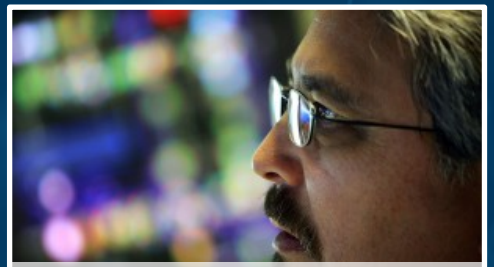

Smals
ICT for society
Blockchain & Privacy
Two cases from the government field
16/07/2019
KRISTOF VERSLYPE
SMALS RESEARCH

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

Introduction

BeSure
(2018 – Live?)

Medical Prescriptions
(2016 - PoC)

Remark: permissioned blockchains only

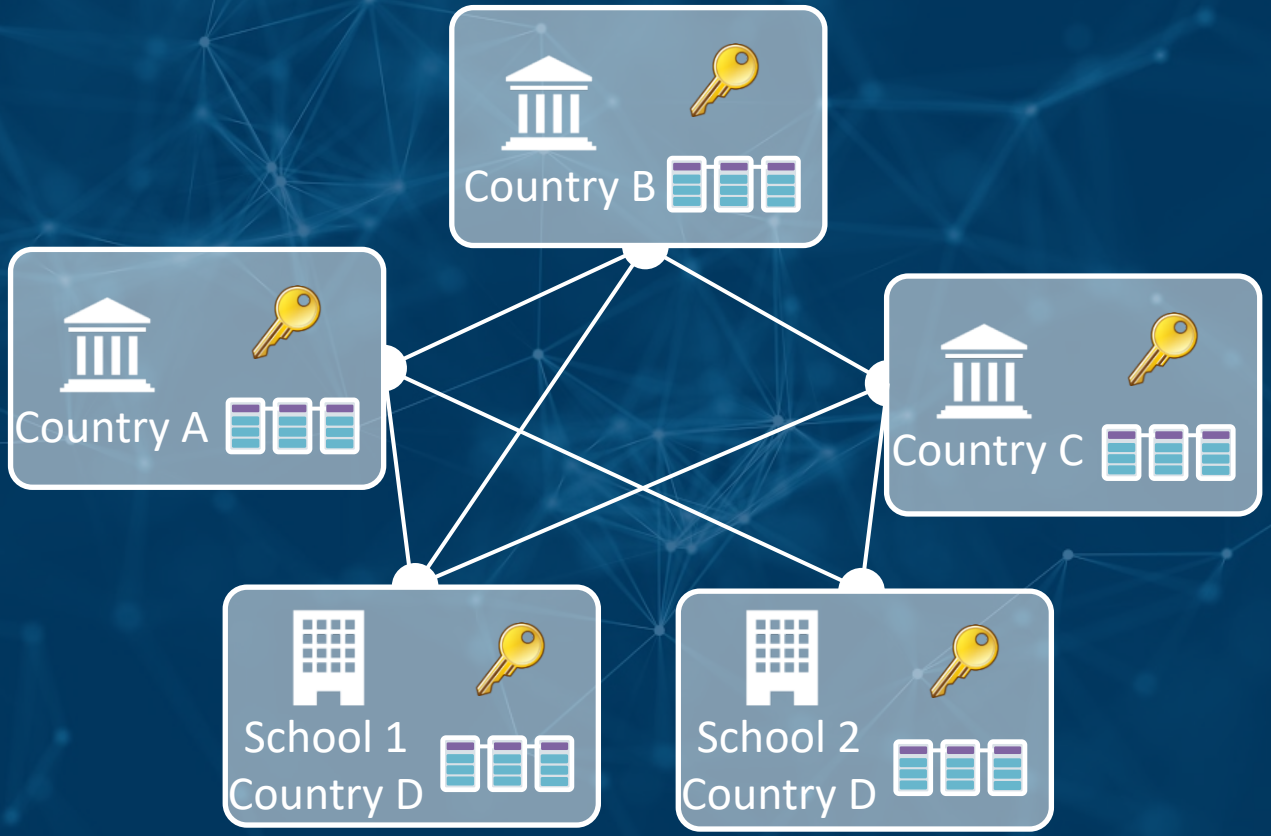
“We make abstraction of the GDPR”

PoC Diplomas

Citizens & employers outside blockchain network

Schools and governments add diplomas

Citizens have overview and dermine who can see what (with access link)



https://medium.com/wearetheledger/certified-for-life-international-exchange-authentication-of-diplomas-via-blockchain-4e947720edd9

PoC Diploma's

All diploma data in plain text on blockchain

- All participants should be trusted (abuse/theft)
- GDPR ignored
- Competing schools see each others' data

https://medium.com/wearetheledger/certified-for-life-international-exchange-authentication-of-diplomas-via-blockchain-4e947720edd9

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

GDPR

Anonymized data	Pseudonimised data	Identifiable data
Not linkable to a natural person	**Linkable with additional info** to a natural person	**Linkable without extra info** to a natural person

Personal data

Registration of data

Transfer of assets

More accurate:

Smart contract function calls

Every icon icon (and, hence every transaction) potentially personal data

Very quickly personal data in blockchain context

ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) https://www.pdpjournals.com/docs/88197.pdf

Blockchain contains potentially maby personal data

GDPR applicable

Storage limitation	**Right to be forgotten**	**Right to restriction of processing**	**Appropriate security measures (moving)**

PERMISSIONED BLOCKCHAIN

- Removal of extra data may suffice
- Controller-controller relationship → shared responsibility
- Right to be forgotten: Citizen send request to SPOC, which forwards request to relevant blockchain participants
- Privacy Impact Assessment may be required

https://www.r3.com/wp-content/uploads/2018/04/GDPR_Blockchains_R3.pdf

"Most current blockchain projects are likely incompatible with the GDPR."

