Notes to this translation:
1) We use a different numerical formatting in Russia. Decimal separator is a comma. For example, one and a half is 1,5 instead of 1.5 in English.
Rank separator is a point (dot). Example: 1.000.000 – one million

2) Spelling of the word Bitcoin.
There are two possible ways to spell it: биткоин and биткойн. I use the first variant.
It's based on the State Russian Encyclopedia spelling:
https://bigenc.ru/economics/text/4934993
There is ongoing discussion on Wikipedia about the correct spelling of the word Bitcoin in Russian language.
The point is - it's doesn't matter which spelling I choose – but there will be people who will say it's wrong anyway.

3) Section 12. References should go unmodified since all the sources in this section are non-Russian.

Bitcoin Private
Белая книга

Революция в конфиденциальности
Претворяя в жизнь видение Сатоши Накомото

Февраль 2018

Авторы:

Сообщество Bitcoin Private
Дкт. Наук Джекоб Брутман (Jacob Brutman)
Джон Лайтон (Jon Layton)
Кристофер Сулмон (Christopher Sulmone)
Джузеппе Стуто (Giuseppe Stuto)
Джеф Хопкинс (Geoff Hopkins)
Рет Крейгтон (Rhett Creighton)

WWW.BTCPRIVATE.ORG

Аннотация

Изобретение интернета ознаменовало собой появление единого информационного пространства в масштабе всей планеты. Это привнесло неоспоримые преимущества для обмена и доступа к любой информации. Однако в тоже время это привело к тому, что конфиденциальность пользователей оказалась под угрозой. И очень часто это происходит не по вине самого пользователя, а по причине того, что сервисы, используемые им в сети, могут быть взломаны и частная информация может попасть в руки третьих лиц. Все это привело к потребности в создании системы, в которой нет необходимости в посреднике между двумя пользователями. Применительно к денежным переводам в сети интернет это стало возможным благодаря появлению новой криптовалюты Bitcoin Private. Bitcoin Private предоставляет возможность осуществлять переводы между пользователями, которые нельзя отследить или подвергнуть цензуре. В то же время эти переводы имеют низкую комиссию и достаточно быстрое время подтверждения. Тем самым Bitcoin Private является реализацией видения будущего крипровалют, как их представлял и описывал Сатоси Накомото - создатель Биткоина. Bitcoin Private появился в результате объединения блокчейна биткона и Zclassic. Новый блокчейн позволяет осуществлять переводы с комиссией, которая значительна ниже, чем в сети биткоин, а скорость подтверждения быстрее от 4 до 6 раз. Но самое важное то, что в Bitcoin Private реализован научно-обоснованный криптопротокол zk-SNARK, который был изначально применен Zcash Foundation. Этот протокол позволяет осуществлять анонимные и конфиденциальные денежные переводы - достижение, которым не может похвастаться ни одна другая реализация технологий анонимных платежей. Непогашенные выходы транзакций (UTXO) биткоина и Zclassic будут объединены вместе, тем самым составив первоначальную денежную массу новой криптовалюты. Это значит, что примерно 20,4 миллиона монет из максимально возможных 21 миллиона будет доступно в момент запуска сети, что делает Bitcoin Private криптовалютой с самой низкой инфляцией среди других криптовалют. Эта “белая книга” описывает технические преимущества Bitcoin Private, его коммерческие применения, а также потенциал дальнейшего развития.

Содержание

1. Введение.

В течение всей письменной истории человечества, обмен информацией между людьми был конфиденциальным и анонимным. Информация, которая была частью взаимодействия между людьми, была доступна только отправителю и получателю. Однако в последнее время денежные транзакции проводятся посредством и с применением новых технологий, что ведёт к всёвозрастающей сложности обеспечения конфиденциальности таких транзакций. При использовании самых распространённых современных методов оплаты, таких как кредитные карты, ApplePay и т.д., вся информация о транзакции сохраняется в цифровой форме. Такие методы проведения транзакций несут в себе значительные плюсы, но в тоже время они не должны осуществлять это за счет потери конфиденциальности конечным пользователем. Принимая во внимание, как часто происходят утечки пользовательских данных из финансовых институтов, становится ясно, что требуется определённое решение для осуществления конфиденциальных транзакций.[1,2] Более того, имеются факты, что финансовые организации продавали данные пользователей третьим лицам.[3] В других же случаях они осуществляли блокировку транзакций без каких-либо оснований для этого.[4]

