NEXT GENERATION CRYPTOCURRENCY:

OUROBOROS

OUROBOROS

Ouroboros White Paper 2019

TABLE OF CONTENTS

INTRODUCTION

Since the emergence of cryptocurrency, there has been a huge anticipation for cryptocurrencies to significantly transform the online payment system and even other aspects of the world.

For this to be fully accomplished, it is necessary for cryptocurrencies to be user-friendly, convenient, and highly scalable.

In this regard, many blockchain-based technologies have been created to tackle the challenges posed by attempting to provide high transaction throughput while remaining inexpensive, but these have been met with little success.

Another challenge faced is the lack of trust between unknown parties, which leads to countless chargebacks and transaction cancellations.

Towards fixing the existing issues, Ouroboros has been designed. Built on Cosmos-SDK and Tendermint, Ouroboros aims to foster the real-life application of digital Assets.

This is a Delegated Proof of Stake (DPOS) cryptocurrency with a few unique features.

OVERVIEW

Ouroboros is a next-generation cryptocurrency that achieves high transaction throughput and low fees while being easy to manage.

We're focused on fast and secure transactions since that's the most important thing for most users.

One of our features is the transaction throughput - the blockchain generates a new block every ~6 seconds, and it can handle up to 1k transactions per second (based on our stress-testing results).

But the most exciting feature is "Posmining" - a blockchain-based technology that generates new coins to your wallet depends on your current balance.

PRIZM introduced the Posmining technology, but unfortunately, the developers made some serious mistakes, and that led to the problems - we have considered all the mistakes of our predecessor and designed both technical and economics parts with keeping their mistakes in mind.

WHAT MAKES IT UNIQUE

Safety: there are always hundreds and thousands of blackhat guys trying to steal your money, but don't worry - your safety is our top priority.

We're using two-factor authentication (Google Authenticator) for our web-wallet version and we conduct security audits through our private bug-bounty program.

Optimal Economic Model: we've developed an optimal economic model that keeps the price stable and high, sp it won't let it down.

Throughput: currently, it takes ~6 seconds to generate a new block, and the blockchain can handle up to 1k transactions per second. It means that your transaction will be confirmed within 12 seconds (max) after sending it.

Democracy: within a few months, we're going to launch a governance module for blockchain-based proposals - it'll allow anyone to add a proposal and vote for it. If the proposal is related to some blockchain settings (max number of validators, for example), the blockchain will automatically update its settings.

Fairness: we strictly follow the principles of justice and honesty - we believe that's the most important thing in the world.

Open source: before the end of this year, we're going to publish all the services under the open-source license - we're totally fine if anyone wants to use it for his purposes or somebody wants to launch a fork. Also, we're going to publish a few examples of how to work with our blockchain per different language (PHP, Python, JS)

POSMINING

Perhaps the most outstanding factor Ouroboros has to offer is its very own creation, Posmining. Mining itself is often a very expensive, inefficient process that is difficult for users as it often requires special hardware and massive amounts of energy.

All Posmining requires is a user having at least 0.1 OURO in their wallet, whereupon additional coins will be Posmined into the wallet.

The speed of extraction of new coins with the help of Posmining is calculated from 3 main parameters: this is the number of coins in your personal wallet, the number of coins on the wallet of your followers at 100 levels in-depth and how many days pass since the latest transaction ("savings multiplier").

Adding somebody to your followers is pretty simple - all you have to do is just send some OURO to a new wallet (that didn't have any transactions yet).

After creating a new wallet, the system captures the first transaction from another wallet (sender) and sets up a permanently referral\follower chain (receiver => sender) that cannot be changed, which makes it easy to build global networks and increase the speed of new coinage.

The Posmining system is the perfect tool for promotion and popularization, as it has no analogs in any modern cryptocurrency. The main advantage of Posmining is that no network user can interfere with this mechanism and falsify new coins; anyone can monitor the number of coins issued by the system.

The savings multiplier is another interesting feature - every 30 days without out coming transactions give you additional posmining multiplier. Incoming and reinvest transactions won't reset your savings multiplier, but any out coming transaction will do that.

COIN ECONOMY

10 MLN.
Initial Emission

8 MLN.
Will Be Realized

2 MLN.
For Covering Expenses

The initial emission is 10 million OURO to the genesis wallet, 8 million will be realized through the cryptocurrency exchanges.

We aren't making any presales or suspicious direct sales to someone - every coin transfer from the genesis wallet could be checked via the blockchain explorer.

We're going to keep 2 million coins on the genesis wallet - they'll be used for covering marketing and development expenses.

7.53 BLN.

The final emission: after reaching that threshold, the paramining will stop working for everyone. We're going to update that number every year based on the earth population number (from the official United Nation report).

For the personal wallets, the paramining will stop working after getting 2 million coins to the balance.

SCC

The algorithm for correcting the growth of coins SCC-Smart Correction Coin.

Depending on the value of the coin on the market - once every 100 blocks, the blockchain requests price data from public sources, updating the speed of coin mining.

