TeleTrusT
Pioneers in IT security.

TeleTrusT-Informationstag "Blockchain"

Frankfurt a.M., 13.07.2017

Blockchain Identity & Access

Bring Your Own Identity

Dr. André Kudra, CIO esatus AG, Leiter TTT AG "Blockchain"

esatus AG
The CISO Consulting Company

Blockchain I&A
Bring Your Own Identity

Agenda

esatus AG
The CISO Consulting Company

1. Warum Blockchain für I&A?
2. Stand der Entwicklung – Lösungsbeispiele
3. Eigenes Prototyping – Erfahrungsbericht
4. Fazit

esatus AG
The CISO Consulting Company

1. Warum Blockchain für I&A?

Warum Blockchain für I&A?

esatus AG
The CISO Consulting Company

Gute Gründe gegen Blockchain…

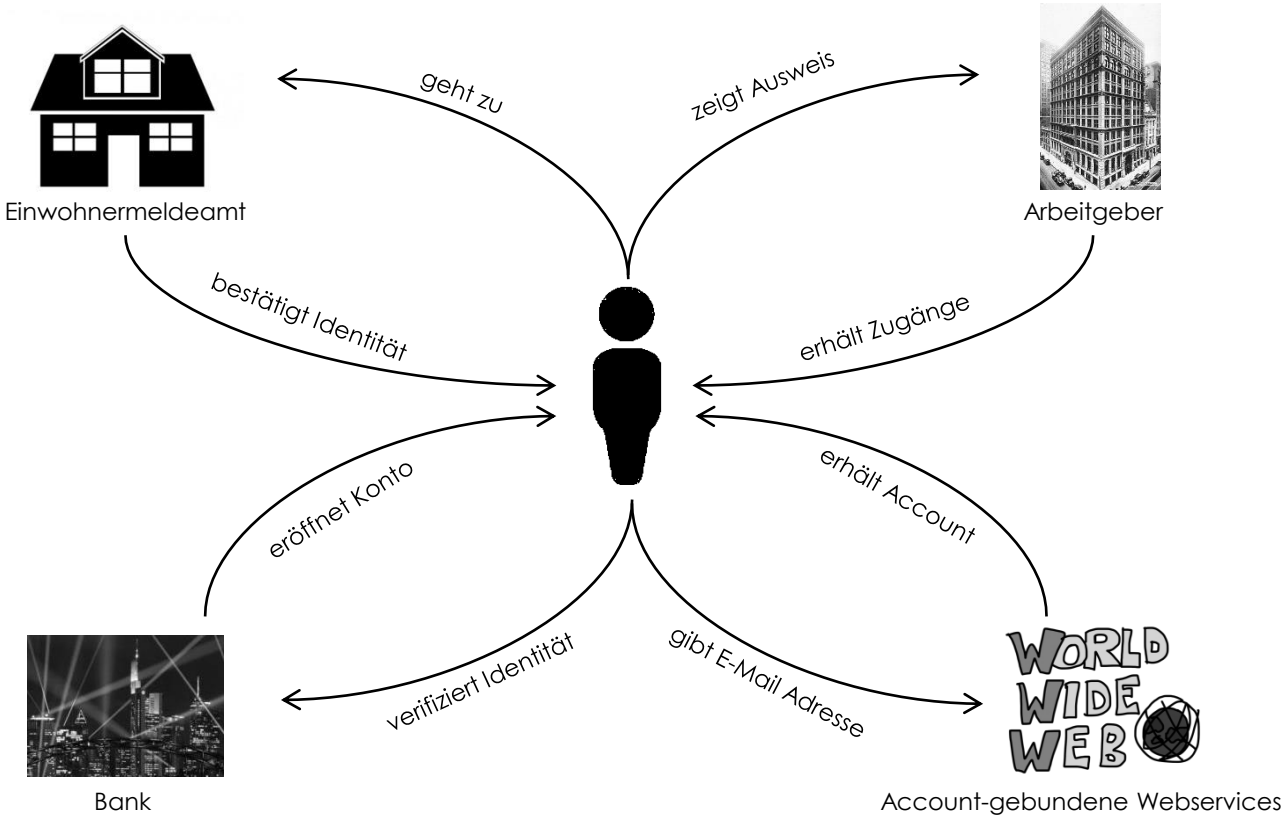
- Es gibt bereits etablierte I&A Software am Markt
- Ökologisch und ökonomisch bessere Lösung
- Schneller Support möglich

Aber:

