Mit freundlicher Unterstützung:

bank-verlag

Informationstag
"Elektronische Signatur und Vertrauensdienste"
Gemeinsame Veranstaltung von TeleTrusT und VOI

Berlin, 18.09.2018

Langfristige Beweiswerterhaltung zwischen eIDAS und Blockchain

Steffen Schwalm & Tomasz Kusber, Fraunhofer Fokus

LANGFRISTIGE BEWEISWERTERHALTUNG ZWISCHEN EIDAS UND BLOCKCHAIN

Tomasz Kusber, Steffen Schwalm: Fraunhofer Institut für Offene Kommunikationssysteme FOKUS
Dr. Ulrike Korte, Dr. Christian Berghoff: Bundesamt für Sicherheit in der Informationstechnik

Berlin, den 18. September 2018

Fraunhofer FOKUS

Bundesamt für Sicherheit in der Informationstechnik

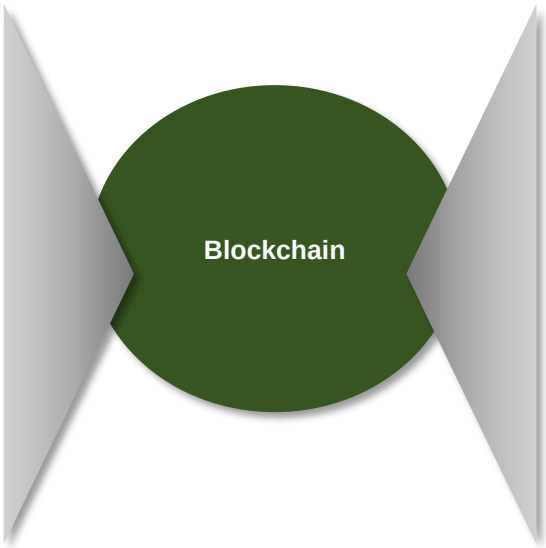
AGENDA

1. Einführung
2. Wesentliche Rahmenbedingungen zur Beweiswerterhaltung
3. Digitale Identitäten und Datenschutz
4. Herausforderungen an die Blockchain
5. Lösungsoptionen
6. Fazit und Ausblick

BLOCKCHAIN – VERTEILTE JOURNALE IN PEER-TO.PEER-NETZWERK ALS 4. (DIGITALE) REVOLUTION?

Permissionless/Public Chain

- Keine zentrale Instanz (Vertrauensmodell)
- Vertrauen durch die Community (51%-Modell)
- anreizbasierter Konsens-mechanismus z.B. PoW
- Mining durch alle Nutzer möglich
- Typisch bspw. für Kryptowährungen wie Bitcoin
- Zugriff für beliebige Nutzer faktisch keine Nutzerkontrolle
- Hoher Energieverbrauch bei geringen Datendurchsatz



Permissioned/Private Chain

- Stärker zentralisiert
- Vertrauen auch durch betreibende Instanz (vertrauenswürdiger Dritter)
- Nachrichtenbasierte Konsensverfahren
- Mining nur durch berechtigte User
- Kein Anreizsystem notwendig
- Begrenzter Energie-/Rechenaufwand
- Nur autorisierte Nutzer
- Eindeutige wie sichere Identifizierung notwendig

