Bitcoin

Seedmanagement

und

Privatsphäre

Seedmanagement

Seed (engl. für „Samen“)

11011010010 00010110010 11110010011 …

Seed
zufällige Folge von 128 bis 256 Nullen und Einsen

surge bind venue …

Seed-Phrase
12 bis 24 Worte aus einer BIP39-Liste mit 2048 Wörtern
Letztes Wort: Prüfsumme

E9873D79C6D87DC0FB6A5778633398 …

Privater Schlüssel
Transaktionen signieren

offline

online

034DAB19972EEC17E0670C6D162F9A …

Öffentlicher Schlüssel
Transaktionen erstellen

bc1p0g75u54m6yxfznkpf4qlpcfzpgn5k …
bc1qf9hm37lcualt66kc6m4mrt7rqfucs …

Bitcoin-Adressen…
virtuelle Kontonummer für den Empfang von Bitcoin

1. Erzeugung der Seed-Phrase

- Immer **offline** erstellen (Offline-Computer, Hardwarewallet, airgapped, Tails[1]) - Coldstorage

Passport[2]

SeedSigner[3]

- Prozessor für echte Zufallszahlen verwenden (z. B. Bitbox02[4], Passport[2]) oder alternative Verfahren (Seed aus Bild erzeugen oder selbst würfeln, z. B. SeedSigner[3])

- Wenn würfeln, dann echte Casinowürfel empfohlen

Bitbox02[4]

USB (nicht airgapped)

[1] https://tails.net
[2] https://foundationdevices.com
[3] https://seedsigner.com
[4] https://bitbox.swiss

1. Erzeugung der Seed-Phrase

- 24-Wort-Seed-Phrase erstellen (höhere Entropie)
- keine Beobachter oder Zuhörer (Person, Kamera, Spiegelung im Fenster, Alexa, ..)
- Seed nicht sprechen oder flüstern (beim Aufschreiben oder eingeben)
- Beim Aufschreiben: Harte Unterlage (Stift drückt durch)
- Ggf. selbst Worte verändern (Achtung: Prüfsumme, SeedSigner[1] oder Specter[2])
- zusätzliche Passphrase mit genügender Länge nutzen (s. auch [3]).

Beispiel: Passwort mit Zahlen, Groß- und Kleinbuchstaben

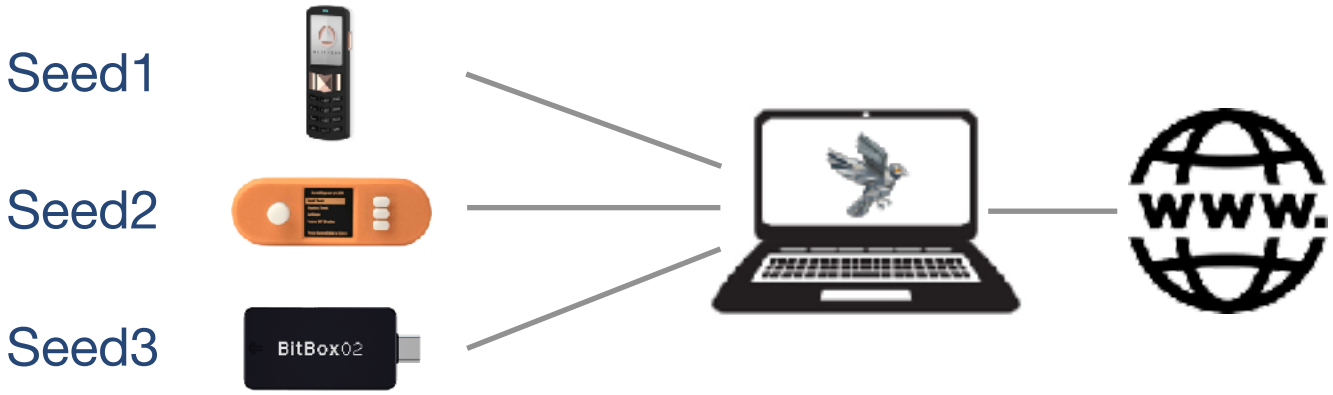
Länge Pass-Phrase (Zeichen)	**6**	**9**	**12**	**15**
benötigte Zeit zum Knacken	**1 Sek.**	**3 Tage**	**2000 Jahre**	**600 Mio Jahre**

[1] https://seedsigner.com
[2] https://specter.solutions/hardware
[3] https://www.snafu.de/sichere-passwoerter-einsetzen

