STABILA
ОТКРЫТАЯ
СЕТЬ

Децентрализация финансовой системы

БЕЛАЯ КНИГА

Развитие децентрализованных финансов.

1.ВВЕДЕНИЕ

STABILA — это проект, целью которого является децентрализация финансовой системы. Протокол STABILA предлагает публичный блокчейн-сервис и поддержку высокой пропускной способности, высокой масштабируемости и высокой доступности для всех децентрализованных приложений (DApps) в экосистеме STABILA.

"Цифровая трансформация позволяет миру полностью перестроиться — и Moneta с удовольствием принимает участие в этих изменениях, предоставляя клиентоориентированные услуги и налаживая долгосрочные отношения."

www.stabilascan.org

2.ТЕРМИНОЛОГИЯ

Адрес/кошелек

Адрес или кошелек, который содержит данные учетной записи в сети STABILA, создается с помощью пары ключей, состоящей из закрытого и открытого ключей. Открытый ключ обычно используется для шифрования сеансовых ключей, верификации подписи и шифрования данных, которые можно расшифровать с помощью соответствующего закрытого ключа.

ABI

Двоичный интерфейс приложения (ABI) — это интерфейс между двумя двоичными программными модулями; обычно один из этих модулей - это библиотека или операционная система, а другой — программа, запускаемая пользователем.

API

Программный интерфейс приложения (API) в основном используется для разработки пользовательских клиентов. Благодаря поддержке API разработчики могут самостоятельно создавать платформы для выпуска токенов.

Актив

Согласно документации STABILA, актив - это то же самое, что и токен, который также обозначается как токен TRC-10.

Очки пропускной способности (BP)

Для поддержания бесперебойной работы сети, для транзакций в се ти STABILA в качестве топлива используются BP. Ежедневно каждый аккаунт получает 500 бесплатных BP, а дополнительное количество можно получить, если обменять STB за BP (в соответствии с Соглашением о депонировании). Передача STB и токенов TRC-10 - это обычные транзакции, на которые расходуются BP. Для транзакций по развертыванию и исполнению смарт-контрактов используются как BP, так и UCR.

Блок

Блоки содержат цифровые записи транзакций. Полный блок состоит из номера, размера блока, заголовка блока, счетчика транзакций и данных транзакции.

Вознаграждение за блок

Вознаграждения за создание блоков отправляются на субсчет (адрес/кошелек). Управляющие и исполнители могут получить свои вознаграждения на stabilascan или напрямую через API.

Заголовок блока

Заголовок блока - это его часть. Заголовки блоков STABILA содержат хэш предыдущего блока, корень Меркла, временную метку, версию и адрес свидетеля.

Холодный кошелек

Холодный кошелек, также известный как оффлайн-кошелек, позволяет хранить закрытый ключ полностью в автономном режиме. Холодные кошельки обычно устанавливают на "холодные" устройства (например, компьютеры или мобильные телефоны, работающие в автономном режиме), чтобы обеспечить безопасность закрытого ключа STB.

DApp

Децентрализованное приложение - это приложение, которое работает без участия централизованной доверенной стороны. Это приложение обеспечивает прямое взаимодействие/договоренности/коммуникацию между конечными пользователями и/или ресурсами без посредника.

gRPC

(Удаленный вызов процедур) - это система удаленного вызова процедур (RPC) с открытым исходным кодом, первоначально разработанная в Google. В качестве транспорта используется HTTP/2, в качестве языка описания интерфейса — Protocol Buffers. gRPC предоставляет такие функции как аутентификация, двунаправленная потоковая передача и управление потоком, блокирующие или неблокирующие привязки, а также отмена и тайм-ауты. Эт система генерирует кроссплатформенные привязки клиента и сервера для многих языков. Среди наиболее распространенных случаев использования можно отметить подключение служб в микросервисном стиле архитектуры и подключение мобильных устройств и браузерных клиентов к серверным службам.

Горячий кошелек

Горячий кошелек, также известный как онлайн-кошелек, позволяет использовать закрытый ключ пользователя в режиме онлайн, поэтому он может подвергаться потенциальным угрозам или перехватываться злоумышленниками.

