



# Blockchain / DLT / Smart Contracts

Patrick Comboeuf



**There's nothing more  
powerful, than an idea  
whose time has come.**



Victor Hugo, Medieval Tech Visionary

Im Jahre 1999 meinte Wirtschaftsnobelpreisträger Milton Friedman:



# Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto

[satoshi@gmx.com](mailto:satoshi@gmx.com)

[www.bitcoin.org](http://www.bitcoin.org)

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

# Eine logische Weiterentwicklung



Web 1.0

- Broadcasting - 1toN Kommunikation
- Verbinde die Information und erstelle eine Datenbasis für alles.
- Online Kataloge, E-mail...
- B2B

PIPELINE ECONOMICS



Web 2.0

- Bidirektional – Nutzer lesen UND schreiben (Blogs)
- Web Applikationen steuern Prozesse
- Transfer von dynamischen Daten
- B2B – Einkaufsplattformen
- B2C – E-Commerce / Mobile Commerce
- “Social Network Plattformen”, Online Gaming, Streaming & Online Stores

PLATFORM ECONOMICS



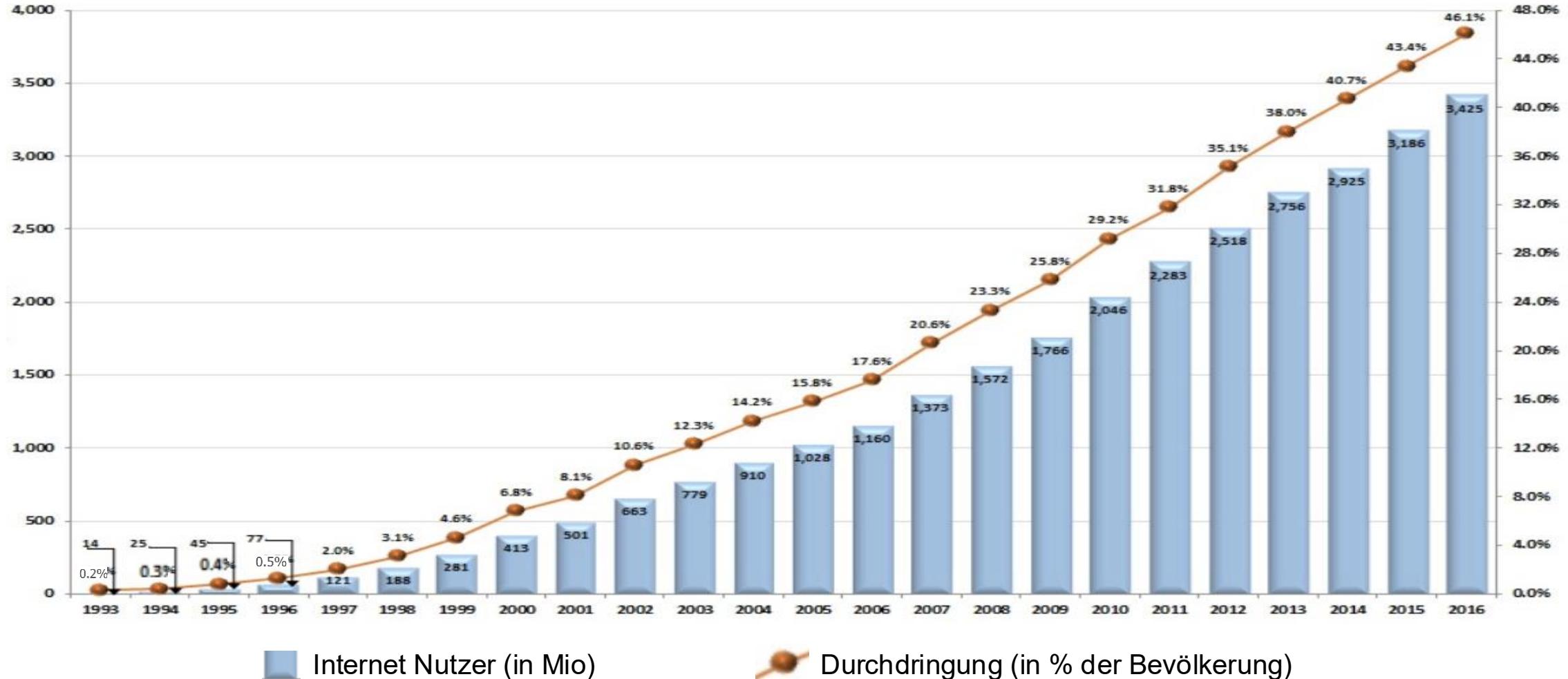
Web 3.0

- Peer-to-peer (P2P) Technologie & dezentralisierte Computer / Netzwerke
- “Internet of Things”
- Datenfokus: Höhere Sicherheit & Vertraulichkeit
- Verbindet Wissen & semantische Suche
- **Transfer von Werten & Rechten**

NETWORK ECONOMICS



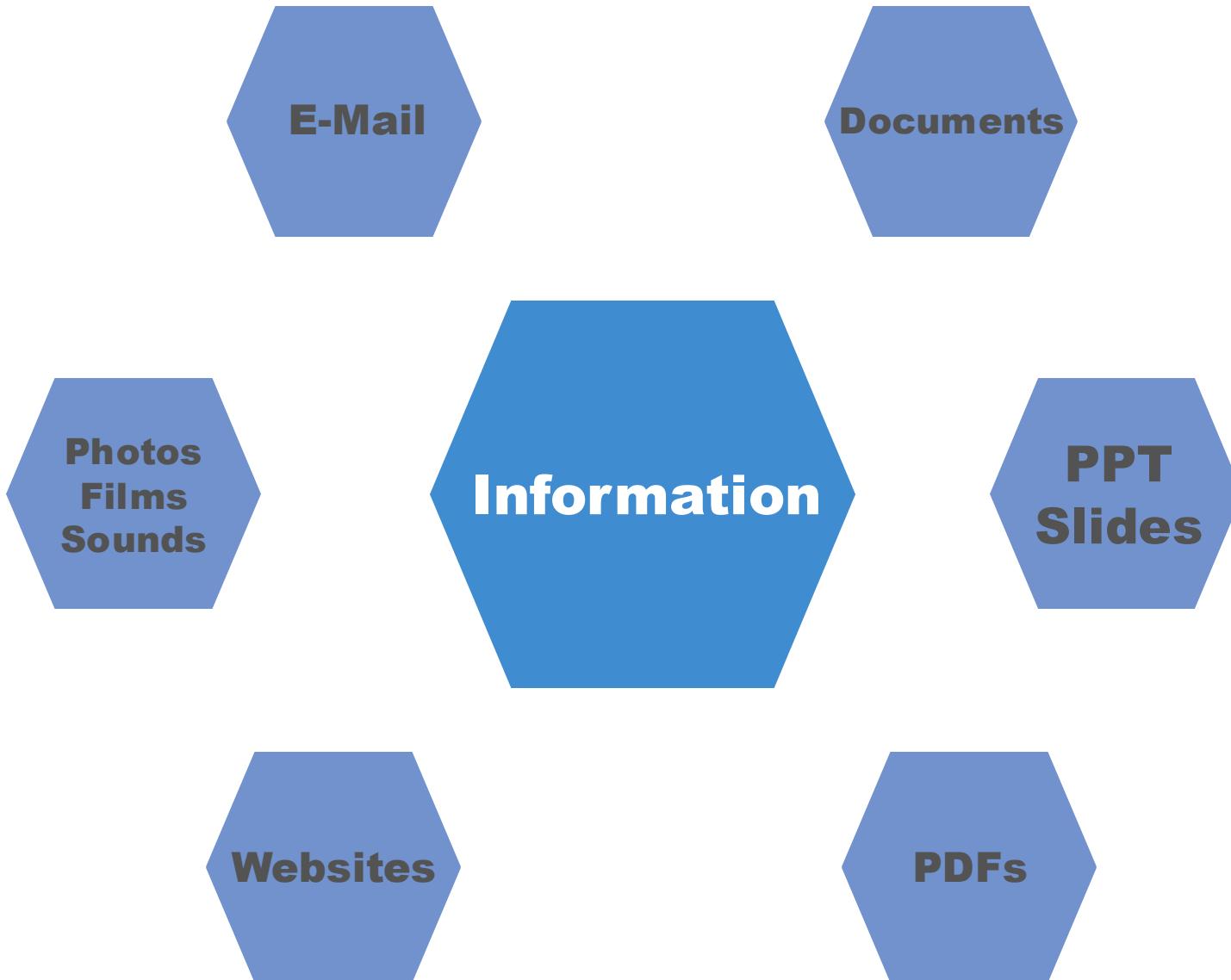
# Die Internet Revolution hat einen langen Weg hinter sich...



