eidoo

Technology White Paper

Техдокументация - Версия 0.2 – Черновой вариант – 21.09.2017

СОДЕРЖАНИЕ

Цели проекта

В последние месяцы и годы ажиотаж вокруг криптовалют и так называемых «технологий блокчейна» (из структуры данных «блок-цепочки», введенной в биткойне в качестве первой успешной попытки решить проблему двойного расхода в открытой, децентрализованной сети) вырос и достиг новых высот. Новые бизнес-модели и приложения постоянно предлагаются как стартапами, так и консорциумами и предприятиями. Многие из предложенных вариантов использования этого набора технологий, помимо простых и очевидных применений безрисковых платежей и сохранения стоимости, демонстрируют серьезные ограничения, основные недостатки, неясные цели и порождают наивные ожидания. Однако, один конкретный класс приложений четко определяет себя как явную рыночную тенденцию: использование технологий блокчейн для выдачи, передачи, хранения и обмена пользовательских цифровых активов или «токенов». Общий случай для цифровых активов довольно очевиден, в то время как конкретные преимущества технологий blockchain для их управления - сложная тема, включающая глубокий и не тривиальный компромиссный анализ таких функций, как безопасность, простота использования, устойчивость к цензуре, эффективность, конфиденциальность, аудитоспособность, беспроблемная инновация и грядущая стандартизация. Оптимизация этих компромиссов - это амбициозная и сложная проблема, включающая в себя такие дисциплины как прикладная криптография, теория игр, разработка распределенных систем, разработка с открытым исходным кодом, анализ пользовательского опыта, безопасная электроника, и многое другое. До сих пор усилия по созданию основных потребительских продуктов, которые можно было использовать таким образом, чтобы сбалансировать все варианты, максимизировать преимущества и минимизировать негативные аспекты, были незначительными, неполными, недофинансированными и неудовлетворительными.

Проект EIDOO является первым открытым, всеобъемлющим глобальным мероприятием, направленным на создание эффективного «интерфейса блокчейн/человек», упрощающего взаимодействие между пользователями

и активами на основе блокчейн, без потери главных преимуществ, которые может принести эта технология. Полученный в результате набор продуктов и услуг обеспечиит новый интуитивный, простой, последовательный и безопасный пользовательский интерфейс, ориентированный на простой и безопасный способ хранения, покупки, продажи, передачи и обмена цифровыми активами на базе блокчейна, включая все основные «криптовалюты» и «токены», а также покупки или продажи любых товаров, оплачиваемых в криптовалютах без участия какого-либо центрального органа.

Кошелек EIDOO станет сердцем всего проекта. Он будет изначально многофункциональным и предназначен для мобильного мира: будет использоваться единая интегрированная среда для управления всеми токенами интуитивно, без необходимости осуществлять сложные конфигурации, но в соответствии с лучшими стандартами безопасности и методами . В платформу будут непосредственно внедрены инновационные услуги по обмену криптотерминами и токенами . Эти интегрированные системы обмена никогда не потребуют передачи активов какой-либо третьей стороне централизованного депозитария, которая может привести к финансовым потерям из-за ошибок, взломов или мошенничества с отложенным бегством: пользователь всегда будет полностью контролировать свои средства. В конечном счете, дорожная карта EIDOO также включает полностью децентрализованный рынок на основе блокчейнов. Вокруг этих децентрализованных инструментов будут созданы дополнительные службы, чтобы облегчить использование криптоконверсий. В частности, пользователям будет предоставлена возможность пополнять дебетовую карту непосредственно из приложения EIDOO, не выходя из приложения. Для тех, кто в этом нуждается, EIDOO также предложит решения для цифровой идентичности, используя такие проекты, как «Сеть доверия» для псевдонимной суверенной идентичности, а также интеграцию цифровых удостоверений личности.

EIDOO станет интегратором, обладающим дополнительными преимуществами и объединяющим проверенные технологии и уже существующие сервисы наряду с другими, которые в данный момент можно

только представить. Цель EIDOO заключается не только в том, чтобы делать то, чего нет у других, а в том, чтобы переосмыслить все, что уже сделано, с помощью более безопасных и простых методов, и при этом уделять особое внимание опыту пользователя и предлагать ему свободу выбора, одновременно предоставляя возможность более простого управления сложно устроенным «криптомиром». Мы хотим построить мост к мирам, которые на сегодняшний день еще далеко друг от друга. Наше внимание сосредоточено на предоставлении пользователям полного продукта, позволяющего им интуитивно и безопасно управлять сложными функциями.

Амбициозная задача этого проекта - также дать общий дом и общие цели тем технологическим сообществам, которые защищают очень разные взгляды, что приведет к здоровой конкуренции подходов, методологий, философии дизайна. Компромиссы в блочном пространстве трудные и сложные: простой «компромисс» - это просто способ получить наихудший из двух миров, в то время как лучший выбор - это иногда диверсифицировать пути, чтобы достичь одних и тех же конечных целей с тем же глобальным пользовательским опытом. Это также стратегия управления рисками: инвестирование в проект, который не опирается на единую парадигму, позволяет нам снизить воздействие очень высоких технологических рисков в инновационной отрасли, полной финансовых последствий и последствий в плане безопасности. В динамичном мире никакие хорошие решения не остаются такими, если они не развиваются: в качестве методологического подхода EIDOO будет продолжать улучшать технологическую эффективность, безопасность и пользовательский опыт.

Опыт взаимодействия

Наша миссия - создать единый интерфейс для безопасного взаимодействия с различными стеками технологий и различными философиями дизайна, всегда обеспечивая уникальный, последовательный и простой пользовательский интерфейс. Команда EIDOO включает в себя вертикальных экспертов, работающих в этой области совместно с разработчиками технологий для выполнения этой миссии.

