Atomic Commitment Across Blockchains

Victor Zakhary, Divyakant Agrawal, Amr El Abbadi

victorzakhary,divyagrawal,elabbadi@ucsb.edu

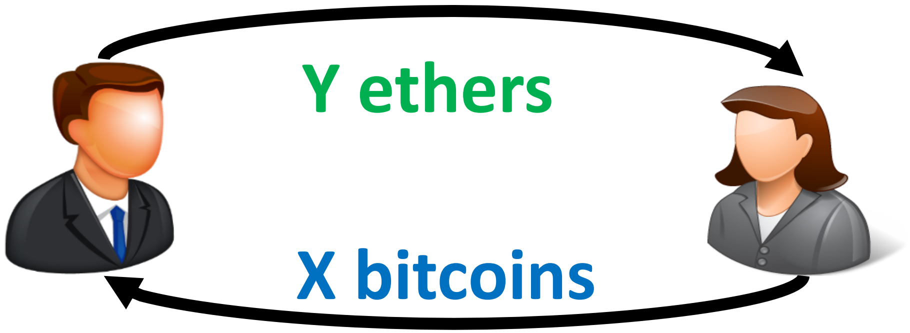
University of California Santa Barbara

Open Blockchain Landscape

- Thousands of Blockchains and tokens
- Exchanges to trade tokens for USD
- Direct token transactions in one blockchain
- Direct token transactions across blockchains, how?
- Cross-chain transactions

Cross-Chain Transaction Example

Atomic Cross-Chain Commitment Protocol



Atomic Swap[Nolan'13, Herlihy'18]

- Alice wants to trade Bitcoin for Ethereum with Bob

Atomic Swap[Nolan'13, Herlihy'18]

- Alice wants to trade Bitcoin for Ethereum with Bob

- Create a secret s
- Calculate its hash h = H(s)

Atomic Swap[Nolan'13, Herlihy'18]

- Alice wants to trade X Bitcoin for Y Ethereum with Bob

SC_1 Move X bitcoins to Bob if Bob provides secret s | h = H(s)

Refund SC_1 to Alice if Bob does not execute SC_1 before **48** hours

s and h

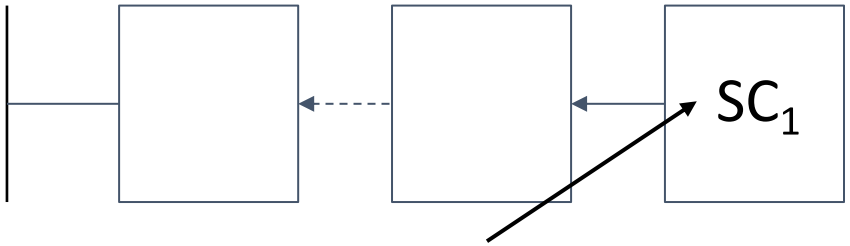
Bob

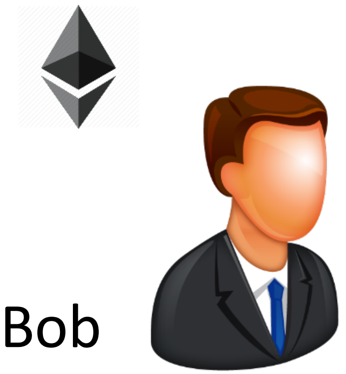
Alice

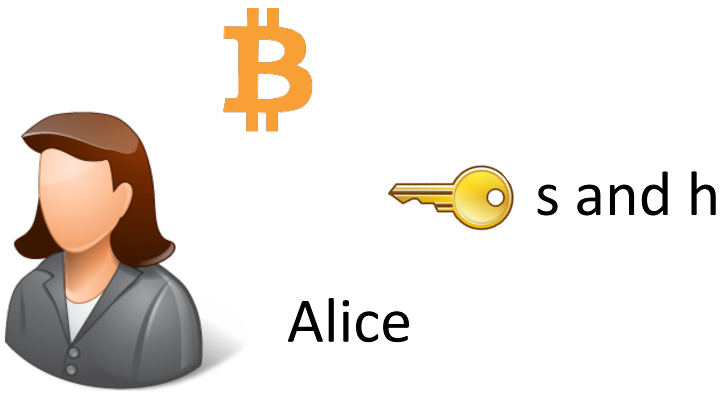
Atomic Swap[Nolan'13, Herlihy'18]

