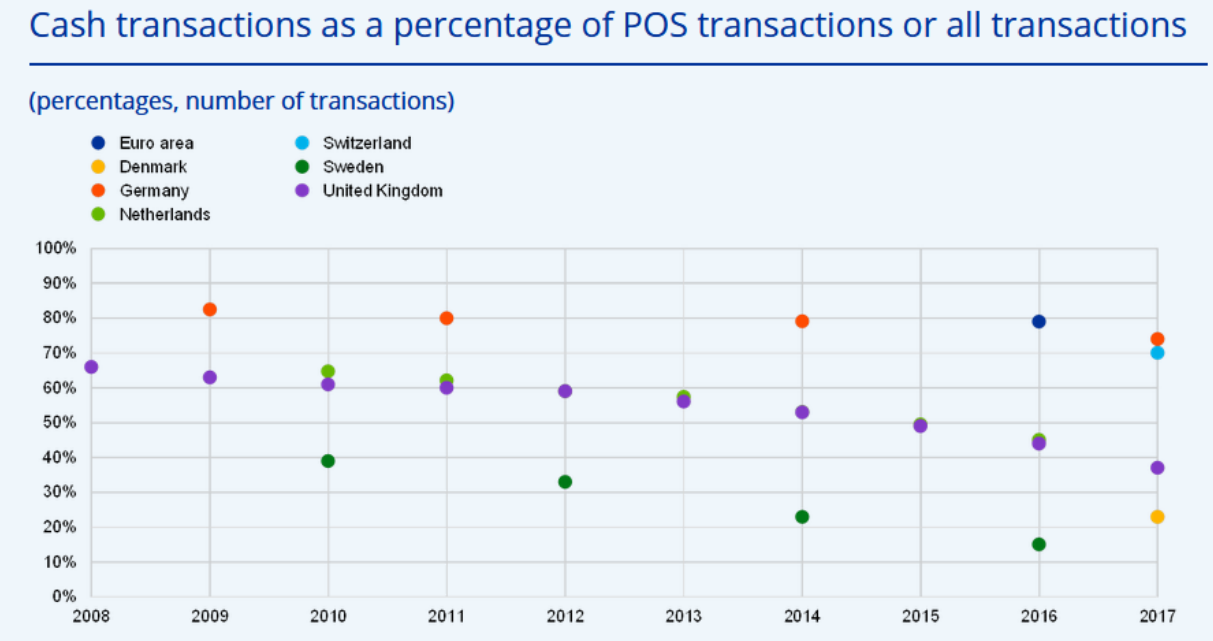
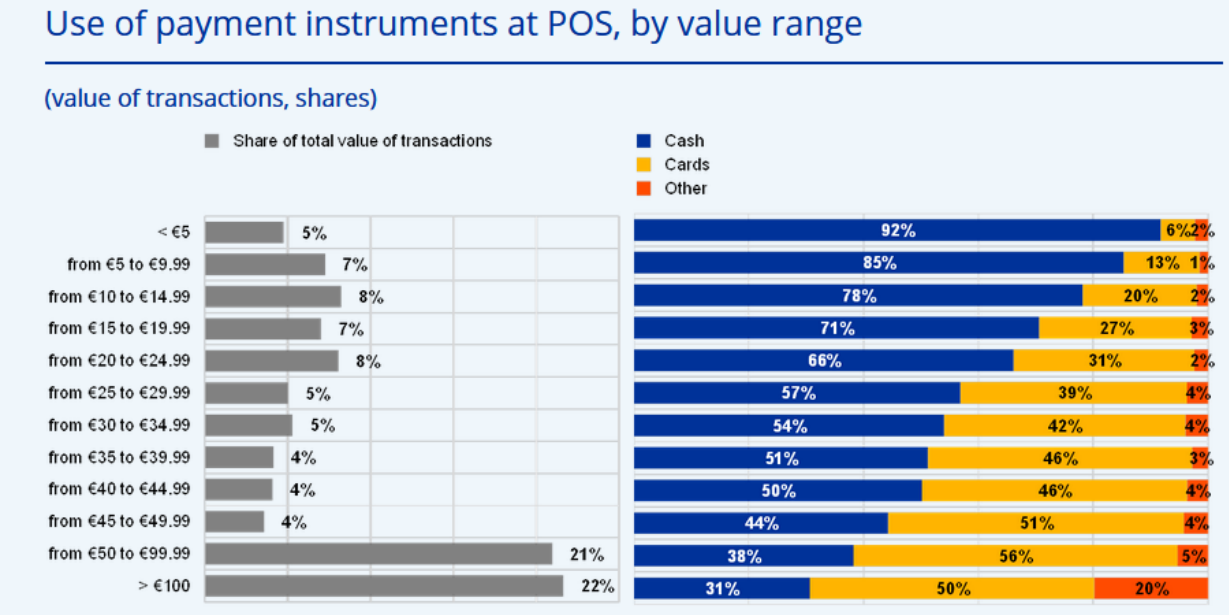
Design-Optionen des digitalen Euros

Welche Rolle können neue Technologien wie Blockchain spielen?

Johannes Sedlmeir, 27.02.2023
GI, Regionalgruppe Rhein-Neckar

Beweggründe für die Diskussion eines digitalen Euros



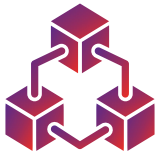


https://www.ecb.europa.eu/pub/economic-bulletin/articles/2018/html/ecb.ebart201806_03.en.html

Beweggründe für die Diskussion eines digitalen Euros?

