Децентрализованная Платежная Сеть Построенная на Блокчейне

Slava Gomzin, Dan Itkis

Версия 3

Октябрь 2018

Первоначальная версия была опубликована в Июне 2017

Аннотация
Происхождение
Назначение децентрализованного процессинга
Терминология
- Выборки Авторизации
- DAPI
- Брокер Конверсии
- Полная Супернода
- GRAFT
- GRAFT Point of Sale
- GRAFT Wallet
- GRFT
- Токен Продавца
- Платежный Шлюз
- Токены Выплат (“Стабильное значение”)
- Прокси Супернода
- VChain

Комиссии за транзакции
- Платить Комиссии или не Платить
- Покупатель Не Должен Платить Комиссии
- Микроплатежи: Как Мне Заплатить за Чашку Кофе?

Комиссии за транзакции GRAFT
- Комиссии Продавцов и Сервис Провайдеров
- Бесплатные Денежные Переводы: Авторизированные Транзакции

Конфиденциальность
- Почему Необходим Приватный Блокчейн?
- CryptoNote как Основа Конфиденциальности
- Конфиденциальные Транзакции

Обработка Транзакций
- Проблема Долгого Подтверждения: Вводим Авторизации в Реальном Времени.
- Суперноды
- DAPI
- Подтверждение в Реальном Времени Выборками Авторизации
- Блокировка Аккаунта для Авторизации.
- Уровни Супернод
- Полные Суперноды
- Майнинг Узлы
- Расчет Вознаграждения за Майнинг
- Уровни Полных Супернод

Делегированные Доли
Выборка Авторизации
Прокси Суперноды
Вознаграждения Суперноды
Масштабируемость
Оффлайн Подтверждение Транзакций
Платежные Шлюзы для Продавцов и Поставщиков Услуг

Типы Транзакций и Потоки Платежей
Авторизация
Предварительная Авторизация
Завершение
Продажа
Перевод
Отмена
Выпуск
Погашение
Конверсия
Расписание
Депонирование
Возврат
Обработка Транзакций с Помощью Токенов GRAFT в Качестве Оплаты
Обработка Транзакций с Помощью Альтернативных Способов Оплаты.

Посредники Конверсии
Посредник Приема Платежей
Дизайн и Экономика Посредника Приема и Выплат Платежей
Двойной Обмен Посредников.
За Пределами Торговых Сетей: DEX (Децентрализованный обменник)
Посредник Взаимообмена
Посредник Выплат
Посредник Пополнения

Выплаты Продавцам
Волатильность
Токен Выплат (“Стабильное значение”)
Андеррайтинг Токенов Выплат
Обработка Выплат

Токены продавца и VChain
Токены Продавца
Типы Токенов Продавца
Типы Транзакций Токенов Продавца

Комиссии за Токены Продавца
VChains (Виртуальные Сети)
Комиссии VChain
Децентрализованные Краудфандинг Кредиты
Безопасность
Доступность
Управление Идентификацией
Идентификация, Аутентификация и Авторизация
Доказательство Идентификации
Рейтинг Репутации. Проливаем Свет
Поддержка Клиентов, Разрешение Споров и Страхование Платежей.
Клиентские Приложения
Заключение
Источники

Аннотация

Global Real-Time Authorizations and Funds Transfers (GRAFT) это глобальный децентрализованный платежный шлюз, основанный на блокчейне с открытым исходным кодом, а также процессинговая платформа, которой может пользоваться каждый. Это недорогой и полностью децентрализованный способ обработки транзакций. Экосистема GRAFT открыта, поэтому любой желающий может стать участником и поддерживать блокчейн GRAFT, а также внедрять сетевые сервисы.

GRAFT использует протоколы обработки платежей аналогичные традиционным электронным платежам, такие как кредитные, дебетовые и предоплаченные пластиковые карты, которые уже знакомы и которым доверяют миллионы покупателей и продавцов. Этот подход позволяет проще и быстрее принимать GRAFT как основную платформу платежей, без необходимости использовать централизованных посредников (платежные шлюзы и процессоры). В настоящее время необходимо упростить переводы между покупателям и продавцами.

Происхождение

Bitcoin[1] был создан как “цифровая наличность”— безопасная, но относительно медленная расчетная система, которая не смогла заменить платежные карты или конкурировать с ними, а также наличными деньгами в обычных магазинах. (Рисунок 1).

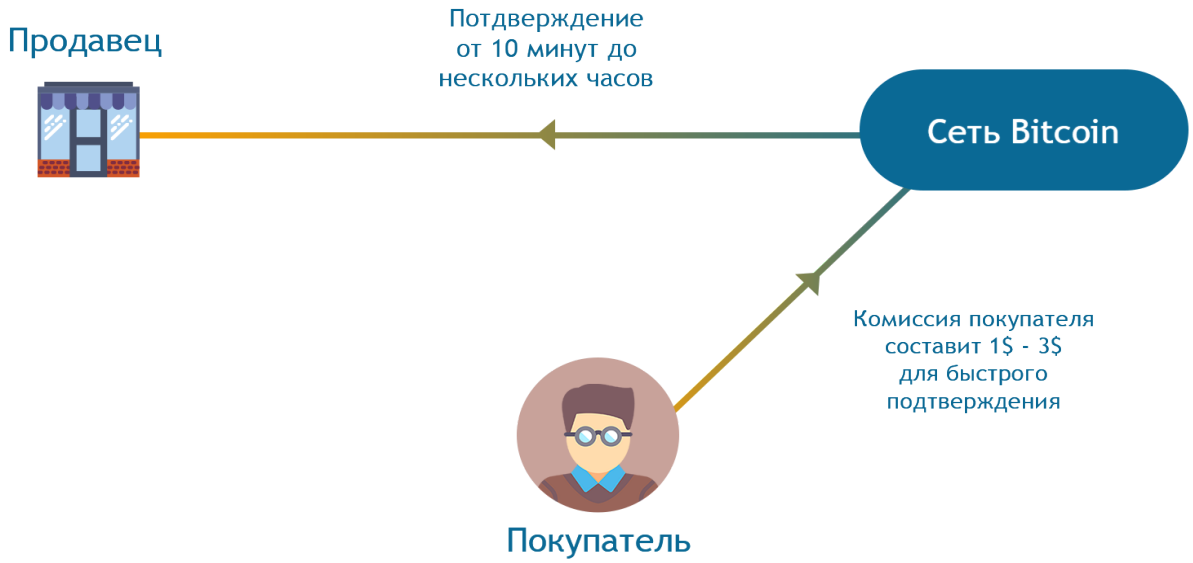

Рисунок 1: Транзакция Bitcoin без централизованного посредника.

Несмотря на то, что некоторые существующие криптовалюты и токены[2] имеют сокращенное время подтверждения, они все еще не способны конкурировать с основными моделями традиционных транзакций, такими как авторизация и завершение. Мы считаем, что эти модели способны увеличить принятие криптовалют розничными, гостиничными, и другими отраслями, где невозможно обойтись без быстрых платежных процессоров и шлюзов[3]. Сторонние шлюзы обработки транзакций заполняют этот пробел (Рисунок 2). Однако, само существование сторонних платежных шлюзов — противоречит фундаментальным принципам криптовалют, таким как децентрализация, приватность и независимость. Сторонние шлюзы обычно являются централизованными коммерческими организациями, регулируются правительством, а также контролируются акционерами.

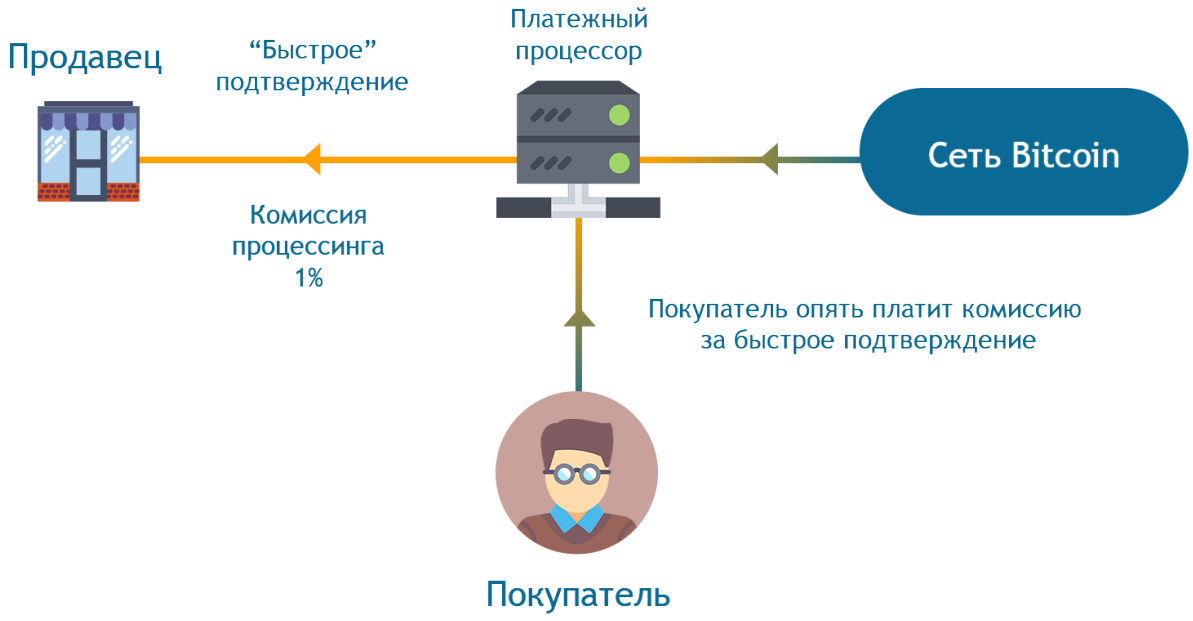

Рисунок 2: Обработка Bitcoin транзакции централизованным посредником.

Большинство продавцов не могут принимать криптовалюты без участия стороннего платежного процессинга из-за уникального способа обработки блокчейн транзакций. Этот процесс концептуально отличается от традиционных электронных платежных систем. Несмотря на некоторые недостатки традиционных платежных систем, технологии, которые разработаны вокруг них, накопили огромное количество торгового опыта, а также заработали пользовательское доверие.

Существует несколько больших отличий между традиционными и криптографическими платежными системами обработки транзакций, которые в большинстве случаев делают криптовалюты менее привлекательными для продавцов и покупателей. Вот список нескольких технических ограничений и недостатков существующих криптовалютных платежей по сравнению с традиционными платежными системами:

- Отсутствие основных моделей транзакций
- Неудобные платежные потоки
- Долгое время подтверждения
- Несбалансированные и непредсказуемые комиссии
- Невозможно обрабатывать микроплатежи и частые платежи (подписки)
- Отсутствие оффлайн-транзакций
- Малая масштабируемость
- Недостаточная безопасность
- Открытый блокчейн ограничивает конфиденциальность
- Отсутствие доверия между покупателем и продавцом
- Сомнительная практичность
- Неудобный интерфейс пользователя
- Отсутствие техподдержки

В попытке решить эти проблемы, цель GRAFT – создать платформу, которая позволит широко использовать криптовалютные платежи между покупателями и продавцами, сохранив при этом основные принципы криптовалют и токенов.

Назначение Децентрализованного Процессинга.

Почему у покупателя может возникнуть желание начать использовать криптовалюты или токены вместо (или в дополнение) пластиковых карт или платежных систем PayPal или Apple, и зачем продавцу использовать криптовалюты или токены в дополнение к (или вместо) существующим способам оплаты. Очевидно, что если мы не найдем ответы на эти простые вопросы, нет смысла в создании данного документа.

Если на первую часть этого вопроса нельзя ответить однозначно, ведь у покупателей может быть несколько причин использовать криптовалюты, то ответ на вторую часть вопроса относительно прост. Продавцы хотят расширить клиентскую базу для того, чтобы увеличить свои доходы. Если многие потенциальные клиенты предпочтут, по какой-либо причине использовать криптовалюту или токены, то продавцы начнут принимать их к оплате. Процессинговая система GRAFT дает уникальную возможность продавцам принимать платежи криптовалютой или токенами напрямую от своих клиентов, без посредников, и с низкой комиссией.

Поскольку процессинговая система GRAFT представляет собой децентрализованную платежную систему, она способна обеспечить платежные операции без использования сторонних криптовалют. Однако процессинговая система GRAFT будет поддерживать Биткоин, альткоины токены в качестве дополнительного способа оплаты для участников сделки. Это позволит продавцам отказаться от централизованных посредников, а покупателю не придется изучать и держать у себя различные криптовалютные кошельки.

Терминология

Выборки Авторизации

Выбранная группа полных супернод обрабатывает транзакции в реальном времени и гарантирует, что покупатель не сможет потратить средства дважды, пока транзакция не записана в блокчейн.

