

From Blockchain to Reality



Cases • ervaringen • lessons learned

AGENDA

Blockchain
Een snelle intro

Cases nationaal
& internationaal

Reality check

Onze aanpak

BeSure

AGENDA

Blockchain
Een snelle intro

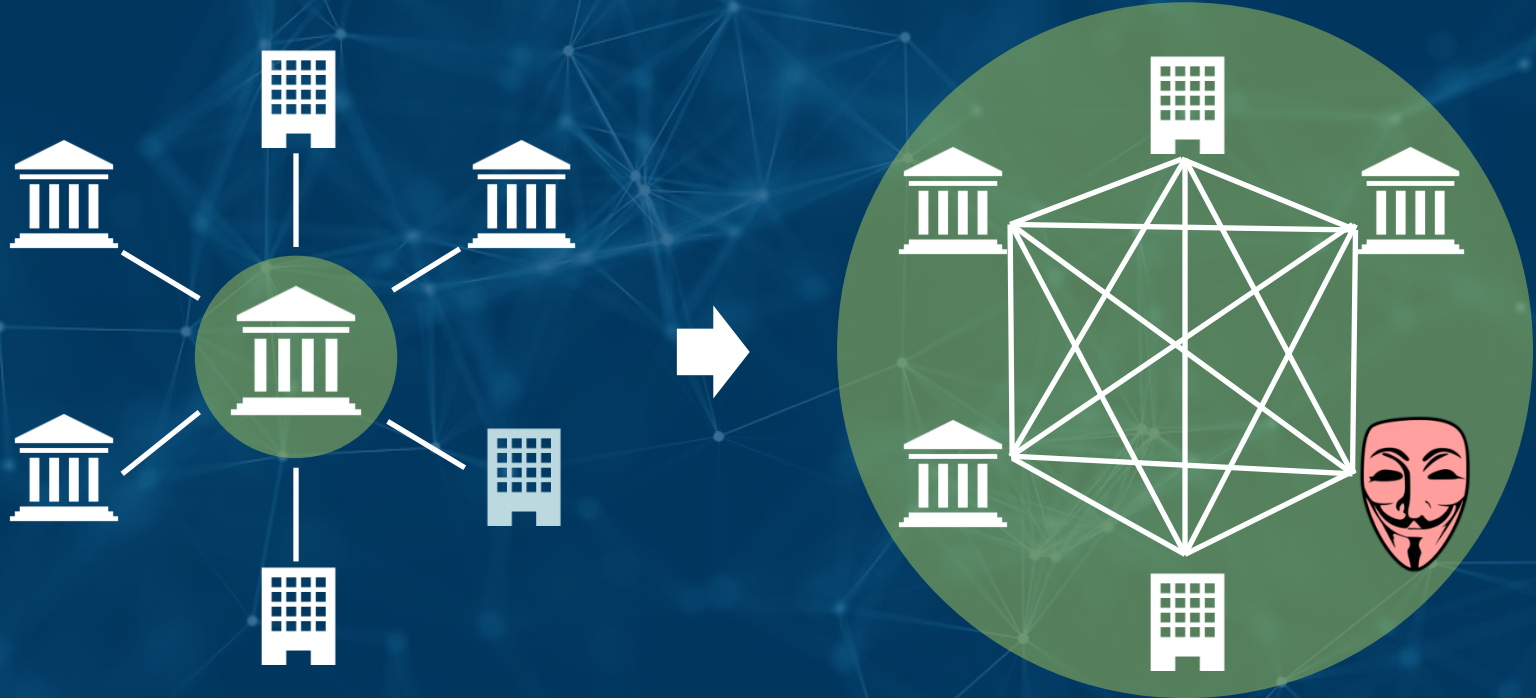
Cases nationaal
& internationaal

Reality check

Onze aanpak

BeSure

Blockchain gaat over **vertrouwen**



HET BLOCKCHAIN NETWERK KAN HELPEN BIJ:

Registratie feiten

Transfereren activa

Afdwingen regels

Idee

Ik transfereer
0,4 BTC naar .



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

Bob

Ok!



Dave

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

Ok!



Alice

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

Ok!



Charlie

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

Idee

B

Geldig

Enkel geldige transacties aanvaard door netwerk
Vb. Bob is eigenaar van geld en heeft nog niet uitgegeven

L

O

Atomisch

Iedereen aanvaardt transactie of niemand
→ Consensus mechanisme

C

K

**Snel &
goedkoop**

Dit is relatief

C

H

Veilig

Het systeem blijft correct werken, zelfs indien deel van de
participanten oneerlijk of onbeschikbaar

A

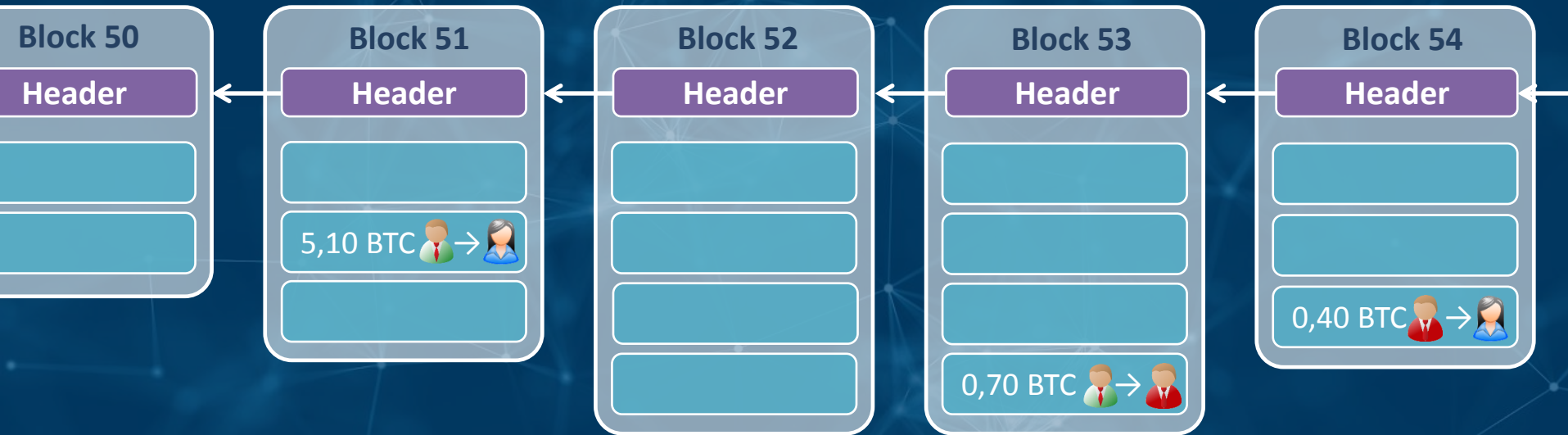
I

N

Gedistribueerd

Geen nood aan een centrale partij bij uitvoering

Een ketting van blokken



Aaneenschakeling van blokken, die op hun beurt transacties bevatten

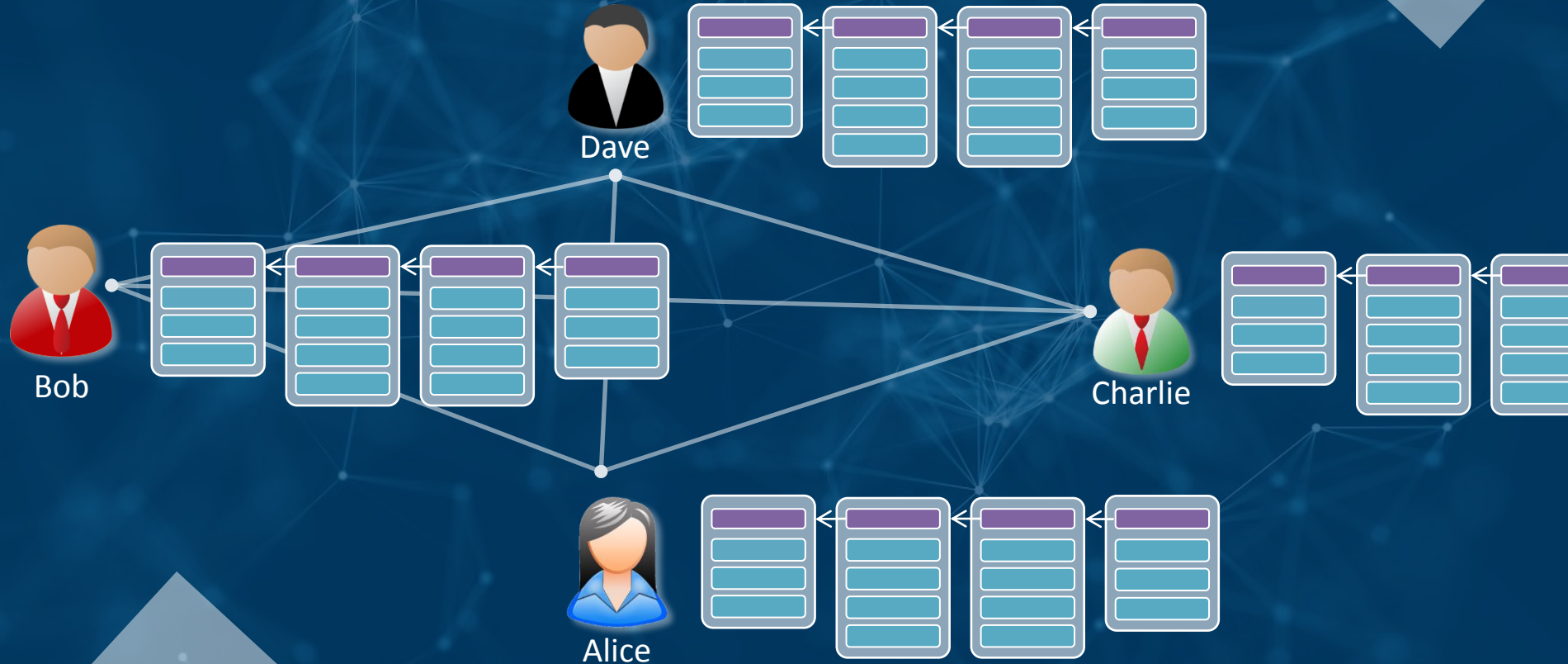
Aan streeffrequentie worden nieuwe blokken met meest recente transacties toegevoegd aan blockchain

Blockchain bevat ALLE transacties

Transacties in blockchain onverwijderbaar

Vele entiteiten bezitten dezelfde kopie van de blockchain

Idee



Pseudoniemen & sleutels

Not

0,40 BTC



but

0,40 BTC



Vereist om transactie te ondertekenen namens het overeenkomstige pseudoniem

This is the

*PIN,
ret.
ling
ints.*



5Ked81nsjhxanZWMtsF1cXo6M
JUf8ppsWU43EgFr76Ve15U7aVY

online import: <http://blockchain.info/wallet>

This is the

public address.

Use it to check the balance.

*Like an **account number**,
share it with anyone
to receive coins.*



1HJ8C1iGhoVpnqUEp
69LpxdB67gysmVrw

made with: <http://bitaddress.org>

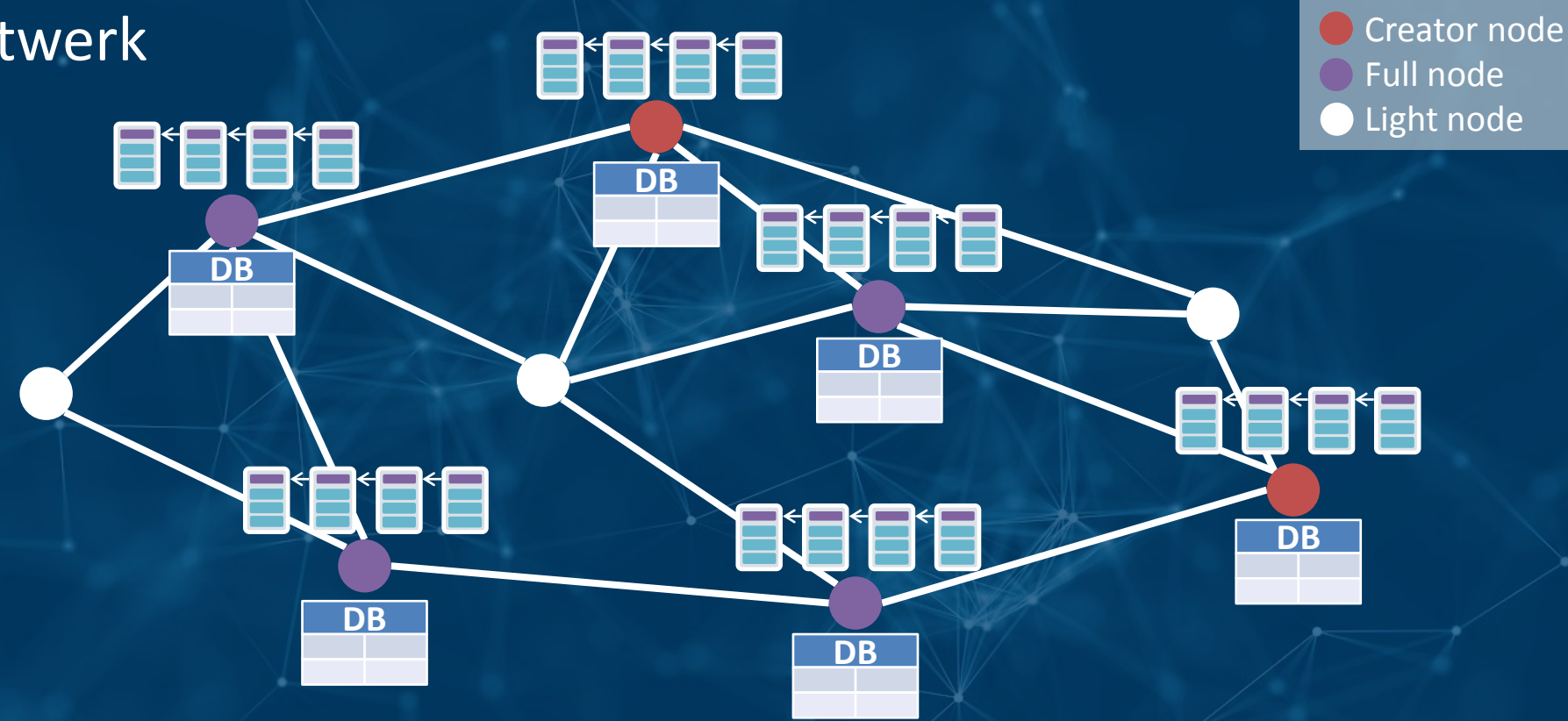


***bitcoin
paper wallet***

private key folded inside!

