



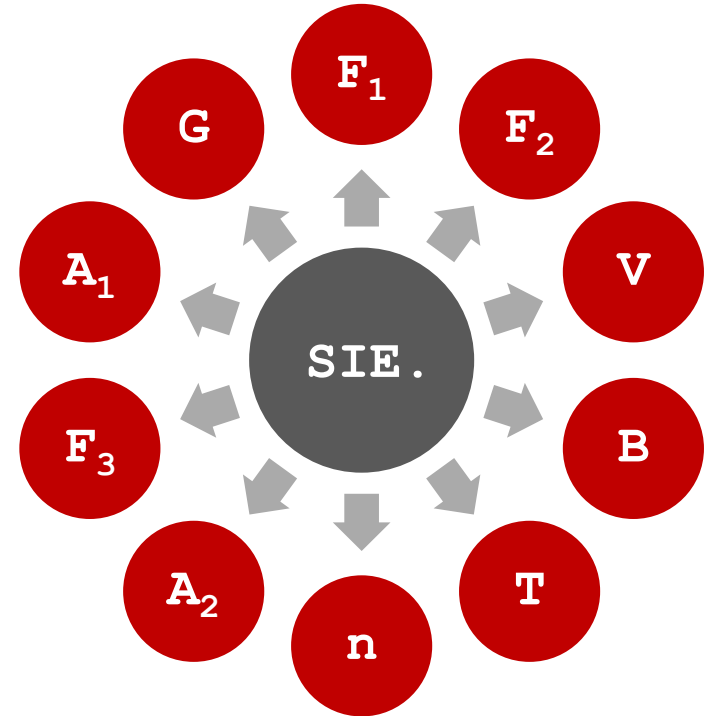
## Blockchain Identity – Bring Your Own Identity

- ▶ *Einführung*  
Self-Sovereign Identity (SSI) | Bring Your Own Identity (BYOI)
- ▶ *Technik*  
Die Eignung von Blockchain | Das Beispiel Sovrin
- ▶ *Gesellschaft*  
Das Crypto-Dogma | Die Hackerethik
  
- ▶ Für die behandelten Themen sensibilisieren
- ▶ Eine kritische Diskussion unterstützen und führen
- ▶ Anknüpfungspunkte für weitere Auseinandersetzung schaffen

# *Einführung* Self-Sovereign Identity & Bring Your Own Identity

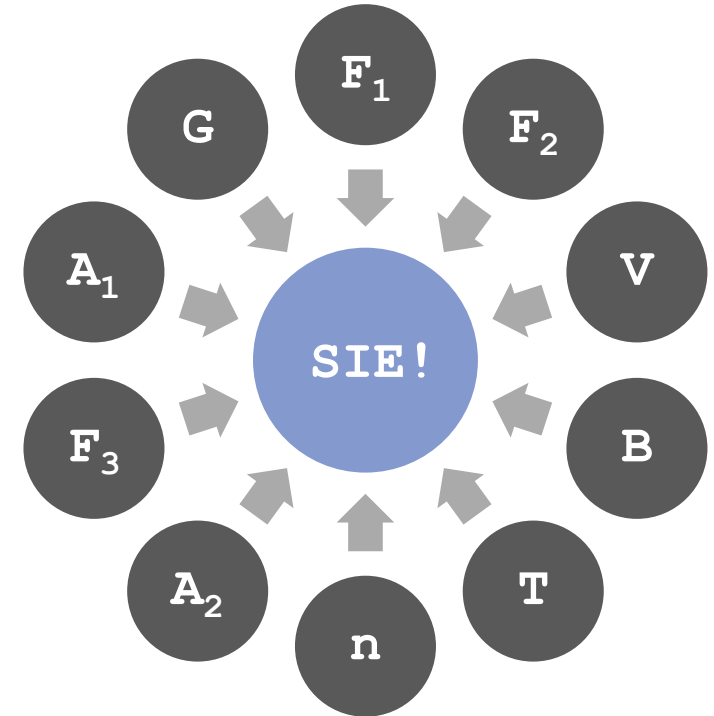
# Die digitale Identität ist eines der schwierigsten Probleme in unserer vernetzten Welt

