cryptar

Establishing legal proof for data validity

Tim Schojohann

Data is the foundation of our digital future

but we lack legal protection for digital trust

Invalid VISA as extension process is simply delayed

Vaccination certificates purchasable via Telegram

World Bank Group „Ease of doing Business Report“ discontinued 2021

Commonly known realities

Paper processes are not scalable

Media breaches are being exploited

Data can be manipulated / mispresented

Digitalization is without alternative

while incentive to fake data scales across all sectors

Competing best practices with adoption blockers

Digital signatures (market: $4bln +28% CAGR)
- Only as trustworthy as key holder

-Timeline

Private blockchain (market: $7 bln +56% CAGR)
- Limited scalability and expensive maintainance

+ Operation$

Digital Identity / SSI (market: $8bln +16.7% CAGR)
- Focused on identity and data sharing within network

-Decentral

Public smart contracts (market: $149m +26% CAGR)
- Reliant on public community with limited experience

-Self-verification

Timestamping / hash-anchor (OpenSource)
- No version controls due to indefinite validity

-Control

Blockchain initatives die through complexity

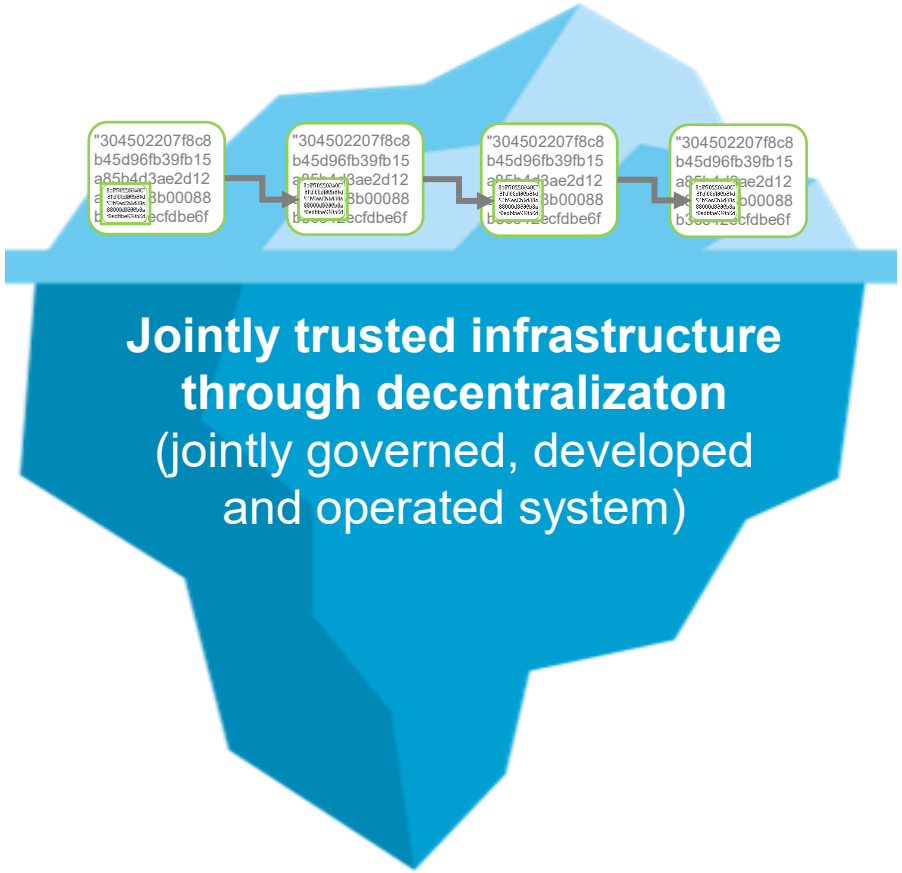
Projects fail to scale for positive return of investment

Complexity of requirements
(e.g. data formats, storage, throughput, latency, security, transparency, privacy, governance)

Complexity of interdependency
(e.g. change impact (OFAC ETH) or cost of innovation - investment vs. individual value chain)

Complexity of operations
(own skills & resources or trust in skills and intentions of operators)

