QRAX: Quantum-Resistance Anonymous Transaction

[White paper version 1.0 (non-technical)]

Alex McKeys(@QROSLABS), Nebula(@Nebula0id)

QRAX это сеть конфиденциальных платежей и хранилище криптовалютных активов. Децентрализованная, одноранговая, квантово резистентная, анонимная, с открытым исходным кодом, ориентированная на развитие криптосообществом.

Аннотация.

QRAX создан на основе Bitcoin Core, которая была изготовлена организацией имени Satoshi Nakamoto, но вводит ряд улучшений в своей архитектуре. А именно двухуровневая сеть узлов и мастернод, DAO для развития, самоуправления и самофинансирования, а также уникальная денежная монетарная система. Ядро модифицировано и включает в себя улучшения для применения принципов анонимности и безопасности транзакций, подтверждения транзакций без централизованного управления. В цифровом виде реализована децентрализованная система которая управляется и развивается держателями узлов и монет - криптосообществом.

QRAX - это форма цифровых онлайн-денег, использующая технологию Blockchain, которая может быть легко распространена по всему миру, мгновенно и с достоверным подтверждением транзакций сетью в течении одного блока (около 60 секунд). Сеть QRAX включает в себя решения безопасности и конфиденциальности.

Абстрактное введение.

Заинтересованное, вовлеченное, надежное, компетентное и активное сообщество людей имеющих инструменты для адекватного управления, развития и процессов принятия решений имеет главное значение для успеха любой децентрализованной системы. Защита информации, особенно личной и тем более финансовой, крайне важна для защиты прав любого человека. Фидуциарные монетарные системы показали свою непрактичность и историческую неразумность в доверии централизованным регулирующим органам полноценную защиту личных данных. Кроме того, без логичной и не заинтерисованной системы управления столь же неблагоразумно доверять криптовалютному проекту или конкретному блокчейну с заявлениями о децентрализации, поскольку один человек может узурпировать сеть, в одностороннем порядке принять решение или, что еще хуже, потерять доступ, утратив кодированную основу, приватные ключи и тд.
Для процветания развивающегося криптовалютного сообщества во всем мире, где:
1. Энергия не должна восприниматься как обязательство для исполнения процесса,

2. Имеется прочная экономическая модель для роста и масштабируемости сети,
3. Есть возможность получить доступ к глобальной сети и зарабатывать на ней с любого устройства с минимальными затратами и энергопотреблением,

необходимо осознать выбранный алгоритм (доказательство работы или доказательство доли), лежащую в основе экономических систем и средств участия в сети.

При осознании такой модели сообщества проявляются качества и инструментарий системы Квантово Резистентных Анонимных Транзакций (QRAX). Сохранение прав и свобод, защищенные финансовые данные и блокчейн, защищающий конфиденциальность, все это повышает рентабельность и обеспечивает широкое внедрение эффективным, экономически обоснованным и экологически безопасным способом на уровне протокола. QRAX одновременно повышает безопасность и обеспечивает сопротивление цензуре или эксплуатации прав и свобод во всемирной сети.

Чтобы решить вышеперечисленные задачи в текущем очень пересеченном криптовалютном ландшафте сообщества людей, QRAX стимулирует каждый узел в сети участвовать в процессе генерации блоков посредством реализации алгоритма консенсуса Proof of Stake, чтобы решить, какой блок будет связан следующим. Другой уровень сети содержит мастерноды, которые обеспечивают сетевые функции второго уровня, такие как механизмы самоуправления, саморазвития и самофинансирования.
Дополнительные характеристики:
1. Уравновешивание монетарных потоков на уровне протокола с помощью балансирования инфляционных / дефляционных механизмов стимулирует децентрализацию и сводит к минимуму участие внешних денежно-кредитных систем.
2. Корелляция активности узла сети в виде вознаграждения за активность и популяризацию системы, а также ставка со статичной эмиссией наград за блок и конечной инфляцией позволяет более эффективно распределять ресурсы.
3. Награды за активность узла в сети создают мотивированную среду для сообществ и бизнеса.
4. Незначительные затраты на оборудование / устройства для участия и / или управления Мастернодами, что снижает барьер стоимости участия, позволяет любому человеку участвовать в работе сети в любом масштабе и превосходит другие системы сетей, требующие расточительных затрат на энергию и к аппаратному обеспечению.
5. Глобальное децентрализованное управление, управляемое сообществом, позволяет осуществлять надзор за параметрами сети без участия централизованных механизмов государств и сообществ, а также обеспечивает прямое участие вовлеченного сообщества и непрерывный диалектический рост и управление монетарной системы.
6. Расширенные функции Proof of Stake, например DPoS, дополнительно улучшают доступ, безопасность и свободы людей без обременительных требований к оборудованию.
Экосистему QRAX, для лучшего понимания ее принципов организации, можно сравнить с так называемой “луковой” маршрутизацией (TOP), но в тоже время абсолютно децентрализованную, самоорганизующуюся, самофинансируемую и приносящую вознаграждения за участие.

Квантово Защищенные Анонимные Транзакции | Официальный документ, версия 1.0, 2021 г.

1. ВВЕДЕНИЕ

Наступление эры блокчейна произошло в 2009 году благодаря созданию Биткоин и лежащая в его основе технология Блокчейн - созданная организацией, известной как Сатоши Накамото. После успеха Биткоина были созданы многие конкурирующие криптовалюты называемые альт-коины. Запуск Биткойна и оригинальный технический документ, основанный на концепции широко известной математической задачи “китайских генералов”, решил задачу сравнимую с изобретением колеса, и создал цифровую бухгалтерско-учетную систему, которая получила название блокчейн или связанная цепь блоков. Каждый блок содержит часть предыдущего блока и это невозможно изменить без полного контроля над всеми узлами сети. Этот процесс получил название децентрализации так как не имеет центра управления и информационная достоверность каждой транзакции имеет наивысший уровень верификации. Потенциал применения технологий блокчейн и децентрализации вызвал взрывной интерес сообществ для его применения во всех отраслях человеческой деятельности.

