Белая Бумага

28 СЕНТЯБРЯ, 2017 Г.

Aion: The third-generation blockchain network

Мэтью Споук
matt@aion.network

Инженерная команда Nuco
aion@nuco.io

Опубликовано v1.0.0, 31 Июля, 2017 г.

Аннотация

Повсеместная адаптация блокчейн-систем до сегодняшнего дня была ограниченной в связи с нерешенными вопросами масштабируемости, конфиденциальности и совместимости. В данной работе мы опишем архитектуру и дизайн сети Aion – многоуровневой блокчейн-системы третьего поколения, созданной для решения этих вопросов. В основе нашей гипотезы лежит идея, что множество блокчейнов будут созданы для решения уникальных бизнес задач, возникающих в различных индустриях. Сеть Aion спроектирована для обеспечения безопасного механизма взаимодействия между блокчейн-сетями, при этом поддерживая индивидуальные блокчейн-архитектуры. В своей работе данный механизм не полагается на доверие. В основе этой системы лежит первый в мире специализированный корпоративный блокчейн Aion-1. Он является ультрасовременным блокчейном, внедряющим новую парадигму надежности и справедливых, объективно представительных крипто-экономических стимулов.

Стратегический план

Данная работа предназначена для технического введения и будет дополнена последующими исследованиями и разработками. В ближайшие несколько месяцев команда Aion опубликует серию научно-исследовательских работ, которые более подробно объяснят концепции предложенного консенсусного алгоритма, виртуальной машины (VM), скриптового языка, моста, межсетевой транзакционной функциональности и экономической системы, лежащей в основе сети. В дополнение, вскоре после публикации этой работы Aion опубликует стратегию по сбору средств и установленные сроки. Мы охотно делимся с Вами нашими идеями и с нетерпением ждём Ваших отзывов.

Contents

1 ВВЕДЕНИЕ **4**

2 ИСТОРИЯ **4**
2.1 Блокчейн первого поколения . . . 4
2.2 Блокчейн второго поколения . . . 4
2.3 Aion: блокчейн третьего поколения . . . 5

3 МНОГОУРОВНЕВАЯ БЛОКЧЕЙН-СЕТЬ AION **5**
3.1 Соединяющиеся Сети . . . 5
3.2 Межцепная транзакция . . . 6
3.2.1 Формат . . . 6
3.2.2 Маршрутизация . . . 7
3.2.3 Статус . . . 8
3.3 Мосты . . . 8
3.3.1 Регистрация . . . 8
3.3.2 Конкуренция . . . 9
3.3.3 Мостовой консенсус . . . 9
3.3.4 Распределение платежа . . . 9
3.4 Участвующие сети . . . 10
3.4.1 AION совместимые блокчейны . . . 10
3.4.2 Существующая сетевая совместимость . . . 11
3.4.2.1 Из AION в Ethereum . . . 11
3.4.2.2 Из Ethereum в AION . . . 11

4 БЛОКЧЕЙН AION-1 **12**
4.1 Высокоуровневый обзор . . . 12
4.2 Консенсус . . . 12
4.2.1 Определения . . . 13
4.2.2 Процесс подачи заявки на валидатор . . . 15
4.2.3 Распределение поощрений от валидатора . . . 16
4.2.4 Многоуровневый активный комплект . . . 16
4.2.5 Бэкинг . . . 16
4.2.5.1 Путём стэйкинга . . . 17
4.2.5.2 Путём решения . . . 17
4.2.5.3 Путём функций стэйков и решений . . . 17
4.2.6 Стимулы . . . 17
4.2.7 Репутация . . . 18
4.2.8 Доказательство интеллекта . . . 19
4.2.8.1 Механизм . . . 19
4.2.8.2 Валидация . . . 19
4.2.8.3 Пулинг . . . 19
4.3 Виртуальная машина Aion (AVM) . . . 20
4.3.1 Реализация . . . 20
4.3.2 Ограниченное потребление . . . 20
4.3.3 Блокчейн-ориентированная модель параллелизма . . . 21
4.4 Язык скриптов . . . 21
4.4.1 Спецификации . . . 21
4.4.2 Защитное программирование . . . 21
4.4.3 Операционная среда блокчейна . . . 22
4.4.4 Инъекция в контексте блокчейна . . . 22
4.4.5 Безопасность . . . 22

5 СТРАТЕГИЧЕСКИЙ ПЛАН **22**

5.0.1 Этап 1 23
5.0.2 Этап 2 23
5.0.3 Этап 3 23

6 ЗАКЛЮЧЕНИЕ **23**

7 КОНТАКТЫ **23**

Ссылки **25**

1 ВВЕДЕНИЕ

Повсеместная адаптация блокчейн систем была ограничена в связи с нерешенными вопросами масштабируемости, конфиденциальности и совместимости. Aion является первой многоуровневой блокчейн-сетью, разработанной для решения этих задач.

В основе нашей гипотезы лежит идея, что множество блокчейнов будут созданы для решения уникальных бизнес задач, возникших в уникальных индустриях. Сеть Aion спроектирована для поддержки индивидуальных блокчейн архитектур, в то же время предоставляя механизм для совместимых межцепных операций. В своей работе данный механизм не полагается на доверие. В основе этой системы лежит первый в мире специализированный корпоративный блокчейн: Aion-1. Aion-1 – это ультрасовременный блокчейн третьего поколения, который вводит новую парадигму надежности и справедливых, объективно представительных криптоэкономических стимулов.

Данная публикация:

- Представляет и объясняет сеть Aion – блокчейн-технологию следующего поколения и первую многоуровневую блокчейн-сеть – а также необходимую инфраструктуру и протоколы для её работы.
- Детализирует видение и технические концепты Aion-1, специализированного, общественного блокчейна третьего поколения и компонента в Aion сети.
- Предоставляет стратегический план будущих применений Aion-1 и сети Aion.

Эти концепты являются незавершенной работой. Данная публикация предназначена для установления намерений и носит исследовательский характер, а не декларативный. Присоединитесь к списку рассылки сети Aion , чтобы получать оповещения о последующих публикациях, относящихся к конкретным аспектам Aion, по мере того, как они становятся доступными.

2 ИСТОРИЯ

Ландшафт цифровых валют и относящихся к ним блокчейн-технологий значительно изменился с тех пор, как Биткойн был впервые введен в 2008 г.

2.1 Блокчейн первого поколения

Биткойн [1], как первое поколение блокчейн технологии, был лидером в создании многих альтернативных валютных платформ. Эти блокчейны первого поколения предоставляли решение для обычных транзакционных ограничений путем внедрения криптографически безопасных одноранговых цифровых транзакций, которые проверяются децентрализованной глобальной сетью и фиксируются в неизменном публичном регистре. Результатом являлась цифровая платформа, которая в то же время сохраняла экономику дефицита.

2.2 Блокчейн второго поколения

С появлением второго поколения блокчейна, Ethereum [2] представил возможность создание логики, специфичной для приложения, в блокчейн-сети. Это открыло новые возможности, выходящие за пределы финансовых транзакций, и позволило подключить состояние, бизнес логику, а также хранить и решать на блокчейне многопартийные контракты, и вести записи в неизменном регистре. Эти концепты были включены в другие технологии распределенных регистров и в результате привели к различию между “построением блокчейна” и “построением на блокчейне.”

Появление приложений, основанных на блокчейнах, благоприятно для индустрии. Приложения с новыми вариантами использования демонстрируют возможность блокчейн технологии развиваться не только как средство передачи ценностей, но и для решения широкого спектра других задач. Тем не менее, эти отдельные сети становятся разрозненными, так как они изолированы друг от друга и способны лишь передавать данные с цепи или передавать ценность через централизованные обмены. В каком-то смысле, экономические и индустриальные границы между крошечными государствами затвердевают. По мере роста численности сетей, индустрия становится более разъединенной и разбросанной.

Как и в период сразу после появления интернета, разрозненным блокчейн-сетям всё ещё предстоит по-настоящему осознать преимущества взаимосвязи. В то время как специализированные блокчейн-сети будут и должны быть разработаны, возможность взаимосвязи с другими сетями дает существенные преимущества, в особенности, если есть возможность сохранить конфиденциальность и масштабируемость. Механизм соединения разрозненных сетей будет представлять огромную ценность для каждой участвующей сети.

2.3 Aion: блокчейн третьего поколения

В будущем, блокчейны будут объединять данные и ценности в модели в виде колеса со спицами, схожей с интернетом. В будущем многие блокчейны будут все больше нуждаться в технологии, позволяющей взаимодействовать друг с другом и при этом сохранять собственную уникальную архитектуру - этой технологией станет Aion, который является интегрированной блокчейн-сетью, связывающей различные блокчейны.

Aion – это блокчейн сеть третьего поколения, которая позволит организации любого частного или государственного сектора: * **Объединять**: обмениваться данными и ценностями между любыми Aion-совместимыми блокчейнами и Ethereum. * **Масштабировать**: обеспечивать быструю обработку транзакций и повышенную ёмкость данных для всех Aion блокчейнов. * **Конструировать**: делать возможным создание индивидуальных общественных или частных блокчейнов, которые поддерживают совместимость и возможность работы с другими блокчейнами, при этом позволяя издателям выбирать управление, консенсусные механизмы, регулировать выпуск и участие.

