

TeleTrust-Auditorium
„IT-Sicherheit“
it-sa Forum M10 - Management

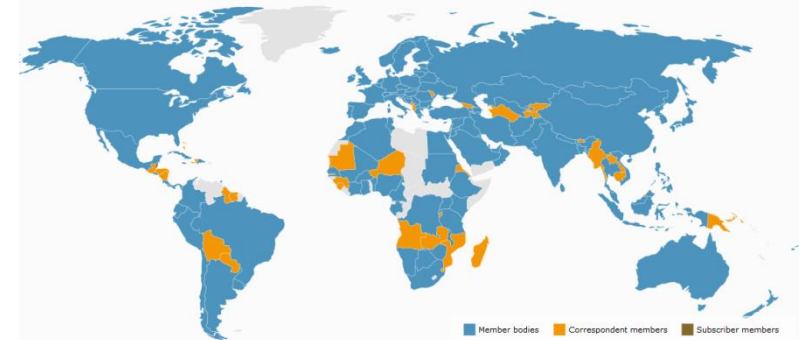
Nürnberg, 09.10.2018

Blockchain – Mit Standardisierung gegen Adoptionsbarrieren?

Dr. André Kudra, Leiter TeleTrust-AG "Blockchain" / esatus AG

Standardisierung über die International Organization for Standardization (ISO)

- ISO ist eine unabhängige nicht-staatliche internationale Organisation mit 162 nationalen Standardisierungsorganisationen (bspw. DIN in Deutschland) als Mitgliedern.
- Über Ihre Mitglieder kommen Experten zusammen um Wissen zu teilen und freiwillige, konsensbasierte und marktrelevante internationale Standards zu entwickeln, die Innovation fördern und Lösungen für globale Herausforderungen stellen.
- Internationale Standards liefern Spezifikationen für Produkte, Services und Systeme, um Qualität, Sicherheit und Effizienz zu gewährleisten. Sie sind wesentlich förderlich für internationalen Handel.
- ISO hat 22.336 internationale Standards und verwandte Dokumente publiziert, die fast alle Industrien abdeckt, von Technologie über Sicherheit zu Landwirtschaft und Gesundheitswesen. ISO Standards betreffen jeden überall.



<https://www.iso.org/about-us.html> | <https://www.iso.org/members.html>

ISO Leistungen – Verschiedene Arten von ISO-Publikationen

Publikation	Inhalt
International Standards	Ein Internationaler Standard stellt Regeln, Empfehlungen und Charakteristika von Aktivitäten oder deren Ergebnissen zur Verfügung. Zielsetzung ist die Erreichung eines optimalen Ordnungsgrades in einem bestimmten Kontext. Er kann verschiedene Formen annehmen. Neben Produktstandards gibt es bspw. Testmethoden oder Managementsysteme.
Technical Specification (ISO/TS)	Eine TS adressiert Arbeiten, die sich noch in der technischen Entwicklung befinden oder dort, wo davon ausgegangen werden kann, dass es eine zukünftige, aber nicht unmittelbare, Möglichkeit für die Vereinbarung eines internationalen Standards gibt. Sie wird zur unmittelbaren Verwendung veröffentlicht, stellt aber auch ein Mittel für die Erlangung von Feedback dar. Zielsetzung ist die spätere Überführung in einen Internationalen Standard.
Technical Report (ISO/TR)	Ein TR beinhaltet Informationen, die von den beiden vorherigen abweichen. Er kann bspw. Daten von einer Umfrage beinhalten, von einem Informationsreport oder von Informationen, die als "Stand der Technik" angesehen werden.
Publicly Available Specifications (ISO/PAS)	Eine PAS wird veröffentlicht, um ein dringliches Marktbedürfnis zu adressieren, und repräsentiert Konsens von Experten in einer Arbeitsgruppe oder den Konsens einer Organisation extern zur ISO. Wie bei TS wird sie zur unmittelbaren Verwendung und zur Erlangung von Feedback veröffentlicht für die spätere Überführung in einen Internationalen Standard. Maximale Lebensspanne ist sechs Jahre, nach der sie entweder überführt wurde oder zurückgezogen wird.
International Workshop Agreements (IWA)	Ein IWA ist ein Dokument, das außerhalb der normalen ISO-Komiteesystems mit Marktteilnehmern in einem "offenen Workshop" entwickelt wird. Sie werden typischerweise von einer Mitgliedsorganisation administrativ unterstützt. Die Publikation enthält Indikationen über die mitwirkenden Organisationen. Maximale Lebensspanne ist sechs Jahre, nach der sie entweder in eine andere ISO-Publikation überführt wurde oder zurückgezogen wird.
ISO Guides	Orientierungshilfe, die den Leser unterstützt, mehr über einen Bereich zu erfahren, in dem Standards Mehrwert schaffen.