В настоящее время рынок наполнен токенами и монетами с разными намерениями, мотивацией и принадлежностью. Хотя существует множество проектов, некоторые из которых являются инновационными и амбициозными, но по сути являются клонами с запоминающимися названиями и служат сдерживающим фактором для более широкого внедрения криптовалюты в качестве законной и не имеющей границ альтернативе бумажной валюте. Биткойн, несмотря на свои революциоонные решения, на наш взгляд не может получить широкого применения и принятия в качестве мировой и единственной валюты и рассматривается сегодня как средство сбережения, а не средство ведения транзакций и повседневного бизнеса. Многие энтузиасты биткоина со временем превращаются в спекулянтов и маркетологов что негативно сказывается на первой децентрализованной сети транзакций. Биткоин также не может решить энергетических задач из-за чрезмерного использования электроэнергии, необходимой для обслуживания работы сети и добычи монет.

Прошло более одиннадцати лет с момента старта сети Биткойн, но окончательная идентичность и архитектура криптовалют постоянно формируется и видоизменяется. Общая неоднородность заставила общественность рассматривать криптовалюту как некий фондовый рынок, а не как средство платежей и транзакций. Присущая биткоину волатильность и насыщенность не подходит для потенциально всех пользователей, которые рассматривают ее не как альтернативу фиатным валютам, а как возможность для рискованного инвестирования.

QRAX стремится объединить в сообщества и дать в пользование инструменты для технически образованных, думающих людей, понимающих реальность окружающего мира. QRAX предоставляет безопасные средства, с помощью которых инвесторы и

широкая общественность могут вести бизнес без необходимости в централизованных финансовых учреждениях и посредниках. QRAX предоставляет людям во все более взаимосвязанном мире практичные и защищенные средства ведения бизнеса от своего имени.

“Суть криптовалют и блокчейнов - решить проблемы традиционных валют, передав власть и ответственность держателям валюты.” ~ Майк Чу, DataOverhaulers.com

2. СЕТЕВОЙ ДИЗАЙН

2.1 Введение в QRAX Network Genesis

Сеть QRAX была обявлена на bitcointalk.org April 12, 2021.
https://bitcointalk.org/index.php?topic=5330036.msg56763889#msg56763889

Первый блок QRAX был создан Mon, 12 Apr 2021 06:07:08 UTC.
https://explorer.qrax.net/block/0000005379c37c08e8c639938403824c3291377a324580705854812d67615b11

Сегодня QRAX, как и при первом запуске, децентрализован, мотивирован и имеет открытый исходный код.
https://github.com/QRAX-LABS

Первая фаза (первый суперблок или 44000 блоков) была запущена по технологии Proof of Work, который обеспечил справедливый старт сети для первоначального майнинга монет для создания опорных мастернод в количестве 21.
https://explorer.qrax.net/charts/supply

На 44000 блоке в сети сгенерировано 20M монет для распределения монет среди опорных мастернод и формирование криптосообщества QRAX.
https://explorer.qrax.net/charts/supply

PoW необходим для справедливого запуска сети. QRAX реализовал первую фазу на алгоритме хеширования Quark поскольку он был признан наиболее справедливым из-за его не высоких технических требований и достаточной надежности. Сеть началась с премайнинга 1M- QRAX (одноименные монеты QRAX) на генезис-блоке. Цель- создание 21 начальных опорных мастернод. Далее на 44000 блоке осуществлен переход на PoS алгоритм и старт примерно 6-недельного (по 10080 блоков шесть раз) пресейл периода для удовлетворения интереса к монете со стороны крипто сообщества. Все остатки этого премайна будут сожжены в блоке 104480. Нет искуственных генераций и никакие QRAX монеты не будут заблокированы, чтобы манипулировать экономикой QRAX. После периода в 44000 блоков, PoW был заменен на Proof of Stake (PoS) модель консенсуса, чтобы обеспечить наиболее надежные, более низкие экономические барьеры, энергоэффективные и долгосрочные устойчивые средства защиты сети. При этом награждая тех участников, которые

помогают обеспечивать безопасность, развивать и управлять сетью. Таким образом, дорогостоящее оборудование, ограничивающее майнинг, было заменено энергоэффективными, более простыми в эксплуатации стейкнодами и мастернодами. Также был перенесен второй уровень в блокчейн, который часто называют сетевым протоколом второго уровня. В настоящее время это обеспечивает механизмы децентрализованного управления и полноценного развития с самофинансированием. Период фазы PoW: 12 апреля 2021 г. - 14 мая 2021 г. (ЗАВЕРШЕНО)

Высота блока
1 блок - старт сети
2-43999 блоки - блоки PoW фаза
44000 блок - по настоящее время фаза PoS

Мастерноды
21 опорная мастернода

Бюджет
Накапливается на каждом блоке, выделяется по результатам активных голосований мастернодами на каждом суперблоке.

Таблица 1. Фазы вознаграждения за стекинг (PoS ноды/мастерноды)

Phase	Block interval		Total Reward	Masternode / Staker		Budget		
#	Start	End	QRAX	QRAX	QRAX	QRAX	%	Max
1	44000	87999	70	50	10	10	16.67	440000
2	88000	131999	63	45	9	9	16.67	396000
3	132000	175999	56	40	8	8	16.67	352000
4	176000	219999	49	35	7	7	16.67	308000
5	220000	263999	42	30	6	6	16.67	264000
6	264000	307999	35	25	5	5	16.67	220000
7	308000	351999	28	20	4	4	16.67	176000
8	352000	395999	21	15	3	3	16.67	132000
9	396000	439999	14	10	2	2	16.67	88000
10	440000	~	7	5	1	1	16.67	44000

Таблица 2. Фазы вознаграждения за активы (халвинг награды за популяризацию сети)

Phase #	Block interval		Year %
1	44000	307999	255.5
2	308000	571999	127.8
3	572000	835999	63.9
4	836000	1099999	31.9
5	1100000	1363999	16.0
6	1364000	1627999	8.0
7	1628000	1891999	4.0
8	1892000	2155999	2.0
9	2156000	~	1.0

