AKRA NETWORK

White Paper

2021

Содержание

Введение

Появление децентрализованной финансовой системы на основе криптовалюты связано с нарастающими проблемами классической банковской системы. Эмитентом денег является центральный банк делегируя часть функций другим организациям (частным банкам и финансовым организациям). Наличие этих факторов влияет на конфиденциальность и приватность конечных пользователей. Криптовалюта, работающая на блокчейне предлагает альтернативу классической финансовой системе, позволяя достичь полной децентрализации финансового управления.

Одной из проблем массового внедрения криптовалюты в финансовый сектор является проблема взаимодействия между блокчейнами. Одним из решений этой проблемы может послужить создание экосистемы способной объединить несколько блокчейнов.

AKRA Network предлагает универсальную и простую блокчейн инфраструктуру базирующуюся на Binance Smart Chain (BSC) и Ethereum (ETH). Проект AKRA построен таким образом, чтобы стать полноценной альтернативной финансовой системы, работающий с криптовалютой и подходящий как для физических лиц, так и компаний различного уровня капитализации.

Внутрисетевая цифровая экономика представлена токеном AKRA использует протоколы ERC-20 и BEP-20. В перспективе планируется перевод инфраструктуры на собственный блокчейн с выпуском монеты coin AKRA blockchain.

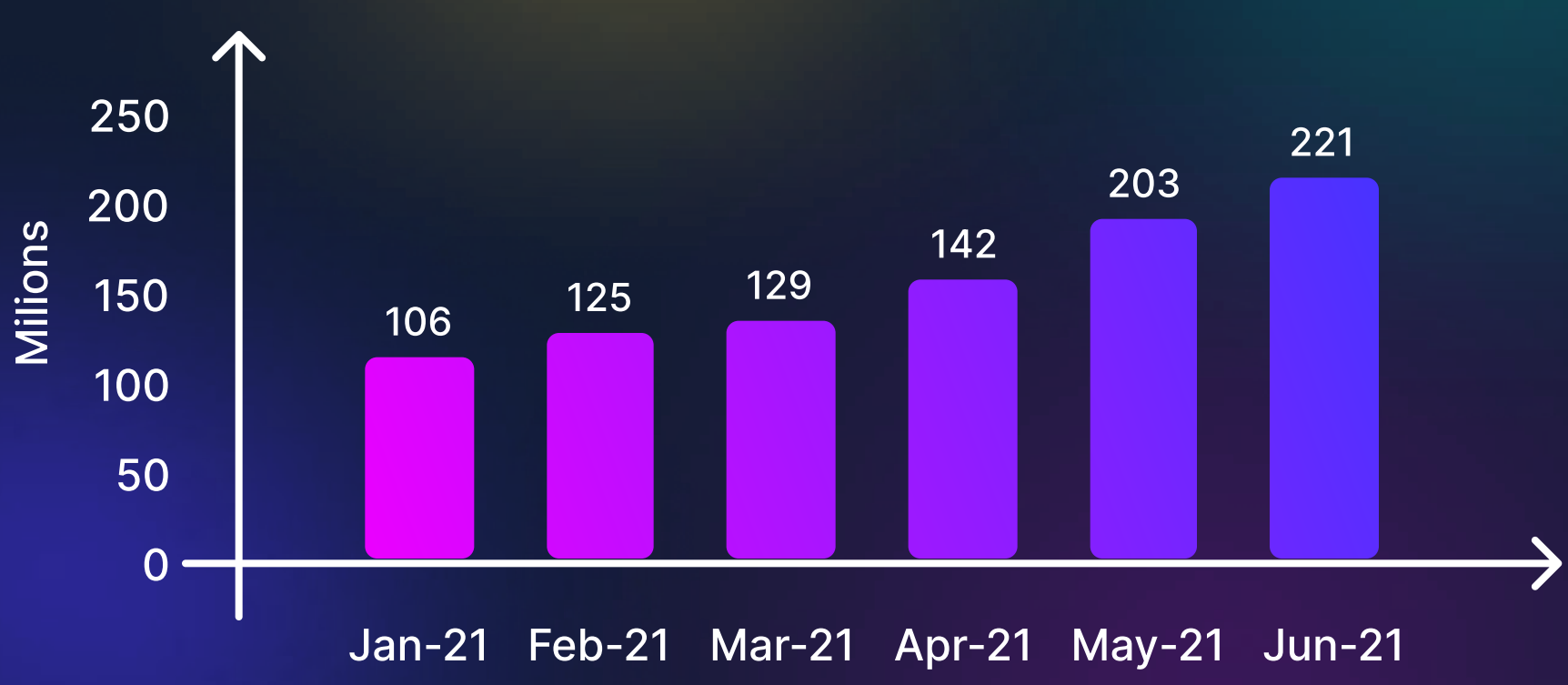
Разработчики экосистемы AKRA предлагают эффективное решение проблемы взаимодействия между блокчейнами используя блокчейн-мосты. Технология позволяет решить проблему обмена данными и финансовыми активами между блокчейнами, снижая стоимость переводов и повышая скорость транзакций цифровых активов.

