Far beyond (or nearer) trust:

addressing the main challenges associated to privacy protection and security management in the data era

David Arroyo Guardeño
Tenured Scientist

CSIC
Consejo Superior de Investigaciones Científicas

iteefi
Instituto de Tecnologías Físicas y de la Información

UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional

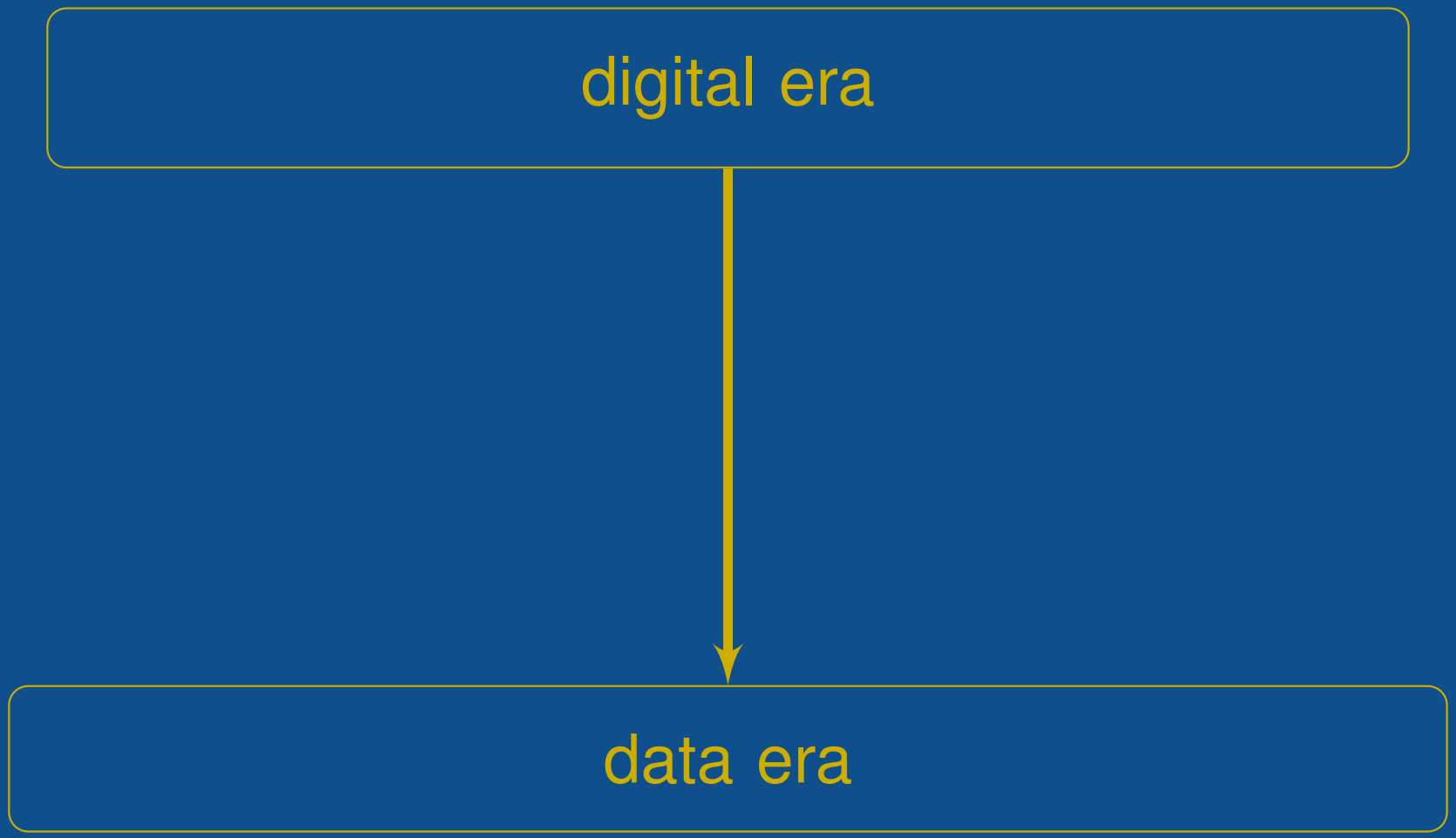
SP|RS

TRESCA

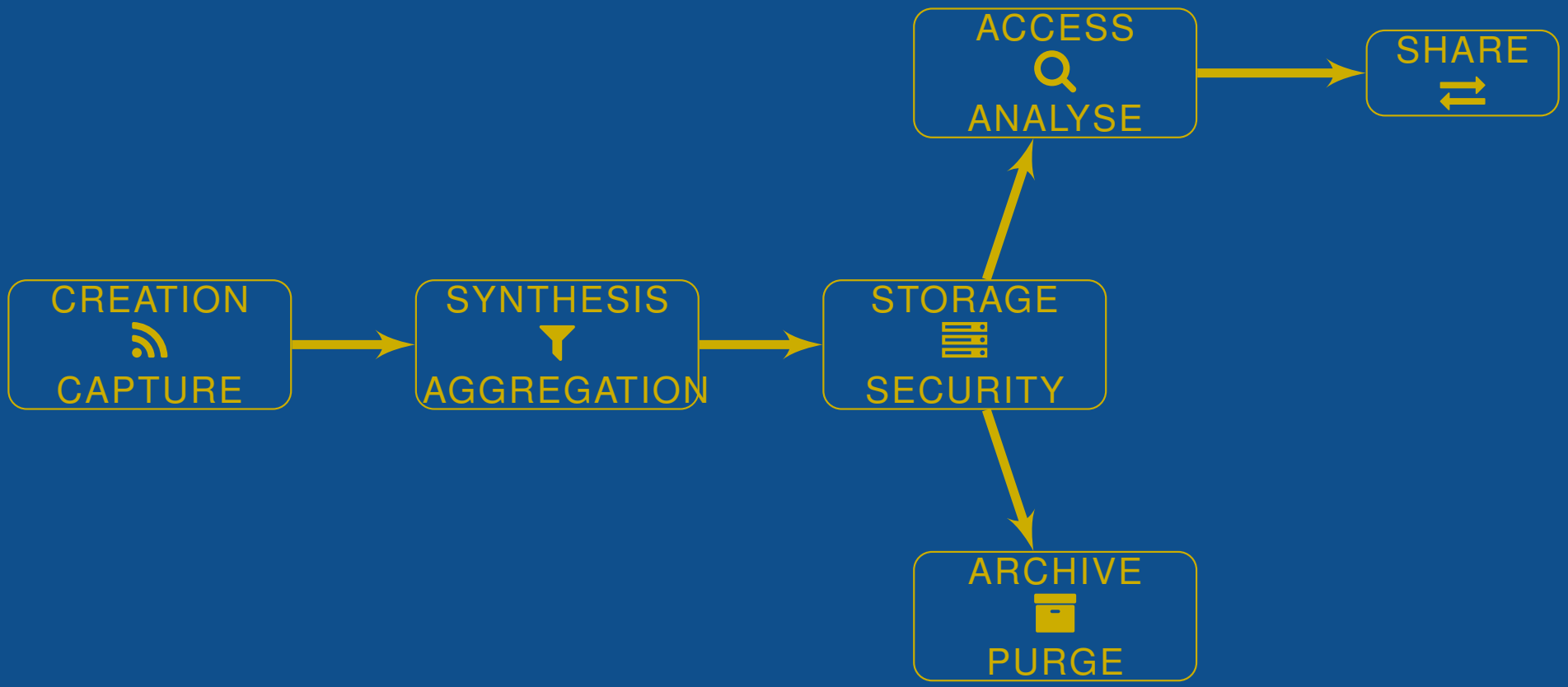
This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 872855.

1. *Introduction*
2. *ICT relevance*
3. *Cybersecurity*
4. *Main challenges in cybersecurity*
5. *Conclusions*
6. *GiCSI's role in SPIRS*

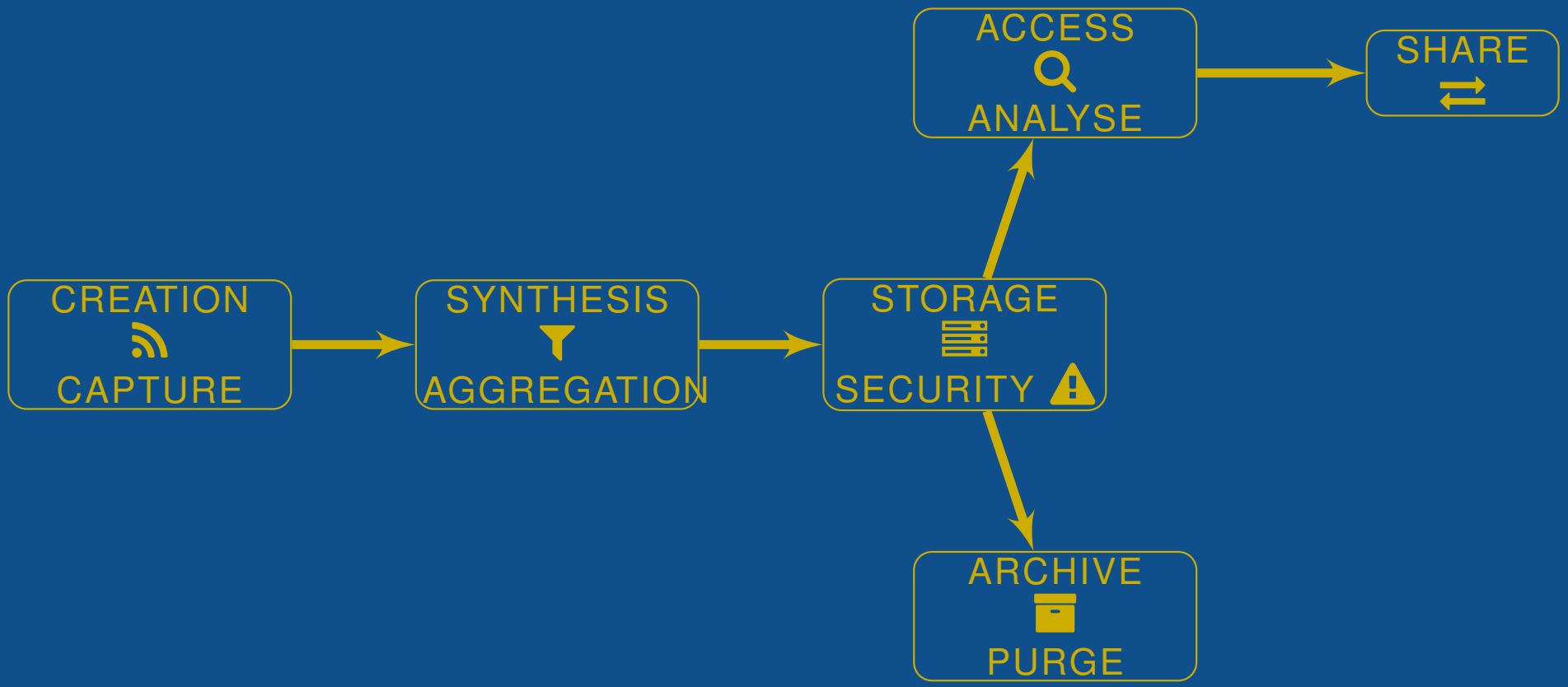
digital era


digital era
data era

Data lifecycle



Data lifecycle



Our daily activities are organized around ICT…

BRITISH AIR WOES British Airways website suffering technical issues as customers struggle to access bookings

Frustrated passengers alerted the airline to the issue on social media

john shammas
5 Jan 2018, 10:34 | Updated: 5 Jan 2018, 23:03

Comment now

BRITISH Airways customers were struggling to access their account online as the website experienced technical issues this morning.

A number of frustrated passengers alerted the airline to the issue on social media.

THREAT INTELLIGENCE

1/23/2020
10:00 AM

Kelly Jackson Higgins
News

Connect Directly

0 COMMENTS
COMMENT NOW

Login

50% 50%

Like Tweet Share

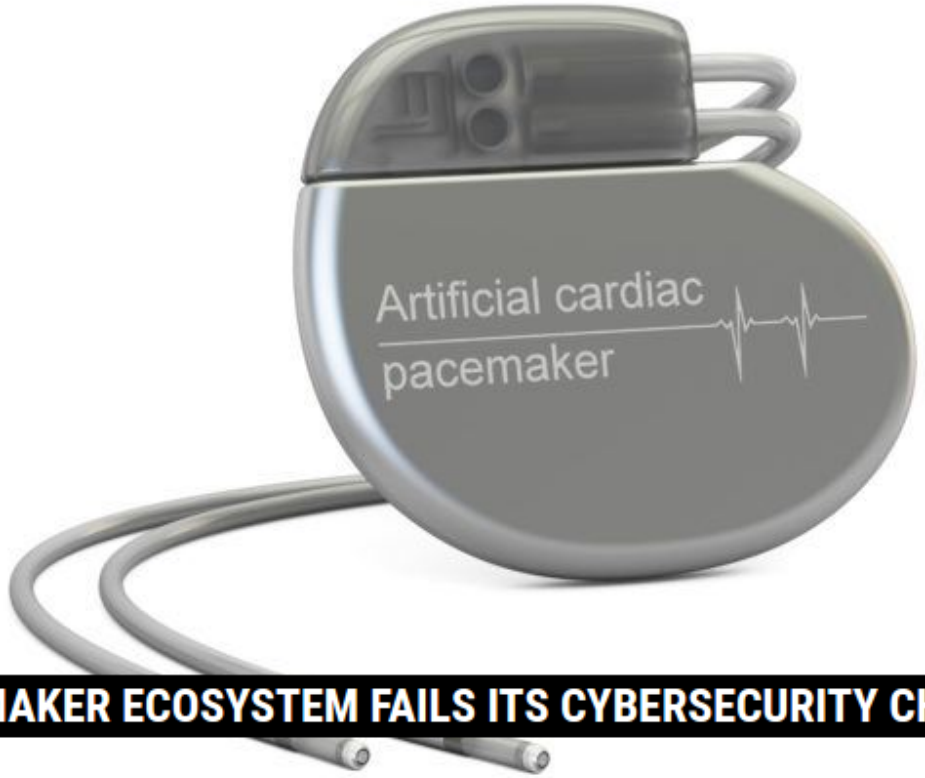
Ryuk Ransomware Hit Multiple Oil & Gas Facilities, ICS Security Expert Says

Attackers 'weaponized' Active Directory to spread the ransomware

threatpost

CATEGORIES | FEATURED | PODCASTS | VIDEOS

Welcome > Blog Home > IoT > Pacemaker Ecosystem Fails its Cybersecurity Checkup



PACEMAKER ECOSYSTEM FAILS ITS CYBERSECURITY CHECKUP

by Michael Mimoso Follow @mike_mimoso

May 26, 2017 , 11:00 am

. . . we should take care of ICT

Information is valuable itself...

- Who can access information

Information is valuable itself...

- Who can access information
- What can she do with the information?

Information is valuable itself...

- Who can access information
- What can she do with the information?
- How long should she have access to information?

Information is valuable itself...

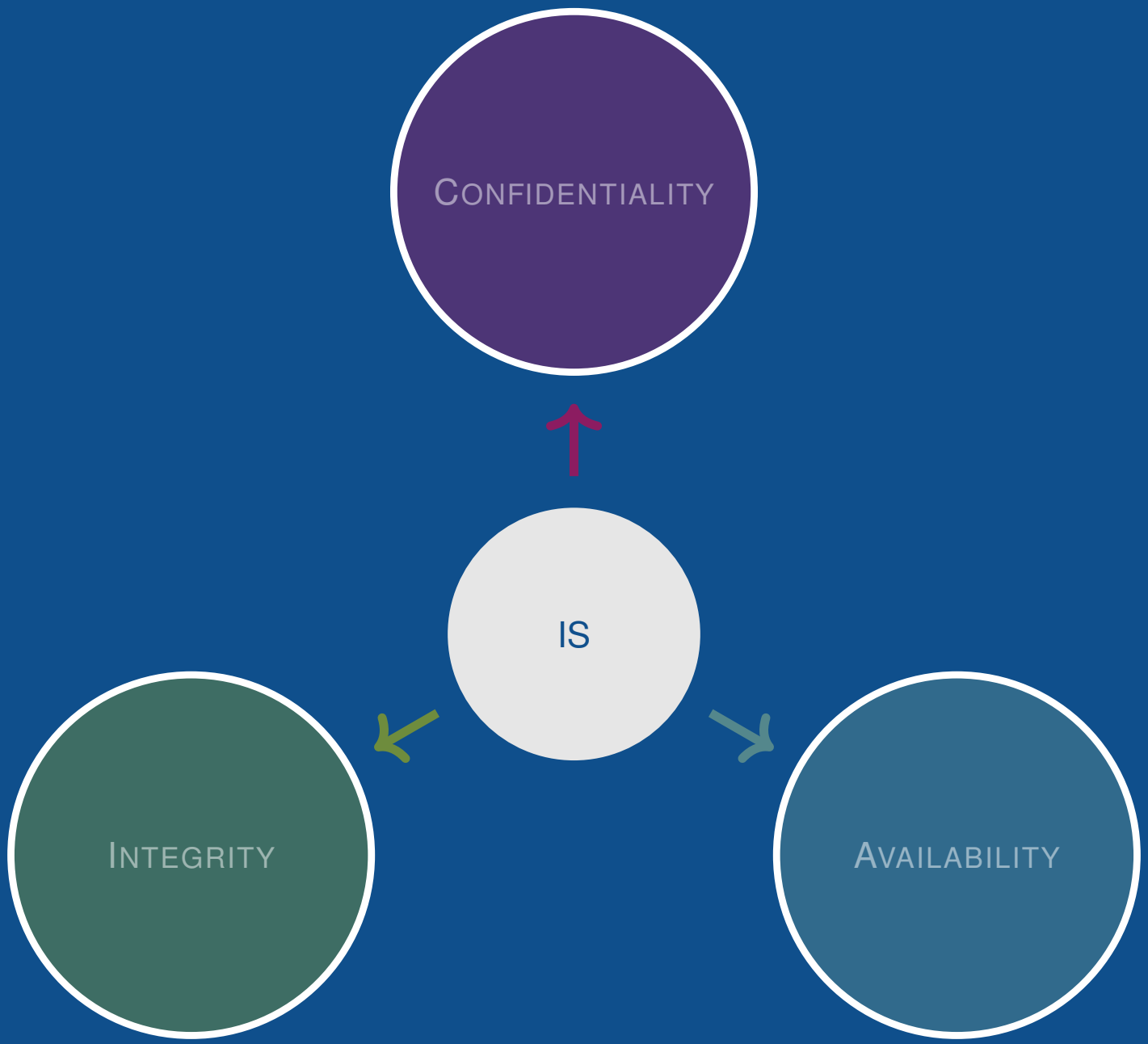
- Who can access information
- What can she do with the information?
- How long should she have access to information?
- How can she access information

Information is valuable itself...

- Who can access information
- What can she do with the information?
- How long should she have access to information?
- How can she access information
- When a source of information can be considered as trusted?

Information is valuable itself...

- Who can access information
- What can she do with the information?
- How long should she have access to information?
- How can she access information
- When a source of information can be considered as trusted?


CONFIDENTIALITY
IS
INTEGRITY
AVAILABILITY

Cryptography

Cryptography

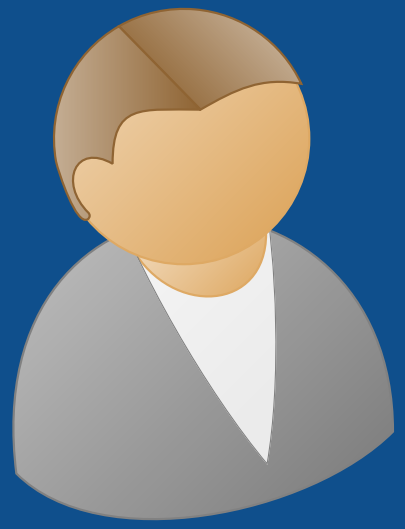
SYMMETRIC
or secret key

Cryptography

SYMMETRIC
or secret key

ASYMMETRIC
or public key

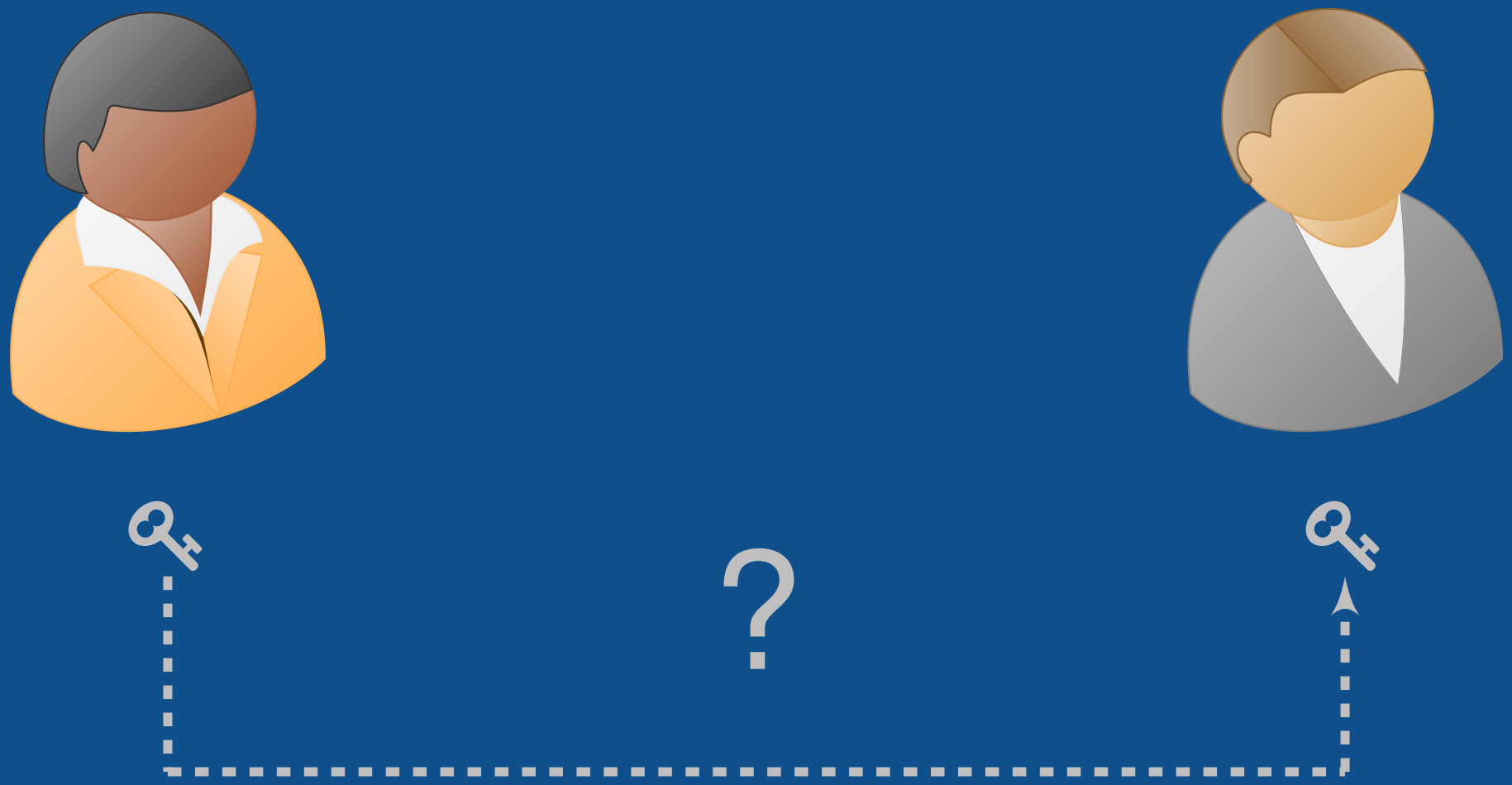
Symmetric cryptography (e.g., AES)



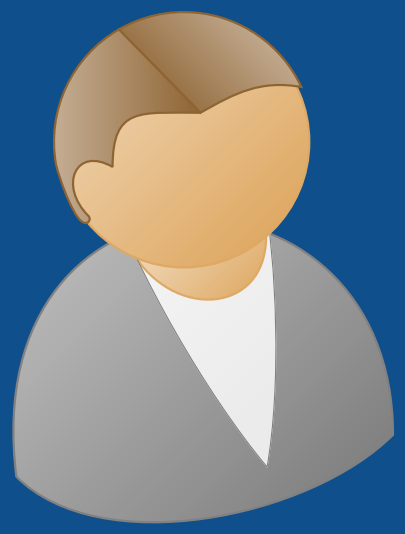
Secret key

session

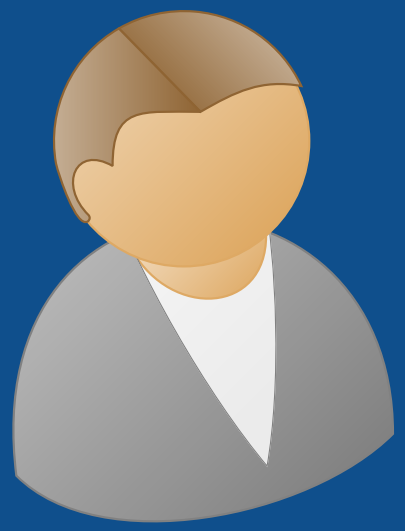
Symmetric cryptography (e.g., AES)



Asymmetric cryptography (e.g., RSA)



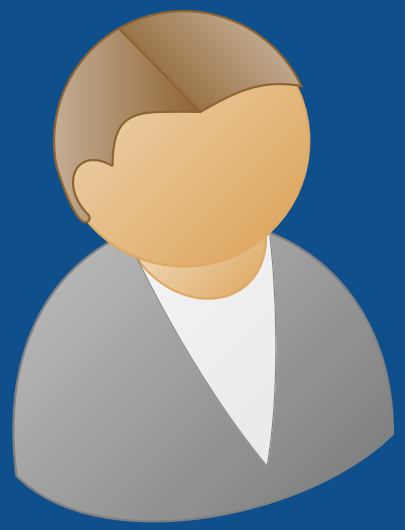
Asymmetric cryptography (e.g., RSA)



Asymmetric cryptography (e.g., RSA)

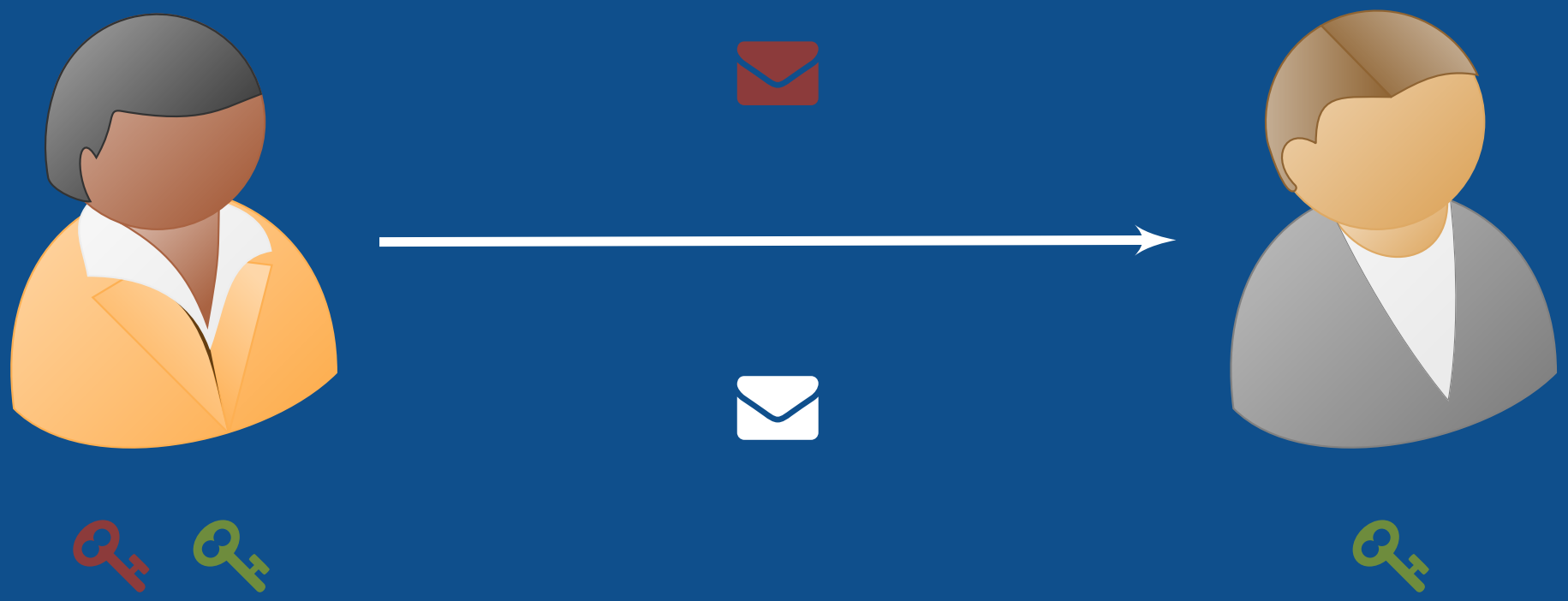
Asymmetric cryptography (e.g., RSA)

Asymmetric cryptography (e.g., RSA)