Complexity of establishing trust
Trusted authorities and/or true decentralization needed for accepted immutability



cryptar

Blockchain simplified for data provenance

Focus on core feature: Immutable and self-verifiable data

Blockchain cryptography

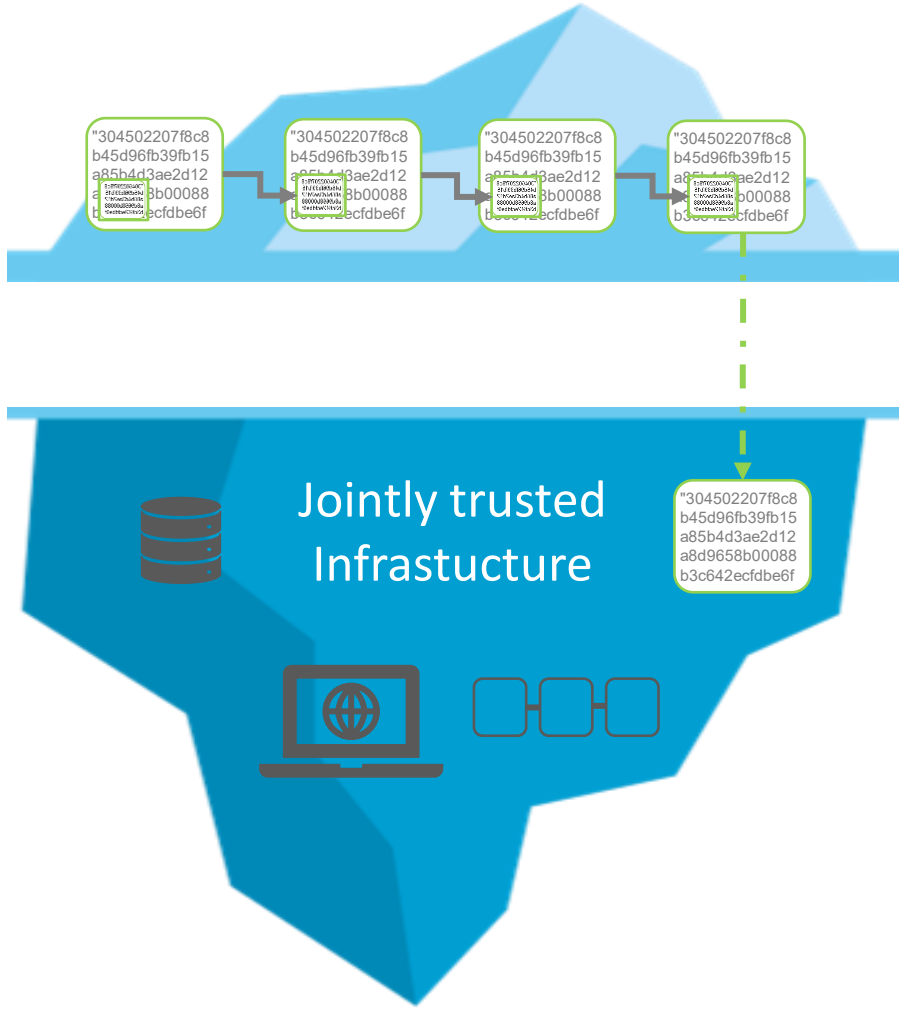
Secures data history in unchangable sequence as
Any single trusted block verifies all previous blocks

Why write all blocks in coordination with all stakeholders?

Blockchain infrastructure

Prevents data history to be rewritten by individual actor(s)

Why try to rebuild trust when there are already multiple trust-silos?



