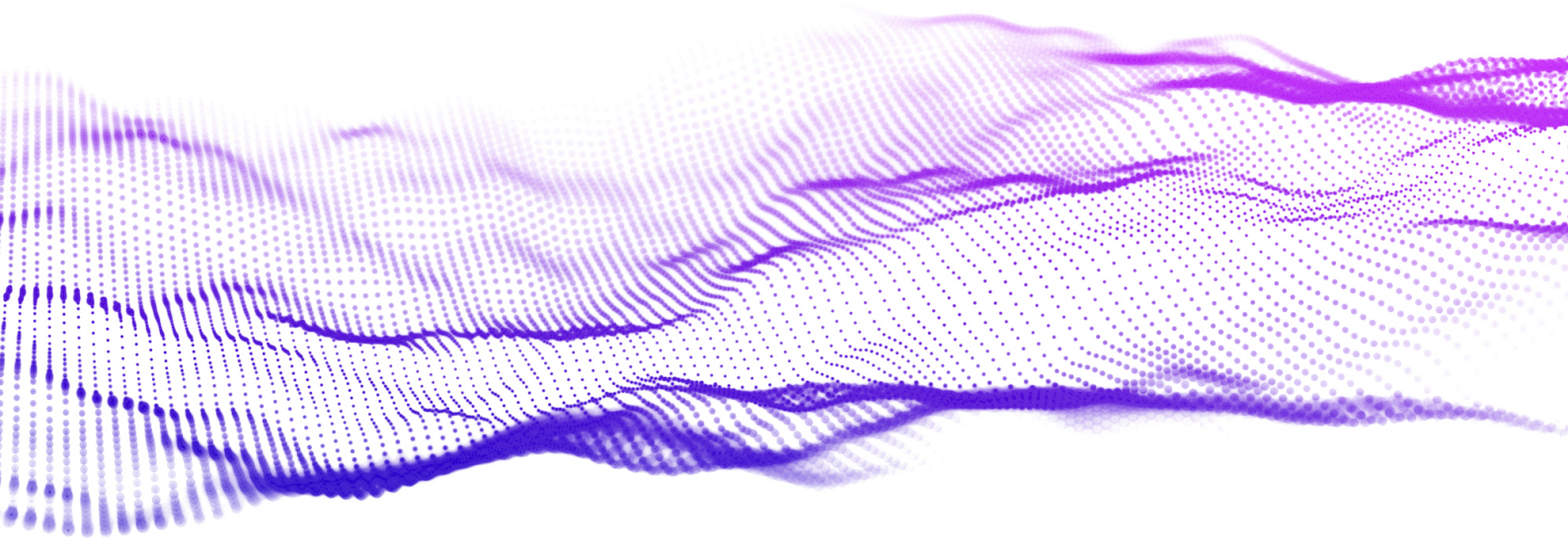




Acrona Club



Acrona Blockchain White paper v. 1

Введение	3
Алгоритм PoS (Proof-of-Stake)	3
Выбор валидаторов (Forger Selection)	3
Техническое описание криптовалюты ACRN	3
Определение	3
Алгоритм консенсуса	3
Узлы	4
Блоки	4
Создание блоков (Forging)	4
Алгоритм создания блоков	5
Основные особенности	5
Acrona Mining	6
Выбор валидаторов	6
Облачная инфраструктура	7
Cloud network	8
Масштабирование облачной инфраструктуры	8
Сторожевые узлы (Sentry Node)	9
Ретрансляционные узлы (Relay Node)	9
API узлы (API Node)	9
Географическая распределенность	10
Безопасность Acrona Shield	10
Инфраструктура	10
Программный код	10
Управление процессами	10
Возможности Acrona Blockchain	11
Привлечение средств для развития	11
Оплата товаров и услуг в собственной криптовалюте	11
Выгодный Cashback	11
AirDrop для клиентов	11
Достижение децентрализации	12

Введение

Технология Blockchain произвела настоящий переворот в области хранения данных, создав новую модель экономических отношений. Но по мере развития, сеть все чаще сталкивается с трудностями: большие энергозатраты, медленные транзакции, высокие комиссии. К сожалению, поиск решений по данным вопросам ведется крайне медленно.