- 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

Status Quo I&A

esatus AG
The CISO Consulting Company



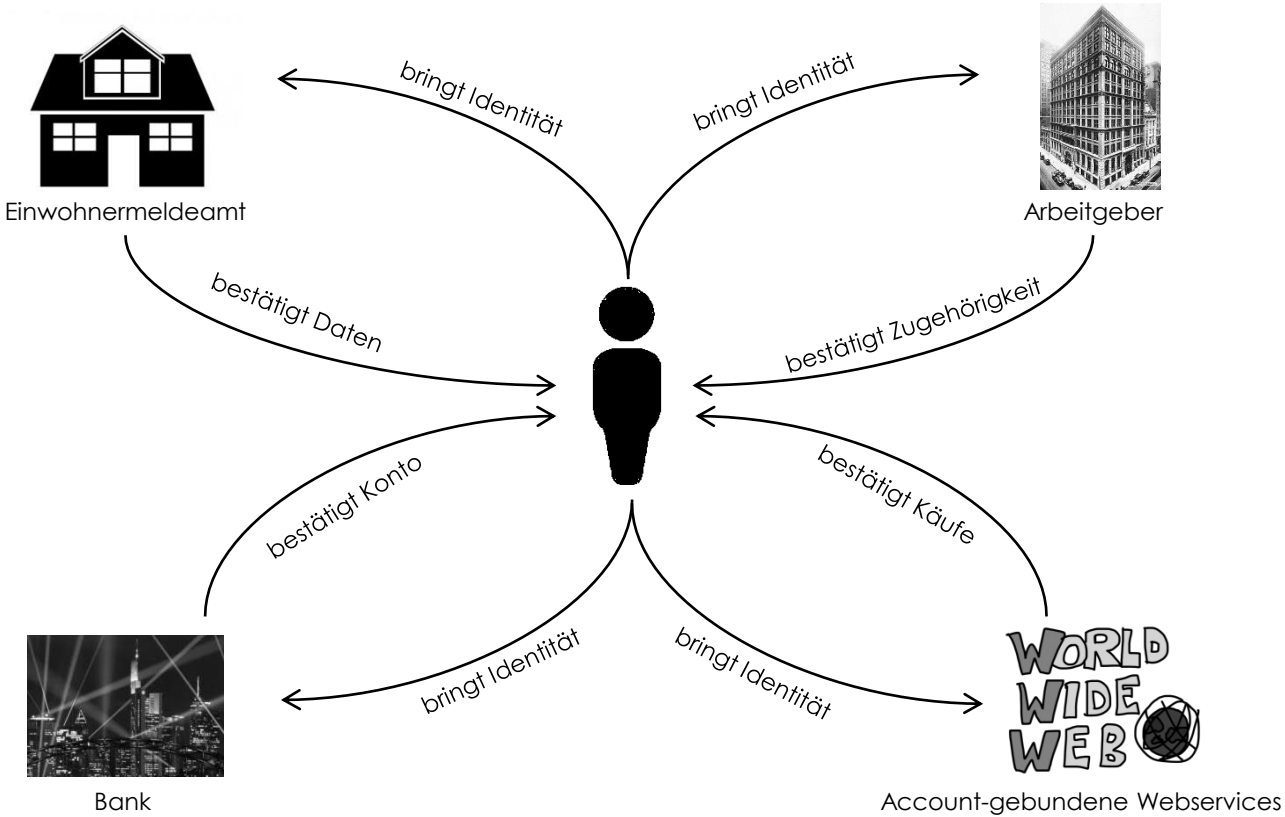
Warum Blockchain für I&A?

esatus AG
The CISO Consulting Company

- Blockchain als dezentrales Transaktionssystem, verspricht:
  - Verwaltung der Identität vom Nutzer selbst
  - Keine Datenschutzverletzung (Diebstahl oder Verlust von Daten)
  - Schnelles und einfaches Mitnehmen der Daten (Anwendung)

Bring Your Own Identity

esatus AG
The CISO Consulting Company



Warum Blockchain für I&A?

esatus AG
The CISO Consulting Company

- Blockchain als dezentrales Transaktionssystem, verspricht:
  - Verwaltung der Identität vom Nutzer selbst
  - Keine Datenschutzverletzung (Diebstahl oder Verlust von Daten)
  - Schnelles und einfaches Mitnehmen der Daten (Anwendung)

...doch welche Blockchain?

