# 

学号 142010020132

年级 14级



**本科毕业论文**

**基于区块链技术的虚拟货币矿机的实现**

|  |  |
| --- | --- |
| **专 业** 应用物理学 |  |
| **姓 名** 王朋飞 |  |
| **指导教师** 邰非 |  |
| **评 阅 人** |  |

**2018年5月**

**中国 南京**

**BACHELOR'S DEGREE THESIS**

**OF HOHAI UNIVERSITY**

**Realization of virtual currency mining machine based on blockchain technology**

College ：Faculty of Science

Subject ：Applied Physics

Name ： Wang Pengfei

Directed by ： taifei Professor

May 2018

NANJING CHINA

学术声明：

**郑 重 声 明**

本人呈交的毕业论文，是在导师的指导下，独立进行研究工作所取得的成果，所有数据、图片资料真实可靠。尽我所知，除文中已经注明引用的内容外，本设计（论文）的研究成果不包含他人享有著作权的内容。对本设计（论文）所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确的方式标明。本设计（论文）的知识产权归属于培养单位。

摘 要

虚拟货币从诞生到现在，已被越来越多的人接收，并有很多商家开始尝试以虚拟货币作为支付方式，这完全得益于虚拟货币去中心化的属性，这种属性能保证货币不会滥发、超发，也不受任何行政干预，从而能有效应对通货膨胀，通货膨胀正是当前各国央行无法解决的难题。从技术层面上来看，去中心化属性的实现是基于区块链技术，这项技术是结合加密、解密、链表、Hash处理、树及工作量证明来实现，当前这项技术已成为应用研究的热点领域。各国政府、机构、公司已投入大量的人力、物力去研究、开发基于区块链技术的相关应用。

论文中，我们选择了最为著名的虚拟货币：BTC比特币作为研究对象，通过对比特币源代码的分析和研究，同时利用更通俗易懂的编程语言Python来进行直接简单地模拟比特币的运行原理。使用SDK集成平台Anaconda，IDE编辑器为IntellJ IDEA,实现比特币的挖矿程序，从而完成比特币去中心化中的核心功能。

**关键词：**BitCoin；BlockChain；Python；flask；web；

**ABSTRACT**

Since the birth of virtual currency, it has been accepted by more and more people, and many businesses have begun to try to use virtual currency as a payment method. This is entirely due to the decentralized nature of virtual currency, which guarantees that currency is not It will be spamming, hyperventilation, and without any administrative intervention, so that it can effectively cope with inflation. Inflation is precisely the problem that central banks cannot solve. From a technical perspective, the realization of the decentralized attributes is based on blockchain technology. This technology is combined with encryption, decryption, linked lists, Hash processing, trees, and workload proofing. The current technology has become an applied research. Hot areas. Various governments, agencies, and companies have invested a lot of human and material resources to research and develop related applications based on blockchain technology. In the paper, we chose the most famous virtual currency: BTC Bitcoin as a research object, through the analysis and research of the bitcoin source code, and at the same time using a more straightforward programming language Python to directly and simply simulate the operation of Bitcoin. principle. Bitcoin's mining process is implemented to complete the core functions of Bitcoin decentralization.

**Key words:** BitCoin；BlockChain；Python；flask；web；

1. 相关介绍
   1. **Bitcoin**

Bitcoin,缩写BTC，其概念最初由中本聪在2009年提出，比特币是一种P2P形式的数字货币。点对点的传输意味着比特币是一个去中心化的支付系统。

与传统货币相比，比特币有如下的三个优势：

1. 去中心化。比特币不依靠特定的货币发行机构，它根据特定的算法，通过大量的计算产生，产生的比特币通过众多节点构成的分布式数据库进行确认，使用密码学来保证比特币被真实的拥有者进行交易。
2. 隐私性。比特币账号由特定摘要算法根据用户公钥生成，不需要进行实名登记，即没有任何的身份信息。对于比特币来说，交易是支付给地址，而不是某个人，而用户可以根据私钥来申明账户的所有权。一个人可以拥有多个地址。
3. 公开性。比特币系统其实就是一个公开账本系统，任何人只要想查看比特币系统的交易记录，都可以从它附近的节点进行下载这些交易记录。每个账户的余额也是通过这些公开的交易记录中计算得来的。
   1. **Python**

