



题目 比特币白皮书读书报告

作者姓名 刘瑞洋

作者学号 22051216

所在学院 软件学院

提交日期 二〇二一 年 一 月

目录

[摘要 3](#_Toc62992895)

[一、比特币之前的数字货币 4](#_Toc62992896)

[二、白皮书中的主要内容 4](#_Toc62992897)

[1.简介 4](#_Toc62992898)

[2.交易 5](#_Toc62992899)

[3.工作量证明 6](#_Toc62992900)

[4.网络 6](#_Toc62992901)

[5.激励 7](#_Toc62992902)

[三、关于比特币的一些思考 8](#_Toc62992903)

[1.不可篡改，亦正亦邪 8](#_Toc62992904)

[2.激励制度不健全 8](#_Toc62992905)

[3.有中心化的趋势 8](#_Toc62992906)

[参考文献 9](#_Toc62992907)

摘要

自2009年初上线以来，比特币正在革新全球支付行业，引发世界各地的人们都在重新思考他们的钱的含义。作为了解比特币最直接也是最基本的读物，比特币白皮书（Bitcoin: A Peer-to-Peer Electronic Cash System[1]），是由 Satoshi Nakamoto 在 2008 年发布的。本文将通过阅读比特币白皮书，总结比特币的交易、共识、网络等方面的内容，并提出自己的一些关于比特币的思考。

**关键词**：比特币， 数字货币，区块链

# 一、比特币之前的数字货币

1982年，大卫·乔姆最早提出了不可追踪的密码学网络支付系统[2]。1990年，乔姆将他的想法扩展为最初的密码学匿名现金系统，这个系统就是后来所谓的ecash[3]。1998年，戴维（Wei Dai）发表文章阐述一种匿名的、分布式的电子现金系统，他将其命名为“b-money” [4]。同一时期，尼克·萨博发明了“Bit gold”。但是这些早期的加密货币并没有成功的生存下来。

以B-money为例分析，他继承了前人利用POW进行造币的思想，并把记账的工作分配到了分布式节点上，但是他缺乏必要的共识系统，解决双花的工作还是要通过一个第三方来进行。

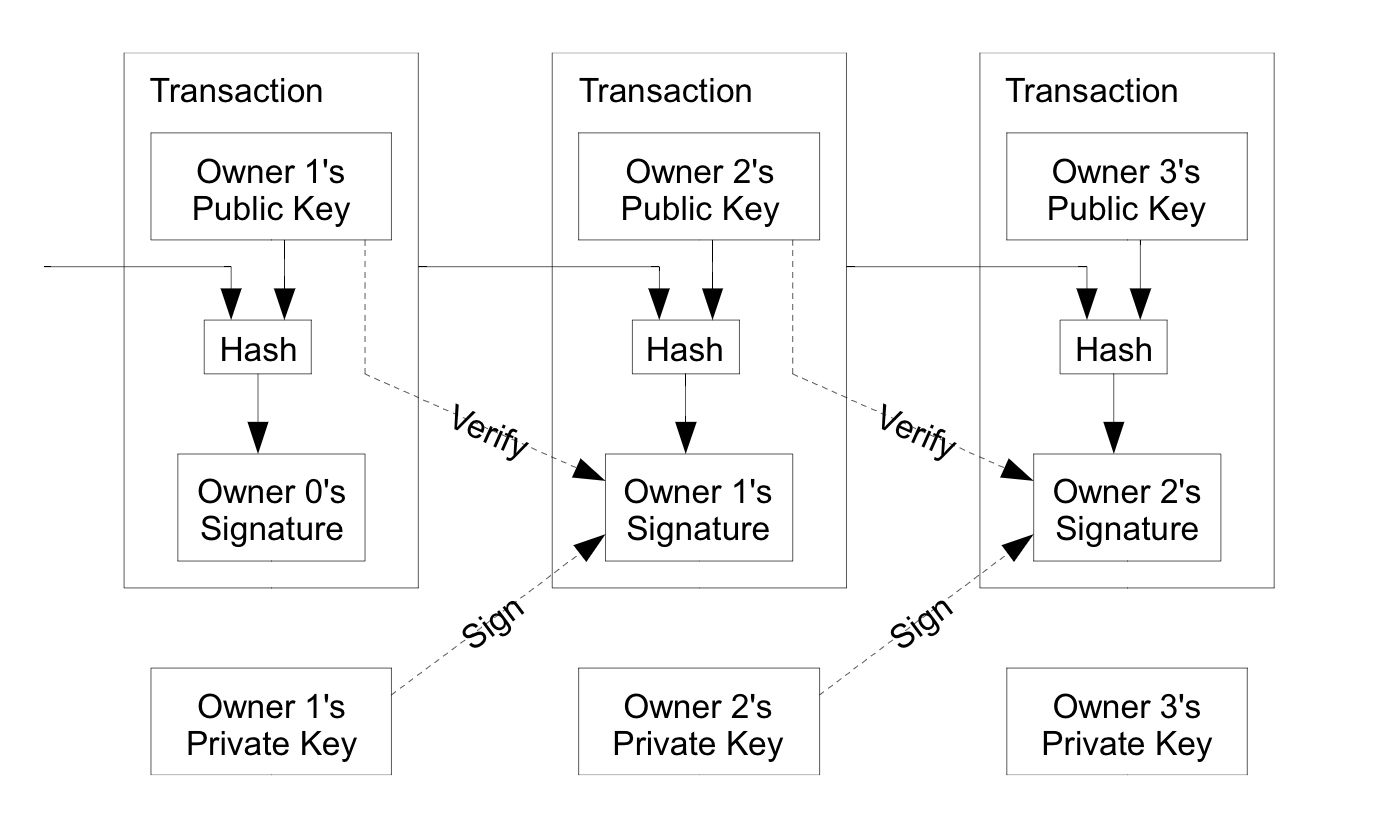
在比特币白皮书的摘要中，作者也强调了这一问题: “Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.We propose a solution to the double-spending problem using a peer-to-peer network.”,所以这个问题的解决也是比特币的一大亮点，也是它富有生命力的一个关键，只有用去中心化的方法解决双花才能真正实现一个去中心化的数字货币。