Abgrenzung relevanter Dimensionen

esatus AG
The CISO Consulting Company

- Public vs. Private: Wer darf zugreifen?
  - Daten lesbar ohne Zugriffsbeschränkungen ("Public")
  - Zugriff eingeschränkt auf bekannte Netzwerk-Teilnehmer ("Private")
- Permissionless vs. Permissioned: Wer darf validieren?
  - Jeder Client hat dieselben Rechte, neue Blöcke zu schaffen ("Permissionless")
  - Beschränkte Liste von Clients, die in die Blockchain schreiben dürfen ("Permissioned")

Blockchain Berechtigungsarchitektur

esatus AG
The CISO Consulting Company

		Validierung	
		Permissionless	Permissioned
Zugriff	Public	"Jeder darf lesen und validieren"	"Jeder darf lesen, nur Berechtigte validieren"
	Private	"Nur Berechtigte dürfen lesen, jeder darf validieren"	"Nur Berechtigte dürfen lesen und validieren"

esatus AG
The CISO Consulting Company

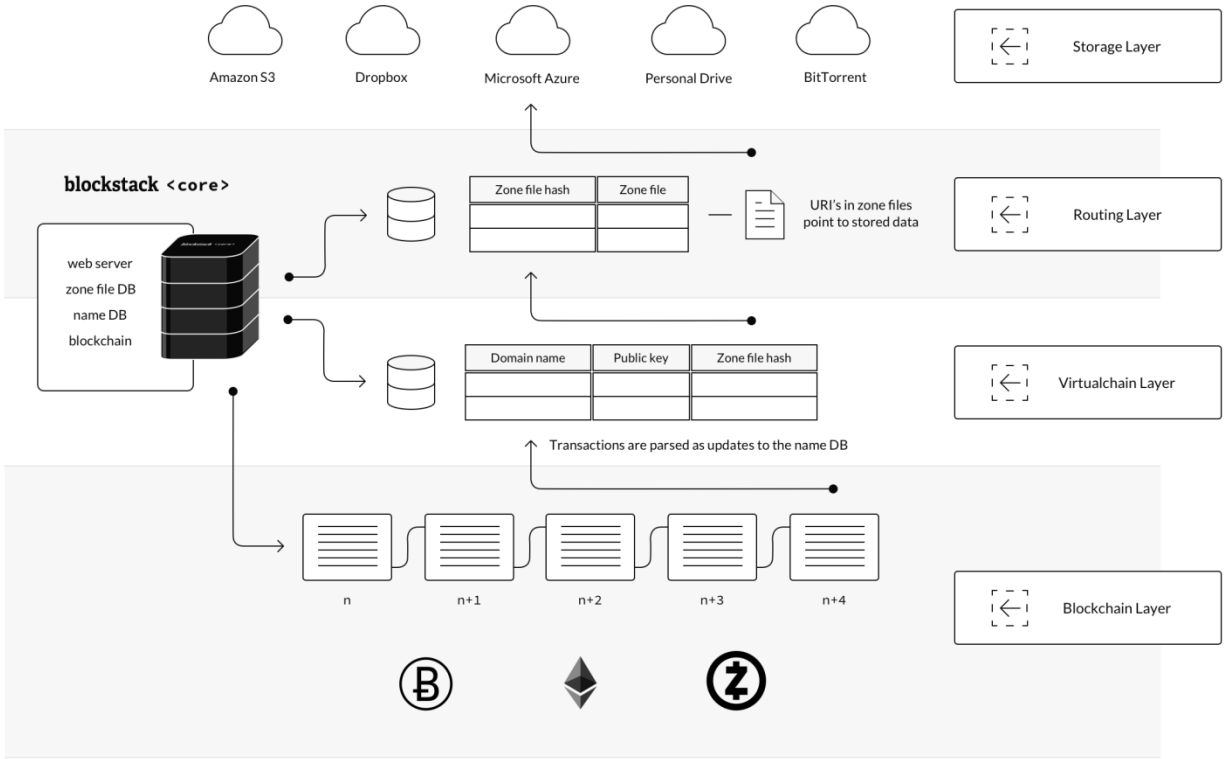
2. Stand der Entwicklung – Lösungsbeispiele

Verschiedene I&A-Lösungsansätze

esatus AG
The CISO Consulting Company

- Blockstack – I&A durch virtuelle Chain
- uPort – I&A auf Basis von Ethereum
- Sovrin – I&A mit differenziertem Konsens
- …

