Cashiva Standard Token (CST) Whitepaper

1. Введение

Cashiva Standard Token (CST) — это серия токенов, полностью обеспеченных криптовалютой и выпускаемых на блокчейне Ethereum. В отличие от традиционных стейблкоинов, CST обеспечивает фиксированную стоимость в выбранной фиатной валюте только на момент транзакции, при этом само обеспечение всегда представлено ликвидными криптоактивами (например, BTC, ETH, XMR).

Каждый токен CST соответствует уникальной валютной паре, и его обозначение строится по следующей схеме:

- XXYYY, где:
  - XX — код фиатной валюты (например, RUB, USD, KGS);
  - YYY — код криптовалюты, выступающей обеспечением (например, BTC, ETH, XMR).

Примеры:

- RUBTC — токен, обеспеченный биткоином, номинированный в российских рублях;
- USETH — токен, обеспеченный эфиром, номинированный в долларах США;
- KGXMR — токен, обеспеченный Monero, номинированный в кыргызских сомах.

Ключевая особенность CST — фиксирование справочной стоимости токена в фиатной валюте в момент подтверждения транзакции, что позволяет точно учитывать эквивалент передаваемой суммы без зависимости от рыночной волатильности.

2. Проблематика

2.1 Волатильность криптовалют

Криптовалюты подвержены высокой ценовой волатильности, что делает расчёты в них непредсказуемыми. Передав 0.1 BTC, нельзя заранее точно сказать, сколько это будет в рублях или долларах при получении. CST решает эту проблему, фиксируя цену токена в фиате в момент транзакции. Это делает расчёты прозрачными, даже если обеспечение — криптовалюта.

2.2 Почему не использовать фиатные стейблкоины?

Фиатные стейблкоины (USDT, USDC и другие) широко распространены, но у них есть критические ограничения:

- **Централизованное хранение:** Эти токены обеспечены фиатом, который хранится на счетах эмитента. Это делает их уязвимыми для блокировок, санкций, заморозки или отзыва.
- **Доверие к эмитенту:** Пользователи вынуждены полагаться на отчётность эмитента и аудит. При этом неоднократно возникали случаи недообеспечения и скрытых рисков.
- **Банковская зависимость:** Такие токены зависят от банков и юрисдикций. В случае регуляторных ограничений актив может быть заблокирован или делистнут с бирж.

2.3 CST — децентрализованная альтернатива

CST решает эти проблемы благодаря архитектуре:

- **Обеспечение криптовалютой:** Нет зависимости от банков. Все активы находятся в блокчейне и доступны для проверки.
- **Прозрачность в реальном времени:** Любой пользователь может в любой момент убедиться в 100% обеспеченности токенов.
- **Фиат — только единица измерения:** CST не хранит фиат, а лишь отображает курс, что даёт удобство расчётов без системных рисков фиатных платформ.

3. Описание токенов CST

Каждый токен CST представляет собой обёртку (wrapped token), обеспеченную конкретной криптовалютой и номинированную в выбранной фиатной валюте. Это означает, что пользователи получают токен, номинированный, например, в рублях или долларах, но фактически хранящий в себе эквивалентную стоимость в ETH, BTC, XMR и других криптовалютах.

3.1 Схема обозначений

Каждый токен обозначается по формуле **XXYYY**, где:

- `XX` — код фиатной валюты (например, RUB, USD, KGS);
- `YYY` — код криптовалюты обеспечения (например, ETH, BTC, XMR).

3.2 Примеры токенов

- `RUBETH` — номинирован в российских рублях, обеспечен эфиром;
- `USETH` — номинирован в долларах США, обеспечен эфиром;
- `KGXMR` — номинирован в кыргызских сомах, обеспечен Monero;
- `RUBBTC` — номинирован в российских рублях, обеспечен биткоином.

3.3 Принцип работы

- Токены CST всегда обеспечены в соотношении 1:1 соответствующей криптовалютой.
- При каждом выпуске или погашении CST фиксируется **справочная цена** в фиатной валюте, полученная через оракул. Эта цена не влияет на количество выпускаемых токенов, но служит для точной финансовой отчётности, расчётов и отображения стоимости.
- Курс фиксируется в момент подтверждения транзакции и записывается в блокчейн для прозрачности.

3.4 Отличие от фиатных стейблкоинов

В отличие от традиционных стейблкоинов (USDT, USDC), CST:

- **Не зависит от банков** и не хранит фиатные резервы;
- **Обеспечен криптовалютой** с полной проверяемостью в блокчейне;
- **Использует фиат как единицу счёта**, а не как актив обеспечения.

