Цифровое казначейство

Иван Косарев | Директор по продукту Web3 Tech

Дмитрий Багин | Руководитель испытательной лаборатории КриптоПро

О Web3 Tech

Web3 Tech – ведущий разработчик в сфере блокчейн-технологий в России и СНГ, создатель полностью российской блокчейн-платформы «Конфидент» (СКЗИ КС2).

На основе наших технологий реализованы проекты для крупнейших частных и государственных компаний в различных отраслях — Цифровая платформа распределенного реестра ФНС, финтех-сервисы Альфа-Банка, национальная система дистанционного электронного голосования (совместно с ПАО «Ростелеком») и другие решения, требующие распределенной и доверенной инфраструктуры.

- Создаем блокчейн-решения с 2019 г
- >100 высококлассных специалистов
- >30 реализованных проектов
- Разработали крупнейшую блокчейн-сеть в России (ЦПРР ФНС)
- >4,5 млн. пользователей на платформе ДЭГ

Проект «Единое блокчейн-хранилище МЧД на базе ЦПРР ФНС», реализованный компаниями Web3 Tech, КриптоПро и ГНИВЦ, признан победителем конкурса Global CIO Проект года–2023 в номинации «Лучшее отраслевое решение в Госуправлении/НКО».

web3 tech

КРИПТОПРО

Предпосылки создания решения

Федеральный закон от 08.08.2024 N 223-ФЗ

В целях проведения организованных торгов цифровой валютой должны быть предусмотрены порядок допуска (прекращения допуска) цифровых валют в качестве товара к организованным торгам, а также требования к организаторам торговли, осуществляющим проведение организованных торгов цифровой валютой.

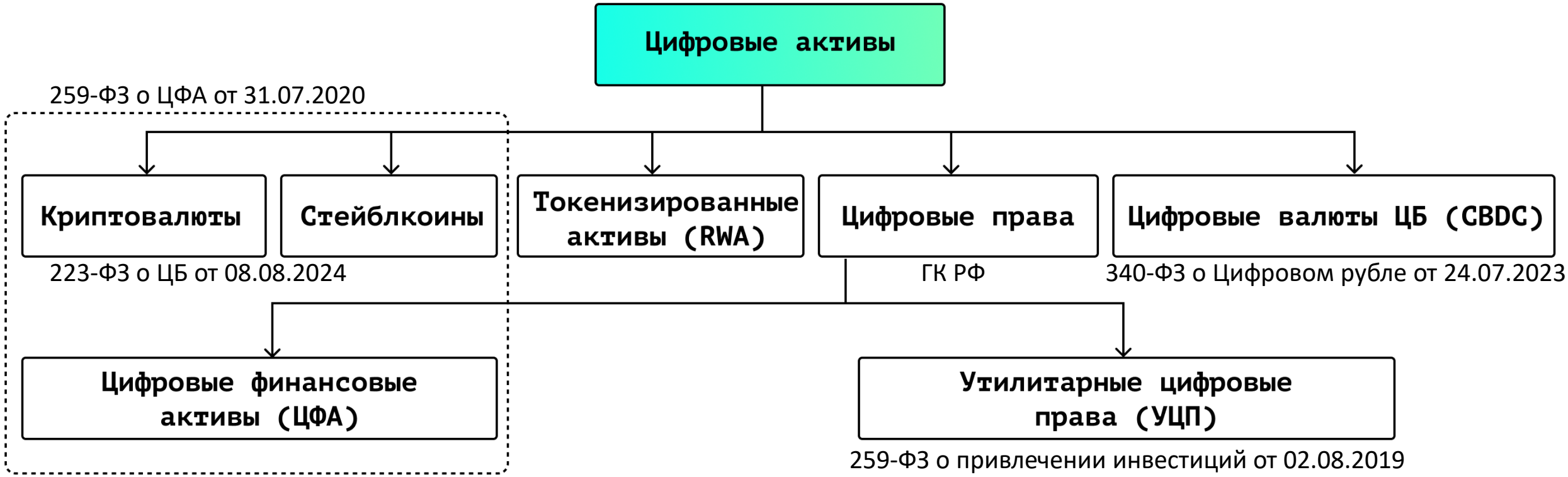
Цифровая валюта позволяет обеспечить ведение экономической и торговой деятельности, защищенное от влияния третьих сторон (включая санкционное давление на контрагентов, блокировку активов и счетов

