Ghost

Монета конфиденциальности John McAfee

ghostbymcafee.com | @ghostbymcafee

"*Призрак бродит по современному миру, призрак криптоанархии.*"

Тим Мэй – Манифест криптоанархизма (1992)

СОДЕРЖАНИЕ

Краткий обзор

Миссия проекта Ghost заключается в создании ориентированной на конфиденциальность, анонимной и децентрализованной платежной сети, основанной на устойчивом алгоритме согласования доказательств заинтересованности с мотивированными операторами. Предложенные продукты и услуги будут ориентированы на простоту и в то же время будут предлагать доступные и практичные решения для широкого применения.

Этот документ будет состоять из краткого обзора происхождения биткойна, механизмов, приводящих в действие блокчейн, и краткого объяснения вариантов использования этой технологии. В нем также будет обсуждаться, как можно значительно улучшить самую продаваемую монету на рынке, биткойн, различными способами. Кроме того, текущие решения, которые были представлены на рынке до сих пор, будут проанализированы при рассмотрении базовой технологии, на которой они работают.

Кроме того, в нем будет подробно описано, как и почему эти решения должны быть еще более усовершенствованы, и, в конечном счете, как эти изменения будут подталкивать криптовалюты в целом к созданию большего экономического влияния на общество для действительно функциональной, конфиденциальной и доступной децентрализованной системы электронных платежей.

Также будет представлена Particl, монета, ориентированная на конфиденциальность, из которой изначально был создан Ghost. Первоначально отличающийся от биткойна, этот проект был значительно проработан и улучшен их командой инженеров. Вместо того, чтобы начать с нуля, Ghost пришел к выводу, что Particl обеспечит прочную основу для запуска инициативы. Это позволило проекту начать реализацию собственных инновационных технологических достижений без необходимости «изобретать велосипед».

Однако видение Ghost выходит далеко за рамки его предложения. В документе будет представлена его текущая и будущая повестка дня в области развития с пояснениями после каждого основного дополнения. Также будут предоставлены

полные технические характеристики, относящиеся к внутренней работе и функциональным функциям программного обеспечения. Наконец, будет дана информация о текущей команде Ghost вместе с видением и планами на будущее.

GHOST

вошёл в чат.

Введение

В 2008 году объект, известный как Сатоши Накамото, опубликовал статью [Nak08], описывающую цифровую валюту, которая была направлена на решение проблем ее предшественников. Это включало такие проблемы, как двойные расходы [1] и непереносимость византийских ошибок [2] - это валюта биткойн. Биткойн использует криптографию для определения прав собственности на средства и использует доказательство работы (Proof of Work) [3] с предопределенными правилами для достижения консенсуса и выявления нечестных участников сети.

Несмотря на успешное решение многих проблем предшественников, являющихся первой широко распространенной децентрализованной системой цифровых наличных средств, есть и ряд недостатков. В частности, мы ссылаемся на отсутствие специфических функций, которые другие криптовалюты решили исправить и использовать. Например, вскоре после того, как в 2014 году появился Ethereum, он предоставил инновационную возможность децентрализованного выполнения компьютерных программ, что позволяет достичь консенсуса среди распределенных систем. В этом техническом документе мы обсуждаем криптовалютный продукт, который фокусируется на конфиденциальности его пользователей - Ghost.

Право собственности на средства в биткоине

Биткойн использует криптографию с эллиптической кривой[4] для назначения средств различным пользователям, владение которыми связано с владением

---

[1] Двойные расходы - это возможность обмануть цифровую систему денежных средств, потратив сумму более одного раза.

[2] Непереносимость византийских ошибок является проблемой в распределенных вычислительных системах, где невозможно отличить честные узлы от нечестных узлов для достижения консенсуса.

[3] Proof-of-work - это механизм, с помощью которого честные узлы доказывают свою честность в общении, доказывая, что их сообщенное состояние или сообщение создается путем решения проблемы, требующей сложных вычислений, которые, в зависимости от системы, были бы непрактичными для нечестных узел

[4] Криптография с эллиптической кривой - это подход к криптографии с открытым ключом, основанный на алгебраической структуре эллиптических кривых над конечными полями. ECC позволяет использовать меньшие ключи по сравнению с не-EC криптографией для обеспечения эквивалентной безопасности

личным ключом, из которого можно сгенерировать адрес. Средства могут быть отправлены на этот адрес и могут быть потрачены только с использованием цифровой подписи, которая авторизует транзакцию.

Блокчейн

Когда владелец подписывает транзакцию, чтобы потратить ее, программное обеспечение кошелька транслирует транзакцию в сеть биткойна. Эти транзакции получают майнеры, которые собирают все транзакции и помещают их в блок, который в настоящее время может содержать до 1 МБ данных транзакций. После заполнения блока всеми доступными транзакциями, майнер «добывает» блок, процесс, в котором используется доказательство работы Proof of Work (т. е. тратится электричество), чтобы решить вычислительную головоломку. Все майнеры соревнуются, чтобы решить эту загадку. Как только кто-то успешно решает её, они передают свой блок в сеть, которая принимает его в качестве своего нового состояния (следовательно, достигается консенсус). Успешные майнеры получают вознаграждение за новый биткойн и комиссионные за свои усилия.

Блоки гарантируются неизменяемыми с помощью хэш-функций, где хэш данных в блоке шифруется и сохраняется. Любая попытка изменить данные блока будет немедленно распознана. Хеши используются для связывания блоков вместе. Каждый блок содержит хэш данных в блоке, который предшествовал ему. Это поднимает термин blockchain, «цепочка блоков» (прим. перев.), где блоки «объединяются» вместе с использованием их криптографических хэшей.

Попытка изменить что-либо в блоке из прошлого изменит его хэш, что, в свою очередь, изменит хэш, сохраненный в следующем блоке, что, в свою очередь, изменит блок после этого, что приведет к лавине, где все блоки станут другими. Это то, что гарантирует неизменность блокчейна.

Майнинг в Proof-of-Work

Сатоши планировал, что майнинг биткойнов будет эгалитарным, то есть любой человек может участвовать в майнинге сети и зарабатывать биткойны на своих персональных компьютерах. Однако, поскольку добыча биткойнов зависит от бесконечного выполнения функций хеширования, SHA256, устройства, известные как ASIC, которые намного более эффективны, чем компьютеры, могут специально подходить для этой задачи. ASIC труднодоступны для большинства людей, и, как правило, дорого стоят. Это сделало практически невозможным участие обычного человека в майнинге и открыло двери для больших «ферм», делающих это на профессиональной основе. Попытки избавиться от ASIC неуклонно росли на протяжении многих лет, поскольку другие криптовалюты применяли алгоритмы хеширования, которые требуют значительную память для своих вычислений, и другие функции, которые трудно реализовать на чипе без процессора. Однако большинство этих попыток провалилось, и «борьба» с ASIC продолжается. Некоторые проекты решили позиционировать себя как движущуюся цель, их алгоритм майнинга постоянно меняется. Хорошим примером этого является Monero, который ранее менял свой алгоритм майнинга каждые шесть месяцев. В конце концов был изобретен новый алгоритм майнинга RandomX [Ran19]. RandomX использует комбинацию инструкций ЦП в процессе интеллектуального анализа, фактически считая ASIC бесполезными по определению, поскольку выполнение инструкций ЦП является противоположным тому, чем должен быть ASIC (т.е. быть специфичным для приложения).

Тем не менее, мы рассматриваем проблему как нечто большее, чем просто запрет ASIC из-за вышеупомянутого. Мы находим, что добыча сама по себе неэгалитарна, потому что, помимо высокой стоимости оборудования, стоимость электроэнергии также никогда не будет одинаковой для всех. Исследование, проведенное Elite Fixtures [Eli18], показало, что существует значительная разница в расходах на майнинг одного биткойна в разных странах, учитывая, что все остальные факторы равны (то есть ASIC доступны для всех). Это несоответствие показывает, что некоторые люди всегда будут более удачливыми, чем другие, и

будут иметь более дешевое электричество и, следовательно, получать больше прибыли от добычи полезных ископаемых. Следовательно, это ведет к централизации добычи полезных ископаемых. Это особенно очевидно в настоящее время в биткойнах, где «объединённые фермы» китайского происхождения занимают более 65% рынка этих операций [Cry19]. Явление, которое является результатом системы свободного рынка, только неизбежно будет усугубляться.