В основе сети Aion лежит специально разработанный публичный блокчейн третьего поколения Aion-1. Предназначенный для того, чтобы связать другие блокчейны и управлять собственными надёжными приложениями, Aion-1 также предоставляет экономическую систему, которая стимулирует функциональную совместимость в экосистеме.

AION токены являются “топливом”, которое используется для создания новых блокчейнов, монетизации межцепочных мостов и защиты сети в целом.

3 МНОГОУРОВНЕВАЯ БЛОКЧЕЙН-СЕТЬ AION

Многоуровневая блокчейн-сеть Aion похожа на компьютерную сеть; она предоставляет протокол и стандарт для непохожих систем, чтобы они могли взаимодействовать. Однако, в дополнение к информации сеть Aion будет передавать логику и ценность среди участвующих блокчейнов с целью создания непрерывной цепи значений, в которой каждая транзакция происходит по цепи, причем логика и ценность передаются между цепями так же свободно, как и ликвидные активы.

Эти инфраструктуры, протоколы и концепты будут совместно работать, чтобы гарантировать передачу от источника до пункта назначения посредством межцепной связи. Ценность этих технологий заключается в том, что они позволяют одному блокчейну совершать транзакции с другим блокчейном; также они позволяют данному блокчейну совершать транзакции со всеми соединяющимися блокчейнами.

3.1 Соединяющиеся Сети

Соединяющиеся сети – это сети, которые упрощают межцепную связь и межцепные транзакции между множеством частных и публичных блокчейн-сетей. Соединяющиеся сети определяются требованиями, которые определяют их роль в контексте сети Aion. Соединяющиеся сети и межцепные транзакции предоставляют универсальный интерфейс, который позволяет блокчейн-разработчикам и пользователям отправлять информацию из одной сети в другую. В частности, соединяющая сеть должна предоставлять следующие основные технические возможности:

- Отправлять информацию между разными блокчейн-сетями с помощью общего протокола преобразования данных (протокола моста), включающий в себя перевод и распространение информации, которая должна считаться окончательной.
- Предоставлять децентрализованную подотчетность.
- Предоставлять протокол преобразования данных.

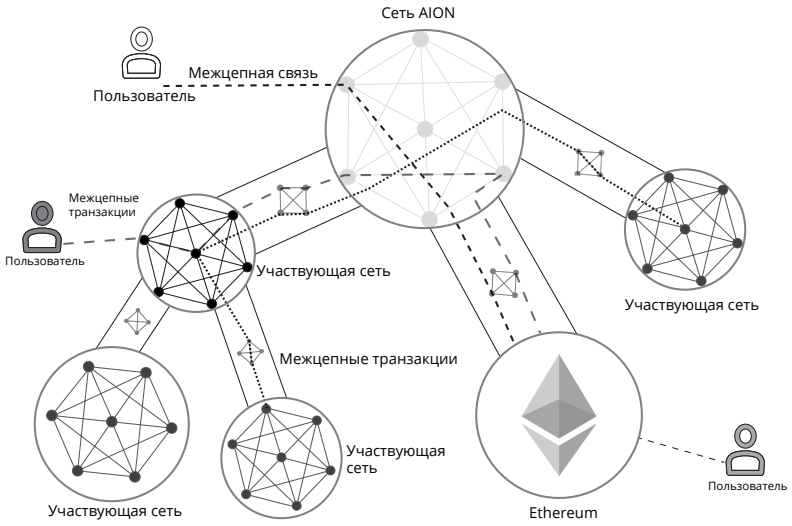

Figure 1: Пример простой многоуровневой блокчейн сети, состоящей из всех основных игроков.

Протоколы сети Aion устанавливают стандарты для внешних компонентов. В то время как фактическая функциональность и внутренние компоненты каждой соединяющейся сети могут варьироваться в зависимости от разработчика и заданной цели, эти основные функции должны быть реализованы.

Двухточечные связи, такие как межблокчейновые узлы, или специализированные сети, такие как BTC Relay, являются центральными концентраторами. Несмотря на то, что такие протоколы являются простыми и эффективными, они часто приводят к сложным государственным каналам, которые могут вызвать спорные ситуации и часто оказываются во власти одной избранной группы лиц, которая управляет сетями ретрансляции.

Вместо этого, соединяющая сеть использует межсетевые мосты и бездоверительную блокчейн-сеть для проверки и обеспечения точности следующих транзакций. Благодаря введению третьей стороны, которая занимается проведением информации из точки A в точку B, сетям больше не придется самим урегулировать сложные и непонятные ситуации.

3.2 Межцепная транзакция

Межцепная транзакция является бездоверительным сообщением между блокчейн-сетями; и является критическим компонентом инфраструктуры, обеспечивающим межцепную связь. С помощью межцепных транзакций любые соединённые блокчейн-сети могут обмениваться информацией, вроде компьютеров в интернете.

Межцепные транзакции первоначально создаются на основе блокчейна и затем передаются дальше соединяющимися сетями и мостами, прежде чем они окончательно достигают целевого блокчейна. Создатель межцепной транзакции должен уплатить транзакционный гонорар за расходы на связь используя AION токены, тем самым стимулируя всех участников на каждом соединении маршрута.

Межцепные транзакции являются в какой-то степени пакетными аналогами в том плане, что они указывают переходы, которые они должны выполнить на пути от источника к целевой сети, что потенциально означает переход через множество соединяющихся сетей.

3.2.1 Формат

В идеальном варианте, формат межцепной транзакции состоит из трёх частей:

- **Данные о полезной нагрузке**, различные для отдельных разработчиков и обычно являющиеся обычной обменной информацией, но которые потенциально могут распространяться на произвольные данные, по усмотрению создателя и исходной сети.
- **Метаданные** (“данные о данных”, примеч. переводчика) о межцепной транзакции, которая содержит информацию о маршрутизации и платежах.
- **Доказательство Меркла**, которое используется лишь когда отправитель хочет обойти мост.

Соединяющиеся сети и мостовые валидаторы должны проверять достоверность транзакции в целом, а не интерпретировать данные. При необходимости конфиденциальные информационные приложения могут сделать выбор шифровать данные.

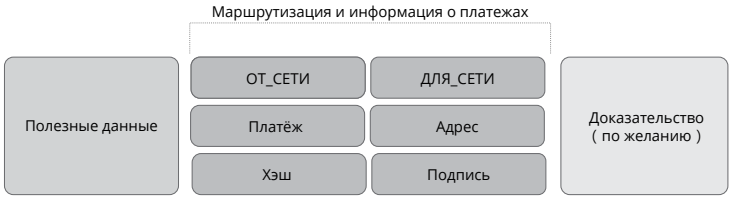

Figure 2: Визуальное представление межцепной транзакции

3.2.2 Маршрутизация

Маршрутизация межцепных транзакций – это многоуровневый процесс. На каждом уровне валидаторы проверяют информацию и принимают решение относительно того, должна ли транзакция быть проведена или отвергнута.

Траекторию маршрутизации можно разделить на две субтраектории: цепь прямой передачи и цепь обратной передачи. В цепи прямой передачи межцепная транзакция переходит от цепи-источника до цепи-назначения. В цепи обратной передачи подтверждение межцепной транзакции передается назад.

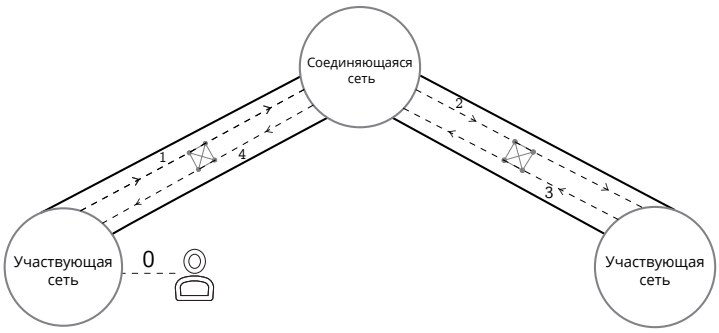

Figure 3: Изображение жизненного цикла ICT, начиная с цепи A и заканчивая подтверждением.

Если по какой-то причине мост отказывается проводить межцепную транзакцию, отправитель может принять решение пропустить межцепную транзакцию, в том числе и доказательство, и сразу перейти к соединяющейся цепи. Та, в свою очередь, признает действительной межцепную транзакцию исходя из своего знания о хэш цепи Меркла участвующей сети и проведёт её, если та окажется действительной.

Дизайн межцепной транзакции всё ещё находится на рассмотрении. По мере развития проекта будет опубликована подробная работа, посвящённая межцепным транзакциям.

3.2.3 Статус

Статус межцепной транзакции был введен в употребление с целью представления различных статусов транзакции с точки зрения соединяющихся сетей.