Сегодняшние решения часто делятся между двумя противоположными крайностями: с одной стороны, надежные и безопасные инструменты, которые задуманы и разработаны «только для вундеркиндов», без особых усилий, чтобы хоть в какой-либо степени обеспечить простоту использования; с другой стороны, простые, «блестящие» и хорошо выглядящие продукты, которые могут вводить пользователя в заблуждение, поощрять небезопасные методы или даже принуждать к ним, а также подвергать риску его финансовый актив. Для проекта, связанного с блочными цепями, разработчики довольно часто используют термины и понятия, не беспокоясь о их полном понимании. Хотя некоторые из компромиссов по своей сути невозможно избежать, мы считаем, что технологические передовые технологии и лучшие технологии безопасности должны приносить пользу всем пользователям, а не только «экспертам», поскольку часто безответственное использование этой технологии может отрицательно повлиять на всех остальных, и понимание пользователя необходимо для создания надежных отношений с инструментами, с которыми он имеет дело. Мы считаем, что когда-то необходимо *осознать* внутреннюю сложность проектирования инструментов будущего: упрощение сложного часто является просто иллюзией. Мы стремимся к тому, чтобы наша работа содействовала внедрению этих технологий, которые все еще способствуют ответственному, устойчивому и тщательному их использованию. Управление безопасностью цифровых активов в контексте децентрализованных систем имеет разные последствия для традиционного мира финансов: для этого требуется больше внимания, практики и осведомленности пользователей. Сила «быть своим собственным банком» несет огромную ответственность. Безопасность, прозрачность и понятность являются отправными точками, для которых мы хотим разработать наши пользовательские решения.

Единая кодовая фраза безопасности, независимая от конкретных типов блокчейн-платформ, стандартов и технологических стеков, используемых под капотом, важна для упрощения управления безопасностью и поддержки даже для не строго технических пользователей. Это ядро модели безопасности технологий blockchain. В то же время существующая уникальная, легко защищаемая точка доступа к платформе не должна

ослаблять функции безопасности, такие как модульные функции конфиденциальности, хорошее создание энтропии, удобство переноски, безопасные подпрограммы резервного копирования и т. Д. Поэтому мы решили использовать подход «Иерархический детерминированный кошелек» (Hierarchical Deterministic Wallet), чтобы сделать наше приложение безопасным, позволяя пользователям иметь гораздо больший контроль над своими активами и применять более легкие процессы. С его помощью пользователи могут защитить все свои учетные записи и адреса нескольких активов, а также их ключи подписи с помощью одной секретной фразы, удобно закодированной в двенадцати общих словах. Признание и уважение частной собственности людей также означает, по нашему мнению, дать им возможность организовать ее так, как они считают лучшим. Именно поэтому мы предоставляем специальный инструмент, который без центральных серверов позволяет нашим пользователям извлекать и восстанавливать цифровые активы везде, где это необходимо. Инструмент восстановления EIDOO разработан, чтобы обеспечить пользователям полную доступность своих токенов простым способом, если это необходимо, в чрезвычайных ситуациях.

Люди склонны оценивать качество обслуживания на основе своего прошлого опыта, и это также относится к обмену цифровыми активами. История транзакций Кошелька для цифровых активов всегда должна быть легко читаемой и доступной, последовательной, детализированной, интуитивно организованной. Мы разработали решение, которое, по желанию, позволяет перенаправить из локального приложения на серверы большую часть сложых действий, необходимых для обработки и организации информации, хранящейся в блочных системах, без ущерба для конфиденциальности и безопасности. Новый тип пользовательских токенов будет автоматически обнаружен кошельком и предоставлен для использования с простой и безопасной системой именования (Naming System), чтобы избежать попыток фишинга и мошенничества. Оптимальное управление идентичностью, репутацией и адресами - еще одна важная часть хорошо продуманного пользовательского интерфейса. Кошелек EIDOO будет сосредоточен на этом, сочетая лучшие практики безопасности с легкостью использования.

“Умные” активы

При разработке кошелька Eidoo и всех связанных с ним продуктов и услуг особове внимание уделяется безопасному и простому управлению цифровыми, основанными на блокчейне «умными» активами.

Постоянный и растущий интерес к цифровым активам каким-то образом представляет собой доверенность на акции, облигации, долговые расписки (IOU), права и т. д. Традиционные способы выпуска и передачи активов по-прежнему медленны, дороги, неэффективны и вызывают много трений, как с технологической, так и и нормативной точки зрения. В последние годы были предприняты некоторые усилия, чтобы попытаться использовать технологии blockchain для улучшения ситуации. Хотя иногда фактическая причина этого может быть связана, вероятно, с маркетингом (из-за обмана «blockchain» и «cryptocurrency»), мы считаем, что есть веские причины использовать технологии blockchain в сочетании с централизованными фидуциарными системами или вместо них для выдачы, хранения и передачи цифровых активов. При разработке кошелька EIDOO будет уделено основное внимание этой причине для получения максимальной пользы от новых инструментов и практик, связанных с блокчейнами, и минимизации болевых точек, избыточности, бесполезных чрезмерных инженерных и технологических тупиков.

Одна из этих причин иногда называется «социальной масштабируемостью» открытого цифрового протокола активов: в то время как централизованное и проприетарное решение будет трудно подталкивать, стандарты де-факто с открытым исходным кодом могут быть использованы для снижения трения до принятия и повышения функциональной совместимости. Когда технологии blockchain достигают критической массы принятия в какой-то рыночной нише для их внутреннего ценностного предложения, тогда и цифровые активы могут быть выпущены на той же платформе с использованием существующих сильных сторон: кошельки, рынки, биржи, поставщики ликвидности, библиотеки, исследователи блоков, API, нормативные рамки, защищенное оборудование, пользовательские

привычки и т. д. Чем меньше требуемых настроек, тем более тщеславный процесс.

Еще одна убедительная причина - «модульная конфиденциальность»: в то время как централизованное и основанное на доверии решение будет подвергать пользователей проблемам конфиденциальности, а эмитента - к чрезвычайной регламентационной нагрузке (KYC, AML, законы о конфиденциальности, правила и разрешения для конкретных активов и т. д.), , некоторые из этих проблем можно было бы облегчить в рамках технической невозможности.