В октябре 2008 года Сатоси Накомото опубликовал научную статью, озаглавленную “Биткоин: децентрализованная электронная денежная система”, в которой он описал основу первой криптовалюты.[5] По мнению Сатоси, криптовалюта должна была обладать следующими свойствами: отсутствием контроля со стороны третьих лиц при проведении транзакций, ограниченной инфляцией и финансовой свободой пользователей через анонимность транзакций. С момента запуска сети биткоин в 2009 году, было создано более 1000 различных криптовалют, также был достигнут значительный прогресс в блокчейн технологиях в целом.[6] В самом деле многие новые криптовалюты опережают биткоин, как по скорости транзакций, так и имеют более низкие комиссии за транзакции. Тем не менее, биткоин остаётся самой популярной криптовалютой, поскольку он является первопроходцем в мире криптовалют, также большинство торговли криптовалютами осуществляется относительно биткоина.

Вместе с ростом популярности биткоина, стали выявляться и проблемы, такие как: постоянный, маленький размер блока, который является причиной высоких комиссий при проведении транзакций; долгий период подтверждения транзакций (в среднем 10 минут); двух недельный период коррекции сложности майнинга; а также разработка специализированных интегральных микросхем для майнинга, что привело к дальнейшей централизации сети. Для того чтобы исправить эти проблемы, требуется чтобы по крайней мере 50% майнеров выразили согласие с предлагаемыми способами решения вышеуказанных проблем. Однако за всю историю биткоина такие изменения ни разу не случались. Это привело к разделению сети биткоина на основании предложенных новых правил для протокола сети, так называемый процесс хард форка. Bitcoin Cash и Bitcoin Gold являются примерами таких хард форков. Данные хард форки вносят улучшения в протокол, для примера Bitcoin Cash увеличил размер блока в сети до 8 Мб против 1 Мб в оригинальном биткоине, что привело к снижению комиссий за транзакции и увеличило общую пропускную способность сети. Однако эти изменения имели и негативную сторону, значительное увеличение размера блока привело к тому, что перестал работать рыночный механизм для определения размера комиссии для транзакций. Рынок комиссий за транзакции формируется за счёт того, что при ограниченном размере блока, транзакции, находящиеся в данный момент в

очереди на подтверждение вынуждены конкурировать между собой для включения в блок. Чем выше комиссия транзакции, тем быстрее она будет включена в блокчейн. Форком Bitcoin Gold был выбран другой путь. В этом форке было уменьшено время между блоками до 2,5 минут; сменён алгоритм доказательства выполненной работы на Эквихеш (Equihash), который более устойчив к реализации на специализированных микросхемах; также коррекция сложности сети происходит каждый блок. Эти изменения позволили создать форк биткоина доступный для майнинга на графических процессорах. Однако этот форк биткоина не получил широкого распространения, в не последнюю очередь по причине того, что разработчики осуществили значительный премайн данной монеты.[7] В результате на четвертый квартал 2017 года все форки биткоина уступают ему по капитализации и популярности.

Принцип, озвученный Сатоси, о существовании денежной единицы, обладающей дефляционной природой и определённым уровнем анонимности, нашла отклик среди многих людей. “Право на конфиденциальность” главенствующий принцип свободного мира.[8] Это один из основных принципов, озвученных Сатоси Накамото, и принятый в криптовалютном сообществе, несмотря на это многие пользователи до сих пор используют псевдо-анонимные транзакции. Более того существуют правительственные и частные организации, которые с помощью анализа больших объёмов данных и машинного обучения, разрабатывают алгоритмы по деанонимизации пользователей криптовалют. Компания BitFury уже сейчас имеет возможность по деанонимизации до 15% всех транзакций в сети биткоин (данные на январь 2018 года). И этот процент имеет тенденцию к росту, что может изменить всю сферу криптовалют в ближайшие годы.[9] Отсутствие возможности проведения конфиденциальных транзакций в биткоине явно противоречит первоначальным планам создателя этой криптовалюты. Однако существует решение этой проблемы.