POSMINING CALCULATIONS

The posmining speed is calculated from 3 main parameters: this is the number of coins in your personal wallet, the number of coins on the wallet of your followers and how many days since the latest transaction.

FOR EXAMPLE:

You have 1000 OURO in your wallet (0.09% per day), your followers have 1000 coins (followers multiplier is 2.18), and you didn't send any transaction in the last 30 days (savings multiplier is 1.5).
Based on that, you'll be getting (0.09% * 1.5) * 2.18 = 0.29% or 2.9 OURO every day.
So after a month (30 days) you'll get 2.9 * 30 = 87 OURO to your wallet.

Your Personal Balance

Number of coins in a wallet	Growth per day, %
500.000 to 1.000.000	0.16
100.000 to 499.999	0.14
50.000 to 99.999	0.12
10.000 to 49.999	0.10
1000 to 9999	0.09
100 to 999	0.07
0.1 to 99	0.06

SCC - Smart Correction Coin

This regulation algorithm will control the issue of new coins preventing a glut of coins in the market excluding hyperinflation.

The coefficients of regulation:

~	Price	Regulation %
> =	1$	speed doesn't change
0.75 -	0.99$	speed is reduced -20%
0.5 -	0.75$	speed is reduced -40%
0.2 -	0.5$	speed is reduced -60%
$ <	0.2$	speed is reduced -80%

Your Followers Balance

Number of coins	Followers Multiplier
1.000.000.000	4,37
100.000.000 to 999.999.999	3,88
10.000.000 to 99.999.999	3,36
1.000.000 to 9.999.999	3,05
100.000 to 999.999	2,77
10.000 to 99.999	2,36
1000 to 9999	2,18

Days Since Last Transaction

Days Since	Savings Multiplier
360	2
180	1.55
150	1.54
120	1.53
90	1.52
60	1.51
30	1.50

COSMOS и Tendermint

We chose the Cosmos-SDK as the framework for developing our blockchain.

The main goal of Cosmos is to create an "Internet of Blockchains" that will allow many easy-to-develop blockchains to scale and interact with each other on the basis of Cosmos-Hub.

For this purpose, the Cosmos-SDK was developed, which is one of the most convenient frameworks for blockchain development at the moment.

Cosmos uses Tendermint because it is very efficient and uses a more Mature solution to the problem of Byzantine generals (BFT).

Cosmos uses proof-of-stake, which means there is no need to buy low-cost equipment and huge electricity costs for block validation. However, Cosmos uses a slightly different approach from the classic proof-of-stake approach inherited from Tendermint.

Tendermint is a software solution for safely reproducing the application state on multiple machines.

Secure means that even if 1\3 of all machines are compromised, Tendermint will work.

The ability to continue working when machines fail (in case they were compromised or as a result of an error) is a solution to the classic problem of Byzantine generals (Byzantine fault tolerance, BFT). The idea behind BFT has been known for several decades, but interest in it only increased after the advent of blockchain.

In General, Blockchain technology is nothing more than BFT with an emphasis on cryptography and p2p networks. Tendermint consists of two main components - the Tendermint Core and the Application Blockchain Interface (ABCI).

Tendermint Core is responsible for managing the state of the blockchain, achieving consensus, validating transactions and blocks, reading and returning the state of the blockchain through a specially created socket Protocol.

ABCI provides developers with an interface for interacting with the blockchain, which allows integrating applications written in any programming language.

More detailed Cosmos и Tendermint.

GENERATING A BLOCK

One of the key features of Ouroboros is the limited number of " validators " who participate in making decisions about blocks - at the moment, Ouroboros allows no more than 100 validators.

This restriction allows generating blocks fairly quickly (on average every 5-10 seconds), because a small number of validators allows all participants to exchange information quickly enough.

Each validator has a "voting power" parameter, which is determined by how many coins the validator has put on the stack (proof-of-stake). the more coins the validator risks in case of an attempt to cheat (cutting coins for incorrect behavior is called slashing), the more important his vote is.

Before starting to select a new block, a special algorithm selects one of the validators as a" proposer", depending on the significance of the validator's voice - the higher this parameter, the more likely it is to be selected by the proposer.

The circular block selection algorithm looks like this:

NewHeight -> (Propose -> Prevote -> Precommit)+ -> Commit -> NewHeight ->...

