江西财经大学
JIANGXI UNIVERSITY OF FINANCE & ECONOMICS

学校代码_____

密　　级_____

中图分类号_____

UDC_____

# 硕士学位论文
# MASTER DISSERTATION

论文题目（中文）：加密货币币价决定与挖矿行为的探索性研究——以比特币为例

论文题目（英文）：An exploratory study on the determination of currency Price and Mining behavior of Cryptocurrency——A case study of Bitcoin

作　　者：楼尧　　导　　师：喻国平　教授

申请学位：硕　士　　培养单位：经济学院

学科专业：西方经济学硕士　　研究方向：国际金融

二〇一九年六月

# 独创性声明

本人声明所呈交的论文是我个人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写的研究成果，也不包含为获得江西财经大学或其他教育机构的学位或证书所使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

签名：[illegible] 日期：2019年5月5日

# 关于论文使用授权的说明

本人完全了解江西财经大学有关保留、使用学位论文的规定，即：学校有权保留送交论文的复印件，允许论文被查阅和借阅；学校可以公布论文的全部或部分内容，可以采用影印、缩印或其他复制手段保存论文。

（保密的论文在解密后遵守此规定）

签名：[illegible] 导师签名：[illegible] 日期：2019年5月5日

# 目 录

# Contents

# 摘　要

基于区块链技术的加密货币从诞生以来不断吸引着学界特别是经济学学者的关注，比特币代表的加密货币拥有去中心化的运行模式、更快更广泛的流动性以及稳定可控的发行量，一度被当做是未来全球货币的进化方向。然而这一新兴的货币类型也面临着诟病，譬如高能耗的挖矿、币值不稳定、交易流量受限、51%算力攻击风险、监管缺位等问题。区块链技术目前还在不断发展和变化，网络科技与金融的结合受到各界瞩目并吸引投资的同诞生了很多不确定性，譬如比特币可以跨越传统资管渠道，又比如比特币常用作暗网交易。去中心化的比特币系统在互联网分散式的土壤下迅速萌芽发育。然而在商业设施配套和监管法规制定方面怎么跟随和管控这场所谓的货币革命是所有国家面临的难题。

介于种种原因，世界各国各地区对比特币在传统经济和国际贸易上的利弊影响存在很大分歧。2017 年 9 月 4 日，中国人民银行等七部委联合下发《关于防范代币发行融资风险的公告》，所有国内数字货币交易所和大型矿商被关停或被迫出海。一定程度上是因为比特币固有的风险性和其对现存金融秩序的破坏性影响，虽然加密货币的交易和挖矿在中国暂时被禁，然而并不妨碍对比特币及其相关技术的继续研究，所谓“知己知彼，百战不殆”。面临比特币代表的加密货币对传统经济的挑战，投资者和监管者将何以处之？比特币到底是未来货币的进化方向，又或是一种仅存在于网络中的虚拟资产？其价格受何影响而大起大落？笔者将带着这些问题展开研究。

本文聚焦讨论以比特币为代表的加密货币币价的影响因子以及矿商挖矿行为和币价间的内在联系，并试图找到比特币矿商行为和币价剧烈波动间的因果证据。根据以比特币为代表的加密货币的系统运行，本文首先使用经济学的经典分析方法，在比特币市场供求范畴和矿商行为范畴分别分析归纳出若干比特币价格的影响因素。其中，比特币市场供求范畴分析指的是，对以比特币为代表的加密货币使用凯恩斯的流动性偏好理论构建出比特币价格的数学模型；矿商行为范畴分析指的是，在垄断竞争性均衡假设下，用规模报酬不变的科布-道格拉斯生产函数构建出矿商行为的数学模型；而后结合二者推导出比特币价格的综合决定模型进行定性分析。其次，本文抛开传统经济学理论，依据比特币运行机制，单独分析比特币系统内价格和算力间的相互影响，并推导出刻画系统内部的比特币价格——算力模型。最后，在实证部分结合数据，先通过 OLS 最小二乘法对比特币价格综合决定模型进行回归估计，再利用时间序列 VAR 模型的脉冲响应分析比特币价格——算力模型。实证发现比特币币价综合决定模型的各项主要估计系数显

著，币价受到短期投机资本和矿工算力等影响波动较大，模型基本成立；VAR 脉冲响应的结果显示比特币价格和算力图形为发散状，比特币系统存在天生的内在不稳定性。实证研究结果与近几年现实情况中比特币价格的大起大落相吻合，归根结底是比特币在设计上的缺陷所造成的。

本文得出结论：一方面比特币价格容易受到短期资本涌入和能源价格等外在市场性因素影响，另一方面比特币价格还受到比特币算力和交易量等内在因素影响。比特币价格偏离平稳状态，促使比特币丧失储存价值手段，因此正如一部分学者的论述，比特币目前不具备替代主权货币的条件，仅是一种风险较大的虚拟资产。基于以上分析论证，本文针对以比特币为例的加密货币系统的内在问题，提出在社区自治的范畴下，为比特币系统引进一种负反馈机制，降低因矿商行为造成的币价波动；针对外在市场性因素造成的波动，本文提出以各大主要经济体为主体的联合共治策略，从而降低因比特币交易导致对经济的负面影响。以期达到将比特币这头技术的野兽关进牢笼，在有计划的利用加密货币的同时最大化避免其对经济运行带来的不确定性。

**关键词**：比特币；区块链；加密货币；风险；货币

# Abstract

The encryption currency based on block-chain technology has attracted the attention of the academic circle, especially the economist, since its birth, which has a central operating mode and faster and more extensive liquidity, and a stable and controllable rate of inflation. Once used as the direction of evolution of the future global currency. However, such emerging currency types are also faced with such problems as high energy consumption, unstable currency, limited transaction flow, risk of double-flower attacks, and lack of legal regulation. In that meantime, the block chain technology is also in the constant change. Digital currency, block chain, encryption technology. These nouns with high-tech concepts have subverted the original financial order and attracted people's eyes and investments. The central character of the Internet itself provides the soil for the development of the Bitcoin distributed general ledger system. But how the so-called currency revolution follows, how to regulate, is the problem of all countries. Non-regulation, financial fraud, various P2P, crowdfunding schemes, online social communication and advisory promotion activities make it difficult for investors to be damaged by real and false. More lawbreakers use the digital currency to central and anonymous, such as extortion, money-laundering, tax evasion, illegal trade, and the like, and disrupt the whole country's financial order. The digital currency is facing a technical risk, a risk of payment and a risk of investment. The funds of the investor in the trading platform, such as the fresh meat on the chopping block, can be damaged by the trade-platform operator and the employee's own morality, and may also be attacked by the hacker and the loss is harmed by the transfer. More people use the block chain to make all kinds of tokens, that is, the ICO is facing the public sell-off, which is so easy to reach several times of the income, with high-tech banner, become the barbarous game of the barbaric growth, which seriously affects the health and orderly operation of the financial market. For the above reasons, the influence of Bitcoin on the traditional economy and international trade in various regions of the world is very different. The current Bitcoin transaction is prohibited in China. On September 4,2017, seven ministries and other ministries, such as the People's Bank of China, issued the Announcement on Prevention of the Risk of the Issue of the Token, and the domestic digital currency exchange was ordered to shut down. This is partly because of the risk of bitcoin and its devastating impact on the inherent financial order, but this does not

prevent continued research on bitcoin and its technology, so-called "If you know each other, you can't do it.".

This paper focuses on the influencing factors of the currency value of the encrypted currency represented by bitcoin and the internal relationship between the mining behavior and the currency value, and tries to find out the evidence of the influence of the bitcoin miners' behavior on the currency price fluctuation. According to the operation mechanism of encrypted currency represented by bitcoin, this paper first speculates some influential factors related to the fluctuation of currency price. Then through the classical economic analysis methods in the category of supply and demand of Bitcoin market, the paper analyzes the liquidity preference theory of the encrypted currency represented by Bitcoin, and constructs the mathematical model of Bitcoin price. At the same time, in the field of Bitcoin mining, using the traditional microeconomic theory, under the assumption of complete competition equilibrium in the field of Bitcoin mining, the mathematical model of miner is constructed. In the empirical part, the OLS least square method is used to analyze the currency model and the miner model respectively, and then the impulse response of the time series VAR model is used to analyze the intrinsic interaction between the behavior of the miner and the price of the currency. The empirical results show that the estimation coefficients of the Bitcoin currency model and the miners' behavior model are significant, and the currency price is affected by the short-term speculative capital, and the model is basically valid. The results of VAR pulse response show that the price and computing power of bitcoin are divergent, and there is inherent instability in bitcoin system. The results of empirical research are consistent with the rise and fall of bitcoin price in recent years, which is also caused by the design defects of Bitcoin.

Finally, this paper draws a conclusion: on the one hand, bitcoin price is easily influenced by external market factors such as short-term capital influx, on the other hand, bitcoin price is also influenced by internal factors such as bitcoin calculation power. The price of Bitcoin deviates from the stationary state, but also causes Bitcoin to lose its storage value, so, as some scholars have argued, Bitcoin can not exist as a real currency, it is only a risky investment product. Based on the above analysis and demonstration, this paper proposes to introduce a negative feedback mechanism for the bitcoin system under the category of community autonomy, aiming at the inherent problems of the encrypted currency system taking Bitcoin as an example. Reduce the sharp fluctuation of the currency caused by the behavior of the miners; In view of the

fluctuations caused by external market factors, this paper proposes a joint governance strategy with major economies as the main body, so as to reduce the negative impact on the economy caused by bitcoin trading. The goal is to put the beast of Bitcoin in jail, maximizing its planned use of encrypted currency while avoiding uncertainty about economic performance.

**Keywords:**Bitcoin; block chain; Cryptocurrency; risk; currency

# 第 1 章 绪论

## 1.1 研究背景和研究意义

### 1.1.1 研究背景

美国 2018 年发生的次贷危机对全球经济运行造成了沉重打击。对固有金融体系的不满促使化名中本聪（Satoshi Nakamoto）的学者开始寻找一种解决中心化机构主导导致的信息不对称问题的方法。加密货币世界始于一篇名为《比特币：一种点对点的电子现金系统》的论文，这篇被它的作者中本聪创作于 2008 年的论文起初只发表于一个不起眼的网络论坛上。而随着比特币的影响不断扩大，这篇论文被后来的研究者奉为《比特币白皮书》。比特币区块链系统的第一个区块也是中本聪在 2009 年 1 月于芬兰赫尔辛基的一个私人服务器上挖掘出来的。这个区块被称为创世区块，是唯一没有任何交易信息的区块，其中只包含了一段文字“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.（财政大臣处于第二次银行援助的边缘）”这是当天英国《泰晤士报》的头版标题，被看做是中本聪对现有货币体系的一种嘲讽。

比特币是一种集合了加密计算、共识机制、点对点传输、分布式数据存储等已有计算机网络技术的去中心化加密货币，在此基础上利用工作量证明（Pow）完美克服了去中心化系统存在的拜占庭问题。比特币出现后，区块链技术作为比特币的底层技术才被广泛定义。可以说区块链技术脱胎于比特币，而在比特币市场甚至全球加密货币市场近来遭遇挫折的同时，区块链技术依然是各大研究机构热衷讨论的对象。其应用不断扩大，从最初只用于加密货币的运行，到后来的物联网、社交通讯、文件存储、供应链金融、电子商务、物流跟踪、身份验证、证券交易、股权众筹、智能合约等多个领域。

比特币出现后的市场表现证明其本身也存在很多缺陷，最主要的是，比特币价值波动剧烈。其经历了价格的平稳上升期、爆发期和下跌期，2017 年 6 月以前比特币价格都在 2500 美元以下平稳上升，2017 年 6 月以后出现爆发式增长，同年 12 月达到 19000 美元的顶点，总市值达 3270 亿美元，但在而后短短半年时间下跌到单价不足 7000 美元，总市值市值不足 1000 亿美元，跌幅近 70%（比特币有稳定发行量，数量在短时间内基本保持不变）。近半年来比特币单价维持在 6000 美元左右，但波动方差依然高于 2017 年 6 月之前。

其他缺陷也使得研究者对比特币持有谨慎态度，譬如比特币交易流量受限，一笔交易通常需要十分钟以上的验证时间；比特币钱包存在安全漏洞，频发钱包被盗事件；比特币工作量证明（Pow）挖矿方式产生巨大的能源浪费，其一年耗

电量相当于葡萄牙全国用电量，且截止本文发稿还在不断上涨中；比特币分布式总账始终面临着51%算力攻击的风险；比特币存在大量涉及毒品军火等违禁品的暗网交易；比特币同时还可以绕过传统资金监管实现快速的资本跨国流动，成为国家金融安全的隐患。基于以上种种原因，比特币交易在一些国家被禁止或限制，而在不受限制的地区，关于比特币的法律监管也多是一片空白。

### 1.1.2 研究意义

自2008年中本聪提出的一种去中心化的密码学货币——比特币（Bitcoin）诞生以来，作为其底层技术的区块链技术逐渐被各行各业引入。包含匿名性、自治性、开放性、去中心化、信息不可篡改等特点的区块链技术本质上是一种存在于网络各个节点的分布式总账，通过协议相互验证保证账本的一致性，并用工作量证明（Pow）来抵御篡改账本的攻击。比特币能否作为货币存在的问题一度困扰着研究者，支持者认为比特币具有交易媒介、储藏价值和记账单位等货币属性，更重要的是，比特币具有稳定的发行量和可靠的信用，因此可以看做是一种货币；反对者认为比特币缺乏监管，价格波动剧烈，且交易流量受限，因此不适用于作为一种普遍使用的货币。在笔者看来，比特币虽然名为货币，但非真正的货币，其应用场景多作为投资品交易而不是商品购买，在本文下面的论述中，比特币还存在着巨大风险，不适用于作为一种国际广泛使用的货币。

本文通过归纳分析比特币的运行原理和产业现状来深度剖析其风险存在的根本原因，对在金融领域防控比特币带来的风险有参考作用。本文还通过对比国外法规为我国监管制度的制定提供借鉴思路，并通过分析比特币的内在风险成因为比特币的风险监控提供参考。文章最后还通过OLS回归估计和VAR模型脉冲响应分析等计量经济学方法对比特币系统内部稳定性影响因素和币价综合决定因素进行深度剖析，并得出结论：比特币市场受短期资本流动和国际能源波动等因素影响显著，比特币价格和算力存在双向放大影响。文末结论给比特币市场的国际监管提供了参考，为比特币社区自治提供了改进建议，具有较大的理论意义和实际意义。

## 1.2 国内外文献综述

一直以来，经济活动中都需要一个中心化的组织者，集中处理各种交易或是监管领域内的违规行为。尤其对于涉及互联网的交易几乎都需要借助金融机构作为可信赖的中间人来处理电子转账信息（中本聪，2008）。而2008年次贷危机爆发给人们以警示，中心化的金融机构始终不可避免委托代理问题。比特币主要

使用没有任何中间方、点对点、可追溯但难以篡改的技术，实现一个高度可信的数据库总账（姜立文和胡玥，2013），以比特币为代表的加密货币体系被认为是网络支付去中心化的有益尝试。当前部分学者认为区块链技术可以在货币虚拟化、数字资产、支付与结算等金融领域产生创新性的应用前景（鲜京宸，2016 ；任安军，2016）。比特币恰恰满足了人们的需要——它基于网络协议而不是基于信用，使得达成一致的任何人能够快速交易，并且避免金融中介过度获取交易方信息，侵犯用户隐私（中本聪，2008）。

作为一项新兴的网络技术集成，比特币处于不断异变的过程中，一些研究者正从不同需求出发，作出更多创新来深化比特币的应用。Gregory Maxwell（2013）[①]对比特币提出一种加强隐私保护的技术升级，使得交易者能够对大众隐藏其转账数额，进一步强化了加密货币对隐私的保护。Ittay Eyal 和 Adem Efe Gencer 等人（2013）[②]提出使用一种新的挖矿协议，将传统区块分为含工作证明的首领块和不含工作证明的微区块，交易账本可以在任何区块中更新而矿工只需付出首领区块的挖掘算力，有效解决比特币吞吐和延迟问题。类似的还有 Joseph Poon 和 Thaddeus Dryja（2015）[③]，他们的方案是开发一条平行于比特币主链的副链，大量的交易只存储于副链，一段时间内副链的交易在计算和压缩后向主链转移，这种被称为比特币闪电网络的方案显著降低了比特币的交易成本，尤其是小额交易。在挖矿优化上，随着哈希（hash）值长度不断增加，一种基于多核 CPU 多线程设备的挖矿比传统 PC 挖矿有更高效率（张嘉洺，2015）[④]。

另一些研究者从比特币对传统经济的作用出发，讨论了比特币存在的意义。Robert Viglione 通过统计学的方式，证明经济自由度与比特币溢价的反比关系，使比特币价格指数成为指导宏观经济政策的一项参考（Robert Viglione，2015）。Charles W Evans 认为比特币流通形式和传统伊斯兰教义之间存在很大重叠，穆斯林世界的银行可以将这种加密货币列入业务范围，考虑到穆斯林人群占全球人口的四分之一，这篇论文迅速获得了来自穆斯林世界的惊人关注量（Charles W Evans，2015）。国际清算银行结算委员把比特币的分布式账本技术看做是一种“电子货币方案中切实的创新元素”，这类分布式账本相对于传统中心化的管理方式，能够显著降低终端用户的交易成本（Digital Currencies,Bank for International Settlement,2015）。Winston moore 和 Jeremy Stephen（2016）认为对于一些市场经济体量较小的国家，在储备货币中持有一些比特币能够在提升收益的同时降低

