Demystifying Blockchains: *Decentralized, Secure and Fault-tolerant Storage*

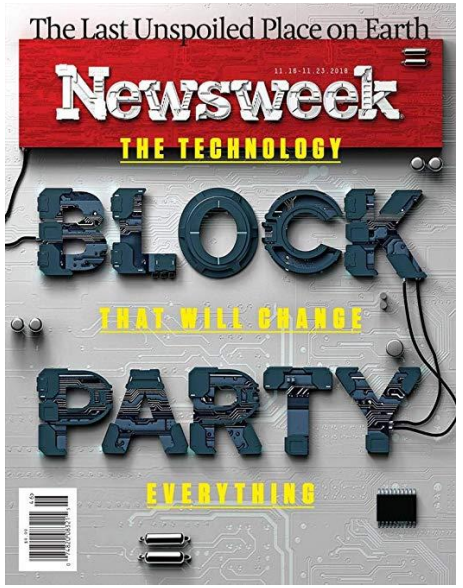
Amr El Abbadi
University of California, Santa Barbara

In Collaboration with:

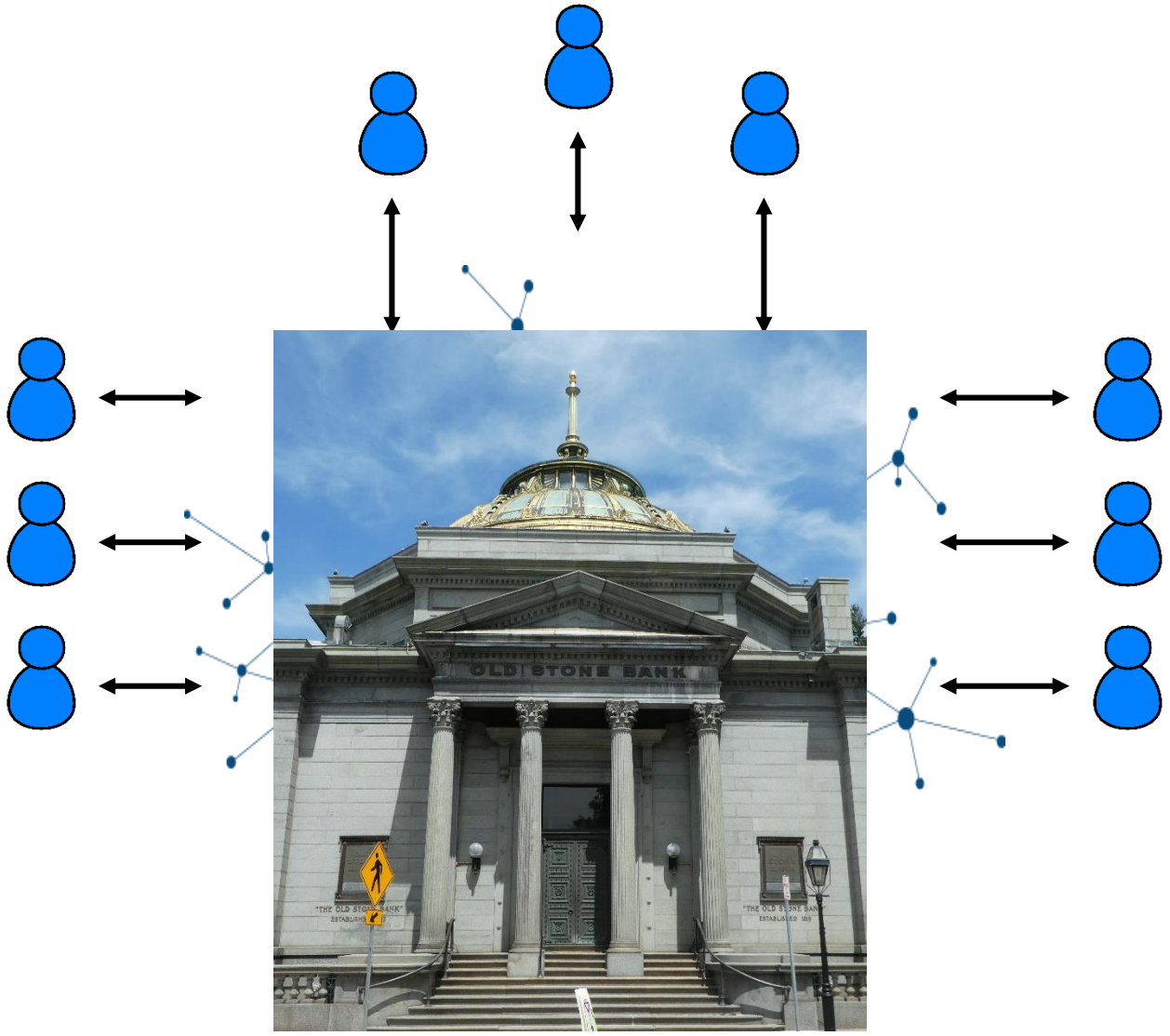
Mohammad Amiri, Sujaya Maiyya, Victor Zakhary, and **Divyakant Agrawal.**

Blockchains

- Many interesting (controversial?) problems in new guises.
  - Distributed Systems: Consensus, replication, etc
  - Data Management: Transactions, replication, commitment, etc
  - Security: Encryption, hashing, etc
  - Economics: Money, tokens, assests, etc



