WHITEPAPER

PZM CASH

Криптовалюта с алгоритмом
консенсуса Proof - of - Stake

Версия Март 2020

Оглавление

1. Абстракт

PZM Cash – это криптовалюта, созданная в качестве платежного средства для быстрорастущей экосистемы, в которой экономические мотивы каждого отдельного участника обеспечивают рост общего благосостояния. Главный стратегический фактор успеха PZM Cash – ставка на нарастающее масштабирование и балансировку спроса и предложения денежной массы.

Преимущества архитектуры PZM Cash:

- сайдчейны, обеспечивающие безопасность основного леджера;
- алгоритм консенсуса Proof-of-Stake;
- максимальные возможности для разработчиков децентрализованных приложений (DApps).

Команда PZM Cash существенно модернизировала алгоритм консенсуса POS, использовавшийся ранее. Комиссия за транзакции в сети PZM Cash фиксирована, что гарантирует справедливое распределение вознаграждения между форжерами.

Ключевое отличие PZM Cash от «классической» концепции POS заключается в механизме заполнения сети денежной массой. Команда PZM Cash отказалась от полной эмиссии при генерации первого блока – при запуске сети с помощью премайнинга будет распределен лишь 1% от общего числа монет. Остальные монеты будут выпущены в ходе PoS майнинга – выплаты поощрения лояльным держателям PZM Cash за поддержку сети.

Форжеры за добавление блоков в цепочку получают комиссии за транзакции. При этом шанс на добавление блока линейно зависит от величины актива кошелька, то есть текущего стека PZM Cash. Никаких дополнительных выплат за форджинг, помимо комиссий, не предусмотрено – вся эмиссия после запуска сети будет осуществляться за счет PoS майнинга.

Механизм PoS майнинга имеет два основных компонента:

- «ведущий» активированный кошелек;
- кошельки поддержки – кошельки, активированные транзакцией с ведущего кошелька.

Выплаты вознаграждения производятся на ведущий кошелек, однако на их размер влияет как баланс ведущего кошелька, так и балансы всех кошельков поддержки. При этом количество монет на балансе – единственный фактор, влияющий на выплаты. Изменения размера выплат со временем не предусмотрено.

Если величина стека на кошельке достигает 0,011% от итоговой эмиссии (1 000 000 PZM Cash), PoS майнинг останавливается. Таким образом сеть защищается от риска чрезмерной централизации активов.

Вознаграждение пользователей за лояльность с помощью PoS майнинга обеспечивает сеть платежеспособной пользовательской базой и формирует спрос на услуги в экосистеме PZM Cash. Вдобавок, ориентированность архитектуры на удобство разработки DApps с максимальной функциональностью позволит обеспечить широкий набор услуг и пользовательских кейсов за счет создания большого количества независимых приложений.

Реализация PZM Cash на JavaScript дополнительно расширяет возможный ассортимент сторонних приложений – относительная простота языка дает возможность широкому кругу разработчиков присоединиться к работе над расширением функционала экосистемы PZM Cash. Это также позволяет значительно расширить функционал браузерных решений, связанных с PZM Cash.

Финальное преимущество PZM Cash, которое обеспечивается благодаря использованию JavaScript, – это возможность применить для кошелька Web3 js решение. Таким образом будет обеспечен доступ широкого круга партнеров к балансу и унификация PZM Cash как платежного инструмента.

2. Продукт и сценарии использования

Сценарии использования

PZM Cash – это в первую очередь международное независимое и прозрачное в связанных с ним операциях платежное средство.

Каждый пользователь, независимо от своего местоположения, может осуществлять транзакции и при желании участвовать в администрировании сети, развернув ноду и установив необходимое для этого программное обеспечение.

Любому пользователю PZM Cash доступны два сценария использования криптовалюты: пассивный и активный. Они отличаются степенью участия в развитии сети. При пассивном сценарии участник сети является ее простым пользователем, при активном участии пользователь является также администратором сети (форжером) и активно участвует в ее развитии и расширении.

Таким образом, в сети присутствуют два типа участников:

- простые пользователи, которые используют горячие кошельки (в web среде). Они не выделяют места под нужды сети на своих компьютерах, не разворачивают ноды и получают доход исключительно за счет держания PZM Cash на своих кошельках;
- форжеры, получающие доход от форджинга – добавления новых блоков в цепочку.

Пассивный сценарий использования

Данный сценарий предполагает использование клиентом браузерной (web) версии кошелька (горячий кошелек), позволяющей осуществлять основной функционал – транзакции в сети (включая исполнение смарт-контрактов).

Зарегистрированный и активированный кошелек позволяет клиенту получать доход в виде дополнительных монет, начисляемых по алгоритму двухфакторного PoS майнинга. Чем больше

монет находится в кошельке у пользователя, тем выше его поощрение. Подробнее о факторах начисления можно прочитать в соответствующем разделе.

Браузерное решение позволяет пользователю не выделять пространство на жестком диске под нужды блокчейна и не разворачивать ноду.

Для того чтобы реализовать пассивный пользовательский сценарий, участнику необходимо:

1. Создать и активировать горячий кошелек на сайте PZM Cash. Активация осуществляется посредством входящей транзакции.
2. Процесс PoS майнинга будет запущен с момента появления минимального значения в 1 PZM Cash на балансе кошелька.
3. Сумма дополнительного начисления PZM Cash зависит от факторов PoS майнинга – баланса ведущего кошелька и суммарного баланса кошельков поддержки.
4. Излишек монет (лишнюю ликвидность) пользователь может обменять на другую необходимую валюту на криптовалютных биржах и диверсифицировать свои цифровые активы; либо использовать для оплаты услуг DApps и проведения транзакций.

Активный сценарий использования

Данный сценарий предполагает активное участие пользователя в построении сети – добавление новых блоков и записей в леджер и их подтверждение, то есть синхронизацию и администрирование блокчейна.

За подтверждение транзакций других пользователей и добавление новых блоков участник получает доход в виде комиссии форжера – процент от суммы транзакций в блоке.

Для того, чтобы реализовать активный пользовательский сценарий, участнику необходимо:

1. Развернуть полную ноду: выделить под нужды блокчейна пространство на HDD на своего компьютера и установить специальное ПО PZM Cash.
2. Постоянно держать на балансе как можно большее число монет PZM Cash. Увеличение числа монет на балансе повышает шансы на добавление блока.
3. Держать ноду онлайн, формировать новые блоки и выстраивать ветки блокчейна, содержащие хэшированные записи о транзакциях.
4. Получать вознаграждение за подтвержденные транзакции в виде комиссионного сбора – процента с сумм транзакций (форжинг).

