

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 Investerings

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



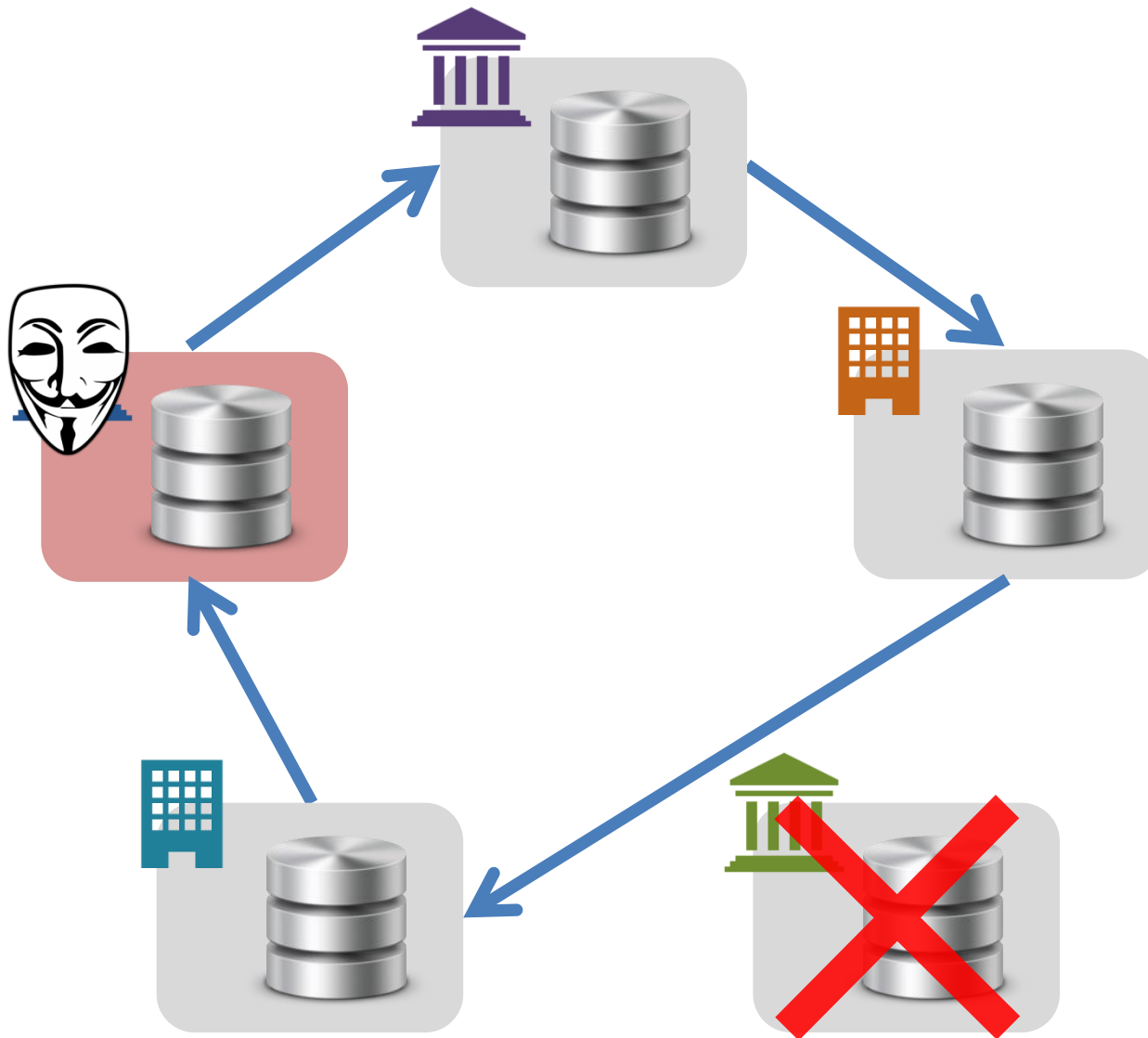
Dan Boneh,
Professor Stanford University
Crypto expert

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

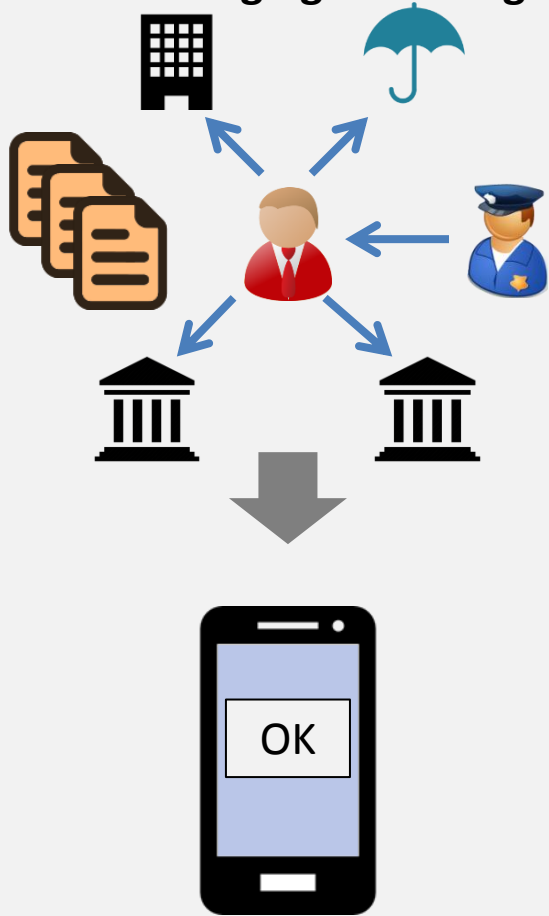
Append-only

Robuust

Schaalbaar

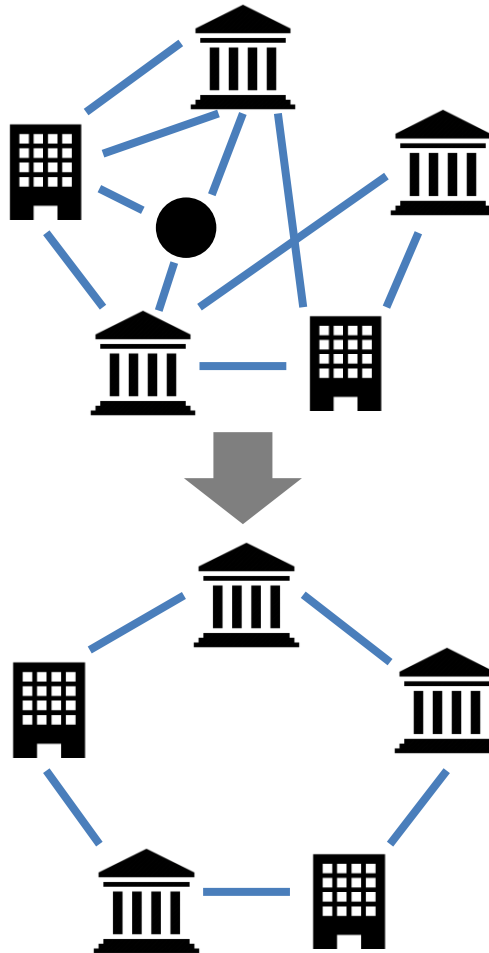
Beter bestuur

Vereenvoudiging voor burger



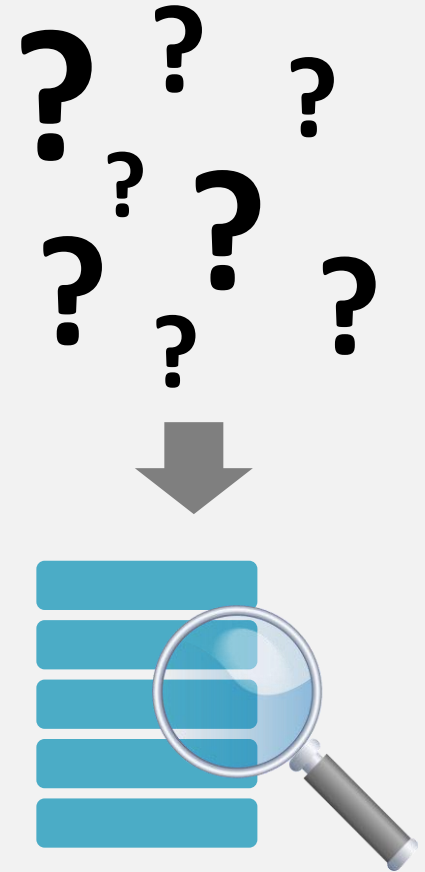
Levensloop

Gestroomlijnde processen



Schuldafhandeling

Transparantie



Voedselveiligheid

Blockchain veelbelovende technologie

Blockchain & overheid



Silo 2.0
Gevaar data verspreid in diverse
geïsoleerde blockchains



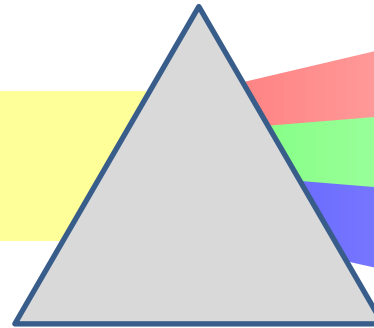
Gecoördineerde aanpak noodzakelijk
om te komen tot blockchain
ecosystemen over instellingen heen

Gemeenschappelijk platform

Gemeenschappelijke visie

Doelstelling sessie

H Y P E



B e p e r k i n g e n

U i t d a g i n g e n

P o t e n t i e e l

Opportunities



Risico's



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

Blockchain & Smart Contracts

Agenda

Blockchain 1.0



Pauze

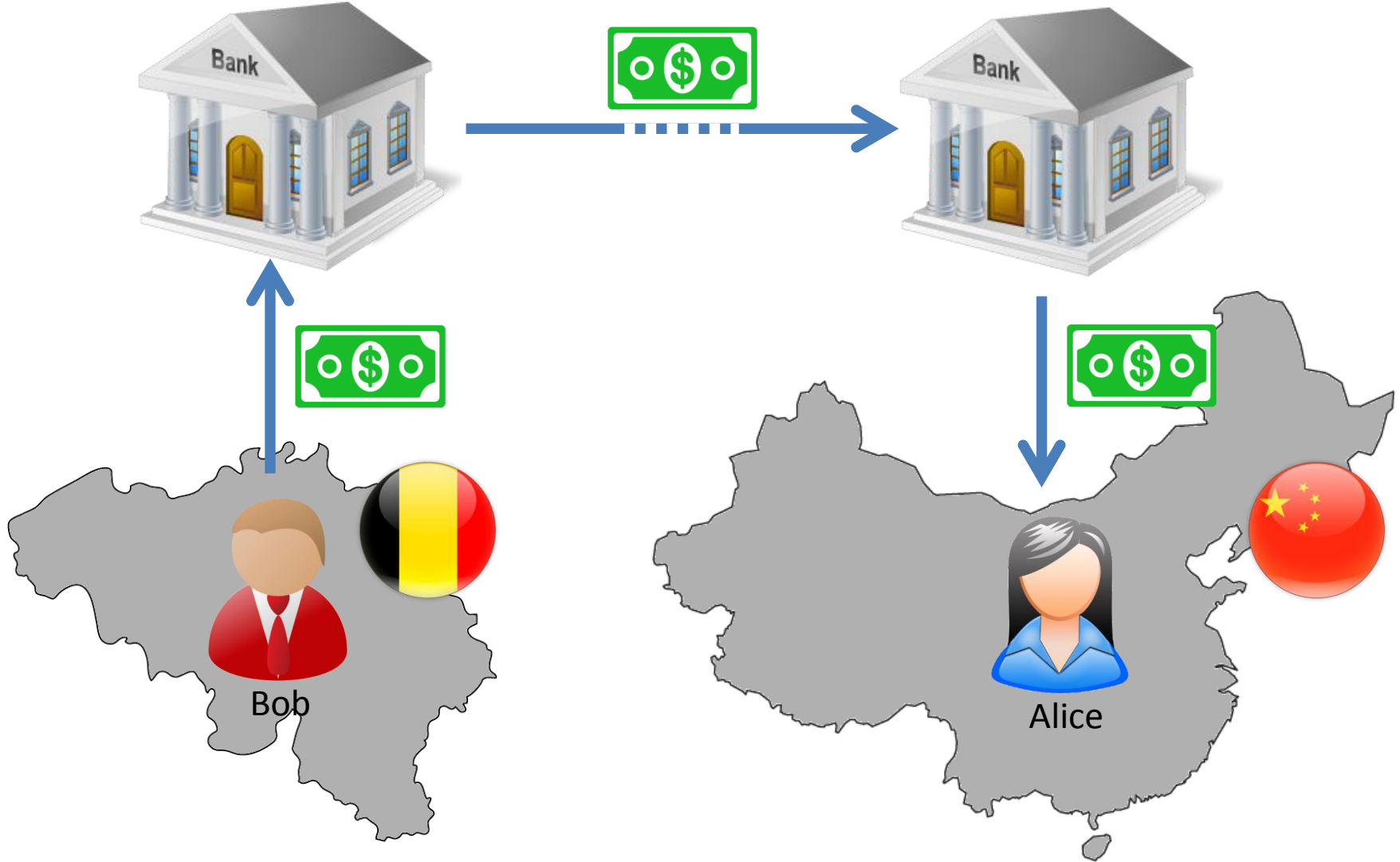
Blockchain 2.0



Bitcoin Blockchain



Traditionele Internationale Transactie



Traditionele Internationale Transactie

Kan dit zonder vertrouwde partijen?



1^e gedistribueerde cryptomunt (2009)

**Schok doorheen de financiële wereld
Financiële wereld veel aandacht voor Bitcoin/Blockchain**

Idee

Ok!



Dave

Transactions

5,1 BTC		→	
0,7 BTC		→	
0,4 BTC		→	

Ik transfereer
0,4 BTC naar .



Bob

0,7 BTC		→	
0,4 BTC		→	

Ok!



Charlie

Transactions

5,1 BTC		→	
0,7 BTC		→	
0,4 BTC		→	

Ok!



Alice

Transactions

5,1 BTC		→	
0,7 BTC		→	
0,4 BTC		→	

Idee

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

Ok!

Ik tra
0,4 BTC



Bob

Transactions

Transactions



Alice

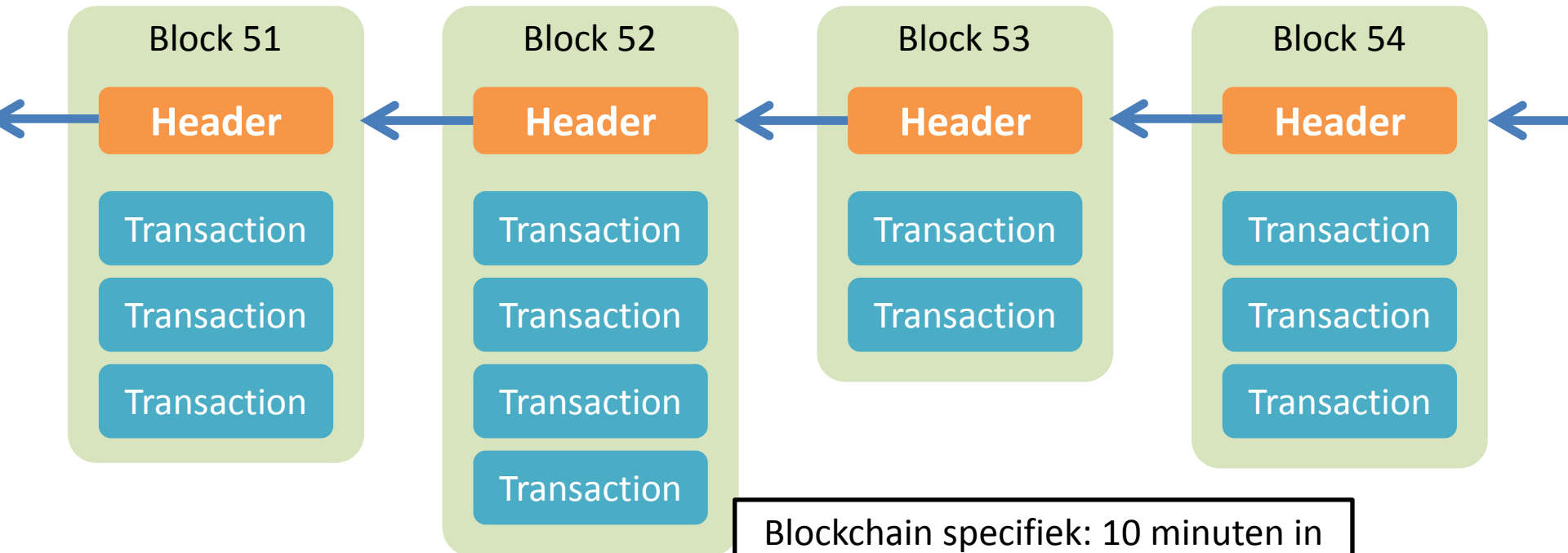
0,7 BTC



0,4 BTC



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

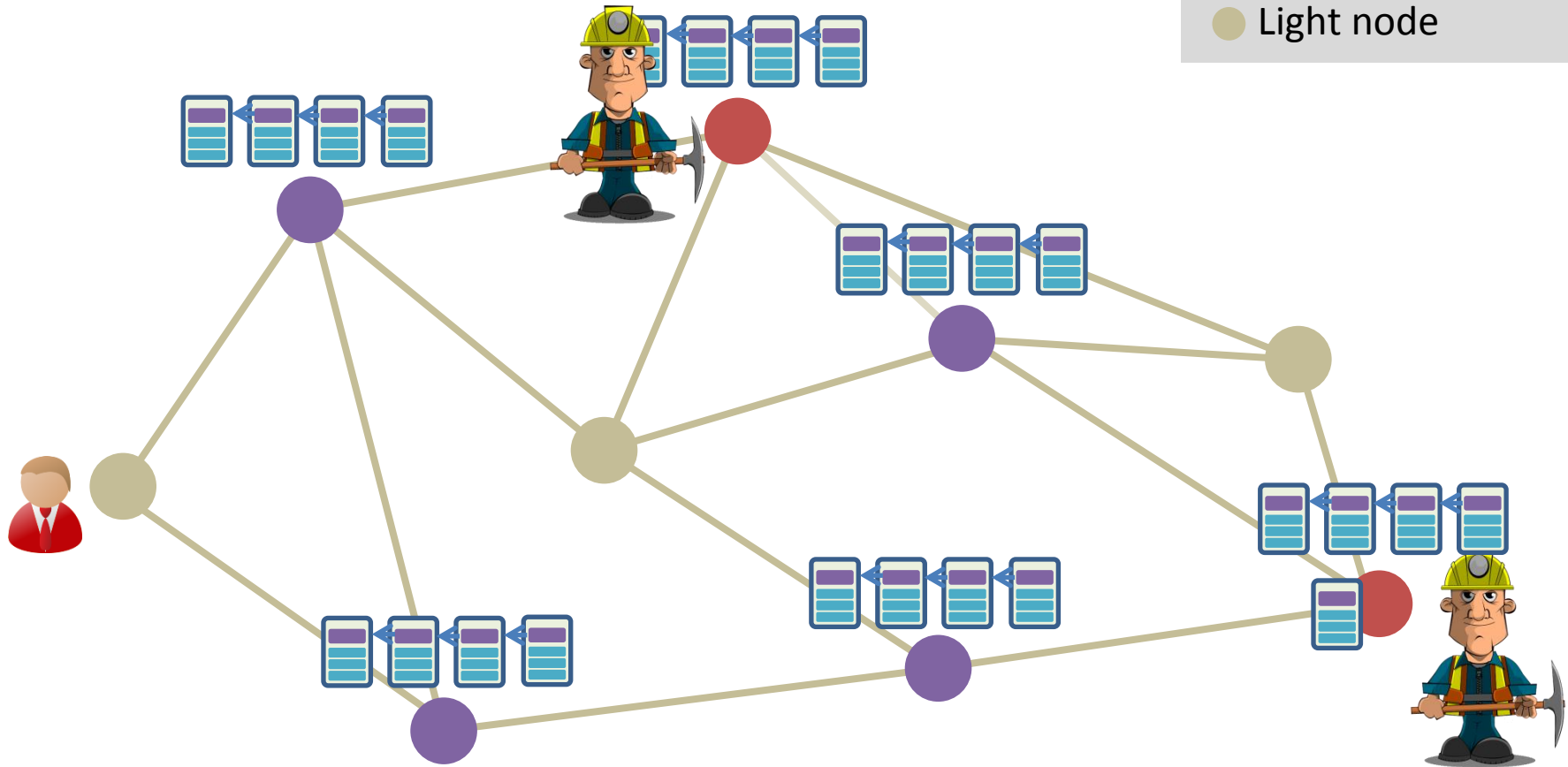
blockchain bevat ALLE transacties

Transactie in blockchain quasi onmogelijk te verwijderen

Vele entiteiten beschikken over dezelfde versie van de blockchain

Network & Consensus

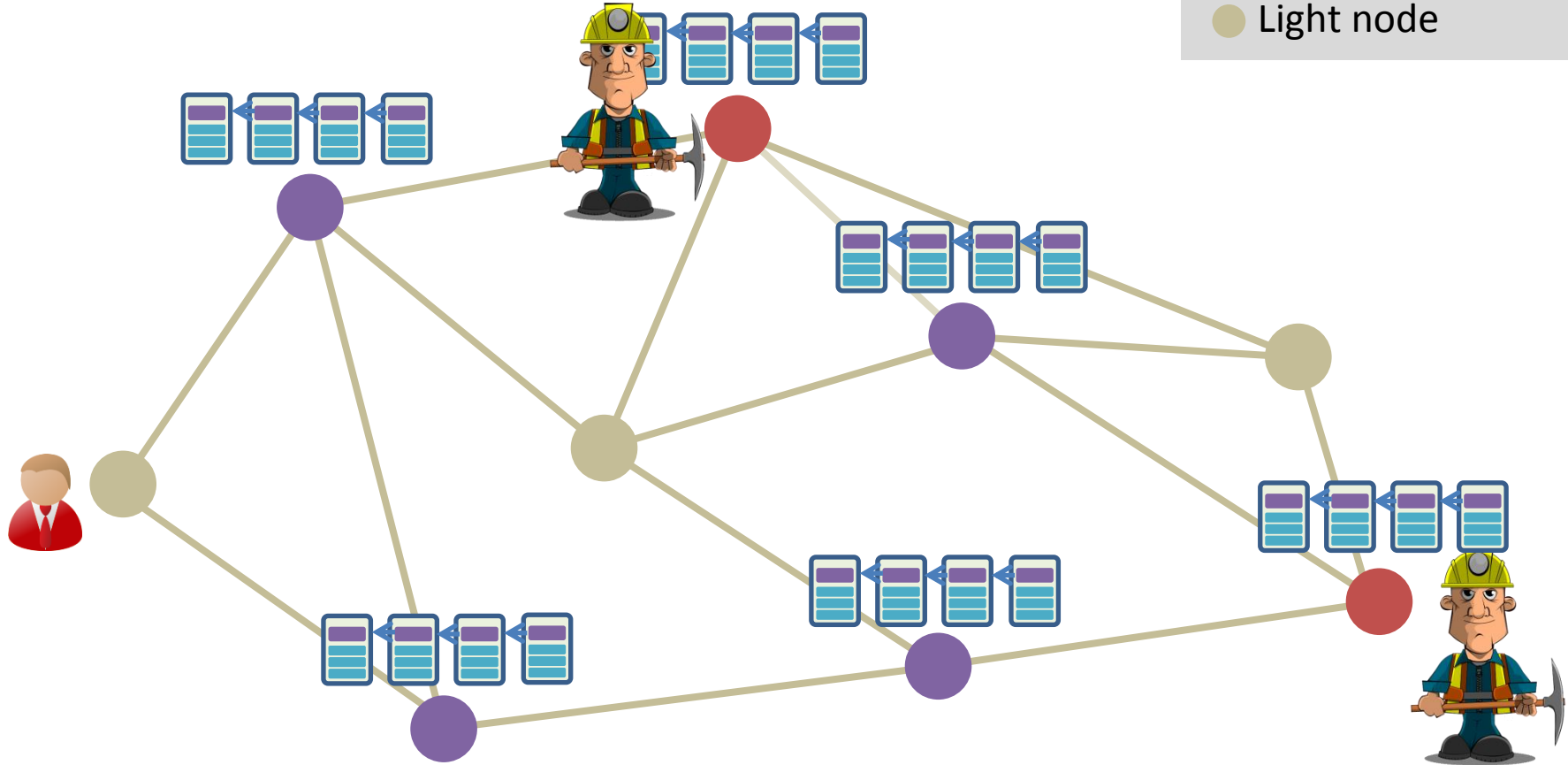
- Miner
- Validating (full) node
- Light node