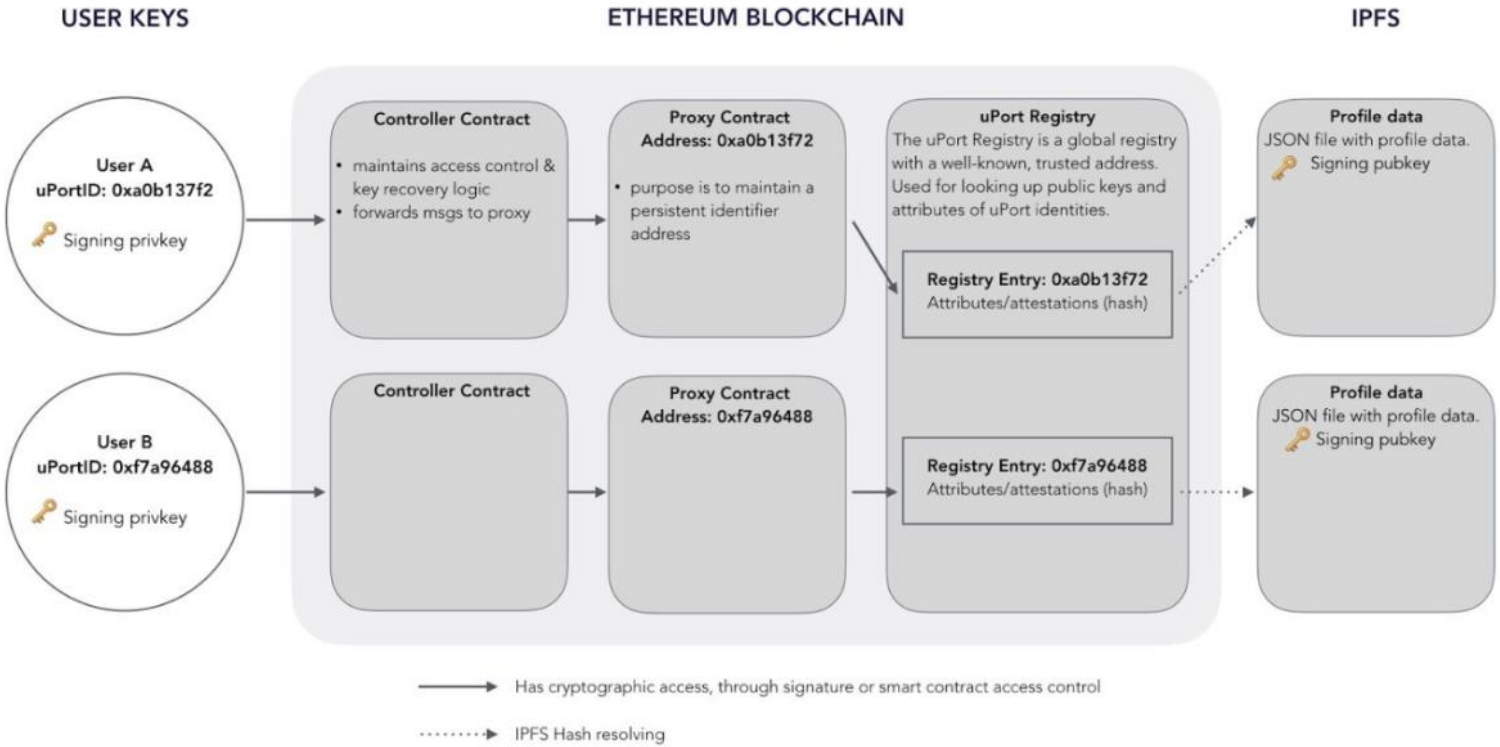
Blockstack



Quelle: https://github.com/blockstack/blockstack

uPort

esatus AG
The CISO Consulting Company

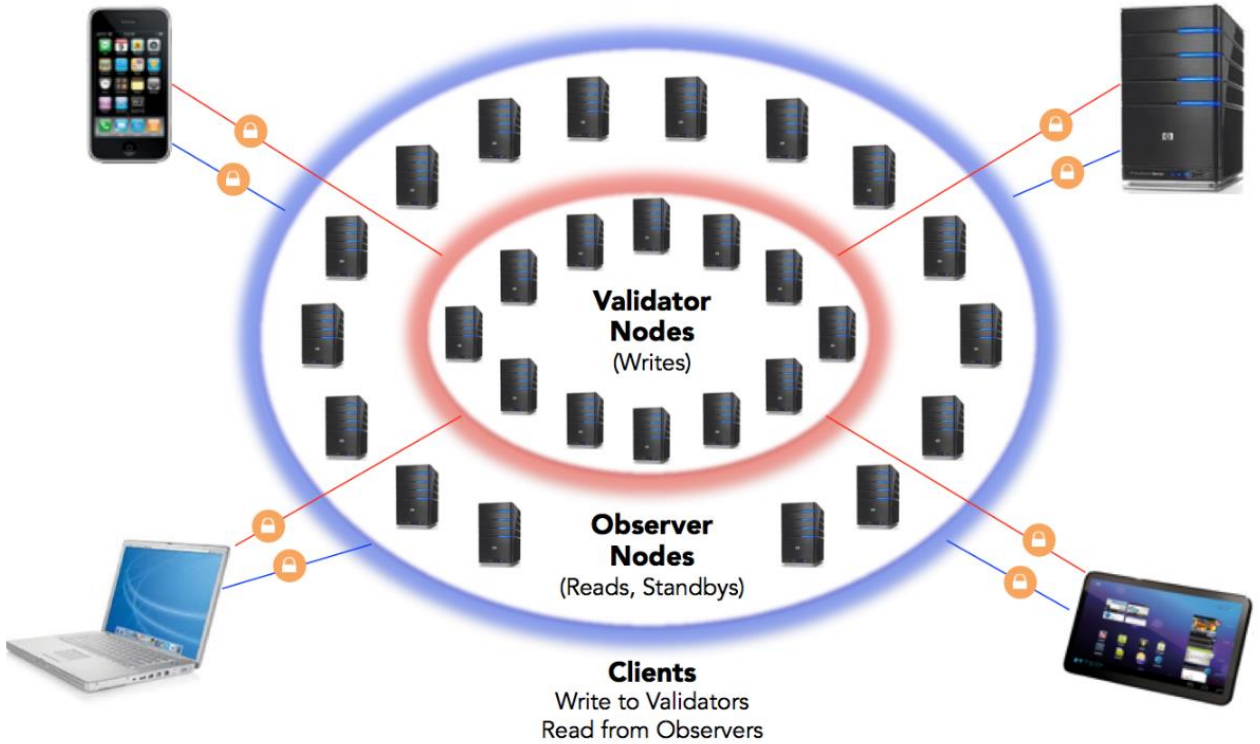


Quelle: https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf (Seite 5)

