UWIM - YELLOWPAPER

UWIM - Сетевая распределенная криптографическая платформа для удобного создания, использования и учета децентрализованных приложений (смарт-контрактов или «умных контрактов»).

В основу нашей технологии мы заложили идею идеального баланса централизации и децентрализации данных и функций системы. Развитие, дополнение и обновление системы проходит централизованно через компанию, а валидация, контроль, принятие решение (согласие или несогласие) с обновлениями происходит децентрализовано и определяется только участниками платформы.

Архитектура платформы UWIM была спроектирована с учётом большого числа пользовательских токенов с типизированными смарт-контрактами. В основе UWIM лежит собственная блокчейн-технология, как самостоятельный программный продукт, не являющийся форком Bitcoin.

Децентрализованная часть

Устойчивость и открытость платформы достигаются технологией блокчейн (распределённый реестр данных) с собственной модифицированной версией консенсуса Proof Of Stake (модель принятия решений между участниками).

Все данные распределены между серверами (Исходный код нод в открытом доступе со свободной лицензией). Любой участник сети может развернуть один из типов нод (полная нода - со всей историей операций сети, возможностью валидации блоков и всем функционалом API JSON-RPC, легкая нода - с функционалом API JSON-RPC). Полная нода может стать валидатором при выполнении требований и участвовать в основном конесенсусе.

Сеть может включать в себя неограниченное число токенов, смарт-контрактов и участников (адресов) и свободно контролироваться участниками.

Собственные сборки нод были созданы для дальнейшей оптимизации и развития платформы в целом.

Технологические особенности

Хранение и шифрование данных

> Для оптимизации объема и быстрого доступа к необходимым данным используется leveldb с открытой лицензией (Технология для хранения большого количества нереляционных данных формата ключ>значение).

Доступ к данным участников сети осуществляется посредством иерархически сгенерированных ключей BIP39.

В формате bech32 адреса для каждого участника разделяются на три типа: основной адрес (префикс uw), адрес смарт-контракта (префикс sc), адрес ноды (префикс nd).

Далее участники обмениваются данными посредством отправки сообщений на ноду, подписав при этом сообщения своим секретным ключом. Данные проходят первичную валидацию на ноде, получившей сообщение, рассылаются всем валидаторам, объединяются в блоки и отправляются на консенсус. Хэширование осуществляется при помощи кодировки sha256.

В ядре ноды нами созданы несколько уровней валидации данных для полной проверки и исключения ошибок от момента поступления на ноду до момента консенсуса.

Консенсус

Модифицированная версия консенсуса ProofOfStake заключается в принятии решений в зависимости от числа монет на nd адресе валидатора (либо nd+sc в зависимости от наличия смарт-контракта делегирования), а так же от общего числа валидаторов.

Каждая нода постоянно принимает транзакции от участников сети, данные попадают в первоначальный пул для обработки, исключающий переполнение данных и задержку в консенсусе. Далее нода валидирует транзакцию на основании собственной цепочки блоков и принимает решение: одобрить или сразу отклонить транзакцию, принятые транзакции сразу же отправляются другим валидаторам сети, список которых автоматически подгружается с основного или других узлов.

Параллельно с принятием данных, ноды, получившие статус валидатора, принимают участие в консенсусе: в заранее определенной очередности валидаторы становятся пропоузером (proposer - валидатор, предлагающий на рассмотрение данные). В случае, если блок принят – пропоузер нолучает вознаграждение. Данные о вознаграждениях имеют собственный тип транзакций. Наградную транзакцию пропоузер добавляет при отправке блока на консенсус, она валидируется наряду с остальными.

Каждый раунд консенсуса происходит в следующем порядке:

1) Proposer создает блок исходя из собственного пула поступивших транзакций (своих и чужих), подписывает и отправляет его другим валидаторам. Другие валидаторы получив блок сохраняют его в свою временную память. В случае, если proposer не представил блок - система коллективно назначает ему штрафные санкции. Так же proposer добавляет в блок транзакцию с собственной наградой за создание верного блока (Все наградные транзакции поступают с Genesis-адреса при наличии на нём средств).

