# Account-Wise Ledger:

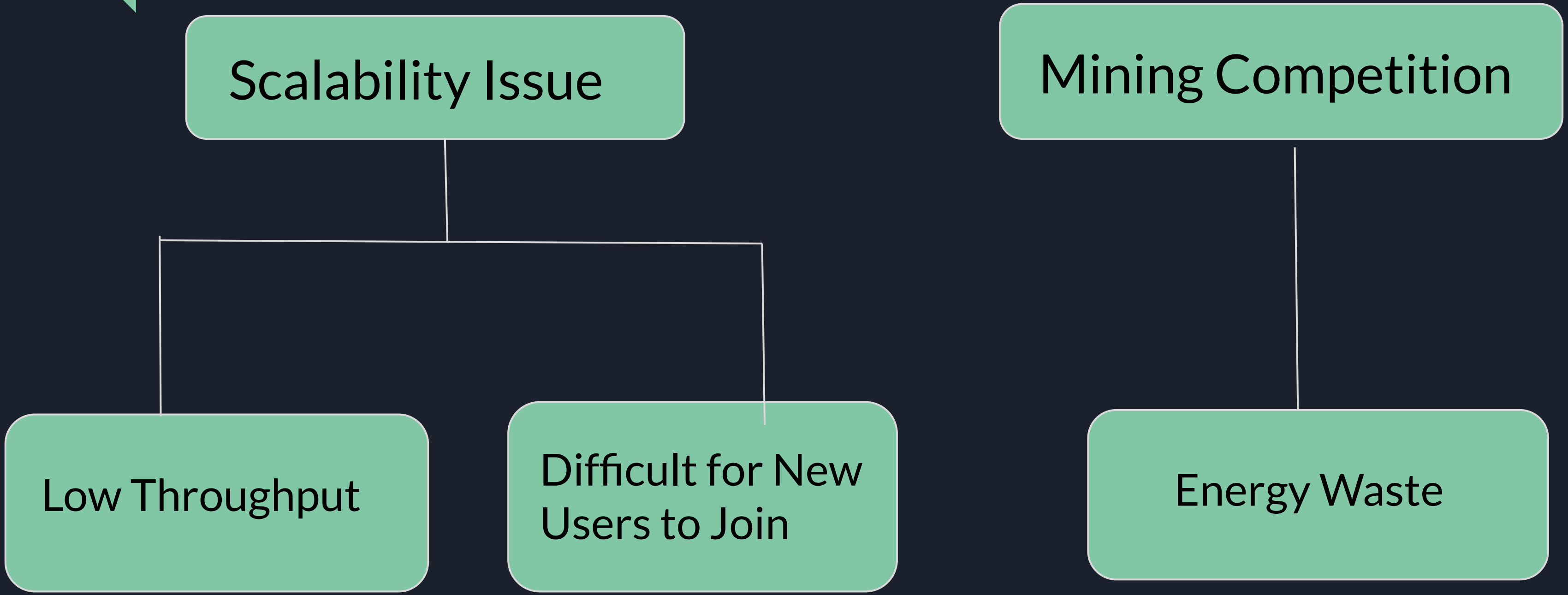
## Implementation

Che-Yu Liu, Jia-Wei Liang, Yi-Chen Liu

# Agenda

- Current Situation and Our Motivations
- Summary and Our Contribution
- Mechanism and How We Overcome
- Security Discussion
- Implementation
- Q&A

# Current Situation of Blockchain



Scalability Issue

Low Throughput

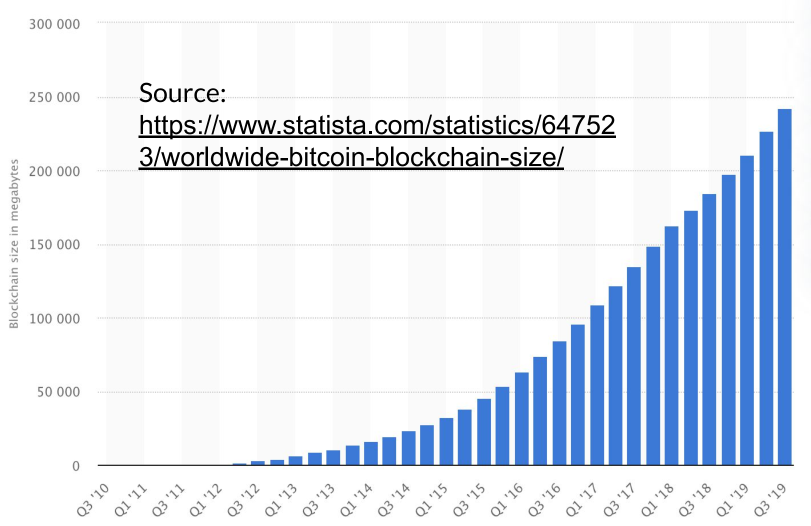
Difficult for New Users to Join

Mining Competition

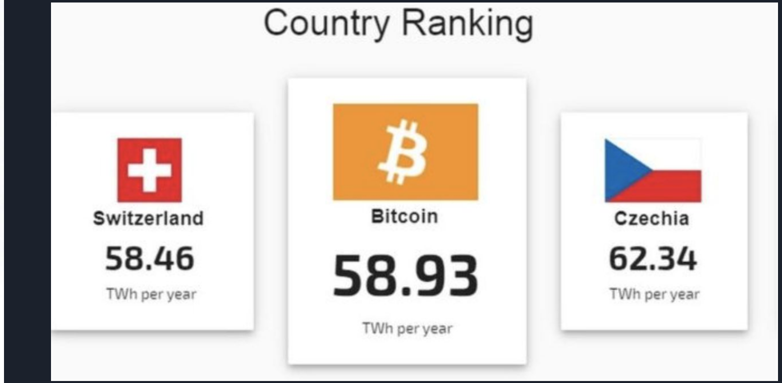
Energy Waste

# Why is Scalability/Mining Important?

| Real World Applications | Cryptocurrency |
|---|---|
| ● VisaNet: 4K transaction per sec.<br>● Alipay: 256K transaction per sec. | ● Bitcoin: 7 transaction per sec.<br>● Ethereum: 15 transaction per sec. |