Поэтому, любое решение гибридного обмена, внутри которого часть данных поддерживается внутри облака Eidoo, будет подвергнуто обычным практикам KYC-AML, в то время как децентрализованное решение будет поддерживать эти данные, если они существуют, только на устройстве пользователя.

Эта функция будет не просто преимуществом для пользователей в плане конфиденциальности, которая вызывает серьезную и растущую обеспокоенности при разработке цифровых платформ, а также уменьшит ответственность самого эмитента относительно регулирования.

Третьей причиной использования «умных» активов на основе блокчейн является «модульная аудитоспособность»: в то время как централизованное и основанное на доверии решение позволит эмитенту всячески модифицировать регистр, например, накачивать предложение, изменять распределение, вводить суммы и пользователей в черный список , изменять историю транзакций. Технологию blockchain можно использовать (с учетом определенного условия), чтобы обеспечить надежные доказательства правильного поведения. Количество выпущенных активов, резерв, неизменность истории бухгалтерской книги могут быть доказаны криптографически проверены и подвергнуты независимой ревизии с использованием технологий блочной цепи в правильном порядке.

Последней релевантной причиной является возможность «сильной автоматизации»: надежные или минимизирующие доверие, автоматические и непреодолимые контракты с низким или нулевым риском

контрагента являются потенциальным естественным продолжением актива на базе блокчейна. Автоматические, все-цифровые прокси широко распространенных финансовых инструментов и инструментов, таких как «дивиденды», «роялти», права голоса, интересны уже для текущих централизованных и гибридных вариантов использования, но могут иметь первостепенное значение для более сложных сценариев: «умные» (смарт) контракты, «умная» собственность,«DAO» и т. д. Отсутствие риска контрагента было бы полезно для социальной масштабируемости многих финансовых, коммерческих и логистических случаев использования.

Обмен

Появление криптовалют произвело большой толчок к децентрализации услуг, позволяя повысить прозрачность и безопасность в отношении пользователей, поскольку это позволяет избежать единственной точки отказа, и каждый может иметь полный журнал учета того, что происходит. Централизованные, основанные на доверии обмены просты в использовании и предлагают расширенные торговые функции, но они представляют собой угрозу в плане безопасности и цензуры. Хотя некоторые обмены лучше охраняются, чем другие, хаки не являются необычным событием в криптовалютной сцене. Основные неудачи (от MtGox до более поздних хаков) показали чрезвычайную хрупкость этой конкретной точки экосистемы, в противном случае чрезвычайно надежную или даже анти-хрупкую.

Возможное решение может быть децентрализованным, бездоверительным обменом, который не полагается на центральную, доверенную третью сторону для хранения средств клиента. В этом случае сделки происходят непосредственно между пользователями через автоматизированные процессы. Некоторая польза от децентрализованного обмена над централизованным будет: «бездоверительность» (нет требования доверять относительно безопасности или честности обмена), публичная аудитоспособность, гарантии непрерывности работы, конфиденциальность.

Тем не менее, у этой идеи есть, серьезные минусы. В настоящих экспериментах пользователям иногда приходится постоянно находиться в сети или выполнять сложные действия, сделки чрезвычайно медленные и дорогостоящие, ликвидность очень низкая, расширенные функции отсутствуют. Несмотря на большую пользу, чисто децентрализованная среда на данный момент была омрачена тем фактом, что она не может выполнять так же эффективно то, что могут делать централизованные системы. Для такой услуги, как обмен, скорость имеет первостепенное значение, поэтому лучшие трейдеры конкурируют за самые короткие линии волоконно-обменных линий.

Идентичность

Существует ряд применений, для которых необходимо связать адреса с точными цифровыми удостоверениями личности, а именно:

- адреса, связанные с удостоверениями личности, которые признаны правительством, например, для уплаты налогов или получения токенов, применяемых в конкретных целях и в рамках государственного управления, или для использования, требующего соблюдения норм KYC-AML, например, недецентрализованный обмен криптовалюты.

- Адреса, которые должны иметь определенный уровень сертифицированной репутации, например, магазин, чья идентичность может быть гарантирована с помощью механизма сети доверия.

Eidoo будет поддерживать связь хорошо видимых адресов цифровым удостоверениями личности, и, следовательно, обеспечивать несколько

уменьшенный уровень конфиденциальности. Пользователь всегда будет нести ответственность за использование адресов с более низким уровнем конфиденциальности.

Одна цель — две команды

Eidoo - это амбициозный проект, который будет охватывать два разных подхода и практических метода. Будет реализовано одно и то же видение простого, надежного кошелька для умных активов на основе блокчейн:

- в быстрой, простой в использовании, революционной, гибкой, многофункциональной реализации "под ключ" Ethereum. Эта система основана на стандарте ERC20 и контрактах EVM со встроенной системой токенов для финансирования разработки;

- в безопасной, масштабируемой, долгосрочной реализации Bitcoin в соответствии нормам конфиденциальности, на основе нового протокола RGB и доверенных вычислений вне блокчейна, с использованием традиционного некоммерческого подхода к финансированию с открытым исходным кодом

Команда Ethereum

Ethereum: подход и методология

В прошлом году блокчейн Ethereum привлек большое внимание к себе, и многие компании решили использовать его для своих проектов, воспользовавшись экстремальной гибкостью, предлагаемой «умным контрактом» Ethereum.

Это привело к распространению токенов Ethereum, но, что касается данных обещаний, пользовательские приложения не были достаточно удобны в использовании и безопасны.

Причиной того является то, что Ethereum представляет собой высоко экспериментальную технологию, еще неполную и быстро изменяющуюся. Кроме того, подход, основанный на «учетной записи» и приспособленный для смарт контракта, предлагаемого Ethereum, очень ненадежный в отношении других аспектов, во-первых, и особенно в отношении конфиденциальности.

Цель Eidoo заключается в том, чтобы предлагать наилучший опыт пользователям в применении используемых в настоящее время технологий, заполнить основные технические пробелы, следить за эволюцией платформы и адаптироваться к ней.

