SMARTBOARD

Technical Drawing

Техническая документация

Оглавление

1. Общее описание блокчейн-сети платформы

1.1. Описание блокчейн-сети проекта

Для реализации проекта будет запущен публичный блокчейн на базе исходного кода платформы izzz.io. Алгоритм консенсуса основан на подтверждении времени генерации блока (Dynamic Limited Confidence Proof-of-Activity, DLCPoA), который не требует больших вычислительных ресурсов, а также на системе доверенных нод (Proof-of-Authority) для ускорения работы сети.

1.2. Техническая сводка блокчейна

Способ подтверждения блоков	DLCPoA (Dynamic Limited Confidence Proof of Activity) + Proof-of-Authority
Программная платформа	Node.js 10
Хеширование	Фильтрованный SHA256
Цифровые подписи	ECDSA-secp256k1, основанная на bitcore-lib
Криптопровайдер	bitcore-lib 1.0.4
Структура основной цепи блоков	JSON блоки с произвольным содержимым до 2 мегабайт (с возможностью перенастройки)
База данных	LevelDB 1.20, Sqlite3 3.24.0
Смарт контракты	EcmaContracts V8: JavaScript ES6, с управляемым состоянием
p2p протокол	WebSocket Based + DNS-SD Multicast Discovery

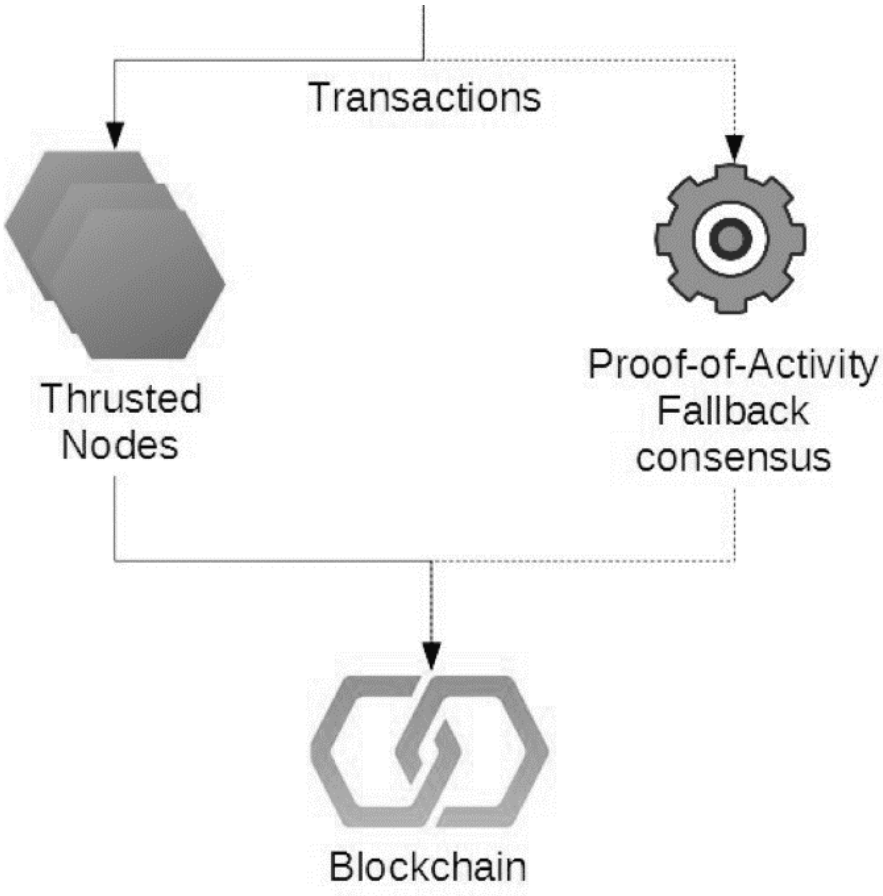
Основная цепочка состоит из JSON блоков со следующей структурой:

— Хеш блока SHA256.
— Порядковый номер блока.
— Время начала генерации блока.
— Время окончания генерации блока.
— Цифровая подпись.
— Данные блока.

