Smals
ICT for society

Blockchain lessons from the government field

KRISTOF VERSLYPE
SMALS RESEARCH

21/03/2019

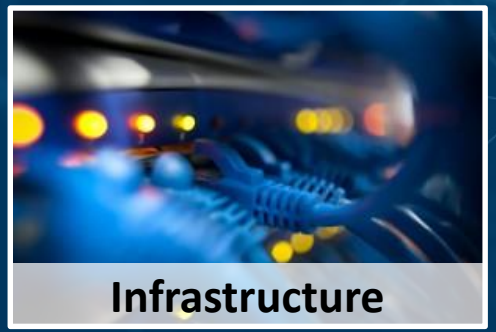
Smals
ICT for society

SUPPORT OF E-GOVERNMENT

Knowhow

Development

Staffing



Infrastructure

g-cloud

top EMPLOYER BELGIË BELGIQUE

CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

WWW.SMALS.BE

Smals Research

Innovation with new technologies

Consultancy & expertise

Internal & external knowledge transfer

Support for going live

2019

- Data Quality
- Productivity in AI
- AI for Public Sector
- NewSQL Databases
- Conversational Interfaces
- Robotic Process Automation
- Web Scraping for Analytics
- Blockchain
- Advanced Cryptography

Smals
ICT for society

www.smalsresearch.be

AGENDA

Smals
ICT for society

- Finding a good case
- Privacy & confidentiality
- Choice blockchain technology
- Rights management
- Hosting the nodes

AGENDA

Smals
ICT for society

Finding a good case

Privacy & confidentiality

Choice blockchain technology

Rights management

Hosting the nodes

Finding a good case

Everything that is possible with a blockchain can be done – from a technical point of view – more efficiently with a centralized approach.

TRUSTING - EACH OTHER OR A CENTRAL PARTY - IS CHEAPER

Sufficiently deep distrust

Finding a good case (Ctd)

Ambition to go beyond PoC

Technology not yet very mature & evolving quickly

Low complexity

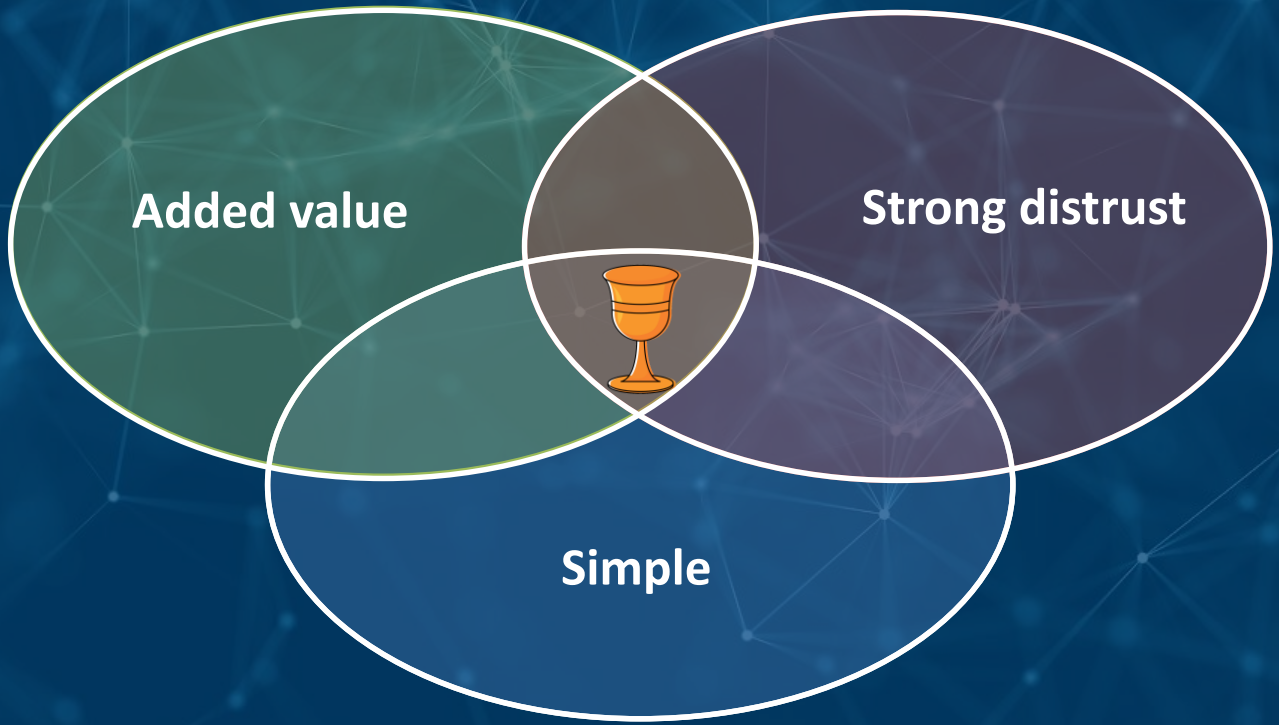
Finding a good case (Ctd)

