区块链相关综述论文读书报告

学号：16340023

姓名：陈明亮

1. 对于区块链的基本认识

《区块链技术发展现状与展望》一文中，作者充分地阐述了区块链的定义，用途，以及当今社会大环境下的发展现状与前景。为了更好地理解和掌握区块链课程的内容，我们首先需要弄清楚区块链的`基本含义`与`技术堆栈`。

区块链是以比特币为代表的数字加密货币体系的核心支撑技术，建立在区块链技术之上的应用从一开始的比特币系统，到号称是BlockChain2.0版本应用的以太坊，这两种区块链代表性应用无不处处体现着其优势所在，迅速地在中国社会上引起广泛关注。同时，当谈到区块链技术的核心优势，其最具有代表的则是去中心化体系，将正常交易中的中介节点去除，使用高 安全性的数据加密算法，以及具有唯一标识性的时间戳，还有分布式共识，经济激励机制，建立起节点与节点之间无需相互信任即可开启交易行为的分布式去中心化系统。

区块链技术的起源是于2008年由化名为"中本聪"的学者(或团队)在密码学邮件组发表的第一篇关于区块链技术的阐述和奠基性论文《比特币：一种点对点电子现金系统》。在该篇论文中，作者详细地介绍了当今中心化交易技术的缺点：高成本，低效率以及数据信息存储不安全等方面，首次引入比特币数字货币的概念，提出了现代历史上继个人电脑，Web技术之后的颠覆式创新。比特币点对点交易方式被当今的许多学者认为是人类交易史上，继血亲信用，贵金属信用，央行纸币信用发展史之后的第四个里程碑，实际上影响着社会上的金融活动和交易平台，也是这些领域发展去中心化趋势的核心推动力。

2. 区块链采用的技术堆栈

- 去中心化系统构建
  区块链整体数据的存储，记账，验证，维护，传输等过程并非在中心媒介上运作，而是基于分布式系统结构，在每个节点上均能够查看到交易记录，账本信息。
- 时序数据维护
  对每一个区块都分配创建时间戳，标识其整个区块数据的时间维度，实际上为之后的区块验证行为，以及整条链上的数据追溯提供了依据。
- 安全性保障
  通过采用非对称加密算法RSA，很大程度上规避了节点交易密钥被破解或者数据被解密的极端行为，同时运用分布式系统多节点的运行模式，采用共识算法，组成强大的算力和规模来抵御外部对于区块链内部数据，如交易账本，个人账户额度的篡改或伪造。
- 集体维护激励
  采用经济激励机制，为特定的纯数学难题悬赏一定额度的虚拟货币，鼓励节点用户参与解题过程，即"挖矿"行为。首先使用强大计算资源解出难题者即获得奖金，同时获得所有权开辟新的区块，添加到当前的链上。
- 可编程性
  区块链内的节点用户可以通过脚本编程，创建自定义的智能合约，或者其他的基于区块链上的去中心化应用，甚至发行自己的虚拟货币。

3. 区块链面临的挑战

1. 去中心化带来的安全性威胁
   区块链技术中最核心的部分在于去除了多余的中介机构，然而这也为其内部的权利问题带来了困扰。理论上，基于PoW共识算法过程中，只要掌握全链上超过或等于51%的算力，就有能力更改并重写链上的数据和规则，从而获取巨额的虚拟货币，甚至实现双重支付。
2. 加密算法潜在的不安全性
   当前的区块链上广泛运用的数据加密算法为非对称加密算法，如SHA256等。实际上，当前的密码学与数学理论正蓬勃发展，虽然对于一般的计算机来说，暴力破解RSA系列的哈希密钥是完全不可能的事情，但是量子计算机的发展，以及近日的网传黎曼猜想的证明，都将矛头指向了大数的质数因子快速分解的算法上，这对RSA算法具有实质性的威胁。
3. 节点完全备份数据导致效率低下
   区块链要求系统内每个节点完全备份一份当前链上的所有数据，这实际上是非常消耗存储空间的，不利于当今货币交易爆炸，信息产生迅速的背景，所以造成链上交易的低下，据统计，当前比特币系统上每秒只能够处理7笔交易。
4. 政治方面因素
   对于大多数国家，尤其是中国政治圈，都实施着一党一国的政治制度，推崇实质的纸币流通，崇尚中心机构的建立。国家前段时间为了让人民币流通性增加，曾明文下令移动支付不允许太过"放肆"，不得贬低货币支付。而区块链技术，这里尤其指虚拟货币系统，实际上是比移动支付更加高级，更加便利的支付手段，但其去中心化的思想，在当今的货币支付大环境下是否能得以生存，又有谁能够得知呢?

4. 区块链的应用

1. 虚拟货币系统
   比特币，以太坊等都是建立在区块链技术上的交易应用，实际上依靠其强大的分布式存储功能，以及高可靠性，许多投资者通过购买相应的虚拟货币等待升值赚取利润，这直接鼓励设备商们大量购入设备建设矿池，挖取货币。同时，技术人员通过编写相应的智能合约，直接更新或巩固货币系统的安全性。
2. 分布式数据库系统
   采用区块链去中心化核心，以`Distributed`为特点的DBMS也在迅速发展。此类型的数据库系统能够大量存储隐秘数据，具有优秀的抵御攻击性能，和数据恢复弹性，规避了中心化机构容易丢失数据的致命缺点。此外，数据库内部的加密可通过RSA哈希运算，生成Merkle树打包记入系统。同时，还可以结合多重签名技术强化数据库的访问权限，设定特定秘钥授权才可以进入内部访问权限。
3. 数据公证认证系统
   利用区块链的强追溯性，以及多节点数据存储带来的不可篡改性，我们可以建立其之上的个人证件认证系统，将个人所得的许可证，资格证，身份证等等，此类的重要证件提供虚拟电子认证记录，帮助实际情况下的高效率审计核实个人身份。