<http://bitcoin.ars.is>

Network

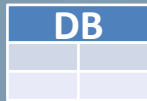


Blockchain



Append-only
Historiek

Database



Relevante info
Meest actuele status

PERMISSIONLESS

Publiek / open

Vergelijk met
Internet



Publiek toegankelijk en bruikbaar

Kan erg energie-inefficiënt zijn

Trager

Trust gedistribueerd

Virtueel geld vereist



PERMISSIONED

Enterprise / Consortium

Vergelijk met
extranet



Extra laag voor toegangscontrole

Energie-efficiënter

Sneller (meer tx/s, meer blocks/s)

Trust gedecentraliseerd

Geen virtueel geld vereist



MultiChain



HYPERLEDGER



Quorum

Smart contracts

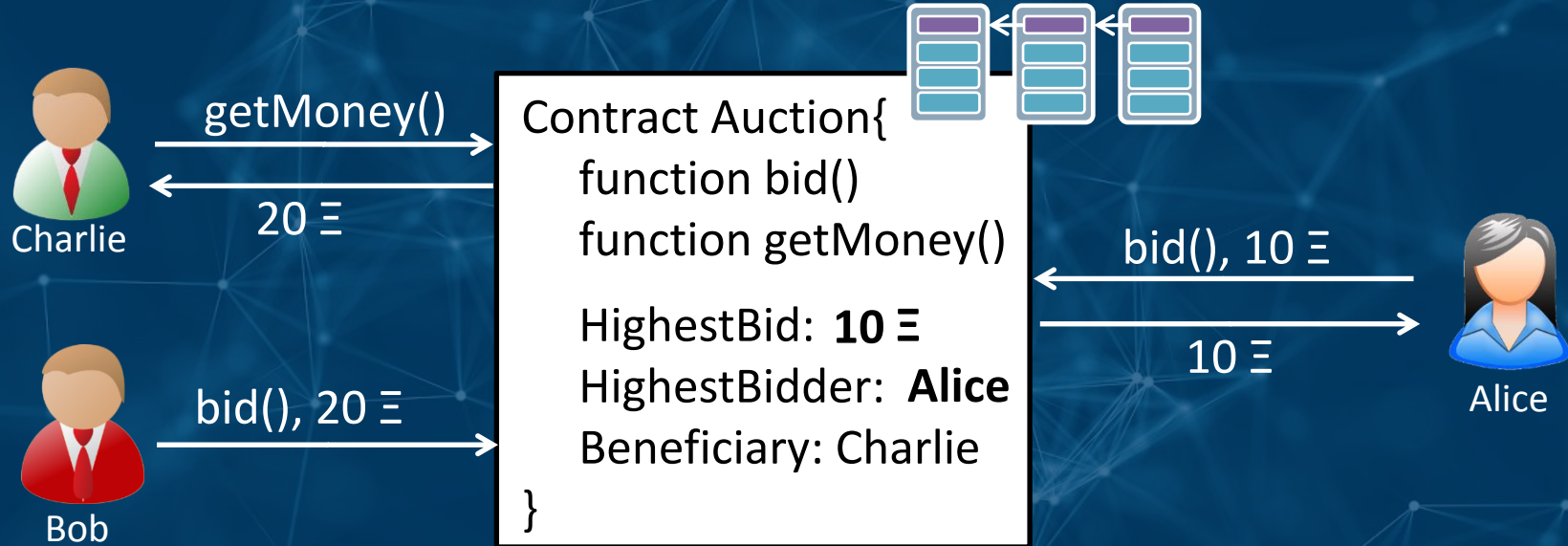
**Automatiseren & afdwingen van
regels / afspraken**

**Tussen partijen die elkaar niet 100%
hoeven te vertrouwen**

**Zonder afhankelijkheid
van een centrale partij**

Smart contracts

Ether (Ξ) is de virtuele munt op Ethereum



Kan waarde ontvangen,
blokkeren en transfereren

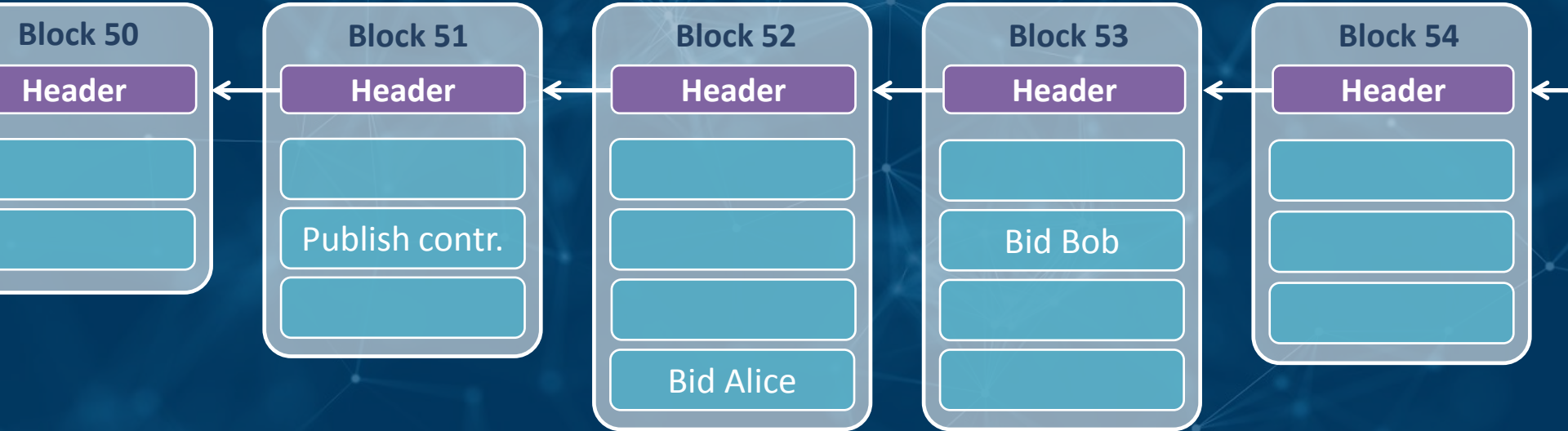
Geen enkele entiteit kan eenzijdig
correcte uitvoering beïnvloeden

Reactief

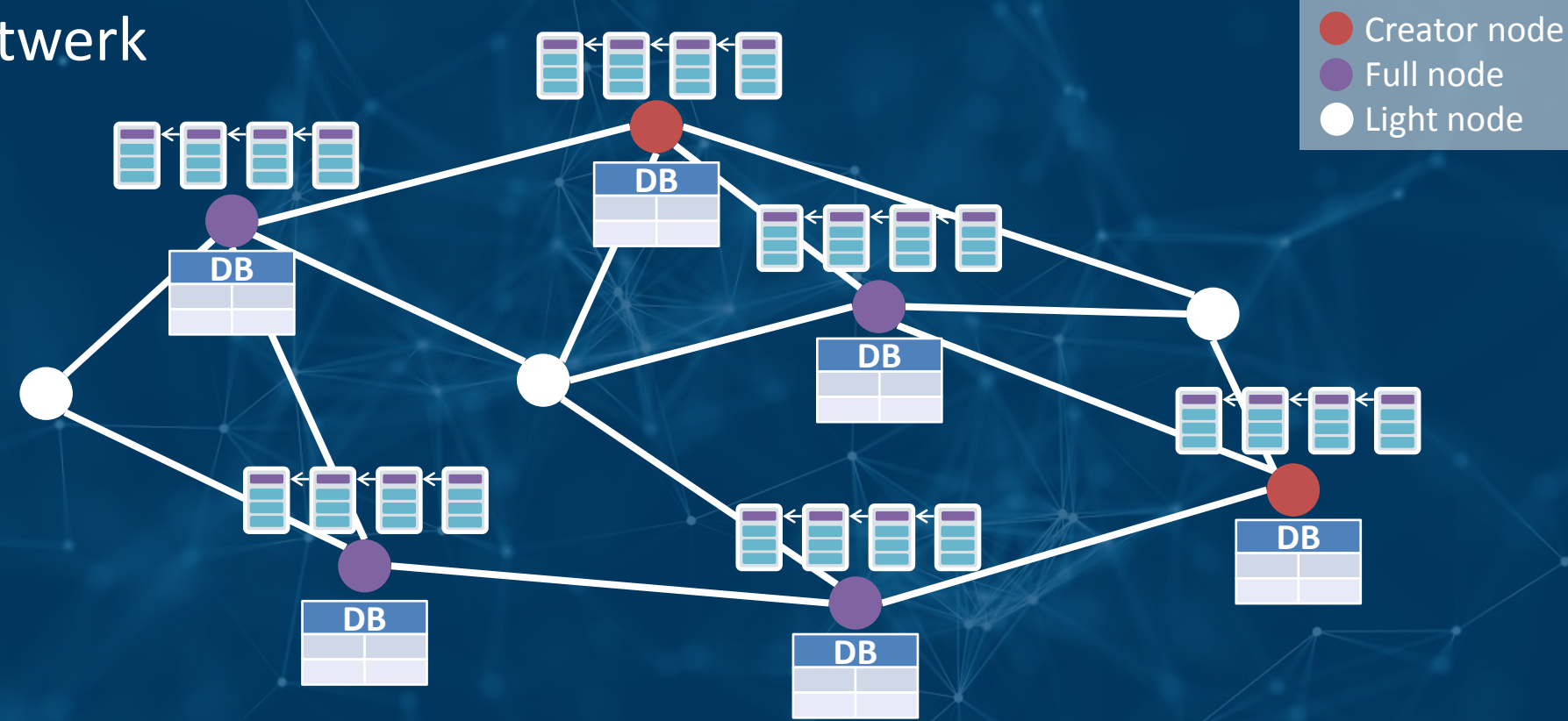
Doof & blind

Smart contracts

Alle activiteit gerelateerd met het smart contract gebeurt d.m.v. transacties op de blockchain



Network

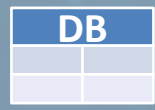


Blockchain



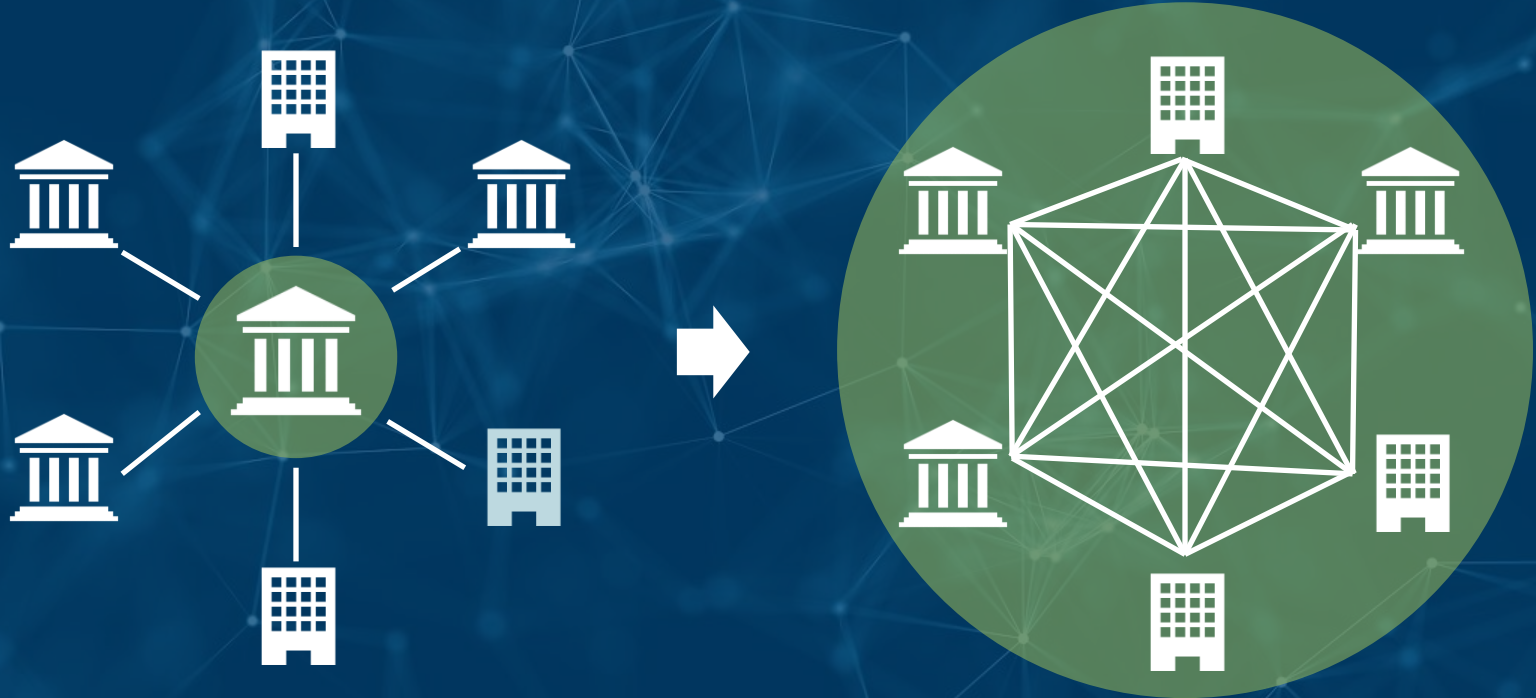
Append-only
Historiek

Database



Relevante info
Meest actuele status

Blockchain gaat over **vertrouwen**



HET BLOCKCHAIN NETWERK KAN HELPEN BIJ:

Registratie feiten

Transfereren activa

Afdwingen regels

Alles wat met blockchain kan, kan beter met een gecentraliseerde benadering

WAAROM BLOCKCHAIN?

Een gecentraliseerde benadering is niet steeds wenselijk

Politiek
(Vb. cross-border
uitwisselingen)

Afwezigheid vertrouwde
autoriteiten
(Vb. Bitcoin)

Misbruik (quasi-)
monopolieposities

Illegale activiteiten
(Vb. Dark Web)

ANDERE AAN BLOCKCHAIN TOEGESCHREVEN VOORDELEN OOK MOGELIJK MET ANDERE TECHNOLOGIEËN

Process
automatisatie

Consistentie

Gestroomlijnde
processen

Real-time
updates

Inzicht in
beslissingsproces

Is het een probleem dat een centrale partij vertrouwd moet worden, dat we er dus afhankelijk van zijn?