Ethereum: архитектура кошелька

Легкий клиент

В Ethereum термин «легкий клиент» означает технологию, которая является SPV-корреспондентом среды биткоинов.

В общем, технология заключается в способности «клиента» проверять все хеш-цепи (hash chains), необходимые для проверки информации, полученной другими узлами и касающейся только собственного адреса Ethereum, без необходимости загружать и проверять весь блокчейн.

К сожалению, не было найдено солидных применений Light Client Ethereum, поскольку они все экспериментальные, и технология плохо работает на мобильном устройстве.

Eidoo намеревается использовать технологию "легкий клиент" Ethereum на мобильном устройстве, но с некоторыми поправками:

- Серверы индексируют данные блокчейн
- Клиент на пользовательском устройстве получает информацию об этом с серверов индексирования
- В некоторых случая, полный узел доверия Ethereum пользователя, к которому его клиент обратится, чтобы проверить данные, полученные от серверов индексирования

Одного полного узла недостаточно, потому что таким образом можно было бы узнать только адресные остатки. Нет необходимости в том, чтобы полный узел Ethereum индексировал все транзакции, относящиеся к адресу (или даже знал его остаток); он не индексирует данные токена, которые с его точки зрения представляют собой простые коды для выполнения (смарт

контракт (smart contract)). Эти коды изменяют группу общих данных, составляющих занесенное в память состояние в блокчейне.

Серверы индексирования должны выполнить высокоуровневый анализ всех транзакций блочной цепи, индексировать движения по адресам, определить и индексировать движения токена.

Все эти действия слишком тяжело выполнить непосредственно на мобильных устройствах.

Мнемоническое семя

Ethereum использует тот же алгоритм цифровой подписи, что и Bitcoin, а также многие другие блок-цепи. Биткойн давно определил стандарты для генерации и хранения ключей: BIP32 и BIP39.
Эти стандарты определяют, как вывести большое число ключей из одного семени в соответствии с иерархией, и как генерировать и использовать мнемоническое словосочетание и получить семя для генерации ключей.
Eidoo будет использовать одну и ту же мнемоническую фразу для создания ключей для всех управляемых кошельков. Не имеет значения, используется ли Ethereum, Bitcoin или другие блокчейны, разница будет только в пути деривации. Это означает, что пользователю придется беспокоиться о сохранении только мнемонической фразы.

Мультикошелек

Ethereum — блокчейн на основе учетной записи. Это означает, что учетная запись Ethereum имеет постоянный адрес, и все связанные с ней активы (эфир, токен, а также все смарт контракты, с которыми происходит взаимодействуе) публично соотносятся с этим одним адресом, при чем конфиденциальность совсем не соблюдается.
К сожалению, при нынешнем положении дел единственный способ для пользователя попытаться достичь минимального уровня конфиденциальности, - это вручную разделить активы на несколько кошельков, стараясь не смешивать их.
Вот почему для пользователя очень важно, чтобы Eidoo предоставил

возможность управлять несколькими отдельными кошельками. Это делается путем создания соответствующих ключей из одного и того же семени. При этом сохраняется только одна мнемическая фраза для всех кошельков при использовании различных путей вывода BIP32.

История транзакций

Блокчейн Ethereum хранит статус каждой учетной записи напрямую. Следовательно, чтобы узнать баланс определенного адреса, нет необходимости знать, какие транзакции он затрагивает. По этой причине большинство клиентов кошелька в обращении не предоставляют информацию об истории транзакций (особенно для денежных поступлений ETH с других счетов).

С точки зрения пользователя, хронология переводов Ethereum или токена является фундаментальной информацией почти так же, как и баланс.

Чтобы усложнить ситуацию, когда мы находимся в середине смарт контрактов Ethereum (а все токены - это смарт контракты), между концепцией перемещения актива и транзакцией Ethereum больше нет взаимно однозначного соответствия блочной цепи.

Клиент Eidoo использует «индексные» серверы в первую очередь для идентификации транзакций с их адресом. Вся логика анализа транзакционных данных (например, обнаружение сдвигов токенов) также воспроизводится на клиенте, чтобы он мог в конечном счете проверить информацию с помощью полностью доверенного узла Ethereum.

Ethereum: “Умные” активы

Протокол Ethereum в мире блокчейнов предоставил возможность записывать, а затем глобально проверять состояния виртуальной машины общего назначения, находящейся на каждом отдельном узле сети. Эта конструкция позволяет обобщенно и гибко использовать блокичейны, выходящие далеко за рамки простого переноса стоимости. Помимо выполнения и сертификации статуса смарт контрактов, блокчейны Ethereum можно использовать изначально для создания и управления настраиваемыми активами. Эти активы фактически являются смарт контрактами, которые соответствуют известному стандарту ERC20.

EIDOO Ethereum Wallet полностью поддерживает технологию токенов ERC20.

В настоящее время невозможно использовать уникальные имена и символы для токенов ERC20: пользователи могут создавать новые токены с тем же именем или символом, что и другие ранее существовавшие токены. Этот факт представляет собой проблему для простого и безопасного использования кошелька: у каждого токена есть свой отличный адрес Ethereum, но, будучи сложным алфавитно-цифровым кодом, который человеку трудно читать, писать, запоминать и сравнивать, каждый токен обычно распознается по имени, аббревиатуре и символу значка. Кошелек EIDOO Ethereum применяет специальный индекс (special index), который будет группировать токены, выпущенные компаниями с юридически официальными и/или неофициальными реквизитами, или допустимые токены. Токены с тем же названием / аббревиатурой / символом, что и токены в этом специальном индексе, обозначены EIDOO как ненадежные, во избежание мошенничества, попыток фишинга и / или недопонимания.

Автоматическое обнаружение токенов

В статусе учетной записи, хранящейся в блокчейне Ethereum, можно найти баланс Ethereum, но не токен. Фактически, токены в отношении Ethereum являются смарт контрактами, как и все остальные, и их баланс остается в состоянии «умного» токен-контракта. Следовательно, пользователю

необходимо знать баланс для конкретного токена, непосредственно запрашивающего смарт контракт, поскольку нет способа заранее знать, какие токены принадлежат определенной учетной записи.