Развитие

Недостаток конфиденциальности на блокчейне

Блокчейны, как правило, не предназначены для обеспечения конфиденциальности. Конфиденциальность в этом случае означает, что отправитель, получатель и отправляемая сумма не должны быть видны ни одной сущности в блокчейне, кроме тех, кто имеет финансовый интерес в транзакции. Однако в биткойнах, и в большинстве блокчейнов, вся упомянутая ранее информация видна. Любой, кто просматривает блокчейн, может видеть адреса назначения каждой транзакции, суммы, отправляемые на эти адреса, и, поскольку каждый адрес имеет только один приватный ключ, из которого он получен, мы знаем, что владелец этого адреса является подписавшей стороной этой транзакции. Чтобы ухудшить ситуацию; с помощью статистического анализа и машинного обучения адреса могут быть связаны друг с другом, и даже можно найти их конечного владельца. Кроме того, есть компании, которые проявили инициативу в предоставлении услуг связывания адресов и раскрытия информации о пользователях блокчейна. Примером является Chainalysis[5]. Он также предоставляет его как услугу правительствам[6]. Это особенно опасно для людей, которые живут в странах с репрессивными властями, где эта информация может свободно использоваться для вторжения в гражданские права.

Другими словами, несмотря на то, что адреса являются псевдонимными и не раскрывают владельца по имени, целесообразно проследить отправителей и получателей транзакций вплоть до обмена, где пользователь представил свою личную информацию в соответствии с законами KYC[7] и AML[8] которые в

---

[5] https://www.chainalysis.com/
[6] https://www.chainalysis.com/government-agencies/
[7] Know-Your-Customer, процедура идентификации личности
[8] Anti-Money Laundering, борьба с отмыванием денег

конечном итоге покажет владельца. Мало того, но это также ставит под угрозу фунгируемость криптовалюты.[9]

Например, если какой-либо биткойн должен был быть использован для гнусных действий, а затем он вступил во владение кем-то, кто не знал о своей предыдущей истории, человек может непреднамеренно понизить свою ценность / использование, поскольку монеты будут считаться «Испорченный» [Min15]. Это особенно заметно на событиях, когда недавно добытые биткойны продавались за премию [Red20], так как у них не было предыдущей истории транзакций.

Помимо проблем, упомянутых выше, это также может привести к проблемам безопасности. Например, в результате раскрытия их владений были случаи, когда людям угрожали их жизни и заставляли платить выкуп в указанной криптовалюте [Gua17].

Принимая во внимание вышеизложенное, очевидно, что существует настоятельная необходимость в устранении связности[10] и отслеживаемости[11] в блокчейне, чтобы обеспечить конфиденциальность своих пользователей.

Proof-of-Stake против Proof-of-Work

В проекте Ghost используется алгоритм консенсуса с подтверждением доли (Proof of Stake). В этом процессе участники используют свои цифровые активы в качестве обеспечения (в отличие от расходов на электроэнергию в качестве доказательства работы), где они доказывают, что имеют положительные значения в сети. Другими словами, вместо того, чтобы тратить электричество, чтобы доказать другим узлам, что майнер работал над созданием блока, «стейкер» в другой модели доверия использует свою криптовалюту, чтобы подтвердить свою честность через свою долю в сети. Участники имеют большее влияние в сети, если владеют большей долей общего объёма в сети. Не в интересах

---

[9] Фунгируемость - это свойство денег или валюты, где нет практического способа различить разные его единицы по стоимости. Например, нет разницы между 1 долларом в моем кармане и 1 долларом в вашем. Они оба имеют одинаковую ценность, признание и характеристики.

[10] Связность - это возможность связать несколько транзакций с одним человеком, адресом или подписью.

[11] Отслеживаемость - это способность проследить или предугадать источник монеты по ее истории.

заинтересованного лица быть нечестным в сети, потому что если оно попытаются нарушить его, игнорируя правила, оно потеряет ценность своей части монет на свободном рынке. Будучи честным участником сети, участники получают вознаграждение (как и майнеры) за создание новых и действующих блоков.

Проходят большие споры о том, лучше ли доказательство доли или доказательство работы. Тем не менее, стоит отметить, что никогда не было ни одной успешной атаки 51% на сеть с доказательством доли. Это особенно актуально по сравнению с несколькими атаками на системы для проверки работоспособности (например, Ethereum Classic [Coi19], Bitcoin Gold [Btg51]), где майнеры, которые осуществляют атаку, не заботятся о работоспособности сети. Даже в онлайн-списках, в которых подробно описываются затраты на атаку каждого блокчейна в течение определенного времени [Bie18, Pow51], есть четкая основа для предпочтения доказательства доли.

Однако, поскольку для доказательства доли не требуется физическая работа, такая как доказательство работы, теоретически можно заменить весь блокчейн на новый, созданный за короткое время [Ioh18]. Эта проблема обычно решается с помощью «контрольных точек», где список контрольных точек блоков сохраняется вручную, чтобы защитить от стирания истории цепочки блоков и замены ее другой. Такой метод считается спорным в сообществе криптовалют, поскольку это «централизованное» решение, так как разработчики должны поддерживать это. Тем не менее, многие блокчейны для проверки работоспособности в настоящее время используют этот инструмент для защиты от будущих атак, например, Monero. Сродни им, Ghost также видит в этом хороший компромисс.

Cold-Staking

«Стейкинг» (т. е. использование доказательства доли для участия в сети) практически требует, чтобы владелец средств криптовалюты оставил программное обеспечение своего кошелька открытым, чтобы блоки могли создаваться и подписываться с использованием закрытых ключей, которые

содержат указанные средства. Однако это может быть очень рискованным. Если кто-то держит свой компьютер открытым с доступными средствами, любое нарушение в системе может привести к потере их средств. Тогда возникает вопрос, можно ли сохранить средства на 100% в безопасности и одновременно делать стейкинг? Ответ на эту дилемму: Cold-Staking («холодный стейкинг» - прим. перев.).

Cold-staking представляет собой механизм, посредством которого средства передаются в хранилище холодного типа для распределения делегированных ресурсов[12] . Горячее хранилище (то есть программное обеспечение для стейкинга) может только подписывать транзакции, которые выполняют стейкинг. Таким образом, гарантируется, что нарушение никогда не приведет к краже денежных средств пользователей.

[12] Холодное хранилище, в отличие от горячего хранения, представляет собой метод хранения средств криптовалюты, при котором кошелек, управляющий приватным ключом, не подключен напрямую к Интернету. Хорошим примером этого являются аппаратные кошельки, такие как Ledger Nano и Trezor.

Конфиденциальность

Что такое конфиденциальность на блокчейне и как её можно улучшить

Конфиденциальность в криптовалюте обычно влечет за собой сокрытие трех элементов в транзакции:

1. Получателя сделки
2. Отправителя транзакции
3. Отправляемой суммы

Сокрытие получателя сделки

В биткойне, как обсуждалось ранее, адрес получателя напрямую рассчитывается из публичного ключа, который, в свою очередь, выводится из приватного ключа, который должен использоваться для расходования средств с этого адреса. Это напрямую означает, что адрес всегда можно использовать повторно, и он всегда будет указывать на владельца приватного ключа. Соответственно, участники всегда могут знать, сколько принадлежит каждому адресу, и куда поступили средства с этого адреса. Следовательно, это приводит к их прослеживаемости. В результате пользователи подвергаются изучению своих финансовых привычек, социальной инженерии и общего контроля со стороны других, в частности государственных организаций (например, правительств).

Чтобы решить эту проблему, вместо обычного адреса Ghost использует скрытые адреса (Stealth Addresses)[13].

Ниже приведено более подробное описание того, как это работает.

[13] Скрытые адреса были впервые введены в протокол Cryptonote [Van12].

