Bitcoin, Blockchain, NFTs: Was steckt dahinter?

Marcel Waldvogel

VHS Stein am Rhein • 2022-05-18

Es gibt zwei Arten von Vorträgen

1. Was Sie gerne hören würden
2. Was Ihnen mal jemand sagen müsste

Dies ist ein Kategorie-2-Vortrag.

Folie original von Felix von Leitner: *Hype-Tech*, 2021. (Vortrag vor Bankern, weshalb Banken wahrscheinlich Blockchain, Smart Contracts, Big Data, Machine Learning/KI etc. nicht brauchen, auch wenn es ihnen alle, insbesondere Berater und ihre eigenen IT-ler, verkaufen wollen.)

NFT

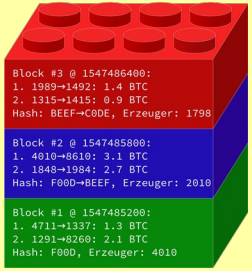
DAO

Smart Contract

Rote Titel =
Inhalt für
Fortgeschrittene

Kryptowährung

Bitcoin
Ether
+10'000 andere



Blockchain

1. Versprechen
2. Technik
3. Vergleich

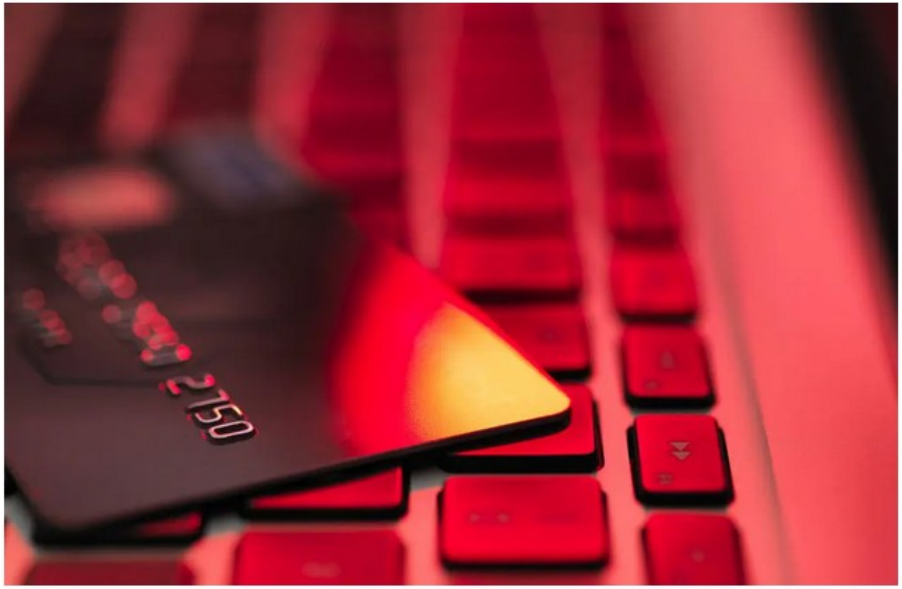
Neue Zürcher Zeitung

Blockchain – der nächste Wohlstandsschock

Blockchain ist mehr als eine digitale Technologie. Es ist ein System, das die Chance bietet, Eigentumsverhältnisse viel einfacher und günstiger zu sichern und zu ordnen. Das wird Konsequenzen haben.

Konrad Hummler

03.05.2016, 07.00 Uhr



Eigentum etabliert eine herrschaftliche Beziehung zwischen Person und Sache. (Bild: Imago)

Startpage

blockchain anwendungen

Web Images Videos News

Any time All regions Family filter: On

Web results

https://morethandigital.info/blockchain-moeglichkeiten-und-anwendung...

28 Blockchain Use Cases - Mögliche Anwendungen der Distributed ...

Blockchain Anwendungsbeispiele bei Banken und Finanzinstituten · Internationale Zahlungen · Peer-to-Peer (P2P) Transaktionen · Kapitalmärkte · Handelsfinanzierung.

https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain...

BLOCKCHAIN: GRUNDLAGEN, ANWENDUNGEN UND POTENZIALE

oretische Einordung der Technologie vorgenommen, **Blockchain-Anwendungen** untersucht so- wie die aktuellen Entwicklungen in der Praxis analysiert.

https://weissenberg-group.de/wofuer-kann-die-blockchain-technologie...

Wofür kann die Blockchain-Technologie eingesetzt werden?

... kann im Rahmen zahlreicher **Anwendungen** implementiert werden. Im Folgenden geben wir einen Überblick über die Vielseitigkeit der **Blockchain**-Technologie.

https://www2.deloitte.com/ch/de/pages/risk/articles/security-controls-f...

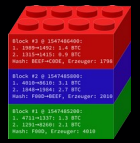
Sicherheitskontrollen für Blockchain-Anwendungen | Deloitte Schweiz

Sicherheitskontrollen für **Blockchain-Anwendungen**. **Blockchain**-Technologie hat ihre Einsatzfähigkeit über das Gebiet der Kryptowährungen hinaus bewiesen und ...

https://www2.deloitte.com/de/de/pages/innovation/contents/Blockchain...

Was sind die Chancen und Risiken der Blockchain? - Deloitte

Blockchain Anwendungsbeispiele bei Banken und Finanzinstituten



Internationale Zahlungen

Da wir bereits oben die Kryptowährungen wie Bitcoin, Ethereum und Co. erwähnt haben, starten wir mit den Möglichkeiten der Blockchain in der Finanzwelt. Blockchain ist eine stark verschlüsselte aber auf [illegible] Bank, wo jeder Eintrag verifiziert und verschlüsselt wird. Man kann sich vorstellen [illegible] und auch Transparenz zu Vorteilen führen kann. [illegible] Daten sicher sind und die gegenseitige [illegible] vermeiden.

Sinn der [illegible] zu [illegible] wie eine Bank, abzuwickeln und dadurch die Transaktionen zu [illegible] Schnelligkeit der Überweisungen zu erhöhen. Auch Banken [illegible] Prozesse [illegible] um ihre manuellen internationalen Transaktionen durch ein einfaches [illegible] System [illegible].

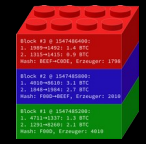
Peer-to-[illegible] (P2P) Transaktionen

Es gibt diverse Anbieter für direkte Transaktionen zwischen einzelnen Personen, [illegible] oder andere sind ist egal. Ziel ist es die Übermittlung von virtuellem Geld zwischen einzelnen [illegible] ermöglichen. Leider haben viele dieser Systeme [illegible] Schwachstellen bei [illegible] andere Limitationen. Um die Gefahr [illegible] zu [illegible], könnte Blockchain eingesetzt werden.

Kapitalmärkte

Die Möglichkeit auch die Kapitalmärkte mit Hilfe der Blockchain Technologie abzuwickeln, ist auch für Grossbanken wie die Credit Suisse und Santander Bank interessant. Da die Komplexität für die Abwicklung von Kapitalmarkttransaktionen

Verkettung: Einzelblattsammlung



Transaktionsliste #1
vom 2022-02-22:

1. Hans → Regula: 500 CHF
2. Karin → Peter: 800 CHF

Die Richtigkeit bestätigt
Backofficerin Bea

Transaktionsliste #2
vom 2022-02-23:

1. Peter → Katja: 300 CHF
2. Miriam → Nora: 120 CHF

Die Richtigkeit bestätigt
Backofficer Bruno

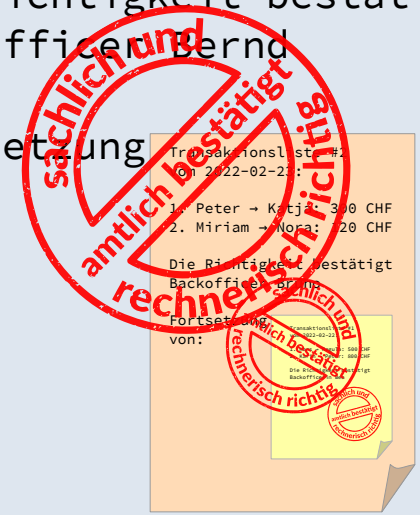
Fortsetzung
von:

Transaktionsliste #3
vom 2022-02-24:

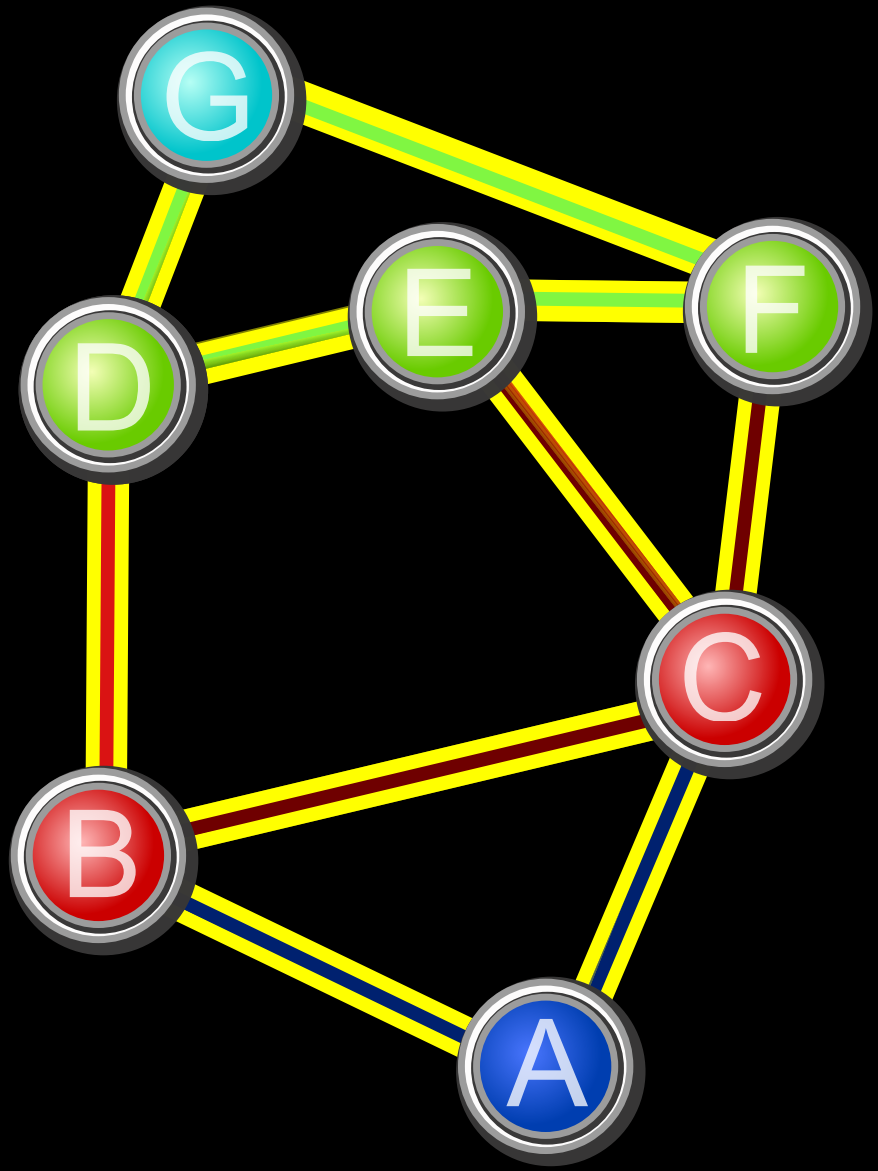
1. Heidi → Ernst: 620 CHF
2. Sepp → Hannah: 120 CHF