Python 是一个高层次的结合了解释性、编译性、互动性和面向对象的脚本语言。作为一种[解释型语言](https://zh.wikipedia.org/wiki/%E7%9B%B4%E8%AD%AF%E8%AA%9E%E8%A8%80" \o "直译语言)，Python的设计哲学强调代码的[可读性](https://zh.wikipedia.org/wiki/%E5%8F%AF%E8%AF%BB%E6%80%A7" \o "可读性)和简洁的语法（尤其是使用空格缩进划分代码块，而非使用大括号或者关键词）。相比于C++或Java，Python让开发者能够用更少的代码表达想法。不管是小型还是大型程序，该语言都试图让程序的结构清晰明了。Python 的设计具有很强的可读性，相比其他语言经常使用英文关键字，其他语言的一些标点符号，它具有比其他语言更有特色语法结构。同时，Python也是一种面向对象的语言，为代码编写的灵活性提供了充足的保障。

另外，Python有相对较少的关键字，结构简单，和一个明确定义的语法，学习起来更加简单，同时用Python书写的代码定义更加清晰，非常易于阅读，对于源代码的维护也非常容易，而对于Python来说，它最大的优势之一就是拥有丰富的库，跨平台的，在UNIX，Windows和Macintosh兼容很好。同时它还有可移植，可扩展，可嵌入等特点。因此，在这篇论文中，我选择使用Python来进行系统的模拟，原因之一就是因为使用Python书写的代码更容易让阅读者理解，同理，对于代码的编写也是较其他语言为简单的。

* 1. **Flask**

Flask是一个使用[Python](https://zh.wikipedia.org/wiki/Python" \o "Python)编写的轻量级[Web应用框架](https://zh.wikipedia.org/wiki/Web%E5%BA%94%E7%94%A8%E6%A1%86%E6%9E%B6" \o "Web应用框架)。基于Werkzeug [WSGI](https://zh.wikipedia.org/wiki/WSGI" \o "WSGI)工具箱和Jinja2 [模板引擎](https://zh.wikipedia.org/wiki/%E6%A8%A1%E6%9D%BF%E5%BC%95%E6%93%8E" \o "模板引擎)。Flask使用BSD授权。

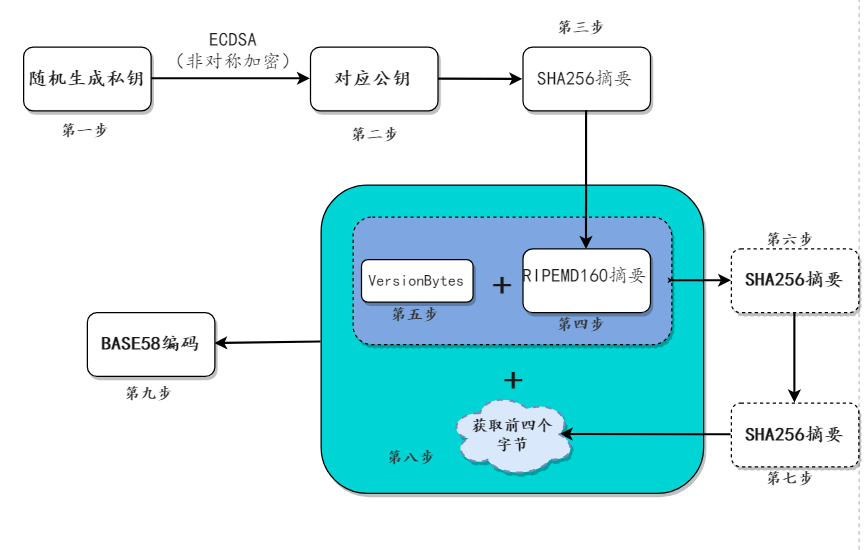
Flask被称为“microframework”，因为它使用简单的核心，用extension增加其他功能。Flask没有默认使用的数据库、窗体验证工具。然而，Flask保留了扩增的弹性，可以用[Flask-extension](http://flask.pocoo.org/extensions/)加入这些功能：[ORM](https://zh.wikipedia.org/wiki/%E5%B0%8D%E8%B1%A1%E9%97%9C%E4%BF%82%E6%98%A0%E5%B0%84" \o "对象关系映射)、窗体验证工具、文件上传、各种开放式身份验证技术。

