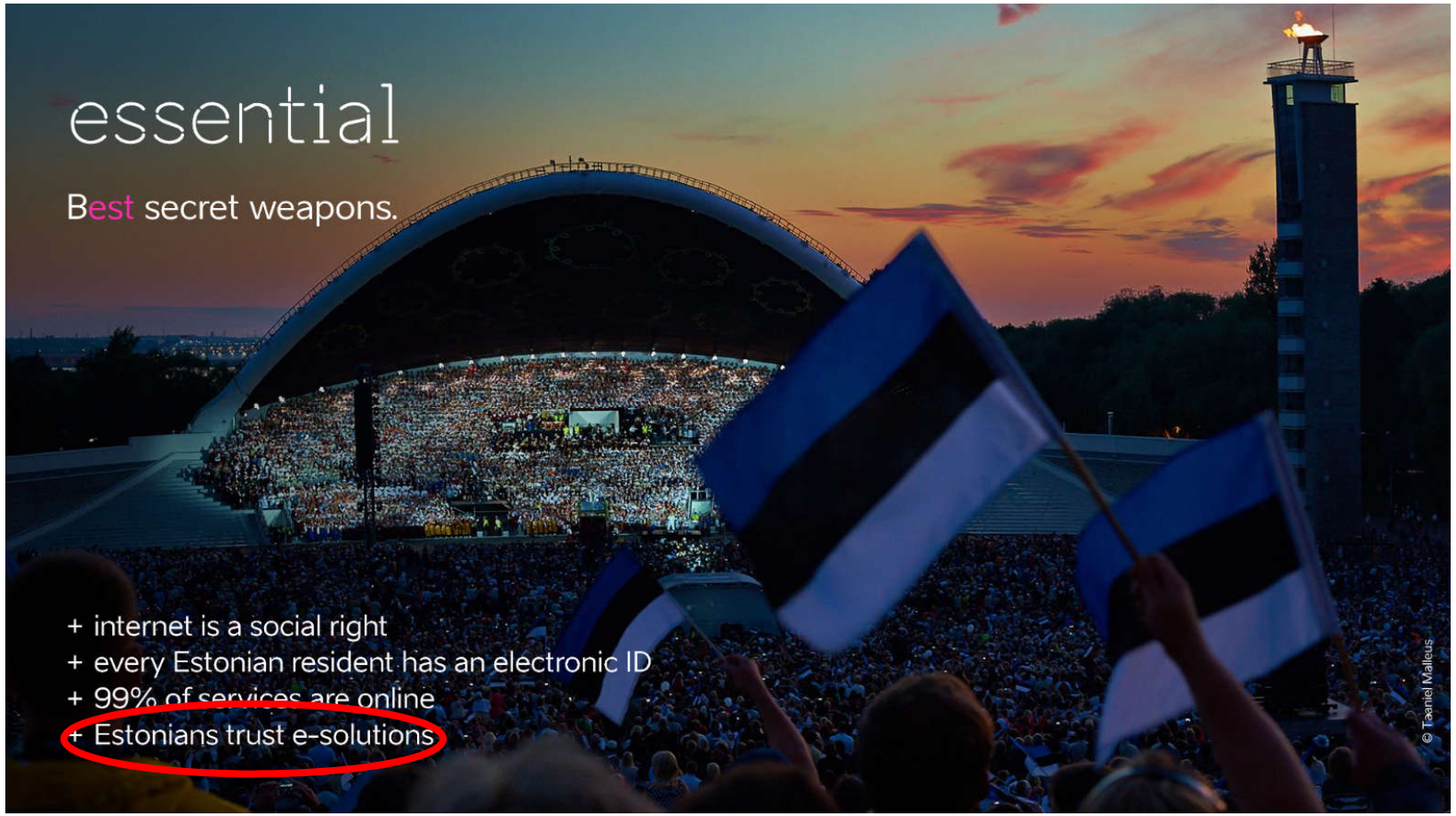
CSI Herbsttagung 2018
e -Government: KSI Blockchain

