10. – 13.12.2018
Frankfurt am Main

#ittage

Dr. André Kudra, esatus AG

Mit der Blockchain zurück zur eigenen Datenhoheit

Ein Exkurs zu Bring Your Own Identity

Agenda

esatus® AG
Enforcing Information Security

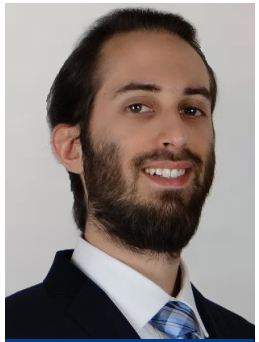
1. Self Sovereign Identity & Bring Your Own Identity
2. Die Vorzüge der Blockchain Technologie
3. Dezentralisiertes Vertrauen realisiert mit Sovrin
4. Internationale Blockchain-Standardisierung
5. Die aktuell größten Adoptionsbarrieren
6. Status und mögliche Entwicklung

esatus AG
Enforcing Information Security

Einführung
1. Self-Sovereign Identity & Bring Your Own Identity

Das **esatus** Blockchain Team

esatus® AG
Enforcing Information Security



Marcello di Biase

Marcello di Biase studied mathematics at the Goethe University in Frankfurt and finished with a master's degree. He focused on number theory and dynamical systems with computer science as a secondary subject. Today he is working as an IT Security consultant at esatus and is also part of the Blockchain team.

With special interest in processes and algorithms, he pays close attention to development in Blockchain technology and smart contracts in particular.

Dr. André Kudra

André Kudra studied business administration with a focus on information management at the European Business School (ebs) and computer science at the James Madison University (JMU). He finished his studies with the degrees Diplom-Kaufmann of the ebs and Bachelor of Science of the JMU. He finalized his academic career with a doctorate at the ebs in which he analyzed resistance against IT-based change in the public sector.

He is a Blockchain enthusiast as he believes this is the next big thing after the Internet. He is especially focused on promoting the advantages of Digital Identity via distributed ledgers.

Sebastian Pirozhkov

Sebastian Pirozhkov is an undergraduate at the Ludwig Maximilians University in Munich. He is currently studying mathematics with his minor in economics. Sebastian early on dived into technical research about the Blockchain as he is highly attracted to decentralized empowerment. After several months of self-driven work on the Blockchain topic he joined the esatus Blockchain team.

As a founding member of the team, he strives to transfer Blockchain knowledge to new esatus consultants and eagerly drives forward all Blockchain developments.

Christopher Hempel

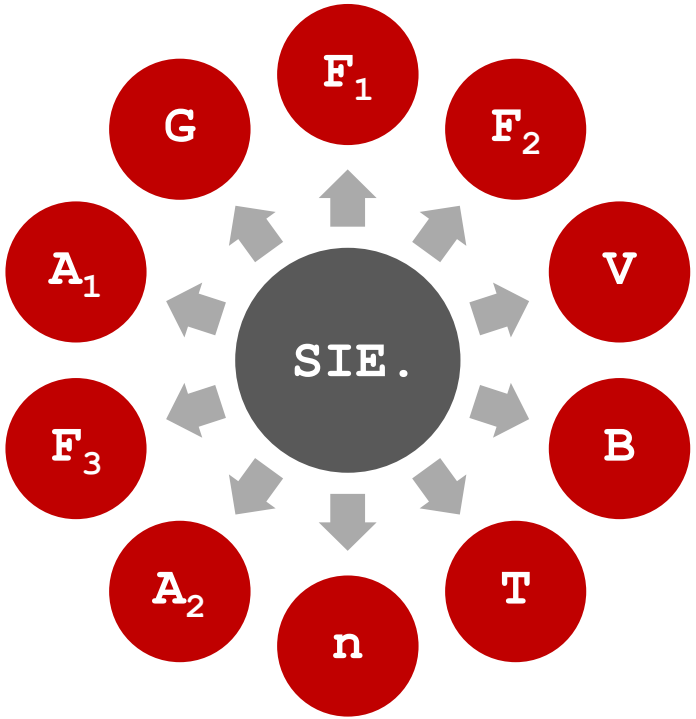
Christopher Hempel studied computer science at Hochschule Darmstadt – University of Applied Sciences. He completed his bachelor's degree by designing and implementing a virtualized test and development environment for information security software solutions.