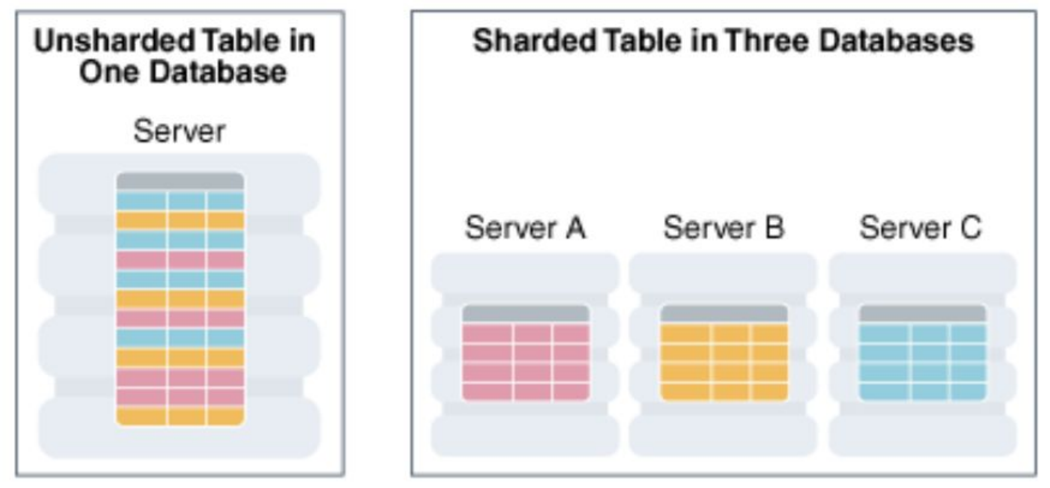
Source: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/



Source: https://www.bbc.com/news/technology-48853230

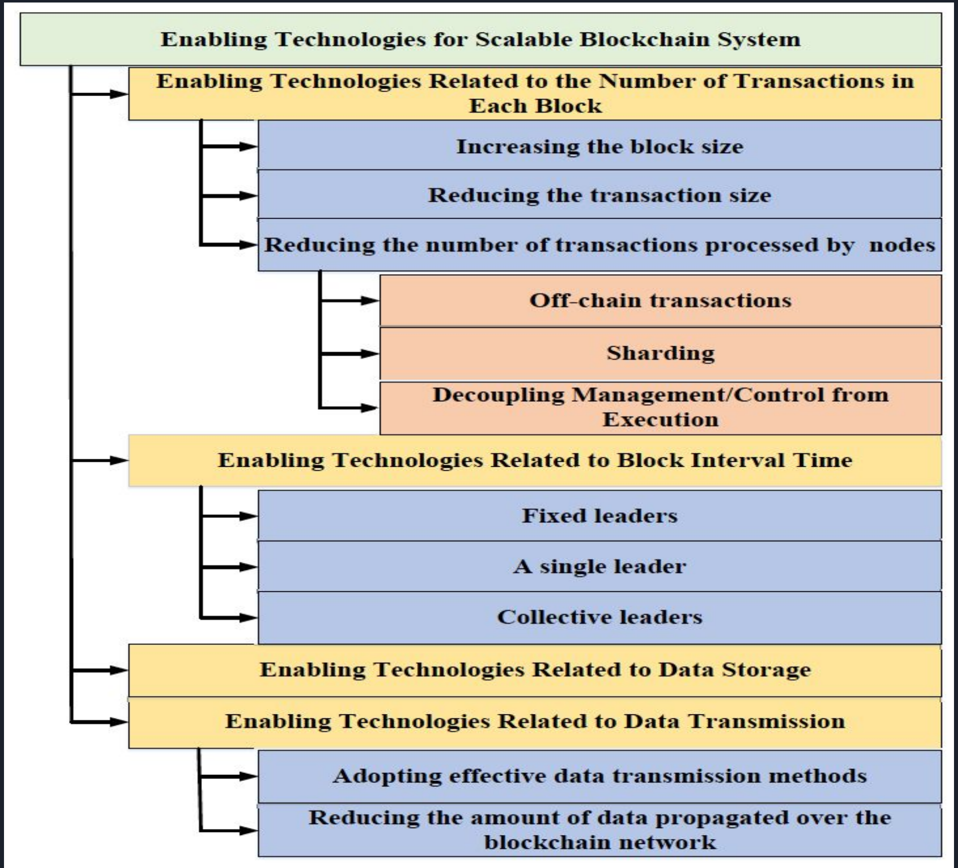
# Current Solutions:

- Scalability Issue => Solution: Database Sharding
- Mining Competition => Solution: Proof of Stack


Unsharded Table in One Database
Server
Sharded Table in Three Databases
Server A
Server B
Server C

https://blogs.oracle.com/dev2dev/java-scalability-with-sharded-database

# Related Studies



- Enabling Technologies for Scalable Blockchain System
  - Enabling Technologies Related to the Number of Transactions in Each Block
    - Increasing the block size
    - Reducing the transaction size
    - Reducing the number of transactions processed by nodes
      - Off-chain transactions
      - Sharding
      - Decoupling Management/Control from Execution
  - Enabling Technologies Related to Block Interval Time
    - Fixed leaders
    - A single leader
    - Collective leaders
  - Enabling Technologies Related to Data Storage
  - Enabling Technologies Related to Data Transmission
    - Adopting effective data transmission methods
    - Reducing the amount of data propagated over the blockchain network

J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu and Y. Liu, "A Survey on the Scalability of Blockchain Systems," in *IEEE Network*, vol. 33, no. 5, pp. 166-173, Sept.-Oct. 2019.