Michèle Finck
Max Planck Institute for Innovation
& University of Oxford

February 2018

https://www.law.ox.ac.uk/business-law-blog/blog/2018/02/blockchains-and-gdpr

“We make abstraction of the GDPR”

→ Importance *privacy by design & security by design*

AGENDA

Smals
ICT for society

Introduction

BeSure
(2018 – Live?)

Medical Prescriptions
(2016 - PoC)

BeSure

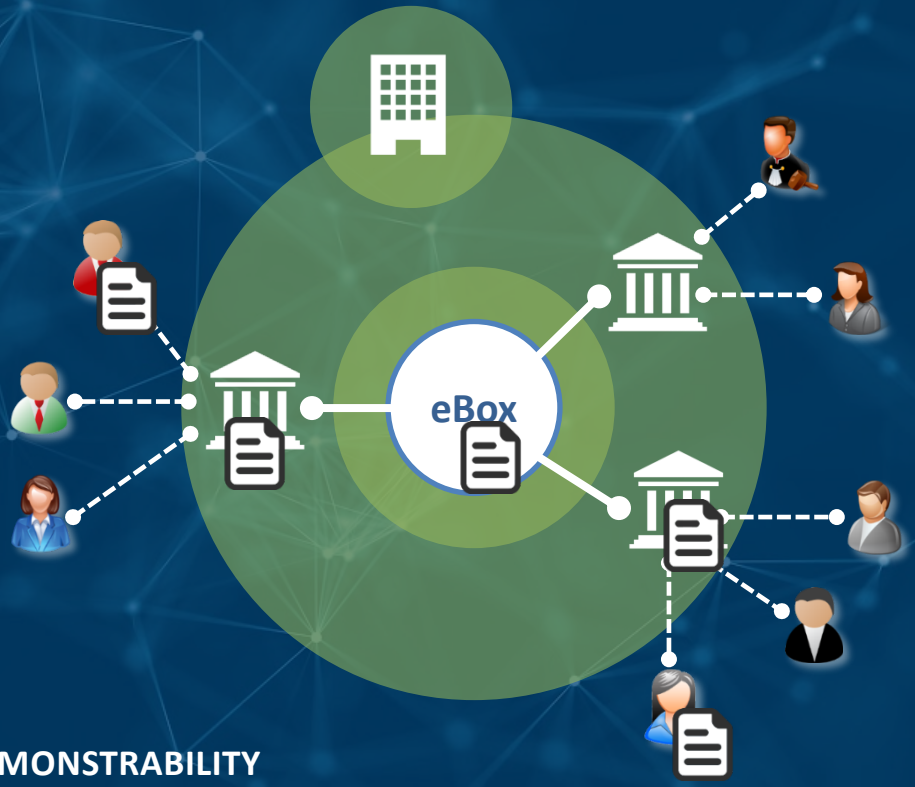
Demonstrability service

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

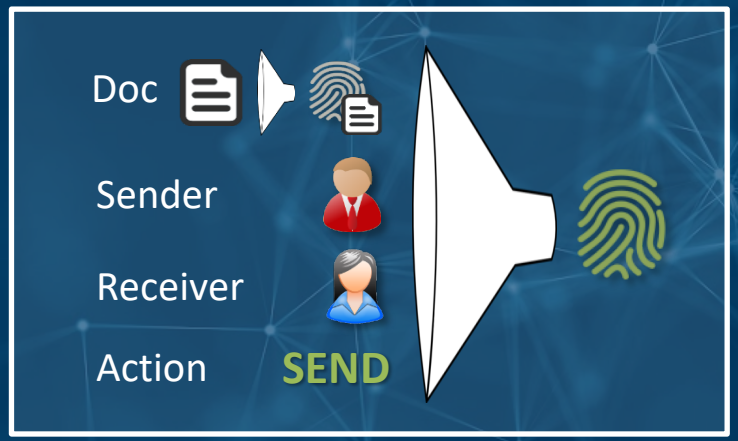


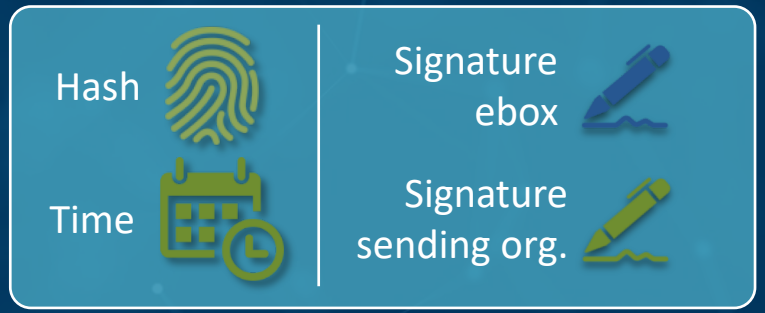
Demonstrability

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

: Circle of trust

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 .