DAPI

Децентрализованный API, реализуемый супернодами для поддержки тонких клиентских приложений, таких как GRAFT Wallet, GRAFT Point of Sale, а также сторонних торговых приложений и платежных карт. Исходный код GRAFT SDK предоставляется сторонним разработчикам для облегчения интеграции GRAFT.

Брокер Конверсии

Протокол GRAFT размещается на суперноде или группе супернод. Конверсионный посредник реализовывает дополнительный функционал, который невозможно выполнить в полностью децентрализованной сети. Этот функционал требует специальной системы регулирования. Примером конверсионного посредника может служить Биткоин обменник или фиатный биржевой брокер.

Полная Супернода

Полная супернода – это независимый узел, постоянно подключенный к сети сервер, на котором выполняются: комбинированная нода блокчейна GRAFT; GRAFT DAPI нода; обработка авторизаций в реальном времени; обменные вызовы DAPI между покупателями, конверсионными брокерами, и продавцами; а также размещаются сторонние сервисы такие как мгновенный криптовалютный обмен с сетью GRAFT, прием банковских карт и выплаты

продавцам. Суперноды поддерживают второй уровень сети GRAFT, используя Proof of Stake алгоритм.

GRAFT

1. Глобальная сеть перевода средств с авторизациями в реальном времени, децентрализованная глобальная платформа с открытым исходным кодом. Она служит для обработки платежей в реальном времени, расчетов между участниками сделки и перевода средств. GRAFT - это устойчивый к анализу блокчейн, децентрализованный API, и открытое сообщество конверсионных брокеров, которые поддерживают различные методы оплаты, включая криптовалюты, токены, а также традиционные банковские карты и переводы.
2. Почему мы используем слово Graft? Растение, у которого есть веточка или бутон от другого растения связаны, и будут расти вместе.[4] Графтинг – это продвинутая техника, которую используют фермеры, садоводы, и любители, чтобы добавить часть одного растения другому.[5] Эта техника позволяет сочетать лучшие черты разных растений, для того, чтобы создать что-то лучшее и более ценное.

GRAFT Point of Sale

Приложение Graft Point of Sale – это “тонкое” мобильное и настольное приложение, которое позволяет продавцам принимать токены GRAFT, а также Биткоины, альткоины и банковские карты; выпускать подарочные сертификаты и выкупать их; реализовывать программы лояльности; настраивать удобный способ выплат для продавцов.

GRAFT Wallet

GRAFT Wallet – это “тонкий” кошелек, который доступен для персонального компьютера, смартфона, а также как расширение браузера. Приложение позволяет осуществлять переводы токенов GRAFT, токенов других криптовалют, а также привычных фиатных валют, используя GRAFT DAPI.

GRFT

Основной криптографический токен сети GRAFT, он работает в основном блокчейне и используется для авторизации транзакций в реальном времени, передачи средств и расчетов между участниками сделки.

Токен продавца

Определенный смарт-контракт, который позволяет продавцу создавать свой частный токен. Токены продавцов помогают реализовать важный функционал. Например, они могут быть использованы как токены для оплаты товаров (“стейблкоин”), а также для собственных бонусных систем, например программы лояльности, подарочные сертификаты, или скидочные купоны.

Платежный шлюз

Позволяет продавцам и поставщикам услуг управлять их платежным оборудованием, настраивать параметры (например, адрес кошелька), устанавливать комиссии, а также позволяет вести отчетность и аналитику транзакций.

Токены Выплат (“Стабильная цена”)

Представляют местную фиатную валюту. Они могут быть мгновенно переведены в блокчейн GRAFT, используя для этого суперноду. Токены выплат основаны на токенах продавца GRAFT, подобно подаркам, баллам, или другим типам токенов продавцов.

Прокси Супернода

Супернода упрощает торговые операции. Она связывает терминал продавца (POS), кошелек покупателя с одной стороны и остальную часть супернод для авторизации с другой стороны.

VChain

Виртуальная децентрализованная независимая сеть, где продавец может создавать торговые токены, устанавливать правила авторизации и выплат, а также настраивать различные события, которые будут влиять на транзакции конкретно этого продавца.

Комиссии за Транзакции

Почему взимаются комиссионные за обработку транзакций? В конце концов, за блокчейном не стоит коммерческое предприятие. Почему пользователь должен платить комиссию, кто их собирает, и сколько должен взимать сборщик этих комиссий?

Платить Комиссии или не Платить?

Для поддержания сети безопасных и доступных криптовалют и токенов требуются множество мощных серверов, которые работают по всему миру. Кто будет поддерживать эти сервера и зачем им это делать? Сети Биткоина и альткоинов финансируются майнингом и комиссиями сети. Майнеры зарабатывают деньги за добычу новых блоков, а также на комиссиях за каждую транзакцию.

У майнинга также есть и другая цель: постоянный выпуск новых токенов в системе, чтобы поддерживать ликвидность с растущим спросом на токены, по мере увеличения использования. По мере развития системы, владелец ноды получает больше доходов от комиссий в сети, поэтому награда за майнинг постепенно уменьшается с каждым новым блоком, а общая эмиссия ограничена.

В идеальном мире, переводы криптовалют или токенов могут быть доступны для каждого без комиссий. На самом деле существуют сети, которые обещают бесплатные транзакции.[6] В других сетях, включая Биткоин, комиссии используются для различного приоритета транзакций, таким образом, комиссии решают проблему масштабирования.

В сети GRAFT, комиссии включены по двум причинам:

Первая причина - злоупотребления в сети. Это касается проблем производительности сети, а также быстрый рост размера блокчейна. Если комиссии будут отсутствовать, то можно будет использовать реальную сеть для тестирования. Если транзакция полностью бесплатна, можно перемещать одну и ту же сумму между двумя адресами бесконечно.

Вторая причина – это будет единственный стимул для операторов узлов, после того как награда за майнинг станет очень маленькой.

Покупатель Не Должен Платить Комиссии.

Проблема комиссий Битокоина и других криптовалют в том, что комиссию платит отправитель. Это делает использование криптовалют менее привлекательным, чем использование обычных пластиковых карт. При оплате банковской картой комиссию за операцию платит продавец. За перевод криптовалют бремя комиссий сети ложится на отправителя. Продавцу также приходится платить комиссию централизованного платёжного процессора за обработку транзакции в криптовалюте. Обычный плательщик часто путается в этом процессе, который больше похож на лотерею и не дает возможности точного

планирования суммы комиссий, что, безусловно, делает криптовалютные платежи менее привлекательными.

Микроплатежи: Как Мне Заплатить за Чашку Кофе?

Еще одна проблема, с которой столкнулся Биткоин – это невозможность совершать микро-платежи из-за высоких комиссий.[7] GRAFT решает эту проблему, за счет уникального подхода к транзакционным сборам.

Комиссии за Транзакции GRAFT

В экосистеме GRAFT, **плательщик не платит комиссию**. Все комиссии оплачиваются получателем (продавцом). GRAFT делает микро-платежи доступными, за счет очень низких комиссий (по сравнению с банковскими картами, онлайн платежами, а также по сравнению с другими криптовалютами или токенами).[8]

Таблица 1: GRAFT Структура комиссий/вознаграждений за транзакции

		1	2	3
		Обычные P2P Переводы	**RTA Tx (GRFT)**	**RTA Tx с участием конверсионного брокера (например, чтобы принять bitcoin)**
a	**Вознаграждение Прокси Суперноды кошелька отправителя.**	0.1 GRFT *	0.05% *	0.05% *
b	**Вознаграждение Полной суперноды (участника выборки авторизации)**	Не применяется	0.0625% **	0.0625% **
c	**Вознаграждение Брокера конверсии**	Не применяется	Не применяется	0.25% **

d	**Вознаграждение Майнера**	Непостоянное, основывается на размере Tx в KB	Настраиваемое *** Мин: 0.1 GRFT	Настраиваемое *** Мин: 0.1 GRFT
e	**Вознаграждение POS/Платежного шлюза Прокси Суперноды продавца ******	Не применяется	0.05% ****	0.05% ****
	Общая комиссия отправителя Tx (покупатель использует RTA)	a1 + d1	0	0 *****
	Общая комиссия получателя Tx **(продавец использует RTA)**	0	a2 + b2*8 + d2 + e2	a3 + b3*8 + c3 + d3 + e3
	Общая сумма комиссий, начисленная отправителю Tx	Сумма Tx + a1 + d1	Сумма Tx	Сумма Tx
	Общая сумма, доступная получателю Tx	Сумма Tx	Сумма Tx – (a2 + b2*8 + d2 + e2)	Сумма Tx – (a3 + b3*8 + c3 + d3 + e3)

* Кошелек прокси суперноды может быть собственным сервером или публичным кластером обслуживаемый поставщиком услуг. Вы можете запустить и использовать собственную прокси суперноду чтобы полностью исключить комиссию ноды. Супернода должна внести залог, для того, чтобы взимать комиссии.

** Полной суперноде или посреднику конверсии требуется залог, для участия в RTA Tx, чтобы получать вознаграждения.

*** Устанавливается сервис провайдером продавца или владельцем POS прокси суперноды.

**** POS прокси супернода может быть собственным автономным сервером, частью торговой инфраструктуры, частью платежного терминала или шлюзом электронной торговли, который обслуживает сервис провайдер продавца.

***** Комиссии сети альткоинов не учитываются.

Награды Прокси Супернод (a1, a2, a3, e2, и e3 в Таблице 1) обеспечат полную децентрализацию сетевой инфраструктуры. Если вам не нравится кластер супернод, который обслуживает конкретный сервис провайдер, вы всегда можете выбрать альтернативный. Для получения награды, прокси супернода должна внести залог на кошелек, связанный с публичным IP адресом суперноды. Общая сумма залога составляет 250,000 GRFT.

В отличие от супернод авторизаций, прокси супернода может работать без доли, однако супернода без доли не сможет получать комиссионные. Эта опция сделана для возможности запуска частных прокси супернод. Таким образом, пользователи с повышенными требованиями к конфиденциальности могут размещать свои собственные точки входа в сеть. Без доли, вознаграждения прокси будут направлены на кошелек пожертвований сообщества GRAFT. Общая сумма комиссии, которая собирается из разных частей, всегда неизменна и не зависит от статуса супернод.

Фиксированная плата выплачивается майнерам за RTA транзакции (d2, d3). Комиссии майнерам традиционно рассчитываются из размера записи транзакции в KB (d1). Используя RTA, мы не можем сделать комиссию майнерам переменной, так как это сделает общую комиссию продавца непредсказуемой, что неприемлемо в большинстве случаев.

Кроме того, мы не можем сделать комиссию пропорциональной стоимости перевода (подобно комиссиям супернод) потому, что комиссии майнерам видны в блокчейне. Это значит, что сумма транзакции может быть рассчитана пропорционально комиссии (хотя мы можем исправить это в будущем). Поэтому, мы сделали простую фиксированную комиссию, минимум 0.1 GRFT.

Комиссии за RTA, а также переводы совместно с брокерами конверсии совпадают с комиссией RTA (столбец 2), 0.25% и берутся посредником (оплачиваются продавцом).

Комиссии Продавцов и Сервис Провайдеров

Сервис провайдеры продавца могут устанавливать комиссии, которые будут соответствовать их бизнес модели. Комиссии могут быть настроены опционально, например:

Транзакция менее $10: 2%
Транзакция более $10: 1%
Минимальная сумма транзакции: $1
Майнер: 0.1 GRFT

Транзакции в альткоинах: +0.25%

Мгновенные выплаты в альткоинах или фиатной валюте: +0.25%

Ниже приведен пример транзакции альткоина стоимостью $20 и сопутствующие комиссии с учетом установленной комиссии сервис провайдера продавца.