Lots of them address scalability problem but…

disregard “security discussion”

# Our Goals and Contribution

- Account-Wise Ledger: *Reduce the Burden of Each Node*

(1) Divide the blockchain into different sub-networks

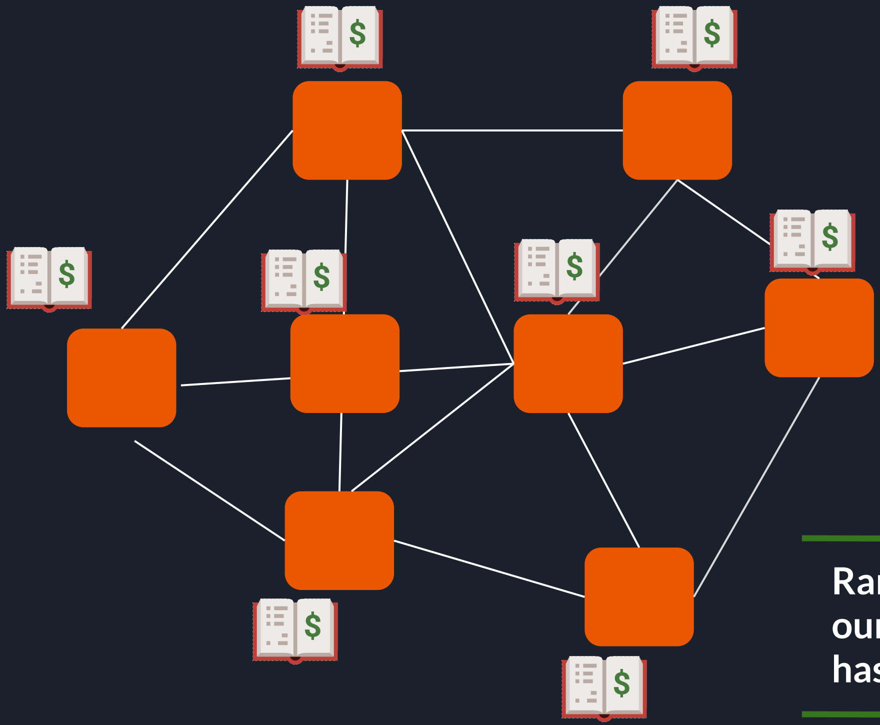
(2) Each node only needs to store the data in its own sub-network

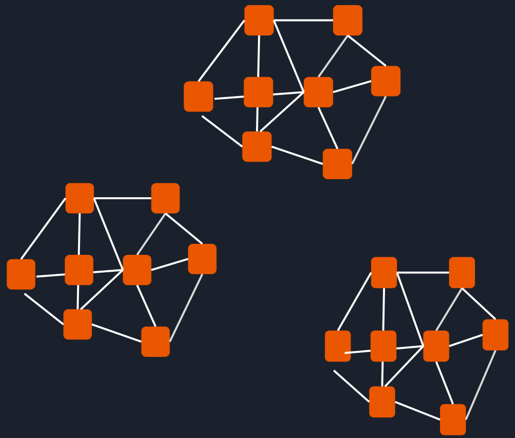
- Three-End Commitment Protocol: *Cancel Mining Competition*

