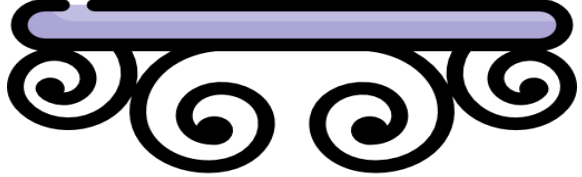
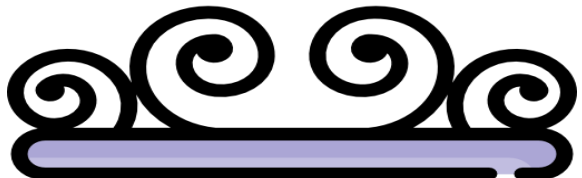


Blockchain

Privacy and Security

https://youtu.be/SxWWeB5luSE

https://youtu.be/_6SQNu6ZUAs



Pros and Cons

- Pros
  - Data integrity
  - Decentralizing

  → All user have the same data
- Cons
  - Security
  - Privacy

Privacy Invasion

- Public ledger (Bitcoin, Ethereum)
  - Opened database
    - Transaction
  - Pseudonymity
    - Address

  → Usage Analysis

- Private ledger (Hyperledger)
  - Permissioned database
  - Real-name system

Can't be preserved

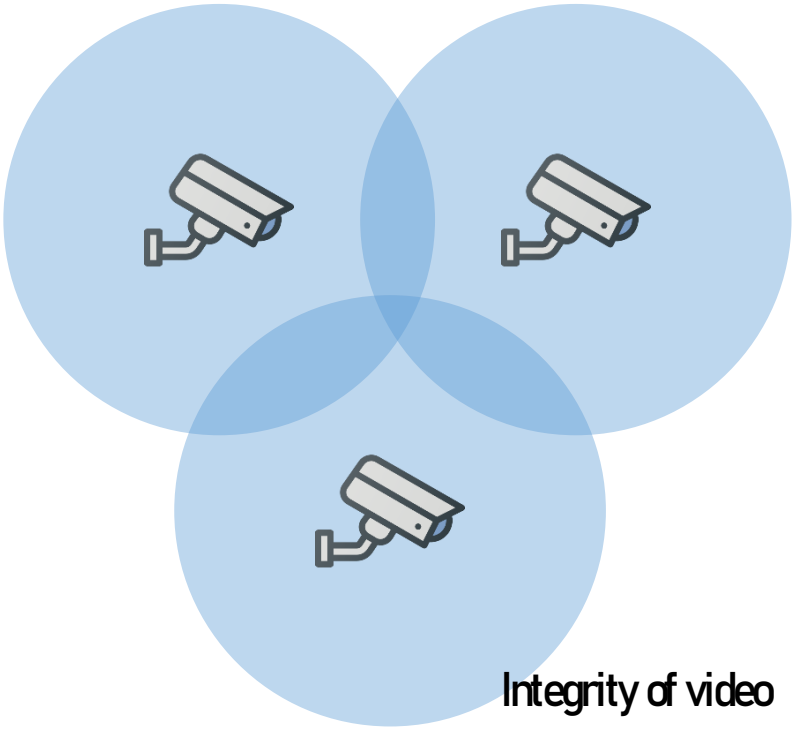
Why Privacy?