Zuzana Trubini
05.09.2018

cnlab

© 2018

Paradebeispiel e-Estonia



https://e-estonia.com/wp-content/uploads/e-estonia-v18.pdf

e-Estonia Prinzipien von e-Governance

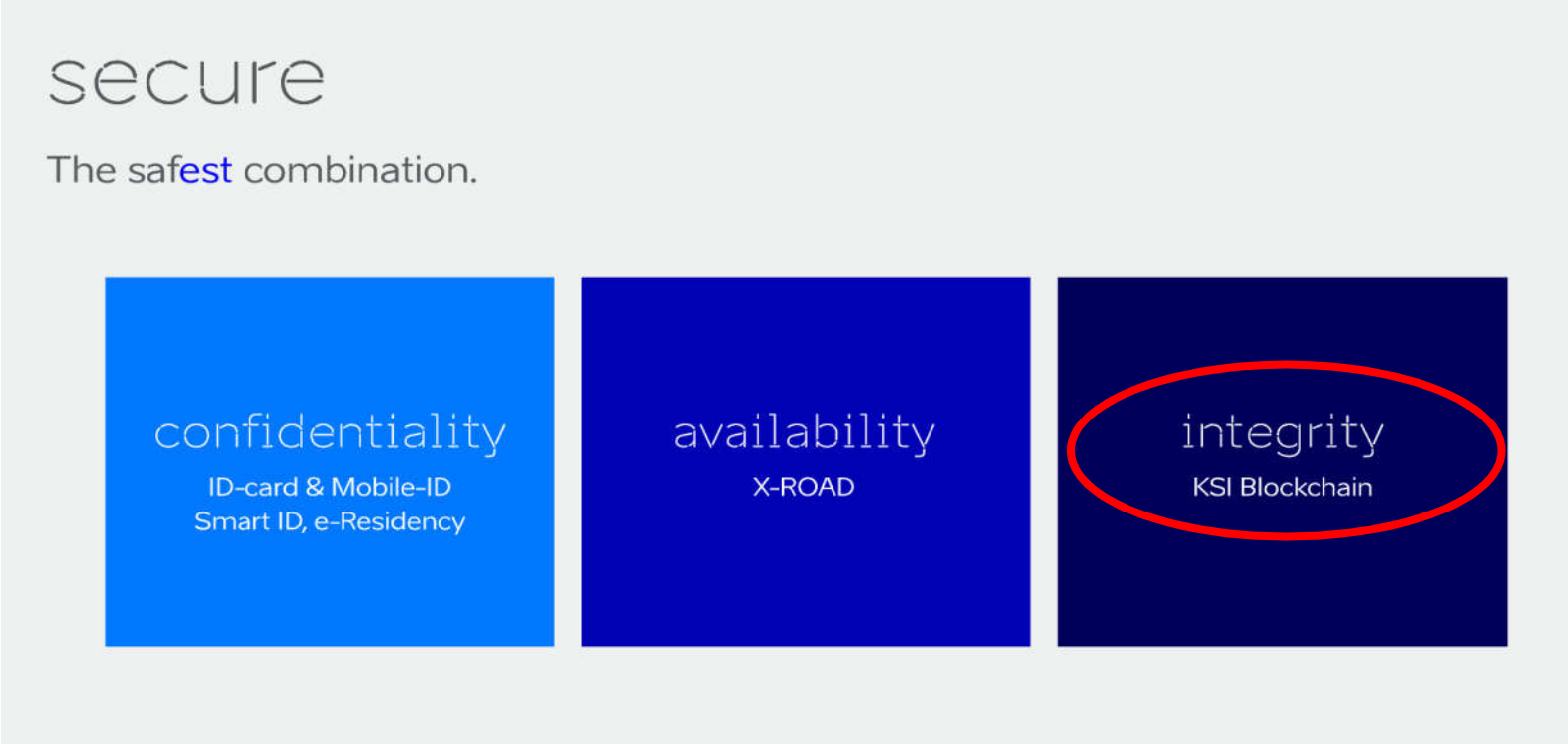
Principles of Estonian e-governance:

- **Decentralisation** — There's no central database and every stakeholder, whether a government department, ministry, or business, gets to choose its own system.
- **Interconnectivity** — All system elements exchange data securely and work smoothly together.
- **Integrity** — All data exchanges, M2M communications, data at rest, and log files are, thanks to KSI blockchain technology, independent and fully accountable.
- **Open platform** — Any institution may use the infrastructure and it works as an open source.
- **No legacy** — Continuous legal change and organic improvement of the technology and law.
- **Once-only** — Data is collected only once by an institution, eliminating duplicated data and bureaucracy.
- **Transparency** — Citizens have the right to see their personal information and check how it is used by the government via log files.

No. 1 in Freedom of the Net (Freedom House 2016)