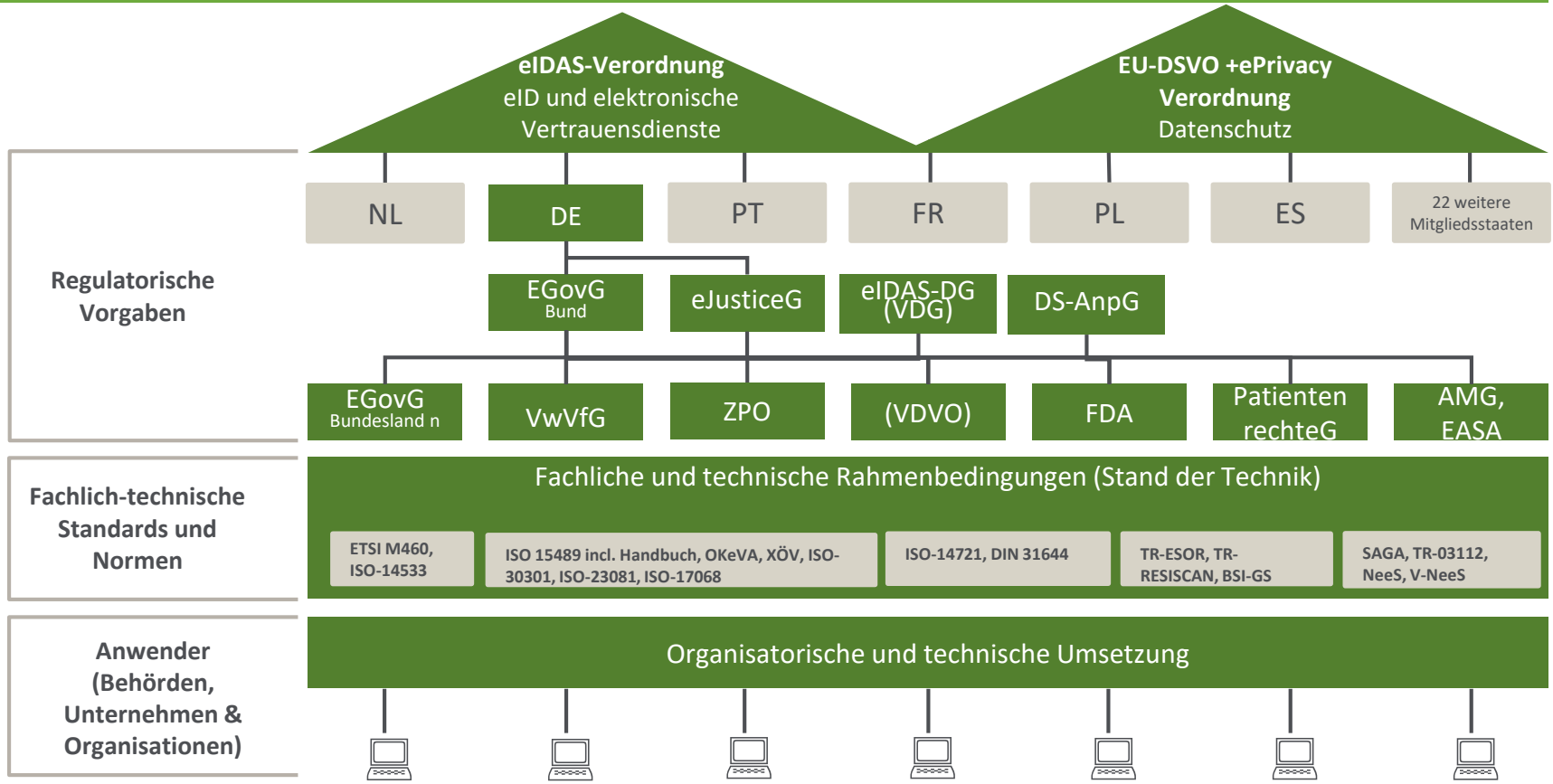
UsesCases (Beispiele)

- Kryptowährungen, Hochfrequenzhandel
- Registerautomatisierung, intelligente Energienetze
- Überwachung von Lieferketten, Vertragsinhalten (SmartContracts)

