

分类号：  
U D C :

密级：  
学号：

南昌大学专业学位硕士研究生  
学位论文

**数字加密货币市场风险分析—以比特币、以太币为例**

**Risk Analysis of Cryptocurrency Market - Bitcoin and Ethereum**

黄洛

培养单位（院、系）：经济管理学院

指导教师姓名、职称：王玉帅 副教授

指导教师姓名、职称：

专业学位种类：金融硕士

专业领域名称：

论文答辩日期：

答辩委员会主席： 肖山俊

评阅人： 杨伊

肖强

年 月 日

## 一、学位论文独创性声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。据我所知，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过的研究成果，也不包含为获得南昌大学或其他教育机构的学位或证书而使用过的材料。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谢意。

学位论文作者签名（手写）: 黄洛

签字日期: 2020 年 6 月 10 日

## 二、学位论文版权使用授权书

本学位论文作者完全了解南昌大学有关保留、使用学位论文的规定，同意学校有权保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权南昌大学可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编本学位论文。同时授权北京万方数据股份有限公司和中国学术期刊（光盘版）电子杂志社将本学位论文收录到《中国学位论文全文数据库》和《中国优秀博硕士学位论文全文数据库》中全文发表，并通过网络向社会公众提供信息服务，同意按“章程”规定享受相关权益。

学位论文作者签名（手写）: 黄洛

导师签名（手写）: 陈伟

签字日期: 2020 年 6 月 10 日

签字日期: 2020 年 6 月 10 日

|        |                         |    |              |      |  |
|--------|-------------------------|----|--------------|------|--|
| 论文题目   | 数字加密货币市场风险分析—以比特币、以太币为例 |    |              |      |  |
| 姓名     | 黄洛                      | 学号 | 415436617442 | 论文级别 | <input type="checkbox"/> 博士 <input checked="" type="checkbox"/> 硕士 |
| 院/系/所  | 经济管理学院                  | 专业 | 金融专硕         |      |  |
| E-mail |                         |    |              |      |  |
| 备注:    |                         |    |              |      |  |

公开  保密（向校学位办申请获批准为“保密”，\_\_\_\_\_年\_\_\_\_月后公开）

## 摘 要

自从 2008 年中本聪提出比特币概念，大量的加密货币不断涌现，加密货币的价格也不断暴涨暴跌。大量的投资者疯狂地涌入加密货币市场，希望能够在这狂热的市场中分得一杯羹。但是这些投资者们却忽视了加密货币背后的潜在风险，对于加密货币发展全貌、市场风险的大小和成因知之甚少，进而对加密货币做出了错误的判断和投资选择。

本文旨在系统地分析加密货币的市场风险。首先，本文介绍了加密货币的相关概念和技术原理，并详细展现比特币和以太币的技术特点。其次，从产业链和监管两个角度，对数字加密货币进行现状研究。不仅从宏观视角分析了数字加密货币产业链发展情况，以上中下游三个环节视角切入产业链发展的现状和困境，而且梳理了当前各国对加密货币的监管态度。进而，微观聚焦至比特币和以太币两个主要的加密货币，详细分析了两者的发展历程、特征和应用变化。并且，以比特币和以太币为例，引入 GARCH-EVT 方法度量两者的价格风险，在以 Kuipiec 回测方法对比检验该方法的精确度。进而，再针对加密货币市场风险，从市场供给两侧以及投资者主观层面分析其风险成因。最后，结合前文分析，从宏观监管者层面到微观参与者层面，提出相应的风险应对建议，希望让加密货币的参与者对于加密货币市场风险有一个全面的认知和了解，做好风险应对，营造一个良性的加密货币市场环境。

**关键词：** 加密货币，比特币，以太币，市场风险

## ABSTRACT

---

## ABSTRACT

Since Satoshi Nakamoto proposed the concept of Bitcoin in 2008, a large number of new cryptocurrencies have continuously emerged, and the price of cryptocurrencies have also skyrocketed and plunged. A large number of investors have poured into the cryptocurrency market frantically, hoping to get a great share of this frenzy market. However, having little knowledge about the overall development of cryptocurrencies, the size and causes of market risks, these investors have overlooked the potential risks behind cryptocurrencies and have made wrong judgments and investment choices about cryptocurrencies.

This article aims to systematically analyze the market risk of the cryptocurrency . Firstly, this article introduces the relevant concepts and technical principles of cryptocurrencies, and shows the technical characteristics of Bitcoin and Ethereum in detail. Secondly, from the macro perspective, the development of the digital cryptocurrency industry chain is analyzed. At the same time, it sorts out the current regulatory attitudes of various countries towards cryptocurrencies. Furthermore, it focused on the two major cryptocurrencies, Bitcoin and Ethereum, and analyzed the development process, characteristics and application changes of the two in detail. And, taking Bitcoin as an example, the GARCH-EVT method is introduced to measure the price risk of Bitcoin, and the accuracy of this method is compared with the Kuipiec backtest method. Furthermore, the causes of risk are analyzed from both sides of the market supply and the subjective level of investors. Finally, combined with the previous analysis, this article proposes corresponding risk response suggestions from the level of macro regulators to the level of micro participants.

**Key Words:** Cryptocurrency, Bitcoin, Ethereum, Market risk

## 目 录

|                           |    |
|---------------------------|----|
| 第1章 绪论 .....              | 1  |
| 1.1 研究背景与意义 .....         | 1  |
| 1.1.1 研究背景 .....          | 1  |
| 1.1.2 研究意义 .....          | 3  |
| 1.2 文献综述 .....            | 4  |
| 1.2.1 对数字加密货币研究 .....     | 4  |
| 1.2.2 对数字加密货币市场风险研究 ..... | 6  |
| 1.2.3 文献述评 .....          | 7  |
| 1.3 研究思路和方法 .....         | 8  |
| 1.3.1 研究方法与思路 .....       | 8  |
| 1.3.2 研究框架 .....          | 9  |
| 1.4 研究内容和创新 .....         | 10 |
| 1.4.1 研究内容 .....          | 10 |
| 1.4.2 本文创新点 .....         | 10 |
| 第二章 基本概念和相关理论基础 .....     | 12 |
| 2.1 数字加密货币的相关概念 .....     | 12 |
| 2.1.1 数字加密货币的概念 .....     | 12 |
| 2.1.2 比特币的概念 .....        | 14 |
| 2.1.3 比特币的基本技术原理 .....    | 15 |
| 2.1.4 以太币的概念 .....        | 17 |
| 2.1.5 以太币的基本技术原理 .....    | 18 |
| 2.2 加密货币的相关理论基础 .....     | 19 |
| 2.2.1 哈耶克的货币非国家化理论 .....  | 19 |
| 2.2.2 弗里德曼的货币数量论 .....    | 20 |
| 2.3 市场风险度量相关理论基础 .....    | 20 |
| 2.3.1 VaR 值理论 .....       | 20 |
| 2.3.2 极值理论 .....          | 23 |
| 第三章 数字加密货币发展概况 .....      | 25 |
| 3.1 数字加密货币产业链 .....       | 25 |
| 3.1.4 采矿部门 .....          | 25 |
| 3.1.1 交易平台 .....          | 26 |
| 3.1.3 支付部门 .....          | 29 |
| 3.2 数字加密货币监管现状 .....      | 31 |
| 3.2.1 世界各国监管程度 .....      | 31 |
| 3.2.2 中国监管政策 .....        | 32 |
| 3.2.3 美国监管态度 .....        | 34 |

## 目录

---

|                               |           |
|-------------------------------|-----------|
| 3.2.4 欧盟监管政策 .....            | 35        |
| 3.3 比特币的发展现状 .....            | 37        |
| 3.3.1 比特币的发展历程 .....          | 37        |
| 3.3.2 比特币的应用变化 .....          | 39        |
| 3.3.3 比特币的主要特征 .....          | 41        |
| 3.4 以太币的发展现状 .....            | 44        |
| 3.4.1 以太币的发展历程 .....          | 44        |
| 3.4.2 以太币的应用变化 .....          | 46        |
| 3.4.3 以太币的主要特征 .....          | 49        |
| 3.4.4 比特币和以太币的对比分析 .....      | 50        |
| <b>第四章 数字加密货币市场风险度量 .....</b> | <b>52</b> |
| 4.1 数据来源 .....                | 52        |
| 4.2 数据检验 .....                | 52        |
| 4.2.1 正态性检验 .....             | 52        |
| 4.2.2 平稳性和自相关检验 .....         | 54        |
| 4.3 GARCH-VaR 模型 .....        | 56        |
| 4.3.1 滞后阶数选取 .....            | 56        |
| 4.3.2 模型参数估计 .....            | 56        |
| 4.4 GARCH-EVT-VaR 模型 .....    | 58        |
| 4.4.1 模型构建方法 .....            | 58        |
| 4.4.2 模型应用 .....              | 59        |
| 4.5 Kuipiec 回测检验 .....        | 62        |
| 4.5.1 比特币回测结果 .....           | 63        |
| 4.5.2 以太币回测结果 .....           | 64        |
| 4.6 实证结论 .....                | 65        |
| <b>第五章 风险成因和风险应对建议 .....</b>  | <b>66</b> |
| 5.1 数字货币市场风险成因分析 .....        | 66        |
| 5.1.1 发行机制缺乏灵活性 .....         | 66        |
| 5.1.2 市场集中度过高 .....           | 68        |
| 5.1.3 投机需求旺盛 .....            | 69        |
| 5.1.3 政策环境的变化 .....           | 71        |
| 5.2 风险应对建议 .....              | 72        |
| 5.2.1 宏观监管层面 .....            | 72        |
| 5.2.2 微观参与者层面 .....           | 74        |
| <b>第六章 结论与展望 .....</b>        | <b>76</b> |
| 6.1 结论 .....                  | 76        |
| 6.2 研究展望 .....                | 77        |
| 致谢 .....                      | 78        |
| 参考文献 .....                    | 79        |