2.2 Доказательство ставки

Сеть QRAX в настоящее время работает на алгоритме консенсуса PoS, который был представлен в статье Санни Кинг и Скотт Надаль в 2012 году.
Первоначальная концепция в значительной степени основывалась на понятии «возраста монеты» или продолжительности модели UTXO.
Таким образом, модель PoS отличается от PoW тем, что не сосредотачивается на майнерах и оборудовании и не награждает майнеров, а скорее награждает всех, кто желает участвовать в работе сети (удерживая свои монеты на узле). Протокол был дополнительно доработан во второй версии PoS для BlackCoin Павлом Васиным (@Rat4) с несколькими исправлениями безопасности потенциально отмеченными в изначальном протоколе . Исправления Васина включали в себя не возможность злонамеренного узла злоупотреблять возрастом монет, чтобы выполнить двойное расходование, возможность честных узлов злоупотреблять системой, делая ставки только периодически, и отрицание возраста монет на основе консенсуса. Надежность и новаторство модели PoS QRAX очевидны.
QRAX вышел за рамки оригинальных концепций PoS, постоянно развиваясь, обеспечивая превосходную безопасность и новизну соответствующего уровня мастернод и функций защиты финансовых данных.
Благодаря реализации PoS сеть имеет доступные вычислительные ресурсы, которые автоматически выбирают узел для генерации предстоящего блока в цепочке на основе

разграниченной конкуренции. В случае QRAX эти ограничения разграничены с учетом баланса (UTXO), выставленного кошельком - каждый узел стекинга конкурирует за создание действительного блока, что очень похоже на PoW. Однако узлы технически ограничены по количеству попыток в заданное время (устраняя необходимость в более высокой вычислительной мощности), а сложность получения действительного блока обратно пропорциональна ставке. Более высокий баланс означает более высокий шанс и задачу удовлетворения критериев сложности, проверки блока и получения вознаграждения. Стейкинг требует значительно меньше ресурсов, чем PoW-майнинг, поскольку нет необходимости стремиться к постоянно возрастающей сложности решения алгоритмов, необходимых для генерации монет, и связанного с этим увеличения вычислительной мощности для решения упомянутых алгоритмов. PoS по своей сути является экологически чистой альтернативой PoW.
Хотя фактор окружающей среды уже помогает PoS отличаться от PoW, следует учитывать еще один фактор: поддержание справедливого распределения мощности по сети, что должно быть высокоприоритетной целью любой криптовалюты. С растущей сложностью PoW майнинг, которая требует более мощных устройств и майнинг ферм, которые стоят дороже в эксплуатации и на рынке, возможность людей реально управлять такими устройствами становится более эксклюзивной. Реальные препятствия для обычного человека, участвующего в операциях PoW, включают стоимость оборудования, потребление электроэнергии, потраченное на вычисления, и дальнейшее потребление на охлаждение. Это неизбежно приводит к тому, что большая часть власти может принадлежать меньшим группам майнеров, из которых еще меньшее количество сможет оставаться конкурентоспособными, что приведет не только к монополии на вознаграждение, но и к контролю над сетями. Использование сетью QRAX алгоритма PoS вместо PoW представляет собой гораздо более низкий экономический и ресурсонезависимый выбор для участия в сети и глобального использования. Кроме того, для настройки устройства PoW-майнинга требуется больше технических / продвинутых знаний, чем создание узла стекинга, который открывает пространство для более широкого внедрения и вовлечения нетехнических пользователей.

2.3 Мастерноды

Сеть QRAX имеет два уровня. Уровень стекинга - это первый уровень, в котором все держатели QRAX могут участвовать, размещая свои монеты QRAX; второй - уровень мастерноды. Мастерноды - это набор мотивированных узлов в сети QRAX, отвечающих за выполнение определенных специальных задач. Сеть QRAX Masternode берет свои истоки от криптовалют Dash и PIVX, со значительной реструктуризацией до алгоритма консенсуса Proof of Stake. Таким образом, эти узлы являются неотъемлемой частью цифровой экосистемы QRAX и необходимы для работоспособности сети.
Сеть мастернод выполняет ряд функций независимо от узлов стекинга. Эти различные функции ограничены мастернодами и не могут быть выполнены стандартными узлами стекинга. Эти обязанности распределены по сети мастернод, и ни одна мастернода не имеет власти или полномочий, превышающих другие мастерноды в сети.

2.3.1 Детерминированные мастерноды

Детерминированные списки мастернод - это списки мастернод, построенные в каждом блоке, основанные только на данных в цепочке (предыдущий список и транзакции,

включенные в текущий блок). Детерминированные списки постоянно на каждом блоке пересчитываются образуя опрос всех мастернод в сети для достижения консенсуса. Все узлы получают (и проверяют) свои списки мастернод независимо, из одних и тех же транзакций в цепочке, таким образом, они немедленно достигают консенсуса по состоянию второго уровня (количество мастернод, свойства и статус каждой из них). Как четко объяснено в разделе «мотивация» документа DIP17, это кардинально отличается от предыдущей системы :
«Предыдущая система поддерживалась консенсусными механизмами, которые существовали до решения Сатоши Накамото проблемы китайских генералов. Это означало, что каждому узлу необходимо было поддерживать свой собственный индивидуальный список мастернод с сообщениями P2P, а не решение на основе блокчейна. Из-за характера системы P2P не было никакой гарантии, что узлы придут к такому же выводу о том, как должен выглядеть список мастернод. Расхождения могут, например, возникать из-за другого порядка приема сообщений или из-за того, что сообщения не были получены вообще. Это создавало определенные риски для достижения консенсуса и ограничивало возможное использование кворумов системой. В качестве конкретного примера, предыдущая система требовала реализации обходных решений, таких как «голосование за вознаграждение мастерноды», которое выполнялось за несколько блоков заранее для каждого блока, чтобы гарантировать, что консенсус будет найден и согласован. Однако соблюдение этого консенсуса по-прежнему сопряжено с риском, который может привести к разветвлению форку сети, поэтому попытка отключить Мастерноду в принудительное выполнение платежей было добавлено, чтобы предотвратить возникновение этой проблемы. Spork периодически использовался после крупных обновлений приложений и ядра сети. Это капитальный ремонт, который также приносит много улучшений в пользовательской среде и опыте, устраняя при этом недостатки предыдущей системы. Для более глубокого анализа детерминированных мастернод ознакомьтесь с DIP3.18 документ, который прекрасно описывает преимущества новой системы.

