

cracc

Self custody сервисы для Free TON

[* English version of this presentation \(.pdf\)](#)

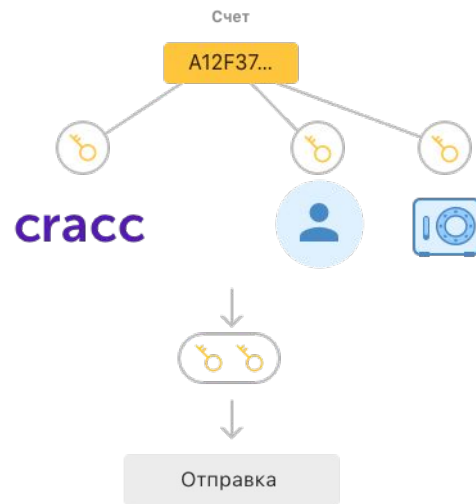
[** Demo of the product \(.pdf\)](#)

Потребность: Хранить и управлять криптоактивами с высоким уровнем безопасности для компаний

- ❑ Для компаний при работе с криптоактивами, нужны решения по депозитарному (кастодиальному) обслуживанию с высокими требованиями к уровню безопасности
- ❑ Решения должны предоставлять готовые процессы необходимые для организации — настройки прав и ролей, схемы восстановления доступов, дополнительные проверки, интеграция со сторонними сервисами и пр.
- ❑ Компаниям сложно самостоятельно разрабатывать решения по работе с криптоактивами. Необходимо иметь компетенции в безопасности и технологии блокчейн

Решение: PaaS/SaaS платформа для управления цифровыми активами на основе Multisig решения

- ❑ Компания получает готовое решение с набором схем для хранения приватных ключей на разных устройствах (HSM, HW), схемы проверок, настройками прав и ролей.
- ❑ Реализован функционал выгрузки отчетов и интеграция с внешними поставщиками по API
- ❑ Для запуска решения достаточно выбрать размещение приватных ключей и необходимую схему работы



Идеальный клиент: Компания заинтересованная в работе с цифровыми активами

- ❑ Есть готовый или планируемый значимый объем цифровых активов под хранение и управление
- ❑ Есть задачи по автоматизации приема и отправки цифровых активов, а также организации управления активами внутри организации

Компании принимающие криптоактивы, осуществляющие выплаты клиентам/сотрудникам, крипто-фонды и пр.

Метрики

- ❑ От 1 года — запуск собственного решения (найм сотрудников, развитие нужных компетенций, согласование)
- ❑ \$400 млн — объём рынка Custody решений
- ❑ В разы дешевле и быстрее — запустить решение с готовыми процессами от Cracc
- ❑ SaaS модель монетизации — в зависимости от объемов используемых модулей оплачивается ежемесячно доступ к сервису

Развитие проекта

2018

- MVP продукта
- Self-custody решения (ledger, trezor, JSON, metamask) — Multisig onchain BTC

2019

- Резидент Сколково
- Поддержка HSM Gemalto, Multisig onchain ERC20
- Финалист конкурса стартапов Уральского форума
- Стратегический партнер ITI Funds / DaVinciCapital, пилот Self-custody платформы фонда фондов

2020

- Сотрудничество с KeepCrypt (Швейцария)
- White label Custody (на базе HSM Gemalto)



Перспектива для экосистемы Free TON

За счет использования безопасного onchain MultiSig решения Free TON возможно создание набора сервисов, необходимых для компаний на базе Cracc:

- ❑ **TON Self-custody service.** MultiSig сервис для хранения и управления токенами TON (восстановление, дополнительное подтверждение).
- ❑ **TON business account.** Создание сервиса с многопользовательским режимом работы. С функционалом распределения ключей между пользователями для подтверждений, ролей, доступов к модулям и пр.
- ❑ **TON payment solutions.** Сервисы необходимые для приема и отправки криптоактивов, интеграции с платежными сервисами и пр.
- ❑ **Интеграция с TON Labs Security Card.** Возможность настраивать как один из способ хранения карты безопасности от TON Labs с разным набором сценариев работы