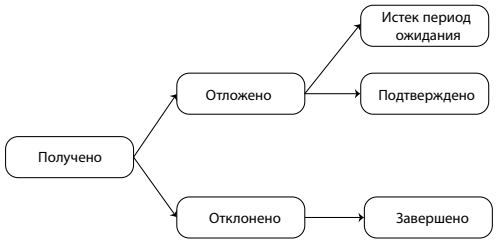

Figure 4: Схема возможных статусов, которые могут появиться за время жизненного цикла ICT

- Статус изменяется на “получено”, когда межцепная транзакция впервые замечена мостовыми валидаторами в участвующей цепи.
- В случае, если более двух третьих мостовых валидаторов голосуют “да” в отношении межцепной транзакции, соединяющая сеть изменит статус межцепной транзакции на “приостановлено”, что, в свою очередь приведёт к тому, что соответствующий токен соединяющейся сети будет заблокирован до тех пор, пока транзакция не будет завершена.
- В случае, если менее двух третьих мостовых валидаторов голосуют “да” в отношении межцепной транзакции, статус изменяется на “отклонено”.
- Транзакция со статусом “приостановлено” перейдёт к мостовым валидаторам, которые по пути свяжут соединяющуюся сеть со следующими блокчейнами.
- Как только подтверждение получено, статус изменяется на “подтверждено”.
- В случае, если подтверждение не получено, статус изменяется на “истёк период ожидания”.
- Для подтвержденных межцепных транзакций статус изменяется на “завершено”, и все заблокированные гонорары распределяются в соединяющуюся сеть и мостовые валидаторы.

3.3 Мосты

Мост – это протокол связи, который обеспечивает связь между участвующими сетями и соединяющимися сетями. Мост состоит из своей собственной сети валидаторов. Эта сеть гарантирует перевод протоколов и отчётность между сетями. Мосты задают направление. Блокчейн-исходник – это цепь, в которой транзакции выпускаются (распространяются), в то время как блокчейн-цель - это цепь, в которой транзакции переправляются.

У моста есть две основные задачи:

- Подписание и трансляция (передача) межцепных транзакций только в том случае, если они были скреплены в блокчейн-исходнике и платеж за переправление межцепной транзакции был осуществлён.
- Информирование соединяющихся сетей об обновлениях хэша Меркла в участвующих сетях.

Мостовые валидаторы используют алгоритм, основанный на BFT* (BFT протокол: протокол передачи данных в двоичной форме; примеч. переводчика), чтобы достичь консенсуса. Транзакции подтверждаются только тогда, когда две трети общих голосов будут получены и взвешены.

3.3.1 Регистрация

Соединяющиеся сети являются ответственными за регистрацию их прямоподключённых мостов. Специализированная таблица валидаторов, сортированная по долям, будет поддерживаться на блокчейне для каждого моста. Кто угодно может присоединиться к публично доступному мосту посредством залога доли. В частности, существует контракт (протокол), целью

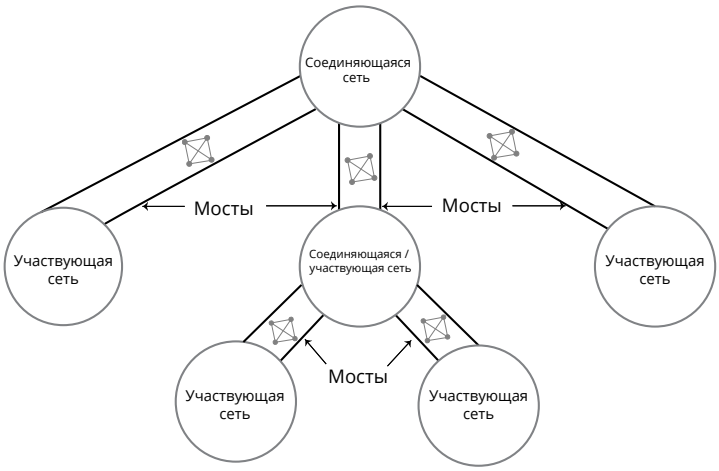

Figure 5: Общий обзор мостов, связывающих сетевые взаимоотношения

которого является поддержка глобальной мостовой регистрации, которая динамично обновляется по мере того, как узлы (nodes) присоединяются или покидают мостовые сети.

Для того, чтобы мост был действующим, необходима минимальная итоговая (общая) доля. Только ведущие валидаторы смогут участвовать в мостовом консенсусе.

3.3.2 Конкуренция

Когда многочисленные валидаторы регистрируются на одну блокчейн-сеть с помощью разных идентификаторов, может быть сгенерировано множество мостов. С точки зрения соединяющейся сети, эти мосты – отделенные, несмотря на то, что они распространяют и получают информацию в рамках одной и той же сети.

Выбор моста для работы в таком случае осуществляется пользователем с помощью определения идентификации целевой сети. В данном случае целью является введение свободного рынка путем побуждения различных мостовых сетей к конкуренции с точки зрения стабильности, репутации и ценообразования с целью установления оптимальной величины гонорара, обусловленной рыночными требованиями.

3.3.3 Мостовой консенсус

Консенсус достигается мостовыми валидаторами с помощью использования упрощенного протокола, основанного на BMT. В этом случае транзакции обрабатываются за один раунд вместо нескольких раундов. Каждый валидатор анализирует транзакцию исходя из его представлений о предыдущем блокчейне. Если две трети или более валидаторов голосуют “да”, то межцепная транзакция признается действительной. Тогда следующий блокчейн тоже признает транзакцию действительной.

Начиная с первичного статуса мостовой валидатор должен ждать до тех пор, пока он не получит межцепную транзакцию. Затем он должен проверить достоверность подписи и платежа за транзакцию. Исходя из результатов этой проверки валидатор либо исключает (не подписывает) транзакцию, либо подписывает и далее распространяет её в соединяющуюся или целевую сеть

3.3.4 Распределение платежа

Мостовые валидаторы получают гонорары за счёт платежей за межцепные транзакции и потенциально за счет вознаграждений за блок. Цель распределения вознаграждения - справедливая политика распределения.

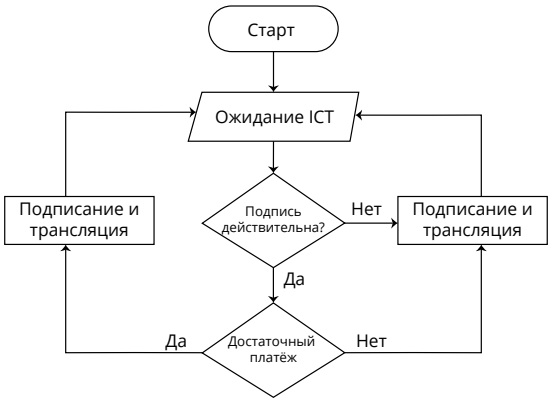

Figure 6: Алгоритмический график поведения мостового валидатора

На внутреннем уровне все платежи, проходящие через мост, распределяются на мостовые валидаторы. Это может быть сделано либо пропорционально ставке (доле), которую каждый валидатор поставил на мост, либо в равной степени вне зависимости от ставки.

На внешнем уровне мосты разделяют платежи с соединяющимися сетевыми валидаторами, а также между собой за транзакции на маршрутном пути.

Существуют две возможные модели распределения внешних платежей:

- Отправитель межцепной транзакции уточняет, как платежи будут распределены между мостами и соединяющимися цепями. Преимущество этого подхода заключается в том, что у пользователей есть возможность оптимизировать платежи исходя из нагрузки моста и минимальных ставок. Недостаток заключается в том, что перед отправкой транзакции пользователям необходимо базовое понимание маршрутизации и требований к оплате для каждого моста.
- Отправитель уточняет лишь общий платёж, и соединяющаяся сеть разделяет этот платеж исходя из соглашений жестко закодированного протокола. Преимущество этого подхода состоит в том, что так проще для пользователя. Недостаток состоит в том, что изменение соотношения между мостом и соединительной сетью происходит медленно и сложно.

3.4 Участвующие сети

Один из основных концептов в архитектуре сети Aion заключается в том, что она предназначена для федерирования совместимых блокчейнов или связанных с блокчейнами сетей. Это могут быть целенаправленные блокчейны, частные сети или блокчейны консорциумов, представляющие коллекции субъектов. Независимо от контекста взаимосвязь и способность взаимодействовать друг с другом эффективным, безопасным и несложным образом увеличивают ценность каждой сети в отдельности, а также обеспечивают стабильность для блокчейн-экосистемы в целом.

Участвующей сетью является любая сеть, которая успешно выполнила требования для интеграции с соединительной сетью. Учствующие сети должны быть блокчейнами, но не обязательно. Некоторыми полезными участниками могут быть оракулы, криптлеты [3], или кластеры баз данных, нуждающиеся в проверяемой информации. Единственное ограничение - это гибкость участвующей сети для интеграции с соединяющейся сетью. После интеграции с сетью Aion участвующие сети получают доступ к протоколу связи (Межцепная транзакция) оговоренному ранее. Это предоставляет многочисленные варианты использования.

