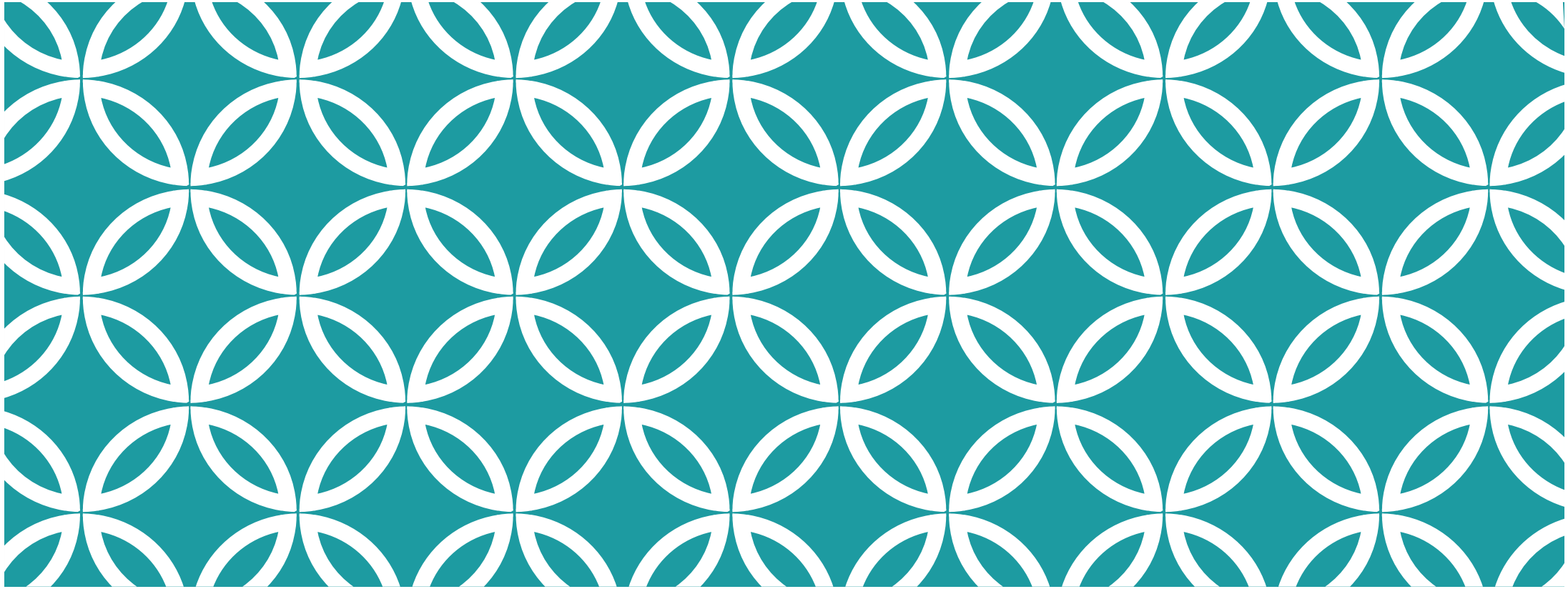
BLOCKCHAINS AND ENERGY

S. Keshav
June 22, 2020
Tutorial and ACM eEnergy '20

OUTLINE

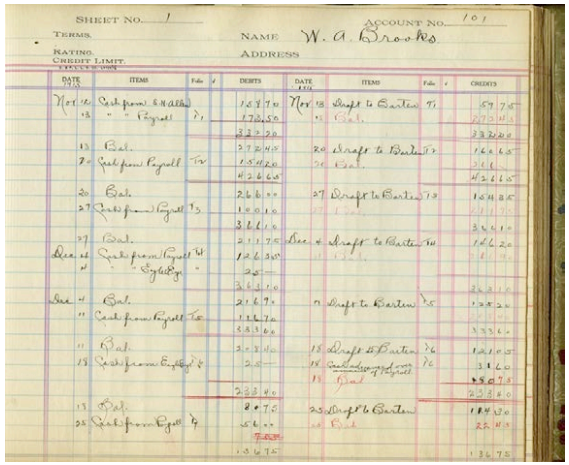
1. Introduction to blockchains
2. Fundamentals of Bitcoin (with kind permission of DSL, UC Santa Barbara)
3. A skeptical look at permissionless blockchains
4. Energy applications
5. Open research areas



INTRODUCTION

WHAT IS A BLOCKCHAIN?

A globally visible ledger that is owned by no one but can be trusted by everyone



WHY BOTHER?

HOW TO BUY A HOT DOG

HOW TO BUY A HOT DOG

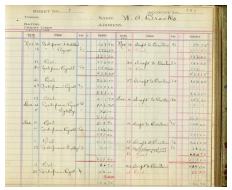
Go to the bank

HOW TO BUY A HOT DOG

Go to the bank

Get $5

- Bank reduces your account balance by $5



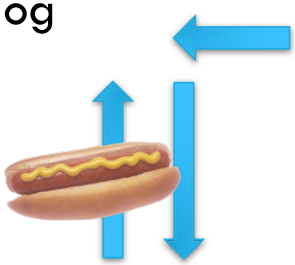
HOW TO BUY A HOT DOG

Go to the bank

Get $5

- Bank reduces your account balance by $5

Pay $5 to vendor and get a hot dog



HOW TO BUY A HOT DOG

Go to the bank

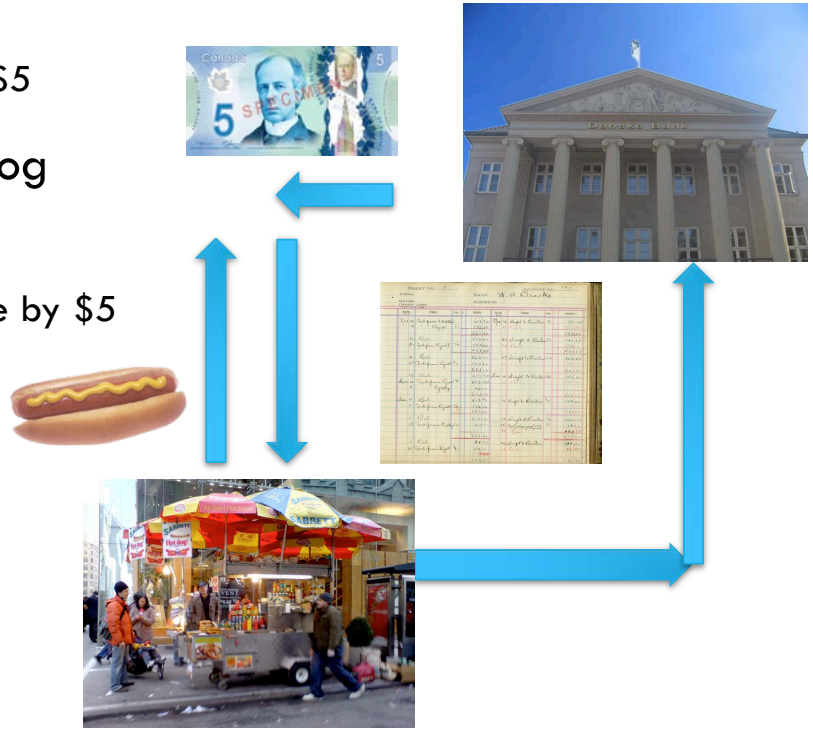
Get $5

- Bank reduces your account balance by $5

Pay $5 to vendor and get a hot dog

Vendor deposits $5

- Bank increases vendor's account balance by $5



HOW TO BUY A HOT DOG

Go to the bank

Get $5

- Bank reduces your account balance by $5

Pay $5 to vendor and get a hot dog

Vendor deposits $5

- Bank increases vendor's account balance by $5

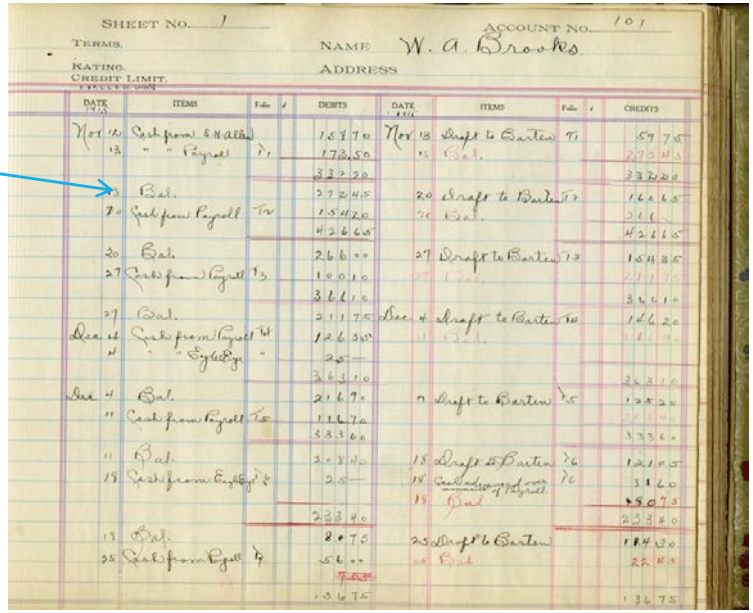
It's all about manipulating a ledger!

- Why bother with bank notes?

BUYING WITH A LEDGER

Transfer hotdog to buyer

Transfer $5 to vendor



SHEET NO. 1 ACCOUNT NO. 101

TERMS. NAME W. A. Brooks

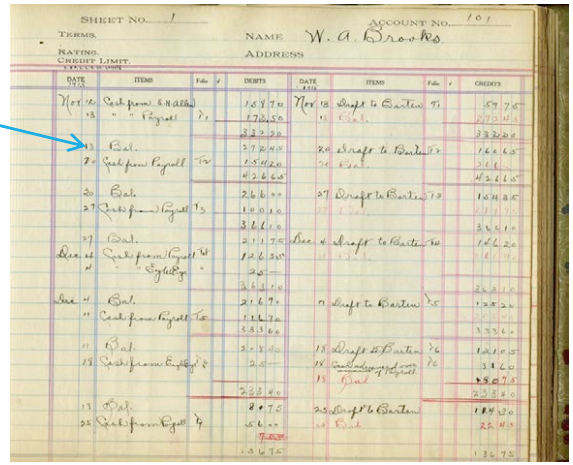
RATING. ADDRESS

CREDIT LIMIT.

DATE	ITEMS	Folio	✓	DEBITS	DATE	ITEMS	Folio	✓	CREDITS
Nov 12	Cash from S. N. Allen			158 70	Nov 13	Draft to Barton	T1		59 75
13	" " Payroll	J1		173 50	13	Bal.			273 45
				332 20					332 20
13	Bal.			272 45	20	Draft to Barton	T2		166 65
20	Cash from Payroll	T2		154 20	20	Bal.			271 [illegible]
				426 65					426 65
20	Bal.			266 00	27	Draft to Barton	T3		154 85
27	Cash from Payroll	T3		100 10	27	Bal.			211 75
				366 10					366 10
27	Bal.			211 75	Dec 4	Draft to Barton	T4		146 20
Dec 4	Cash from Payroll	T4		126 35	4	Bal.			191 90
4	" " Sylvester	"		25 —					
				363 10					363 10
Dec 4	Bal.			216 90	7	Draft to Barton	T5		135 20
7	Cash from Payroll	T5		116 70					81 70
				333 60					333 60
7	Bal.			208 40	18	Draft to Barton	T6		121 05
18	Cash from Sylvester	"		25 —	18	Cash advanced on Payroll	T6		31 60
					18	Bal.			80 75
				233 40					233 40
18	Bal.			80 75	25	Draft to Barton			114 30
25	Cash from Payroll	T7		56 00	25	Bal.			22 45
				136 75					136 75

WHY NOT USE A PRIVATE CURRENCY

Transfer 5 SolarCoins
to vendor



BUT…

What if the ledger is corrupted?

CS TO THE RESCUE

Distribute the ledger

- A copy of the ledger is stored at many servers
- Needs computer networks and distributed databases

CS TO THE RESCUE

Distributed

Transparent

- Everyone can easily validate transactions
  - Though private transactions possible
- Needs cryptographically secure hashes

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

CS TO THE RESCUE

Distributed

Transparent

Immutable

- Once in the ledger, information cannot be changed
- Needs cryptographically secure hashes

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

CS TO THE RESCUE!

Distributed

Transparent

Immutable

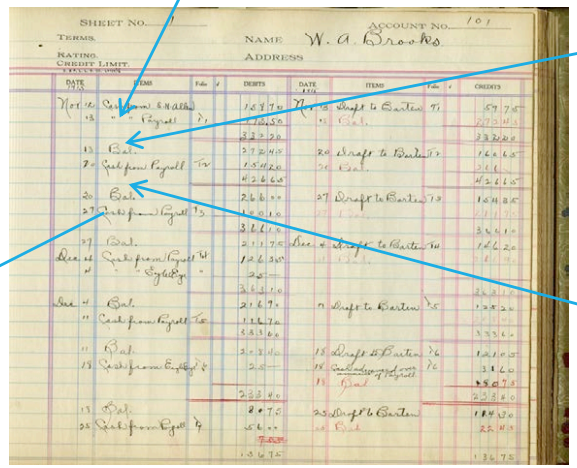
Secure

- Non-repudiable
- Allows a certain fraction of servers to be hacked/become untrusted
- Needs a consensus algorithm

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

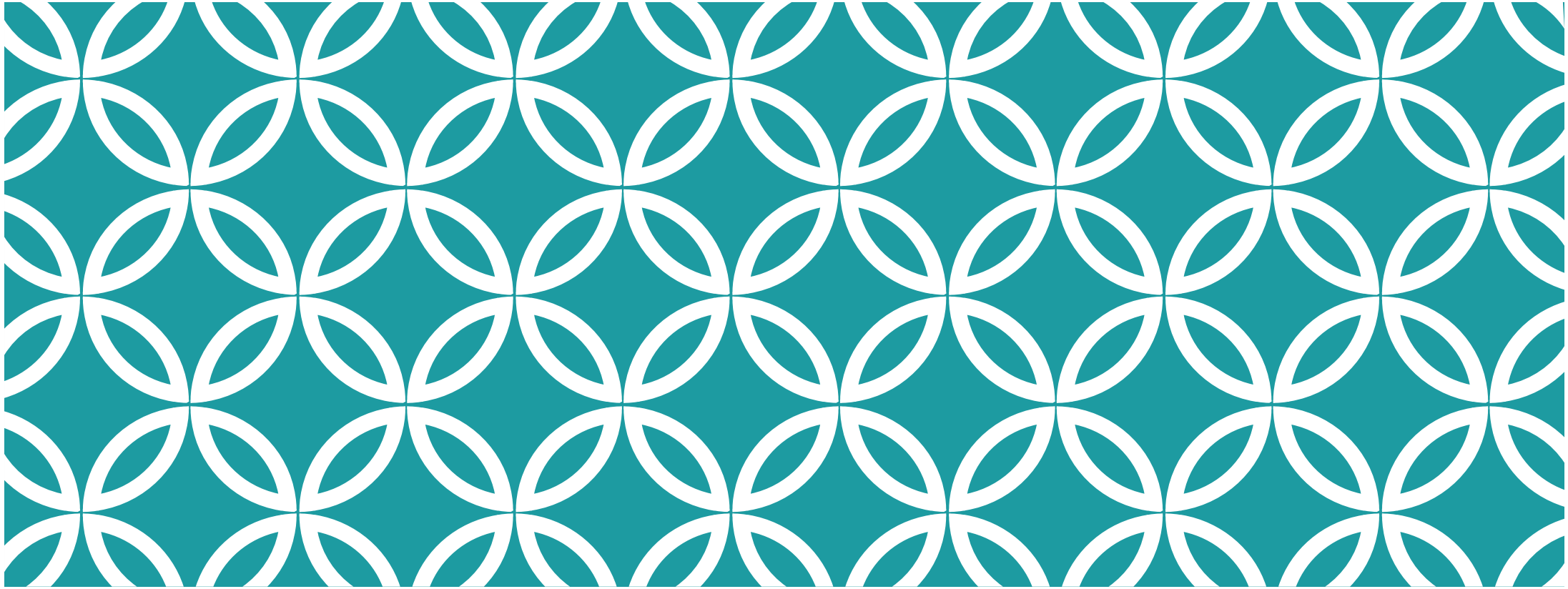
SMART CONTRACTS

"If you receive 1 unit of energy from me, I will get 1 SolarCoin from you"



Needs a sandboxed execution environments

NO NEED FOR A TRUSTED ENTITY!



FUNDAMENTALS

DSL

UCSB

Fundamentals of Blockchains

Sujaya Maiyya, Victor Zakhary, Divyakant Agrawal, Amr El Abbadi

DSL

UCSB

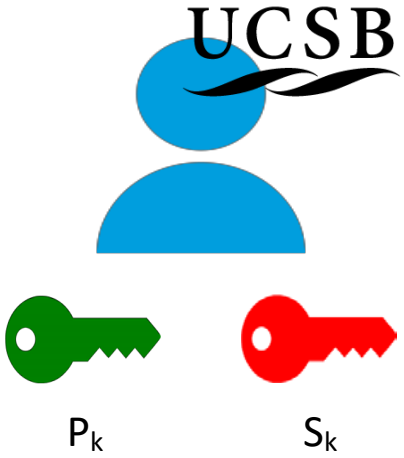
DIGITAL SIGNATURES

DSL

DIGITAL SIGNATURES

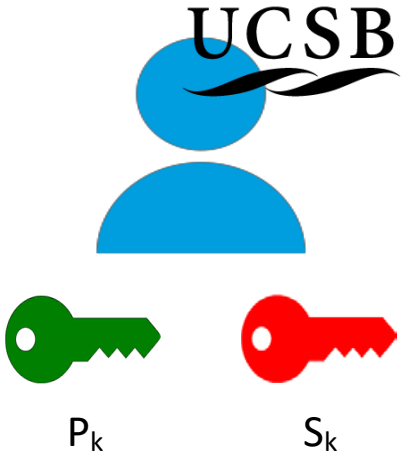
P_k, S_k = Keygen(keysize)

$P_k(S_k(\text{text}) = S_k(P_k(\text{text}))$

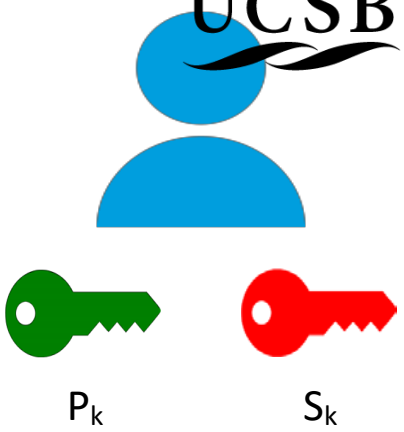


DIGITAL SIGNATURES

- P_k, S_k = Keygen(keysize)
- Your P_k is your identity (username, e-mail address)

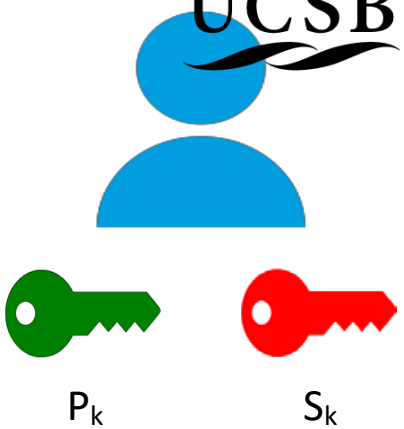


DIGITAL SIGNATURES



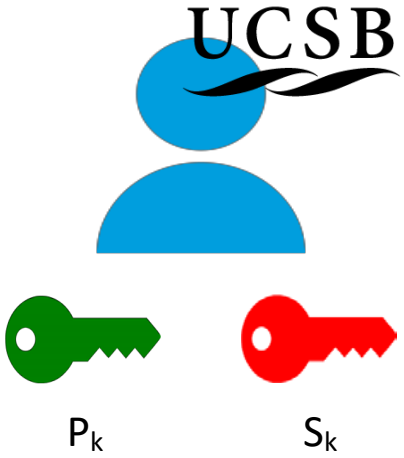
- P_k, S_k = Keygen(keysize)
- Your P_k is your identity (username, e-mail address)
- Your S_k is your signature (password)
- P_k is made public and used to verify documents signed by S_k
- S_k is private

DIGITAL SIGNATURES



- P_k is made public and used to verify documents signed by S_k
- S_k is private

DIGITAL SIGNATURES

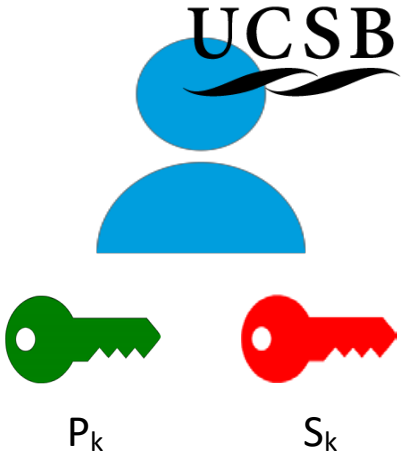


- P_k is made public and used to verify documents signed by S_k
- S_k is private

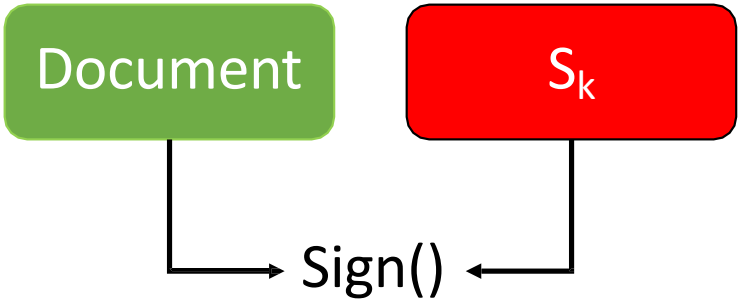
Document

S_k

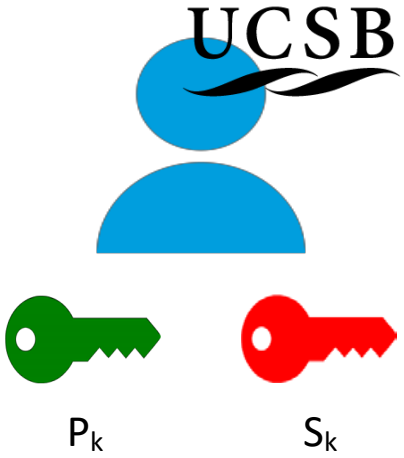
DIGITAL SIGNATURES



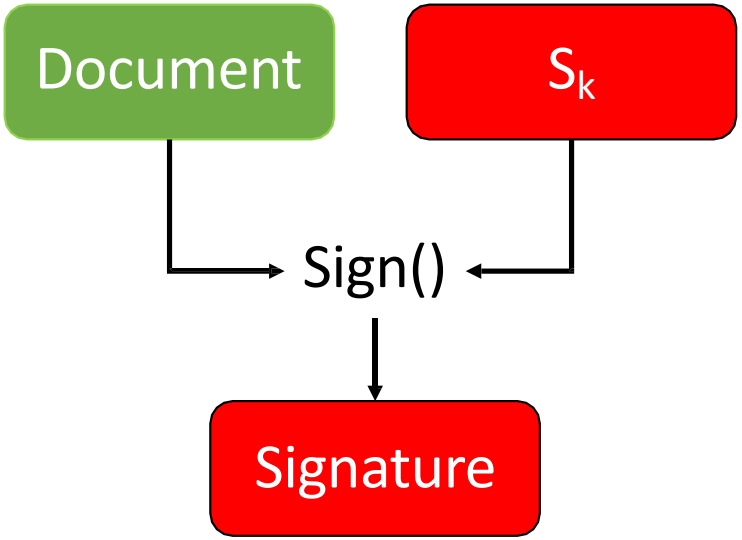
- P_k is made public and used to verify documents signed by S_k
- S_k is private



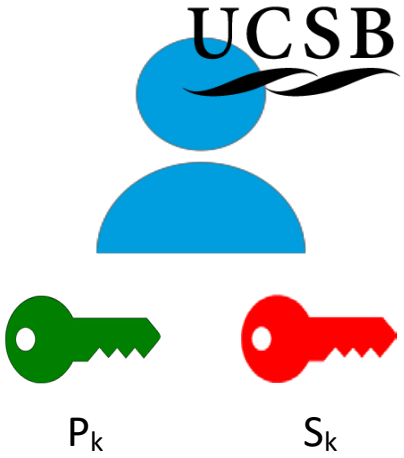
DIGITAL SIGNATURES



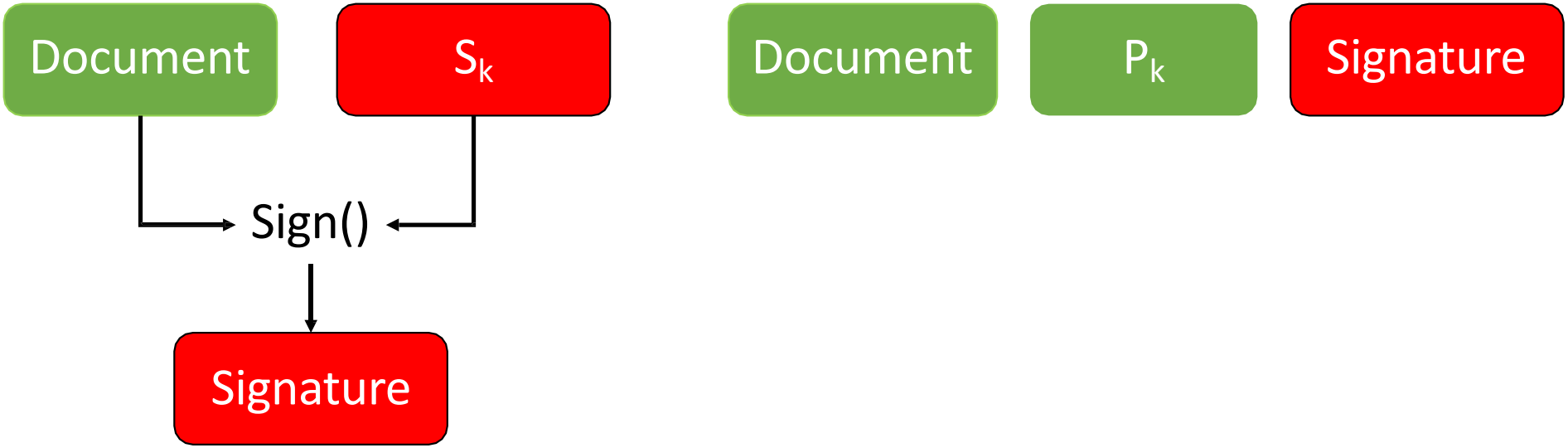
- P_k is made public and used to verify documents signed by S_k
- S_k is private



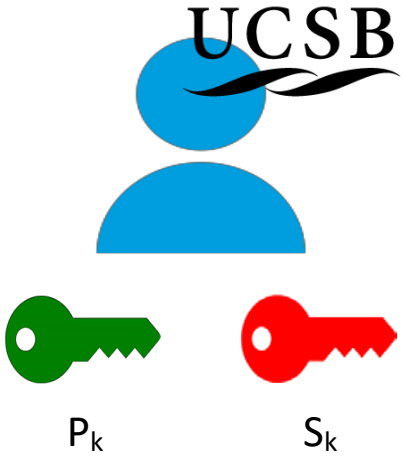
DIGITAL SIGNATURES



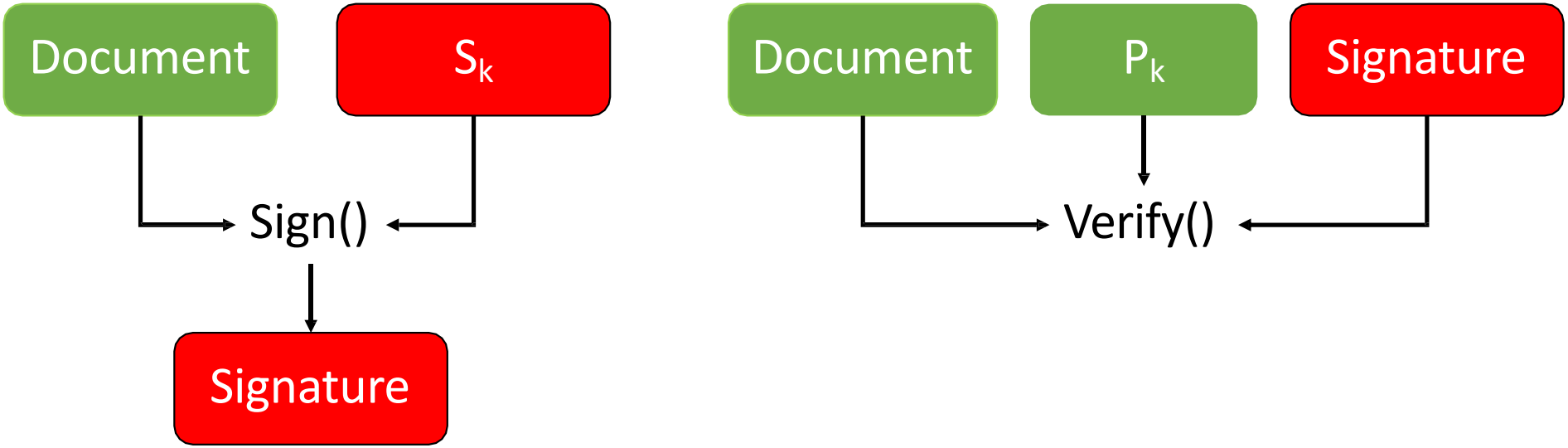
- P_k is made public and used to verify documents signed by S_k
- S_k is private



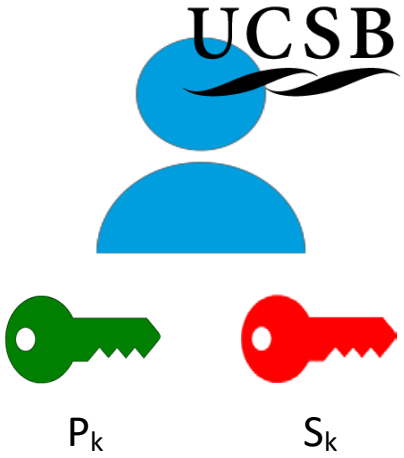
DIGITAL SIGNATURES



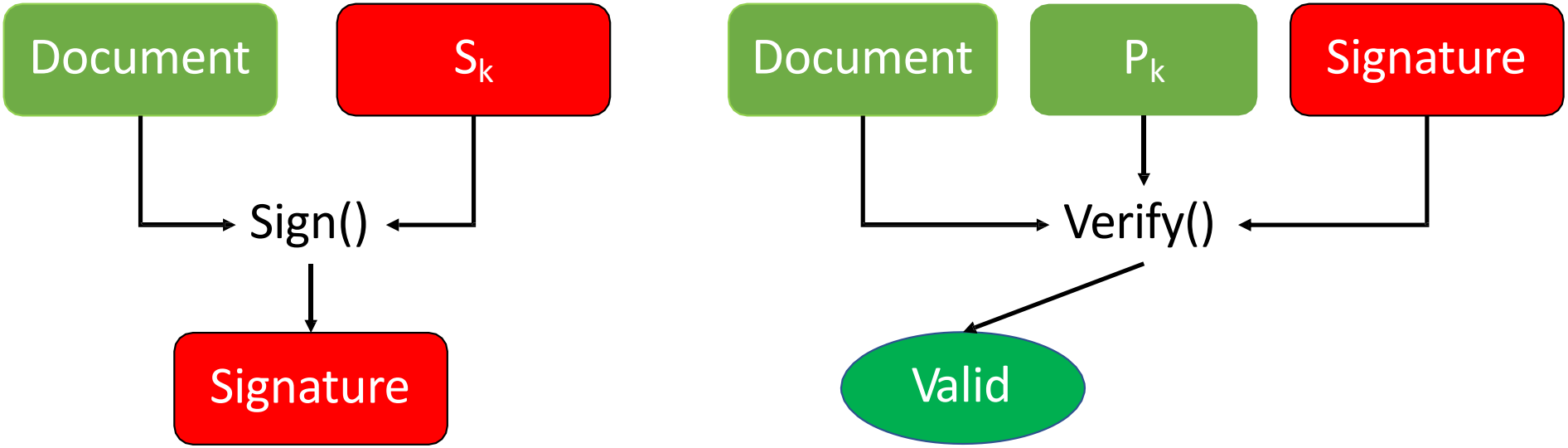
- P_k is made public and used to verify documents signed by S_k
- S_k is private



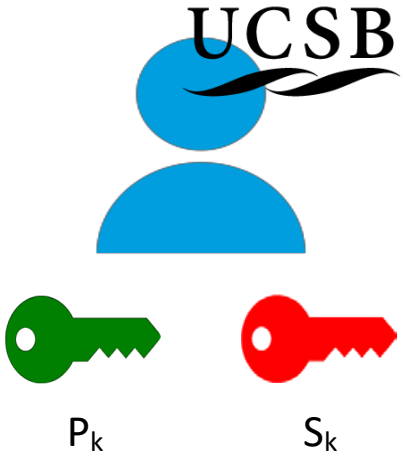
DIGITAL SIGNATURES



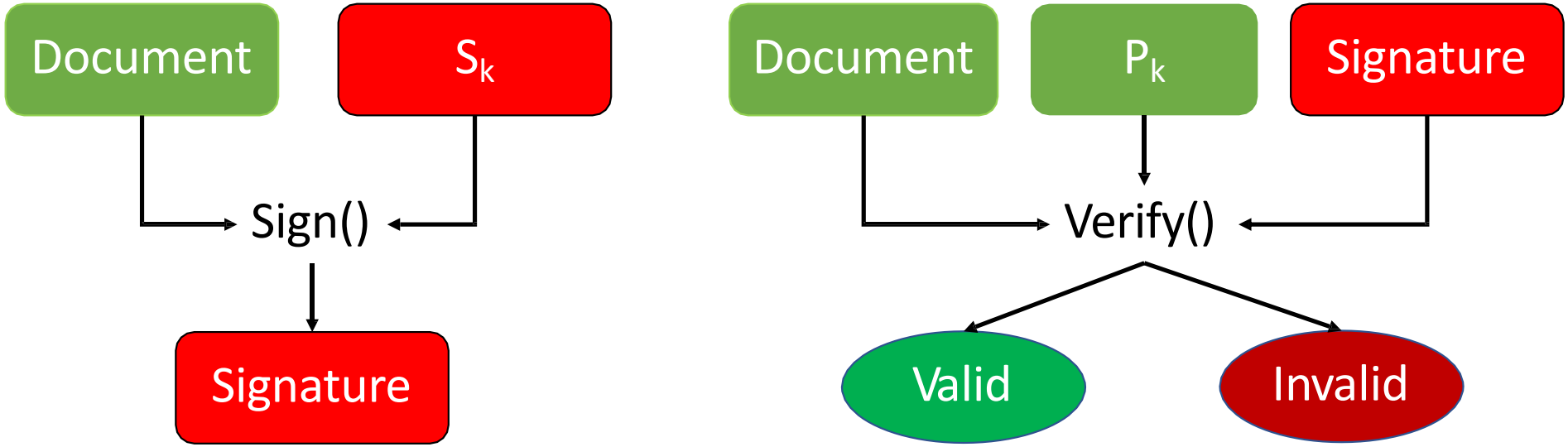
- P_k is made public and used to verify documents signed by S_k
- S_k is private



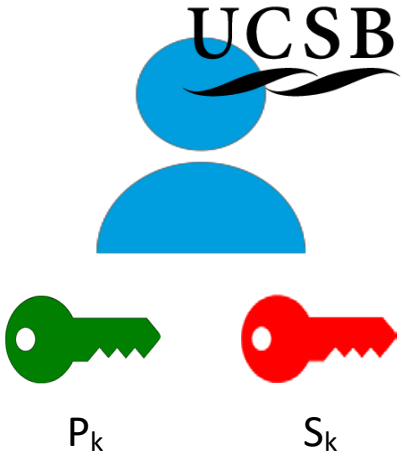
DIGITAL SIGNATURES



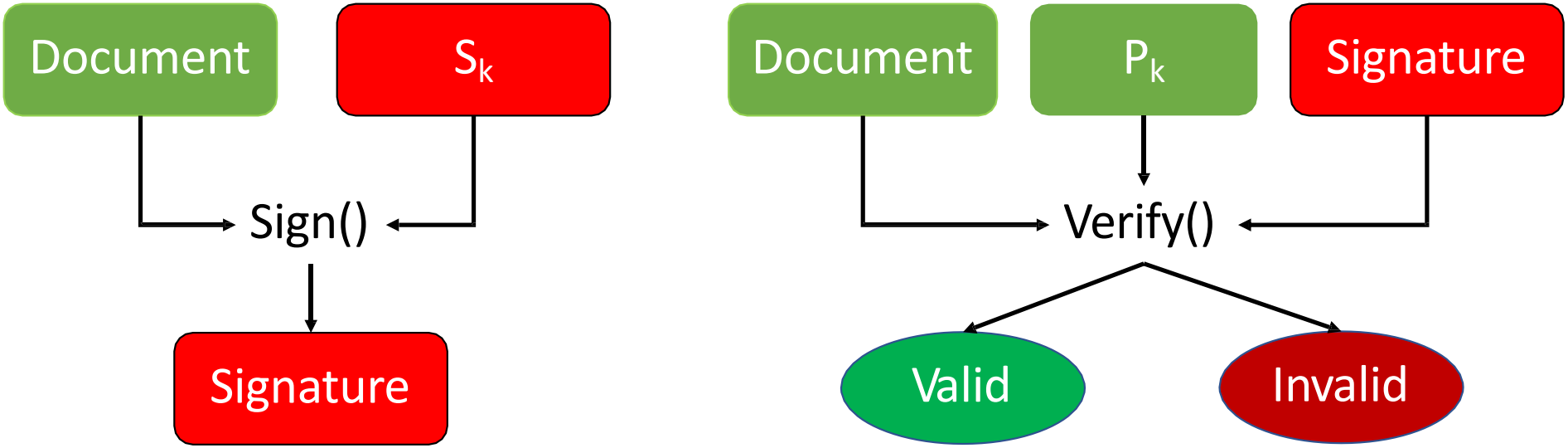
- P_k is made public and used to verify documents signed by S_k
- S_k is private



DIGITAL SIGNATURES



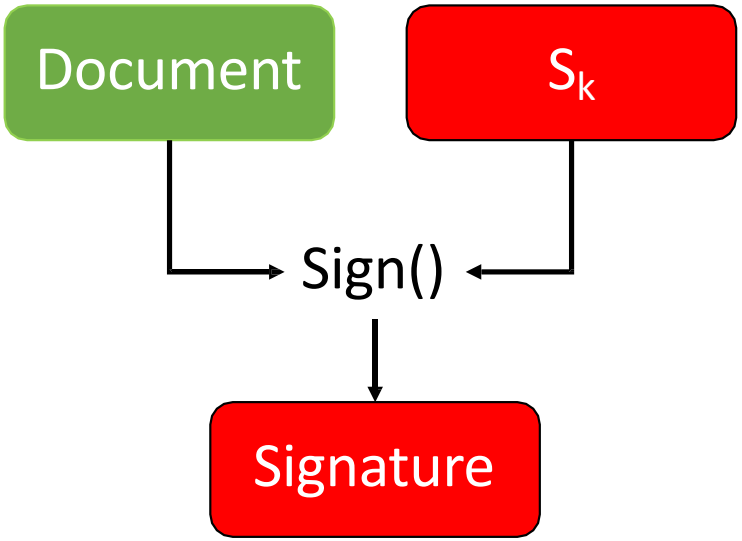
- P_k is made public and used to verify documents signed by S_k
- S_k is private

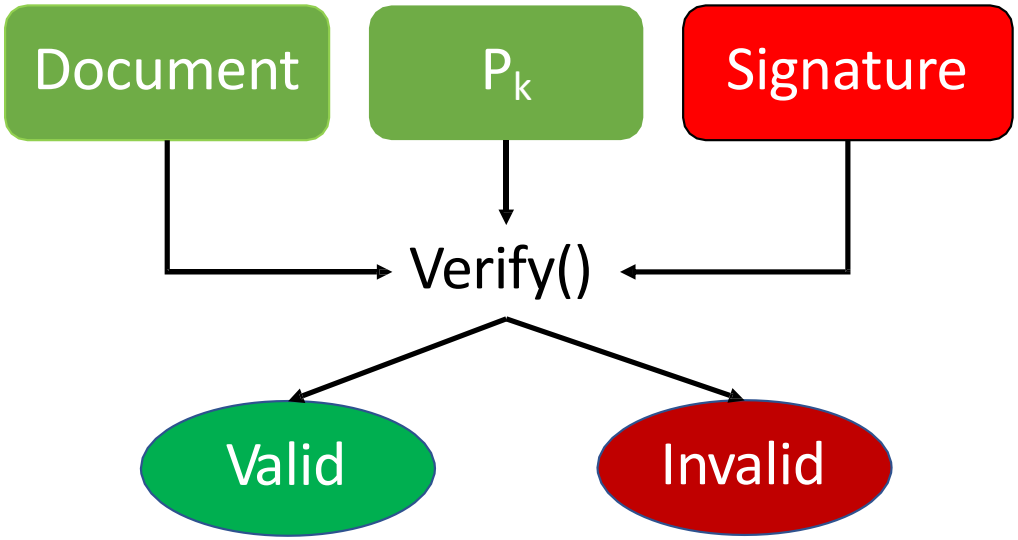


Used for Authentication not privacy

DIGITAL SIGNATURES

- Unique to the signed document
- Mathematically hard to forge
- Mathematically easy to verify





DIGITAL SIGNATURES AND BITCOIN

- A bitcoin is a chain of digital signatures
  - Coin owners digitally sign their coins to transfer them to other recipients

DIGITAL SIGNATURES AND BITCOIN

- A bitcoin is a chain of digital signatures
  - Coin owners digitally sign their coins to transfer them to other recipients
  - Alice wants to move a bitcoin to Bob

DIGITAL SIGNATURES AND BITCOIN

- A bitcoin is a chain of digital signatures
  - Coin owners digitally sign their coins to transfer them to other recipients
  - Alice wants to move a bitcoin to Bob

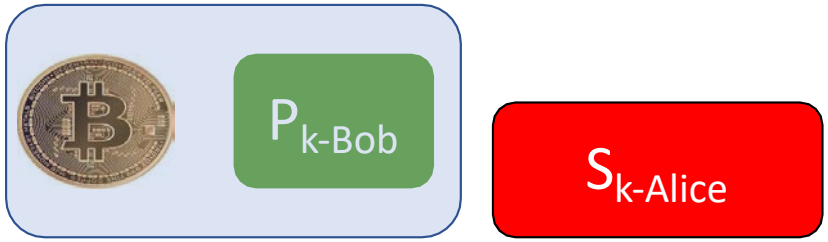
$P_{k\text{-}Bob}$

DIGITAL SIGNATURES AND BITCOIN

- A bitcoin is a chain of digital signatures
  - Coin owners digitally sign their coins to transfer them to other recipients
  - Alice wants to move a bitcoin to Bob

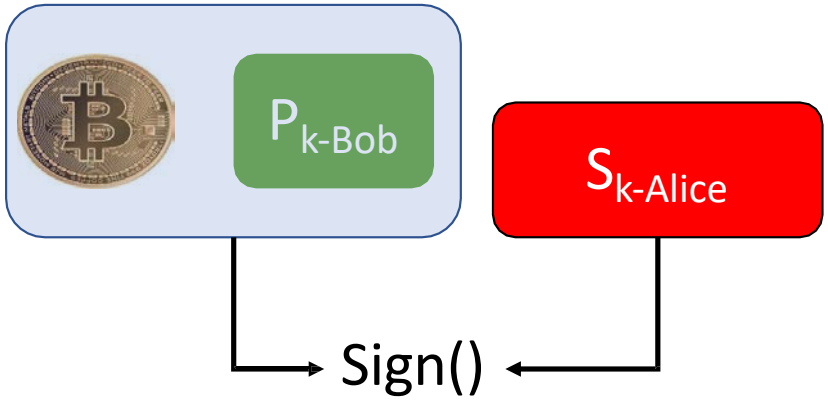
DIGITAL SIGNATURES AND BITCOIN

- A bitcoin is a chain of digital signatures
  - Coin owners digitally sign their coins to transfer them to other recipients
  - Alice wants to move a bitcoin to Bob



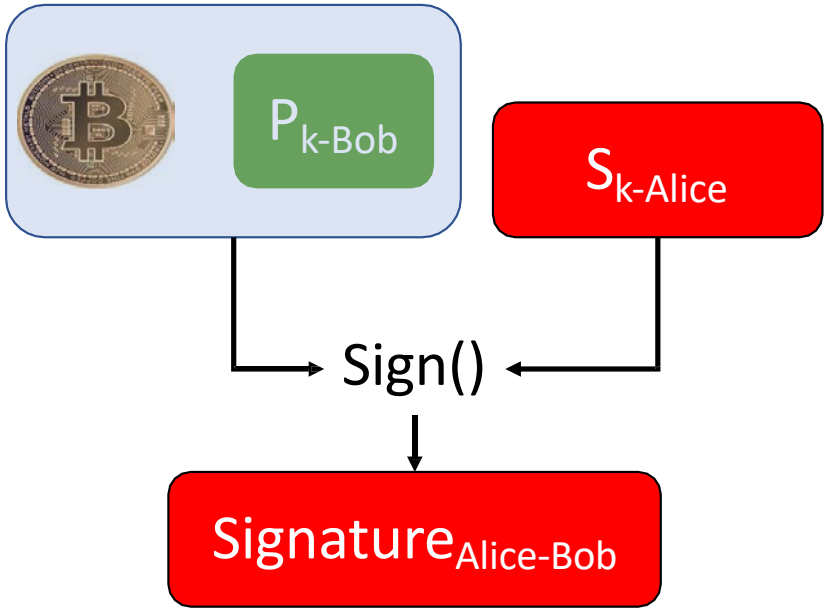
DIGITAL SIGNATURES AND BITCOIN

- A bitcoin is a chain of digital signatures
  - Coin owners digitally sign their coins to transfer them to other recipients
  - Alice wants to move a bitcoin to Bob



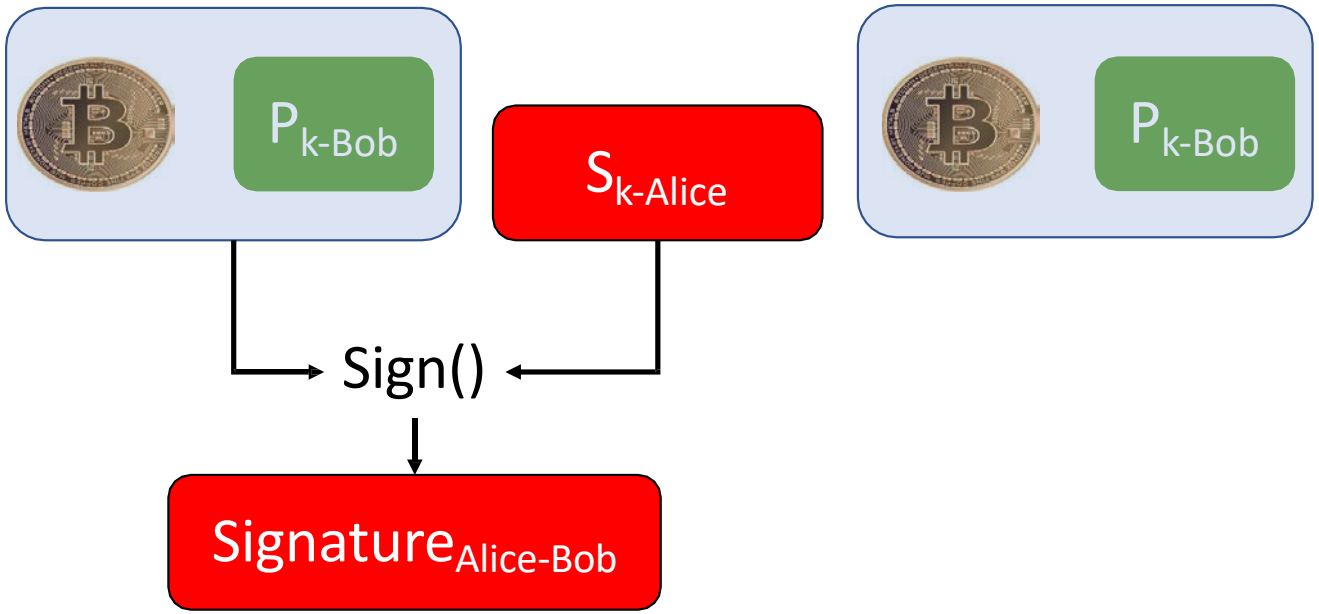
DIGITAL SIGNATURES AND BITCOIN

- A bitcoin is a chain of digital signatures
  - Coin owners digitally sign their coins to transfer them to other recipients
  - Alice wants to move a bitcoin to Bob



DIGITAL SIGNATURES AND BITCOIN

- A bitcoin is a chain of digital signatures
  - Coin owners digitally sign their coins to transfer them to other recipients
  - Alice wants to move a bitcoin to Bob

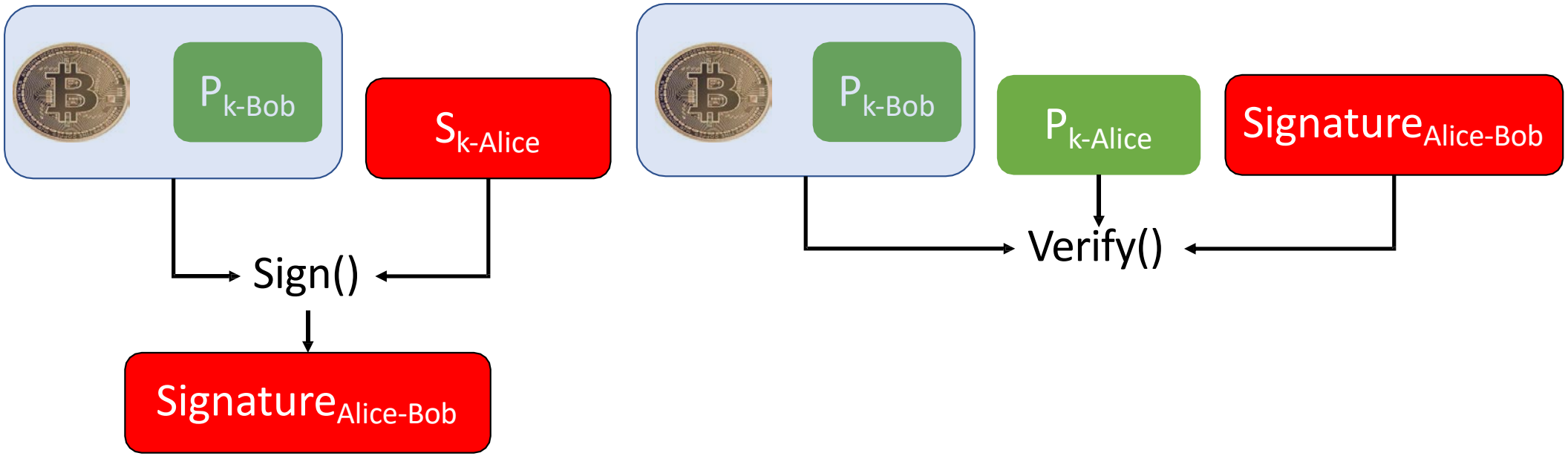


DIGITAL SIGNATURES AND BITCOIN

- A bitcoin is a chain of digital signatures
  - Coin owners digitally sign their coins to transfer them to other recipients
  - Alice wants to move a bitcoin to Bob

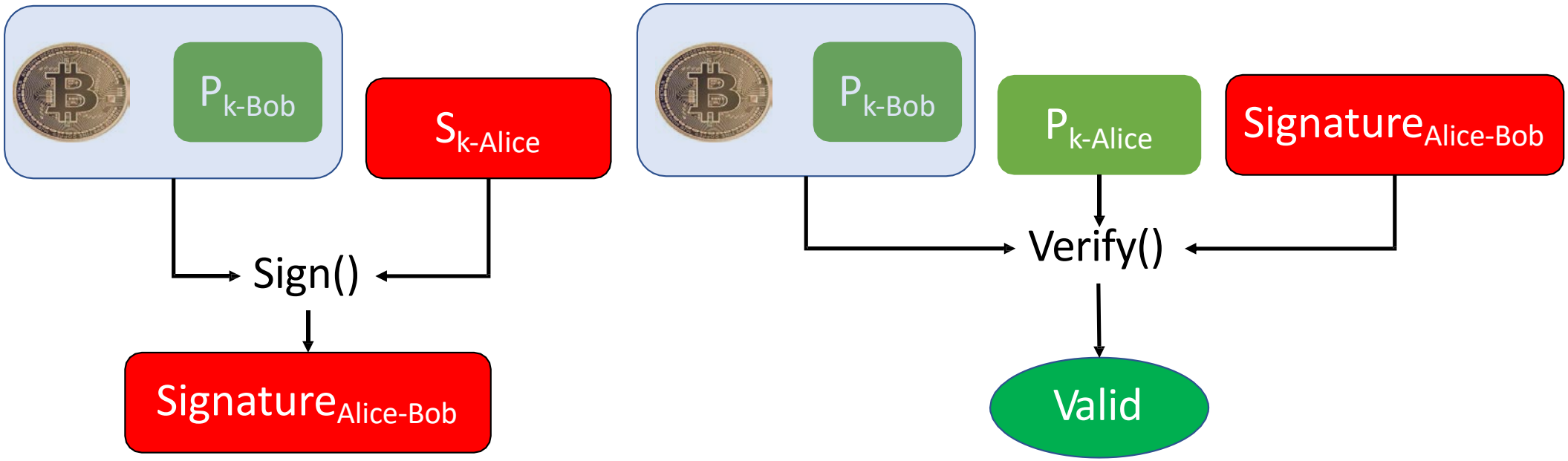
DIGITAL SIGNATURES AND BITCOIN

- A bitcoin is a chain of digital signatures
  - Coin owners digitally sign their coins to transfer them to other recipients
  - Alice wants to move a bitcoin to Bob



DIGITAL SIGNATURES AND BITCOIN

- A bitcoin is a chain of digital signatures
  - Coin owners digitally sign their coins to transfer them to other recipients
  - Alice wants to move a bitcoin to Bob