Алгоритм PoS (Proof-of-Stake)

Proof-of-Stake (доказательство доли владения) – это алгоритм консенсуса, альтернативный способ подтверждения транзакций в Blockchain. В отличие от Proof-of-Work (PoW), в алгоритме PoS создатель нового блока выбирается в зависимости от количества средств на балансе. PoW валидатор может вовсе не иметь на балансе монеты, транзакции которой он подтверждает. Следовательно, у него нет сильной мотивации поддерживать устойчивость сети, ведь инфраструктуру можно в любой момент переключить для майнинга другой криптовалюты. В алгоритме PoS все обстоит иначе.

Выбор валидаторов (Forger Selection)

Условием PoS является обязательное наличие на балансе у валидатора определенного количества монет, транзакции которых он подтверждает. Вероятность создания нового блока зависит от общего количества средств на балансе. Для того чтобы подтвердить транзакцию и создать новый блок, валидатору необходимо «заморозить» часть монет на своем счете. Все валидаторы заинтересованы в корректной работе сети, по двум причинам:

- Автоматическая потеря всех средств, при намеренном подтверждении мошеннической транзакции;
- Перспектива роста цены добываемого актива, размещенного на балансе.

Техническое описание криптовалюты ACRN

Определение

Acrona (ACRN) – это децентрализованная Proof-of-Stake криптовалюта с открытым исходным кодом. Acrona Blockchain реализован на базе ядра NEXT, что позволяет совершать тысячи транзакций в каждом блоке.

Алгоритм консенсуса

Чем больше у валидатора средств на балансе, тем выше вероятность создать следующий блок и получить вознаграждение. Этот процесс не зависит от вычислительной мощности оборудования.

По правилам PoS, для создания новых блоков, устройство валидатора должно находиться online, на постоянной основе. Применив технологию Cloud Network, нам удалось решить эту задачу. Кошельки валидаторов в процессе добычи всегда находятся online.

Узлы

Узлы являются основой Acrona Blockchain и обеспечивают его работоспособность. По сути, узлами можно назвать любое устройство с доступом в интернет и собственным IP-адресом. Роль узлов состоит в поддержании сети, распространении и хранении копий Blockchain.

Помимо транзакций, узлы передают всю информацию блоков по мере их поступления. При игнорировании, узел временно заносится в черный список для устранения ложных данных. В каждый узел встроена надежная защита от DDOS атак, которая ограничивает сетевые запросы от пользователей.

Блоки

Acrona Blockchain хранит историю и учет всех выполненных транзакций. Копии Blockchain фиксируются в каждом узле, позволяя аккаунту создавать блоки.

Параметры блоков:

- Версия, значение высоты и идентификатор;
- Временная метка (в секундах от блока Genesis);
- ID валидатора создавшего блок и открытый ключ его аккаунта;
- Хэш предыдущего блока и его идентификатор;
- Количество транзакций хранящихся в блоке;
- Общее количество монет ACRN, представленные в блоке транзакциями и комиссиями;
- Данные всех транзакций, включая их идентификаторы в блоке;
- Длина полезной нагрузки блока и значение ее хеш-функции;
- Кумулятивная сложность для блока и базовое целевое значение;
- Цифровая подпись.

Создание блоков (Forging)

Существуют 3 фактора повышающие вероятность валидации:

Базовое целевое значение

В процессе валидации, аккаунты пытаются создать хеш-значение, ниже заданного базового целевого значения. Это значение изменяется от блока к блоку и выводится из базового целевого значения предыдущего блока, умноженного на количество времени создания данного блока.