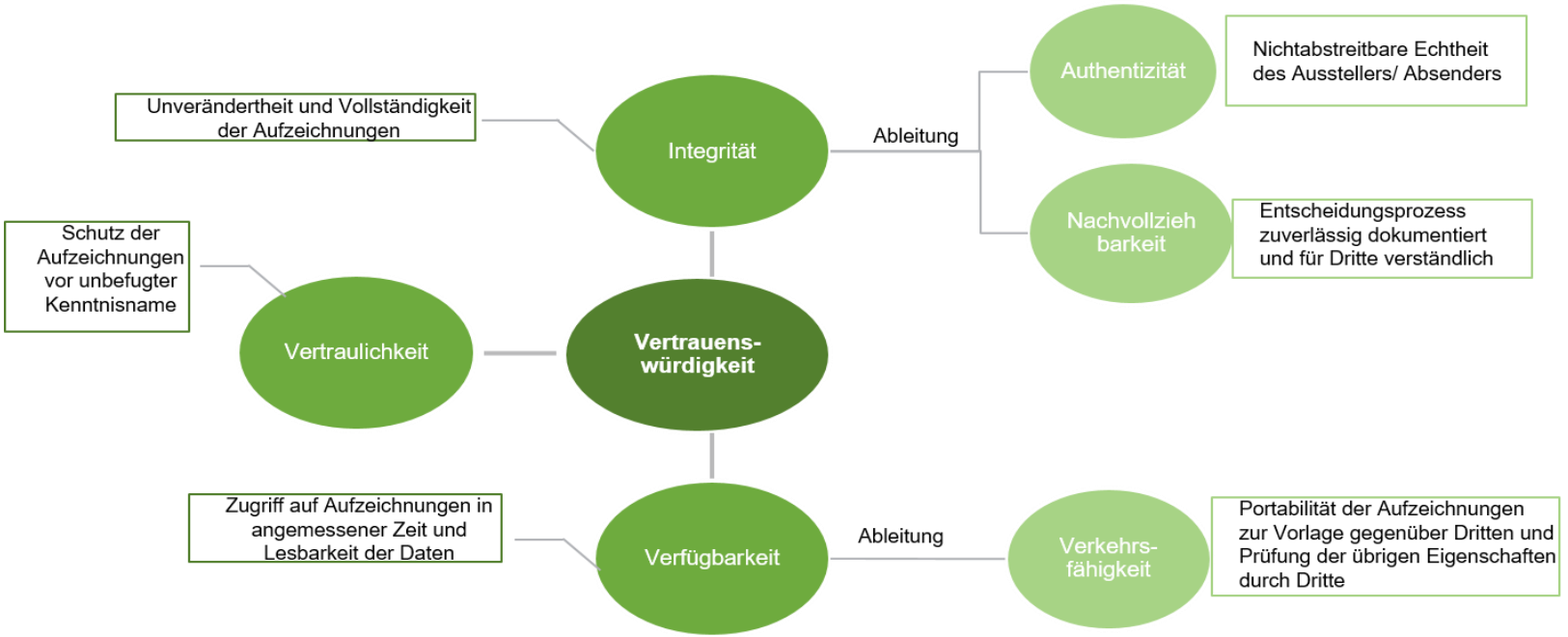
AGENDA

1. Einführung
2. Wesentliche Rahmenbedingungen zur Beweiswerterhaltung
3. Herausforderungen der Blockchain
4. Lösungsoptionen
5. Fazit und Ausblick

