



ШМІ

Универсальный денежный
инструмент

Содержание

- 3 Введение.
- 4 Основные технические особенности.
- 6 Алгоритм консенсуса и ноды.
- 7 Блоки.
- 8 Адреса.
- 10 Транзакции.
- 15 База данных PostgreSQL (node-master).
- 16 Подпись сообщения.
- 16 Функция `umi_get_balance`.
- 16 Запуск ноды.
- 17 Смарт-контракт по стейкингу.
- 20 Ссылки.

Введение

UMI — универсальный денежный инструмент. Децентрализованная криптовалюта, позволяющая совершать практически мгновенные, бесплатные и максимально безопасные переводы.

Это разработанная с нуля полноценная блокчейн-платформа, умеющая создавать и исполнять смарт-контракты, работающая на основе мастер-нод и уникальной модели Proof-of-Authority.

UMI — единственная криптовалюта, которая использует технологию стейкинга на смарт-контракте, позволяя участникам сети объединяться в структуры и увеличивать количество монет до 40% в месяц, просто держа их в своем кошельке.

Yellowpaper содержит исключительно техническую информацию о децентрализованной криптовалюте UMI. Здесь собраны подробные сведения о том, как работает код сети и смарт-контракта по стейкингу.

Если вы хотите изучить преимущества, особенности и цели UMI — ознакомьтесь с Whitepaper: umi.top/about.

Основные технические особенности

- При запуске сети создано 18 000 000 монет UMI. Все последующие монеты создаются исключительно посредством стейкинга внутри смарт-контракта.
- В каждый блок помещается 65535 транзакций. Новые блоки генерируются примерно раз в 15 секунд, что обеспечивает пропускную способность сети более 250 000 транзакций в минуту.
- Стандартные адреса в сети начинаются с префикса «umi» и содержат 62 символа (формат Bech32). Пример адреса:
`umi1qqqumpt2jchfa63qc0jxztud75x89ya49h58sw34hdls8kl3a60cl4qmrfr`.
Адреса внутри структур (смарт-контракт по стейкингу) начинаются с другого префикса, в зависимости от настроек структуры.
- Адрес кошелька генерируется с помощью мнемонической seed-фразы (256-bit), которая представляет собой случайный ряд слов. Например:
`water prize useless put surface laundry neck because expire sing dawn digital salon nerve timber fog caution squirrel banner age repeat column venture meadow`
- Хэш/ID транзакций (TxID) состоит из 64 символов и содержит цифры от 0 до 9, а также латинские буквы от «a» до «f». Пример транзакции:
`6c30a24bcb33d540739dade880e98f9d18b12dc6f411fef715f748600b77b`.
- Каждая монета UMI делится на сотые, как фиатные валюты, а не на 100-миллионные, как биткоины. Таким образом, минимальная величина — 0,01 UMI.
- UMI не является стейблкоином. Курс монеты не привязан к USD или какой-то другой валюте.
- UMI — полностью самостоятельная монета с собственным блокчейном.
- Блокчейн сети открыт и доступен для публичного просмотра через специализированные блокчейн-эксплореры.
- Все транзакции псевдо-анонимны. Они не анонимны, потому что адреса и суммы видны всем в целях обеспечения прозрачности.
- В сети не используется файл «wallet.dat» и отсутствует необходимость хранить что-либо в электронном виде.
- Для обеспечения защиты сети от злонамеренного флуда и DDoS-атак UMI использует модель безопасности по принципу PoW, позволяющую работать без комиссий. Чтобы отправить транзакцию в сеть, устройству требуется совершить небольшую математическую операцию.
- Дерево Меркла, API- и SDK-инструменты упрощают и ускоряют процесс подтверждения

транзакций сторонними платежными шлюзами, обеспечивая интеграцию с существующими платежными системами, обменниками и биржами криптовалют.