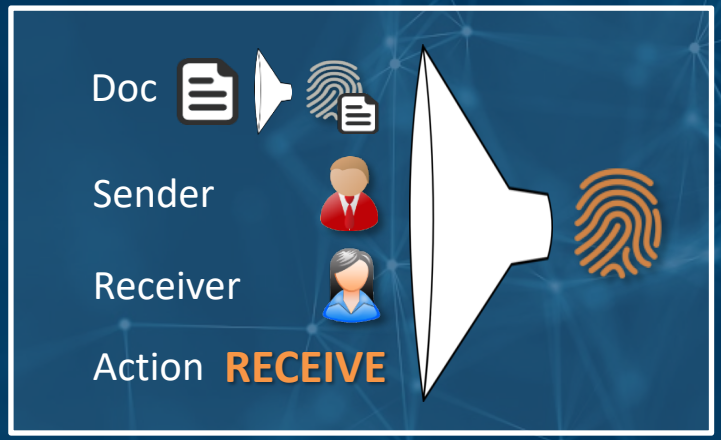
Document known (and +)

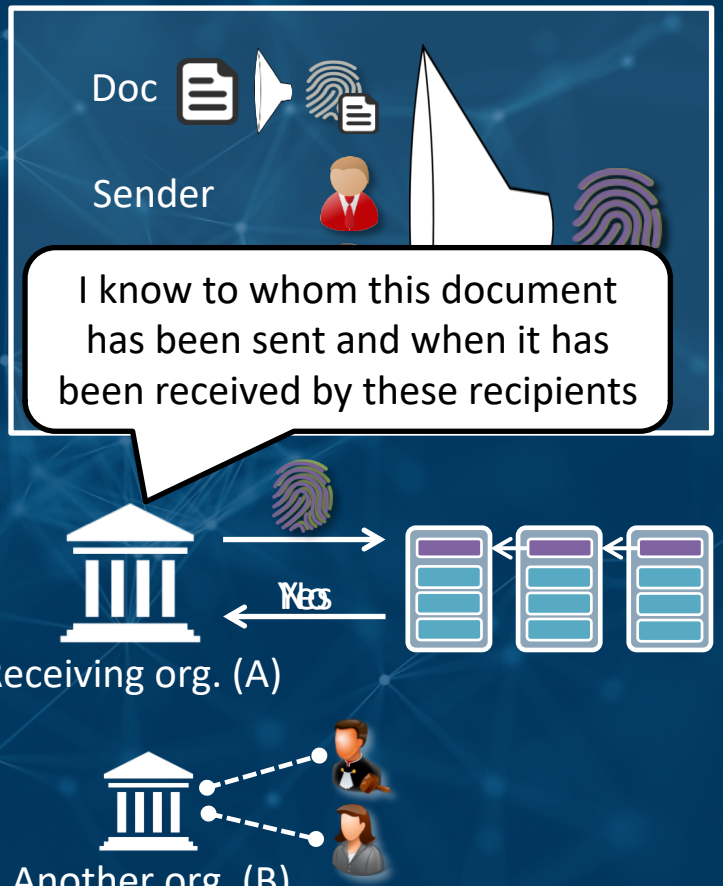
Proof that has sent the document at moment to .

Watch out for low-entropy documents!

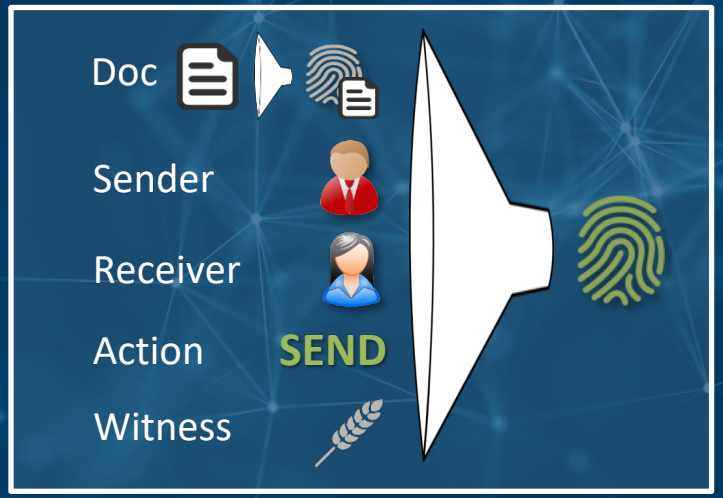
RECEIVE is analogous

Confidentiality & privacy





Transfer-specific witnesses



Disclosure of single witness to proof delivery to eBox / receipt by organization

Witness should be stored well (or deriveable from well-protected private key + public key)

Right to be forgotten (GDRP): remove witness

Confidentiality & privacy

HIDDEN

- Sender id, recipient id, doc content
- Action type (SEND, RECEIVE, REQUEST)
- SEND-RECEIVE link

REVEALED

- Identity of organisation.

BeSure

Watch out with naive blockchain solutions!

