Bitcoin Weesen

https://bitcoinweesen.ch

Bitcoin Lightning

16. Januar 2024

Intro & Ziele

Das erreichen wir heute gemeinsam

Bitcoin Weesen

Intro

Bitcoin und Zahlungen

Am letzten Meetup im November 2023 haben wir die Grundlagen von Geld und Bitcoin angeschaut.

Dabei wurde klar, dass Bitcoin auf der Blockchain kein skalierenden Zahlungssystem sind kein. (Mining-Aufwand teuer und nicht instant, sondern mit längeren Zeitverzögerung.

Als Lösung für diese erwähnten Herausforderungen wurde Bitcoin Lightning entwickelt. Dieses gibt Antworten auf die Herausforderungen und bietet sich als schnelles und günstiges Zahlungssystem an.

Bitcoin Weesen

Ziele

Am Ende des Treffens habt Ihr

- ein Recap über die Sicherung einer Wallet erhalten
- ein Gefühl für Phising Angriffe im Bitcoin-Umfeld
- ein Verständnis über die Grundlagen von Bitcoin Lightning
- ein Verständnis bzgl. der Unterschiede von Bitcoin und Bitcoin Lightning
- ein Bitcoin Lightning Wallet erstellt und damit Bitcoin transferiert

Aktuelles

Entwicklung seit dem letzten Treffen

Aktuelles

Bitcoin ETF Freigabe in den USA

Die US-Wertpapieraufsicht SEC hat 11 ETF (Exchange Traded Funds). Normalerweise werden mit ETFs Börsenindexe nachgebildet. Die neuen Bitcoin-ETF bilden keinen Index nach, sondern reflektieren die Preisentwicklung des Bitcoin.

Die Zulassung gilt derzeit nur für die USA, aber die Schweiz bietet eine Vielzahl an Alternativen, die in den USA nicht zugänglich sind.

Aktuelles

Gut oder Böse? Ein paar Gedanken dazu

- Bitcoin Spot ETF investieren direkt in Bitcoin (physisch nicht synthetisch). D.h. die ETF-Anteile bildet Anteile der Fonds ab.
- ETF sind leicht kauf und handelbar (aber nicht 7 x 24) und nun auch für institutionellen Anleger zugänglich.
- Bitcoin entstand in der Zeit der Finanzkriese der traditionellen Finanzwelt, nun umarmt genau diese den Bitcoin!
- Spekulation, aber ja nach politischer Situation nicht unmöglich: Erster Schritt, damit in den USA gesetzlich der direkte Besitz von Bitcoin nur noch institutionellen Anleger vorbehalten sein wird.