https://e-estonia.com/wp-content/uploads/eas-eestonia-vihik-a5-180404-view.pdf

e-Estonia Bausteine



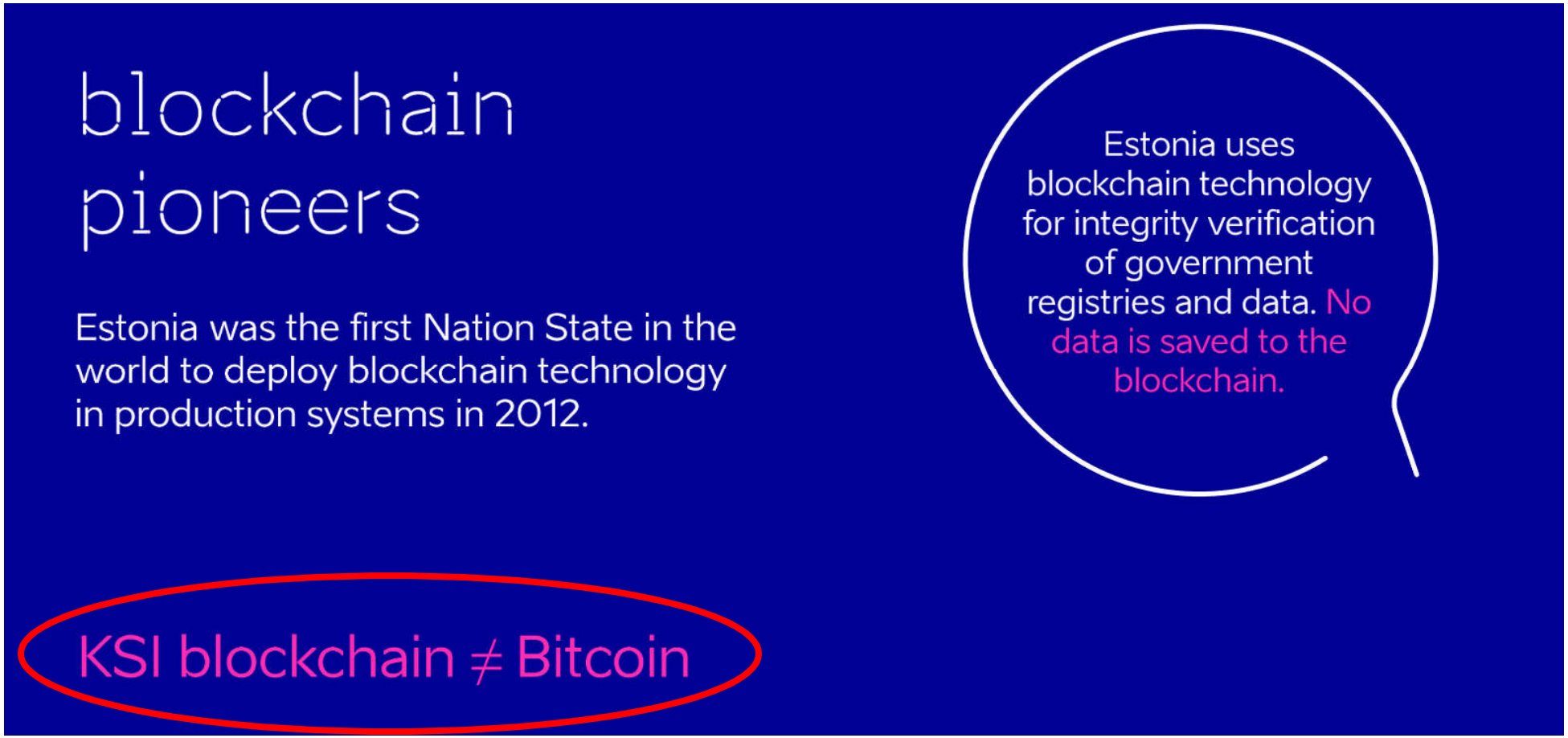
Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen (BSI).

https://e-estonia.com/wp-content/uploads/e-estonia-v18.pdf

e-Estonia Blockchain Anwendung

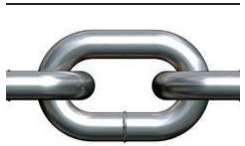
https://e-estonia.com/wp-content/uploads/e-estonia-v18.pdf

e-Estonia Blockchain vs. Bitcoin

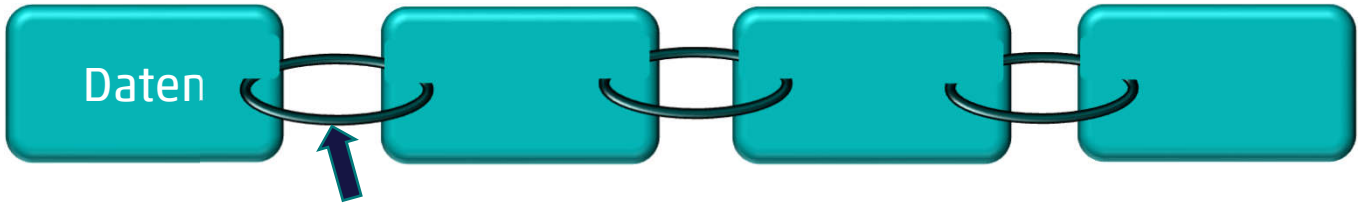


https://e-estonia.com/wp-content/uploads/e-estonia-v18.pdf

Blockchain - Definition



- **Eine Blockchain** (englisch für Blockkette) ist eine **dezentral** geführte, kontinuierlich erweiterbare **Liste von Datensätzen**, genannt „Blöcke“, welche mittels kryptographischer Verfahren **miteinander verkettet** sind (Wikipedia).



- **Was?** verteilte Datenbank, Register, Logbuch - append only
- **Warum?** Keine zentrale Instanz (der man vollumfänglich vertrauen muss)

  Vertrauen in eine Technologie

Blockchain - Inhalt, Rechte, Konsensus

Blockchain = ein verteiltes Logbuch bestehend aus miteinander verketteten Datenblöcken

1) **Was ist in den Blöcken enthalten?**
   - Transaktionen (Bitcoin), Hashes (KSI Blockchain), Kontrakte (Ethereum)...
2) **Wer darf lesen?**
   - Jeder -> Public (Bitcoin, KSI, ...)
   - Auserwählte -> Private (Consortium Blockchains)