- Alice wants to trade X Bitcoin for Y Ethereum with Bob

Bitcoin blockchain



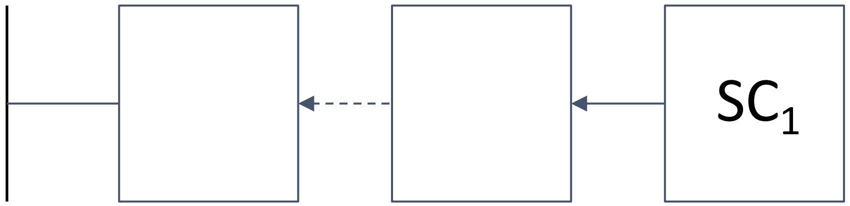




Atomic Swap[Nolan'13, Herlihy'18]

- Now, h is announced in Bitcoin blockchain and made public

Bitcoin blockchain



SC_2 Move Y Ethereum to Alice if Alice provides secret s | h = H(s)

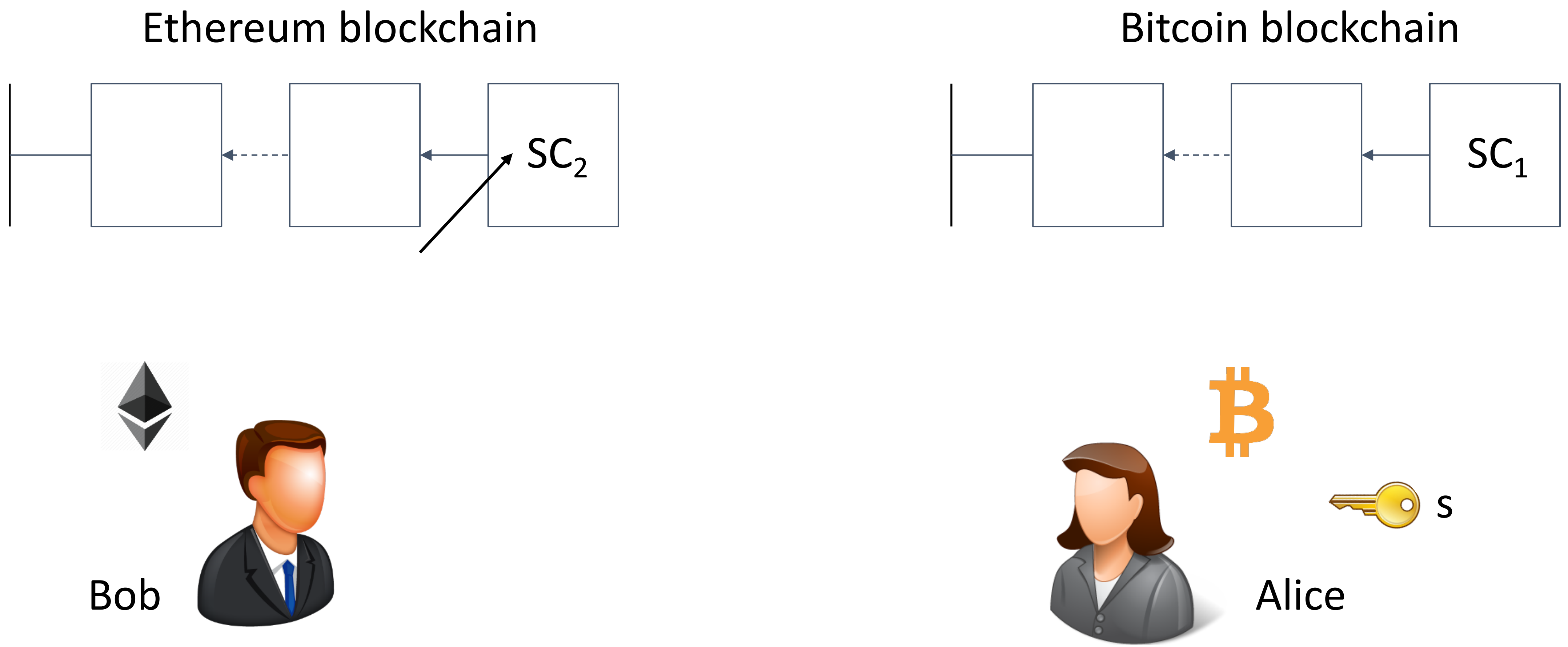
Refund SC_2 to Bob if Alice does not execute SC_2 before **24** hours