Sufficiently large delta compared to what already exists

Clear added value

Finding a good case

… is challenging



BeSure

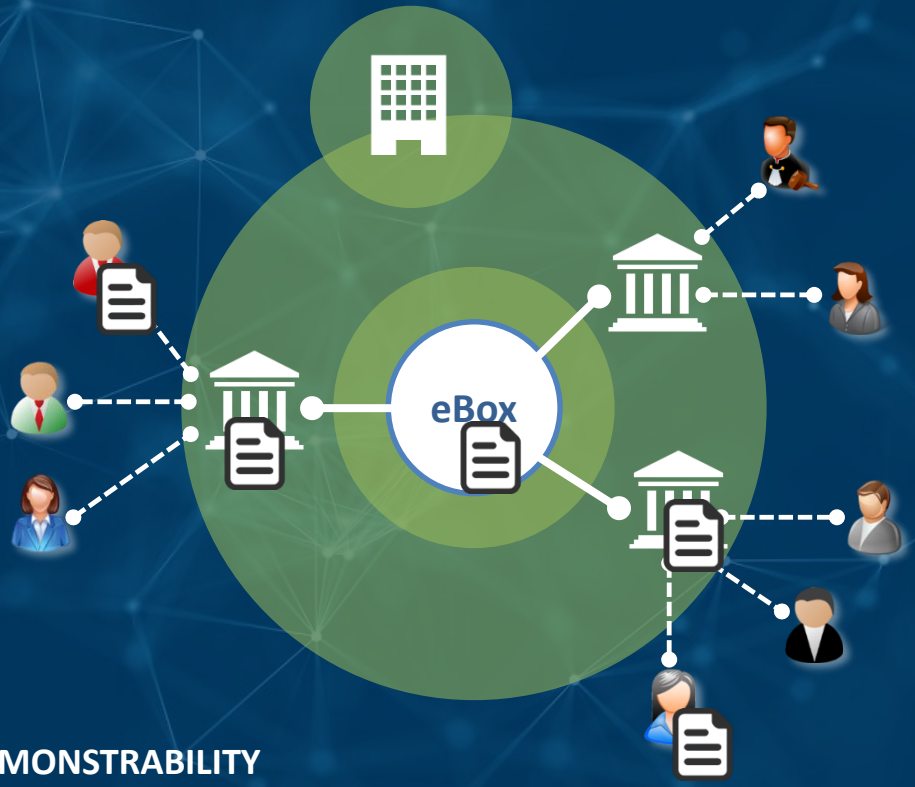
Demonstrability service

Creation & storage proofs becomes collective process

Organisations and eBox don't need to trust each other (members do trust their organisation)

