

## **TeleTrust-Informationstag "Blockchain"**

**Berlin, 27.06.2018**

# **Identity und PKI – Symbiose möglich?**

**Dr. André Kudra**

**CIO esatus AG und Leiter Blockchain AG TeleTrust**

# Das esatus Blockchain Team



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.



Philipp Lang

Philipp Lang earned a bachelor of science degree in mathematics at the Goethe University in Frankfurt. He is currently pursuing his master of science degree in computer science. In parallel to his studies, he worked at the technology branch of a major German logistics enterprise. After completing his bachelor degree he started as an IT Security consultant at esatus where he first got in contact with Blockchain.

He is now contributing to the esatus Blockchain research and facilitates development of Blockchain based Identity & Access solutions.



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.



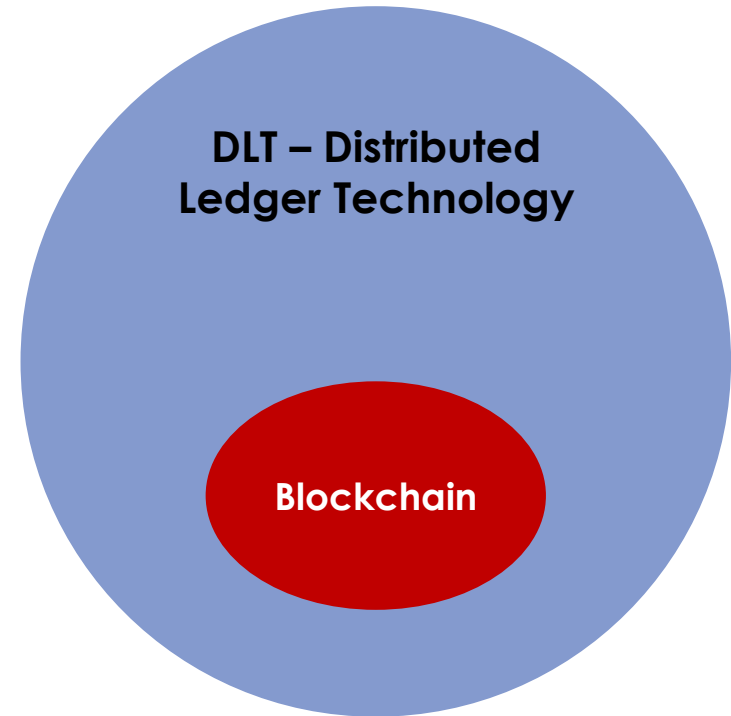
Christopher Hempel

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.

# Nutzung der Distributed Ledger Technology für digitale Identitäten

- 🔒 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?

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

- ▼ Kein sinnvolles Anwendungsszenario

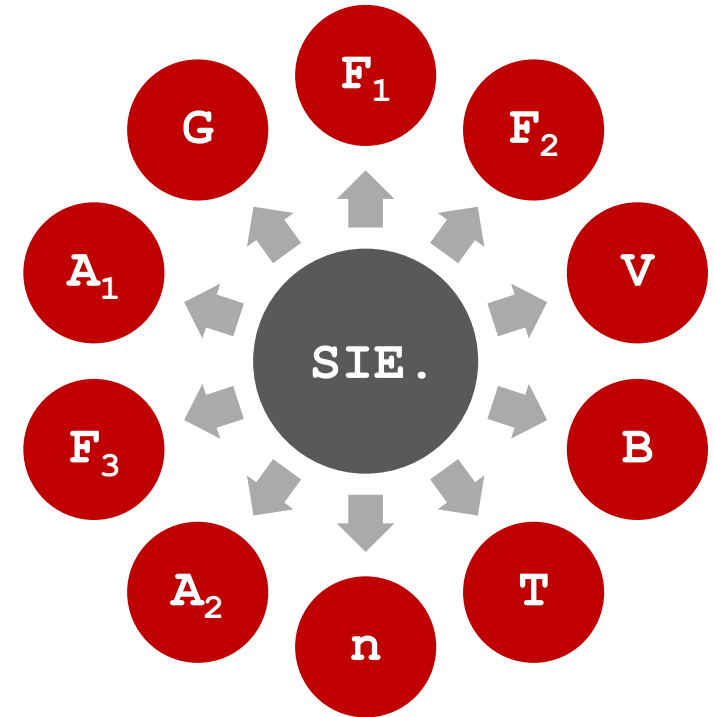
		Wer kann validieren?	
		Permissionless	Permissioned
Wer hat Zugriff?	Public	„Jeder darf lesen und validieren“   <b>bitcoin</b> <small><a href="https://bitcoin.org">https://bitcoin.org</a></small>	„Jeder darf lesen, nur Berechtigte validieren“   <b>sovrin</b> <small><a href="https://sovrin.org">https://sovrin.org</a></small>
	Private	„Nur Berechtigte dürfen lesen, jeder darf validieren“	„Nur Berechtigte dürfen lesen und validieren“   <b>c.rda</b> <small><a href="https://www.corda.net">https://www.corda.net</a></small>