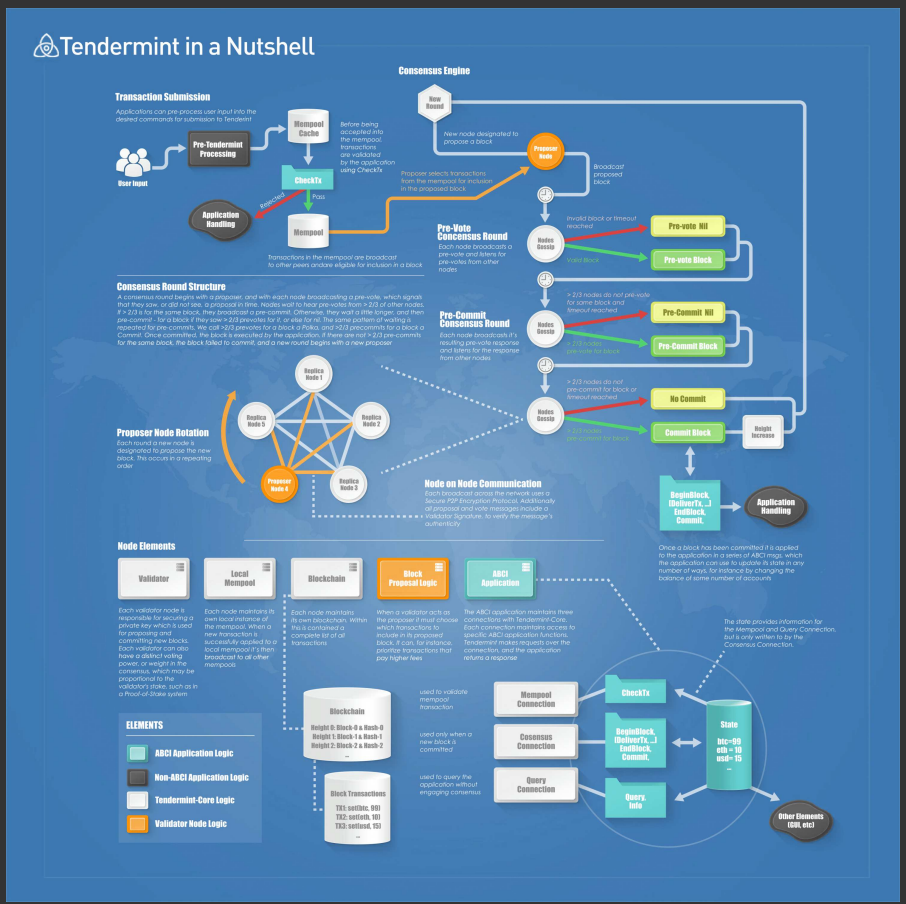
The proponent signs and offers the block for voting (propose), after which the other validators vote for it (prevote). If a block receives at least 2\3 votes on Pre-commit, the process goes to Commit and is added to the blockchain, after which everything starts over again.

GENERATING BLOCK

(Propose - > Private -> Pre commit)+ is called a round. block validation may require more than 1 round, in cases where:

- The selected proposer is not online.
- The block selected by the proposer is invalid.
- Received less than 2\3 votes from other validators by the time the algorithm reached Precommit

If the round was unsuccessful, a new proposer will be selected and the algorithm will be repeated until the block is selected.



Detailed article from Tendermint on this topic

VALIDATORS

Validators are nodes with a vote value greater than zero (coins placed on the stack) that participate in the decision-making process regarding the next block using their own cryptographic signatures (votes).

Any node can become a validator, but for the effectiveness of the blockchain, the top 100 nodes by the number of coins placed on the stack become validators.

To solve the problem of malicious behavior of validators (nothing-at-stake, generating fake transactions), the concept of slashing was introduced - the essence is that malicious behavior leads to the loss of coins placed on the stack.

Did the validator suggest a fake transaction? Loses coins.

The validator node has fallen and is not involved in block selection for some time? Loses coins.

Therefore, with nothing-at-stake, the validator who made fork #2 loses coins in fork #1 and the whole idea loses meaning. Responsibility for missed votes leads to the fact that the validator is interested in supporting the infrastructure and 100% uptime of its node.

After the launch of the blockchain, we will publish a detailed guide on how to protect your node from ddos attacks as much as possible and build an infrastructure - thanks to the Games of Stakes held by Cosmos in the test network, the community has implemented many useful tools for monitoring and protecting nodes.

Other network participants can participate in the process of selecting a validator, and share the risks and rewards of validation with it.for this purpose, there is a "Delegator"role.

DELEGATES

Any network user who has at least 1 OURO in their wallet can become a delegate.

Delegates "delegate" their tokens to validators, thereby voting for them and adding their coins to the validator stack.

When a validator receives a reward for a block, it shares it with all the delegates who have contributed their coins to its stack.

If the validator does something malicious and their coins are cut, the delegates ' coins are also cut, so you need to be careful in choosing validators and delegate coins only to those whose integrity you are sure of.

The delegator can take their coins back from the stack at any time, so validators are interested in bona fide behavior for their personal benefit.

This division of roles and" skin on the line allows all users of the blockchain to regulate it. If a validator loses the trust of the community, it is enough to remove him from the role of a validator, taking all the delegated coins, and find someone else to trust.

Becoming a delegate will be available from the official wallet and via the console interface. We are well aware that the reward for delegates is less than the profit from paramining, but we decided to leave this mechanism for the settlement of the blockchain and the ability to resist possible" cartels of validators.

ADDITIONAL MATERIALS

https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md

https://allquantor.at/blockchainbib/pdf/buchman2016tendermint.pdf

https://tendermint.com/docs/spec/consensus/consensus.html

https://medium.com/coinmonks/deep-dive-into-cosmos-tendermint-cf5bff5cb0c