Strong evidential value without central authority

Integrity, non-repudiability, correct timestamp, authenticity



Demonstrability

- Proof-of-delivery & proof-of-receipt
- Storage duration: 40-50 years

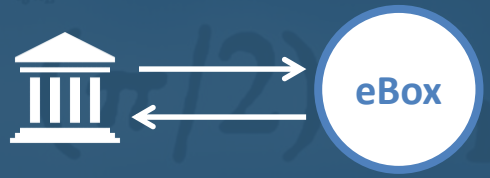
: Circle of trust

BeSure

Demonstrability service

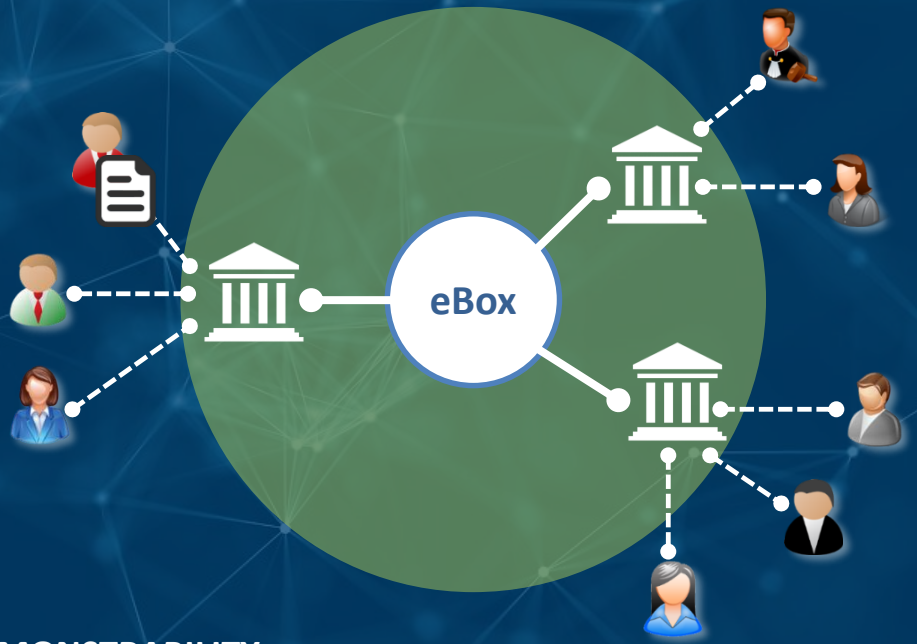
1 Proof creation

Collaboration between eBox and involved organisation



2 Adding proof on blockchain

Collective process between organisations

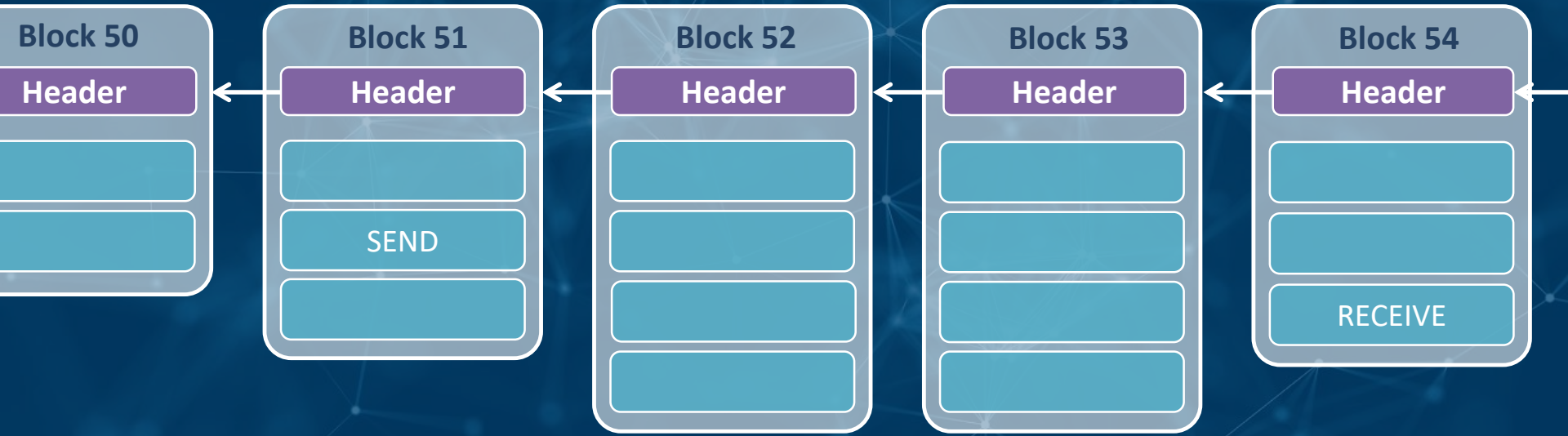


Demonstrability

- Proof-of-delivery & proof-of-receipt
- Storage duration: 40-50 jaar

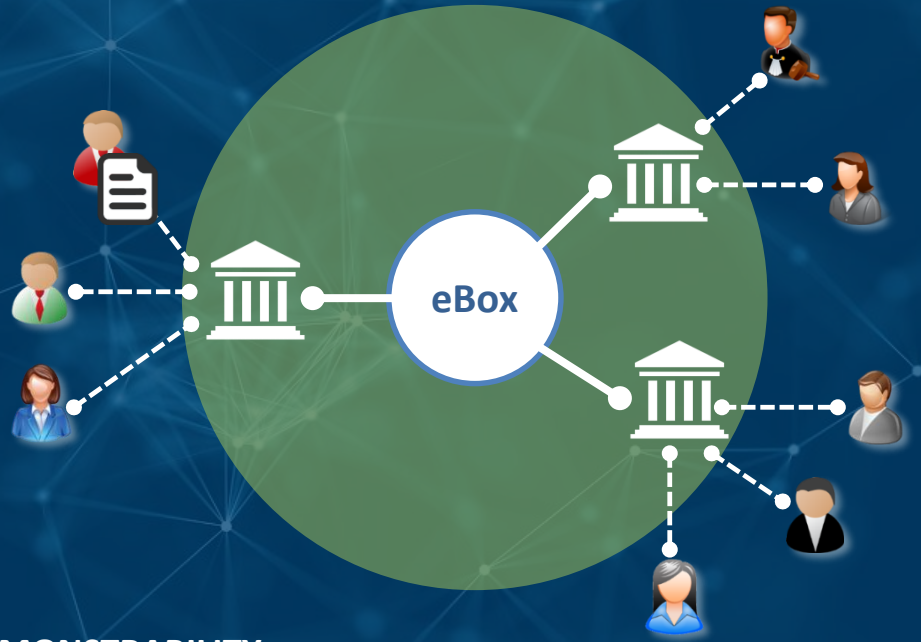
: Circle of trust

Proofs in the blockchain



Finding a good case

BESURE



DEMONSTRABILITY

- Proof-of-delivery & proof-of-receipt
- Storage duration: 40-50 years

AGENDA

Smals
ICT for society

Finding a good case

Privacy & confidentiality

Choice blockchain technology

Rights management

Hosting the nodes

Blockchain & transparency

COLLECTIVE ACTION
- Maintaining history **(data)**
- Applying **rules** on data

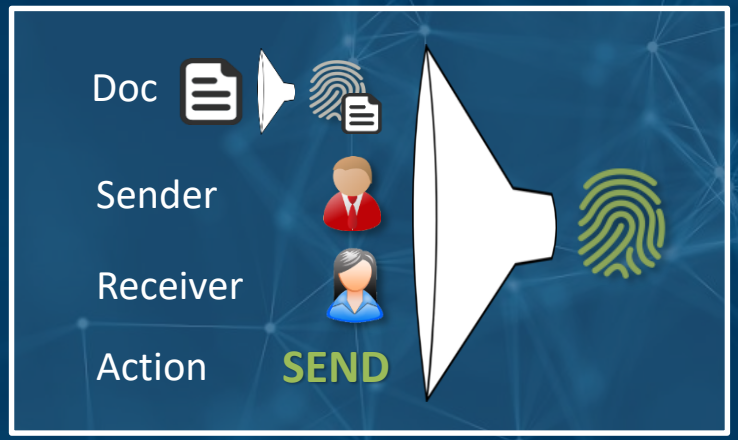
Multiple participants have access to the same data and rules on the blockchain

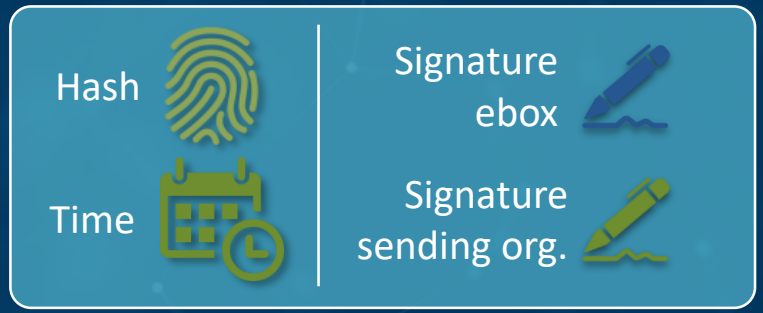
Blockchain / DLT

Transparency TENSION **Confidentiality**

Personal & enterprise data

Evidence





NO EXTRA DATA KNOWN

Identifiable organisation involved in proof of unknown type, created around .