1.1 Централизованные финансы в мировой системе и существующие проблемы

Первая криптовалюта Bitcoin подарила миру децентрализованную цифровую финансовую систему, работающую на блокчейне. Открытый исходный код позволил изучать и открывать новые перспективы в цифровых финансах, а также других сферах жизни, позволяющие вносить инновации. Это стало основным фактором внедрения криптовалюты во многие сферы жизни.

Согласно данным из различных аналитических источников популярность криптовалюты растёт высокими темпами в различных уголках мира. На графике представлены данные прироста новых пользователей цифровых финансов за период с января по июнь 2021 года подтверждающий высокую заинтересовать пользователей со всего мира.

Рост количества пользователей криптовалюты в 2021 году



По данным: *crypto.com*

Централизованная финансовая система имеет ряд существенных недостатков и по этой причине криптовалюта постепенно укрепляет свои позиции в финансовом секторе. Среди основных проблем классической финансовой системы, выделяется:

Централизация

Контроль движения финансовых средств осуществляется через банки, которые в случае необходимости могут заблокировать средства владельца счёта.

Контроль эмиссии и инфляции регулирующим органом

Выпуск денежной массы осуществляется центральным банком в зависимости от различных факторов и обстоятельств. К этой структуре также относиться механизм сдерживания инфляции.

Доступность

Для открытия банковского счёта необходимо посетить отделение банка, а для осуществления оплат банковской картой в торговых точках необходим платёжный терминал. Эти факторы могут быть недоступны в отдаленных точках мира, несмотря на развитую банковскую инфраструктуру.

Высокие комиссии

Посреднические функции банков требуют значительных финансовых затрат. Это отражается на стоимости финансовых операции возлагаемых на конечных пользователей.

2.1 Решение проблемы, предлагаемые сетью AKRA

В основу идеи создания сети AKRA является запуск универсального платежного инструмента доступного в любой точке мира, где есть Интернет. При этом обеспечить максимальный охват потенциальных клиентов, предоставляя удобство пользования, функциональность и низкую стоимость финансовых услуг.

Платёжная система, разработанная в экосистеме рассчитана как на физических, так и на юридических лиц. Для компаний нет ограничений в месте регистрации, что позволяет решить проблему некоторых законодательных запретов присутствующих в определённом государстве.

Комиссионные сборы и взаимодействие между блокчейнами, являющиеся значительной частью расходов в большей степени решаемо благодаря использованию блокчейн-мостов.

3.1 Описание сети AKRA

Появление децентрализованной финансовой системы на основе криптовалюты связано с нарастающими проблемами классической банковской системы. Эмитентом денег является центральный банк делегируя часть функций другим организациям (частным банкам и финансовым организациям). Наличие этих факторов влияет на конфиденциальность и приватность конечных пользователей. Криптовалюта, работающая на блокчейне предлагает альтернативу классической финансовой системе, позволяя достичь полной децентрализации финансового управления.

AKRA network предоставляет многофункциональную платежную систему, которая поддерживая работу как с криптовалютой, так и с традиционными финансами. Основой цифровой экономики является токен AKRA token, созданный на двух блокчейнах Ethereum и Binance Smart Chain с равной эмиссией по 1 000 000 000 единиц.

Широкий функционал

При создании токена используются различные параметры и готовые шаблонные решения, позволяющие выполнить запросы разработчиков и наделить необходимыми функциями требуемые для проекта AKRA.