AGENDA

Blockchain
Een snelle intro

Cases nationaal
& internationaal

Reality check

Onze aanpak

BeSure

Cases nationaal & internationaal

Aanvraag rolstoel

Ondersteunen
vluchtelingen

Identiteitsbeheer

Diploma's

Financiële sector

Herkomst &
toeleveringsketen



OP BASIS PUBLIEKE INFORMATIE

- Niet steeds even gedetailleerd
- Voldoende om uit te leren

Cases nationaal & internationaal

Aanvraag rolstoel

Ondersteunen
vluchtelingen

Identiteitsbeheer

Diploma's

Financiële sector

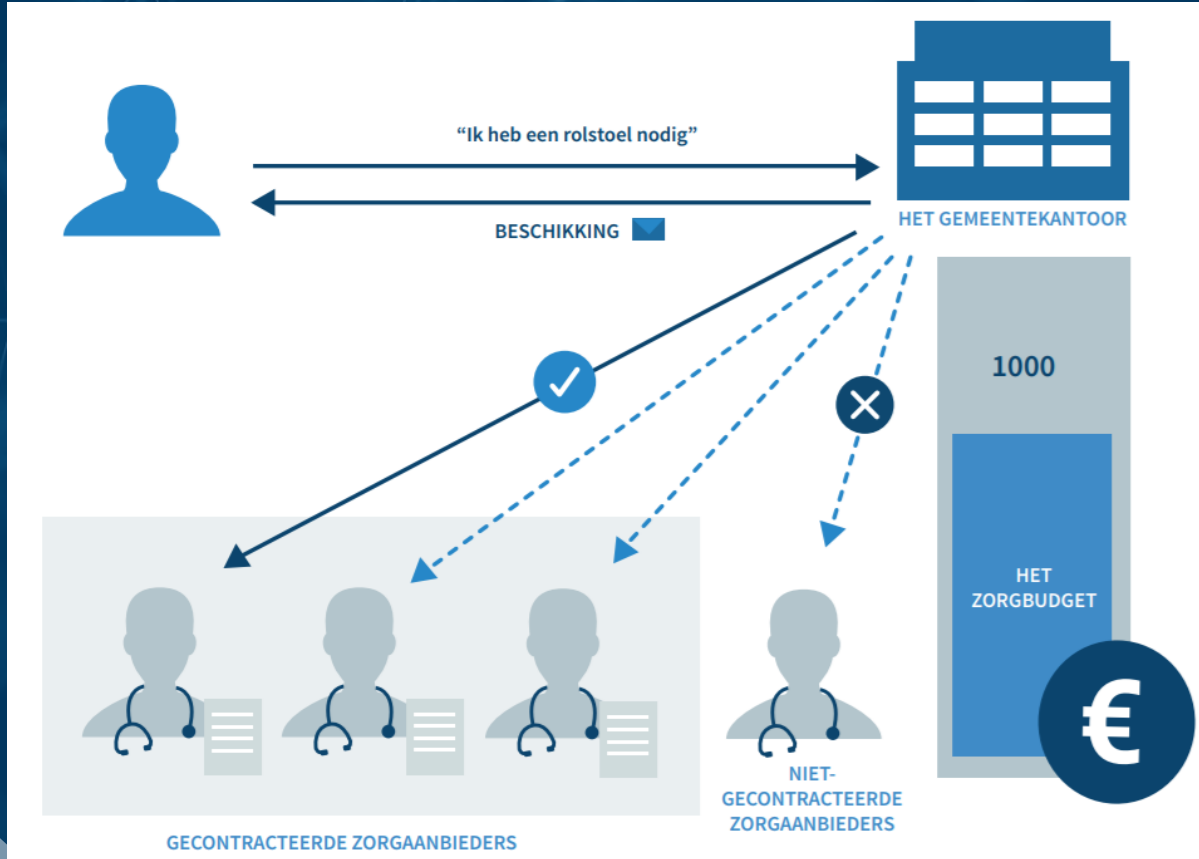
Herkomst &
toeleveringsketen



OP BASIS PUBLIEKE INFORMATIE

- Niet steeds even gedetailleerd
- Voldoende om uit te leren

Aanvragen rolstoel (NL)



Aanvragen rolstoel (NL)

	PUBLIC BLOCKCHAIN	PRIVATE BLOCKCHAIN	CENTRAL DATABASE
EIGEN SERVER NODIG	NIEMAND	GEMEENTE & ZORGLIVERANCIERS	GEMEENTE
CONTROLE DAT DATA NIET VERANDERT	GEMEENTE & ZORGLIVERANCIERS	GEMEENTE & ZORGLIVERANCIERS	GEMEENTE
€ / ACTIE	HOOG	AFWEZIG	AFWEZIG
IMPLEMENTATIE COMPLEXITEIT	MIDDEL	HOOG	LAAG
BEVEILIGING TEGEN DATA MANIPULATIE	HOOG	VRIJ HOOG	NORMAAL
BEVEILIGING TEGEN DATA LEZEN	HOOG		
AUDIT (WIE LAS DATA WANNEER)	ONMOGELIJK		
EERST POC			

Weegt de extra complexiteit op tegen het vertrouwensvoordeel dat de gemeente de data niet kan wijzigen ? Wellicht zorgleveranciers geen vragende partij

The diagram shows a central figure (a person) connected by arrows to eight different property icons. The arrows are labeled "Registratie". The properties are categorized as SHM (Social Housing Medium) or SVK (Social Rental Housing). The connections are as follows:

- Top: SHM (Building icon)
- Top-left: SVK (House icon)
- Top-right: SVK (House icon)
- Right: SHM (Building icon)
- Bottom-right: SVK (House icon)
- Bottom: SVK (House icon)
- Bottom-left: SHM (Building icon)
- Left: SHM (Building icon)

Legend: SVK: Sociaal verhuurkantoor

SVK: Sociaal verhuurkantoor
SHM: Sociale huisvestingsmaatschappij

- Burger registreert meermaals
- Niet transparant: *“Waarom ben ik nog niet aan de beurt?”*

Sociale huisvestingsmaatschappijen
geen vragende partij: **Toegenomen
complexiteit, kost, onderhoud**
→ **Liever gecentraliseerd**



Het distribueren van vertrouwen d.m.v. blockchain technologie
Kan gepaard gaan met verhoogde complexiteit en verhoogde kosten
($\leftrightarrow$ de blockchain belofte)

Cases nationaal & internationaal

Aanvraag rolstoel

Ondersteunen
vluchtelingen

Identiteitsbeheer

Diploma's

Financiële sector

Herkomst &
toeleveringsketen



OP BASIS PUBLIEKE INFORMATIE

- Niet steeds even gedetailleerd
- Voldoende om uit te leren

Ondersteunen vluchtelingen (1)



Cash-for-food programma

- Helpt 100 000 Syrische vluchtelingen in Jordaanse vluchtelingenkampen
- Transactiekosten, die nu naar lokale banken gaan, met 98% verminderd





Sterke kostenreductie mogelijk

Ondersteunen vluchtelingen (2)



Prepaid Mastercard (Finland)

- Gekoppeld aan digitale identiteit op blockchain
- Op blockchain financiële transactiehistoriek

Voordelen

- Uitgeven en ontvangen geld (zonder echte bankrekening)
- Betere begeleiding → betere integratie
- Minder frauderisico

Privacy bezorgdheden

Financiële historiek kan misbruikt worden om gedrag vluchtelingen te analyseren en tegen hen te gebruiken.

~ blockchain experiment UK 2016 voor traceren uitgaven uitkeringsgerechtigde mindervaliden & werklozen

Ondersteunen vluchtelingen (2)

Indien persoonsgegevens betrokken zijn is sterke beveiliging & heldere communicatie nodig om mogelijke bezorgdheden weg te nemen.

(Of misschien moeten we het project beter afvoeren)

Cases nationaal & internationaal

Aanvraag rolstoel

Ondersteunen
vluchtelingen

Identiteitsbeheer

Diploma's

Financiële sector

Herkomst &
toeleveringsketen



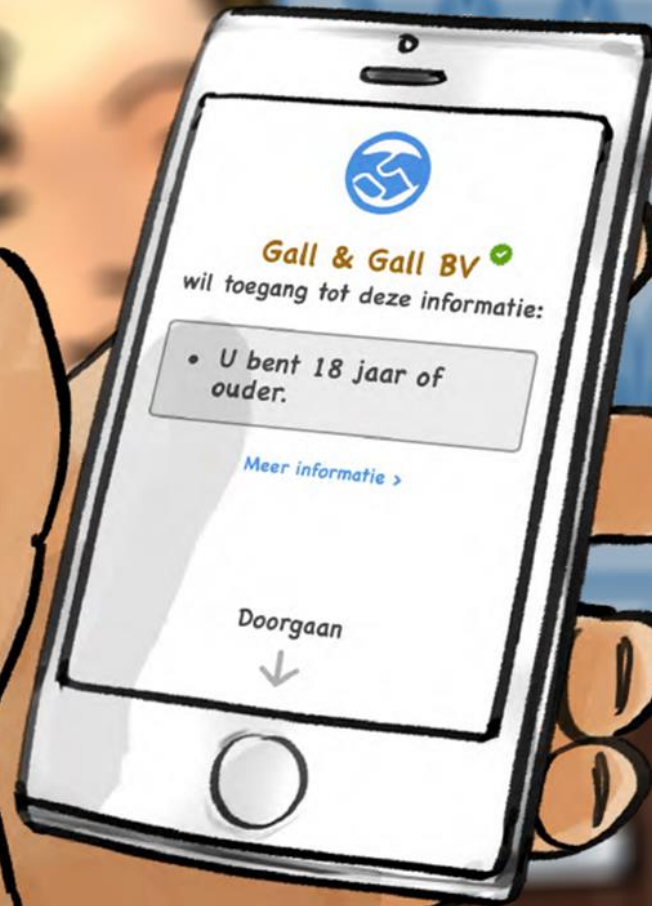
OP BASIS PUBLIEKE INFORMATIE

- Niet steeds even gedetailleerd
- Voldoende om uit te leren

*Combinatie van blockchain
technologie & zero-
knowledge proofs*

*“de combinatie van alle
informatie die op een
identiteitsbewijs zichtbaar
is kan misbruikt worden.”*

***Dit kan al sinds 2001
zonder blockchain
dankzij attribute-based
credentials (complexe
zero-knowledge proofs)***



Voordelen

- *Veiligheid & privacy voor burger*
- *Burger bepaalt zelf met wie gegevens gedeeld worden*

Positief dat naar nieuwe technologieën
zoals blockchain gekeken wordt

Niet vergeten ook alternatieve, minder zichtbare, maar
eveneens waardevolle technologieën te bekijken
(als alternatief of in synergie)

Self-sovereign identity (SSI)

DIGITALE IDENTITEIT

- Ongecertificeerde, eigen beweringen
- Gecertificeerde beweringen (Diploma's, rijbewijs, vergunningen, ...)
- Profielen op Facebook, Instagram, Twitter, ...
- Digitale persoonsgegevens in data-silo's (overheidsadministratie, gezondheidszorg, privé, ...)
- ...

SELF-SOVEREIGN IDENTITY

- Burger heeft een overzicht van zijn persoonsgegevens
 - Burger bepaalt wie wat mag zien
 - Burger kan zijn profiel verhuizen van bedrijf A naar bedrijf B
 - Burger niet afhankelijk van één bedrijf
- ↔ Finse case vluchtelingen

Complexe uitdaging die een synergie tussen technologieën kan vereisen: zero-knowledge proofs, blockchain, (Vb. Sovrin)

Identiteit ook mogelijk voor dingen & ondernemingen (Vb. Validata)

Cases nationaal & internationaal

Aanvraag rolstoel

Ondersteunen
vluchtelingen

Identiteitsbeheer

Diploma's

Financiële sector

Herkomst &
toeleveringsketen



OP BASIS PUBLIEKE INFORMATIE

- Niet steeds even gedetailleerd
- Voldoende om uit te leren

Diploma's

Mobielere
burgers
(studie & werk)

Burger wil
geselecteerde
diploma's kunnen
tonen

Werkgever wil
onvervalsbare
diploma's

Opvragen bij
scholen
tijdrovend

Beheer
onpraktisch

Situatie vandaag:
Geen dienst op
Europees niveau



**INFORMATIE
VLAANDEREN**



**FÉDÉRATION
WALLONIE-BRUXELLES**



Vlaanderen
is onderwijs & vorming
AHOVOKS

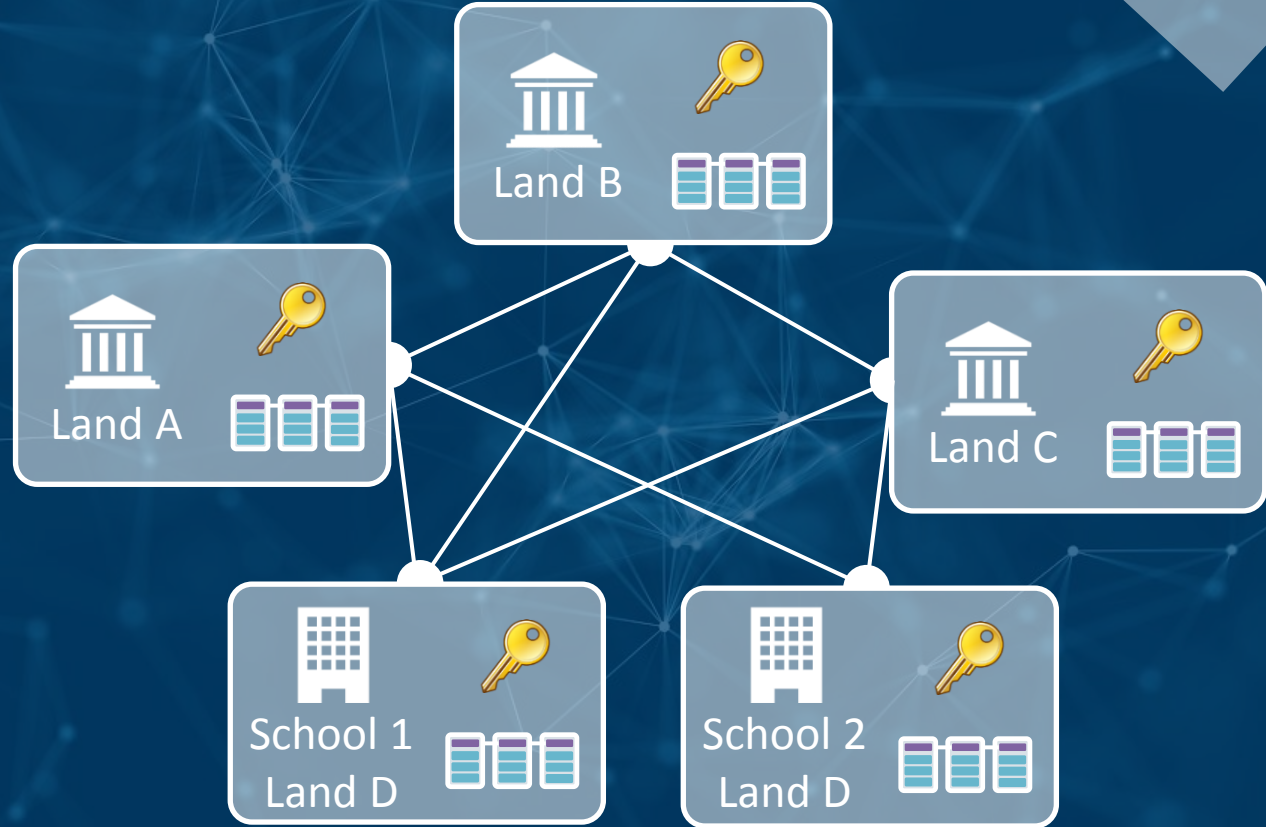
THELEDGER.