A	**B**
Public Key 1	Public Key 2

Stealth Address

Скрытый адрес состоит из двух открытых ключей, давайте их назовем (A, B). Мы называем закрытые ключи, связанные с ними (a, b)[14]. Первый открытый ключ A, связанный с приватным ключом, позволяет расходовать средства, отправленные на этот адрес, а второй публичный ключ B используется как часть протокола соглашения и называется протоколом Диффи-Хеллмана.

Допустим, Алиса и Боб хотят общаться по небезопасному каналу. Оба имеют возможность генерировать приватные ключи и связанные с ними публичные ключи. Но им нужен способ безопасной передачи информации по этому небезопасному каналу. Протокол Диффи-Хеллмана решает эту проблему, позволяя создать общий ключ между отправителем и получателем, только совместно используя их открытые ключи. Соглашение в основном подразумевает, что Алиса отправляет Бобу свой открытый ключ, а Боб отправляет Алисе свой. Сразу после этого они могут комбинировать свои закрытые ключи с другими (личный ключ Алисы с Бобом и личный ключ Боба с Алисой), чтобы создать общий секретный ключ, который они могут использовать для шифрования любых обменов данными между ними[15].

Второй открытый ключ в скрытом адресе Б действует как один открытый ключ в *протоколе Диффи-Хеллмана*. Создатель транзакции генерирует случайный закрытый ключ, давайте пометим его как r и скомбинируем его со вторым открытым ключом скрытый адрес. Затем открытый ключ Ris вычисляется из закрытого ключа r и добавляется к транзакции. Получатель транзакции может

---

[14] Если мы назовем базовую точку в используемой эллиптической кривой G, то aG = A и bG = B.

[15] Если базовая точка эллиптической кривой - G, и если мы должны были пометить закрытый ключ Алисы и открытый ключ, то xG = закрытый ключ и открытый ключ Боба yG = Y; общий секрет протокола Диффи-Хеллмана: xY = yxG = xyG = yX.Hence. Алиса или Боб могут использовать свой закрытый ключ и открытый ключ другого, чтобы получить тот же общий секретный ключ xyG.

использовать закрытый ключ ключа представления b и комбинировать его с R, который был включен в транзакцию, для восстановления общего секрета.

Наконец, после создания общего секрета создатель транзакции также комбинирует его с первым открытым ключом A скрытого адреса. Результатом является новый случайный адрес (так как появился новый случайный закрытый ключ), который может быть раскрыт только владельцем второго закрытого ключа B скрытого адреса (называемого ключом просмотра) и может быть потрачен только владельцем первого и второго закрытых ключей (a, b) скрытого адреса (ключ расходов).

Таким образом, каждый раз, когда кто-то отправляет транзакцию на скрытый адрес, может быть создан новый открытый ключ (и, следовательно, фактически новый адрес), что делает практически невозможным отслеживание и связность транзакций.

Сокрытие отправителя / подписанта транзакций

Поскольку входные данные представляют собой средства, которые должны быть израсходованы, отправитель должен подтвердить, что он уполномочен их тратить. В биткоине каждый вход должен сопровождаться цифровой подписью, которая показывает, что создатель этой транзакции разрешил его тратить. Хотя это работает безупречно, его можно использовать для отслеживания транзакций и их истории, а также связи трат для распознавания поведения пользователя. Это считается проблемой в конфиденциальности биткоина.

Как также продемонстрировано в этом проекте, потенциальным решением этой проблемы может быть использование цифровых подписей для маскировки реального лица, подписавшего транзакцию. Эта технология обычно называется кольцевой подписью.

Круговые подписи

Чтобы объяснить, как работают круговые подписи, давайте использовать следующий пример. Допустим, Алиса работает на коррумпированную

правительственную организацию. Алиса заслуживает доверия, и, выполняя свою работу, она достала документы, которые считаются свидетельством коррупции, которую она хочет остановить. Теперь она хочет открыть эту информацию общественности. Однако, если она это сделает, у ее работодателя всегда будет правдоподобное отрицание, утверждающее, что эти документы не были получены внутри учреждения, и поэтому ее усилия будут бесполезными. С другой стороны, если она использует свою официальную институциональную пару приватного / публичного ключа для подписания этих документов, она рискует уличить себя (то есть, как это сделал Эдвард Сноуден, публикуя правительственную информацию для общественности). Что ей делать?

Возможное решение: кольцевые подписи. Вместе со своим закрытым ключом Алиса может взять открытые ключи 9 других должностных лиц и создать круговую подпись этих документов. Круговая подпись раскрывает все открытые ключи, которые подписали документы. Это, однако, не раскрывает, кто является действительным подписавшим лицом (то есть лицом, использовавшим свой закрытый ключ для подписания документа). Нет никакого практического способа подтвердить, что Алиса является той, кто фактически разрешил эту подпись. Таким образом, Алиса поддерживает правдоподобное отрицание, и в то же время придает достоверность подписанным документам, доказывая коррупцию, которую она хочет обнародовать.

По сути, кольцевые подписи, вместо того, чтобы просто использовать один закрытый ключ для подписания транзакции, включают в себя набор открытых ключей непроизвольных лиц, случайным образом выбираемых из блокчейна, которые называются приманками. Таким образом, транзакция с размером кольца 10 будет иметь 10 участников, любой из которых мог бы потенциально подписать эту транзакцию. Любой создатель транзакции поддерживает правдоподобное отрицание того, кто подписал транзакцию. Что еще более важно, эта технология в сочетании со скрытыми адресами означает, что транзакция никогда не увидит тот же самый закрытый ключ, что еще больше затруднит связывание или отслеживание любых транзакций.

Сокрытие сумм, отправленных в блокчейн

Биткоин использует чистые суммы, записанные в блокчейне, чтобы указать числа, которые транзакция содержит в своих входах и выходах. Это облегчает отслеживание людей, которые имеют большие сальдо и помогает социальной инженерии и преступлениям с выкупом, где блокчейн можно проанализировать, чтобы определить, кто является отправителями и получателями значительных транзакций. Чтобы решить эту проблему, можно использовать механизм, который скрывает суммы в транзакции, в то же время поддерживая их правдоподобность (чтобы предотвратить отправку «отрицательных» сумм или отправку денег, которые не существуют).

Чтобы наиболее просто проиллюстрировать, как суммы хранятся в секрете и в то же время проверяются на общедоступность, рассмотрим следующий пример. Алиса хочет отправить 10 монет Бобу. Предположим, что у Алисы есть два входа, которые составляют 12 монет (4 и 8). Транзакция будет выглядеть следующим образом:

$$4+8 \rightarrow 10+2$$

Левая сторона представляет входные данные, а правая сторона представляет выходные данные, где Алиса возвращает 2 монеты на свой собственный адрес. Давайте также проигнорируем комиссию за транзакцию. Что может сделать Алиса, чтобы скрыть суммы таким образом, чтобы их мог просматривать только Боб, и в то же время позволить майнерам проверить правдоподобность транзакции?

Упрощенное решение будет следующим. Вы знаете, что скрытые адреса состоят из ключа просмотра и ключа расходов. Можно построить общий секретный ключ Диффи-Хеллмана (как обсуждалось ранее), используя ключ просмотра, назовем его k, и, поскольку общий секретный ключ является просто огромным целым числом, мы умножаем это число на всю транзакцию:

$$4k + 8k \rightarrow 10k + 2k$$

Если предположить, что k = 50, уравнение становится следующим:

$$200 + 400 \rightarrow 500 + 100$$

Валидатор может гарантировать, что эта транзакция действительна, потому что сумма входных данных по-прежнему равна сумме выходных данных. Это позволяет ему выполнять свою задачу, не зная исходных сумм.