Целевое значение

Каждый аккаунт в системе рассчитывает свое собственное целевое значение, которое равно:

$$T = Tb \times S \times Be$$

Где:

T – новое целевое значение

Tb – базовое целевое значение

S – время (в секундах), прошедшее с момента последнего блока

Be – эффективный баланс аккаунта

Целевое значение растет ежесекундно и его максимум: **1,53722867 x 1017**. Минимальное целевое значение – это половина базового целевого значения предыдущего блока. Оба значения, целевое и базовое целевое одинаковы для всех аккаунтов, пытающихся создать новый блок. Истинным параметром аккаунта является эффективный баланс.

Совокупная сложность

Совокупное значение сложности получается из базового целевого значения, по следующей формуле:

$$Dcb = Dpb + 264 / Tb$$

Где:

Dcb – сложность текущего блока

Dpb – сложность предыдущего блока

Tb – базовое целевое значение текущего блока

Алгоритм создания блоков

При создании нового блока, активный аккаунт с помощью своего приватного ключа подписывает предыдущий созданный блок подписью в 64-байт. Далее подпись хешируется с использованием SHA256.

Первые 8 байт полученного хеша создают число – хит аккаунта, который сравнивается с текущим целевым значением. Если вычислительный хит ниже целевого, то следующий блок становится доступным для генерации. Так как целевое значение увеличивается ежесекундно и в результате становится слишком большим, даже несколько активных аккаунтов могут создавать новые блоки, обеспечивая работоспособность сети.

Основные особенности

JavaScript клиент

С помощью клиент приложения, пользователь получает доступ к сети через обычный интернет браузер. Специфика работы приложения защищает данные от злоумышленников и полностью исключает попадание личных ключей в открытый доступ.

Платежная система

Acrona Blockchain выполняет функции децентрализованной платежной системы, что позволяет совершать транзакции между пользователями внутри сети.

Интеграция API, SDK

Благодаря интеграциям API и SDK пользователи могут внедрять собственные программы и услуги, а также привлекать партнеров в различные отрасли, используя готовые продукты Acrona.

Acrona Mining

Acrona Mining – это сервис для добычи ACRN валидаторами Acrona Blockchain, на базе алгоритма Proof-of-Stake. На скорость майнинга влияют 3 критерия: количество монет на балансе, продолжительность работы монет, суммарный объем средств в ноде. Минимальное количество монет на балансе для запуска Acrona Mining – 10 ACRN.

Выбор валидаторов

Вероятность валидатора создать новый блок и получить вознаграждение, зависит от трех параметров.

1. Количество монет на балансе кошелька

Чем больше монет на балансе кошелька, тем больше шансов на создание нового блока.

2. Продолжительность работы монет

Это условие подразумевает удержание средств на балансе кошелька. Как только с баланса Acrona Mining производится транзакция (отправка) – данное значение обнуляется.

3. Суммарный объем средств в ноде

Представьте, на балансе вашего кошелька 100 ACRN (**кошелек-1**). Под вами размещается новый кошелек с балансом 70 ACRN (**кошелек-2**). Под ним размещается новый кошелек с балансом 20 ACRN (**кошелек-3**).

Кошелек-1 (вы): **100 ACRN**

Кошелек-2: **70 ACRN**

Кошелек-3: **20 ACRN**

Складываем все значения и получаем суммарный объем средств в ноде:

190 ACRN (100+70+20=190)

Обратите внимание, ваш личный баланс (кошелек 1) также участвует в подсчете.

Связь между вашим кошельком и другими кошельками под вами, закрепляется на бесконечное количество линий в глубину структуры.

Расчет эффективности майнинга

Если перемножить все 3 параметра, мы узнаем точный ежемесячный % добытых кошельком монет.

Примечание:

Ежемесячный % считается от общего количества монет на балансе вашего кошелька.