## 第1章 绪论

### 1.1 研究背景与意义

#### 1.1.1 研究背景

中国互联网基础资源行业不断壮大发展，推动前沿技术不断创新，互联网行业交流愈发频繁，互联网也在规范有序发展。数字加密货币也正是在互联网蓬勃发展的宏观大环境中应运而生。在这背景下也衍生出三种不同的数字网络货币：电子货币、虚拟货币以及数字加密货币。

电子货币实质上是法定货币的电子化记账形式，如“微信”、“支付宝”、“银行卡”中记载的数字，代表着实际的纸质货币，其地位也与法定货币相同，适用国家法律规范的各类金融与货币政策。

虚拟货币又分为与法定货币相关的部分网络运营商提供的币，和与法定货币无关的积分或金币。网络运营商提供的某些币可由法定货币兑换而来，在指定的范围内能够进行购买交易活动，换取特定商品，但这种兑换是单向的，通常无法再兑换回法定货币。而与法定货币无直接联系的积分或金币，有时可用于兑换实际商品，但其通常只作为一种促销手段，与法定货币无关。

而数字加密货币理论上是一种可以与法定货币互换的数字资产，人们通过加密钱包地址对数字加密货币进行交易投资，但是目前在我国，数字加密货币还不具有与法定货币同等的地位。

货币在市场经济的发展中由以物易物交换而自然而然的产生，社会生产交易对货币的选择不断适应着市场经济的发展，货币作为一般等价物的形态也在随之改变，从最原始的贝壳形态到金银，再到现代发展的信用货币，甚至是脱离实体的电子货币，货币作为一种交易媒介，提高了物物交换的效率，促进了更大范围的经济活动。法定货币以国家公信力为支撑，一般不存在信用风险，但是其不可避免的面临通货膨胀的威胁。比如 2008 年美国次贷危机所引发的全球性金融危机，美国“雷曼兄弟”宣布破产，政府不断增发国债及美元使得美元不断缩水贬值。

数字加密货币研究所处背景可以从理论、技术、宏观背景三方面进行总结。

理论背景而言，经济学家哈耶克在《货币的非国家化》中驳斥了国家对货币拥有垄断权力的固化思维，他认为应当废除中央银行制度，允许私人发行货币并自由竞争，由此产生适合市场的最优货币；这一想法的诞生在一定程度上为阻止政府肆意发行货币提供的思路。

从技术背景来说，密码学的应用与发展为数字加密货币的诞生创造了条件，密码学家戴维创造的 B-Money，一种匿名式分布电子现金系统，无法被政府控制，也难以被机构监管。

从时代背景来说，2008 年 9 月，以美国四大投行之一的“雷曼兄弟”倒闭为开端，美国金融危机爆发，并迅速向全世界蔓延。美国政府采取量化宽松等政策，不断增发美元以达到刺激经济的目的，由此引发人们对政府采取的经济措施合理性的广泛讨论。人们不再满足于由政府主导的传统中心化记账方式，由此产生的信赖危机促使人们寻求不依赖于第三方金融机构参与的独立货币系统，数字加密货币应运而生。

数字加密货币的产生有利有弊，一方面它独立于政府权力和传统金融机构发行，相比于传统法定货币，具有去中心化及难以被篡改的优势，数字加密货币的使用者能以更低的交易成本完成更高效的交易活动；另一方面，由于去中心化导致数字加密货币不受任何政府或机构监管，存在一定程度上的法律风险问题。

实际社会中，数字加密货币的技术并不成熟，相关的社会监管仍存在较大漏洞，利用数字加密货币进行违法犯罪活动的案例也时有发生，相关的安全性还有待进一步提高。法律与监管的双重缺失，加之数字加密货币市场的迅猛发展，足以引起人们的重视，以保障相关数字加密货币持有者的合法正当权益。

积极了解并接纳数字加密货币所运用的新技术的原理，明白加密货币的市场风险，有利于规范数字加密货币的监管，解决现实社会中存在的风险及问题，引导新事物进一步为经济活动服务，形成更加良性的数字加密货币发展业态。

### 1.1.2 研究意义

数字加密货币作为一项特殊的虚拟金融投机标的物，与互联网有紧密而深刻的联系，既产生于互联网，又依托于互联网不断发展更新，研究有实践及理论两方面的意义。

从实践角度而言，由于市场尚未成熟，投资者对数字加密货币的认识并不清晰全面，对其潜在的市场风险及成因认识也不清晰。对数字加密货币的投资者来说，数字加密货币仍处于波动震荡的市场中，价格变动起伏较大，投资者在未把握数字加密货币市场风险点时盲目投资，容易蒙受巨大的资金损失。而本文通过具体分析研究数字加密货币的风险成因，有利于投资者明悉风险点，更好的应对风险以作出投资决策。

对监管方来说，由于数字加密货币的本质特性，其交易不受地域限制，交易活动在国际范围内自由流通，各国就交易资金的来源、流向管控在现实监控中也存在着较大难度，把握数字加密货币的产业链能在一定程度上帮助监管者进行资金监管活动。除此之外，也有助于政府或其他监管机构规范数字加密货币市场的种种交易活动，针对现存的违法行为采取措施进行处罚并深入解决违法风险隐患，以使得市场进一步良性发展。

即使是未参与数字加密货币市场的普通民众，在现实生活中可能也都对“比特币”、“区块链”等热词略有耳闻，人们的日常生活离不开互联网技术，却又对新兴数字加密行业了解甚少，通过深入研究数字加密货币的市场风险，有助于普通大众消除对数字加密货币的误解，揭开新技术的“神秘”面纱，既可以避免投资者盲目跟风进入市场，也有利于促进数字加密货币市场的进一步发展。

理论上，数字加密货币基于网络支付系统及虚拟计价工具，相比于传统货币其具有去中心化、匿名性和稀缺性等特点，在一定程度上更有益于被市场所接受信任，数字加密货币的发展伴随着互联网的不断升级与创新，数字加密货币行业不断壮大，丰富了区块链等新技术的领域及密码学等知识领域的应用。

## 1.2 文献综述

### 1.2.1 对数字加密货币研究

#### 1.2.1.1 数字加密货币整体性研究

国内外数字加密货币的研究主要针对于加密货币的内涵和特征、货币属性探讨、监管以及对于金融体系的影响等方面。

在对数字加密货币内涵和特征方面，周光友（2015）认为电子货币是由分散的发行主体发行的，交易更加隐秘，过程更加安全，成本更加低廉的虚拟化电子化的货币<sup>[1]</sup>。谢平等（2013）认为电子货币是能够存储于电子设备，以虚拟账户代表货币价值的货币<sup>[2]</sup>。李志杰等（2017）认为数字货币是一种基于节点网络和数字加密算法的虚拟货币，呈现出电子化、网络化、数字化的特征<sup>[3]</sup>。戴文桥（2020）通过研究我国数字加密货币的发展过程，指出应用数字加密货币的优势，即不可篡改及去中心化的特征，相较于传统货币更加安全可靠；依托于互联网和云计算，能大幅降低交易成本，提高持有者的消费意愿；提高市场反馈的准确性，有利于在国家层面进行宏观调控<sup>[4]</sup>。

在对加密货币的货币属性探讨方面，国内外学者都对此有较大的争议。Wallace（2011）<sup>[5]</sup>和 Grinberg（2012）<sup>[6]</sup>认为电子货币虽然目前仍然应用于灰色地带，但是其效率高、成本低的特点能够使其成为未来商业世界的潜在支付方式。Swan（2015）在其书中认为，数字货币已经能够在货币交易中承担起三个职能，即交换媒介、交易软件、记账工具，因而能够给未来货币发展提供更多可能性<sup>[7]</sup>。但是，大多数的学者却不认可数字加密货币的货币性。Surda(2012)认为比特币的内在价值不稳定，其价值更多取决于市场和使用者的信任，而不同于传统货币价值来自于权威国家机构背书，因而比特币的货币价值无法被保证<sup>[8]</sup>。Yermack（2015）认为比特币价格波动大，同时无法为正常的商业合同计价，因而更多是一种投机性工具而非货币<sup>[9]</sup>。Hanley（2015）<sup>[10]</sup>和 Alstyne（2014）<sup>[11]</sup>认为比特币只是一种投机性商品，不具有任何的货币属性，其价值纯粹是投机者推动的市场价值。