(1) Removes competition reward

(2) Increases the overall blockchain security

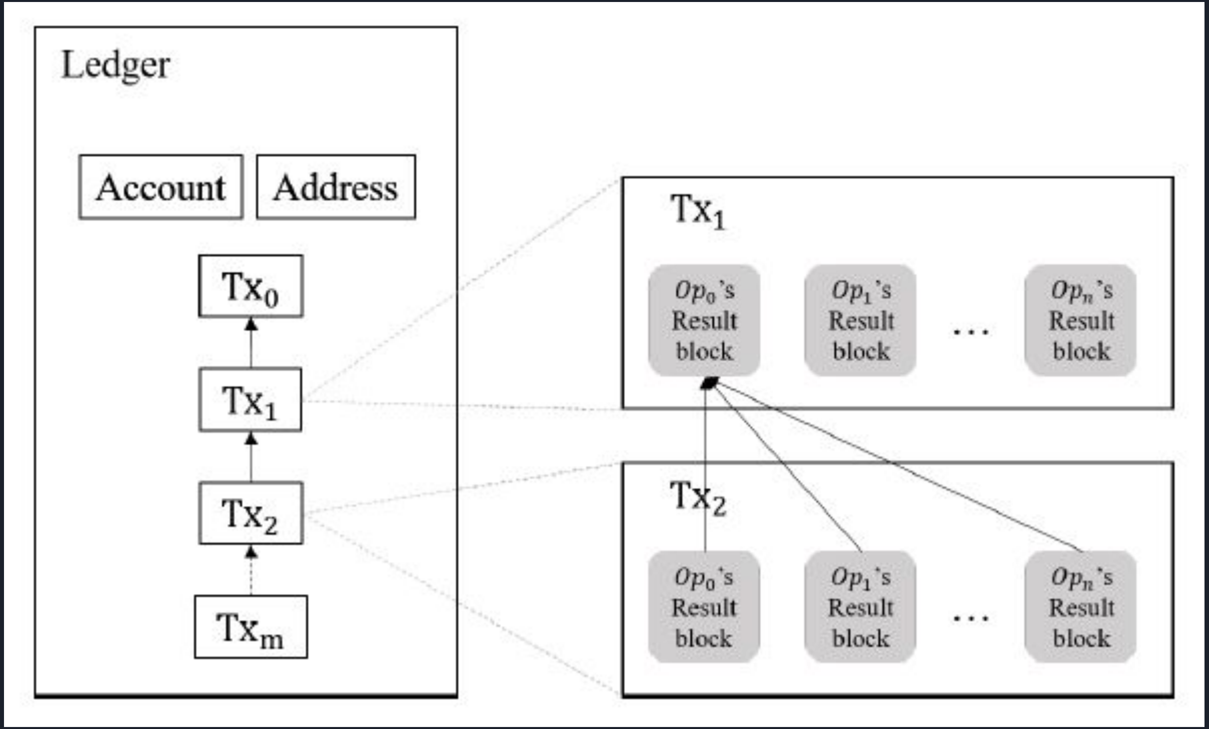
# Account-Wise Ledger



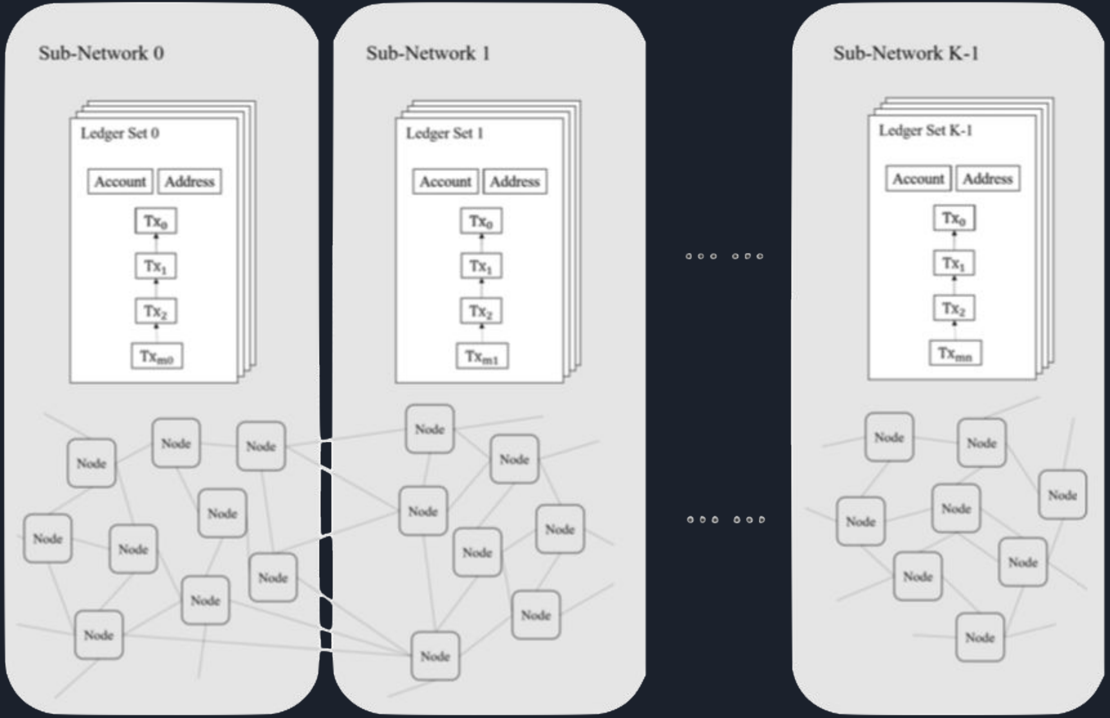


Randomly assigned to each network but our protocol makes sure each network has similar numbers of nodes

# Account Wise Ledger (cont.)



# Account Wise Ledger (cont.)



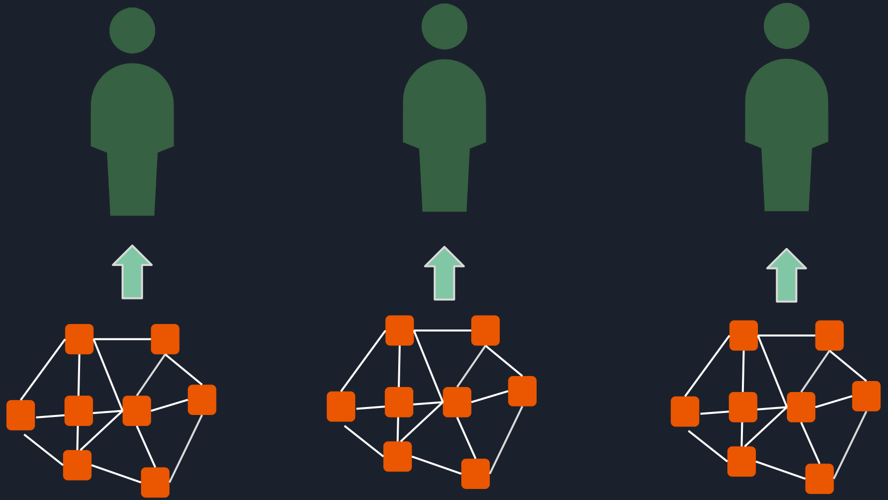
# Three-End Commitment

STEP 1: Sender announces the transaction task to the receiver and each subnetwork

STEP 2: Receiver announces the acknowledgement of each subnetwork

# Three-End Commitment (cont.)

STEP 3: Each subnetwork randomly selects one node as the representative operator (High Council)