Для хранения цифровых валют и управления ими необходимо решение, отвечающее российской практике криптографической защиты информации и современным подходам ИБ по защите хранения и операций с цифровыми активами

web3 tech

КРИПТОПРО

Классификация цифровых активов



web3 tech

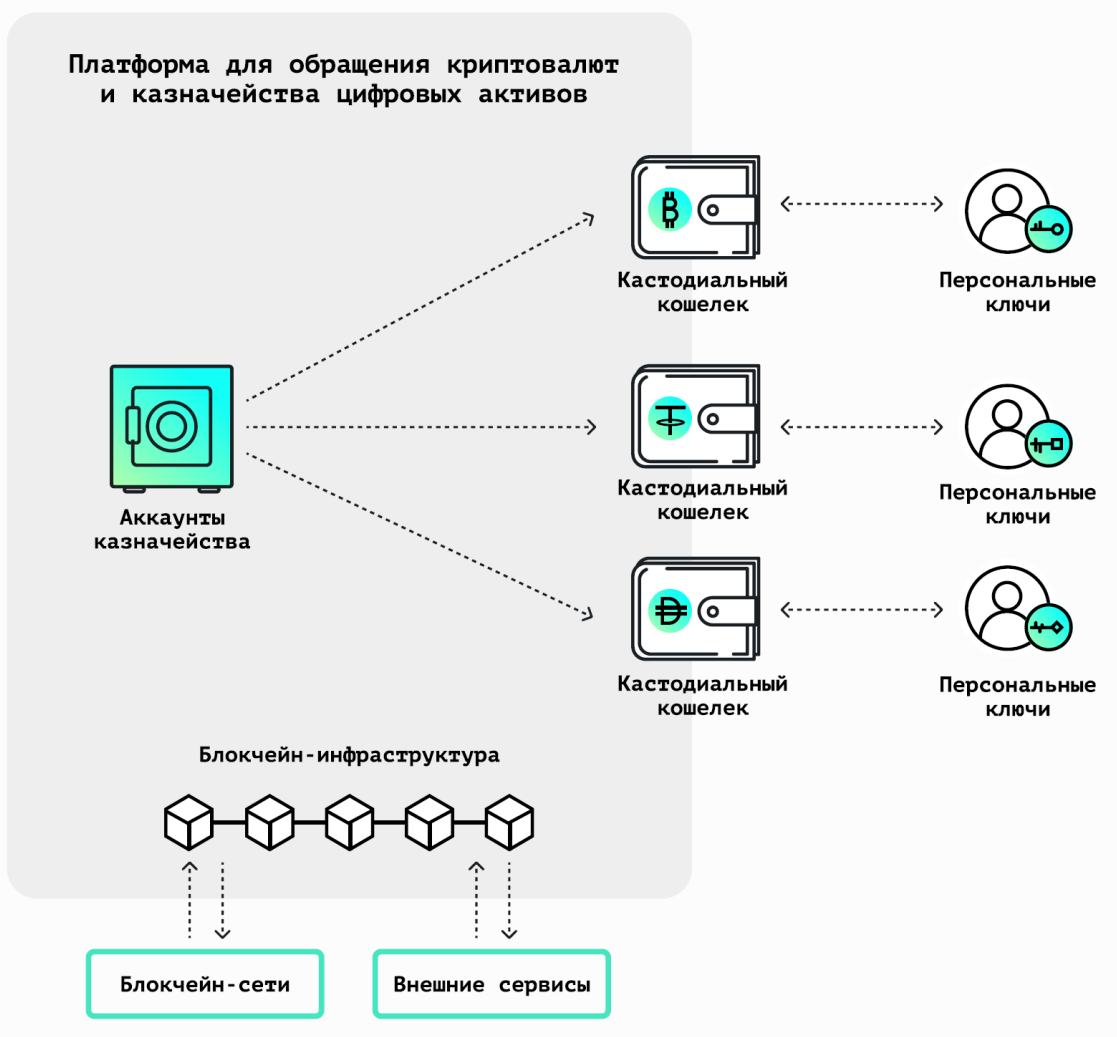
КРИПТОПРО

Цифровое казначейство

Кастодиальное решение по защищенному хранению блокчейн-активов (криптовалюты, ЦФА и т.д.) соответствующее современным практикам

