Всех приветствую!

Биткоин на сегодняшний день бесспорно является ведущей криптовалютой в мире. Документ, опубликованный анонимно в 2008 году, как представляется, является прямым ответом на глобальный финансовый кризис и недоверие общественности к традиционным банковским и финансовым системам. Криптографические средства используются в Биткоине для обеспечения того, что:

Только владелец определенного кошелька имеет право управлять средствами этого кошелька

Общедоступный адрес связан, с частным, но не может быть отслежен третьей стороной

Информация хранится с помощью криптографического хеширования в структуре дерева меркла для обеспечения целостности данных

Фактическая информация о транзакциях общедоступна в блокчейне и может быть прослежена до отдельного лица посредством анализа цепочки. Это вызвало опасения по поводу возможной финансовой цензуры или метафорической "порчи" денег из-за их происхождения, как продемонстрировала катастрофа произишедшая с Silk Road. Это может произойти, потому что в определенный момент фиатные деньги обычно обмениваются на криптовалюту, поскольку криптоэнтузиасты рождены в реальном мире и неизбежно обналичивают деньги. Существует как программное обеспечение,так и организации по анализу цепей , которые с каждым днем все более эффективно отслеживают транзакции в блокчейне Биткоина. Несоблюдение полной конфиденциальности является одним из ограничений Биткойн, которое в свою очередь привело к созданию альткойнов, которые экспериментируют с различными функциями криптовалют. Создатели пытаются сделать их достаточно конфиденциальными в дополнение к удобной платежной сети. Данный топик как раз посвящен различным протоколам, которые обеспечивают конфиденциальность пользователя.

**CryptoNote** - Кольцевые подписи и стелс-адреса

*Монеты: Monero (использовался), Particl (использовался), Bytecoin. Технология перекочевала в Ring-CT*

В декабре 2012 года CryptoNote представила использование кольцевых подписей и скрытых адресовдля улучшения конфиденциальности криптовалюты. Обновленная версия CryptoNote 2 вышла в октябре 2013 года, автором которой является Николя ван Саберхаген. Кольцевые подписи скрывают информацию об отправителе, поскольку отправитель подписывает транзакцию, используя подпись, которая может принадлежать нескольким пользователям. Это делает транзакцию недоступной для отслеживания. Скрытые адреса позволяют получателю давать один адрес, который генерирует разные публичные адреса для средств, которые будут получены при каждой отправке средств на него. Это делает транзакцию несвязываемой. Что касается конфиденциальности, CryptoNote предоставил нам протокол для отслеживаемых и несвязываемых транзакций. Первой реализацией технологии CryptoNote был Bytecoin в марте 2014 года, от которой в последующие годы получили развитие другие технологии , ярким примером является Monero, основанный на CryptoNote v2, появившийся в апреле 2014 года.

Плюсы:

* Обеспечивает конфиденциальность отправителя и получателя
* Конфиденциальность по умолчанию
* Проверенная технология
* Повышенная масштабируемость с ошибкоустойчивостью
* Не требует участия третьей стороны

Минусы:

* Отсутствие большого объема может не дать нужной приватности
* Не скрывает информацию о сумме транзакции, если та не была связана с другим протоколом обспечивающим это CoinJoin/

**Монеты: Dash**

Разработчик Bitcoin Core Грегори Максвелл предложил набор решений для обеспечения конфиденциальности биткоинов и криптовалют, первым из которых был CoinJoin. CoinJoin (также называемый CoinSwap) позволяет нескольким пользователям объединять свои транзакции в одну , получая входные данные от нескольких пользователей, а затем отправляя свои выходные данные нескольким пользователям, независимо от пользователей которым пришли входные данные. Таким образом, адресат получит любую сумму выходных данных, которую он должен был получить и при этом не будет отслежен. Похожими, но не очень популярными протоколами основанными на CoinJoin являются, Coinshuffle, появившийся в 2014 году и Tumblebit разработанный в 2016 году. Они устранили необходимость в доверенной третьей стороне для «смешивания» транзакций. Существуют реализации технологии CoinJoin, над которыми активно работают, но они не являются самыми популярными решениями для обеспечения конфиденциальности на сегодняшний день. Известная криптовалюта, использующая технологию CoinJoin, - это Dash, выпущенная в январе 2014 года, с применением мастернод вместо доверенной стороны.

Плюсы:

* Обеспечивает конфиденциальность отправителя и получателя
* Легко реализовать в любой криптовалюте
* Повышенная масштабируемость с ошибкоустойчивостью
* Проверенная технология
* Легковесная

Минусы:

* Суммы транзакций могут быть рассчитаны
* Даже без стороннего миксера, зависит от качества централизации мастер ноды

**ZeroCoin**

Монеты: Zcoin, PIVX

В мае 2013 года протокол Zerocoin был представлен профессором университета Джона Хопкинса Мэтью Д. Грином и его аспирантами Яном Майерсом и Кристиной Гарман. В ответ на необходимость использования третьей стороны для протокола CoinJoin, протокол Zerocoin позволял уничтожить и переделать монету, чтобы стереть данные об ее использовании каждый раз, когда она тратится. Криптография с нулевым разглашением и доказательства с нулевым разглашением используются, чтобы доказать, что новые монетыдля трат, созданы надлежащим образом. Доказательство с нулевым разглашением позволяет одной стороне доказать другой, что она обладает конкретными данными,при этом не раскрывая их содержания.Биткоин сообщенство не приняло Zerocoin как реализацию, которая могла быть добавлена биткоин, поэтому необходимо было создать новую криптовалюту. Zcoin была первой криптовалютой, которая внедрила протокол Zerocoin в 2016 году.

