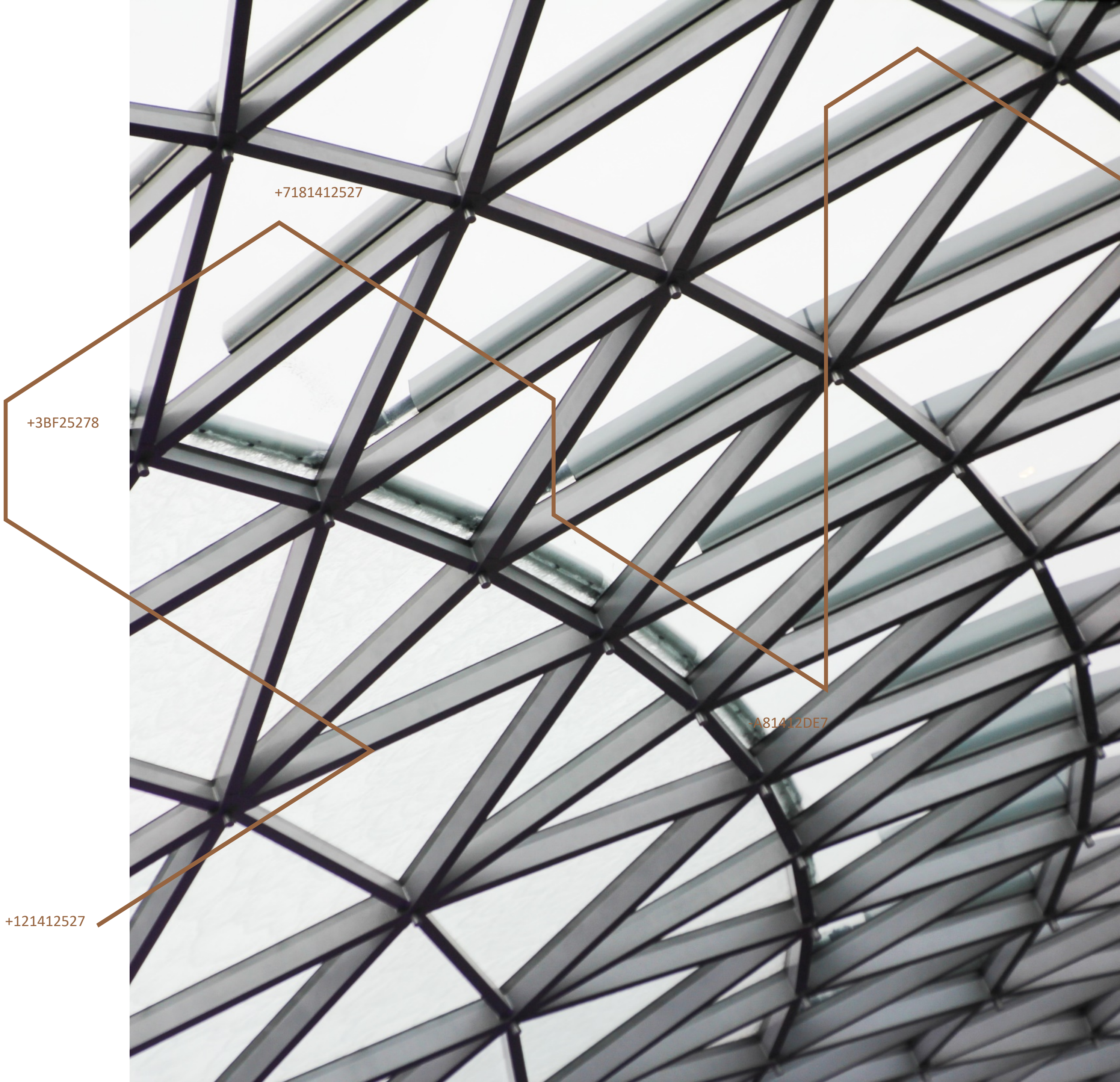
guardtime

# BLOCKCHAIN IN ESTONIA & PROJECT PRIVILEDGE H2020



INTRODUCTION

ANNA-MARIA OSULA, PHD

DECEMBER 2019

# ESTONIA

- Regained independence from Soviet Union in 1991
- 100% Electronic Banking
- 100% Electronic Health Care
- Over 3000+ Online Government Services using Blockchain
- Victim of a world's first coordinated attack against a State in 2007
- Headquarters of NATO Cooperative Cyber Defense since 2008