- GDPR (General Data Protection Regulation)
  - Privacy policy in EU
  - Trends

- Blockchain Application
  - Diverse use case

Use case

1. CCTV cooperation
2. Peer review system
3. Emission trading scheme



Integrity of video

	CCTV A	CCTV B	CCTV C
Traffic Accident	Yes	Yes	Yes
Violence	No	No	Yes

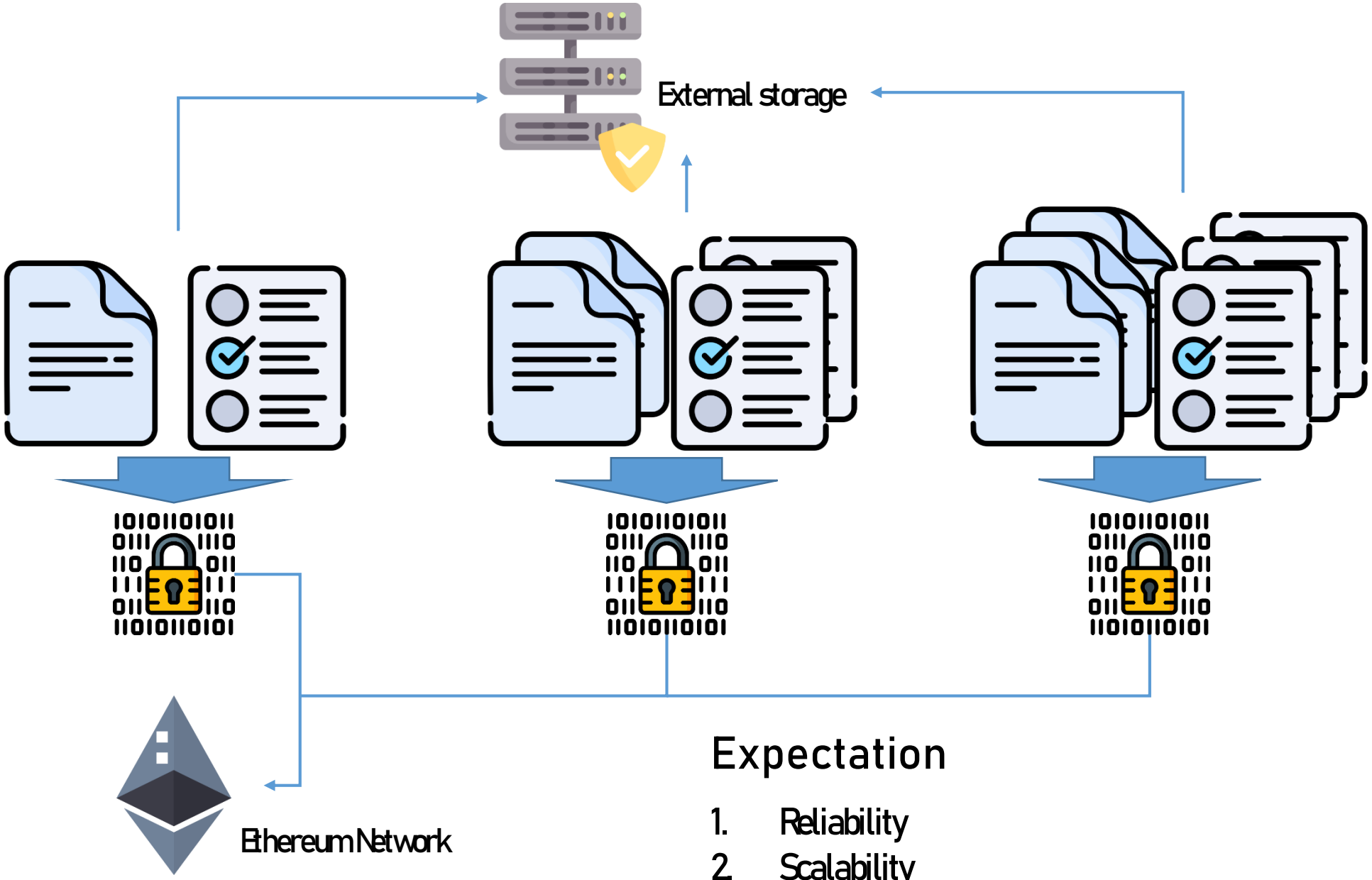
Data

Expectation