Плюсы:

* Обеспечивает конфиденциальность отправителя и получателя
* Доказательство с нулевым разглашением
* Проверенная технология
* Повышенная масштабируемость с ошибкоустойчивостью

Минусы:

* Требуется надежная настройка (если, используется протокол Sigma данная проблема отпадает)
* Доказательства занимают слишком много места
* Сумма транзакций может быть раскрыта

**ZeroCash**

Монеты: Zcash, Horizen, Komodo, Zclassic, Bitcoin Private

Zerocash, был создан в мае 2014 года, Мэтью Грином, как преемник протокола Zerocoin. Он улучшил концепцию Zerocoin, используя преимущества доказательств с нулевым разглашением, называемых zk-snarks (сжатый неинтерактивный аргумент знания с нулевым Разглашением). В отличие от Zerocoin, который скрывал происхождение монет и историю платежей, Zerocash был быстрее, с меньшими размерами транзакций и скрывал информацию транзакций об отправителе, получателе и сумме. Zcash - первая криптовалюта, которая внедрила протокол Zerocash в 2016 году.

Плюсы:

* Обеспечивает полную анонимность. Отправитель, получатель и сумма скрыты
* Скорость обеспечивается благодаря небольшим размерам доказательств
* Не требует участия третьей стороны

Минусы:

* Требуется надежная настройка
* Монеты потенциально могут быть подделаны без надлежащей реализации.
* Конфиденциальные транзакции

**Монеты: Monero и Particl, используются c кольцевыми подписями как Ring-CT**

Вернёмся к Грегори Максвеллу. В 2015 году он представил конфиденциальные транзакции. Было предложено скрыть сумму транзакции и тип актива (например, депозиты, валюты, акции), чтобы о сумме знали только отправитель и получатель, если только они не решат обнародовать сумму. Протокол использует гомоморфное шифрование зашифровывая входные и выходные данные, при помощи слепых коэффициентов и своего рода кольцевых подписей в схеме фиксации выполнения транзакций для того, чтобы можно было «зафиксировать» транзакцию без знания ее фактической суммы. Рекомендую ознакомится более детально, чтобы понять принцип работы. Вывод заключается в том, что сумма транзакции может быть скрыта от посторонних во время верификации.

Плюсы:

* Скрывает суммы транзакций
* Конфиденциальность по умолчанию
* Проверенная технология
* Не требует участия трерьей стороны

Минусы:

* Скрывает сумму транзакции только когда используется отдельно Ring-CT

**Монеты: Monero и Particl**

В октябре 2015 года появился протокол Ring-CT, предложенный Monero Research Labs. RingCT сочетает применение кольцевых подписей для сокрытия информации об отправителе, с использованием конфиденциальных транзакций (которые также используют кольцевые подписи) для сокрытия сумм. , В предложении был описан новый тип кольцевой подписи - многоуровневая связываемая спонтанная анонимная групповая подпись, которая "позволяет скрыть суммы, источники и места назначения транзакций с рациональной эффективностью и верификацией, при создании монет." Протокол RingCT был внедрен в Монеро в январе 2017 года и стал обязательным к использовантю после сентября 2017 года.

Плюсы:

* Скрывает суммы транзакций, а также обеспечивает конфиденциальность получателя. Полная анонимность.
* Конфиденциальность по умолчанию
* Проверенная технология
* Повышенная масштабируемость с ошибкоустойчивостью
* Не требует участия третьей стороны

Минусы:

Отсутствие большого объема может не дать нужной приватности

**Mimblewimble**

Монеты: Grin

Протокол Mimblewimble был предложен человеком под псевдонимом Том Элвис Джедусоран в июле 2016 года , а в октябре 2016 года Эндрю Поэльстра продолжил его разработку. Протокол Mimblewimble - это "предложение структуры криптовалюты, ориентированной на конфиденциальность и гибкость". Ключевыми аспектами стали предложения по структуре транзакций, поэтому способ построения блокчейна различен для того, чтобы совмещать в себе конфиденциальность и функциональность. Mimblewimble использует концепцию конфиденциальных транзакций, чтобы скрыть суммы, секретные ключи, и информацию о транзакциях,для того чтобы подтвердить право собственности на активы, а не использовать адреса. А также объединяет транзакции вместо того, чтобы перечислять их отдельно в блокчейне. Протокол также вводит новый метод сокращения блокчейна. Grin - это криптовалюта находящаяся в разработке, которая использует Mimblewimble. Mimblewimble находится еще на ранней стадии разработки.

Плюсы:

* Скрывает суммы транзакций, а также обеспечивает конфиденциальность получателя. Полная анонимность.
* Конфиденциальность по умолчанию
* Леговесный
* Отсутствие публичных адресов

Минусы:

* Отсутствие большого объема может не дать нужной приватности
* Отправитель и получатель должны быть онлайн
* Относительно новая технология

Со временем появились и внедряются новые технологии по обеспечению конфиденциальности, предлагающие инновационные и захватывающие решения. Важно отметить, что эти технологии основаны на предварительных исследованиях и их применении. Протоколы предлагаются на основе криптографических концепций, которые показывают, как они будут работать, а затем разработчики фактически реализуют их. Очень важным моментом является то, что разработчики монет могут также адаптировать новые технологии обеспечения конфиденциальности, поскольку их достоинства становятся очевидными, даже если изначально при их создании были использованы другие конкретные протоколы конфиденциальности.

Следующая часть будет больше о плюсах и минусах, и даст Вам представление о том, каким образом можно сравнивать монеты, дабы выбрать оптимальную.