He is interested in classic computing but eagerly absorbs new technologies. To the Blockchain team he contributes with his profound technical skills and experiences as developer. He is the lead developer of the esatus I&A prototypes, which leverage Sovrin and Ethereum technologies.

Die digitale Identität ist eines der schwierigsten Probleme in unserer vernetzten Welt

esatus® AG
Enforcing Information Security

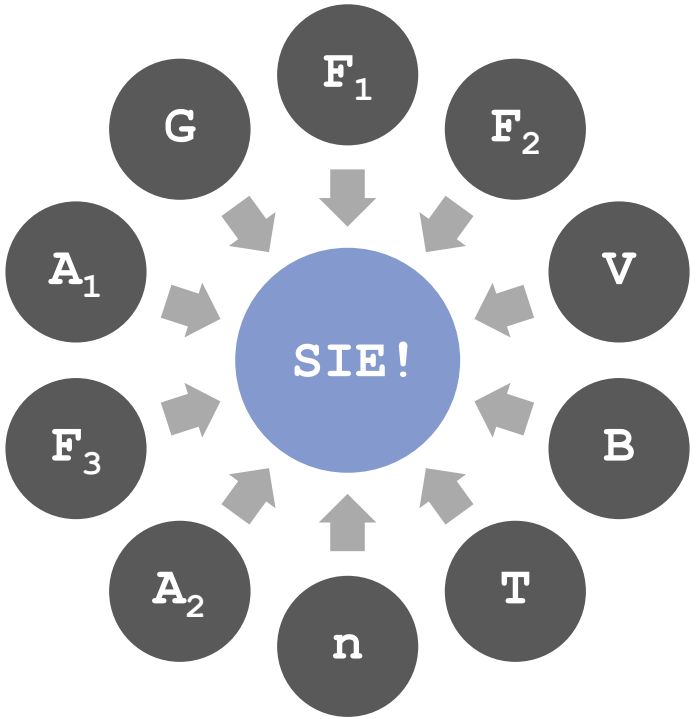
- In einer vernetzten Welt besitzen nur Maschinen Identitäten, nicht die Menschen
- Jeder genutzte Online-Service zwingt uns dazu, eine neue digitale Identitäten anzulegen
- Der Umgang mit Accounts und Passwörtern ist ein ständiger Kampf – der schwer zu gewinnen ist
- Jeder Service sammelt Daten über seine Nutzer – mit unbekanntem Zweck und zum eigenem Vorteil
- Diese Art der digitalen Identität kann entzogen werden oder ihre Regeln können geändert werden
- SIE HABEN KEINE KONTROLLE!
  SIE SOLLTEN SIE ABER HABEN!!!



Durch die Self-Sovereign Identity erhält der Nutzer die Kontrolle über seine Daten zurück

esatus® AG
Enforcing Information Security

- Eine Self-Sovereign Identity gehört zu 100% einer Person und wird nur von ihr kontrolliert
- Niemand kann sie ohne Zustimmung des Eigners einsehen, nutzen, abschalten oder wegnehmen
- Eine Self-Sovereign Identity ist privat, sehr sicher und bewegt sich flexibel mit ihrem Eigentümer
- Alles richtet sich auf den Nutzer aus – genau so wie es sein soll
- **BRING YOUR OWN IDENTITY** wird endlich möglich



esatus AG
Enforcing Information Security

Technik

2. Die Vorzüge der Blockchain-Technologie

Warum Blockchain für Identity & Access?