在针对数字加密货币监管层面，各学者提出了不一样的监管建议。Hofert E（2019）研究强调了分布式协调与数字加密货币之间的相互关系，以理解新货币现象的功能，并且提出基于技术的金融服务监管以建立完整性标准。研究重点介

绍了当前欧盟监管制度的缺陷，尤其是金融服务、支付服务和电子货币监管框架的缺陷<sup>[12]</sup>。庄雷等（2019）结合数字加密货币的发行模式及机制特点，探讨在私人化与法定化两种发行模式下，数字加密货币的发行风险及监管对策<sup>[13]</sup>。Peter Van Valkenburgh（2017）构建出针对数字加密货币进行证券监管的框架，该框架基于投资合同的 Howey 检验及证券监管的基本政策目标<sup>[14]</sup>。Sarah Jane Hughes 等（2014）回顾了自 2013 年数字加密货币及其交易者的发展现状，并结合支付系统、反洗钱、经济制裁和消费者保护法规对数字加密货币进行了评估。研究中涉及交易者对匿名性和安全性的要求，讨论了数字加密货币的技术如何使用于支持其他支付方式和电子商务<sup>[15]</sup>。

### 1.2.1.2 比特币的相关文献研究

当前针对比特币的研究主要集中于对比特币市场特征、市场价格波动和风险研究等方面。Nakamoto（2008）在提出比特币理论时候就将比特币定义为一个可以点对点交易的电子货币，为后续比特币研究提供了重要参考<sup>[16]</sup>。

由于比特币价格波动剧烈，国内外学者对于研究比特币价格行为有着浓厚的兴趣。曾莹莹（2019）通过理论分析与数据仿真，探索比特币价格行为机理，得出交易者的非理性情绪及重大事件对比特币价格影响较大，噪音交易者对比特币价格有助长助跌效应，挖币成本上升也抬高了比特币的市场价格<sup>[17]</sup>。邓伟（2017）运用正态分布检验及 sup ADF 检验等多种方法，从价格背离性和爆炸性的角度研究比特币价格泡沫，研究认为比特币是一种完美的金融投机对象，其优点被过度夸大导致价值高估，可能存在市场操纵<sup>[18]</sup>。闫方玲等（2018）理论上分析了国家政策、自身需求对比特币价格的影响，实证中分析了汇率以及投资工具黄金、股票对比特币价格的影响，研究结果指出比特币价格的波动不受单一投资工具的影响<sup>[19]</sup>。Kalyvas A 等（2019）研究认为经济不确定性与比特币价格崩盘风险呈显著负相关关系，即经济不确定性高时，比特币的崩盘风险低；而行为因素与比特币价格暴跌风险之间关系微弱，表明投资者可以通过投资比特币来对冲经济不确定性<sup>[20]</sup>。因而，大部分学者认为比特币的价格暴涨都有投资者投机心理的助推。

### 1.2.1.2 以太币的相关文献研究

以太币作为近些年备受关注的新型数字加密货币，当前学者的关注点更多是以太坊在未来的技术应用前景。

Wood（2014）在以太坊黄皮书中正式提出了新一代加密货币系统以太坊的

技术设想和架构，将以太币定义为一个受比特币启发的去中心化的公用区块链网络<sup>[21]</sup>。

而以太坊提出的智能合约概念备受学者关注和研究。Atzei (2017) 等肯定了以太坊是作为智能合约框架的内在技术价值，同时也分析了以太坊智能合约的潜在安全漏洞，这些漏洞能够使对手窃取金钱或造成其他损失<sup>[22]</sup>。Grishchenko 等 (2018) 认为在以太坊上运行的智能合约能够在分布式的环境中无需任何第三方就可以自动执行金融交易，这点使得智能合约具备长期的发展价值，但是其安全性仍然值得考量<sup>[23]</sup>。

当前针对以太币，国外学者更多将目光投向其未来应用上，肯定其智能合约的应用价值，但是对其安全性也提出了相应的怀疑。国内对以太坊和以太币的研究稍显不足。

### 1.2.2 对数字加密货币市场风险研究

当前对加密货币市场风险研究主要聚焦于对比特币这单一货币的风险研究，并且主要用定性和定量两种方法研究加密货币风险。

在对加密货币风险定性研究方面，刘刚等 (2015) 通过事件研究法，探讨中美政策信息对比特币价格波动的影响，实践表明比特币价格剧烈波动，无法发挥货币的基础职能——价值尺度，其“合法货币地位”难以被市场认可，政策风险和市场风险较大<sup>[24]</sup>。

练雅祺 (2019) 分析认为数字加密货币价格高频大幅波动是其主要的市场风险之一，其次挖币成本不断攀高也是不容忽视的成本风险，加之，数字加密货币不以实体经济做支撑，本质上是不具有价值的，这也使得其存在一定的信用风险，最后，现有数字加密货币市场上存在许多违法交易乱象也值得引起人们的关注，网络安全漏洞也值得人们进一步针对性处理<sup>[25]</sup>。

Trucios C (2019) 研究了数字加密货币风险衡量的可预测性，并运用多种波动模型比较波动性与比特币风险价值的可预测性，结果表明在预测波动率和评估风险价值时，稳健的程序要优于非稳健的程序，离群值在比特币风险度量中起着重要作用<sup>[26]</sup>。Octavian Nica 等 (2017) 在报告中回顾了数字加密货币的潜在利益和风险，并介绍了其在当前市场交易中的用法<sup>[27]</sup>。

在对比特币的市场风险度量方面，郭文伟、刘英迪等 (2018) 运用条件风险

自回归模型（CAViaR）和极值理论（EVT）组合模型，测算比特币价格波动的极端风险并分析描述风险演化的模型，得出比特币市场存在结构性突变点和显著的“自我增强”特征，在不同子区间不存在统一的市场风险演化模型，同时还比较了中美两国监管政策对比特币市场风险的影响<sup>[28]</sup>。

Zhai Y 等（2019）选取 2012 至 2016 年以美元标价的比特币市场数据进行实证研究，发现收益率序列具有尖峰厚尾、波动集聚等特征，相比于 GARCH-t 模型，用 GEV 模型拟合收益率尾部分布能更精确衡量比特币市场风险<sup>[29]</sup>。

Troster V 等（2019）研究发现具有重尾分布的 GAS 模型可以为比特币收益和风险建模提供最佳的样本外预测和拟合优度属性，对于风险管理者和投资者，在最佳对冲或投资策略中使用比特币具有重要意义<sup>[30]</sup>。

### 1.2.3 文献述评

虽然数字货币的发展仅有短短十二年的时间，但是其发展的迅猛程度伴随着其价格的不断上涨而被不断助推。从 2008 年中本聪提出比特币概念，到如今加密货币市场大量加密货币不断涌现，学者们也是不断的调整着对于加密货币的研究重点和方向。在早期，学者们的研究主要是针对比特币的属性界定，探讨其是否具备内在价值。之后随着比特币等加密货币的价格暴涨，对其价格泡沫，价格波动背后的原因和风险研究也层出不穷。而后，众多数字加密货币的不断涌现，学者们开始聚焦于新型货币们真实的应用价值和未来前景。因而前人对于加密货币的认识和对加密货币风险的研究已经十分成熟和完备。但是，国内对于加密货币的风险研究主要聚焦于比特币这一最初的加密货币，同时对于后来的新型加密货币的实际应用价值关注不够。因此，本文以加密货币的市场风险为研究对象，通过展现比特币和以太币发展的产业链，分析加密货币的市场风险，同时基于极值理论度量加密货币的市场风险大小，进而针对其市场风险探求其背后的风险成因。

## 1.3 研究思路和方法

### 1.3.1 研究方法与思路

本文主要采用了比较分析法、定性分析法、定量分析法和历史分析法等研究方法。

本文首先采用了定性分析法针对加密货币的相关、相关技术原理和特征概念进行阐述，同时对比特币和以太币的相关概念进行定性分析。其次，运用历史分析法对两种加密货币的价格走势和发展脉络进行回顾。再而利用比较分析法，对国内外的监管政策进行比较分析。最后利用定量分析法对比特币的市场风险进行量化分析。

本文的结构安排如下（图 1.1）：

第一章先概述研究的背景与意义，其次介绍本文的研究方法和思路，然后介绍国内外研究现状，最后阐述本文的创新点和不足。

第二章主要阐述加密货币的相关概念和理论，首先介绍加密货币的基本含义和分类，其次详细介绍比特币和以太币的定义以及技术原理，最后再阐述了加密货币的相关理论和市场风险度量方法的理论基础。

第三章主要介绍加密货币的发展概况，首先宏观上梳理加密产业链情况以及分析了当前国内外的监管现状，最后再微观上描述比特币和以太币特征、发展历程、交易现状和应用变化。

第四章主要以比特币和以太币为例，度量加密货币的市场风险。首先分别使用 GARCH-VaR 和 GARCH-EVT-VaR 模型量化以太币和比特币的市场风险，再对两个模型进行回测。

第五章主要分析市场风险成因进而提出风险应对建议。首先对市场风险分析结果，从供给侧、需求侧、加密货币技术缺陷、投资者等角度分析影响数字加密货币波动的因素，然后提出风险应对建议。