1. Erzeugung der Seed-Phrase

MultiSig-Wallets

- Nutzung mehrerer Seeds + ggf. Pass-Phrasen für 1 (MultiSig)Wallet
- Erstellung von *m* aus *n* Wallets
  - Erstellung mit *n* Seeds
  - nur *m* Seeds zum Signieren notwendig
  - Wiederherstellung mit allen *n* Seeds oder Outputdescriptor (+ *m* Seeds)
- Minimierung des Vertrauens in einzelne Hardware



1. Erzeugung der Seed-Phrase

Besonderheit bei Seed-Erzeugung mit Electrum

- standardmäßig keine BIP39 - Seed-Phrase[1]
- nicht mit anderen Wallets wiederherstellbar
- nur 12 Wörter
- längere Seed-Phrasen nur über Kommandozeile
- verarbeitet BIP39-Seed-Phrasen beim Wiederherstellen einer Wallet (Import)

[1] *https://electrum.readthedocs.io/en/latest/seedphrase.htm*

2. Aufbewahrung | physischer Verlust

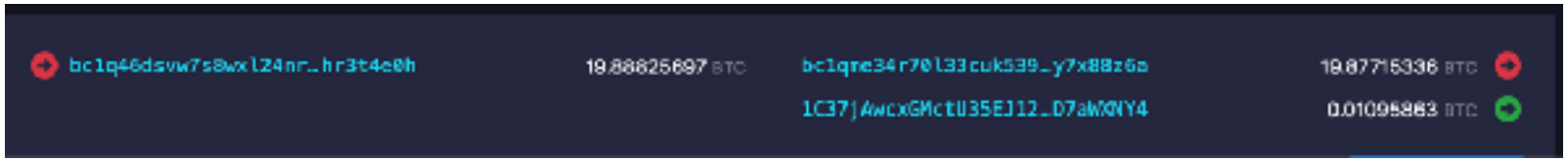
NOT-Todo-List (was solltet ihr NICHT mit der Seed-Phrase machen):

- nur im Gehirn abspeichern (Brainwallet)
- nur auf einem Speichermedium (z. b. USB-Stick) speichern
- offen rumliegen lassen
- jemandem geben, der z.B. ein Metall-Backup erstellen soll
- bei einem Notar/ Anwalt hinterlegen (ggf. nur als MultiSig oder ohne Passphrase)
- Auf einem Online-Gerät oder gar auf einem Online-Dienst speichern oder ausdrucken
- fotografieren
- per Messenger, Mail, etc. verschicken
- Aufzeichnung (z. B. Zettel mit Seed-Phrase) nicht gut genug venichten

2. Aufbewahrung | physischer Verlust

Macht euch nicht selbst zum Ziel!

- möglichst niemandem erzählen ob und wieviele Bitcoin ihr habt
- wenn, dann eher von Satoshis sprechen
- für jeden Empfang eine neue Adresse, nicht zu viele Bitcoin pro Adresse (ein Empfänger sieht, wieviele BTC auf der Senderadresse lagen)



- Wallet nicht an Halskette oder Ledger-Mütze[1] mit Wallet-Tasche tragen! 🙄

Bildquellen:
https://farm1.static.flickr.com/176/420757246_ae1e9ad260.jpg?v=0
[1] https://shop.ledger.com/products/fvckrender-lvcidia-ledger-nano-x-bundle

2. Aufbewahrung | physischer Verlust

Gefahren	Lösung	
Feuer, Wasserrohrbruch, physischer Verfall des Papiers, Vergilben der Schrift	Metall-Backup[1]	
	Metallplatte[2]	
	Eigenbau[3,4]	
Verschüttet (Erdbeben) oder verbaut	Redundanz (weitere Kopien des Seeds an entfernten Orten)	

[1] *https://unchained.com/blog/seed-phrase-backup-methods-recording-paper-metal*
[2] *https://bitbox.swiss/steelwallet*
[3] *https://nodesignal.space/2021/07/08/bitcoin-seed-stahl-backup/#2*
[4] *https://3d-printfarm.de -> „Real Shop..“*

2. Aufbewahrung | unbefugter Zugriff

Gefahren	Lösung
Diebstahl (Einbruch), Hausdurchsuchung, Hacker testen Kombinationen von Seed-Phrasen	• zus. Passphrase[1] (nicht mit im Backup) • Seedworte vertauschen (!) • (Shamir-Backup[1] (Kompatibilität?, online?..)) • MultiSignature[1] • ersten x Bitcoinadresse nicht nutzen
Herausgabe unter Zwang	• „Opferwallet“
Seed aus Hardware auslesen	• Secure Element verwenden (z. B. Bitbox02[2]) • Seed nicht auf Hardware speichern (SeedSigner[3])
Hackerangriff	• Coldstorage • airgapped Geräte

[1] https://www.seedor.io/en-int/blogs/info/bitcoin-recovery-seed-phrase-verschlusseln-shamir-backup-vs-seed-spliting-vs-passphrase
[2] https://bitbox.swiss/de/bitbox02/sicherheit
[3] https://seedsigner.com

3. Vererbung

(keine steuerliche Betrachtung!)