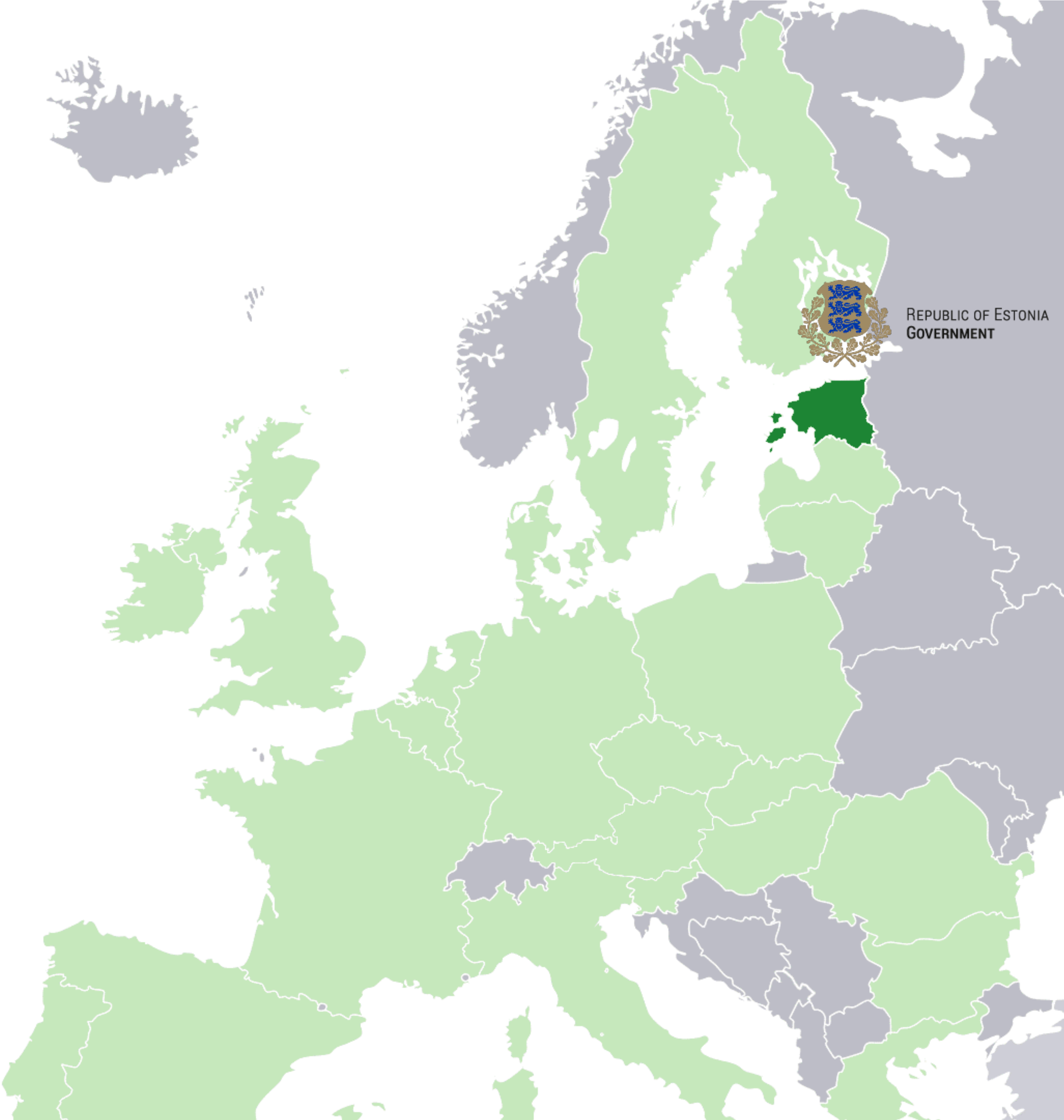
ESTONIA
NATO
CCDCOE
RUSSIAN
FEDERATION

# BLOCKCHAIN PIONEERS

- Estonia was the first country in the world to deploy blockchain technology

- Estonia uses blockchain technology for integrity verification of government registries and data