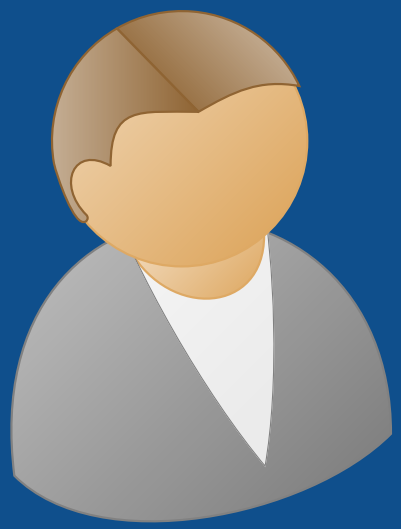


Conventional digital signature

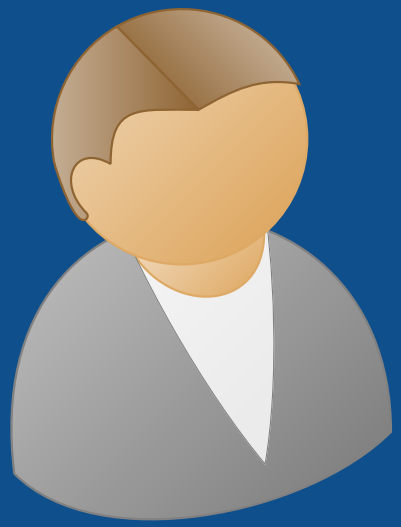
Conventional digital signature



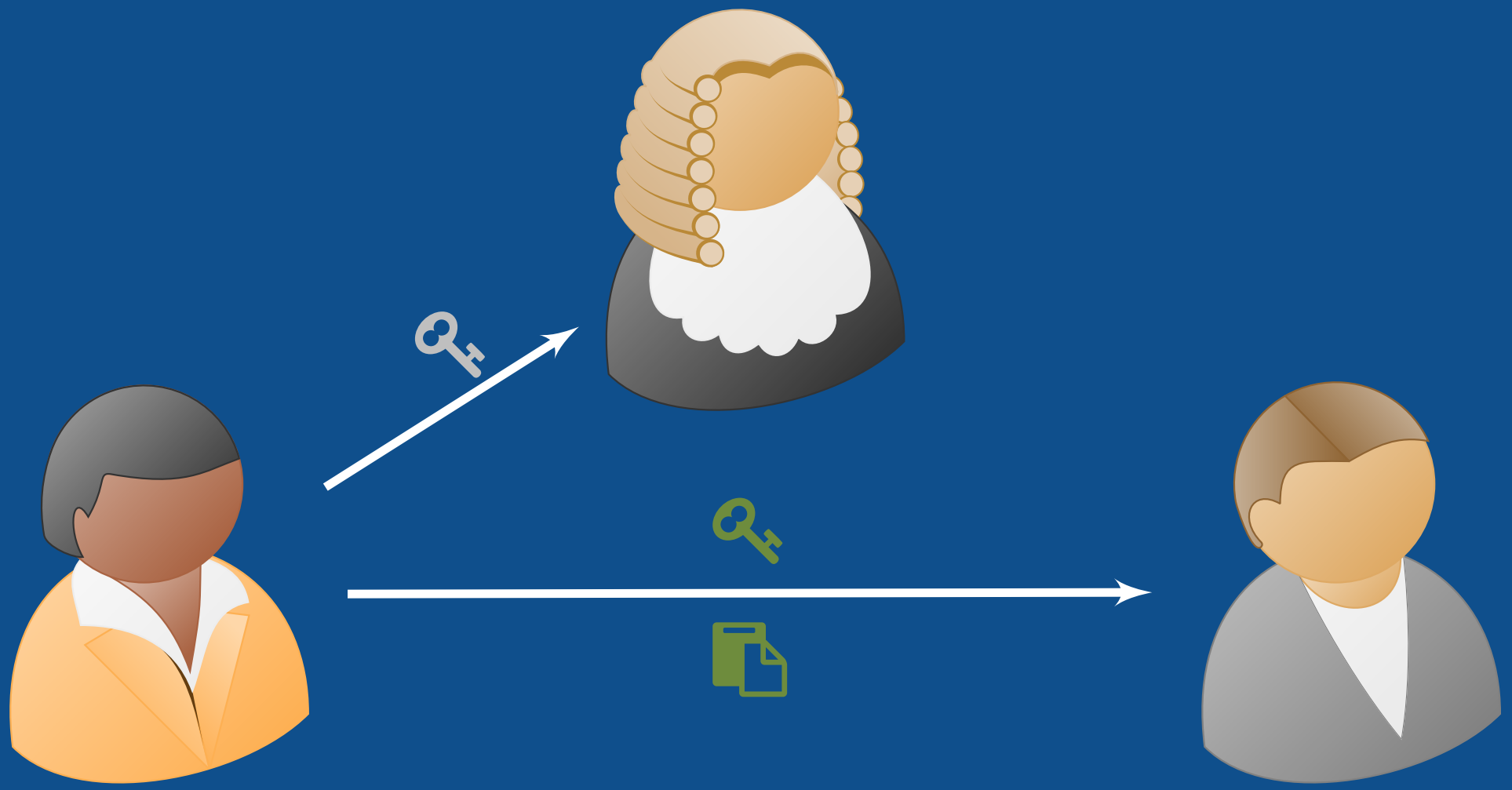
Conventional digital signature



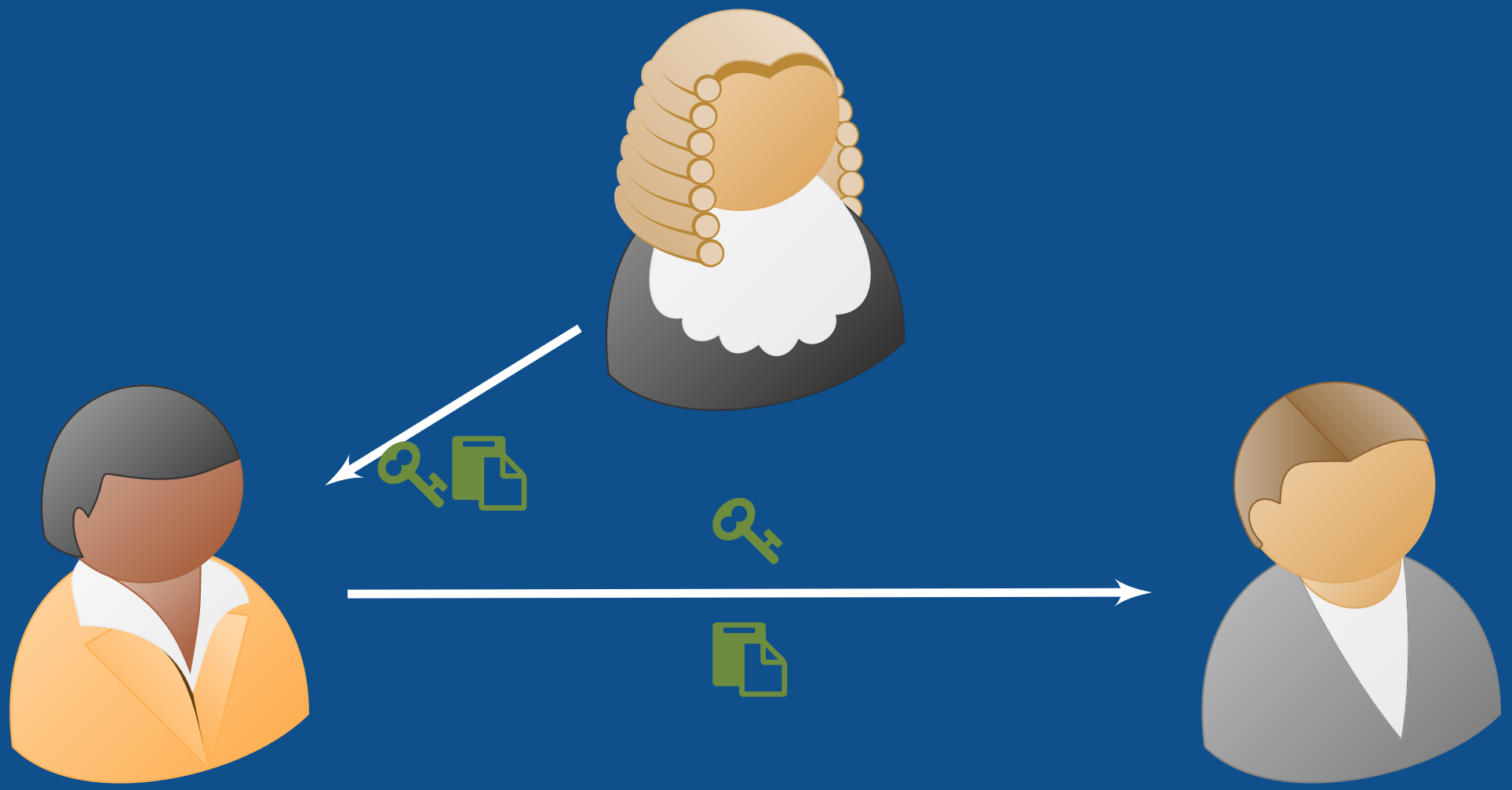
Conventional digital signature



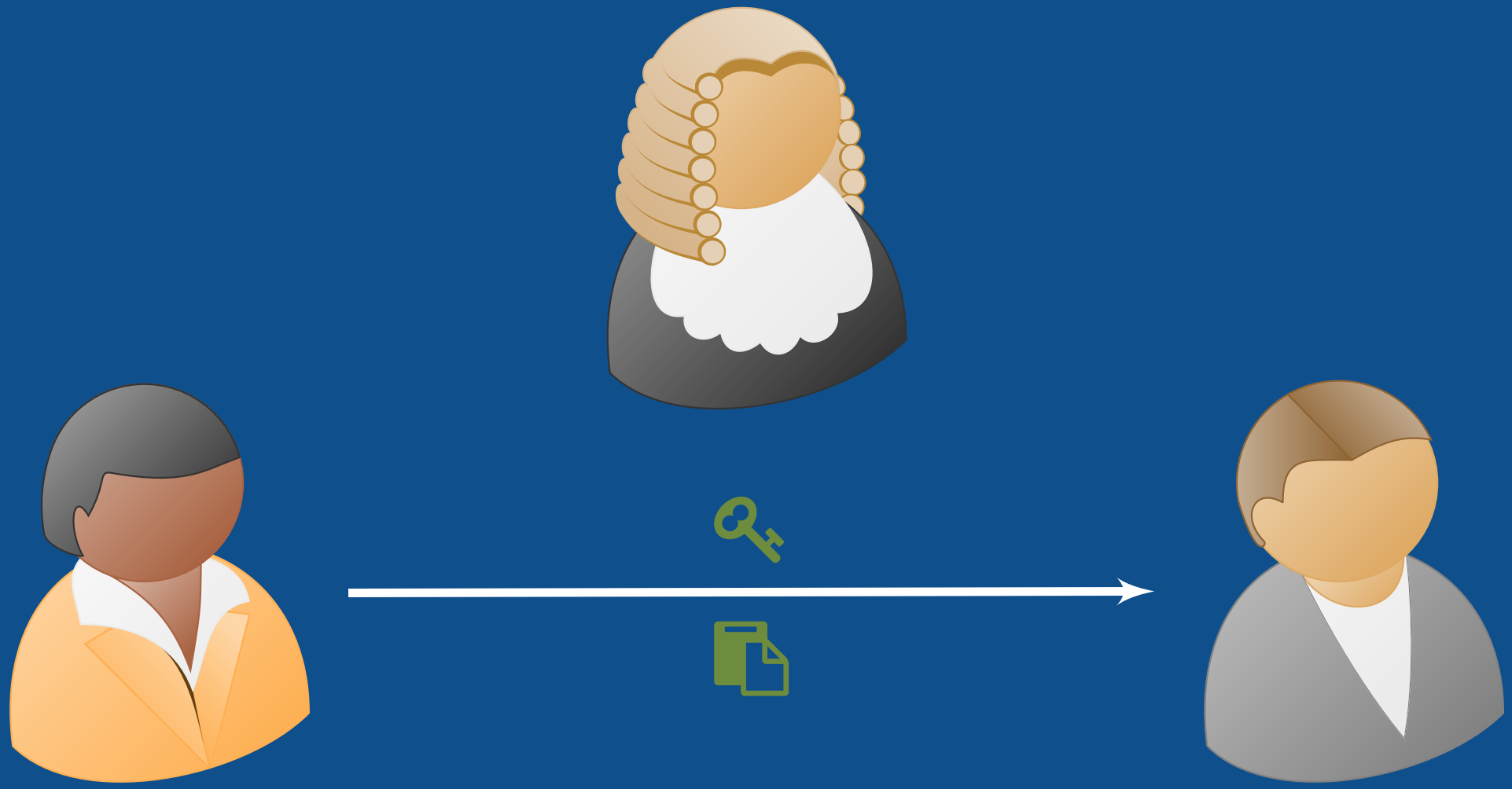
Who guarantees the public key is not fake?



Who guarantees the public key is not fake?



Who guarantees the public key is not fake?



X.509 standard

Trust centralization

Digital identity

Digital identity

Something you know

Password

Digital identity

Something you know

Something you have

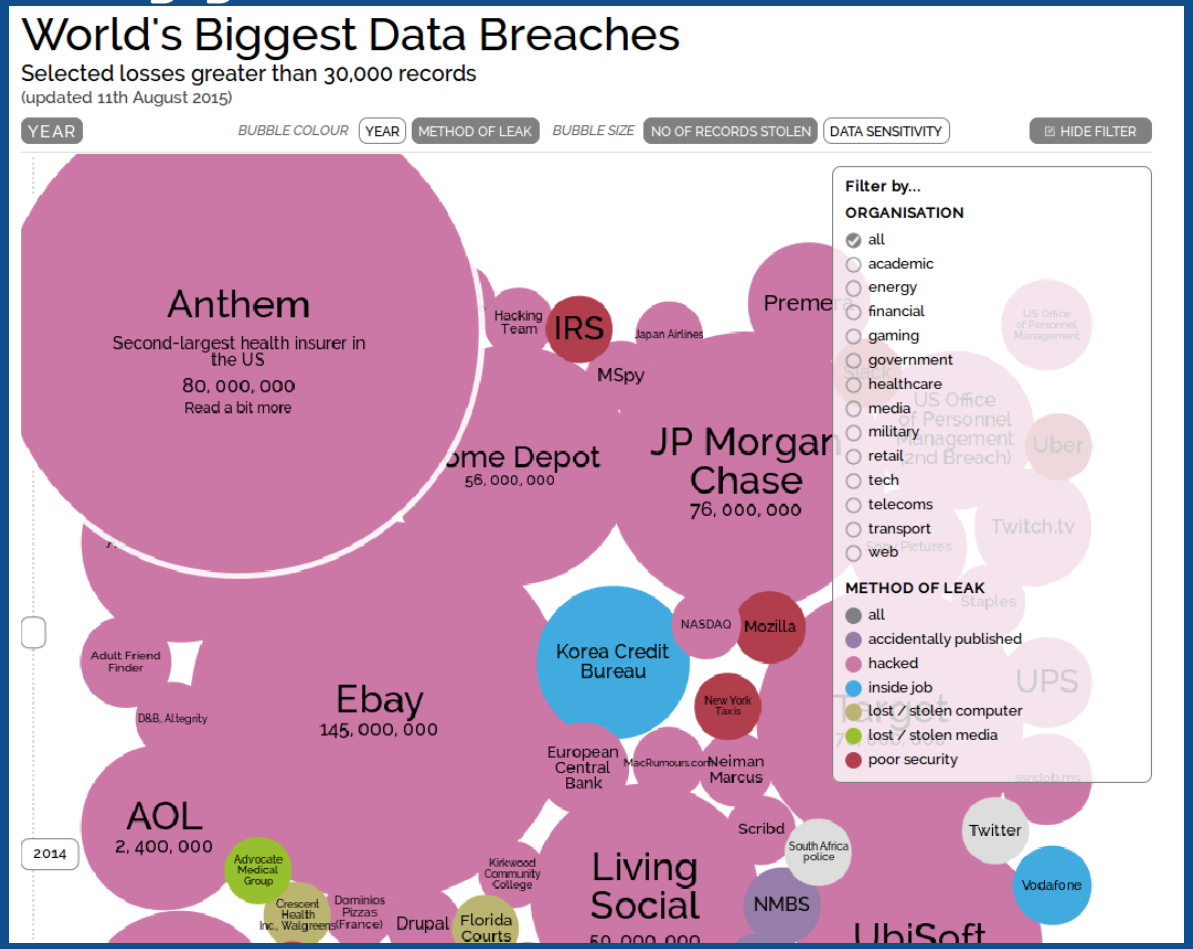
Digital identity

Something you know

Something you have

Something you are

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



Call for integral solutions I

- have i been pwned? Check if you have an account that has been compromised in a data breach
- 'Worse Than KRACK' – Google And Microsoft Hit By Massive 5-Year-Old Encryption Hole
- Vietnamese researcher shows iPhone X face ID 'hack'

Call for integral solutions II

- Japan researchers warn of fingerprint theft from ’peace’ sign
- Hacker fakes German minister’s fingerprints using photos of her hands
- Side channel attacks
  - Eavesdropping attacks on computer displays

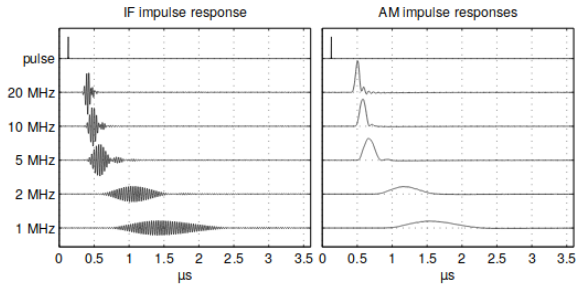


Figure 1: Receiver output resulting from a single nanosecond-short impulse at the antenna input.

Figure 2: Text displayed on a cathode-ray tube (top) and signal seen by eavesdropper (bottom).

Call for integral solutions III

- Acoustic side-channel attacks on printers

COHERENCE AND CONGRUENCE

BUSINESS GOALS

LEGAL/NORMATIVE REQUIREMENTS

TECHNOLOGY

SU-ICT-02-2020-Building blocks for resilience in evolving ICT systems

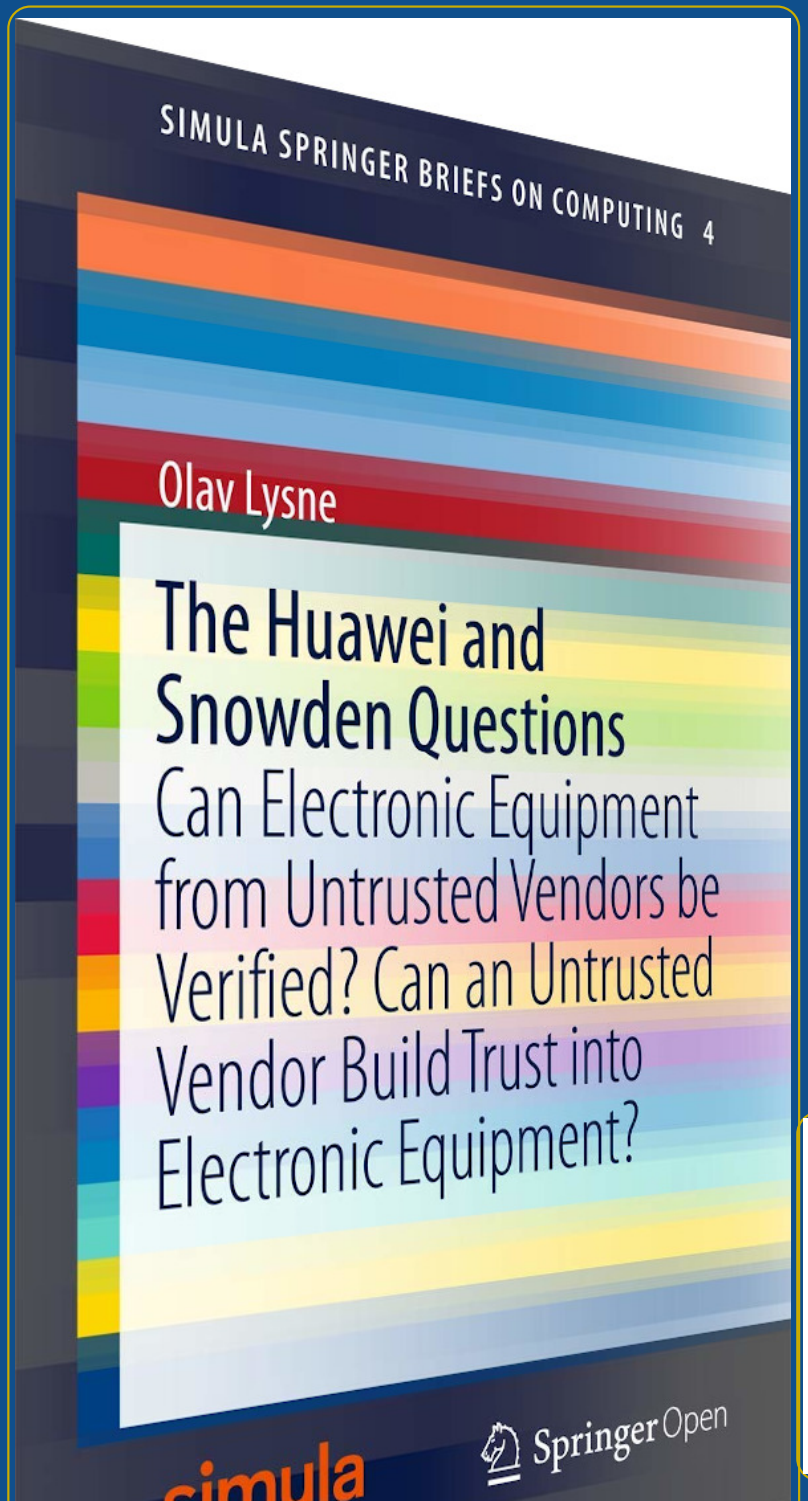
SECURE PLATFORM FOR ICT SYSTEMS ROOTED AT THE SILICON MANUFACTURING PROCESS

Acronym: SPIRS

List of participants

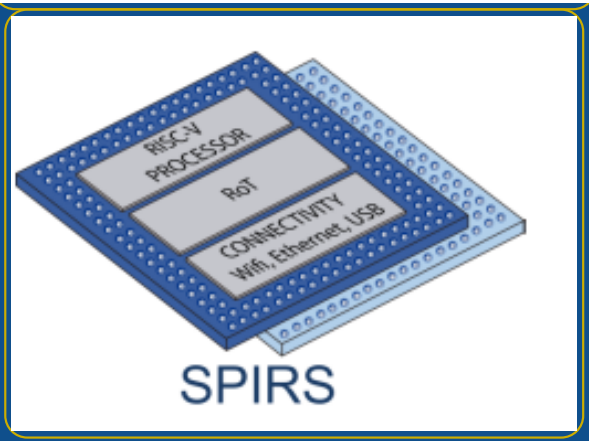
Participant No. *	Participant organisation name	Country
1 (Coordinator)	Agencia Estatal Consejo Superior de Investigaciones Científicas (CSIC)	Spain
2	Tampere University (TAU)	Finland
3	Politecnico di Torino (POLITO)	Italy
4	Telefónica Investigación y Desarrollo SA (TID)	Spain
5	Commissariat à l'Energie Atomique et aux Energies Alternatives (CEA)	France
6	Fondazione LINKS – Leading Innovation & Knowledge for Society (LINKS)	Italy
7	Next SRL (NEXT)	Italy
8	NEC Laboratories Europe GmbH (NEC)	Germany
9	Thales DIS Design Services SAS (THALES)	France

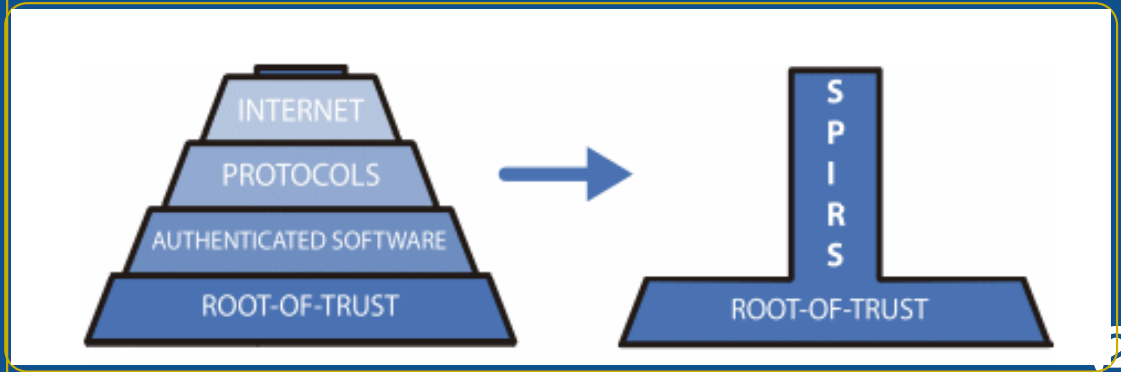

CASA DE LA CIENCIA



European Processor Initiative

Industrial Alliance for Processors and Semiconductor Technologies

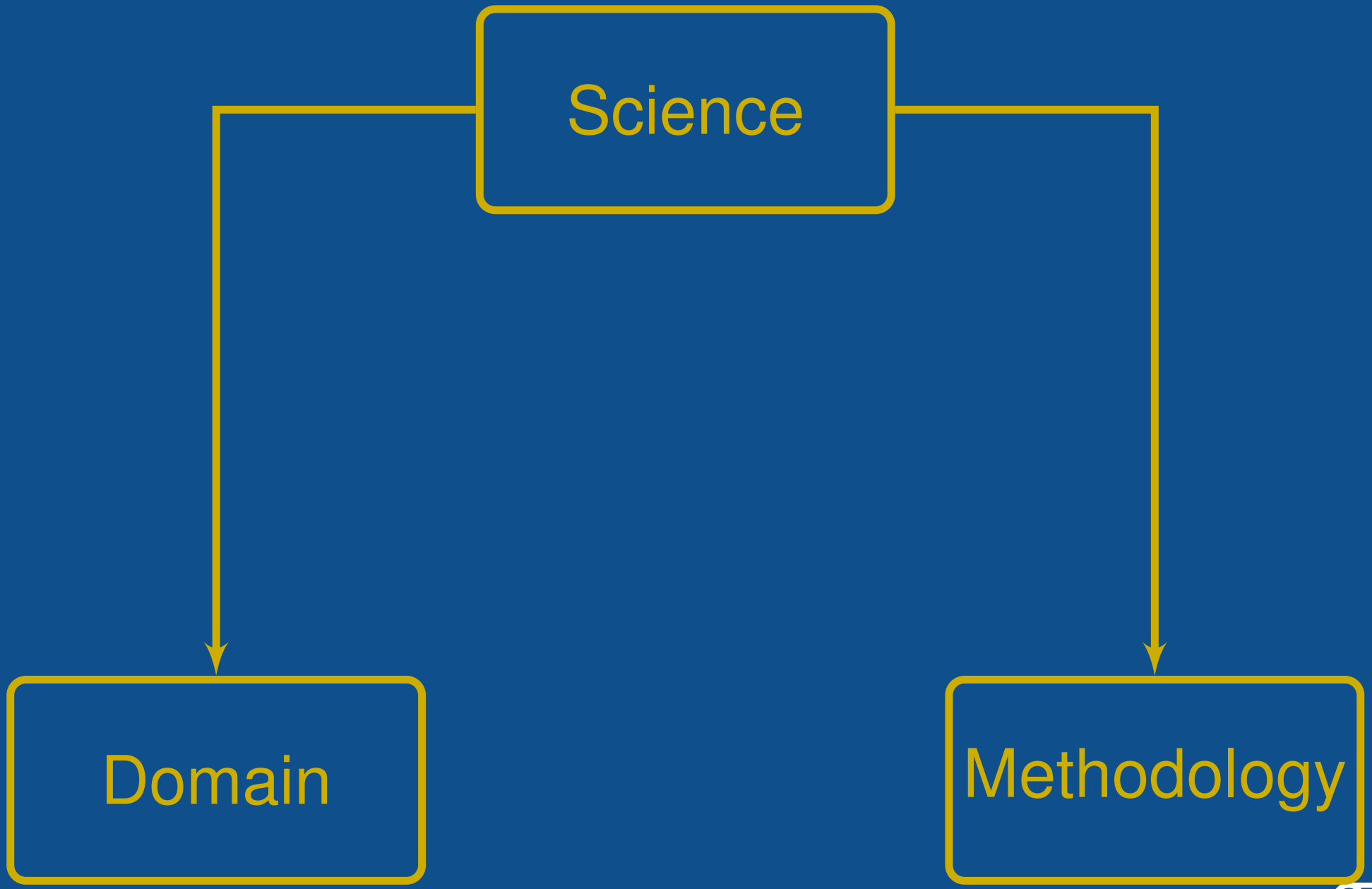


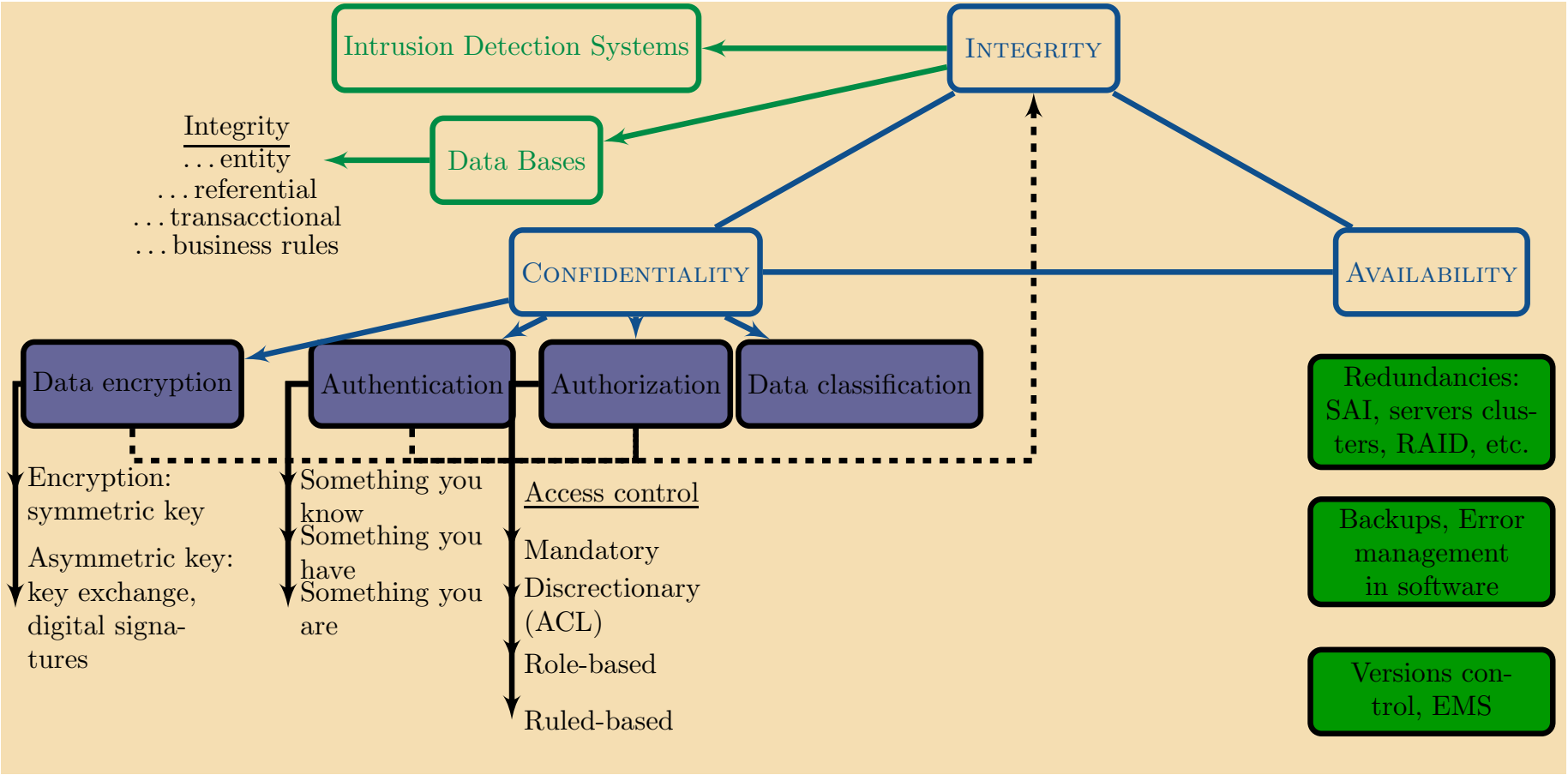


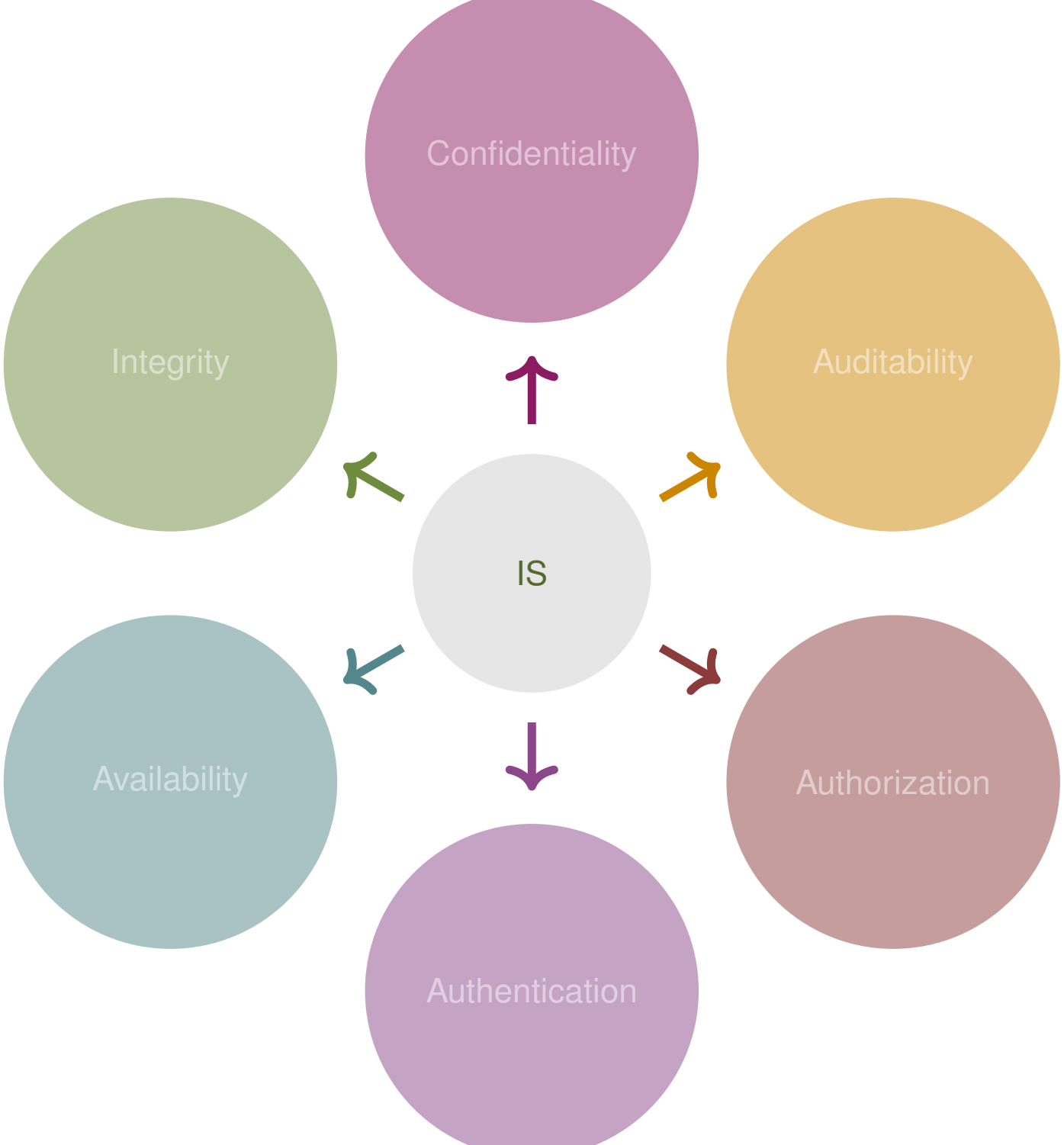
3 *Cybersecurity*

What is cybersecurity?

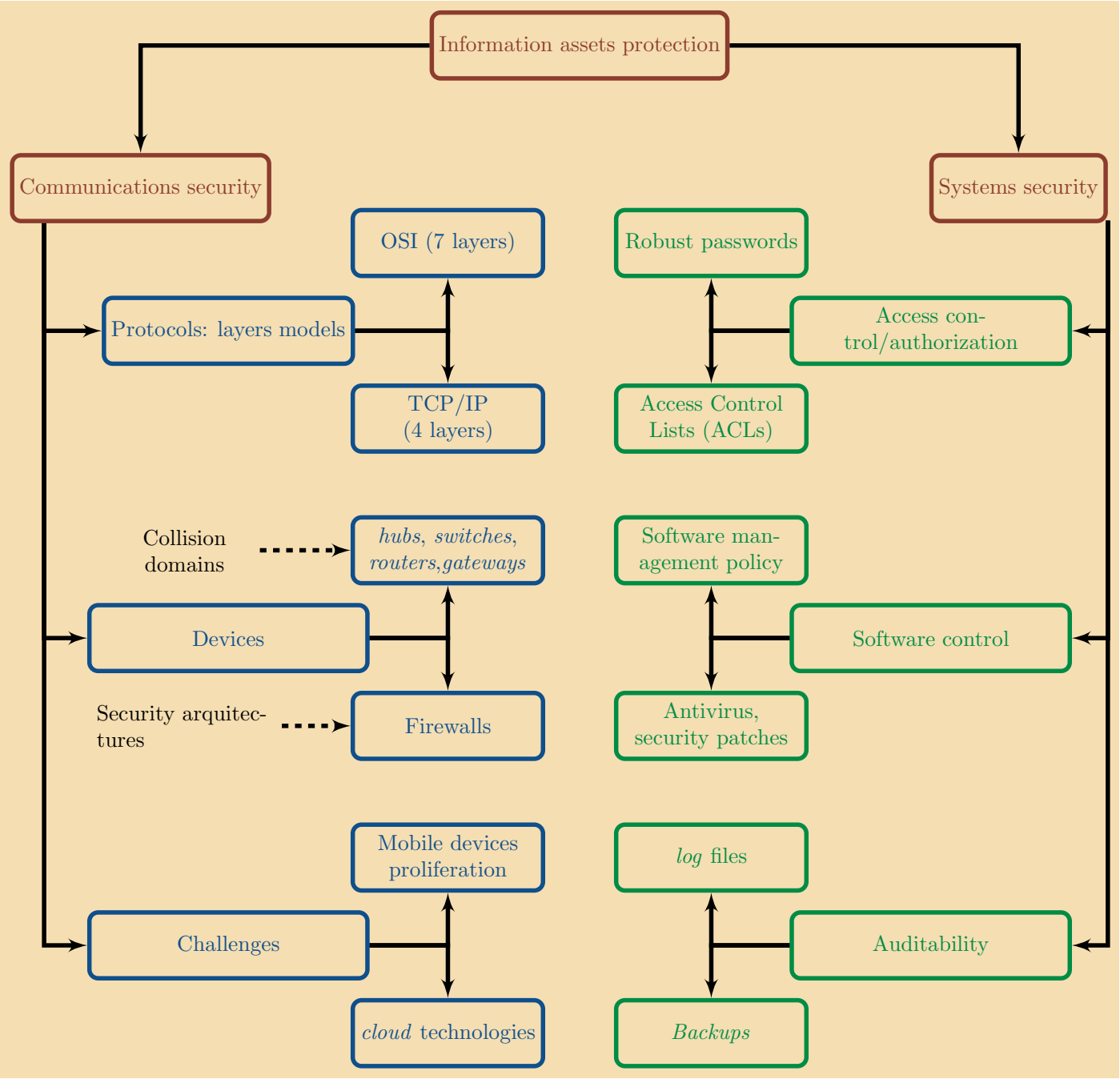
What is cybersecurity?