Bitcoin

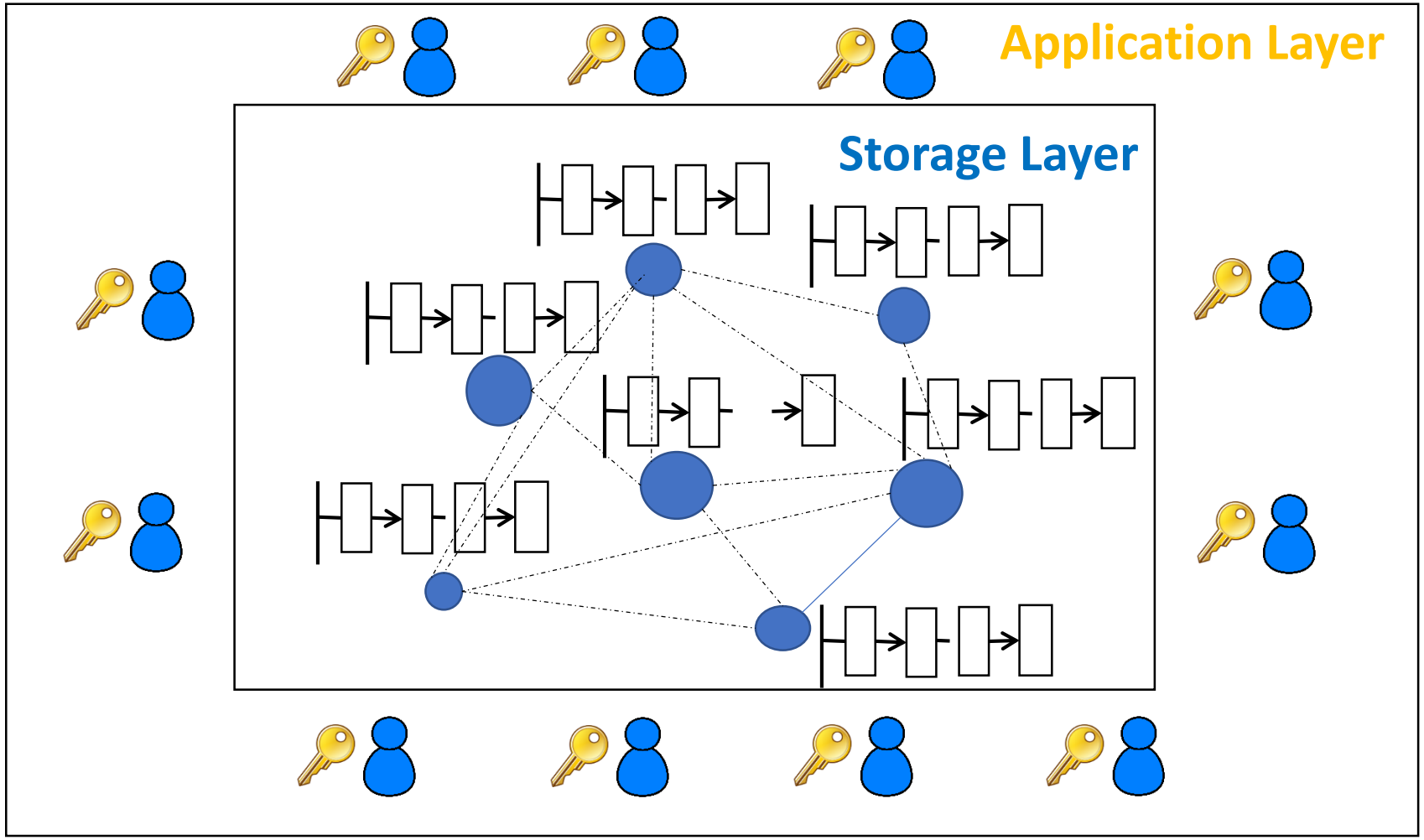


Traditional Banking Systems

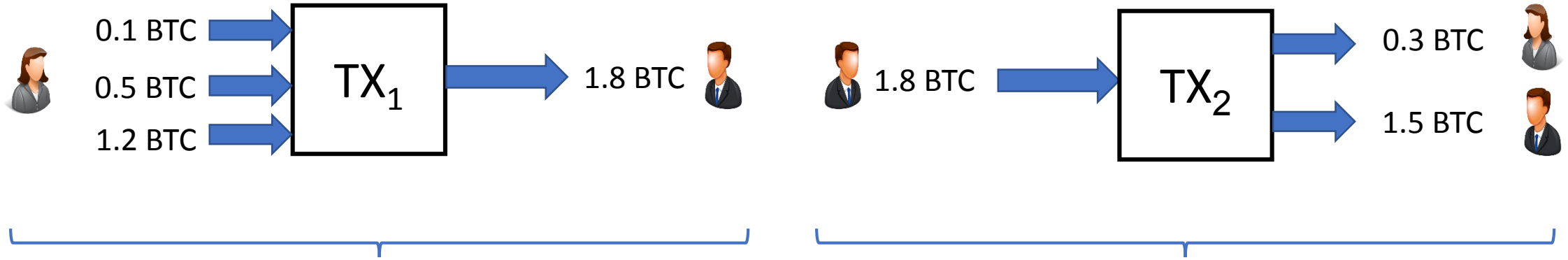
- From Database and Distributed Computing Perspective
- Identities and Signatures
  - You are your signature: IDENTITY
  - ➔ Private and Public Digital signatures
- Ledger
  - The balance of each identity (saved in a DB)
  - ➔ Blockchain (basically a linked list!)
- Transactions
  - Move money from one identity to another
  - Concurrency control to serialize transactions ➔ Mining and Proof of Work
  - Typically backed by a transactions log
    - Log is persistent (disk) ➔ Replication to the whole world
    - Log is immutable and tamper-free (end-users trust this) ➔ HashPointers

Blockchain Architecture

- The ledger is fully replicated to all network nodes
  - A Block is a set of transactions submitted by the clients.

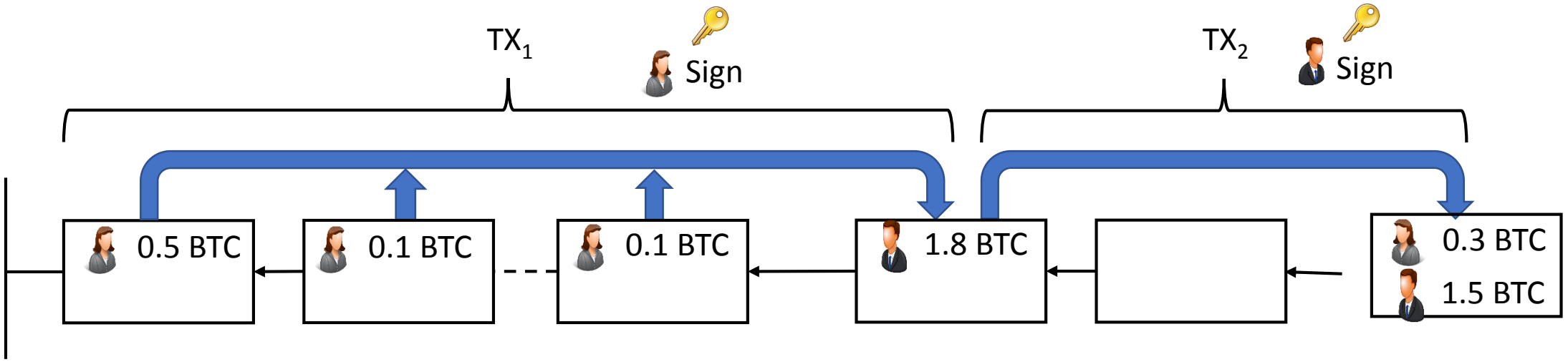


Transaction Model



Assuming no imposed transaction fees!

Transaction Model

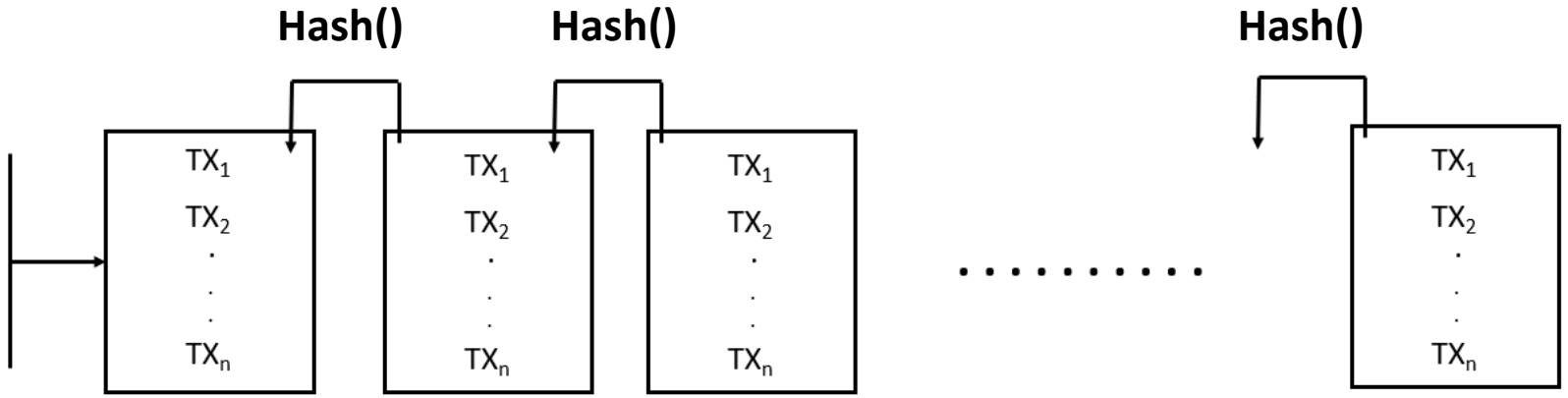


The Ledger: Some Technical Details

- How is the ledger tamper-free?

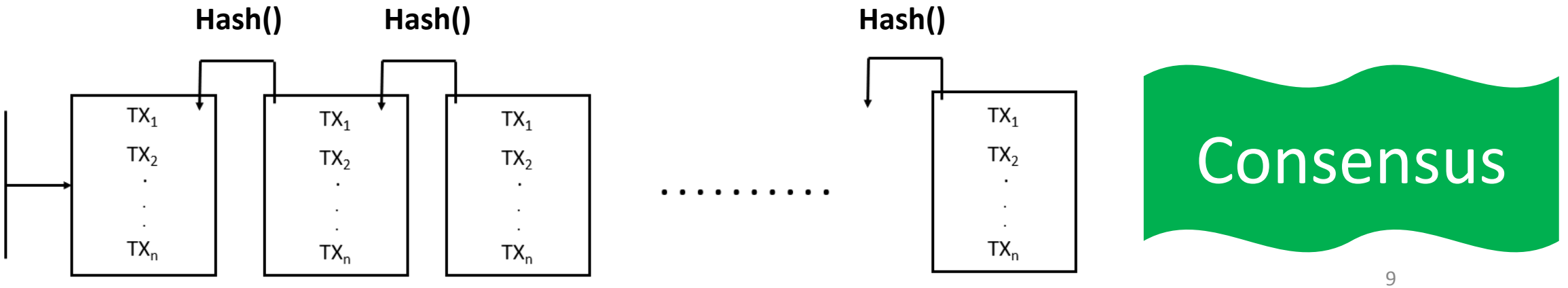
  Blocks are connected through **hash-pointers**

  - Each block contains the hash of the previous block header
  - Tampering with the content of any block can easily be detected



Making Progress

- To make progress:
  - Network nodes **validate** new transactions to make sure that:
    - Transactions on the new block do not conflict with **each other**
    - Transactions on the new block do not conflict with **previous blocks transactions**
  - Network nodes need to agree on the next block to be added to the blockchain
- New assets are generated and registered through mining.
  - Reward transaction in every mined block