Abnahme der Bedeutung von Bargeld

Abhängigkeit von ausländischen Technologiekonzernen



Wunsch nach regulierten Transaktionen auf Blockchains

86% der Zentralbanken weltweit erwägen die Einführung einer digitalen Zentralbankwährung (CBDC).

Anforderungsanalyse

Sicherheit

Zugänglichkeit

Kooperation mit Marktteilnehmern

Integrität

Verfügbarkeit

Nachhaltigkeit

Transaktionsdauer und schnelles Settlement

Schutz der Privatsphäre

Interoperabilität

Niedrige Kosten

Programmierbarkeit

Nutzerfreundlichkeit

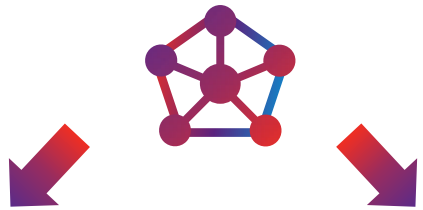
Designoptionen

Wholesale CBDC

Retail CBDC

Zentrale Lösung

Dezentrale Lösung



Permissioned DLT

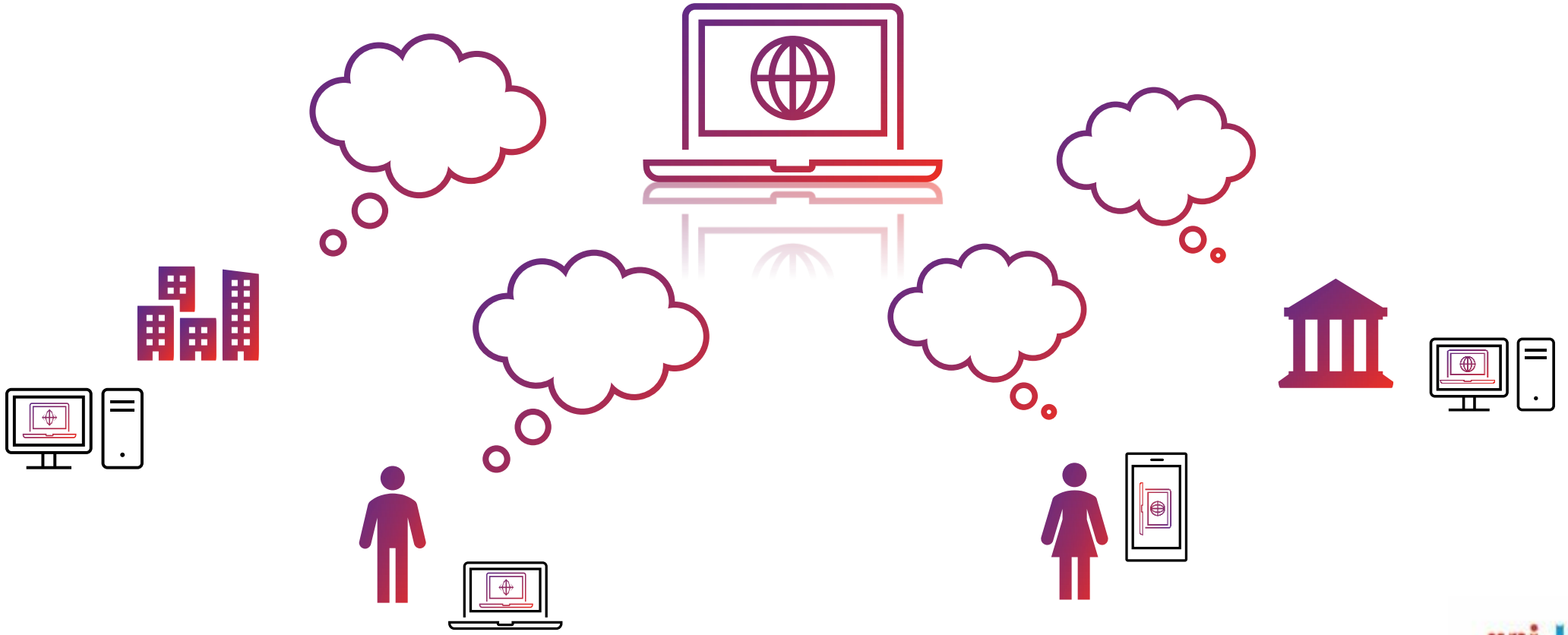
Permissionless DLT

Exkurs: Wie funktioniert Blockchain / DLT?

Repliziertes Speichern und Ausführen von Transaktionen

“Fault Tolerance“: Robustheit gegenüber Ausfällen oder Angriffen Einzelner

Dezentraler Konsensmechanismus

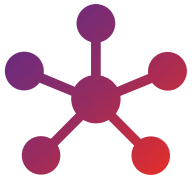


Exkurs: Grundlegende Eigenschaften von Blockchain-Technologie

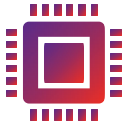
- ✓ “Programmierbare Cloud”
- ✓ Transparente, durchsetzbare Regeln
- ✓ Extrem hohe Verfügbarkeit
- ✓ **Nicht-proprietär**

- ❑ Langsam
- ❑ Teuer
- ❑ Keine feingranularen Beschränkungen beim Lesezugriff

Ebenen der Dezentralisierung

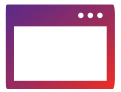


Hersteller von Halbleitern (CPUs, …)