Bob

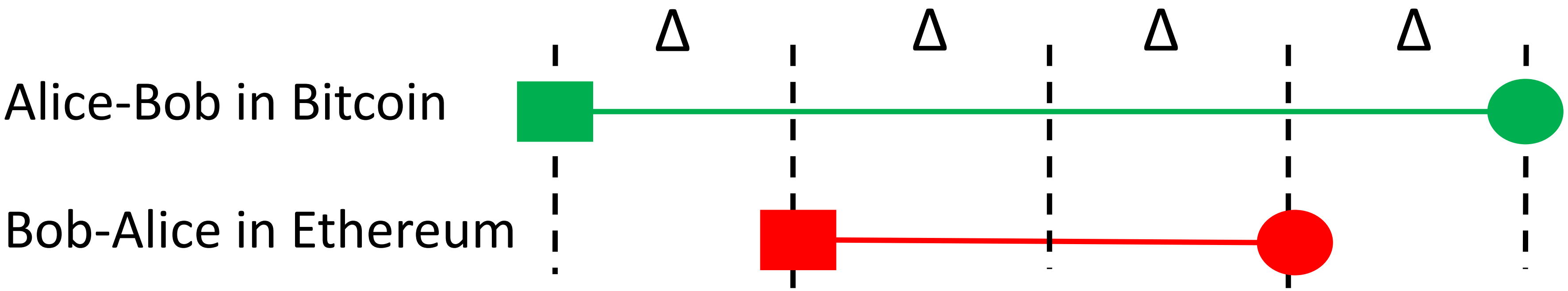
s

Alice

Atomic Swap[Nolan’13, Herlihy’18]

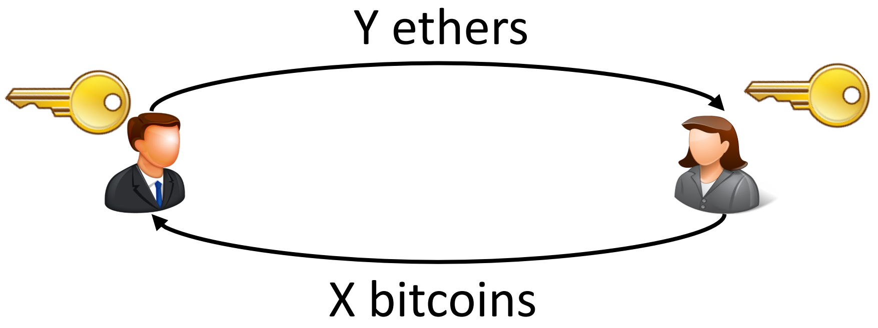


Atomic Swap Example [Nolan’13, Herlihy’18]



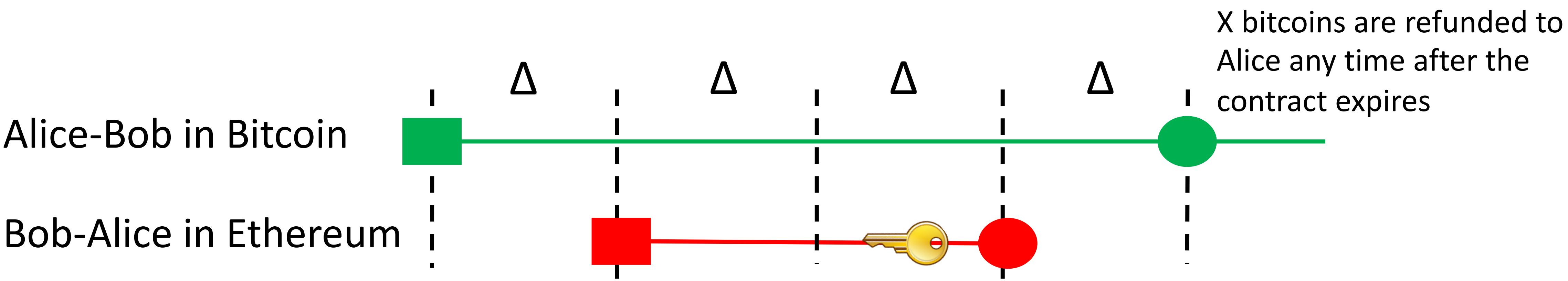
Alice reveals the secret to Bob’s contract and claims the Y ether

Supposedly, Bob takes the secret, reveals it to Alice’s contract and claims the X bitcoins



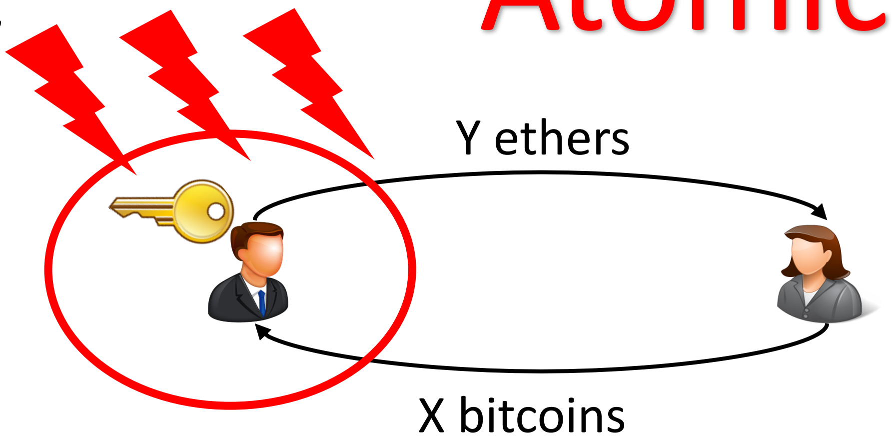
e.g., Δ = 12hr

What can go wrong?