1.3. Особенности блокчейна

— Одномерный блокчейн (принцип 1 транзакция – 1 блок).
— Алгоритм генерации блоков DLCPoA надежно защищает сеть от спама и поддельных транзакций, при этом не требует больших затрат вычислительных ресурсов.
— Отсутствие майнинга в системе.
— Транзакции в сети платформы – бесплатны.
— Скорость работы сети: до 1000 вызовов смарт-контрактов в секунду.

1.4. Схема работы транзакционной системы



Proof of Authority – это ноды, которые работают с ключами, выпущенными при старте блокчейн-сети, и используются для ускорения транзакций за счет отсутствия распределенного консенсуса (блоки считаются валидными, если подписаны ключом одной из Trusted Nodes).

Proof-of-Activity Fallback Consensus – дополнительная система консенсуса в сети. Полностью децентрализованная, используется для первичного запуска сети.

Для распределенного консенсуса используется зависимый от времени **DLCPoA**.

DLCPoA (Dynamic Limited Confidence Proof of Activity, рус. Динамическое доказательство активности с ограниченным

доверием) – модификация алгоритма LCPoA с регулируемой сложностью генерации блока.

LCPoA (Limited Confidence Proof of Activity, рус. Доказательство активности с ограниченным доверием) – гибридный алгоритм консенсуса сети блокчейн, состоящий из двух технических элементов:

1. Proof of Activity – принцип, основанный на решении задачи, схожей с задачей принципа Proof of Work, но со значительно сниженной сложностью, благодаря которому решение задачи занимает от долей секунды до нескольких минут.
2. Limited Confidence («Ограничение доверия») – система автоматического создания «контрольных точек» в блокчейн-сети.

1.5. Преимущества алгоритма консенсуса LCPoA

— Средняя скорость работы на устройствах разного класса – 1 блок в 5 секунд.
— Ограничение максимальной скорости подбора блока для всех устройств – 1000 хешей в секунду, что делает использование майнеров бессмысленным.
— Генерация блока может легко выполняться устройством любой мощности.
— Полностью децентрализованный алгоритм, для генерации нового блока необходима только информация о последнем блоке сети.
— Не требует существования токенов и вознаграждения в сети для работы.

1.6. Безопасность и атака 51%

Базово, без использования защиты со стороны механизма Limited Confidence, описанный вариант Proof of Activity сам по себе сильно уязвим к атаке 51%. С использованием ограничения доверия –

атака 51% возможна только на очень малом количестве блоков, что делает ее бессмысленной в большинстве случаев.

DLCPoA – алгоритм консенсуса, позволяющий регулировать скорость сети. Для генерации хеша нового блока в сети необходим подбор подходящего хеша, валидность которого определяется определенными фильтрами. В алгоритме LCPoA фильтры задаются в конфигурации, тогда как в DLCPoA фильтры рассчитываются автоматически, по формуле, исходя из скорости работы сети. Если скорость близка к целевой, то фильтр становится сложнее, если далека от целевой, то фильтр легче, вплоть до нулевой сложности, когда подходит любой хеш.

Формула, определяющая сложность сети

abs(log10(1000 — расстояние мсек между блоками) / (1000/целевая скорость сети)

Формула, определяющая выбор хеша

hashSigma* <= round(допустимое количество вариантов хеша — (допустимое количество вариантов хеша * сложность)

**hashSigma: последние 6 или более символов хеша в 16-ричном представлении, т.е. 6 байт*

Динамическая конфигурация сложности алгоритма позволяет предотвратить атаки на скорость работы сети и поддерживать сеть работоспособной под любыми нагрузками.

1.7. Описание работы блокчейн-сети Системы

Блокчейн Системы в качестве основы сети будет использовать систему смарт-контрактов, выполняющихся в специальной среде выполнения EcmaContracts, которая использует JavaScript-движок V8 для создания виртуализированного окружения исполнения

кода контрактов. Это позволит полностью изолировать произвольный код контрактов как от системы, так и от других контрактов, а также контролировать доступность ресурсов (ОЗУ, процессорное время, лимиты вызовов) для каждой сущности виртуальной машины.