RingCT

Вышеприведенное обсуждение является упрощенным объяснением того, как работают скрывающие суммы и круговые подписи по сравнению с тем, что мы имеем в настоящее время. Современная технология прогрессировала, и теперь круговые подписи сочетаются с сокрытием сумм в так называемых RingCT или Ring Confidential Transactions («кольцевых конфиденциальных транзакциях» - прим. перев.). Первоначально, начиная с борромеевских подписей Грегори Максвелла и др. [Max15], они были использованы Шеном Нетером и др. [Noe16]. Сделав еще один шаг вперед, RingCT можно также объединить с Bulletproofs [Bue17] (который уже является частью кодовой базы Particl и Ghost), чтобы доказать, что входные и выходные данные транзакций попадают в допустимый диапазон (то есть не происходит отрицательных выходных сумм или перерасходов).

Particl

Полученный из биткоина

Particl, как и многие другие, начинал как форк биткоина. Его идея направлена на добавление новых технологий на вершине успеха, которого биткоин уже достиг. Прежде всего, добавляя конфиденциальность каждому аспекту цепочки и внедряя доказательство заинтересованности, чтобы отойти от механизма консенсуса по проверке работы Proof of Work для создания блоков.

Через разветвление исходного кода новые проекты могут сосредоточиться на постоянных обновлениях и улучшениях сети, поскольку уже существует надежная архитектура. Используя существующую основу, на которую можно опираться, проекты часто могут в основном сосредоточить свои усилия на конкретной целевой точке. Как и Ghost, в конкретном случае цель этого проекта - конфиденциальность.

Децентрализованный рынок

Блокчейн от Particl предлагает децентрализованный, анонимный и частный рынок для покупки и продажи товаров между пользователями в сети. Любой пользователь их блокчейна может публично выставить список товаров или услуг для продажи, и их список может быть куплен так, чтобы никто в цепочке не знал, кто на самом деле купил или продал его.

Кроме того, этот открытый рынок предлагает *TOR-соединение*, которое позволяет покупателю и продавцу подключаться к цепочке с IP-адреса TOR, что означает, что их исходный IP-адрес маскируется во время транзакции. Платежи также обрабатываются с использованием технологий CT и *RingCT*, которые обсуждались ранее. Это означает, что продавец и покупатель могут анонимно отправлять и получать средства на скрытый адрес без какого-либо способа отслеживания конечных пользователей.

Несмотря на то, что сам список может быть обнародован, что делает его доступным для поиска и категоризации на внешнем рынке, исходный IP-адрес и пользовательские данные не предоставляются. Единственным идентификатором является идентификатор анонимного поставщика, который никак не связан с пользователем.

Проект стремится обеспечить полную конфиденциальность при заключении сделок, и его рынок выполняет это обещание. Это полностью анонимная квази-пиринговая система, работающая исключительно в собственной сети.

Зашифрованный чат

Их сетевой демон также поддерживает протокол защищенных сообщений, называемый *SecureMessaging*. Эта система полностью построена на C++ и работает в существующей сетевой инфраструктуре[16]. В широком смысле, когда пользователь отправляет зашифрованное сообщение, это сообщение защищено хешем, который сообщает узлам в сети, какой узел имеет право дешифровать сообщение. Это сообщение затем транслируется и шифруется по всей сети, и каждый узел попытается расшифровать сообщение. Если они являются назначенным узлом, они будут успешными, и сообщение будет отправлено пользователю для просмотра.

Их процесс хеширования использует метод, называемый HMAC[17]. Пакет чата будет иметь добавленный компонент, хеш, который состоит из идентификатора DSN (сети хранения данных) принимающего узла или публичного ключа этого узла. Когда сообщение передается по сети, каждый узел будет пытаться стереть этот хеш. Однако, если они этого не делают, то сообщение либо является фальшивым, либо неверным, либо не предназначено для них, и они ничего не сделают, кроме как сохранят это сообщение в течение 48 часов.

[16] https://github.com/particl/particl-core/tree/master/src/smsg

[17] HMAC, или Коды аутентификации сообщений на основе хэширования, - это криптографический инструмент для проверки подлинности и целостности данных сообщения. Он объединяет ключ и функцию хеширования таким образом, что, если у верификатора есть ключ, они могут проверить, что никто не вмешивался в сообщение, кроме тех, кто имеет этот ключ.

Этот процесс объясняется более подробно в разделе о рынке данного документа, поскольку функция SSMS также используется в качестве поставщика DSN для рынка.

Почему Particl?

Когда Ghost был изначально запущен, команда разработчиков единодушно приняла решение раскрутить базу кода из этого проекта с открытым исходным кодом [18] . В дополнение к своей первоначальной раздаче биткойнов они расширили функциональность своей сети[19] в направлении, которое аналогично совмещало их цели с теми, которые имеет призрак.

[18] https://github.com/particl
[19] https://github.com/particl/particl-core

Ghost

Enhanced Privacy

В настоящее время Ghost использует RingCT и скрытые адреса в качестве средств обеспечения конфиденциальности пользователей и сохранения их анонимности при совершении сделок в сети. Тем не менее, проект стремится оставаться на вершине технологии конфиденциальности, в дополнение к проведению исследований в области лучшей анонимности с меньшими затратами и вычислениями для предотвращения DDoS-атак («отказ в обслуживании» - прим. перев.).

Одна из технологий, которые в настоящее время исследуются для реализации в инфраструктуре Ghost, - это круговые подписи Триптиха [Noe20], которые увеличивают пространственную сложность круговых подписей с O (1) до O (log (N)). Это уменьшает объем дискового пространства, необходимого для значительного хранения круговых подписей, позволяя храниться сотням ложных сигналов в круговых подписях вместо нескольких десятков при той же цене.

Больше конфиденциальности - Dandelion++

Dandelion++ - это простое и понятное решение сетевого уровня с формально гарантированной анонимностью [Fan18], которое может быть внедрено в существующие криптовалюты.

Обычно криптовалютные транзакции транслируются по сети с использованием протокола Gossip, в котором каждый узел отправляет транзакцию всем узлам, к которым он подключен. В то время как текущая система эффективна, также возможно деанонимизировать исходного отправителя транзакции [Fan18]. Dandelion++ вносит простые, но важные изменения в текущую модель трансляции транзакций.

Вместо отправки транзакций на все подключенные узлы в сети, Dandelion++ первоначально отправляет их только на один другой узел. Затем этот следующий узел случайным образом решает, будет ли он транслировать транзакцию только

одному или всем своим подключенным узлам. С введением элемента случайности шаблон распространения теперь становится непредсказуемым, что делает невозможным отслеживание конкретной транзакции до исходного IP-адреса вещателя. Это особенно полезно в криптовалюте Ghost, ориентированной на конфиденциальность, чтобы предотвратить отслеживание вашей транзакции на ваш IP-адрес, что в конечном итоге приведет к деанонимизации приблизительного местоположения отправителя на основе его IP-адреса.

Мастерноды (Ветераны Ghost)

После долгих раздумий Ghost решил не внедрять мастерноды. Проект считает, что отсутствие каких-либо существенных улучшений функциональности сети в сочетании с присущими ей недостатками просто не соответствует стандартам, которые группа имеет для проекта. К ним относятся:

- Мастерноды DIP3 и их зависимости не требуются для достижения каких-либо целей, которые мы ставим перед проектом.
- Сложно настроить для большинства новых пользователей, которые не имеют предварительных знаний о системе Protx.
- Потенциальная нестабильность сети и безопасности.

Тем не менее, Ghost не регулирует структуру вознаграждения, которая была в первоначальном плане. Вместо этого будет выпущена новая инициатива, которая заменит ее – «Ветераны Ghost». Упоминания мастернод на веб-сайте[20] теперь будут ссылаться на эту программу.

Ветераны Ghost будут состоять из отдельного пула GHOSTS, которые накапливались для каждого блока в течение 30 дней. Чтобы иметь право на получение этих наград, пользователь должен соответствовать следующим требованиям в течение 30-дневного периода наград:

1) Выполнить публичную транзакцию не менее 20.000 GHOST для проверки баланса.

[20] https://www.ghostbymcafee.com/

2) Средства не должны быть потрачены или перемещены в течение этого времени[21].

Для адресов, кратных 20000 GHOST, где выполнены вышеуказанные требования, награда будет соответственно увеличена. Например, пользователь с 40000 GHOST получит в два раза больше, чем тот, у кого 20000 GHOST.

