DeepOnion

DeepOnion
White Paper

https://deeponion.org

Анонимность –
неотъемлемая часть свободы

Автор:
Jimmybob

редакция 1.0A

DeepOnion
White Paper

Команда разработчиков: Monocolor, Deeper, Jimmybob

В данном документе приведена концепция DeepOnion и соответствующие авторские инновационные блокчейн-разработки, которые и являются фундаментом этой новой, ориентированной на конфиденциальность криптовалюты.

Прежде всего, определены поставленные задачи проекта в аспекте состояния современной криптовалютной экосистемы: проведен анализ существующих недостатков и предложены способы их устранения, реализованные в DeepOnion.

Во-вторых, представлены основные технологические разработки проекта с подробным обоснованием их спецификаций, внедрения, тестирования и развертывания.

Наконец, изложено видение дальнейшего развития DeepOnion, обеспечивающего успешный путь к созданию безопасной и конфиденциальной платежной экосистемы.

Ключевые слова: анонимность, конфиденциальность, криптовалюта, DeepSend, DeepVault, смарт-контракты, VoteCentral, TOR.

Краткое оглавление

1. Введение

DeepOnion является гибридной криптовалютой, в которой одновременно реализованы PoS (англ. *proof of stake,* дословно: «подтверждение доли») и PoW X13 (англ. *proof of work,* доказательство выполнения работы) алгоритмы.

DeepOnion нативно поддерживает протокол TOR (англ. *the onion router*)[1], обеспечивая безопасность и анонимность peer-to-peer соединений (кошельки функционируют как промежуточные ноды в сети TOR). Основная цель DeepOnion – обеспечение безопасности и конфиденциальности платежей через создание анонимной, надежной и масштабируемой платформы, которая гарантирует неотслеживаемость проводимых транзакций.

DeepOnion обеспечивает безопасность и анонимность, значительно снижая вероятность идентификации пользователей различными государственными и частными службами, за счет использования передовых криптографических достижений и анонимных сетевых протоколов.

В ближайшем будущем в DeepOnion будут внедрены инновационные блокчейн-технологии, такие как DeepSend (авторская технология сокрытия транзакций), реализующие

Автором данного документа является Jimmybob. Соавторы: Deeper, Monocolor, а также остальные представители команды DeepOnion. E-mail: monocolor, deeper @deeponion.org
Документ создан в октябре-ноябре 2017 г.; опубликован в декабре 2017 г.

обфускацию транзакций, что делает невозможным отслеживание движения платежей в сети DeepOnion. Все эти особенности обеспечивают функционирование защищенной анонимной платформы, позволяющей ее пользователям осуществлять платежи, скрытые от наблюдения государства и различных злоумышленников.

1.1. Развитие DeepOnion

За счет постоянного улучшения действующего функционала и внедрения новых технологий, DeepOnion стремится стать одной из ведущих криптовалют. В стеке разработки используются только передовые стандарты обеспечения безопасности и конфиденциальности, такие как, например, поддержка крайней версии протокола TOR. В дальнейшем будет также добавлена система анонимного голосования VoteCentral для предоставления сообществу возможности определения направления дальнейшего развития DeepOnion.

Мы твердо убеждены, что право на анонимность является неотъемлемым атрибутом проявления свободы, и у каждого должна быть возможность реализовать это право, защитив свою личность и финансы от нежелательного изучения государственными ведомствами или другими организациями. Наша цель – создание 100% анонимной криптовалюты, полностью соответствующей всем требованиям современного мира

финансов и гарантирующей безопасность и конфиденциальность. DeepOnion – непрерывно развивающийся проект, учитывающий в своем развитии изменчивые условия мира криптовалют, что позволяет ему все время находиться в авангарде современных криптовалютных технологий.

И самое главное, что DeepOnion – это сильное сообщество, одна большая семья с общими взглядами и убеждениями, а также непоколебимой верой в необходимость обеспечения безопасности и финансовой анонимности в сети. Сообщество DeepOnion сделало неоценимый вклад в развитие проекта, и мы гордимся тем, что за такое короткое время у нас появились многие тысячи однодумцев, помогающие нам двигаться дальше. Вместе – мы сила, вместе – мы DeepOnion!

2. Актуальные проблемы криптовалют

Биткоин (BTC), несмотря на присущие ему недостатки, является современной доминирующей криптовалютой с капитализацией $598 млрд., что составляет 37,6% от общего рынка криптовалют. Для внесения ясности необходимо проанализировать эти недостатки и показать, как они устранены в DeepOnion.

2.1. Конфиденциальность и безопасность

Биткоин[1] основан на общедоступном, защищенном от искажений, блокчейне с использованием шифрования SHA-256, который распределен по децентрализованной сети, поддерживаемой майнерами и владельцами кошельков. Поскольку блокчейн надежно обеспечивает сохранность данных, то, как только определенный адрес будет сопоставлен с личностью владельца кошелька (при выполнении операций на бирже или в обменнике) – в дальнейшем уже будет невозможно скрыть эти данные без необходимости перемещения монет с исходного адреса, а также обеспечения сокрытия проведенных транзакций с использованием дополнительных сервисов (миксеры и т. п.). Это все аналогично общедоступному отчету по вашему банковскому счету, с указанием всей информации по проведенным транзакциям, которая доступна абсолютно всем. Приведем типичную схему обмена биткоинов на фиат:

- пользователь создает учетную запись на бирже и верифицирует ее (требование большинства крупных бирж);
- биржа генерирует биткоин-адрес, который будет сопоставлен с учетной записью;
- пользователь отправляет средства со своего личного (пока еще деперсонифицированного) биткоин-адреса на созданный биржевой адрес (который уже привязан к конкретной личности);
- выполняется операция обмена (на фиат либо другие криптовалюты).

Неутешительным следствием такой последовательности действий является то, что когда-то ваш биткоин-адрес, до этого бывший вполне анонимным, уже теперь полностью сопоставлен с вашей личностью. Т. е. биржа может точно определить балансы на всех ваших адресах (личном и созданным на бирже), а также объемы и направления всех производимых (и произведенных) транзакций. Особенно тревожно осознавать, что такая информация может быть передана государственным ведомствам или при других обстоятельствах (например, взлом биржи) – стать доступной для злоумышленников.

Можно вспомнить недавнюю массовую волну распространения вируса Wannacry[10], в результате которой были заражены миллионы компьютеров по всему миру. Выкуп, который необходимо было заплатить за дешифрование данных (которое

не производилось даже после оплаты), необходимо было отправить на биткоин-адрес, ставший впоследствии объектом пристального внимания как спецслужб, так и обычных пользователей сети по всему миру. Публичная доступность транзакций привела к значительным трудностям по переводу и обмену полученных злоумышленниками биткоинов.

Конечно, в данном случае можно утверждать, что общедоступность наблюдения транзакций способствовала борьбе против преступности, но давайте также рассмотрим и другой пример. Представьте обычные переговоры для тендерного соглашения: если один участник сможет отследить все финансовые операции конкурентов, это даст ему огромное преимущество в оценке их позиций и возможность использовать полученную информацию для недобросовестной конкуренции. Вполне вероятно, что эта особенность и является одной из основных причин, препятствующих масштабному использованию биткоина в корпоративном сегменте и вообще, для массового частного применения. Из этого можно сделать вывод, что часто навязываемый ореол «анонимности» биткоина является грубым заблуждением.

2.2. Анонимность

Отсутствие обеспечения анонимности является одним из главных недостатков биткоина: ноды обмениваются незашифрованным трафиком, а IP-адреса доступны для наблюдения, что дает возможность реализации целенаправленных атак и, следовательно, нарушения работоспособности сети. Такую информацию легко получить с помощью выполнения команды *getpeerinfo* в обычном биткоин-кошельке. Раскрытие личного IP-адреса без необходимых на то причин, является серьезным нарушением безопасности вашего компьютера, особенно, если не приняты дополнительные защитные меры.

Существует вполне реальный риск идентификации личности пользователя кошелька через определение его IP-адреса с последующей тщательно спланированной атакой. Таким образом, сокрытие IP-адреса кошелька – важная составляющая в общей системе принимаемых мер по обеспечению безопасности и анонимности проводимых операций. В DeepOnion такая защита реализована за счет функционирования нод (кошельков) внутри сети TOR.