При развертывании ноды аккаунт получает право на добавление новых блоков в блокчейн PZM Cash (форжинг). Если во время формирования блока в какой-либо точке мира совершается транзакция и попадает в данный блок из пула нераспределенных транзакций, то аккаунт, сформировавший блок, получает фиксированную комиссию за проведение транзакции. Сумма комиссий за проведение всех транзакций в блоке и составляет вознаграждение форжера, начисляемое аккаунту, сформировавшему блок.

Шансы на добавление нового блока в блокчейн определенным аккаунтом тем выше, чем выше баланс статичных монет PZM Cash в кошельке и чем дольше новый блок не добавлялся в блокчейн.

PZM Cash Wallet

Кошелек PZM Cash – это универсальный инструмент для управления монетами на балансе уникального аккаунта пользования. Он позволяет как осуществлять исходящие транзакции, используя закрытый ключ пользователя, так и генерировать реквизиты (публичные ключи) для получения транзакций от других пользователей.

Функционал кошелька:

- проведение p2p транзакций;
- проведение транзакций при исполнении смарт-контрактов;

- создание смарт-контрактов с использованием шаблонов;
- предоставление доступа к децентрализованным приложениям экосистемы PZM Cash;
- отображение баланса кошелька и динамики его изменения.

В основе криптографии блокчейна лежит ассиметричное шифрование. Это означает, что каждый кошелек имеет открытый и закрытый ключи. Цифровые ключи – это записи (набор символов), которые контролируют доступ к монетам, хранящимся в кошельке.

Цифровые ключи всегда парные: каждый кошелек имеет закрытый и открытый ключ. Открытый ключ требуется для идентификации кошелька в сети и используется в качестве реквизитов для получения входящих транзакций. Закрытый ключ используется для подписи исходящих транзакций и перевода монет на другие кошельки в блокчейне. Закрытый ключ отвечает за контроль над монетами в кошельке и потому всегда должен находиться под контролем владельца учетной записи.

Кроме того, цифровые ключи создаются и сохраняются пользователями или могут генерироваться и управляться программным обеспечением кошелька пользователя и, следовательно, полностью не зависят от протокола блокчейна.

При первом обращении к PZM Cash каждый участник должен воспользоваться web-клиентом (браузерный доступ) и создать аккаунт – путем несложных действий сгенерировать закрытый ключ.

Генерация закрытого ключа осуществляется на основе данных, введенных пользователем при первом входе в личный кабинет на сайте. Необходимо либо подтвердить стандартное заполнение поля, в котором в виде символьной записи указан приватный ключ, либо ввести набор символов самостоятельно. При подтверждении ввода будет сгенерирован приватный (закрытый) ключ.

Приватный ключ необходимо записать, поскольку он уникален и сгенерировать заново его нельзя. Если приватный ключ будет утерян, войти в аккаунт будет невозможно и средства кошелька станут недоступными. Именно приватный ключ дает вам доступ в кошелек. Закрытый ключ аналогичен цифровой подписи, его рекомендуется хранить в переносном хранилище или на локальном диске.

После этого требуется активировать кошелек на сайте PZM Cash. Это позволит полноценно использовать функционал кошелька, осуществлять транзакции и участвовать в PoS майнинге.

Для этого необходимо сгенерировать публичный ключ – реквизит, который будут указывать другие пользователи для перевода монет на ваш кошелек. После того, как первая транзакция на кошелек будет подтверждена (информация о транзакции будет записана в блокчейн), ваш кошелек станет полностью работоспособным. Открытый ключ хранится в ветви данных проверки вместе с ее данными.

Чтобы получать и отправлять PZM Cash, нужно использовать еще два элемента, которые генерируются из этих двух ключей. Один из них – адрес. Адрес – это строка цифр и букв, созданная из открытых и закрытых ключей и представляющая собой «отпечаток» этих ключей. Поскольку закрытые и открытые ключи имеют сложный формат, для удобства они преобразуются в более удобный формат по математическому алгоритму. Эти версии открытого и закрытого ключей называются общедоступными и частными адресами соответственно.

Частный адрес предоставляет доступ к аккаунту и, соответственно, доступ к монетам, а публичный адрес – это номер кошелька, используя который, другие пользователи могут переводить на него монеты.

Чтобы создать исходящую транзакцию, требуется подтвердить право собственности на монеты в ней. Для этого необходимо показать, что пользователь знает секретный ключ. Для этих целей используется цифровая подпись. Подписи – это криптографические элементы, которые вычисляются из закрытого ключа и комбинации другой информации, включенной в транзакцию (которую вводит пользователь, создающий транзакцию). Поэтому подпись является подтверждением желания осуществить исходящую транзакцию и уникальна. Поскольку подписи вычисляются с использованием закрытого ключа и комбинации другой информации о транзакции, они также демонстрируют знание секретного ключа и право подтверждения данных в транзакции. Поэтому каждая подпись действительна только для одной конкретной транзакции.

Web3js

Реализация PZM Cash на JavaScript позволила использовать технологию Web3js, которая значительно расширила возможности PZM Cash Wallet за счет унификации. Кошелек может использоваться на ресурсах наших партнеров (например, на биржах и в казино) без создания отдельного кошелька под каждый проект. Более того, браузерная реализация позволяет не обращаться к ядру блокчейна для интеграции новых ресурсов.

Web3js – это коллекция JavaScript-библиотек, которая позволяет удаленно взаимодействовать с нодой через HTTP- или IPC-соединение, что упрощает интеграцию PZM Cash Wallet через выделенный API. В результате партнерам не требуется разворачивать полную ноду для интеграции.

Смарт-контракты

Наш кошелек позволяет отправлять транзакции не только на адреса других участников сети, но и на адреса смарт-контрактов, инициируя различные сделки на основе цифрового алгоритма.

Смарт-контракты – это цифровые протоколы, которые используют математические алгоритмы для автоматического осуществления транзакции после выполнения установленных условий. Процесс полностью контролируется логикой алгоритма, поэтому для выполнения смарт-контракта не требуется участие третьей стороны – гарантом выступает неизменность кода. Неизменность самого кода гарантируется за счет записи кода смарт-контракта в блокчейн при его создании. Смарт контракт приводится в действие входящей транзакцией, с помощью которой он «извлекается» из блокчейна и получает данные.

Для того чтобы обратиться к смарт-контракту, пользователю требуется создать исходящую транзакцию на адрес конкретного контракта. Как только транзакция будет подтверждена, начнется его исполнение.