* 1. **Anaconda**

1. 比特币系统介绍
   1. **比特币地址**

在上面，我们提到，比特币进行交易的时候是向比特币地址进行交易的，这个比特币地址就相当于我们银行卡的账号一般，谁拥有这个比特币的地址，那么在这个比特币地址下面的比特币就属于谁，那么地址是怎么生成的呢？

下面是比特币地址的生成过程详细图解：

图2.1 比特币地址计算过程

上面的过程中，涉及到九个步骤，分别使用了不同的算法，包括椭圆曲线加密算法（ECDSA），SHA256，RIPEMD160消息摘要算法，BASE58加密算法。其中ECDSA，SHA256，PIPEMD160算法是不可逆的。BASE58算法是可逆的。

具体过程介绍如下：

1. 第一步。随机生成私钥，私钥取值范围为32个字节的数字，即范围为0~2^256,这个范围大到比地球上原子数还要大，可以保证私钥唯一性。
2. 第二步。利用椭圆曲线加密算法ECDSA加密私钥生成公钥。由于使用非对称加密，外人无法通过公钥推算出私钥的内容，因此公钥可以对外公开而无需担心安全问题。
3. 第三步。计算公钥SHA256摘要。获取Hash值。
4. 第四步。对第三步的结果再进行RIPEMD160摘要，获取Hash值。
5. 第五步。在第四步的结果前面添加地址的版本号，这个版本号一般是一个字节的。
6. 第六步。对第五步的结果进行SHA256摘要，获取Hash值。
7. 第七步。对第六步的结果再进行SHA256摘要，获取Hash值。
8. 第八步。获取第七步结果的前四个字节（我们称之为校验码），并添加到第五步的结果后面。因此这个时候数据结果为“版本号+第五步结果+校验码”。
9. 第九步。对第八步的结构进行BASE58编码。这个结果就是我们的比特币地址了。例如：“16UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM”。

上面的过程中，私钥就相当于银行卡的密码，比特币地址就相当于银行卡的账号，比特币地址是从私钥经过密码学运算得到的，我们可以看到第二、三、四、六、七这几个步骤是不可逆的，因此是没有办法从比特币的地址获取到比特币的私钥的，也就是说虽然银行卡账号是从密码得来的，但是却没有办法从账号计算得到密码。

一个人可以生成多个比特币地址，并用在不同的交易上面，而且除非使用者自己披露

外人是没有办法看出这些地址之间的联系的。

* 1. **比特币交易**
     1. **简介**

比特币交易是比特币系统中最重要的部分。根据比特币系统的设计原理，系统中任何其他的部分都是为了确保比特币交易可以被生成、能在比特币网络中得以传播和通过验证，并最终添加入全球比特币交易总账簿（比特币区块链）。比特币交易的本质是数据结构，这些数据结构中含有比特币交易参与者价值转移的相关信息。比特币区块链是一本全球复式记账总账簿，每个比特币交易都是在比特币区块链上的一个公开记录。

* + 1. **交易的输入输出**

比特币交易中的基础构建单元是交易输出。 交易输出是比特币不可分割的基本组合，记录在区块上，并被整个网络识别为有效。 比特币完整节点跟踪所有可找到的和可使用的输出，称为 “未花费的交易输出”（unspent transaction outputs），即UTXO。 所有UTXO的集合被称为UTXO集，目前有数百万个UTXO。 当新的UTXO被创建，UTXO集就会变大，当UTXO被消耗时，UTXO集会随着缩小。每一个交易都代表UTXO集的变化（状态转换）。