Die Richtigkeit bestätigt
Backofficer Bernd

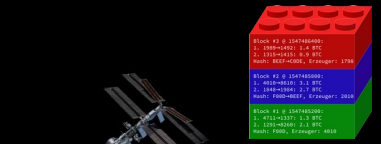
Fortsetzung
von:



Zusammenarbeit ohne Hierarchie und Vertrauen



Ehrlichkeit durch Investition



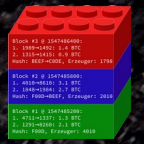
Proof of Work
120 Trilliarden Seiten
=120'000'000'000'000'000'000'000

Tätigkeitsbeschreibung

- Entgegennahme von Transaktionen (Einträgen)
- Weitergabe davon
- Transaktionen kontrollieren (Kontostand?)
- Liste führen
- "Genau genug" arbeiten
- Lange(!) Würfeln

- Arbeiten, wann, wo und so oft sie wollen (oder eben auch nicht)
- Lohn nur für Würfelglück

Prüfsummen und Hashes



gelb: Produkt, blau: Prüfziffern

EAN-13 (1 Ziffer)

```
7611613001105
7611613001112
7611613001129
7611613001136
7611613001143
```

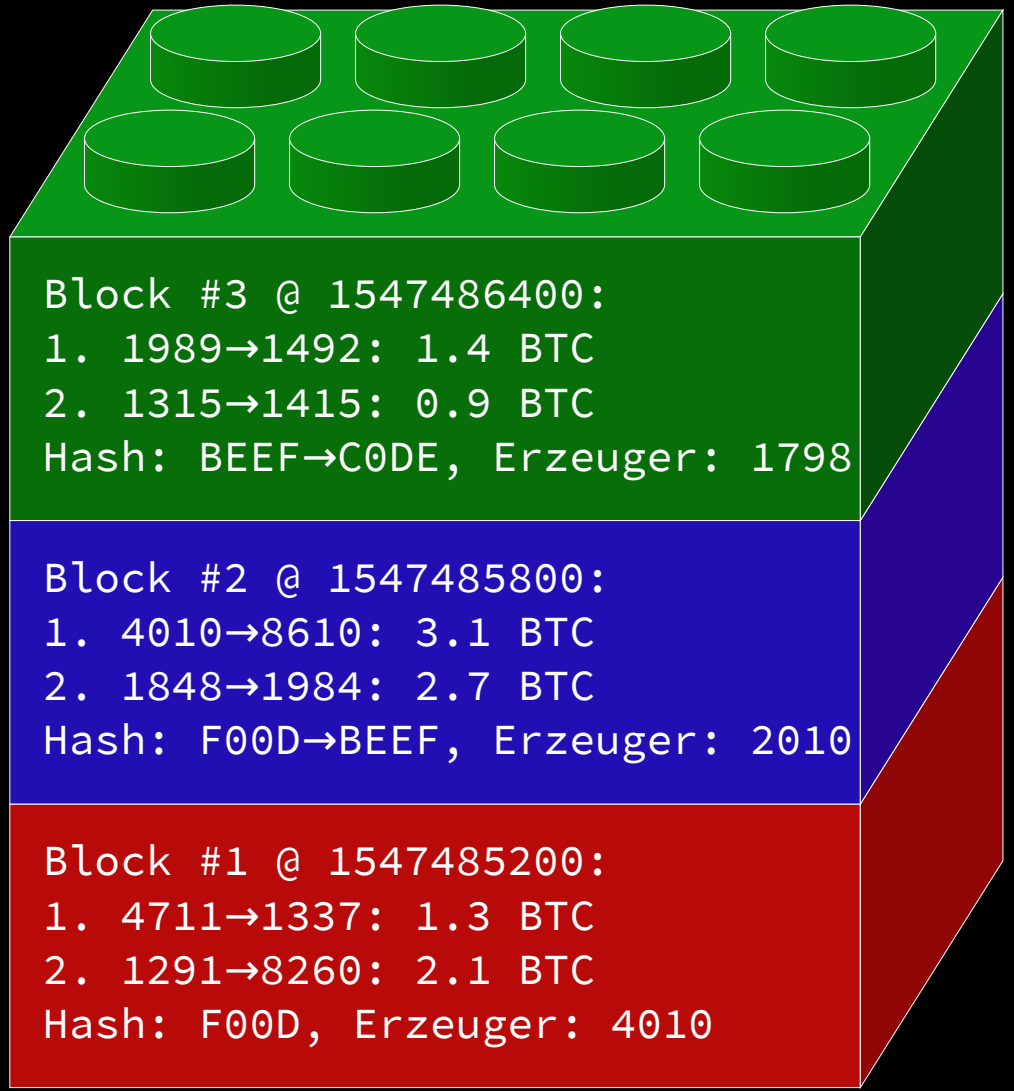
IBAN (2 Ziffern)

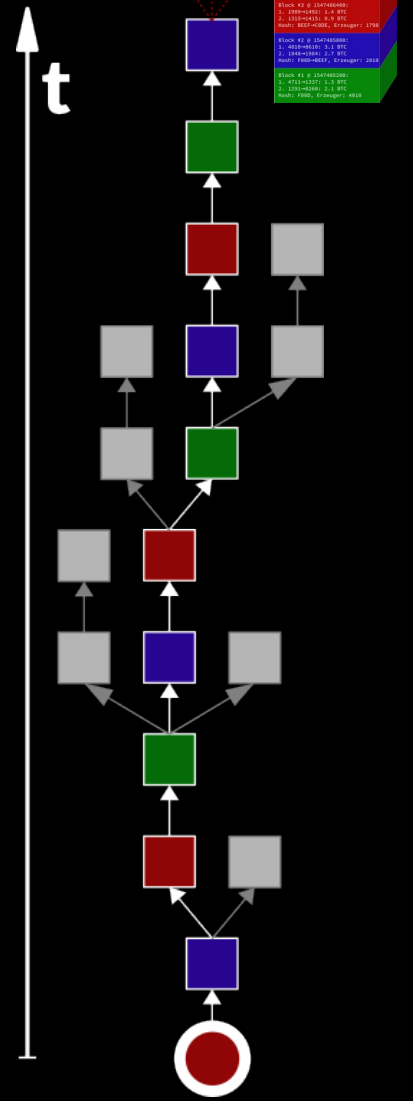
```
CH56 0123 4012 3456 7890 0
CH29 0123 4012 3456 7890 1
CH02 0123 4012 3456 7890 2
CH72 0123 4012 3456 7890 3
CH45 0123 4012 3456 7890 4
```

SHA-256 (256 Bits, 32 Bytes, 64 Hex-Ziffern)

```
Hallo 0 → a060ce3dd665ee29a9bddaaff21a45cfcdaf566da5ef81b
Hallo 1 → 2501750962e59064415a8658d31e090617553b7ccd1a53a
Hallo 2 → 312612b71656d102b831c5c1d2ea802180fd546eb24da70
Hallo 3 → bd631c05af2386c54855a5e1814861d33f333a4cef450e4
Hallo 4 → 8b586bcc4fa7ab2e477c1d57c2acda9c23438b0702cb3e4
```

Verkettung digital





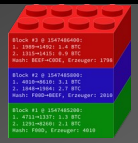
Ziel:

Zuverlässige und integre Geschäfts-prozesse

Daten-integrität

Verteilte Buchführung

Verkettung



Zuverlässigkeit

Verteilter Konsens

Dezentrale Speicherung

Nachvollziehbar wie Buchhaltung (meist *nicht* mani-pulationssicher!)

Schnelle Speicherung

Kryptographie

Konsens

Wenn verteilt, dann konsistent (wider-spruchsfrei, nicht unbedingt Konsens)

Analyse, Transparenz

Geschäfts-prozesse

Manipulations-sicherheit

Häufig Wünsche: Geschwindigkeit, Vertraulichkeit, Verarbeitbarkeit

MoreThanDigital
Cachin/IBM
Wikipedia

Nichtabstreit-barkeit

Transparenz, Vertraulichkeit

Ziel:

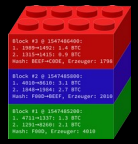
Zuverlässige und integre Geschäfts-prozesse

Nachvollziehbar wie Buchhaltung (meist *nicht* mani-pulationssicher!)

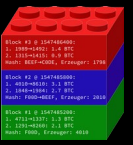
Wenn verteilt, dann konsistent (wider-spruchsfrei, nicht unbedingt Konsens)

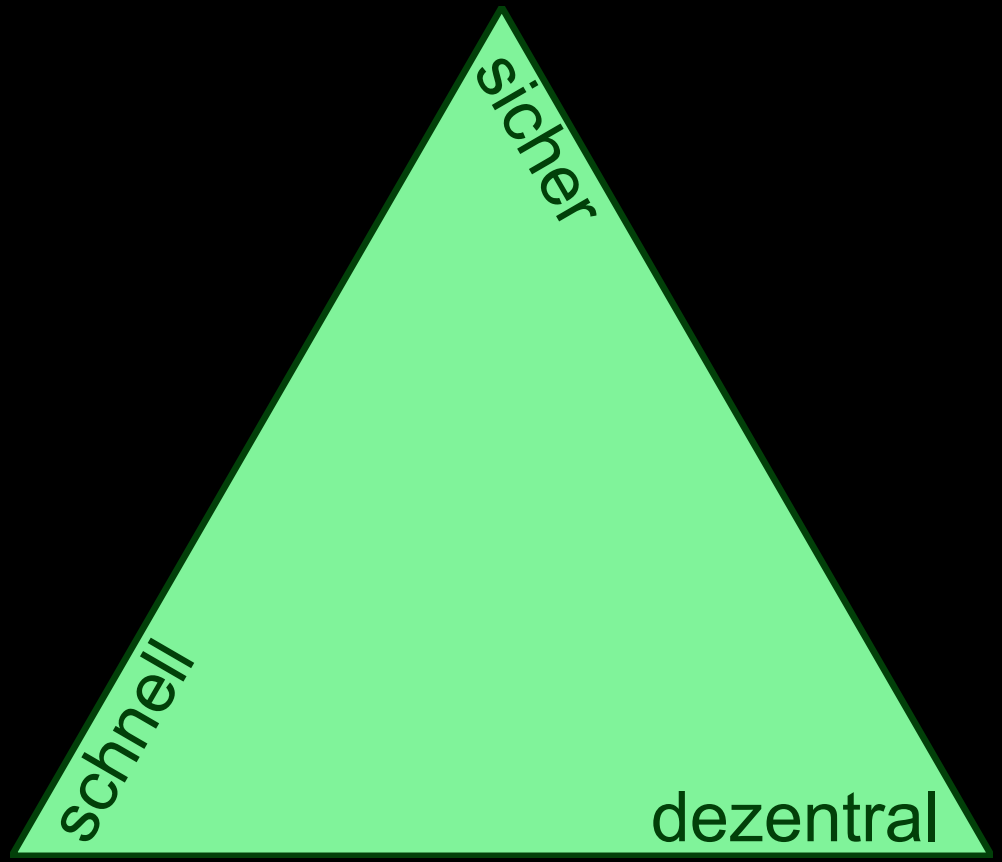
Häufig Wünsche: Geschwindigkeit, Vertraulichkeit, Verarbeitbarkeit