Различные криптовалюты пытались решить проблему с отсутствием конфиденциальности при проведении транзакций. К сожалению, многие из предлагаемых решений не обеспечивают должного уровня анонимности и могут быть скомпрометированы различными средствами. Однако в 2014 году была опубликована научная работа о новом криптографическом алгоритме zk-SNARKs.[10] Авторами данной работы являются исследователи из Массачусетского технологического института. Криптовалюты, которые внедрили бы технологию zk-SNARKs, могли бы использовать защищённые транзакции – транзакции были бы скрыты на уровне протокола сети и не были бы доступны путём анализа блокчейна. В 2016 году, авторами нового протокола была разработана и запущена новая криптовалюта Zcash. Это была первая криптовалюта использующая протокол zk-SNARKs. Создатели Zcash включили в код монеты налог, который распределяется в пользу разработчиков и инвесторов данного проекта. Размер этого налога составляет 20% от монет добытых майнерами. Этот налог вызвал непонимание среди части майнеров и во многом по этой причине Рет Крейтон (Rhett Creighton) решил произвести форк Zcash. Этот форк был осуществлён через 8 дней после запуска Zcash. Суть этого форка заключалась в отмене налога на майнеров. Новая криптовалюта получила название Zclassic. К сожалению,для Zclassic, его сильная сторона – отсутствие налога на майнеров, оказалась и его слабой стороной. Отсутствие налога привело к отсутствию активного развития. Однако существуют различные способы управления криптовалютой, которые позволят избежать таких проблем в будущем.

Bitcoin Private представляет собой объединение блокчейнов биткоина и Zclassic. Целью данного форка является добавление конфиденциальных транзакций в протокол биткоина, а также внесение других улучшений в протокол. В тоже же время Bitcoin Private постарается избежать ошибок, допущенных предыдущими форками биткоина.

Bitcoin Private будет иметь следующие параметры: больший размер блока (2 Мб), более короткий период генерации блоков (2,5 минуты), устойчивость к майнингу с помощью специализированных интегральных схем (ASIC), что будет достигнуто за счёт использования алгоритма Эквихеш (Equihash)б как доказательства выполнения работы (PoW). Более того, поскольку Bitcoin Private объединяет два блокчейна, это вызовет рост количества участников нового крипто сообщества. После форка владельцы Zclassic (t адреса и z адреса) и владельцы биткоина (простые адреса и адреса segwit) получат новую монету в пропорции 1 к 1. Также Bitcoin Private является первым форком, в котором происходит объединение двух блокчейнов.

Таблица 1. Сравнение Bitcoin Private, Биткоин, Bitcoin Cash и Bitcoin Gold.

	Bitcoin Private	Биткоин	Bitcoin Cash	Bitcoin Gold
Максимальное количество монет	21 миллион	21 миллион	21 миллион	21 миллион
Конфиденциальность транзакций	zk-SNARKs	x	x	x
Период между блоками	2,5 мин.	10 мин.	10 мин.	2,5 мин.
Размер блока	2 Мб	1 Мб	8 Мб	1 Мб
Алгоритм доказательства выполнения работы (PoW).	Эквихеш (Equihash)	SHA256	SHA256	Эквихеш (Equihash)
Коррекция сложности сети	Каждый блок	Раз в две недели	Раз в две недели	Каждый блок
Премайн	x	x	x	Да
Развитие проекта направляется сообществом	Да	x	x	x
Управление проектом направляется сообществом	Да	x	x	x

2. Методология объединения блокчейнов.

Применительно к Bitcoin Private объединение двух блокчейнов предложено осуществить путём слияния баз данных непогашенных выходов транзакций (UTXO) биткоина и Zclassic. Формально новая цепочка блоков будет реализована на основе Zclassic, поскольку последний уже имеет реализацию zk-SNARKs и JoinSplit транзакций на уровне протокола. Можно провести аналогию удлинения цепочки блоков криптовалюты, с эффектом полимеризации молекул. В блокчейне каждый следующий блок зависит от предыдущего и добавляется к концу цепочки блоков. Также, при полимеризации пластиков, каждая следующая молекула добавляется к существующей цепочке и чем длиннее становится молекула, тем более высокой прочностью обладает пластик, сформированный из этих молекул. Но рост цепочки блоков в криптовалюте ведет и к увеличению используемого места на диске пользователя и к значительному увеличению времени первоначальной синхронизации между узлами сети. Однако поскольку при объединении блокчейнов будет использоваться информации о балансах адресов на строго определённом блоке, а не вся предыдущая история транзакции для обоих блокчейнов, это позволит сократить общий размер объединённой цепочки блоков с 157 Гб до 10 Гб (в момент запуска сети). Более того пользователи Bitcoin Private получат возможность дальнейшего сокращения системных требований путём использования технологии упрощённой проверки платежей (SPV). Эта технология уже используется в программных кошельках на основе программы Электрум (Electrum). Также будет возможно использовать режим удаления блоков, которые не содержат транзакции данного пользователя (blockchain pruning) это приведёт к ещё большей экономии системных ресурсов для конечного пользователя.