Probleme:

- BTC-Vermögen soll so sicher sein, dass ein unbefugter Zugriff so sehr wie möglich erschwert ist
- für Erben soll der Zugriff dennoch einfach möglich sein, ohne dass der Erblasser unterstützen kann
- Erben haben ggf. kaum Wissen über Bitcoin und Seedhandling
- Streit zwischen den Erben
- Erben sollten zu Lebzeiten des Erblassers keinen Zugriff haben.

Ziel:

- die Erben dürfen (auch gemeinsam) zu Lebzeiten des Erblassers **nicht** alle Informationen zur Wallet-Wiederherstellung haben
- bei Eintreten des Erbfalls, **müssen** alle notwendigen Informationen für die Erben vorliegen
- Bei mehreren Erben darf die Wallet-Wiederherstellung nur gemeinsam möglich sein
- Verlust von einzelnen Informationen einkalkulieren

3. Vererbung | Materialbeschaffung

je Erbe:

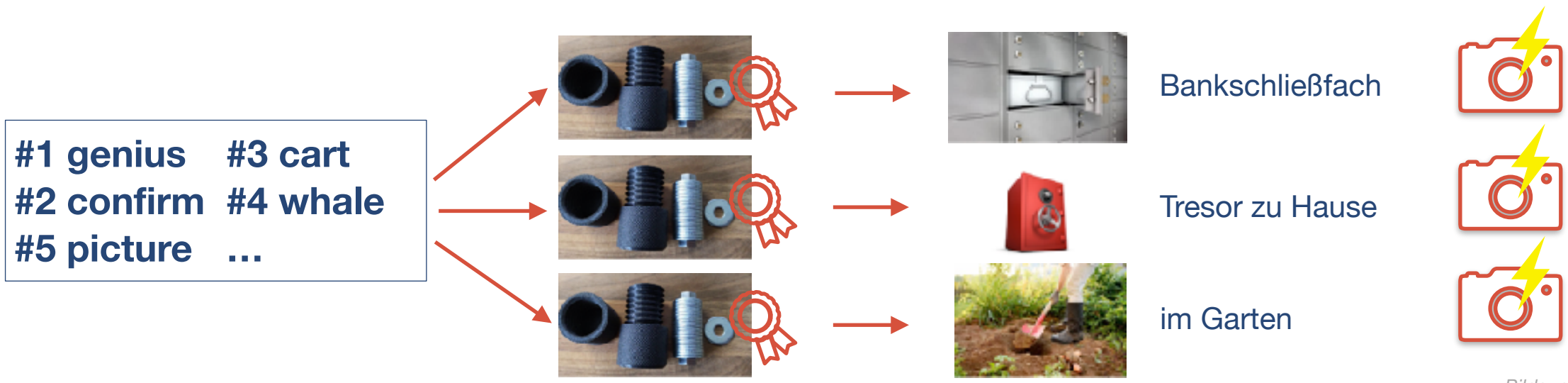
- 1 x Hardwarewallet (ggf. unterschiedliche Fabrikate) + zus. Speichermedium für Firmwarebackup
- 2 x Briefumschläge und Material zum Versiegeln (z. B. Siegelwachs, Stempel oder Papierklebestreifen)
- Papier für Handlungsanweisungen
- 1 x Vererbungskiste (Dokumentenbox oder -tasche)

- 3 x Material für Seed-Metall-Backup + Behälter
- Möglichkeit zum Laminieren der Handlungsanweisungen

3. Vererbung | Lösungsidee

1. Schritt:

- Erstellung eines Masterseed (24 Worte) -> 3 x Metallbackup -> einzeln verpacken und versiegeln
- Hinterlegen je einer Kopie an 3 verschiedenen, möglichst sicheren Orten (Bankschließfach, Safe, Vergraben)+Foto