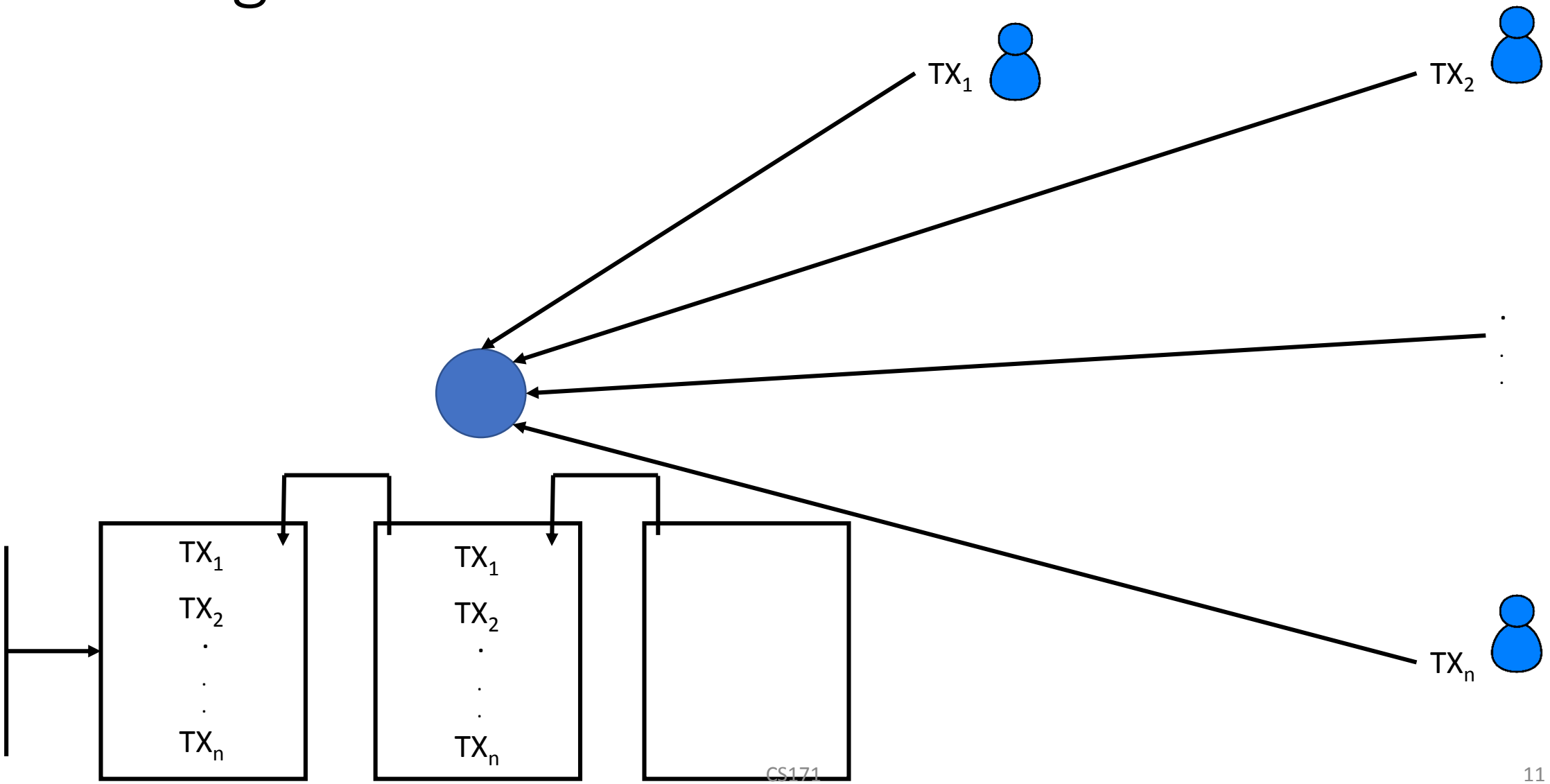


Consensus Protocols

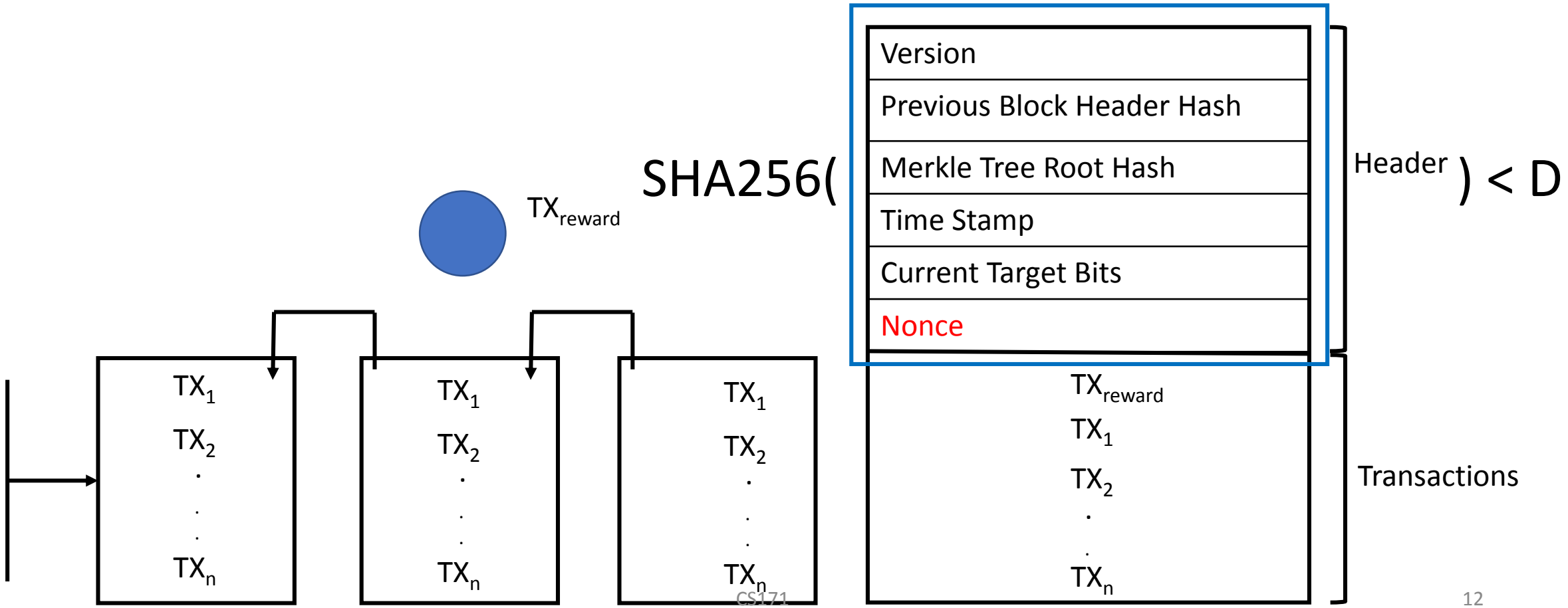
All **participants** should be known **a priori**

- **Permissioned** vs **Permissionless** settings
- **Permissionless** Blockchains:
    - Network nodes freely join or leave at anytime
    - Nakamoto's Consensus: Proof of Work (PoW)
    - Ethereum's Consensus: Proof of Stake (PoS)
- :Permissioned Blockchains
    - Paxos (Crash failures only)
    - Byzantine Fault-tolerance (malicious failures)

