X-CASH: Глобальная блокчейн-сеть для осуществления платежей на базе криптовалют

Гийем Шомон, Пол Буниот, Зак Хильдрет

Аннотация. **С момента зарождения биткойна в 2009 году и до настоящего времени появляется все больше и больше препятствий, мешающих ежедневному использованию криптовалют основной аудиторией. Данный документ содержит подробное описание концепции криптовалюты X-CASH и то, как она планирует решать поставленные задачи. Одним из ключевых понятий, описанных в этой статье, является тройственная связь между покупателями, продавцами и банками. Предлагая решение "всё в одном", которое соединит их, сможет выполнять конвертацию криптовалюты в фиатные деньги и обрабатывать платежи, X-CASH нацелен на революцию в индустрии платежей, обеспечивая низкие затраты при одновременном повышении безопасности и гарантируя при этом масштабируемость и приемлемое время обработки транзакций.**

Для того, чтобы удовлетворить растущий спрос на регулирование в криптовалютном пространстве, X-CASH также разрабатывает обновление сети для частичной анонимности, где пользователи смогут раскрывать часть информации о транзакциях. Это станет возможным благодаря включению дополнительных данных в блокчейн.

С целью удовлетворения потребностей корпоративных клиентов в технологии блокчейн и решения проблемы масштабируемости X-CASH также разрабатывает технологию сайдченов, благодаря которой операторы смогут запускать свои собственные цепочки с нестандартными транзакциями. Благодаря доказательному характеру сети с нулевым разглашением участники смогут обмениваться документами или информацией, не раскрывая свою личность или содержание данных. Одним из ключевых бизнес-кейсов этого решения могло бы служить скрытое подписание контрактов между двумя субъектами, в котором сеть является свидетелем транзакции. Суть и детали сделки будут оставаться неразглашенными до тех пор, пока не возникнет необходимость в раскрытии информации, например, в юридических целях.

Ключевые слова: **блокчейн, криптовалюты, платежный шлюз, платформа для конвертации криптовалюты в фиат, X-CASH, сайдчейны, доказательство с нулевым разглашением.**

СОДЕРЖАНИЕ

I. ВВЕДЕНИЕ

Цифровые платежи в реальном мире уже являются распространенной практикой - почти 500 млрд. транзакций в год осуществляется по всему миру [1]. Несмотря на надежность с технической точки зрения, современные цифровые платежные решения предполагают высокие комиссии для продавцов в диапазоне от 0,1% до 2%. Кроме того, эти решения сопряжены с дополнительными расходами с точки зрения клиентов, особенно если они не используются на территории их государства.

В то же время, цены на криптовалюты продемонстрировали экспоненциальный рост начиная с 2017 года [2]. Несмотря на способность криптовалют преодолевать географические барьеры, они все еще редко используются для повседневных платежей. Этому есть ряд причин: трудная конвертация в фиатные валюты, низкая масштабируемость, высокие затраты на отправку [3], отсутствие законодательной базы и прозрачности сделок в мировом масштабе. [4].

Когда дело доходит до оформления юридических документов или осуществления какого-либо платежа, корпорации, банки и прочие учреждения по-прежнему широко используют процедуры, отнимающие много времени и денег, не взирая на тот факт, что всё вокруг имеет тенденцию к цифровизации.

Используя PoW сеть, построенную на алгоритме Cryptonote криптовалюты Monero с интегрированным сетевым решением "сайдчейн", команда X-CASH полагает, что имеется серьезный потенциал для слома действующих методов осуществления расчетов, и готова предложить корпорациям новый способ выполнения транзакций.

II. ПРОЕКТ X-CASH

A. Цели проекта

X-CASH [5] - финтех стартап, зарегистрированный в г.Париж, Франция в начале 2018 года. Проект полностью самофинансируется и управляется тремя блокчейн-энтузиастами разных специализаций (финансы, инженерия, компьютерные науки). Основная цель X-CASH - предложить на основе технологии блокчейн глобальное решение для осуществления цифровых платежей и вознаграждений за транзакции, которое позволит снизить размер комиссий и время исполнения транзакций.

Будучи зарегистрированной во Франции, компания стремится соответствовать всем действующим и разрабатываемым нормам законодательства Франции и ЕС. Так же X-CASH намерено тесно сотрудничать с финансовой отраслью в целях создания крепкой связи с существующими банковскими системами. Эти шаги являются обязательными для повсеместного внедрения криптовалюты. Регламенты обеспечат защиту пользователей и инвесторов, а банки послужат катализатором благодаря серьезной базе розничных клиентов.

B. Базовая технология

X-CASH основана на исходном коде Monero v7 [6], который в свою очередь является производным от Cryptonote [7] и использует хэш-функцию CryptoNight [8] [9]. Для разработки X-CASH выбор пал на указанный исходный код блокчейн, в связи с тем, что он является проверенным, систематически улучшается и обновляется.

Главная привлекательность Monero заключается в анонимности. Monero использует запутанную публичную книгу. Это значит, что любой пользователь может транслировать или отправлять транзакции, а сторонний наблюдатель не может определить источник, сумму или назначение платежа. Анонимность является важным фактором в управлении личными финансами, в то время как банки и учреждения должны владеть информацией об источнике средств в целях трассировки платежа. По этой причине X-CASH предлагает пользователям возможность выбора: хотят ли они, чтобы их транзакция была публичной, или нет.

Кроме того, чтобы сделать синхронизацию блокчейна более быстрой, чем у других криптовалют, а также уменьшить задержки транзакций, была реализована международная сеть выделенных серверов. Это крайне важный компонент развёртывания для будущего развития ядра X-CASH.