① Gregory Maxwell,Confidential Transactions[OL].https://bitcointalk.org/index.php.2013

② Ittay Eyal、Adem Efe Gencer, Bitcoin-NG: A Scalable Blockchain Protocol[J].Networked Systems Design and Implementation.2016(5)21~38

③ Joseph Poon、Thaddeus Dryja,The Bitcoin Lightning Network:Scalable Off-Chain Instant Payments[OL].2016

④ 张嘉洺,电子货币系统研究及比特币挖矿优化[D].长春：吉林大学，2015

投机损失，并且不会显著影响准备金价值波动，这篇文章还提到，新兴的比特币也许能成为全球央行储备货币。

针对比特币价格影响因素的研究如下。Halvor Aarhus Aalborga, Peter Molnára 和 Jon Erik de Vries（2018）发现异质自回归模型适用于比特币价格预测，同时从谷歌系统的“比特币”搜索量数据能够预估比特币的交易量。Michal Polasik 以及 Anna Iwona Piotrowska 等人同样指出比特币价格表现和相关话题的媒体热度呈正比，他们同时指出比特币在电子商务支付场景上有很广阔的前景。Ladislav Kristoufek（2015）的工作涉及面则更广，他从传统金融资产运行、比特币的技术特征和大众关注度等多角度对比特币价格进行小波相干分析，发现比特币在长期内拥有传统金资产的属性，在短期内更多受到大众关注的影响。Pavel Ciaiana 和 Miroslava Rajcaniova（2015）等人则使用 Barro（1975）提出的货币分析模型，从传统市场力量和比特币对投资者短期吸引力两个方面分析币价构成因素，结论显示传统市场力量和投资者短期行为一样显著推高比特币价格。Dirk G. Bau 和 Thomas Dimpflb（2018）通过基于 GARCH 模型的实证分析，对比了比特币与黄金和美元的收益率波动参数，发现比特币既不像美元也不类似黄金，具有全新的收益率特性和波动特性。本文对比特币价格的分析部分继承了学术界惯用的路线，在比特币的货币属性基础上分析币价的决定因素，与此同时创新性地结合了矿商行为的影响因素。

关于比特币是否会成为未来应用的基本形式一直是学术界的一个讨论焦点，比特币是货币还是准货币，或是一种极度类似货币的电化子资产，当前仍然没有一个确切答案。李文杰（2013）认为，随着网络社会高速变化，传统主权货币必必然会被数字加密货币所取代，实物货币体系将被彻底打破。郑晓彤等人（2012）预计比特币代表的加密货币在网络环境下会变成下一个和黄金有着类似作用的新货币形态。Mendelson 等人（2014）认为在当前加密货币与金融的关系下，加密货币需要渐进式地展示其自身价值才被更多人接受，另外传统货币被取代不过是时间问题。Woo 等人（2013）也对加密货币的内在价值进行了深入探究，并对其日后发展持有乐观看法；与此同时，他们也强调，市场过度投机会造成加密货币价格剧烈波动，从而降低大众对其接受程度。张苑（2016）将区块链技术看作继大型计算机、个人电脑、互联网、社交网络和移动终端之后的第五次颠覆性新计算范式，尤其在金融领域，区块链将颠覆现存中心化的融资方式，使具有更高效率、更低成本、更快速的去中心化融资成为可能。王毛路和陆静怡（2016）认为区块链因其分布式、透明性、可追溯性和公开性等特征，在政府政务公开和政务电子化中有广阔的应用前景。周光友和王燕（2014）以货币五大属性为出发点，分析比特币的是否属于货币，并得出结论，比特币具有货币五大属性，但是由于

其发行总量和速度固定、技术方面还有待进一步完善，因此在与传统中心化货币的竞争中比特币代表的加密货币难以胜出。

与此相对地，另一些研究者对比特币持有消极看法。Yermack（2013）的研究表明，第一，特币的汇率轨迹与其他主要货币汇率轨迹缺乏关联性使得比特币不能应用于风险管理。第二，比特币用户也很难对比特币持有头寸进行套期保值。第三，比特币不能给消费信贷或其他贷款协议计价从而难以被银行体系纳入业务范围。因此，比特币属于货币，应将其看做是一种投机工具。Jacobs（2011）和 Grinberg（2012）对比特币涉及的法律问题进行了剖析，认为比特币在各国的使用都面临较大的法律风险。刘延莉和赵世明(2014)认为，比特币的信用和安全性得不到保证，不具备排他性且易引发通货紧缩问题。陈道富(2014) 认为，当比特币发挥货币职能时，存在交易平台不稳定、缺乏货币锚以及法律地位不明确等风险。孟鑫(2014)指出，比特币等加密货币是促进国际货币体系完善和扩展投融资渠道的有意尝试，但比特币不具备排他性和唯一性，且由于供应量有限，比特币难以成为国际普遍接受的流通货币，比特币不会是货币发展的最终形式。谭淞（2014）认为比特币的有点被过度发放大，其投机性过大而价值波动剧烈，在用于资产配置上难以与美元和黄金抗衡，作为小范围内的支付工具也许是比特币最乐观的应用前景。

关于比特币存在的泡沫和金融风险问题，一些学者提出了他们的看法。邓伟（2017）早在比特币泡沫破裂前的 2017 年 3 月就使用 sup ADF 检验和正态分布检验等多种统计学方法对比特币价格进行考察，得出比特币存在大量泡沫的结论，并把投机兴盛和监管缺乏作为泡沫存在的原因。经济学家任泽平（2017）通过分析比特币市场交易者构成，同样得出比特币存在投机造成的泡沫的相似结论。但他同时提出，比特币的风险来自于其不完备的运行机制，这与本文的立场不谋而合。Shaen Corbeta 和 Brian Lucey 等人（2018）研究了比特币和其他两种加密货币的价格走势，发现在 2017 年的比特币存在明显的泡沫。Ross C. Phillips 和 Denise Gorse（2018）也通过对 2017 年比特币泡沫时期的币价表现进行研究，发现币价的波动和网络关注度有极大相关性，而在非泡沫时期这种关联性不那么明显。

## 1.3 研究思路与文章结构

### 1.3.1 研究思路

近几年以比特币为代表的加密货币交易火爆的同时币价波动剧烈，累积大量风险且给监管造成难题。本文秉持着从理解研究中得到解决方法的思路，通体分

析比特币系统运行的方式，用传统经济学分析方法和基于比特币运行机制的创新型分析方法同时进行考察，最后总结出比特币价格剧烈波动的原因所在，并提出解决办法。本文逻辑路线图如下图 1.1 所示。

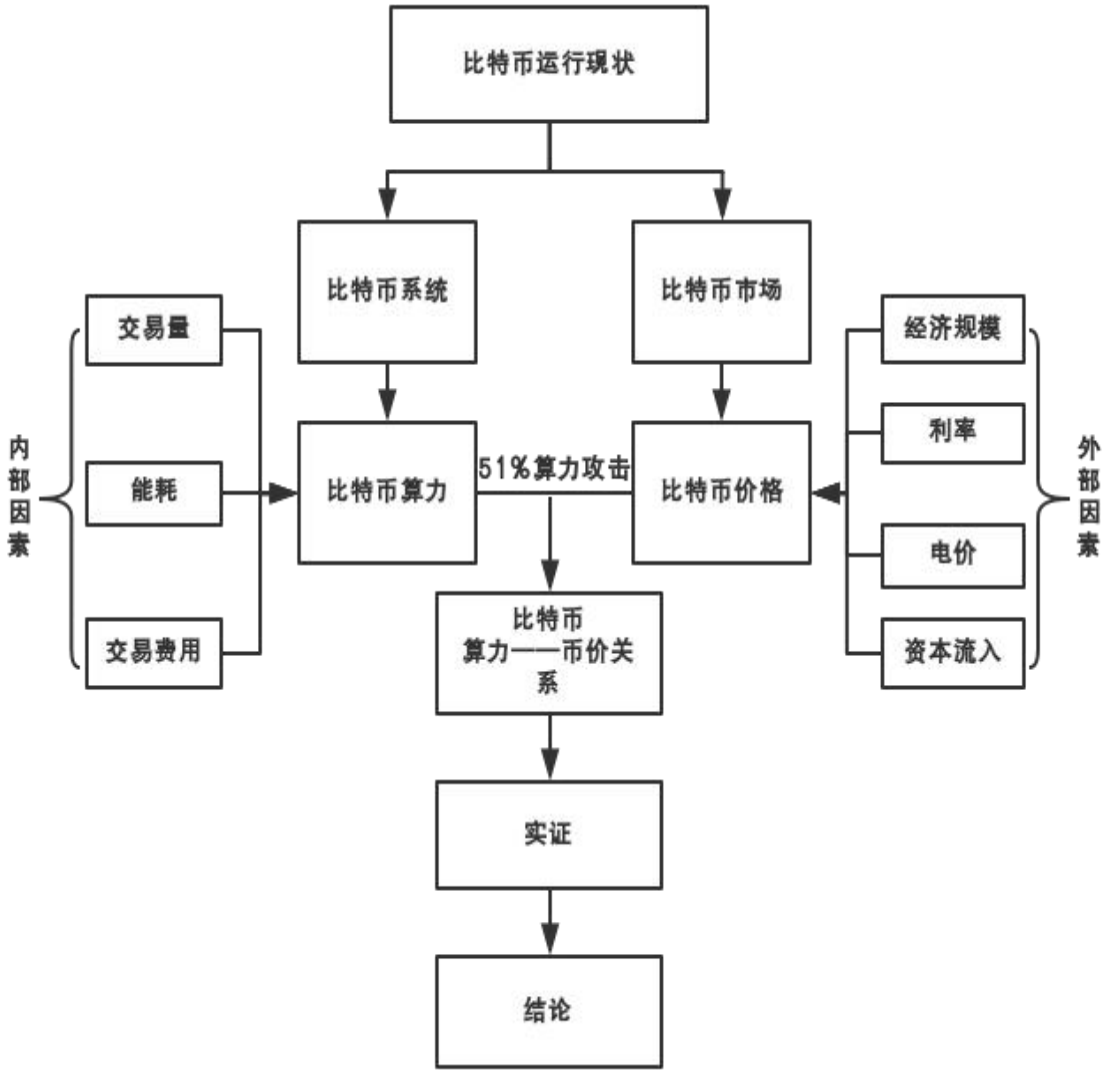


图 1.1 全文逻辑图

先根据比特币运行原理和市场现状，分别从比特币系统中提取内部算力影响因素，从比特币市场提取外部影响因素。再结合比特币面临的“51%算力攻击”风险权衡比特币算力——币价关系。最后使用收集的数据进行实证，验证这种关系并得出结论。

（1）理论分析。在对比特币运行机制详细展示后，本文将运用经济学经典理论分析比特币。用凯恩斯的货币流动性偏好理论为比特币推导出一套短期均衡状态下的币价决定模型；用不完全竞争市场的厂商行为理论，再比特币矿商可以

获得短期超额利润的假设下，推导出比特币挖矿行为模型，再将二者整合，推导出比特币价格的综合决定模型。为了从多方面分析比特币系统，本文最后搁置经济学理论，只基于比特币系统内部传导机制，对比特币价格和算力进行单独的分析。

（2）实证分析。建立数学模型之后还需对其有效性进行检验。本文采集从 2016 年 1 月到 2018 年 12 月的相关变量数据，以周为单位取平均值。第一部分实证使用 OLS 最小二乘法对比特币价格综合决定模型进行回归估计，考察各变量的系数估计值及其显著性；第二部分实证使用时间序列 VAR 模型分析比特币价格——算力双向影响模型，通过单变量稳定性检验、Grange 因果检验和协整性检验，发现被考察变量间存在统计学上的相互影响且序列稳定，VAR 模型成立，最后用脉冲响应分析各个变量受其他变量脉冲扰动后在时间上的反应变化。

### 1.3.2 文章的结构安排

本文对所考察问题研究遵循由内而外，先细节后宏观的撰写顺序，在经济学范畴内深入探究比特币币价和矿商行为间的影响关系。本文先从传统货币供需角度考察比特币价格决定，再从矿商决策角度考察算力与币价的关系，最后用时间序列 VAR 模型做币价与算力间的脉冲响应分析，考察其影响在时间上的变化。安排章节依次为，加密货币发展的现状、介绍作为代表性加密货币比特币的运行原理、比特币价格和矿商行为的经济学分析、结合实际数据的实证探究、提出针对所发现问题的政策建议，最后总结全文，得出结论。以下是具体章节安排。

第一章，绪论。深入介绍文章研究背景和研究现状，总结归纳国内外研究路径，提出比特币为代表的加密货币存在的问题，并阐述本文对加密货币研究领域的主要贡献。

第二章，加密货币发展现状。集中梳理市值排名靠前的几种加密货币，归纳加密货币的种类和作用，追溯加密货币发展的历史，例举加密货币产业，梳理当下加密货币产业的分布和职能，同时收集整理全球关于加密货币的法律法规，展示一幅加密货币的全球法规地图。

第三章，比特币运行原理。使用图文结合的展示方式，深入浅出的介绍比特币系统的运行原理，对加密货币领域的专有名词做出解释，为本文后面的经济学范畴研究找到技术上的抓手，末尾对比特币系统提出待考察的问题。

第四章，比特币的理论分析。使用经济学传统理论对比特币挖矿行为和比特币价格构成进行分析。根据比特币的货币属性，用凯恩斯的货币流动性偏好理论为比特币推导出一套均衡状态下的币价决定模型。用微观经济学不完全竞争市场的厂商行为理论，在比特币矿商可以获得短期超额利润的假设下，借助规模不变

的科布-道格拉斯生产函数推导出比特币矿商贡献算力在均衡情况下的决定模型。末尾跳出传统经济学理论框架，对比特币价格——算力的双向影响进行单独分析。

第五章，实证分析。对第四章推导的比特币价格综合决定模型结合实际数据进行 OLS 回归分析，采用时间序列 VAR 模型对比特币算力和币价进行脉冲响应分析。结果显示各主要变量系数估计值均显著，币价和算力间的脉冲响应呈现发散状，比特币价格和矿商贡献算力之间存在不稳定且随时间扩大的相互影响。

第六章，政策建议和结论。第一部分在比特币特有的社区自治框架下提出针对矿商的一段时间内持币建议，为比特币系统内部的不稳定引入负反馈通道。第二部分是对世界各个主要经济体的联合共治提出建议，有效避免资本利用比特币绕过监管以及比特币通过暗网产生非法交易。最后总结全文得出结论，本文有力证明了比特币存在矿商行为与币价间的不断放大的相互扰动，比特币在设计上有天然的内部不稳定性，这也是造成近年来现象级的币价暴涨又崩溃的原因。交易媒介、记账单位、储存价值被普遍归纳为货币所应具备的特性，币价剧烈波动的比特币显然不具备储存价值，因此本文认为比特币不能被当做一种广泛适用的货币。

## 1.4 本文贡献与不足

### 1.4.1 本文的主要贡献

已有的加密货币相关领域的研究可以分为如下几个方面。（1）从技术层面对加密货币的解释和改良策略。（2）区块链技术在其他已有行业的扩展应用。（3）加密货币对经济活动的影响分析，包括本文涉及的币价影响因素分析。（4）加密货币合法性地位的探究。而对加密货币挖矿活动与币价之间的影响分析在国内学术圈并不多见。本文的贡献主要有以下几点。（1）推导比特币价格决定模型，发现比特币价格受短期流动资本、国际能源价格、综合利率、算力等因素影响较大。（2）进一步分析币价与算力的双向动态影响，发现币价与算力存在双向放大的脉冲响应，比特币系统内部缺少对币价——算力的稳定机制。本文理论结合实证有力论证了所提出的推测，为加密货币的改良策略和法律规范提提供了重要参考。

### 1.4.2 本文的不足

本文的不足主要体现在在以下几个方面。

（1）受到专业知识所限，本文只从经济学角度出发，缺乏法律和计算机网

络技术层面的专业分析角度。因此作出的结论可能在其他相关专业看来还有很多需要补充的地方。

（2）受到数据可获得性限制。鉴于数据的可获得性，本文只截取了从 2016 年 1 月到 2018 年 12 月的相关考察变量的数据，一些变量比如比特币综合能耗指数的统计在 2017 年才开始。控制变量中很多受到长短不一的周期性影响，在本文中没有予以纳入。

（3）受到分析方法的限制。本文使用的是已有且经过长时间考验的经济学理论，而加密货币是一个新型事物，已有的经济学理论对其分析可能存在不适用之处。因此本文属于探索性研究，更加精确和具体的研究要等到相关学科充分发展后才能进行。

# 第 2 章 加密货币发展现状

自中本聪生成创世区块起以比特币为代表的加密货币已经走过了整整十个年头。加密货币世界从最初只有极少人参与的比特币网络，发展成了一个包含各类应用的生机勃勃的生态体系。随着网络参与者的不断增加与币价的不断上升，比特币和其他加密货币逐渐引起各国（地区）监管者的注意，一些国家和地区已经优先针对加密货币制定了法规，为加密货币的国际联管提供了先决条件。理解加密货币特有的生态体系有助于后面我们对比特币币价决定因素的选取工作，下面我们将就比特币代表的加密货币发展的历史及现状作简要介绍。

## 2.1 比特币及其他加密货币

### 2.1.0 比特币

比特币（BTCoin）是最早出现的去中心化加密货币，也是目前市值最大、交易量最大且覆盖面最广的加密货币。在此先对比特币做概括性介绍：比特币系统以区块链为底层技术，通过 P2P 技术构建分布式总账网络；通过计算机加密和网络签名技术保障交易的安全性；通过工作量证明（Pow）[①]解决去中心化网络存在的拜占庭问题。与此同时由于比特币价值波动剧烈，用于商品购买的支付场景少，缺乏规范与监管，又被多数学者排除在货币定义之列。