Digital Signatures and Bitcoin

- Now what if Bob wants to move his coins to Diana

DIGITAL SIGNATURES AND BITCOIN

- Now what if Bob wants to move his coins to Diana

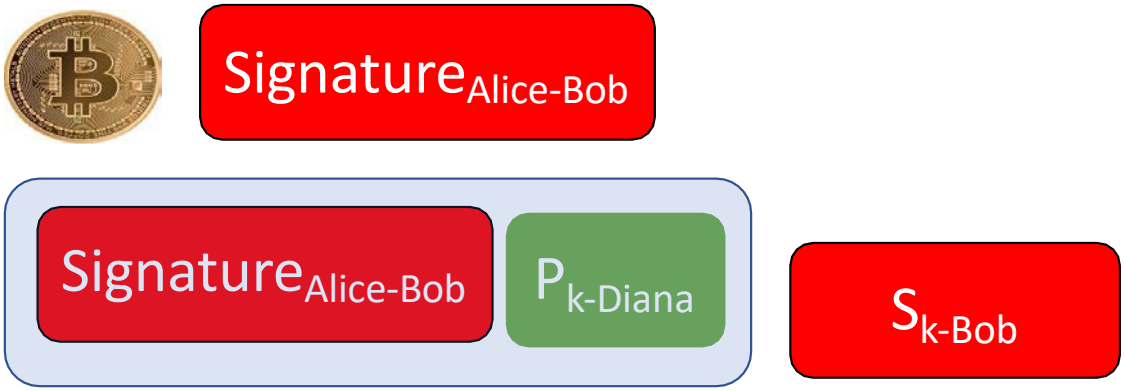
$\text{Signature}_{\text{Alice-Bob}}$

DIGITAL SIGNATURES AND BITCOIN

- Now what if Bob wants to move his coins to Diana

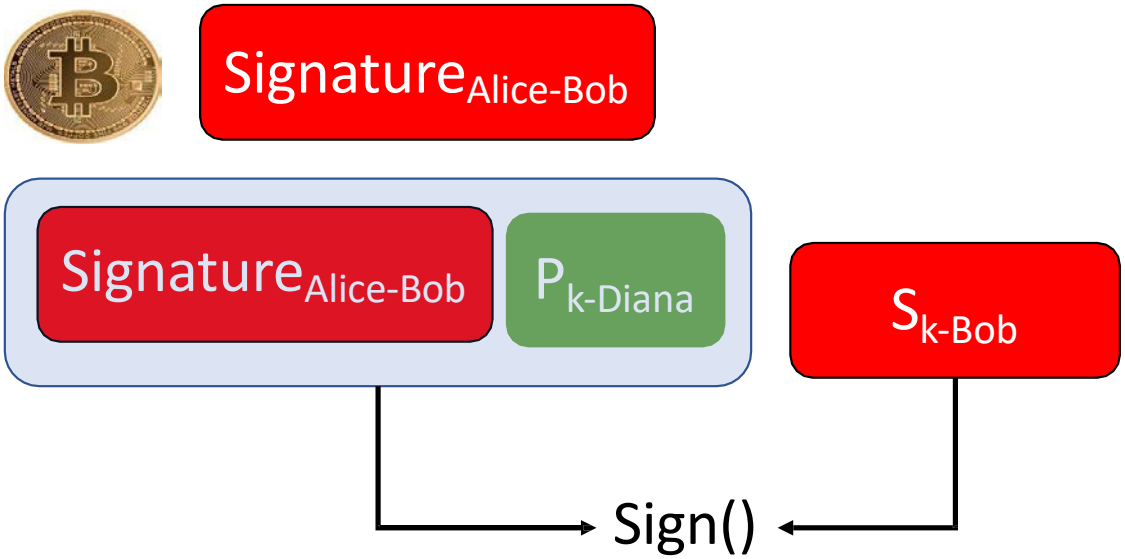
DIGITAL SIGNATURES AND BITCOIN

- Now what if Bob wants to move his coins to Diana



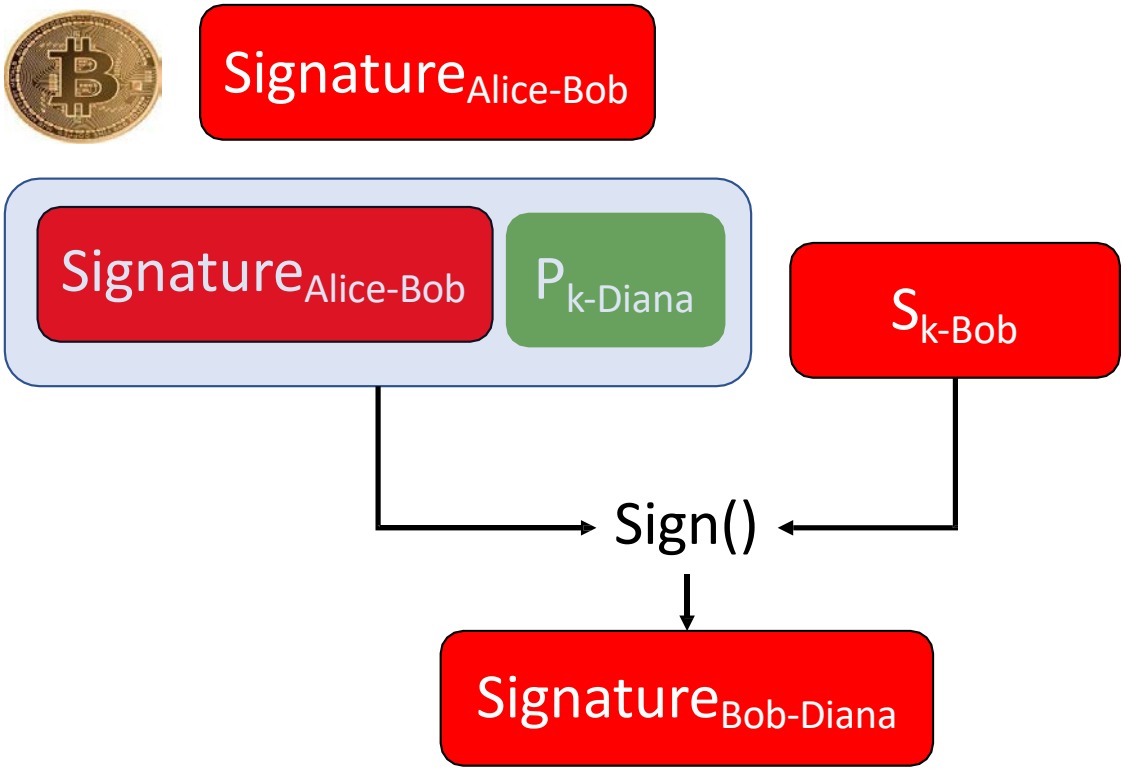
DIGITAL SIGNATURES AND BITCOIN

- Now what if Bob wants to move his coins to Diana



DIGITAL SIGNATURES AND BITCOIN

- Now what if Bob wants to move his coins to Diana



A BITCOIN BIG PICTURE

A Bitcoin Big Picture

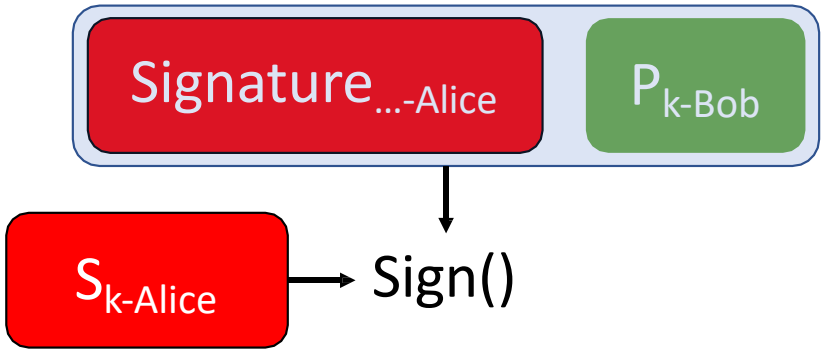
Signature$_{\ldots\text{-Alice}}$

A BITCOIN BIG PICTURE

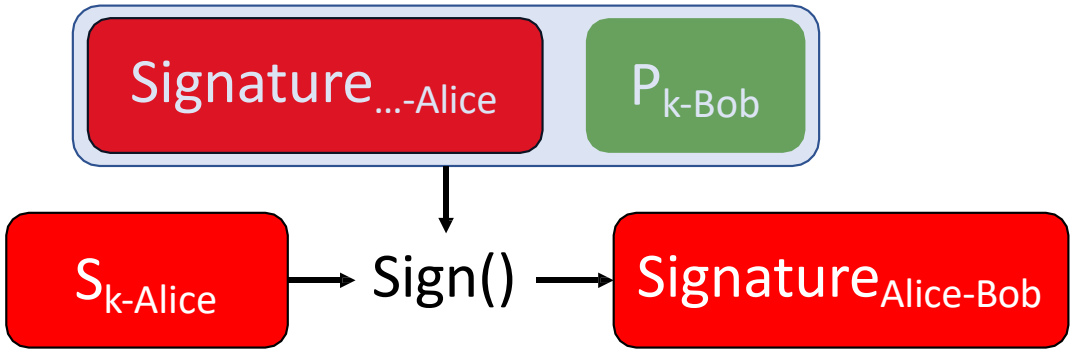
Signature$_{\ldots\text{-Alice}}$

$P_{k\text{-Bob}}$

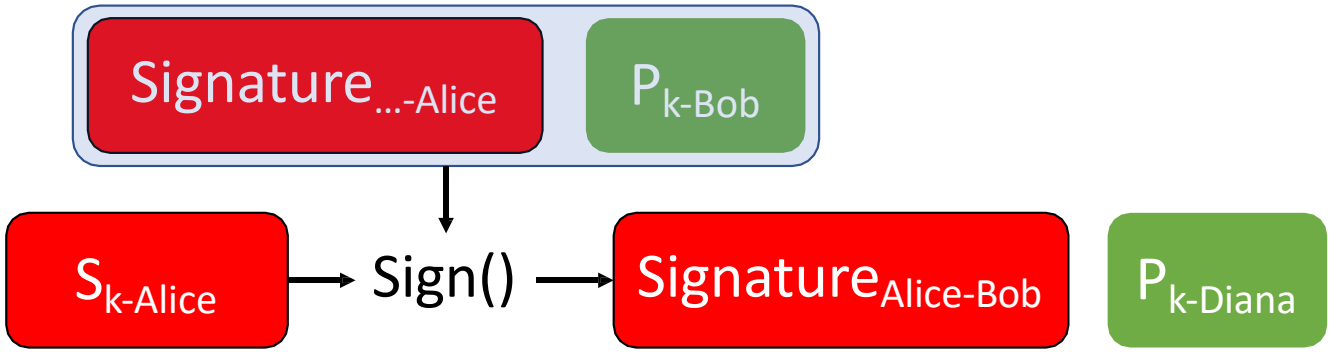
A BITCOIN BIG PICTURE



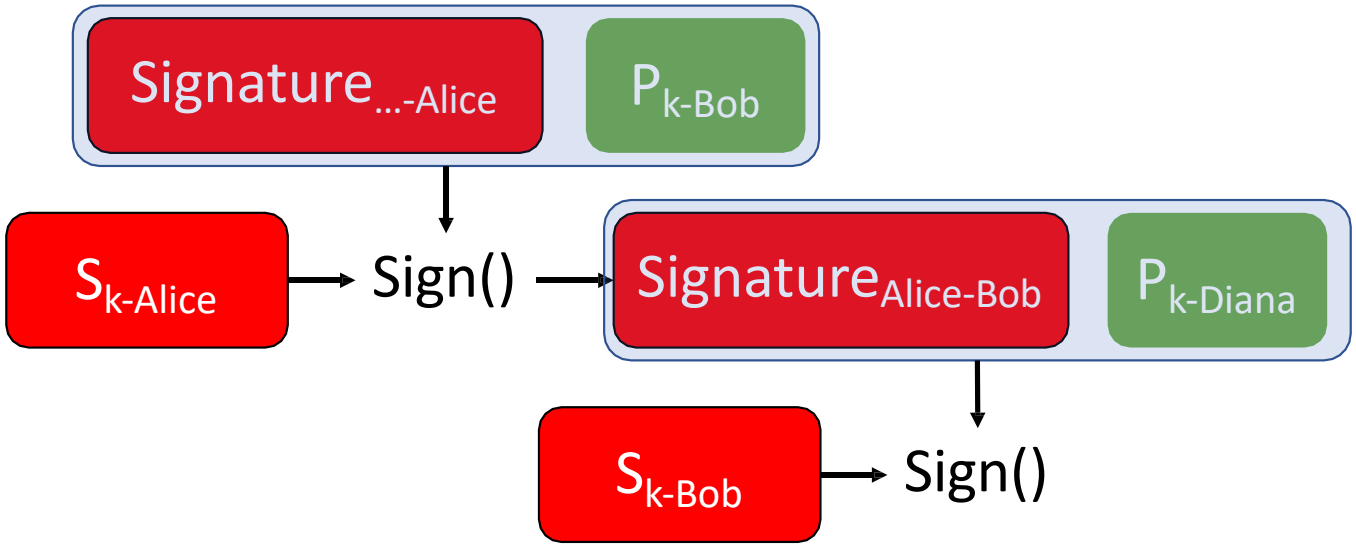
A BITCOIN BIG PICTURE



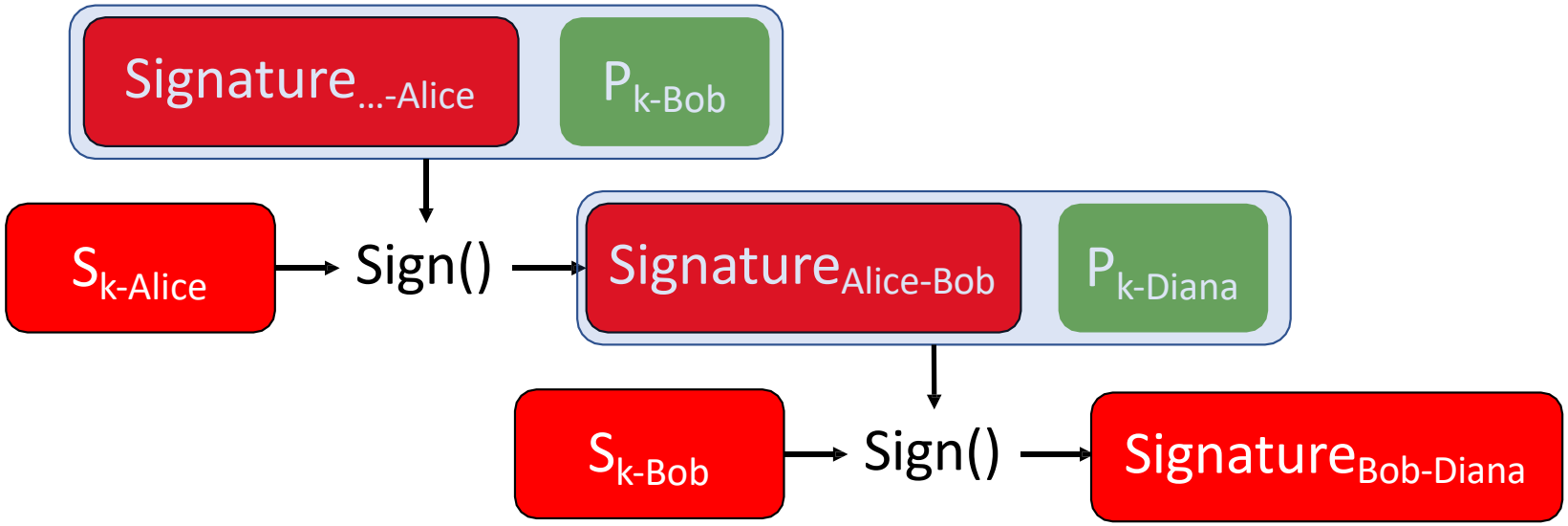
A BITCOIN BIG PICTURE



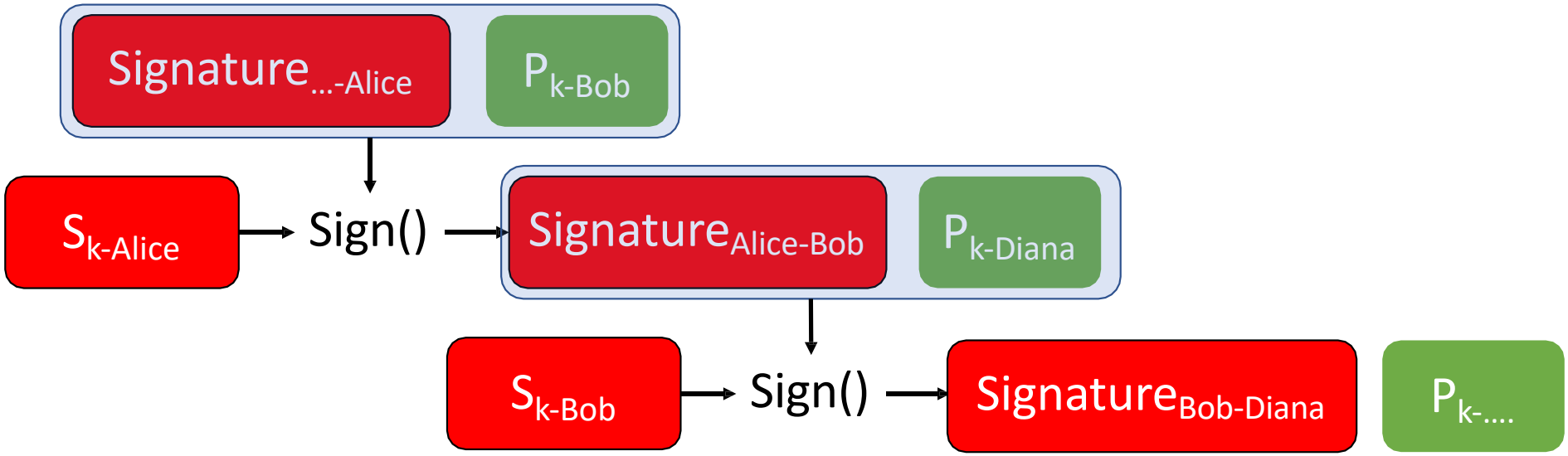
A BITCOIN BIG PICTURE



A BITCOIN BIG PICTURE



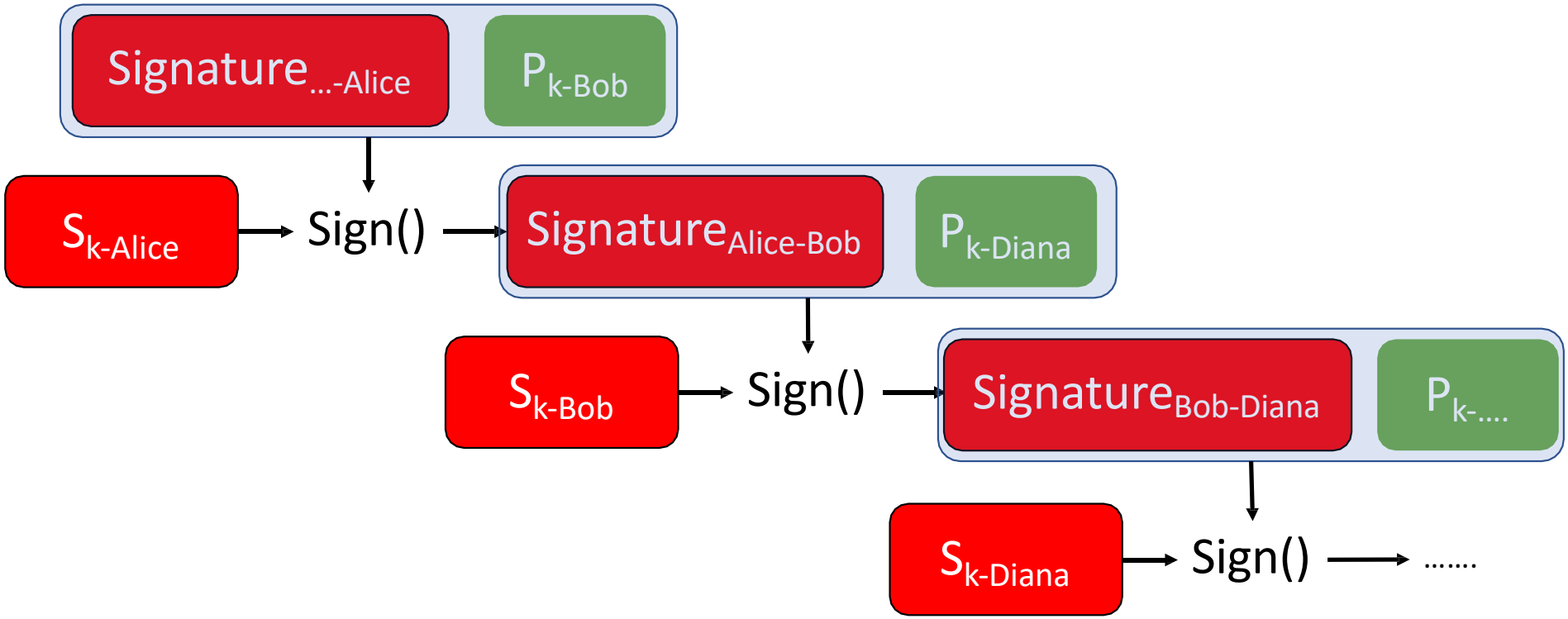
A BITCOIN BIG PICTURE



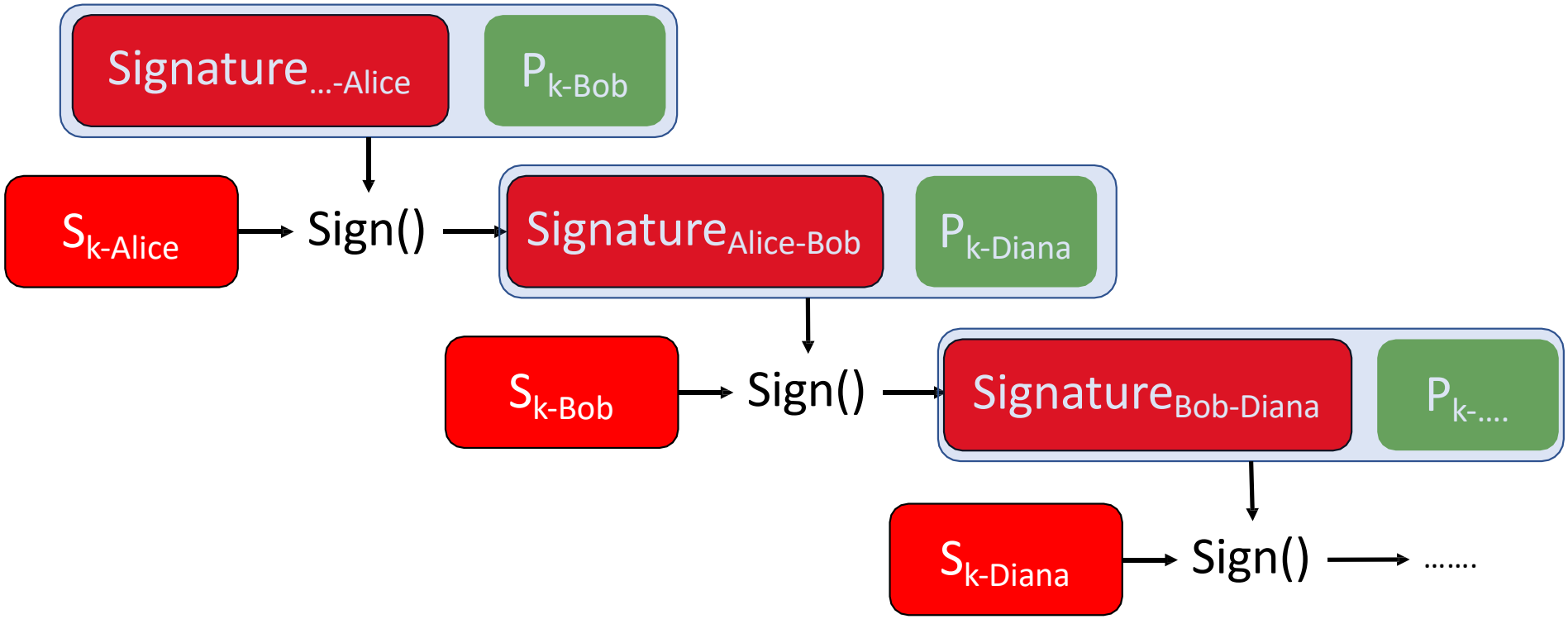
DSL

UCSB

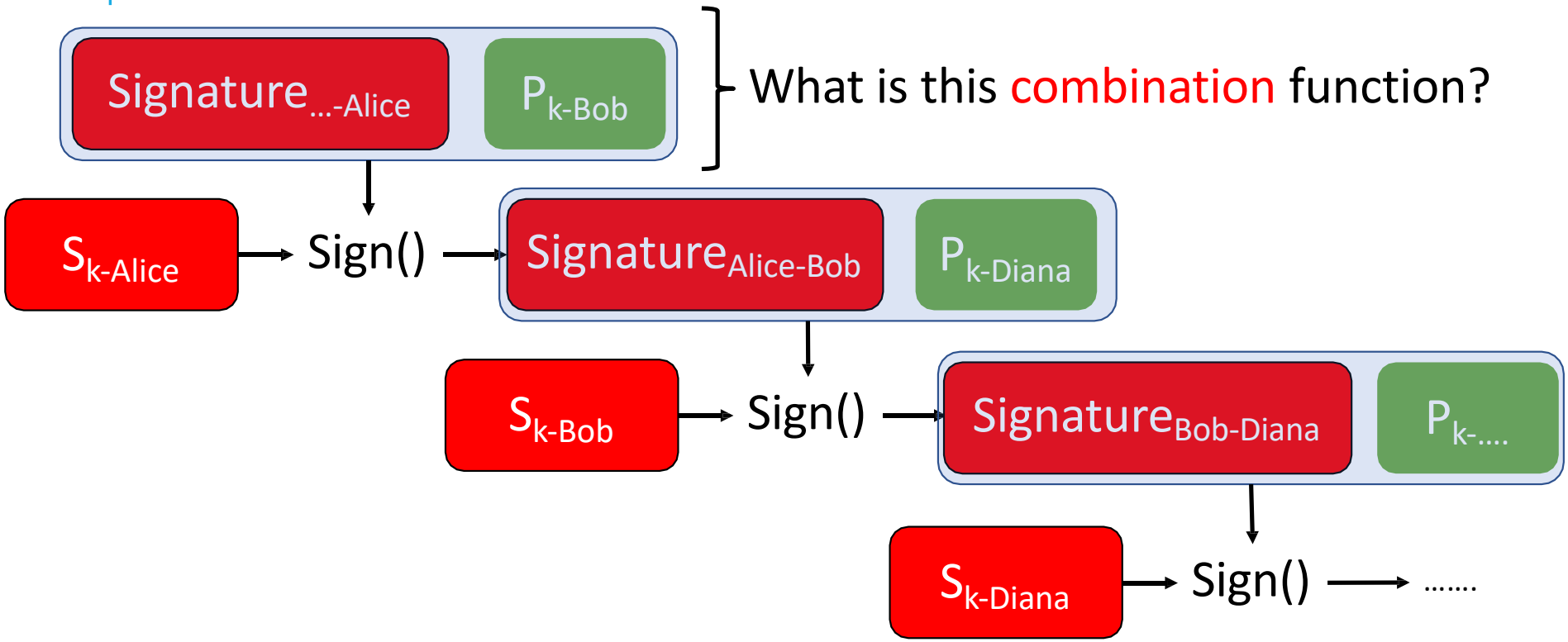
A BITCOIN BIG PICTURE



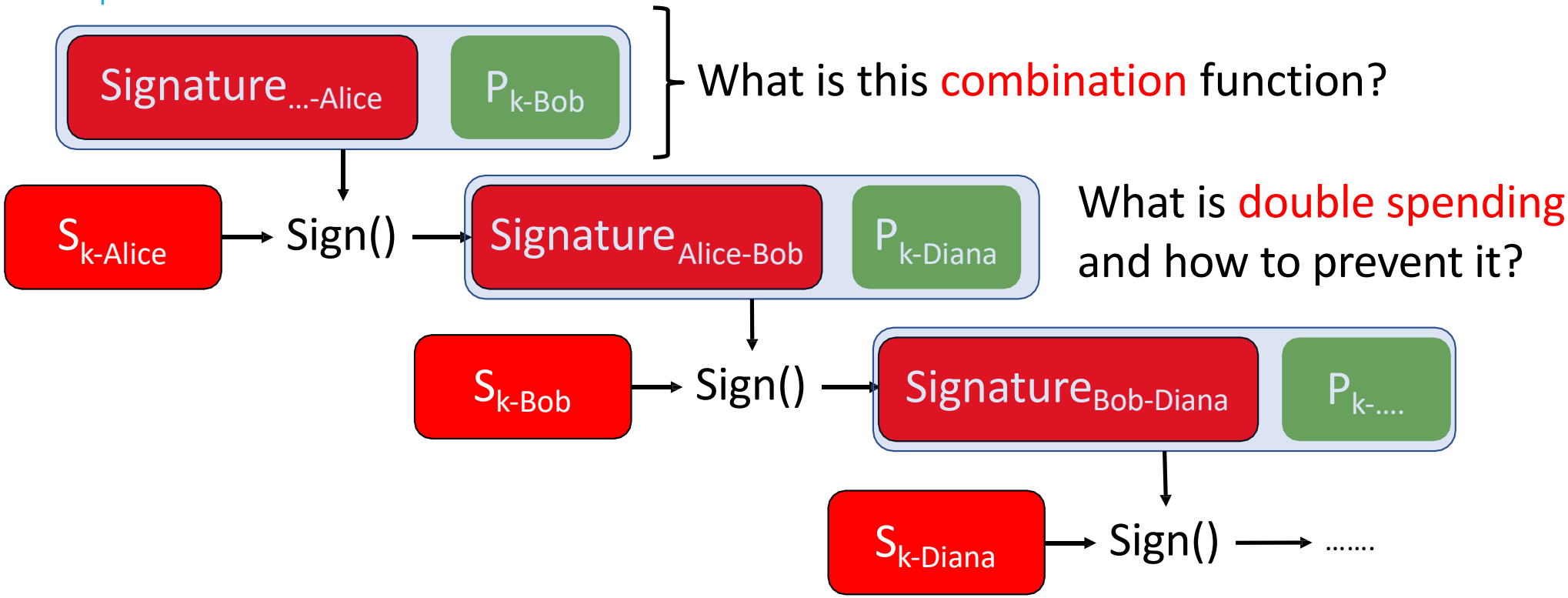
WHAT ABOUT'S?


Signature...-Alice
Pk-Bob
Sk-Alice
Sign()
SignatureAlice-Bob
Pk-Diana
Sk-Bob
Sign()
SignatureBob-Diana
Pk-....
Sk-Diana
Sign()
.....

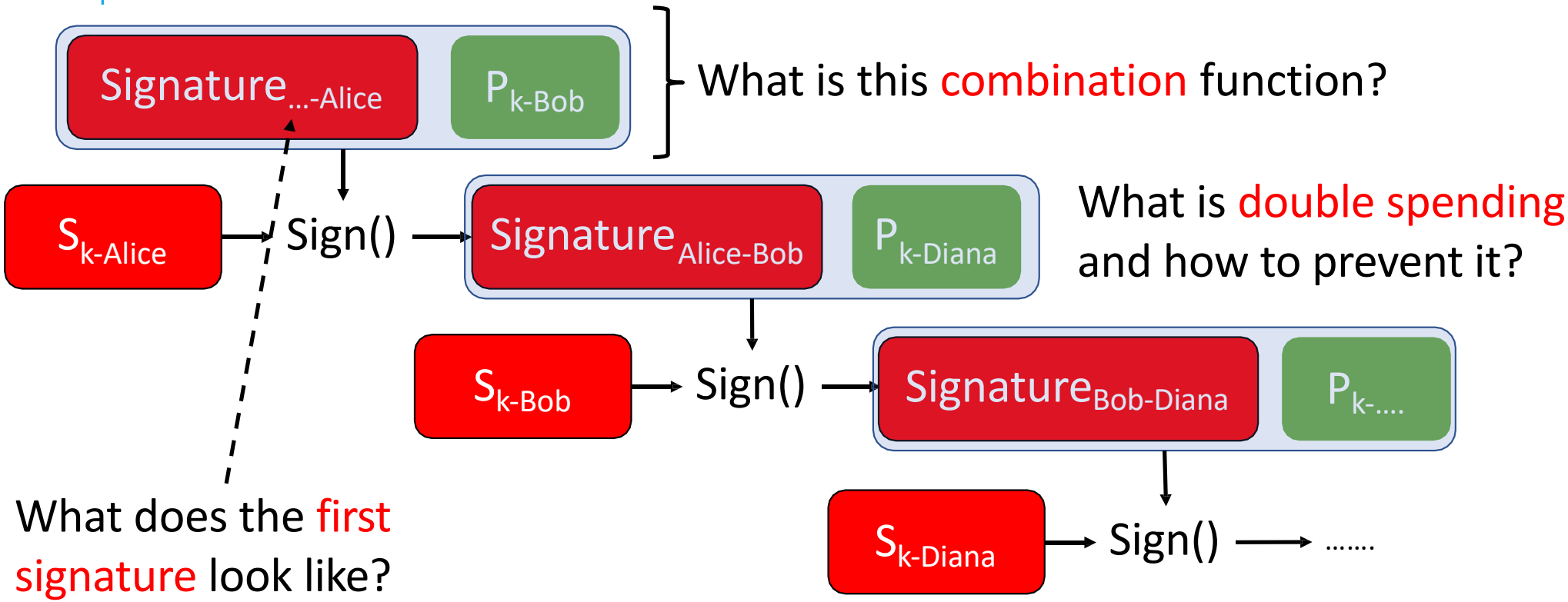
WHAT ABOUT'S?


Signature...-Alice
Pk-Bob
What is this combination function?
Sk-Alice
Sign()
SignatureAlice-Bob
Pk-Diana
Sk-Bob
Sign()
SignatureBob-Diana
Pk-....
Sk-Diana
Sign()
.....

WHAT ABOUT'S?


Signature...-Alice
Pk-Bob
What is this combination function?
Sk-Alice
Sign()
Signature Alice-Bob
Pk-Diana
What is double spending and how to prevent it?
Sk-Bob
Sign()
Signature Bob-Diana
Pk-....
Sk-Diana
Sign()
.....

WHAT ABOUT'S?


Signature...-Alice
Pk-Bob
What is this combination function?
Sk-Alice
Sign()
Signature Alice-Bob
Pk-Diana
What is double spending and how to prevent it?
Sk-Bob
Sign()
Signature Bob-Diana
Pk-....
Sk-Diana
Sign()
.....
What does the first signature look like?

HASHING H(X)

Hashing H(x)

- Signatures and public keys are combined using Hashing

HASHING H(X)

- Signatures and public keys are combined using Hashing
- Takes **any** string x **of any length** as input
- **Fixed** output size (e.g., 256 bits)

HASHING H(X)

- Signatures and public keys are combined using Hashing
- Takes **any** string x **of any length** as input
- **Fixed** output size (e.g., 256 bits)
- Efficiently computable.
- **Satisfies:**
  - Collision Free: no two x, y s.t. H(x) = H(y)
    - Message digest.
  - Hiding: Given H(x) infeasible to find x (one-way hash function)
    - Commitment: commit to a value and reveal later
  - Puzzle Friendly: Given a random puzzle ID and a target **set** Y it is hard to find x such that: H(ID | x) ε Y

BITCOIN USES SHA-256

BITCOIN USES SHA-256

$\text{Signature}_{\text{Alice-Bob}}$ $P_{\text{k-Diana}}$

SHA256($\text{Signature}_{\text{Alice-Bob}}$ || $P_{\text{k-Diana}}$) =
256-bit (32-byte) unique string

BITCOIN USES SHA-256

$\text{Signature}_{\text{Alice-Bob}}$ $P_{\text{k-Diana}}$

SHA256($\text{Signature}_{\text{Alice-Bob}}$ || $P_{\text{k-Diana}}$) =

256-bit (32-byte) unique string

BITCOIN USES SHA-256

$\text{Signature}_{\text{Alice-Bob}}$ $P_{\text{k-Diana}}$

SHA256($\text{Signature}_{\text{Alice-Bob}}$ || $P_{\text{k-Diana}}$) =

256-bit (32-byte) unique string

SHA256(abc) =
ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad

BITCOIN USES SHA-256

$\text{Signature}_{\text{Alice-Bob}}$ $P_{\text{k-Diana}}$

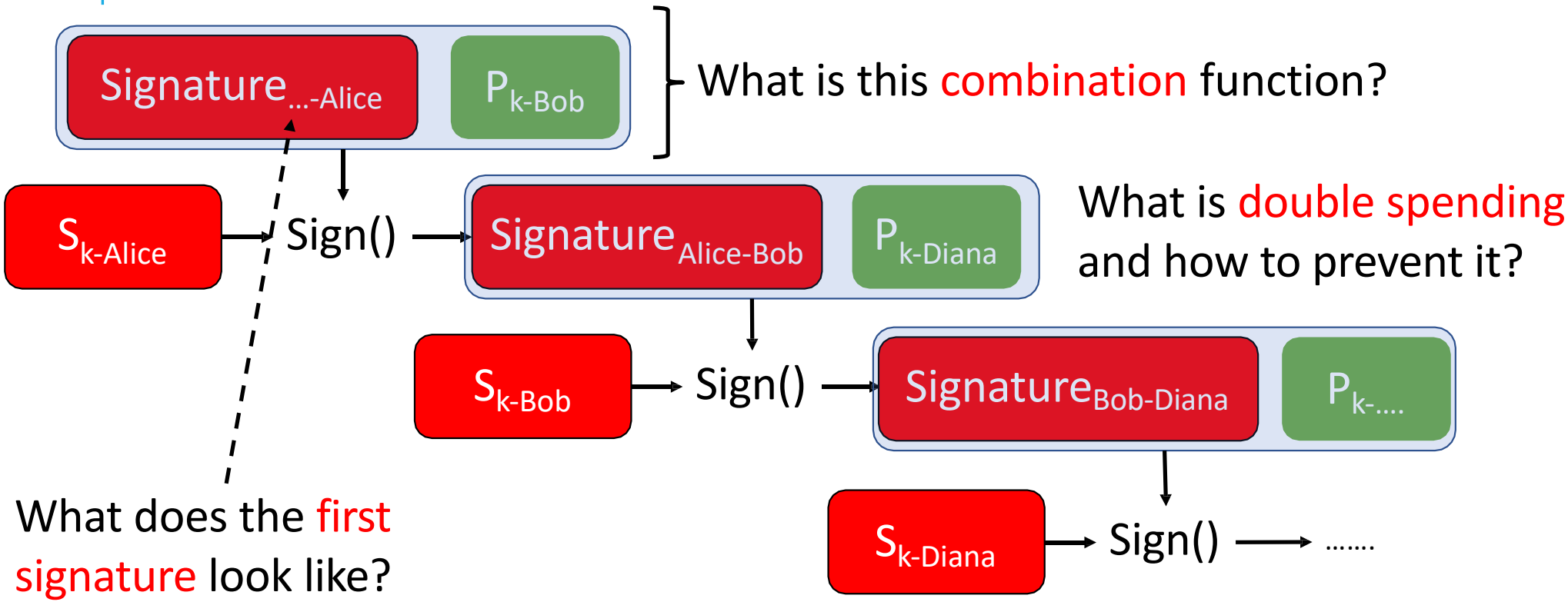
SHA256($\text{Signature}_{\text{Alice-Bob}}$ || $P_{\text{k-Diana}}$) =

256-bit (32-byte) unique string

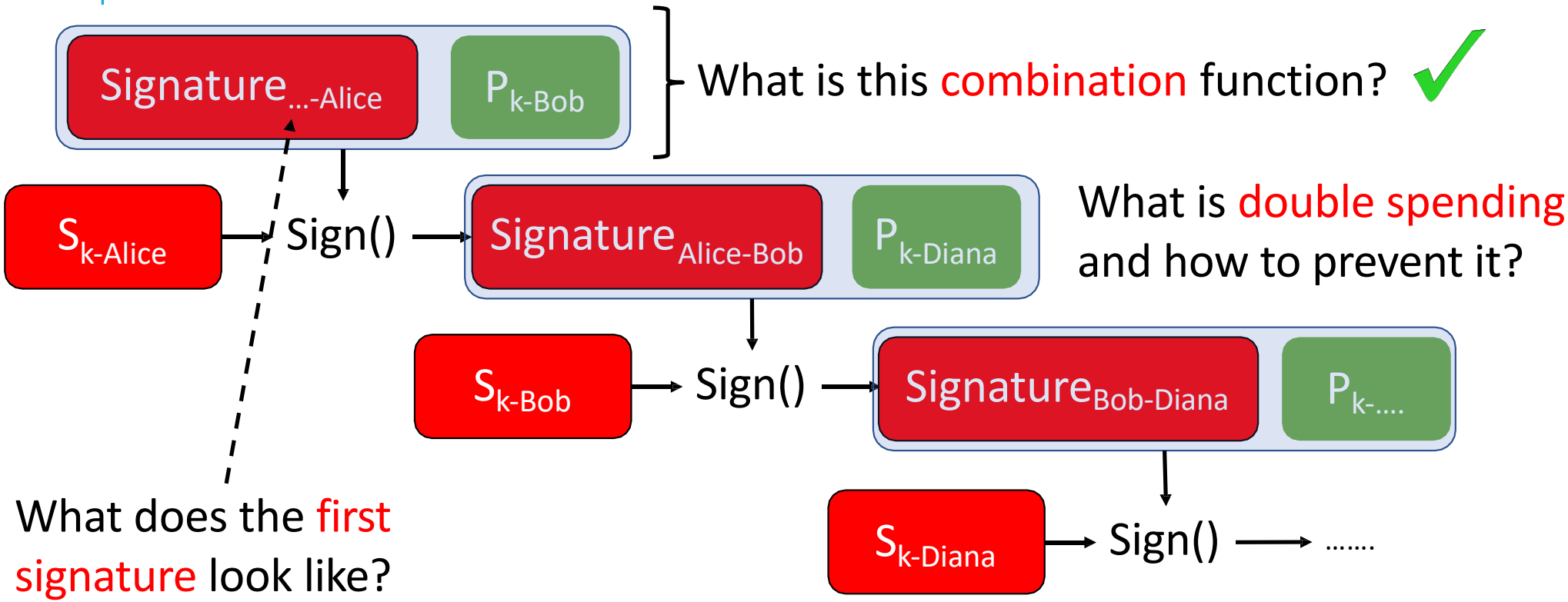
SHA256(abc) =
ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad

SHA256(abC) =
0a2432a1e349d8fdb9bfca91bba9e9f2836990fe937193d84deef26c6f3b8f76

WHAT ABOUT'S?


Signature...-Alice
Pk-Bob
What is this combination function?
Sk-Alice
Sign()
Signature Alice-Bob
Pk-Diana
What is double spending and how to prevent it?
Sk-Bob
Sign()
Signature Bob-Diana
Pk-....
Sk-Diana
Sign()
.....
What does the first signature look like?

WHAT ABOUT'S?


Signature...-Alice
Pk-Bob
What is this combination function?
Sk-Alice
Sign()
Signature Alice-Bob
Pk-Diana
What is double spending and how to prevent it?
Sk-Bob
Sign()
Signature Bob-Diana
Pk-....
Sk-Diana
Sign()
.....
What does the first signature look like?

DOUBLE SPENDING

- Spending the same digital cash asset more than once
- Impossible to do in physical cash
- Prevented in traditional banking systems through concurrency control

DOUBLE SPENDING

- Spending the same digital cash asset more than once
- Impossible to do in physical cash
- Prevented in traditional banking systems through concurrency control

$\text{Signature}_{\text{Alice-Bob}}$

DOUBLE SPENDING

- Spending the same digital cash asset more than once
- Impossible to do in physical cash
- Prevented in traditional banking systems through concurrency control

$\text{Signature}_{\text{Alice-Bob}}$

$\text{Signature}_{\text{Alice-Bob}}$

DOUBLE SPENDING

- Spending the same digital cash asset more than once
- Impossible to do in physical cash
- Prevented in traditional banking systems through concurrency control

$\text{Signature}_{\text{Alice-Bob}}$ $P_{\text{k-Diana}}$

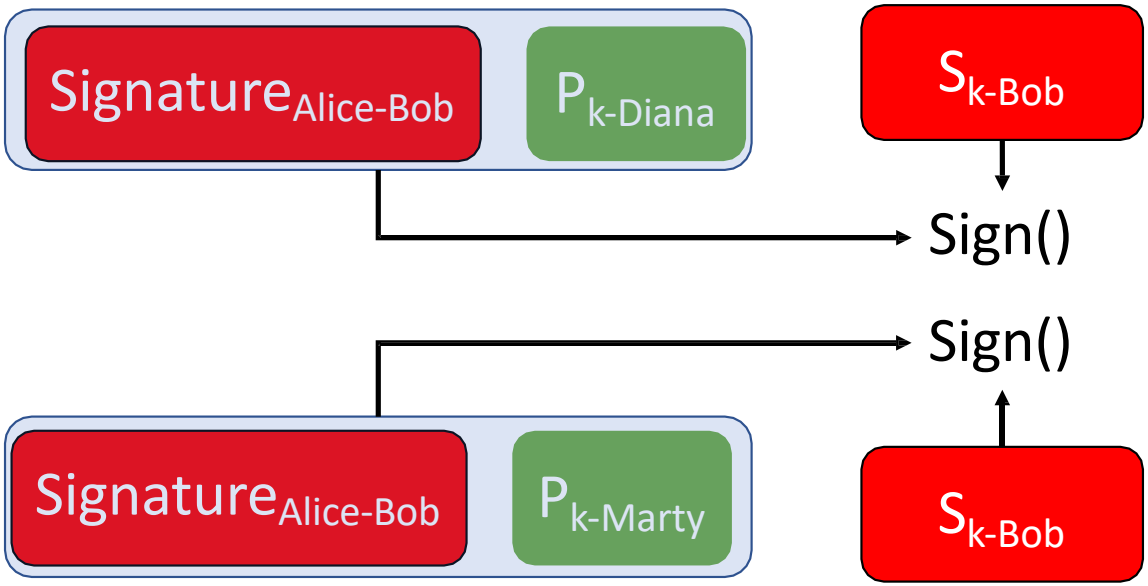
$\text{Signature}_{\text{Alice-Bob}}$ $P_{\text{k-Marty}}$

DOUBLE SPENDING

- Spending the same digital cash asset more than once
- Impossible to do in physical cash
- Prevented in traditional banking systems through concurrency control

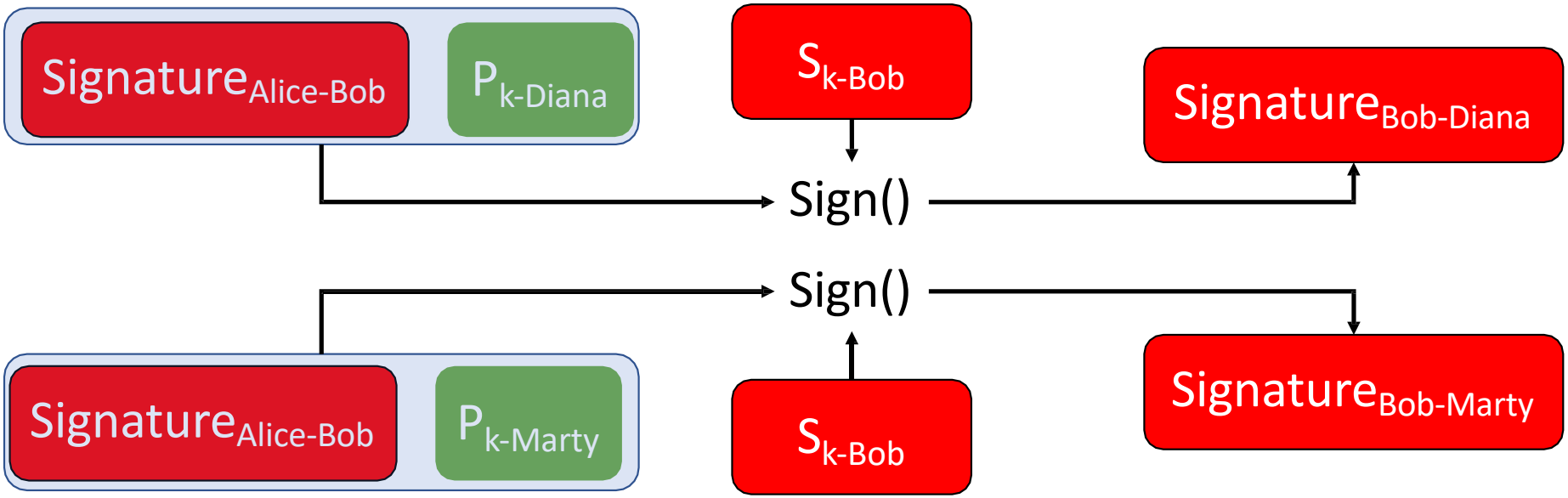
DOUBLE SPENDING

- Spending the same digital cash asset more than once
- Impossible to do in physical cash
- Prevented in traditional banking systems through concurrency control



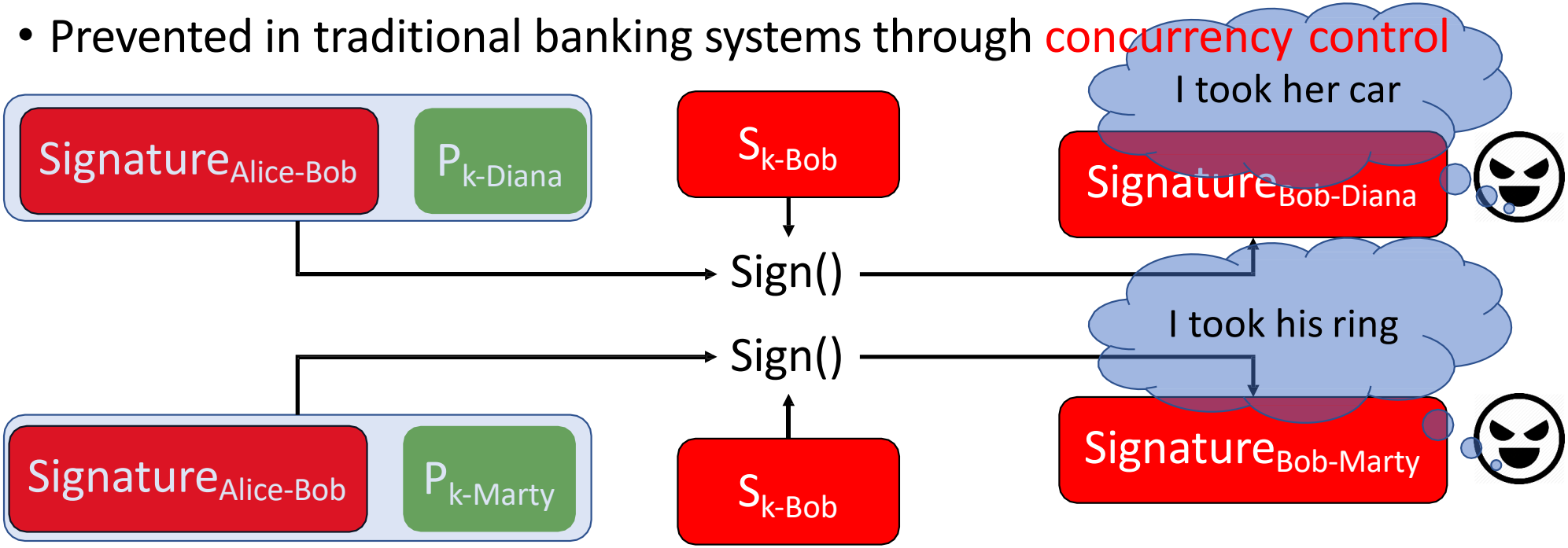
DOUBLE SPENDING

- Spending the same digital cash asset more than once
- Impossible to do in physical cash
- Prevented in traditional banking systems through concurrency control



DOUBLE SPENDING

- Spending the same digital cash asset more than once
- Impossible to do in physical cash
- Prevented in traditional banking systems through concurrency control



Double Spending Prevention

- Centralized

DOUBLE SPENDING PREVENTION

- Centralized
  - Transactions on coins go through a trusted 3rd party (Trent)

DOUBLE SPENDING PREVENTION

- Centralized
  - Transactions on coins go through a trusted 3rd party (Trent)

50 BTC

$\text{Signature}_{\text{Trent-Bob}}$

DOUBLE SPENDING PREVENTION

- Centralized
  - Transactions on coins go through a trusted 3rd party (Trent)