C. Объем и структура эмиссии

Общий объем эмиссии X-CASH составит 100,000,000,000 (100 миллиардов) XCASH. Средства будут распределены следующим образом:

- Из 5%, предназначенных команде, 2% монет уже распределены. Остальные будут доступны для новых участников. Выпуск этих монет регулируется жесткими условиями, связанными с рыночной капитализацией монеты.
- 10% монет предоставляется компании для выплат зарплат членам команды и разработчикам, и расходов на развитие инфраструктуры.
- 5% от общего объема эмиссии будет реализовано частным инвесторам через внебиржевые торги со скидкой 5-30% от спотовой рыночной цены. Идея заключается в том, чтобы привлечь некоторое финансирование на ранней стадии проекта, не влияя на спотовую цену монеты (проданные монеты должны пройти этап наделения имущественными правами).
- 20% будет распределено в течение 20 месяцев по программе аирдропов. Этот вариант был выбран в связи с тем, что это справедливый способ распределить монеты людям не имеющим оборудование для майнинга, одновременно позволяющий привлечь комьюнити.

Рост текущей эмиссии составит ориентировочно 4% в месяц, это значит, что 95% монет будет выпущено приблизительно в конце 2020 года. К этому моменту релиз X-CASH 2.0 будет работать уже с помощью алгоритма PoS, а уровень инфляции составит 0,1-0,5%.

Кроме того, эмиссия распределяемых команде средств находится в зависимости от рыночной капитализации монеты. Начиная с капитализации в 10 миллионов долларов США и каждый раз, когда она будет увеличиваться в 10 раз, 20% выделенных команде монет будут разблокированы. Такой подход обеспечит достижение поставленных целей и позволит избежать жесткого дампа на биржах, вместо блокировки монет на неопределенный срок.

Поскольку не существует способа отслеживать количество монет в кошельке через публичный адрес, премайн подлежит ежеквартальной проверке с момента его зачисления на счет. Независимый аудит должен подтвердить, что средства всё ещё находятся в отдельном кошельке. Эта процедура будет осуществляться с непосредственным привлечением членов команды, поскольку их монеты находятся в холодных кошельках, ключи от которых хранятся в банковских ячейках.

В связи с тем, что премайн подлежит зачислению на отдельные счета и сможет попадать в оборот только постепенно, будет существовать разница между количеством выпущенных монет и их реальным оборотом. На приведенном ниже рисунке представлен график, показывающий изменение прогнозируемого оборота монет с течением времени.

D. Команда основателей

Основателями X-CASH являются три человека, обладающие различными академическими и профессиональными навыками и объединенные общей задачей: разработка реалистичного блокчейн-проекта с разумными целями. Команда выглядит следующим образом:

Гийем Шомон
Управляющий

Гийем - бывший трейдер, который оставил свою работу, чтобы сконцентрироваться на разработке новой криптовалюты и заполнить пробел между блокчейн-технологией и её практическим внедрением. С 2016 года Гийем является активным трейдером и инвестором, что привело его к созданию майнингового центра в конце 2017 года.

Гийем владеет двумя степенями магистра: в области энергетики от Ecole Centrale de Lyon и в области международных финансов от HEC Paris. Благодаря своему двухлетнему опыту торговли деривативами в одном из крупнейших банков, Гийем приобрел хорошее понимание механизмов управления в финансовой сфере. До этого он был студентом-исследователем в области ядерной инженерии в Commissariat à l'Energie Atomique.

Зак Хильдрет
Главный технолог

Обладатель степени бакалавра в области компьютерных наук. Зак является фулстек-разработчиком, владеющий навыками web-программирования, разработки игр и программного обеспечения. Специализируется также на кибербезопасности, благодаря чему возник его интерес к технологии блокчейн. Инвестирует в криптовалюты с 2013 года и с тех принимает активное участие в блокчейн-комьюнити.

Зак также является автором детальных инструкций по майнингу криптовалют и техническим директором одного из самых активных майнинг-сообществ.

Пол Буниот
Исполнительный директор

После получения степени магистра в области нанотехнологий в Национальном Институте прикладных наук, Пол работал инженером-исследователем в Национальном научно-исследовательском центре, затем патентным адвокатом в автомобильной промышленности. В поисках интересных возможностей он возглавил компанию по распространению нанотехнологических решений во Франции и Европе.

Увлеченный новыми технологиями и стартующим предприятием, Пол присоединился к проекту X-CASH.

E. Дорожная карта

С начала 2018 года по сентябрь 2018 года: старт разработки, релиз майннета, старт ежемесячных айрдропов, листинг на биржах.

Проект X-CASH дал ростки в первом квартале 2018 года. Первая цепочка блокчейна была успешно опробована, и на её основе запущен проект.

Разработан web-сайт и его функционал. Чтобы дать возможность технически не подкованным пользователям быстро начать пользоваться кошельком, была выпущена и протестирована первая версия GUI-кошелька.

После тщательного тестирования и оценки работы сети, выполненной в июне 2018 года, 31 июля сеть X-CASH была представлена общественности. Через три недели после релиза майннета, 21 августа, стартовала программа ежемесячных аирдропов. После распределения первого аирдропа, 11 сентября X-CASH объявила о своем выходе на рынок с листингом на четырех биржах.

3й - 4й квартал 2018: X-CASH 1.3 - bulletproof и публичные транзакции.

Первым обновлением проекта X-CASH послужит реализация bulletproof-транзакций. Bulletproof-транзакции обеспечат последовательное уменьшение размеров транзакций, что позволит замедлить процесс увеличения размера блока и уменьшить комиссию за осуществление транзакций. В то же время появится возможность выполнять публичные транзакции, что позволит пользователям раскрывать информацию о транзакциях.

4й квартал 2018: Выпуск мобильной версии кошелька.

Одной из ключевых составляющих успеха X-CASH сможет стать его использование населением. Для этого пользователям необходим максимально понятный и удобный интерфейс на всех устройствах.

Кошелек GUI был разработан с учетом кроссплатформенного применения. Идея состоит в том, чтобы спроецировать навыки пользователя на любое устройство, будь то рабочий стол компьютера, ноутбука или мобильное устройство.

Благодаря мобильной версии кошелька пользователи смогут автоматически подключаться к сети, не беспокоясь о настройках, отвечающих за оптимальный пользовательский интерфейс.

