比特币白皮书  
观后感

# 摘要

### 比特币是一种点对点的电子现金系统，其去中心化、安全、高效需求在整个系统构建过程中起着关键性的作用，旨在科学有效地反映客户真实需求，直接关系到后续工程是否能顺利开展以及最终产品是否能预期满足客户要求。本文结合作者实践，以观看比特币白皮书为观后感为背景，讨论了核心需求获取方法及其应用。首先简要说明与传统技术的区别及要点。其次详细阐述白皮书中区块链分模块(包含交易、时间戳服务器工作量证明、网络、激励、隐私及算力等)实现主要采用的技术及其应用：通过有针对性的分模块逐个实现去中心化、安全高效的区块链。最后简要概括项目运行效果及其不足。

# 引言

### 随着互联网信息技术的迅速发展，互联网贸易日趋成熟，用户规模不断上升，但几乎都需要借助金融机构作为可资信赖的第三方来处理电子支付信息。虽然这类系统在绝大多数情况下都运作良好，但仍然内生性地受制于传统的”基于信用的模式”的弱点。无法实现完全不可逆的交易。鉴于此弊端，非常需要这样一种电子支付系统，它基于密码学原理而不基于信用，使得任何达成一致的双方，能够直接进行支付，从而不需要第三方中介的参与。杜绝回滚支付交易的可能。至于双花问题，可通过点对点分布式的时间戳服务器来生成依照时间前后排列并加以记录的电子交易证明，从而解决双重支付问题

# 正文

### 科学有效的获取需求并设计求往往需要综合多种方法折中取舍。针对比特币区块链的设计，其在交易、时间戳服务器工作量证明、网络、激励、隐私及算力等模块都进行了精心的设计。比如：网络通过随机散列对全部交易加上时间戳，将它们合并入一个不断延伸的基于随机散列的工作量证明的链条作为交易记录；最长链条不仅将作为被观察到的事件序列的证明且被看做是来自 CPU 计算能力最大的池 ... 下面就具体设计细节展开详细论述：

### 交易模块(主要通过签名实现)：电子货币是一串数字签名，每一位所有者通过对前一次交易和下一位拥有者的公钥签署一个随机散列的数字签名，并将这个签名附加在这枚电子货币的末尾，电子货币就发送给了下一位所有者。而收款人通过对签名进行检验，就能够验证该链条的所有者。

### 时间戳服务器：通过对以区块形式存在的一组数据实施随机散列而加上时间戳，并将该随机散列进行广播，该时间戳用于证实特定数据必然于某特定时间是的确存在的，因为只有在该时刻存在了才能获取相应的随机散列值。每个时间戳应当将前一个时间戳纳入其随机散列值中，每一个随后的时间戳都对之前的一个时间戳进行增强，如此往复形成链条。

### 工作量证明：在进行随机散列运算时工作量证明机制引入了对某一个特定值的扫描工作，一般随机散列值以一个或多个 0 开始。且随着 0 的数目的上升找到这个解所需要的工作量将呈指数增长，而对结果进行检验则仅需要一次随机散列运算。其特点是难计算易证明，另外该工作量证明机制还用于解决在集体投票表决时谁是大多数的问题。

### 网络：节点始终都将最长的链条视为正确的链条并持续工作和延长它。如果有两个节点同时广播不同版本的新区块，那么其他节点在接收到该区块的时间上将存在先后差别。当此情形时他们将在率先收到的区块基础上进行工作，但也会保留另外一个链条，以防后者变成最长的链条，该僵局的打破要等到下一个工作量证明被发现，当其中一条链条被证实为是较长时另一条分支链条上工作的节点将转换阵营，开始在较长的链条上工作。广播时，其实际上不需要抵达全部的节点。只要交易信息能够抵达足够多的节点，其将很快被整合进一个区块中且区块广播对被丢弃的信息是具有容错能力。如果一个节点没有收到某特定区块，那么该节点将会发现自己缺失了某个区块，也就可以提出自己下载该区块的请求。

### 激励：对每个区块的第一笔交易进行特殊化处理，该交易产生由该区块创造者拥有的新电子货币，此种增加了节点支持该网络的激励，并在没有中央集权机构发行货币的情况下提供了一种将电子货币分配到流通领域的一种方法。另外一个激励的来源则是交易费

### 回收空间及简化支付：如果最近的交易已经被纳入了足够多的区块之中，那么就可以丢弃该交易之前的数据，以回收硬盘空间。为了同时确保不损害区块的随机散列值，交易信息被随机散列时，被构建成一种梅克尔树的形态，使得只有根被纳入了区块的随机散列值。并能够通过梅克尔树的分支加上时间戳并纳入区块的交易。节点通过追溯到链条的某个位置，它就能看到某个节点曾经接受过它且于其后追加的区块也进一步证明全网曾经接受了它，如下图示:

### 隐私：维持隐私可通过切断信息流来实现-公钥匿名。公众可以看到某转账一定的金额但是没有任何信息指向某个确定的人。即公众得知的信息仅仅是有某个人将一定数量的货币发所给了另外一个人，但是难以将该交易同特定的人联系在一起。作为额外的预防措施，使用者可以让每次交易都生成一个新的地址，以确保这些交易不被追溯到一个共同的所有者。

### 算力：用于避免一定程度的攻击。诚实链条和攻击者链条之间的竞赛，可以用二叉树随机漫步来描述，如此其攻击者攻击成功的概率就因为区块数的增长而呈现指数化下降。故攻击一般得不偿失且需要强大的算力

# 结论

### 数字签名及工作量这证明使得攻击者事实上难以改变交易记录。网络强健之处在于它结构上的简洁性。节点间工作大部分彼此独立的只需很少协同，结点可随时离开或加入网络。结点通过CPU 计算力进行投票表决对有效区块的确认。但在具体实施过程中也存在些许不足：比如工作量证明，其矿工只能于拥有算力强大的个体中产生，针对大众用户，难免有失公允；另外：攻击虽有很大难度但并非不可能及分叉会对原有数据造成一定影响等等，有望未来的区块链框架(如” Substrate ：Rust 语言开发，其于升级、高效及创新方面有很大的改进 ”)尽善尽美。总而言之，软件设计及其应用对整个过程影响深远，科学有效地综合选用技术更能反映客户真实需求，同时增强软件可用性、可扩展性和可维护性，从而降低软件风险。