CLOAK

ENIGMA V2.1

белая книга

Февраль, 2018-го года

# ENIGMA

**Частная, безопасная и непревзойденная транзакционная система для CloakCoin (Монета Cloak).**

# 1. АННОТАЦИЯ

CloakCoin - это криптовалюта, которая предназначена обеспечить конфиденциальность, безопасность и отсутствие возможности отслеживания децентрализованных переводов с помощью Enigma.

Cloak представляет собой двойную монету PoW / PoS (доказательство работы, доказательство доли), которая на данный момент находится в стадии PoS (% интерес).

Enigma - это частная, безопасная и непревзойденная платежная система CloakCoin, которая формирует основы будущих разработок и предоставляет базовую транзакционную систему для децентрализованных приложений, запущенных в сети CloakCoin.

На сегодняшний день, конфиденциальность важнее, чем когда-либо. Огромные темпы технологического прогресса быстро расширили наши горизонты и соединили мир. Благодаря представлению первой криптовалюты Биткоин в 2009-ом году, криптовалюта неуклонно становится популярным платежным средством, и теперь мы можем мгновенно переводить цифровую валюту по всему миру, используя мощь блокчейна. По мере того, как принятие криптовалюты становится более распространенным, ужесточение регулирования неизбежно. Остается наблюдать, какую форму это регулирование примет, но многие обеспокоены тем, что это регулирование может стать чрезмерно жестким и спроектировано так, чтобы подавить некоторые, более либертарианские аспекты криптовалюты.

# ENIGMA

Enigma - это децентрализованная, не-блокчейн, перемешивающая система, которая позволяет пользователям сети CloakCoin конфиденциально и безопасно передавать Cloak друг к другу. Она была разработана, чтобы обеспечить безопасный процесс перемешивания и обеспечить отсутствие отслеживаемости сторонними лицами. Это гарантирует, что Cloak монеты пользователя, во время трансфера, находятся в безопасности и что отправитель и получатель не могут быть никак привязаны или связаны. Монеты Cloak никогда не переправляются на промежуточную сторону во время Cloaking-а (Клоукинг), поэтому монеты всегда находятся в безопасности. Мы также много работали над тем, чтобы система Enigma вознаграждала пользователей, которые помогают осуществить операции трансферов Cloaking. Мы и впредь будем совершенствовать этот процесс и стимулировать активных участников. Любой, кто имеет монеты Cloak, может участвовать в операциях Cloaking, которая разрешит ему выйти из своего кошелька (работающего в режиме Стэкинг / Клоукинг), чтобы позволить ему пассивно помогать в операциях Cloaking и зарабатывать значительные вознаграждения.

# 2. ОБЗОР ENIGMA V1.0

Enigma - первая публичная итерация частной, безопасной и беспроблемной платежной системы Cloak. Транзакции Enigma “скрыты” другими пользователями, которые получают вознаграждение за помощь. Другие пользователи предоставляют входы и выходы для транзакции Enigma, что делает невозможным определение истинного источника и пункта назначения трансфера Cloak. Все сообщения системы Enigma, которые находятся в сети, хэшируются и шифруются для получателя с использованием CloakShield, который обеспечивает безопасность и целостность данных. Дополнительную информацию Вы можете найти в Разделе номер 3 - “CloakShield”.

## 2.1. ПРОЦЕСС ENIGMA (ДЛЯ ПОДДЕРЖИВАЮЩИХ УЗЛОВ СИСТЕМЫ ENIGMA)

### СООБЩЕНИЯ ENIGMA

Узлы Enigma коммуницируют в сети Cloak и узел будет отслеживать другие активные узлы Enigma. Передачи Сообщений Enigma (Enigma Announcement Broadcasts) предупреждает другие узлы Enigma о наших публичных ключах сеанса и о текущем балансе маскировки (именуемого, как Cloaking) Enigma.

### ЗАЯВКИ НА МАСКИРОВКУ (КЛОАКИНГ) ENIGMA

Когда пользователи хотят отправить маскированную транзакцию Enigma, они выбирают серию узлов Enigma (с достаточно высоким балансом Enigma) и запрашивают их помощь в клоукинге.

Узел Enigma может выбрать помощь в маскировке и отправить запрос для получения подтверждения со стороны инициатора запроса. Если узел Enigma отказывается участвовать в клоукинге или своевременно не отвечает, тогда выбирается альтернативный узел Enigma и осуществляется связь с ним. Защита DDoS (распределенный отказ в обслуживании) закроет любые “непослушные” узлы на оставшуюся часть сеанса. Узел считается “непослушным”, если он неоднократно отказывается подписывать транзакцию Enigma или отказывается перенаправлять сообщения Enigma. Маскирующиеся узлы Enigma используют обмен ключами “Elliptic Curve Diffie Hellman” (ECDH) для получения общего секрета с инициирующим узлом Enigma. Он используется для создания общего секретного ключа для симметричного шифрования данных RSA-256 между маскирующимся узлом и узлом-отправителем.

