ecash and **privacy**

Ein Chaumsches electronic cash-Protokoll

Einundzwanzig Linz
Block 954401 #957d80

Agenda

- Das “**Warum?**”
- Das “**Was?**”
- Das “**Wie?**”

Ziele

- Grundlegendes Verständnis von …
  - … **was ecash ist**
  - … **Vertrauensannahmen** und **Auswirkungen auf die privacy**
- Bildet die **Grundlage** für **weiteres Selbststudium**
- Nicht-Ziele
  - Expertenwissen

Wer von euch…

…hat schon von **ecash** gehört?

…hat schon einmal eine **ecash-Payment** gemacht?

…hat schon einmal eine **Lightning-Payment** gemacht?

…betreibt eine **Lightning-Node**?

ecash and **privacy**

Warum?

Warum...?

- **Custody**
  - … weil niemand seinen eigenen Key selbst verwahrt
- **Infrastruktur**
  - … weil niemand eine Lightning-Node betreibt

Warum...?

- **Sicherheit**
  - … weil niemand Backups erstellt
- **Privacy**
  - … weil niemand collaborative transactions nutzt

Warum...?

- **Skalierbarkeit**
  - … weil bitcoin nicht skalieren kann

ecash and **privacy**

Was?

Was?

- Eine **custodial** Infrastruktur
  - Aber mit Fokus auf privacy
- **Anonymes** digitales bearer token
  - Keine Accounts
- Transaktionen sind **instant** und **final**
  - Genau wie physisches Bargeld

Was?

- Blind signatures erhalten die privacy der Nutzer
- Transaktionen sind „peer-to-peer“
- Offenes und interoperables Protokoll
- Kostenlos und open source

Entitäten

- **Mint** := Aussteller & Einlöser von Vouchern
- **Ecash token** („bearer asset“) := Voucher
- **Wallet** := Sammlung von Vouchern

Mint

Mints sind **Lightning nodes**, die **Infrastruktur als Service** bereitstellen. Sie **agieren als Custodian** für satoshis im Lightning-Netzwerk und **geben dabei ecash aus** an die Nutzer.

Mint

- Setzt auf einer Lightning-Node auf
- Agiert als Custodian
- Gibt ecash aus

Token

Ein **token** ist ein Datensatz, der aus einem **blindly signed secret** besteht. Es wurde **vom Mint signiert** mit dem privaten Schlüssel für einen bestimmten Betrag und ist eine **IOU-Repräsentation** von satoshis, die **vom Mint verwahrt werden**. Ein token ist ein „**bearer asset**“.

Token

- Datensatz, signiert von einem Mint
- Fungiert als IOU („I owe you“) von satoshis
- Ein „bearer asset“

Bearer Asset

Ein **bearer asset** ist ein Vermögenswert, der **demjenigen gehört, der ihn physisch besitzt**, ohne dass eine **Registrierung des Eigentums** erforderlich ist. Die **Eigentumsübertragung** erfolgt einfach durch **Übergabe** des physischen Vermögenswerts.

Bearer Asset

- Gehört demjenigen, der es physisch besitzt
- Keine Registrierung des Eigentums
- Übertragung erfolgt durch „Übergabe“

Token

cashuAeyJ0b2tlbiI6W3sicHJvb2ZzIjpbeyJpZCI6IjAwO
WExZmY5ZTVkYzA4NzMiLCJhbW91bnQiOjIsImMiOiIwMjY5
YzcyYjcwZjZmMTEzNzY5Y2YwZDNmN2I3NWY5MjczZTQ2MjU
zMzI2YzVkYWQzODkxNmRlYTk3ZjEwNzU0ZjMiLCJzIjoiZT
g4MzY0YzJhMDY4MzdhODU1MWZmMTU0MTQ0M2NhYzQ0ZDgyY
zc3YWJmYjBjY2E3YTJhYzJkYzYwNDJiOWZhOSJ9XSwibWlu
dCI6Imh0dHBzOi8vdGVzdG1pbnQuY2FzaHUuc3BhY2UifV0
sInNjcmlwdCI6bnVsbH0

