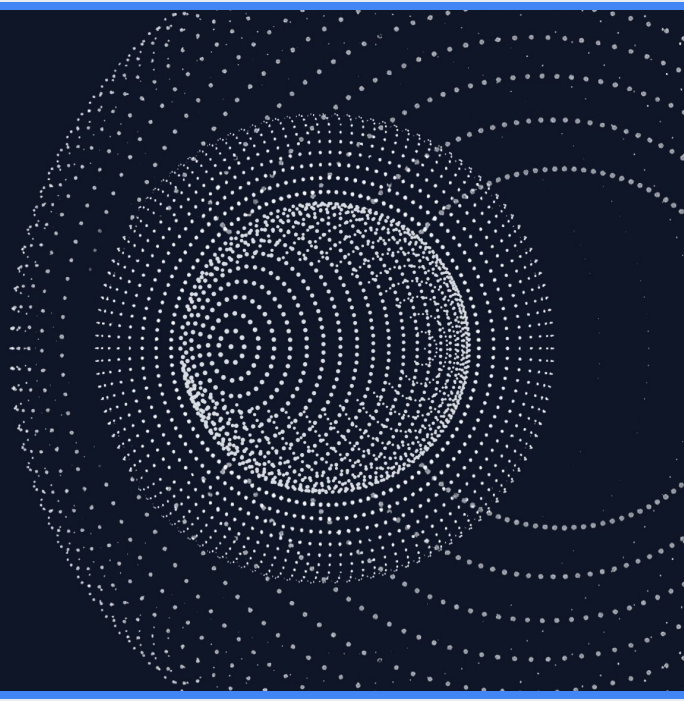
Fairgate

Benchmarking Bridge Designs for Bitcoin



Sergio Demian Lerner | CTO, Fairgate Labs

SEPT 2025

Agenda

1. Difficulty of Bridging Blockchains
2. Basic “Bridge” types
3. Peg-in Peg-out functionality
4. Bridge Designs
    a. Federated vs BitVM vs Validating Bridges
    b. Contestable vs Non-contestable Bridges
5. Summary

Bridge Hacks

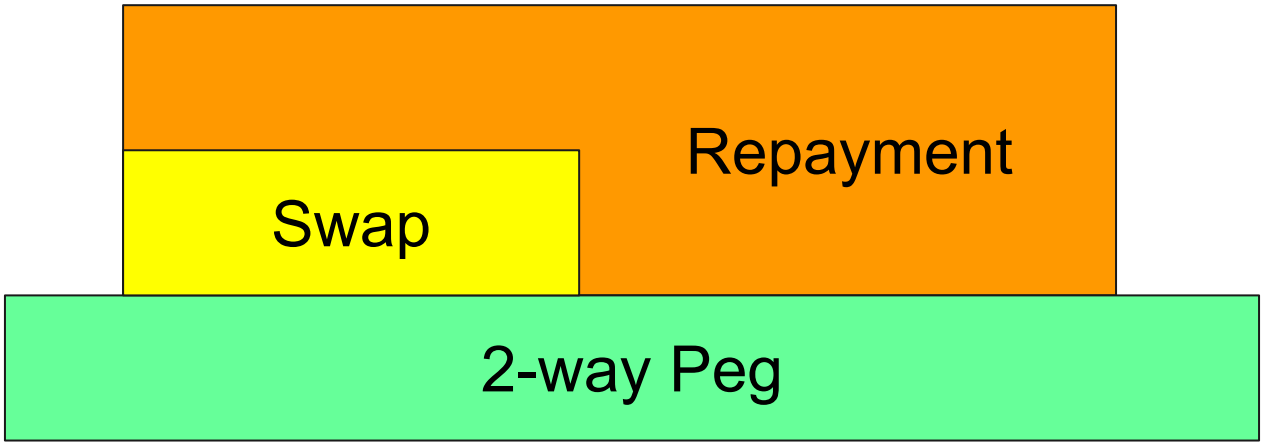
- **Nomad Bridge hack:** In August 2022, around $200 million. Code vulnerability in Nomad smart contracts.
- **Harmony Horizon Bridge hack:** In June 2022, ~$100 million in crypto. The hackers compromised two of the four validators on the Horizon Bridge's multi-signature wallet.
- **Ronin Bridge:** In 2022, roughly $625 million in crypto. Five of nine validators on the network were hacked.

Basic “Bridge” types

Types of Bridges

- 2-way pegs (2WP)
  - Locks X, creates a new asset pX
- Swaps:
  - exchanges X for pX and vice-versa
- Repayment protocols
  - Fast swap + slow transfer over a 2WP to balance liquidity