Обязательства участников фиксируются в форме «если – то», то есть в виде сделки. Например: «если

А переводит цифровые деньги, то Б передает права (в оцифрованном виде) на какой-либо актив». В блокчейн делается соответствующая запись, которая не может быть изменена. Обратившись к этой записи, всегда можно подтвердить свое право на актив и факт осуществления сделки.

Смарт-контракт получает информацию касательно оцифрованных прав на актив из внешнего источника, при этом каждый узел блокчейна исполняет умные контракты независимо. Это означает, что каждый узел получает данные из внешнего источника самостоятельно. Однако, чтобы в блокчейне не возник конфликт и был достигнут консенсус, каждый узел должен получить одинаковый (неизменный на промежутке времени) ответ от внешнего источника. Для этого существуют «оракулы», которые являются программной прослойкой между внешним источником и смарт-контрактом, находящимся непосредственно в блокчейне.

Смарт-контракт обращается не напрямую к внешнему источнику, а к соответствующему оракулу, который создает входящую транзакцию, записывающую нужные данные в леджер. Таким образом, каждым узлом принимается идентичная копия данных, и исполнение умного контракта становится возможным.

3. Техническая реализация (core)

Говоря о технической реализации или «ядре» криптовалюты, необходимо иметь в виду алгоритм консенсуса и протокол блокчейна, а также понимать, что это далеко не одно и то же. Протокол – это архитектура и первичные правила блокчейна, а алгоритм – это механизм, с помощью которого они будут выполняться. В то время как протокол определяет правила, алгоритм сообщает системе, какие меры необходимо предпринять для соблюдения всех условий этих правил и получения желаемых результатов. Иными словами, протокол представляет собой сеть «в статике», а алгоритм консенсуса отвечает за ее динамику: внесение в нее изменений и приобретение сетью новых состояний согласно протоколу.

Протокол: распределенная книга (леджер) и узлы (ноды)

Блокчейн – это база данных (леджер), реализованная посредством концепции связного списка, в которой каждая новая запись содержит информацию о предыдущей в зашифрованном (хешированном) виде. Леджер обеспечивает постоянный учет транзакций, которые имели место быть, а также устанавливает порядок, в котором были совершены транзакции. Основным преимуществом блокчейна является устойчивость к изменяемости. Если будет изменен какой-либо блок (например, в результате атаки), то автоматически изменятся все последующие блоки, что приведет к мгновенному выявлению любой попытки подлога.

Криптовалюта PZM Cash реализована на блокчейне, ориентированном на разработку, развитие и расширение функционала децентрализованных приложений. В отличие от Ethereum и других блокчейнов, использующих специализированные языки программирования для создания децентрализованных приложений и запуска «умных» контрактов (например, Solidity), в PZM Cash применяется значительно более распространенный и более простой JavaScript. Данная особенность делает платформу доступной для большого количества разработчиков и обеспечивает масштабирование и развитие пользовательских кейсов. Иными словами, чтобы разработать свое децентрализованное приложение (Dapps) для PZM Cash, не требуется изучать специальные языки.

JavaScript-реализация позволяет обеспечить разработчиков большим количеством специальных библиотек, облегчающих разработку в области криптографии, транзакций, p2p и т. д. Каждая библиотека соответствует протоколу ZPM Cash. Таким образом, PZM Cash концептуально рассчитан на как можно более широкую аудиторию.

Главной отличительной особенностью блокчейна является использование технологии сайдчейнов для запуска полностью отлаженных приложений и независимых блокчейнов в пределах одной платформы. Сайдчейны представляют собой обособленные леджеры, реализованные поверх основной книги. Создаваемые сайдчейны никак не влияют на размер основной сети.

Таким образом достигается:

1. Неограниченная масштабируемость: использование технологии сайдчейнов позволяет масштабировать сеть бесконечно.
2. Повышенная безопасность сети: благодаря тому, что сайдчейны находятся поверх основной сети, невозможно нарушить работу последней путем создания багов в «дочерних» сетях или нарушения стабильности их работы. Например, в Ethereum в случае возникновения ошибки требуется проводить хардфорк для ее исправления.
3. Расширение возможностей разработки: разработчики могут экспериментировать со своими приложениями в сайдчейнах, не опасаясь того, что возникающие ошибки нарушат работу основной сети. Каждый проект (dApp) создается в отдельном сайдчейне, поэтому разработчики имеют широкие возможности по настройке приложений.
4. Реализация сайдчейнов позволяет не разворачивать виртуальную машину для исключения багов. Например, это требуется для исключения багов в EVM (Ethereum Virtual Machine).

Платформа также предоставляет децентрализованное хранилище файлов и услуги условного депонирования для выполнения смарт-контрактов. Сервис оракулов подтверждает информацию о произошедших или совершающихся в текущий момент событиях.

Пользователям предоставляется каталог децентрализованных приложений (в том числе и для портативных устройств: смартфонов, планшетов и т. д.). Каждая утилита регистрируется на основной цепочке, и клиенты могут видеть все приложения и сервисы, доступные на каждом сайдчейне. Пользователь получает доступ ко всем децентрализованным приложениям в одном месте, наподобие GooglePlay или Apple Store.

Важной отличительной особенностью PZM Cash является PoS майнинг – алгоритм наполнения сети дополнительной ликвидностью помимо первоначального генезиса монет.

Разработчики, отдавая себе отчет в том, что это достаточно агрессивная модель расширения денежной массы, выбрали ядро, изначально рассчитанное на создание дополнительных пользовательских сценариев. Таким образом достигается балансировка спроса и предложения на монеты PZM Cash во избежание возникновения инфляционных механизмов в экосистеме и падения обменного курса.

Главный блокчейн содержит хэши сайдчейнов – зашифрованные особым образом записи, которые позволяют проверить целостность и подлинность исходной записи, но не дают возможности ее расшифровать. Это сделано для того, чтобы повысить требуемую скорость работы сети.

Каждый блок PZM Cash содержит следующую информацию:

1. Информация о блоке:

- версия блока и уникальный идентификатор блока;
- временная метка блока, выраженная в секундах;
- идентификатор и криптографический хэш предыдущего блока; информация, получаемая от сайдчейнов;
- метрика статуса сети (слепок);
- ID аккаунта, создавшего блок, а также публичный ключ аккаунта для его идентификации.

2. Информация о транзакциях:

- количество транзакций, хранящихся в блоке;
- данные о транзакциях: данные всех транзакций, включенных в блок, включая их идентификаторы;
- общая сумма PZM Cash по транзакциям, входящим в блок, включая суммы комиссий;
- данные о смарт-контрактах. Информация о статусах смарт-контрактов;
- длина полезной нагрузки блока и значение хэш-функции полезной нагрузки блока;
- значение планки форжинга и кумулятивная сложность для блока.

