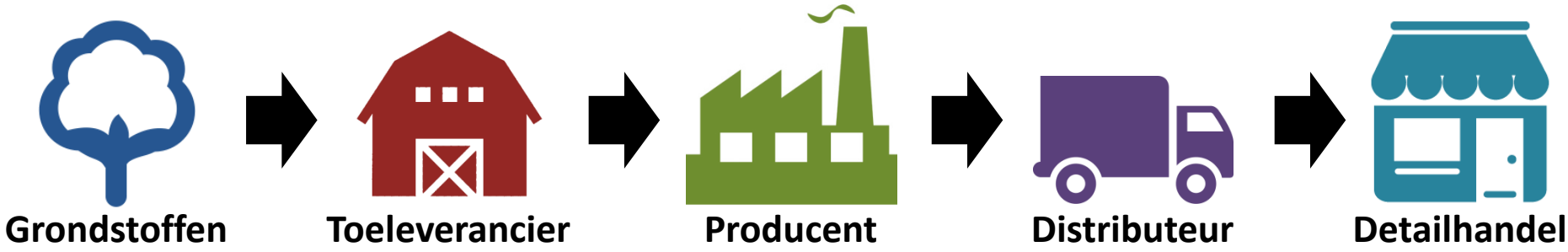
Bewijs

Geboortedatum **< vandaag – 18 jaar**

Gebruik complexe cryptografie (zero-knowledge proofs)

Tracking Supply Chain

voedsel, diamanten, auto's en hun onderdelen, ….

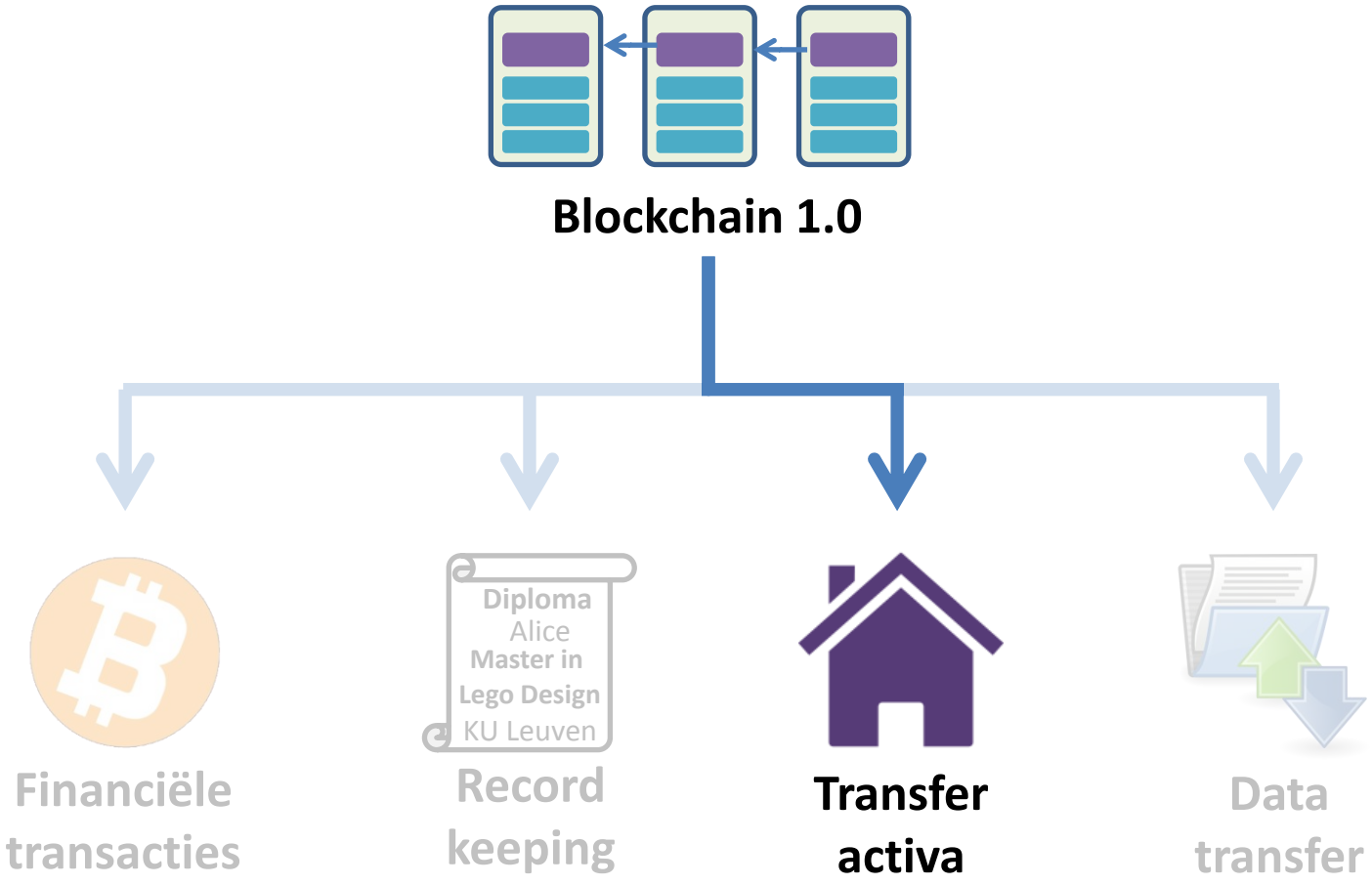


Waar bevindt zich het noodzakelijke onderdeel?

Hoe zit het met de herkomst van mijn product?

Mogelijke cases: Voedselveiligheid, afvalverwerking

Blockchain Toepassingen



Verminderd vertrouwen vereist in centrale / intermediaire partijen

Transfer Activa

Vastgoed
Kadaster

Wagen

Diamant

Auteursrechten

Ticket

.bit
Domeinnaam

Zo weinig mogelijk data op blockchain → Vaak slechts fingerprint (hash)

Applicaties

Auteursrechten

Kadaster

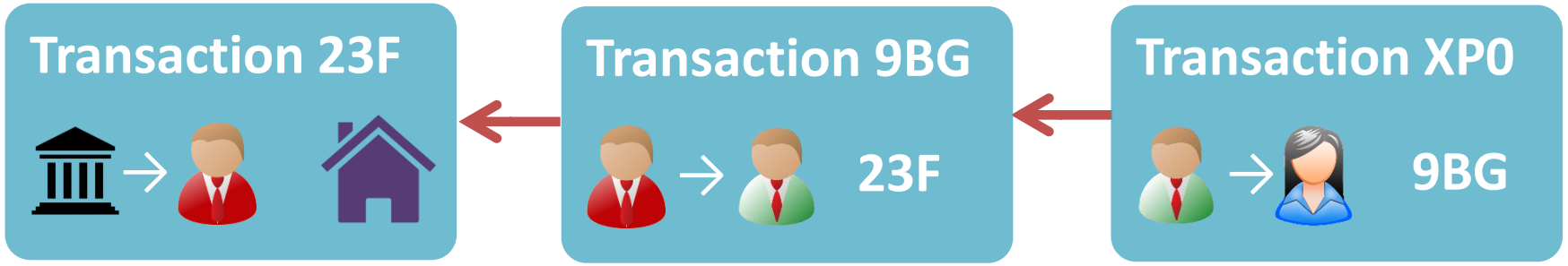
Domeinnamen

Domeinnamen

Diamanten

Platform

Value Transfer



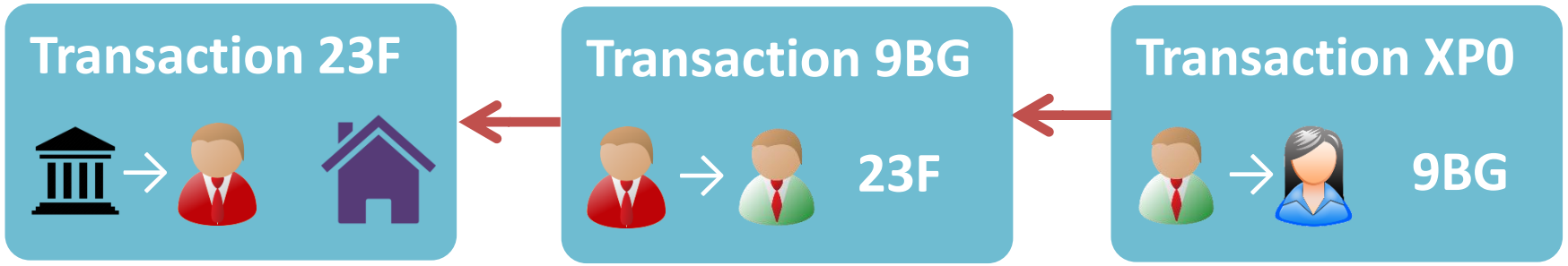
Erkende authoriteit (hypotheekbewaarder)

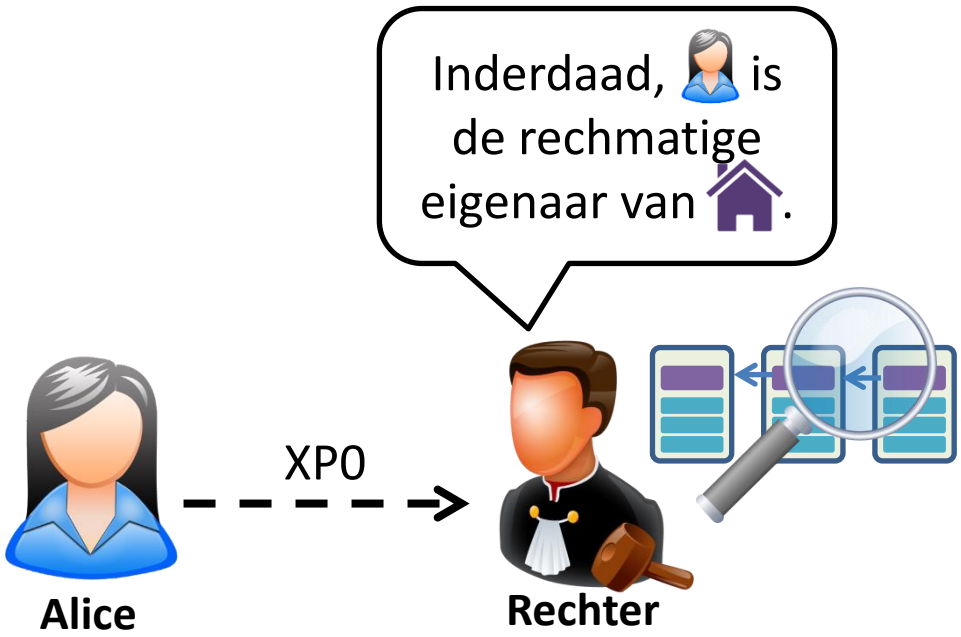
Eigenaar 1 (Bob)

Eigenaar 2 (Charlie)

Autoriteit blijft nodig

Bewijs van Bezit





Alice hoeft zelf geen kopie van blockchain te hebben

Volledige historiek zichtbaar

Blockchain Toepassingen

Blockchain 1.0

Financiële transacties

Record keeping

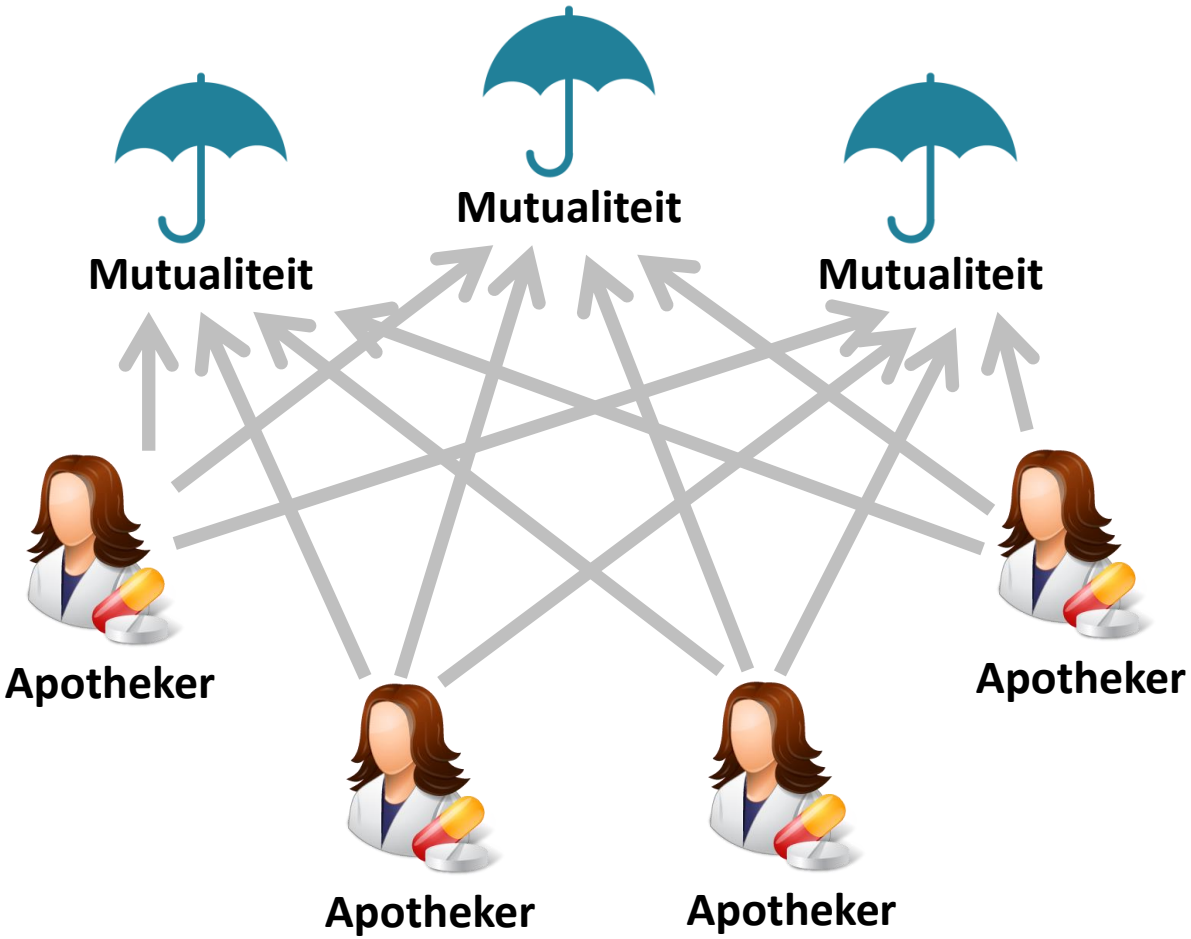
Transfer activa

Data transfer

Verminderd vertrouwen vereist in centrale / intermediaire partijen

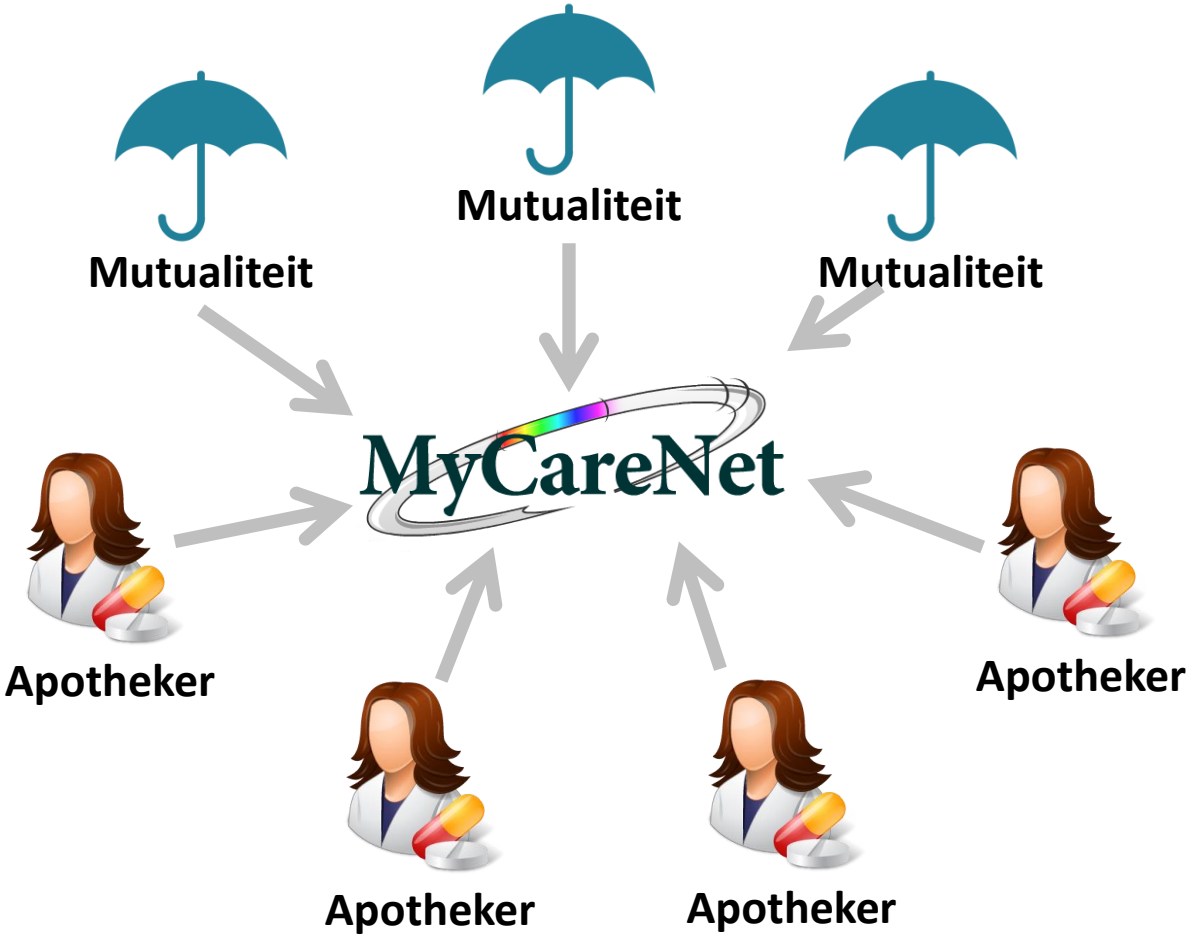
Data Transfer

Vb. Verzekerbaarheid: Is burger aangesloten bij een ziekenfonds?