Прозрачность работы смарт-контрактов

Условия функционирования сети прописываются в смарт-контракте, что позволяет обеспечить равные условия для всех участников сети.

Скорость транзакции

Средняя скорость обработки транзакций составляет 2000-4000 операций за секунду.

3.2 Структура сети

3.3 Блокчейн

Блокчейн состоит из блоков содержащие данные о работе сети, связанные между собой цепочкой. Связь между блоками обеспечивается не только нумерацией, но и тем, что каждый блок содержит свою собственную хеш-сумму предыдущего блока. Изменение информации переноситься в следующий блок, не затрагивая предыдущие. Копии реестра блокчейна хранятся на разных устройствах, что значительно увеличивает безопасность в случае отключение большей части их от сети.

Сеть AKRA построена на базе двух блокчейнов Binance Smart Chain и Ethereum. Binance Smart Chain, обладает хорошей функциональностью и совместимостью с виртуальной машиной Ethereum Virtual Machine (EVM). Компоненты, работающие в экосистеме:

1

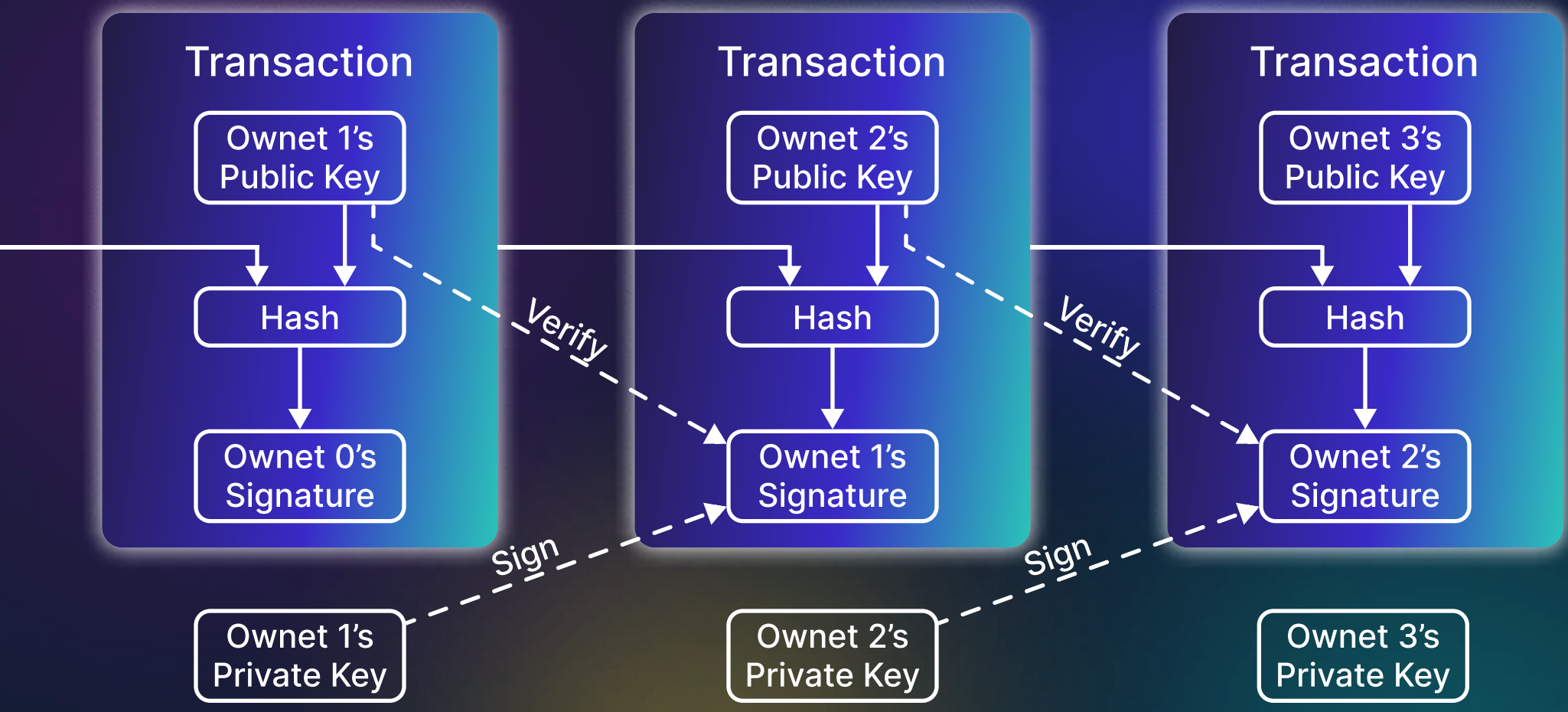
Полные узлы: «обычные» полнофункциональные узлы и кошельки.