REGULATORISCHE RAHMENBEDINGUNGEN VERTRAUENSWÜRDIGER DIGITALER PROZESSE

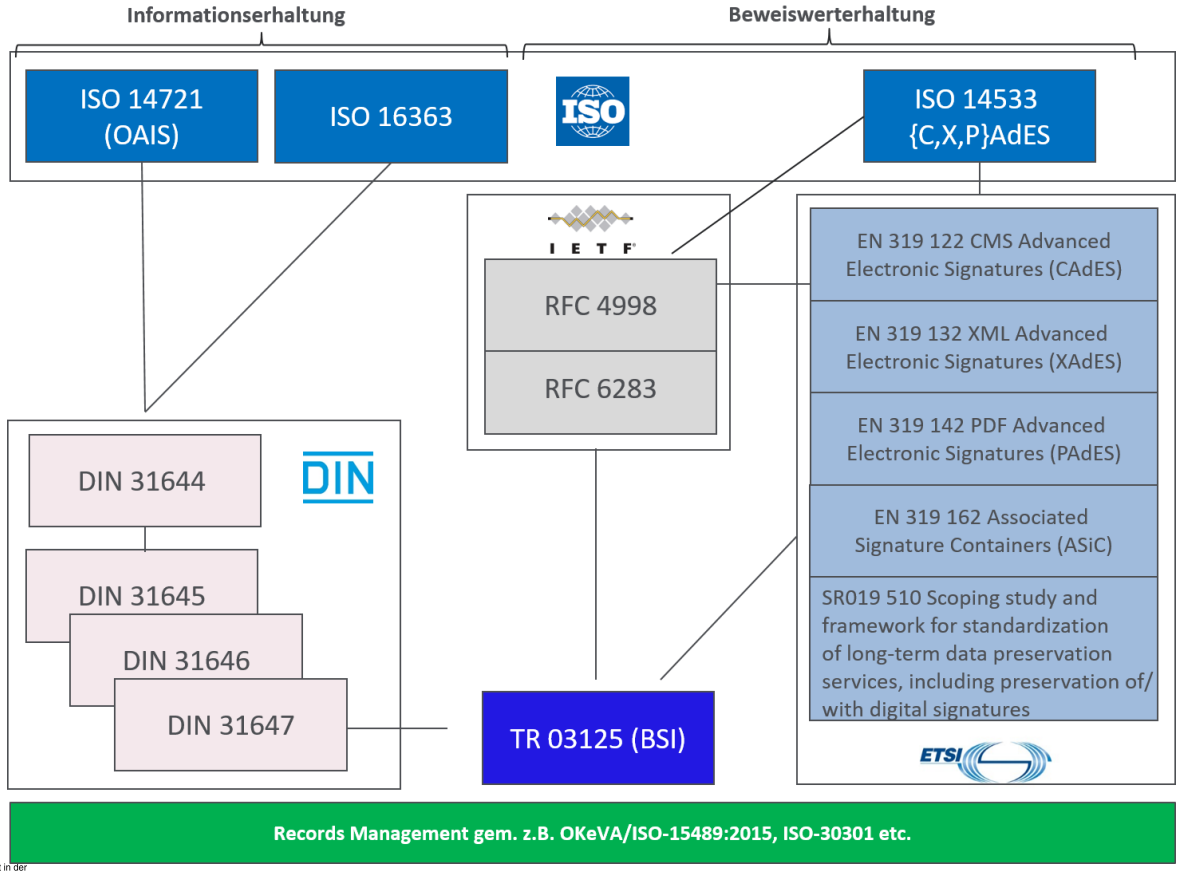


FÜR VERTRAUENSWÜRDIGE DIGITALE GESCHÄFTSPROZESSE SIND IM WESENTLICHEN DIE FOLGENDEN ANFORDERUNGEN ANHAND DER GESCHÄFTSRELEVANTEN UNTERLAGEN NACHZUWEISEN



Gewährleistung durch definierte Prozesse, Organisation, Governance, IT (Records Management)