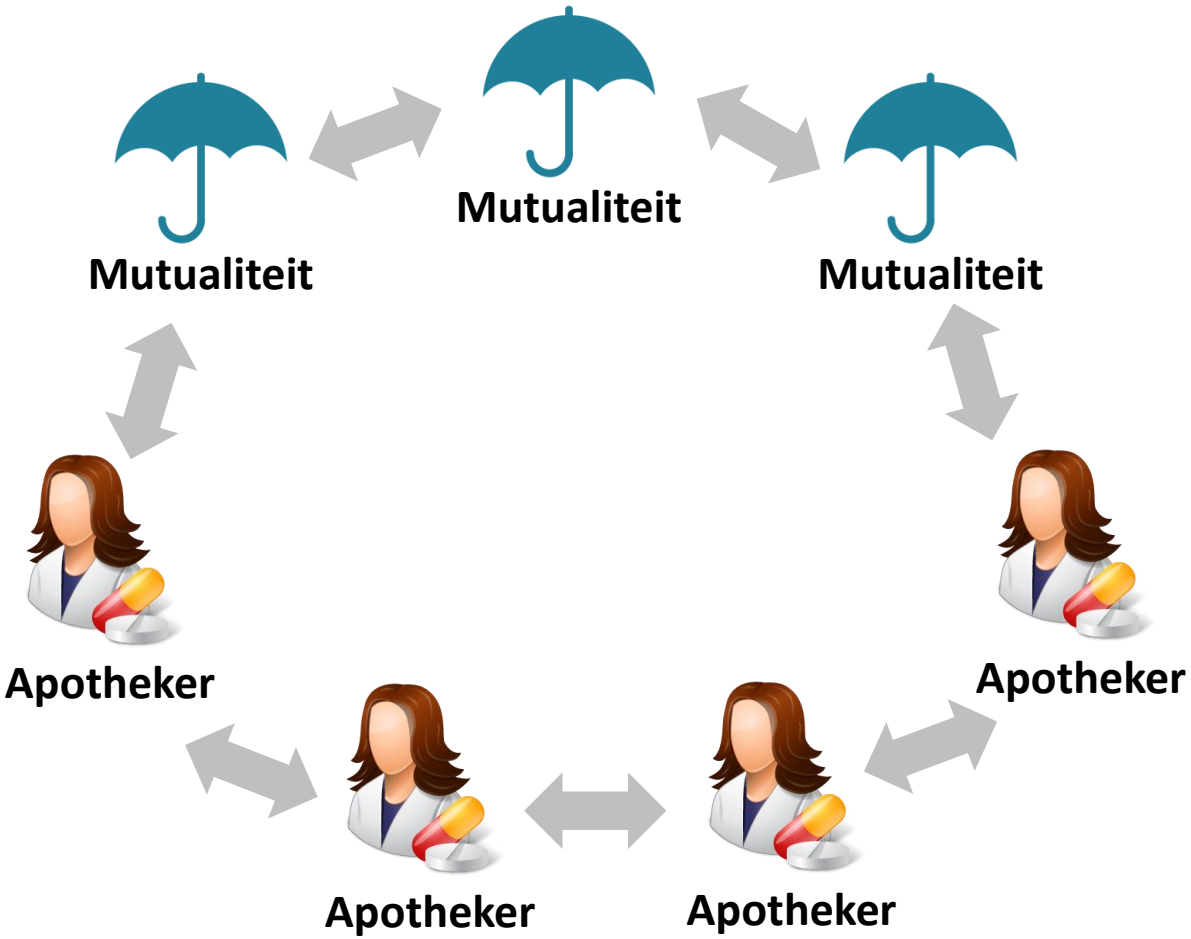
Data Transfer

Vb. Verzekerbaarheid: Is burger aangesloten bij een ziekenfonds?



Data Transfer

Vb. Verzekerbaarheid: Is burger aangesloten bij een ziekenfonds?

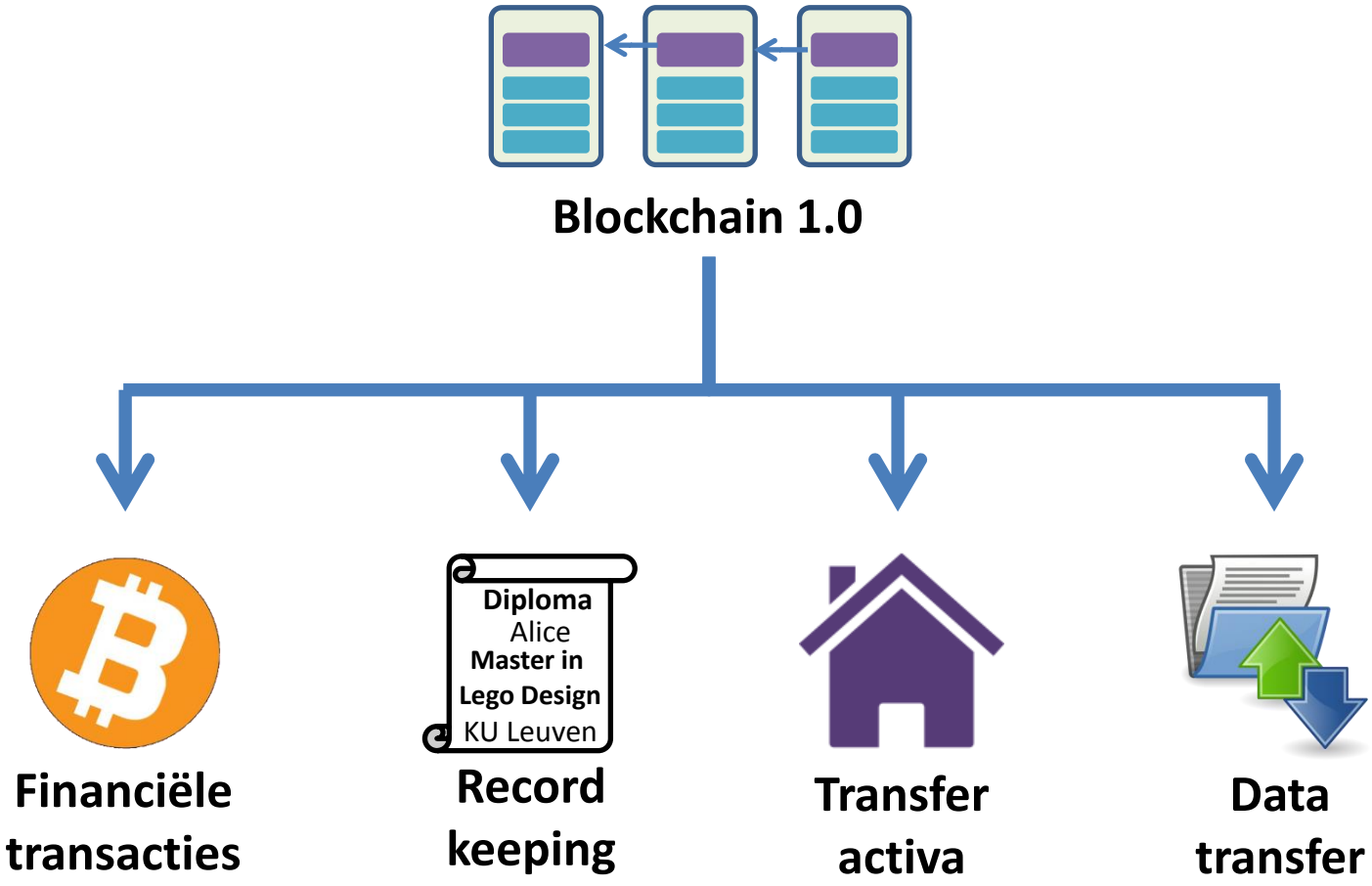


Iedereen steeds meest recente informatie

Geen high availability vereist

Mogelijks extra bescherming (cryptografie) vereist→ extra complexiteit

Blockchain Toepassingen

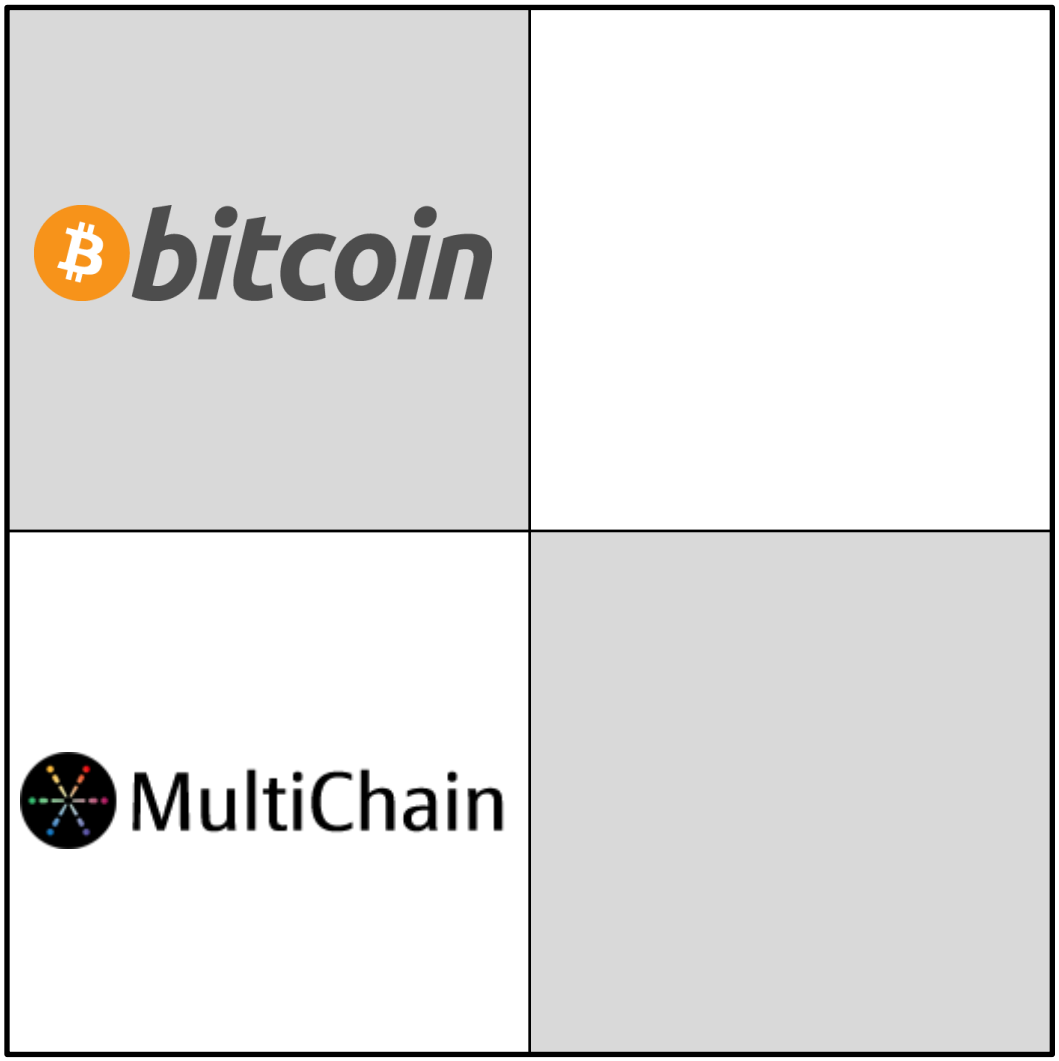


Verminderd vertrouwen vereist in centrale / intermediaire partijen

Enkele Blockchain Platformen

Unpermissioned
- Iedereen kan blokken creëren
- Gedistribueerder
- Incentives d.m.v. cryptogeld
- Vaak resource intensive

Permissioned
- blokcreatie door geselecteerden (whitelist)
- Gecentraliseerder
- Cryptogeld niet vereist
- Resource efficiënt



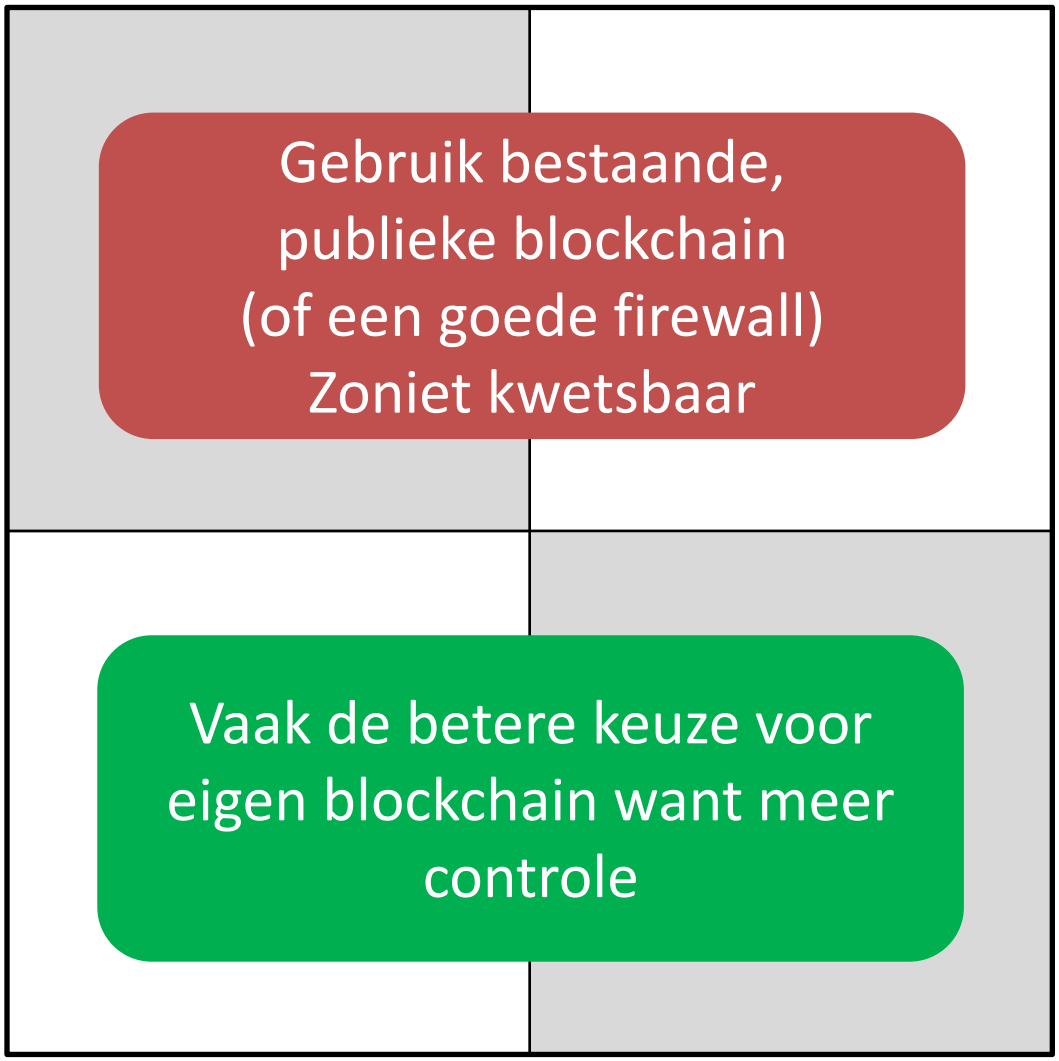
Blockchain 1.0
Opslag
op blockchain

Blockchain 2.0
Rekenkracht
op blockchain

Enkele Blockchain Platformen

Unpermissioned
- Iedereen kan blokken creëren
- Gedistribueerder
- Incentives d.m.v. cryptogeld
- Vaak resource intensive

Permissioned
- blokcreatie door geselecteerden (whitelist)
- Gecentraliseerder
- Cryptogeld niet vereist
- Resource efficiënt



Uitdagingen

Security

- Vertrouwen onderliggende crypto
- Privacy & confidentialiteit
- Sleutelbeheer, end-point protection

Andere

- Schaalbaarheid
- Standaardisatie
- Paradigmashift
- Wisselkoersen

=> Veel onderzoek om deze uitdagingen aan te pakken

Conclusies

Enorme hype - overoptimisme?

- Uitdagingen (schaalbaarheid, sleutelbeheer, etc.)
- Het is mogelijk met blockchain ≠ Blockchain is de beste aanpak
- Technologie evolueert snel

Explosie van initiatieven

- Weinig volwassen applicaties
- Vaak weinig technische details (lijken in de kast?)

Applicaties

- Financiële transacties, record keeping, transfer activa & data transfer
- Verschillende blockchain platformen