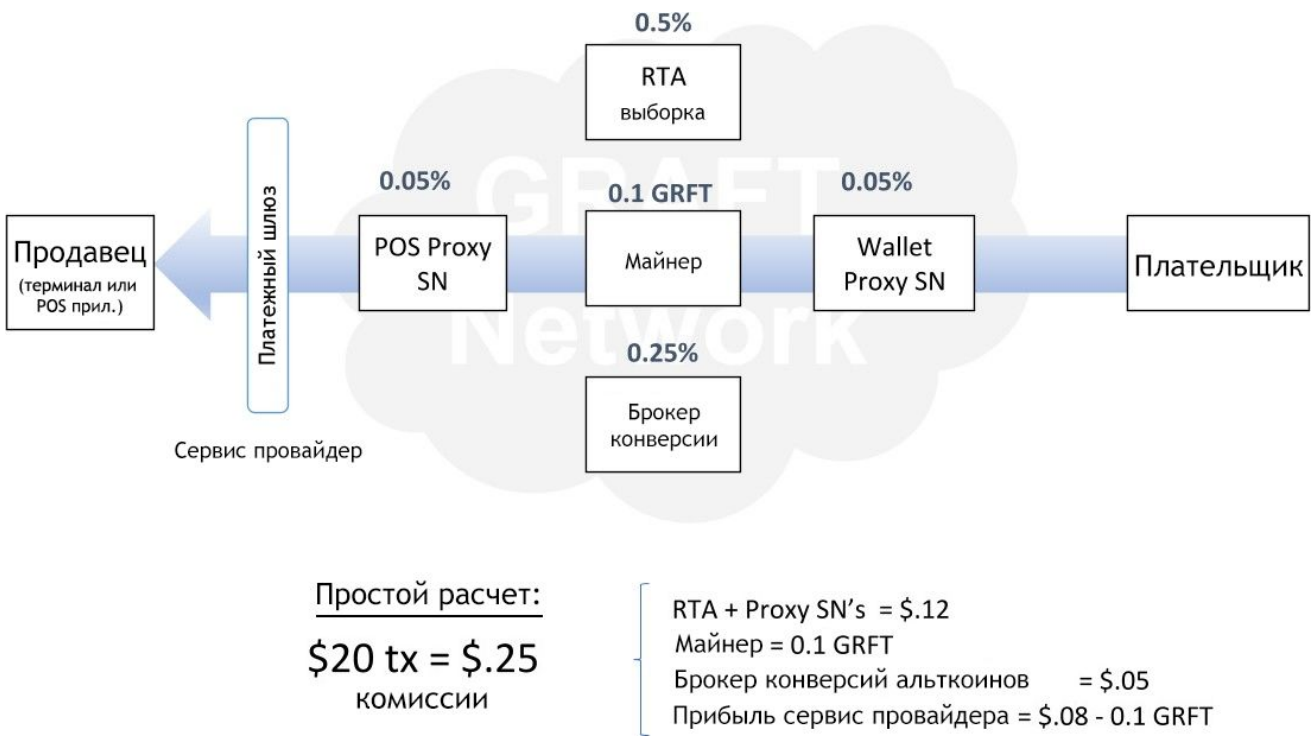

Рисунок 3: Пример Распределения Комиссий / Распределение Вознаграждений GRAFT

Бесплатные Денежные Переводы: Авторизированные Транзакции

Некоторые платежные сети, такие как Автоматизированная Расчетная Палата (ACH) или PayPal, предоставляют бесплатные переводы между учетными записями пользователей. Чтобы конкурировать с традиционными платежными системами GRAFT будет предоставлять ограниченные бесплатные переводы между подтвержденными кошельками пользователей. Криптовалютные сети обычно не могут "позволить" бесплатные переводы по трем основным причинам:

- Отсутствие стимула майнеров
- Угроза атак отказ в обслуживании (DDoS)

- Неконтролируемый рост блокчейна

GRAFT решает первую проблему путем разделения платежей и переводов. Суперноды и майнеры получают комиссии за моментальные регулярные платежи, которые составляют большую часть всех транзакций, в то время как бесплатные переводы обрабатываются с более низким приоритетом.

Вторая проблема решается добровольной идентификацией и авторизацией пользователя. Конечно, “бесплатный сыр бывает только в мышеловке”, поэтому пользователи будут “платить” собственной идентификацией для обеспечения разумного использования сети (ограничением количества и частоты бесплатных переводов пользователя). Таким образом, злоупотребление сетью становится невозможным. Использование технологии доказательства аутентификации с нулевым разглашением, позволяет пользователям подтвердить свою личность, не нарушая их приватность.

Для решения последней проблемы рассматривается несколько решений: малый интервал блока; неограниченный размер блока; ограничение количества бесплатных транзакции. Кроме того, одна из сторон бесплатного перевода должна быть проверена. Сторона должна доказать, что проводила “коммерческие” транзакции в прошлом.

Конфиденциальность

Зачастую возникает неправильное понимание необходимости приватности. На самом деле большинство легитимных клиентов готовы раскрыть личность продавцу, особенно если они извлекают из этого выгоду, или если раскрытие их личности необходимо для обработки транзакции. Аналогичным образом, покупатели хотят быть уверены, что продавец, которому они переводят деньги, является указанным получателем, а не мошенником. Ни продавец, ни покупатель, ни кто-либо еще не заинтересован в раскрытии их личности и доступа к деталям их операций, посредством анализа открытого блокчейна.

Конфиденциальность - это деликатная тема для криптовалют и индустрии платежей в целом. Конфиденциальность разнится от полной анонимности до полной прозрачности, на усмотрение продавцов и покупателей. У продавца, могут быть требования: собрать и проверить определенные личные данные, например возраст для покупки алкоголя или сигарет, или почтовый индекс для расчета налогов при онлайн торговле. С другой стороны

покупатель может согласиться или не согласиться раскрывать все или некоторые данные своей личности и должен иметь возможность выбирать, какую информацию о себе раскрывать. Если покупатель и продавец смогут договориться о раскрытии конкретных идентификационных данных, транзакция может быть обработана. Более того, в большинстве случаев продавцу необходимо проверить подлинность данных покупателя.

Мы считаем, что наилучший способ решения этой проблемы, является использование системы идентификации и проверки подлинности установленными государством регуляторами, ориентированные на повышение конфиденциальности (например, NIST 800-63 в США или GDPR в Европе) – стандарты, которые требуют дифференцированной проверки подлинности и аутентификации.[9]

GRAFT будет внедрять цифровой персональный профиль, который будет привязан к GRAFT Wallet. Покупатель сможет делиться личными цифровыми данными с контрагентом, на основе своих предпочтений на момент сделки. Эти предпочтения включают различные атрибуты (такие как возраст, место проживания, почтовый адрес, и другие) и могут разниться для каждой транзакции.

GRAFT использует **CryptoNote**[10] в качестве протокола записи транзакций, который обеспечивает высокий уровень конфиденциальности по сравнению с Биткоином, другими криптовалютами, и токенами, скрывая информацию об отправителе и получателе транзакций.

Почему Необходим Приватный Блокчейн?

Ключевой инновацией Биткоина является открытый блокчейн, доступный для всех. Это дает возможность проверки транзакций, чтобы убедиться в отсутствии двойной траты. Но это также означает, что любой человек в мире может посмотреть транзакции и балансы на любом кошельке.

В отличие от пластиковых карт, кошельки Биткоина напрямую не связаны с личностью владельца. На первый взгляд, эта функция компенсирует тот факт, что все записи транзакций записаны в блокчейне, и каждый может их посмотреть. Однако существуют методы, которые позволяют наблюдателю связывать адреса с личностями[11]. Если это происходит, то все ваши транзакции становятся видимыми в публичном блокчейне. Транзакции не могут быть удалены или стерты.
Протокол CryptoNote необходим, чтобы конкурировать с традиционными платежными системами. Такими, как Visa или PayPal, которые фактически, гораздо лучше обеспечивают конфиденциальность своих пользователей, чем большинство существующих криптовалют.

Когда вы вставляете вашу карту в терминал оплаты или нажимаете кнопку “Оплатить с помощью PayPal” о вашей операции знают только два объекта во всем мире: Платежная сеть (Visa или PayPal в нашем случае) и продавец. На самом деле, конечно же, больше организаций знают о вашей транзакции. Платежные сети устроены несколько сложнее, чем кажется на первый взгляд. Этот список, по крайней мере, включает в себя банк эмитент (банк, выпустивший вашу карту), банк эквайринг (банк, который подтверждает ваш платеж), платежный шлюз (шлюз, который направляет вашу транзакцию на правильный платежный процессор/эквайринг банк), и платежный процессор (который обрабатывает платежи и выплаты продавцу). Однако, список этих организаций ограничен и все они соблюдают регламенты безопасности и конфиденциальности, а также реализуют серьезный контроль безопасности. Это защищает ваши транзакции от посторонних глаз. Разумеется, эти организации могут быть взломаны или могут передавать информацию правоохранительным органам. Давайте упростим. Предположим, что обычные люди не могут получить доступ к транзакциям вашей банковской карты в большинстве случаев, чего нельзя сказать о большинстве блокчейнов.

CryptoNote как Основа Конфиденциальности

CryptoNote отличается от других протоколов блокчейна. Он предоставляет нам главное: конфиденциальность. В вопросах обмена ценностей мы воспринимаем конфиденциальность как неотъемлемую часть, как должное, и потеря конфиденциальности может привести к негативным последствиям. Иронично, но Биткоин и его производные сделали шаг назад в области конфиденциальности по сравнению с более ранними платежными системами, такими как наличные деньги или банковские карты, которые в свою очередь, стали символом угрозы безопасности и конфиденциальности. Создатель Биткоина, возможно не думал о конфиденциальности или ему просто не хватило времени для решения всех проблем, что абсолютно понятно. Ему нужно было решить более важную проблему: реализовать технологию блокчейн.

CryptoNote сохраняет все преимущества технологии блокчейн, которые хорошо известны, но при этом “возвращает” потерянные функции конфиденциальности: **неотслеживаемые платежи, несвязанные транзакции**, **устойчивость блокчейна к анализу**, и **конфиденциальные суммы сделок**. Кроме того, GRAFT, для полной картины, добавляет конфиденциальность суммам комиссий сделки. CryptoNote создает идеальный фундамент для создания множества самых разнообразных функций для всей отрасли, которые обнаружил GRAFT, чтобы завоевать мир платежей.

Конфиденциальные Транзакции

GRAFT использует несколько криптографических механизмов, разработанных разработчиками CryptoNote и Monero для того, чтобы, информация о транзакциях была видна только владельцам этой информации:

Одноразовые “Невидимые” Адреса

Вместо отправки платежа напрямую на адрес получателя, для каждой транзакции создается уникальный одноразовый ключ назначения. Этот ключ криптографическая производная публичного ключа получателя, таким образом, это предотвращает привязку ключа к адресу или другим ключам. Таким образом, **получатель может опубликовать один адрес и получать неотслеживаемые платежи. Ни один наблюдатель не сможет определить были какие-нибудь транзакции отправлены на этот адрес** или связать адреса между собой.

Одноразовые Кольцевые Подписи

Эти подписи **запутывают личность отправителя**. Каждая транзакция в любом блокчейне подписывается приватным ключом отправителя. С помощью этого ключа сеть подтверждает подлинность транзакции. Вместо создания одной подписи создается несколько подписей (кольцо) и все эти подписи действительны, поскольку это выходы от других отправителей. Однако наблюдатель не может определить, кто является настоящим отправителем. Сеть не знает, какой конкретно выход является скрытым среди других подписей в кольцевых подписях. Вместо этого сеть проверят, что ни один выход из всего кольца не был потрачен более одного раза, что эффективно предотвращает двойную трату.

Кольцевые Конфиденциальные Транзакции

Кольцевые Конфиденциальные транзакции **делают суммы транзакций невидимыми в блокчейне.** Сумма транзакции шифруется отправителем. Только получатель может расшифровать сумму транзакции. Сторонние наблюдатели не могут расшифровать сумму, но они могут проверить, что деньги не были потрачены более одного раза и, что в этой транзакции не было создано «новых денег».

Обработка Транзакций

Мир движется к “тонким” устройствам. Люди во всем мире используют больше смартфонов и планшетов, нежели ноутбуков и настольных компьютеров. Поэтому мы считаем, что лучшая модель для криптографических платежных систем будет основываться на небольших

индивидуальных узлах. Суперноды будут базироваться на мощных компьютерах, и обслуживаться профессионалами. Пользователи будут использовать тонкие клиенты, которые будут соединиться с группой случайных супернод, через вызовы DAPI, для предотвращения мошенничества.

Проблема Долгого Подтверждения: Вводим Авторизации в Реальном Времени.

Длительное время подтверждения.[12] (От нескольких минут до нескольких часов, в зависимости от суммы комиссии) одна из основных причин недостаточного принятия криптовалют и токенов в секторах розничной торговли и гостиничном бизнесе. Клиентам не нравится долгое время ожидания, а продавцам необходима мгновенная обработка платежей. В отличие от других криптовалютных сетей, которые пытались решить эту проблему внедряя специальные дополнительные механизмы обработки, GRAFT будет обрабатывать все платежи в “реальном времени” (мы ожидаем, что большинство транзакций будут завершены менее чем за 3 секунды.). Очень важно, что GRAFT реализует моментальные платежи без дополнительных комиссий для клиента.

Это достигается за счет использования консенсуса супернод (выборки авторизации) с использованием распределенной блокировки средств на аккаунте покупателя и получением ответа в течение нескольких миллисекунд. Суперноды также следят за сетью GRAFT, поэтому никакие транзакции не будут одобрены “вне сети”.