Участвующие сети имеют полноценную гибкость в настройке различных модулей своей инфраструктурной цепочки, включая алгоритм согласования, алгоритм хэширования, виртуальную машину (VM) и скриптовые языки.

3.4.1 AION совместимые блокчейны

Aion-совместимые блокчейны – это участвующие блокчейны, которые соответствуют протоколу Aion, и на которых могут быть легко установлены мосты для пересылки межсетевых транзакций через Aion-1.

Для того, чтобы быть совместимым с Aion, блокчейн должен отвечать определенным требованиям. Среди прочего, он должен:

- В какой-то мере быть децентрализованым и поддерживать процедуры, которые обычно встречаются в таких блокчейнах, такие как атомарная передача и транзакции. Точная реализация остается на усмотрение мостового протокола и самой сети.
- Уметь распознавать межцепные транзакции и отличать их от обычных транзакций.
- Знать протокол консенсуса, используемый мостом, и сохранять информацию о транзакции, признанной действительной.
- Внедрять период блокировки или аналогичную функцию, позволяющую сети удерживать токены в течение определенного периода времени.

Трейдеры Блокчейна смогут адаптировать свои предложения к Aion и сделать их Aion-совместимыми. Инфраструктура блокчейна Nuco станет одной из первых сетей, совместимых с Aion.

Более конкретные детали о требованиях будут опубликованы по мере развития проекта.

3.4.2 Существующая сетевая совместимость

В отличие от совместимых с Aion блокчейнов, существующие блокчейны не предназначены для взаимомсвязи. Для того, чтобы запустить межсетевую маршрутизацию транзакций между сетью Aion и существующими блокчейнами, требуются дополнительные предположения и / или компромиссы. В этом разделе мы обсудим возможность подключения блокчейна Ethereum к сети Aion.

3.4.2.1 Из AION в Ethereum

В рамках мостового протокола валидаторами используется простой консенсусный алгоритм на основе BFT. В соединяющихся сетях эти BFT голоса изначально агрегируются и обрабатываются блокчейн валидаторами. Блокчейн Ethereum не имеет таких встроенных функций, поэтому для этого ему необходим межсетевой транзакционный контракт.

В этой модели межсетевой транзакционный контракт будет периодически синхронизировать публичные ключи мостовых валидаторов в зависимости от спецификации сети Aion. Когда запрашивается межцепная транзакция, валидаторы моста подписывают для нее свой секретный ключ и отправляют подпись в межсетевой транзакционный контракт. Тот, в свою очередь, соберет все голоса (подписи) и предоставит проверяемый отчет о событии, которое содержит данные межсетевых транзакций и информацию о голосовании. В случае, если получено не менее двух третьих голосов, валидаторы моста будут использовать этот отчет в качестве доказательства при подтверждении межцепной транзакции. Поскольку расчетная стоимость проверки нескольких подписей в блокчейне Ethereum высока (3000 gas за один ECDSA), можно ожидать более высокие мостовые платежи. Чтобы уменьшить эту стоимость, блокчейн с полной функциональностью BFT может использоваться в мосте, и только результат голосования будет сохранен на блокчейне Ethereum.

3.4.2.2 Из Ethereum в AION

Отправка межцепных транзакций из блокчейна Ethereum в сеть Aion более упрощённая благодаря программируемому размеру транзакций Ethereum. Транзакции, предназначенные для других блокчейнов, должны включать информацию о маршрутизации в поле данных.

Существует два возможных сценария, которые могут возникнуть в результате межцепной транзакции Ethereum (межсетевая транзакция из блокчейна Ethereum в сеть Aion), в зависимости от адреса получателя. Если транзакция отправляется во внешнюю учетную запись, то поле данных можно использовать без изменений. Если транзакция отправляется на контрактную учетную запись, потребуется обходное решение, так как данные также интерпретируются виртуальной машиной Ethereum. Одним из решений было бы добавление магического тега транзакции и маршрутизация информации к исходным данным, только в случае если логика контракта не полагается на операционный код `CALLDATASIZE`.

Чтобы обеспечить завершение транзакции, мост может потребовать дополнительные подтверждения блока. Обычно крупные обмены используют 120 (полчаса) для уверенности в транзакции.

4 БЛОКЧЕЙН AION-1

Блокчейн Aion-1 является генезисной реализацией соединяющейся сети. Он спроектирован как справедливая, распределенная, открытая блокчейн-архитектура, способная выполнять требования, указанные в многоуровневой сетевой блокчейн-архитектуре.

Aion-1 в качестве открытого блокчейна был разработан для следующих целей:

- Соединить блокчейны и внешние службы (такие как оракулы и базы данных) через непрерывную сеть и обеспечить отчетную связь, поддерживаемую через децентрализованную сеть.
- Предоставить необходимую инфраструктуру для разработки высокоэффективных, децентрализованных, межблокчейновых приложений.
- Создать поддерживаемую сеть с помощью надежной и устойчивой экономической модели.

Пользователи смогут задействовать смежные участвующие сети, подходящие для своих собственных потребностей, и общаться с другими сетями через подотчетную архитектуру маршрутизации. К участию приглашаются все желающие, от крупных предприятий, занимающихся ассоциативными сетями, до общественных открытых сетей. В будущем децентрализованные приложения смогут находиться на вершине соединительной сети с логикой, основанной на интеграции данных из множества блокчейн сетей.

В дополнение, блокчейн Aion-1 оснащен полностью функционирующей экономической системой, предназначенной для обеспечения непрерывного обслуживания и целостности сети.

4.1 Высокоуровневый обзор

В данном проекте Aion-1 ссылается на генезис и внедрение соединяющейся сети. Реализация Aion-1 также служит полностью функциональной блокчейн-архитектурой, сопоставимой с новейшими решениями на сегодняшнем рынке. Мы представляем Aion-1 стандартизованным шаблоном, который предоставляет строительные блоки для будущих сетевых реализаций. Ключевыми составляющими блокчейна Aion-1 являются:

- **Консенсус** Он будет использоваться для реализации предлагаемой архитектуры соединения двух или более блокчейнов. Два варианта протокола BFT будут разработаны для достижения консенсуса по мосту и соединяющейся сети:
  - **Мостовой консенсус** , являющийся простой вариацией, позволяющей быстро достичь консенсуса на мосту.
  - **Консенсус соединяющейся сети**, являющийся консенсусным протоколом, направленным на обеспечение стабильности в требуемом масштабе.
- **Виртуальная машина Aion (AVM)** Она представляет собой настраиваемую, простую, эффективную и стабильную виртуальную машину, которая использует ключевые характеристики виртуальной машины Java (JVM), обеспечивая параллелизм и надежность в контексте, специфичном для блокчейна. AVM отвечает за запуск приложений поверх Aion-1. AVM будет включать в себя собственный скриптинг язык (подробности далее).

4.2 Консенсус

Для начала мы рассмотрим алгоритм консенсуса, представленный в Aion-1, для решения требований, предъявляемых концепцией соединяющейся сети. Выбранный консенсусный алгоритм должен поддерживать консенсус блокчейна как для транзакций по цепи, так и для межсетевых транзакций. Чтобы эффективно и точно выполнить эти требования, Aion-1 использует консенсусный алгоритм, основанный на BFT (см. “Задача византийских генералов”).

(BFT) алгоритм соединился с гибридным протоколом, целью которого является справедливое представление обеих сторон в бэкинге (поддержке) - частично через систему токенов, и частично - через новый алгоритм проверки, основанный на концептах, используемых в современных нейронных сетях, называемых “доказательством интеллекта“.

Чтобы соответствовать масштабам работ и обеспечить широкое участие в процессе проверки сети, Aion-1 будет использовать модель репрезентативной валидации, похожей на делегированную модель, разработанную командами BitShares [4] и Lisk [5]. Эта модель валидации позволит участникам сети Aion вернуть валидаторы, которые активно участвуют в процессе консенсуса, что позволит резко увеличить участие, которое будет выше технически разрешенного обычными алгоритмами BFT. Специфика протокола на основе BFT ещё не доработана, но она гарантирует стандартные свойства жизнеспособности и безопасности.

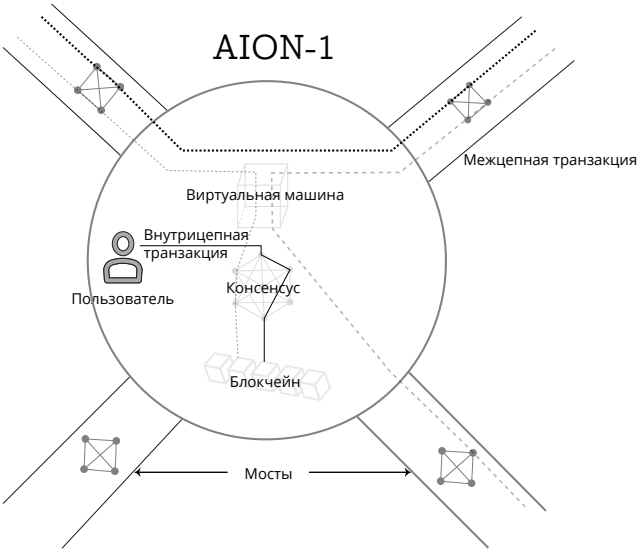

Figure 7: Взгляд издалека на архитектуру AION-1. На диаграмме изображены важнейшие компоненты сетей: соединяющаяся сетевая структура, состоящая из протокола консенсуса и приложений, построенных поверх виртуальной машины.