К счастью, транзакции Ethereum, которые перемещают токены Ethereum, распознаются структурой данных, хранящейся в блокчейнах которые называются чеками транзакции.

Серверы индексирования вносят в каталог все транзакции, относящиеся к определенному адресу, включая перемещения токенов. Клиент Eidoo из этого списка транзакций также вычитает токен, запрашивая их смарт контракты, чтобы узнать баланс.

Механизм продажи токенов

Механизм участия во всех продажах токенов Ethereum основан на публикации на сайте данных подписки (особенно, адреса, на который можно отправить ETH). К сожалению, веб-сайт не является подходящим инструментом для публикации таких критически важных данных, поскольку он не содержит механизмов для проверки опубликованных данных.

В результате система публикации данных подписки на продажу токенов является первой точкой атаки и в последнее время использовалась несколько раз.

Можно было бы применить инструменты цифровой подписи, такие как PGP, но они не особо знакомы пользователям, которые в конечном итоге могут даже не знать о них.

Eidoo предоставит организаторам продаж токенов услугу безопасного распространения, используя цифровые подписи для данных подписки. Внедрение этой услуги в кошелек обеспечит полную прозрачность подписей для пользователя и подписки благодаря упрощенному пользовательскому интерфейсу, поскольку все параметры могут быть автоматизированы.

Ethereum: обмен

Кошелек Ethereum EIDOO нацелен на внедрение безопасного, прозрачного и частично децентрализованного обмена активами, созданного посредством смарт контрактов Ethereum, которые устанавливают и завершают сделки. Безопасность будет обеспечиваться за счет того, что каждый пользователь будет иметь средства, которыми он торгует в рамках собственного смарт кошелька контрактов. Проблему традиционной вялости и дороговизны децентрализованного обмена можно будет решить с помощью книги заказов и сервера вне блокчейна. Это обеспечит конечному пользователю знакомый опыт традиционного обмена, при котором пользователь сможет создавать столько заказов, сколько позволит его торговый баланс. Пользователю ничего не придется платить, пока заказ не будет согласован и не исполнен на Ethereum. Архитектура не ограничивается просто предоставлением возможности создавать заказы вне блокчейна, но она также очищает заказы от лица пользователей и напрямую передает их в Ethereum для урегулирования. Это обеспечивает несколько уровней безопасности, так как все различные части, такие как сервер интерфейса и сервер заказов, выполняют учетные проверки, чтобы определить, являются ли заказы действительными и могут ли они выполняться. В случае успешного прохождения проверок заказы перенаправляются в сеть Ethereum для урегулирования, в результате чего проводятся окончательные неизменные проверки, после прохождения которых сделки будут урегулированы. Эта гибридная система обеспечивает гораздо более быструю скорость, чем даже другие децентрализованные обмены, для которых используется центральная книга заказов, но которые требуют от пользователей самостоятельно очищать сделки. Тем самым создаются дополнительные проблемы, когда несколько пользователей могут даже соперничать за один и тот же заказ, и им приходится ждать майнера чтобы решить, кому будет отдано предпочтение. Система смарт контрактов, работающих на Ethereum, может быть разработана для использования ключевой пары, находящейся на чипе в качестве ключа собственности для криптовалютного баланса (как для токенов, так и для эфира). Затем ключ собственности привязан к цифровому удостоверению

личности, сертифицированному правительством. Это позволило бы получить некоторые интересные дополнительные функции, такие как восстановление от потери ключа (потеря или кража смарт-карты) или более безопасная проверка транзакций, получающих адрес (например, отправка токенов или эфира непосредственно на удостоверение, подтвержденное правительством).

Это решается центральным сервером заказов EIDOO, поскольку он автоматически очищает и убирает из списка любые заказы, ожидающие решения в блокчейне. Таким образом, конечному пользователю, ожидающему работы вблизи эффективности централизованных обменов, будет казаться, что операция проходит намного быстрее.

Благодаря доказательству криптографической достоверности процесса, выполняемого по централизованному коду, EIDOO обеспечит надежные гарантии для правильного выполнения такого кода: злонамеренное изменение алгоритма согласования ожидаемого заказа осуществить будет невозможно.

Кроме того, эта архитектура обеспечивает как минимум три уровня бухгалтерского учета и безопасности, оставляя окончательный и самый критический уровень неизменному смарт контракту.

Ethereum: Идентичность

В странах с высоким уровнем доходов за последнее десятилетие правительство опробовало и развернуло инфраструктуру открытых ключей (public key infrastructures - PKI) для обеспечения гражданам цифровой идентичности и более простого и эффективного доступа к государственным услугам. Эти инфраструктуры обычно предоставляют каждому гражданину персональную смарт-карту с чипом. Чип содержит ключевую пару: частная часть ключевой пары может использоваться для цифровой подписи документов или для аутентификации в разных государственных службах. Правительство сохраняет открытые части ключевой пары, занимается организацией и управлением сертификационного центра PKI. Эти смарт-

карты сохраняют те же гарантии безопасности, что и аппаратные кошельки, а именно, частную часть пары ключей невозможно легко извлечь из чипа.

Ethereum: рынок

Криптовалюты могут также исключать посредников в торговле товарами, позволяя пользователям и продавцам экономить на комиссионных, выплачиваемых за транзакции. В целях содействия этой коммерческой деятельности мы также планируем развивать децентрализованный рынок.

Здесь пользователи смогут свободно открывать свой магазин и продавать результаты своей работы. Содержимое магазина будет размещаться на их собственном сервере, но с поддержкой протокола IPFS. (https://ipfs.io/)

В начале, как и для обмена, функция поиска в магазинах будет предоставляться централизованным сервисом от EIDOO.

Как только мы будем уверены в его надежности, мы добавим более децентрализованный способ выполнения поиска. Возможно, для достижения этой цели мы воспользуемся сетью Kademlia (Kademlia-network).