第六章结合上文，得出研究结论与展望。

### 1.3.2 研究框架

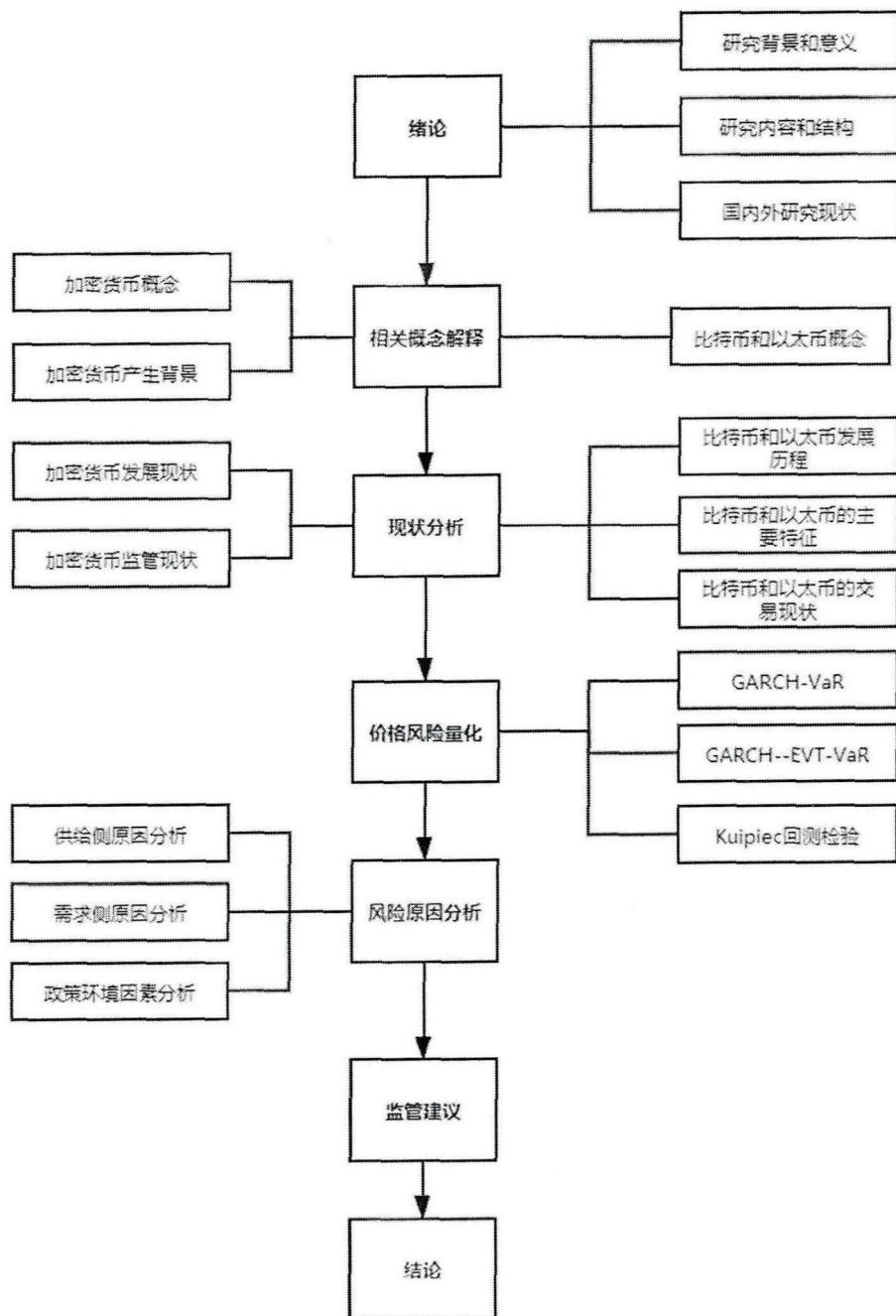


图 1.1 论文结构图

## 1.4 研究内容和创新

### 1.4.1 研究内容

本文的研究对象是数字加密货币的市场风险。为了更好的分析已有的数字加密货币的市场风险，法定数字加密货币并没有被纳入到此次的研究范围。同时为了更好的分析加密货币的市场风险，本文选取了比特币和以太币两种加密货币市场上最为主要的两种货币作为主要的研究对象，剖析加密货币的市场风险。

本文首先针对加密货币相关概念和技术原理进行界定，同时总结前人对于加密货币市场风险度量的理论经验。

其次，从产业链和监管两个角度，对数字加密货币进行现状研究。不仅从宏观视角分析了数字加密货币产业链发展情况，以上中下游三个环节视角切入产业链发展的现状和困境。而且，梳理了当前各国对加密货币的监管态度。进而，微观聚焦至比特币和以太币两个主要的加密货币，详细分析了两者的发展历程、特征和应用变化。

再者，以比特币和以太币为例，引入 GARCH-EVT 方法度量两者的价格风险，在以 Kuipiec 回测方法对比检验该方法的精确度。进而，再针对加密货币市场风险，从市场供给两侧以及投资者主观层面分析其风险成因。最后，结合前文分析，从宏观监管者层面到微观参与者层面，提出相应的风险应对建议。

### 1.4.2 本文创新点

本文创新点主要在以下方面：

#### 1. 风险度量方法的创新

针对比特币价格波动剧烈且存在许多极端值的情况下，创新性将 GARCH 方法和极值理论相结合以估计比特币的 VaR 值；

#### 2. 加密货币产业链的梳理

本文联系目前加密货币发展的实际情况，根据加密货币参与主体，清晰的梳理了加密货币产业链的各个环节发展情况，展示了加密货币产业全貌；

#### 3. 新角度切入比特币分析

通过横向对比以太币和比特币的发展历程和主要特征，清晰的展示了两个

货币的发展优劣势，以及未来发展前景。

#### 4. 供需角度分析市场风险原因

通过分析加密货币供给和需求两侧的现状，详细的解构了加密货币市场风险的影响因素。

## 第二章 基本概念和相关理论基础

### 2.1 数字加密货币的相关概念

#### 2.1.1 数字加密货币的概念

##### 2.1.1.1 数字加密货币的含义

互联网技术的不断更迭发展，不仅深深影响着人们的生活方式，而且推动着互联网金融业的蓬勃发展，由此产生的数字加密货币以其新颖的架构设计和飞涨的价格得到了投资者广泛的关注。

国际清算银行将数字加密货币定义为以数字形式表现的价值，透过数据交易实现流通、记账及价值储存等功能的货币<sup>[31]</sup>。欧洲银行管理局认为数字加密货币虽不与法定货币挂钩，也并非央行或公共当局发行，但被市场认可接受，也能以电子形式存储或交易<sup>[32]</sup>。国际货币基金组织的报告指出，数字加密货币是且以电子形式呈现，并以此实现价值交换、存储等多种功能的，能够衡量价值的数字化表示<sup>[33]</sup>。

因而本文总结以上观点，将数字加密货币定义为，基于于 P2P 网络与密码学，以互联网为载体，不依托于任何实物，运用密码学技术理论提供安全保障，能够实现交易媒介功能的数字资产。

##### 2.1.1.2 数字加密货币的分类

比特币被视为世界上第一种也是迄今为止最为主要的数字加密货币，其概念由中本聪于 2008 年 11 月 1 日最先提出，比特币是可以依据特定算法，实现点对点支付的货币系统。而后在比特币的基础上，不断有新的数字货币涌现。

根据数字货币所依赖技术，数字加密货币可以分类为以下三种：一种是以比特币为典型的第一代区块链技术，将数据及信息存储于共享数据库中，基于互联网 P2P、加密技术、区块链技术等架构电子资金系统；另一种是围绕智能合约的以太坊（Ethereum）技术，通过搭建具有开放源的公共区块链平台，及其智能合约功能，运用专用加密货币——以太币处理点对点合约；最后一种是以物联网区

块链交易为代表的 IOTA 技术，即新型大数据架构，设定基于 AI 生态下的标准数据模型，并据此提高整体计算效率。

自 2011 年开始，数字加密货币不断引起广泛关注，随之出现各种模仿比特币的数字加密货币。莱特币于 2011 年秋季发布，并在比特币之后获得了最高的加密货币市值，直到 2014 年 10 月 4 日被瑞波币取代。莱特币在比特币基础上修改了相关协议条款，以更合适的想法提高了交易速度以适应日常交易活动。瑞波币于 2013 年推出，运用了一种完全不同于比特币的模型，目前市值排名第三。点点币（Peercoin）也是数字加密货币进化链中另一个值得注意的数字加密货币，它利用革命性的技术发展来保护和维持其货币发展。点点币将比特币和莱特币使用的 PoW 技术与其自身的权益证明（PoS）机制相结合，以采用混合网络安全机制。