If Bob fails or suffers a network denial of service attack for a Δ, Alice's contract will expire and Bob will lose his X bitcoins

Atomicity Violation



e.g., Δ = 12hr

Atomicity Violation

- Using timelocks leads to Atomicity violation
- Liveness over Safety
- Our Atomicity-based Approach:
  - The decision of both transactions should be made atomic
    - Once the decision is taken, both transactions either commit or abort
  - A transaction cannot commit unless a commit decision is reached
  - A transaction cannot abort unless an abort decision is reached

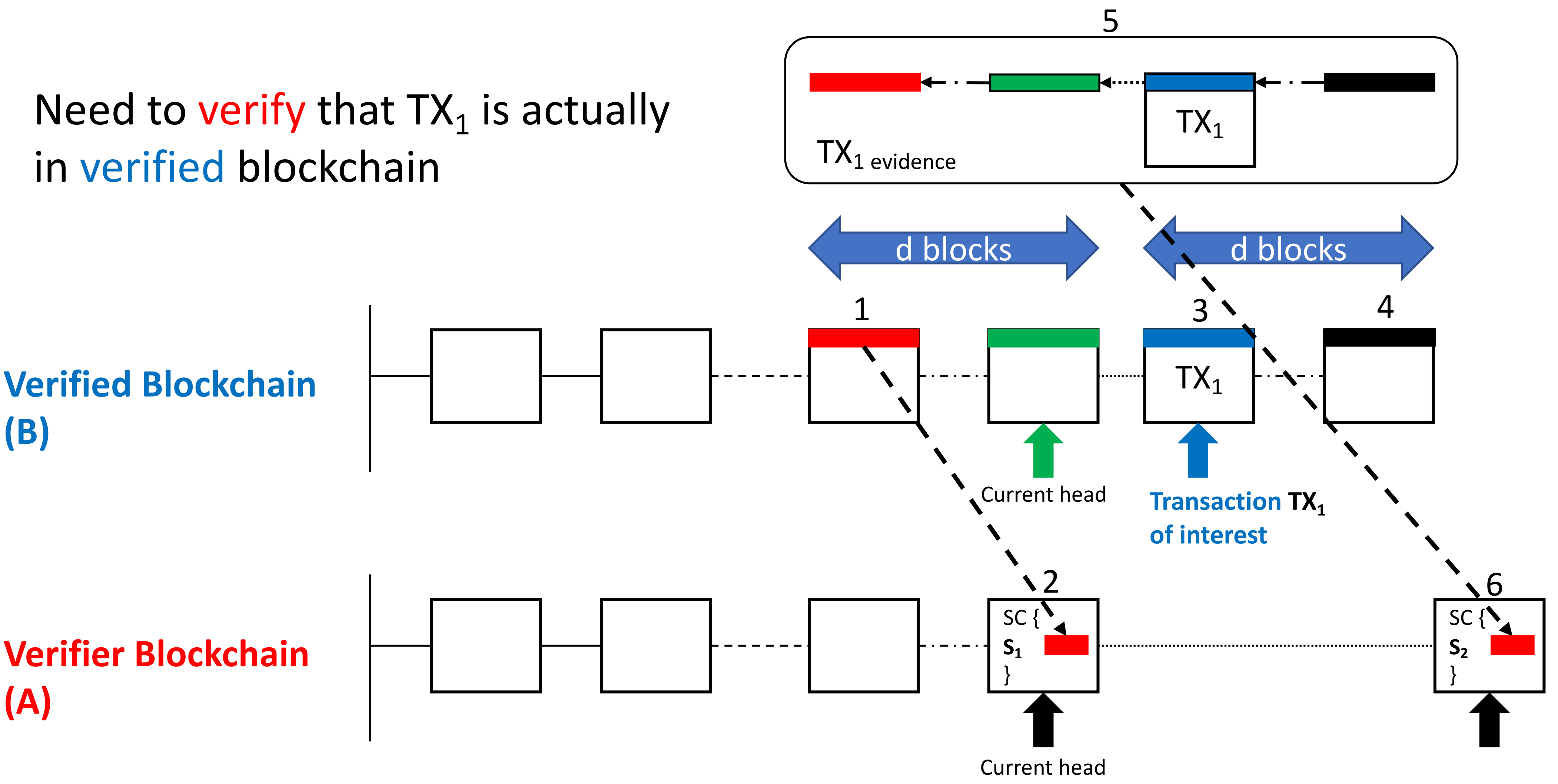
Building block: Cross-Chain Verification

- How can miners of one blockchain:
  - Verify a transaction in another blockchain?
  - Without maintaining a copy of this other blockchain.