Agenda

Smals
ICT for society

Blockchain 1.0

Pauze

Blockchain 2.0

Pauze

Agenda

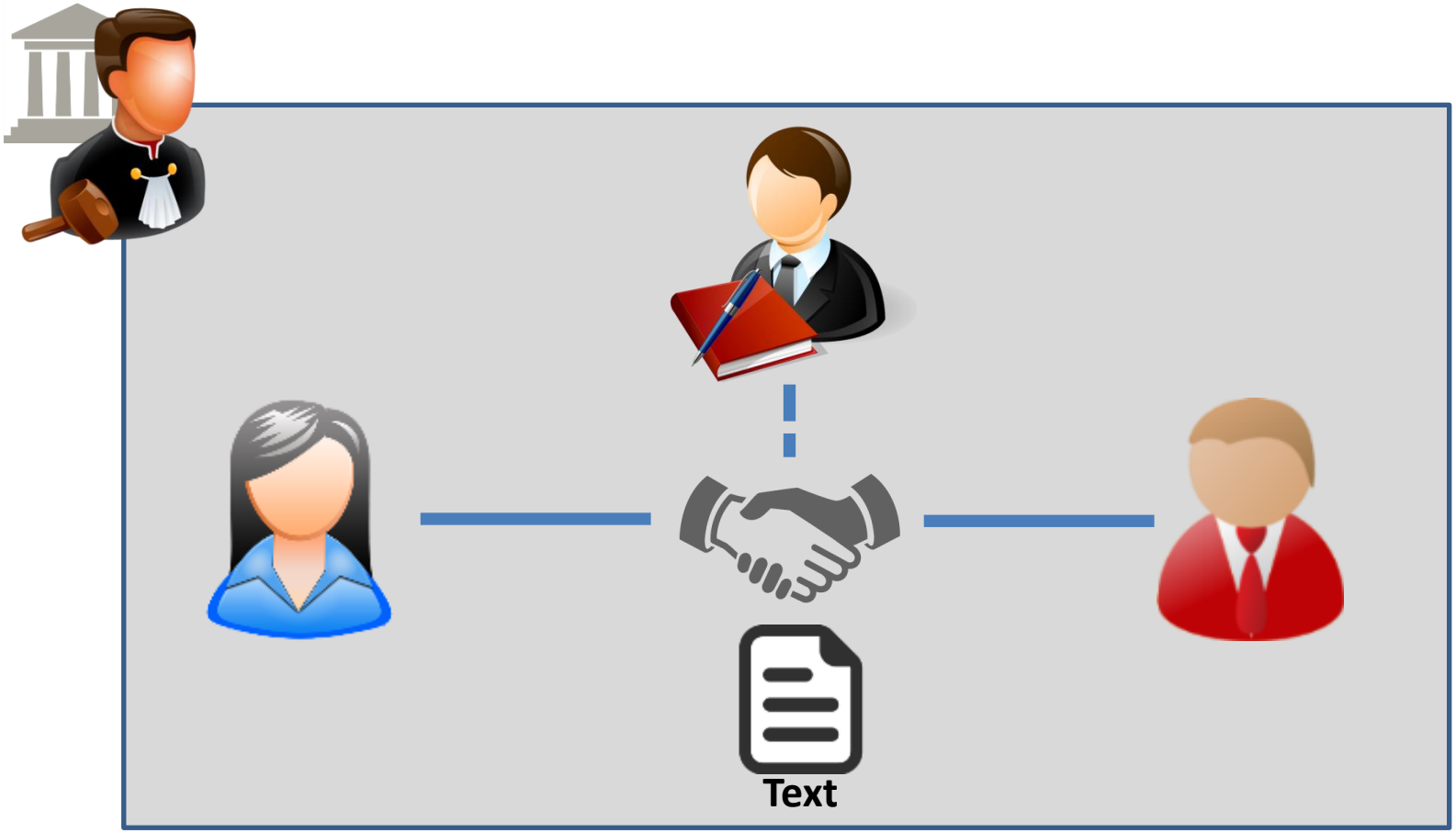
Blockchain 1.0

Pauze

Blockchain 2.0

Smart Contracts

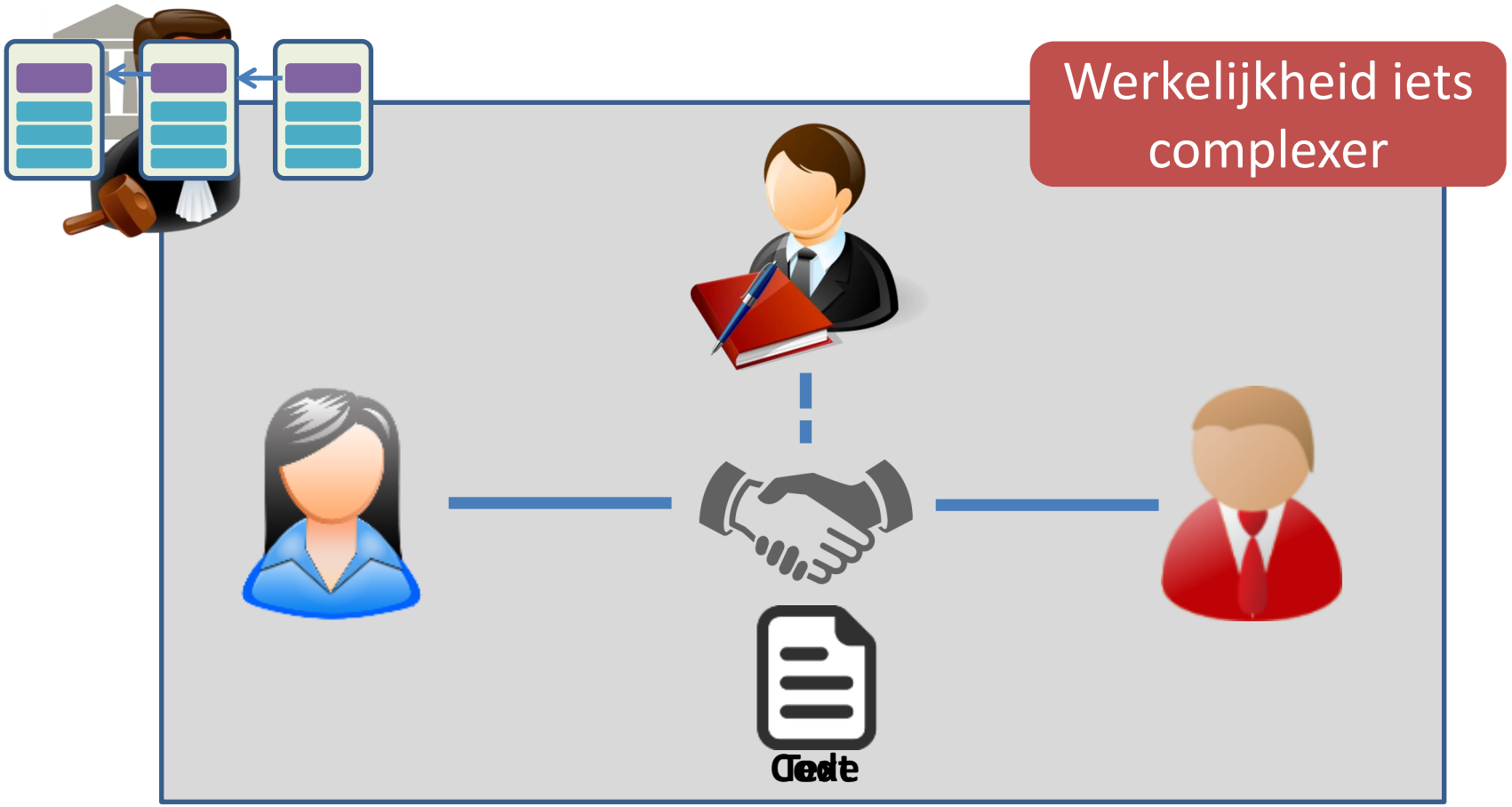
Traditioneel Contract



Contract afgedwongen door wetgeving (bindend)

Mogelijks vertrouwde autoriteit vereist

Smart Contract



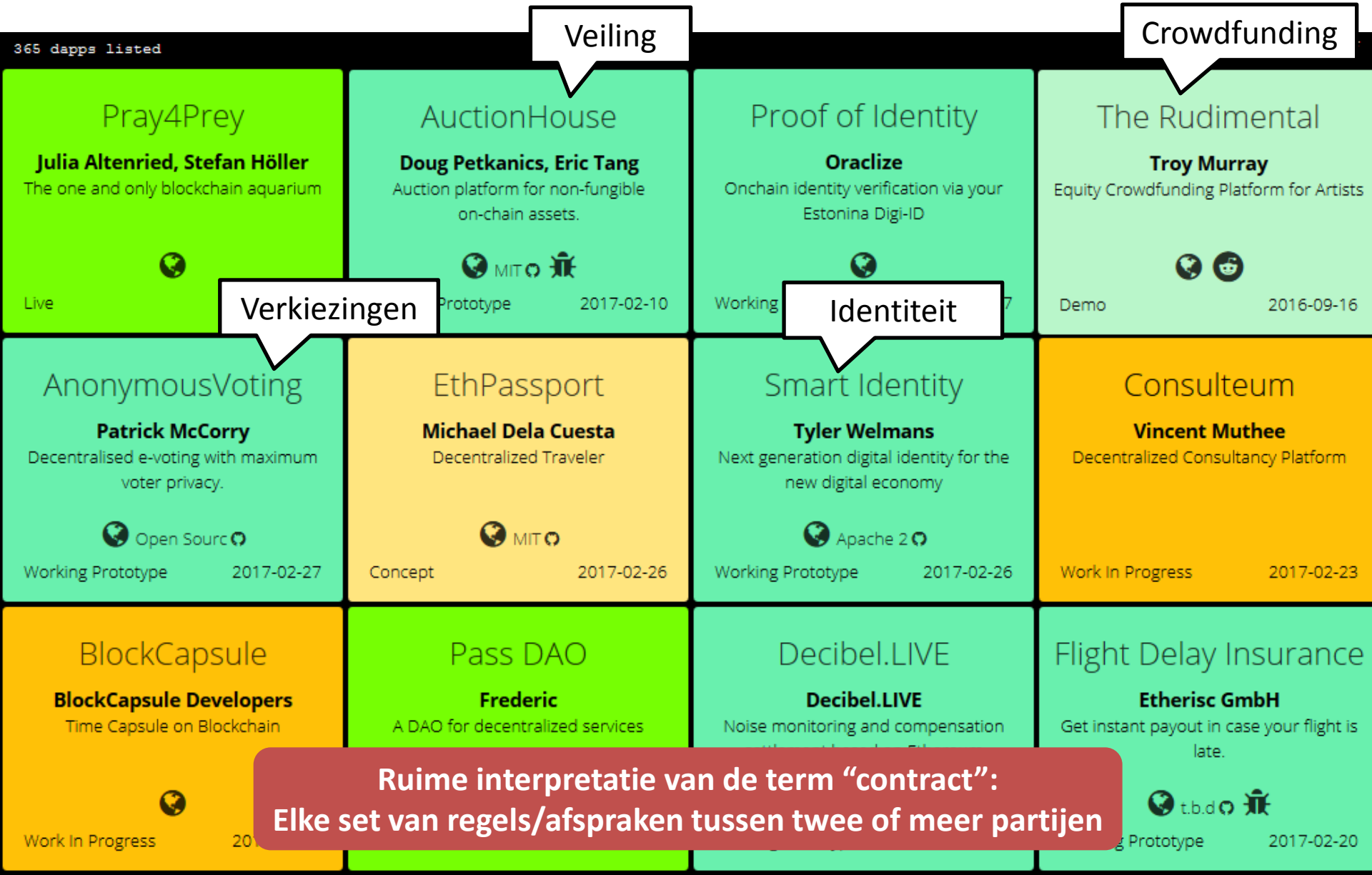
Contract afgedwongen door technologie

Geen vertrouwde autoriteit nodig

Sneller & efficiënter

Voorbeelden

http://dapps.ethercasts.com/



Ruime interpretatie van de term “contract”:
Elke set van regels/afspraken tussen twee of meer partijen

Smart Contracts

Meer mogelijkheden

- Meer flexibiliteit voor blockchain 1.0 toepassingen
- Nieuwe toepassingen

Veiling

- Bod plaatsen → Geld onmiddellijk naar smart contract
- Overboden → Smart contract betaalt je terug
- Einde veiling → Bedrag hoogste bieder naar verkoper

Een aantal nieuwe uitdagingen

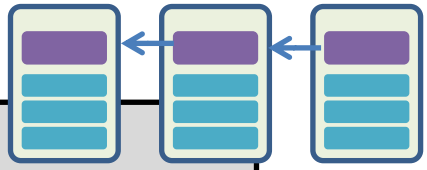
- Zie later

Smart Contracts (Blockchain 2.0)

Charlie

end(...)

20€



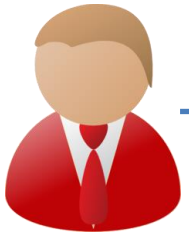
Contract{
function bid(){...}
function end(){...}

HighestBid: **10€**
HighestBidder: **Alice**
Beneficiary: Charlie
}

bid(...), 10€

10€

Alice



Bob

bid(...), 20€

Uitvoering van contract gedistribueerd

Geld tijdelijk geblokkeerd door contract

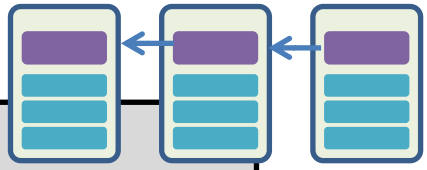
Oproepen functies in contract via transactie

Events in Smart Contracts

Charlie

end(...)

20€



Contract{
function bid(){...}
function end(){...}
HighestBid: **10€**
HighestBidder: **Alice**
Beneficiary: Charlie
}

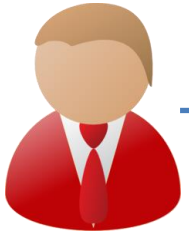
bidEvent: 10€

bid(...), 10€

10€

Alice

bidEvent: 10€



Bob

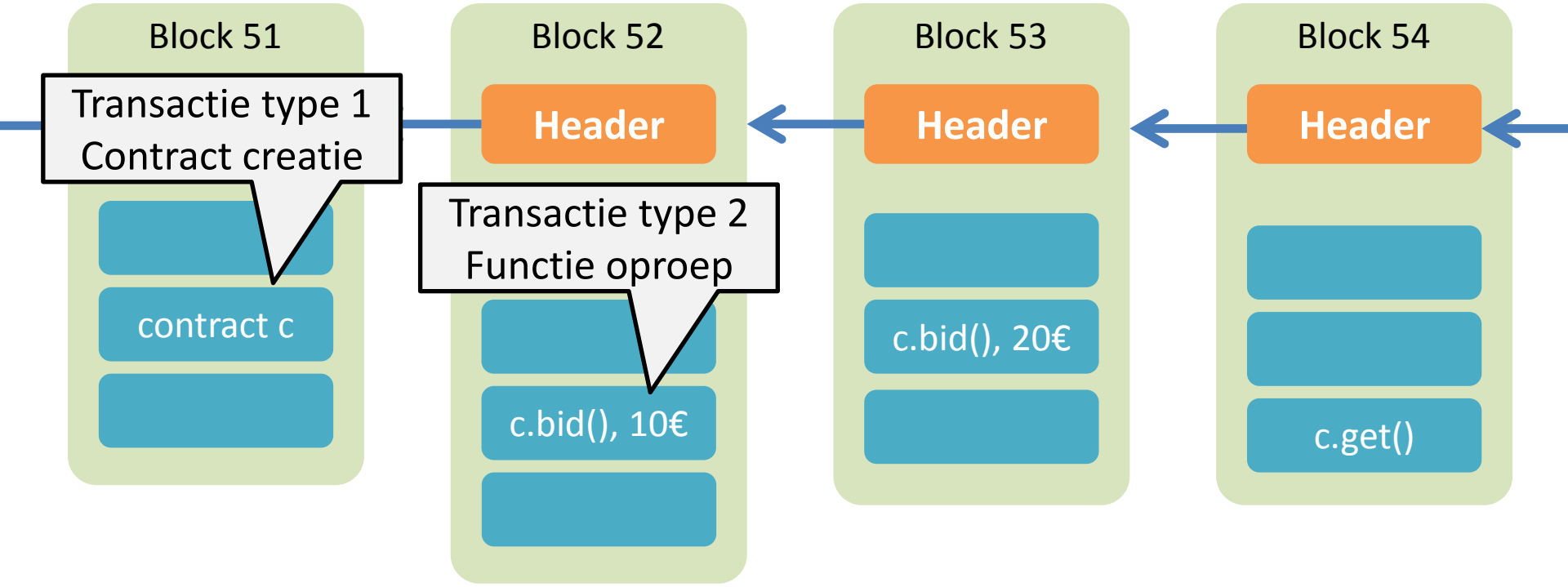
bid(...), 20€

Dave

Events informeren Charlie & Dave over nieuwe biedingen

Oude events zichtbaar: Charlie & Dave niet per se permanent online

Smart Contract Blockchain



Transactie voor functieoproep bevat

- Id contract
- Naam functie
- Argumenten
- Bedrag

Een Concreet Smart Contract

```
contract SimpleAuction
{
    address public beneficiary;
    uint public auctionStart;
    uint public biddingTime;

    address public highestBidder;
    uint public highestBid;

    bool ended;

    event HighestBidIncreased(address bidder, uint amount);
    event AuctionEnded(address winner, uint amount);

    function SimpleAuction(uint _biddingTime, address _beneficiary)
    {
        beneficiary = _beneficiary;
        auctionStart = now;
        biddingTime = _biddingTime;
    }
    ...
}
```

http://solidity.readthedocs.io/en/develop/solidity-by-example.html

```
contract SimpleAuction
{
    ...
    function bid() payable
    {
        if (now > auctionStart + biddingTime) throw;
        if (msg.value <= highestBid) throw;
        if (highestBidder != 0) highestBidder.send(highestBid);

        highestBidder = msg.sender;
        highestBid = msg.value;
        HighestBidIncreased(msg.sender, msg.value);
    }

    function end() {
        if (now <= auctionStart + biddingTime) throw;
        if (ended) throw;

        ended = true;
        AuctionEnded(highestBidder, highestBid);
        beneficiary.send(this.balance)
    }
}
```

Disclaimer: Een Ethereum exploit wordt genegeerd voor de eenvoud

http://solidity.readthedocs.io/en/develop/solidity-by-example.html

Doe dit **NOOIT**…

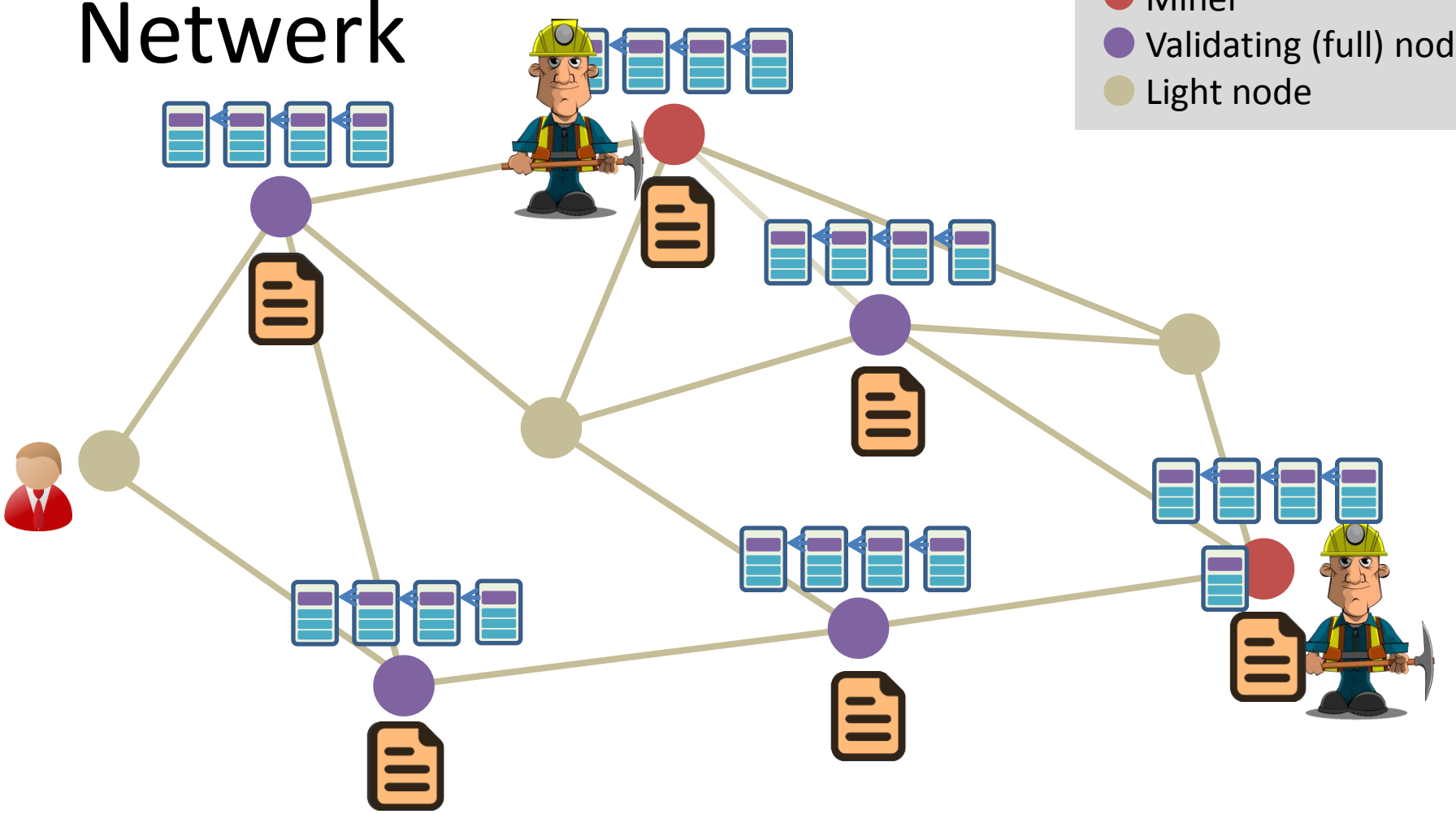
proofs:	c0796844c3cbc…	→ true
	5d5f4926be230…	→ true
	c56d58202b0aa…	→ true
	17f8f6699a8948…	→ true
	…	

```
// Proof of Ownership contract
contract ProofOfOwnership{
        mapping(bytes32=>bool) proofs;

        //calculate and store the proof for a document
        function notarize(string document){
                var proof  = sha256(document);
                proofs[proof] = true;
        }

        // check if a document has been notarized
        function checkDocument(string document) returns (bool){
                var proof = sha256(document);
                return proofs[proof];
        }
}
```

document volledig bewaard in transactie op blockchain
⇒ blockchain snel zeer groot & bevat gevoelige data
⇒ Toch minder evident dan op eerste zicht lijkt

Ernstig voorbeeld op seminarie in november ‘16 door veelgevraagde blockchain spreker

Netwerk



Full nodes houden lokale kopie van contracttoestand up-to-date

Elke full node voert lokaal dezelfde functieoproepen uit

Veiligheidsmechanismes zodat iedereen correcte versie

Ontwikkelomgeving Programmeertaal: Solidity

```
contract SimpleAuction
{
    address public beneficiary;
    uint public auctionStart;
    uint public biddingTime;

    address public highestBidder;
    uint public highestBid;

    bool ended;

    event HighestBidIncreased(addre
    event AuctionEnded(address winr

    function SimpleAuction(uint _bi
    {
        beneficiary = _beneficiary;
        auctionStart = now;
}
```

Gecompileerde Ethereum byte code op blockchain

```
606060405234610000576040516037c380380
37c833981016040528080518201919050505b5
360006000610100a8154173ffffffffffffffffffff
ffffffffffff02191690837fffffffffffffffffffffffffffff
ffff16021790555505b80600190805190602001906
805460018160011615610100020316600290004
600052602060002090601f016020900481019282
01f106100b557805160ff1916838001178555610
3565b828001600101855582156100e35791820
b828111156100e25782518255916020019190
101906100c7565b5b5090506101091905b808
1156101045760008160009055506001016100e
5b5090565b50505b505b6102608061011c6000
6000f300606060405260003 57c010000000000
0000000000000000000000000000000000000000
00900463ffffffff16806341c0e1b514610049578
```

Turing compleet (↔ Bitcoin scripts). Alles wat te berekenen is met een computer kan ook in Solidity / Ethereum byte code

Oracles - Voorbeelden

Vertrouwde, exclusieve leverancier van real-world data aan een smart contract

IoT, autoriteiten ,…

Electriciteitsmeters

- Meter plaats waardes gemeten consumptie geregeld op blockchain
- Contract berekent te betalen bedrag
- Indien niet betaald (via blockchain) enkel minimumlevering 10 ampère.