Combining best practices through Cryptar

to complement standards and overcome shortcomings

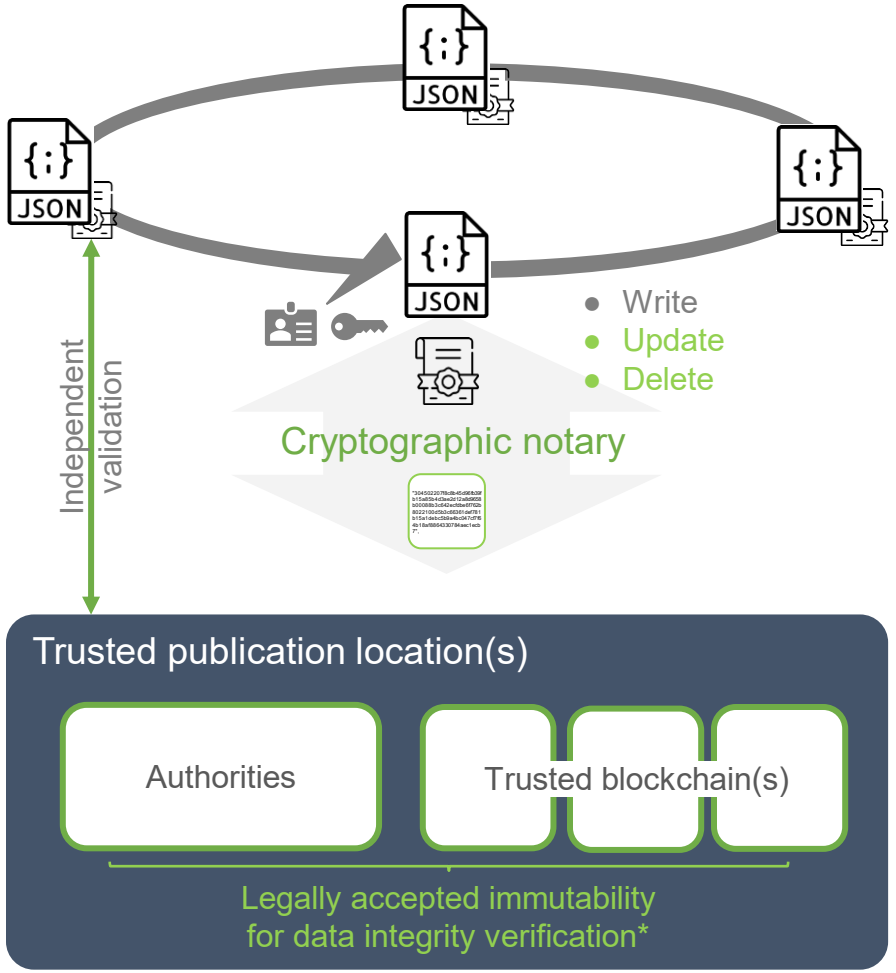
Run processes and data lifecycle as needed
- Preferred data management and sharing (incl. phygital)

Use established identity and signature standards
- Private key infrastructure / W3C etc. (incl. multi-signature)
- Adopt new standards as needed (IDUnion, eIDAS,..)

Integrate Cryptar (IaaS / OnPremise / Hybrid)
- Sign after writing, **updating and deleting** data
- Share signed fingerprints only

Leverage established legally trusted location(s)
- Authorities and blockchain (legal precedents established)
- Scalable and future-proof by adding / changing locations