Mining Details: Block Creation

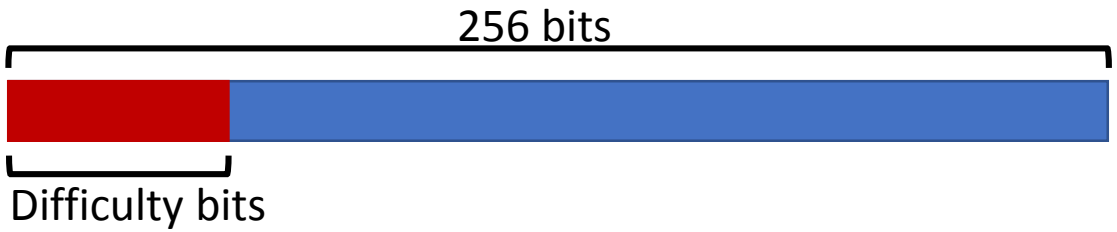


Mining Details: Block Contents



Mining Details

- D: dynamically adjusted difficulty



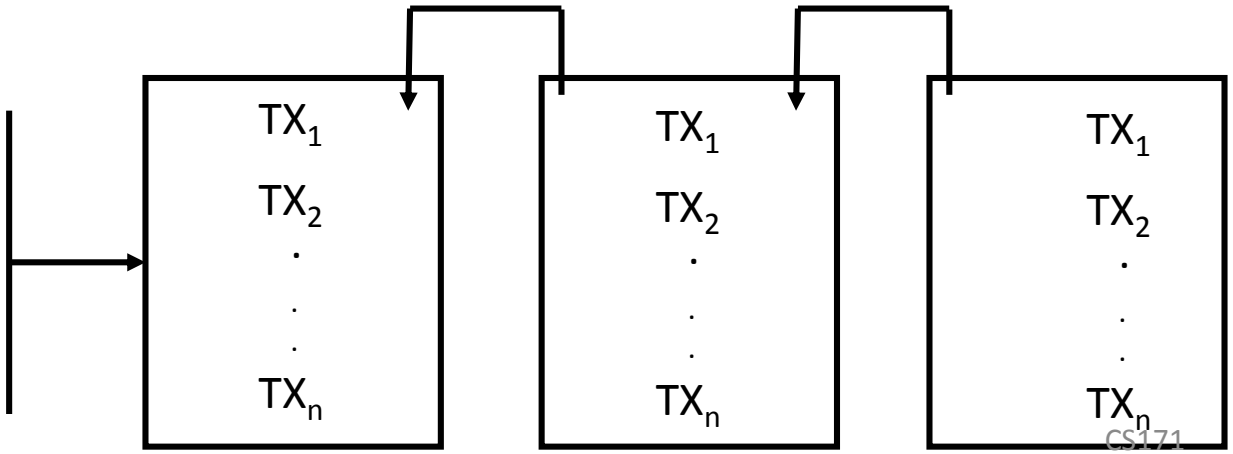
- Difficulty is adjusted every 2016 blocks (almost 2 weeks)

SHA256(Header) < D

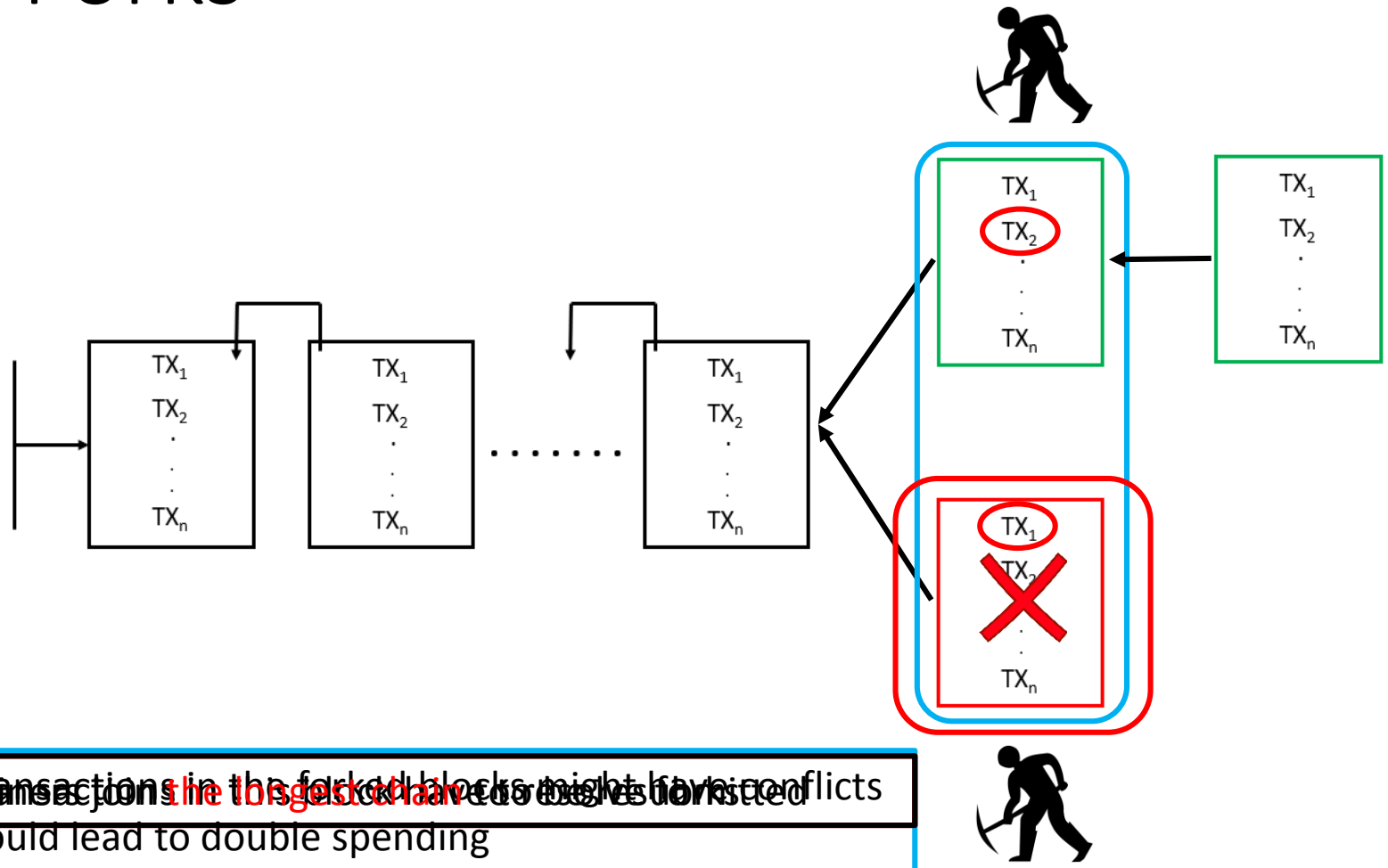
Version
Previous Block Header Hash
Merkle Tree Root Hash
Time Stamp
Current Target Bits
Nonce

TX_{reward}
TX_1
TX_2
.
.
TX_n

Transactions



Forks



- Transactions in the forked blocks might have conflicts
- Could lead to double spending
- Forks have to be eliminated

Some Limitations of Bitcoin

- High transaction-confirmation **latency**
- **Probabilistic** consistency guarantees
- Very **low TPS** (Transactions per second) - average of **3 to 7 TPS**
- **Transparency** leads to lack of **privacy**
- **Energy** consumption due to **PoW.**

Atomic Commitment Across Blockchains

The Landscape

Cryptocurrencies: 2225 • Markets: 18851

Market Cap: $257,486,187,861 • 24h Vol: $66,548,083,112

Search

ion

Cryptocurrencies ▾ | Exchanges ▾ | Watchlist | USD ▾ | Next 100 → | View All

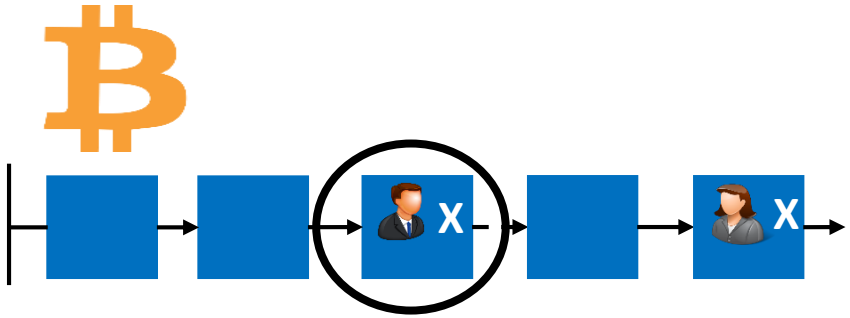
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$142,627,334,795	$8,036.77	$19,138,268,181	17,746,837 BTC	3.15%	
2	Ethereum	$26,732,290,299	$251.25	$8,364,736,132	106,397,463 ETH	1.70%	
3	XRP	$17,876,222,703	$0.423217	$1,658,461,942	42,238,947,941 XRP *	1.25%	
4	Litecoin	$7,281,728,951	$117.21	$5,141,138,982	62,124,551 LTC	6.28%	
5	Bitcoin Cash	$7,157,820,741	$401.55	$1,572,103,916	17,825,688 BCH	2.02%	

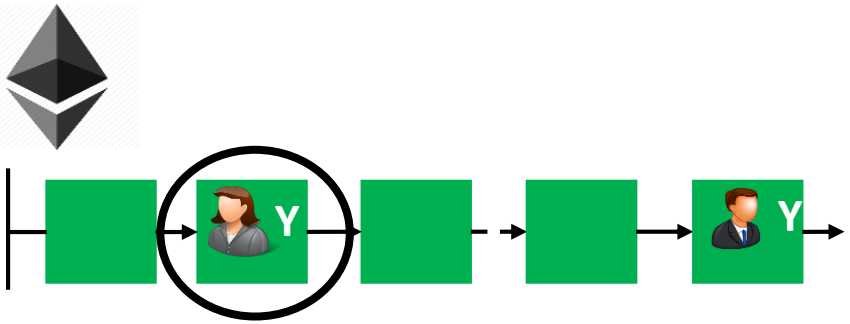
Source: coinmarketcap.com on June 7th 2019 at 5:00pm PST