# 二、白皮书中的主要内容

## 1.简介

简介中，中本聪认为比特币要完成的是一种基于密码学原理而不是基于信用的支付手段。这里比特币使用密码学原理取代的是用户对中心化的支付中介的信任，而不是对于交易双方的信任。并且在交易中，比特币系统主要保护的是卖家的权利，而对于买家，中本聪认为：“routine escrow mechanisms could easily be implemented to protect buyers”。

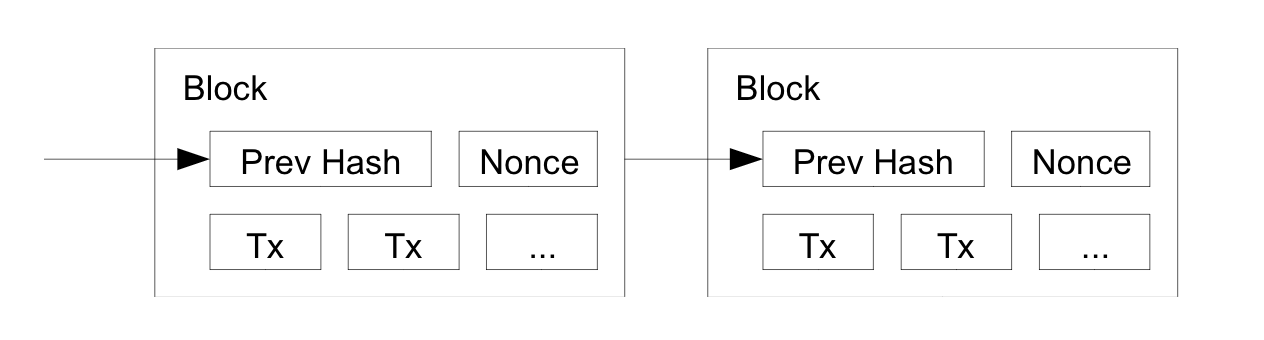
## 2.交易



区块链账本是一种基于交易的账本模式，也就是说，当你拥有一个向你支付比特币的交易时，你就拥有了相应数量的比特币，而当你想要转出比特币时，则需要创建一个向外支出的交易。每一笔交易都如上图所示，使用非对称加密的方式加密，来验证身份。但是仅仅采用这种机制难以验证双花的情况，传统的解决方案是引入一个中心化的机构来解决这一问题。类似每次交易后，硬币必须归还给铸币厂才能发行新的硬币，而且只有直接从铸币厂发行的硬币才被认为是没有双花。

但是这种方案很明显与去中心化的思想相违背。中本聪是这样分析这个问题的。他认为，对于双花交易的验证范围是在本次交易发生之前的所有交易。也就是说，只需要验证本次交易之前那笔交易是否已经被花过即可。而验证的唯一方式是知晓之前的所有交易。在中心化的“铸币厂”中，它知晓所有的交易，并且决定了交易的顺序，而在去中心化的比特币中，则需要将所有的交易信息公开，并且需要整个系统内的所有参与者，都有唯一公认的历史交易序列，这种情况下可以通过调查之前是否有交易已经消费过了现在正在进行的交易来判定双花。比特币的交易是一个时间序列的链条，在产生一条新的交易记录时永远有先后顺序，所以即便是双花也总有先后顺序，不可能同时创造两笔交易，因此只需要证明其中一条是有效的，并且将其记录到交易链条上即可，那么其他的交易就是无效的了。