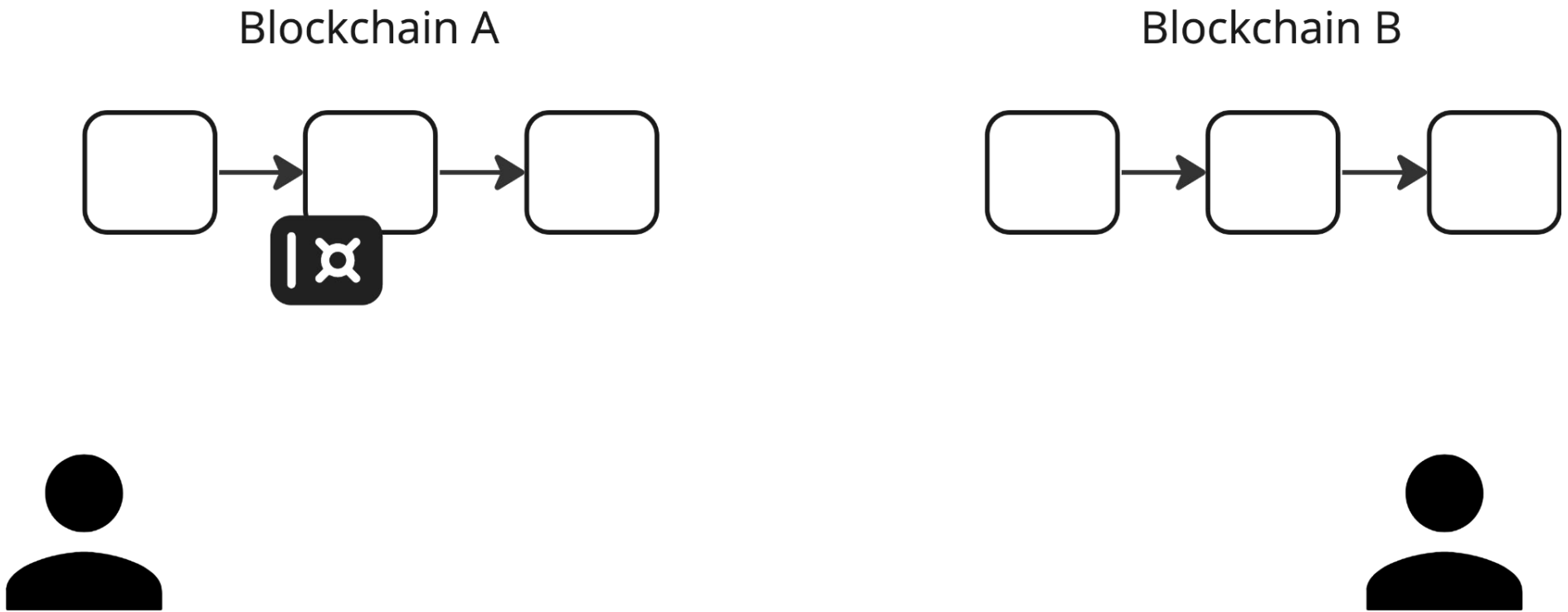
Types of Bridges

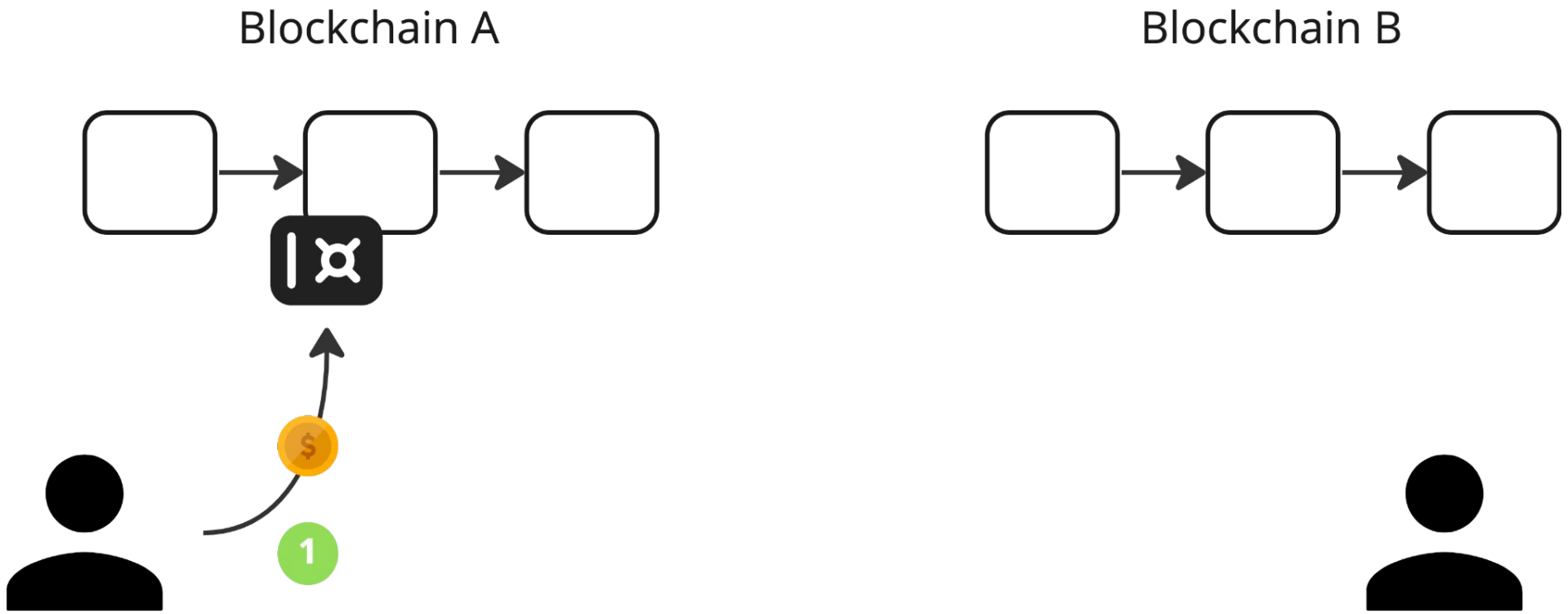


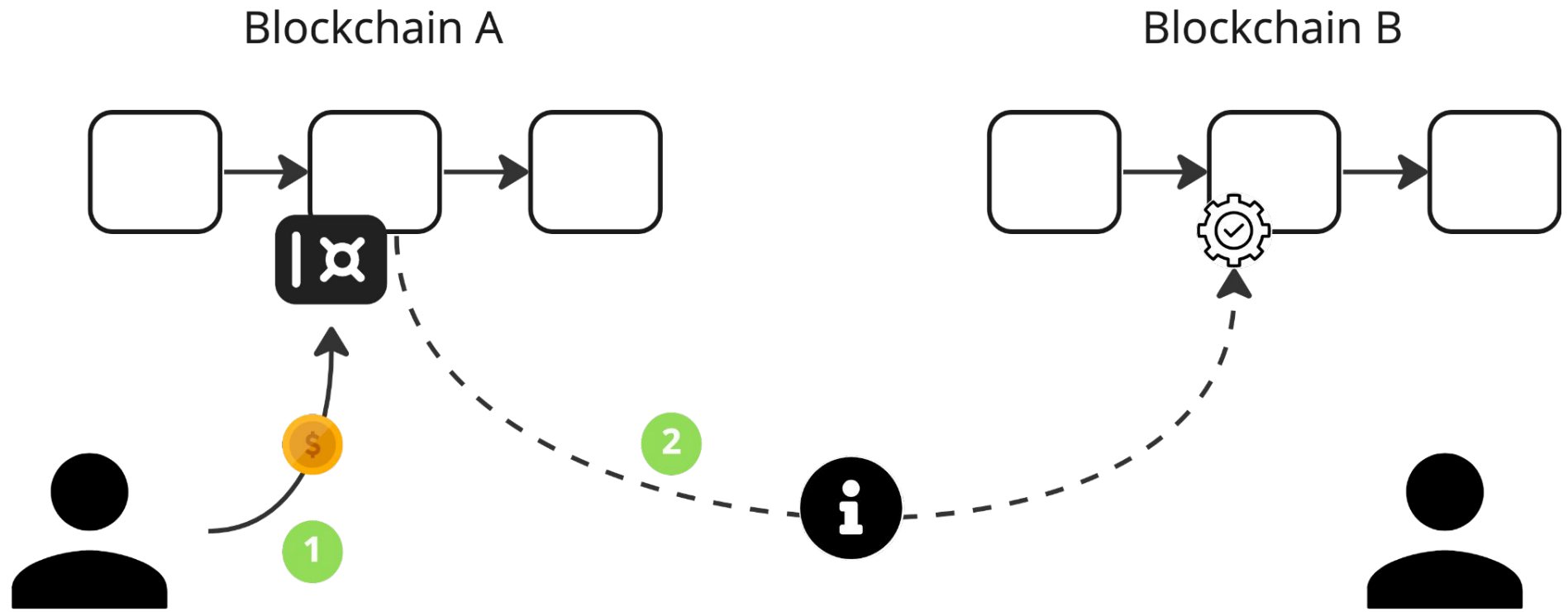
Properties of a Two-way-peg

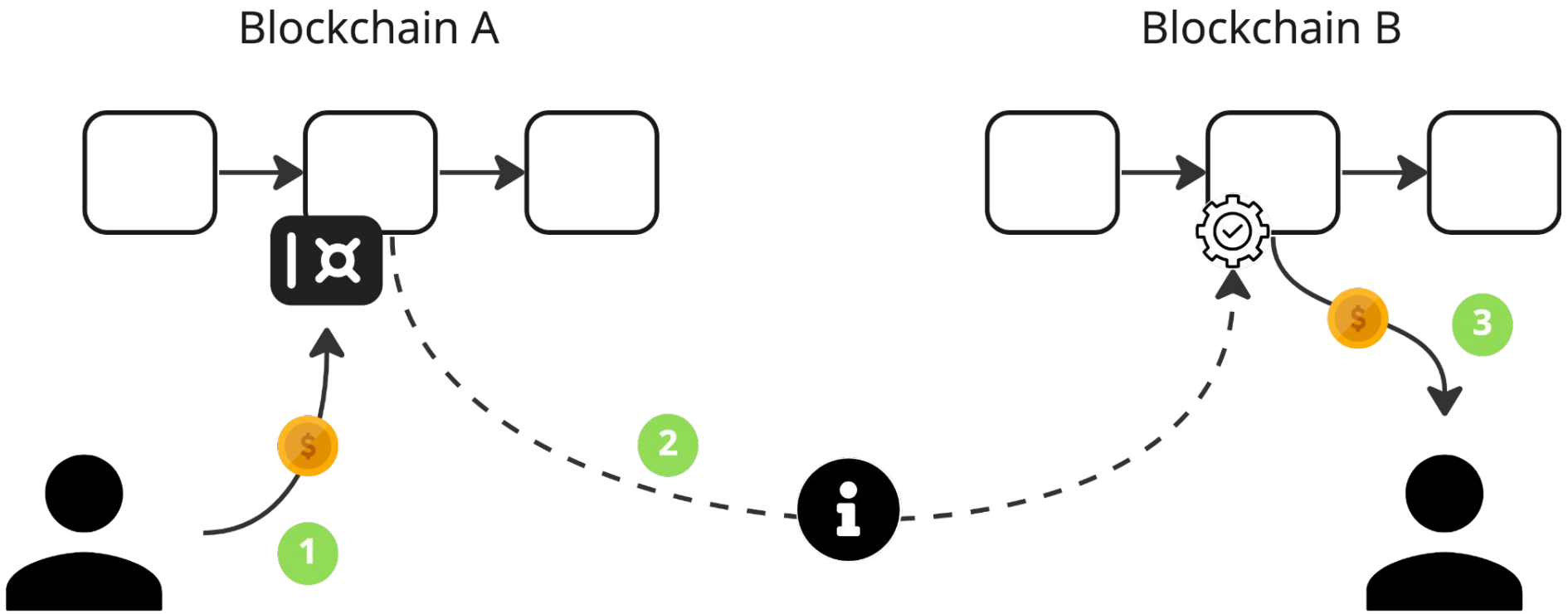
- Connects a parent and a child blockchain
- The parent chain has a digital asset X.
- Creates a proxy digital asset pX on the child blockchain
- Parent -> Child
  - Locks an amount of asset X
  - Issues the same amount of asset pX and transfers it
- Child -> Parent
  - Burns an amount of asset pX
  - Unlocks the same amount of asset X and transfers it