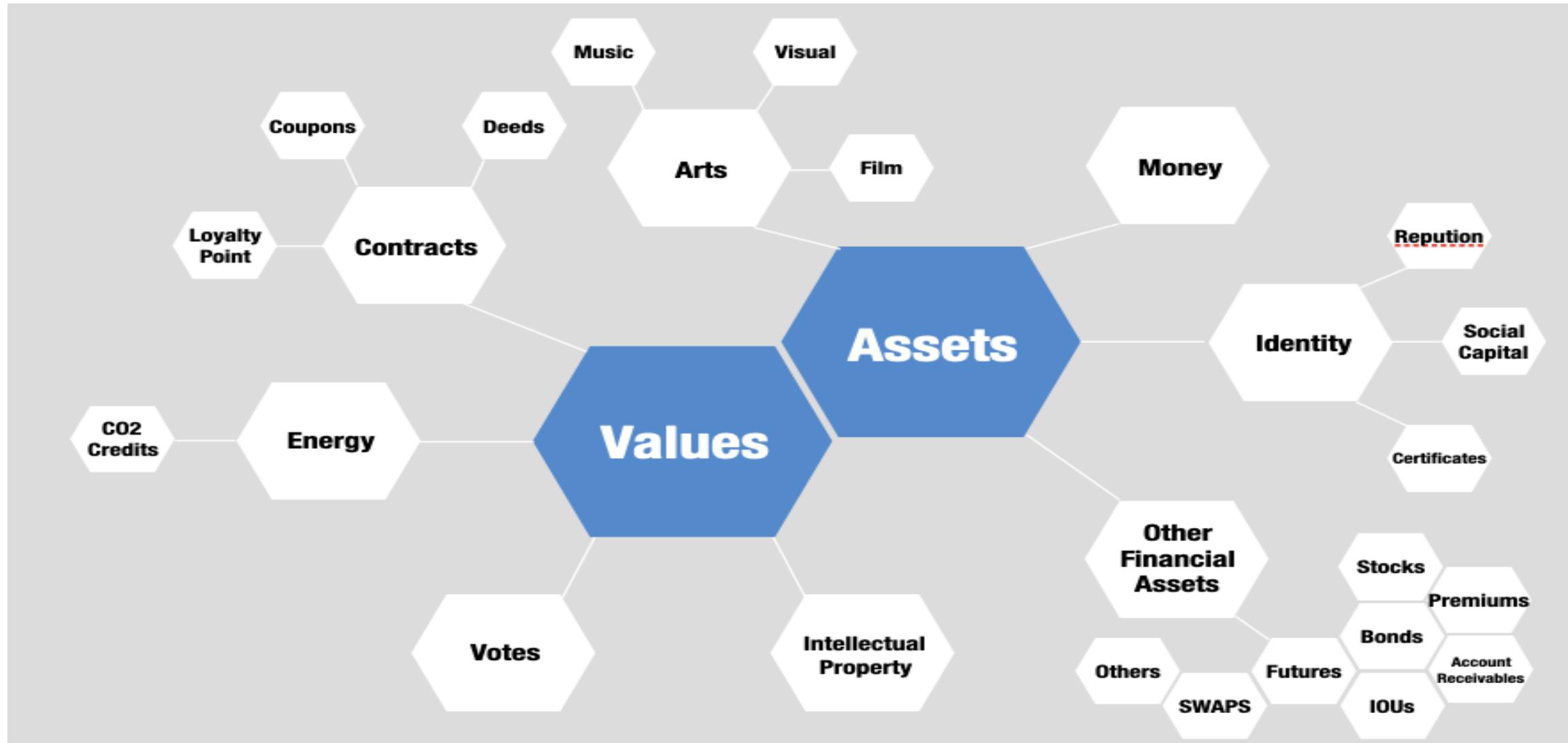
... und Blockchain Adoption (immer) noch einen weiten vor sich.



