TeleTrusT
Pioneers in IT security.

TeleTrusT-Informationstag "Blockchain"

Frankfurt a.M., 13.07.2017

Was ist "die Blockchain"? Strategien und Möglichkeiten

Volker Skwarek, HAW Hamburg

DER VORTRAG
ÜBERSICHT

- Ursprung
- Funktion im Überblick
- Kerneigenschaften
- Mehr als nur Geldtransfer
- Perspektiven für zukünftige Technologien
- Blockchain und Security
- Standardisierung
- Bedeutung für Deutschland und Europa
- Zusammenfassung

BLOCKCHAINS UND DISTRIBUTED LEDGER TECHNOLOGIES (DLT)
WOHER KOMMEN SIE?

Haber, S., Stornetta, W.: How to time-stamp a digital document. Advances in Cryptology-CRYPT0'90. 437–455 (1991).

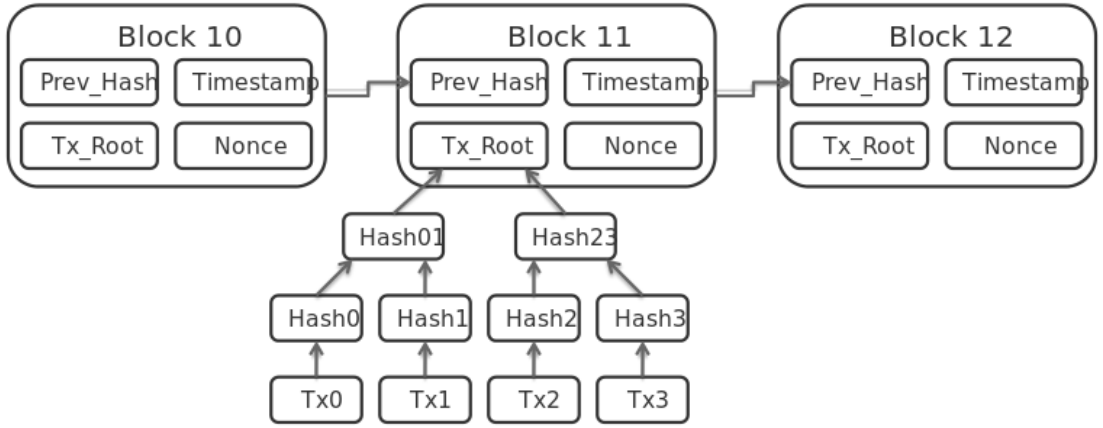
Schneider, B., Kelsey, J.: Cryptographic Support for Secure Logs on Untrusted Machines. San Antonio, Texas, USA (1997).

- **Anwendungsfall**: unveränderbares Speichern von vertrauenswürdigen Informationen auf vertrauenslosen (engl.: trustless) Maschinen
- **Randannahmen**:
    - Kein System ist so sicher, dass es nicht manipuliert werden kann
    - Jedes System kann gelöscht werden
    - Es besteht ausreichend viel Bandbreite zur Datenkommunikation

- **Ziel**: auch wenn Manipulation zum Zeitpunkt t möglich ist, dürfen die Daten vor t nicht (unbemerkt) verändert werden