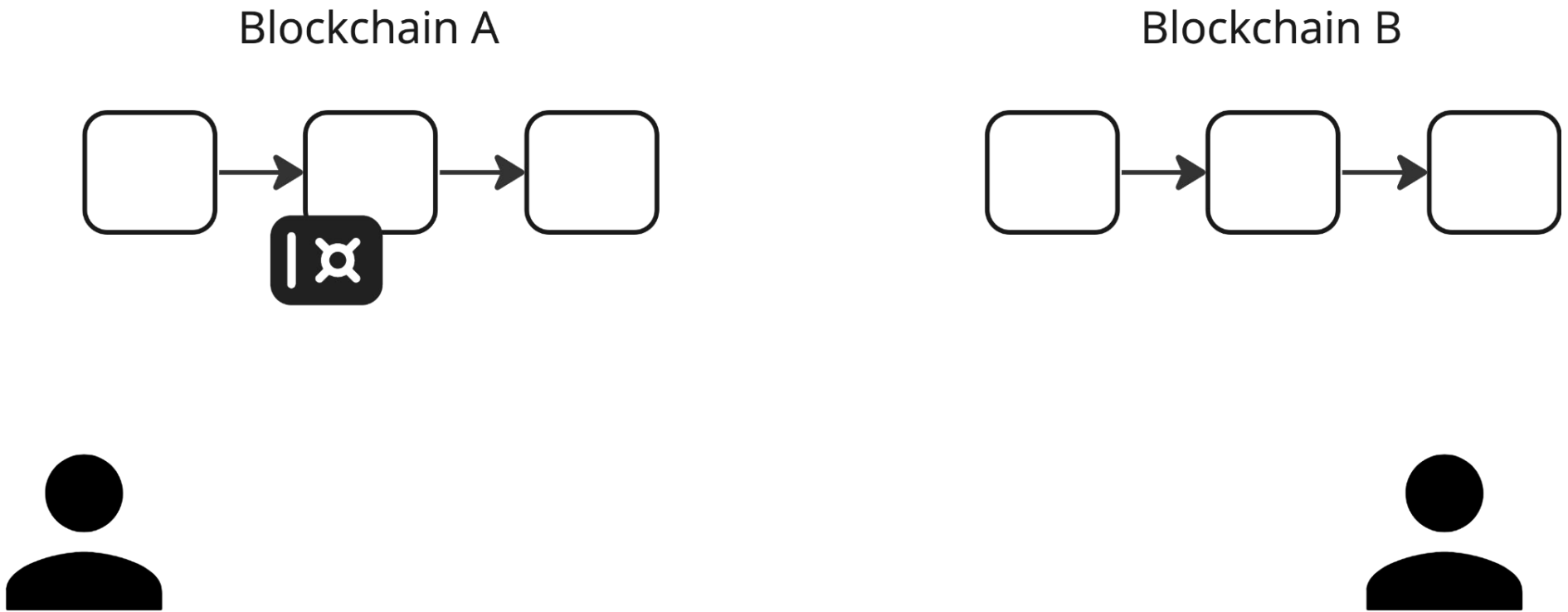
Peg-in and Peg-out

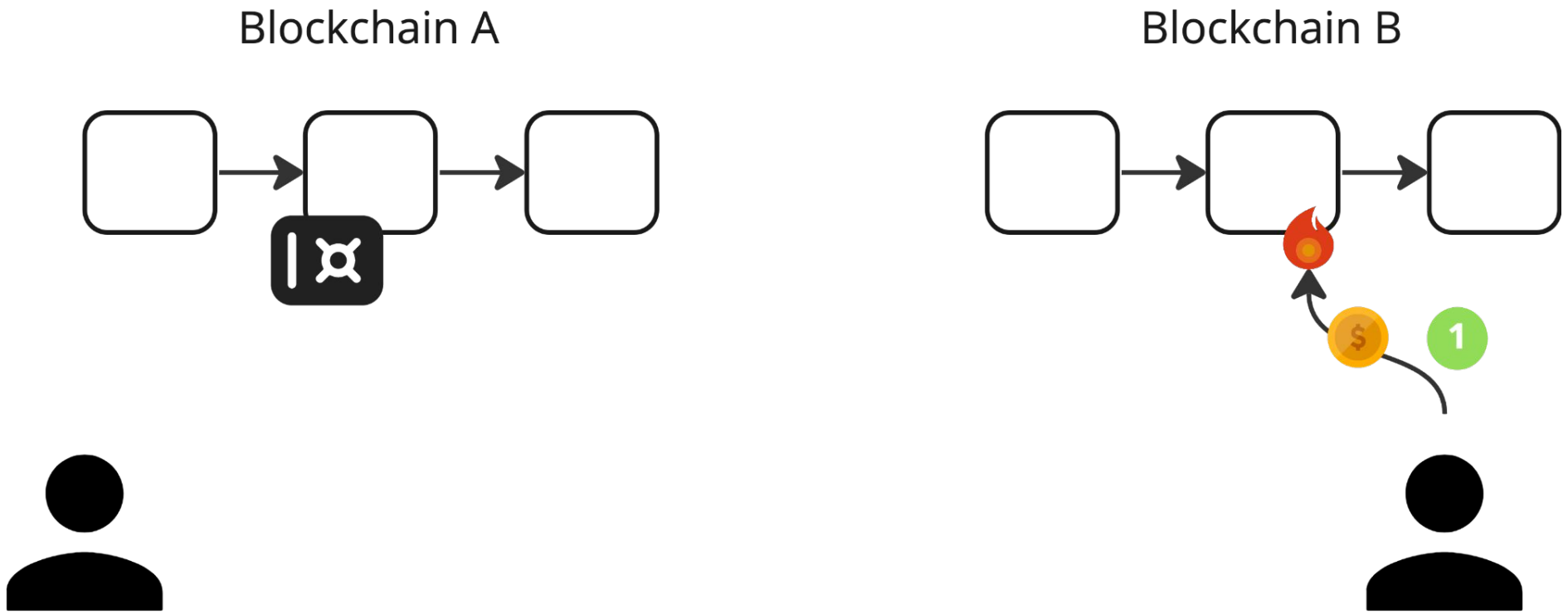

Blockchain A
Blockchain B

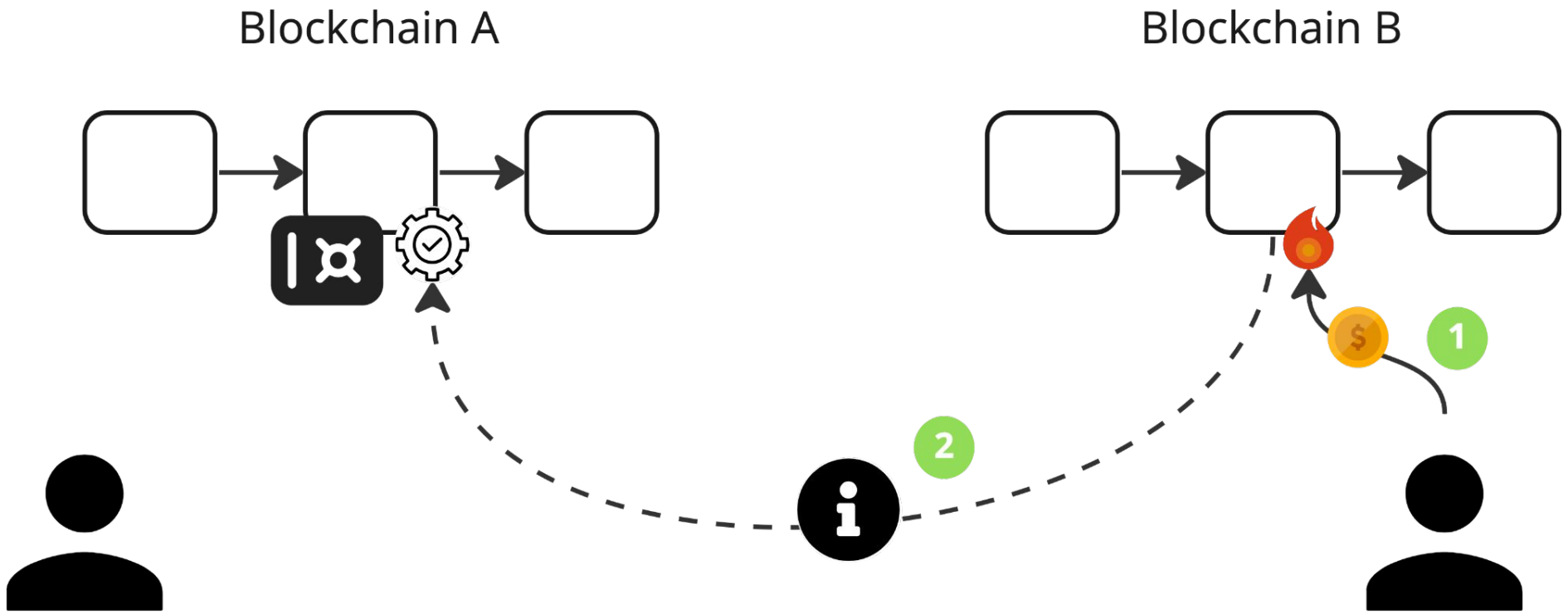

Blockchain A
Blockchain B
1

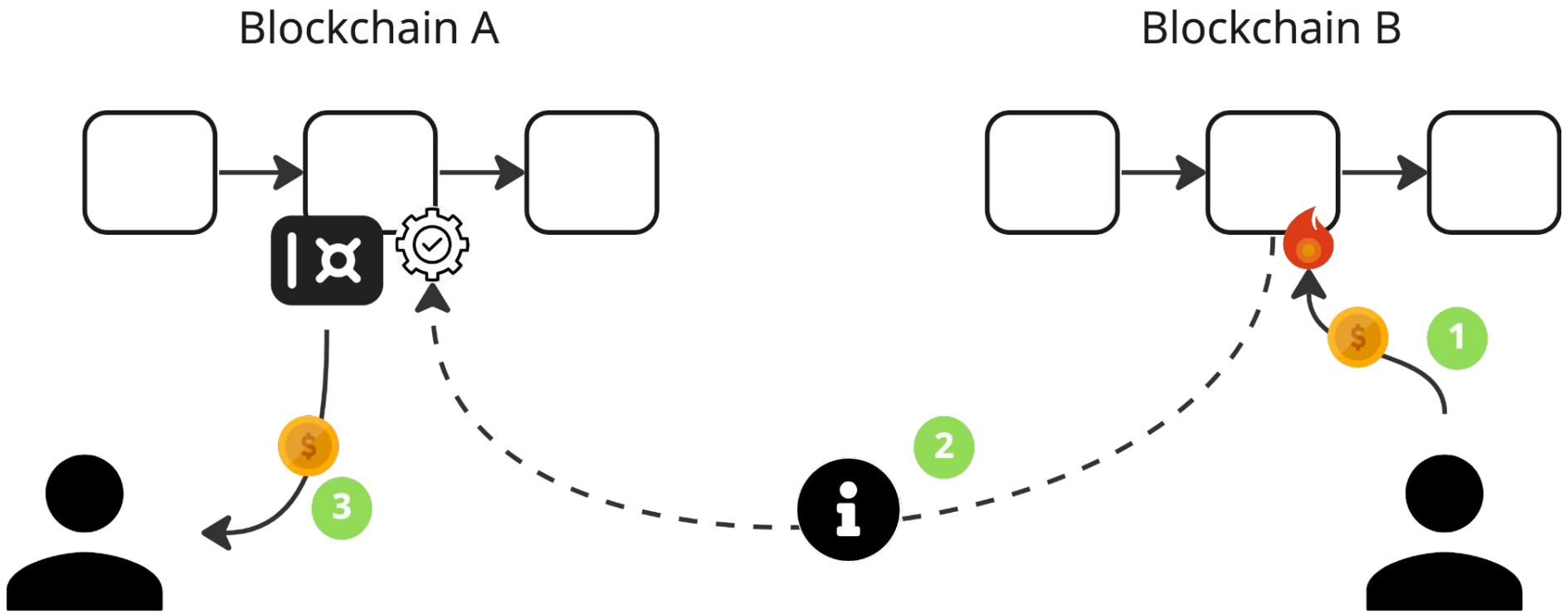

Blockchain A
Blockchain B
1
2


Blockchain A
Blockchain B
1
2
3


Blockchain A
Blockchain B


Blockchain A
Blockchain B
1

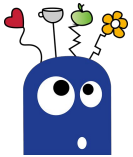

Blockchain A
Blockchain B
1
2


Blockchain A
Blockchain B
1
2
3