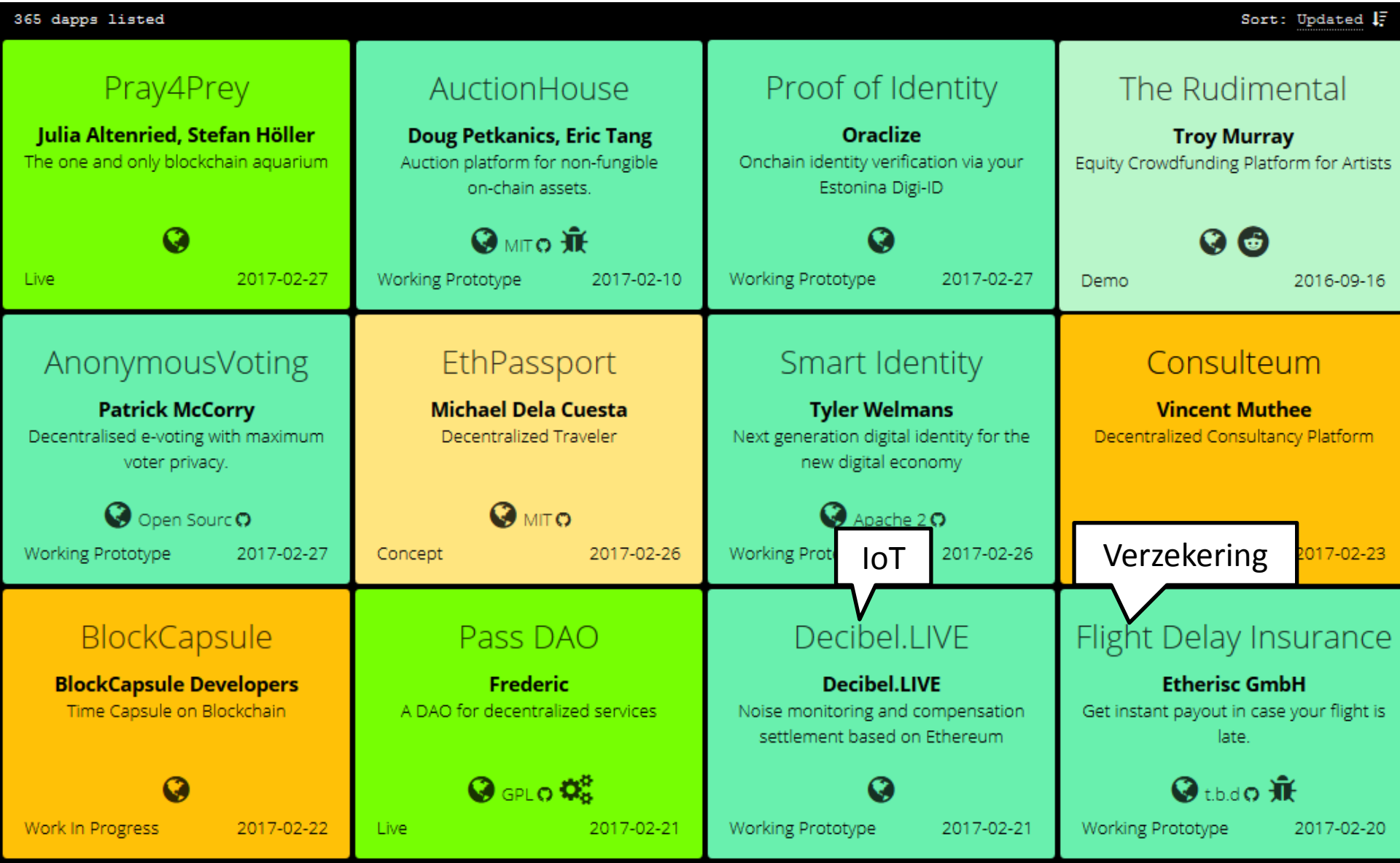
Transport van goederen

- Slager bestelt vlees en transfereert geld naar Smart Contract
- Sensor in koelwagen registreert frequent temperatuur op blockchain
- Indien temperatuur steeds binnen aanvaardbare waarden betaalt contract de leverancier. Zoniet betaalt het de slager.

Elke update van smart contract door oracle resulteert in transactie op blockchain

Voorbeelden

http://dapps.ethercasts.com/



Enkele Blockchain Platformen

Unpermissioned
- Iedereen kan blokken creëren
- Gedistribueerder
- incentives d.m.v. cryptogeld
- Vaak resource intensive

Permissioned
- blokcreatie door geselecteerden (whitelist)
- Gecentraliseerder
- Cryptogeld niet vereist
- Resource efficiënt

Blockchain 1.0
Opslag
op blockchain

Blockchain 2.0
Rekenkracht
op blockchain

Voorbeelden binnen Overheid

P R I V A C Y !

Studentenarbeid

- Op smart contract: #uur & #dagen gewerkt, verdiende €
- Werkgever betaalt via smart contract dat deel doorstort naar staat.
- Link student-ouders vereist.

Medische voorschriften

- Voorschriften op blockchain geplaatst
- Contract dwingt correct gedrag af (vb. geen double spending)
- Details volgen dadelijk

Andere cases

- Meer flexibiliteit voor Blockchain 1.0 cases
- Alle suggesties welkom!

Extra Uitdagingen

Confidentialiteit & Privacy
Alle nodes zien contract variabelen en hun historiek
=> Extra crypto kan eventueel helpen

Bugs
- Geen patching mogelijk, iedereen ziet byte code
- The DAO hack (*)

Interpretatie
- Code voor meeste mensen moeilijker te interpreteren dan menselijke taal

Verloren financiële opportuniteiten
- Geld wordt door smart contract geblokkeerd
- Niet bruikbaar voor andere investeringen

* https://www.smalsresearch.be/smart-contracts-autonome-code-op-een-blockchain/

Conclusies

Wat?

Set van regels tussen verschillende partijen afgedwongen zonder vertrouwde autoriteit

Young potential

- Disruptief / hype / onvolwassen => experimenteer
- Evolueert snel
- Meer mogelijkheden

Een concrete applicatie bouwen

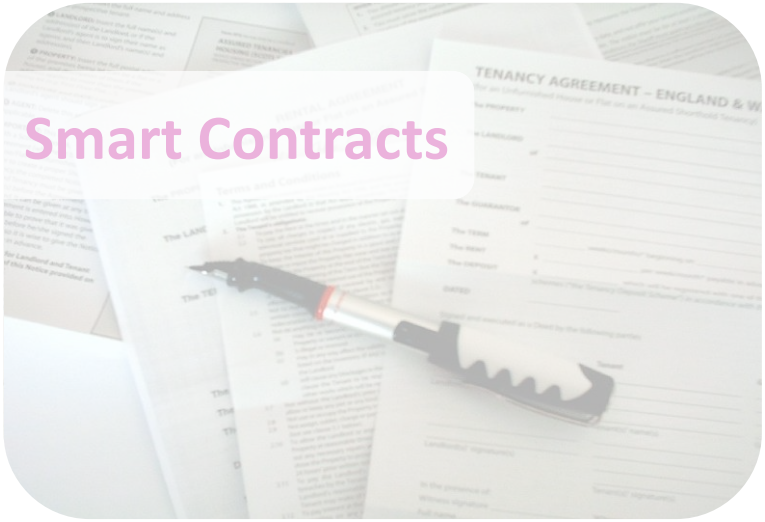
Kan minder evident zijn dan het lijkt

Agenda

Blockchain 1.0

Pauze

Blockchain 2.0



Voorschriften op een Blockchain

Smals
ICT for society

Waarom deze case?

- Geen expliciete vraag vanuit RIZIV
- Leek interessante case om mee te experimenteren