1. Reliability
2. Scalability
3. Privacy

Use case

1. CCTV cooperation
2. Peer review system
3. Emission trading scheme

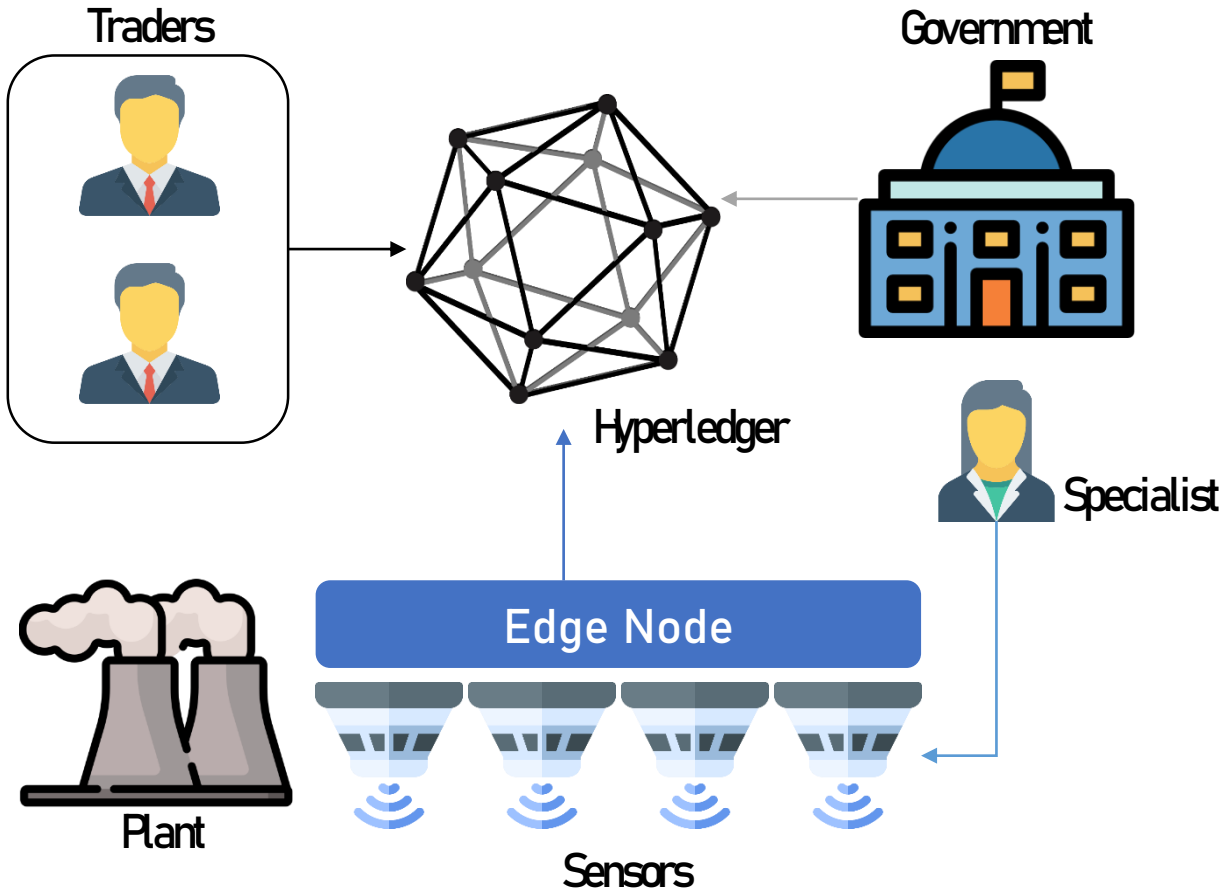


Expectation

1. Reliability
2. Scalability
3. Privacy

Use case

1. CCTV cooperation
2. Peer review system
3. Emission trading scheme



Expectation

1. Reliability
2. Scalability
3. Privacy

How to Preserve?