Суперноды

Все транзакции обрабатываются сетью за счет постоянно активных супернод GRAFT в реальном времени. Комиссии супернодам, которые участвуют в авторизации, а также (опционально) посреднику конверсии, оплачивает получатель платежа (продавец).

Владельцы супернод несут ответственность за любые транзакции, которые они обрабатывают. Такая ответственность достигается за счет финансового интереса владельца (комиссии за транзакции).

DAPI

В отличие от обычных API интерфейсов, размещенных на обычных серверах или кластере, DAPI не имеет единого адреса, потому, что работает на большом количестве супернод. Любой единственный узел, может обслужить вызов DAPI в любое время. Суперноды не

поддерживают постоянный сеанс с клиентом, и все данные для обработки мгновенно распределяются по всем доступным узлам в сети. Клиентское приложение, которое использует DAPI, хранит список прокси супернод, с которыми взаимодействует. Тем не менее, клиентское приложение может выбрать любую доверенную суперноду и “придерживаться” этого узла. Например, продавцы могут размещать на своем собственном оборудовании прокси суперноду, которой они будут доверять. Такая супернода не сможет участвовать в авторизации транзакции из-за ограниченных ресурсов (см. алгоритм выбора авторизаций ниже), она лишь предоставляет дополнительный уровень конфиденциальности своему владельцу.

Подтверждение в Реальном Времени Выборками Авторизации

Существуют криптовалюты с (расчетным) временем блока менее двух минут. Однако сокращение этого интервала не делает эти транзакции “моментальными”. Схема супернод GRAFT решает эту проблему, используя выборку авторизации. Подтверждение происходит моментально благодаря группе супернод. Такое решение гарантирует, что покупатель не сможет потратить средства более одного раза, пока транзакция не подтвердится (не будет записана в блокчейн). Вычисления (майнинг), типично занимают несколько минут.

В отличие от большинства криптовалют, и аналогичных систем оплаты, каждый платеж в сети GTAFT разделен на два этапа: авторизация и подтверждение.
Как и в привычных мировых платежных системах, авторизация происходит моментально, тогда, как подтверждение выполняется позже, обычно в течение двух минут (в привычных для нас платежных сетях подтверждение может занимать несколько часов или даже несколько дней).

Блокировка Аккаунта для Авторизации.

Механизм “образ ключа” используется в протоколе CryptoNote для проверки новых транзакций и предотвращения двойной траты, не нарушая конфиденциальности отправителя. Образ ключа – это одноразовый уникальный отпечаток, который создается для каждой транзакции, не раскрывая при этом адрес отправителя и сумму транзакции. Так как образ ключа уникален для каждой транзакции, майнеры могут легко проверить, происходит ли двойная трата при участии конкретной монеты. Предоставляя уникальный образ ключа для предстоящей транзакции в сеть супернод, кошелек покупателя временно блокирует счет отправителя, при этом никакая другая транзакция с таким же образом ключа (этой учетной записи) не сможет пройти до тех пор, пока транзакция не подтвердится и не снимется

блокировка. Если покупатель пытается завершить транзакцию с образом ключа, который отличается от образа блокировки, транзакция будет отклонена супернодами.

Образ ключа не содержит никакой информации о покупателе или его кошельке, такой подход обеспечивает безопасность, анонимность и не дает возможности отслеживать транзакции. В дополнение к этому все следы связи между покупателем (приложение Graft Wallet), продавцом (приложение Point of Sale), и супернодами (ретрансляторы и выборки супернод) во время фазы авторизации будут удалены после подтверждения транзакции (записаны в блокчейн и подтверждены 10-ю блоками)

Уровни супернод

Узел в сети GRAFT называется “супернода”, потому, что он выполняет больше функций, чем обычные узлы в привычных блокчейнах. Это повышает требования к владельцам супернод. В это же время GRAFT это открытая и децентрализованная сеть, где каждый может запустить суперноду, поэтому существуют разные уровни супернод с разными условиями и вознаграждениями на каждом уровне.

Прокси Супернода это “начальный уровень” — кто угодно может установить программное обеспечение и разместить суперноду. Прокси супернода предоставляет следующий функционал:

- Доверенный ретранслятор для тех, у кого повышенные требования конфиденциальности. Они могут развернуть свой собственный “сервер-кошелек”;
- Для крупных торговых сетей в роли “сервера магазина”, тем самым, они могут повысить скорость обработки транзакций.
- В качестве публичного “выходного узла”, который соединяет мобильные кошельки с точками продаж в сети GRAFT (потребуется публичный IP адрес). Публичная прокси супернода может получать вознаграждения, если у нее есть ставка.

Полные суперноды

Выполняют функцию авторизаций транзакций и также являются поставщиками услуг. Чтобы использовать полный функционал необходимо связать залоговый баланс доли с адресом суперноды. Комиссии за транзакции платятся полным супернодам, имеющим долю, если она участвует в RTA.

Майнинг Узлы

В то время как второй уровень сети GRAFT, состоящий из Proof of Stake супернод, которые выполняют функции авторизации и обмена, первый уровень сети состоит из узлов Proof of Work (POW) и выполняет функцию вычислений, путем создания новых блоков и добавлением их в блокчейн.

Расчет Вознаграждения за Майнинг

Майнинг узлы получают вознаграждения за создание блоков (POW), а также комиссии за обычные транзакции и RTA транзакции.

Расчет Вознаграждения (в RTA Tx): Непостоянные

Определяется поставщиком услуг продавца через платежный шлюз, но не может быть ниже, чем 0.1 GRFT.

Комиссии майнеров (не-RTA переводы): Непостоянные

Непостоянные, основаны на размере Tx в KB.

Майнинг (Создание токенов) Награда за блок

Награда за найденный блок платится узлу, который сможет первым найти новый блок. Награда за блок постепенно уменьшается с каждым новым блоком, используя следующую формулу: (M – A) * 2-19 * 10-10 / 2, где A = текущая эмиссия и M = общая эмиссия (264 − 1) в атомных единицах (10-10). Идея заключается в том, что в будущем будет больше транзакций, которые смогут обеспечить стабильный доход майнеров за счет комиссий.

Уровни Полных Супернод

GRAFT реализует 4-х уровневую модель стейкинга. Чем выше уровень суперноды, тем больше шанс быть выбранным для авторизации транзакций, но при этом процесс выбора остается случайным.

50,000 GRFT – уровень 1

90,000 GRFT – уровень 2

150,000 GRFT – уровень 3

250,000 GRFT – уровень 4.

Каждый уровень участвует в случайном отборе 2 супернод (где N это уровень суперноды). Таким образом, уровень 4 имеет больше шансов быть выбранной из-за ограниченного количества супернод 4-го уровня. “Свободные места” заполняются нодами более высокого уровня (или более низкими при отсутствии супернод высокого уровня). Этот алгоритм также адаптивен, так как он будет “регулировать” среднее количество полных супернод на каждом уровне.

Делегированные доли

Балансы нескольких кошельков могут быть “делегированы” в одну полную суперноду, чтобы сформировать общую сумму залога. Доходы распределяются между кошельками в соответствии с их долей участия. Минимальный баланс для делегированной доли составляет 5,000 GRFT.

Выборка Авторизации

Чтобы выполнять авторизацию в реальном времени, сеть GRAFT опирается на выборку авторизации. Это группа выбранных доверенных супернод, которые будут “представлять” сеть и проверять транзакции; предотвращать двойные траты; разрешать мгновенные транзакции прежде, чем они будут “подтверждены” в блокчейне GRAFT (т.е. прежде чем они попадут в блок, и блок будет добавлен в блокчейн).

Выборка авторизации, состоит из восьми супернод, случайно выбранных из динамического списка супернод. Выбор происходит случайно, в то время как результат детерминистический для тех, кто считает формулу. Владелец суперноды должен держать залоговой баланс в связанном с супернодой кошельке. Минимально необходимый баланс 50,000 GRFT.

Когда новый запрос транзакции инициируется торговой точкой продавца, ему назначается текущий номер блока, который определяет выборка авторизации. Номер может увеличиться во время выполнения транзакции, но он не может измениться после назначения номера, который был первоначально назначен транзакции. Прокси супернода продавца, которая первоначально формирует запрос на транзакцию, делает выборку супернод. Эта выборка проверяется каждым членом выборки, а также прокси-сервером кошелька.

Чтобы ускорить процесс авторизации, приложение торговой точки может дать указание супернодам выборки авторизации игнорировать ответы из остальной части выборки, как

только приложение получит более 50 процентов одобренных ответов от “самых быстрых” супернод и при условии, что не будет отклоненных ответов.

Прокси Суперноды

Любая супернода из выборки авторизации может быть также прокси супернодой - ретранслятором, которая облегчает обработку транзакций продавца. Она связывает торговую точку продавца, кошелек покупателя с одной стороны, и остальные суперноды выборки авторизации с другой. Прокси супернода может быть выбрана случайным образом торговой точкой или кошельком из текущей выборки авторизации, связанного с транзакцией. Точка продаж или кошелек также может выбрать любую суперноду, которая не является частью выборки. На самом деле, продавец или клиент могут размещать свои собственные прокси-суперноды, если они ищут дополнительный уровень безопасности и конфиденциальности. Прокси-супернода может получать вознаграждение за обработку транзакций, если внесет сумму залога на кошелек.

Вознаграждения Суперноды

Каждая супернода получает долю комиссии за каждую транзакцию, которую она обрабатывает. Вознаграждение выплачивается получателем (продавцом).

Вознаграждение Полной Суперноды RTA (любые RTA Tx): 0.5%.
Одна восьмая часть этой платы, или 0.0625% от общей суммы RTA Tx, идет на каждую полную суперноду, участвующей в выборке авторизации RTA.

Вознаграждение Прокси Суперноды (любые RTA Tx): 0.1%
Половина этой платы, или 0,05% от общей суммы RTA Tx, идет на каждый супер-узел в прокси-паре, который обеспечивает подключение к сети (Wallet и POS прокси-суперноды).

Вознаграждение Wallet Прокси Суперноды (не-RTA переводы): 0.1 GRFT.
Эта комиссия будет взиматься прокси супернодой с мобильного или настольного кошелька отправителя в дополнение к существующей комиссии сети (вознаграждение майнера).

Масштабируемость

Масштабируемость для платежной системы – это возможность обрабатывать большое количество транзакций одновременно без падения производительности. В сети GRAFT интервал создания блока равняется двум минутам, размер блока не ограничен. Блоки

создаются часто, и каждый блок вмещает много транзакций. Такие меры не являются уникальными, и используются также в других криптовалютах. Тем не менее, GRAFT поддерживается быстрыми супернодами и авторизует транзакции моментально.

Каждая супернода не только хранит самую актуальную копию блокчейна, но также хранит список всех ожидающих запросов авторизации и завершенных транзакций, пока они не добавлены в блокчейн. Такая двухуровневая архитектура позволяет сглаживать большие всплески активности (например, сезонные или связанные с какими-то событиями увеличения активности покупателей и продавцов).

Оффлайн Подтверждение Транзакций

Люди, которые знакомы с обработкой платежных карт, знают, что иногда транзакция может быть одобрена продавцом без одобрения банка. Это называется автономным разрешением или автономной авторизацией, иногда S&F ("store and forward"). Такая оффлайн авторизация отправляется на сервер, при первом подключении к сети.

Однако криптовалютные платежные сети должны быть онлайн 24/7, круглосуточно и без перерывов.
Это предположение не совсем верно. В некоторых случаях продавец готов взять на себя риск и одобрить транзакцию автономно. Риск единичного возврата платежа ниже, чем риск потерять клиентов. Обычно есть предел суммы для автономных авторизаций. Когда система достигнет этого предела (максимальный риск), она прекращает выдавать автономные авторизации, пока не подключится к сети. Но в случае короткого отключения от сети, автономную авторизацию могут не заметить, ни продавец, ни покупатель.

Основываясь на тех же принципах, торговое приложение GRAFT Point of Sale и одиночная прокси супернода могут обрабатывать транзакции автономно, если не могут связаться с выборкой авторизации. Это возможно только в том случае, если продавец готов взять на себя такой риск. Решение об автономном подтверждении будет основываться на рейтинге покупателя и суперноды.

Платежные Шлюзы для Продавцов и Поставщиков Услуг

Важной частью в экосистеме GRAFT является Поставщик Торговых Услуг (MSP). Роль поставщика услуг заключается в подключении и поддержке платежной сети продавца,

обеспечение ее бесперебойной работы (обычно называется «Соглашение об уровне сервиса» или SLA). Поставщик услуг может предоставлять и обслуживать оборудование (например, платежные терминалы).
Чтобы тут можно было применить MSP, нужен другой тип сервера, например, который сможет:

- Управлять конфигурацией терминала (например, адресом кошелька).
- Обрабатывать характерные для MSP комиссии (MSP может выбирать разные уровни сервиса, или брать разные комиссии за разные суммы транзакций).
- Вести отчеты и аналитику для продавцов.