比特币系统主要特性归结为：匿名性、开放性、自治性、去中心化和信息不可篡改性。其中去中心化指的是不存在一个掌握完全信息和绝对权威的中心化机构作为管理者，一切运行都在相互可信赖的网络环境下进行。开放性是指比特币系统对任何个人和机构都是开放的，使用者可以自行生成一个公钥即账户并持有一个相对应的私钥即启动交易的密码，使用者也可随时访问所有分布式总账中的数据。自治性，区块链采用协商一致的协议，譬如采用同一种哈希 hash 算法和采用同一种新区块验证规则，这套事先设计好的协议使得交易中对使用者相互间的信任需求转化成对网络程序的信任。匿名性指的是，加密货币使用者在交易活动中只需对外展示自己的公钥接受转账并且使用私钥开启交易，公钥和私钥的使用类似银行系统中户头和密码的使用，交易中任何一方不知道对手的真实身份，面对的只是一串字符表示的公钥。信息不可篡改特性源于区块链庞大而分散的分

① 工作量证明（Proof-of-Work，PoW）：是一种对抗服务与资源滥用或是 DOS 攻击的经济策略。其要求参与者进行某些耗时适当的复杂运算，并且答案能被服务器快速验算，以过程中耗费的时间、设备和能源做为担保成本，确保服务与资源是被真正的需求所使用。此一概念最早由 Cynthia Dwork 和 Moni Naor 于 1993 年的学术论文提出。

布式账本体系，记载着最新交易的新区块接入主链时都会附上矿工节点的工作量证明、时间戳和签名，而已经接入主链的原有区块不可篡改且在每个节点间相互验证，除非能够同时控制超过 50%的节点，否则任何攻击者试图篡改已有账本都是徒劳的。

比特币网络也存在着诸多缺陷，一是比特币分布式总账始终面临“51%算力攻击”；二是比特币挖矿使用的工作量证明（Pow）容易造成大量能源浪费；三是比特币系统交易吞吐量受限，交易确认时间过长；四是比特币价格起伏剧烈，极易受外界因素影响产生泡沫，如以下图 2.1，比特币在考察期内以美元计价的币价变化[①]，可见其波动剧烈。


图 2.1 比特币价格（单位：美元）

本文选取能更好的反映币价波动的代表性考察区间，可以看到在比特币在 2017 年 5 月之前属于平稳期，其价格在 2000 美元内波动，波动率较小；在 2017 年 5 到 2017 年 12 月属于飙升期，其价格一路上涨到 18000 美元附近；在 2017 年 12 月时候属于下跌期，其价格震荡下跌，波动率较大。

### 2.1.1 以太坊

根据比特币的运行原理，维塔利克·布特林[②]在向比特币核心开发者提出发展更加完善的编程语言来简化比特币的开发的意见被拒绝后，独自开发了一种交易

① 数据来源 CoinMarketCap 网站

② 维塔利克·布特林（Vitalik Buterin；1994 年 1 月 31 日生），俄罗斯裔加拿大人，电脑工程师，以太坊共同创办人，著有《以太坊白皮书》。

速度更快、智能合约更灵活的新加密货币——以太坊（Ethereum），并在 2013 年写下《以太坊白皮书》，而后在网上向投资者募集开发资金，投资者用比特币向开发者购买以太币，这也是现在 ICO 方式的雏形。对比比特币来看，以太坊允许使用者在区块上加入智能合约——一种条件触发交易的短小程序，用户只要向记账节点支付相应的手续费即可，使得以太坊对使用者来说极具开发性，例如游戏开发者可以利用智能合约让游戏当中的虚拟货币永不消逝且可以变现从而提升可玩性吸引玩家；它计划升级使用的权益证明系统（Pos）[①]，区别于比特币的工作量证明（Pow），更加节省计算机挖矿资源，同时避免矿池中心化；以太坊还计划使用支链挖矿，在较小的支链上运算交易，只将最终账本添加到主链，有效避免了主链交易拥堵。在 2014 年 6 月，以太坊已成为市值第二大的加密货币，它的成功极大地激励了后来的开发者，此后针对区块链的创新如雨后春笋般出现，以致后来的 ICO 体系诞生。

### 2.1.2 莱特币

另一种加密货币是诞生于 2011 年的莱特币（Litecoin）。莱特币模仿了比特币的系统架构，是一种基于分布式账本的电子加密货币，在网络上建立并交易一种开源的加密协议，从而不受任何中央机构的控制。不同的是，莱特币交易确认速度快于比特币，大约每 2.5 分钟（比特币是约每 10 分钟）生成一个区块；莱特币发行总量大于比特币，预计最终生成 8400 万个（比特币是 2100 万个）；莱特币的工作量证明引入 scrypt 加密算法，这种算法简化普通 PC 挖矿过程；莱特币的记账单位小到单位电子货币的 1/100000000,使得它更平滑地与其他币种实现兑换。

### 2.1.3 比特币现金

截止本文完稿，比特币现金是目前市值排名第四的加密货币。比特币现金（BCH）在 2017 年 8 月 1 日诞生于比特币的一个硬分叉，一部分矿工从比特币第 478558 个区块开始脱离主链挖矿，往后挖掘的支链区块开始执行新的代码并启用 8M 的更大区块（截止本文完稿为 32M）。

### 2.1.4 瑞波币

瑞波币（Ripple），用于跨网关在线快速汇款，现已停止挖矿，而由其创造公司 Ripple Labs 向使用者分发，瑞波币是 ripple 系统中唯一可以跨网关提现的通

① 权益证明 Pos（Proof-of-Stake）：权益证明机制的运作方式是，当创造一个新区块时，矿工需要创建一个“币权”交易，要求参与人一定时间内冻结一定数量加密货币的所有权，根据所占全网总冻结数目的比例来获取新发行币。交易会按照预先设定的比例把一些币发送给矿工本身。

用货币，而其他货币只能在本网关内交易。瑞波币目前流通量为 1000 亿个，并且随着交易的增多而逐渐减少。瑞波币现已脱离去中心化的加密货币行列。

### 2.1.5 EOS 币

EOS 代币又称柚子币，是由 Blockone 公司开发的全新的区块链架构，其分布式应用性能更加广泛。EOS 通过并行链和 DPos（股权授权证明共识机制）的方式部分解决了延迟和数据吞吐量的难题，使其每秒可以记录数百万个交易。

按照市值排名的六种主要加密货币基本信息如下表 2.1 所示。

表格 2.1 主要加密货币

| 币种（代码） | 诞生年份 | 挖矿证明 | 截止 2018 年 10 月市值（单位：亿美元） | 区块产生速度 |
|---|---|---|---|---|
| 比特币（BTC） | 2009 | Pow | 108764.936 | 10min |
| 以太坊(ETH) | 2014 | Pow、Pos | 20660.463 | 15s |
| 瑞波币(XRP) | 2013 | 无 | 16499.502 | 无 |
| 比特币现金（BCC） | 2017 | Pow | 7853.030 | 10min |
| 莱特币(LTC) | 2011 | Pow | 3056.790 | 205min |
| 柚子币（EOS） | 2017 | DPos | 51.471 | 3s |

数据来源：笔者整理所得

## 2.2 比特币相关产业

### 2.2.1 比特币钱包

比特币系统中给予用户一对来自非对称加密算法的公钥和私钥，其作用好比账户和密码，公钥经过一些转换就成为了 27~34 位的地址。而比特币钱包可以用于保管同一使用者的多对公钥和私钥。最基础的比特币钱包客户端程序 BitcoinQT（通常被称为 " 官方客户端 " 由比特币基金会开发）其中就包含钱包管理的功能，可在用户指令下自动生成新的公钥和私钥。BitcoinQT 的使用需要先下载当前完整的区块链账本到本地（目前大小已超过 50G），其包含了从创世区块到现在的所有数据。这对普通用户来说其实用处不大，由此诞生了轻量化本地数据的各种网络移动钱包。最流行的轻量级应用是 MultiBit，它是比特币官方主页 bitcoin.org 上推荐使用的应用。使用 MultiBit 只需要几分钟的数据同步时间就可开始使用，对于普通用户是一个更好的选择。

在线钱包服务让使用者可以在任何有网络的地方参与比特币交易，且无需花费太多时间对钱包文件（保存所有地址与私钥）进行管理，而只要像使用其他网络程序一样记住自己的帐户名和登陆密码即可。由于比特币的开放性账本，所有钱包之间都是相互兼容的，用户只需经过简单的步骤就可以在不同钱包中迁移或者同时使用自己的公钥与私钥。总体来说，这些不同的钱包可以归为两类，一类是完全基于比特币网络的，比如 Bitcion－QT 和 Bitcoin Wallet，另一类则是需要依赖某些中间数据提供商，如 blockchain.info。选择何种类型的服务，要看用户如何在便利性和可靠性中做出权衡。

### 2.2.2 比特币交易所

2017 年比特币价格的暴涨吸引了全球的注意力，而交易所是比特币价格变化的源头。鉴于目前比特币用于购买的场景还相当有限，收到比特币转账的人通常需要将其兑换成法币使用，与此同时一些想持有比特币但却不想挖矿的人则希望用法币来购买比特币，交易所便应运而生。

成立于 2017 年 7 月 17 日的 Mt.Gox 总部坐落在东京，其一度是世界上最大的比特币交易所，当时比持币的单价还不到 5 美分。而由于创立较早，Mt.Gox 积累了大量用户，每日交易量一度占全球比特币交易的 80%以上，是交易所中当之无愧的巨头。在相当长一段时间里，Mt.Gox 的举牌价格都被当做比特币的指导价格，其首席执行官 Mark Kapeles 也被产业界推举为代表进入比特币基金会。但是从 2013 年下半年起，随着比特币价格一路上升，Mt.Gox 却因合作伙伴的起诉和监管部门的调查而逐渐陷入混乱中。Mt.Gox 在 2014 年 2 月公告由于技术漏洞被黑客盗窃 85 万枚比特币，造成其最终破产。在在 Mt.Gox 倒闭之前，总部位于斯洛文尼亚的 Bitstamp 是它最主要的竞争对手。

伴随着比特币在中国受到越来越多的关注，诞生了以国内用户为主要服务对象的交易所，并深刻改变了比特币交易所的世界版图。中国第一家比特币交易所是成立于 2011 年 6 月的 BTCChina（比特币中国），它在 2013 年某些交易日的交易量曾高达世界第一。由于 BTCChina 在收费与免费道路上来回摇摆，同时账户提现也不稳定，其地位逐渐被后起之秀诸如 OKCion 和火币网赶上，后两者的交易量均已排名世界前列（截止本文完稿，国内交易所受法规影响已关闭或转移至海外）。交易所作为比特币产业最重要的基础设施之一，是比特币用户最常面对的机构。比特币价格的剧烈波动，吸引了很多投机者投身于比特币交易。然而，由于技术不足和监管不到位，交易所也成为比特币市场最大的风险来源。

### 2.2.3 比特币挖矿产业

矿工的挖矿活动是比特币网络运转的支撑，挖矿市场的算力投入越大，比特币网络受到“51%攻击”的概率就越低。自比特币诞生以来，挖矿产业大致经历了以下 5 个发展阶段：

（1）CPU 时代；在比特币网络出现伊始，参与者基本依靠自有的 PC 内的 CPU 进行挖矿，由于 CPU 采用指令集过于复杂，致使使用哈希算法的计算效率低下。

（2）GPU 时代；GPU 的架构使用了大量并行处理内核，一个普通 GPU 的挖矿效率最高可达到普通 CPU 的 20 倍以上，因此被一度大量用于挖矿。而 GPU 挖矿的缺陷是部署搭建困难、发热量高、能耗高。

（3）FPGA（现场可编程阵列）与 GPU 共存：2011 年开始，使用 FGPA 芯片架构的挖矿设备出现，其能耗仅为 GPU 的四十分之一而挖矿效率与 GPU 类似。但是 FGPA 价格高昂且使用方式复杂，致使只有少量具备专业知识的矿工使用，这个时期 FPGA 和 GPU 同为主要挖矿工具。

（4）ASIC 专用集成电路时代。随着新的挖矿设备出现，FPGA 与 GPU 挖矿逐渐被替代，专为挖矿设计的 ASIC 矿机开始兴盛，国内设计生产的烤猫、阿瓦隆和蚂蚁等矿机都曾名噪一时，这一时期全网参与挖矿的计算能力飞速上升。

（5）大规模集群挖矿时代。因为全网算力的飙升，单独矿工越来越难以获得稳定的挖矿回报，矿工们开始组建矿池，按各自的算力贡献量分配比特币收益，现存最大的矿池有 Bitcoin、ViaBTC、SlushPool、AntPool 等，根据 bitcoin.com 的调查，前四大矿池占全球总算力已超过 51％，到 2016 年，排名前 10 的矿池挖掘的区块数量占总数的 89％，比特币挖矿已经进入规模化、集群化时代。当前，整个比特币网络的计算能力已经超过 3PH/s(1PH/s 表示每秒可进行 10^15 次哈希运算），较 2013 年上升超过一万倍。运算速度的快速上升，导致挖矿投资难得到预期的收益。

### 2.2.4 加密货币 ICO 产业

加密货币 ICO（initial coin offering），又称首次代币发行，是以初始生产的数字加密货币作为回报的一种融资方式，是币圈类比 IPO（首次公开发行上市）打造出的一个名词，就本质上而言加密货币 ICO 对比 IPO，是用数字加密货币代替了 IPO 中的股票证券。回望 ICO 历史，最早可追溯到 2013 年，当时还没有形成 ICO 这个概念，直到 2013 年 6 月，万事达币在 Bitcointalk 论坛上发起了比特币众筹，获得 5000 多个比特币，这被认为是最早有记录的 ICO 项目，然而万

事达币未能在加密货币激烈的竞争中存活下来，现在已经销声匿迹。此后币圈出现出了大量的 ICO 项目，当中便有至今交易火爆的几个大币种。以太坊创始人 Vitalik Buterin 在 2013 年写下《以太坊白皮书》后在网络上向其他人募集以太坊项目实现的启动资金，以以太坊代币回馈出资人，在项目成功上马后，这些募资人将当初获得的以太坊代币出售，通过差价谋取收益，以太坊被认为是最成功的一次加密货币 ICO。

鉴于比特币在加密货币中的不可动摇的重要地位，加密货币 ICO 主要以比特币作为募集对象，间接增加了市场对比特币的需求，也是投机资本流入比特币市场的重要渠道。据比特币中国统计，光 2016 年国内就陆续涌现了不下 9 家 ICO 平台，累计为 20 多个加密货币项目筹集资金超过 1.41 亿元。国家互联网金融风险分析技术平台统计显示，截至 2017 年 7 月 20 日，国内提供加密货币 ICO 融资的相关平台达到 43 家，共计完成 ICO 项目 65 个，2017 年以来通过 ICO 方式共筹集 63520 个比特币和 852750 个以太币，按照当时比特币 18000 元和以太币 200 元单价来看，共筹集人民币约 30 亿元，远超 2016 年全年水平。

然而加密货币 ICO 也是风险极大的融资方式，Bitcoin.com 对 2017 全年的 ICO 融资的调查显示，在 TokenData 公司跟踪的 902 个 ICO 项目中，有 143 个项目在融资完成前就停滞了，还有 275 个项目也在融资完成后破产。这样看来在 2017 年 ICO 项目的失败率达到了 45%。Bitcoin.com 指出此外还有 113 个项目处于“半失败”状态，有的是发起人失去了音信，有的是其已经无人挖矿，如果加上这 113 个“半失败”的项目，ICO 失败率就上升到了 58%。Bitcoin.com 调查显示，在 2017 年这些失败的 ICO 项目总共获得了 2.32 亿美元的融资。加密货币 ICO 以比特币为募集对象的方式为风险资本涌入比特币市场提供了窗口，在本文实证过程中，ICO 融资额将作为短期内风险资本流入比特币市场，并对比特币价格产生影响的反映指标。

## 2.3 比特币在主要地区合法性

### 2.3.1 亚洲地区

目前比特币在中国是被禁止交易和挖矿的，2017 年 9 月 4 日中国人民银行等七部委联合下发《关于防范代币发行融资风险的公告》，内容指出大量涌现的 ICO（首次代币发行）活动涉嫌非法，其严重扰乱了经济金融秩序，要求各类代币发行活动应当立即停止，国内数字货币交易也所被勒令关停。尽管目前国内已停止比特币场内交易，但风险仍然没有消失，境外交易所仍在进行人民币兑换业务，扰乱人民币金融与外汇市场；在重重监管下，场外交易与项目“出海”或将成为新

的潜在风险，给后续监管进一步增加了难度。香港和台湾对加密货币实行严格监控，2018 年 4 月，中国台湾当局宣称，将推行基于现有反洗钱法规的加密货币监管规定。台湾地区法务部门发言人邱太三称，为避免比特币等加密货币成为洗钱方式，将对加密货币进行监控，预计于 2018 年 11 月底以前完善好相关法规。

日本对比特币交易态度最友好，日本在 2017 年 4 月实行的《资金结算法》修订案中承认了加密货币在国内的合法使用地位，对交易所落实挂牌经营，数字货币交易经营需要持有政府授予的牌照。目前已获得合法牌照的日本交易所有 16 家，根据规定这些交易所要按照经营利润上缴一定税目。

在韩国交易比特币需要获得牌照，交易所像银行那样被监管，根据韩国法律，ICO 融资是违法的，但韩国并未落实具体细则，也没有清退国内的 ICO 平台，国内投资者仍然能够参与 ICO 项目 ，数字货币交易所经营也未受影响。