STAND DER TECHNIK ZUR BEWEISWERTERHALTENDEN LANGZEITSPEICHERUNG BZW. DEM LANGFRISTIGEN NACHWEIS DIGITALER TRANAKTIONEN



AGENDA

1. Einführung

2. Wesentliche Rahmenbedingungen zur Beweiswerterhaltung

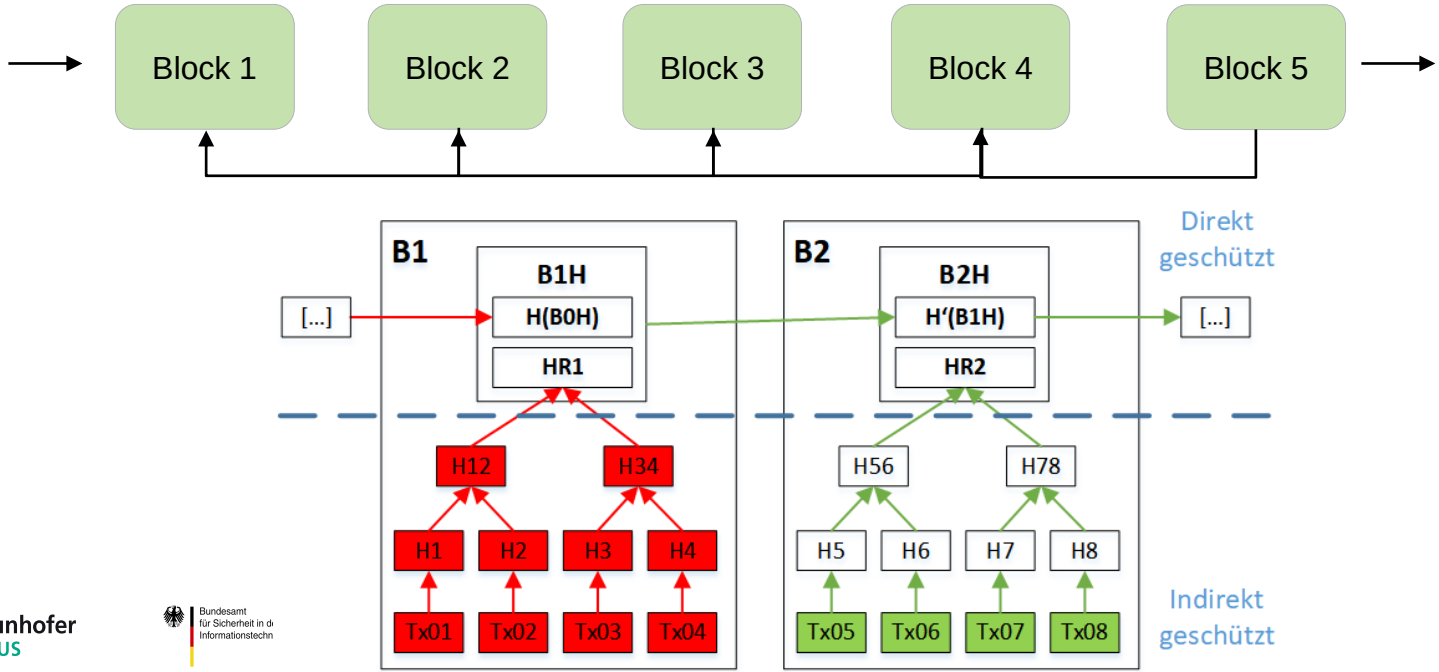
3. Herausforderungen der Blockchain

4. Lösungsoptionen

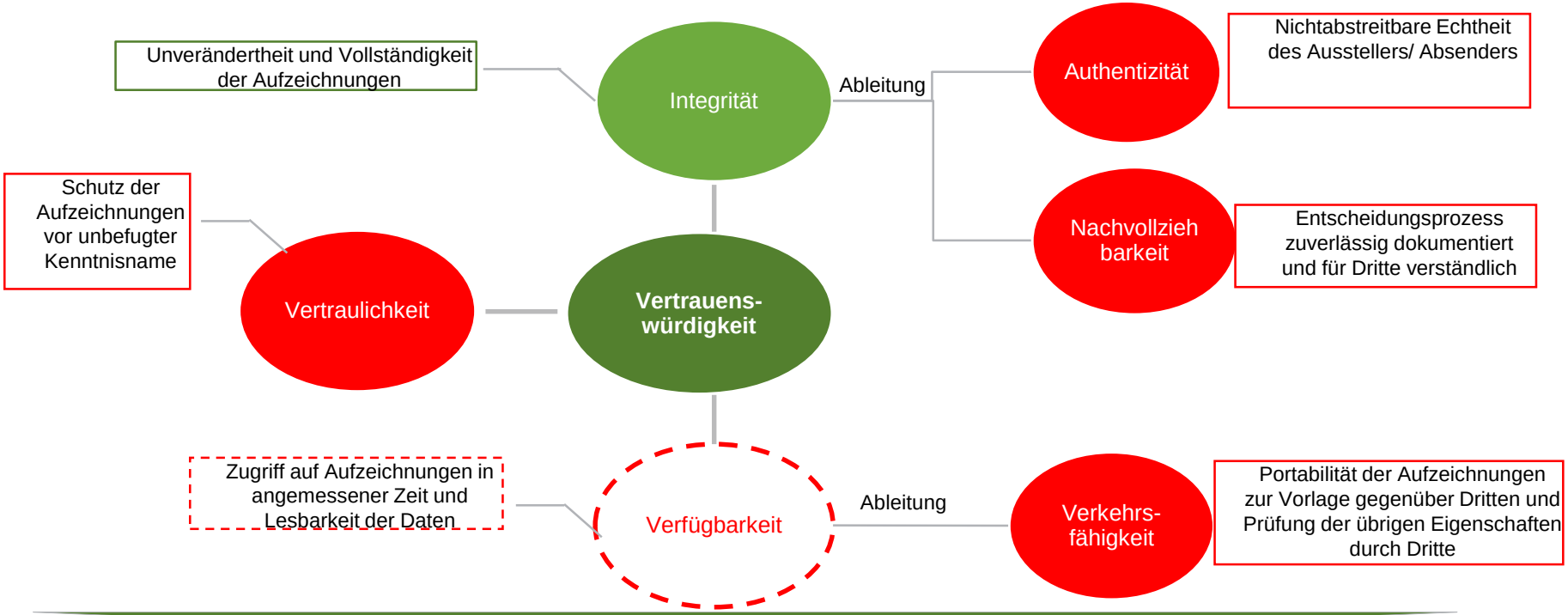
5. Fazit und Ausblick

DIE BLÖCKE WERDEN NACH DEM VATER-SOHN-PRINZIP VERHASHT – ES BESTEHT ABER KEIN REHASHING DER (BLOCK)CHAIN

- Block 2 hasht 1, Block 3 hasht 2, aber kein Block enthält alle Hashs und kein Mechanismus zum Rehashing der Chain
- Was passiert wenn die Hashalgorithmen der Blöcke veralten (Verlust der Integrität)?
- Unbemerkte Manipulation der Blöcke durch Nachrechnen der Hashwerte möglich, nach Ablauf der Sicherheitseignung
- Kein immanenter Proof of Existence durch rechtsgültige Zeitstempel, damit keine Beweiswerterhaltung
- Derzeit keine Strategien zur Informationserhaltung der Blöcke und deren Inhalte