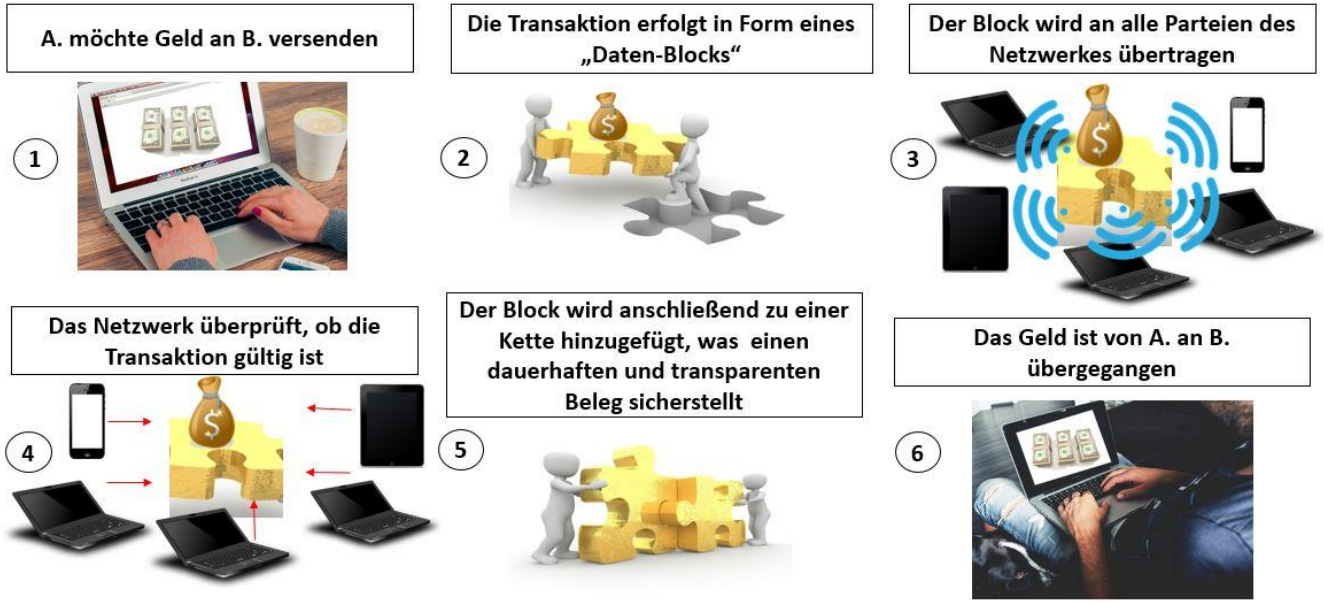
BLOCKCHAINS UND DLT
WIE FUNKTIONIEREN SIE?

Blockchain = Hash-verkettete Liste



Quelle: https://www.basicthinking.de/blog/2014/10/09/das-bitcoin-handbuch-tutorial-zur-digitalen-waehrung-wie-entstehen-bitcoins-und-was-heisst-bitcoin-mining/

Distributed Ledger = verteilte Journale



Quelle: https://cloudikon.de/wp-content/uploads/2016/02/Blockchain-Bild-Neu.jpg

BLOCKCHAINS UND DLT
WOFÜR STEHEN SIE?

- **Verteilte Systeme:** das Systemwissen einschließlich der gesamten Historie kann vollständig an jedem Knoten zur Verfügung stehen
- **manipulationsgeschützt**: Verkettung der Transaktionen, Verteilung und Konsens erfordern einen >50%-Angriff, um eine Transaktion zu manipulieren
- **vertrauenswürdig**: die Authorisierung von Transaktionen durch einen Nutzer ist durch kryptographische Verfahren sichergestellt und nachvollziehbar
- **systematisch und aufwandsgesteuert:** Aufwand der Transaktionsabsicherung ist skalierbar
- **konsensbasiert:** Transaktion gewinnt zunehmend an Zuverlässigkeit, je mehr Teilnehmer diese bestätigen

BLOCKCHAINS UND DLT
PERSPEKTIVEN FÜR ZUKÜNFTIGE TECHNOLOGIEN

Potenzial, DIE grundlegende Technologie für verteilte, öffentliche, konsensbasierte Prozesse ohne Mittelsmann zu werden.

- **Transparenz** für öffentliche Verwaltung und **demokratische Abläufe**:
  - öffentliche Akten wie Geburts- und Standesregister, Einwohnermeldeamt, Grundbuch, Handelsregister, …
  - Basis für transparente Durchführung von Wahlen
- **Lizenzmanagement**: Code in einer öffentlichen Chain ablegen und lizensierte Verwendung transparent machen
- **Energiemarkt**: Trading und Netzmanagement koppeln und transparent abwickeln
- **Industrie 4.0**:
  - Datenkommunikation und Systemsteuerung zwischen Produkten und Anlage leichtgewichtig und transparent gestalten
  - offene Plattform für automatisiert und dezentral ausführbare Software

LANDVERWALTUNG DURCH BLOCKCHAINS

Honduras to build land title registry using bitcoin technology

By Gertrude Chavez-Dreyfuss

Reuters 15 May 2015

A bitcoin sticker is seen in the window of the 'Vape Lab' ca
possible to both use and purchase the bitcoin currency, in
2015. REUTERS/Peter Nicholls/Files

By Gertrude Chavez-Dreyfuss

NEW YORK (Reuters) - Honduras, one of the poorest countrie
agreed to use a Texas-based company to build a permanent a
system using the underlying technology behind bitcoin, a com
Thursday.