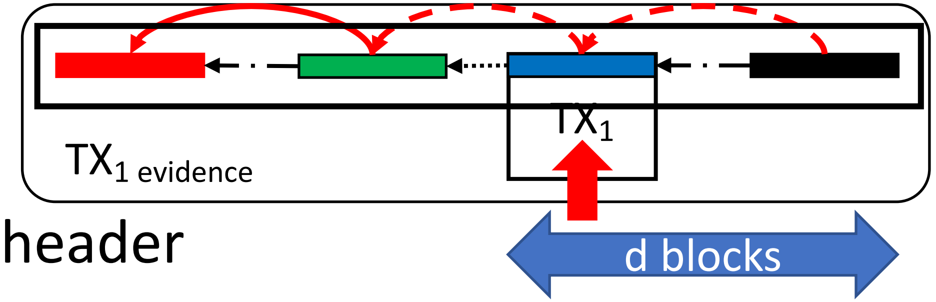
Building block: Cross-Chain Verification

Need to verify that TX_1 is actually in verified blockchain

TX_1 Evidence



Building block: Cross-Chain Verification



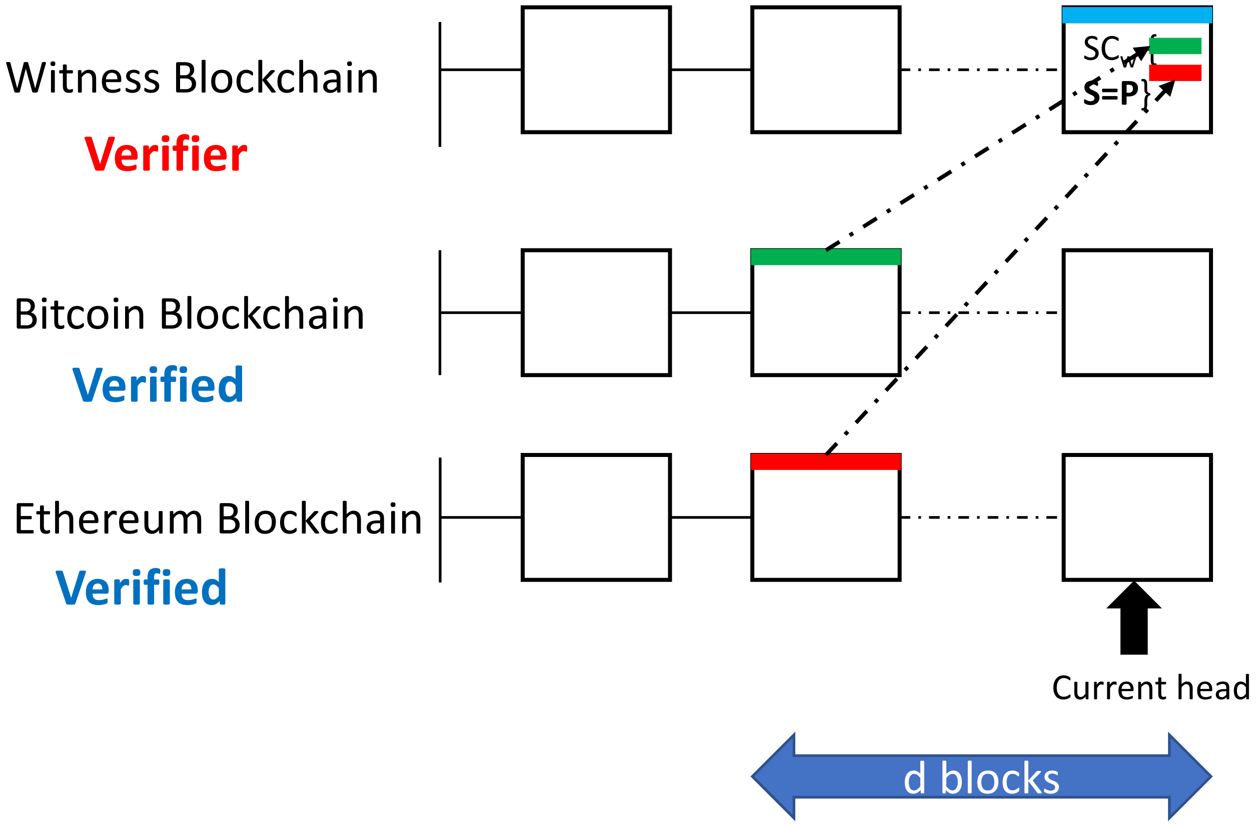
- Verification process:
  - Each header includes the hash of the previous header
  - The proof of work of each header is correct
  - TX_1 is correct
  - TX_1 is buried under d blocks
- The cost of generating evidence:
  - Choose d to make this cost > the value transacted in TX_1
  - If true, a malicious user has no incentive to create a fake evidence