3.5 Статус и планы выпуска

- В момент запуска доступны токены: `RUBETH`, `KGSETH`, `PRRUBETH`.
- В течение трёх месяцев планируется выпуск `RUBBTC`, `KGXMR` и `USDETH`.
- Новые пары будут добавляться в зависимости от спроса и предпочтений сообщества.

4. Целевая аудитория и рынки применения

4.1 Пользователи, нуждающиеся в прозрачности расчётов и защите от волатильности

- Физические и юридические лица, которым важно заранее зафиксировать сумму в фиате при переводах или оплате.
- Онлайн-бизнес, принимающий криптовалюту.
- Пользователи из стран с высокой инфляцией.

4.2 Криптовалютные трейдеры и инвесторы

- Для временной фиксации стоимости активов.
- Для расчётов без зависимости от курса обеспечения.

4.3 DeFi-платформы и разработчики

- Для использования CST в кредитовании, торговле, деривативах.

5. Техническая архитектура

CST реализован в виде смарт-контрактов стандарта ERC-20, размещённых в сети Ethereum. Каждый контракт соответствует отдельной валютной паре и содержит жёстко заданные параметры обеспечения и единицы измерения.

5.1 Смарт-контракт CST

- Обеспечение токена хранится:
  - непосредственно на адресе смарт-контракта, если криптовалюта обеспечения находится в той же сети (например, ETH в сети Ethereum);
  - через доверенного хранителя, если обеспечение находится в другой сети (например, BTC или XMR).
- При каждой операции (wrap, burn, transfer) запрашивается курс у оракула и фиксируется справочная стоимость в фиатной валюте.
- Ключевые методы контракта:
  - `wrap()` — приём криптообеспечения и выпуск CST-токенов;
  - `burn()` — приём CST и возврат криптовалюты обеспечения;
  - `transfer()` — перевод токенов CST между пользователями;
  - `transferFrom()` — перевод по разрешению;
  - `setOracle()` — установка нового адреса оракула;
  - `setWrapFeeParams()` — установка параметров комиссии;
  - `setValidTimePeriod()` — настройка срока актуальности данных оракула.
- Логика фиксации курса реализована через обращение к контракту оракула, с записью зафиксированной справочной стоимости в события блокчейна.
- Методы `wrap` и `burn` используют внутреннюю защиту от повторного вызова (Reentrancy Guard).

5.2 Оракул oracle.cashiva.com

- Оракул управляется компанией LTD Cashiva Community (Киргизия).
- Источники данных: крупные централизованные и децентрализованные биржи (например, Binance, Coinbase, Uniswap), а также официальные сайты центробанков.
- Данные о курсе считаются устаревшими, если не обновлялись более одного часа.
- При переводе токенов пользователь может вручную инициировать обновление курса.
- Если курс неактуален или оракул недоступен, транзакция автоматически отклоняется.

6. Механизм работы токена

Работа CST основана на простом и прозрачном процессе выпуска и погашения токенов, при котором вся информация об операциях и стоимости фиксируется в блокчейне. Обеспечение криптовалютой, автоматическое получение курса и прозрачность резервов делают процесс безопасным и проверяемым.

6.1 Выпуск (Minting)

- Пользователь отправляет криптовалюту на адрес контракта или хранителя (в зависимости от блокчейна обеспечения).
- Контракт вызывает оракул для получения актуального курса обеспечения относительно выбранной фиатной валюты.
- Контракт выпускает токены CST в эквивалентном криптовалютном объёме (за вычетом комиссии).
- Одновременно в блокчейн записывается справочная цена (в фиате), полученная от оракула, которая может использоваться для бухгалтерии, расчётов и внешнего отображения стоимости.

6.2 Погашение (Burning)

- Пользователь отправляет токены CST обратно в контракт.
- Контракт запрашивает актуальный курс у оракула и фиксирует его в момент транзакции.
- CST сжигается, а пользователь получает обратно криптовалюту обеспечения за вычетом комиссии.
- Записанный курс сохраняется как справочный в событиях блокчейна.

6.3 Фиксация курса

- Курс всегда фиксируется в момент подтверждения транзакции: выпуска, погашения или перевода.
- Если курс не обновлялся более одного часа или оракул недоступен, транзакция отменяется.
- При необходимости пользователь может инициировать немедленное обновление курса.

6.4 Прозрачность

- Вся информация об объёме выпущенных токенов, размере обеспечения, зафиксированных курсах и транзакциях доступна в открытом блокчейне.
- Это позволяет любому участнику проверить 100% обеспеченность и историю операций в любой момент времени.

7. Безопасность и аудит

Безопасность архитектуры CST имеет ключевое значение для доверия пользователей и стабильной работы протокола. Она обеспечивается через совокупность технических, организационных и процедурных мер, направленных на защиту средств, предотвращение ошибок и обеспечение постоянной проверяемости.

