上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

第六次作业

Log Creative

2023 年 11 月 27 日

1. (1) 备份层次确定钱包只要备份主私钥（master secret key）。备份方式可以考虑记忆法、纸笔记录法、多重备份法，但是它们都有或易遗失或易被盗的风险，更好的做法是门限法：储存 n 份，只要有 t 份找到即可恢复。

   (2) 在新设备上首先以安全的方式传输主私钥，生成主公钥。联网后，设置一个足够大的 N 以覆盖之前已经生成的公钥，遍历 $1,\cdots,N$，根据层次确定钱包的生成方法得到公钥 $pk_1,\cdots,pk_N$，扫描区块链得到所有相关的交易，即可恢复钱包。

2. 支持 BIP32。

   - BIP32 中明确说明了一种漏洞：

     给定父公钥 $(K_{\text{par}}, c_{\text{par}})$ 和未加固子私钥 (k_i)，可以找到父私钥 k_{par}。

     这也是审计漏洞的来源：即审计员拿到父公钥 $(K_{\text{par}}, c_{\text{par}})$ 与部门经理串通拿到未加固子私钥 (k_i)，即可得到父私钥 k_{par} 得到父节点下所有的钱。
   - 但是如果所有的账户都采用“加固”的子密钥，就可以避开这种风险。派生出这种加固的子密钥不仅需要使用父公钥还要使用父私钥（主要使用父私钥），

     父私钥生成子私钥 $\text{CKDpriv}((k_{\text{par}}, c_{\text{par}}), i) \to (k_i, c_i)$

     父私钥生成子公钥 $\text{N}(\text{CKDpriv}((k_{\text{par}}, c_{\text{par}}), i)) \to (K_i, c_i)$

     这样，即使父公钥和加固子私钥同时被泄漏也无法推导出父私钥，因为这种情况下破解的困难程度与暴力破解 HMAC-SHA512 相当。
   - 当然，使用加固密钥增加了安全性，也牺牲了便捷性，以前或许可以从父公钥派生出未加固子公钥而不需要知道私钥，

     $\text{CKDpub}((K_{\text{par}}, c_{\text{par}}), i)$ 只能从父公钥派生出未加固子公钥，从父公钥派生出子私钥是不可能的。

     现在将无法从父公钥直接派生出加固子公钥，生成加固子密钥必须使用父私钥。是否使用未加固子密钥取决于权衡，如果追求便捷性使用未加固子密钥而牺牲了安全性使得父私钥可能泄漏，这种后果应该由进行这种操作的人自负。