Verwerking Medische Voorschriften

Arts

Patient

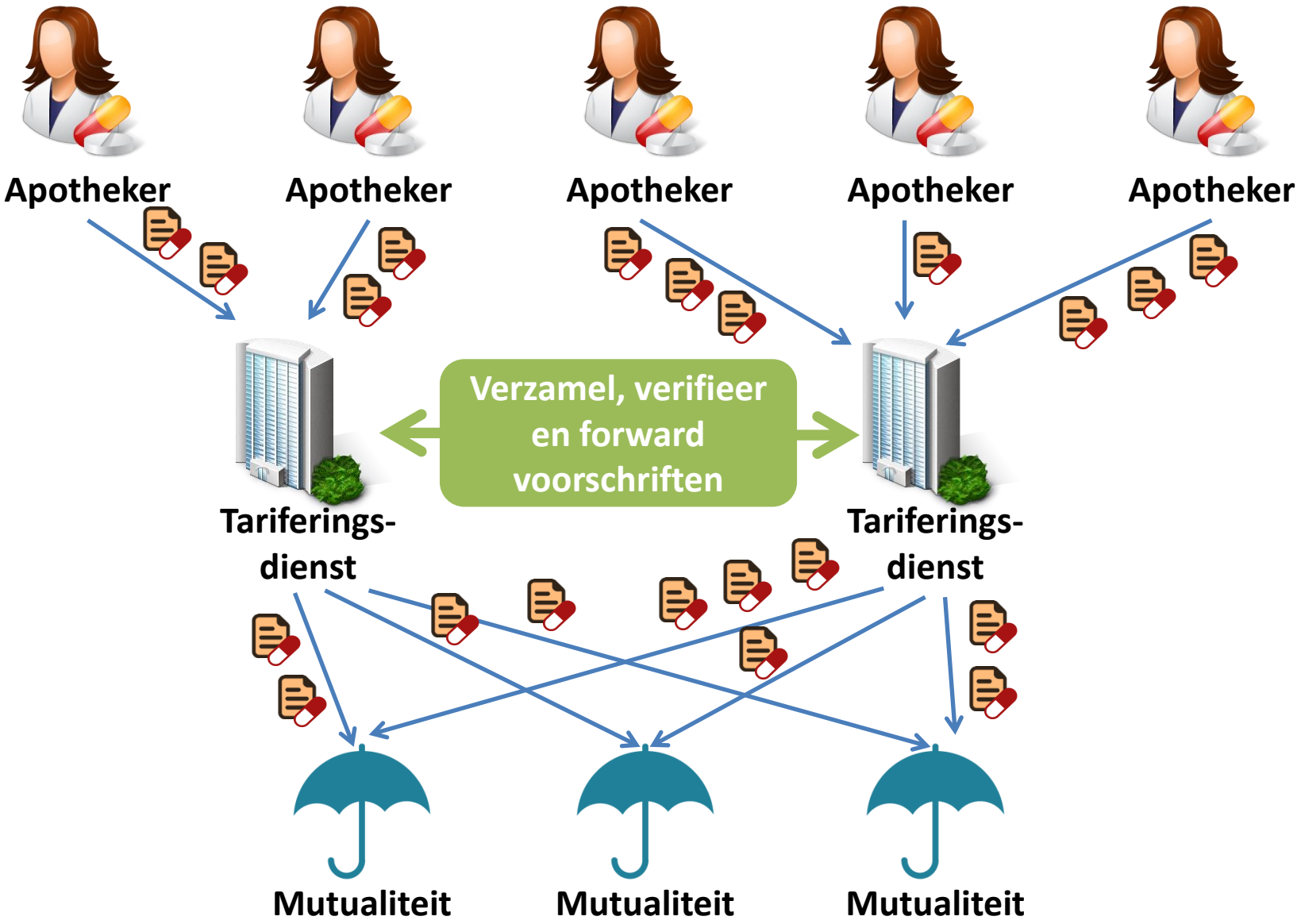
Apotheker

INAMI
RIZIV

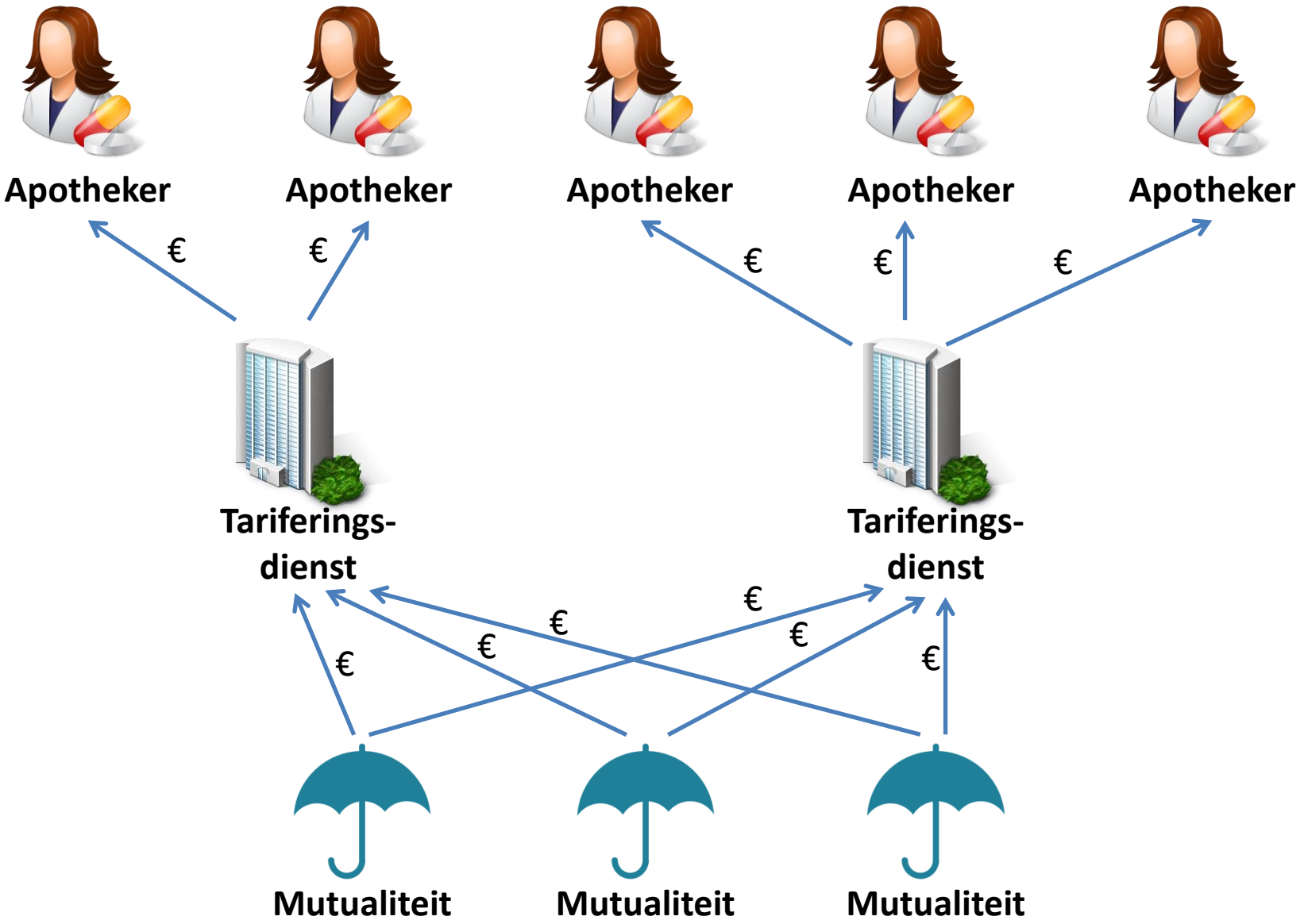
Mutualiteit

Tariferings-dienst

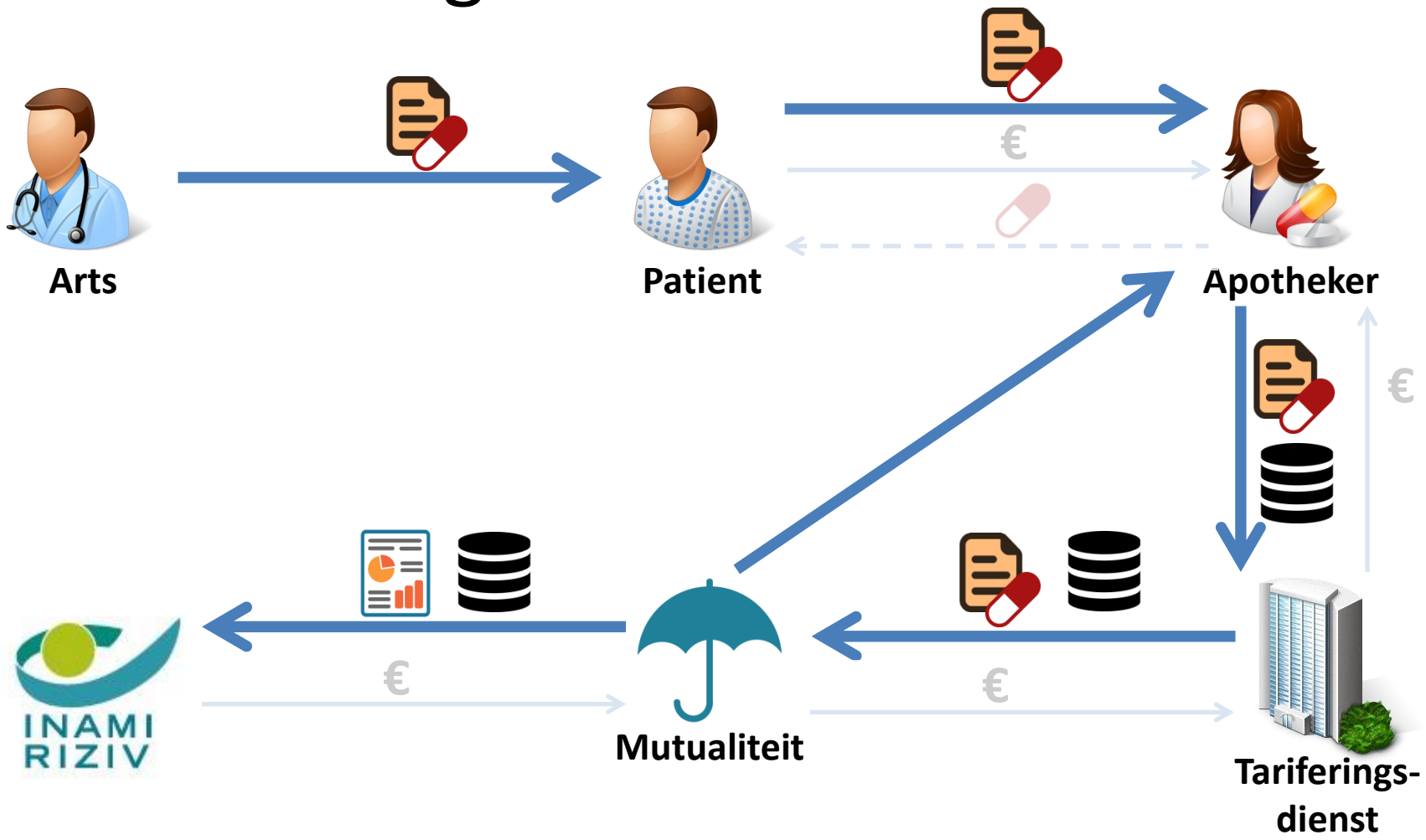
Tariferingsdienst



Tariferingsdienst



Verwerking Medische Voorschriften



Show on smartphone

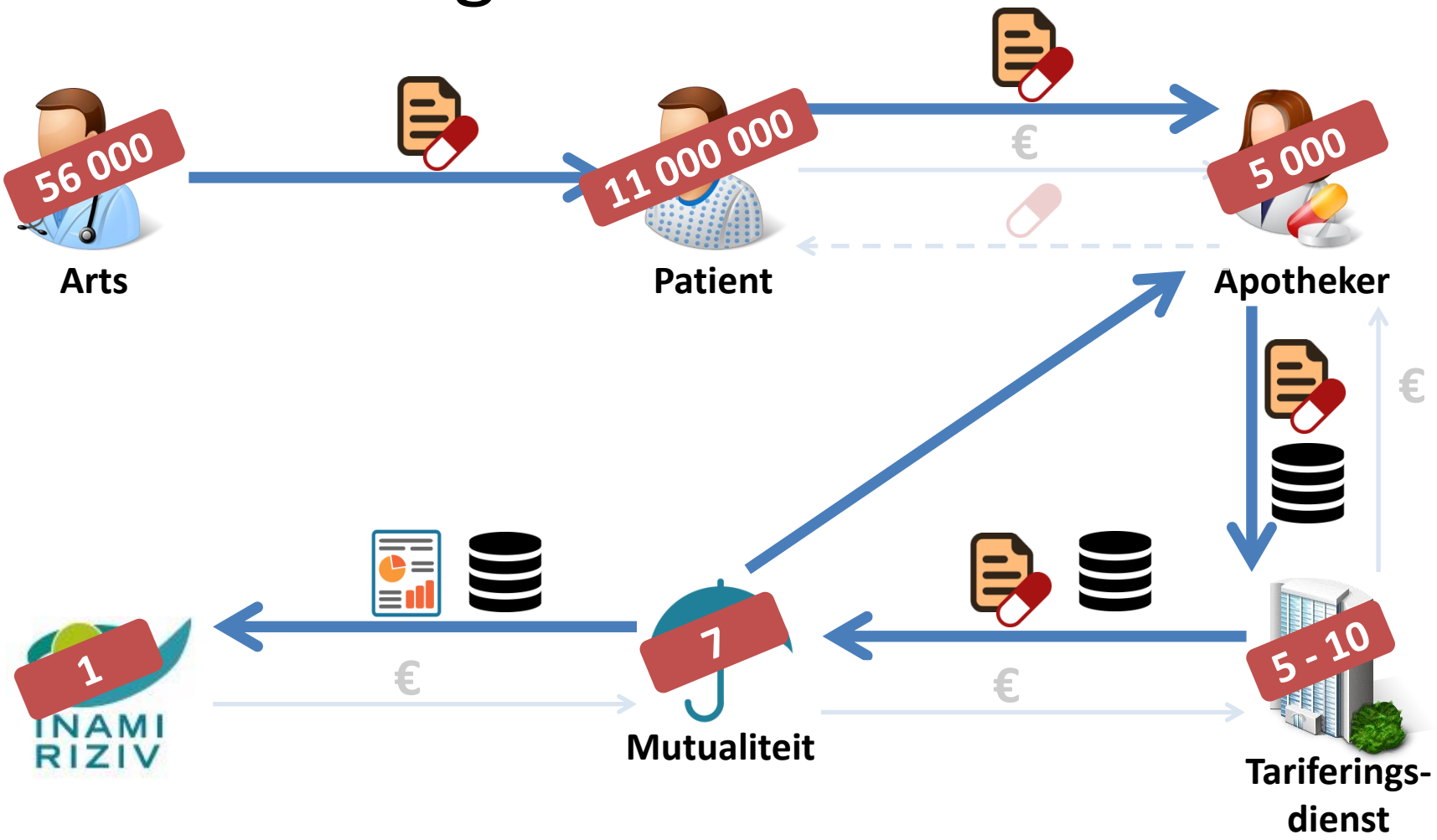
Traditional money transfer

Physical delivery

Verwerking voorschriften zodat iedereen info voor terugbetaling

Real-time analyse RIZIV

Verwerking Medische Voorschriften



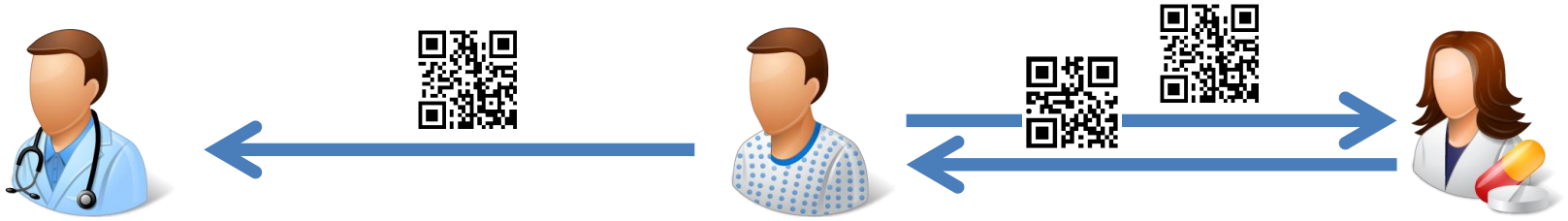
Show on smartphone

Traditional money transfer

Physical delivery

Complexe informatiestromen

Verwerking Medische Voorschriften



Show on smartphone

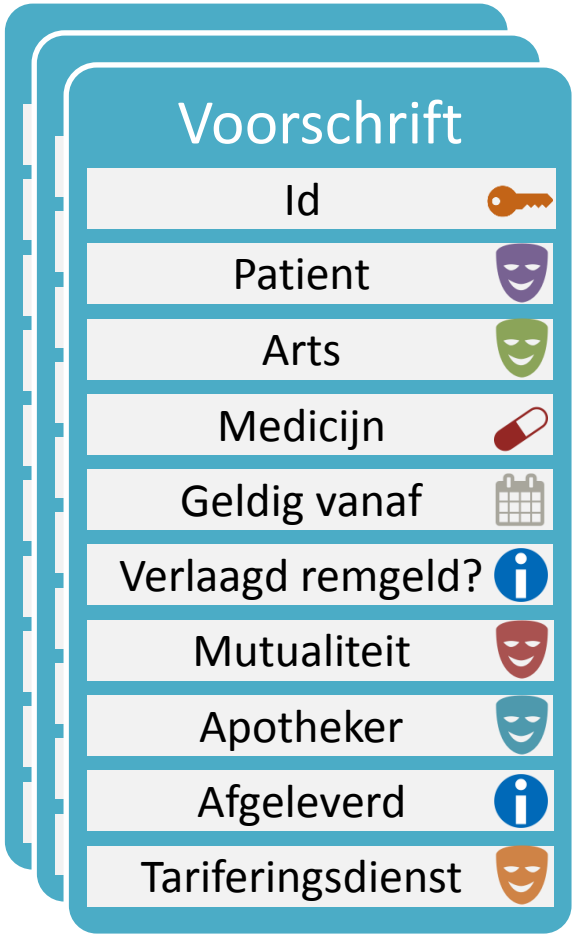
Traditional money transfer

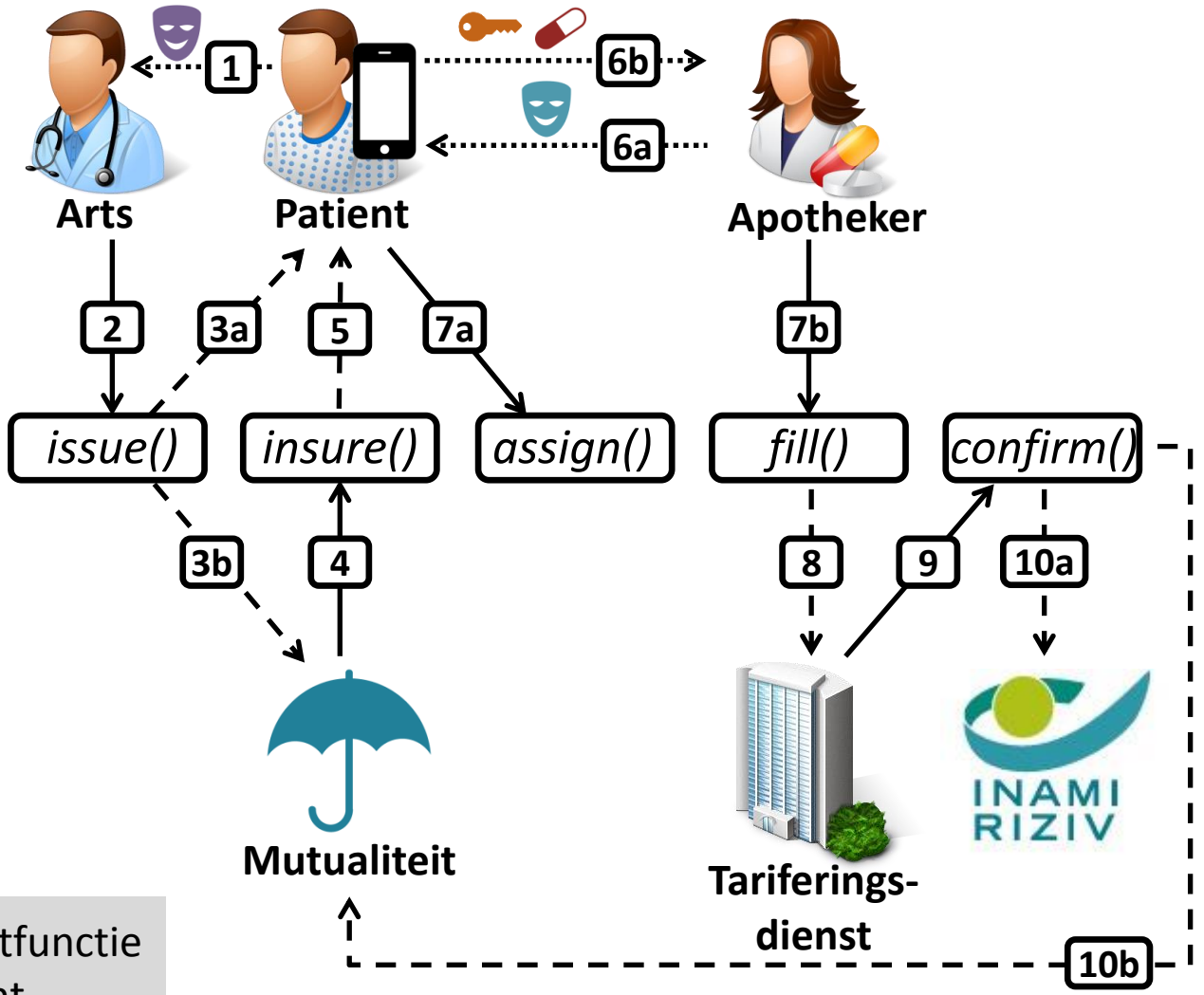
Physical delivery

Alle andere communicatie via blockchain

Privacy & confidentialiteit bedrijfsgegevens gegarandeerd

Voorschriften op een Blockchain





Oproep contractfunctie

Observatie event

Directe communicatie

function() Contractfunctie

Permanente Pseudoniemen

Fysieke wereld

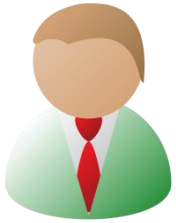
Blockchain netwerk

Bob

1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX

Alice

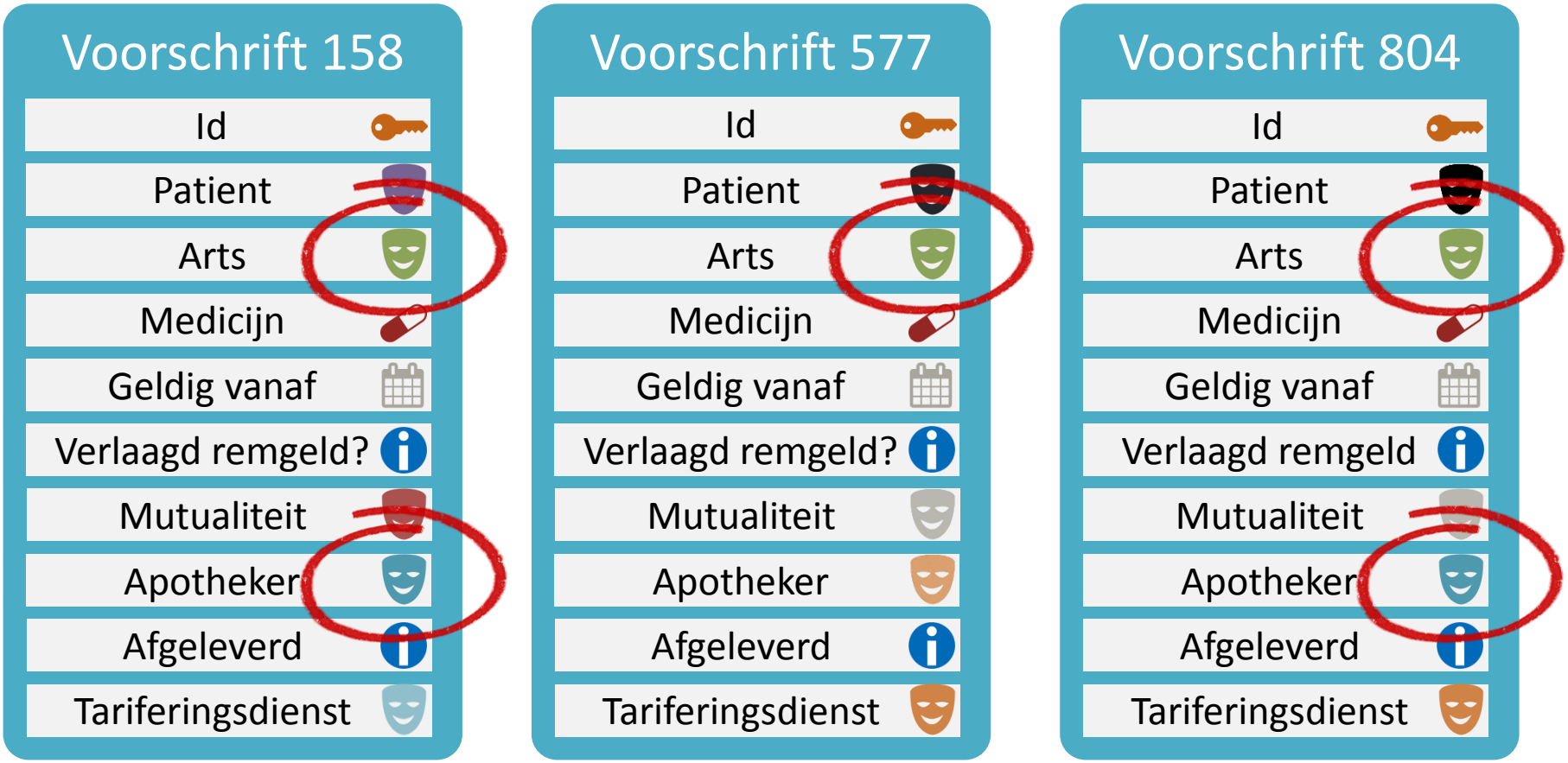
3BcMuv1VJqmwY5Wim8MPAzKAAiAKby9LcN



Charlie

1Nf311Qb8rLDkWTHrhpmNewZzkcWFYptfc

Anonimiteit



Permanente pseudoniemen bieden onvoldoende bescherming voor de privacy van de burger en confidentialiteit van bedrijfsgegevens

One-Time Pseudoniemen

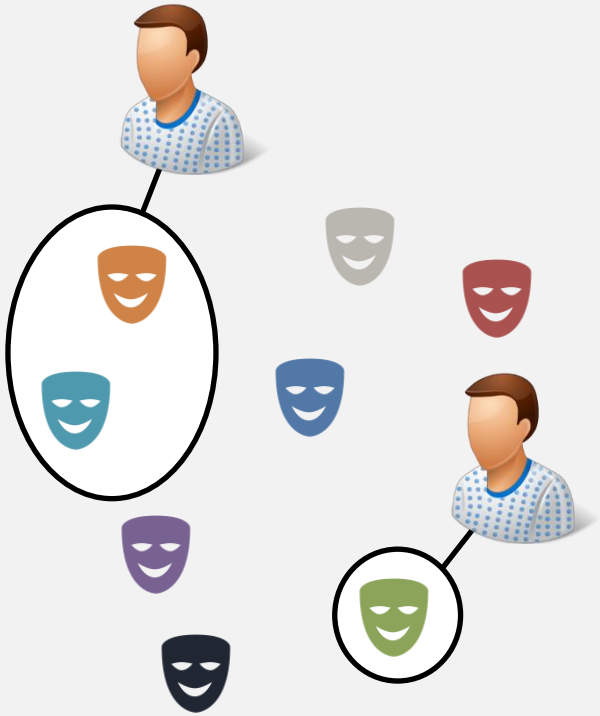
	INAMI RIZIV	CHRISTELIJKE MUTUALITEIT	Blockchain netwerk
Bob	Link		
Alice	Link	Link	
Charlie	Link		

Verschillende Views

Pseudoniemen patienten op de blockchain

INAMI RIZIV

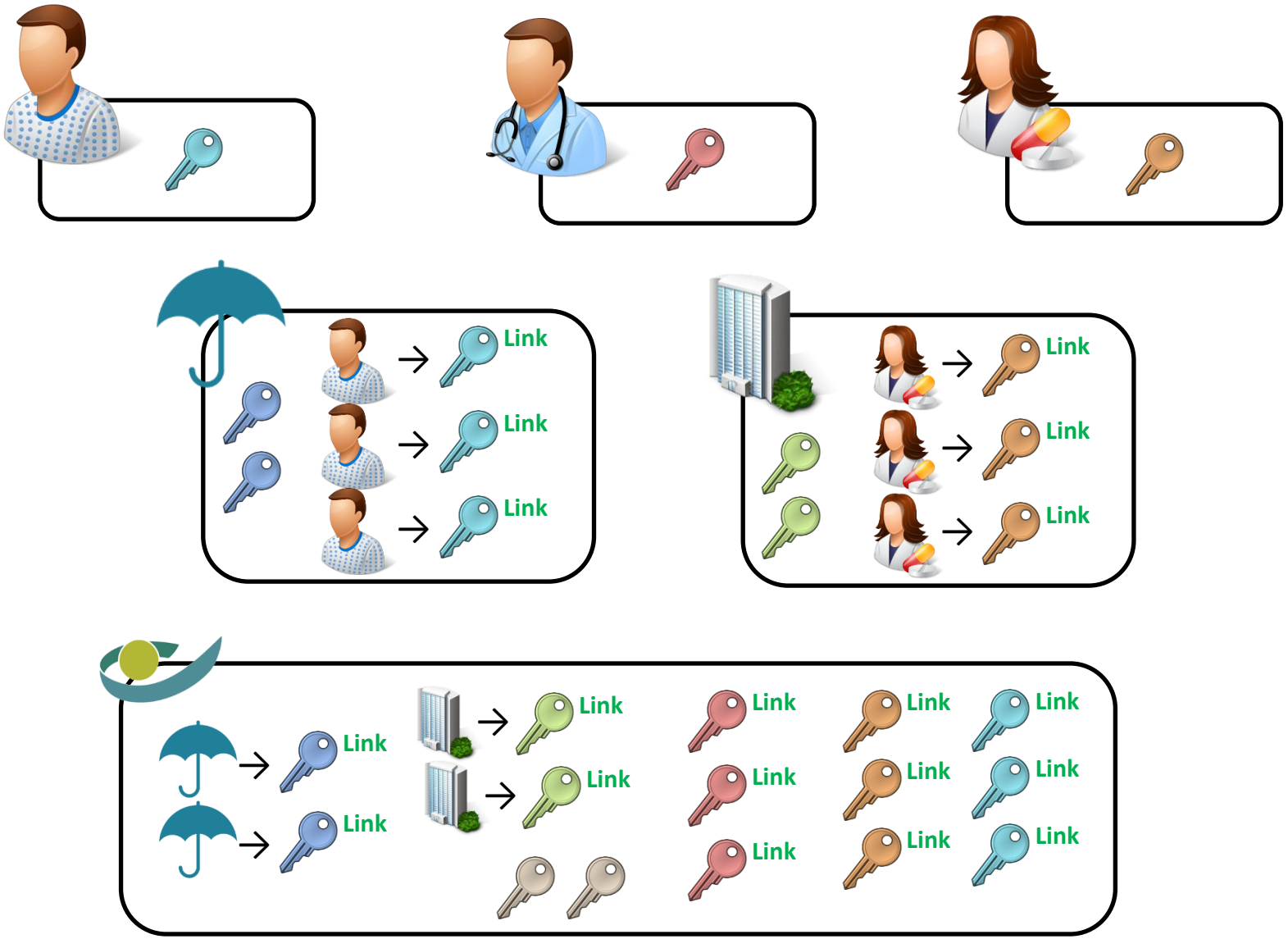
CHRISTELIJKE MUTUALITEIT



Rest of the world

Gelijkaardig voor artsen, apothekers, mutualiteiten en tariferingsdiensten

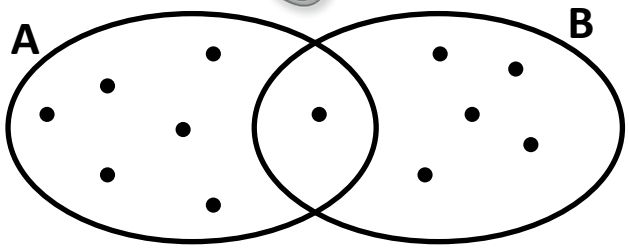
Sleutelbeheer



Goede bescherming sleutels vereist!

