Lecture 19: Bridges

https://web3.princeton.edu/principles-of-blockchains/

Professor Pramod Viswanath
Princeton University

This lecture:
Moving assets across chains
Boosting the trust across chains

Interoperability

- Each blockchain is isolated
  - Separate community (miners, users, stakers)
  - Separate token (medium of commerce)

- Similar to different countries
  - Separate currencies
  - Geographical boundaries
  - Distinct methods of protecting commerce/boundaries (“security”)

- Trade between countries a major source of ”scaling” of the human condition
  - GDP
  - Population size

Interoperability Infrastructure

- Inter-country trade needs:
  - Physical mechanisms (shipping routes, airlines): ”container” revolution
  - Security mechanisms (bridging the trust barrier across countries): who is responsible “during transit”

- Financial interoperability
  - Trade one currency to another
  - SWIFT
  - Bank of International Settlements
  - Intertwined physical mechanisms and security – centralization helps

Interoperability in blockchains

- Canonical use case: move assets from one blockchain to another
  - Example: move BTC from Bitcoin blockchain to ETH in Ethereum
  - BTC is “store of value” (gold) while ETH is a medium of capitalism (borrow/lending)

- Questions:
  - What is the infrastructure (e.g., network, counterparty)?
  - How is the security of assets managed during transfer?

What Can Go Wrong?

- Securely transfer assets across chains
  - Hold BTC in “**escrow**” while ETH is deposited
- Insecurity in one chain can creep into the other
  - 2008 financial crisis was largely US-based but spread around the world

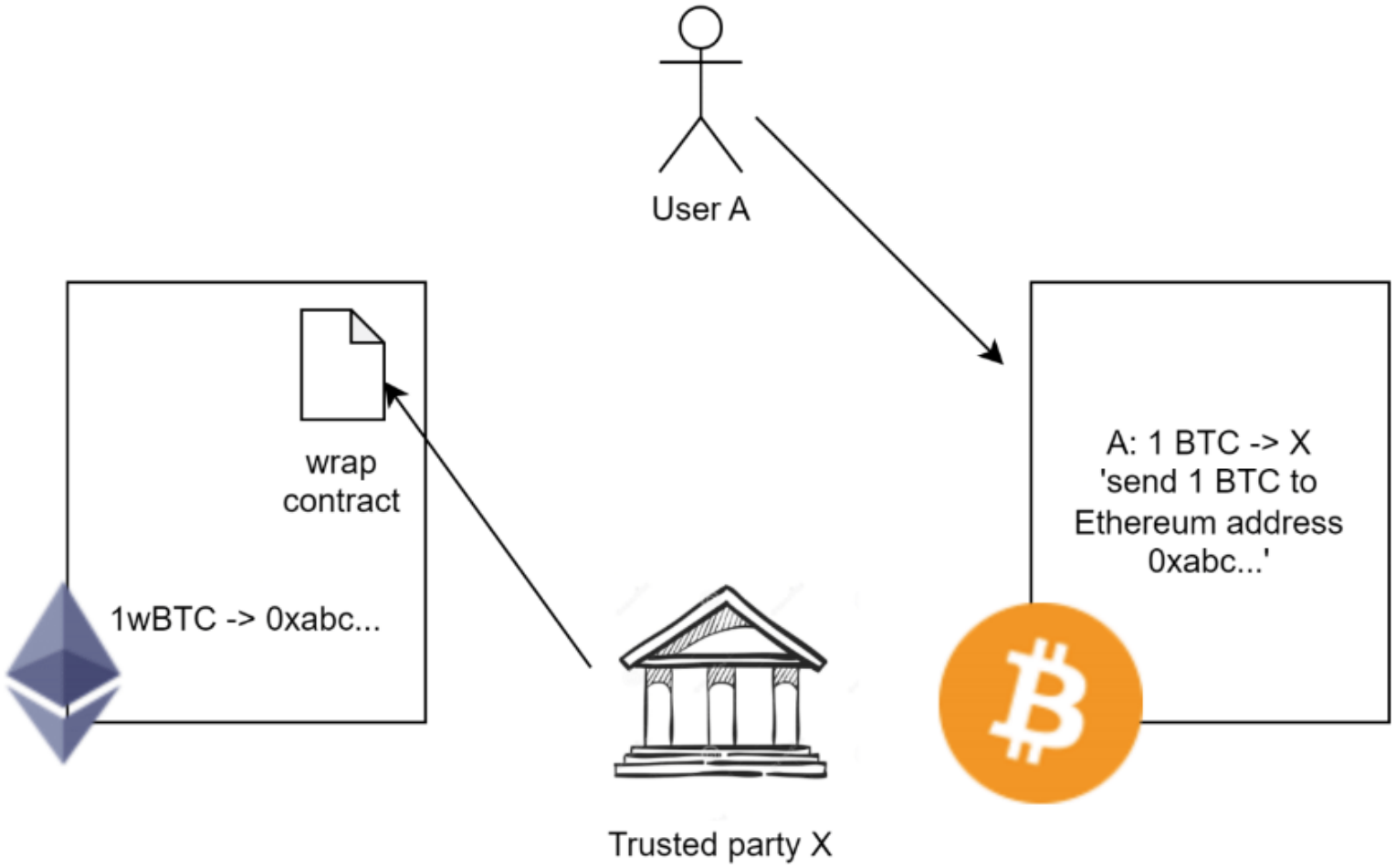
Trusted Parties

- Exchanges like Binance and CoinBase
- Only support swaps
  - More general goal: “import state of one blockchain into the other”
- High source of trust
  - We saw what happened with FTX

