2.8 小结

01 概念回顾

矿工

矿池

公钥

私钥

钱包

交易

区块

算力

02 概念回顾

- 矿工：是指参与比特币挖矿的个体，也就是说，每一个致力于生产新区块的比特币节点的主人，就是一个矿工，也就是比特币网络参与的主体。
- 矿池：一些矿工集合起来，集合各自的算力，提高挖到矿的可能性。这种矿工的集合体就是矿池。
- 公钥、私钥：公钥和私钥是一组配合使用的概念，他们之间有着紧密的联系。简单来说，私钥是系统随机生成的，公钥是由私钥计算得出的；公钥负责加密，私钥负责解密；私钥负责签名，公钥负责验证。

03 概念回顾

- 钱包：用来装密钥的容器，它只包含密钥而不包括具体的多少个比特币。
- 交易：利用矿工掌握的私钥，把比特币从一个地址转到另一个地址的行为。
- 区块：区块是构成区块链的基本单元，由区块头和区块主体构成。在区块头中包含了前一个区块的哈希信息，可以帮助新区块和之前的区块联系起来；而区块主体则包含了这一段时间内所有的交易信息。
- 算力：是用来衡量进行哈希运算的能力的指标，它可以用每秒完成哈希碰撞次数来衡量。

04 哈希加密算法

- 哈希加密算法是目前在比特币网络中广泛使用的加密算法。通过哈希加密，能够将一段任意长度的数据信息在较短的时间内转换为定长的哈希值。而且一旦输入的数据发生了哪怕一比特的改变，输出的哈希值也将产生极大的改变。因此，通过哈希算法加密的数据，具有很强的防篡改能力。

05 共识算法

- 共识算法是区块链网络中用来决定如何选出那个可以生成新区块的节点的机制，同时对于每一笔在这条区块链上进行的交易是否准许完成进行了约束和规定。
- POW机制，全称叫做工作量证明机制，是要求矿工通过不断进行哈希碰撞，不断尝试直到一个矿工最先找到正确的nounce值，就获得了生成新区块的资格。

06 UTXO

- UTXO全称是“尚未使用的交易输出”，UTXO技术的使用，是为了解决电子货币交易中存在的双花问题。具体来说，比特币分布式账本由一笔一笔的交易构成，每一笔交易都要花费一笔输入，产生一笔输出，而其所产生的输出，就是UTXO。当一笔交易被广播到区块链网络之后，接收到交易的节点会对交易进行验证，检查其是否被花费过，即是否存在于UTXO中。如果交易输出已不存在于未花费交易列表中，则验证失败。通过这种方法，比特币有效杜绝了大部分的双花问题。