

BLOCKCHAINS IN DER STANDARDISIERUNG: ISO TC 307

Warum, was und mit wem?

Prof. Dr.-Ing. Volker Skwarek
Hochschule für Angewandte Wissenschaften Hamburg
16.06.2017

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

**semantische und prozessuale Vergleichbarkeit von Inhalten =
Basis für Standardisierung!**



Grad an
automatisierter
Interaktivität

STANDARDISIERUNG – WEITERE GRÜNDE

- konsensuale Suche nach einer besten gemeinsamen, übergreifenden Lösung
- Vermeidung von ineffizienten und wirtschaftlich ungewünschten Monopolstellungen
- Grundlage für Vereinbarungen der World Trade Organisation im gemeinsamen Welthandel
- (gewünschte) Basis für Erteilung öffentlicher Aufträge

Weiterentwicklung von Blockchain- und DLT erfordern Kommunikation und Kooperation zwischen Technologien → **Basis für einen Standard**

STANDARDISIERUNG – ÄNGSTE UND SORGEN

Standardisierung

- ist Bürokratie...: Ja – Für diejenigen, die aktiv mitmachen, damit **keine Meinung unberücksichtigt** bleibt.
- zwingt ein, weil zwingend...: Nein – fast gar kein Standard erzwingt etwas, sondern **bietet eine Basis** für gleichartige Kommunikation
- ist unnötig, weil sich das Beste am Markt sowieso durchsetzt...: gerade in globalen kommunikationsbasierten Technologien **funktioniert das oft nicht!**

Standards bieten denjenigen, die mitmachen, die **Chance, Commodity-Kosten zu senken**, um sich über relevante **Unterschiede zu differenzieren!**

ISO TC 307: „BLOCKCHAIN UND DISTRIBUTED LEDGER TECHNOLOGIES“

WARUM GIBT ES DIE, WAS MACHEN DIE? (1/2)

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“

WARUM GIBT ES DIE, WAS MACHEN DIE? (2/2)

- 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)	

ISO TC 307: „BLOCKCHAIN UND DISTRIBUTED LEDGER TECHNOLOGIES“

ARBEITSGRUPPE WG TERMINOLOGY

- noch nicht gestartet
- Vorsitz: befindet sich in internationaler Abstimmung. Voraussichtlich Canada, Universität von Toronto
- Beispiel der Definition eines (1) Termes (Auszug): Blockchain

This definition does not include (yet) the "may be reduced to a list" remark, since I did not fully understand its meaning. Is it referring to the fact that each path in the tree is a "list of blocks, securing itself"?

The term "tree" is scientifically correct and more general, but misleading as the standard blockchain is a linear list only – and not a tree. I would propose to add this into a Note 3: "Usual applications connect child and parent blocks to lists, which is only a specific form of the more general tree."

As for the other discussion. I agree with the separation to two different object ("The blockchain" and a "distributed ledger"), with some remarks.

1. I suggest to expand the definition of a distributed ledger you provided to:

"A distributed ledger is a communication protocol which is used to distribute transactions over a peer-to-peer network. The protocol contains a consensus mechanism ensuring data immutability"

ISO TC 307: „BLOCKCHAIN UND DISTRIBUTED LEDGER TECHNOLOGIES“

ARBEITSGRUPPE SG IDENTITY

- Gestartet am 8.6.2017
- Vorsitz: Prof. Nick Lee, Korea
- Status: Definition und Konkretisierung des Arbeitsauftrages

Scope

- Identify the types of identities and entity types needed for data and functionality within blockchains;
- Identify the identity management requirements needed outside a blockchain, upon which the operation of the blockchain depends, such as for data integrity and for access control;
- Review existing identity-related standards and identify which existing standards, and standards under development, could be relevant for ISO/TC 307;
- Identify any regulations that could impact the creation, use and management of identities in relation to blockchains;