Аппаратный модуль безопасности с ГОСТ-шифрованием от ведущего российского разработчика СКЗИ — КриптоПро

Проверка KYT/AML/CTF/санкционных рисков реквизитов контрагентов и «чистоты» цифровых активов



web3 tech

КРИПТОПРО

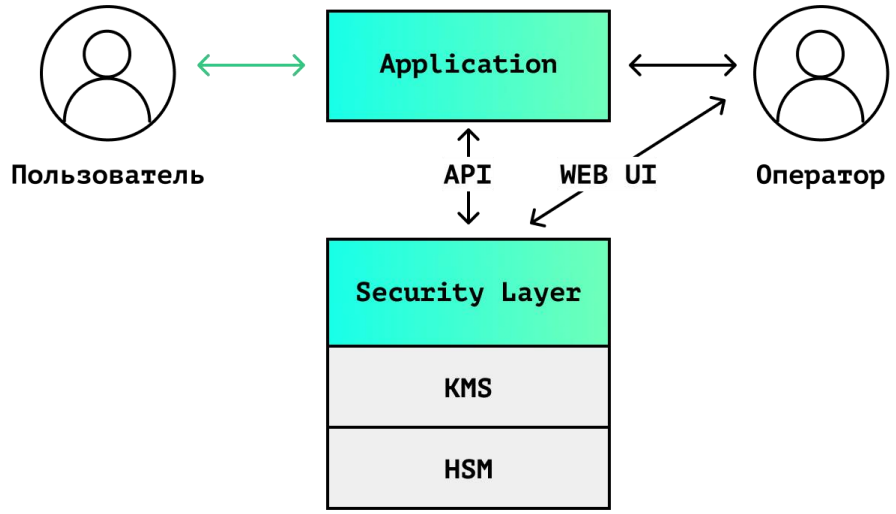
Цифровое казначейство | Принцип работы

- **Цифровое казначейство** позволяет разделить уровень приложения и уровень обеспечения безопасности цифровых активов

- Пользователь приложения формирует распоряжения на совершение операций с цифровым активом
  - Ввод/Вывод/Внутренний перевод

- Слой безопасности проводит проверку соответствия операции правилам:
  - ПОД/ФТ
  - Лимиты
  - «Чистота активов»

- Система управления ключами (KMS) и аппаратный модуль безопасности (HSM) обеспечивают исполнение транзакции



web3 tech

КРИПТОПРО

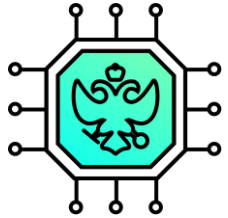
Цифровое казначейство | Интеграция

- On-premise внедрение или доступ по модели SaaS
- Удобное API для бесшовного встраивания кастодиального решения в собственную информационную систему
- Поддержка российских форматов цифровых активов - ЦФА, ГЦП, УЦП
- Поддержка международных блокчейн-протоколов и публичных блокчейн-сетей (Bitcoin, Ethereum и т.д.)
- Интеграция с российским провайдером KYT (с возможностью смены провайдера)

web3 tech КРИПТОПРО

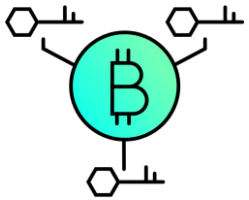
Цифровое казначейство | Безопасность

Автоматическая проверка «чистоты» крипто-активов и оценка риска контрагентов



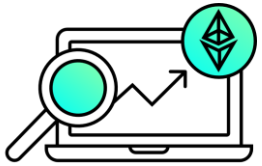
Программно-аппаратная защита активов, опирающаяся на ГОСТ-алгоритмы