Важной проблемой при разделении одного блокчейна на два является проблема ретрансляции транзакций между двумя блокчейнами (replay attack). Она выражается в том, что транзакция, осуществлённая в одной сети, является действительной в другой сети. Соответственно при разделении блокчейнов новая цепочка блоков должна иметь защиту от этой проблемы. Bitcoin Private будет иметь двухстороннюю защиту от ретрансляции транзакций как от сети биткоин, так и от сети Zclassic. Двухсторонняя защита означает, что транзакции из сети биткоин и Zclassic не будут действительны в сети Bitcoin Private и транзакции Bitcoin Private не будут действительными транзакциями в сети биткоин и Zclassic. Проблема ретрансляции транзакций хорошо изучена и как готовое стандартное решение будет реализован вариант с использованием метода SIGHASH_FORKID, который использовался и доказал свою эффективность для криптовалюты Bitcoin Gold.[11]

Снимок балансов произойдёт на первых блоках, которые будут найдены в сетях биткоин и Zclassic после 17:00 по Всемирному времени 28 февраля 2018 г. Сама же новая сеть будет запущена примерно через 48 часов после этого события. После запуска сети примерно 700.000 Bitcoin Private будет доступно для добычи майнерами. Начальная награда за блок установлена в 1,5625 монеты. Уполовинивание награды будет происходить каждые 210.000 блоков, т.е. примерно раз в год. Однако если приведённые параметры покажут свою несостоятельность, то будет реализован альтернативный план, который в общих чертах будет описан в части 7 данной работы.

3. Доказательство выполнения работы: Эквихеш (Equihash)

Как уже обсуждалось в первой части, добыча биткоина в основном осуществляется с помощью специализированных интегральных микросхем (ASIC), которые по своей скорости и энерго-эффективности значительно опережают графические процессоры. В отличие от графических процессоров, специализированные интегральные схемы значительно менее распространены среди майнеров-любителей, вследствие их более высокой цены и узкой специализации. Этот факт привёл к очень высокой централизации майнинга биткоина. Егор Хомаков (Egor Homakov) в своём исследовании предполагает, что более 60% всех мощностей майнинга в сети биткоин находятся на территории Китая.[12] В тоже время, алгоритмы доказательства выполнения работы, которые более устойчивы к реализации на специализированных интегральных микросхемах, ведут к децентрализации. Это возможно главным образом потому, что графические процессоры более доступны для конечных пользователей. Децентрализация является важным фактором для любой криптовалюты, поскольку она снижает вероятность проведения атаки на сеть на 51%. Также, децентрализация обеспечивает более равномерное распределение добытых монет и комиссий за переводы среди пользователей сети. Децентрализация понижает вероятность манипулирования рынком криптовалюты и снижает способность крупных майнеров вмешиваться в процесс развития криптовалюты.