## ПОДТВЕРЖДЕНИЕ КЛОУКИНГА ENIGMA

Когда узел Enigma принимает запрос “клоукинга”, он предоставляет список входов и выходов транзакций, которые будут использоваться для транзакции Enigma. Суммы входа, предоставляемые маскирующимся узлом, должны быть больше или равны сумме отправки Enigma (плюс любые сборы). Выходы тщательно выбираются так, чтобы они, как можно ближе, соответствовали истинному результату транзакции Enigma. Если адрес выхода Enigma ранее не использовался, новый ключ изменения генерируется “Клоукером”. Если адрес выхода Enigma ранее получал средства, тогда существующий адрес с подобной деятельностью выбирается “Клоукером”, чтобы вернуть свои фонды входа и получить награду Enigma за “клоукинг”.

## МАСКИРОВОЧНАЯ ТРАНЗАКЦИЯ ENIGMA

Отправитель Enigma создает транзакцию “маскировка”, используя входы и выходы, предоставляемые узлами Клоукера Enigma. Затем, Отправитель Enigma добавляет свои собственные входы и выходы в транзакцию, прежде чем перетасовывать все

транзакционные входы и выходы, чтобы содействовать процессу маскировки. Затем, замаскированная транзакция зашифровывается и отправляется (используя CloakShield) каждому участвующему Клоукеру. Узлы Клоукеров проверяют транзакцию, чтобы уверить входы и выходы, которые они поставляли, о присутствии маскированной транзакции и чтобы один или несколько из их выходов также были вознаграждены. Если транзакционные проверки пройдены, транзакция будет подписана (SIGHASH_ALL + SIGHASH_ANYONECANPAY), зашифрована и передана обратно отправителю Enigma. После того, как все Клоукеры Enigma подписали транзакцию, Отправитель Enigma подтверждает, что подписанная транзакция действительна и тоже ее подписывает. Ну и затем замаскированная транзакция готова для отправки в сеть Cloak.

### 2.2.1. ОТСЛЕЖИВАНИЕ УЗЛОВ МАСКИРОВКИ ENIGMA

Enigma позволяет узлам, находящимся в сети Cloak, транслировать объявления другим узлам. Эти объявления Enigma содержат открытый ec-ключ идентификатор узла и текущий доступный баланс для операций клоукинга Enigma. Узлы поддерживают список других активных узлов Enigma в сети, чтобы они могли общаться для маскировочных целей. Идентификаторы узлов генерируются на базе сессия к сессии; перезапуск клиента обновит текущий идентификатор.

1. Каждый кошелек для начала процесса создает пару ключей для открытого / секретного (secp256k1) сеанса.
2. Кошелек объявляет свой открытый ключ, а также периодически Клоукинг баланс для сессии другим узлам сети Cloak.
3. Узлы отслеживают другие активные узлы Клоукинга Enigma и могут связываться с ними напрямую или косвенно (через CloakShield Onion Routing (Луковая Маршрутизация CloakShield)).

# 2.2.2. ИНИЦИИРОВАНИЕ ТРАНЗАКЦИИ ENIGMA

Алиса хочет отправить Кэтрин 10 монет Cloak, используя 1 микшер:

1. Алиса транслирует запрос в сеть Enigma, содержащий ее открытый ключ сеанса Enigma и количество монет Cloak, которое она хочет отправить. Ее просьба надежно маршрутизируется через ряд узлов Enigma, чтобы замаскировать отправителя.

2. Боб включил режим Клоукинг и создает защищенный канал шифрования CloakShield для безопасной связи с Алисой. Затем, Боб создает пакетный ответ Enigma и надежно передает его Алисе. Ответ содержит список входов и выходов Боба, которые Алиса будет использовать для маскировки ее транзакции.

3. Алиса расшифровывает и обрабатывает Enigma ответ Боба и создает Enigma транзакцию с использованием собственных входов и выходов, смешанных с входами и выходами Боба. Весь этот процесс зашифровывается и отправляется Бобу для подписания.

4. Боб расшифровывает транзакцию Enigma и выполняет ряд проверок целостности транзакции, чтобы удостовериться, что входы и выходы, которые он предоставил, были использованы правильно и что он был вознагражден. Если транзакция Enigma проходит тестирования, тогда Боб подписывает ее, шифрует и передает Алисе.

5. Алиса выполняет дальнейшие проверки подписанной транзакции перед ее подписанием. Затем, транзакция отправляется в сеть (безопасно маршрутизируется через узлы Enigma) для включения в блок.

6. Когда сделка будет завершена, Кэтрин получит средства от Алисы, а Боб получит вознаграждение за помощь в маскировке транзакции Enigma.

7. Из-за того, что входы и выходы Боба отражают Алису, невозможно установить истинного отправителя и получателя транзакции Enigma.

# ПРИМЕР ТРАНЗАКЦИИ ENIGMA

АЛИСА хочет отправить монеты анонимно БОБУ.

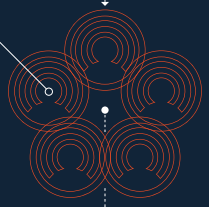
АЛИСА (-10.0992) CLOAK

(-10) CLOAK + (-0,0992) сбор Enigma
= всего (-10,0992) CLOAK

Микшерные узлы ENIGMA начинают общаться.