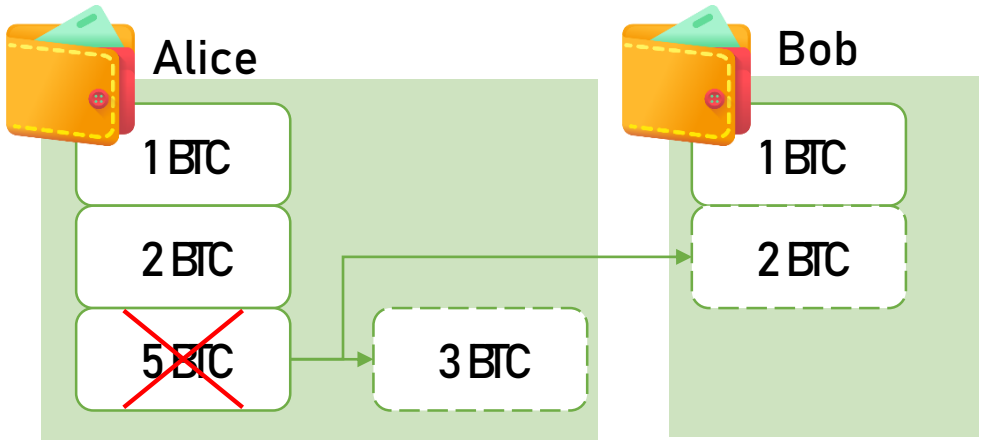
- Add something to existing blockchain

- Create new blockchain
  - Zero-knowledge

Method

1. UTXO
2. Mixing
3. Ring signature
4. Zero-knowledge

UTXO (Unspent transaction output)