Пользователям также будет разрешено одновременно ставить свои монеты на стейкинг, зарабатывая GHOST каждый раз, когда они успешно создают блок (то есть, стейкинг не лишит вас возможности получать награды ветеранов Ghost).

Приняв эту структуру вознаграждения, ветеранам Ghost не нужно будет проходить сложный процесс установки и запуска полного узла, как это было бы в противном случае. Они также будут свободны от необходимости постоянно держать свой кошелек открытым или выполнять какие-либо передовые технические требования.

Структура вознаграждений

GHOST использует инфляционную структуру вознаграждения, обычно наблюдаемую в сетях PoS. Каждые 120 секунд (2 минуты) в сети создается новый блок, таким образом чеканя 12 монет GHOST (6 GHOST в минуту), которые в конечном итоге присоединяются к общему обороту в соответствии с данной структурой вознаграждений:

6 GHOST выделены в фонд вознаграждений ветеранов.

4 GHOST отправляется на стейкинг-адрес, который создает блок.

2 GHOST распределяются в фонд разработки для будущего развития.

** Эта структура может быть изменена с согласия сообщества и, вероятно, уменьшится, когда сеть достигнет зрелости.*

[21] Исключением из этого правила является стейкинг. Несмотря на то, что распределение считается видом затратных результатов, результаты, которые ставятся на стейкинг, все еще учитываются в вознаграждении для ветеранов Ghost. Единственное другое исключение - 1 публичная транзакция, необходимая для проверки средств на счете.

После первых двух лет, уровень эмиссии выше будет снижаться каждый год примерно на 5%. Уравнение, которое регулирует уровень инфляции каждый год:

$$12\frac{\text{round}\left(100 \times 0.95^{n}\right)}{100}$$

Уровень эмиссии останется на уровне 100% (т.е. 12 GHOST) в течение первых двух лет (6 для ветеранов Ghost, 4 для стейкеров, 2 для фонда разработчиков). Затем он начнёт падать, пока не достигнет 10%. Когда будет достигнут уровень 10% (через 45 лет в будущем), оно никогда больше не уменьшится. Это даст заинтересованным сторонам стимул продолжать хранить монету для стейкинга.

Фонд разработчиков распространяется на администраторов и основных разработчиков GHOST и будет в основном использоваться для финансирования проектов сообщества, а также новых функций.

Выплата вознаграждения происходит автоматически при правильной высоте блока за установленный период без вмешательства пользователя. С помощью этого метода у обычного пользователя есть несколько возможностей участвовать в сети и зарабатывать GHOST.

Квантовое сопротивление

Криптография с открытым ключом, вид криптографии, который использует биткоин, может быть относительно легко взломана с помощью квантовых компьютеров[22] с использованием алгоритма Шора, что невозможно сделать на классических компьютерах [23] и является основой безопасности биткоинов и многих других криптовалют. Квантовые компьютеры могли бы восстановить

[22] Квантовый компьютер - это компьютер, который не использует обычное двоичное состояние «бит» или {0,1} для выполнения основных логических и арифметических операций, но использует квантовые состояния {0,1}, которые называются кубитами. Кубиты могут одновременно находиться в нескольких состояниях (технически это называется суперпозицией состояний). Кубит может быть 0 и 1 одновременно с вероятностью, связанной с каждым состоянием (например, 30% «0» и 70% «1»). Это приводит к очень интересным результатам и новым алгоритмам, которые масштабируются намного лучше, чем классические компьютеры, которые мы используем в настоящее время.

[23] Классические компьютеры - это компьютеры, которые мы используем в настоящее время. Термины классика против кванта происходят из физики, где физика Ньютона сравнивается с квантовой физикой.

секретный ключ из публичного ключа относительно быстро[24]. К счастью, квантовые компьютеры еще не существуют, но им суждено появиться и стать более популярными в будущем. В то время как компании обещают «квантовые чипы» в ближайшем будущем [IBM17], скептики все еще верят, что квантовые компьютеры не появятся в наши жизни [Dya18]. В этой атмосфере криптовалюты должны готовиться к этой «квантовой угрозе».

Фактически, для вновь созданных закрытых ключей, которые никогда не тратили какие-либо выходные данные, использующие связанные адреса, биткоин уже безопасен для квантовых вычислений. Адреса биткоина генерируются из открытых ключей. Эти адреса рассчитываются путем хеширования открытого ключа. Квантовые компьютеры не могут разбивать хэши по сравнению с классическими компьютерами[25]. Однако, если что-то будет потрачено с этого адреса, открытый ключ будет раскрыт в общедоступной цепочке блоков. При наличии квантовых компьютеров это станет угрозой.

В Ghost используется та же адресная инфраструктура биткоина. Чтобы решить проблему квантовой угрозы, пользователям рекомендуется использовать адреса только один раз. Однако, как правило, это невозможно при использовании стейкинга, так как для них требуется раскрытие открытого ключа. Следовательно, с помощью холодного стейкинга эта проблема решается, поскольку вам не нужно раскрывать свой закрытый ключ, поскольку делегат раскрывает только свой открытый ключ, и, следовательно, он является квантово-защищенным.

Адреса-псевдонимы

Еще одна особенность блокчейна Ghost - возможность отправлять средства по зарезервированному псевдониму, который соответствует скрытому адресу. Проект мотивирован на реализацию этого, чтобы обеспечить удобство и конфиденциальность для всех, кто участвует в экосистеме. Хотя эта функция не является особенно новой, поскольку она была реализована с помощью сервисов, предоставляющих информацию DNS для криптовалют, Ghost считает, что такой

---

[24] Теоретически, можно вычислить закрытый ключ из открытого ключа в классических компьютерах, но даже с суперкомпьютером, на самом деле, это займет пару миллионов или даже миллиардов лет.

[25] На самом деле квантовые компьютеры намного быстрее, чем классические компьютеры, разбивают хеш-коды, однако этого недостаточно. Используя квантовый алгоритм, названный алгоритмом Гровера, поиск может быть выполнен с временной сложностью O (sqrt (N)), где sqrt является квадратным корнем, по сравнению с классическими компьютерами, которым требуется O (N) сложность поиска. Другими словами, при условии, что все равны, квадратный корень потребует времени, чтобы взломать хэш в квантовом компьютере, но этого недостаточно, чтобы быть угрозой.

сервис централизует криптовалюты. Нашим решением этой проблемы будут псевдонимы, определенные в децентрализованной сети. Это не зависит от каких-либо третьих сторон и, следовательно, будет децентрализовано на 100%.

Одной из серьезных проблем псевдонимов является возможность связывать имена с адресами и, следовательно, с суммами. Если кто-то решит использовать свое имя и фамилию в качестве псевдонима или если везде используется одно и то же, его баланс может стать общедоступным. Таким образом, эти проблемы противоречат самим принципам Ghost, где конфиденциальность наших пользователей имеет первостепенное значение.

Чтобы решить эти проблемы, Ghost будет разрешать псевдонимы адресов только с помощью скрытых адресов, чтобы обрабатывать ссылки. Учитывая, что скрытые адреса генерируют новый эффективный адрес при каждой транзакции, невозможно связать или отследить баланс любого пользователя по его псевдониму.

Чтобы встроить адрес против псевдонима в цепочку блоков, мы будем использовать тип вывода OP_RETURN. Когда должен быть создан новый псевдоним, должна быть создана новая транзакция с OP_RETURNoutput. Этот вывод будет содержать следующие данные

Объём	Тип	Данные
1 или более	Целое число переменной длины	Номер версии протокола в формате с прямым порядком битов
1 или более	Целое число переменной длины	Функция или идентификатор хранилища, цель которого функция в формате с прямым порядком битов
2	Целое число	Размер строки псевдонима
Переменный	Двоичные данные	Двоичные данные, которые представляют псевдоним
2	Целое число	Размер строки адреса
Переменный	Двоичные данные	Адрес, на который указывает псевдоним

Это пример протокола, который будет использоваться для добавления дополнительных децентрализованных функций в Ghost, что является частью консенсуса.