2.3.2 Роли мастерноды

Для каждой Мастерноды определены три разные «роли». Каждая роль представлена парой закрытых / открытых ключей.

1. Владелец: должен быть уникальным в сети. Может обновлять две другие роли и адрес выплаты Мастерноды.
2. Оператор: должен быть уникальным в сети. Ключ оператора сохраняется в QRAX.conf удаленного узла и используется для подписи P2P-сообщений, связанных с мастернодами (например, завершение бюджета или победители мастернод в коде совместимости). Его также можно использовать для обновления IP-адреса Мастерноды или адреса выплаты оператора (если Мастернода настроена так, чтобы разрешить выплату процента вознаграждения оператору).
3. Голосование: не обязательно должно быть уникальным (несколько мастернод могут использовать один и тот же ключ для голосования). Он используется для голосования по бюджету.

Одна и та же пара ключей может использоваться для всех трех ролей (по крайней мере, на данный момент ключ оператора скоро будет изменен на ключ BLS?), но они должны отличаться от ключа дополнительного адреса.

2.3.3 Новый тип транзакции

В QRAX, вводится четыре новых типа транзакций, каждая из которых идентифицирует конкретную полезную нагрузку транзакции со своими собственными правилами проверки:

- КОЛЛАТЕРАЛ (провайдер-регистр): это основная специальная сделка. Используется для регистрации новой Мастерноды,
установки всех ее свойств (например, ключей для каждой роли). Он создает обеспечение Мастерноды в качестве
одного из своих выходов или ссылается на неизрасходованный выход 50000 QRAX в цепочке блоков (в этом случае он должен включать подпись со своими ключами в качестве доказательства владения 50000 QRAX). ПРОУПСЕРВ (поставщик-обновление-сервис):
- отправляется оператором mn для обновления свойств, связанных с услугой (IP-адрес, адрес выплаты оператора).
- ПРОУПРЕГ (поставщик-обновления-регистратор): отправлено владельцем mn для обновления ключа оператора, ключа голосования или адреса выплаты.
- ПРОУПРЕВ (provider-update-revoke): отправлено оператором mn для отзыва услуги и перевода mn в состояние запрета PoS (например, в случае взлома ключей). Мастерноду можно «оживить» позже, отправив ProUpReg tx, который устанавливает новый ключ оператора, а затем ProUpServ tx (подписанный новым ключом), который устанавливает новый IP-адрес для Мастерноды.

2.3.4 Архитектура кода

Детерминированные мастерноды представлены как объекты класса CDeterministicMN. Этот класс включает переменную-член, в которой хранится общий указатель на постоянный объект CDeterministicMNState, который инкапсулирует состояние DMN (обновленные свойства и статус).
Список мастернод представлен классом CDeterministicMNList, который использует неизменяемые функциональные карты для хранения актуальной информации о каждой записи.
Новый список создается в каждом блоке и поддерживается CDeterministicMNManager.
Использование неизменяемых функциональных карт - это элегантное решение, разработанное Codablock, чтобы уменьшить накладные расходы памяти, необходимые для обновления списка мастернод в каждом блоке, путем принятия подхода копирования при записи.
Неизменяемые структуры данных предоставляются по умолчанию в языках, ориентированных на функциональное программирование, таких как Clojure или Scala, но для C ++ в настоящее время нам нужно полагаться на сторонние библиотеки. В будущем можно будет изучить реализацию, основанную на std :: maps, но это серьезно

повлияет на производительность и потребует сотни МБ в оперативной памяти только для обслуживания списка MN.

2.3.5 Голосование мастерноды по распределению бюджета

Как децентрализованная автономная организация (DAO), QRAX действует и подчиняется собственному самоуправлению сообщества. Ни одна сущность, ни небольшая группа согласованных сущностей не обладают способностью определять направление, в котором растет QRAX. Этот органичный подход к управлению призван максимально использовать преимущества членов сообщества QRAX, которые сами действуют в своих общих интересах. Одним из способов достижения этой формы управления является голосование мастернодами по ежемесячным бюджетным расходам. В настоящее время операторам мастерноды предоставляется возможность голосовать за предложения, сделанные членами сообщества с целью улучшения QRAX или обстоятельствам для него по каким-либо причинам. Имея более 100+ мастернод, которые требуют значительных инвестиций в QRAX для работы, в настоящее время используются, этот подход значительно разделяет власть,

2.4 Стейк ноды или простые узлы

В принципе, PoS выполняет ту же функцию, что и PoW, для достижения консенсуса по блокчейну. Однако, как отмечалось ранее, он гораздо менее ресурсоемкий, поэтому он стал выбранным методом консенсуса для QRAX и многих других проектов.
Использование модели Proof of Stake требует, чтобы пользователи инвестировали в узел путем ставка (размещая) свои монеты / QRAX на узле (основной кошелек QRAX). В обмен на ставки пользователи получают взамен определенное количество монет. Stakenodes несут ответственность за то же, что и майнеры, в Proof-of-Work: упорядочивание транзакций и создание новых блоков, чтобы все узлы могли согласовать состояние сети.
Proof-of-Stake и Stakenodes содержат ряд существенных улучшений в отличии от системы Proof-of-Work: https://www.investopedia.com/tech/what-dao/

- Лучшая энергоэффективность - не нужно использовать много источников энергии, снижая барьеры для входа.
- Сниженные требования к оборудованию - не нужно дорогое или специализированное оборудование, чтобы иметь шанс создавать новые блоки.
- Более сильный иммунитет к централизации - доказательство ставки ведет к большему количеству узлов в сети.

Чтобы запустить Stakenode, пользователи должны просто запустить последнюю версию основного приложения-кошелька QRAX (на устройстве, которое будет поддерживать его работу - ноутбук, настольный компьютер, raspberry pi и т. д.) И иметь как минимум 1 QRAX в своем кошельке и иметь кошелек, разблокированный для стекинга. .