# Das Internet der Information – Fundament der Digitalisierung

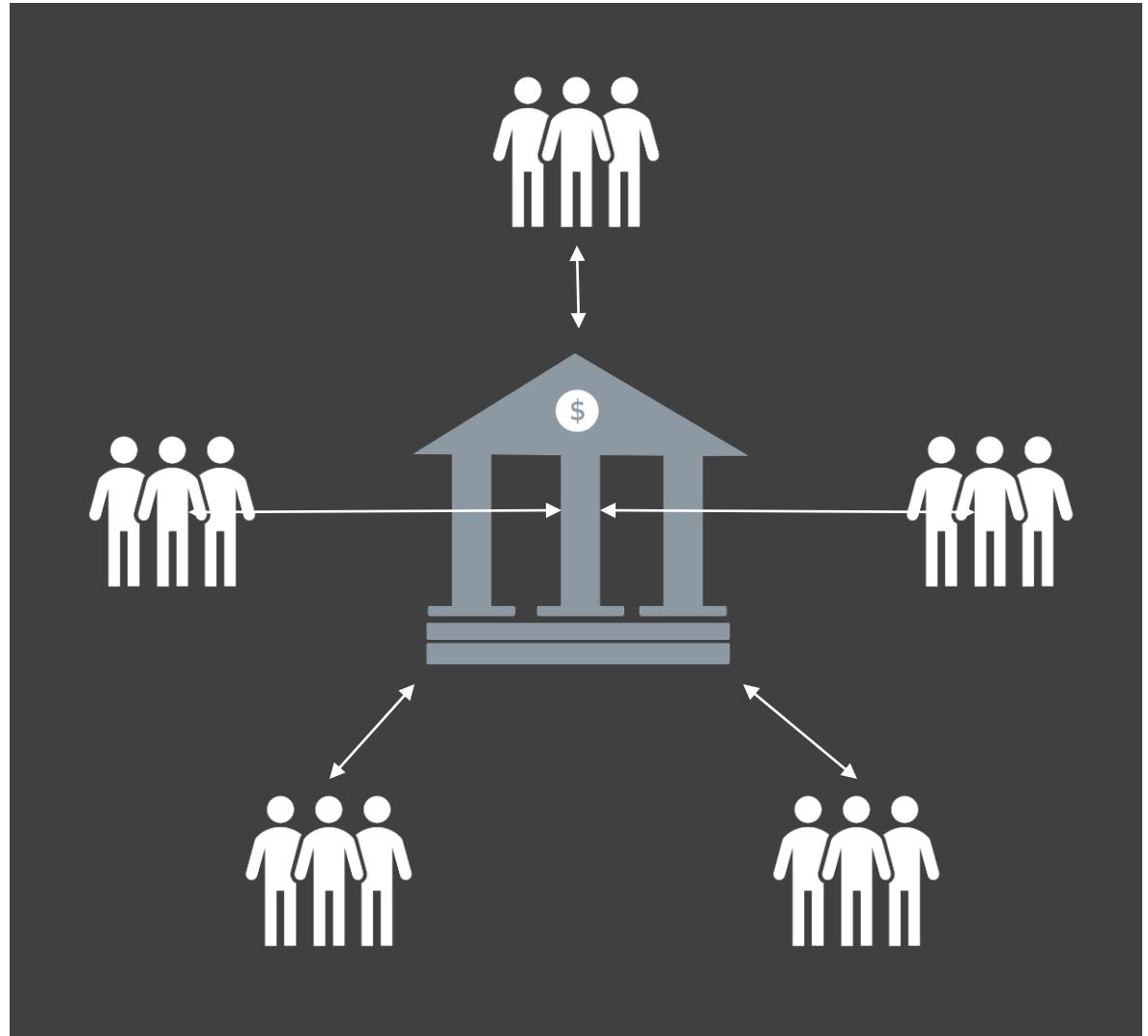


# Erst das Internet der Werte macht digitale Wertschöpfung real



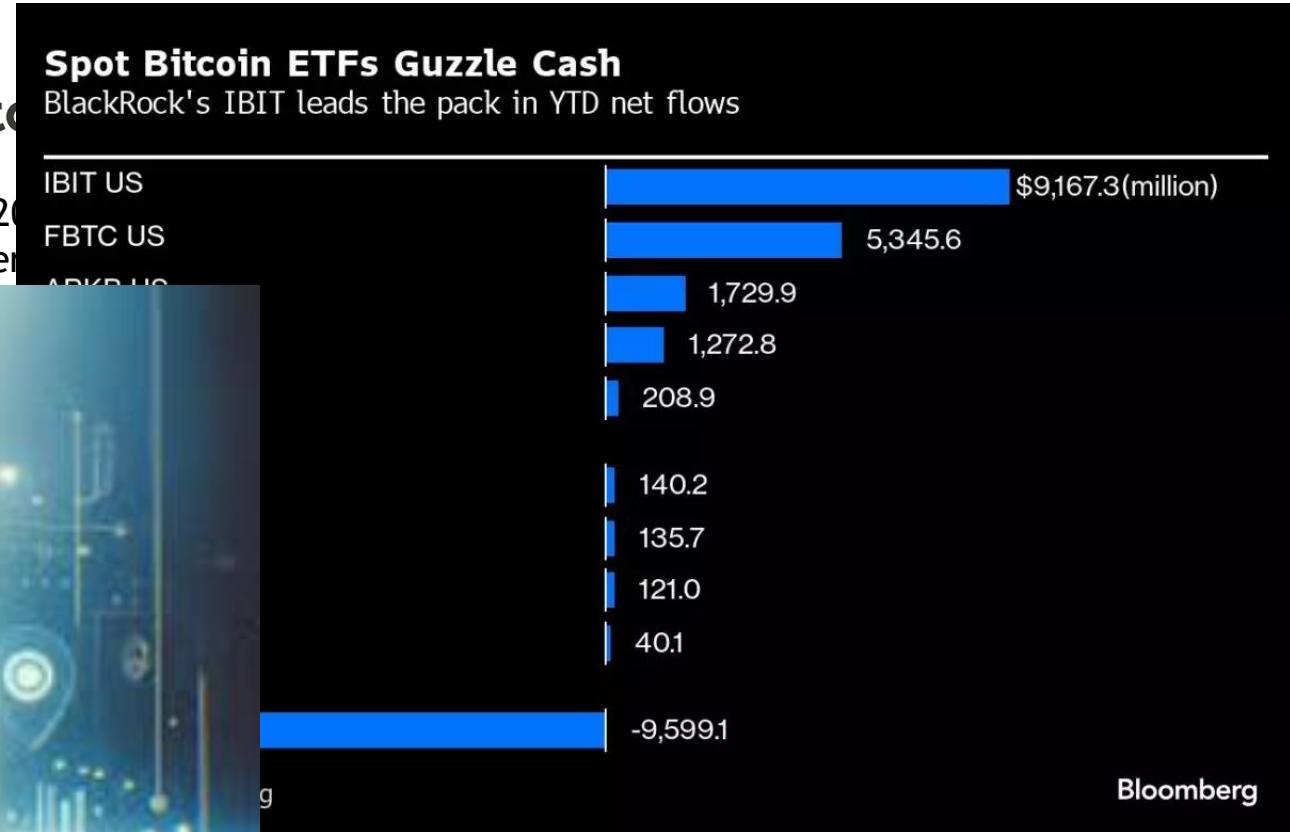
# Der Intermediär

- Der Intermediär garantiert die Transaktionen
  - Daten
  - Rechte
  - Werte
- Der Intermediär garantiert dass Daten zugänglich, sicher speicherbar, nicht duplizierbar, verifizierbar und skalierbar sind.
- Keine direkte Interaktion der Teilnehmenden.



# BLOCKCHAIN UND SMART CONTRACTS

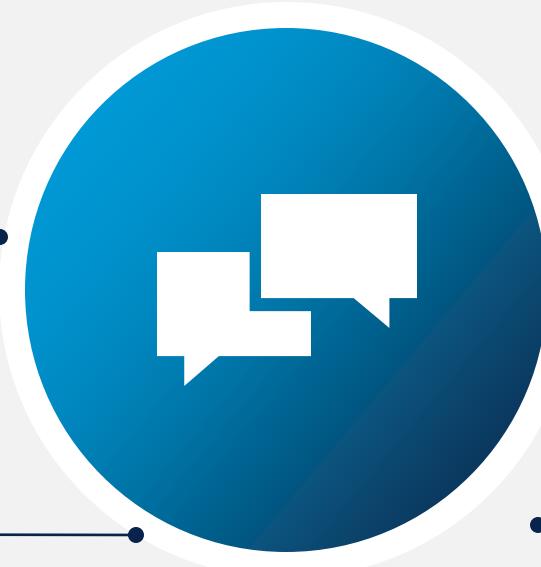
# Vom Spielplatz der Nerds zum Fundament der Finanzindustrie 2.0



# Die öffentliche Meinung wandelt sich...

„A central bank issuing its own crypto currency is no science fiction. Embrace change!“  
Christine Lagarde, Governor, European Central Bank

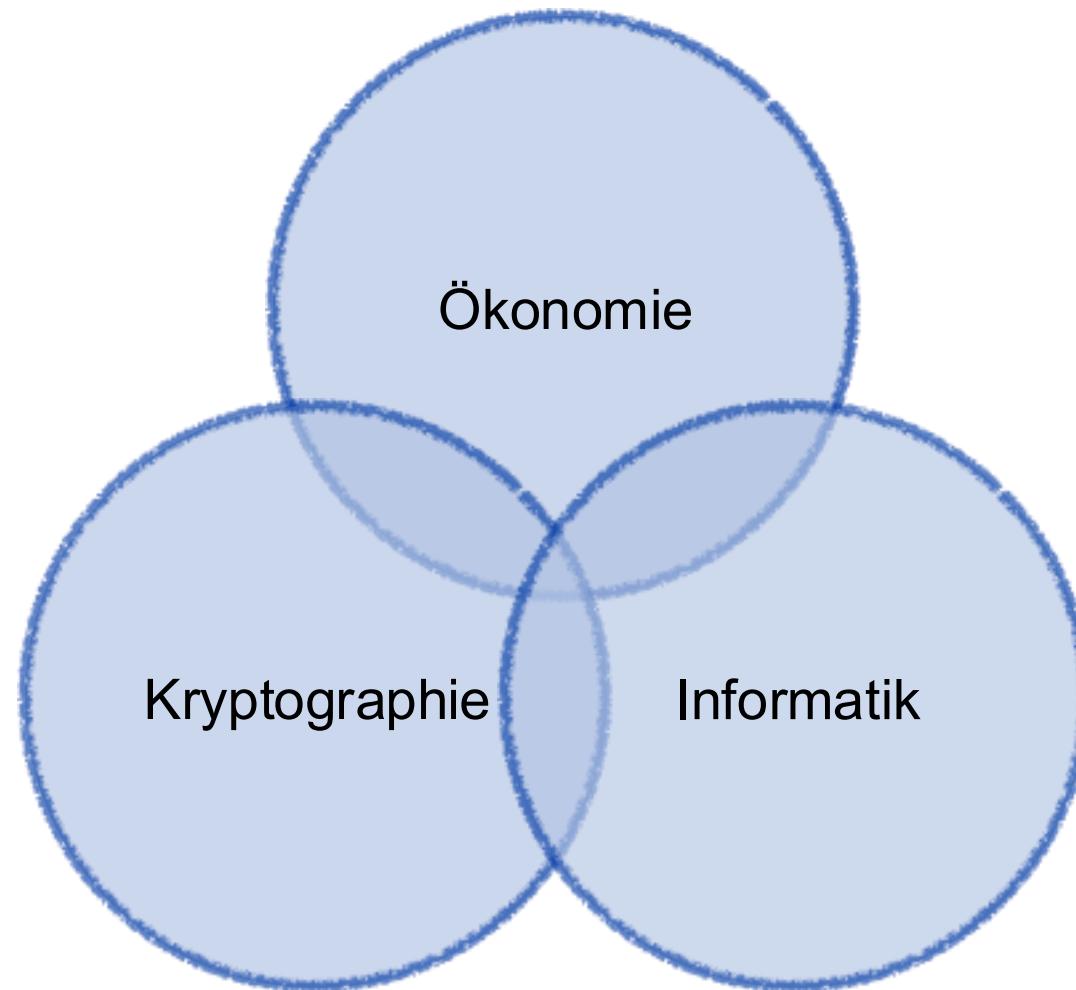
„Blockchain is the single biggest discovery this generation is going to witness in their life time“  
Anton Golub, Slovenian-Swiss Entrepreneur



“Most technologies tend to eliminate workers on the periphery. Blockchains automate away the center. Instead of putting the taxi driver out of a job, blockchain puts Uber out of a job and lets taxi drivers & clients interact directly.”  
Vitalik Buterin, Co-founder Ethereum

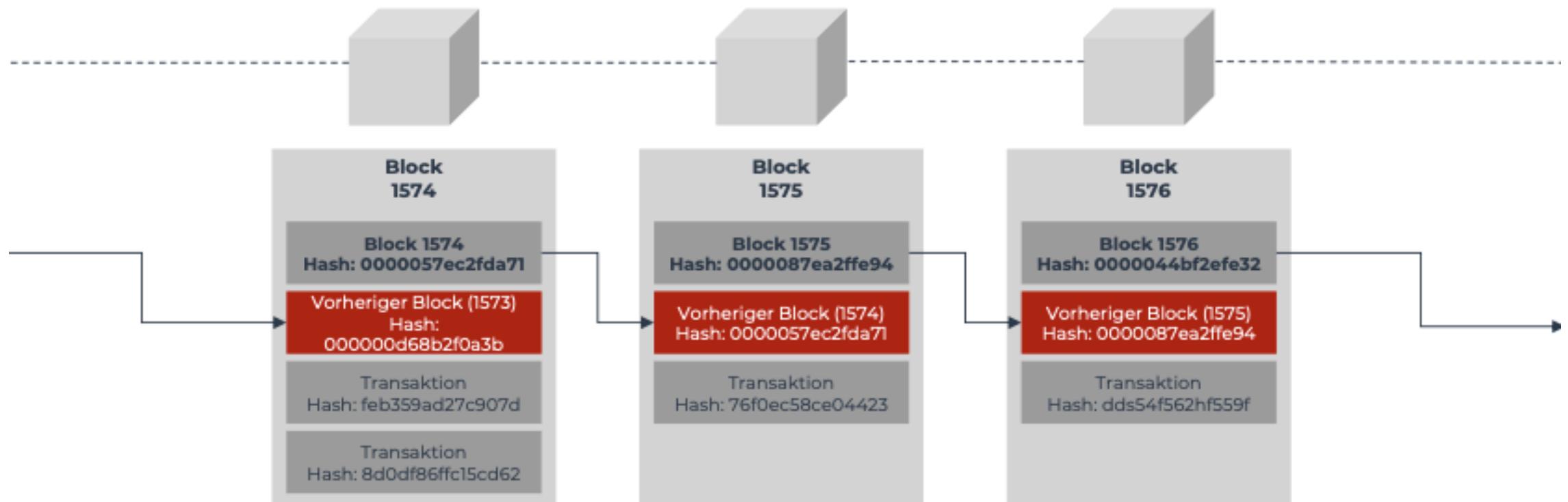
“Every informed person needs to know about Blockchain because it might be one of the world’s most important developments.”  
Leon Luow, Nobel Peace Prize Nominee