Защита активов от внутреннего и внешнего нарушителя



Использование механизмов «распределенной» и «пороговой» подписи для аутентификации и подтверждения операций подписи

Ролевое распределение прав доступа в хранилище

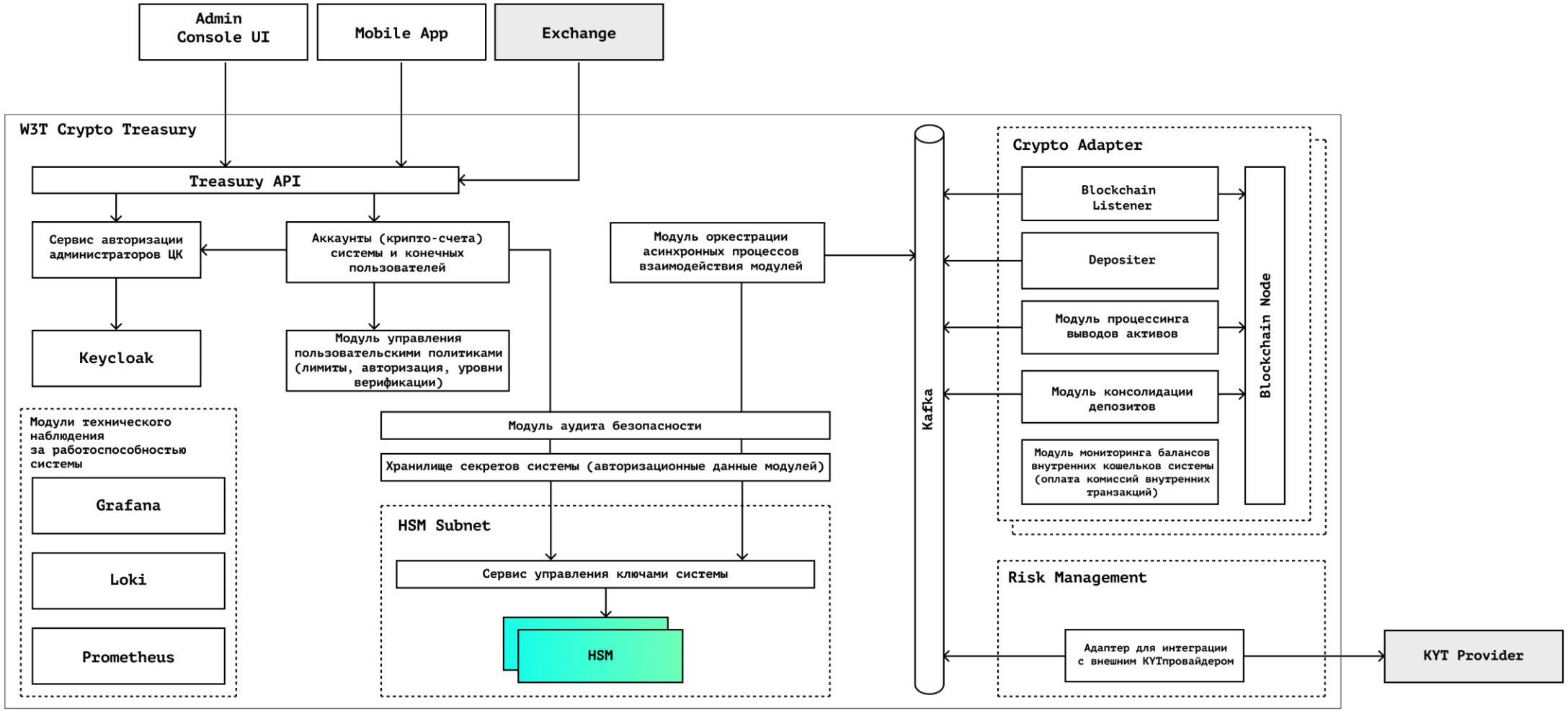


Мониторинг доступа в реальном времени

web3 tech

КРИПТОПРО

Цифровое казначейство | Архитектура



web3 tech

КРИПТОПРО

W3T Treasury. Требования законодательства

Банк России

Центральный банк Российской Федерации

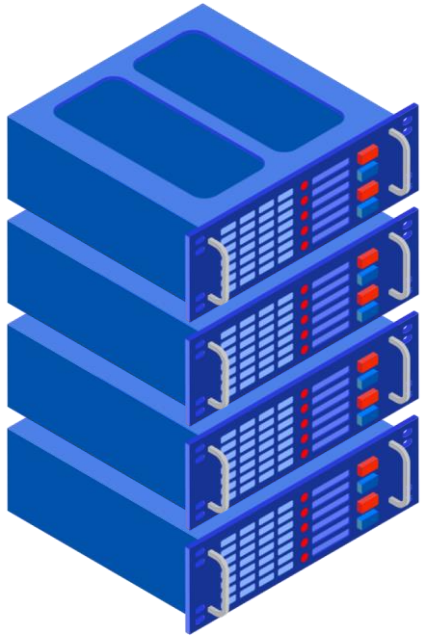
ФСБ России

- Использование сертифицированных СКЗИ
- Аутентификация пользователя
- Защита каналов между компонентами

web3 tech

КРИПТОПРО

W3T Treasury. Ключевая система



КриптоПро HSM

- Подписание по ECDSA и EdDSA внутри HSM
- Неэкспортируемые ключи подписи
- Количество хранимых ключей – сотни тысяч

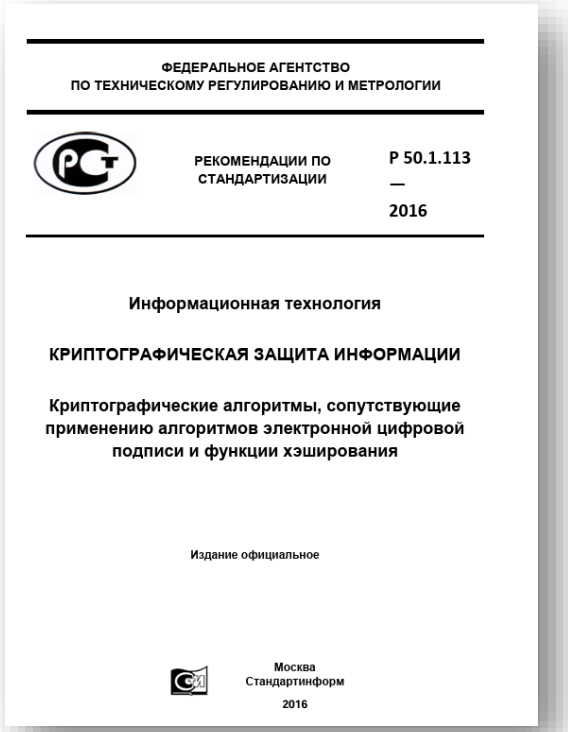
- Возможность работы в режиме кластера

- Возможность построения дерева ключей
- Аутентификация пользователя (подтверждение операции) – в соответствии с ГОСТ Р 34.10–2012

web3 tech

КРИПТОПРО

W3T Treasury. Ключевая информация
Дерево ключей



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 50.1.113
—
2016

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования

Издание официальное

Москва
Стандартинформ
2016

- Схема выработки дерева ключей на основе KDF_GOSTR3411_2012_256

  (в соответствии с Р 50.1.113–2016)

- Долговременное хранение только мастер ключей (секрет системы, generic secret)

- Вычисление ключей подписи (листовых ключей) – в момент подписания транзакции

web3 tech

КРИПТОПРО

W3T Treasury. Ключевая информация
Дерево ключей

- Генерация секрета системы S
- Вычисление предварительного секрета кошелька

  DTTREE(S, i) = Divers3(Divers2(Divers1(S, i&C1), i&C2), i), где

  Divers1(K, D) = KDF256(K, “DT T REE_level1“, D)

  Divers2(K, D) = KDF256(K, “DT T REE_level2“, D)

  Divers3(K, D) = KDF256(K, “DT T REE_level3“, D).