2.5 Assets Network

2.5.1 Описание

Разработка Assets создана для привлечения участников в работу сети, поддержание состояния, развитие и популяризацию. Каждый участник создает свою структуру дочерних узлов. При получении первой транзакции кошелек участника активируется в сети и встраивается в общую структуру данных. Assets представляет собой процент начислений в день/месяц/год, размер награды от основного баланса, сумму балансов дочерних узлов до 100 уровня в глубину.

2.5.2 Термины

Структура - совокупность узлов и связей между ними, имеющая древовидную форму, с неограниченным количеством узлов в ширину и 100 узлов в глубину.

Идентификатор - уникальная хеш строка кошелька, создаваемая при первом получении транзакции.

Узел - отдельный кошелек, активированный транзакцией и привязанный к идентификатору вышестоящего узла.

Пул - участник сети, организующий прием dpos для предоставления большего процента награды участникам.

dpos - процедура делегирования своего баланса на пул, для получения награды по проценту пула.

2.5.3 Как работает Assets

Каждый кошелек может быть включен в структуру только в одном ее месте, он имеет единственный вышестоящий узел и множество нижестоящих узлов. При получении первой транзакции происходит активация узла и установка его в структуру. Данные записываются в блокчейн. Просмотреть свою структуру можно во вкладке Assets. При изменении баланса кошелька (входящая или исходящая транзакция) происходит расчет накопленных начислений Assets по проценту и балансу на момент получения транзакции. Награда выплачивается в следующем блоке после блока, содержащего транзакцию. Начисление награды не зависит от доступности кошелька (выключен/включен).

2.5.4 Delegated POS

Каждый участник может делегировать свои монеты на удаленный адрес, который выступает в роли пула. Участник делегируя определенную сумму монет, будет получать вознаграждение Assets по проценту пула, при этом, делегированная сумма не будет учитываться в начислении Assets в собственном кошельке. Оператор пула получает 10% от награды, рассчитанной участнику пула.

2.5.5 Техническая реализация

При отправке транзакции, в ее структуру записывается идентификатор отправителя, на стороне получателя данные считываются и записываются в память. Идентификатор кошелька и вышестоящего узла записываются в wallet.dat файл. Любой узел сети имеет идентичную структуру всех узлов. Идентификаторы записываются в блок. Транзакция награды имеет тип “assetsmint”, все узлы, которым необходимо получить награду записываются в получатели в одну транзакцию.

2.6 Сжигание монет

Сжигание монет происходит при отправке любой суммы на адрес genesis кошелька: QU1yzBpsPpbg6BN5pgsVbssW6WWAcxHFHd

3. УПРАВЛЕНИЕ

Децентрализованное управление, разработанное сообществом - это управляющая функция QRAX DAO. В рамках этой системы существует возможность ежемесячного финансирования предложений из бюджета QRAX. Предложения подаются любым узлом для голосования мастернодами 2-го уровня. Владельцы МастерНод, расположенные по всему миру, определяют, целесообразно ли финансировать предложение.

3.1 Управление бюджетом и голосование

3.1.1 Бюджет Сообщества:

Примерно каждый месяц у казначейства QRAX есть фиксированное количество монет в свободном доступе. Эти средства направляются на реализацию предложений, получивших достаточный процент голосов «за» по отношению к голосам «против» (~ 10%). Например, если существует 100 мастернод, предложение должно иметь 10 (10% от 100) или более чистых голосов «Да». (Да голосов минус Нет голосов).
Бюджет QRAX финансируется через один QRAX на каждый блок, добавленный в сеть. Это создает единый доступный бюджет в каждом цикле блока. Эти QRAX не «создаются» сами по себе, а только распределяются как имеющиеся в наличии для создания / использования. Предложения подаются в систему сообщества, голосуются, и тем предложениям, которые приняты, выделяются запрошенные ими средства. Выплата этих бюджетных фондов происходит в виде «суперблока», который происходит каждые 44000 блоков (примерно 1 месяц). Суперблоки были созданы для беспрепятственного администрирования платежной стороны предложений децентрализованного голосования. Если предложение проголосовано и подтверждено, Superblock появится при определенном количестве блоков и автоматически позаботится обо всех выплатах, как это подтверждается кодом. Это обеспечивает децентрализованную систему процесса голосования / оплаты.
Суперблоки работают рука об руку с бюджетной системой. На первом этапе бюджетной системы предложение готовится и передается в сеть. По прошествии 24 часов он считается правомочным, и по нему может быть проведено голосование. Как только это

произойдет, необходимо, чтобы по крайней мере 10% сети проголосовали «за», чтобы попасть в «бюджетный прогноз». Бюджетный прогноз - это просто все предложения, которые имеют право на получение оплаты, отсортированные в порядке {YesCount - NoCount} (количество мастернод, проголосовавших за данное предложение, за вычетом количества узлов, проголосовавших против). Поскольку предложения оплачиваются, это продолжается до тех пор, пока в бюджетной системе не закончится QRAX для этого периода оплаты и она не перестанет добавлять предложения в прогноз. Впоследствии сеть QRAX примет бюджетный прогноз и доработает его. На этом этапе остальная часть сети Мастерноды сравнит свой прогноз с окончательным бюджетом, и, если они совпадут, они проголосуют «Да». Если более 10% сети проголосуют за окончательный бюджет, то при достижении следующего суперблока сеть создаст эти блоки. Суперблоки просто платят одно предложение за блок до тех пор, пока не будет выплачен ежемесячный бюджет.
Доступные средства для каждого суперблока равны количеству блоков с момента последнего суперблока, умноженному на количество QRAX, выделенных для суперблока из каждого блока. Математика здесь довольно проста, особенно потому, что именно здесь вступает в игру «выделенный» QRAX. Один QRAX на блок и один блок каждую минуту в течение 24 часов каждый 31 день Это формирует «бюджет», доступный для предложений.
Предложения сортируются по их чистым голосам «да» (голоса «да» минус голоса «нет»), и затем они оплачиваются в порядке от наивысшего «чистого да» до самого низкого.
Общая сумма QRAX, необходимая для финансирования всех проходящих предложений, редко бывает равна доступным QRAX, смотрите таблицу 1. Если общие средства, необходимые для всех проходящих предложений, находятся в рамках бюджета, не все QRAX будут созданы. Например, если все проходящие предложения составляют 20000 QRAX, тогда только 20000 QRAX создаются и оплачиваются этим предложениям.
И наоборот, если принятые предложения превышают выделение 44000 QRAX, предложения финансируются в порядке их положительных голосов до тех пор, пока бюджет QRAX не будет исчерпан. Например, если есть пять проходящих предложений с просьбой по 10 000 QRAX (всего 50 000), только первые четыре будут профинансированы, а оставшийся не получит финансирования. Протокол будет финансировать только те проекты, которые могут быть полностью профинансированы. Любые оставшиеся неизрасходованные средства не переносятся и никогда не создаются. Возможно, что ровно 44000 QRAX могут финансировать проходящие предложения, и ничего не останется.