Intrusion Detection Systems
Integrity
Integrity
. . . entity
. . . referential
. . . transacctional
. . . business rules
Data Bases
Confidentiality
Availability
Data encryption
Authentication
Authorization
Data classification
Encryption: symmetric key
Asymmetric key: key exchange, digital signatures
Something you know
Something you have
Something you are
Access control
Mandatory
Discretionary (ACL)
Role-based
Ruled-based
Redundancies: SAI, servers clusters, RAID, etc.
Backups, Error management in software
Versions control, EMS

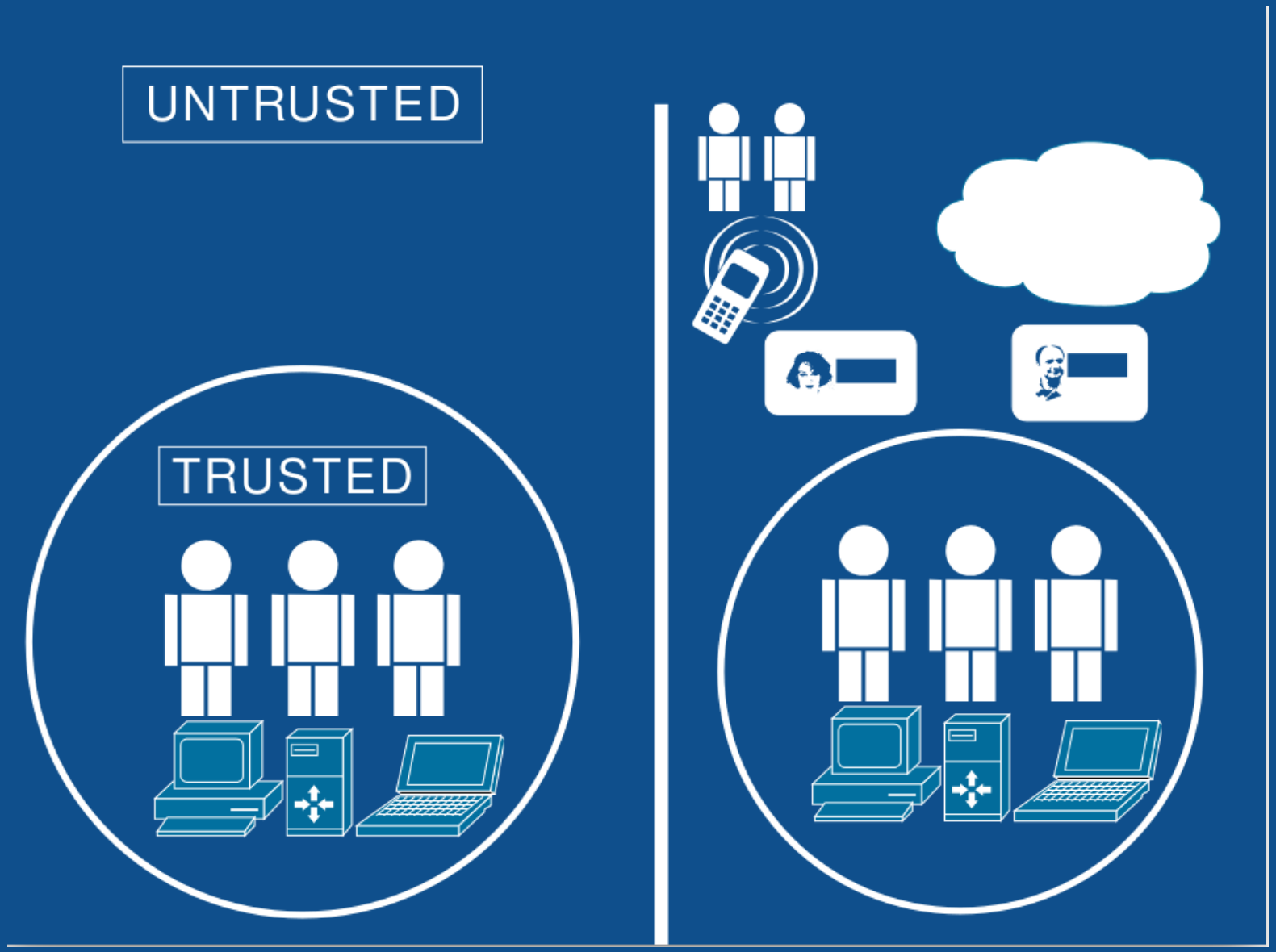

Confidentiality
Integrity
Auditability
IS
Availability
Authorization
Authentication

CIA + 3Au


Information assets protection
Communications security
Systems security
OSI (7 layers)
Robust passwords
Protocols: layers models
Access con-
trol/authorization
TCP/IP
(4 layers)
Access Control
Lists (ACLs)
Collision
domains
hubs, switches,
routers,gateways
Software man-
agement policy
Devices
Software control
Security arquitec-
tures
Firewalls
Antivirus,
security patches
Mobile devices
proliferation
log files
Challenges
Auditability
cloud technologies
Backups


NO PEDESTRIAN
TRAFFIC ALLOWED

CID + 3Au + Perimetral Security


UNTRUSTED
TRUSTED

4 *Main challenges in cybersecurity*

- *Data and computing outsourcing*
- *Privacy*
- *Distributed trust management*
- *Do you need a blockchain in your life?*

Urbi et orbi: cloud, what would I do without you?

Cloud computing | D...

debates.economist.com/debate/cloud-computing?state=opening

Blog de Seguridad ... | eternal-todo.com | Hack Players | 887 × 481 - phynxlabs... | Últimas noticias | Save to Mendeley | Latest security vuln... | →Inglés | WordReference | Definición | Noticias | El Ministerio

The Economist

Help & Information | More Debates | Archive | Login

Cloud computing

Should companies do most of their computing in the cloud?

May 26th 2015 to Jun 5th 2015

Debate Complete

Sponsored by Microsoft

MICROSOFT'S PERSPECTIVE

ABOUT SPONSORSHIP

ABOUT THIS DEBATE | OPENING PHASE Day 1 to 3 | REBUTTAL PHASE Day 4 to 8 | CLOSING PHASE Day 9 to 10 | POST DEBATE PHASE

DEBATE PROGRESS: DAY 1 | DAY 2 | DAY 3 | DAY 4 | DAY 5 | DAY 6 | DAY 7 | DAY 8 | DAY 9 | DAY 10 | DAY 11

Yes 64%

138 Debate Votes

No 36%

Make your vote

Participants 111

Opening Statements

MODERATOR

Ludwig Siegele, The Economist's technology editor

Ludwig Siegele is *The Economist*'s technology editor. He joined the newspaper as US technology correspondent in 1998. In 2003 he went to Berlin as Germany correspondent, relocated to London in 2008 to cover the IT industry until 2011, and then ran part of *The Economist*'s website as online business and finance editor. He started his journalistic career in 1990 as the Paris business correspondent of *Die Zeit*, a Germany weekly.

YES

Simon Crosby, Co-founder and chief technology officer (CTO) of Bromium Inc.

Simon Crosby is a co-founder and chief technology officer (CTO) of Bromium Inc., a pioneer of micro-virtualisation, which enables PCs to defend themselves by design from all malware. Previously he was CTO, data centre and cloud, at Citrix Systems, which acquired XenSource, where he was co-founder and CTO; a principal engineer at Intel, where he led strategic research on platform security and

NO

Bruce Schneier, Chief technology officer at Resilient Systems

Bruce Schneier is a security technologist. He is chief technology officer at Resilient Systems, a cyber-security firm, a fellow at Harvard University's Berkman Center and a board member of the Electronic Frontier Foundation (EFF). His latest book is "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World". He blogs and tweets at @schneierblog.

cloud | Resaltar todo | Coincidencia de mayúsculas/minúsculas | Más de 100 aciertos

Proliferation of mobiles devices

Bussiness teams full control of their applications with little or nor IT

Easy to use/ to integrate

Innovation

Agility

Security

The proposer's opening remarks in full

YES

Simon Crosby, Co-founder and chief technology officer (CTO) of Bromium Inc.

26th May 2015

Loss of control

A large provider is a juicier target

Easy to use/ to integrate

Limited customisation

Legal and regulatory compliance

Weigh the benefits vs. the risks

The opposition's opening remarks in full

NO

Bruce Schneier, Chief technology officer at Resilient Systems
26th May 2015

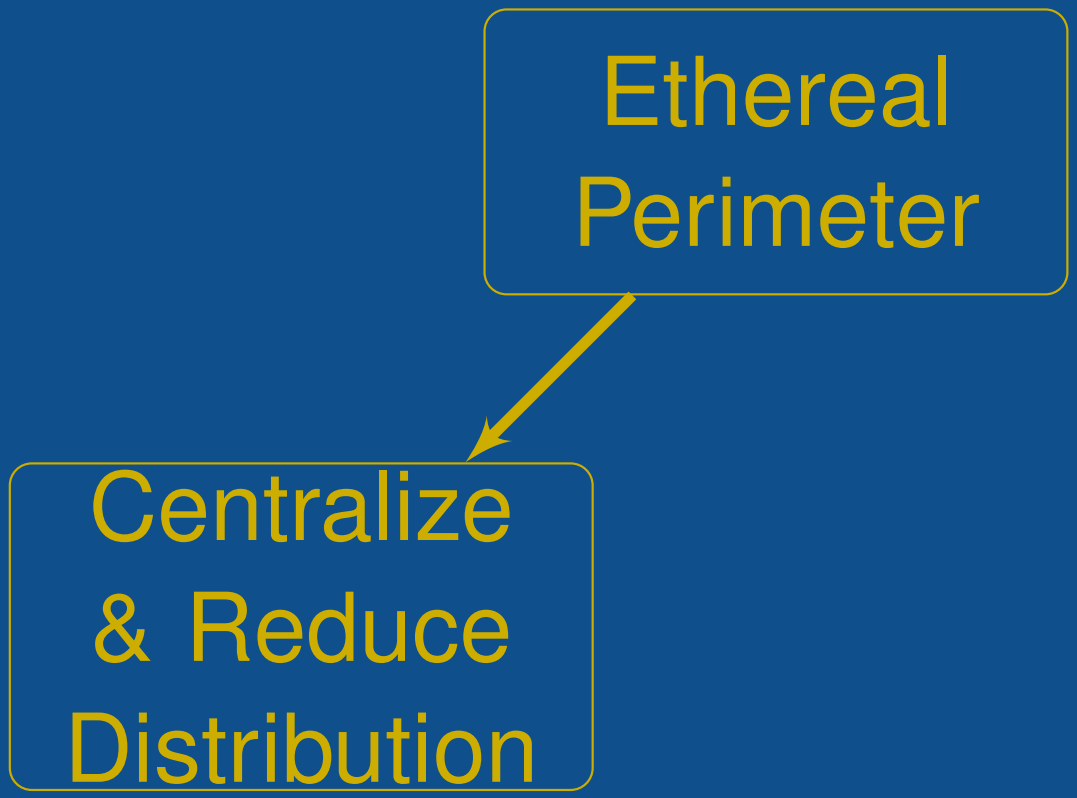
Yes. No. Yes. Maybe. Yes. Okay, it's complicated.

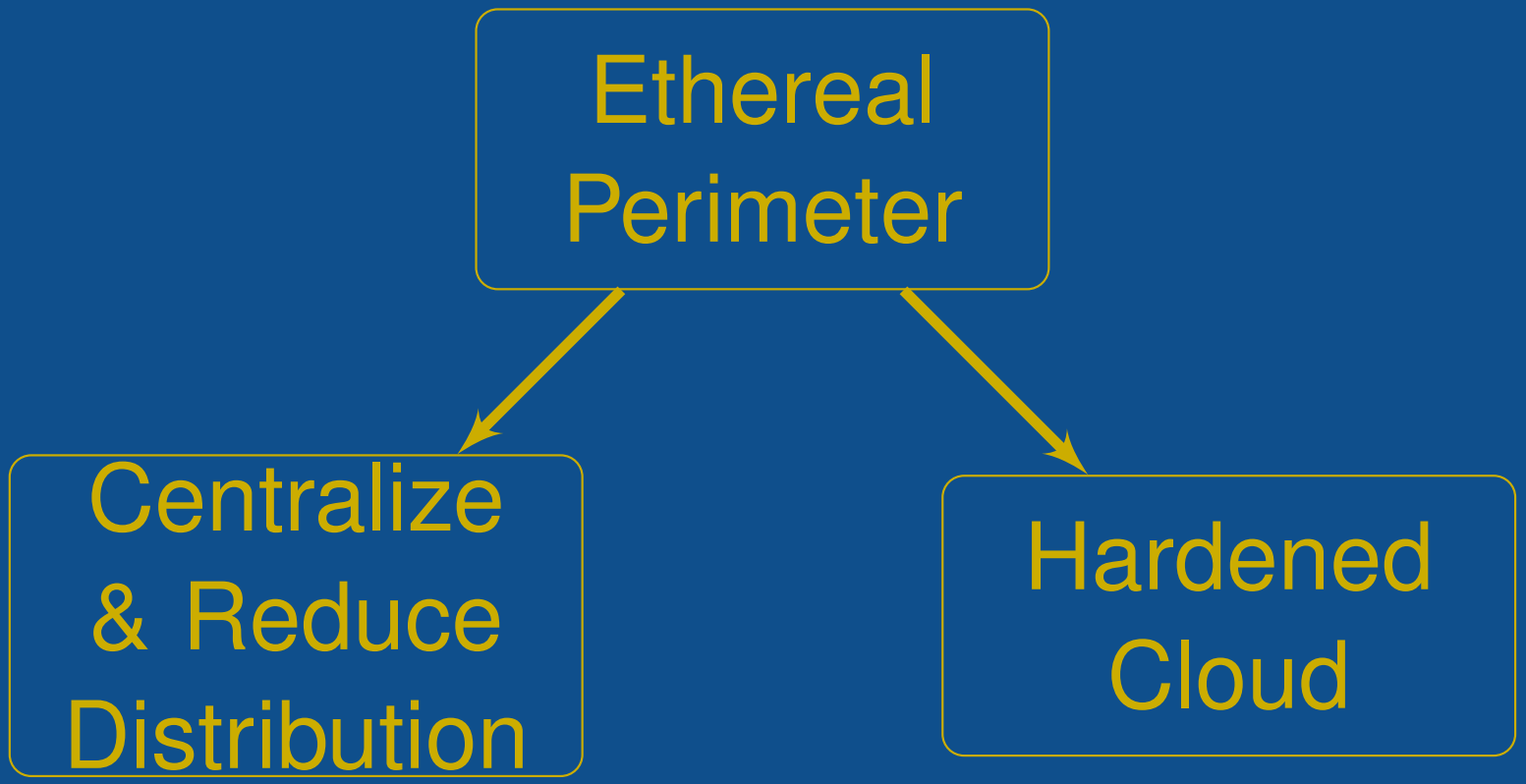

There is no cloud
it's just someone else's computer

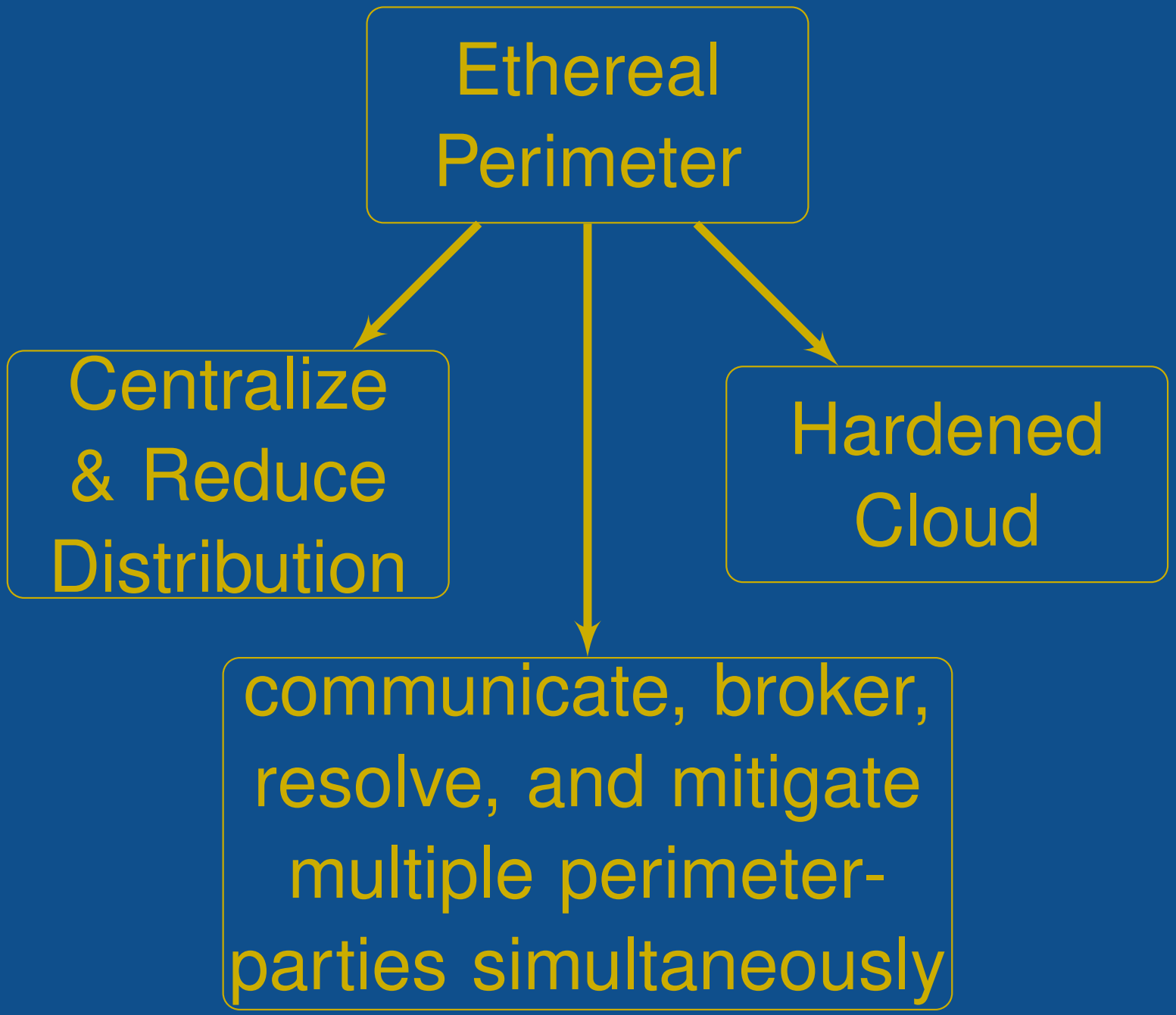
Is identity the new perimeter?

- ✓ Classical perimeter is not identity aware: network security, malware protection, identity protection
  - ✗ Isolated silos
  - ✗ No integral solution
- ✓ Identity isn’t malware-aware or network-aware

Ethereal
Perimeter


Ethereal Perimeter
Centralize & Reduce Distribution


Ethereal Perimeter
Centralize & Reduce Distribution
Hardened Cloud


Ethereal Perimeter
Centralize & Reduce Distribution
Hardened Cloud
communicate, broker, resolve, and mitigate multiple perimeter-parties simultaneously

NO steel-belt layer

Ethereal Perimeter

Centralize & Reduce Distribution

Hardened Cloud

communicate, broker, resolve, and mitigate multiple perimeter-parties simultaneously

NO steel-belt layer

Ethereal Perimeter

YES network / cloud organism

Centralize & Reduce Distribution

Hardened Cloud

communicate, broker, resolve, and mitigate multiple perimeter-parties simultaneously

NO steel-belt layer

Ethereal Perimeter

YES network / cloud organism

Centralize & Reduce Distribution

Hardened Cloud

communicate, broker, resolve, and mitigate multiple perimeter-parties simultaneously

Alejandro Sanchez-Gomez, Jesus Diaz, Luis Hernández Encinas, et al. (2017). “Review of the Main Security Threats and Challenges in Free-Access Public Cloud Storage Servers”. In: *Computer and Network Security Essentials*. Ed. by K. Daimi. Vol. In Press. Studies in Computational Intelligence. Springer Berlin Heidelberg

Ten challenges in the adoption free-access cloud storage

- Advantages for SMEs: costs reduction

Ten challenges in the adoption free-access cloud storage

- Advantages for SMEs: costs reduction
- Threats models and countermeasures

Ten challenges in the adoption free-access cloud storage

- Advantages for SMEs: costs reduction
- Threats models and countermeasures
- Mechanisms for the detection of SLA non-compliance

Ten challenges in the adoption free-access cloud storage

- Advantages for SMEs: costs reduction
- Threats models and countermeasures
- Mechanisms for the detection of SLA non-compliance
- Cryptographic tools for <u>zero-trust schemes</u>

Ten challenges in the adoption free-access cloud storage

- Advantages for SMEs: costs reduction
- Threats models and countermeasures
- Mechanisms for the detection of SLA non-compliance
- Cryptographic tools for <u>zero-trust schemes</u>

Zero-trust model

- Trust the cloud only as storage medium
- Don't assume the cloud provider adheres to informed consent procedures to access users' data: ☠ privacy ☠
- Don't assume the cloud provider only modifies your data after being explicitly granted by the data owner


ProtonMail
Encrypted email, based in Switzerland.

Zero-trust model

- Preserve privacy through confidentiality (privacy as confidentiality)
- Integrity verification
- Availability protection

Zero-trust model

- Preserve privacy through confidentiality (privacy as confidentiality)
  1. Homomorphic encryption $\Leftrightarrow$ compatible provider (e.g., CryptDB)
  2. Client-side encryption
- Integrity verification
- Availability protection

Zero-trust model

- Preserve privacy through confidentiality (privacy as confidentiality)
- Integrity verification
  - Digital signatures
- Availability protection

Zero-trust model

- Preserve privacy through confidentiality (privacy as confidentiality)
- Integrity verification
- Availability protection
  - Avoid dependency on only one cloud storage provider
  - Data redundancy privacy: store information on several cloud servers


IT is TOO RISKY

Alejandro Sanchez-Gomez, Jesus Diaz, and David Arroyo (2017). “Encrypted Cloud: a software solution for the secure use of free-access cloud storage services”. In: *The 10th International Conference on Computational Intelligence in Security for Information Systems CISIS 2017*, Accepted. In Press

Network aaS

Infrastructure aaS

Network aaS

Platform aaS

Infrastructure aaS

Network aaS

Software aaS

Platform aaS

Infrastructure aaS

Network aaS

Software aaS

Platform aaS

Infrastructure aaS

Network aaS

Software aaS

Platform aaS

Infrastructure aaS

Network aaS

Software aaS

Platform aaS

Infrastructure aaS

Network aaS

Security as a Service

4 *Main challenges in cybersecurity*

Data and computing outsourcing

Cloud computing

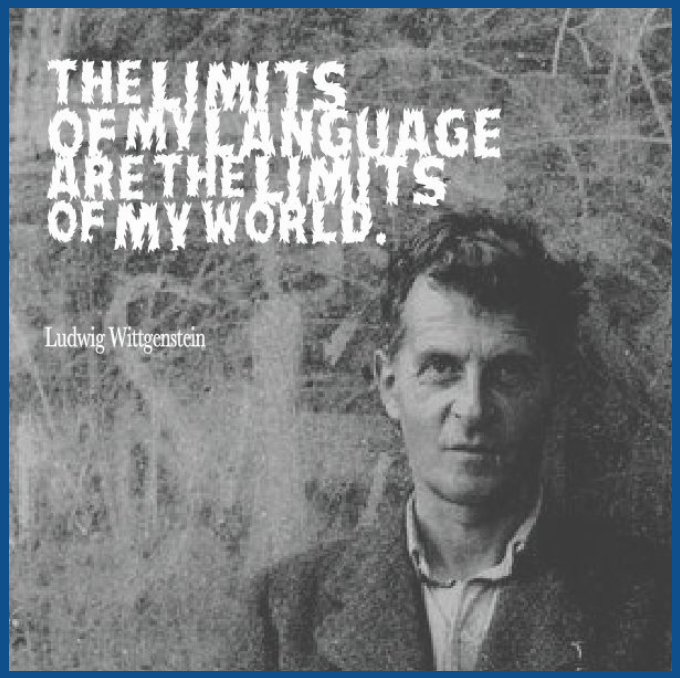
Artificial Intelligence

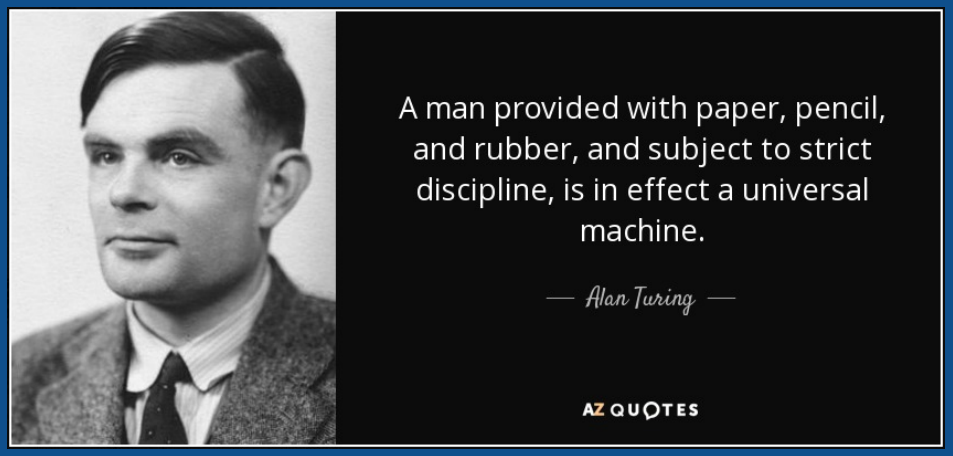
Privacy

Distributed trust management

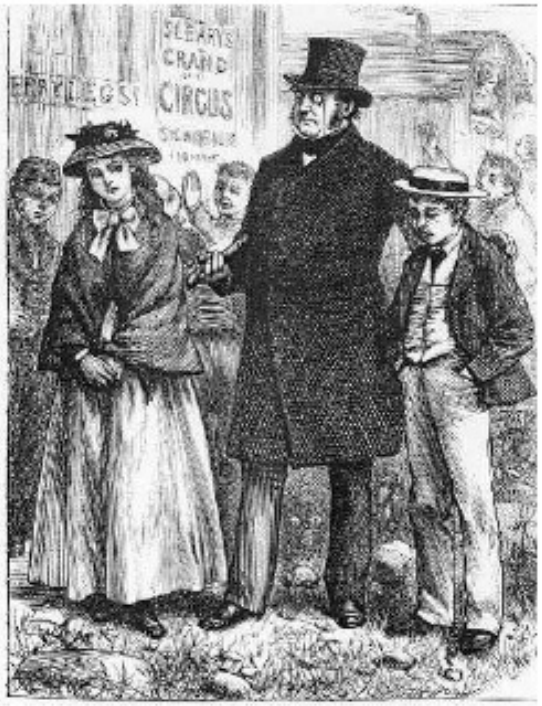
Do you need a blockchain in your life?

Wittgenstein vs. Turing





Fill them up with facts!

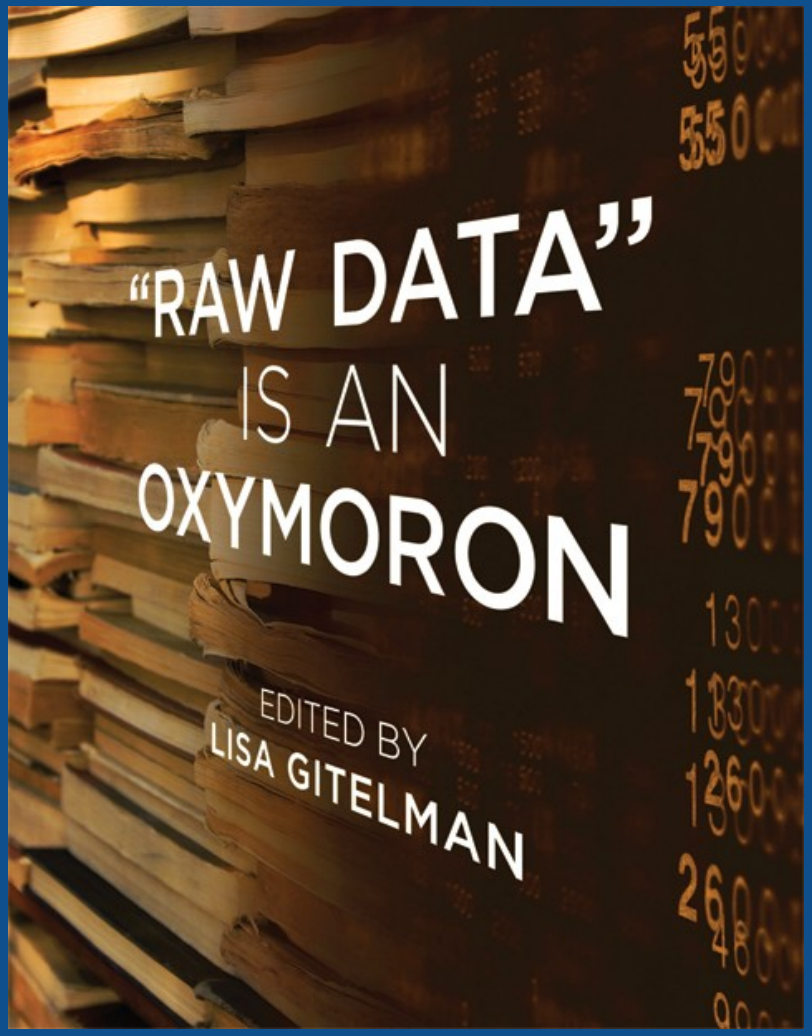


HARD TIMES.

BOOK THE FIRST. SOWING.

"Now, what I want is, Facts. Teach these boys and girls nothing but Facts. Facts alone are wanted in life. Plant nothing else, and root out everything else. You can only form the minds of reasoning animals upon Facts: nothing else will ever be of any service to them."