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

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

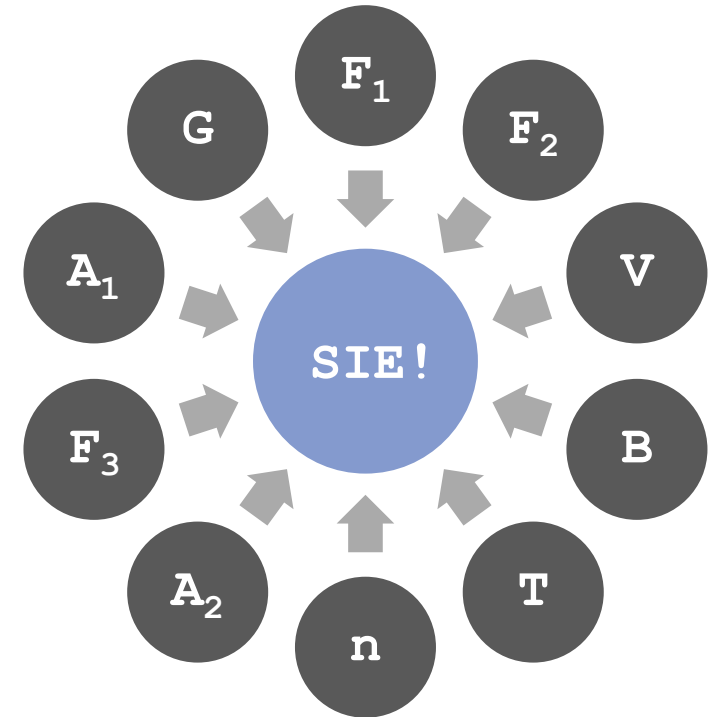
# Die digitale Identität ist eines der schwierigsten Probleme in unserer vernetzten Welt

- 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

- 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



# PKI vs. Blockchain Identity: Kriterien zur vergleichenden Betrachtung

Kriterium	Bedeutung/Verständnis
<b>Organisation</b>	Organisatorische Strukturen, die das Konstrukt betreiben
<b>Steuerung</b>	Steuerungsmechanismen, die das Konstrukt steuern und Entscheidungen treffen
<b>Technik</b>	Technische Systeme und Infrastrukturkomponenten, die den Betrieb des Konstrukts sicherstellen
<b>Vertrauensbildung</b>	Mechanismen der Vertrauensbildung innerhalb des Konstrukts
<b>Effizienz</b>	Wirtschaftliche und energetische Effizienz des Konstrukts
<b>Angriffsvektoren</b>	Mögliche Angriffsvektoren gegen das Konstrukt
<b>Regulatorik</b>	Verfügbare verlässliche rechtliche Bedingungen, die das Konstrukt betreffen
<b>Transparenz</b>	Nachvollziehbarkeit der durch das Konstrukt unterstützten Transaktionen und Entscheidungen
<b>Reifegrad</b>	Organisatorischer und technischer Reifegrad des Konstrukts
<b>Verbreitung</b>	Verbreitungsgrad des Konstrukts in der praktischen Anwendung
<b>Zukunftssicherheit</b>	Erwartung zur Zukunftssicherheit des Konstrukts
<b>Interoperabilität</b>	Interaktionsmöglichkeit zwischen verschiedenen Instanzierungen des Konstrukts
<b>Skalierbarkeit</b>	Skalierbarkeit des Konstrukts, um sehr hohe Anwenderzahlen zu ermöglichen
<b>Integrationsaufwand</b>	Integrationsaufwand für die Nutzbarmachung des Konstrukts allgemein und in Fachanwendungen
<b>Endanwenderkreis</b>	Mögliche Zielgruppe für die praktische Anwendung des Konstrukts