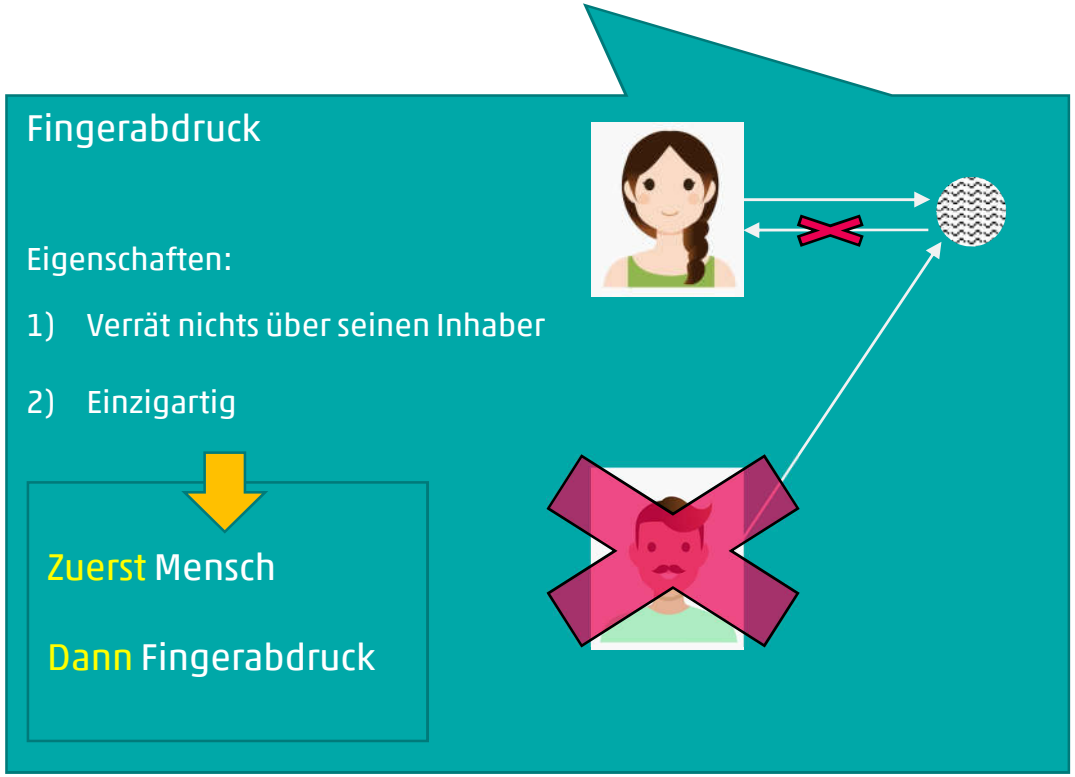
   Wer darf schreiben?
   - Jeder (der sich an gewisse Regeln hält) –> Permissionless (Bitcoin)
   - Auserwählte –> Permissioned (KSI)
3) **Wie wird Einigkeit erzielt?**
   - Proof of Work (Bitcoin), Proof of Stake, Proof of Space, ...
     Longest chain rule
   - Einigkeit bei jedem Block - «Klassischer Konsensus» – BA, BFT (KSI)
     Gültige Chain = die publizierte Chain (KSI-Blockchain)

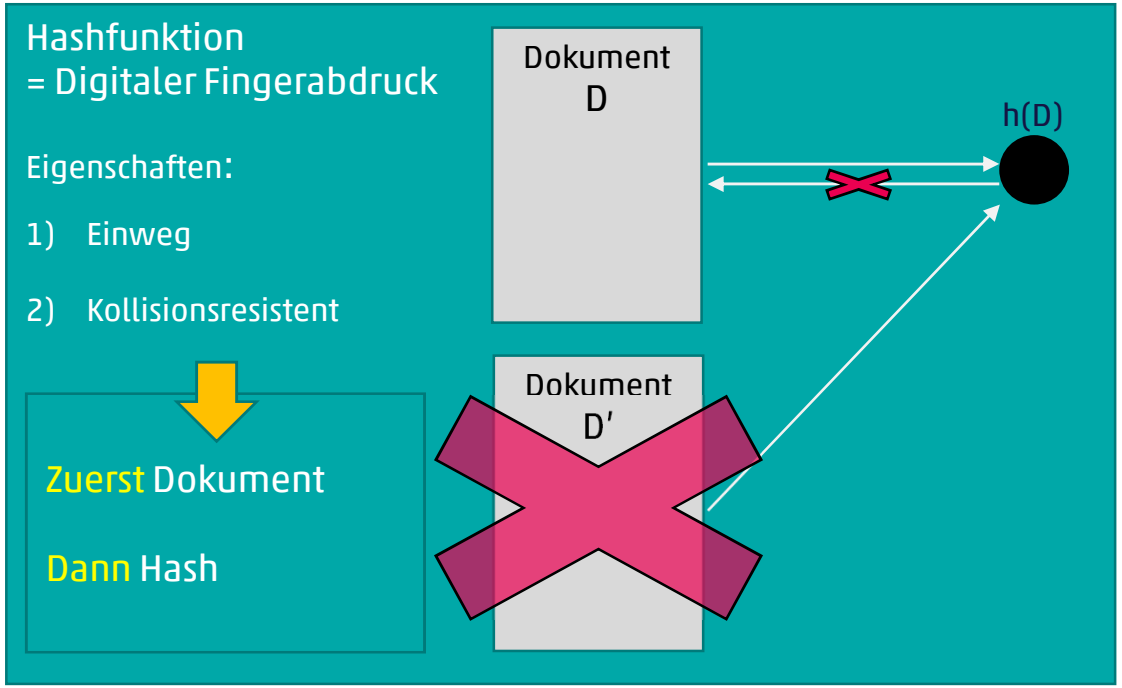
Blockchain - Bitcoin vs. KSI

	Bitcoin Blockchain	KSI Blockchain
Funktion	Kryptowährung	Integritätssicherung
Blockinhalt	Transaktionen	Hashes
Kette	Hashfunktion	Hashfunktion
Typ	Public, Permissionless Blockchain	Public, Permissioned Blockchain
Einigkeit	PoW, längste Chain	Konsensus (BA, BFT), publizierte Chain
Forkable ?	Ja (Vorübergehend)	Nein
Settlement Time	10 Minuten - 1 Stunde	1 Sekunde

Hashfunktion – Definition, Eigenschaften

Eine **Hashfunktion** bildet einen beliebig langen Datensatz auf einen kurzen (z.B. 256 Bit) Datensatz ab. Der (kurze) Hashwert soll als **Identifikator** des Originals dienen.