Количество монет на балансе кошелька		Суммарный объем монет в финансовом пуле, под вашим кошельком		Продолжительность работы монеты	
10 – 49	7,07 %	10 – 99	1,01	0	1,00
50 – 99	7,73 %	100 – 499	1,05	30	1,03
100 – 499	8,91 %	500 – 999	1,09	60	1,06
500 – 999	10,12 %	1 000 – 9 999	1,15	90	1,09
1 000 – 4 999	11,8 %	10 000 – 49 999	1,24	180	1,18
5000 +	12,98 %	50 000 – 99 999	1,32	360	1,36
		100 000 – 499 999	1,40		
		500 000 +	1,46		

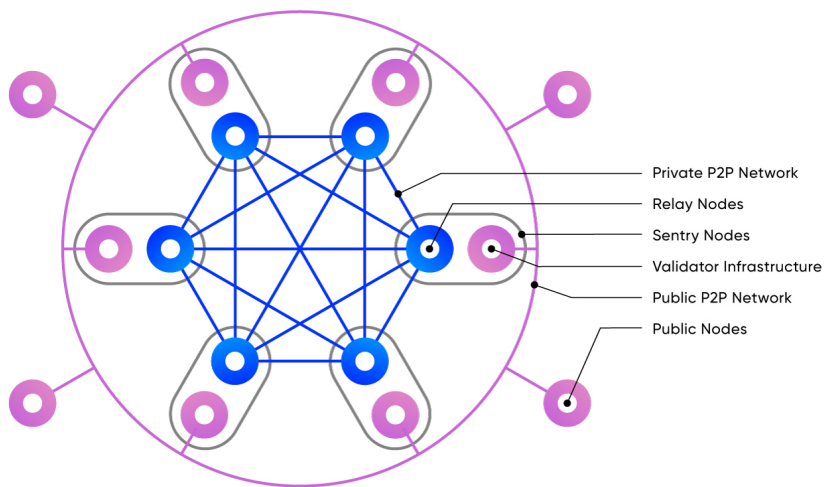
Облачная инфраструктура

Несмотря на свой потенциал, алгоритм консенсуса Proof-of-Stake нуждается в серьезной реконструкции. Плохое интернет соединение между валидаторами, дешевые облачные сервисы, погрешности в настройках, слабая защита от DoS атак. Все это сильно затрудняет развитие сети, снижая ее работоспособность в разы. Для стабильной работы требуются сплоченные действия всех валидаторов. Данная концепция легла в основу Acrona Blockchain – облачной сети с неограниченными возможностями для коллективного развития.

Взаимодействие между валидаторами происходит без потери скорости, из-за географического расположения узлов. Скорость передачи блоков приближена к локальной сети, как будто сервера расположены в одном помещении.

Cloud network

Мы создали виртуальную облачную сеть, которая обеспечивает слаженную работу всех валидаторов.

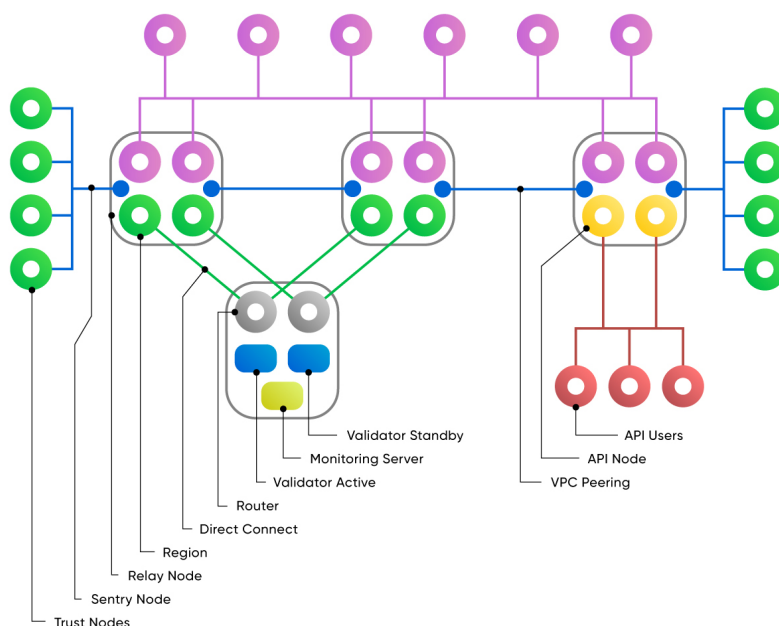


Технология Kubernetes позволила добиться значительных преимуществ над традиционными сетями.