2

Легкие узлы: узлы SPV и ещё более легкие узлы (например, те, которые просто подписывают транзакции)

3

Сервисные узлы: узлы со специальными функциями для предоставления данной услуги сверх обычной работы блокчейна.



AKRA считает, что блокчейн является одной из основ для следующего поколения информационных технологий, наряду с новыми направлениями, такими как Интернет-вещи, умный дом, 5G и другие. Благодаря защищенным от несанкционированного доступа характеристикам технологии, блокчейн, как инфраструктурная технология, обладает уникальными возможностями для обеспечения беспрецедентной ценности и передачи данных среди широкого круга пользователей без доверия, повышая эффективность и подлинность самой передачи информации.

3.4 Информация о блокчейне

Функции в блокчейне доступные для токенов AKRA (BEP-20):

Transfer

отправка токенов

Approve

разрешение смарт-контракту распоряжаться токенами по требованию вызывающего.

Increase Allowance

увеличение количества токенов, которыми можно распоряжаться используя функцию Approve.

Decrease Allowance

уменьшение количество токенов, которыми можно распоряжаться используя функцию Approve.

Transfer From

передача токенов под управление смарт-контракта.

Функции токенов доступные для мониторинга в реестре блокчейна:

Total Supply

общее количество выпущенных токенов (эмиссия).

Name

название токенов.

Symbol

символ токена.

Decimals

количество знаков после запятой в токене.

Balance Of

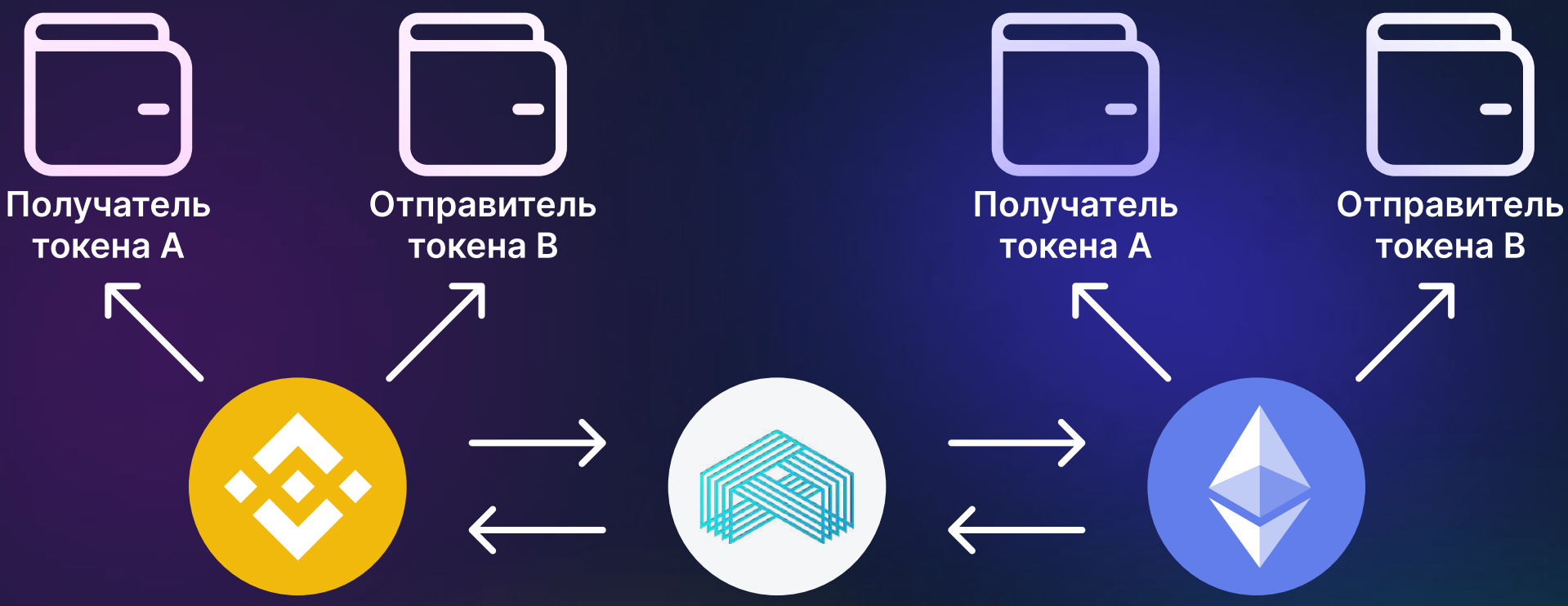
проверка баланса токенов на кошельках.

