

Распределённые реестры: мошеннические действия и технические ошибки

Артемий Гусак
Людмила Латонова
Натела Кордзахия
Михаил Огородников
Максим Пешков

Токенизация активов с помощью технологии распределенных реестров – перспективное направление для Московской Биржи

Привлечение новых клиентов

- Более простое размещение активов на цифровых биржах
- Привлечение менее крупных эмитентов и инвесторов

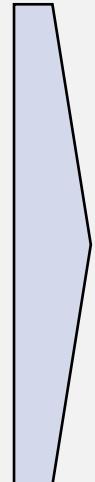
Необходимость новых платформ для крупных компаний

- Разработка собственных платформ для токенизации сырьевыми компаниями
- Стимулирование спроса на активы через использование современных технологий

Выход на новый технологический уровень

- Преимущество перед другими мировыми биржами
- Возможность стать одним из мировых центров токенизации на заре внедрения технологии

Однако технология распределённых реестров пока еще имеет слабые места, позволяющие совершать мошеннические действия



• Компрометация данных в реестре

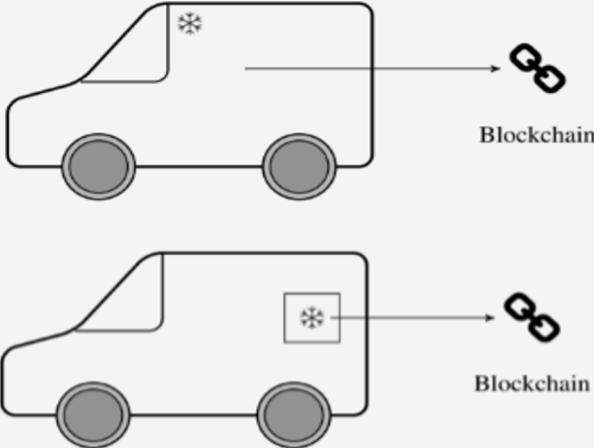
• Отмывание денег

• Проведение кибератак

• Манипулирование

Возможность создать несоответствие между записями в реестре и реальной ситуацией провоцирует мошенничество

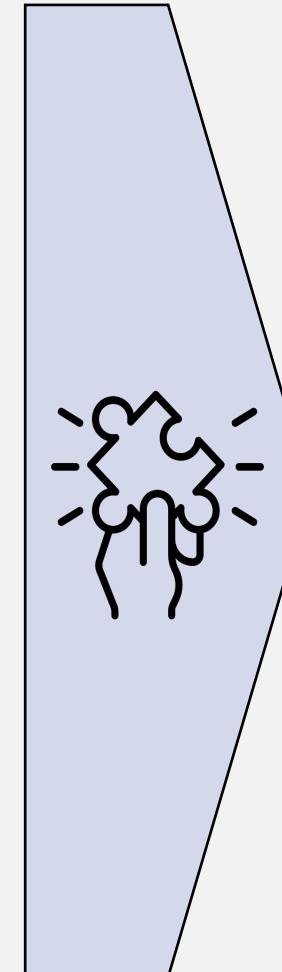
Мошенник может изменить ситуацию в реальном мире и не отразить это в распределенном реестре:



Система, контролирующая температуру внутри грузового отсека автомобиля, не может отследить перемещение датчика в отдельное пространство



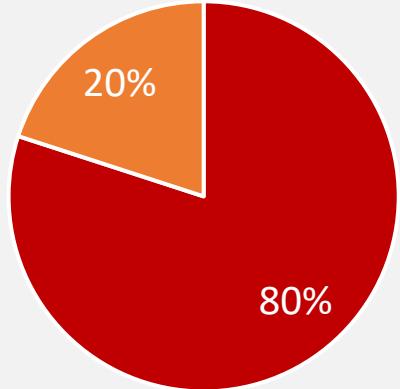
Метка, которую отслеживает распределенный реестр, может быть помещена на другой физический объект



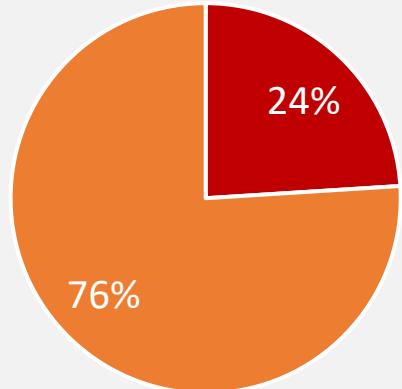
- Физические объекты могут быть связаны в единую сеть, регистрирующую изменения
- Метки могут быть чувствительны к перемещению

