LACERTAS

Grundlagen Bitcoin

21. November 2023

DIGITAL TRANSFORMATION WITH PASSION

Intro & Ziele

Das erreichen wir heute gemeinsam

Intro

Kryptowährungen wie Bitcoin Hype oder gekommen, um zu bleiben?

Was man heute mit Sicherheit sagen kann, ist, dass Kryptowährungen gekommen sind, um zu bleiben!

Im Jahr 2009 wurde mit dem Bitcoin die erste Kryptowährung lanciert, heute gibt es bereits mehrere Tausend Cyberwährungen. Es werden ganz bestimmt nicht alle bleiben und viele neue dazu kommen.

Heute Abend bringen wir Euch den Bitcoin näher und zeigen Euch auf, weshalb der Bitcoin nach so vielen Jahren und diversen weiteren Kryptowährungen immer noch einzigartig ist.

Ziele

Am Ende des Treffens habt Ihr

- ein Verständnis bezüglich der Unterschiede von «Geld» und Bitcoin
- ein Verständnis über die Grundlagen von Bitcoin
- ein Bitcoin Wallet erstellt und sichert
- den Ablauf einer Bitcoin Transaktion verfolgt

Theorie

Was ist «Geld»?

Bild: Claudio Schwarz auf Unsplash

Was ist Geld?

Was ist Geld?

Wenn man **mit Münzen** und **Noten aufgewachsen** ist, dann kann man sich nur **schwer andere Formen** von Geld **vorstellen**.

Dass zum Beispiel Systeme mittels **Kryptografie**, wie bspw. bei **Bitcoin**, in der Tat **wie „echtes" Geld funktionieren** sollen, ist **für viele kaum nachvollziehbar**.

Das „echtes" **Geld** in **unterschiedlichen Formen** existieren kann, **zeigt** uns die **Geschichte**.

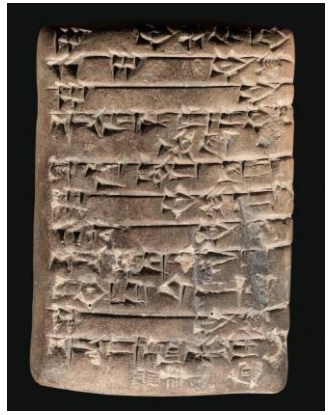
Was ist Geld?

Was ist Geld?

In **Afrika** war bspw. **Salz** als eine **Form des Geldes** anerkannt, weil es eine gewisse Härte und Haltbarkeit garantiert. Doch **in feuchteren Weltregionen** war Salz **ungeeignet.** Also wurden normalerweise robuste Dinge zum Zahlungsmittel der Wahl: Muscheln oder Kokosnüsse, Pfeilspitzen oder Äxte, Vogelfedern oder Reis.

Die **Geschichte zeigt**, es ist eine **Einigung auf** ein einheitliches **Bezahlungsmittel notwendig**, damit das **Bedürfnis** nach **Bezahlung sicherstellen** kann. Selbst **primitivste Wirtschaften** entwickelten **irgendeine Form von Geld**. In der **Frühzeit** waren es **vor allem Rohstoffe**, die als Standardtauschmittel zum Einsatz kamen.

Was ist Geld?



Eine Tontafel in sumerischer Keilschrift bestätigt den Erhalt eines Ochsen.
Quelle: https://spectravest.ch/

Lydische Elektron-Münze, frühes 6. Jahrhundert vor Christus
Quelle: Von Classical Numismatic Group, Inc. http://www.cngcoins.com, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=547604

Steingeld
Quelle: Von Eric Guinther - English Wikipedia, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=161923 & Von Peter2pan - Eigenes Werk, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=32139015

Was ist Geld?

Chinesisches Kaurigeld ist eine Art des Muschel- und Schneckengeldes
Quelle: Von PHGCOM - Eigenes Werk, photographed at Japan Currency Museum, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=9580208

Im 8. Jahrhundert wurden in Japan Pfeilspitzen, Reis und Goldpuder als Tauschmittel benutzt
Quelle: Von PHGCOM - Eigenes Werk, photographed at Japan Currency Museum, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=9579952

Was ist Geld?

Das neue Papiergeld der amerikanischen Kolonien musste zuerst ausgegeben werden.