Thomas Gradgrind
in Charles Dickens, *Hard Times*



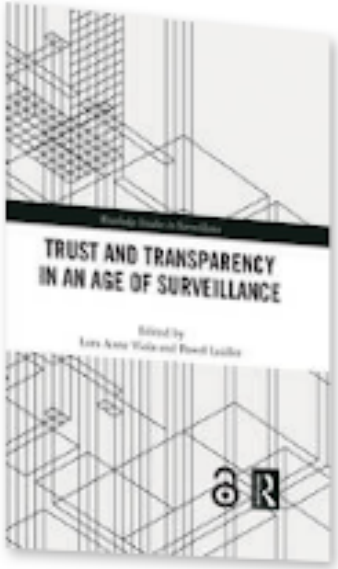
data is not a natural resource but a cultural one

Algocracy: the difficult tradeoff between trust and trustworthiness I

- Overtrust technology is not always justified
- Statistics models and algorithms implementation are based on decision making and taking with human intervention (human in the loop)
- It is not rare that algorithms lead to results diverging from expected values in the design stage

Algocracy: the difficult tradeoff between trust and trustworthiness II

- Data preparation, in general terms, has a political and ideological component



OPEN ACCESS

Chapter

Trustworthy humans and machines

Vulnerable trustors and the need for trustee competence, integrity, and benevolence in digital systems

By Sara Degli-Esposti, David Arroyo

Book Trust and Transparency in an Age of Surveillance

Edition	1st Edition
First Published	2021
Imprint	Routledge
Pages	20
eBook ISBN	9781003120827
OA Funder	Jagiellonian University in Krakow

Share

ABSTRACT

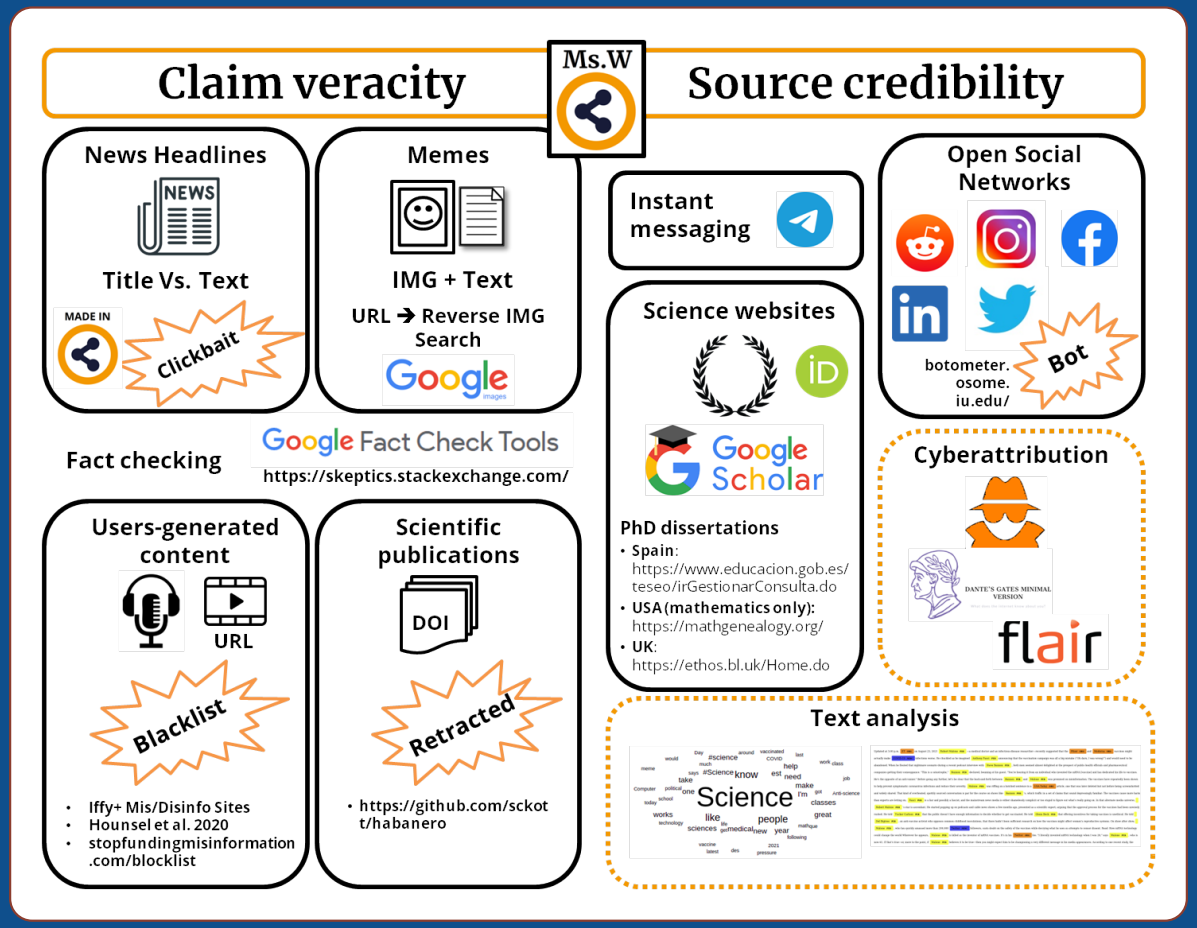
Trust in the Trustworthy I

- Foreground issues of dependence in the trust relationship
- A dependent trustor has no control over the trustee and can only bet everything on the trustee's willingness to deliver on abstract promises of competence, integrity and benevolence
- Inscribe trustworthiness into human beings

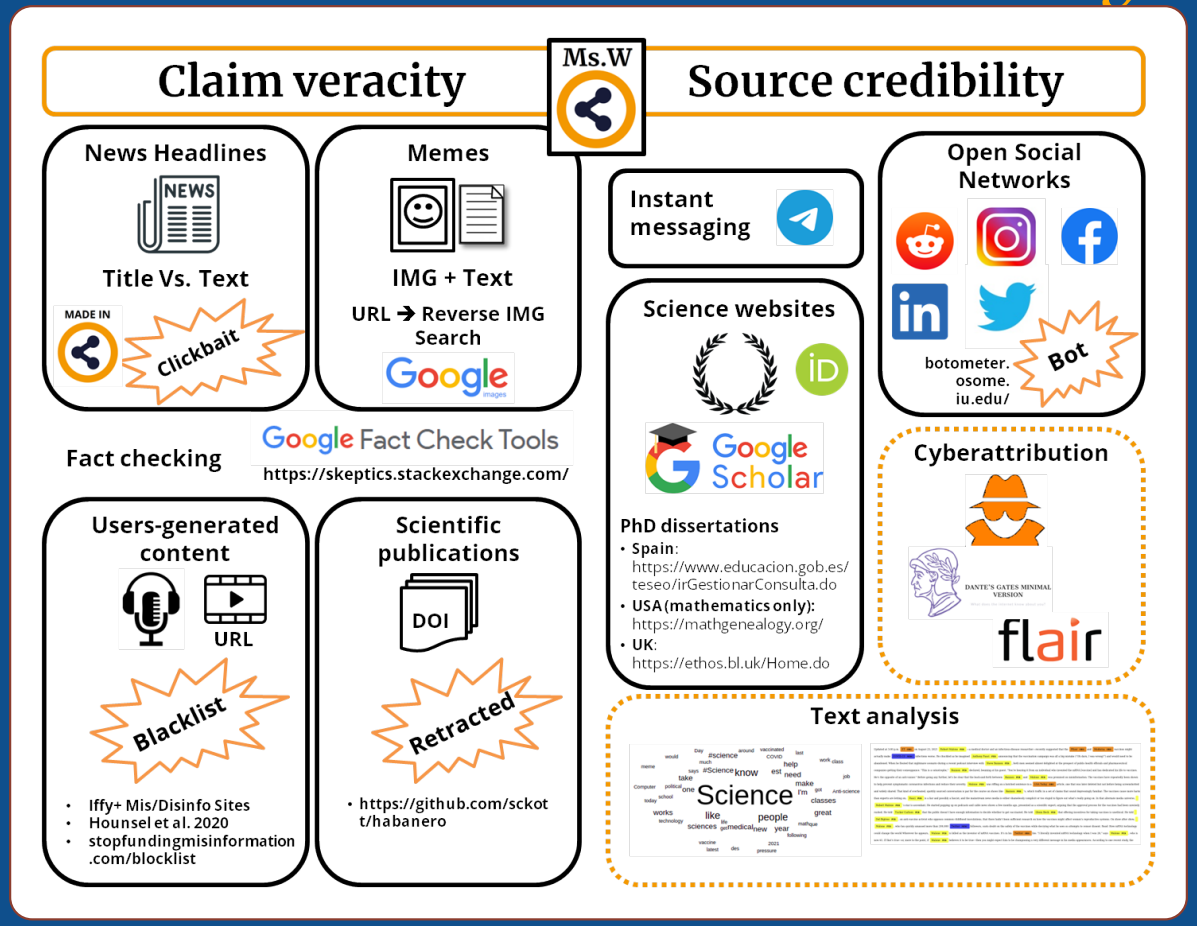
Trust in the Trustworthy II

- Governance architecture to avoid collusion or a paternalistic takeover
- Peer-review and peer-pressure
- Collegial bodies (standardization authorities associations and fora, and the scholarly and scientific community) supporting the activities of, and decisions taken by, the trustees

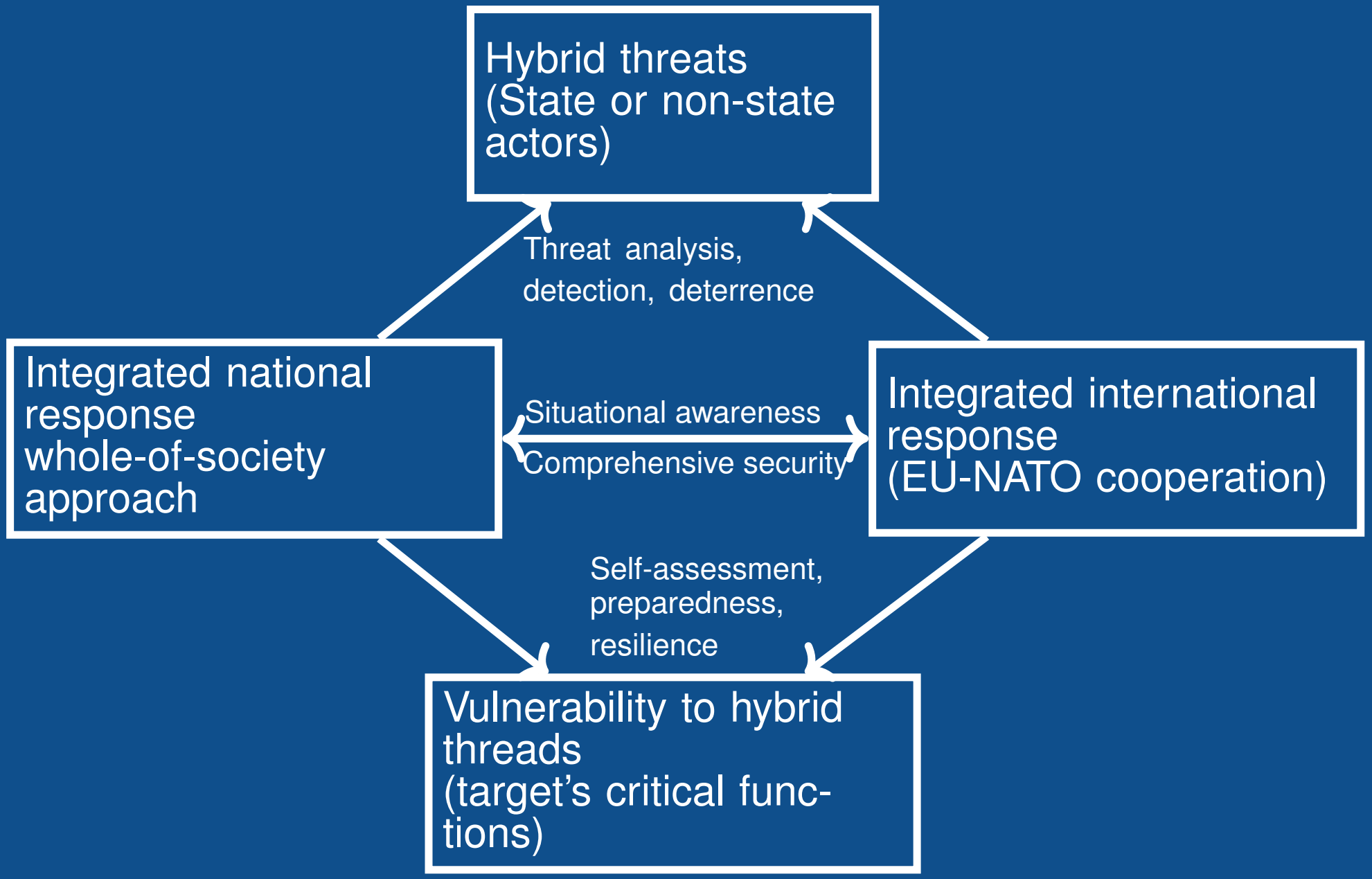
Trust in the trustworthy



Trust in the trustworthy



An interdisciplinary view of the role of control, accountability, and digital surveillance in building trust relationships


Hybrid threats
(State or non-state
actors)
Threat analysis,
detection, deterrence
Integrated national
response
whole-of-society
approach
Situational awareness
Comprehensive security
Integrated international
response
(EU-NATO cooperation)
Self-assessment,
preparedness,
resilience
Vulnerability to hybrid
threads
(target's critical func-
tions)

4 *Main challenges in cybersecurity*

Data and computing outsourcing

Privacy

Distributed trust management

Do you need a blockchain in your life?

What is that thing called privacy? I

one term, three possible visions

general Westin 1968

> "Privacy is the claim of individuals, groups and institutions to determine for themselves , when, how and to what extend information about them is communicated to others"

What is that thing called privacy? II

information privacy *Vacca 2012*(*p. 755*)

"the right to informational self-determi

spatial privacy, right
to be let alone

identity privacy (← *anonymity*)

Property of an entity to be
inside a set and NOT being
identifiable within that set

KatherineJ Strandburg (2014). “Monitoring, Datafication and Consent: Legal Approaches to Privacy in a Big Data Context”. In: *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, p. 5

Data acquisition

Monitoring

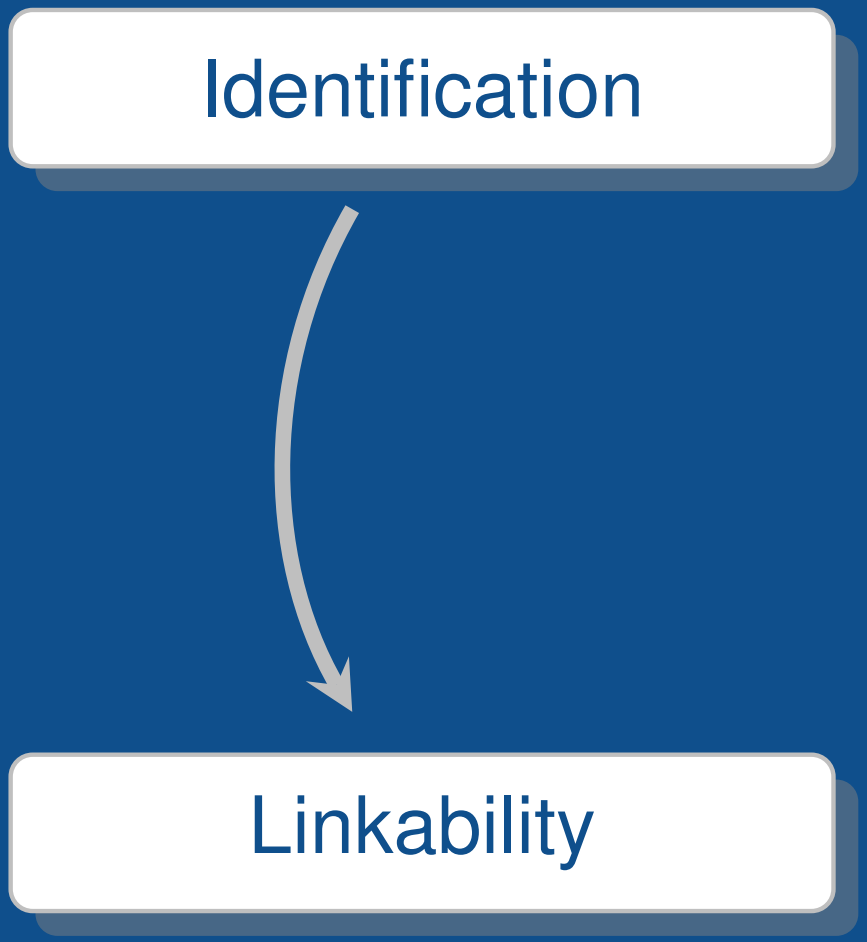
As a byproduct of another activity

Transfer of pre-existing information

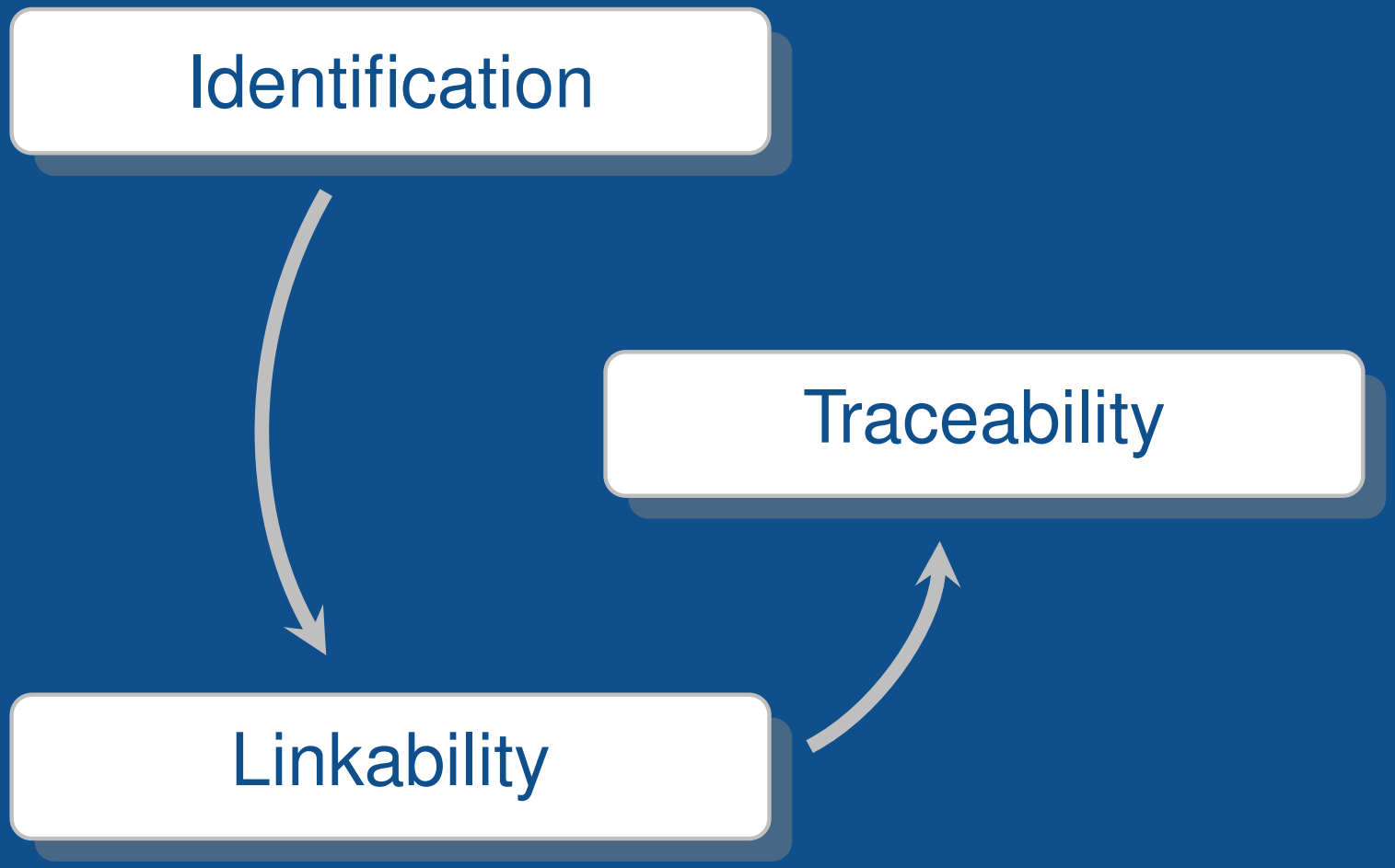
What is that thing called identity?

Identification

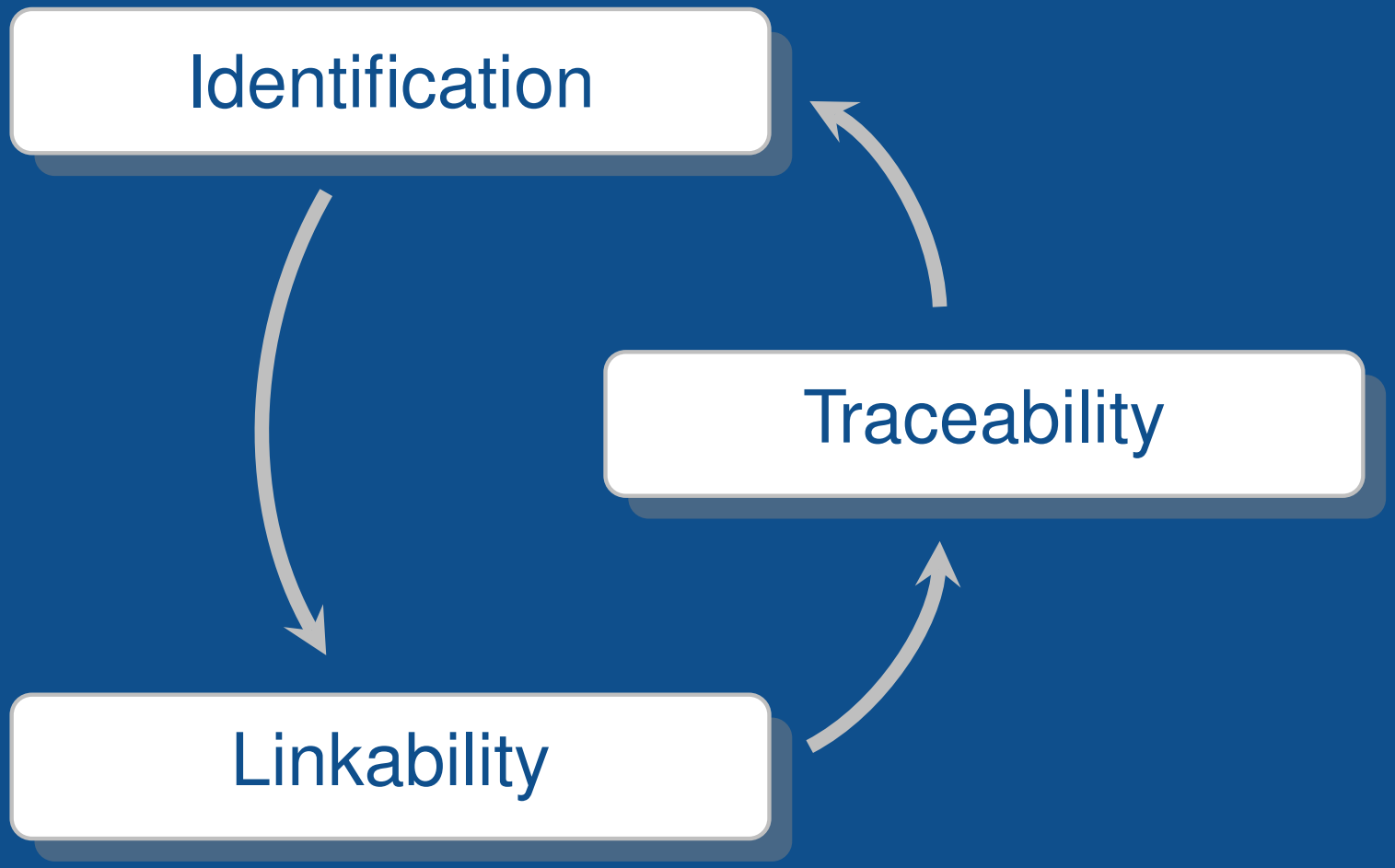
What is that thing called identity?



What is that thing called identity?

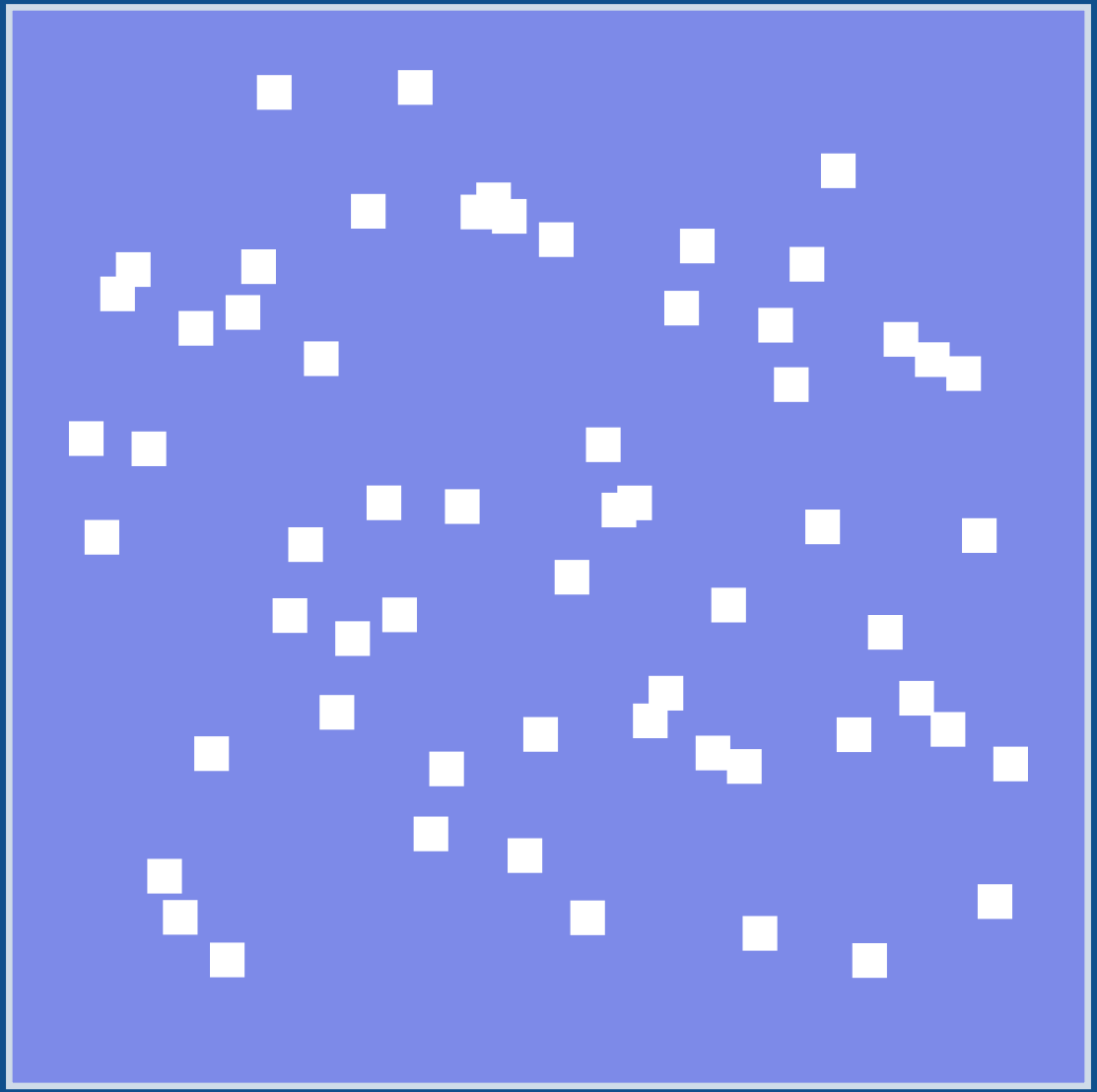


What is that thing called identity?