Одним из драйверов для внедрения X-CASH является возможность использовать систему непосредственно для осуществления расчетов между покупателями и продавцами услуг. Не смотря на то, что API-интерфейсы уже сейчас могут быть предложены третьим лицам для интегрирования X-CASH-платежей, основной целью является создание инфраструктуры, которая позволит конвертировать X-CASH в фиатные валюты.

Чтобы добиться этого, X-CASH планирует предложить рынку платежные операции, позволяющие легко ликвидировать позицию с переводом её в фиатную валюту для независимой обработкой таких платежей.

В итоге, X-CASH сможет предложить покупателям возможность оплаты либо в фиате, либо в X-CASH. Платежи в X-CASH не будет облагаться существенными комиссиями, а комиссии для фиатных платежей составят 30-50 базисных пунктов (0,3-0,5%).

1й квартал 2019: релиз X-CASH 2.0

Несмотря на то, что в настоящий момент команда сосредоточена на успешном запуске первой версии X-CASH, она уже сейчас планирует будущее блокчейна. В релизе X-CASH 2.0 предстоит проработать две важные темы: масштабируемость и фундамент для разработки API. Существует три варианта:

- Развитие текущего кода: это естественный путь, на котором сконцентрирована команда. Он состоит из пошаговых релизов, которые позволят проекту постепенно достичь своих целей при сохранении cryptonote и cryptonight PoW в качестве исходного кода. Следующий релиз X-CASH 1.3 запланирован на конец сентября, в котором будут добавлены bulletproof-транзакции.
- Создание новой технологии / кода ядра с нуля: для достижения целей X-CASH возможно создание нового кода блокчен, включая блокчейн постоянного размера или сжимаемый блокчейн. Это, конечно, увлекательный путь, но он требует много времени и ресурсов.
- Внедрение X-CASH в существующий протокол: внедрение X-CASH в более развитую блокчейн-сеть - это еще один вариант развития. Контракты ERC20, как и другие стандарты на блокчейне Ethereum, могут быть интересны, но не жизнеспособны на данный момент, поскольку они всё ещё не масштабируемы. Аналогичным образом, EOS предлагает решения, которые могут снять ряд проблем, с которыми сталкивается проект X-CASH. Подведя итог, можно сказать, что в настоящее время указанная технология не является достаточно зрелой, но запуск параллельных практических решений и соответствующий пересмотр позиций X-CASH поможет найти верный путь.

После внимательного осмысления представленных вариантов, в начале сентября 2018 года было выбран первый вариант эволюции существующего кода X-CASH. Это приведет к релизу PoS-версии cryptonote в начале 2019 года с последующей реализацией сайдчейнов.

1й квартал 2019: внедрение X-CASH в розничные банковские протоколы

Если говорить о розничных платежах, то конечной целью является партнерство с банками (скорее всего с онлайн-банками), для того, чтобы предложить пользователям возможность управлять своими X-CASH непосредственно со своего банковского счета.

Это было бы интересной особенностью и для банков, так как спрос на криптовалюты все еще растет, а такой вариант мог бы стать быстрым решением для клиента обзавестись криптовалютой, поскольку банк по-прежнему играет роль надежного держателя средств от имени клиента.

В то же время, это позволит реализовать блокчейн технологию для нужд банка, в таких сферах как аккредитивы, кредитные контракты и других услугах.

2й квартал 2019: производные инструменты, связанные с X-CASH

В то время как конвертация X-CASH в фиатные валюты для розничных клиентов будет конкурентоспособной с первого дня, имеются возможности для ряда улучшений, способных снизить комиссии.

В этих целях X-CASH планирует выпустить производные инструменты, которые увеличат ликвидность X-CASH и позволят пользователям легче хеджировать позиции трейдеров.

Первый шаг - фьючерсные контракты для выпуска опционов, которые позволят избежать рисков большой волатильности.

Благодаря широкому использованию этих инструментов, мы сможем обеспечить "plug and play" решение для покупателей и продавцов с фиксированной комиссией от 10 до 35 базисных пунктов (0,10-0,35%).

III. X-CASH 1.0 АЛГОРИТМ CRYPTONOTE

A. Proof of Work (доказательство работы)

Proof of Work (PoW) - тип алгоритма, используемый для достижения консенсуса в сети блокчейн на основе количества работы (хэшей) участников сети. В то время как сеть объединяет потенциальные транзакции, чтобы добавить их в следующий блок, майнеры корректируют nonce так, чтобы хэш блока соответствовал определенному набору параметров (обычно это хэш, начинающийся с нулей). Этот процесс требует много вычислительной мощности, поскольку невозможно заранее предопределить nonce, который бы удовлетворял решению майнинг-уравнений. Поэтому майнеры вынуждены перебирать значения nonce в случайном порядке или пошаговым способом, после чего делать расчеты хэшей и проверять, удовлетворяют ли они требуемым параметрам. Набор параметров может быть преобразован в то, что называют "сложностью", которая отражает количество nonce, необходимое для расчета хэша при поиске блока. На момент написания статьи сложность сети X-CASH составляет около 186M [10]; из чего следует, что сеть вычисляет около 3M хэшей в секунду, чтобы удовлетворить параметру "время нахождения блока" (60 сек).

X-CASH использует новейший ASIC-устройчивый алгоритм Cryptonote v7 от Monero. Мы все еще обсуждаем, будем ли мы модифицировать алгоритм, чтобы сделать его устойчивым к NiceHash. Если не будут происходить серьезные манипуляции с хэшрейтом сети, мы будем придерживаться текущей версии, поскольку NiceHash в настоящее время позволяет повысить конкурентоспособность вычислительной сети.

B. Кольцевая подпись

Кольцевая подпись является основой анонимности Monero. В транзакцию публичной блокчейн-сети, такой как биткоин, добавляется только сигнатура отправителя. В X-CASH каждая транзакция должна быть подписана как минимум двумя участниками. По умолчанию транзакции подписываются 6-ю участниками, что затрудняет идентификацию истинного отправителя. В контексте будущего развития X-CASH мы также рассматриваем возможность включения уникальной кольцевой подписи [11].