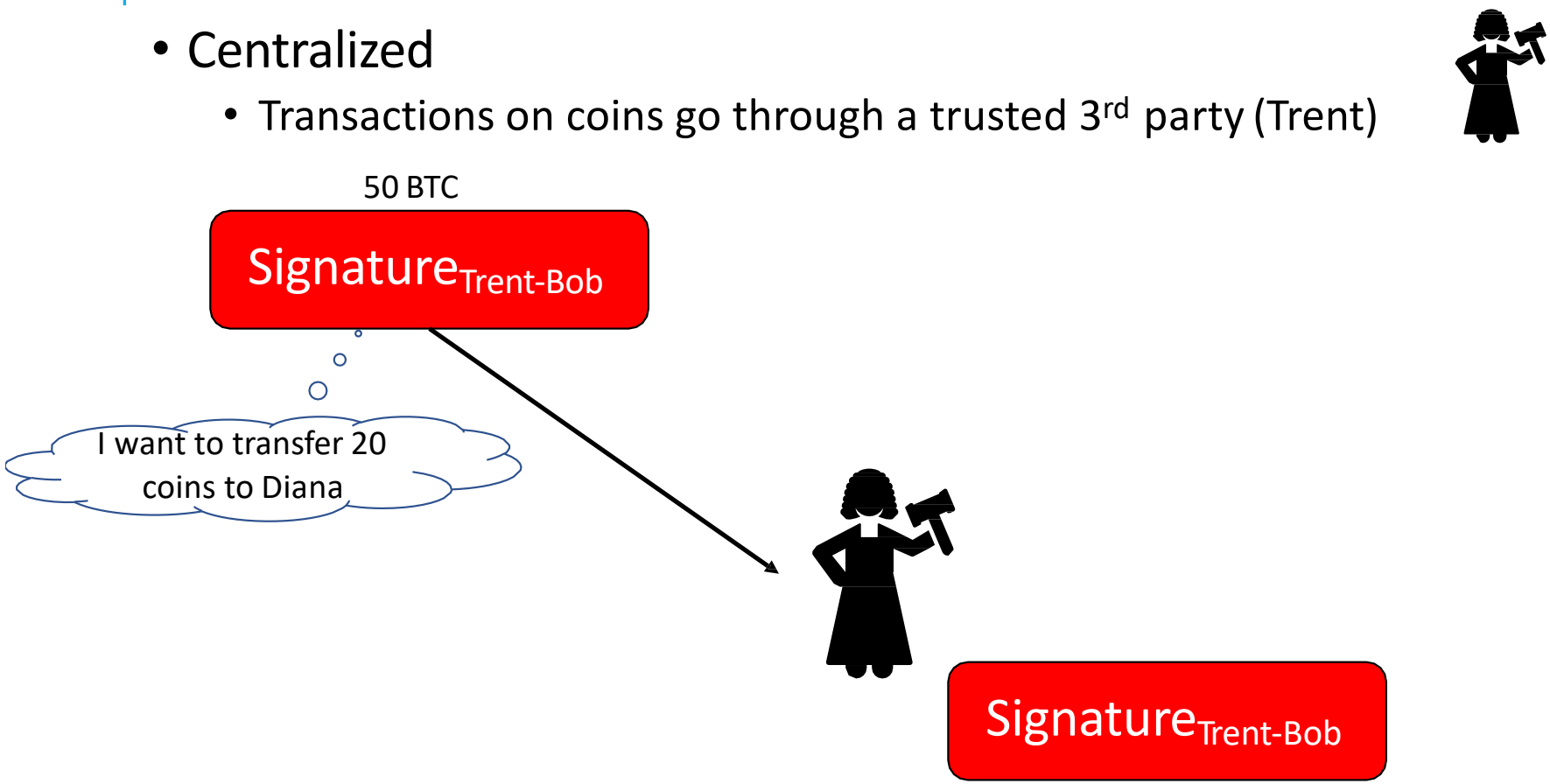
50 BTC

$\text{Signature}_{\text{Trent-Bob}}$

I want to transfer 20 coins to Diana

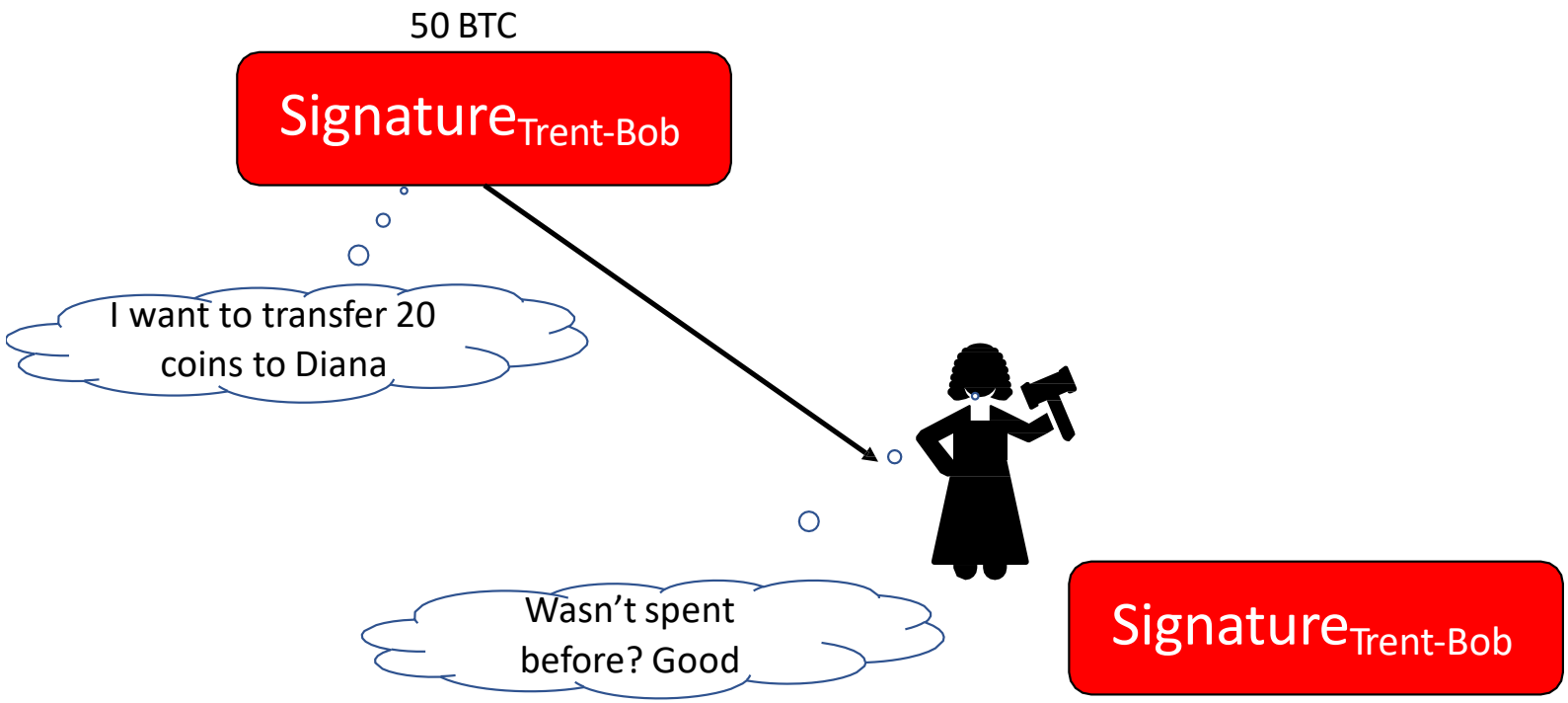
DOUBLE SPENDING PREVENTION

- Centralized
  - Transactions on coins go through a trusted 3rd party (Trent)



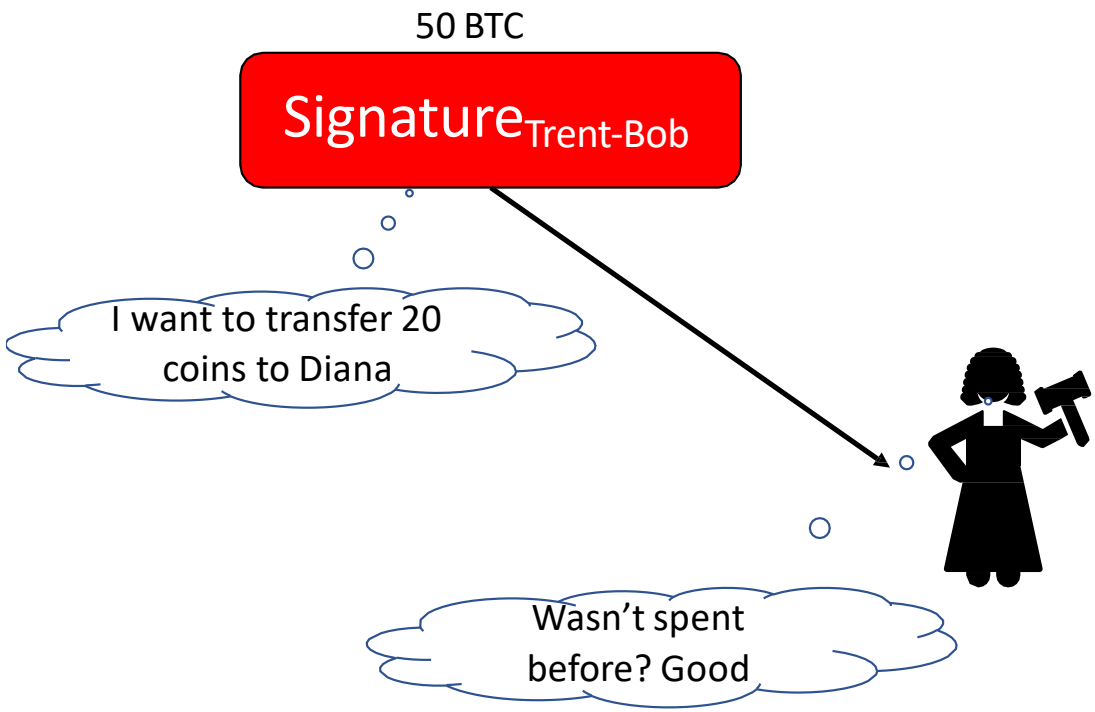
DOUBLE SPENDING PREVENTION

- Centralized
  - Transactions on coins go through a trusted 3rd party (Trent)



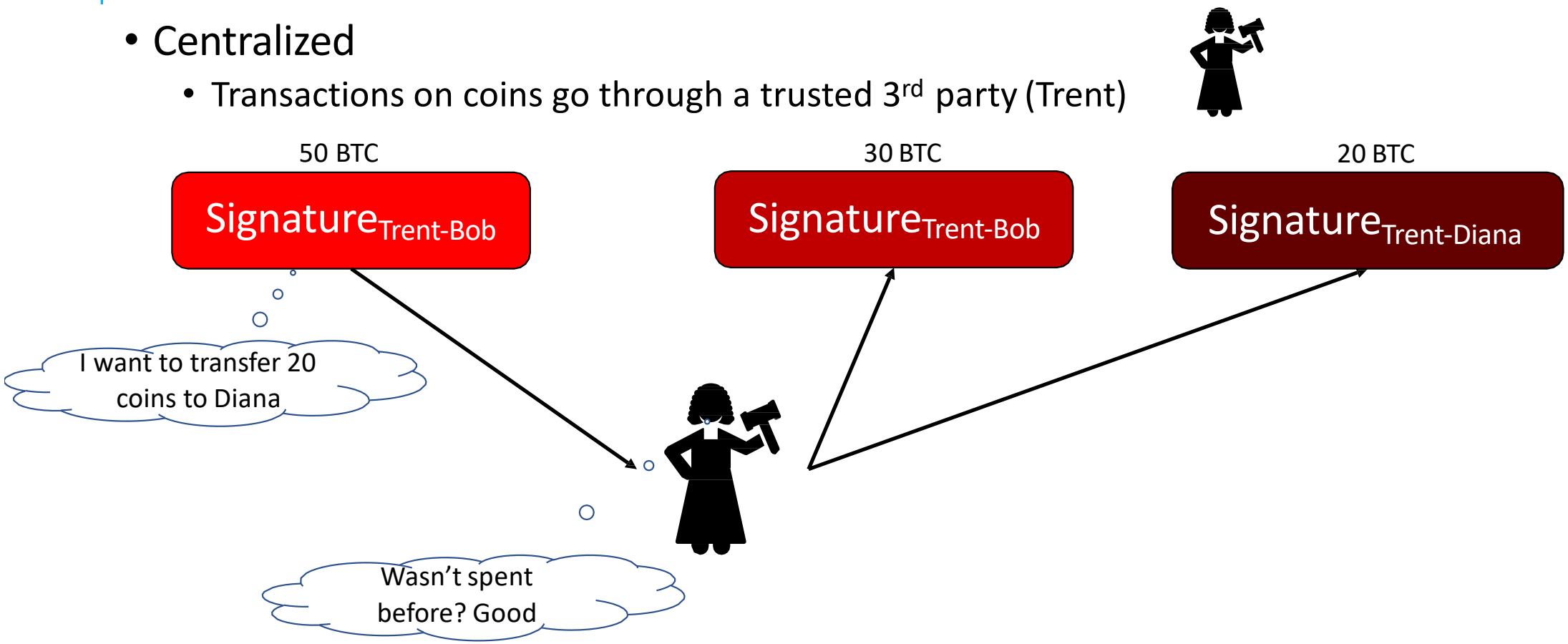
DOUBLE SPENDING PREVENTION

- Centralized
  - Transactions on coins go through a trusted 3rd party (Trent)



DOUBLE SPENDING PREVENTION

- Centralized
  - Transactions on coins go through a trusted 3rd party (Trent)

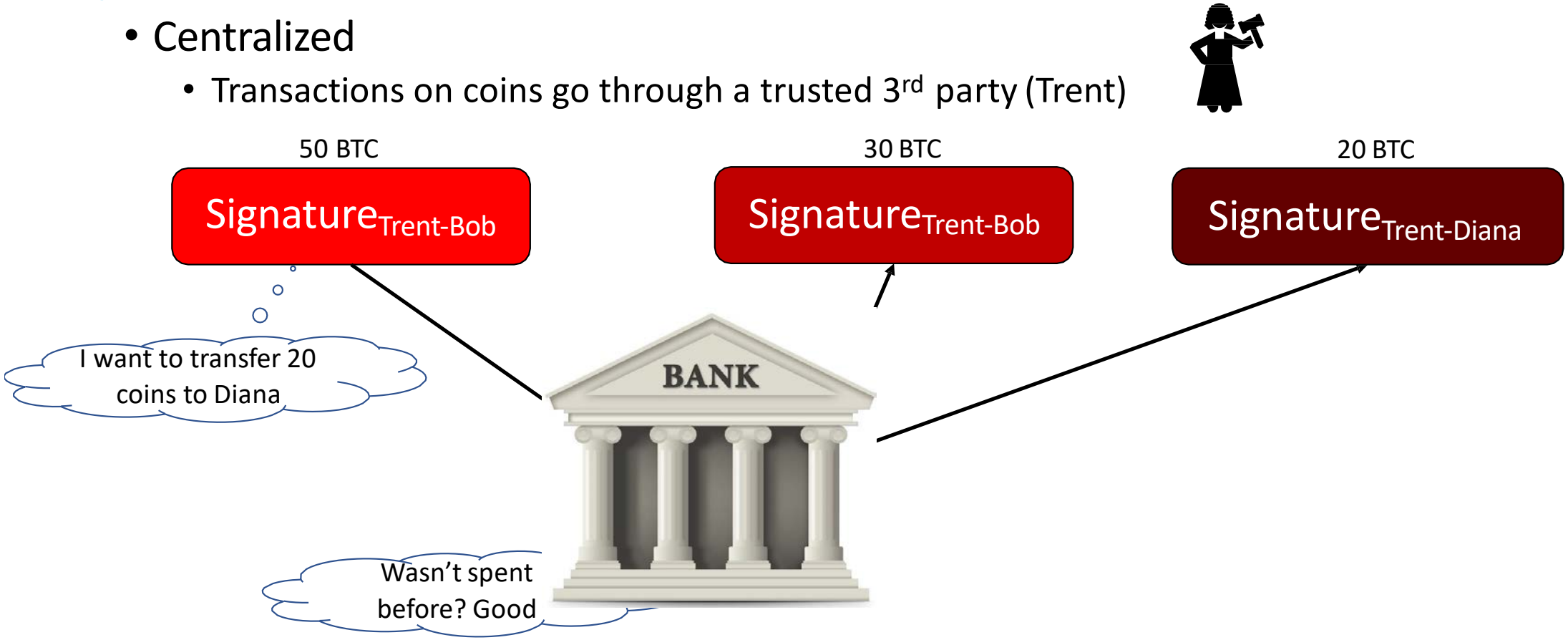


DSL

UCSB

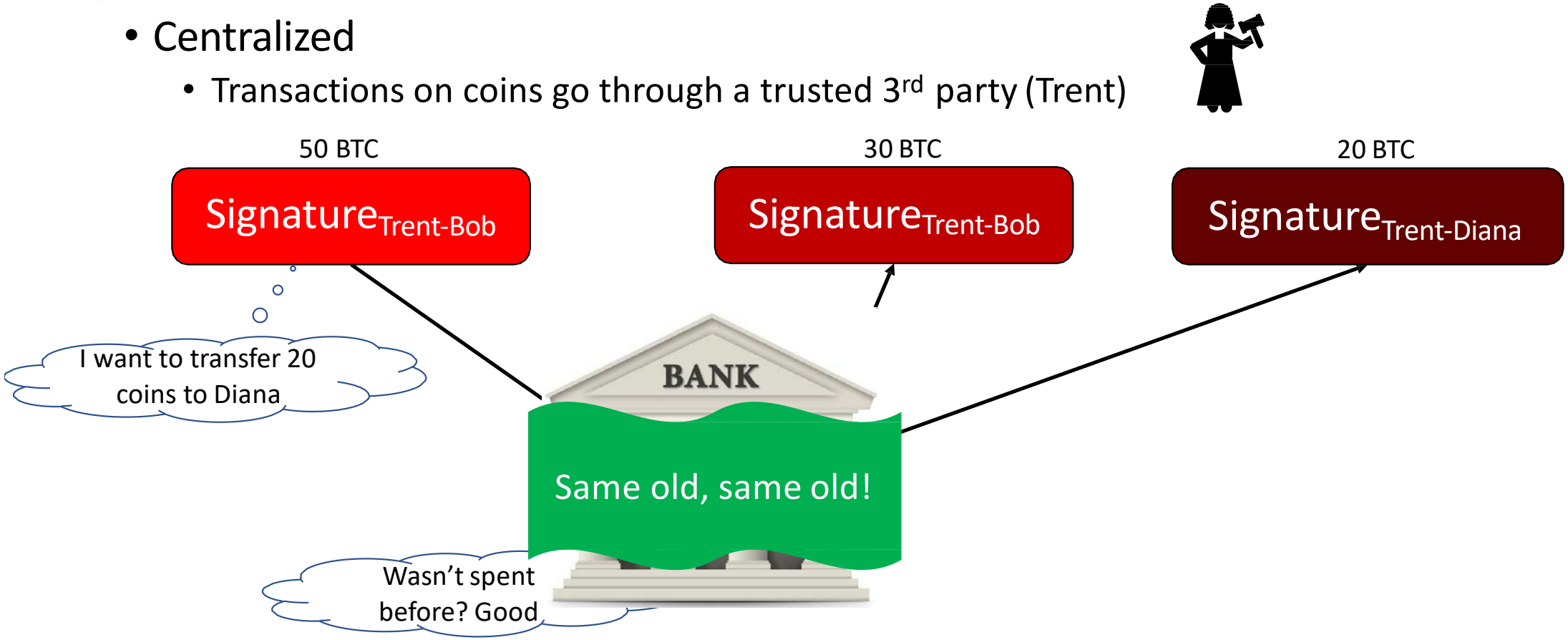
DOUBLE SPENDING PREVENTION

- Centralized
  - Transactions on coins go through a trusted 3rd party (Trent)



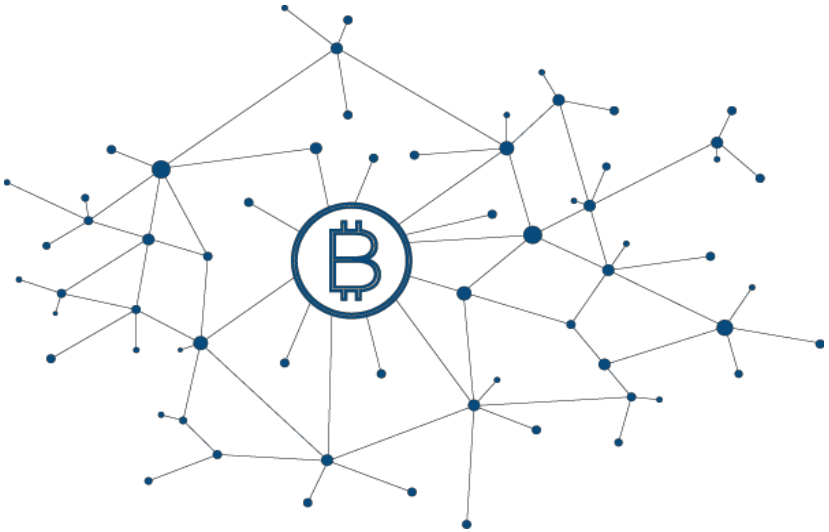
DOUBLE SPENDING PREVENTION

- Centralized
  - Transactions on coins go through a trusted 3rd party (Trent)



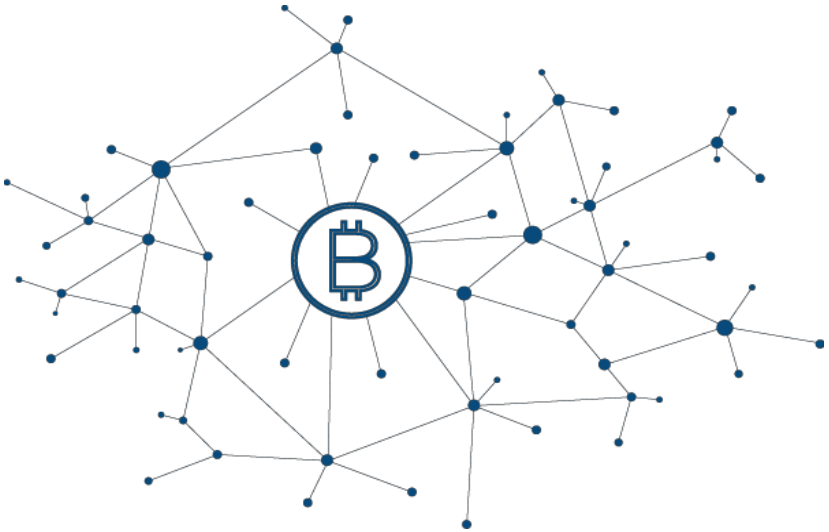
Double Spending Prevention

- Decentralized



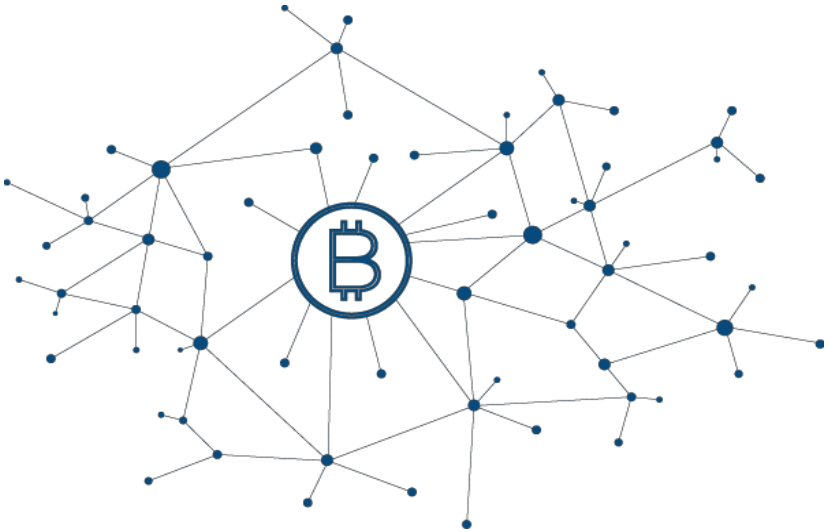
DOUBLE SPENDING PREVENTION

- Decentralized
  - A network of nodes maintains a ledger



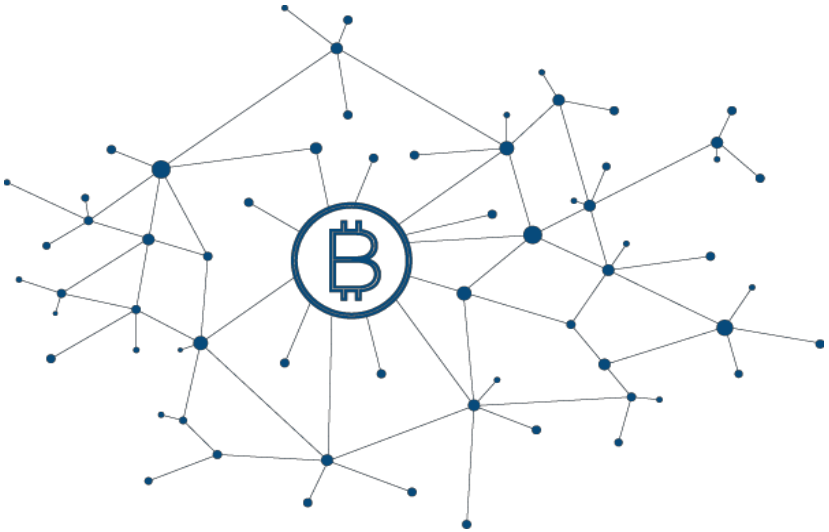
DOUBLE SPENDING PREVENTION

- Decentralized
  - A network of nodes maintains a ledger
  - Network nodes work to agree on transaction order
    - Serializing transactions on every coin prevents double spending



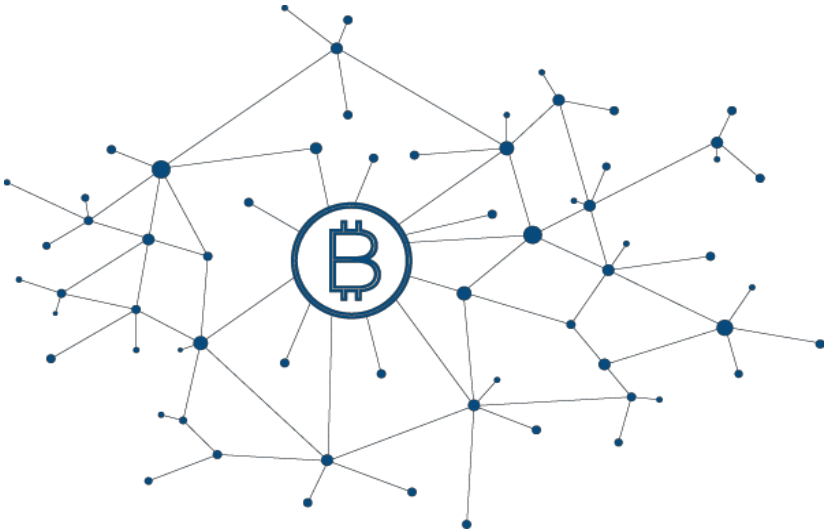
DOUBLE SPENDING PREVENTION

- Decentralized
  - A network of nodes maintains a ledger
  - Network nodes work to agree on transactions order
    - Serializing transactions on every coin prevents double spending
  - What is the ledger?



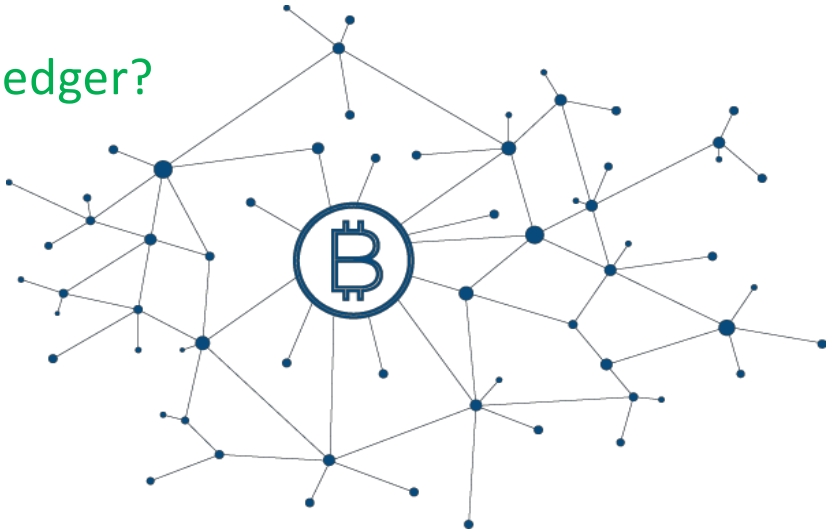
DOUBLE SPENDING PREVENTION

- Decentralized
  - A network of nodes maintains a ledger
  - Network nodes work to agree on transactions order
    - Serializing transactions on every coin prevents double spending
  - What is the ledger?
  - How to agree on transaction order?



DOUBLE SPENDING PREVENTION

- Decentralized
  - A network of nodes maintains a ledger
  - Network nodes work to agree on transactions order
    - Serializing transactions on every coin prevents double spending
  - What is the ledger?
  - How to agree on transaction order?
  - What incentives network nodes to maintain the ledger?



WHAT IS THE LEDGER?

What is the Ledger?

- Blockchain

What is the Ledger?

- Blockchain

WHAT IS THE LEDGER?

- Blockchain

- Transactions are grouped into blocks

WHAT IS THE LEDGER?

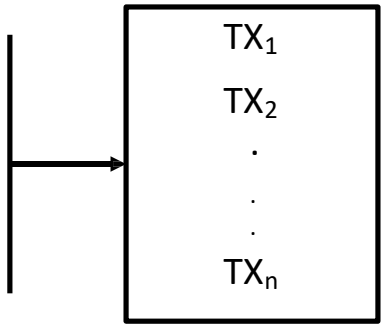
- Blockchain 

- Transactions are grouped into blocks
  - Blocks are chained to each other through pointers (Hence blockchain)

WHAT IS THE LEDGER?

- Blockchain

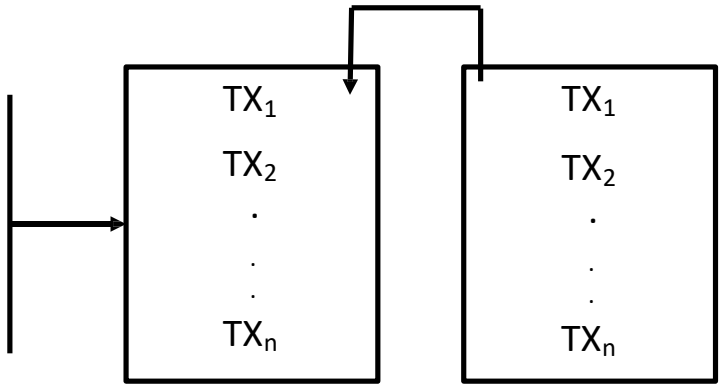
- Transactions are grouped into blocks
  - Blocks are chained to each other through pointers (Hence blockchain)



WHAT IS THE LEDGER?

- Blockchain 

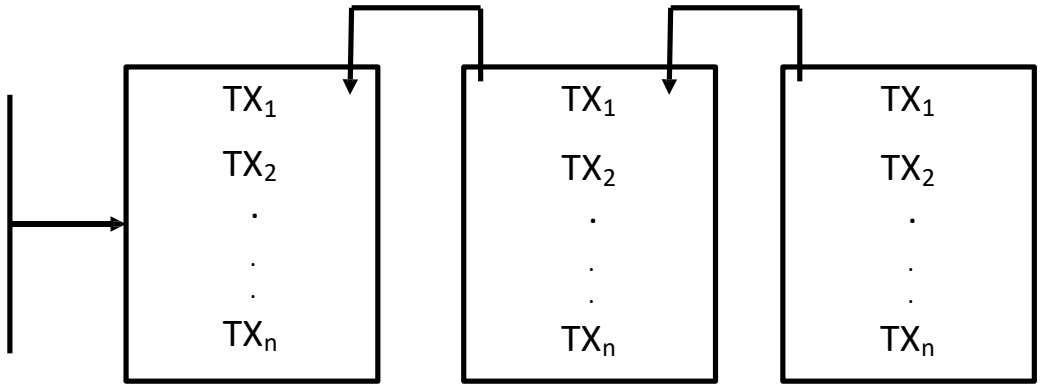
- Transactions are grouped into blocks
  - Blocks are chained to each other through pointers (Hence blockchain)



WHAT IS THE LEDGER?

- Blockchain

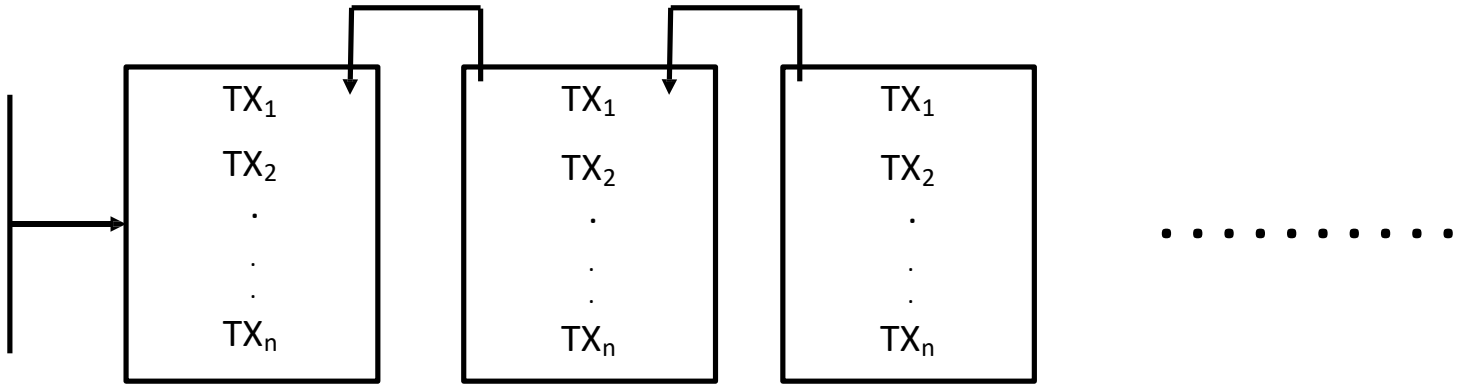
- Transactions are grouped into blocks
  - Blocks are chained to each other through pointers (Hence blockchain)



WHAT IS THE LEDGER?

- Blockchain 

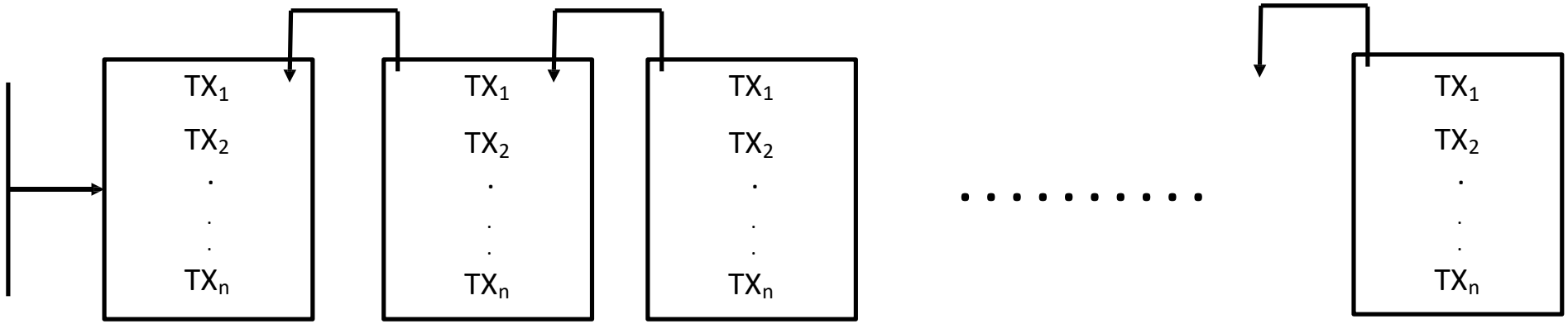
- Transactions are grouped into blocks
  - Blocks are chained to each other through pointers (Hence blockchain)



WHAT IS THE LEDGER?

- Blockchain 

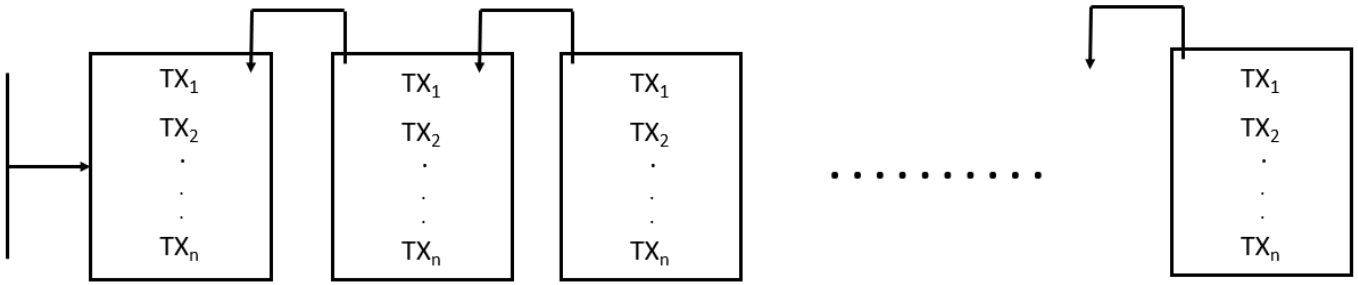
- Transactions are grouped into blocks
  - Blocks are chained to each other through pointers (Hence blockchain)



DSL

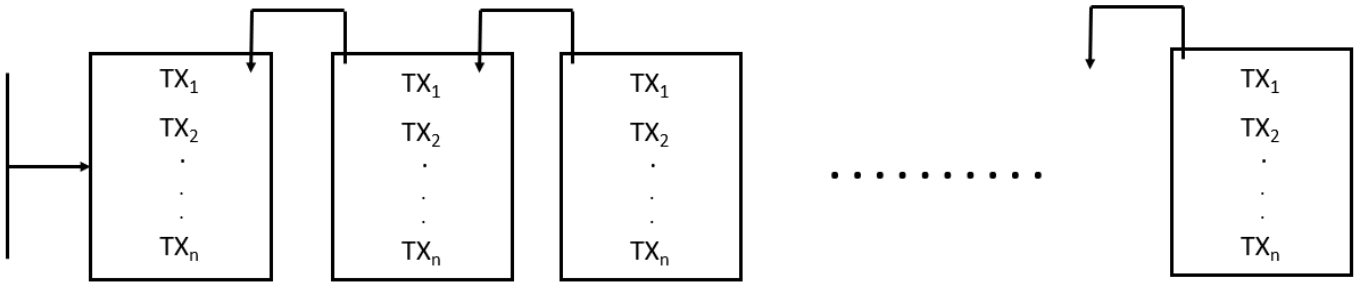
UCSB

THE LEDGER'S WHAT ABOUTS?



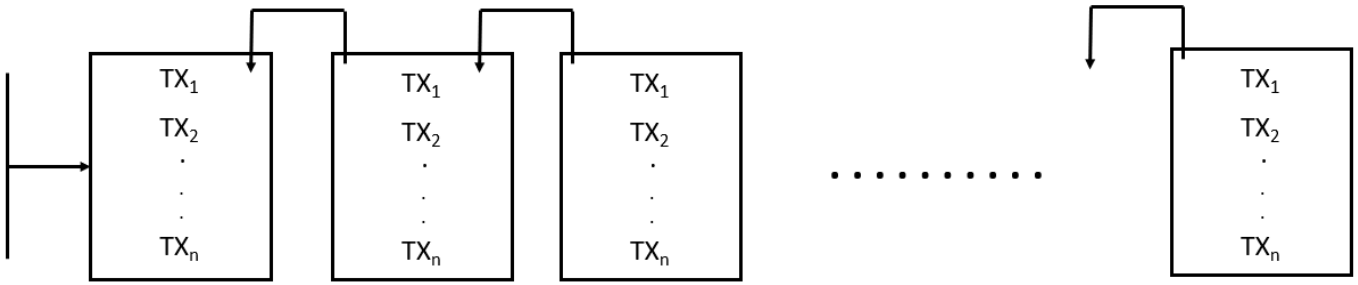
The Ledger's What About's?

- Where is the ledger stored?



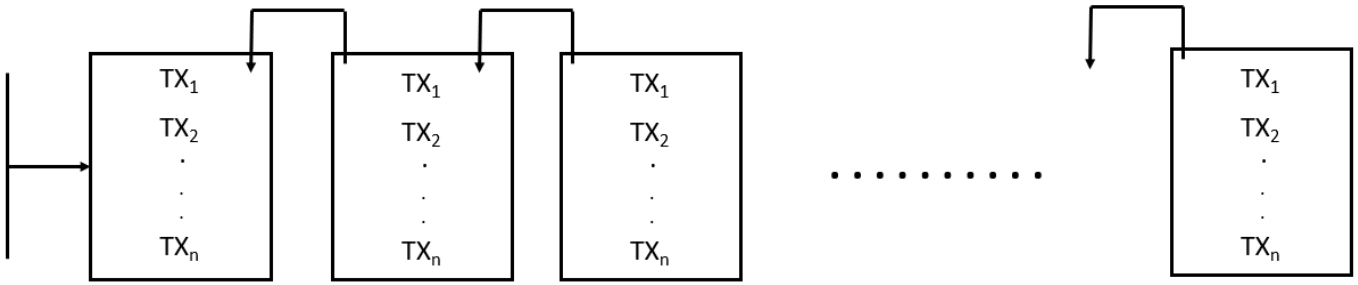
THE LEDGER'S WHAT ABOUTS?

- Where is the ledger stored?
  - Each network node maintains its copy of the ledger



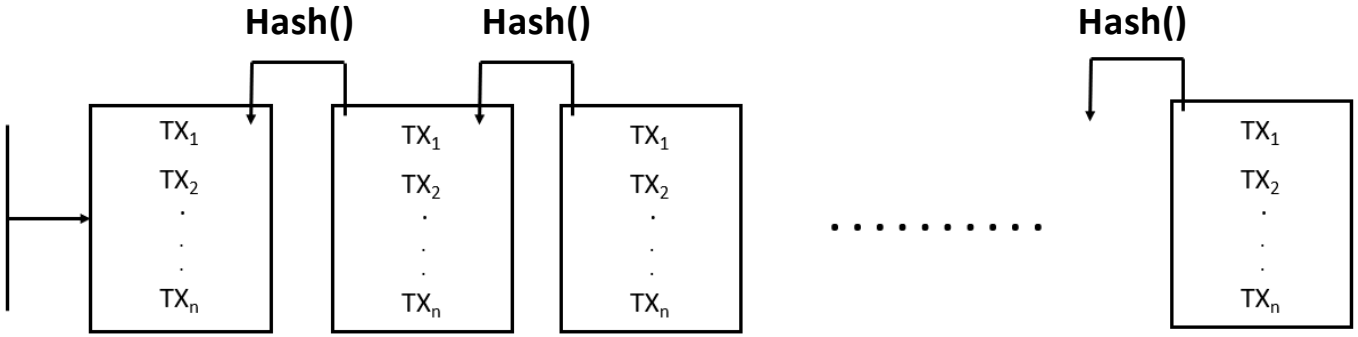
THE LEDGER'S WHAT ABOUTS?

- Where is the ledger stored?
  - Each network node maintains its copy of the ledger
- How is the ledger tamper-free?



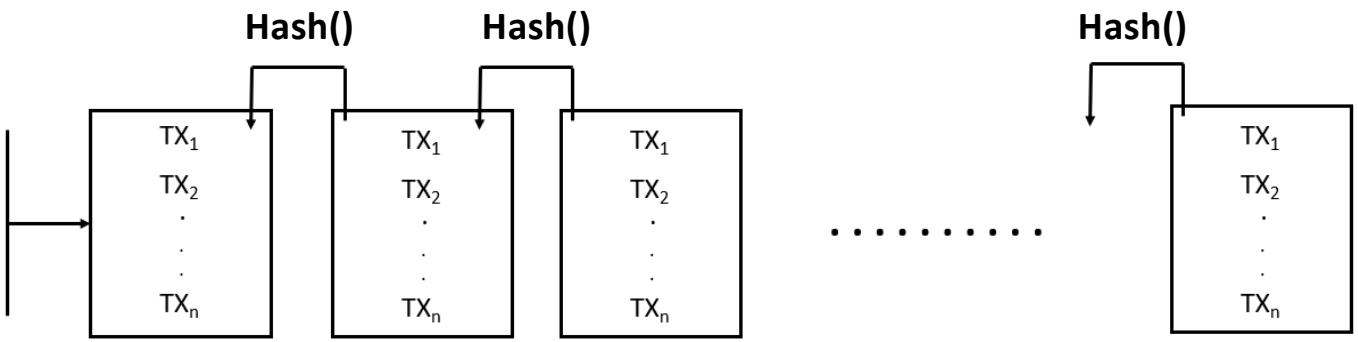
THE LEDGER'S WHAT ABOUTS?

- Where is the ledger stored?
  - Each network node maintains its copy of the ledger
- How is the ledger tamper-free?
  1. Blocks are connected through **hash-pointers**



THE LEDGER'S WHAT ABOUTS?

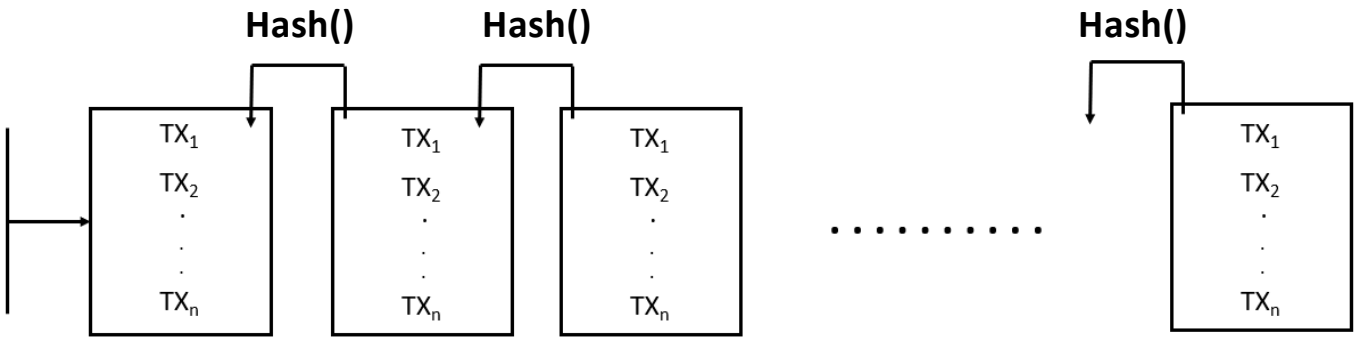
- Where is the ledger stored?
  - Each network node maintains its copy of the ledger
- How is the ledger tamper-free?
  1. Blocks are connected through **hash-pointers**
     - Each block contains the hash of the previous block
     - This hash gives each block its location in the blockchain
     - Tampering with the content of any block can easily be detected (**is this enough? NO**)



DSL

UCSB

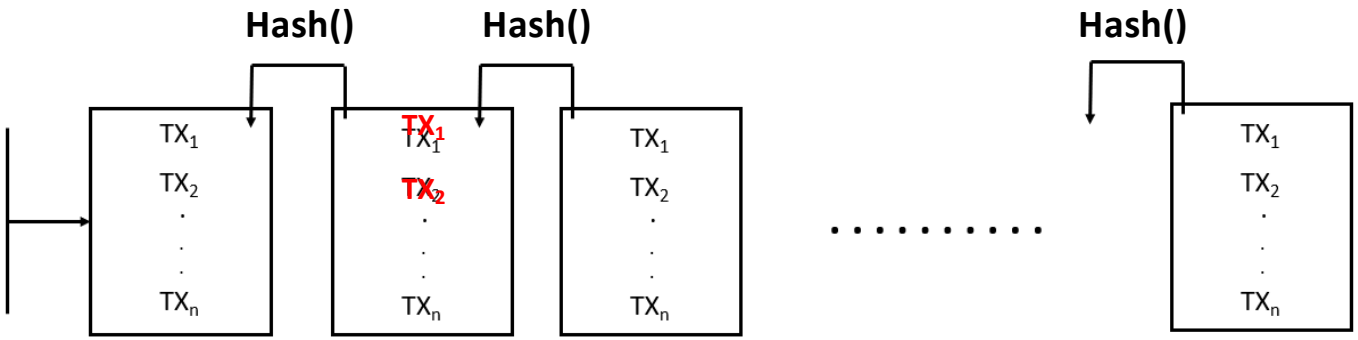
TAMPERING WITH THE LEDGER



DSL

UCSB

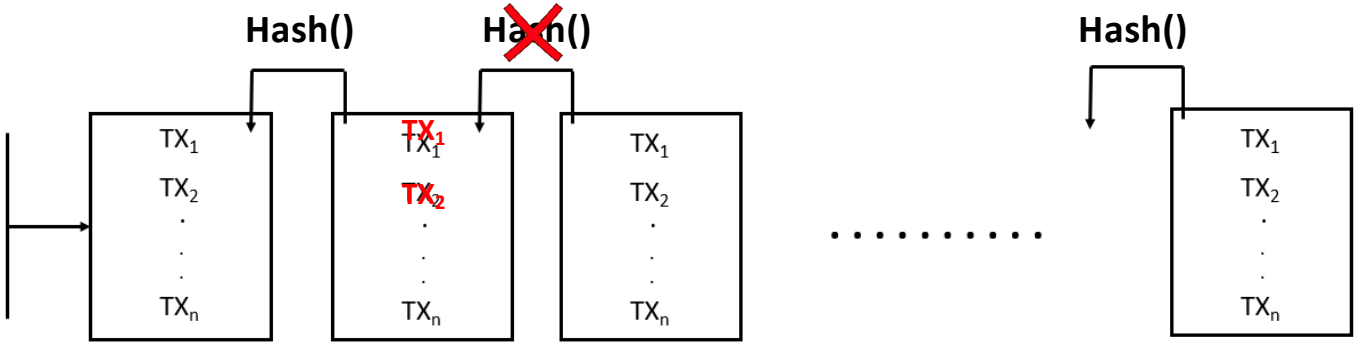
TAMPERING WITH THE LEDGER



DSL

UCSB

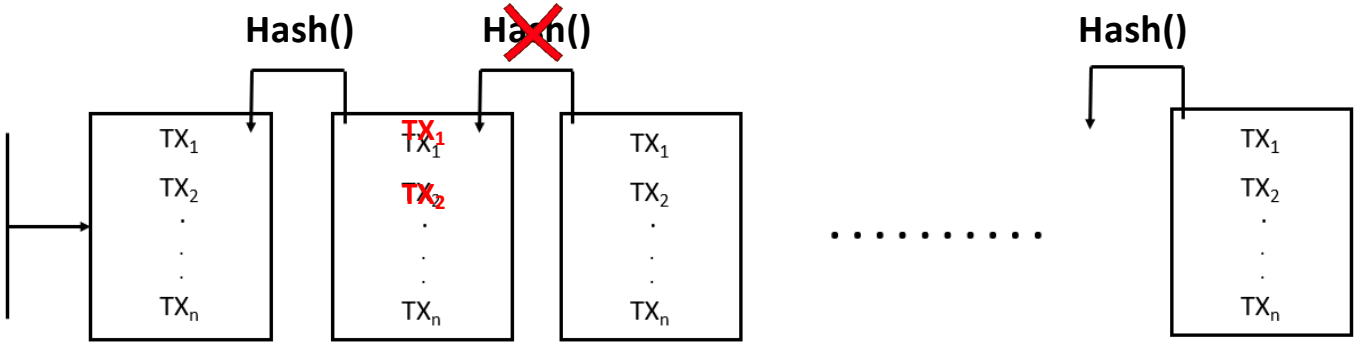
TAMPERING WITH THE LEDGER



DSL

UCSB

TAMPERING WITH THE LEDGER

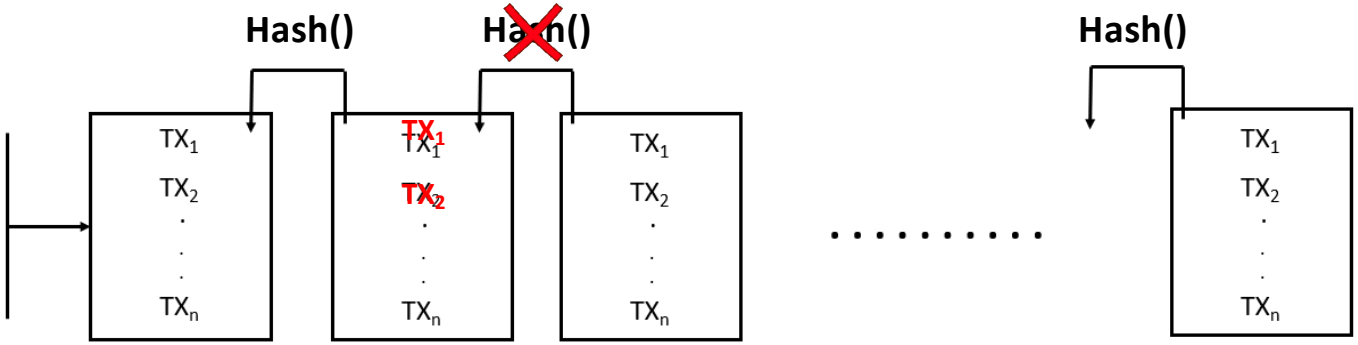


Inconsistent Blockchain

DSL

UCSB

TAMPERING WITH THE LEDGER



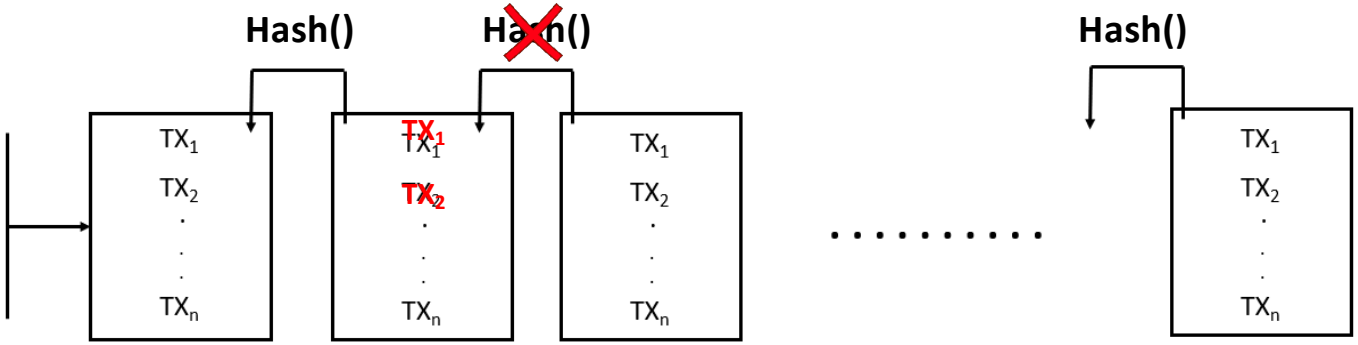
Inconsistent Blockchain

However,

DSL

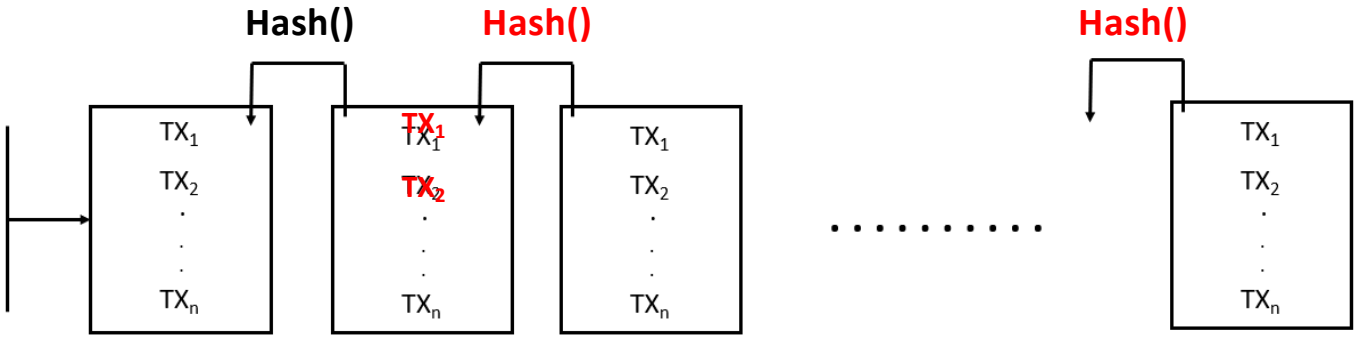
UCSB

TAMPERING WITH THE LEDGER



Inconsistent Blockchain

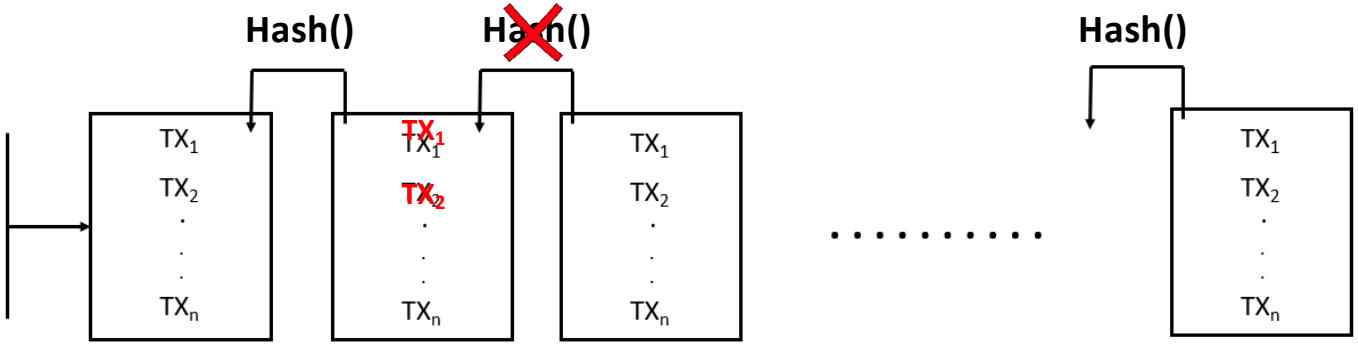
However,



DSL

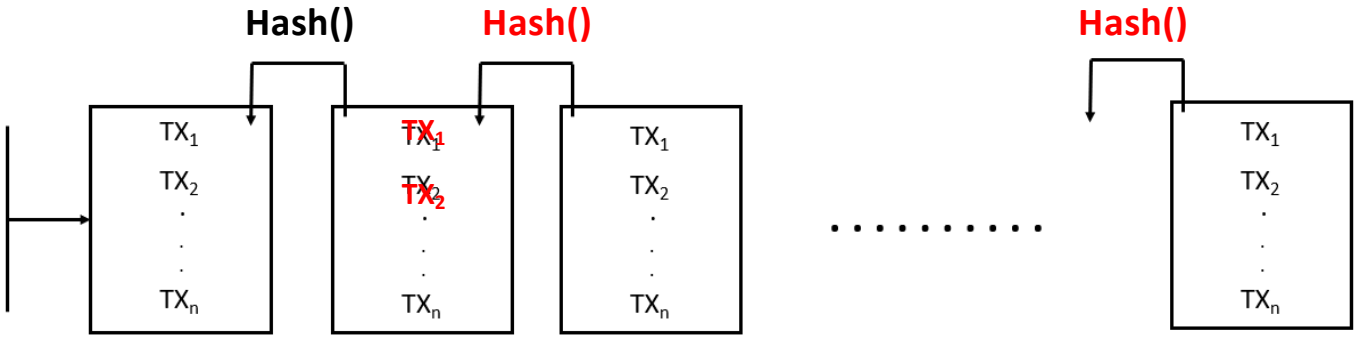
UCSB

TAMPERING WITH THE LEDGER



Inconsistent Blockchain

However,



Consistent Blockchain

THE LEDGER'S WHAT ABOUT'S?