- В России пока отсутствует понятие цифрового актива и их формальная привязка к объектам реального мира
- В Сингапуре и Мальте уже найдены сбалансированные решения

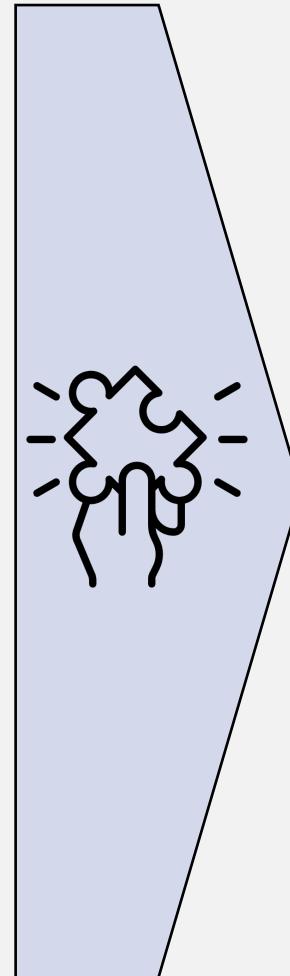
Мошенники под видом перспективных стартапов активно используют токенизацию для сбора денег



20% ICO имеют прямые
признаки мошенничества



76% ICO убыточны для
инвесторов



Развитие законодательной базы

Применение тех же
норм как для
традиционных
ценных бумаг

- США
- Дорого и сложно для честных маленьких стартапов

Разработка
специфических
регулирующих
законов

- Сингапур
- Стимулирует развитие технологии

Проекты, созданные на основе распределённых реестров, часто используются для легализации доходов

Основные способы отмывания

Анонимные
криптовалюты

Сговор с инвесторами в
ICO

Сайты-миксеры

Криpto-казино и онлайн-
игры

Методы противодействия

Рекомендации
FATF

Международная
система
передачи
информации и
совершения
платежей

Алгоритмы
отслеживания
криpto-потоков

- Рекомендации – готовая основа для законопроекта
- Принцип «Know your transaction»
- Ориентация на лидеров: Мальта, Сингапур, Швейцария

- Travel Rule Information Sharing Architecture – аналог SWIFT в отношении криpto-транзакций (Cipher Trace)

- «Анализ кластеризации»
 - Концепция графа
- 
- AML-сервисы (CipherTrace, Chainalysis)

Кибератаки являются серьезной угрозой для систем на основе технологии распределенных реестров

Атаки на пользователей

Кража данных вирусами и троянами
Подмена адресов транзакций

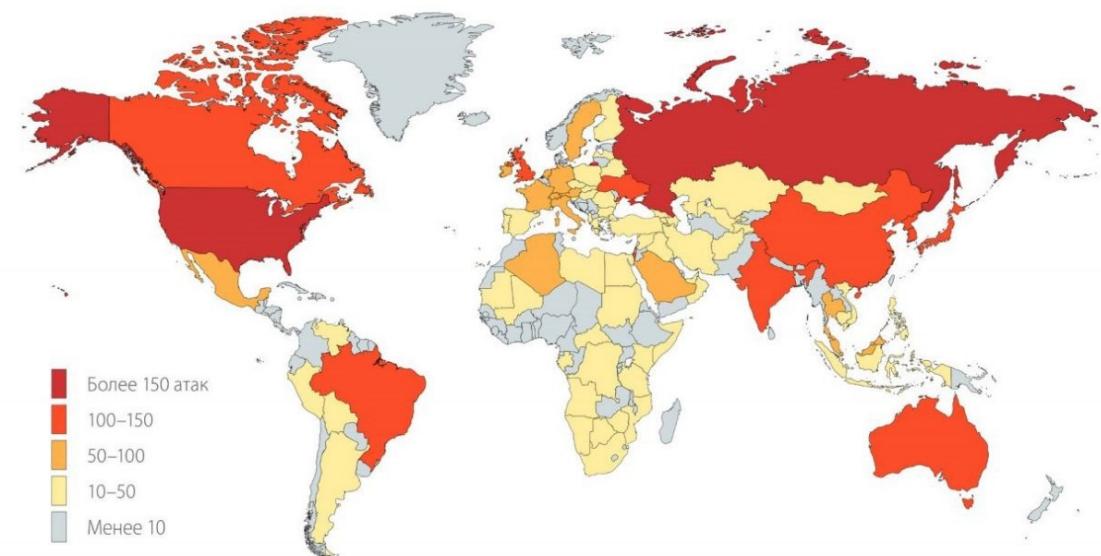
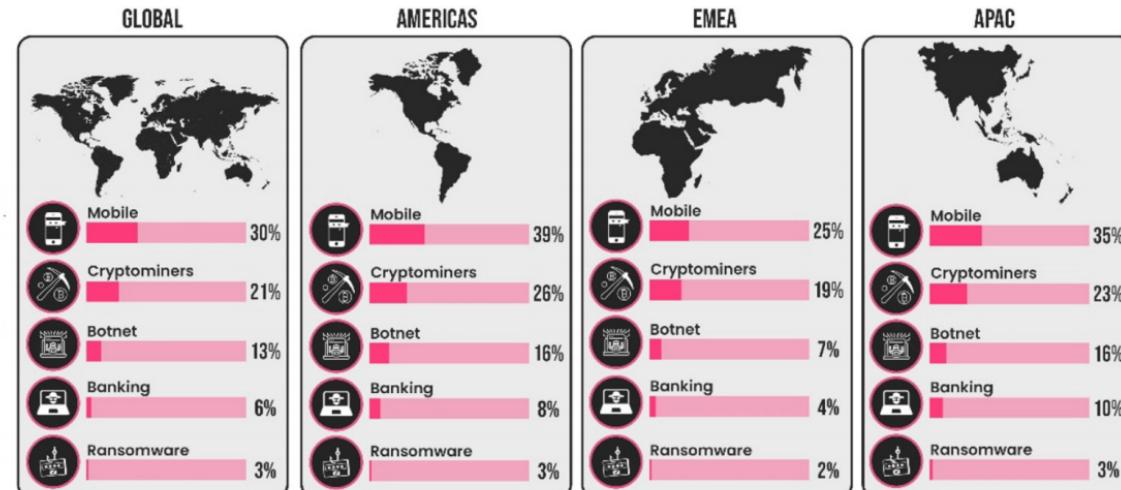
Частое обновление антивирусов и паролей
Разбиение ключей на несколько частей и их шифрование
Использование специальных решений, например, Trezor или SatoshiLabs