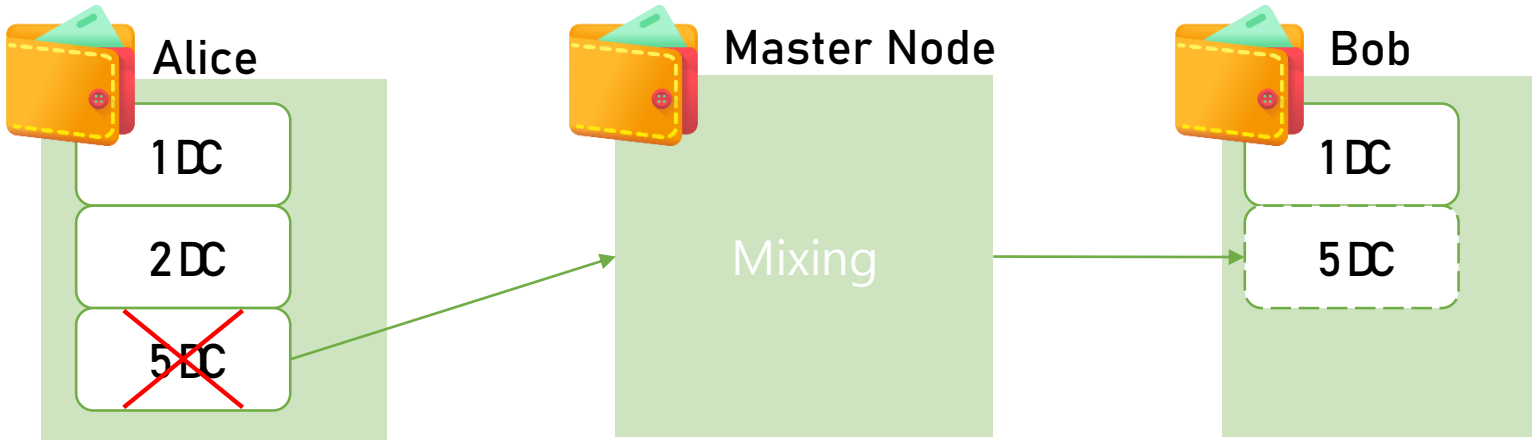


Bitcoin

Method

1. UTXO
2. Mixing
3. Ring signature
4. Zero-knowledge

Mixing

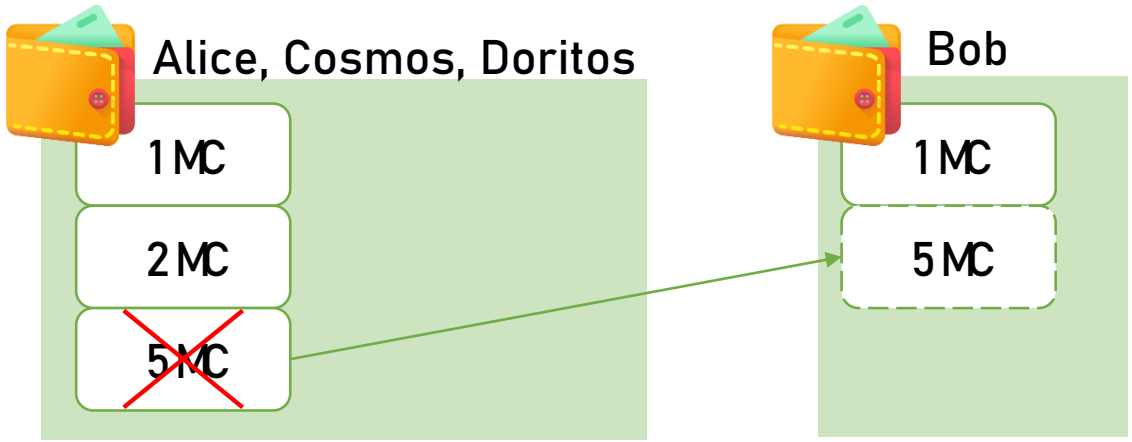


Dash

Method

1. UTXO
2. Mixing
3. Ring signature
4. Zero-knowledge

Ring signature



Monero

Method

1. UTXO
2. Mixing
3. Ring signature
4. Zero-knowledge

Zero-knowledge

Bitcoin Tx

Wallet A sent 3 BTC to wallet B on May 5th

. . .

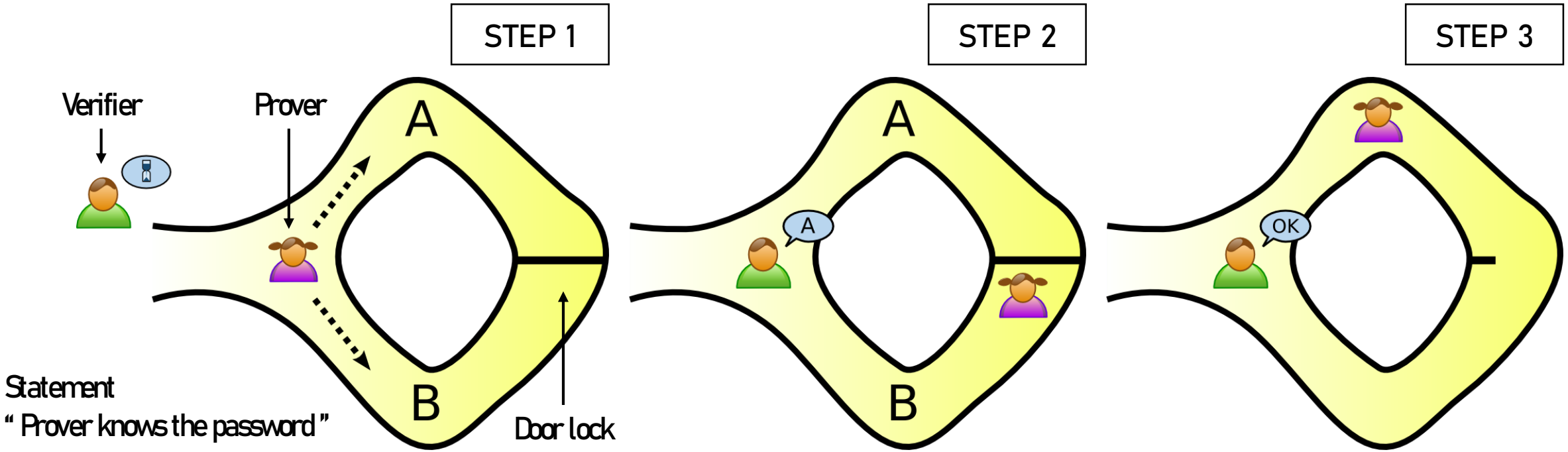
Zcash Tx

Wallet X sent X ZEC to wallet X on May 5th

. . .

Zcash

Zero-Knowledge Proof (ZKP)



ZKP Family

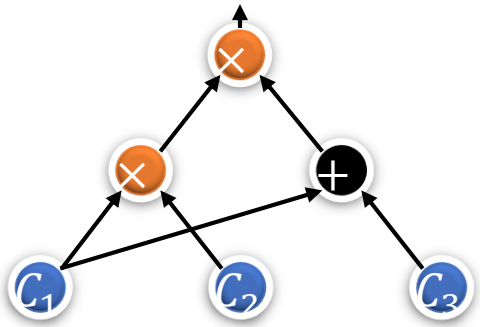
- ZK-SNARKs
  - Succint Non-interactive ARgument Knowledge