1. Node creëert transactie en stuurt het naar zijn burens.
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

Network & Consensus

- Miner
- Validating (full) node
- Light node



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")



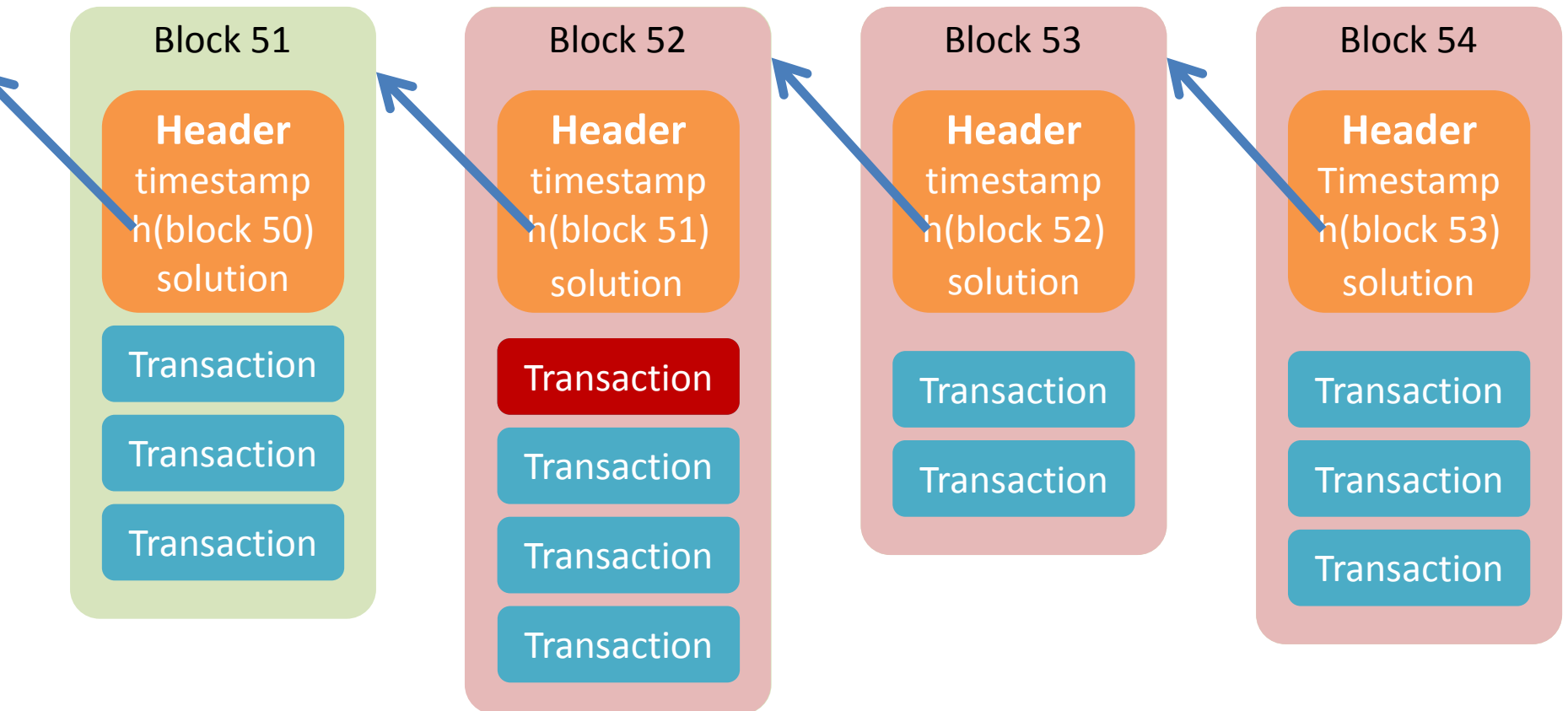
Eén Bitcoin transactie
verbruikt naar schatting
evenveel elektriciteit als
14 382 VISA transacties.

Bron: <http://digiconomist.net/beci>

Bitcoin is niet volledig
gedistribueerd

Bitcoin is erg vervuילend

Veiligheid

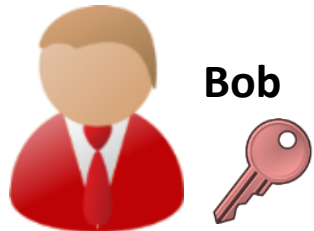


Pas indien nieuwe blockchain langer dan originele -> aanvaard
=> Hoe ouder de transactie, hoe beter beschermd

Pseudoniemen



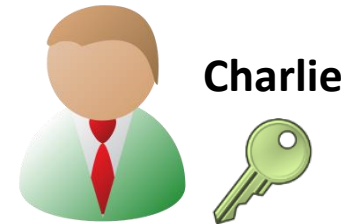
Fysieke wereld



Bob



Alice



Charlie



Bitcoin netwerk



1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX

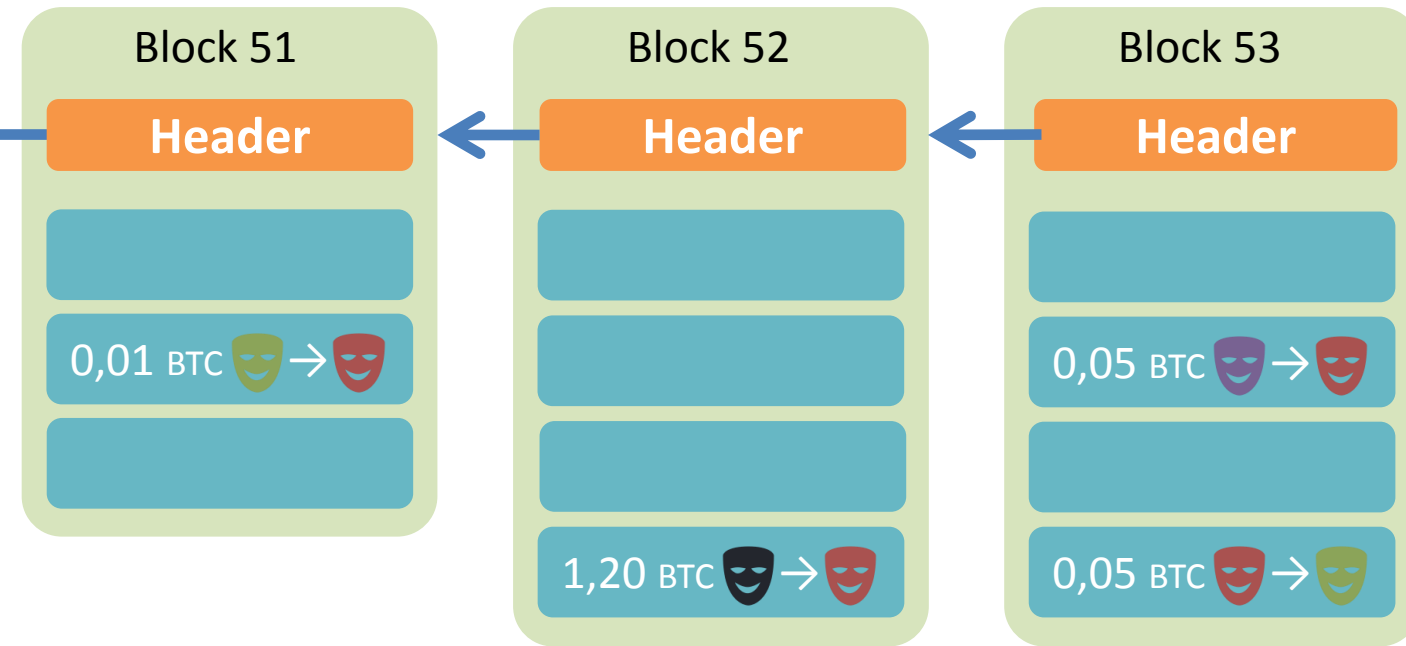


3BcMuv1VJqmwY5Wim8MPAzKAAiAKby9LcN



1Nf311Qb8rLDkWTHrhpmNewZzkcWFYptfc

Transacties (Vereenvoudigd)



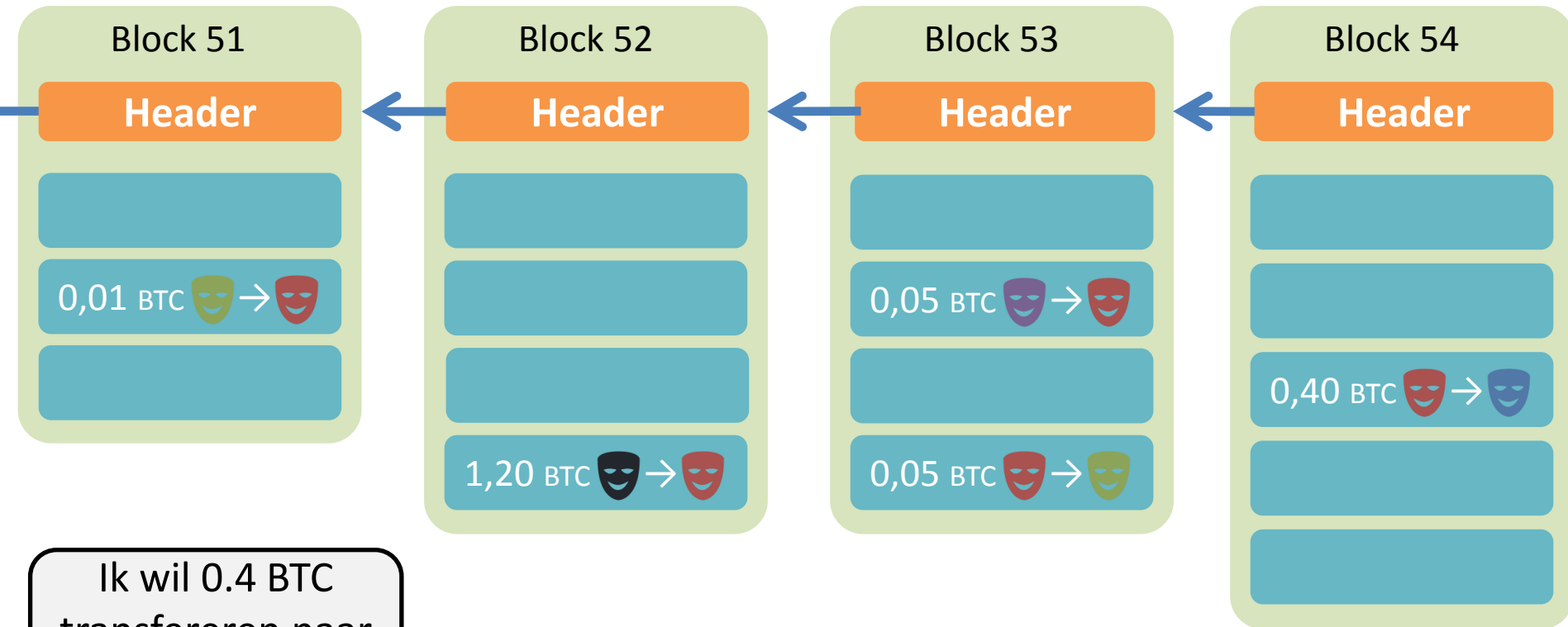
Mijn bitcoins zijn verspreid in de blockchain over meerdere transacties



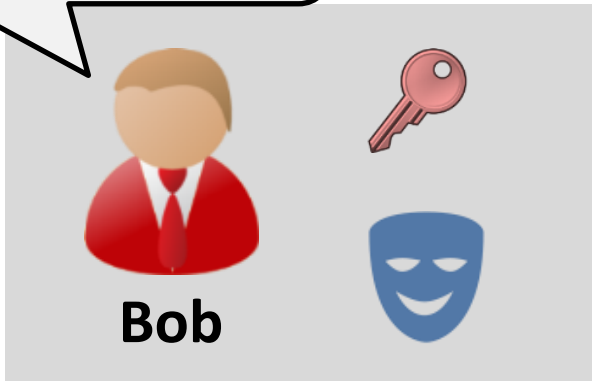
Bob



Transacties (Vereenvoudigd)



Ik wil 0.4 BTC
transfereren naar
Alice

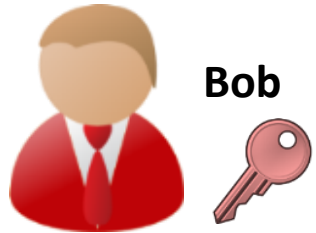


Full nodes verifiëren
op efficiënte manier of
Bob wel over het
nodige geld beschikt.

Pseudoniemen



Fysieke wereld



Bitcoin netwerk



1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX



3BcMuv1VJqmwY5Wim8MPAzKAAiAKby9LcN



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

ACCEPTED HERE



SUBWAY
eat fresh.®

Bitcoin & Anonimiteit



The screenshot shows a forum post interface. On the left, the user profile for 'user98326' is displayed, including a 'Brand new' status, an 'Online' indicator, and a 'Trust: 0: -0 / +0(0)' score. The post title is 'Re: New on here' with a timestamp of 'Today at 11:20:15 PM'. Action buttons for 'quote', 'edit', and 'delete' are visible, along with a post count of '#19'. The post content is a single line: '"I'm new in town, and it gets worse."' followed by a 'Report to moderator' link. Below the post, a Bitcoin transaction is shown with the address 'BTC : 1PFP3mUPhFnoHaebWZM3cFeCSLD7BnaHsA' and a code snippet: '\$bitcoin->sendfrom("1", "1LDNLreKJ6GawBHPgB5yFVLBERi8g3SbQS", 10);'.

user98326
Brand new
Online
Activity: 0
Trust: 0: -0 / +0(0)

Re: New on here
Today at 11:20:15 PM
quote edit delete #19

"I'm new in town, and it gets worse."

Report to moderator

BTC : 1PFP3mUPhFnoHaebWZM3cFeCSLD7BnaHsA

```
$bitcoin->sendfrom("1", "1LDNLreKJ6GawBHPgB5yFVLBERi8g3SbQS", 10);
```

Gebruikers onthullen hun pseudoniem

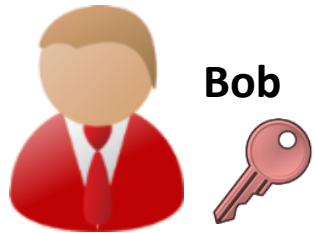
- Op het Internet
 - Aan anderen bij een transactie
- Linken aan persoon / nickname

One-Time Pseudoniemen

Betere privacy



Fysieke wereld



Bob



Alice



Charlie



Bitcoin netwerk



0,4 BTC

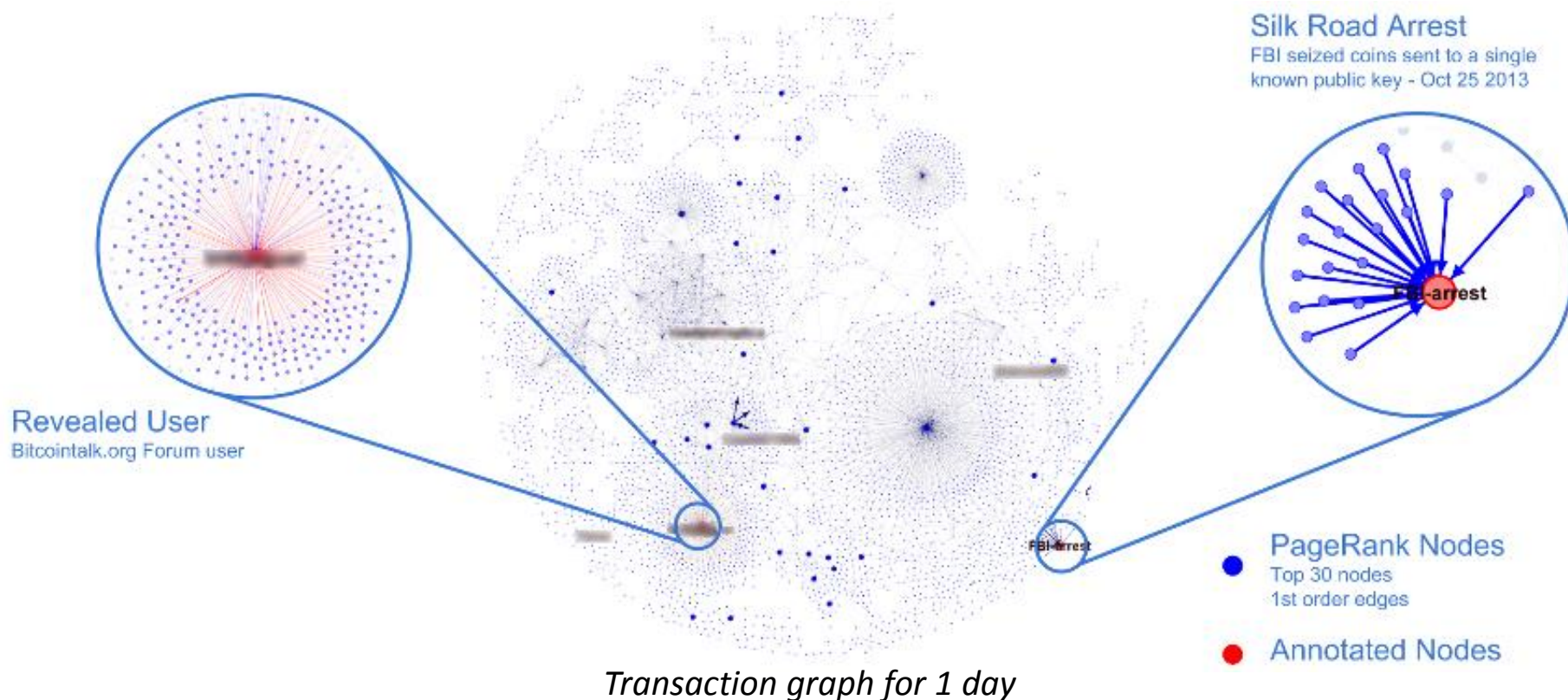


Transaction

0,4 BTC



Bitcoin Anonimiteit



'Geïdentificeerde' personen gelinkt aan

- Silk Road
- Wikileaks
- SatoshiDICE

Bitcoin beschermt slecht
uw privacy

Blockchain.info

Size (kB)

927.97

998.04

Height	Time	Relayed By	Hash
454964 (Main Chain)	2017-02-27 09:21:15	GoGreenLight	00000000000000000b20ef49806f854445f06a7708e78f30d3ffa01da9
454963 (Main Chain)	2017-02-27 09:09:25	BW.COM	000000000000000001e8c35fc00282e12b0a248c1957407e2cf4f2767fe
454962 (Main Chain)	2017-02-27 09:06:25	AntPool	00000000000000000178bf3ee6643f361ec341dc33ddd1959d0470e5cd
454961 (Main Chain)	2017-02-27 08:52:03	SlushPool	00000000000000000024a996b9be8a408fd8189029f5731300207ea92
454960 (Main Chain)	2017-02-27 08:50:45	AntPool	0000000000000000016e802c1c9e9d14b03fa463a52be714b0f714451
454959 (Main Chain)	2017-02-27 08:47:52	ViaBTC	00000000000000000bb1b9dcd6cee5d43e0b2b339d36aba4d8bc20a
454958 (Main Chain)	2017-02-27 08:41:19	AntPool	00000000000000000a8c666c88a64d8207075e9234e1fac623feadcc2
454957 (Main Chain)	2017-02-27 08:39:27	Unknown	00000000000000000208d781c6c4d6d7a185aaa4dfebbc5c971388fb1
454956 (Main Chain)	2017-02-27 08:29:35	AntPool	00000000000000000bda8c59fc2d0e57a35f6728d4d7d730f164a7836
454955 (Main Chain)	2017-02-27 08:11:00	HaoBTC	00000000000000000c5dc465e585e2d6a14333e5a77b5758dcabb2c
454954 (Main Chain)	2017-02-27 08:10:57	AntPool	000000000000000001d0155f281523dd319b6a98a290723754abd5b91

0.2

Bitcoin zit aan
maximumcapaciteit

998.21

Blockchain.info

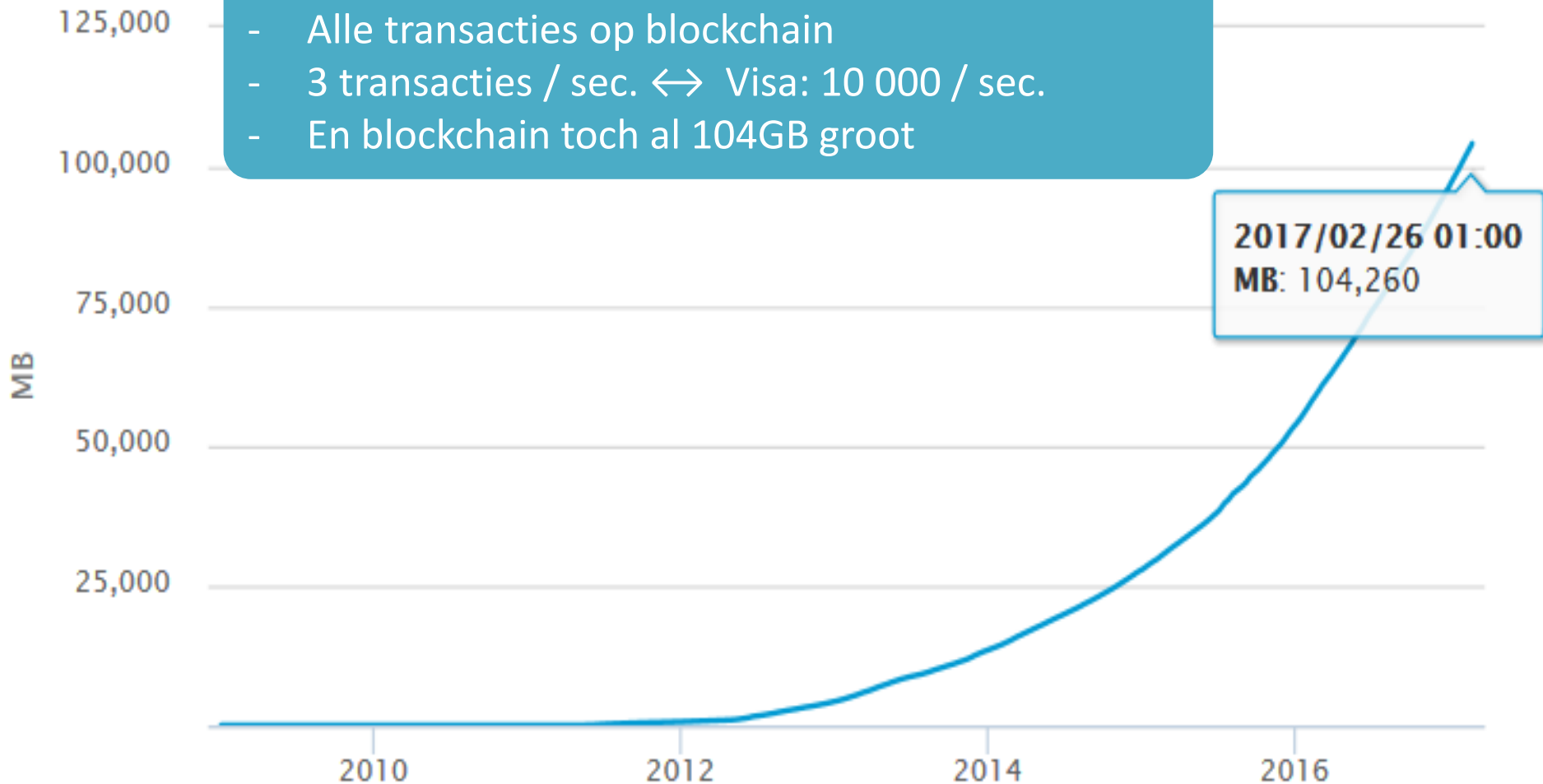
Block #454961

Summary		Hashes	
Number Of Transactions	370	Hash	000000000000000000000024a996b9be8a408fd8189029f5731300207ea92cfc372
Output Total	2,802.2884713 BTC	Previous Block	000000000000000000000016e802c1c9e9d14b03fa463a52be714b0f714451346bc66
Estimated Transaction Volume	365.84939391 BTC		
Transaction Fees	0.28159014 BTC		c0062a16ad514719b69addb3af290be4cc8b606335c73a128515c
Received Time	2017-02-27 08:52:03	Network Propagation	
Relayed By	SlushPool		
Difficulty	440,779,902,286.59		
Bits	402816659		
Size	966.645 KB		
Version	0x20000002		
Block Reward	12.50 BTC		