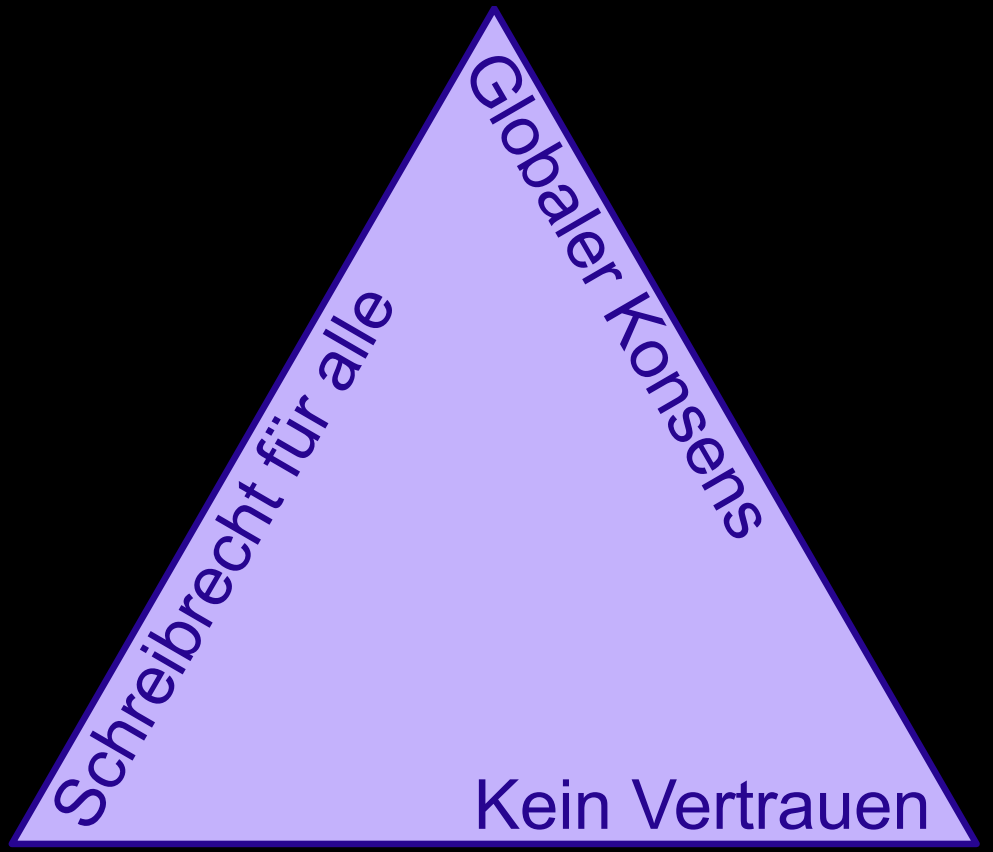
Komplexität



Unnötige Komplexität
(3 sind 1 zu viel)







Blockchain

- Komplexe Lösung für ein sehr spezifisches Problem
- Fehlendes Vertrauen kommt teuer zu stehen
- Meist nicht alles benötigt; Kombination aber deutlich teurer
- Nicht kompatibel mit Datenschutzgesetzen
- Keine Fehlerkultur
- Unmenschlich

- Hinreichend fortschrittliche Technologie ist nicht von Magie zu unterscheiden
- Wenn Sie einen Scheissprozess mit einer Blockchain versehen, haben Sie einen Scheiss-Blockchain-Prozess
- Eine gute Idee alleine ist nicht automatisch Teil einer guten Lösung
- Vertrauen bzw. Struktur erhöhen Effizienz und reduzieren Komplexität
- Gewisse Komponenten/Ideen ja, aber nicht das Gesamtpaket

Blockchain

Keine einzelne Technologie alleine
kann alle unsere Probleme lösen.

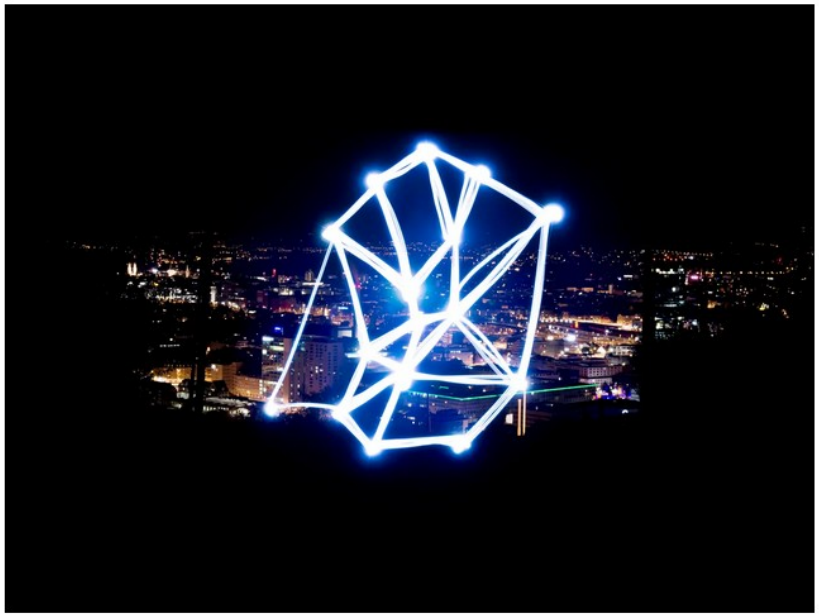
Schon gar nicht eine, welche
Unveränderbarkeit zum Ziel hat.

Neue Zürcher Zeitung

Alle Macht dem Kryptobürger!

Von Blockchains hört man einstweilen vor allem im Zusammenhang mit Finanztransaktionen und der Kryptowährung Bitcoin. Aber sie könnten ein neues Zeitalter einläuten – nicht nur in der Wirtschaft.

Melanie Swan
18.07.2017, 05.30 Uhr

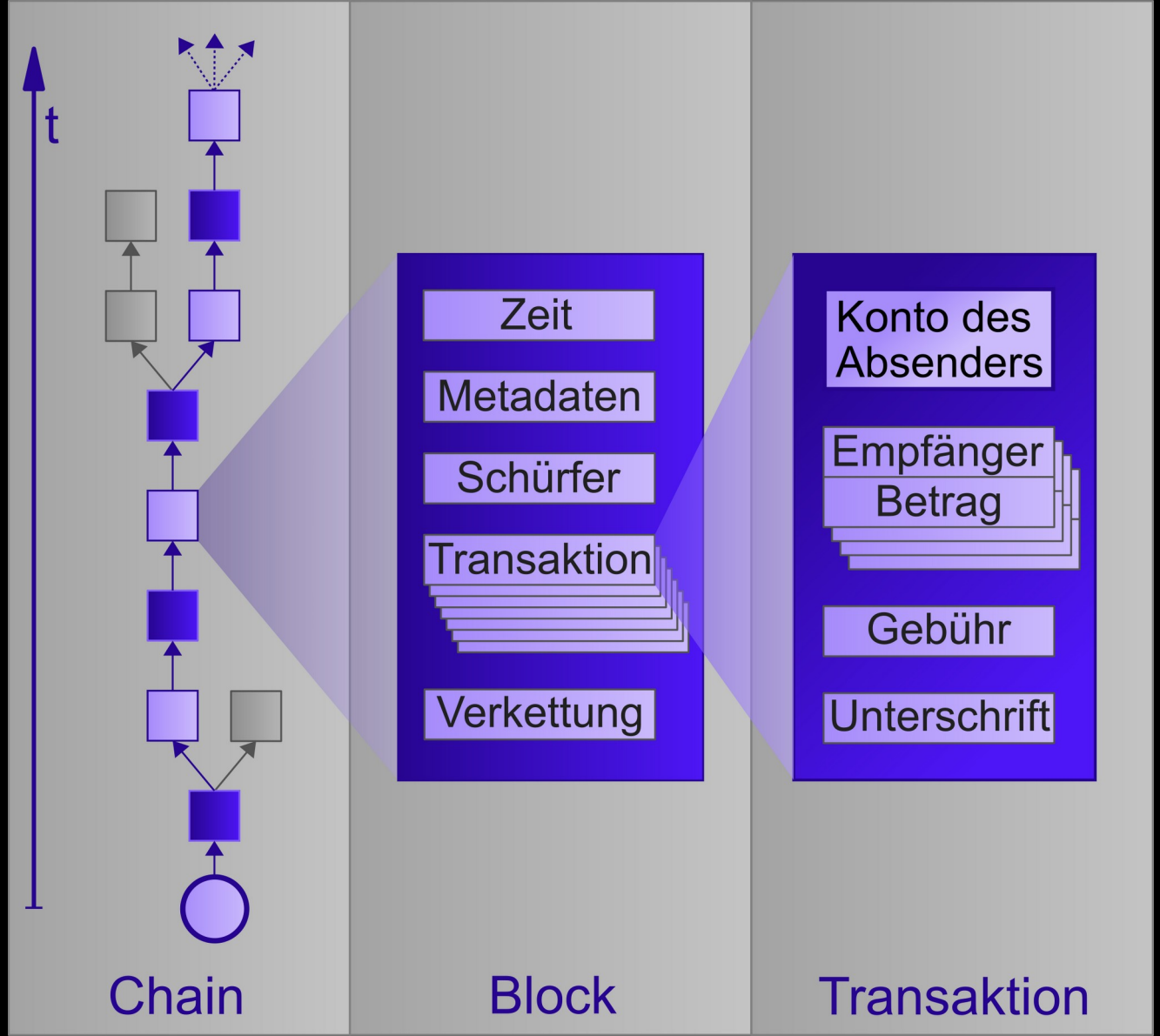


Eine Blockchain-Datenbank verteilt sich auf ein Netzwerk von Computern mit zahlreichen Knotenpunkten, wie es diese improvisierte Installation vor der Kulisse Zürichs illustriert. (Bild: Goran Basic / NZZ)

Kryptowährungen: Die Versprechen

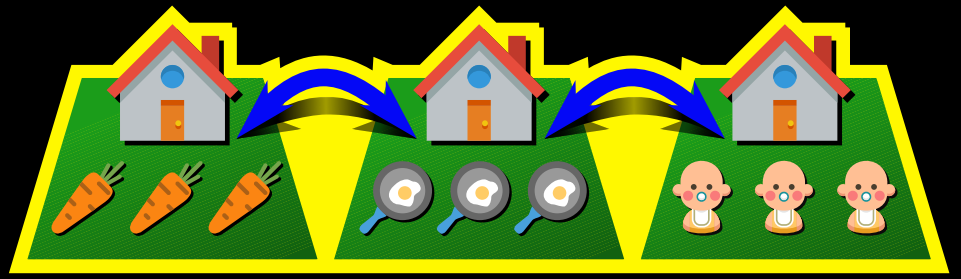
- Internationale Finanztransaktionen
- Vermeidung von Geldwäsche
- Handelsfinanzierung
- Audit/Regulatory Compliance