C. Stealth-адреса

Stealth-адреса [12] [13] являются дополнительным уровнем конфиденциальности в транзакциях, что потребует от отправителя сгенерировать одноразовый случайный адрес. Это означает, что никакой публичный адрес не будет записан в блокчейн, и что нет возможности просматривать баланс публичных адресов с помощью блокчейн-эксплорера. В то время когда использование кольцевых подписей является способом избежать отслеживание истории транзакций, stealth-адреса можно рассматривать как решение для скрытия деталей транзакций. В разделе E описывается, как анонимность может быть снята по усмотрению пользователей путем использования расширенного реестра для хранения дополнительных данных.

D. Bulletproof-транзакции

Bulletproof-транзакции [14] [15] заменят range proofs, используемые в текущем алгоритме, и позволят уменьшить размер транзакции. Bulletproof представляет собой улучшение

по сравнению с range proofs, которое основано на изменении математического алгоритма, используемого для скрытия и подтверждения сумм транзакции. X-CASH планирует осуществлять bulletproof-транзакции, как только они будут проработаны и запущены Monero с ожидаемым уменьшением размера транзакции на 80%. Имплементация bulletproof-транзакций в сети Монро запланирована на сентябрь 2018 года и будет добавлена в X-CASH код сразу же после релиза.

E. Реализация частичной анонимности

Конфиденциальность в криптовалютном пространстве, как и в финансовом мире, является очень чувствительной темой. Цель этого раздела - представить краткий обзор философии X-CASH в отношении анонимности.

1) Три вида анонимности

Любая транзакция, которая включает в себя передачу информации (например, платеж с помощью криптовалюты), может быть разделена на три основных компонента:

1. Отправитель: кто инициирует транзакцию
2. Получатель: кто получает выгоду от сделки
3. Содержание: какая сумма перечисляется в случае финансовой оплаты, иная информация подлежащая отправке.

Конфиденциальную информацию можно также разделить на три вида анонимности:

1. Полная анонимность: нет способа узнать информацию без ключа или пароля
2. Частичная анонимность: информация отслеживается, но основные сведения скрыты. Например IBAN (адрес банковского счета) или BTC-адрес. Этот адрес отслеживается и представляет собой потенциального отправителя или получателя, но окончательные сведения скрыты за адресом, т.е. личность человека, контролирующего адрес, не разглашается
3. Отсутствие анонимности: внутренняя информация доступна для всех.

Сочетание этих факторов приводит к двум примечательным случаям:

a) Полная анонимность всей информации

Любая информация, включенная в транзакцию, скрыта от обычных пользователей. Это так или иначе относится ко всем монетам Cryptonote, использующим исходный код Monero.

b) Частичная анонимность отправителя и/или получателя, при котором содержание остается публичным

Наиболее очевидным вариантом такого использования является транзакция биткоина, когда отправители и получатели скрыты за публичным адресом, но сумма транзакции полностью отображается.

Идея реализации частичной анонимности в коде Monero обусловлена необходимостью предложить пользователям, осуществляющим транзакции в сети, первые два варианта анонимности. Это позволит удовлетворить львиную долю потребностей для частной жизни, при этом предоставит необходимый базис для реализации публичных сделок, которые будут актуальны в контексте усиления регулирования в криптовалютном пространстве [16] [17]. Несмотря на то, что другие случаи, такие как раскрытие всей информации, могут быть интересны для изучения, они не рассматриваются в этом документе, поскольку какие-либо задачи по их реализации в ближайшее время отсутствуют.

2) Техническое воплощение

Решение, выбранное для технического воплощения транзакций с частичной анонимностью, представляет собой компромисс между простотой развертывания, масштабируемостью исходного кода, функционалом и безопасностью. Чтобы избежать хард-форка исходного кода Monero, было решено не изменять компоненты транзакций в коде ядра X-CASH. Преимущество такого решения заключается в том, что остается возможность для бирж, майнинг-пулов, трейдеров и других лиц, использующих сеть X-CASH, либо реализовать его, либо нет. Одновременно тестируются два варианта. Первый представляет собой включение дополнительных данных в отдельный реестр, в то время как второй будет интегрировать данные в блок транзакций. Для первого решения одним из основных недостатков является необходимость обеспечения высокого уровня безопасности, дабы гарантировать, что информация второго реестра не будет скомпрометирована. В то же время, поскольку исходный код оригинального блокчейна не будет затронут, нет каких-либо дополнительных угроз безопасности со стороны первого блокчейна.

F. Публичные ноды

Для увеличения пропускной способности сети с точки зрения скорости синхронизации, будет создана сеть публичных нод, работающих на выделенных серверах [16]. Планируется три этапа развертывания, в ходе которых постепенно увеличится как географический охват, так и пропускная способность сети.

1) Действующие ноды

В настоящее время сеть состоит из 15 выделенных серверов с ограниченным географическим охватом. Происхождение серверов было определено на основе предварительной оценки мест расположения пользователей. В настоящее время серверы размещены в США, Канаде, Франции, Германии, Польше, Китае, Индии, Японии, Сингапуре и Австралии. Общая пропускная способность составляет 5 Гбит/с, что позволяет синхронизировать 100 000 полных блокчейн-файлов[1] в сутки.

2) 4й квартал 2018

- Количество серверов: 30
- Пропускная способность: 10 ГБ /с
- Добавятся: Мексика, Бразилия, Западная Европа, Великобритания, Россия, Индонезия, Марокко и Саудовская Аравия.

3) 1-й - 2й квартал 2019

- Количество серверов: 75
- Пропускная способность: 25 ГБ / с
- Добавятся: Аляска (США), остальная часть Европы, Южная Корея, остальная часть Южной Америки и Тайланд.