Diploma's – 1^e PoC

Burgers &
werkgevers buiten
blockchain
netwerk

Scholen &
overheden kunnen
diploma's
toevoegen

Burgers behouden
overzicht &
bepalen wie wat
hoe lang mag zien
(d.m.v. access link)



Diploma's – 1^e PoC

Alle diploma-info onvercijferd op blockchain



We moeten ALLE
participanten in
netwerk vertrouwen
(misbruik, diefstal)



GDPR genegeerd:
Recht op vergetelheid,
Passende beveiliging



Concurrerende scholen
zien elkaars gegevens
(confidentialiteit)

Nadenken over gebruik blockchain



Belang *privacy by design & security by design*

Valse Dichotomie

GECENTRALISEERDE BENADERING



BLOCKCHAIN BENADERING

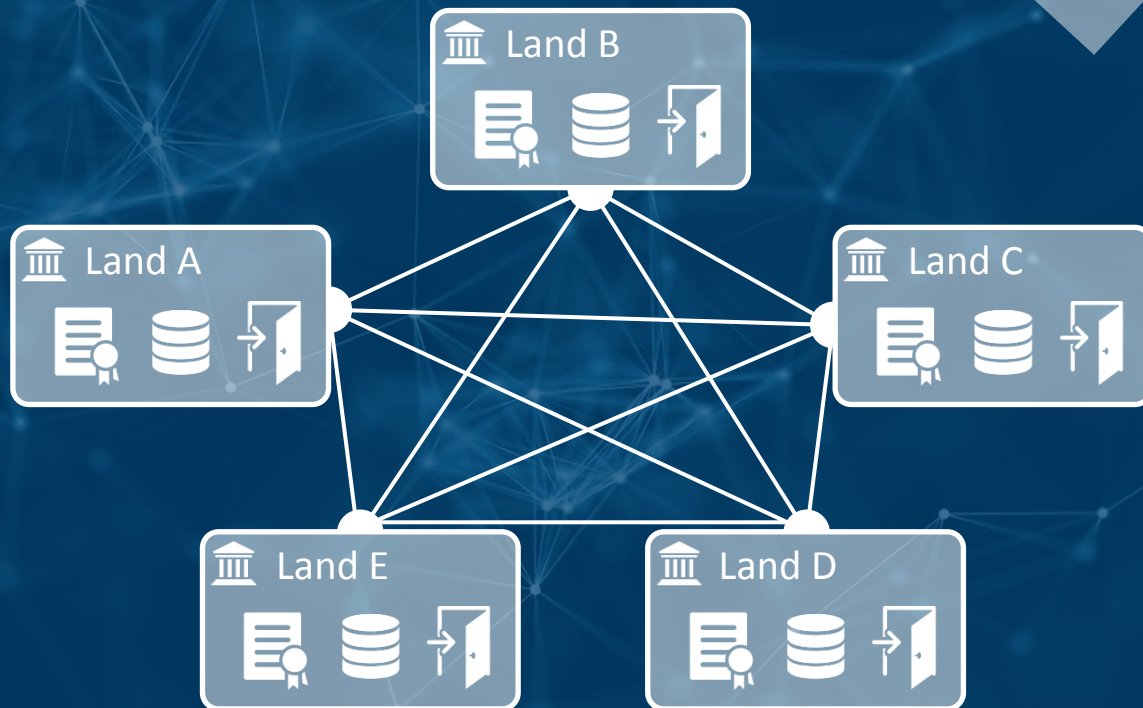


Er kunnen meer opties zijn dan deze twee

Valse Dichotomie

Voorbeeld 3^e optie

Elk land eigen
gecentraliseerde dienst
met toegangscontrole &
database met eigen
diploma's



Cases nationaal & internationaal

Aanvraag rolstoel

Ondersteunen
vluchtelingen

Identiteitsbeheer

Diploma's

Financiële sector

Herkomst &
toeleveringsketen

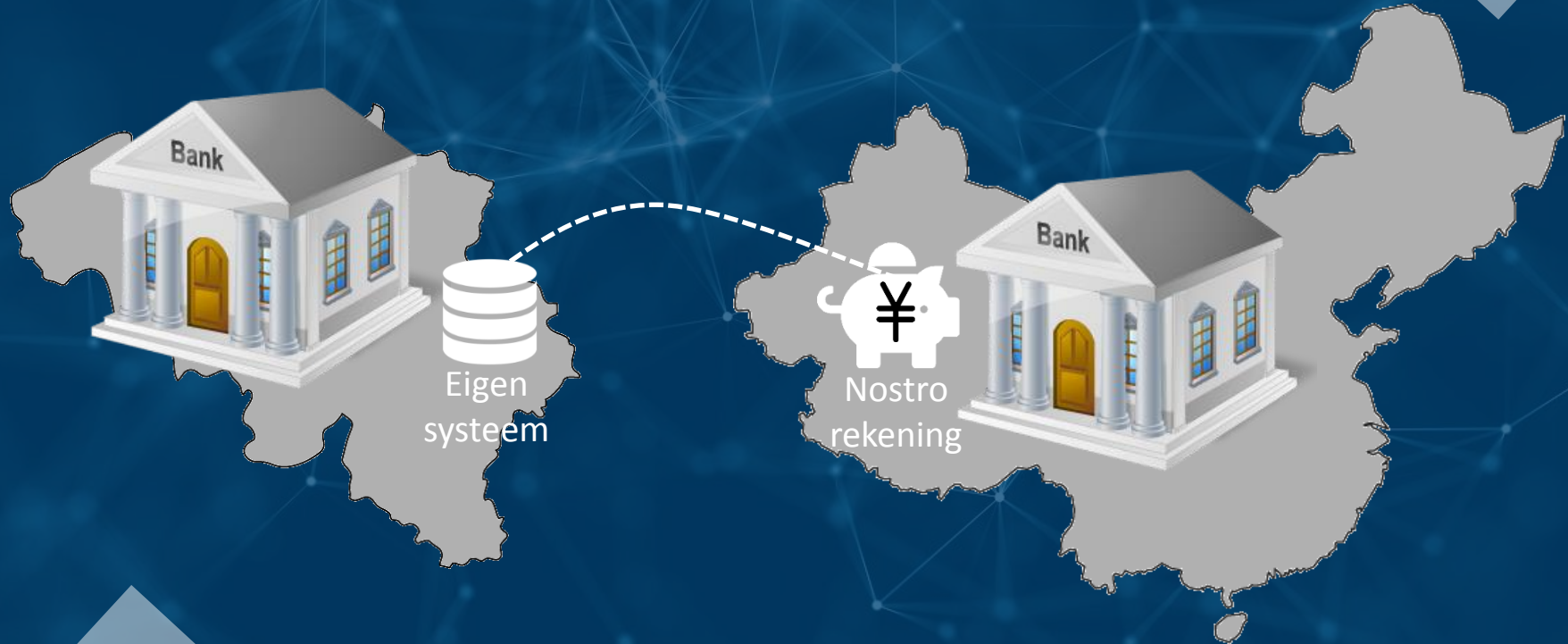


OP BASIS PUBLIEKE INFORMATIE

- Niet steeds even gedetailleerd
- Voldoende om uit te leren

Inter-bank transacties

Rekeningafstemming (account settlement)



Inter-bank transacties

Rekeningafstemming (account settlement)



“Een daverend success”

“De PoC ging uitzonderlijk goed, wat de fantastische vooruitgang bewijst in DLT en in het bijzonder in Hyperledger Fabric

DLT PoC

- Afstemmen internationale nostro rekeningen in real time
- Gebaseerd op Hyperledger Fabric v1.0
- 34 banken betrokken

Functionaliteit

- Transactie status updates
- Full audit trails
- Definiëren & afdwingen toegangsrechten tot data

Inter-bank transacties

Rekeningafstemming (account settlement)

Re-engineering

“Aanzienlijke re-engineering vereist in bestaande systemen, bijvoorbeeld real-time i.p.v. batch rapportering & verwerking”

Operationele uitdagingen

“Om naar productie te gaan zouden meer dan 100 000 kanalen opgezet en onderhouden moeten worden, wat aanzienlijke operationele uitdagingen met zich meebrengt”

“Een daverend success, maar verwacht wel geen werkende oplossing in de nabije toekomst.”

“We werken al aan volgende PoCs.”

Positieve resultaten, aanzienlijke uitdagingen

Internationale betalingen



“Ik moet toegeven dat we er nog niet zijn”

David Schwartz, chief cryptographer

“Distributed ledgers zijn onvoldoende schaalbaar en privaat voor banken.”

*“Wat we horen van veel van onze klanten is dat het noodzakelijk is om transacties **privaat** te houden, om **duizenden transacties per seconde** te verwerken en om **elk denkbaar type munt of activa** te ondersteunen [...]*

*De feedback van de banken is dat je **niet de hele wereld in een blockchain** kan steken”.*

Keuze voor xCurrent

- Geen distributed ledger
- Onwijzigbare transacties
- Toegenomen snelheid ('instant settlement'), transparantie en efficiëntie



**Ogenblikkelijke afhandeling,
transparantie & efficiëntie
geen monopolie van DLT**

Nog aanzienlijke uitdagingen

Financiële effecten



THE WORLD BANK

Wereldbank heeft aangekondigd obligaties uit te zullen geven d.m.v. blockchain technologie

Tijd nodig voor afhandeling
(settlement) gereduceerd van
vijf dagen naar enkele seconden

Beloftes van transparantie &
verlaagde transactiekosten nog
niet gerealiseerd

Financiële sector

Inter-bank transacties ○ Internationale betalingen ○ Financiële Effecten

Veelbelovend

Hier en daar positieve resultaten

Zal toch noch ettelijke jaren duren om volle
potentieel te realiseren

Cases nationaal & internationaal

Aanvraag rolstoel

Ondersteunen
vluchtelingen

Identiteitsbeheer

Diploma's

Financiële sector

Herkomst &
toeleveringsketen



OP BASIS PUBLIEKE INFORMATIE

- Niet steeds even gedetailleerd
- Voldoende om uit te leren

Herkomst & toeleveringsketen

2006



- 2006 project gelanceerd om m.b.v. RFID tags de herkomst van producten te traceren
- Stopgezet omwille van hoge investeringskosten en complexiteit aan de kant van de producenten

2018



- **Food Trust**
Platform gebaseerd op blockchain
- Leveranciers kregen een deadline om het platform te vervoegen

Deze kosten blijven in blockchain benadering
Blockchain is in het beste geval maar een deel van de oplossing
Niet steeds eenvoudig alle belanghebbenden mee aan boord te krijgen

Herkomst & toeleveringsketen

Vaak meer dan 30
partijen bij
transport container
A→B

Lage graad
digitalisering, veel
op papier. >50%
totale kosten

Eenzelfde pincode
wordt doorgegeven
en hergebruikt

Joint venture



100-tal
andere
bedrijven



Meer transparantie en eenvoud in het transport van
goederen tussen grenzen en handelszones d.m.v.
een open blockchain platform voor de sector

Herkomst & toeleveringsketen

Negatief onthaald!

Binnen de sector experimenteren nog heel wat bedrijven – naast elkaar - met blockchain technologie

*“Zo gaat momenteel veel
geld verloren”*

Hapag-Lloyd CEO Rolf Habben Jansen

*“Nood aan standaarden &
gemeenschappelijk beheer”*

Hapag-Lloyd CEO Rolf Habben Jansen

Intellectueel
eigendom blijft bij
Maersk & IBM

Een technische oplossing uitwerken is één ding, alle
belanghebbenden mee aan boord krijgen nog iets anders