ONLY (AND +) KNOWN

Proof that unknown document has been sent at moment by to .

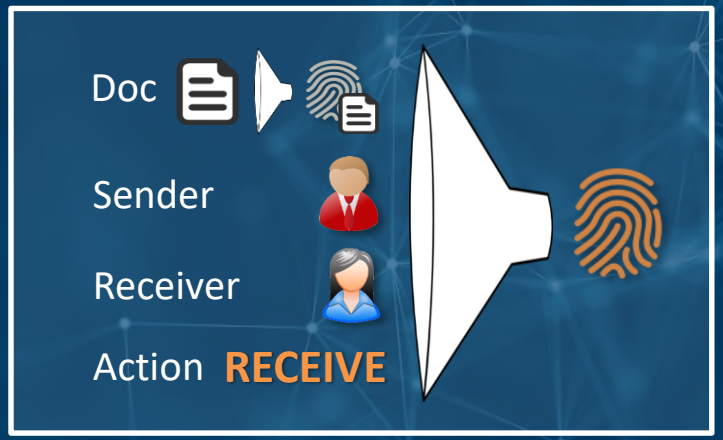
DOCUMENT KNOWN (AND +)

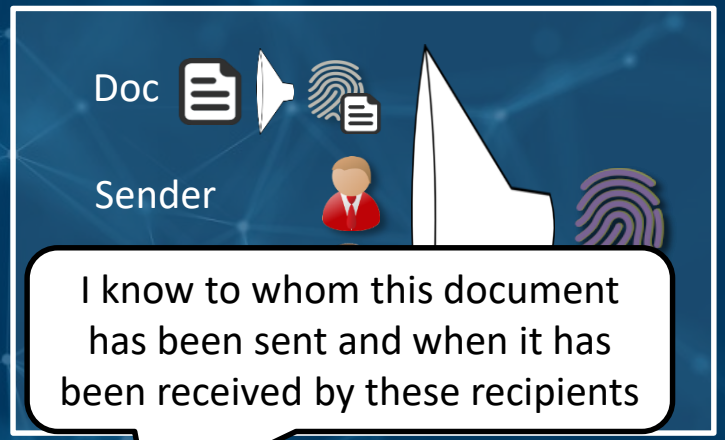
Proof that has sent the document at moment to .

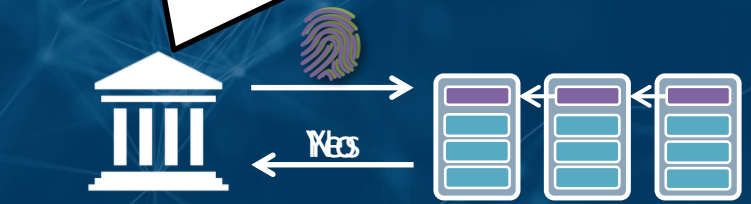
Watch out for low-entropy documents!

RECEIVE is analogous

Confidentiality







Privacy & confidentiality

“We make abstraction of the GDPR”

→ A thorough security analysis is necessary

AGENDA

Smals
ICT for society

Finding a use case

Privacy & confidentiality

Choice blockchain technology

Rights management

Hosting the nodes

PERMISSIONLESS

Public / open

- Publicly accessible
- Can be very energy-inefficient
- Slower
- Trust distributed
- Virtual money required

bitcoin ETHEREUM

PERMISSIONED

Enterprise / Consortium

- Extra layer for access control
- More energy-efficient
- Faster (more tx/s, more blocks/s)
- Trust decentralized
- No virtual money required

MultiChain HYPERLEDGER Quorum

Choice blockchain technology

	Hyperledger Fabric	Multichain
When tested?	End 2017 - beginning 2018	End 2017 - beginning 2018
By	IBM, large dev. community	Coin Sciences, small dev. community
Functionality	Extended: smart contracts, channels, PKI, …	More limited: data registration, token transfer, no smart contracts
Network deployment	Months	Hours
Stability	Insufficient	Very stable. Fork of bitcoin code → tested widely in practice
Conclusion	Promising, but we wait a bit to use it.	Careful use in production environments can be considered.

MULTICHAIN SEEMED APPROPRIATE CHOICE

STILL, MIGRATION PATH REQUIRED

Multichain Performance

Total transactions	1.0 alpha 3	1.0 alpha 21	1.0 alpha 22	1.0 beta 1	1.0 beta 2
100	6.5 tps	7.8	541.7	830.6	1465.7
1,000	7.0	7.6	583.9	889.4	1199.6
10,000	4.1	6.4	566.9	746.6	1071.2
100,000	—	6.6	558.0	771.9	1034.2
1,000,000	—	—	548.6	773.6	1055.4

Average transactions per second, including API overhead and building, signing, mining and verifying transactions and blocks.
Tests performed using the `ab` HTTP server benchmarking tool sending two concurrent requests to the `sendtoaddress` API.
Server specifications: Intel Core i7-4770, 4 cores @ 3.4 MHz, 32 GB RAM, Seagate 2 TB 7200 RPM SATA, CentOS 6.4.