加密货币交易在新加坡属于灰色地带，2018 年 5 月 24 日新加坡金管局 (MAS)对 8 家数字货币交易进行了出书面警告，禁止其在未受到允许的情况下交易证券或期货合约形式的电子代币。金管局的新举措是为了通过加强对交易所的监管，保护加密货币投资者，引导加密货币市场走向正规合法化。

印度央行禁止银行提供加密货币业务相关服务，2018 年 9 月 12 日，印度央行(RBI)向印度最高法院提交了一份宣誓书，在宣誓书中，印度央行澄清了自己对数字货币的立场，称根据现行法律制度，比特币及其同类货币无法得到认可。

2018 年 3 月，马来西亚推出针对加密货币新政，适用于数字货币交易所业务，并且对交易所颁发了牌照。目前，马来西亚国家银行（Bank Negara Malaysia）和马来西亚证券委员会正在一起订立适用于 ICO 和加密货币交易的监管规则。此外马来西亚官方正延用某些证券法监管 ICO，目前更加完善的法规正在进一步制定中。

### 2.3.2 欧洲地区

欧盟委员会一直在对有关监管细则进行讨论。负责协调各成员国监管标准任务的欧洲证券与市场管理局建议，应当禁止个体投资者参与加密货币所涉及金融衍生品的交易，另一边也在评估欧盟出台不久的新监管规定《现行金融工具市场指令》要怎样适用于虚拟资产。新的监管法规也将颁布，限制使用主权货币进行加密货币交易的平台必须对客户身份进行核实记录。欧洲证券和市场管理局(ESMA)最近也发出了一项公告，强化对虚拟货币的差价合约规定。欧盟最近还推行了针对加密货币的反洗钱规定（AML），这是欧盟推行的第 5 个反洗钱规定，旨在发现、调查以及防范该领域内的金融犯罪，授权金融监管情报机构（Financial Intelligence Units）获取数字货币钱包信息，并记录加密货币地址拥有者。

尽管英国目前尚未明确表态监管加密货币，但其一直在积极推动监管落地工作。2018 年 4 月英国金融行为监管局 FCA 公告表示提供与加密货币衍生品关联服务的公司必须遵守 FCA 手册中的所有相关法规，否则将面临强制执法措施。由此通过 ICO 发行代币相关的交易活动以及提供建议或其他服务的行为需要获得 FCA 的审查授权，包括加密货币期权、加密货币期货和加密货币 CFD 合约。

德国的数字货币交易被允许但需挂牌经营。德国监管机构希望对加密货币按种类采取逐案审查的方式。根据个案情况审查 ICO 代币发行，以决定适用何种法律框架。当前德国联邦机构建议有关部门参考适用于传统金融工具的规定并遵守当前的法律规定。

法国监管部门表示加密有关的衍生品在线服务平台需要遵循更加严苛的汇报机制和商业准则。法国政府已决定将虚拟货币视为“流动资产”，降低虚拟货币个体交易者的税率，此举措为个体交易者减少了 50%的收益损失，而虚拟货币企业的税点并未下调。在 ICO 监管方面法国金融市场监管机构 AMF 宣称正准备出台有关于 ICO 的立法，以鼓励在该国开展新型的融资活动。

瑞士金融市场监管局(FINMA)于 2018 年 2 月发布了 ICO 指导方针，制定的指导方针旨在为 ICO 增加透明度。监管局宣称将审核该国进行中的 ICO 是否符合已发布的 ICO 法规。目前尚不明了 FINMA 是否会倾向于针对违规平台采取那种行动。

俄罗斯联邦金融监控局 (FFMS) 宣称加密货币交易平台必须符合俄罗斯联邦法律中的反恐怖主义和反洗钱融资条款，否则将被取消营业牌照。俄罗斯虽然早在 2014 年 2 月宣布全面禁用比特币，但俄罗斯联邦税务局在 2016 年 11 月宣布比特币“并非违法”。

### 2.3.3 美洲及其他地区

虽然美国各州对加密货币监管规定都有不同，但近年来总体上趋于严格。美国商品期货交易委员会（CFTC）将比特币看做大宗商品，并宣称其监管对象包含洲际贸易中涉及比特币的操纵和诈骗等行为以及与比特币直接挂钩的大宗商品期货交易

加拿大政府在 2017 年 6 月颁发了关于数字货币交易所和支付处理供应商的新法规草案。该草案中将数字货币交易所和支付处理供应商视为货币服务业务范围（MSB），要求其上报超过 1 万加元（约合 7700 美元）的大额交易。

澳大利亚没有明文禁止加密货币交易和 ICO，但其官方称会对 ICO 进行更严格的监管。该国监管机构表示会着重强调禁止误导或欺骗性引导投资者的 ICO 项目。

### 2.3.4 加密货币监管总述

本文搜集整理出下表 2.2，截止本文完稿时，世界主要国家官方对加密货币交易和 ICO 的限制。反对加密货币使用的国家考虑到加密货币交易的匿名性，且常在暗网黑市用于非法商品的交易，且过度的加密货币热潮容易导致投机风险，从而对以比特币为代表的加密货币实行限制措施。支持加密货币使用的国家把这种基于区块链技术的资产，看做是加速商业运转的一次技术升级，出台法规在规定的范围内允许比特币等加密货币的存在。其他国家由于种种原因尚未明确表示对比特币等加密货币的态度，但随着加密货币和区块链技术应用范围扩大，相信以后法规会陆续加以明确。

表 2.2 各国对加密货币限制

| 州 | 国家 | 加密货币交易 | 加密货币 ICO | 是否出台对口法规 |
|---|---|---|---|---|
| 亚洲 | 中国 | 禁止 | 禁止 | 否 |
| | 日本 | 放开 | 放开 | 是 |
| | 韩国 | 禁止 | 禁止 | 是 |
| | 泰国 | 监管 | 监管 | 是 |
| | 新加坡 | 未定 | 未定 | 是 |
| | 印度 | 禁止 | 禁止 | 是 |
| | 伊朗 | 禁止 | 未定 | 否 |
| | 阿联酋 | 未定 | 未定 | 否 |
| | 以色列 | 未定 | 未定 | 否 |
| 澳洲 | 澳大利亚 | 监管 | 监管 | 是 |
| | 新西兰 | 未定 | 未定 | 是 |
| 欧洲 | 英国 | 未定 | 未定 | 否 |
| | 法国 | 未定 | 监管 | 是 |
| | 德国 | 未定 | 未定 | 否 |
| | 俄罗斯 | 监管 | 监管 | 是 |
| | 瑞士 | 未定 | 未定 | 否 |
| | 意大利 | 未定 | 未定 | 是 |
| | 西班牙 | 未定 | 未定 | 否 |
| 美洲 | 美国 | 监管 | 监管 | 否 |

接上表：

| 州 | 国家 | 加密货币交易 | 加密货币 ICO | 是否出台对口法规 |
|---|---|---|---|---|
| 美洲及其他 | 加拿大 | 监管 | 未定 | 否 |
| | 墨西哥 | 未定 | 禁止 | 是 |
| | 巴西 | 未定 | 未定 | 否 |
| | 智利 | 禁止 | 未定 | 否 |

数据来源：笔者整理所得

表中 23 个被考察国家中有 5 个国家禁止比特币等加密货币交易，5 个国家的加密货币交易需要在监管下进行，12 个国家未对加密货币交易做出表态，只有日本对加密货币交易持开放态度。对于加密货币 ICO 的态度：4 个国家禁止加密货币 ICO，5 个国家需要在监管下进行，13 个国家未对加密货币 ICO 表态，允许加密货币 ICO 的国家同样只有日本。对口法规出台方面 23 个国家中 11 个出台了针对加密货币的管理法规，剩余未出台。

## 2.4 本章小结

本章主要讲述了比特币代表的加密货币的种类和特性、加密货币相关产业现状、加密货币在各地区的监管现状。据统计目前在运行的加密货币达 2112 种，总市值高达 1392.82 亿美元（数据来源 CoinMarketCap）。如此体量巨大的加密货币市场附带的是体量更加巨大的相关产业，包括加密货币钱包、交易所、矿业和 ICO。虽然一些国家（地区）监管部门已经出台了政令和标准，但大部分没有形成针对加密货币的专管法规。重要的是加密货币的交易跟随互联网的触角伸到世界上每个角落，而各大经济体之间对加密货币的定义尚不统一，更没有产生一个监管网络。目前阶段的加密货币产业存在诸多风险，包括币值波动风险、被盗风险、非法交易风险，一个国家和地区想要单独管控加密货币领域的风险是不可能的。在文章末尾，笔者将根据存在的问题，提出一套国际联合共管策略来应对加密货币挑战。

# 第 3 章 比特币运行机制

## 3.1 比特币挖矿

比特币挖矿（Mining）是比特币新币发行的唯一途径，挖矿活动的过程如下:（1）每个矿工节点以本地区块链中最新区块的内容作为输入值计算其哈希解（Hash）[①]；（2）比特币的矿工们筛选其他节点转发或发布的交易信息，删掉已经被包含在区块链中的、余额不足的或是有其他错误的交易信息，同时也不断向外广播收录的交易；（3）随机生成一组字符串，通过将这个字符串与前面得到的哈希值和录入的交易信息合并作为输入，输出产生一个新的哈希值；（4）检测这个新的哈希值是否小于当前的难度阈值，如果是则挖矿成功，同时产生一个新的区块并向全网广播，如果哈希值结果大于阈值则从第 3 步重新计算。（5）其他节点接收这个新诞生的区块，并验证其哈希值是否符合要求，如果足够多的矿工节点证明了该区块是唯一有效的，则其它节点将接收该区块并将其添加到本地区块链上。成功挖掘新区块的矿工将获得一定数目的比特币奖励，比特币系统平均约十分钟便会产生一个新的区块。（6）如果其他矿工节点成功挖掘出合法新区块，则剩余节点会将这个区块添加至本地，然后从第 1 步开始重新挖矿。比特币挖矿过程示意图如图 3.1 所示。

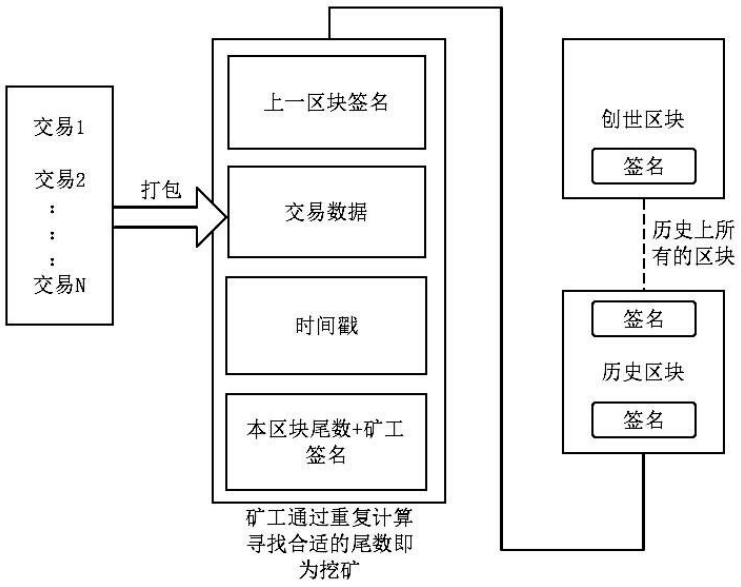


图 3.1 比特币挖矿示意图

① 哈希算法（Hash），是把任意长度的输入（又叫做预映射）通过散列算法变换成固定长度的输出，该输出就是散列值。这种转换是一种压缩映射，也就是，散列值的空间通常远小于输入的空间，不同的输入可能会散列成相同的输出，所以不可能从散列值来确定唯一的输入值。

为了能够有效的控制新区快的生产速度，比特币系统依据目前已经具有的全网总算力不断的调节哈希算法的难度阈值，全网算力越庞大，阈值越小，难度也越高。当一个新区块被挖掘的时间间隔小于 10 分钟，系统自动增加下一个区块的哈希算法难度，而当一个新区块被挖掘的时间间隔大于 10 分钟，系统将减少下一个哈希算法难度，最终使平均每隔 10 分钟产生一个新区快。也即一段时间里投入生产的平均算力和挖矿难度有着成正比的关系，全网算力越高，挖矿难度越大。矿工凭着自身算力参与全网竞争，按照其算力与全网算力的比值决定的概率挖矿，若是成功最先计算出上一区块的哈希值，则将其公布到网络中，并被整个节点网络所认可，那么就可以算作是挖矿成功。若是有人在十分钟内超前挖矿，那么之前运算就作废，可以重新创建一个区块。比特币挖矿使用的付出算力解决哈希问题的工作方式，又称为工作量证明 Pow（proof-of-work），这种挖矿方式伴随着极高的电力消耗，耗电量和代表矿工收益的比特币价格又成正比关系。

## 3.2 比特币网络

比特币网络的运行步骤如下：（1）新的交易向全网进行广播；（2）每个节点将所有录入的合法交易信息记录在新区块中；（3）每个矿工节点都试图在本地的区块数据中找到包含足够难度的工作量证明；（4）当某个节点找到了合适的工作量证明，便立刻向节点网络进行广播；（5）当且仅当包含在该区块中的所有交易都是有效的且是未存在过的，其他节点才认可该区块的合法性；（6）其他节点跟随该区块的末尾继续挖矿以延长区块链主链，便表示他们接受并承认该区块的合法性。

节点选择区块链主链的方式是将最长的链条视为正确的链条，并在该链上持续工作以延长主链。矿工节点通常会保留一段较短时间内接收到的若干由其他矿工挖掘出的新区快，优先选择在最先接收到的区块后面进行 hash 运算，若是保留的其余新区快被挖掘成最长的链，则矿工节点将立马抛弃当前区块转至在最长链后面进行 hash 运算，否则继续在当前链上工作。节点网络中新的交易信息不需要到达全部的节点，只需要到达足够的节点，那么在二次甚至多次广播后，完整的交易信息将被全部整合进区块中。比特币网络对错误信息具有容错能力，只要过半数的节点记载着正确信息，其他节点可以通过下载其区块数据达到更正目的。比特币网络运行示意图如图 3.2 所示。

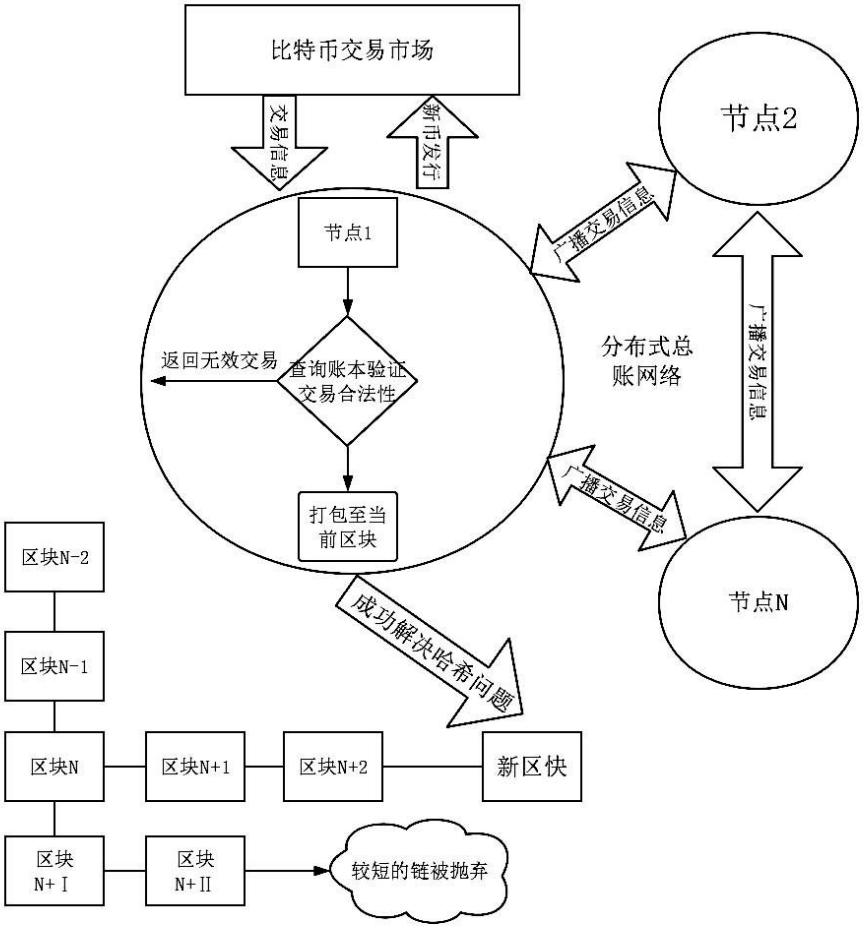


图 3.2 比特币网络示意图

## 3.3 比特币交易

比特币交易由发起人 A 转移给接受人 B 时的过程如下：（1）A 将比特币数目加上自己的私钥和接收人 B 的公钥作为交易信息广播到网络中；（2）若是这条交易信息第一次发生且 A 账户余额足够，则其将被网络节点接受验证并转发；（3）当一个新区块被某一节点成功挖掘时，节点曾今验证的 A、B 之间的交易信息将被永久的记录在新区块中；（4）若是这则交易信息没有被新区块及时收录，它将在节点之间继续被广播，直至被收入到一个区块中；（5）接收人 B 只要持有自己的公钥就能随时追溯和验证这笔交易。比特币交易的每位参与者的公钥、私钥好比是银行系统中每位用户的账户和密码，公钥代表身份，私钥则是付款密码。这样保证了比特币的交易的匿名性——交易者身份信息只有一串代码组成的公钥，他们相互间并不能知道对方的真实身份；同时也方便了被授权的执法