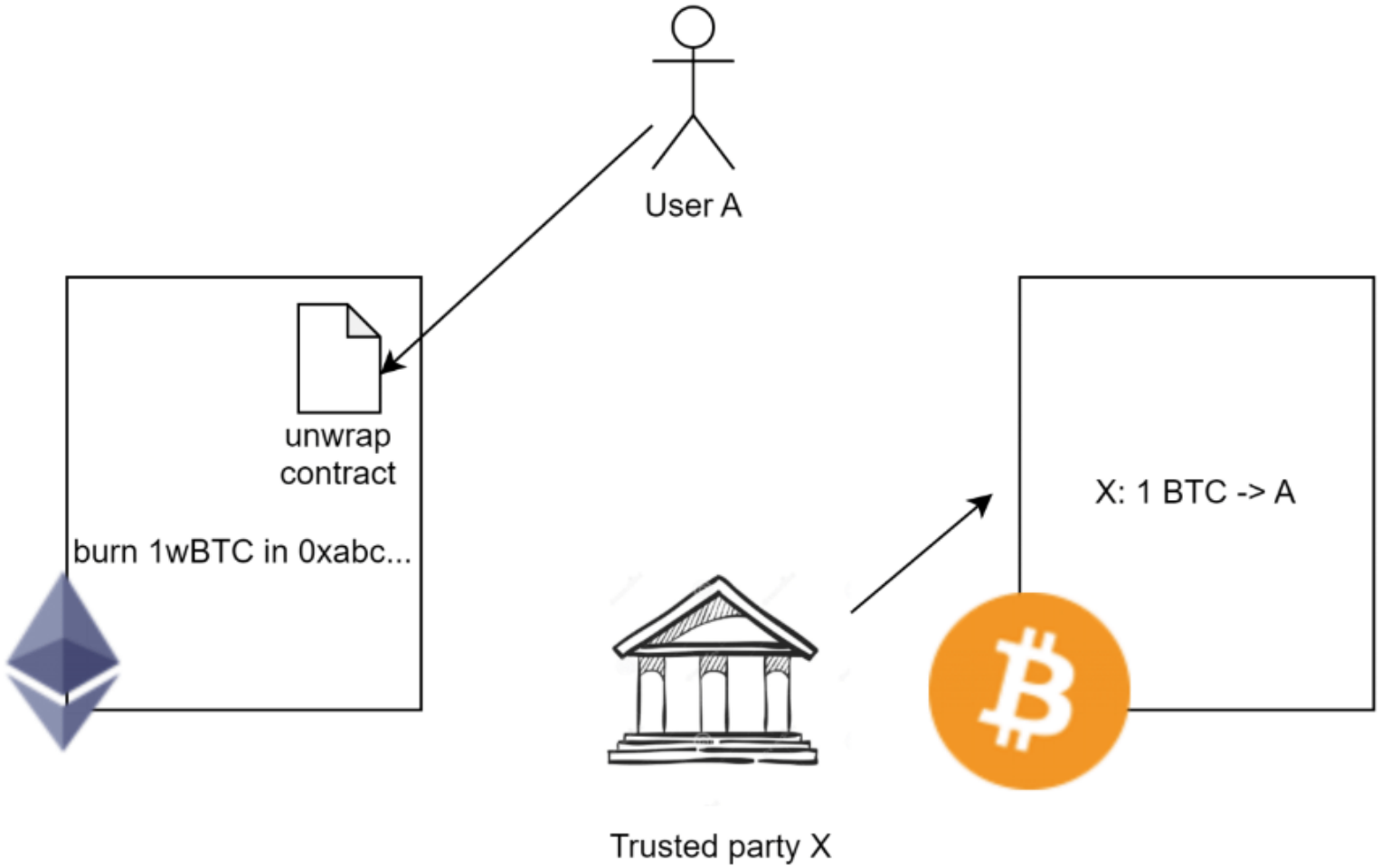
Wrapped Bitcoin

- Move BTC from Bitcoin blockchain to Ethereum blockchain
- **Lock** BTC on Bitcoin and get equivalent amount of **WBTC** on Ethereum (1 to 1)
- Trust the entity that holds the BTC Locked BTC is on-chain in Bitcoin so everyone (both Bitcoin and Ethereum users) can see it
  - Trust the entity with locked BTC that they do not move it
- WBTC is a new token in the Ethereum blockchain (tracks value of BTC)