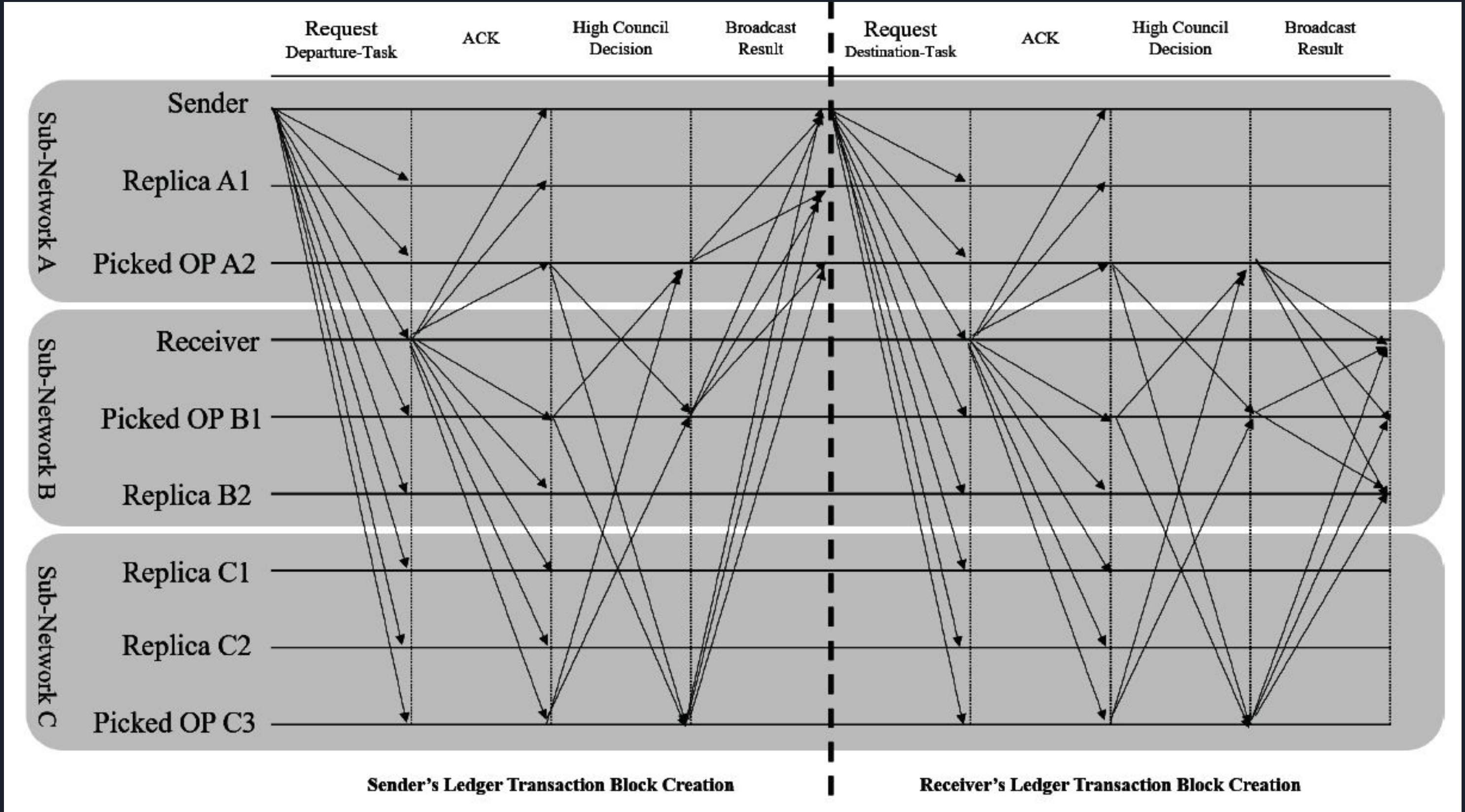


# Three-End Commitment (cont.)

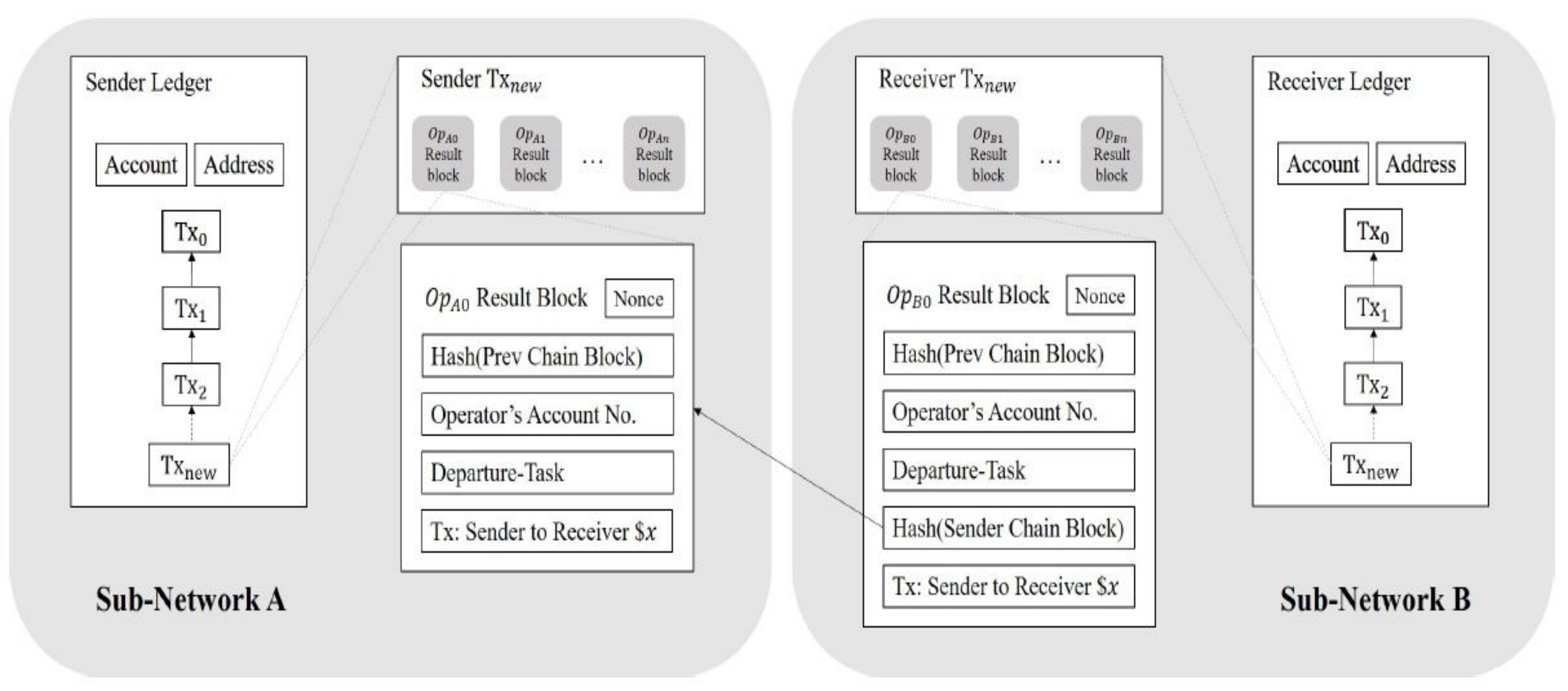
STEP 4: Representative operator do the mining and broadcast to each node in the whole network