Recap: Sicherung einer Bitcoin Wallet

Wie bewahrt man seinen Seed auf

Bitcoin Weesen

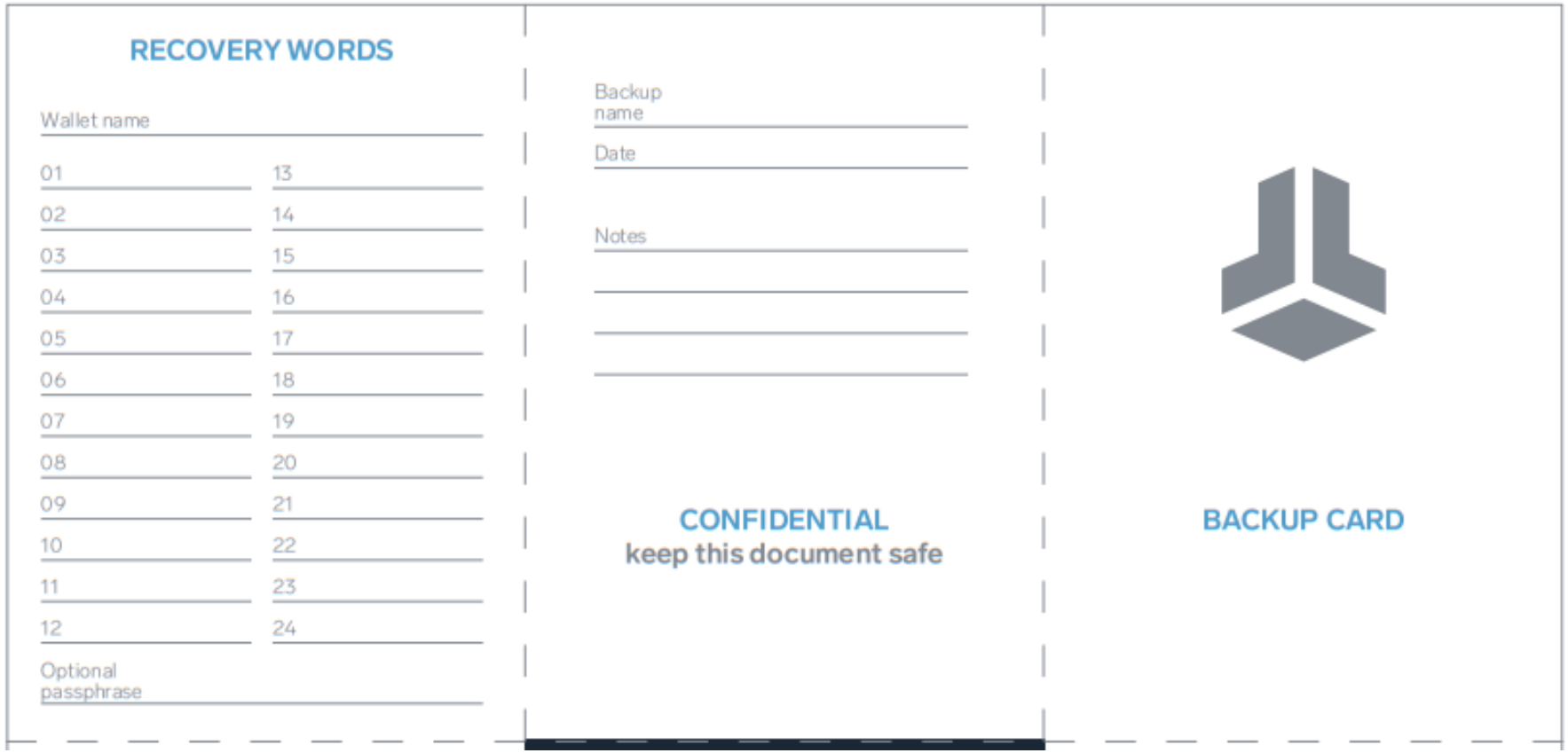
Recap: Sicherung einer Bitcoin Wallet

Häufig beobachtete Fehler beim Backup

- Man macht kein Backup!
- zu glauben, dass man nach jeder Transaktion ein Backup erstellen muss
- Backup auf dem Computer/Smartphone speichern
- Backup nicht an einem sicheren Ort aufbewahren
- Digitale Backups nicht regelmässig verifizieren

Bitcoin Weesen

Bitcoin Wallet – Backup Recovery Words



Quelle: https://bitbox.swiss/

Bitcoin Weesen

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

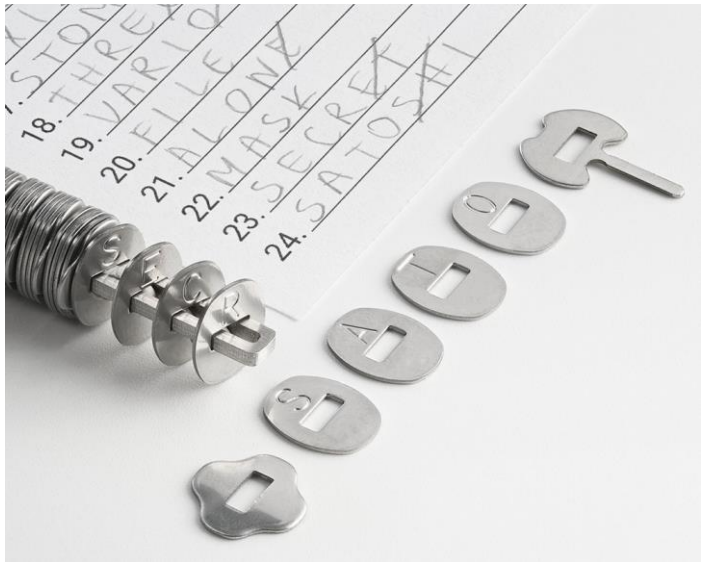
01		13	account
02		14	cinnamon
03		15	achieve
04		16	yellow
05		17	indoor
06		18	flame
07		19	office
08		20	column
09	pink	21	daring
10	sauce	22	runway
11	access	23	vault
12	topic	24	scorpion