Sovrin

esatus AG
The CISO Consulting Company

sovrin
identity for all



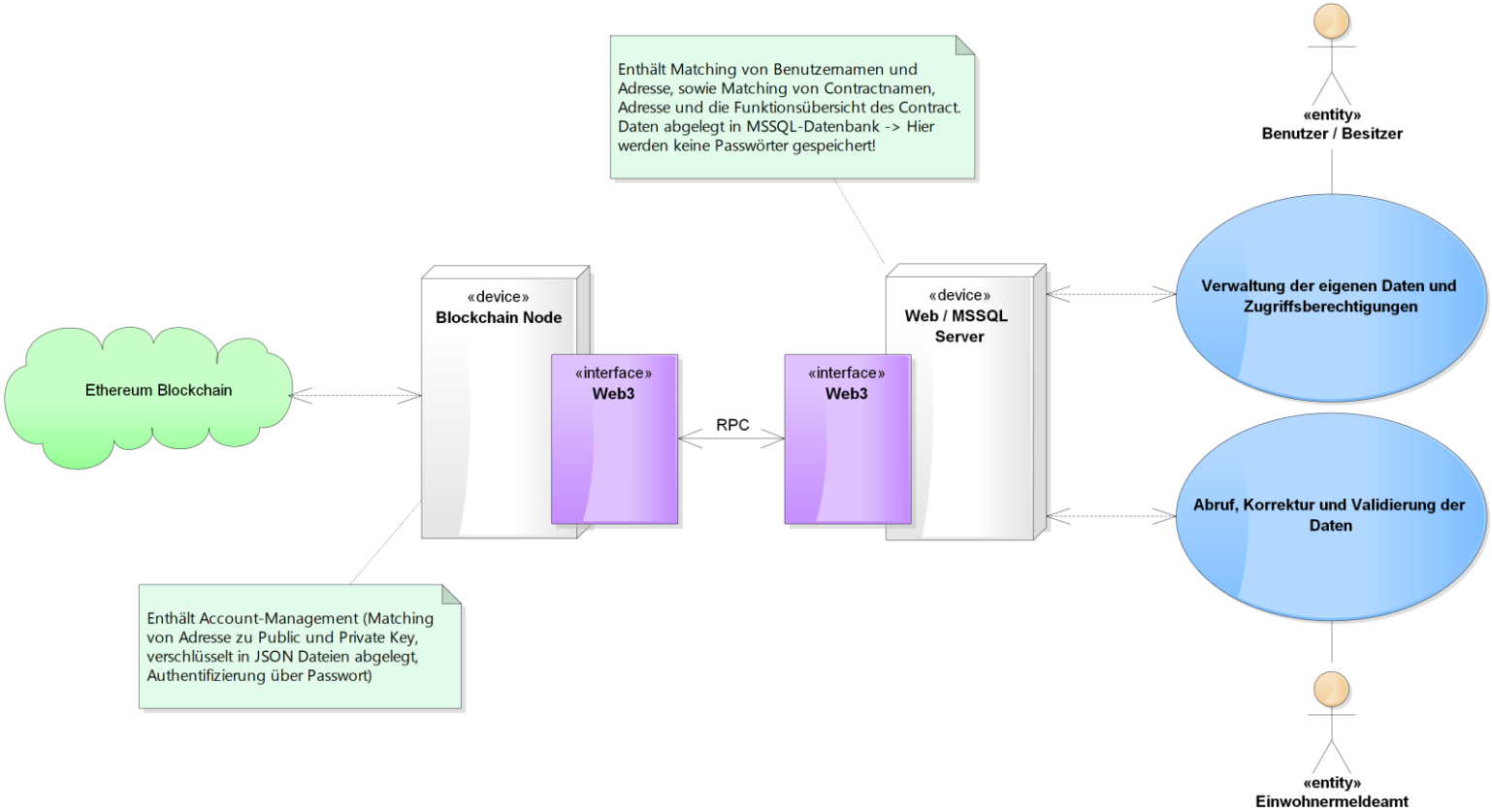
Quelle: https://sovrin.org/wp-content/uploads/2017/04/The-Technical-Foundations-of-Sovrin.pdf (Seite 7)