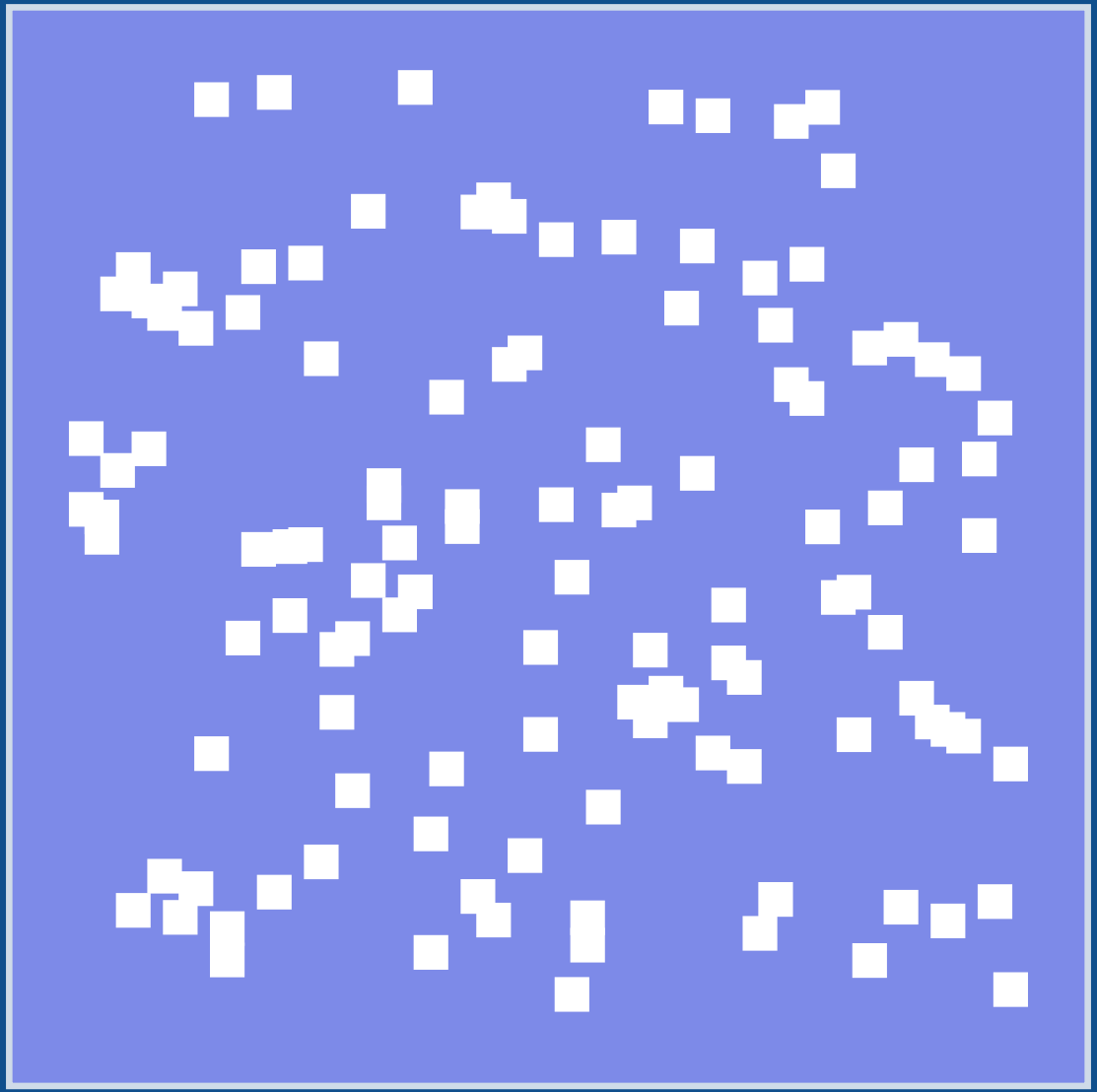


Linkability

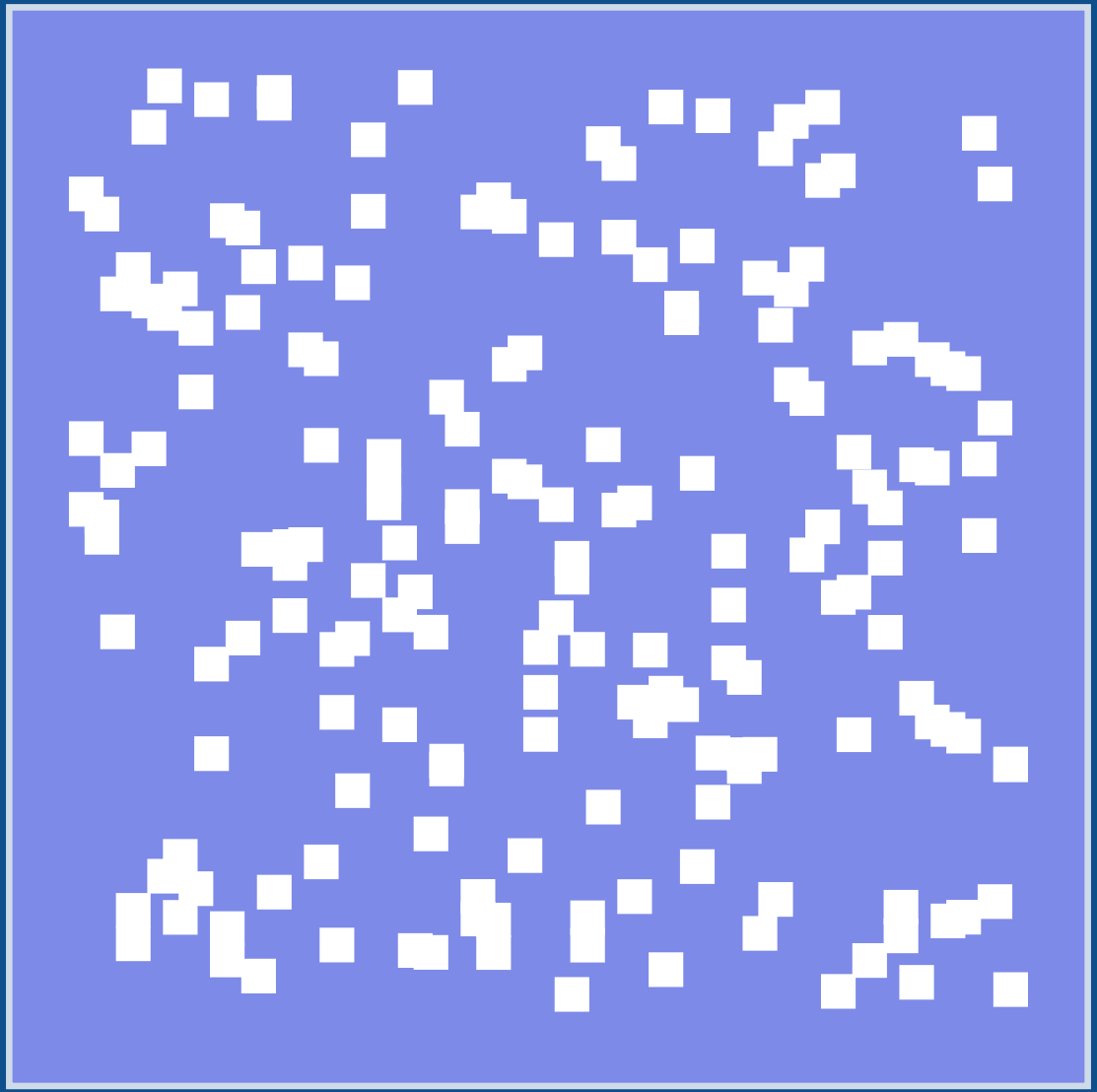
Linkability



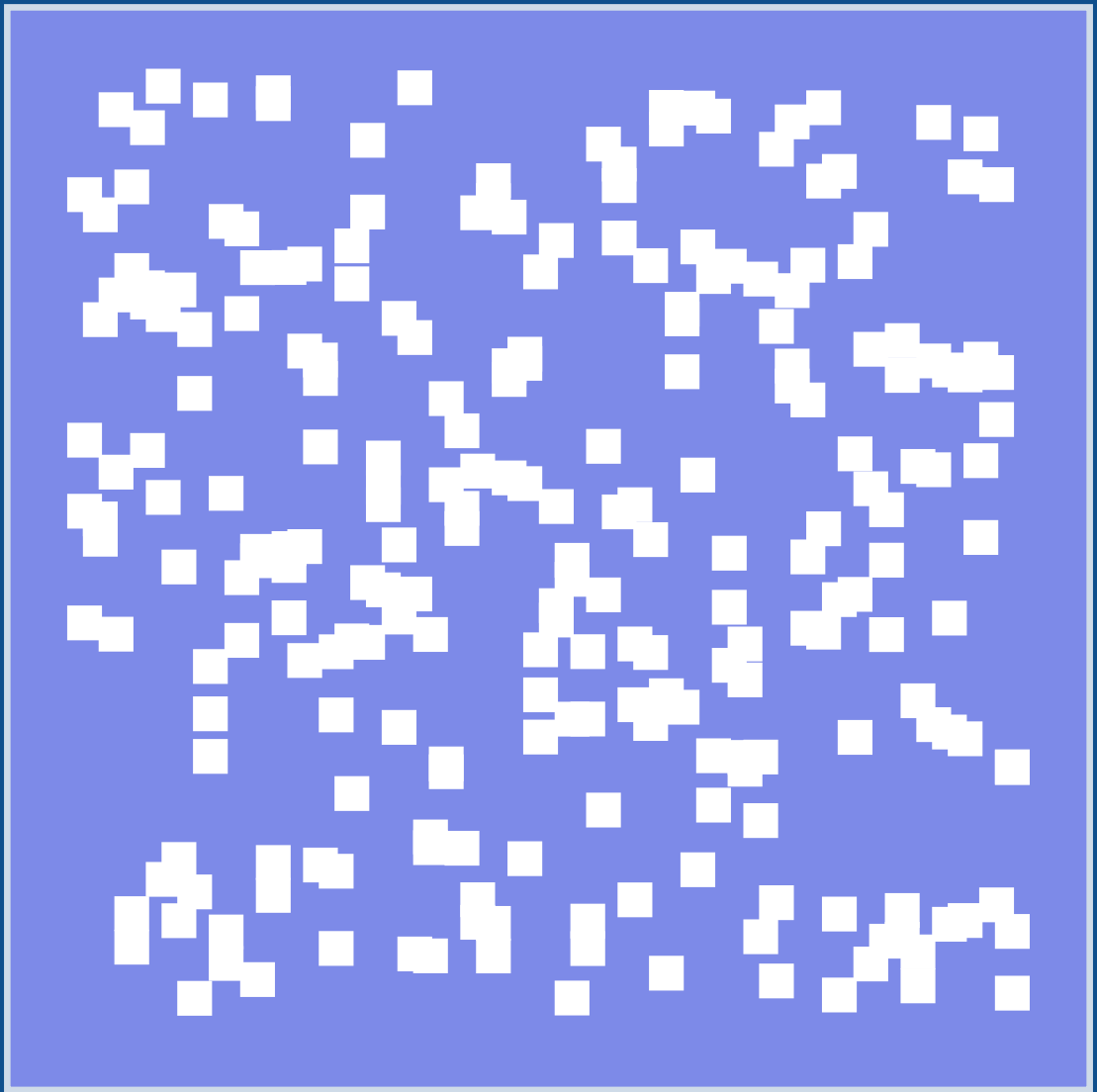
Linkability



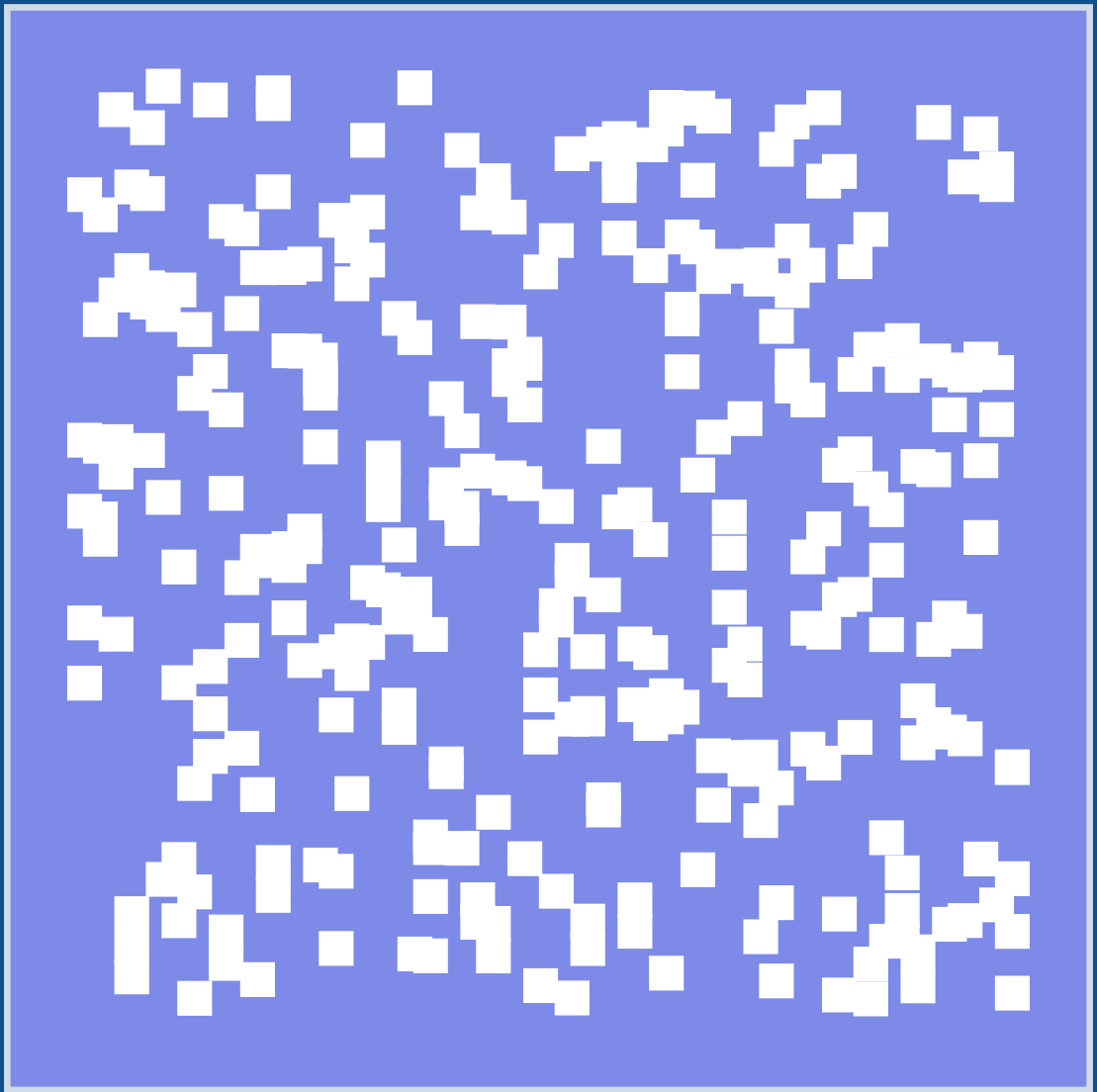
Linkability



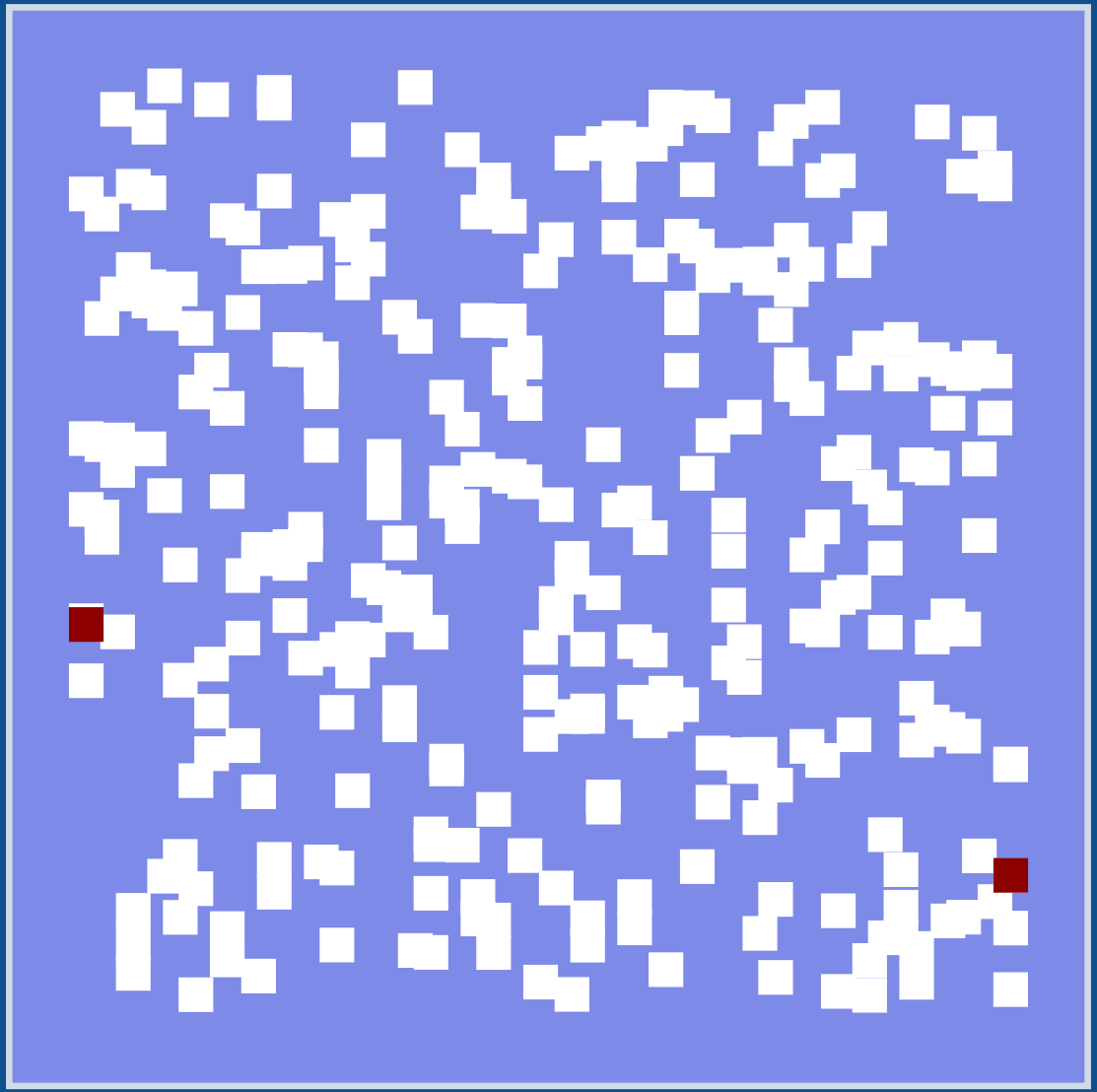
Linkability



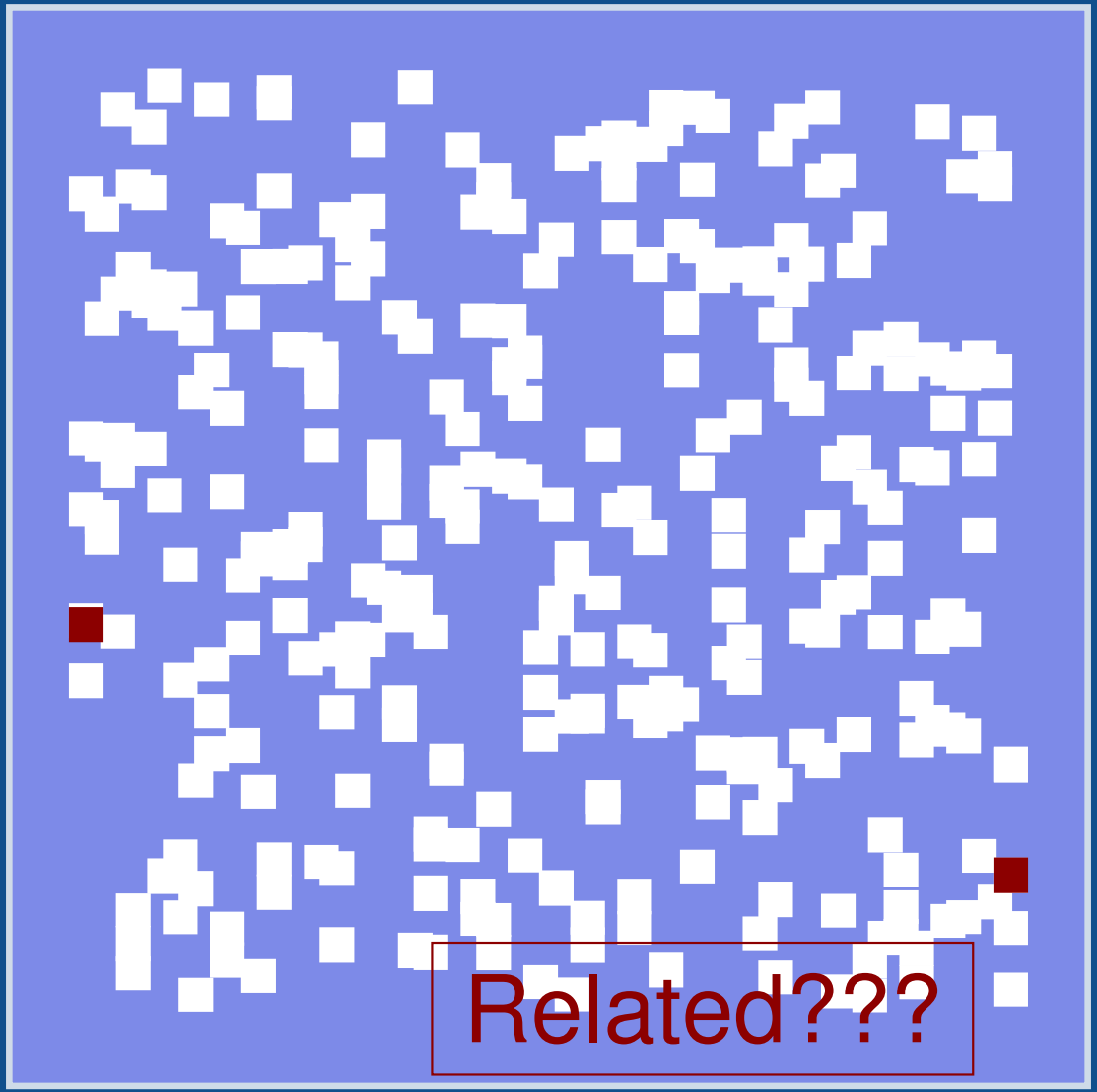
Linkability



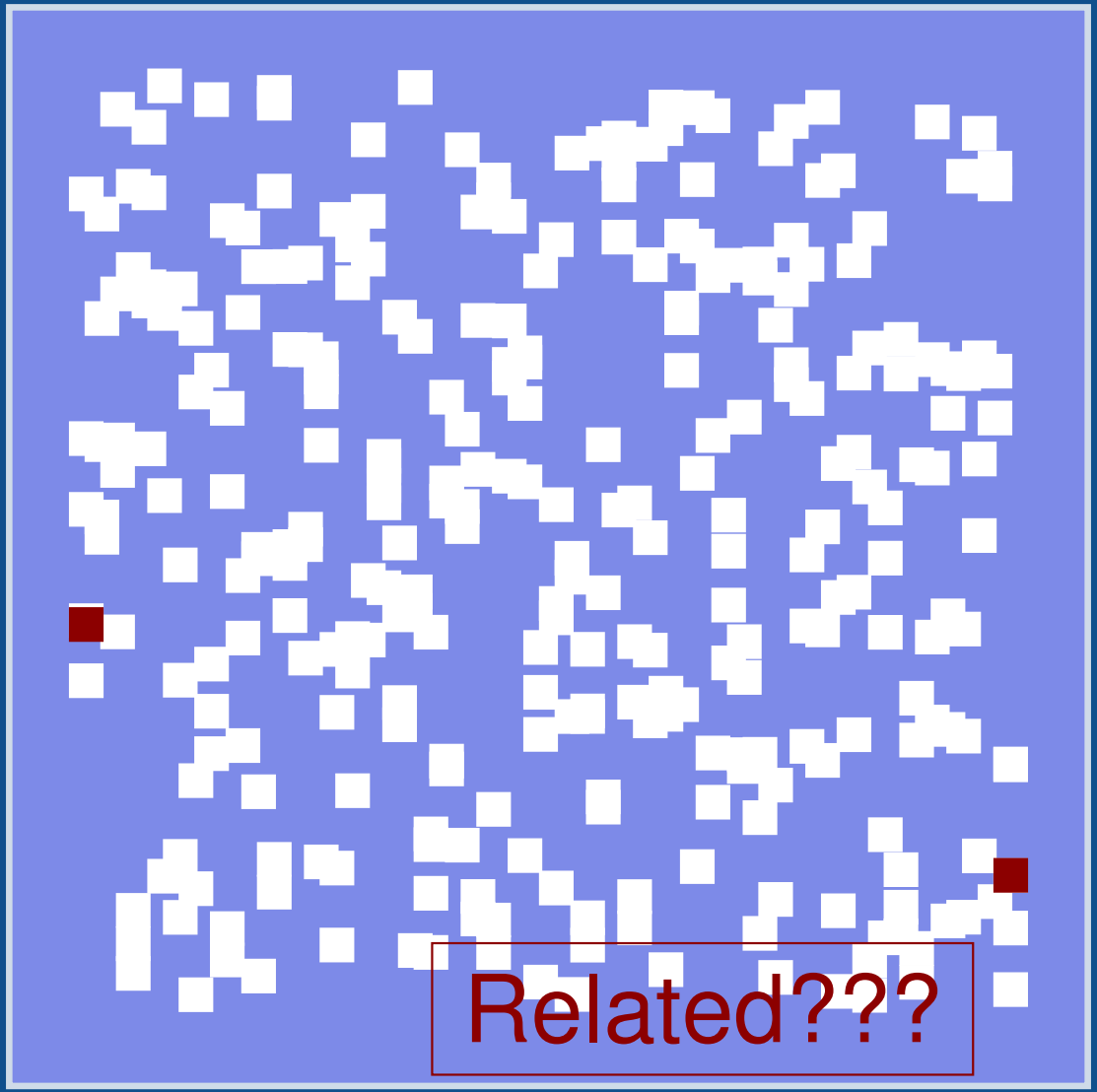
Linkability



Linkability

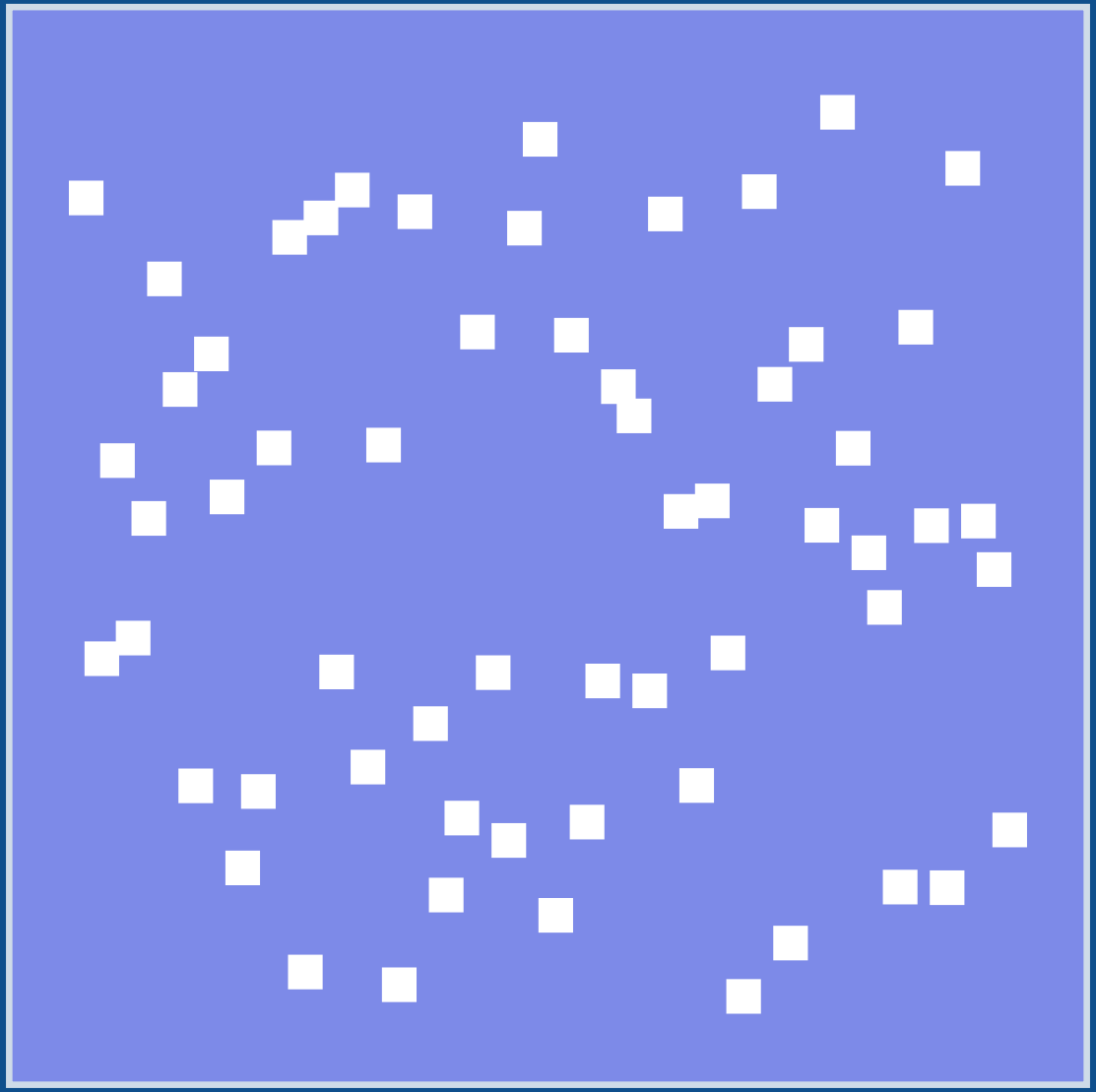


Linkability

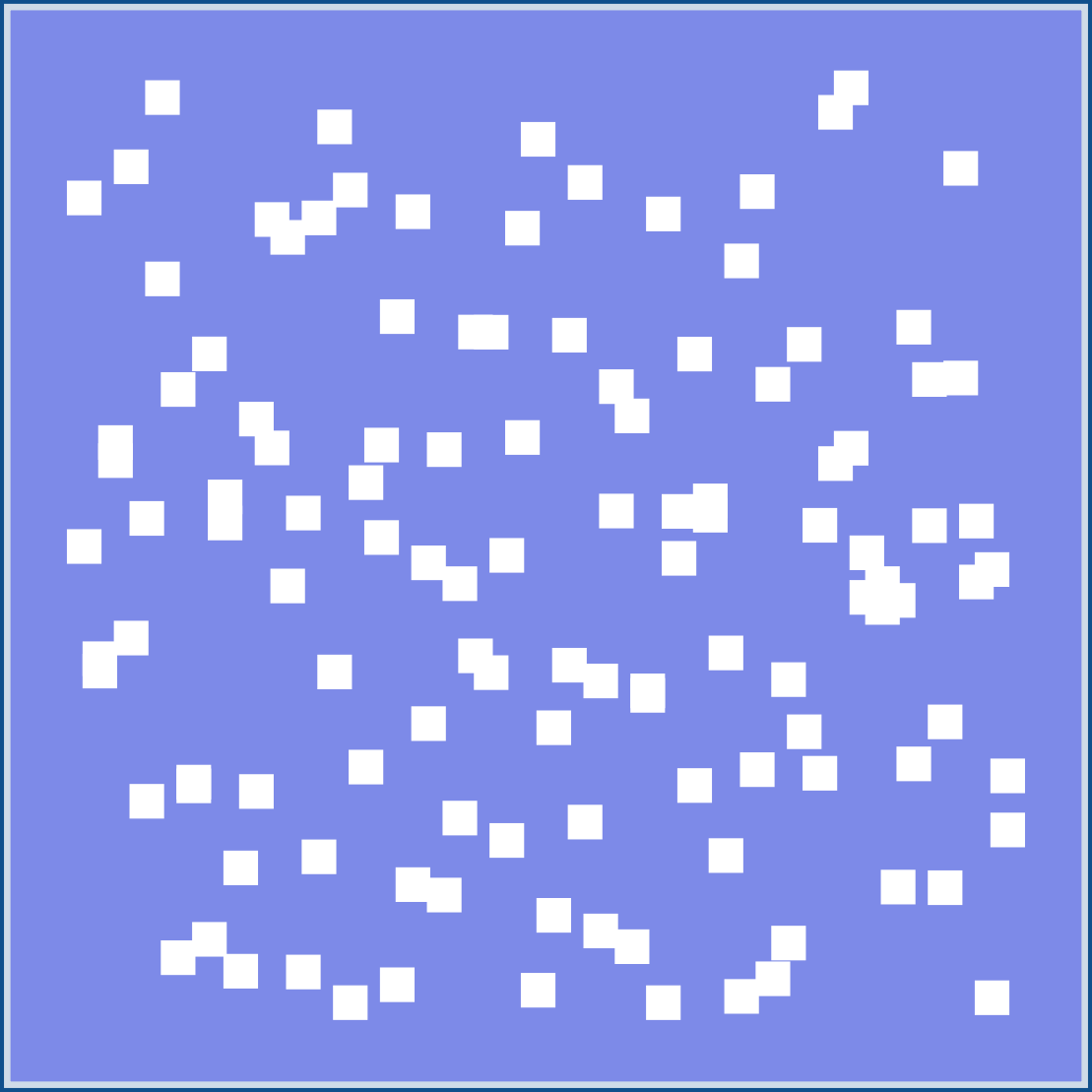


Traceability

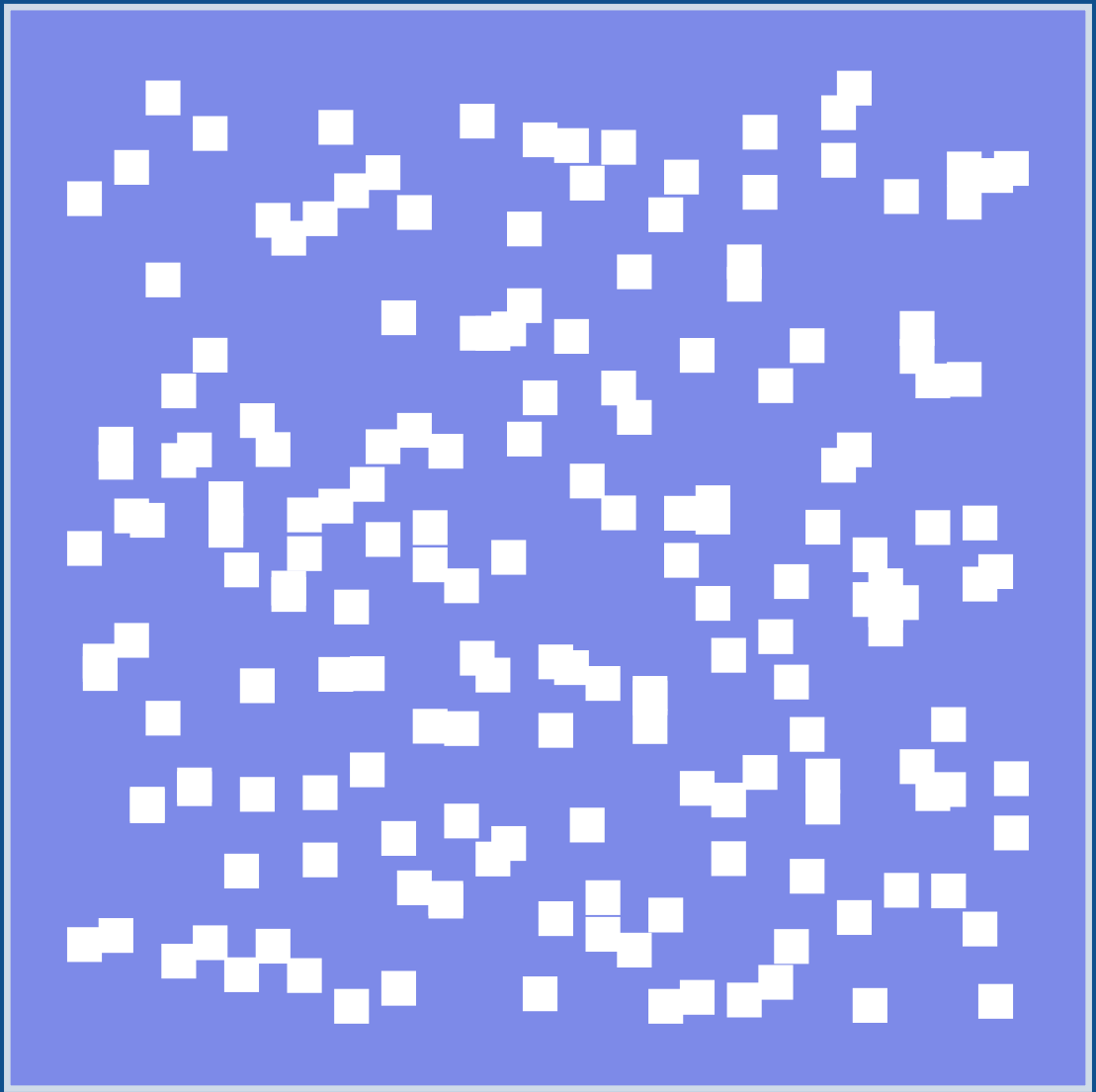
Traceability



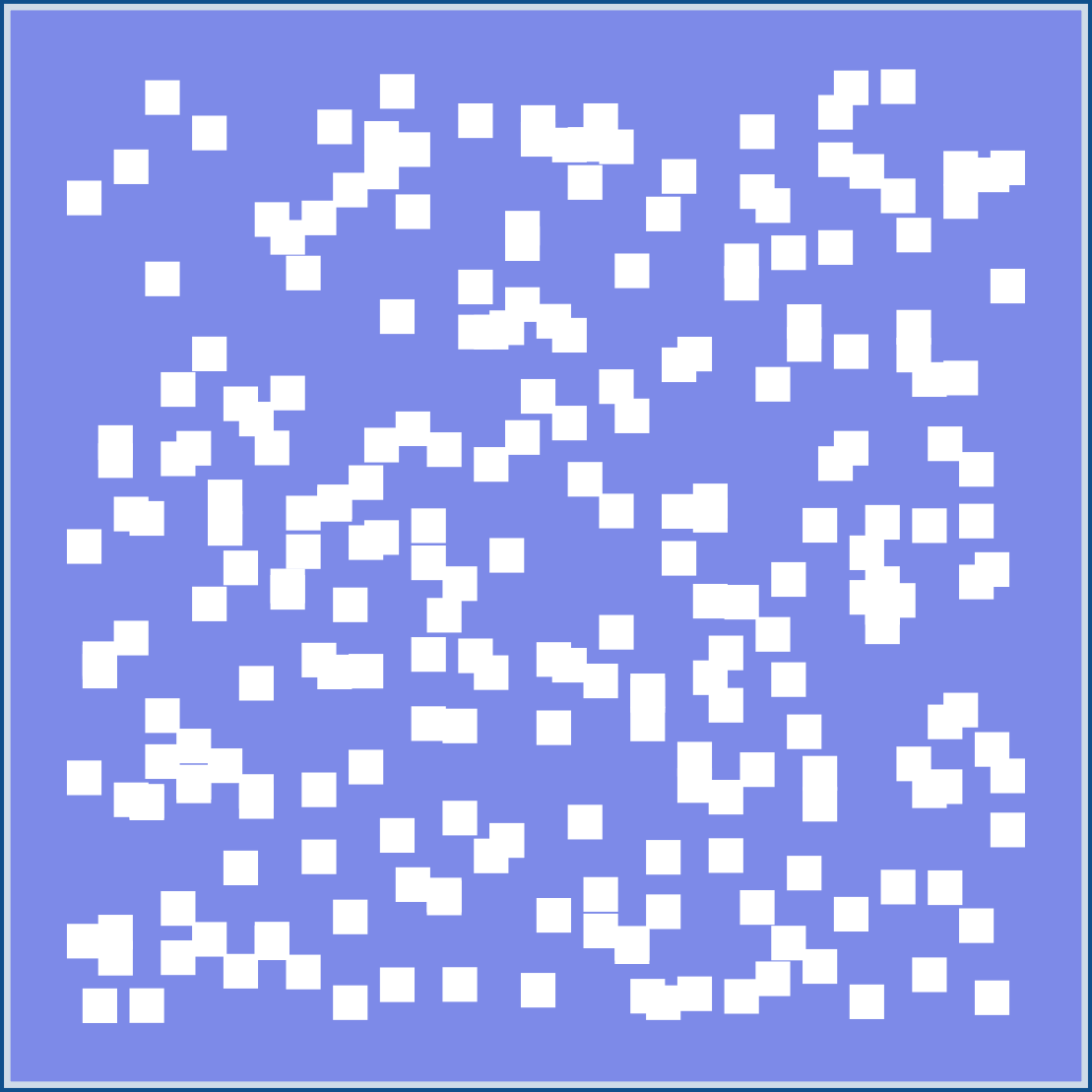
Traceability



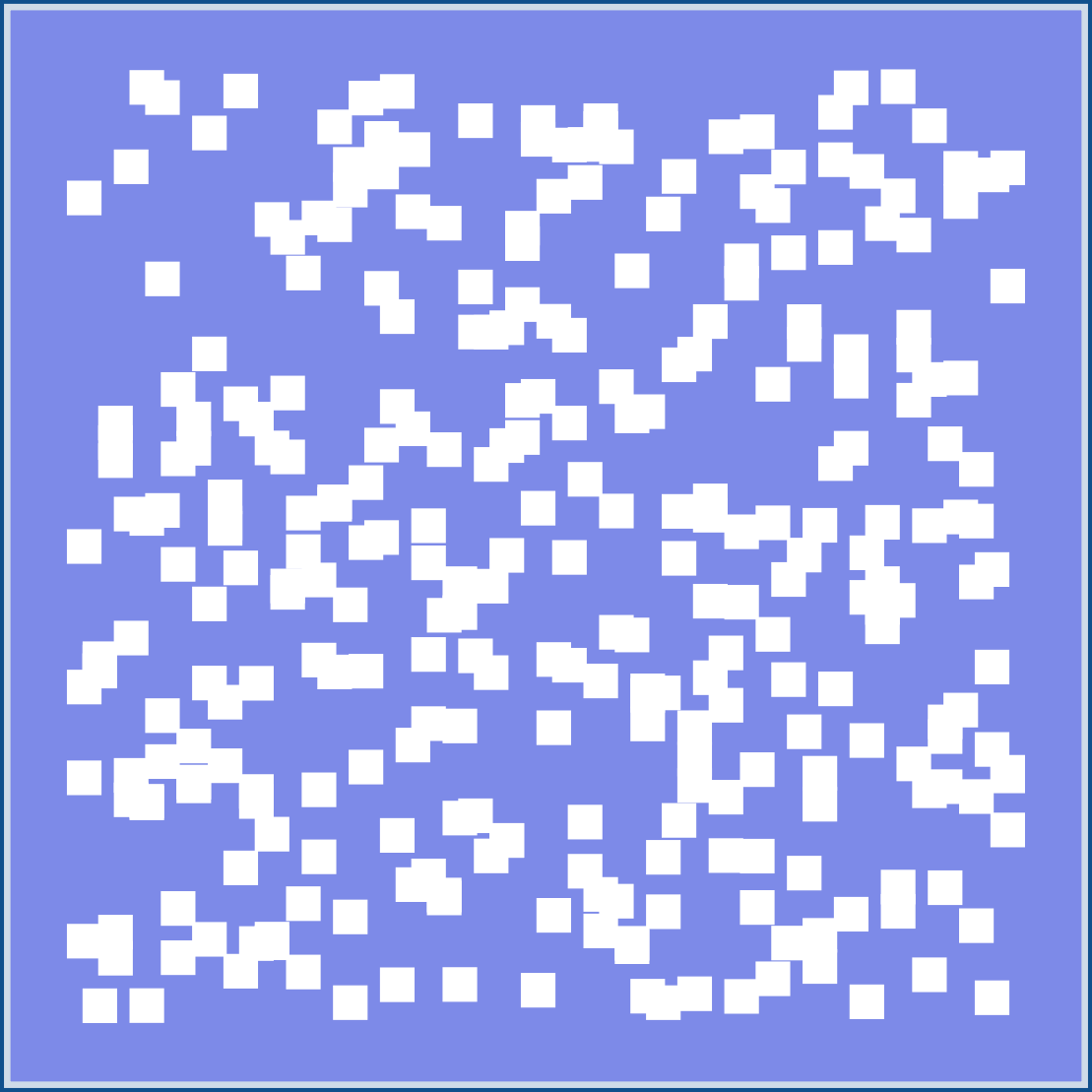
Traceability



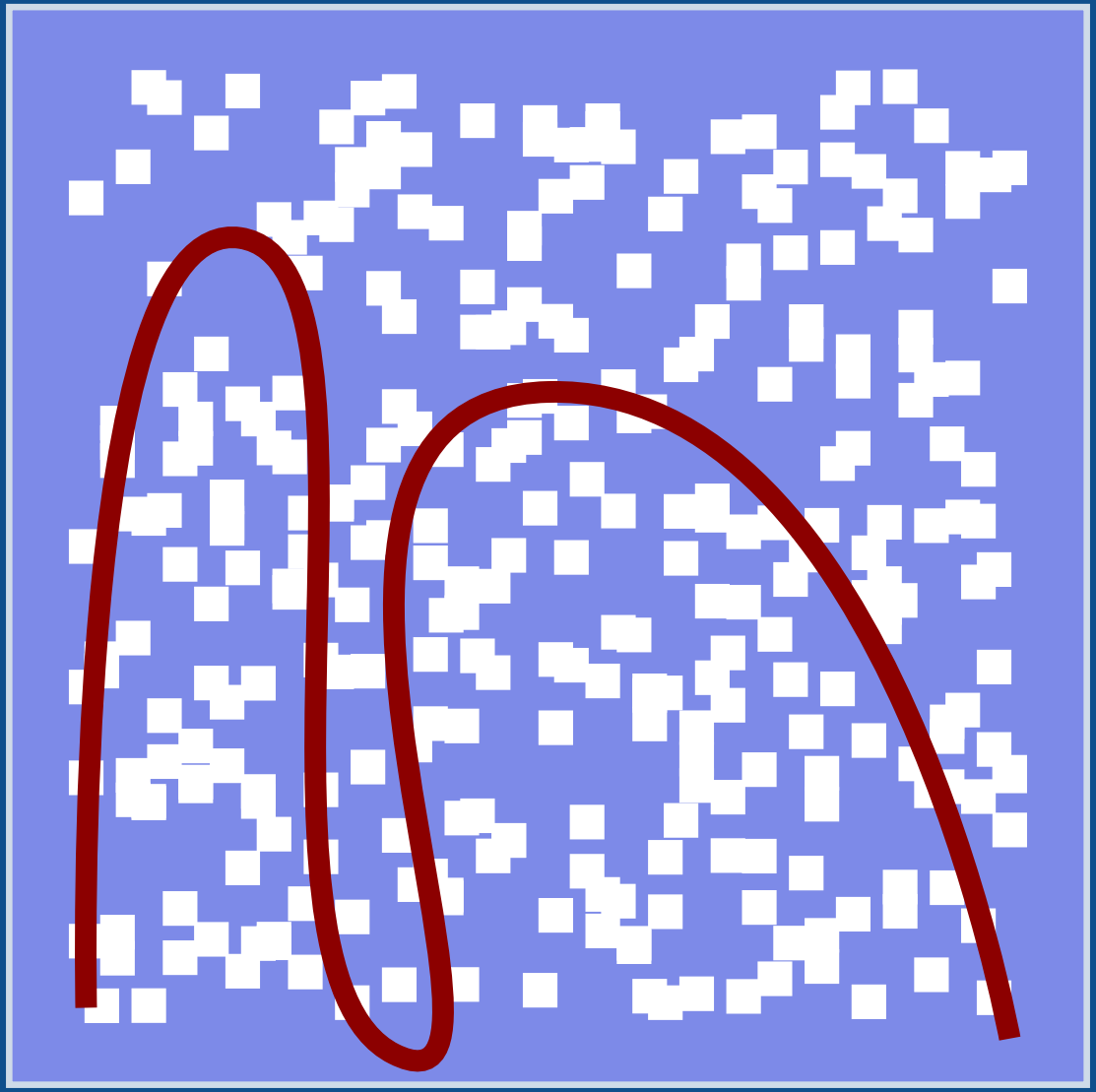
Traceability



Traceability



Traceability



Conventional Digital Signatures

Conventional Digital Signatures

Publicly verifiable, transferable

Conventional Digital Signatures

Publicly verifiable, transferable

Deniability

Conventional Digital Signatures	Publicly verifi-able, transferable
Deniability	e-voting, e-coin

Conventional Digital Signatures	Publicly verifi-able, transferable
Deniability	e-voting, e-coin
Linkability	

Conventional Digital Signatures	Publicly verifi-able, transferable
Deniability	e-voting, e-coin
Linkability	Fairness in anony-mous communications

Conventional Digital Signatures	Publicly verifiable, transferable
Deniability	e-voting, e-coin