<https://www.iso.org/deliverables-all.html>

Blockchain-Standardisierung auf internationalem Level via ISO

🔒 ISO/TC 307 Blockchain and distributed ledger technologies

🔒 Scope: Standardisation of blockchain technologies and distributed ledger technologies.

🔒 Gestartet in 2016

🔒 Secretariat Standards Australia

🔒 Zwei Präsenzmeetings im Jahr

🔒 39 Participating Members,
12 Observing Members

🔒 Diverse Liaisons außerhalb ISO

EC - European Commission, EEA Inc. - Enterprise Ethereum Alliance Inc., FIG - International Federation of Surveyors, IEEE - Institute of Electrical and Electronics Engineers, ITU - International Telecommunication Union, SWIFT - Society for Worldwide Interbank Financial Telecommunication, UNECE - United Nations Economic Commission for Europe

Arbeitsgruppe	Inhalte
ISO/TC 307/CAG 1	Convenors coordination group
ISO/TC 307/JWG 4	Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Blockchain and distributed ledger technologies and IT Security techniques
ISO/TC 307/SG 2	Use cases
ISO/TC 307/SG 6	Governance of blockchain and distributed ledger technology systems
ISO/TC 307/SG 7	Interoperability of blockchain and distributed ledger technology systems
ISO/TC 307/WG 1	Foundations
ISO/TC 307/WG 2	Security, privacy and identity
ISO/TC 307/WG 3	Smart contracts and their applications

<https://www.iso.org/committee/6266604.html>

Standards und Projekte in der Entwicklung unter Verantwortung von ISO/TC 307

- ▶ ISO/CD 22739 Terminology
- ▶ ISO/NP TR 23244 Overview of privacy and personally identifiable information (PII) protection
- ▶ ISO/NP TR 23245 Security risks and vulnerabilities
- ▶ ISO/NP TR 23246 Overview of identity management using blockchain and distributed ledger technologies
- ▶ ISO/AWI 23257 Reference architecture
- ▶ ISO/AWI TS 23258 Taxonomy and Ontology
- ▶ ISO/AWI TS 23259 Legally binding smart contracts
- ▶ ISO/NP TR 23455 Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems
- ▶ ISO/NP TR 23576 Security of digital asset custodians
- ▶ ISO/NP TR 23578 Discovery issues related to interoperability

<https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0>

Weitere internationale Standardisierung – World Wide Web Standards via W3C

- ▶ **About W3C** The World Wide Web Consortium (W3C) is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards. Led by Web inventor and Director Tim Berners-Lee and CEO Jeffrey Jaffe, W3C's mission is to lead the Web to its full potential.
- ▶ **W3C Mission** The W3C mission is to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web. W3C's standards define key parts of what makes the World Wide Web work.
- ▶ **W3C Groups** A variety of W3C groups enable W3C to pursue its mission through the creation of Web standards, guidelines, and supporting materials. Community and Business Groups offer more ways for innovators to bring work to W3C.
- ▶ **Credentials Community Group** The mission of the W3C Credentials Community Group is to explore the creation, storage, presentation, verification, and user control of credentials. We focus on a verifiable credential (a set of claims) created by an issuer about a subject—a person, group, or thing—and seek solutions inclusive of approaches such as: self-sovereign identity; presentation of proofs by the bearer; data minimization; and centralized, federated, and decentralized registry and identity systems. Our tasks include drafting and incubating Internet specifications for further standardization and prototyping and testing reference implementations.

W3C Credentials Community Group – Identity-relevante Standardisierungsbeiträge

▶ **Decentralized Identifiers (DIDs) v0.11**

Draft Community Group Report, 23 August 2018

Decentralized Identifiers (DIDs) are a new type of identifier for verifiable, "self-sovereign" digital identity. DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority. DIDs are URLs that relate a DID subject to means for trustable interactions with that subject. DIDs resolve to DID Documents — simple documents that describe how to use that specific DID. Each DID Document contains at least three things: cryptographic material, authentication suites, and service endpoints. Cryptographic material combined with authentication suites provide a set of mechanisms to authenticate as the DID subject (e.g. public keys, pseudonymous biometric protocols, etc.). Service endpoints enable trusted interactions with the DID subject.