WBTC


User A
wrap
contract
1wBTC -> 0xabc...
A: 1 BTC -> X
'send 1 BTC to
Ethereum address
0xabc...'
Trusted party X

WBTC


User A
unwrap
contract
burn 1wBTC in 0xabc...
X: 1 BTC -> A
Trusted party X

More Decentralized Solutions

- External layer of trust
  - Committee of validators
  - Blockchain
- Atomic swaps
  - HTLC

External Layer of Trust

- Another blockchain or committee of validators coordinate the swap
- High extensibility but weak trust assumptions
- Example: Thorchain
  - Liquidity pools are needed for every supported currency
  - They have a separate chain to coordinate and execute the swaps

Hash TimeLock Contract (HTLC)

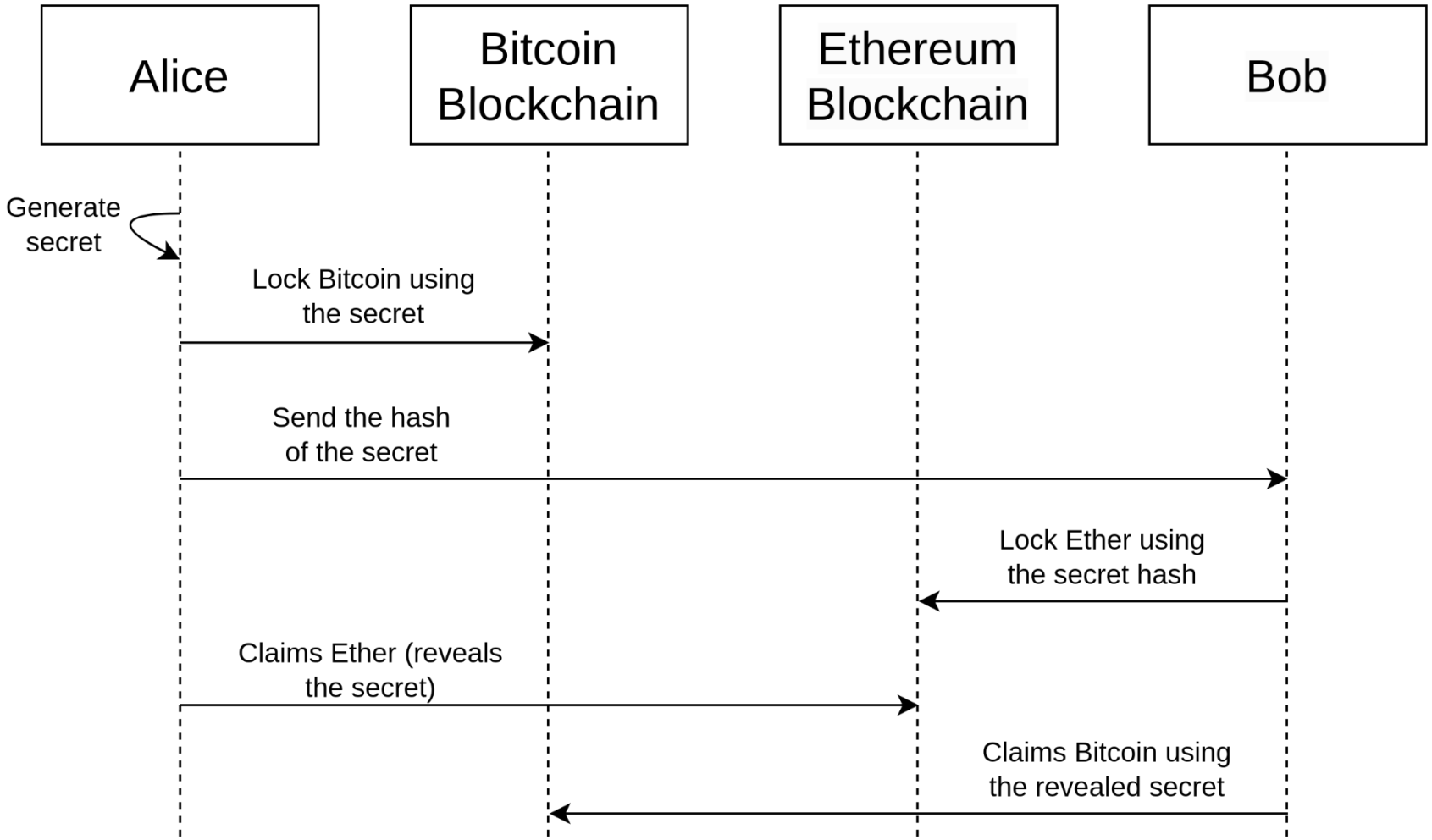
- **Hashlock key**
  - Restrict spending an output until some specific data is provided by the recipient.
  - The recipient can spend the output by providing that data and a valid signature in a predetermined time limit.