Linkability	Fairness in anonymous communications
Traceability	

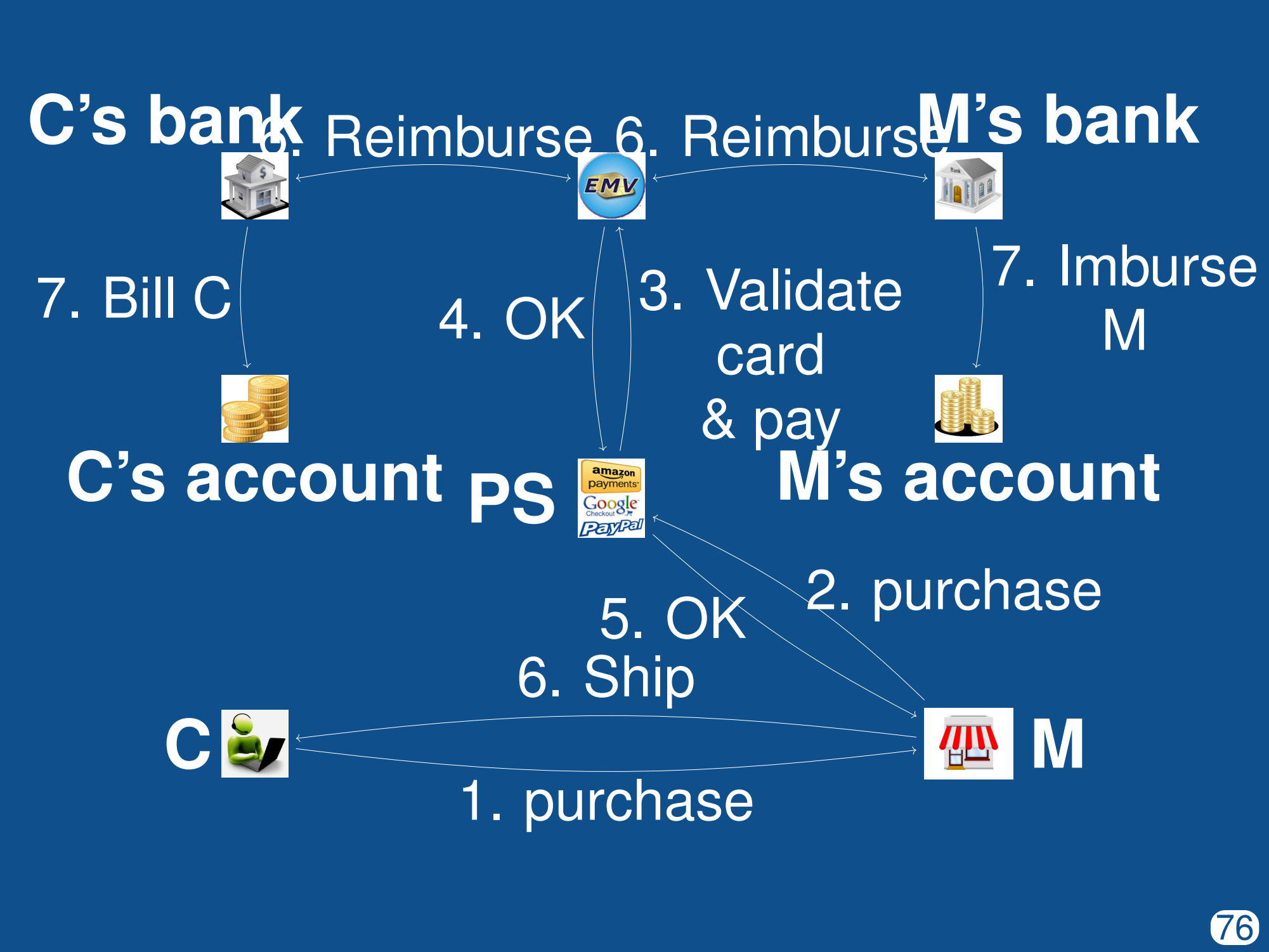
Conventional Digital Signatures	Publicly verifiable, transferable
Deniability	e-voting, e-coin
Linkability	Fairness in anonymous communications
Traceability	promotions in privacy respectul e-commerce

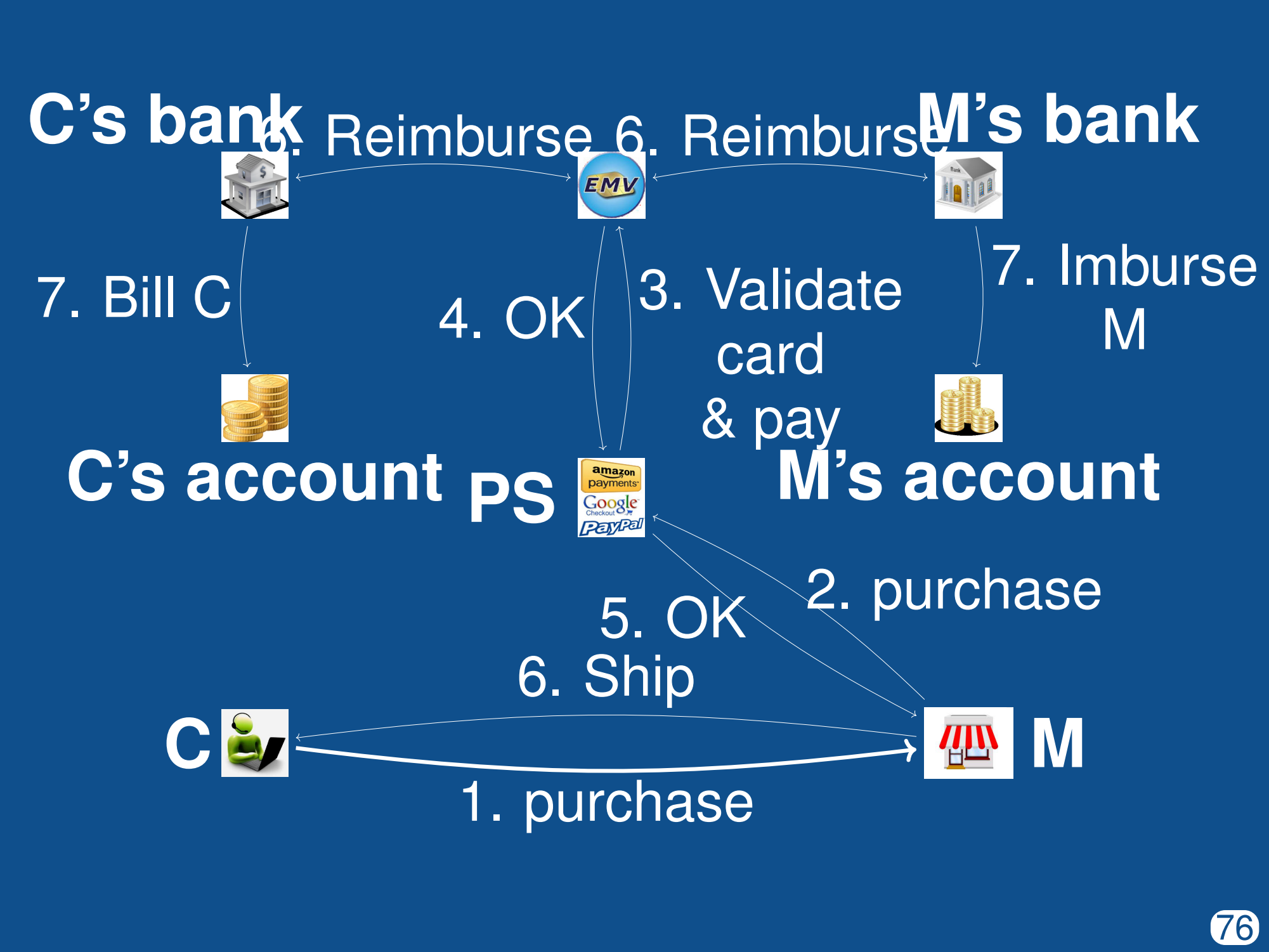
Jesus Diaz, David Arroyo, and Francisco B. Rodriguez (2014). “New X.509-based mechanisms for fair anonymity management”. In: *Computers & Security* 46, pp. 111–125

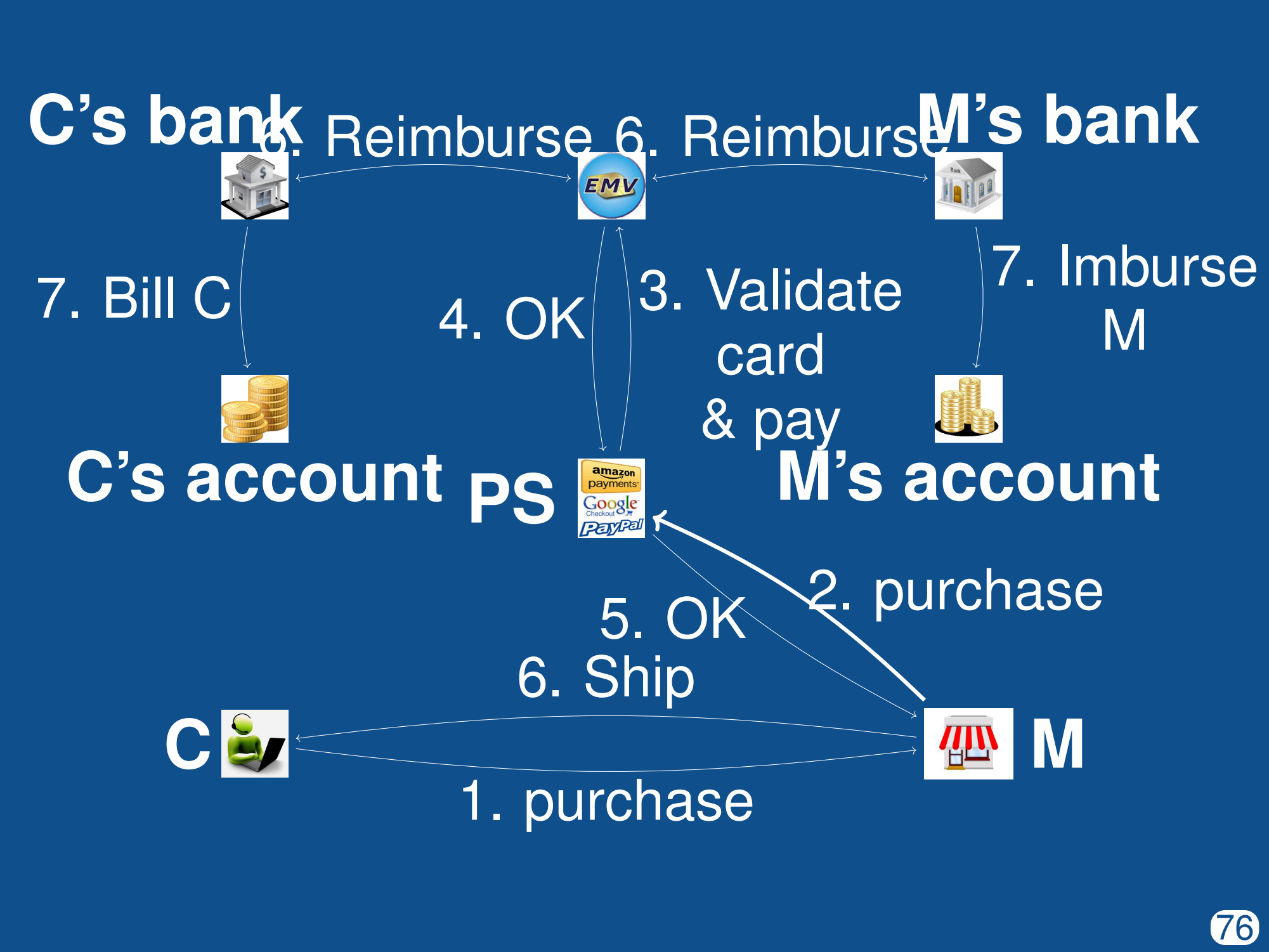
Privacy preserving e-commerce

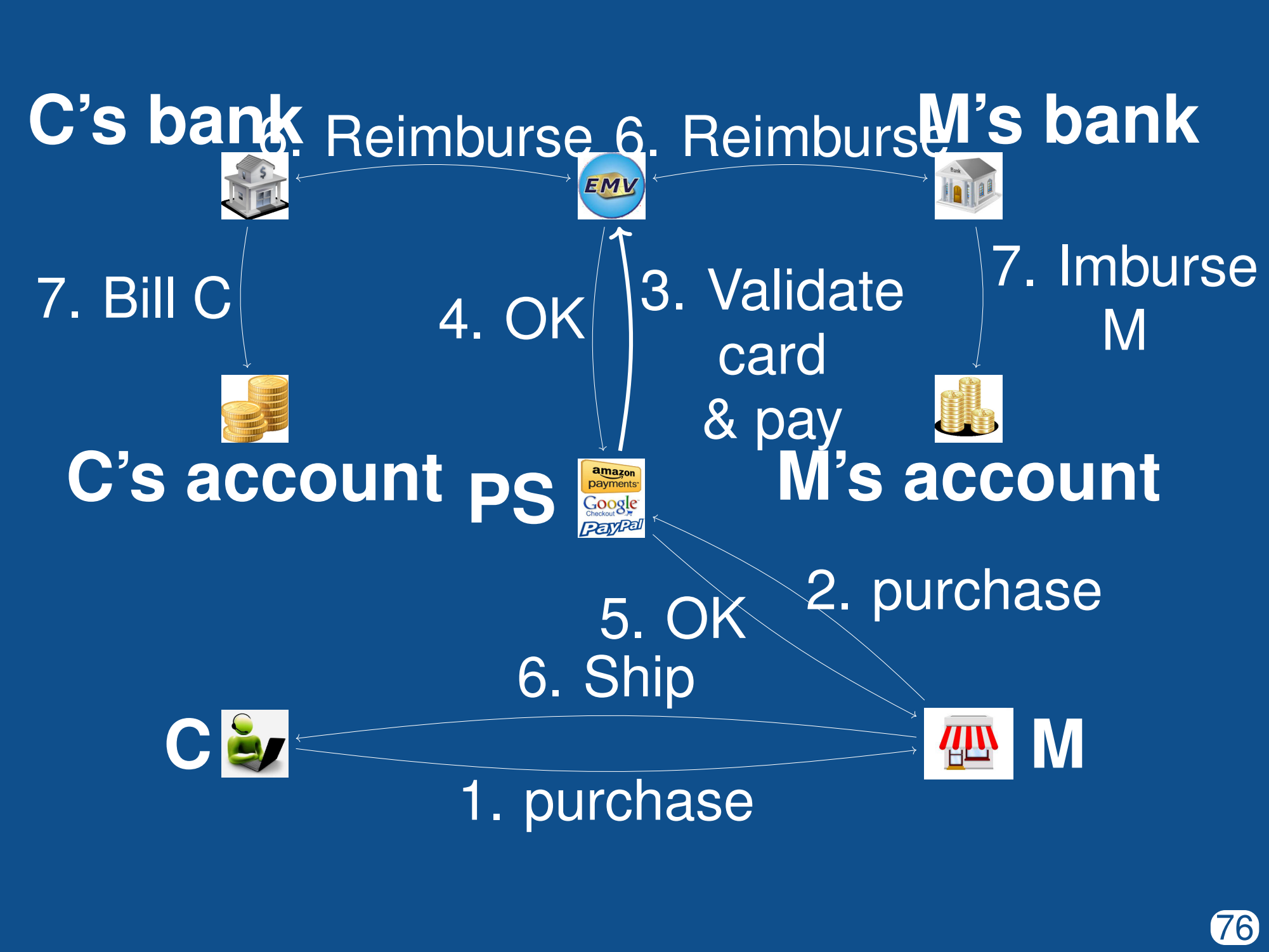
Jesús Díaz et al. (2016). “Privacy Threats in E-Shopping (Position Paper)”. In: *Lecture Notes in Computer Science*

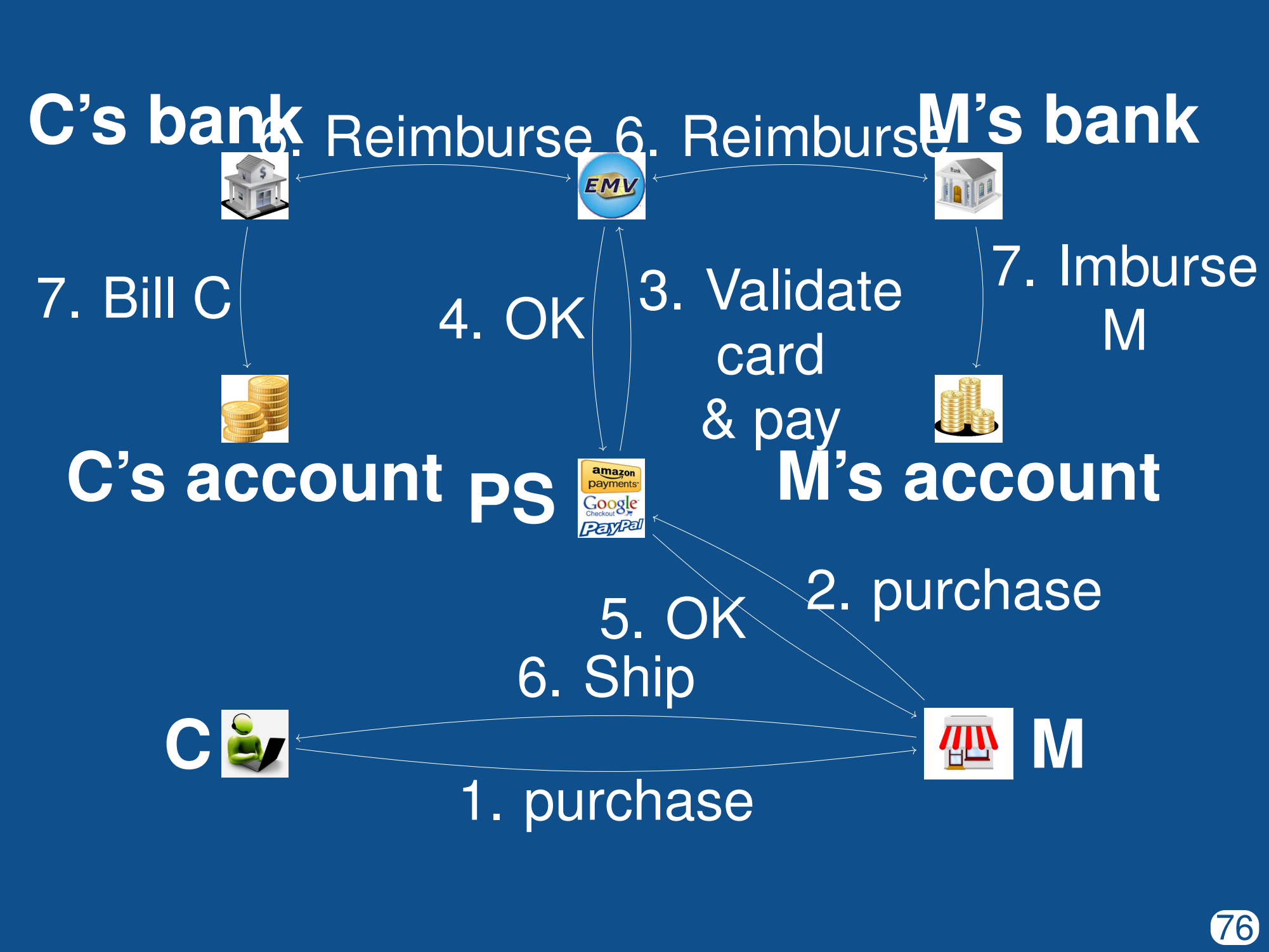
Jesus Diaz, Seung Geol Choi, et al. (2018). “Privacy in e-shopping transactions: Exploring and addressing the trade-offs”. In: *International Symposium on Cyber Security Cryptography and Machine Learning*. Springer, pp. 206–226

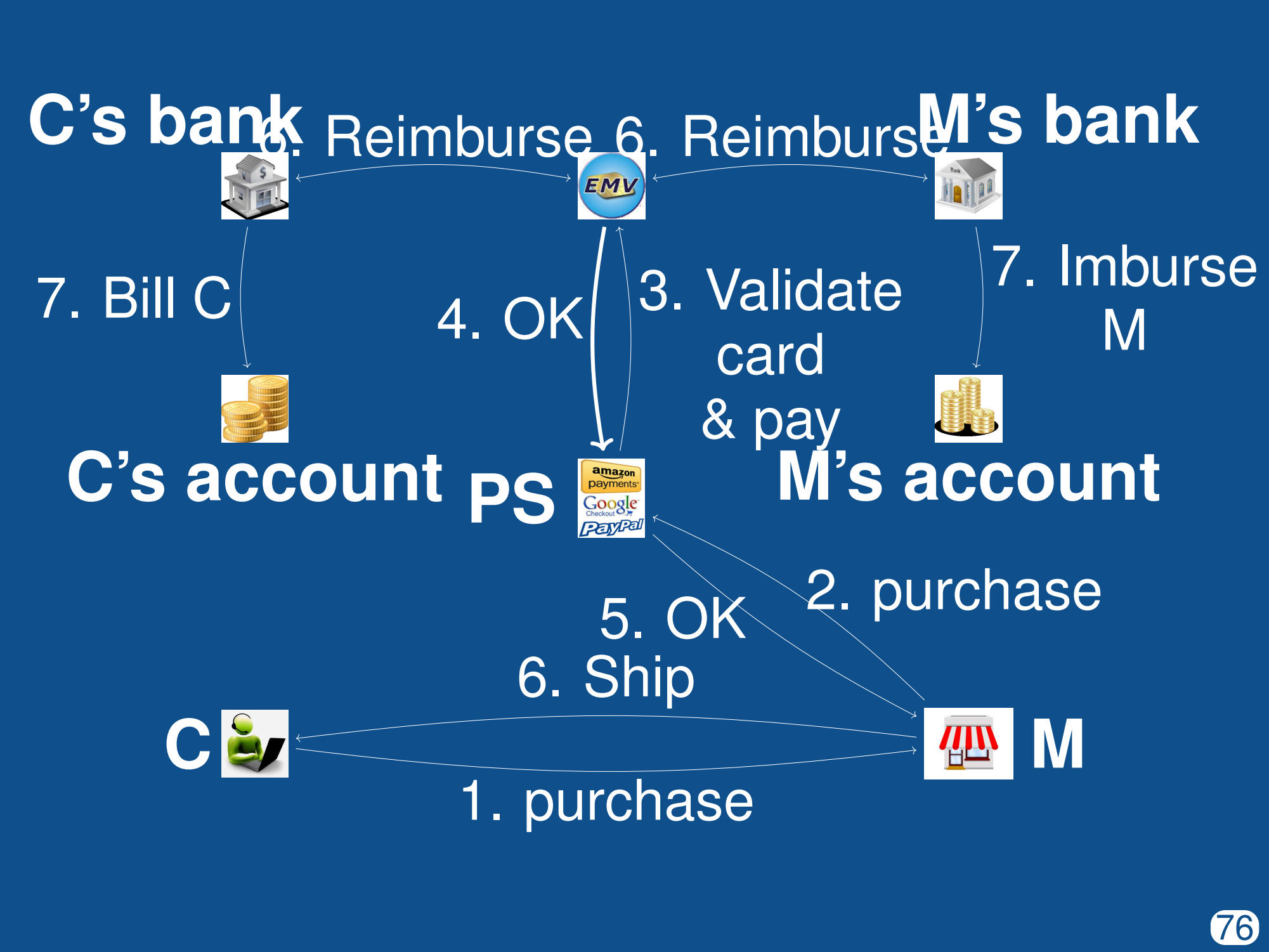

C's bank
6. Reimburse
6. Reimburse
M's bank
7. Bill C
4. OK
3. Validate card & pay
7. Imburse M
C's account
PS
M's account
2. purchase
5. OK
6. Ship
C
M
1. purchase

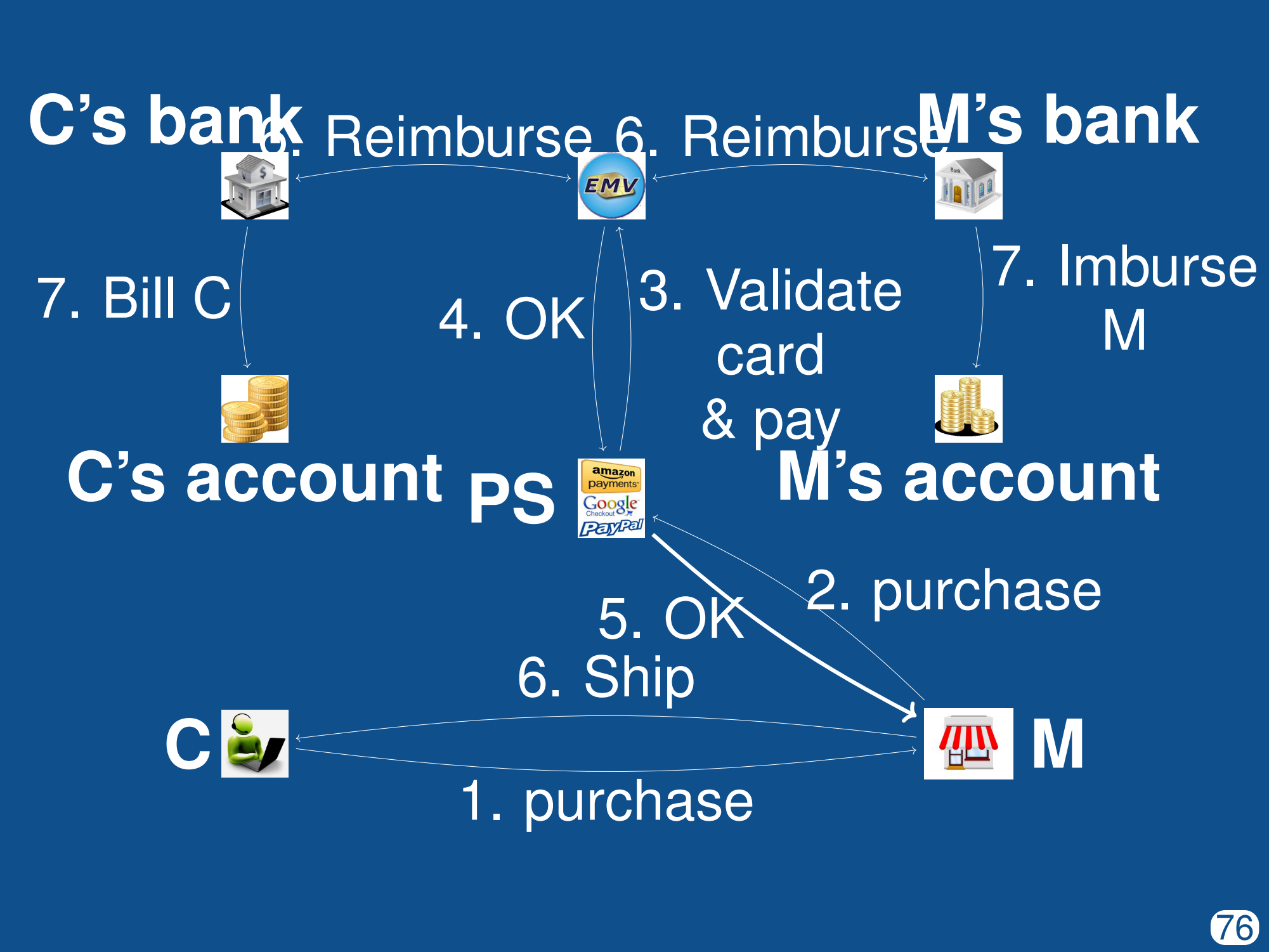

C's bank
6. Reimburse
6. Reimburse
M's bank
7. Bill C
4. OK
3. Validate card & pay
7. Imburse M
C's account
PS
M's account
2. purchase
5. OK
6. Ship
C
M
1. purchase