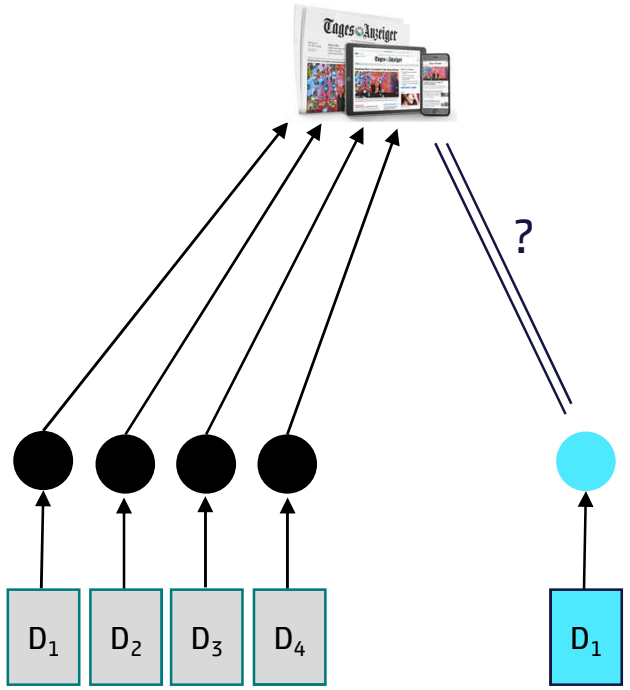




KSI Blockchain – Linked Timestamping

Time Stamping (Zeit-Stempel) – belegt die Existenz eines digitalen Dokuments zu einem gegebenen Zeitpunkt

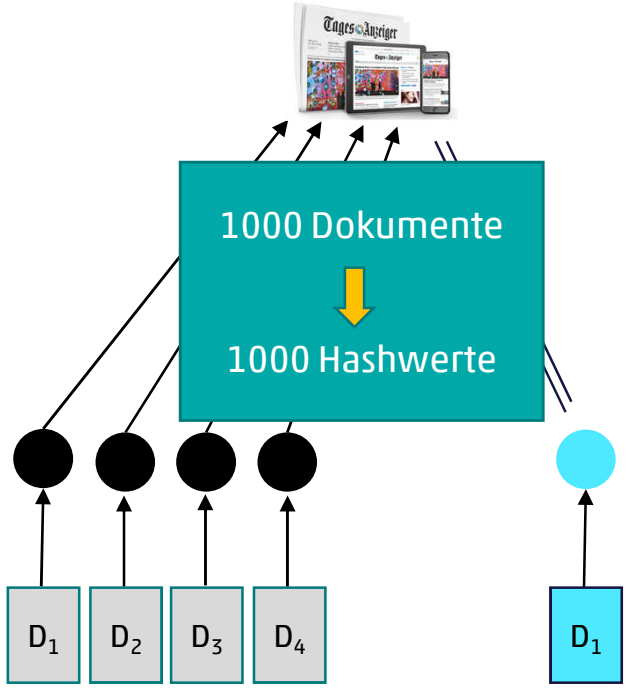
1.) Hash & Publish



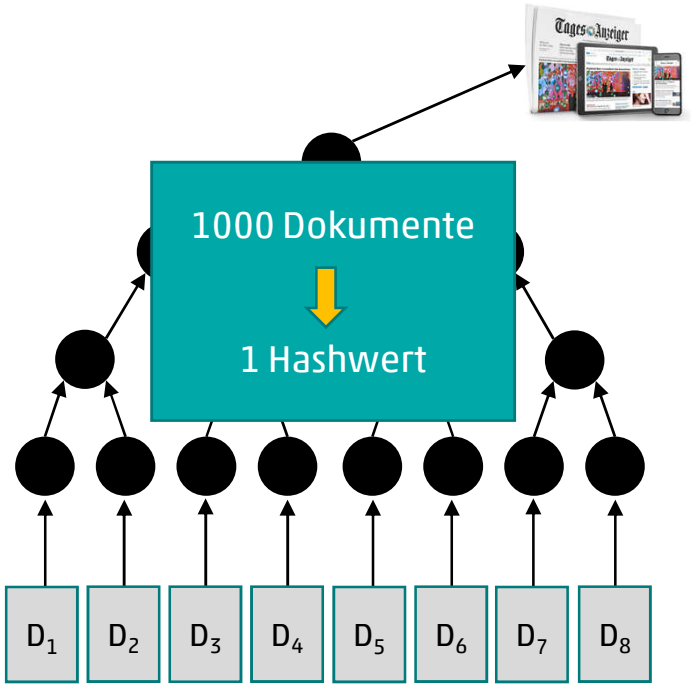
KSI Blockchain – Linked Timestamping

Time Stamping (Zeit-Stempel) – belegt die Existenz eines digitalen Dokuments zu einem gegebenen Zeitpunkt