Нода (узел) PZM Cash

Узел или нода блокчейна представляет собой еще один архитектурный элемент, без которого невозможно представить себе блокчейн. Наличие множества независимых узлов позволяет создать сеть с распределенной (децентрализованной) структурой. Идея в том, что каждое независимое устройство хранит на выделенном HDD текущую актуальную версию леджера, то есть любое устройство с программным обеспечением PZM Cash рассматривается как отдельный узел.

При этом узлы синхронизированы, поэтому при нарушении работы даже значительного числа узлов остальные узлы укажут на ошибку. Это приводит к тому, что для осуществления атаки на блокчейн злоумышленнику требуется синхронно поменять данные в огромном количестве узлов, что становится сложнее и сложнее по мере роста сети.

Каждый узел в сети PZM Cash имеет возможность обрабатывать и передавать транзакции и информацию в блоках. Более того, узлы синхронизированы между собой (содержат идентичные записи актуального состояния блокчейна). Это приводит к исключению возможности возникновения ошибки двойного расходования монет (double spending), заключающейся в том, что одна и та же монета может участвовать одновременно в разных транзакциях.

PZM Cash использует двухуровневую структуру узлов:

1.Полная нода.

Полная нода представляет собой устройство с установленным ПО PZM Cash, где хранится полная текущая и актуальная версия блокчейна. Полная нода может выступать в качестве узла консенсуса (участвовать в создании новых блоков – осуществлять форжинг). Держатель полной ноды может активно участвовать в формировании блокчейна, постоянно группируя входящие транзакции в блоки и распространяя их по сети.

Также полная нода выступает в качестве узла аудита. В данном контексте нода регулярно проверяет (и подтверждает) результаты форжинга других нод и занимается распределением нагрузки по сети, выполняя функцию своеобразной сети доставки контента (CDN) для данных блокчейна.

2. Легкие клиенты

Второй тип узлов –легкие клиенты. Легкими они называются потому, что не имеют полной версии блокчейна и содержат лишь те данные, которые важны для узла, что позволяет ограничить требуемый объем выделенной памяти на HDD и вычислительную мощность. По этой причине они являются хорошим вариантом для организации выделенного криптовалютного кошелька.

В легком клиенте хранятся только те данные, которые требуются для реализации пользовательских сценариев использования. Например, такой легкий клиент позволяет формировать транзакции и отслеживать баланс кошелька. Если пользователю ничего больше не требуется, ничем лишним его устройство нагружаться не будет.

На выходе мы получаем клиента, способного работать на мобильных устройствах или в личном кабинете на сайте PZM Cash Wallet. При этом пользователи не хранят локальную копию блокчейна, поскольку для отправки транзакций достаточно хранить закрытые ключи, при помощи которых данные транзакции подписываются.

Однако, в отличие от других криптовалют, пользователи легкого клиента PZM Cash могут получать вознаграждение за поддержку экосистемы. Да, легкий клиент не может участвовать в форжинге и добавлении новых блоков, но алгоритм PoS майнинга обеспечивает стабильное поступление новых монет на баланс легких кошельков.

Алгоритм консенсуса

Основным процессом для сети является процесс проведения транзакций, который технически связан с добавлением нового блока в леджер. Добавление блока осуществляется по определенному непротиворечивому алгоритму – алгоритму консенсуса.

Алгоритм консенсуса позволяет установить и подтвердить истинность каждой операции, а также синхронизировать версию блокчейна на всех нодах. Более того, он должен обеспечивать одинаковую «точку зрения» на блокчейн каждым узлом при условии, что некоторые узлы могут зависать или падать. Также он призван защищать систему от несанкционированного доступа, изменения списка прошедших транзакций и хакерских атак. Делать это он должен, руководствуясь лишь общими правилами обработки сообщений в сети.

Алгоритм консенсуса обеспечивает динамику системы, то есть ее развитие и рост, при этом сохраняя уникальные свойства блокчейна: равноправие узлов (каждый может участвовать в добавлении блока) и объективность (для определения текущей версии журнала транзакций не нужно доверять неким сторонним авторитетным источникам – корень доверия находится в самом блокчейне и заложен в него алгоритмически).

При этом консенсус обеспечивается постоянно: каждый узел сети достигает одинакового состояния после обработки каждой транзакции и каждого блока. То есть алгоритм консенсуса гарантирует, что все узлы сети всегда имеют одинаковую версию блокчейна, и исключает конфликты между нодами.

Алгоритм консенсуса определяет условие, выполняя которое, участник сети, имеющий право на добавление блока в сеть, получает первоочередную возможность разместить сформированный им блок в леджер. Этот блок будет признан сетью, в сети достигнут консенсус о ее новом состоянии, а «автор» блока получит вознаграждение.

Существует множество различных алгоритмов консенсуса, отличающихся друг от друга этим условием и тем, что считать выполнением этого условия. Самыми популярными из них являются две разновидности: доказательство работы (Proof of work) и доказательство доли (Proof of stake).

Алгоритм Proof of work требует от автора нового блока решения математической задачи, причем эта задача решается только прямым перебором значений. Классический вариант – нахождение особого значения хэша заголовка блока, содержащего ссылку на предыдущий блок, реализованный в Bitcoin.

Задачу решают все претенденты на добавление блока, а шанс решить ее быстрее других и, соответственно, получить вознаграждение, зависит от величины располагаемых вычислительных мощностей. Чем больше вычислительная мощность узла, тем выше шанс. Необходимая скорость работы при этом обеспечивается подбором сложности решаемой задачи в зависимости от совокупной мощности узлов сети.

Недостатки Proof of Work очевидны: огромные вычислительные мощности тратятся впустую, проводя бесполезные вычисления. Справедливость алгоритма также очень спорна. Грубо говоря, он сводится к простому правилу: «У кого мощнее оборудование, тот и прав». Иными словами, успех всецело зависит от объема средств, вложенных в оборудование. И это не говоря о расходах электроэнергии, вызванных ими экологических проблемах и появлении целой индустрии производства специализированных устройств – ASIC, абсолютно бесполезных для чего-либо, кроме решения задач в блокчейне конкретной криптовалюты. Вдобавок крупный игрок может фактически захватить контроль над сетью, заполучив 51% от совокупных вычислительных мощностей.