Schweden nutzt jetzt offiziell die Blockchain für Grundbucheintragungen

7. Juli 2017 | Sven Wagenknecht

Schon seit 2016 ist bekannt, dass Schweden an einer Blockchain-Lösung diesbezüglich forscht. Ende Mai wurde dann die letzte Testphase erfolgreich abgeschlossen. Trotz der fortschrittlichen Digitalisierung des Grundbuchamtes, soll die Blockchain zu deutlichen Effizienzsteigerungen führen.

Konkret sollen so um die 100 Millionen Euro eingespart werden können, die für Bürokratie und Betrugsfälle jedes Jahr fällig werden. Das es tatsächlich zu so hohen Einsparungen kommt, bleibt jedoch zu bezweifeln. Darüber hinaus haben aber auch die Banken Interesse an dem Projekt, da sich so in der Zukunft auch Hypothekengeschäfte über eine Blockchain darstellen lassen. Entsprechend wundert es auch nicht, dass zwei schwedische Banken bei dem Projekt involviert sind.

Georgia: Authorities Use Blockchain Technology for Developing Land Registry

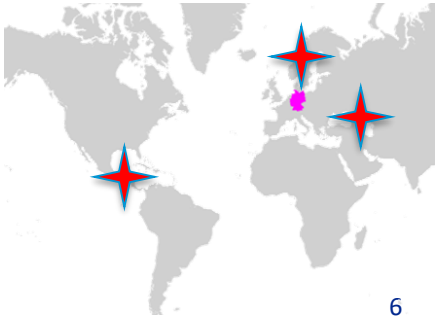
in Innovation

neering
erty

tcoin.