The operators who creates the majority answer share the reward

# Three-End Commitment (cont.)



# System Design



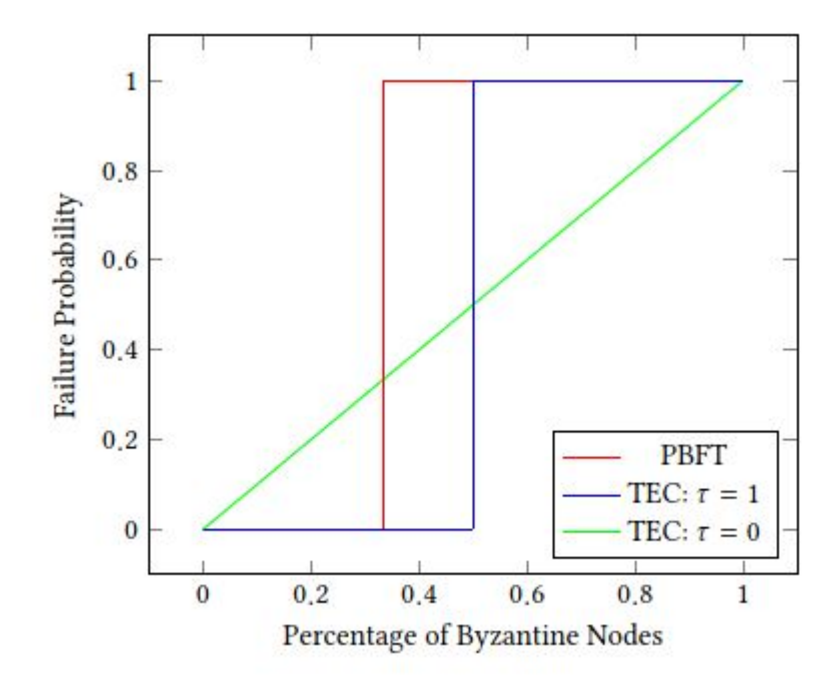
# Advantages of Our Design

- Speed up the response time of request
  - Queries  go over fewer data and the results are returned much more quickly by sharing one table into multiple tables.
- More reliable by mitigating the impact of outages
  - An outage is likely to affect only a single shard
- Solve the major drawback of database sharding (Sharding incorrectly)
  - All the related users in the account will do the verification

# Security Discussion

- Faulty Type - Sender:
  - The Receiver would not send the ACK, attack failed.
- Faulty Type - Receiver:
  - The Receiver would not receive any money, meaningless.
  - Always-Accept Principle: Whatever decision made by the High Council, accept it anyway
- Faulty Type - Sender & Receiver Collusion:
  - The High Council will consult the sender side sub-network and the receiver side sub-network to ensure the validity of the transaction
- Faulty Type - Operators:
  - $K$: the number of sub-networks
  - $\tau$: the distribution coefficient

# Security Discussion - $\tau$



- $\tau = 0$: the distribution of faulty participants is extremely unevenly
- $\tau = 1$: the distribution of faulty participants is extremely evenly