- Легкая масштабируемость: увеличить размер блока или внедрить какую-либо разработку можно без хардфорков и угроз для сети.
- Блокчейн-платформа UMI позволяет создавать различные смарт-контракты и является многофункциональной. Например, с ее помощью можно выпускать стейблкоины с мгновенной конвертацией прямо через кошелек.
- Сеть UMI использует технологию стейкинга на смарт-контракте в качестве модели стимулирования пользователей.
- Исходный код сети и смарт-контракты выложены на самый популярный в криптосообществе репозиторий GitHub: www.github.com/umi-top.

Алгоритм консенсуса и ноды

UMI использует алгоритм Proof-of-Authority на основе мастер-нод и нод-валидаторов (нод-верификаторов). Нода, или узел, в сети UMI — устройство со специальным программным обеспечением. Ноды проверяют транзакции (ноды-валидаторы), создают блоки и отправляют их в сеть (мастер-ноды).

UMI имеет три базовых реализации ноды: мастер-нода, нода-верификатор и легкая нода:



В мастер-ноде реализован полный функционал. Блокчейн хранится в бинарном виде в файлах на дисках, а текущее состояние всех балансов сохраняется в PostgreSQL.



Нода-верификатор не имеет возможности создавать и публиковать новые блоки. Блокчейн хранится в бинарных файлах на диске, а текущее состояние сохраняется во встраиваемой базе данных BadgerDB (аналог LevelDB).



Легкая нода не сохраняет блокчейн на диск, проксирует запросы к полным нодам сети и валидирует ответы.

Блоки

Учет транзакций в сети UMI осуществляется посредством цепочки из неразрывно связанных между собой блоков информации. Это основа блокчейн-технологии и надежный способ хранения данных, который представляет собой цифровой реестр всех транзакций, проведенных в сети UMI. Реестр защищен от несанкционированного доступа и не может быть изменен.

Блокчейн-цепочка постоянно растет в объеме — по мере того, как ноды добавляют в нее новые блоки с проведенными транзакциями. Блоки сохраняются в цепочке в линейном последовательно-хронологическом порядке.

Информация обо всех транзакциях в сети сохраняется в блокчейне с учетом порядка их проведения. Также в блокчейне хранится вся информация об адресах и балансах, начиная с первичного блока — genesis-блока — и до самого последнего добавленного в сеть.

Технически в блок помещается 65535 транзакций суммарным весом около 9 МБ. Блок генерируется в среднем раз в 15 секунд.

Каждый блок содержит набор обязательных параметров:

- Временную метку блока;
- Хеш предыдущего блока;
- Количество транзакций в блоке;
- Информацию по всем транзакциям внутри блока, включая идентификационные номера транзакций;
- Цифровую подпись и публичный ключ ноды (генератора блока).

При генерации нового блока нода ставит криптографическую подпись с публичным ключом. Каждый блок имеет цифровую подпись с использованием криптографически безопасного алгоритма хеширования SHA256.

Адреса

Информация обо всех публичных адресах хранится в сети UMI, а приватные ключи генерируются непосредственно из кодовых фраз.

Формат адресов

Базовый адрес UMI имеет длину 34 байта. Первые два байта отвечают за формат адреса, последующие 32 байта - публичный ключ. На данный момент доступны два типа адресов:

0x00 0x01 — основной токен.

0x00 0x02 — токен смарт-контракта.

Для удобства пользователей адреса закодированы в Besh32 и имеют тег umi.

Тэг никак не влияет на адрес и может использоваться, например, для удобного визуального разделения токенов.

Пример: Токен с префиксом 0x00 0x02 может иметь как тег `imi` так, и, например, тег `mzx`, соответственно, одному реальному адресу будут соответствовать два представления:

`umi1ggggsqqgggggggggggggggggggggggggggggggggggggggggggggu8hk5k`

mzx1qqqqsqqre36qv

Версии адресов

Genesis	Существует только в genesis-блоке
UMI	Базовый адрес. Токены на балансе не увеличиваются, нет ограничений на перевод на другие адреса.
FST (префикс структуры, название «FST» взято для примера)	Смарт-контракт. Баланс кошелька подчиняется правилам структуры «FST», к которой он принадлежит.