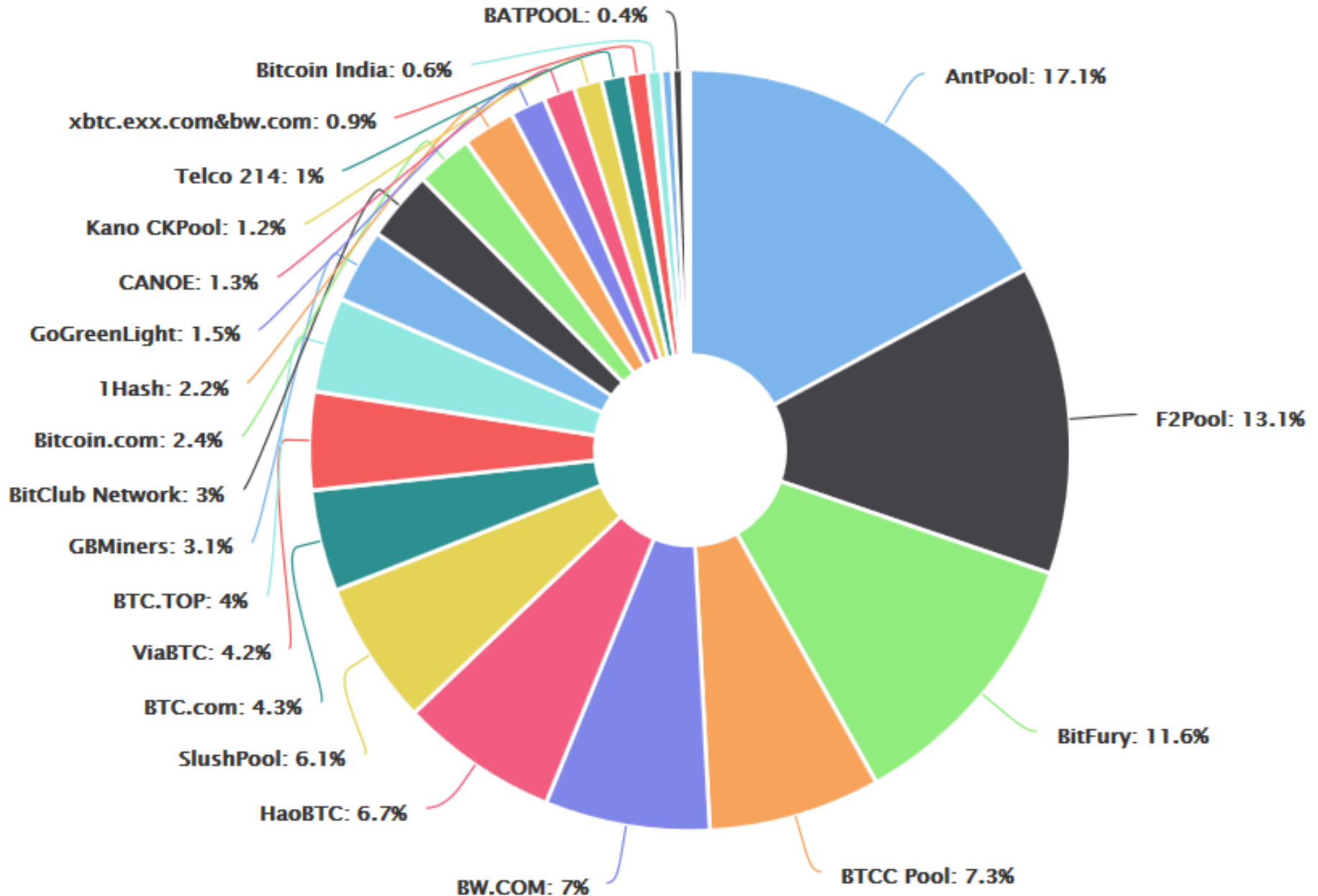
Blockchain.info

Schaalprobleem

- Alle transacties op blockchain
- 3 transacties / sec. $\leftrightarrow$ 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





 Confirm sending
0.0469 BTC
to
1Nuu2753n7h3ZnCQJ
CT2HYKTffQjhpXhew

X 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

Inefficiënt / competitie

Gebruik cryptogeld

Open voor iedereen

Agenda

Blockchain 1.0

Bitcoin



Toepassingen



Pauze

Blockchain 2.0

Smart Contracts



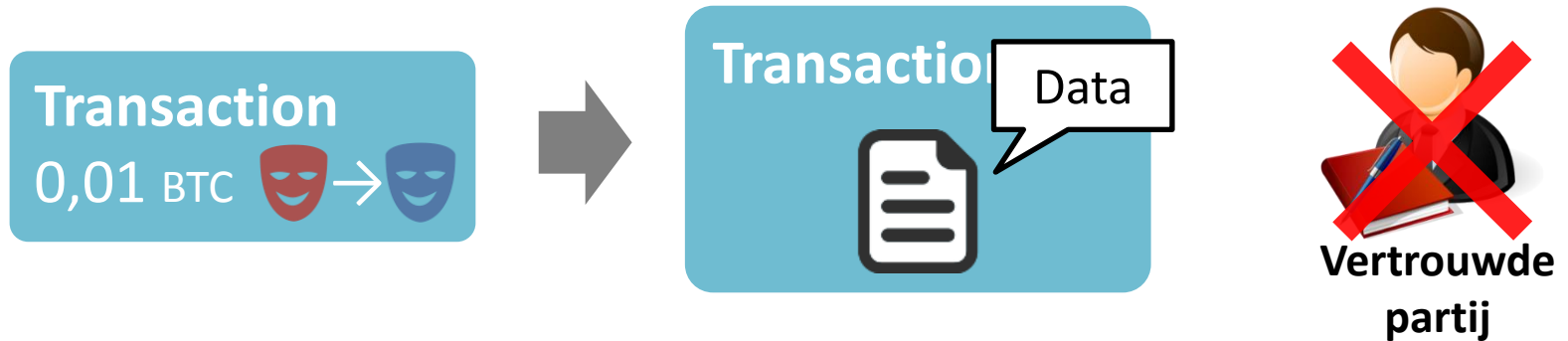
Voorschriften



Blockchain Toepassingen



Data in the Blockchain



Eigenschappen data in blockchain

Onwijzigbaar
(integriteit)

Timestamped

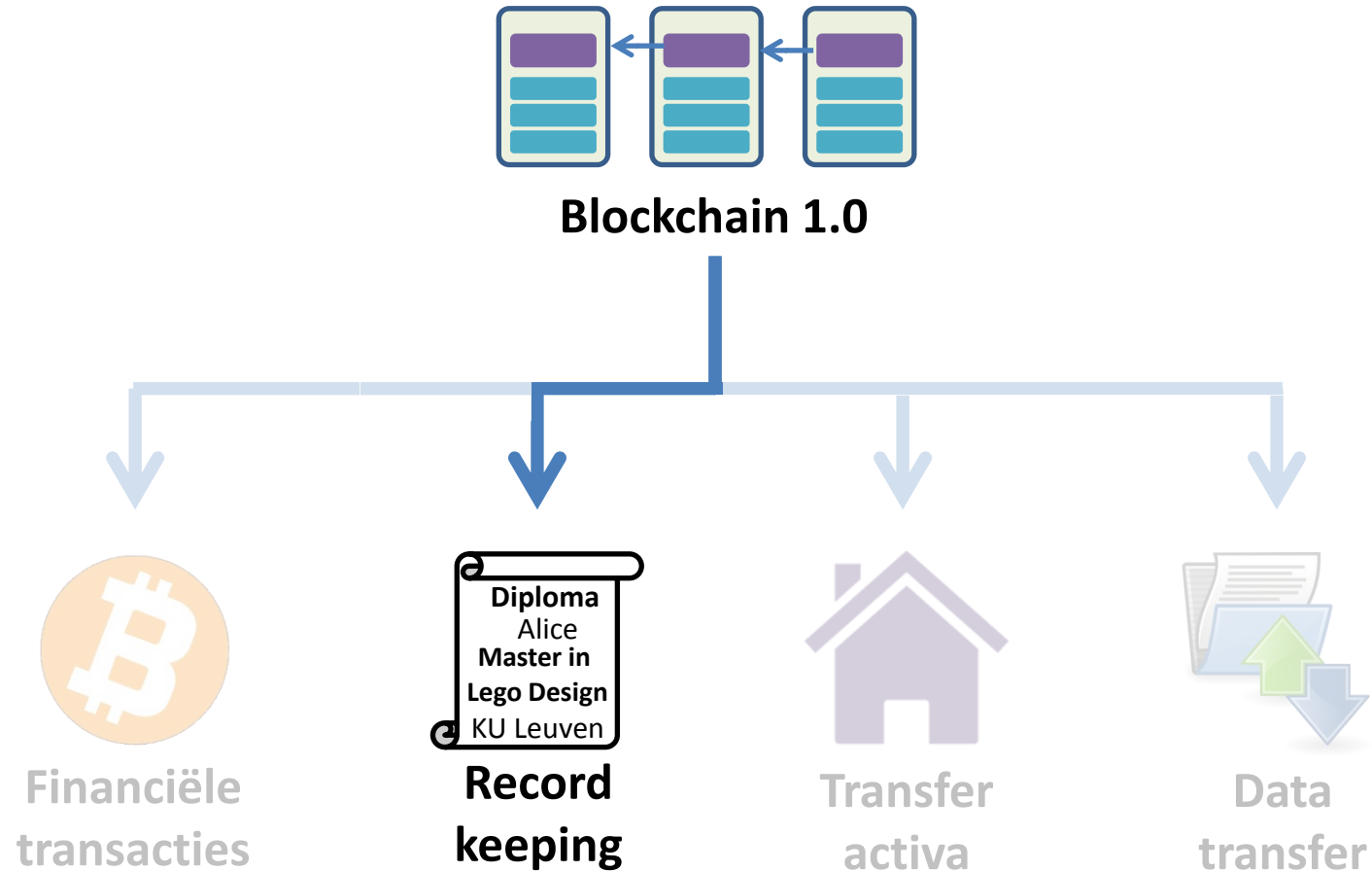
Onweerlegbaar /
Verifieerbaar

→ 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

Digitale handtekeningen

guardtime

Interne verkiezingen

 Deense
LIBERAL
ALLIANCE

Integriteit & timestamping EHR

HealthNautica  **com**
+ **factom** 

Identiteit



ShoCard

Diploma



ÉCOLE
D'INGÉNIEURS
PARIS-LA DÉFENSE



Diploma



HOLBERTON
school()

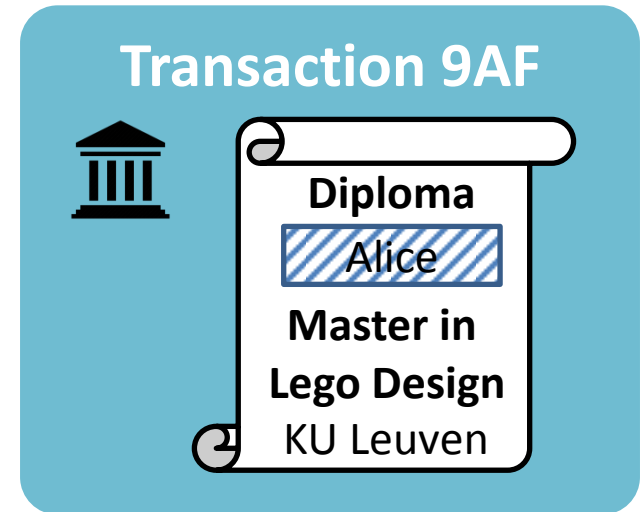
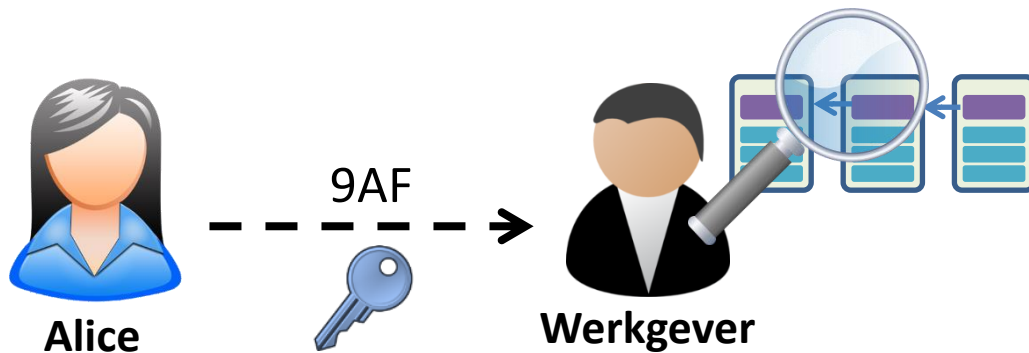


Uitgaven mensen met uitkering



Department
for Work &
Pensions

Record Keeping (Vereenvoudigd)



Alice zelf hoeft geen blockchain account of kopie te hebben

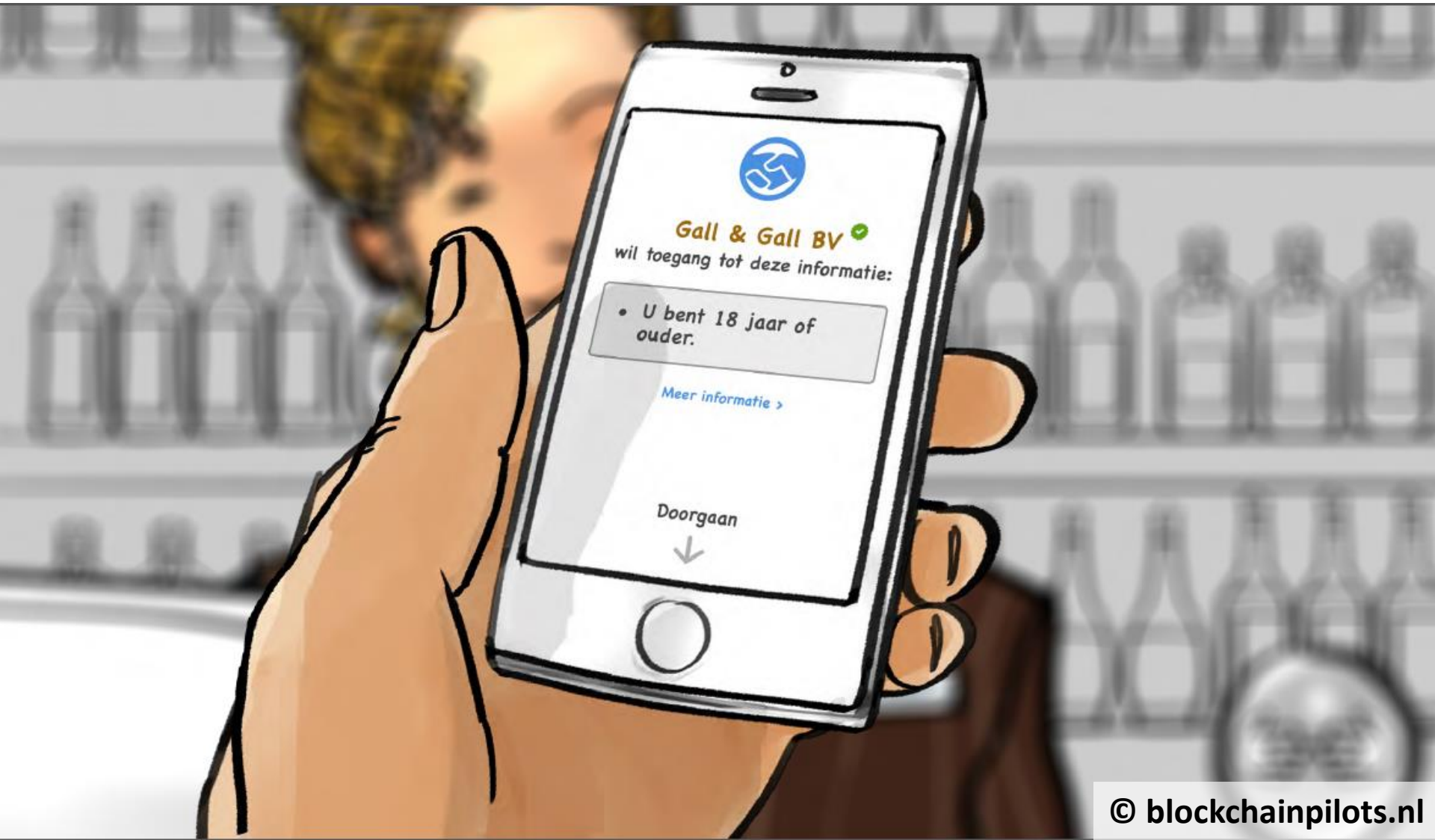
In werkelijkheid vaak extra crypto (hashing, encryptie, pseudoniemen)

Gelijkaardig aan digitale handtekening, maar meer mogelijkheden

Identiteitsgegevens



Identiteitsgegevens



Identiteitsgegevens



Bewijs

Geboortedatum < vandaag – 18 jaar

Gebruik complexe cryptografie (zero-knowledge proofs)

Tracking Supply Chain

voedsel, diamanten, auto's en hun onderdelen,

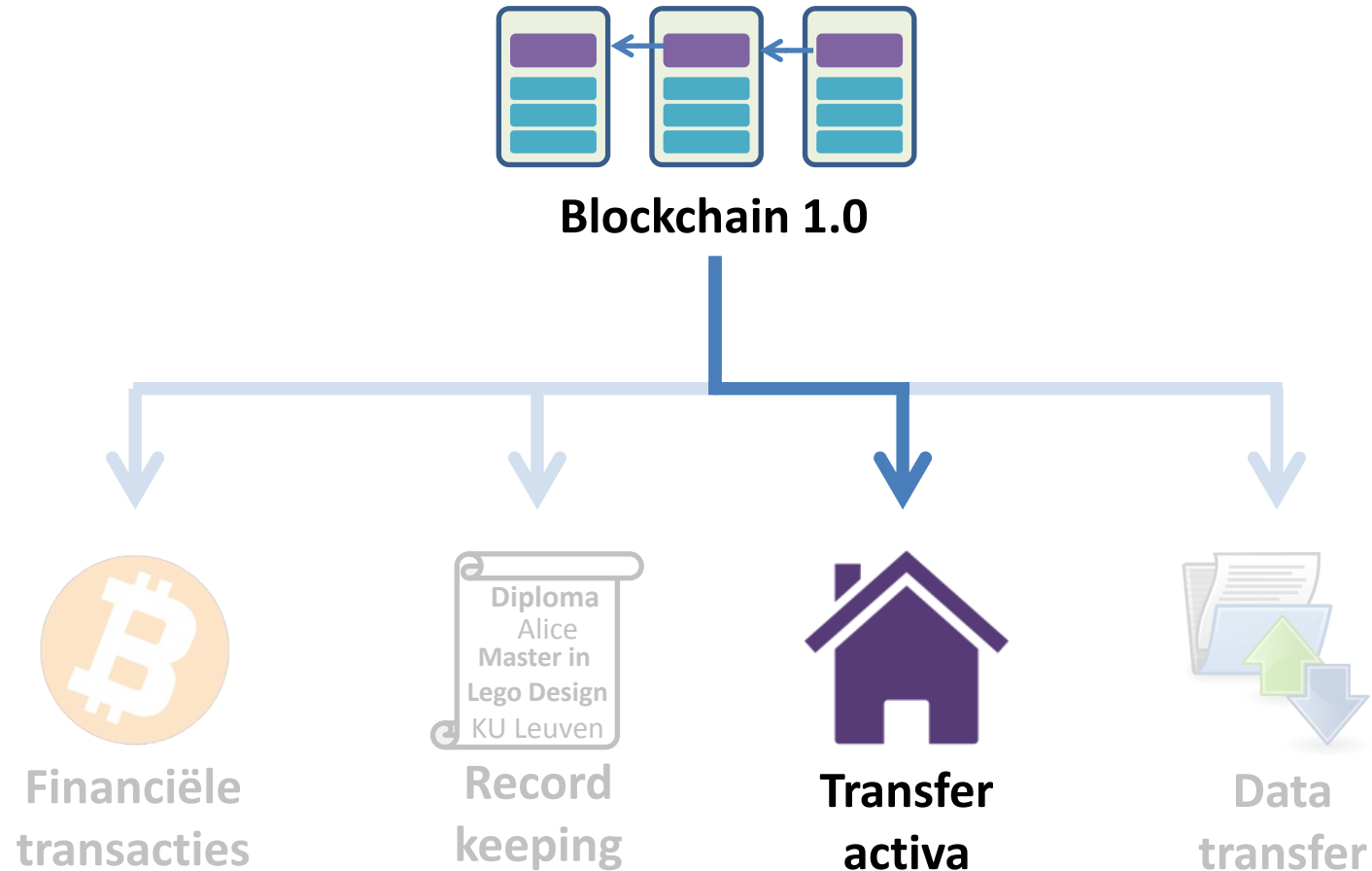


Waar bevindt zich het noodzakelijke onderdeel?

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



Domeinnaam

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

Applications

Auteursrechten



Kadaster



ChromaWay



Domeinnamen



blockstack



Domeinnamen



namecoin

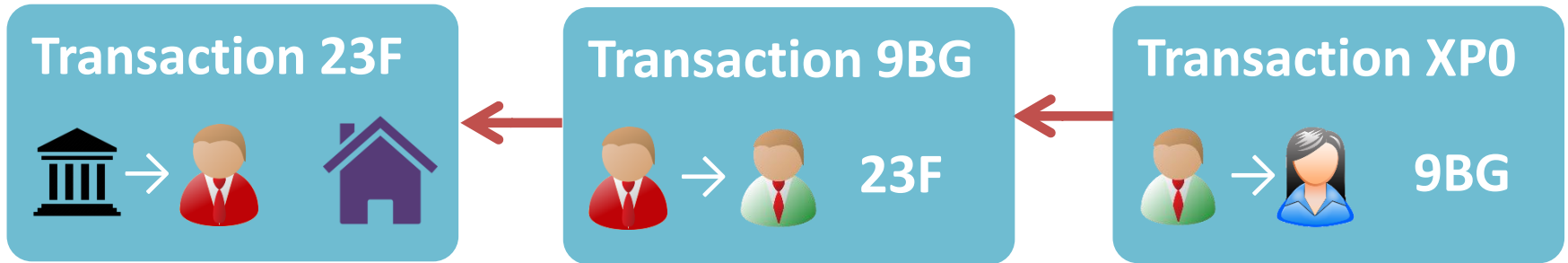
Diamanten



Platform



Value Transfer

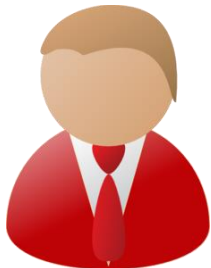


De rechtmatige
eigenaar van
 is .



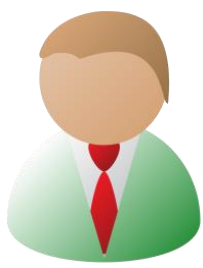
Erkende autoriteit
(hypotheekbewaarder)

De nieuwe
eigenaar van
 is .



