《比特币白皮书》读后感

按照课程安排通读完《比特币白皮书》一遍，我有几个方面的感悟记述如下。

比特币的创新点

我认为比特币一定程度上是数十年分布式系统和密码学研究的阶段成果。主要体现在四个方面：

- 去中心化的点对点对等网络（比特币协议）
- 不受中心化控制的，任何人均能够参与的独立的验证交易（共识规则）
- 分布式且公开的交易账本（区块链）
- 通过区块链实现全球去中心化共识机制（工作量证明算法）
  由此，比特币可以被视为一种价值互联网，一个通过分布式计算传播价值，确保数字资产所有权的网络。比特币是上述四项创新成果的第一个实际成功实践。

比特币的个人理解

比特币首先是一种构成真正意义上数字货币生态系统基础的概念和技术的总称。其次，它是一种价值单位，用于在分布式网络中的参与者间传输和存储价值，具备防篡改、去监管的天然属性，安全和无地域限制。与传统现实的法币不同，它没有任何中心机构发行和操控。再次，比特币的UTXO账户模型解决了双重支付问题，用户利用私钥签署转账交易，证明自己的比特币所有权。最后，在比特币的这种对等网络里任何参与者都可以作为矿工来验证和记账交易。平均每隔10分钟，一个比特币矿工如果打包并验证了过去10分钟的交易（即挖出一个新的区块），就能获得这个区块全新的比特币奖励。比特币挖矿从根本上解决了中央银行的货币发行和结算功能，取代了任何中央银行的功能。

重点理解的几个知识点

- UTXO账户模型。比特币没有传统现实生活中的银行账户概念，取而代之的是一种被称为未花费的交易输出，它表示区块链上未被花费的交易，可作为新交易的输入。需要扫描整个区块链并按照每个交易依次更新记录才能得到当前状态。
- 非对称加密。公钥可以加密数据或验证数据，私钥可以解密数据和对数据签名。
- 工作量证明。由于PoW机制存在，提升了分布式系统中的作恶成本，让作恶的投入产出比低于作诚实节点的投入产出比，是一种技术与经济学、博弈论结合的点睛之笔。
- p2p网络。打包成区块后，通过p2p协议向全网广播，不是说这个区块在记账完成就是有效的，还是要经过“多数人即正义”的验证的，当且仅当包含在该区块中的所有交易都是有效的且之前未存在过的，其他节点才认同该区块的有效性。“所有交易都有效”，“之前未存在过”这两点就是指全网节点验证交易和验证时间戳，占据绝大多数都验证通过后，这个区块方可被承认。

- Merkel Hash Tree方式存储。由于处于比特币网络中的每个节点都会同步全部的交易记录，这个体积是在不断膨胀的。白皮书提出的解决方案是，使用Merkel Hash Tree 方式存储被消费过的交易信息。
  只把这个Tree的Root节点保存进区块。而Merkel Hash Tree则由一些IPFS、公共节点、信任度高的节点来保存。同时如果想回溯交易，只需去对于的Tree里下载回所有交易记录即可。
- 隐私。比特币网络没有实名账户概念，只有公钥hash后得到的钱包地址。钱包地址无法推断出用户姓名。公众可以看到有一个钱包地址发送一笔数目给另一个钱包地址，但是没有信息能把钱包地址于某个人联系在一起，这样就保证了用户的隐私。这就是只看到有交易在发生，但是不知道是谁在交易。

作为一名初学者，还有很多待验证和思考的问题，留在日后的学习和实践中探索体会，同时能够通过substrate课程的系统学习，找出异同点以期达到触类旁通的效果为最佳。