Специальные типы адресов внутри структуры

Dev	Начисляются повышенные проценты пропорционально балансу структуры. Автоматически создается и привязывается при создании новой структуры. Не учитывается в общем балансе структуры. Нет ограничений на переводы внутри структуры. При переводе с UMI на dev не начисляется комиссия. Менять нельзя.
Master	Адрес, имеющий право изменять настройки структуры. Подчиняется общим правилам структуры. Привязывается при создании структуры. Менять нельзя. Имеет право изменять настройки структуры.
Profit	Адрес с повышенным коэффициентом, пропорциональным балансу структуры. Не учитывается в балансе структуры, но баланс структуры учитывается при расчете начислений. Нет ограничений на перевод внутри структуры. С помощью master-адреса можно назначить новый Profit-адрес.
Fee	Адрес для автоматического перевода комиссии. Повышенный процент. Нет ограничений на переводы внутри структуры. Не учитывается в общем балансе. С помощью master-адреса можно назначить новый Fee-адрес.
Transit	Нет ограничений для переводов внутри структуры. При переводе не взимается комиссия. Master-адрес может создавать неограниченное количество Transit-адресов. Активировать и деактивировать адрес можно только один раз.

Транзакции

За исключением стейкинга, транзакции — это единственная возможность для адресов UMI изменять состояние своих балансов. Каждая транзакция выполняет одну функцию, информация о ней сохраняется в сети навсегда с момента включения ее в блок.

Благодаря общедоступности записей в блокчейне, с помощью публичных средств просмотра можно легко проверить транзакции, которые проводились на конкретном адресе. К примеру, в собственном кошельке вы увидите все транзакции, которые когда-либо совершали в сети UMI — от первой до последней.

В сети UMI отсутствуют комиссии за внутренние транзакции. Без исключений даже для случаев, когда происходит чрезмерно большой объем транзакций с одного адреса.

Формат транзакций

Длина	Тип	Описание
1 байт	Tx Version	Тип транзакции. Сейчас используется базовый тип 0x1 - передача токенов от одного адреса к другому.
34 байта	Sender	Адрес отправителя
34 байта	Recipient	Адрес получателя
8 байт	Value	Количество токенов
8 байт	None	Уникальная строка. В базовой реализации ноды используется timestamp. Внимание! С целью защиты сети от флуда и атак по-прежнему может использоваться для PoW.
64 байта	Signature	Подпись

Создание и обработка транзакции

Ниже приведены детали создания и обработки транзакции UMI.

1. Отправитель указывает обязательный набор параметров транзакции:

- сумму;
- адрес получателя;
- адрес и цифровую подпись отправителя (указывается автоматически).

2. Все показатели входящих транзакций проверяются.

3. Транзакции считаются валидными, если цифровая подпись проверена и баланс адреса отправителя больше или равен сумме транзакции.

4. Если на адресе отправителя хватает средств для осуществления перевода:

- Создается новая транзакция с включением всех указанных параметров и генерируется уникальный идентификационный номер транзакции;
- Сервер отвечает и выдает следующие варианты кода в зависимости от результата:
 - сообщение о принятии сетью транзакции;
 - ошибку кода или сообщение об ошибке, если какой-то из параметров не отвечает требованиям.

Варианты транзакций

- Доступный баланс — сумма, доступная для перевода.
- Составной баланс — сумма, от которой рассчитывается процент начисления.

№	Краткое описание	Получатель	FST-Fee	FST-Profit	FST-Dev	Структура
1	UMI -> UMI	Увеличивается на сумму транзакции.	Не меняется.	Доступный баланс и составной баланс не меняется.	Доступный баланс и составной баланс не меняется.	Не меняется.
2	UMI -> FST	Увеличивается на 90% от суммы транзакции.	Увеличивается на 10% от суммы транзакции.	Доступный баланс не меняется. Составной баланс увеличивается на 90% от суммы транзакции.	Доступный баланс не меняется. Составной баланс увеличивается на 90% от суммы транзакции.	Увеличивается на 90% от суммы транзакции.
3	UMI -> FST-fee	Увеличивается на сумму транзакции.	Увеличивается на сумму транзакции.	Доступный баланс и составной баланс не меняется.	Доступный баланс и составной баланс не меняется.	Не меняется.