Betreiber von Servern

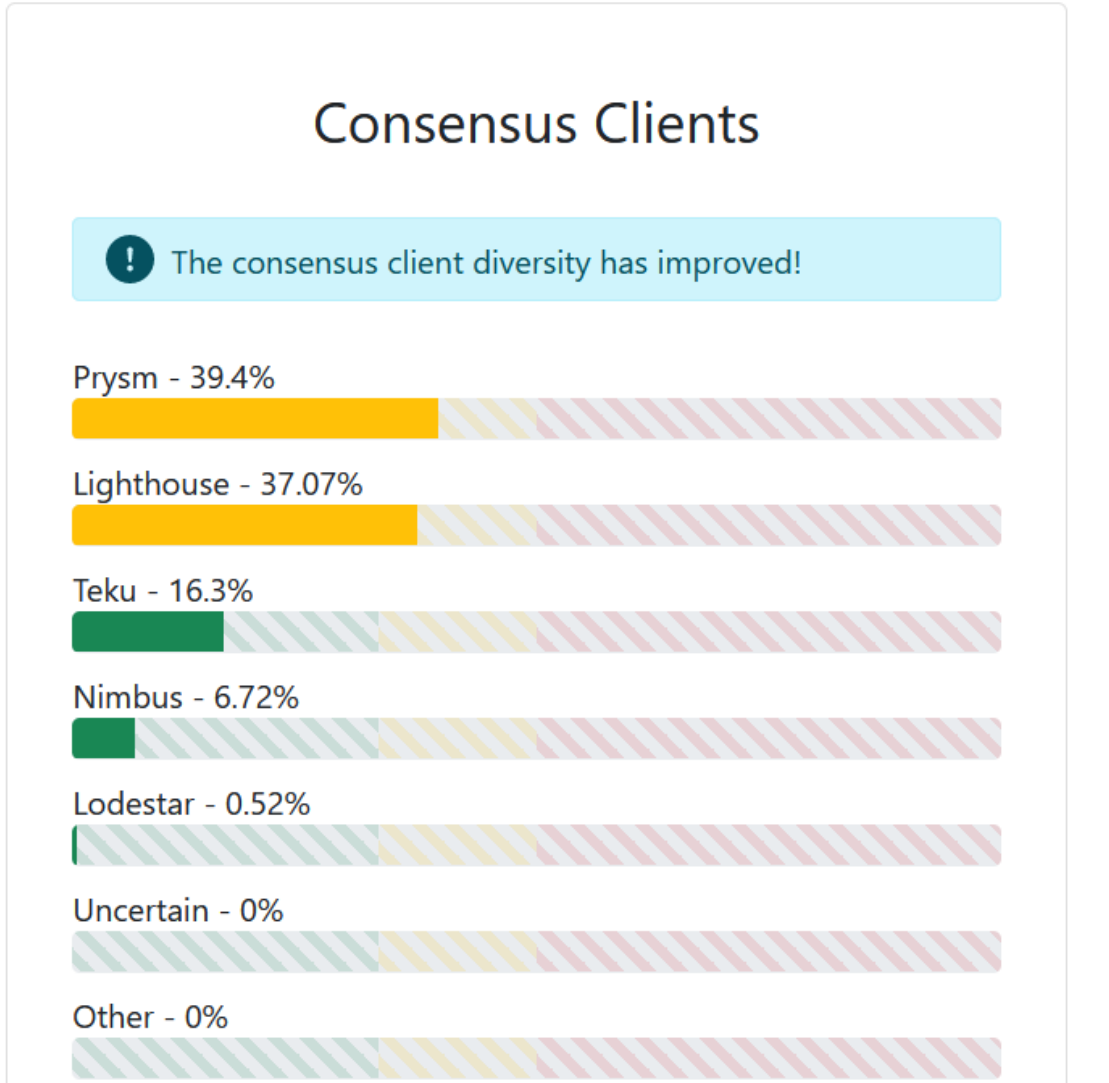
Hersteller von Betriebssystemen

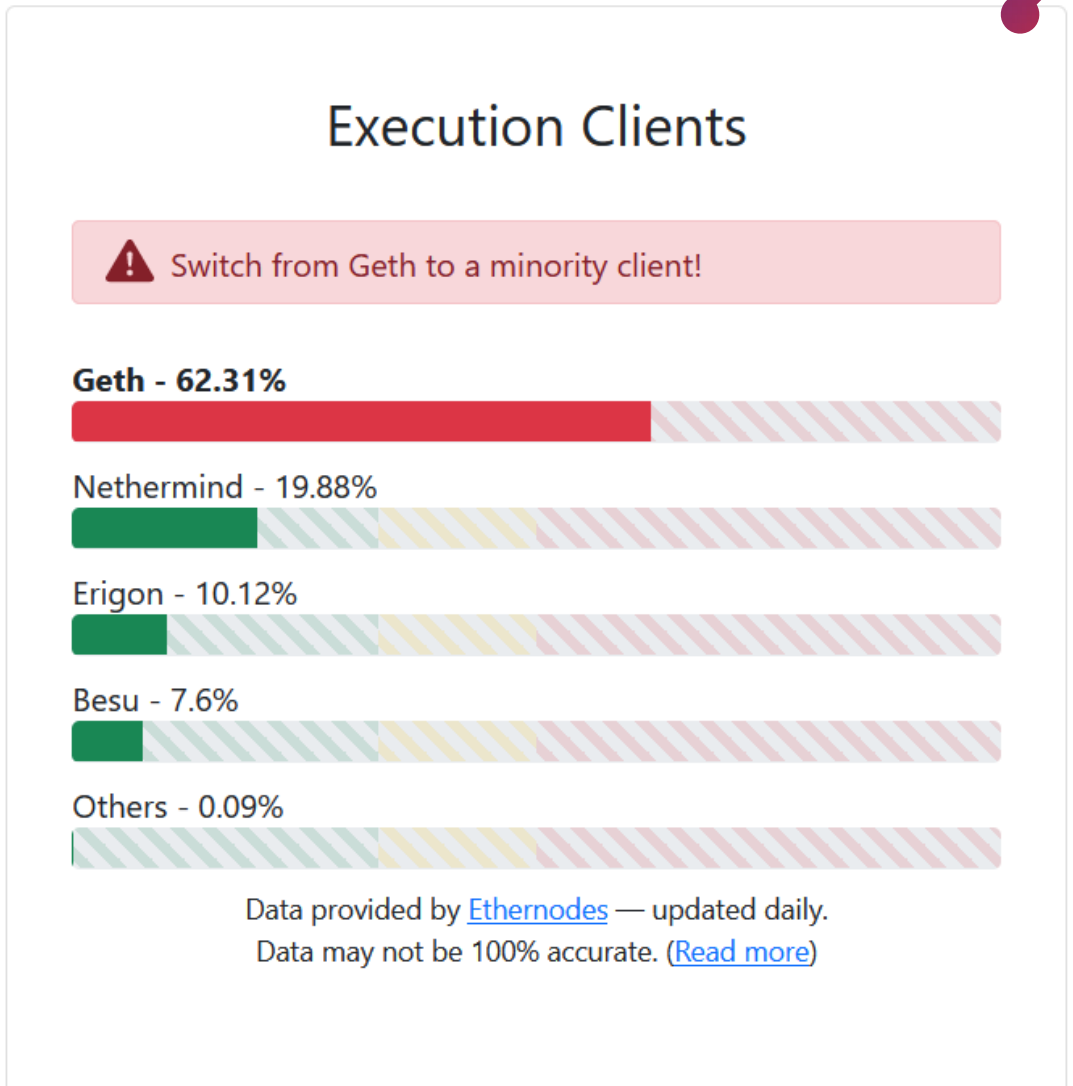


Open Source Entwickler

Internet Service Provider

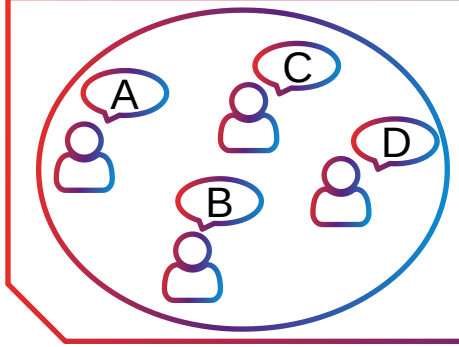
Beispiel: Client-Diversität bei Ethereum





https://clientdiversity.org/

Warum Konsensmechanismen und „Proof of X“



Herausforderung:

Einigung unter den ehrlichen Teilnehmern finden.

Geschlossenes System (permissioned)

“Einfache“ Lösung:

- Wahlbasiert
- Wiederholte zufällige Auswahl

Offenes System (permissionless)

Problem:

- Lösung: Kopple die Gewichtung der Stimme an eine knappe Ressource, die innerhalb des digitalen Systems verifizierbar ist.

Proof of Stake (PoS)

Proof of Work (PoW)