3.1.2 Подача предложений:

Любой желающий может подать свое предложение на голосование. Каждая подача предложения стоит 100 QRAX, которые сжигаются. Неважно, какой вклад в развитие проекта вносит человек - дизайнер, кодер, певец, финансист и другое, важен полезный вклад в экосистему.

3.1.3 Децентрализованное голосование:

Владельцы мастерноды голосуют за выдвинутые предложения. Это голосование децентрализовано и анонимно. Каждый владелец мастерноды имеет один голос за

предложение на каждую принадлежащую им мастерноду. То есть одна мастернода это один голос.

3.2 Управление и организация сообщества

Как упоминалось выше, система предложений подается в сеть (кем угодно) для голосования мастернодами 2-го уровня. Эти владельцы узлов, расположенные по всему миру, определяют, следует ли финансировать предложение.
Есть еще один аспект QRAX (не связанный напрямую с блокчейном или выплатами бюджета), который относится к тому, как сообщество (люди, которые решают участвовать, развивать и работать, чтобы помочь большей экономике и экосистеме QRAX расти) управляют собой и самими собой то есть организовывать экосистему. Эти аспекты относятся к вспомогательным областям социальных коммуникаций, таким как Telegram, Твиттер, Дискорд и тд. В некоторых случаях люди подают предложения о поиске финансирования, чтобы взять на себя роль (например, координатора социальных сетей и тд) в управлении аспектами экосистемы. Однако в большинстве случаев люди добровольно жертвуют своим временем, талантами и энергией в поддержку более широкого видения QRAX.
Первым руководящим принципом, вокруг которого собираются эти люди, является манифест QRAX, который гласит: КОНФИДЕНЦИАЛЬНОСТЬ не подлежит обсуждению. Это основное право человека.
СВОБОДА - это главное.
ТЕХНОЛОГИИ развиваются, УПРАВЛЕНИЕ также должно развиваться.
Конфиденциальность ПОЗВОЛЯЕТ иметь свободу делиться тем, что вы хотите, ВСЕМ, а также свободу ОГРАНИЧИТЬ для тех, кто видит вашу информацию.
Мы считаем, что это ВЫБОР каждого человека.
УПРАВЛЕНИЕ используется для достижения целей и развития
ФОНДА.
DAO НЕПРИКАСАЕМО.
Присоединяйтесь к нам, КОГДА хотите, ПОТОМУ ЧТО вам нравится, и НАСКОЛЬКО ДОЛГО как вас устраивает.
Давайте изучим ВСЕ варианты ВМЕСТЕ.
Вы ВАЖНЫ для НАС, ВАЖНОСТЬ во взаимодействии предложенными инструментариями.
Пришло время использовать ваш ПОЛНЫЙ потенциал.
«Это руководство для вербовки и руководства десятками тысяч активистов с миссией изменить мир к лучшему, не имея доступа к деньгам, ресурсам или славе....,
Основанное на опыте Фальквинге по руководству Шведской пиратской партией в Европейский парламент, начинающийся с нуля, охватывает все аспекты того, как привести толпу активистов к массовому успеху.22 ”
Вот некоторые из ключевых навыков «мудрого» лидерства, основанные на книге Фалвинджа:
1. Освободить контроль
Освобождение от контроля - первое правило роя лидерства. Вождь роя ведет прежде всего через вдохновение. Делегирование полномочий может быть пугающим, но для того, чтобы рой функционировал, все его части должны стать самодостаточными и автономными. Это единственный способ воспользоваться преимуществами роевой эффективности и скорости выполнения. Чтобы вести за собой, высвободив контроль,

лидер должен руководить через вдохновение и пример и давать возможность любому из членов роя выступить и взять на себя роль. Это происходит органически; когда требуется задача или функция, никто ее не назначает; кто-то добровольно возглавит его и вдохновляет других добровольно следовать за ним. Архитектура роя позволяет создавать лидеров по мере необходимости; как только роль, задача или функция выполнены, руководитель этой функции перестает руководить. Никто в организации не имеет преимущества перед кем-либо другим, и никому не назначается роль кем-либо другим; лидерство происходит естественно, когда потребность удовлетворяется талантом.

2. Формируйте культуру лидерства и доверия

Чтобы децентрализованное руководство было успешным, оно должно поддерживаться культурой доверия. Основатель создает эту культуру для организации, задавая тон и пример и руководя больше как архетип, чем как менеджер или наставник. Поэтому основатель и все лидеры в организации должны поддерживать отличную личную репутацию, избегать негатива и всегда демонстрировать такие ценности, как терпение, коллегиальность, страсть и понимание.

3. При принятии решений соблюдайте «правило трех пиратов».

«Правило трех пиратов» - это метод делегирования принятия решений в локальную область роя, где решение необходимо, ускорение действий и избежание бюрократической инерции. Обычно, если трое активистов соглашаются, что что-то хорошо, им не нужно спрашивать разрешения действовать от имени организации.

4. Определите сообщение, оставьте «брендинг» рою.