VERTICAL SCALING POSSIBLE, HORIZONTAL SCALING MORE DIFFICULT (AGREEMENTS NECESSARY)

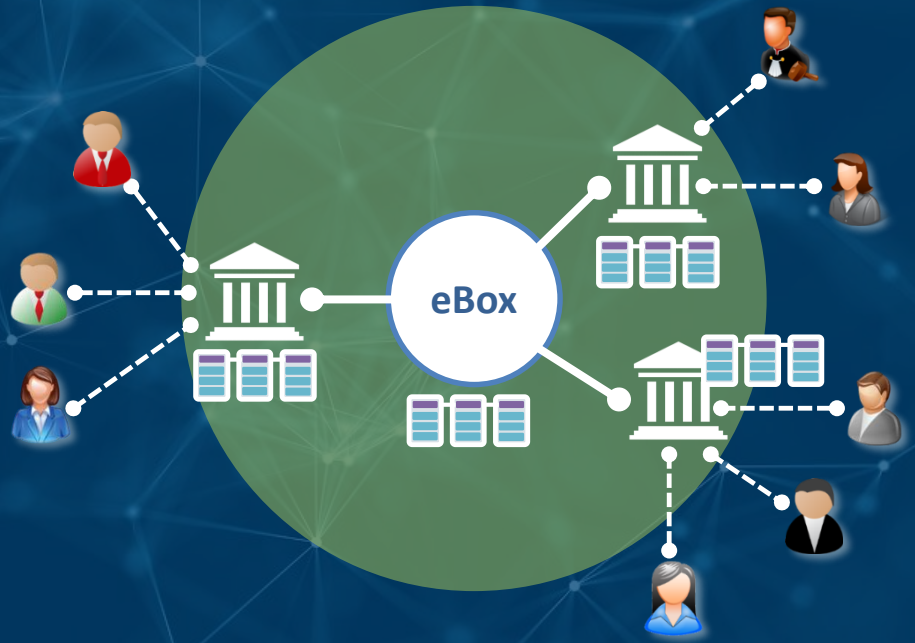
https://www.multichain.com/blog/2017/06/multichain-1-beta-2-roadmap/

Storage

- |proof| = 400 bytes.
- 2 transactions (proofs) / document
- 100 000 documents in first year,
- +10%/year.

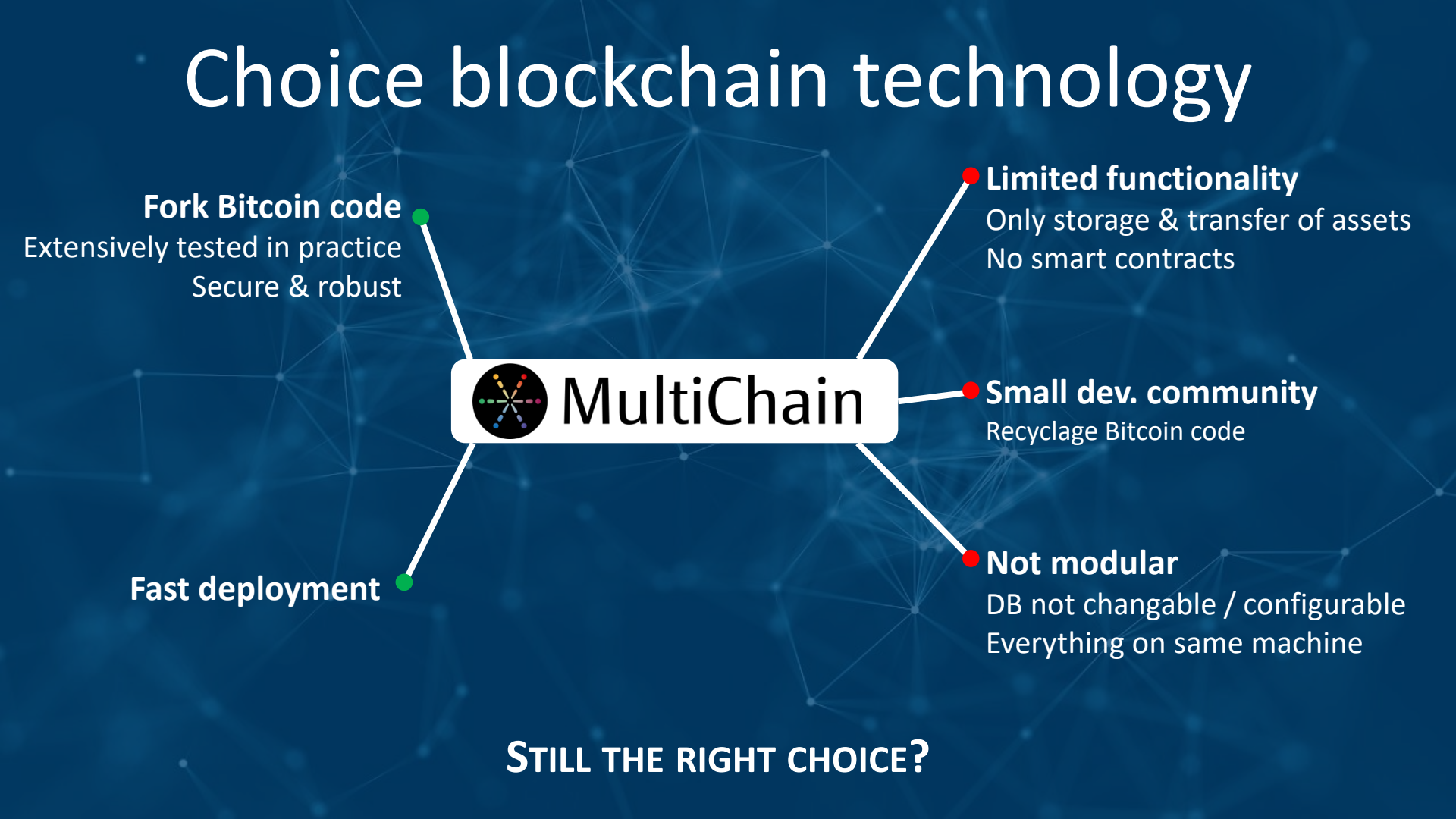
→ After 50 years: 116M documents, < 100 GB blockchain