2) Валидаторы анализируют блоки на основании своих данных и отвечают другим валидаторам о принятии или отклонении.

3) Каждый валидатор оценивает ответы других по двум критериям (Суммарное число балансов валидаторов, проголосовавших ЗА, которое должно составить не менее 66% и

количество валидаторов проголосовавших ЗА от их общего числа, которое должно составить не менее 50%). Если оба требования выполняются – каждый валидатор отправляет блок на запись и выполнение всех транзакций.

4) Каждый валидатор анализируем метрики, очищает временную память и готовится к новому раунду

Контракты

Кроме обычных адресов в системе могут присутствовать смарт-контракты, обладающие собственной логикой и оперативной памятью. И логика и память контрактов так же используются децентрализованно (хранятся в идентичном состоянии на всех нодах).

Смарт контракты разделяются на основные группы: Контракты для поддержания развития системы и пользовательские контракты.

Добавляются контракты исключительно через централизованный узел (Подробнее в разделе «Централизованная часть»). Контракт может принимать транзакцию, а далее на основании собственной логики производить ряд вычислений и множественную отправку транзакций. На нодах каждый контракт представлен отдельным приложением, все результаты деятельности контрактов после выполнения отправляются в консенсус для подтверждения другими участниками и исключения модификации кода или данных памяти.

В системе существует основной токен и может быть создано множество токенов участников (альты), сам токен аналогично представляет собой смарт-контракт и имеет владельца (адрес). Владелец может пользоваться балансом смарт-контракта, но не может непосредственно в самом блокчейне менять условия контракта. Также в отдельных случаях владелец может отказаться от владения смарт-контрактом, тогда его подпись не будет приниматься валидаторами при обработке транзакций.

При отправке любой транзакции присутствует комиссия, исчисляющаяся в основном токене, которая зависит от текущей нагрузки на сеть. Возможно увеличение и уменьшение комиссии для замедления и ускорения транзакций. Все комиссии забирает себе валидатор, предложивший блок с данной транзакцией.

Обмен между токенами осуществляется через смарт-контракт обмена: По каждой паре основного и пользовательского токена создается «Пул ликвидности», определяющий соотношение при обмене. Так же при обмене пользовательского токена на другой пользовательский токен применяются два пула ликвидности (от каждой пары).

В каждой ноде присутствует шлюз для отправки и принятия данных (API) в формате JSON-RPC. Посредством API любой участник сети может подключать собственные IT-решения к блокчейну и связывать собственный смарт-контракт со своим централизованным продуктом в зависимости от собственных потребностей.

Реализация ноды может быть на различных языках программирования и для различных ОС.

Централизованная часть

Централизованная часть проекта представляет собой удобный пользовательский интерфейс для использования блокчейна UWIM. Исходный код централизованной части является собственностью компании и не распространяется.

Пользователи через web-сервис могут получить исчерпывающую информацию, а так же пользоваться бесплатными продуктами:

Обозреватель блокчейна - позволяющий просматривать данные и получать статистику по всем операциям, не запуская при этом полноценную ноду.

Веб-терминал, доступ в который осуществляется через персональный ключ BIP39 (уже уточнялось в децентрализованной части).

Мобильные терминал, доступ в который осуществляется через персональный ключ BIP39 (уже уточнялось в децентрализованной части).

В личном кабинете пользователь может хранить и использовать токены, представленные в блокчейне другими участниками. Пользователь может использовать графический интерфейс для работы со смарт-контрактами, представленными в блокчейне, а так же для:

Создания типовых шаблонов токенов и смарт-контрактов.

