区块链技术调研报告

学号：1120180207　姓名：唐小娟　班级：07111801

一、引言

区块链是近些年来较受欢迎的一项技术，它的集成应用在新的技术革新和产业变革中起着重要作用，在金融市场、物联网、供应链、医疗等许多领域和服务中也有了相应的应用。本文查阅了引用量较高的论文，对区块链技术的概念、特点、结构以及它的某些算法进行介绍，同时还补充了一些自己对区块链的见解和想法。

二、概念

区块链来源于 2008 年由“中本聪”发表的论文《比特币：一种点对点电子现金系统》，文献[1]中说到区块链是一种按照时间顺序（时间戳）的方式将区块以链接的方式组成的分布式存储系统，同时用密码学技术、时间戳、共识机制保证数据的不可篡改性和不可伪造性，它具有去中心化、匿名化、开放、自治、不可更改等特性。

目前我们所说的比特币，是区块链技术的一个典型应用。所谓比特币，其实是数字货币，它和我们现实生活中的人民币不一样，它具有虚拟性，而且难以保证交易双方互相承认，而区块链技术解决了数字货币面临的两个问题：双重支付问题和拜占庭将军问题[3]。双重支付问题是指同一笔钱可以进行多次交易，拜占庭将军问题是指缺少可信任的中央节点的情况下，分布式如何达成共识和建立互信。

在我看来，双重支付问题最本质的原因是数字货币的虚拟性导致它可以被复制，所以我们需要找到一个唯一性事物对它进行标记，而根据自然物理观点，时间是唯一的，所以在区块中添加时间戳可以唯一标识。而拜占庭将军问题，古时候皇帝管辖偏远地方的臣子，采用相互牵制的手段，每个人都想要获取利益，而只要获取利益的手段是唯一的，那么即使缺乏可信任的中央节点，分布式依然可以达成共识，也就是采用了 PoW（工作量证明）机制。

接下来，我会从区块链的架构上来讲述它所运用的一些算法以及算法所带的好处。

三、架构

3.1 数据层

数据层将交易信息和代码封装到区块的区块体中，而时间戳、Merkle 树根、随机数，前一个区块的哈希值、当前区块的哈希值等其他信息封装在区块的区块头中，整个区块链接到最长的主区块链上，如下图所示。主要实现功能是 Merkle 树的交易验证、利用时间戳的哈希封装、以及非对称加密。

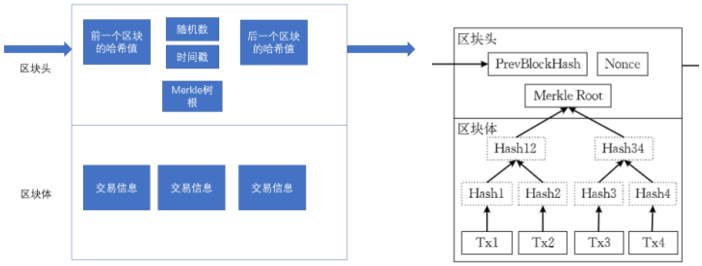

图 1　　图 2

Merkle 树：它的构建过程是一个递归计算散列值的过程，将区块体的数据进行分组哈希，生成的新哈希值插入到 Merkle 树节点中，如此递归，直到生成 Merkle 树根，存储在区块头中。比特币采用的是二叉 Merkel 树，采用这样的数据结构一方面是为了解决快速比对交易信息是否完全正确的问题，要验证每一个交易是否在区块里不必遍历区块交易信息的每一个 Hash 值，而采用二叉树的方式，查找路径长度复杂度为 O（logN），这里举例说明，图 2 中，如果要验证交易 Tx1 是否在区块中，只需要节点 Hash2、Hash34、Merkle 根就可以验证，不需要区块全部数据。这种高效在大交易规模中异常明显[4]。另一方面，实现了轻客户端模式，只需要下载区块头，不需要下载整个区块链数据，这样，哈希运算可以高效的运行在智能手机甚至物联网设备上。

时间戳：采用了带有时间戳的链式区块结构存储结构，主链上各区块是按照时间顺序依次排列的，时间的不可重复性使得区块链具有可验证性和可追溯性，同时也防止了双重支付问题。