If n organisations, the total storage is $(n + 1) * |blockchain|$
Less necessity for backup



: Circle of trust

Choice blockchain technology



STILL THE RIGHT CHOICE?

AGENDA

Smals
ICT for society

Finding a use case

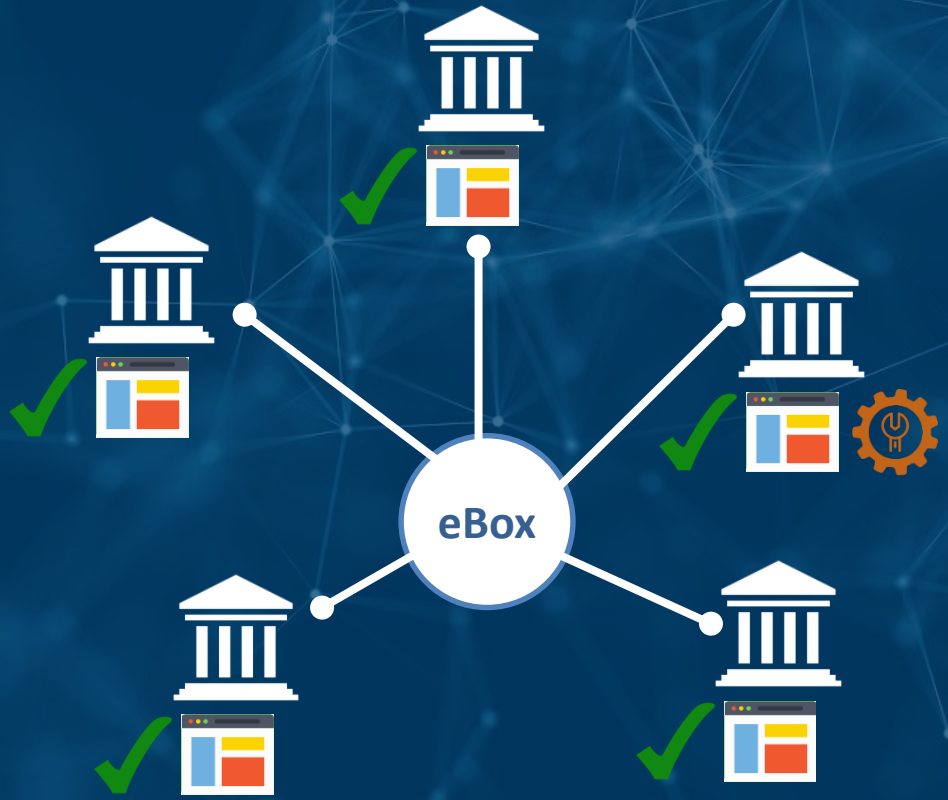
Privacy & confidentiality

Choice blockchain technology

Rights management

Hosting the nodes

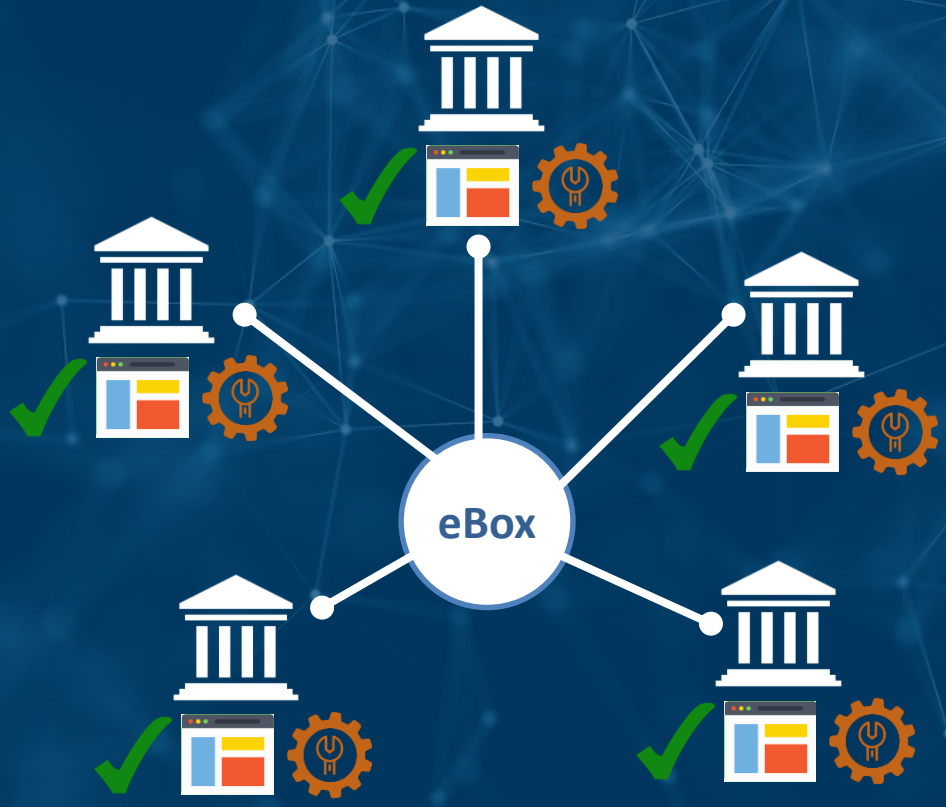
Rights management



WHO GRANTS AND REVOKES RIGHTS?

- Centralised → Single entity
  SPOF!

Rights management



WHO GRANTS AND REVOKES RIGHTS?

- Centralised → Single entity
  SPOF!
- Decentralised → majority of organisations

Rights management

WHO GRANTS AND REVOKES RIGHTS?

- Centralised → Single entity
  SPOF!
- Decentralised → majority of organisations