2.3. Скорость и масштабируемость

В сети биткоина необходимо чтобы все ноды выполняли проверку всех предыдущих блоков в общей последовательности блоков. Для этого требуется значительная вычислительная мощность и большой объем дискового пространства (все транзакции с момента запуска сети), а также время для обработки таких данных. Поскольку в биткоине реализован только основанный на SHA-256 алгоритм PoW для обработки блоков и генерации монет, то существует и предел скорости транзакций, зависящий от текущей сложности сети и ее технологических особенностей. В данный момент, среднее время подтверждения одного блока составляет примерно 350 мин. При этом большинство сервисов требуют не менее 6 подтверждений для проверки транзакций, что может увеличить общее время проведения платежа до 35 ч., что крайне неприемлемо в современном финансовом мире.

3. Концепция DeepOnion

Большинство приведенных в предыдущей главе проблем решены в DeepOnion за счет внедрения передовых технологий в процесс разработки. Прежде всего все ноды (кошельки) функционируют внутри сети TOR (см. гл. 6), что делает крайне затруднительной идентификацию пользователей без способности компрометировать обширную часть сети TOR. Это означает, что определение IP-адреса (местоположение) владельца кошелька DeepOnion практически невозможно. Напротив, в сети биткоина трафик не шифруется, хотя сквозное шифрование уже было предложено в BIP 151 разработчиком Bitcoin Core Джонасом Шнелли (Jonas Schnelli). Таким образом становится возможным определение IP-адресов с помощью анализа трафика.

Это может привести не только к юридическим последствиям (если биткоин запрещен в вашей стране), но также и к раскрытию факта использования кошельком биткоина, что является крайне нежелательным.

В DeepOnion реализуется многоуровневая безопасность с применением передовых технологических стандартов в криптографии и сетевой безопасности (рис. 1). На транспортном уровне интегрирована поддержка протокола TOR для обеспечения защиты и анонимизации сетевого трафика между

нодами. В дорожной карте DeepOnion (рис. 2) указаны сроки внедрения протокола Zero Knowledge Proofs[11] (протокол нулевых доказательств), который реализует обфускацию источников транзакций для всех, кроме получателя, предоставляя ему необходимые подтверждения платежа.

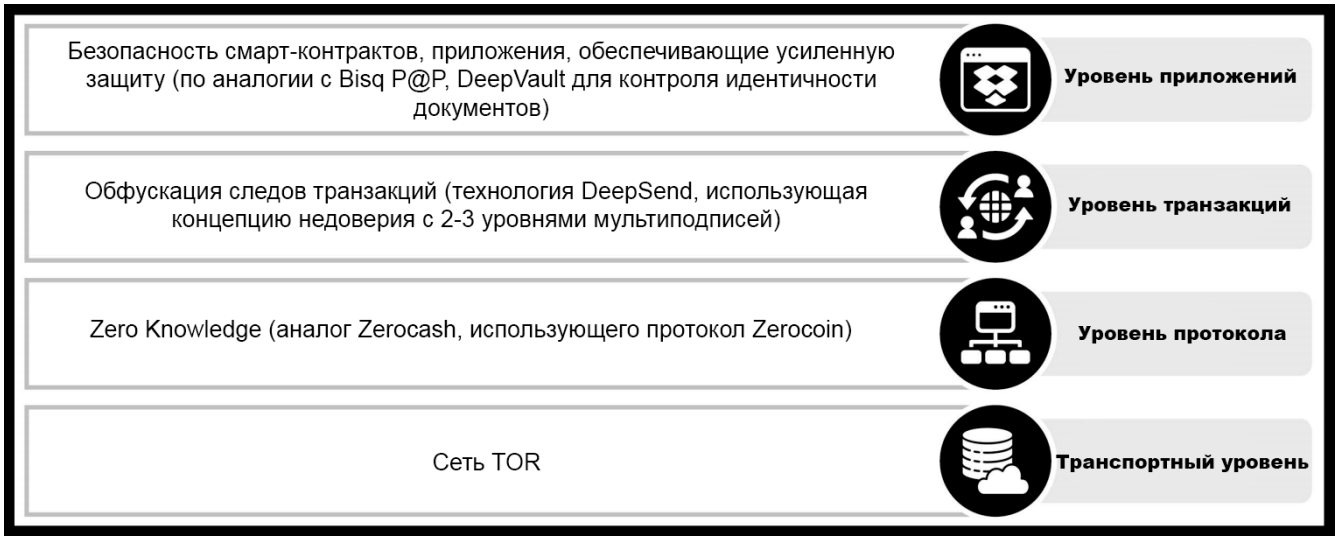

Рис. 1. Реализация многоуровневой безопасности в DeepOnion

Впоследствии следы транзакций будут также скрыты с помощью технологии DeepSend[12], реализующей концепцию недоверия, основанную на мультиподписях. На уровне приложений реализована заключительная составляющая обеспечения безопасности и анонимности посредством поддержки децентрализованных бирж, различных торговых площадок и других сервисов, функционирующих на основе использования криптографической защиты, предоставления анонимности и децентрализации.

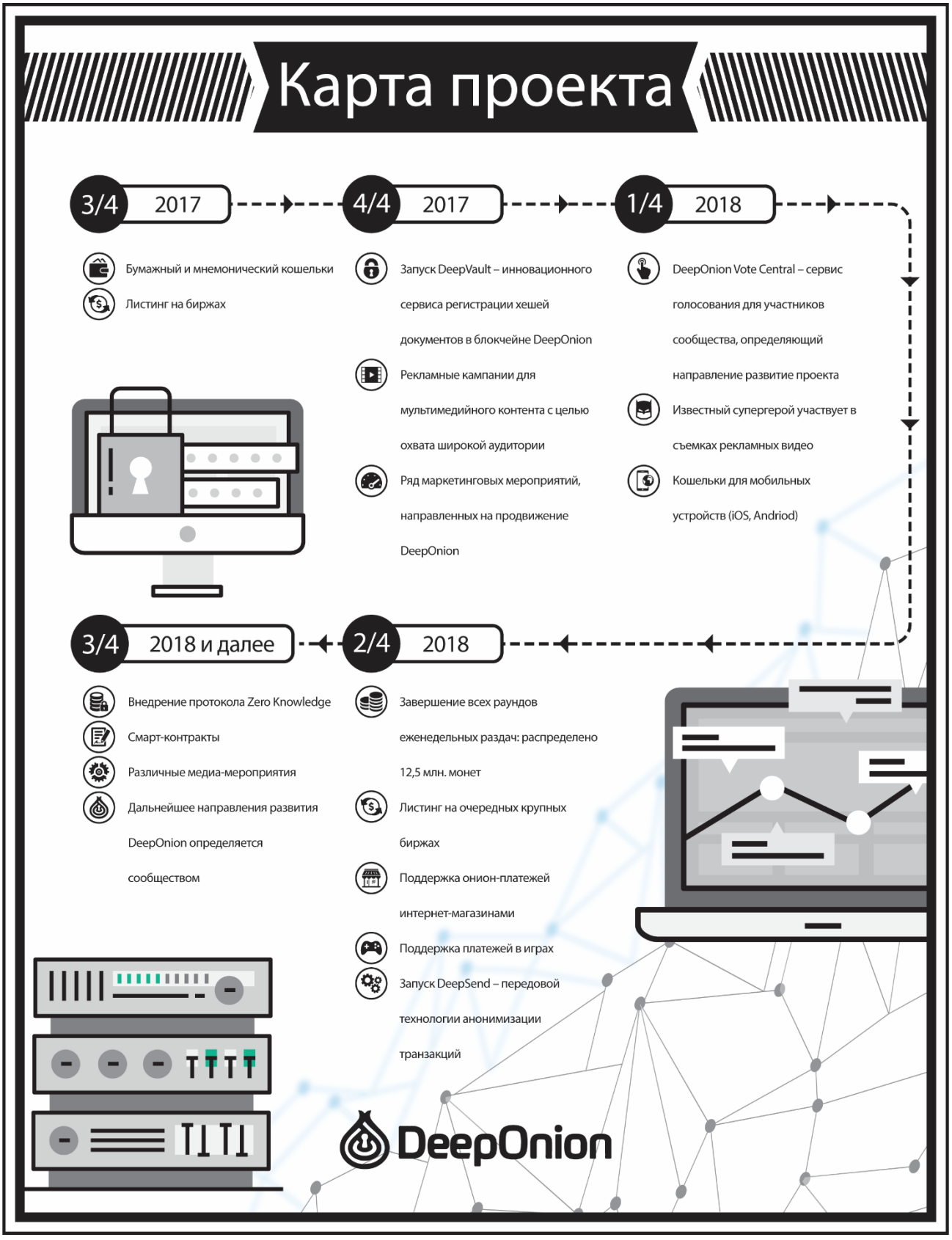

Рис. 2. Дорожная карта DeepOnion

3.1. Дорожная карта DeepOnion

Дорожная карта проекта (рис. 2) детально отображает все поставленные цели, а также сроки их реализации. Естественно, что вполне вероятны и небольшие отклонения от намеченных временных интервалов, что характерно для проекта такого масштаба. На случай непредвиденных обстоятельств, были разработаны соответствующие планы реагирования, предусматривающие в т. ч. и привлечение сторонних разработчиков. В любом случае, будет опубликована детальная информация о подобных изменениях.