  C1=0xfffffffffc000000

  C2=0xfffffffffffe000
- Вычисление ключей подписи

- Для схемы ECDSA с кривой secp256k1

$$
\begin{aligned}
&\mathsf{sk}_i = K_i \bmod q,\\
&\textbf{while } \mathsf{sk}_i == 0:\\
&\quad K_i = \mathsf{KDF}_{256}(K_i, \text{“}DTTREE\_zerokey\text{”}, i \| count),\\
&\quad count = count + 1,\\
&\quad \mathsf{sk}_i = K_i \bmod q,
\end{aligned}
$$

q — порядок подгруппы группы точек эллиптической кривой secp256k1
count — значение счётчика длины 1 байт

- Для схемы EdDSA с кривой Ed25519

$$\mathsf{sk}_i = K_i$$

W3T Treasury. Подтверждение операции подписи

Схема VerifySignForSign

- Для аутентификации используется УНЭП
- Привязка ключа подписи к ключу аутентификации

web3 tech

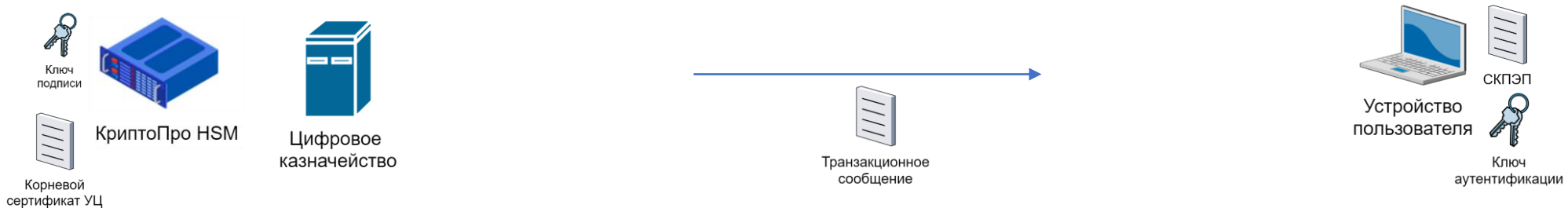
КРИПТОПРО

W3T Treasury. Подтверждение операции подписи

Схема VerifySignForSign. Взаимодействие

W3T Treasury. Подтверждение операции подписи

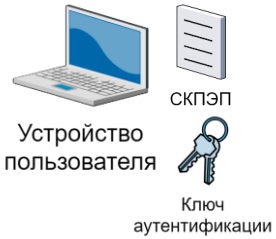
Схема VerifySignForSign. Взаимодействие



W3T Treasury. Подтверждение операции подписи

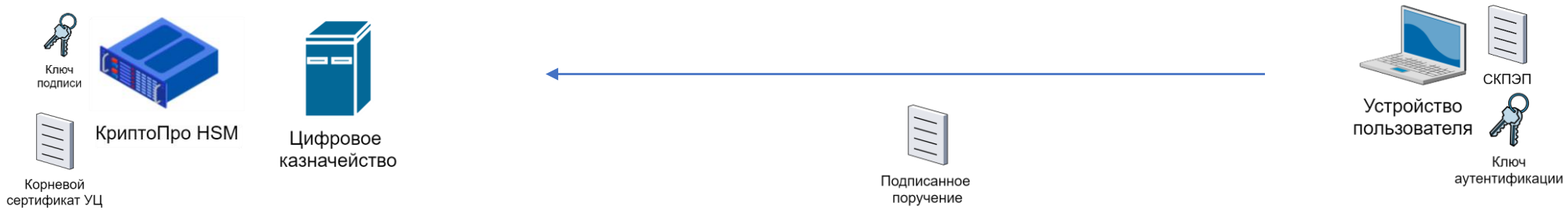
Схема VerifySignForSign. Взаимодействие

- Визуализация
- Формирование подписанного поручения



W3T Treasury. Подтверждение операции подписи

Схема VerifySignForSign. Взаимодействие



Поручение содержит:

- Хэш исходного сообщения
- служебная информация
- сертификат ключа аутентификации

W3T Treasury. Подтверждение операции подписи

Схема VerifySignForSign. Взаимодействие

- Проверка корректности поручения (ЭП)
- Проверка цепочки сертификатов
- Проверка наличия прав

Подписание транзакции возможно только в случае положительного результата всех проверок

web3 tech

КРИПТОПРО

W3T Treasury. Подтверждение операции подписи несколькими участниками

Схема VerifyNSignForSign

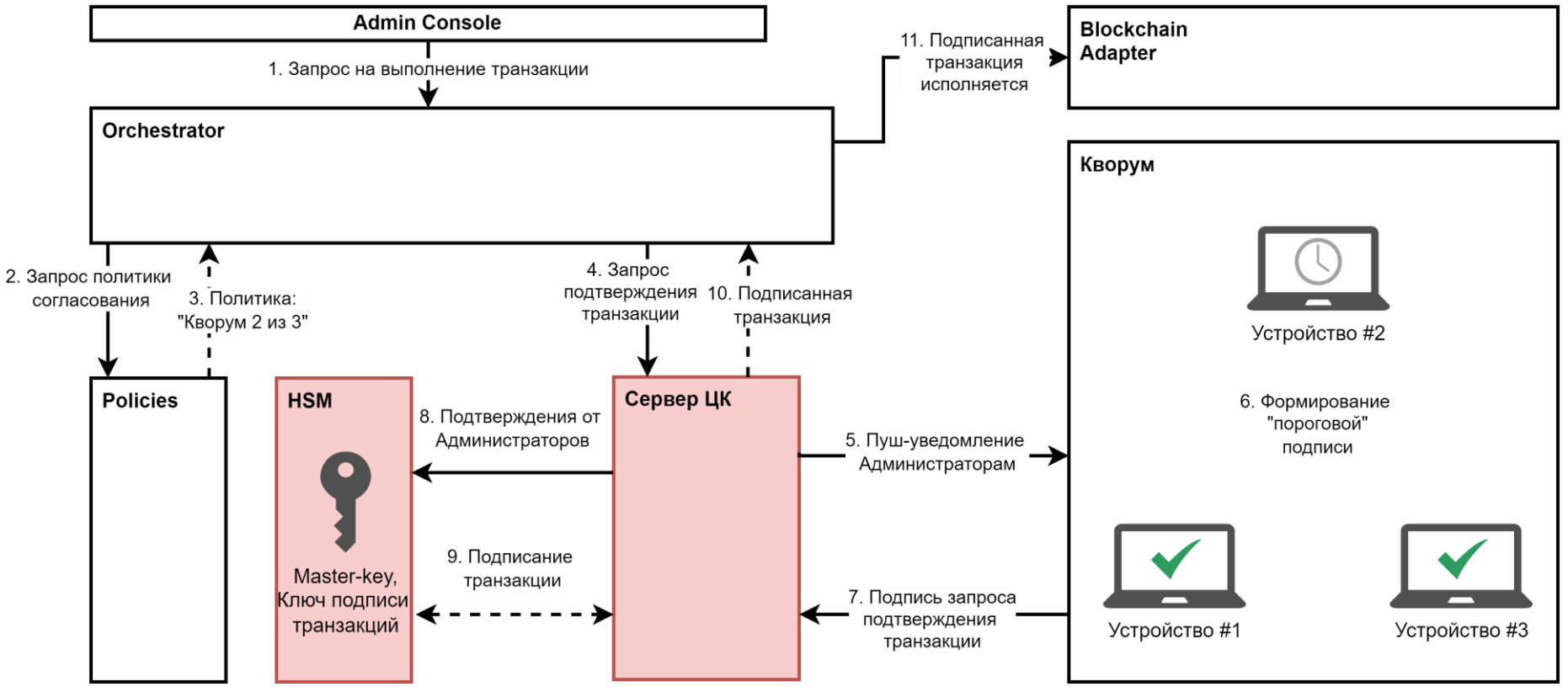
- Для аутентификации используется УНЭП
- Привязка ключа подписи к ключу аутентификации
- Дополнительное расширение в сертификате, определяющее необходимое количество подтверждений