- Hybrid (E.g. Smals + 2 ministries)

AGENDA

Smals
ICT for society

- Finding a use case
- Privacy & confidentiality
- Choice blockchain technology
- Rights management
- **Hosting the nodes**

Where?

On-premise

Every participants maintains the infrastructure for her own node

Properties

- Cumbersome
- Expensive
- Insecure
- Distributed

Common infra provider

Everyone uses the same infrastructure provider (Blockhain as a Service)

Properties

- Convenient
- Cheaper
- More secure
- But, again central party!

Multiple infra providers

Max. x% of the nodes on the same infrastructure provider

Properties

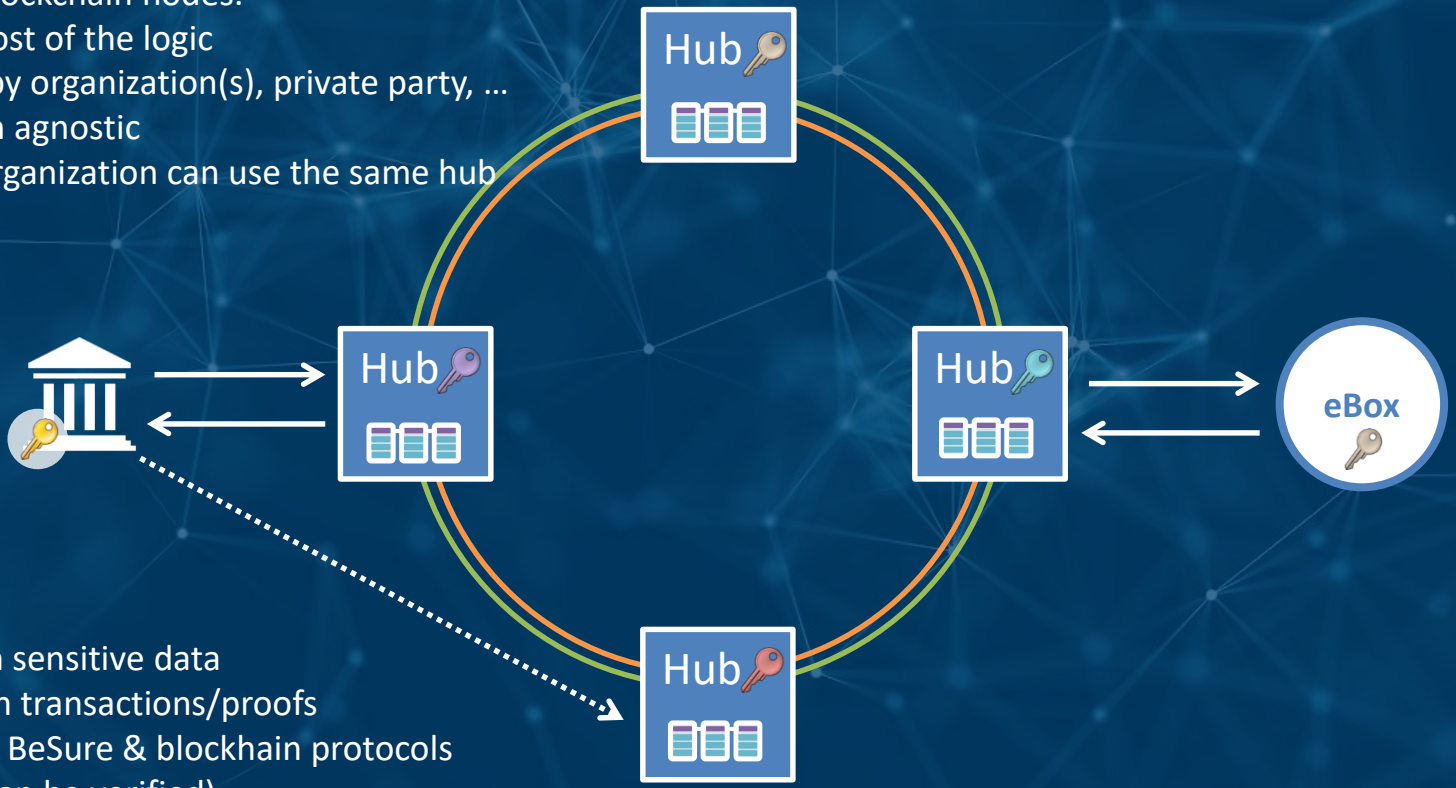
- Best compromise
- Governance overhead
- [Geographic distribution]