4. Основные характеристики

В данном разделе будут приведены детальные характеристики DeepOnion, чтобы подготовить читателя к более углубленному и тщательному анализу, проведенному в разделе 6.

DeepOnion является гибридной криптовалютой, одновременно поддерживающей PoS и PoW (алгоритм X13), с запланированной эмиссией порядка 25 млн. монет в течение последующих 10 лет.

- 5 подтверждений для проведенной транзакции;
- 50 подтверждений для найденного блока;
- 18 млн. монет (90%) были добыты премайнингом в начальном блоке и будут свободно распределены между участниками сообщества в еженедельных раздачах;
- 2 млн. монет будут добыты майнерами;
- порт для подключений: 17570 – порт RPC: 18580.

4.1.1. Характеристики PoW

- алгоритм X13;
- новый блок через каждые 240 с;
- пересчет сложности после каждого блока;

- начальное вознаграждение за каждый найденный блок: 8 онионов (будет уменьшатся в 2 раза каждый год, пока не достигнет 1 ониона, что и станет постоянным значением).

4.1.2. Характеристики PoS

- новый блок через каждые 60 с;
- пересчет сложности после каждого блока;
- вознаграждение за найденный блок: 1-й год – 10%, 2-й год – 5%, 3-й и последующие – 1%;
- минимальный возраст монет, необходимый для запуска PoS: 24 ч.;
- максимальный возраст монет: 30 дней.

4.1.3. Алгоритм X13

Как и следует из названия алгоритма, в нем предусмотрено 13 раундов хеширования с использованием разных хеш-функций (в т. ч. такие известные, как blake, bmw, groestl, jh, keccak, skein, luffa, cubehash), что делает его более защищенным, чем SHA-256 и Scrypt. Кроме того, существует возможность выбора конкретных хеш-функций[13], что очень важно в свете недавно обнаруженных вероятных коллизий в данном алгоритме.

4.1.4. Эмиссия

Спецификации эмиссии DeepOnion выглядит следующим образом:

- PoW: новый блок через каждые 240 с, т. е. 15 блоков в час или 360 блоков в сутки;
- начальная награда за найденный блок – 8 онионов, каждый год будет уменьшаться вдвое;
- общее количество монет, полученных с помощью PoW-майнинга: 365×360×8×(1+1/2+1/4+1/8+…) = **2 102 400,** поэтому, общее количество PoW-монет (с учетом 18 млн. монет, добытых премайнингом в первом блоке) – **20 102 400.**
- PoS: награда 10% в течение первого года, 5% – второй год и 1% – все последующие годы;
- общее количество монет через 10 лет – примерно **25 млн.**

4.1.5. Модель сети

Сеть DeepOnion функционирует внутри TOR, благодаря чему обеспечивается защита и анонимность проводимых транзакций. Коммуникация между нодами (кошельками) осуществляется с использованием адресов сети TOR (пример адреса: **bb3ebyhgfkj3jzfd.onion**). Такие адреса являются самоаутентифицирующимися: это означает, что адрес как таковой, представляет собой криптографическое доказательство идентичности сервиса, позволяющее защитить

его подделку злоумышленниками. Интеграция с TOR, совместно с другими технологиями DeepOnion, предоставляет большое количество преимуществ в аспекте безопасности, в т. ч.:

- дополнительная защита конфиденциальности устройства, на котором хранится кошелек DeepOnion (ваш IP-адрес анонимен, его невозможно отследить);
- криптографическая верификация подлинности сети, к которой вы подключаетесь (DeepOnion внутри TOR);
- свобода от контроля и наблюдения за сетью;
- невозможность блокировки вашего клиента по конкретному IP-адресу;
- усовершенствование целостности системы связи и защиты от несанкционированного доступа с помощью шифрования.

4.2. Распределение монет

Справедливое распределение имеет решающее значение для получения любой новой криптовалютой повсеместного признания. В целях удовлетворения этих требований DeepOnion проводит бесплатные раздачи монет (airdrop) и дополнительные баунти-кампании (см. детальную информацию по распределению в приложении А).

Принцип, положенный в основу данного метода, многогранен. 40-недельный период бесплатных раздач содействует хранению монет, так как участники, ранее уже получившие их, доверяют модели распределения и, соответственно, ждут его завершения с целью максимального увеличения своих накоплений. Алгоритм PoS обеспечивает дополнительное вознаграждение (см. раздел 4.1.4) для тех, кто хранит монеты. Большая продолжительность кампании гарантирует достаточные возможности участия для новых пользователей, что способствует ускоренному росту сообщества. Выбранная модель распределения гарантирует, что будет происходить увеличение количества участников еженедельных раздач с последующим ростом децентрализации.

Большие суммы монет хранятся на адресах, предназначенных для оплат баунти, различных рекламные кампаний, а также для спонсирования разработок, направленных на развитие DeepOnion.

Основные предъявленные замечания по поводу такой модели распределения предполагают вероятность того, что разработчики избавятся от своих монет сразу же по достижении максимальной цены. Приведем основные контраргументы по данному аспекту:

- основатели DeepOnion владеют 2 млн. монет – это всего лишь часть, стремительно снижающаяся в процентном

отношении в сравнении с теми суммами, которые уже были распределены в еженедельных раздачах;

- текущий ежесуточный объем торгов на биржах с учетом глубины рынка также не позволяет осуществить сценарий «сброса» монет.
- исходные коды проекта являются общедоступными (за исключением технологии DeepVault, что сделано с целью защиты от недобросовестного копирования). С учетом размеров сообщества и компетентности его участников, всегда возможно проведение форка по возникшей необходимости;
- подобный «сброс» категорически противоречит установленной этике в команде разработчиков и концепции развития экосистемы DeepOnion.

4.3. Сообщество

Сильные стороны DeepOnion обусловлены в первую очередь большой численностью сообщества проекта, его репутацией и поддержкой его сети. Существует много криптовалют, не получивших повсеместного признания по причине малочисленности последователей и неудачного продвижения. Мы хорошо понимаем важность социального аспекта, и с самого начала всегда придавали первостепенное значение

формированию сообщества. С этой целью мы реализуем платформу для голосования, с помощью которой наши пользователи смогут определять направление развития DeepOnion.

Чтобы гарантированно выполнить данное требование, мы создали большое количество социальных медиа-площадок и сопутствующих технологий. Пожалуй, самой примечательной из них является официальный форум DeepOnion (https://deeponion.org/community/ru), который представляет собой основу нашего сообщества; сама платформа обладает многими функциями, которые отсутствуют в программном обеспечении других форумов. Наш проект также представлен на нескольких сторонних платформах с большим числом посетителей, таких как Facebook, Twitter, Reddit и YouTube, которые мы используем для продвижения.

Избранная нами стратегия является в высшей степени эффективной: на сегодняшний день наша тема на форуме BitcoinTalk.org входит в число наиболее обширных и популярных. Такой уровень воздействия имеет большую практическую значимость, и мы намерены продолжать работу в данном направлении. Что особенно важно, было продемонстрировано отношение людей к проекту DeepOnion и их готовность вовлекаться в него, обеспечивая поддержку и дальнейшее развитие.