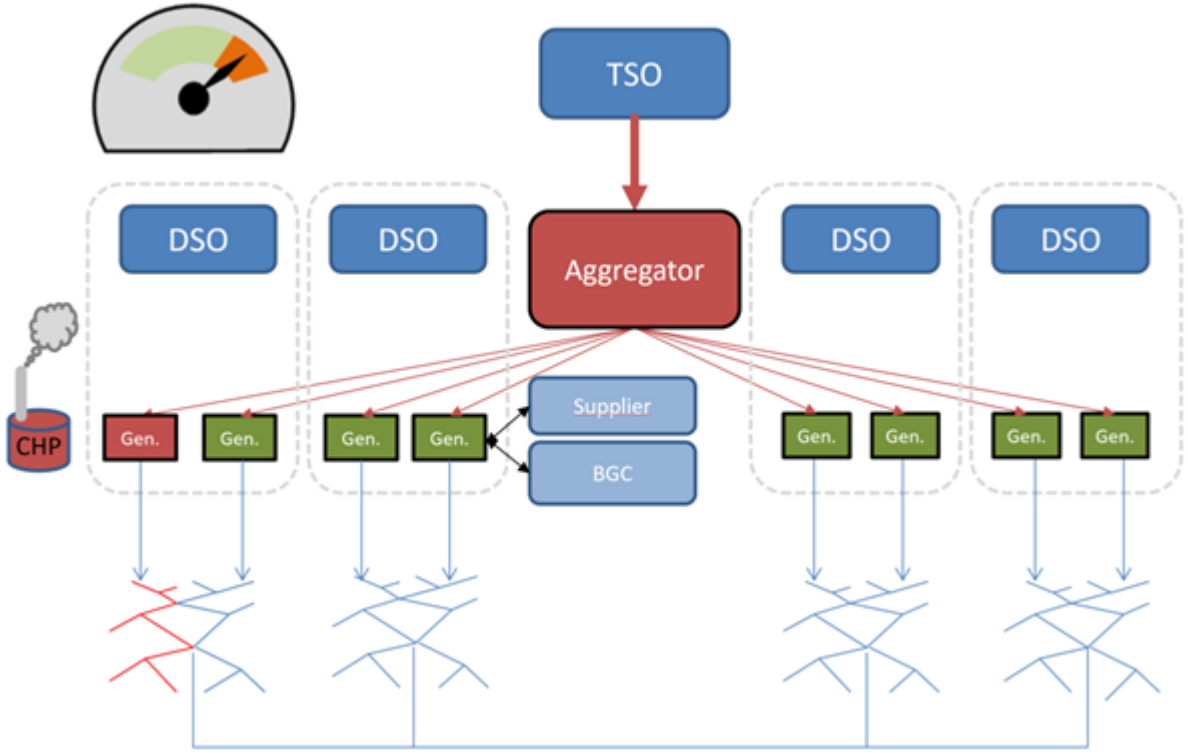
oping
an a
land
n
am
es,

The chairman of Georgia's National Agency of Public Registry, Mr. Papuna Ugrekhelidze, signs a new memorandum of understanding with the CEO of the BitFury Group, Mr. Valery