- Dezentral
- Garantiert selten
- Profit/Rendite
- Gesetzliches Zahlungsmittel
- Schutz vor Manipulationen durch Regierungen/Zentralbanken
- "Banking the Unbanked"

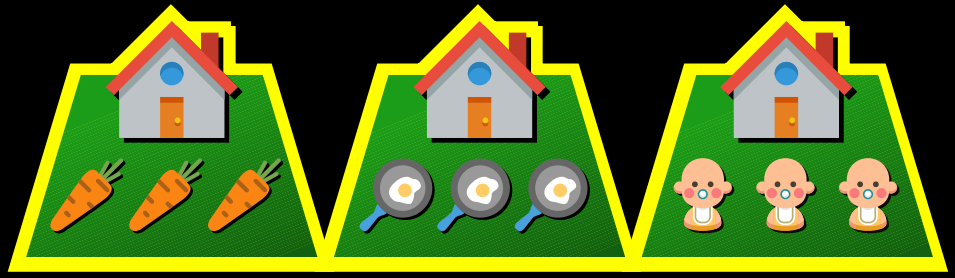

t
Zeit
Metadaten
Schürfer
Transaktion
Verkettung
Konto des Absenders
Empfänger
Betrag
Gebühr
Unterschrift
Chain
Block
Transaktion

Funktion des Geldes: Wirtschaft

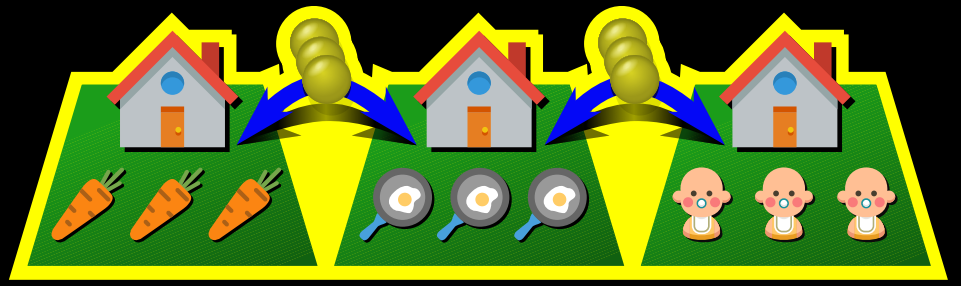
Selbstversorgung



Tauschhandel



Arbeitsteilung



Handel

Geld

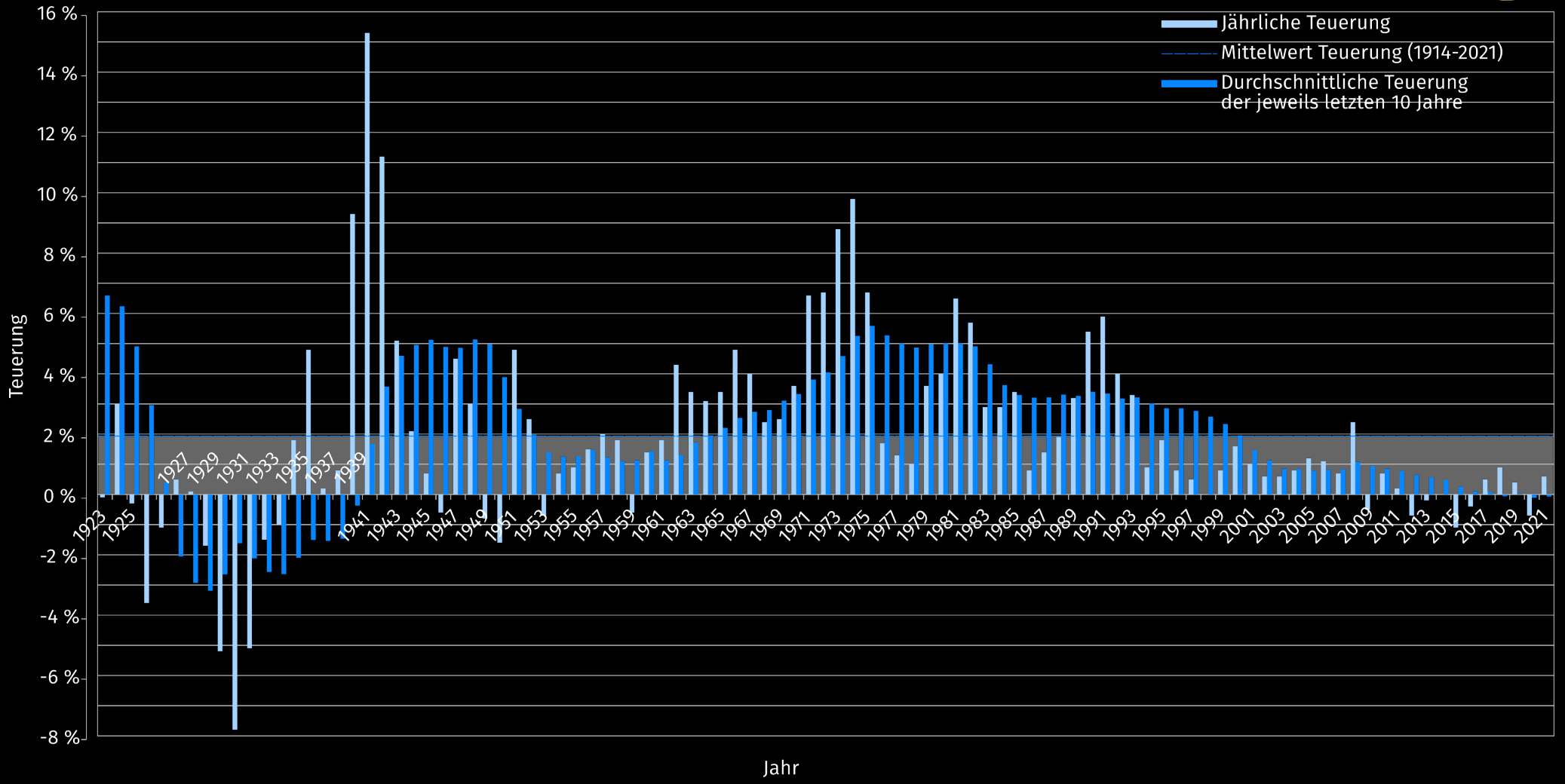
- Tauschmittel
  - Auch Kreditgewährung
- Wertmessung
  - Wirtschaftsrechnung
  - Geschäftsbilanz
  - Vergleichbarkeit
  - Planbarkeit
- Wertaufbewahrung
  - Kurz- bis langfristig

- Leichte Handhabbarkeit
- Gute Transportierbarkeit
- Akzeptanz
  (erst Netzwerkeffekt ergibt einen Nutzen)
- Preisstabilität
- Fungibilität (Austauschbarkeit)
- Geschlossener Kreislauf!

- Volkswirtschaftliche Funktionen

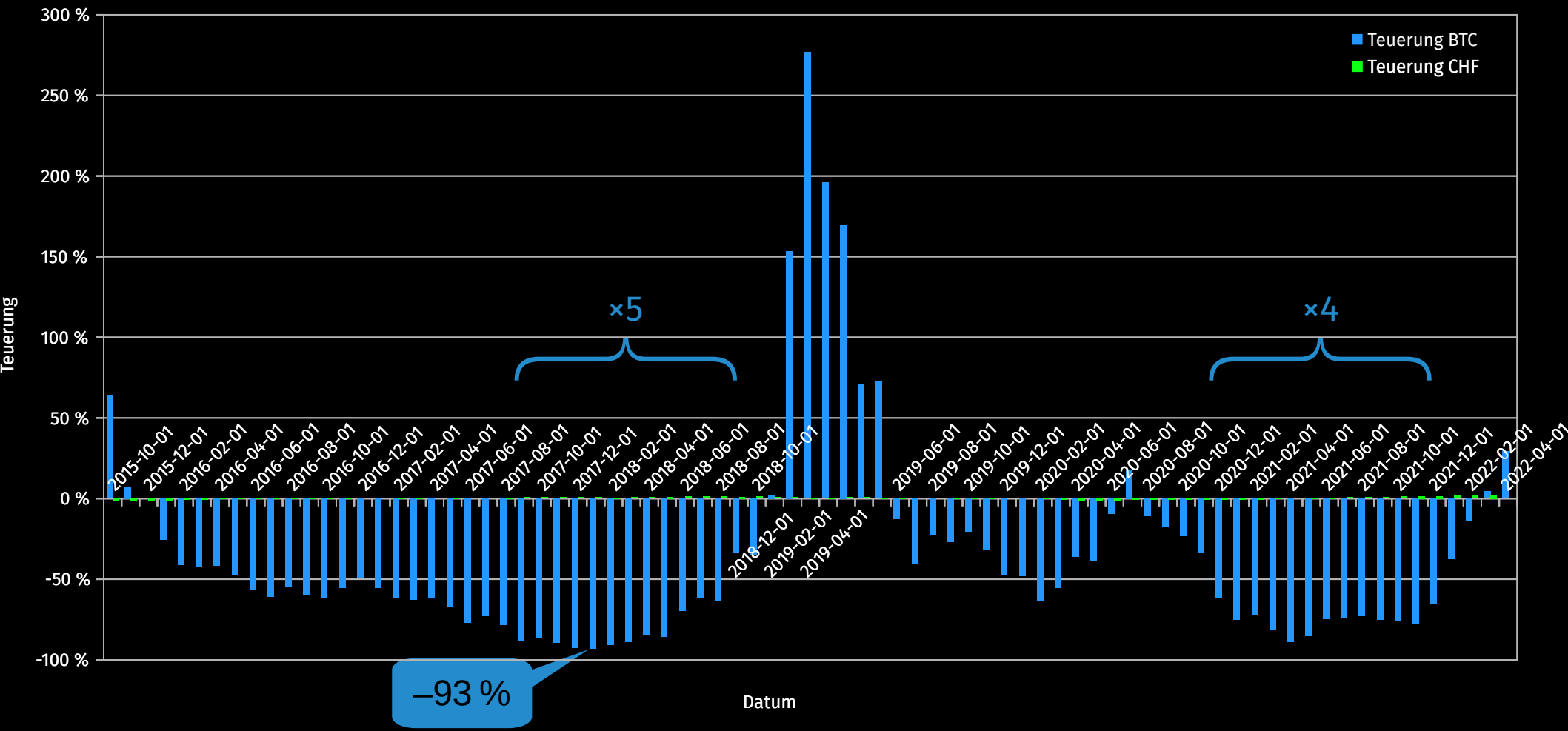
Teuerung in der Schweiz

Datenbasis: Landesindex der Konsumentenpreise 1914-2021 (Bundesamt für Statistik)