Gemeenschappelijk project

Cases nationaal & internationaal

Aanvraag
rolstoel

Ondersteunen
vluchtelingen

Identiteits-
beheer

Diploma's

Financiële
sector

Herkomst &
toelevering

BEMOEDIGENDE RESULTATEN

Hier en daar succesvol

NIET STEEDS KOSTENREDUCTIE

ER IS MEER DAN BLOCKCHAIN

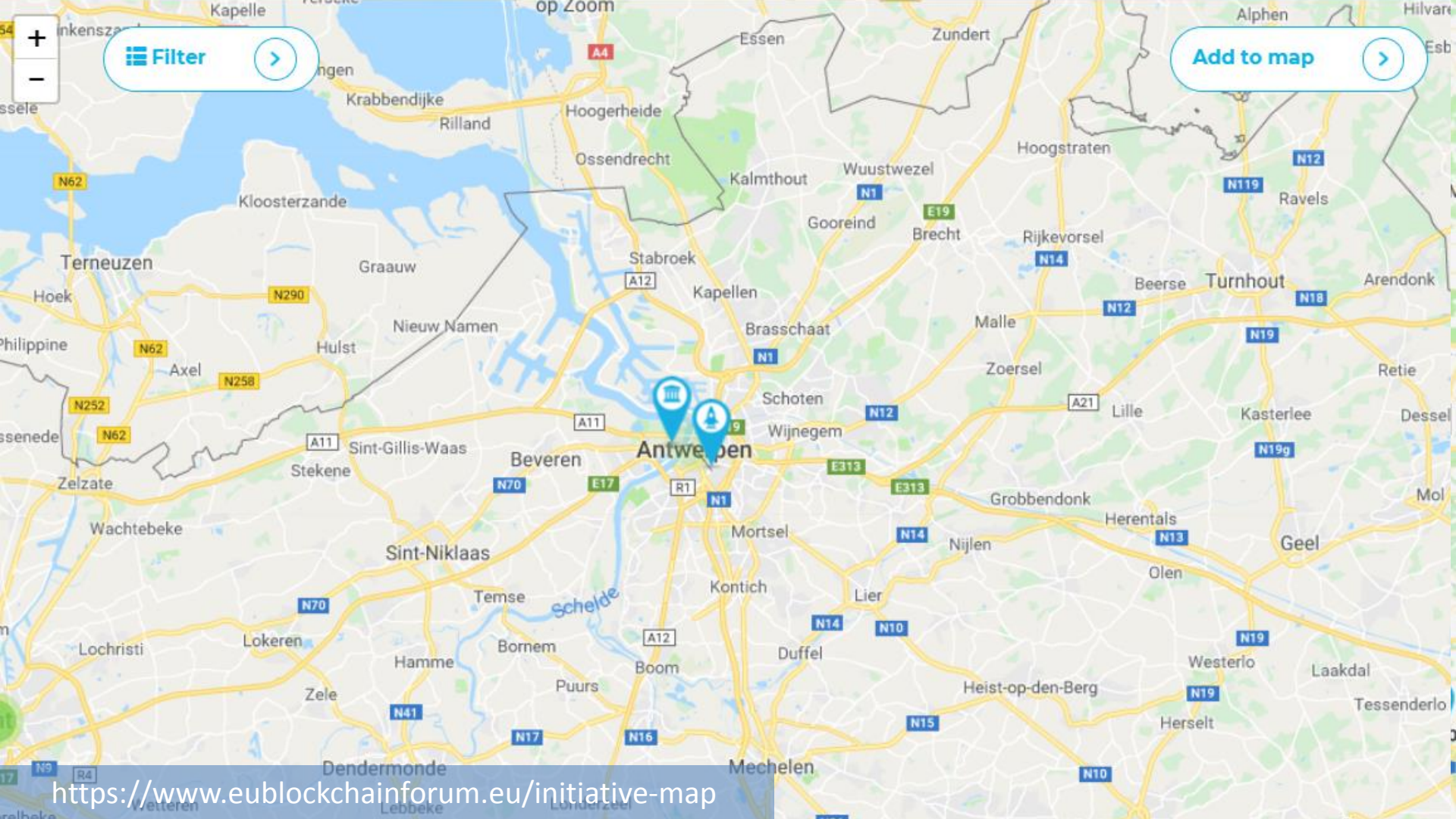
Synergieën tussen technologieën

BLOCKCHAIN DEEL VAN OPLOSSING

- Re-engineering
- Extra kosten voor registraties

UITDAGINGEN

- Privacy & confidentialiteit
- Schaalbaarheid
- Operationeel
- Samenwerking



Samenvatting

lablabla

lablabla

lablabla

lablabla

lablabla

lablabla

Pauze – Break – Διακοπή – Pause – وقفة – 暫停 – Pausa

AGENDA

Blockchain
Een snelle intro

Cases nationaal
& internationaal

Reality check

Onze aanpak

BeSure

Reality check

Confidentialiteit &
privacy (GDPR)

Waar situeert zich de
noodzaak aan vertrouwen?

Zijn er fundamentele
beperkingen?

Blockchain & transparantie

COLLECTIEVE ACTIE

- Bijhouden historiek (**data**)
- Toepassen **regels** op data



Meerdere participanten hebben toegang tot dezelfde data en regels op de blockchain



Blockchain & transparantie



Blockchain & transparantie

Minder data on-chain

- Minder collectief gevalideerd
- Data moet elders bewaard worden

Pseudoniemen

- Deanonimisatierisico
- Vaak nodige maar onvoldoende maatregel

Minder participanten toegang tot data (afgeschermd netwerk en/of vercijfering)

- Minder collectief gevalideerd
- Hogere operationele complexiteit
- Aanvallen mogelijk (Quantum computing, diefstal sleutel (auth/enc), ...)

Geavanceerde cryptografie

- Hogere technologische complexiteit
 - Computationale en opslag overhead
 - Vaak toepassingsspecifiek (vb. Zcash)
-

Vandaag geen praktische generieke oplossingen

Toepassingsspecifieke afweging

Blockchain & GDPR

"Een groot deel van de blockchainprojecten is waarschijnlijk onverenigbaar met de GDPR"

Michèle Finck
Max Planck Institute for Innovation
& University of Oxford

GDPR

ANONIEME GEGEVENS

Onlinkbaar

aan natuurlijk persoon

GEPSEUDONIMISEERDE GEG.

Linkbaar met extra info

aan natuurlijk persoon

GEÏDENTIFICEERDE GEGEVENS

Linkbaar zonder extra info

aan natuurlijk persoon

← Persoonsgegevens →

Registratie van feiten



Elk icoontje (en dus elke transactie) mogelijks persoonsgegevens

Transfereren van virtueel geld



Accurater:



Er is al erg snel van sprake van persoonsgegevens in een blockchain context

Oproepen smart contract functie



Blockchain bevat erg snel erg veel
gepseudonimiseerde persoonsgegevens



GDPR van
toepassing

Minimale
gegevens-
verwerking

Recht op
vergetelheid

Recht op beperking
van de verwerking

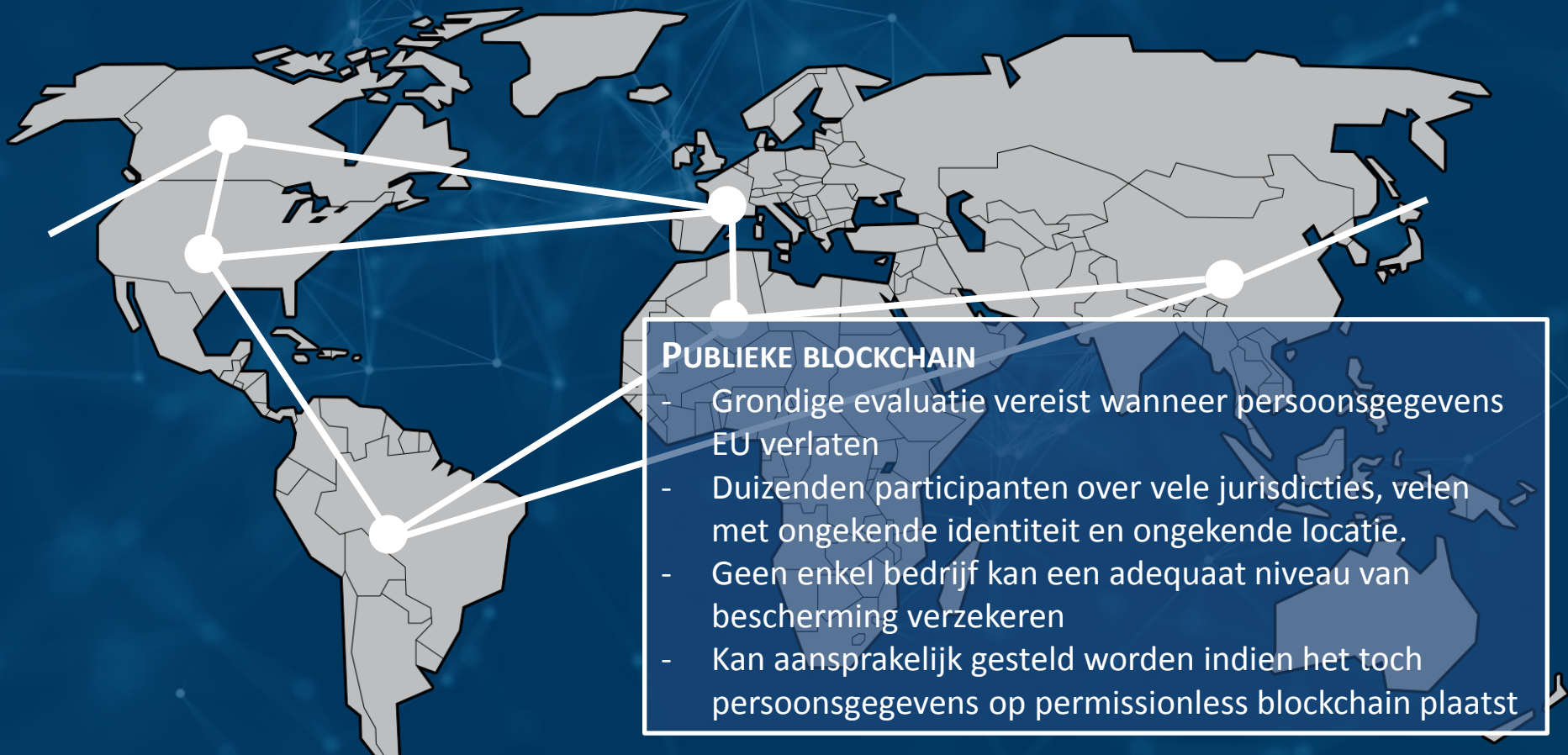
Passende beveiliging
(moving)

AFGESCHERMDE BLOCKCHAIN

- Verwijderen link-data kan volstaan
- Recht op vergetelheid: Door data subject gecontacteerde participant verwijdt link-data en vraagt aan andere participanten hetzelfde te doen
- Contractueel vastgelegde gedeelde verantwoordelijkheid verwerkingsverantwoordelijken. Samenvatting beschikbaar aan betrokkene
- Privacy Impact Assessment kan nodig zijn

Opletten voor minder zichtbare link info. Vb. Belastingaangifte op blockchain

Permissionless blockchain



PUBLIEKE BLOCKCHAIN

- Grondige evaluatie vereist wanneer persoonsgegevens EU verlaten
- Duizenden participanten over vele jurisdicties, velen met ongekende identiteit en ongekende locatie.
- Geen enkel bedrijf kan een adequaat niveau van bescherming verzekeren
- Kan aansprakelijk gesteld worden indien het toch persoonsgegevens op permissionless blockchain plaatst

GDPR

Snel sprake van persoonsgegevens op de blockchain

Enkel gepseudonimiseerde data op de blockchain bewaren kan volstaan om aan het principe '*recht op vergetelheid*' te voldoen. Alle extra info nodig voor de koppeling moet dan vernietigd kunnen worden.

Verwerking persoonsgegevens op een blockchain mogelijk
Duidelijke afspraken nodig tussen participanten
Data Protection Impact Assessment (DPIA) mogelijks vereist

Belang privacy by design & security by design

Publieke blockchains ongeschikt

Reality check

Confidentialiteit &
privacy (GDPR)

Waar situeert zich de
noodzaak aan vertrouwen?

Zijn er fundamentele
beperkingen?

‘The trustless machine’?

Bitcoin Spinoff Hacked in Rare '51% Attack'

By [JEFF JOHN ROBERTS](#) May 29, 2018

Hackers compromised the cryptocurrency Bitcoin Gold—a lesser known offshoot of the original Bitcoin—this month, using superior computing power to falsify the currency's ledger and swindle at least \$18 million from online exchanges.

The hacking incident, which was reported in [a blog post](#) earlier this month, is significant because it shows how a so-called 51% percent attack, which poses an existential threat to any Bitcoin-like currency, is not just a theoretical

Business Impact

If quantum computers threaten blockchains, quantum blockchains could be the defense

Quantum computers could break the cryptography that conventional blockchains rely on. Now physicists say a way of entangling the present with the past could foil this type of attack.

by Emerging Technology from the arXiv May 1, 2018

The unlucky man who accidentally threw away bitcoin worth \$100 million



Welsh IT worker James Howells accidentally threw away bitcoin worth more than \$100 million CREDIT:

WE VERTROUWEN EROP DAT
WE ONZE SLEUTEL NIET
ZULLEN VERLIEZEN

27 januari 2018

Coincheck: World's biggest ever digital currency 'theft'

OF WE VERTROUWEN
DE BEHEERDERS VAN
ONS VIRTUEEL GELD



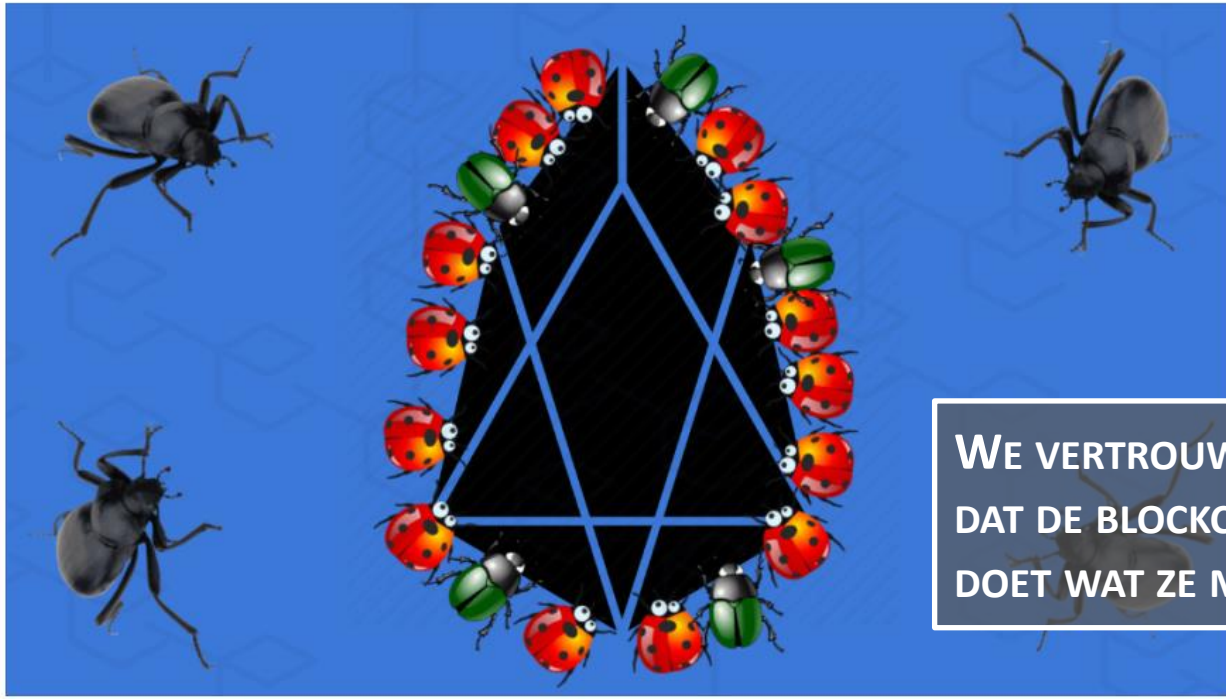
Coincheck representatives looked numb when they faced journalists

One of Japan's largest digital currency exchanges says it has lost some \$534m (£380m) worth of virtual assets in a hacking attack on its network.

14 juni 2018

Researchers continue to find vulnerabilities in \$9 billion cryptocurrency EOS

You could get really rich discovering blockchain bugs!



WE VERTROUWEN EROP
DAT DE BLOCKCHAIN CODE
DOET WAT ZE MOET DOEN

Time is running out to stop a \$53 million cryptocurrency heist

Developers are starting over with just two weeks left

By [Russell Brandom](#) | [@russellbrandom](#) | Jun 30, 2016, 12:42pm EDT

On June 17, [someone stole \\$53 million from the DAO](#), an experimental investment bank built in the Ethereum cryptocurrency system — and the developers have spent the last two weeks trying to get it back.