Bitcoin Private использует в качестве доказательства выполнения работы алгоритм Эквихеш, который был разработан Алексом Бирюковым (Alex Biryukov) и Дмитрием Ховратовичем (Dmitry Khovratovich) в Университете Люксембурга, в качестве ассиметричного доказательства выполненной работы.[13] В отличие от других алгоритмов, которые также устойчивы к реализации с помощью специализированных интегральных схем, Эквихеш основан на решении “Парадокса дней рождений” и использует улучшенный алгоритм Вагнера для его решения. Более того, важной особенностью алгоритма Эквихеш является то, то он требователен к объему памяти; попытка снижения объёма памяти, необходимой для расчёта, ведёт к нелинейному увеличению требований к скорости расчётов. Эта особенность алгоритма делает Эквихеш устойчивым к реализации с помощью специализированных интегральных схем. Поскольку такие решения потребовали бы установки дополнительных модулей памяти, что в свою очередь привело бы к существенному удорожанию решений на специализированных микросхемах, что сделало бы их неконкурентоспособными по сравнению с графическими процессорами, и даже с центральным процессором ЭВМ. Авторы алгоритма подчеркивают, что требовательность Эквихеш к объёму памяти не защищает от использования ботнетов для майнинга криптовалюты. Однако, большой объём памяти, задействованный алгоритмом, вызовет замедление работы зараженного компьютера, что, скорее всего, будет замечено пользователем и приведет к удалению вредоносной программы.

4. Открытые и защищённые транзакции.

Bitcoin Private представляет собой сплав двух технологий транзакций – открытых и защищённых. Открытые транзакции функционируют по тому же принципу что и транзакции в сети биткоин. Они содержат вход и выход транзакции, количество монет в транзакции и ЭЦП. Количество денег в транзакции, отправитель и получатель транзакции: вся эта информация хранится в открытом виде внутри блокчейн. С другой

стороны, защищённые транзакции шифруют все детали касающиеся транзакции и хранят их в специальной части, внутри блока, именуемой JoinSplit. Эти транзакции обладают следующим свойством, они проверяемые, но в тоже время не расшифровываемые для третьих лиц. Когда происходит расход монет, скрытых в защищённой транзакции, целостность блокчейна поддерживается благодаря специальному алгоритму zk-SNARKs.[6] Этот алгоритм осуществляет подтверждение того, что сумма монет на входах транзакции равна сумме монет на выходе транзакции, для каждой защищённой транзакции. После этого отправитель транзакции приводит криптографическое доказательство того, что он обладает закрытыми ключами, позволяющими потратить входы данной транзакции. В заключение происходит процесс подписи транзакции с помощью ЭЦП и после этого транзакция не может быть изменена третьими лицами.[14] Эта технология опирается на процесс доверительной установки, используемый криптовалютой Zcash. В момент запуска Zcash, были сформированы криптографические ключи для доказательства с нулевым разглашением информации и для защищённых транзакций. Впоследствии, данные ключи были уничтожены. Весь этот процесс создания и уничтожения ключей команда разработчиков Zcash назвала “Церемонией”.[6] Эта процедура гарантирует, что система будет устойчива против возможной подделки ЭЦП в результате атаки на протокол защищённых транзакций.[10]

5. Программа пожертвований в фонд проекта путём добровольного майнинга.

Для создания денежного фонда, который позволил бы осуществлять поддержку и развитие Bitcoin Private, была запущена программа пожертвований путём добровольного майнинга. Суть программы заключается в распределении 62.500 монет Bitcoin Private среди майнеров, пожертвовавших свои мощности для добычи до 50.000 Zclassic в фонд поддержки Bitcoin Private. Распределение монет осуществляется по следующей формуле:

$$P = Z_m * 62.500 / Z_p$$

Где P - вознаграждение майнера в Bitcoin Private, Z_m - количество Zclassic добытых майнером для пула, Z_p - общее количество Zclassic добытых пулом.

62.500 монет Bitcoin Private будет создано в момент запуска сети, и они будут распределены между майнерами-участниками программы. Кошелёк программы будет содержать до 50.000 ZCL и эти средства будут направлены на разработку, маркетинг и программу вознаграждения для Bitcoin Private. Это поможет избежать проблем с разработкой, с которыми столкнулся Zclassic в связи с отсутствием достаточного финансирования.

В некотором смысле эта программа может представляться как премайн. Однако, команда разработчиков Bitcoin Private выступает против концепта премайна как такового. Обычно, премайн осуществляется в интересах узкой группы разработчиков. В случае Bitcoin Private это не так. В данном случае майнеры могут выбрать добровольно, сколько мощности они готовы пожертвовать с целью получения Bitcoin Private после запуска сети. Более того поскольку количество монет Bitcoin Private в данной программе фиксировано, а количество монет пожертвованных майнерами через добычу определяется самими майнерами, то данное рыночное распределение монет,

как нельзя более полно соответствует первоначальному видению биткоина. Средства из фонда будут потрачены в следующих пропорциях: 50% будут потрачены для добавления на биржи, торгующие криптовалютами, 25% будет потрачены на дальнейшую разработку, 15% на маркетинг, оставшиеся 10% пойдут на административные и текущие расходы.