Данные предположения дополняются репрезентативным подходом к выбору, в том плане, что сеть должна быть стимулирована для выбора оптимальных и правильных валидаторов. Мы исследуем несколько реализаций, включая HoneyBadger [6], Tangaroa [7] и Stellar [8]. Особый интерес вызывает поведение предложений в HoneyBadger и протоколы голосования в Stellar и Tangaroa.

Концептуальная архитектура репрезентативной сети валидации аналогична концепции представительной демократии, в которой кандидаты могут регистрироваться на выборах и избираться на основе голосов, которые они получают от своих избирателей. Однако в этой системе валидаторы должны поддерживаться бэкерами, и каждый бэкер получает часть гонорара. В основе такой архитектуры лежит вера в самоуправление сети, в которой коллективные действия напрямую влияют на безопасность сети посредством надлежащего голосования.

Предложенный консенсусный протокол состоит в том, что каждый узел в сети может представлять себя кандидатом и заверять другого кандидата в бэкинге. В начале каждого периода валидаторы избираются из наиболее подходящих кандидатов. Эти валидаторы вносят вклад в процесс генерации блоков с помощью протокола на основе BFT и получают за это распределенные вознаграждения блоков. Это продолжается до конца периода, затем начинается следующий период, который перезапускает процесс.

4.2.1 Определения

Чтобы обеспечить контекст для различных аспектов репрезентативного консенсуса, обращайтесь к следующему набору определений, которые последовательно используются во всей остальной части документа:

- **Номинация** это процесс, с помощью которого узел может зарегистрироваться, чтобы стать валидатором для участия в представительном консенсусе на Aion-1. Номинация должна быть завершена до того, как любые другие пользователи сети смогут пообещать кураторство.
- **Ранговый список** используется для определения назначенных валидаторов с максимальной поддержкой. Этот список становится активным, что означает, что узел валидатора может внести свой вклад в консенсусный процесс.
- **Активный набор** это многоуровневый список активных валидаторов. Другими словами, это количество валидаторов в активном наборе.
- **Резервные сэты** (наборы) состоят из активных кандидатов-валидаторов, но не тех, что находятся в активном сэте. Резервный сэт - это следующие наиболее важные поддерживаемые валидаторы, с наибольшим бэкингом. В случае злонамеренного поведения или бездействия сеть обращается к этому набору для замены валидаторов.
- **Бэкеры** это узлы, которые поддерживают валидаторов. В сети будет больше бэкеров чем валидаторов, и их участие

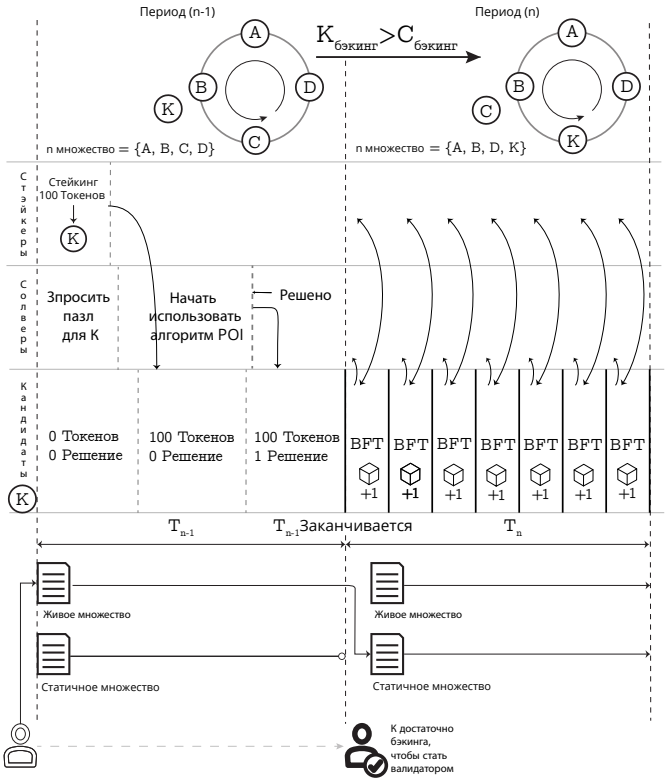

Figure 8: Активное / статичное множество и Staking Lifecycle, демонстрирует процесс проверки достоверности кандидата, присоединяющегося к консенсусу.

напрямую влияет на ранг валидаторов в активном наборе. Кроме того, бэкеры пропорционально вознаграждаются на основании гонораров их валидаторов. Бэкеры состоят из двух отдельных групп: стэйкеров и солверов (решателей).

- **Стэйкеры** это пользователи, которые закладывают токены валидаторам в качестве поддержки и являются подгруппой бэкеров.
- **Стэйки** (ставки) – это фиксированное количество токенов, удерживаемых сетью до заранее определённого времени, когда они возвращаются обратно к стейкеру.
- **Солверы** (решатели) - это пользователи, которые используют "доказательство интеллекта" для решения криптографической головоломки, заданной сетью. Затем "доказательство интеллекта" преобразуется в бэкинг. Солверы - это подгруппа бэкеров.
- **Периоды** представляют собой определенную продолжительность времени, когда статический набор используется сетью для целей консенсуса на основе BFT. В каждом периоде статический набор валидаторов проверяет новые блоки. В конце каждого периода активный набор блокируется для создания нового статического набора, основанного на изменениях ставки.

4.2.2 Процесс подачи заявки на валидатор

Любой узел может самостоятельно самономинироваться и регистрироваться, чтобы стать валидатором, но для этого требуется достаточная поддержка для активной проверки на Aion-1. Между периодами, сеть поддерживает и обновляет сетевой репозиторий кандидатов-валидаторов и контракт на номинацию.

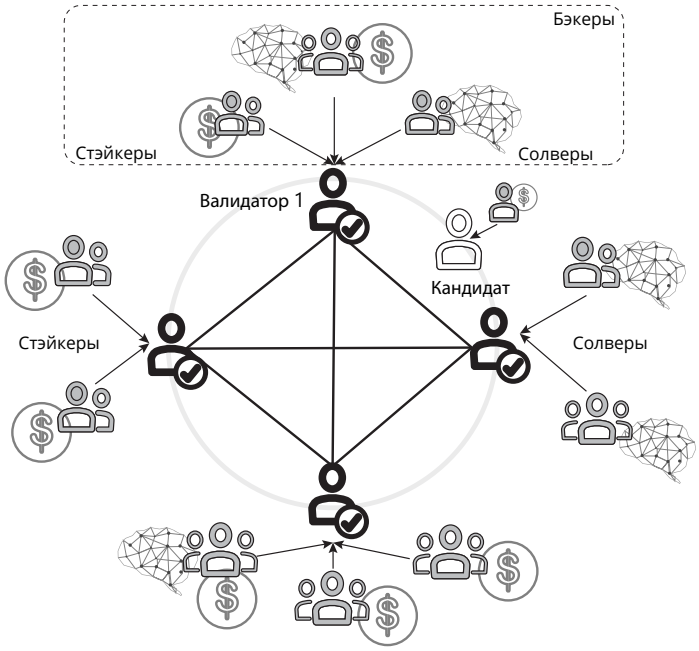

Figure 9: Структурное представление репрезентативного голосования - диаграмма представляет активный набор, где каждый валидатор поддерживается несколькими пользователями либо путем стэйкинга, либо путём солвинга. Также изображен валидатор-кандидат – это валидатор, который не имеет достаточной поддержки для присоединения к активному набору.

Валидаторы становятся активными с помощью непрерывной поддержки сети. Члены активного сэта всегда являются кандидатами с наивысшим приоритетом. Два экземпляра контракта на номинацию находятся в постоянной доступности, чтобы облегчить этот непрерывный процесс поддержки. Живой набор обновляется по мере того, как сетевые пользователи возвращаются или выводят свою поддержку от кандидатов, а статический набор существует только на время действия этого периода. Консенсусный протокол получает свой активный набор из статического набора. В конце каждого периода статический набор перезаписывается живым набором в течение следующего периода.

Валидаторы смогут установить, как награждаются их бэкеры. Таким образом, валидатор предлагает условия его поддержки и, если эти условия приемлемы, бэкеры будут передавать ресурсы этому валидатору. Данная схема поддерживает баланс влияния,

так как ранг (как и последующий процесс вознаграждения) активного валидатора зависит от суммы его бэкинга по сравнению с другими валидаторами.