Другой фундаментальный изъян, связанный с алгоритмом работы, – архитектурно заложенные предпосылки к централизации сети. Постоянно повышающаяся сложность задачи нахождения

консенсуса требует нарастающих затрат вычислительных мощностей. Пока сеть сравнительно небольшая, достаточно ресурсов домашнего компьютера. Но по мере ее развития необходимые затраты на оборудование постоянно увеличиваются. Это приводит к объединению игроков с целью увеличить шансы на добавление блока для достижения бесперебойности награды и стабильной окупаемости и заработка (появление майнинговых пулов). Однако потенциально это делает сеть подконтрольной крупным игрокам.

Принципиально важно отметить, что за свою работу каждый участник сети получает вознаграждение. Вознаграждение выплачивается за успешно добавленный блок и, как правило, состоит из двух частей: комиссии с общей суммы транзакций, которые вошли в блок (здесь некоторые реализуют возможность установить повышенную комиссию в своей транзакции, чтобы у майнера был стимул добавлять транзакцию в формируемый им блок), и фиксированного вознаграждения за блок (за майнинг). Фиксированное вознаграждение за блок может уменьшаться со временем, например, так работает халвинг биткоина.

В PZM Cash мы отказались от делегированного Proof of Stake и применили значительно усовершенствованный «классический» PoS-алгоритм. Благодаря этому возможность участия в работе сети и получения вознаграждения получил очень широкий круг пользователей – для этого нет значимых ограничений и каких-либо существенных барьеров.

POS консенсус PZM Cash

Алгоритм консенсуса PoS подразумевает, что вероятность добавления участником нового блока зависит от размера его стека – количества монет на балансе его кошелька, находящегося в сети. Чем монет на балансе больше, тем шанс выше.

Для добавления блока все также необходимо решить целевую задачу (аналогично PoW), однако сложность этой задачи рассчитывается для каждого пользователя индивидуально. Чем больше монет в кошельке, тем проще вычисления.

Классический POS предполагает распределение с открытием сети (формирования блока генезиса) сразу всех монет между пользователями и использование комиссий за проведение транзакций в качестве награды за обслуживание сети. Встречаются модели, где размер выплаты за добавление блока зависит от показателя возраста монеты – результата умножения общего числа монет на длительность их хранения одним пользователем. Тем самым обеспечивается стимул удерживать монеты на своем кошельке и гарантируется их дефицит в обращении.

POS также подвержен централизации, однако купить монеты гораздо проще, нежели купить оборудование и наладить майнинг (как в POW), что обеспечивает внутренний механизм, сдерживающий монополизацию за счет большого числа лиц, приобретающих монеты и владеющих ими.

Главное преимущество алгоритма Proof of Stake и главная причина его появления заключается в гарантированной защите от «атаки 51%». Для осуществления атаки необходимо выкупить 51% общей текущей массы монет. Фактически один пользователь должен выкупить «контрольный пакет акций», что маловероятно. Вдобавок, поскольку в случае «атаки 51%» большинство монет будет находиться на балансе инициатора атаки, главным пострадавшим в результате нее неизбежно будет он сам. Это делает атаку не только крайне затрудненной, но и совершенно бессмысленной.

Основные постулаты POS PZM Cash:

1. Шансы добавить новый блок зависят от количества монет на счету (баланс форжинга).
2. Возраст монеты никак не влияет на сумму вознаграждения за добавление блока.
3. Баланс форжинга представляет собой монеты, которыми располагает пользователь: статичные на кошельке за определенный период времени (монеты не были задействованы в транзакциях, в том числе неподтвержденных).
4. Величина комиссионного сбора составляет 0,5% от суммы транзакций и фиксирована. Участнику, добавившему блок, выплачивается 0,5% от общей суммы всех транзакций, вошедших в блок.
5. Никаких иных выплат за форжинг не предусмотрено.

Процесс добавления блока

Процесс добавления нового блока связан с основным процессом сети – осуществлением транзакций – и начинается на стороне пользователя. Чтобы описать работу PZM Cash, мы должны четко ограничить процессы пользовательской части и ядра. Транзакции не имеют никакого отношения к ядру – их инициирование производится на пользовательской стороне.

Пользователь заходит в свой кошелек, используя для этого закрытый ключ, и после принятия решения о проведении транзакции создает ее. Для этого:

1. Он указывает ее параметры: сумма, публичный ключ (адрес) получателя и т. д. Создать транзакцию можно только после корректного заполнения всех ее параметров в кошельке. Публичный ключ (адрес) лица или контракта, которому пересылается PZM Cash, обязателен для указания.
2. Формируется запрос на проведение транзакции. Программное обеспечение, которое подключается к сети криптовалюты, сообщает сети о намерении провести транзакцию. Самый простой вариант – использовать легкий криптовалютный кошелек PZM Cash Wallet.
3. Активные ноды (узлы) в сети криптовалюты перепроверяют историю блокчейна и убеждаются, что на балансе пользователя действительно есть монеты, которые он намерен отправить.
4. После подтверждения возможности совершения транзакция подписывается закрытым ключом и отправляется в пул нераспределенных транзакций, ожидающих добавления в блокчейн. Именно из этого пула форжеры набирают транзакции в блоки, которые они пытаются добавить.
5. Далее транзакция должна попасть в блок. Его впоследствии также должны будут перепроверить ноды в сети. После подтверждения транзакция не может быть отменена или изменена, можно лишь начать новую транзакцию.

Далее эта транзакция должна быть записана в блокчейн, что происходит уже на стороне ядра, к которому относится также алгоритм консенсуса. Ядро оперирует не отдельными транзакциями, а блоками, в которых транзакция – лишь одна из записей, поэтому блоки – это продукт алгоритма консенсуса. Они определяют, в каком порядке транзакции будут включены в журнал транзакций и в каком порядке «проведены».

Следующим шагом является принятие решение о том, кто сформирует следующий блок в леджере.

Кто имеет право добавлять блоки?

Как уже было отмечено, локальная копия блокчейна хранится на каждом узле в сети PZM Cash. Каждый аккаунт, который не заблокирован путем огласки закрытого ключа этой учетной записи, имеет возможность генерировать блоки, при условии, что по меньшей мере одна входящая транзакция в аккаунте была подтверждена 1440 раз. Любой аккаунт, соответствующий этим критериям, имеет право на форжинг.

Как выбирается генератор блока?

Для участия в процессе форжинга блока допущенный аккаунт подписывает предыдущий сгенерированный блок своим публичным ключом. Подпись далее хешируется с использованием хеш-функции SHA256.

Уникальность алгоритма консенсуса PZM Cash связана с механизмом вычислений, который имеет некоторое сходство с алгоритмом доказательства работы.