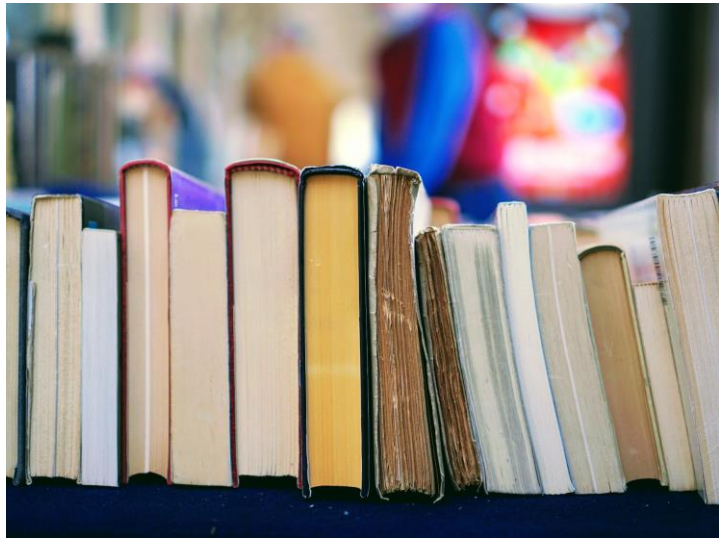
Quelle: https://spectravest.ch/

Was sind die Funktionen von Geld?

Bild: Pixabay: https://www.pexels.com/de-de/foto/goldbarren-lot-47047/

Wertaufbewahrungsmittel

Foto von Tom Hermans auf Unsplash



Tauschmittel

Foto von Diana Polekhina auf Unsplash

Preismassstab

Was ist Geld?

Grundformen des Geldes?

Grundsätzlich hat es immer nur **zwei Grundformen** von **Geld** gegeben:

- **Physische Objekte**
  Zeitlos, Beständig und Permission-less

- **Listen (Guthaben- und Schuldenverzeichnis)**
  Kopierbar, kann falsch sein und damit nicht die Realität repräsentieren, braucht zentrale Stelle für Überwachung (Nachvollziehbarkeit; Double Spend), Steuerung über Transaktionen

Was ist Bitcoin?

Ein Coin, der kein Coin ist

Bild: Michael Förtsch auf Unsplash

Bitcoin

Eine zentrale Stärke von Bitcoin:

Keine Behörde kann deine Transaktionen zensieren oder dein Geld beschlagnahmen oder verwässern.

Eine zentrale Schwäche von Bitcoin:

Keine Behörde kann dir dein Geld zurück geben wenn es verloren oder gestohlen wird.

Was ist Bitcoin

Bitcoin: Verschmelzung von Coin und Liste

Bitcoin vereint in der digitalen Welt die Eigenschaften von Physischen Objekte (Coins) und Listen (Informationen).

Das Bitcoin-Netzwerk baut die Liste so auf, dass es keine zentrale Stelle braucht und Informationen nicht kopiert werden können und löst damit ebenfalls das Double Spend Problem.

Das Resultat sind Informationen, welche wie physische Coins verwendet werden können.

Was ist Bitcoin

Entstehung / Satoshi Nakamoto

Whitepaper: Bitcoin: A Peer-to-Peer Electronic Cash System
https://www.bitcoin.com/satoshi-archive/whitepaper/

1 Bitcoin = 100'000'000 Satoshis, somit 8 Dezimalstellen (Deflationäre Währung)

Peer to Peer Zahlungssystem

Bitcoin Vermögenswert im Vergleich

	Dauerhaft	Teilbar	Fungibel	Portabel	Verifizierbar	Knapp	Erfolgsbilanz
Gold	+	−	+	−	−	+	+
Bitcoin	+	+	+	+	+	+	−
Fiat	−	+	+	+	−	−	−