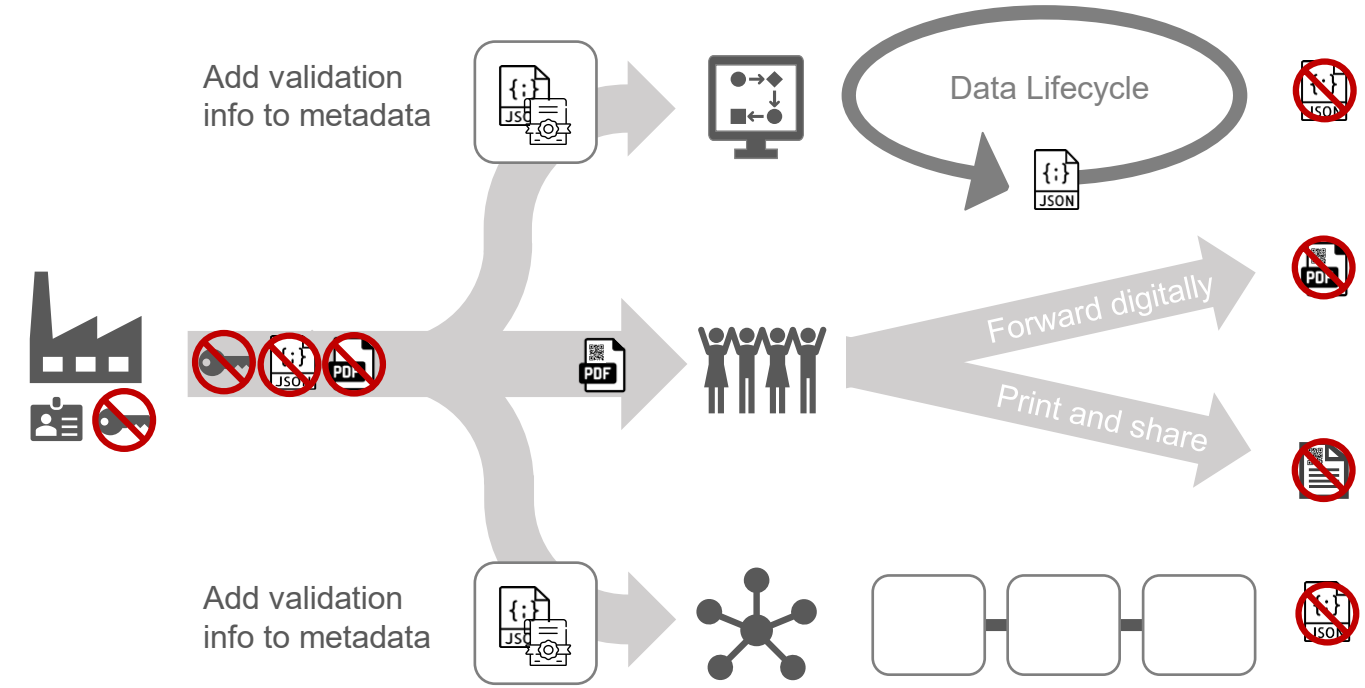
Maintain control while enabling verification
- Evidentially control signature validity after sharing
- Establish independently verifiable legal evidence



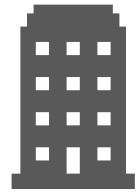
cryptar

Example: Trusting data in collaborations