- **Timelock key**
  - If the proof is not submitted within a time limit, the coins are returned to the original owner.
  - In other words, the owner can spend the output by providing a valid signature after the time limit is passed.

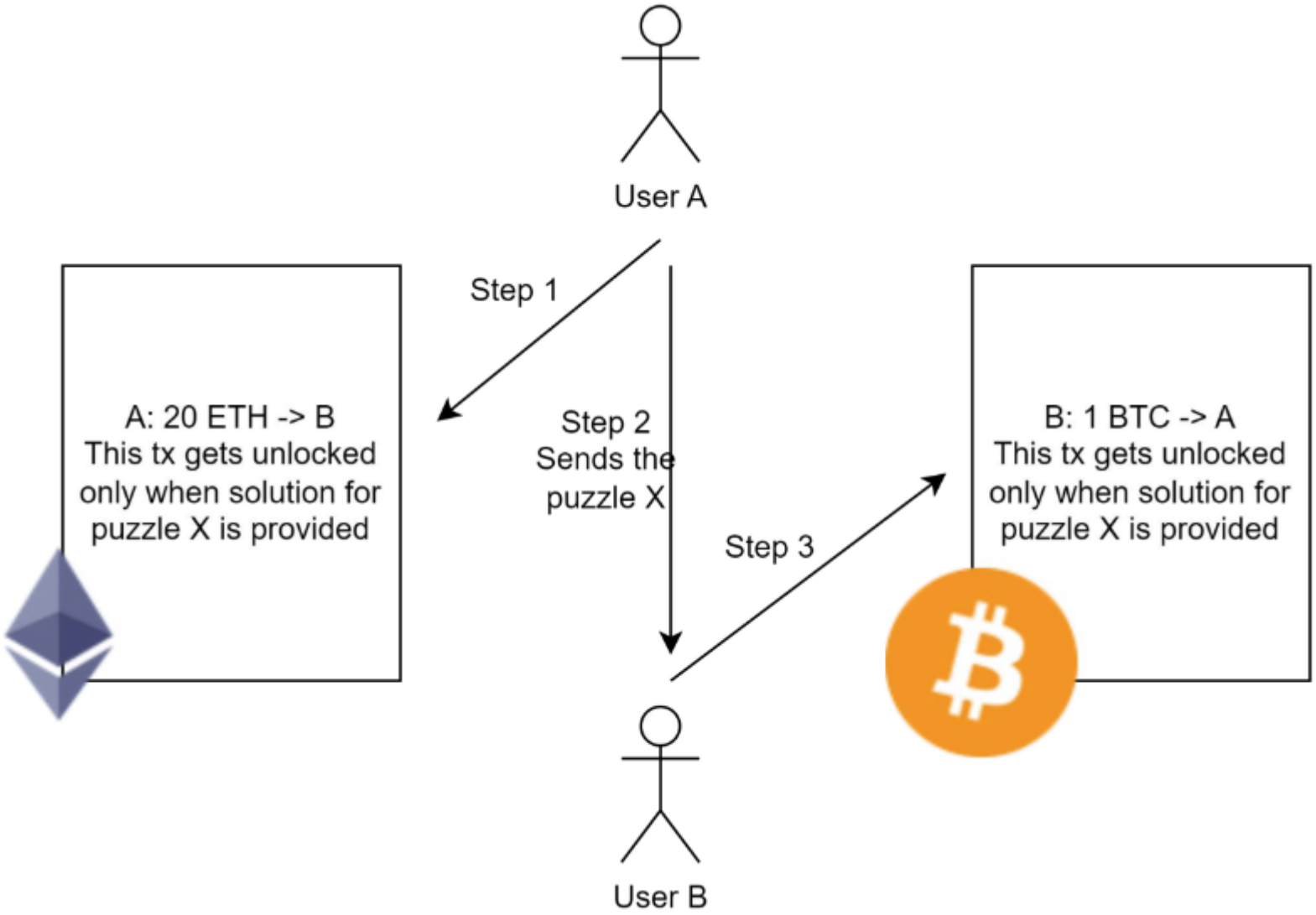
Atomic Swap

- Alice wants to pay 1 BTC and get 15 ETH, Bob has 15 ETH and wants to sell it for 1 BTC. They can perform an atomic swap.
- Atomic swap uses Hash TimeLock Contract (HTLC).
- Need a counterparty for every swap; hard to create a market.