Все ключи для перемещения токенов по-прежнему будут полностью контролироваться пользователями. Торги будут проводиться с использованием как смарт контрактов, так и депонирования, управляемого человеком. Этот пункт будет согласован покупателем и продавцом при заключении договора.

В результате каждой сделки будет оставлен отзыв, подписанный как пользователем, так и магазином. Все отзывы будут сохранены как локально, так и в Интернете снова с помощью протокола IPFS.

Предложения, касающиеся удостоверения личности на EIDOO, будут играть очень важную роль в этой части проекта. Они будут изучены, чтобы найти лучшее решение для этого варианта использования. В настоящее время существует также большое число команд, которые работают над разработкой технологии Lightning Network на Ethereum (Raiden Network и Plasma) и Bitcoin.

Мы внимательно следим за их разработкой, чтобы быть готовыми к их внедрению, как только они будут стабильными для использования обычными пользователями.

Команда Bitcoin

Bitcoin: подход и методология

Кошелек Bitcoin EIDOO максимально улучшает ключевые аспекты, которые, по нашему мнению, приносят наибольшую пользу от решений на базе блокчейн для цифровых активов: социальная масштабируемость, аудитоспособность, автоматизация и, в частности, конфиденциальность. Все это сочетается с консервативным и ориентированным на безопасность подходом, основанным на состязательном мышлении, при особом внимании к технической масштабируемости вне блокчейна, что свойственно философии биткойнов.

Мы считаем, что продвижение нового решения специально для конкретного варианта использования, в частности, для распределения общих активов, это очень сложная задача. Вместо этого мы полагаем, что эффективнее улучшить уже широко распространенное и хорошо принятое решение, для реализации которого применяется не только сама инфраструктура, но и ее экосистема, уменьшающая требуемые настройки, минимизирующая риски, связанные с нарушением обратной совместимости, и повышающая скорость внедрения. Благодаря этим преимуществам, проект будет более охотно принят и станет более привлекательным.

Более того, использование уже существующей экосистемы, которая оказалась неизменной, безопасной и не поддающейся цензуре, создает для эмитента надежную, справедливую и доказуемую среду. Благодаря доказуемо честному и детерминированному характеру этой среды, у эмитента есть возможность криптографически доказать достоверность любой транзакции без централизованной и основанной на доверии стороны.

Мы также уделяем особое внимание рискам, связанным с контрагентами, потому что даже если в настоящее время разрабатываются надежные,

непрерывные и полностью автоматические контракты, они еще не скоро будут доступны для реального коммерческого использования. Такие решения как автоматические атомные свопы и прокси-серверы для «дивидендов» или «выкупов» уже используются для некоторых централизованных вариантов использования и могут быть составными элементами фьючерсных сценариев, в частности для децентрализованного обмена, смарт контрактов на основе оракула, «умной» собственности и т. д. Разумеется, эти сценарии предполагают прямое использование независимых активов блокчейна в качестве залога.

Кроме того, первостепенное значение имеет концепция масштабируемости, которая сыграла ключевую роль в течение прошлого месяца. Наличие возможности обрабатывать большое количество транзакций является одним из фундаментальных требований проекта, поскольку это ограничение может препятствовать развитию проекта.

Lighting Network предлагает качественное решение не только для преодоления этой проблемы, но и для совершенствования других уже обсуждавшихся основных аспектов проекта, таких как конфиденциальность.

Тем не менее, наиболее важным аспектом всего проекта является обеспечение конфиденциальности и неприкосновенности частной жизни пользователей. Основанные на доверии решения и Ethereum ERC20 имеют для эмитента некоторые недостатки, из-за которых порой бывает технически невозможно обеспечить отслеживание, управление или регулирование транзакций. Конечно, это будет представлять особый интерес для неофициальных эмитентов и, может быть, для регулируемых юридических лиц, для которых осуществление этих действий может быть более рискованным в плане правового статуса и репутации.

Bitcoin: архитектура кошелька

Кошелек Bitcoin EIDOO сможет управлять активами общего назначения в блокчейне Bitcoin безопасным и удобным для пользователя способом. Мы решили создать кошелек в соответствии с лучшими методами, доступными в настоящее время в экосистеме Bitcoin, чтобы обеспечить не только более высокий уровень безопасности, но и более высокий уровень взаимозаменяемости и совместимости с существующими решениями и услугами.

Ключевой особенностью кошелька является генерация детерминированных ключевых пар из 12/24 слов, называемых семенами по стандарту BIP39. Этот дизайн выбран в целях обеспечения безопасности. Другие альтернативы, такие как создание кошелька с использованием парольной фразы (мозгового кошелька - brainwallet), не принимаются во внимание из-за их низкого уровня энтропии, что делает их более легкой мишенью для мошенников. Сверх того, в целях повышения безопасности пользователь может во время создания кошелька ввести парольную фразу, которая будет использоваться для шифрования закрытого ключа, сгенерированного вышеуказанным способом, как описано в BIP38.

Еще одной важной особенностью кошелька является создание закрытых ключей и адресов в соответствии с BIP32. Таким образом используется иерархическое детерминированное дерево. Это исключает необходимость использовать пул ключевых пар, который неудобен в использовании, чреват ошибками и может оказаться неисправным. Этот процесс также усовершенствован за счет двух дополнений, описанных в BIP43 и BIP44, направленных на стандартизацию создания дерева. Этот элемент является основополагающим для обеспечения совместимости с лучшими кошельками в экосистеме биткойнов.

Лучшие методы используются по умолчанию. Фактически, поскольку конфиденциальность является предметом первостепенной важности, каждый раз, когда требуется новый адрес, например, в случае обмена, кошелек будет генерировать новый адрес, исключающий повторное

использование старого, в соответствии с BIP32, BIP43 и BIP44, как обсуждалось выше.

Помимо конфиденциальности, большое внимание уделяется возможности максимально использовать инфраструктуру Bitcoin и ее экосистемы. По этой причине кошелек будет выполнен с использованием кросс-платформенной и кросс-языковой библиотеки LibWally, содержащей коллекцию хорошо протестированных примитивных функций, сфокусированных на разработке кошелька. Это повысит надежность, безопасность и скорость разработки проекта.