## 3.工作量证明



所谓工作量证明，具体如下。首先在SHA-256下，随机散列值以一个或多个0开始。而工作量证明的目的是找到一个随机数，使得该随机数在hash之后的值小于等于给定的目标值。那么随着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，但是检验结果仅需要一次随机散列运算。每个区块中有一Nonce域，这个随机数要使得该给定区块的随机散列值出现了所需的那么多个0。而要满足这种条件，唯一的方式就是不停的尝试，理论上没有直接构造的得出结果的方法。由于之后的区块是链接在该区块之后的，所以想要更改该区块中的信息，就还需要重新完成之后所有区块的全部工作量。

Pow保证了即使节点作恶，他的成本跟正常的节点是一样的高，这样有效的提高了作恶的门槛和难度。此外即使有人有能力发动51%攻击，他将击垮整个比特币的价值，他的作恶回报将变得一文不值。

同时，该工作量证明机制还解决了在集体投票表决时，谁是大多数的问题。大多数表现为最长链，因为最长链包含了最多的工作量。此外，针对硬件设备的进步，比特币系统会通过调整挖矿难度使得出块时间保持稳定。

## 4.网络

白皮书中是这样描述网络的比特币网络的

1)新的交易向全网进行广播

2)每一个节点都将收到的交易信息纳入一个区块中

3)每个节点都尝试在自己的区块中找到一个具有足够难度的工作量证明

4)当一个节点找到了一个工作量证明，它就向全网进行广播

5)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

6)其他节点表示他们接受该区块，而表示接受的方法，则是在跟随该区块的末尾，制造新的区块以延长该链条，而将被接受区块的随机散列值视为先于新区快的随机散列值

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，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。直到其中的一条链条被证实为是较长的一条，那么在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。所谓“新的交易要广播”，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，那么他们将很快被整合进一个区块中。而区块的广播对被丢弃的信息是具有容错能力的。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。

## 5.激励

比特币中的激励分为两类：挖矿出块奖励和交易费。前者是指每个区块的第一笔交易将进行特殊化处理，该交易产生一枚由该区块创造者拥有的新的电子货币。后者是从交易的金额中取出一部分作为交易费用。出块奖励在每生成21万个区块的时候就会减半，于是比特币的总数是确定的，也就是2100万个。中本聪认为固定数量的比特币可以保证不发生通胀，并且在挖矿奖励逐渐变低的情况下，交易费用可以保证打包有持续的收益。并且他认为，奖励机制会让有作恶想法的节点放弃作恶，因为他们可以通过诚实的工作获得更大收益

在一个去中心化的系统中，激励是必要的，因为一个p2p系统要想好好运行，必然需要更多的节点参加，并且这种参与不能是基于一时激情，而是要长久稳定的。激励机制可以为p2p系统形成一种纽带，最直接的莫过于经济激励。而激励机制必须与维持系统运行的核心相关，例如PT站，PT是一种以你需要的资源为代价的带宽激励机制，你必须有足够的上传量才能获取下载量，这种激励制度保障了PT站点的长期存在。比特币系统需要大量的计算资源，所以对付出工作量的节点给予激励是必要和关键的。

# 三、关于比特币的一些思考

## 1.不可篡改，亦正亦邪

根据白皮书的描述，区块链记账不可篡改虽然是有前提的，但是客观上更改是不现实的。即使拥有了超过51%的算力的支持，由于工作量证明的存在，回滚交易需要耗费大量的资源，这使得回滚交易通常是不划算的。介于这个事实，有时即使交易双方认为应该回滚或者全网多数节点认为应该撤销的交易，实际上也无法回滚和恢复的。例如暗网中的非法交易、勒索、盗用比特币、交易所跑路等事件，都是利用了不可篡改的特性。即使多数人支持回滚，实际情况上也很难操作。

## 2.激励制度不健全

随着比特币挖矿进入后期，激励的主要部分将依靠服务费来维持。如果比特币不能大规模应用，那么矿工为了维持挖矿成本，必然会提高服务费用，高昂的服务费将更不利于比特币的大规模应用。或者造成节点萎缩，服务打包时间过长或者更易受到攻击，如此往复下去会造成恶性循环，不利于比特币的发展。

## 3.有中心化的趋势

随着时代的发展，挖矿的主力从通用CPU到GPU再到专门的ASIC芯片越来越专精，大型矿场的出现也使得算力越发集中，普通用户基本沦为了旁观者。比特币之后的很多竞争币也采用了很多不同的机制改良POW，例如ETH2、DOT[5]使用的POS[6]，但是基本也会有走向中心化的趋势。

# 参考文献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[R]. Manubot, 2008.

[2] David Chaum, Blind signatures for untraceable payments, Advances in Cryptology - Crypto '82, Springer-Verlag (1983), 199–203.

[3] Chaum, David; Fiat, Amos; Naor, Moni. Untraceable Electronic Cash (PDF). Lecture Notes in Computer Science.

[4] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[5] Wood G. Polkadot: Vision for a heterogeneous multi-chain framework[J]. White Paper, 2016.

[6] Kiayias A, Russell A, David B, et al. Ouroboros: A provably secure proof-of-stake blockchain protocol[C]//Annual International Cryptology Conference. Springer, Cham, 2017: 357-388.