Также существует механизм репутации для узлов валидатора. Валидаторы кандидатов могут использовать свою репутацию как способ привлечения первоначального бэкинга. Конкретные особенности репутации находятся на рассмотрении; они будут количественными, измеримыми и четко определенными. Цель состоит в том, чтобы побудить всех участников рассмотреть возможность стать кандидатами-валидаторами, в дополнение к использованию сети Aion-1 по причинам ее выгодности.

4.2.3 Распределение поощрений от валидатора

Все пользователи должны предъявить сети определенную долю (стейк), чтобы считаться кандидатом-валидатором. Однако вознаграждения валидатора не обязательно пропорциональны их ставке. Вместо этого, соотношение вознаграждений, направляемых валидатору и бэкерам, предлагается валидатором во время предложения к контракту на номинацию. Идея заключается в том, чтобы сторонники и валидаторы кандидатов пришли к некоторой рыночной стоимости, на которую согласны обе стороны.

4.2.4 Многоуровневый активный комплект

Валидаторы будут организованы в многоуровневую структуру внутри активного набора. Многоуровневая структура оценивается на основе поддержки, в порядке убывания, от максимально поддерживаемого валидатора до самого низкого в ранге. Каждый уровень дополнительно стимулирует добродетельное поведение, предоставляя более высокую награду в качестве компенсации. Идея состоит в том, чтобы стимулировать децентрализацию путем введения точки равновесия с точки зрения затрат и выгод для централизованной поддержки, тем самым стимулируя бэкеров диверсифицироваться.

Мы убеждены в том, что этот проект будет стимулировать оптимизацию и добродетельные действия посредством взаимодействия между участниками. Валидаторы будут комментировать, чтобы получить более высокий бэкинг, а бэкеры в свою очередь получат поддержку от валидаторов, но только до тех пор, пока они не будут лучше компенсированы путем диверсификации их поддержки, включая поддержку неактивных валидаторов. Одна потенциальная схема распределения вознаграждения представлена ниже.

Table 1: Таблица показывает размер премии(%) и мощность голоса (%) приходящиеся на индивидуального валидатора данного уровня. Допуская, что

Уровень	Валидаторы	Премии/Валидатор	Мощность голоса/Валидатор
1	10	2.5%	1%
2	20	1.25%	1%
3	30	0.83%	1%
4	40	0.625%	1%

Согласно схеме вознаграждения, показанной в таблице, вознаграждения распределяются поровну между уровнями (25%), а затем распределяются среди всех валидаторов на этих уровнях. Валидаторы в более высоких уровнях имеют более высокие пропорциональные вознаграждения из-за ограниченного размера уровня. Заранее определенная награда представляет для бэкеров экономическую модель для оценки альтернативных затрат на поддержку валидаторов, тем самым стимулируя бэкеров распределять свои доли между несколькими валидаторами (процесс децентрализации) или даже назначать себя валидаторами. Точная модель и структура мотивации будут проходить тщательное симуляционное тестирование.

4.2.5 Бэкинг

Бэкинг ссылается либо на стэйкинг токенов, либо на доказательство интеллекта в отношении конкретного валидатора. Сеть спроектирована в виде гибрида, который подчеркивает двойственность сторон для равномерного распределения мощности и денежной стоимости по всей сети. Мы верим в то, что сеть, основанная исключительно на стэйкинге (доказательство доли),

создает централизацию денежной величины в рамках отдельной группы лиц. Таким образом, подчеркивается возможность для другого класса пользователей, класса, который не обладает денежной величиной для участия в стэйкинге с целью внесения вклада в сеть.

Алгоритм бэкинга разбит на две различные категории:

- Бэкинг путём стэйкинга
- Бэкинг путем решения

Эти два фактора объединяются для создания поддержки, концептуального промежуточного значения, используемого для определения ранга валидатора, а также доли вознаграждений, предоставляемых бэкеру. В следующих разделах описывается каждый алгоритм и исследуется корреляция между этими тремя переменными.

4.2.5.1 Путём стэйкинга

Бэкинг осуществляется через токены путем стэйкинга токенов для конкретного валидатора. В течение одного периода пользователь может сделать ставку (stake) к определенному валидатору в пределах +1. Следствием является то, что токены передаются сетью до конца +1, и в этот момент токены возвращаются к пользователю (при условии, что никаких вредоносных действий не произошло). До этого пользователь может отправить другое сообщение, указывающее, что пользователь хотел бы, чтобы токены оставались закрепленными за одним и тем же валидатором.

Обновление ставки означает, что бэкер сохраняет ставки с помощью валидатора. В этом случае концепция “чеканки монет”, где ставки имеют половину жизни, может быть полезным механизмом. Это будет стимулировать ликвидность и поддерживать конкуренцию между валидаторами. В обмен на стэйкинг, бэкер получает часть вознаграждения валидаторов. Вознаграждение пропорционально количеству ставок, а также текущему уровню валидатора.

4.2.5.2 Путём решения

Другая форма поддержки выполняется путем решения криптографической головоломки, подробности которой объясняются в [доказательстве интеллекта][Proof of intelligence]. Уникальная головоломка создается для каждого запроса, и головоломка должна быть решена с помощью алгоритма доказательства интеллекта для создания доказательства интеллекта. Затем доказательство подается в сеть в качестве доказательства количества поддержки для конкретного валидатора. Солверы (решатели) также вознаграждаются пропорционально бэкинг-сумме.

4.2.5.3 Путём функций стэйков и решений

Чтобы стимулировать гибридную сеть, необходимо определенное распределение ставок и доказательство интеллекта. В настоящее время это соотношение условно рассчитано на 60/40 для ставок и доказательств соответственно. Общая сумма акций и решений накапливается за период, а коэффициент поддержки для сети корректируется до тех пор, пока он не будет соответствовать ожидаемому коэффициенту. Поэтому, ситуация, в которой доля больше, чем ожидаемое соотношение, приводит к более низкому бэкингу на ставки / доказательство интеллекта и имеет меньшую долю, чем ожидалось, в большей степени бэкинга.

4.2.6 Стимулы

Предлагаемая система предназначена для того, чтобы препятствовать недобросовестным участникам или действиям. Однако некоторые вредоносные события могут произойти. В таких случаях валидатор будет понижаться по уровням или окажется удалён из активного набора, тем самым предотвращая его участие в консенсусе и аннулируя любые вознаграждения для себя и своих бэкеров.

Чтобы препятствовать злонамеренным бэкерам, последствия контролируются с помощью их метода бэкинга. Последствия, налагаемые сетью, предназначены для устранения возможностей вознаграждения, а не наказания путем удаления или перераспределения ставок между другими валидаторами. Таким образом, этот механизм устраняет выигрыш в формате “всё или ничего”, где чья-то потеря непременно является чьим-то выигрышем. Вместо этого он выравнивает мотивации и поощряет благотворные коллективные действия. Мы верим, что с помощью этой системы индивидуум понимает последствия своих

действий, поэтому у него есть стимул действовать добродетельно и согласовано с другими добродетельными участниками. Плохие участники будут идентифицированы сетью, а благодаря уменьшению репутации и поддержки валидатора они немедленно получат замечание и предпримут корректирующие действия, или же будут удалены из активного набора.

Table 2: Эффект предлагаемой системы наказания, главный представитель является двуличным и исключен из консенсуса. Все остальные представители сдвинутся наверх, и кандидат станет представителем.

Активные участники набора	Предыдущий уровень	Новый уровень
1	1	Удалён
2	2	1
3	3	2
4	4	3
конец активного набора		
5	Кандидат	4

- **Дублицируемые действия** наказываются путем блокировки всех ставок, представленных валидатором, в течение определенного периода времени и немедленного удаления валидатора из консенсуса. Бэкеры валидатора наказываются в зависимости от метода, которым они его поддерживают. Стэйкеров наказывают за то, что они блокируют свои ставки в течение длительного времени. Солверы наказываются удалением валидатора из консенсуса, тем самым делая их решения о неверности доказательств недействительными.
- **Неактивность** валидатора в течение определенного периода времени наказывается понижением рейтинга валидатора в уровневой системе. Если неактивный валидатор находится на самом низком уровне, он сразу же сбрасывается с консенсуса.

Валидаторы замены (в следующий высшем ранге) являются доступными и сразу будут перенесены в консенсусный процесс до конца периода.

4.2.7 Репутация

Представительский консенсус оставляет за собой ответственность за выбор оптимальных узлов валидатора в сети. Этот процесс тяжело достичь без механизма для сети, который позволяет наблюдать за прошлым поведением кандидатов и активных валидаторов. Один из вариантов - полагаться на внешнюю статистику для выбора оптимального кандидата. Однако это бы являлось стимулом для манипулирования этими данными. Поэтому в сети должна быть создана система репутации, в которой прошлые действия и статистика узла являются частью сетевого протокола, предоставляя надежные данные, чтобы пользователи могли выбирать подходящих им кандидатов. Некоторые функции, которые могут быть включены в репутацию узлов, включают:

- **Срок службы** это время, в течение которого узел был активен в сети и имеет важное значение при определении возраста (и, следовательно, надежности) узла.
- **Общий бэкинг** общая или суммарная величина бэкинга, полученная до этого момента, которая суммируется на конец периода (так как ставки блокируются в течение этого времени) и может указывать прошлую производительность для узла.
- **Центральность** используется в том же контексте, что и в социальной сети. Она указывает, какие узлы лучше других связаны внутри сети, и может служить хорошим показателем надежности и производительности.
- **Источник транзакции** относится к первому экземпляру транзакции, появляющейся в сети (которая была принята блокчейном) и может быть легко рассчитана с требованием, чтобы узлы подписали транзакции, которые они производят.
- **Сетевое доверие** это глобальная сетевая ценность для конкретного однорангового узла, которая указывает на удовлетворительное поведение этого узла с точки зрения сети. Концепт был первоначально разработан для систем обмена файлами P2P [9], и имеет алгоритм, который можно адаптировать для рассмотрения параметров, имеющих отношение к нашему варианту использования.