Такой платежный шлюз может быть создан и внедрен третьей стороной, такой как традиционный платежный процессор, который хочет добавить криптовалютные платежи в список своих услуг.
GRAFT создает “эталонную реализацию”, для быстрого внедрения, в рамках стратегии выхода на рынок.

Поскольку GRAFT является децентрализованной платежной сетью, платежный шлюз - это многопользовательское приложение с несколькими экземплярами. Его исходный код открыт, поэтому любой желающий может разместить свой собственный платежный шлюз и стать поставщиком услуг сети. Платежный шлюз – это “пятый элемент” который должен управлять платежными приложениями GRAFT на аппаратных терминалах и интерфейсах электронной коммерции GRAFT, а также связывать их с супернодами. Поскольку платежный шлюз видит операционную деятельность, то он считаются частью бэк-офиса продавца.

Типы Транзакций и Потоки Платежей

GRAFT вводит следующие типы и потоки транзакций, в целях упрощения торговых транзакций, а также поддержки существующих торговых приложений (Point-of-Sale).

Авторизация

Авторизация используется, когда окончательная сумма транзакции неизвестна на момент начала продажи. Например, оплата топлива на заправке, аренда автомобиля, резервация номера в отеле или оплата счета в ресторане.

Это аналогично авторизациям банковской карты. Авторизацию транзакции начинает продавец, затем ее подтверждает плательщик. Счет плательщика временно блокируется на

сумму и продолжительность (количество блоков), запрошенную получателем и подтвержденную плательщиком, до тех пор, пока сумма не будет подтверждена “Завершением” транзакции. Блокировка авторизации также может быть снята операцией “Отмена” инициированной получателем, прежде чем выйдет срок. Заблокированные средства плательщика автоматически освобождаются сетью, после истечения срока, если получатель не потребовал их, отправив запрос на “Завершение” транзакции.

Предварительная Авторизация

Предварительная авторизация похожа на долгосрочную авторизацию, но отличается тем, что плательщик не гарантирует, что средства будут доступны во время завершения транзакции. Предварительная авторизация – это долгосрочный контракт между плательщиком и получателем. В отличие от обычной авторизации, которая не может быть отменена отправителем, предварительная авторизация может быть отменена в любое время путем перемещения средств со счета, связанного с транзакцией предварительной авторизации.

Предварительная авторизация подходит для долгосрочных платежей, такие как ежемесячная абонентская плата или посуточная оплата номера в гостинице. Получатель уточняет (а плательщик подтверждает) максимальную сумму каждого платежа, общее количество платежей и минимальный интервал между платежами.

Завершение

Завершение окончательно проводит транзакцию, которая начиналась с авторизации или предварительной авторизации. Фактическая сумма завершения может быть меньше, чем ранее авторизованная сумма. Возможно несколько завершений, но общая сумма не может быть больше суммы авторизации.

Завершение используется после того, как прежде авторизированная транзакция завершается и известна точная сумма. Например, оплата топлива после заправки, оплата по чеку за аренду автомобиля, оплата счета гостиницы перед выездом или оплата ресторана после трапезы.

Продажа

Продажа авторизуется и завершается автоматически сетью как одна транзакция. Продажа – это типичная транзакция продавцу онлайн магазина или магазина в торговом центре.

Перевод

Перевод используется для перевода средств между аккаунтами сети GRAFT. По сути это то же самое, что и продажа, но может быть инициирована отправителем, без согласия получателя. Переводы можно использовать для p2p платежей, переводов на биржу и переводов между разными аккаунтами сети.

Отмена

Отмена используется для отмены авторизации и освобождает авторизированные средства (снимает блокировку суммы).

Выпуск

Выпуск активирует предоплаченную карту GRAFT, подарочный сертификат, карту лояльности, баллы магазина, или купон на скидку.

Погашение

Погашение позволяет оплачивать, используя предоплаченную карту, подарочный сертификат, карту лояльности, баллы магазина, или купоны на скидку, ранее выпущенный сетью GRAFT.

Конверсия

Конверсия используется для обмена средств между токенами GRAFT и другими криптовалютами, токенами, или фиатными валютами используя лучшие предложения супернод.

Расписание

Расписание используется для запланированных транзакций. Транзакции можно откладывать на более позднее время или дату. Эта функция требует дополнительного согласия пользователя.

Депонирование

Депонирование используется для хранения средств, до определенного события, когда средства будут освобождены.

Возврат

Операция возврата возвращает средства выбранной транзакции. Для операции возврата требуется разрешение продавца.

Обработка Транзакций с помощью токенов GRAFT в качестве оплаты

В отличие от Биткоина, других криптовалют и токенов, а также платежных карт, запрос транзакции формируется получателем (продавцом). Исключение составляет перевод и конверсия, эти операции инициируются отправителем. В отличие, от банковских карт запросы платежей явно подтверждает покупатель, с помощью приложения GRAFT Wallet, затем транзакция подписывается и отправляется в сеть. Единственным исключением является функция "Выкуп" при использовании бумажного или пластикового подарочного сертификата или купона, который может быть отсканирован платежным приложением продавца, если клиент не использует мобильное приложение или аккаунт GRAFT.

Обработка Транзакций с Помощью Альтернативных Способов Оплаты.

Чтобы обеспечить лучший пользовательский опыт и лучшие курсы обмена для продавцов, GRAFT может конвертировать различные криптовалюты, токены, а также фиатные валюты через приложение GRAFT Wallet. Комиссии за обмен и обработку платежей (оплачиваются продавцом в токенах GRAFT) могут применяться в дополнение к стандартным комиссиям GRAFT. Мы рассчитываем, что эти комиссии будут оплачиваться продавцом и будут незаметны для плательщика, поэтому способ оплаты не окажет влияния на итоговую стоимость покупки. Автоматическая конверсия в сети GRAFT поможет использовать криптовалютные платежи тем пользователям, которые недостаточно знакомы с экосистемой криптовалют или токенов. Например, пользователям, которые используют традиционные методы оплаты, но при этом хотят полностью сохранить свою анонимность.

Если покупатель решил оплатить с помощью криптовалют, токенов, или банковской карты, то сеть GRAFT автоматически обменяет средства в токены GRAFT. Это происходит моментально при участии брокеров конверсии. Брокер конверсии запускает суперноду и несет ответственность за выполнение обменных сделок, принимает оплату от покупателя и совершает выплаты продавцам. Если покупатель решил оплатить с помощью криптовалют, токенов, или банковской карты, то супернода автоматически выбирает лучшее предложение

для обмена среди всех посредников конверсии, основываясь на предыдущем выборе продавца, а также на основании лучшего обменного курса и рейтинга.

Брокеры Конверсии

Если оба участника сделки хотят использовать для расчета токены GRAFT, то сеть GRAFT автоматически мгновенно спишет токены со счета покупателя и зачислит на счет продавца.
Однако если клиент хочет оплатить другим способом оплаты, или продавец хочет получить оплату в другой валюте, то сети GRAFT придется использовать специальный механизм.

Чтобы облегчить процесс обработки платежей, которые не могут быть обработаны сетью самостоятельно, но при этом востребованы клиентами и продавцами, сеть GRAFT предоставит брокера конверсии.
Всякий раз, когда сеть GRAFT самостоятельно не может выполнить операцию полностью или частично, она будет делегировать эту операцию брокеру конверсии. Продавцы могут выбрать единственного (например, самого надежного или более выгодного) брокера или группу брокеров.

Брокер конверсии отвечает за обеспечение безопасности и ему необходимо соблюдать правила обработки платежных карт, включая требования PCIDSS, а также правила для борьбы с отмыванием денег.[13]

Ниже перечислены типы брокеров конверсии:

Посредники конверсии со стороны продавца(POS):

- Брокер приема платежей
- Брокер выплат платежей

Брокеры конверсии со стороны покупателя(Wallet):

- Брокер взаимообмена
- Брокер пополнения

Брокеры конверсии криптовалют будут доступны для каждой крупной криптовалюты, которая есть на https://coinmarketcap.com/, начиная с первых “топ-10” по рыночной капитализации. Брокеры повысят ликвидность каждой криптовалюты, включив различные варианты оплаты для участников сделки.

Брокеры конверсии криптовалют будут реализованы в сотрудничестве с существующими, а также новыми биржами. В конечном итоге, будет доступно множество брокеров для различных криптовалют. Они смогут конкурировать и будут обеспечивать лучшие курсы и сервисы. Автоматические процессы регистрации, выбора и конверсии сохранят децентрализованный характер сети. Каждый набор включает в себя четыре брокера конверсии для каждой криптовалюты.

Брокеры приема платежей и брокеры выплат работают с приложением GRAFT POS, а также с аппаратными платежными терминалами. Они позволяют продавцу принимать выбранную им криптовалюту при оплате через приложение GRAFT Wallet или других криптовалютных кошельков.

Брокеры взаимообмена и пополнения работают с приложением GRAFT Wallet и позволяют покупателю использовать любую удобную криптовалюту, как способ платежа. С помощью GRAFT Wallet покупатель может оплачивать покупки не только на любом терминале оплаты, который подключен к GRAFT DAPI, но и на кошельки других криптовалют.

Брокер Приема Платежей

Брокер приема платежей позволяет принимать способы оплаты отличные от токенов GRAFT. Он моментально конвертирует сумму платежа в токены GRAFT, затем отправляет средства на счет продавца. Брокер приема платежей работает в реальном времени и становится частью сделки между покупателем и продавцом. С точки зрения покупателя, оплата похожа на обычную транзакцию его криптовалютного кошелька.

Брокер приема платежей работает с приложением GRAFT POS. С его помощью продавец сможет принять криптовалюту, даже если у покупателя нет приложения GRAFT Wallet. В этом случае комиссию сети выбранной криптовалюты оплачивает покупатель. Если покупатель будет использовать GRAFT Wallet, то кошелек автоматически распознает GRAFT POS и конвертирует транзакцию в GRAFT. В этом случае продавец моментально получает токены GRAFT (Если задействовать брокера выплат, то выплата продавцу может быть произведена в любой другой криптовалюте или фиатной валюте).

Примеры брокера приема платежей:

- Bitcoin брокер принимающий платеж
- Ether брокер принимающий платеж
- CreditCard брокер принимающий платеж

Экономическая структура Брокера Приема и Выплат Платежей

Брокер приема платежей идет на риск, принимая криптовалютный платеж, моментально отдавая токены GRAFT взамен (не дожидаясь подтверждений транзакции другой криптовалюты). Этот риск для брокера смягчается относительно небольшими суммами розничных транзакций и попадает под действие выборки авторизации, подтверждающего транзакцию, и проходит через сеть выбранной валюты. Риск продавца также смягчается эквивалентной облигацией транзакции GRAFT равной сумме выплаты, которая генерируется брокером в начале транзакции. Облигация хранится выборкой авторизации до тех пор, пока брокер не одобрит платеж альткоинов продавцу. Как только транзакция альткоина (от покупателя к брокеру) будет получена и подтверждена, выборка авторизации подтверждает платеж продавцу и освобождает выплату GRAFT (от брокера к продавцу). Брокер может устанавливать разные лимиты для разных сумм и уровней риска.

В обмен за эту услугу, брокер получает 0.25% комиссии от платежа GRAFT продавцу, тогда как суперноды участвующие в авторизации, берут свою стандартную комиссию GRAFT (0.5%)

Рисунок ниже наглядно показывает последовательность обработки Биткоин транзакции брокером приема платежей. Продавец получает выплату в токенах GRAFT.