4.4. Официальный форум

Официальный форум проекта DeepOnion используются и для социального взаимодействия, и для координации наших призывов к действию во время мероприятий по продвижению. Официальный форум способствовал исключительному росту проекта в течение крайних 6 месяцев и является одной из основных движущих сил дальнейшего успеха DeepOnion.

Форум доступен по адресу: https://deeponion.org/community/ru, регистрация открыта для всех желающих. Здесь вы сможете узнать больше о DeepOnion и задать нашему замечательному дружелюбному сообществу любые вопросы. Вас приятно удивит огромное количество ярких, талантливых, разноплановых личностей в нашем сообществе, и мы будем рады, если вы решите присоединиться.

5. Технологический обзор

Сильные стороны проекта DeepOnion обусловлены многосторонним подходом к обеспечению безопасности и конфиденциальности, который реализован в использовании передовых технологий. Наряду с использованием ряда общепризнанных технологий, уже применяемых для других валют (мы охотно перенимаем современные передовые методы), в DeepOnion также имеется немало собственных разработок, которые обеспечивают высокий уровень надежности и еще больше конфиденциальности, анонимности и безопасности.

Для дальнейшего обсуждения этих аспектов необходимо понимание распространенных технологических особенностей, характерных для многих криптовалют, использующих блокчейн.

5.1. Блокчейн

Блокчейн, по сути, представляет собой «постоянно растущий список записей, называемых блоками, которые связаны и защищены с помощью криптографии. Каждый блок обычно содержит ссылку на предыдущий блок в виде хеш-указателя, метку времени и данные транзакций. По своей конструкции блокчейн устойчив к модификации данных»[3].

Использование блокчейна для денежных транзакций становится эффективным решением множества проблем, стоящих перед существующими финансовыми системами. Блокчейн обеспечивает наличие неизменяемого публичного реестра, в котором содержатся данные обо всех транзакциях, совершенных во всей сети. Это позволяет верифицировать любую транзакцию с момента создания монеты (с очевидными компромиссами конфиденциальности, описанными в разделе 2.2), благодаря чему разрешение конфликтов становится несложной задачей.

5.1.1. Масштабируемость блокчейна

В силу того, что блокчейн представляет собой постоянный реестр всех транзакций, важно понимать границы максимальной пропускной способности. Для биткоина и эфира максимальная пропускная способность составляет соответственно 4 и 7 транзакций в секунду. Такое ограничение обусловлено размером блока (т. е. объемом данных о транзакциях, которые могут храниться в каждом блоке) и временем блока (средним временем обработки хеша блока и добавления его в блокчейн). Как вы наверняка знаете, по этой причине время подтверждения транзакций в сети биткоина может занимать более суток, что является существенным недостатком этой, по идее, моментальной платежной системы. В DeepOnion ситуация значительно улучшена

за счет использования PoS, большего размера блоков и меньшего времени генерации блока. Все это обеспечивает максимальную теоретическую пропускную способность в 62,5 транзакций в секунду:

- средний объем транзакции – примерно 500 байт. Объем блока в DeepOnion равен 1,5 Мб; таким образом, каждый блок может вмещать приблизительно 3000 транзакций;
- в DeepOnion одновременно используются алгоритмы PoW и PoS; в PoW интервал между блоками составляет в среднем 240 с, в PoS он значительно меньше – новый блок через каждые 60 с: это означает, что примерное время генерации блока (от двух алгоритмов) равно 48 с (240/5).

Чтобы убедиться в этом, был произведен произвели подсчет общего количества блоков за последние 24 часа:

- блок 223460 появился 25.11.2017 в 11:59:36;
- блок 225285 появился 26.11.2017 в 11:59:05.

Это означает следующее:

- было получено 1825 блоков за 24 часа, т. е. среднее время блока равно 47 с, что полностью соответствует нашему расчетному среднему значению времени появления блока;
- таким образом, каждые 48 с генерируется 1 блок, который способен вместить 3000 транзакций; следовательно,

максимальная скорость проведения транзакций для DeepOnion будет равна: 3000/48 = 62,5 транзакций/с.

Это почти в 10 раз выше пропускной способности эфира и служит доказательством большей эффективности и масштабируемости DeepOnion, а также его пригодности для массового применения. Скорость проведения транзакций DeepOnion может быть еще увеличена за счет последующего внедрения технологии lightning network[8]. В этом случае скорость транзакций может стать такой же, или даже выше, чем в VISA (приблиз. 56 000 транзакций/с)[8]. Столь высокая скорость в сочетании с интеграцией с TOR – делает DeepOnion идеальной платежной платформой.

5.2. Криптовалюта

Криптовалюта (или крипто-валюта) – это цифровой актив, используемый в качестве средства обмена, с применением криптографии для обеспечения защиты транзакций, контроля эмиссии и верификации переводов активов[4]. Первой децентрализованной криптовалютой стал биткоин, созданный Сатоши Накамото в 2009 г.

5.3. Децентрализация

Децентрализация – это процесс перераспределения, рассеивания функций, сил, власти, людей или вещей от центрального местоположения или управляющего органа[5].

Применительно к криптовалютам, определение дается следующим образом: это ликвидация органа централизованной обработки данных (подобно упомянутой выше системе VISA). Вместо этого каждая нода в сети (кошелек либо майнер) осуществляет независимую проверку каждого блока в блокчейне с использованием процессов криптографического хеширования.

Преимущество данного подхода заключается в том, что он позволяет повысить уровень безопасности в сети и существенно уменьшает зависимость от платежного оператора. Чтобы нарушить нормальное функционирование, потребовалось бы скомпрометировать 51% всей мощности сети, а это практически недостижимо с учетом глобального распределения нод, использования различных протоколов и операционных систем. Преимуществом для сети также является возможность для каждой ноды осуществлять верификацию новых блоков. В DeepOnion эта возможность реализована еще лучше, чем в биткоине, за счет внедрения PoS, другой формы майнинга и верификации, в результате чего, для нарушения функционирования сети, потребовалось бы нарушить работу еще большей ее части по двум каналам (что по сути невозможно).

В то время как верификация каждой транзакции обеспечивает максимальную безопасность, по этой же причине проведение транзакций занимает значительно больше времени, чем при использовании традиционных способов оплаты. Одним из вариантов решения данной проблемы масштабирования являются такие технологии, как lightning network, однако всякий раз при проведении транзакций вне основной цепочки будет снижаться и безопасность, поскольку уменьшается количество верификаций. Выбор необходимого уровня обеспечения достоверности (необходимого количества подтверждений) – довольно сложная проблема, на которой в настоящее время сосредоточено внимание разработчиков различных проектов, в т. ч. биткоина и эфира.

6. Инновации

В предыдущем разделе было дано определение общих характеристик всех криптовалют и сейчас необходимо уже рассказать о принципиально новых блокчейн-технологиях, которые будут реализованы в проекте DeepOnion в целях удовлетворения постоянно повышающихся требований к криптовалютам и в аспекте необходимости дальнейшего повышения уровней конфиденциальности и анонимности.

DeepOnion является форком Supercoin – анонимной криптовалюты со скрытыми транзакциями за счет использования технологий «смешивания монет». Supercoin стал отличной базой для дальнейшего развития и усовершенствования. Далее будут приведены подробные пояснения по внедрению новейших блокчейн-разработок в проекте DeepOnion и обоснования их выбора.

6.1. TOR

Для системы TOR дается следующее определение: служба коммуникации с низкими задержками, основанная на цепочках. Эта система «луковой маршрутизации» второго поколения решает проблемы оригинального проекта путем добавления совершенной секретности, контроля перегрузки, серверов каталогов, проверки

целостности, настраиваемых политик выхода трафика и практичной схемы доступа к службам со скрытым местоположением. TOR работает в обычном интернете, не требует специальных привилегий или программно-аппаратных изменений, надежно функционирует даже при небольшом количества синхронизаций между узлами и представляет собой разумный компромисс между анонимностью, эффективностью и простотой использования[2]. Это все является идеальной платформой для создания анонимной криптовалюты. На момент написания данного документа было произведено ступенчатое обновление DeepOnion до использования новейшей версии протокола 0.3, что позволит реализовать в нашем кошельке наиболее защищенные, анонимные функции и обеспечить защиту наших пользователей. Важно отметить, что все соединения в кошельке DeepOnion осуществляются через сеть TOR. Ваш публичный IP-адрес никогда не показывается.