6. Управление фондом поддержки проекта.

Совет по управлению денежным фондом будет состоять из трёх человек, представляющих сообщество Bitcoin Private, и двух человек, представляющих сообщество майнеров. Юридически совет будет зарегистрирован как компания BTCP Developer Community, LLC. На момент публикации состав совета: др. наук Джекоб Брутман (Jacob Brutman) - Операционный руководитель, Джузеппе Стуто (Giuseppe Stuto) - директор по макретингу и Питер Хатзипетрос (Peter Hatzipetros) - заместитель по правовым вопросам, представляют сообщество Bitcoin Private. Адиб Алами (Adib Alami) и Эван Дарби (Evan Darby) представляют сообщество майнеров. Также на данный момент подготовлен регламент совета.[15]

7. Будущее Bitcoin Private

Конфиденциальность транзакций важная часть проекта Bitcoin Private. В данный момент, zk-SNARKs протокол создает достаточно высокую нагрузку на память и процессор при формировании цифровой подписи транзакции. Этот процесс может занимать до нескольких минут. Одно из первых улучшений, которое будет реализовано в сети Bitcoin Private после её запуска, будет технология Jubjub, которая в данный момент находится в процессе разработки командой Zcash.[16] Эта новая технология значительно ускорит скорость формирования ЭЦП для защищённых транзакций использующих протокол zk-SNARKs. Другой метод планируемый для реализации - проект Одуванчик (Dandelion).[17] Этот метод позволит улучшить конфиденциальность в сети Bitcoin Private. Данную технологию можно описать как “стебель” - сама транзакция и “пух” - механизм запутывания. В то время как этот механизм запутывания сам по себе не может обеспечить той степени конфиденциальности, какую обеспечивает zk-SNARKs, он может быть использован как дополнительная мера, как для открытых, так и для защищенных транзакций.

Возможность улучшения технологии блокчейна Bitcoin Private является одной из важнейших особенностей данного проекта. С этой целью BIP9 был внедрён в текущую версию протокола, это позволит проводить софт форки блокчейна и с помощью них вносить улучшения.[18] После того как необходимый программный код готов для внесения в текущую версию протокола, майнеры начинают сигнализировать свою готовность к принятию данных изменений. Когда 95% всех майнеров просигнализировали свою готовность, то форк считается состоявшимся. Если же недостаточное количество майнеров сигнализировало свою готовность к форку в отведенное для этого время, то данный софт форк считается не принятым, и никакие изменения в текущую версию протокола вноситься не будут. Поддержка и развитие проекта Bitcoin Private будет зависеть от сбора средств в фонд проекта. Однако, команда Bitcoin Private не поддерживает навязывание налогов или каких-либо отчислений без демократического одобрения принятия таких решений. Вот почему одно из первых предложений, которое может быть применено через процедуру голосования BIP9, будет определение параметров пожертвований со стороны майнеров

в фонд поддержки проекта. Майнеры будут иметь возможность выбрать какое количество средств они готовы жертвовать в фонд. Это обеспечит дальнейшее развитие проекта.

Как уже упоминалось во второй части, небольшое количество Bitcoin Private доступное для майнинга может вызвать некоторые проблемы. В частности низкую мощность хеширования в сети. Одним из возможных решений этой проблемы является изъятие монет, которые не были востребованы пользователями после форка. Такое решение может быть принято на основании голосования через механизм BIP9. Если такое решение будет принято, то балансы невостребованных кошельков Bitcoin Private будут уменьшаться на 0,14% каждый день на протяжении двух лет. Изъятые монеты будут вводиться обратно в оборот майнерами. Такое решение проблемы позволит вернуть невостребованные монеты обратно в оборот, и с другой стороны даст достаточно времени пользователям воспользоваться их монетами. Более того, поскольку количество изъятых монет будет составлять достаточно малый процент, то оно не вызовет колебаний обменного курса и следовательно общей капитализации монеты.