者和监管者——如果法律进行强制性实施，执法者能够借助于高端网络技术去追踪所有交易情况，这样就能够找到所有比特币的动向，并找到对应的使用者。

## 3.4 比特币安全性

比特币的设计中每一个节点都拥有全部的交易账本信息，并且实时相互验证，如果攻击者想在这些账目中凭空创造或者掠夺本不属于自己的比特币，那么其他节点很难想相信并验证这一伪造账本，除非能成功说服所有节点，然而这种可能性概率极小。攻击者能做的只有抹除自己曾经付出的比特币，但这也不是轻易就能完成的。他必须设法将附带篡改账本的区块接入区块链主链，基于目前协议中规定等待 6 轮区块挖掘后都存在的交易方是确定的交易，又由于矿工会优先选择在最长的链上继续挖掘，因此攻击者必须快于主链挖掘到第 6 个区块，并接入主链。这种攻击成功的概率取决于攻击者算力在全球算力中的占比，占比越大成功概率越大，当攻击者占有算力超过全网算力的 50%时，便可以随意篡改比特币的分布式账本的即时交易，比特币系统存在的这种风险被称为“51%算力攻击”风险。

自私挖矿（Ittay Eyal,Adem Efe Gencer,2013)阐明了，只要矿工联合体的算力占比达到 25%以上，他们始终会选择在自己挖掘速度有优势时秘密挖掘一条私链。即矿工联合体第一个挖到新区块时暂不广播，发现其他人广播新区块则己方也立马广播，至少保证新区块与竞争区块同时广播，在网络情况较好时依然有极大把握赢得竞争；在捂住新块同时矿工也将秘密挖掘一条私链，私链也有一定概率超过主链（在算力占比达到 1/3 时有(1/3)^2/(2/3)^2=1/4 的概率在第二个块上超越主链）。日蚀攻击（Ethan Heilman,Alison Kendler,2015）则说明了，只要矿工联合体算力达到全网算力的 33%，就可以通过日蚀攻击阻断一部分其他矿工节点的对外联络从而控制这部分矿工的算力，使得总体算力超过 50%。

任何针对比特币的攻击方式都围绕算力争夺。为了争取挖矿奖励的矿商会通过增加挖矿设备和相互联合来增加自身算力占比。而算力过度集中于某个矿商的情况是危险的，因为掌握 51%算力的一方具备篡改账本的能力，算力集中也意味着比特币去中心化的努力失败。预防攻击的方式是，一方面争取全网算力最大化，另一方面分散算力防止矿工联合。比特币拥有越大的全网总算力决定了其拥有更高的安全性。

## 3.5 拜占庭容错

“拜占庭容错”（Byzantine Generals Problem），是由莱斯利·兰波特在其同名论文中提出的分布式对等网络通信容错问题。问题背景是，曾经的拜占庭王国宫

殿内贮藏着极其丰富的金银财宝，在它周边围绕着 10 个虎视眈眈的敌对城邦，试图侵略并占有它的巨额财富，城邦们必须在同一时间集体进攻才能获胜。这些城邦面临这样一个问题，假如所有城邦向另外 9 个邻邦分派一位使者传递书信询问是否在某一时间一起进攻，这样 10 个城邦分派的 9 位使者将在某一时刻共计产生 90 回传送，而且每一个城邦将依次接收 9 个信息。意想不到的情况是，城邦中可能混有拜占庭的内奸，它可以在给 9 个邻居的书信中投反对票，也可以伪造其他城邦的信件，使得进攻计划变得不可能实现。现在区块链系统的各个节点就好比是围绕着拜占庭的城邦。

比特币通过对系统进行一个简单的更改来解决这个问题，就是使用 Pow 工作量证明增加发送信息的成本，就是在每次发送信息时附加上一定的费用投入，使得伪造信息和增发信息成本变得高昂。好比是拜占庭将军在签名和确认消息时使用的“印章”，这样所有的参与者都可以在一件事情上达成一致。按照多数原则攻击者必须操控比特币超过 50%的算力方可作假。拜占庭容错理论的解决方案，佐证了比特币无需信任的分布式总账本机制是安全的，在核心设计上没有缺陷，所以产生的风险只可能出现在平台等其他原因方面。

## 3.6 本章小结

本章讲述了比特币系统的运行机制，了解其特有的运行机制有助于后文对比特币经济学分析的精准性。比特币的运行原理和加密货币现状表明以比特币为代表的加密货币存在以下问题，也是本文着重讨论的问题。

（1）比特币挖矿是比特币系统内部运行的重要一环，它与比特币的价格表现是否存在关联，这种关联在时间上是如何变化的？

（2）比特币价格近年来波动剧烈，鉴于节点算力是预防比特币遭受篡改攻击的防御物质，那么比特币价格波动有多少部分是算力变化造成的？

（3）比特币名为去中心化的新兴货币，而在实际应用中比特币是否适合作为一种货币存在？

本文将带着这些问题继续下面的讨论，通过经济学分析和实证分析来解答以上三个问题。

# 第 4 章 比特币的经济学理论分析

## 4.1 币价的决定

本节是对比特币价格决定因素的核心讨论部分，作为对比特币的探索性研究，首先使用的分析方式属于定性分析，即不考虑影响因子的具体作用大小和曲线，而主要考虑影响因子的选取范围及影响因子的作用方向。因此推导的方程中略去了部分影响因子的幂次、系数和截距项，最后也能方便将比特币市场和比特币挖矿两方面的影响因子综合起来讨论。定性分析是定量分析的前提，通过定性分析得出的模型在不断拟合实际数据后方能起到具体预测的作用。本文的建模过程也是在基本线性模型的设定下展开的，限于数据的稀缺和理论的不完善，更加完整的币价模型有待以后的研究发现。

### 4.1.1 比特币的货币属性

货币的职能是在从古至今的商品交易中的变化体现出来的，货币最早具有的是价值尺度和流通手段的职能。商品进入市场流通之前，首先在货币层面衡量其价值，执行货币的价值尺度的职能；商品进入市场流通后，货币是其交易的媒介，执行货币的流通手段职能，以上是货币的两种基础职能。货币作为社会财富的一般代表，停止流通时可作为价值储存从而发挥贮藏手段的职能。随着商品经济发展赊销交易开始出现，货币此时不再执行流通手段的职能，而是在协定的交割日期才被用于债务清偿，进而发挥支付手段的职能。

货币作为价值融通的手段，其媒介也经历了一系列的演变，包括使用盐、贝壳、石头等做交媒介的商品货币时代，以金、银、铜等金属做媒介的金属货币时期；和以纸币代金银等贵金属的金本位时代；直到现在世界通行的信用货币时代，货币的流通速度更快，货币的流通成本更低，货币的总量更能符合经济活动需要。已有的研究讨论了未来货币的形式还会有哪些变化，它应该具备更快的流通速度、更灵活的流通总量、更广泛的使用场景。而集合了包括分布式存储数据库技术、P2P 通信协议、共识算法、加密算法等技术的以区块链技术为底层技术的比特币恰好符合了这些联想。

比特币是一种全新的币种，超越以往任何时候的货币定义范畴，它不同于其他主权货币，它没有固定的发行方，不依靠信用创造，而是在市场上保持一个增发速度可控的流动总量，这一点和黄金类似，而又不完全和黄金一样。按照货币供需理论的范畴讨论，在供给侧，比特币有着恒定发行速度：从 2009 年开始每十分钟挖掘一个区块并创造 50 个比特币，而后每 4 年发行量减半，到 2019 年将

有 1800 万个比特币被挖掘，最终比特币的发行总量将是 2100 万个。在需求侧，人们持有比特币是考虑它在全球范围交易的便捷性、账本不可篡改的安全性和去中心化的公平性，使得比特币价格从最初的 0.003 美元飙升到最高 18674 美元。比特币有着和黄金类似的总量稳定的优势，同时有着比传统货币更灵活的使用场景，注定了它会成为满足投资者日常配置资产的备选项。

总体而言比特币是一种具备货币属性的电子化资产，需要从传统货币的研究范畴和比特币特有的挖矿行为两方面来对其进行讨论。

### 4.1.2 流动性偏好理论

针对比特币的货币属性讨论是基于凯恩斯的流动性偏好理论。凯恩斯在 1936 年出版了《就业、利息和货币通论》，书中阐述了货币的价值贮藏功能，不论是放在口袋还是锁进银行保险柜都不会像储存食物那样担心腐败烂掉，即便隔上若干年拿出来照样能用。货币用于交易时流动性最强，这一点是其他诸如债券和股票等资产望尘莫及的，后者必须先转换成货币才能用于交换商品和服务。

凯恩斯及其学派着重突出货币流动性的地位，因此他的货币理论又被称作流动性偏好理论。凯恩斯认为公众持有货币的动机主要分成三种：一是交易动机，泛指个人和企业为了购买商品而持有货币的动机，交易动机的货币需求量主要取决于收入，比特币的交易动机主要取决于比特币的经济规模、交易成本和交易速度。二是谨慎动机，又称预防性动机，指的是预防意外性支出而持有一部分货币的动机，这部分动机在比特币系统中同样取决于比特币经济规模、交易成本和交易速度。三是投机动机，指的是人们为了抓住有利的购买有价证券或者其他金融产品的机会而持有一部分货币的动机，投机动机的比特币需求主要取决于全球的综合利率，并和全球综合利率成反比，全球综合利率越高，人们更倾向于卖出比特币而持有其他传统货币计价的金融资产。

从上面阐述可以得出，利率与投机性货币需求呈反比。凯恩斯学派认为， 控制货币需求需要先控制利率。因此凯恩斯学派建议，政府可以通过改变货币供给来控制利率，必要时应该实行利率管制。他的货币政策具体建议是，经济萧条时应采取扩张性货币政策增加货币供给从而降低利率刺激经济回升；在经济高速前进时则实行紧缩的货币政策，降低货币供给从而提高利率抑制经济过快增长。货币政策要逆经济趋势，相机抉择。

### 4.1.3 比特币供需分析

比特币拥有恒定的发行量和逐渐减小的发行速度，从 2016 年 7 月到 2020 年 7 月间预计发行约 263 万个，平均每年发行 66 万个。在本文实际考察的 2016 年

1 月到 2018 年 12 月 1 日，此期间共发行比特币约 164 万个，在存量约 1800 万个比特币中占比很小，可以认为比特币供给是恒定的常数。我们用凯恩斯的货币供需模型来探究比特币的问题。用 $M^S$ 表示比特币供给如式 4.1 所示：

$$M^S = P_B \cdot B \tag{式 4.1}$$

其中 $P_B$ 表示比特币的价格指数，B 是一个常数，表示比特币的流通总量。据前文论述，比特币的需求包括交易动机、投机动机、谨慎动机。他们的影响指标如下：比特币购买商品的价格 P、一段时间的比特币交易量 EOV、比特币价格指数 $P_B$、比特币经济规模 Y、比特币的交易速度 V、全球综合利率 r、比特币交易成本 C。设比特币的交易和谨慎动机为 $M_1^D$、投机动机为 $M_2^D$，那么比特币的需求 $M^D$ 可表示为式 4.2：

$$M^D = M_1^D + M_2^D = \frac{EOV \cdot P \cdot Y}{V \cdot \mathrm{r} \cdot \mathrm{C}} \tag{式 4.2}$$

即比特币的需求与比特币交易量、商品价格、经济规模成正比，与比特币交易速度、综合利率成反比、比特币交易成本成反比。根据完全竞争的货币市场均衡理论，当 $M^D = M^S$ 时，货币市场取得均衡，此时的比特币价格表示为式 4.3。

$$P_B = \frac{EOV \cdot P \cdot Y}{r \cdot V \cdot B \cdot C} \tag{式 4.3}$$

方程两边取对数有

$$\ln P_B = \ln EOV + \ln P + \ln Y - \ln C - \ln r - \ln V - \ln B \tag{式 4.4}$$

介于本文考察时间段不涉及长期变化，此时方程中应加入短期影响因素：比特币市场的资本流入 I。前文论述了以比特币为媒介的加密货币 ICO 代表的资本涌入，从而影响比特币价格 $P_B$。因此用加密货币的 ICO 融资量 I 表示比特币受到的短期资本的影响，更改的方程为式 4.5。

$$\ln P_B = \ln EOV + \ln P + \ln Y - \ln C - \ln r - \ln V - \ln B + I \tag{式 4.5}$$

用 $P_B'$ 简化表示 $\ln P_B$,以此类推得简化后的方程 4.6

$$P_B' = EOV' + P' + Y' - C' - r' - V' - B' + I \tag{式 4.6}$$

需要特别指出的是，比特币世界没有银行体系，也不存在有记录的借贷市场，因此不存在专门刻画比特币的利率。本文使用全球综合利率作为描绘比特币系统的“利率”概念，而全球综合利率是外部利率，其影响方式与内部利率相反，即

外部利率上升使得持有比特币的机会成本上升，投资者偏向卖出比特币而持有其他资产，进而比特币价格下跌，反之则上升。倘若存在内部利率，其上升将使得持有其他资产的机会成本上升，则投资者偏向卖出其他资产而持有比特币，进而比特币价格上升。简而言之内部利率和外部利率对比特币价格的影响方向相反，本文采用的是外部利率，这一改变与传统的流动性偏好理论对利率的描述不同。

### 4.1.4 挖矿市场的属性

传统微观经济学将市场定义为，物品买卖双方相互作用并得以决定其交易价格和交易数量的一种组织形式或制度安排。它可以是一个有形的买卖物品的交易场所，如菜市场、百货商场等，也可以是利用现代化通讯工具进行物品交易的接洽点，如股票市场、外汇市场。加密货币挖矿市场是一种虚拟市场，不存在具体的地点和交易人。挖矿的参与者称为矿工，与现实意义中的矿工不同的是，加密货币矿工并不付出实际的体力劳动，而代之以付出所拥有的集成化处理器的计算能力。挖掘过程也不像现实当中的针对有限的矿石资源，而是针对取用不尽的加密货币区块。

加密货币挖矿市场中，矿工们生产的是几乎无差别的算力，获得的也是价值相同的代币报酬。从长期来看挖矿市场更偏向于完全竞争市场。完全竞争市场的经济学定义是，不包含任何垄断因素的市场，市场上有大量的买卖者，每个厂商提供的商品都是完全同质的，所有资源具有完全流动性，市场信息也是完全的。但是在短期内，加密货币矿商面对的是不同的电力成本、不同的挖矿设备、不同的挖矿软件和不完全的市场信息，因此本文的研究暂把比特币挖矿市场归为垄断竞争市场。垄断竞争市场的经济学定义为，市场中有许多厂商生产和销售有差别的同种产品且面对相同的产品价格的市场组织，市场的进入和撤出都很轻易，市场中的厂商可以获得短期超额利润。

### 4.1.5 比特币矿商的成本收益分析

以比特币为代表的加密货币挖矿市场属于垄断竞争市场，因此假设矿商的生产函数为规模报酬不变的科布—道格拉斯生产函数。算力产出 $Q_h = AE^{\alpha}K^{\beta}$，其中α+β=1，0≤α≤1，0≤β≤1，E 为矿商的电力消耗量，反映短期可变成本，K 为矿商的资本投入量，反映长期固定成本，$Q_h$ 为矿商的算力产出,$Q_T$ 为全网算力总和。再设全球范围的综合电力价格为 $P_E$、比特币挖矿能耗为 E、资本价格为综合利率 r，则有单个矿商的收益函数如式 4.8 所示

$$\pi = \frac{Q_h}{Q_T} \cdot P_B - E \cdot P_E - K \cdot r = \frac{A \cdot P_B \cdot E^{\alpha} \cdot K^{\beta}}{Q_T} - E \cdot P_E - K \cdot r \quad \text{（式 4.8）}$$

当矿商取得边际收益和边际成本相等的一阶条件时获得最大收益，即有

$$\frac{\partial \pi}{\partial E} = \frac{\alpha A P_B E^{\alpha-1} K^{\beta}}{Q_T} - P_E = 0 \quad \text{（式 4.9）}$$

等式左右变化得式 4.10

$$Q_T = \frac{\alpha A P_B K^{\beta}}{E^{\beta} P_E} \quad \text{（式 4.10）}$$

上式两边取对数得算力与资本投入的关系如式 4.11 所示

$$\ln Q_T = \ln \alpha \mathrm{A} + \ln \mathrm{P_B} + \beta \ln \mathrm{K} - \beta \ln \mathrm{E} - \ln \mathrm{P_E} \quad \text{（式 4.11）}$$

其中的α、β和 A 为常数，厂商固定投资在短期内基本不变化，因此公式中把固定投资 K 也看做常数。根据前文规律化简得式 4.12：

$$Q_T' = P_B' - P_E' - \beta E' + D \quad \text{（式 4.12）}$$

其中 D 为某一常数且有

$$D = \ln \alpha A + \beta \ln K \quad \text{（式 4.13）}$$

为了方便计算，假设矿商是无差别的，每个矿商提供相等的算力，且市场上有数目不变的 n 个矿商，则全网总算力 $Q_T = nQ_h$，即二者成正比关系，在实证中用全网总算力代替单个矿商算力进行回归。

### 4.1.6 模型综合

经过对比特币市场和比特币挖矿的经济学分析，研究范围内所有对比特币价格的影响因素已经清晰展示，为了方便下一章的 OLS 回归估计，在这里需要产生一个涵盖所有影响因子的综合方程。根据式 4.6 和式 4.12 可得综合方程如下式 4.14 所示。

$$P_B' = EOV' + P' + Y' + I + Q' + P_E' + \beta E' - C' - r - V' - Z \quad \text{（式 4.14）}$$