# Blockchain = Dezentrale Interdisziplinarität

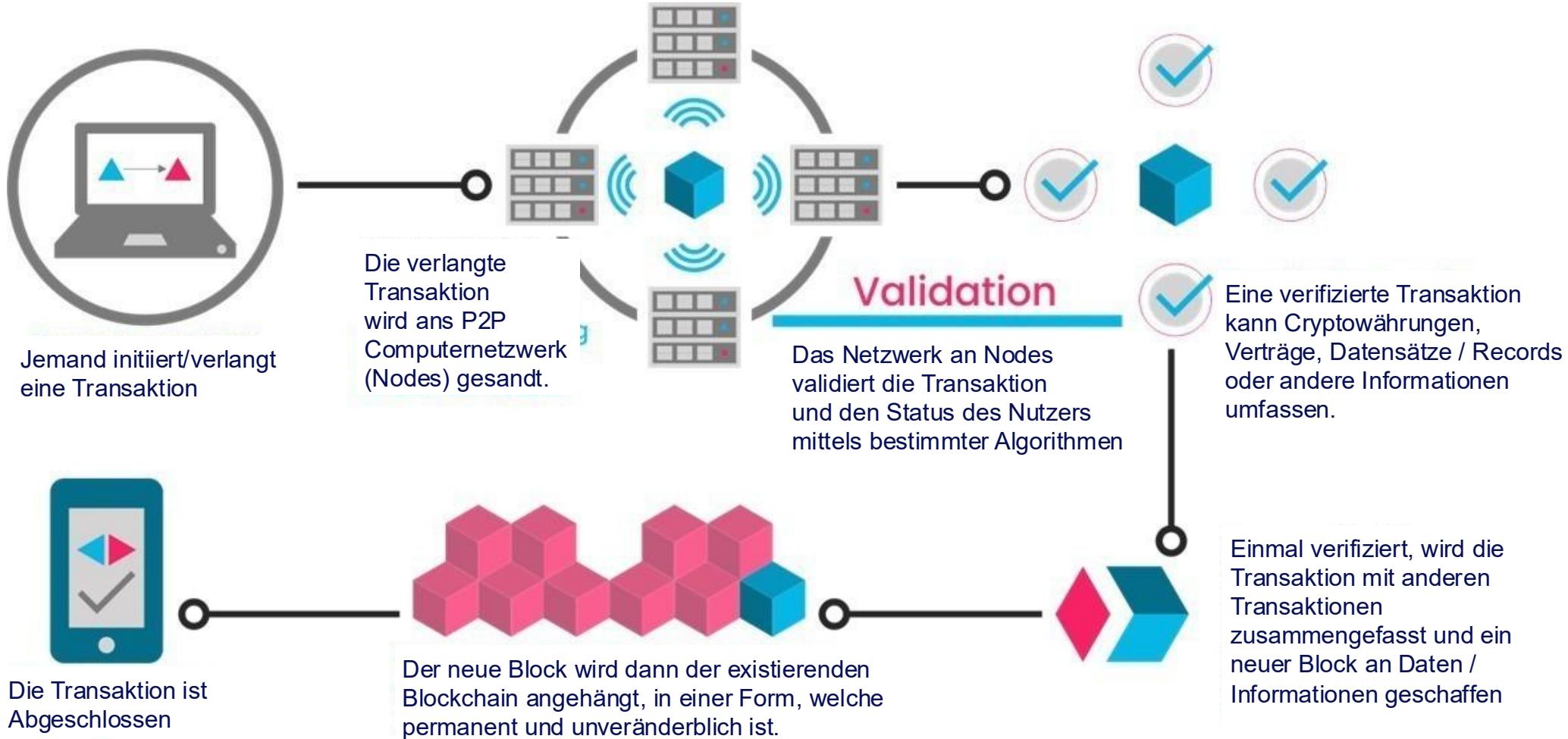


# Die grundlegende Funktionsweise einer Blockchain

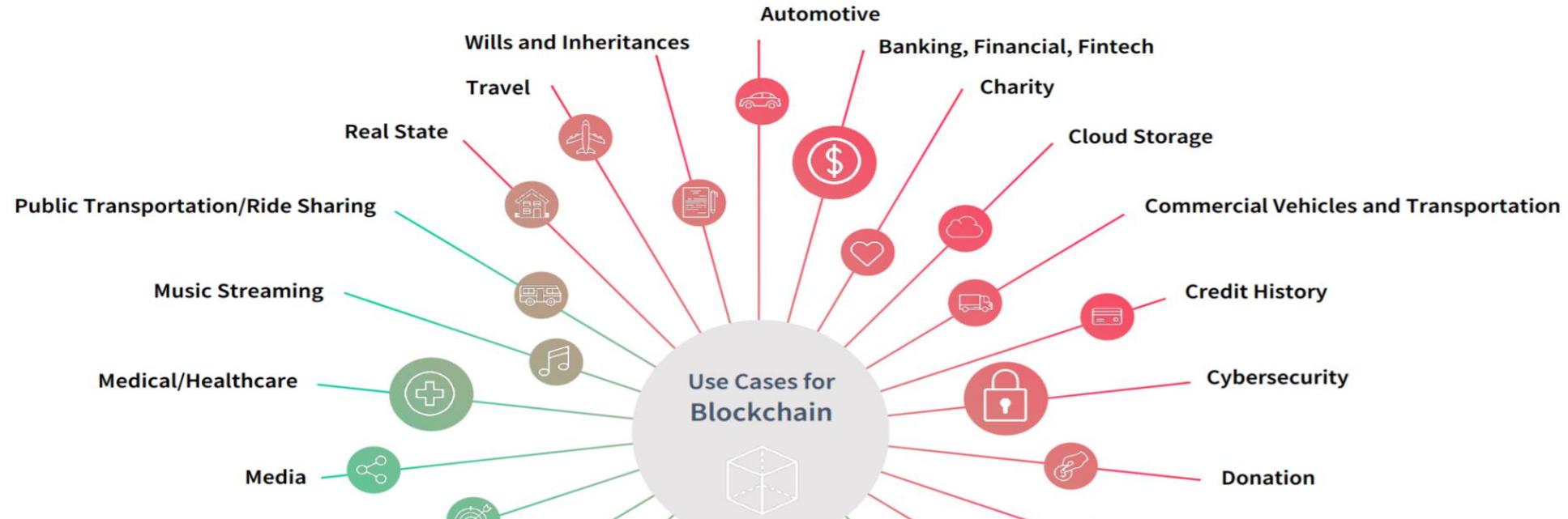
Die Blockchain verdankt ihren Namen der Art und Weise, wie sie Transaktionsdaten speichert – in Blöcken, die zu einer Kette verknüpft sind. Diese Blöcke erfassen und bestätigen die Zeit sowie die Reihenfolge der Transaktionen, die anschließend durch Knoten (Nodes) in einem dezentralen Netzwerk protokolliert werden.



Ein kontinuierlich erweitertes Hauptbuch, mit Datensätzen (Blöcken), die über kryptographische Verfahren miteinander verkettet sind.



