

КРИПТОВАЛЮТА  
НОВОГО ПОКОЛЕНИЯ:  
**OUROBOROS**



**OUROBOROS**

*Ouroboros White Paper 2019*

# ОГЛАВЛЕНИЕ



**Страница 3**  
О Проекте



**Страница 5**  
Парамайнинг



**Страница 6**  
Экономика проекта



**Страница 7**  
Таблицы Парамайнинга



**Страница 9**  
Технические детали



# ВСТУПЛЕНИЕ

С момента появления первой криптовалюты, весь мир ожидает существенного изменения систем онлайн-платежей в нашей повседневной жизни.

Для реализации этого, криптовалюты должны быть просты в использовании, безопасны и легко масштабируемы.

В связи с этим, был создан ряд технологий для решения проблемы обеспечения высокой пропускной способности транзакций, но все они сталкивались с проблемами и так и не вошли в нашу жизнь.

Другой проблемой является отсутствие доверия между неизвестными сторонами, что приводит к бесчисленным проблемам с подтверждением и отменой транзакций.

Для решения существующих проблем был разработан Ouroboros - Ouroboros, созданный на базе Cosmos SDK и Tendermint, стремится содействовать применению цифровых активов в реальной жизни.

Это Delegated Proof of Stake (DPOS) криптовалюта с уникальными преимуществами.

---

## ОБЗОР OUROBOROS

Ouroboros - это DPOS криптовалюта следующего поколения, созданная на базе Cosmos-SDK и Tendermint, которая обеспечивает высокую пропускную способность транзакций при низкой комиссии и простоте в управлении.

Мы сфокусированы на быстрых и безопасных транзакциях, которые являются ключевым моментом для большинства пользователей криптовалют.

Важным фактором является пропускная способность блокчейна - в среднем, генерация одного блока занимает ~5 секунд и по результатам стресс-тестинга мы можем гарантировать обработку минимум 1 тысячи транзакций в секунду.

Однако по-настоящему уникальным Ouroboros делает Парамайнинг — механизм, генерирующий новые монеты основываясь на монетах в кошельке пользователя.

Впервые, механизм парамайнинга появился в криптовалюте PRIZM - мы внимательно наблюдали за развитием этой криптовалюты и учли все ошибки в технической составляющей и экономической модели при разработке Ouroboros.

# ПРЕИМУЩЕСТВА



**Безопасность:** вокруг любого популярного проекта собираются десятки хакеров и мошенников, поэтому безопасность является нашим главным приоритетом.

Для официального кошелька мы используем двухфакторную аутентификацию через Google Authenticator и проводим аудит информационной безопасности всех наших проектов через частную bug bounty программу.



**Эффективная экономическая модель:** для обеспечения устойчивости курса и избежания инфляции, мы разработали эффективную экономическую модель, которая учитывает неудачный опыт наших предшественников.



**Пропускная способность:** наша минимальная планка составляет 1 тысячу транзакций в секунду и 5 секунд в среднем на генерацию одного блока. Таким образом, ваша транзакция будет гарантировано подтверждена в течение 10 секунд (максимум) с момента отправки.



**Демократия:** наследованная от Cosmos система голосования реализует по-настоящему демократический подход — любой пользователь может вынести на голосование любое изменение в системе.



**Честность и открытость:** мы считаем это ключевыми качествами, необходимыми для развития проекта - мы уведомляем пользователей о всех наших планах через официальные каналы и обсуждаем с комьюнити решения, прежде чем реализовывать их.



**Open source:** исходный код всех проектов будет выложен на Github под open source лицензией — мы не против форков или новых криптопроектов на базе нашей. Так же, на Github будут выложены несколько примеров с интеграцией нашего блокчейна, чтобы облегчить разработчикам задачу реализации сервисов.



# ПАРАМАЙНИНГ

Парамайнинг является одной из самых интересных особенностей, которую может предложить Ouroboros - классический майнинг, приносящий прибыль, зачастую является крайне дорогим и неэффективным процессом, недоступным большинству.

В свою очередь, всё, что требуется для Парамайнинга - наличие в кошельке хотя бы 1 OURO, при котором запускается процесс парамайнинга дополнительных монет прямо в кошелек.