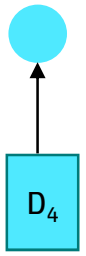
1.) Hash & Publish



2.) Hash-Tree



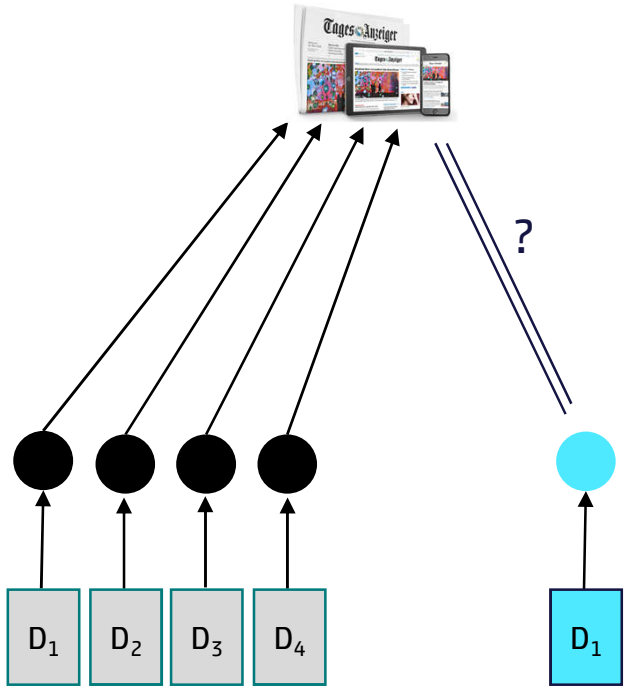
?



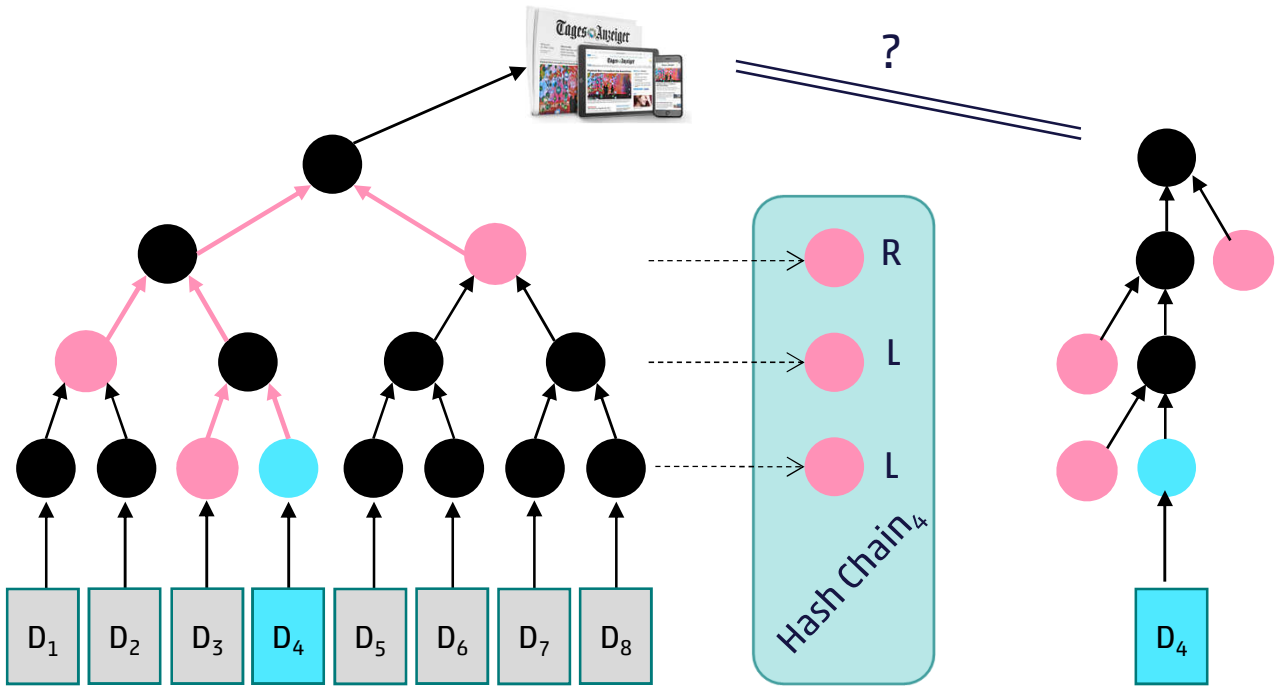
KSI Blockchain – Linked Timestamping

Time Stamping (Zeit-Stempel) – belegt die Existenz eines digitalen Dokuments zu einem gegebenen Zeitpunkt