web3 tech

КРИПТОПРО

W3T Treasury. Схема подписания транзакции

Вариант с несколькими подтверждениями

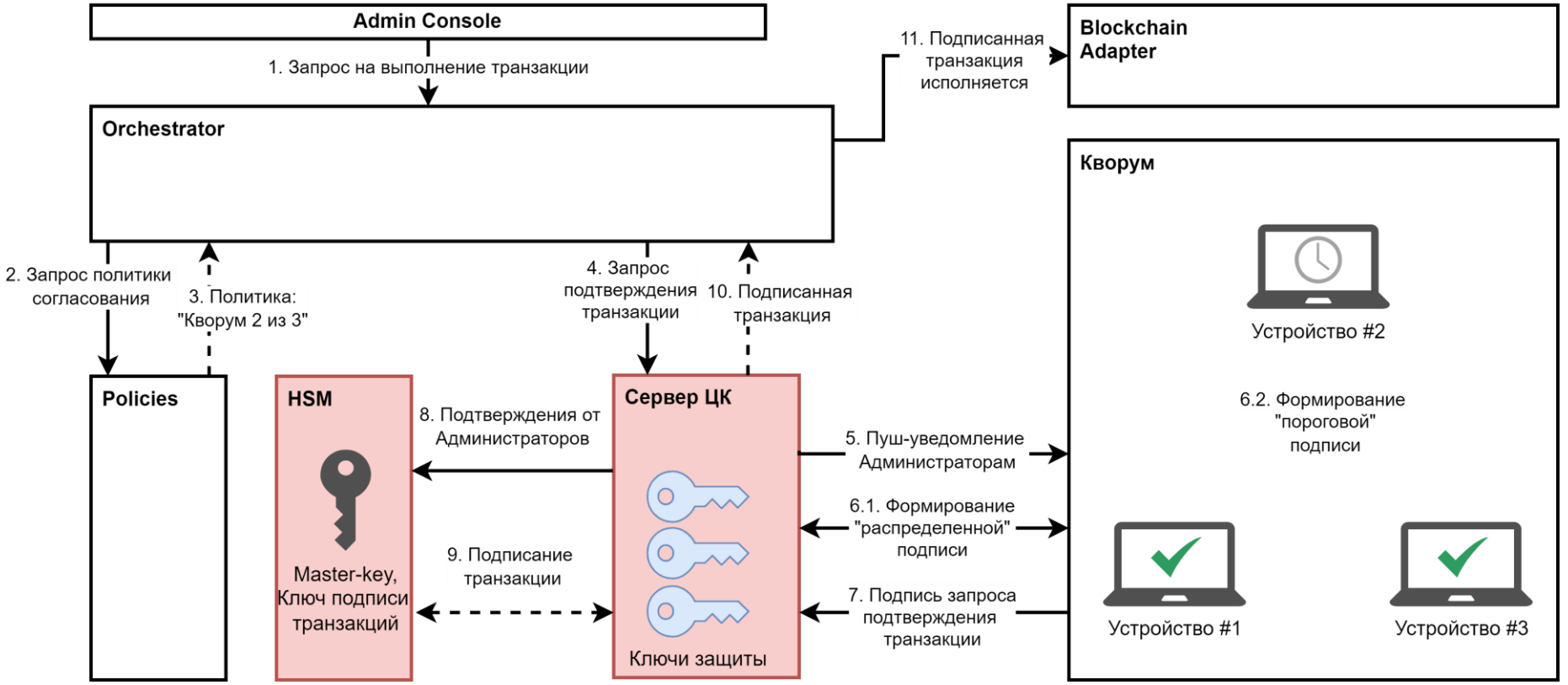


web3 tech

КРИПТОПРО

W3T Treasury. Схема подписания транзакции

Вариант с несколькими подтверждениями и «распределенной» подписью



web3 tech

КРИПТОПРО

Спасибо
за внимание!

https://cryptopro.ru/
https://web3tech.ru/