„Anchoring“

Anchoring für APBS & PSBC

3/2025 (v1)

AUSTRIA PRO

BLOCKCHAIN INITIATIVE AUSTRIA

Übersicht

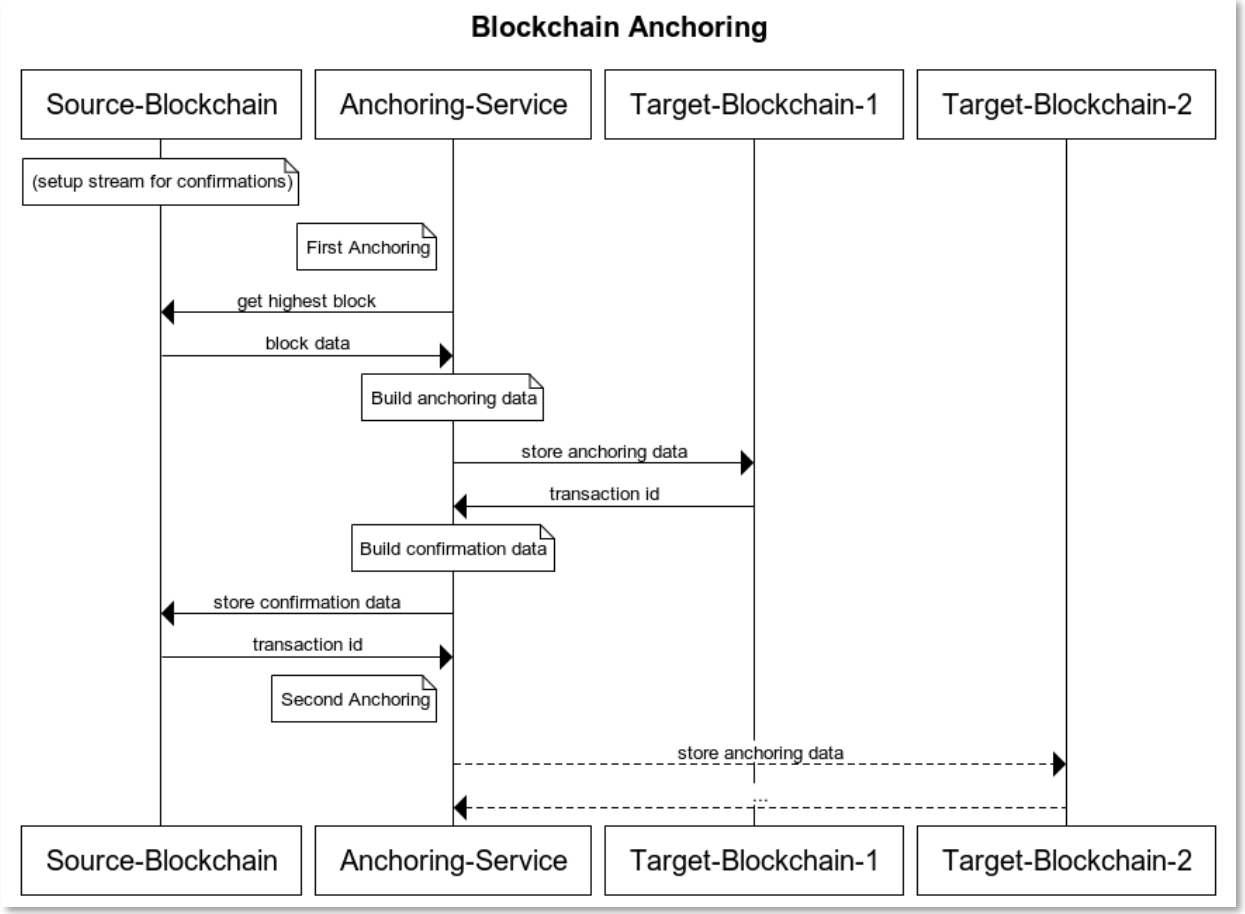
- Zweck
  - Erster Prototyp 2023
- Ablauf Anchoring
- Ablauf Verifikation
- Neue Umsetzung 2025
  - Beispiel Anchoring
  - Beispiel Verifikation
- Next steps