* 1. **比特币账簿、区块链、区块**
     1. **比特币账簿**

比特币账簿上面记录着整个比特币网络的所有的交易记录，比特币账簿保存在彼此链接运行的比特币网络上面。前面提到，比特币网络是一个P2P网络，因此任何链接这个网络的人只要有意愿即可从比特币网络上面下载到比特币账簿上的记录，即上面提到的公开性。比特币账簿上面的已经被打包的交易记录不可被更改。每个比特币地址下的比特币数量是通过这个比特币的账簿的交易记录计算得来的。通俗来说即：查询比特币地址支出和获取的比特币交易记录，那么对这些记录进行运算就可以的到比特币账户的剩余比特币数量。

* + 1. **区块链**

提到比特币账簿就不得不提区块链技术，比特币账簿中的所有交易记录都以区块链这么一种数据结构进行存储，而区块链又是一个一个的区块连接起来的，你可以把它想象成一个环环相扣的锁链。每一个区块里面都包含着整个比特币网络约十分钟内的交易记录。这是因为打包计算的个区块的信息，将近要花费全部网络将近十分钟的算力。

对每个区块头的信息进行SHA256摘要，可以得到一个Hash值。这个Hash值就对应着区块链中的区块。每一个区块都会保存上一个区块的Hash值，一直追溯到创世区块（中本聪创造的第一个区块）。区块链结构如下所示：

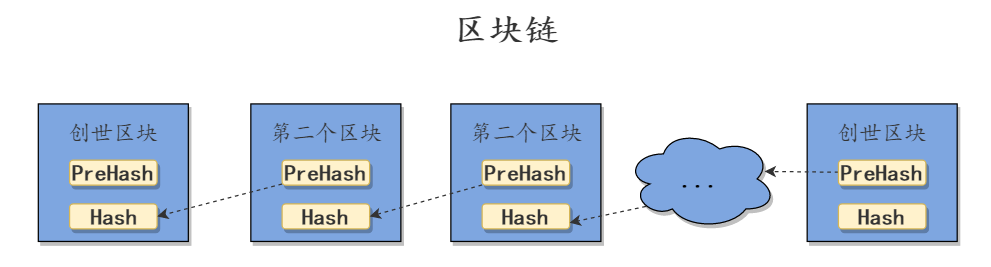


图2.2 区块链结构

从上面的区块链结构中看出，每一个区块包含有上一个区块的Hash，而当前区块的Hash的计算又依赖者上一个区块的Hash。也就是说，如果当前区块信息发生改变，就会导致所有它之后的区块都会相应的改变，一旦某区块之后有很多区块后，这种瀑布效应将会保证区块的信息不可变，因为如果要修改某一区块信息，则必须重新计算当前区块和其之后所有区块的信息，而上面提到，每一个区块的计算要耗尽全网络将近十分钟的算力。因此，要想更改区块的信息需要极大的算力，是一件不可能完成的事情。所以一个长区块链的存在可以让区块链的历史不可改变，这也是比特币安全性的一个关键特征。

* + 1. **创世区块**

区块链中的第一个区块创建时间为2009年，称为创世区块。它是区块链里面所有区块的共同祖先，这意味着你从任一区块，循链向后回溯，最终都将到达创世区块。创世区块中隐藏着一条信息“The Times 03/Jan/2009 Chancellor on brink of second bailout forbanks.”。消息由比特币的创立者中本聪嵌入创世区块中。这句话是泰晤士报当天的头版文章标题，引用这句话，既是对该区块产生时间的说明，也可视为半开玩笑地提醒人们一个独立的货币制度的重要性，同时告诉人们随着比特币的发展，一场前所未有的世界性货币革命将要发生。

* 1. **比特币挖矿**
     1. **简介**

上面已经介绍了比特币的交易以及比特币账簿，上面提到比特币是一个去中心化的网络，即没有“中央”服务器或者控制点。也就是说比特币账簿的记账权不在某个中心机构身上，而在所有参与者手中。但是并不是参与比特币网络的任何人都有比特币的记账权，因为比特币网络的价值“比特币”就包含在这些账簿的记录中，比特币的记账权分配将决定这比特币系统的安全性。那么就涉及到比特币的挖矿了。