Рост количества монет при парамайнинге зависит от трех факторов: кол-во монет в кошельке пользователя, кол-во монет в кошельках последователей (в глубину на 100 уровней) и время, прошедшее с последней транзакции (так называемое "накопление"). После создания нового кошелька, система записывает нового пользователя в "последователи" отправителя первой полученной им транзакции и устанавливает между ними постоянную связь, которая не может быть изменена в будущем.

Таким образом, привлекая новичков в проект и отправляя им монетку для активации, любой пользователь может собрать структуру последователей и увеличить скорость парамайнинга собственных монет.

Функционал "накопления" является уникальным преимуществом Ouroboros, созданным для мотивирования пользователей накапливать монеты - в случае, если с момента последней исходящей транзакции прошло 30 или больше дней, включается механизм накопления, который увеличивает ежедневный процент парамайнинга в зависимости от кол-ва дней с момента последней транзакции.

При отправке монет, счетчик накопления сбрасывается, однако это не касается реинвеста.

Парамайнинг может быть получен двумя способами: отправкой транзакции любому пользователю или при помощи функционала "реинвеста", который доступен из официального кошелька и через консольную оболочку.



# ЭКОНОМИКА

**10 МЛН.**

**Начальная  
Эмиссия**

**8 МЛН.**

**Будет  
продано**

**2 МЛН.**

**Останется у  
создателей**

Первоначальная эмиссия - 10 миллионов OURO на генезис кошельки, 8 миллионов из которых будут проданы через официальные криптобиржи.

Мы не проводим никаких presale и не совершаем никаких подозрительные продажи в прямые руки - все переводы монет можно будет отследить через blockchain explorer.

2 миллиона монет будут оставлены на генезис кошельке для оплаты маркетинг-компаний и разработки сервисов в экосистеме Ouroboros.

**7.53 млрд.**

**Конечная  
Эмиссия**

Конечная эмиссия, при которой парамайнинг остановится, зависит от населения Земли и будет обновляться каждый год на основании данных ООН.

Для персональных кошельков, парамайнинг останавливается при достижении баланса в 2 млн. монет.

# ФАКТОРЫ ПАРАМАЙНИНГА

На рост количества монет влияют 3 фактора - монеты в личном кошельке, монеты в кошельках последователей и количество дней с момента последней транзакции (накопление).

## НАПРИМЕР

У вас в кошельке 1000 монет (0.09% в день), в кошельках ваших последователей 1000 монет (2.18 повышающий коэффициент) и вы не отправляли транзакции более 30 дней (1.5 дополнительный коэффициент).

В результате, ваш доход с парамайнинга будет  $(0.09\% * 1.5) * 2.18 = 0.29\%$  или 2.9 OURO в день.

Таким образом (без учета реинвестирования) за 30 дней вы заработаете  $2.9 * 30 = 87$  OURO.

## Монеты в личном кошельке

Кол-во монет в личном кошельке	Рост кол-ва монет в день, %
500.000 до 1.000.000	0.16
100.000 до 499.999	0.14
50.000 до 99.999	0.12
10.000 до 49.999	0.10
1000 до 9999	0.09
100 до 999	0.07
1 до 99	0.06

## Монеты в кошельках последователей

Кол-во монет последователей	Повышающий коэффициент
1.000.000.000	4,37
100.000.000 до 999.999.999	3,88
10.000.000 до 99.999.999	3,36
1.000.000 до 9.999.999	3,05
100.000 до 999.999	2,77
10.000 до 99.999	2,36
1000 до 9999	2,18

## Дней с момента последней транзакции

Дней	Дополнительный коэффициент
360	2
180	1.55
150	1.54
120	1.53
90	1.52
60	1.51
30	1.50



# COSMOS и Tendermint

Мы выбрали Cosmos-SDK в качестве фреймворка для разработки нашего блокчейна.

Основной целью Cosmos является создание "Интернета Блокчейнов", который позволит многим простым в разработке блокчейнам масштабироваться и взаимодействовать друг с другом на базе Cosmos-Hub.

Для этого, был разработан Cosmos-SDK, который является одним из самых удобных фреймворков для разработки блокчейна на текущий момент.

Cosmos использует Tendermint, поскольку он очень эффективен и использует более зрелое решение проблемы византийских генералов (BFT).

Cosmos использует proof-of-stake, что означает отсутствие необходимости в покупке дорогостоящего оборудования и гигантских затрат электроэнергии на валидацию блоков. Тем не менее, Cosmos использует немного отличный от классического proof-of-stake подход, наследованный с Tendermint.