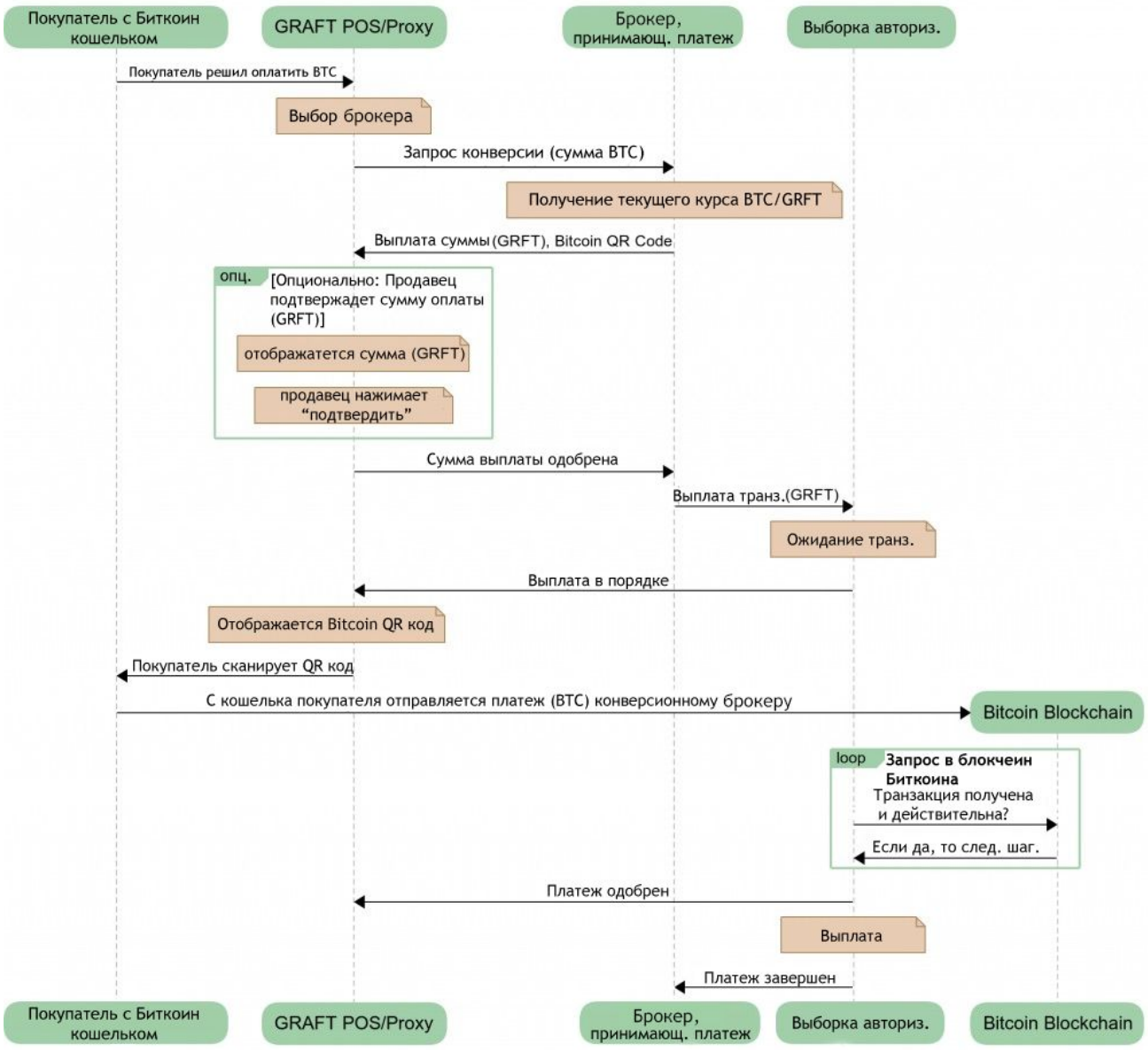

Рисунок 5: Схема транзакции брокера приема платежа GRAFT и Bitcoin

Брокеры выплат платежей обменивают GRAFT на валюту по выбору продавца. Транзакция является асимметричной – это означает, что на втором этапе платежа может пройти много времени перед тем, как ее получит сторона получателя. Брокер заключает облигацию, которая эквивалентна сумме выплаты. Облигация гарантирует, что брокер доставит транзакцию, а также исключает двойную трату. Сделка выполняется путем удержания суммы платежа в GRAFT выборкой авторизации от продавца. Если выборка авторизации обнаружит, что средства не были получены продавцом, она отменит транзакцию и брокер выплат не получит платеж GRAFT от продавца.

За эту услугу, брокер получает 0.25% комиссии от платежа GRAFT продавцу, тогда как суперноды участвующие в авторизации, берут свою стандартную комиссию GRAFT (0.5%)

Двойной Обмен Брокеров.

Конверсионные брокеры могут чередоваться в качестве брокеров приема и выплат платежей. Для примера давайте рассмотрим брокера обмена Биткоина, который хочет выполнять операции приема и выплат.

У брокера есть Биткоин кошелек, на котором есть 0.01 BTC. Брокер получает запрос от продавца обменять 100 GRFT на 0.01 BTC (при условии, что текущий обменный курс 0.01 BTC = 100 GRFT). Схема такой транзакции показан на диаграмме ниже.

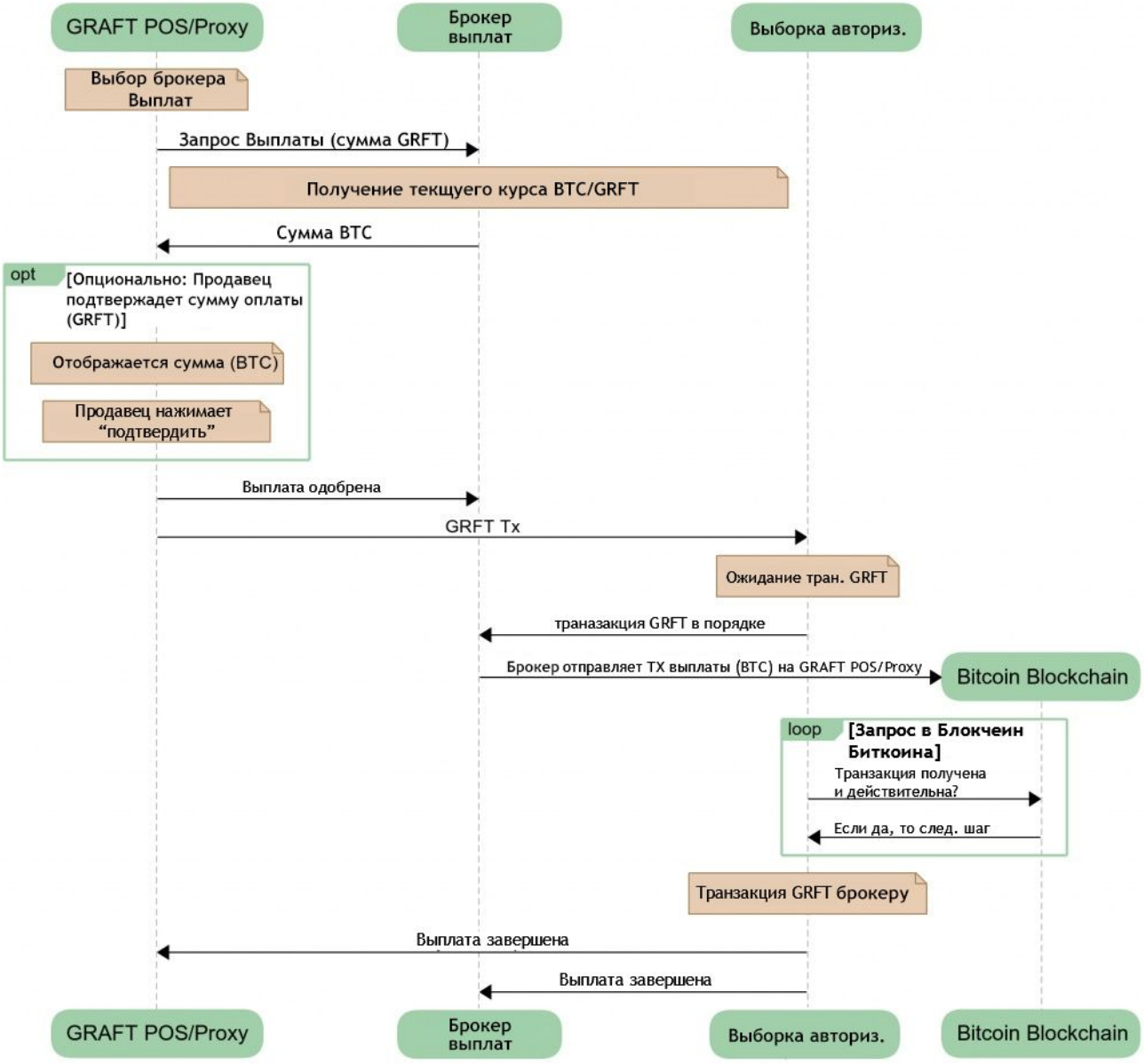

Рисунок 6: Схема транзакции брокера выплат GRAFT Bitcoin

Брокер принимает запрос и отправляет продавцу 0.01 BTC (за вычетом комиссии сети Биткоина), продавец генерирует платеж в размере 100,75 GRFT (100 GRFT сумма + 0.25 GRFT

комиссия брокера + 0.5 GRFT комиссия авторизации) брокеру и передает его выборке авторизации. Выборка ставит транзакцию 100.75 GRFT на удержание и уведомляет брокера, который затем отправляет 0.01 BTC продавцу. После получения BTC (10-60 минут в зависимости от суммы комиссии сети), транзакция 100 GRFT освобождается и брокер получает 100 GRFT плюс 0.25 GRFT прибыли.

Теперь брокер выплаты платежей может перейти в режим брокера приема платежей. Как брокер приема платежей он получает запрос обменять 0.01 BTC на 100 GRFT. Брокер принимает запрос и перечисляет 100 GRFT (за вычетом комиссии). Как только брокер получит 0.01 BTC, он снова может стать брокером выплат платежей, и теперь у него будет 0.01 BTC и 0.25 GRFT прибыли.

Предположим, (гипотетически), что один цикл обмена приема/выплат занимает 1 час, в этом случае брокер заработает примерно 12% за 24 часа (если не будет осложнений), таким образом, это выгодная бизнес модель для брокера обмена*.
(* Примерная оценка).

За Пределами Торговых Сетей: DEX (Децентрализованный Обменник)

Вышеописанная система брокеров конверсии способна функционировать над экосистемой платежей, использующей GRAFT. Она может быть расширена до децентрализованной биржи (DEX). Это является следствием того, что ненадежные операции обмена (атомарные свопы) выполняются моментально даже с внешними валютами, используя суперноды авторизации GRAFT, что позволяет использовать атомарные свопы для моментального обмена BTC <-> ETH.

Брокер Взаимообмена

Брокер взаимного обмена работает с приложением GRAFT Wallet, чтобы упростить процесс обмена и оплаты любой криптовалютой. Брокер взаимного обмена создает обычную транзакцию выбранной криптовалюты и отправляет ее на адрес получателя. Комиссия за транзакцию берется сетью выбранного альткоина. Эта комиссия взимается с отправителя, поскольку транзакция обрабатывается не только сетью GRAFT. Платеж не может быть обработан мгновенно, поскольку получатель не является участником сети GRAFT.

Этот сценарий менее выгоден, чем транзакция GRFT как для покупателя, так и для продавца, из-за более низкой скорости транзакции, а также комиссионных сборов, которые оплачивает покупатель.
Тем не менее, он поддерживается сетью GRAFT, для того, чтобы кошелек покупателя был гибким и работал, даже вне экосистемы GRAFT.

Брокер взаимного обмена мгновенно меняет необходимое количество токенов GRFT со счета покупателя в другую криптовалюту. Покупатель платит небольшую комиссию брокеру, которая оплачивается по обменному курсу.

Примеры Брокера взаимного обмена:

- Bitcoin Брокер взаимообмена
- Ether Брокер взаимообмена

Брокер выплат

Брокер выплат позволяет продавцу конвертировать GRAFT в Биткоины, альткоины или местную фиатную валюту. Выплаты можно делать вручную или автоматически.

Сумма комиссии за выплаты/обмен взимается брокерами, и зависит от частоты выплат. В зависимости от объема транзакций выплата раз в день может стоить значительно меньше, чем множественные моментальные выплаты. Брокер может накопить больше средств и выплатить одной транзакцией единовременно, в таком случае продавец заплатит комиссию за одну дневную транзакцию, а не за несколько моментальных.

Примеры брокеров выплат:

- Брокер выплат GRAFT (“Стабильная Цена ”)
- Брокер выплат USDT
- Брокер выплат Bank ACH
- Брокер выплат PayPal
- Брокер выплат Bitcoin

Брокер пополнения

Брокер пополнения позволяет конвертировать Биткоин, альткоины или местную валюту в токены GRFT. Этот сценарий является наиболее выгодным, потому, что всю комиссию (включая комиссию сети других криптовалют) оплачивает продавец. Оплата любой криптовалютой моментально и без комиссий – это очевидные преимущества для покупателя. Продавцу очень важно получать моментальные авторизации, чтобы он смог обслужить

больше клиентов. Тот факт, что все комиссии оплачиваются продавцом, как при оплате обычной банковской картой, позволяет значительно улучшить показатели привлеченных клиентов.

Брокер пополнения также может обрабатывать более крупные суммы и предлагать лучшие ставки обмена по запросу.