The DAO's withdrawal system froze the money for 27 days, and rather than let the money slip away permanently, Ethereum's coders have decided to stop the theft by changing the basic code that the currency runs on. But making those changes is delicate and complex — and if nothing changes before July 14th, the money will be lost permanently, and the theft will be complete.

WE VERTROUWEN EROP DAT
HET SMART CONTRACT DOET
WAT WE VERWACHTEN

Wie schrijft code & wie waakt
over kwaliteit?
=> Vertrouwde autoriteiten

'\$300m in cryptocurrency' accidentally lost forever due to bug

User mistakenly takes control of hundreds of wallets containing cryptocurrency
Ether, destroying them in a panic while trying to give them back

More than \$300m of cryptocurrency has been lost after a series of bugs in a
popular digital wallet service led one curious developer to accidentally take

WE VERTROUWEN EROP DAT
HET SMART CONTRACT DOET
WAT WE VERWACHTEN

News

EOS Bet Hacked Again: Attackers Siphon \$338,000 in Funds from the dApp



Jimmy Aki on October 17, 2018 / 1 Comment



Post Views: 1,880

WE VERTROUWEN EROP DAT
HET SMART CONTRACT DOET
WAT WE VERWACHTEN

NEWS

[Home](#)[Video](#)[World](#)[UK](#)[Business](#)[Tech](#)[Science](#)[Stories](#)[Entertainment & Arts](#)

'Foreshadow' attack affects Intel chips

**Dave Lee**

North America technology reporter

🕒 15 August 2018



Share

Researchers have found another serious security flaw in computer chips designed by Intel.

Nicknamed Foreshadow, this is the third significant flaw to affect the company's chips this year.

The US government's body for computer security said "an attacker could exploit this vulnerability to obtain sensitive information".

WE VERTROUWEN EROP
DAT DE HARDWARE DOET
WAT ZE MOET DOEN

Orakels

Vertrouwde leverancier van data aan de blockchain

VOORBEELD: VERZEKERING VLUCHTVERTRAGINGEN

Orakel levert vluchtinformatie aan smart contract



Smart contract beslist hoeveel het aan wie
uitbetaalt en doet dit ogenblikkelijk



WE VERTROUWEN EROP DAT HET ORAKEL CORRECTE INFORMATIE AANLEVERT



A Sensor Was Replaced One Day Before Lion Air Flight JH 610 Crashed

Mounting evidence that something was very wrong with the sensors on board the Boeing 737 MAX and the flight information being sent to the pilots.



By [Barbara S. Peterson](#) Nov 8, 2018

WE VERTROUWEN EROP DAT ORAKELS
CORRECTE INFORMATIE AANLEVEREN

The FAA has issued an emergency directive to anyone flying the Boeing 737 MAX, the type of plane that crashed in the [Lion Air Flight JH 610](#) incident, related to the faulty sensors that reportedly fed bad information to the pilots. Meanwhile, investigators have reported that the plane [received a replacement angle-of-attack sensor](#) (a system that measures whether the plane's nose is too high relative to the current of air) the day before the deadly crash.

Disclaimer: deze crash heeft niets met blockchain te maken

We vertrouwen...

HET CONCEPT

- Wiskundige aannames
- Speltheoretische aannames

HET SYSTEEM

- Cryptografische sleutels niet verloren of gestolen
- Participanten niet gehackt
- Veilige software: client & smart contract
- Veilige hardware

DIVERSE PARTIEN

- Orakels
- Handelsplatformen & wallet aanbieders
- Public key infrastructure
- Blockchain-as-a-Service aanbieders
- **Opstellers regels (enkel uitvoering gedistribueerd)**

Nog steeds vertrouwen vereist, maar op een minder zichtbaar, abstracter en daardoor minder inzichtelijk niveau

Vertrouwen verdwijnt niet, maar betere 'balance of powers' mogelijk

Reality check

Confidentialiteit &
privacy (GDPR)

Waar situeert zich de
noodzaak aan vertrouwen?

Zijn er fundamentele
beperkingen?

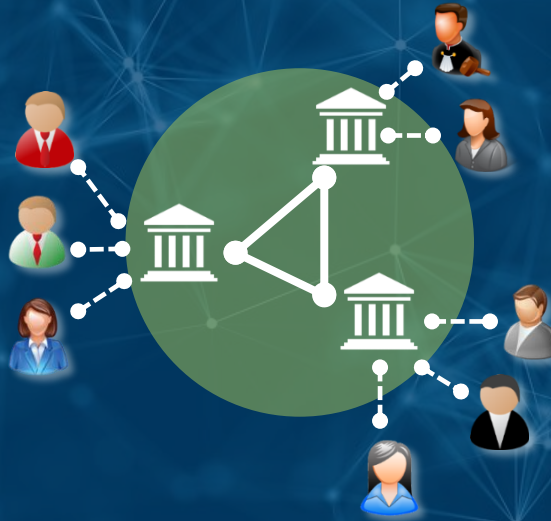
Schaalbaarheid – Distributie vertrouwen

GEDISTRIBUEERD



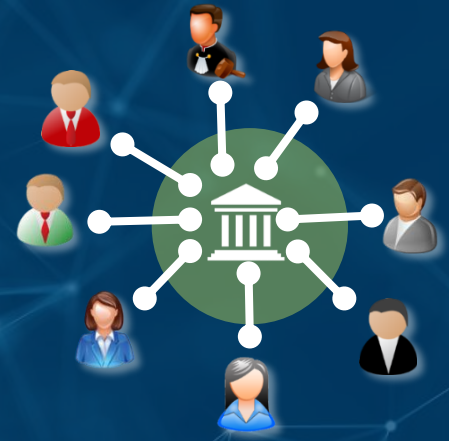
Bitcoin: 10 tx/s
Ethereum: 25tx/s

GEDECENTRALISEERD



Ripple: 1500 tx/s
EOS: 2000 tx/s

GECENTRALISEERD



VISA: 65000 tx/s

Schaalbaarheid – Distributie Vertrouwen

Men kan niet alle participanten in een groot, druk netwerk laten instaan om constant alles te valideren

- Sterk gedistribueerde Uber, eBay, Facebook, ... onmogelijk
- Per toepassing oefening van vinden juiste evenwicht
Allerlei technologieën kunnen ons daarbij helpen: sharding, child chains, DPoS, ...

Reality check

Confidentialiteit &
privacy (GDPR)



Niet steeds even evident

Waar situeert zich de
noodzaak aan vertrouwen?



Niet weg: Autoriteiten,
code, veronderstellingen, ...

Zijn er fundamentele
beperkingen?



Niet iedereen kan alles
valideren

AGENDA

Blockchain
Een snelle intro

Cases nationaal
& internationaal

Reality Check

Onze aanpak

BeSure

Waarom een PoC?



Prestige & media-aandacht



Ontdekken mogelijkheden nieuwe technologie



Verwerven technische kennis & competenties
→ Integreer een leertraject



Voorbereiding inproductiestelling
→ Vereist gedegen analyse

Minst uitdagend
Minst nuttig

Meest uitdagend
Nuttigste

PoC-industrie: proeftuinbedrijfjes

“We maken abstractie van de GDPR”

“Gezien het beperkte budget maken we geen voorafgaandelijke analyse”

“De blockchain PoC was niet bedoeld om gedistribueerd te draaien”

Maak duidelijke afspraken indien je van plan bent verder te gaan dan een PoC, zo vermijd je verrassingen achteraf

Periode van de Poc om de Poc is sowieso voorbij

Stand van de technologie

In volle ontwikkeling & soms onvolwassen

	Hyperledger Fabric	Multichain
<i>Wanneer</i>	Eind 2017 - begin 2018	Eind 2017 - begin 2018
<i>Wie</i>	Informatie Vlaanderen, Digipolis, Fed. Wallonie-Bruxelles & Smals	Smals Onderzoek
<i>Functionaliteit</i>	Uitgebreid: smart contracts, channels, PKI, ...	Beprekter: registratie data, transfer tokens, geen smart contracts
<i>Opzetten netwerk</i>	Maanden	Uren
<i>Stabiliteit</i>	Onvoldoende	Zoals het hoort
<i>Conclusie</i>	Veelbelovend, maar we wachten hier toch nog even mee	Voorzichtig gebruik in productieomgeving te overwegen

Naar productie

High complexity
of blockchain tech

Low complexity
of blockchain tech

	Vandaag erg risicovol Medische voorschriften
Te overwegen bij duidelijke meerwaarde Beperkt risico BeSure	

Application
not critical

Application
critical

Belgische blockchains live

VOEDSELVEILIGHEID

Controle toeleveringsketen
verse producten (gestart met
eieren uit Auvergne regio)



GEZONDHEID & ECOLOGIE

Stimuleren scholieren om
met de fiets of te voet naar
school te gaan
(3 gemeentes: Bonheiden,
Peer, Crisnée)



STRIJD TEGEN FAKE-NEWS

Nagaan integriteit KBC
persberichten
Plan om uit te breiden naar
facturen



We beginnen ook in België blockchain applicatie in productie te zien
Er wordt klein begonnen, met de ambitie om uit te breiden

Meer dan technologie

1 SAMENWERKING & GOVERNANCE

- Hoe iedereen aan boord krijgen en houden
- Welke afspraken onderling?
- Hoe upgrade organiseren

2 JURIDISCH

- GDPR
- Aansprakelijkheden
- Smart contract met juridische waarde

3 KOST

- Analyse, ontwikkeling, licenties, infrastructuur, governance
- Wie betaalt wat? (prijsmodel)

Ook voor Smals
nieuw terrein

Onze aanpak

SHORT-TERM

Bescheiden zaken naar productie

- Beperkte scope, complexiteit & risico
- Voorafgaandelijke analyse: security, privacy, schaalbaarheid, ...
- Vb. BeSure

LONG-TERM

Klaarstaan voor de toekomst

- Veelbelovende technologieën opvolgen
- Analyse complexere business cases: Wat nodig en wat missen we nog? (Vb. Therapeutische relaties)

**Competenties op peil houden in snel evoluerend landschap
In functie van de behoeften bij onze klanten**

Inschakelen in samenwerkingsverbanden

Validata, Beltug Blockchain Task Force, Blockchain Coalition

**Samenwerking voor
juridische aspecten**



Juridische publicaties

MAGISTRATEN & ADVOCATEN

Blockchain & smart contracts: het einde van de vertrouwde tussenpersoon?



Auteurs

Jurgen Goossens (Phd, UGent)

Kristof Verslype

Voorwoord : Pierre Thiriar

Publicatie

12/2018

Seminarie

6 December, Gent

NOTARISSEN

Blockchain & smart contracts: impact op de notaris als vertrouwde tussenpersoon?



Auteurs

Benjamin Verheye (KU Leuven)

Kristof Verslype

Voorwoord: Paul Danneels

Publicatie

11/2018

Seminaries

11 december, Brussel

18 december, Antwerpen

AGENDA

Blockchain
Een snelle intro

Cases nationaal
& internationaal

Reality check

Onze aanpak

BeSure

PoC - BESURE

AANTOONBAARHEIDSDIENST

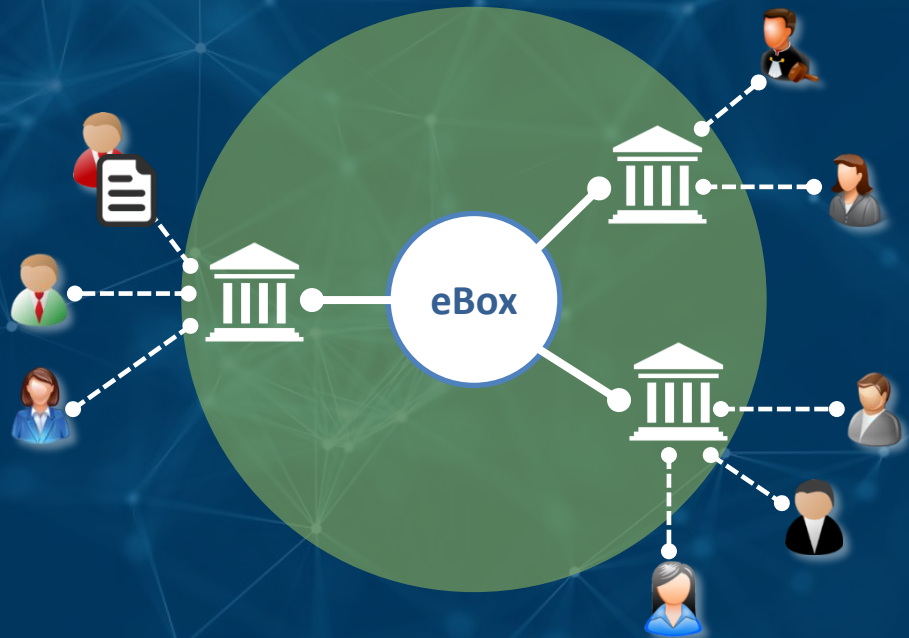
Creatie & bewaren bewijzen
wordt collectief proces

Organisaties en eBox hoeven
elkaar niet te vertrouwen (Leden
vertrouwen wel hun organisatie)