В POW все майнеры участвуют в своеобразном соревновании по нахождению хэша требуемого вида (с определенным количеством нулей в начале записи хэша). Получить требуемое значение можно только их перебором. При этом количество нулей в начале требуемой записи постепенно растет, растет количество вариантов, которые нужно перебрать, и требуемая мощность для добавления блока в требуемое время.

В PZM Cash поиск искомого хеша устроен сходным образом, однако расчеты не усложняются, а упрощаются со временем, так как число подходящих под критерии значений постепенно растет. Именно уровень сложности расчета хэша следующего блока определяет вероятность генерации блока: чем расчет сложнее, тем вероятность ниже. При этом сложность для каждого конкретного форжера различна.

Основное правило в том, что генератор, который первым получит хэш-значение ниже установленной планки, получает право сформировать блок. Со временем планка повышается, что гарантирует требуемую скорость добавления блока (для обеспечения скорости работы сети), поскольку «допустимая погрешность» искомого хэш-значения выше и число корректных исходов больше.

В POS участник, обладающий большим стеком (балансом монет) имеет большие шансы сформировать блок. Чем больше монет в кошельке, тем выше «индивидуальная планка» и шанс добавить блок. В PZM Cash в расчет принимается баланс кошелька (монеты), который был статичен на этом аккаунте для 1440 блоков за вычетом монет, участвующих в неподтвержденных отправленных транзакциях. Каждая нода обращается к кошельку для запроса баланса и вычисления степени повышения планки.

В итоге тот форжер, который раньше остальных получит требуемое хэш-значение (ниже установленной ему планки) получает право сформировать блок и добавить его в блокчейн. Транзакции в блок набираются из пула нераспределенных транзакций (максимальное число транзакций для одного блока – 255). В блоке делается запись о транзакциях, попавших туда из пула, также вносятся другие данные (например, хэш) и т. д. Суммарное количество транзакций ограничено размером блока. Сформированный блок отправляется на валидацию нодам, которые подтверждают его корректность. Транзакции считаются безопасными после десяти подтверждений блока. После корректного добавления блока все входящие в него транзакции считаются подтвержденными (то есть проведенными), монеты перераспределяются (в том числе

выплачиваются комиссии). Подтвержденные транзакции нельзя скорректировать или изменить, поскольку они записаны в блокчейн навсегда.

Форжинг

Термин «форжинг» используется в противовес термину «майнинг», характерному для POW. Он означает использование минимальных вычислительных мощностей для достижения консенсуса (в отличие от доказательства работы).

Уникальность форжинга PZM Cash состоит в том, что он не добавляет никаких новых монет в сеть, поскольку какое-либо вознаграждение за форжинг, приводящее к появлению дополнительной ликвидности в сети, отсутствует. Единственная предусмотренная плата за форжинг – это транзакционный сбор в размере 0,5% от общей суммы монет PZM Cash в транзакциях, которые попали в блок.

Транзакционные сборы присуждаются аккаунту, когда он успешно создает блок. По мере расширения сети будет расти и количество транзакций внутри нее – соответственно, и заработок в виде форжинга будет увеличиваться.

Параметры сети

Для интерактивного отображения и доступного мониторинга состояния сети PZM Cash на сайте реализована аналитическая интерактивная форма PZM Cash Explorer, где каждый участник может увидеть текущую производительность сети, оборот монет и размер транзакционных сборов.

В среднем новый блок генерируется каждые 60 секунд. Эта логика не зависит от количества транзакций, однако максимальное число транзакций, которые может содержать один блок, ограничено 255-ю. При максимальной производительности сети (максимально допустимое число транзакций в блоке) PZM Cash способна подтверждать до 367 200 транзакций в сутки (1440 блоков в сутки).

Безопасность

- Используется проверенный временем криптографический алгоритм хэширования SHA256, построенный на структуре Меркла – Дамгора.
- Для осуществления «атаки 51%» (возможность исключения транзакций или изменения порядка транзакций) злоумышленнику требуется получить контроль над 51% всех монет PZM Cash, то есть получить контроль или подкупить, подговорить форжеров, что с развитием сети становится все более маловероятным.
- Злоумышленник может попытаться повысить свою вероятность форжинга путем перетасовки, то есть перемещения большого количества монет на один аккаунт. Во избежание подобных действий вводится правило статичности PZM Cash в аккаунте для 1440 блоков в сутки. Именно эти монеты на балансе определяют вероятность форжинга. В случае подобной атаки злоумышленник не сможет форжить ничего в течение суток, что сулит ему большие потери.

4. Модель развития

Наша стратегическая задача – быстрый рост экосистемы. Это важно, потому что:

1. Появление новых проектов создает дополнительные ценности для потребителей за счет добавления новых продуктов и услуг.
2. Увеличение спроса ведет к балансировке предложения, а увеличение оборота способствует стабильности PZM Cash по отношению к внешней среде (стабильности и укреплению обменного курса).

Для успешного развития необходимо предусмотреть обоснованный алгоритм наполнения сети ликвидностью (эмиссия монет PZM Cash), а также каналы масштабирования сети.
Участниками публичной экосистемы PZM Cash могут быть:

- частные проекты;
- индивидуальные пользователи;
- разработчики и создатели проектов и приложений;
- провайдеры фондирования и инвестирования (VC, бизнес-ангелы – инвесторы, акселераторы, инкубаторы);
- публичные и государственные агенты;
- ассоциации, союзы и объединения;
- другие участники.

Участие в экосистеме обеспечивает комплекс конкурентных преимуществ:

- доступ к растущей платежеспособной клиентской базе, которая позволяет масштабировать бизнес и наращивать прибыль;
- получение многих технических и технологических решений и автоматизация бизнес-процессов: системы взаиморасчетов, системы умных контрактов, формирование истории

работы компании, отслеживание репутации контрагентов, противодействие фальсификации и т. д.

- возможность выстраивать партнерские отношения и ценностные цепочки;
- повышение деловой репутации и статуса по мере развития окружающей среды;
- доступ к финансированию и внимание венчурных фондов и других источников финансирования;
- выход на международный рынок при присоединении к сети.

Ликвидность сети

Очевидно, что спрос и предложение формируют цену товаров и услуг. Именно спрос и предложение на валюту формируют ее обменный курс. Ключевым вопросом любой криптовалюты является вопрос стабильности ее курса по отношению к фиатным деньгам и другим криптовалютам. Для того чтобы курс был стабильным, необходимо обеспечить достаточное предложение монет PZM Cash, которое формируется в экосистеме по алгоритму наполнения ликвидности. А также достаточный спрос, который обеспечивается за счет роста количества доступных услуг и сценариев использования для участников.