DERZEIT ERFÜLLT BLOCKCHAIN NUR EINEN MARGINALEN TEIL DER ANFORDERUNGEN AN VERTRAUENSWÜRDIGE DIGITALE TRANSAKTIONEN



Gewährleistung durch definierte Prozesse, Organisation, Governance, IT (Records Management)

AGENDA

1. Einführung

2. Wesentliche Rahmenbedingungen zur Beweiswerterhaltung

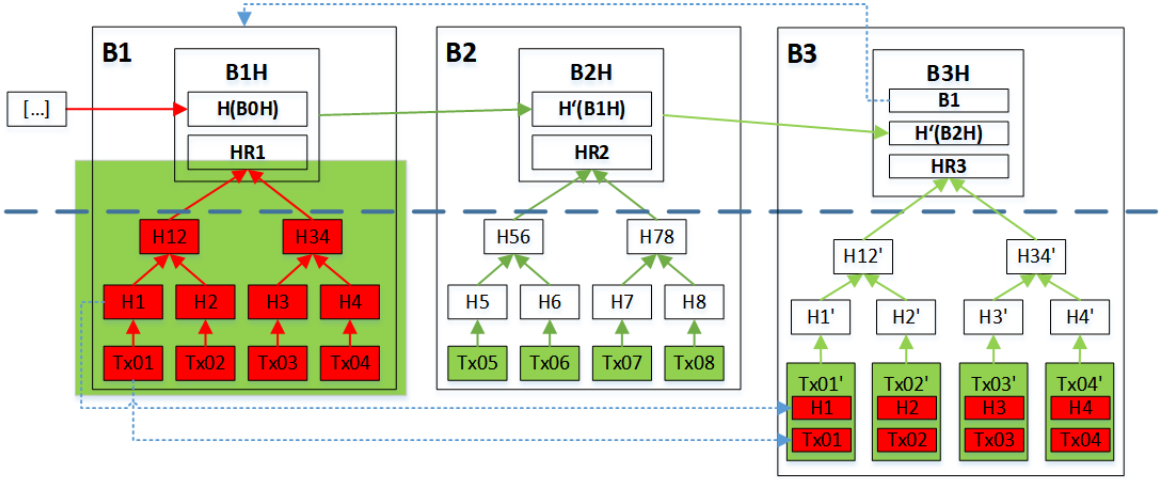
3. Herausforderungen der Blockchain

4. Lösungsoptionen

5. Fazit und Ausblick

LÖSUNGSOPTION 1:
ERHALTUNG DER INTEGRITÄT DURCH DEDIZIERTE BLÖCKE IN BLOCKCHAIN

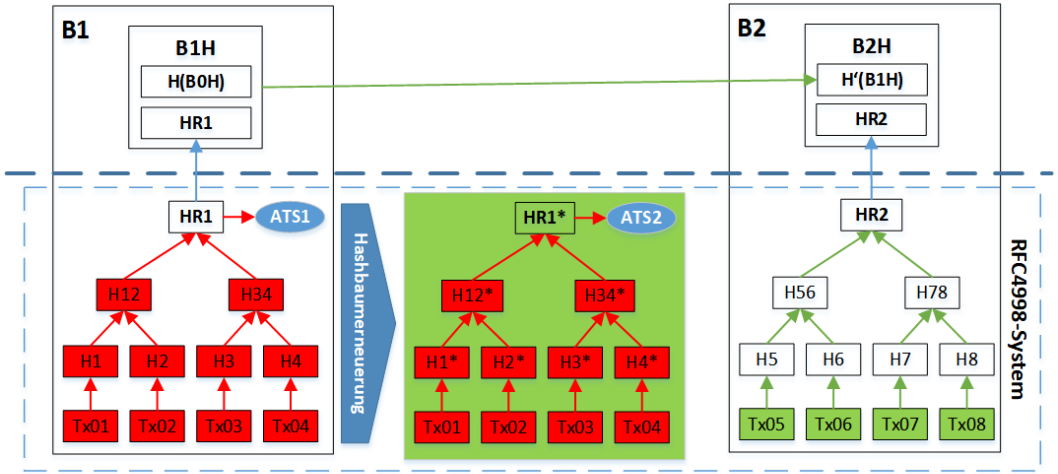
Wesentliche Maßgabe: aufbewahrungspflichtige **Daten** befinden sich **in** der **Blockchain**