IV. X-CASH 2.0 & BEYOND: ВНЕДРЕНИЕ POS

Для того, чтобы цели эффективности, масштабируемости и модульности были достигнуты, сеть X-CASH подвергнется двум значительными апгрейдам. Первый запланирован на начало 2019 года и будет включать изменение алгоритма консенсуса. Имеется также серьезное намерение внедрить

[1] Текущий размер блокчейна составляет 3,09 ГБ

новую техническую опцию, которая позволит значительно продвинуть функционал сети - сайдчейны. Не смотря на то, что есть сильное желание включить эту функцию в релиз X-CASH 2.0, и принимая во внимание затраты на разработку, время, а также необходимость уточнения некоторых характеристик, существует значительная вероятность того, что эта функция будет добавлена позднее. Текущая цель - предоставить альфа-версию в течение 2-го квартала 2019 года, а полностью рабочую версию - к концу 2019 года.

A. Proof of Stake (доказательство доли)

Proof of Stake (PoS) - это тип алгоритма, используемого для достижения консенсуса в сети блокчейн на основе количества монет (долей) участников сети. Основным его преимуществом по сравнению с консенсусом PoW является расход электроэнергии [17], который сводится к энергопотреблению серверов, на которых генерируется консенсус таким образом, как если бы в PoS-алгоритме могли просчитываться хэши. Данный алгоритм является менее затратным в части расходов на вычислительные мощности и электроэнергию. Мы оценили порядок величин и полагаем, что достаточно работы 20 нод на алгоритме PoS, чтобы уровень безопасности сети сравнился или превзошел аналогичную сеть на алгоритме PoW с учетом её хэшрейта на момент написания статьи [2]. При этом PoS потребует 4 кВт электроэнергии вместо 220 кВт для PoW.

Раскрытие блока и получение вознаграждения происходит в случайном порядке, пропорционально количеству монет, депонированных на PoS-адресах участников сети. В процессе генерации блока участники должны доказать пирам, что они владеют долей с определенной суммой. Это достигается без раскрытия какой-либо информации о собственнике доли благодаря использованию кольцевых подписей и протокола Zero-knowledge proof (доказательство с нулевым разглашением).

B. Мастерноды

X-CASH планирует использовать по аналогии с DASH [18] сеть мастернод, которая будет подтверждать транзакции в обмен на комиссии и доходы от майнинга. Как и в текущем процессе майнинга, в схеме с мастернодами не будет комиссии разработчиков. Решение оставить 100% вознаграждения владельцам мастернод принято для стимулирования процесса развития мастернод.

1) Размер депозита и технические требования

При обсуждении минимального порога, необходимого для запуска мастерноды, было решено, что размер депозита для создания мастерноды должен составлять значительную сумму по двум причинам. Первая - ограничение общего числа мастернод в сети с целью увеличения скорости и надежности нод. Вторая, связанна с первой, - это необходимость поддерживать сеть мастернод для серьезных участников. Один из лучших способов сделать это - поднять порог входа, чтобы затраты на запуск самого сервера были незначительными. Также обсуждалось, должны ли быть заданы какие-либо минимальные технические требования к оборудованию, необходимому для запуска мастерноды, и должны ли они быть обязательными для того, чтобы участник мог стать частью сети.

В настоящее время принято решение о минимальном пороге входа для формирования мастерноды в 100 млн. X-CASH, которое может быть пересмотрено. Концепция команды состоит в том, что около половины эмитированных монет должно использоваться для работы мастернод, в то время как остальная половина будет использована в качестве "истинных" оборотных средств. Это означает, что на полную мощность из 500 мастернод сеть выйдет при использовании 50 млрд. монет. Команда считает, что это хороший компромисс между децентрализацией и качеством сети. Если будет достигнута долгосрочная цель X-CASH в отношении его широкого внедрения, то стандартное распределение мастернод X-CASH может выглядеть следующим образом:

Держатели	**Количество мастернод**
Государственные органы	120
Банки и корпорации	150
Учреждения и ведомства	50
Неправительственные организации	30
Прочие	150

Для нескольких инвесторов с количеством монет меньше 100 млн, будет возможна организация совместных мастернод. Минимальная ставка, которая позволит владеть долей в 1% от размера мастерноды, составит 1 млн. X-CASH. До сих пор рассматривается вопрос о том, будет ли это решение непосредственно внедрено в код X-CASH 2.0 или будет реализовано через внешнего поставщика услуг, поскольку они уже присутствуют на рынке [18] [19].

2) Окупаемость инвестиций (ROI)

В краткосрочной перспективе будет значительный стимул для запуска мастерноды, поскольку переход на PoS будет выполнен в момент, когда около 30% монет от общей эмиссии ещё не будут добыты. В таблице, представленной ниже, показана зависимость ROI от прогнозируемого количества работающих мастернод в сети:

Год	**Предполагаемое количество мастернод**	**Годовой ROI X-CASH (%)**
2019	100	255%
2020	350	30%
2021	450	9%
2030	500	1%

Важно подчеркнуть, что высокий ROI, наблюдаемый в 2019 году, будет достигнут за счет значительного "размытия" эмиссии X-CASH (42%). Аналогично, в долгосрочной перспективе, ROI мастерноды значительно снизится, однако нужно иметь в виду, что уровень инфляции при этом будет близок к нулю. По этой причине изложенная выше концепция достигнет своих целей и ROI составит 1%, что выше текущего уровня инфляции доллара США.

[2] По состоянию на 06.09.2018 хешрейт сети X-CASH на алгоритме Cryptonote v7 составляет немногим больше 2 MH/s

C. Сайдчейны

1) Описание

Внедрение сайдчейнов (боковых цепочек) является одним из наиболее важных обновлений, запланированных в сети X-CASH. При работающем сайдчейне информация не будет вноситься в основной блокчейн, а лишь транслироваться между участниками [20]. Для повышения безопасности и надежности количество мастернод X-CASH, необходимых для работы сайдченов будет сделано минимальным, с выделенной долей в консенсусе в размере 33%. В момент образования сайдчейна, каждый участник будет иметь возможность передавать определенное количество X-CASH через боковую цепочку, которая будет изолирована от основной цепочки блоков до момента деактивации сайдчейна. С помощью сайдчейнов участники смогут использовать свои депозиты для запуска сторонних мастернод, а также выполнять транзакции по заранее оговоренным для этого условиям.