- ▶ 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

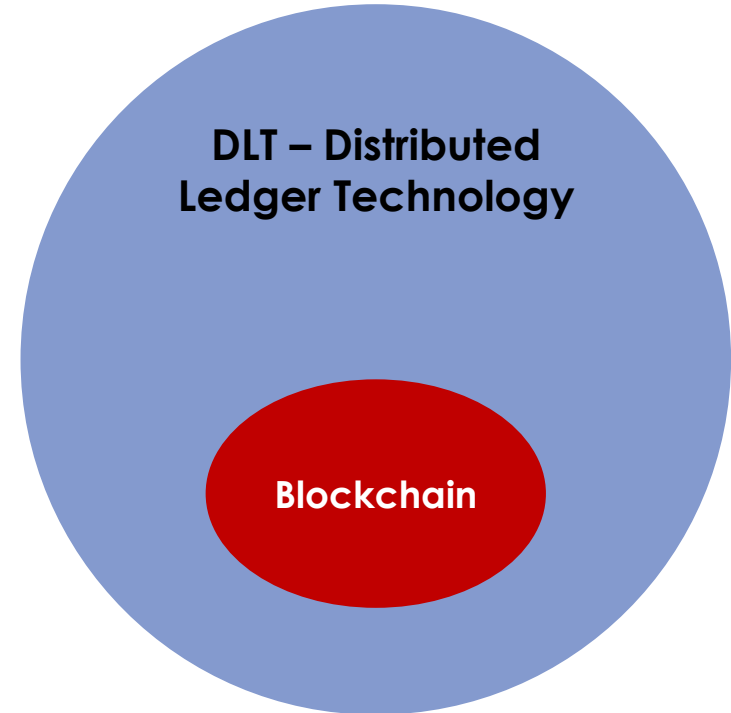


## *Technik*

# Die Eignung von Blockchain | Das Beispiel Sovrin

# 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>

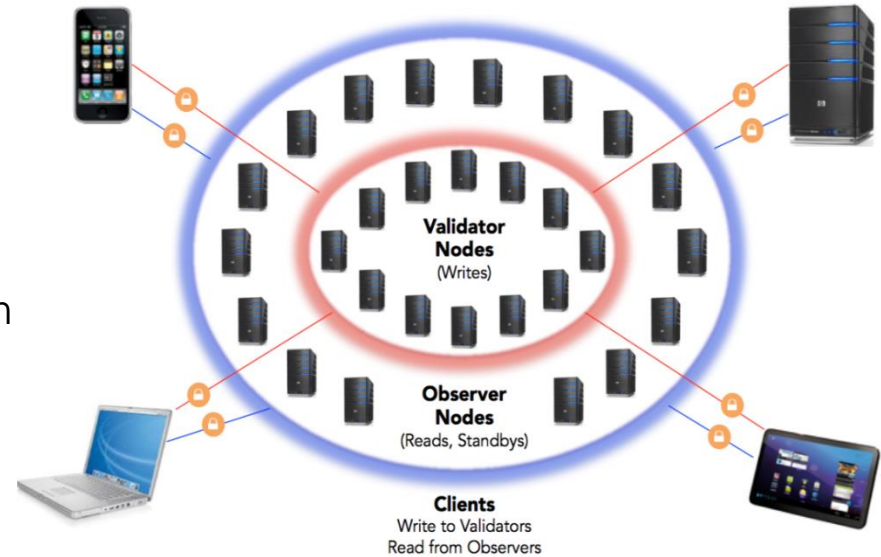
- ▲ Robustheit
- ▲ Berechtigungen
- ▲ Transparenz
- ▲ Schneller Konsensus
- ▲ Rollback möglich
- ▼ Missbrauch möglich

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



# 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



# *Gesellschaft* Das Crypto-Dogma | Die Hackerethik

Well, many people wonder how Religion and Bitcoin are related? The answer to this is simple; faith brings people together, it makes them believe in something strong and emerge as a strong person. Bitcoin is working in a similar direction. It is not only about a few people who fell that cryptocurrency is a right investment decision. But for some, Bitcoin has the force to remodel our society. To sum, it can be said that Bitcoin is an article of faith.

„How Is Bitcoin making people religious?“  
von TOSHENDRA KUMAR SHARMA am 26. Dezember 2017  
Quelle: <https://www.blockchain-council.org/blockchain/how-is-bitcoin-making-people-religious>

A collective insanity has sprouted around the new field of 'cryptocurrencies', causing an irrational gold rush. I know you're tempted, but don't be a fool.

„So you're thinking about investing in bitcoin? Don't!“  
von "Mr Money Mustache" am 15. Januar 2018  
Quelle: <https://www.theguardian.com/technology/2018/jan/15/should-i-invest-bitcoin-dont-mr-money-moustache>

## ...oder neue Religion?



Bild von Nick Little in „Why People Get Religious about Bitcoin“ von Mike Orcutt am 3. November 2017  
Quelle: <https://www.technologyreview.com/s/609313/why-people-get-religious-about-bitcoin>

I argue that Cryptocurrencies function as distinct religious beliefs, which affect ego permeability by playing into our natural tendencies to perceive attributes of money and value as inherently magic and spiritual. The longer you have spent in the cryptocurrency community, the more you will be able to identify with these statements.