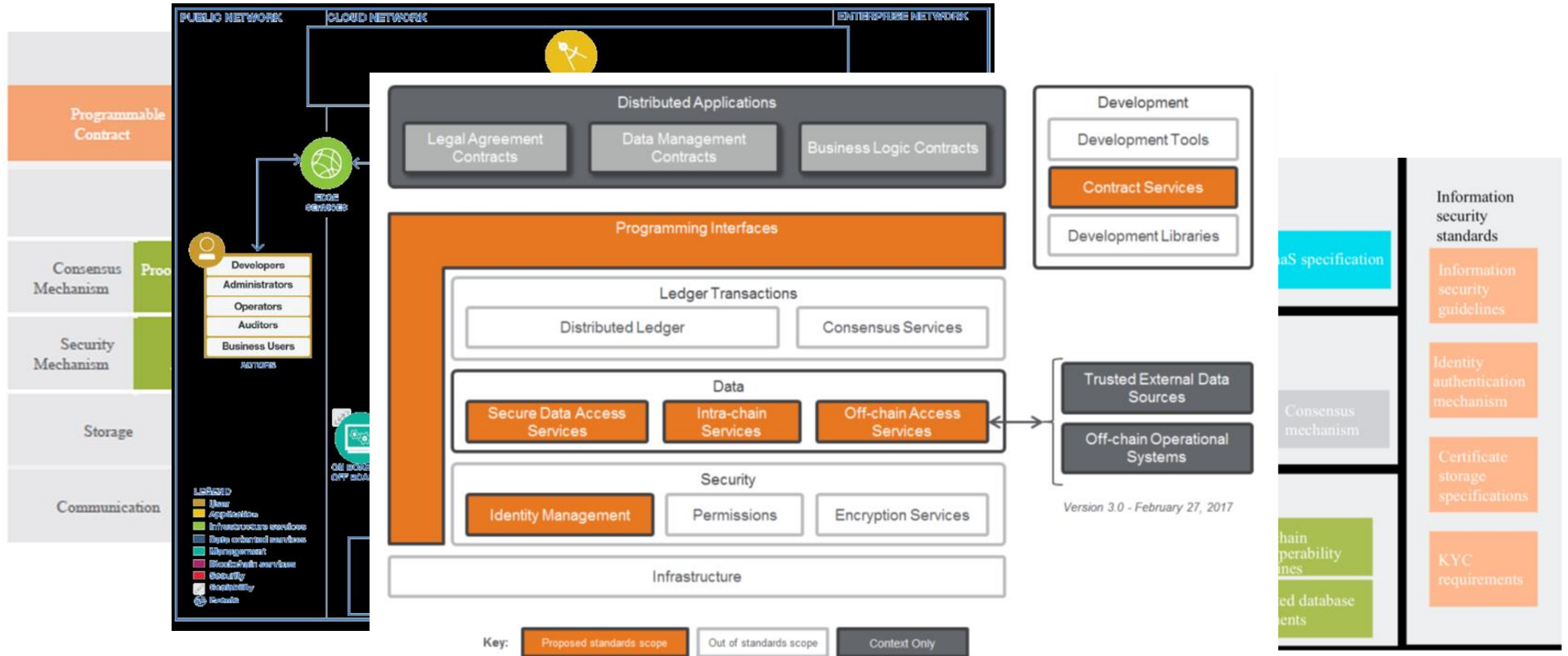
ISO TC 307: „BLOCKCHAIN UND DISTRIBUTED LEDGER TECHNOLOGIES“ ARBEITSGRUPPE SG TAXONOMY/ONTOLOGY/REFERENCE ARCHITECTURE

- Gestartet am 25.5.2017
- Vorsitz: Heather Kreger, USA
- Status: Definition und Konkretisierung des Arbeitsauftrages

Scope

- To **review Reference Architectures** from closely related fields, including ISO/IEC 17789 Cloud Computing Reference Architecture;
- To **produce a recommendation on how to proceed in the area of Reference Architecture**, Taxonomy and Ontology and NWIPs as appropriate;