# Gegenüberstellung PKI und Blockchain Identity

Kriterium	PKI	Public Permissionless	Public Permissioned
<b>Organisation</b>	Zentralistisch (bspw. ein Unternehmen)	Dezentral („freiwillige“ Betreiber)	Dezentral (selektierte Betreiber)
<b>Steuerung</b>	Betreiberorganisation	„Community“	Konsortium
<b>Technik</b>	Hierarchische Server	Verteilte Nodes	Verteilte Nodes
<b>Vertrauensbildung</b>	Vertrauen in zentrale Entität	Konsensmechanismus	Vertrauen in Konsortium, Konsens
<b>Effizienz</b>	Hoch da singulärer Aufbau	Gering da paralleler Wettlauf (PoW)	Hoch da „alternativer“ Konsens
<b>Angriffsvektoren</b>	CA Kompromittierung (z. B. DigiNotar)	51%-Attacke	Kompromittierung
<b>Regulatorik</b>	Vorhanden (eIDAS-Verordnung)	Nicht oder nur gering vorhanden	Nicht oder nur gering vorhanden
<b>Transparenz</b>	Eingeschränkt da kaum überwachbar	Nachvollziehbarkeit durch Verkettung	Nachvollziehbarkeit mit Protokollierung
<b>Reifegrad</b>	Ausgereift und aktiv im Einsatz	Erprobungsstadium	Erprobungsstadium
<b>Verbreitung</b>	Hauptsächlich große Organisationen	Relativ weit bei Kryptowährungen	Prototypischer Einsatz
<b>Zukunftssicherheit</b>	Im geschlossenen Kontext ja	Ja, mit Einschränkungen	Ja
<b>Interoperabilität</b>	Verbund möglich (z. B. EBCA)	Standard in Arbeit (ISO, W3C DID Spec)	Standard in Arbeit (ISO, W3C DID Spec)
<b>Skalierbarkeit</b>	Mit hohem Aufwand	Mit hohem Aufwand	Möglich und vorgesehen
<b>Integrationsaufwand</b>	Hoch (insb. bei „Nachrüstung“)	Hoch (insb. bei „Nachrüstung“)	Hoch (insb. bei „Nachrüstung“)
<b>Endanwenderkreis</b>	Hauptsächlich professionelles Umfeld	Jedermann und „Things“ (IoT)	Jedermann und „Things“ (IoT)

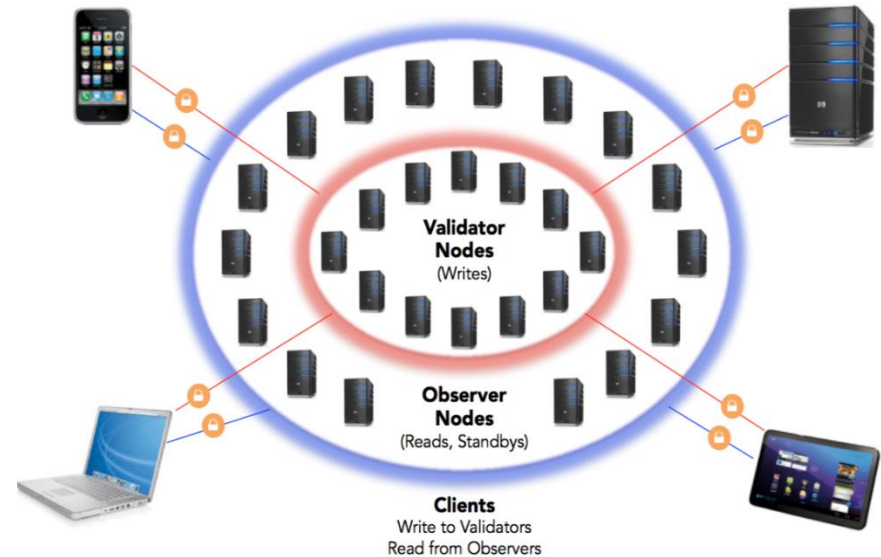


# Chancen und Anknüpfungspunkte für CAs

- CAs betreiben eine Public Permissioned Blockchain
  - Nur CAs können in die Blockchain schreiben, **jeder** kann lesen
- Zertifikate bestehen weiterhin wie bisher
- Blockchain ersetzt aktuell genutzte Certificate Revocation Lists
- Gesteigerte Sicherheit des Netzwerkes durch den Konsens der Blockchain
- Historie durch Verkettung der Transaktionen
- Zertifikate können nicht einfach durch gefälschte getauscht werden
- Bei Fehlverhalten durch eine einzelne CA keine Gefahr → Konsens

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

- 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



Vielen Dank für Ihre  
Aufmerksamkeit!







## **CIO esatus AG und Leiter Blockchain AG TeleTrust**

Dr. André Kudra

Telefon: +49 6103 90295-0

Mail: [a.kudra@esatus.com](mailto:a.kudra@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;  
tostphoto/Fotolia; envfx/Fotolia; opka/Fotolia;  
andrei45454/Fotolia