[illegible]

№	Краткое описание	Получатель	FST-Fee	FST-Profit	FST-Dev	Структура
30	FST-transit -> FST	Увеличивается на сумму транзакции.	Не меняется.	Доступный баланс и составной баланс не меняется.	Доступный баланс и составной баланс не меняется.	Не меняется.
31	FST -> UMI	Увеличивается на сумму транзакции.	Не меняется.	Доступный баланс не меняется. Составной баланс уменьшается на сумму транзакции.	Доступный баланс не меняется. Составной баланс уменьшается на сумму транзакции.	Уменьшается на сумму транзакции.
32	FST -> FST-dev	Увеличивается на сумму транзакции.	Не меняется.	Доступный баланс не меняется. Составной баланс уменьшается на сумму транзакции.	Доступный баланс увеличивается на сумму транзакции. Составной баланс не меняется.	Уменьшается на сумму транзакции.
33	FST -> FST-profit	Увеличивается на сумму транзакции.	Не меняется.	Доступный баланс увеличивается на сумму транзакции. Составной баланс не меняется.	Доступный баланс и составной баланс не меняется.	Уменьшается на сумму транзакции.
34	FST -> FST-fee	Увеличивается на сумму транзакции.	Увеличивается на сумму транзакции.	Доступный баланс не меняется. Составной баланс уменьшается на сумму транзакции.	Доступный баланс не меняется. Составной баланс уменьшается на сумму транзакции.	Уменьшается на сумму транзакции.
35	FST -> FST-transit	Увеличивается на сумму транзакции.	Не меняется.	Доступный баланс и составной баланс не меняется.	Доступный баланс и составной баланс не меняется.	Не меняется.
36	FST -> FST	Увеличивается на 90% от суммы транзакции.	Увеличивается на 10% от суммы транзакции.	Доступный баланс не меняется. Составной баланс уменьшается на 10% от суммы транзакции.	Доступный баланс не меняется. Составной баланс уменьшается на 10% от суммы транзакции.	Уменьшается на 10% от суммы транзакции.
37	Сменить FST-profit	-	Не меняется.	Доступный баланс не меняется. Составной баланс увеличивается на размер доступного баланса кошелька старого profit-адреса и уменьшается на размер доступного баланса нового profit-адреса.	Доступный баланс не меняется. Составной баланс увеличивается на размер доступного баланса кошелька старого profit-адреса и уменьшается на размер доступного баланса нового profit-адреса.	Увеличивается на размер доступного баланса кошелька старого profit-адреса и уменьшается на размер доступного баланса нового profit-адреса.
38	Сменить FST-fee	Не меняется.	Не меняется.	Доступный баланс не меняется. Составной баланс увеличивается на баланс старого fee-адреса и уменьшается на баланс нового fee-адреса.	Доступный баланс не меняется. Составной баланс увеличивается на баланс старого fee-адреса и уменьшается на баланс нового fee-адреса.	Увеличивается на баланс старого fee-адреса и уменьшается на баланс нового fee-адреса.
39	Создать FST-transit	Не меняется.	Не меняется.	Доступный баланс и составной баланс не меняется.	Доступный баланс и составной баланс не меняется.	Не меняется.
40	Удалить FST-transit	Не меняется.	Не меняется.	Доступный баланс и составной баланс не меняется.	Доступный баланс и составной баланс не меняется.	Не меняется.

База данных PostgreSQL (node-master)

В мастер-ноде данные балансов и mempool сохраняются в PostgreSQL.

Три базовые таблицы доступны для чтения:

Mempool

Транзакции опубликованные в сети, но еще не подтвержденные.

hash	bytea, 32 байта	Хэш транзакции
sender	bytea, 34 байта	Отправитель
recipient	bytea, 34 байта	Получатель
value	bigint	Сумма
created_at	timestamptz	Время, когда транзакция была первый раз получена из сети
raw	bytea, 149 байт	Бинарное представление транзакции.