JDK

Java Development Kit - это комплект для разработки программного обеспечения, который используется для приложений на языке Java. Это ядро разработки Java, которое включает в себя среду приложений Java (JVM + библиотека классов Java) и инструменты Java.

LevelDB

Изначально LevelDB создавался с целью удовлетворить потребности в быстром обмене данными и оперативной разработке.

Корень Меркла

Корень Меркла - это хэш всех хэшей всех транзакций, которые содержатся в блоке сети блокчейн.

Открытая тестовая сеть

Версия сети, которая работает в конфигурации с тремя узлами. Разработчики могут подключаться и тестировать функции, не беспокоясь об экономических потерях. Токены Testnet ничего не стоят, и любой желающий может запросить больше из открытого сайта-крана.

RPC

В распределенных вычислениях удаленный вызов процедуры (RPC) означает, что компьютерная программа вызывает выполнение процедуры (подпрограммы) в другом адресном пространстве (обычно на другом компьютере в общей сети), что кодируется так, как если бы это был обычный (локальный) вызов процедуры, без явного кодирования программистом деталей для удаленного взаимодействия.

Масштабируемость

Масштабируемость - это свойство протокола STABILA. Это способность системы, сети или процесса справляться с растущим объемом работы или потенциал их расширения для обеспечения этого роста.

UNIT

UNIT это наименьшая единица STB. 1 STB = 1,000,000 UNIT.

Пропускная способность

Высокая пропускная способность является характерной особенностью сети STABILA Mainnet. Она измеряется в транзакциях в секунду (TPS), а точнее, это максимальная пропускная способность транзакций за одну секунду.

Временная метка

Приблизительное время создания блока записывается в виде временной метки Unix, которая представляет собой количество миллисекунд, прошедших с 00:00:00 01 января 1970 года по UTC.

TRC-10

Стандарт криптографического токена на платформе STABILA. Во время проведения первичного предложения монет на блокчейне STABILA необходимо соблюдать определенные правила и принципы.

STB

STB обозначает Stabila и является официальной криптовалютой STABILA.

3. АРХИТЕКТУРА

STABILA работает на основе 3-уровневой архитектуры.

1. *Уровень хранения*
2. *Основной уровень*
3. *Уровень приложений.*

Протокол STABILA использует Google Protobuf, который по своей сути поддерживает многоязычное расширение.

Виртуальная машина STABILA (SVM)

SVM - это легкая, Тьюринг-полная виртуальная машина. SVM без проблем подключается к существующей экосистеме.

Децентрализованная биржа (DEX)

Сеть STABILA изначально поддерживает функции децентрализованной биржи. Децентрализованная биржа содержит несколько торговых пар. Торговая пара (условно "Биржа") - это биржевой рынок между токенами TRC-10 или между токеном TRC-10 и STB. Любой аккаунт может создать торговую пару между любыми токенами.

Код блокчейна STABILA выполнен на языке Java и изначально был форком от STABILA.

4. КОНСЕНСУС

Делегированное доказательство доли (DPoS)

Механизм консенсуса Доказательство доли (Proof of Stake, PoS) применялся во многих новых сетях. В сетях PoS держатели токенов блокируют свои балансы токенов, чтобы стать валидаторами блоков. Валидаторы по очереди предлагают и голосуют за следующий блок. Однако проблема стандартного механизма PoS заключается в том, что влияние валидаторов напрямую зависит от количества заблокированных токенов. В результате стороны, накопившие большое количество базовой валюты сети, получают неправомерное влияние на экосистему сети.

Механизм консенсуса STABILA использует инновационную систему Делегированного доказательства доли, в которой 21 управляющий (Gs) создает блоки для сети. Каждые 6 часов владельцы STB-аккаунтов, открывшие свои счета, могут голосовать за выбор Исполнителей, а 21 лучший Исполнитель становится Управляющим.

Сеть протокола STABILA генерирует один блок каждые три секунды.

5. АККАУНТ

В сети STABILA существует три типа аккаунтов.