- How is the ledger tamper-free?
  1. Blocks are connected through **hash-pointers**
     - Each block contains the hash of the previous block
     - This hash gives each block its location in the blockchain
     - Tampering the content of any block can easily be detected (**is this enough? NO**)

THE LEDGER'S WHAT ABOUT'S?

- How is the ledger tamper-free?
  1. Blocks are connected through **hash-pointers**
     - Each block contains the hash of the previous block
     - This hash gives each block its location in the blockchain
     - Tampering the content of any block can easily be detected (**is this enough? NO**)
  2. Replacing a consistent blockchain with another tampered consistent block chain should be **made very hard**, How?

DSL

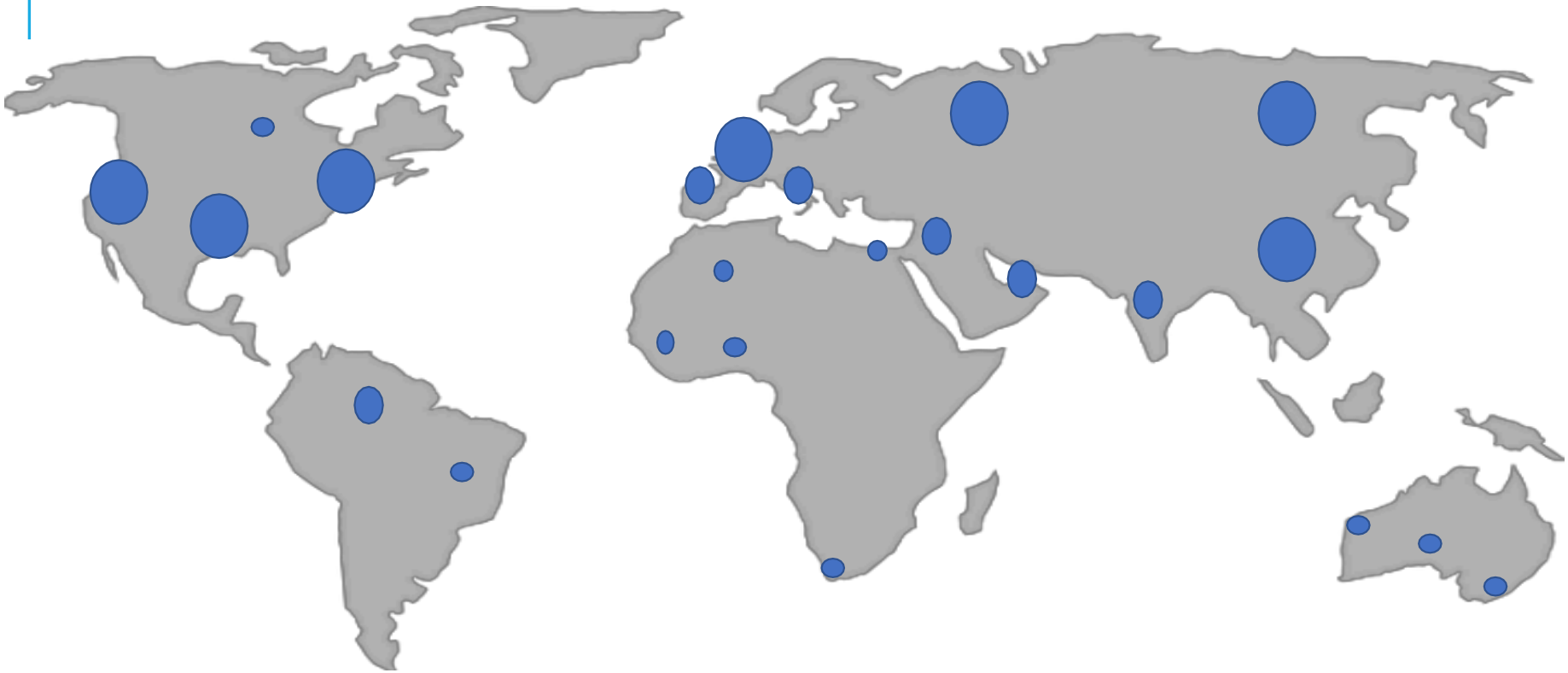
UCSB

NETWORK NODES BIG PICTURE

DSL

UCSB

NETWORK NODES BIG PICTURE



NETWORK NODES BIG PICTURE

MAKING PROGRESS

Making Progress

- The ledger is fully replicated to all network nodes

MAKING PROGRESS

- The ledger is fully replicated to all network nodes
- To make progress:

MAKING PROGRESS

- The ledger is fully replicated to all network nodes
- To make progress:
  - Network nodes group new transactions into a block

MAKING PROGRESS

- The ledger is fully replicated to all network nodes
- To make progress:
  - Network nodes group new transactions into a block
  - Blocks are fixed in size (1MB)

MAKING PROGRESS

- The ledger is fully replicated to all network nodes
- To make progress:
  - Network nodes group new transactions into a block
  - Blocks are fixed in size (1MB)
  - Network nodes **validate** new transactions to make sure that:

MAKING PROGRESS

- The ledger is fully replicated to all network nodes
- To make progress:
  - Network nodes group new transactions into a block
  - Blocks are fixed in size (1MB)
  - 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**

MAKING PROGRESS

- The ledger is fully replicated to all network nodes
- To make progress:
  - Network nodes group new transactions into a block
  - Blocks are fixed in size (1MB)
  - 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

MAKING PROGRESS

- The ledger is fully replicated to all network nodes
- To make progress:
  - Network nodes group new transactions into a block
  - Blocks are fixed in size (1MB)
  - 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

Consensus

NAKAMOTO CONSENSUS

- Intuitively, network nodes race to solve a puzzle
- This puzzle is computationally expensive
- Once a network node finds (mines) a solution:
  - It adds its block of transactions to the blockchain
  - It multi-casts the solution to other network nodes
  - Other network nodes accept and verify the solution