Атаки на смарт-контракты

Вызов алгоритма злоумышленника
Изменение в процессе работы

Внимательность при использовании:
необходимо просмотреть код контракта перед использованием

CYBER ATTACK CATEGORIES BY REGION



Кибератаки являются серьезной угрозой для систем на основе технологии распределенных реестров

Атаки на сетевое взаимодействие

Атака «Сибиллы», атака «затмения»

Увеличение объема сети:
Создание финансового интереса по развертыванию сети
Привлечение большого числа узлов создателем сети

DoS и DDoS атаки

Увеличение лимитов мощностей
Экономическое дестимулирование создания большого числа запросов

Атака Финни

Постоянный мониторинг сети и улучшение бдительности пользователей
Валидация транзакций при помощи различных методов, например, PoW и PoS

Атака на криптографию

Применение новых более совершенных методов шифрования информации

Вероятность успешной атаки	Для 7000 нод	для 8000 нод	для 9000 нод	для 10000 нод	для 15000 нод	для 20000 нод
10 %	44250	50888	58521	67299	77394	89003
20 %	48322	55570	63906	73492	84516	97193
30 %	54807	63028	72482	83354	95857	110236
40 %	64520	74198	85328	98127	112846	129773
50 %	78778	90595	104184	119812	137784	158452
55 %	95173	109449	125866	144746	166458	191427
60 %	109414	125826	144700	166405	191366	220071
65 %	128976	148322	170570	196156	225579	259416
70 %	159349	183251	210739	242350	278703	320508
75 %	193720	222778	256195	294624	338818	389641
80 %	255410	293722	337780	388447	446714	513721
85 %	350277	402819	463242	532728	612637	704533
90 %	542886	624319	717967	825662	949511	1091938
95 %	1129019	1298372	1493128	1717097	1974662	2270861
99 %	5775834	6642209	7638540	8784321	10101969	11617264

Большинство случаев манипулирования связаны с удерживанием цен на определенном уровне, выгодном некоторому кругу лиц

Виды ценового манипулирования

Action-based manipulation

Манипуляторы предпринимают какие-либо действия, что влияет на цену актива.

Information-base manipulation

Манипуляторы распространяют слухи или неверную информацию, чтобы повлиять на цены активов

Pump&Dump

Преднамеренное раздувание цен → вброс инфоповода → продажа активов на пике и резкое падение цены

Trade-based manipulation

- Создание ложного впечатления о рыночной цене, глубине или ликвидности рынка
- Ввод bid или ask/offer с намерением их отзыва до совершения сделки

Причины возникновения манипулирования



Низкая ликвидность и высокая волатильность активов



Нестабильность крипторынка



Отсутствие правового регулирования



Государственное регулирование



Биржевой мониторинг