Команда



Александр Курогло
CEO

10+ лет в создании и
управлении стартапов
Fintech, AdTech
МФТИ

Валерий
CTO, blockchain dev

7+ лет в разработке в
компаниях Mail.ru
(OK.RU), TNS
МГТУ им. Баумана

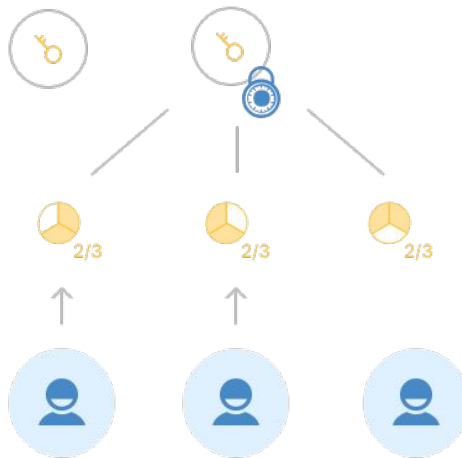
Виталий
backend dev

7+ лет в разработке в
компаниях Mail.ru,
TNS, Marilyn
МГТУ им. Баумана

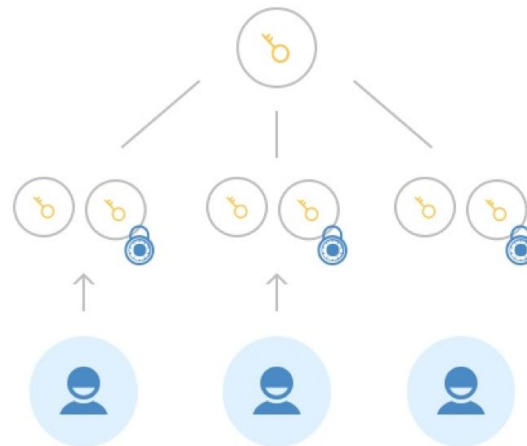
Уникальность технологии Onchain MultiSig



Shamir's Secret Sharing



MultiSig (OnChain)

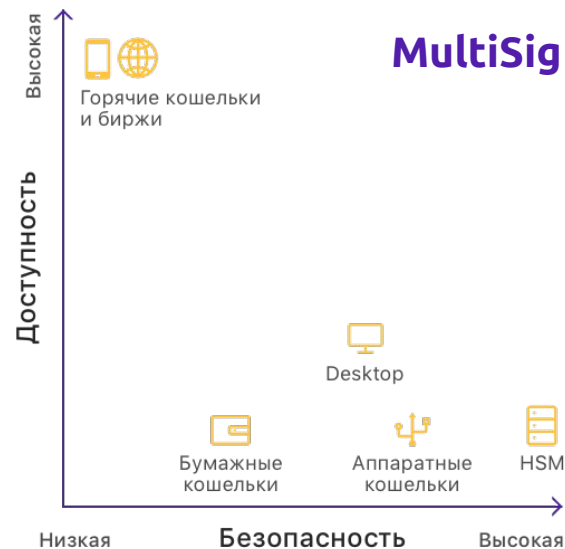


Уникальность технологии хранения

- ❑ **Ключи доверяем «кому-то»**
Горячие кошельки, биржи — мобильно, но с риском потери доступа к криптоактиву
- ❑ **Ключи храним у себя**
На компьютере, мобильном или холодном кошельке — меньше мобильности и риск физической потери актива
- ❑ **Собственное решение**
Разработка и поддержка инфраструктуры с требованиями к безопасности и процессам — долго, дорого и остается риск хищений

MultiSig

Решение, сочетающее преимущества горячих и холодных кошельков с высоким уровнем безопасности, гибкостью построения процессов и возможность работать как через готовый UI, так и по API