Token


```
{
  "token": [
    {
      "mint": "https://8333.space:3338",
      "proofs": [
        {
          "amount": 2,
          "id": "009a1f293253e41e",
          "secret": "407915bc212be61a77e3e6d2aeb4c727980bda51cd06a6afc29e2861768a7837",
          "C": "02bc9097997d81afb2cc7346b5e4345a9346bd2a506eb7958598a72f0cf85163ea"
        },
        {
          "amount": 8,
          "id": "009a1f293253e41e",
          "secret": "fe15109314e61d7756b0f8ee0f23a624acaa3f4e042f61433c728c7057b931be",
          "C": "029e8e5050b890a7d6c0968db16bc1d5d5fa040ea1de284f6ec69d61299f671059"
        }
      ]
    }
  ],
  "unit": "sat",
  "memo": "Thank you."
}
```

Blind Signature

Eine **blind signature** ist eine kryptografische Technik, bei der ein Signierer **eine Nachricht signiert, ohne deren Inhalt sehen zu können**. Die Person, die die Signatur anfordert, blindet (verschleiert) die Nachricht, bevor sie sie an den Signierer sendet, der die geblindete Version signiert, **ohne zu wissen, was er signiert**. Anschließend kann der Anfragende die Nachricht **entblinden** und erhält eine **gültige Signatur auf dem Original**.

Wallet

Eine **wallet** ist Software, die **ecash tokens verwaltet**. Da tokens selbst keinen Wert haben, repräsentieren sie immer nur **verwahrte Gelder** . Eine wallet kann **alle Daten lokal speichern**, nichts muss auf irgendwelchen Servern gespeichert werden.

Wallet

- **Verwaltet** ecash tokens
- **Keine Accounts** erforderlich
  - Mints verfolgen oder speichern keine Salden der Nutzergelder
- **Senden** und **empfangen** von tokens
  - Ermöglicht out-of-band- oder air-gapped-Wertübertragungen
- Gelder werden **lokal gespeichert**
  - Wird der Speicher gelöscht, gehen die Gelder verloren

ecash and **privacy**

Wie?

Token lifecycle

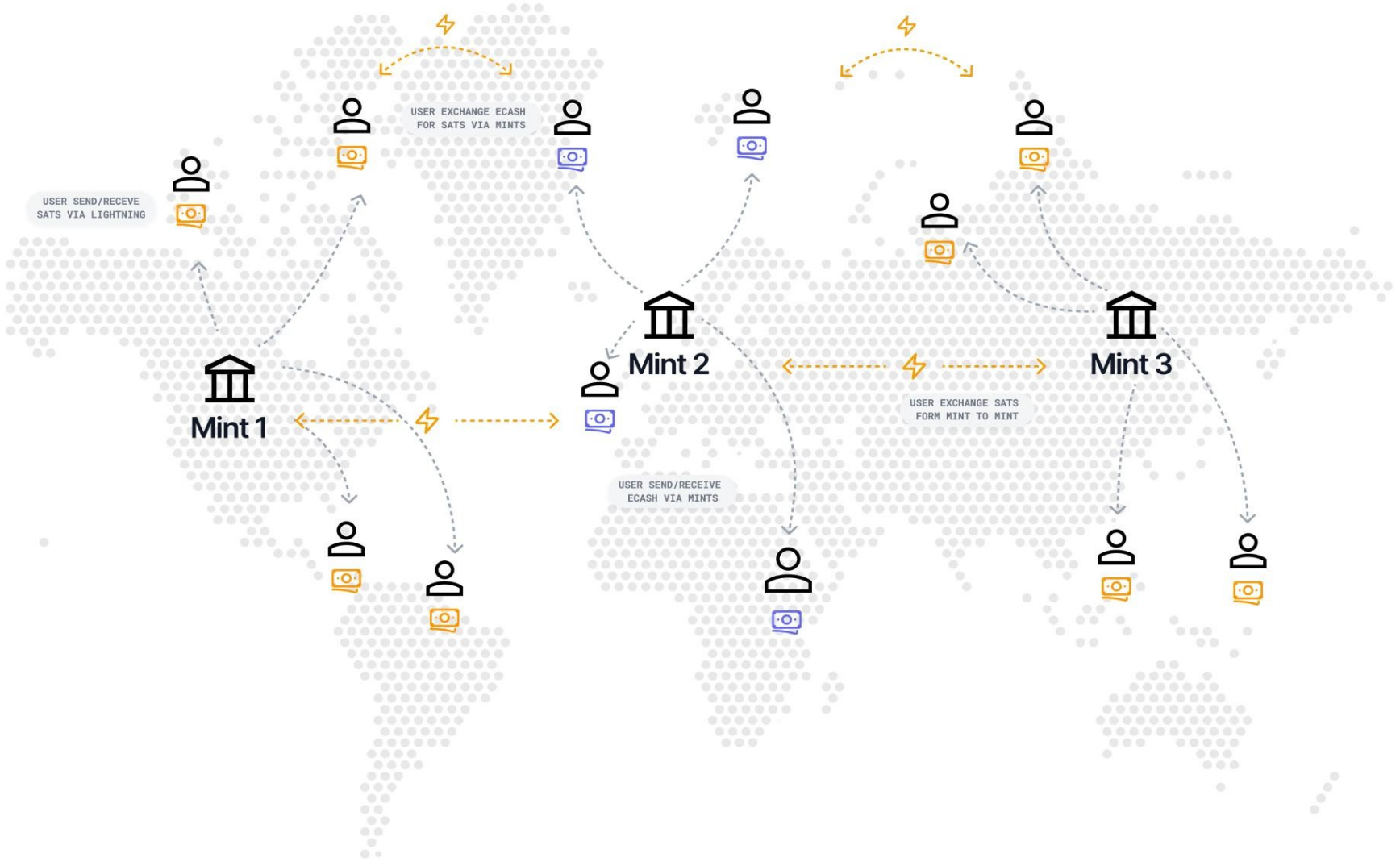
- **Mint** := Einen Voucher erstellen
- **Swap** := Einen Voucher tauschen
- **Melt** := Einen Voucher einlösen