Current best practice as dynamic as signatures



Inspect QR & metadata



Benefits:

- Signature ensures data integrity
- QR enables phygital
- Digital ID / Public key validates authenticity

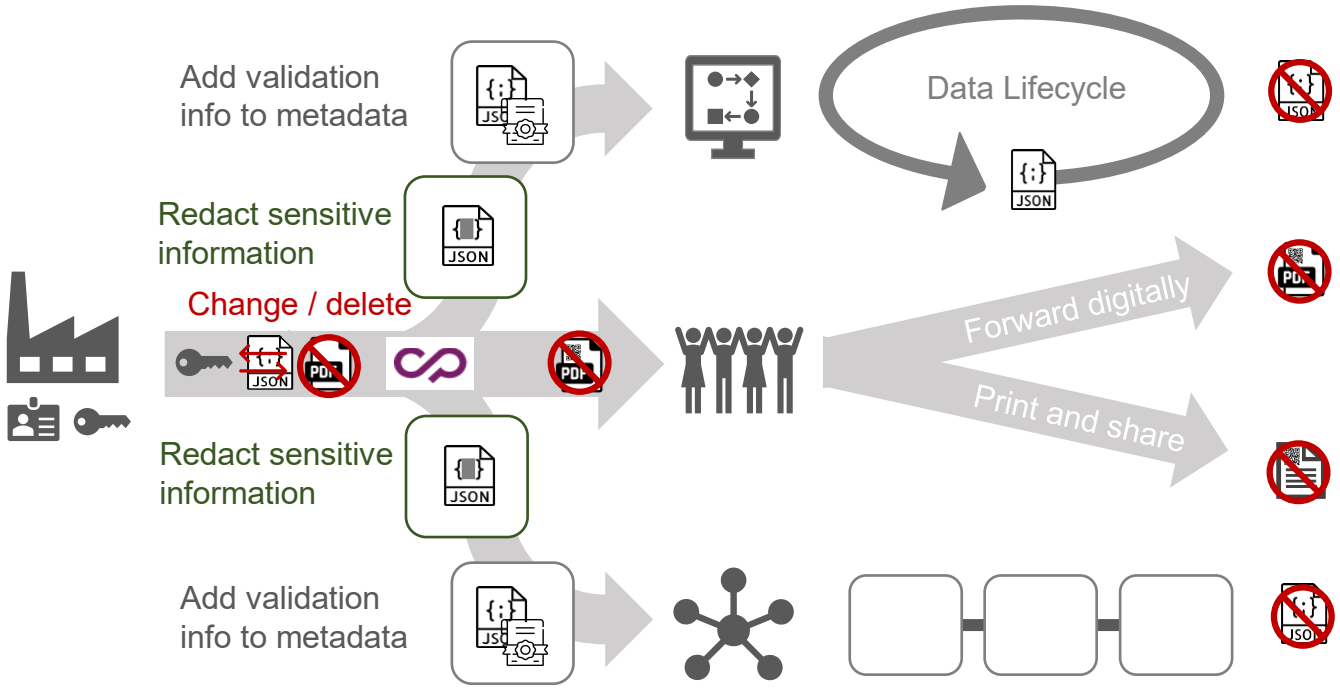
Shortcomings:

