Technical presentation

Rodolfo Pietro Calabrò
Pasquale Gatto

Two kind of users

- Client

  Send a transaction (event,vote) to miners

- Miner

  Receive a transaction and validate it

  Apply Proof of Lottery and send solution to other miners

  Storing in Blockchain if all correct

Communication protocol “Tri da chiazza”

This protocol take the name from a simple italian dialect word.

When in typical calabrian town the people see three friends in group, they often call it "i tri da chiazza".

This communication protocol a part every joke is very simple and useful for a didactic purpose.

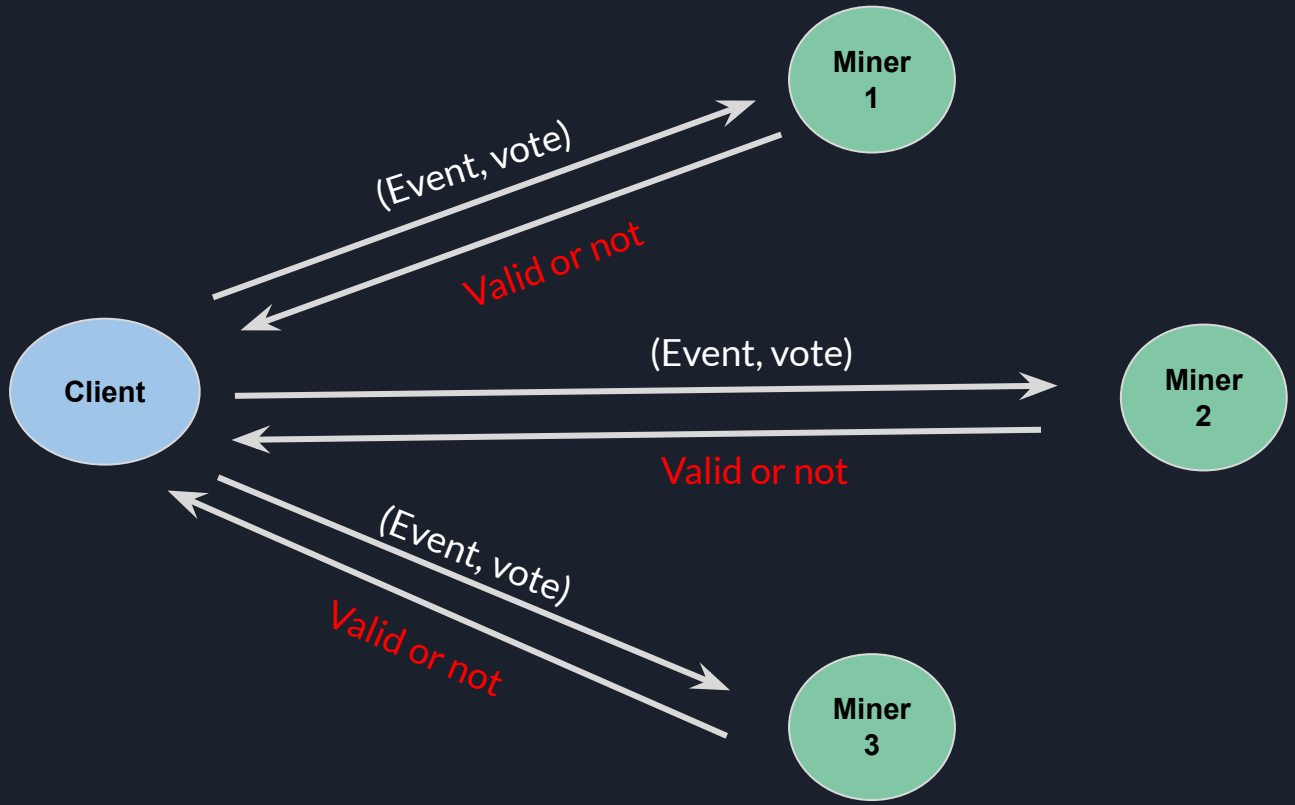
To avoid problem with p2p, such as nat, firewalls hole punching, and a lot of stuff...

We make a simple choice/requirement.

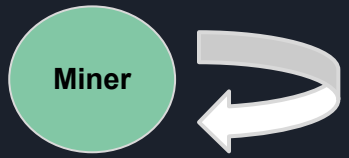
We need to know at least 3 know miners ip to send transactions.

In practical terms a blockchain to work must have at least 3 miners.

Client - Send transaction



Miner - Receive a transaction and validate it



(event,vote) validation:

Semantic

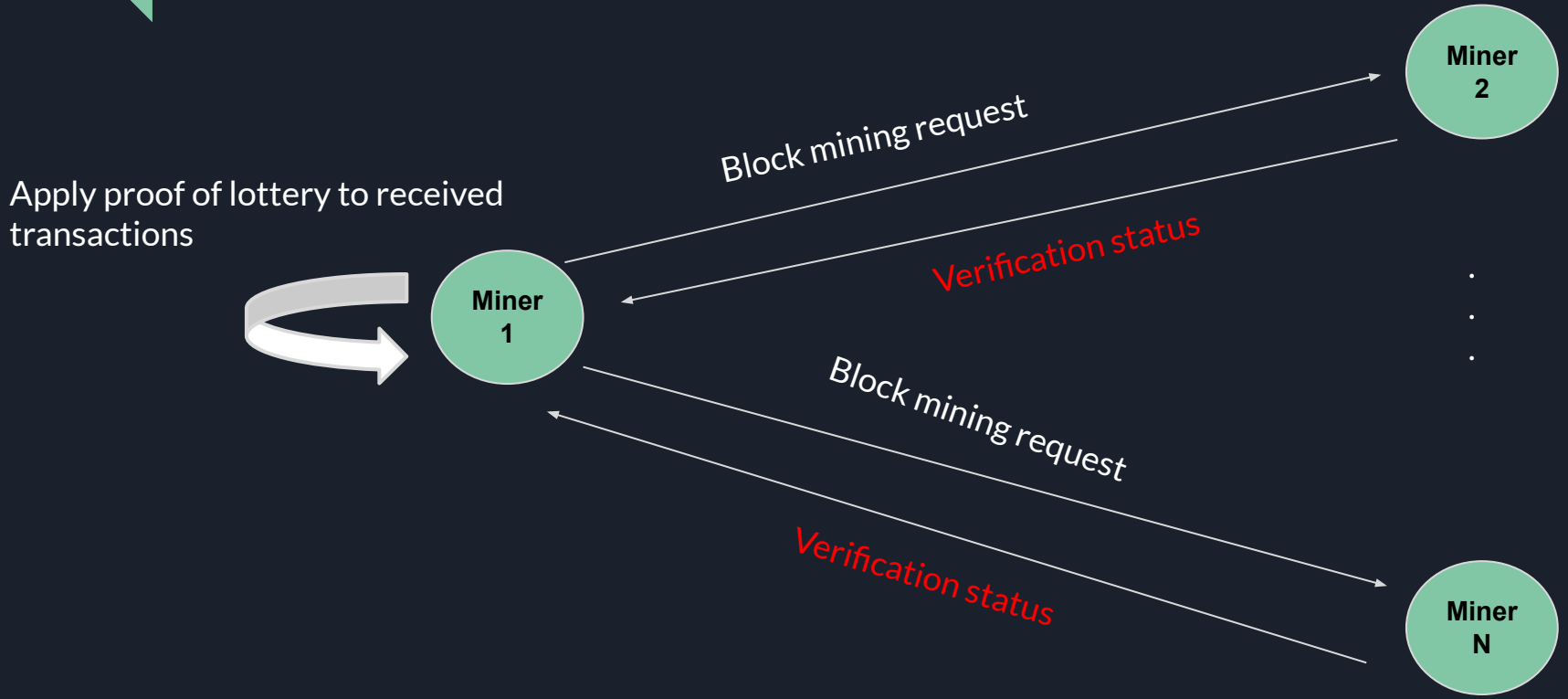
- **(event, vote)** isn't already sented
- **(event, vote)** isn't in the ledger

(Obviously by the same address of sender)

Syntax

- **vote** is numeric
- **event** is not empty and doesn't contain |,; and other special characters

Miner - Apply Proof of Lottery and send solution to other miners



Proof of Lottery in nutshell

SHA256(miner_address)

LOTTERY NUMBER (L1)

LOTTERY FUNCTION

WINNING CONDITION

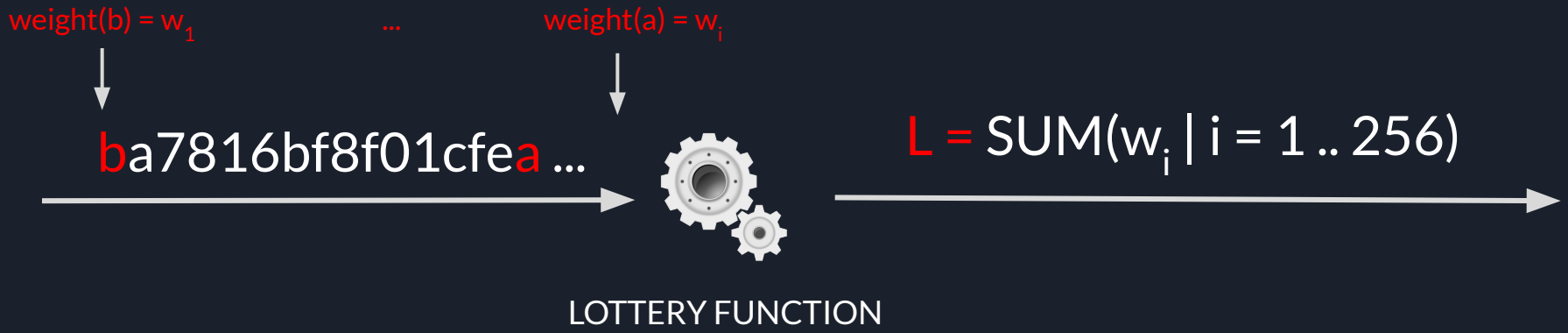
random **seed** such that
L1 = L2

SHA256(block_hash)
block_hash = str(transactions_list + seed)

LOTTERY NUMBER (L2)

LOTTERY FUNCTION

Lottery Function Definition



Proof of Lottery

A notebook is better than 10000 slides:

- https://colab.research.google.com/drive/16ZdbruvQAx86ywlbiMWN7jkjJzaUF1Wv?usp=sharing

Storing in Blockchain if all correct

NOTE:
Each miner attend all notifications of other miners (Miners are fully connected).

If more miners mine the same transactions, the winner is the miner that find the solution with the smallest seed

Let’s see the code

GitHub repository:

- https://github.com/packo97/Blockchain_Project