Bitcoin: “умные” активы

Другим основным продуктом наряду с кошельком RGB является протокол RGB, целью которого является разработка иного способа обмена активами общего назначения. Тем самым, эта технология отводит приоритетное место конфиденциальности и совместимости с существующей экосистемой Bitcoin.

Для того чтобы архивировать необходимые уровни конфиденциальности, мы разработали новый способ маркировки цветного актива, который является уникальным для любого другого уже существующего протокола цветной монеты и неотличимым для любой стороны, выполняющей криминалистический анализ на блокчейне Bitcoin или на своей сети.

По существу, наше решение сосредоточено на конфиденциальности истории активов. Оно отличается от существующих протоколов цветной монеты тем, что вместо использования порядка, порядка заполнения или любой другой версии, основанной на позиции индекса выходов, мы используем только наличие выходного адреса для идентификации цветной транзакции и проверки ее целостности. Ключом к достижению желаемого уровня конфиденциальности является то факт, что цветная транзакция не может быть расшифрована кем-либо другим, кроме двух сторон, участвующих в транзакции.

Конфиденциальность - это не единственное преимущество, к которому мы стремились. Важными функциями также являются совместимость с узлами SPV, что не удалось архивировать большинству протоколам, и сборы, настраиваемые различными активами, что достигается благодаря высокому уровню конфиденциальности до тех пор, пока один из владельцев токенов не решит выкупить актив. Обе функции считаются необязательными. Это означает, что, во-первых, любые изменения в протоколе не оказывают особого влияния на сам протокол, а во-вторых, предоставляют эмитенту полный контроль над выпуском его собственного актива.

Масштабируемость - еще один главных фактор в протоколе RGB. По этой причине мы рассмотрим реализацию новой концепции, разработанной Питером Тоддом под названием «Доказательные цепочки» (Proof Chains). На самом деле, просто смотреть историю активов для операции выдачи недостаточно, поскольку возникают проблемы, связанные с удвоением расходов. Чтобы решить эту проблему, фактическое решение приносит в жертву конфиденциальность и масштабируемость. Используя эту новую концепцию, мы можем улучшить текущую ситуацию с помощью издателя, который, используя обязательство об одноразовой печати и не имея возможности обмануть, создаст доказательство, что сторона с этой печатью не осуществляет двойные расходы.

В протоколе RGB также будет свой собственный сценарный язык, позволяющий эмитентам активов создавать функции для описания поведения, которого переводы токенов не должны придерживаться. Этот язык не будет тьюринг-полным (Turing complete) во избежание непредсказуемости смарт контрактов и неопределенных кодовых поведений.

Непосредственно в сочетании со сценарным языком существует также система проверки, которая проверяет правильность истории активов в соответствии с правилами, описанными в скрипте контракта. Наконец, эмитент будет прикреплять пользовательский читаемый контракт к каждой цветной монете RGB. В таком примечании будет четко указано, на что будет иметь право носитель актива при выкупе актива посредством его окончательной сделки, направленной эмитенту. Этот контракт будет

подписан эмитентом с помощью цифровой подписи, датирован и зафиксирован за транзакцией выдачи. Контракт будет передаваться каждым пользователем следующему пользователю и храниться вместе с необходимыми доказательствами, цифровой подписью и доказательством временной отметки непосредственно на кошельке EIDOO. Таким образом, пользователю EIDOO будет еще проще отстаивать свои права и предоставлять возможность эмитенту действовать как можно честнее.

Сценарный язык RGB будет версироваться, и его первичная версия предоставит правила проверки для передачи цифровых активов между пользователями на вторичном рынке. Следующие версии не только гарантируют, что цифровой актив всегда правильно передавался всеми пользователями в каждой транзакции, но также и то, что транзакция учитывала множество более сложных условий, обеспечивающих окончательный выкуп актива. Примером таких правил может быть вознаграждение, пропорциональное сумме передаваемого актива, или высота блока, которая должна быть привязана в каждой транзакции и предназначена для эмитента активов для окончательного погашения актива. Этот консервативный подход обеспечит безопасность и удобство использования протокола для передачи активов с первого дня, в то время как дополнительные функции, требующие дополнительного тестирования и проверки, будут легко внедрены без нарушения обратной совместимости.

Наконец, чтобы улучшить выразительность сценариев, в протоколе RGB будет использоваться аппаратный модуль безопасности (Hardware Secure Module, HSM). HSM — надежные аппаратные компьютерные устройства, защищенные от несанкционированного доступа и способные запускать общие сценарии, такие как те, которые используются для описания поведения актива. Серверы HSM не только позволят произвольно обеспечивать исполнение более сложных смарт контрактов непосредственно на блокчейне биткойнов, а также будут служить аппаратными оракулами, получая данные, которые запускают смарт контракт из выходов вне блокчейна. Фактически, RGB-протокол, как и любой другой протокол передачи на блокчейне, может использовать данные, являющиеся внутренними для своего блокчейна. Поэтому это

очень элементарные данные, такие как время, сборы или суммы. Когда эмитент хочет запрограммировать цифровой актив, который должен быть передан, только когда происходит какое-то событие в реальном мире, тогда требуется оракул для запуска смарт контракта. Именно для этого может служить HSM, аппаратный оракул, который обеспечивает надежную вычислительную среду, что предоставляет невообразимые варианты использования как для эмитентов, так и для пользователей.

Используя такую технологию, эмитент или трейдеры, обменивающие активы, вынуждены подчиняться условиям контрактов и различным условиям передачи активов. Эмитентам или пользователям остается единственная возможность только лишь частично обманывать, нарушая HSM. Однако они в любом случае не смогут ничего украсть. Таким образом, EIDOO предоставит несколько машин HSM, которые будут надежно сохранены и будут предоставлять услуги смарт-контракта и оракула всей сети.

Bitcoin: обмен

Lightning Network будет активно использоваться для разработки децентрализованного обмена, который позволит пользователям EIDOO передавать активы общего назначения или криптовалюту в более безопасной, дешевой и конфиденциальной среде.