Allowance

проверка доступных токенов, которыми смарт-контракт сможет распоряжаться после вызова функции Approve, Increase Allowance.

4.1 Блокчейн-мост (Кросс-чейн)

Блокчейн-мост или кросс-чейн используется для решения проблем связанных с переводом цифровых средств между различными блокчейн-сетями. Не используя данную функцию переводить монеты можно с помощью криптовалютных бирж или P2P обменников, а это значительно увеличивает время, затрачиваемое на транзакцию и стоимость комиссии. Биржевой метод подразумевает использование внутренних пулов ликвидности и внутренних кошельков. Этот метод не является децентрализован. Используя технологию блокчейн-моста весь процесс полностью децентрализован, работающий на уровне блокчейнов. За соблюдениями условий в процессе работы отвечают смарт-контракты.



Принцип работы заключается в передачи цифрового актива из базовой цепочки во вторичную цепочку и наоборот. Практически происходит блокирование средств в одной цепочке и разблокирование такого же количество активов в другой, действуя по принципу двойной привязки (2WP).

Проблемы, решаемые технологией блокчейн-моста:

Масштабирование и снижение нагрузки на сеть

Работа в цепочках L1 и L2 эффективней распределяет нагрузку на сеть, что особенно важно при большом количестве транзакций.

Снижение стоимости комиссии

Достигается путём прямого взаимодействия между блокчейнами не привлекая централизованных посредников.

Безопасность

В процессе обмена вся последовательность действий работы контролируется смарт-контрактами, что исключает риски вмешательства третьей стороны.

Взаимодействие

Технология позволяет поддерживать работу с различными блокчейнами, которые подключены к блокчейн-мосту AKRA.

5.1 Криптографические примитивы

Схема разделения секрета Шамира применяется в криптографии и реализована в сети AKRA. Принцип работы заключается в разделении секрета (***t***, ***n***) между участниками ***Pn***, ... ***Pn*** так, чтобы любое количество участников ***t*** могли восстановить секрет ***s***. В то же самое время меньшая группа участников не получает никакой информации о секрете ***s***.

- Дилер выбирает $\in R$ ***Zq*** (где ***n*** < ***q***).
- Дилер выбирает случайного участника ***f*** (.) над ***Zq*** степени не более ***t-1*** удовлетворяющий ***f(0) = s***.
- Каждый игрок ***Pi*** получает ***si = f(i)*** в качестве своей доли.
- Дилер вычисляет открытый ключ участников как ***P = s.G***.
- Открытый и закрытый ключ делятся на: ***(pk,(sk1, ... , skn)) = (P,(s1, ... , sn))***.

5.2 Секретная конструкция

Произвольная группа ***P*** из ***t*** участников может восстановить многочлен ***f(.)*** по формуле Лагранжа следующим образом:

$$f(u) = \sum f(i)\omega(u) \text{ , где } \omega_i(u) = \prod_{i \in \rho, j \neq i} \frac{u-i}{i-j} \ mod\ q$$

5.3 Обмен секретными ключами

Используется обозначение эллиптической кривой для задачи дискретного логарифмирования. Предположим, что ***q*** — большое простое число, а ***G,H*** — образующие подгруппы порядка ***q*** эллиптической кривой ***E***. Предположим, что ***E*** выбрана таким образом, что задача дискретного логарифмирования в подгруппе, порожденной ***G***, трудна, поэтому невозможно вычислить целое число ***d*** такое, что ***G = dH***.