挖矿是使得比特币与众不同的发明，他实现了去中心化的机制。挖矿即参与比特币记账权竞争的所有参与者中，要比赛解决一道数学难题，谁先得到这道题的正确答案谁就有比特币的记账权，那么他需要将比特币网络中未被打包的交易记录进行打包成一个区块，并挂载到总的区块链（总账簿）上面，同时他将有机会向区块中写入一条交易记录，即给自己一定数量的比特币作为奖励。等到打包的区块被其他参与者确认后，拥有者就可以使用他写入区块中的那笔交易中的比特币了。因此新比特币的生成过程被称为挖矿。而参与挖矿的参与者被称为矿工，由于比特币交易中会付出一部分的交易费。因此矿工不但可以获取创建的新币的奖励还可以获取到他所打包的所有交易中包含的交易费。

* + 1. **比特币总量**

按照挖矿的奖励机制，可以知道随时间的进行，比特币的数量将会越来越多，最终将会有无限多个比特币被创造出来，然而实际情况却并不是如此。比特币的数量上限约为2,100万比特币。这是因为初始的比特币奖励为50枚，之后每四年奖励的比特币将会减半。比如在2012年时比特币奖励为25枚，2016年的时候变为12.5枚，预计将会在2020年变为6.25枚。

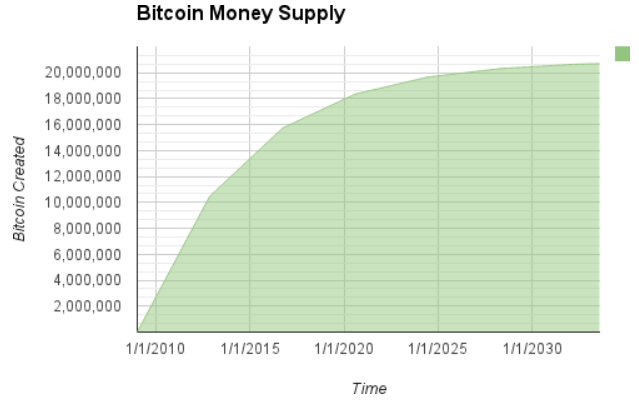


图2.3 比特币总量变化趋势（摘自精通比特币第二版图10-1）

从上图中可以看到，比特币最终总量将会接近2100万，预计将在2140年左右会存在这么多的比特币。在那之后，新的区块不再包含比特币奖励，矿工的收益全部来自交易费。

* + 1. **工作量证明机制**

上面提到矿工门要想获得比特币网络的记账权，就需要去解答一个数学难题，而这个数学难题有一个特点就是会衡量当前整个网络的算力，保证全网络的参与者算出这个数学难题的时间在10分钟左右，这个数学难题就是工作量证明机制。

工作量证明机制使用Hash函数来进行，Hash函数输入一个任意长度的数据会输出一个长度固定的值，对于相同输入会有相同输出，但是如果输入只是存在细微的不同，例如多了一个标点，少了一个字母，或者多了一个数字其输出结果就会截然不同。因此Hash的结果将是不可预测的，也就是说，凭空设想一个输入来获取到一个想要的Hash值是不可能的。而工作量证明机制就是找到特定的组合使得这个组合Hash后的结果小于某个值。即过程如下：

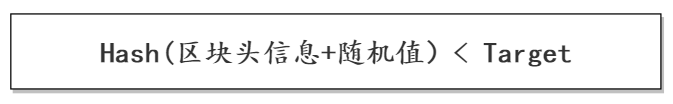


图2.4 工作量证明机制公式

最终的目的就是要找到这么一个随机值使得上面的式子成立。可以看到Target越小，找到这么一个随机值将会越难，这也就可以做到动态调整公式求解的难度了。另一方面，如果某个矿工找到了一个随机值使得上面的式子成立，那么其他矿工去验证是非常简单的，他们之后对输入进行Hash就可以和结果进行比对。