Bildquellen:
https://3d-printfarm.de -> „Real Shop..“
https://www.teckbote.de/cms_media/module_img/84/42186_1_topstorybox_589a71d3a539b.jpg
https://t3.ftcdn.net/jpg/00/17/41/00/240_F_17410035_1FjoFD9sEWe4PDDMqkE6rXH1xw8Y4CRv.jpg
https://m3.paperblog.com/i/164/1641508/gartenschaufeln-die-das-graben-im-garten-einf-L-EVt4P1.jpeg

3. Vererbung | Lösungsidee

2. Schritt:

- Erstellung je einer persönlichen Passphrase je Erbe, bestehend aus einem gleichen (gemeinsamen) Teil und je einem persönlichen Teil
- Notieren des persönlichen Teils der Passphrasen (je ein Dokument je Erbe und Anwalt) jeweils in einen Umschlag, versiegeln, beschriftet mit dem Namen des Erbes (könnte z. b. auch Teil des Testaments sein)

3. Vererbung | Lösungsidee

3. Erstellen der MultiSig Wallet:

- Erstellen der beiden Seeds (je: Masterseed + (zusammengesetzte) persönliche Passphrase)
- Notieren von Ableitungspfad (und Fingerprint?)

Masterseed		pers. Passphrasen		Ableitungspfad
#1 genius	**#3 cart**	+ **Sei deine eigene Bank! a1b2c3 kPvkDi7bQ8wc**	= Seed 1	m/84’/0’/0
#2 confirm	**#4 whale**			
#5 picture	**…**	+ **Sei deine eigene Bank! a1b2c3 nEFGsLouJoEL**	= Seed 2	

Erstellung der Watch-Only-MultiSig-Wallet (2 aus 2) auf dem Online-PC (z. b. Sparrow) über die öffentlichen Schlüssel

3. Vererbung | Lösungsidee

4. Handlungsanweisungen

- Erstellen einer Schritt-für-Schritt-Handlungsanweisung für die Erben
  - wo die Backups der Seedphrasen zu finden sind (inkl. Fotos)
  - gemeinsame Teil der Passphrase
  - dass ein privater Teil der Passphrase erforderlich ist, den sie von entspr. Stelle erhalten werden
  - Anweisung über „Zusammenbau“ der persönlichen Passphrase
  - Handhabung der Hardware-Wallets, Eingabe Seed/ Passphrase inkl. Ableitungspfad
  - Installation Sparrow
  - Erstellung der MultiSig-Wallet
  - Handhabung der Wallets zum erstellen und Signieren von Tansaktionen
- Handlungsanweisung möglichst einlaminieren (Schutz vor Schimmel, Wasser, ..)

3. Vererbung | Lösungsidee

4. Abschluss + Vererbungskiste:

- Die erstellte Handlungsanweisung sollte nochmals selbst durchgespielt und auf Korrektheit der Daten und Nachvollziehbarkeit geprüft werden. Auch Menschen, die kein Wissen von Bitcoin haben, sollen damit umgehen können
- Hinterlegung der versiegelten Briefe bei den Anwälten (jeder der Anwälte erhält für jeden der Erben je einen Brief)
- Hinterlegen der Handlungsanweisung, Hardwarewallet, ggf. notwendige Kabel sowie Firmware auf entsprechendem Speichermedium (z. B. microSD-Karte) in Vererbungskiste (eine Kiste pro Erbe)
- Verschließen/ Versiegeln der Vererbungskisten => Übergabe an Erben
- Die Schlüssel könnten ggf. mit bei den Anwälten in den jeweiligen Briefen hinterlegt werden
- Wenn möglich, Schulung der Erben zu Bitcoin und generelle Handhabung der Wallets

=> 1 .. 2 x pro Jahr: Prüfen der Seed-Lagerorte und ggf. Vererbungskisten auf Vorhandensein und Unverletztheit der Siegel

Bildquelle: https://www.wagner-sicherheit.de/tresore/master-lock-h0100eurhro-wasserdicht-feuerbestaendig.html

Privatsphäre

Generell

- Betriebssystem und Apps aktuell halten
- Blickschutzfolie
- Downloads von Wallet Software prüfen! (Anleitungen auf den jeweiligen Download-Seiten)

Browser

- Sicheren Browser nutzen
  - Brave[1] (blockt: Tracking, Fingerprints, Cookies, Phishing, …)
  - Mullvad Browser[2]
- Suchmaschine:
  - startpage.com
  - SearXNG[3] (eigene Suchmaschine), SearXNG-Instanzen[4]