- Estonia uses KSI blockchain by Guardtime



# SECURE

## THE SAFEST COMBINATION.

### CONFIDENTIALITY

ID-card, Mobile-ID

Smart ID, e-Residency

### AVAILABILITY

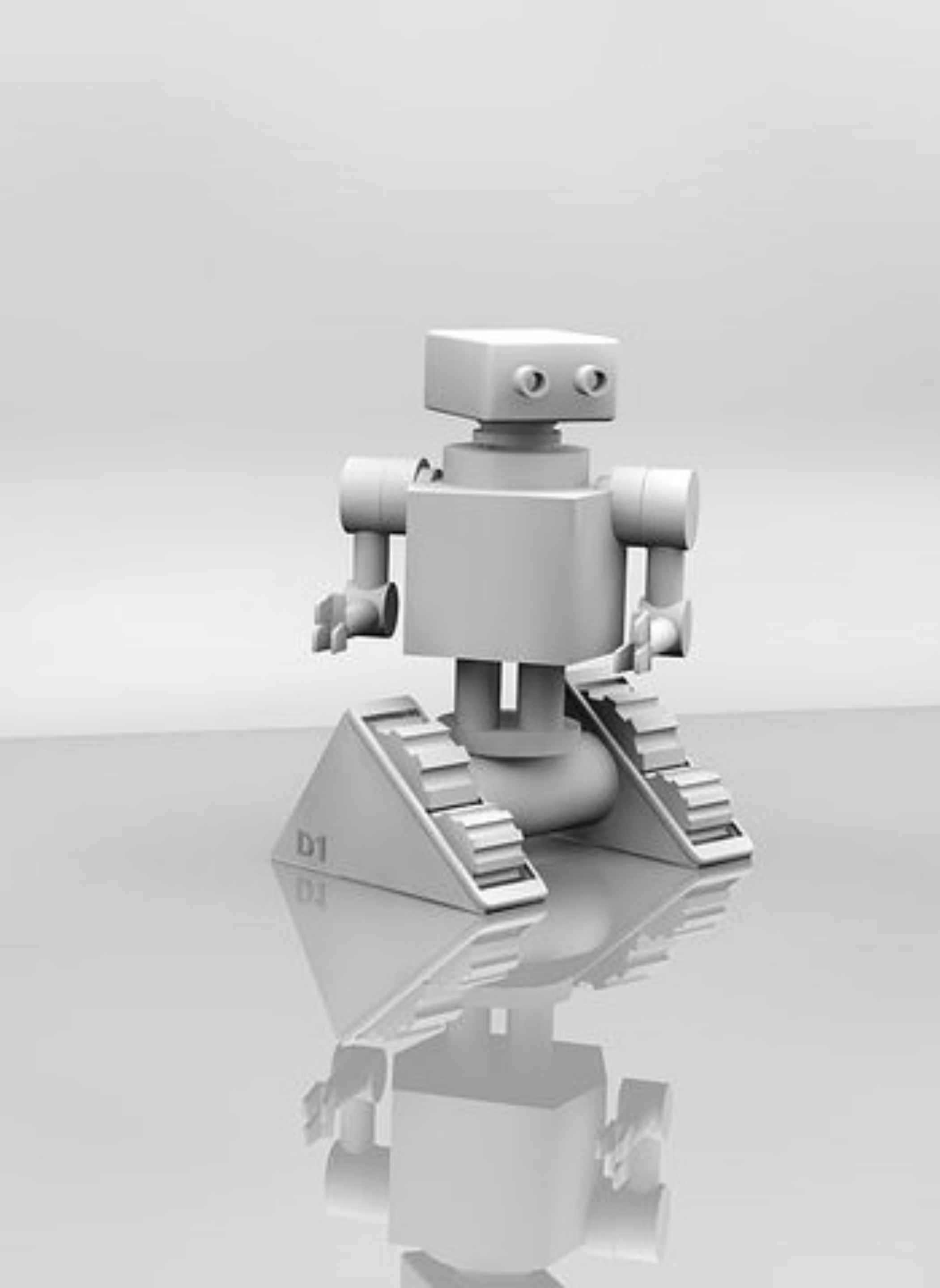
X- Road

### INTEGRITY

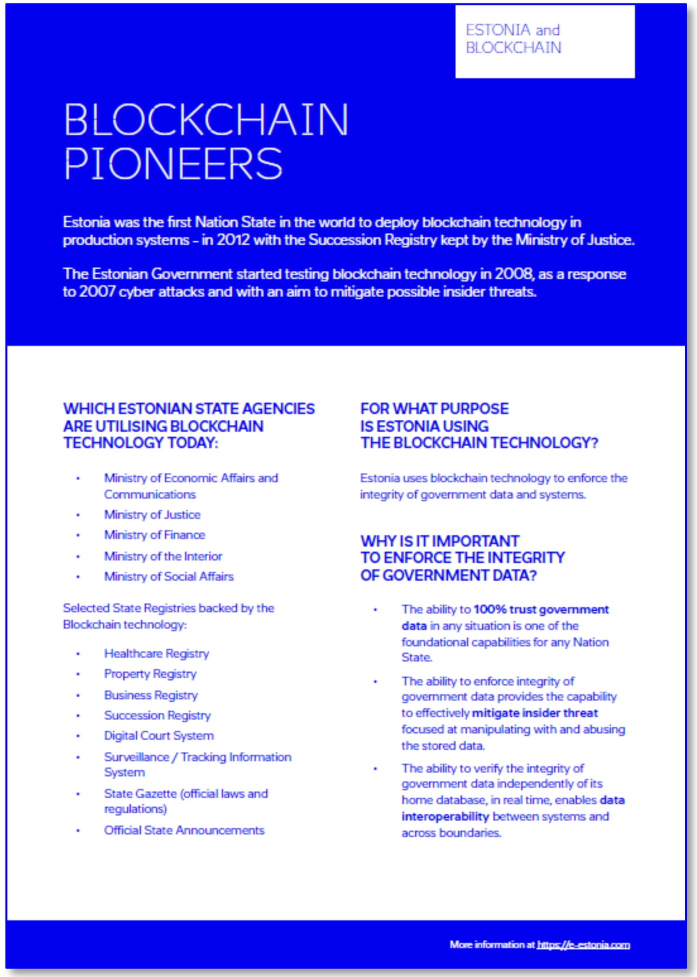
KSI Blockchain

# BLOCKCHAIN
## GUARDING THE INTEGRITY

- e-Health
- Property and Land Registry
- Business Registry
- Succession Registry
- e-Court
- Surveillance / Tracking Information System
- State Gazette
- Official State Announcements



# THE REFERENCE : ESTONIA



ESTONIA and BLOCKCHAIN

## BLOCKCHAIN PIONEERS

Estonia was the first Nation State in the world to deploy blockchain technology in production systems – in 2012 with the Succession Registry kept by the Ministry of Justice.

The Estonian Government started testing blockchain technology in 2008, as a response to 2007 cyber attacks and with an aim to mitigate possible insider threats.

### WHICH ESTONIAN STATE AGENCIES ARE UTILISING BLOCKCHAIN TECHNOLOGY TODAY:

- Ministry of Economic Affairs and Communications
- Ministry of Justice
- Ministry of Finance
- Ministry of the Interior
- Ministry of Social Affairs

Selected State Registries backed by the Blockchain technology:

- Healthcare Registry
- Property Registry
- Business Registry
- Succession Registry
- Digital Court System
- Surveillance / Tracking Information System
- State Gazette (official laws and regulations)
- Official State Announcements

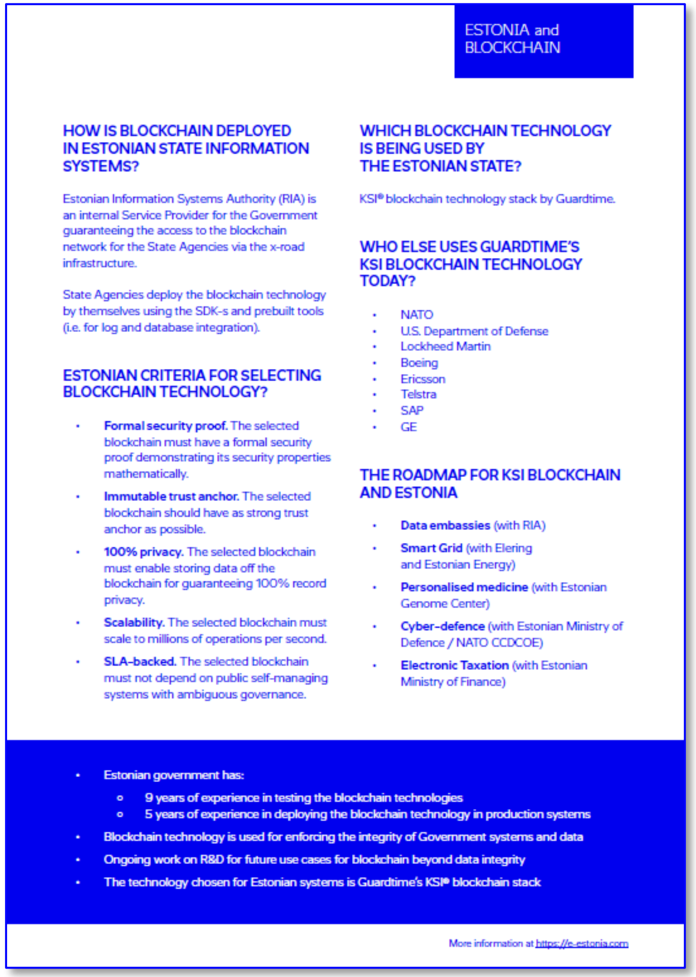
### FOR WHAT PURPOSE IS ESTONIA USING THE BLOCKCHAIN TECHNOLOGY?