EcmaContracts реализует принцип управления состоянием (state) сущностей контракта, при котором в цепочку блокчейн сохраняется только информация о вызовах методов смарт-контрактов и их аргументах. Результаты работы смарт-контрактов сохраняются локально на ноде пользователя и загружаются при следующем вызове контракта. Все ноды в сети одновременно повторяют каждую транзакцию цепочки с самого первого блока до последнего существующего, что приводит к полной синхронизации состояний контрактов на каждой из нод.

1.8. Язык смарт-контрактов

Система выполнения смарт-контрактов позволяет писать контракты с помощью языка JavaScript ES6. Смарт-контракты являются полными по тьюрингу и имеют широкий функционал возможностей. При разработке доступно большинство стандартных методов и классов.

1.9. EcmaContracts

EcmaContracts реализует среду управления и выполнения смарт-контрактов.

EcmaContracts контролирует состояние, запущенные сущности виртуальных машин, потребление ресурсов и обеспечивает среды выполнения контрактов необходимыми для работы методами и объектами. Взаимодействие с такими объектами позволяет реализовывать мощные и функциональные децентрализованные системы.

1.10. DApp

Децентрализованные приложения (DApp) в сети позволят создавать добавочный функционал для ноды. DApp приложения имеют широкий функционал:

1. Взаимодействие с цепочкой блоков, предобработка, реакция на изменения цепочки.
2. Взаимодействие со смарт-контрактами, в том числе запуск новых.
3. Взаимодействие с другими децентрализованными приложениями посредством встроенных протоколов.
4. Интеграция централизованных приложений с децентрализованными.

2. Общее описание платформы

2.1. Терминология

SmartBoard Coin (SBC) – Utility-токен для оплаты внутренних услуг платформы.

Валютный токен (далее «Т-токен» / «Т-валюта» или «валютный токен») – токен, заменяющий реальную криптовалюту для операций внутри экосистемы. За каждой единицей валютного токена находится криптовалюта-оригинал, хранящаяся на подконтрольном кошельке.

DAC – децентрализованная автономная компания. Коллективный счет для хранения и управления цифровыми активами (SBC + 1 валюта на выбор). Может выпускать криптоакции, обеспеченные балансом организации.

Участник (DAC) – участник компании (DAC). Может выставлять на голосования различные действия и подписывать другие голосования. Участник DAC может не быть акционером.

Акционер (DAC) – пользователь, купивший криптоакции DAC. Может принимать участие в голосовании (если установлено в правилах). Не может инициировать голосования.

DAF – децентрализованный автономный фонд. Коллективный мультивалютный счет для хранения и управления цифровыми активами (SBC + 1 валюта на выбор при старте, остальные можно разблокировать после создания) и криптоакциями других компаний (DAC). Может выпускать собственные криптоакции, обеспеченные балансом фонда. Акционеры фонда могут принимать участие в управление другими организациями, чьи криптоакции фонд имеет на балансе, а также предлагать действия и подписывать действия от имени фонда.

Акционер (DAF) – пользователь, купивший криптоакции DAF. Может принимать участие в голосованиях и инициировать их.

Право голосования – право инициировать голосования. В DAC им обладают участники, в DAF – акционеры.

Право подписи – право подписывать голосования. В DAC правом подписи обладают: участники, акционеры (в том числе фонды). В DAF правом подписи обладают акционеры фонда.

Цифровые акции фондов и организаций – криптоакции устанавливают права на имущество организаций и могут использоваться в качестве инструмента управления в голосованиях.

Токен SBC (SmartBoard Coin) – токен для оплаты внутренних услуг платформы.

Цифровая подпись – пароль для подтверждения действий.

2.2. Цифровые активы

Цифровые активы – это внутренние токены, использующиеся в экосистеме для различных целей.

Принимаемые в системе криптовалюты:

— Bitcoin.
— Ethereum.
— USDT (ETH).

