“从数字货币到信用时代”

-BFChain入职区块链主题分享

Module 2

区块链是什么?

- ## 概念打磨：

1.区块

时间戳服务器通过对以区块形式存在的一组数据，某个区块好比账本中的一页。

2.链

每个区块被打上时间戳，并时间先后顺序连接。

3.公链、私链、联盟链

公链 ： 对所有人开放、任何人都可以参与的区块链。

私链：对单独的个人或实体开放的区块链，参与的节点只有自己。存在一定的的中心化控制的区块链。

联盟链：对特定的组织团体开放，参与区块链的节点事先选择好。

4.侧链、子链、软分叉、硬分叉

侧链：

楔入式侧链技术（ pegged sidechains），它将实现比特币和其他数字资产在多个区块链间的转移，这就意味着用户们在使用他们已有资产的情况下，就可以访问新的加密货币系统。

子链：

构建在底层母链基础上的区块链，链上之链，即为子链。

硬分叉：

当比特币协议规则发生改变，如果旧节点拒绝接受新节点创造的区块时，区块链将分成两条独立的链。

软分叉：

当比特币协议规则发生改变，旧节点不会意识到规则是不同的，它们将遵循改变后的规则，并且接受新节点创造的区块。不产生2条区块链，而是在原区块链新旧并存，区块链向前兼容。

5.共识机制、工作量证明、权益证明、股份授权证明机制

共识机制：

由于加密货币多数采用去中心化的区块链设计，节点是各处分散且平行的，所以必须设计一套制度，来维护系统的运作顺序与公平性，统一区块链的版本，并奖励提供资源维护区块链的使用者，以及惩罚恶意的危害者。这样的制度，必须依赖某种方式来证明，是由谁取得了一个区块链的打包权（或称记账权），并且可以获取打包这一个区块的奖励；又或者是谁意图进行危害，就会获得一定的惩罚，这就是共识机制。

工作量证明Pow：

是一种对应服务与资源滥用、或是拒绝服务攻击的经济对策。一般是要求用户进行一些耗时适当的复杂运算，并且答案能被服务方快速验算，以此耗用的时间、设备与能源做为担保成本，以确保服务与资源是被真正的需求所使用。

权益证明 PoS：

根据在网络中拥有权益的多少来获得竞争记账的权利。即：持有权益越多，获得记账权利的概率越大。

股份授权证明机制DPoS：

是由被社区选举的可信帐户（受托人，得票数排行靠前指定位数）来创建区块。

6.挖矿、矿场、矿池

挖矿：

是消耗计算资源来处理交易，确保网络安全以及保持网络中每个人的信息同步的过程。当产生交易时，矿工有偿提供算力，赚取电子货币。

矿场：

把成千上万台矿机连接起来一起挖矿就是矿场。（物理层面）

矿池：

矿机的算力集合起来就是矿池，矿池可以是若干矿机的集合，也可以是若干矿场中的矿机算力的集合。接入这个矿池的既有中国矿机也有国外的矿机，部分区域，大家按劳分配。（比特层面）

7.分布式计算、点对点技术、时间戳

分布式计算：

分布式计算(Distributed computing)是一种把需要进行大量计算的工程数据分割成小块，由多台计算机分别计算，在上传运算结果后，将结果统一合并得出数据结论的科学。

点对点技术：

（peer-to-peer， 简称P2P）又称对等互联网络技术，它依赖网络中参与者的计算能力和带宽，而不是把依赖都聚集在较少的几台服务器上。P2P 技术优势很明显。点对点网络分布特性通过在多节点上复制数据，也增加了防故障的可靠性，并且在纯P2P网络中，节点不需要依靠一个中心索引服务器来发现数据。在后一种情况下，系统也不会出现单点崩溃。

时间戳：

时间戳是一份能够表示一份数据在一个特定时间点已经存在的完整的可验证的数据。 它的提出主要是为用户提供一份电子证据， 以证明用户的某些数据的产生时间。简单来说就是记录该区块产生的时间，精确到秒。

7.全节点

是拥有完整区块链账本的节点，全节点需要占用内存同步所有的区块链数据，能够独立校验区块链上的所有交易并实时更新数据，主要负责区块链的交易的广播和验证。

8.公钥、私钥

公钥（Public Key）与私钥（Private Key）是通过一种算法得到的一个密钥对（即一个公钥和一个私钥），公钥是密钥对中公开的部分，私钥则是非公开的部分。公钥通常用于加密会话密钥、验证数字签名，或加密可以用相应的私钥解密的数据。通过这种算法得到的密钥对能保证在世界范围内是唯一的。使用这个密钥对的时候，如果用其中一个密钥加密一段数据，必须用另一个密钥解密。比如用公钥加密数据就必须用私钥解密，如果用私钥加密也必须用公钥解密，否则解密将不会成功。

9.哈希算法、非对称加密、数字签名

哈希算法：

是将任意长度的二进制值映射为较短的固定长度的二进制值，这个小的二进制值称为哈希值。它的原理其实很简单，就是把一段交易信息转换成一个固定长度的字符串。

特点：1信息相同，字符串也相同，2信息相似不会影响字符串相同，3可以生成无数的信息，但是字符串的种类是一定的，所以是不可逆的。

非对称加密：

其需要两个密钥：公开密钥（publickey）和私有密钥（privatekey）。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。

数字签名：

是一种类似写在纸上的普通的物理签名，但是使用了公钥加密领域的技术实现，用于鉴别数字信息的方法。

10.UTXO

Unspent Transaction output,即未花费的交易输出。

12.区块链的6层模型

区块链技术的模型是由自下而上的数据层、网络层、共识层、激励层、合约层和应用层组成。

13.比特币的最小单位

聪是比特币最小单位，一亿个聪相当于一个比特币。

14.冷钱包、热钱包、轻钱包、全节点钱包、硬件钱包

全节点钱包：

下载网路中所有的节点，从异地区块至今所有的数据，由这个钱包自己维护全网的数据，自己验证竞争挖矿的结果。

轻钱包：

只维护与节点相关的交易数据，不同步其他数据。

冷钱包：

也叫离线钱包，即不联网。

热钱包：

也叫在线钱包，连着网生成私钥或者连着网运行的钱包。

硬件钱包：

硬件钱包是指将数字资产私钥单独储存在一个芯片中，与互联网隔离。

15.区块链浏览器

提供区块、交易、账户等查询功能的搜索工具。