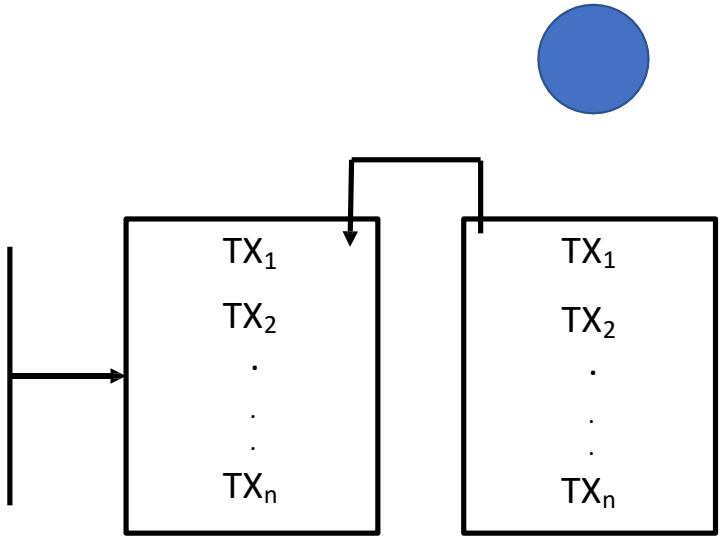
MINING DETAILS

MINING DETAILS

DSL

UCSB

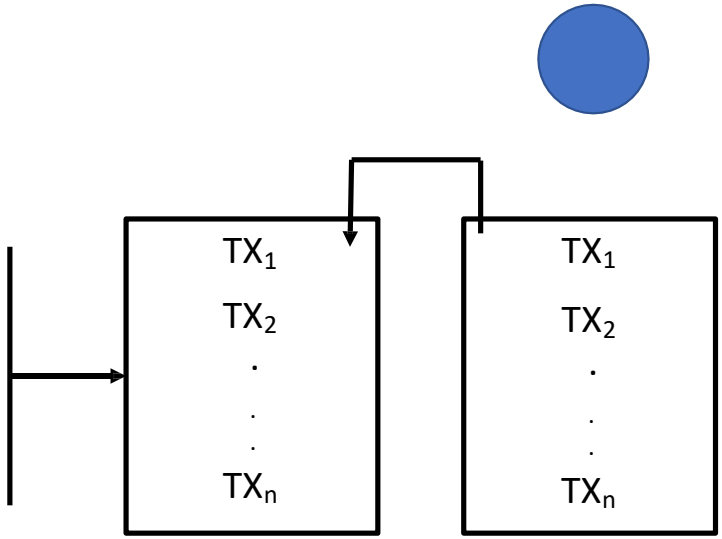
MINING DETAILS

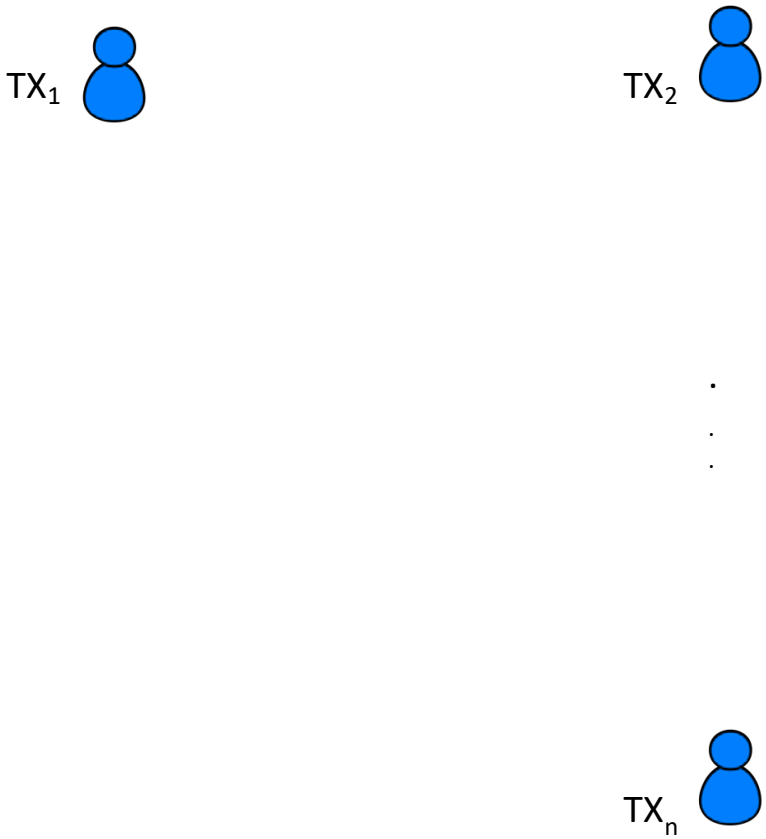


DSL

UCSB

MINING DETAILS

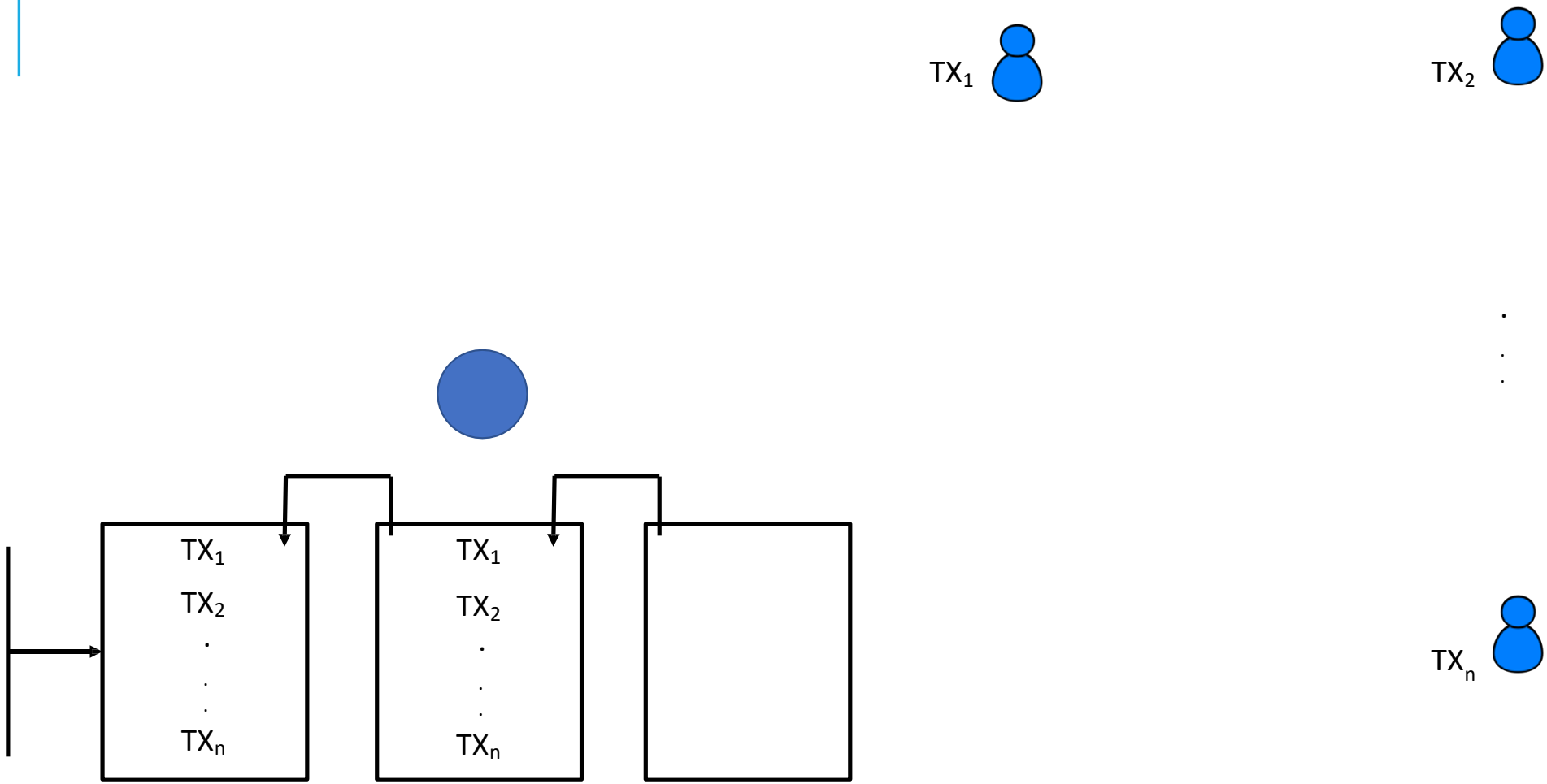




DSL

UCSB

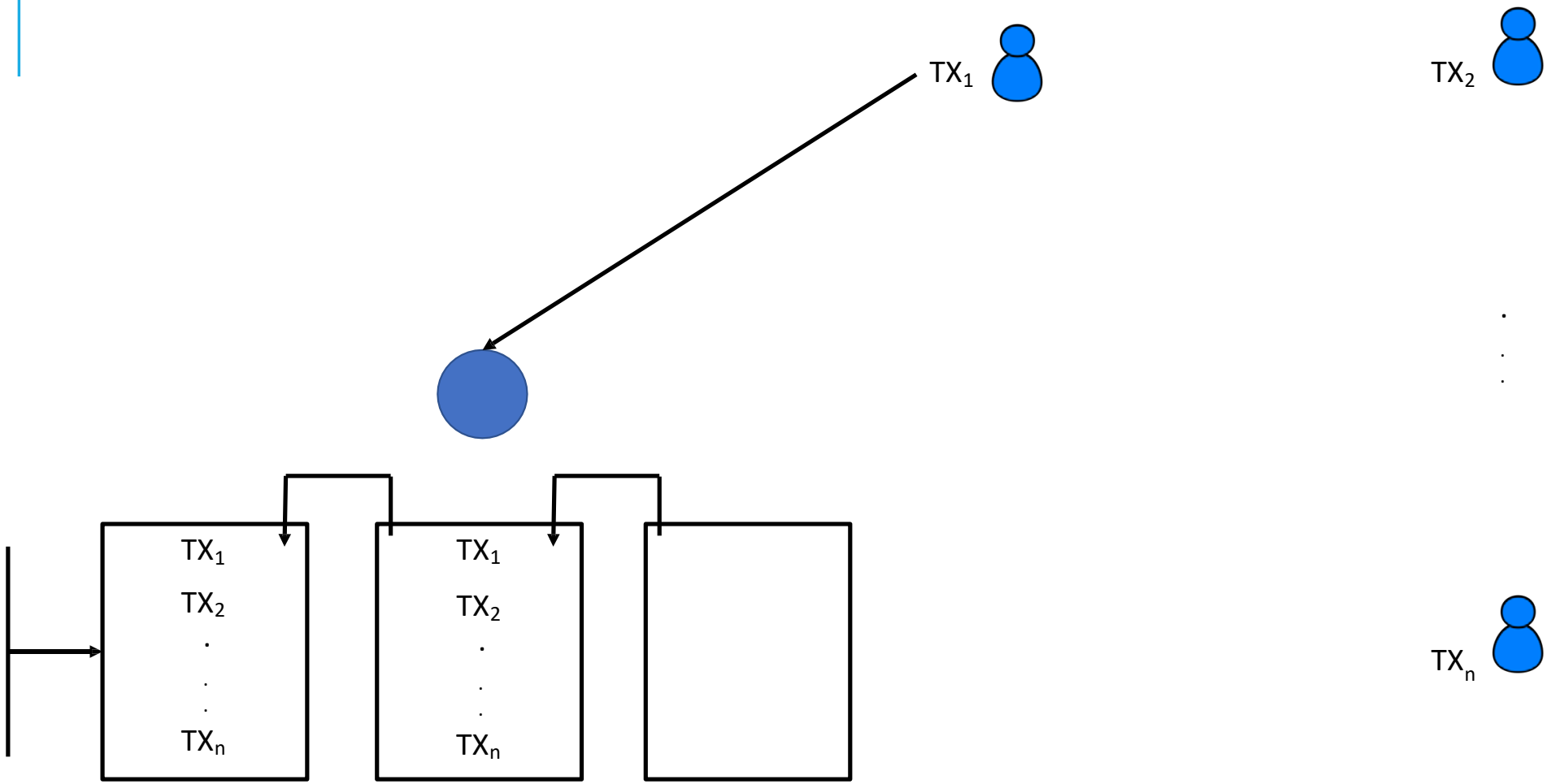
MINING DETAILS



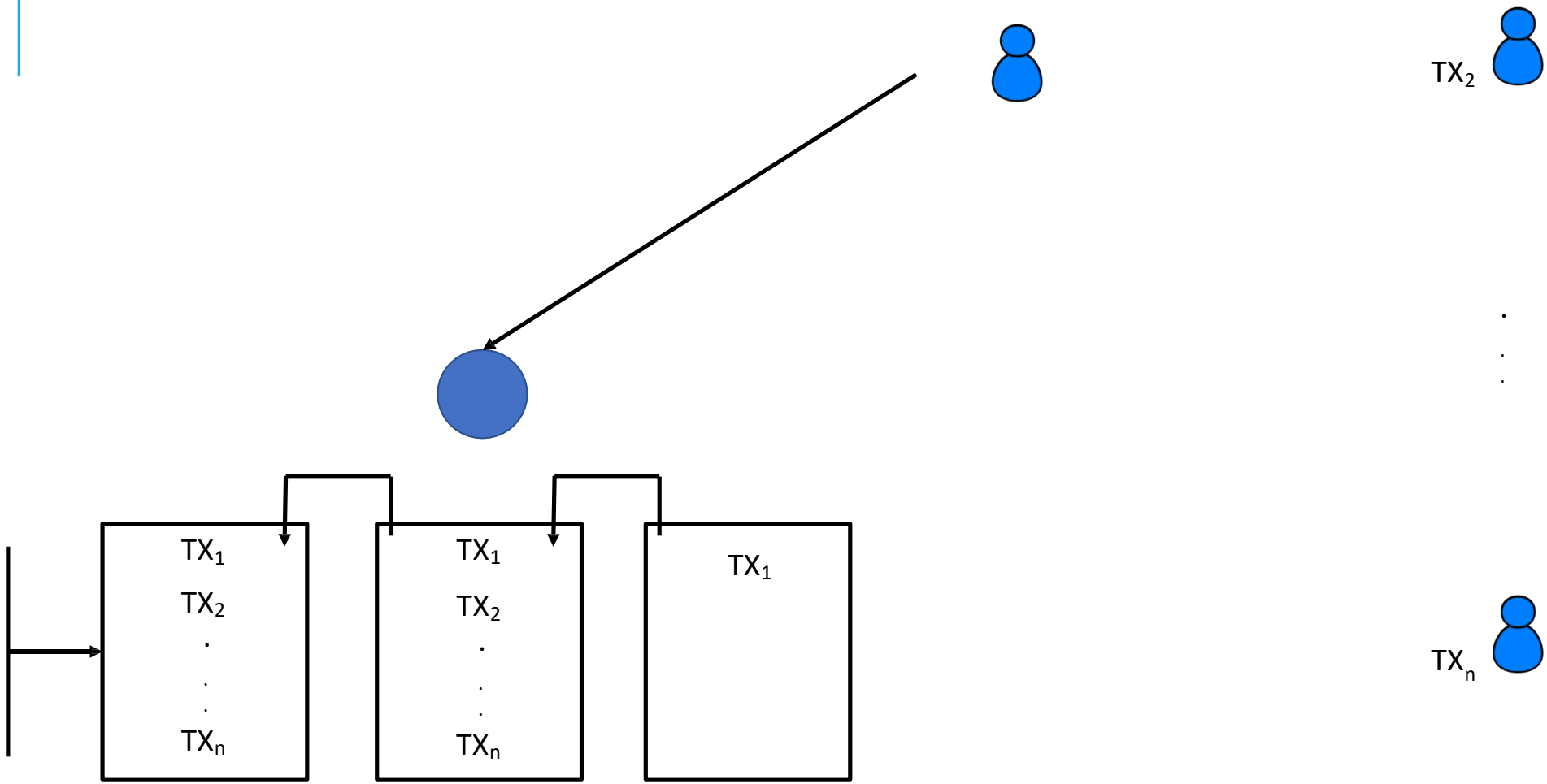
DSL

UCSB

MINING DETAILS



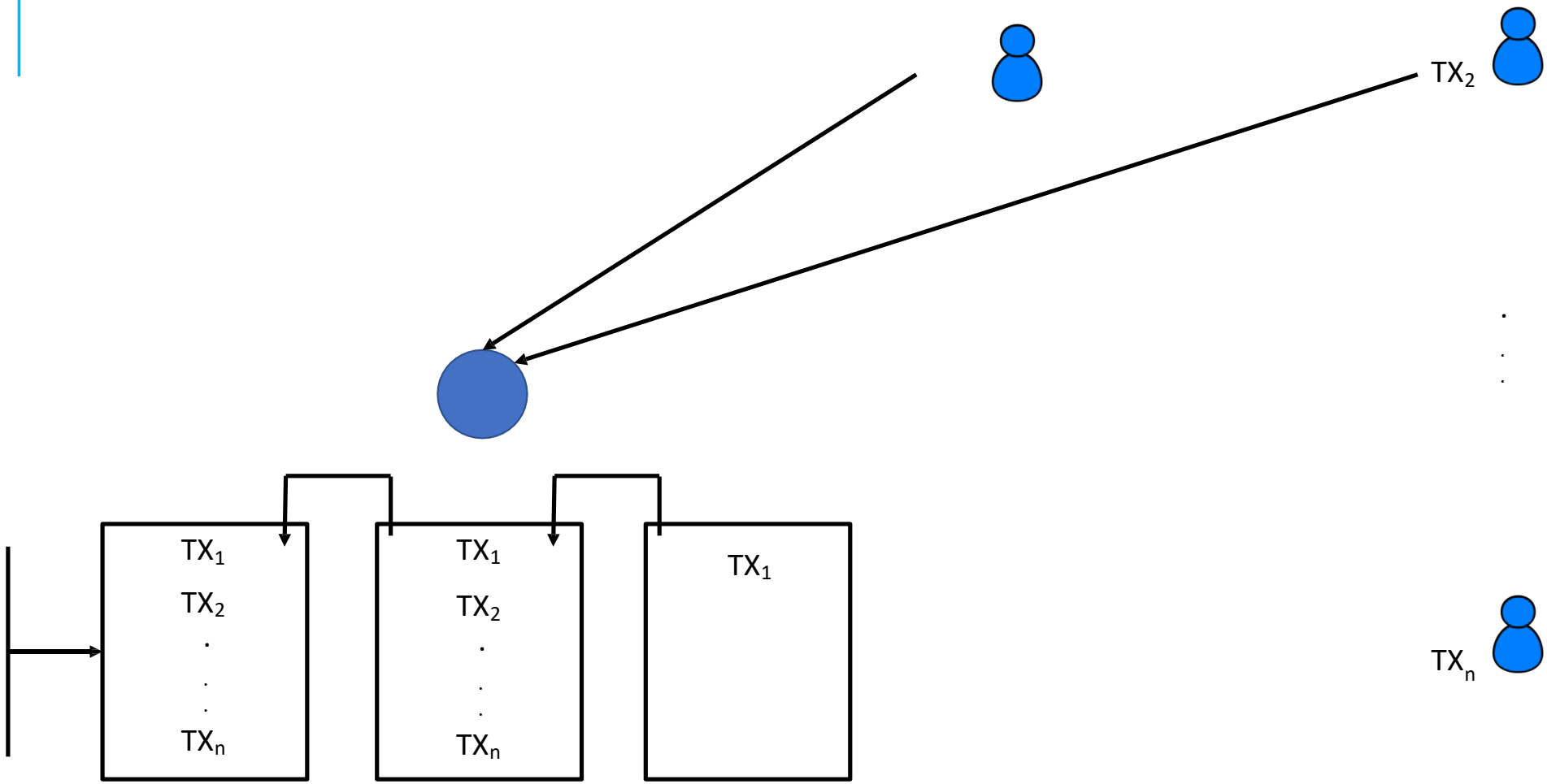
MINING DETAILS



DSL

UCSB

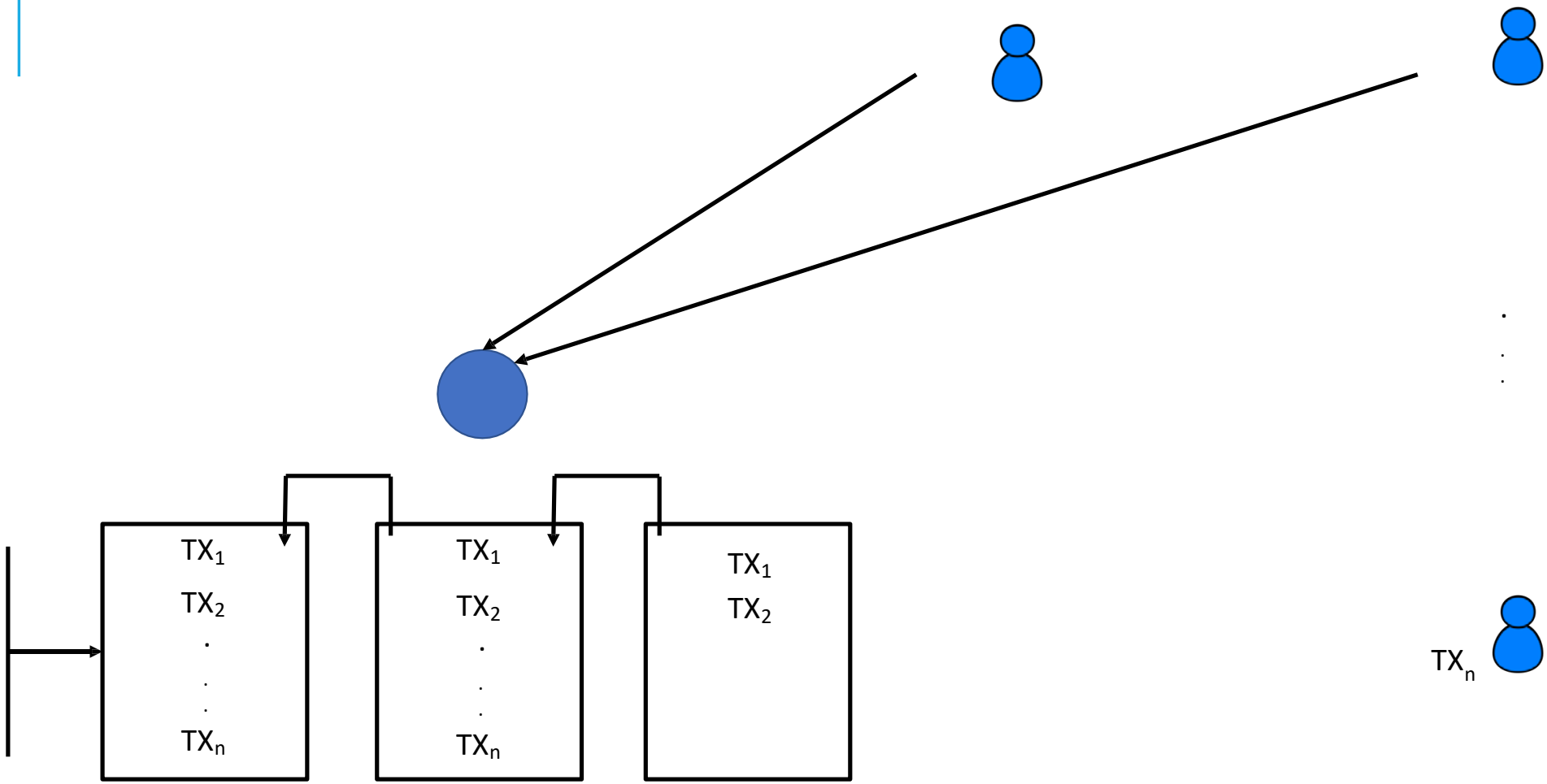
MINING DETAILS



DSL

UCSB

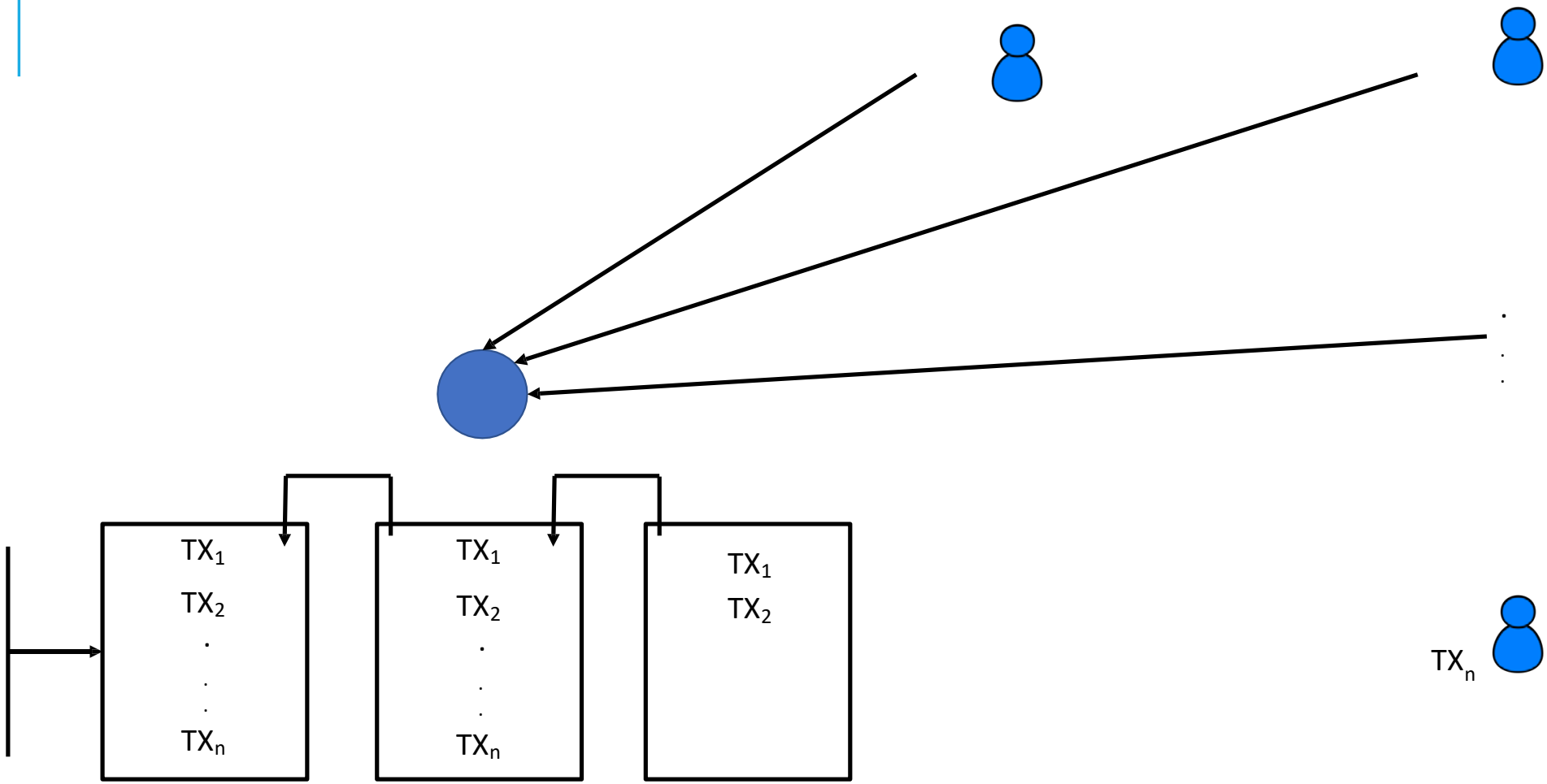
MINING DETAILS



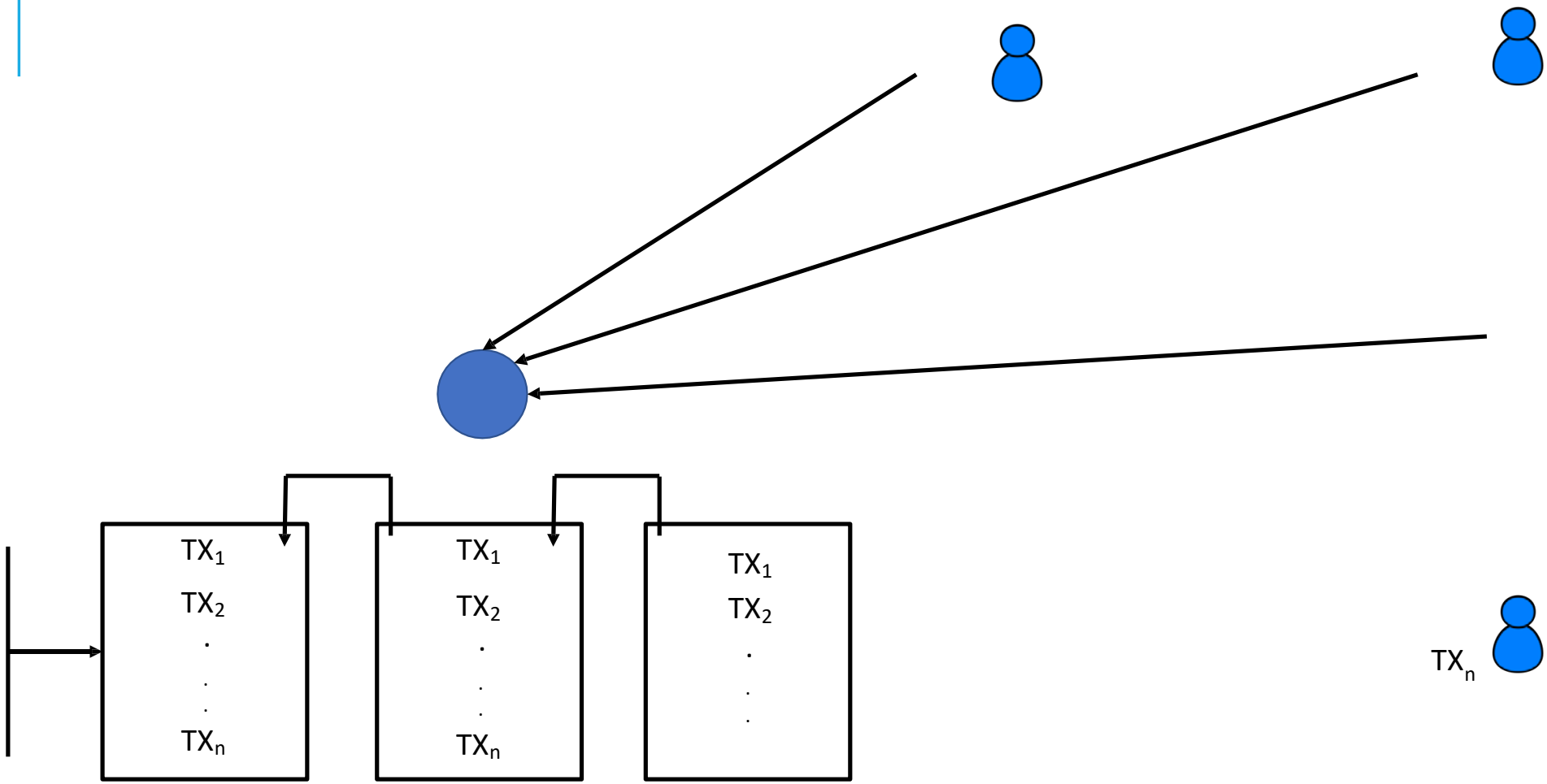
DSL

UCSB

MINING DETAILS



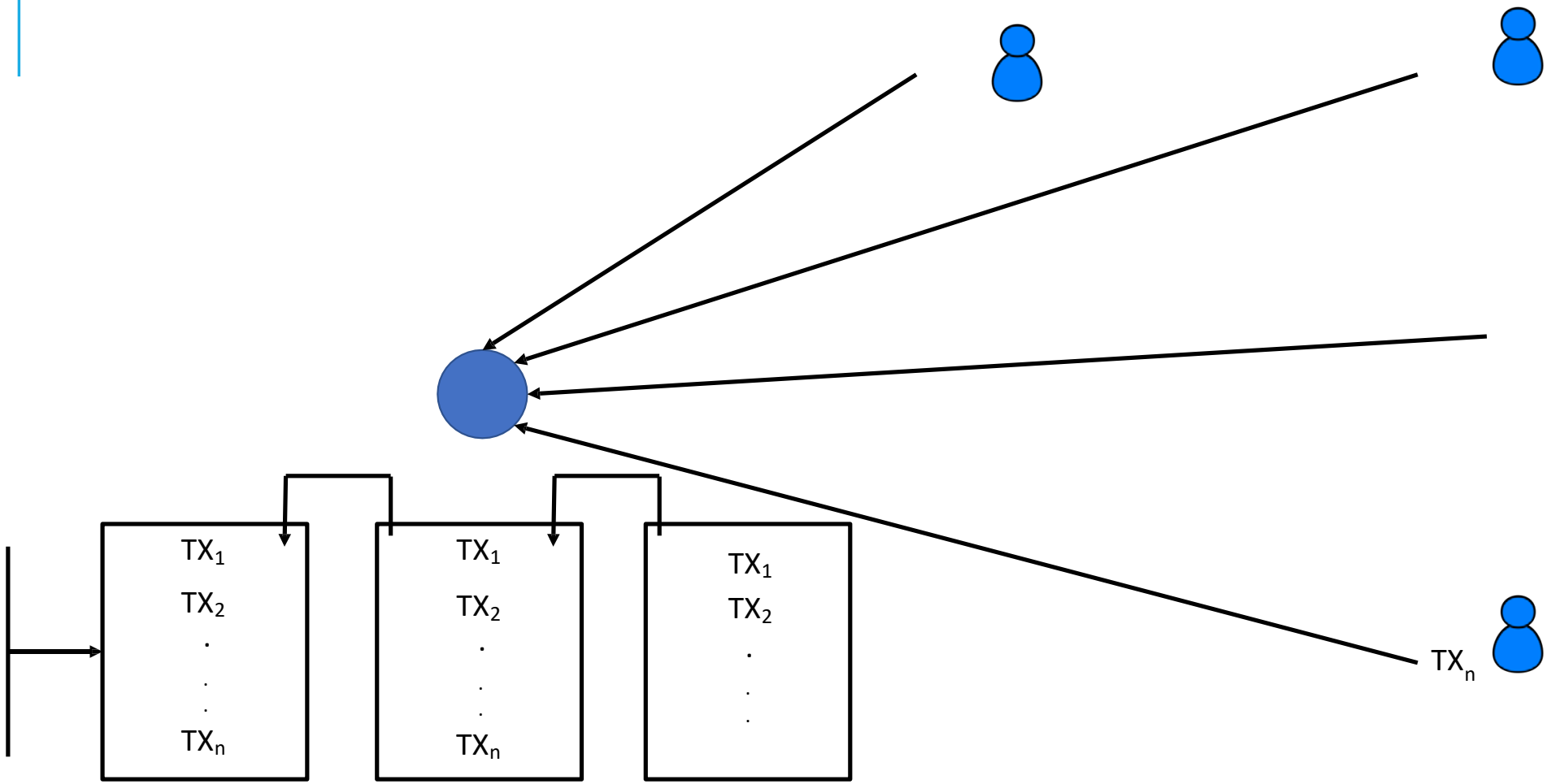
MINING DETAILS



DSL

UCSB

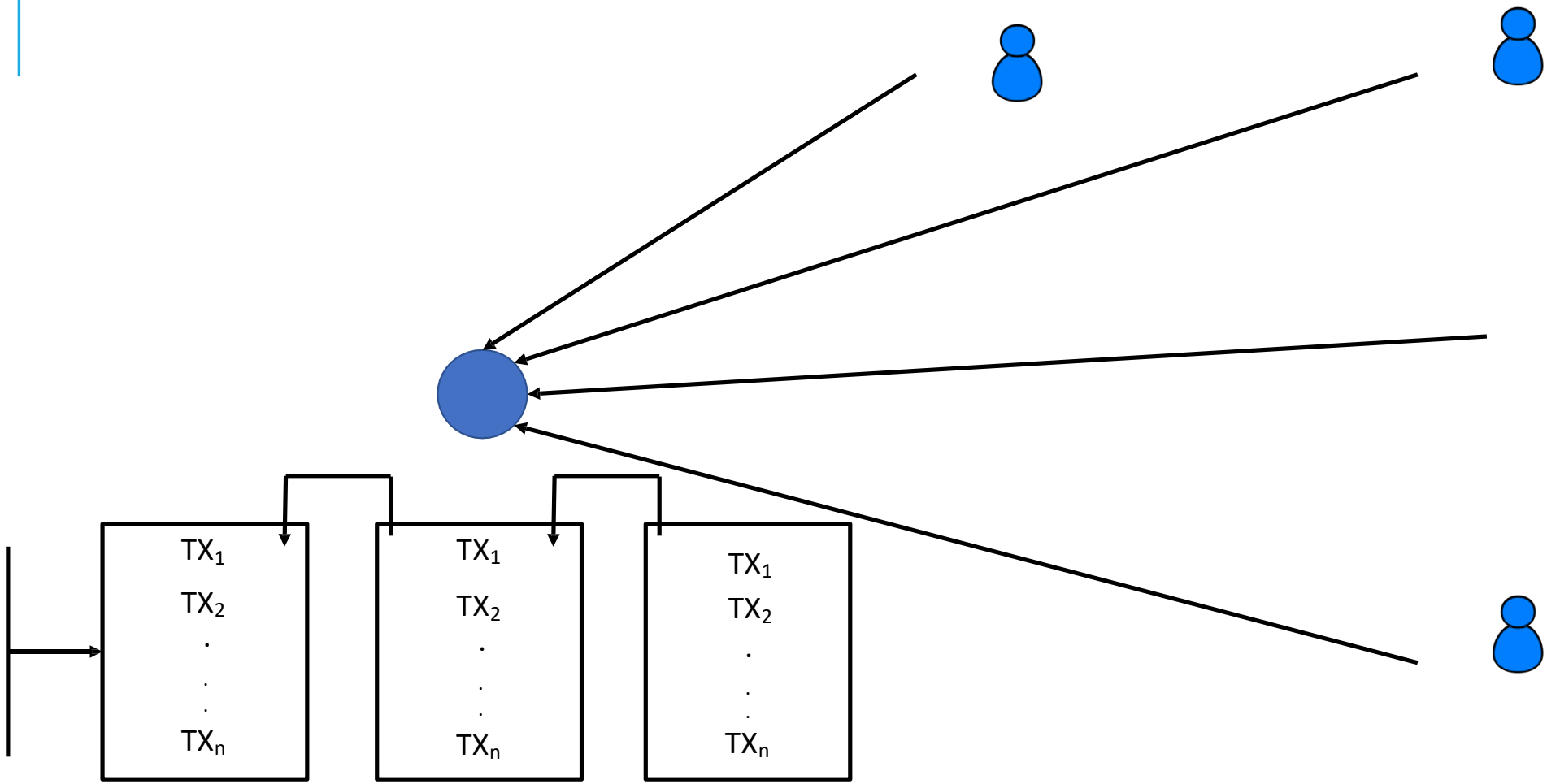
MINING DETAILS



DSL

UCSB

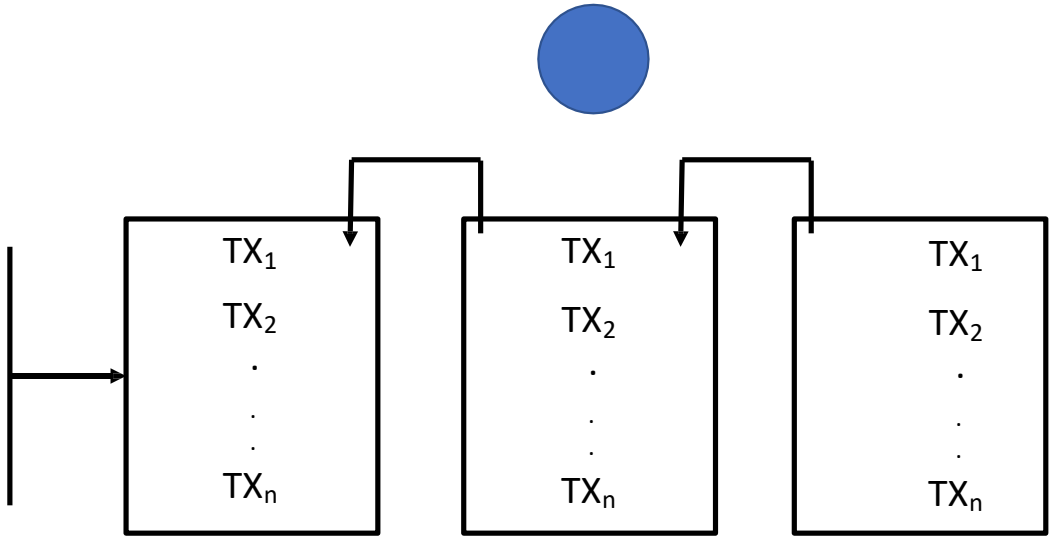
MINING DETAILS



DSL

UCSB

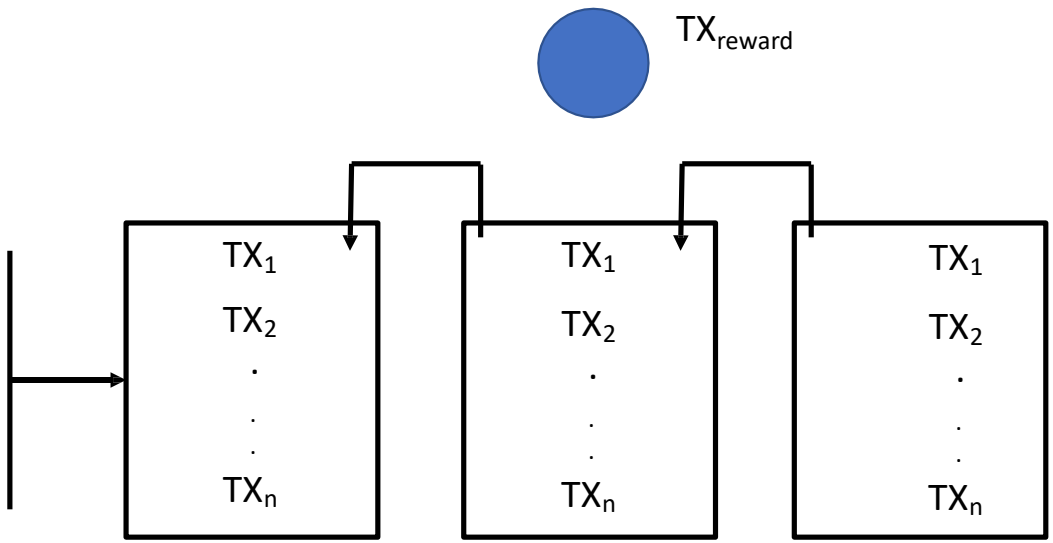
MINING DETAILS



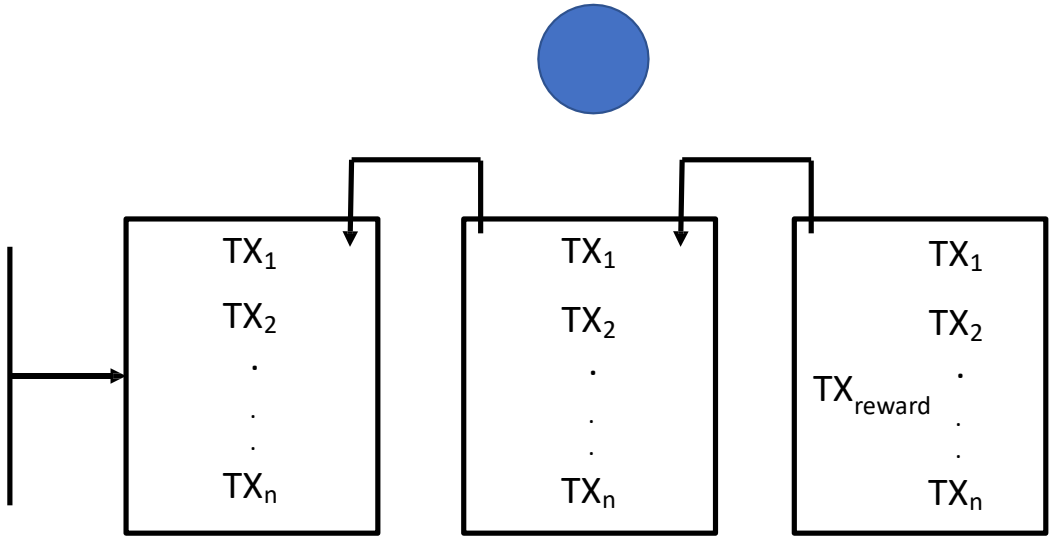
DSL

UCSB

MINING DETAILS



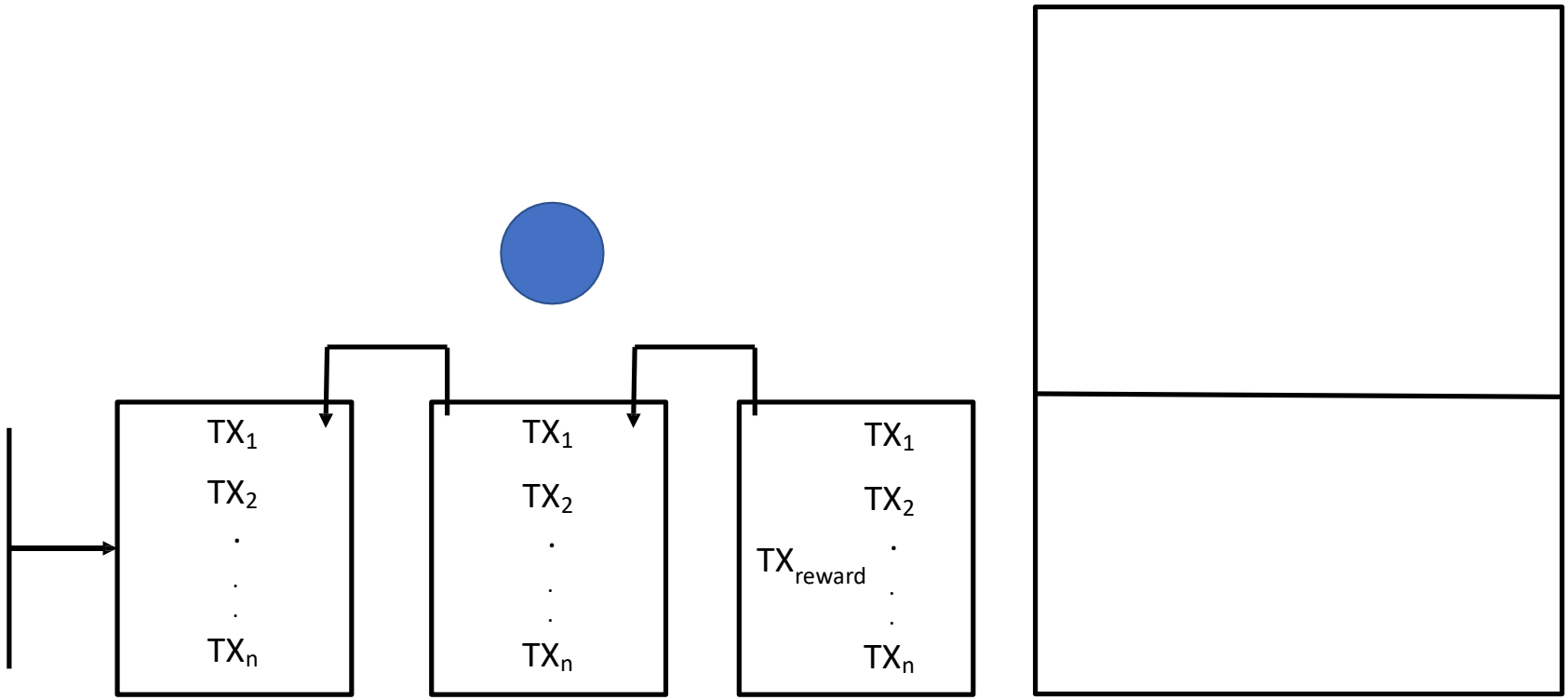
MINING DETAILS



DSL

UCSB

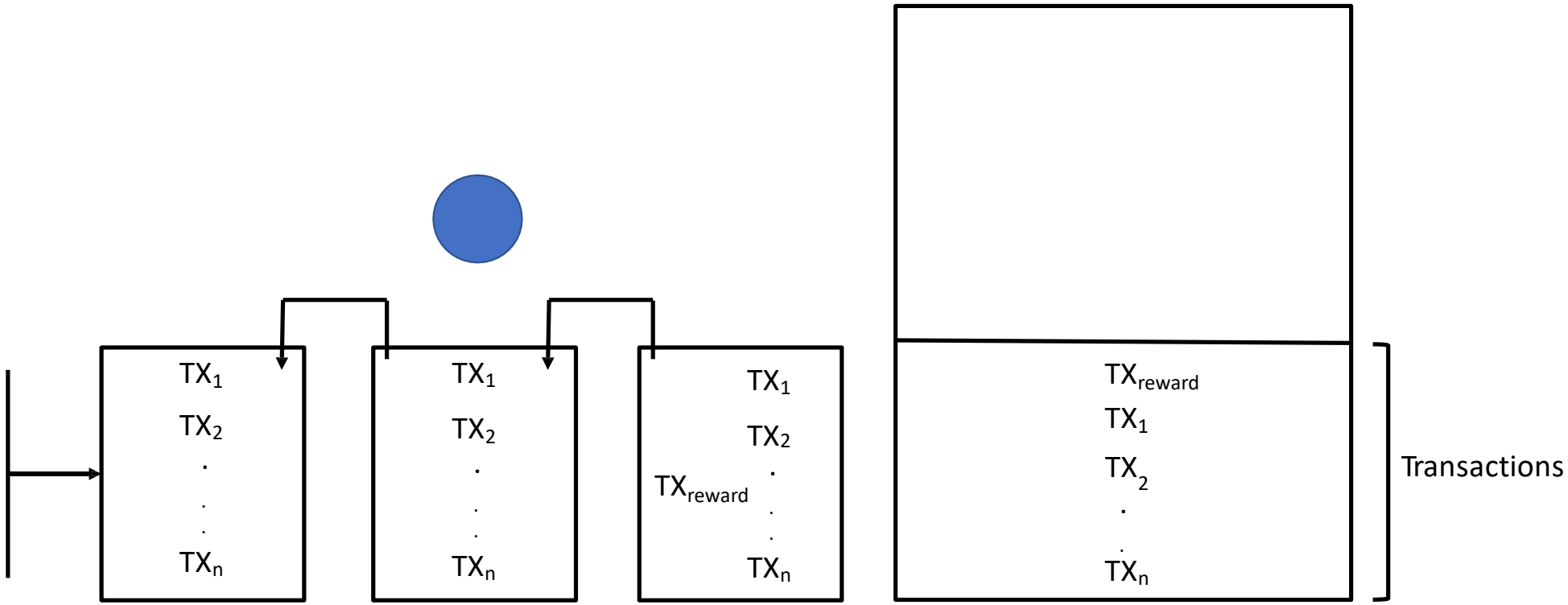
MINING DETAILS



DSL

UCSB

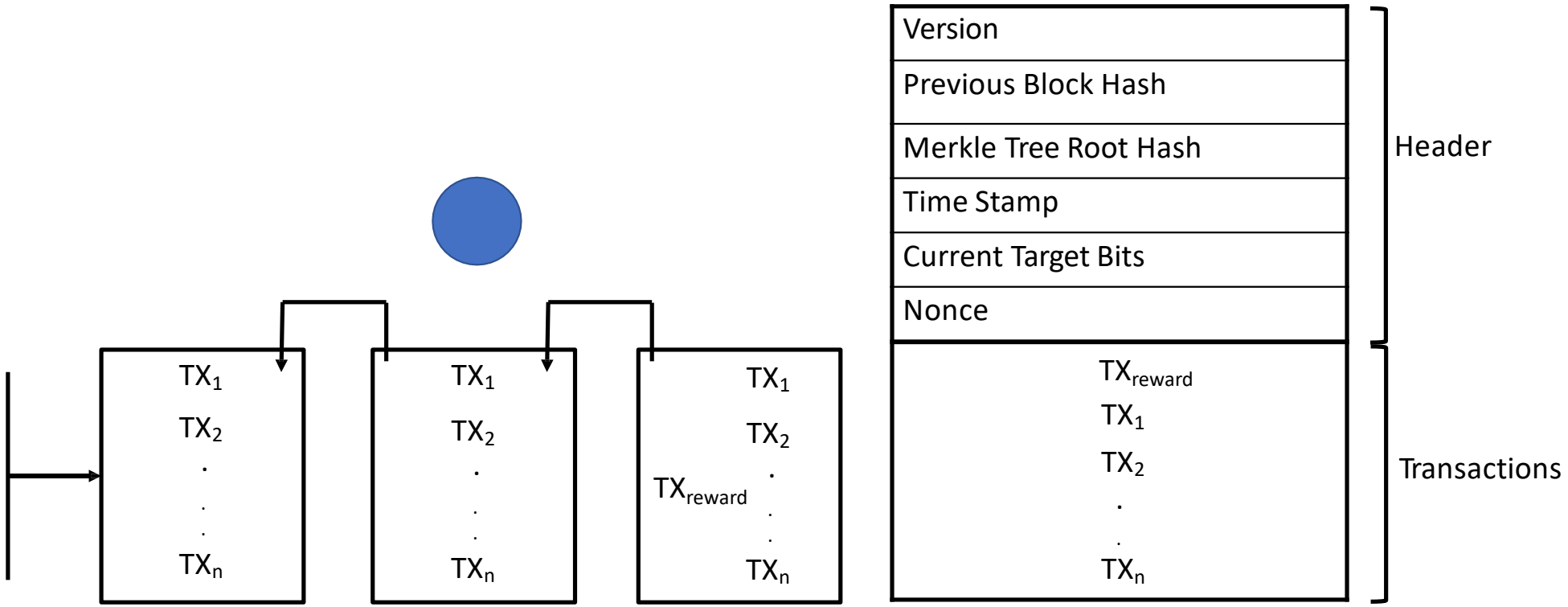
MINING DETAILS



DSL

UCSB

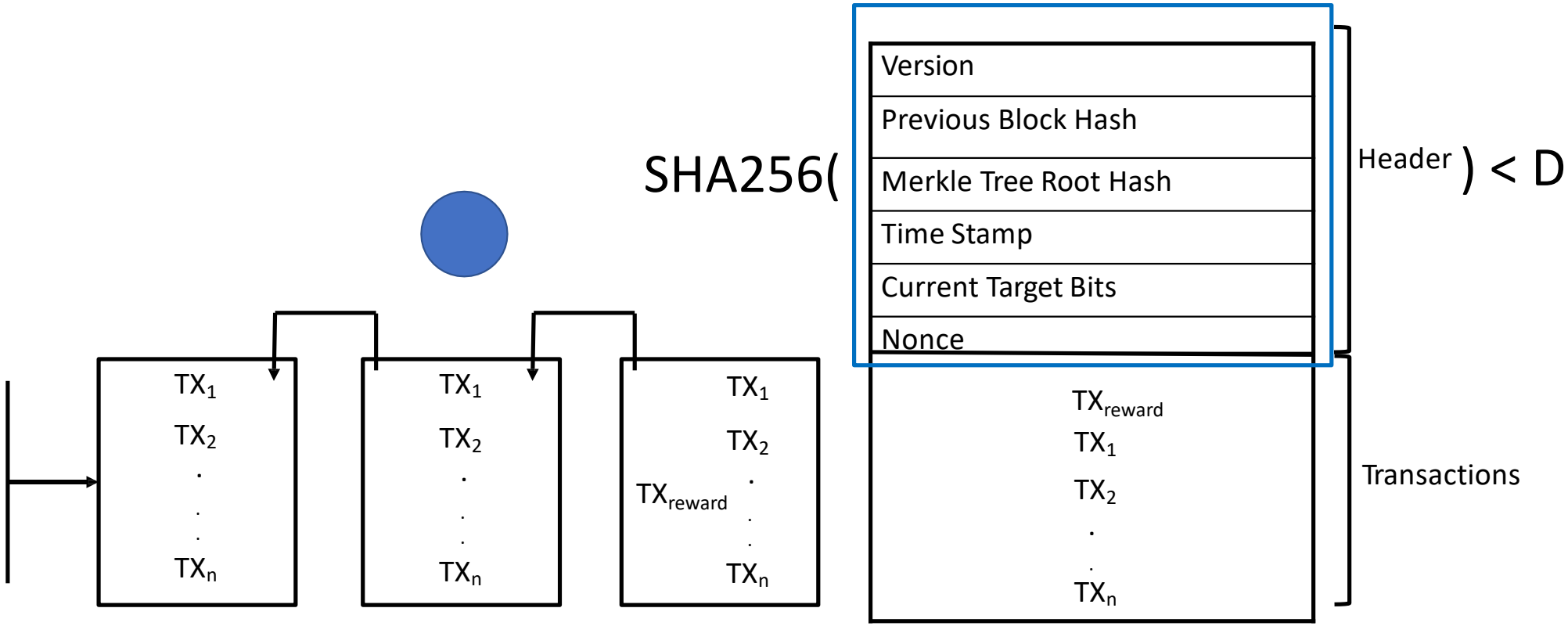
MINING DETAILS



DSL

UCSB

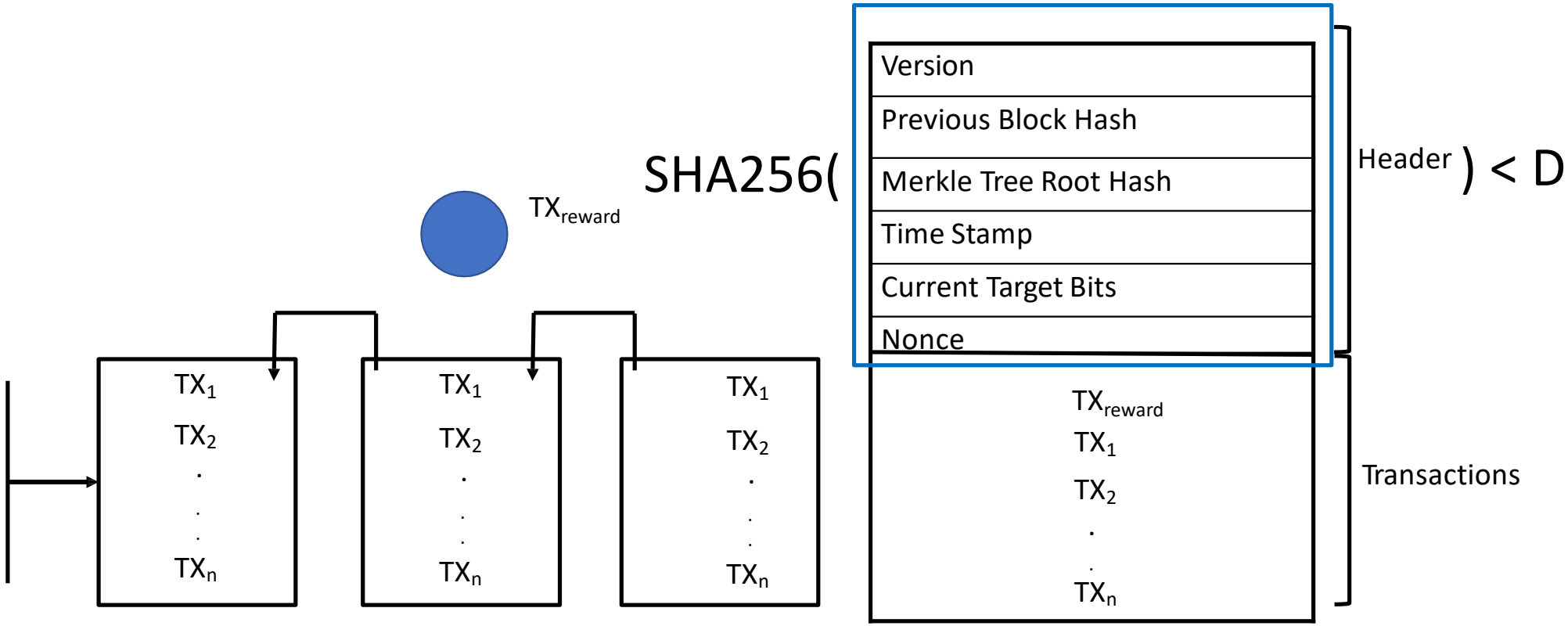
MINING DETAILS



DSL

UCSB

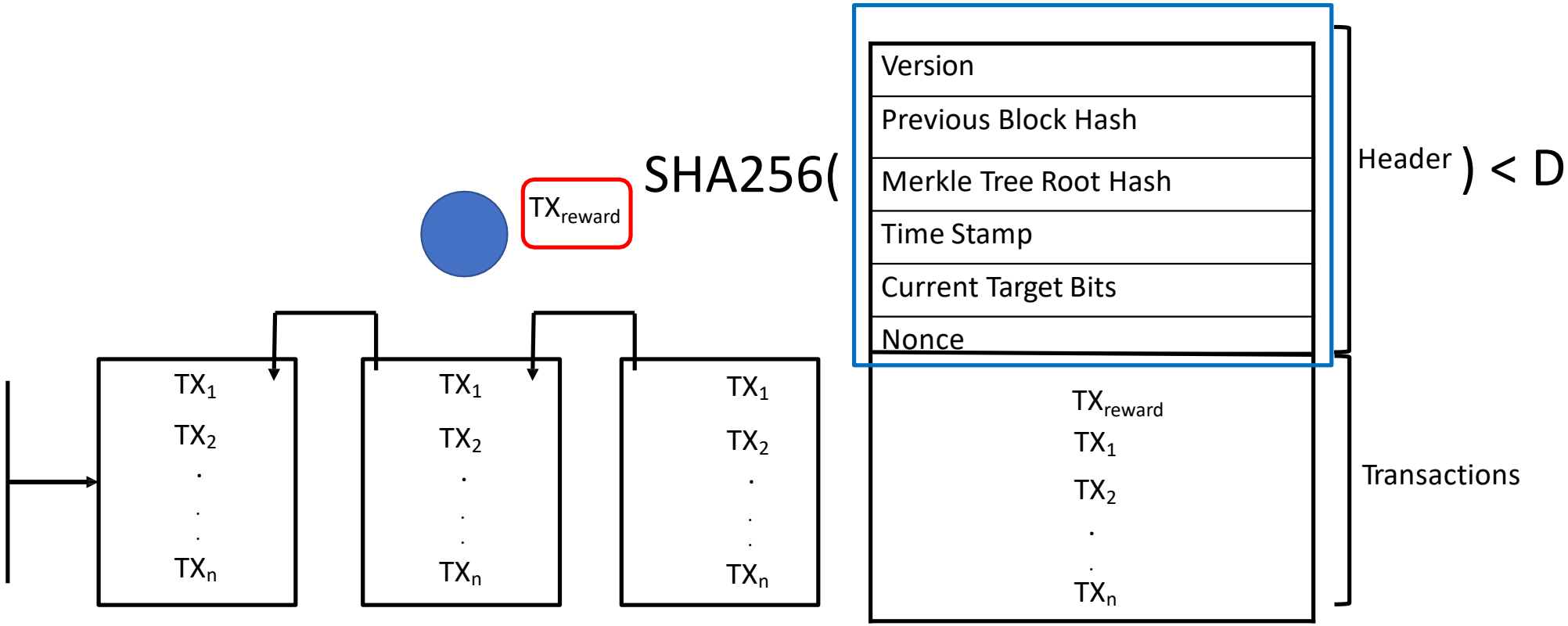
MINING DETAILS



DSL

UCSB

MINING DETAILS

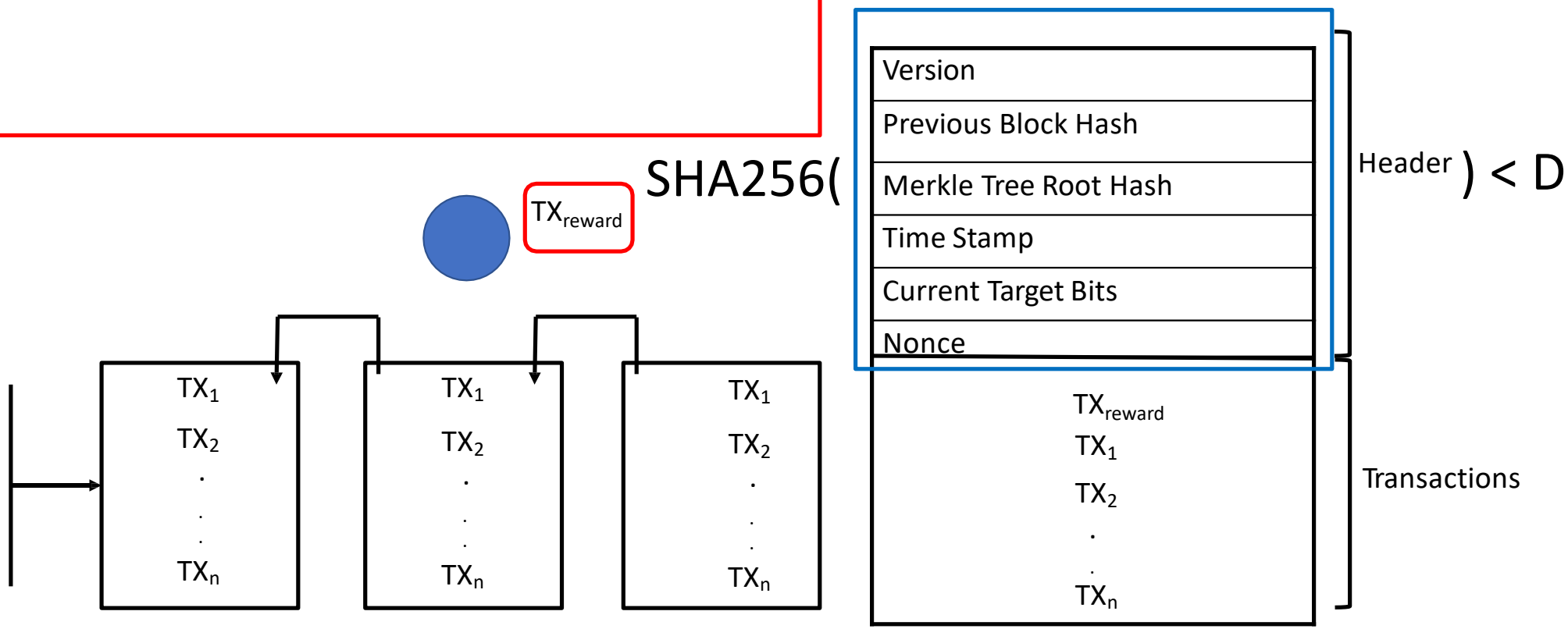


DSL

UCSB

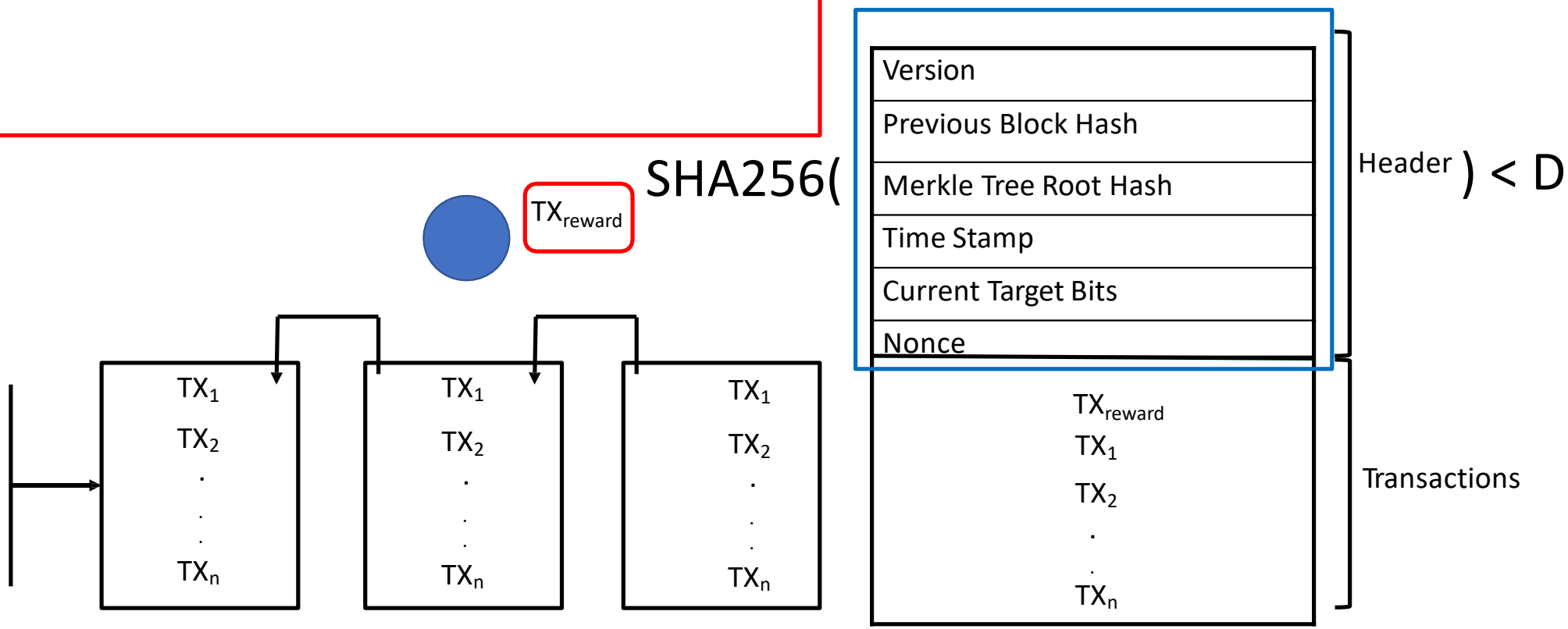
MINING DETAILS

- TX_{reward} is self signed (also called coinbase transaction)



MINING DETAILS

- TX_{reward} is self signed (also called coinbase transaction)
- TX_{reward} is bitcoin's way to create new coins

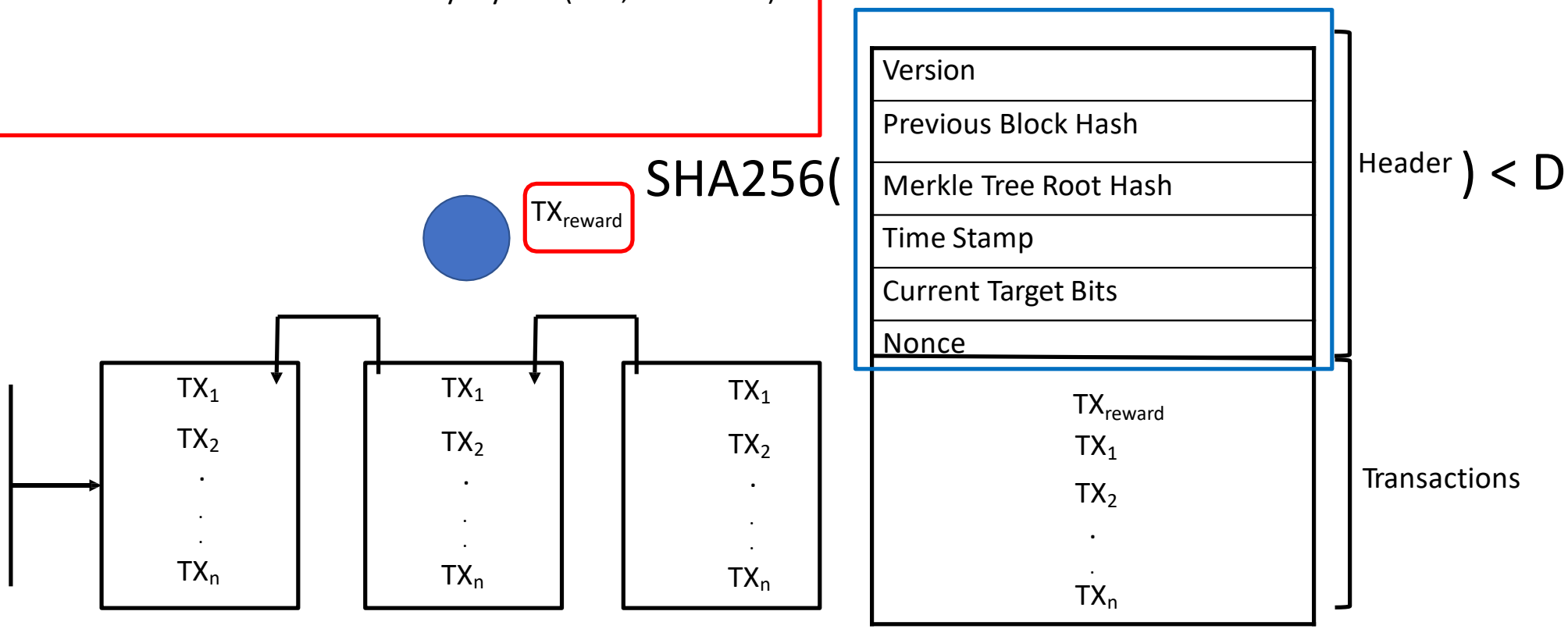


DSL

UCSB

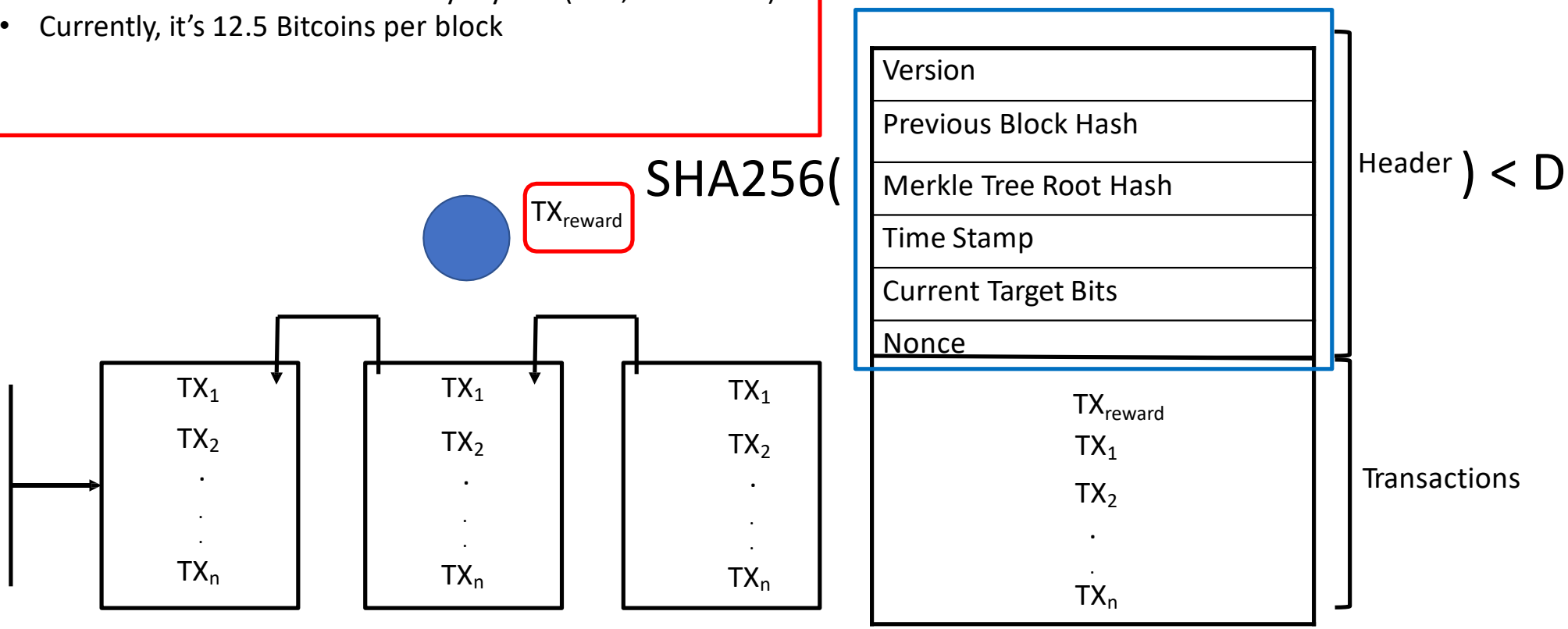
MINING DETAILS

- TX_{reward} is self signed (also called coinbase transaction)
- TX_{reward} is bitcoin's way to create new coins
- The reward value is halved every 4 years (210,000 blocks)



MINING DETAILS

- TX_{reward} is self signed (also called coinbase transaction)
- TX_{reward} is bitcoin's way to create new coins
- The reward value is halved every 4 years (210,000 blocks)
- Currently, it's 12.5 Bitcoins per block

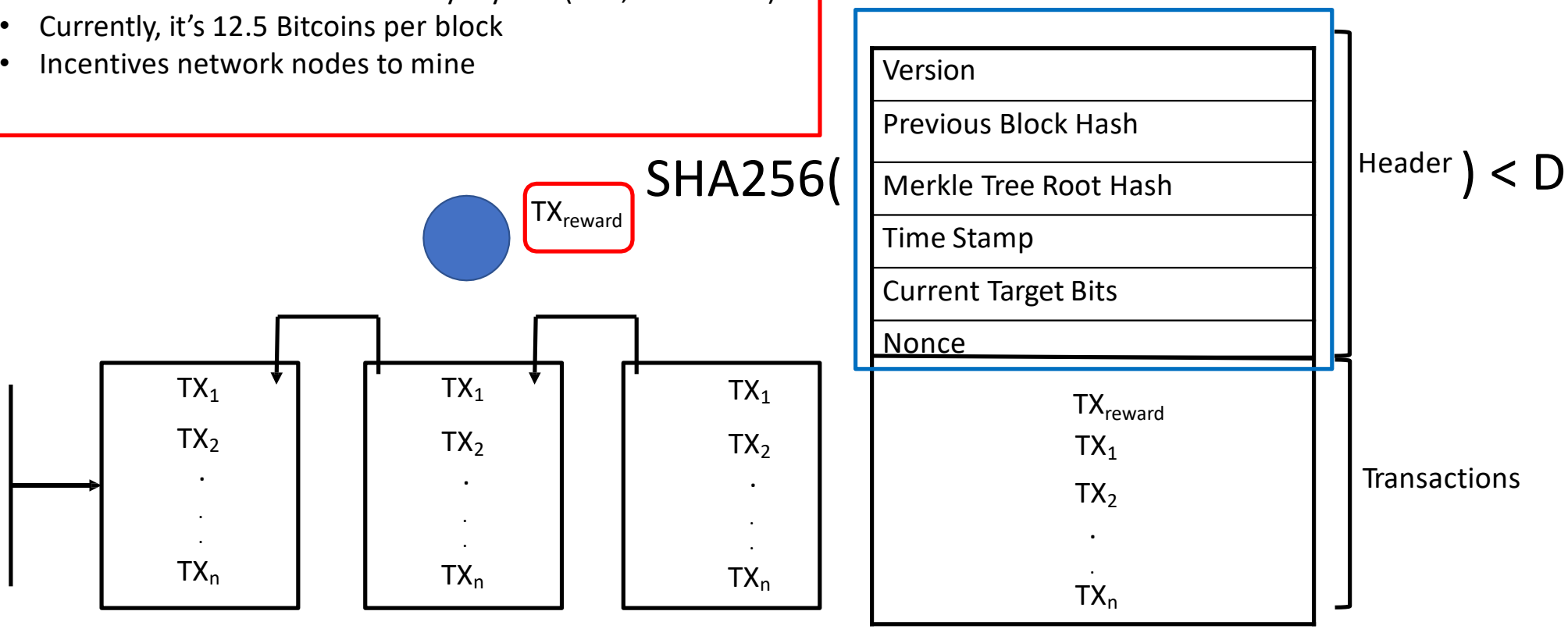


DSL

UCSB

MINING DETAILS

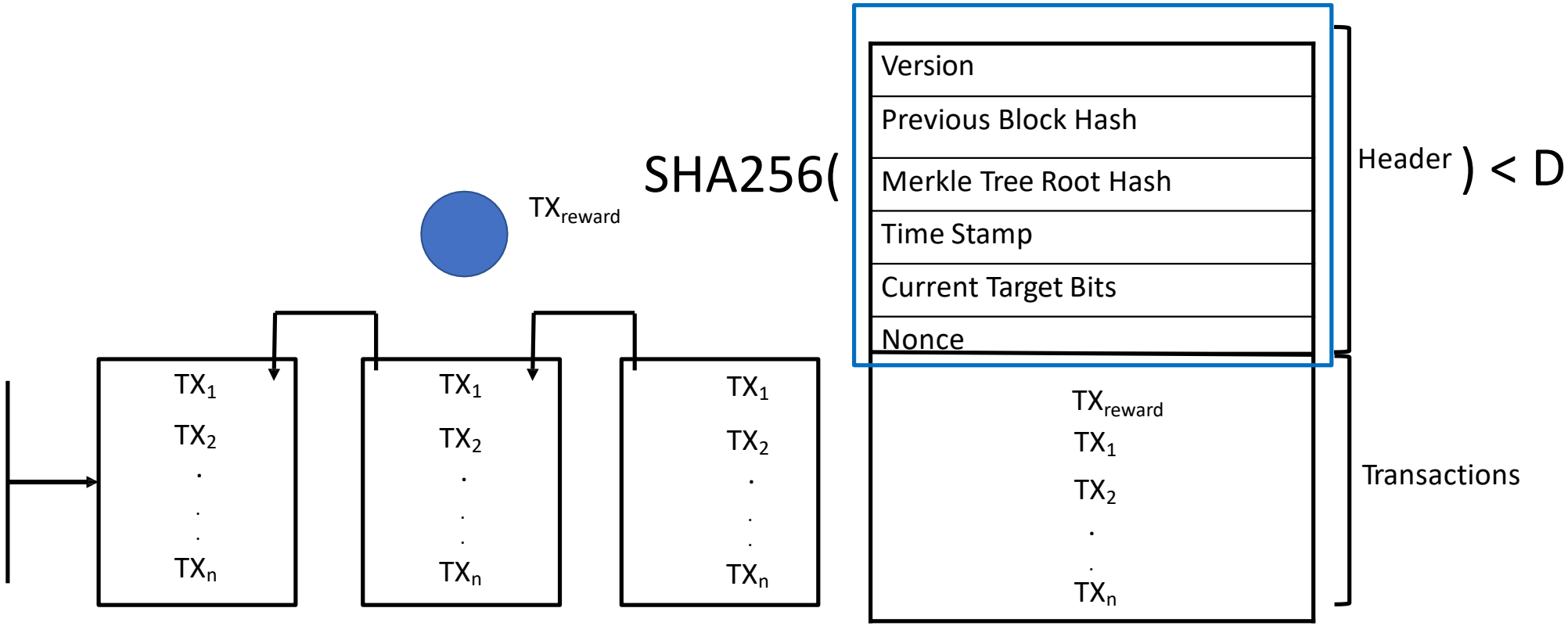
- TX_{reward} is self signed (also called coinbase transaction)
- TX_{reward} is bitcoin's way to create new coins
- The reward value is halved every 4 years (210,000 blocks)
- Currently, it's 12.5 Bitcoins per block
- Incentives network nodes to mine



DSL

UCSB

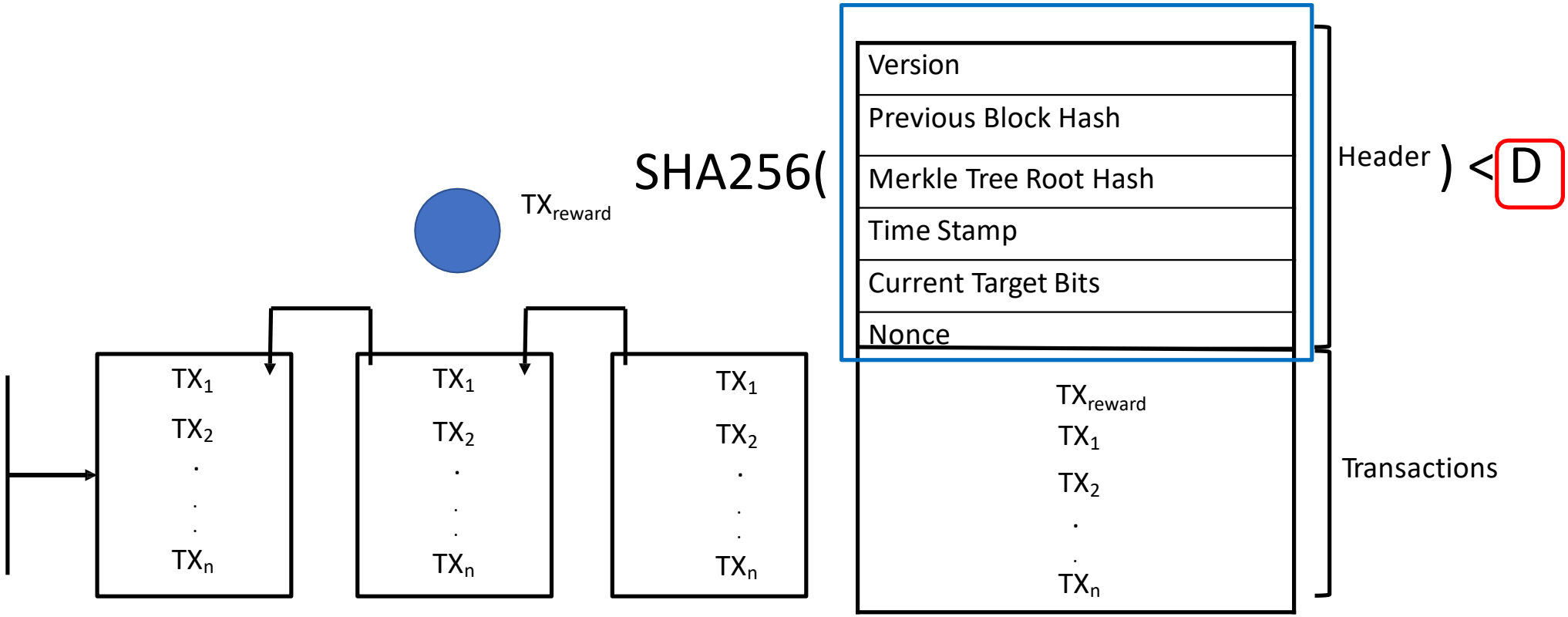
MINING DETAILS



DSL

UCSB

MINING DETAILS

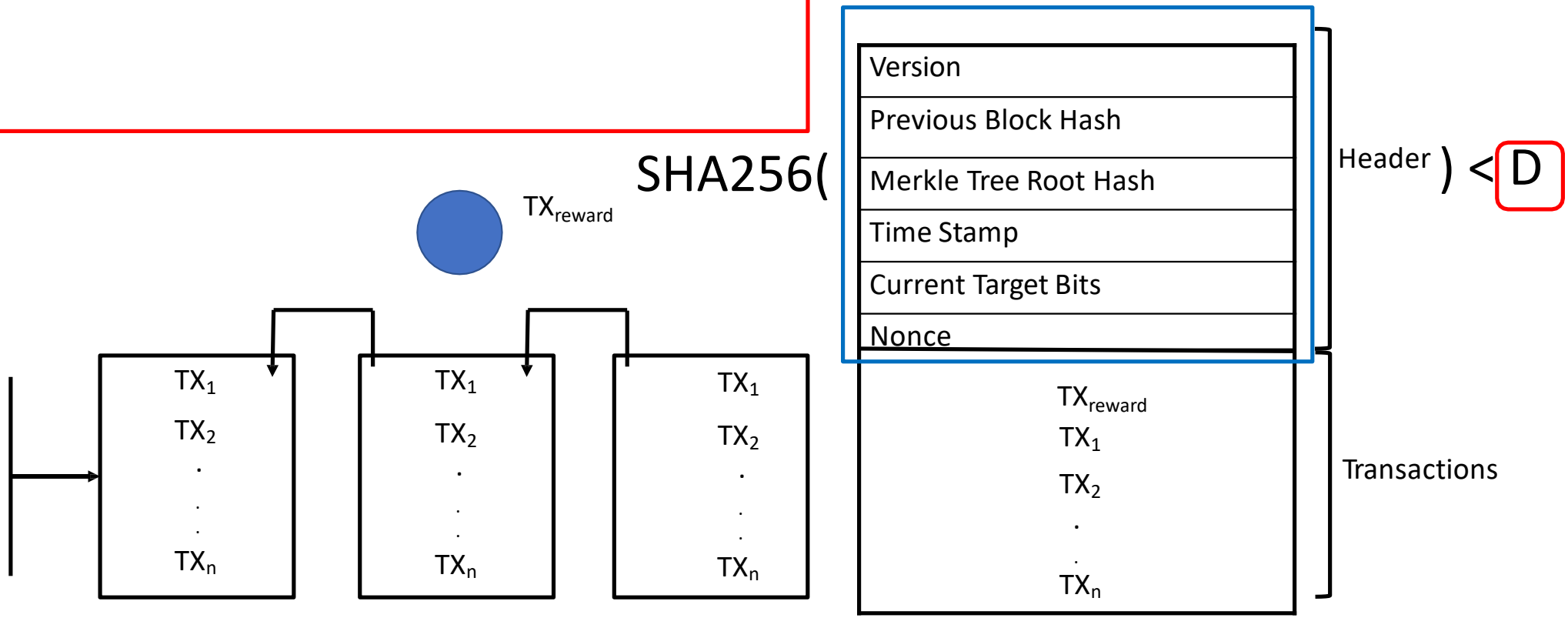


DSL

UCSB

MINING DETAILS

- D: dynamically adjusted difficulty



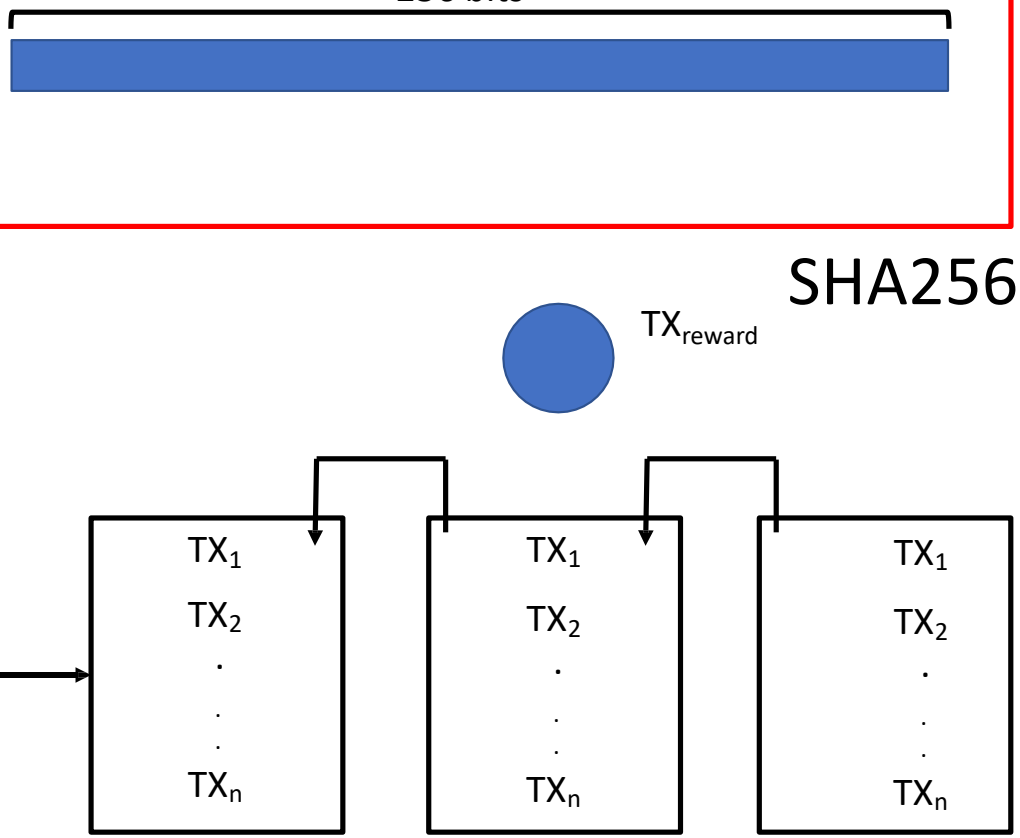
DSL

UCSB

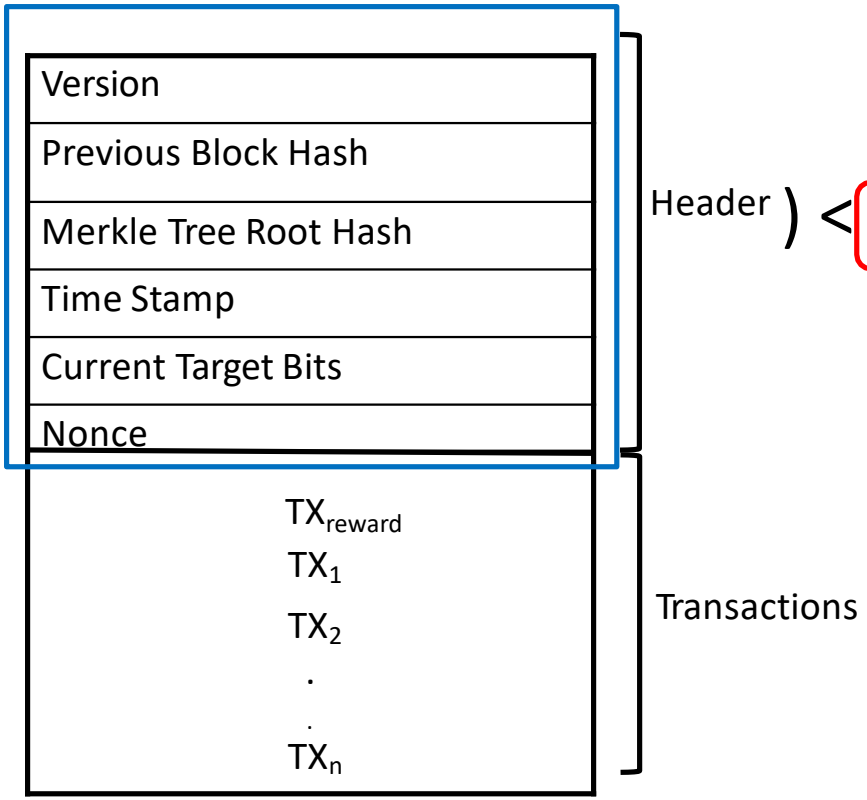
MINING DETAILS

- D: dynamically adjusted difficulty

256 bits



SHA256(



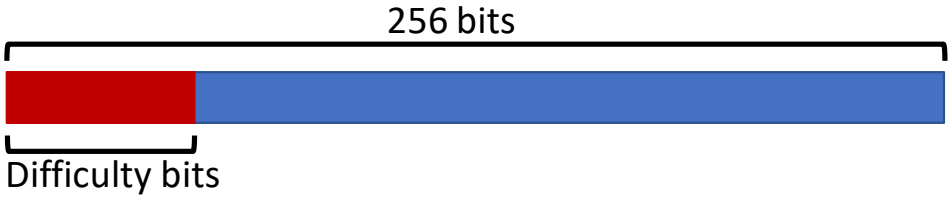
) < D

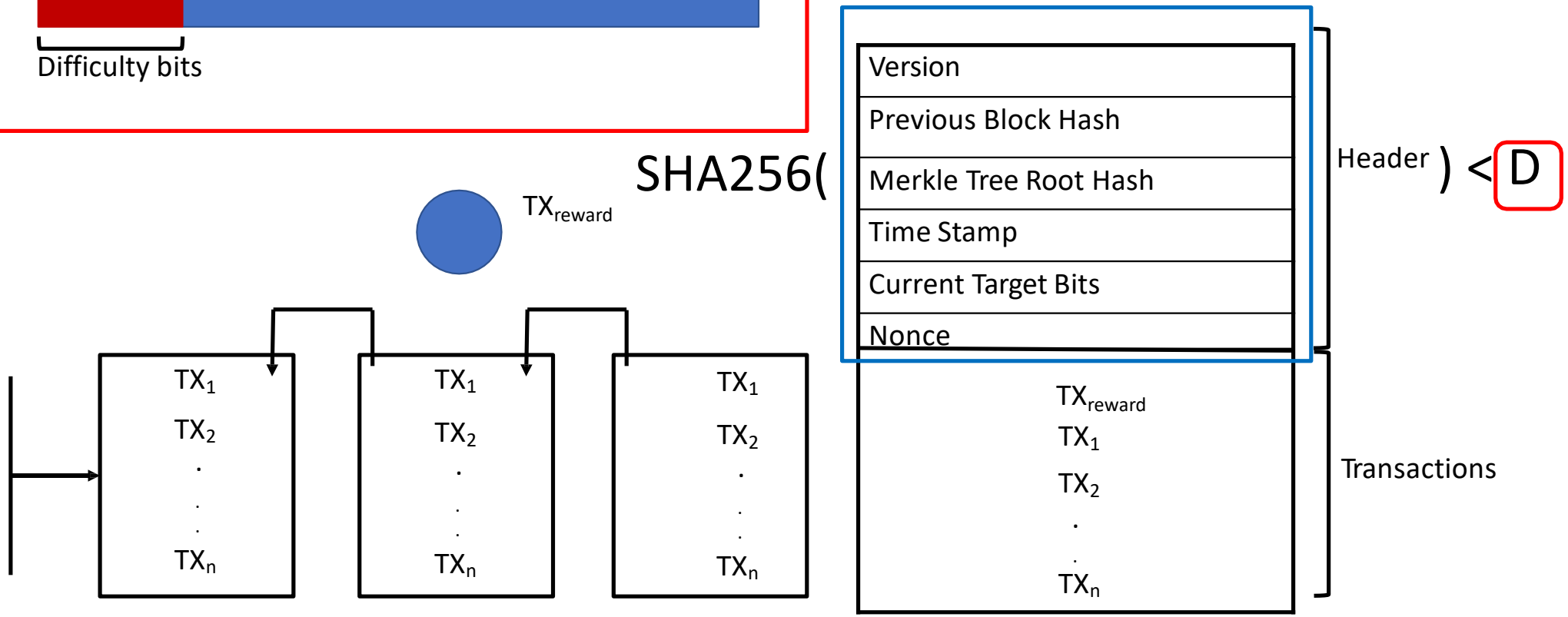
DSL

UCSB

MINING DETAILS

- D: dynamically adjusted difficulty



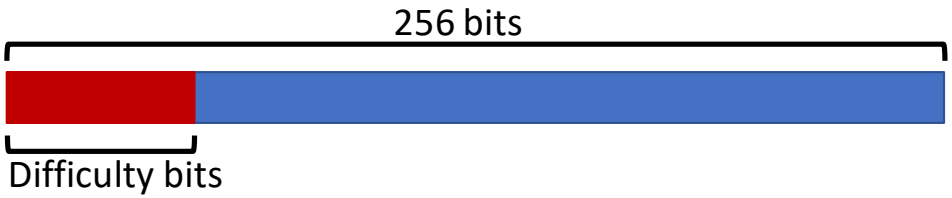


DSL

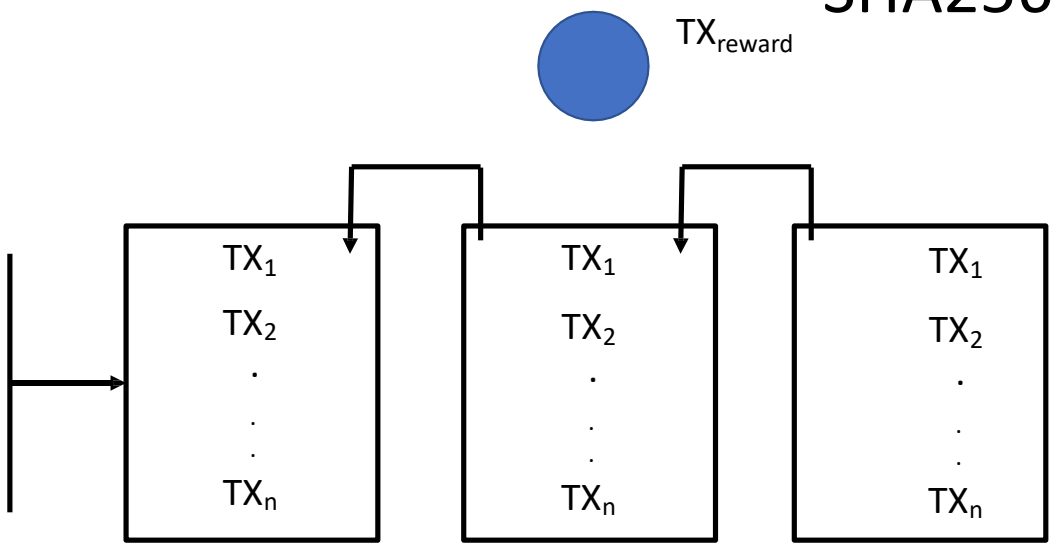
UCSB

MINING DETAILS

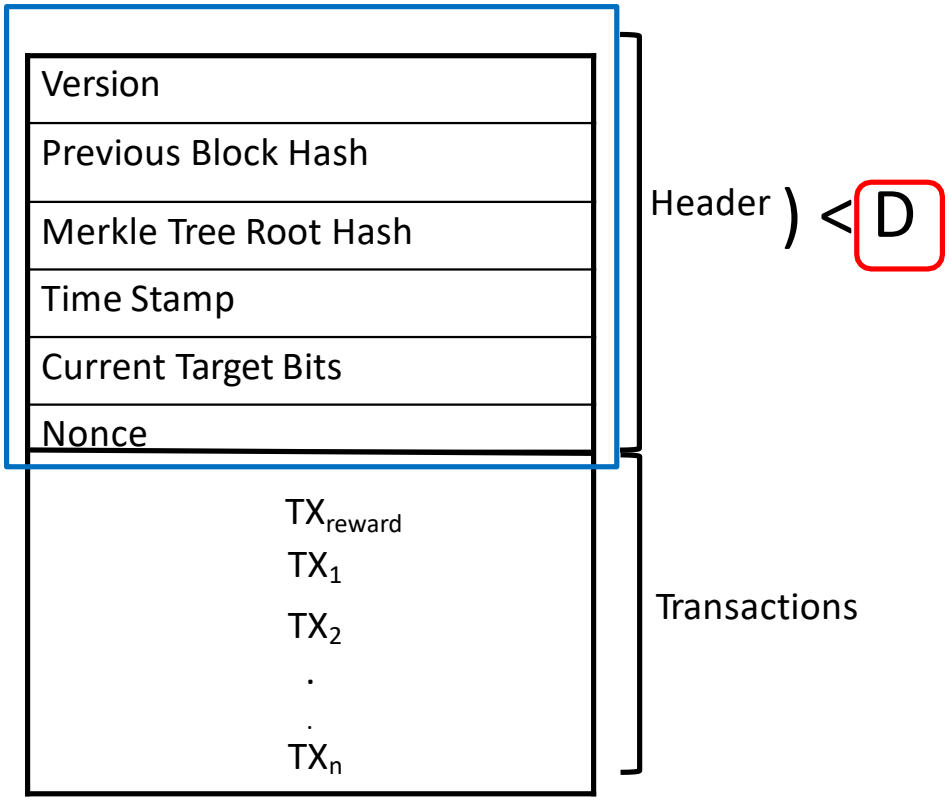
- D: dynamically adjusted difficulty



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



SHA256(



) < D

DIFFICULTY

DIFFICULTY

- Adjust difficulty every 2016 blocks

DIFFICULTY

- Adjust difficulty every 2016 blocks
- Expected 20160 mins to mine (10 mins per block)