- Высокая скорость передачи блоков между валидаторами, независимо от географического расположения;
- Работа виртуальной сети в Cloud network на уровне провайдера, в отличие от частных VPN-соединений.

Масштабирование облачной инфраструктуры

Рассмотрим строение инфраструктуры валидатора.



Ее можно разделить на две части:

- Облако из нескольких зон доступности, каждая из которых состоит из множества узлов;
- Центр обработки данных, в котором установлено оборудование валидатора.

В облаке находится множество виртуальных серверов, каждый из которых является полной нодой. Сервер выступает в качестве участника сети, но выполняет разные функции.

Сторожевые узлы (Sentry Node)

Sentry Node – это публичные узлы, которые совершают обмен данными с другими публичными узлами через интернет.

Они защищают сервер от потенциальных угроз из интернета (DDoS атаки). Другие узлы валидатора без выхода в интернет, опираются на работоспособность сторожевых узлов. В случае, если DDoS атака «убьет» все сторожевые узлы валидатора, это неминуемо приведет к остановке его работы и исключению из списка активных валидаторов.

Для защиты валидатора предусмотрены следующие меры:

- Заблаговременное создания бóльшего количества сторожевых узлов, вместо стандартных 3-5 шт;
- Автоматическое клонирование существующих сторожевых узлов, при угрозе вредоносных атаках;
- Непрерывная связь с другими «надежными» валидаторами по внутренней облачной сети.

Ретрансляционные узлы (Relay Node)

Relay Node – это внутренние узлы, которые совершают обмен данными исключительно с доверенными узлами, через внутреннюю облачную сеть.

Доверенными узлами могут выступать другие ретрансляционные узлы (Trust Nodes), сторожевые узлы и API узлы инфраструктуры валидатора. А также ретрансляционные узлы других валидаторов сети, которые доверяют друг другу, с настроенным обменом данными через соединение виртуальных сетей в облаке (VPC Peering).

Валидатор осуществляет прямые соединения только со «своими» ретрансляционными узлами. Они надежно защищены от DDoS атак, взлома и являются дополнительной защитой валидатора после сторожевых узлов.

API узлы (API Node)

API Node – это публичные узлы, которые совершают обмен данными с другими публичными узлами через интернет.

API узлы позволяют валидаторам взаимодействовать с сетью, отправлять API запросы напрямую, с помощью кошельков и других приложений. Для децентрализации Acrona Blockchain и максимально качественной связи, всем валидаторам необходимо поднять свои

API узлы для публичного использования. Это уверенный шаг в сторону глобального развития технологии, что принесет всем участникам сплошные плюсы.

Географическая распределенность

Важнейшую роль в построении облачной инфраструктуры играет географическое распределение узлов, по разным регионам и центрам обработки данных (зон доступности облака) внутри регионов.

Благодаря независимой работе одного узла или целого облака, где располагается множество узлов – связь между валидаторами гораздо устойчивей. Внутренняя сеть в облаке позволяет сохранить высокую связь при распределении узлов, а разнообразие вариантов расположений обеспечивает баланс между децентрализацией и скоростью.

Безопасность Acrona Shield

Безопасность Acrona Blockchain делится на три составляющие:

- Инфраструктура;
- Программный код;
- Управление процессами.

Инфраструктура

Узлы сети разделены на уровни, закодированы и не зависят друг от друга. Таким образом, инженер имеет доступ только к своему уровню. Любые вмешательства будут обнаружены и заблокированы системой безопасности. В случае внутренней диверсии с установкой на узел вредоносного ПО, произойдет идентификация злоумышленника и ограничение его доступа, с полным восстановлением поврежденных узлов. По такому принципу работают современные системы защиты крупных банковских систем.