esatus AG
The CISO Consulting Company

3. Eigenes Prototyping – Erfahrungsbericht

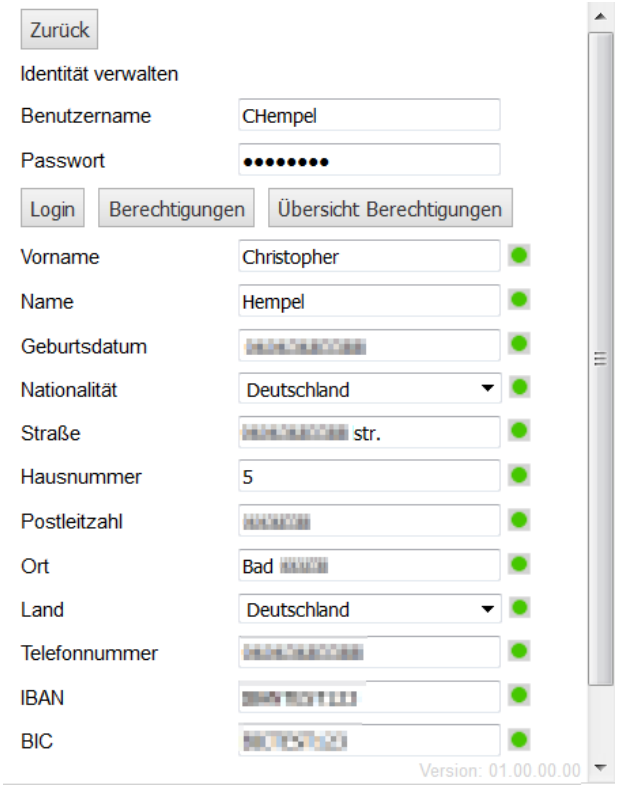
I&A Prototyp für Bring Your Own Identity