ЕКАТЕРИНА

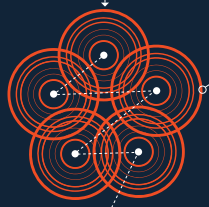
Каждый держатель монет может объявить себя Микшерным Узлом, также известным, как “Клоукер”.



Каждый участник остается анонимным и общается через зашифрованный канал.

Кошелек АЛИСЫ теперь подключен к микшерным узлам.

Каждый микшерный узел помогает АЛИСЕ перетасовывая транзакцию.



Эта сеть узлов создает децентрализованную анонимизацию, похожую на Луковую Маршрутизация TOR.

Микшерные узлы получают вознаграждение за Клоукинг АЛИСИНОЙ транзакции.

(+0.0992) CLOAK

Прямой сбор от 0,2% (более 1000 монет) до 1% (0 монет) распространяется на всех участвующих Клоукеров.

Система работает бесперебойно, чтобы обеспечить полную анонимность и полную конфиденциальность.

Затем БОБ получает зашифрованный платеж АЛИСЫ.

БОБ (+10)

БОБ анонимно и благополучно получает 10 CLOAK.

# 3. CLOAKSHIELD

CloakShield обеспечивает безопасную связь между узлами сети Cloak, используя симметричное шифрование RSA, поддерживаемое обменом ключами Elliptic Curve Diffie Hellman (ECDH). Это позволяет узлам безопасно обмениваться данными, обеспечивая защиту от подглядывающих (человек посередине) и самозванцев (атака sybil). CloakShield предназначен для защиты как Enigma, так и децентрализованных приложений CloakCoin и гарантирует, что ваши данные будут закрытыми.
CloakShield разрешает зашифрованную отправку данных одному или нескольким получателям.
Во время отправки одному получателю, полезный груз RSA зашифровывается, используя общий секретный ключ ECDH.
Во время отправки нескольким получателям, полезная груз зашифровывается с использованием одноразового ключа, а затем ключ шифруется для каждого получателя с использованием метода ECDH / RSA.

## СОЗДАНИЕ ОБЩЕГО КЛЮЧА ШИФРОВАНИЯ

Чтобы Алиса и Боб могли безопасно общаться, они должны договориться об общем ключе шифрования. CloakShield использует ECDH для выполнения этой задачи:

- Алиса имеет закрытый ключ Enigma dA и открытый ключ Enigma QA = dAG (где G - генератор для эллиптической кривой). У Боба есть частный ключ Enigma dB и открытый ключ Enigma QB = dBG.

- У Алисы есть публичный ключ Боба - Enigma dB полученный от объявлений Enigma, которые Боб отправляет в сеть, чтобы сообщить о его намерении помочь с маскировкой транзакции. Алиса использует свой закрытый ключ dA и открытый ключ Боба QB для вычисления общего секретного значения dAQB = dAdBG (ECDH_compute_key в OpenSSL).

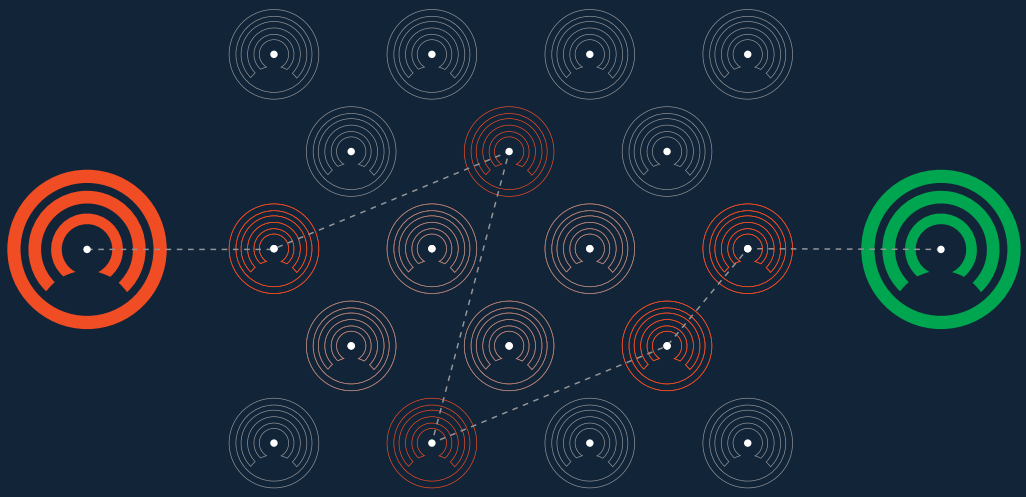
- Затем, Алиса создает засекреченный хэш SHA256 и передает хэш OpenSSL EVP_BytesToKey методу для того, чтобы получить ключ шифрования и IV, который будет использоваться для шифрования данных для Боба (с использованием симметричного шифрования RSA).

- Алиса теперь может создавать защищенные сообщения CloakShield для Боба.

Когда Боб получает от Алисы сообщение CloakShield, он читает из заголовка сообщения открытый ключ Алисы и генерирует тот же общий секретный ключ, что и Алиса, в соответствии с приведенными выше шагами (с его секретным ключом, а не Алисы). Кошелек Cloak поддерживает список активных ключей CloakShield и проверяет список существующего ключа CloakShield перед его генерированием.