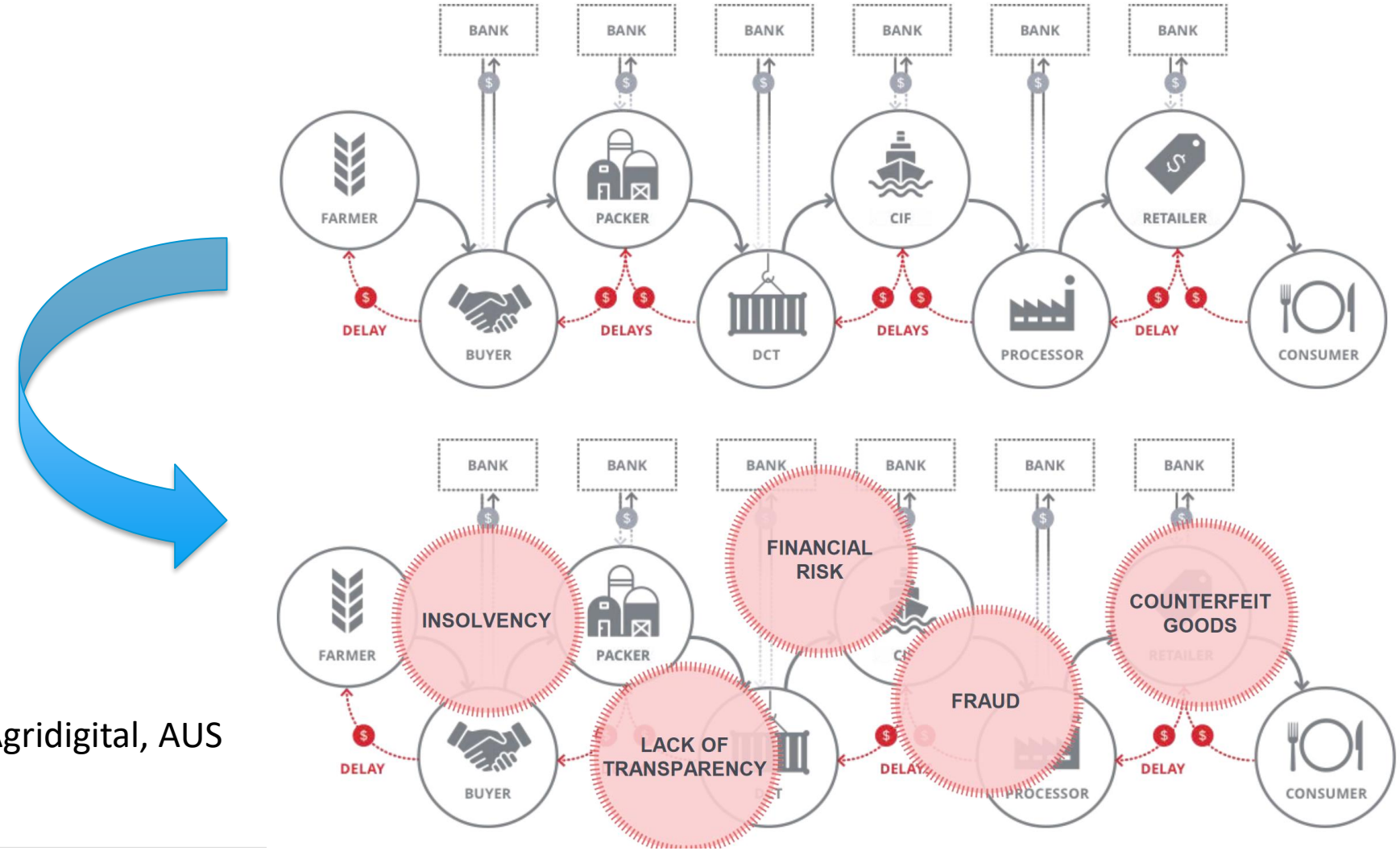
AUTOMATISCHER ENERGIEHANDEL UND NETZMANAGEMENT

- Netzmanagement: Projekt Gridchain (Fa. Ponton)
- Energiemanagement und Handel:
  - Projekt Enerchain (Fa. Ponton)
  - Solarcoin (Fa. Lykke)



Quelle: https://enerchain.ponton.de/index.php/16-gridchain-blockchain-based-process-integration-for-the-smart-grids-of-the-future