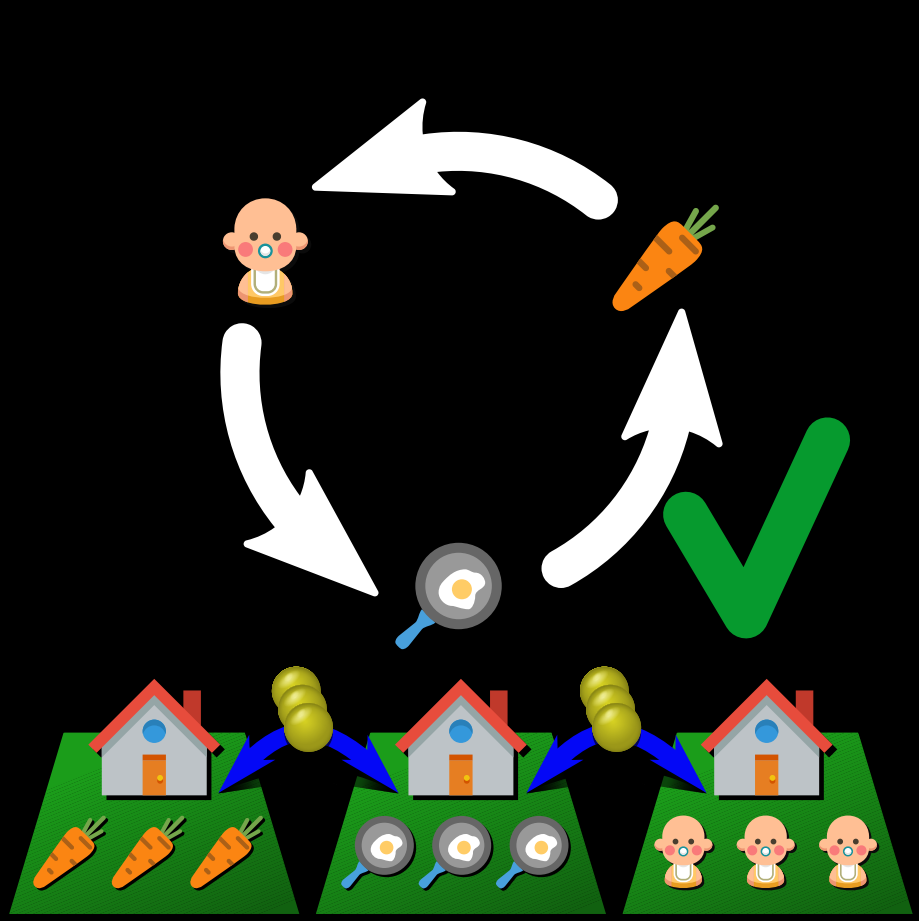


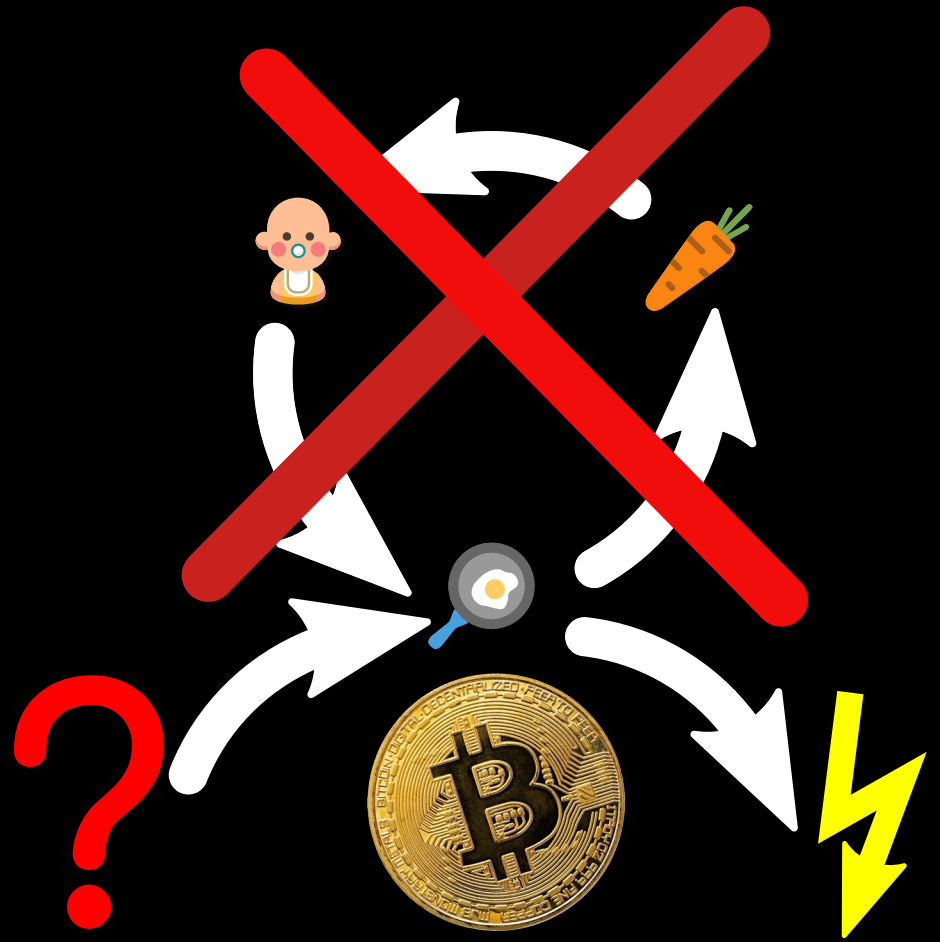
Vergleich Teuerung Bitcoinland und Schweiz

Bitcoin auf Basis USD-Wechselkurs (Yahoo Finance); CH: LIK (BFS)



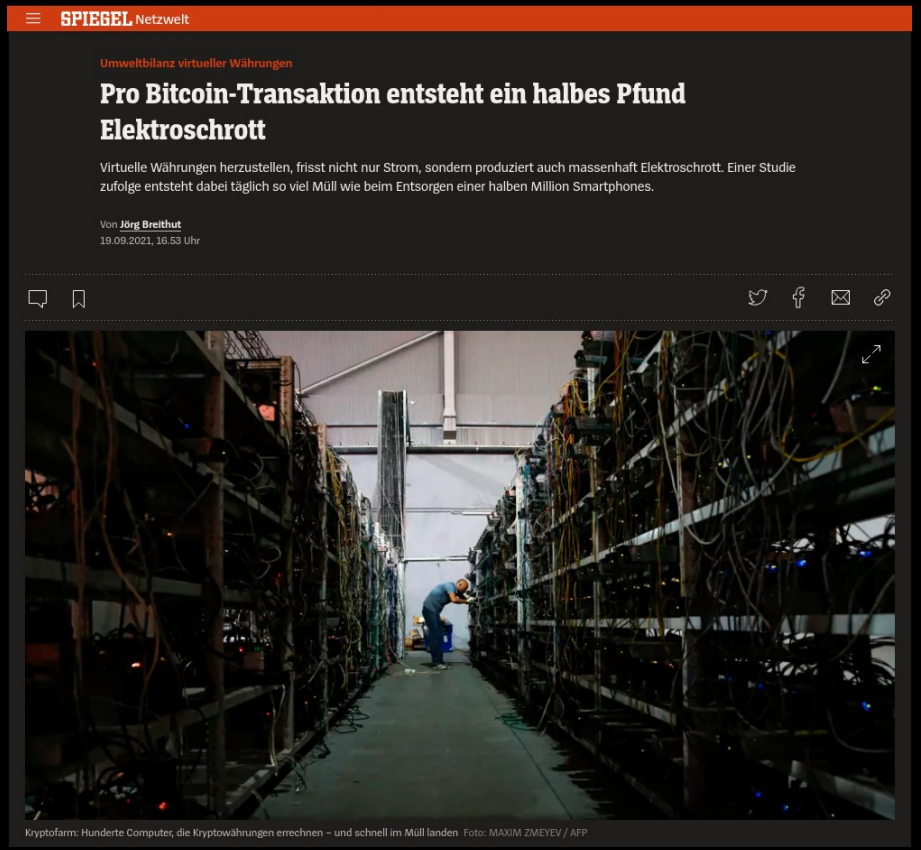
Geldkreislauf





Kryptowährungen

- Widersprüche
  - Währung und Investitionsvehikel
  - Anonymität und Geldwäschevermeidung
  - Akzeptanz/Anonymität
  - Dezentralität/Gateways
- Nachhaltigkeit
  - Währungsabfluss von 20-30 Millionen CHF/Tag durch Strom
  - 20'000 Tonnen Elektroschrott pro Jahr
  - (Proof of Stake noch komplizierter und risikoreicher)



SPIEGEL Netzwelt

Umweltbilanz virtueller Währungen

Pro Bitcoin-Transaktion entsteht ein halbes Pfund Elektroschrott

Virtuelle Währungen herzustellen, frisst nicht nur Strom, sondern produziert auch massenhaft Elektroschrott. Einer Studie zufolge entsteht dabei täglich so viel Müll wie beim Entsorgen einer halben Million Smartphones.

Von Jörg Breithut
19.09.2021, 16.53 Uhr

Kryptofarm: Hunderte Computer, die Kryptowährungen errechnen – und schnell im Müll landen Foto: MAXIM ZMEYEV / AFP

Kryptowährungen

Kein einzelnes Finanzprodukt alleine kann alle Bedürfnisse einer diversen globalisierten Wirtschaft und Gesellschaft abdecken.

Schon gar nicht eine, welche dies völlig autonom und automatisch erledigen soll.