The Landscape

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

Cross-ChainTransaction Example



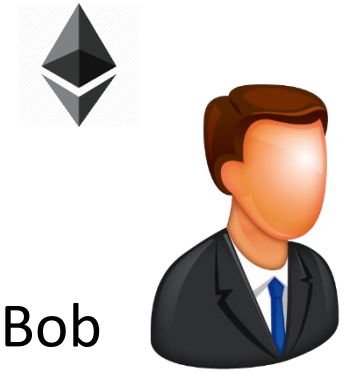


Atomic Cross-Chain Commitment Protocol

Swap of Ownership

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

- Alice wants to trade Bitcoin for Ethereum with Bob



Bob

Alice

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

- Alice wants to trade Bitcoin for Ethereum with Bob

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

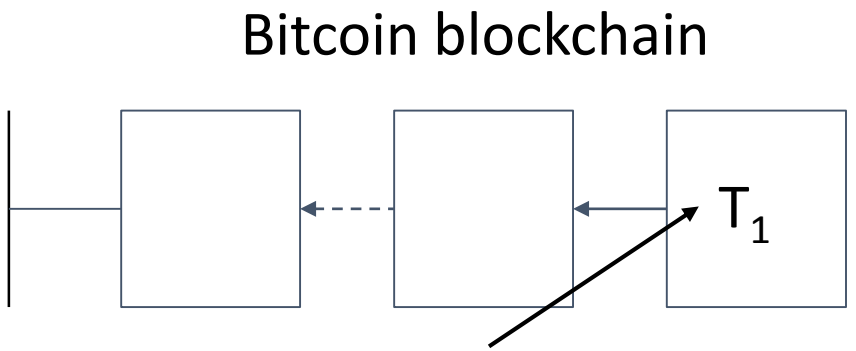
Bob

s and h

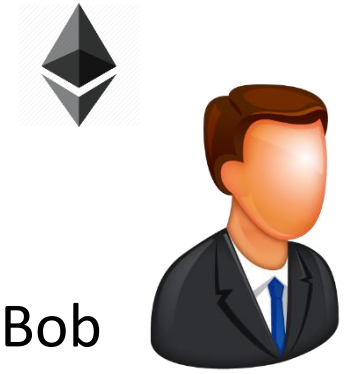
Alice

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

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



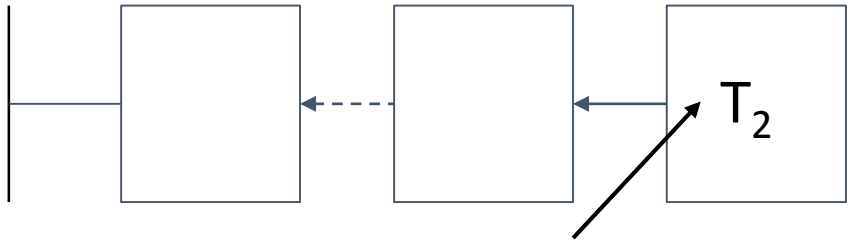
T_1 Move X bitcoins to Bob if
Bob provides secret s | h = H(s)



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

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

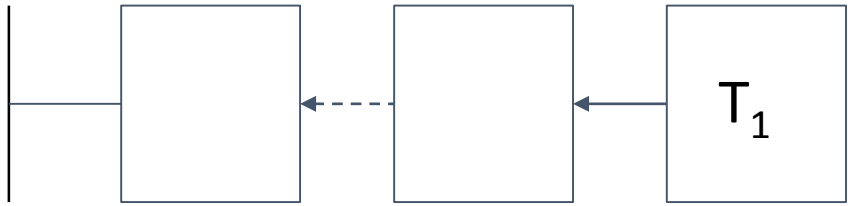
Ethereum blockchain



T_2 Move Y Ethereum to Alice if Alice provides secret s | h = H(s)

Bob

Bitcoin blockchain



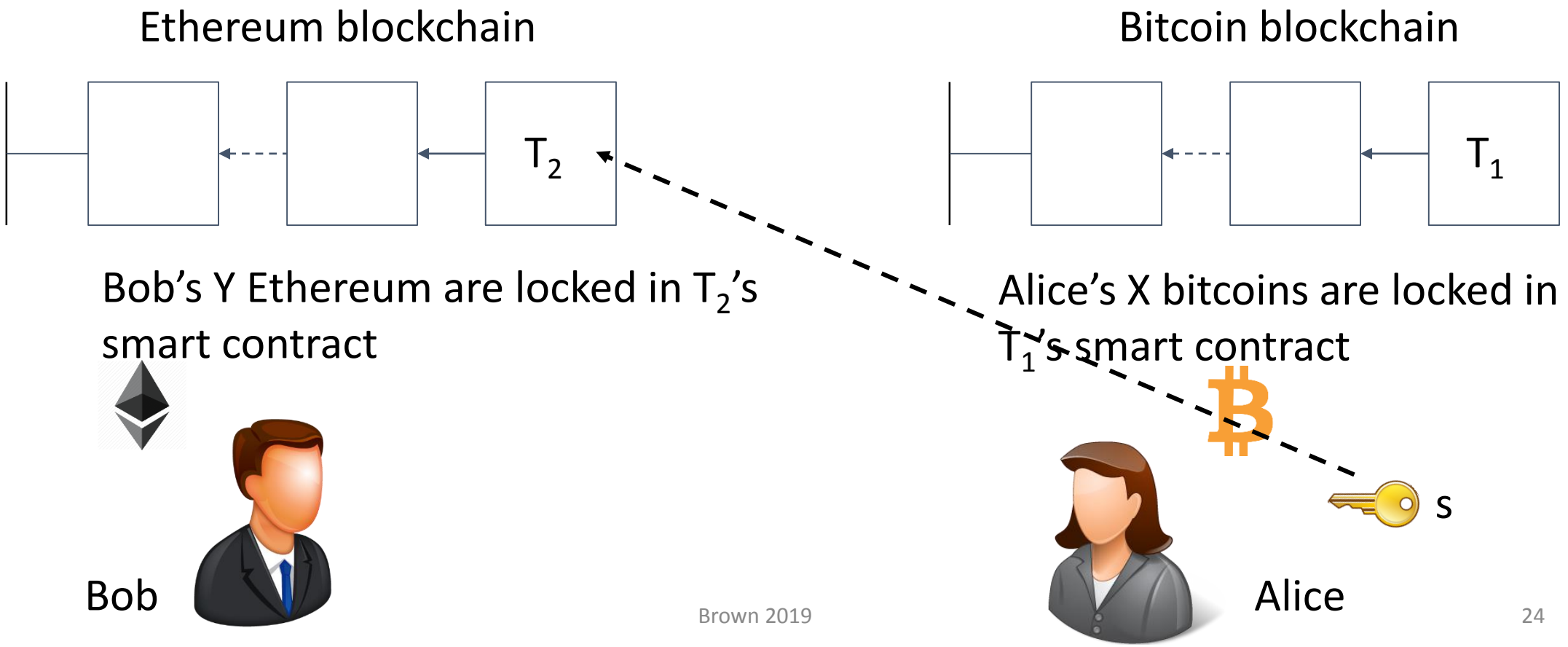
Alice's X bitcoins are locked in T_1's smart contract

s

Alice

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

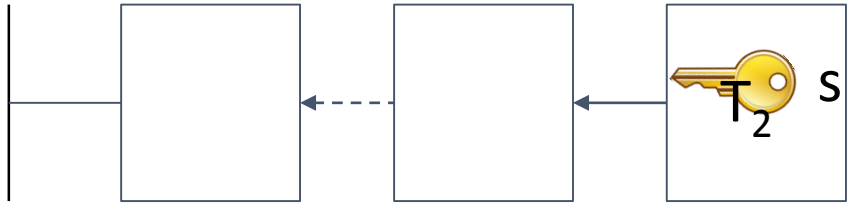
- Now, for Alice to execute T_2 and redeem Y Ethereum, she reveals s



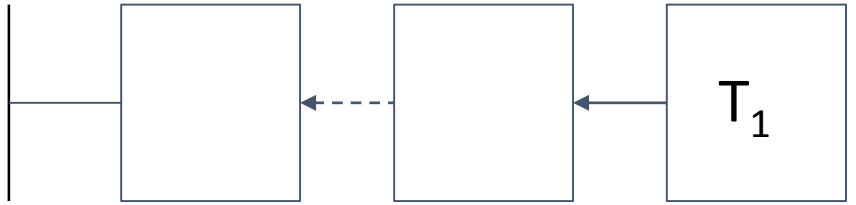
Atomic Swap Example [Nolan'13, Herlihy'18]