Eigenaar 1 (Bob)

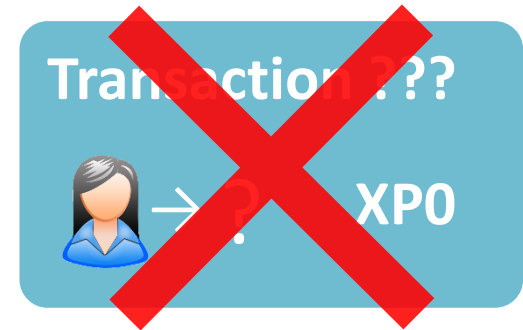
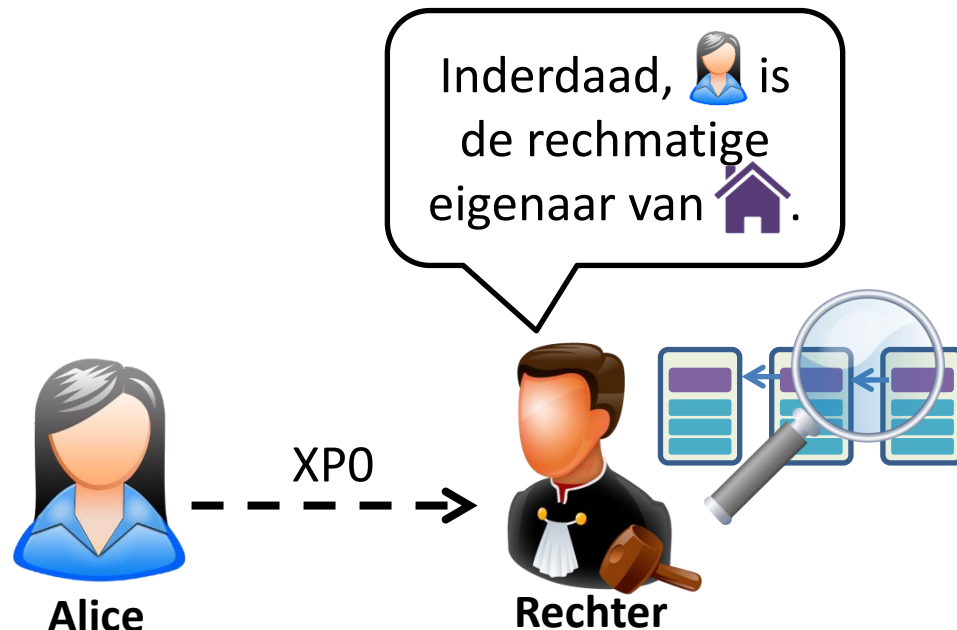
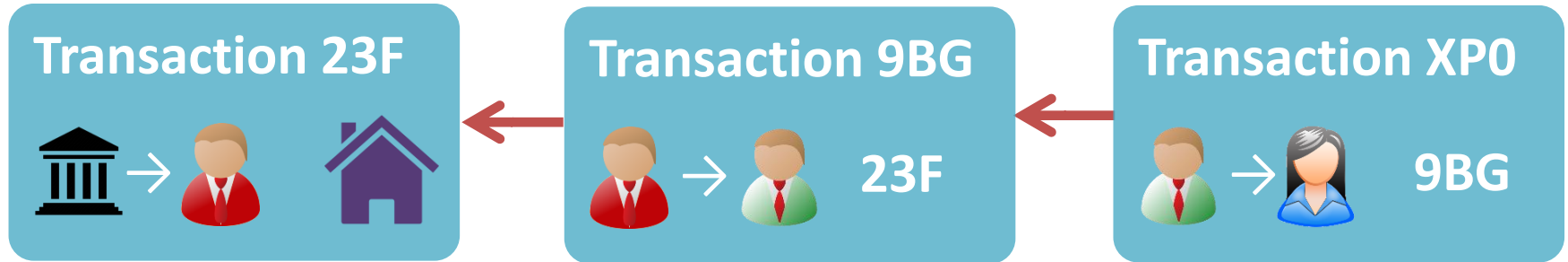
De nieuwe
eigenaar van
 is .



Eigenaar 2 (Charlie)

Autoriteit blijft nodig

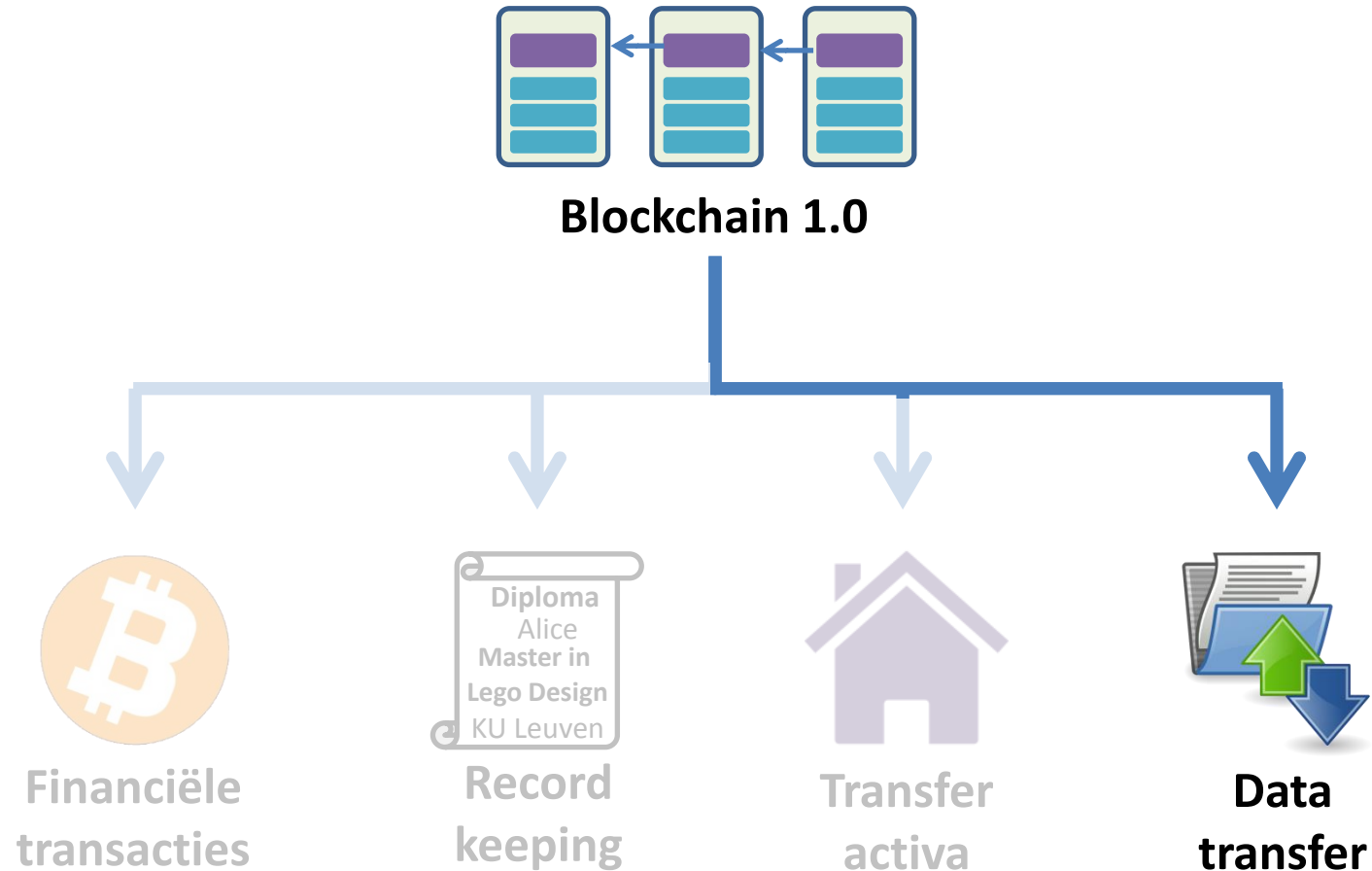
Bewijs van Bezit



Alice hoeft zelf geen kopie van blockchain te hebben

Volledige historiek zichtbaar

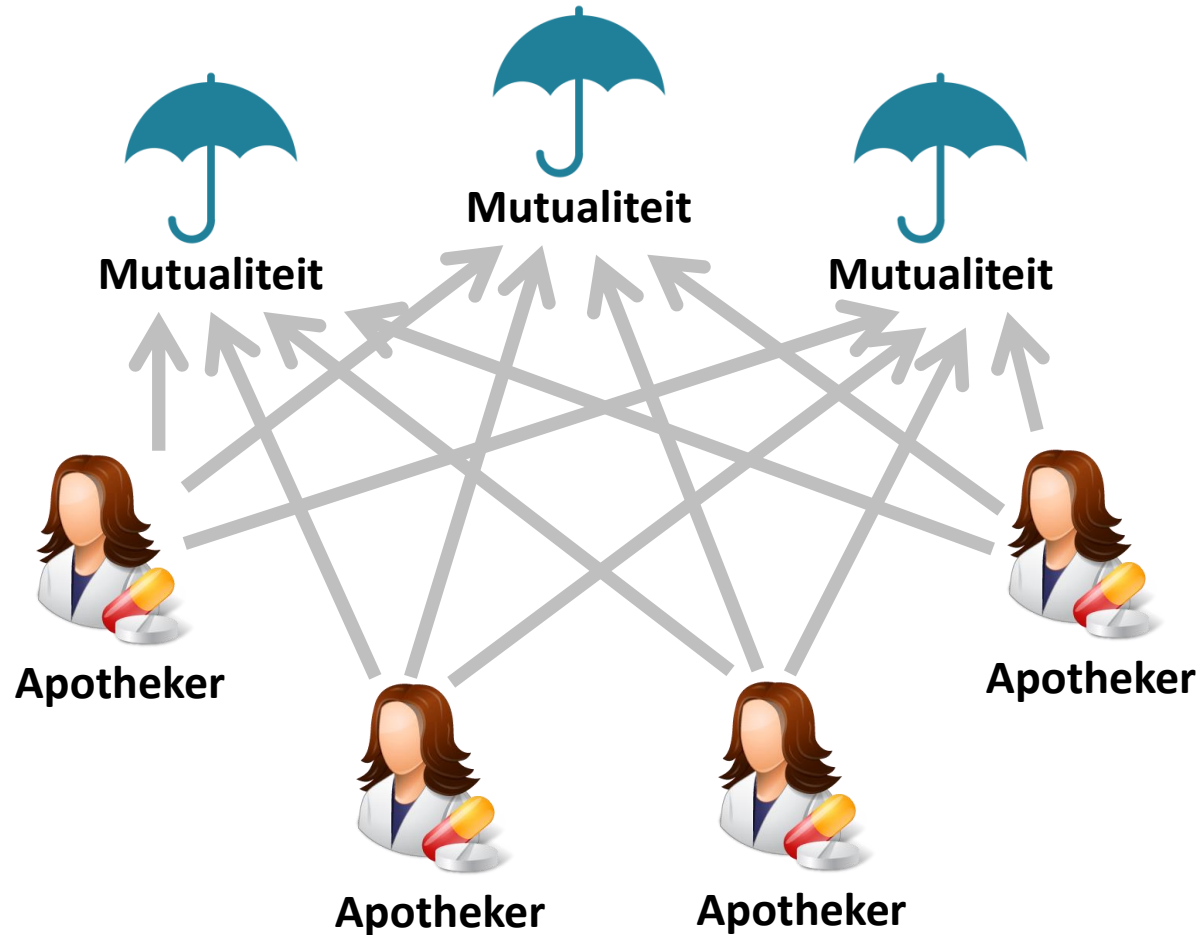
Blockchain Toepassingen



Verminderd vertrouwen vereist in centrale / intermediaire partijen

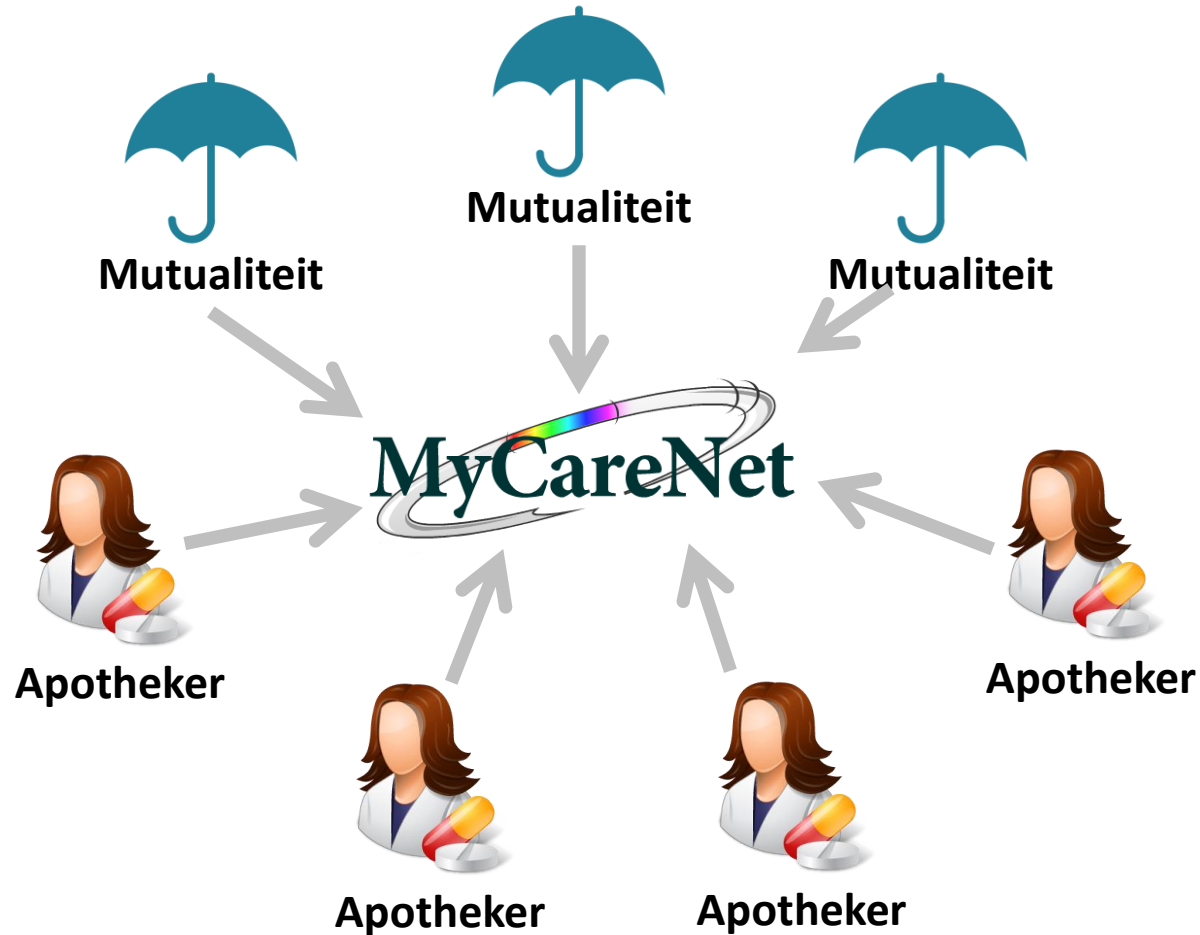
Data Transfer

Vb. Verzekerbaarheid: Is burger aangesloten bij een ziekenfonds?



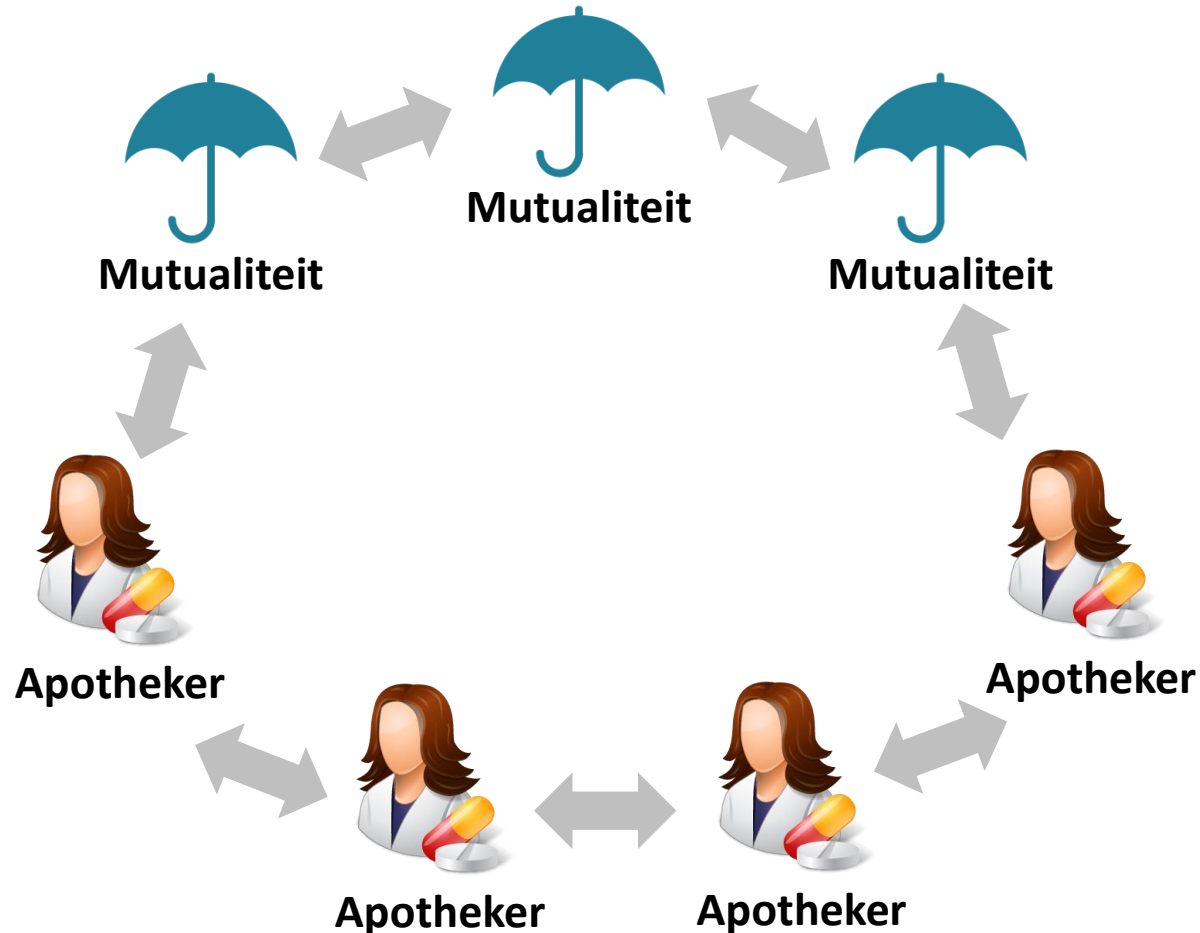
Data Transfer

Vb. Verzekerbaarheid: Is burger aangesloten bij een ziekenfonds?



Data Transfer

Vb. Verzekerbaarheid: Is burger aangesloten bij een ziekenfonds?

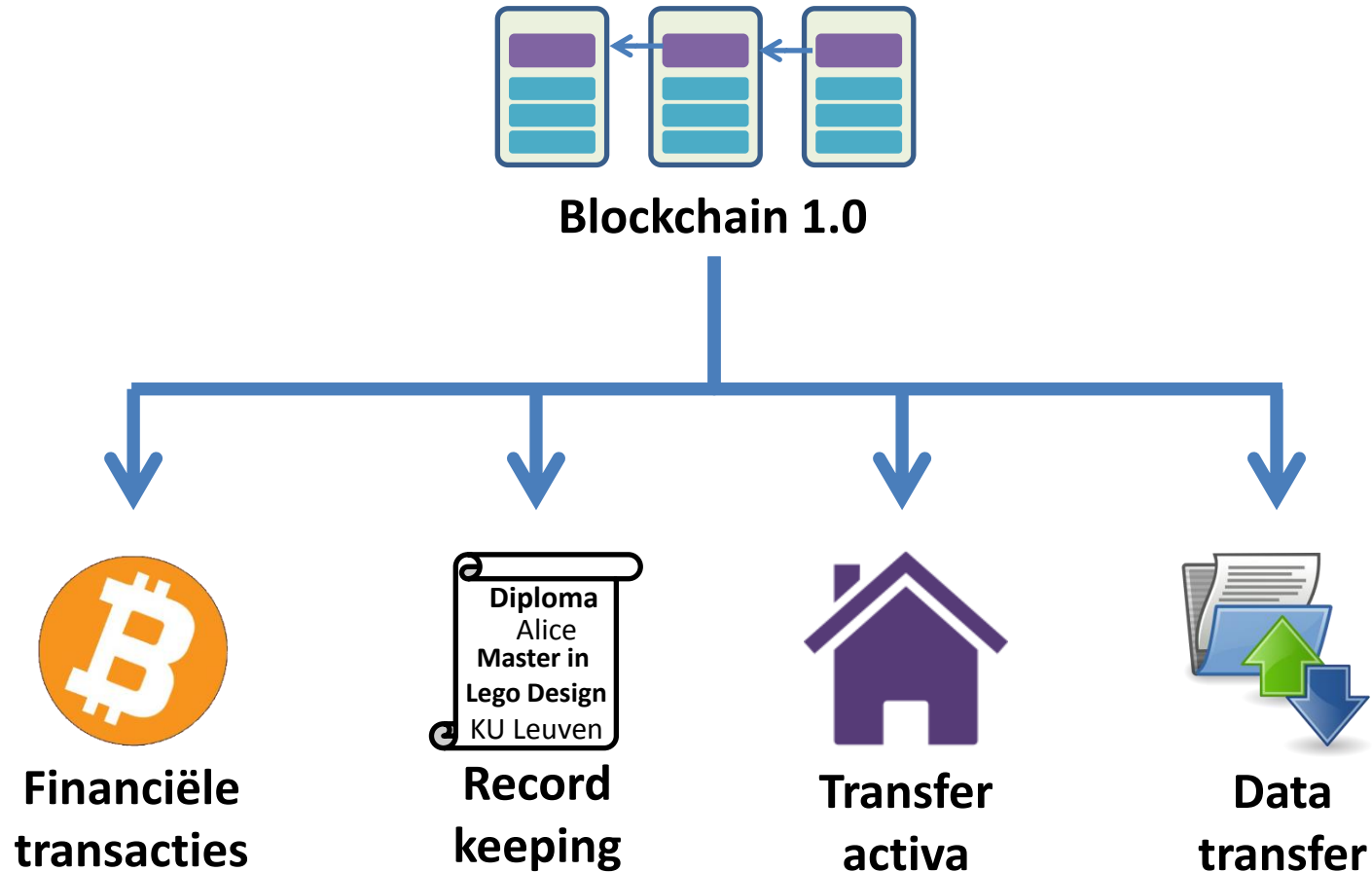


Iedereen steeds meest recente informatie

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

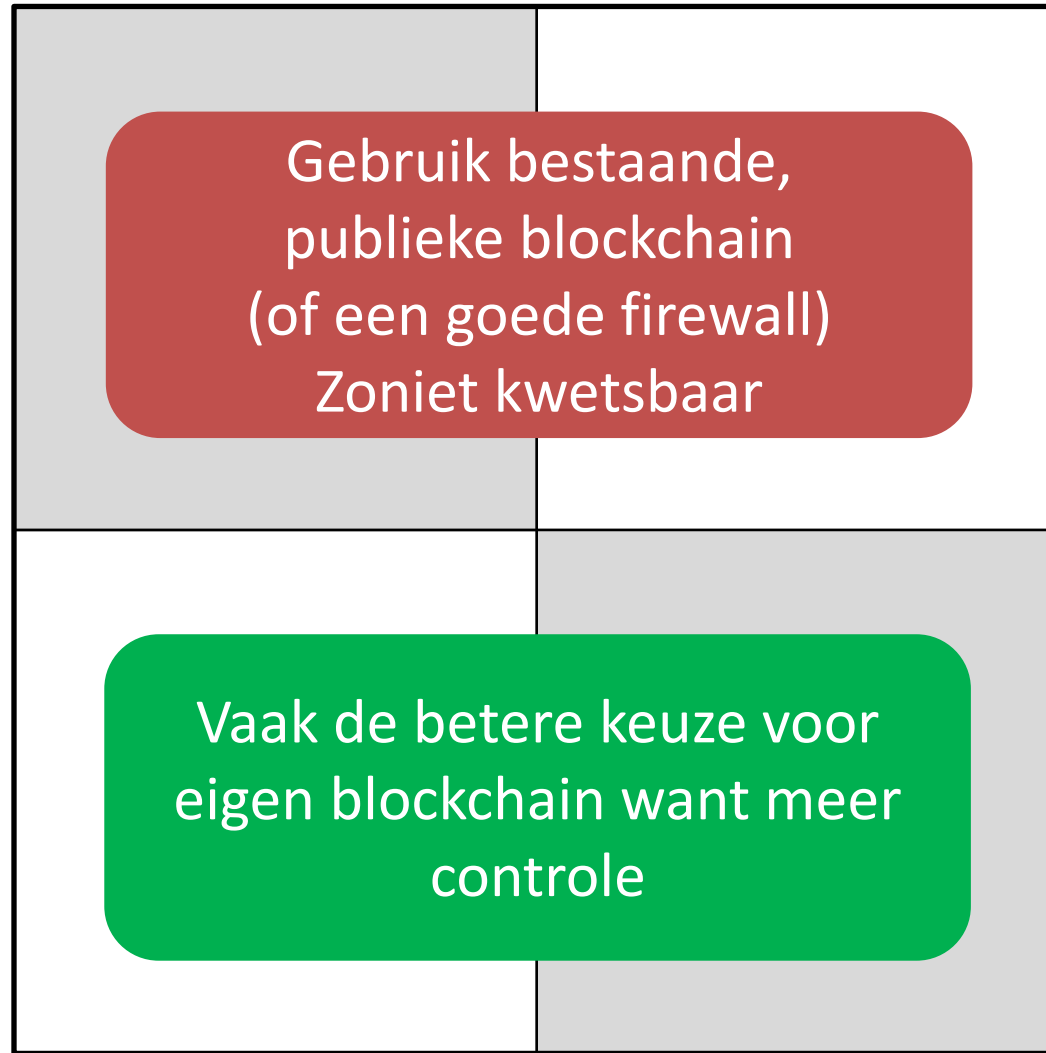
Enkele Blockchain Platformen

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



Blockchain 1.0

Opslag
op blockchain

Blockchain 2.0

Rekenkracht
op blockchain

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 $\neq$ 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