Эти статистические данные свободно доступны для пользователя. Будут приложены все усилия, чтобы эти статистические данные стали легко доступными через Интернет.

Такая система создает хорошо осведомленную базу пользователей, которая необходима для формирования основы демократической сети.

Наконец, система репутации является механизмом, который иллюстрирует инвестиции узла в сеть. Эти инвестиции зависят от добродетельных или злонамеренных действий узла и эффективны при оценке риска бэкинга.

4.2.8 Доказательство интеллекта

Доказательство интеллекта - это экономическая мера для предотвращения атак на отказ в обслуживании, требуя от участников, солверов в Aion-1, выполнить вычисления искусственного интеллекта (AI). Цель состоит в том, чтобы мотивировать создание AI-специального или специализированного оборудования, которое может быть использовано для машинного обучения и обучения нейронной сети в будущем.

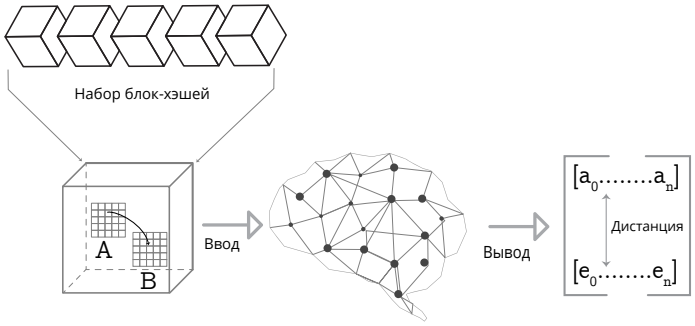

Figure 10: Обзор “Доказательства интеллекта”

4.2.8.1 Механизм

Доказательство интеллекта работает, требуя от участников обучать предопределенную нейронную сеть, чтобы она выдавала аналогичные результаты предполагаемой истине (например, хеш текущего блока, учитывая хэши предыдущих блоков в качестве входных данных). Параметры обученной нейронной сети будут служить доказательством того, что расчеты проводились и их легко проверить, введя параметр и подтвердив результаты.

4.2.8.2 Валидация

Проверка доказательства проходит быстрее в сравнении с учебным процессом и выполняется в следующих этапах:

1. Загрузите нейронную сеть согласно определенному предоставленному параметрическому вектору.
2. Поддержите нейронную сеть хэшами предыдущих блоков.
3. Запустите и соберите выводимые данные.

Процесс проверки исследуется и развивается.

4.2.8.3 Пулинг

Пулинг (сбор) доказательств интеллекта достигается путем разделения пространства параметров на подпространства. Похожим на пулинг является концепт доказательств работы, где каждый майнер работает в диапазоне nonce-пространства, солверы доказательств интеллекта работают независимо на подпространстве параметра. Они разделяют доказательства и вознаграждение блока.

4.3 Виртуальная машина Aion (AVM)

Архитектура AVM создана как решение, ориентированное на блокчейн с акцентом на производительность, детерминизм и надежность. AVM - это индивидуальная простая реализация JVM, адаптированная к выполнению логики цепи (логики приложения) в распределённых сетях и защищенная от сценариев, возникающих в такой среде.

AVM обеспечивает инфраструктуру для одной из основных функциональных возможностей соединительной сети, позволяя абстрагироваться между блочной цепью и конкретной логикой приложения и прокладывать путь к мощным межцепным приложениям. В следующих разделах приводятся обоснования этого выбора дизайна и другие доводы.

4.3.1 Реализация

В основе архитектуры AVM лежит простой, удобный для машин, блокчейн-специфический байткодовый интерпретатор, после тщательного рассмотрения практических и технических задач. Для реализации необходимы:

- **Производительность** близкая к родной, с использованием набора удобных для пользователя инструкций.
- **Устойчивость** AVM, которой можно достигнуть с помощью изолированной VM среды “песочницы“ и тщательного измерения вычислений и использования ресурсов. Новые функции VM будут проходить через формализованный запрос функций и спецификации, что означает, что новые функции тщательно документированы и протестированы перед переходом в производственную среду.
- **Детерминизм** для AVM, гарантированный с помощью полнофункционального блока разработки блокчейнов в качестве замены любого обычного SDK. Предложеный срок службы будет выстроен с нуля с детерминизмом в качестве основной цели. Это вводится в сочетании с виртуальной машиной Aion, которая поддерживает только функциональные возможности, выстроенные поверх срока службы блокчейна Aion в нативном и байткодовом контексте.
- **Совместимость** будет направлена назад, что означает, что логика цепи всегда будет действительной и исполняемой при развитии инфраструктуры виртуальной машины.
- **Инструменты** из существующего байткодового анализа также могут быть адаптированы к байт-коду AVM. Использование этой интероперабельности делает возможным использование инструментов, которые подходят для критически важного кода, такого как логика цепи.

AVM использует существующие значимые исследования и разработки. Кроме того, использование машинного байт-кода делает выполнение цепочки логики очень эффективным.

Индивидуальные параметры означают, что легкая VM сконфигурирована для целей измерения потребления (объясняется в следующем разделе) и изоляции от главной машины (сеть, ввод-вывод файлов, нефильтрованные системные данные). Изолированная среда гарантирует, что в цепочной логике не будет иметься никакой значимой информации о главной машине и что никакая нефильтрованная связь (non-oracle) не будет проходить в цепной логике. Это важно для обеспечения безопасности главной машины и детерминизма цепной логики.

Пользователи, желающие использовать программу, должны отправить транзакцию с необходимыми данными (определенными некоторым двоичным интерфейсом). Получив сообщение, оператор цепи объявляет start(), чтобы инициировать последовательность загрузки и принимает данные через accept(data). Затем логика обрабатывает данные, изменяет их состояние, возвращает ответ на сеть и объявляет stop(), чтобы инициировать последовательность выключения.

4.3.2 Ограниченное потребление

Одной из ключевых проблем в работе виртуальной машины, которая оперирует поверх общедоступной среды, является потенциальная возможность неправильного поведения посредством реализации вредоносной логики. При наличии языка (полного по Тьюрингу) расходный бюджет должен быть установлен таким образом, что исполняющая логика не может работать бесконечно или вести себя таким образом, что она может повредить хост-машину или нарушить механизм консенсуса с помощью неправильного временного поведения. В частности, мы определяем бюджетный механизм как ограниченное потребление, которое является механизмом, в котором выделенная ценность определяется использованием, пространством и потреблением пропускной способности исполняющей логики.

По сути, логическое выполнение будет происходить в изолированной среде, вроде ”песочницы”. В нашем контексте под использованием подразумевается использование CPU, выделенного для этой конкретной цепной логики. Под “пространством”

подразумевается распределение памяти, инициируемое логикой выполнения. Это предотвращает выполнение кода, который использует большую величину памяти. Пропускная способность относится к потреблению входа и выхода виртуальной машины. Используя эти механизмы, пользователи, выполняющие логику, будут эффективно арендовать виртуальную машину.

Протоколы указывают, что использование этого механизма требует от пользователя точно указать количество ресурсов, предоставленных виртуальной машине. Отсюда может следовать один из двух вариантов (оба из которых дают ответ):

- Успешное выполнение логики и последующий ответ
- Исключение в логическом исполнении, либо путем превышения предлагаемых границ ресурсов, либо с помощью самой логики.

В случае исключения в исполнении логики AVM будет информировать сеть о событии с помощью ответа ERROR (ошибка).

4.3.3 Блокчейн-ориентированная модель параллелизма

Блокчейн-сети классически считаются серийными в использовании. Изменения состояния и транзакции происходят в серийном порядке для обеспечения детерминизма, необходимого для достижения консенсуса. Однако это создает помеху для количества транзакций, которые могут быть обработаны в любой период времени. Решением этой проблемы является идея параллелизма транзакций. В частности, транзакции должны быть реализованы таким образом, чтобы предоставлялся конспект о состоянии, которое им необходимо. Если это определение является официальным, то может быть реализован планировщик транзакций, который позволяет осуществлять определенное параллельное выполнение транзакции.

С точки зрения AVM, поддержка параллелизма на уровне программ и параллельная обработка нескольких цепочно-логических программ необходимы. Для достижения этой цели AVM должна быть масштабной, автоматически кластеризуя несколько виртуальных машин (VMs) и контрактов для процесса обработки определенным образом.