esatus AG
The CISO Consulting Company



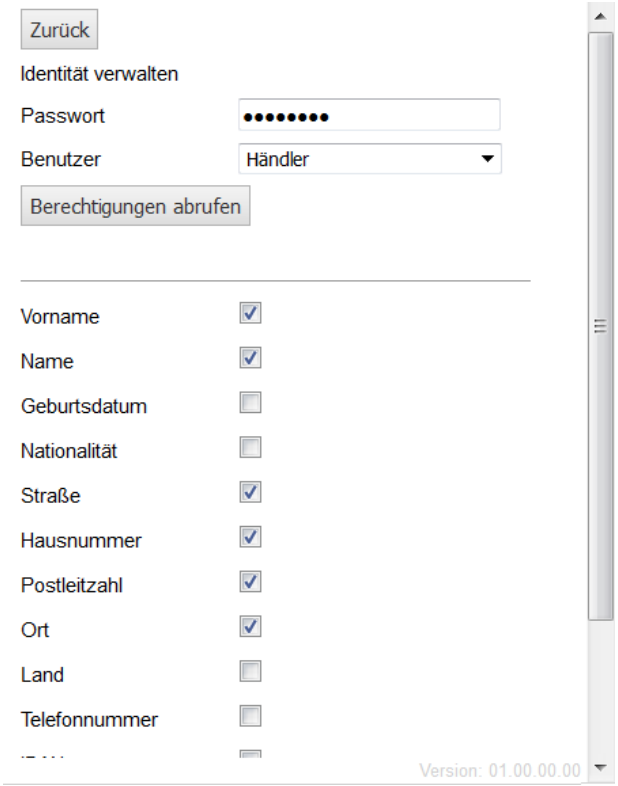
Anlegen und verwalten der Identität

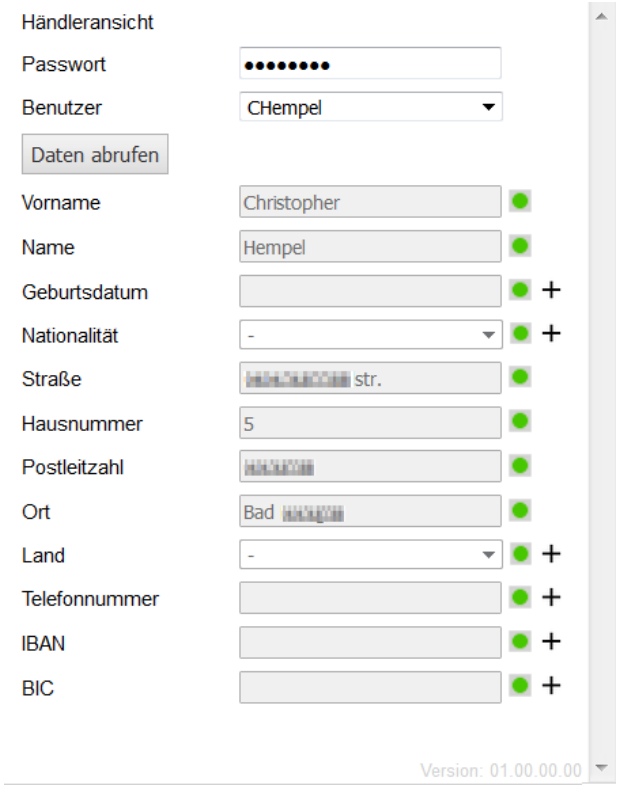
esatus AG
The CISO Consulting Company



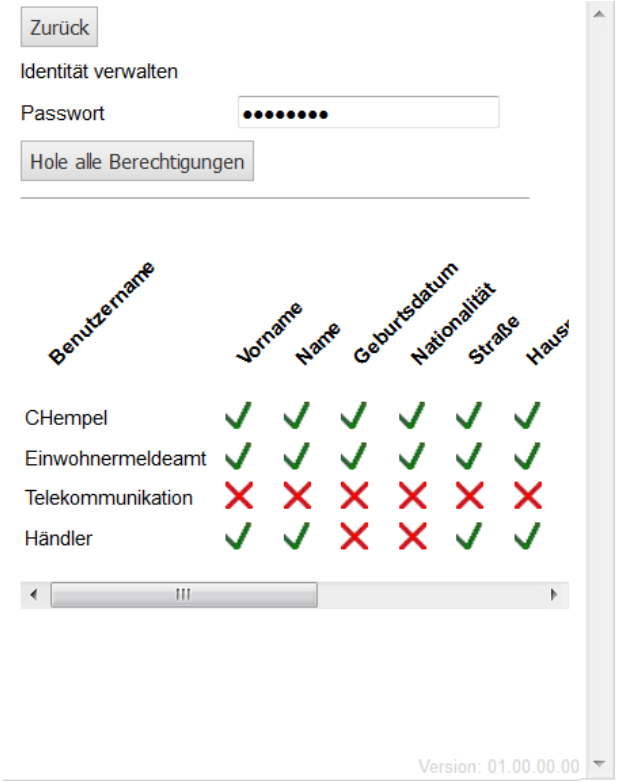
Eigentümer- vs. Konsumentensicht

esatus AG
The CISO Consulting Company



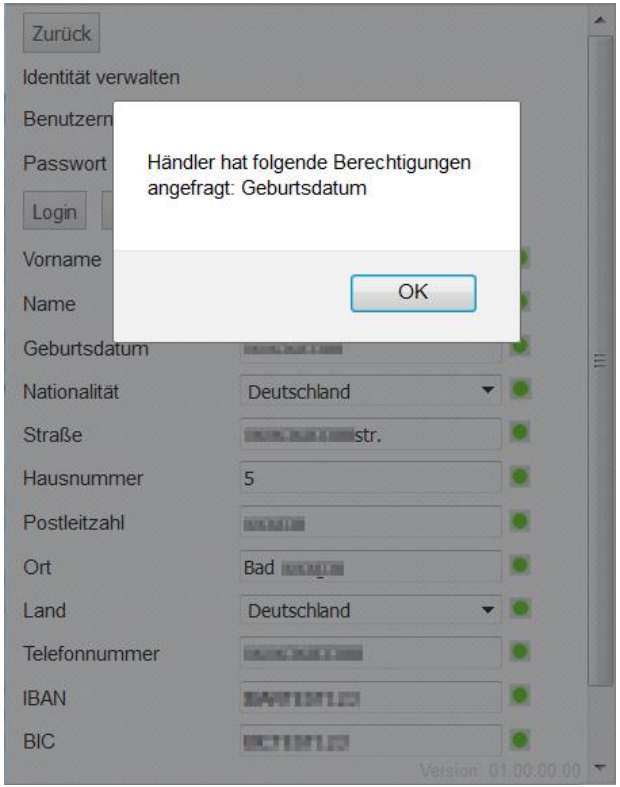


Berechtigungsübersicht für Eigentümer



Anfrage für Datenfreigabe

esatus AG
The CISO Consulting Company



Prototyping Erfahrungsbericht

esatus AG
The CISO Consulting Company

- Unterschiede im Design von Blockchain Nodes: Funktionsumfang (geth) vs. Ausgereiftheit (Parity)
- Einschränkungen von Smart Contracts durch Größe und Kosten motiviert Ausweichen auf Private (Konsortium) Chain
- Parity unterstützt kein HTTP**S** weshalb RPC dort unverschlüsselt übertragen wird
- Mangelnde oder schnell veraltete Dokumentationen

esatus AG
The CISO Consulting Company

4. Fazit

Bestehende Herausforderungen

esatus AG
The CISO Consulting Company

- Klärung von Architekturfragen
- Sicherstellung der Skalierbarkeit
- Erreichen von Marktdurchdringung
- Definition einheitlicher Standards
- Limitierungen der Public Permissionless Blockchains
- Erprobung neuer technischer Konzepte
- Mögliche Lösungen durch Konsortium

➔ **Erfinder- und Pioniergeist erforderlich!**

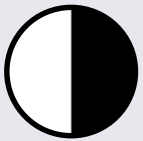
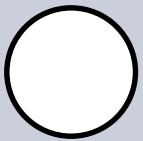
Berechtigungsarchitektur Vor-/Nachteile

esatus AG
The CISO Consulting Company

Zugriff	Validierung: Permissionless		Validierung: Permissioned	
Public	⊕ Robustheit ⊕ Teure Angriffe ⊕ Transparenz ⊙ Dezentralität	⊖ Trägheit ⊖ Langsamer Konsens	⊕ Robustheit ⊕ Berechtigungen ⊕ Transparenz ⊕ Schneller Konsens ⊕ Rollback	⊖ Missbrauch
Private	⊖ Kein sinnvolles Anwendungsszenario		⊕ Berechtigungen ⊕ Schneller Konsens ⊕ Rollback	⊖ Missbrauch ⊖ Erprobtere Datenbanken

Bewertungsmatrix I&A

esatus AG
The CISO Consulting Company

		Validierung	
		Permissionless	Permissioned
Zugriff	Public		
	Private		

Fragen & Diskussion