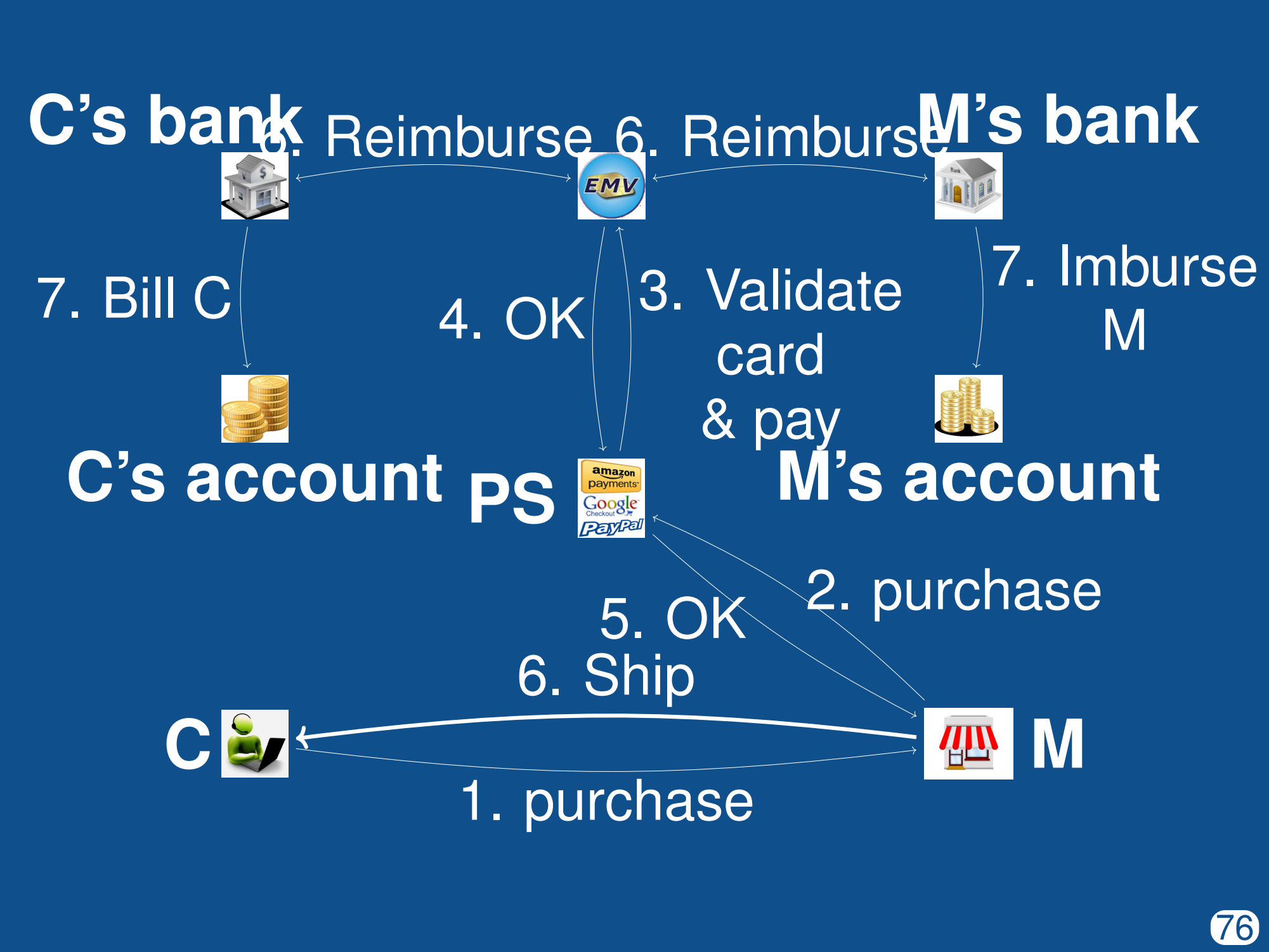

C's bank
6. Reimburse
6. Reimburse
M's bank
7. Bill C
4. OK
3. Validate card & pay
7. Imburse M
C's account
PS
M's account
2. purchase
5. OK
6. Ship
C
M
1. purchase

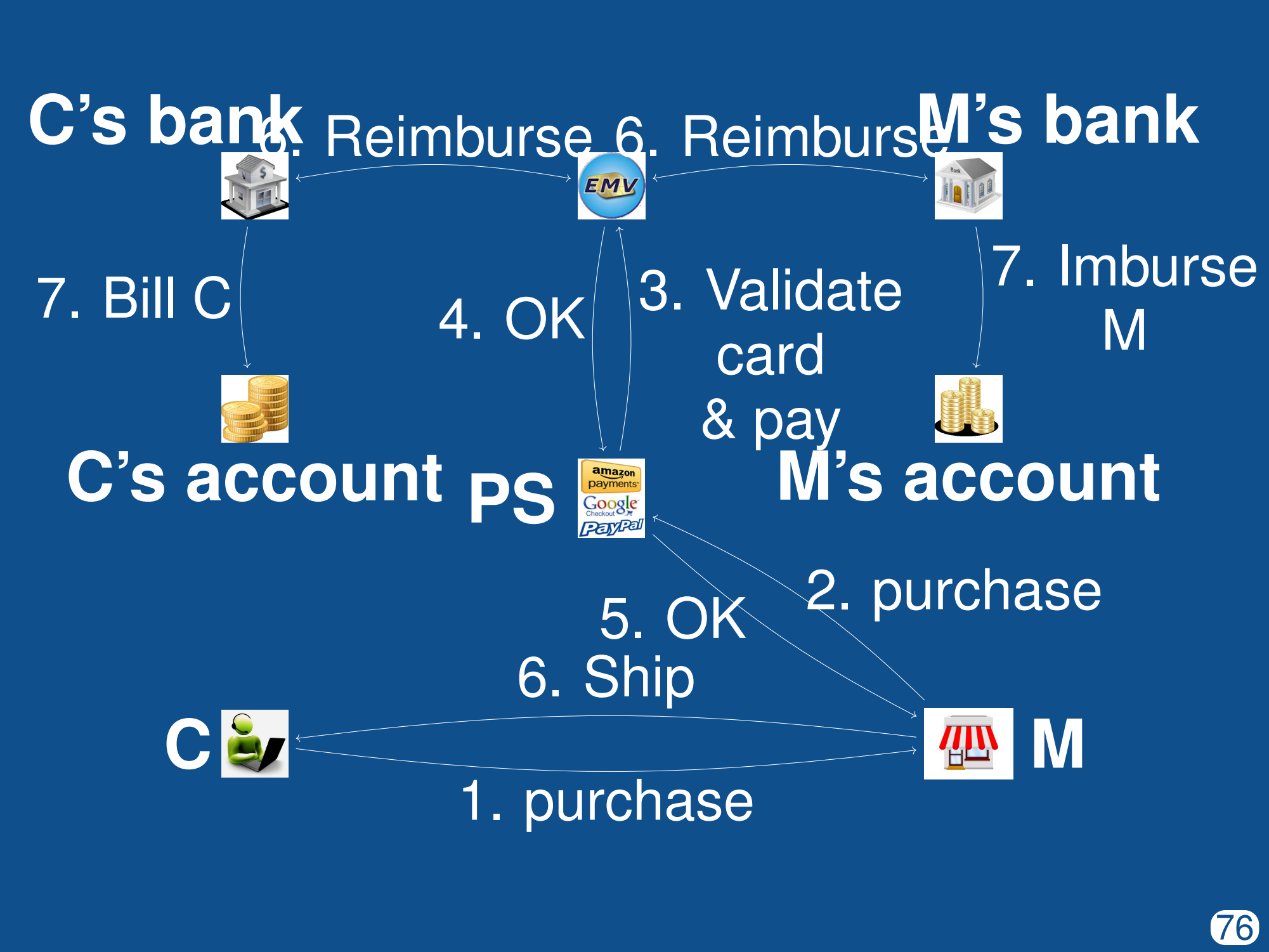

C's bank
6. Reimburse
6. Reimburse
M's bank
7. Bill C
4. OK
3. Validate card & pay
7. Imburse M
C's account
PS
M's account
2. purchase
5. OK
6. Ship
C
M
1. purchase


C's bank
6. Reimburse
6. Reimburse
M's bank
7. Bill C
4. OK
3. Validate card & pay
7. Imburse M
C's account
PS
M's account
2. purchase
5. OK
6. Ship
C
M
1. purchase


C's bank
6. Reimburse
6. Reimburse
M's bank
7. Bill C
4. OK
3. Validate card & pay
7. Imburse M
C's account
PS
M's account
2. purchase
5. OK
6. Ship
C
M
1. purchase


C's bank
6. Reimburse
6. Reimburse
M's bank
7. Bill C
4. OK
3. Validate card & pay
7. Imburse M
C's account
PS
M's account
2. purchase
5. OK
6. Ship
C
M
1. purchase


C's bank
6. Reimburse
6. Reimburse
M's bank
7. Bill C
4. OK
3. Validate card & pay
7. Imburse M
C's account
PS
M's account
2. purchase
5. OK
6. Ship
C
M
1. purchase


C's bank
6. Reimburse
6. Reimburse
M's bank
7. Bill C
4. OK
3. Validate card & pay
7. Imburse M
C's account
PS
M's account
2. purchase
5. OK
6. Ship
C
M
1. purchase

e-voting

Iñigo Querejeta-Azurmendi et al. (2020). “NetVote: A Strict-Coercion Resistance Re-Voting Based Internet Voting Scheme with Linear Filtering”. In: *Mathematics* 8.9, p. 1618

Registration agent

Voter

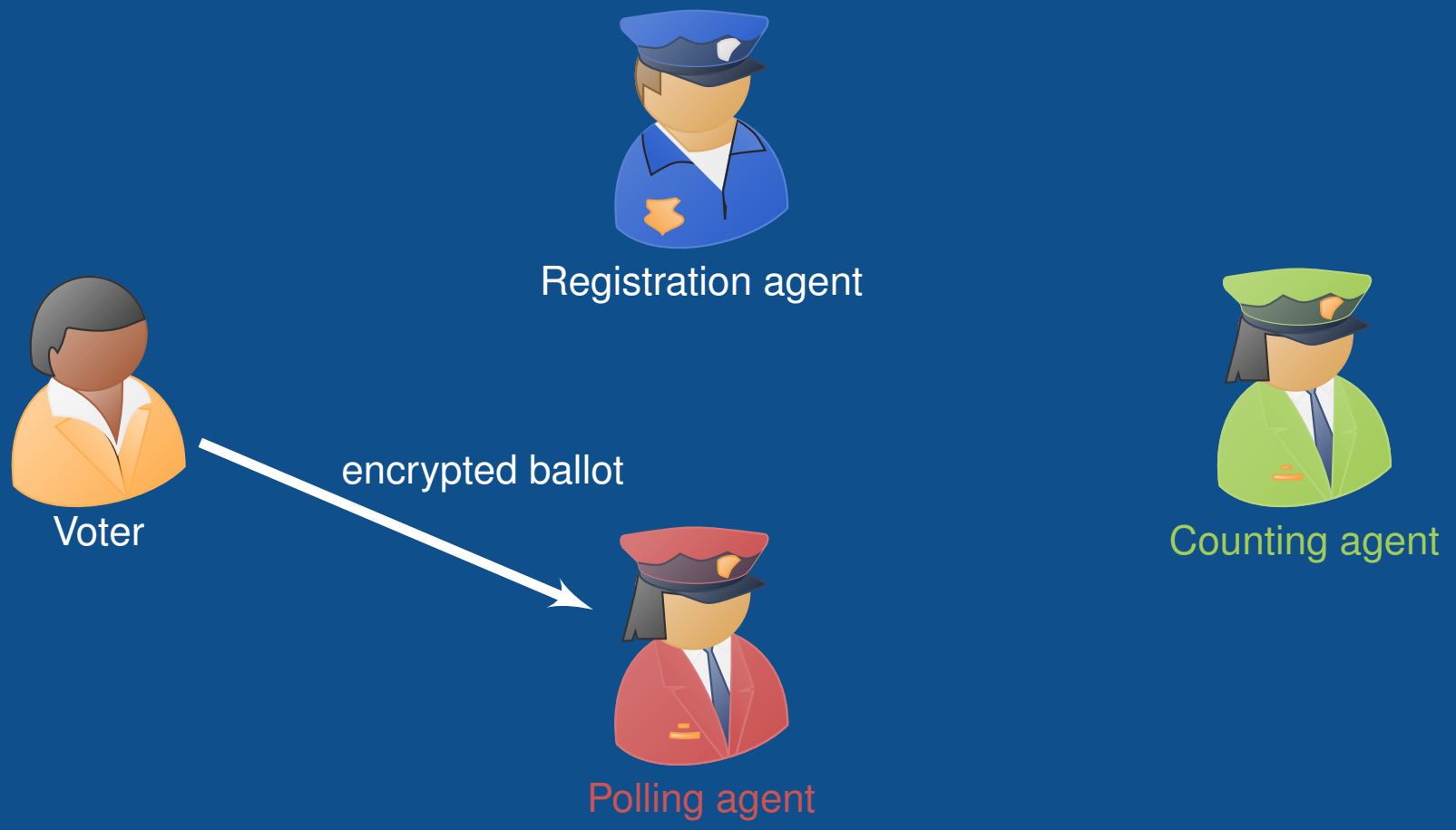
Counting agent

Polling agent

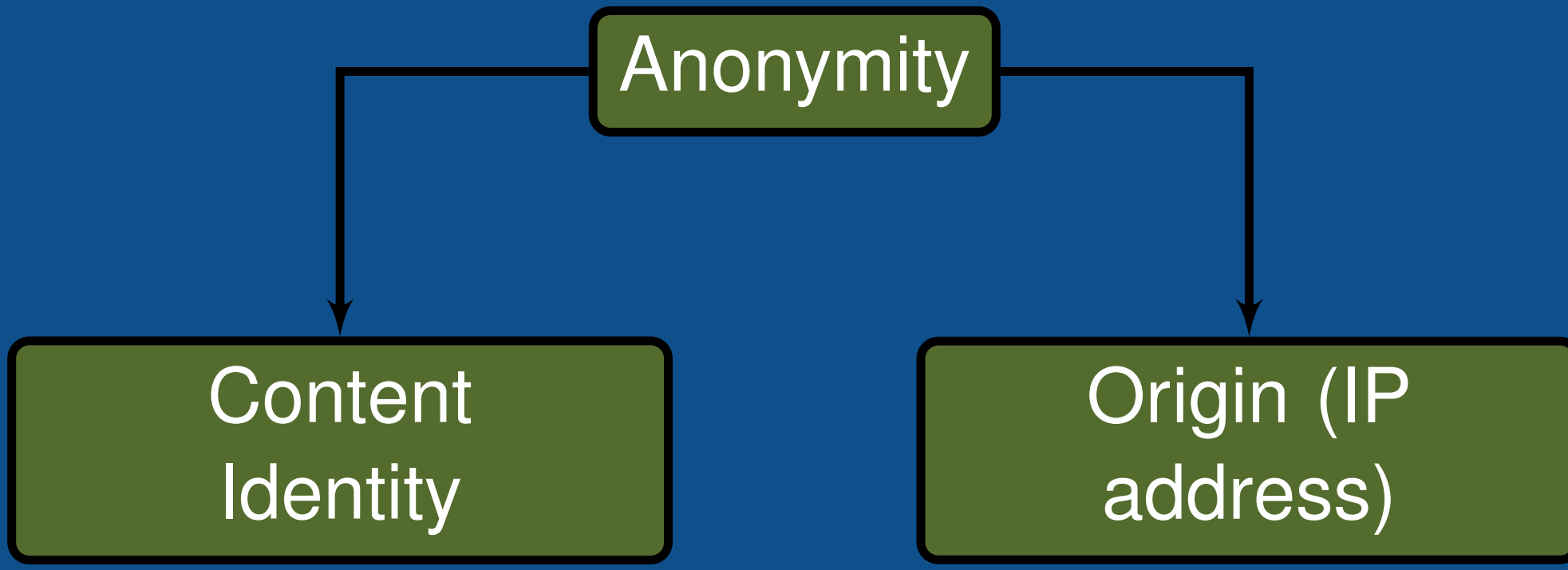

authentication
Registration agent
Voter
Counting agent
Polling agent

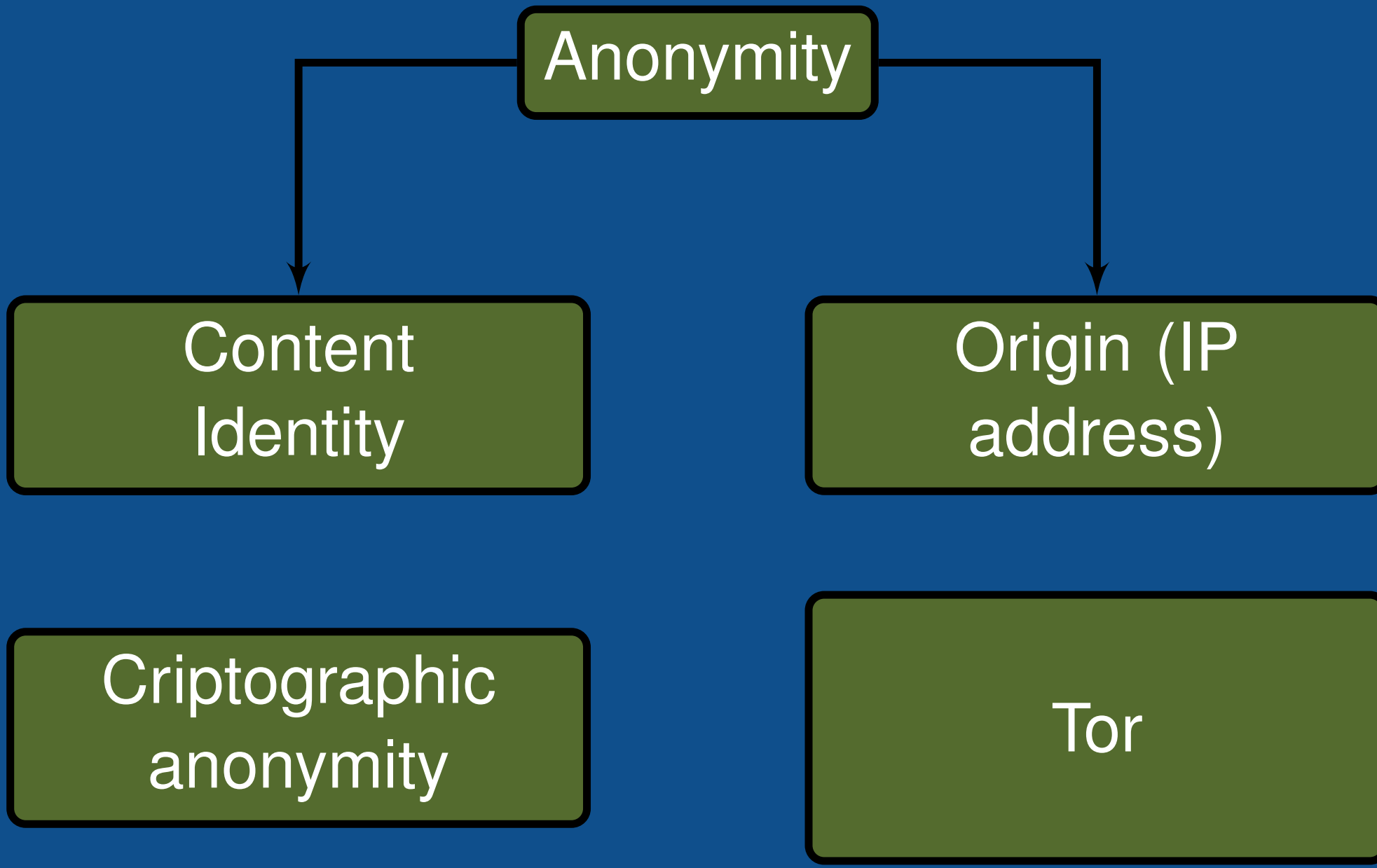
Designated Verifier Proofs: ZK/Deniability

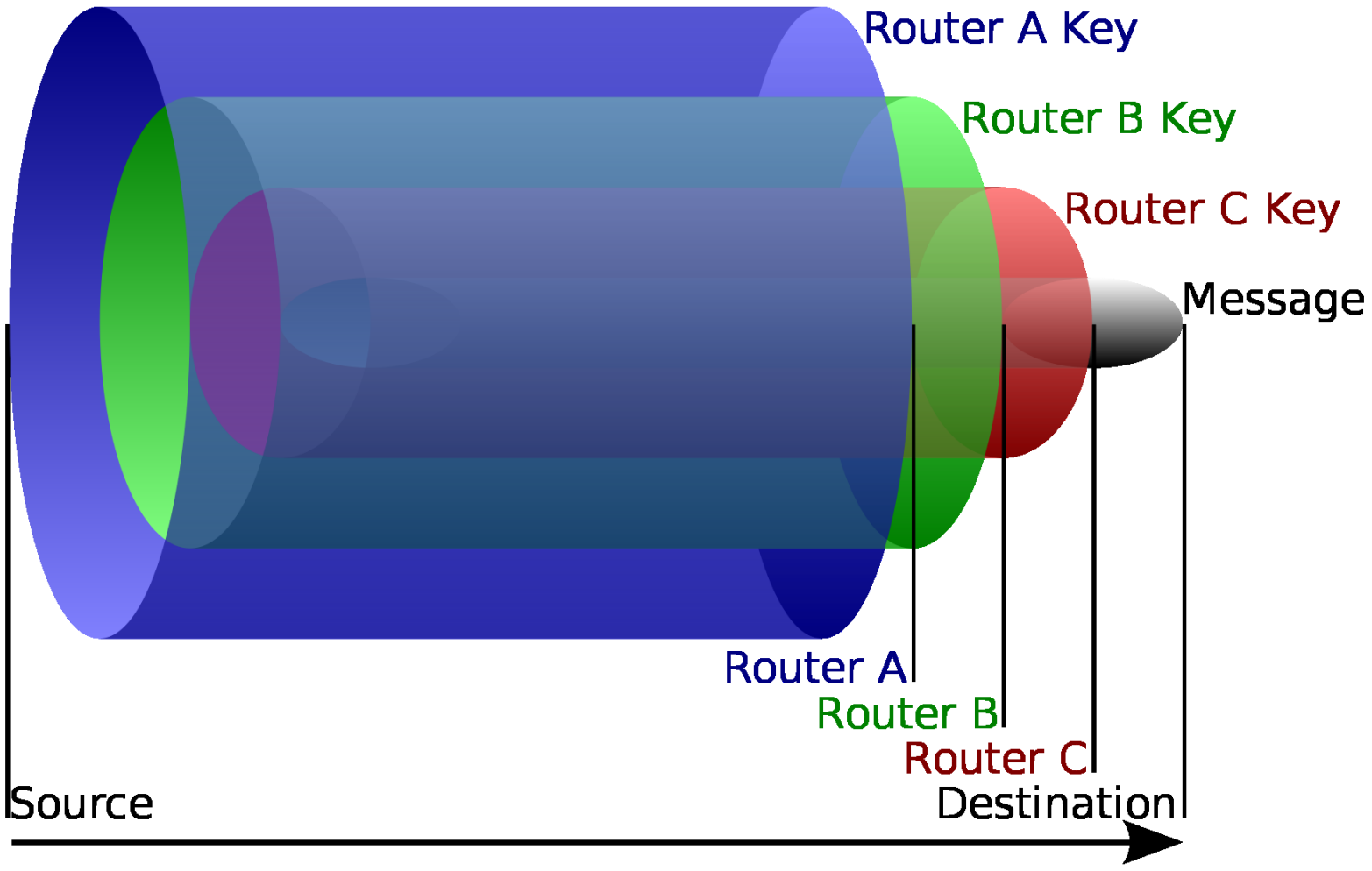
Vote format verification: ZK



Votes counting: homomorphic encryption


Anonymity
Content Identity
Origin (IP address)


Anonymity
Content Identity
Origin (IP address)
Criptographic anonymity
Tor


Router A Key
Router B Key
Router C Key
Message
Router A
Router B
Router C
Source
Destination

Use and abuse of Tor

- It is associated to Darknet

Use and abuse of Tor

- It is associated to Darknet
  - A portion of the DeepWeb: content unreachable through Google, Bing, etc.

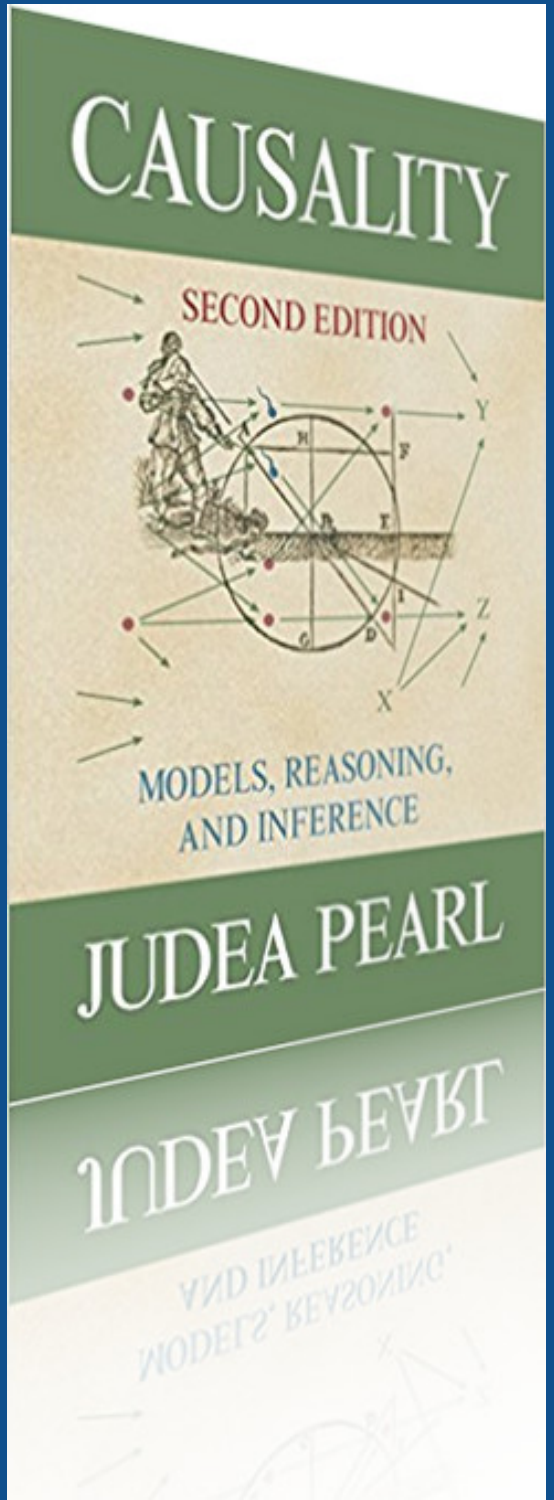
Use and abuse of Tor

- It is associated to Darknet
  - A portion of the DeepWeb: content unreachable through Google, Bing, etc.
  - Illegal activities: weapons traffic, stolen goods, drugs trafficking , cyberterrorism, etc.

Use and abuse of Tor

- It is associated to Darknet
  - A portion of the DeepWeb: content unreachable through Google, Bing, etc.
  - Illegal activities: weapons traffic, stolen goods, drugs trafficking , cyberterrorism, etc.
- Tor is blocked by many service providers

Technology is not define by the way it is used. . .



Behind any causal conclusion there must be some causal conclusion, untested in observational studies

http://www.tylervigen.com/spurious-correlations

4 *Main challenges in cybersecurity*

Data and computing outsourcing

Privacy

Cryptographic anonymity management

Distributed trust management

Do you need a blockchain in your life?

Fair anonymity in Tor

Jesus Diaz, David Arroyo, and Francisco B Rodriguez (2017). “Fair anonymity for the Tor network”. In: *The 14th International Conference on Security and Cryptography (SECRYPT 2017)*, Accepted as Position Paper. In Press

Fairness as a Service

4 *Main challenges in cybersecurity*

Data and computing outsourcing

Privacy

Distributed trust management

Do you need a blockchain in your life?

What is that thing called blockchain?

- P2P mechanism for consensus generation

What is that thing called blockchain?

- P2P mechanism for consensus generation
- Collaborative activity

What is that thing called blockchain?

- P2P mechanism for consensus generation
- Collaborative activity
- No TTP

What is that thing called blockchain?

- P2P mechanism for consensus generation
- Collaborative activity
- No TTP
- As result of the collaboration, information is stored in a *distributed ledger*

What is that thing called blockchain?