1. *Обычные счета используются для стандартных транзакций.*
2. *Токен-аккаунты используются для хранения токенов TRC-10.*
3. *Контрактные аккаунты - это аккаунты смарт-контрактов, которые создаются на обычных аккаунтах и также могут запускаться обычными аккаунтами.*

Создание аккаунта

Существует три способа создания аккаунта STABILA:

1. *Создать новый аккаунт через API*
2. *Перевести STB на новый адрес аккаунта*
3. *Перевести любой токен TRC-10 на новый адрес аккаунта*

Генерация закрытого ключа и адреса

Можно сгенерировать пару ключей в автономном режиме, состоящую из адреса (открытого ключа) и закрытого ключа. Алгоритм генерации адреса пользователя заключается в генерации пары ключей, а затем извлечении открытого ключа (64-байтовый массив, представляющий координаты x, y). Хешируйте открытый ключ с помощью функции SHA3-256 (принятый протокол SHA3 - KECCAK-256) и извлеките последние 20 байт результата. Добавьте 3F в начало массива байтов и убедитесь, что исходная длина адреса составляет 21 байт. Хешируйте адрес дважды с помощью функции SHA3-256 и используйте первые 4 байта в качестве кода верификации. Добавьте код верификации в конец исходного адреса и вы получите адрес в формате base58check путем шифрования base58. Зашифрованный адрес Mainnet начинается на S и составляет 34 байта в длину.

6. ТРАНЗАКЦИИ

Подписание

Процесс подписания транзакций в STABILA осуществляется по стандартному криптографическому алгоритму ECDSA с кривой выбора SECP256K1. Закрытый ключ - это рандомное число, а открытый ключ - это точка на эллиптической кривой. Процесс генерации открытого ключа заключается в том, что сначала генерируется случайное число для закрытого ключа, а затем базовая точка на эллиптической кривой умножается на закрытый ключ для получения открытого ключа. Когда проводится транзакция, сначала исходные данные транзакции преобразуются в формат байтов. Затем исходные данные проходят процедуру хэширования SHA-256. Закрытый ключ, который соответствует адресу контракта, подписывает результат хэширования SHA256. Результат подписи добавляется к транзакции.

7. ПРОПУСКНАЯ СПОСОБНОСТЬ

Модель пропускной способности

Для обычных транзакций требуются только очки пропускной способности, но для операций по смарт-контрактам используются как UCR (единицы обычных ресурсов), так и очки пропускной способности.

Существует два типа очков пропускной способности.

Пользователи могут получить очки пропускной способности, заключив Соглашения о депонировании (CD) с STB, при этом каждый день предоставляется 500 бесплатных очков пропускной способности. Когда производится трансляция транзакции STB, она передается и хранится в виде массива байтов по сети.

Количество очков пропускной способности, необходимых для одной транзакции, равно количеству байтов транзакции, умноженному на скорость передачи очков пропускной способности.

***Например**:*

длина массива байтов транзакции составляет 200, значит, на эту транзакцию расходуется 200 очков пропускной способности.

Однако если в результате передачи STB или токена будет создан целевой счет, тогда будут списаны только очки пропускной способности, затраченные на создание счета, а дополнительные очки пропускной способности сниматься не будут.

В случае создания счета сеть сначала будет расходовать очки пропускной способности, которые инициатор транзакции получил от Соглашения о депонировании STB. Если этого количества недостаточно, то сеть расходует STB инициатора транзакции. В стандартных случаях передачи STB с одного STB-счета на другой сеть сначала расходует очки пропускной способности, полученные инициатором транзакции за Соглашения о депонировании STB. Если этого недостаточно, то расходуются бесплатные 500 ежедневных очков пропускной способности. Если и этого недостаточно, то сеть расходует STB инициатора транзакции.

Сумма рассчитывается по количеству байтов в транзакции, умноженному на 6 UNIT. Таким образом, для большинства держателей STB, которым не обязательно иметь Соглашение о депонировании своих STB для участия в голосовании управляющих, автоматически пропускается первый шаг (так как депонированный баланс STB = 0), и транзакция выполняется за счет 500 ежедневных бесплатных очков пропускной способности.