- Revealing s, executes T_2. Now s is public in Ethereum's blockchain

Ethereum blockchain



Bitcoin blockchain



Bob's Y Ethereum are locked in T_2's smart contract

Bob

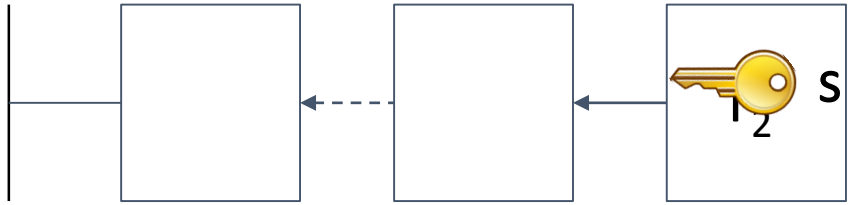
Alice's X bitcoins are locked in T_1's smart contract

Alice

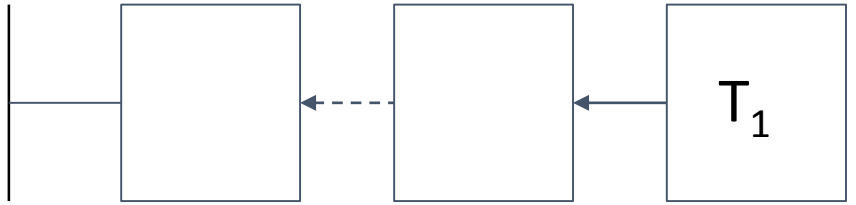
Atomic Swap Example [Nolan'13, Herlihy'18]

- Now, Bob uses s to execute T_1 and redeem his Bitcoins

Ethereum blockchain

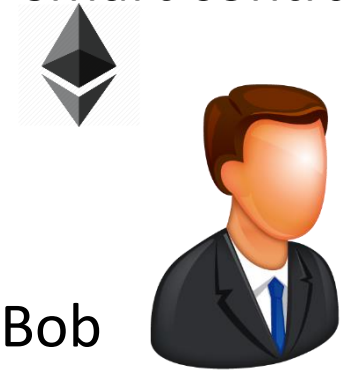


Bitcoin blockchain



Bob's Y Ethereum are locked in T_2's smart contract

Alice's X bitcoins are locked in T_1's smart contract



Bob

Alice

Atomic Swap Example: What can go wrong?

- Alice locks her X Bitcoins in Bitcoin's blockchain through T_1
- Bob sees T_1 but refuses to insert T_2
- Now, Alice's Bitcoins are locked for good
  - A conforming party (Alice) ends up worse off because Bob doesn't follow the protocol
- Prevention
  - Use timelocks to expire a contract
  - Specify that an expired contract is refunded to the creator of this contract

Atomic Swap Example: Timelocks

How to determine the time period of a timelock?

T_4: Refund T_2 to Bob if Alice does not execute T_2 before 24 hours

T_2: Move Y Ethereum to Alice if Alice provides secret s | h = H(s)

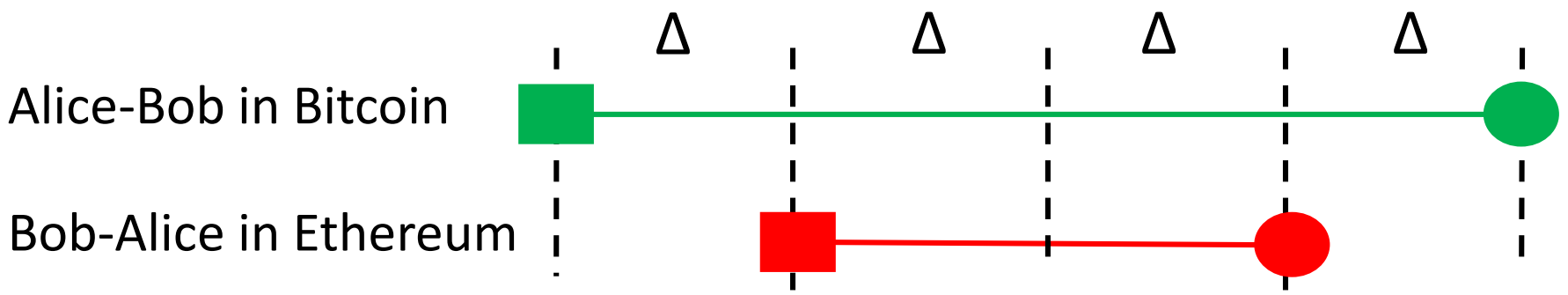
Bob

T_3: Refund T_1 to Alice if Bob does not execute T_1 before 48 hours

T_1: Move X bitcoins to Bob if Bob provides secret s | h = H(s)

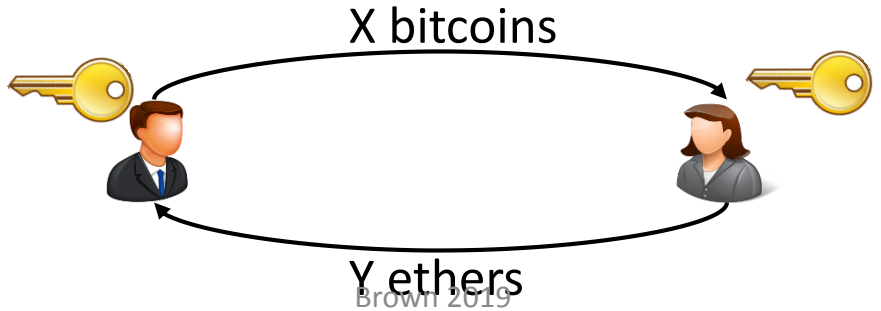
Alice

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



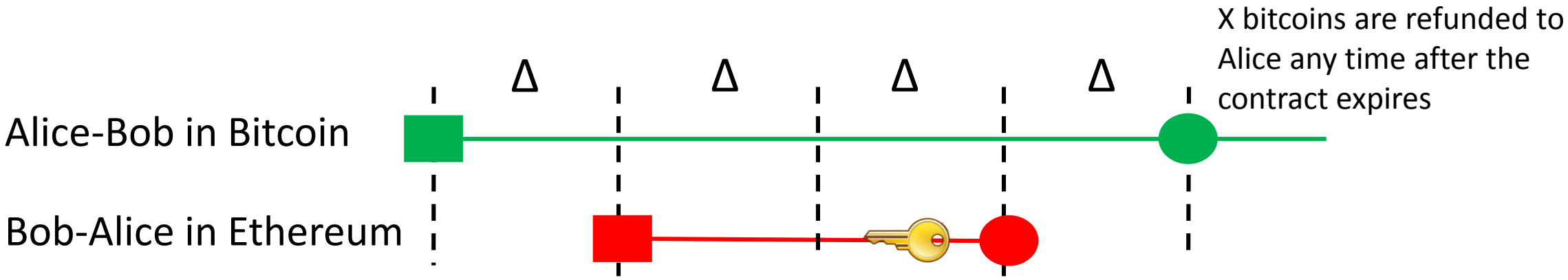
Alice reveals the secret to Bob's contract and claims the Y ether

Now, Bob takes the secret, reveals it to Alice's contract and claims the X bitcoins



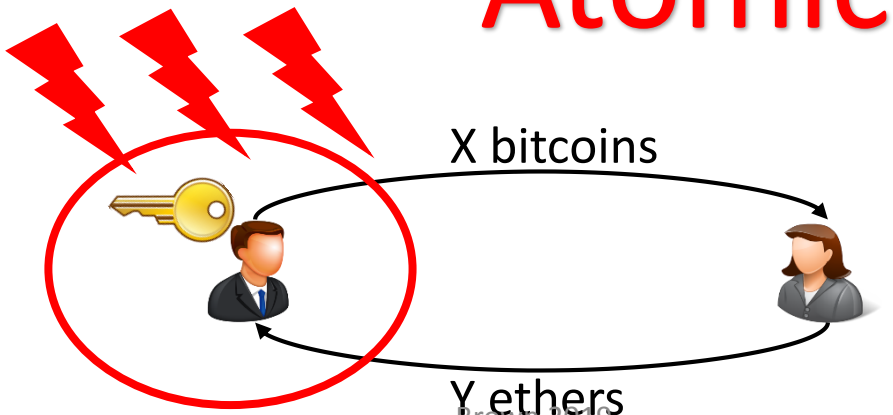
e.g., Δ = 12hr

What can go wrong?