式中 Z 表示某一常数，且有 $Z = \ln \alpha A + \beta \ln K - \ln B$。

实证中同样采用对数化的变量进行回归，即使用多元双对数线性回归模型。这么做的好处，一是贴合模型推导过程，二是有效减少回归存在的异方差性。

## 4.2 比特币算力与价格内在关系分析

经济理论是经过长时间观察，分析归纳得出的，传统经济理论在对比特币这一新兴事物进行的分析上，可能没有包含全部的逻辑框架。为了强化本文的分析论证，还需要结合比特币体系特有的实际运行原理，对比特币币价与算力的关系进行脱离经济原理的单独分析。

对比特币币价与算力间的影响路线分析，是以比特币系统存在针对分布式总账的 51%算力攻击为前提的。具体解释如下：假设不存在外部因素影响，如果矿商在激烈争夺算力占比后不再能承受高昂算力带来的巨大的赤字，又或者他们发现一种更加有利可图的加密货币挖矿，便会在短时间内撤出算力。算力下降会引起比特币投资者的注意，介于 51%算力攻击存在的可能性增加，为了避免可能发生的算力攻击篡改分布式账本中的余额，投资者对比特币的抛售会在短时间内发生。币价下跌又反过来进一步打击矿商收益，此时的比特币算力和价格呈现同向下跌。投资者和矿商谁也不知道比特币价格和算力哪一方会先触底，为了避开风险任何一方都会不断逃离。即在比特币价格或算力下降的情况下，比特币价格——算力存在双向成正比的影响，触发过程如图 4.1 所示。

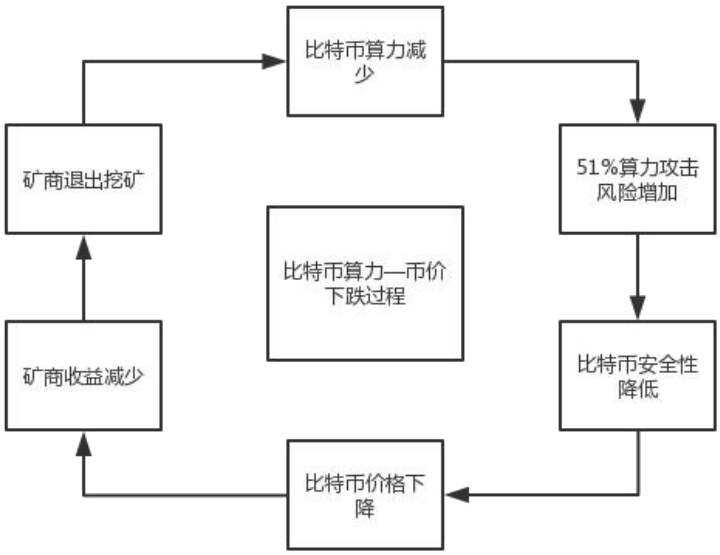


图 4.1 比特币算力——价格下跌过程

反过来看，比特币更高的算力意味着比特币系统对 51%算力攻击的防御力增

强，潜在攻击者必须通过更大的算力投入发动攻击，而攻击成本往往比得到的收益更高。投资者观察到比特币安全性的提高会更放心地持有比特币，促使比特币价格随算力提高而提高。比特币价格提高使矿商获得更高收益，又促使矿商进一步投入算力竞争。即在比特币币价或算力上升的情况下，比特币币价——算力同样存在双向成正比的影响，过程就是图 4.1 的反向变化，具体过程如下图 4.2 所示。

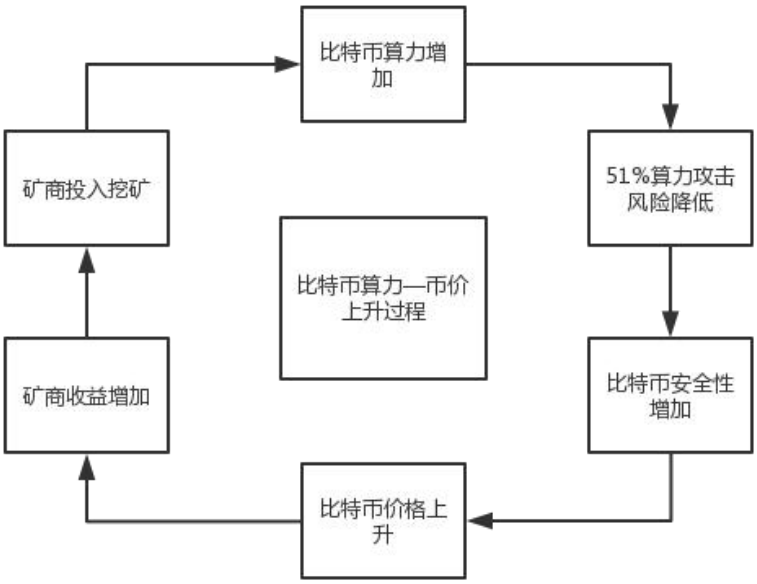


图 4.2 比特币算力——价格上升过程

综上所述，比特币价格和算力存在双向影响，且影响过程有随时间放大的趋势。这种双向影响在外生性因素的冲击下才发生变化，假设比特币系统一段时间内不存在外生因素影响，那么比特币价格和算力只受制于内部影响，将双双冲向一个极值。比特币设计上有一定缺陷，致使系统内部缺乏促使币价和算力稳定的负反馈通道，对比特币价格稳定造成了一定程度上的破坏。

在下一章的内容中，本文将使用时间序列 VAR 模型的脉冲响应验证这种随时间不断扩大的正向影响。VAR 模型可以不依赖具体的经济理论而建立，将相互影响的若干变量放在一起作为一个系统进行考察，模型中各个变量具有同等地位，模型安排如下式 4.16 所示。

$$P_{Bt}+Q_t+r_t=C+\begin{bmatrix}\Phi_{11} & \Phi_{12} & \cdots & \Phi_{1p}\\ \Phi_{21} & \Phi_{22} & \cdots & \Phi_{2p}\\ \Phi_{31} & \Phi_{32} & \cdots & \Phi_{3p}\end{bmatrix}\begin{bmatrix}P_{Bt} & Q_t & r_t\\ P_{Bt-1} & Q_{t-1} & r_{t-1}\\ \cdots & \cdots & \cdots\\ P_{Bt-p} & Q_{t-p} & r_{t-p}\end{bmatrix}+\varepsilon_t \qquad \text{（式 4.16）}$$

其中 $\Phi_{ij}$ 是系数矩阵，$\varepsilon_t$ 代表白噪声过程，模型设置将 $r_t$ 作为外生性因素加入到对比特币币价——算力双向影响的分析当中，$r_t$ 代表比特币系统运行过程所面对的外部综合利率。

## 4.3 本章小结

本章作为全文的核心分析所在，从三个角度对比特币系统进行了讨论。

首先，将比特币作为传统货币，基于凯恩斯的流动性偏好理论，在供需均衡状态下对比特币价格的影响因素进行了列举；同时考虑到流动性偏好理论是长期过程的描述，本章还加入了比特币价格的短期影响因素资本流入，作为模型的完善。

其次，比特币与传统货币的发行过程有很大不同，比特币系统中的矿商承担着记账和发行的工作，而矿商生产的算力是抵御 51%篡改攻击的防御物质。比特币算力和币价间的相互作用是比特币系统运行的核心内容。本章对矿商行为的分析从垄断竞争的挖矿市场出发，对挖矿行为进行成本收益分析，得出比特币算力与币价的数学模型。然后进行整理，得出用于实证的比特币币价综合模型。

最后，由于比特币市场表现和矿商行为受到多方面、多渠道的影响，传统的经济学分析方式不能全面揭示比特币系统存在的问题。因此还需对比特币币价和算力相互影响进行单独分析。以比特币面临的针对分布式总账的 51%算力攻击为介质，分析得出比特币价格和算力间存在双向成正比的影响，且影响力度随时间有扩大趋势。产生的模型还控制了综合利率 r 作为外生性变量，在下一章用时间序列 VAR 模型进行验证。

# 第 5 章 实证分析

本文实证部分将使用最小二乘法（OLS）对币价综合决定模型进行回归估计，最小二乘法是一种数学优化技术。其寻找数据的最佳函数匹配的方法是使拟合函数与实际值的误差平方和最小化。最小二乘法可以方便地用于求解已知趋势下的未得数据且使其与真实情况更吻合。最重要的应用场景是在曲线拟合上，最小平方和所概括的最佳拟合是指残差（残差为：观测值与模型提供的拟合值之间的差距）平方总和的最小化。而后用时间序列 VAR 模型对比特币币价—算力影响做脉冲响应分析，时间序列 VAR 模型可以考察多组单整变量间的相互影响，而不需考虑每两组变量间是否存在协整关系。该模型可以不依赖具体经济理论而直接建立多变量时间序列模型。

## 5.1 变量设置

### 5.1.1 多重共线性指标

多重共线性是指，线性回归模型中的解释变量之间由于存在相互关联的变化趋势而使模型难以准确估计或估计失真。多重共线性成因主要有：经济变量间包含共同趋势、引入滞后变量、样本数目不足。多重共线性对回归估计的影响有：（1）完全共线性情况下估计系数不存在（2）近似共线性下估计系数解释无效（3）参数估计量经济意义不准确（4）变量的显著性检验失去意义，从而可能将重要的解释变量遗漏（5）模型的预测功能无效，变大的方差容易使区间预测的“区间”变大使预测失去意义。本文实证中将剔除存在多重共线性的变量，避免自变量之间存在多重共线性，从而对回归估计造成偏差。

在上一章建立的模型中，比特币交易量 EOV、比特币经济规模 Y、比特币交易速度 v 以及比特币交易成本 C 存在明显的多重共线性。首先比特币交易量和比特币经济规模存在同向相关性，比特币经济规模越大，体现在纳入用比特币购买的商品增加，此时发生更多购买行为使得以美元测算的比特币交易量随之增加。另外比特币交易速度与比特币交易成本存在正相关，这是由于比特币的交易流量存在限制，当网络中产生拥堵，大量交易无法通过验证，节点将收取提供更高交易费用的交易，反映在交易费用上就是交易速度越快交易成本越高。

由此，币价模型中的比特币经济规模 Y 和比特币交易速度 V 分别作为比特币交易量 EOV 和比特币交易成本 C 的共线性变量应当剔除。而之所以不舍去 EOV 和 C 是因为此二者的数据获取更加方便。

### 5.1.2 模型指标含义

实证过程的变量有：比特币价格 $P_B$、比特币交易量 EOV、加密货币 ICO 融资额 I，美元指数 P，比特币交易成本 C，一年期美元国债收益率 r，比特币算力 Q，比特币能耗指数 E，国际综合能源价格 $P_E$。本文的美元宏观市场数据来源包括美国财政部和美联储官网，比特币交易数据及其矿业统计指标来源于区块链和比特币研究机构 BlockChain.info、CoinDesk、和 BTC.com 网站，资本市场数据来源于 Quandl 数据库和 RESSET 金融数据库。

（1）比特币价格 $P_B$ 在这里用比特币兑美元汇率表示，用来反映比特币的价格浮动变化。

（2）比特币交易量 EOV 是比特币在一周内的平均日交易量，用于反映比特币市场的需求变化情况。

（3）资本涌入 I 不好直接观测，本文用全球加密货币 ICO 的募款规模表示。加密货币 ICO 是以发行新加密货币为目的，以收取比特币为募资手段的融资方式，最初受到以太坊项目融资的启发，现在已经成为区块链项目的主要融资模式。

（4）美元指数 P，是综合体现美元的国际外汇市场的供需情况的变量，用来衡量美元兑换一揽子货币的比值变化程度。在这里用于反映比特币购买商品的价格。

（5）比特币交易成本 C 表示比特币在交易过程中的阻力因素，用比特币交易费用可以直接表示。比特币交易费用是矿商节点验证记录交易信息而收取的“手续费”，会随着交易量的上涨而上升，完美地贴合了交易成本的概念。

（6）一年期美元国债收益率 r，反映国际市场上的综合利率水平，用来衡量比特币的投机性需求。

（7）比特币算力 Q，指的是比特币哈希率，它是每秒钟哈希难题被计算的次数，直接反映全网算力情况，本文用它来表示全网算力 Q，它的单位是 Ph/s，表示每秒钟产生 10 的 15 次方的哈希计算。

（8）比特币能耗指数 E，用来表示比特币系统在全球的用电情况，电力是矿商的主要生产成本，占到总成本的 60%以上。

（9）国际能源价格 $P_E$，鉴于电力价格在全球范围内高低不一，难以统计，本文使用欧派克产油国原油价格作为替代变量。欧派克产油国原油价格是欧派克十二个成员国使用的共同原油出口价格，而石油作为热能能源和电力能源具有替代作用，能很好地反映能源总体供需情况。

### 5.1.3 指标的描述性统计

实证部分所有数据均以周为时间统计单位，比特币交易量、比特币价格、美元指数、一年期美元国债收益率和比特币算力取一周平均值，ICO 融资和比特币交易成本取一周内的累计量。从 2016 年 1 月 1 日起到 2018 年 12 月 1 日止，共包含 9 个变量及 1279 个数据。币价模型的数据描述性统计如下表 5.1 所示。

表 5.1 变量描述性统计

| 变量 | 均值 | 中位数 | 最大值 | 最小值 | 标准差 | 偏度 | 峰度 | 单位 |
|---|---|---|---|---|---|---|---|---|
| 比特币价格 Pb | 4019.1 | 2622.24 | 17882.5 | 374.686 | 3935.22 | 1.1 | 3.76 | 美元 |
| 比特币交易量 EOV | 2808.8 | 1244.02 | 18304.3 | 42.94 | 3642.67 | 1.81 | 6.62 | 百万美元 |
| ICO 融资 I | 1579.5 | 158.6 | 7800 | 2.1 | 2463.38 | 1.49 | 3.75 | 万美元 |
| 美元指数 P | 95.67 | 95.45 | 103.01 | 89.07 | 3.23 | 0.16 | 2.63 | 美元指数 |
| 比特币交易成本 C | 956.59 | 468 | 6771.28 | 112.73 | 1123.46 | 2.28 | 9 | 比特币 |
| 一年期美元国债收益 | 1.35 | 1.17 | 2.72 | 0.46 | 0.75 | 0.51 | 1.79 | 百分比利 |
| 比特币算力 Q | 14461.8 | 5129.91 | 57499.3 | 707.46 | 17075.16 | 1.14 | 2.85 | Ph/s |
| 比特币能耗 E | 170.17 | 127.2 | 418.8 | 22.28 | 133.77 | 0.48 | 1.75 | TWh |
| 国际能源价格 Pe | 61.6 | 61.71 | 83 | 43.42 | 10.56 | 0.09 | 1.79 | 美元/桶 |

数据来源：CoinDesk，BlockChain.info，BTC.com，Quandl 数据库，Resset 金融数据库。

从描述性统计可以看出，比特币价格、比特币交易量、ICO 融资、比特币交易成本四者都拥有大于零的偏度和大于标准峰度 3 的峰度值。峰度大于 3 意味着它们的概率密度具有“尖峰厚尾”的特征，即存在大量中间值数据和少量极值数据，偏度大于零意味着它们的概率密度峰值位于均值左侧，即有算术平均数大于中值，直观表现为右边的尾部相对于与左边的尾部要长，由于少量样本值很大导致曲线右边尾部延长。反映在时间轴波动上是以上四者变量具有较大突变性，受到冲击因素影响时具有较大反映，这也是投机性过高的体现，一些不成熟或者“盘子”小的投资品市场也具有相似的图形特征。而美元指数和一年期美元国债收益率在具有正值偏度同时则表现出相对平坦的概率密度，这得益于美元作为体量巨大的经济指标，受到各种短期冲击因素影响较小，好比物理学中“质量”很大的物体在相同“冲量”作用下较“质量”小的物体速度变化更小。比特币算力、比特币能耗和国际能源价格正偏同时拥有较为扁平的概率密度，是由于此三者的变动依赖于建设性投入，往往有滞后性。比特币算力的标准差值很大，是由于一个矿商往

往参与多种加密货币挖矿，在比特币挖矿回报率不高或者其他加密货币挖矿回报率更高时，他们可以立即撤出算力，反之也可以立即增加算力。

## 5.2 币价综合决定模型的回归估计

本文使利用 OLS 最小二乘法对多元线性模型进行回归估计。根据上一章综合币价决定模型式 4.14，刨去多重共线性变量，多元线性双对数回归模型设置为如下式 5.1 所示

$$\log(P_B) = C_1 + C_2\log(C) + C_3\log(E) + C_4\log(EOV) + C_5\log(I)$$
$$+ C_6\log(P) + C_7\log(P_E) + C_8\log(Q) + C_9\mathrm{r} + \mu \qquad (式\ 5.1)$$

$C_1$~$C_9$ 表示解释变量的估计系数，μ表示残差。$P_B$ 为比特币价格指数、C 为比特币交易成本、E 为比特币能耗指数、EOV 为比特币交易量、I 为加密货币 ICO 融资规模、P 美元指数、$P_E$ 为欧派克原油出口价格、Q 为比特币全网算力、r 为一年期美元国债收益率。由于除一年期美元国债收益率 r 外的其他变量样本值普遍超过三位数，因此用对数处理，表示相互间以百分比变动的影响，r 的样本值很小，有些甚至小于 1，不适用于对数表达。用 Eviews9 软件进行回归处理，得出如下表 5.2 结果。