Blockchain 1.0

Bitcoin



Toepassingen



Pauze

Blockchain 2.0

Smart Contracts



Voorschriften



Pauze



Agenda

Blockchain 1.0

Bitcoin



Toepassingen



Pauze

Blockchain 2.0

Smart Contracts



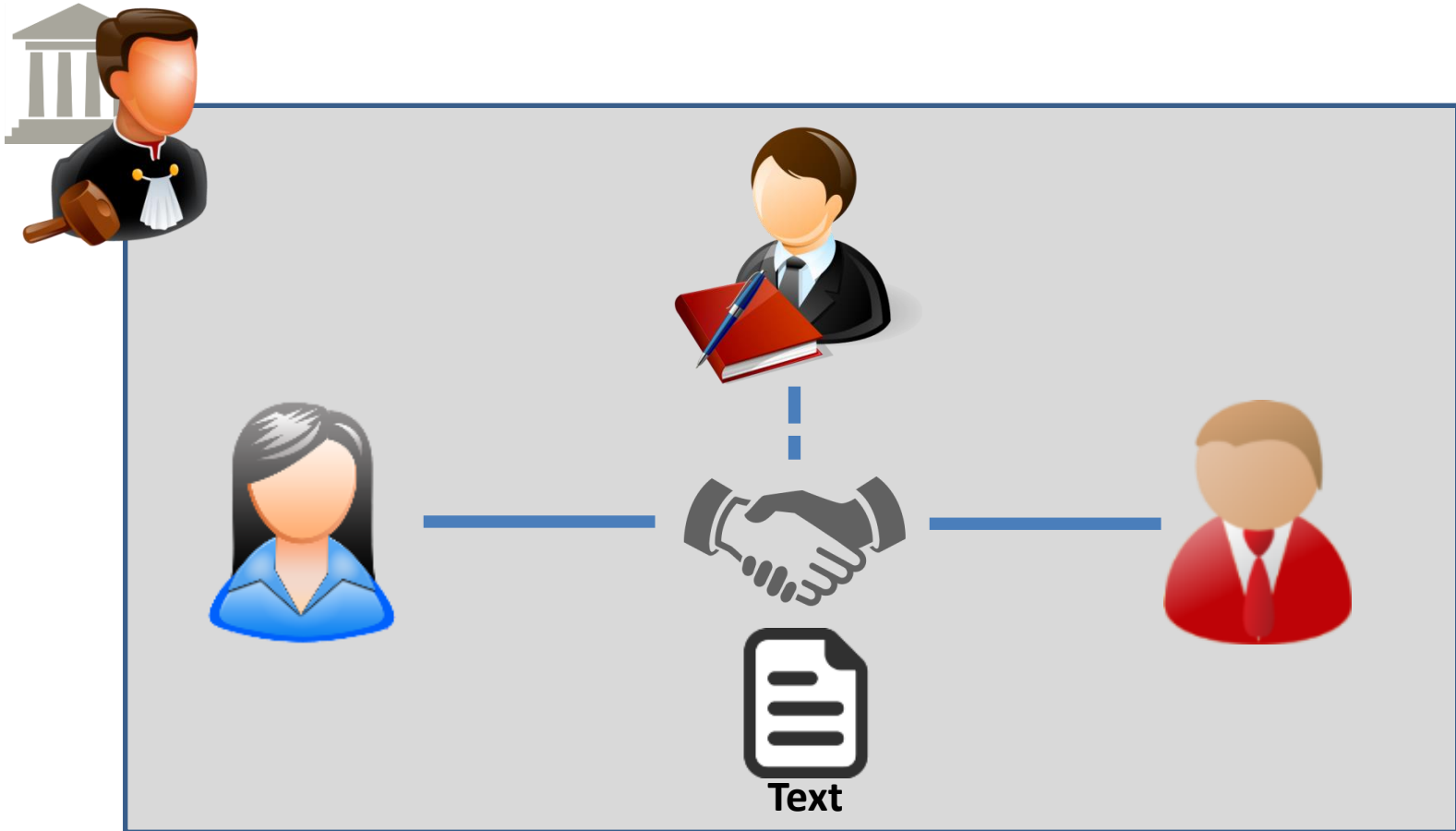
Voorschriften



Smart Contracts



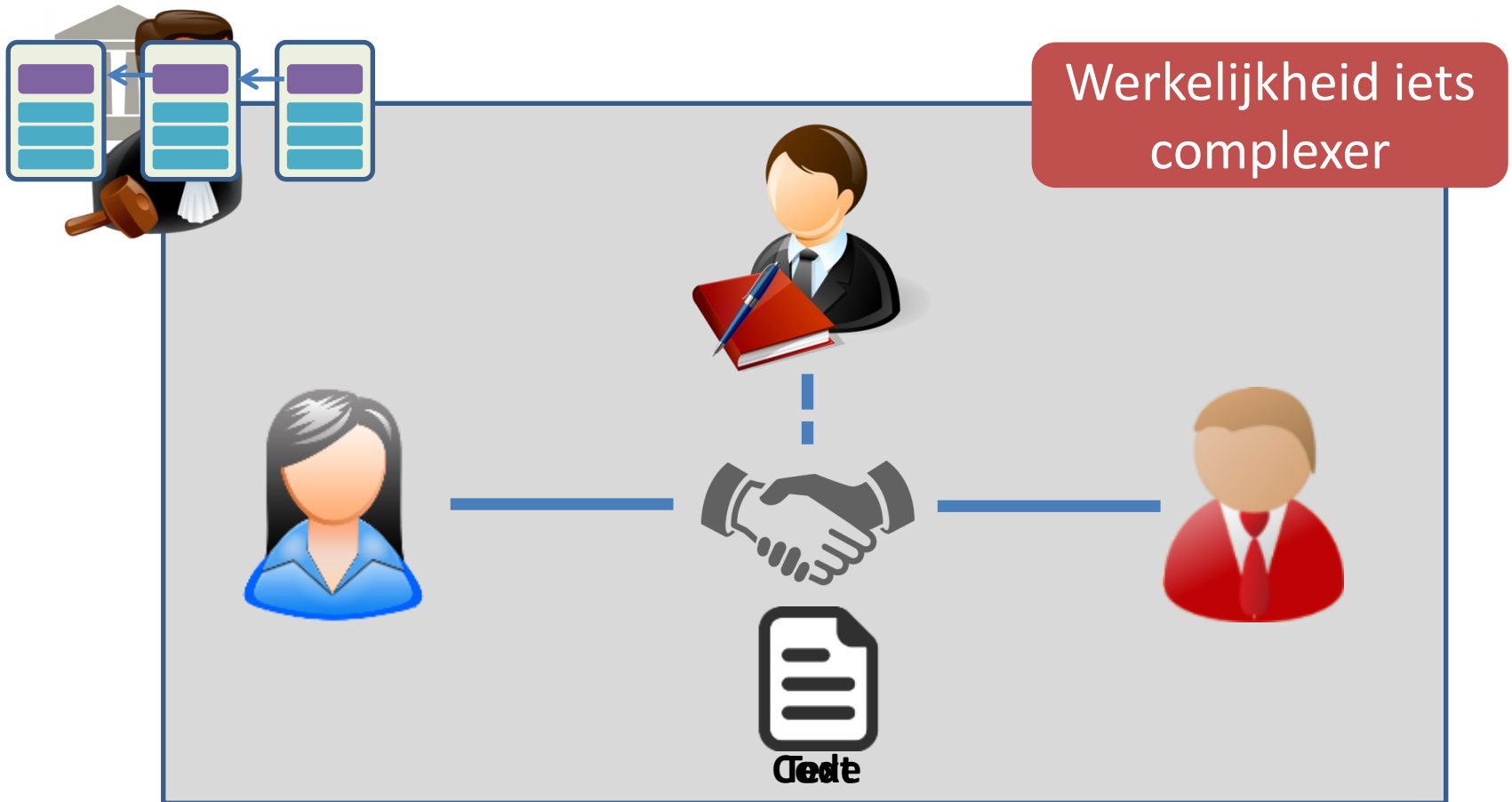
Traditioneel Contract



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/>

365 dapps listed

Pray4Prey Julia Altenried, Stefan Höller The one and only blockchain aquarium Live	AuctionHouse Doug Petkanics, Eric Tang Auction platform for non-fungible on-chain assets. MIT Prototype 2017-02-10	Proof of Identity Oracize Onchain identity verification via your Estonian Digi-ID Working	The Rudimental Troy Murray Equity Crowdfunding Platform for Artists Demo 2016-09-16
AnonymousVoting Patrick McCorry Decentralised e-voting with maximum voter privacy. Open Source Working Prototype 2017-02-27	EthPassport Michael Dela Cuesta Decentralized Traveler MIT Concept 2017-02-26	Smart Identity Tyler Welmans Next generation digital identity for the new digital economy Apache 2 Working Prototype 2017-02-26	Consultrum Vincent Muthee Decentralized Consultancy Platform Work In Progress 2017-02-23
BlockCapsule BlockCapsule Developers Time Capsule on Blockchain Work In Progress	Pass DAO Frederic A DAO for decentralized services	Decibel.LIVE Decibel.LIVE Noise monitoring and compensation	Flight Delay Insurance Etherisc GmbH Get instant payout in case your flight is late. t.b.d Prototype 2017-02-20

**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

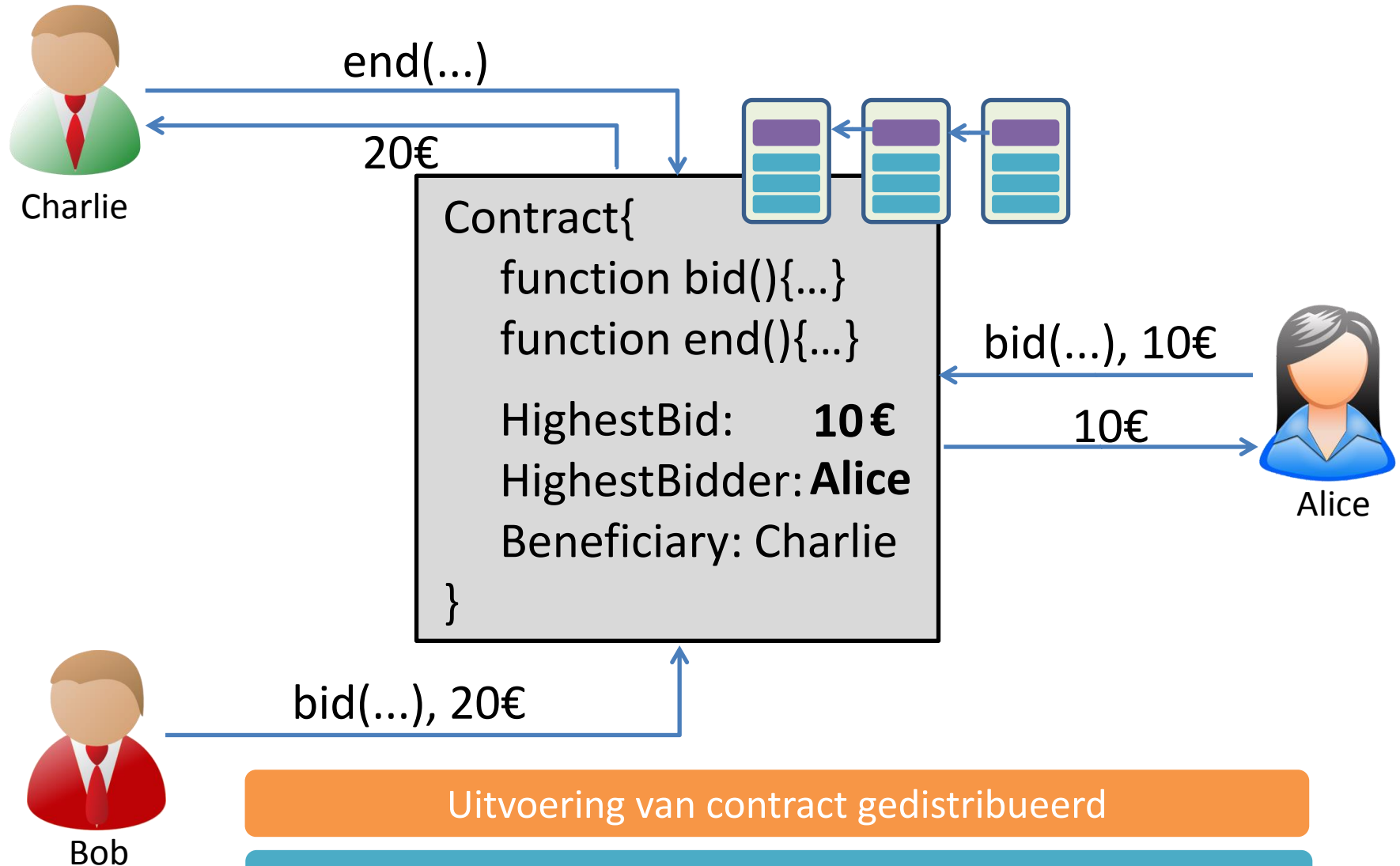
- Bod plaatsen → Geld onmiddellijk naar smart contract
- Overboden → Smart contract betaalt je terug
- Einde veiling → Bedrag hoogste bieder naar verkoper



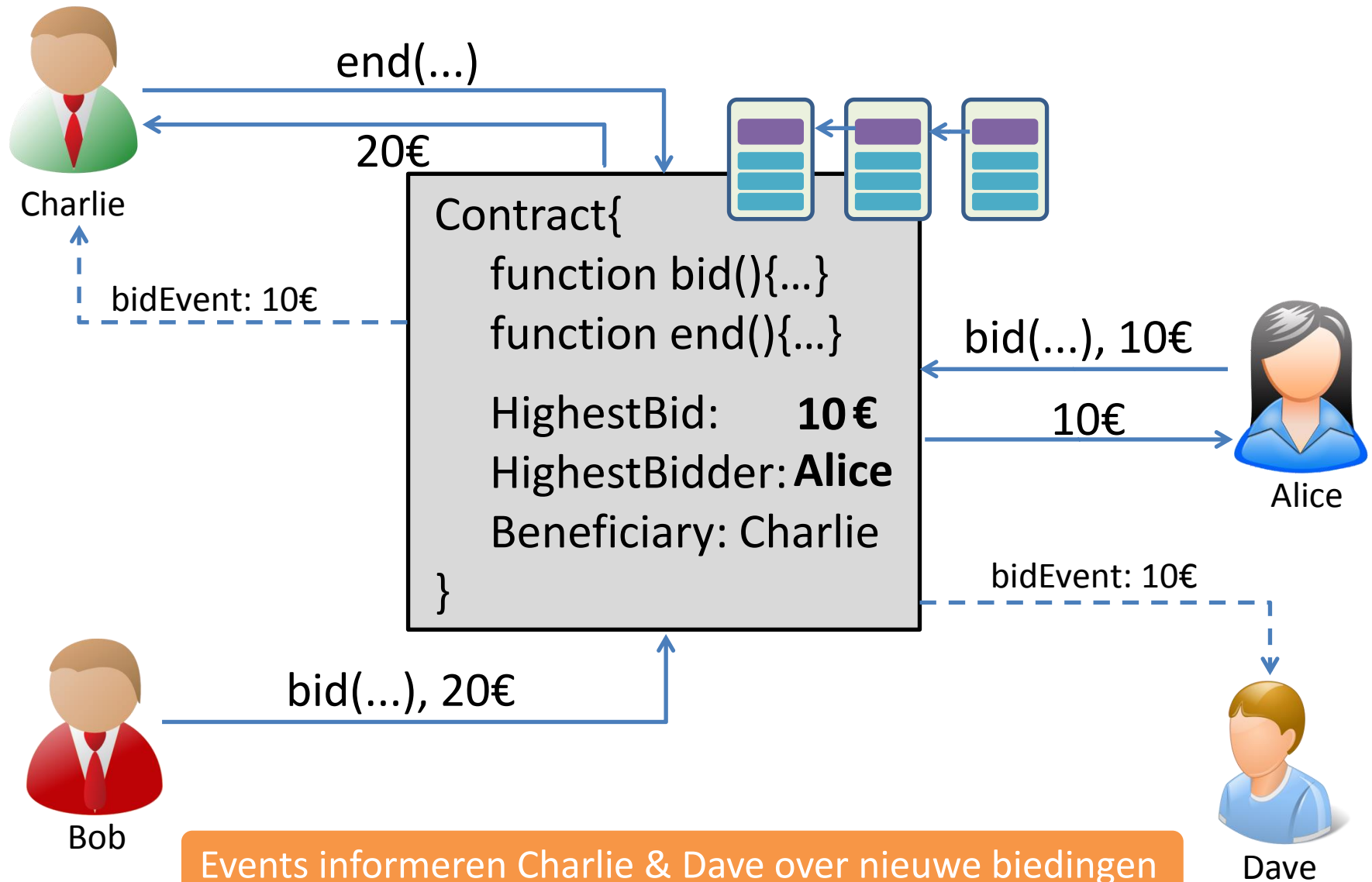
Een aantal nieuwe uitdagingen

- Zie later

Smart Contracts (Blockchain 2.0)

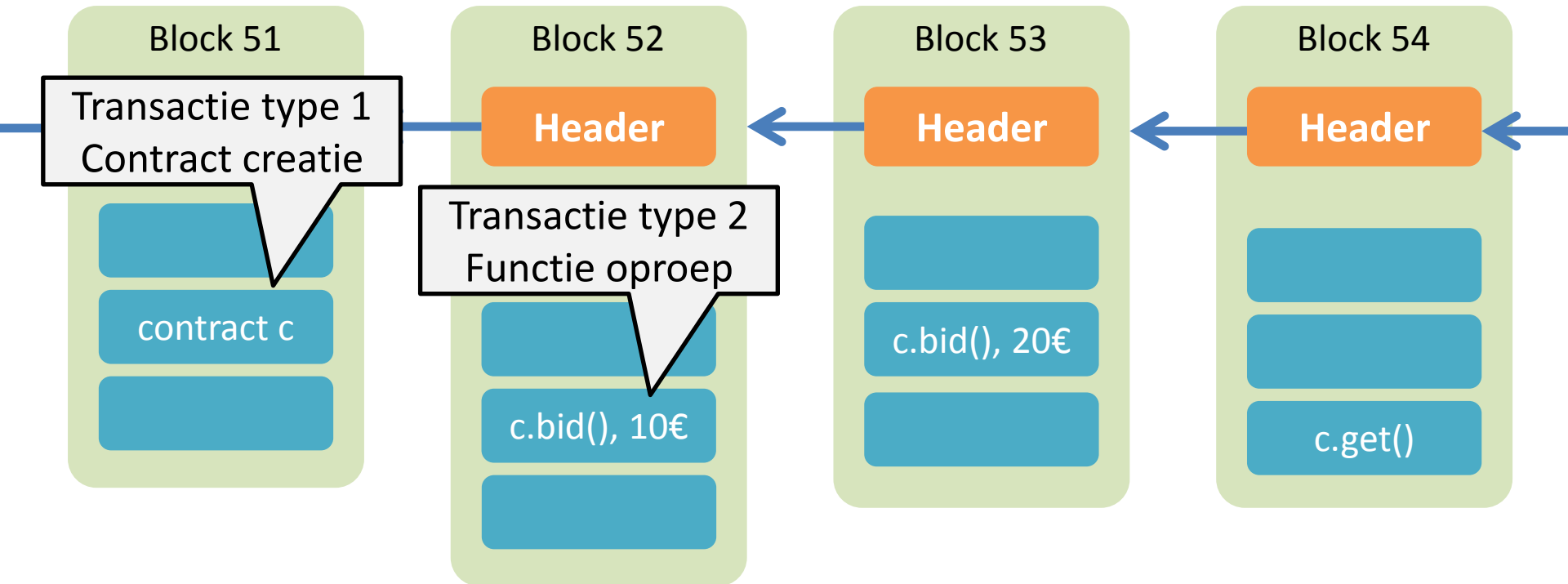


Events in Smart Contracts



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

Smart Contract Blockchain



Transactie voor functieoproep bevat

- Id contract
- Naam functie
- Argumenten
- Bedrag

Een Concrete 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;
    }
    ...
}
```



```

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)
    }
}

```

Doe dit NOOIT...