Nachhaltigkeit: Bitcoins Stromverbrauch in a Nutshell

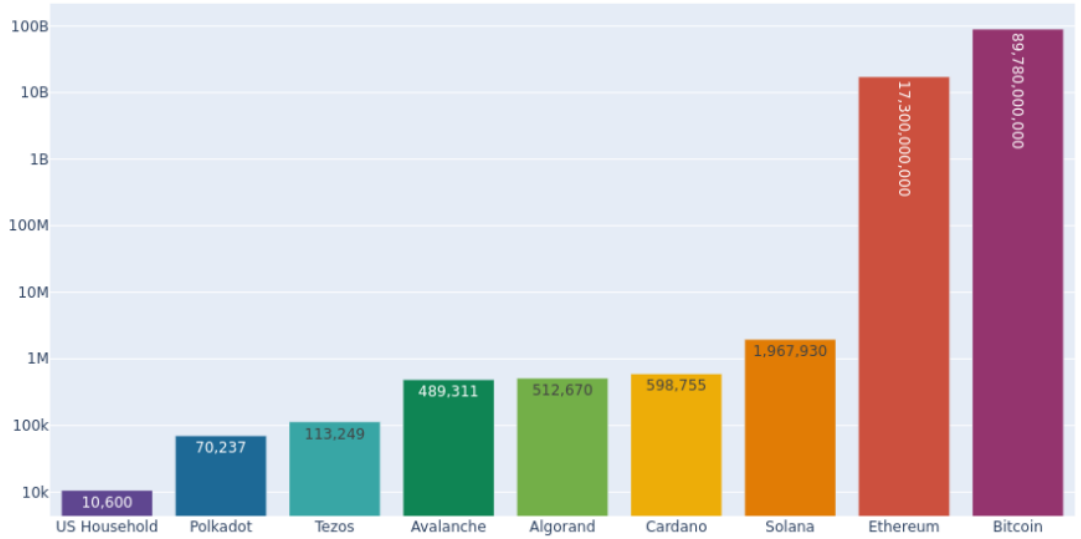
Belohnung für Miner pro Block

50

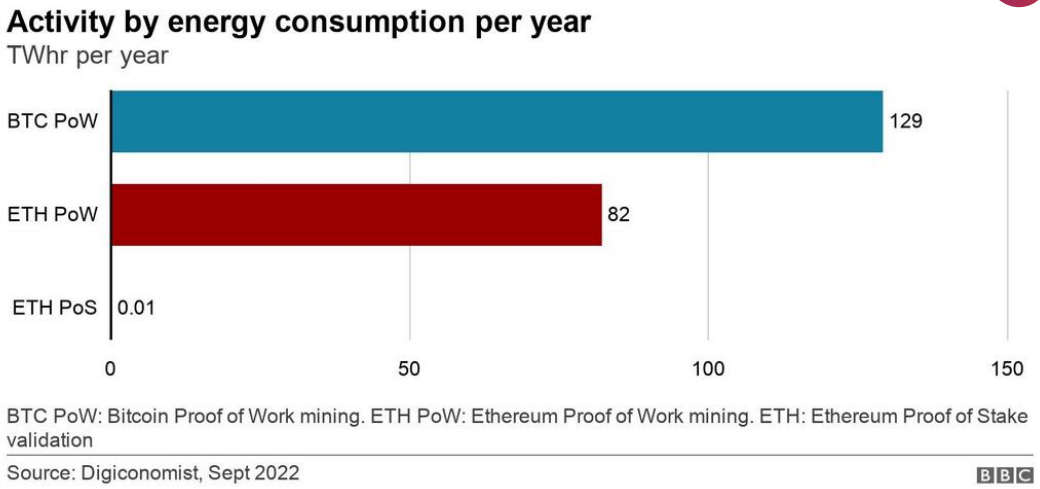
6.25

	Ende 2009	Heute
Bitcoin Preis	0.0006 €	20,000 €
Stromverbrauch (Obergrenze)	5 kW	20 GW = 10,000,000 kW

Nachhaltigkeit

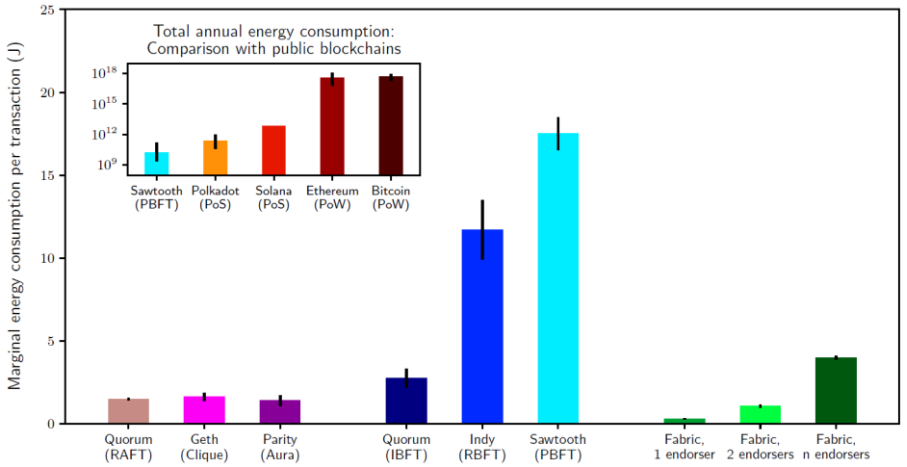


https://carbon-ratings.com/dl/pos-report-2022



https://www.bbc.com/news/technology-62891715

Ethereum Pre-Merge
(noch Proof-of-Work Konsensmechanismus)



Rieger, A., Roth, T., Sedlmeir, J., & Fridgen, G. (2022). We need a broader debate on the sustainability of blockchain. Joule, 6(6), 1137-1141.

Performance (Throughput)

Permissionless Blockchains
~5 – 50 tx/s

Enterprise / Permissioned Blockchains

Hyperledger Fabric, Quorum / Hyperledger Besu, …
~50 – 5.000 tx/s

Serverless Blockchains
(Vendia)
> 10.000 tx/s

High-performance Blockchains
(Solana, Aptos, …)
> 50.000 tx/s

Permissionless Blockchains mit Scaling Lösungen

Payment Channels (nur Bezahlungen): > 100.000 tx/s

Optimistic Rollups: 100 tx/s

Beweis-basierte Rollups („zk-Rollups“): > 1.000 tx/s
(mit Sharding: zusätzlich x 50)

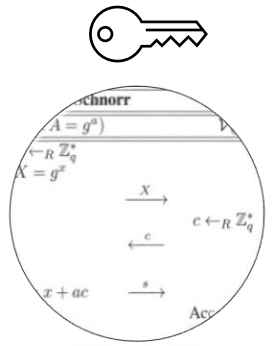
„Validium“: > 10.000 tx/s

Verifiable Computation und Zero-Knowledge Proofs

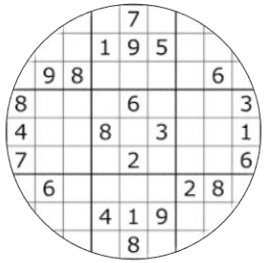
Zero-Knowledge Proofs: “those proofs that convey no additional knowledge other than the correctness of the proposition in question“ (GMR, 1985)

Beispiele:

Proof of Knowledge für einen privaten Schlüssel (verbunden mit einem öffentl. Schlüssel), ohne Informationen preiszugeben, die es der verifizierenden Partei erleichtern würde, den privaten Schlüssel zu finden.