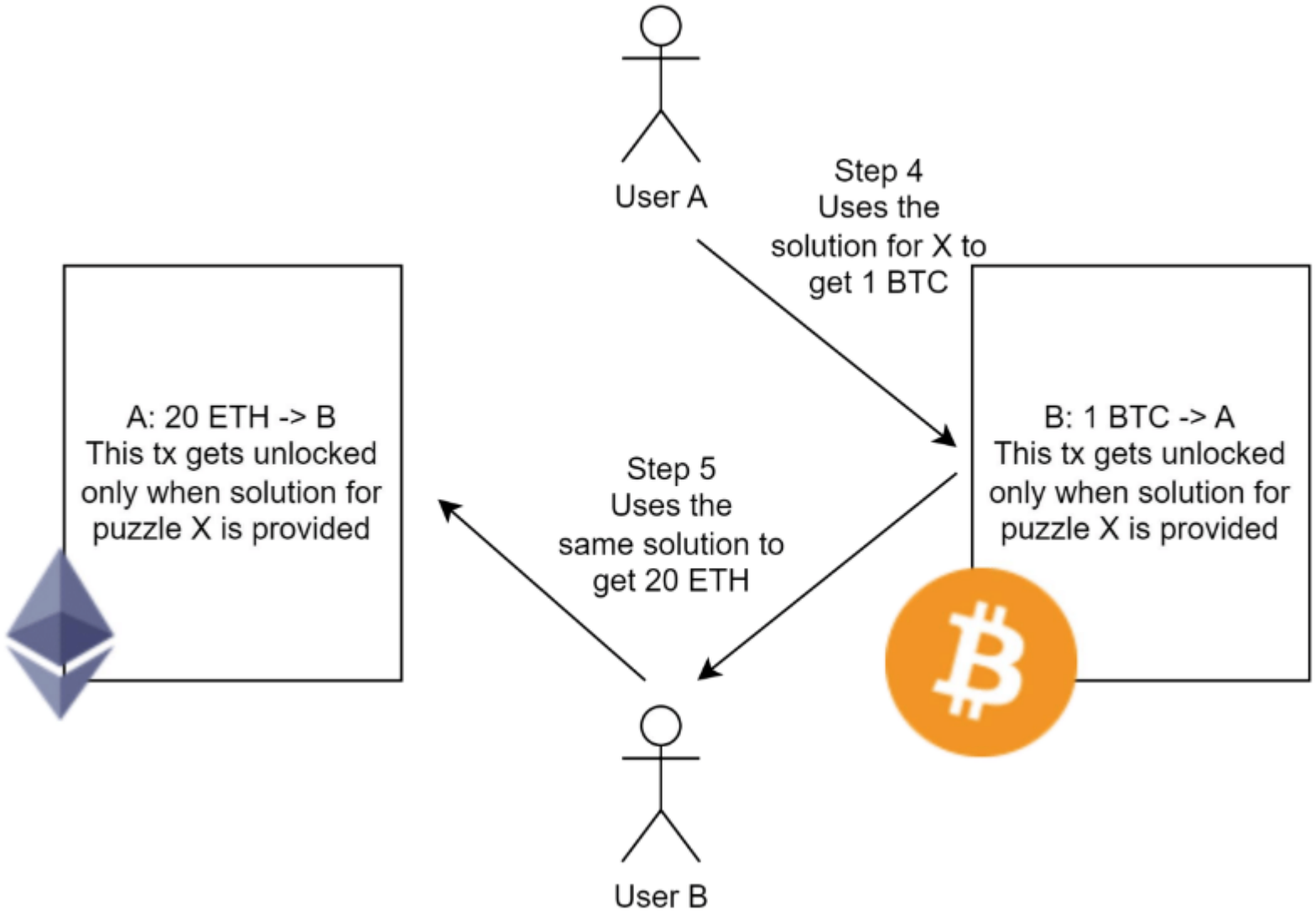
Atomic Swap (Overview)