```
// 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
```

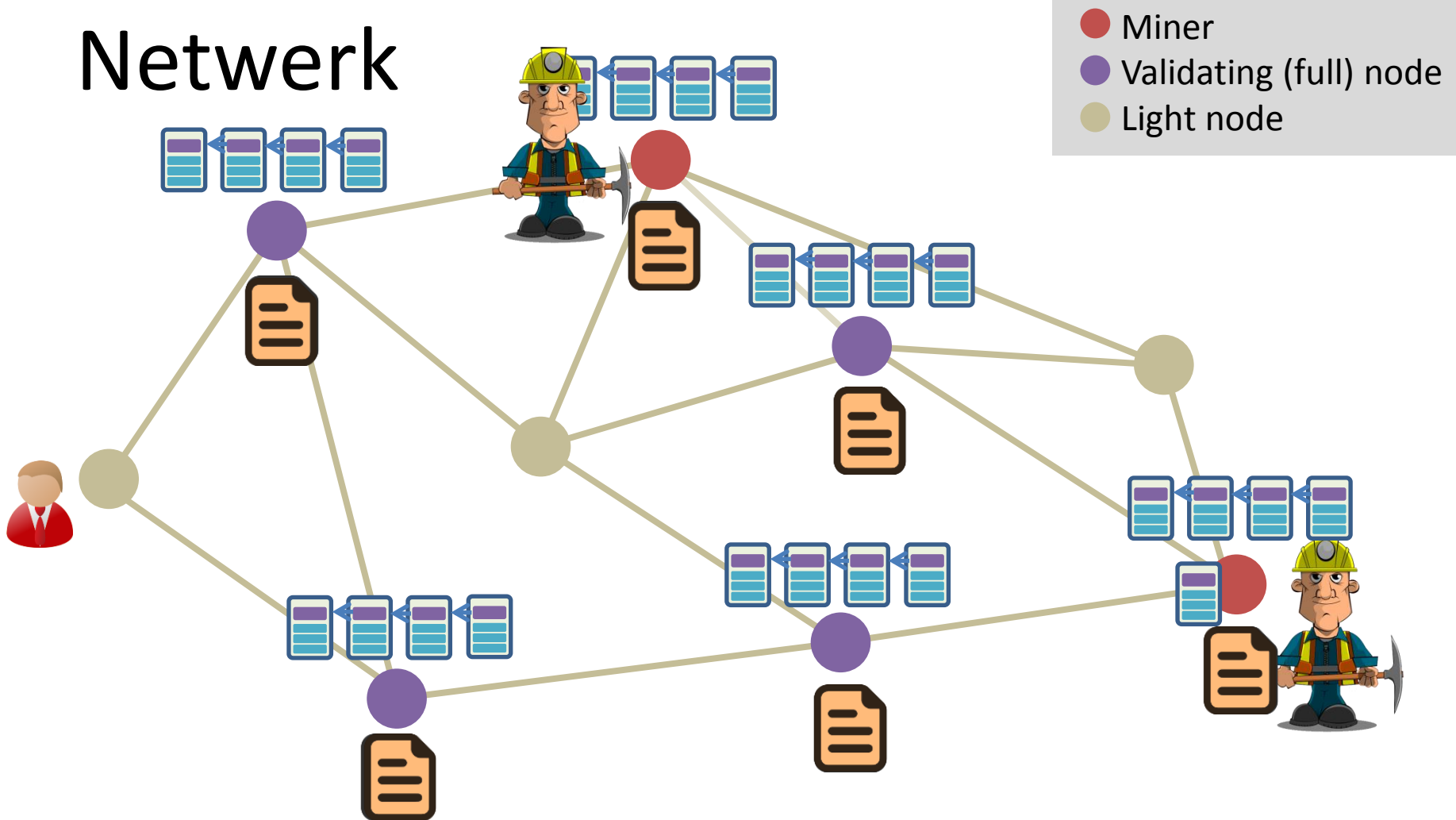
```
function checkDocument(string document) returns (bool){  
    var proof = sha256(document);  
    return proofs[proof];  
}
```

```
}
```

```
proofs:  c0796844c3cbc...  → true  
         5d5f4926be230...  → true  
         c56d58202b0aa...  → true  
         17f8f6699a8948...  → true  
         ...
```

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

Network



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

Elke full node voert lokaal dezelfde functieoproepen uit

Veiligheidsmechanismes zodat iedereen correcte versie

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

    address public highestBidder;
    uint public highestBid;

    bool ended;

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

    function SimpleAuction(uint _beneficiary,
        uint _auctionStart,
        uint _biddingTime,
        address _highestBidder,
        uint _highestBid) public {
        beneficiary = _beneficiary;
        auctionStart = now;
        biddingTime = _biddingTime;
        highestBidder = _highestBidder;
        highestBid = _highestBid;
    }
}
```

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/>

365 dapps listed		Sort: Updated	
Pray4Prey Julia Altenried, Stefan Höller The one and only blockchain aquarium  Live 2017-02-27	AuctionHouse Doug Petkanics, Eric Tang Auction platform for non-fungible on-chain assets.  MIT  Working Prototype 2017-02-10	Proof of Identity Oracize Onchain identity verification via your Estonina Digi-ID  Working Prototype 2017-02-27	The Rudimental Troy Murray Equity Crowdfunding Platform for Artists   Demo 2016-09-16
AnonymousVoting Patrick McCorry Decentralised e-voting with maximum voter privacy.  Open Source  Working Prototype 2017-02-27	EthPassport Michael Dela Cuesta Decentralized Traveler  MIT  Concept 2017-02-26	Smart Identity Tyler Welmans Next generation digital identity for the new digital economy  Apache 2  Working Prototype 2017-02-26	Consulteum Vincent Muthee Decentralized Consultancy Platform  2017-02-23
BlockCapsule BlockCapsule Developers Time Capsule on Blockchain  Work In Progress 2017-02-22	Pass DAO Frederic A DAO for decentralized services  GPL   Live 2017-02-21	Decibel.LIVE Decibel.LIVE Noise monitoring and compensation settlement based on Ethereum  Working Prototype 2017-02-21	Flight Delay Insurance Etherisc GmbH Get instant payout in case your flight is late.  t.b.d   Working Prototype 2017-02-20

IoT

Verzekering

Enkele Blockchain Platformen

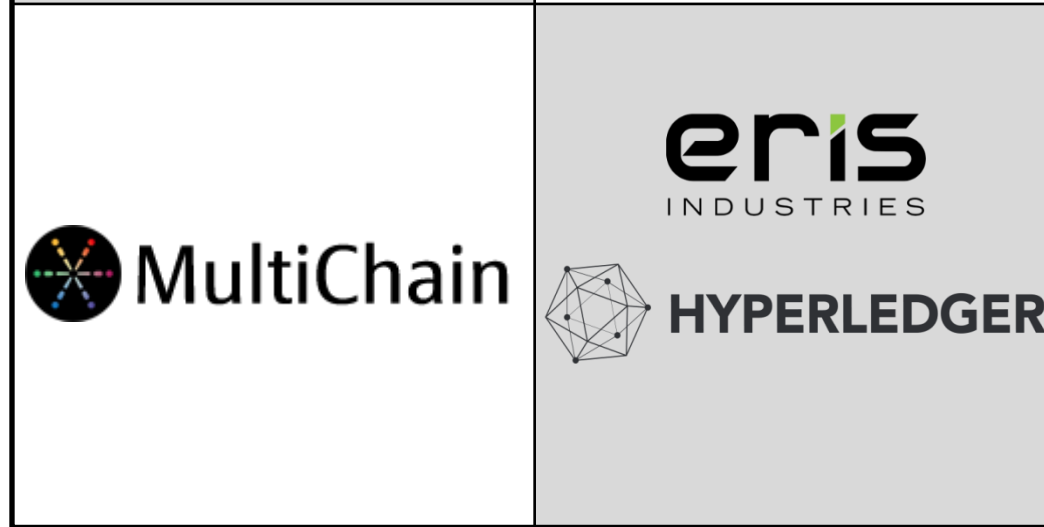
Unpermissioned

- 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

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

Bitcoin



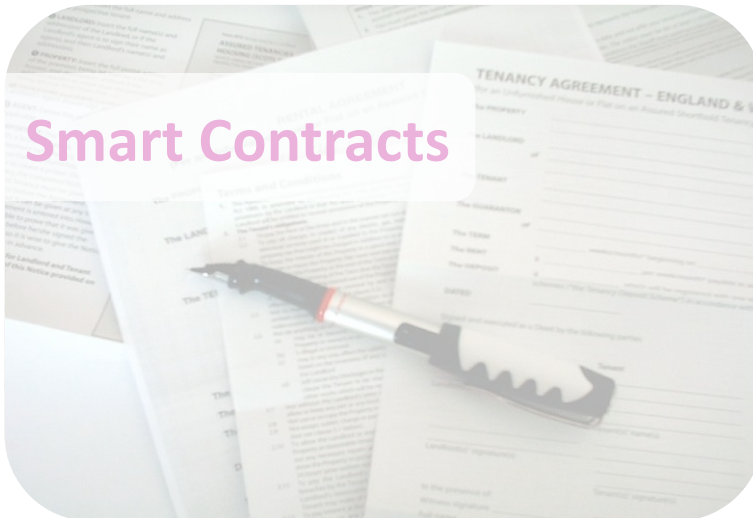
Toepassingen



Pauze

Blockchain 2.0

Smart Contracts



Voorschriften



Voorschriften op een Blockchain



Waarom deze case?

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

Verwerking Medische Voorschriften



Arts



Patient



Apotheker

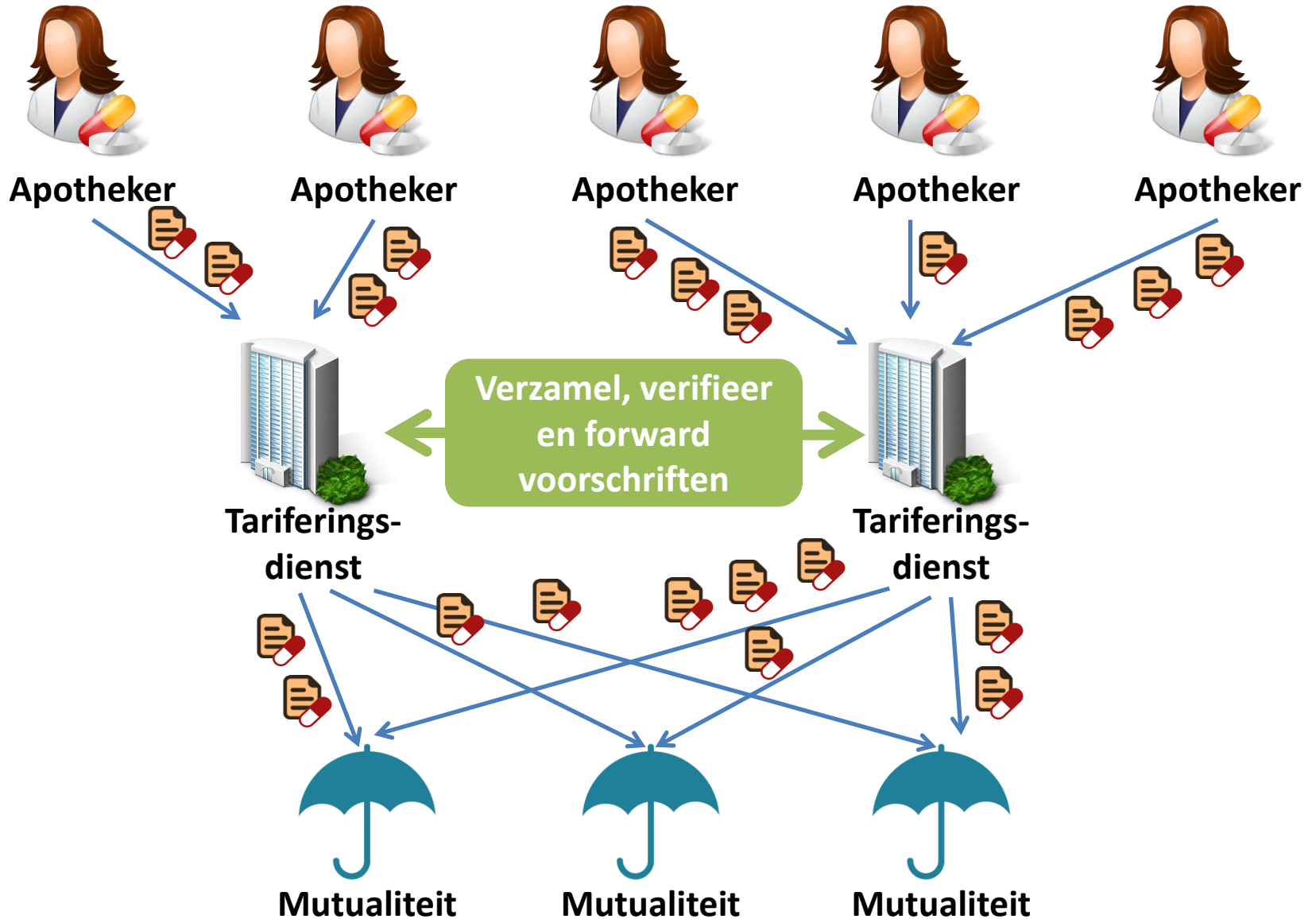


Mutualiteit

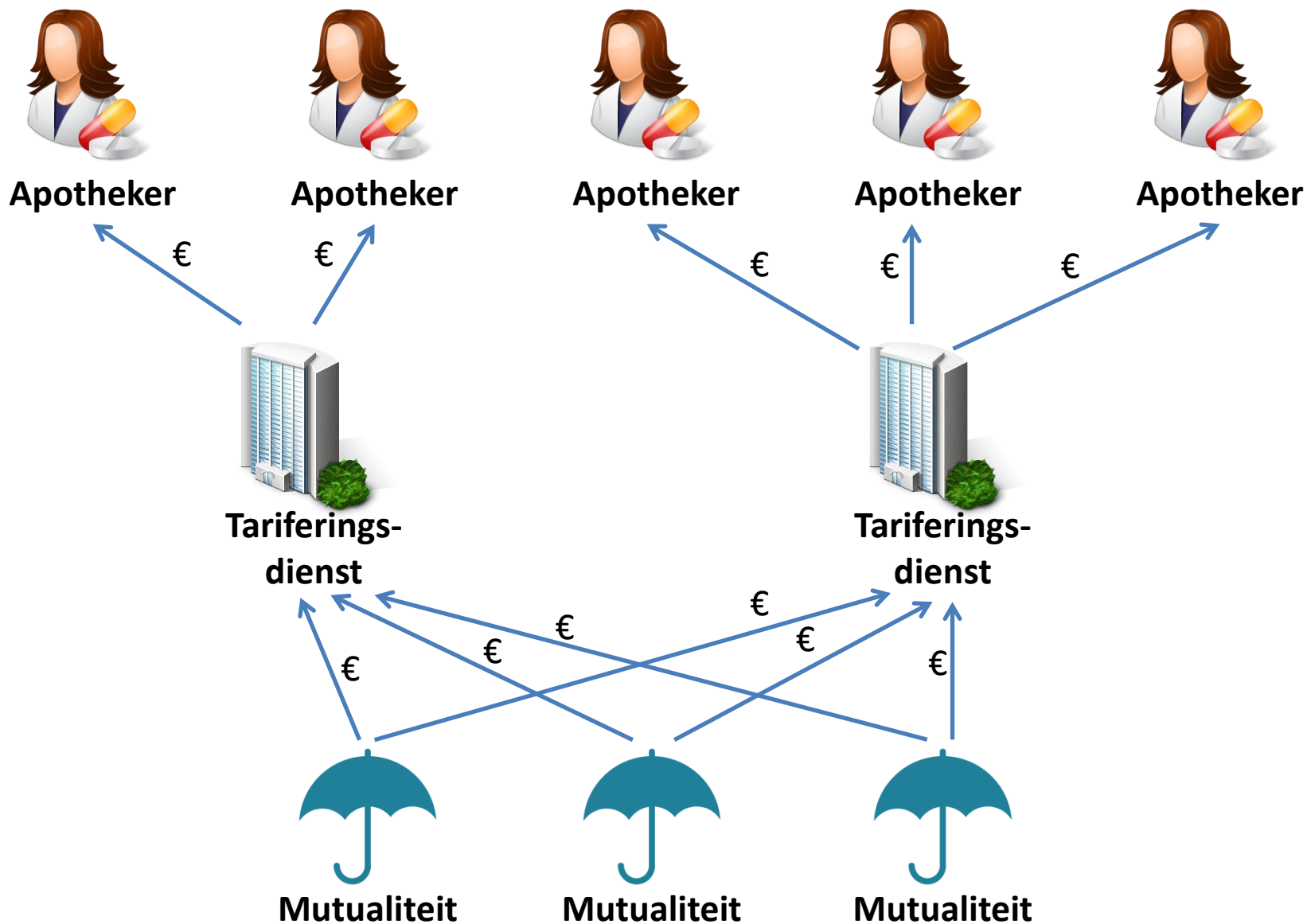


**Tarifierings-
dienst**

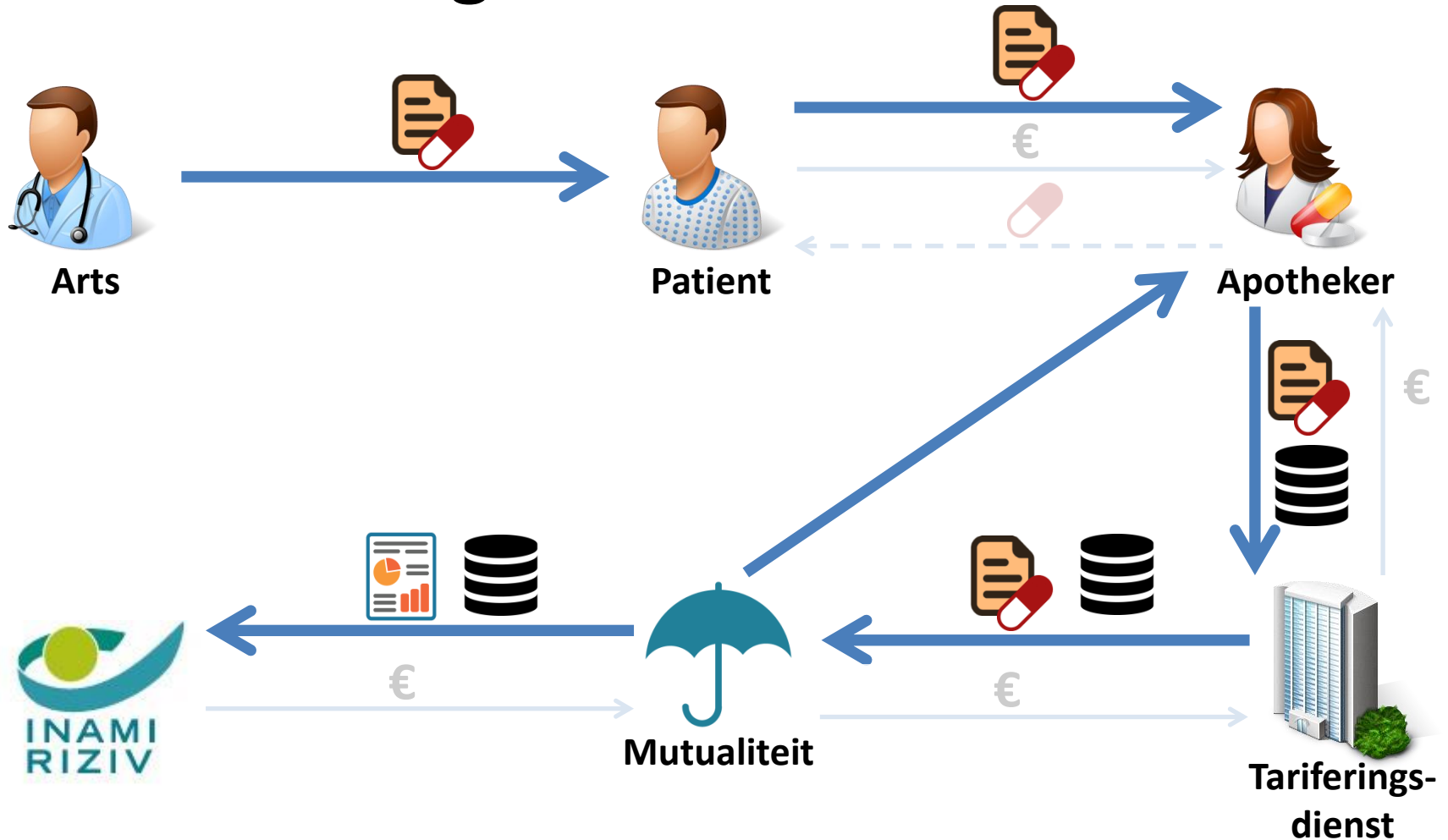
Tarifieringsdienst



Tarifieringsdienst



Verwerking Medische Voorschriften



Verwerking voorschriften zodat iedereen info voor terugbetaling

Real-time analyse RIZIV

The diagram illustrates the flow of complex information and traditional money transfer between various stakeholders in a healthcare system. The stakeholders and their associated values are:

- Arts** (Doctor): 56 000
- Patient**: 11 000 000
- Apotheker** (Pharmacist): 5 000
- Mutualiteit** (Mutual): 7
- Tarifieringsdienst** (Billing service): 5 - 10
- INAMI RIZIV**: 1

The flows are categorized into two types:

- Complex informatiestromen** (Complex information flows): Represented by thick blue arrows.
- Traditional money transfer**: Represented by thin blue arrows.

The diagram shows the following flows:

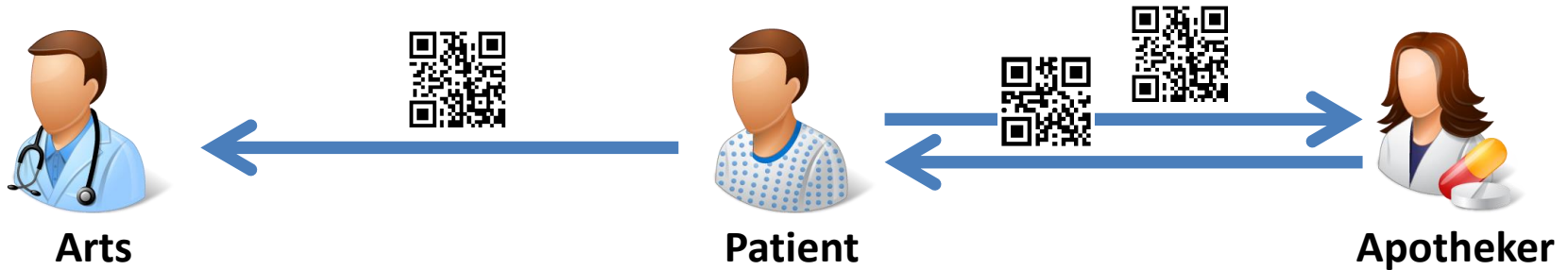
- Complex informatiestromen**:
 - Arts to Patient
 - Patient to Apotheker
 - Apotheker to Mutualiteit
 - Mutualiteit to INAMI RIZIV
 - Mutualiteit to Tarifieringsdienst
 - Tarifieringsdienst to Apotheker
- Traditional money transfer**:
 - Patient to Arts
 - Patient to Apotheker
 - Apotheker to Mutualiteit
 - Mutualiteit to INAMI RIZIV
 - Mutualiteit to Tarifieringsdienst
 - Tarifieringsdienst to Apotheker

Legend:

- Thick blue arrow: Show on smartphone
- Thin blue arrow: Traditional money transfer

- ➔ Show on smartphone
- ➔ Traditional money transfer
- ➔ Physical delivery

Verwerking Medische Voorschriften



-  Show on smartphone
-  Traditional money transfer
-  Physical delivery

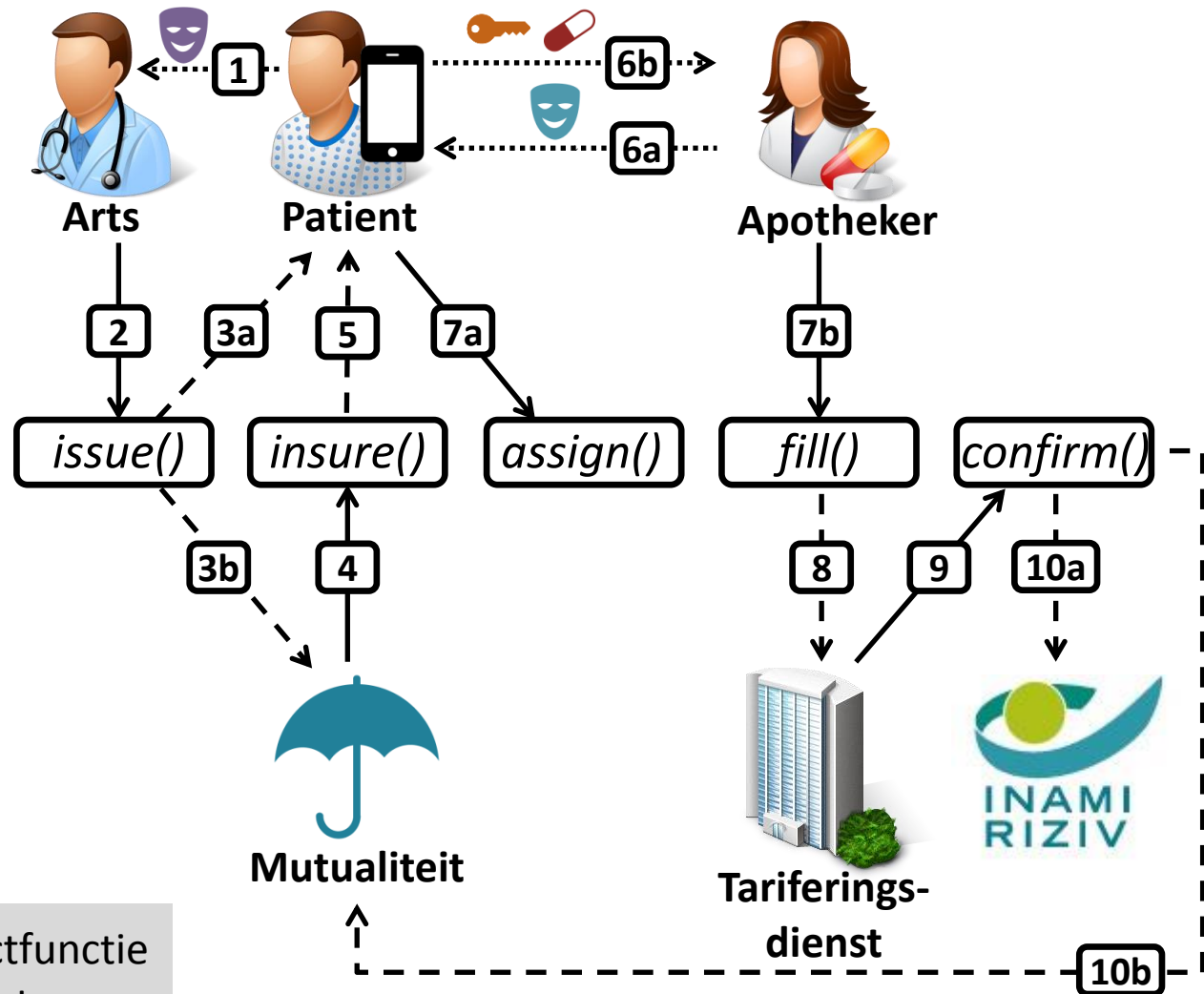
Alle andere communicatie via blockchain

Privacy & confidentialiteit bedrijfsgegevens gegarandeerd

Voorschriften op een Blockchain

Voorschrift

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

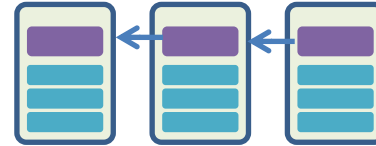


- Oproep contractfunctie
- - - - -> Observatie event
-> Directe communicatie
- function()** Contractfunctie