Proof of Knowledge für die Lösung eines gegebenen Sudokus, die es der verifizierenden Partei nicht einfacher macht, die Lösung selbst zu finden.



Allgemein beweisen (Succinct) (Zero-Knowledge) Proofs die korrekte Ausführung eines Programms in Form einer sehr kurzen / schnell zu verifizierenden kryptographischen Attestierung, wobei nur explizit gewählte Inputs, Zwischenergebnisse und Outputs vorgezeigt werden.

Häufig verwendet:
(zk-)SNARKs (Succcinct Non-Interactive Arguments of Knowledge).

Transaktionsdauer und schnelles Settlement

Permissionless Blockchains
Wenige Sekunden bis wenige Minuten

Enterprise/Permissioned Blockchains

Hyperledger Fabric, Quorum / Hyperledger Besu, …
0,5 - 3 Sekunden

Serverless Blockchains (Vendia)
Wenige Sekunden bis wenige Minuten

High-performance Blockchains (Solana, Aptos, …)
Wenige Sekunden

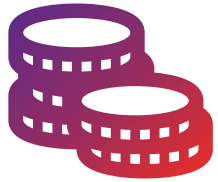
Permissionless Blockchains mit Scaling Lösungen

Payment Channels (nur Bezahlungen): < 1 Sekunde bis wenige Sekunden

Optimistic Rollups:
einige Tage

Beweis-basierte Rollups („zk-Rollups“): wenige Minuten

Niedrige Kosten

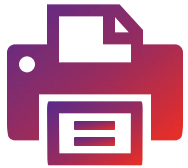


Zahlreiche isolierte Systeme
mit unkoordinierten Backups

Ineffiziente
organisationsübergreifende
Prozesse

Ineffizienz durch Redundanz

➔ Setup
➔ Rechenleistung
➔ Speicherplatz



(Konsensmechanismus)

Programmierbarkeit

Zentrale API für Upload von Skripten

Blockchain mit Smart Contracts

➔ Replizierte Ausführung
➔ Determinismus (?)

Interoperabilität

Austausch digitaler Assets zwischen Blockchains

Verwendung von Funktionalitäten eines Systems von einem anderen System aus

Notary Schemes
(Multisig)

Algorithmische Cross-Chain Communication
(Proof of Consensus)

Sicherheit

Sicherheitslücken durch Kombination von Anwendungen (Smart Contracts)

Sicherheitslücken durch Transparenz, Atomicity und Determinismus (Flashloans etc.)

Konsensmechanismus

Integrität („Safety“) → „51%-Angriffe“

Verfügbarkeit („Liveness“)

Passwort-/Schlüsselmanagement

(Smart Contract) Bugs

Schutz der Privatsphäre: Forschungsprojekt

Matthias Babel

Alexander Bechtel

Jonas Gross

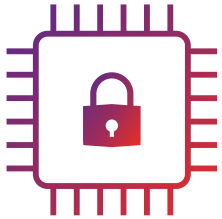
Benjamin Schellinger

Johannes Sedlmeir

Designing a Central Bank Digital Currency with Support for Cash-like Privacy

Schutz der Privatsphäre

Hardware-basiert

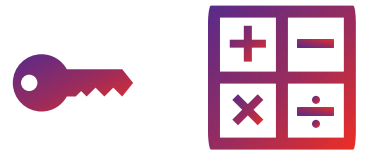


Beschränkung auf legitime Vorgänge durch Chipdesign; Nachweis durch Remote Attestation

Erfahrung: Sidechannel Attacks möglich
Single Point of Failure (Hersteller, privater Schlüssel)

➔ Notwendigkeit, den Grad an Privatsphäre zu reduzieren, um das Risiko zu mindern