DIFFICULTY

- Adjust difficulty every 2016 blocks
- Expected 20160 mins to mine (10 mins per block)
- Actual time = timestamp of block 2016 – time stamp of block 1

DIFFICULTY

- Adjust difficulty every 2016 blocks
- Expected 20160 mins to mine (10 mins per block)
- Actual time = timestamp of block 2016 – time stamp of block 1
- New_difficulty = old_difficulty * expected/actual

DIFFICULTY

- Adjust difficulty every 2016 blocks
- Expected 20160 mins to mine (10 mins per block)
- Actual time = timestamp of block 2016 – time stamp of block 1
- New_difficulty = old_difficulty * expected/actual
- Difficulty decreases if actual > expected, otherwise, increases

DSL

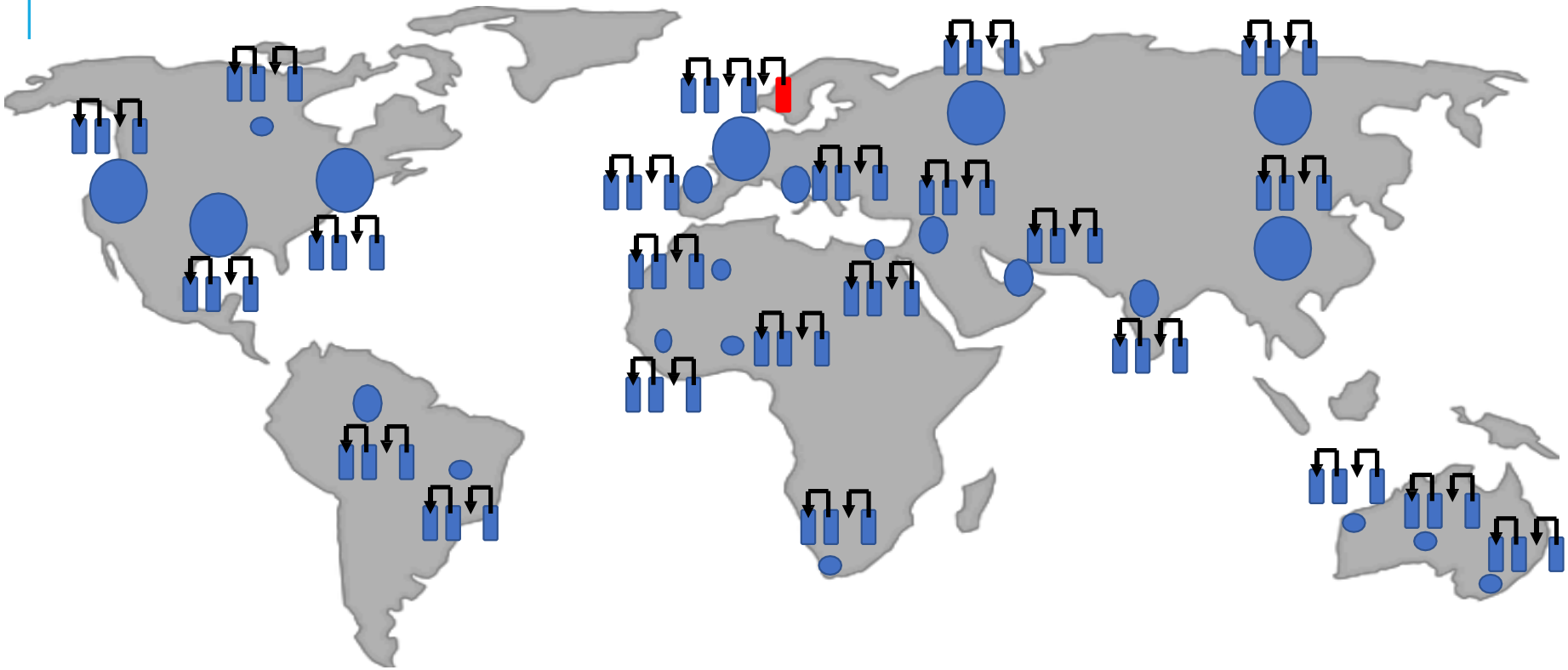
UCSB

MINING BIG PICTURE

DSL

UCSB

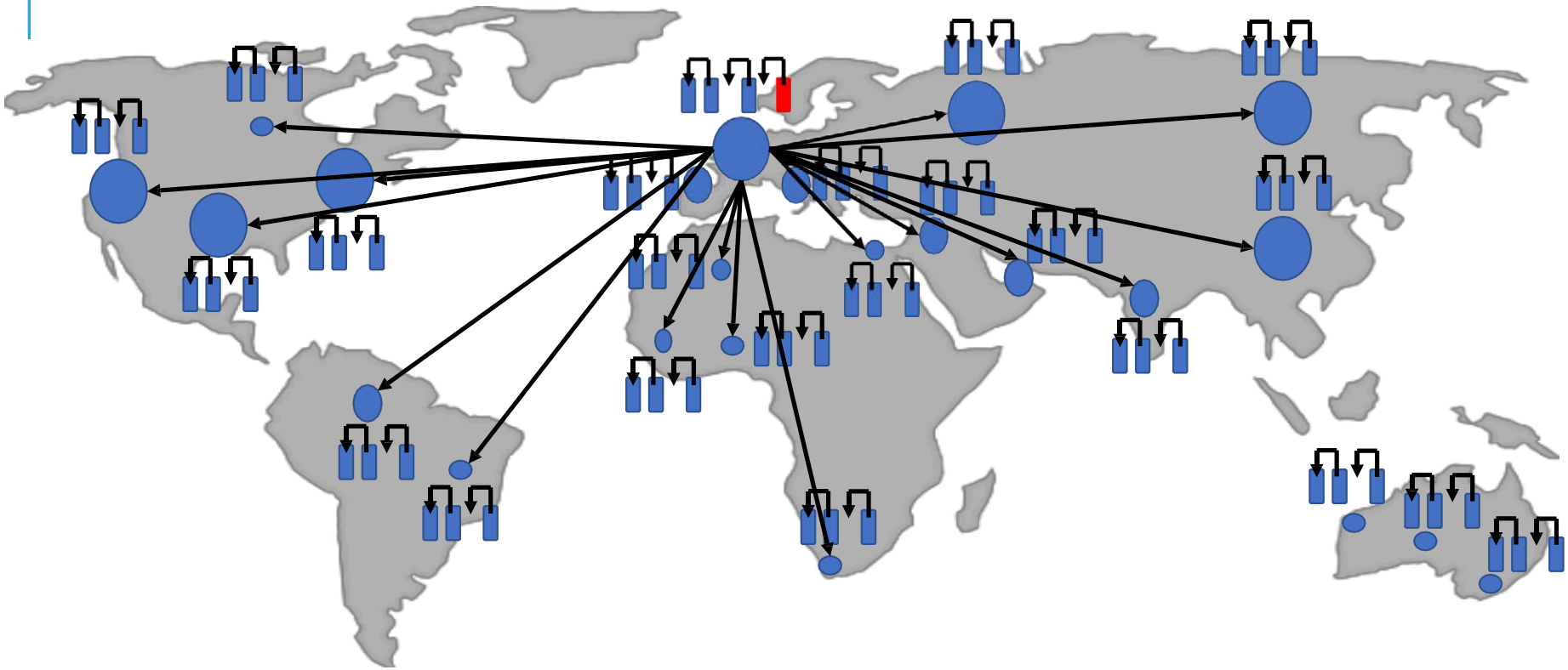
MINING BIG PICTURE



DSL

UCSB

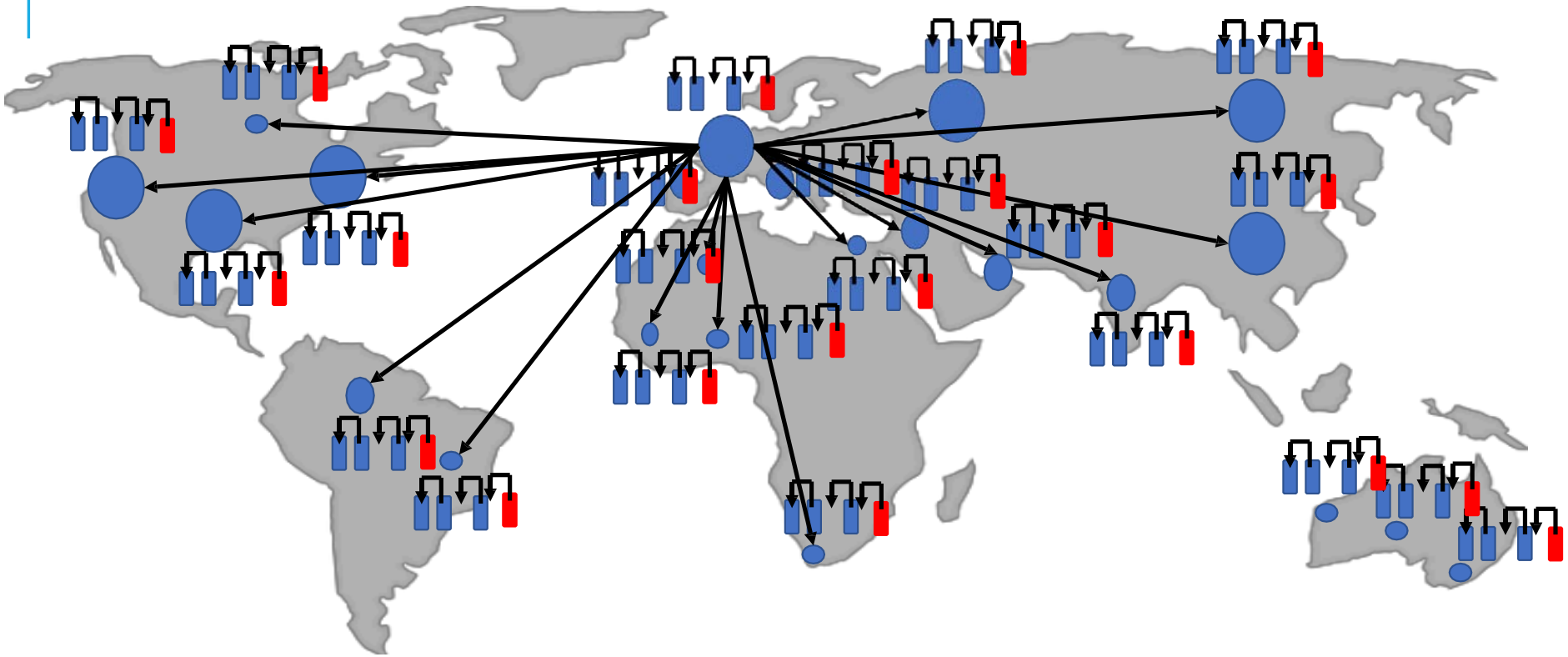
MINING BIG PICTURE



DSL

UCSB

MINING BIG PICTURE



MINING DETAILS

- Find a nonce that results in SHA256(block) < Difficulty

MINING DETAILS

- Find a nonce that results in SHA256(block) < Difficulty
- The solution space is a set. Once a solution is found, a block is mined

MINING DETAILS

- Find a nonce that results in SHA256(block) < Difficulty
- The solution space is a set. Once a solution is found, a block is mined
- Easily verified by network nodes

MINING DETAILS

- Find a nonce that results in SHA256(block) < Difficulty
- The solution space is a set. Once a solution is found, a block is mined
- Easily verified by network nodes
- Cannot be precomputed
  - Depends on current block transactions and previous blocks

MINING DETAILS

- Find a nonce that results in SHA256(block) < Difficulty
- The solution space is a set. Once a solution is found, a block is mined
- Easily verified by network nodes
- Cannot be precomputed
  - Depends on current block transactions and previous blocks
- Cannot be stolen
  - Reward Transaction is signed to the public key of the miner

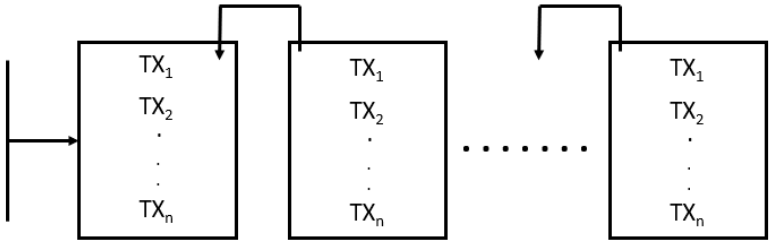
MINING DETAILS

- Find a nonce that results in SHA256(block) < Difficulty
- The solution space is a set. Once a solution is found, a block is mined
- Easily verified by network nodes
- Cannot be precomputed
  - Depends on current block transactions and previous blocks
- Cannot be stolen
  - Reward Transaction is signed to the public key of the miner
- Network nodes accept the first found block:
  - The problem is difficult, there is no guaranteed bound to find another block

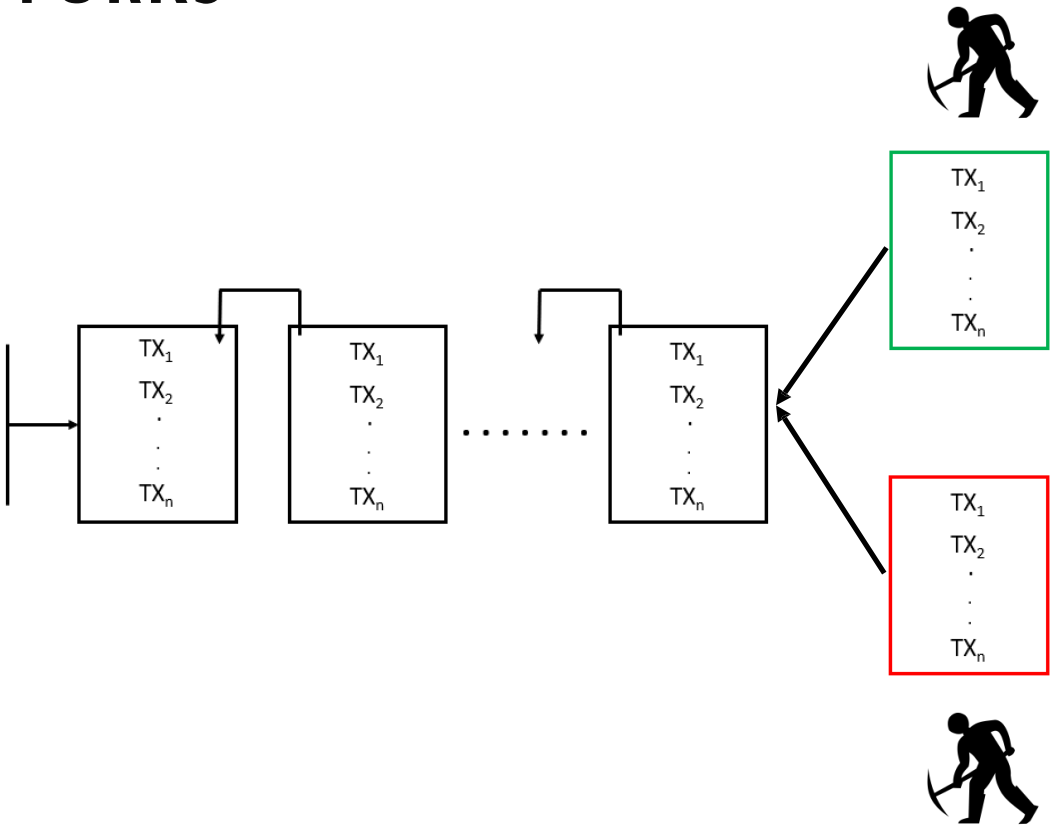
MINING DETAILS

- Find a nonce that results in SHA256(block) < Difficulty
- The solution space is a set. Once a solution is found, a block is mined
- Easily verified by network nodes
- Cannot be precomputed
  - Depends on current block transactions and previous blocks
- Cannot be stolen
  - Reward Transaction is signed to the public key of the miner
- Network nodes accept the first found block:
  - The problem is difficult, there is no guaranteed bound to find another block
- What happens when 2 nodes concurrently mine a block? Fork

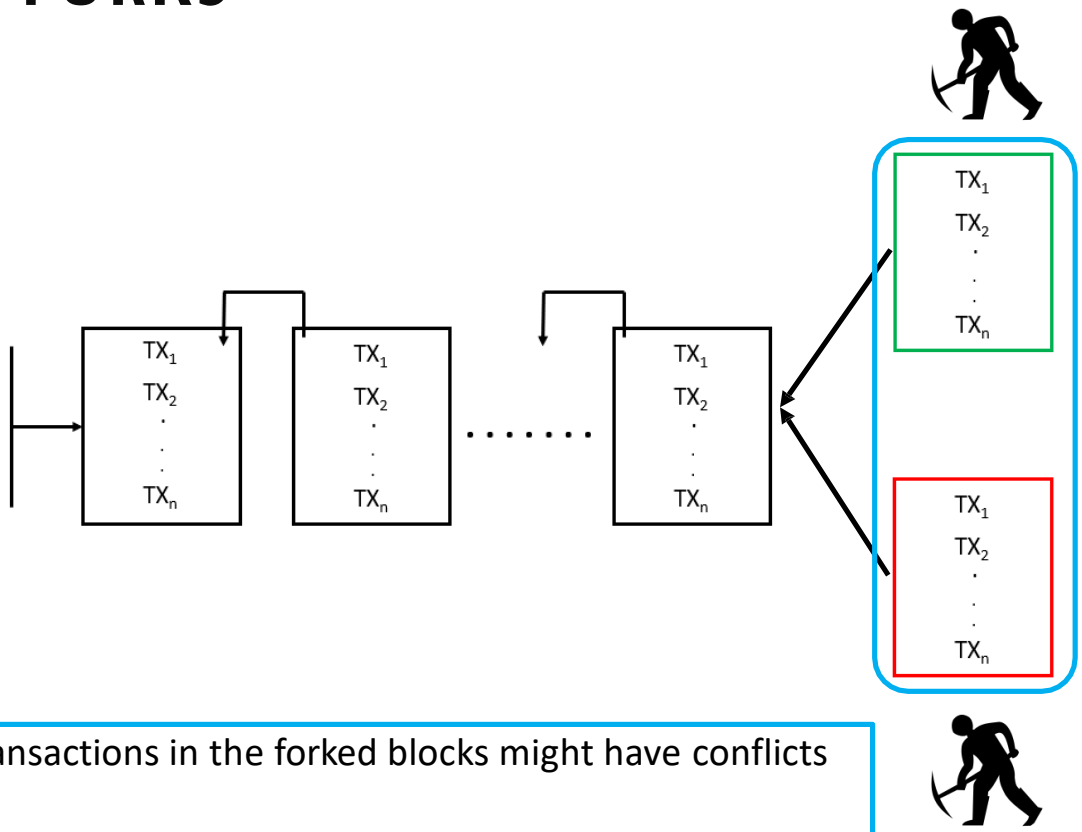
FORKS



FORKS

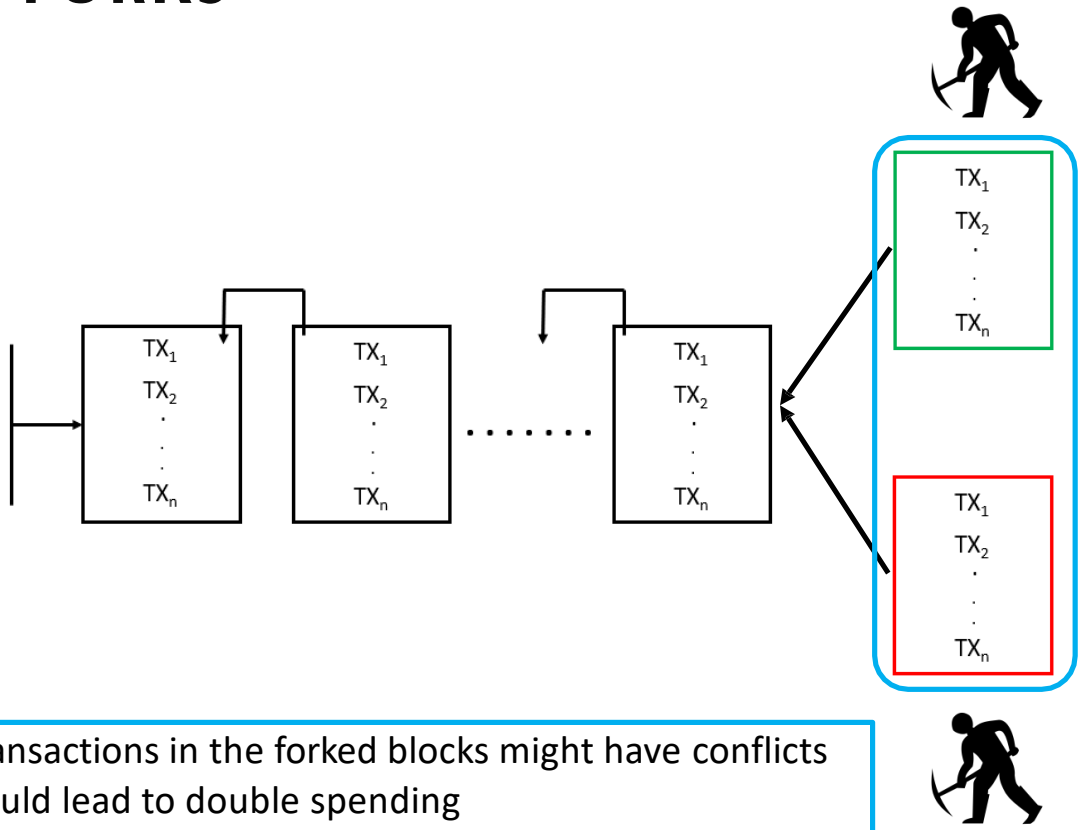


FORKS



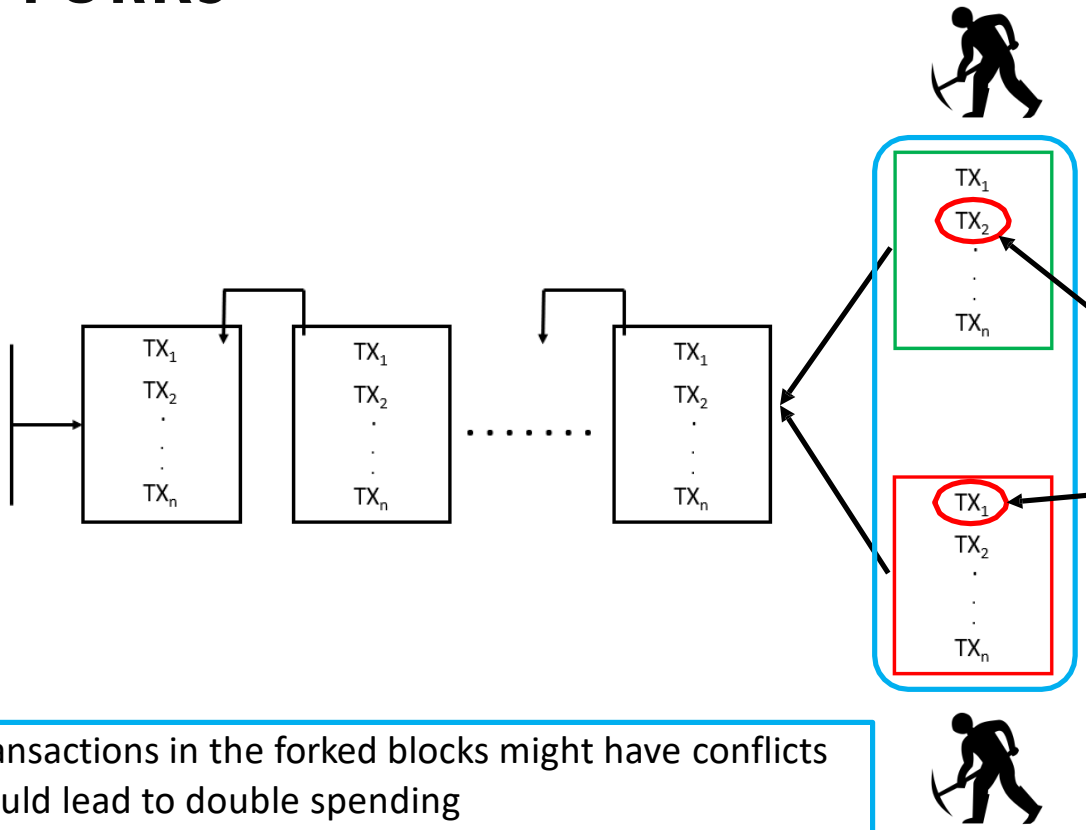
- Transactions in the forked blocks might have conflicts

FORKS



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

FORKS



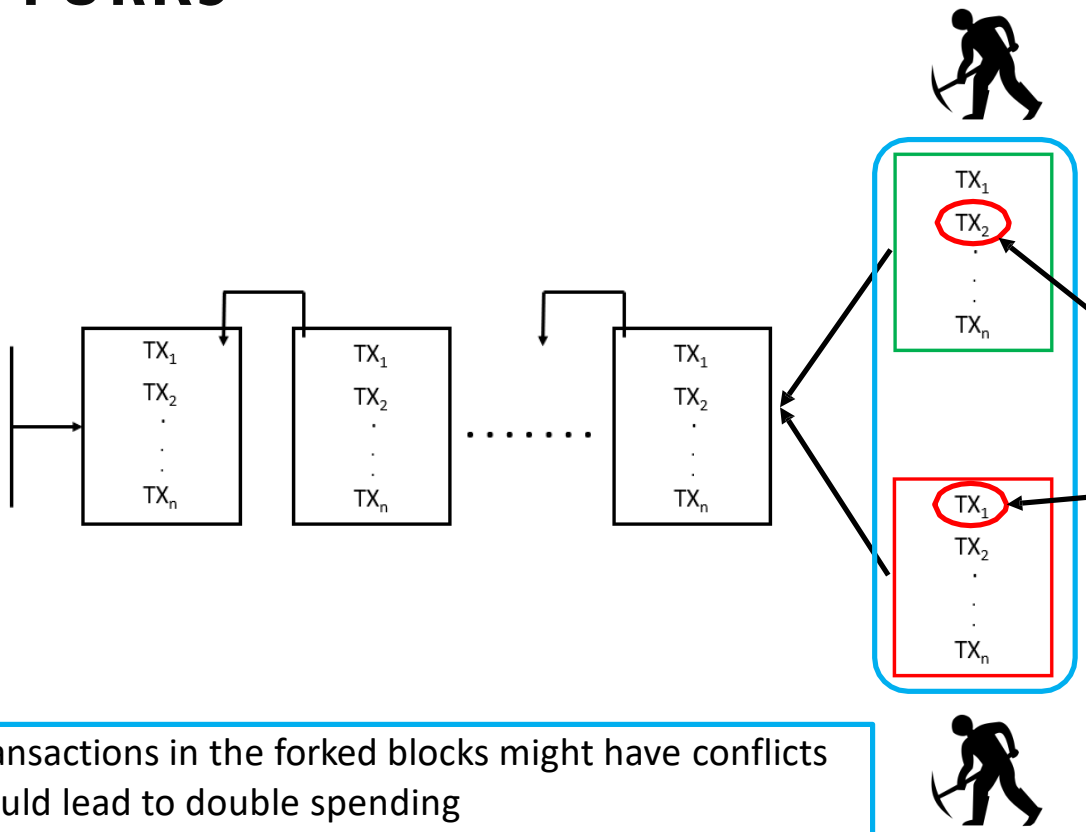
Bob tries to double spend the same coin twice in two transactions

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

DSL

UCSB

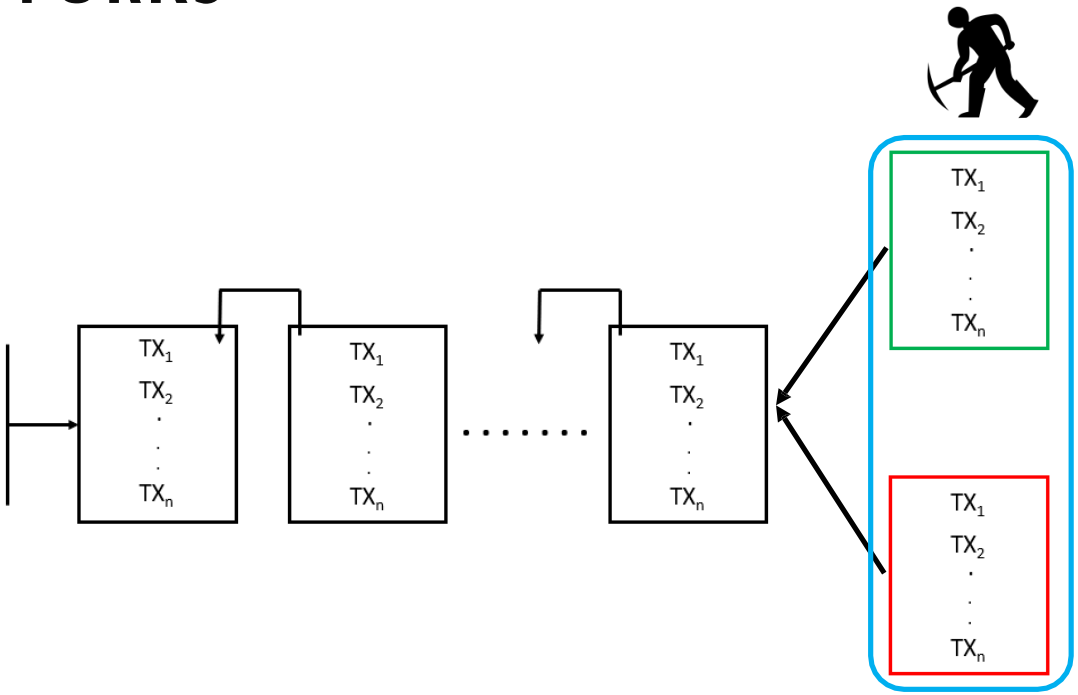
FORKS



Bob tries to double spend the same coin twice in two transactions

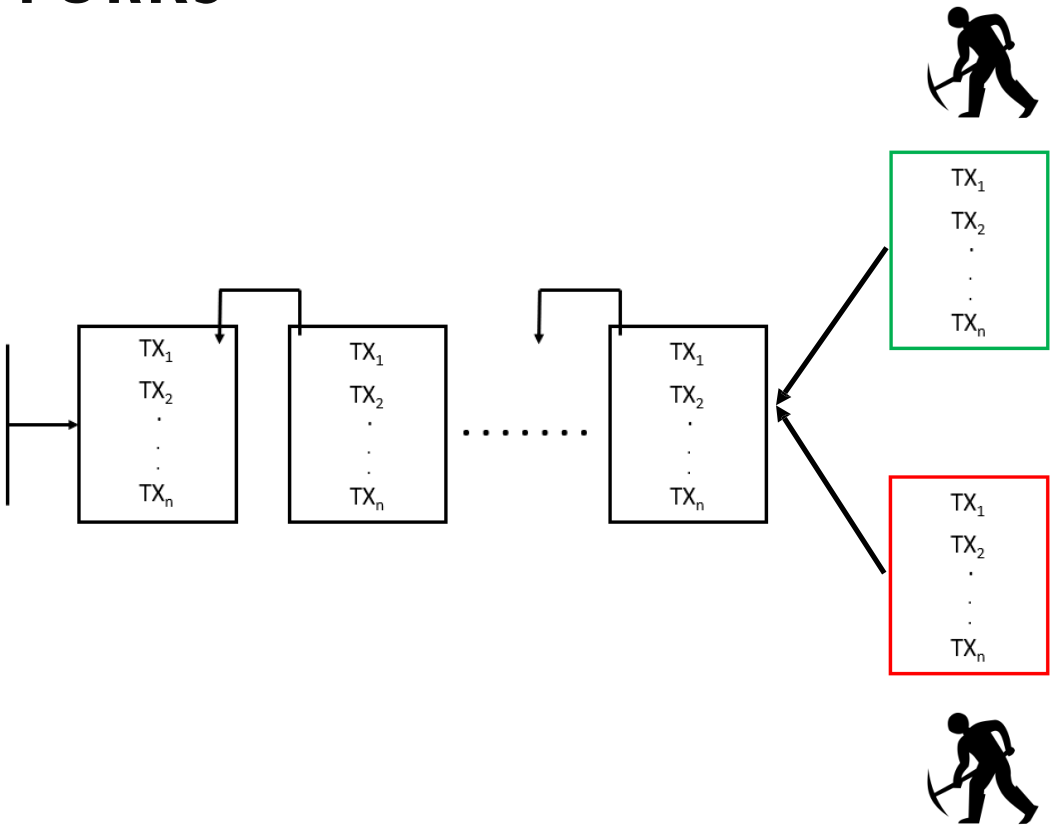
- Transactions in the forked blocks might have conflicts
- Could lead to double spending
- Forks have to be eliminated

FORKS



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

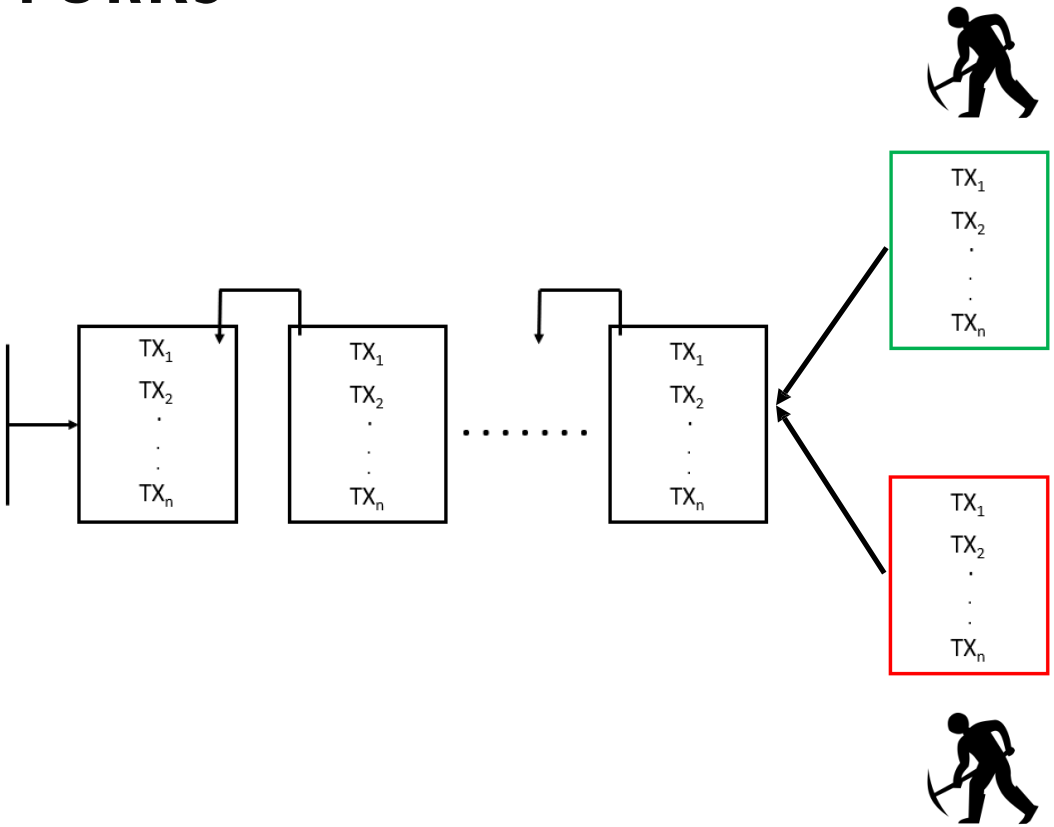
FORKS



DSL

UCSB

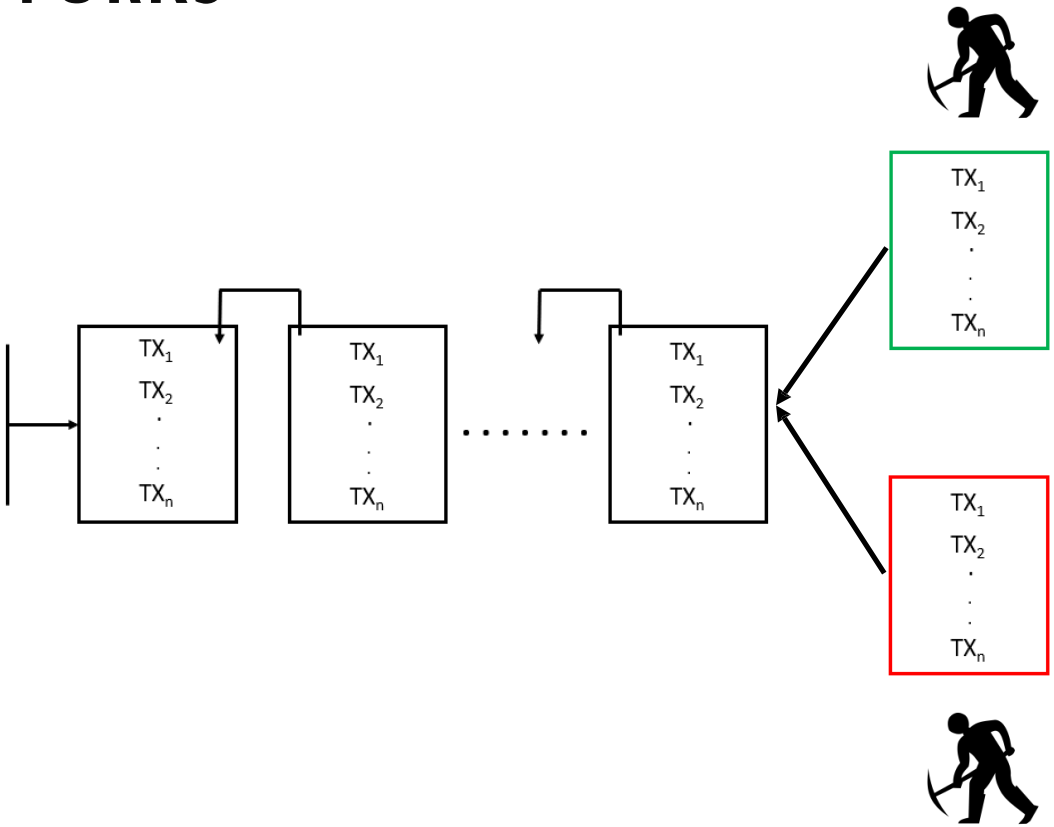
FORKS

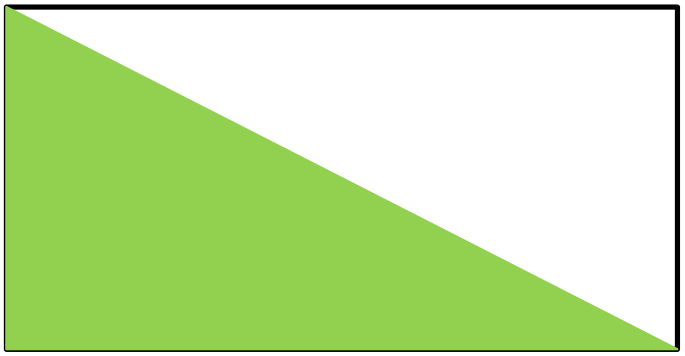


DSL

UCSB

FORKS

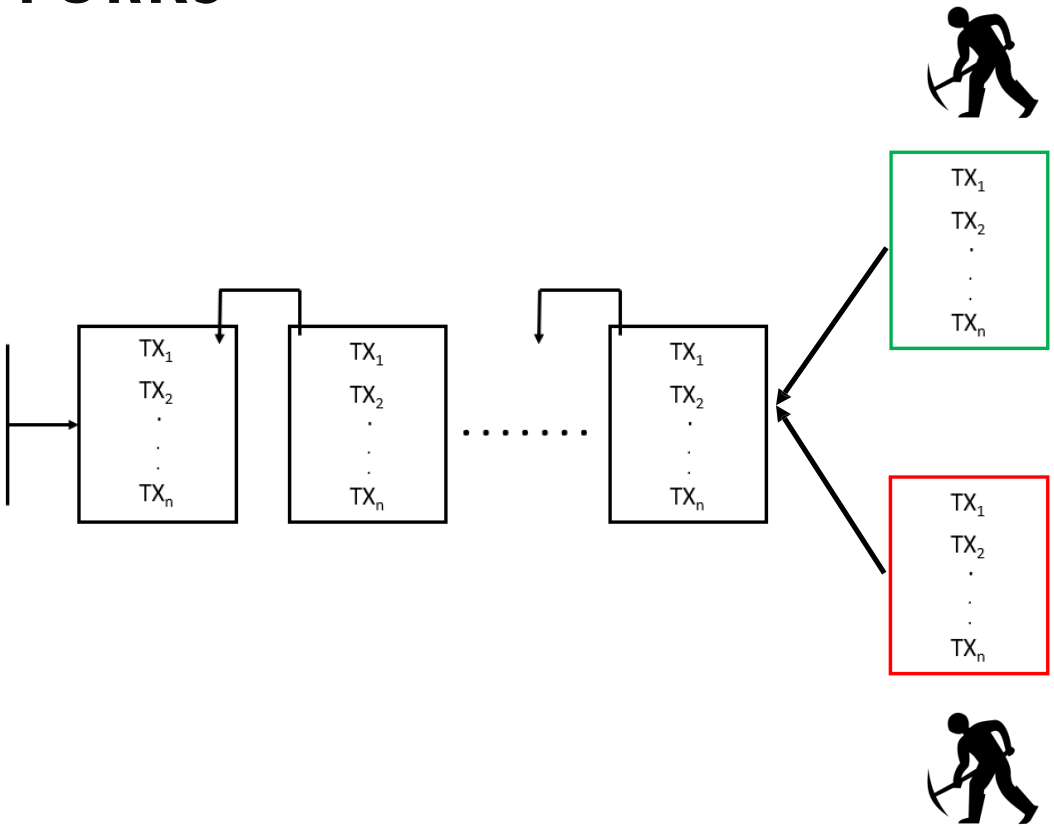


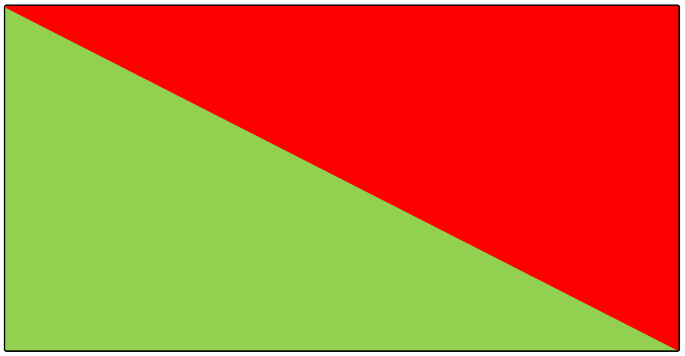


DSL

UCSB

FORKS

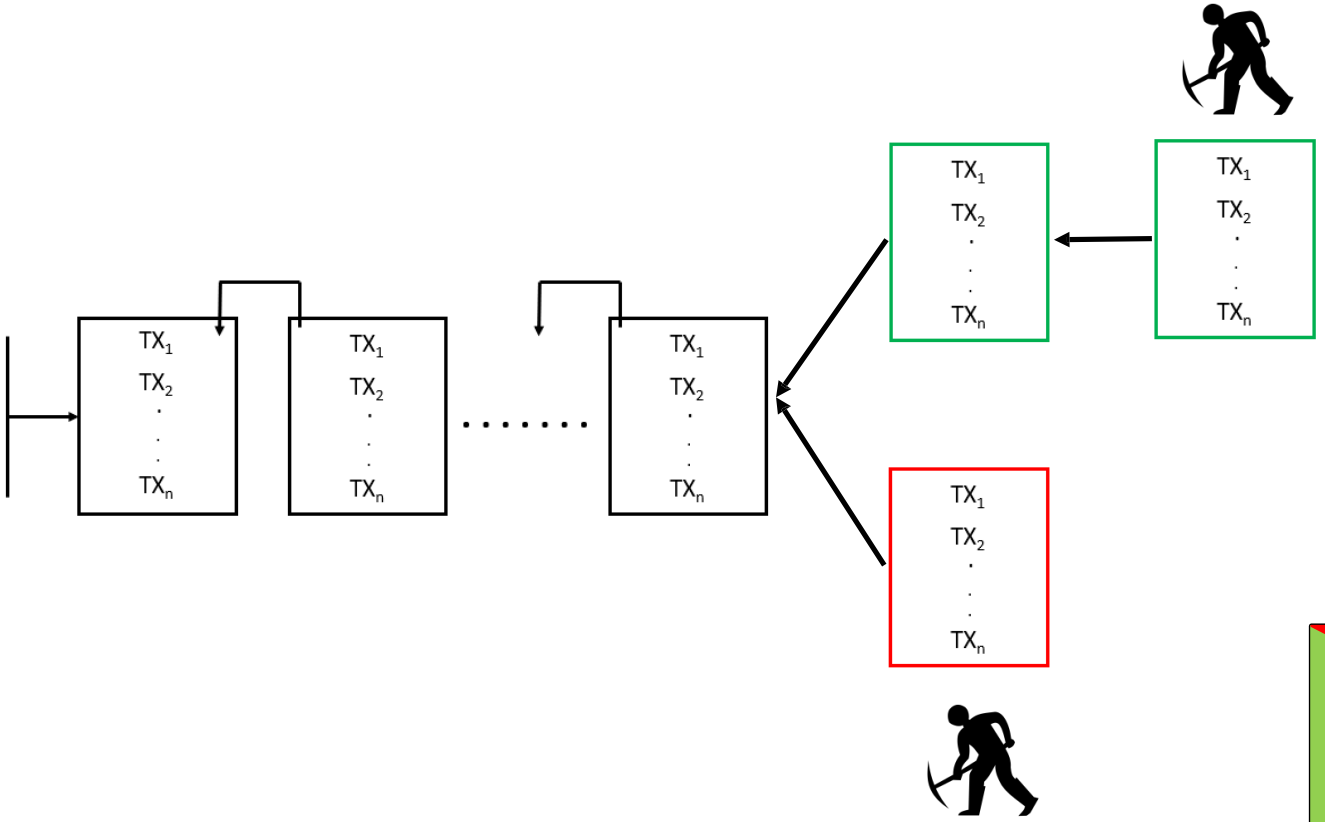


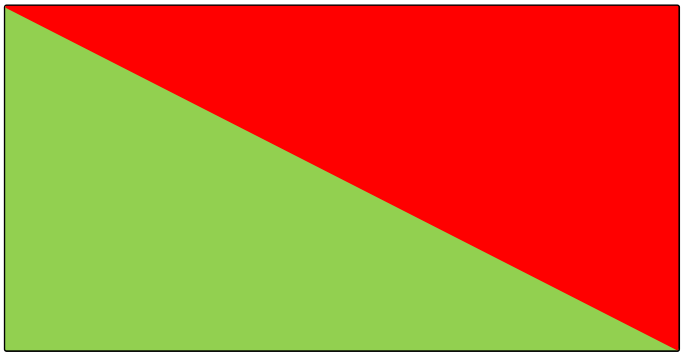


DSL

UCSB

FORKS

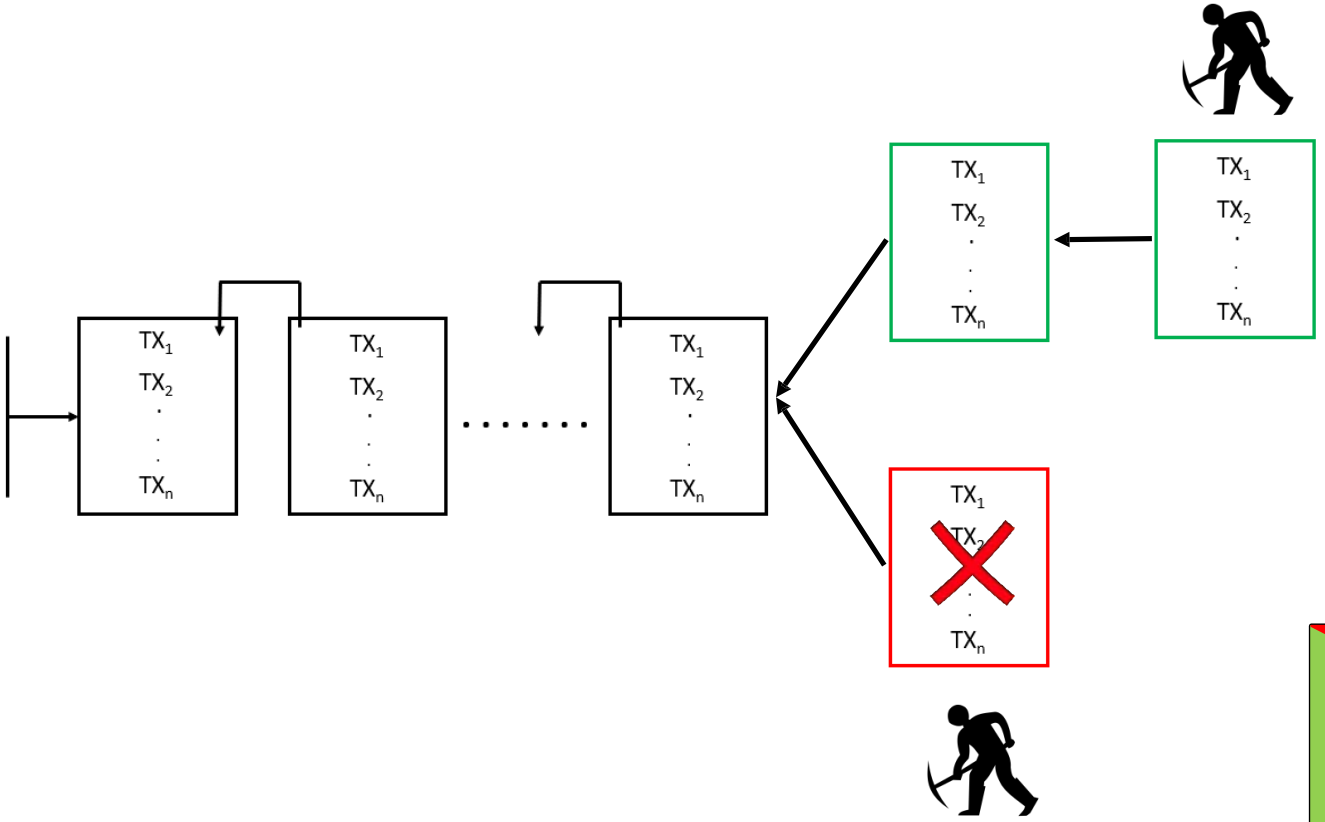


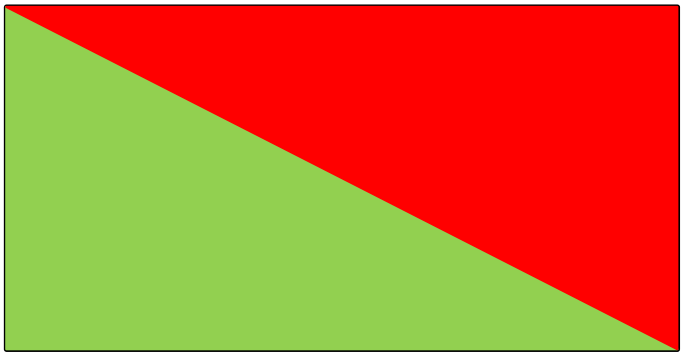


DSL

UCSB

FORKS

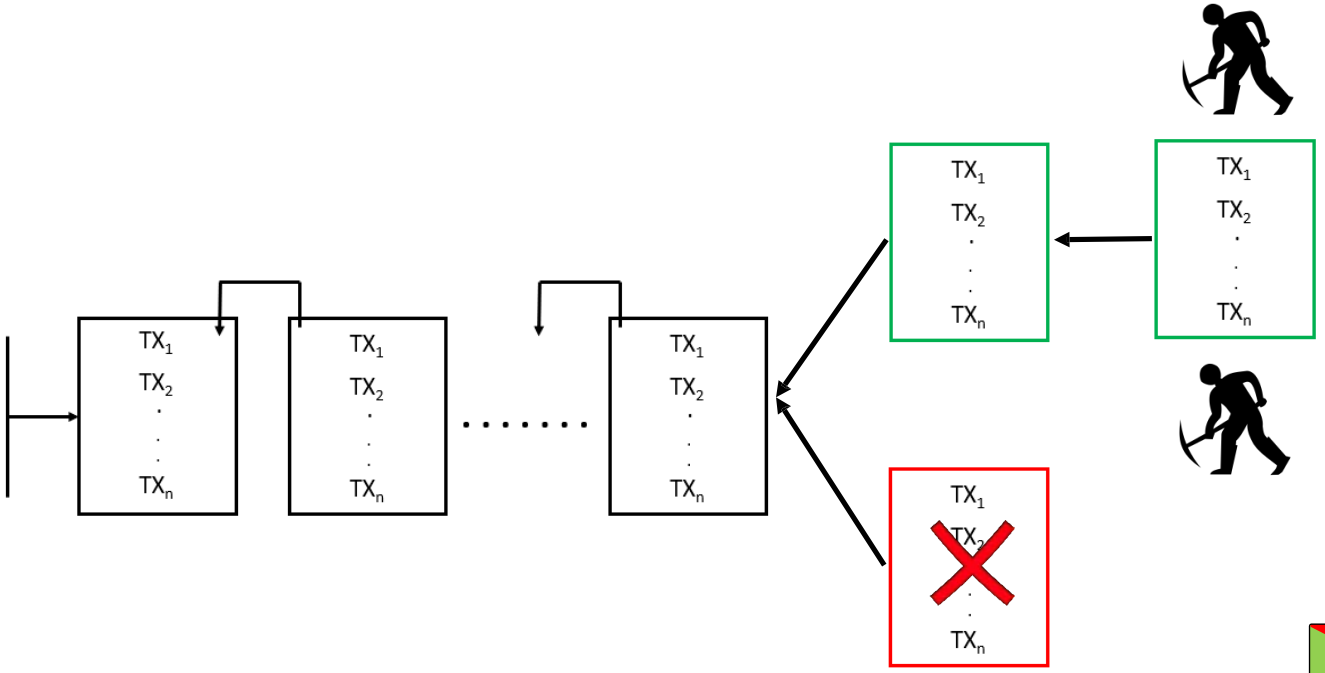




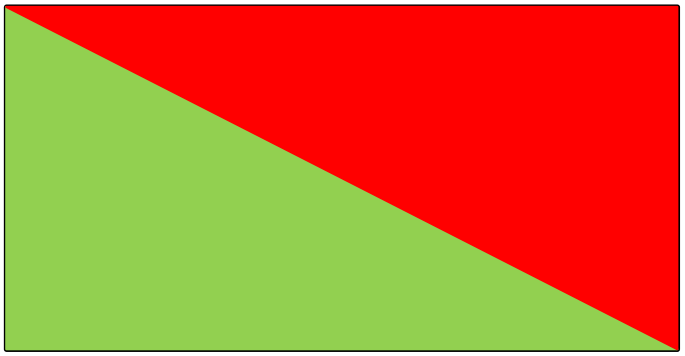
DSL

UCSB

FORKS



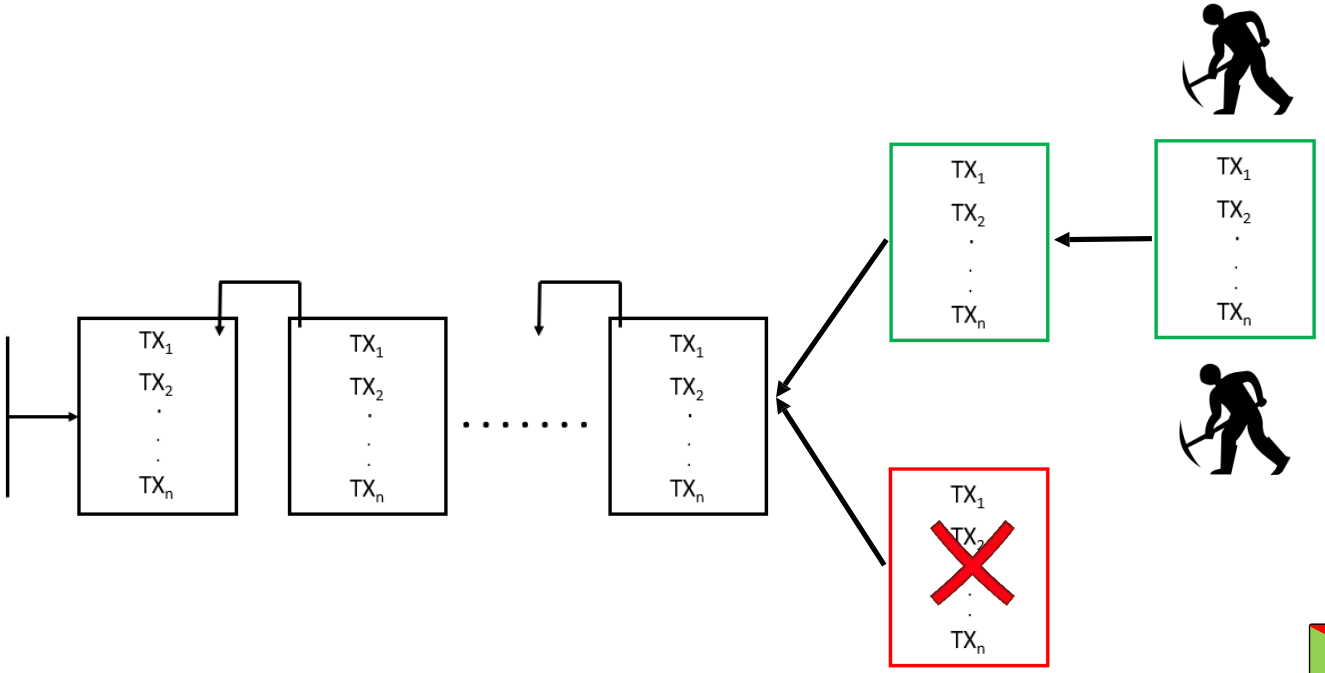
- Miners join the longest chain to resolve forks