Link Aanval 1

Combineren info fysieke wereld & blockchain kan data lekken
Aanvaller kent identiteit patient & observeert hem fysiek

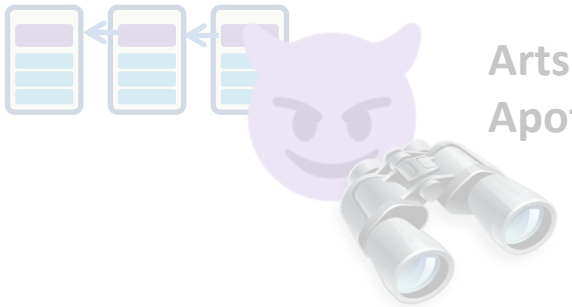


Arts: 02/04/17, 21h30 (A)
Apotheker: 28/04/17, 20h45 (B)

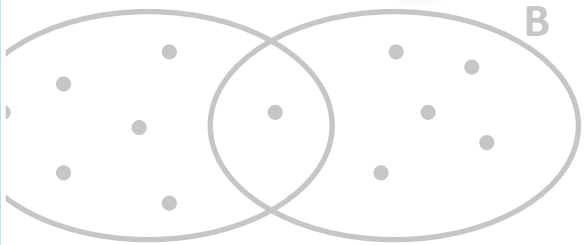
Link Aanval 1

Combineren info fysieke wereld & blockchain kan data lekken
Aanvaller kent identiteit patient & observeert hem fysiek

Voorschrift
Id
Patient
Arts
Medicijn
Geldig vanaf
Verlaagd remgeld?
Mutualiteit
Apotheker
Afgeleverd
Tariferingsdienst



Arts: 02/04/17, 21h30 (A)
Apotheker: 28/04/17, 20h45 (B)



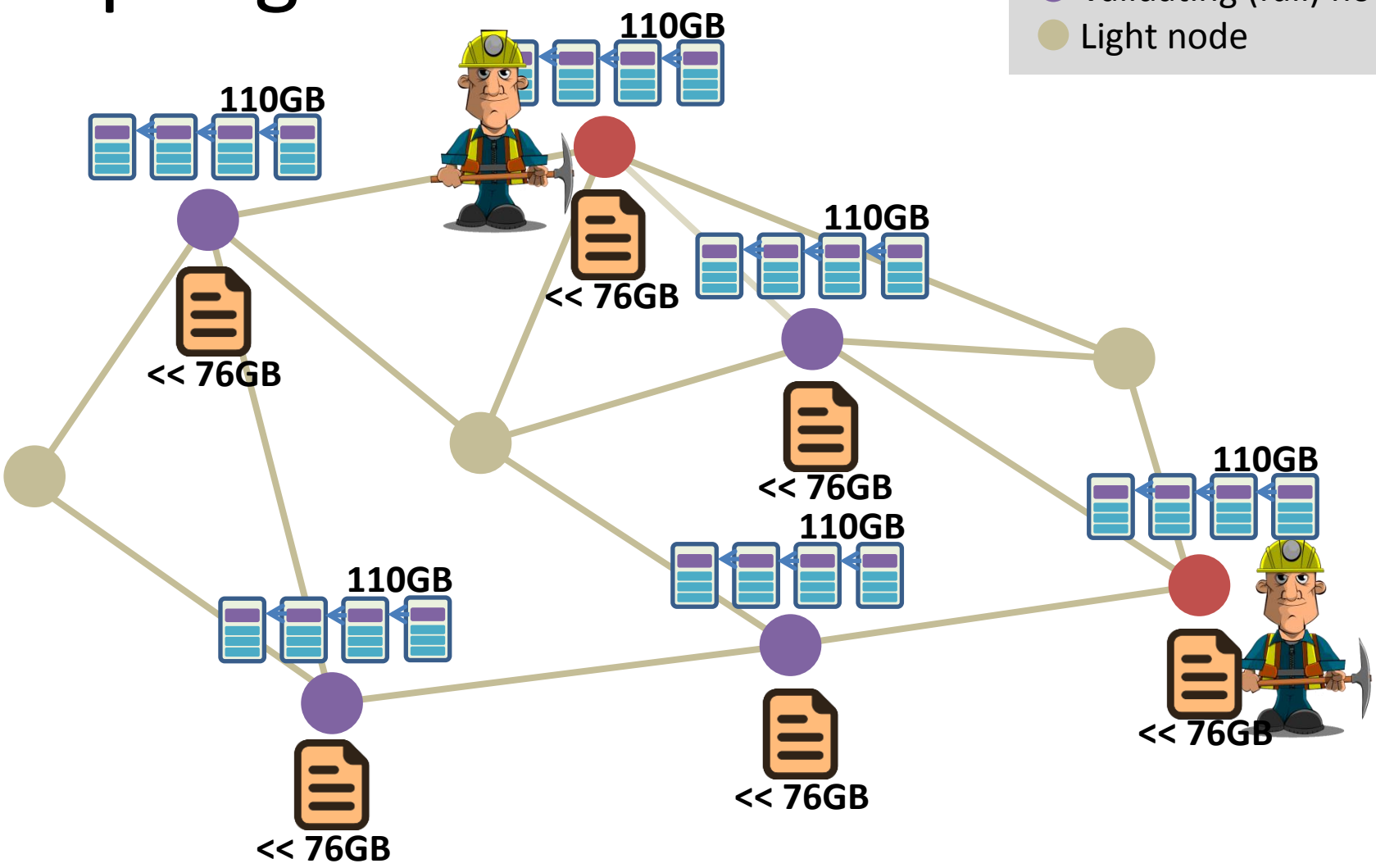
Moeilijke aanval, maar één succesvolle genoeg om project te torpederen

→ All gevoelige data op blockchain geëncrypteerd

Verschillende views

=> fine grained access control m.b.v. encryptie

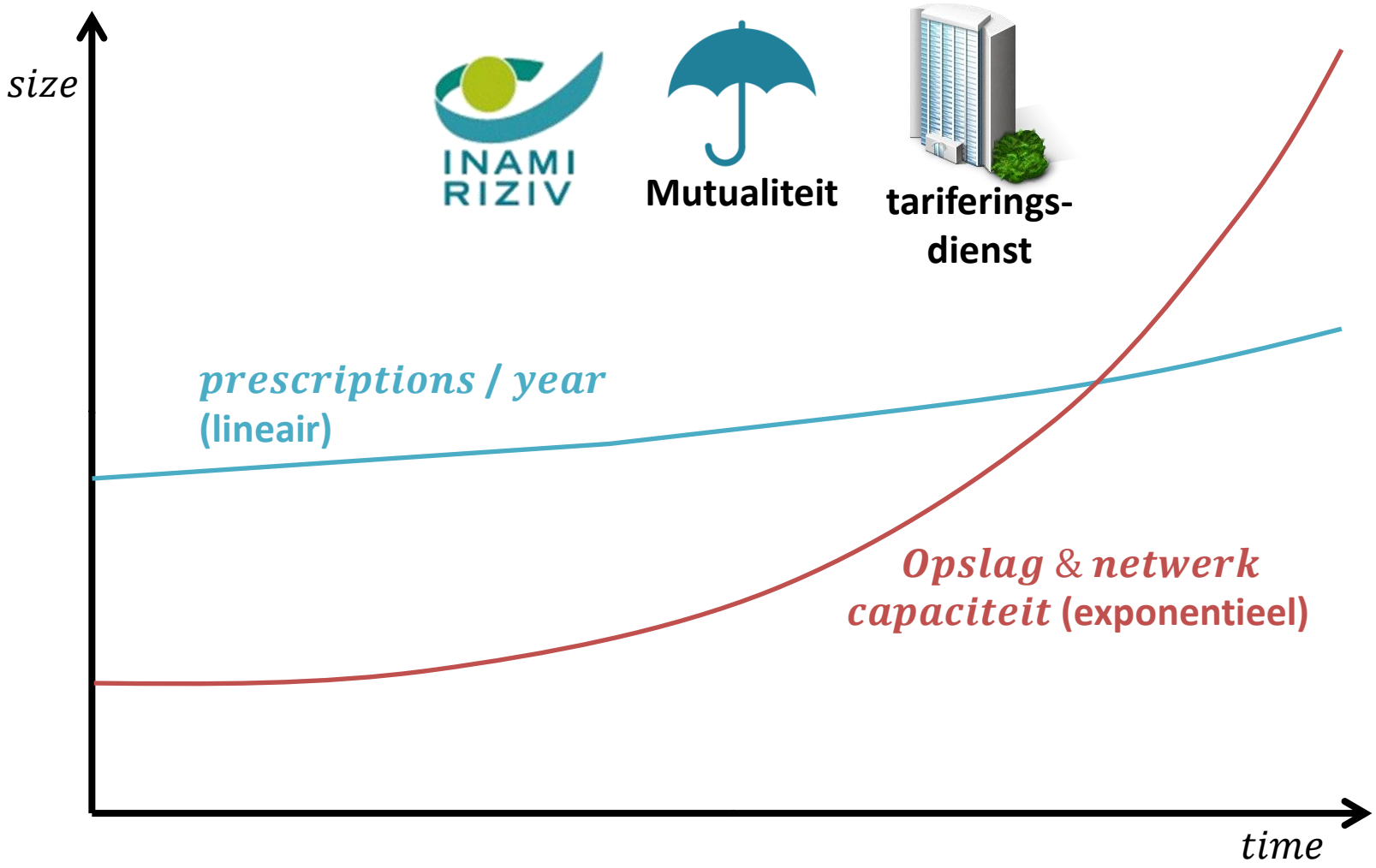
Opslag



Indien voorschriften max. 1 jaar geldig, kunnen transacties ouder dan een jaar weg.

Enkel RIZIV, Mutualiteiten en tariferingsdiensten hebben volledige kopie nodig van blockchain.

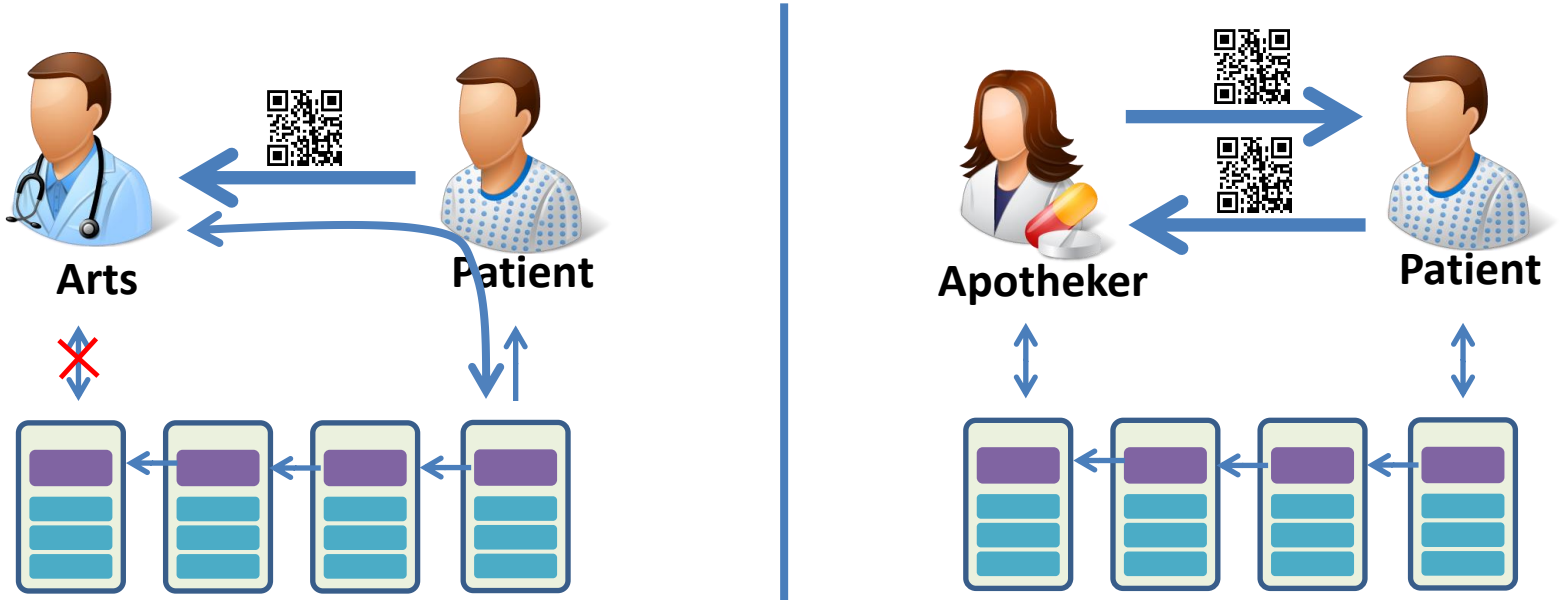
Blockchain Grootte



Mettertijd wordt de blockchain grootte minder een issue

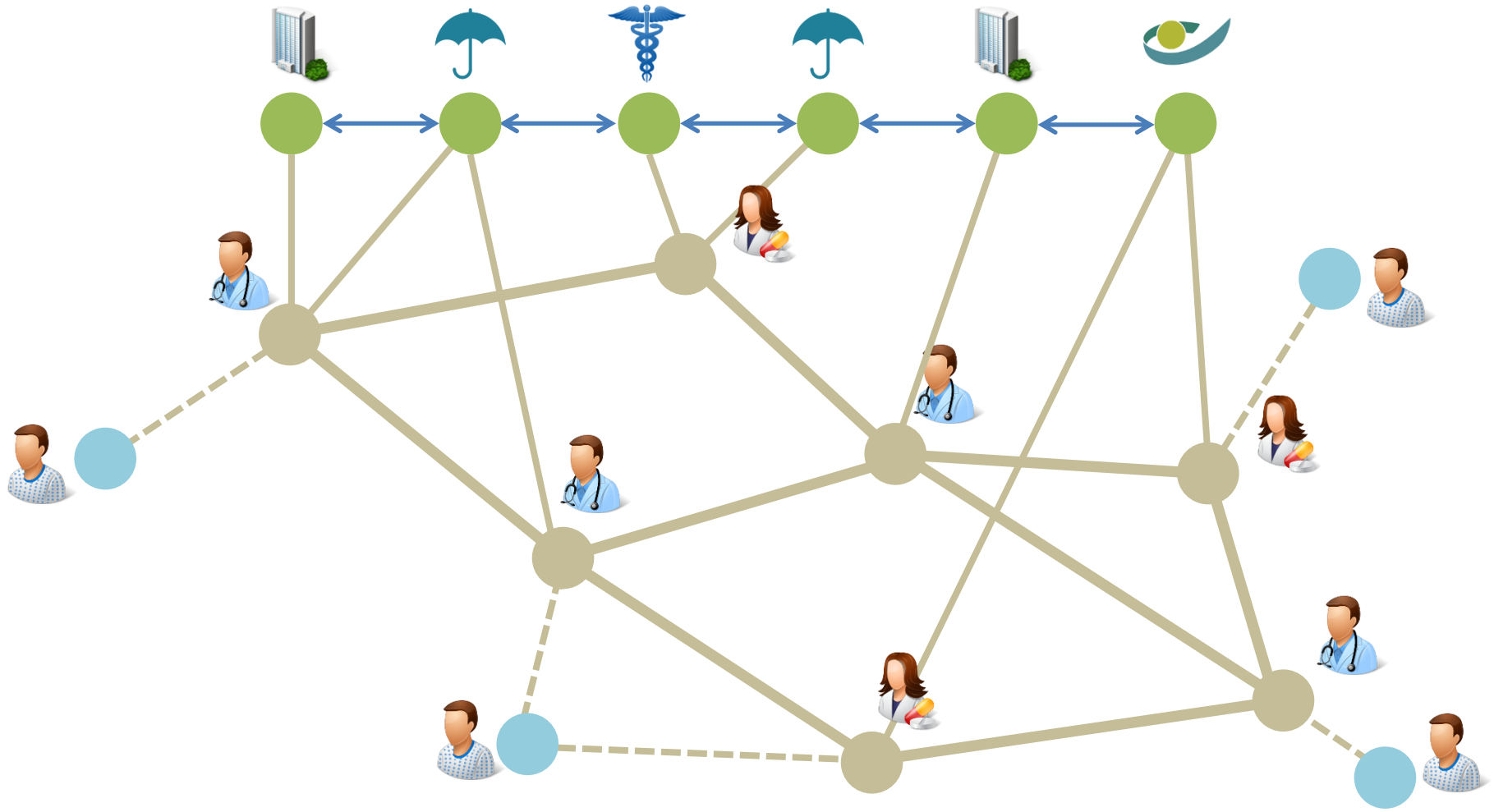
Geen Internettoegang…

Normaal: Beide partijen internettoegang
Transacties gepubliceerd op blockchain klein (<250 bytes)



