区块链技术综述（笔记） 2019.11.12

<http://www.infocomm-journal.com/cjnis/CN/10.11959/j.issn.2096-109x.2016.00107>

一、概念：

区块链是一种按照时间顺序将数据区块用类似链表的方式组成的数据结构，并以密码学方式保证不可篡改和不可伪造的分布式去中心化账本，能够安全存储简单的、有先后关系的、能在系统内进行验证的数据。

（区块链是比特币和加密货币的技术基础。）

二、特点：

1、去中心化：可以理解为“多中心化”。区块链的所有参与者（账本拥有者）都是一个平等的中心，通过一个独有的物理设备，保持一个独立的账本。通过所有中心的一致表决来实现平等。

（体现的意义：1）系统安全性；2）交易安全性；3）节约性；4）自主高效性）

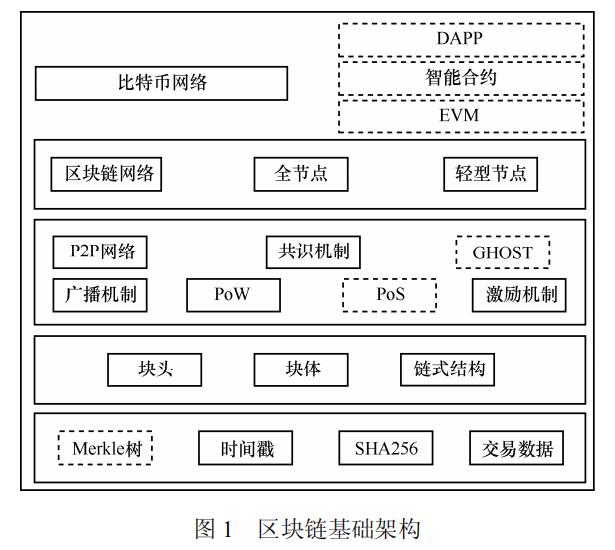
2、开放性：区块链技术基础是开源的，除了交易各方的私有信息被加密外，区块链的数据对所有人开放，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。

3、匿名性：它的匿名性基于它的算法实现了是以地址来寻址的 ，而不是以个人身份，这也是政府比较担心的。

4、可追溯性:他的机制就是设定后面一个区块拥有前面一个区块的一个哈希值就像一个挂钩一样，只有识别了前面的哈希值才能挂得上去，是一整条完整的链。

5、防篡改性：任何人要改变区块链里面的信息，必须要攻击网络里面的51%的节点才能把数据更改掉，这个难度非常非常大。

三、区块链架构：



四、区块链关键技术：（上图框架即为下述内容的框架）

1、底层数据

其中，涉及到算法的有SHA256算法（散列算法）、Markle树（二叉树）

2、分布式记账本

（本文中介绍的是狭义上的区块链，即分布式记账本是时序链式结构，广义上的是完整的带有数学证明的系统框架。）

3、组网方式和核心机制

（基于分布式账本之上的区块链网络，采用的是对等式网络--P2P网络，将所有节点连接在一起，设计PoW或其他共识机制使无信任基础的双方在不需要第三方的情况下建立互信，使用广播的方式传播交易信息，加上激励机制来保证节点提供算力以维持整个网络的顺利进行。）

4、区块链节点

5、智能合约

6、上层应用

五、区块链技术存在的问题

1、效率问题（同步时间问题、交易效率问题）

2、中心化问题（51%攻击问题、中心化趋势）

3、隐私和安全问题（数据隐私问题、使用安全问题）

4、公有链、联盟链和私有链的问题（联盟链问题、私有链问题）