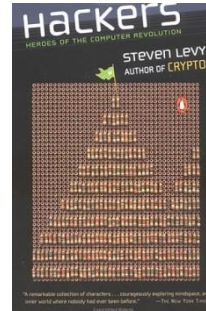
„Why Bitcoin is a Religion“  
von Filip Martinka am 3. Mai 2016  
Quelle: <https://medium.com/@fmartinka/why-bitcoin-is-a-religion-f605ff968910>

Bitcoin's buckets of media attention -- way out of proportion to its roughly \$6.9 billion in value (assuming there are 12.34 million minted Bitcoins trading at \$556 a piece) -- leads me to conclude that the force is strong with the argument that it's a cult.

„Is Bitcoin An Investment Or a Cult?“  
von Peter Cohan am 26. Februar 2014  
Quelle: <https://www.forbes.com/sites/petercohan/2014/02/26/is-bitcoin-an-investment-or-a-cult>

# Die Hackerethik: Eine kurze Rekapitulation

- ▶ Ein Konzept eingeführt vom Autor Steven Levy in 1984 in seinem Buch *Hackers: Heroes of the Computer Revolution*
- ▶ Erkundet „AI“ Hacker des MIT, Hardware-Hacker im Silicon Valley und Game Hacker
- ▶ Reflektiert Levy's Verständnis der Hackerkultur basierend auf Interviews mit Hackern
- ▶ Erweitert vom Chaos Computer Club (CCC) in den 1980ern
- ▶ Betont die individuelle Privatsphäre und stärkt die Informationsfreiheit



<http://www.stevenlevy.com/index.php/books/hackers>



<http://www.wauland.de/en/index.php>

## Die Hackerethik

- ▶ Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
- ▶ Alle Informationen müssen frei sein.
- ▶ Mißtraue Autoritäten – fördere Dezentralisierung.
- ▶ Beurteile einen Hacker nach dem, was er tut, und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung.
- ▶ Man kann mit einem Computer Kunst und Schönheit schaffen.
- ▶ Computer können dein Leben zum Besseren verändern.
- ▶ Mülle nicht in den Daten anderer Leute.
- ▶ Öffentliche Daten nützen, private Daten schützen.

<https://www.ccc.de/de/hackerethics> | <http://www.stevenlevy.com/index.php/books/hackers>

# Die Hackerethik in den SSI-Kontext gesetzt – eine Einschätzung

Die Hackerethik	SSI-Technologie	SSI angewandt
▶ Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.	▲ Fördert den IT-Zugang und ist für jedermann zugänglich im Sinne eines „öffentlichen Gutes“	▼ Nutzer schützen ihre digitale Welt
▶ Alle Informationen müssen frei sein.	▲ Ist Open Source und frei nutzbar	▼ Nutzer schützen ihre digitale Welt
▶ Mißtraue Autoritäten – fördere Dezentralisierung.	▲ Ist vollständig dezentralisiert	▲ Nutzer dezentralisieren ihre Daten
▶ Beurteile einen Hacker nach dem, was er tut, und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung.	▲ Eine würdige Hackerleistung und promotet stark die Diversifizierung	▲ Jeder ist frei zu hacken und zu programmieren, wie es ihm gefällt
▶ Man kann mit einem Computer Kunst und Schönheit schaffen.	▶ Hängt von der Definition ab...	▶ Evtl. neue Art der Computerkunst?
▶ Computer können dein Leben zum Besseren verändern.	▲ Fördert digitale Identität für jeden	▲ Digitale Identität hilft vielen
▶ Mülle nicht in den Daten anderer Leute.	▲ Ermöglicht volle Kontrolle für alle	▲ Nutzer schützen ihre digitale Welt
▶ Öffentliche Daten nützen, private Daten schützen.	▲ Unterstützt Privatsphäre und Teilen	▲ Nutzer schützen ihre digitale Welt

<https://www.ccc.de/de/hackerethics> | <http://www.stevenlevy.com/index.php/books/hackers>

**Was ist  
Ihre Meinung?**





**CIO esatus AG | Leiter AG Blockchain TeleTrust**

Dr. André Kudra

Tel.: +49 6103 90295-0

[a.kudra@esatus.com](mailto:a.kudra@esatus.com)

[esatus AG | esatus.com](https://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; tostphoto/Fotolia;