Estonia uses blockchain technology to enforce the integrity of government data and systems.

### WHY IS IT IMPORTANT TO ENFORCE THE INTEGRITY OF GOVERNMENT DATA?

- The ability to **100% trust government data** in any situation is one of the foundational capabilities for any Nation State.
- The ability to enforce integrity of government data provides the capability to effectively **mitigate insider threat** focused at manipulating with and abusing the stored data.
- The ability to verify the integrity of government data independently of its home database, in real time, enables **data interoperability** between systems and across boundaries.

More information at https://e-estonia.com



ESTONIA and BLOCKCHAIN

### HOW IS BLOCKCHAIN DEPLOYED IN ESTONIAN STATE INFORMATION SYSTEMS?

Estonian Information Systems Authority (RIA) is an internal Service Provider for the Government guaranteeing the access to the blockchain network for the State Agencies via the x-road infrastructure.

State Agencies deploy the blockchain technology by themselves using the SDK-s and prebuilt tools (i.e. for log and database integration).

### ESTONIAN CRITERIA FOR SELECTING BLOCKCHAIN TECHNOLOGY?

- **Formal security proof.** The selected blockchain must have a formal security proof demonstrating its security properties mathematically.
- **Immutable trust anchor.** The selected blockchain should have as strong trust anchor as possible.
- **100% privacy.** The selected blockchain must enable storing data off the blockchain for guaranteeing 100% record privacy.
- **Scalability.** The selected blockchain must scale to millions of operations per second.
- **SLA-backed.** The selected blockchain must not depend on public self-managing systems with ambiguous governance.

### WHICH BLOCKCHAIN TECHNOLOGY IS BEING USED BY THE ESTONIAN STATE?

KSI® blockchain technology stack by Guardtime.

### WHO ELSE USES GUARDTIME'S KSI BLOCKCHAIN TECHNOLOGY TODAY?

- NATO
- U.S. Department of Defense
- Lockheed Martin
- Boeing
- Ericsson
- Telstra
- SAP
- GE

### THE ROADMAP FOR KSI BLOCKCHAIN AND ESTONIA

- **Data embassies** (with RIA)
- **Smart Grid** (with Elering and Estonian Energy)
- **Personalised medicine** (with Estonian Genome Center)
- **Cyber-defence** (with Estonian Ministry of Defence / NATO CCDCOE)
- **Electronic Taxation** (with Estonian Ministry of Finance)

- Estonian government has:
  - 9 years of experience in testing the blockchain technologies
  - 5 years of experience in deploying the blockchain technology in production systems
- Blockchain technology is used for enforcing the integrity of Government systems and data
- Ongoing work on R&D for future use cases for blockchain beyond data integrity
- The technology chosen for Estonian systems is Guardtime's KSI® blockchain stack

More information at https://e-estonia.com

This paper has been published by the Government of Estonia, to explain the history, the WHY, the HOW and the WHAT of Blockchain in e-Estonia since 2008

https://bit.ly/2BJqBuX

# HOW THE KSI BLOCKCHAIN IS DEPLOYED IN ESTONIA

## HOW IS BLOCKCHAIN DEPLOYED IN ESTONIAN STATE INFORMATION SYSTEMS?

+ Estonian Information Systems Authority (RIA) is an internal Service Provider for the Government guaranteeing the access to the blockchain network for the State Agencies via the x-road infrastructure.
+ State Agencies deploy the blockchain technology by themselves using the SDK-s and prebuilt tools (i.e for log and database integration).

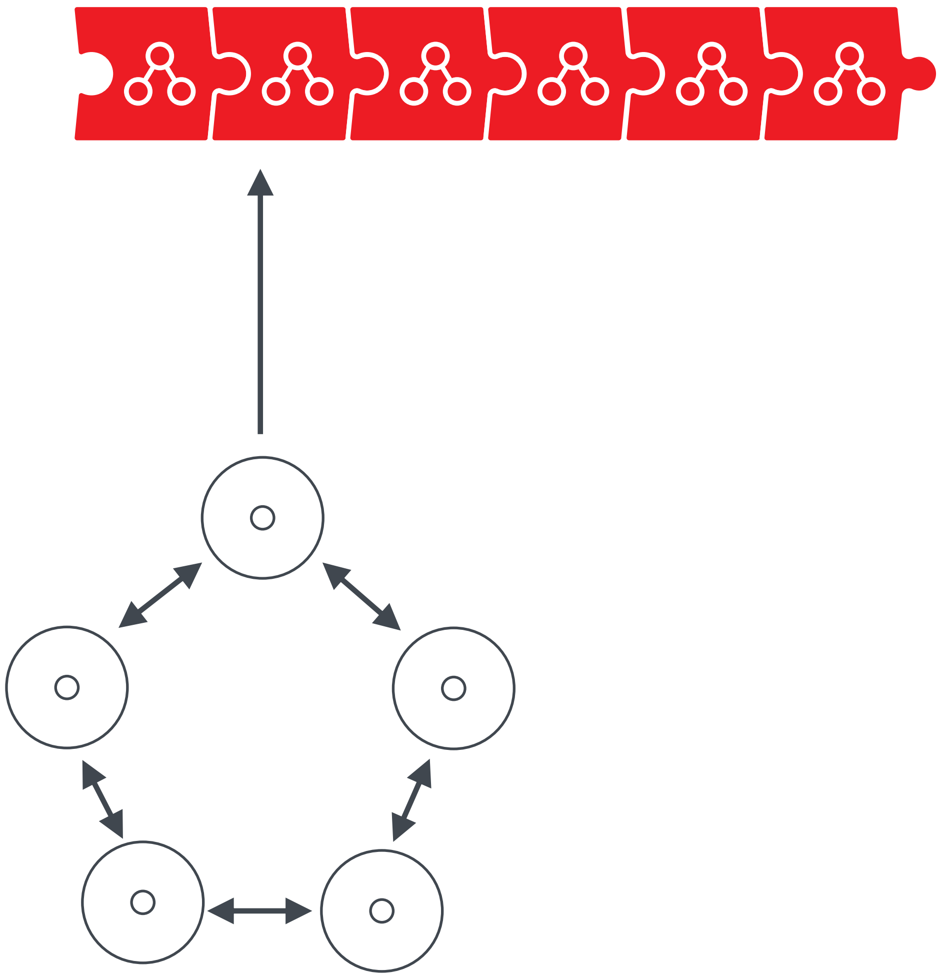
The Estonian Government (through its RIA Agency) is today totally autonomous in connecting the KSI Blockchain to all its Public services.