- Predetermed validity
- Unnoticed key theft
- No proof of timing

Digital ID

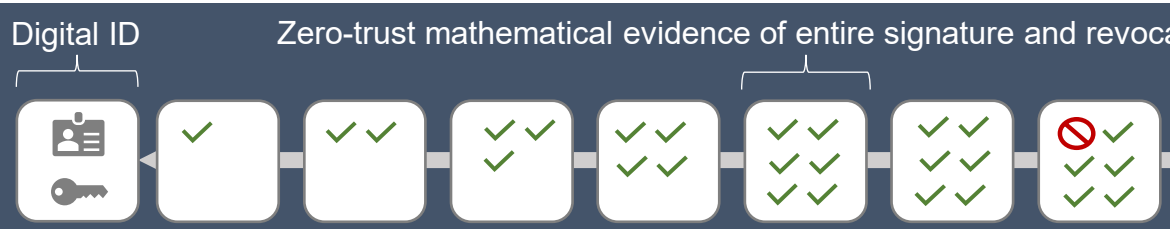
cryptar

Cryptar expands digital signatures
with advanced control for dynamic collaboration



Added benefits:
- Hide data maintaining verification integrity
- Control data validity after sharing
- Evidence of signature and revocation history

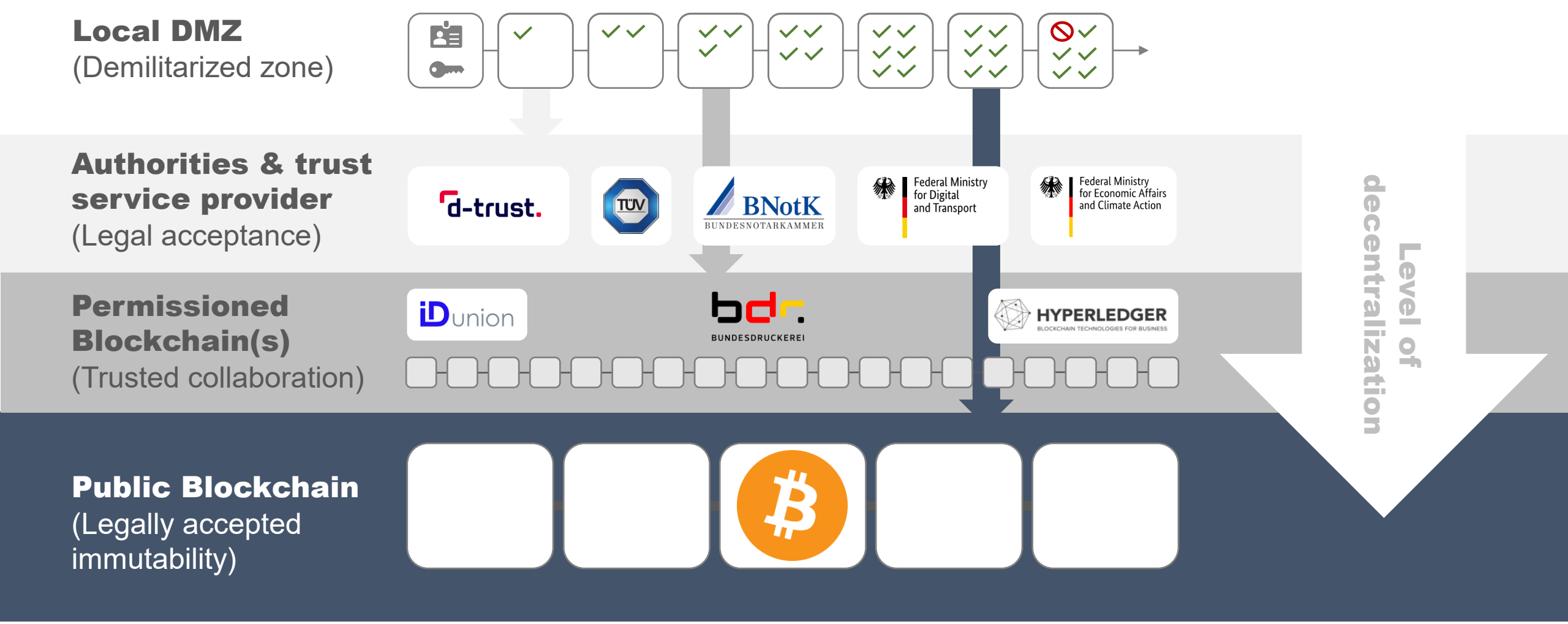
Extended benefits:
- Detect key abuse
- Legal evidence of data validity and timing
- Enable automated data cleanup