Tendermint - это программное решение для безопасного воспроизведения состояния приложения на множестве машин.

Под безопасным подразумевается, что даже при компрометации  $1/3$  всех машин, Tendermint будет работать.

Возможность продолжать работу при сбое машин (в случае, если они были скомпрометированы или в результате ошибки) является решением классической задачи византийских генералов (Byzantine fault tolerance, BFT). Идея, лежащая в основе BFT, известна уже несколько десятилетий, но интерес к ней возрос только после появления блокчейна.

В целом, технология Blockchain - это не что иное, как BFT с акцентом на криптографию и p2p-сети. Tendermint состоит из двух главных компонентов - Tendermint Core и Application Blockchain Interface (ABCI).

Tendermint Core ответственен за управление состоянием блокчейна, достижение консенсуса, валидацию транзакций и блоков, чтение и возвращение состояния блокчейна через специально созданный socket протокол.

ABCI представляет разработчиками интерфейс для взаимодействия с блокчейном, что позволяет интегрировать приложения, написанные на любом языке программирования.

[Подробнее о Cosmos и Tendermint.](#)

# ГЕНЕРАЦИЯ БЛОКА

Одной из ключевых особенностей Ouroboros является ограниченное количество "валидаторов", которые участвуют в принятии решений относительно блоков - на текущий момент, Ouroboros разрешает не более 100 валидаторов.

Это ограничение позволяет генерировать блоки достаточно быстро (в среднем каждые 5-10 секунд), т.к. малое количество валидаторов позволяет всем участникам достаточно быстро обмениваться информацией.

У каждого валидатора есть параметр "значимость голоса" (voting power), который определяется тем, сколько монет поставил на стек (proof-of-stake) валидатор - чем большим количеством монет валидатор рискует в случае попытки обмана (урезание монет при некорректном поведении называется slashing), тем большую значимость имеет его голос.

Перед началом выбора нового блока, специальный алгоритм выбирает одного из валидаторов в качестве "предлагающего" (proposer), в зависимости от значимости голоса валидатора - чем этот параметр больше, тем больше вероятность быть выбранным предлагающим.

Круговой алгоритм выбора блока выглядит следующим образом:

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

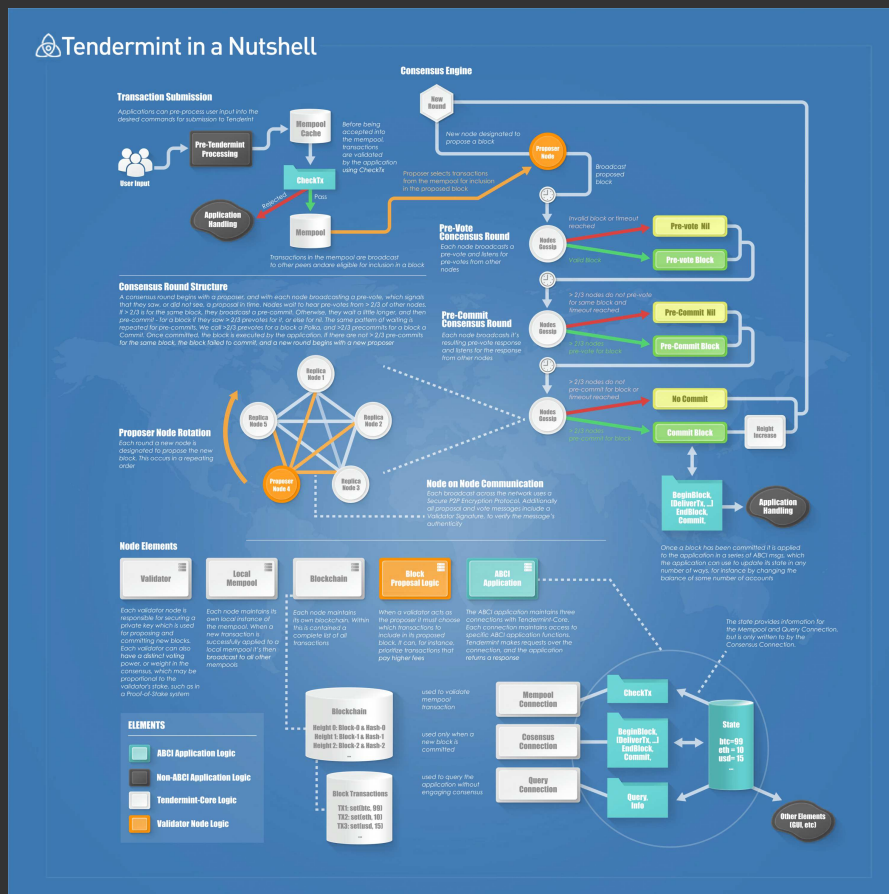
Предлагающий подписывает и предлагает на голосование блок (propose), после чего другие валидаторы голосуют за него (prevote). В случае, если на Precommit блок получает хотя бы  $\frac{2}{3}$  голосов, процесс переходит в Commit и добавляется в блокчейн, после чего начинается всё повторяется сначала.