表 2.2 市值排名靠前的加密货币特征

| 新币种            | 特征描述  |
|----------------|---|
| ETHEREUM       | 分散的计算平台，具备独特的图灵完备的编程语言。区块链记录由每个参与节点运行和执行的脚本或合同，并通过使用本机加密货币“以太币”进行付款来激活。以太坊于 2015 年正式启动，引起了许多开发商和机构参与者的浓厚兴趣。             |
| DASH           | 2014 年初推出的以隐私为中心的加密货币，自 2017 年初以来，最近市值已大幅增长。与大多数其他加密货币相比，矿工和“主节点”之间平均分配了区块奖励，收入的 10% 到“资金”以资助开发，社区项目和营销。                |
| MONERO (XMR)   | 旨在通过使用环签名，机密交易和隐身地址来提供匿名数字现金以混淆交易硬币的来源，交易金额和目的地的加密货币系统。它于 2014 年推出，2016 年市值大幅增长。  |
| RIPPLE (XRP)   | 此列表中只有没有区块链而是使用“全球共识分类帐”的加密货币。大型银行和金融服务公司等机构参与者都使用 Ripple 协议。本机令牌 XRP 的功能是充当很少交易的本国货币对之间的桥梁货币，并防止垃圾邮件攻击。                |
| LITECOIN (LTC) | Litecoin 于 2011 年推出，由于其 8400 万 LTC 的更丰富的总供应量，被认为是比特币“黄金”的“银”。它借鉴了比特币的主要概念，但更改了一些关键参数（例如，挖矿算法基于 Scrypt 而不是比特币的 SHA-256）。 |

数据来源：coinmarketcap.com 笔者整理

## 2.1.2 比特币的概念

### 2.1.2.1 比特币的含义

传统的电子支付几乎都需要专门的金融机构提供第三方信用以促进双方的交易，然而第三方的信用机构往往会产生巨额的中介费用。因而，为了取代原有基于第三方信用的交易方式，中本聪为比特币设计了一个基于加密认证的电子支付系统，允许任何交易的双方都可以不通过第三方信用直接进行交易。此外，电子货币一般都会遇到双重支付问题，即一个货币在同一个持有者手中被支付多次的欺诈性支付行为。为了解决这个问题，中本聪将提出一种通过点对点分布式的时间戳服务器来生成依照时间前后排列并加以记录的电子交易证明方案。从这个角度而言，比特币也是一种新的可溯源的交易链条。

因而，根据中本聪在比特币白皮书中对于比特币的设计，本文将比特币界定为，一种基于密码学原理实现去中心化，以时间戳认证解决双重支付问题，能够实现点对点交易的数字加密货币支付系统。

### 2.1.2.2 比特币的相关技术概念

#### （一）比特币网络节点

网络节点是比特币网络中最为基础的组成单位，即参与到比特币网络的的计算机终端。众多网络节点参与到比特币网络的挖矿和交易活动当中，也就保证了整个比特币网络的正常运转。

#### （二）哈希函数与哈希值

比特币以其匿名性著称，其中的加密方法便是使用哈希函数加密。哈希函数，简单而言，能够将任意大小的数据，诸如数字、字母、媒体文件，转换为固定的字母和数字的字符串，而输出的值则是哈希值。哈希函数有两个独特的属性，一是只产生唯一的输出，二是仅仅是单项功能。这也就意味着不能通过哈希值反向推导原始数据，保证了其加密性。比特币的区块链使用的是 SHA-256 哈希值算法，意味着哈希值是 256 位的字母数字字符串。

#### （三）公钥、私钥和地址

公钥和私钥是非对称密码学的核心，共同致力于对数据的加密。公钥，指公用密钥，是对比特币系统任何人开放的。与之相对的，私钥，是私有密钥，它被储存于用户的设备上，用于解密数据。在比特币网络中用于验证消息发布者的地

址，进而给出消息签名。

而比特币地址是由用户的公开密钥经过加密算法计算后得出的字符串，以方便显示和传播。因而在比特币网络中，公钥可被视作是私钥和地址之间的桥梁，是交易验证的关键。

#### (四) 区块和区块链

区块是比特币货币网络的一个基本单位，实质上是一个数据包，区块里面记录着特定时间内交易的详细数据。如图 2.1 所示，区块分为头部和体部两个部分，区块体部往往包含在特定时间内的详细交易信息，而这部分信息通过哈希算法和 Merkle 树，生成唯一的 Merkle 根于区块头部。区块头部则包含了前一个区块的哈希值和 Merkle 根。进而通过区块头部信息，区块便可以串联成链条难以篡改。

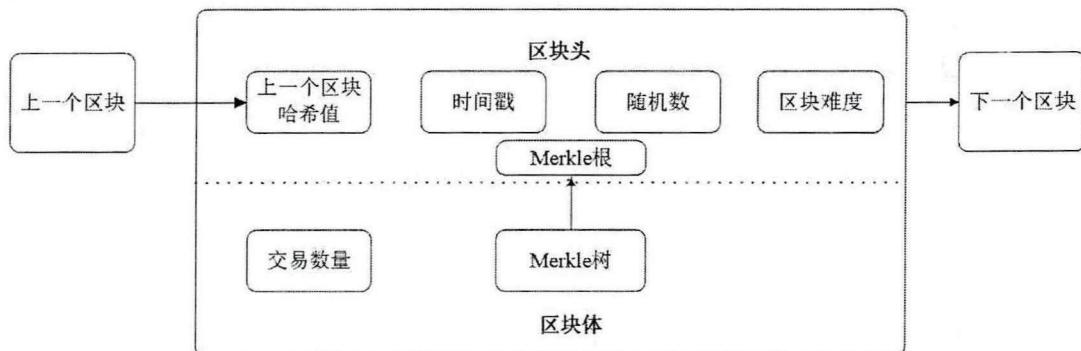


图 2.1 区块链结构

### 2.1.3 比特币的基本技术原理

#### 2.1.3.1 比特币的产生机制

比特币是一个去中心化的点对点货币系统，参与节点分散且数量庞大。当网络中发布了新的交易信息，则迫切需要其他节点对这一交易信息进行验证，串联到区块链中。因而在缺乏权威中心运维的前提下，比特币利用工作量证明的激励机制，使得网络中每个节点都愿意参与到区块验证和网络运维的工作当中来。而节点运算验证区块信息的行为也正是新的比特币产生方式。

比特币的产生也被称作是挖矿，参与到挖矿的节点也被称作是矿工。矿工们想要挖到的矿，也就是新的区块，即将对网络中广播的交易进行验证写入新的区块，而这新的区块中就含有比特币激励。

挖矿的具体过程为：首先挖矿节点综合上一个区块的验证内容，计算当前区块链中最后一个区块的哈希值；其次，过滤比特币网络中的交易信息，将已经记录、余额不足的或者存在信息错误的交易单过滤；再者，随机猜想一个数字，通过这个数字，将这个数字和之前计算得到的上一个区块哈希值和过滤后的交易单，再次计算得到一个新的哈希值；然后，验证这一哈希值是否小于当前的难度阈值，如果小于难度阈值，则新的区块产生，向全网广播。最后，其他尚未计算完成的节点收到这一消息后，对这一区块进行验证，成功后便自动加入当地区块链。因而，最快速完成这一计算流程的矿工便可以获得相应的比特币奖励。

### 2.1.3.1 比特币的交易机制

比特币从表现形式上而言，是一串数字签名，是一条加密的数据记录。所有者拥有的比特币都将会有上一次交易时候上个持有者签署留下的一个随机数列的数字签名，而当该持有者将比特币交易至下一个比特币持有者时候，相应验证的数字签名也会附加在这个比特币末尾，形成一个完整的链条。

从图 2.1 也可以看出比特币的交易记录方式是一个带有时间戳的链式结构，就如一个完整的账本，里面记录了涉及这个比特币交易的历史各方交易数据。在这个链条中，下一个收款人通过私钥和原区块链中的公钥进行签名验证，并将这个验证写入这个比特币，即完成了比特币的转移。所以，比特币就如一个交易链条，当要转移出去时候，就可以和下一个交易者的公钥一同创造一个新的交易记录，进而将这个交易链条转移到了下一个持有者。

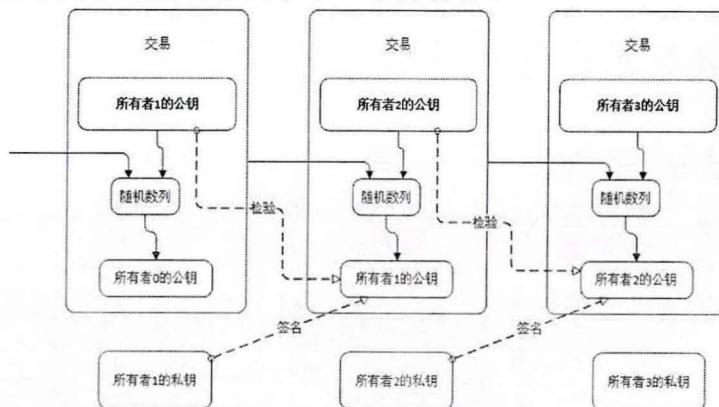


图 2.2 比特币交易过程

## 2.1.4 以太币的概念

### 2.1.4.1 以太币的含义

根据《以太坊白皮书》，以太坊是一个受比特币启发的去中心化的公用区块链网络，基于比特币网络存在的一些缺陷而创新设计的一个区块链网络。其被设计成一个通用的全球性区块链，克服了比特币的只适配数字货币应用场景、效率和资源浪费等固有问题，将应用场景扩充到商业环境，支持智能合约等应用场景。因而以太坊是一个有着高效编程语言的平台，同时也提供了一个功能强大的合约编程环境，用户可以在这个平台创建智能合约应用程序。