Bridge Designs

The Ideal 2-Way peg

- Secure
- Trustless
- Decentralized
- Censorship resistant
- Capital Efficient
- Fast and autonomous

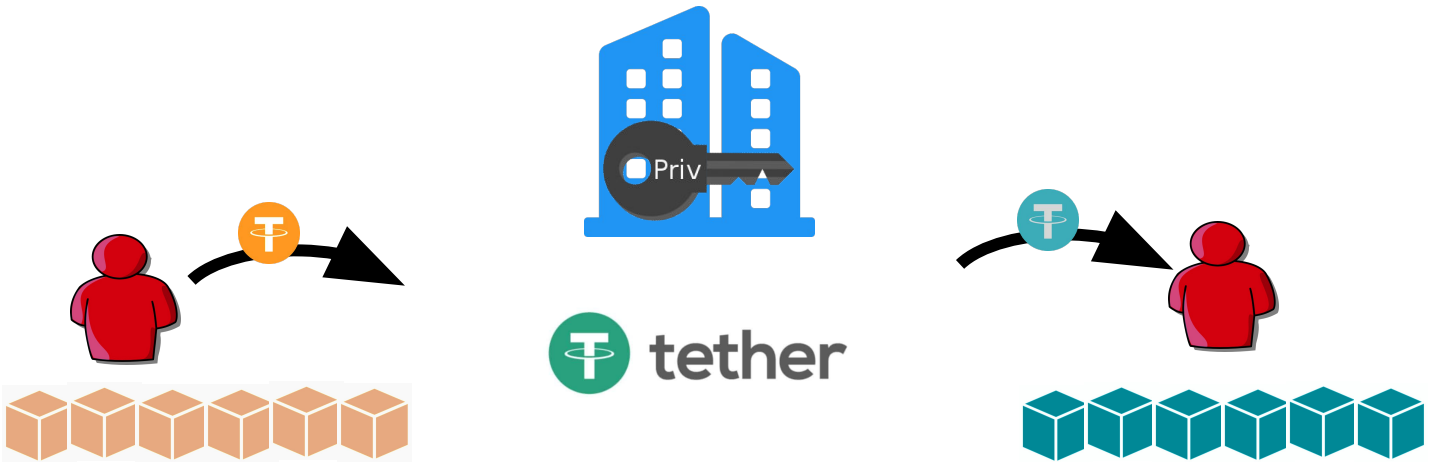


Single authority Bridge

Properties

- Security depends on single party
- Centralized
- Single point of failure

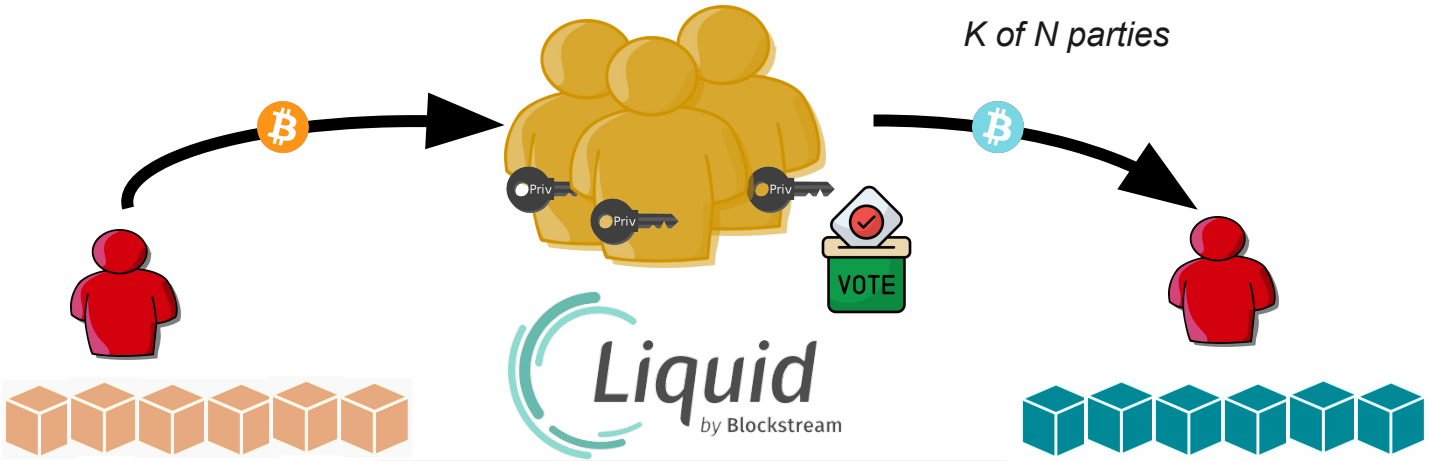
Single authority Bridge



Properties

- \- Slow
- \- KYC required
- \- Censorship
- \+ Circuit breakers
- \+ Rate limiters
- \+ Behavioral alerts