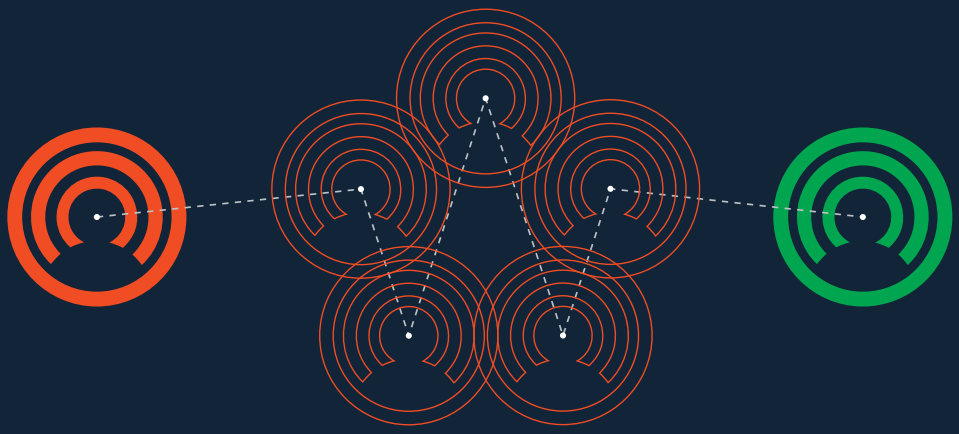
## ДАННЫЕ CLOAKSHIELD

CloakShield позволяет любым объектам данных Cloak сериализоваться (своего рода упорядочиться) и безопасно передаваться одному или нескольким получателям. Заголовок пакета данных CloakShield содержит открытый ключ отправителя Enigma и хэши открытых ключей получателей.
Заголовки CloakShield содержат хеш верификации, который генерируется с использованием открытого ключа отправителя и необработанных незашифрованных данных. Этот хэш верифицируется при расшифровке данных CloakShield, чтобы гарантировать, что информация в заголовке получателя совпадает с ключом шифрования и что данные не были изменены.



## ЛУКОВАЯ  МАРШРУТИЗАЦИЯ CLOAKSHIELD

Луковая  Маршрутизация - это метод (используемый TOR) для анонимной связи через компьютерной сеть. В луковой сети, сообщения фиксируются в слои шифрования, аналогичные слоям лука. Зашифрованные данные передаются через ряд сетевых узлов, называемых луковыми маршрутизаторами, каждый из которых “снимает” один слой, открывая следующий пункт назначения данных. Когда окончательный уровень расшифровывается, сообщение поступает в пункт назначения. Отправитель остается анонимным, потому что каждый посредник знает местоположение только предшествующих и следующих узлов.



## АНАЛОГИЯ ЛУКОВОЙ МАРШРУТИЗАЦИИ

Добавление функциональности “луковая маршрутизация» в сеть Enigma (с использованием CloakShield), позволяет узлам косвенно связываться, чтобы обойти анализ трафика. Это затрудняет определение того, какие узлы взаимодействуют друг с другом и какие узлы отправляют транзакции в сеть CloakCoin. Когда узел Enigma захочет связаться с другим узлом Enigma, он выбирает ряд других узлов Enigma, которые будут выступать в качестве, так называемого, реле для связи. Каждый зашифрованный уровень может быть расшифрован только предполагаемым реле [для которого был зашифрован определенный уровень]. После расшифрования уровня, реле передает данные на следующий узел ретрансляции. Эта маршрутизация продолжается до тех пор, пока данные не достигнут своего предполагаемого получателя, и все слои не будут расшифрованы поочередно выбранными узлами ретранслятора. Из-за “самостоятельного” характера сети Enigma, выходные узлы не требуются, и CloakShield гарантирует, что для узла нет риска ретрансляции или изменения зашифрованных данных.

# 4. СКРЫТЫЙ АДРЕС

Клоук использует систему Enigma для обеспечения конфиденциальных / безопасных транзакций.

## CLOAKSHIELD - ЭТО КОММУНИКАЦИИ УЗЛА К УЗЛУ

При запуске, каждый кошелек Cloak генерирует пару ключей [NID_secp256k1] (Cloaking Encryption Key / CEK), чтобы они могли создавать специальные секреты, используя ECDH с помощью своих закрытых ключей и открытого ключа получателя. Эта коммуникация формирует основу для всех связей между узлами, которые связаны с системой Enigma. Для получения дополнительной информации просмотрите ‘Src / enigma / cloakshield.h / .cpp’. Эта, основанная на ECDH, зашифрованная связь также используется для данных с луковой маршрутизацией, которые обрабатываются CloakShield.

Когда включена луковая маршрутизация, клиент попытается построить действительный луковый маршрут для данных, используя список осведомленных пиров Enigma. Узел может не иметь прямого подключения к пирам Enigma и это необязательно, поскольку CloakData (данные, упакованные для маршрутизации с помощью CloakShield) пакеты передаются одноранговo. Луковая маршрутизация, в основном, будет состоять из 3 отдельных маршрутов к узлу назначения, с 3 переходами узла на один маршрут. Для управления ситуациями используются несколько маршрутов, где узел маршрутизации отключается.