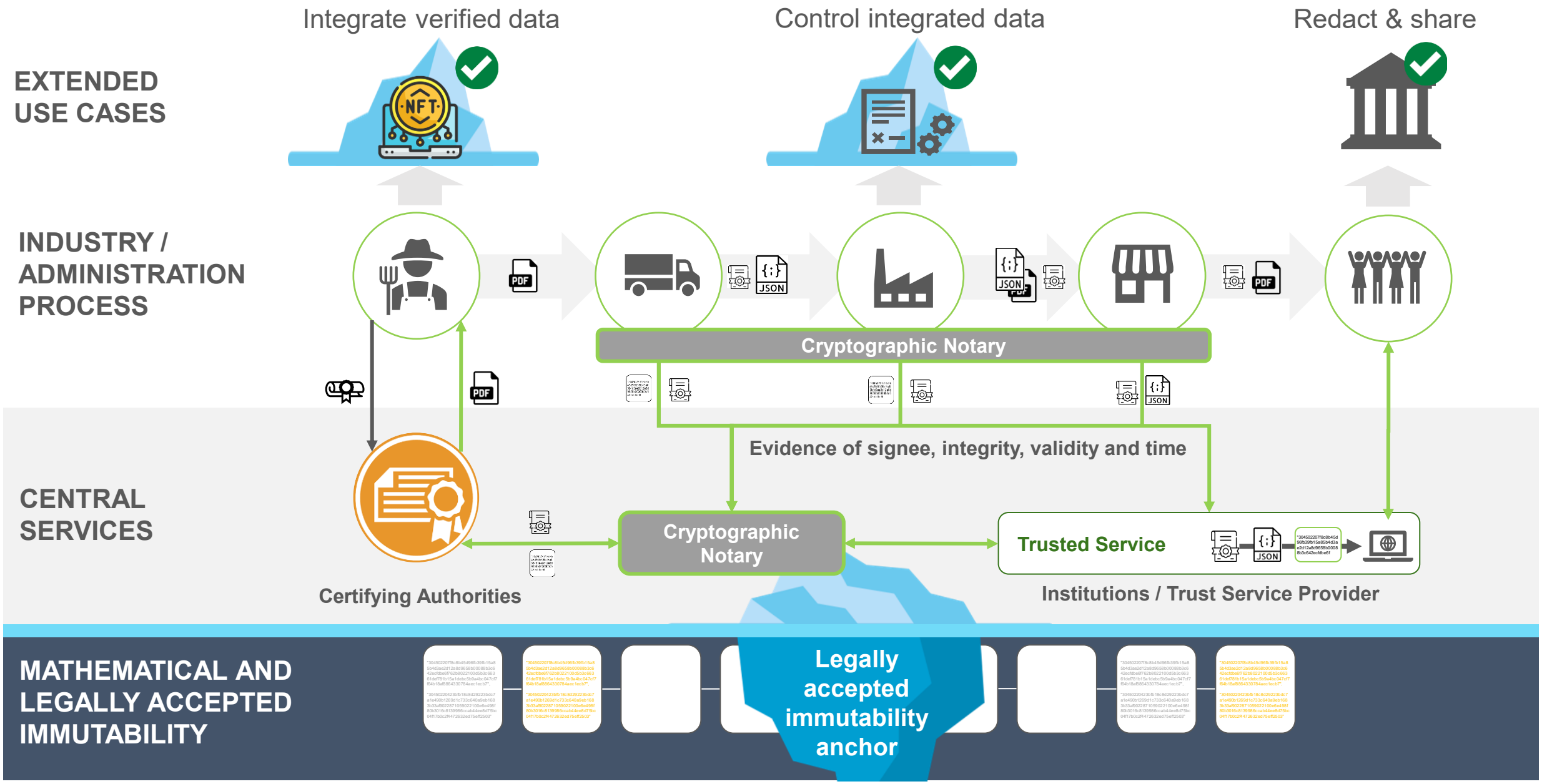


cryptar

Decentralize verification as per requirement

asynchronously publish across multiple trusted locations




Integrate verified data
Control integrated data
Redact & share
EXTENDED USE CASES
INDUSTRY / ADMINISTRATION PROCESS
CENTRAL SERVICES
MATHEMATICAL AND LEGALLY ACCEPTED IMMUTABILITY
NFT
PDF
JSON
Cryptographic Notary
Evidence of signee, integrity, validity and time
Cryptographic Notary
Trusted Service
Certifying Authorities
Institutions / Trust Service Provider
Legally accepted immutability anchor

cryptar

Cryptar expands digital trust beyond identities
by establishing legal evidence during digital interactions

Digital identity / signature

+Timeline

Mathematically verifiable data ~~integrity~~ validity
- When was data integrity verified?
- When (if ever) was data devalidated?

+Decentral

Trusted immutable signature history evidence
- Decentralize across blockchain(s) for ultimate security
- Include authorities where trust is centered already

- Operation$

Minimal complexity, alignment needs & costs
- Usage based subscription (Cloud / OnPremise)
- Zero-trust extension of new / existing processes

Enabling trusted collaboration

+Control

Maintain control as data owner
- Evidentially devalidate data after sharing
- Proactively detect signature abuse
- Minimize risk through must-know sharing

+Self-verification

Build trust as data recipient
- Prevent insecurity based on versioning / validity
- Protect input-data based actions with evidence
- Gain ability to proof authenticity to 3rd parties

+Scaleable

Scale processes across trust silos
- Low complexity for certifier and attester integration
- Add / change trusted locations with user needs

cryptar

cryptar

- Patent pending protocol (Europe & US)
- Bitflow GmbH spin-off as Cryptar planned
- Prototype ready - trial accounts in development
- Looking for concrete requirements of scalable use case for Go-Live

Mitglied INNOVATORS NET

Florian Weigand

→ M.Sc. Computer Science (TUM)
→ Formerly Foodora Lead Developer
→ Bitflow CEO focused on Technical Due Diligence

Tim Schojohann

→ BA International Business Management
→ ITILv3 & MIT Professional Blockchain certified
→ Formerly MongoDB Director of Partners Central Europe

Thank you

E-Mail: info@cryptar.de
Website: https://www.cryptar.de/

Office phone: +49 (0) 89 1250 1227 1

Office address:
Leopoldstr. 102
80802 Munich
Germany