TeleTrusT-Informationstag "Elektronische Signatur"

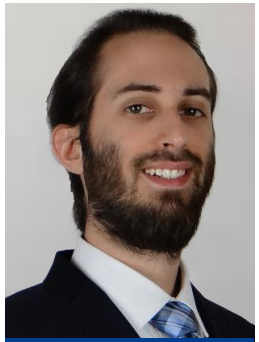
Berlin, 18.09.2018

Blockchain vs. PKI – Symbiose möglich?

Christopher Hempel
Blockchain Lead Developer esatus AG

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.

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

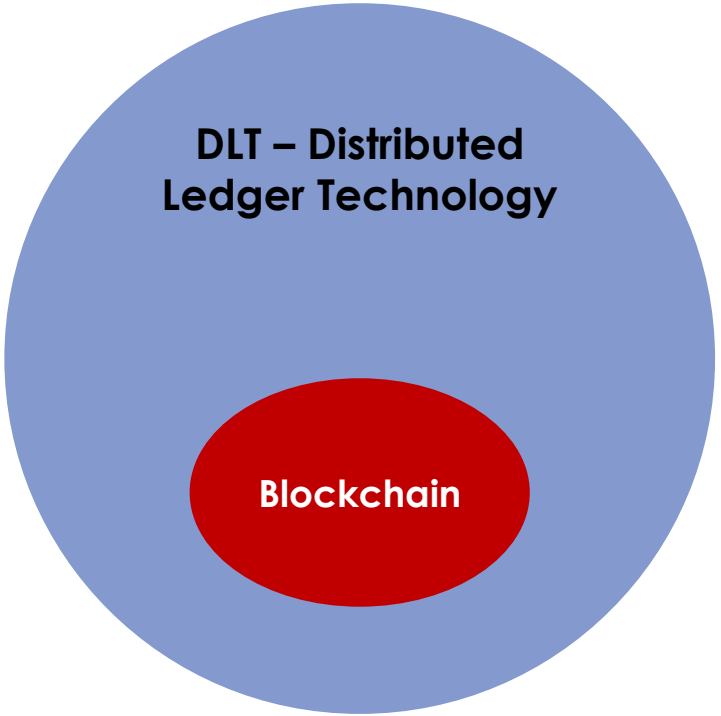
Christopher Hempel studied computer science at Hochschule Darmstadt – University of Applied Sciences. He completed his bachelor's degree by designing and implementing a virtualized test and development environment for information security software solutions.

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

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

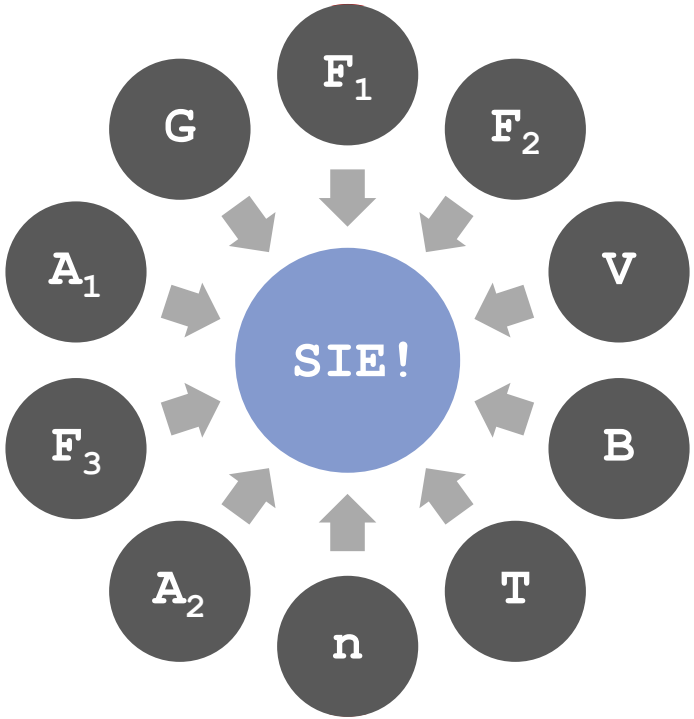
- ▲ Robustheit
- ▲ Berechtigungen
- ▲ Transparenz
- ▲ Schneller Konsens
- ▲ Rollback möglich
- ▼ Missbrauch möglich

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

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

esatus® AG
Enforcing Information Security

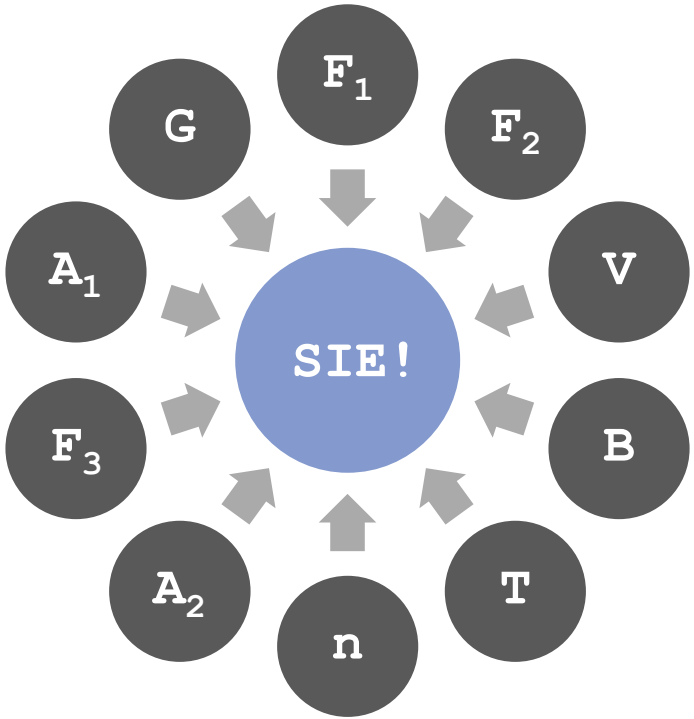
- In einer vernetzten Welt besitzen nur Maschinen Identitäten, nicht die Menschen
- Jeder genutzte Online-Service zwingt uns dazu, eine neue digitale Identitäten anzulegen
- Der Umgang mit Accounts und Passwörtern ist ein ständiger Kampf – der schwer zu gewinnen ist
- Jeder Service sammelt Daten über 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



PKI vs. Blockchain Identity: Kriterien zur vergleichenden Betrachtung

esatus AG
Enforcing Information Security

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

Gegenüberstellung PKI und Blockchain Identity

esatus AG
Enforcing Information Security

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

Chancen und Anknüpfungspunkte für CAs

esatus AG
Enforcing Information Security

- 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

esatus® AG
Enforcing Information Security

Vielen Dank für Ihre Aufmerksamkeit!

Fragen & Diskussion

esatus® AG
Enforcing Information Security

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

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