4.4 Язык скриптов

Язык скриптов Aion используется для написания логики цепей, которая работает на Aion-1 и потенциально любой сети соединения / участия. Язык Aion транслируется в байт-код AVM и выполняется AVM.

Язык Aion предоставляет следующие возможности:

- Защитное программирование
- Среда периода выполнения блокчейна
- Инъекция в контексте блокчейна
- Безопасность

4.4.1 Спецификации

Язык Aion соответствует подмножеству спецификаций языка Java и предназначен для блочной логики. Для этой цели существующий байт-код будет рассмотрен и, возможно, реорганизован для соответствия данному контексту.

Кроме того, спецификации языка Aion включают в себя срок службы блокчейна / комплект разработки (BRE / BDK). Цель состоит в том, чтобы предоставить разработчикам высоко оптимизированные библиотеки разработки, которые реализуют функциональные возможности, связанные с блочной связью. Они включают в себя отправку транзакций, издание событий, получение данных, относящихся к блокчейну, связь между цепно-логическими приложениями, но при этом не ограничиваются ими. Этот срок службы используется для замены обычных наборов для разработки, найденных в общих вычислительных средах. В целом, пользователи этого языка должны ожидать ту же синтаксическую структуру, но совершенно уникальный набор разработчика.

4.4.2 Защитное программирование

Защитное программирование будет поддерживаться языком Aion. Согласно прошлым исследованиям [10], ошибки, допущенные разработчиками цепочки логики, возникают из-за неожиданных входных данных, исключений в сроке службы и неожиданного

изменения состояния после повторного входа. Язык Aion предоставит механизмы для уменьшения вероятности этих распространенных ошибок. Эти механизмы таковы:

- Aion проверяет входные данные перед тем, как передать их в цепочную логику и проверяет выходные данные после выполнения.
- Язык скриптов вводит предварительное условие, постусловие и утверждение, чтобы помочь программистам четко организовывать свои мысли в защитный шаблон.
- Исключения try / catch полностью поддерживаются цепной логикой, что подчёркивает обработку состояния приложения после исключения, вместо возврата в исходное состояние.
- Границы доступа к массиву проверяются во время выполнения.

Дополнение к инструментам поможет привести разработчика к образу мышления, описанному выше. Возможно, необходимо добавление предупреждений и лучших практик в областях, где обнаружен незащищенный код. Другие функции также будут рассмотрены в будущем.

4.4.3 Операционная среда блокчейна

Операционная среда блокчейна облегчает выполнение цепной логики путем предоставления детерминированной библиотеки. Эта библиотека тщательно адаптирована для удовлетворения требований детерминизма цепной логики. Доступ по времени будет ограничен, используя время блокировки вместо текущего системного времени. Распределение объектов будет реализовано детерминированным образом, чтобы функции на основе адресов памяти продолжали работать (например, функция `hashCode()` по умолчанию). Кроме того, общие утилиты и алгоритмы будут тщательно изучены и включены в операционную среду блокчейна.

4.4.4 Инъекция в контексте блокчейна

Инъекция зависимостей - это метод, при котором один объект предоставляет зависимости другого объекта. Он позволяет клиенту, такому как цепной логике в контексте блокчейн, иметь гибкость для настройки и скрывает детали того, как предоставляются зависимости.

В языке скриптов Aion контекст блокчейна и информация о сроке службы считаются зависимостями. Любая цепная логика, которая запрашивает эту информацию, может предъявлять требования с помощью аннотаций. По мере развития Aion к инъекционным объектам будет добавлено больше ресурсов.

4.4.5 Безопасность

Безопасность языка Aion получена благодаря защитному характеру языка и AVM, в котором время, пространство и использование ресурсов ограничены и строго оцениваются. Кроме того, безопасность следует подчеркивать с помощью инструментов, предоставляемых для языка скрипта. Например, логическая корректность кода цепи Aion может быть обеспечена существующими инструментами проверки байт-кода, подтверждения и проверки модели. Другие примеры включают Java Pathfinder [12], FindBugs [13], and PMD [14].

5 СТРАТЕГИЧЕСКИЙ ПЛАН

В данной работе изложены амбициозные и экспериментальные цели и идеи. Для того, чтобы подойти к этому вопросу прагматичным образом, Aion-1 будет развернут итеративным способом, начиная с существующих технологий и постепенно продвигаясь к намеченным целям.

В данной работе изложены амбициозные и экспериментальные цели и идеи. Для того, чтобы подойти к этому вопросу прагматичным образом, Aion-1 будет развернут итеративным способом, начиная с существующих технологий и постепенно продвигаясь к намеченным целям.

5.0.1 Этап 1

В центре внимания первого этапа релизов Aion лежит межцепная связь и инфраструктура моста. Функциональность первого этапа будет включать в себя:

- Измененный, высокоэффективный EVM
- Функционирующие бриджинг и межцепную связь
- Изменённый согласованный алгоритм доказательства работы

5.0.2 Этап 2

Второй этап плана выпуска Aion нацелен на переход от нашей модифицированной архитектуры EVM к предлагаемой AVM-архитектуре. Приоритеты развития этого этапа следующие:

- Виртуальная машина Aion
- Язык скриптов Aion
- Продолжение поддержки унаследованной от EVM кодовой базы

5.0.3 Этап 3

Третий этап завершает предусмотренную сетевую инфраструктуру, обеспечивая инфраструктуру для быстрой, эффективной межцепной связи и межцепных приложений. В дополнение к межцепным функциям с этапа 1 и реализации VM с этапа 2, этот этап представит наш репрезентативный консенсус, в том числе и репрезентативный консенсусный алгоритм.

6 ЗАКЛЮЧЕНИЕ

Сформулированные в этой работе предлагаемые решения являются результатом нескольких лет реализации и экспериментирования в области блокчейн. Команда Aion имела непосредственное отношение к нескольким крупномасштабным корпоративным проектам, где проблемы, изложенные ранее, оказались очень выражены. Сеть Aion предназначена для решения этих проблем и предлагает решение, которое позволит блокчейн-приложениям достичь своего полного потенциала. В наших исследованиях и разработках нам посчастливилось натолкнуться на невероятные находки и эксперименты ведущих мыслителей и исследователей, работающих над взаимодополняющими концептами. Мы сделали всё возможное, чтобы все зафиксировать и отдать им должное в приведенных ниже ссылках.

По мере того, как мы продолжаем наше путешествие, чтобы превратить Aion в реальность и связать постоянно растущую фрагментированную экосистему блокчейнов, мы с нетерепением ждём взаимодейтсвий с Вами и будем рады Вашему участию.

7 КОНТАКТЫ

В этом вводном техническом документе представлены концепты блокчейн-сети третьего поколения Aion. Команда, стоящая за этим документом, предана реализации идеи о взаимосвязи между блокчейнами, которая будет играть решающую роль в будущих предприятиях, правительственных и общественных цифровых инфраструктурах и других областях жизни человека. В ближайшие месяцы мы проведем углубленное исследование каждого из компонентов, представленных в этой статье, а также создадим первую версию этого проекта.

Присоединитесь к списку рассылки сети Aion чтобы получить оповещения о более подробных работах, связанных с конкретными аспектами Aion-1 по мере их появления. Вы также можете оставаться в курсе нашего прогресса:

- Twitter
- GitHub
- LinkedIn

Ссылки

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] V. Buterin, “Ethereum whitepaper,” 2014. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper.

[3] M. Gray, “Introducing project ‘bletchley’,” 2016. [Online]. Available: https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/bletchley-whitepaper.md.

[4] Bitshares, “Delegated proof of stake,” 2015. [Online]. Available: http://docs.bitshares.org/bitshares/dpos.html.

[5] O. Beddows and M. Kordek, “Lisk whitepaper,” 2016. [Online]. Available: https://github.com/slasheks/lisk-whitepaper/blob/development/LiskWhitepaper.md.

[6] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, “The honey badger of bFT protocols,” 2016.

[7] C. Copeland and H. Zhong, “Tangaroa: A byzantine fault tolerant raft,” 2014.

[8] D. Mazières, “The stellar consensus protocol: A federated model for internet-level consensus,” 2015.

[9] S. Kamvar, M. Schlosser, and H. Garcia-Molina, “The eigenTrust algorithm for reputation management in p2P networks,” 2003.

[10] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making smart contracts smarter,” 2016.

[11] N. Atzei, M. Batoletti, and C. Tiziana, “A survey of attacks on ethereum smart contracts,” 2016.

[12] NASA, “What is jPF?” 2009. [Online]. Available: https://babelfish.arc.nasa.gov/trac/jpf/wiki/intro/what_is_jpf.

[13] U. of Maryland, “FindBugs™ - find bugs in java programs,” 2015. [Online]. Available: http://findbugs.sourceforge.net/.

[14] PMD, “Welcome to pMD,” 2017. [Online]. Available: https://pmd.github.io/pmd-5.8.1/.