При создании транзакции, которая использует это, сам протокол будет отвечать за проверку того, был ли взят псевдоним. Владелец закрытого ключа ввода также может выполнить этот запрос.

Чтобы предотвратить спам, резервирование большого количества псевдонимов обойдется примерно в 5 долларов США за транзакцию, которые на момент написания будут установлены в 5 GHOST. Эта сумма может быть изменена, чтобы оставаться доступной. Собранные сборы будут сожжены и больше не будут частью сети.

Как это работает? При сканировании блокчейна программное обеспечение узла GHOST будет считывать транзакции, которые следуют формату из таблицы выше. Когда такая транзакция обнаружена, программное обеспечение узла сохраняет псевдоним, адрес и транзакцию, которая создала псевдоним, в хранилище значения ключа[26].

Когда необходимо создать транзакцию для отправки средств на этот псевдоним, запрашивается хранилище значения ключа, чтобы проверить, используется ли псевдоним. Затем программное обеспечение кошелька проверит, находится ли эта транзакция в основной цепочке. Кроме того, это обеспечит синхронизацию цепочки, чтобы перезаписанные адреса не использовались. Затем адрес назначения псевдонима будет использоваться для создания транзакции. Пользователь не заметит ни одной из этих деталей, и ему будет казаться, что псевдоним является истинным адресом.

Движимый сообществом

Одним из основных принципов проекта Ghost является прозрачность в конфиденциальности. Это означает, что мы стремимся быть полностью прозрачными для общественности в том, что мы делаем и почему, не нарушая конфиденциальность пользователей на платформе. Наше развитие как сообщества - это один из способов, которым мы надеемся достичь этого.

---

[26] В настоящее время leveldb используется в качестве хранилища значений ключей для GHOST, но это может измениться в будущем.

Владельцы GHOST будут иметь возможность проголосовать за будущие события и изменения дорожной карты, в то время как финансирование реализации этих новых инициатив будет производиться через фонд развития. Ghost надеется продвинуть проект за счет участия сообщества, создав продукт, который соответствует потребностям пользователей, сохраняя при этом желаемый высокий уровень безопасности, конфиденциальности и функциональности.

Голосование будет простым, пользователь сможет заплатить небольшую сумму GHOST, чтобы предложить тему для рассмотрения. Это может быть любая новая функция, которая, по их мнению, могла бы принести пользу платформе. Оттуда любой пользователь может проголосовать через одну из существующих платформ. Их голос будет взвешен в зависимости от количества GHOST, которое они имеют.

Если голосование соответствует минимальному порогу, оно считается утвержденным. Следовательно, он направляется команде для выделения средств из вознаграждений разработчиков и, в конечном итоге, для создания вознаграждения за задачи, связанные с этим проектом. Все участники сообщества имеют право на получение награды, включая основных членов Ghost. Это означает, что любой может начать работу на платформе с открытым исходным кодом, решить проблему или создать новую функцию и получить оплату непосредственно в токенах GHOST за свою работу. Публичные участники представят PR для одобрения основной командой так же, как если бы это сделал основной член команды.

Весь этот процесс помогает создать совершенно новую перспективу для разработки блокчейна и крипто-пространства в целом. Пользователи, имеющие право голоса в том, как продвигается проект, обеспечивают уровень прозрачности и направления, что редко встречается в этом пространстве.

Расширение зашифрованного чата для мобильного приложения «Telaghost»

Децентрализованная частная сеть, которая может общаться анонимно, должна использоваться для гораздо большего, чем просто отправка числовых значений туда и обратно. Движущим фактором в миссии Ghost является обеспечение значительной стоимости уникальных внешних продуктов и услуг. Сеть может быть столь же ценной, как и предоставляемая ею утилита.

Цель состоит не в том, чтобы просто создать новое приложение для чата и заставить пользователей перейти на другую платформу, потерять все свои сообщения и контакты. Это не практично и станет серьезным препятствием для принятия. Именно поэтому в рамках проекта планируется полная интеграция с сетью Telegram[27] в виде гибридного решения. Это позволит пользователю войти в систему с использованием существующей учетной записи, иметь доступ к тем же контактам, тем же группам и настройкам. Ghost предоставит дополнительные функции поверх своей платформы[28], что позволит пользователям приложения получать доступ к приватному чату, отправлять/получать GHOST, запускать частные группы, а также сообщать о дополнительных функциях. Это приложение будет для iOS, Android, а также настольных версий для ПК, MacOS и Linux.

Планы на будущее и конкретные детали для зашифрованного мобильного приложения «Telaghost» будут опубликованы в отдельном документе в ближайшее время. Это приоритетный пункт в дорожной карте.

Расширение Google Chrome и Firefox Wallet, «MetaGhost»

Как и при любом запуске новой сети, одной из основных проблем является адаптация. Пользователи привыкли к существующим решениям из-за знакомства, простоты использования и удобства. Это снижает вероятность того, что пользователь примет новый кошелек, например.

Призрак мог потратить больше года на создание чего-то нового и еще один год, пытаясь заставить людей использовать это. Тем не менее, проект решил, что предпочтительной альтернативой будет создание существующего популярного

---

[27] https://telegram.org/

[28] https://core.telegram.org/tdlib

решения. MetaMask[29] - это проект с открытым исходным кодом[30], широко используемый различными онлайн-сервисами [Yah19]. Это расширение для браузера, которое позволяет запускать dApps [Cho18], не будучи частью сети Ethereum как узел Ethereum. Это создало множество случаев, когда пользователи могли напрямую взаимодействовать с веб-сайтами для отправки и получения токенов Ethereum и ERC-20[31].

Цель проекта - использовать ту же функциональность, которая уже существует в MetaMask и сети Ethereum, а также добавить дополнительную поддержку для подключения к основной сети Ghost. Это обеспечит пользователям то же удобство и простоту использования, с которыми они знакомы, при этом добавляя дополнительный уровень конфиденциальности, который можно использовать по мере необходимости. В будущем планируется использовать в сети обернутый токен GHOST на основе Ethereum в сочетании с «атомными свопами» (мгновенным обменом на блокчейне – прим. перев.), что позволит беспрепятственно интегрироваться во многие функции веб-сайтов, совместимых с MetaMask, и при этом использовать преимущества конфиденциальности сети Ghost. Кроме того, это также позволит Ghost стать частью DeFi[32].

Вкратце, пользователи смогут напрямую тратить свои монеты GHOST (в основной сети) через совместимые с MetaMask веб-сайты (используя обернутый токен ERC-20 Ghost), оставаясь анонимными в «MetaGhost».

Будущие разработки

Направление Ghost должно постоянно меняться, чтобы успешно адаптироваться на стремительно развивающемся рынке, где новые проблемы и препятствия появляются быстро и требуют внимания таким же образом.

---

[29] https://metamask.io/

[30] https://github.com/MetaMask

[31] ERC-20 is a protocol on the Ethereum blockchain that allows for creating tokens for assets.

[32] DeFi, или децентрализованные финансы, - это набор протоколов в блокчейне Ethereum, которые заменяют традиционные финансы, где можно управлять такими организациями, как центральные банки, предоставлять кредиты, короткие, длинные и многие другие финансовые услуги; все на блокчейне.