Erhöhung des Vertrauens durch „Anchoring“ (2023ff)

- Notarisieren des aktuellen Zustandes einer Blockchain in einer anderen Blockchain („snapshot“)
  - Typischerweise um eine „kleine“ Blockchain …
  - … in eine „große“ zu verankern
  - Z.B. private oder Konsortiumchain mit wenigen Nodes in eine public Blockchain
- Zweck: Nachweis dass die Source-Chain
  - nicht manipuliert wurde
  - bzw. potentielle Manipulationen erkannt würden
- Anchoring Daten: Status des jeweils aktuellen „höchsten“ Blocks
  - Blocknummer
  - Block-Hash
  - Zeitstempel
  - (diverse Metadaten)

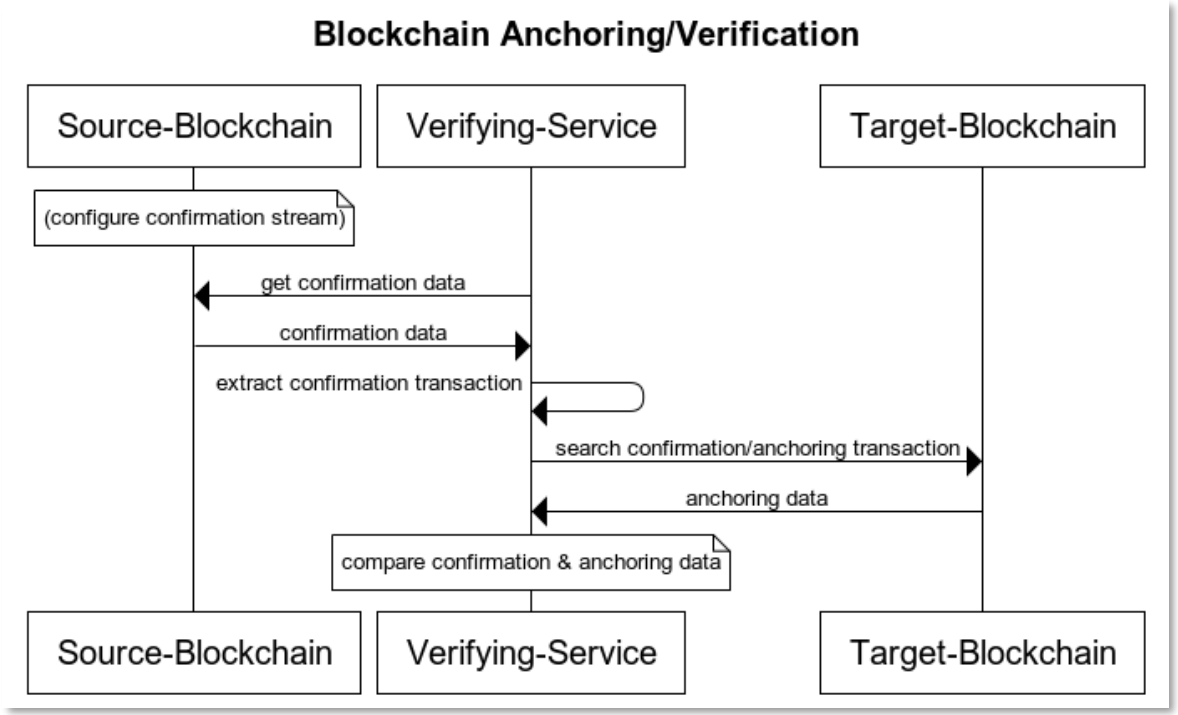
Anchoring - Ablauf

- Aktuelle Blockdaten von Source-Chain abfragen
- Daten aufbereiten
- Daten in Target-Chain Transaktion speichern
- Bestätigung zusammensetzen (=Blockdaten plus Transaktions-Id)
- Bestätigung in Source-Chain speichern