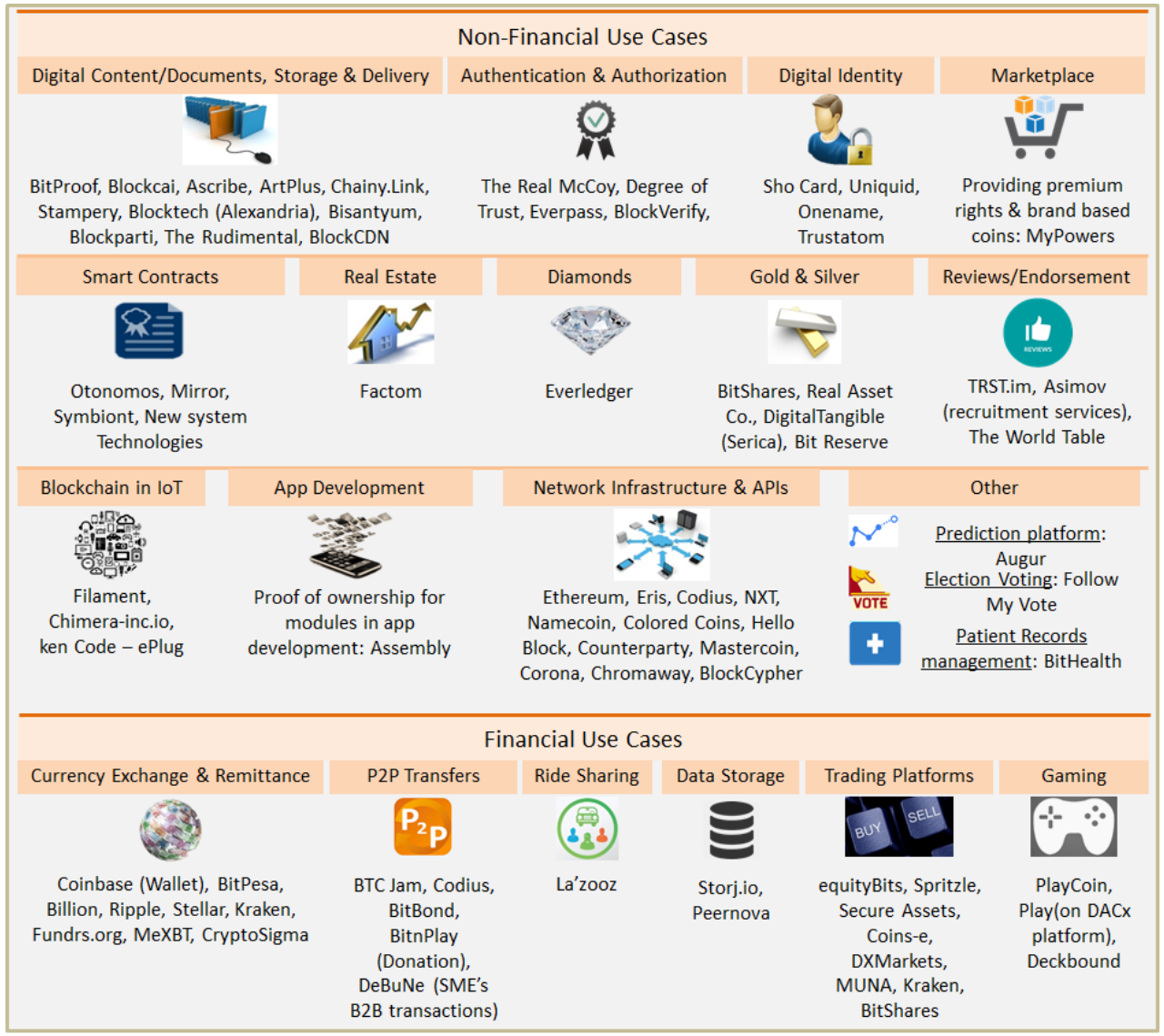
GLOBALER LEBENSMITTELHANDEL
BEISPIEL AGRIDIGITAL



Quelle: Agridigital, AUS

BLOCKCHAINS UND DLT - MEHR ALS NUR GELDTRANSFER

Quelle: https://marmelab.com/images/blog/blockchain_infographic.png



BLOCKCHAINS UND DLT
BEDEUTUNG FÜR DEUTSCHLAND UND EUROPA

- **Digitale Agenda und Demokratisierung**:
  - Blockchains bieten eine Basis für einen öffentlichen, sicheren Datenverkehr: Gerade für Deutschland sollten Blockchain-Aktivitäten durch öffentliche Projekte koordiniert werden. Sonst überholen internationale "Mega-Communities" disruptiv.
  - Internet-of-Things kann sensorseitig durch Blockchain-Mechanismen abgesichert werden – insbesondere in Industrie 4.0 und Smart City-Aktivitäten.
- **Öffentliche Verwaltung**: Auskunfts- und Informationspflichten können durch automatische Datenablage in Blockchains manipulationsfrei abgelegt werden (Beispiel Estland).
- **Gesetzgebung**:
  - Wie lässt sich ein internationales, anonymes System legislativ absichern? Hier ist die Europäische Kommission aktiv!
- **(Finanzmarkt-)Regulierung:**
  - Inflations- und Deflationsmechanismen lassen sich nicht mehr in gewohnter Art durchführen.
  - Steuergesetzgebung muss an internationale, anonyme Transaktionen angepasst werden. Es liegen sehr komplexe Urteile des EuGH vor.

STANDARDISIERUNG – WARUM EIGENTLICH (BLOCKCHAINS)?

Übliche Technologieevolution:

- Technologie 1.0: Präsentation, Verwaltung
- Technologie 2.0: Dynamische Modifikation von Inhalten
- Technologie 3.0: Mehrwerte durch Semantik = (automatisierte) Deutung von Inhalten
- Technologie 4.0: Dezentrale, automatisierte Anpassung und Steuerung

Grad an automatisierter Interaktivität

semantische und prozessuale Vergleichbarkeit von Inhalten =

Basis für Standardisierung!

ISO TC 307: "BLOCKCHAIN UND DISTRIBUTED LEDGER TECHNOLOGIES"

Historie

- Standards Australia (SA): Wunsch der Harmonisierung öffentlicher Transaktionen
- Ende 2014: Anfrage von SA an ISO zur Standardisierung von Blockchain-Technologien
- Ende 2016: Entscheidung auf ISO-Kongress zur Gründung des Gremiums mit 20:7:8
- 7.4.2017: Gründungssitzung in Sydney mit ca. 100 Teilnehmer aus ca. 20 Nationen

Government services that survey respondents would like to see using blockchain technologies to improve efficiencies and public access

Land Transfers and Property Title registrations	72.1%
Personal Identification and Passport Documentation	68.9%
Management of Health Records	65.6%
Vehicle Registrations	54.1%
Welfare Distribution and Monitoring	37.7%
Urban planning; wider pedestrian sidewalks, increased times for crossings	21.3%
Public Transport Scheduling	16.4%

Source: Blockchain survey, Standards Australia analysis

ISO TC 307: "BLOCKCHAIN UND DISTRIBUTED LEDGER TECHNOLOGIES" AKTIVITÄTEN

- Teilnehmer: 17 Mitgliedsstaaten, ca. 20 beobachtende Konsortien, NGOs und internationale Organisationen, ca. 200 weltweite Experten
- Arbeitsprogramm:
  - Terminology
  - Reference Architecture/Taxonomy/Ontology
  - Use Cases
  - Security/Privacy
  - Smart Contracts
  - Interoperability
  - Governance