1.) Hash & Publish



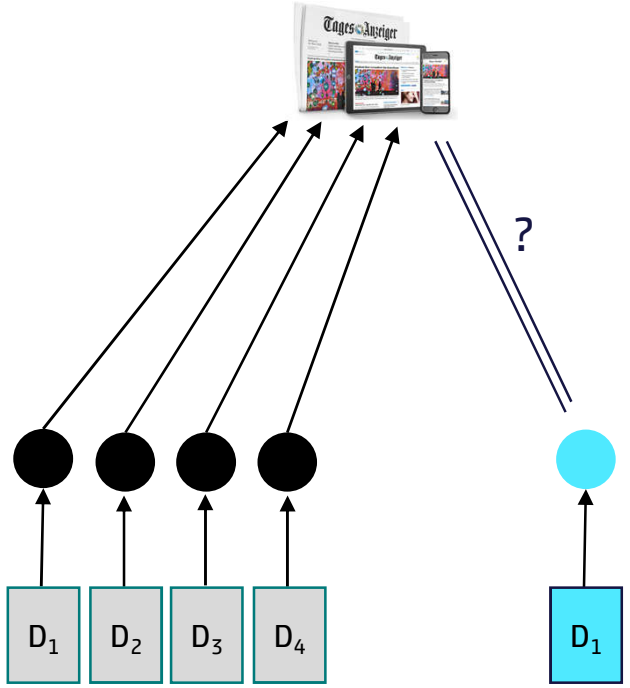
2.) Hash-Tree



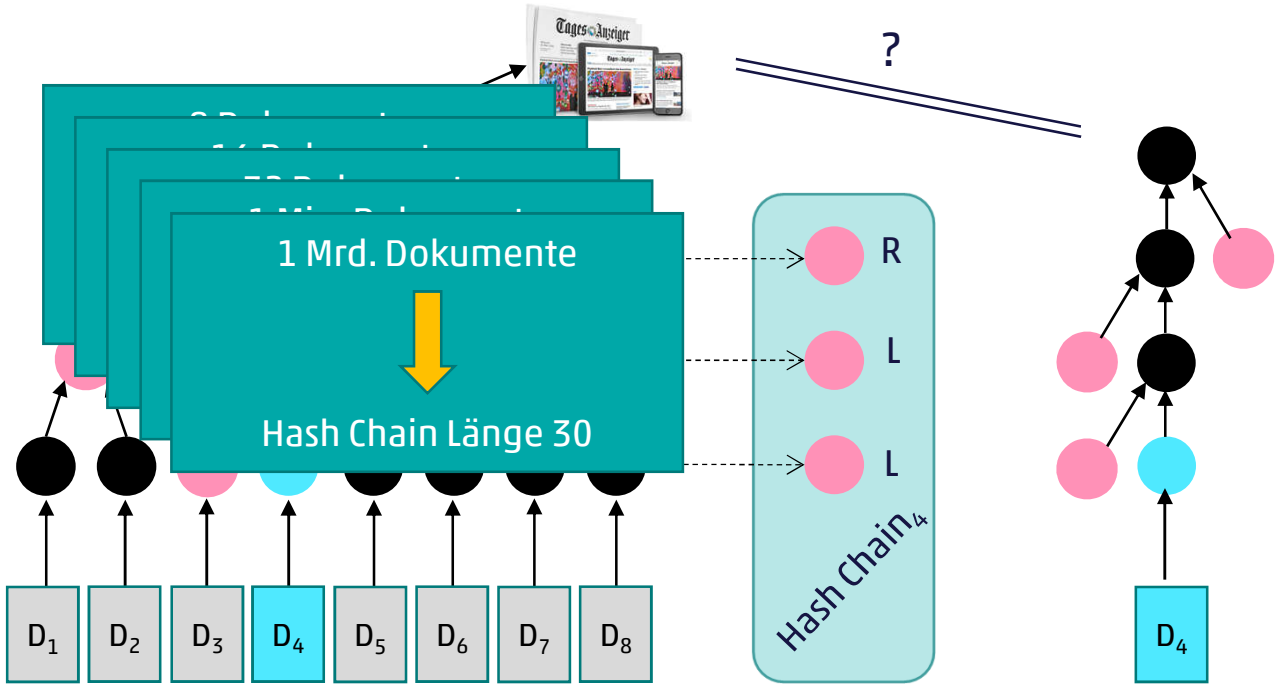
KSI Blockchain – Linked Timestamping

Time Stamping (Zeit-Stempel) – belegt die Existenz eines digitalen Dokuments zu einem gegebenen Zeitpunkt