# **Security Discussion** - K

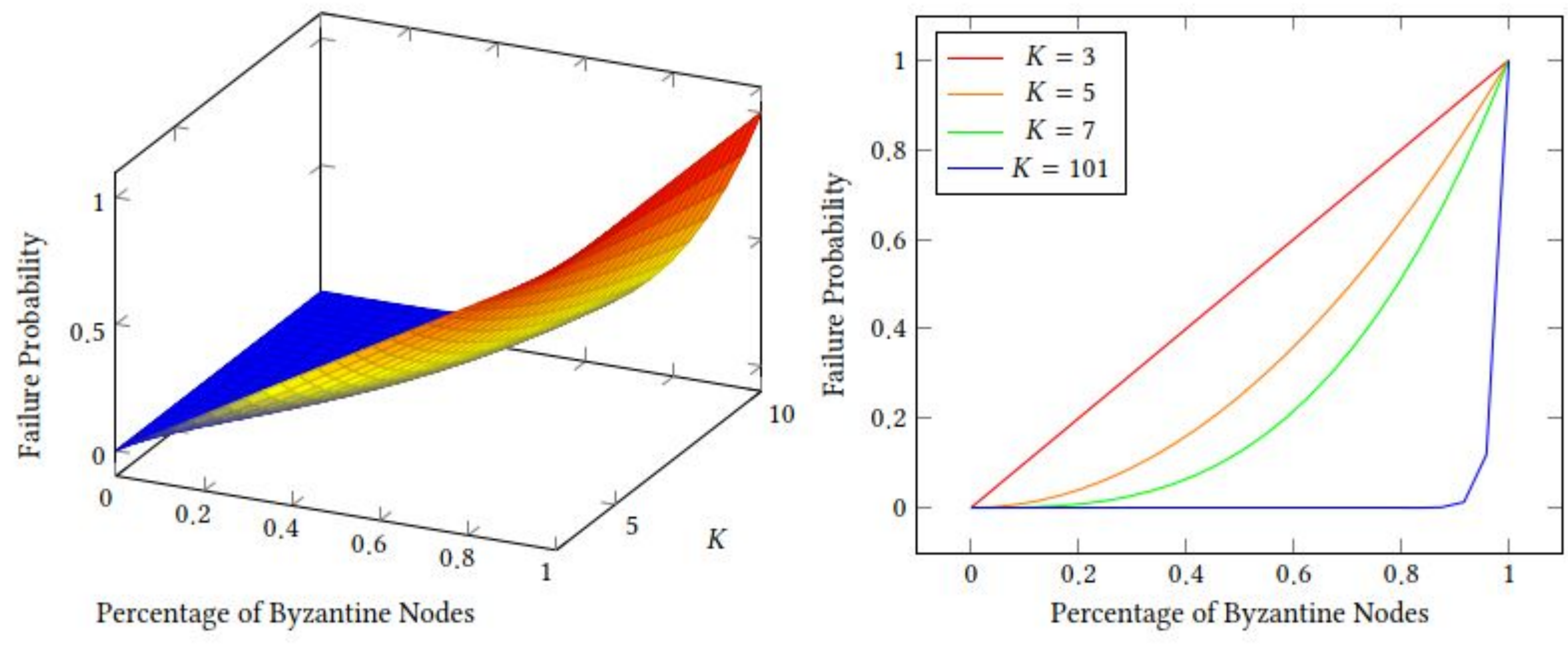
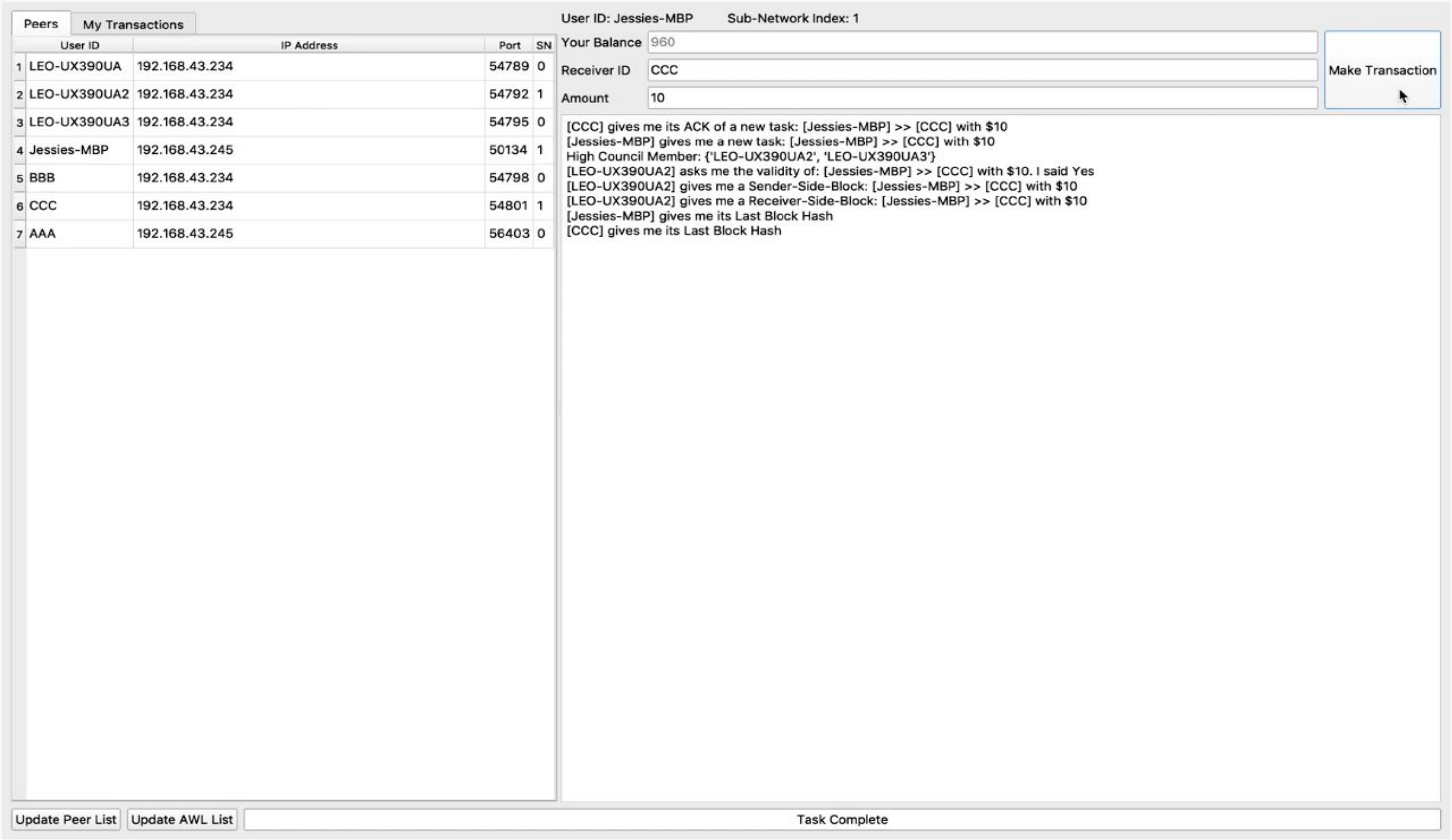


**Figure 6: The changes of the failure probability of a transaction corresponding to the number of $K$. Assume $\tau = 0$**

# Implementation

- Inter and Cross Sub-network transaction
  - Send task and receive ACK
  - Broadcast
  - High Council is elected