Лидер роя определяет содержание сообщения и оставляет его другим решать, как лучше всего передать сообщение с учетом контекста и аудитории. В рое нет последовательных сообщений, лозунгов, крылатых фраз или руководств по стилю. Одно и то же сообщение может быть доставлено множеством различных способов, чтобы удовлетворить потребности, ценности и характеристики местной аудитории.

5. Будьте лицом СМИ

Остальному миру нужен аватар, чтобы ассоциироваться с роем, поэтому для лидера роя важно лично взаимодействовать со средствами массовой информации, включая все выступления в прессе, крупные публичные мероприятия и митинги.

6. Постройте временную шкалу.

Члены роя должны понимать, где они находятся, куда они направляются и как они собираются туда попасть. Чтобы добиться доверия, лидеру необходимо установить прозрачную временную шкалу и определить ключевые этапы, которые участники роя могут понять, принять участие и почувствовать выполненное задание по мере их достижения.

7. Ставьте видимые, активные, всеобъемлющие цели

Рой людей не привлекает по социальным причинам; они присоединяются к рой, потому что верят в миссию роя и хотят ее выполнить. Чтобы люди были вовлечены, необходимо определить цели, которые должны быть инклюзивными и увлекательными. Измерение и геймификация - это способы удержать рой вовлеченным и сфокусированным, а также задействовать естественную конкуренцию, чтобы делать дела и достигать целей. Чтобы поддерживать мотивацию членов роя, вознаградите их признанием и вниманием - это важный шаг к поддержанию морального духа и веры. Лидерство роя увеличивает устойчивость организаций; лидер роя создает экосистему,

которая является адаптируемой, избыточной и самоорганизующейся. В конечном итоге лидерство роя радикально сокращает бюрократию, предлагая каждому члену возможность свободно проявлять инициативу, участвовать и руководить в соответствии с их навыками и уровнем интересов.

4. ЗАЩИТА ФИНАНСОВЫХ ДАННЫХ HUSH

В этом направлении ведется широкая разработка, согласно роад мап она должна появится в ближайшее время.

5. ЭКОНОМИЧЕСКАЯ МОДЕЛЬ

Денежно-кредитная политика QRAX предназначена для обеспечения устойчивой инфраструктуры и услуг, способных поддерживать масштабируемую, децентрализованную и отказоустойчивую инфраструктуру узлов. Это позволит осуществлять защищенные, верифицированные и быстрые транзакции во всем мире без астрономического количественного смягчения и соответствующая результирующая девальвация собственной монеты. Эта политика оказала пагубное влияние на другие криптовалютные проекты, многие из которых используют протокол PoS.

5.1 Денежно-кредитная политика

Денежно-кредитная политика QRAX будет определяться тем, как ее основные экономические рычаги будут влиять и корректироваться с течением времени. Утверждения проекта обеспечивают долгосрочную стабильность, устойчивость и доступность протокола. Денежно-кредитная политика конкретно регулируется кодовой базой блокчейна, косвенно путем использования сети ее пользователями и контролируется через QRAX DAO через его модель управления на уровне протокола. Основные экономические рычаги, управляемые денежно-кредитной политикой, включают, но не ограничиваются:

- Стоимость и сжигание комиссии за транзакцию
- Скорость эмиссии монет на блок.
- Распределение вознаграждений за эмиссию монет за блок между стэйкнодами и мастернодами.
- Минимальная сумма для стейкинга.
- Требования к Мастернодам.

5.2 Экономика монет

- QRAX имеет фиксированную скорость генерации на блок (каждые 60 секунд).
- 70 QRAX в качестве награды за блок (10 QRAX для стейкернод, 50 QRAX для мастернод).
- 10 QRAX «выделяется» (не создается) в бюджет.
- QRAX полагается на то, что как стейкеры, так и мастерноды владеют своей собственной монетой QRAX, чтобы помочь децентрализовать, управлять и защищать сеть.
- И мастерноды, и стейкерноды получают вознаграждение.

- Равновесие между доходностью стекинга и мастернод достигается естественным образом.Прибыльность стекинга снижается с увеличением общего количества выставляемых монет, а прибыльность мастернод снижается с ростом активных мастернод сети.
- Пользователи QRAX платят небольшую комиссию за транзакцию.
- Все комиссии за транзакции сжигаются, удаляя монеты из общего количества.
- QRAX имеет хвостовую эмиссию. (Конечная эмиссия важна, потому что вознаграждение за блок является стимулом для
участников сети продолжать хостинг и обеспечивать работоспособность сети без перекладывания затрат на
пользователей в виде высоких комиссий.)

Сжигание комиссии за транзакцию действует как экономический термостат - по мере увеличения транзакций увеличивается и соответствующее сжигание монет.

5.3 Максимальное количество монет

Цифры ниже представляют собой теоретическое максимальное количество монет. Фактическое количество будет определяющим при сжигании комиссии за транзакцию и выделении не требуемых QRAX из максимально возможного ежемесячного генерирования бюджета. В результате этих факторов фактическое число, скорее всего, будет меньше этих теоретических максимумов.

5.4 Динамическое предложение монет

Хотя QRAX не имеет жесткого ограничения на количество монет (определенный абсолютный предел), у него есть мягкий предел (ограничение на количество монет, производимых при выполнении определенного условия). Условие soft-cap QRAX выполняется, когда плата, взимаемая за сетевые действия, равна сумме, установленной в блоке. Затем блокчейн начнет сжигать то же количество монет, что и генерирует, ограничивая рост. Таким образом, QRAX имеет динамическую подачу монет, откалиброванную блокчейном в ответ на действие сети. Механизм мягкой крышки в кипящей среде показывает, каким будет максимальное количество монет, если каждый ежемесячный бюджет будет использован на 100%, и какой будет новый мягкий предел, а он будет выглядеть при различных значимых (нестандартных) объемах транзакций (что приведет к значительному снижению комиссии). Когда выгорание комиссии превышает количество монет, сгенерированных в качестве вознаграждения за блок, график имеет тенденцию вниз, а не вверх.
Чтобы объяснить более подробно, динамическое предложение монет QRAXX имеет философию, аналогичную философии эластичной валюты, где денежная масса корректируется в ответ на экономическое давление - т. е. на объем бизнеса - для