Software-basiert



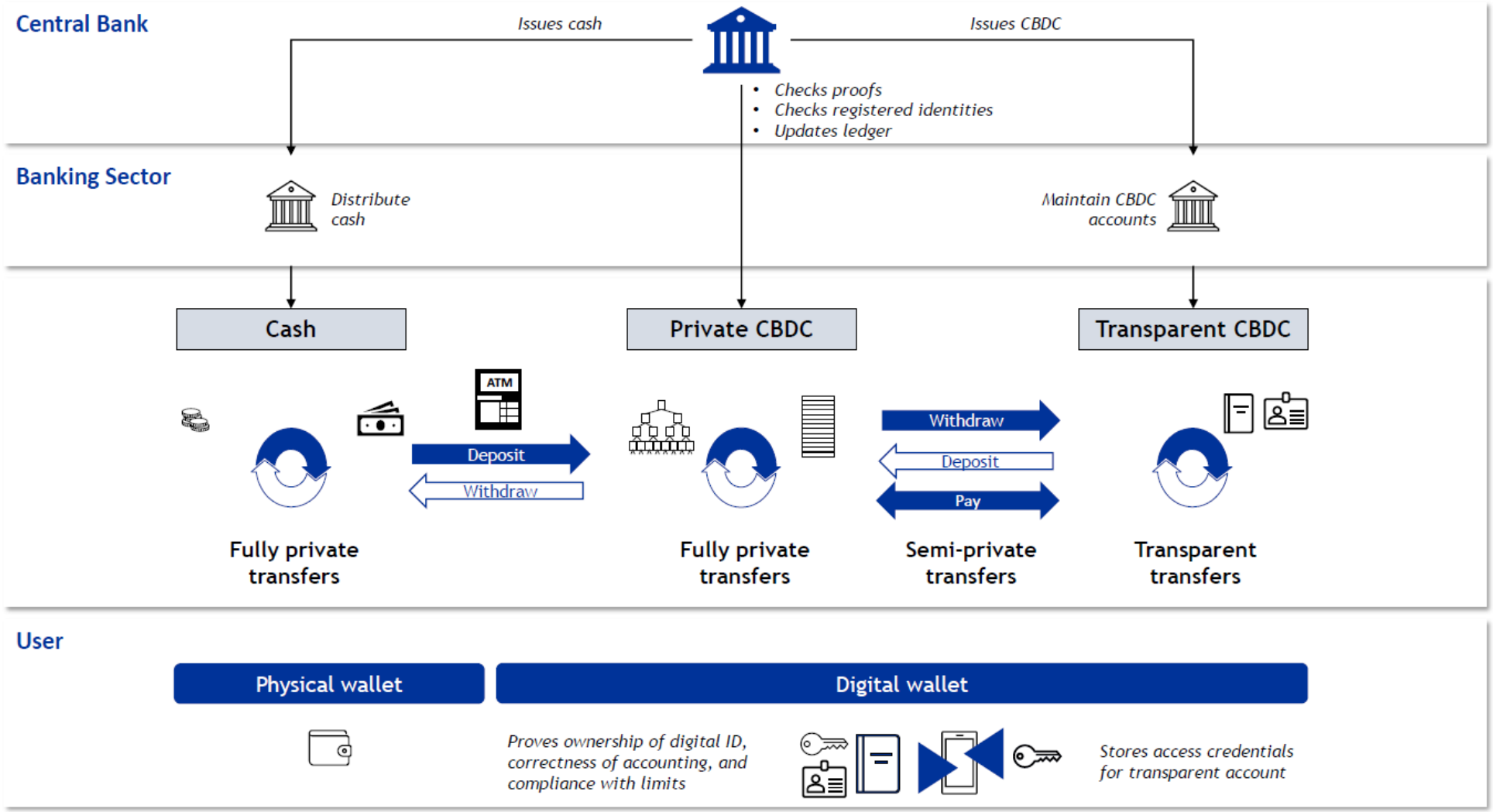
Nachweis der Legitimität von Vorgängen durch Kryptographie (ZKP) oder Möglichkeit, im Falle von Fehlverhalten persönliche Informationen zu extrahieren (blind signatures)

Basiert auf von Experten begutachteter Mathematik und bewährten kryptografischen Annahmen

Schutz der Privatsphäre

Herausford.	Spannungsfeld zwischen Grad an Privatsphäre und Compliance (insbes. Vermeidung von Geldwäsche und Terrorfinanzierung).
Ziel	Gewährleistung eines umfassenden Datenschutzes bis zu einem bestimmten Transaktionslimit. (Zentral-)Banken und Regulierungsbehörden haben keinen Zugriff auf Transaktionsdetails.
Ansatz	Bargeldähnliche Privatsphäre (Sender und Empfänger anonym, Betrag nicht bekannt) durch Kryptographie ohne Vertrauen in eine dritte Partei, z. B. eine Bank oder eine Zentralbank.
Nutzer-zentrische Compliance	In Ermangelung von Dritten, die die Einhaltung der Vorschriften überprüfen können, müssen Nutzer die Einhaltung von Regeln selbst überprüfen ➔ Nachweis, dass Anforderungen (Obergrenze für Saldo / monatl. Umsatz) erfüllt sind. Überprüfung der Einhaltung der Vorschriften mittels Zero-Knowledge-Proofs (ZKPs) ➔ Beweis der Korrektheit von Aussagen, ohne weitere (sensitive) Informationen über die Transaktion preiszugeben.