Anchoring – Ablauf Verifikation

- Daten aus Source-Chain lesen (behauptetes Anchoring und Bestätigungs-Transaktion)
- Transaktion (Anchoring data) in Target-Chain suchen
- Daten vergleichen
- Optional: Blockdaten in Source-Chain verifizieren



Anchoring – Umsetzung 2025 (Beispiel Multichain)

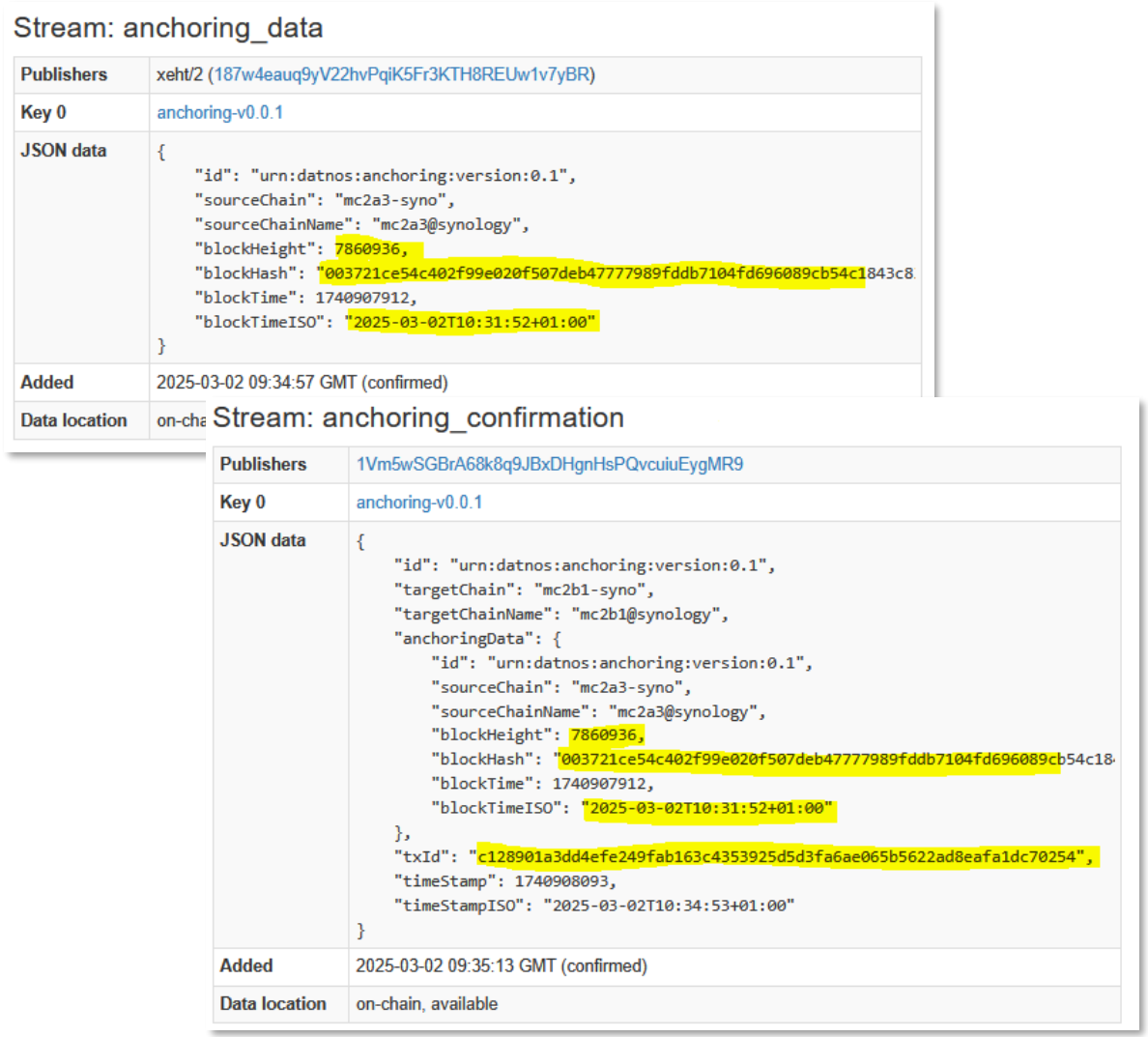
- Anchoring von Node “mc2a3”
  - sourceChain
- An “mc2b1”
  - targetChain
  - stream “anchoring_data”
- Bestätigung zurück an “mc2a3”
  - stream “anchoring_confirmation”
- Status sourceChain
  - zB. Block 7860936