Smart Contract

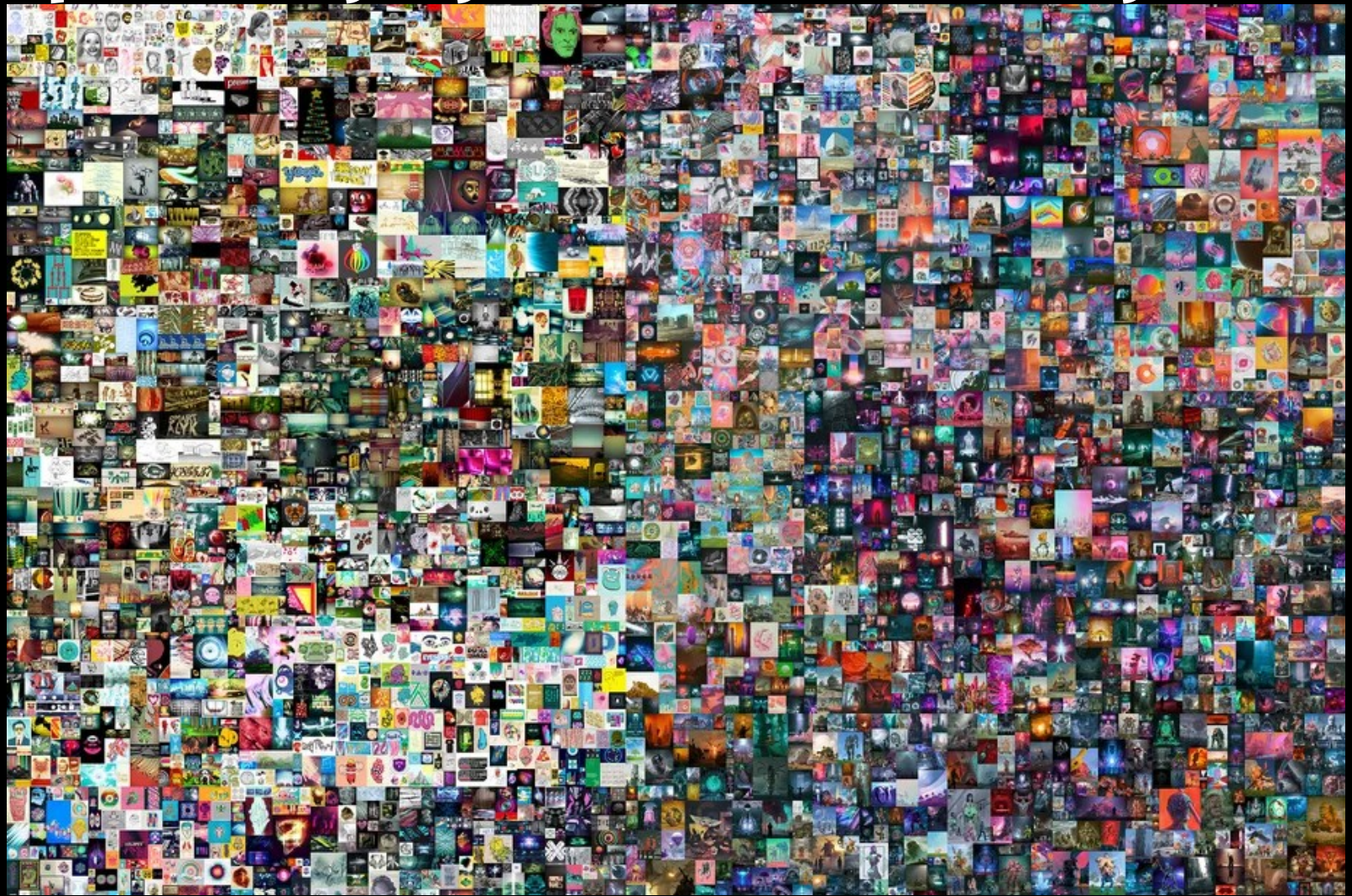
- Nur innerhalb der Blockchain (Orakel-Problem)
- "Code is Law" (Programm ist Gesetz [...])
- "Jedes Programm hat mindestens einen Fehler"
- Unveränderbar (oder ...)
- Keine Fehlertoleranz
- Keine Rückfallstrategie
- Keine "Gnade vor Recht"
- ... ausser ...
- Beschäftigungsprogramm

Smart Contracts

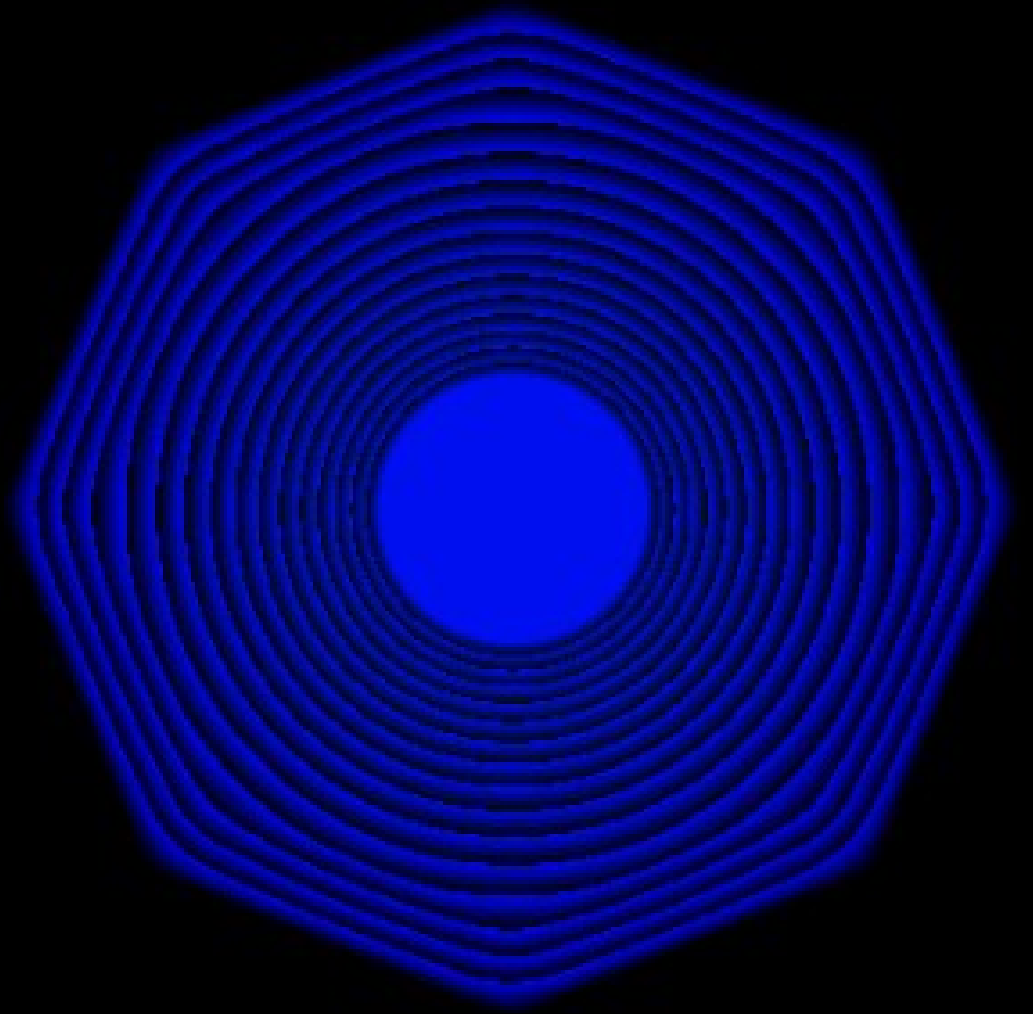
Kein Vertrag deckt alle Sonderfälle ab bzw. kann zukünftige Entwicklungen voraussehen.

Ganz besonders nicht, wenn es weder Fallbacks (Gesetze, Moral) noch Anpassungsmöglichkeiten gibt.

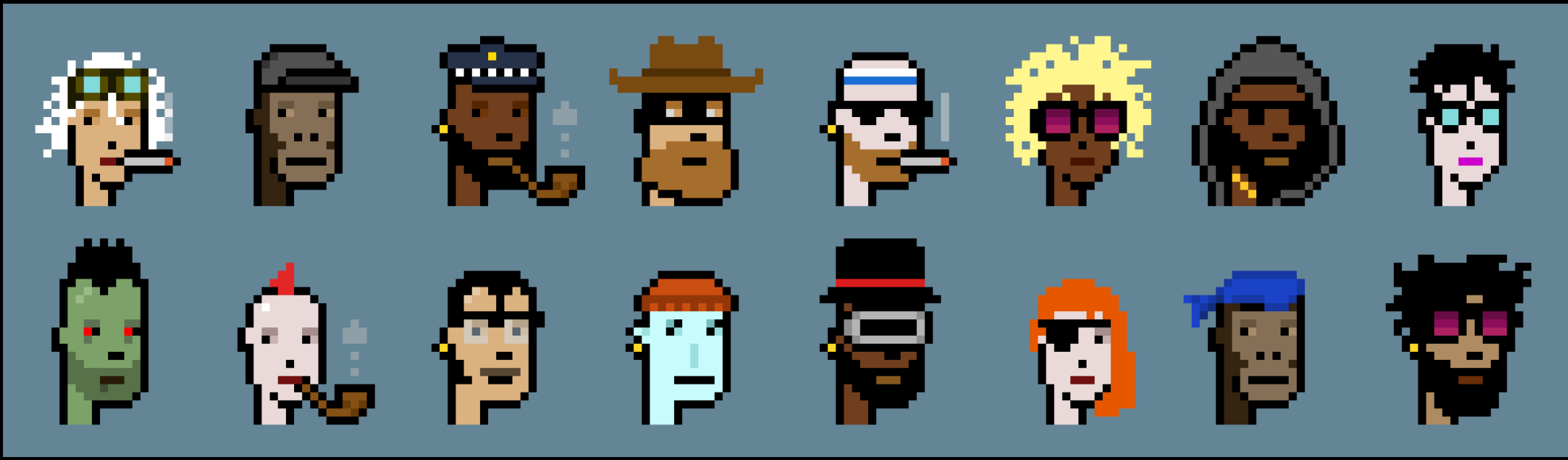
Beeple: "Everydays – The First 5000 Days" (2021)



Kevin McCoy: "Quantum" (2014)



Larva Labs: "Crypto Punks" (10'000x, 2018)



Bored Apes Yacht Club (10'000x, 2021)








NFT: Non-Fungible Token (Nicht austauschbare Marke)

Versprechen

- Markt für digitale Kunst
- Wertsteigerungen zugunsten der Künstler
- Beweis des Besitzes
- Löse Problem der Einmaligkeit
- Authentizität
- Dezentralisiert

Umsetzung

- Smart Contract
- URL (ohne Bindung)
- Primär zentrale Marktplätze

NFT

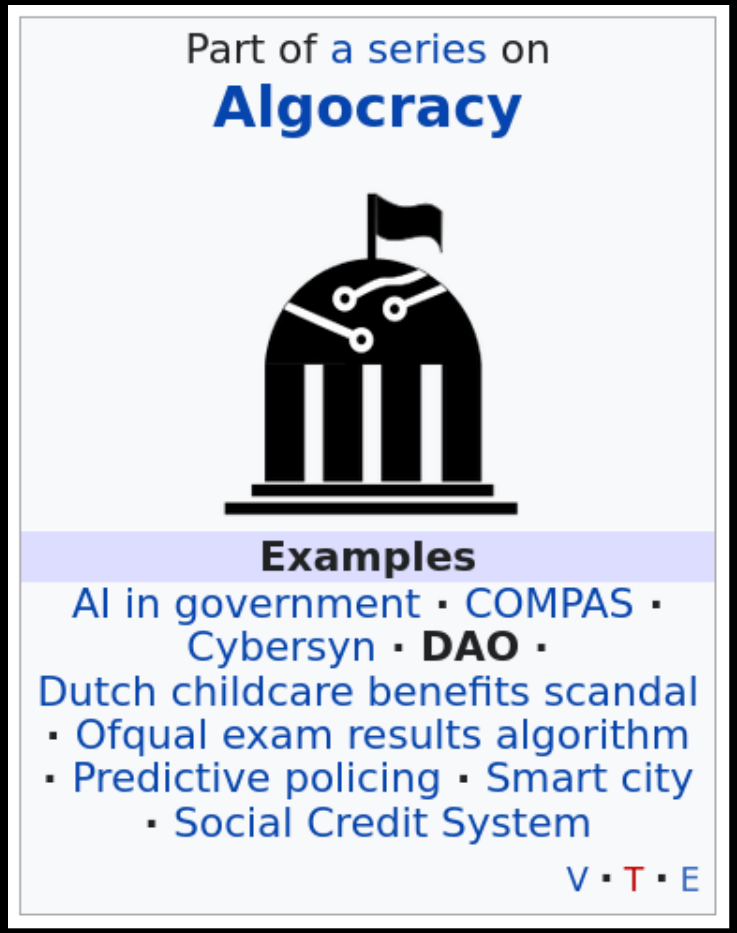
Digital sind Original und Kopie ununterscheidbar.