Спрос на PZM Cash будет расти за счет:

- интеграции партнеров, которые будут использовать PZM Cash в качестве платежной единицы;
- Dapps и Apps разработок (расширения услуг сети).

С другой стороны, мы должны предусмотреть корректный механизм наполнения сети ликвидностью (эмиссия монет PZM Cash). Ликвидность экосистемы (монеты PZM Cash) будет обеспечена в два этапа:

- начальное предложение PZM Cash (на стадии премайнинга);
- расширение ликвидности PZM Cash (на стадии PoS майнинга).

Начальное предложение – это монеты PZM Cash, которые будут распределены в ходе предварительной реализации (премайнинга) при генезисе первого блока. Начальное предложение представляет собой то количество PZM Cash, с которым сеть начинает свою работу – то есть это стартовая ликвидность для запуска системы. Любой, кто станет участником сети на данном этапе, будет иметь преимущество за счет раннего входа, поскольку раньше остальных получит право на обеспечение дополнительной ликвидности за счет PoS майнинга.

С началом работы сети (запуском основной сети) будет запущен процесс расширения ликвидности – PoS майнинг. Увеличение ликвидности в экосистеме PZM Cash произойдет за счет получения участниками сети дохода за участие в ней.

PoS майнинг – единственный механизм дополнительной эмиссии PZM Cash, других механизмов не предусмотрено. Форжинг как способ получения монет за счет оказания услуг по обслуживанию сети не создает дополнительной ликвидности, а представляет собой поток перераспределения монет от участников транзакций к участникам, регистрирующим их. Потоки перераспределения не приводят к увеличению общего количества PZM Cash в системе и росту ликвидности в сети. К ним можно отнести:

- комиссии за транзакции (fee);
- платежи, связанные со смарт-контрактами;
- платежи по другим операциям;
- обменные операции (PZM Cash – крипта, PZM Cash – фиат).

Премайнинг

- Первоначальная эмиссия составляет 90 млн PZM Cash (или 1% от общей итоговой ликвидности, которая составит 9 млрд PZM Cash).
- Распределение монет будет реализовано следующим образом:
    - 0,7% (63 млн PZMC) направлено на Public Sales;
    - 0,1% (9 млн PZMC) – команде проекта PZM Cash с блокировкой вывода на один год;

    - 0,2% (18 млн PZMC) – на маркетинговые кампании в течение трех лет после запуска блокчейна.
- Монеты будут выпущены и распределены (отправлены на адреса) со стартом сети (генерацией исходного – первого блока в сети).
- Монеты по первоначальной эмиссии будут распределены децентрализовано между большим числом участников, которые составят первоначальную пользовательскую базу.
- Согласно логике PoS первоначальные пользователи получат преимущества раннего входа, что позволит им начать форжить раньше остальных.

PoS майнинг

PoS майнинг предусмотрен в качестве единственного механизма роста ликвидности сети и представляет собой механизм предоставления увеличения баланса монет лояльным пользователям PZM Cash. Он предусматривает начисление PZM Cash по ставке наращения на остаток средств на любом активированном кошельке участника. При этом в расчет берется только эффективный баланс кошелька, куда не входят монеты, включенные в неподтвержденные транзакции.

Ставка наращения выражается в месячном процентном исчислении и зависит от двух параметров:

1. Текущего баланса на активном ведущем кошельке.
2. Текущего суммарного баланса на кошельках поддержки – тех, которые были добавлены владельцем ведущего кошелька в качестве поддержки.

Ставки наращения не меняются со временем. Во избежание опасной централизации сети максимальный баланс одного кошелька может составлять 1 000 000 PZM Cash (или 0,011% от общей итоговой ликвидности, которая составит 9 млрд PZM Cash). По достижении данного значения баланса PoS майнинг для данного кошелька становится недоступным.

Как происходит добавление кошелька поддержки

Как было сказано ранее, активация кошелька происходит путем входящей транзакции на этот кошелек по публичному ключу. Здесь имеет значение, от кого пришла данная транзакция, – именно отправитель и является ведущим кошельком, поскольку вводит нового пользователя в сеть. Таким образом, активированный по его транзакции кошелек становится его кошельком поддержки. При этом вновь активированный кошелек получает права ведущего; поэтому каждый ведущий кошелек имеет уникальную структуру кошельков поддержки.

PoS майнинг становится доступен для кошелька с момента его активации. Для этого ведущий кошелек должен перечислить во входящей транзакции минимум 1 PZM Cash.

Как считается ставка прироста баланса монет на кошельке

Ставка прироста баланса на кошельке представляет собой обычную ставку наращения по простому проценту, вычисляемую на двухфакторной основе. Ставка наращения является базовой ставкой увеличения баланса монет и зависит от текущего баланса кошелька. Мультипликатор зависит от количества монет на кошельках поддержки для каждого конкретного ведущего кошелька. Оба значение тем выше, чем выше суммарное количество монет. Кошельки поддержки объединяются в структуру на максимальную глубину в 2 уровня.

Начисление производится по значению эффективной ставки, которая вычисляется умножением ставки наращения на мультипликатор. Максимальная ставка прироста баланса монет участника составляет 21% в месяц, минимальная – 1,2% в месяц или 14,4% в год.

Таблица 1

«Метрики расчета ставки прироста монет»

Баланс ведущего кошелька	Ставка в месяц	Сумма балансов кошельков поддержки	Мультипликатор	Порядок (min и max значения) в % в мес
Топ-держатели		Зрелая сеть		
700 000 – 1 000 000	6,89%	Свыше 100 000 000	3,14	21%
500 000 – 699 999	5,35%	30 000 000 – 99 999 999	3,0	
300 000 – 499 999	4,14%	10 000 000 – 29 999 999	2,9	
Простые держатели		Развитая сеть		
200 000 – 299 999	3,69%	5 000 000 – 9 999 999	2,7	
100 000 – 199 999	3,15%	1 000 000 – 4 999 999	2,5	
50 000 – 99 999	2,63%	500 000 – 999 999	2,3	
20 000 – 49 999	2,11%	200 000 – 499 999	2,1	
Миноритарии		Начальная сеть		
10 000 – 19 999	1,70%	100 000 – 199 999	1,7	
5000 – 9999	1,61%	50 000 – 99 999	1,6	
2000 – 4999	1,52%	20 000 – 49 999	1,5	
1000 – 1999	1,43%	10 000 – 19 999	1,4	
500 – 999	1,37%	5000 – 9 999	1,3	
100 – 499	1,28%	1000 – 4 999	1,2	
1 – 100	1,20%	Менее 1000	1,16	
		0	0	1,20%

Когда начисляются дополнительные монеты

Начисление накопленных монет производится при подтверждении любой исходящей транзакции кошелька (изменение текущего баланса). В этот момент производится «слепок» баланса кошельков

поддержки – за исключением монет, которые попали в пул нераспределенных транзакций, то есть ожидают отправки). Таким образом, чем больше с аккаунта проходит исходящих транзакций, тем чаще производятся выплаты. С другой стороны, также имеется экономический смысл держать монеты на кошельке и получать начисления по схеме сложных процентов.