Sterke bewijskracht zonder
centrale autoriteit

Integriteit, onweerlegbaarheid,
geen antidatering, authenticiteit

Documenten zelf elders bewaard

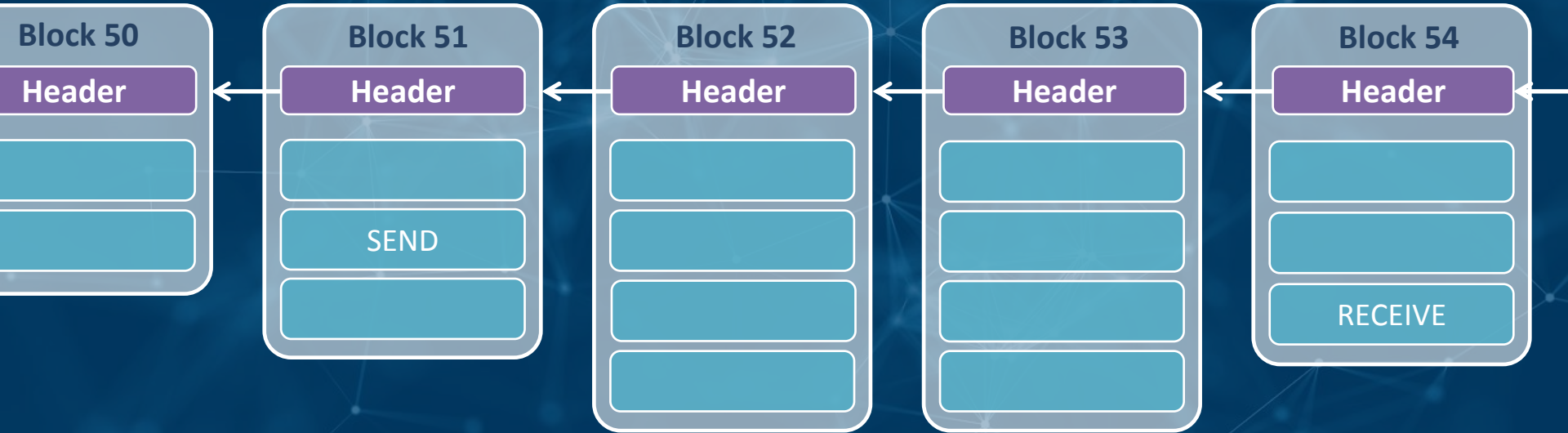


AANTOONBAARHEID

- Proof-of-delivery & proof-of-receipt
- Bewaartermijn: 40-50 jaar

 : Circle of trust

Proofs in the Blockchain



Proof of concept



Validating full node
Admin rights (vote)
Offers web interface to members

eBox

Non-validating full node
No admin rights

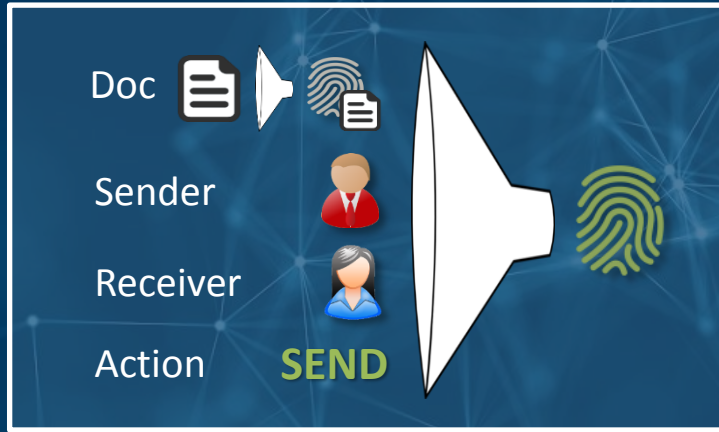


MultiChain

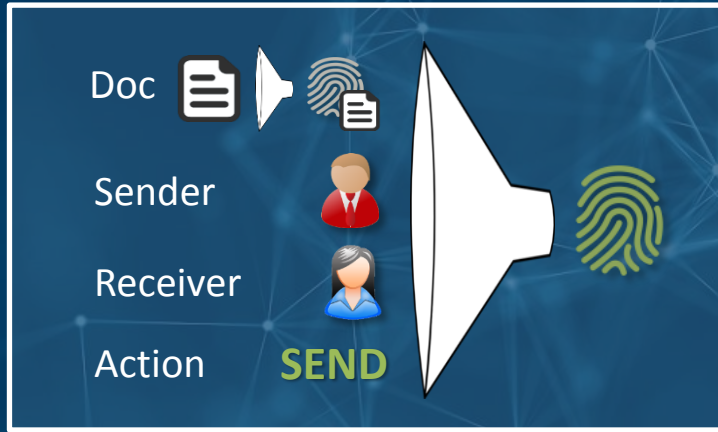


ubuntu

Hashes & transacties (vereenvoudigd)



Bewijskracht



GEEN EXTRA INFO GEKEND

Identificeerbare organisatie betrokken in bewijs van ongekend type, gecreëerd omstreeks .

ENKEL GEKEND

Bewijs dat een ongekend document bestemd voor  op moment  door  verstuurd is.

DOCUMENT GEKEND

Bewijs dat  op moment  document bestemd voor  verstuurd heeft. 

Stappen



1 CREATIE BEWIJS

Samenwerking tussen eBox en betrokken organisatie

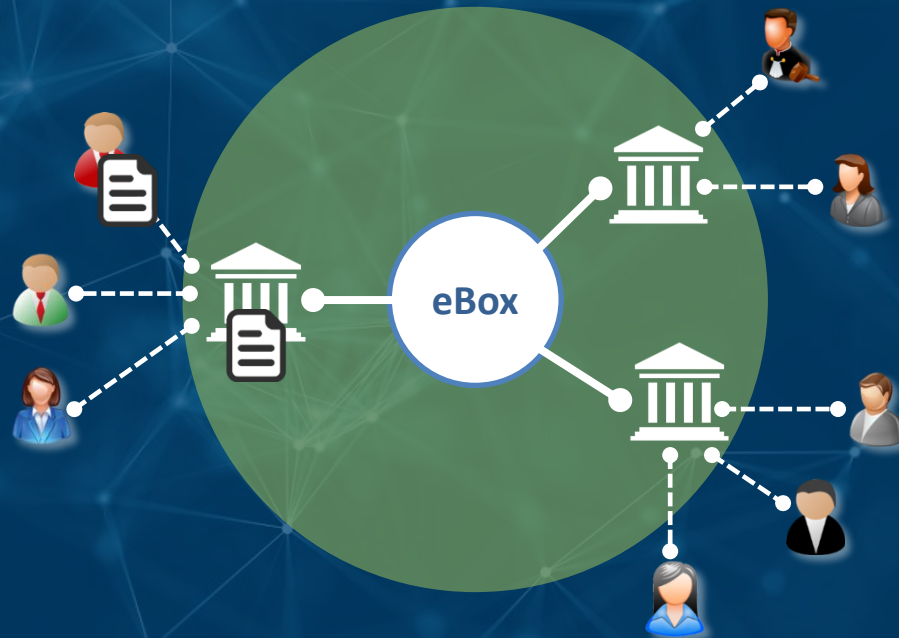


2 TOEVOEGEN BEWIJS AAN BLOCKCHAIN

Collectief proces tussen organisaties



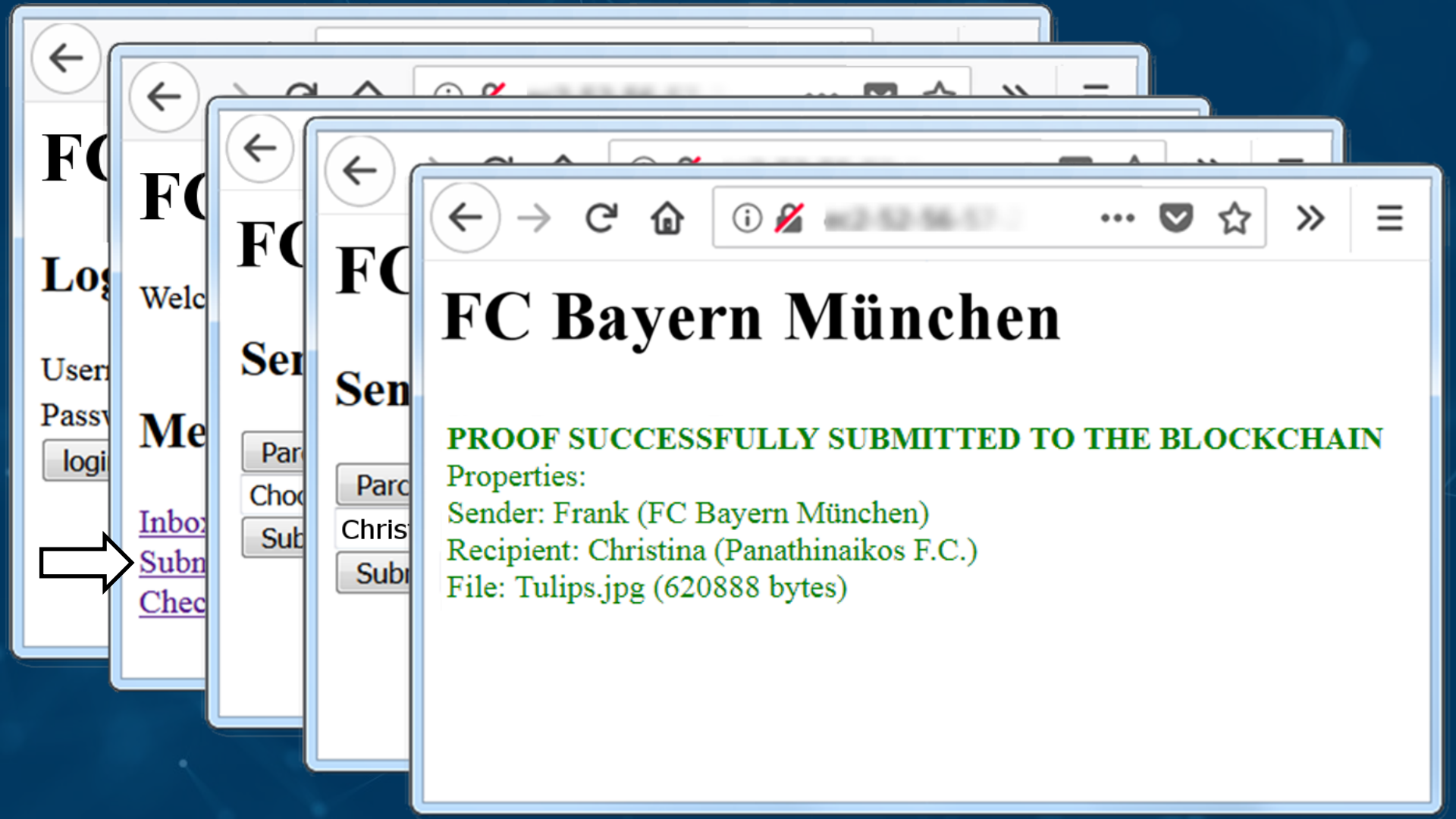
1. VERSTUREN BERICHT



AANTOONBAARHEID

- Proof-of-delivery & proof-of-receipt
- Bewaartermijn: 40-50 jaar

 : Circle of trust



FC Bayern München

PROOF SUCCESSFULLY SUBMITTED TO THE BLOCKCHAIN

Properties:

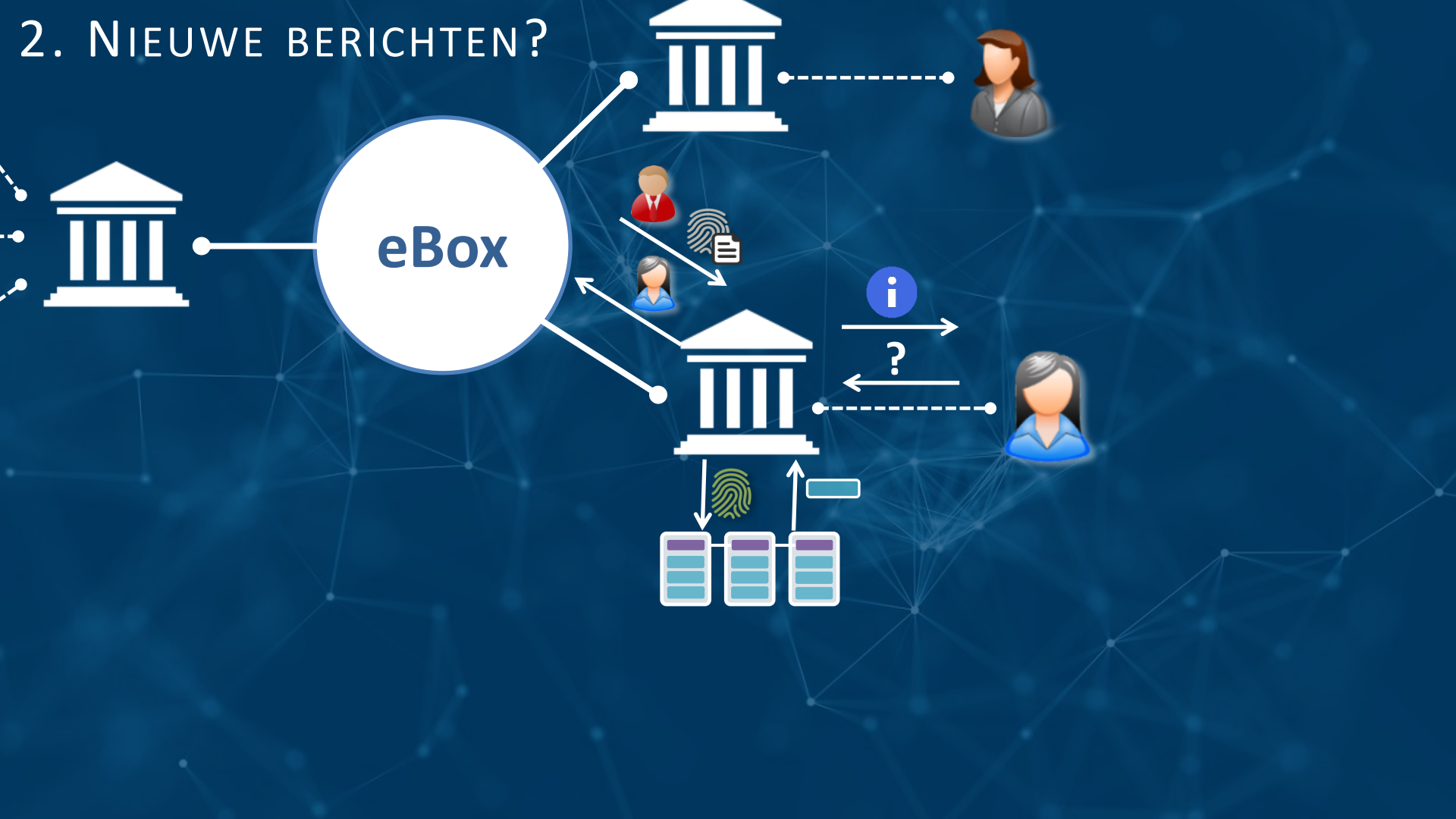
Sender: Frank (FC Bayern München)

Recipient: Christina (Panathinaikos F.C.)

File: Tulips.jpg (620888 bytes)

2. NIEUWE BERICHTEN?

The diagram illustrates the eBox system architecture. A central white circle labeled "eBox" is connected to three white classical building icons representing different institutions. One institution is connected to a user icon (woman) via a dashed line. Another institution is connected to a user icon (woman) via a solid line, with an information icon (i) and a question mark (?) above the connection. A third institution is connected to a user icon (woman) via a solid line, with a fingerprint icon and a document icon above the connection. Below the institutions, there are three server rack icons. A fingerprint icon is shown above the servers, and a document icon is shown below the servers. The background is a dark blue network of white dots and lines.