- ZK-STARKs
  - Succint Transparant ARgument Knowledge

ZK-SNARKs Overview

- Computation → Arithmetic Circuit → Quadratic Arithmetic Program

$$(C_1 \cdot C_2) \cdot (C_1 + C_3) = 7$$



$$L := \sum_1^5 C_i \cdot L_i,$$
$$R := \sum_1^5 C_i \cdot R_i,$$
$$O := \sum_1^5 C_i \cdot O_i$$

- Prove it
  - With Pinocchio Protocol (Evaluation)
  - With Pairing in Elliptic Curve Cryptosystem (Hding Evaluation)

ZK-STARKs Intro

- SNARKs Assumption
  - ECC Pairing

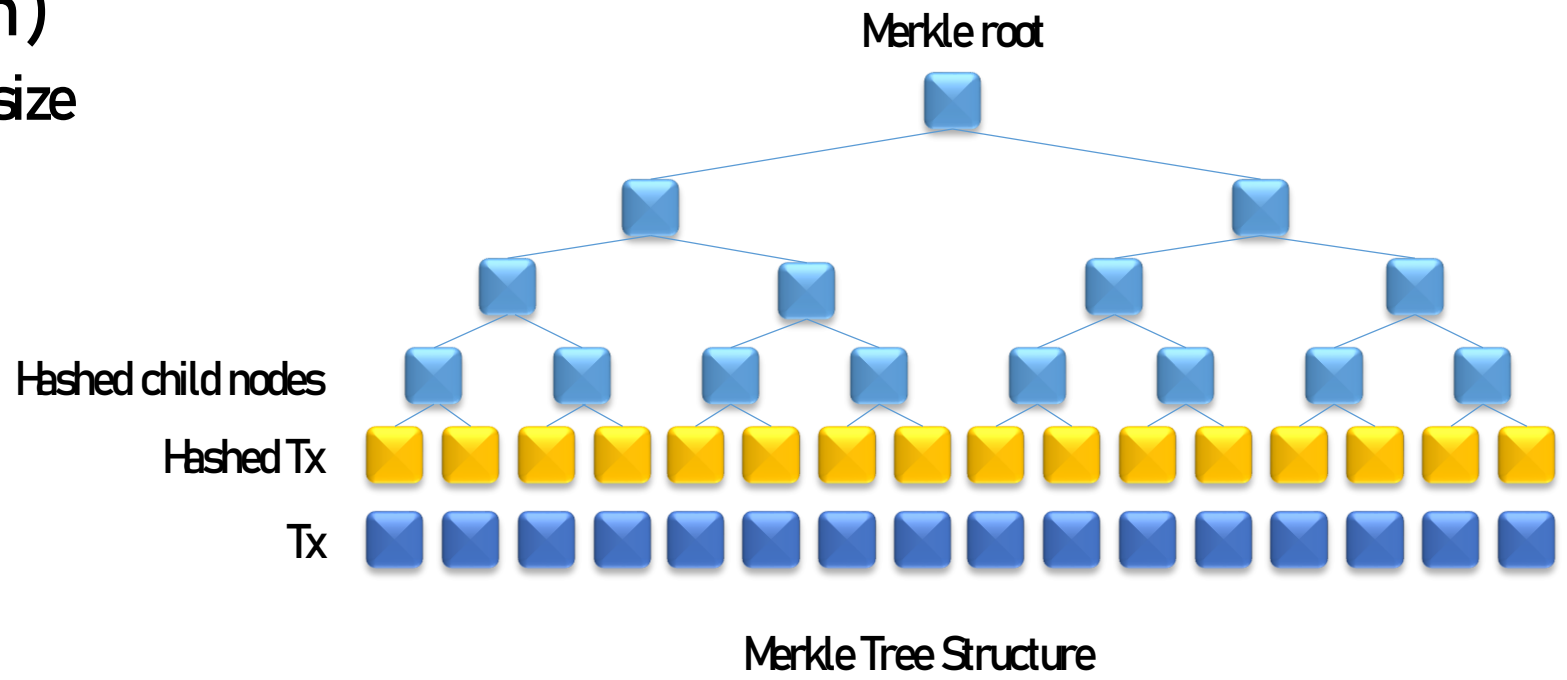
  → Vulnerable from Quantum Algorithms

- STARKs Assumption
  - Merkle Tree

  → Safe from Quantum Algorithms
  → Increase Size of Proof (hundreds of byte to hundreds of kilobyte)