This is the result of 10 years of collaboration and technology transfer between Guardtime and RIA.

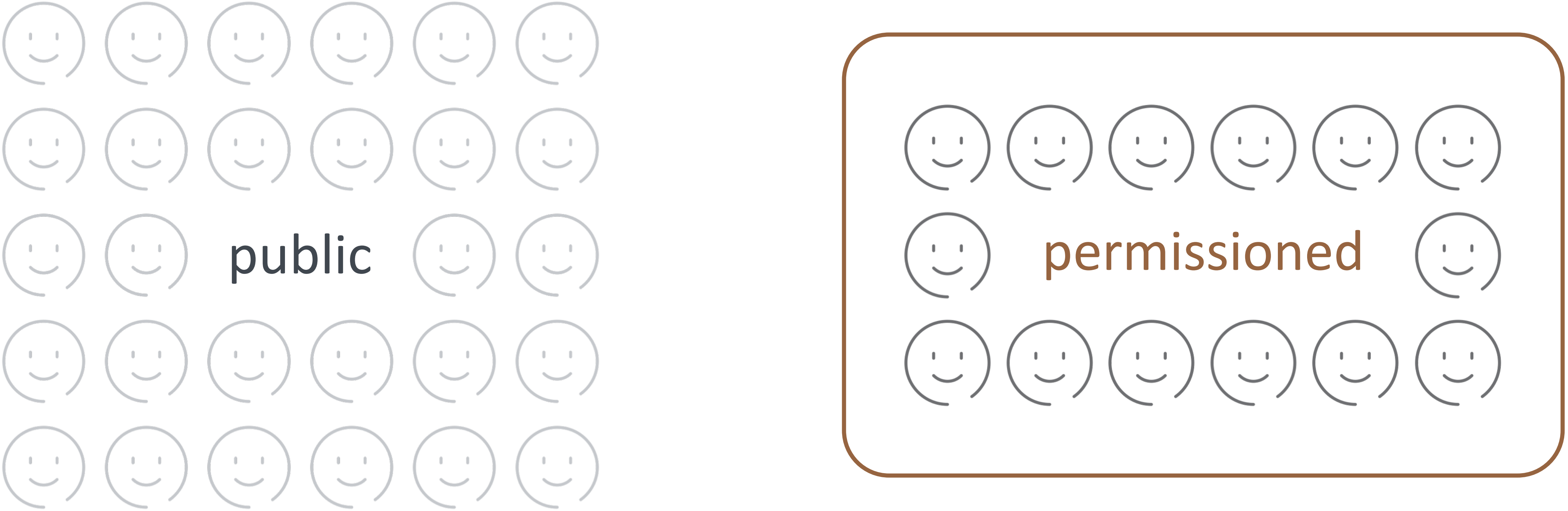
# BLOCKCHAIN – DISINTERMEDIATED TRUST MACHINE

BLOCKCHAIN is a distributed database that maintains a continuously growing list of data records, chained together against revision and tampering.

DISTRIBUTED CONSENSUS is an agreement between different compute-nodes over what is a true or false record.



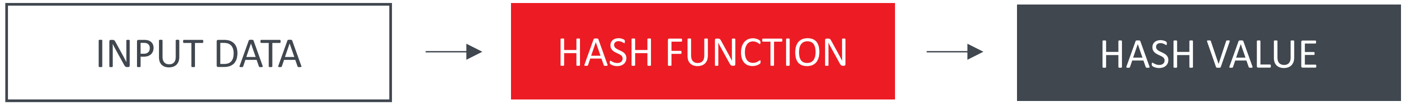
# GOVERNANCE



# CRYPTOGRAPHIC HASH FUNCTIONS

## HASH VALUE IS THE DIGITAL FINGERPRINT OF THE INPUT DATA.

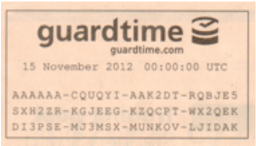
A hash function takes arbitrarily-sized data as input and generates a unique fixed-size bit sequence as output.