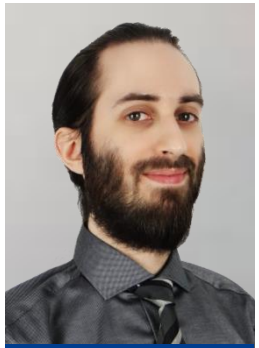
esatus AG
The CISO Consulting Company

esatus AG
The CISO Consulting Company

Vielen Dank für Ihre Aufmerksamkeit!

Meet the esatus Blockchain Team!

esatus AG
The CISO Consulting Company



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.

Christopher Hempel

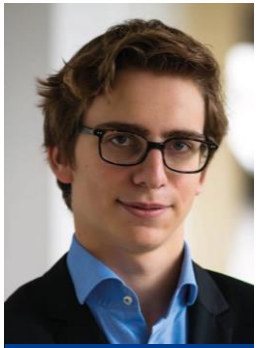
Christopher Hempel studied computer science at Hochschule Darmstadt – University of Applied Sciences. He completed his bachelor's degree by designing and implementing a virtualized test and development environment for information security software solutions.

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 prototype on Ethereum Blockchain technology.

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.

For more than a year now he is contributing to the esatus Blockchain research and facilitates development of Blockchain based Identity & Access solutions.



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 began his first technical research about the Blockchain two years ago. 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.

Michael Wirth

Michael Wirth completed a vocational training as information technology officer. He completed an integrated degree program in economic computer science at the University of Applied Science in Würzburg, with a specialization in information security. He is currently studying computer science at the University of Applied Science in Darmstadt with a specialization in IT security.

Based on his security interests, he is convinced that the distributed ledger can easily improve the information security and can raise the privacy for each person.

esatus Blockchain Ansprechpartner

esatus AG
The CISO Consulting Company

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.

CIO esatus AG

Tel.: +49 170 9677099
a.kudra@esatus.com

esatus AG | www.esatus.com

Copyright

esatus AG
The CISO Consulting Company

Herausgeber: esatus AG

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