表 5.2 币价模型参数估计

| 变量 | 估计系数 | 标准差 | t-统计值 | P-值 | 与模型符号一致 |
|---|---|---|---|---|---|
| 比特币交易费用 C | -0.059687 | 0.027237 | -2.191417 | 0.0309** | 是 |
| 比特币能耗指数 E | 0.439149 | 0.212477 | 2.066809 | 0.0424** | 是 |
| 比特币交易量 EOV | 0.498591 | 0.065596 | 7.600961 | 0.0000*** | 是 |
| ICO 融资规模 I | 0.092682 | 0.039279 | 2.359604 | 0.0205** | 是 |
| 美元指数 P | -0.382330 | 1.418517 | -0.269428 | 0.7882 | 否 |
| 欧派克原油出口价格 $P_E$ | 1.080513 | 0.277539 | 3.893199 | 0.0002*** | 是 |
| 比特币全网算力 Q | 0.187117 | 0.093282 | 2.005936 | 0.0479** | 是 |
| 一年期美元国债收益率 r | -1.043711 | 0.263789 | -3.956621 | 0.0002*** | 是 |

注释：D 表示变量经过一阶差分；*、**、***表示显著水平为 10%、5%、1%的临界值。

观察上表结果，除了美元指数的回归结果在 5%显著性水平上不能拒绝原假设，估计结果不显著外，其余解释变量皆在 5%显著性水平上对被解释变量影响

显著。模型调整后的判定系数 $R^2$ 值为 0.944235，即模型对比特币价格解释度达到 94.42%。将系数估计结果对比上一章比特币价格综合决定模型的公式，观察到所有被显著估计的变量左侧的符号都相同，即本文使用的经济学理论推导的解释变量对作为被解释变量的比特币价格影响方向与实证结论一致，模型设置正确。

上文中笔者把美元指数作为衡量比特币所购买商品价格的指标，这一指标上升会引起比特币交易动机的需求上升，从而抬高比特币价格。美元指数的估计结果不显著，一是由于比特币作为资产被持有的情况多于作为交易媒介用于购买商品的情况，二是由于比特币交易确认时间过长导致在商品交易场景下的应用不便。可以进一步推导比特币不适合作为一种货币存在。本文用加密货币 ICO 融资规模代表投机资本进入比特币市场的强度，在回归估计结果中显著，表示短期内比特币价格受投机资本流入影响显著，国际游资频繁进出比特币市场导致币价波动剧烈。比特币算力与比特币价格存在显著的正向关系，证明矿商活动对币价是有影响的，下一节 VAR 模型的脉冲响应分析中将讨论这种影响在时间上的变化特征。

## 5.3 基于时间序列 VAR 模型的实证分析

本文聚焦分析币价波动与矿商行为之间的相互影响，并考察这种影响的大小和时间上的持续性，因此需要用到时间序列模型。时间序列 VAR 模型可以考察多组单整变量间的相互影响，而不需考虑每两组变量间是否存在协整关系。该模型可以不依赖具体经济理论而直接建立多变量时间序列模型。用各个变量的当期值作为因变量，根据信息指标 AIC 取最小值原则选取若干滞后期作为解释变量，所有变量在此框架中都具有同等地位，变量之间的滞后期用滞后变量来刻画，对变量之间的协整关系检验转化为对压缩矩阵秩大小的检验。本文的实证过程使用计量软件 Eviews9.0 完成。

### 5.3.1 VAR 模型的定义和推导

满足下列向量随机差分方程 $\{X_t\}$，$t \in T$ 为 p 阶向量自回归过程，记为 VAR（p）。则有

$$X_t = C + \Phi_1 X_{t-1} + \Phi_2 X_{t-2} + \ldots + \Phi_p X_{t-p} + \varepsilon_t \qquad \text{（式 5.1）}$$

其中 $\varepsilon_t$ 为白噪声过程，C 为 n 维常数项量 $\Phi_i$ 的 n 阶参数矩阵。此时引入滞后算子 L，并令 $\Phi(L) = I_n - \Phi_1 L - \Phi_2 L^2 - \ldots - \Phi_p L^p$，显然 $\Phi(L)$ 为矩阵多项式，上述 VAR（p）可表示为

$$\Phi(L) X_t = C + \varepsilon_t \qquad \text{（式 5.2）}$$

设白噪声过程 $\varepsilon_t$ 满足 $\varepsilon_t \sim IIN(0,\Omega)$，且有 T+p 个观测值，以从前的 p 个观测

为初始条件，利用条件密度函数推导得出的对数条件似然函数为

$$\ln L(X_1, X_2, \ldots, X_T, \Pi \mid x_{-p+t} \ldots x_{-1}, x_0) = -\frac{nT}{2}\ln(2\pi) + \frac{T}{2}\ln \mid \Omega \mid^{-1} - \frac{1}{2}\sum_{t=1}^{T} \varepsilon_t' \Omega^{-1} \varepsilon_t$$

（式 5.3）

利用上述条件似然函数对Π求偏导得到极大似然估计为

$$\hat{\Pi}' = [\sum_{t=1}^{T} X_t Y_t'][\sum_{t=1}^{T} Y_t Y_t']^{-1}$$

（式 5.4）

从而 $\varepsilon_t$ 的协方差矩阵极大似然估计为

$$\hat{\Omega} = \frac{1}{T}\sum_{t=1}^{T} \hat{\varepsilon}_t \hat{\varepsilon}_t'$$

（式 5.5）

其中 $\hat{\varepsilon}_t = X_t - \hat{\Pi}' Y_t$，因此参数的条件极大似然估计与单方程的条件最小二乘法（OLS）结果完全相同，但Ω的估计结果略有差异。通过矩阵迹的特性经过计算得到似然函数表达式结果为

$$l(p) = -\frac{nT}{2}[\ln(2\pi) + 1] + \frac{T}{2}\ln\left|\hat{\Omega}(p)\right|^{-1}$$

（式 5.6）

其中的 p 表示滞后阶数，将在后面进行界定。

### 5.3.2 单变量平稳性检验

使用 ADF 单位根检验法检验比特币对美元汇率、比特币算力和一年期美元国债收益率变量的平稳性，只有通过平稳性检验才能使用 VAR 模型，检验结果如下表 5.4 所示。

表 5.4 变量原值的 ADF 单位根检验

| Augmented Dickey-Fuller test statistic | t-Statistic | Prob.* |
|---|---|---|
| Pb | -1.531378 | 0.8146 |
| Q | -1.821250 | 0.6897 |
| r | -1.955596 | 0.6204 |

可见检验结果在 5%的显著性水平上均不能拒绝原假设，三个变量的根都不在单位圆范围内，即不具备 VAR 模型所需的平稳性条件，继续建立模型将会产生伪回归。因此对三个变量做一阶差分处理，再看看是否满足平稳性条件，结果如下表 5.5 所示。

表 5.5 变量一阶差分值的 ADF 单位根检验

| Augmented Dickey-Fuller test statistic | t-Statistic | Prob.* |
|---|---|---|
| DPb | -6.694288 | 0.0000** |
| DQ | -17.96830 | 0.0000** |
| Dr | -10.01535 | 0.0000** |

注释：D 表示变量经过一阶差分；*、**、***表示显著水平为 10%、5%、1%的临界值。

DPb、DQ 和 Dr 分别是比特币兑美元汇率 Pb、比特币全网总算力 DQ 和一年期美元国债收益率 r 的一阶差分项。经过一阶差分的三个考察变量的 ADF 单位根检验全部在 0.1%的显著性水平上明显拒绝原假设，表明差分后的变量符合平稳性要求，下面的过程中将使用一阶差分后的变量进行分析。

### 5.3.3 VAR 模型定阶

传统经济学计量分析过程确定 VAR 模型阶数的方法是通过观测信息指标 AIC 和 BIC 来判断，本文主要采用信息指标是 AIC。赤池信息量准则（Akaike information criterion，简称 AIC）是评价计量模型的复杂度和对比计量模型“拟合”适用性的一种指标，是由日本统计学家赤池弘次独创和完善的，赤池信息量准则建立在信息熵的概念基础上。AIC 的计算公式如下式 5.7 所示。

$$AIC(p)=\ln|\hat{\Omega}(p)|+\frac{2n^2p}{T} \tag{5.7}$$

使用 Eviews9 进行定阶分析，建立数据组后创建 VAR 模型，选择最高为 8 阶的滞后阶数 p，依次观察信息指标 AIC，结果如下表 5.6 所示。

表 5.6 不同滞后阶数的 AIC 值

| Lag | AIC |
|---|---|
| 0 | 2.989786 |
| 1 | -6.055281 |
| 2 | -6.403564* |
| 3 | -6.336534 |
| 4 | -6.343140 |
| 5 | -6.364197 |
| 6 | -6.305604 |
| 7 | -6.365792 |
| 8 | -6.293034 |

注释：*、**、***表示显著水平为 10%、5%、1%的临界值。

根据最小值原则，应选取滞后 2 阶作为模型的滞后阶数，表示为 VAR（2）。

### 5.3.4 模型平稳性检验

VAR 模型平稳性条件与单变量自回归模型的平稳性条件一样，都是使得特征根多项式对应的行列式的根在单位圆以内。在 Eviews9 中使用特征根图形分析得到如下图 5.10 所示。

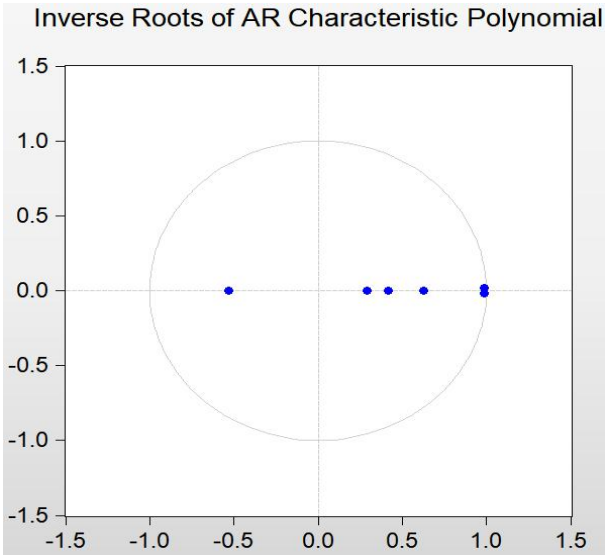


图 5.10 VAR 模型中根的图形显示

上图可见模型方程有六个特征根，包含四个实数根和两个复数根，但是最右侧点是否在单位圆内在图形上不好区分，因此用表格分析，如下表 5.7

表 5.7 VAR 模型中根模的表格表示

| Root | Modulus |
|---|---|
| 0.984635-0.015655i | 0.984659 |
| 0.984635+0.015655i | 0.984659 |
| 0.628157 | 0.628157 |
| -0.532042 | 0.532042 |
| 0.419900 | 0.419900 |
| 0.293245 | 0.293245 |

显然每个根都落在单位圆以内，因此该模型满足平稳条件。

### 5.3.5 协整检验

稳健的 VAR 模型必须以数据为前提条件，在数据序列不平稳时模型就会产生伪（虚假）回归。协整检验的目的就是检查模型包含的回归方程所体现的因果关系是否含有伪回归，即检验变量之间有无包含稳定的关系。因此非平稳序列的因果关系检验就称为协整检验。协整检验多用于考察非平稳时间序列是否存在长期稳的定协整关系。

用 Eviews9 进行协整检验，得出两个输出结果，第一个是基于迹统计的检验结果，第二个是基于最大特征根的检验结果，如下表 5.8 和表 5.9 所示

表 5.8 协整检验的迹统计结果

| Hypothesized No.of CE(s) | Eigenvalue | Trace Statistic | 0.05 Critical Value | Prob.** |
|---|---|---|---|---|
| None | 0.112322 | 24.78793 | 29.79707 | 0.1691 |
| At most 1 | 0.042946 | 6.677744 | 15.49471 | 0.6154 |
| At most 2 | 3.75E-05 | 0.005693 | 3.841466 | 0.9391 |

注释：D 表示变量经过一阶差分；*、**、***表示显著水平为 10%、5%、1%的临界值

表 5.9 协整检验的最大特征根统计结果

| Hypothesized No.of CE(s) | Eigenvalue | Max-Eigen Statistic | 0.05 Critical Value | Prob.** |
|---|---|---|---|---|
| None | 0.112322 | 18.11019 | 21.13162 | 0.1691 |
| At most 1 | 0.042946 | 6.672051 | 14.26460 | 0.5286 |
| At most 2 | 3.75E-05 | 0.005693 | 3.841466 | 0.9391 |

注释：D 表示变量经过一阶差分；*、**、***表示显著水平为 10%、5%、1%的临界值

两种检测结果都在 5%的显著性水平上拒绝接受原假设，即二者都表明不存在协整关系，因此不存在伪回归，不需要对方程进行误差修正。

### 5.3.6 Grange 因果关系检验

若是一个随机变量对另一个随便量的预测有帮助，则称前者是后者的 Grange 原因。Grange 检验首先必须证明随机变量是平稳序列,平稳性是 Grange 的前提，前文已经证明变量组序列是平稳的，因此可以进行 Grange 检验。

在 Eviews9 上运行滞后 2 阶的 VAR 模型的 Grange 检验，得到如下表 5.10。

表 5.10 Grange 因果关系检验结果

| Dependent variable: | Excluded | Chi-sq | Prob.* |
|---|---|---|---|
| DPb | DQ | 6.045593 | 0.0487** |
| | Dr | 7.567264 | 0.0386** |
| DQ | DPb | 11.348964 | 0.0164** |
| | Dr | 5.517974 | 0.0634* |
| Dr | DPb | 1.109738 | 0.5741 |
| | DQ | 2.590137 | 0.2739 |

注释：D 表示变量经过一阶差分；*、**、***表示显著水平为 10%、5%、1%的临界值。

结果显示在滞后 2 阶的 VAR 模型中，比特币算力的差分变量 DQ 对比特币兑美元汇率的差分变量 DPb 的影响显著，对一年期美元债券收益率的差分变量 Dr 影响不显著；比特币兑美元汇率的差分变量 DPb 对比特币算力的差分变量 DQ 影响显著，对一年期美元债券收益率的差分变量 Dr 影响不显著；一年期美元国债收益率的差分变量 Dr 对余下二者影响都显著。即比特币算力的差分变量与比特币兑美元汇率的差分变量存在双向 Grange 因果关系，和上一章推导相符。而此二者对一年期美元债券收益率影响不明显，是因为比特币交易的美元使用量占所有美元涉及的交易比例微乎其微，不足以撼动整个美元市场，反过来美元市场波动对比特币却有着直接明显的影响。

### 5.3.7 脉冲响应分析

由于上述过程证明了比特币兑美元汇率的差分和比特币算力的差分对一年期美元国债收益率的差分的影响不显著，因此这里仅考察 DPb 受 DQ 和 Dr 的脉冲响应，以及 DQ 受 DPb 和 Dr 的脉冲响应。在 Eviews9 中设置 10 期响应，输出结果如下图 5.11 所示。

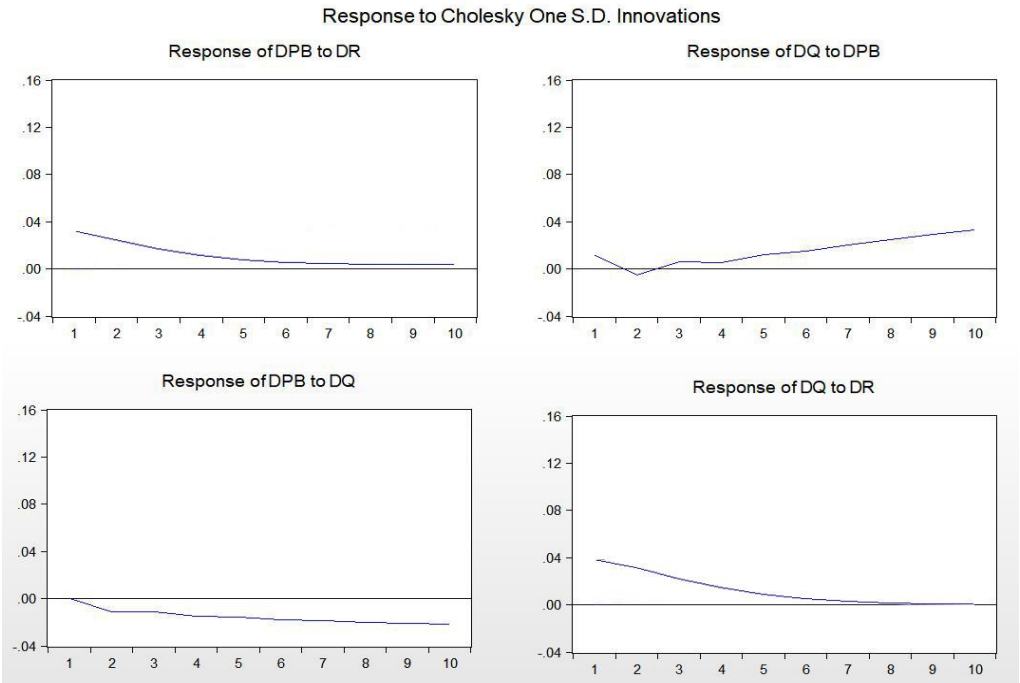


图 5.11 脉冲响应结果

DPb 和 DQ 对 Dr 的脉冲响应呈现出趋于零的现象，Dr 表示的一年期美元国债收益率作为外部变量，对比特币系统的影响是单向的，且随着时间递减，在第 10 期 Dr 脉冲扰动的影响几乎消失。DPb 和 DQ 相互间的脉冲响应呈现发散状，表明比特币系统中矿商行为和币价之间存在不断放大的影响，比特币系统在设计上没能消除内在的不稳定因素。这也是比特币价格不断剧烈波动的原因之一，进一步导致比特币无法作为一种在商品购买场景下广泛使用的货币，甚至导致作为投资类产品的比特币也存在着极大风险。