Thourough analysis necessary

Privacy & confidentiality can be well protected

But adds extra complexity

AGENDA

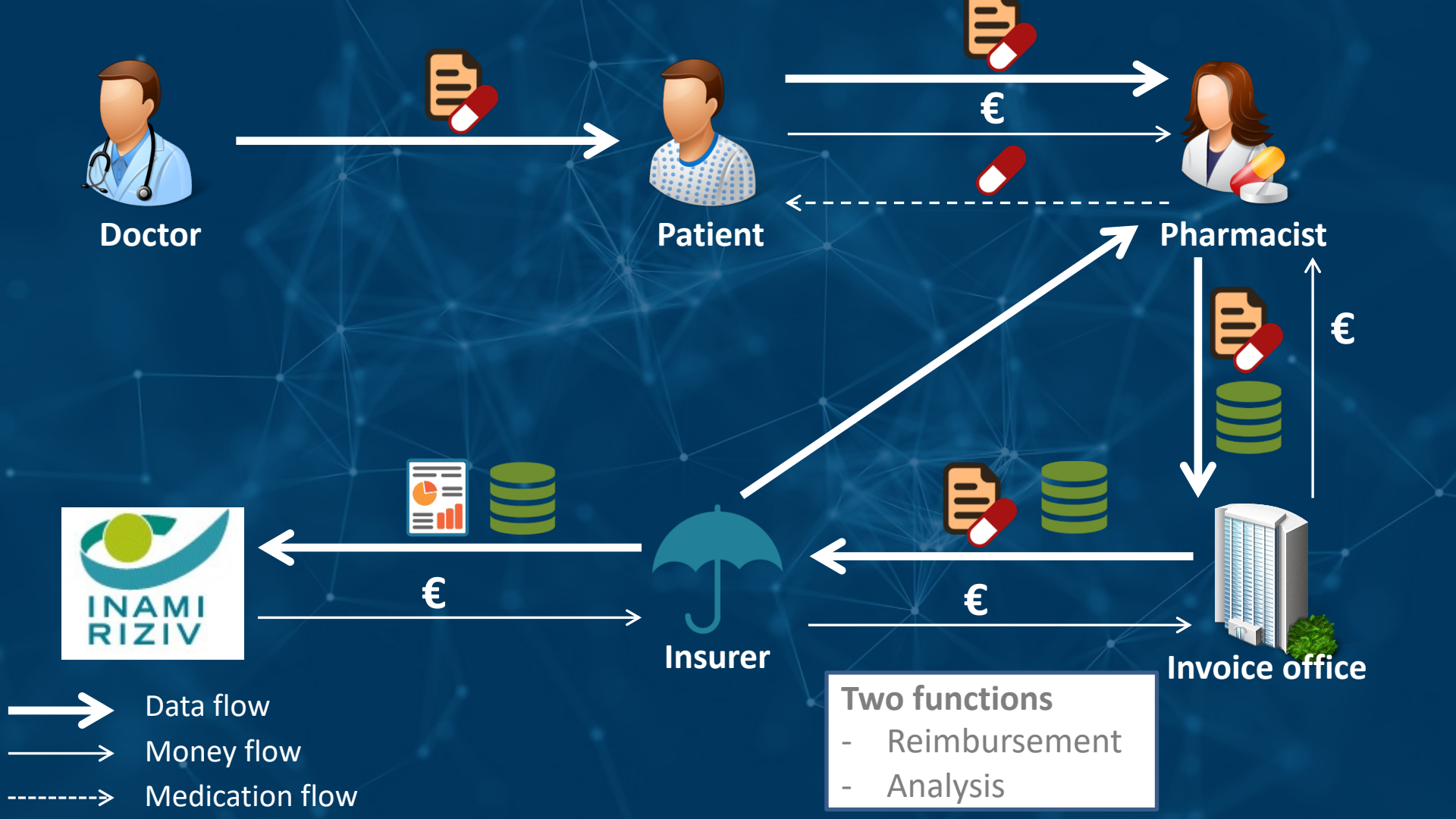