Eén van beide partijen geen internet?
De andere partij plaatst transactie op blockchain
=> Gratis redundantie

e-Voorschrift Blockchain Netwerk



- Permanent, validating node
- Frequent node
- Occasional node

Blokcreatie

Door RIZIV, mutualiteiten en/of tariferingsdiensten

Vb 1. Enkel RIZIV → Hoge blokfreqentie

Vb 2. Handtekening door 3 van de 7 mutualiteiten

Proof of Concept

Platform

ethereum

Smart contract

solidity

Web Clients

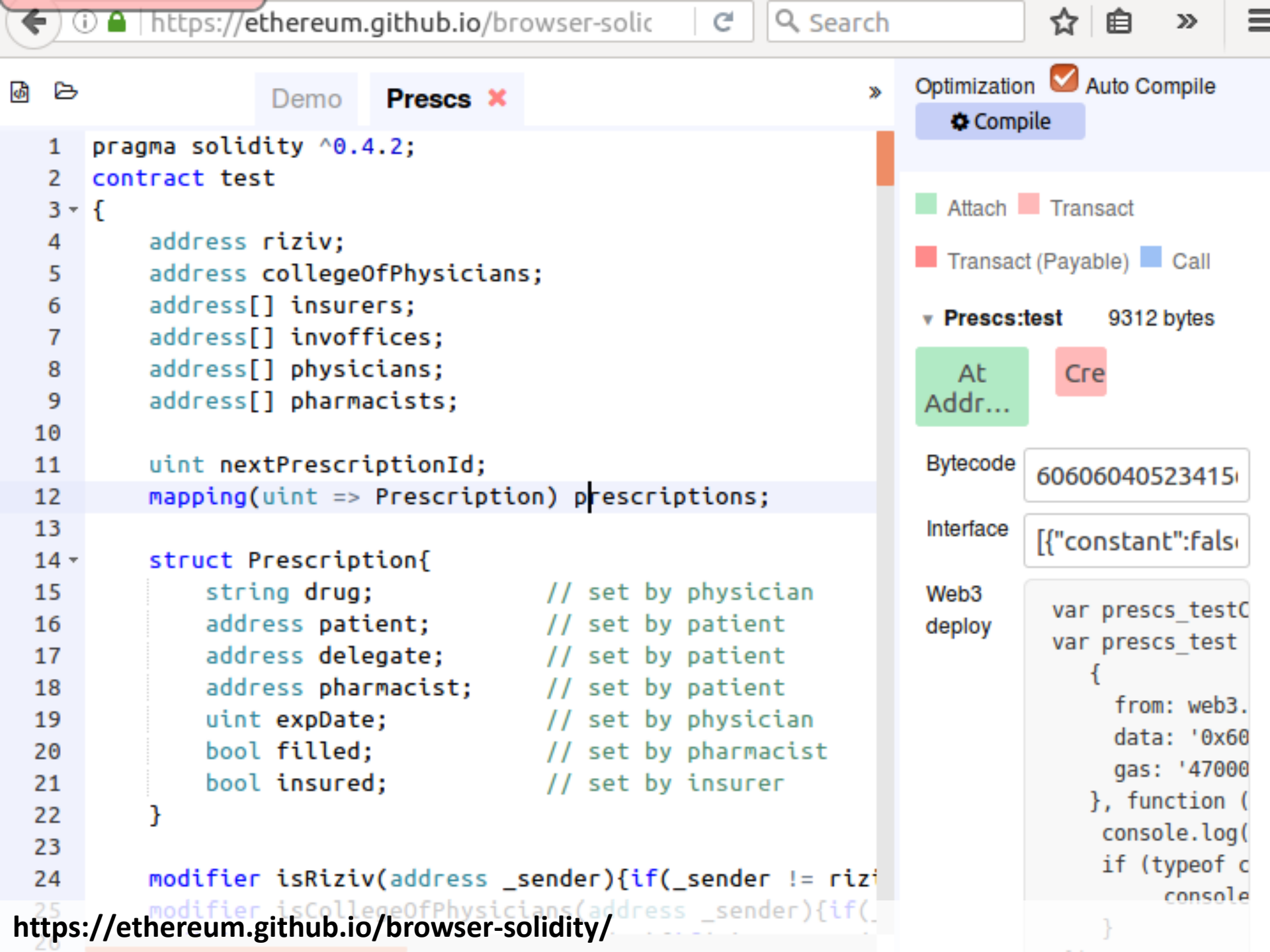
JavaScript

php

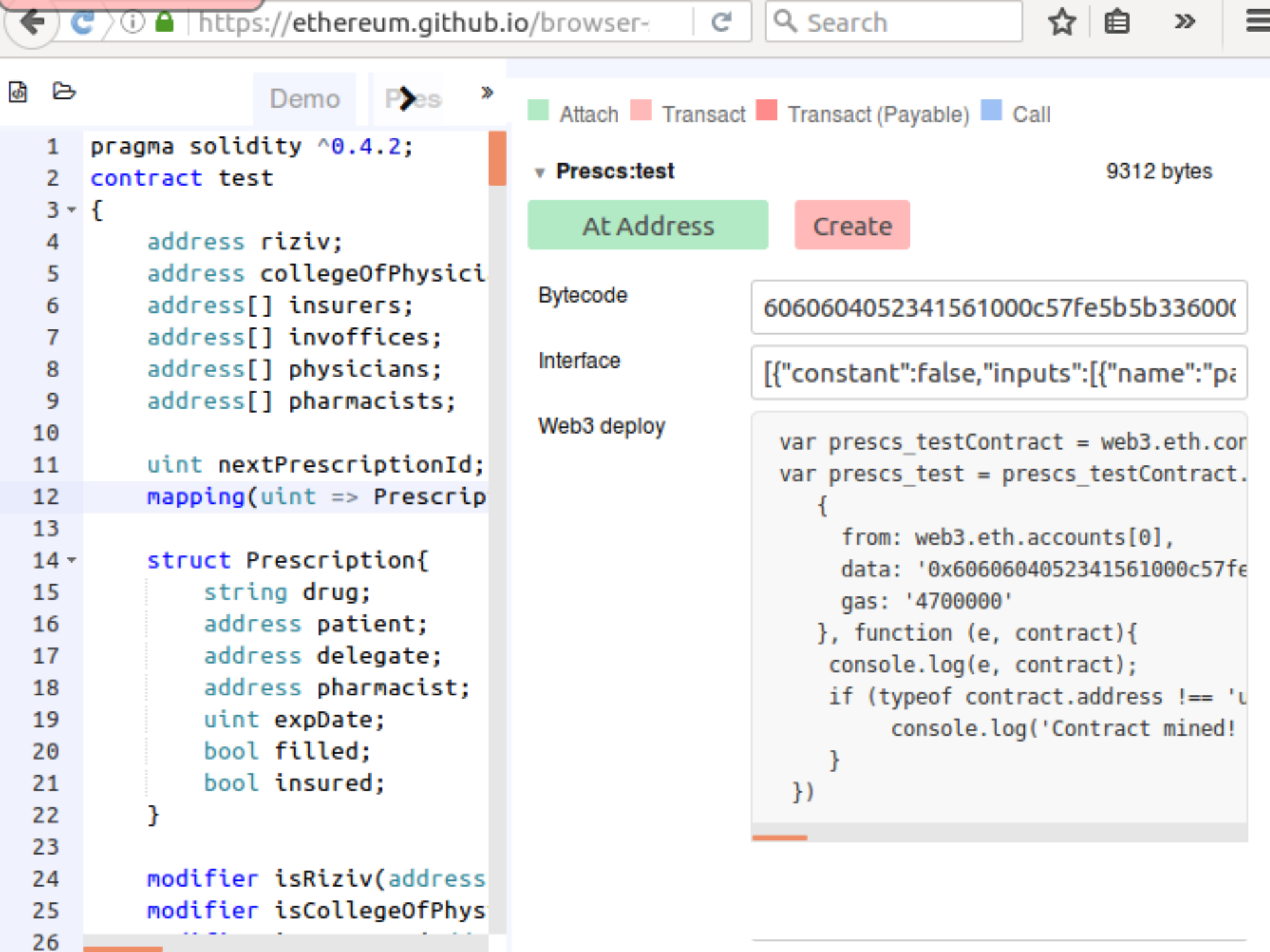
Virtuele Machines

App (Light client)

Op moment van ontwikkeling nog geen Ethereum light client (smart phone)



https://ethereum.github.io/browser-solidity/

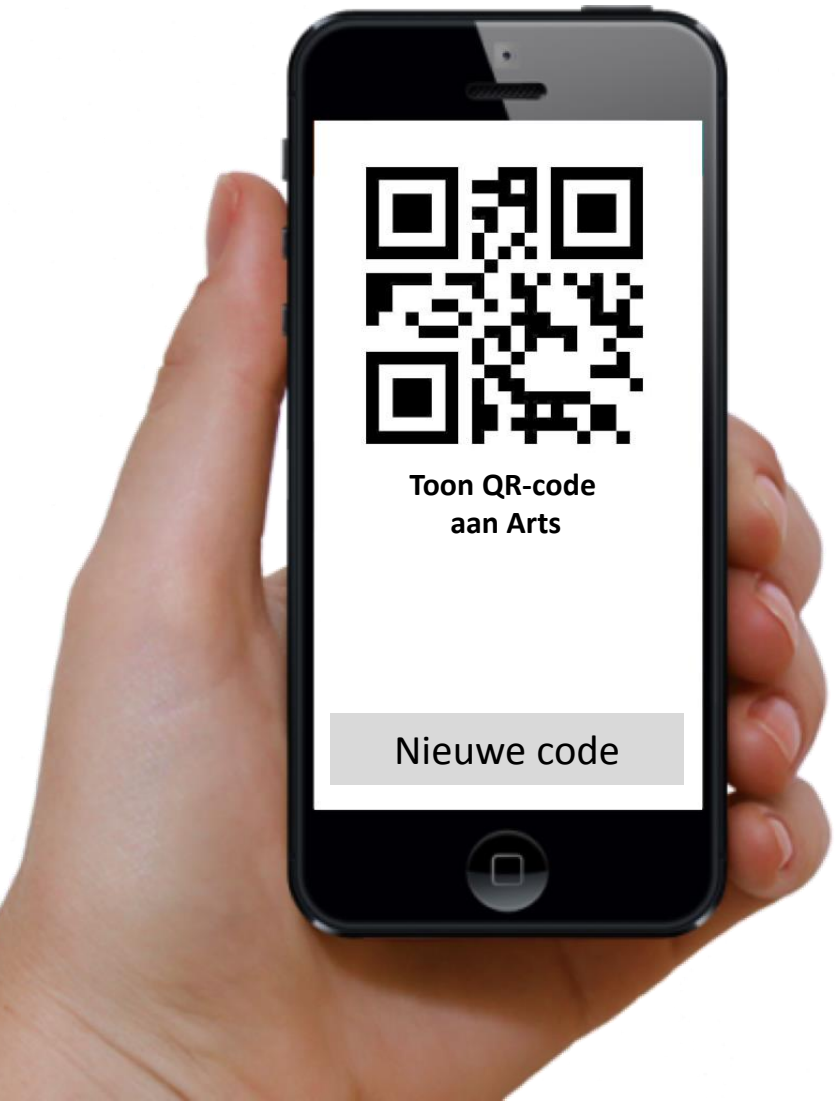

https://ethereum.github.io/browser-
Search
Demo
Attach
Transact
Transact (Payable)
Call
Prescs:test
9312 bytes
At Address
Create
Bytecode
Interface
Web3 deploy
pragma solidity ^0.4.2;
contract test
{
address riziv;
address collegeOfPhysici
address[] insurers;
address[] invoffices;
address[] physicians;
address[] pharmacists;
uint nextPrescriptionId;
mapping(uint => Prescrip
struct Prescription{
string drug;
address patient;
address delegate;
address pharmacist;
uint expDate;
bool filled;
bool insured;
}
modifier isRiziv(address
modifier isCollegeOfPhys
var prescs_testContract = web3.eth.cor
var prescs_test = prescs_testContract.
{
from: web3.eth.accounts[0],
data: '0x6060604052341561000c57fe
gas: '4700000'
}, function (e, contract){
console.log(e, contract);
if (typeof contract.address !== 'u
console.log('Contract mined!
}
})

Interface

Oproep functie in contract

Observatie event

Interface



Arts

Interface


Mijn voorschriften
Ontvang
Consumeer
Nieuw Voorschrift
Etanercept 1mg

Interface

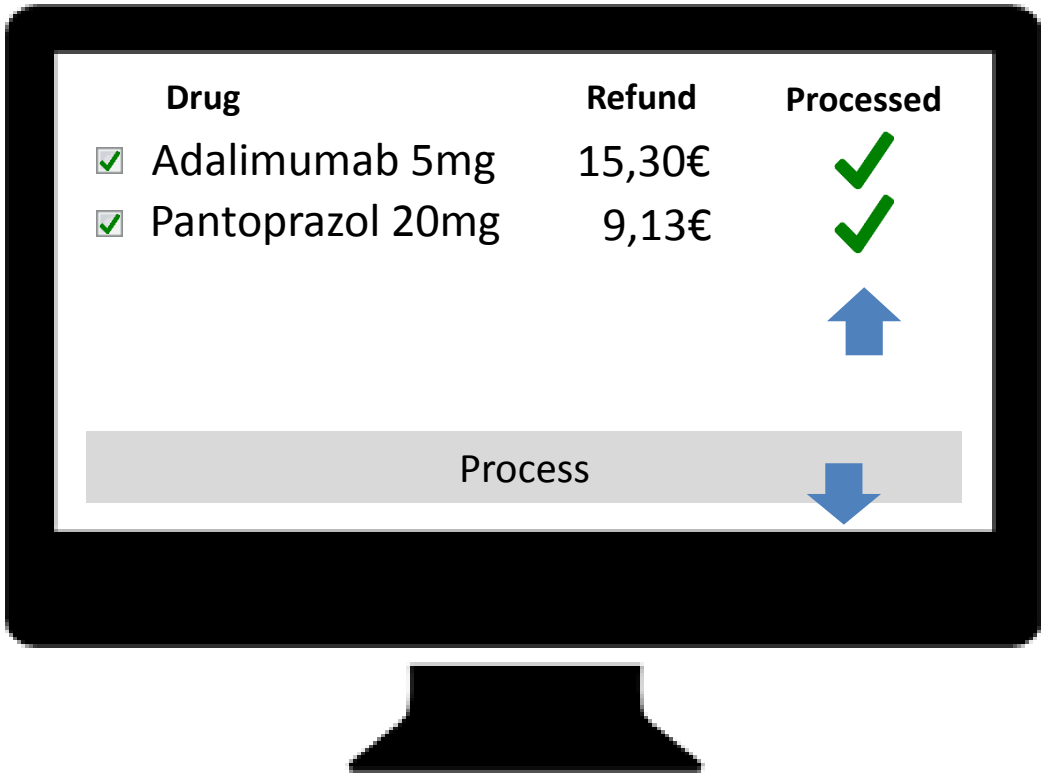
Interface


Mijn voorschriften
Adalimumab 5mg
Adalimumab 5mg
Pantoprazol 20mg
Etanercept 1mg

Interface - Dispense

Apotheker

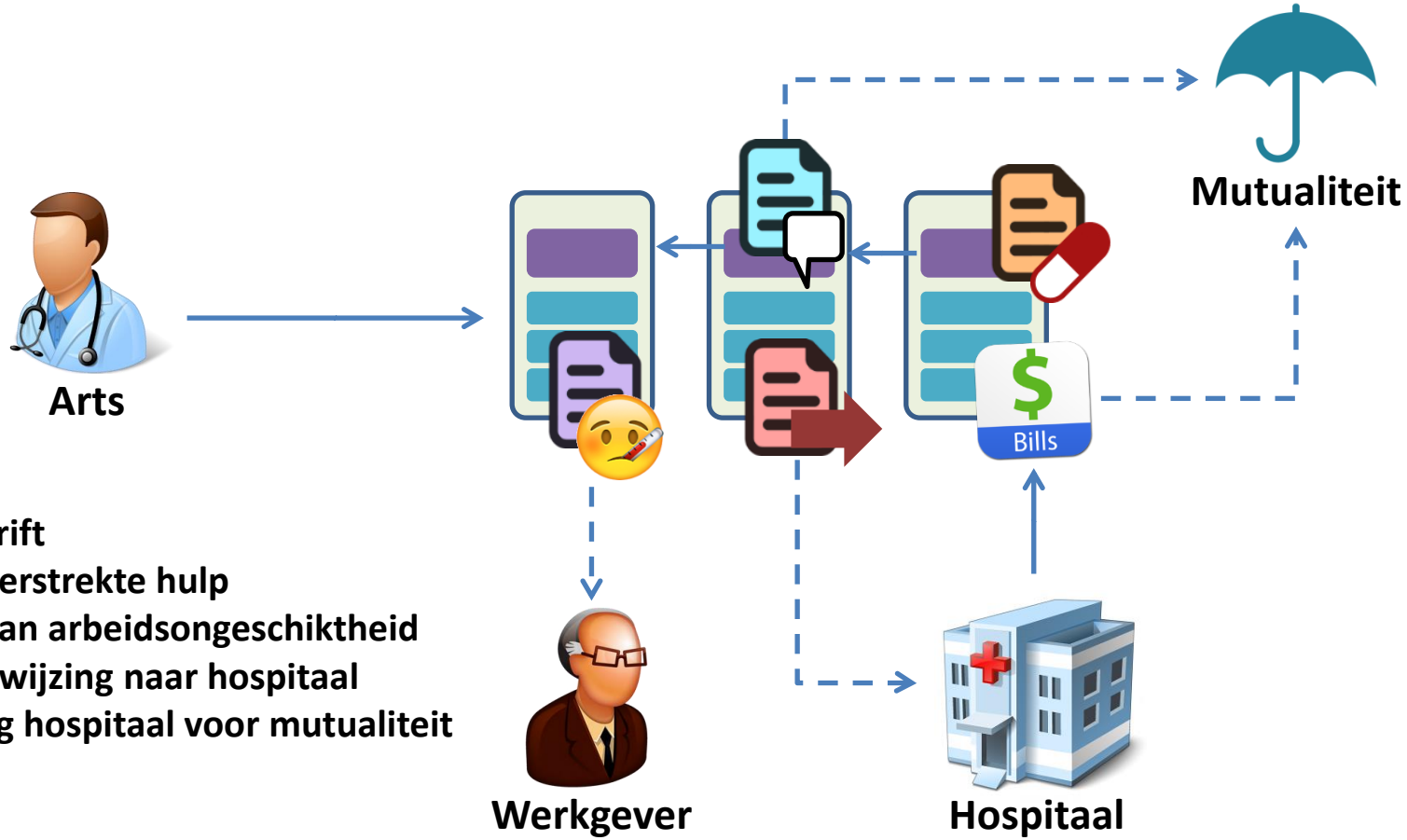
Interface - Dispense



Interface - Dispense

The bigger picture

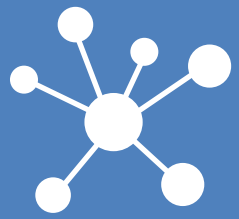
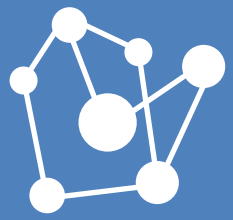
Een Blockchain Ecosysteem



Voorschrift
Bewijs verstrekte hulp
Bewijs van arbeidsongeschiktheid
Doorverwijzing naar hospitaal
Rekening hospitaal voor mutualiteit
…

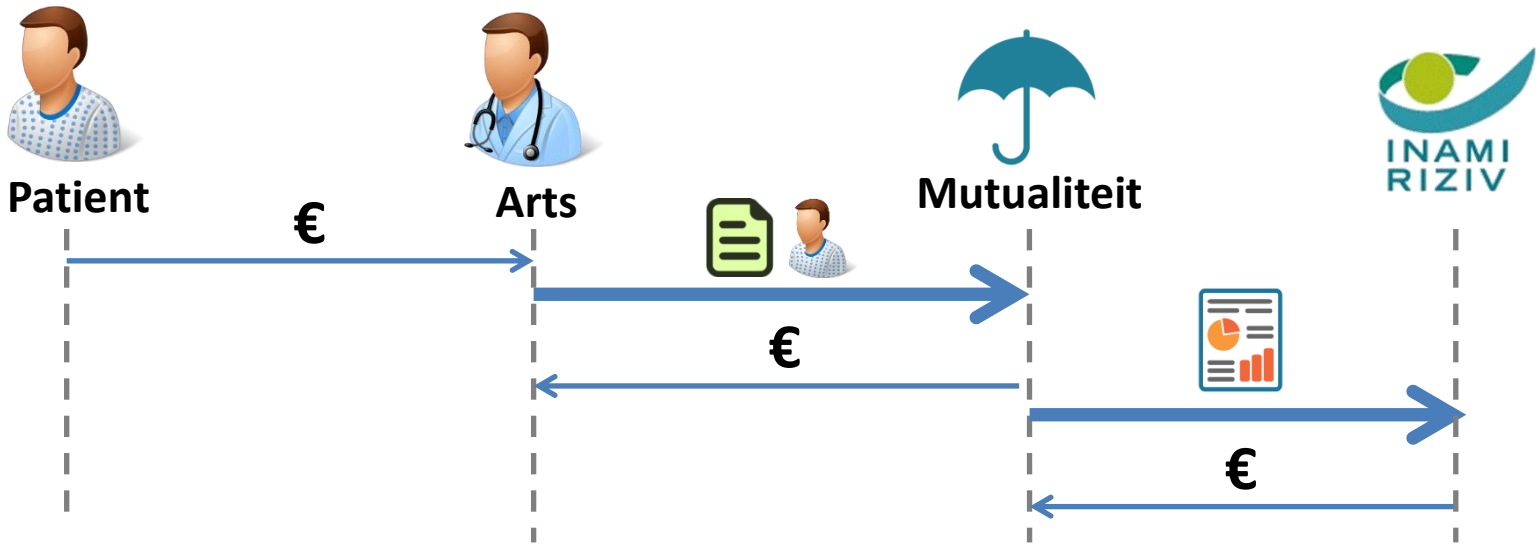
Eén medische consultatie kan een hele set acties in gang zetten, met blockchain als centrale as.