Узлы периодически отправляют пирам Enigma Сообщение (src / enigma / enigmaann.h) для рекламы своих услуг в сфере луковой маршрутизации. Другие узлы в сети хранят объявления (пока они не истекут или не будут заменены на обновление) и используют их для создания луковых маршрутов.

## ПРИМЕР ТРАНЗАКЦИИ СКРЫТОГО АДРЕСА

Когда узел отправляет транзакцию Enigma на скрытый адрес, то происходит следующее:

1. Отправитель генерирует входы для покрывания отправленной суммы, вознаграждений Enigma и сетевых сборов (1% при 0 монетах до 0,2% при 1000 и более монетах).

2. Отправитель генерирует объект CloakingRequest (содержащий для этого запроса уникальное скрытое число, которое может быть использовано один раз).

3. Отправитель генерирует от 2 до 4 одноразовых платежных скрытых адресов, используя скрытый адрес получателя и случайным образом распределяет отправленную сумму между адресами.

4. Отправитель решает, сколько участников будет использовано в этом процессе. Может быть выбрано от 5 до 25 участников (каждый участник получает 80-120% от равного разделения сборов Enigma).

5. Отправитель осуществляет луковую маршрутизацию CloakRequest к сети. Запрос содержит “сумму отправки”, чтобы Клоукеры могли знать, сколько нужно зарезервировать.

6. Клоукер выбирает CloakRequest и решает принять ли участие.

7. Клоукер снабжает отправителя X-входами, скрытым адресом и скрытым хешем (для их изменения).

8. Клоукер посылает CloakingAcceptResponse отправителю. Это сообщение содержит скрытый адрес, скрытое число, которое может быть использовано один раз и TX-входы.

9. Отправитель ждет до тех пор, пока не получит подтвержедние от достаточного количества Клоукеров.

10. Отправитель создает транзакцию Enigma, используя собственные входы и входы Клоукера. Затем входы перетасовываются.

11. Отправитель создает TX-выходы для всех Клоукеров. Выходы случайным образом разделяют их изменения и возвращают обратно. Этот процесс клоукинга также дает возможность получить Клоукеру награду.

12. Отправитель создает свои собственные изменения для Enigma TX. Это и есть одноразовые скрытые платежные адреса.

13. Отправитель подсчитывает сборы за TX сети и вычитает их из своего собственного возврата изменений.

14. Отправитель посылает Клоукерам Enigma TX для подписания.

15. Клоукеры проверяют TX, чтобы подтвердить что их входы сходятся и что есть одноразовые адреса оплаты, присвязанные к одному из их скрытых адресов с оплатой, превышающей сумму входа.

16. Клоукеры подписывают или отклоняют TX и отправляют подписи Отправителю.

17. Отправитель сопоставляет подписи и передает завершенный, подписанный TX в сеть.

18. Узлы сканируют входящие транзакции для скрытых платежей и Enigma платежей, и обнаружают любые платежи или изменения. Пара ключей и адреса генерируются для любых сопоставимых платежей, а сгенерированные ключи / адреса сохраняются в локальном кошельке.

# 5. БУДУЩЕЕ ПРОЕКТА ENIGMA - В ДАЛЬНЕЙШЕМ РАЗВИТИИ

Enigma формирует основу CloakCoin и будет продолжать работать над развитием и улучшениями, поскольку мы движемся только вперед, благодаря CloakCoin. Вот некоторые из тех функций, которые мы запланировали улучшить/изменить:

## УЛУЧШЕННЫЙ АЛГОРИТМ PROOF-OF-STAKE

Доказательство доли (PoS) - это метод защиты криптовалютной сети, которая полагается на пользователей, показывающих свое владение монетами для подписи блоков. В конечном счете, вероятность подписания блоков пропорциональна количеству принадлежащих монет - кто-то, владеющий 1% от общего объема монет, сможет подписать 1% всех proof of stake блоков. По сравнению с proof of work (доказательство работы), PoS требует значительно меньше вычислительной мощности и, следовательно, уменьшает в разы потребление энергии.

## ВОЗРАСТ МОНЕТЫ И ЛИНЕЙНОЕ PROOF-OF-STAKE

Основополагающим моментом для большей части реализации PoS, в том числе CloakCoin, является концепция Возраста Монеты. По существу, это показатель того, как долго владелец монет держал свои монеты, при этом не тратя и не перемещая их. С момента завершения транзакции, монеты, которые были частью этой транзакции, начинают накапливать свой возраст (начинающийся с нуля). В своей простейшей форме, под названием “Линейный возраст монеты”, монеты будут накапливать свой возраст в минутах / часах / днях / годах. Например, человек, который имеет 365 монет в течение 100 дней, аккумулирует 36 500 “монетных дней” или примерно 100 “монетных годов” (в данном случае возраст определен с учетом високосных лет, поэтому не 365 дней, а ~ 365,24 дней).