SearXNG

[1] https://brave.com
[2] https://mullvad.net/de/browser
[3] https://github.com/searxng/searxng
[4] https://searx.space

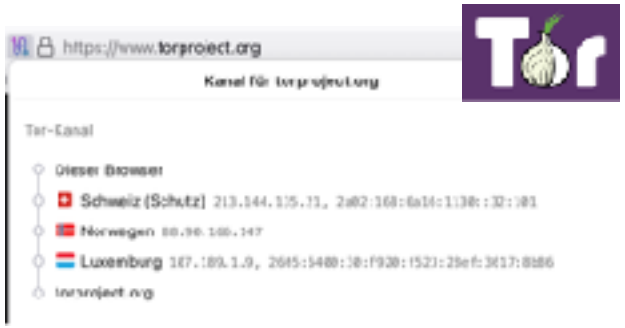
Privatsphäre

Mobilgeräte

- De-Googled-Betriebssystem nutzen (z. B. GrapheneOS[1], LineageOS[2], CalyxOS[3])
- No-KYC eSIM (silent.link[4]) (nur Daten)

Verstecken der eigenen IP

- Virtuelles Privates Netzwerk (VPN) nutzen (z. B. Mullvad[5])
- Tor - Browser[6] nutzen
- Orbot[7] nutzen (PC, mobile)



[1] https://grapheneos.org
[2] https://lineageos.org
[3] https://calyxos.org
[4] https://silent.link
[5] https://mullvad.net
[6] https://www.torproject.org
[7] https://orbot.app

Privatsphäre

Kommunikation

- Ende-zu-Ende-Verschlüsselte Messenger, die nicht auf Kontakte zugreifen
- „Erstellen der Linkvorschau“: ausschalten
- verschwindende Nachrichten
- verschlüsseltes Mailsystem (z. B. Proton[5])

SIMPLEX[1]

- keine eindeutige Kennung für Nutzer
- Inkognito-Modus
- kein zentraler Server
- untersch. Server für Senden und Empfangen
- …

Eigener Server mit Fullnode + Apps

- Umbrel[2], Start9[3], Raspiblitz[4], u. a.
- Apps: Bitcoin Fullnode, LightningNode, Electrs Server, Nostr Relay, SimpleX Server, …

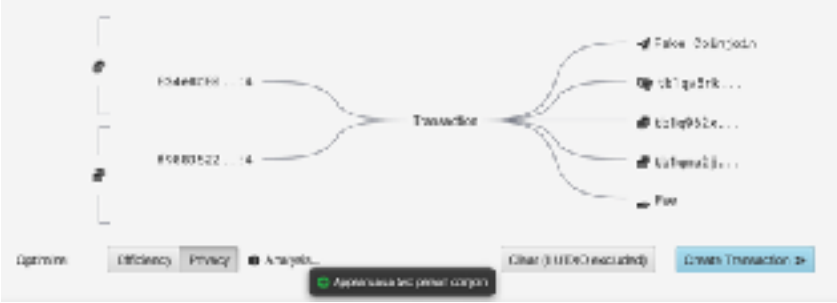
Sparrow-Wallet — eigener Server — Lightning-Wallet

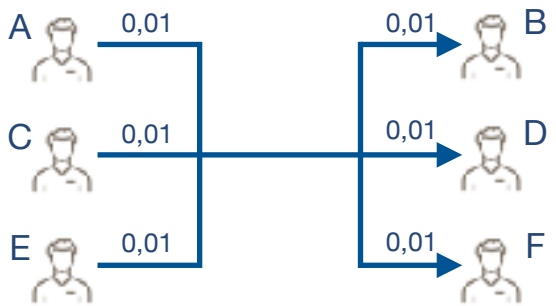
[1] https://simplex.chat
[2] https://umbrel.com
[3] https://start9.com
[4] https://raspiblitz.org
[5] https://proton.me

Privatsphäre

CoinJoin[1]

- Mehrere Transaktionen werden zu einer einzelnen zusammengefasst
- Sparrow Wallet





Whirlpool Mixing[2]

- Coinjoin mit anderen Usern und mehreren Durchgängen (Mixing-Runden)
- Nutzung von Mixing-Pools
- Coins landen wieder in der eigenen Wallet

[1] *https://sparrowwallet.com/docs/spending-privately.htm*
[2] *https://sparrowwallet.com/docs/mixing-whirlpool.html*

Sei Deine eigene Bank!

Vielen Dank!