11 比特币 Q&A

Q: 给对方转账的时候对方不在线怎么办?

A: 没啥影响，只需要知道对方的地址就可以了。

Q: 假设某个全节点收到了某个交易，有没有可能交易的首款地址，这个全节点以前从来没听说过?

A: 有可能的。创建比特币账户的时候只需要本地生成一个公私钥对，不需要通知其他的节点。

Q: 如果账户的私钥丢失了，怎么办?

A: 没有办法，账户上的钱变成了死钱。再也取不出来了，因为没办法转给别人因为没办法签名了。但如果去交易所，因为交易所是中心化机构，会需要身份证明，和银行差不多。私钥是由交易所保管的，还会让你设置一个二次的密码。二次的密码可以重置。但是交易所保管私钥并不比自己安全。比特币的交易所是不受监管的，和股票的交易所是很不一样的。历史上有黑客黑进交易所偷了很多的比特币。Mt Gox 门头沟是历史上的一个很大的交易所，就被黑了。也有的是交易所监守自盗，捐款跑路了。

Q: 如果账户的私钥泄露了怎么办？ 比如说发现了一些可疑的交易

A: 这个时候应该尽快把自己账户上的钱转到其他的安全账户上。和银行不太一样，平常我们希望改变密码（私钥），但是这个在去中心化系统中是无法做到的。

Q: 如果转账的时候，写错了地址怎么办?

A: 没有办法取消已经发布的交易。写错了就认命。如果知道是谁的地址，可以商量一下能否退回。但是不能强迫。

Q: 收到Proof of Burn，实际当中是怎么操作的？当全节点收到一个合法的交易的时候，才会写入到区块链里。但是RETURN无条件返回false，怎么能通过合法交易的检验呢?

A: 验证的过程中，proof of burn是写在当前的交易的输出脚本里的，但是验证当前交易的合法性是验证当前的交易的输入脚本和之前交易的输出脚本，所以proof of burn根本就不会出现在验证的过程中，所以没有问题。

Q: 怎么能知道某个矿工是最先找到这个nonce的？就是一个矿工发布了一个合法的区块，我不能直接拿过来也发布一个一样的?

A: 因为区块中需要填铸币交易中收款人的地址。当你偷块的时候需要把收款人地址要改成自己的，会导致merkle tree的根哈希发生改变，会导致原本的根哈希不适用了。

Q: 交易的时候怎么知道交易费改付给谁?

A: 事先不需要知道哪个矿工会得到这个交易费。total inputs - total outputs就是交易费。所以最后挖到矿的那个矿工，只需要把所有的差额收集起来，作为他自己赚得的交易费就可以了。