2) Особенности транзакций

Одной из ключевых особенностей а также практическим применением сайдчейнов является возможность параметризации деталей транзакций. Пользователи смогут изменять большинство параметров, включая комиссии, минимальное количество перемешиваний и время подтверждения транзакции.

Основное свое применение сайдчейны могут найти в способности изменять максимальный размер транзакции и использовать переменный x-блок. X-блок представляет собой предварительно заданный дополнительный блок данных, встроенный в транзакцию, характеристики которого (с точки зрения размера) также устанавливаются при зарождении сайдчейна. Одним из примеров может быть создание боковой цепи между покупателями и продавцами для обмена информацией о контрактах. Характеристики транзакций будут аналогичны характеристикам основной сети, но дополнительный блок данных позволит добавлять контракты с цифровой подписью любого размера (например, 10 МБ). Поскольку все данные будут зашифрованы, а транзакции будут производиться с использованием тех же скрытых адресов, что и в основной сети, только две стороны, участвующие в транзакции, будут владеть всей информацией до тех пор, пока не возникнет необходимость раскрыть её содержание другим участникам. Одна из интересных и ключевых особенностей заключается в том, что такая транзакция, хотя и не поддается расшифровке, будет подтверждена всеми участниками и ей будет присвоен timestamp.

V. ПЛАТЕЖНЫЙ ШЛЮЗ И ТРАНЗАКЦИОННЫЕ РЕШЕНИЯ

В этом разделе будут описаны два основных уровня разработки, которые будут реализованы поверх основной блокчейн-сети. Первый представляет собой простое решение для клиентов по оплате с помощью X-CASH. С точки зрения продавцов, это решение будет являться альтернативой традиционным межбанковским расчетам, при этом основное внимание будет уделено снижению комиссий.

Второй уровень, который будет встроен в протокол X-CASH, является новым типом подтверждения транзакций - доказательством с нулевым разглашением. Запустив сайдчейны поверх основной сети, учреждения, банки, корпорации или частные лица смогут запускать свою собственную сеть блокчейн и производить обменные операции с помощью X-CASH либо передавать какую-либо информацию. Поскольку такие сайдчейны будут использовать основные принципы Monero, пользователи будут иметь возможность скрывать/раскрывать свою транзакцию для определённой аудитории, предусмотренной протоколом Zero-Knowledge Proof (доказательство с нулевым разглашением).

A. Процесс конвертации XCASH в фиат

1) Описание

Процесс конвертации XCASH в фиатные валюты можно описать как "plug and play" решение, предлагаемое X-CASH. Основной целевой аудиторией этого решения могут быть интернет-магазины и ритейл-компании. Указанное опция содержит два ключевых компонента: финансовый и технический. Поскольку процесс конвертации подразумевает покупку или продажу XCASH в обмен на (скорее всего) другие альткоины, необходимо иметь хорошую глубину рынка и большое количество бирж и/или значительный объемов торгов в секунду. Это будет достигнуто путем регистрации X-CASH на большом количестве бирж с хорошими объемами торгов. В связи с ранним характером начала регулирования криповалют эта деятельность может быть реализована той же компанией, которая осуществляет разработку X-CASH. В ближайшем будущем будет рассмотрен вопрос о переводе этой деятельности в отдельную компанию, зарегистрированную в Китае, с передачей всей необходимой информации, касающейся проекта X-CASH.

Второй уровень - технический с фактической ликвидацией монет на бирже и их конвертацией в фиатные валюты. Этот процесс зависит от позиции команды и может принимать несколько форм. В следующем подразделе описан стандартный процесс с точки зрения покупателя и продавца, а также процесс ликвидации, происходящий на сервере (бэкэнд процесс).

2) Процесс с позиции покупателя

- Клиент выбирает товар, заходит в корзину, нажимает кнопку оплаты на сайте продавца и выбирает платежное решение X-CASH.
- Клиент отправляет сумму в Евро, эквивалентную количеству XCASH, в течение x (вероятно одной или двух) минут.
- Клиент получает информацию об успешной оплате после того, как подтверждение 1-го уровня выполнено и перенаправлено на сайт продавца.

3) Процесс с позиции продавца

- Продавец получает подтверждение заказа и информацию о том, что оплата ожидается (статус «pending»)
- Продавец получает подтверждение оплаты 1-го уровня
- Продавец получает подтверждение оплаты 2-го уровня и информирует клиента по электронной почте, что товар оплачен.
- Продавец получает подтверждение оплаты 3 уровня и может доставить товар.
- Продавец получает средства по сделке в фиатной валюте.

4) Процесс с позиции бэкэнда

- Подтверждение оплаты 1-го уровня получено.
- Определение лучшей биржи для конвертации XCASH в альткоин и выполнение обмена.
- Продажа альтоина и получение фиатной валюты.
- Подтверждение оплаты 3-го уровня получено, фиатная валюта отправляется продавцу.
- Сверка сумм альткоина и фиатной валюты.

Процесс конвертации XCASH в альткоины, необходимо осуществлять в короткие сроки, чтобы избежать рыночных рисков. Поскольку конвертация, скорее всего, будет производится на разных биржах, важно быстро продать актив, поэтому последний шаг заключается в отправке альткоина на биржу, где они были проданы, чтобы ликвидировать позицию.

5) Трехуровневый процесс подтверждения

Не смотря на то, что блокчейн-транзакции относительно быстры по сравнению с другими платежными средствами, они все еще несовместимы с миром реальных платежей, где подтверждение должно быть получено в считанные секунды. Чтобы реализовать мгновенную оплату и обеспечить бесперебойный процесс с пользовательской стороны, вводятся три уровня подтверждения:

- 1й уровень - транзакция транслируется в сеть и добавляется в mempool.
- 2й уровень - транзакция включена в блок.
- 3й уровень - обработано определенное количество блоков (подтверждений) после добавления транзакции в блок.

