OWLCOINS

A Hybrid of POS and POW

HELLO!

We are the InvincibleOwls

Afnan Haq

Monplaisir Hamilton

David Nakhapetian

Claudia Rodriguez

1. PROOF OF WORK

> *Proof of work miners compete against each other to complete transactions on the network and get rewarded*

HOW DOES THE PROCESS WORK?

- Miners are responsible for adding new blocks into the blockchain
- The data in the block is passed through a hash function
- If the resulting hash solves the cryptographic puzzle, the miner node is rewarded

PROS & CONS

What's working:

- Defense against DoS attacks.
- Mining possibilities: amount of money does not matter as much as computational power

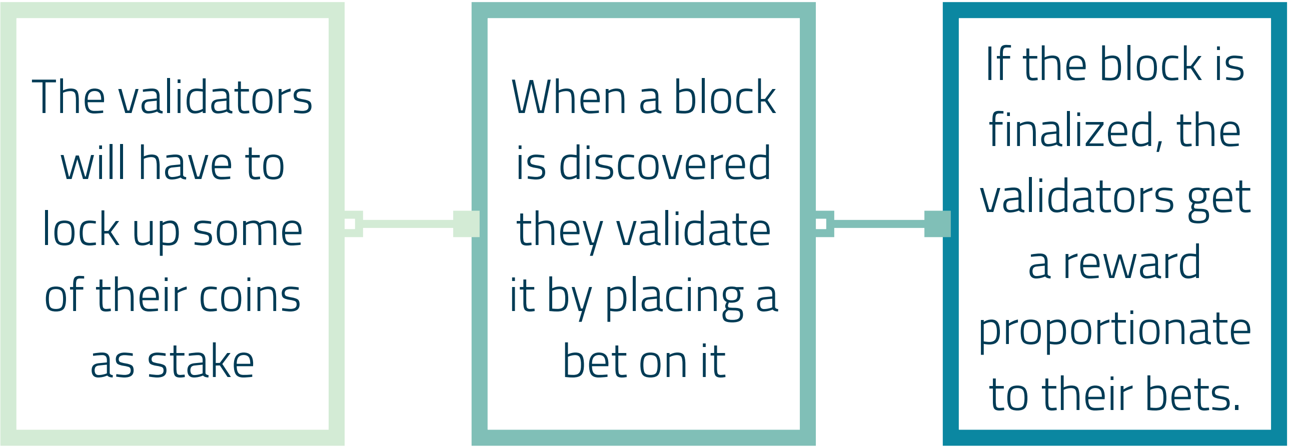
What's not:

- Huge Expenditures: hardware costs a lot of money
- 51% attack: miners monopolize the network
- Reward declines

2.
PROOF OF STAKE

> “Proof of stake will make the entire mining process virtual and replace miners with validators.

HOW DOES THE PROCESS WORK?



The validators will have to lock up some of their coins as stake

When a block is discovered they validate it by placing a bet on it

If the block is finalized, the validators get a reward proportionate to their bets.

PROS & CONS

What's working:

- Voting System: message created, signed and broadcasted.
- Checkpoint System: blocks need to be justified then finalized.

What's not:

- Having justified checkpoints is not enough because 2 conflicting checkpoints can be justified.

3.

IN COMES THE HYBRIDS

Hybrids are a combination of POS and POW

WHAT ARE HYBRIDS?

- Take the pros of both POS & POW
- Try to mitigate their weaknesses
- Exact mechanisms vary between each consensus algorithm

WHERE WE FOUND INSPIRATION

decRED

casper

How Decred Works

- Hybrid consensus mechanism
- Miners mine like other POW protocols
- Validators hold “tickets” until they are randomly chosen to validate

Weakness:

Does not solve electricity problem

Does not solve nothing-at-stake problem

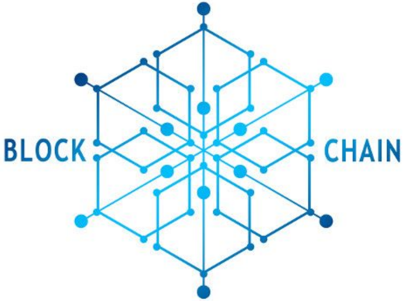
4.