Эмиссия Т-валютных токенов осуществляется служебным контрактом, создающим Т-валютные токены эквивалентно конвертируемым средствам.

Перемещение Т-валютных токенов

Т-валютные токены могут свободно перемещаться между организациями и пользователями внутри экосистемы, операции с перемещением фиксируются в блокчейне.

Виды Т-валют в экосистеме (внутренние токены системы – аналоги криптовалют):

— (T) Bitcoin.
— (T) Ethereum.
— (T) USDT (ETH).

Правила обмена криптовалют на Т-валюты

Обмен осуществляется в пропорции 1:1 без учета комиссии, которая взимается с пользователя.

В процессе обратной конвертации уничтожаются Т-валютные токены, высвобождая равную им часть с кошелька платформы на личный кошелек пользователя на платформе в пропорции 1:1 без учета комиссии, которая взимается с пользователя.

Конвертация на ввод и вывод осуществляется в автоматическом режиме.

Обмен валют в рамках Системы будет осуществляться через интеграцию со сторонним сервисом – CoinPayments.

Внутренние покупки

Все внутренние покупки могут осуществляться за счет баланса Т-валютных токенов (Т). Они используются для покупки акций организации.

Внутренние покупки осуществляются без дополнительной информации, но если в настройках подключена цифровая подпись, то при выполнении действий (покупка/уничтожение криптоакций; покупка SBC; транзакции; подпись в голосовании) запрашивается подтверждение подписи.

Чтобы эмитировать SBC пользователь должен сначала пополнить баланс Т-валюты и лишь затем осуществить конвертацию в SBC за:

— (Т) Bitcoin.
— (Т) Ethereum.
— (Т) USDT (ETH).

Цифровые акции организации можно приобрести за валютные токены. 1% криптоакций = 1% от имущества организации (валютных токенов). Криптоакции можно уничтожить и забрать свою долю с баланса организации, на личный счет.

В случае получения иррационального числа в системе такие числа округляются до 2-х знаков после запятой (в меньшую сторону).

Участники выкупают криптоакции после создания организации.

В случае уничтожения криптоакций валютные токены, равные их доле уничтожаются, а Т-токены поступают на личный кошелек пользователя.

Выход из организации влечет уничтожение криптоакций, права подписи и выделения равной им доли на личный кошелек

пользователя. Уничтожение без владения токеном-подписи (в случае его передачи) невозможно.

2.3. Токеномика

Лимит эмиссии: 1 млрд SBC.

Эмиссия: обращение новых монет создают пользователи, обменивая криптовалюты на SBC по установленному курсу, согласно алгоритму PFP.

Алгоритм эмиссии: Proof Freeze Provision – пользователи платформы создают новые монеты, обменивая криптовалюты на SBC по установленному курсу $1. Процесс обмена происходит внутри личного кабинета платформы. Средства, полученные за обмен SBC, будут заморожены на открытом счете. Все счета будут доступны для проверки.

Эмиссия на старте: 150 млн SBC.

Правила продажи токенов после стартовой эмиссии: остальные токены будут продаваться по курсу SBC. Средства за продажу будут замораживаться, в будущем предполагается обеспечение возможности обратного выкупа SBC.

Курс SBC: изначально равен $1. После размещения на публичных торгах может меняться. Показатель динамический.

Уничтожение: количество SBC сокращается по мере оплаты пользователями внутренних услуг платформы (токены сжигаются). Внутренние услуги, за которые берется оплата в SBC – это создание DAC, DAF, а также разблокировка дополнительных счетов на T-валюты в DAF.

2.4. Регистрация пользователя

При регистрации в системе пользователь задает логин и пароль. Также в системе задается ID пользователя для его идентификации в системе (может быть задано в личном кабинете после регистрации).

Каждый пользователь при регистрации получает сгенерированный счёт/кошелек для операций внутри системы:

— SmartBoard Coin.
— (T) Bitcoin.
— (T) Ethereum.
— (T) USDT (ETH).