6.2. DeepSend

DeepSend – это технология анонимизации транзакций, предназначенная для запутывания их следов в блокчейне (одна из проблем, ранее показанных для биткоина). Его использование совершенно отличается от уже реализованной интеграции с TOR, которая обеспечивает защиту и анонимизацию сетевого трафика на транспортном уровне.

DeepSend включает в себя следующие технологии:

- технология Zero knowledge (нулевого разглашения) от Zerocash и Zerocoin (ZCash и ZCoin);
- технология CoinJoin, с централизованными (например, мастернодами) или случайными микшерами (Dash и SuperCoin);
- Ring signatures (кольцевые подписи) от CryptoNote (Bytecoin и Monero).

У каждой из приведенных технологий есть свои преимущества и недостатки. К примеру, в технологии Zero knowledge монеты каждый раз «сгорают», и «чеканятся» новые, но уже нераспознаваемые, что требует дополнительного места в блокчейне. В настоящее время планируется, что DeepSend станет технологией, подобной CoinJoin/Mixer, основанной на не требующих доверия технологиях мульти-подписей, тем самым обеспечивая самый современный уровень анонимности и конфиденциальности. Чтобы представить себе, как это выглядит, рассмотрим следующий сценарий:

- некто *А* хочет заплатить *Б* определенное количество $x монет;
- вместо того чтобы заплатить их непосредственно *Б,* тем самым публично разглашая транзакцию всем (что сейчас происходит в биткоине), *А* платит *В, В* платит *Г,* и т. д.; наконец, после n итераций, *Я* платит *Б;*

- таким образом, все платежи между *А* и *Б* гарантируются мультиподписями, и ни один из адресов не связывается с конкретными лицами;
- это происходит за счет того, что *В* получает деньги от *Б,* однако платит *Г,* используя другой, не связанный с ним адрес; благодаря этому проследить транзакцию становится практически невозможным (при условии достаточного числа итераций).

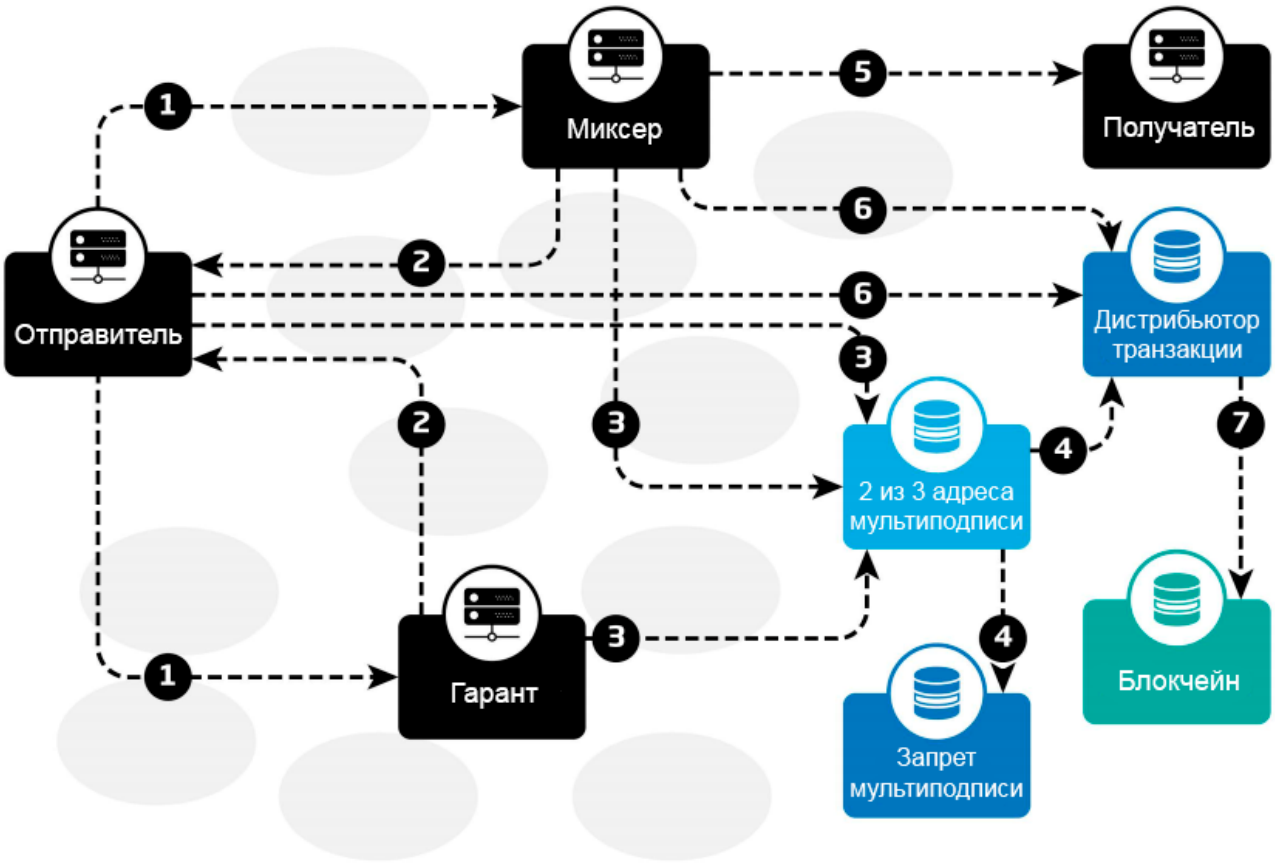

Рис. 3. Реализация транзакций в DeepSend (обфускация при помощи CoinJoin и мультиподписей)[9]

Схема реализации транзакций в DeepSend приведена на рис. 3:

- отправитель случайным образом выбирает 2 ноды из списка нод и запрашивает анонимизацию транзакций;
- миксер и гарант подтверждают запрос;
- 3 задействованные стороны обмениваются открытыми ключами и создают 2 из 3 адрес мультиподписи, обеспечивая данную операцию необходимым депозитом, отправитель также формирует депозит из суммы транзакции и комиссии;
- после верификации депозита, идет подготовка транзакций распределения мультиподписи для подтверждения и отмены операции, уведомления о которых отправляются всем сторонам;
- после проверки 2 транзакций мультиподписи, миксер отправит необходимую сумму получателю, а также подтверждающие транзакции для проверки всем задействованным сторонам;
- миксер подпишет транзакцию распределения мультиподписи и отправит ее всем остальным, отправитель проверит информацию от миксера и в случае успешной проверки подпишет ее;
- отправитель вышлет транзакцию распределения в сеть, всем гарантам возмещены депозиты, сумма платежа

отправлена в миксер, оплачена комиссия, анонимная транзакция завершена.

6.3. DeepVault

DeepVault – это неизменяемое хранилище информации, которое реализовано в блокчейне DeepOnion. Точнее говоря, DeepVault позволяет генерировать и сохранять хеши электронных документов (файлов) в блокчейне DeepOnion. Очевидные достоинства использования этой технологии заключаются в том, что пользователи получают возможность проверять идентичность электронных документов (файлов) по прошествии времени. Таким образом, в случае изменения хеша файла это доказывает, что файл был изменен или поврежден. Данный инструмент станет незаменимым при проверке защищенности важных документов и отсутствия фальсификаций. Вероятной сферой применения DeepVault станет юриспруденция, так как полностью реализована возможность проверки того, что документ, а следовательно, и его содержание, не подвергался изменениям – с преступным намерением, по ошибке или вследствие повреждения файла. DeepVault можно рассматривать как дальнейшее развитие концепции смарт-контрактов, в которых валидация условий или целостности также осуществляется при помощи криптографии.

Вы можете ознакомиться с видеоинструкцией по использованию технологии DeepVault, реализованной в

функционале кошелька DeepOnion, которую подготовил @escapefrom3dom[6] либо прочитать руководство[7].