# Anwendungsfälle mit offensichtlichem Nutzenpotential

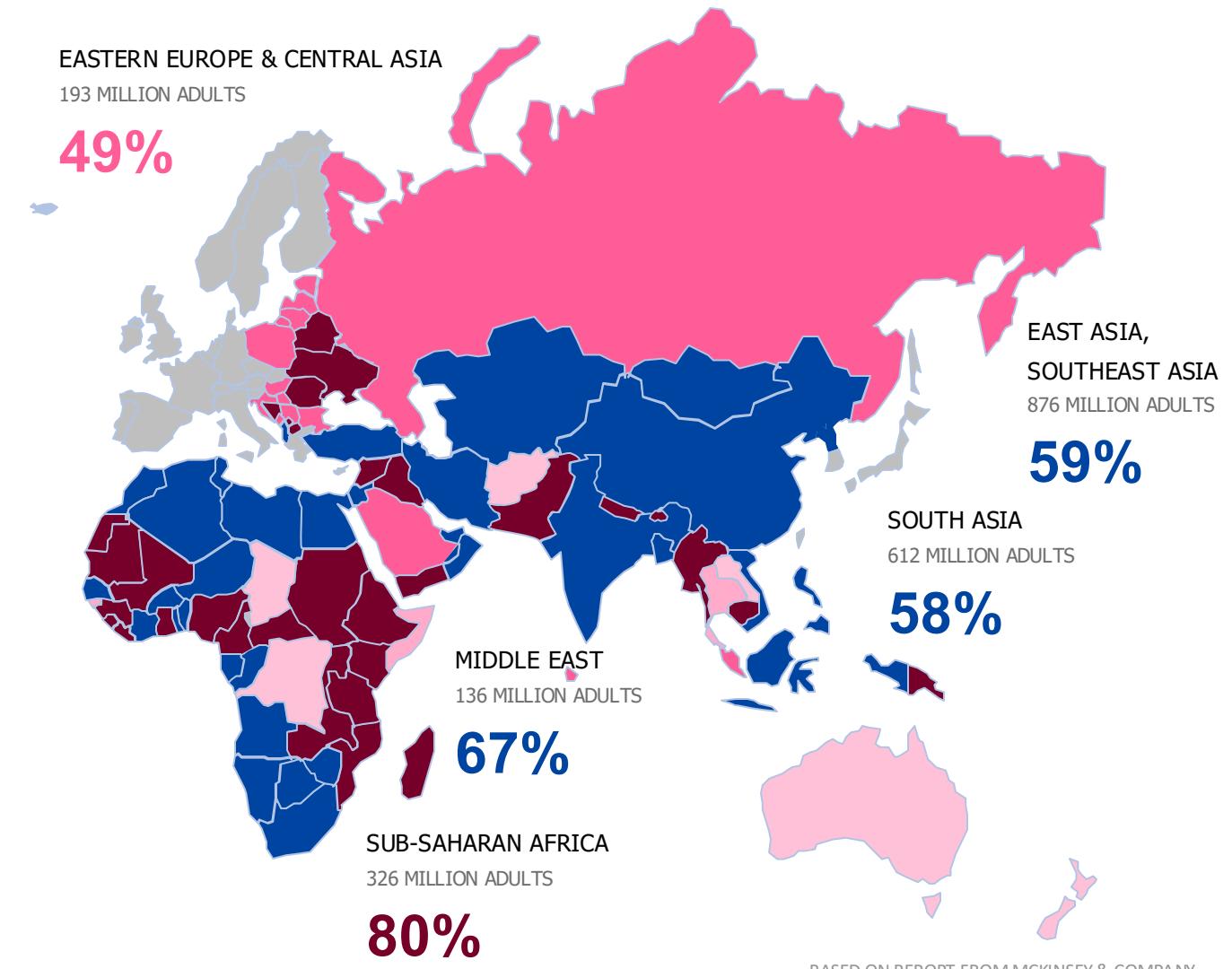
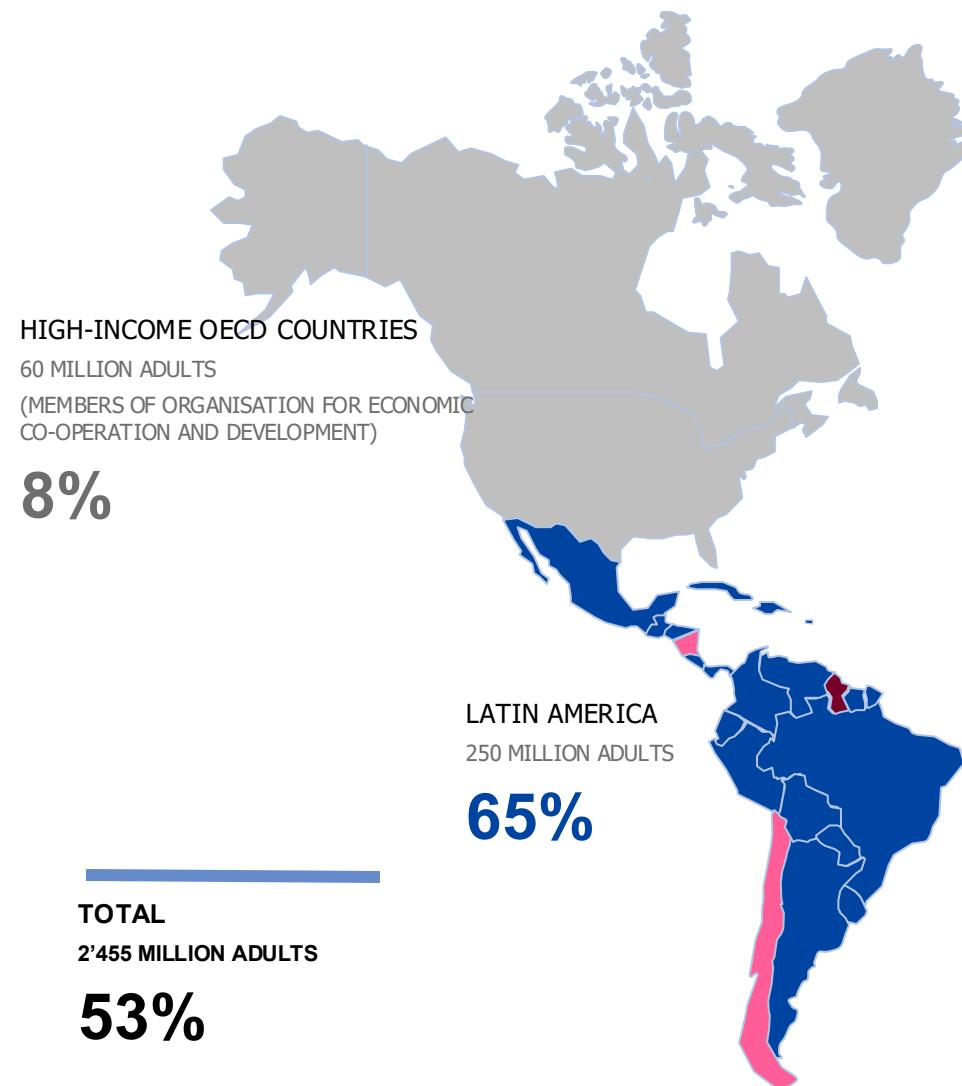


The background of the slide is a close-up photograph of numerous gold-colored digital currency coins, such as Bitcoin and Ripple, scattered across a dark surface. The coins are highly reflective, with bright highlights and deep shadows, giving them a metallic and valuable appearance.

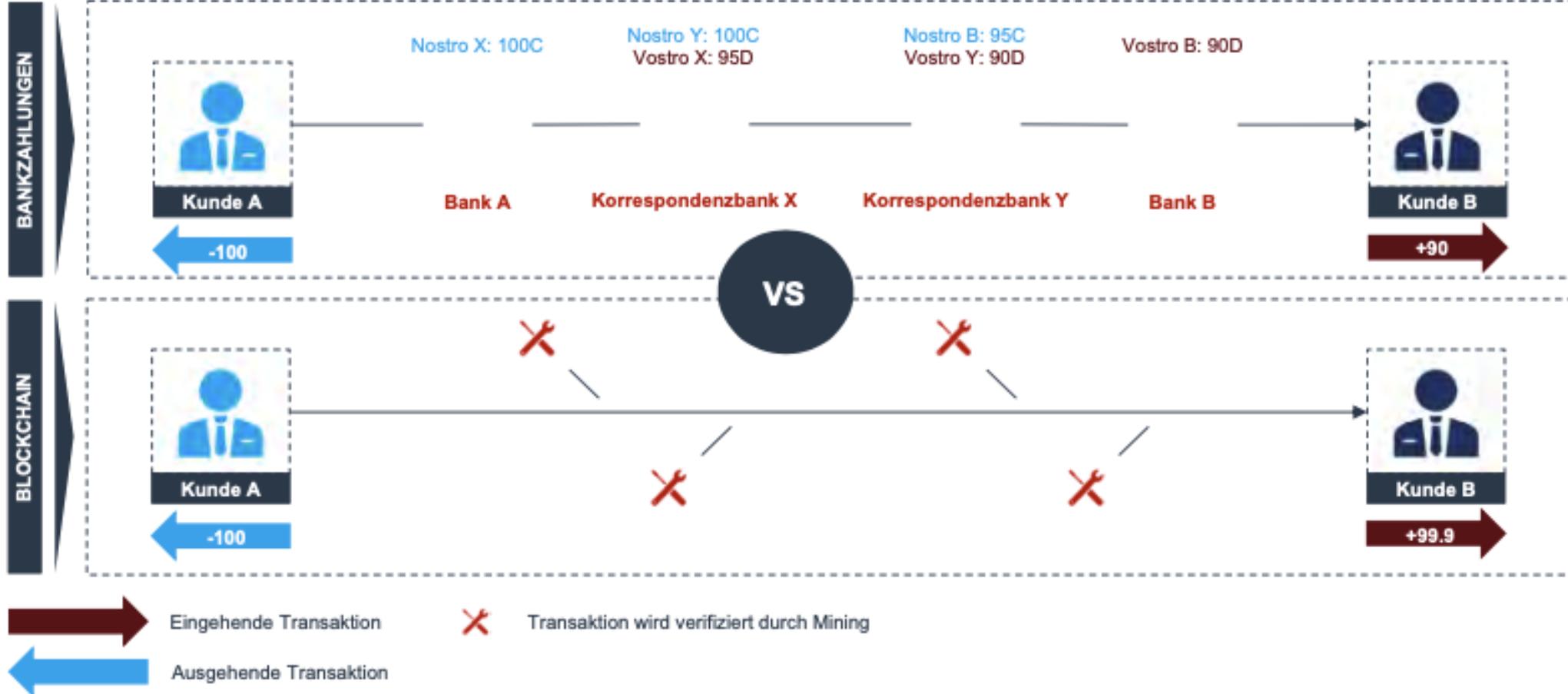
# CRYPTOWÄHRUNGEN

## BANKING THE UNBANKED? UNBANKING THE BANKS?

# Heute sind mehr als 2 Milliarden Menschen von der globalen Wirtschaft ausgeschlossen



# Bankzahlungen vs. Blockchain Transaktionen



# Reality Check: Kryptoassets als Zahlungsmittel?

**Fakt: Bitcoin ist als Zahlungsmittel eher ungeeignet**



## Kryptoassets als Zahlungsmittel

- Skalierbarkeit ✓
- Wartezeit ✓
- Volatilität ?