Данные счета привязываются к аккаунту пользователя. Используя средства с баланса, можно осуществлять прямые покупки SmartBoard Coin, используя пароль и двухфакторную аутентификацию (если включена).

Для криптовалют Ethereum, Bitcoin и USDT (ETH) обработка ввода/вывода осуществляется через интегрированный с системой сервис CoinPayments.

2.5. Кошелек

Каждый кошелек имеет внутренний адрес, к которому привязываются все цифровые активы внутри экосистемы. По внутреннему адресу можно отправлять токены без комиссии внутри сети.

Система самостоятельно отделяет внутренние адреса от внешних (других блокчейнов) и осуществляет нужную транзакцию.

В кошельке доступны для хранения:

— SmartBoard Coin.
— (T) Bitcoin.

— (T) Ethereum.
— (T) Tether (ETH).
— Криптоакции.
— Права подписи.

3. DAC – децентрализованная автономная компания

Децентрализованная автономная компания – коллективный криптовалютный счет с детальной настройкой внутренних правил.

3.1. Настройка компании

3.1.1. Выбор валюты

Помимо SmartBoard Coin DAC может хранить одну валюту на выбор:

— (T) Bitcoin.
— (T) Ethereum.
— (T) USDT (ETH).

3.1.2. Настройки команды

Приглашение участников происходит по внутреннему @ID. Каждый участник получает приглашение после настройки всех правил создателем организации. После создания участники получают права подписи в кошелек.

Право подписи предоставляет возможность принимать участие в голосованиях. Передача прав подписи устанавливается при создании.

Удаление участников: голос удаляемого не учитывается при голосовании. Удаление влечет отчуждение права подписи.

3.1.3. Настройка криптоакций

Эмиссия криптоакций устанавливается во время создания. Стартовый размер эмиссии ограничен диапазоном от 10 до 1000 криптоакций. Криптоакции выкупаются после создания организации. Купить криптоакции может любой пользователь платформы.

Криптоакции могут свободно передаваться внутри экосистемы.

Цена криптоакций устанавливается в выбранной валюте, оплата происходит в валютных токенах.

3.1.4. Настройка транзакций

Под транзакциями в системе понимаются любые переводы цифровых активов (внутренние покупки, прямой перевод, внешний перевод). Данными настройками регулируются правила выполнения всех действий.

В настройках транзакций есть 2 типа правил: общие и частные.

Общее правило является обязательным и действует на все транзакции, которые не покрываются частными правилами. Частные правила позволяют создать отличное правило на перевод средств, превышающий определенную сумму. Частных правил может быть несколько, а общее только одно.

Пример. В случае, если установлено общее правило на все транзакции, а также установлено частное правило на транзакции >100 USDT, то при отправке транзакций на сумму менее 100 USDT, будет действовать общее правило, при отправке транзакций на сумму более 100 USDT будет действовать частное. Кроме того, можно задать еще одно частное правило >1000, тогда в диапазоне от 100 до 999 будет действовать первое частное правило, а в диапазоне от 1000 – второе.

3.1.5. Создание компании

После настройки всех правил создатель организации отправляет приглашение выбранным участникам. Для создания компании необходимо получить согласие от всех участников. Комиссию за создание оплачивает создатель. Создатель получает право менять описание организации и логотип.

3.2. Конструктор правил

Конструктор правил позволяет детально настроить условия выполнения для различных действий.

В конструкторе есть 3 типа различных подписей:

1. Подпись конкретного участника.
2. Голосование акционеров.
3. Голосование участников.

Участники и акционеры – 2 разных вида членов компании. Участник может быть акционером, а акционер может быть участником. Однако могут быть члены компании, которые состоят лишь в одной категории. Являются участниками, но не имеют криптоакций или наоборот.

В случае, если пользователь является и участником, и акционером, он голосует единожды.

Порядок согласования подписей

Все виды подписей обязательны для исполнения, если они установлены в одном «стакане».

Альтернативное правило

Альтернативное правило позволяет установить дополнительное условие выполнения действия. Оно действует наравне с основным.

3.3. Управление компанией

3.3.1. Проведение голосований

Для подтверждения действия необходимо соблюсти условие основного или альтернативного правила.