\+ Gewährleistung langfristiger Integritätsschutz
– Keine Beweiswerterhaltung, da kein Proof of Existence durch qualif. Zeitstempel
– Hohe Komplexität, lange Blockkette
– Datenschutzvorgaben nicht erfüllbar
– Zum Nachweis ist immer die komplette Kette vorzulegen (ggf. Vertraulichkeits-/Datenschutzherausforderung

LÖSUNGSOPTION 2: BLOCKCHAIN UND RFC4998

Wesentliche Maßgabe: aufbewahrungspflichtige Daten befinden sich in der Blockchain

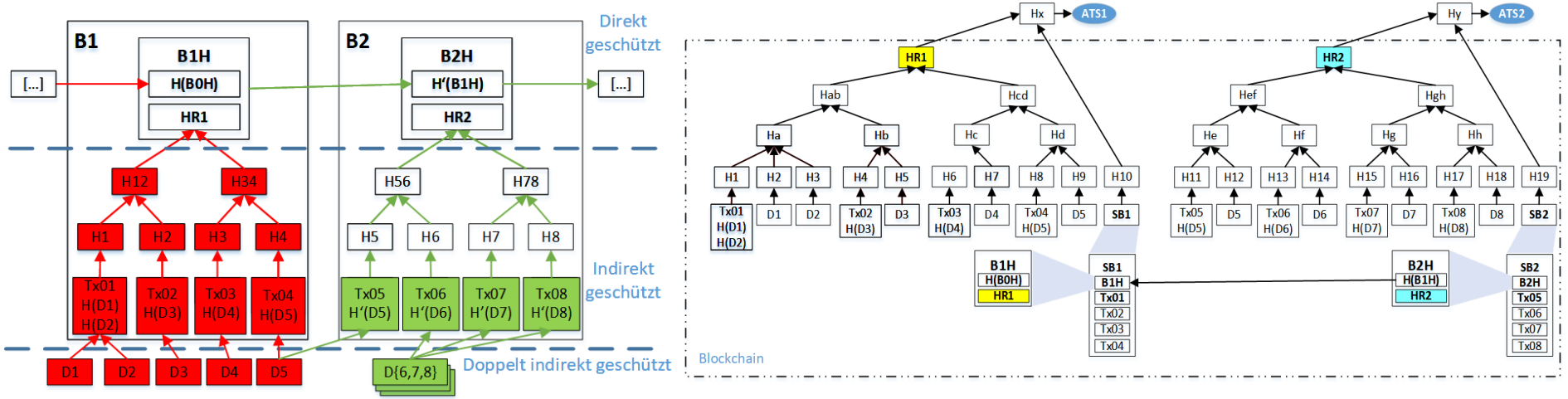


wobei, z.B. H1*=H*(H*(Tx01) || H*(atsc1)) – vgl. hierzu Kap. 5.2 RFC4998

+ Gewährleistung langfristiger Integritätsschutz
+ Gewährleistung Beweiswerterhaltung
+ begrenzter Implementierungsaufwand
– Hohe Komplexität durch zwei parallele wie autonome Systeme und Nachweis nur mit Artefakten aus beiden Systemen möglich
– Datenschutzvorgaben nicht erfüllbar
– Zum Nachweis ist immer die komplette Kette vorzulegen (ggf. Vertraulichkeits-/Datenschutzherausforderung

LÖSUNGSOPTION 3: LOGISCHE BLOCKCHAIN AUF BASIS VON RFC4998

Wesentliche Maßgabe: aufbewahrungspflichtige Daten befinden sich außerhalb der Blockchain, Blockchain beinhaltet nur Hashwerte der Daten



+ Gewährleistung langfristiger Integritätsschutz
+ Gewährleistung Beweiswerterhaltung
+ Gewährleistung Datenschutz für Content über Fremdsystem in dem die Daten gespeichert sind (z.B. digitales Langzeitarchiv gem. OAIS [ISO-14721:2012] und TR-ESOR)
- Identifizierungsdaten befinden sich weiterhin in Blockchain mit entspr. Datenschutzproblem