Smals
ICT for society

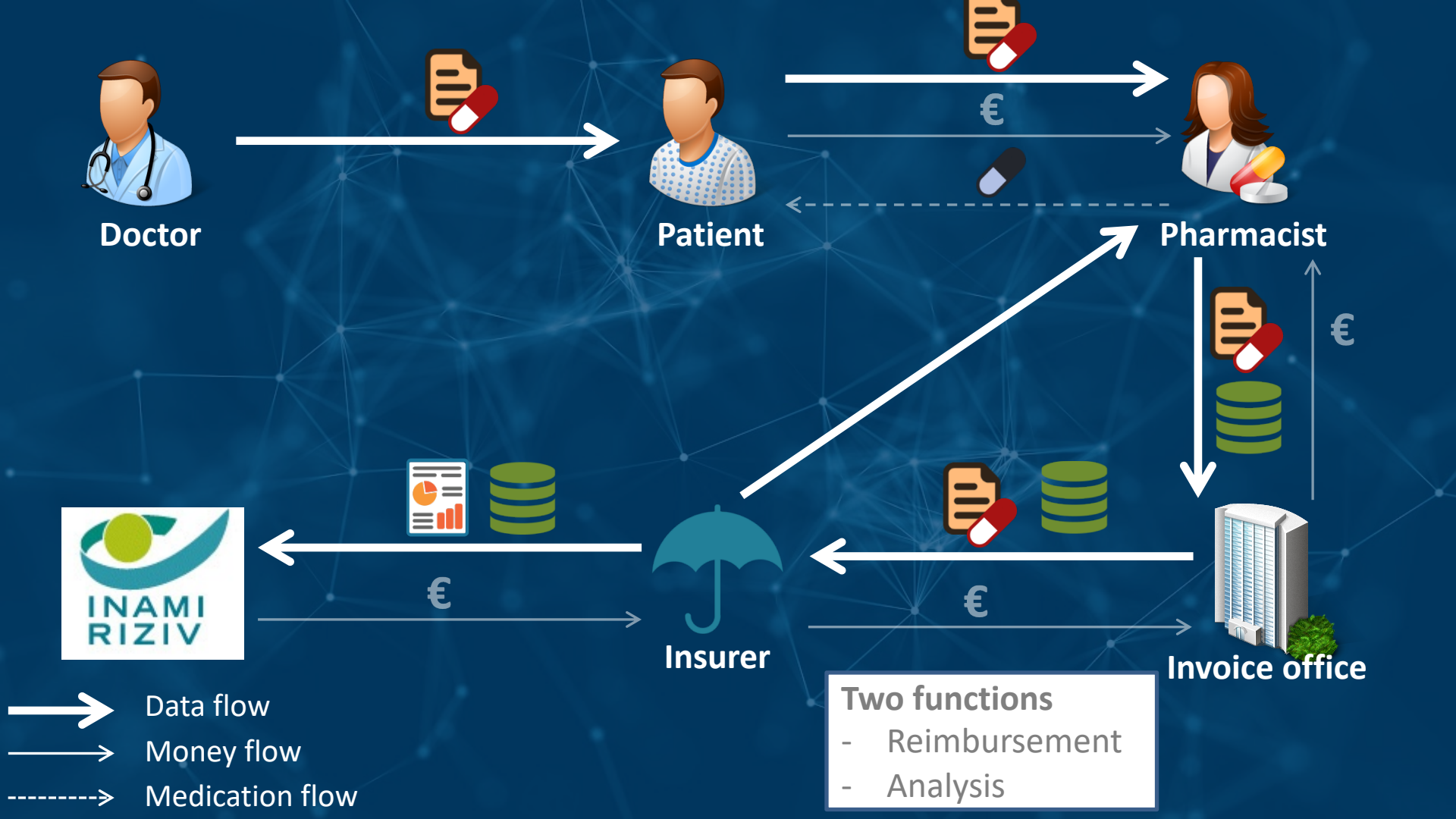
Introduction

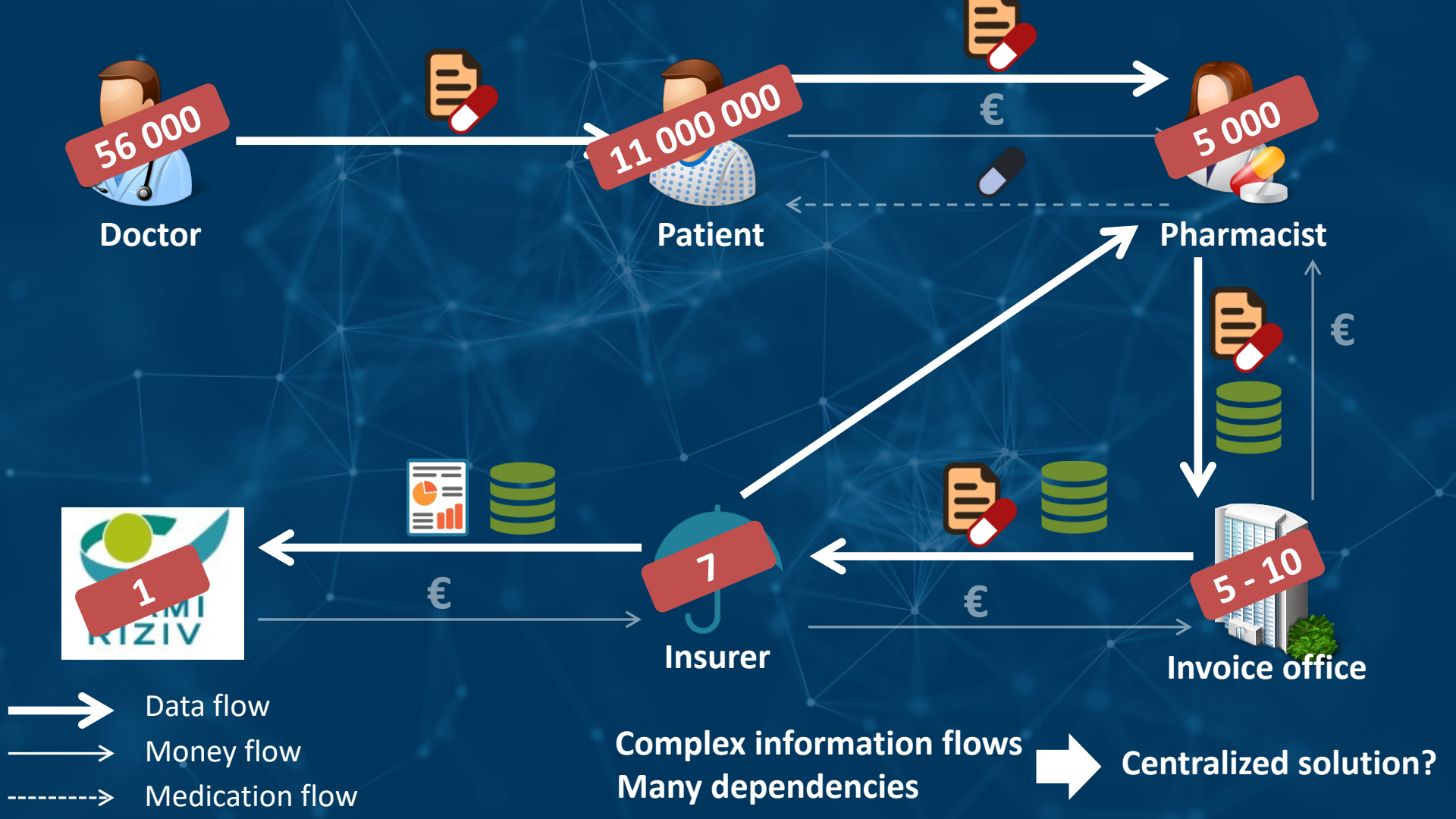
BeSure
(2018 – Live?)