5.4 Схема обмена секретными ключами для предотвращения мошенничества

Схема проверки секретного обмена (VSS) реализованного в сети AKRA предотвращает возможное мошенничество участников. В VSS каждый пользователь может подтвердить свою долю, если кто-то распространяет несогласованные транзакции, то он будет обнаружен.

Предположим, что у участника есть секрет ***s0*** $\in$ ***Zq*** и случайное число ***s0*** $\in$ ***Zq***, и он привязан к паре ***(s,s0)*** через общедоступную информацию ***C0 = sG + s0H***. Секрет ***s*** может быть разделен между ***P1,⋯ ,Pn*** следующим образом.

Участник выполняет следующие действия:

1. Случайные полиномы $f(u) = s + t_1 u + \ldots + f_{t-1} u^{t-1}$, где $s, s', f_k, f'_k \in \mathbb{Z}_q$ for $k \in \{1, \ldots, t-1\}$
2. Вычисляем $(s_i, s'_i) = (f(i), f'(i))$ for $i \in \{1, \ldots, n\}$
3. Отправляем (s_i, s'_i),секрет для участника Pi для $i \in \{1, \ldots, n\}$
4. Транслируя значения $C_k = f_k G + f'_k H$ for $k \in \{1, \ldots, t-1\}$

5.5 Формулы

Ключи

- Секретный ключ: $s = x \in \mathbb{Z}_n^*$
- Публичный ключ: ***P = x.G***

Подпись

1. $k \leftarrow \$\mathbb{Z}_n^*$
2. ***(x1,y1) = k.G***
3. ***q = x1 mod n.*** если ***q = 0***, вернемся к шагу 1
4. ***r = k–1(h + qs) mod n.*** если ***r = 0***, вернёмся к шагу 1
5. Возврат ***(q,r)***

Подпись

1. $w = r^{-1}\ mod\ n$
2. $u_1 = hw\ mod\ n$
3. $u_2 = qw\ mod\ n$
4. ***(x1,y1) = u1.G + u2.P***. если ***(x1,y1)*** равен тождеству, то подпись недействительна

Подпись действительна, если $q = x_1\ mod\ n$ **,недействительным в противном случае**

6.1 Безопасность

В сети AKRA реализован механизм криптошифрования обеспечивающий высокую степень безопасности криптовалютных операций. Детальный принцип функционирования описан выше. Хранение токенов производиться как на «холодных», так и на «горячих» типах кошельков. Для наибольшей степени надёжности разработчики AKRA создали собственную линейку криптокошельков.

Основным решением проблемы безопасности сети AKRA является механизм двусторонней привязки (2WP), позволяющий передавать актив из базовой цепочки во вторичный блокчейн и наоборот. Принцип действия заключается во временной блокировке в базовом блокчейне необходимого количества монет. В этот момент разблокируется это же количество токенов, во вторичном блокчейне. Активы базового уровня могут быть разблокированы, когда эквивалентное количество токенов во втором блокчейне снова заблокировано. Механизм действия 2WP безопасности основывается на честности большинства участников сети, задействованных в работе 2WP.

При отправке средств на адрес кошелька сети AKRA проверяется внешняя транзакция внутри смарт-контракта. После этого возможна проверка включения транзакция в блок, и далее вычисляя уровень сложности по цепочки, минимизируя возможность мошеннических действий.

7.1 Токеномика

Основу цифровой экономики составляет токен AKRA Token работающий на протоколах BEP-20 (Binance Smart Chain) и ERC-20 (Ethereum). Эмиссия каждого протокола составляет 1 000 000 000 токенов (общая 2 000 000 000 единиц). После запуска coin AKRA blockchain на собственном блокчейне существующие токены будут обменяны на монету по курсу 1:1.

График распределения токенов AKRA

7.2 Технический стандарт токенов BEP-20 и ERC-20

Разработка токенов AKRA базируется на стандартах BEP-20 (Binance Smart Chain) и ERC-20 (Ethereum). Обе платформы работают на одной виртуальной машине EVM (Ethereum Virtual Machine). Адреса криптовалюты в BEP-20 (BSC) и ERC-20 (Ethereum) идентичны, что позволяет проводить транзакции между собой.