Каждый уровень представляет собой компромисс между временем и безопасностью. Чем выше уровень, тем ниже вероятность отказа либо задвоения расходов и т. д. С точки зрения пользователя, время транзакции должно быть близким к мгновенному, что разрешено уровнем 1, поскольку трансляция осуществляется в течение 1-3 секунд. В то же время это несет в себе рыночный риск, поскольку транзакция еще на включена в блокчейн, а процесс ликвидации XCASH для выполнения платежа уже начат. Наихудшим сценарием был бы отказ от транзакции (что может произойти по ряду причин, если это не сделано намеренно) и, как следствие, необходимость конвертации обратно из фиатной валюты в XCASH. Это приведет к потерям в 1-2%, которые в одном случае из ста обернутся затратами в 1-2 базисных пункта (0,01-0,02%), связанные с резервированием средств для осуществления сделки.

6) Отчет по расходам

Приведенная ниже таблица показывает состав затрат, связанных с конвертацией:

Операция	**Комиссия (базисные пункты)**
XCASH/альткоин	25
Альткоин/фиат	5
Сверка суммы фиата	1
Сверка суммы альткоина	2
Затраты на биржевые сделки	0
Комиссия X-CASH	0
Итого комиссия	**33**

На критическом этапе конвертации XCASH / альткоин, стоимость 25 базисных пунктов (0,25%) является скромной оценкой, рассчитанной с учетом рыночной стоимости XCASH ~400 сатош и bid/ask спредом в 1 сатошу. Поскольку X-CASH будет осуществлять свою собственную рыночную деятельность, ожидается, что комиссия будет ниже, чем обозначенная выше. Цели по снижению рыночных издержек также будут достигнуты благодаря использованию деривативов, которые обеспечат более высокую ликвидность.

B. Сайдчейн-сети

1) Описание

Сайдчейн-сети будут выполнять важную дополнительную функцию в сети X-CASH, которая в целом является опцией, позволяющей любому инициировать свою собственную сеть блокчейн с заданными характеристиками блока. Идея заключается в том, чтобы предложить простое и легко изменяемое решение для банков, корпораций, учреждений или правительств, которым необходимо использовать блокчейн без учета транзакций основной цепочки блоков. Кроме того, ограничение на размер блоков и транзакций является существенным препятствием для использования основных блокчейнов большинством профессиональных организаций, ввиду существующих лимитов по объему передаваемой информации в несколько килобайт. С целью удовлетворения индивидуальных потребностей корпораций и разрабатываются сайдчейн-сети. Одновременно, сайдчейн-сети могут послужить решением проблемы масштабируемости, так как любой сайдчейн может использоваться для выполнения транзакций в основном блокчейне. В этой способности кроется большой потенциал, особенно в отношении электронных платежей [21], где комиссии основного блокчейна не смогли бы позволить осуществление микроплатежей.

2) Сайдчейн-сети

a) Информационная сеть

Информационные сети можно рассматривать как полу-частные сети, в которых только некоторым ограниченным участникам разрешено совершать сделки. Но сеть не остается полностью частной, так как сайдчейны в целях их работоспособности должны включать мэйнчейн мастернод. По этим же причинам они открыты для общественности, но при отсутствии доступа или просмотра ключей, присвоенных им, содержимое остается недоступным.

Основная функциональность информационных сетей основана на возможности добавить дополнительную информацию в любой блок с транзакцией. Какие-либо ограничения на тип или размер добавляемых данных, кроме тех, что установлены в начале цепочки, отсутствуют. Это решение является простым способом для группы (скорее всего) корпораций или банков обмениваться документами и файлами с цифровой подписью и отметкой времени. Двумя основными преимуществами данного решения перед традиционным методом являются высокая скорость исполнения (несколько минут) и минимальные затраты (ежегодная стоимость сайдчейн-сети из 20-ти нод с аппаратной точки зрения составит менее $10 000) [22].

Существует несколько возможных вариантов использования этой технологии и новые практические применения, подлежащие изучению. Представьте себе сеть банков, работающих под управлением сайдчейна для выполнения основных транзакций. Такое потенциальное

использование часто называют одним из наиболее перспективных вариантов применения блокчейна для финансовой индустрии [22]. Банки и корпорации могут также совместно использовать сеть, в которой они будут обмениваться аккредитивами в цифровой форме без необходимости раскрывать ее другим участникам. Аналогично обмен документами, наделяющими субъекта правами собственности, также могут быть переданы с помощью сайдчейна. В связи с изложенным, основная проблема заключается не в технических аспектах, а скорее в признании юридической природы таких операций.

b) Платежные сети

Поскольку проект X-CASH будет набирать обороты, он будет быстро перегружен транзакциями, особенно если платежный шлюз окажется успешным и экономически эффективным. По этой причине важно включить off-chain транзакции, иначе микроплатежи станут невозможными, поскольку взлетит стоимость комиссионных сборов.

Один из способов реализовать это - создать сайдчейны, которые будут иметь те же характеристики с точки зрения транзакций, что и основная цепь. Цель этих цепочек состоит в том, чтобы найти наилучший компромисс между более низкой децентрализацией и экономической эффективностью, гарантируя при этом приемлемый уровень конфиденциальности. Очевидно, что транзакция, реализуемая в определенной стране, не должна быть подтверждена серверами с другой части света. Однако, все еще предстоит определить, по какому критерию должны создаваться платежные сайдчейны: географическому (страна, городской округ и т. д.), отраслевому или исходя из специфики субъектов, осуществляющих платеж. Предложение, лежащее в основе последнего критерия, заключается в том, что каждый банк может управлять своей собственной сетью (сетями), что также вызывает вопросы с точки зрения регулирования.