Bitcoin Wallet

Einrichten eines Bitcoin Wallet

Bild: Michael Förtsch auf Unsplash

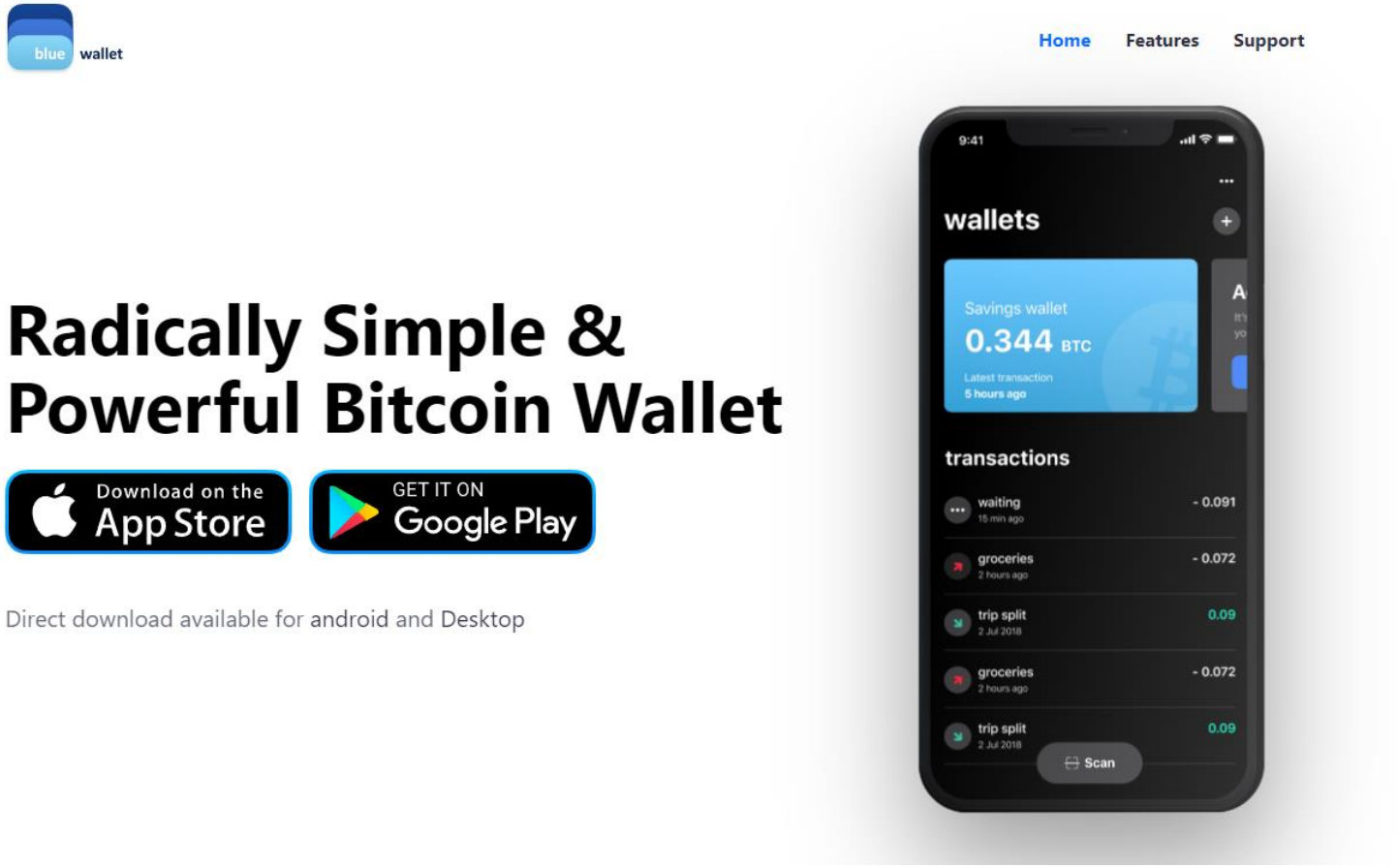
Wichtig

Not your keys, not your coins!

Nur wer die Private Keys besitzt, hat schlussendlich Zugriff auf die Coins.

Bitcoin Wallet (https://bluewallet.io/)

Bitcoin Brieftasche bzw. Wallet



Bitcoin Wallet – Backup Recovery Words

Quelle: https://bitbox.swiss/

Bitcoin Wallet – Backup Recovery Words

Aufteilung der Recovery Words auf drei Dokumente (mit zweien alle Recovery Words). Diese drei Backups bewahrt man geographisch an unterschiedlichen Orten auf.