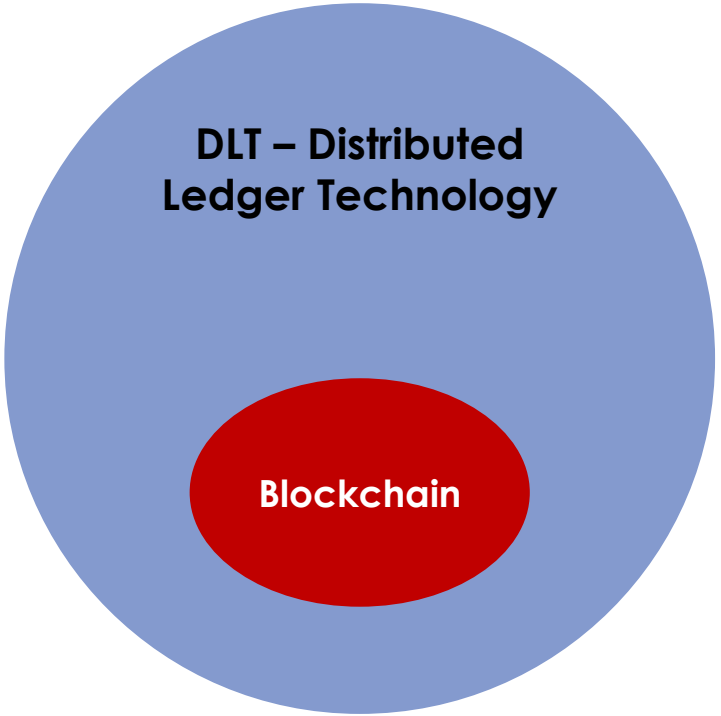
esatus AG
Enforcing Information Security

Gute Gründe gegen Blockchain…	Aber…
• Es gibt bereits etablierte I&A Software am Markt • Ökologisch und ökonomisch bessere Lösung • Schneller Support möglich	• Alles ist zentral gesteuert → Abhängigkeit & Single Point of Failure • Wem soll der Kunde die Identität anvertrauen? → Datenschutz • Zu viele Lösungen am Markt, keine Integration → Identity Spam

Nutzung der Distributed Ledger Technology für digitale Identitäten

esatus® AG
Enforcing Information Security

- Dezentralisiertes Ledger
- Transaktionen bestätigt durch Konsens-Algorithmus
- Teilnehmer sind Nodes / Nutzer / Miner
- Alle Informationen befinden sich auf allen Nodes
- Integrität wird durch Verkettung sichergestellt
- Authentizität durch asymmetrische Verschlüsselung
- Technische Durchsetzung der CIA-Triade:
  Confidentiality | Integrity | Availability
  Vertraulichkeit | Integrität | Verfügbarkeit
- Geeignet für Kryptowährungen, Supply Chains, Nachverfolgungen und **digitale Identitäten!**



Blockchains sind nicht immer gleich: Welches Konzept ist das richtige?

esatus® AG
Enforcing Information Security

- ▲ Robustheit
- ▲ Teure Angriffe
- ▲ Transparenz
- ▼ Träge Änderungen
- ▼ Langsamer Konsens

- ▼ Kein sinnvolles Anwendungsszenario

- ▲ Robustheit
- ▲ Berechtigungen
- ▲ Transparenz
- ▲ Schneller Konsens
- ▲ Rollback möglich
- ▼ Missbrauch möglich

- ▲ Berechtigungen
- ▲ Schneller Konsens
- ▲ Rollback möglich
- ▼ Missbrauch möglich
- ▼ Erprobtere Datenbanken