Multi-authority Bridge

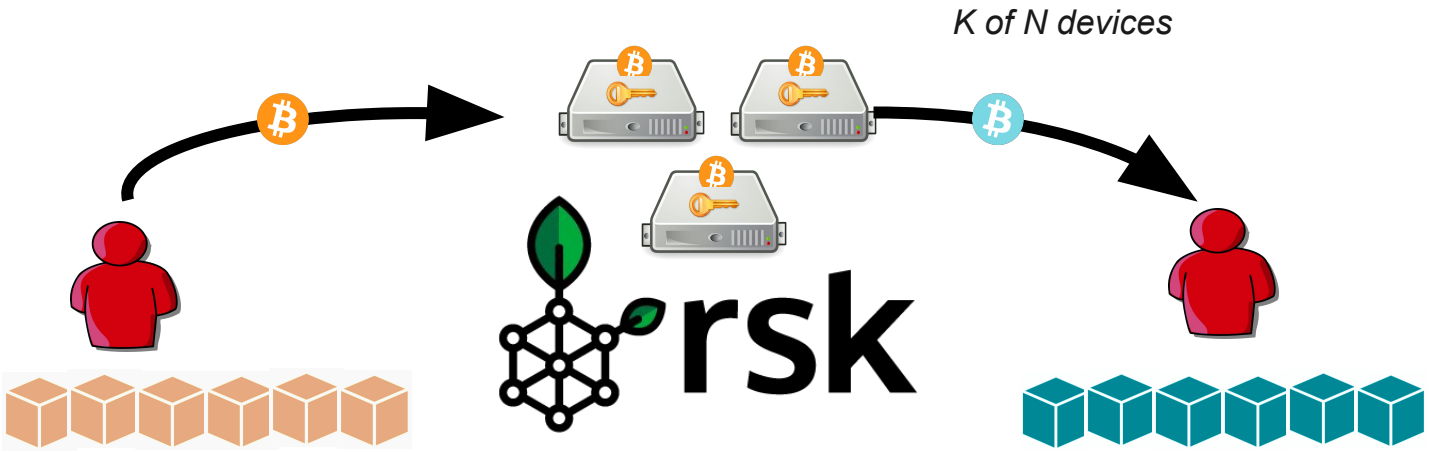


Properties

\+ More secure, Censorship resistant
\+ More Decentralized, No single point of failure

\- Not permissionless

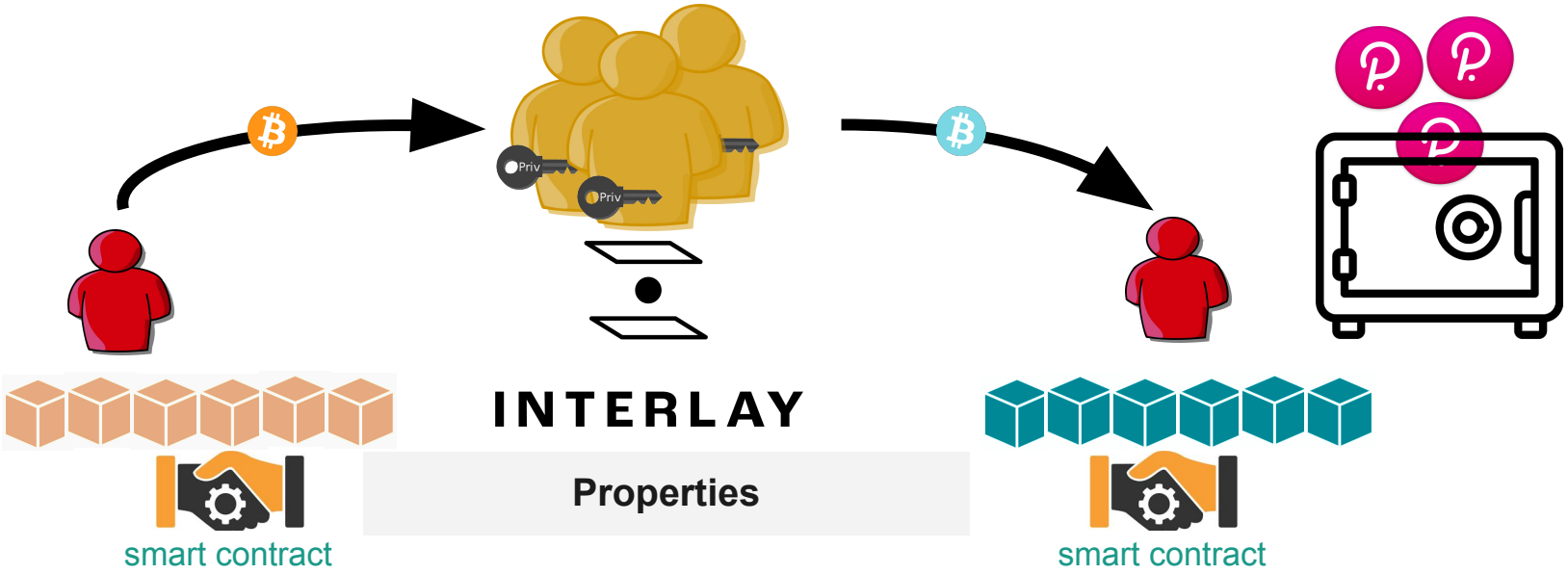
Powpeg Bridge (simplified)



Properties

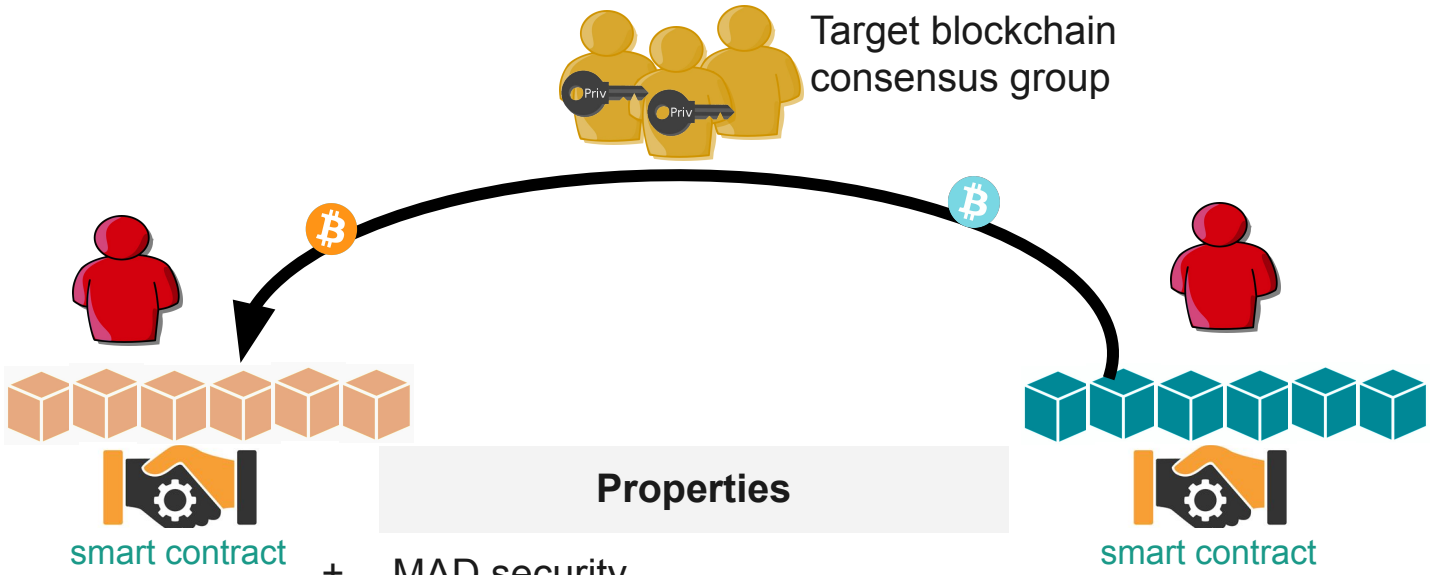
\+ Even more secure
\+ SPV consensus enforced by PowHSMs
\- Less open

Collateralized Bridge



\+ Fully decentralized
\- Capital inefficient

Drivechain Bridge

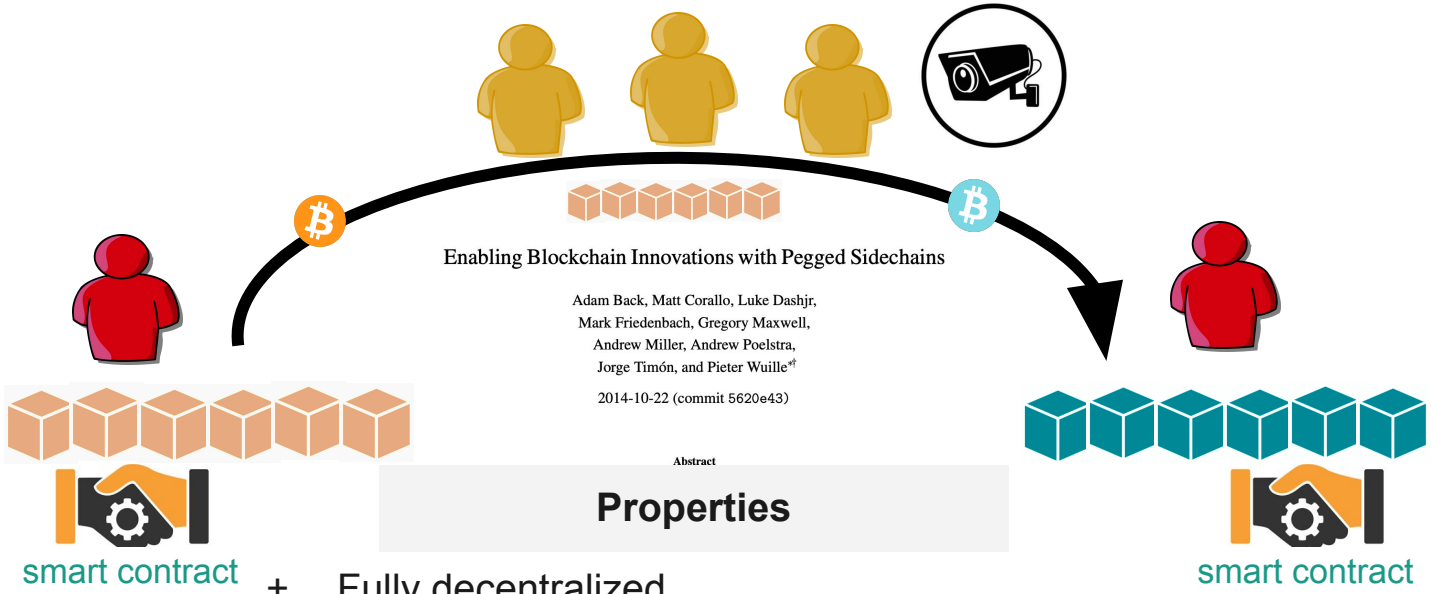


Properties

\+ MAD security
\+ Much simpler than consensus bridge

\- Explicit honest majority
\- Requires watchtowers and social contracts
\- Very slow