1.) Hash & Publish

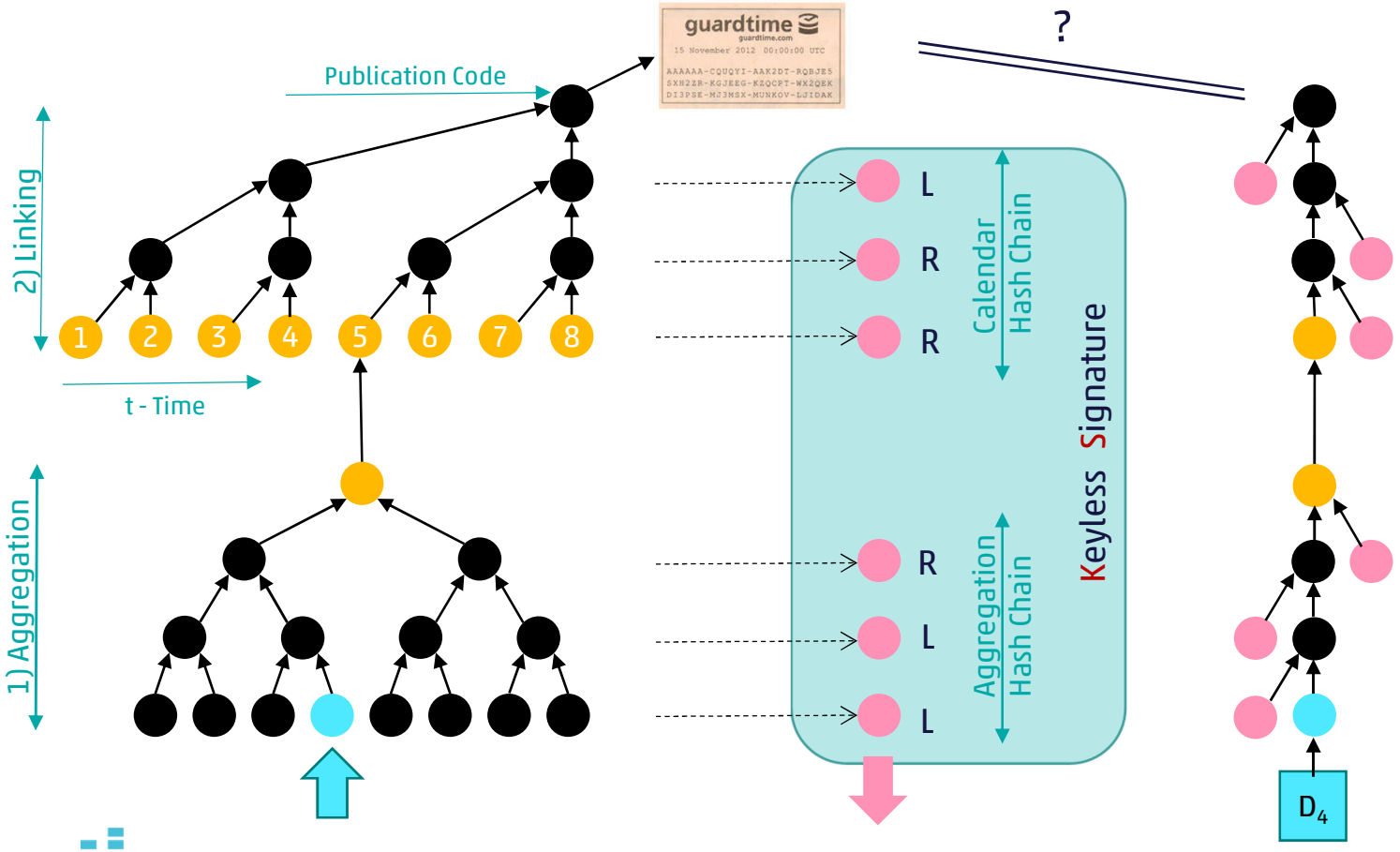


2.) Hash-Tree



KSI Blockchain – Hash Calendar

1) Jede Sekunde wird ein neuer Baum berechnet und der Top-Wert in einer publiken Datenbank gespeichert.
2) Jeden Monat werden alle (gelben) Top-Werte in einen neuen Baum verlinkt, der Top-Wert wird publiziert.



Seit 1.1.1970 (00:00) ein Eintrag pro Sekunde.

Bis jetzt etwa 1.5 Mrd. Einträge.

Der Calendar-Tree hat Tiefe 31.

KSI Blockchain - Was kann sie, was kann sie nicht?

blockchain technology helps detect who looks at a person's digital health data and changes it and when;

Millions of lives and resources are saved as the potential manipulation of defence data or smart war machines is prevented using blockchain technology.

Blockchain technology makes it possible to discover any and all changes made to digital data, no matter how small, no matter by whom, immediately and with zero error.

As a result, while it today takes on average about 7 months to discover the breach or misuse of an organisation's data, the blockchain helps to discover such threats instantly. For example, cases like Snowden would never have happened if the NSA had been using blockchain technology like in Estonia. It is important to point out that although blockchain may not prevent the crime itself, it is 100% effective in detecting it.

In order to keep health information completely secure and at the same time accessible to authorised individuals, the electronic ID-card system used by the Estonian e-Health Record uses blockchain technology to ensure data integrity and mitigate internal threats to the data. In this way every occurrence of data use and misuse is detectable and major damages to a person's health can be prevented (such as the wrong medicine or the wrong dose).

https://e-estonia.com/wp-content/uploads/faq-a4-v02-blockchain.pdf

Referenzen

- https://guardtime.com/files/BuKL13.pdf
- https://e-estonia.com/wp-content/uploads/e-estonia-v18.pdf
- https://e-estonia.com/wp-content/uploads/eas-eestonia-vihik-a5-180404-view.pdf
- https://de.wikipedia.org/wiki/Blockchain
- https://en.wikipedia.org/wiki/Linked_timestamping
- https://www.slideshare.net/GuardTimeEstonia/hash-functions-lecture-series-by-ahto-buldas
- https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html
- https://de.freepik.com

Vielen Dank für Ihre Aufmerksamkeit_

Zuzana Trubini
zuzana.trubini@cnlab.ch
+41 55 214 33 34

info@cnlab-security.ch
+41 55 214 33 33

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland

cnlab

© 2018