достижения стабильности. Это достигается путем калибровки объема в обращении по объему кредита. В денежной экономике эластичность достигается за счет изъятия валюты из обращения. Это происходит при принятии решения в ответ на разворачивающийся рынок. Это действие подталкивает экономику в желаемом направлении.
Однако, в отличие от эластичной валюты, QRAX не сжимается по решению руководства и не реагирует на калибровку объема обращения в соответствии с объемом кредита. Единственные влияющие факторы - это те, которые основаны на объеме транзакции и сжигании комиссии, как это интерпретируется алгоритмом. При высокой скорости транзакций в секунду количество сжигаемых монет будет равно той сумме, которую они генерируют, создавая нейтрализующий эффект на поставку монет. Однако это значение мягкого ограничения непросто предсказать, поскольку размер комиссии варьируется. Эти переменные делают невозможным предоставление фиксированной ставки транзакции на блок для нейтрализующего эффекта.
Важно отметить, что алгоритм балансировки эмиссии и сжигания контролирует поставку монет в ответ на самое последнее состояние цепочки блоков. Ни разработчик, ни владелец, ни майнеры, ни какая-либо другая сторона не могут создавать новые запасы монет. Алгоритм гарантирует, что отсутствие жесткого ограничения предложения монет работает в пользу здоровой экономики для QRAX как валюты. Поскольку целевое время блока составляет 60 секунд с QRAX, экономия поддерживается поминутно, ежедневно.
В случае, если баланс алгоритма сжигания QRAX становится неблагоприятным для здоровья экономики QRAX, децентрализованное правительство состоящее из владельцев мастернод может поднять этот вопрос, чтобы проголосовать за лучшее решение.

6. СООБРАЖЕНИЯ НА БУДУЩЕЕ

6.1 За пределами надежности

Хотя еще рано говорить о точной конструкции и философии идеальной сети транзакций, которая будет использоваться в будущем, ведущей к постквантовому сопротивлению до того, как они станут значительным риском. Это означает, что QRAX следит и стремится избавиться от доверия к надежным криптографическим доказательствам, созданным случайными участниками, чтобы добиться надежной настройки PoS в технологии блокчейн, возможно в версии 2.0 будет предложена новая концепция децентрализации и протокольная реализация.

6.2 Воздействие QRAX на окружающую среду

Хотя это, по общему признанию, не является первоначальной целью проекта QRAX, коллективная организация осознала, что сфера криптовалюты и блоучкйнов раздвинула экологические границы шире и гораздо глубже по сравнению с тем, что мы имели в 2009 году. С чего мы начали в 2018 году. С нормализацией компенсации выбросов углерода в деловом мире QRAX сдвинулась с мертвой точки. чтобы не

только стать первым криптовалютным проектом, который стал углеродо-нейтральным (декарбонизация планеты), но и первым, охватывающим все годы своего существования.
На дату публикации GRAX стал тем, что мы считаем необходимым; CO зеро-эмиссион

6.3 Частный стейкинг

QRAX представит в версии 2.0 совершенно новую функцию ставок HUSH. Это позволит человеку ставить защищенные монеты и получать вознаграждение за стейкинг непосредственно на адрес HUSH. Эта функция защитит данные пользователей, поддержит защиту их финансовых данных и увеличит процент экранированных монет в сети QRAX, дополнительно укрепив все используемые протоколы PoS.

6.4 Децентрализованные автономные пулы ставок (DPoS)

Идея «пула» пришла из PoW. В PoW вы можете майнить либо напрямую (аналогично тому, как это было во времена Сатоши), либо присоединиться к «конгломерации» майнеров, называемой пулом (именно так добывается подавляющее большинство монет PoW). В QRAX мы сейчас в основном «соло-стейкинг» (аналогично соло-майнингу PoW). Стейкер получит вознаграждение за блок только в том случае, если он найдет действительный блок (в этом случае он получит полную часть вознаграждения за блок, то есть 10 QRAX). С пулами вам не нужно искать блок-победитель, вы просто указываете хешрейт (в случае QRAX: мощность ставок). Когда блок обнаруживается пулом, оператор пула берет свою долю и распределяет оставшуюся часть в «пуле вознаграждений». Каждые X блоков (например, один раз в день или при каждой транзакции) оператор пула распределяет между стейкерами средства, накопленные в пуле вознаграждений, в процентах, исходя из того, сколько ставок было предоставлено каждым из них. Однако в этом случае стейкерам необходимо доверить оператору новые награды (так же, как это делают PoWminers, когда они указывают свои асики на майнинг-пул). Идея пула «без доверия» (или, скорее, «децентрализованного автономного» пула ставок DPoS) состоит в том, чтобы удалить этот элемент централизации, позволив любому игроку с полным узлом участвовать (и конкурировать) в качестве оператора пула, а также сделав распределение вознаграждений проверяемым с помощью консенсус (принудительный платеж на определенной высоте, как и в случае с суперблоками).

6.5 Эволюция управления

Значительное количество времени и исследований было потрачено на изучение того, как может выглядеть следующая эволюция управления DAO в QRAX. Подборку этих исследований можно найти
https://qrax.org

7. БЛАГОДАРНОСТИ

QRAX исходит из бесчисленных идей, мечтаний и видений, существовавших до его создания. Видение децентрализованных, защищающих права, реализующих свободу цифровых средств обмена и передачи ценностей обсуждалось даже Милтоном Фриддманом еще в 1999 году. Есть много людей, которым следует воздать должное и поблагодарить их. Без помощи многих выдающихся людей QRAX не существовало бы. Тем не менее, особенно нынешняя «команда» людей, первого сообщества QRAX FOREVER, поддерживающих и развивающих экосистему QRAX в целом, будь то разработчики, социальные менеджеры, отраслевые сообщества, бизнес-разработчики и многие другие. Эти группы людей, многие из которых добровольно жертвуют своим временем и усилиями, - вот что движет QRAX вперед.
За этот технический документ особая благодарность приведенным ниже лицам:
FelixNoctuae - концепт, корректура и компоновка
Daydry - каверзные вопросы и уточнения)))