Vergelijking

	Gecentraliseerd	Gedecentraliseerd	Smart Contract
			
Vertrouwen in entiteiten	**Hoog**	**Medium**	**Laag**
Complexe fluxen	**Nee**	**Ja**	**Nee**
PKI vereist	**Altijd**	**Altijd**	**Enkel bij registratie**
Risico inconsistenties	**Laag**	**Hoog**	**Laag**
Hoge beschikbaarheid	**Ja**	**Ja**	**Ja / Nee**
Sleutelbeheer	**Medium**	**Medium**	**Complex**
Opslag & transfer	**Laag**	**Medium**	**Hoog**

Een blockchain benadering heeft meerwaarde

Sociale Derdebetaler



Probleem: Arts kan onbestaande consultaties aangeven
→ moeilijk detecteerbare fraude

Oplossing

- Arts plaatst op moment van consultatie aangifte op blockchain → timestamped, onweerlegbaar
- RIZIV analyseert in real-time (leert geen identifiers)
- Verdacht → record in patientendossier? (met mutualiteit)
- [Optioneel] Notificatie op smartphone patient
- [Optioneel] Medewerking patient vereist bij creatie aangifte

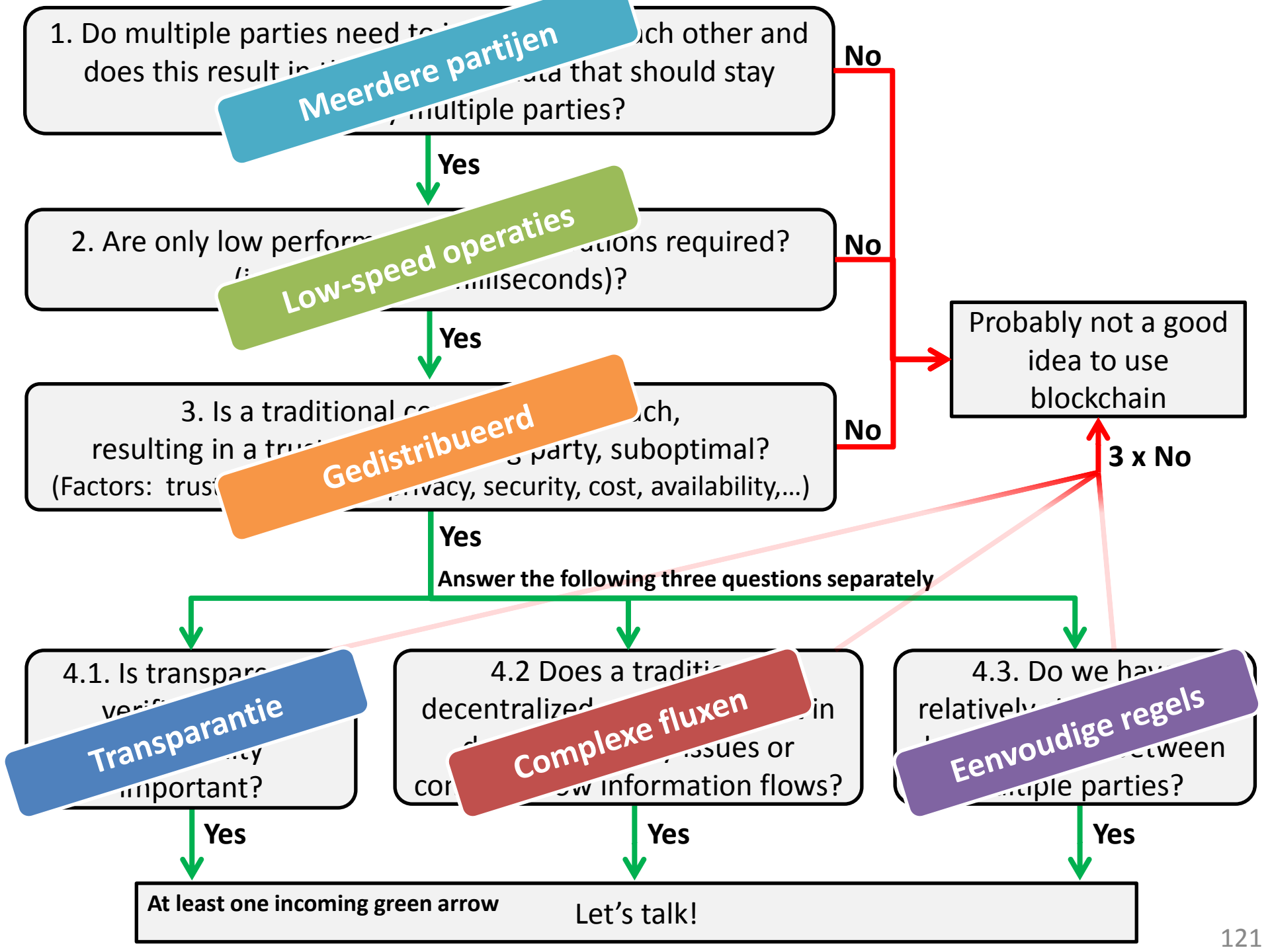
Lessen & Conclusies

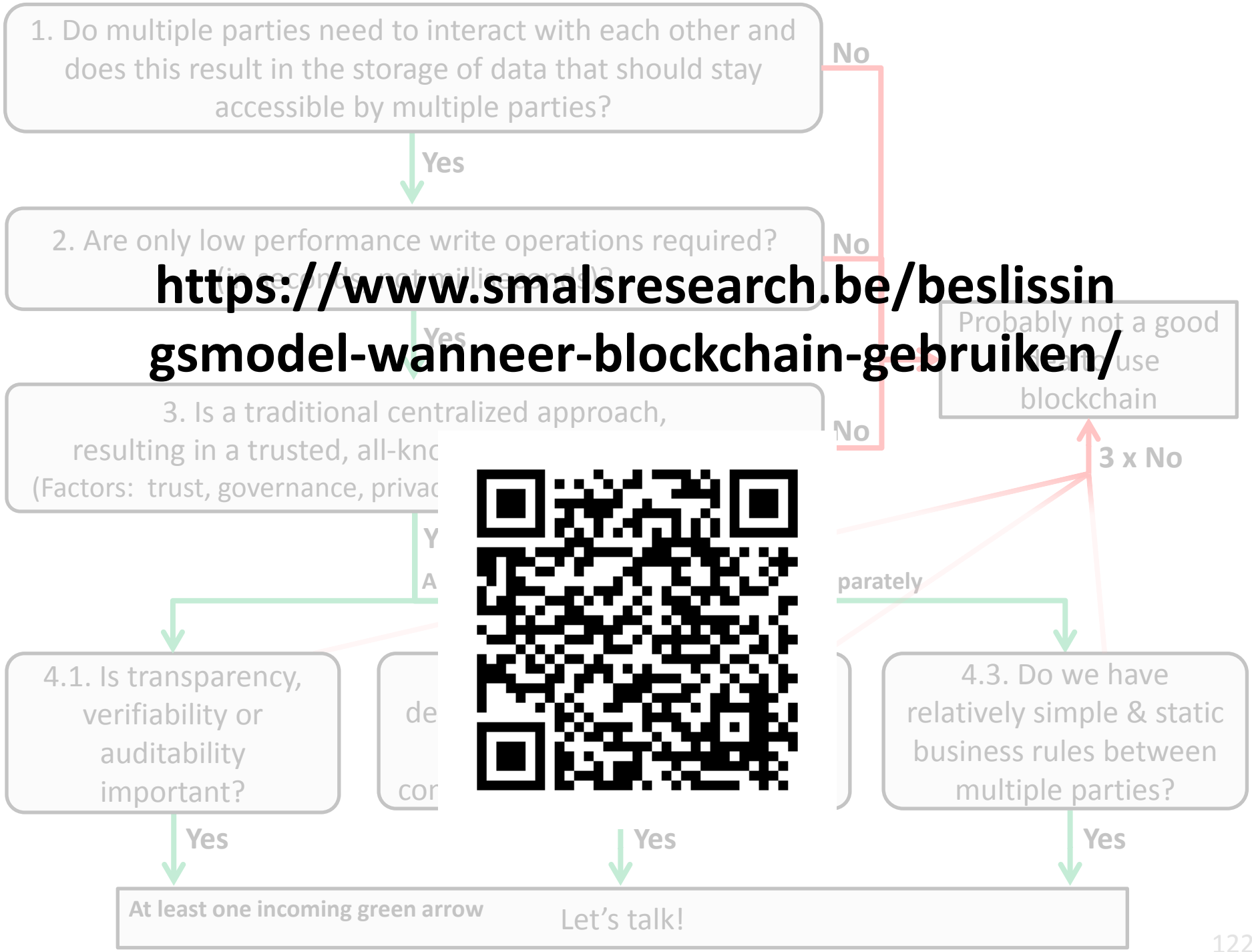
Nauwgezette case by case analyse onontbeerlijk

- Privacy burgers
- Confidentialiteit bedrijfsgegevens
- Fine-grained access control
- Fallback
- Schaal-baarheid

Nog steeds centrale partij vereist, maar vertrouwen erin sterk gereduceerd

Blockchain kan toegevoegde waarde hebben!
Maar wanneer wel? En wanneer niet?
=> blockchain beslissingsmodel (volgende slide)


1. Do multiple parties need to
ch other and
does this result in
ata that should stay
multiple parties?
Meerdere partijen
No
Yes
2. Are only low perform
ations required?
(i
milliseconds)?
Low-speed operaties
No
Yes
3. Is a traditional c
ch,
resulting in a trus
party, suboptimal?
(Factors: trust
rivacy, security, cost, availability,…)
Gedistribueerd
No
Probably not a good idea to use blockchain
3 x No
Yes
Answer the following three questions separately
4.1. Is transpar
verif
important?
Transparantie
4.2 Does a traditi
decentralized
in
issues or
cor
w information flows?
Complexe fluxen
4.3. Do we hav
relatively
tween
ltiple parties?
Eenvoudige regels
Yes
Yes
Yes
At least one incoming green arrow
Let's talk!



https://www.smalsresearch.be/beslissingsmodel-wanneer-blockchain-gebruiken/

Afronding

Smals
ICT for society

Blockchain 1.0

Pauze

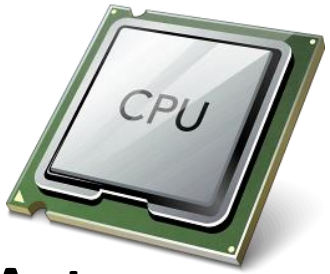
Blockchain 2.0

Mentaal Model

Blockchain 1.0

Autonome opslag

Blockchain 2.0



Autonome rekenkracht

Autonome computer

Niemand kan opgeslagen data wijzigen of uitvoering code beïnvloeden (Maar iedereen kan de data zien)

Correcte werking, zelfs met oneerlijke en/of onbeschikbare nodes

Conclusies

Nieuw paradigma

- Nieuwe manier van denken, organiseren & communiceren
- Terughoudendheid & aanpassingspijnen

Geen oplossing voor alles

- Het kan met blockchain ≠ Blockchain is de beste keuze
- Vaak evident van ver, maar soms verre van evident

Uitdagingen

- Schaalbaarheid, sleutelbeheer, privacy, confidentialiteit, silo's, …
- Veel onderzoek (MIT, KU Leuven, TU Delft, IBM, …)

Blockchain & smart contracts voor de overheid

- Denk na over cases, discussieer, experimenteer, piloot?
- Voorbereidingen voor productie-ready systemen

Publicaties op **www.smalsresearch.be**

Blogpost

Blockchain, het kloppend hart van Bitcoin

Februari 2016

Presentatie

Blockchain & Smart Contract

Maart 2017

Blogpost

Smart Contracts – Autonome code op een blockchain

Oktober 2016

Rapport

Medische voorschriften op een publieke blockchain

Binnenkort

Blogpost

Beslissingsmodel: Wanneer blockchain gebruiken?

Januari 2017

…

Kristof Verslype

02 787 53 76

kristof.verslype@smals.be

@KristofVerslype

be.linkedin.com/in/verslype

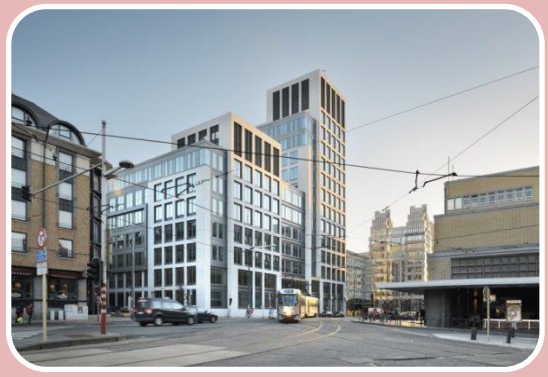
Smals

www.smals.be

@Smals_ICT

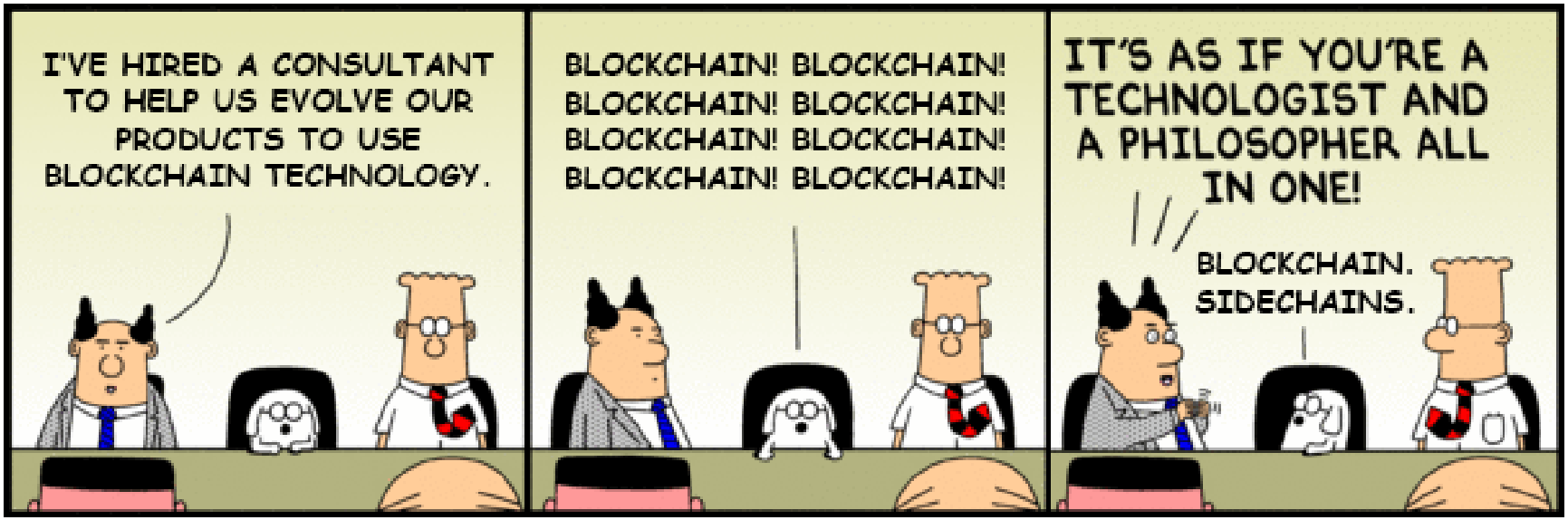
www.smalsresearch.be

@SmalsResearch



Dilbert


I THINK WE SHOULD BUILD A BLOCKCHAIN
UH-OH
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM.
S. Adams E-mail: SCOTTADAMS@AOL.COM
© 1995 United Feature Syndicate, Inc.(NYC)


I'VE HIRED A CONSULTANT TO HELP US EVOLVE OUR PRODUCTS TO USE BLOCKCHAIN TECHNOLOGY.
BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN!
IT'S AS IF YOU'RE A TECHNOLOGIST AND A PHILOSOPHER ALL IN ONE!
BLOCKCHAIN. SIDECHAINS.

Referenties

- Nakamoto Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2009 https://bitcoin.org/bitcoin.pdf
- Arvind Narayanan, Joseph Bonneau, Edward W. Felten, Andrew Miller, Steven Goldfeder. **Bitcoin and Cryptocurrency Technologies**. 2016 http://bitcoinbook.cs.princeton.edu/
- Fleder, Michael, Michael S. Kester, and Sudeep Pillai. MIT. **Bitcoin transaction graph analysis**. arXiv preprint arXiv:1502.01657 (2015). https://people.csail.mit.edu/spillai/data/papers/bitcoin-transaction-graph-analysis.pdf
- Patrick McCorry, Siamak F. Shahandashti and Feng Hao. **A Smart Contract for Boardroom Voting with Maximum Voter Privacy.** 2017. https://eprint.iacr.org/2017/110.pdf
- World Economic Forum. **Deep Shift Technology Tipping Points and Societal Impact.** 2015 http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf#page=24
- Peter Kelly-Detwiler, Forbes. **Mining Bitcoins Is A Surprisingly Energy-Intensive Endeavor**. 2016 http://www.forbes.com/sites/peterdetwiler/2016/07/21/mining-bitcoins-is-a-surprisingly-energy-intensive-endeavor
- Kristof Verslype, Smals Research. **Blockchain, het kloppend hart van Bitcoin.** 2016. https://www.smalsresearch.be/blockchain-het-kloppend-hart-van-bitcoin/
- Kristof Verslype, Smals Research. **Smart Contracts – Autonome code op een blockchain.** 2016 https://www.smalsresearch.be/smart-contracts-autonome-code-op-een-blockchain/
- Kristof Verslype, Smals Research. **Beslissingsmodel: Wanneer blockchain gebruiken?** 2017 https://www.smalsresearch.be/beslissingsmodel-wanneer-blockchain-gebruiken/
- blockchainpilots.nl. **Resultaten Blockchainpilots (Nederland)**. November 2016 http://media.wix.com/ugd/df1122_10b215b09d7447ac97fc8a12d21e4b40.pdf
- **Available Solidity Integration**s. 2017. http://solidity.readthedocs.io/en/latest/#available-solidity-integrations