INTRODUCING OWLCOINS

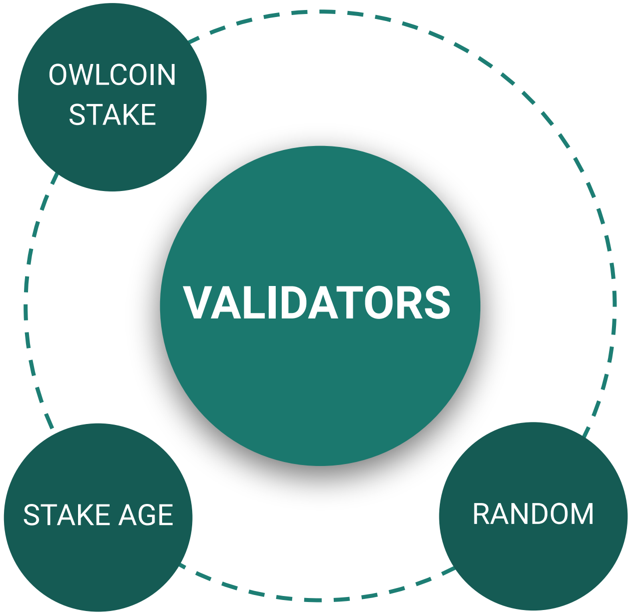
and how it works

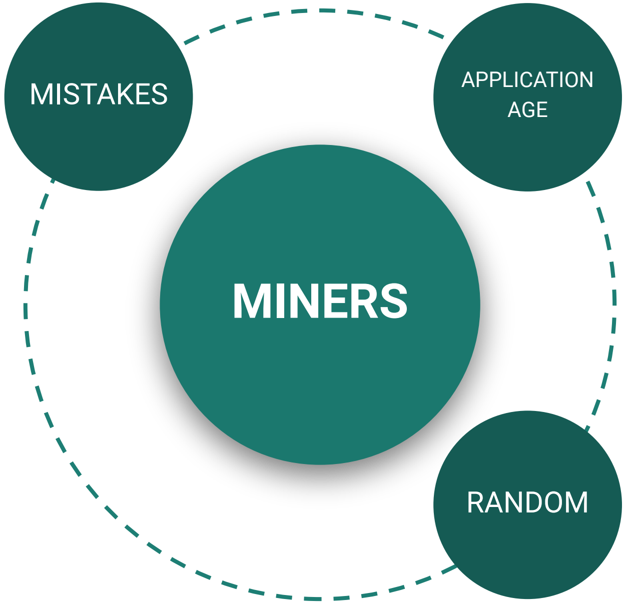
IMPLEMENTING OUR OWN BLOCKCHAIN

- Validators stake OwlCoins into the vault
- Miners apply to get picked for a block
- System receives up to 5 random transactions
- 10 miners, 5 validators



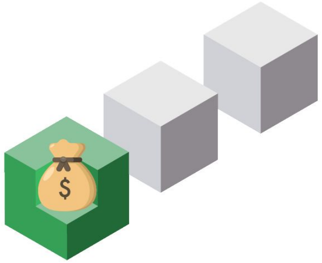
HOW ARE THEY PICKED?





HOW THE BLOCK GETS FINALIZED:

- After miners do POW, miners get added to the queue based on who finished first.
- Validators check miners POW and if it's wrong they discard it and move on.
- Block gets added to the chain if 3/5 of the validators validate the block.



THE BREAKDOWN OF REWARD

5

Minimum entrance fee by validators

50

Total reward

06%

Each Validator

60%

Winning Miner

10%

System

LOSING AND ERROR CHECKING

- If 3 validators approve and 2 do not.
  - 2 lose their stake, and 3 get reward
- If 2 validators approve and 3 do not
  - 2 lose 0.6% of their reward