VI. ПОВЫШЕНИЕ ЛИКВИДНОСТИ И СНИЖЕНИЕ ВОЛАТИЛЬНОСТИ С ПОМОЩЬЮ ДЕРИВАТИВОВ

Одним из основных составляющих комиссионных сборов, описанных в разделе V *A. 6)* является спред между XCASH и другим альткоином. Этот спред возникает из двух основных источников: волатильности пары и ее ликвидности, которые также тесно связаны между собой.

Эффективным методом снижения волатильности является внедрение производных инструментов - деривативов [22] [23]. Это в особенности применимо к криптовалютам, и уже произошло с рынком биткоина [24]. Что касается X-CASH, то реализация схожей цели может быть осуществлена в два этапа.

Первым станет внедрение фьючерсных инструментов, которые увеличат ликвидность и уменьшат влияние крупных операций по конвертации XCASH в фиат на рыночный курс монеты. Они также позволят легче хеджировать сделки, путем "размывания" по времени расчетов по контрактам.

Вторым этапом станут различные релизы с дополнительными опциями. Задача деривативов будет такая же, как и у фьючерсов, но они помимо прочего застрахуют сделки от сильных колебаний цен, создав «длинную волатильность». В целом, комбинация этих двух инструментов должна снизить и нейтрализовать волатильность спрэда при конвертации XCASH в альткоин.

VII. ВЫВОДЫ

Проект X-CASH намерен предложить эффективное платежное решение с использованием криптовалют. Разработав простой в использовании API и платформу, которая соединит покупателей, биржи и продавцов, это решение послужит стандартом в цифровых платежах, в частности, благодаря низким комиссиям.

Поскольку его основная цель заключается в удовлетворении сетевых потребностей, X-CASH внедрит для пользователей функционал, который позволит сделать детали сделки публичными. Это также станет важным шагом по пути навстречу растущим требованиям регулирующих органов в отношении технологии блокчейн.

Наконец, усовершенствовав сеть через внедрение алгоритма PoS и задействовав сайдчейны, X-CASH надеется решить проблему масштабируемости платежной сети, удовлетворив тем самым нужды корпораций в информационных системах с нулевым разглашением.

VIII. БИБЛИОГРАФИЯ

[1] Capgemini, "World Payments Report 2017," 2017.

[2] CoinMarketCap, "Global Charts - Total Market Capitalization," [Online]. Available: https://coinmarketcap.com/charts/.

[3] bitcoinfees, "Historic daily average Bitcoin transaction fees (in dollars per transaction)," [Online]. Available: https://bitcoinfees.info.

[4] A. I. Joy, "THE FUTURE OF CRYPTO-CURRENCY IN THE ABSENCE OF REGULATION, SOCIAL AND LEGAL IMPACT".

[5] "X-CASH - Global blockchain network to receive & send payments across the world using cryptocurrency," X-CASH, [Online]. Available: https://www.x-cash.org.

[6] T. M. Project.. [Online]. Available: https://github.com/monero-project/monero.

[7] "An open-source technology and concepts for the cryptocurrencies of the future," [Online]. Available: https://cryptonote.org/.

[8] M. J. T. N. N. A. M. J. Seigen, "CRYPTONOTE STANDARD 008 : CryptoNight Hash Function".

[9] "SHA-3," [Online]. Available: https://en.wikipedia.org/wiki/SHA-3.

[10] X-CASH, "X-CASH Explorer," [Online]. Available: https://explorer.x-cash.org/.

[11] R. Mercer, "Privacy on the Blockchain: Unique Ring Signatures".

[12] R. M. Nicolas T. Courtois, "Stealth Address and Key Management Techniques in Blockchain Systems".

[13] Monero, "Monero - Stealth Addresses," [Online]. Available: https://getmonero.org/resources/moneropedia/stealthaddress.html.

[14] J. B. D. B. A. P. P. W. a. G. M. Benedikt Bünz, *Bulletproofs: Short Proofs for Confidential Transactions and More.*

[15] S. Noether, 07 12 2017. [Online]. Available: https://getmonero.org/2017/12/07/Monero-Compatible-Bulletproofs.html.

[16] Smartereum, "Japan’s Financial Regulators want Cryptocurrency Exchanges to delist hard-to-track coins.," [Online]. Available: https://smartereum.com/11843/japans-financial-regulators-want-cryptocurrency-exchanges-to-delist-hard-to-track-coins/.

[17] Cryptobriefing, "Privacy coins under threat regulation - Governments: Privacy Is Bad. Everyone Else: No It’s Not.," [Online]. Available: https://cryptobriefing.com/privacy-coins-under-threat-regulation/.

[18] X-CASH, "X-CASH - Official remote nodes," [Online]. Available: https://x-cash.org/remotenodes/.

[19] BitFury Group, "Proof of Stake versus Proof of Work".

[20] D. D. Evan Duffield, "Dash: A Privacy-Centric Crypto-Currency".

[21] "CoinWatch," [Online]. Available: https://coinwatch.center.

[22] "MyNode," [Online]. Available: https://mynode.rocks/.

[23] Forbes, "Explaining Side Chains, The Next Breakthrough In Blockchain," [Online]. Available: https://www.forbes.com/sites/shermanlee/2018/02/07/explaining-side-chains-the-next-breakthrough-in-blockchain/#795c287d52eb.

[24] O. Hueber, "The blockchain and the sidechain innovations for the electronic commerce beyond the Bitcoin's framework".

[25] X-CASH, "Memo on sidechain network: characteristics, pricing and transaction output".

[26] Techcrunch, "Bank-based blockchain prokects are going to transform the financial services industry," [Online]. Available: https://techcrunch.com/2018/01/28/bank-based-blockchain-projects-are-going-to-transform-the-financial-services-industry/?guccounter=1.

[27] A. S. Nair, "Impact of Derivative Trading on Volatility of the Underlying: Evidence from Indian Stock Market".

[28] S. N. P. N. Drimbetas Evangelos, "The effect of derivatives trading on volatility of the underlying asset: evidence from the Greek stock market".

[29] S. Shi, "The Impact of Futures Trading on Intraday Spot Volatility and Liquidity: Evidence from Bitcoin Market".