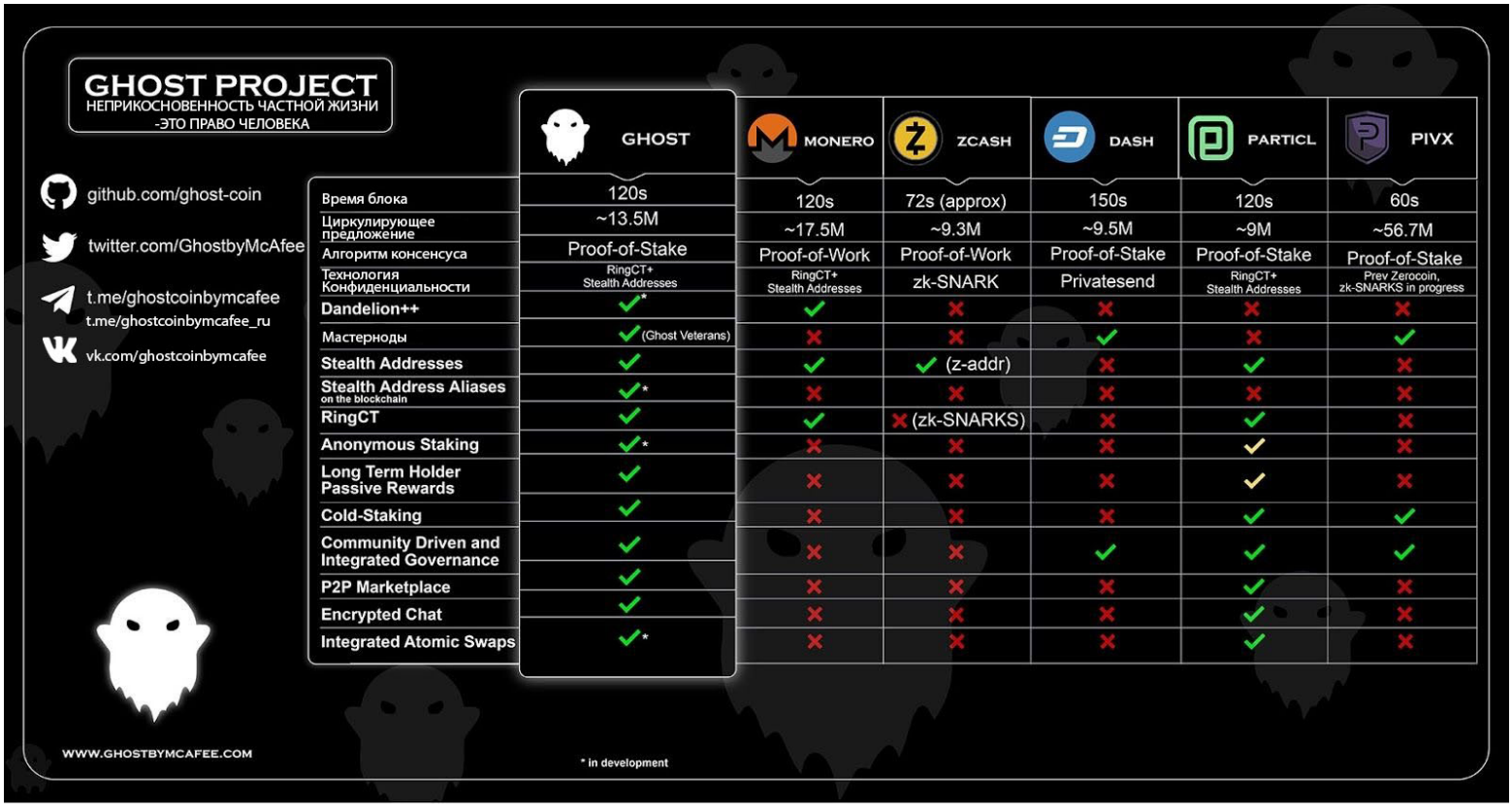
Технический документ и особенности, которые мы обрисовали в общих чертах, являются только началом для Ghost. Для того, чтобы по-настоящему воплотить концепцию и сохранить стабильное и безопасное решение, держателям монет GHOST необходимо предложить средства, которые будут расширены. В совокупности именно они должны вносить изменения, в противовес единому решающему органу.

Эта идеология считается одной из важных частей, которая действительно делает этот проект уникальным. Ghost обязуется выделить большую часть пула фонда разработчиков для финансирования утвержденных сообществом предложений и разрешить сообществу одобрить или отклонить эти изменения.

В конечном счете, в будущем Ghost хочет продолжить расширение собственной экосистемы продуктов и услуг, одновременно преодолевая разрыв между существующими платформами.

Схема сравнения

Ниже мы сравниваем Ghost наряду с другими криптовалютами с соответствующими функциями, которые обсуждались до сих пор:



* *Версия в полном разрешении доступна по ссылке:*
https://www.ghostbymcafee.com/assets/ghost-project-chart.jpg

Технические характеристики Ghost

Далее мы расскажем о рабочих характеристиках криптовалюты Ghost

- Время блока: 2 минуты
- Максимальный размер блока: 8 МБ
- Механизм консенсуса: подтверждение участия
- Холодный стейкинг: поддерживается
- Атомные свопы: будут поддерживаться в будущем
- Уровень эмиссии: 12 GHOST за блок за первый год; затем, следуя уравнению, где n - номер года, рассчитанный в блоках::

$$12\frac{\text{round}\left(100\times 0.95^{n}\right)}{100}$$

Эта ставка будет снижаться до 10% от 6 GHOST. Как только это будет достигнуто, награда за блок навсегда останется 0,6 GHOST.

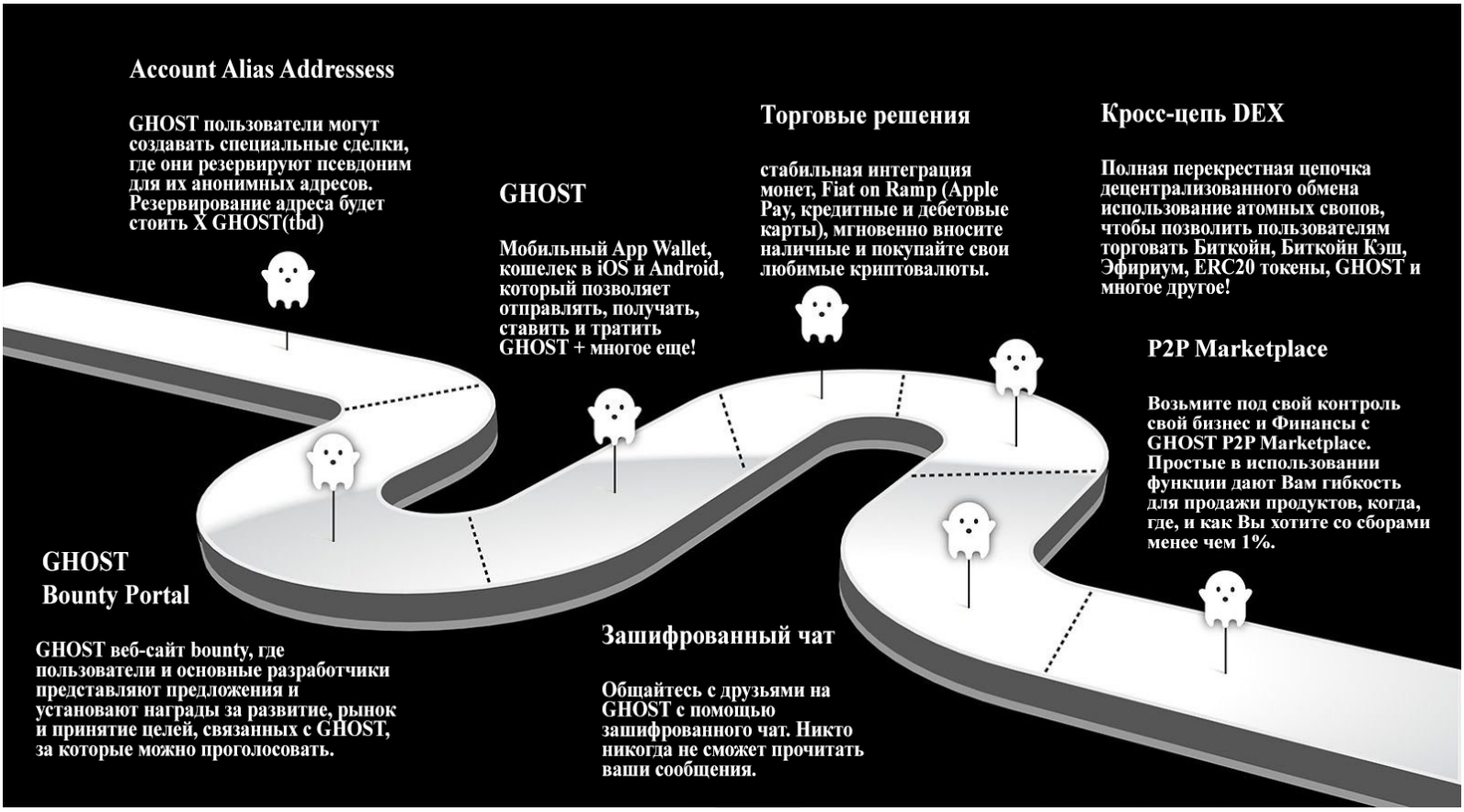
- Награды, из вышеупомянутого:
  - 50% за холодную награду (Призрачные ветераны)
  - 33% для стейкеров
  - 17% для фонда разработки
- Срок погашения: 225 подтверждений
- Конфиденциальность: существуют как анонимные (с использованием RingCT и скрытые адреса), так и неанонимные транзакции[33]. ● Поддержка аппаратного кошелька: несколько, которые будут поддерживаться в ближайшем будущем.