Medical Prescriptions
(2016 - PoC)

Experiment: How far can we go with blockchain?


Doctor
Patient
Pharmacist
€
€
€
€
INAMI
RIZIV
Insurer
Invoice office
Two functions
- Reimbursement
- Analysis
Data flow
Money flow
Medication flow


Doctor
Patient
Pharmacist
€
€
€
€
INAMI
RIZIV
Insurer
Invoice office
Two functions
- Reimbursement
- Analysis
Data flow
Money flow
Medication flow


56 000
Doctor
11 000 000
Patient
5 000
Pharmacist
€
1
RIZIV
7
Insurer
5 - 10
Invoice office
€
€
€
Data flow
Money flow
Medication flow
Complex information flows
Many dependencies
Centralized solution?

Doctor

Patient

Pharmacist

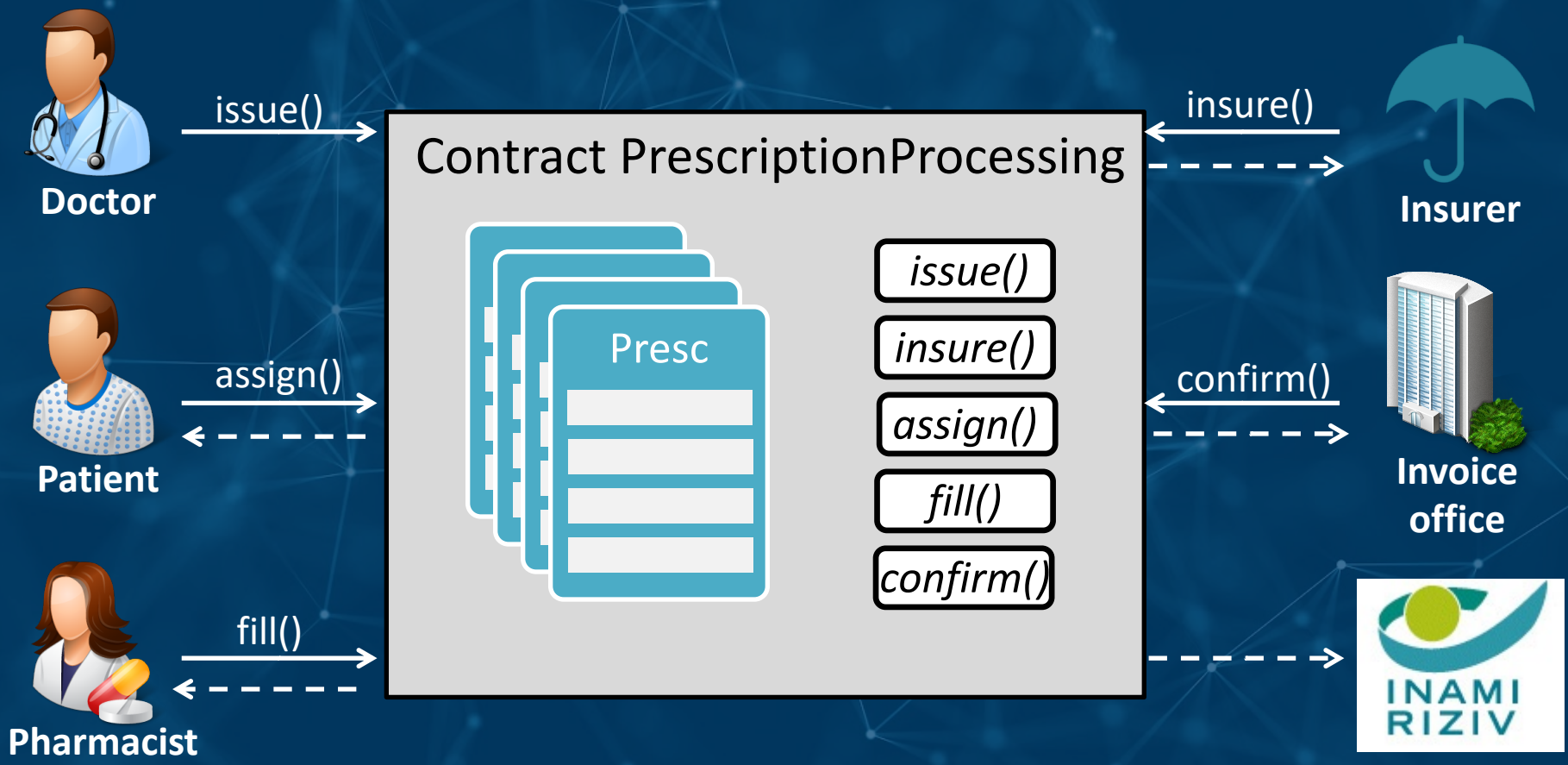
Insurer

Invoice office

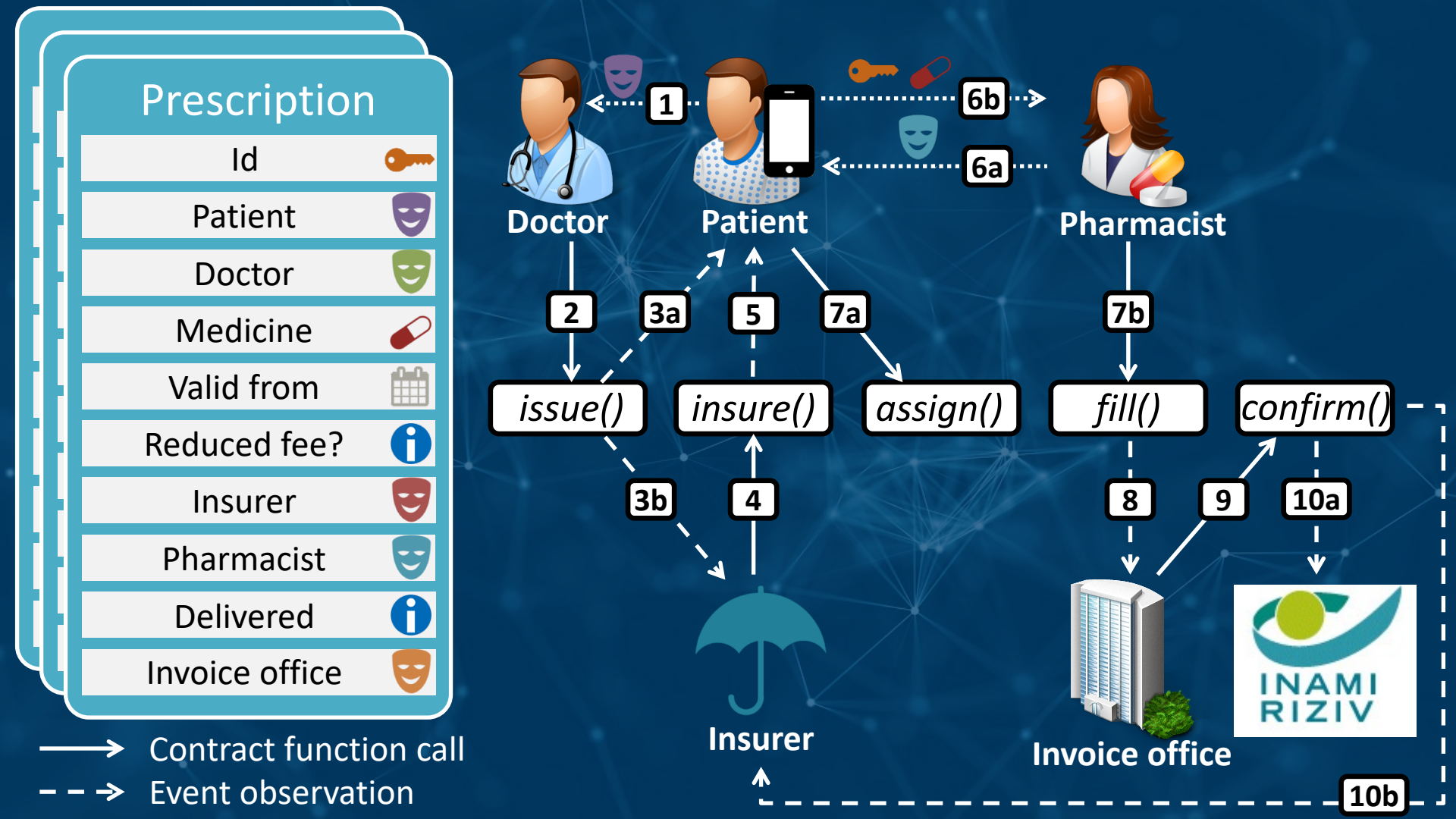
Shown on smartphone

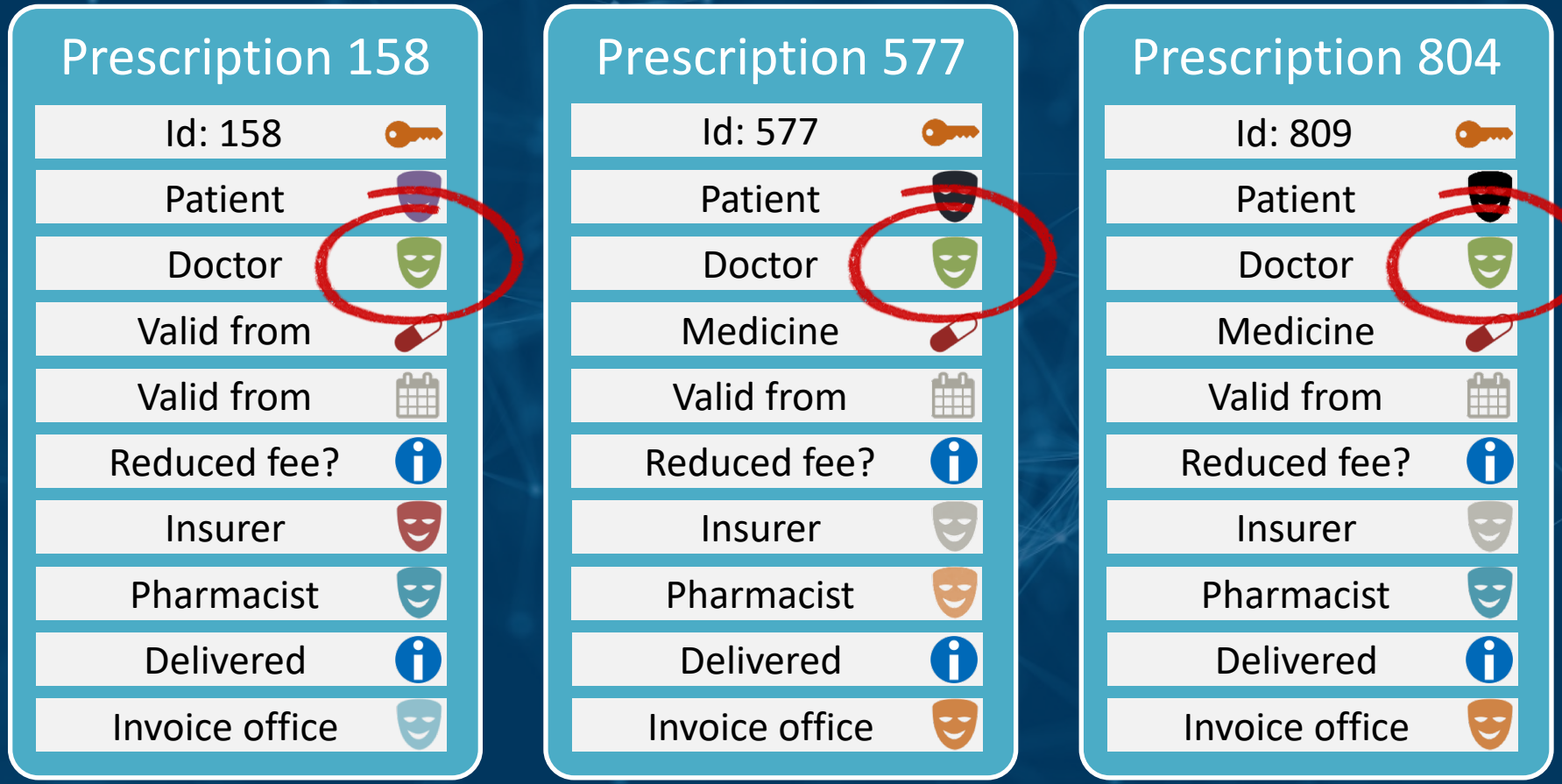
All other communication with blockchain

Privacy & confidentiality enterprise data guaranteed