## Kryptoassets als Anlageklasse

- Hochrisikoanlage
- Interessant zur Diversifikation & als Inflationsschutz

# Stablecoins – digitale Abbildung eines analogen Vermögenswerts



[https://www.swissbanking.ch/\\_Resources/Persistent/1/5/7/f/157f655cec38f6e67e25dc346034786a35e81190/SBVg\\_Der\\_Buchgeld\\_Token\\_DE\\_2023.pdf](https://www.swissbanking.ch/_Resources/Persistent/1/5/7/f/157f655cec38f6e67e25dc346034786a35e81190/SBVg_Der_Buchgeld_Token_DE_2023.pdf)



Fiat-backed



Commodity-backed



Crypto-backed



Algorithmic

Bildquelle: SwissBanking.org

# VENTURE CAPITAL

## CROWDFUNDING ON STEROIDS

# Kapitalbeschaffung - Token Offerings über die Blockchain

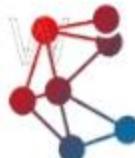
Token Offerings werden zu einer bevorzugten Alternative zu klassischen Kredit- / Kapitalfinanzierungen für KMUs, StartUps aber auch für etablierte Unternehmen und Projekte

<b>ICO</b>	Finanzierung einer neuen Kryptowährung	Website des Krypto-Startups	Kaum reguliert, Gefahr eines <b>Scams</b>
<b>IEO</b>	Finanzierung einer neuen Kryptowährung	Kryptobörse	Reguliert über die Kryptobörse
<b>STO</b>	Finanzierung einer neuen Kryptowährung	Security-Token-Plattform	Reguliert durch die SEC



## Case Study Daura AG

Wir bringen KMU an den Kapitalmarkt.

**Einfach. Digital.**  daura

# Vom Wertpapier zur digitalen Aktie



**Token Download**

Hier können Sie ihre digitale Aktie als Token herunterladen.

Issuer	Anzahl	Nominalwert pro Aktie
Schoggi AG	10	CHF 1.00

Bitte markieren und kopieren Sie den Token in die Zwischenablage. Sie benötigen ihn im nachfolgenden Schritt.

**Token**

```
LZBTrYgzVFLKOkYip9AT3v2tVTIla/ZIWeUFUe1fe4MQliYec/QcyYAIP6gNBF3Ai  
7KZ9bkt+tE8UaE/bXO9+w
```

Speichere Token in Token Speicher.

Mit der Token Speicher Funktion können Sie Ihren Token verschlüsselt in Ihrem Browser speichern.

**Abbrechen** **Weiter**

# Vorteile von Token gegenüber herkömmlichen Aktien



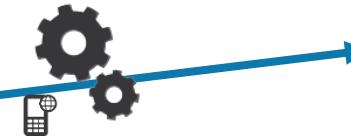
## Wertpapier

- Direkter Eigentumsnachweis durch Urkunde
- Herausgabe, Verteilung und Corporate Actions aufwendig
- Funktionen manuell (Transfer, Dividenden Zahlungen, ...)



## Bucheffekte

- Effizienter als Wertpapier, jedoch hohe IT-Komplexität
- Zentralisierte Administration durch Bankensystem – Eigentumsnachweis über Intermediär
- Funktionen werden als Dienstleistung durch Banken erbracht



## Token

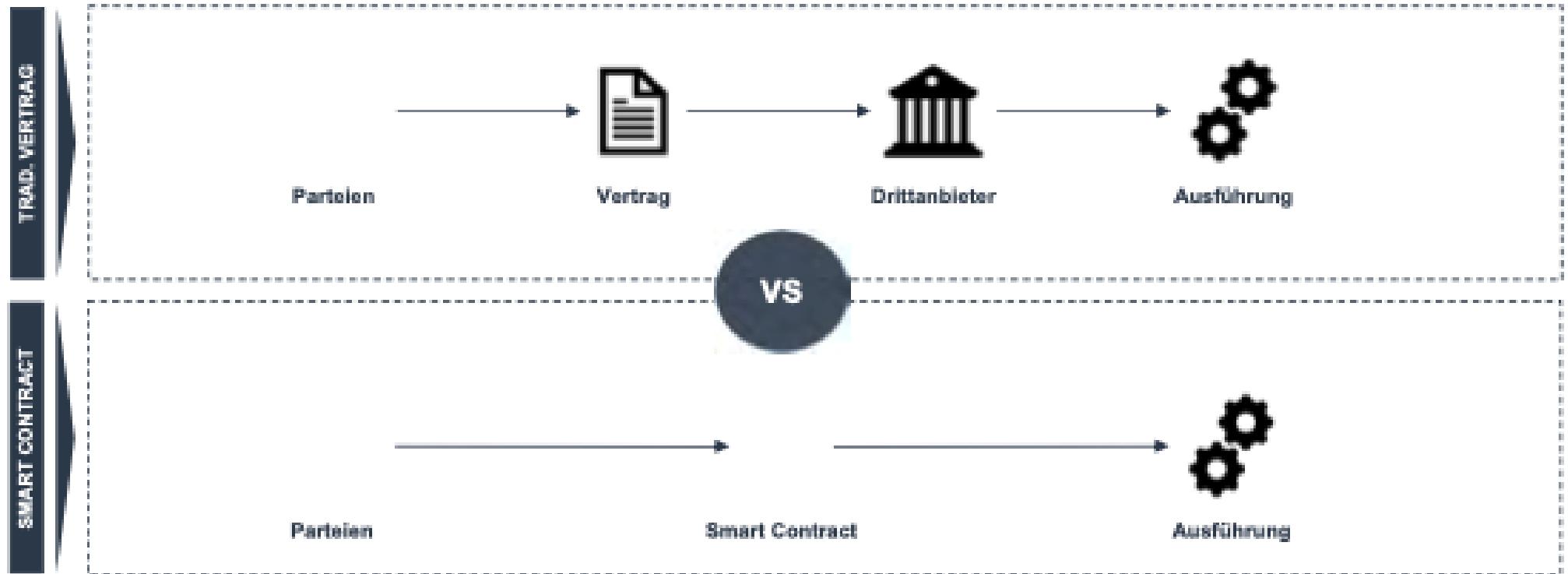
- Herausgabe und Verteilung direkt durch den Emittenten
- Direkter Eigentumsnachweis und Übertragung\* durch Token
- Funktionen in der Aktie integriert: Software defined security

\*Bei Registerwertrecht nach OR 973d

# SMART CONTRACTS

PROZESSINNOVATION &  
RECLAIM DATA SOVEREIGNITY

# Traditionelle Verträge vs. Smart Contracts



Quelle: Eigene Darstellung

# Was ist ein Vertrag? (Hint: steht in Art. 1 OR)

## Art. 1 OR

A. Abschluss  
des Vertrages  
I. Überein-  
stimmende  
Willensäußerung  
1. Im  
Allgemeinen

- 1 Zum Abschlusse eines Vertrages ist die übereinstimmende gegenseitige Willensäußerung der Parteien erforderlich.**
  
- 2 Sie kann eine ausdrückliche oder stillschweigende sein.**

# Smart Contracts: Selbstausführende Programme (Code)



## Was ist ein Smart Contract?

- Dezentral ausgeführtes Skript
- „Lebt“ auf der Blockchain
- Berechnet von tausenden von Computern

## Beispiel: Dezentrales Casino

- If, then, else



## Ganze dezentrale Organisationen

- Governance, Voting

# Smart Contracts & Prozessinnovation: 4 zentrale Hebel

## Datenversiegelung



### Dateneigentum & Datenspeicherung

- Digital ID & Reputation
- Kein Identitäts-Diebstahl
- Rechte an den eigenen Daten