Permanente Pseudoniemen



Fysieke wereld



Blockchain netwerk



Bob



Alice



Charlie



1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX



3BcMuv1VJqmwY5Wim8MPAzKAAiAKby9LcN



1Nf311Qb8rLDkWTHrhpmNewZzkcWFYptfc

Anonimiteit

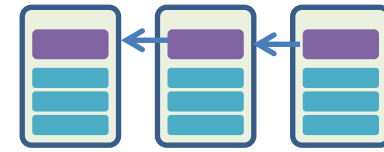
Id	
Patient	
Arts	
Medicijn	
Geldig vanaf	
Verlaagd remgeld?	
Mutualiteit	
Apotheker	
Afgeleverd	
Tarifieringsdienst	

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

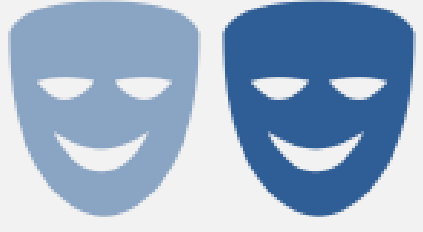
Id	
Patient	
Arts	
Medicijn	
Geldig vanaf	
Verlaagd remgeld	
Mutualiteit	
Apotheker	
Afgeleverd	
Tarifieringsdienst	

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

One-Time Pseudoniemen

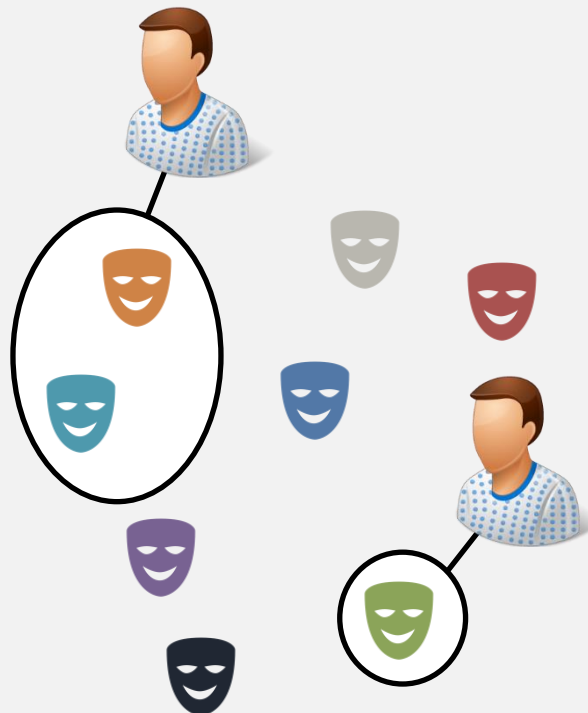


Blockchain netwerk

 Bob 	 Link		
 Alice 	 Link	  Link	
 Charlie 	 Link		

Verschillende Views

Pseudoniemen patienten op de blockchain

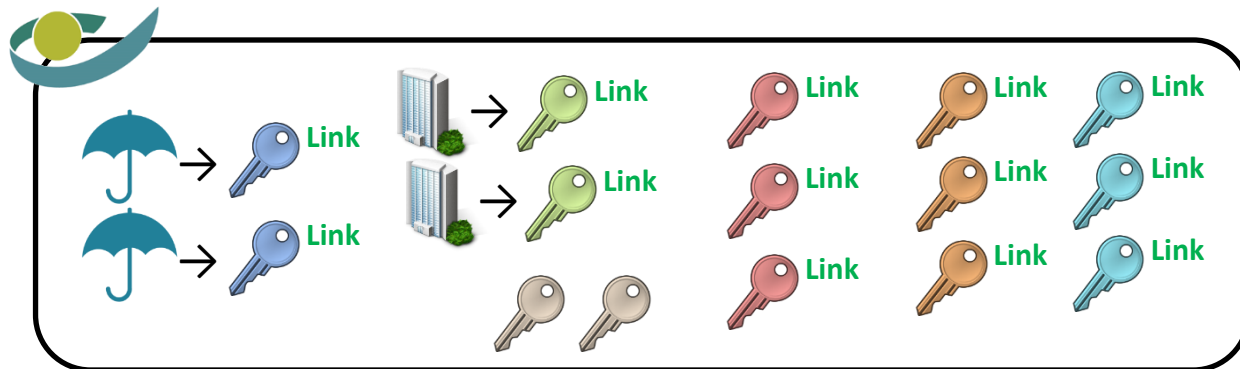
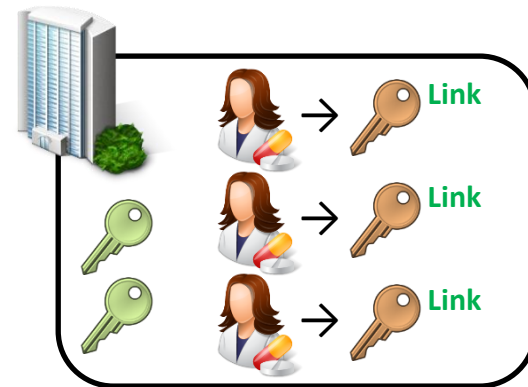
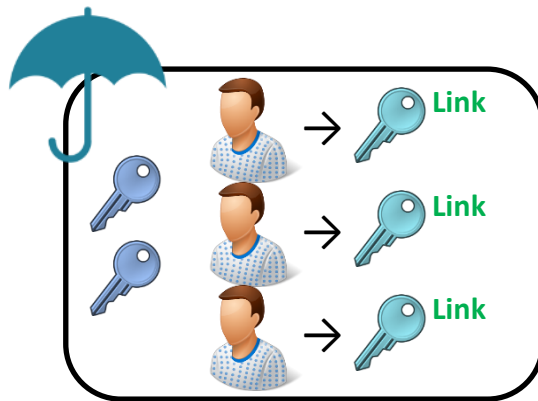
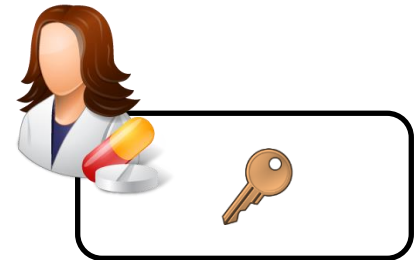
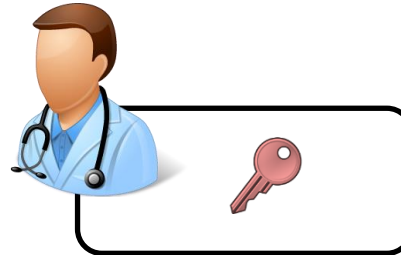
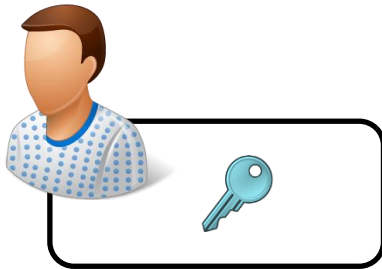


Rest of the world



Gelijkwaardig voor artsen, apothekers, mutualiteiten en tarifieringsdiensten

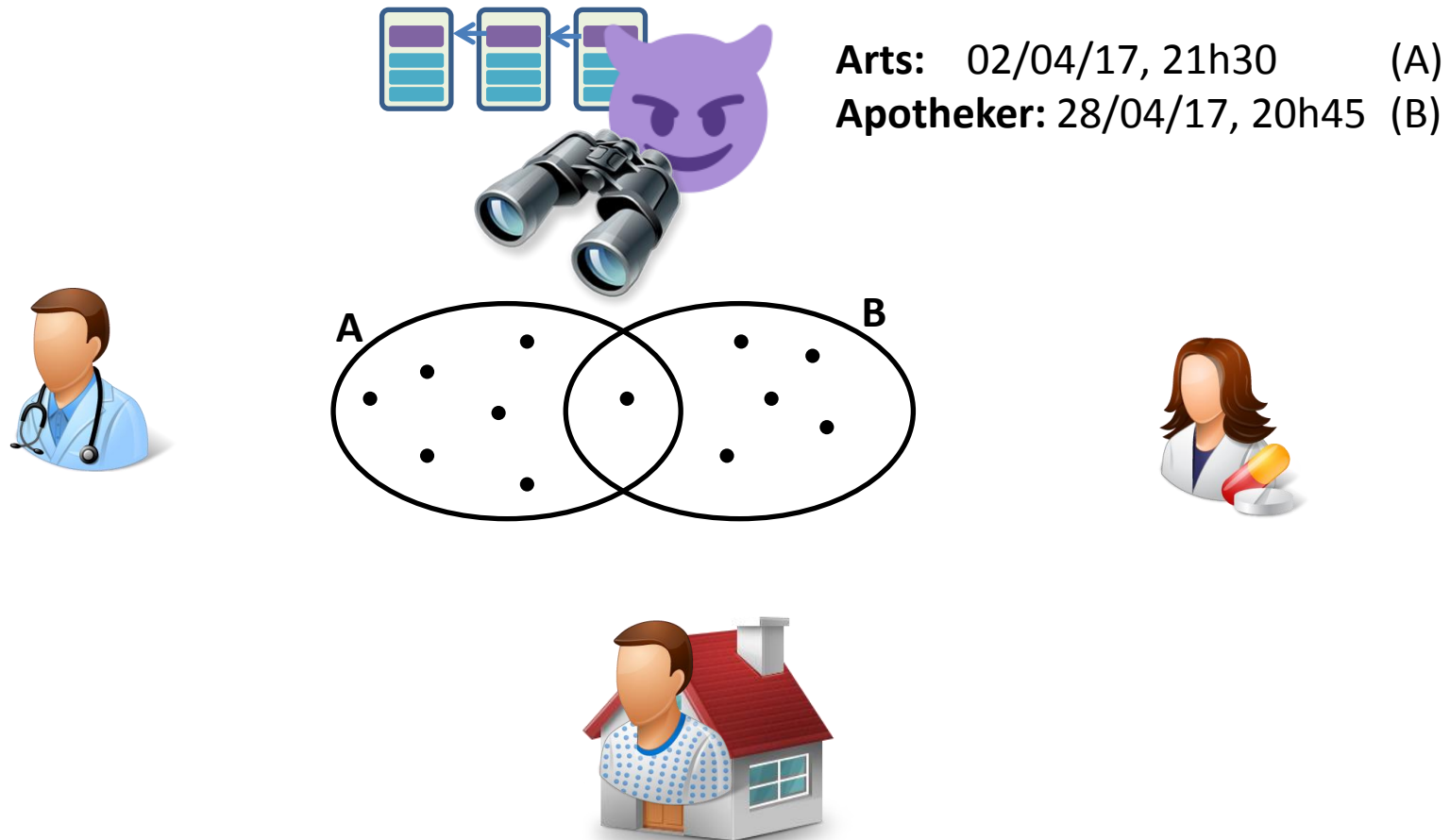
Sleutelbeheer



Goede bescherming sleutels vereist!

Link Aanval 1

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



Link Aanval 1

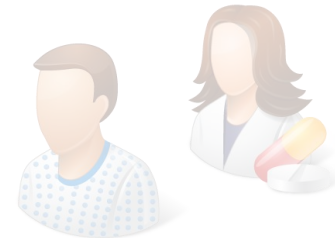
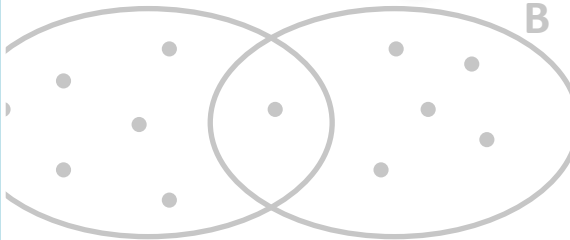
Combineren info fysieke wereld & blockchain kan data lekken
Aanvaller kent identiteit patient & observeert hem fysiek

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



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



Mijn 

Voorschrift

Pantoprazol 20mg 

True 

...

Mijn 

Voorschrift

Pantoprazol 20mg 

??? 

...


De rest van de wereld

Voorschrift

??? 

??? 

...



De **West**vlaamse
apothekersvereniging 

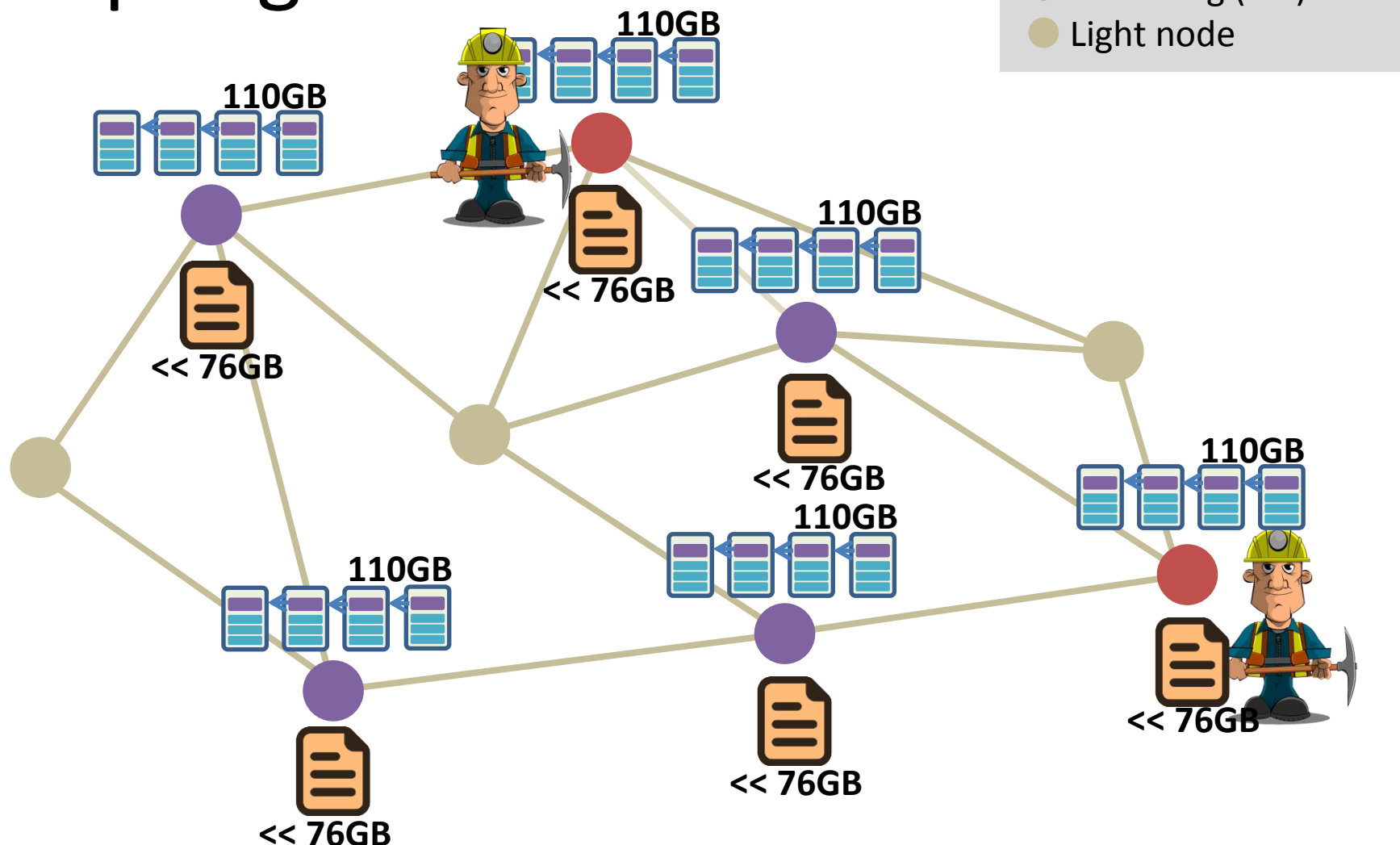
    

... 

Socialistische Mutualiteiten

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

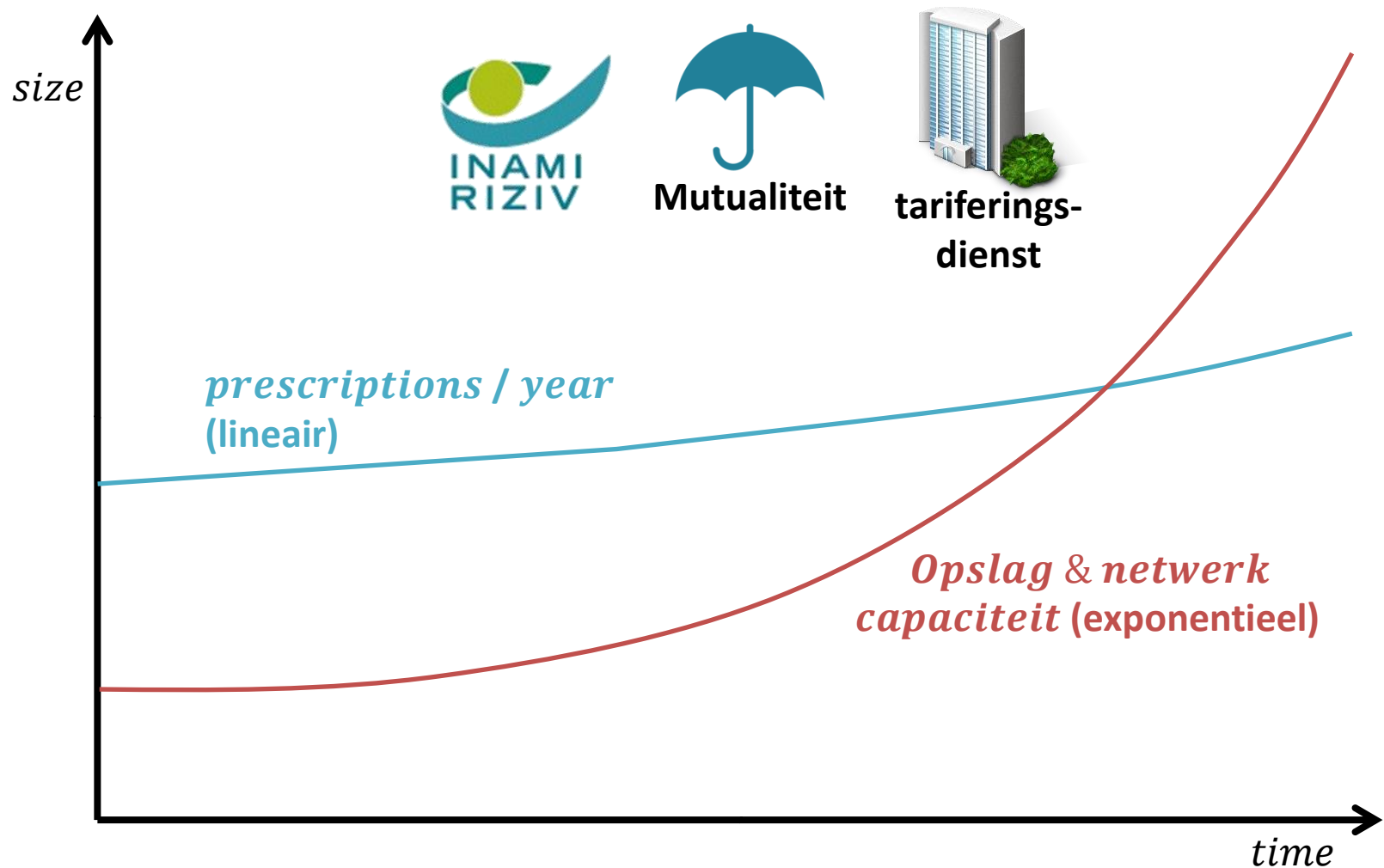
Opslag



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

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

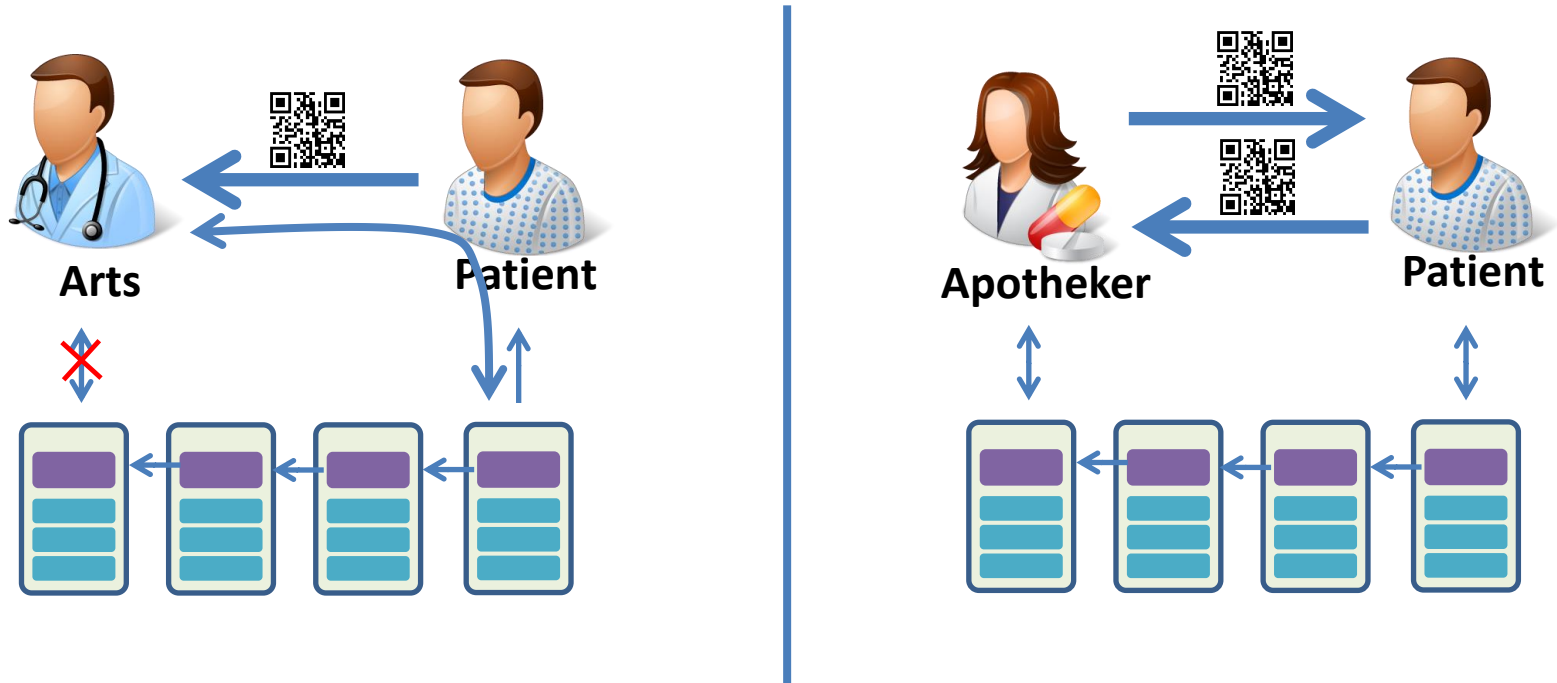
Blockchain Grootte



Mettertijd wordt de blockchain grootte minder een issue

Geen Internettoegang...