5. Масштабирование сети

Как уже отмечалось, главная характеристика PZM Cash – это ориентация на быструю масштабируемость как денежной массы, так и предложения услуг со стороны разработчиков и партнеров. Развитие и масштабирование инфраструктуры PZM Cash может осуществляться по нескольким направлениям.

1. Создание Dapps

В данном случае любой разработчик может развернуть свое децентрализованное приложение. В этом случае ему будет выделен собственный сайдчейн, записанный поверх основного леджера. При этом у каждого пользователя приложения будет свой собственный кошелек.

2. Экспорт протокола

Исходный код PZM Cash открыт для всех, что позволяет любому разработчику внедрить протокол PZM Cash в свой проект в качестве ядра. Для этого необходимо развернуть и запустить полную ноду (сетевой узел) и установить и синхронизировать специальный API-модуль.

3. Валюта у партнеров

Валюту PZM Cash можно использовать в качестве средства платежа на партнерских проектах и платформах. Web3js-технология, реализованная в PZM Cash Wallet, позволяет использовать кошелек для осуществления расчетов на ресурсах партнеров (обменник, биржа, ИМ).

6. Дорожная карта

Q2.2020

- Публичная продажа PZM Cash
- Запуск основной сети PZM Cash и онлайн-кошелька
- Листинг на CoinMarketCap

Q3.2020

- Запуск кошельков Android/iOS
- Запуск Web3js
- Создание сети обменных пунктов
- Выход на рынки Азии
- Активное привлечение разработчиков приложений и сервисов

Q4.2020

- Возможность создания смарт-контрактов
- Выход на рынок Латинской Америки

Q1.2021

- Создание сети банкоматов и выдача дебетовых карт
- Открытие технологического хаба PZM Cash Foundation

Q2.2021

- Проведение первой международной конференции PZM Cash Summit

Q3.2021

- Внедрение новых партнеров и сервисов для расширения способов оплаты

7. ВНИМАНИЕ! ОТНОСИТЕЛЬНО ЗАЯВЛЕНИЙ

Все заявления, содержащиеся в данном документе, сделанные в пресс-релизах или в любом месте, доступном для общественности, а также устные заявления, которые могут быть сделаны PZM CASH или их соответствующими директорами, должностными лицами или сотрудниками, действующими от имени PZM CASH (в зависимости от обстоятельств), которые не являются заявлениями об историческом факте, представляют собой «заявления о перспективах». Некоторые из этих заявлений могут быть определены с помощью прогнозных терминов, таких как «цель», «предвидеть», «поверить», «оценить», «ожидать», «если», «намереваться», «может», «план», «возможный», «вероятный», «проект», «должен», «будет» или другие подобные термины. Однако эти условия не являются исключительным средством определения прогнозных заявлений. Все заявления, касающиеся финансового положения PZM CASH, бизнес-стратегий, планов и перспектив, а также будущих перспектив отрасли, в которой находится PZM CASH, являются прогнозными заявлениями. Эти прогнозные заявления, включая, но не ограничиваясь заявлениями о доходах и прибыльности PZM CASH, перспективах, планах на будущее, других ожидаемых тенденциях в отрасли и других вопросах, обсуждаемых в данном документе относительно PZM CASH, являются заявлениями, которые не являются историческими фактами, но лишь прогнозами.

Эти прогнозные заявления включают известные и неизвестные риски, неопределенности и другие факторы, которые могут привести к тому, что фактические будущие результаты или достижения PZM CASH будут существенно отличаться от любых будущих результатов или достижений, ожидаемых, выраженных или подразумеваемых.

Эти факторы, среди прочего, включают:

а) изменения в политических, социальных, экономических и рыночных условиях на фондовом рынке или рынке криптовалют, а также в нормативной среде в странах, в которых PZM CASH осуществляет свою деятельность;

б) риск того, что PZM CASH может оказаться не способным или выполнить, или реализовать свои соответствующие бизнес-стратегии и планы на будущее;

в) изменения в процентных ставках и обменных курсах фиатных валют и криптовалют;

г) изменения в стратегиях ожидаемого роста и ожидаемого внутреннего роста PZM CASH;

д) изменения в наличии и сборах, подлежащих уплате PZM CASH, в связи с их деятельностью;

е) изменения в наличии и заработной плате сотрудников, которые требуются PZM CASH для управления соответствующими предприятиями и операциями;

ж) изменения в предпочтениях клиентов PZM CASH;

з) изменения условий конкуренции, в которых работает PZM CASH, и способность PZM CASH конкурировать в таких условиях;

и) изменения будущих потребностей в капитале PZM CASH и наличия капитала для финансирования таких потребностей;

к) война или акты международного или внутреннего терроризма;

л) случаи катастрофических событий и стихийных бедствий, которые влияют на бизнес и/или деятельность PZM CASH;

м) другие факторы, не зависящие от PZM CASH;

н) любые риски и неопределенности, связанные с PZM CASH и их предприятиями и операциями, XXX-токенами, первоначальной продажей токенов PZM CASH и кошельком PZM CASH (каждый из которых указан в Белой книге).

Все прогнозные заявления, сделанные или относящиеся к PZM CASH или лицам, действующим от имени PZM CASH, прямо квалифицированы такими факторами. Принимая во внимание, что риски и неопределенности, которые могут привести к тому, что фактические будущие результаты или достижения PZM CASH будут существенно отличаться от ожидаемых, выраженных или подразумеваемых в прогнозных заявлениях в настоящей Белой книге, не следует чрезмерно полагаться на эти заявления , Эти прогнозные заявления применимы только на дату настоящей Белой книги.

Ни PZM CASH, ни какое-либо другое лицо не заявляют, не гарантируют и/или не обязуются, что фактические будущие результаты или достижения PZM CASH будут такими, как обсуждено в этих

прогнозных заявлениях. Фактические результаты или достижения PZM CASH могут существенно отличаться от ожидаемых в этих прогнозных заявлениях.