INPUT DATA → HASH FUNCTION → HASH VALUE

ONE-WAY ONLY.
REVERSING IMPOSSIBLE

# KSI BLOCKCHAIN HIGHLIGHTS



guardtime
guardtime.com
15 November 2012 00:00:00 UTC

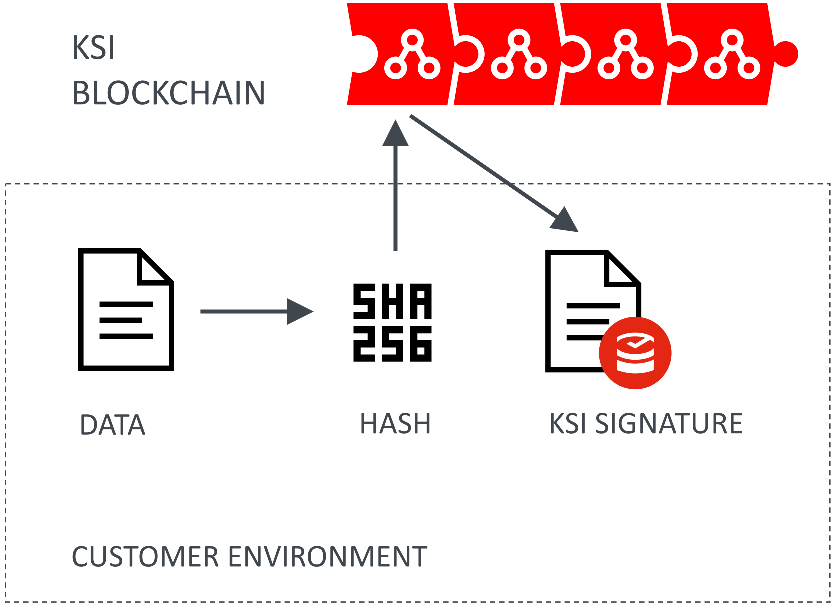
AAAAAA-CQUQYI-AAK2DT-RQBJE5
SXH2ZR-KGJEEG-KZQCPT-WX2QEK
DI3PSE-MJ3MSX-MUNKOV-LJIDAK

Signature platform – customer sends asset's hash, receives a token which proves participation in the blockchain.

Data NEVER leaves customer premises (only hash is sent to KSI service) – privacy guaranteed!

## KSI Signature proves:

- Asset Integrity
- Signing Time
- Signing Entity



## KSI Blockchain Benefits:

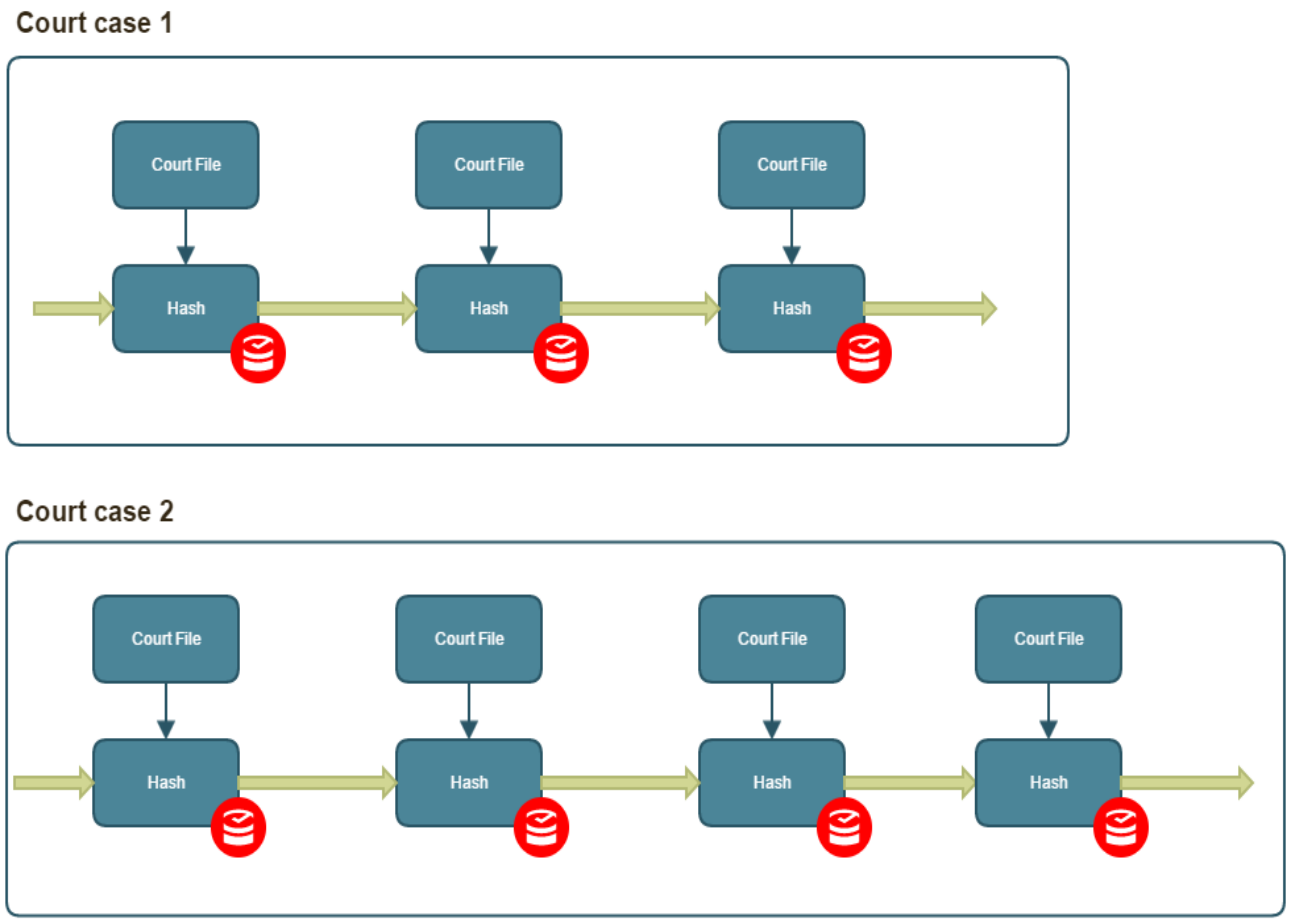
- Signatures independently verifiable by any 3rd party
- Do not expire, provide long-term forensic proof
- Overcomes technical limitation of other blockchain technologies (commitment time, scalability etc)

# CASE STUDY: DIGITAL COURT FILES

REPUBLIC OF ESTONIA
GOVERNMENT

All documents produced in courts of Estonia are hashed, chained and signed with KSI.