При передаче токенов TRC-10 сеть сначала проверяет, достаточно ли общего количества бесплатных очков пропускной способности выпущенного актива токена. Если нет, то используются очки пропускной способности, полученные от Соглашения о депонировании STB. Если очков пропускной способности все еще не хватает, то используются STB инициатора транзакции.

8. КОМИССИЯ

Комиссия

Сеть STABILA, как правило, не взимает комиссию за большинство транзакций, однако, в силу ограничений и объективности системы, за использование пропускной способности и проведение некоторых транзакций взимается определенная плата.

1. *Для обычных транзакций используются очки пропускной способности.*
2. *Для смарт-контрактов нужны UCR, но очки пропускной способности понадобятся для трансляции и подтверждения транзакции.*
3. *Все транзакции по запросам проводятся бесплатно. Для них не нужны ни UCR, ни пропускная способность.*

Сеть STABILA также установила ряд фиксированных комиссий для следующих транзакций:

1. *Создание узла-свидетеля: 1000 STB*
2. *Выпуск токена TRC-10: 1000 STB*
3. *Создание нового аккаунта: 1385 UNIT*
4. *Создание валютной пары: 14 STB*

Подтверждение транзакции

Транзакция попадает в будущий блок после ее трансляции в сеть. После того как на STABILA майнится 19 блоков (включая собственный блок), транзакция подтверждается. Каждый блок майнит один из 21 лучших управляющих. На майнинг каждого блока на блокчейне уходит 3 секунды.

9. ВИРТУАЛЬНАЯ МАШИНА STABILA

Виртуальная машина STABILA (SVM)

SVM - это легкая, Тьюринг-полная виртуальная машина, разработанная для экосистемы STABILA. Ее цель заключается в обеспечении эффективного, удобного, стабильного, безопасного и масштабируемого блокчейн-сервиса. SVM изначально была форком от STABILA и может легко взаимодействовать с существующей экосистемой разработки смарт-контрактов Solidity.

Кроме того, SVM поддерживает консенсус DPoS. SVM использует концепцию UCR. Операции с транзакциями и смарт-контрактами в SVM выполняются бесплатно, без потребления STB.

Компилятор сначала переводит смарт-контракт Solidity в байткод, который можно прочитать и выполнить на SVM. Затем SVM обрабатывает данные с помощью операционного кода, который аналогичен функционированию стекового конечного автомата.

10. СМАРТ-КОНТРАКТЫ

Совместимость

SVM является совместимой с EVM и в будущем станет совместимой с более распространенными виртуальными машинами. Однако в связи с мошенничеством в среде смарт-контрактов прежде чем любой пользователь сможет развернуть смарт-контракт, будет предложена процедура лицензирования.

Лицензирование смарт-контрактов

Смарт-контракты являются бесполезными и будут такими оставаться в ближайшем будущем. В них отсутствует механизм проверки активов и они не могут взаимодействовать с внешним миром. Предлагаемая модель лицензирования заключается в том, чтобы разрешить только те смарт-контракты, которые имеют практическое применение и подтверждены активами, основанными на логике и корпоративной структуре. В случае, если владелец смарт-контракта не сможет обеспечить выполнение своего смарт-контракта, ответственность будет нести третья сторона, таким образом, клиенты сети STABILA будут защищены.

Модель единиц обычных ресурсов (UCR)

Максимальный предел UCR для развертывания и запуска смарт-контракта зависит от нескольких переменных:

- *Динамический UCR от Соглашения о депонирования 1 STB = 30,000,000,000 (Общий лимит UCR) / (Общий вес UCR)*
- *Лимит UCR - это ежедневный лимит UCR счета из Соглашения о депонировании STB*
- *Остаток ежедневного UCR счета из Соглашения о депонировании STB рассчитывается как Лимит UCR - Использованный UCR*
- *Лимит комиссии в STB устанавливается при развертывании/пусковом вызове смарт-контракта*
- *Остаток используемых STB на счету*

Функция смарт-контрактов будет активирована в феврале 2022 года.