Wie?

1) **Mint**: Nutzer zahlen bitcoin in einen Mint ein und erhalten ecash

2) **Swap**: Für Übertragungen innerhalb eines Mints werden tokens peer-to-peer ausgetauscht und anschließend über den Mint eingelöst

3) **Melt**: Für Übertragungen zwischen Mints werden Zahlungen über das Lightning-Netzwerk geroutet


USER EXCHANGE ECASH
FOR SATS VIA MINTS
USER SEND/RECEVE
SATS VIA LIGHTNING
Mint 1
Mint 2
Mint 3
USER EXCHANGE SATS
FORM MINT TO MINT
USER SEND/RECEIVE
ECASH VIA MINTS

Cashu 

- Cashu ist kostenlos und open-source
  - https://cashu.space/
- Basiert auf Spezifikationen (NUTs)
  - https://github.com/cashubtc/nuts
- Referenz-Web-Wallet
  - https://cashu.me

ecash and **privacy**

https://mint.21linz.at

https://cashu.me

Überlegungen zur privacy

- **Lightning**
  - Das Swappen in den und aus dem Mint erfordert Lightning-Transaktionen
  - Ein Mint kann einen Empfänger identifizieren und Zahlungen zensieren
- **Token-Beträge**
  - Cashu verwendet feste (Zweierpotenz-)Token-Stückelungen („hide-in-the-crowd effect“)
  - Größere tokens sind „einzigartiger“
  - „*Wenn es nur ein token einer bestimmten Stückelung gibt, kann es immer auf seine Entstehung zurückverfolgt werden.*“

Überlegungen zur privacy

- **Privacy auf Netzwerkebene**
  - Mints können Netzwerkdaten wie Zugriffszeit, IP-Adressen und andere Metadaten sammeln
  - Tools wie Tor, I2P, VPNs usw. verwenden
- **Payment-Kanäle**
  - Zahlungen sind „out-of-band“: Du bist selbst für deren Übertragung verantwortlich (d.h. verschlüsselte Kanäle verwenden)
  - Der sicherste Kanal ist, tokens air-gapped zu senden (über QR-Codes)

ecash and **privacy**

Fragen und **Antworten**

Fragen und **Antworten**

- Betreibe deine eigene ~~node~~ **mint**.
- Bleib bescheiden, stack sats.
- Fix the money, fix the world.