Любой пользователь сети может прикрепить в личном кабинете к своему адресу один собственный токен. При создании определяются лэйбл и эмиссия (изменить которые в дальнейшем нельзя), название и прочие данные (которые можно изменять в дальнейшем посредством транзакций). Кроме того, при создании токена пользователь определяет его тип (personal – токен которым управляет только создатель; team – токен для управления которым нужны подписи определённого числа участников; nft – токен, каждый экземпляр которого уникален, управляется только одним участником). Кроме того у каждого токена есть карточка владельца и карточка токена, данные в которых обновляются посредством транзакций владельца (Подробности описаны далее в разделе «Площадка токенов»). В зависимости от данных в карточках токены подразделяются на стандарты. В зависимости от стандарта к нему могут добавляться различные смарт-контракты. После прохождения систем мониторинга и безопасности созданный токен/смарт-контракт выгружается в общую сеть и становится децентрализованным и доступным для каждого. В процессе развития пользователь сможет дополнять его новыми узлами, но все прежние части становятся неизменными и напрямую зависящими от первоначальных условий.

Создание нестандартных монет и смарт-контрактов на заказ и их интеграция в бизнес

В случае если пользователь (человек или компания) хочет реализовать нестандартные решения (токен/смарт-контракт/api/приложение) он может воспользоваться услугами компании, данный процесс начинается с заявки в личном кабинете и прохождения верификации. Для данной ситуации будет разработан SDK, на базе которого будут создаваться расширенные решения.

Инструменты для платформы

– Площадка токенов

Каждый созданный пользовательский токен в блокчейне имеет карточку владельца (или владельцев если тип токена – team) и карточку токена, все данные которых так же подлежат децентрализации (каждое последующее обновление фиксируется и остаётся неизменным на протяжении существования). Токен может быть прикреплён к личности владельца, посредством аккредитации. Человек или компания последовательно проходят этапы подтверждения персональных данных (Количество и верность данных приближает каждый конкретный токен к полной персонализации). Так же пользователь может прикрепить к токену конкретный продукт или ресурс, так же пройдя аккредитацию. Может добавлять roadmap своего продукта, контент итд. Каждый пройденный этап делает токен прозрачнее, персонализированнее и привлекательнее для других участников сети.

На площадке все пользовательские токены разделены на стандарты, информация о стандартах представлена на официальном сайте проекта.

– Биржа для dex-обмена токенов

Пользователи могут осуществлять обмен между различными токенами в блокчейне через смарт-контракты обмена. Контракт может использоваться через личный кабинет на основном сайте проекта, так же через любую ноду (не обязательно валидатор) и через мобильное приложение. В основе контракта была заложена идея пулов ликвидности: всегда у каждой пары токенов есть зарезервированный объем каждого токена, в рамках данного пула в любой момент может произойти операция обмена, а комиссию за обмен распределяют между собой держатели пула ликвидности (может состоять из неограниченного числа токенов). В зависимости от типов токена, созданного пользователем, его обмен может проходить по разным алгоритмам. Кроме того владельцы токенов, определённых стандартов, могут добавлять дополнительные смарт-контракты, которые дополняют функционал на бирже, например «Payable-token», который может автоматически распределять основную монету, отправленную владельцем, среди всех держателей пула ликвидности, так же владелец токена может его «доэмитировать» через Genesis адрес, отправив в ответ эквивалентное число (по текущему курсу) основной монеты платформы, и т.д.

– Прочие инструменты

Кроме основных инструментов (площадка токенов и биржа), платформа имеет ряд дополнительных, число которых пополняется и будет расти вместе с платформой, такие, как

- «Фонд Маска» - Команда UWIM планирует номинировать не менее 10 известных личностей-экспертов со всего мира, которые будут оценивать самые яркие инициативы участников платформы. Любая команда может создать токен, представить свой проект и заполнить все соответствующие данные. Каждый проект подавший заявку, получит оценку независимых экспертов. По результатам оценки иголосования экспертов, проекту будет присвоен специальный статус и ,в зависимости от назначенного статуса, номинируемый получит вознаграждение единовременно или поэтапно в виде UWM (Основной единицы платформы).
- Поддержка personal-токенов – Специальный смарт-контракт для поддержки новых токенов на платформе, который по определённым условиям распределяет основную монету платформы среди участников пула ликвидности нового personal-токена.
- Контракт баунти-компании – Специальный смарт-контракт для тех, кто активно развивает платформу.