[33] В будущем мы полностью откажемся от неанонимных транзакций. Они существуют сейчас для оперативной необходимости, чтобы позволить работать протоколу Proof of Stake.

Команда и участники

Джон Макафи	**основатель**
Технический пионер, программист и эксперт по безопасности. Основатель антивируса McAfee и конфиденциальной анонимной монеты GHOST.	
reborn1002 Разработчик проект-менеджер	Разработчик с 10-летним опытом работы C++, C #. Внесенный в список проектов компании Fortune 100.
TheQuantumPhysicist Старший разработчик	Кандидат физико-математических наук. Участник Bitcoin & Monero и разработчик блокчейна. Эксперт в области компьютерной безопасности с акцентом на криптовалюту.
Akshay CM Разработчик ядра	Участник PIVX, ZCoin & Qtum. Опытный разработчик C++, который хорошо разбирается в области криптовалюты.
Kaddar Разработчик ядра	Сетевой инженер и разработчик со степенью CS. Знание C ++, JS, Solidity и глубокое понимание блокчейн
Luna Программист	Разработчик Solidity. Инженерный менеджер крупного финансового провайдера.
Joao Программист	Соавтор Switch и DEX. Опыт работы в Angular, PHP / HTML / JS. Разработчик Ghost Wallet.
melvin Веб-программист	Соавтор Switch и DEX. Опыт работы в Angular, PHP / HTML / JS. Разработчик Ghost Wallet.
Luis Сообщество	Сообщество, цифровой маркетинг
Geo Бизнес-стратег	Развитие бизнеса, принятие пользователей, обмен отношениями и маркетинг.

Будущая дорожная карта



* *Версия в полном разрешении доступна по ссылке:*

https://www.ghostbymcafee.com/pdfs/GHOST2020_Roadmap_v1.0.2.jpg

Благодарности

Этот документ был подготовлен в сотрудничестве Ghost Team.

Мы особенно хотели бы поблагодарить Particl и их талантливую команду разработчиков. С точки зрения конфиденциальности, их консенсусного алгоритма, обновленной базового кода биткоин, чистого кода и уже существующих функций, решение о форке было довольно простым.

Наконец, мы хотели бы поблагодарить наше сообщество, которое поддержало нас с самого раннего этапа. Мы с нетерпением ждем продолжения совместной работы над нашим общим видением Ghost.

Ссылки

[Nak08] Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System.*
[Min15] Minichiello, N. (2015) *The Bitcoin Big Bang: Tracking Tainted Bitcoins, BraveNewCoin, 21st June.* Available at:
https://bravenewcoin.com/insights/the-bitcoin-big-bang-tracking-tainted-bitcoins

[Red20] Redman, J. (2020) *Industry Execs Claim Freshly Minted 'Virgin Bitcoins' Fetch 20% Premium,March.*Available at:
https://news.bitcoin.com/industry-execs-freshly-minted-virgin-bitcoins/

[Eli18] Jeff (2018) *Bitcoin Costs Throughout the World, Elite Fixtures, February.* Available at:
https://www.elitefixtures.com/blog/post/2683/bitcoin-mining-costs-by-country/?mod=article_inl ine

[Ran19] Github (2020) *The github repository for RandomX.*Available at:
https://github.com/tevador/RandomX

[Cry19] Moos, M (2019) *Bitcoin Mining Centralization Reaches Record Levels, Majority China, Crypto Briefing,* Dec 12th,Available at:
:https://cryptobriefing.com/bitcoin-mining-centralization-record-levels-majority-china/
[Btg51] Iskra, E (2018). *Responding to attacks, Bitcoingold, 24th May.* Available at:
(https://bitcoingold.org/responding-to-attacks/
[Coi19] Nesbitt, M (2019). *Deep Chain Reorganization Detected on Ethereum Classic*(ETC), *Coinbase, Jan 7th.*Available at:
https://blog.coinbase.com/ethereum-classic-etc-is-currently-being-51-attacked-33be13ce32de
[Bie18] BitcoinExchange Guide News Team (2018), *List of PoW 51% Attack Costs for Each Cryptocurrency, BitcoinExchange, May 28th. Available at:*
https://bitcoinexchangeguide.com/list-of-pow-51-proof-of-work-mining-attack-costs-for-each-cryptocurrency/
[Pow51] Crypto 51 (2020) *PoW 51% Attack Cost, Crypto51, June 9th.*Available at:
https://www.crypto51.app/
[Ioh18] Gaži P. (2018) *Stake-Bleeding Attacks on Proof-of-Stake Blockchains, IOHK, June.* Available at:
https://iohk.io/en/research/library/papers/stake-bleeding-attacks-on-proof-of-stake-blockchains/
[Van12] Van Saberhagen, N. (2012) *The Cryptonote Protocol,December 12th.*Available at
https://cryptonote.org/whitepaper_v1.pdf

[Max15] Maxwell, G. et al (2015) *Borromean Ring Signatures, June 2nd.* Available at:
https://pdfs.semanticscholar.org/4160/470c7f6cf05ffc81a98e8fd67fb0c84836ea.pdf

[Noe16] Noether, S. et al (2016) *Ring Confidential Transactions, Monero Research Labs, February.* Available at:
https://web.getmonero.org/resources/research-lab/pubs/MRL-0005.pdf

[Bue17] Buenz, B. et al (2017) *Bulletproofs: Short Proofs for Confidential Transactions and More, Stanford University.* Available at:
https://eprint.iacr.org/2017/1066.pdf

[Noe20] Noether, S. (2020) *Triptych: Logarithmic-Sized Linkable Ring Signatures With Applications, Monero Research Labs, May 18th.* Available at:
https://eprint.iacr.org/2020/018

[Gua17] Reuters in Kiev (2017) *Ukraine Kidnappers Release Hostage After $1m bitcoin Ransom Paid, The Guardian, December 29th*.Available at: https://www.theguardian.com/uk-news/2017/dec/29/ukraine-kidnappers-release-hostage-after-1 m-bitcoin-ransom-paid

[IBM17] Anthony, S (2017) *IBM Will Sell 50-qubit Universal Quantum Computer "In The Next Few Years", ArsTechnica, June 3rd.* Available at: https://arstechnica.com/gadgets/2017/03/ibm-q-50-qubit-quantum-computer/

[Dya18] Dyakonov M. (2018) *The Case Against Quantum Computing, Spectrum, November 15th.* Available at: https://spectrum.ieee.org/computing/hardware/the-case-against-quantum-computing

[Yah19] Dantoni, J (2019) *MetaMask Releases Metrics That Show How It's Being Used, Yahoo Finance, May 25th.* Available at: https://finance.yahoo.com/news/metamask-releases-metrics-show-being-224953895.html

[Cho18] Choi, S (2018) *What is MetaMask? Really...What is it?, Medium, July 18th.* https://medium.com/@seanschoi/what-is-metamask-really-what-is-it-7bc1bf48c75

[Fan18] Fanti et al. (2018) *Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees,ACM, June. Available at:* https://dl.acm.org/doi/10.1145/3224424

Примечание: все ссылки были посещены, и содержание проверено после выпуска этого документа