Линейные разработки Proof-of-Stake получили критику в отношении Возраста Монеты. Многие утверждают, что линейный Proof-of-Stake поощряет накопление монет (что может иметь пагубное влияние на объем торговли). Еще одна жалоба на линейное Proof-of-Stake состоит в его возможно оказанном эффекте на безопасность сети. Реализация Линейного Proof-of-Stake часто страдает из-за того, что пользователи периодически подключаются к сети Cloak, чтобы запустить стэкинг своих монет, а затем отключиться от сети, как только возраст монеты будет обнулен. Затем пользователь ждет, пока возраст монеты не пополнится, прежде чем повторить процесс заново. Этот ньюанс не обеспечивает лучшую безопасность для сети, и алгоритм Proof-of-Stake, который вознаграждает за частый или постоянный стэкинг, был бы наиболее полезен для CloakCoin и соответствующих Proof-of-Stake валют.

Для того, чтобы гарантировать, что Enigma Клоукеры получает как можно больше вознаграждений, возраст монеты должен быть удален из CloakCoin алгоритма Proof-of-Stake. Это обеспечило Клоукерам получение как полных вознаграждений, так и любые вознаграждений за маскируковку Enigma. Дополнительное включение компонента скорости при вычислении вознаграждений за стэкинг, дальше будет вознаграждать активные узлы маскировок Enigma, поощряя пользователей участвовать в маскировке Enigma для дальнейшего увеличения их заработанных процентов в дополнение к заработанным доселе вознаграждениям. Помимо предоставления увеличенного вознаграждения активно участвующим пользователям, улучшенный алгоритм Proof-of-Stake, также обеспечит вышеупомянутые улучшения в сетевой безопасности.

## ОБЪЕДИНЕНИЕ И РАЗДЕЛЕНИЕ ТРАНЗАКЦИЙ ENIGMA

Enigma в настоящее время создает единую “Cloaked” (замаскированную) транзакцию “Cloaked” за 1 трансфер. В настоящее время, мы работаем над обновлением основной деятельности Enigma, которое разрешит большому числу транзакций Enigma объединиться в супер-транзакцию Enigma. Эта транзакция будет эффективно содержать несколько замаскированных транзакций и обеспечит еще большую анонимность пользователей Cloak. Данное расширение позволит пользователям выбрать число кооперативных транзакций Enigma, которые они дополнительно требуют к числу Клоукеров. Это конкретное добавление, конечно, остается полностью децентрализованным, частным и безопасным.

Еще одним дополнением к Enigma, которое в настоящее время разрабатывается командой Cloak, является способность замаскировать большое количеств Cloak, как серию небольших транзакций Enigma. Чтобы достичь этого, пользователь будет выбирать количество Cloak, который он хотел бы отправить замаскированным на определенный адрес. Затем CloakCoin будет работать в фоновом режиме, чтобы создать ряд небольших транзакций Enigma равнозначного количества, которое может быть замаскировано и отправлено в сеть Cloak в течение установленного периода времени. Этот процесс дозирования будет совместим с “комбинированными” транзакциями Энигма, обеспечивая дополнительную маскировочную защиту для трансферов.

# 6. FAQ (ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ)

## В. КАК КЛОУКЕРЫ ПОМОГАЮТ СОВЕРШАТЬ ТРАНЗАКЦИИ ENIGMA?

О. Клоукеры (Cloakers) предоставляют один или несколько входов, которые используются для маскировки входа отправителя. Также, Клоакеры предоставляют серию обратных адресов, которые возвращают их вход, а также платят Клоукерам вознаграждения. Обратные адреса выбираются тщательно, чтобы дать приоритет активным адресам. Этот процесс делает сложным, для любого, кто выполняет анализ блокчейна, определение истинного выхода транзакции Enigma. Система Enigma, также проверяет целевой адрес так, чтобы замаскированные выходы зеркально отображали истинный выход настолько близко, насколько это возможно.

## В. СКОЛЬКО ВРЕМЕНИ ЗАНИМАЕТ ВЫПОЛНЕНИЕ ТРАНЗАКЦИИ ENIGMA?

О. В настоящее время, транзакции Enigma длятся одну минуту. Замаскированные узлы помогают маскировать транзакции Enigma резервируя необходимые средства до завершения транзакции Enigma или до истечения определенного времени. В случае просроченной или прерванной транзакции Enigma, средства будут разблокированы локально для повторного использования.