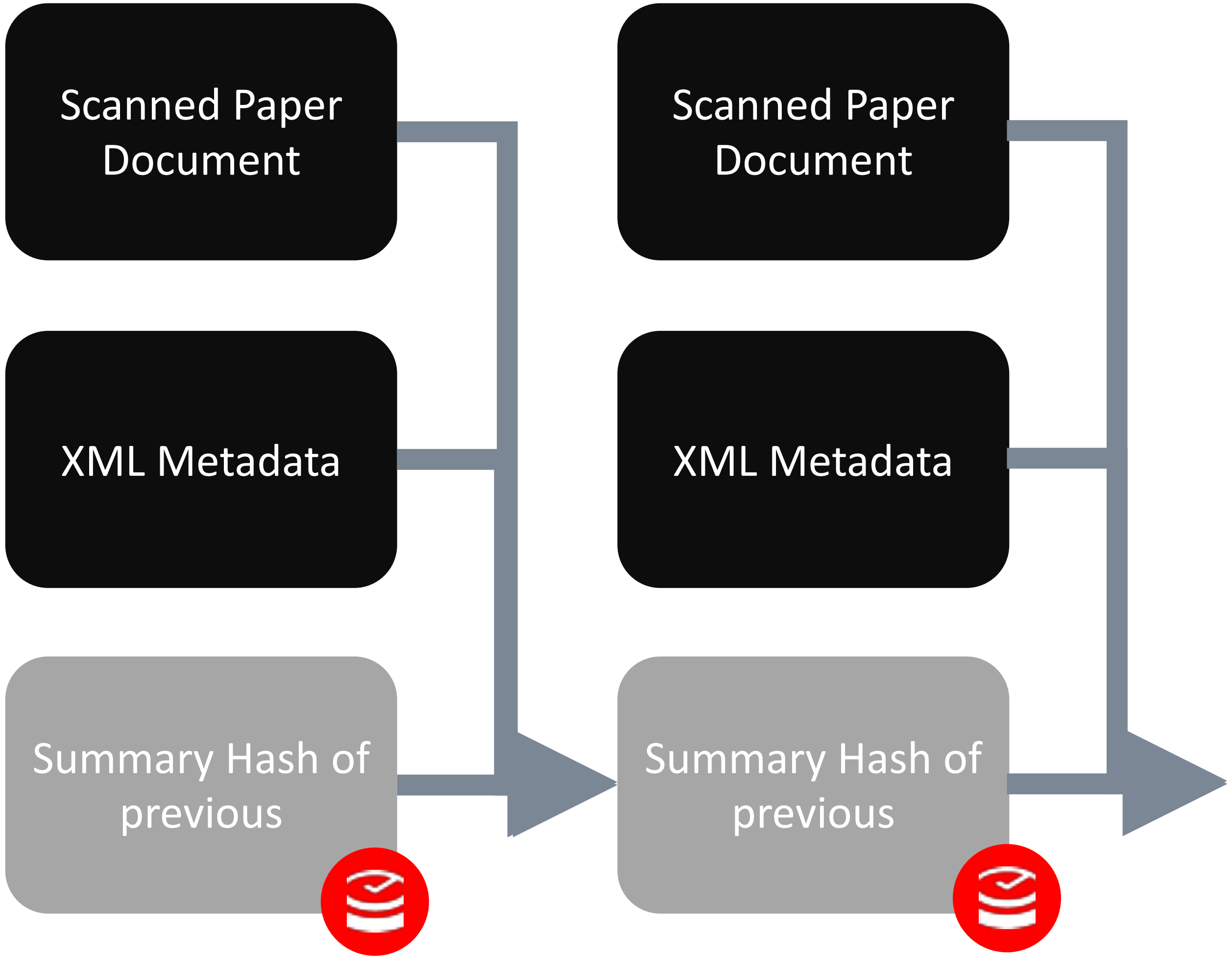
+ Guaranteed Integrity
+ Transparently auditable
+ Impossible to delete  a record undetectably
+ Legally sound



# CASE STUDY: ESTONIAN SUCCESSION REGISTRY

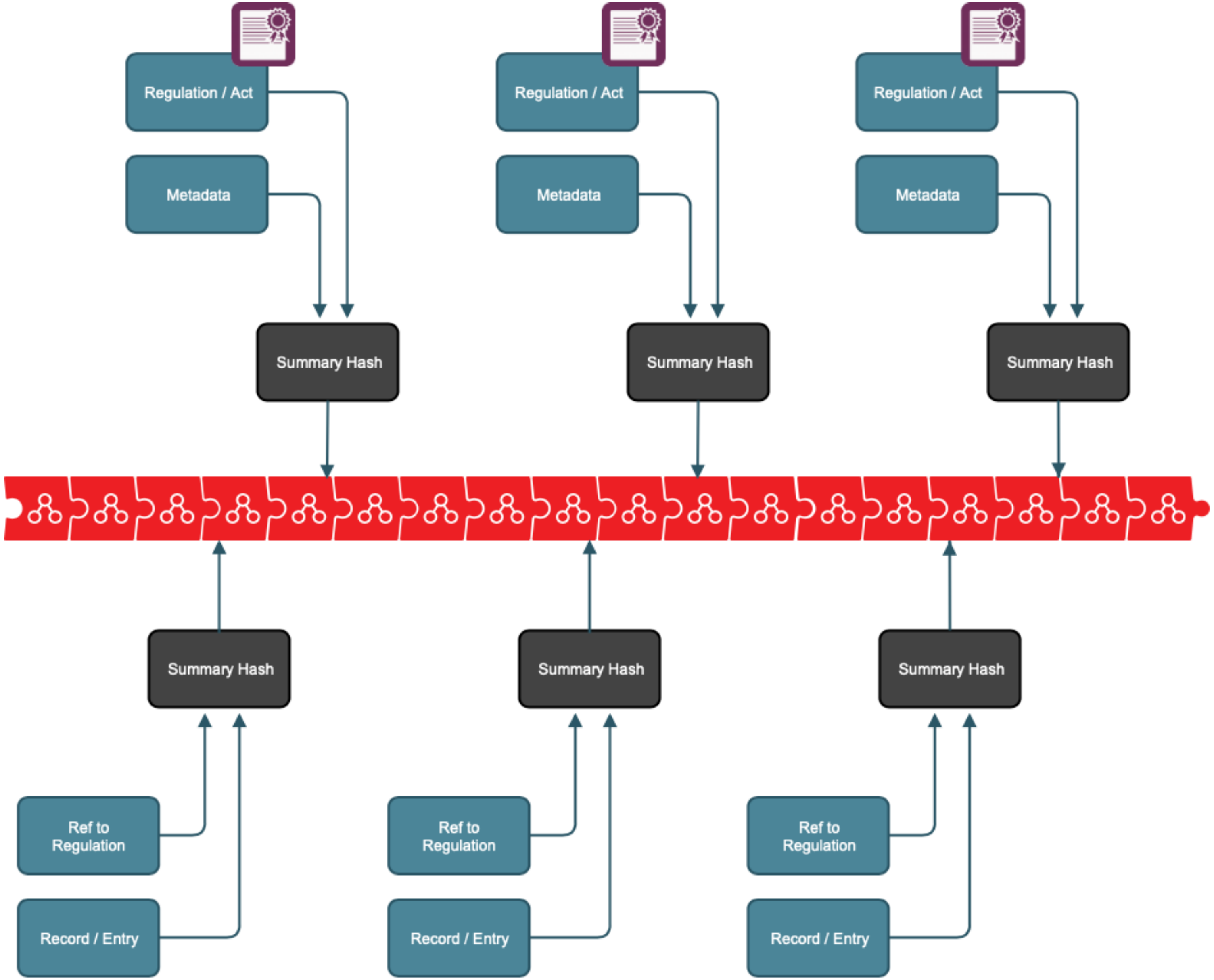
Records and associated metadata are chained to the previous record, signed and stored in a database.