VERGLEICH DER OPTIONEN (1/2)

Anforderung	Blockchain nativ	Option 1: dezidierte Blöcke in der Blockchain	Option 2: Blockchain und RFC 4998	Option 3: logische Blockchain auf Basis von RFC 4998
Erhalt Integritätsschutz	Nein	Ja	Ja	Ja
Beweiswerterhaltung	Nein	Nein kein Proof of Existence und keine Neusignierung, nur Integritätsschutz	Ja Verkehrsfähigkeit des Evidence Records gegeben	Ja Verkehrsfähigkeit des Evidence Records gegeben
Verkehrsfähigkeit	Nein	Nein	Ja	Ja
Komplexität	Abhängig vom Vertrauensmodell	Höheres Datenaufkommen	Ggf. zusätzliche Komplexität durch externes System	Ggf. zusätzliche Komplexität durch externes System

VERGLEICH DER OPTIONEN (2/2)

Anforderung	Blockchain nativ	Option 1: dezidierte Blöcke in der Blockchain	Option 2: Blockchain und RFC 4998	Option 3: logische Blockchain auf Basis von RFC 4998
Gewährleistung Datenschutz	nein	nein, Keine Verkehrsfähigkeit und damit keine Übertragbarkeit mittels standardisierter Austauschformate, keine Löschmöglichkeit, keine Möglichkeit zur Berichtigung personenbezogener Daten sowie identitätsbezogener Zugangskontrolle	Nein Keine Verkehrsfähigkeit und damit keine Übertragbarkeit mittels standardisierter Austauschformate, keine Löschmöglichkeit, keine Möglichkeit zur Berichtigung personenbezogener Daten sowie identitätsbezogener Zugangskontrolle	Grundsätzlich vorhanden Hohe Komplexität, da Teile des AIP (Content, Metadaten) in Fremdverfahren und Erhaltung des Kontexts zu Teilen (Prozessdaten, ggf. Identitätsdaten) in Blockchain <u>Im Fremdsystem:</u> Übertragbarkeit, Löschung, Berichtigung standardisiert möglich; hinsichtlich der Identitäts- und Prozessdaten, die in der Blockchain verbleiben, sind weitere Untersuchungen im Kontext Datenschutz notwendig

AGENDA

1. Einführung
2. Wesentliche Rahmenbedingungen zur Beweiswerterhaltung
3. Herausforderungen der Blockchain
4. Lösungsoptionen
5. Fazit und Ausblick

FAZIT UND AUSBLICK

Blockchain für vertrauenswürdige digitale Prozesse

Datenschutz und Nachweis

- Grundsätzlich kommt aufgrund der Eigenschaften faktisch nur pemissioned blockchain in Frage
- Derzeit keine standardisierten Mechanismen zur Gewährleistung der Übertragbarkeit, Berichtigung, Löschung personenbezogener Daten
- Begrenzte Mechanismen zur eindeutigen wie sicheren Identifikationen und Authentisierung der Nutzer
- Derzeit keine standardisierten Prozeduren zum Informations-/Beweiswerterhalt sowie zur Verfügbarkeit

Lösungs-optionen

- Option 1 gewährleistet weder Datenschutz noch Beweiswerterhaltung
- Option 2 gewährleistet die Datenschutzvorgaben nicht
- Beide Optionen bergen vergleichsweise hohe Komplexität
- Option 3 setzt auf standardisierte Mechanismen und birgt derzeit größten Praxisbezug und Umsetzbarkeit

Praktikabilität

- Kritische Prüfung der Komplexität und Performance einer Blockchain-Anwendung im Rahmen der Konzeption und Anforderungserhebung notwendig (bei allen Optionen)
- falls nachweispflichtige oder personenbezogene Daten verarbeitet werden, faktisch keine Ablage in Blockchain möglich
- ggf. zunächst reine Verwendung von SmartContracts als Infrastrukturservice (übergreifender Zugriff)

Option 3 einer logischen Blockchain erscheint derzeit als die praktikabelste Variante und sollte die Basis weiterer Standardisierungs-/Forschungsarbeiten bilden; ebenso gilt es Mechanismen zur Gewährleistung des Datenschutzes von Identitätsdaten in Blockchain zu entwickeln


Fraunhofer
FOKUS


Bundesamt
für Sicherheit in der
Informationstechnik