Atomic Commitment Across Blockchains

- AC3WN: Atomic Cross Chain Commitment using Witness Network
- Use another blockchain to witness the Atomic Swap
- The witness blockchain decides the commit or the abort of a swap
- Once a decision is made:
  - All sub-transactions in the swap must follow the decision
  - Achieves atomicity, either all committed or all aborted
- Cross chain verification is leveraged twice
  - Miners of the witness network verify the publishing of contracts in asset blockchains
  - Miners of assets' blockchains verify the decision made in the witness network

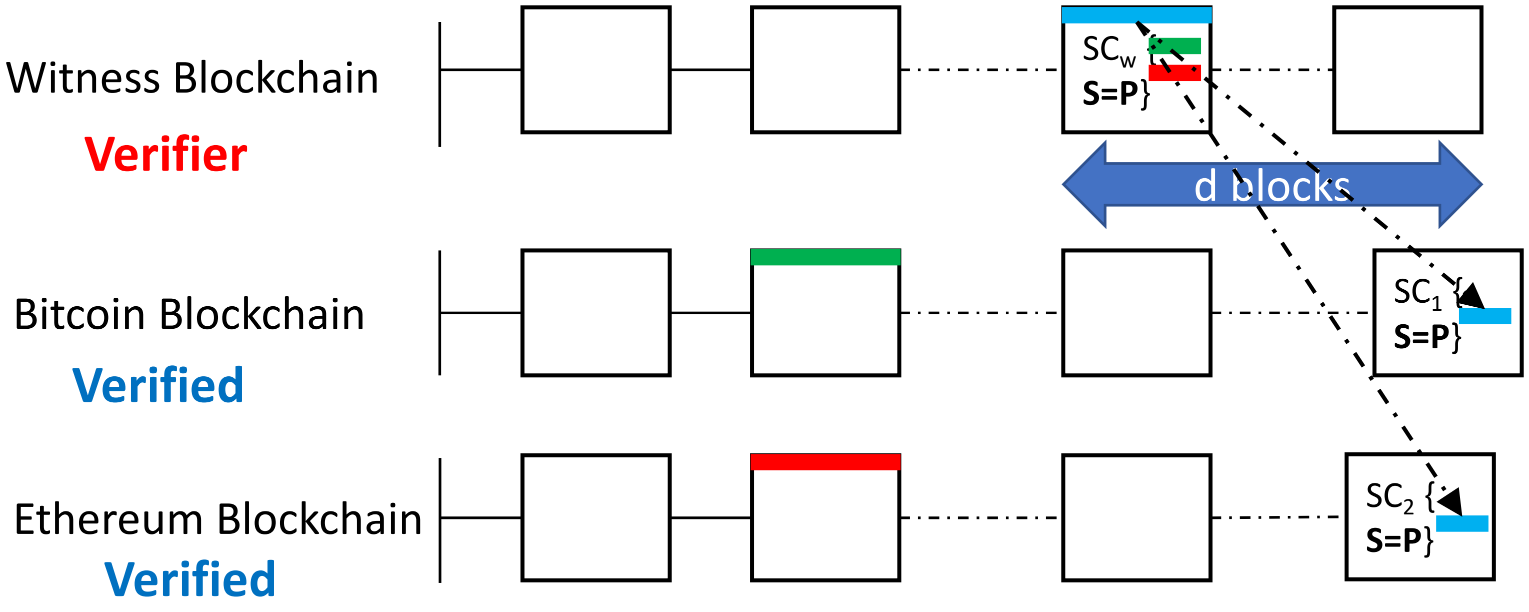
Protocol Sketch

- Deploy a contract SC_w in the witness network with state *Published (P)*
- SC_w has a header of a block at depth **d** of all blockchains in the swap