Optional passphrase

Quelle: https://bitbox.swiss/

Bitcoin Weesen

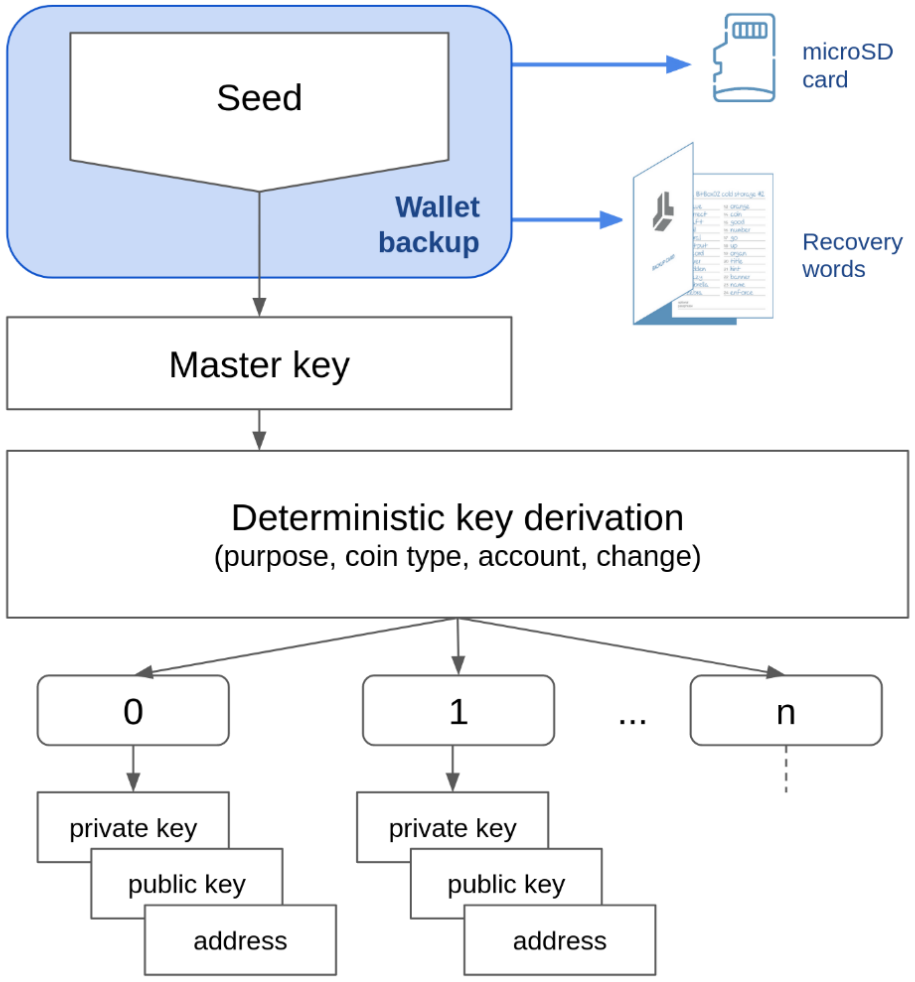
Bitcoin Wallet – Backup Recovery Words



Quelle: https://bitbox.swiss/
Quelle: https://cryptosteel.com/product/cryptosteel-capsule-solo/

Bitcoin Weesen

Bitcoin Wallet – Backup Recovery Words



Quelle: https://bitbox.swiss/

Bitcoin Weesen

Vermeiden von Phishing-Angriffen

- Wenn ich Bitcoin bei mir gespeichert habe (in "cold storage", z.B. auf einem Hardware-Wallet wie der Bitbox oder Trezor oder Coldcard) kann ich Nachrichten getrost ignorieren.
- Wenn jemand behauptet, dass die Bitcoin nicht sicher wären, dass sie unbedingt verschoben werden müssen, dass neue Bestimmungen erlassen wurden oder werden können Sie das ignorieren.
- Man kann die Bitcoin auch mal fünf Jahre liegen lassen ohne Nachrichten zu lesen.
- Wenn Sie Sich unsicher fühlen, so können Sie Sich also immer viel Zeit nehmen, der Sache in Ruhe nachzugehen und einfach nichts zu machen.