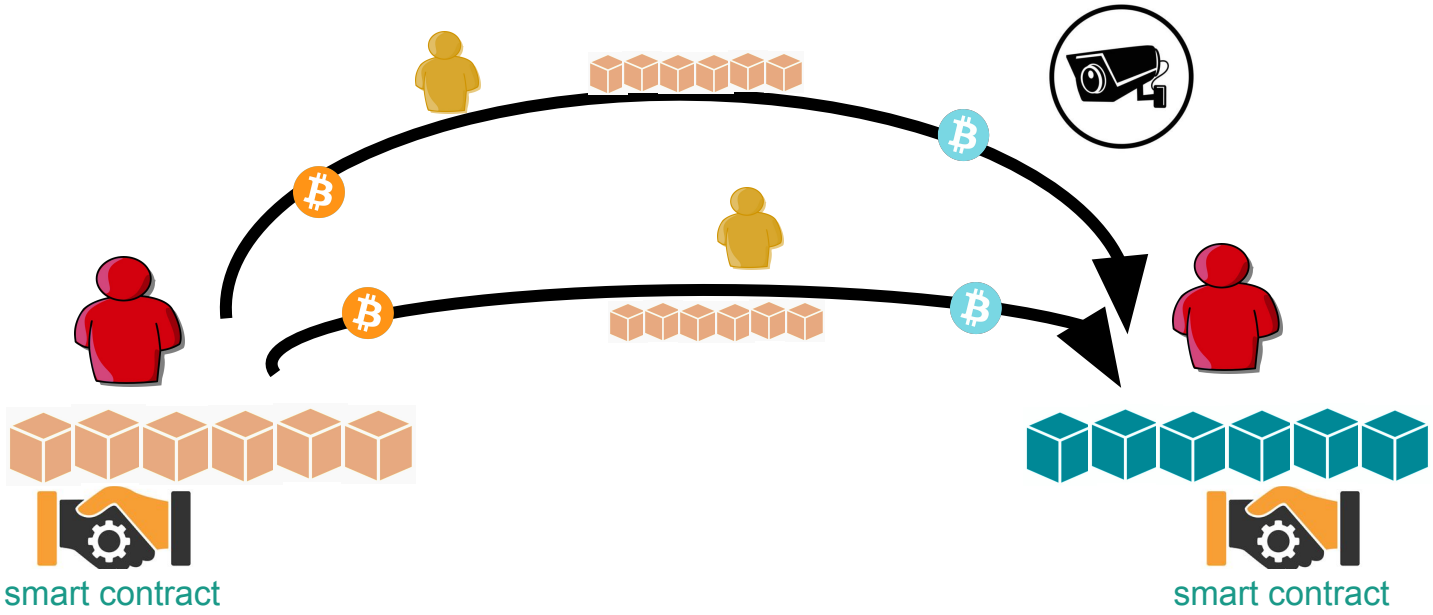
Optimistic SPV-Validating Bridge



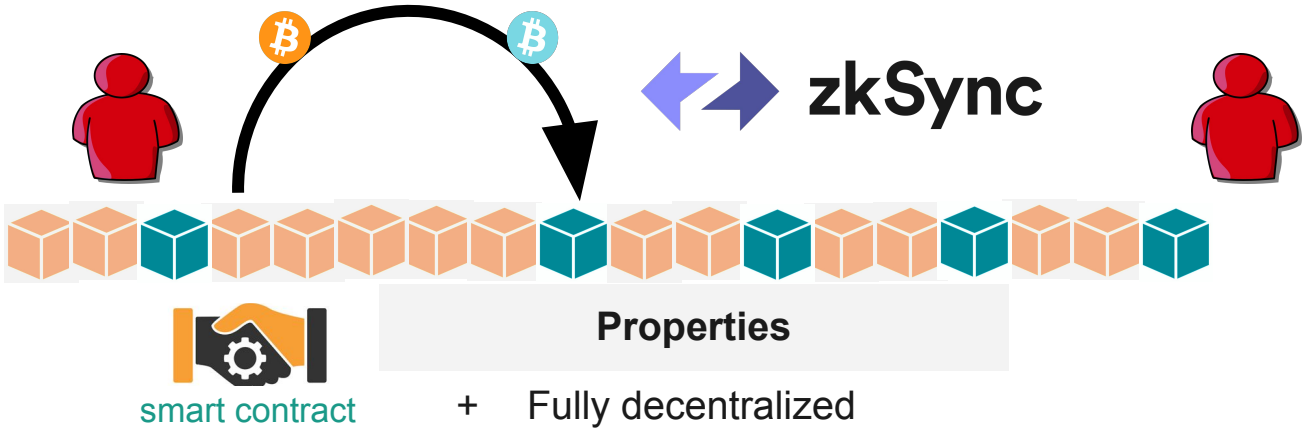
Properties

\+ Fully decentralized
\+ Capital efficient
\- Requires uncensorable transactions → implicit honest majority
\- Requires watchtowers (choose honest fork)
\- Requires new opcode `OP_SIDECHAINPROOFVERIFY`

Optimistic SPV-Validating Bridge



Rollup Validating Bridge



Properties

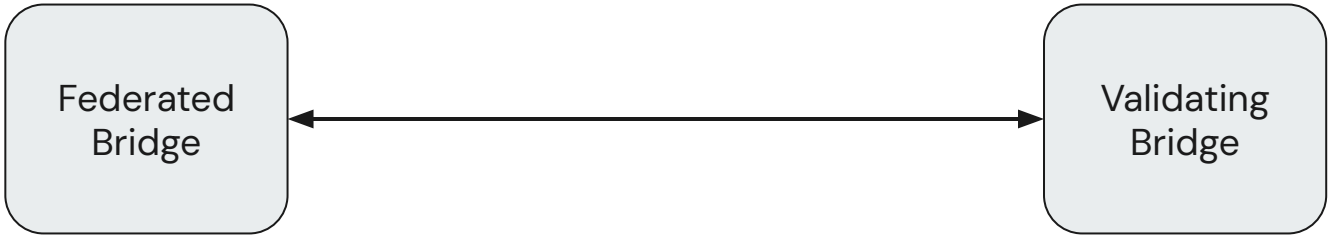
\+ Fully decentralized
\+ Linked consensus chooses honest fork automatically
\- Only works for linked consensus

Federated vs BitVM vs Validating Bridges

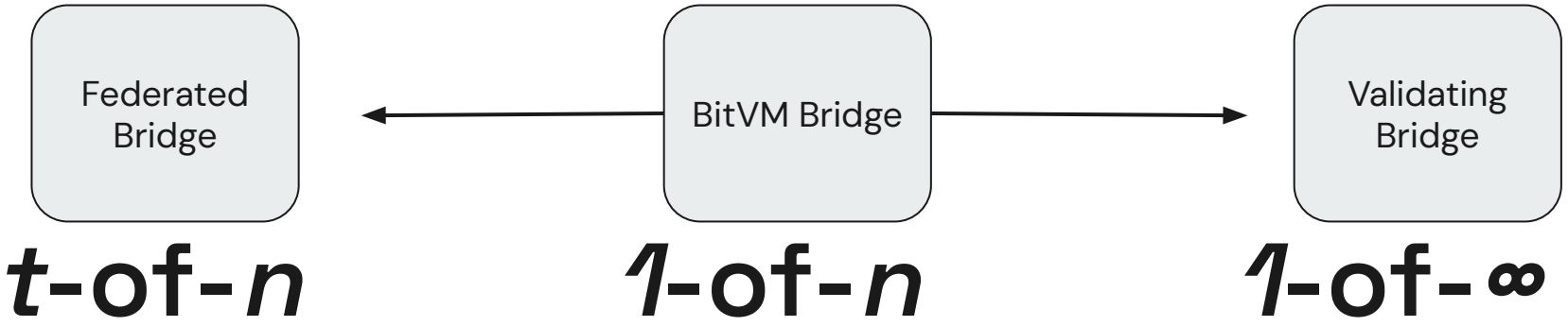
Federated Model (t-of-n)

All federated bridges are based on the *t*-of-*n* security model. It assumes *t* members of a security committee of N are honest, to protect the funds. Normally *t* is the majority.
Committee cannot by permissionless: anonymous newcomers dilute the security using a Sybil attack.