而以太币则是这个以太坊系统中所流通的数字加密货币，是在以太坊基础上用以支付交易手续费和运算服务的媒介。以太币不仅如比特币是一种去中心化的加密货币，同时能够在以太坊网络中充当智能合约的交易媒介，同时用以支付交易服务费和运算服务的媒介，进而推动了以太坊金融服务场景的落地。

### 2.1.4.2 以太币的相关技术概念

#### (一) 度量体系

以太币用于支付以太坊虚拟机计算的燃料费用，因而也被设计出一套专门用于以太币面额的度量系统，每个面额都有一个特定的名字。如表 2.1 所示，以太币最小的面额单位是 Wei，而 ether 作为一个以太币是最大的面额。

表 2.1 以太币面额度量体系

| 单位                  | Wei 价值   | Wei 值                     |
|---------------------|----------|---------------------------|
| wei                 | 1 wei    | 1                         |
| Kwei (babbage)      | 1e3 wei  | 1,000                     |
| Mwei (lovelace)     | 1e6 wei  | 1,000,000                 |
| Gwei (shannon)      | 1e9 wei  | 1,000,000,000             |
| microether (szabo)  | 1e12 wei | 1,000,000,000,000         |
| milliether (finney) | 1e15 wei | 1,000,000,000,000,000     |
| ether               | 1e18 wei | 1,000,000,000,000,000,000 |

数据来源：Ethereum Homestead

#### (二) Gas 燃料、Gas 供给上限和 Gas 费

在以太坊中，GAS 燃料被设计成使用固定资源或者工具的固定资源。例如，

在以太坊中发起每笔交易，都会花费固定的 GAS 燃料。每一种计算所消耗的 Gas 数量是恒定的，设计的意图就是为了保证随着时间的推移，同一个操作所消耗的 gas 是保持不变的。虽然每种操作对应着固定的 GAS 值，但是用于购买燃料的以太币价格却是波动的，gas 价格是由用户愿意承担的出价和节点愿意接受的报价动态调整。

Gas 供给上限是指每个区块所能使用 Gas 数量的最大值，它受最大计算负荷、交易总量、区块的大小和矿工的影响，随着时间慢慢的变化。Gas 费是一个特定的交易或程序（被成为合约）执行成功需要的 Gas 总数量。Gas 费受到计算负载、交易总量、区块大小等因素影响。Gas 费被支付给矿工

### （二）EOA(外部账户)和 CA (合约账户)

与比特币不同，以太坊的基础单位是账户。以太坊区块链当中的区块会记录着每一个账户的状态变化。

EOA 是外部账户(Externally Owned Account)的缩写，一个账户由一个私钥控制，一旦用户拥有一个账户所对应的私钥，那么就拥有通过账户发送以太币和消息的能力。CA 合约账户（Contract Account）指的是由合约代码来控制并且只能由外部账户激活的账户。合约账户也拥有一个地址，可以查看账户的详细信息。外部账户和合约账户在将来的宁静(Serenity)版本中可能会合并成一个单一账户。

### （三）以太坊虚拟机（EVM）

以太坊虚拟机，是以太坊去中心化的计算平台，它构成了以太坊功能的核心。以太坊是一个可编程的区块链，以太坊允许用户创建任意复杂度的操作而不是提供一组预设好的操作指令。在这种方式下，区块链就成为一个分布式应用的平台，可以实现但不局限于加密货币应用。开发人员可以使用现有的语言的计算机语言方便地创建运行于 EVM 上的应用程序。

## 2.1.5 以太币的基本技术原理

### 2.1.5.1 以太币的产生机制

以太币的挖矿机制与比特币大致相同，都是通过矿工们的运算挖出新的区块，进而奖励一定量的以太币。在挖矿过程中，矿工会使用计算机反复计算，对以太坊的区块头元数据进行哈希值运算，最先运算出来的矿工将获得相应的一天比奖励，并在全网广播区块。这种工作量证明方法跟比特币的挖矿过程是一致

的，但是以太币采用新的工作量证明方法，被称作 Ethash<sup>[34]</sup>。在原有工作量证明基础上，通过控制出块的难度阈值控制矿工们计算出哈希值的时间，即控制在 15 秒一个区块速度。

#### 2.1.5.1 以太币的交易机制

以太坊与比特币最大的不同就是将其区块链的应用场景从单纯的数字货币场景进行了更加深度的扩展，而这个扩展的重要环节就是智能合约的加入。因而也可以将以太坊视作是数字货币和智能合约的集合。以太坊为智能合约的编写提供了具备图灵完备性的脚本语言和运算环境，允许每个人在以太坊上使用该语言编制相应的智能合约。而一旦该合约编写完毕，就会成为一个自动代理，收到特定交易就会执行程序，完成进一步交易。而以太币在其中充当着燃料（GAS）购买的作用<sup>[34]</sup>，为合约执行充当支付媒介。在以太坊智能合约执行当中，每个执行都要在以太坊各个节点完成已达到去中心化目的。但是这个执行需要耗费成本，例如计算和存储的消耗，才可以驱动矿工们处理交易。交易方需要用以太币购买燃料，来吸引矿工验证处理交易，以驱动智能合约的完成。

## 2.2 加密货币的相关理论基础

### 2.2.1 哈耶克的货币非国家化理论

哈耶克是自由主义的推崇者，在其《货币的非国家化》一书中，他将其自由主义的思想引入货币政策，认为货币也是一种商品，既然所有的行业都应该是自由竞争才能达到最优，那么货币就不应该被国家垄断，应当实现货币的非国家化。

在其货币非国家化理论中，其认为国家垄断货币发行有诸多弊端。首先，政府因一己私利而垄断且滥用货币的发行权，伤害人民的信任；其次，纸币的发行数量经常基于政治考量，会损害整个经济效率；最后，货币发行权的垄断进一步支持着政府权力集中，进一步破坏自由市场机制，进而引发失业和通胀。

因而，哈耶克认为，应该打破政府对于货币发行权的垄断，允许银行自由发行货币，实现多元货币的流通，以达成货币的自由市场。进而优质货币淘汰劣质货币，币值也会因自由市场而保持稳定，进而实现物价水平的稳定。

当然，哈耶克的非国家化理论并没有预见未来数字加密货币的诞生。以比特币为例，比特币的一个重要特征就是去中心化，将货币的产生和交易交付给比特

币网络，依靠特定的网络程序而非权威中心完成。以此，实现脱离国家央行的控制和垄断，完全实现非国家化。

### 2.2.2 弗里德曼的货币数量论

同样崇尚经济自由的弗里德曼，在其《通货膨胀和失业》一书中将通胀定义成一种货币现象，指的是价格的稳定和持续性上涨，因而也应该由货币变化解释通货膨胀。他认为，通胀的发生是因为货币数量增加远远超过了社会产品增加，社会每单位产品所匹配的货币量增长过快，就会导致通胀速度过快。

由于国家垄断了货币供给，因而他认为政府的主观原因同样也是造成通胀的原因之一。政府盲目的增加政府开支，用铸币权弥补赤字，以及错误的货币政策都会造成其盲目的扩大货币供给，造成通胀压力，影响经济效率。因而，弗里德曼主张“单一规则”的货币政策，保持固定的数量的货币供给增长率，保证货币供给与实际经济需求相符合。

以比特币和以太币为代表的数字货币就基本实现了这一设想，他们的发行和产生方式遵循特定的程序，发行数量和机制都是预先设定，可以被估计。同时其发行总量在一定时间后保持固定，以控制通胀。

## 2.3 市场风险度量相关理论基础

### 2.3.1 VaR 值理论

#### 2.3.1.1 VaR 含义

VaR (value at risk)，即在险价值，被定义为给定置信区间内最大的预期损失<sup>[35]</sup>。因而，VaR 值就是，在给定置信水平下，某个资产在持有期内可能的最大损失。可以简单表示为以下公式：

$$\text{Prob}(\text{Loss} > \text{VaR}) = 1 - \alpha \quad (2.1)$$

其中，Loss即该资产在特定时间端内的损失。给定置信水平，VaR 为在该置信水平下的在险价值，由最小的x给出，进而使得损失超过 x 的可能性低于  $1 - \alpha$ 。

VaR 在险价值特点之一即是容易理解，直观的反映出当前持有资产在持有时间内的风险程度，是对资产组合潜在损失的简单统计。此外，VaR 值是对“正

常市场波动”的度量，不考虑一些特殊的极端情况。

### 2.3.1.2 VaR 值传统计算方法

#### (一) 历史模拟法

历史模拟法是一种基于过去历史数据估计未来市场变化的方法，即假设历史收益率变化和未来收益率变化一致，进而利用过去的历史数据去估计未来资产收益率分布，进而计算出置信水平下所在分位数，得出 VaR 值。因而是一种简单而且直观的计算方法，核心思想是基于历史数据模拟未来损益分布。