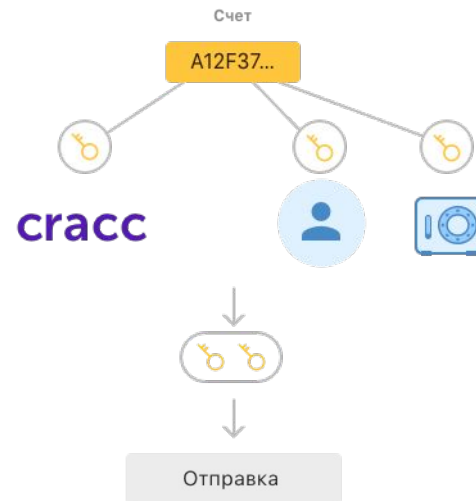


Безопасное хранение

- ❑ Все счета созданы с технологией мультиподписи (MultiSig), с 3-мя ключами
- ❑ Для перевода актива необходимо наличие 2-х ключей
- ❑ Два ключа хранятся у пользователя (один рабочий, другой бэкапный)*, третий ключ хранится в сервисе Сгасс

Преимущества:

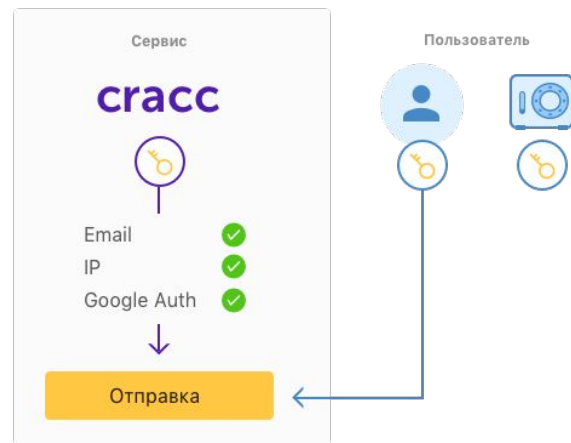
- ❑ Полный контроль над криптоактивами остается у пользователя
- ❑ Возможность восстановление доступа к криптоактивам



*Ключи можно хранить в «холодных кошельках» различных поставщиков, например «Gemalto / Ledger»

Отправка и прием

- ❑ Пользователь инициирует отправку криптоактива и подтверждает ее своим ключом (рабочим)
- ❑ Сервис проверяет, что
 - ❑ пользователь зашел с авторизованного IP
 - ❑ пользователь ввел корректно Google Authenticator
 - ❑ получатель входит в белые списки
 - ❑ отправку подтвердил другой пользователь и т.д.
- ❑ Если проверка прошла успешно, то сервис ставит свою подпись и транзакция совершается



Преимущества:

- ❑ Идентификация пользователей
- ❑ Настройка последовательности подтверждений, в соответствии с политикой и требованиями
- ❑ Уведомления, трекинг действий
- ❑ История транзакций, отчеты, контрагенты

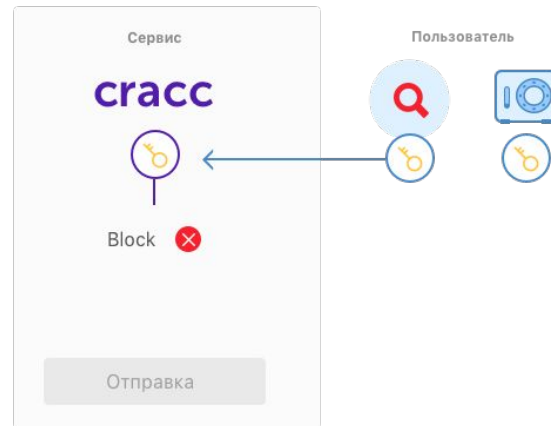
Мониторинг киберриска

В решении заложено автоматическое отслеживание киберугроз и автономность работы

- ❑ Идентификация и мониторинг действий пользователей
- ❑ Создание сценариев автоматического реагирования на инциденты и угрозы.
- ❑ Возможно использовать бэкапные ключи для экстренной отправки криптоактивов, без обращения в сервис.
- ❑ Гибкая настройка прав и ролей, с необходимым уровнем доступа и параметров аутентификации