Jeglicher Versuch, das zu ändern ist zum Scheitern verurteilt.

DAO: Dezentrale Autonome Organisationen

- Verein, Firma, ... alleine auf Basis von Smart Contracts
- Regeln werden automatisch durch- und umgesetzt

- Sportwetten
- Wechselstuben
- gemeinsamer Kauf (ConstitutionDAO)
- Spiele ("play to earn")



DAO

Starre Regeln und teure Umsetzung sind untauglich um neue Formen wirklich auszunützen.

"Play to earn"-Spiele (u.a.) ermöglichen neue Formen der Leibeigenschaft.

Anfangsfolgerungen

Digitalisierung

- ohne zu überlegen, was es eigentlich braucht,
- ohne Umfeld/Auswirkungen zu betrachten,
- ohne zukünftige Veränderungen/Eingriffe zu berücksichtigen,
- im Glauben, dass alles messbar bzw. mit Geld möglich sei und
- Mitleid, Interpretationsspielraum, Vertrauen aus unserem Leben zu verbannen.

Schlussfolgerung

Blockchain und Kryptowährungen entstanden als Gegenströmung zu der Immobilien-/Finanzkrise von 2008, die durch ein Wirtschaftssystem geprägt durch Gier, Ineffizienz, Intransparenz und übermässige Komplexität ausgelöst worden sei.

Ersetzt werden soll es durch ein neues, nun digitales, Wirtschaftssystem, das geprägt wird von noch mehr Gier, Ineffizienz, Intransparenz und übermässiger Komplexität.

Mögliche Fragen

- Aber in El Salvador (+neu CAF) ist Bitcoin offizielle Währung?
- Und die Pläne von Klaus Schwab (WEF)?
- Fachhochschulen und Universitäten sind aber auch dabei!
- Wird mit Proof of Stake nicht alles besser?
- Wofür kann man denn Blockchain nutzen?
- Hast du in Kryptowährungen investiert? Empfiehlst du das?
- Wie funktionieren Stablecoins? Wieso will man sowas (nicht)?
- Sollen NGOs in Kryptowährungen/NFTs investieren?
- Wie müsste man denn eine Kryptowährung aufbauen?
- Der Kunstmarkt (u.a.) schafft ja aber Wert aus dem Nichts. Wie/wieso?

Weiterführendes Material:

https://marcel-waldvogel.ch/anhalter

Digitalisierung

Wenn Sie einen Scheissprozess digitalisieren, dann haben Sie einen scheiss digitalen Prozess.

— Thorsten Dirks

Erfolgreiche Digitalisierung zeichnet sich aus durch

1. radikale Vereinfachung des Hauptprozesses und
2. Verzicht auf seltene Sonderfälle zugunsten von Flexiblität.

— Marcel Waldvogel

Struktur

Wenn Ihre Prozesse so weit strukturiert sind, dass Sie eine Blockchain dafür einsetzen könnten, dann brauchen Sie keine Blockchain mehr.

— Unbekannt

Neues Wirtschaftssystem

Blockchain und Kryptowährungen entstanden als Gegenströmung zu der Immobilienkrise von 2008, die durch ein Wirtschaftssystem geprägt durch Gier, Ineffizienz, Intransparenz und übermässige Komplexität ausgelöst worden sei.

Ersetzt werden soll es durch ein neues, nun digitales, Wirtschaftssystem, das geprägt wird von noch mehr Gier, Ineffizienz, Intransparenz und übermässiger Komplexität.

— Marcel Waldvogel

Komplexe Lösung

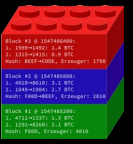
For every complex problem there is an answer that is clear, simple, and wrong.

— Henry L. Mencken

Jedes komplexe Problem hat eine Lösung, welche klar, einfach und falsch ist.

Unsere Welt braucht nicht mehr Komplexität sondern weniger.

— Marcel Waldvogel



Magie

Any sufficiently advanced technology is indistinguishable from magic.

— Arthur C. Clarke

Hinreichend fortschrittliche Technologie ist nicht von Magie zu unterscheiden.

Aber taugt die Technologie zu mehr als Taschenspielertricks?

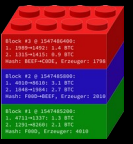
— Marcel Waldvogel

Gute Idee, aber…

Eine gute Idee ist nicht automatisch Teil einer guten Lösung.

(Auch ein Hammer sollte mal andere Freunde kennen als Nägel.)

— Marcel Waldvogel



Orakel-Problem

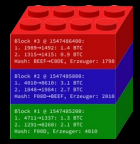
The blockchain can't lie to you, but you can lie to the blockchain.

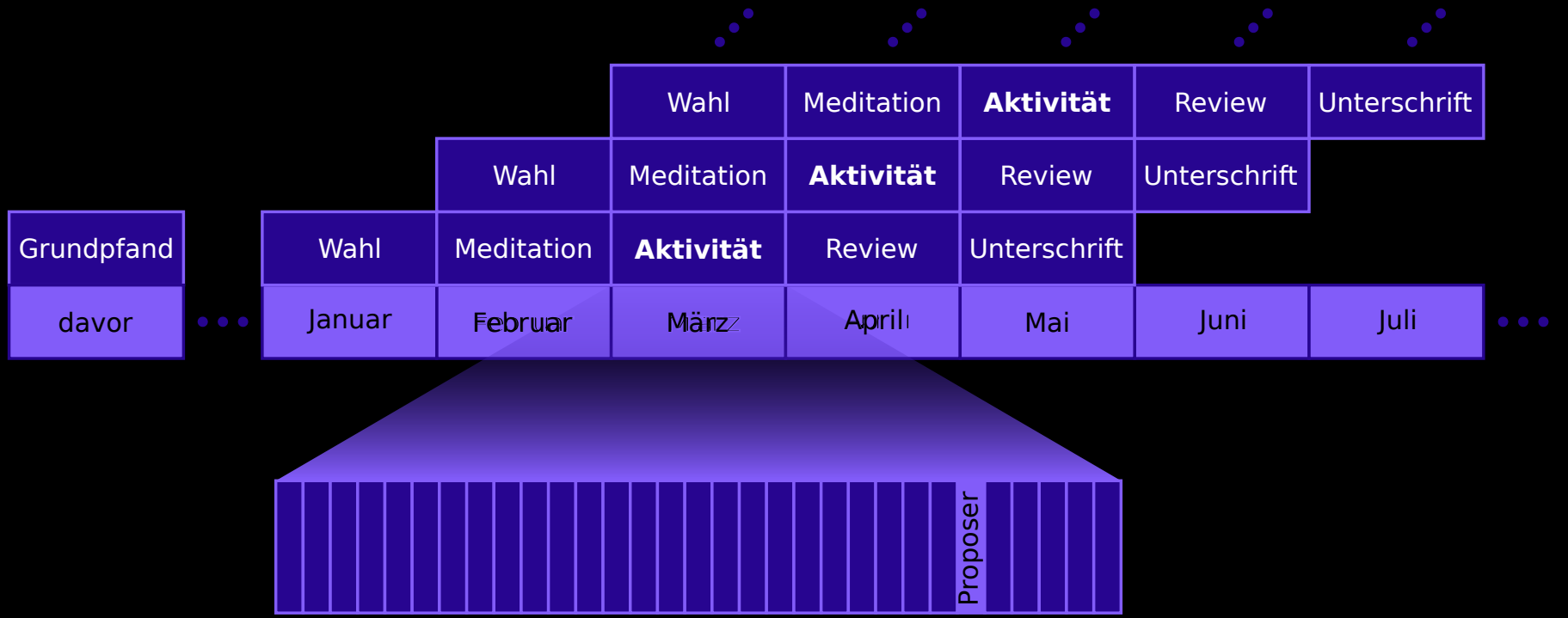
— Author unknown

Die Blockchain kann dich vielleicht nicht anlügen [naja…], aber du kannst sie jederzeit belügen.

(Die eine Hälfte des Blockchain-Oracle-Problems.)

Proof of Stake (Ethereum, geplant)





Daten

- Wie sehen Umfang, Format, Struktur der Daten aus?
- Abhängigkeiten der Felder innerhalb und zwischen Datensätzen?
- Für welche Aspekte sind Integrität, Nachvollziehbarkeit, Unveränderbarkeit, Vertraulichkeit und globaler Konsens notwendig?
- Bei welchen Daten soll der aktuelle Stand öffentlich sein?
- Bei welchen soll auch die Entstehungsgeschichte öffentlich sein (Nachvollziehbarkeit)?
- Gibt es weitere Datensätze/-felder/-relationen, welche differenzierte Behandlung bedingen?

Eingabe

- Welches sind die Datenquellen?
- Woher kommen die Daten?
- Wie kommen sie ins System?
- Was ist mit Bestandsdaten?
- Wie wird Qualitätssicherung betrieben? (Korrektheit, Einheitlichkeit/Konsistenz, Authentizität,Vollständigkeit, ...)

Verarbeitung

- Welche Verarbeitungsschritte sollen auf den Daten ausgeführt werden?
- Wer kontrolliert deren Korrektheit? Kann sie automatisch überprüft werden? Immer?

Ausgabe

- Was soll mit den Daten geschehen?
- Welche Aktionen sollen aufgrund dieser Resultate ausgeführt werden? Automatisch?
- Wie sollen die Ausführung dieser Aktionen überprüft bzw. durchgesetzt werden?

Zusammenarbeit

- Welche Personengruppen dürfen welche Daten einsehen, ändern, administrieren oder Programmcode ändern?
- Welche Risiken ergeben sich aus berechtigten Personen, welche ihre Rechte missbrauchen (bzw. deren Rechte missbraucht werden)?
- Ist dauerhaftes Misstrauen zwischen Akteuren zu erwarten? Lässt sich dieses Misstrauen durch Hierarchien, Zuständigkeiten oder (Arbeits-)Verträge managen?

Zukunftssicherheit

- Werden sich Format, Struktur oder Abhängigkeit der Daten irgendwann verändern?
- Falls sich Teile der Daten ändern: Sollen sich historische Daten weiterhin auf die damals gültigen Werte beziehen (z.B Name/Adresse vor Namens-/Adressänderung)?
- Wie sollen diese Änderungen umgesetzt werden (Bestandsdaten, Neudaten)?
- Haben die Daten ein Ablauf-/Löschdatum? Statisch oder dynamisch? Was sieht ihr Lebensende aus?
- Wie soll mit (abschichtlich oder unabsichtlich) falschen Eintragungen umgegangen werden? Welchen Einfluss hat das auf die Nachvollziehbarkeit?
- Wie wird der Anspruch auf Korrektur bzw. Löschung von persönlichen Daten umgesetzt?
- Wie werden allfällige gerichtliche Anordnungen zu Korrektur/Löschung umgesetzt?