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

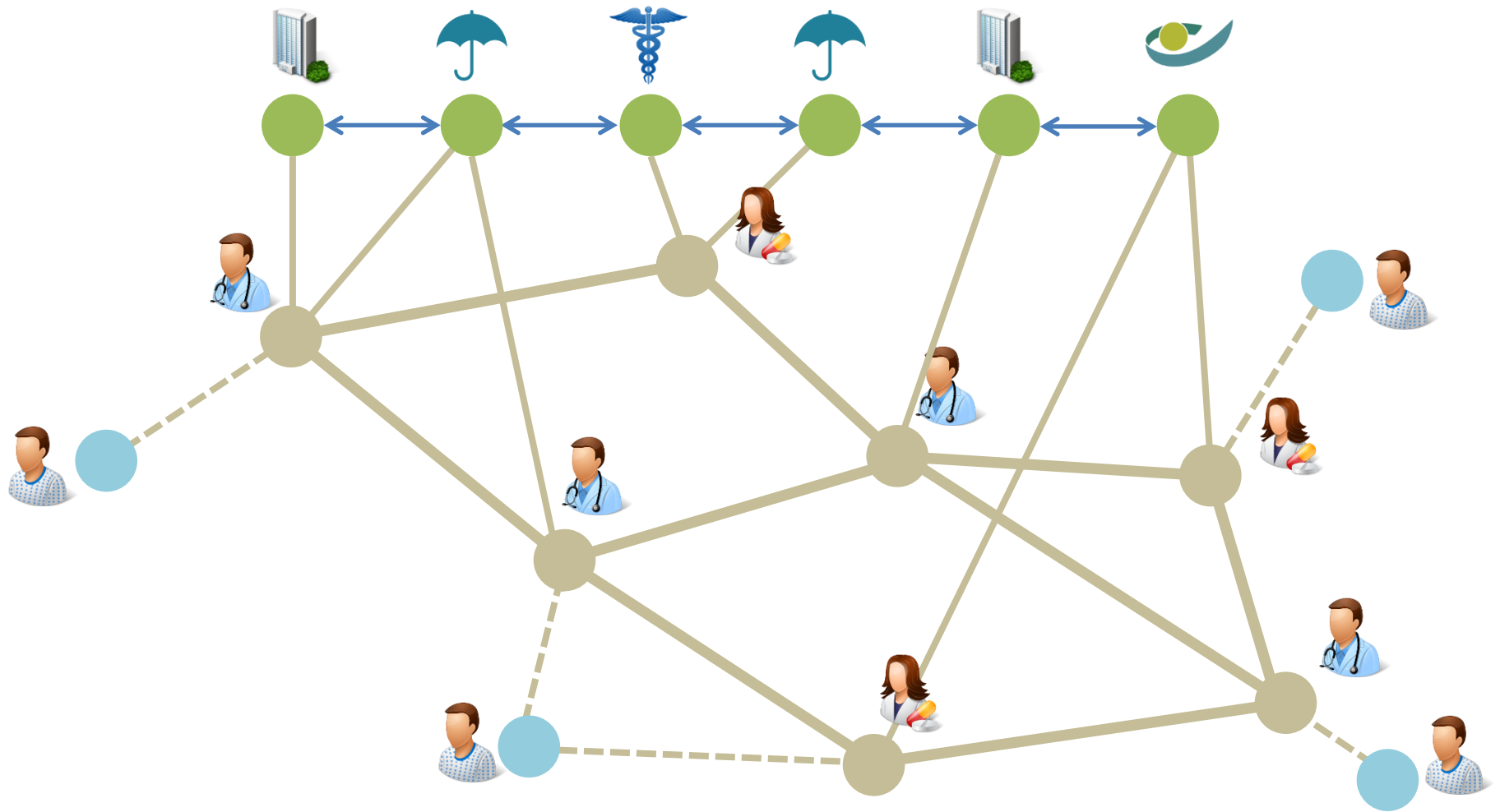


Eén van beide partijen geen internet?

De andere partij plaatst transactie op blockchain

=> Gratis redundantie

e-Voorschrift Blockchain Network



Blokcreatie

Door RIZIV, mutualiteiten en/of tarifieringsdiensten
Vb 1. Enkel RIZIV → Hoge blokfrequentie
Vb 2. Handtekening door 3 van de 7 mutualiteiten

Proof of Concept

Platform



ethereum

Smart contract



solidity

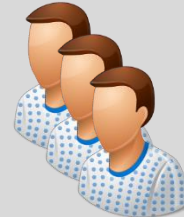
Web Clients



JavaScript



Virtuele Machines



App (Light client)

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

Demo Prescs x

```
1 pragma solidity ^0.4.2;
2 contract test
3 {
4     address riziv;
5     address collegeOfPhysicians;
6     address[] insurers;
7     address[] invoffices;
8     address[] physicians;
9     address[] pharmacists;
10
11     uint nextPrescriptionId;
12     mapping(uint => Prescription) prescriptions;
13
14     struct Prescription{
15         string drug; // set by physician
16         address patient; // set by patient
17         address delegate; // set by patient
18         address pharmacist; // set by patient
19         uint expDate; // set by physician
20         bool filled; // set by pharmacist
21         bool insured; // set by insurer
22     }
23
24     modifier isRiziv(address _sender){if(_sender != riziv){
25         modifier isCollegeOfPhysicians(address _sender){if(
```

Optimization ☒ Auto Compile
Compile

Attach Transact
Transact (Payable) Call

Prescs:test 9312 bytes
At Addr... Cre

Bytecode 60606040523415

Interface [{"constant":false,

Web3 deploy
var prescs_testC
var prescs_test
{
 from: web3.
 data: '0x60
 gas: '47000
}, function (
 console.log(
 if (typeof c
 console

```

1  pragma solidity ^0.4.2;
2  contract test
3  {
4      address riziv;
5      address collegeOfPhysici
6      address[] insurers;
7      address[] invoffices;
8      address[] physicians;
9      address[] pharmacists;
10
11     uint nextPrescriptionId;
12     mapping(uint => Prescrip
13
14     struct Prescription{
15         string drug;
16         address patient;
17         address delegate;
18         address pharmacist;
19         uint expDate;
20         bool filled;
21         bool insured;
22     }
23
24     modifier isRiziv(address
25     modifier isCollegeOfPhys
26

```

■ Attach ■ Transact ■ Transact (Payable) ■ Call

```
▼ Prescs:test 9312 bytes
```

At Address

Bytecode	6060604052341561000c57fe5b5b33600c
----------	------------------------------------

Interface

```
[{"constant":false,"inputs":[{"name":"p"
```

```
Web3 deploy
```

```
var prescs_testContract = web3.eth.con  
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



Interface



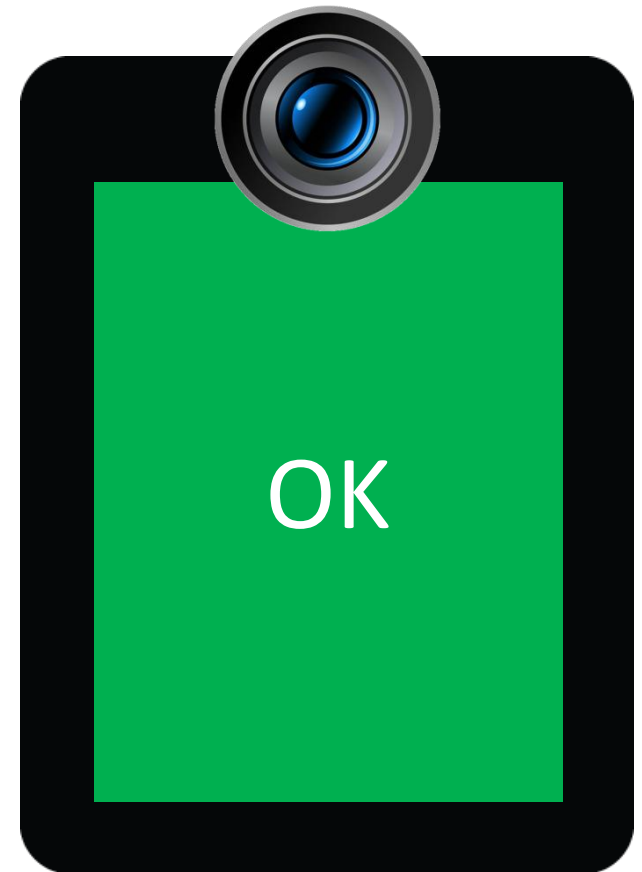
Interface



Interface - Dispense



Apotheker



Interface - Dispense

Apotheker

Drug	Refund	Processed
☒ Adalimumab 5mg	15,30€	☒
☒ Pantoprazol 20mg	9,13€	☒

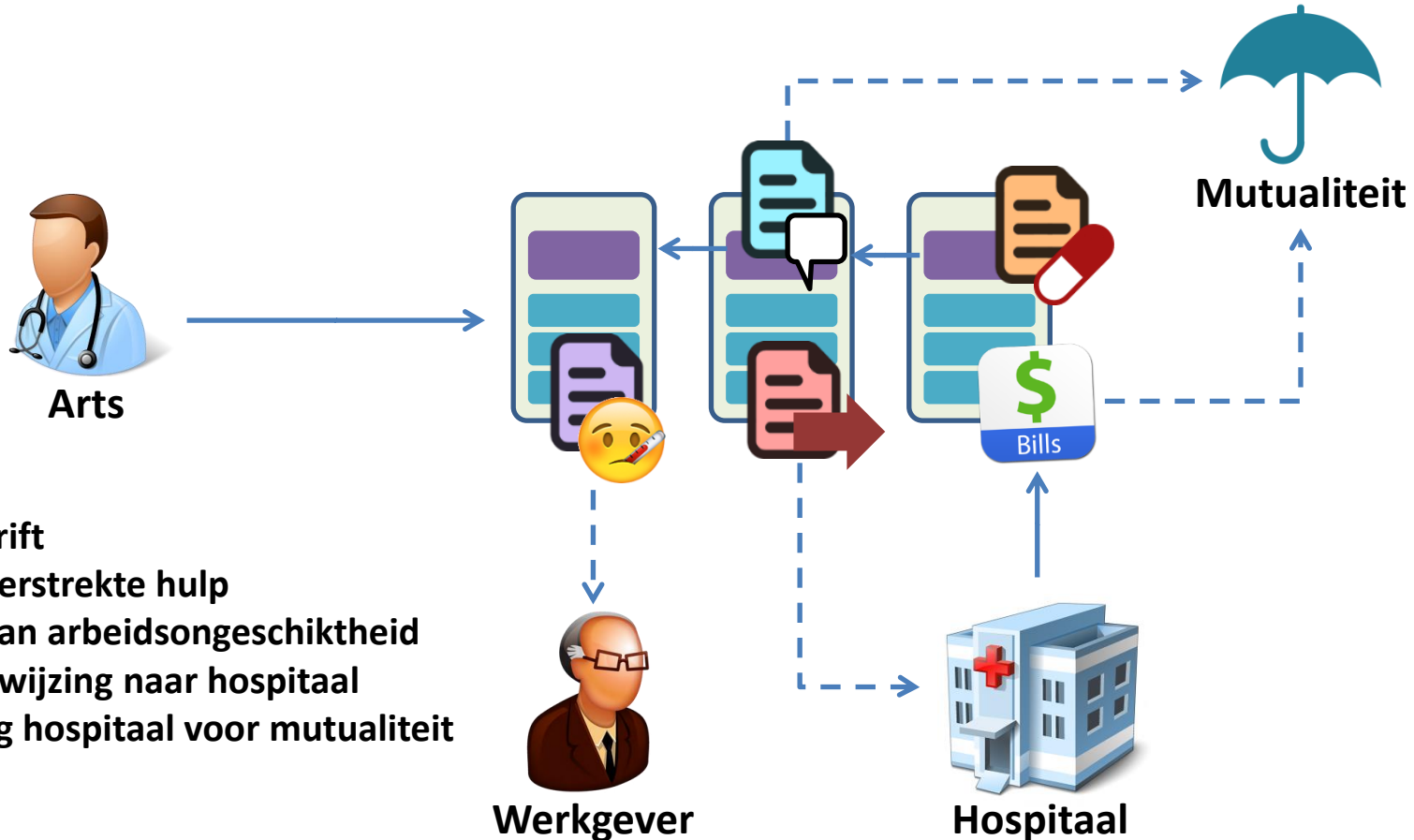
Process

Interface - Dispense



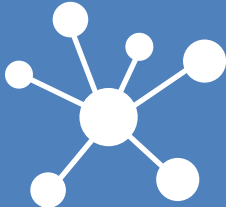
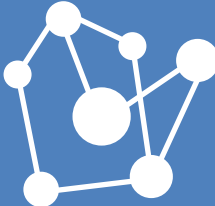
The bigger picture

Een Blockchain Ecosysteem



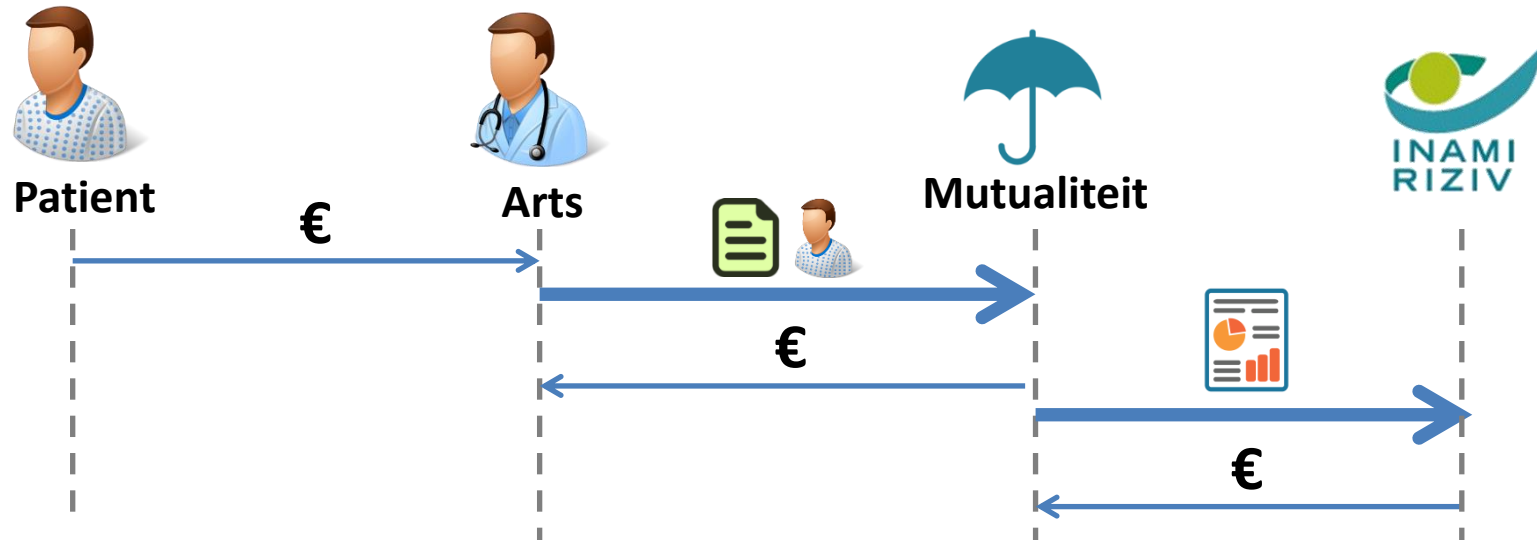
Eén medische consultatie kan een hele set acties in gang zetten,
met blockchain als centrale as.

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



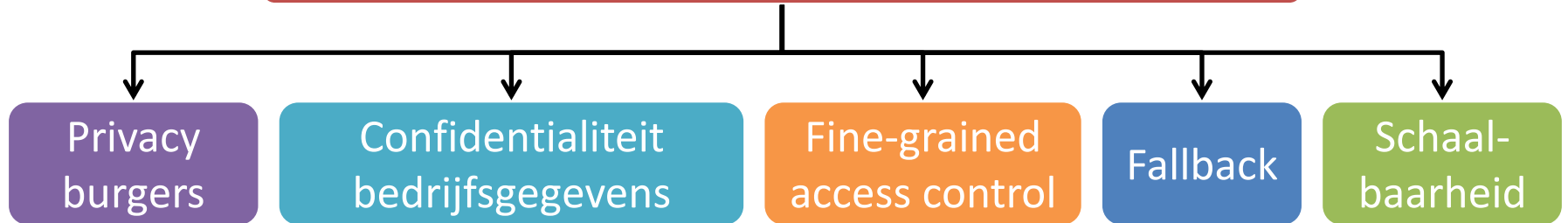
**Probleem: Arts kan onbestaande consultaties aangeven
→ moeilijk detecteerbare fraude**

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

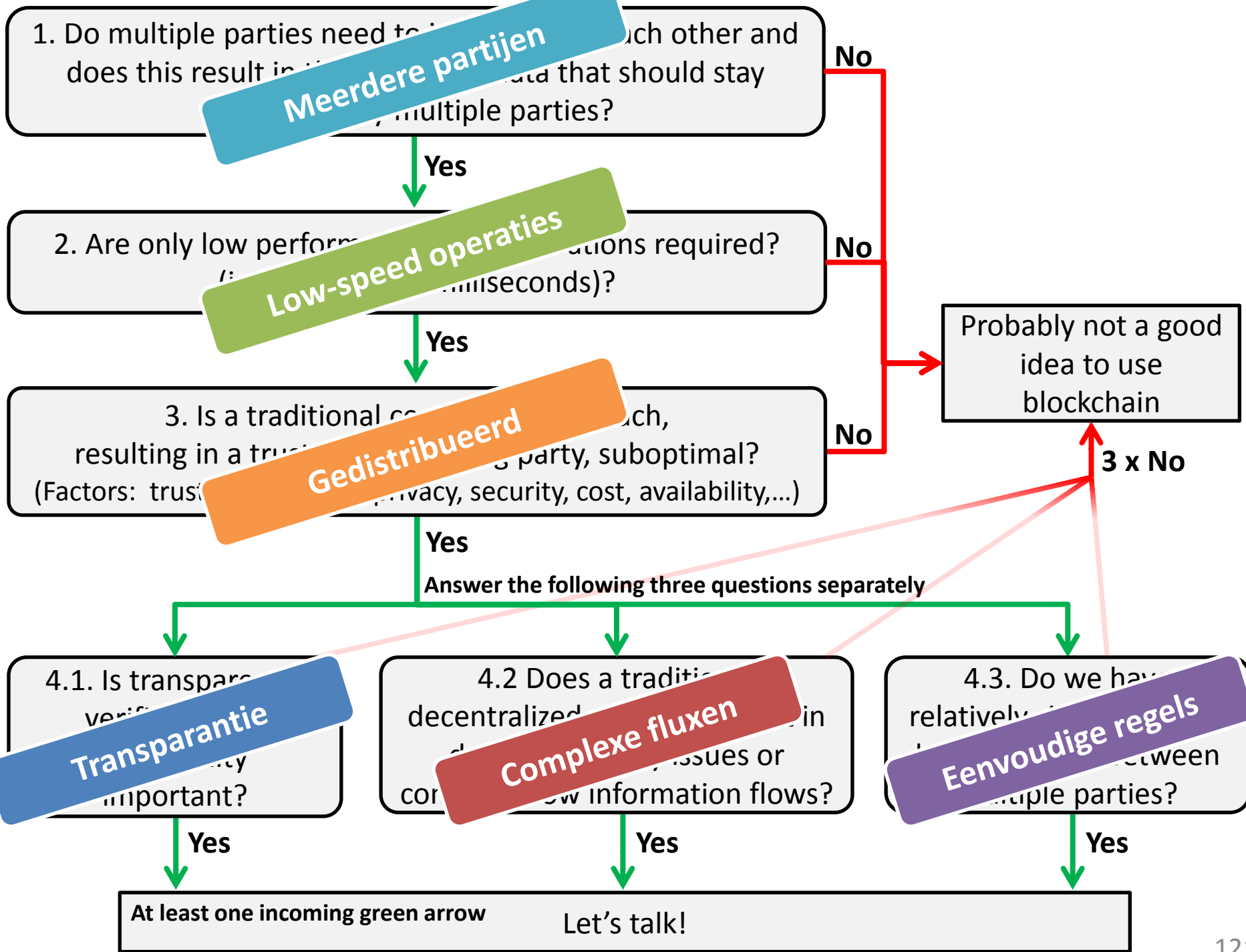
Lessen & Conclusies

Nauwgezette case by case analyse onontbeerlijk



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 interact with each other and does this result in the storage of data that should stay accessible by multiple parties?

Yes

2. Are only low performance write operations required?
(in seconds, not milliseconds)?

Yes

3. Is a traditional centralized approach, resulting in a trusted, all-known entity?
(Factors: trust, governance, privacy)

Yes

4.1. Is transparency, verifiability or auditability important?

Yes

de
cor



Yes

4.3. Do we have relatively simple & static business rules between multiple parties?

Yes

At least one incoming green arrow

Let's talk!

No

No

No

Probably not a good idea to use blockchain

3 x No

separately

<https://www.smalsresearch.be/beslissingmodel-wanneer-blockchain-gebruiken/>

Afronding

Blockchain 1.0



Pauze

Blockchain 2.0



Mentaal Model

Blockchain 1.0



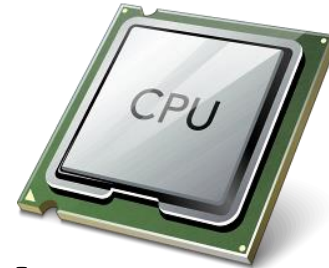
**Autonome
opslag**



**Autonome
computer**

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

Blockchain 2.0



**Autonome
rekenkracht**



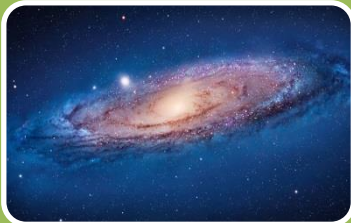
Correcte werking,
zelfs met oneerlijke en/of
onbeschikbare nodes

Conclusies



Nieuw paradigma

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



Geen oplossing voor alles

- Het kan met blockchain $\neq$ 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



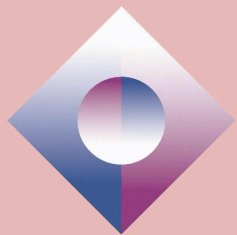
@KristofVerslype



be.linkedin.com/in/verslype



Smals



www.smals.be



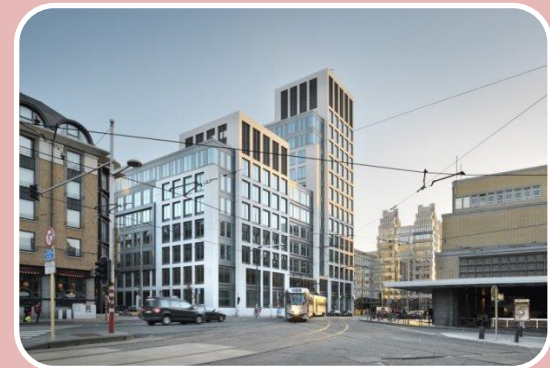
@Smals_ICT



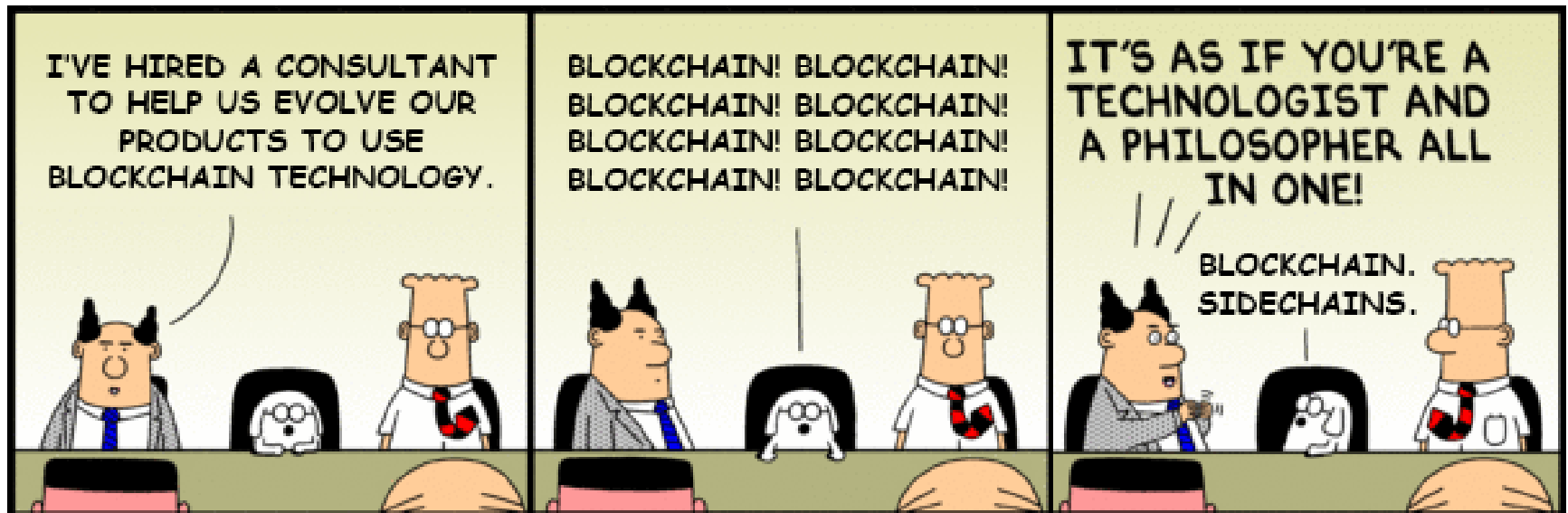
www.smalsresearch.be



@SmalsResearch



Dilbert



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 Integrations**. 2017.
<http://solidity.readthedocs.io/en/latest/#available-solidity-integrations>