Применение двух блокчейнов позволяет расширить возможности сети AKRA и увеличить, тем самым количество потенциальных пользователей. Использование токенов на основе BEP-20 решает проблему с высокими комиссиями за переводы, а стандарт ERC-20 увеличивает безопасность и масштабируемость сети.

Технические характеристики BEP-20 и ERC-20

Характеристики	BEP-20	ERC-20
Блокчейн	Binance Smart Chain	Ethereum
Время создания блока	3 секунды	13 секунд
Средняя стоимость комиссия	$ 0,05 – 0,20	$ 5 – 20
Пропускная способность	300+ TBs	15 TBs
Количество транзакций	До 4000/сек	25/сек
Майнинг/стейкинг	+	+

7.3 Комиссионные сборы

Оплата комиссий за транзакции в сети AKRA (ERC-20) производиться в GAS, так же, как и в сети Ethereum. Используя протокол ERC-20 механизм ценообразования меняется в зависимости от спроса на транзакцию. Следует учитывать, что транзакционные издержки в Ethereum выше, чем в BSC. Если установить более низкую комиссию, то перевод в этом случае займёт больше времени.

Цены на GAS для оплаты комиссии колеблются в зависимости от рыночных факторов. При осуществлении перевода токена AKRA на BEP-20 (BSC) механизм начисления комиссии за переводы аналогичный сети Ethereum. Транзакции рассчитываются с использованием вычислительной мощности, необходимой для выполнения транзакций.

7.4 Хранение токенов

С целью обеспечения максимального удобства при пользовании токенами разрабатываются несколько типов криптовалютных кошельков и платёжная система Web Akra Wallet v1 работающая не только с криптовалютой, но и с фиатными деньгами. Представленные варианты имеют свои особенности в зависимости от определенных целей их использования.

Хранение цифровых активов на бирже не является самым надёжным вариантом по той причине, что ключи от кошелька хранятся у администрации биржи. В случае сбоев или взлома, высокая вероятность потери средств.

Разработка криптокошельков

1 **Akra Wallet mobile**
Мобильное приложение криптокошелька для работы на IOS и Android

2 **Web Akra Wallet v1**
Система фиатных платежей для физических и юридических лиц

3 **Akra Wallet Plagin**
Браузерная версия криптокошелька

4 **Akra Wallet desktop**
Криптокошелёк для десктопных версий

Токены AKRA также работают с другими типами кошельков поддерживающие протоколы ERC-20 и BEP-20. К ним относятся MetaMask, TrustWallet и другие мультивалютные криптокошельки представленные на рынке. Корректную и безопасную работу с токенами AKRA можно гарантировать только из линейки собственных разработок.

7.5 Ценообразование. Рыночное регулирование

Уникальная система с использованием двух протоколов для токенов (BEP-20 и ERC-20) значительно помогает отделить стоимость использования блокчейна от рыночных спекуляций. Из-за корреляции с использованием ресурсов блокчейна стоимость более предсказуема при мониторинге спроса и предложения AKRA token. Кроме того, механизм управления Фондом еще больше стабилизирует стоимость. Предполагаемая оценочная стоимость токена на рынках будет составлять 2$.

Изучив экономические модели большинства публичных блокчейн-сетей и проведя аналитику обнаружено самое большое препятствие для принятия массовых приложений на блокчейне: стоимость использования блокчейна напрямую связана с оценкой стоимости токенов. В то время как оценка токена обычно повышается по мере роста использования блокчейна, стоимость использования блокчейна варьируется в зависимости от того, хочет ли сторона проводить платежные транзакции или транзакции смарт-контрактов. Это даже не упоминает спекуляции инвесторов и трейдеров, как вкладчика в ценность блокчейна. Ни один владелец бизнеса не будет запускать приложения или бизнес на блокчейне или где-либо еще с непредсказуемой и нестабильной стоимостью.

8.1 Рекомендации для безопасной работы

Для безопасной работы в сети AKRA и криптовалюты в целом следует придерживаться некоторых рекомендаций, изложенных ниже.

Не разглашать пароль от кошелька

Ни при каких обстоятельствах не разглашать пароль от криптокошелька. Ответственность за сохранность средств лежит только на его владельце. Децентрализованное управление не позволяет заморозить или заблокировать цифровые активы, а также вернуть обратно отправителю в случае необходимости.