Block

Height	7860936
Time	2025-03-02 09:31:52 GMT
Hash	003721ce54c402f99e020f507deb47777989fddb7104fd696089cb54c1843c83
Miner	1KzUbXU7QGm8ecNSeBGgCQKX8JYzNZjYxgmoFq
Confirmations	12844
Version	3
Size	268
Merkleroot	e3ab403f6fdb64b4b33b2eb036cce7714a91c2df90cd8fef7ede5ea14b27fe2c
Nonce	223
Bits	2000ffff
Difficulty	5.9604644775391E-8
Chainwork	00000000000000000000000000000000000000000000000000000077f2c900
Previous	00ceed099ddabfffabf201aa4b9f131080d87d54c4aab853385f681c373e9a68
Next	0051a3f21deda15c5b79b29f9c6ff0adbf863d78cf06fbca50092824bc3c8171
Transactions	1

Anchoring – Umsetzung 2025 (Beispiel Multichain)

- “anchoring_data” in der targetChain
- “confirmation_data” zurück an die sourceChain



Stream: anchoring_data

Publishers	xeht/2 (187w4eauq9yV22hvPqiK5Fr3KTH8REUw1v7yBR)
Key 0	anchoring-v0.0.1
JSON data	{ "id": "urn:datnos:anchoring:version:0.1", "sourceChain": "mc2a3-syno", "sourceChainName": "mc2a3@synology", "blockHeight": 7860936, "blockHash": "003721ce54c402f99e020f507deb47777989fddb7104fd696089cb54c1843c8 "blockTime": 1740907912, "blockTimeISO": "2025-03-02T10:31:52+01:00" }
Added	2025-03-02 09:34:57 GMT (confirmed)
Data location	on-cha

Stream: anchoring_confirmation

Publishers	1Vm5wSGBrA68k8q9JBxDHgnHsPQvcuiuEygMR9
Key 0	anchoring-v0.0.1
JSON data	{ "id": "urn:datnos:anchoring:version:0.1", "targetChain": "mc2b1-syno", "targetChainName": "mc2b1@synology", "anchoringData": { "id": "urn:datnos:anchoring:version:0.1", "sourceChain": "mc2a3-syno", "sourceChainName": "mc2a3@synology", "blockHeight": 7860936, "blockHash": "003721ce54c402f99e020f507deb47777989fddb7104fd696089cb54c18 "blockTime": 1740907912, "blockTimeISO": "2025-03-02T10:31:52+01:00" }, "txId": "c128901a3dd4efe249fab163c4353925d5d3fa6ae065b5622ad8eafa1dc70254", "timeStamp": 1740908093, "timeStampISO": "2025-03-02T10:34:53+01:00" }
Added	2025-03-02 09:35:13 GMT (confirmed)
Data location	on-chain, available

Anchoring - Umsetzung 2025

Verifikation

- „behauptetes“ Anchoring aus sourceChain auslesen
- Transaktion in targetChain suchen und Transaktionsdaten lesen

- Beide Datensätze vergleichen
- -> Verifikation OK

Next steps

- Implementierung in Echt-Systemen der APSB und PSBC „wechselweise“
- Vorhandenen Prototypen erweitern
  - „große“ public Blockchains
  - zB. Ethereum
  - Varianten
    - Anchoring Daten direkt in Transaktionsdaten
    - Oder: Smart Contract zur Speicherung und zur Verifikation
- Code Opensource?
  - Mindestens f. Verifikation

- Konnex zu EBSI?