



Криптовалюты и вопросы AML/KYC

Тихонов Иван

Bits.media

Совместно с

Law&Trust international

LawsTrust.com

Способы децентрализованного создания кошельков

- Кошельки создаются локально на компьютерах пользователей. Без уведомления кого-либо.
- Проверки на дублирование не производится.
- Нет ограничений на количество кошельков или адресов.
- Рассчитаем 50% вероятность сгенерировать нужный адрес при скорости генерации $2 \cdot 10^7$ ключей/сек:

$$T = \frac{\log_{\left(1 - \frac{1}{2^{160}}\right)} 0,5}{6,3 \cdot 10^{14}} = 1,6 \cdot 10^{33} \text{ лет.}$$



Проблемы идентификации по адресу кошелька

Очевидные:

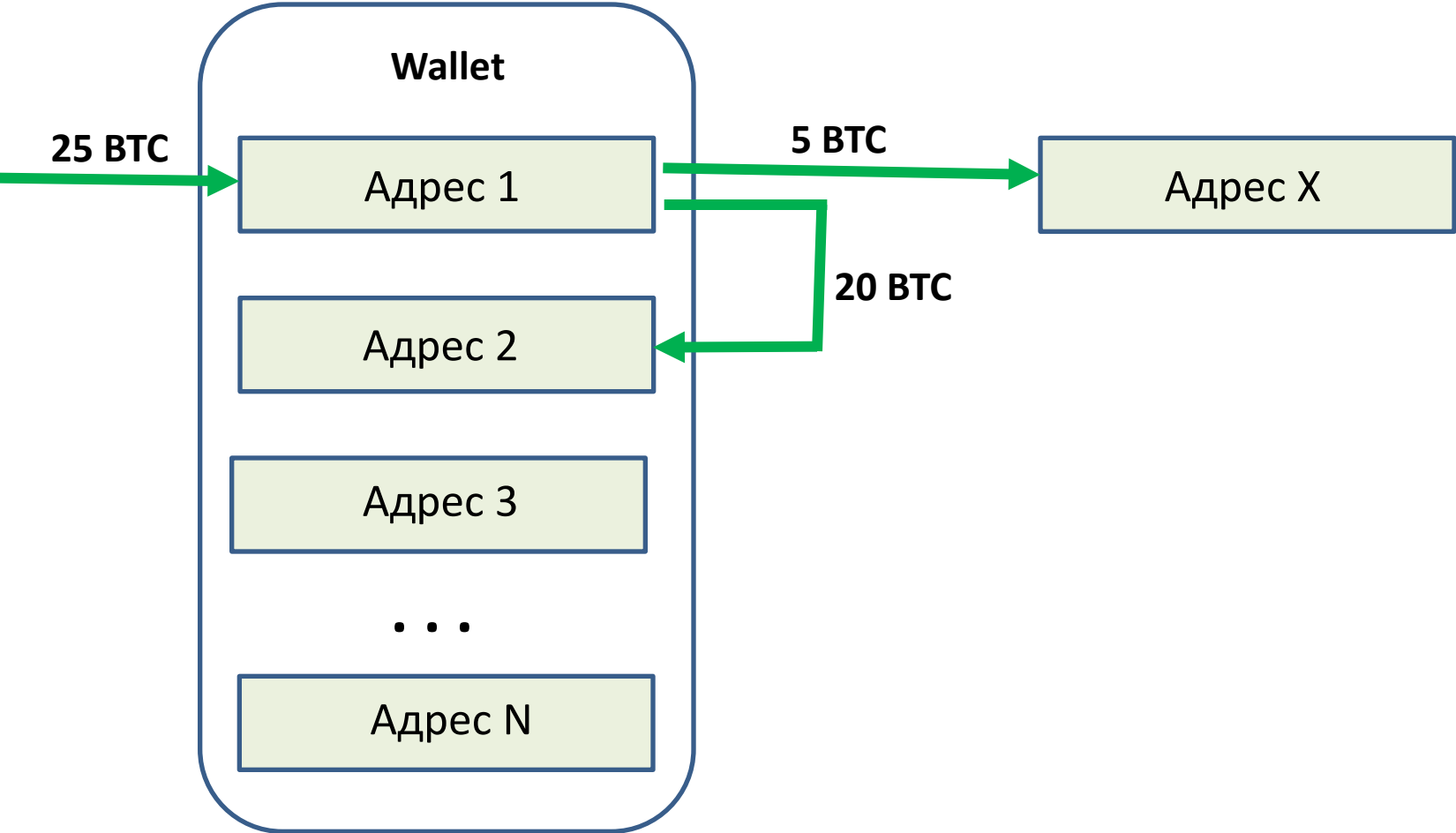
Нет обязательной привязки адреса к реальной личности или организации.

Не очевидные:

Технические особенности реализации программного обеспечения.



Bitcoin транзакции



Понятие аккаунта в криптовалютах

- Аккаунтов в классическом понимании НЕТ
- Аккаунты вводятся в централизованных сервисах (биржи, обменники, иные услуги)
- Требования AML/KYC выполняются на централизованных сервисах



Различия в разных юрисдикциях

- **Бангладеш, Боливия, Эквадор:**

Операции запрещены.

- **Остров Мэн:**

Разрешено. Принят «Proceeds of crime act»

- **Великобритания:**

Казначейство намеревается применить AML к сервисам после проведения двусторонних консультаций

- **США, Нью-Йорк:**

BitLicense от Департамента Финансовых услуг штата Нью-Йорк (NYDFS)

- **США, Калифорния:**

Законопроект регулирования криптовалют от Собрания штата Калифорнии (California's State Assembly)

Какие операции и в какой момент нужно отслеживать?

Стоит руководствоваться местным законодательством:

- Криптовалюты приравниваются к деньгам: идентично контролю над финансовыми институтами.
- Нематериальный актив, имущество и тому подобное: понять источник рисков, применять общие правила OECD и FATF в части AML политики.



В какой момент нужно начинать идентификацию пользователя?

- При регистрации пользователя
- Перед началом финансовых операций
- При конвертации в фиатные деньги
- При выводе средств
- При запросе клиента на увеличение лимитов



AML и фрод - проблема определения "грязных монет"

- Из-за ограниченности все монеты рано или поздно станут «грязными»
- Из-за наличия миксеров и сервисов без AML, отследить весть путь «грязных» монет невозможно.
- Наличие криптовалют со встроенными миксерами, кольцевыми подписями и иными технологиями повышения анонимности.





Криптовалюты и вопросы AML/KYC

ТИХОНОВ ИВАН

<http://Bits.media>
admin@bits.media
Skype: btcsec

Law&Trust international
<https://LawsTrust.com>
info@lawstrust.com

+7 (499) 403 11 13
+7 (812) 424 43 08
+1 (206) 279 26 46
+38 (094) 712 03 21
+44 (20) 376 933 94