## Wertetransfer



### Globaler Transfer von digitalem Eigentum

- Währungen
- Eigentumsrechte
- Tokenisierte Assets

## Rückverfolgbarkeit



### Unveränderbare, transparente Transaktionen

- Unabänderliches Register
- Vertrauenswürdigkeit
- Herkunfts-nachweise

## Automatisierung



### Smart Contracts in parametrisierten Prozessen

- Event-gesteuerte Automatisierung
- Schlichtung

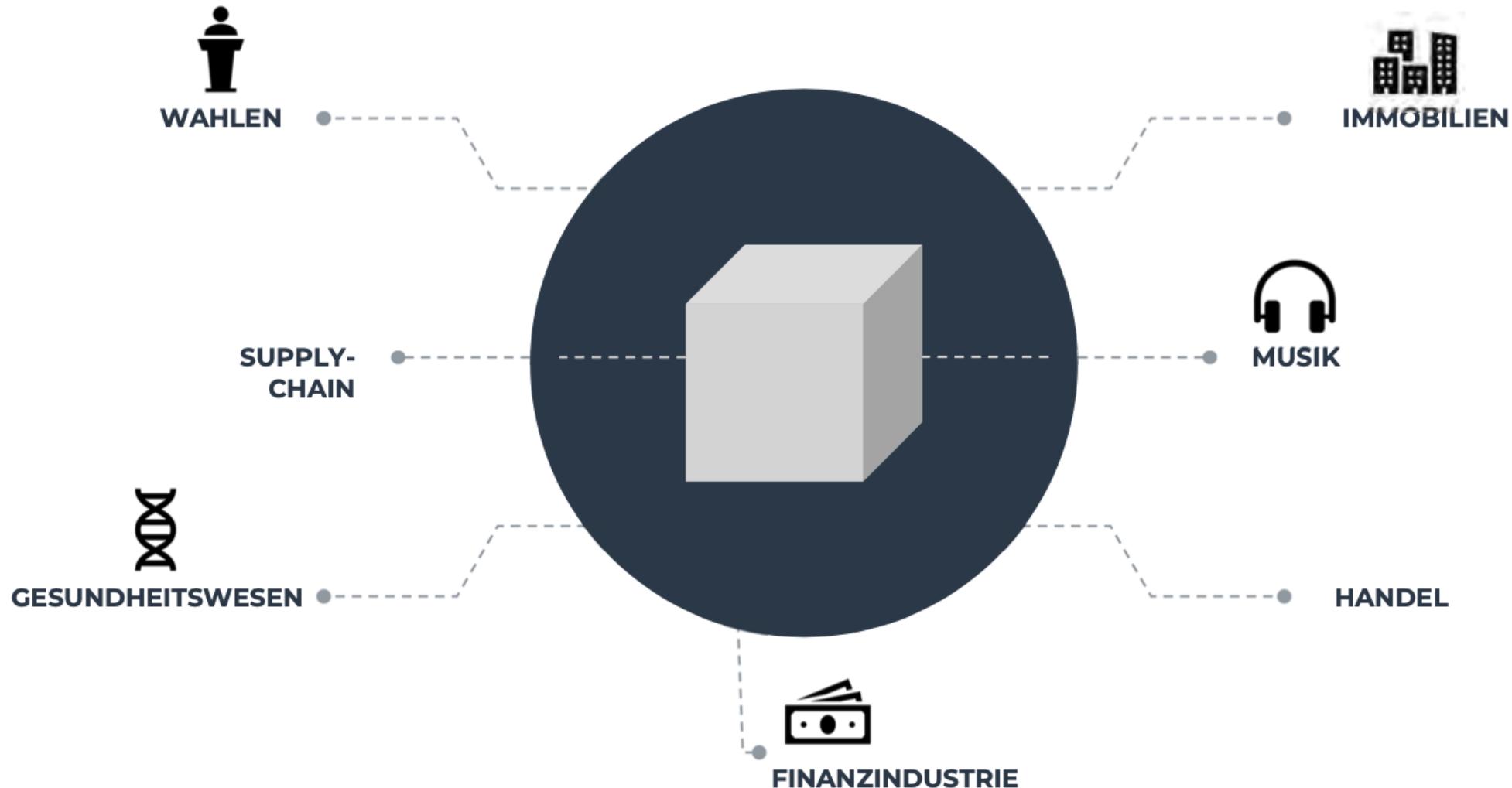
# Pros and Cons



**Komplexität**  
**Falscher Code**  
**Nachträgliche Änderungen**

**Autonomie**  
**Vertrauen**  
**Backup**  
**Sicherheit (Kryptografie)**  
**Schnelligkeit**  
**Günstig**  
**Genauigkeit**

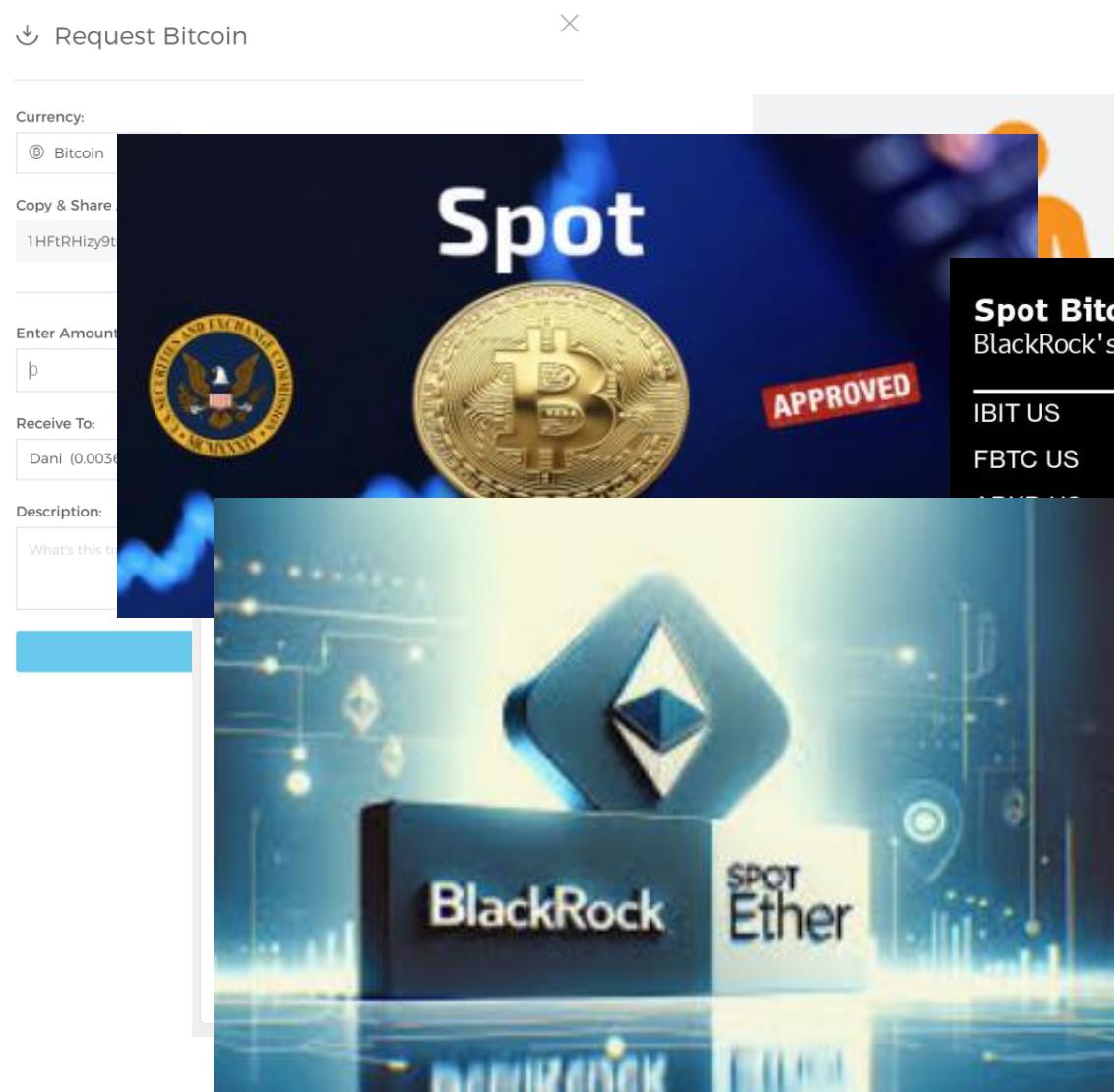
# Praktische Anwendungsgebiete von Smart Contracts



# Weitere Finanz- Instrumente

The background image shows a panoramic view of the Tokyo skyline at dusk or night. The Tokyo Tower is prominently featured on the left side, its illuminated orange-red structure standing out against the darkening sky. The city is densely packed with numerous skyscrapers of varying heights, their windows glowing with lights. In the foreground, there's a mix of lower residential buildings and taller commercial structures. A river or bay area is visible in the middle ground, with several bridges spanning it. The overall atmosphere is one of a bustling, modern metropolis.

# Klassische Finanzabsicherungsinstrumente für Crypto



# Tokenisierung realer Vermögenswerte z.B. von Kunstwerken

Aufteilen des Eigentums in Bruchteile erlaubt die Umwandlung von Millionen-teuren Kunstwerken in digitale Finanzeinheiten, die einfach ver- & gekauft werden können.