Программный код

Диагностика программного кода ядра системы выполняется непрерывными циклами, с помощью статических анализаторов. Все угрозы исправляются мгновенно, что полностью исключает их проникновение в исходную версию кода.

Управление процессами

Чтобы исключить риски «человеческого фактора», в системе отключены все ручные процессы, выполняемые оператором. Данный подход отлично зарекомендовал себя во многих крупных Blockchain системах. Среди аккаунтов абсолютное равноправие, что гарантирует работу сети по строго заданному алгоритму.

Возможности Acrona Blockchain

Ежедневно появляются новые компании и стартапы, нуждающиеся в децентрализованных платежных системах. Онлайн продажи, аренда, транспортные услуги, сервисы доставки, удаленное обслуживание, бронирование и другие востребованные направления. Благодаря интеграции с использованием API и SDK пользователи могут внедрять собственные программы и услуги, а также привлекать партнеров в различные отрасли, с помощью готовых сервисов ACRN.

Привлечение средств для развития

Любой бизнес в определенный момент сталкивается с необходимостью масштабирования. Это может быть увеличение ассортимента товаров/услуг или подключение новых регионов. Чаще всего компания выпускает и продает акции, привлекая подобным образом новые средства. Но с помощью криптовалюты этот процесс осуществляется гораздо проще, и что немаловажно, без сильной нагрузки на бюджет. Суть заключается в продаже доли компании за собственную криптовалюту. Бизнес получает финансирование, а покупатель доли становится его партнером. Подобное сотрудничество благоприятно для всех участников сделки, чей доход напрямую зависит от общего успеха компании.

Оплата товаров и услуг в собственной криптовалюте

Вы можете интегрировать новую платежную систему в свой бизнес и позволить покупателям оплачивать ваши товары/услуги за собственную криптовалюту. Это не только расширит целевую аудиторию, но и повысит лояльность уже существующих клиентов.

Выгодный Cashback

Принцип поощрения лояльных клиентов посредством Cashback чрезвычайно прост и эффективен. Примените этот инструмент и возвращайте % от покупки, в виде своей криптовалюты. Чем выгодней будет Cashback, тем чаще клиент будет возвращаться именно к вам и рекламировать вашу компанию.

AirDrop для клиентов

AirDrop – это бесплатная раздача криптовалюты клиентам, за выполнение каких-то целевых действий. Его часто проводят сами разработчики для PR кампаний. При адекватном использовании AirDrop не принесет сильной финансовой нагрузки, так как часть этих монет досталась практически бесплатно. Во-первых, бесплатные монеты несут гораздо больше ценности, чем какие-то купоны, дисконтные карты и тд. Во-вторых, условия для получения AirDrop выполняются без особых усилий. Это может быть вступление в группу, чат, репост, лайк, комментарий и тд. Совершив простое действие, довольный пользователь получает приятный бонус, а вы – рост подписчиков.

Достижение децентрализации

По мере роста сети и увеличения числа ее участников, выполняется обновление и доработка отдельных элементов. Когда сеть достигнет необходимых размеров для обеспечения децентрализации, документация API и SDK, а также подробная информация по интеграции будут выложены в открытый доступ. Мы не преследуем цель частного владения, но хотим защитить технологию до финального этапа реализации, для автономного существования. Описание отдельных частей экосистемы и принципов работы ACRN будут опубликованы в специальном порядке, до релиза основной сети блокчейн:

Декабрь 2018:

- Запуск тест-нета Acrona Blockchain (28.12.2018);
- Февраль 2019:
- Публикация White Paper Acrona Blockchain (25.02.2019).

Март 2019:

- Спецификация Acrona Blockchain;
- White Paper ACRN;
- One page ACRN;
- White Paper ACRN Ecosystem;
- Roadmap 2019-2021.

Апрель 2019:

- Запуск мейн-нета Acrona Blockchain;
- Релиз ACRN на GitHub;
- Запуск Acrona Ecosystem и децентрализация.