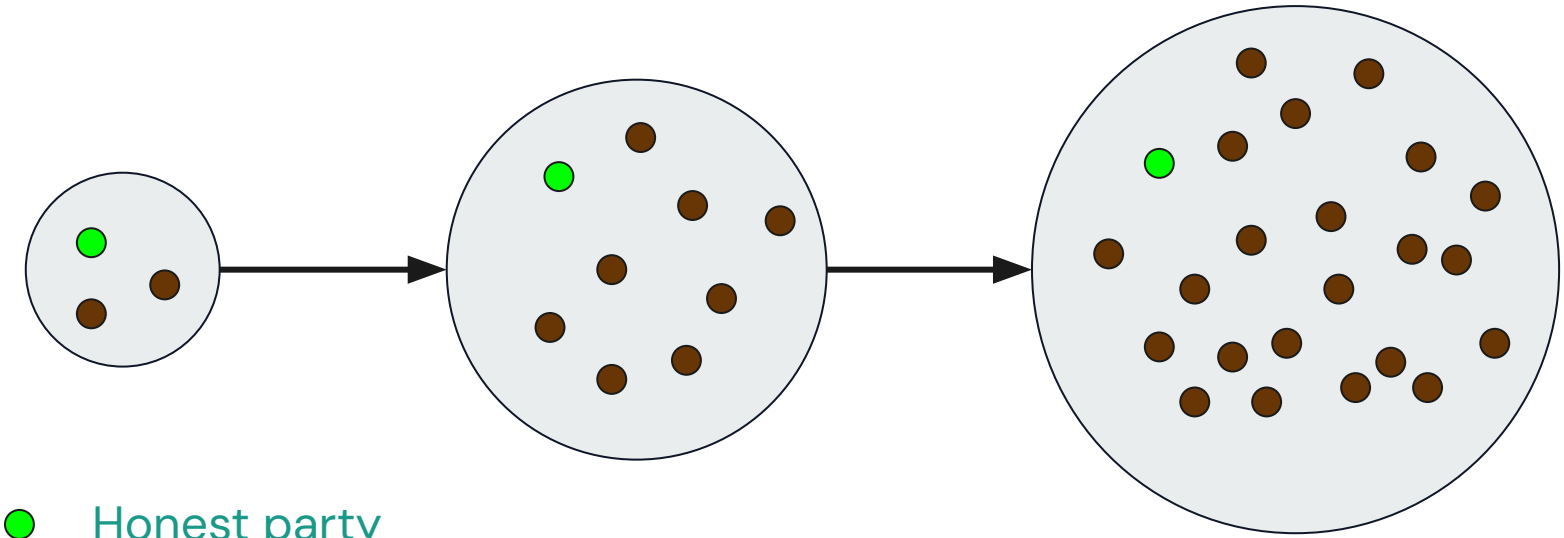
From *t*-of-*n* to *1*-of-∞



New *1*-of-*n* honesty assumption

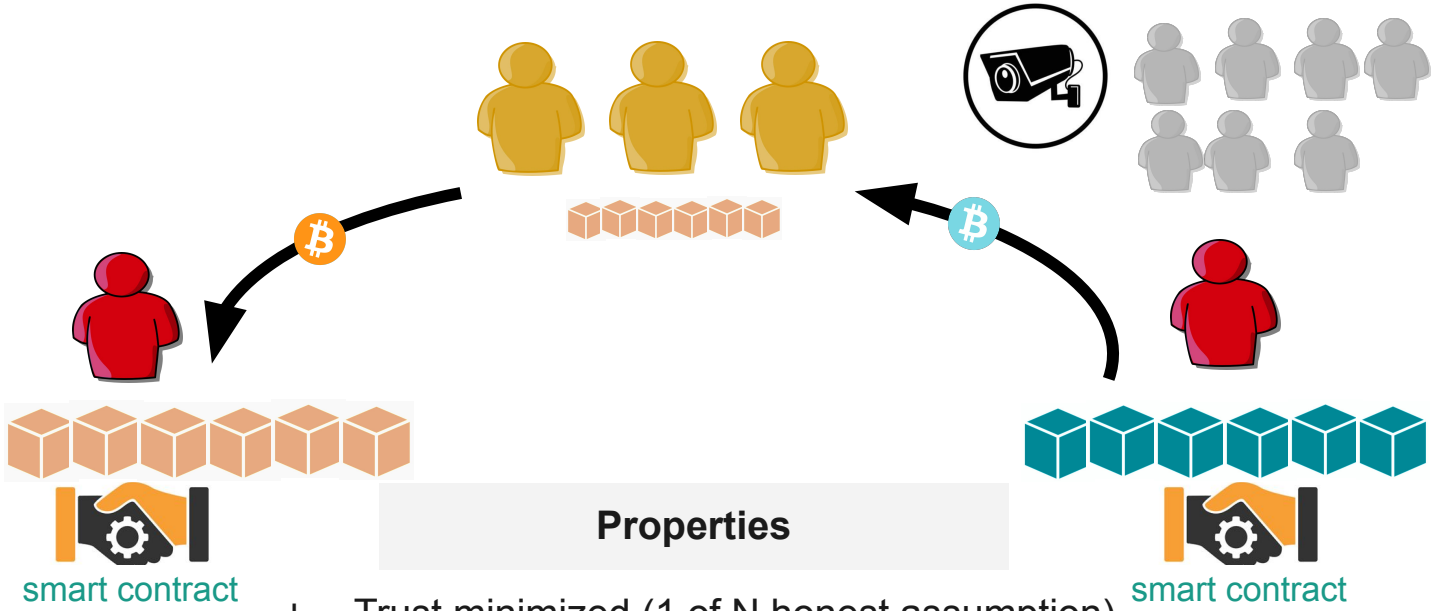


Openness Without Security Dilution



- Honest party
- Party of unknown behaviour

BitVM2 Optimistic Bridge (permissionless watchtowers)



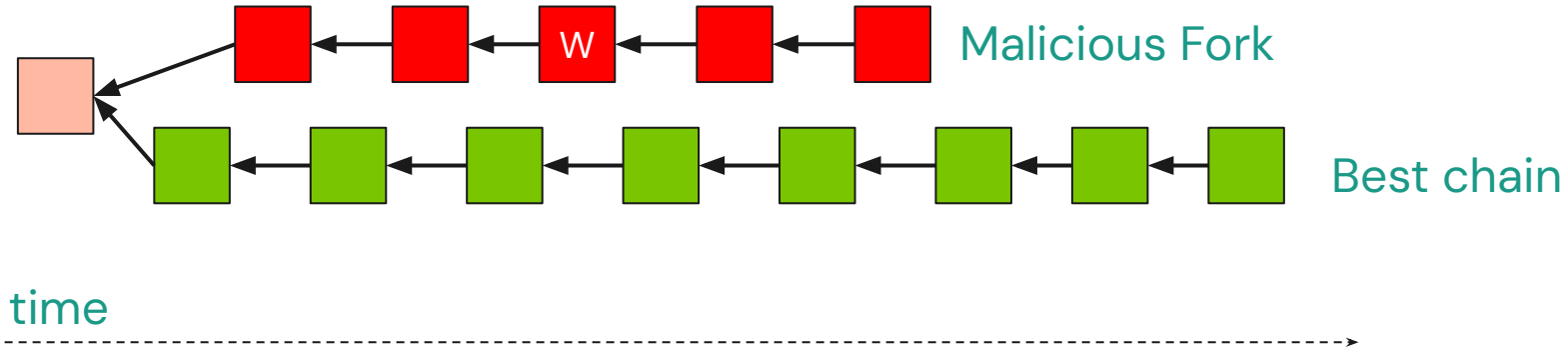
Properties

\+ Trust minimized (1 of N honest assumption)
\- Capital inefficient (requires fronting funds)
\- Watchtowers must pay high disputes fess
\- Operators lock high security bonds
\- **Insecure due to non-contestable proofs**

Contestable vs Non-contestable Bridges

Validating Bridges (Insight 1)