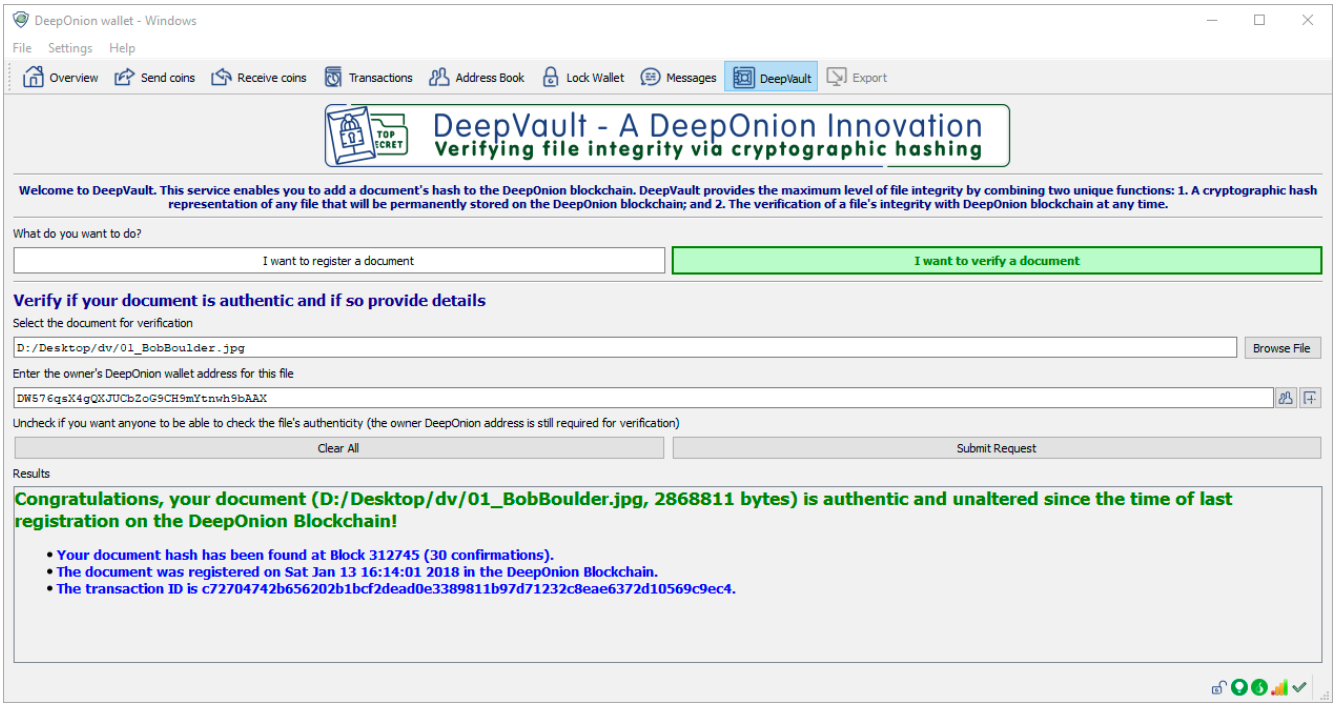

Рис. 4. Интерфейс DeepVault в кошельке DeepOnion

DeepVault эффективно интегрирован в кошелек DeepOnion, а его интерфейс интуитивно понятен (см. рис. 4). Эта инновационная функция обеспечивает практическое решение давней проблемы валидации электронных документов (файлов). DeepVault позволяет усовершенствовать процессы хеширования и процессы последующей верификации файлов за счет ряда простых в использовании преимуществ:

- Хеш файла генерируется с использованием графического интерфейса кошелька DeepOnion;
- при хешировании используется безопасный и надежный алгоритм SHA-256;

- DeepVault обеспечивает защиту хеша файла в неизменяемом блокчейне DeepOnion, это означает, что сам хеш защищен от внесения изменений;
- верификация файла может быть привязана к пользователю, что не позволит кому-либо еще осуществить валидацию файла.

Мы убеждены, что DeepVault – это важный инструмент, который поможет нашим пользователям обезопасить и защитить себя в цифровую эпоху. Возможность верификации целостности файлов предоставляет бесчисленные преимущества и может быть реализована практически во всех сценариях.

В 1 кв. 2018 г. запланировано расширение DeepVault с развертыванием решения с облачным хостингом, которое позволит создать веб-интерфейс для защиты ваших файлов. Подробные сведения о нем будут вскоре опубликованы.

6.4. Мобильный кошелек

Релиз мобильного кошелька DeepOnion на для операционной системы Android состоится в начале 2018 г. Он будет обеспечивать возможность пользования теми же функциями, что и со стационарного компьютера (окончательный набор функций подлежит уточнению) и естественным образом работать в сети TOR, защищая ваши идентификационные данные «на ходу». Одной из важных функций мобильного кошелька станет поддержка

DeepVault, обеспечивающий защиту ваших документов (в т. ч. защиту фотографий).

Помимо этого, пользователи смогут просматривать свои транзакции, адресную книгу, использовать VoteCentral, а также формировать платежные транзакции и получать онионы.

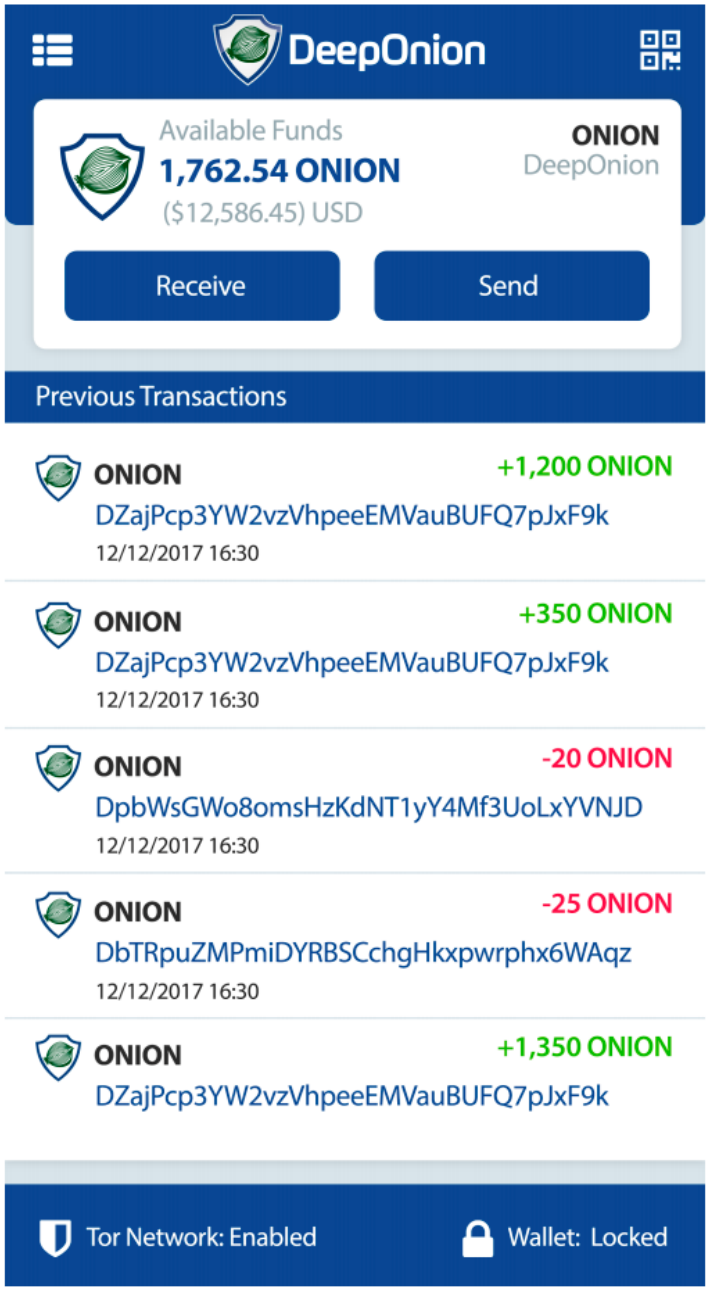

Рис. 5. Мобильный кошелек DeepOnion

В настоящий момент мы проводим поиск iOS-разработчика, задачей которого будет создание мобильного кошелька DeepOnion для устройств Apple. Читайте наш официальный форум и информационные рассылки, чтобы быть в курсе событий.