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

Atomicity Violation



Atomicity Violation

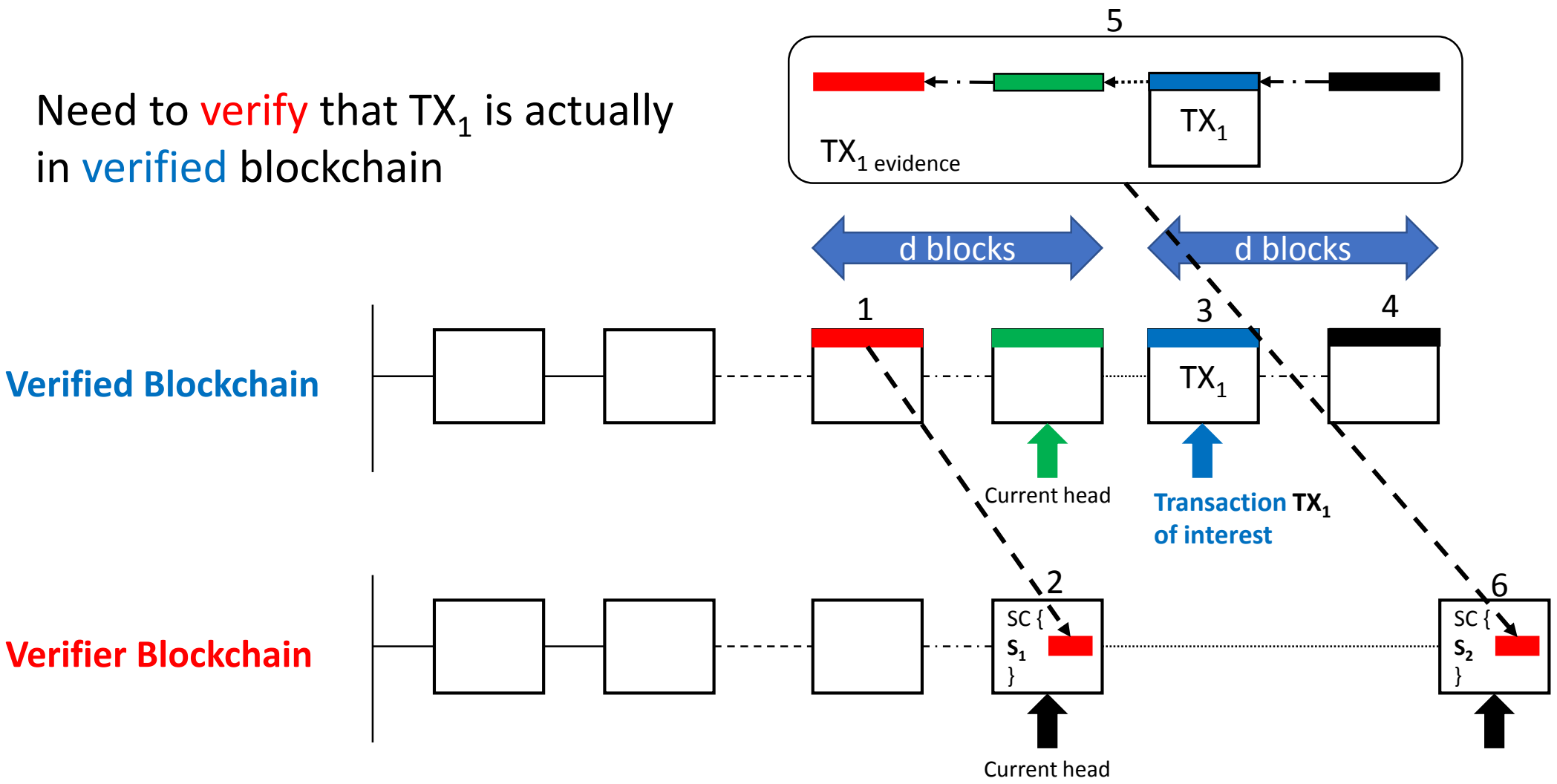
- Using timelocks leads to Atomicity violation
- Our Atomicity-based Approach:
  - The decision of both transactions should be made atomic
    - Once the decision is taken, both transactions either commit or abort
  - A transaction cannot commit unless a commit decision is reached
  - A transaction cannot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

Building block: Cross-Chain Verification

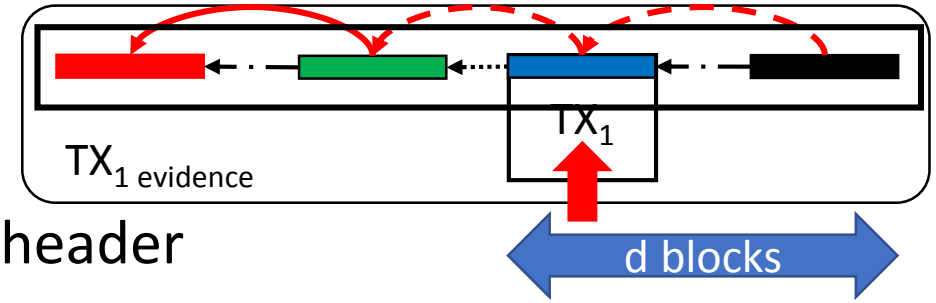
- How can miners of one blockchain:
  - Verify a transaction in another blockchain?
  - Without maintaining a copy of this other blockchain.

Building block: Cross-Chain Verification

Need to verify that TX_1 is actually in verified blockchain



Building block: Cross-Chain Verification



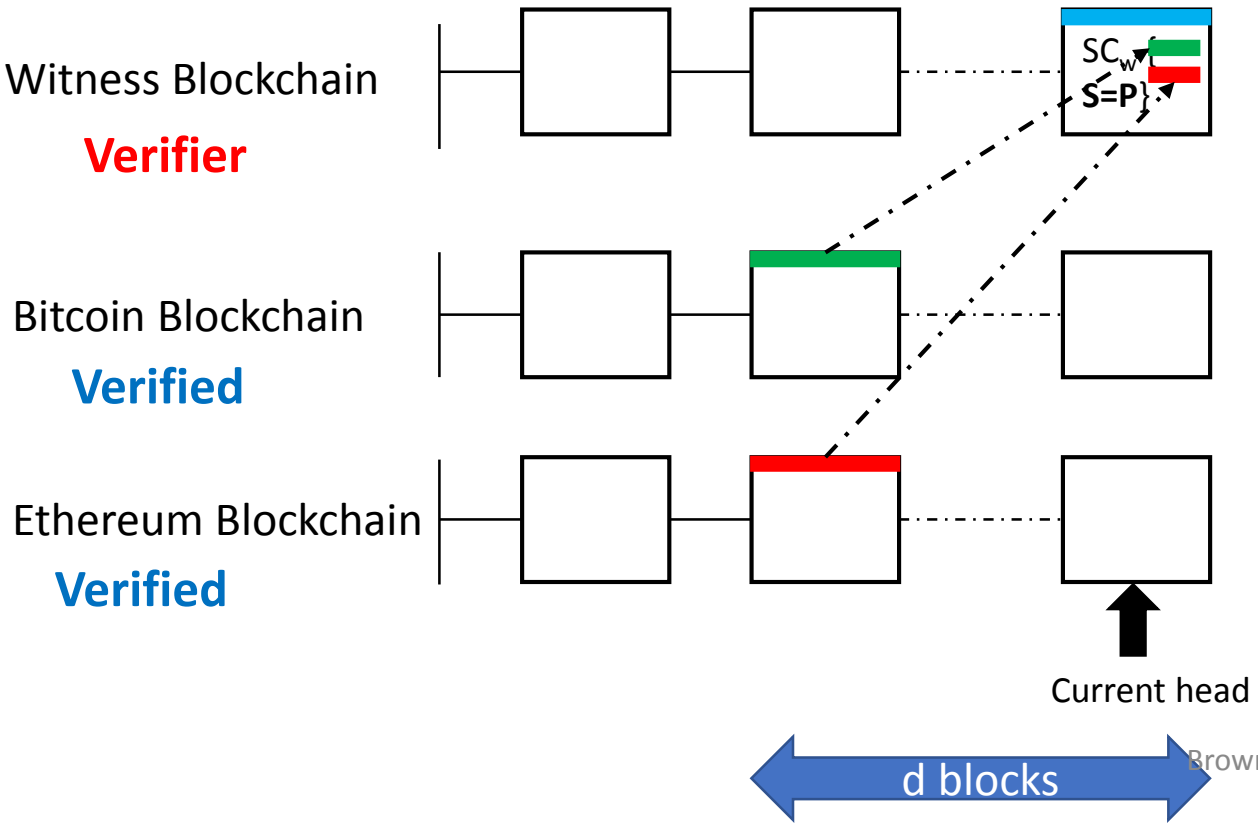
- Verification process:
  - Each header includes the hash of the previous header
  - The proof of work of each header is correct
  - TX_1 is correct
  - TX_1 is buried under d blocks
- The cost of generating evidence:
  - Choose d to make this cost > the value transacted in TX_1
  - If true, a malicious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