Проверять адрес транзакции перед отправкой

Указание неправильного адреса кошелька может повлечь за собой потерю средств, без возможности восстановления. Следует внимательно проверять адрес, на который будет осуществлена транзакция.

Транзакция не имеет обратной силы

Децентрализованная система криптовалюты построенная таким образом, что транзакции невозможно отменить или возвратить обратно отправителю.

Защищённое соединение

При проведении криптовалютных операций следует использовать защищённое соединение, чтобы исключить перехват паролей злоумышленниками, что в последствии может привести к не санкционируемому доступу к кошельку. Особенно следует обратить внимание при подключении через общедоступные сети Wi-Fi и VPN-сервисы.

ROAD MAP

- Q3 2021 — Основание проекта AKRA как универсальный денежный инструмент, (разработка логики экосистемы, разработка базы данных)
- Q4 2021 — Создание Akra
- Q4 2021 — Разработка web Akra Wallet v1 платежные системы для физических и юридических лиц
- Q4 2021 — Запуск стратегических партнерских программ
- Q4 2021 — Интеграция в Российскую компанию платежную систему Akra Wallet Merchant v1
- Q4 2021 — Реализацией платежной системы фиатных платежей для физических и юридических лиц через выставление счета
- Q3 2022 — AKRA Майнинг по технологии Proof of Stake Стейкинг
- Q3 2022 — Краудфандинговая площадка для инвесторов и заемщика
- Q4 2022 — Разработкой мобильного приложения для IOS и Android
- Q4 2022 — Все токены будут обменяны один к одному на coin AKRA blockchain
- Q4 2022 — Создание 13 глобальных офисов в качестве многоязычной поддержки и маркетинга
- Q4 2022 — Частичная продажа токенов 3 этапа продаж. Коллаборации с лидерами мнений из СНГ, нацеленное построение комьюнити
- Q1 2023 — Листинг на крупнейшей бирже криптовалют
- Q3 2023 — Листинг токена на Coinmarketcap, Coingecko. Первые листинги на централизованных биржах
- Q3 2023 — Листинг токена на децентрализованной бирже Pancakeswap, Uniswap
- Q4 2023 — Разработка Akra Wallet desktop для Windows, Mac, Linux
- Q4 2023 — Разработка Akra Wallet Плагин web browser
- Q4 2023 — Мосты между blockchain Binance Smart Chain и Ethereum

Словарь терминов

- **Блок**: представляет собой набор записей об криптовалютных транзакциях, объединённых в блок и соединяющиеся между собой цепочками.
- **Блокчейн** (Blockchain): технология децентрализованного управления реестром сети, построенная на основе криптографического метода защиты информации, что исключает вмешательство в работу сети.
- **Валидаторы**: это узлы в системе блокчейна, которые берут на себя задачи по поддержанию работоспособности криптовалютной сети.
- **Закрытый ключ**: пароль для доступа к конфиденциальной информации.
- **Ключ**: параметр шифра, определяющий выбор конкретного преобразования данного текста.
- **Кросс-чейн (Cross-Chain)**: технология, обеспечивающая передачу данных и транзакций между различными блокчейнами.
- **Открытый ключ**: незашифрованные данные, передаваемые словами.
- **Цифровые подписи**: используются для установления подлинности документа, его происхождения и авторства. Исключает искажения информации в электронном документе.
- **API**: специальный протокол для взаимодействия компьютерных программ, который позволяет использовать функции одного приложения внутри другого.
- **Ethereum Virtual Machine (EVM)**: представляет собой вычислительную машину, которая действует как децентрализованный компьютер с миллионами исполняемых проектов.
- **SPV**: лёгкие узлы в блокчейне подписывающие транзакции.

Юридическая информация

Отношение между поставщиком и покупателем регулируются Федеральным законом «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 N 259-ФЗ.

Источники

- Информационная безопасность — Википедия (wikipedia.org)
- Криптография. Криптография — Википедия (wikipedia.org)
- Berry Schoenmakers, Lecture notes on cryptographic protocols, 2021.
- Создание смарт-контрактов Solidity для блокчейна Ethereum. Практическое руководство.
Фролов Александр Вячеславович
- Mastering Bitcoin: Programming the Open Blockchain. M. Antonopoulos