# 区块链论文阅读

## 比特币系统的设计思想

首先比特币为什么会出现，这是有一定背景关系的，在现实生活中，我们存在着信任问题，尤其是当今"不知道网络那端和你聊天的人是人还是一只狗"的网络世界。

比特币的出现就是为了解决信任问题，利用人对机器的信任而非第三方中介的存在，除此之外中介产生的费用也是个问题，找中介要花时间，如果是两个陌生人就更难找到合适的可信任的中介了。但是机器是没有利益需求的（排除可能有些被写入恶意程序的机器），机器它不像人一样有欲望，没有必要去造假，正常情况下是非常值得信任的，正因如此，所以比特币就是"用机器当中介"的一种交易货币。

交易需要被记录，整个交易系统为了确保效率和安全，采用去中心化的体系，一旦某个节点出了问题不会影响到其他人，所有的机器出问题的概率几乎为 0，这种体系既健壮又简单，这使得我们更加信任这种货币机制。

但是记账是一件苦差事，而且选择谁来做这也是一个问题。比特币的每条交易记录了时间，根据这个时间形成一条账单链，公认最长的一条链为正确的那个账单。比特币的账单每十分钟打包一次，然后出难题，成千上万的人参与计算，最先算出来的人拿到记录权，当然不是白干活，他的奖励则是 50 个比特币（如今是 12.5 个），而且还会得到一些手续费。这是相当诱人的，也许会有作恶的人想要趁此机会修改账单，但是实际上很难，十分钟内他需要通过已经经过隐私处理的一堆匿名的账单编号信息篡改一些信息几乎不可能，而且在十分钟以后就更不可能了。而且作恶得到的资金可能还不如这 50 个比特币的价值高。

这整个运作过程是：某个节点一旦发生交易，就向所有节点广播新交易，每个节点收集新交易到一个块里，同时寻找合法性证明，发现一个证明后就将这个块广播出去，当块中所有事务都被证明有效且没有被使用时，节点就接受这个块，同时在属性中创建下一个块作为对这个块的接受链，使用已接受块的哈希值作为前一个哈希值进行计算新的。

然后我以实际的例子来描述一下整个流程：

假设 Alice 在比特币客户端已经注册了账号，并且已经拥有了一些比特币，现在 Alice 登录自己的钱包，输入对方（假设是 Bob）的地址（相当于银行卡号），输入转账金额 0.1BTC，选择交易手续费（手续费可以为 0，但是这条交易被写入区块链的优先级会被降低，转账就会被延迟，甚至有可能由于其他原因交易失败），创建交易，点击发送，那么这条交易就会被 P2P 广播到比特币网络中去，当某个矿工收到这笔交易时，会先检验一下这笔交易的有效性，当确定这是一笔有效交易之后，会把这笔交易暂存到本地的“待确认交易池”中，同时将这笔交易广播到其他节点，每一个节点都可以独立验证这笔交易的有效性，然后再向外传播，通过这种 P2P 网络，这笔交易迅速的在整个网络中发布。当一个新的挖矿周期开始时（每个周期是十分钟），矿工会从“待确认交易池”中取出合适的交易，将交易打包，随机开始挖矿，也就是做哈希碰撞计算，试图最先找出那个符合条件的目标数字，一旦某个个矿工 A 算出这个数值，矿工 A 便向整个网络公布结果，所有其他矿工收到这条消息后，立刻停止运

算验证这个数值是否有效，当其他节点确认该数值有效后，矿工 A 得到记账权，将他打包的区块添加到区块链上,同时获得新生的比特币和交易手续费奖励,整个网络同步最新的账本，随即进入下一轮挖矿竞争中去，循环往复。当这笔交易写入区块链之后，Bob 就收到了转账。

虽然比特币设计已经相当不错了，但是还是存在很多问题——

(1) 51%算力攻击，现今矿池数量庞大，独立计算机计算能力肯定比不过矿池，矿池算力集中（有点违背去中心化的特点了），有操控的风险，不过造假也只能操作自己的账户金额，因为没有别人的私钥；
(2) 图灵不完备，没有循环语句，不能胜任复杂应用；
(3) 区块容量太小，一秒才 7 笔交易，无法应付现在的金融市场：目前的比特币系统，每一个区块的大小是 1MB，每 10 分钟产生一个区块，平均每一个最基本的比特币交易的大小是大约是 250 字节，因此每秒可以处理的交易数量：每个区块的交易数量：1 * 1024 * 1024 / 250 = 4194 每秒处理的交易数量：4194 /（10 * 60 ）= 6.99 ，约为每秒 7 笔交易；
(4) 确认周期长，相比支付宝微信秒到账的效率，交易确认时间实在太长，需要六个区块也就是一个小时才到账；
(5) POW 耗电量太大，而且这计算是毫无意义的，而且据剑桥大学的工具显示，比特币的耗电量等同于瑞士全国。该工具估计，比特币目前使用了大约 7 千兆瓦的电，占到了全世界电力供应的 0.21%。它需要 7 个 Dungeness 核电站同时发电。比特币全年的耗电量约等于或略超过瑞士全国的用电量。

## 区块链的应用

先谈一谈区块链的特点：

1， 去中心化
2， 不可伪造
3， 不可篡改
4， 不可复制
5， 匿名
6， 基于密码学
7， 分布式可溯源的
8， 账本是公开的，但是匿名货币是加密的

关于区块链的应用，基于它产生的原因和特点分析，区块链是一种打包一定长度（时间维度）数据块然后按照时间节点链接起来的数据结构，主要是为了解决信任问题，区块链就是一种可信任的账单。账单可以用来记录很多东西，因此应用就有如下一些场景：

1，版权保护——时间顺序是固定的，快捷申请版权可当即被记录，且篡改困难，对于保护学者的作品和声誉非常有帮助。也可用于登记一些其他信息，比如土地，房产等的交易证明。
2，代币——比特币
3，物流——防伪简单了很多，哪个环节出了问题清晰了然
4，跨境支付——传统跨境支付手续复杂且费时费钱
5，供应链金融——可以用区块链的私钥签名技术保证企业数据可靠性，比如可以用在金融服务业，企业转化，P2P 金融市场，风险管理，电子商务等方面。

6，信息共享——比如解决了传统对账的困难，可以用来取代纸质版发票。
7，数字资产——实体资产不容易流通且流通不容易被监控

## 区块链的发展和挑战

区块链的发展有三个阶段：数字货币阶段—智能合约阶段—社会治理阶段。
未来可能的方向上，有区块链测试，去中心化，大数据分析，智能合约，同时为人工智能的发展提供了新的机遇。

挑战主要是两个方面--技术，应用。

从技术角度看，区块链的基础技术领域比如密码学等还在发展中，隐私一旦泄露问题极大。另一方面交易数据庞大，智能合约一旦形成就代表规则已经被制定成功，合约的分析就变得非常重要了，合约的合规性验证是防止非法交易必须考虑必须解决的关键，所以可扩展性也是一个挑战。

从应用角度上看，区块链落地到现实生活还有很多限制，影响因素有很多，比如一些挖矿的人也许带有恶意而去攻击区块链，而且私人挖矿越来越多实力越来越强这很难控制。

阅读材料：

《区块链原理，设计与应用》

《区块链基础知识 25 讲 :a non-technical introduction in 25 steps》

《Blockchain_Challenges_and_Opportunities_A_Survey》

《Bitcoin_A_Peer-to-Peer_Electronic_Cash_System》

《中国区块链技术和应用白皮书》