

NEXT GENERATION
CRYPTOCURRENCY:
OUROBOROS



OUROBOROS

Ouroboros White Paper 2019

TABLE OF CONTENTS



Page 3
About the Project



Page 5
Paramining



Page 6
Coin Economy



Page 7
Paramining Calculations



Page 9
Additional Materials



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 "Paramining" - a blockchain-based technology that generates new coins to your wallet depends on your current balance.

PRIZM introduced the Paramining 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, so 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)



PARAMINING

Perhaps the most outstanding factor Ouroboros has to offer is its very own creation, Paramining. 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 ParaMining requires is a user having at least 0.1 OURO in their wallet, whereupon additional coins will be ParaMined into the wallet.

The speed of extraction of new coins with the help of Paramining 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 Paramining system is the perfect tool for promotion and popularization, as it has no analogs in any modern cryptocurrency. The main advantage of Paramining 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 outgoing transactions give you additional paramining multiplier. Incoming and reinvest transactions won't reset your savings multiplier, but any outgoing 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.

**Final
Emission**

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.

PARAMINING CALCULATIONS

The paramining 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

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

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>