Примеры брокера пополнения:

- Брокер, который работает с банковскими картами.
- Bitcoin Брокер пополнения
- Bank ACH Брокер пополнения

Выплаты Продавцам

Продавец может получить свой доход в любых криптовалютах или местной валюте, в зависимости от своих предпочтений. Это гарантирует оплату продавцу строго по текущему курсу выбранной им валюты, за вычетом комиссий. Супернода автоматически выбирает лучшее предложение, из всех брокеров основываясь на лучшем обменном курсе и рейтинге брокера.

Волатильность

Большинство продавцов хотят принимать оплату в местной валюте. Продавцы не используют криптовалюты чтобы закупить товар, оплатить свои счета и выплатить зарплату сотрудникам. Для возврата товаров им также удобнее использовать привычные фиатные средства. Большинство продавцов не могут позволить себе высокую волатильность, особенно это критично для мелкого бизнеса. Так как токены GRAFT (GRFT) торгуются на биржах, волатильность токенов может стать проблемой для продавцов. GRAFT решает проблему волатильности посредством мгновенной обработки транзакций, что в свою очередь минимизирует возможные потери от волатильности, а также использует специальные токены выплат со стабильной ценой. Платежное приложение GRAFT может автоматически конвертировать транзакции продавца в местную валюту.

Токен выплат (“Стабильная цена”)

Токен выплат это специальный тип токена продавца, который будет использоваться для упрощения выплат продавцу в его местной валюте. Токен выплат, наконец, заполнит пробел

между привычными фиатными деньгами и криптовалютными платежами. Он представляет собой местную фиатную валюту, которую можно моментально отправить в блокчейн GRAFT используя суперноду.
Токен выплат основан на технологии токенов продавцов GRAFT и похож на подарочную карту, купон или другой тип токенов продавца.

Андеррайтинг Токенов Выплат

Основная задача токена выплат – предоставить продавцам простой и надежный способ принимать оплату в стабильной местной валюте, не используя при этом централизованный платежный процессор.

Токены выплат выпускаются и обслуживаются ответственными андеррайтерами (например, Банком). Когда кто-то (например, брокер выплат) покупает токены андеррайтера, компания генерирует необходимое количество токенов и переводит их покупателю, в обмен на эквивалентную сумму в фиатной валюте. Когда продавец или брокер выплат, действующий от имени продавца) продает токен выплат обратно андеррайтеру токена, компания уничтожает токены и выплачивает продавцу эквивалентную сумму в фиатной валюте. Таким образом, токен выплат всегда обеспечен достаточным количеством фиатной валюты, и их цена всегда остается эквивалентной курсу фиатной валюты. Например, 100 GRAFT.USD всегда можно купить или продать за 100 US. Токены выплат будут выдаваться андеррайтерами только в обмен на эквивалентную сумму фиатной валюты. Кроме того, права на обработку некоторых токенов могут быть делегированы (лицензированы) местными коммерческими банками или даже национальным правительством.

Обработка Выплат

Существует несколько видов выплат: Токены GRAFT, различные криптовалюты, токены выплат GRAFT или местная фиатная валюта (Таблица 2). Для каждой из этих опций, в сети GRAFT доступны брокеры. Когда продавец выбирает методы оплаты, которые он хочет принимать и метод выплаты своих средств, POS приложение GRAFT предложит ему все доступные варианты брокеров. В зависимости от личности и местонахождения продавца, он может зарегистрироваться для всех подходящих услуг по обменным конверсиям. Если для одного обмена продавцу доступно несколько брокеров, приложение GRAFT POS автоматически выберет лучшее предложение для обработки транзакции.

Таблица 2: Примеры различных методов оплаты и выплат.

Способ оплаты, выбранный покупателем	Способ выплаты, выбранный продавцом	Брокер приема	Брокер выплат
GRFT	GRFT	Нет (сеть GRAFT)	Нет (сеть GRAFT)
Подарочный сертификат, Программа лояльности, Используя Store Credit	Н/Д	Нет (сеть GRAFT)	Н/Д
GRFT	USD	Нет (сеть GRAFT)	Банковский перевод
GRFT	Биткоин	Нет (сеть GRAFT)	Биткоин
Биткоин	GRFT	Биткоин	Нет (сеть GRAFT)
Биткоин	GRFT	Биткоин	Биткоин
Биткоин	USD	Биткоин	Банковский перевод
Банковская карта	GRFT	Брокер, принимающий банковские карты	Нет (сеть GRAFT)
Банковская карта	Биткоин	Брокер, принимающий банковские карты	Биткоин
Банковская карта	USD	Брокер, принимающий банковские карты	Банковский перевод

Токены Продавца и VChain

Помимо быстрых и дешевых транзакций, продавцы высоко ценят лояльность клиентов и брендинг. Этот функционал будет доступен при использовании токенов продавца. Токены продавца представляют определенное коммерческое использование GRAFT. Они предлагают функционал смарт-контрактов, таких как накопление и использование баллов лояльности, скидки на товары, скидочные купоны и другие. Сеть кофеен, например, может создать собственный токен и закрепить за ним условия акции. Это обеспечит клиенту возможность получать скидки на охлажденные напитки в определенное время суток, что приведет к последующим покупкам со стабильными скидками в зависимости от активности или неактивности клиента. Торговые токены GRAFT могут стать очень эффективным механизмом использования купонов, позволяя продавцам создавать купоны и назначать правила в их торговой сети.

Токены Продавца

Токен продавца является предопределенным смарт-контрактом, что позволяет владельцу создать свой приватный токен. В отличие от других смарт-контрактов и платформ для выпуска токенов, создание токена в сети GRAFT не требует знания языков программирования, и может быть создан кем угодно.

Бизнес функции, описанные ранее обычно ассоциируются с использованием сторонних поставщиков услуг и высокими затратами на внедрение, что делает эти сервисы недоступными для малого и среднего бизнеса, в тоже время крупным компаниям это обходится очень дорого.

Торговые токены GRAFT позволят любому продавцу, использовать эти важные бизнес функции с минимальными усилиями и низкой стоимостью.

Типы Токенов Продавца

Торговые токены позволяют продавцам создавать и использовать свои собственные открытые и закрытые продукты[14], например подарочные сертификаты, карты лояльности, или Store Credit – в считанные минуты, без каких либо инвестиций, комиссий или регистраций в централизованном органе. Продавцы могут продавать подарочные сертификаты за местную валюту, криптовалюты, токены или токены GRFT, а затем принимать их на своем сайте, или торговой точке. Все транзакции GRAFT, включая выпуск и погашение подарочных

сертификатов, баллов лояльности и валюту магазина происходят в режиме реального времени, используя API, который может быть легко интегрирован в существующие POS приложения.

Store Credits (Кредит Магазина)

Кредиты магазина обычно используются продавцами для выполнения возвратов и обмена покупок, в том случае если возврат нельзя сделать первоначальным способом оплаты, или политика продавца не позволяет сделать возврат обычных средств. Кредит магазина, по сути, превращает возврат в обмен, поэтому продавец не теряет клиента и свою выручку.

Кредитные токены магазина могут быть привязаны к курсу местной валюты, поэтому клиент может использовать эти токены для следующей покупки или в дополнение к оплате местной валютой.

Кредиты магазина обычно не истекают, либо имеют очень долгий срок действия, поскольку обычно они представляют некую номинальную стоимость в местной валюте.

Программа Лояльности

Программа лояльности – это мощный маркетинговый инструмент, который привлекает клиентов, и увеличивает выручку. Бонусные баллы могут начисляться при каждой покупке или в качестве одноразового бонуса, а также использовать любую другую бонусную модель. Баллы лояльности могут быть использованы для покупки любых или некоторых товаров, а также могут быть конвертированы в наличные.

Баллы лояльности не обязательно связывать с наличными деньгами или криптовалютами, они также могут быть потрачены на предоставление скидки или покупки специальных продуктов, которые недоступны для продажи обычными способами.

Программы лояльности, обычно имеют ограниченный срок действия. Таким образом, продавец стимулирует покупателей зарабатывать больше баллов, при этом не допускает большое накопление баллов у покупателей, ведь в конечном итоге они могут стать бесполезными.

Подарочные Сертификаты

Подарочные сертификаты могут быть выпущены продавцами для привлечения клиентов. Чтобы увеличить эффект, подарочные сертификаты могут быть проданы со скидкой (за меньшую номинальную цену). Подарочные сертификаты обычно не истекают, либо имеют очень долгий срок действия, поскольку они представляют некую номинальную стоимость в местной валюте.

Покупатель может приобретать подарочные сертификаты у разных продавцов, на разных торговых площадках, через интернет либо в магазине, а также оплачивать их криптовалютой или местной валютой.

Платежная сеть и магазин фиксируют номинальную стоимость подарочных сертификатов или кредиты магазина в местной валюте, поэтому они не могут потерять свою первоначальную стоимость.

Клиенты могут приобретать или продавать подарочные сертификаты магазина по их рыночной стоимости, используя для этого местную валюту, криптовалюты или токены.

Купоны на скидку

Купоны на скидку могут быть использованы для одноразовых или долгосрочных рекламных компаний. Купоны можно распространять публично или индивидуально для каждого клиента. Они могут быть в электронном (в кошельке) или бумажном виде. Затем купон необходимо отсканировать в точке продаж, чтобы получить скидку или бесплатный товар.

Типы транзакций токенов продавца:

Создание

Создание нового токена, (“смарт-контракта”). Создать токен можно с помощью приложения POS.

Обновление

Обновление токена, (“смарт-контракта”). Обновить токен также можно с помощью приложения POS.

Добавление

Добавляет больше токенов в обращение.

Выпуск

Точка продаж отправляет токены в кошелек клиента или печатает бумажный вариант.

Погашение

Клиент использует токен продавца в его точке продаж, используя кошелек или бумажный носитель.

Комиссии за Токены Продавца

Все комиссии за использование токенов продавцов, оплачиваются выборке супернод.

Комиссии за транзакции токенов продавца

Комиссию всегда оплачивает продавец, это значит, что покупатель никогда не платит комиссию за их использование. Комиссия применяется к каждой транзакции с использованием токенов продавца, включая добавление, выпуск и погашение.

Комиссии за инициализацию и обновление

Первоначальная транзакция (Создание) подразумевает повышенную комиссию, потому, что она связана с неймингом токена. Первоначальная сумма комиссий будет установлена обоснованно, чтобы предотвратить массовое злоупотребление.

VChains (Виртуальные Сети)

VChain позволяет создавать виртуальные сети из магазинов. Это позволит объединить несколько точек продаж в один частный “виртуальный блокчейн”. Таким образом, у слова “VChain” двойной смысл: виртуальная сеть и виртуальный блокчейн. VChain позволяет создать

простую платформу, которая позволяет продавцу управлять его токенами, а также каталогом товаров.

Продавцы могут создавать свои частные VChain, которые будут доступны только им, и содержать всю информацию о токенах продавцов.

Vchain позволяет соединять несколько точек продаж или даже создавать целые сети из нескольких магазинов. Точки продаж, объединенные в VChain могут выдавать и принимать токены продавца, использовать общий каталог товаров, который хранится в блокчейне, создавать совместные торговые отчеты и многое другое.

Покупатели могут использовать VChain, чтобы связать между собой свои кошельки, разные аккаунты, или перемещать средства между ними без комиссии. Эта функция будет полезна для семейных и корпоративных счетов.

Комиссии VChain

Это единовременная комиссия, за создание VChain смарт-контракта, а также ежегодная комиссия за продление. Эти комиссии необходимы для надежной обработки смарт-контракта и для предотвращения злоупотребления системой. Существуют отдельная ежегодная комиссия за добавление другой точки продаж или кошелька в VChain.

Децентрализованные Краудфандинг Кредиты

Экосистема децентрализованных краудфандинг кредитов включает в себя заемщиков (покупатели, держатели карт), кредиторов (выдающих кредиты), удостоверяющих провайдеров, а также продавцов. Сеть GRAFT облегчает коммуникации и транзакции между сторонами, а также применяет общие правила для минимизации рисков мошенничества.

Сеть GRAFT соединяет потенциальных потребителей кредита с кредиторами. Любой желающий может взять кредит через приложение GRAFT Wallet. Любой желающий, с положительным балансом кошелька может выдать кредит через приложение GRAFT Wallet. Любой желающий, у которого есть приложение GRAFT POS или другое оборудование, с интегрированным GRAFT SDK может стать продавцом. Удостоверяющий провайдер реализован как сервисный плагин на суперноде GRAFT. Удостоверяющий провайдер

использует открытый API, который помогает поддерживать открытый и децентрализованный характер данной экосистемы.