RECOVERY WORDS

Wallet name Seed Bitbox02 1/3

01 abandon	13 account
02 hip	14 cinnamon
03 mango	15 achieve
04 december	16 yellow
05 above	17
06 weekend	18
07 expand	19
08 abstract	20
09 pink	21
10 sauce	22
11 access	23
12 topic	24

Optional passphrase

RECOVERY WORDS

Wallet name Seed Bitbox02 2/3

01 abandon	13
02 hip	14
03 mango	15
04 december	16
05 above	17 indoor
06 weekend	18 flame
07 expand	19 office
08 abstract	20 column
09	21 daring
10	22 runway
11	23 vault
12	24 scorpion

Optional passphrase

RECOVERY WORDS

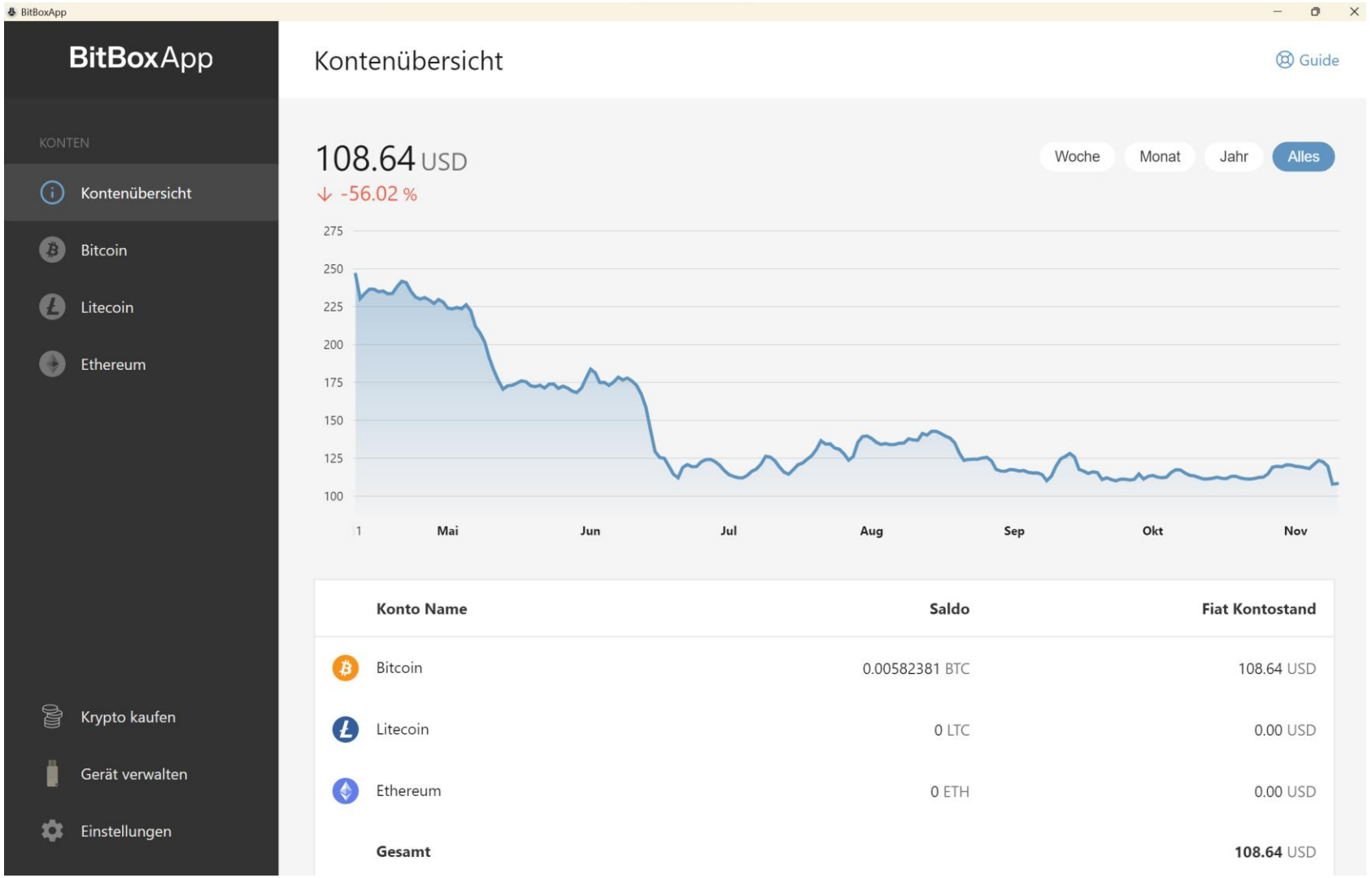
Wallet name Seed Bitbox02 3/3

01	13 account
02	14 cinnamon
03	15 achieve
04	16 yellow
05	17 indoor
06	18 flame
07	19 office
08	20 column
09 pink	21 daring
10 sauce	22 runway
11 access	23 vault
12 topic	24 scorpion