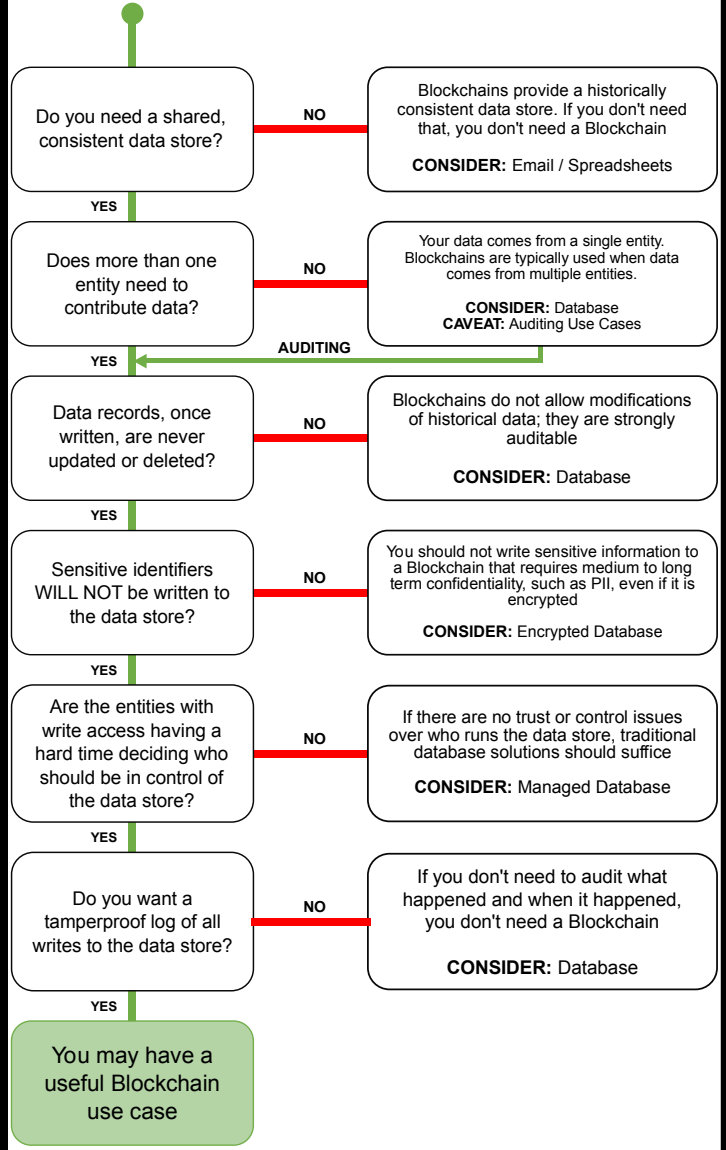


Figure 6 - DHS Science & Technology Directorate Flowchart

FinTech

Crypto isn’t tech. It’s unregulated finance built on shitty tech.
The key part is unregulated finance not the tech.

— Dare Obasanjo

Krypto[währungen] sind nicht Technik ["FinTech"].
Es sind unregulierte Finanz[produkte], gebaut auf verschissener Technik. Die Schlüsselkomponente sind die unregulierten Finanzprodukte, nicht die Technik.

Tech-Industrie

This has been a major part of the model of the tech industry for more than a decade though: start a company in a traditional industry, brand it as “tech”, and use that to evade regulations so you can better exploit people.

— Paris Marx

Dies ist seit über einem Jahrzehnt ein beliebtes Modell der Tech-Industrie: Starte eine Firma in einer traditionellen Branche, bezeichne sie als "Tech" und umgehe damit Vorschriften, damit du Leute besser ausnutzen kannst.

Komplexität

Remember, some things are hard to understand because they're complicated, and some things are complicated so they will be hard to understand.

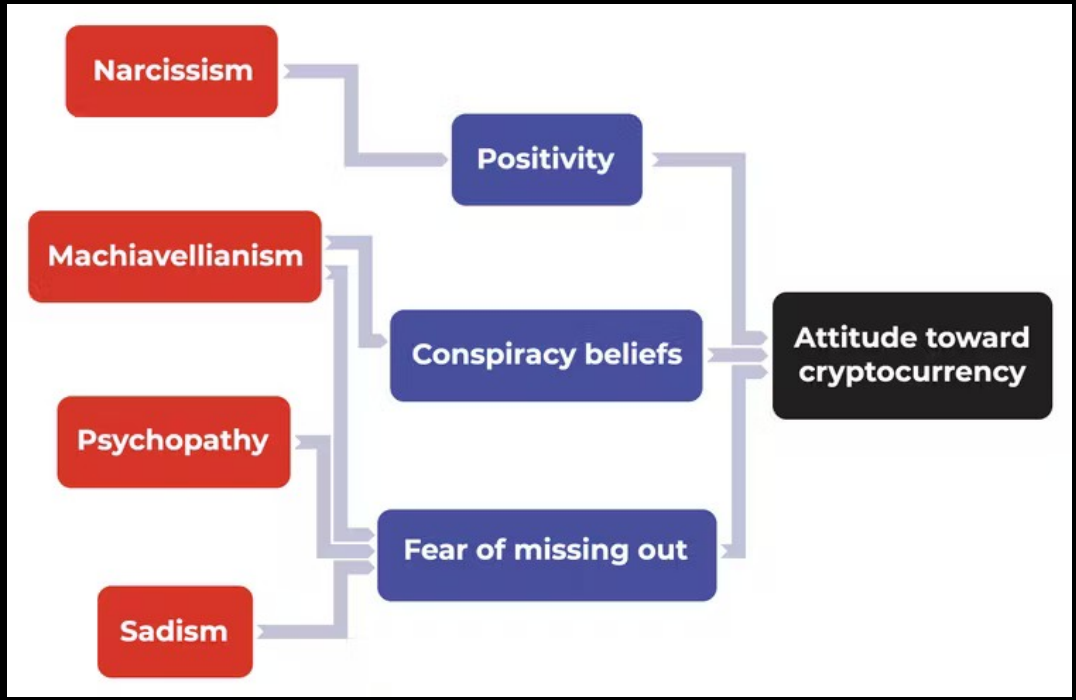
— Cory Doctorow

Merkt euch:
Einige Dinge sind schwer verständlich, weil sie kompliziert sind.
Andere Dinge sind kompliziert, damit sie schwer verständlich sind.

Perpetuum Mobile

Wert kann nicht aus dem Nichts geschaffen werden.
Ein Perpetuum Mobile gibt es auch in der Finanzwelt nicht.

— Marcel Waldvogel



Die "Dunkle Tetrade" fühlt sich besonders zu Investitionen in Kryptofinanzprodukte hingezogen.

Jo Adetunji:
'Impulsive psychopaths like crypto': research shows how 'dark' personality traits affect Bitcoin enthusiasm.
The Conversation, 2022-04-11.

Wahnsinn mit Methode

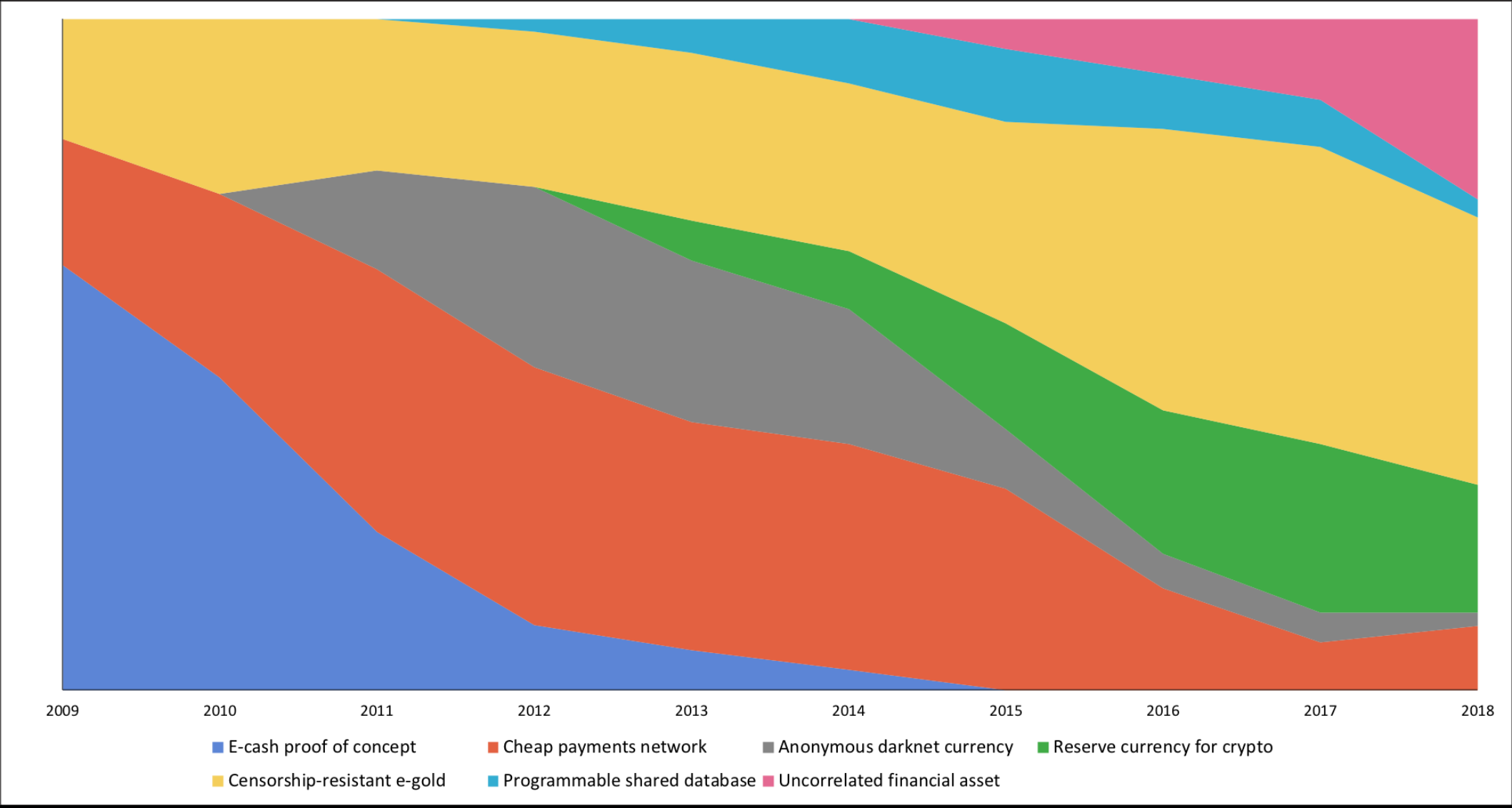
The definition of insanity is doing the same thing over and over and expecting different results.

Grifters gotta grift.

— Grady Booch about resurrecting Luna/Terra

Wahnsinn ist, wenn man immer wieder dasselbe tut, aber andere Resultate erwartet.

Gauner bleiben Gauner.



Quelle: https://uncommoncore.co/visions-of-bitcoin-how-major-bitcoin-narratives-changed-over-time/