France (AFNOR)	Korea, Republic of (KATS)
United States (ANSI)	Netherlands (NEN)
Austria (ASI)	Australia (SA)
United Kingdom (BSI)	China (SAC)
Germany (DIN)	Canada (SCC)
Denmark (DS)	Finland (SFS)
Malaysia (DSM)	Spain (UNE)
Russian Federation (GOST R)	Italy (UNI)
Japan (JISC)	

BLOCKCHAINS UND DLT
RISIKEN

- **Gefahr der Anonymität**: Absolute Anonymität ermöglicht Missbrauch für Straftaten.
- **Gefahr des absoluten Verlustes**: Durch Repräsentation der Identität durch Kryptokey entsteht Risko des absoluten Rechteverlustes bei Verlust des Private Keys.
- **Recht auf Vergessen**: Aktuelle Prinzipien speichern alle Transaktionen bis hin zum Ursprungsknoten – kein Vergessen. Lässt sich aber anpassen.
- **Datenmenge**: überlinear wachsende Datenmenge – wie weit weg von exponentiell (= unhandhabbar)?
- **Arbeitsaufwand/Energiebedarf:** Proof-of-Work Konzept gilt als Sicherstes, skaliert aber Sicherheit mit Arbeits- und Energiebedarf
- **Ausfallsicherheit/Nachvollziehbarkeit** eines vollständig elektronischen Systems: Aus dem alten Ägypten sind Dokumente in Stein und auf Papyrus über mehr als 5000 Jahre überliefert…

- zu guter Letzt: Blockchains müssen (sollten) Probleme lösen, die man nicht ohne diese besser lösen könnte

BLOCKCHAINS UND DLT
SECURITY UND PRIVACY ASPEKTE

- Proof-of-Work, Consensus und Distribution in Verbindung mit Hashing zunächst einmal grundsätzlich als sicher anzusehen
- **Identität** ist zunächst anonym, aufgrund der vollständigen Historie in manchen Systemen grundsätzlich trackbar und somit rekonstruierbar
- **größtes Risiko:** Proof-of-Work in Verbindung mit Distribution. Proof-of-Work-Ergebnis hängt von Rechenleistung ab. Rechenleistung ist kaufbar! Dadurch ist "Gewinnzufall" manipulierbar.
- **geringere Risiken**:
  - fehlende globale Zeitbasis in Verbindung mit Netzwerklatenzen: Ermitteln des korrekten PoW-Blocks bei mehreren zeitnah versendeten Ergebnissen.
  - lokale Nähe zu PoW-erfolgreichen Minern – z.B. in Mining Farms – hat Vorteile, schneller den nächsten korrekten Branch zu bilden und kann "Distribution" verzerren
  - Größe des Systems (130 GB Gesamttransaktionsgröße) schließt kleine Systeme vom Prozess aus
  - regionale "denial-of-service"-attacks
  - unzureichende Absicherung der Wallets
  - einseitige Änderung der Transaktionsregeln
  - Erzeugen und kommunizieren von double-blocks, damit Erzeugen von verwaisten Blocks

BLOCKCHAINS UND DLT
ZUSAMMENFASSUNG

Blockchains und Distributed Ledgers

- bilden im technologischen Zusammenhang eine disruptive Technologie
- bieten des Potenzial für einen gesellschaftlichen Wandel zur digitalen Transparenz ohne vertrauenswürdige Mittelsmänner
- bieten eine Basistechnologie mit hohem Sicherheitspotenzial, sind aber nicht per se sicher
- werden noch längst nicht überwiegend sinnvoll eingesetzt (fehlende und falsche use-cases)
- bedürfen (mindestens) zentral koordinierter Projekte, um gemeinsame Weiterentwicklungen zu ermöglichen
- erfordern legislative Maßnahmen, um Missbrauch zu reduzieren
- müssen vereinheitlicht werden (=standardisiert, genormt?), um vollständig inkompatible Basistechnologien (=Parallelgesellschaften) zu vermeiden