ISO TC 307: „BLOCKCHAIN UND DISTRIBUTED LEDGER TECHNOLOGIES“ ARBEITSGRUPPE SG TAXONOMY/ONTOLOGY/REFERENCE ARCHITECTURE



ISO TC 307: „BLOCKCHAIN UND DISTRIBUTED LEDGER TECHNOLOGIES“

ARBEITSGRUPPE SG IDENTITY

- Gestartet am 8.6.2017
- Vorsitz: Prof. Nick Lee, Korea
- Status: Definition und Konkretisierung des Arbeitsauftrages

Scope

- Identify the types of identities and entity types needed for data and functionality within blockchains;
- Identify the identity management requirements needed outside a blockchain, upon which the operation of the blockchain depends, such as for data integrity and for access control;
- Review existing identity-related standards and identify which existing standards, and standards under development, could be relevant for ISO/TC 307;
- Identify any regulations that could impact the creation, use and management of identities in relation to blockchains;

ISO TC 307: „BLOCKCHAIN UND DISTRIBUTED LEDGER TECHNOLOGIES“

ARBEITSGRUPPE SG IDENTITY

- Gestartet am 8.6.2017
- Vorsitz: Prof. Nick Lee, Korea
- Status: Definition und Konkretisierung des Arbeitsauftrages

Scope

- Identify the types of identities and entity types needed for data and functionality within blockchains;
- Identify the identity management requirements needed outside a blockchain, upon which the operation of the blockchain depends, such as for data integrity and for access control;
- Review existing identity-related standards and identify which existing standards, and standards under development, could be relevant for ISO/TC 307;
- Identify any regulations that could impact the creation, use and management of identities in relation to blockchains;

ISO TC 307: „BLOCKCHAIN UND DISTRIBUTED LEDGER TECHNOLOGIES“

ARBEITSGRUPPE SG SMART CONTRACTS

- Gestartet am 16.5.2017
- Vorsitz: Prof. Volker Skwarek, Deutschland
- Status: Einigung auf eine Arbeitsdefinition und Aufstellen von Use Cases