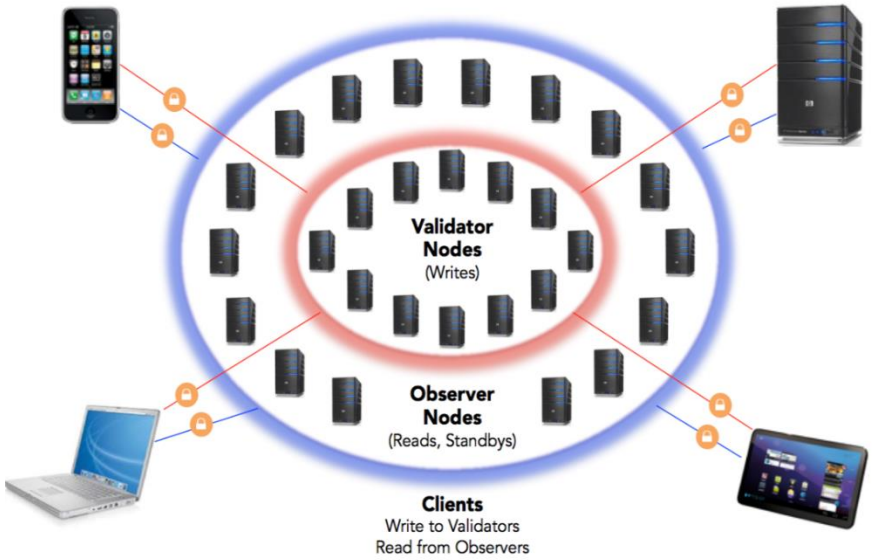
esatus AG
Enforcing Information Security

Beispiel
3. Dezentralisiertes Vertrauen realisiert mit Sovrin

Beispiel Sovrin: Modell für Self-Sovereign Identity & dezentralisiertes Vertrauen

esatus AG
Enforcing Information Security

- Globales DLT-basiertes Identitätsnetzwerk
- Nutzt dezentralisierte Identifikatoren (DIDs)
- Schneller und energiesparender Konsens (RBFT: Redundant Byzantine Fault Tolerance)
- Verwaltet durch Non-Profit-Organisation
- Diverse „Stewards" verpflichten sich zu einem Trust Framework und betreiben die Nodes
- Cross-funktional mit anderen Identity Chains
- Open Source Softwarebasis
- Teil von Hyperledger Indy



sovrin
identity for all

https://sovrin.org/wp-content/uploads/2017/04/The-Technical-Foundations-of-Sovrin.pdf (page 7)

esatus AG
Enforcing Information Security

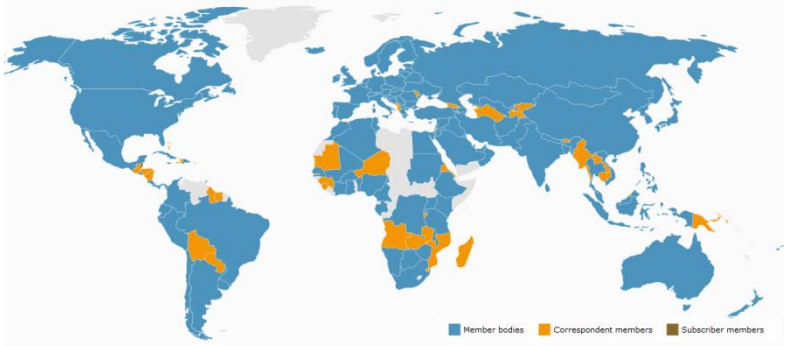
Standardisierung

4. Internationale Blockchain-Standardisierung

Standardisierung über die International Organization for Standardization (ISO)

esatus AG
Enforcing Information Security

- 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 22.399 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

esatus® AG
Enforcing Information Security

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

esatus AG
Enforcing Information Security

- **ISO/TC 307 Blockchain and distributed ledger technologies**
- Scope: Standardisation of blockchain technologies and distributed ledger technologies.
- Gestartet in 2016
- Secrectariat Standards Australia
- Zwei Präsenzmeetings im Jahr
- 39 Participating Members, 12 Observing Members
- Diverse Liaisons außerhalb ISO

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

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

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

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

esatus AG
Enforcing Information Security

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

esatus® AG
Enforcing Information Security

- **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.