Как резервная мера в Bitcoin Private реализована функция “бомбы сложности”. Эта мера позволит быть уверенным в дальнейшем развитии криптовалюты. Механизм “бомбы сложности” похож на то, как он реализован в криптовалюте Ethereum.[19] “Бомба сложности” будет напоминанием майнерам, что для развития Bitcoin Private требуются внесения изменений в протокол сети. Однако, эта мера будет применена только в крайнем случае. Как вариант бомба сложности может быть использована для внедрения новой системы управления, наподобие той, которая используется в криптовалюте Decred[20], либо для любого другого механизма управления. Это сделает проект ещё более демократичным и децентрализованным. В данный момент активация бомбы установлена на 2 марта 2019 г. Однако, с помощью хард форка эта дата может быть отложена. Неслучайно, что дата активации бомбы совпадает с первым уполовиниванием награды за блок, это позволит внести изменения в протокол, если вдруг эксперимент с низкой инфляцией покажет свою несостоятельность.

8. Коммерческое применение.

Обработка платежей остаётся одной из главных областей применения биткоина. Одна только компания Bitpay которая осуществляет обработку транзакций обсуживает переводы в размере 1,5 млрд. долларов в месяц между кошельками пользователей.[21] В своё время интернет произвёл революцию в сфере денежных переводов, сейчас же криптовалюты обуславливают собой новый качественный перёход в этой области.

Пользователи ожидают определённый уровень удобства в процессе осуществления платежей за товары и услуги, и это главная причина, почему оплата через интернет пользуется такой популярностью. Также, кроме удобства, пользователи ожидают определённый уровень конфиденциальности при осуществлении переводов в сети. Однако, за прошедшие два десятка лет с момента начала эпохи интернет торговли появилась масса компаний, которые предлагают услуги составления профиля покупателя на основе покупок, совершённых покупателем в сети интернет.[22] Очевидно, что такая практика вызывает отторжение и неприятие у пользователей. Этим в большой степени и объяснено желание конечных пользователей использовать криптовалюты для платежей в сети. Однако большинство криптовалют не в состоянии обеспечить необходимый уровень конфиденциальности транзакций.[14] В тоже время

Bitcoin Private решает эту проблему предлагая технологию анонимных транзакций zk-SNARKs.

Bitcoin Private будет играть важную роль в осуществлении транзакций между пользователями, а также для осуществления платежей за товары и услуги в сети интернет. Он предлагает проверенное временем, безопасное и широко используемое решение для платежей, в тоже время добавляя анонимность и конфиденциальность для пользователя. Можно найти сотни и тысячи различных коммерческих областей применения для Bitcoin Private. В то же время другие криптовалюты использующие z протокол для осуществления конфиденциальных транзакций не смогли достичь хоть сколь-нибудь широкого применения. Что главным образом обусловлено достаточно большой вычислительной нагрузкой при формировании ЭЦП конфиденциальных транзакций. Новая технология Jubjub, которую мы уже упоминали в части 7, позволит осуществлять конфиденциальные транзакции даже на мобильных устройствах. Команда разработчиков Bitcoin Private стремиться добиться как можно более широкого охвата среди пользователей и новые изменения в протокол, позволяющие осуществить это, будут внесены в ближайшее время. Также использование кошелька для мобильных устройств позволит охватить еще больше потенциальных пользователей. В настоящий момент Bitcoin Private получает большое количество заявок от продавцов, которые хотят использовать Bitcoin Private в качестве средства оплаты за товары и услуги. Если определённый процент от таких коммерческих транзакций было бы возможно направить в фонд поддержки проекта, то это бы устранило необходимость пополнения средств фонда из пожертвований майнеров.

9. Общественно направляемое развитие проекта.

Многие крипотовалютные проекты, в независимости от того относятся ли они к монетам или токенам, заявляют, что их развитие осуществляется в зависимости от решений сообщества, сформированного вокруг данной криптовалюты. До некоторой степени эти заявления могут являться правдой, однако обычно команда разработчиков контролирует все аспекты развития проекта. Конечно, существуют исключения из этого правила, например криптовалюта Decred, в которой сообщество монеты имеет определённый контроль за направлениями будущего развития. Хотя даже в этих редких случаях, разработка кода осуществляется узкой группой лиц. В то время как простые участники сообщества предлагают изменения в программный код монеты, такие предложения остаются незамеченными. В противоположность вышеприведённым примерамб Bitcoin Private представляет собой проект управляемый сообществом. В настоящий момент больше 100 человек вносят изменения в код проекта (данные на 6 февраля 2018) и количество таких людей постоянно растёт.