- P2P mechanism for consensus generation
- Collaborative activity
- No TTP
- As result of the collaboration, information is stored in a *distributed ledger*
- It is *inmutable*

Blockchain inmutability

- Interesting for auditing and forensics

Blockchain inmutability

- Interesting for auditing and forensics
  - *cloud*

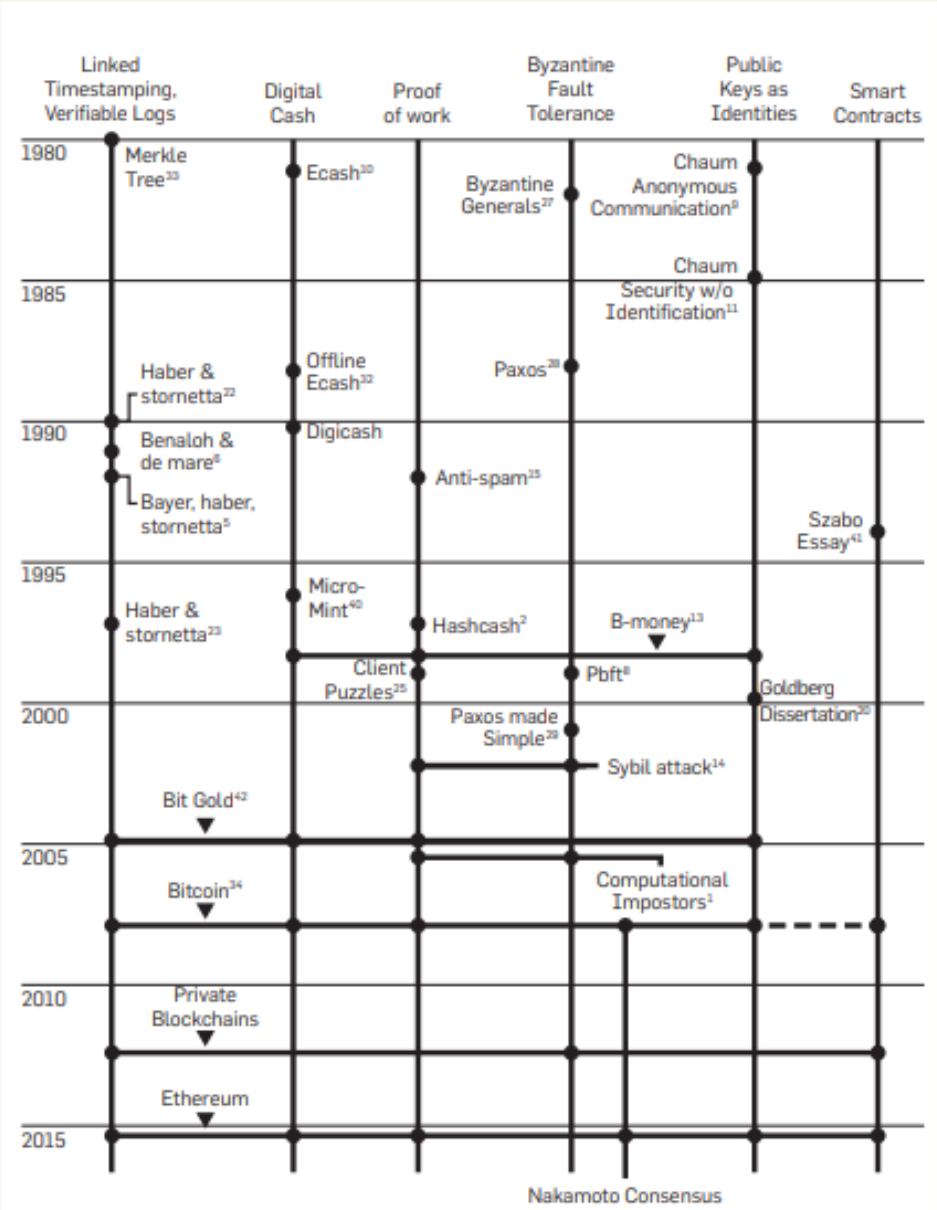
Blockchain inmutability

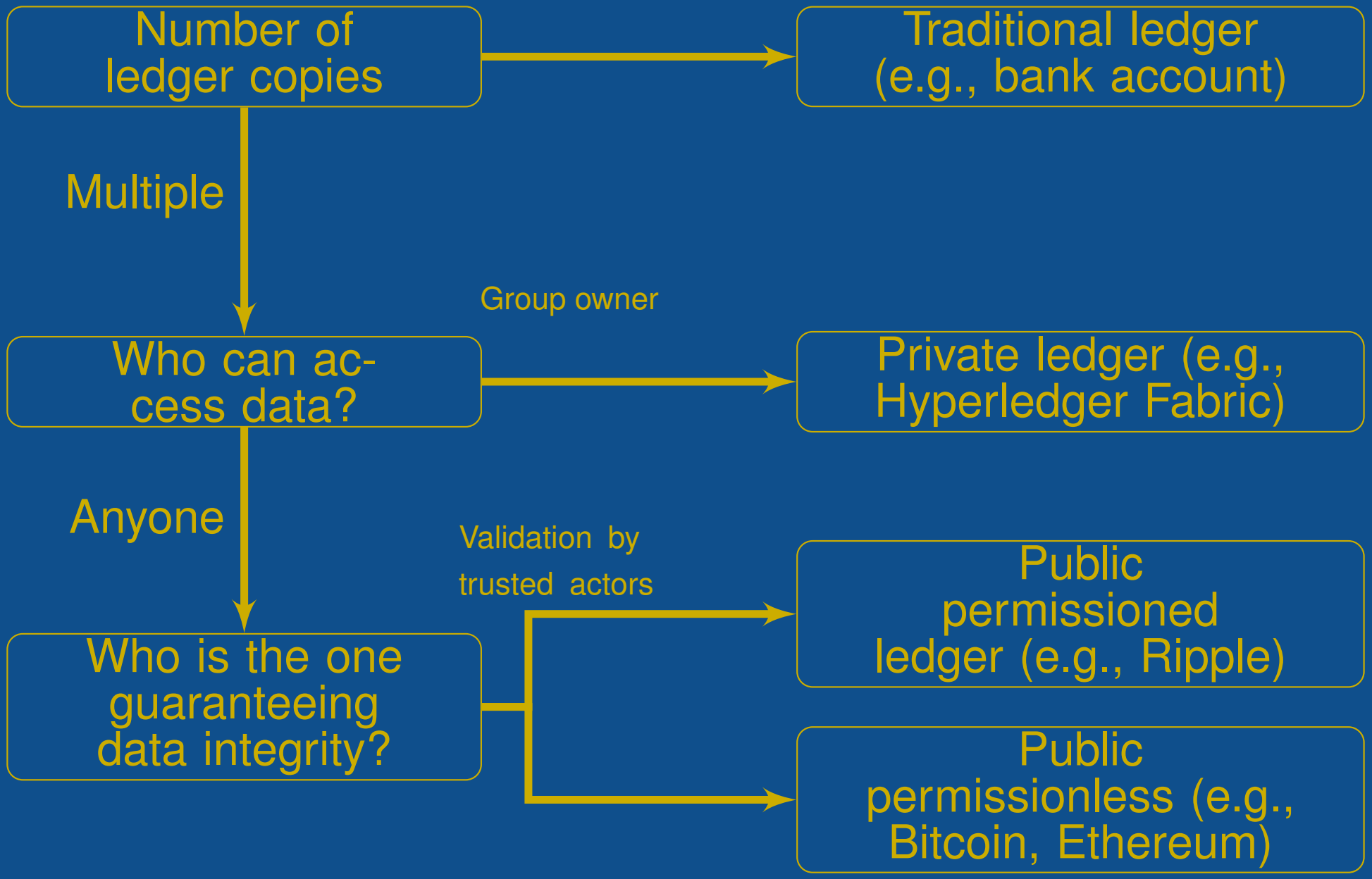
- Interesting for auditing and forensics
  - *cloud*
  - MDM

Blockchain inmutability

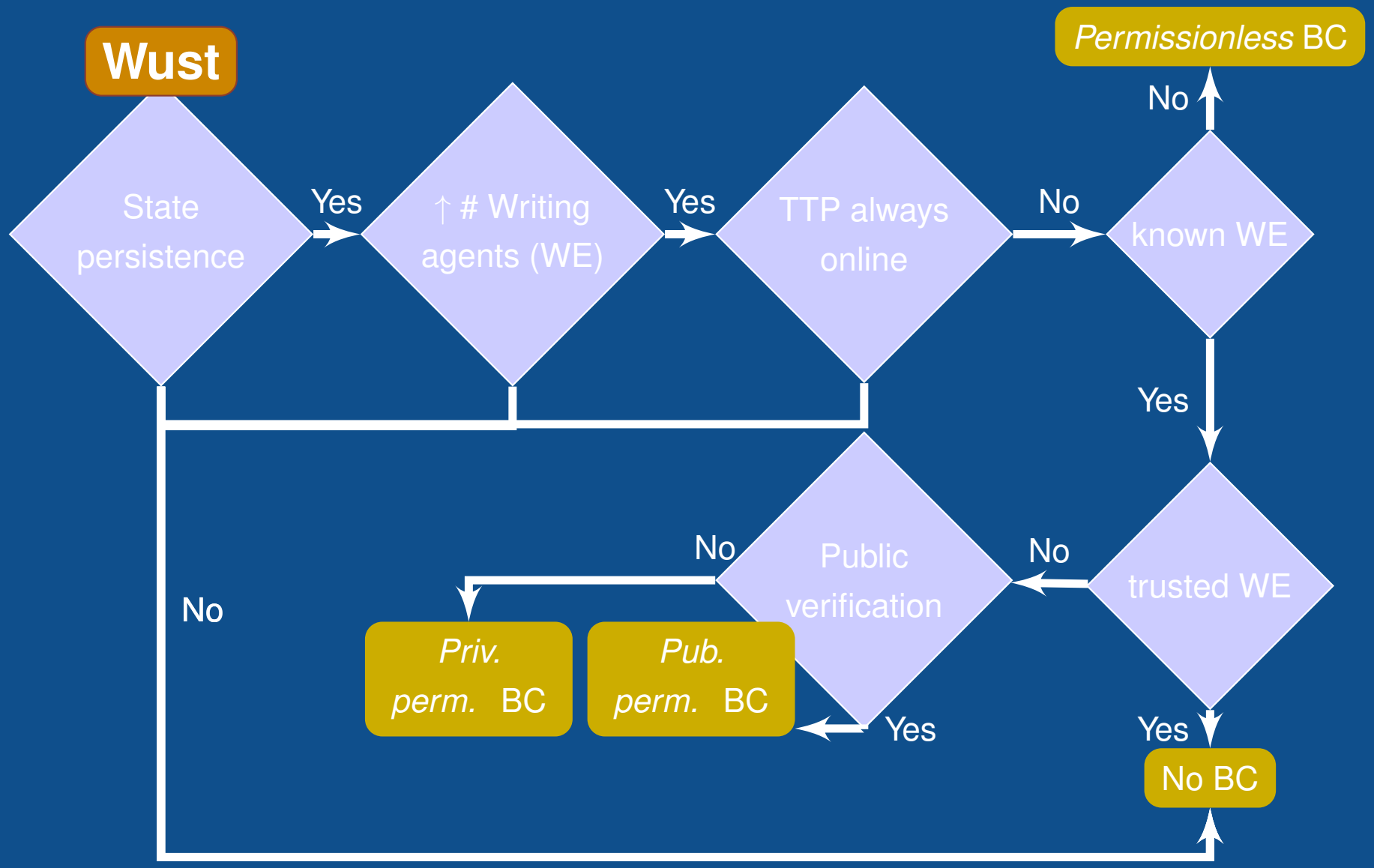
- Interesting for auditing and forensics
  - *cloud*
  - MDM
- Right to be forgotten!!!
  - Anonymous identities for *blockchain*

*narayanan2017bitcoin

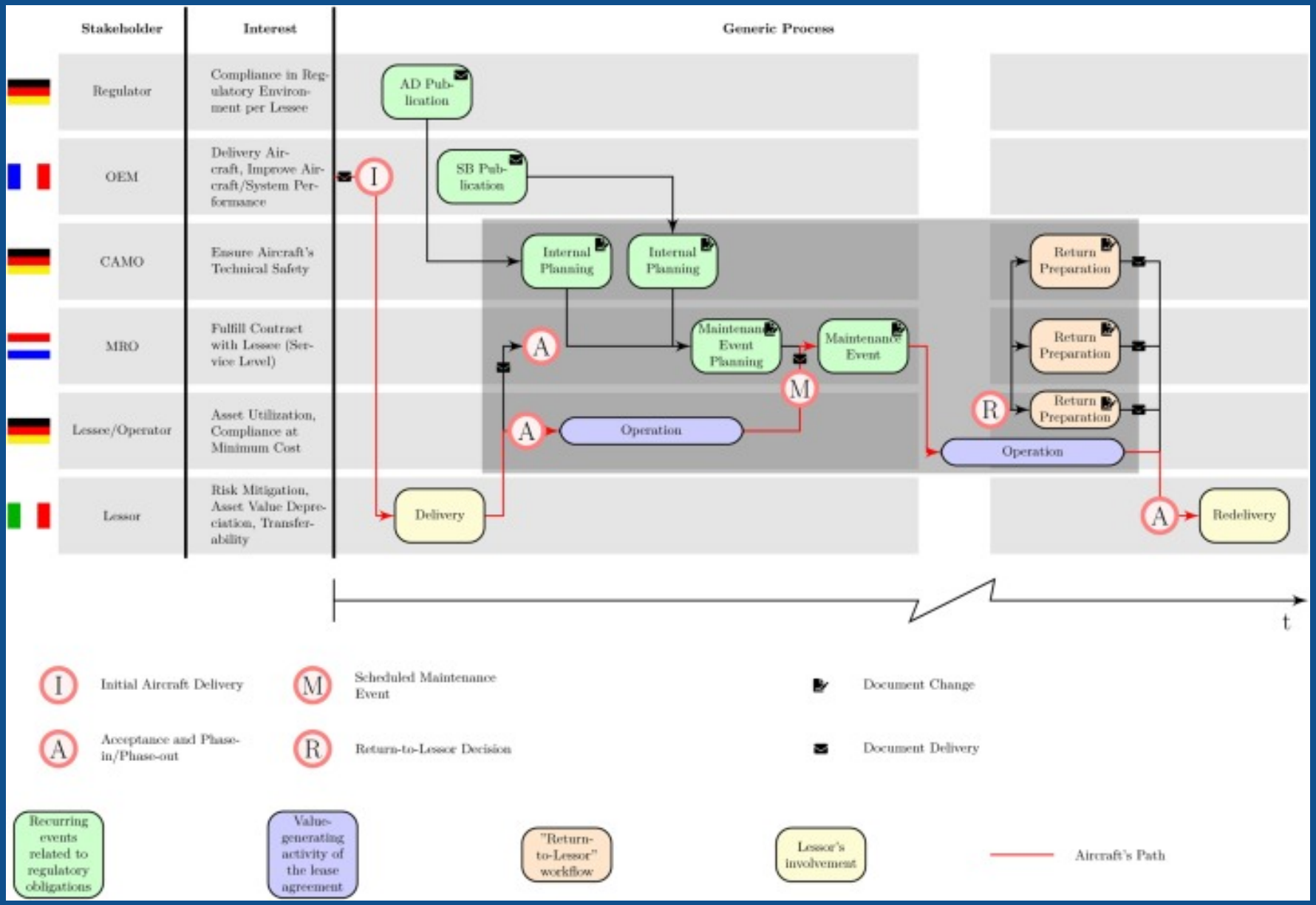



Number of ledger copies
Traditional ledger (e.g., bank account)
Multiple
Group owner
Who can access data?
Private ledger (e.g., Hyperledger Fabric)
Anyone
Validation by trusted actors
Public permissioned ledger (e.g., Ripple)
Who is the one guaranteeing data integrity?
Public permissionless (e.g., Bitcoin, Ethereum)

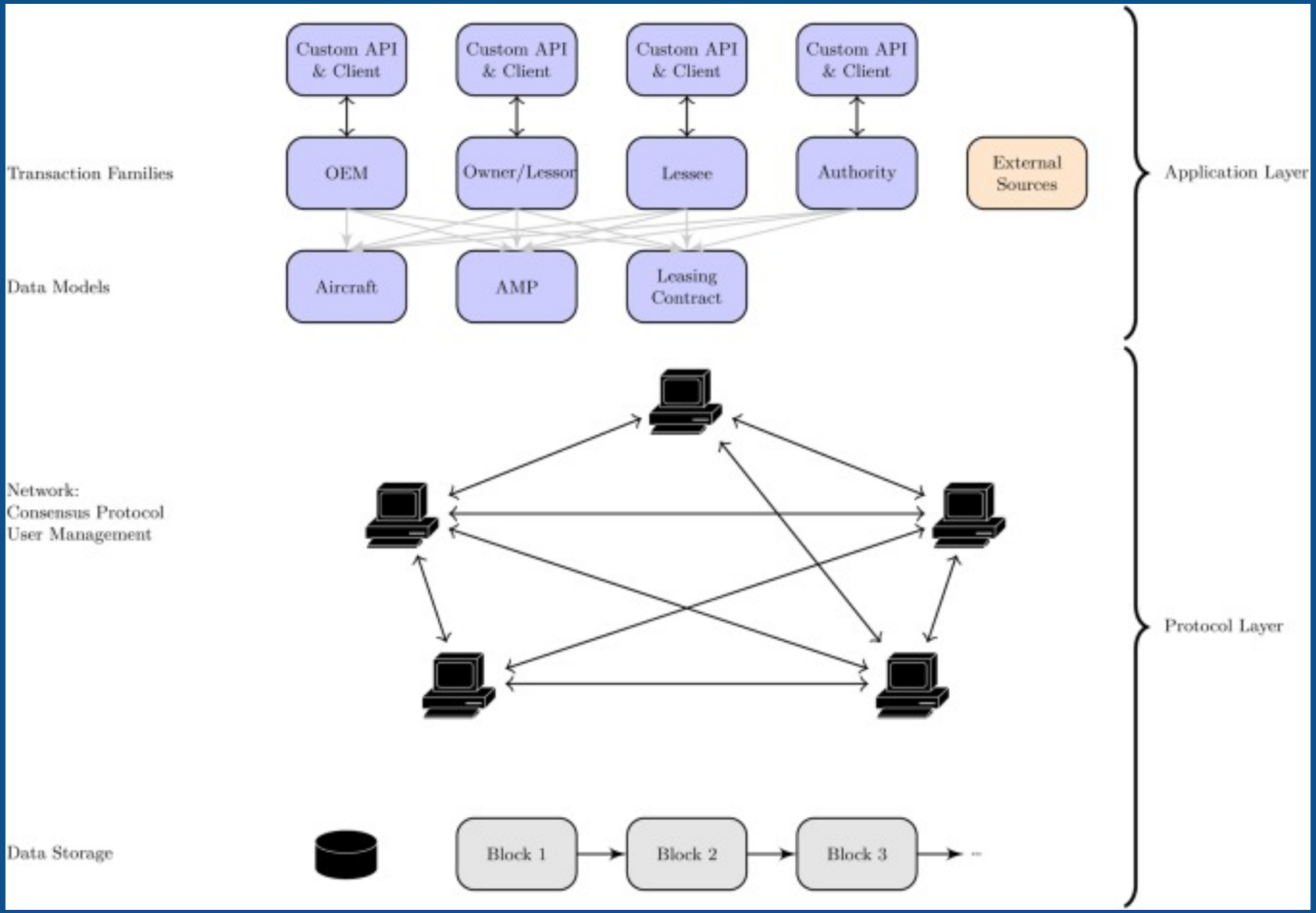
And, do you really need a blockchain?

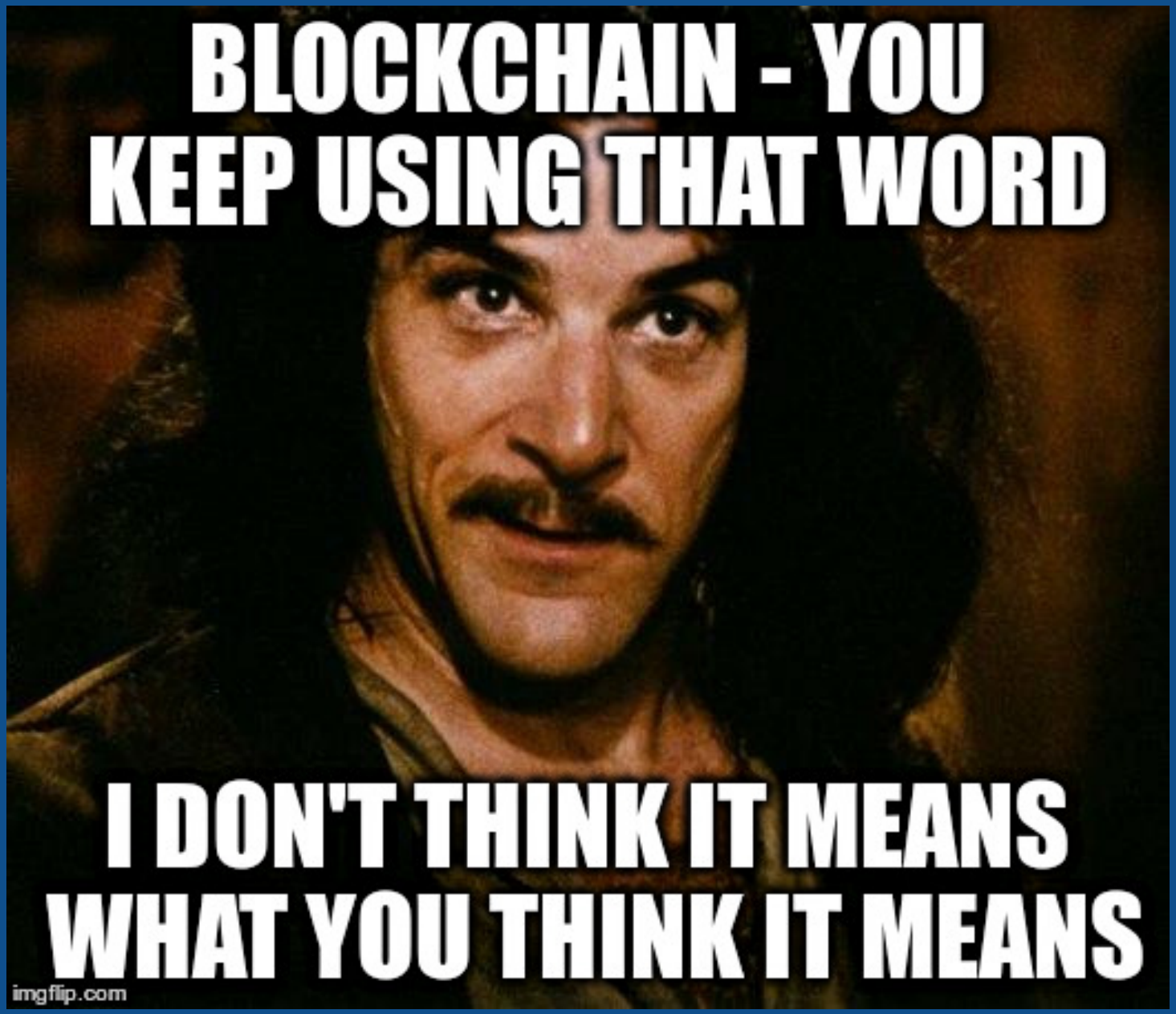


Paul Kuhle et al. (2021). “Building A blockchain-based decentralized digital asset management system for commercial aircraft leasing”. In: *Computers in Industry* 126, p. 103393. ISSN: 0166-3615


Stakeholder
Interest
Generic Process
Regulator
Compliance in Regulatory Environment per Lessee
OEM
Delivery Aircraft, Improve Aircraft/System Performance
CAMO
Ensure Aircraft's Technical Safety
MRO
Fulfill Contract with Lessee (Service Level)
Lessee/Operator
Asset Utilization, Compliance at Minimum Cost
Lessor
Risk Mitigation, Asset Value Depreciation, Transferability
AD Publication
SB Publication
Internal Planning
Internal Planning
Maintenance Event Planning
Maintenance Event
Operation
Delivery
Return Preparation
Return Preparation
Return Preparation
Operation
Redelivery
I
A
A
M
R
A
t
Initial Aircraft Delivery
Acceptance and Phase-in/Phase-out
Scheduled Maintenance Event
Return-to-Lessor Decision
Document Change
Document Delivery
Recurring events related to regulatory obligations
Value-generating activity of the lease agreement
"Return-to-Lessor" workflow
Lessor's involvement
Aircraft's Path


Leasing Contract
Operations
Maintenance
Documentation
Restrictions
Audits & Compliance
Risk
Insurance
IDERA
Deposits
Terms
Payments
Commitment Fee
Rent
Additional Rent
(Re-) Delivery
Documentation
Inspection
Conditions Precedent


Custom API & Client
Custom API & Client
Custom API & Client
Custom API & Client
Transaction Families
OEM
Owner/Lessor
Lessee
Authority
External Sources
Application Layer
Data Models
Aircraft
AMP
Leasing Contract
Network:
Consensus Protocol
User Management
Protocol Layer
Data Storage
Block 1
Block 2
Block 3


BLOCKCHAIN - YOU
KEEP USING THAT WORD
I DON'T THINK IT MEANS
WHAT YOU THINK IT MEANS
imgflip.com

IT ($\rightarrow$ 1994)	Internet years($\rightarrow$ 2015)	Blockchain promise
Data computation		
Database applications	Social interactions	Decentralization of trust
Transaction Processing	e-commerce	
Transaction Processing	Self pub-lishing	Value flow without In-termediaries
Business Intelligence	Personal commu-nications	
Global operations		

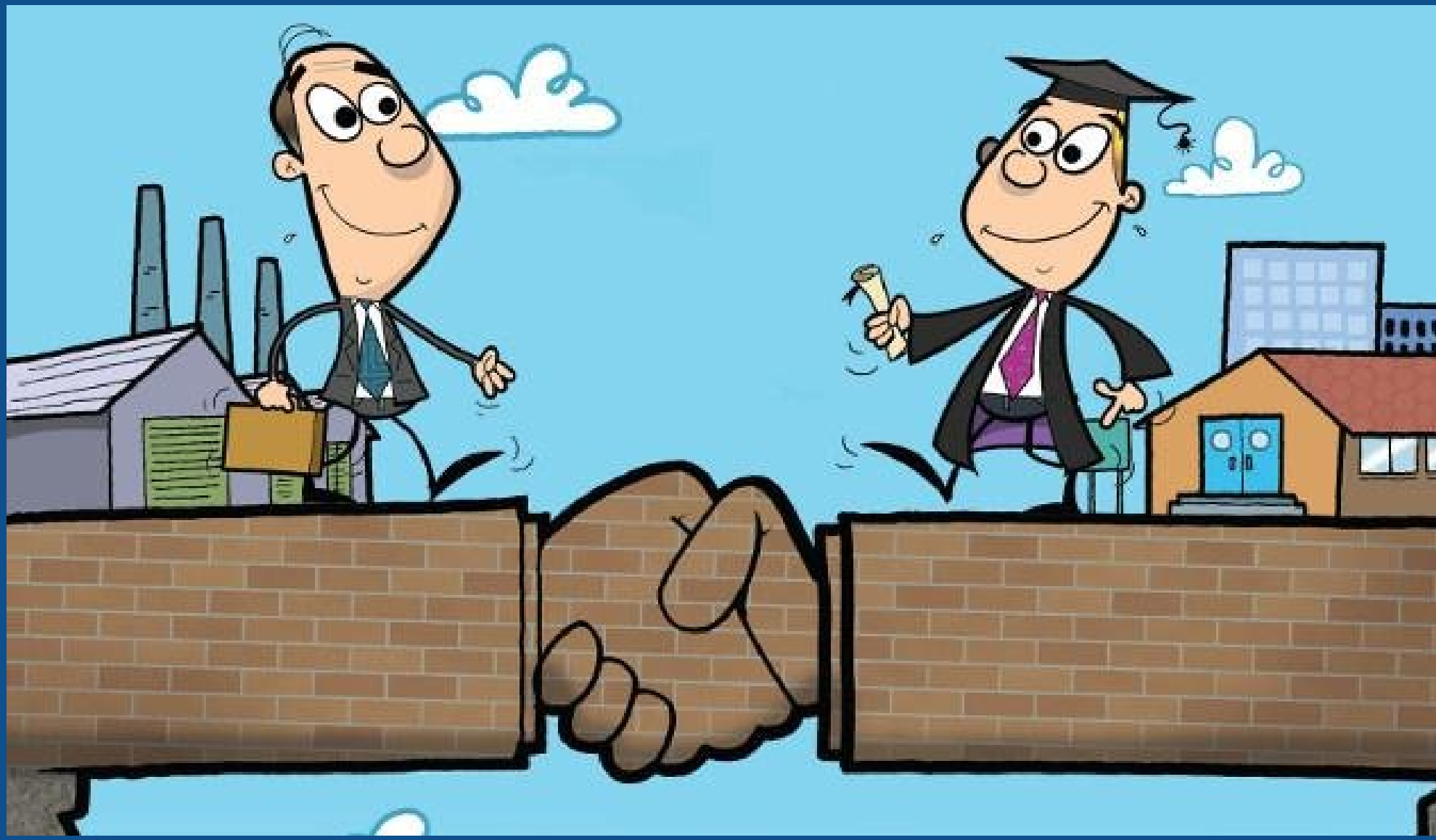
Pablo de Andrés et al. (2022). “Challenges of the market for initial coin offerings”. In: *International Review of Financial Analysis* 79, p. 101966. ISSN: 1057-5219

- Local data and open-source sofware: API to elude dependency (TRUST?) with respect to etherscan and Infura ($\rightarrow$ Amazon)
- ICOs ownership structure
- Portfolio management strategies
- New ERC for better governance of smart contracts
- Policy implications and industry prospects

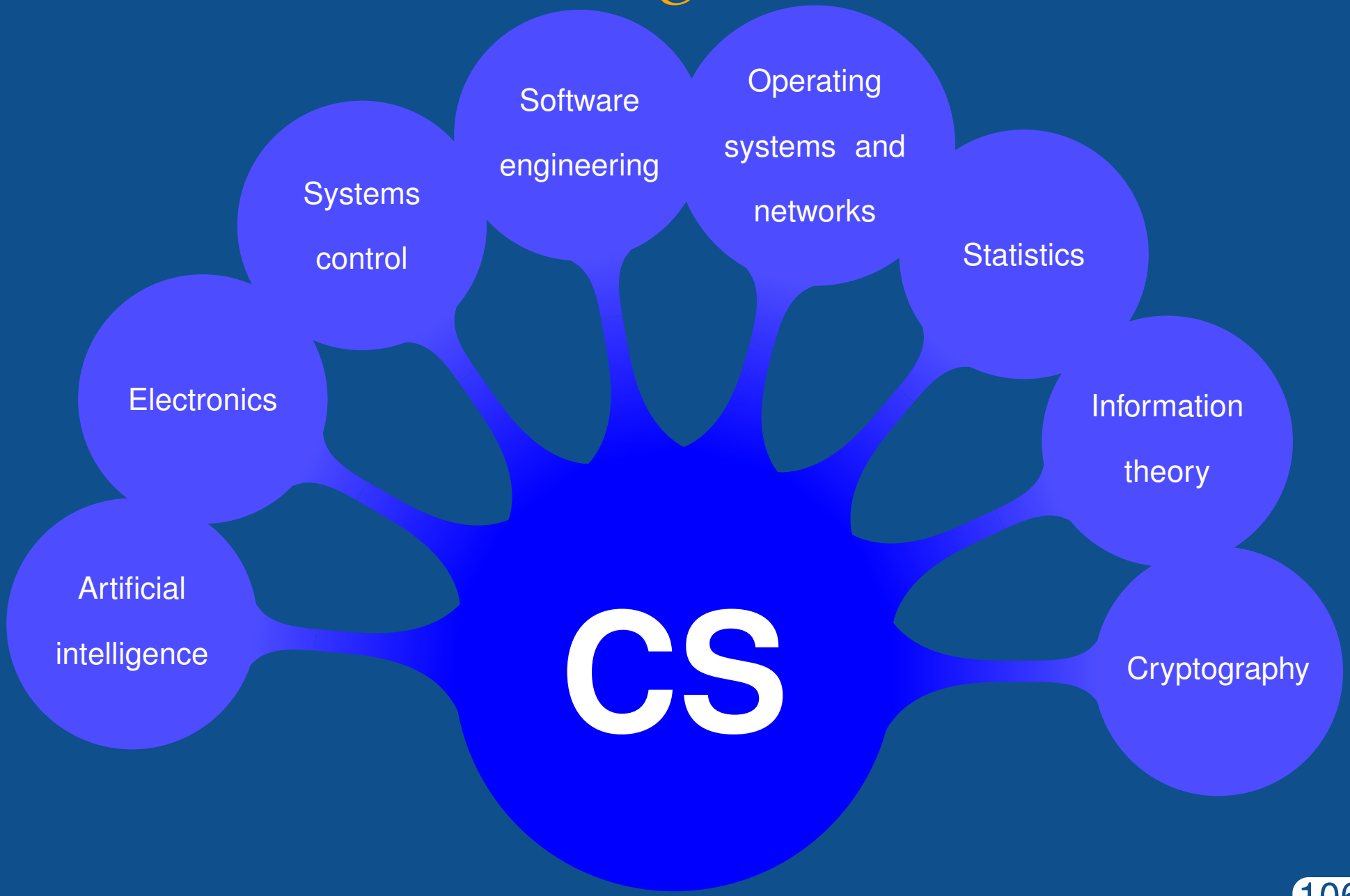
Conclusions

What I trust?

How can I build a network of trust?



Ciberseguridad:



THANKS!!!

https://dargcsic.github.io/

We are hiring

- Highly motivated candidate able to conduct research in the area of cryptographic privacy-enhancing technologies, security and blockchain-based protocols to join the H2020 SPIRS team in Madrid
- Design of a PETs Toolbox (T3.3) associated with a trusted execution environment designed by the team at University of Tampere
- Deployment of blockchain protocols (T3.5) to identify security threats and monitor overall system performance in a privacy repectful way
- Definition of the use cases specification and validation plan (T6.1) and to off-chain governance schemes and validation of privacy respectul protocols (T6.2)

Synergies between SPIRS and other GiCSI projects (⇒ CSIC projects)

cynamon

Blockchain protocols, PETs, PQC, security-by-default

Oracle: ORGANICALLY RESILIENT
AND SECURE WIRELESS NETWORKS FOR NEXT-GENERATION IOT TECHNOLO
TO SERVE FUTURE CONNECTED SOCIETIES (EIG Concert: Europe-Japan)

chanisms and Technologies for cybersecurity and privacy (P2QProMeTe)

⇒ CYBECO ICMAT INSTITUTO DE CIENCIAS MATEMÁTICAS

Colaboration with SMEs in the context of the deployment of eIDAS 2.0 (pending…)

ESSIF

European Self-Sovereign Identity Framework

CDTI

INICIATIVA neotec

GOBIERNO DE ESPAÑA

VICEPRESIDENCIA PRIMERA DEL GOBIERNO

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

Some references... I

de Andrés, Pablo, David Arroyo, Ricardo Correia, and Alvaro Rezola (2022). "Challenges of the market for initial coin offerings". In: *International Review of Financial Analysis* 79, p. 101966. ISSN: 1057-5219.

Diaz, Jesus, David Arroyo, and Francisco B Rodriguez (2017). "Fair anonymity for the Tor network". In: *The 14th International Conference on Security and Cryptography (SECRYPT 2017)*, Accepted as Position Paper. In Press.

— (2014). "New X.509-based mechanisms for fair anonymity management". In: *Computers & Security* 46, pp. 111–125.

Diaz, Jesus, Seung Geol Choi, David Arroyo, Angelos D Keromytis, Francisco B Rodriguez, and Moti Yung (2018). "Privacy in e-shopping transactions: Exploring and addressing the trade-offs". In: *International Symposium on Cyber Security Cryptography and Machine Learning*. Springer, pp. 206–226.

Díaz, Jesús, Seunggeol Choi, David Arroyo, Angelos D Keromytis, Francisco de Borja Rodríguez, and Moti Yung (2016). "Privacy Threats in E-Shopping (Position Paper)". In: *Lecture Notes in Computer Science*.

Kuhle, Paul, David Arroyo, and Eric Schuster (2021). "Building A blockchain-based decentralized digital asset management system for commercial aircraft leasing". In: *Computers in Industry* 126, p. 103393. ISSN: 0166-3615.

Querejeta-Azurmendi, Iñigo, David Arroyo Guardeño, Jorge L Hernández-Ardieta, and Luis Hernández Encinas (2020). "NetVote: A Strict-Coercion Resistance Re-Voting Based Internet Voting Scheme with Linear Filtering". In: *Mathematics* 8.9, p. 1618.

Some references... II

Sanchez-Gomez, Alejandro, Jesus Diaz, and David Arroyo (2017). “Encrypted Cloud: a software solution for the secure use of free-access cloud storage services”. In: *The 10th International Conference on Computational Intelligence in Security for Information Systems CISIS 2017*, Accepted. In Press.

Sanchez-Gomez, Alejandro, Jesus Diaz, Luis Hernández Encinas, and David Arroyo (2017). “Review of the Main Security Threats and Challenges in Free-Access Public Cloud Storage Servers”. In: *Computer and Network Security Essentials*. Ed. by K. Daimi. Vol. In Press. Studies in Computational Intelligence. Springer Berlin Heidelberg.

Strandburg, KatherineJ (2014). “Monitoring, Datafication and Consent: Legal Approaches to Privacy in a Big Data Context”. In: *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, p. 5.

Vacca, John R (2012). *Computer and information security handbook*. Newnes.

Westin, Alan F (1968). “Privacy and freedom”. In: *Washington and Lee Law Review* 25.1, p. 166.