非对称加密算法：实现了某种程度上的安全性，如果区块链是公有链，允许任意节点加入网络，这样很有可能会被女巫攻击，破坏可用性；除此之外，传统数据库系统设计了完善的用户管理和存取控制，用户管理要运行在中心化的节点上，这就和去中心化的区块链有所不同，而存取控制与公有链的数据公开性和透明性矛盾。区块链主要采用数字签名与验证来解决这样的矛盾，以确保不可伪造性和不可否认性。这里的数字签名采用非对称密钥方式，非对称密钥使用两个密码（公钥和私钥），用其中一个密钥加密信息后，只有另一个对应的密钥才能解开。比特币的密码机制是：256 位比特币私钥通过 SHA256 哈希算法和 Base58 转换，形成 50 个字符长度的私钥给用户；而公钥是由比特币私钥经过 Secp256k1 椭圆曲线算法生成的 65 字节长度的随机数。公钥进行双哈希运算后生成 20 字节的摘要，在经过 SHA256 和 Base58 转化形成 33 字符长度的比特币地址[3]

3.2 网络层

网络层，主要进行信息传播，它封装了区块链系统的组网形式、消息传播协议和数据验证机制等要素，通过设定传播协议和数据验证机制，使得每一个节点参与到记账和校验过程中，只有当区块数据通过全网大部分节点校验后，才能记入区块链。

组网方式：采用 P2P 网络，网络中的每个节点均地位平等，而且以拓扑结构相互连通和交互，每个节点都要承担网络路由、验证区块数据、传播区块数据、发现新节点的功能。

数据传播协议：生成数据的节点广播到全网其他所有节点来加以验证。

数据验证机制：主要是从两方面验证有效性，一个是未处理的交易数据，从数据结构和内容进行验证，防止无效的数据在网络中传播；第二是收到区块的时候，验证时间戳、工作量证明等数据。

3.3 共识层

权力分散却可以实现共识，这要归功于共识层，它主要是用来解决分布式一致性的问题，采用的重要算法是 PoW、PoS 和 SPoS，这里详细介绍 PoW 算法。

Pow 算法：它的核心思想就是用算力竞争。步骤如下：①将未确认的交易信息和即将进行奖励的比特币交易形成区块体的交易集合。②计算 Merkle 树根计入区块头，填写其他数据，其中随机数置 0；③随机数+1，计算区块头的双 SHA256 哈希值，如果小于等于当前目标难度值，则获得了区块的记账权；否则继续步骤③一直到某一个节点获得记账权为止；④如果超过一定时间没成功，则更新时间戳和未确认交易集合，重新计算。

目标难度值越小，那么随机数就越难找到，而对某一区块的修改都必须重新计算其后所有区块的 SH256，这需要极强的算力，保证了安全性和不可篡改性。但是物竞天择，适者生存，算力大的往往会留存下来，随之算力越来越大，攻击的能力也越来越强。我设想是否可以加一点随机因素，在算力比较的基础上，添上一点平等的机会，也就是我们所说的摇号必要条件是有一定程度的算力，但是依然要看运气。不过最后专业的解决办法是隔一段时间减少难度目标的值。所以我的设想是否是正确还有待证明。

3.4 激励层

PoW 获胜者具有打包区块的权力，区块链用比特币奖励该矿工。从某种意义上说，采用特定的经济激励机制保证分布式系统中所有节点均可参与数据区块的验证过程。也就是，通过利益化使得个体节点不断提高算力来提高整个系统的安全性和有效性。就像公司奖励制度的年终奖一样，表现好的获得酬劳高，以此激发各个员工的斗志来为整个公司赚取财富。换句话说，用比特币来买安全性和有效性，资本的世界不会损失资本。

3.5 合约层

主要是运行在区块链上的一段计算机程序，扩展了区块链的功能，丰富区块链的上层应用。如果说数据、网络、共识层次作为区块链底层中的数据表示、数据传播、数据验证的功能，那么合约层就是建立在这之上的逻辑与算法，以此实现具体场景的应用[5]。

四、总结

毫无疑问，区块链是近年来的热点，虽然它还存在一些问题，但随着技术的进步和发展，有些问题已经慢慢得到解决。当我们享受区块链的同时，也要对它所带的安全问题保持谨慎。总之，我感叹中本聪先生的智慧，也相信在未来的某一天区块链会带来世界巨大的进步，如今大数据充斥，如何管理数据、存储数据已经变得尤为重要，而区块链的特点决定了它将会是一个很好的解决方案。

[1] NAKAMOTOS. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. https://bitcoin.org/bitcoi n.pdf.

[2]邵奇峰，金澈清，张召，钱卫宁，等 区块链技术：架构及进展[J]. 计算机学报，

[3] 19 Antonopoulos A M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. USA: O Reilly Media Inc., 2014.

[4]沈鑫，裴庆祺，刘雪峰 区块链技术综述[J]，网络与信息安全学报

[5] Iuon-Chang Lin, Tzu-Chun Liao. A Survey of Blockchain Security Issues and Challenges