NOT ALL ORGANISATIONS ARE ABLE TO MANAGE THEIR OWN NODE

Semi-trusted hubs

Properties

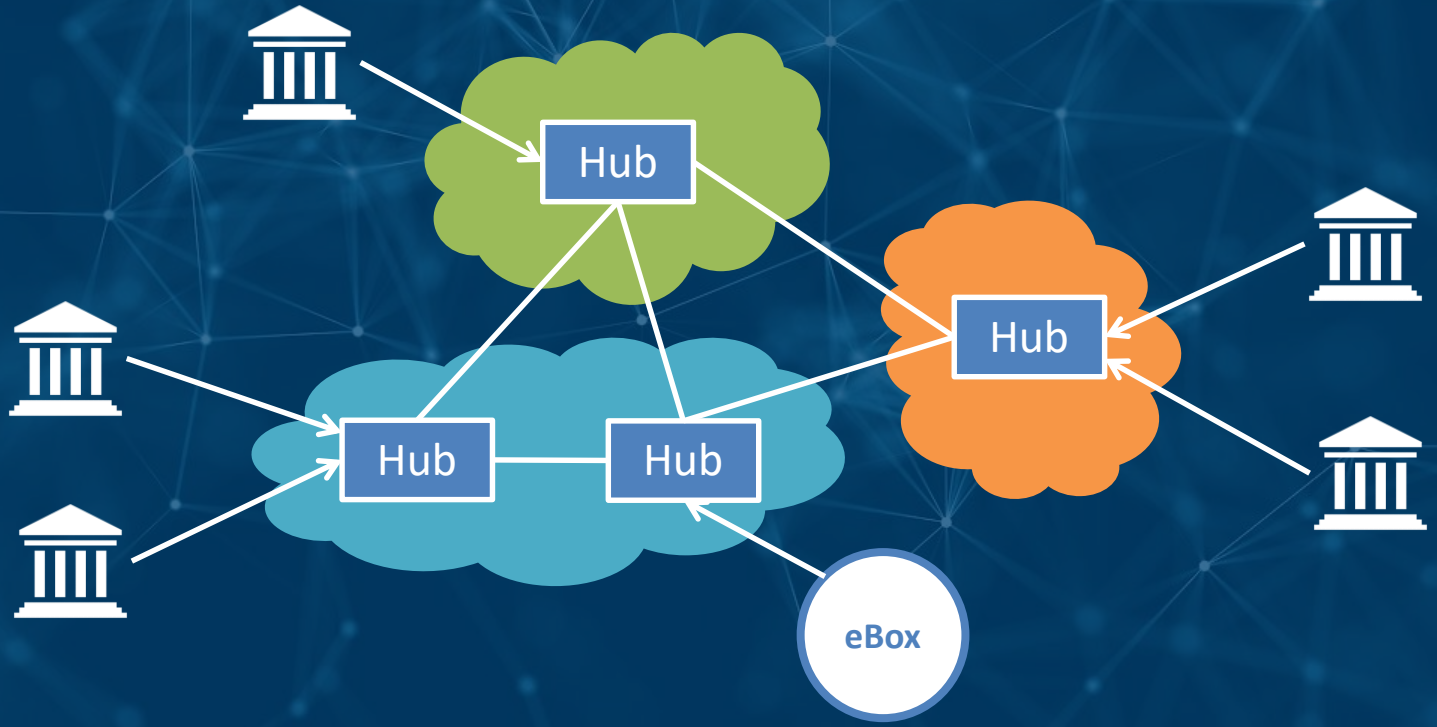
- The only blockchain nodes.
- Contain most of the logic
- Managed by organization(s), private party, …
- Application agnostic
- Multiple organization can use the same hub



Trust

- Don’t learn sensitive data
- Cannot sign transactions/proofs
- Should run BeSure & blockhain protocols properly (can be verified)

Hosting the nodes



AGENDA

Smals
ICT for society

Finding a use case
→ **not easy**

Privacy & confidentiality
→ **don't ignore**

Choice blockchain technology
→ **also tricky**

Rights management
→ **balance**

Hosting the nodes
→ **balance**

Publications

MAGISTRATES & LAWYERS

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

By Jurgen Goossens (Phd, UGent) & Kristof Verslype (Smals)

NOTARIES (FR)

Blockchain & contrats intelligents: Quel impact sur le notaire en tant qu'intermédiaire de confiance ?

By Benjamin Verheye (KU Leuven) & Kristof Verslype (Smals). Preface by Paul Danneels, CTO Fednot.

NOTARIES (NL)

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

By Benjamin Verheye (KU Leuven) & Kristof Verslype (Smals). Preface by Paul Danneels, CTO Fednot.

Questions & Contact

Kristof Verslype

PhD of Engineering (dept. computer science, University of Leuven)

Researcher, advisor, speaker author in crypto, privacy & blockchain tech

Smals Research

www.smalsresearch.be

@SmalsResearch

Smals ICT for society

www.smals.be

@Smals_ICT

www.cryptov.net

@KristofVerslype

kristof.verslype@smals.be

be.linkedin.com/in/verslype