Transaction

Подтвержденные транзакции.

hash	bytea, 32 байта	Хэш транзакции
block_height	integer	Высота блока
block_tx_id	integer	Порядковый номер транзакции в блоке
sender	bytea, 34 байта	Отправитель
recipient	bytea, 34 байта	Получатель
value	bigint	Сумма

Block

hash	bytea, 32 байта	Хэш блока
height	integer	Высота блока
version	integer, 1 байт	Версия (формат) блока
previous_block_hash	bytea, 32 байта	Хэш предыдущего блока
merkle_root	bytea, 32 байта	Дерево Меркла
created_at	timestamptz	Время создания блока

Подпись сообщения

В код UMI интегрирована функция подписи сообщения, которая используется для удостоверения владения адресом без отправки транзакции или передачи мнемонической фразы.

Функция `umi_get_balance`

Мастер-нода кеширует промежуточные значения баланса и сохраняет их в таблицы, однако для получения актуального баланса (с учетом коэффициентов роста) стоит использовать функцию `umi_get_balance()`.

Первым параметром идет адрес, тип - `bytea`. Функция возвращает актуальный на данный момент баланс (тип - `bigint`), и коэффициент прироста (тип: `text`).

Запуск ноды

По умолчанию нода слушает на `127.0.0.1:8080`, переопределить порт и адрес можно через параметр `"-bind"`, например: `node-master-demo -bind=0.0.0.0:9099`

Параметры подключения к базе данных передаются через переменную окружения `DB`.

Пример: `DB="user=umi password=umi host=127.0.0.1 dbname=umi" master-node-demo`

SQL

Для первоначального запуска ноды необходимо создать базу и развернуть дамп из файла `db.sql`. При первом запуске нода автоматически создает генезис-блок, поэтому базу данных можно очищать при необходимости.

Docker

Для примера в архиве на [github](#) лежит `docker-compose` файл. Образы доступны для публичного просмотра.

Смарт-контракт по стейкингу

Концепция стейкинга в UMI реализована на основе смарт-контракта, который подразумевает формирование структур (пулов) и объединение монет с разных адресов для совместного стейкинга.

Смарт-контракт позволяет любому участнику сети:

- Создавать структуры (на балансе должно быть от 50 000 UMI). После создания структуры 50 000 монет списываются с адреса навсегда и становятся недоступны, в том числе они не участвуют в балансе структуры и, соответственно, в стейкинге.
- Присоединяться к другим структурам.

Размер вознаграждения

Размер вознаграждения напрямую зависит от размера структуры, в которой находятся участники сети.

Размер структуры (суммарное количество монет UMI)	Рост в месяц (от)	Рост в месяц (до)
от 50 000	5%	9%
от 100 000	10%	14%
от 500 000	15%	19%
от 1 000 000	20%	24%
от 5 000 000	25%	29%
от 10 000 000	30%	34%
от 50 000 000	31%	35%
от 100 000 000	32%	36%
от 500 000 000	34%	38%
от 1 000 000 000	36%	40%

Активация

Смарт-контракт по стейкингу активируется, когда участник сети переводит монеты на свой личный адрес в той или иной структуре.

- Структура создается и настраивается прямо внутри технического кошелька (ноды).
- Опции, реализованные внутри кошельков, позволяют пользователям вступать в любую структуру (пул), каждая из которых может быть настроена индивидуально.
- После помещения в стейкинг монеты не замораживаются и могут быть использованы для совершения транзакций.
- Несмотря на то, что монеты находятся в структуре, ни один член структуры не имеет возможности завладеть монетами других участников, даже если он эту структуру создал.
- Во время стейкинга пользователю начисляется вознаграждение (до 40% в месяц от суммы) на его личный адрес в структуре в режиме 24/7.
- Остановить стейкинг можно в любой момент. Для этого нужно просто перевести весь баланс вместе с вознаграждением на свой первоначальный адрес или на любой другой.

В любой момент есть возможность редактировать процесс стейкинга: вносить новые монеты или возвращать имеющиеся.

Настройки структур

Создатели структур могут указывать индивидуальные настройки и изменять их в случае необходимости. Также они получают дополнительные дивиденды.