# ГЕНЕРАЦИЯ БЛОКА

(Propose -> Prevote -> Precommit)+ называется раундом, для валидации блока может потребоваться больше, чем 1 раунд, в случаях когда:

- Выбранный proposer не в сети.
- Выбранный proposer-ом блок невалиден.
- Поступило меньше 2/3 голосов от других валидаторов к тому времени, как алгоритм дошел до Precommit

В случае, если раунд прошел неудачно, будет выбран новый proposer и алгоритм будет повторяться до тех пор, пока блок не будет выбран.



Подробная статья от Tendermint на эту тему

# ВАЛИДАТОРЫ

Валидаторами называют ноды со значимостью голоса более нуля (монетами, поставленными на стек), которые участвуют в процессе принятия решения относительно следующего блока при помощи собственных криптографических подписей (голосов).

Любая нода может стать валидатором, однако для эффективности работы блокчейна валидаторами становятся топ-100 нод по кол-ву поставленных на стек монет.

Для решения проблемы злонамеренного поведения валидаторов (nothing-at-stake, генерация фальшивых транзакций) был введен концепт slashing - суть в том, что злонамеренное поведение приводит к потере монет, поставленных на стек.

Валидатор предложил фальшивую транзакцию? Теряет монеты.

Нода валидатора упала и какое-то время не участвует в выборе блока? Теряет монеты.

Поэтому, при nothing-at-stake валидатор, сделавший форк #2, теряет монеты в форке #1 и вся затея теряет смысл.

Ответственность за пропущенные голосования приводит к тому, что валидатор заинтересован в поддержке инфраструктуры и 100% uptime своей ноды.

После запуска блокчейна, мы опубликуем детальный гайд на тему того, как максимально обезопасить свою ноду от ddos атак и построить инфраструктуру - благодаря Games of Stakes, проводимые Cosmos в тестовой сети, комьюнити реализовало множество полезных инструментов для мониторинга и защиты нод.

Другие участники сети могут участвовать в процессе выбора валидатора, и разделять с ним риски и награду за валидацию - для этого существует роль "Делегатор".

# ДЕЛЕГАТОРЫ

Делегатором может стать любой пользователь сети, имеющий хотя бы 1 OURO в кошельке.

Делегаторы "делегируют" свои токены валидаторам, тем самым голосуя за них и добавляя свои монеты к стеку валидатора.

Когда валидатор получает награду за блок, он разделяет ее со всеми делегаторами, которые внесли свои монеты в его стек.

В случае, если валидатор совершает что-то злонамеренное и его монеты урезаются, монеты делегаторов так же урезаются, поэтому необходимо быть аккуратными в выборе валидаторов и делегировать монеты только тем, в чьей добросовестности вы уверены.

Делегатор в любой момент может забрать свои монеты обратно из стека, поэтому валидаторы заинтересованы в добросовестном поведении в силу своей персональной выгоды.

Такое разделение ролей и "шкура на кону" позволяют всем пользователям блокчейна регулировать его - в случае, если какой-то валидатор теряет доверие комьюнити, достаточно просто убрать его с роли валидатора, забрав все делегированные монеты, и найти кого-то другого, кому можно будет доверять.

Становление делегатором будет доступно из официального кошелька и через консольный интерфейс - мы прекрасно понимаем, что награда делегаторов меньше прибыли с парамайнинга, однако мы решили оставить этот механизм для урегулирования блокчейна и наличия возможности противостоять возможным "картелям" валидаторов.

# ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ

<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>