51 %  
49 %



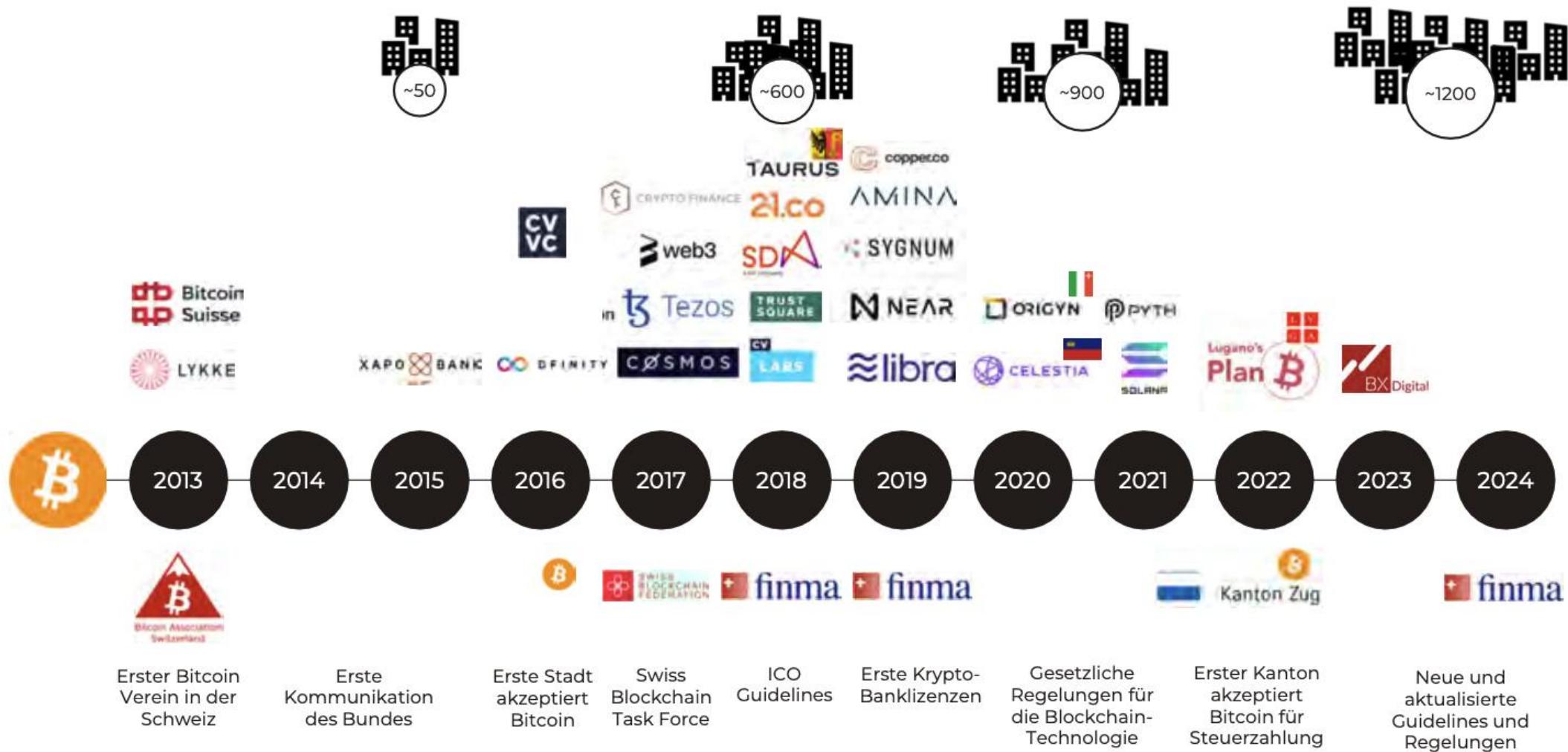
Rembrandt Holy Family

# BLOCKCHAIN

## UND DIE

### SCHWEIZ

# Die Entstehung des Crypto Valley



# Die Schweizer Pioniere

## Krypto-Dienstleister



Zug, seit 2013



Zürich, seit 2017

## Krypto-Banken



Zürich, seit 2019



Zug, seit 2019  
(ehemals SEBA)

## Krypto-Börsen

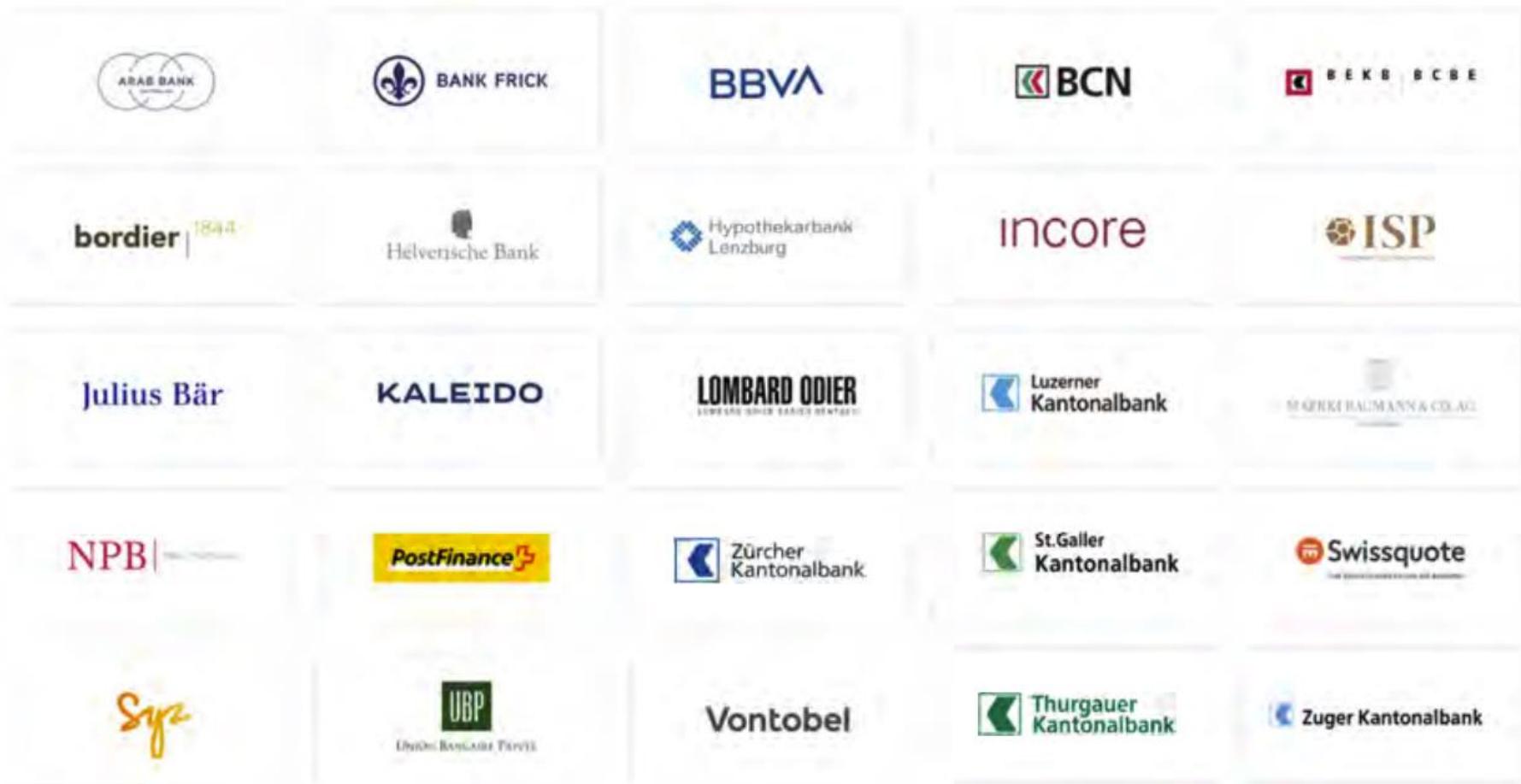


Zürich, seit 2018



Zürich, seit 2023

# (Schweizer) Banken erobern den Krypto Markt



Quelle: Eigene Darstellung / Logos von der Website der jeweiligen Finanzinstitute

# Die Institutionalisierung von Kryptowährungen & Digital Assets



**Professionalisierung**



St.Galler  
Kantonalbank



**Volumina**

AMINA



**Regulation**



PostFinance



SYNUM



**Standardisation**



Zürcher  
Kantonalbank



**Partnerschaften**

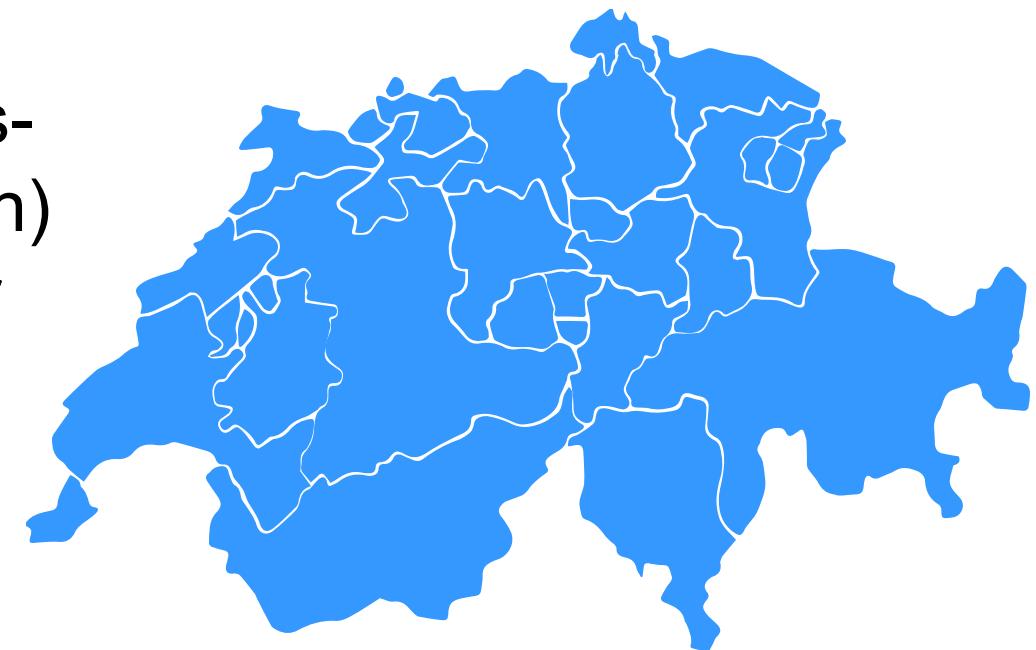


CRYPTO FINANCE | DEUTSCHE BÖRSE  
GROUP

Bildquelle: Eigene Darstellung / Logos von der Website der jeweiligen Finanzinstitute

# Und die Schweiz?

„Für eine kleinräumige Volkswirtschaft ohne natürliche Ressourcen - dafür mit berechenbaren Politik- & Rechts-Strukturen - sind dezentrale (Fintech) Ecosysteme ein wichtiger Hebel zur Wohlstandssicherung.“



#BlockchainNationSwitzerland ist deshalb viel mehr als eine Vision, sondern ein Pakt mit der Zukunft.“

Ex-Bundesrat Ueli Maurer, Finanzminister





Let's break for lunch until

13.00 sharp

# **Vielen Dank**

Please connect on LinkedIn