Несколько новшеств используются в проекте Bitcoin Private, которые выгодно отличают его от других монет. Для примера, программа “Всемирный посол”, в которой могут участвовать члены сообщества, помогая продвигать Bitcoin Private и тем самым увеличивая количество людей, вовлеченных в данный проект. Более того, Bitcoin Private запустил программу “Набор разработчиков”, которая открыта для участия любых программистов, даже для тех, кто не имеет опыта работы с технологиями блокчейн. Путём участия в этой программе разработчики могут получить необходимый опыт в разработке блокчейн технологий. За несколько дней эти две программы добавили около ста новых участников в проект, доведя общее количество участников проекта более чем до 300 человек. Размер команды участников Bitcoin Private показывает насколько большое влияние сообщество оказывает на развитие

данного проекта. Эти примеры подчёркивают по-настоящему децентрализованную природу проекта Bitcoin Private.

10. Выводы

Bitcoin Private это криптовалютаб которая разрабатывается и поддерживается сообществом. Члены команды со всего мира сотрудничают на постоянной основе, чтобы привести проект к успеху. По их мнению, данный проект является наиболее полной реализацией видения будущего криптовалюты, как её представлял Сатоси Накамото. В этом проекте финансовая свобода, дешёвые и конфиденциальные транзакции и децентрализация являются неотъемлемой частью криптовалюты. Включение в проект BIP9, как механизма для внесения изменений в протокол, а также “бомбы сложности”, на случай если BIP9 окажется неэффективным, показывают, что сообщество планирует дальнейшее развитие и улучшение проекта. Коммерческие применения для Bitcoin Private многочисленны, от международных переводов до покупок в сети. Объединение биткоина с технологией конфиденциальных транзакций используемую Zclassic открывает собой новую эру для блокчейн технологий.

11. Благодарности

Мы хотели бы выразить свою благодарность всему сообществу майнеров за их пожертвования через программу добровольного майнинга. Также отдельная благодарность молекуле кофеина, которая помогала нашей команде на протяжении многих дней и ночей. Без кофе этот проект был бы в принципе невозможен. Также благодарности заслуживает наша команда разработчиков - они представляют собой ту основу, на которую опирается весь проект. И в заключение, еще одна благодарность всему сообществу Bitcoin Private - оно представляет собой костяк проекта и мы вряд ли бы достигли чего-либо без их поддержки.

12. Использованные материалы.

13. Обнародование информации и другая информация.

Вся информация, представленная в данном документе является оригинальным трудом Bitcoin Private, если не указанно обратное. Ни какая часть данной публикации не может быть воспроизведена или упомянута без письменного разрешения Bitcoin Private.

Данный документ представлен только в целях информации, он не призывает к покупке или продаже любых финансовых инструментов. Также данный документ не содержит информации, на основании которой могли бы приниматься какие-либо финансовые или инвестиционные решения. Также данная работа не принимает во внимание инвестиционные планы, финансовую ситуацию или другие обстоятельства, в которых находятся читатели данного документа. Читатели должны сами оценивать, применима ли информация из данной работы к ним. Стоимость криптовалюты может колебаться и изменяться. Изменение цены за прошлые периоды не может использоваться как предсказание цены в будущем и как следствие это может привести к потере денежных средств. Информация в данном документе о Bitcoin Private не содержит в себе ни инвестиционных, ни финансовых, ни юридических советов. Также данная работа не содержит в себе рекомендаций или советов по приобретению Bitcoin Private.

Определённая информация в данной работе отражает видение будущего командой Bitcoin Private, однако это не гарантирует, что будущее будет развиваться по предложенному сценарию. Слова типа: может, должно, будет, предполагается, думается и т.д. и т.п. отражают вышеописанное видение будущего. Хотя Bitcoin Private считает что информация, представленная в этой работе, точна на момент публикации, Bitcoin Private не гарантирует этого ни для читателей, ни для третьих лиц.