https://www.w3.org/Consortium | https://www.w3.org/community/credentials

W3C Credentials Community Group – Identity-relevante Standardisierungsbeiträge

esatus® AG
Enforcing Information Security

- **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

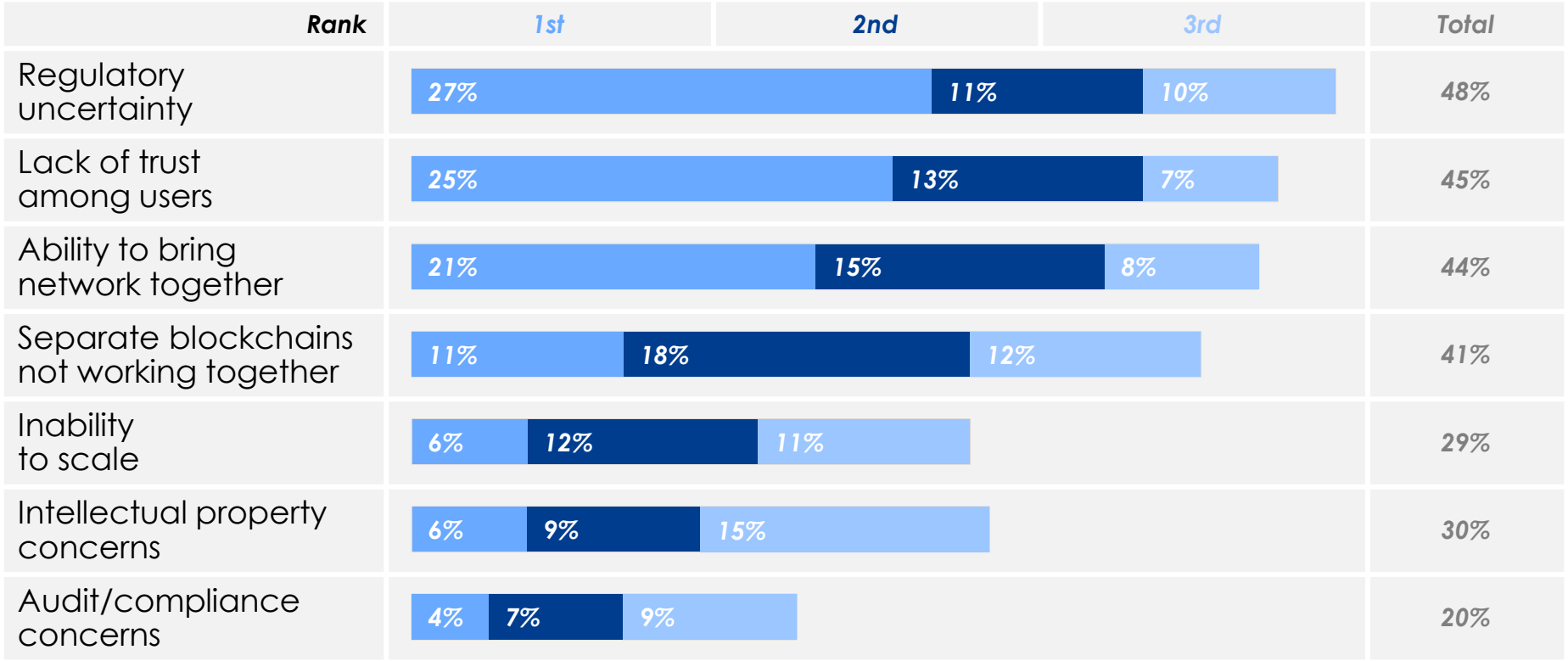
esatus AG
Enforcing Information Security