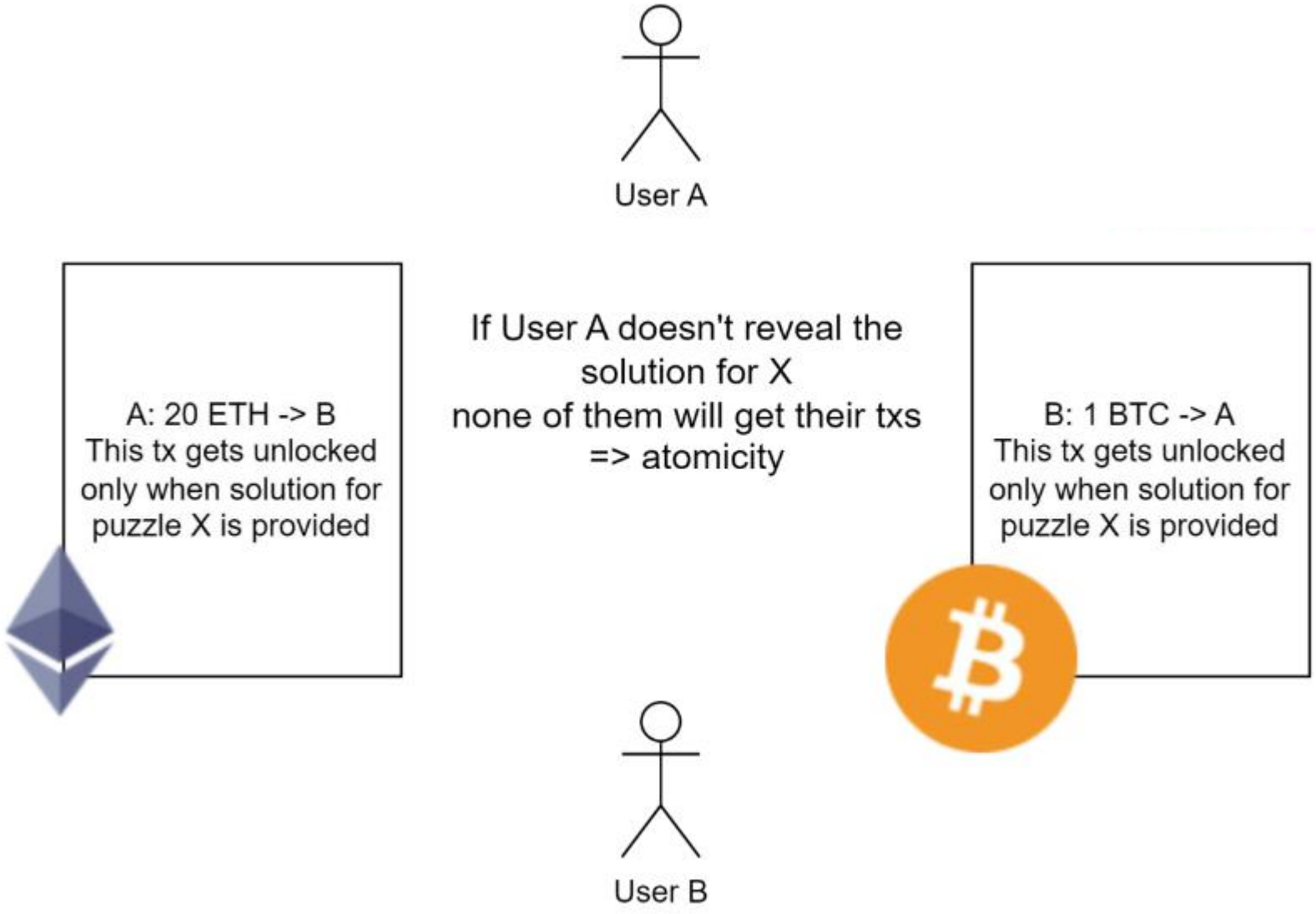
Atomic Swap


User A
Step 1
A: 20 ETH -> B
This tx gets unlocked only when solution for puzzle X is provided
Step 2
Sends the puzzle X
Step 3
B: 1 BTC -> A
This tx gets unlocked only when solution for puzzle X is provided
User B

Atomic Swap (Commit)

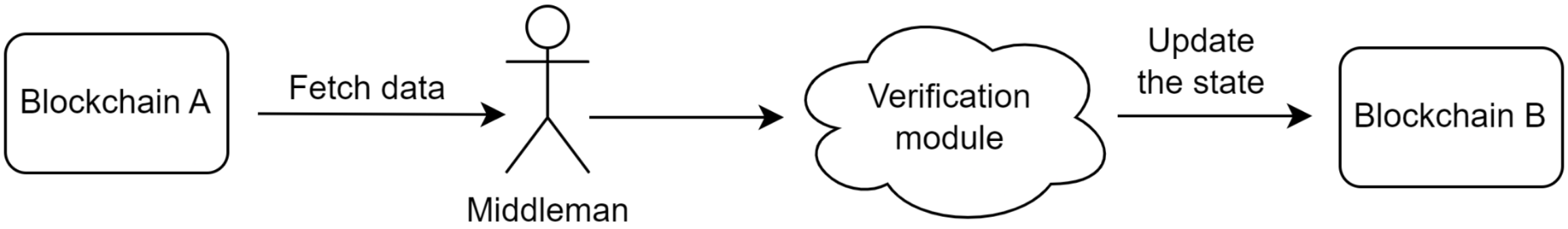


Atomic Swap (Abort)



Messaging Protocols

- Headers include the Merkle root of all transactions
- Moving headers to other blockchains is enough
- Verification module can be on-chain or off-chain



Trustless and Trusted Bridges

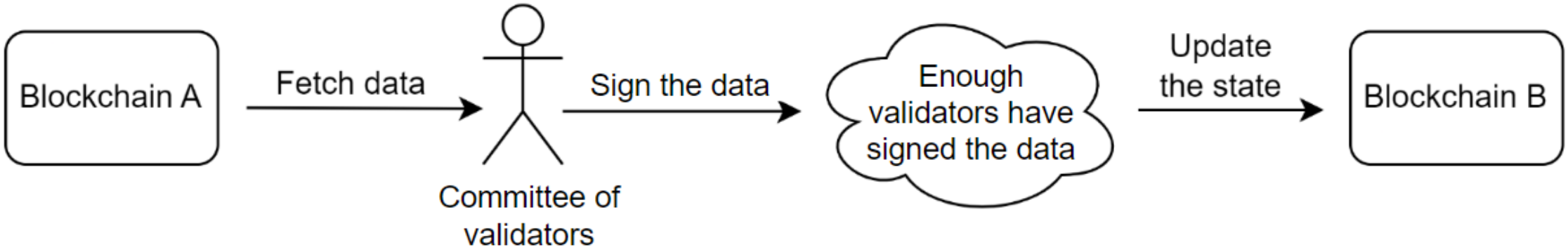
- **Trusted**: validator-based bridges
  - Validators move the data from one blockchain to another
  - Off-chain verification module
  - Trust to committee of validators for the verification module