VISUAL OF VALIDATORS

Block is
NOT VALID

Reward	6	6	6	6	6
Response	Yes	Yes	No	No	No

Block is
NOT VALID

Reward	5.4	5.4	6	6	6
Response	No	Yes	No	No	No

Block is
VALID

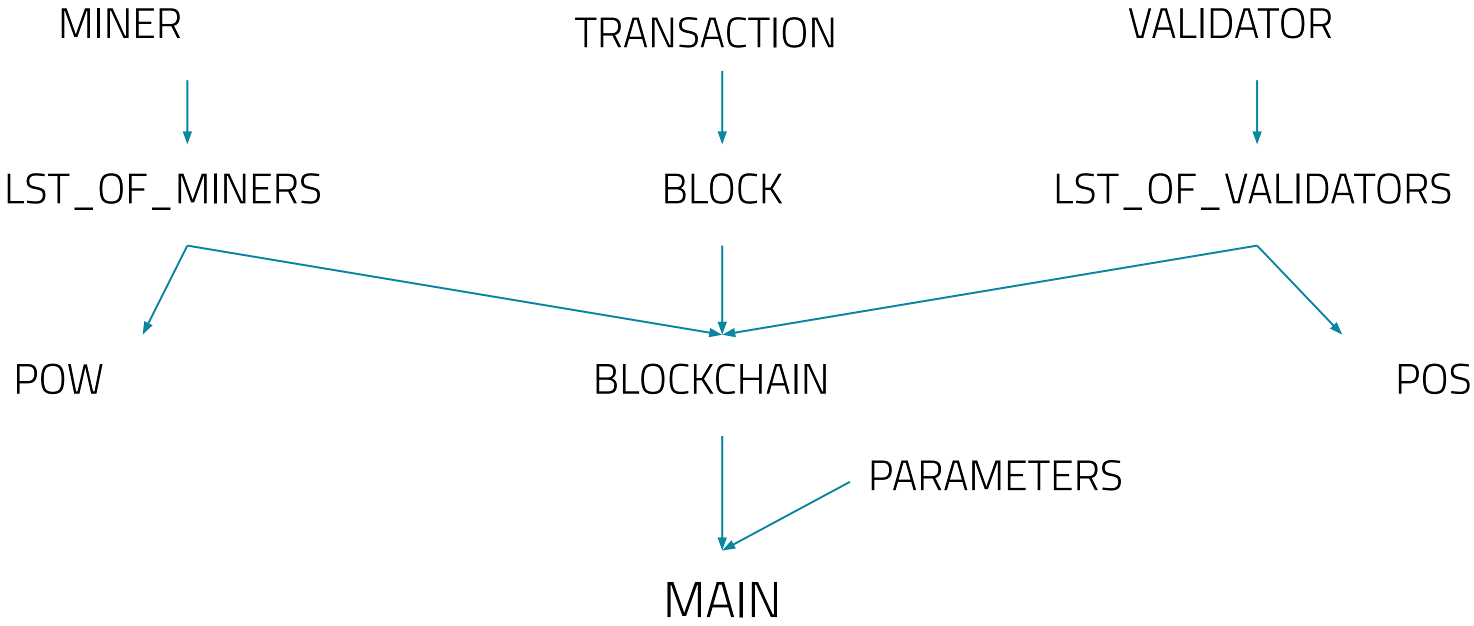
Reward	5.4	4.8	0	6	6
Response	Yes	Yes	No	Yes	Yes

5.

THE CODE

of our implementation

CODE BREAKDOWN



MINER

TRANSACTION

VALIDATOR

LST_OF_MINERS

BLOCK

LST_OF_VALIDATORS

POW

BLOCKCHAIN

POS

PARAMETERS

MAIN

BUILD_NEW_BLOCK

1. Pick 5 validators (weighted random)

2. Pick 10 miners (weighted random)

3. Miners mine and are put into queue

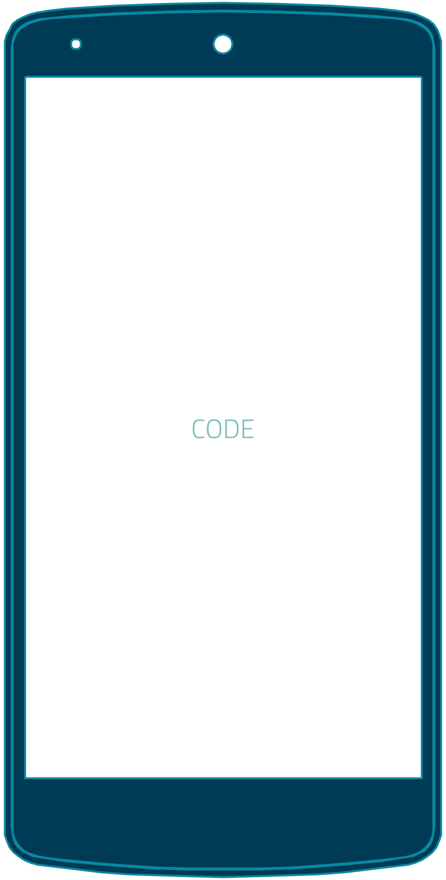
4. While POW does not have consensus:
   a. All validators validate
   b. Slashing operations take place

BUILD_NEW_BLOCK (contd.)

5. Block is added to blockchain

6. Block reward is distributed

7. Clean-up to build next block



CODE

DEMO

ANALYSIS

ADVANTAGES & DISADVANTAGES

- Electricity usage scales
- Safe from 51% attack
- Mining power not important
- Slashing rules apply to validators, no-stake
- Prisoner’s dilemma

- Centralizes system to validators
- Mining GPUs may remain unused

FUTURE

- Online application to be miner or validator
- Build distributed computer system
- Introduce public/private keys to access wallets

THANKS!

Any questions?