6.5. VoteCentral

VoteCentral – это открытая платформа голосования, разработанная на базе блокчейн-технологий, которая обеспечивает сообществе DeepOnion возможность голосования по предложениям и задачам, внесенным членами сообщества в отношении будущих направлений развития проекта DeepOnion.

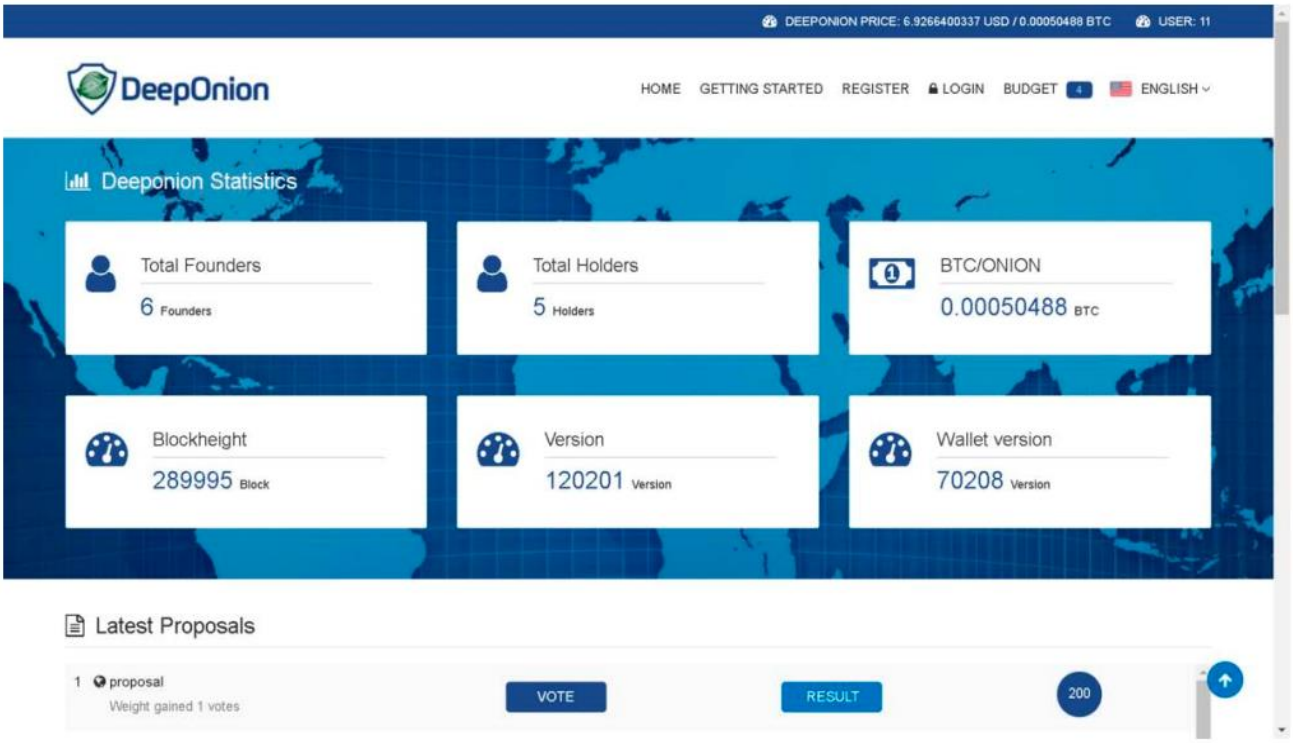

Рис. 6. Лендинг VoteCentral (альфа версия)

Благодаря этой платформе члены DeepOnion смогут оказывать влияние на принимаемые сообществом решения, определяющие направление и темпы развития проекта DeepOnion.

В VoteCentral прослеживаются множество параллелей с существующими в современной политике демократическими системами голосования, с тем отличием, что здесь имеются дополнительные преимущества блокчейн-технологии, позволяющие минимизировать подтасовку голосов. Новые направления или предложения по деятельности сообщества регистрируются в VoteCentral и затем оцениваются командой разработчиков, участниками бесплатных еженедельных раздач и держателями онионов, остаток в кошельках у которых выше заданного минимума (см. правила еженедельных раздач).

Как мы уже упоминали в предыдущих сообщениях, VoteCentral представляет собой многоуровневый подход. Чтобы сформировать представление о данной иерархии, представьте себе 3 концентрические окружности:

- внутренняя окружность (ядро) включает в себя команду разработчиков и первоначальных основателей;
- средняя окружность – участники еженедельных раздач, получившие статус основателя с правом голоса в VoteCentral;
- и наконец, внешний круг – это участники сообщества, которые внесли существенный вклад в развитие DeepOnion.

Принцип голосования основан на подтвержденном вкладе в развитие проекта (или статусе, полученном в результате длительной поддержки). В данный момент, вес голоса каждого участника сообщества (право участия в голосовании) зависит от баланса зарегистрированного адреса кошелька.

VoteCentral реализован двуэтапно: централизованное решение, которое поддерживается исключительно веб-технологиями, и пока что проектируемый следующий слой, который будет поддерживаться на уровне блокчейна.

На первом этапе участникам необходимо подтвердить владение ONION-кошельком путем регистрации сообщения-подписи. Мы сможем ежедневно проверять баланс кошелька членов сообщества и соответственно определять вес голоса каждого участника в отношении предложений, внесенных командой разработчиков или другими участниками и ожидающих решения. Предложения должны соответствовать протоколам и стандартам, которые пока не определены, уточнения по этому поводу будут представлены позже.

Окончательное решение по поводу направления развития проекта будет приниматься командой разработчиков, основателями и держателями онионов, зарегистрированными в VoteCentral, однако свое мнение сможет выразить каждый участник сообщества.

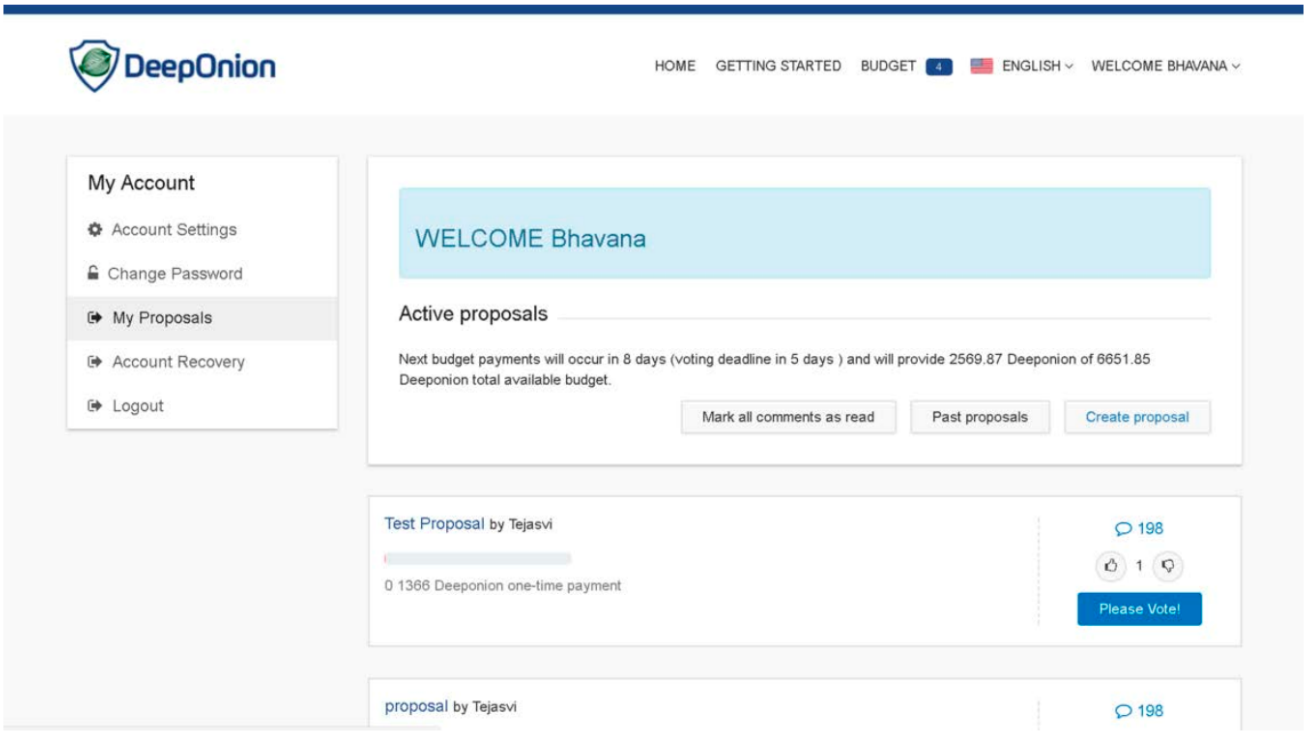

Рис. 7. Просмотр и создание предложений (альфа версия)

Мы полагаем большие надежды на VoteCentral и хотим создать своего рода «живой организм», в котором принятия или отклонении решений будет основано на глубоком анализе и оценке, с опорой на мнения участников сообщества, и демократическим образом взвешивая их. В VoteCentral выбираются самые лучшие и популярные предложения/задачи, направленные на обеспечение дальнейшего расширения (доминирования) проекта DeepOnion.