7.1 Аудит

- Перед запуском контракты CST проходят обязательную проверку силами компании LTD Cashiva Community (владелец оракула).
- Каждый релиз новой версии контракта или изменение параметров сопровождается обязательным аудитом.
- Планируется регулярное привлечение независимых сторонних аудиторов, известных в криптосообществе, для проведения публичных проверок безопасности.
- Результаты аудитов будут публиковаться открыто, включая хэши проверенных контрактов, список уязвимостей и рекомендации.

7.2 Техническая защита

- **Reentrancy Guard** — запрет на повторный вызов в методах `wrap` и `burn`, предотвращает повторные атаки, аналогичные DAO-инциденту.
- **Проверка актуальности курса** — если курс оракула устарел (более 1 часа), операция автоматически отменяется.
- **Верификация доступности оракула** — при недоступности источника данных транзакция блокируется для исключения ошибок в расчётах.
- **Ограниченные права владельца** — несмотря на возможность изменения параметров, базовые свойства контракта (фиат и криптовалюта обеспечения) заблокированы от изменений после деплоя.

7.3 Прозрачность резервов и операций

- Баланс обеспечения и выпущенных токенов всегда доступен в блокчейне.
- Контракты не используют внешние базы данных, только верифицируемое состояние on-chain.
- Любой пользователь может в режиме реального времени проверить, что количество токенов в обращении не превышает объём криптообеспечения.

8. Экономика и комиссии

Экономическая модель CST основана на простоте, предсказуемости и прозрачности. Она исключает скрытые механизмы дохода, полностью опираясь на комиссии, которые взимаются только при ключевых действиях пользователя — выпуске и погашении токенов.

8.1 Структура комиссий

- Комиссия взимается при **mint** (выпуске) и **burn** (погашении) токенов CST.
- По умолчанию установлена ставка **1% от суммы**, но для каждого контракта она может быть задана индивидуально и отличаться от базовой.
- Комиссия рассчитывается как процент от количества криптовалюты, отправляемой или возвращаемой пользователю.
- Комиссия списывается в базовой криптовалюте обеспечения (например, ETH для RUBETH).

Примеры:

- Пользователь отправляет 1 ETH в контракт `RUBETH` — получает 0.99 RUBETH.
- При погашении 1 RUBETH — получает обратно 0.99 ETH.

8.2 Назначение и использование комиссий

Собранные комиссии направляются на:

- **Поддержку инфраструктуры:** хостинг, обслуживание, разработка смарт-контрактов и оракула.
- **Аудит и безопасность:** покрытие расходов на регулярные технические и внешние аудиты.
- **Развитие и масштабирование:** внедрение новых валютных пар, запуск токенов в других сетях.
- **Маркетинг и интеграции:** подключение к DeFi-протоколам, листинг на биржах, привлечение партнёров.

8.3 Прозрачность сбора комиссий

- Все комиссии поступают на контракт и могут быть выведены только владельцем по публичной транзакции.
- Информация о текущем балансе комиссий всегда доступна в блокчейне.
- Контракт обеспечивает невозможность доступа к обеспечению CST — только к комиссиям.

9. Управление проектом

Эффективное управление проектом CST строится на разделении ролей, жёсткой фиксации параметров и контролируемой возможности обновлений. Контракты устроены таким образом, чтобы исключить злоупотребления со стороны владельца и сохранить максимальную прозрачность.

9.1 Структура управления

- **Эмитент токенов:** WMT Prime Corp (Панама). Компания развёртывает контракты CST, устанавливает параметры и управляет комиссиями.
- **Оператор оракула:** Общество с ограниченной ответственностью "Кашива Комьюнити" (Киргизия). Поддерживает инфраструктуру оракула и отвечает за точность и своевременность данных о курсах.

Такое разделение снижает риски, связанные с централизованным контролем.

9.2 Полномочия владельца контракта

- Владелец контракта может изменять технические параметры:
  - адрес оракула;
  - размер комиссии;
  - допустимый интервал устаревания курса.
- Владелец может выводить только накопленные комиссии. Доступ к резервам обеспечения отсутствует на уровне логики контракта.
- Изменение базовых параметров CST (фиат и криптовалюта обеспечения) невозможно после развёртывания контракта.

9.3 Будущее децентрализации управления

- Через 6 месяцев после запуска планируется внедрение мультиподписного управления (multisig) для ключевых операций.
- Адреса и роли участников multisig будут опубликованы заранее, с возможностью верификации в блокчейне.
- В дальнейшем возможен переход на DAO-модель с голосованием за изменения, если это поддержит сообщество.

Управление проектом построено на сочетании строгой дисциплины доступа, неизменности критичных параметров и прозрачности всех действий владельца в публичной среде.