历史模拟法的优点是简单直观，不需要对收益率分布做出假设，能够比较好的处理非对称问题和肥尾问题。然而其缺点也是显而易见，利用历史数据估计未来收益，要求大量有效的历史数据，以充分反映未来资产变化，数据太少或者无效数据太多，则会影响计算精度。

#### (二) 方差协方差法

方法协方差法，是提前假设资产收益率服从特定分布，并利用样本历史数据估计出这一分布的方差和协方差等统计特征，进而求出相应置信水平下的分位数，进而推导出 VaR 值。一般而言，对资产收益率分布大多假设其服从正太分布，但是在实际情况中，对于一些收益率非正太情况，也会引入 t 分布，加强对后尾分布的估计准确度。

方差协方差方法的优点是计算简单，同时能够实现不同持有期和不同置信水平下 VaR 值转换。但是其缺陷在于依赖对资产收益率的分布假设，基于正太分布的假设往往不能够真实反映资产的收益率分布，无法处理肥尾或者非线性回报的资产情况。

#### (三) 蒙特卡洛模拟法

蒙特卡洛模拟法是利用随机过程，多次模拟资产的未来收益变动，进而获得资产收益的预测变动情况，得到资产未来收益率的分布，进而根据这一分布得出 VaR 值。具体而言，首先选定置信水平和影响因素，并根据历史数据假定一个合理的分布。其次，根据这一分布选取合理的随机模型，以此得到相应的随机数和价格变化路径，进而不断重复这一模拟过程。最后，得到一个资产收益率的模拟分布情况，据此计算得到 VaR 值。

蒙特卡洛模拟法的优点在于通过历史数据的不断模拟，得出一个更加可靠和综合的模拟分布，能够处理非线性和肥尾的问题。但是它的缺陷在于依赖于历史数据和假定的随机过程估计在险价值，计算量大且复杂，同时无法考虑变量的

时变性。

### 2.3.1.2 GARCH-VaR 计算方法

#### (一) ARCH 模型

ARCH 模型针对金融序列的残差项进行建模分析，能够较好地符合金融序列中的尖峰肥尾和波动聚集的特征。Robert F. Engle(1982)在其论文中首次提出了这一模型，能够较好地对金融序列的波动特征进行描述与预测<sup>[37]</sup>。

ARCH 模型的基本思想是，当前某时刻的噪声发生服从正太分布，且该正太分布的均值为零。此分布的方差是一个随着时间变化的条件异方差，同时满足与过去噪声值平方成线性关系的自回归性质。其中 ARCH(p) 模型表达式如下：

$$\begin{cases} x_t = \beta_0 + \beta_1 x_{t-1} + \beta_2 x_{t-2} + \dots + \beta_p x_{t-p} + u_t \\ \sigma_t^2 = E(u_t^2) = \alpha_0 + \alpha_1 u_{t-1} + \alpha_2 u_{t-2}^2 + \dots + \alpha_p u_{t-p}^p \end{cases} \quad (2.2)$$

ARCH 模型虽然简单易行，但是其对于参数估计的精确度往往受到分布假设的限制。同时为了更好地估计效果，往往会增大滞后阶数，造成参数冗杂等问题。

#### (二) GARCH-VaR 模型

GARCH 模型是在 ARCH 模型的基础上的改进，首先针对扰动项的分布进行假设，常用的假设分布有正态分布、t 分布和广义误差分布，进而据此对时间序列进行拟合，得到相应的条件方差和条件均值，则 t 时刻的 VaR 可表示为下式：

$$VaR_t = -\mu_t + \sigma_t t^{-1}(\alpha) \quad (2.3)$$

其中  $t^{-1}(\alpha)$  为假定分布下置信水平为  $\alpha$  的分位数。

GARCH 方法估计 VaR 值的优点在于考虑到了波动率的时变性，其所估计出来的标准差是基于第 1 期和 t-1 期的数据估计得到，能够估计动态的 VaR 值。同时，其对收益率的分布假设可以进一步改进，以满足金融序列的尖峰肥尾的特征。

然而，GARCH 方法也存在相应缺陷。其在估计 VaR 值时候，需要假设扰动项  $\varepsilon_t$  服从于特定分布，然而往往金融时间序列的扰动项  $\varepsilon_t$  具有比 t 分布更肥的尾部，此外本文所讨论的数字货币价格波动剧烈，日收益率往往出现大量极端值，难以被 GARCH 模型捕捉<sup>[38]</sup>。因而仅凭 GARCH 模型估计的 VaR 值往往会低估

真实风险。

### 2.3.2 极值理论

极值理论是一种估计和预测小概率事件或者异常现象的风险预测技术，能够很好的度量极端时间的风险。极值理论 EVT 与随机变量极限观察的渐近行为有关。它为极端事件的统计建模提供了基础，并用于计算与尾巴相关的风险度量。在特定时间范围内，可以使用两种不同但相关的方式来识别实际数据中的极端情况，即分块样本极大值模型 BMM 模型和 POT 模型。

第一种 BMM 方法，将时间范围划分为块或周期，并考虑变量在连续周期（例如，几个月或几年）中所占用的最大值。这些选定的观察值构成了极端事件，也称为块最大值（BM）。在这种情况下，广义极值（GEV）分布用于拟合 BM。

另一种办法，POT 方法，仅关注超过给定阈值的观测值。核心思想是在大量数据中找到合适的阈值，基于超过这个阈值的数据，利用广义帕累托分布拟合观测值，得到极值分布，进而求得 VaR 值。由于本文将在第四章使用该方法，故展开说明。

首先假设  $X_1, X_2, X_3 \dots X_n$  是独立同分布的随机变量，分布函数为  $F(x)$ ，阈值为  $u$ ，令  $Y = X - u$ ，则其超过阈值的超额数  $Y$  的分布函数  $F_u(y)$  可以表示为：

$$F_u(y) = \Pr(Y \leq y | X > u) (0 \leq y \leq x_0 - u) \quad (2.4)$$

进而根据条件概率公式，这个分布函数推导得到下式：

$$\begin{aligned} F_u(y) &= \Pr(Y \leq y | X > u) = \frac{\Pr(X-u \leq y, X>u)}{\Pr(X>u)} \\ &= \frac{\Pr(u < X < u+y)}{\Pr(X>u)} = \frac{F(y+u) - F(u)}{1 - F(u)} \end{aligned} \quad (2.5)$$

由于  $X > u$  时候， $X = y + u$ ，所以可得到：

$$F(x) = [1 - F(u)]F_u(y) + F(u) \quad (2.6)$$

根据上述推导和 Fisher-Tippett 定理，当阈值充分大时候，超阈值分布可以近似看做是广义帕累托分布，故可用广义帕累托分布近似拟合超阈值的分布。而  $F(u)$  则可以采用经验分布函数近似估计，其中  $n_u$  是超过样本阈值的个数， $n$  为样本总数。则可以推导出尾部拟合：

$$\hat{F}(x) = [1 - \frac{n-n_u}{n}]G_{\xi,x,u}(y) + \frac{n-n_u}{n} = \begin{cases} 1 - \frac{n_u}{n}(1 + \xi \frac{x-u}{\tau})^{-\frac{1}{\xi}}, & \xi \neq 0 \\ 1 - \frac{n_u}{n}e^{-\frac{x-u}{\tau}}, & \xi = 0 \end{cases} \quad (2.7)$$

根据超阈值分布，就可以得到置信水平 $\alpha$ 下的分位数 $VaR_\alpha$ 。

$$VaR_\alpha = u + \frac{\tau}{\xi} \left\{ \left[ \frac{n}{n_u} (1 - \alpha) \right]^{-\xi} - 1 \right\} \quad (2.8)$$

## 第三章 数字加密货币发展概况

### 3.1 数字加密货币产业链

随着种类纷杂的数字加密货币和区块链技术的发展，一大批公司及项目涌现进入这个行业，寄希望于通过促进数字加密货币使用服务来激发数字加密货币行业的巨大潜能。数字加密货币行业，以及在区块链网络与传统经济的其他部门之间建立联系的服务业，两者的发展与壮大为数字加密货币本身增添了巨大价值。为便于分析数字加密货币行业，将其划分为四个主要领域：交易所，即主要用于买卖数字加密货币或交换各国法定货币；支付部门，即通过使用数字加密货币进行支付活动；采矿部门，主要负责在公共帐本（区块链）中记录交易的部门。

#### 3.1.1 采矿部门

加密货币行业把加密货币的生产称作是采矿，而采矿的人或者部门则被称作矿工，这与加密货币的产生方式不无关系。

矿工负责记录区块链内的交易，并向分类账系统提供必要的计算力，以保障数字加密货币网络的安全，同时维护其真实透明。在采矿部门中，有五种基本的活动类型：采矿，指个人或组织通过数字货币计划处理交易以获取报酬；矿池，在矿池中合并了多个矿工的计算能力，增加了找到新矿区的可能性，同时从采矿中获取的奖励将按照所有矿工共享的计算能力进行重新分配；采矿硬件制造，由专门从事设计和制造的组织购成采矿活动的硬件；云挖掘服务，主要由租用哈希功能的组织构成；远程托管服务，客户将其拥有的采矿设备托管给团队进行维护，主要向用户提供参与采矿过程的可能性而无需自行运行设备。