Кредиторы устанавливают свои требования минимальной идентификации, необходимые для получения кредита, кредитного лимита, максимального кредитного лимита (от нескольких кредиторов), кредитной ставки, а также суммы платежа и график платежей. Заемщики могут получить кредит от нескольких кредиторов, если текущее состояние их аккаунтов соответствует требованиям кредиторов. Удостоверяющие провайдеры проверяют и подтверждают идентификационные данные заемщика, чтобы избавить кредиторов от этого бремени, а также предоставляют определенную степень анонимности и конфиденциальности держателю карты. Таким образом, удостоверяющие провайдеры знают реальную личность заемщика, поэтому могут поддерживать их долгосрочный рейтинг, независимо от сети или кредиторов. Кредиторы получают часть комиссии за транзакцию каждого платежа, который обрабатывается с использованием их кредита.

Заемщику присваивается рейтинг репутации, который рассчитывается динамически и основывается на истории потребителя и полноте проверенных данных о его личности. Начальный рейтинг, при отсутствии истории и без проверки персональных данных равняется 0. Чем больше идентификационных данных предоставлено и проверено (например, водительское удостоверение, биометрика, номер социального страхования), тем выше рейтинг, что означает одобрение большей суммы кредита для этого пользователя. Хорошая кредитная история также повышает рейтинг.

Продавцы являются лишь получателями транзакции от заемщиков, они изолированы от отношений кредиторов, заемщиков и удостоверяющих провайдеров, что полностью исключает риск мошенничества. Кредиторы берут на себя все потенциальные риски и издержки связанные с мошенничеством. Эти риски компенсируются комиссиями за транзакции и ставками по кредитам. Продавцы также могут участвовать в этом процессе, предлагая такие стимулы как кэшбэк или самостоятельно выступая в роли кредитора.

Безопасность

Последние случаи огромных утечек данных в различных сферах показали, что безопасность – это очень важный элемент любой платежной экосистемы. Самый высокий уровень безопасности может быть достигнут если безопасность является частью системы, а не надстройка, созданная после ее внедрения. Безопасность платежной системы – это не только информационная безопасность, но и финансовая безопасность. Помимо стандартных

функций безопасности, которые GRAFT унаследовал от своих предшественников, GRAFT планирует реализовать ряд улучшений, от которых выигрывают как покупатели, так и продавцы.

Доступность

Распределенная сеть постоянно “включенных” супернод обеспечивают общую доступность сети. Клиентские приложения взаимодействуют с несколькими супернодами одновременно, чтобы получить консенсус, необходимый для авторизации. Если одна супернода не работает, она автоматически заменяется другой из списка супернод, который содержит практически бесконечное число кандидатов.

Управление Идентификацией

Если сделать пользовательское управление, опираясь на сторону кошелька пользователя, это откроет большую угрозу безопасности. Кошельки, как правило, могут свободно реализовывать свои собственные меры безопасности и могут быть скомпрометированы индивидуально. Чтобы защитить сеть и обеспечить целостность пользовательских данных, GRAFT будет внедрять распределенную сеть удостоверяющих провайдеров (размещенных на супернодах), и будут доступны кошелькам через вызовы OpenIDConnectoAuth2 API.

Таким образом, независимо от кошелька, проверка и аутентификация пользователя будет выполняться сетью GRAFT, что позволит предотвратить утечку персональных данных, “спуфинг”, атаку “повторного воспроизведения”, а также атаку “человек посередине”.

Идентификация, Аутентификация и Авторизация

Методы аутентификации/авторизации существующих криптовалют осуществляется на стороне приложения пользователя, в кошельке. Это не лучшая мысль. В контексте финансовых операций, между покупателем и продавцом, должна быть установлена определенная степень доверия между сторонами, а также должно быть обеспечено соблюдение определенных правил и требований. Хорошая система аутентификации/авторизации является критически важной.

Доказательство Идентификации

Идентификация личности – это сложная тема, поскольку она касается как нормативных, так и конфиденциальных соображений. Эффективная идентификация не является тривиальной задачей.

Чтобы понять необходимость проверки идентификации, представьте ситуацию, когда продавец, запрашивает высокий уровень проверки идентификации для того, чтобы убедиться, что покупатель имеет право на покупку выписанных ему лекарств, или наивысший уровень проверки идентификации на покупку оружия (как определено в NIST Special Publication 800-63A США). И наоборот, когда покупатель выбирает товар на вторичном рынке, он может запросить у продавца более высокий уровень идентификации, чтобы не купить краденый товар.

GRAFT ожидает, что клиенты приложений будут соблюдать стандарты проверки личности, относящиеся к конкретным законам каждой юрисдикции. Суперноды будут предоставлять ресурсы для “машинной” проверки личности и выявления мошенничества, чтобы помочь продавцам и пользователям обеспечить целостность платежной сети, а также безопасность транзакций. В целях ограничения доступа пользователей к полной идентификационной информации, что нежелательно или противоречит нормативным актам (например, GDPR), GRAFT будет способствовать запросам и обмену идентификационными атрибутами, такими как возраст и адрес человека, для обеспечения соответствия местным законам и правилам. Мы также хотим добавить открытый доступ к коллекции метаданных для использования вспомогательной бизнес логики. Например, проверку взаимодействия с наркотиками или вознаграждения лояльности.

GRAFT разрешит многопользовательский контроль, где несколько пользователей имеют доступ к одному и тому же торговому аккаунту, где нужны два или более пользователей, чтобы разблокировать некоторые функции, например перевод средств из аккаунта.

Рейтинг Репутации. Проливаем Свет

GRAFT использует подход к обработке транзакций на основе риска. Каждому участнику сети присваивается рейтинг репутации, который динамически обновляется системой в

соответствии с новыми данными. Покупатели, продавцы и владельцы супернод по желанию могут связать их личные данные с аккаунтом для повышения рейтинга репутации. Такая связь не ставит под угрозу устойчивость к анализу транзакций.

Система рейтинга помогает участникам экосистемы принимать взвешенные решения, без ущерба для их безопасности и конфиденциальности. Например, продавец может изучить оценку репутации покупателя для принятия решения в отношении лимита авторизации, непосредственно перед авторизацией. Точно также, покупатель может посмотреть оценку репутации продавца, прежде чем производить оплату товаров. Покупатели и продавцы могут проверить репутацию суперноды, прокси суперноды, а также брокера конверсии, чтобы привлечь их к транзакции.

Еще один важный элемент репутации пользователей может быть применен для оценки рисков p2p кредитования, основанный на кредитной истории пользователя.

Суперноды отвечают за мониторинг, расчет, обновление и проверку рейтинга репутации покупателей, продавцов, а также других супернод. Оценки рассчитываются специальным алгоритмом прогнозной аналитики, который легко выдает понятные результаты по шкале от 0 до 100. Эти данные не могут быть использованы для раскрытия конфиденциальной информации, такой как сумма, время или характер транзакции.

Поддержка Клиентов, Разрешение Споров и Страхование Платежей.

Одной из основных причин неохотного внедрения криптовалют и криптографических токенов клиентами и владельцами бизнеса является отсутствие специалистов, которые могли бы ответить на вопросы и обеспечить техническую и бизнес-поддержку. Кроме того, невозможно “исправить” транзакции криптовалют в случае человеческой ошибки, мошеннических действий или технического сбоя. Очевидно, что все эти проблемы обусловлены децентрализованной, анонимной и независимой природой криптовалютных платежей. Тем не менее, эти свойства не помогают решать проблемы. Сообщество свободного программного обеспечения решило эту проблему, путем внедрения дополнительной технической поддержки в свободные продукты с открытым исходным кодом. LinuxOS, поддерживаемая Redhat, и MySQL database, поддерживаемая Oracle, лишь два успешных примера, которые обеспечивают коммерческую техническую поддержку свободным продуктам с открытым исходным кодом.

Чтобы облегчить внедрение платежной сети, GRAFT Foundation предоставляет бесплатную клиентскую поддержку и услуги по разрешению споров владельцев счетов GRAFT. Продавцы с высоким объемом транзакций могут получать техническую поддержку и поддержку в решении споров 24/7. GRAFT Foundation и брокеры конверсии могут застраховать платежи до 100$, тем самым компенсируя клиентам или продавцам потерю средств из-за мошеннической деятельности или технических сбоев.

Клиентские Приложения

Все пользователи сети GRAFT используют “легкие” клиентские приложения, которые не хранят полную копию блокчейна и не обрабатывают транзакции. Пользовательские приложения используют удаленные вызовы API, чтобы соединиться с “онлайн” узлами GRAFT, которые добывают новые блоки и обрабатывают транзакции в режиме реального времени.

Пользователи, которым требуется еще более высокий уровень конфиденциальности, анонимности и доступности (например, большие магазины или секретные организации) могут запустить свою собственную суперноду или несколько супернод, которые будут связаны исключительно с их клиентскими приложениями. Они будут ретранслировать сообщения и транзакции другим супернодам, обрабатывать оффлайн авторизации, и создавать токены GRAFT, которые необходимы для запуска программ кредитования, подарков и лояльности.

Клиентские приложения включают в себя:

- Приложения для компьютера и мобильных устройств POS для приема платежей в токенах GRAFT, Bitcoin, альткоинах, а также банковских карт. Эти приложения позволяют настраивать выплаты в Bitcoin, альткоинах и местных валютах, которые удобно использовать покупателям и продавцам.
- Приложения Wallet для компьютера, смартфона, а также расширение браузера Chrome позволяют совершать платежи в токенах GRAFT, Bitcoin, альткоинах, а также с использованием банковских карт (используя брокеров конверсии).
- GRAFT SDK позволяет интегрировать сеть с крупными точками продаж, а также интернет магазинами для обработки транзакций онлайн или на точке продаж. GRAFT будет внедрять собственную смарт-карту GRAFT как способ оплаты. В дополнение к паролям, карта также будет хранить биометрические подписи пользователя, и настраивать запоминаемые или искаженные секреты, которые можно использовать для аутентификации на терминале.

Помимо поддержки транзакций, ориентированных на потребителя (B2C), GRAFT будет поддерживать транзакции B2B (business-to-business) и интегрироваться в существующие бизнес-процессы. Такие рабочие процессы могут варьироваться от чего-то простого, как автоматический сбор средств, в соответствии с условиями кредита, до более сложных рабочих процессов. Например, расчет таможенных сборов грузоотправителя, учет сборов как часть общей транзакции, распределение средств на основе достижения контрольных точек утвержденных клиентом.

GRAFT также хорошо играет в пространстве интернета вещей (IoT), поскольку IoT устройства должны уметь обрабатывать данные для выполнения их функций. Примером может послужить продавец строительного магазина, вызывающий грузовик с товаром, на основе уровня запасов, определяемый внутренними системами и датчиками.

Заключение

GRAFT не существовал бы без своих предшественников. Он основан на идеях, принципах и технологиях, которые внедряли и тестировали создатели других криптовалют и токенов. Использование новейших технологий, разработанных криптографическим сообществом, наряду с новыми разработанными решениями для обработки транзакций и обеспечения безопасности, позволит конкурировать с традиционными методами оплаты и существующими централизованными платежными процессорами.

Источники

1. Bitcoin. https://bitcoin.org/en/.

1. Dash. https://www.dash.org/.

1. Bitpay. https://bitpay.com/.

1. GRAFT Definition. Merriam-Webster (2017). https://www.merriam-webster.com/dictionary/graft#h2.

1. What Is GRAFTing? - Definition & Methods. Study.com (2017). http://study.com/academy/lesson/what-is-grafting-definition-methods-quiz.html.

1. IOTA. https://iota.org/.

1. Bitcoin, Ethereum, Litecoin, Dash, Monero Avg. Transaction Fee historical chart. Bitinfocharts.com. https://bitinfocharts.com/comparison/transactionfees-btc-eth-ltc-dash-xmr-sma7.html#1y.

1. PayPal. https://www.paypal.com/us/webapps/mpp/merchant-fees.

1. NIST Special Publication 800-63. Revision 3. Digital Identity Guidelines. NIST (2017). https://pages.nist.gov/800-63-3/sp800-63-3.html.

1. CryptoNote. https://cryptonote.org/.

1. Top Seven Ways Your Identity Can Be Linked to Your Bitcoin Address. 99 Bitcoins. https://99bitcoins.com/know-more-top-seven-ways-your-identity-can-be-linked-to-your-bitcoin-address/

1. Median Confirmation Time. Blockchain. https://blockchain.info/charts/median-confirmation-time?timespan=30days.

1. Payment Card Industry (PCI) Data Security Standard. Requirements and Security Assessment Procedures. Version 3.2 PCI Security Standards Council (2016). https://pcicompliance.stanford.edu/sites/default/files/pci_dss_v3-2.pdf.

1. What are Open Loop and Closed Loop Gift Cards? Shelley Hunter. GiftCards.com. https://www.giftcards.com/gcgf/open-loop-versus-closed-loop-gift-cards.