Организаторы структур:

- Устанавливают размер дивидендов. Организаторы структур получают на свой адрес от 1% (минимум) до 5% (максимум) в месяц от стейкинга всей своей структуры.
- Устанавливают размер бонусов. Организаторы структур получают бонусы до 20% от суммы «вкладов» участников.
- Устанавливают название на латинице. Например, структура может называться «FIRST» или как угодно еще. Изменить название после создания структуры невозможно.
- Устанавливают уникальный префикс для адресов структуры. Например, адреса могут начинаться с «fst» и выглядеть примерно так:
`fst1qqqumpt2jchfa63qc0jxztud75x89ya49h58sw34hdl8kl3a60cl4qmr`.
Изменить префикс после создания структуры невозможно.
- Интегрируют логотип 150x150 пикселей (максимальный размер — 300 Кбайт, формат JPG или PNG). При желании логотип можно изменить в будущем.
- Прописывают описание структуры на латинице (до 35 символов с пробелами). При желании описание можно изменить в будущем.
- Добавляют URL-адрес, ведущий на сайт структуры.
- Опционально имеют возможность создать транзитный беспрошлинный кошелек (Transit Wallet) внутри структуры, который не облагается «комиссиями» (с которого не списываются бонусы).

Управление структурой

Создание структуры происходит с помощью технического кошелька (ноды) и доступно любому пользователю.

Управление структурой осуществляется через мастер-кошелек (кошелек с адресом, который использовался для создания структуры). Организаторы структур в любой момент могут:

- Менять логотип;
- Менять URL-адрес сайта;
- Редактировать описание структуры;
- Регулировать размер дивидендов (1-5%);
- Регулировать размер бонусов (0-20%) («комиссий» за вход в структуру);
- Назначать новый адрес дивидендов (Profit wallet);
- Назначать новый адрес для бонусов (Fee wallet);
- Активировать новый транзитный адрес (Transit wallet);
- Деактивировать транзитный адрес (Transit wallet).

Таким образом, у каждой структуры может быть 4 типа уникальных кошельков:

Мастер-кошелек (Master Wallet)

Дивидендный (Profit Wallet)

Бонусный (Fee Wallet)

Транзитный (Transit Wallet)

Дополнительные монеты

Смарт-контракт дополнительно генерирует команде UMI 2% в месяц от всех монет, задействованных в стейкинге. Монеты отправляются на адреса команды и используются для продвижения криптовалюты и выплаты грантов разработчикам, которые создают продукты на базе UMI и способствуют развитию сети.

Ссылки

www.UMI.top

Веб-кошелек: wallet.umi.top

API: umi.wiki

Блокчейн-эксплорер: blockchain.umi.top

Брендбук: umi.top/brandbook

Помощь

FAQ: umi.top/faq

Гайд: umi.top/guide

Обратная связь

Для общих вопросов: info@umi.top

Для коммерческих предложений: up@umi.top

Команда разработчиков: dev@umi.top

Мы в соцсетях



[instagram.com/umi.top.eng/](https://www.instagram.com/umi.top.eng/)



[facebook.com/umi.top.eng/](https://www.facebook.com/umi.top.eng/)



Канал: t.me/umi_news_eng



bitcointalk.org/index.php?topic=5252661



[youtube.com/channel/UC8Beb0iYilkb6YNx_gyQZpw/](https://www.youtube.com/channel/UC8Beb0iYilkb6YNx_gyQZpw/)



twitter.com/umi_top_eng



[reddit.com/user/UMITop](https://www.reddit.com/user/UMITop)



medium.com/@umitopeng



[instagram.com/umi.top](https://www.instagram.com/umi.top)



[facebook.com/umi.top.official](https://www.facebook.com/umi.top.official)



Канал: t.me/umi_news_ru



bitcointalk.org/index.php?topic=5252656



[youtube.com/channel/UCO1_qdYhA0kvsw1lwtVPu4w/](https://www.youtube.com/channel/UCO1_qdYhA0kvsw1lwtVPu4w/)



twitter.com/UMITOP



vk.com/umi_top



[tiktok.com/@umi_top](https://www.tiktok.com/@umi_top)



medium.com/@umi_top