Мультиподпись

История

Электронная подпись начинает свою историю с 1976 года, когда впервые было предложено такое понятие. В 1977 был разработан алгоритм RSA, который можно использовать для создания цифровых подписей.
Существуют несколько схем построения цифровой подписи: на основе симметричного шифрования и на основе асимметричного шифрования. Эти типы были описаны в «Аналитической записке о методах обмена ключами».

На данный момент широко применяется технология электронной подписи, основанная на ассиметричном шифровании с открытым ключом. Она опирается на следующие **принципы**:

- Зная открытый ключ, нельзя вычислить закрытый ключ за разумный срок. Механизм генерации ключей строго определён и является общеизвестным. При этом каждому открытому ключу соответствует определённый закрытый ключ.
- Имеются надёжные методы шифрования, позволяющие зашифровать сообщение закрытым ключом так, чтобы расшифровать его можно было только открытым ключом. Механизм шифрования является общеизвестным.
- Если электронный документ поддается расшифровке с помощью открытого ключа, то можно быть уверенным, что он был зашифрован с помощью уникального закрытого ключа.

Мультиподпись – схема реализации электронной подписи, которая для своей достоверности требует T ключей из N членов.
Принцип мультиподписи может использоваться для повышения уровня безопасности при платежах криптовалютой.
При мультиподписи утрата секретного ключа не становится катастрофической проблемой. Мультиподпись, для которой требуется более половины членов попечительного совета некоего фонда, автоматически будет выполнять роль голосования при рассмотрении решений о направлениях использования средств. Оплачиваться будут только те проекты, которые получат большинство голосов в форме подписей под транзакцией.

Применимость в блокчейне (Bitcoin)

Multisignature address — это такой Биткоин адрес, к которому привязано сразу несколько пар ECDSA ключей. Каждая пара состоит из личного и открытого ключей. Схемы комбинаций, согласно которым можно использовать эти ключи, могут быть различными. Более того, можно установить условия, при которых нужно будет предоставить несколько подписей, чтобы потратить монеты с адреса.

Multisig address формируется путем хеширования сразу нескольких сконкатенированных открытых ключей.

Существуют различные комбинации ключей при использовании multisignature address. Наиболее используемыми вариантами являются 2-из-2, 2-из-3, а также 3-из-3. Максимально возможный вариант — 15-из-15.

Может случиться так, что один из партнеров недобросовестный. Он решил не подписывать транзакции, хотя его подпись необходима (2-из-2, например). Таким образом, все деньги на общем счету становятся недоступными. Для того, чтобы защититься от такого существуют LockTime транзакции, отстроченные транзакции.

Wallet сервис

2-из-3. Один ключ принадлежит непосредственно сервису, второй генерируется только пользователем (и только ему известен), третий ключ генерируется и хранится тоже пользователем, но отдельно. После этого вычисляются открытые ключи, соответствующие этим личным, и составляется multisig address. Туда поступают монеты и теперь условия траты ограничиваются. Третий ключ нужен в случае невозможности использования сервиса. В обычном кейсе используется 1ый и 2ой ключи.

Удобство такого подхода состоит в том, что пользователю не обязательно иметь защищенный доступ к этому сервису. Он может иметь обычное устройство, которое может быть заражено вирусами или контролироваться мошенниками, а данные могут быть скомпрометированы или заменены. Но злоумышленнику недостаточно владеть только этим устройством, потому что из него можно добыть только одну из двух подписей.

Еще одно преимущество состоит в том, что если сервис отказывает в обслуживании, то пользователь не теряет доступ к своим монетам. Это были только некоторые из возможных схем использования multisig адресов, которых достаточно для знакомства.

Источники

1. Электронная подпись - wikipedia.org
2. Мультиподпись - wikipedia.org
3. Как работает мультиподпись в Биткоине – habr.com