Panathinaikos F.C

Inbox

Docum	Date	Sender	
28616539_10216423233560526_.jpg	Fri Mar 09 2018 15:04:34 GMT+0000 (UTC)	Anna (Manchester United F.C.)	download
Penguins.jpg	Fri Mar 09 2018 15:40:10 GMT+0000 (UTC)	Anna (Manchester United F.C.)	download
Chrysanthemum.jpg	Fri Mar 09 2018 15:58:10 GMT+0000 (UTC)	Anna (Manchester United F.C.)	download
Tulips.jpg	Thu Mar 15 2018 12:51:25 GMT+0000 (UTC)	Frank (FC Bayern München)	download

1 CREATIE BEWIJS

Samenwerking tussen eBox en betrokken organisatie

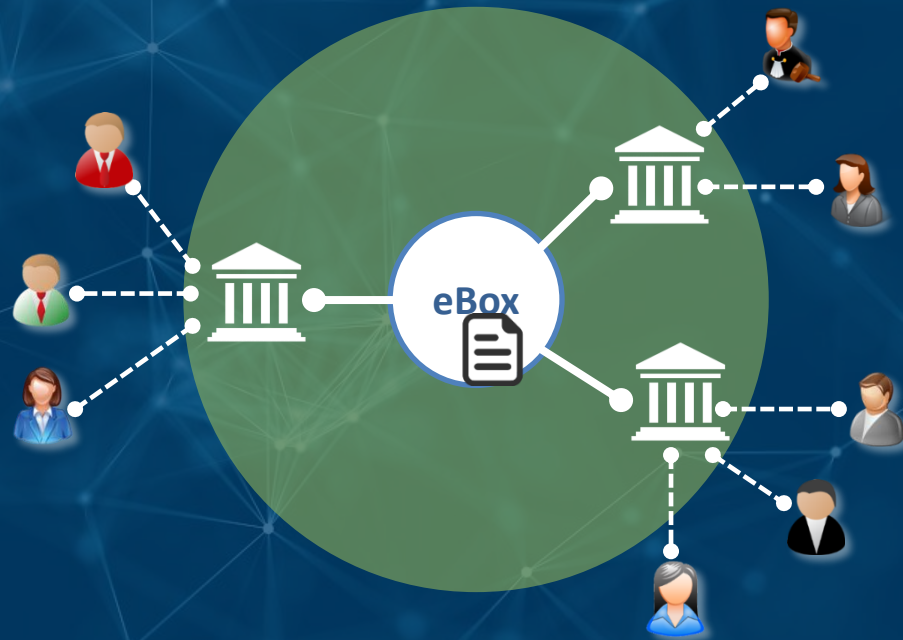


2 TOEVOEGEN BEWIJS AAN BLOCKCHAIN

Collectief proces tussen organisaties



3. DOWNLOADEN BERICHT

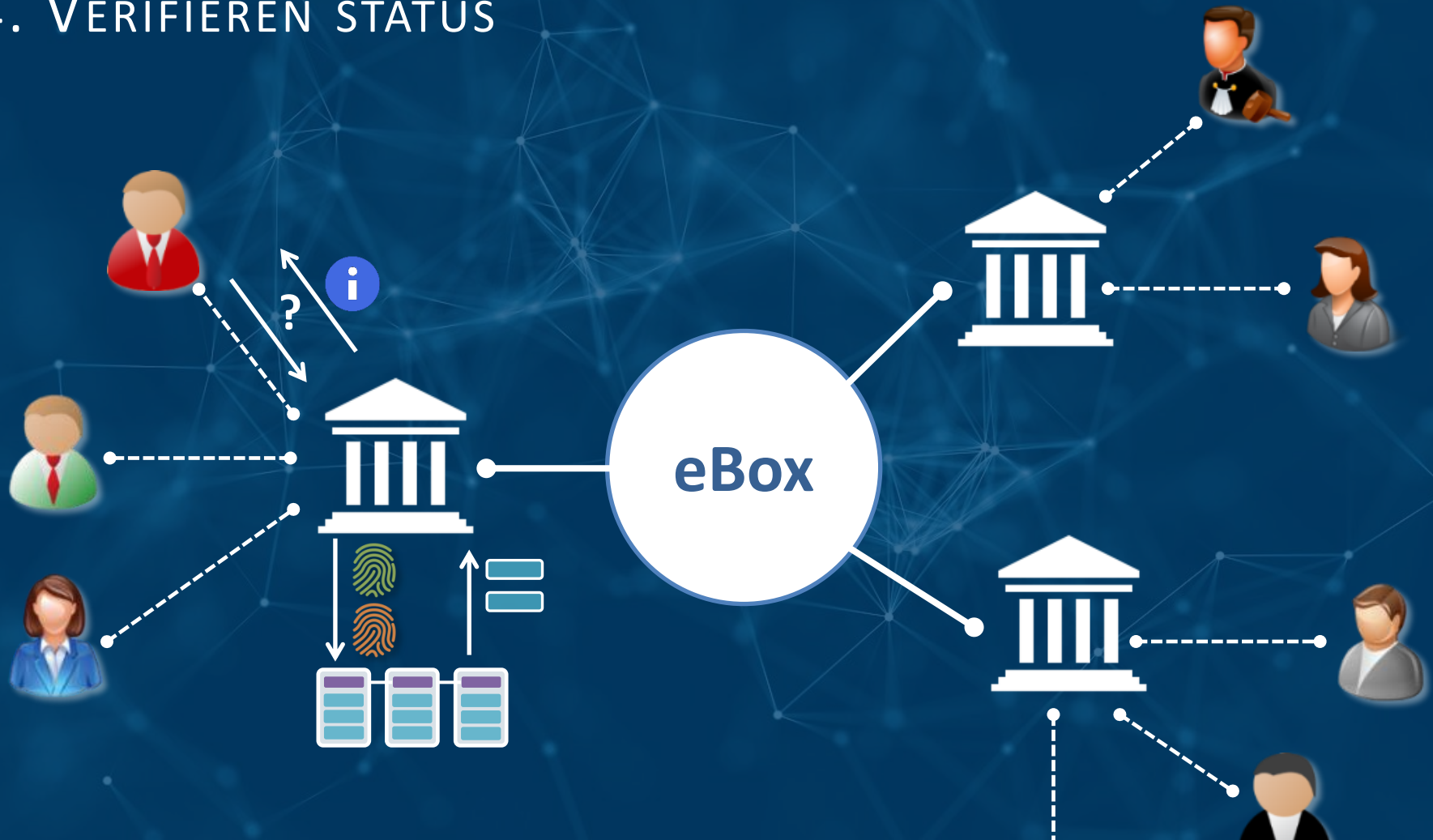


AANTOONBAARHEID

- Proof-of-delivery & proof-of-receipt
- Bewaartermijn: 40-50 jaar

 : Circle of trust

4. VERIFIËREN STATUS



FC Bayern München

Action	Time
send	Thu Mar 15 2018 12:51:25 GMT+0000 (UTC)
receive	Fri Mar 16 2018 10:26:13 GMT+0000 (UTC)

[Inbox](#)
[Submit](#)
[Check](#)

Stappen



Veiligheid & opslag

HOOG NIVEAU VEILIGHEID

Valsspelen gedetecteerd

Geen gevoelige gegevens op blockchain

Compromitteren sleutel niet dramatisch

Flexibel rechtenbeheer

Gedistribueerd tot gecentraliseerd mogelijk

Sleutelbeheer via blockchain

geen externe PKI

Crash individuele node geen probleem

Geen technology lock-in

Migratie mogelijk (vb. indien
blockchaintechnologie niet langer geschikt)

Veilige en stabiele blockchaintechnologie

SCHAALBAAR

Grootte blockchain

| bewijs | = 400 bytes

100 000 berichten in jaar 1

10% groei / jaar

| Blockchain | = 100 GB na 50 jaar

= 116M documenten

Backup overbodig

Doorvoer

1000 bewijzen per seconde met normale server

Horizontaal schalen mogelijk

Afspraken nodig tussen participanten

Welke blockchain technologieën morgen?

VERTROUWEN

Geen vertrouwde autoriteiten

Timestamping service, PKI, opslagdienst

Organisaties blijven een rol spelen

Hun rol wordt opgewaardeerd

**Afweging: Hogere kost versus meer
afhankelijkheden**

GENERIEKE DIENST

Diverse toepassingmogelijkheden

Onweerlegbaar registreren van feiten of afspraken (vb. gezondheids-, financiële, juridische en verzekeringssector)

Herbruikbare code

Daar streven we toch naar

Herbruikbaar netwerk

Eens we een blockchain netwerk hebben is het makkelijker om nieuwe blockchaintoepassing te bouwen met grotendeels dezelfde participanten

Verzachtend effect op kostenaspect

Checklist

VEILIGHEID & PRIVACY		
Veilige blockchain technologie		Fork code meest gebruikte technologie (Bitcoin)
Veilig smart contract	N.v.t	
Privacy / security by design		
Omgaan met verlies sleutel		Telkens minstens twee partijen nodig
Correcte invoer orakels		Door twee partijen gevalideerd
Migratiepad		
SAMENWERKING		
Vertrouwensissue		
Interesse bij participanten		Toch bij de reeds gecontacteerden
Kostenreductie		Speelt minder bij generieke dienst

BeSure - Status



BeSure - Conclusies

Eenvoudige, haalbare blockchaintoepassing

Desondanks goed nadenken: veiligheid, privacy,
schaalbaarheid

Verregaande stappen vanuit Smals Onderzoek
om eventuele inproductiestelling te bevorderen

Doel: generieke aantoonbaarheidsdienst

BLOGPOST

www.smalsresearch.be

**BeSure - Een realistische
blockchain case voor de
overheid**



**BeSure — A realistic
blockchain case for the
Belgian government**



AGENDA

Blockchain
Een snelle intro

Cases nationaal
& internationaal

Reality check

Onze aanpak

BeSure

EEN WERELD ZONDER AUTORITEITEN & ZONDER VERTROUWEN IS EEN ILLUSIE

Bedenking: de juiste vraag

Hoe kunnen we entiteiten waar we afhankelijk van zijn elimineren?

of

Hoe kunnen we, o.a. met technologie, het vertrouwen in noodzakelijke entiteiten versterken?

of

Hoe kunnen we komen tot een betere 'balance of powers' om samenwerking te stimuleren?

Questions & Contact

KRISTOF VERSLYPE

PHD OF ENGINEERING (DEPT. COMPUTER SCIENCE, UNIVERSITY OF LEUVEN)

RESEARCHER, ADVISOR, SPEAKER AUTHOR IN CRYPTO, PRIVACY & BLOCKCHAIN TECH



www.smalsresearch.be



[@SmalsResearch](https://twitter.com/SmalsResearch)



www.smals.be



[@Smals_ICT](https://twitter.com/Smals_ICT)



www.cryptov.net



[@KristofVerslype](https://twitter.com/KristofVerslype)



kristof.verslype@smals.be



be.linkedin.com/in/verslype

Referenties

- [J18] R. JUSKALIAN, Inside the Jordan refugee camp that runs on blockchain, MIT Technology Review, 12 april 2018.
<https://www.technologyreview.com/s/610806/inside-the-jordan-refugee-camp-that-runs-on-blockchain/>
- [M18] J. MOSER, *The Application & Impact of the European General Data Protection Regulation on Blockchains*, R3, 15 February 2017,
https://www.r3.com/wp-content/uploads/2018/04/GDPR_Blockchains_R3.pdf
- [K18] M. KRAMER, Walmart Gives Suppliers Deadline To Join Food Trust Blockchain, ETH News, 25 September 2018,
<https://www.ethnews.com/walmart-gives-suppliers-deadline-to-join-food-trust-blockchain>
- [O17] M. ORCUTT, *How Blockchain Is Kickstarting the Financial Lives of Refugees*, MIT Technology Review, 5 September 2017,
<https://www.technologyreview.com/s/608764/how-blockchain-is-kickstarting-the-financial-lives-of-refugees/>
- [P16] G. PLIMMER, *Use of bitcoin tech to pay UK benefits sparks privacy concerns*, Financial Times, 12 July 2016,
<https://www.ft.com/content/33d5b3fc-4767-11e6-b387-64ab0a67014c>
- [R15] K. RANNENBERG, J. CAMENISCH A. SABOURI. Attribute-based Credentials for Trust: Identity in the Information Society, Identity in the Information Society, Springer, 2015.
- [R17] P. ROUSSEAU & P. BUYTAERT, Sociale woningen toewijzen via blockchain, Infosessie blockchain, Informatie Vlaanderen, 13 November 2017.
- [S18] H. SENDER, World Bank breaks ground with blockchain bond sale, Financial Times, 9 August 2018,
<https://www.ft.com/content/f99186b2-9bb5-11e8-9702-5946bae86e6d>
- [V18] K. VERSLYPE, BeSure - A realistic blockchain case for the Belgian government, Medium, 11 September 2018,
<https://medium.com/@cryptovnet/besure-a-realistic-blockchain-case-for-the-belgian-government-c5b8c62dff38>

Referenties

- [B17] Gemeente Stichtse Vecht - Rolstoelgebruik in Blockchain, Blockchain pilots Dutch Government, blockchainpilots.nl, Pilotronde 2, 2017. <http://hostedby.frogjump.nl/blockchain-magazine#!/stichtse-vecht>
- [B18a] J. BIESEMANS, De blockchain van de kip en het ei, EOS Magazine, 30 april 2018, <https://www.eoswetenschap.eu/voeding/de-blockchain-van-de-kip-en-het-ei>
- [B18b] Belfius lanceert via zijn innovatielab The Studio, een mobiliteitsplatform voor scholen en gemeenten dat gebruik maakt van blockchaintechnologie. Belfius, 10 September 2018. <https://www.belfius.com/NL/publicaties/nieuwsberichten/2018/Pressrelease20180910.aspx>
- [D18] K. DANIELS, Certified for Life — International exchange & authentication of diplomas via blockchain, Medium, 31 july 2018, <https://medium.com/wearetheledger/certified-for-life-international-exchange-authentication-of-diplomas-via-blockchain-4e947720edd9>
- [E18] EU Blockchain Observatory and Forum - GDPR Workshop Report - June 8, 2018 https://www.eublockchainforum.eu/sites/default/files/reports/workshop_2_report_-_gdpr.pdf
- [F18] Adoption of DLT presents significant operational challenges for Swift member banks, Finextra, 8 March 2018, <https://www.finextra.com/newsarticle/31787/adoption-of-dlt-presents-significant-operational-challenges-for-swift-member-banks>
- [G08] S. GAUDIN, Some Suppliers Gain from Failed Wal-Mart RFID Edict, CIO, 29 april 2008, <https://www.cio.com/article/2436434/rfid/some-suppliers-gain-from-failed-wal-mart-rfid-edict.html>
- [I17] M. IANSITI & K. LAKHANI, The Truth About Blockchain. Harvard Business Review, January-February 2017, <https://hbr.org/2017/01/the-truth-about-blockchain>
- [I18] A. IRRERA, Banks unlikely to process payments with distributed ledgers for now, says Ripple, Reuters, 13 June 2018, <https://uk.reuters.com/article/us-blockchain-ripple/banks-unlikely-to-process-payments-with-distributed-ledgers-for-now-says-ripple-idUKKBN1J92JG>