Regulatorik

5. Die aktuell größten Adoptionsbarrieren

Die größten Adoptionsbarrieren

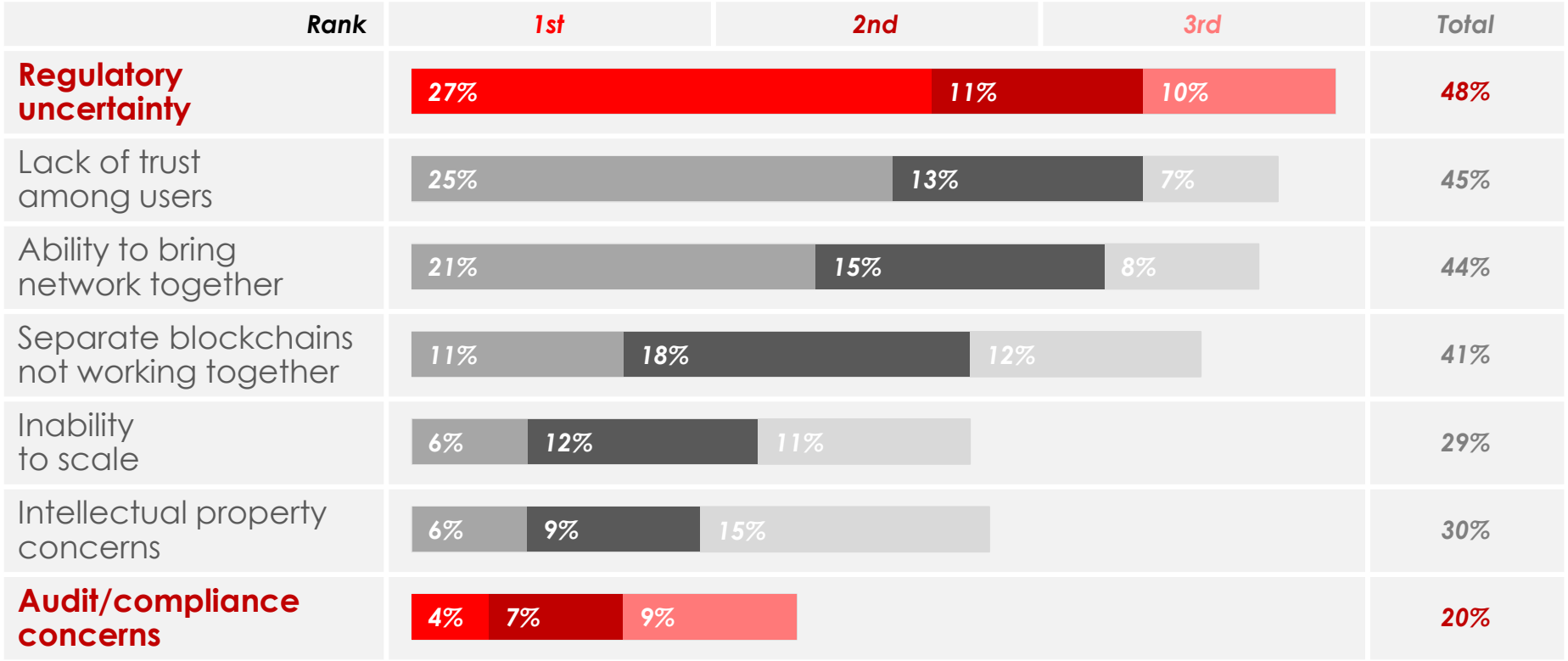
esatus AG
Enforcing Information Security



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

Die größten Adoptionsbarrieren

esatus® AG
Enforcing Information Security



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

esatus AG
Enforcing Information Security

Ausblick

6. Status und mögliche Entwicklung

Status und mögliche Entwicklung

esatus® AG
Enforcing Information Security

1. Technische Entwicklung

2. Standardisierung

3. Rechtliche Rahmenbedingungen

4. Marktdurchdringung

Fragen & Diskussion

esatus® AG
Enforcing Information Security

esatus® AG
Enforcing Information Security

Vielen Dank für Ihre Aufmerksamkeit!

Ihr Blockchain Ansprechpartner

esatus AG
Enforcing Information Security

CIO esatus AG und Leiter Blockchain AG TeleTrusT

Dr. André Kudra

Telefon: +49 6103 90295-0

Mail: a.kudra@esatus.com

IT-Tage 2018 Sprecher 10. - 13.12.2018 Frankfurt am Main

Copyright

esatus AG
Enforcing Information Security

Herausgeber: esatus AG

Copyright Fotos: Tomasz Zajda/Fotolia; bismillah_bd/Fotolia; tostphoto/Fotolia; envfx/Fotolia; opka/Fotolia; andrei45454/Fotolia