Optional passphrase

Quelle: https://bitbox.swiss/

Bitcoin Wallet – Demo Bitbox Hardware Wallet



Quelle: Screenprint aus der BitBox (https://bitbox.swiss/) App

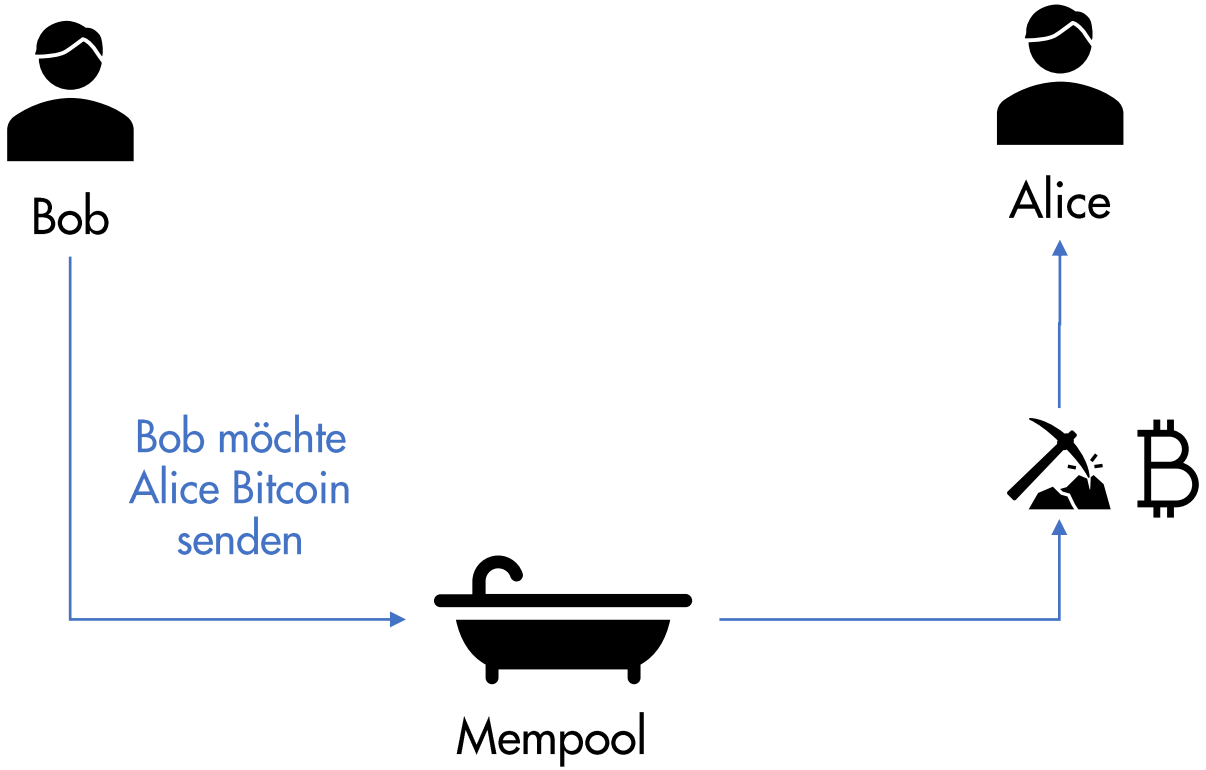
Gestaffelte Aufbewahrung

Wie beim FIAT-Geld werden auch die Bitcoin je nach Bedarf mit verschiedenen Methoden aufbewahrt werden. Hier ein Beispiel:

- Der grösste Teil der Bitcoin wird am besten mit einem dafür spezialisierten Gerät verwaltet werden, z.B. der erwähnten BitBox.
- Ein kleiner Teil wird für die bessere Verfügbarkeit auf dem Smartphone verwaltet, z.B. mit der erwähnten Blue Wallet app.
- Ein weiterer Teil der Bitcoin kann zudem auf dem Lightning-Netzwerk gespeichert werden. Lightning ist die zurzeit die bedeutendste Methode, um kleine und mittlere Zahlungen in Bitcoin abzuwickeln. Dafür kann ebenfalls die erwähnte Blue Wallet app verwendet werden.