# Inter Sub-network Transaction



User ID: Jessies-MBP    Sub-Network Index: 1

Your Balance: 960

Receiver ID: CCC

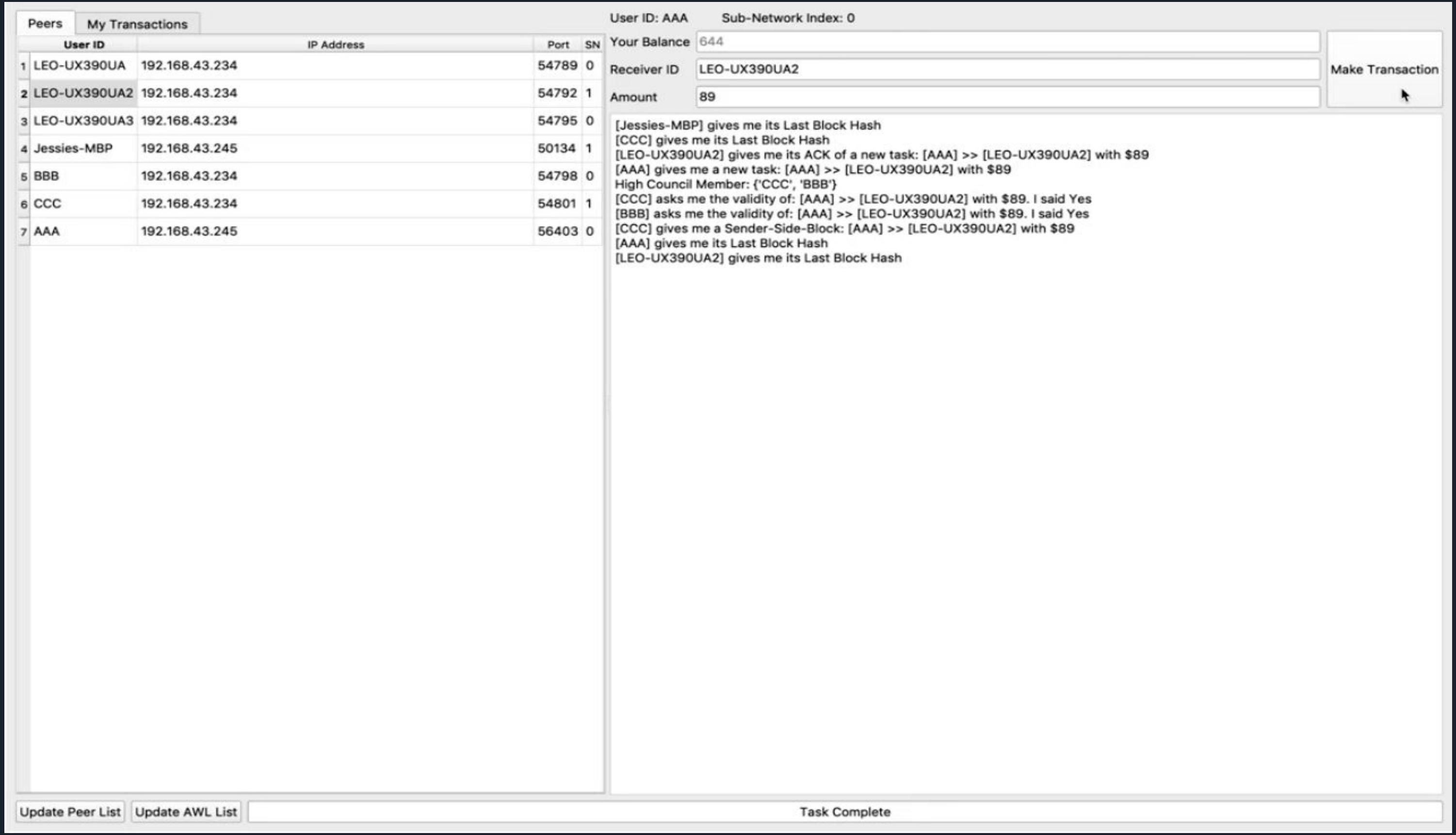
Amount: 10

|   | User ID | IP Address | Port | SN |
|---|---|---|---|---|
| 1 | LEO-UX390UA | 192.168.43.234 | 54789 | 0 |
| 2 | LEO-UX390UA2 | 192.168.43.234 | 54792 | 1 |
| 3 | LEO-UX390UA3 | 192.168.43.234 | 54795 | 0 |
| 4 | Jessies-MBP | 192.168.43.245 | 50134 | 1 |
| 5 | BBB | 192.168.43.234 | 54798 | 0 |
| 6 | CCC | 192.168.43.234 | 54801 | 1 |
| 7 | AAA | 192.168.43.245 | 56403 | 0 |

```
[CCC] gives me its ACK of a new task: [Jessies-MBP] >> [CCC] with $10
[Jessies-MBP] gives me a new task: [Jessies-MBP] >> [CCC] with $10
High Council Member: {'LEO-UX390UA2', 'LEO-UX390UA3'}
[LEO-UX390UA2] asks me the validity of: [Jessies-MBP] >> [CCC] with $10. I said Yes
[LEO-UX390UA2] gives me a Sender-Side-Block: [Jessies-MBP] >> [CCC] with $10
[LEO-UX390UA2] gives me a Receiver-Side-Block: [Jessies-MBP] >> [CCC] with $10
[Jessies-MBP] gives me its Last Block Hash
[CCC] gives me its Last Block Hash
```

Task Complete

# Cross Sub-network Transaction



|   | User ID | IP Address | Port | SN |
|---|---|---|---|---|
| 1 | LEO-UX390UA | 192.168.43.234 | 54789 | 0 |
| 2 | LEO-UX390UA2 | 192.168.43.234 | 54792 | 1 |
| 3 | LEO-UX390UA3 | 192.168.43.234 | 54795 | 0 |
| 4 | Jessies-MBP | 192.168.43.245 | 50134 | 1 |
| 5 | BBB | 192.168.43.234 | 54798 | 0 |
| 6 | CCC | 192.168.43.234 | 54801 | 1 |
| 7 | AAA | 192.168.43.245 | 56403 | 0 |

User ID: AAA    Sub-Network Index: 0

Your Balance: 644

Receiver ID: LEO-UX390UA2

Amount: 89

```
[Jessies-MBP] gives me its Last Block Hash
[CCC] gives me its Last Block Hash
[LEO-UX390UA2] gives me its ACK of a new task: [AAA] >> [LEO-UX390UA2] with $89
[AAA] gives me a new task: [AAA] >> [LEO-UX390UA2] with $89
High Council Member: {'CCC', 'BBB'}
[CCC] asks me the validity of: [AAA] >> [LEO-UX390UA2] with $89. I said Yes
[BBB] asks me the validity of: [AAA] >> [LEO-UX390UA2] with $89. I said Yes
[CCC] gives me a Sender-Side-Block: [AAA] >> [LEO-UX390UA2] with $89
[AAA] gives me its Last Block Hash
[LEO-UX390UA2] gives me its Last Block Hash
```

# Thank You
# Triple L Group