Atomic Commitment Across Blockchains

- 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

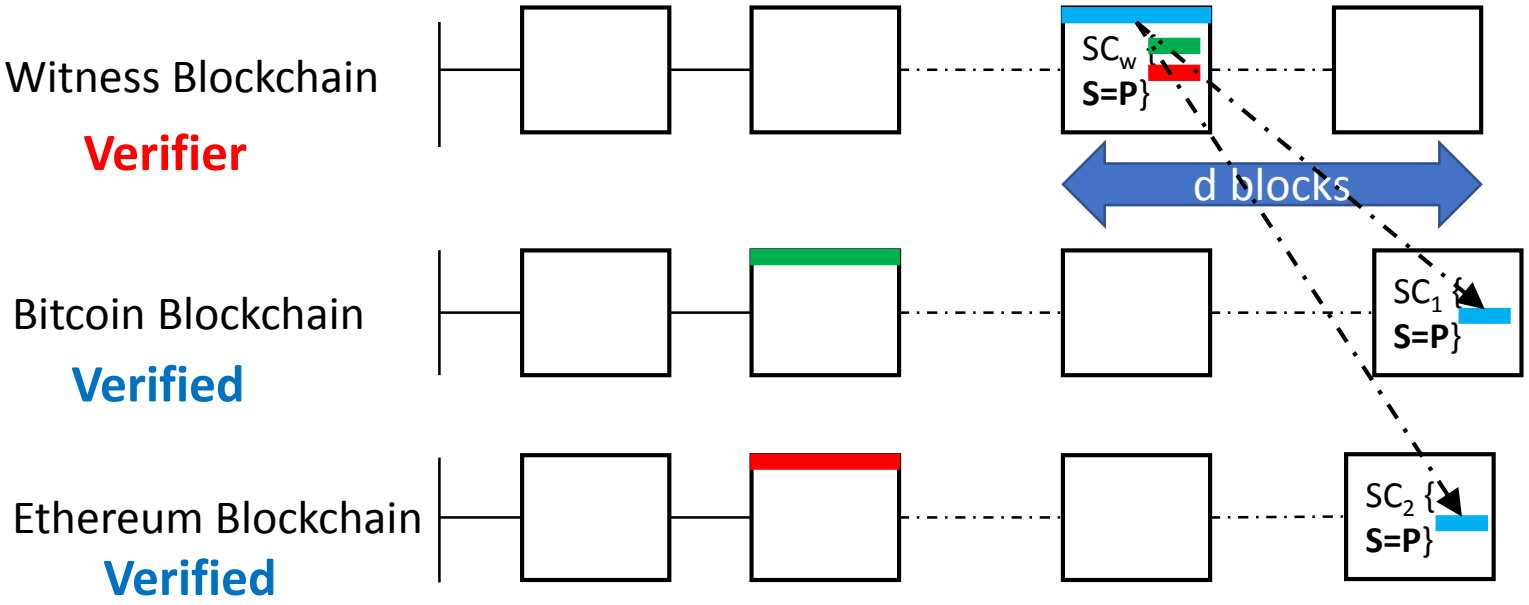
Protocol Sketch

- 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



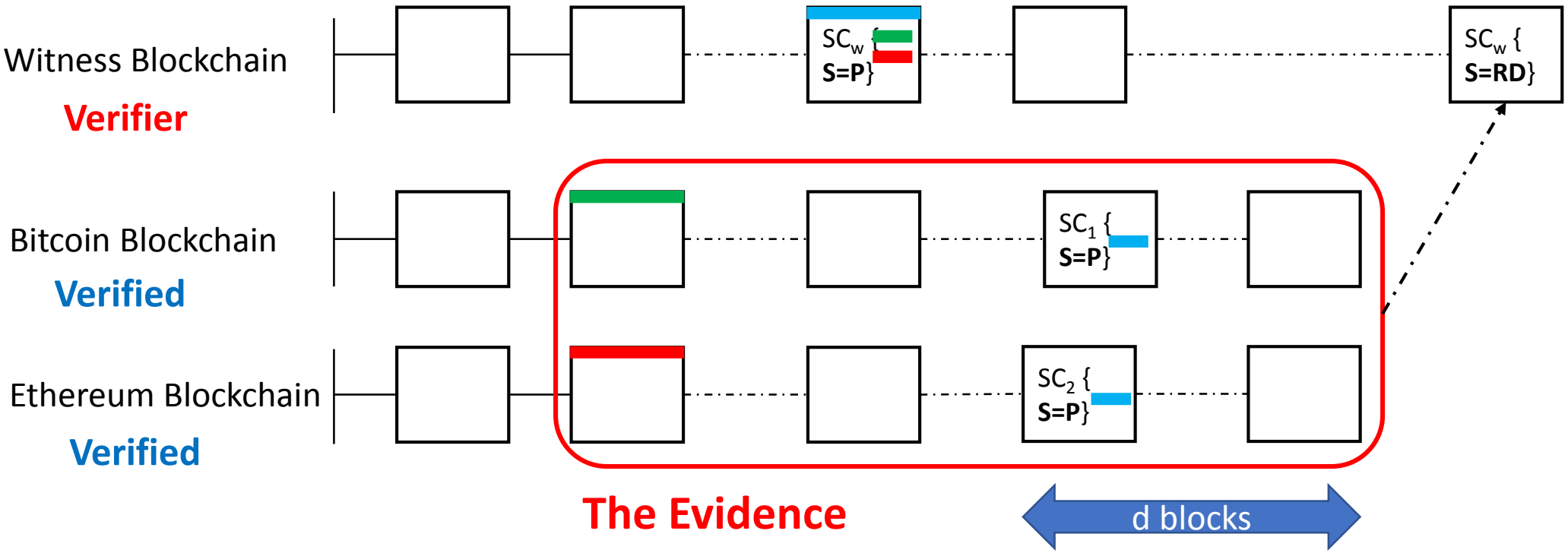
Protocol Sketch Cont'd

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



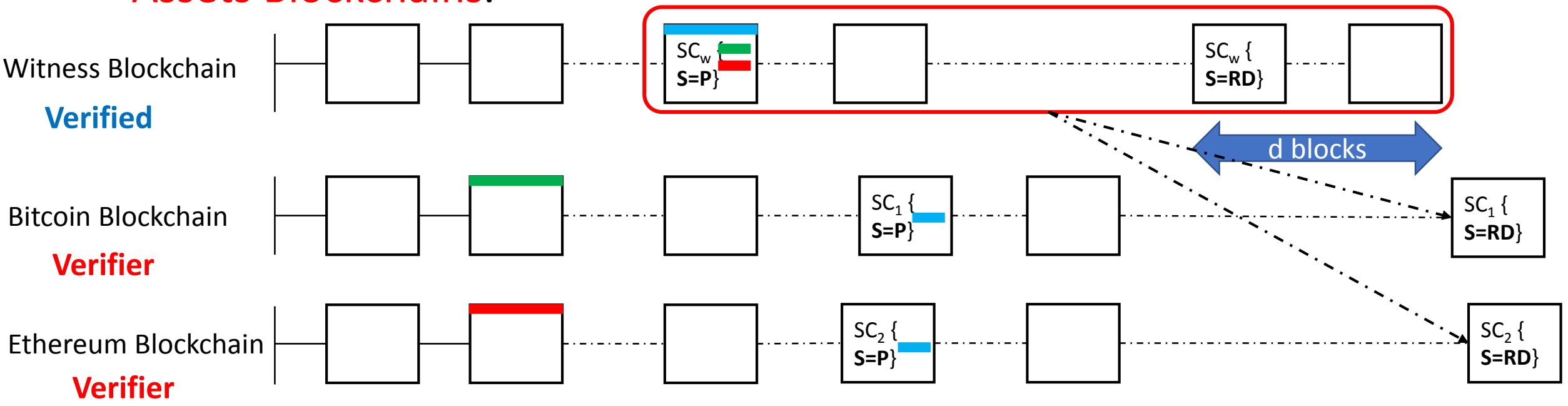
Protocol Sketch Cont'd

- 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

Parting Thoughts

- Building global-scale blockchains is a collective effort.

Distributed Systems

Data Management

Security, Privacy and Crypto

Economics