Вы сможете сыграть важную роль в определении его будущего и высказать свое мнение, доказав свою преданность идее DeepOnion, что впоследствии обеспечит повышение веса вашего

голоса в проекте. Чем сильнее будет наше сообщество основателей, тем лучше станет DeepOnion.

6.6. DeepPoints

DeepPoints – это программа вознаграждений для участников нашего сообщества, позволяющая получать онионы за свой вклад в проект. Мы ставим целью вознаграждать тех, кто регулярно публикует содержательные посты и создает качественные рекламные материалы. Достоинства такого подхода обусловлены возможностью регулировать и направлять наше сообщество к определенной цели, что уже принесло свои плоды в целом ряде случаев, например, в задачах обеспечения листинга на биржах (KuCoin и Satoshi Exchange), и несомненно сыграет решающую роль в экспансии на платформы Bittrex и Binance.

Суть DeepPoints крайне проста: чем больше вы выполните официальных заданий из раздела VIP Domination на официальном форуме (в пределах задокументированных правил и не допуская спама), тем больше баллов (DeepPoints) получите.

Часть монет из наших еженедельных бесплатных раздач резервируется для выдачи вознаграждений по программе DeepPoints. Для участников сообщества – это отличная возможность получить щедрое вознаграждение.

7. Планы на будущее

2017 год был очень успешным для DeepOnion. Кроме того, что наша тема на форуме BitcoinTalk.org стала одной из наиболее популярных, наше сообщество сумело добиться этого всего за 6 месяцев. У нас наблюдается постоянный устойчивый прирост участников сообщества на официальном форуме – примерно на 750 человек в неделю. Также можно отметить стабильность мощности PoW майнинга, обеспечивающей поддержку блокчейна DeepOnion. При имеющейся на данный момент дорожной карте и после недавнего расширения нашей команды разработчиков, 2018 год непременно должен побить все рекорды!

Ежедневно с нами связываются крупные инвесторы, биржи, предлагающие включение в листинги, а также известные в криптосфере лица, желающие принять участие в проекте. Приятно видеть, что упорный труд команды разработчиков и сообщества приносит свои плоды.

Важно отметить, что мы будет упорно трудиться до тех пор, пока DeepOnion не станет признанной конфиденциальной криптовалютой де-факто. Наши идеи распространяются все шире, наши суточные объемы торгов и биржевые листинги ежемесячно возрастают, и мы продолжаем интегрировать новые блокчейн-технологии. Что впечатляет еще больше – мы даже еще не начали рекламную кампанию, отмеченную в дорожной карте. Мы уверены,

что после полной реализации дорожной карты с привлечением знаменитостей («звездной» рекламой) DeepOnion непременно окажется в самых первых рядах признанных криптовалют.

Итак, 2018 год – он непременно должен стать годом впечатляющих результатов!

- DeepSend;
- веб-сервис DeepVault;
- VoteCentral;
- смарт-контракты;
- мобильные кошельки;
- рекламная кампания;
- привлечение знаменитостей.

8. Благодарности

Команда DeepOnion благодарит сообщество проекта и всех тех, кто приобретал онионы и поддерживал нас все это время. Именно благодаря вам этот проект стал тем, что он представляет собой сегодня. У нас есть технология, есть концепция развития, однако именно вы помогаете нам превратить все это в работающую экосистему, которая позволит всем нам пользоваться преимуществами анонимных, конфиденциальных финансовых транзакций в нынешнем мире, где все более широкое распространение получает цифровой шпионаж. Спасибо вам, и продолжайте, пожалуйста, поддерживать нас и далее.

Также команда DeepOnion хотела бы выразить благодарность за непрерывный труд нашей старательной команде модераторов, которая всегда отлично выполняет все поставленные требования проекта и сообщества (и даже во время праздников!).

Особая благодарность – @Impressive и @DogLover за создание рисунков, которые были использованы в данном документе.

Использованные источники

[1] The Bitcoin Project. 2017. *Bitcoin is an innovative payment network and a new kind of money.* https://bitcoin.org

[2] R. Dingledine, N. Mathewson & P. Syverson. 2013. *Tor: The Second-Generation Onion Router, 2nd ed.* https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf

[3] The Economist. 2015. *The great chain of being sure about things*. https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

[4] A. Greenberg. 2011. *Crypto Currency*. Forbes.com. https://www.forbes.com/forbes/2011/0509/technologypsilocybin-bitcoins-gavin-andresen- crypto-currency.html

[5] Merriam-Webster Dictionary. 2017. *Definition of decentralization*. https://www.merriam-webster.com/dictionary/decentralization

[6] @escapefrom3dom. 2017. *DeepVault. Видеоинструкция по регистрации и проверке документов.* https://deeponion.org/community/threads/deepvault-videoinstrukcija-po-registracii-i-proverke-dokumentov.21641

[7] @Jimmybob. 2017. *DeepVault Tutorial Manual*. https://deeponion.org/community/threads/tutorialdeepvault.3868

[8] J. Vermeulen. 2017. *Bitcoin and Ethereum vs VISA and PayPal.* https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-persecond.html

[9] SuperCoin. 2016. *SuperCoin's Revival*. https://bitcointalk.org/index.php?topic=1351548

[10] Wikipedia. 2017. *Wannacry.* https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[11] M. Green. 2014. *Zero Knowledge Proofs: An Illustrated Primer*. https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer

[12] Bitcoin Wiki. 2018. *Multisignature*. https://en.bitcoin.it/wiki/Multisignature

[13] Wikipedia. 2018. *Collision Attack*. https://en.wikipedia.org/wiki/Collision_attack

Приложение А. Спецификация распределения монет

Квоты распределения монет

Были изменены квоты распределения для создания Фонда Разработчиков. Это обусловлено возможностью передачи решения некоторых задач под аутсорсинг, что позволит ускорить развитие DeepOnion и сделать проект действительно исключительным.

Использование средств Фонда Разработчиков будет полностью контролироваться сообществом. После завершения всех раундов еженедельных раздач также будет создан VoteCentral для выбора наиболее важных вопросов с помощью голосования.

План распределения монет

- (0) полное количество монет, полученных премайнингом: **18 000 000;**
- (1А) раунды еженедельных раздач № 1-15: **3 200 000;**
- (1Б) раунды еженедельных раздач № 16-40: **6 800 000** (раунды № 16-30: **250 000** в каждом, раунды № 31-39: **300 000** в каждом, раунд № 40: **350 000**).

Для выплат наград участникам форума сообщества, за участие в различных акциях, будет использоваться 10% от суммы каждой еженедельной раздачи. Оставшиеся 90% будут распределены непосредственно в раздаче.

(2) Фонд Баунти: 3 000 000

Текущий баланс Фонда Баунти, после выплат за выполнение различных задач/наград/прочих распределений, составляет 2 600 000 онионов. Этот фонд используется для выплат за создание статей, видео, значимые вклады в развитие DeepOnion и сообщества, а также для поддержки новых продавцов, использующих онионы.

(3) Награда для основателей DeepOnion: 2 000 000

(4) Фонд Разработчиков: 3 000 000

Средства предназначены для разработки смарт-контрактов и прочих новых функций. Использование средств фонда будет определяться сообществом через голосование в VoteCentral.

(1А) + (1Б) + (2) + (3) + (4) = 18 000 000 = (0).