- **Trustless**: light client and zero-knowledge bridges
  - Relayer nodes move the data from one blockchain to another
  - On-chain verification module
  - Hard to scale for many blockchains

Some solutions go in between these two ends; like Axelar that uses PoS for the committee of validators to get stronger trust assumptions.

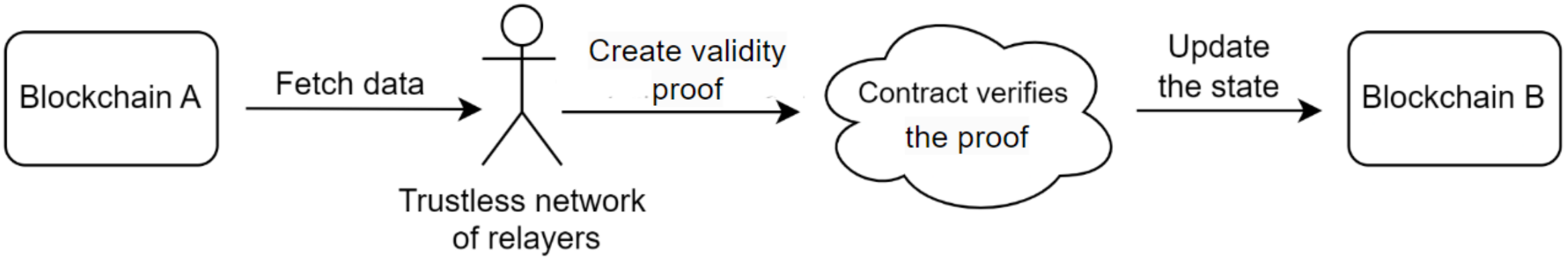
Validator-based Bridges

- Use Multisig or Threshold Signature Scheme (TSS)
- Not safe in practice - many attacks
- High extensibility



Light Client and ZK Bridges

- Strongest trust assumptions



Light Client Bridges

- How to get access to a blockchain's data from another blockchain?
- Need to run a full node on the destination blockchain
  - Too expensive
- Use a light client implementation instead
- Access to all transactions and data of the source blockchain on the destination blockchain

Bitcoin Light Client Bridge (Overview)

- A Bitcoin light client implemented on another blockchain (e.g. Ethereum) can verify any data that gets included on the Bitcoin blockchain.
- Destination blockchain needs to be programmable.
- The light client program checks the validity of the Bitcoin data provided for it.

Bitcoin Light Client Bridge

- The light client only maintains the block headers of Bitcoin blockchain
- Headers get verified by the on-chain light client program
  - PoW check
  - Parent hash link check
  - Difficulty retargeting algorithm
- Longest chain and k-deep confirmation rules are executed
  - Different dApps on top of the bridge can use different k for their confirmation rule

Bitcoin Light Client Bridge (Relayer)

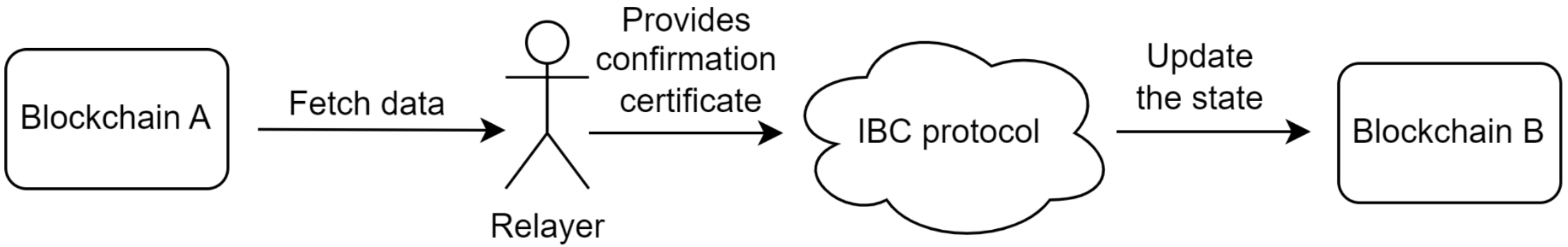
- Relayer nodes move the headers from the Bitcoin blockchain to a destination blockchain
- No need to trust the relayers - only liveness
- If relayers provide invalid data, the light client program will reject it on the destination blockchain

Bitcoin Light Client Bridge

- Use Simple Payment Verification (SPV) for verifying the inclusion of transactions against the stored headers
- Relayers also provide Merkle proofs of inclusion for the transactions included on Bitcoin and submit them on the destination chain