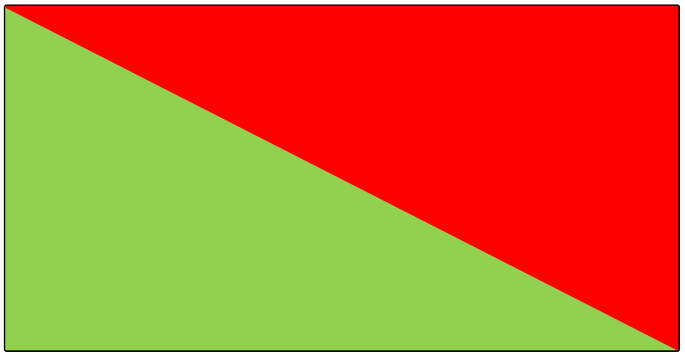


DSL

UCSB

FORKS

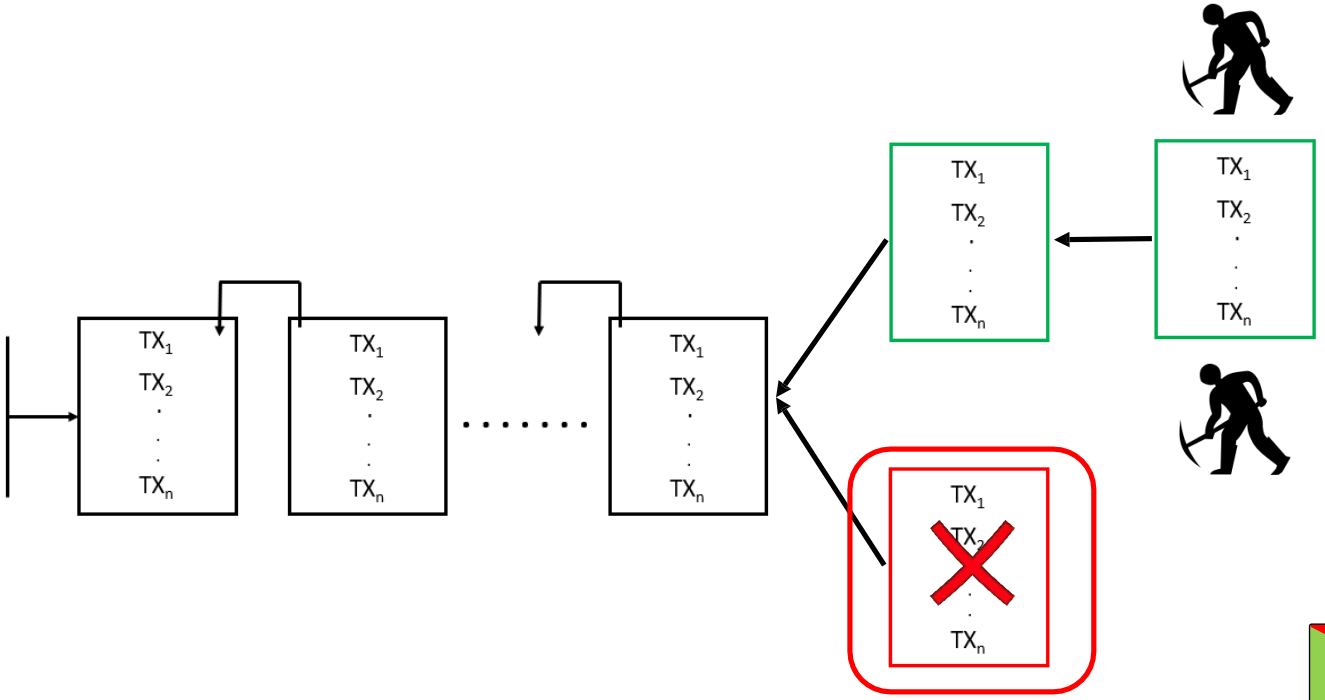




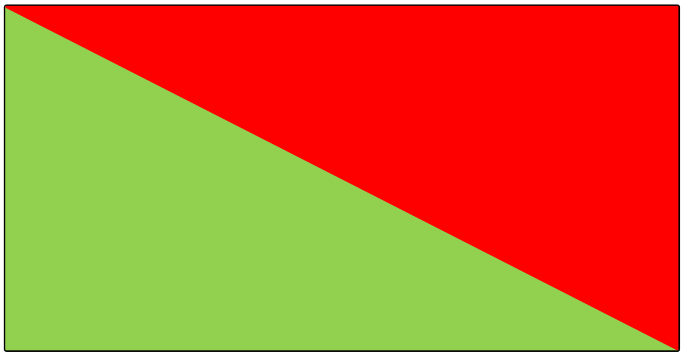
DSL

UCSB

FORKS



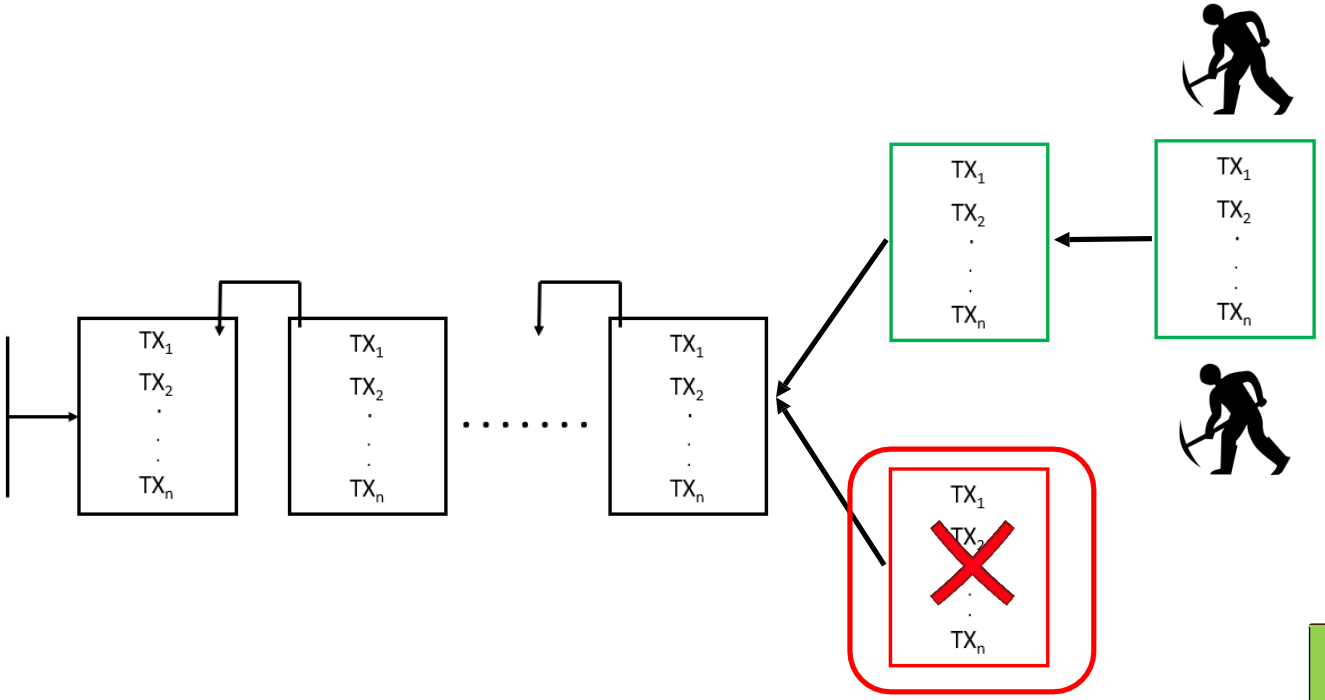
- Transactions in this block have to be resubmitted



DSL

UCSB

FORKS



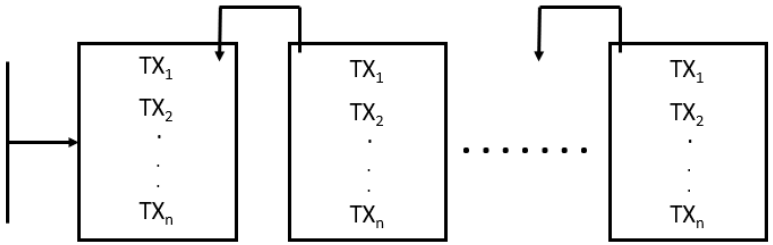
- Transactions in this block have to be resubmitted

51% ATTACK

- If 51% of the computation (hash) power are malicious:
  - They can cooperate to fork the chain at any block
- Can lead to double spending

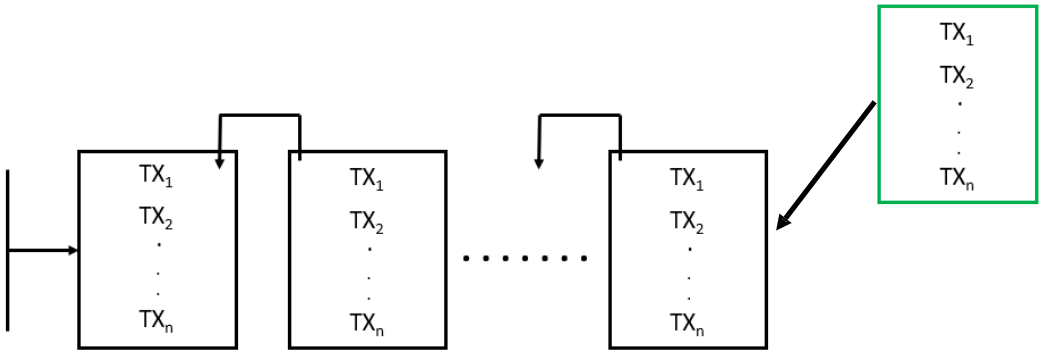
51% ATTACK

- If 51% of the computation (hash) power are malicious:
  - They can cooperate to fork the chain at any block
- Can lead to double spending



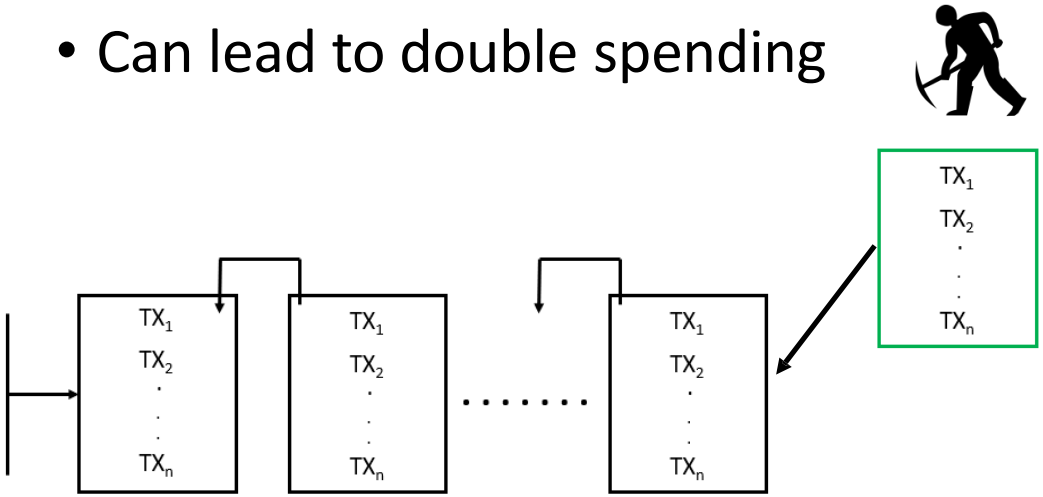
51% ATTACK

- If 51% of the computation (hash) power are malicious:
  - They can cooperate to fork the chain at any block
- Can lead to double spending



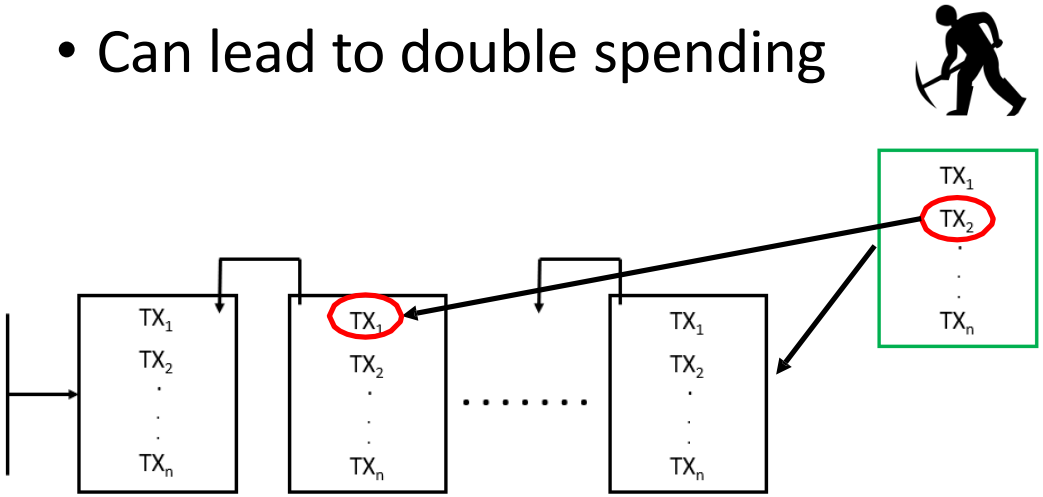
51% ATTACK

- If 51% of the computation (hash) power are malicious:
  - They can cooperate to fork the chain at any block
- Can lead to double spending



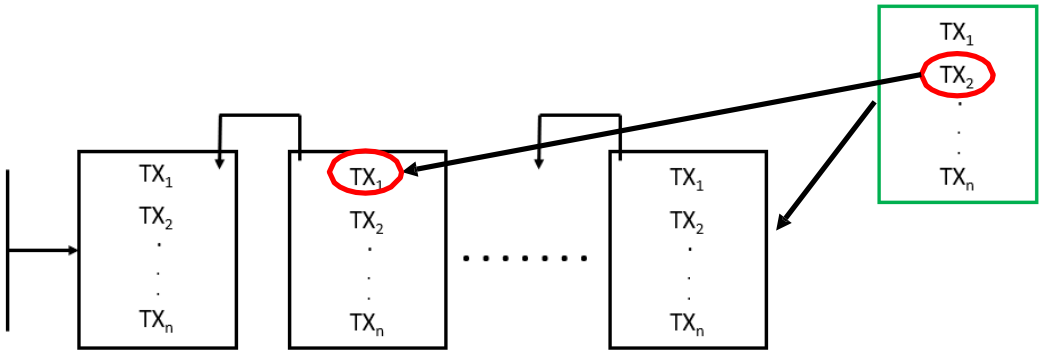
51% ATTACK

- If 51% of the computation (hash) power are malicious:
  - They can cooperate to fork the chain at any block
- Can lead to double spending



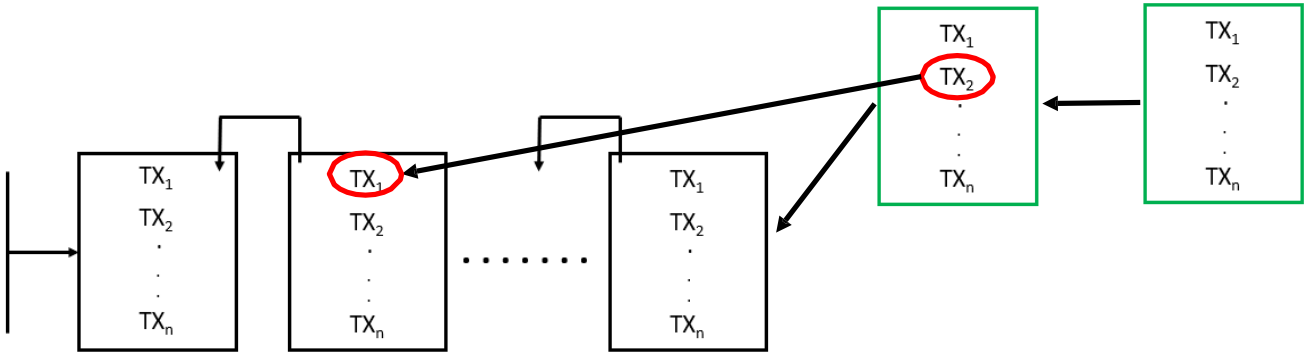
51% ATTACK

- If 51% of the computation (hash) power are malicious:
  - They can cooperate to fork the chain at any block
- Can lead to double spending



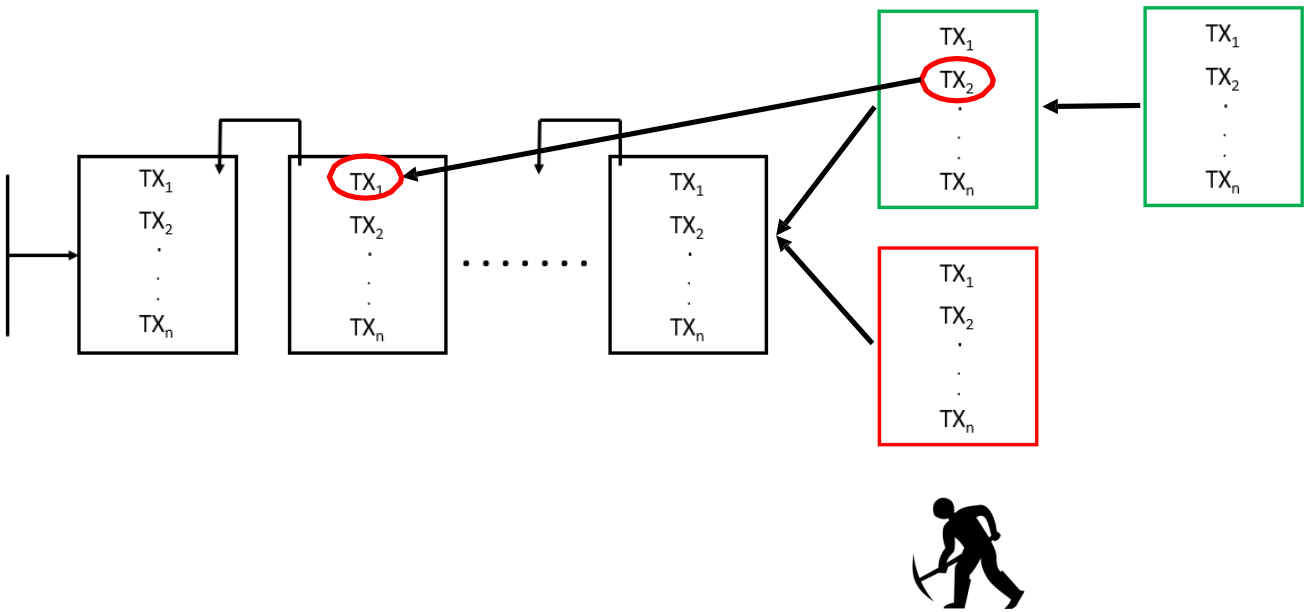
51% ATTACK

- If 51% of the computation (hash) power are malicious:
  - They can cooperate to fork the chain at any block
- Can lead to double spending



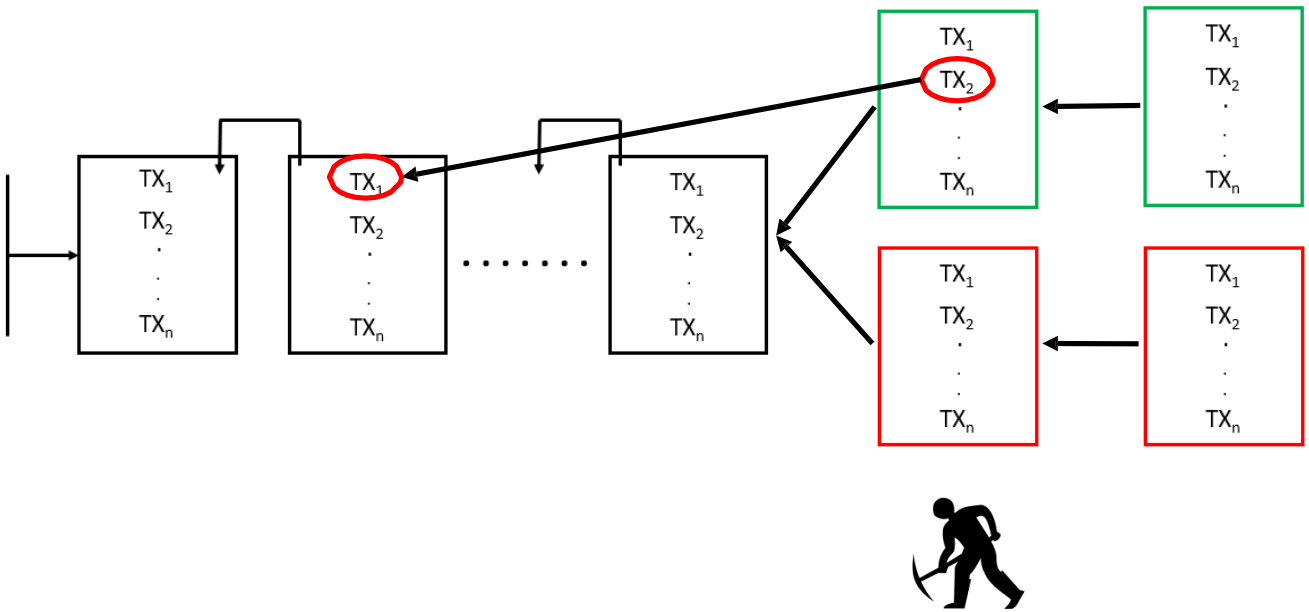
51% ATTACK

- If 51% of the computation (hash) power are malicious:
  - They can cooperate to fork the chain at any block
- Can lead to double spending



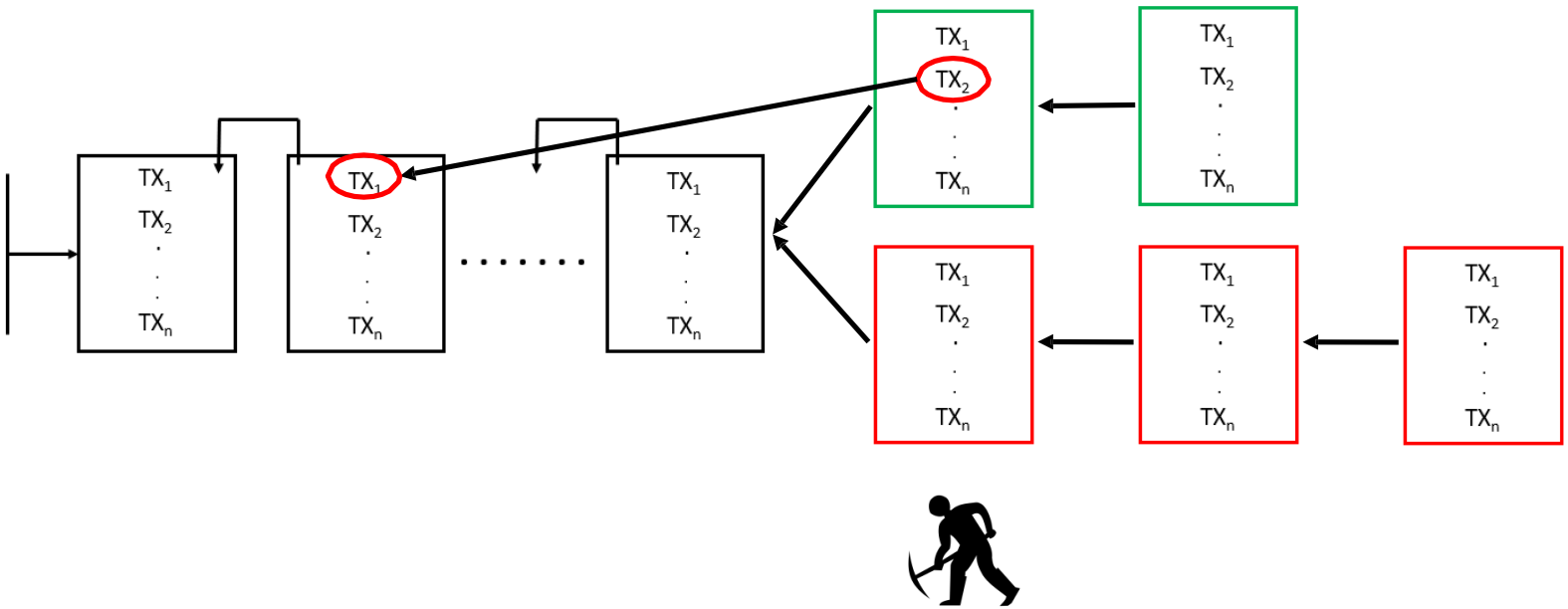
51% ATTACK

- If 51% of the computation (hash) power are malicious:
  - They can cooperate to fork the chain at any block
- Can lead to double spending



51% ATTACK

- If 51% of the computation (hash) power are malicious:
  - They can cooperate to fork the chain at any block
- Can lead to double spending



LIMITATIONS OF BITCOIN

LIMITATIONS OF BITCOIN

- High transaction-confirmation **latency**

LIMITATIONS OF BITCOIN

- High transaction-confirmation **latency**
- **Probabilistic** consistency guarantees

LIMITATIONS OF BITCOIN

- High transaction-confirmation **latency**
- **Probabilistic** consistency guarantees
- Very **low TPS** (Transactions per second) - average of **3 to 7 TPS**

LIMITATIONS OF BITCOIN

- High transaction-confirmation **latency**
- **Probabilistic** consistency guarantees
- Very **low TPS** (Transactions per second) - average of **3 to 7 TPS**
- New block added every **10 minutes**.

HOW TO SCALE BITCOIN?

HOW TO SCALE BITCOIN?

- Two obvious options for increasing Bitcoin's transaction throughput:

HOW TO SCALE BITCOIN?

- Two obvious options for increasing Bitcoin's transaction throughput:

  increase the size of **blocks**, or **decrease** the block **interval**

HOW TO SCALE BITCOIN?

- Two obvious options for increasing Bitcoin's transaction throughput: **increase** the size of **blocks**, or **decrease** the block **interval**

- Why they don't work?

HOW TO SCALE BITCOIN?

- Two obvious options for increasing Bitcoin's transaction throughput: **increase** the size of **blocks**, or **decrease** the block **interval**

- Why they don't work?
  - **Decreases fairness** - giving large miners an advantage

HOW TO SCALE BITCOIN?

- Two obvious options for increasing Bitcoin's transaction throughput: **increase** the size of **blocks**, or **decrease** the block **interval**

- Why they don't work?
  - **Decreases fairness** - giving large miners an advantage
  - Requires more storage space and verification time

HOW TO SCALE BITCOIN?

- Two obvious options for increasing Bitcoin's transaction throughput: **increase** the size of **blocks**, or **decrease** the block **interval**

- Why they don't work?
  - **Decreases fairness** - giving large miners an advantage
  - Requires more storage space and verification time
  - Leads to higher number of **forks**

OPEN PROBLEMS AND CRITICISM

DSL

UCSB

OPEN PROBLEMS AND CRITICISM

Bitcoin mining consumes more electricity a year than Ireland

The Guardian International edition

Network's estimated power use also exceeds that of 19 other European countries, consuming more than five times output of continent's largest windfarm

DSL

UCSB

OPEN PROBLEMS AND CRITICISM

Bitcoin mining consumes more electricity a year than Ireland

The Guardian

Network's estimated power use also exceeds that of 19 other Europe
contine

New study quantifies bitcoin's ludicrous energy consumption

Bitcoin could consume 7.7 gigawatts by the end of 2018.

TIMOTHY B. LEE - 5/17/2018, 10:23 AM

ars TECHNICA

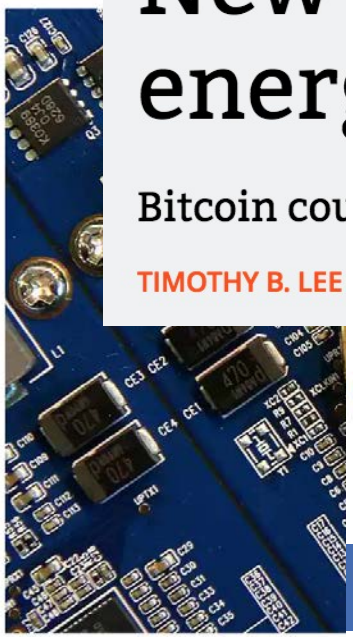
DSL

UCSB

OPEN PROBLEMS AND CRITICISM

Bitcoi
electri

Network's e
Europe
contine



Bitcoin Mining Now Consuming More Electricity Than 159 Countries Including Ireland & Most Countries In Africa

New
ener

Bitcoin cou

TIMOTHY B. LEE

'ous

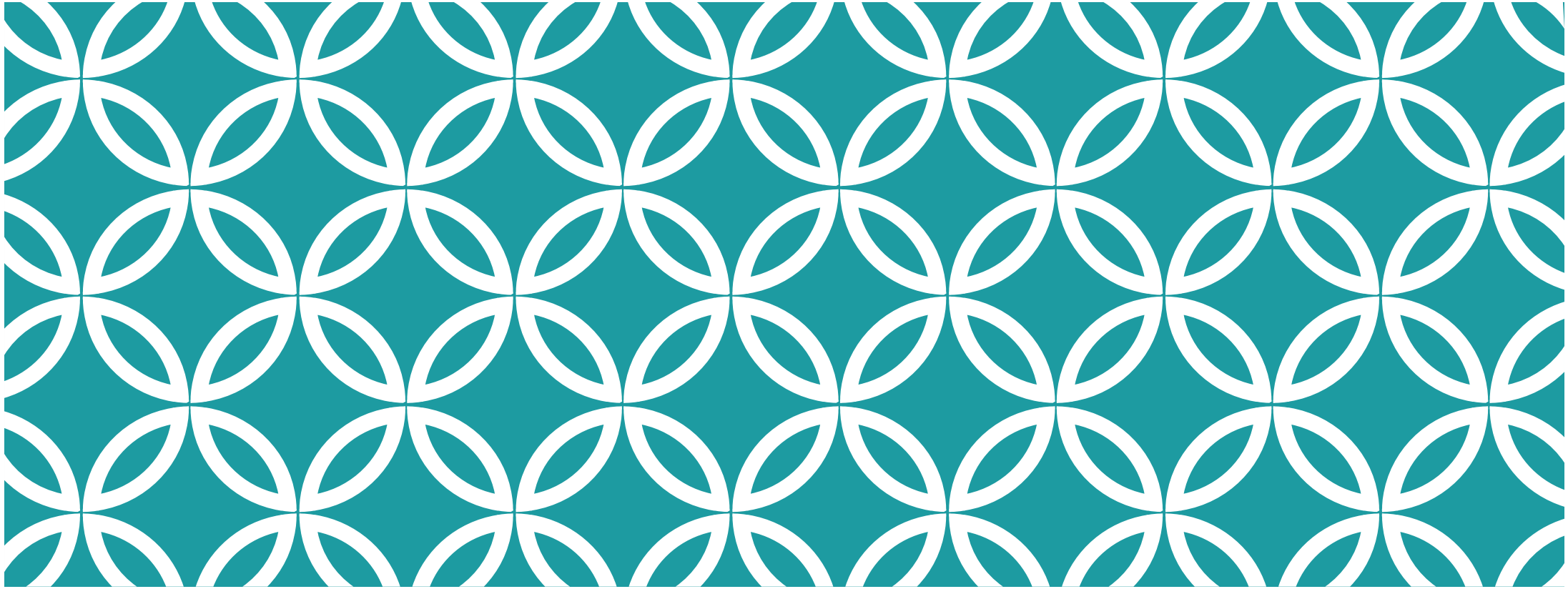
TECHNICA

DSL

UCSB

CONTACT US

- Sujaya Maiyaa: sujaya_maiyya@ucsb.edu
- Victor Zakhary: victorzakhary@ucsb.edu
- Divyakant Agrawal: divyagrawal@ucsb.edu
- Amr El Abbadi: elabbadi@ucsb.edu



A SKEPTICAL LOOK AT PERMISSIONLESS BLOCKCHAINS

THE SEDUCTIVE ELEGANCE OF BITCOIN

Secure

Fair

Private

Verifiable

Incentive to work

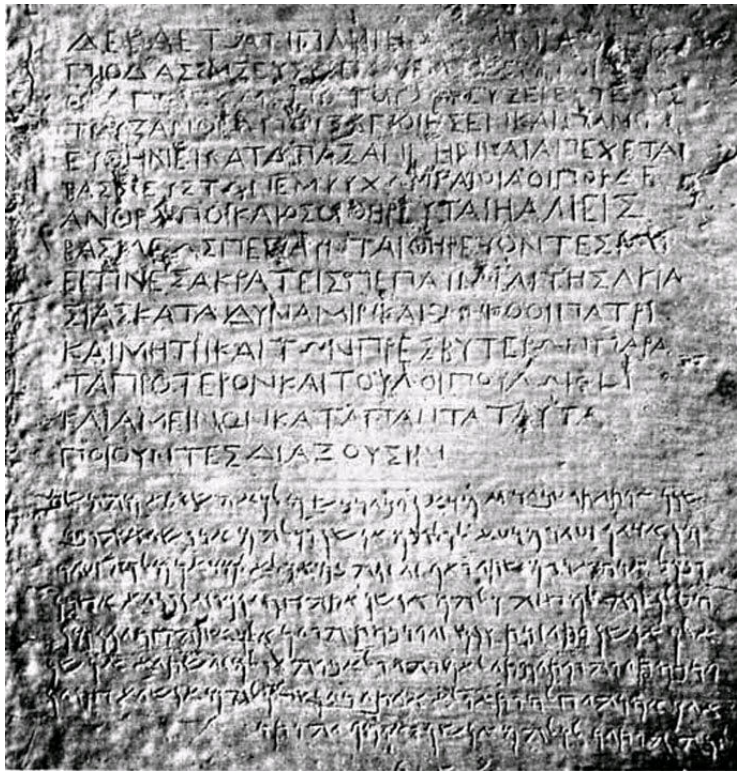
Decentralized

SECURE

Once stable, transaction order is immutable

No double-spending

No unauthorized spending



FAIR

Anyone can participate

Non-repudiability reduces transaction fees,

broadening access

- Nakamoto's insight

PRIVATE

Users identified only by public key strings

- 1EnJHhq8Jq8vDuZA5ahVh6H4t6jh1mB4rq

VERIFIABLE

Easy to verify transaction validity

- No tampering possible because of the blockchain data structure

INCENTIVE TO WORK

'Miners' are paid for their effort

- maintains system health

DECENTRALIZED

Egalitarian

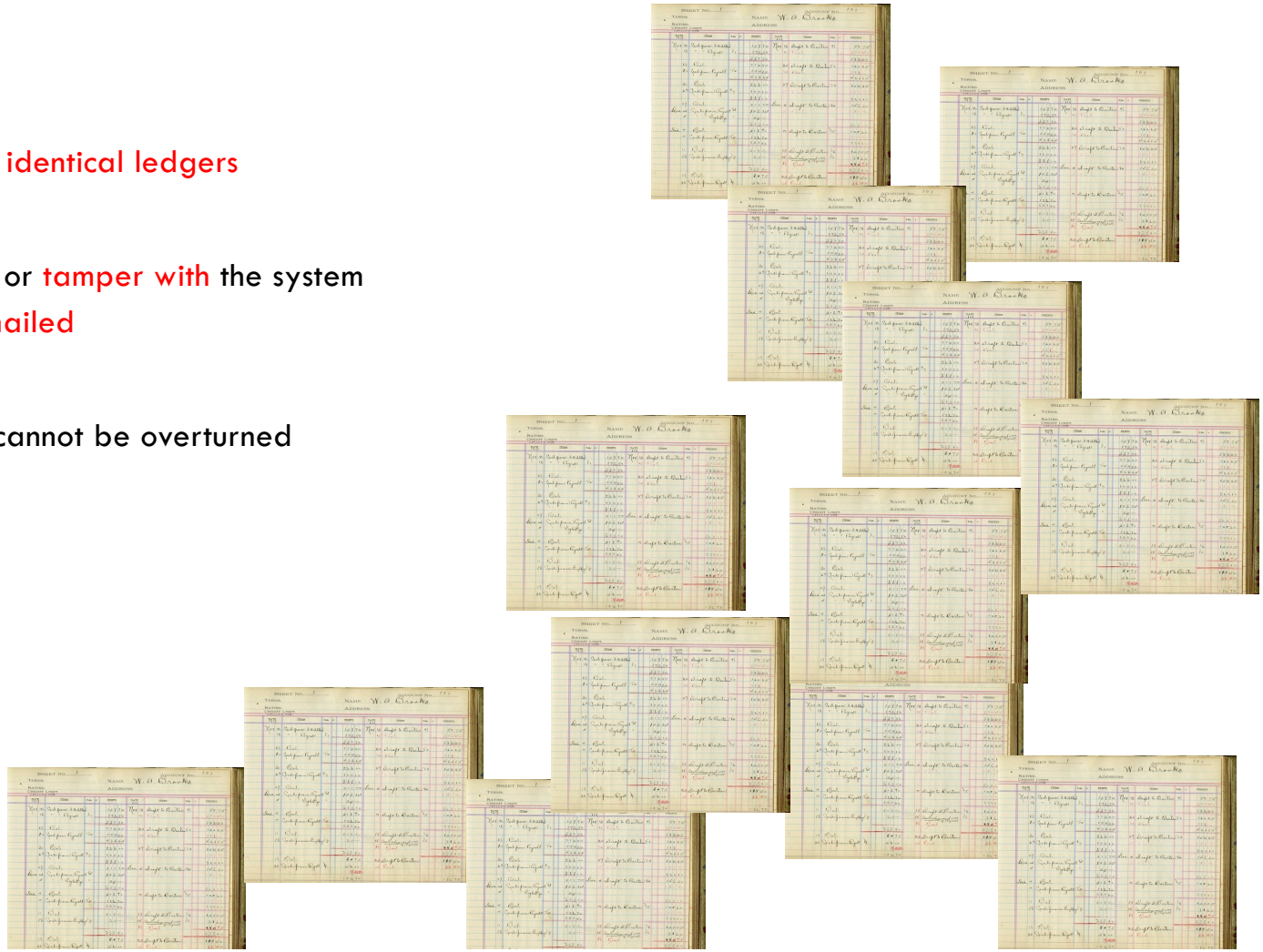
- all peers are equal and all have the identical ledgers

A different kind of security

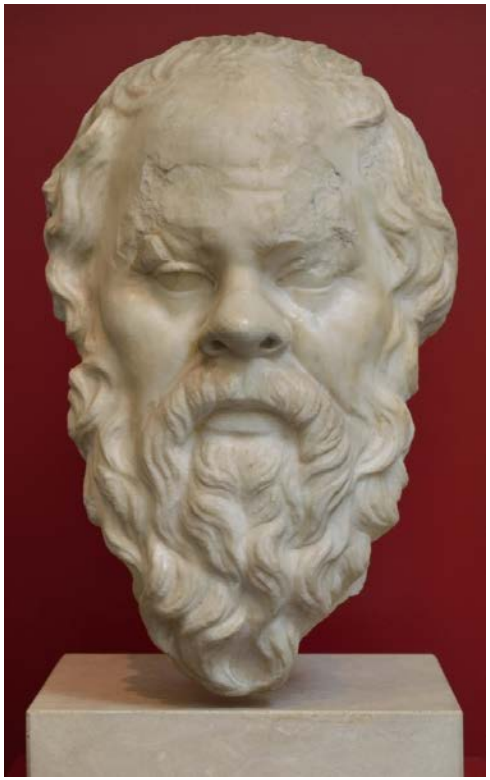
- No central authority who can restrict or tamper with the system
- Peers cannot be pressured or blackmailed

Distributed consensus

- decisions based on `Proof of Work' cannot be overturned



A SKEPTICAL LOOK



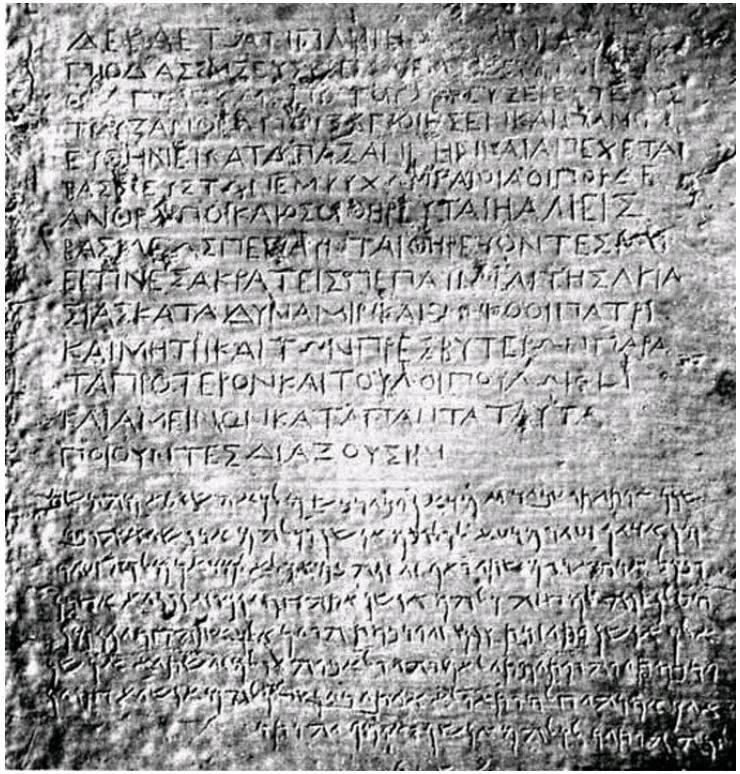
SECURE

Recall this means

- Once stable, transaction order is immutable
- No double-spending
- No unauthorized spending

Assumes

- Honest miners own more than 50% of compute power
- Cryptographic protocols are unbreakable



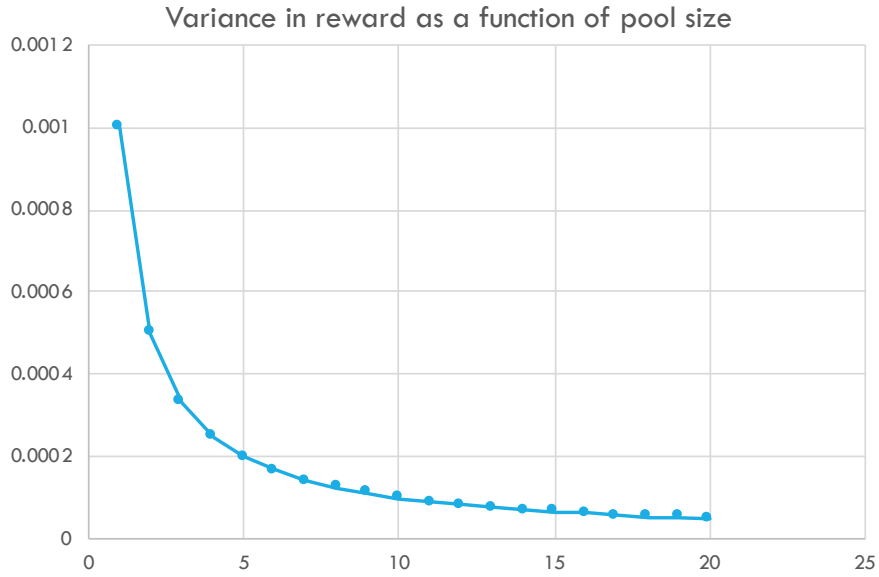
MINING POOLS

Miners are incentivized to join pools to reduce variance in earnings

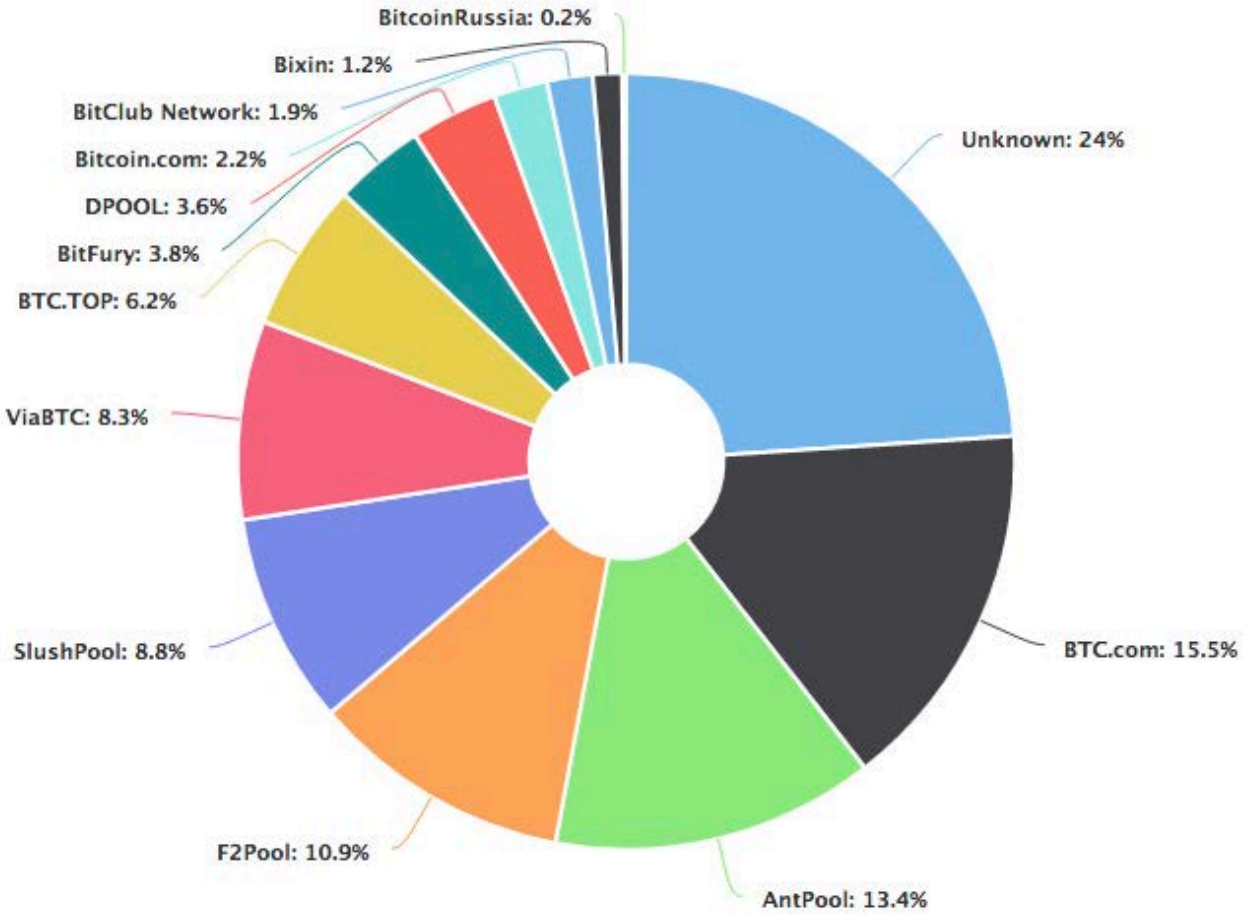
- Block reward B every 10 minutes
- Probability of winning a block reward p per miner
- Individual miner
  - E(reward) = pB, V(reward) = $p(1\text{-}p)B$
- Pool of size K
  - E(reward) = pB, V(reward) = $p(1/K–p)B$

Mining is a natural monopoly [1]

=> natural tendency to centralize



[1] Dowd, Kevin, and Martin Hutchinson. "Bitcoin will bite the dust." *Cato J.* 35 (2015): 357.



Source: Blockchain.com March 29, 2019

CRYPTO IS POTENTIALLY VULNERABLE

" I estimate a 1in 7 chance of breaking RSA-2048 by 2026 and a 1in 2 chance by 2031."

- Prof. Michele Mosca, Institute for Quantum Computing, University of Waterloo [1]

Information stored with insecure crypto can be retrospectively attacked

'Post-quantum' cryptography is under development

- will miners adopt it?
- decentralization hurts!

[1] Mosca, Michele. "Cybersecurity in an era with quantum computers: will we be ready?." *IEEE Security & Privacy* 16.5 (2018): 38-41.

FAIR

Anyone can participate

- but only if they buy specialized hardware

Non-repudiability reduces transaction fees, broadening access

- transaction fees today are about USD 0.25 – 0.50
- fees are voluntary, but transactions with higher fees are more likely to succeed

PRIVATE

Users identified only by public key strings

but can still be identified using network analysis

- Other blockchains are (supposed to be) more secure

Deanonymisation of Clients in Bitcoin P2P Network

Alex Biryukov Dmitry Khovratovich Ivan Pustogarov
University of Luxembourg
{alex.biryukov, dmitry.khovratovich, ivan.pustogarov}@uni.lu

cost of the deanonymisation attack on the full Bitcoin network is under 1500 EUR.

Biryukov, Alex, Dmitry Khovratovich, and Ivan Pustogarov. "Deanonymisation of clients in Bitcoin P2P network." *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014.

INCENTIVE TO WORK

'Miners' are paid for their effort

- maintains system health
- but only if Bitcoin prices are stable

Incentive to invest in mining when prices are volatile?

Reduced decentralization if miners evaporate?

DECENTRALIZED

Distributed consensus

- decisions based on `Proof of Work' cannot be easily overturned
- but only after an hour
- limited to about 10 transactions/s
- comes at a huge energy cost

TO SUM UP

Bitcoin does not provide security, fairness, privacy, incentive compatibility

It is verifiable

Decentralization comes at the cost of energy and time

AN ALTERNATIVE

Can we do better if we don't trust individual nodes but do trust a consortium?

- Legislator vs. Legislature

AN ALTERNATIVE

Can we do better if we don't trust individual nodes but do trust a consortium?

- Legislator vs. Legislature

Idea: let a consortium reach consensus on next block, rather than miners competing with proof of work

AN ALTERNATIVE

Can we do better if we don't trust individual nodes but do trust a consortium?