## 5.4 本章小结

比特币价格综合决定模型的实证结果中除美元指数与币价关系不显著外，其余皆与币价存在显著关系，且影响方向和模型一致。表明本文的比特币价格决定模型设置无误。比特币价格一方面受到系统内部因素诸如矿商算力、交易费用、能耗指数和交易量的影响，另一方面受到系统外部因素诸如短期资本流入、能源价格和综合利率的影响。

对比特币价格——算力的脉冲响应结果表明在不考虑其他外部因素的情况下，比特币系统内部的币价和算力存在时间上发散的相互影响，致使其内部因素成为币价剧烈波动的罪魁祸首。比特币的去中心化运行方式没能在内部设置稳定币价的机制，在外部也没有任何机构执行类似中央银行的调控措施，导致比特币价格存在天然的不稳定性。

# 第 6 章 政策建议与结论

## 6.1 比特币社区治理策略

比特币是去中心化的应用，致使监管方的天然缺位，任何导致币价波动的行为都不会受到约束。同时比特币在设计上没能消除矿商行为和币价间的不断放大的相互影响，近几年比特币价格大涨大落让它的潜在使用者望而却步，而投机者不断涌入又进一步加重了比特币价格的不稳定性。

作为标榜社区治理的比特币系统期望能通过矿商和使用者间的协议来改变现状，因此本文建议比特币矿商可以在挖出新币后持有一段时间，并向市场公布持有的总数。矿商在一定时间内持有比特币可以有效防止矿商在获取短期利益后减少算力投入，也避免矿商对通过“51%算力攻击”获取短期回报，同时投资者会视全网总算力的稳定情况而决定是否持有比特币。矿商持有比特币实际上是对算力——币价双向影响波动引入负反馈，算力受外部因素扰动时矿商可以选择持有更多比特币稳定投资者情绪从而减少币价波动，币价受外部因素扰动时由于矿商持有部分比特币而不会轻易撤出算力从而减少算力的波动。于矿商本身而言比特币价格稳定使得其自身收益稳定，于投资者而言价格稳定的比特币可以更放心的持有，两方都能获得更高效用。

## 6.2 国际联合共治策略

### 6.2.1 严密监控防止金融风险

比特币交易市场的广泛性、便捷性、隐秘性使得投机资本很容易进出该市场，比特币市场没有防止泡沫发生的机制，而其泡沫破裂对全球金融市场又有着广泛且直接的影响。此外比特币交易还给国际风险资本绕过资本管控进出一国金融市场提供了渠道，譬如在 2017 年初人民币汇率出现下跌，资金监控部门观察到有投机者在中国境内交易所购买比特币后转至境外平台出售换取外汇，这种行为躲过了对个人换汇额度及外汇审查的审查管理。中国在遏制比特币交易，防范比特币金融风险上有着杰出的成果。2017 年末之前，人民币参与比特币交易一度占到全球交易额的大半，2017 年 9 月以来，央行会同有关部门审查关闭了若干加密货币交易所和首次代币发行（ICO）融资平台，并基本实现加密货币交易无风险退出，期间全球比特币交易主权货币中的人民币份额降至 1%以下。正是这种提前打击，使得 2017 年 12 月比特币价格崩盘没有对国内金融市场造成冲击。

### 6.2.2 加强国际联管阻止非法交易

比特币的交易有一些是来自暗网的非法交易，包括洗钱、毒品、枪支和人口贩卖，线上黑市网站“丝绸之路”就是很好的例子。该网站的用户在“丝路”上可免费注册，而卖家必须购买新的账户才能入场经营；截至 2012 年为止“丝路”网站的月销售额超过 120 万美元，而其贩售物品多为毒品、枪支等违禁品，“丝路”的大部分的卖家在英国和美国，他们提供的商品包括海洛因、LSD 和大麻等。美国政府曾三次查处该网站，最后都死灰复燃。比特币交易的匿名性使得它成为一些犯罪集团的交易工具，任何地方只要有网络和基本的联网设备，都能进行比特币交易，因此国际上任何国家都很难单独对比特币进行监管。防范比特币助长犯罪，需要受其危害的国际各方组织起来，通过高端网络追踪、共享技术和信息、全球监控、联合打击、国际追逃来遏制比特币市场的非法交易。

### 6.2.3 关注区块链技术变革

比特币虽然有多种弊端，但是它的底层区块链技术却有着很宽广的应用前景。区块链技术是一个分布式账本体系，每个参与者都是记账者，每笔合法的账本变动都会在记账者之间相互广播并验证，这个账本拥有不可篡改、快捷访问的优点。升级版的区块链技术还包含了可编程的智能合约，使用者可以在自己的权限内对账户发生的交易进行编程，使得交易在条件触发时自动进行，若干使用者也可以签署一个共识协议，以实现多方自动交易。区块链的使用者在不需要相互信任的基础上就能进行突破地域限制的即时交易，可以有效简化金融行业譬如交易所和银行的业务流程，提高了金融效率。区块链在其他实体经济行业包括交通、物流、能源、医疗、软件开发等也有很多探索性的应用。我国十三五规划提出在新常态下转变经济发展模式，由外放型传统制造业向创新型知识密集产业发展，变中国制造到中国创造。十三五的创新要求离不开对区块链技术的应用和开发，有关部门应当密切关注技术变革，有效促进区块链技术新成果的研发。

## 6.3 结论

本文梳理了以比特币为代表的加密货币的历史由来和发展现状，从而提出币价和算力内在影响的问题。解释了以比特币为代表的加密货币的运行机制，并透过运行机制找到比特币价格波动的影响因素，进行实证分析。经过对比特币币价决定因素分析，对比特币矿商行为分析，和对算力与比特币价格数据的 VAR 实证过程。本文有力证明了比特币价格在短期内受到流动性投机资本影响显著，比特币价格受到矿商行为影响显著。本文还有力证明了比特币存在矿商行为与币价间

的不断放大的相互扰动，比特币在设计上有天然的内部不稳定性，这也是造成近年来现象级的币价暴涨又崩溃的原因。

交易媒介、记账单位、储存价值被普遍归纳为货币所应具备的特性，币价剧烈波动的比特币显然不具备储存价值，因此本文认为比特币不能作为一种真正的货币存在。政策建议部分，一方面提出在比特币社区治理的范畴内引入矿商持有比特币的负反馈体系，可以有效防止币价和算力的双向扩散扰动，部分解决比特币价格不稳定的问题；另一方面提出国际联合共治，有效防范突发性币价波动对经济运行造成的负面影响和涉及比特币的非法交易的存在。

虽然经过十年的发展，以比特币为代表的加密货币仍是一种新兴的网络技术，距离真正的货币应用还有很长的路要走。比特币在技术上要突破交易流量限制、51%算力攻击风险以及挖矿能耗过高等问题，监管上要建立基于国际联合共治的风险防范体系，才能利于经济运行。而经济学界对此类基于区块链技术的加密货币的理论体系也亟待完善，否则不能更好的解释和预测加密货币的本质和走向。

# 参考文献

[1]博伊尔.金钱的运作,李阳译[M].新星出版社,2005
[2]陈娟娟.数字化信用和新型互联网支付系统[J].理论探索,2014(3)14~26
[3]陈道富.王刚.比特币的发展现状、风险特征和监管建议[J].发展研究,2014(2)11~23
[4]陈岩,周烨.新型虚拟货币对国际货币体系的挑战[J].经济论坛,2015(7)27~39
[5]陈琴.比特币的属性及其对经济的影响初探[J].市场论坛,2014(2)11~19
[6]陈豪.比特币的经济学分析[D].浙江大学,2015
[7]程驰光.当前国际上主要央行对区块链技术的研究及启示[J].武汉金融2017(1)76~78
[8]褚俊虹,王琼,陈金贤.货币职能分离及其在电子货币环境下的表现[J].财政研究,2013(5)43~49
[9]邓伟,唐齐鸣.单位根相关过程：理论的发展与比较[J].经济学动态,2014(5)33~48
[10]端宏斌.比特币悖论[J].中国经济和信息化,2013(5)41~58
[11]樊云慧.比特币监管的国际比较及我国的监管策略[J].法学杂志,2016(3)15~19
[12]冯.哈耶克．货币的非国家化[M].新星出版社,1970
[13]付峥嵘,倪维立.互联网金融红利[M].人民邮电出版社,2016
[14]付蓉.数字货币监管的国际经验借鉴和启示[J].金融科技时代,2016(4)20~35
[15]高荣贵.马克思的货币理论与电子货币[J].当代经济研究,1994(6)15~20
[16]关靖远,尹文渊.比特币的货币属性及发展方向初探[J].时代金融,2014(5)11~15
[17]贾丽平.比特币的理论、实践与影响[J].国际金融研究,2013(5)19~31
[18]姜宇.论比特币法律监管[J].南华大学学报,2014(3)19~31
[19]李威.比特币的风险及其监管[J].中图,2015(6)16~27
[20]李丽琼.探讨区块链技术冲击信用证商业银行的应对与管理[D].云南财经大学,2017
[21]廖愉平.比特币市场发展阶段分析与反思[J].西部论坛,2014(1)14~25
[22]刘宁.迷局待解：比特币的风险挑战及司法应对[J].法制博览,2015(6)38~48
[23]刘道纪.中美比特币监管比较研冗[D].中国政法大学,2015
[24]马可.比特币：终究是一场泡沫[J]．哈尔滨金融学院学报,2014(6)62~71
[25]马磊.比特币不可能成为真正的货币[J].产业经济,2011(3)44~58
[26]米尔顿.弗里德曼.资本主义与自由[M].商务印书馆,2004
[27]钱意心,徐燕燕.规避管制人民币下跌中的比特币异动[N].第一财经 2014(3)
[28]师秀霞.虚拟货币洗钱风险的法律规制[D].铁道警察学院,2016

[29]孙兆东.比特币对主权货币的挑战[J].中国金融,2013(3)31~48
[30]唐平.电子货币对货币政策的影响研究[J].上海金融,2015(1)31~45
[31]王燕,周光友.比特币的货币属性分析[J].金融教育研究,2014(7)23~28
[32]肖规.警惕比特币突破外汇管制参与洗钱[OL].263 理财财富网,2017
[33]谢赤,张太原.证券投资基金投资行为对中国股市波动性影响研究[J].中国社会科学,2008(3)68~78
[34]谢杰,张建.“去中心化”数字支付时代经济刑法的选择[J].法学,2014(3)41~58
[35]许井荣.基于反洗钱视角的比特币风险控制研究[J].中国金融电脑,2014(4)26~40
[36]严伟泰.区块链中的数据加密技术分析[J].科技与信息,2017(8)132
[37]颜拥,赵俊华.能源系统中的区块链:概念、应用与展望[J].电力建设2017(2)12~20
[38]姚前,汤莹玮.关于央行法定数字货币的若干思考[J].金融研究,2017(7)78~84
[39]衣丰.中国数字货币发展研究——以比特币为例[D].对外经济贸易大学,2017
[40]尹龙.货币性质的再认识与货币供给理论的发展[J].金融研究,2002(4)13~27
[41]余宇威.基于区块链的加密代币融资模式研究[D].浙江大学,2018
[42]袁勇.区块链共识算法的发展现状与展望[J].自动化学报,2018(3)20~32
[43]张春丽.比特币监管：风险防范与信用重塑[J].中国社会科学报,2014(8)3~16
[44]张若竹.比特币法律问题研究[D].沈阳师范大学,2014
[45]郑瑜.比特币与通用货币[J].现代经济分析,2014(5)41~58
[46]中本聪.比特币：一种点对点的电子现金系统[J].Consulted,2008
[47]中国人民银行.中国金融稳定报告[R].专栏 17.比特币,2014(5)
[48]Anne H. Dyhrberg,How investible is Bitcoin? Analyzing the liquidity and transaction costs of Bitcoin markets[J].Economics Letters,2018,(8):36~42
[49]Arvind Narayanan,Bitcoin's Academic Pedigree[J].COMMUNICATIONS OF THE ACM,2017
[50]Adem Efe Gencer,On Scalability of Blockchain Technologies[D].Cornell University,2017
[51]Bruno Biais,The blockchain folk theorem[J].TSM-Research,2018
[52]Christian Hotz-Behofsits,Predicting crypto-currencies using sparse non-Gaussian,.Finance Research Letters,(1):36~42
[53]Charles W. Evans,Bitcoin in Islamic Banking and Finance[J].Journal of Islamic Banking and Finance,2015
[54]Dirk G. Baur,Bitcoin, gold and the US dollar-A replication and

extension[J].Finance Research Letters,2018,(4):22~35
[55]Dashiell C. Shapiro,Bitcoin Loans and Other Cryptocurrency Tax Problems[J]. JOURNAL OF TAXATION OF INVESTMENTS,2017,(4):30~48
[56]Daniel E. O'Leary,Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems[J]. wiley,2017
[57]Elie Bouri,On the return-volatility relationship in the Bitcoin market around the price crash of 2013[J].Economics,2017,(9):5~21
[58]Feng Mai,How Does Social Media Impact Bitcoin Value? A Test of the Silent Majority Hypothesis[J].Journal of Management Information Systems,2018
[59]Greg Maxwell,Confidential Transactions[OL].blockstream.com,2014
[60]Halvor Aarhus Aalborga,What can explain the price, volatility and trading volume of Bitcoin?[J].Finance Research Letters,2018,(6):23~39
[61]Ittay Eyal,Adem Efe Gencer,Emin Gun Sirer,Robbert van Renesse,Bitcoin-NG: A Scalable Blockchain Protocol[J].Working Papper of Cornell University,2015
[62]Jérôme Kreuser,Bitcoin Bubble Trouble[J].wilmott magazine,2017,(6):5~13
[63]Jonathan Chiu,The Economics of Cryptocurrencies - Bitcoin and Beyond[J].Queen’s Economics Department Working Paper,2017
[64]John P. Conley,Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings[J].Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings,2017
[65]Kartik Hegadekatti,K-Chains: A New Class of Blockchains and Related Turing Machines Based on Quantum Mechanics[J].Munich Personal RePEc Archive,2017
[66]Ladislav Kristoufek,On Bitcoin markets (in)efficiency and its evolution[J].Physica,2018,(2):47~60
[67]Ladislav Kristoufek,What Are the Main Drivers of the Bitcoin Price? Evidence from Wavelet Coherence Analysis[J].PLOS ONE,2015,(12):16~34
[68]Mark Holub , Jackie Johnson,The Impact of the Bitcoin Bubble of 2017 on BitcoinÕs P2P Market[J]. Finance Research Letters ,2018,(3):23~31
[69]Manmohan Singh,Leverage—A Broader View[R].IMF Working Paper,2018,(1):33~64
[70]Michal Polasik,Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry[J].International Journal of Electronic Commerce,2016,(7):42~65
[71]Nijolė Valinskytė,Leverage Ratio as a Macroprudential Policy Instrument[J].

Lietuvos bankas,2018,(8):52~67
[72]Oscar Jorda,Leveraged Bubbles[BD].2018
[73]Ole Peters,Leverage efficiency[R].London Mathematical Laboratory,2017,(1):25~42
[74]Pavel Ciaiana,The economics of BitCoin price formation[J].Applied Economics,2016,(4):20~33
[75]Ross C. Phillips,Cryptocurrency price drivers: Wavelet coherence analysis revisited[J].PLOS ONE,2018,(11):26~40
[76]Ross C. Phillips,Cryptocurrency price drivers: Wavelet coherence analysis revisited[J].PLOS ONE,2018,(9):15~29
[77]Ryan Derousseau,Why the Air Is Coming Out of the Bitcoin Bubble[OL]. MONEY.COM,2018,(5):36~42
[78]state space models[D].WILEY,2018
[9]Shaen Corbeta,Datestamping the Bitcoin and Ethereum bubbles[J].Finance Research Letters,2018,(7):24~33
[79]Tony Klein,Bitcoin is not the New Gold-A comparison of volatility, correlation, and portfolio performance[J].International Review of Financial Analysis,2018,(4):13~25
[80]Tetsuya Takaishi,Statistical properties and multifractality of Bitcoin[J].Physica A,2018,(4):67~74

# 致谢

本文从 2017 年初定题到 2019 年初定稿经历了整整两个冬夏，笔者对比特币代表的加密货币从仅有耳闻到全翻理解的过程离不开导师喻国平教授的引导。喻老师在国外访学期间为笔者搜罗整理了大量关于加密货币的前沿文章，回国后悉心指导，定期安排学术研讨，使得笔者在本领域的学术水平获得极大精进。在此感谢喻国平老师付出的努力和耐心！

感谢笔者的女友朱梦莹！在论文写作期间，她不厌其烦的帮助我修改论文格式，讨论写作用语。并在生活上对我照顾周到，使我能专注于学术而不用分心其他琐碎事务。

感谢江西财经大学经济学院的领导和老师们！感谢杨飞虎院长、陆长平院长、袁庆明教授、封富育教授和龚立新教授对笔者的论文提出宝贵的修改意见！经过一次开题和三次答辩，论文从空有概念到论述有序，老师们从各个角度提出的意见是我前进路上的指南针。

最后感谢同门师弟和经院同学！感谢陈志愉同学、罗同同同学、叶际彬同学、钟孝江同学、余婷同学！感谢室友李擎和吴亚平！与你们的交流和讨论使我的学术研究路线越发清晰，多亏了你们对我的提醒，让我注意到论文的不足之处。

JIANGXI UNIVERSITY OF FINANCE AND ECONOMICS
1923
江西财经大学