* 1. **比特币运行原理总结**

经过上面的介绍，基本上已经将比特币系统中的关键性的组成部分介绍完毕，当然比特币的系统中还有许许多多的细节部分支撑着比特币系统安全有序的进行，例如比特币系统中的区块链的分叉择长原则，挖矿难度调整细节等等。另外还有随着比特币发展而出现的一些新的技术，如矿池。由于本文的目的并不是完整再现比特币系统，而是从比特币运行的宏观方面模拟比特币运行比特币的原理。同时也为避免比特币知识占据本文的绝大部分篇幅，因此只选择了能快速理解和搭建比特币系统的关键性知识。

总结来说，比特币作为去中心化的对等共识网络，其特有的账号系统确保了其隐私性，另外公共账单即区块链技术和工作量证明机制保证了比特币的安全性以及公开性。使得虚拟货币能够在这几年飞速发展，总结比特币运行原理如下：

比特币参与者是比特币网络的参与者所创建的比特币账号。

首先：比特币网络参与者通过比特币软件随机生成的秘钥生成一个比特币地址。（当然这个秘钥是他要一定记住的）

之后：拥有账号的参与者就可以使用这个账号与其他账号进行交易，账号之间的每一笔交易都会被比特币网络进行缓存（这些创建的交易还没有被矿工打包）。

与此同时：全世界参与比特币网络的矿工会对这些没有打包的交易记录整理并去争分夺秒求解一个数学难题，即找到上面提到的随机值。这个数学难题被解答出来的时间约为10分钟。一旦某个矿工解答出了这个数学题，它便将打包好的区块向网络中传播，等到被其他节点的参与者确认后，这个区块就会被永久的链接入比特币系统总的账簿中去。同时工作量证明机制和区块链结构将会保证这个区块不会被恶意更改。

最后：拥有记账权的矿工可以为自己写一笔交易，给予自己一定数量的比特币作为奖励。即向自己的地址写入一定数量的比特币。之后就可以使用自己获取的比特币了。

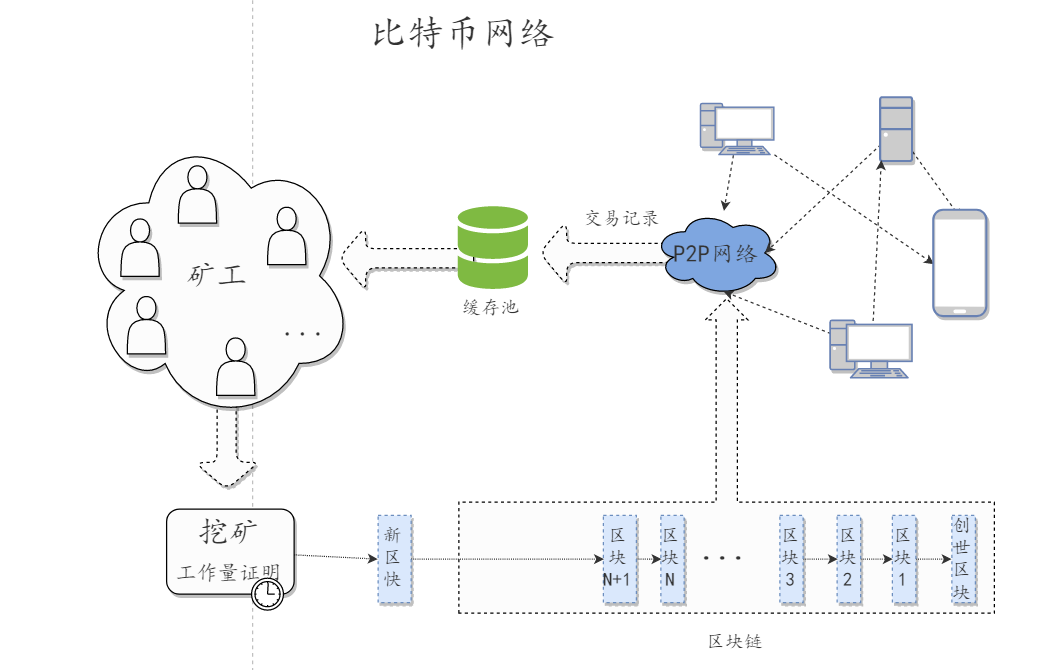


图2.5 比特币网络运行概览

1. 比特币模拟系统设计概要
2. 系统实现
3. 总结