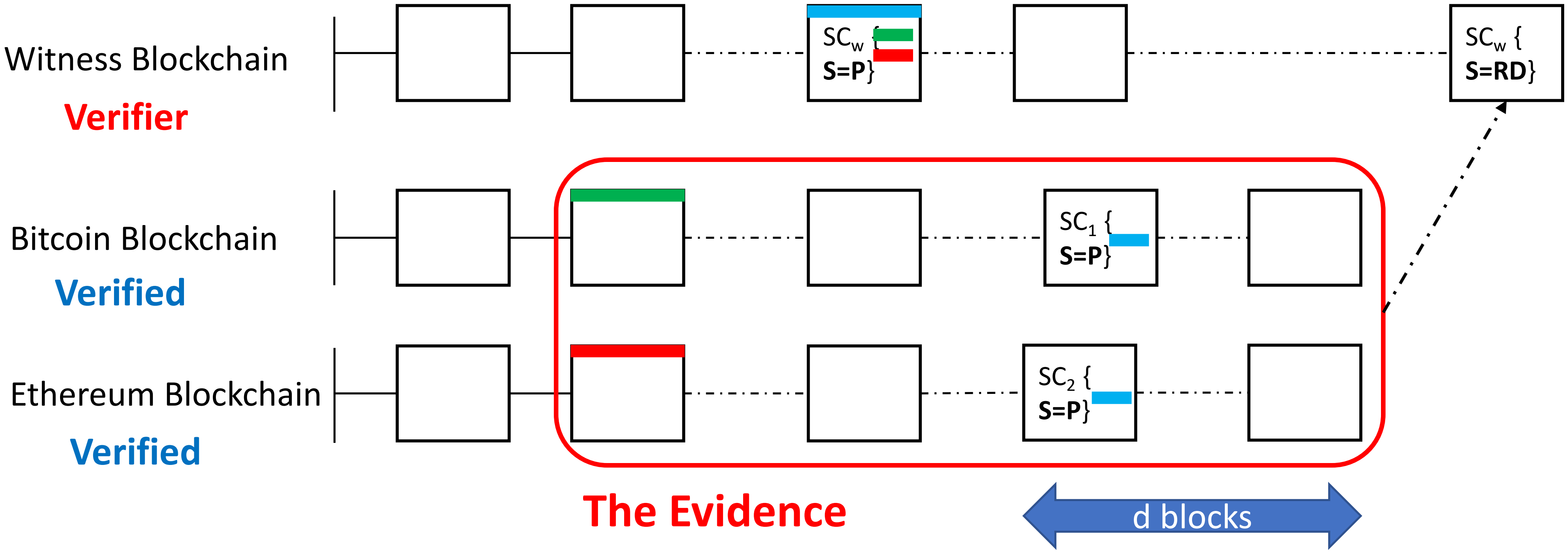
Protocol Sketch Cont'd

- Participants deploy their contracts in the corresponding blockchains
- Participants add the header of SC_w to their contracts



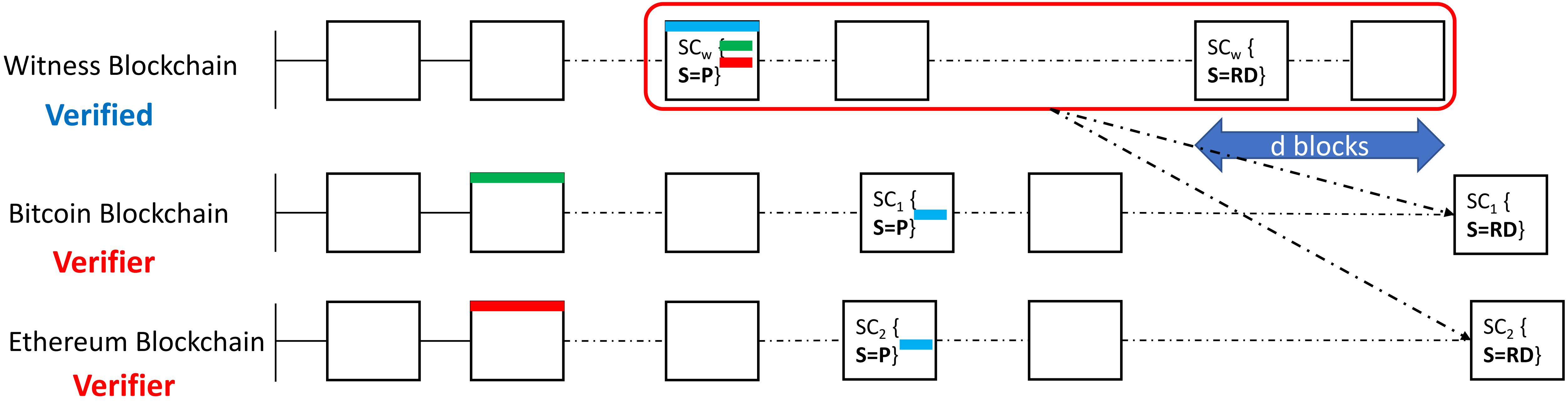
Protocol Sketch Cont’d

- Participants submit evidence of publishing the smart contracts in Assets Blockchains
- If all contracts are published and correct, SC_w’s state is altered to redeem (RD)