## В. КАК ENIGMA ВЛИЯЕТ НА СТЭКИНГ?

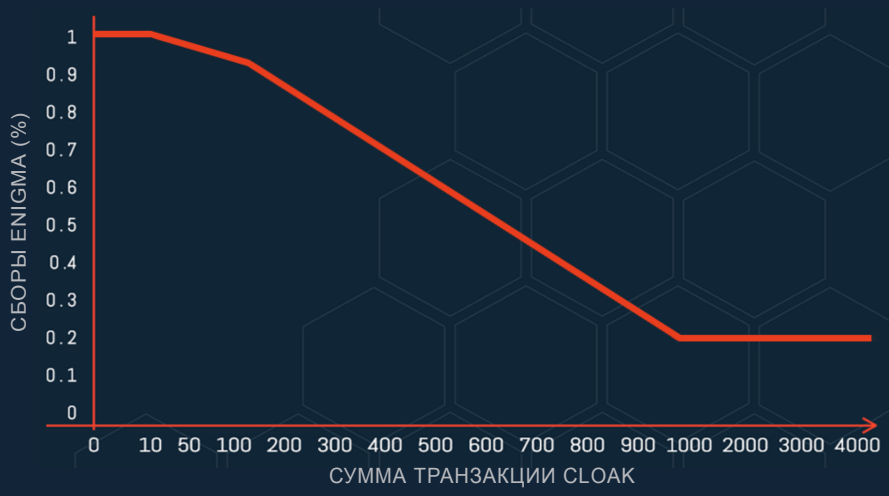
О. Любая монета, используемая в транзакции Enigma (в качестве Отправителя или Клоукера), будут иметь свой сброс Возраста Монеты. Однако, следует отметить, что участие в Клоукинге должно быть обеспечено гораздо более высоким уровнем, чем сам стэкинг. Команда Cloak работает над пересмотром алгоритма Enigma для предстоящего хардфорка (Enigma 1.1). Для дополнительной информации, пожалуйста, просмотрите раздел номер 5 “Будущее проекта  Enigma - В Дальнейшем Развитии”.

## В. КАКАЯ КОМИССИЯ ЗА ОСУЩЕСТВЛЕНИЕ ТРАНЗАКЦИИ ENIGMA?

О. 1% при 0 монетах до 0,2% при 1000 и более монетах. Это делается для того, чтобы наградить узлы Enigma, которые помогают с процессом клоукинга при осуществлении транзакции Enigma. Сборы затем смешиваются с транзакцией и разделяются между клоукерами. Дело не только в вознаграждении для клоукеров. Это также используется для того, чтобы определение суммы сделки было невозможным. Каждый участник получает 80-120% от любой сделки получив равную часть от распределения.

## В. КАК ИМЕННО ОПРЕДЕЛЯЕТСЯ СУММА КОМИССИИ ЗА ТРАНЗАКЦИЮ ENIGMA?

О. Процент сбора за транзакцию Enigma взимается на основе каждой транзакции по следующим ставкам:




| СУММА TX | СБОРЫ ENIGMA (%) | СБОРЫ CLOAK |
|---|---|---|
| 0 | 1.00 | 0 |
| 10 | 0.992 | 0.0992 |
| 50 | 0.96 | 0.48 |
| 100 | 0.92 | 0.92 |
| 200 | 0.84 | 1.68 |
| 300 | 0.76 | 2.28 |
| 400 | 0.68 | 2.72 |
| 500 | 0.60 | 3.00 |
| 600 | 0.52 | 3.12 |
| 700 | 0.44 | 3.08 |
| 800 | 0.36 | 2.88 |
| 900 | 0.28 | 2.52 |
| 1000 | 0.20 | 2.00 |
| 2000 | 0.20 | 4.00 |
| 3000 | 0.20 | 6.00 |
| 4000 | 0.20 | 8.00 |

## В. НУЖНО ЛИ МНЕ ИМЕТЬ ОПРЕДЕЛЕННОЕ КОЛИЧЕСТВО CLOAK НА МОЕМ БАЛАНСЕ КОШЕЛЬКА, ЧТОБЫ БЫТЬ КЛОУКЕРОМ ENIGMA?

О. Вы можете предлагать свои услуги для маскировки, независимо от баланса в вашем кошельке CloakCoin. Когда Enigma Клоукинг включен, CloakCoin зарезервирует часть вашего баланса для участия в маскировке Enigma, за что вы получите награду. Резервная сумма по умолчанию составляет около 50%, но это значение может быть настроено пользователем. Выбранное значение должно быть произвольным, для предотвращения связи объявлений Enigma с объявленным Клоукинг балансом. Следует отметить, что кошельки с более высоким балансом имеют более высокий шанс быть выбранными в качестве Клоукера, поскольку они с большей вероятностью имеют тот баланс, необходимый для более крупных транзакций Enigma.

## В. КАК ЭТО ЗАЩИЩАЕТ ОТ ВРЕМЕННОЙ АТАКИ, КОГДА КТО-ТО НАБЛЮДАЕТ ЗА БЛОКЧЕЙНОМ ДЛЯ ИДЕНТИЧНЫХ ВХОДОВ И ВЫХОДОВ? ТАКИМ ОБРАЗОМ РАЗВЕ НЕВОЗМОЖНО БЫЛО БЫ ОПРЕДЕЛИТЬ МЕСТО НАЗНАЧЕНИЯ?

О. Транзакции Enigma группируют выходы и гарантируют наличие многочисленных совпадений выходов замаскированных, как выход для получателя.

## В. МОЖЕТ ЛИ СОЗДАТЕЛЬ ТРАНЗАКЦИИ ENIGMA ОПРЕДЕЛИТЬ ПУТЕМ ИЗУЧЕНИЯ ПОДПИСИ  СКРИПТА ОПРЕДЕЛЕНИЕ ПОРЯДКА ПОДПИСАНИЯ?

О. Нет. Во время процесса подписания, порядок подписи скрипта рандомизируется (произвольно меняется) при объединении подписей. Это делают отправитель и участвующие Клоукеры.