Merkle Tree

- SHA-256 (Hash function)
  - One way, Fixed output size
- Validation



Merkle Tree Structure

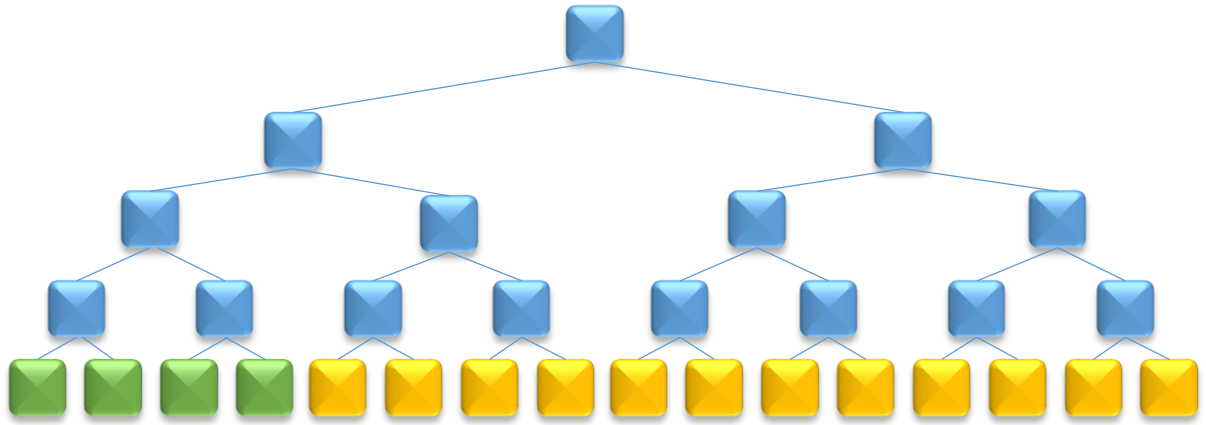
ZK-STARKs

- $Suppose\ P(x)$
  - $0 \leq P(x) \leq 9$
  - $1 \leq x \leq 1{,}000{,}000$

- $How\ to\ prove\ it\ ?$
  - $Try\ 1{,}000{,}000\ times$
  - $Randomly\ sample\ n\ points$
  - $Construct\ C(x), where\ C\big(P(x)\big) = 0$
    - $C(P(x)) = (X-1)(X-2)\ldots(X-1000000) * D(x) = Z(x) * D(x)s$
    - $Then\ we\ prove\ it$

ZK-STARKs

- Communication between prover and verifier
  - First (prover)
    - $evaluation\ P(x)\ and\ D(x)\ on\ 1{\sim}1{,}000{,}000{,}000$
    - $make\ a\ merkle\ tree\ and\ send\ it$
  - Second (verifier)
    - $Choose\ random\ 16\ points$
    - $Require\ branches$
  - Third (prover)
    - $Provide\ branches$
  - Fourth (verifier)
    - $Check\ the\ merkle\ root$
    - $Check\ C\big(P(x)\big) = Z(x) * D(x)$



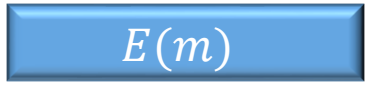
Privacy Communication

- Covert Communication
  - Hding relationship between two party
  - Hding when communication is started

- Covert Channel in Blockchain
  - Condition
    - Accessibility
    - Immutability
    - Reliability

Covert Communication on Blockchain (BLOCCE)

- Encrypt Message



- Start Indicator

- Concatenate

- Example
  - λ is 1011

Transaction List

Address 01001 sent 3 BTC to wallet 00001 on May 5th
Address 00000 sent 3 BTC to wallet 10101 on June 6th
Address 00111 sent 3 BTC to wallet 00001 on June 10th
Address 10011 sent 3 BTC to wallet 10101 on July 5th
→ $E(m) from\ here$
Address 00011 sent 3 BTC to wallet 00001 on July 11th
Address 00001 sent 3 BTC to wallet 00001 on July 21th
. . .

Security Proof

Using history of Alice's payment
→ Indistinguishibility