Contract enforces rules such as “no double spend” & “only doctors can issue”


Prescription
Id
Patient
Doctor
Medicine
Valid from
Reduced fee?
Insurer
Pharmacist
Delivered
Invoice office
Contract function call
Event observation
Doctor
Patient
Pharmacist
1
6b
6a
2
3a
5
7a
7b
issue()
insure()
assign()
fill()
confirm()
3b
4
8
9
10a
10b
Insurer
Invoice office
INAMI
RIZIV

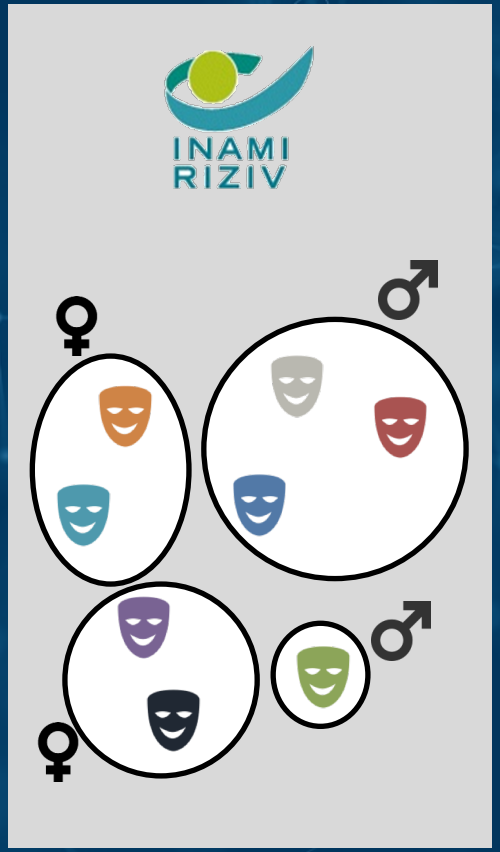


Permanent pseudonyms → insufficient protection of 1) citizen's privacy & 2) confidentiality enterprise data

One-time pseudonyms

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

One-time pseudonyms



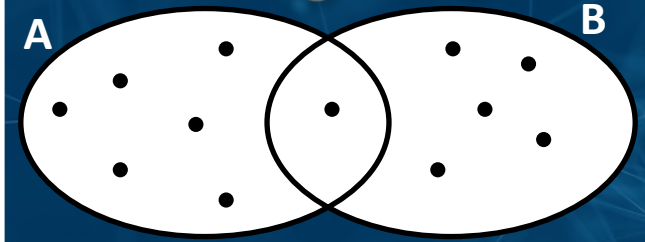
Link attack

er matches physical opbservations to blockchain data

Prescription

- Id
- Patient
- Doctor
- Medicine
- Valid from
- Reduced fee?
- Insurer
- Pharmacist
- Delivered
- Invoice office

Doctor: 02/04/17, 21h30 (A)
Pharmacist: 28/04/17, 20h45 (B)



Difficult attack, but one success enough to torpedo project
→ Encryption of sensitive data in blockchain/smart contract

Encryption

domus medica

CHRISTELIJKE MUTUALITEIT

INAMI RIZIV

My

Prescription

Pantoprazol 20mg

Reduced fee?

...

My

Prescription

Pantoprazol 20mg

???

...

Rest of the world

Prescription

???

???

...

Medical prescriptions

Different views
- One-time pseudonyms
- Encryption

Key management
Every entity needs one or more well-protected keys

Reduced trust in participants

Watch out with naive blockchain solutions!

Thourough analysis necessary

Privacy & confidentiality can be well protected

But adds extra complexity

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 ICT for society

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