- Legislator vs. Legislature

Idea: let a consortium reach consensus on next block, rather than miners competing with proof of work

This is a permissioned system: e.g. Hyperledger Fabric

PERMISSIONED BLOCKCHAIN

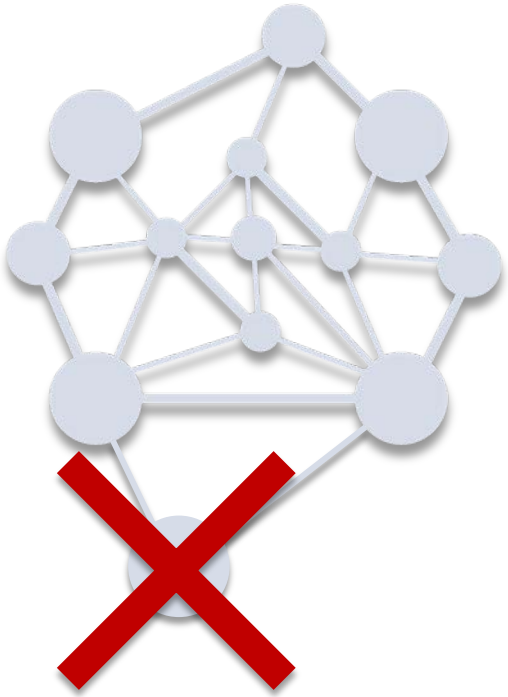
All nodes are known

No new nodes without consensus

Trust through identity

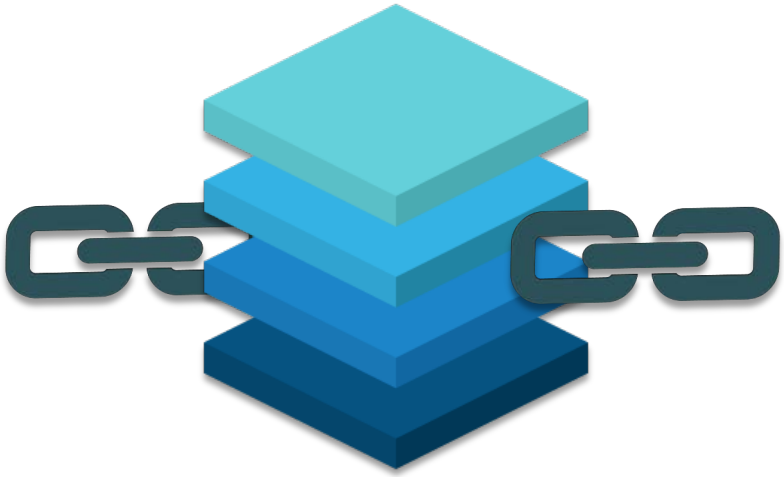
- Membership service issues X.509 certificates

"Proof of Authority"



FABRIC BLOCK CREATION

- Execution
- Consensus
- Dissemination
- Validation



FABRIC ARCHITECTURE

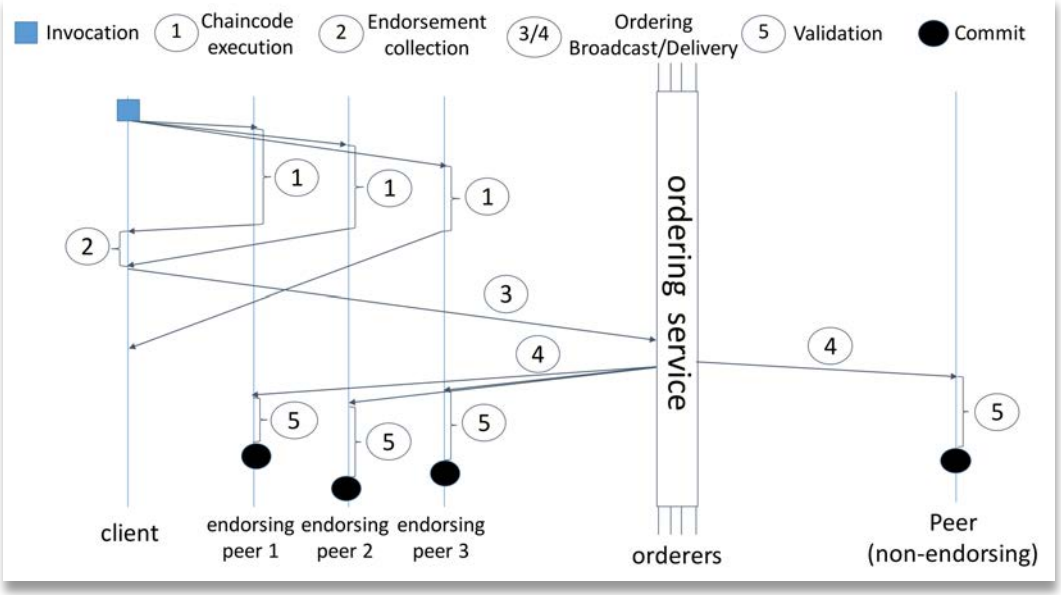
Clients

Peers

- Endorsers
- Committers

Ordering service

Membership service



FABRIC ARCHITECTURE

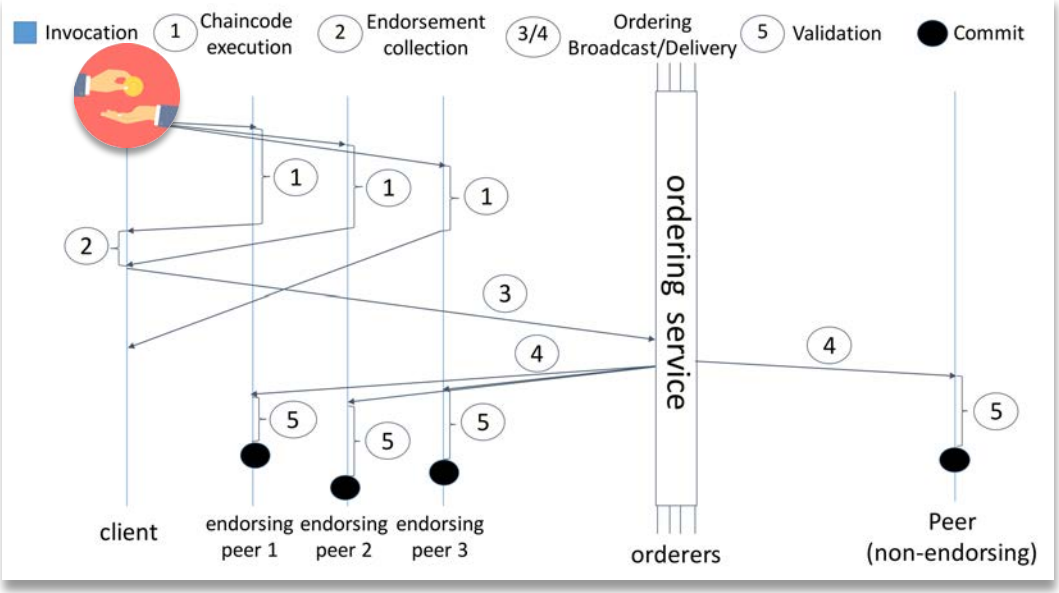
Clients

Peers

- Endorsers
- Committers

Ordering service

Membership service



FABRIC ARCHITECTURE

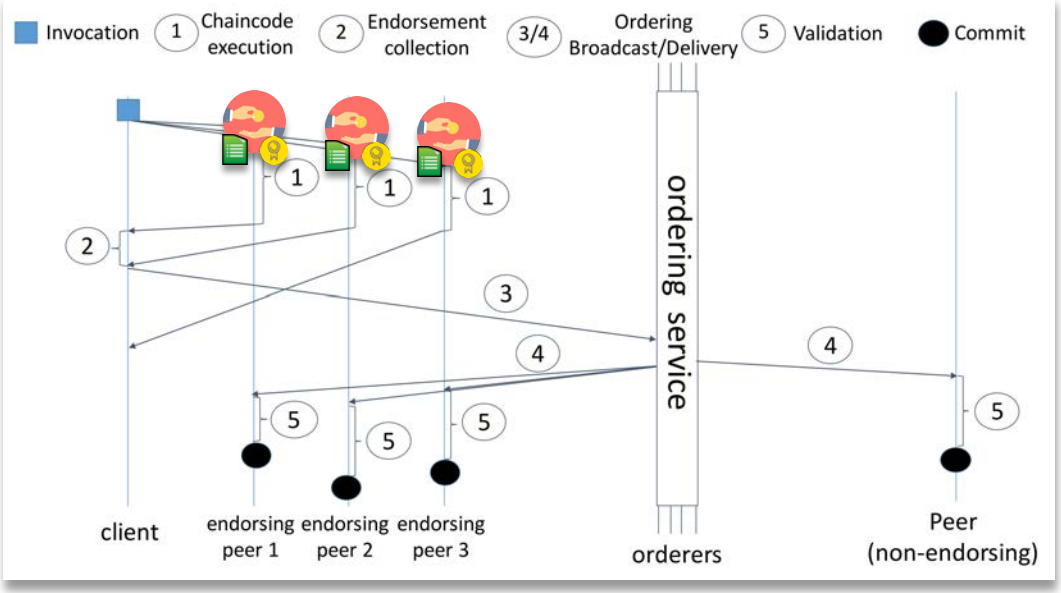
Clients

Peers

- Endorsers
- Committers

Ordering service

Membership service



FABRIC ARCHITECTURE

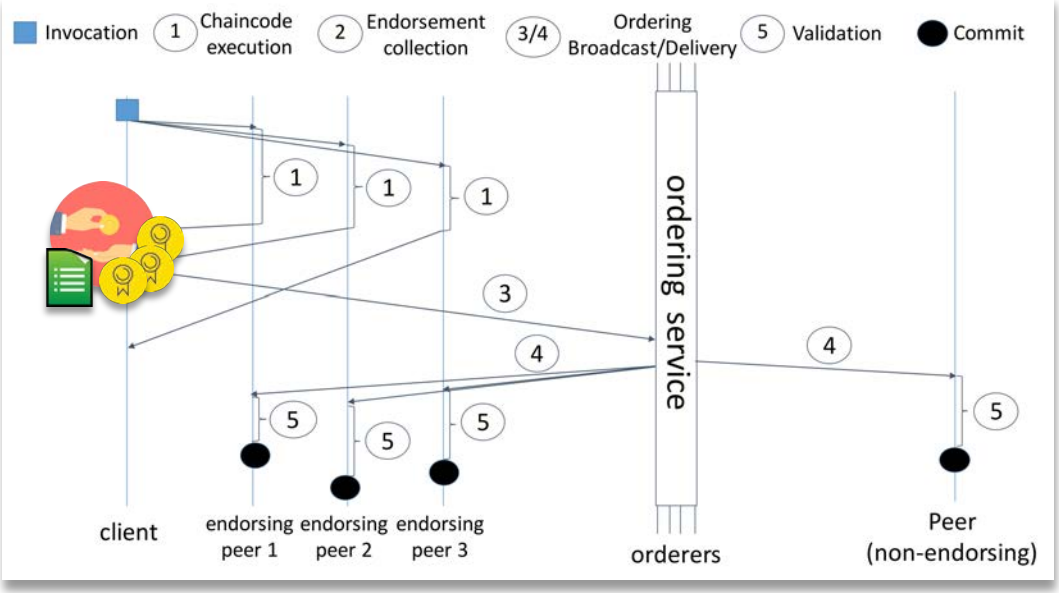
Clients

Peers

- Endorsers
- Committers

Ordering service

Membership service



FABRIC ARCHITECTURE

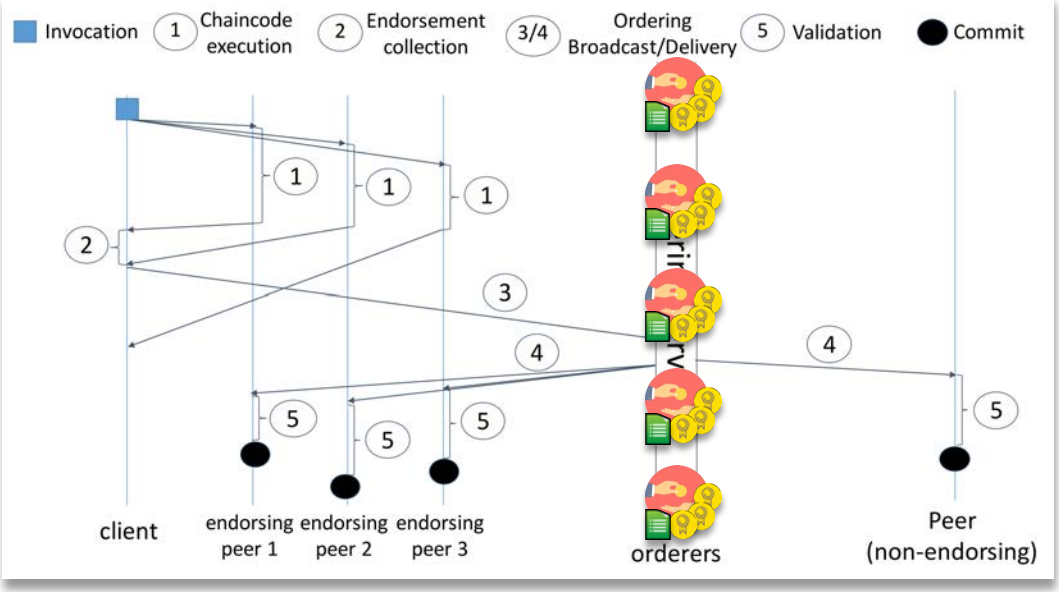
Clients

Peers

- Endorsers
- Committers

Ordering service

Membership service



FABRIC ARCHITECTURE

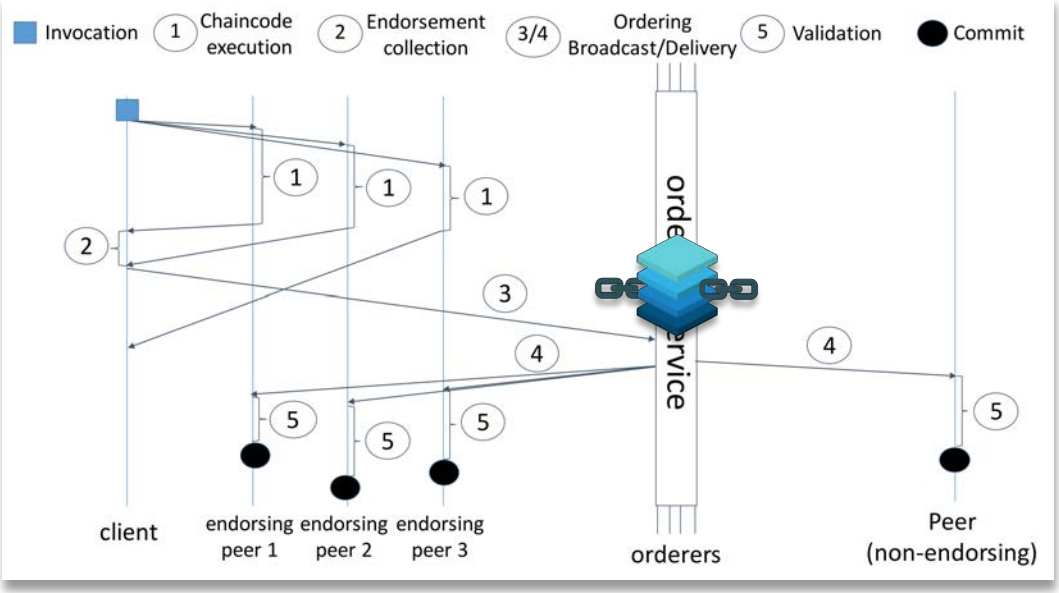
Clients

Peers

- Endorsers
- Committers

Ordering service

Membership service



FABRIC ARCHITECTURE

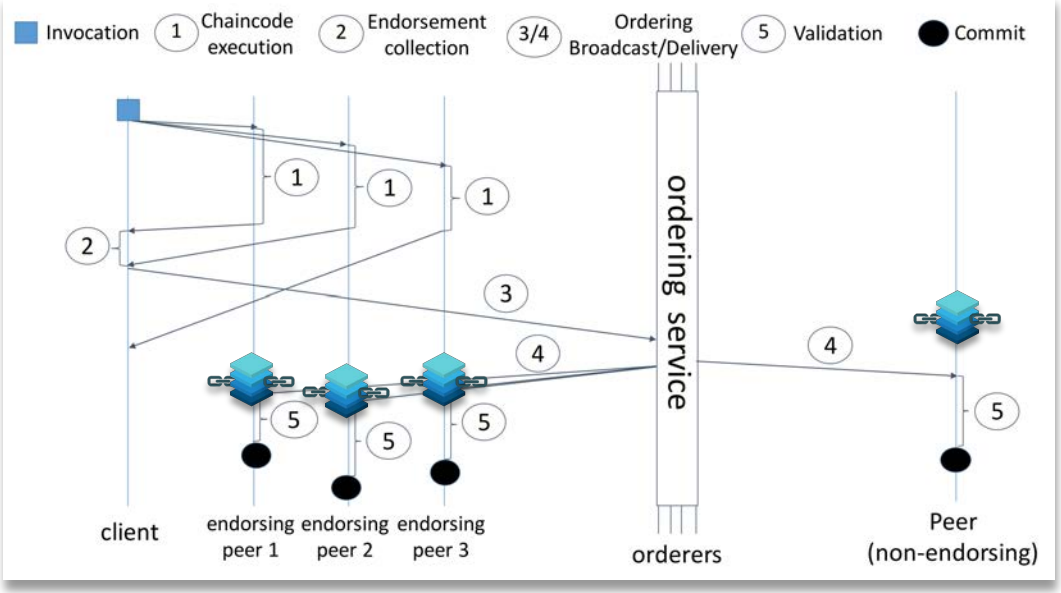
Clients

Peers

- Endorsers
- Committers

Ordering service

Membership service



HOW DOES IT MATCH UP?

As secure as Bitcoin

- Once stable, transaction order is immutable
- No double-spending
- No unauthorized spending

As verifiable as Bitcoin

Fair access

- but not fair in terms of participation

Some support for private data

- no support for node anonymity
- users could be pseudonymous

Does not need to given incentive to work, so no need for cryptocurrencies

Somewhat decentralized

But has high performance, low energy cost, and is legacy compatible

IS IT EVEN A BLOCKCHAIN?

Yes!

Uses blockchain structure for immutable ledger

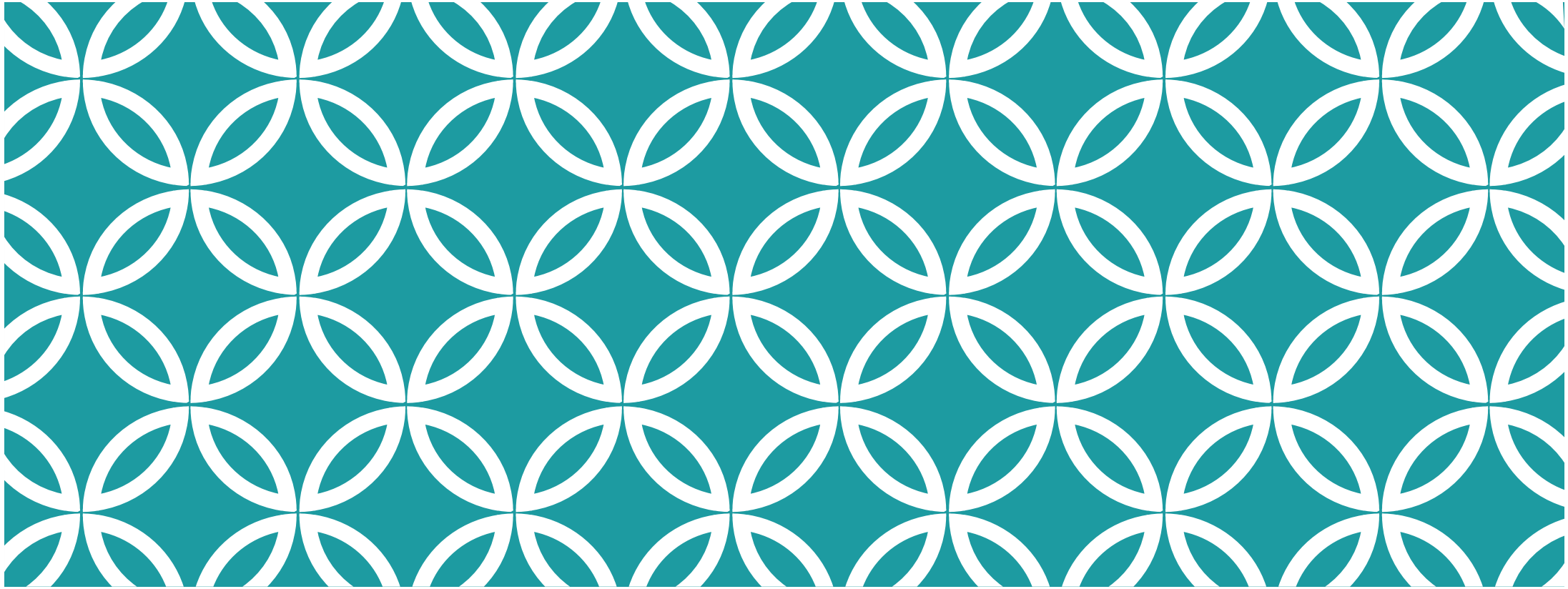
All nodes are mutually suspicious

internal firewall

ENERGY APPLICATIONS OF BLOCKCHAINS

OUTLINE

1. Context
2. Methodology
   - An example
3. Applications
4. Conclusion



CONTEXT

CONTEXT

Three pillars of future energy systems*

- Decarbonization
  - Integrate solar and wind at both utility scale and from prosumers
  - Non-carbon fuels, such as hydrogen ('green molecules')
- Decentralization
  - Breakup monopolies to allow entry of new players
    - E.g. empower prosumers
- Digitalization
  - Better sensing, communication, control: IoT
  - Transparency in existing markets

* World Energy Council

CONTEXT

Players in energy systems

- Generators/Fuel producers
- Transmission system operators/Pipeline and shipping operators
- Distribution system operators
- Regulators
- EV charging station operators
- Prosumers

They may not mutually trust each other. What to do?

FUTURE ENERGY SYSTEMS

Energy systems are becoming more decentralized

- Anyone with a solar panel is an energy producer!
- Argues for a loose coalition instead of a monopoly
- Requires trust in non-traditional actors

Can be mitigated by blockchains

- Audit trail
- Provenance
- Transactions

CONTEXT

What to do?

- Trusted intermediaries (e.g. escrow agents)
  - Raises the cost of a transaction
- Use blockchain
  - Assuming trustworthy metering
  - Provides transparency, accountability, efficiency, and disintermediation

METHODOLOGY

METHODOLOGY

Identify players

What are their trust relationships?

For each relationship:

- Is there reason to doubt this level of trust?
  - If so, use a blockchain to mitigate issues
  - Minimize disruption to existing processes

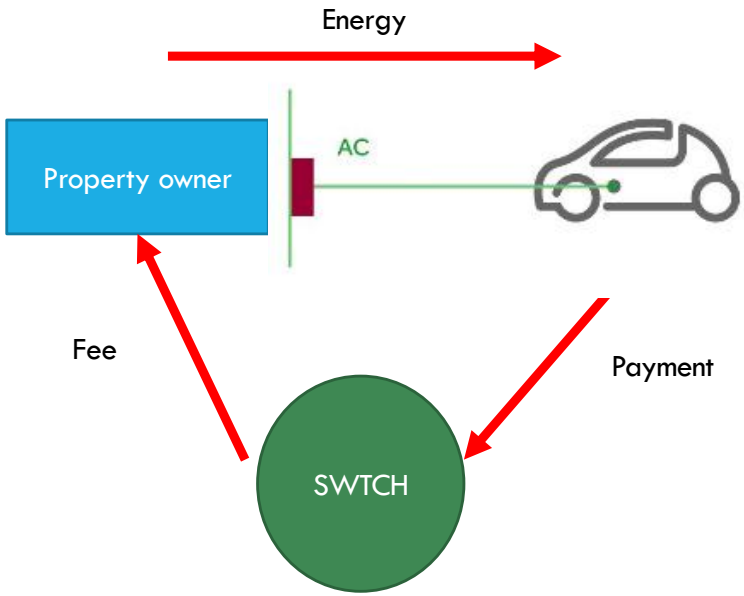
C. Gorenflo, L. Golab, and S. Keshav, Using a Blockchain to Mitigate Trust in Electric Vehicle Charging, *Proc. ACM eEnergy 2019*, June 2019.

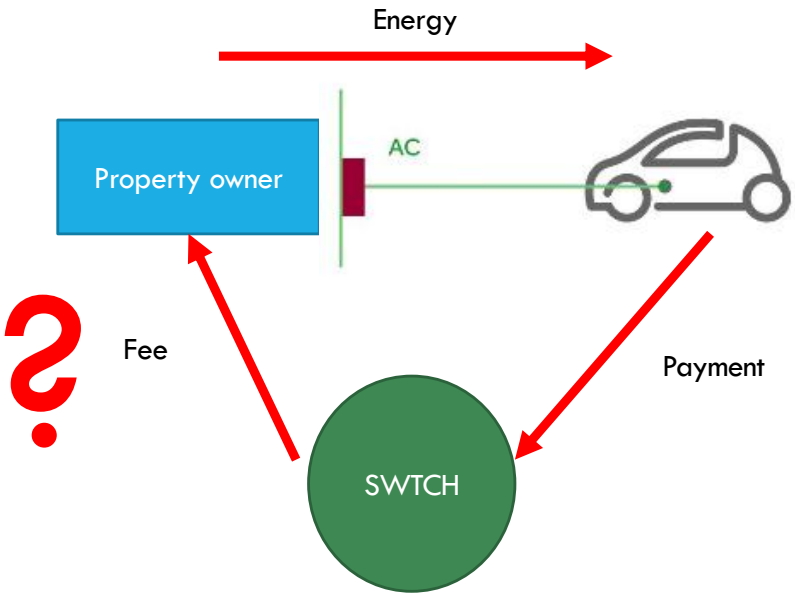
E.G.: BLOCKCHAINS FOR EV CHARGING

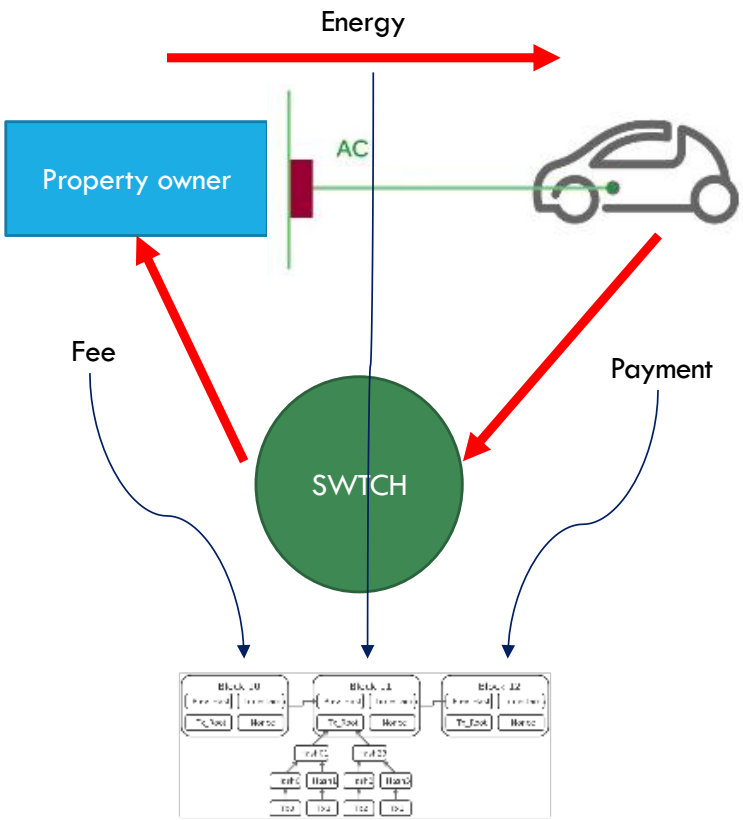
BLOCKCHAINS FOR EV CHARGING


chargepro


SWITCH


Energy
Property owner
AC
Fee
Payment
SWTCH


Energy
Property owner
AC
Fee
Payment
SWTCH



C. Gorenflo, L. Golab, and S. Keshav, Using a Blockchain to Mitigate Trust in Electric Vehicle Charging, To appear, *Proc. ACM eEnergy 2019*.

APPLICATIONS

Blockchain for Governance of Sustainability Transparency in the Global Energy Value Chain

Queen Mary School of Law Legal Studies Research Paper No. 283/2018

59 Pages · Posted: 23 Aug 2018 · Last revised: 8 Nov 2018

Lauren Downes
Queen Mary University of London, School of Law - Centre for Commercial Law Studies

Chris Reed
Queen Mary University of London, School of Law

Date Written: August 22, 2018

Contents lists available at ScienceDirect

Renewable and Sustainable Energy Reviews

journal homepage: www.elsevier.com/locate/rser

Blockchain technology in the energy sector: A systematic review of challenges and opportunities

Merlinda Andoni[a,*], Valentin Robu[a], David Flynn[a], Simone Abram[b], Dale Geach[c], David Jenkins[d], Peter McCallum[d], Andrew Peacock[d]

Proceedings of the 51st Hawaii International Conference on System Sciences | 2018

Dynamics of Blockchain Implementation – A Case Study from the Energy Sector

Simon Albrecht
University of Freiburg
simon.albrecht@is.uni-freiburg.de

Stefan Reichert
University of Freiburg
reichert@iig.uni-freiburg.de

Jan Schmid
Fresenius University
jan.schmid@hs-fresenius.de

Jens Strüker
Fresenius University
jens.strueker@hs-fresenius.de

Dirk Neumann
University of Freiburg
dirk.neumann@is.uni-freiburg.de

Gilbert Fridgen
University of Bayreuth
gilbert.fridgen@uni-bayreuth.de

CATEGORIES

Market creation

Market-based instruments (MBIs)

Auditing

- need to balance privacy and transparency

MARKET CREATION

1. Participation in wholesale market by prosumers
   - Consensys
   - Grid+
2. Peer-to-peer energy exchange
   - Brooklyn Microgrid
   - Conjoule
3. Storage operation market
   - sonnen/Tennet
4. Grid balancing market
   - Ponton

MARKET-BASED INSTRUMENTS (MBIS)

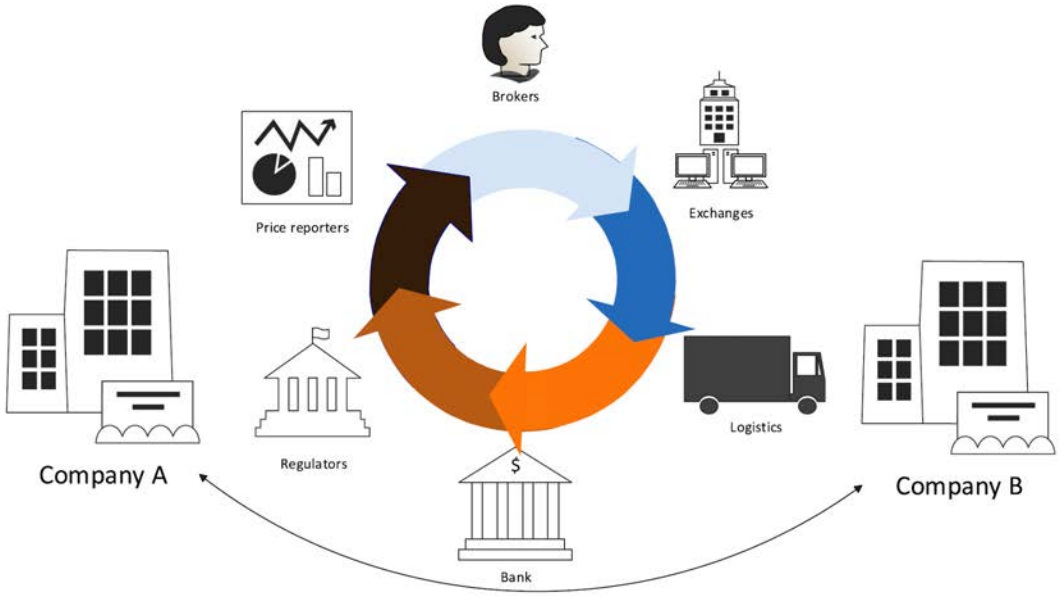
5. Renewable Energy Credits
   - Green
   - White
   - StromDAO, Energy Blockchain Labs, Singapore Power
6. Emissions Trading Schemes (cap-and-trade)
   - Veridium Labs
   - Stellar
7. EV operation

AUDITING

8. Behind-the-meter asset management
   - Energy Blockchain Network
9. EV charging
   - share&charge
   - SWTCH
10. Community sharing
   - enyway

MARKET CREATION

1. WHOLESALE MARKET



- Price discovery
- Trade execution
- Trade entry
- Logistics
- Confirmation
- Margining
- Know-Your-Customer
- Reconciliation
- Settlements
- Reporting

Andoni, Merlinda, et al. "Blockchain technology in the energy sector: A systematic review of challenges and opportunities." *Renewable and Sustainable Energy Reviews* 100 (2019): 143-174.

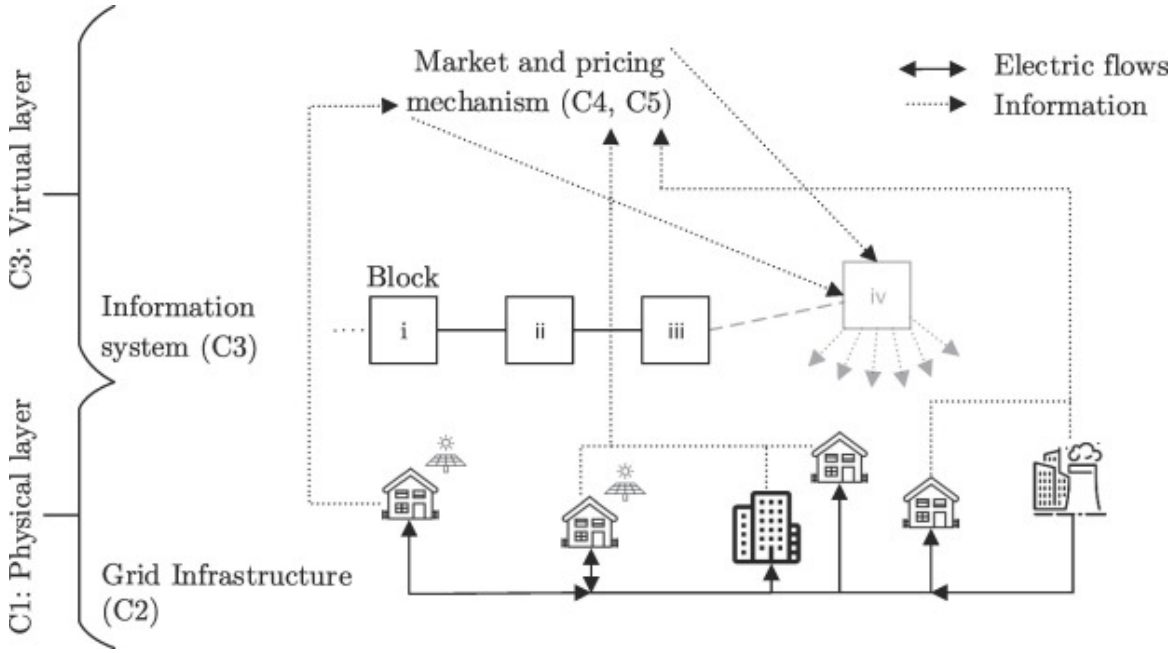
1. WHOLESALE MARKET

Why can't consumers participate?

Increase transparency

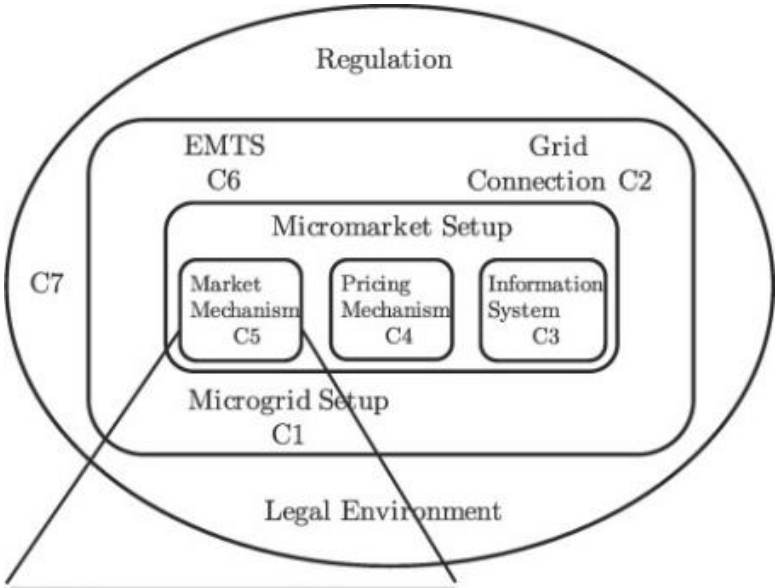
Decrease settlement times

2. P2P MARKET



Mengelkamp, Esther, et al. "Designing microgrid energy markets: A case study: The Brooklyn Microgrid." *Applied Energy* 210 (2018): 870-880.

2. P2P ENVIRONMENT



Sell Orders		Buy Order	
Price (MU/kWh)	Quantity (kWh)	Price (MU/kWh)	Quantity (kWh)
26.00	1	28.23	1
26.98	1	27.71	1
27.05	1	26.00	1
27.75	1	25.95	1
28.00	1	25.50	1

Mengelkamp, Esther, et al. "Designing microgrid energy markets: A case study: The Brooklyn Microgrid." *Applied Energy* 210 (2018): 870-880.

3. STORAGE OPERATION MARKET

Home electricity storage is increasingly possible (Tesla, BYD shown below)

3. GRID SUPPORT FROM STORAGE

Can use home storage to store excess renewable energy generated by local generators

Release when needed

But this can reduce storage lifetime

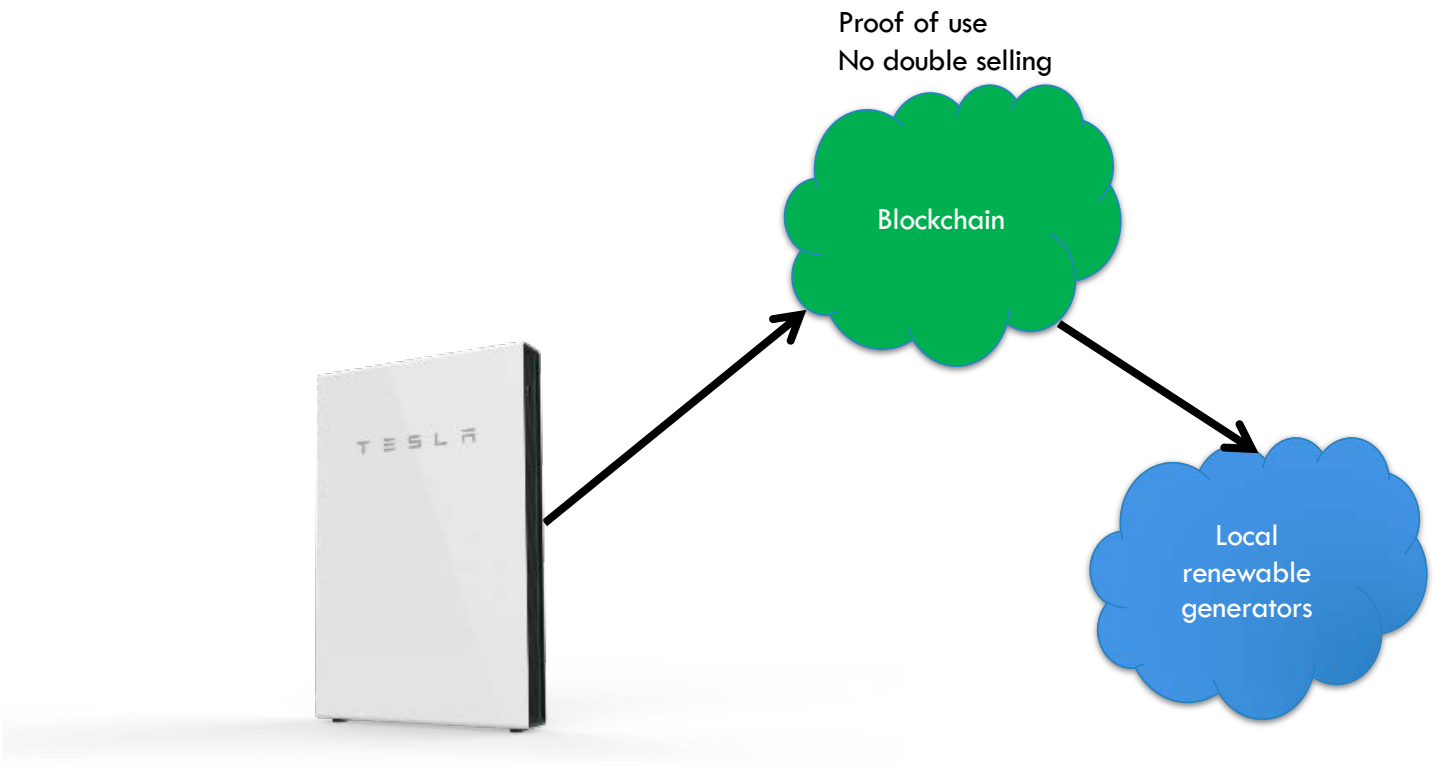
- Homeowners should be compensated

3. POTENTIAL CREDIT STRUCTURE

Suppose you can measure storage use

=> credit for grid support

3. ARCHITECTURE

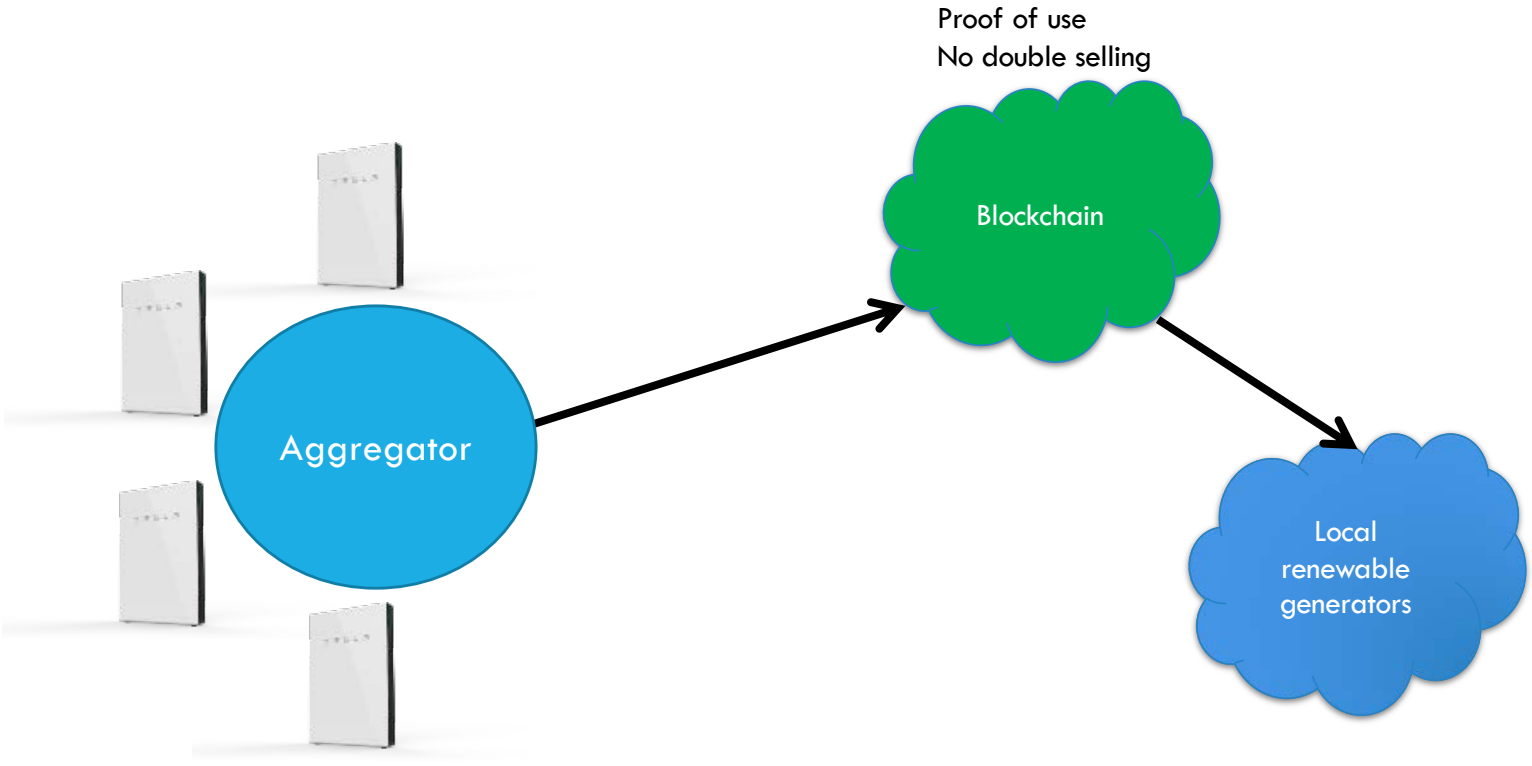


3. BUT…

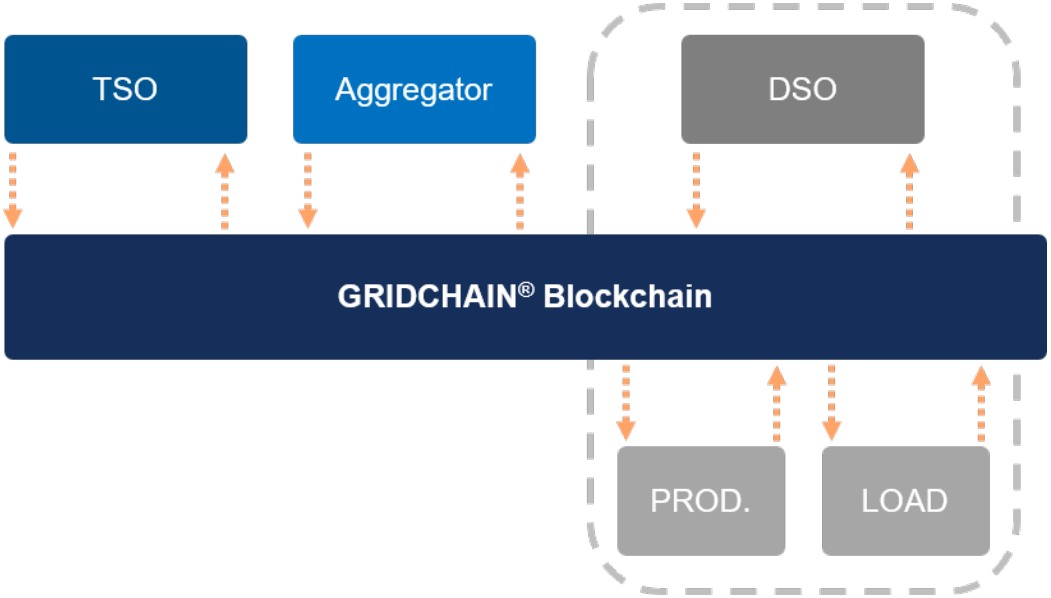
How can generators trust storage meters haven't been tampered with?

Do storage owners want detailed usage data to be known?

3. ARCHITECTURE



4. BALANCING MARKET



https://ponton.de/focus/blockchain/gridchain/

MARKET-BASED INSTRUMENTS

5. RENEWABLE ENERGY CREDIT

Green certificate

- Certifies generation of clean electricity
- Can be traded to electricity consumers to 'green' them
- Clean generators get paid twice

White certificate

- Certifies reduction in usage or energy efficiency
- Can also be traded to electricity consumers
- Energy efficiency gets paid twice (why?)

Issues

- Can we trust certificates?
- How do we trade them?

5. REC TRUST

Need to have an end-to-end chain of trust from generation to sale to resale

- Prevents greenwashing

Perfect use of blockchain!

However, requires a trusted meter

- Azure sphere

Hunt, Galen, George Letey, and Ed Nightingale. "The seven properties of highly secure devices." *Tech. report MSR-TR-2017-16* (2017).

5. REC TRADING

Can use a blockchain-based market

Prevents double-spending of certificates

6. EMISSIONS TRADING SCHEME (ETS)*

Idea: Issue credits to emitters each year

Credits must match emissions

Can sell excess credits

The total number of credits declines over time

*Also called cap-and-trade

6. ETS USING BLOCKCHAIN

Operation of ETS requires self-reporting

- Plenty of opportunity for mistakes or outright fraud!
  - Reduces effectiveness
- Opacity is the problem
- Blockchain provides transparency
  - Storing primary information
    - Can be audited later
  - But needs regulatory support for disclosure and access

6. ETS USING BLOCKCHAIN

How to balance domestic reporting with international impact?

- Need to have a hierarchy of chains
- Per-country chain where regulators have access to details
  - And not competitors!
- International chain only for provenance

7. EV OPERATION

Today, EV incentives are one-time purchase incentives

- easy to implement
- potentially perverse in jurisdictions with carbon-intensive electricity generation

7. OPERATIONAL INCENTIVES?

EVs

- Reduce particulate and SOx and NOx emissions
- In areas with sufficient renewable energy production, reduce carbon emission

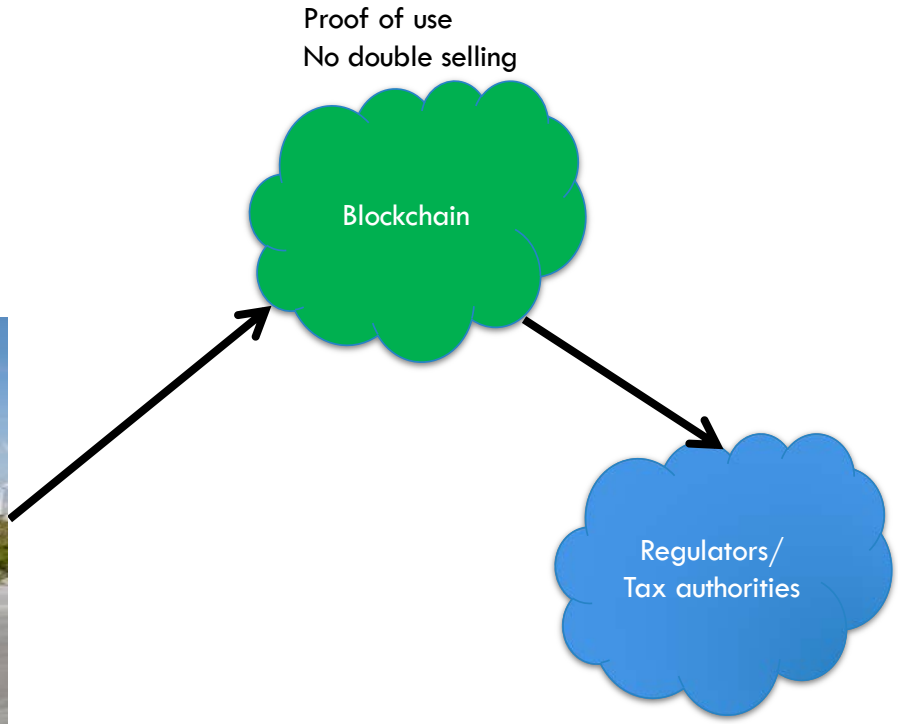
7. POTENTIAL CREDIT STRUCTURE

Suppose you can measure EV use and charging from green sources

=> credit for green operation

Credits can be traded just like RECs

7. ARCHITECTURE



7. BUT…

How can regulators trust odometers haven't been tampered with?

Do EV owners want detailed mobility data to be known?

AUDITING

8. BEHIND-THE-METER ASSET MANAGEMENT

Prosumer assets are mostly invisible to grid operators

- Type
- Capacity
- Maintenance status
- Operation limits
- Current status
- …

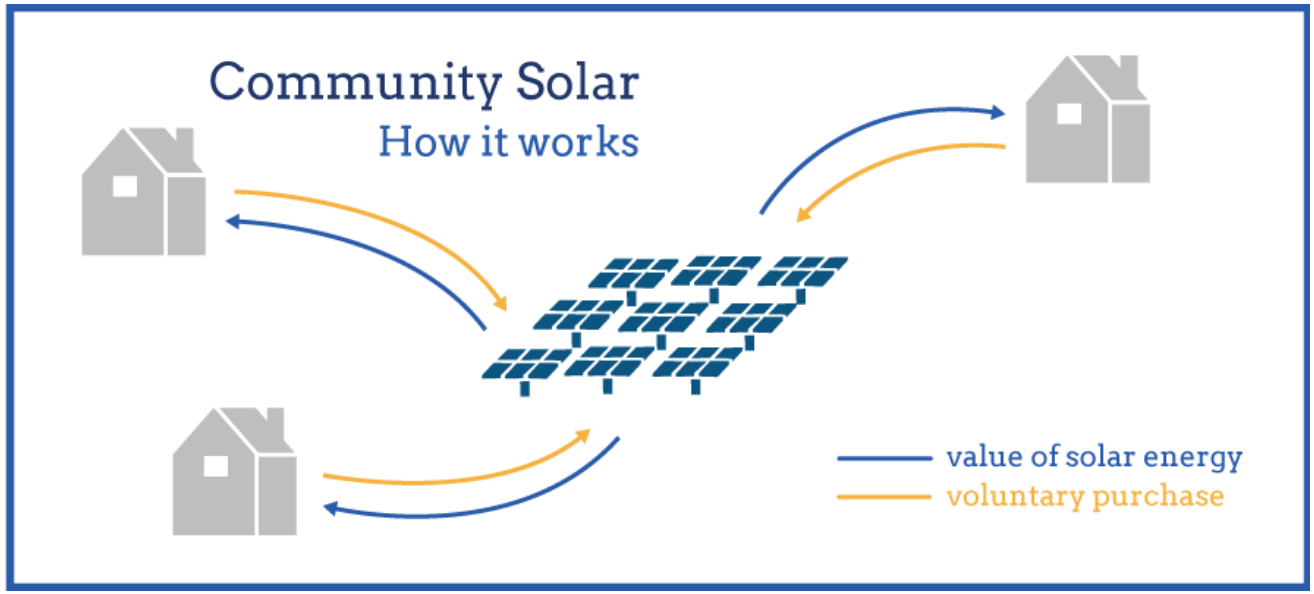
Blockchain allows creation of a digital twin

Allows asset tracking and analysis

9. EV CHARGING

(already discussed)

10. COMMUNITY RESOURCES



https://www.energysage.com/solar/community-solar/community-solar-power-explained/

CONCLUSION

CONCLUSION

Blockchains can be used to build energy systems even when there is lack of trust

- And can be used to improve the operation of existing systems

Three broad areas

- Creation of new markets
- Market-based instruments
- Audits

Many plausible and important use cases

Interesting research areas