Голосование проводится в течение 24 часов. Во время проведения голосования замораживается возможность передачи права подписи.

3.3.2. Управление криптоакциями

Дополнительная эмиссия осуществляется за установленную комиссию. Криптоакции DAC могут покупать пользователи и автономные фонды.

3.3.3. Управление командой

Добавление новых участников осуществляется по внутреннему @ID. Новые участники получают право голоса в «голосованиях участников».

Удаление участников команды влечет отчуждение прав подписи. Если участник команды имеет криптоакции, то после удаления его из команды он остается на правах инвестора, но без полномочий участника.

3.3.4. Выход из организации

Выйти из организации может акционер, имеющий в собственности криптоакции компании. Выход из DAC влечет уничтожение криптоакций и выделение равной доли с баланса компании на личный счет.

4. DAF – децентрализованный автономный фонд

Децентрализованная автономный фонд – коллективный криптовалютный счет с мультвалютным кошельком и возможностью покупки криптоакций других DAC.

4.1. Настройка фонда

4.1.1. Выбор валюты

Помимо SmartBoard Coin DAF может хранить 3 валюты, одна выбирается при создании, 2 другие разблокируются после создания:

— (T) Bitcoin.
— (T) Ethereum.
— (T) USDT (ETH).

4.1.2. Настройки команды

В автономном фонде нельзя устанавливать участников при создании. Все участники фонда – акционеры, которые покупают криптоакции фонда после создания.

4.1.3. Настройка криптоакций

Эмиссия криптоакций

Устанавливается во время создания. Стартовый размер эмиссии ограничен диапазоном от 10 до 1000 криптоакций. Криптоакции выкупаются после создания. Купить криптоакции может любой пользователь платформы.

Криптоакции могут свободно передаваться внутри экосистемы.

Цена криптоакций устанавливается в выбранной валюте, оплата происходит в валютных токенах.

4.1.4. Настройка транзакций

Разновидности транзакций:

1. Прямой перевод (внутренний, внешний).
2. Покупка криптоакций DAC.
3. Покупка SBC.
4. Разблокировка дополнительных счетов.

4.1.5. Настройка управления

a) Правило продажи криптоакций устанавливается для всех операций с криптоакциями на балансе фонда:
    1. Выставление на продажу.
    2. Снятие с продажи.

Средства с продажи поступают на общий счет.

b) Правило принятия решений в дочерних компаниях устанавливает условие для предложения действия от имени фонда.

4.1.6. Создание фонда

После настройки всех правил создатель организации покупает минимум 1 криптоакцию и создает фонд. Другие участники фонда выкупают криптоакции после создания фонда.

4.2. Управление фондом

4.2.1. Проведение голосований

Для подтверждения действия необходимо соблюсти установленный консенсус акционеров.

Голосование проводится в течение 24 часов.

4.2.2. Управление криптоакциями

a) Управление собственными криптоакциями: дополнительная эмиссия осуществляется за установленную комиссию. Криптоакции DAF могут покупать только пользователи.
b) Управление сторонними криптоакциями: акционеры фонда могут предлагать покупку криптоакций других DAC. Предложить покупку может любой акционер. Правило покупки регулируется правилом транзакции.

Продажа криптоакций и снятие с продажи регулируется в настройках управления специальным правилом. Покупать криптоакции у фондов могут пользователи или другие фонды. Средства с продажи поступают на общий счет.

4.2.3. Управление дочерними компаниями

Любой акционер фонда, который владеет криптоакциями компании, может предлагать выполнить действие в компании от имени фонда.

Виды действий

1. Предложить голосование.
2. Проголосовать «за».
3. Проголосовать «против».

Предложенное действие сначала попадает в фонд и выносится на голосование. В случае положительного решения оно выносится на голосование в дочернюю компанию.

4.2.4. Выход из фонда

Выход из фонда влечет уничтожение криптоакций и выделение равной части всех средств с баланса фонда. Среди средств могут быть: SBC, валютные токены, криптоакции DAC.