- Provable ordering
- Impossible to delete a record undetectably
- Metadata provides attribution and government transparency
- Monitored and verified in real-time



# /ESTONIA
# PROPERTY REGISTER

- All legal acts and changes to property / land ownership / usage rights registered on KSI Blockchain.
- When records are altered, they are re-signed, creating an auditable record of process
- Ongoing checking of records to ensure integrity



# BLOCKCHAIN FOR INTEGRITY ASSURANCE

- IMMUTABILITY
- PRIVACY
- PERFORMANCE
- SCALABILITY

- CLEAR GOVERNANCE
- INDEPENDENT PROOF VALUE

CONCLUSION: REALLY POWERFUL **TOOL** – IF APPLIED CORRECTLY

# PRIVILEDGE

The aim of PRIViLEDGE is to develop and advance techniques that enhance privacy, anonymity and efficient decentralised consensus for distributed ledgers technologies.

https://priviledge-project.eu/

# PRIVILEDGE PROJECT

| | | | |
|---|---|---|---|
| guardtime | 🇪🇪🏆 | University of Salerno | IT |
| IBM Research | 🇨🇭🛠️ | grnet | 🇬🇷 |
| UNIVERSITY OF TARTU | 🇪🇪 | THE UNIVERSITY of EDINBURGH | 🇬🇧 |
| TU/e Technische Universiteit<br>Eindhoven<br>University of Technology | 🇳🇱 | GUnet | 🇬🇷 |
| SMARTMATIC CYBERNETICA<br>Centre of Excellence for Internet Voting OÜ | 🇪🇪 | INPUT \| OUTPUT | 🇨🇾 |

# PRIVILEDGE OBJECTIVES

- EFFICIENT PRIVACY-ENHANCING CRYPTOGRAPHY
  for blockchains, such that the privacy of users and data is respected

- CRYPTOGRAPHIC TOOLS
  that aim at anonymity, transparency, and security for practical deployments of DLT and blockchains

- EFFICIENT CRYPTOGRAPHIC CONSENSUS PROTOCOLS
  that satisfy verifiability, transparency, and stake-based governance

- EFFECTIVE EXPLOITATION in real operational environments, for enabling privacy in distributed ledgers

# USE-CASES

UC1: VERIFIABLE ONLINE VOTING WITH LEDGERS (SCCEIV)

UC2: DISTRIBUTED LEDGER FOR MEDICAL INSURANCE (GT)

UC3: UNIVERSITY DIPLOMA RECORD LEDGER (GRNET/GUNET)

UC4: CARDANO STAKE-BASED LEDGER (IOHK)

# UC1: VOTING

**The Challenge of Online Voting**: to find the balance between being transparent about achieving integrity while preserving confidentiality

- Election organisers must gain a capability to provide independent auditors with data to confidently **verify an integrity of an election result**
- These audits **must not undermine voter privacy** even in the future

The main objective of UC1 is to implement a **prototype of an online voting system** using the distributed ledger technologies for achieving the integrity and transparency targets under the condition of a secret ballot

# UC2: MEDICAL INSURANCE

+ Interest to shift from **activity-based costin**g to **outcome-based costing**
+ Need to **share patient records** between stakeholders
+ Need to report on care outcomes to insurers
+ But **without compromising privacy** of patient records

# UC3: E-DIPLOMAS

- Diploma certification is **bureaucratic and vulnerable to fraud**
- The diploma certification workflow will use a distributed ledger to record the steps
- Universities will run the nodes of the ledger
- Fake diplomas **will not be possible** (unless 50%+1 of the nodes are subverted)
- Diplomas will be **certified** so that only a designated verifier will be able to verify the proof attesting a credential (privacy-preserving certifiable credentials)
- GRNET and GUNET will cooperate in this use case, leveraging on the approaches and the protocols developed in WP2 & WP3

# CARDANO STAKE-BASED LEDGER

- Software updates (bugs, change requests, protocol enhancements, etc.) are **inevitable**
- The traditional way of handling software updates **is neither decentralised nor secure**
- We need a **solid framework** for a decentralised, consensus-based, cryptographically secure and transparent software update system

- UC4 will provide the answers in close collaboration with academic partner UEDIN
- Research results will be incorporated in the implementation of a prototype update system for the **Cardano stake-based ledger**

# CONCLUSION

- Blockchain = Immutability = Trust
- Blockchain is not a silver bullet
- A lot of potential is yet to be unleashed

guardtime

# THANK YOU!

Anna-Maria Osula / Senior Policy Manager

annamaria.osula@guardtime.com

guardtime.com