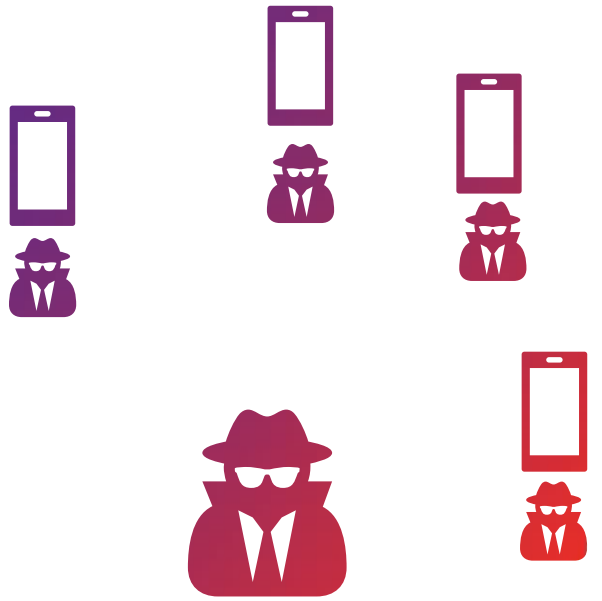
Schutz der Privatsphäre



https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3891121

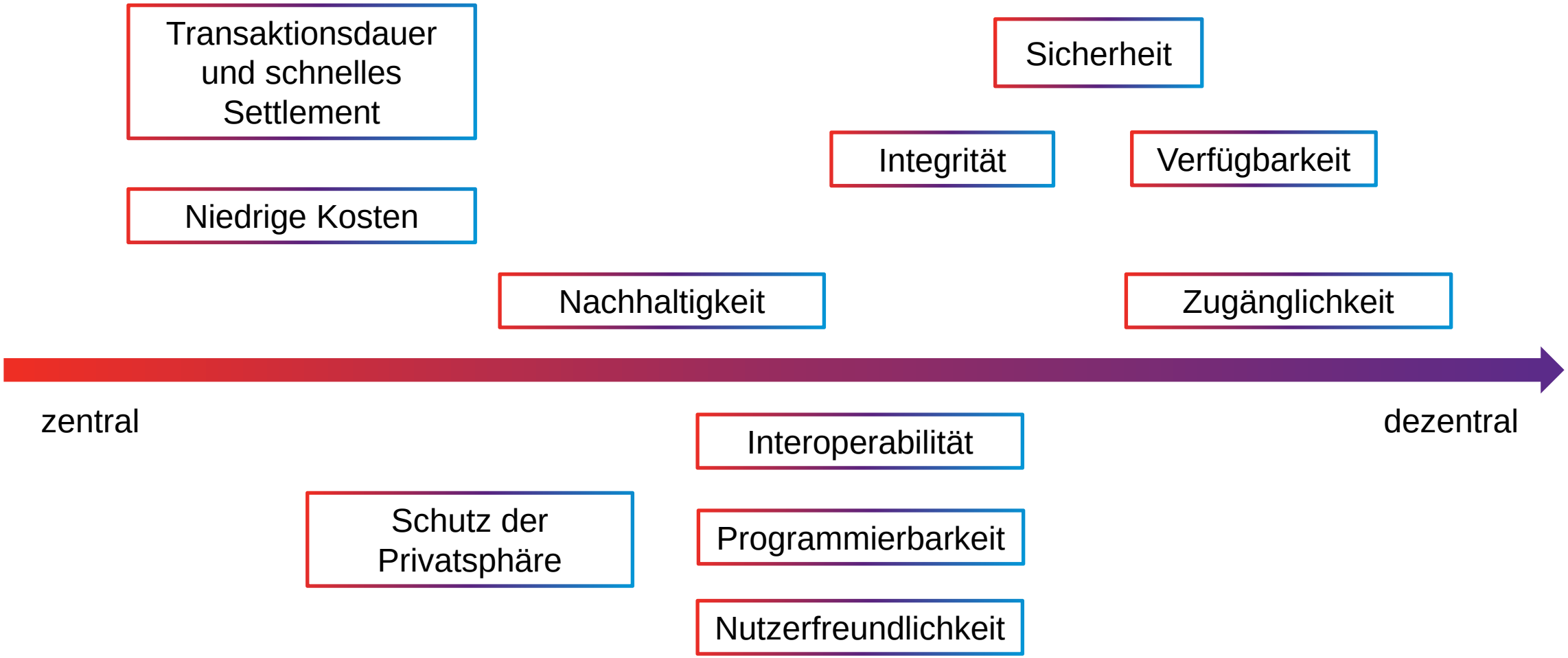
Relevanz digitaler Identitäten für private Zahlungen

Wie kann man “Money Mules“ verhindern, die durch Erpressung / Bestechung erlangt werden können?



- Mann muss es möglichst unbequem und riskant für Personen machen, Zugang zu ihrem Account zu geben
- Private/anonyme Zahlungen sollte man nicht isoliert betrachten, sondern zusammen mit einer digitalen Identität mit hohem Level of Assurance („all or nothing non-transferability“).

Zusammenfassung: Implikationen von zentral vs. dezentral



Limitationen und Ausblick

Nicht nur technologisch zeigen sich in der Diskussion einige Spannungsfelder:

Transparenz
Compliance
Verfügbarkeit

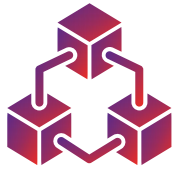
Schutz sensitiver
Daten

Flexibilität
Programmierbarkeit

Sicherheit
Komplexität

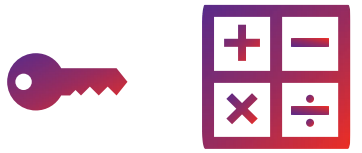
Limitationen und Ausblick

Dezentralisierung in regulierter Umgebung ist ohne die Kombination von Blockchain-Technologie mit anderen Technologien schwer vorstellbar:



Blockchain

Digitale Identitäten



Privacy-Enhancing Technologies

Notwendigkeit interdisziplinärer Forschung
(Informatik, Wirtschaftswissenschaften, Rechtswissenschaften)

Fragen?

Interdisciplinary Centre for Security, Reliability and Trust

Contact:

Johannes Sedlmeir

Research Associate,
FINATRAX Research Group

johannes.sedlmeir@uni.lu

Connect with us

@SnT_uni_lu

SnT, Interdisciplinary Centre for Security, Reliability and Trust