Protocol Sketch Cont’d

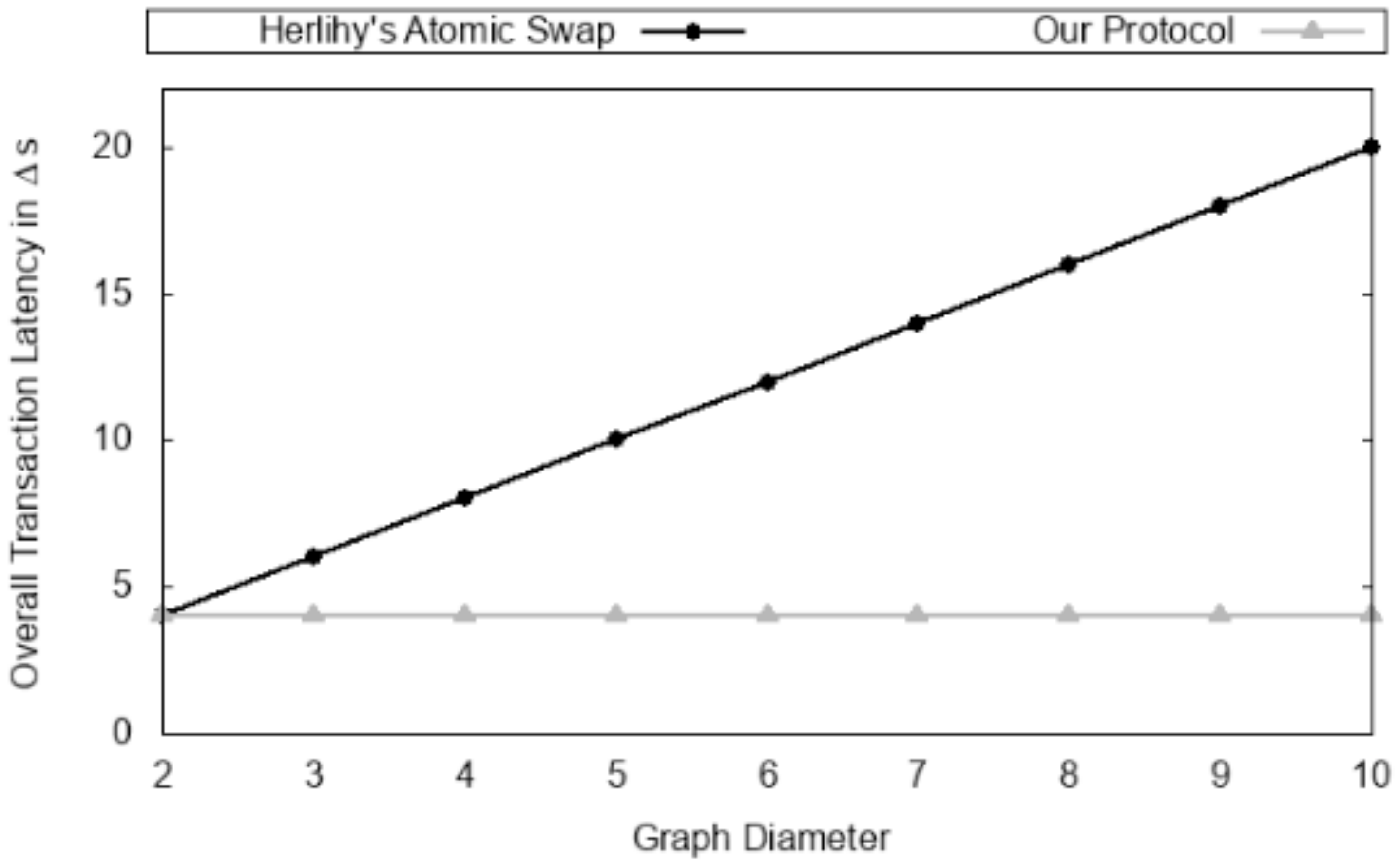
- Participants submit evidence of Redeem State (RD) from the Witness Blockchain to the Assets Blockchains.
- After evidence verification, participants redeem their assets from the Assets Blockchains.



Atomic Commitment Across Blockchains

- SC_w's state determines the commit (RD) or the abort (RF) decision
- Once SC_w's state is altered and the block is buried under d blocks:
  - All sub-transactions must follow this decision
  - None of the sub-transactions can decide on a different decision
- Even if a participant fails or faces a network denial of service:
  - When the participant recovers, the evidence of the decision still exists
  - This evidence can be used to redeem or refund the contracts
- The only way to violate atomicity is to fork the witness blockchain
- Economic incentives prevent this attack
- Any protocol is prone to fork attacks

AC3WN vs Atomic Swap: Latency



The overall Atomic Cross Chain Transaction latency in Δs as the graph diameter, Diam(D), increases.

AC3WN vs Atomic Swap: Cost ($)

- Deployment of the witness network contract
- Evidence validation execution cost at the witness network

Summary

- AC3WM, the first safe Atomic Cross Chain Commitment Protocol
- Constant latency regardless of the swap graph size
- Slightly more deployment cost overhead ($)