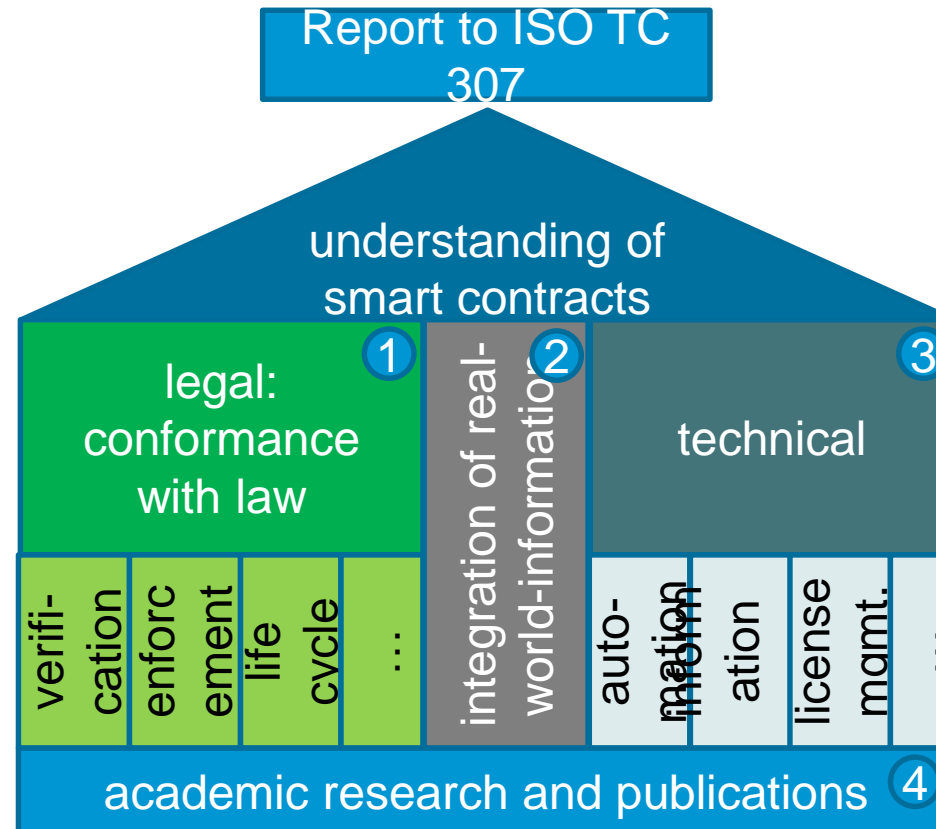
Scope

- The study group will consider **interoperability with the law**, including but not limited to the **verification, enforcement, and life cycle** of smart contracts.
- The study group will also consider **the transfer of the concept** [...] to other domains such as but not limited to **automation, machine2machine information transfer, license management**, as well as the integration of **real world information**
- Further the study group will consider the **application of programming methodology, domain specific language** to also enable non-programmers to express conditions.

ISO TC 307: „BLOCKCHAIN UND DISTRIBUTED LEDGER TECHNOLOGIES“

ARBEITSGRUPPE SG SMART CONTRACTS

Elemente von Smart Contracts



ISO TC 307: „BLOCKCHAIN UND DISTRIBUTED LEDGER TECHNOLOGIES“

ARBEITSGRUPPE SG SMART CONTRACTS

Draft elements of „homework“: Definition

- 9 contributions by 5 countries:
- decentral program on the chain, storing data, sending and receiving cryptocurrency
- programs on the chain, automatically triggered by factors basing on initial agreements
- (quasi) legal contract operated by software, with a penalty for breaching and even higher expenses for hacking it
- smart contracts encapsulate business logic
- smart contracts are like a game which two parties have agreed on the rules
- self-executable software code that runs without any risk of downtime, censorship, or fraud on the blockchain

first working draft

ISO TC 307: „BLOCKCHAIN UND DISTRIBUTED LEDGER TECHNOLOGIES“

ARBEITSGRUPPE SG SMART CONTRACTS

Draft elements of „homework“: Use Cases (1 of 2)

- 5 contributions by 4 countries:
 - smart contracts for energy market (direct energy trading) and control of stability of energy grid
 - data accountability and provenance tracking
 - single or permanent execution of a contract

first working draft

ZUSAMMENFASSUNG

- Standardisierung von Blockchain und DLT hat auf **internationaler Ebene gerade erst begonnen**
- Zeitraum: Standardisierungsabschluss **bis 2020**
- Es ist das Ziel, **offene und elementare Fragen** im internationalen Konsens zu **klären**
 - Begriffe/Terminologien
 - Referenzarchitekturen
 - Smart Contracts/Distributed Apps,
 - ...
- Es ist **nicht das Ziel**, einzelne **Blockchaintechnologien** zu bewerten oder zu **empfehlen/zu bevorzugen**

ISO TC 307: „BLOCKCHAIN UND DISTRIBUTED LEDGER TECHNOLOGIES“

ARBEITSGRUPPE SG SMART CONTRACTS

- Gestartet am 16.5.2017
- Vorsitz: Prof. Volker Skwarek, Deutschland
- Status: Einigung auf eine Arbeitsdefinition und Aufstellen von Use Cases

Scope

- The study group will consider **interoperability with the law**, including but not limited to the **verification, enforcement, and life cycle** of smart contracts.
- The study group will also consider **the transfer of the concept** [...] to other domains such as but not limited to **automation, machine2machine information transfer, license management**, as well as the integration of **real world information**
- Further the study group will consider the **application of programming methodology, domain specific language** to also enable non-programmers to express conditions.

Fragen?
Gerne! ...