中本聪BTC白皮书-chatgpt总结版

1.简介：传统互联网贸易需要金融机构作为第三方信用中介进行电子支付，但存在交易成本高、无法实现完全不可逆交易、欺诈客户等问题。需要一种基于密码学原理而非信用的电子支付系统，该论文提出的方案能够解决双重支付问题。

2.交易：电子货币是一串数字签名，收款人需要确保之前的所有者没有对更早的交易实施签名，为此需要公开宣布交易信息以确保所有参与者都有唯一公认的历史交易序列。这能够排除第三方中介机构，但要确保绝大多数节点都认同该交易是首次出现。

3.时间戳：提出了一个解决方案，其中关键的部分是一个“时间戳服务器”，它通过随机散列对数据进行时间戳，并通过广播进行验证，确保特定数据确实存在于某个特定的时间点。每个时间戳都将前一个时间戳包括在其随机散列值中，并形成一个链条，从而构建出一个不可篡改的时间戳链。

4.工作量证明：工作量证明机制在分散化的时间戳服务器中的应用。通过在区块中补充一个随机数来满足特定数量的0，构建出一个工作量证明机制，只要该CPU耗费的工作量满足该机制，就可以保证区块信息不可更改。同时，最长的链是由大多数CPU控制的，而工作量证明机制确保了每个CPU都拥有一票，这样大多数的决定表达为最长的链。为了应对节点参与网络的程度波动，难度指向令每小时生成区块的速度为某一个预定的平均数，从而保持网络的安全性和稳定性。

5.网络：节点会持续工作和延长最长的链条，如果有不同版本的新区块，其他节点会在先收到的基础上继续工作，但保留另一条链条。当下一个工作量证明被发现，较长的链条将被证实，节点将转换阵营。新交易只需要广播到足够多的节点即可，并具有容错能力。如果某个节点没有收到区块，它可以提出下载该区块的请求。

6.激励：每个区块的第一笔交易会创造一枚新的电子货币，这提供了激励并使得货币能够分配到流通领域。交易费也提供了另一种激励，将被增加到区块的激励中。随着时间的推移，激励机制可以逐渐转换为完全依靠交易费，以免通货膨胀。激励系统也有助于鼓励节点保持诚实，因为按照规则行事和诚实工作更有利可图，攻击者如果破坏系统将自身财富的有效性受损。

7.回收硬盘空间：比特币网络中如何回收硬盘空间，通过构建 Merkle 树将交易信息随机散列，并只将根纳入区块的随机散列值，从而压缩老区块。同时，内部的随机散列值不必保存，区块头的大小仅有80字节，每年产生的数据只有4.2MB，完全可以存储在PC内存中。

8. 简化的支付确认：Bitcoin是一个去中心化的数字货币系统，其中所有的交易被记录在一个分布式账本上。节点通过工作量证明来竞争创建新的区块，并通过“最长链”规则保持一致性。交易信息被构建成Merkle树以确保不损害区块的随机散列值，并通过

追溯到链条的某个位置来确认交易的有效性。除了保持独立完全性和检验的快速性外，商业机构可能会希望运行自己的完整节点。

9. 价值的组合与分割：交易被设计为可以包含多个输入和输出，用于易于组合和分割价值。交易之间的依赖不需要展开检验之前的所有交易历史。

10. 隐私：区块链交易公开透明，但通过匿名公钥保护交易参与者的隐私。每次交易可以生成新的地址，但并行输入会暴露属于同一所有者的货币，导致隐私泄露风险增加。如果某个公钥被确认属于某人，那么该公钥对应的其它交易也可能被追溯出来。

11. 计算：在比特币系统中，攻击者试图制造替代性区块链的情况，但由于节点不会接受无效的交易，因此攻击者只能试图更改自己的交易信息。攻击者与诚实节点之间的竞争可以用二叉树随机漫步来描述，攻击成功的概率呈指数下降。为了防止支付攻击者的欺骗，收款人预留一个较短的时间将公钥发送给付款人。收款人会等待交易出现在首个区块中，并在等到一定数量的区块链接其后后才能确信交易已经完成。

12.结论：介绍了一种无需信用中介的电子支付系统，采用工作量证明机制的点对点网络来记录交易信息，并防止双重支付。该网络具有简洁、分散的结构，节点不需要明确身份，可以随时加入或离开网络。节点通过CPU计算力进行投票，延长有效的区块链来表达确认，并拒绝无效的区块。该框架包含了一个P2P电子货币系统所需要的全部规则和激励措施。