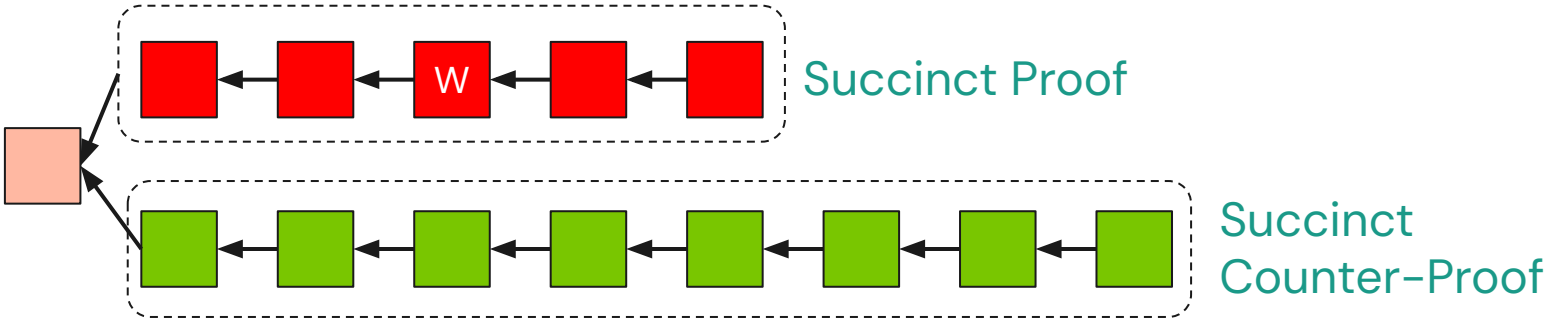
A secure bridge needs to be an interactive system



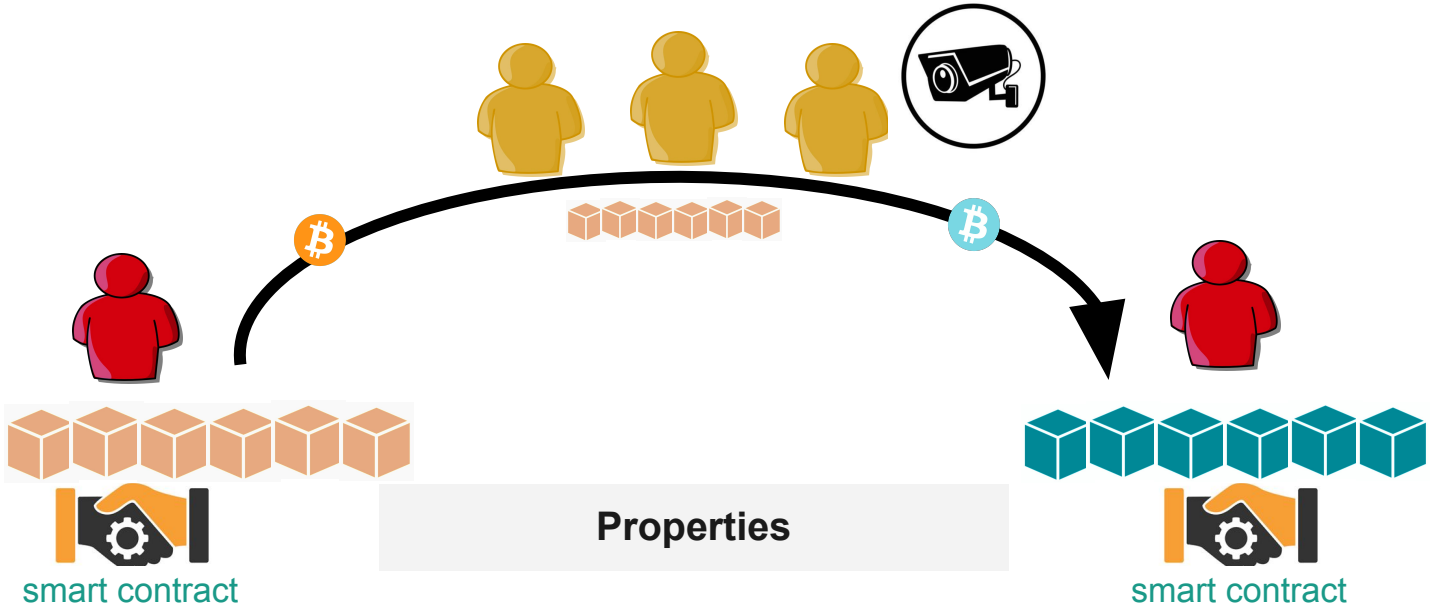
Validating Bridges (Insight 2)

An efficient bridge compresses interactions, so it needs to be a fraud proof system (also called Contestable system)

→ The succinct proof is generally a SNARK.
→ The resulting system has a 1-of-∞ honesty requirement.



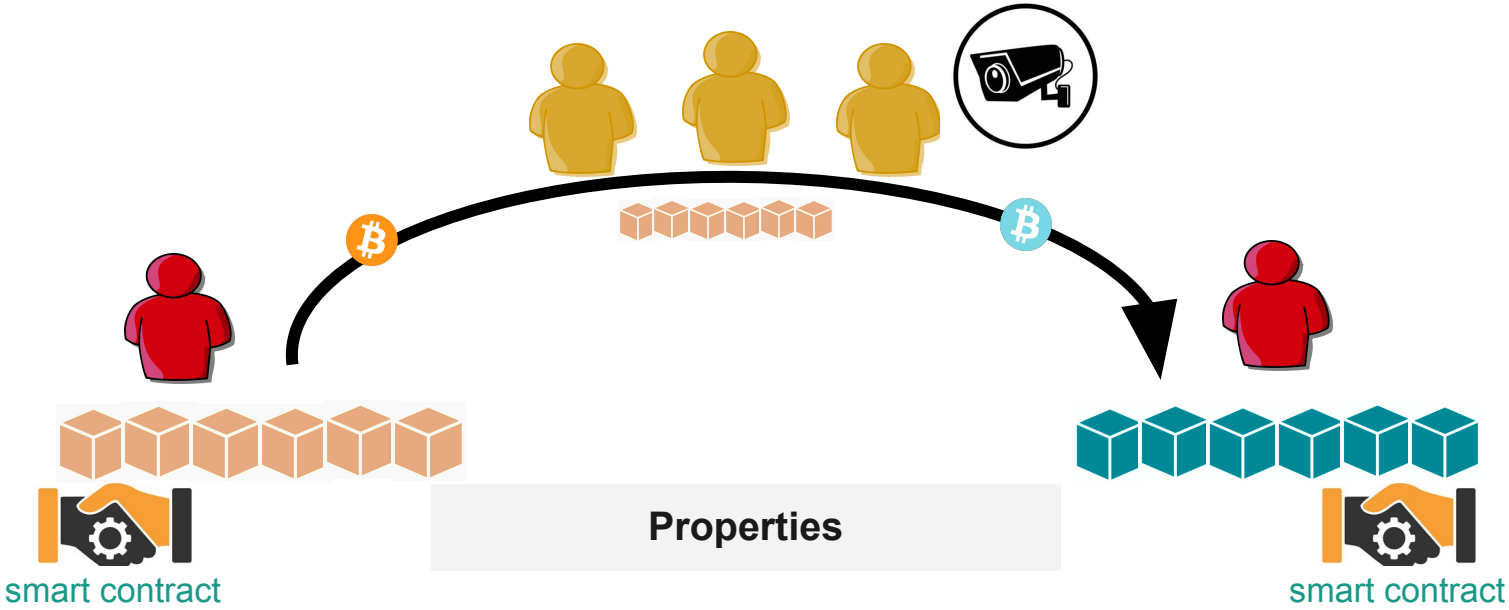
Cardinal/TOOP/BitVMX Contestable Optimistic Bridge



Properties

+ Trust minimized (1 of N honest assumption)
+ Capital efficient with TOOP (no fronting)
+ Low dispute costs (BitVMX CPU)
+ Open committee

BATTLE Optimistic Bridge



Properties

\+ Trust minimized (1 of N honest assumption)
\+ No persistent security bonds (FLEX and Garbled Circuits Based)
\+ Open and very large committees (1000 operators)

\- Requires fronting funds if an operator is offline

Other BitVM-based Bridge Designs

1. Rootstock's Union (BitVMX CPU-based, contestable)
2. Alpen Labs's Strata (Contestable, Glock-based)
3. Citrea's Clementine (currently BitVM2. v2: Contestable, BitVM3s and TOOP-Based)
4. Babylon (Still undecided. Maybe BitVM3s-based)
5. Bitlayer (BitVM2-based)

Summary

- Bitcoin Bridge landscape is evolving fast
- BitVM in 2023 was a theoretical game-changer
- BitVM2 Bridge was a theoretical breakthrough but a practical failure
- Secure Bitcoin bridges must be contestable, which currently implies having a temporarily closed committee of watchtowers
- Fairgate's BitVMX is the BitVM that works. It's cheap, robust and flexible
- Fairgate's TOOP eliminated the need to front funds, improving capital efficiency
- Fairgate's BATTLE enabled thousands of watchtowers
- Fairgate's FLEX enabled on-demand security bonds
- Fairgate's Garbled Circuits (upcoming) will fill the missing piece in the Bitcoin Bridge Stack.

Thank You!

https://github.com/FairgateLabs

BitVMX

https://bitvmx.org