Interoperable Blockchain Ecosystems

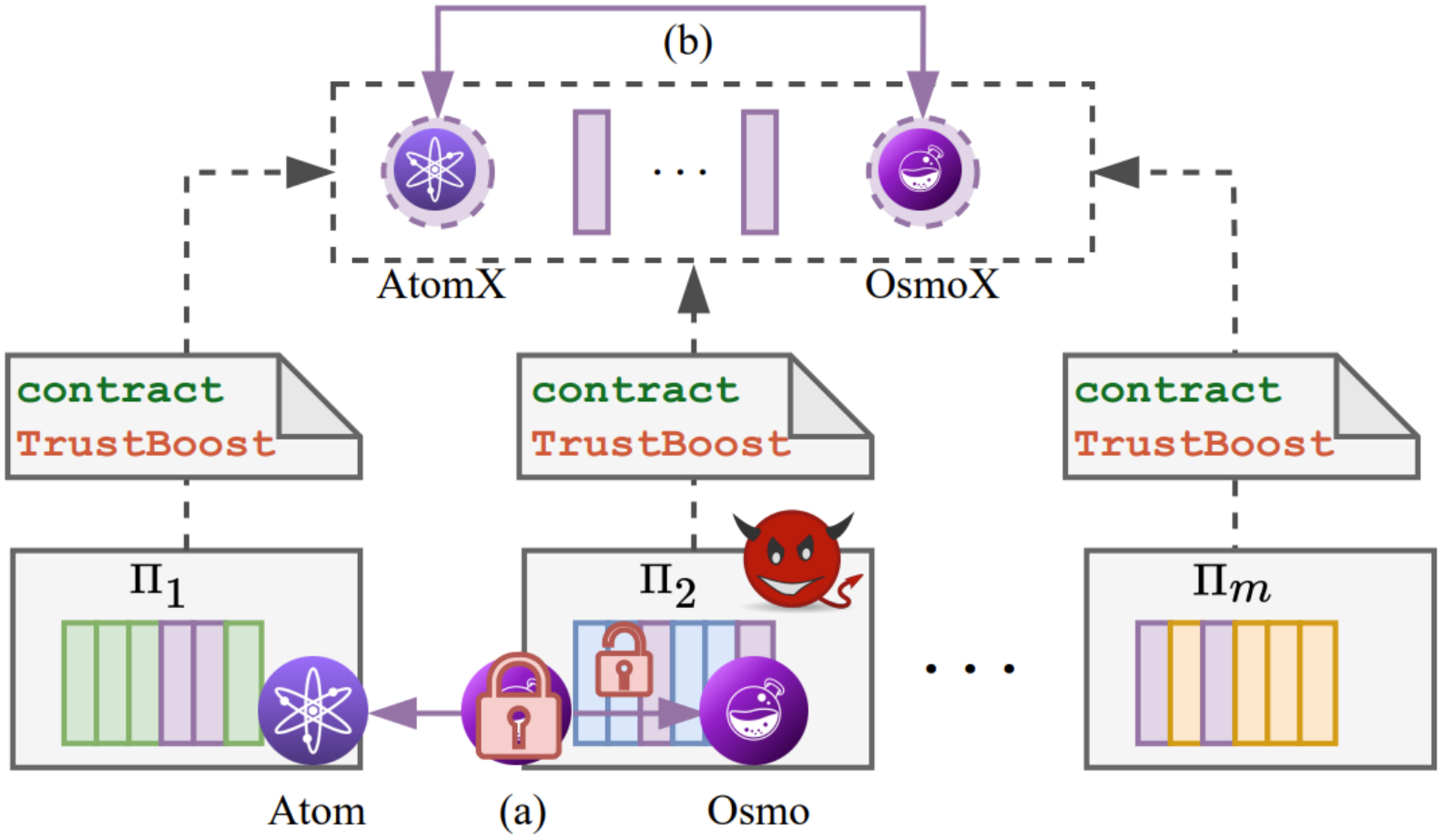
- Inter-Blockchain Communication (IBC) protocol
  - IBC protocol is a part of Cosmos consensus mechanism
  - The validators of the destination chain verify the validity of the data
  - The confirmation certificate is a set of valid signatures



TrustBoost

- Many layer 1 blockchains
- Some blockchains have weak trust guarantees
- When we have connected blockchains, the security problems get spread from one blockchain to others
- Can we create a combined ledger with boosted trust?

TrustBoost


(b)
AtomX
OsmoX
contract
TrustBoost
contract
TrustBoost
contract
TrustBoost
Π_1
Π_2
Π_m
Atom
(a)
Osmo

Oracles: Connecting To The Outside World

- Bridging Internet with Blockchains
  - Google search
  - GPT4
  - Weather.com

Attendance : NFT Drop

https://poap.website/suddenly-hour-explain

- Mint token to Metamask.
- Submit tx hash for attendance claim