Преимущества

- ❑ При подозрении на киберугрозу сервис не подписывает отправку
- ❑ Непрерывность работы в случае киберугроз



Потерян пароль MultiSig

Если потерян пароль для ключа регулярного использования

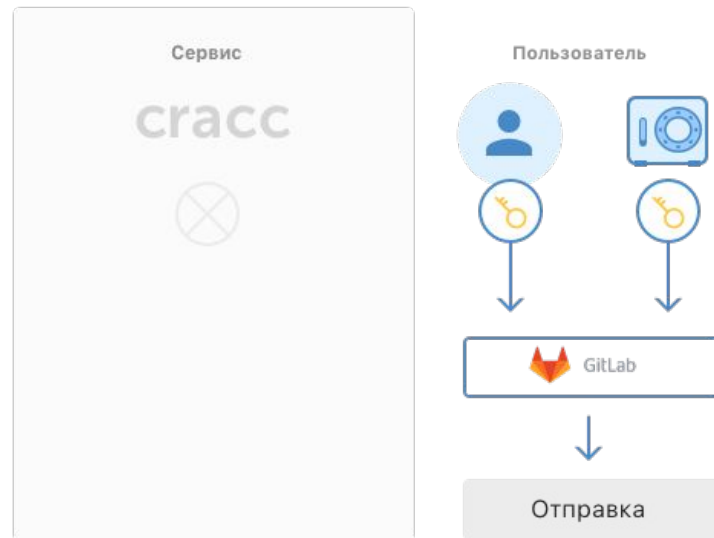
- ❑ Пользователь заходит в систему восстановления ключа (Cracc Key Recovery) и указывает ключ восстановления (второй ключ пользователя)
- ❑ Cracc используя свой ключ и ключ пользователя восстанавливает доступ к ключу регулярного использования
- ❑ Пользователю необходимо только указать новый пароль от ключа регулярного использования



Нет доступа к cracc MultiSig

Если нет доступа к платформе cracc

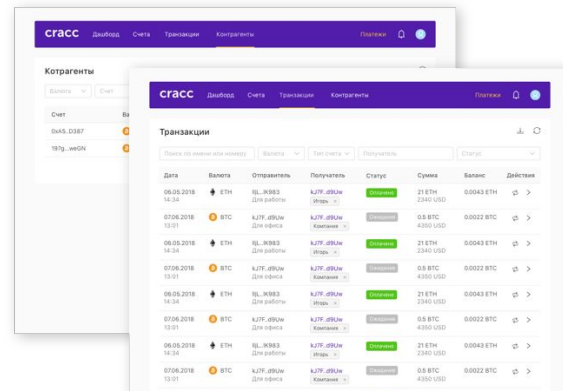
- ❑ Пользователь скачивает хранящуюся в открытом доступе библиотеку Cracc Account Recovery
- ❑ Используя два ключа (восстановления и регулярного использования) и скаченную библиотеку можно отправить криптоактивы на новый счет



Cracc – Корпоративный криптосчет

White-label решение с гибкими настройками

- ❑ Многопользовательские сценарии
- ❑ Безопасное хранение, восстановление, прием и отправка криптоактивов (P2SH / HD - BIP32)
- ❑ Встроенный мониторинг безопасности
- ❑ Интеграция сторонних продуктов — криптобиржи, биржи, custody, поставщики данных и пр.
- ❑ Поддержка BTC, ETH, ERC-20 (добавление под запрос)



Cracc – API

Готовая инфраструктура для работы с криптоактивами

- ❑ Безопасное хранение, восстановление, прием и отправка криптоактивов (P2SH / HD - BIP32)
- ❑ Собственные ноды блокчейна и интеграция с внешними провайдерами, за счет чего обеспечивается скорость и стабильность
- ❑ Кастомизированное решение по «холодному хранению»
- ❑ Интеграция для соответствия политикам и требованиям



Контакты

Александр Курогло — CEO

a.kuroglo@cracc.io
t.me/akuroglo



da **vinci** capital



cracc.io