▶ **Verifiable Claims Use Cases 1.0**

Final Community Group Report, 01 May 2017

A verifiable claim is a qualification, achievement, quality, or piece of information about an entity's background such as a name, government ID, payment provider, home address, or university degree. Such a claim describes a quality or qualities, property or properties of an entity which establish its existence and uniqueness. The use cases outlined here are provided in order to make progress toward possible future standardization and interoperability of both low and high-stakes claims with the goals of storing, transmitting, and receiving digitally verifiable proof of attributes such as qualifications and achievements. The use cases in this document focus on concrete scenarios that the technology defined by the group should address.

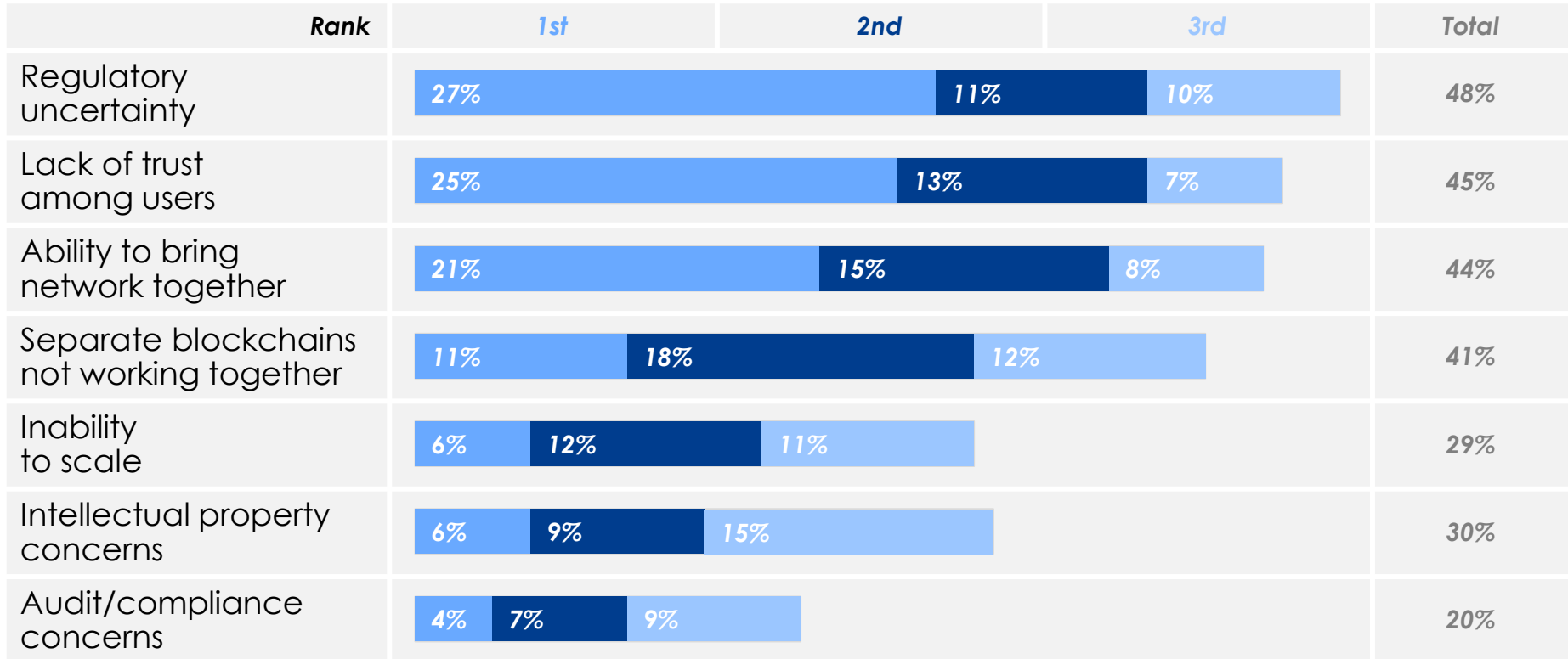
▶ **Verifiable Claims Data Model and Representations 1.0**

Final Community Group Report, 01 May 2017

A self-sovereign architecture for verifiable claims is one where the holder of a verifiable claim is in complete control of their identifier, where their verifiable claims are stored, and how they are used. There is currently no widely used self-sovereign, privacy-enhancing standard for expressing and transacting verifiable claims (aka: credentials, attestations) via the Web. This specification describes a data model for a digital identity profile and a collection of digital entity credentials that assert verifiable claims about that identity profile. It also describes how to express that data model in JSON, JSON-LD, and WebIDL.