Bitcoin Transkation

Bitcoin Transaktion



Sobald die Transaktion von Bob durch die Miner verarbeitet und diese Verifiziert wurde, werden die Bitcoin bei Alice im Wallet angezeigt

Je höher die Transaktionsgebühr von Bob angesetzt wurde, um so schneller wird ihre Transaktion durch die Miner verarbeitet

Miner nehmen die Transaktionen aus dem Mempool, um einen Block zu kreieren und diesen an die Blockchain anzuhängen und damit die Gebühren zu erhalten.

Einzigartigkeit von Bitcoin

Einzigartigkeit von Bitcoin

Komplet dezentral

Für alle akzeptierbar (unpolitisch, unreligiös, global)

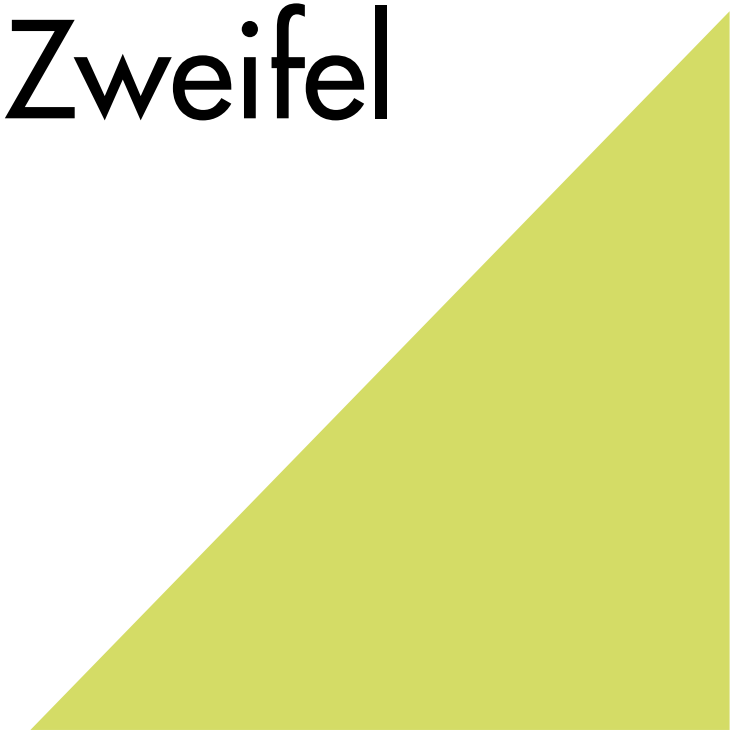
Gehört der Allgemeinheit (kein Staat, keine Firma und keine Stiftung übt eine autokratische Kontrolle aus)

Läuft seit 15 Jahren

FUD

Fear, Uncertainty and Doubt

Angst, Unsicherheit und Zweifel



Bitcoin Stromverbrauch 2021

Bitcoin Carbon-Footprint:	0.08%
Bitcoin Energie-Bedarf:	0.12%
Bitcoin Strombedarf:	0.54%

Bitcoin-Mining ist geographisch unabhängig und dort am rentabelsten, wo Strom im Überfluss vorhanden ist.

Der Stromverbrauch ist daher absolut kein Problem.

Kann man Bitcoin verbieten?

Ja, klar!

…. aber nicht stoppen!

Bitcoin Mythen

- Bitcoin haben keinen wirklichen Wert, und machen keinen und es gibt null Sicherheiten dahinter
- Bitcoin ist anonym
- Bitcoin ist eine Blase/Ponzy-Schema
- Bitcoin ist nicht skalierbar
- Bitcoin ist wegen der Volatilität nur für risiko-affine Trader
- Bitcoin kann schnell verschwinden, wenn die Blockchain gehackt wird, der Strom ausgeht, oder ganze Länder den Handel mit drakonischen Strafen verbieten

Wir wünschen Euch
weiterhin viel Spass mit Bitcoin