Bitcoin Lightning

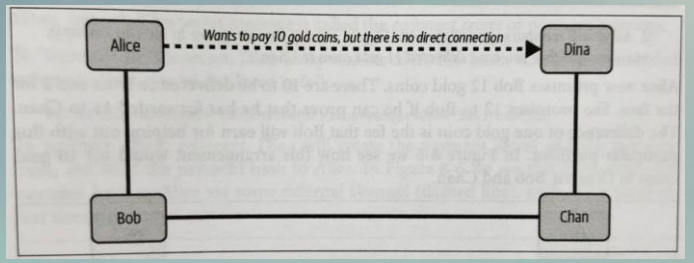
Bitcoin Weesen

Bitcoin Lightning

- **Warum Bitcoin?**
  - **Inflationsschutz, "echtes" Sparen**
  - **Faire Welt, Trennung von Geld und Staat**
  - **Schutz vor Bankrott der Banken, oder vor behördliche Massnahmen**
  - **Schnelle & günstige Zahlungen für Alle**
- **Warum Brauchen Wir Lightning?**
  - **Bitcoin-Blockchain verarbeitet nur 7 Transaktionen pro Sekunde**
  - **Eine Blockchain-Transaktion dauert mindestens 10 Minuten**
  - **Nicht jede Transaktion benötigt die höchste Sicherheitsstufe**
  - **Das Ziel ist Bitcoin für alle 9 Milliarden**

Bitcoin Weesen

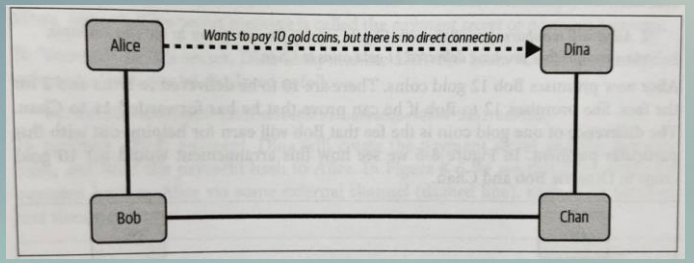
Bitcoin Lightning



- **Lightning *ist* Bitcoin**
- **Wie funktioniert Lightning (vereinfacht)?**
  - **Zwei Parteien erstellen und unterschreiben Bitcoin-Transaktionen, veröffentlichen diese aber nicht, sondern speichern diese privat.**
  - **Sie können in diesem "Zahlungs-Kanal" nun Satoshis hin- und herschieben ohne dass Platz auf der Blockchain beansprucht wird.**
  - **Wenn einer von beiden Parteien "saldieren" will, dann werden die (notwendigen) Transaktionen in die Blockchain geschrieben.**
  - **Zahlungskanäle können auf eine sichere Art und Weise zu einem Netzwerk verknüpft werden (s. Bild).**
  - **Alles ist so implementiert, dass die Satoshis aller Teilnehmer jederzeit gesichert sind.**

Bitcoin Weesen

Bitcoin Lightning



- **Was hat Lightning zu bieten?**
  - Rasche Bestätigung der Zahlung
  - Guter Schutz der Privatsphäre des Senders (weniger beim Empfänger)
  - Zahlung von Kleinbeträgen
  - Value4Value – z.B. Bezahlung von Podcasts pro Minute

Bitcoin Weesen

Bitcoin Lightning

- **Wie kann ich Lightning nutzen?**
  - **Wallet mit eigenen Kanälen**
    - **volle Kontrolle über das eigene Geld**
    - **anfängliche Gebühren bei der Eröffnung eigener Kanäle**
    - **erfordert regelmässige Online-Präsenz**
  - **Bitcoin Bank**
    - **schnell, effizient, einfach, billig**
    - **benötigt Vertrauen in die Betreiber der Bitcoin Bank**

Bitcoin Weesen

Beispiele von Lightning Transaktionen

- **Einkauf auf Dezentralshop.ch**
- **Rechnung für Konsumation**
- **Zap für eine Nostr Note**
  - **Mikro-Zahlung für einen guten Beitrag auf Nostr, einem sozialen Medium**