11. УПРАВЛЕНИЕ

Управляющие

С каждого аккаунта в сети STABILA можно подать заявку и получить возможность стать Исполнителем (обозначается как E). Каждый может голосовать за Исполнителей. 21 лучший Исполнитель, набравший наибольшее количество голосов, станет Управляющим с правом и обязательством генерировать блоки. Голоса подсчитываются каждые 6 часов, и соответственно меняются G. В целях предотвращения атак злоумышленников, за получение статуса руководителя необходимо заплатить. При подаче заявки со счета заявителя будет снято 1000 STB. В случае успеха этот аккаунт может участвовать в выборах G.

Выборы

Для голосования потребуется мощность STABILA (обозначается как SP), и количество SP зависит от депонированных активов избирателя (STB). SP рассчитывается следующим образом: 1 SP = 1 депонированный STB для получения пропускной способности.

Каждый аккаунт в сети STABILA имеет право голосовать за собственного G. После выхода (без депонирования, будет доступно через 3 дня), у пользователей не будет никаких депонированных активов и, соответственно, они потеряют всю SP. В результате, все голоса станут недействительными для текущего и последующего раунда голосования, если только STB не будут снова депонированными для голосования.

Награда для Исполнителей

В качестве награды для Исполнителей 79 лучших Исполнителей, обновляемых каждый раунд (6 часов), разделят между собой 78 STB заработанных в результате майнинга. Вознаграждение будет распределяться в соответствии с весом голосов каждого Исполнителя.

Общее вознаграждение для E за раунд = 10 972 UNIT/блок × 20 блоков/мин × 60 мин/час × 6 часов/раунд.

Ежегодно 79 G получают в общей сложности 28 834 STB.

Вознаграждение за блок

Также известное как Вознаграждение для Управляющего, в рамках которого 21 лучший Управляющий (Gs), избираемый в каждом раунде (6 часов), будет делить между собой примерно 1 596 STB, заработанных в результате майнинга. Награда будет делиться поровну между 21 G.

Общее вознаграждение за раунд = 221 714 Unit/блок x 20 блоков/мин x 60 мин/час x 6 часов/раунд.

В общей сложности 21 Gs будут ежегодно получать 2 330 657 STB.

12 **ПАРАМЕТРЫ СЕТИ** STABILA

Количество токенов в обороте *Количество монет STB, которые находятся в открытом доступе и в обороте на рынке.*	**20,000,000**
Общее предложение *Общее предложение - это количество STB, которые существуют в настоящее время и либо находятся в обороте, либо заблокированы для майнеров.*	**30,000,000**
Максимальное предложение 30,000,000 *Максимальное предложение - это максимальное количество монет STB, которое когда-либо будет создано.*	**30,000,000**
Скорость создания блоков *Количество секунд на создание 1 блока.*	**3**
Майнеры/Управляющие *Узлы для создания блоков.*	**21**
Консенсус *67% управляющих достигают консенсуса по созданию следующего блока.*	**15**
1 STB = () Units *UNIT - наименьшая единица STB.*	**1,000,000**

СПАСИБО

"У нас есть опыт на криптовалютном рынке, и мы стремимся к тому, чтобы инвесторы и трейдеры лучше ориентировались в основах того, что они покупают".

Дэниел Варзари, генеральный директор

"Блокчейн - это новая технологическая парадигма нашего времени. Он кардинально изменит принципы работы всего финансового мира".

Игорь Скворцов, финансовый директор

"Однажды в ближайшем будущем все будет токенизировано и связано с помощью блокчейна".

Анастасия Ковалева, вице-президент по странам Азии

ООО МОНЕТА ХОЛДИНГ

СЕНТ-ВИНСЕНТ И ГРЕНАДИНЫ

ПЕРВЫЙ ЭТАЖ
ПЕРВОЕ ОТДЕЛЕНИЕ БАНКА
СЕНТ-ВИНСЕНТ БЭНК
ДЖЕЙМС-СТРИТ
КИНГСТАУН

ТЕХНОЛОГИЯ БЛОКЧЕЙН

Развитие децентрализованных финансов.

info@moneta.holdings

info@stabilascan.org