## В. МОЖЕТ ЛИ СТОРОННИЙ ЧЕЛОВЕК ОТСЛЕЖИВАТЬ СЕТЬ, ЧТОБЫ СЛЕДИТЬ ЗА ИСХОДЯЩИМИ ТРАНЗАКЦИЯМИ ENIGMA, ОТПРАВЛЯЕМЫМИ В СЕТЬ ДЛЯ ОПРЕДЕЛЕНИЯ ИСТИННОГО ОТПРАВИТЕЛЯ?

О. Нет. Все стороны в случайном порядке предоставляют транзакцию Enigma в сеть. Это обеспечивает смягчение последствий таких подслушивающих атак.

## В. КАКОВА ПЛАТА ЗА ТРАНЗАКЦИЮ ENIGMA?

О. Плата за транзакцию Enigma составляет не более 1% от отправленной суммы ( процент зависит от суммы, которая будет отправлена ), плюс плата за сетевые платежи. Эти платежи используются для вознаграждения узлов Enigma, которые помогают замаскировать транзакцию Enigma.

## В. ТРЕБУЕТ ЛИ ENIGMA ХАРДФОРК СЕТИ CLOAK?

О. Нет. Старые клиенты CloakCoin без проблем смогут обрабатывать транзакции Enigma, но они не будут иметь возможность создавать их или участвовать в их маскировке. Однако, следующий пересмотр Enigma потребует хардфорк из-за изменений в базовом алгоритме Proof-of-Stake и поддержки для дополнительных кодов операций для функций рынка (таких как Block Escrow).

## В. КАК ENIGMA ЗАЩИЩАЕТСЯ ОТ “ПЛОХИХ АКТЕРОВ”?

О. Система Enigma обладает обширной защитой DDoS для составления “черного списка” узлов на время сессии. Если узел Enigma повторно отказывается подписывать транзакцию, он будет исключен из приглашения для Клоукинга Enigma на оставшуюся часть текущей сессии. В настоящее время, мы изучаем дополнительные методологии для дальнейшего наказания неуправляемых узлов Enigma. И скорее всего внедрим систему, которая будет требовать от Клоукеров депонирование номинальной, подлежащей возврату вознаграждению, которое

может быть заявлено как штраф, в случаях, когда узел пытается заблокировать транзакцию Enigma, отказываясь подписывать завершенную транзакцию. Следует отметить, что в то время, как вредоносные узлы могут пытаться помешать транзакциям Enigma, они не смогут украсть или присвоить какие-либо средства.

## В. КАКОВО МАКСИМАЛЬНОЕ КОЛИЧЕСТВО КЛОУКЕРОВ, КОТОРЫЕ МОГУТ ПОМОЧЬ В ТРАНЗАКЦИИ ENIGMA?

О. Максимальное количество Клоукеров установлено, и составляет 25 единиц. Система Enigma является гибкой, и это число можно легко увеличить.

## В. КАК ИМЕННО МОГУТ БЫТЬ ОБНАРУЖЕНЫ / ПОЛУЧЕНЫ СКРЫТЫЕ ТРАНЗАКЦИИ И ТРАНЗАКЦИИ ENIGMA?

О. Все входящие транзакции сканируются. В первую очередь, сканируются скрытые транзакции (используя эфемерный публичный ключ по умолчанию, содержащийся в случайном выходе OP_RETURN TX). После этого транзакции Enigma проверяются. Enigma транзакции также используют стандартный эфемерный публичный ключ, но платежи используют дополнительную ступень, включающую последующий производный ключ. Выходы Enigma генерируются используя хэш эфемерного публичного ключа, приватный, скрытый хэш-адрес и индекс выхода.

При сканировании транзакций Enigma, адреса оплаты с нулевым индексом генерируются для каждого принадлежащего скрытого адреса [HASH (ephemeral_pubkey, hash_stealth_secret, 0)]. Если найдено совпадение скрытого адреса с нулевым индексом, то для остальных индексов создаются дополнительные адреса [num_tx_outputs], и они сканируются против обнаружения платежей. Для получения дополнительной информации взгляните на FindEnigmaTransactions в “wallet.cpp”.

Аналогичный метод сканирования используется Клоукерами до подписания TX Enigma, чтобы гарантировать правильное получение возмещения. Для получения дополнительной информации взгляните GetEnigmaOutputsAmounts в “wallet.cpp”.

## 7. ССЫЛКИ


[01] http://bitcoin.org

[02] https://en.bitcoin.it/wiki/Category:Mixing Services

[03] https://wiki.openssl.org/index.php/Elliptic_Curve_Diffie_Hellman

[04] http://blog.ezyang.com/2012/07/secure-multiparty-bitcoin-anonymization

[05] https://bitcointalk.org/index.php?topic=279249.0
(CoinJoin: Bitcoin Privacy for the Real World)

[06] https://bitcointalk.org/index.php?topic=27787.0
(Proof of Stake Instead of Proof of Work)

[07] https://en.bitcoin.it/wiki/Proof_of_Stake

[08] https://en.bitcoin.it/wiki/Deterministic_wallet

[09] https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

[10] http://www.onion-router.net


www.cloakcoin.com

https://chat.cloakcoin.com

www.twitter.com/CloakCoin