Одной из самых больших и недооцененных проблем, связанных с существующими обменами, является то, что пользователям приходится доверять контрагенту, предоставляя ему полный контроль над собственными товарами. Риски, связанные даже с надежными и заслуживающими доверие контрагентами, всегда должны приниматься во внимание, поскольку все равно кто-то окажется жертвой. Используя Lightning Network, мы можем избавиться от любого риска, связанного с контрагентами, поскольку транзакции происходят между пользователями, которым никак не удастся обмануть.

Еще одним большим улучшением является тот факт, что пользователям обеспечивается большая конфиденциальность благодаря проведению транзакций вне блокчейна в децентрализованной одноранговой среде.

Необходимо упомянуть, что благодаря технологии, называемой транзакциями вне блокчейна, Lightning принесет значительное улучшение в отношении стоимости платы и времени ожидания. Ведь это два из самых слабых мест в биткойне в 2017 году. Воспользовавшись вышеупомянутым механизмом, мы можем создать рынок, почти свободный от комиссионных сборов за проведение транзакций, и сократить время подтверждения более чем в 10 раз.

Кроме того, Lightning Network косвенно внедряет другие важные функции, улучшая безопасность и конфиденциальность. Фактически, транзакции Lightning по умолчанию являются атомарными. Это означает, либо обмен фондами проходит хорошо, либо Вам возвращают Ваши деньги. Контрагент не имеет возможности ни украсть Ваши деньги, ни даже заблокировать их на неопределенное время.

Кошелек позаботится об открытии и управлении каналом lightning с определенным активом, предоставляя пользователю полный контроль над конфигурацией. В то же время, он будет использовать отличный алгоритм поиска маршрута, который будет отвечать за поиск лучшей цены для обмена пользовательскими активами в зависимости от времени, ставки / стоимости и компромиссов в отношении комиссионных сборов.

Bitcoin: идентичность

В течение последних лет были предприняты большие усилия в отношении цифрового удостоверения Digital Identity, т.е. набора информации, на основе которой система может описать внешнего агента.

В настоящее время существуют готовые к производству решения:

- задействовать централизованные органы власти, у которых есть определенное число недостатков, таких как единая точка отказа, склонность к цензуре и неполное обеспечение конфиденциальности;

- предоставить неудобные для пользователя технологии, которые приведут пользователя к принятию плохих решений и поставит под угрозу его безопасность, что и случилось в 1991 году с программой шифрования PGP, обеспечивающей криптографическую конфиденциальность и аутентификацию для обмена данными.

По этой причине мы предоставим решение, основанное на удивительной работе Кристофера Аллена (Christopher Allen), чьи исследования проходят под названием «Перезагрузка Сети доверия» (Rebooting Web of Trust) и основаны на концепции автономной суверенной идентичности (self-sovereign identity).

Автономная суверенная идентичность - это эволюция предыдущих решений. Она не зависит от каких-либо централизованных организаций и основана на трех основных концепциях: пользовательский контроль, безопасность и переносимость, а также ключевые концепции проекта EIDOO.

Вышеупомянутую концепцию можно дополнить такими проектами, как смарт-подпись и децентрализация инфраструктуры открытых ключей. Смарт-подпись — это новая система, разработанная ля улучшения ограниченной традиционной системы криптографической подписи и предоставления возможности определять и программировать условия для проверки. Децентрализация инфраструктуры открытых ключей описывает подход к исправлению нескольких проблем, связанных с использованием и безопасностью старой инфраструктуры открытых ключей, функционирующих в децентрализованной среде.

EIDOO будет следить за исследованиями «Перезагрузка Сети доверия», чтобы интегрировать в кошелек рабочее решение для пользователя и тем самым предоставить ему возможность создавать свою собственную персональную цифровую идентичность.

Bitcoin: рынок

Еще одна технология, которая может быть создана благодаря использованию сети Lightning Network, — это децентрализованный рынок, где пользователи EIDOO могли бы вместо того, чтобы передавать только активы, обменивать также универсальные товары и услуги децентрализованным и доказуемо честным способом, используя либо HSM, либо систему условного депонирования.

Кошелек обеспечит абстрагирование недружественной функции сети Lightning Network, предоставляя конечному пользователю более приятную среду для управления своими активами.

Большинство правил, применяемых к децентрализованному обмену, также относятся к децентрализованному рынку в связи с тем, что Lightning Network является общим элементом для обеих систем: возможность избежать любого присутствия контрагента, что увеличивает конфиденциальность и одновременно подавляет вредоносную третью сторону, возможность использовать новейшие технологии, такие как транзакции атомного свопа или даже транзакции с атомными свопами с перекрестными цепями, что сделает рынок более активным и конкурентоспособным, а также мгновенные транзакции с низкой комиссией, что является огромным улучшением, если мы понаблюдаем за тем, как Биткойн вел себя в отношении этих двух свойств в течение 2017 года.

Разница между децентрализованным рынком и децентрализованным обменом заключается в наличии условного депонирования, задачей которого является решить, какая из двух сторон, участвующих в транзакции, должна получить деньги. Системы условного депонирования, в которых роли основаны на репутации, должны иметь стимулы для того, чтобы выступать в качестве третьих нейтральных сторон без какой-либо возможности отвлекать средства или действовать нечестно по отношению к одному из участников.

Были проведены различные исследования, в результате которых некоторые продукты уже производятся, например, биты. Другие все еще остаются на

начальном этапе разработки, например Discrete Log Contracts; у первых есть некоторые централизованные элементы, которые решают, какая из сторон права, а вторая представляет собой слепой и бездоверительный тип системы условного депонирования. На ее результаты нельзя влиять. В связи с тем, что мы используем Lightning Network, реализация слепого, полностью бездоверительного условного депонирования на нем еще не архивирована.

Мы рассмотрим аргумент, чтобы понять различные компромиссы между аналитиками, рассматривая как готовые образцы производства, например, Bisq или OpenBazaar, так и лучшие исследования, доступные на данный момент в данной области.