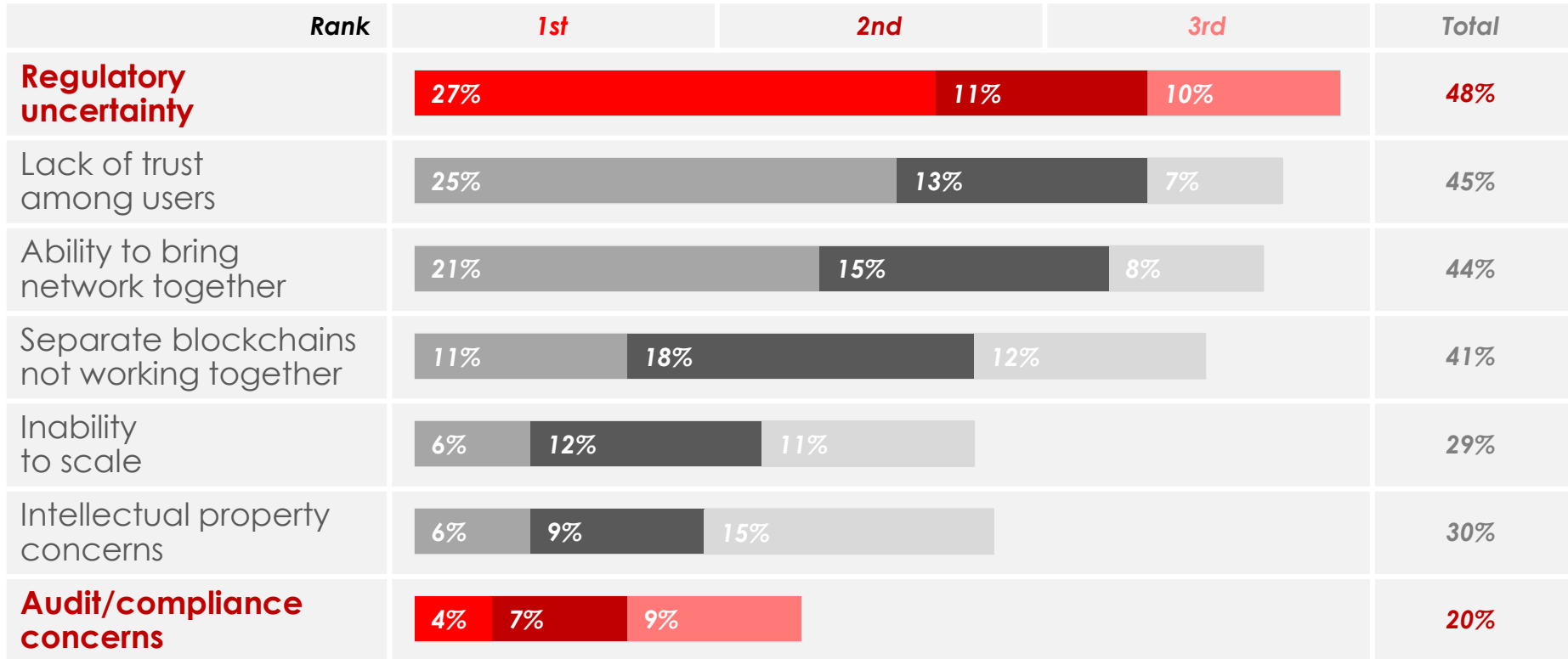
<https://w3c-ccg.github.io/did-spec> | <https://www.w3.org/2017/05/vc-use-cases/CGFR/2017-05-01> | <https://www.w3.org/2017/05/vc-data-model/CGFR/2017-05-01>

Die größten Adoptionsbarrieren



Quelle: PwC Global Blockchain Survey 2018 | <https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html>

Die größten Adoptionsbarrieren



Quelle: PwC Global Blockchain Survey 2018 | <https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html>

Sequenzielle Roadmap?



1. Technische Entwicklung _____



2. Standardisierung _____



3. Rechtliche Rahmenbedingungen _____



4. Marktdurchdringung _____



Vielen Dank für
Ihr Interesse!







CIO

Dr. André Kudra

Tel.: +49 6103 90295-0

a.kudra@esatus.com

esatus AG | www.esatus.com

Copyright © 2018 esatus AG. Alle Rechte vorbehalten

Alle Inhalte, Fotos und Grafiken sind urheberrechtlich geschützt. Sämtliche Teile dieses Dokuments dürfen nicht ohne vorherige schriftliche Genehmigung durch die esatus AG weder ganz noch auszugsweise kopiert, vervielfältigt, verändert oder übertragen werden.

Herausgeber: esatus AG

Copyright Fotos: Tomasz Zajda/Fotolia; bismillah_bd/Fotolia; Puckung/Fotolia; tostphoto/Fotolia; envfx/Fotolia; sdecoret/Fotolia