比特币和以太币同样是在采矿过程中产生的。此类过程由网络参与者基于累积的计算机功能来支持和生成（Scheinert, 2016）<sup>[39]</sup>。与法定货币不同，采矿是使用工作量证明（PoW）区块链算法的CVC的独特功能。这种算法定义了将在区块链旁边添加哪个块，并使用某种证明进行了验证。基于PoW原理的加密货币，采矿被视为区块链验证唯一方式。而挖矿被认为是区块验证的一种低能耗方

式，因此，PoS 现在已被新的数字货币广泛采用。与过去的挖矿相同，节点将获得块验证奖励。当矿工成功解决数学难题时，便会创建比特币。随着时间的流逝，难题变得越来越困难，而丰厚的奖励意味着一个孤独的矿工现在有可能投入资源来尝试解决难题，但是却没有获得任何奖励。为了应对这个情况，众多采矿者便会集中起来，采用更高算力的计算器，而这也就慢慢形成了矿池。

目前，采矿池现在合并了众多采矿者的资源，形成了庞大的加密货币算力的同时，也威胁到了加密货币市场的安全性。截至 2015 年 3 月，算力最为庞大的两个采矿池是 AntPool 和 F2Pool，它们合计占比特币采矿活动的三分之一。然而庞大的矿池却威胁着加密货币去中心化的初衷，分散了加密货币的可信赖性。例如，2014 年 6 月很长一段时间，GHash 矿池算力占据了总采矿能力的 50% 以上，这可能使 GHash 池的矿工们有机会对比特币进行操纵。拥有比特币大部分计算资源的攻击者可以很轻松地更改比特币区块链系统的某些记录，包括插入虚假交易和拒绝实际交易或偏离协议规则。因而矿池的集中化对于要求分布式的比特币的未来发展蒙上了一层阴影。

### 3.1.2 交易平台

交易平台在数字加密货币行业中起着至关重要的作用，因为它不仅提供了一个市场促进了交易的开展，同时有利于数字加密货币的流动性和定价。

比特币和其他加密货币可以通过众多数字货币交易所购买和交易。根据数字货币行业中不同的交易活动可以将平台分为三类：一是订单簿交易，通过使用交易引擎来匹配用户请求的平台；二是提供经纪服务平台，其功能在于可使用户以给定的价格方便地买卖数字加密货币；三是交易平台，提供单一界面链接至交易所，并提供杠杆交易及数字加密货币相关衍生工具。也可根据交易所的大小来区分，不同规模的交易所专门从事不同类型的服务，小型事务所专注于提供经纪服务，而大型的交易所倾向于提供服务组合，而不是某一类专门的服务。相较于小型交易所，大型交易所更有利控制与银行关系相关的风险因素。

交易所是数字加密货币行业中第一个成立的部门，最开始成立于 2010 年，也就是比特币投入使用后的一年，目的是促进比特币的交易并评估其市场价值。从 2010 年到 2012 年，日本数字货币交易平台 Mt. Gox 拥有当时加密货币市场超过 80% 的市场份额，处于行业的领先地位。然而在 2013 年该交易平台的头部地

位被新的交易所 BTC-e 和 Bitmap 取代<sup>[40]</sup>。这个阶段，大多数兑换交易都以美元为主。而后 2014 年第一季度，曾今最大的比特币交易平台 Mt. Gox 被迫宣布破产清算，并声明有 85 万个比特币丢失。

考虑到交易平台 Mt. Gox 较大的市场份额以及当时比特币上升的价格趋势，这个比特币平台破产事件极大地影响了当时的数字货币市场，使得投资者对于平台安全性产生了质疑。而这次事件之后，BTC-e, Bitstamp 和 Bitcurex 占据着领先的加密货币市场份额<sup>[40]</sup>。2015 年 3 月，BTC 中国, OKCoin, Huobi, Bitfinex, LakeBTC, Bitstamp 和 BTC-e 成为了数字货币市场最大的七个交易所。这七家交易平台从 2014 年 10 月至 2015 年 3 月，共同为比特币市场交易提供了 95% 以上的服务<sup>[40]</sup>。

而加密货币交易平台在 2013 年之后开始不断受到监管压力，比特币交易平台的注册资本不断提升。在美国，货币交易所通常作为“货币发送者”运行，因此必须作为货币服务企业向机构金融犯罪执法局（FinCEN）注册。注册包括需要法律费用和过帐保证金的逐州许可。单个州的认证费用通常至少为 10,000 美元。其他国家也有类似的规定，在德国，代表客户管理存款的货币兑换被视为“存款银行”，其最低资本要求为 500 万欧元。

在监管的不断介入下，数字加密货币的缺点和交易平台的不规范暴露无遗。例如，2017 年，美国当局指控加密货币交易平台 BTC-e 参与非法洗钱。该交易平台被叫停了一切数字货币交易活动。根据美国法院文件，嫌疑人 Vinnik 从攻击 Mt. Gox 平台的黑客得到比特币，并在 BTC-e 平台兑换成美元。机构金融犯罪执法局 FinCEN 对此事件共计罚款 1.22 亿美元，其中 BTC-e 罚款 1.1 亿美元，Vinnik 罚款 1200 万美元。然而，不同于之前的 Mt. Gox 的一蹶不振，BTC-e 更换另一个名称 WEX 后重新上线运营，该网站承袭相同的用户数据库和相同的界面，并且允许之前的用户提取部分资金。

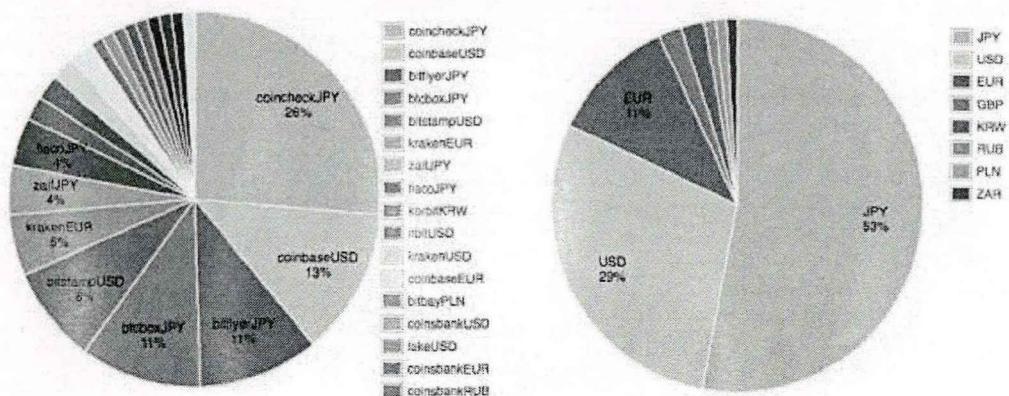


图 2.2 比特币交易市场货币占比和平台占比

数据来源: Bitcoincharts, 2018

以比特币交易平台为例,如图 2.2 所示,当前的比特币市场的兑换货币集中程度高,主要货币集中于日元、美元、人民币和欧元。而当前比特币平台的主要交易货币不再是美元,而是日元,占据了比特币市场 53% 的业务份额。其次是美元和欧元,分别为 29% 和 11%。从平台份额占比来看,目前的市场交易领导者是 Coincheck,其比特币日元业务的大部分占据着市场的大部分,即 34%,同时 Coinbase 的比特币美元业务也占据比特币市场交易的 13% 份额,其次是 Biflyer,其比特币日元业务占据市场的 11%。此外,从上图可以看出,目前 Coinbase 和 Bitstamp 是市场领先的比特币交易平台。

不同于法定货币在各个外汇交易平台的价格一致,加密货币的汇率在不同的交易平台之间变化并存在波动。这跟比特币市场的流动性不足相关,同时比特币的汇兑价格可能会受到市场规模,交易量,购买需求和汇兑货币等特定因素的影响以及经济,技术和媒体因素影响<sup>[40]</sup>。利用特定货币或者地区的交易优势,某些交易平台在特定货币或地区交易的市场份额才能保持领先地位。

目前,考虑到这些影响因素,比特币交易平台已开始专门研究货币,交易地点等因素最大化平台的交易优势。正如 Brandvold, Molnar, Vagstad 和 Valstad (2015) 所描述的情况,数字货币的交易市场正在变得更加多样化和发达,并且交易平台也正努力通过引入身份验证流程来改善隐私功能以保障投资者权益。

### 3.1.3 支付部门

支付部门，即通过使用数字加密货币进行支付活动，通过加密货币支付通道，支付方提供服务以促进用户使用数字加密货币。支付部门属于加密货币产业链的下游环节，目前以支付应用和服务设施为主，而服务环节包含加密货币社区、加密货币钱包，其中以钱包为主要服务设施。

支付部门目前主要以数字钱包为主。数字钱包是一种收集和存储所获取的加密货币的软件程序，通常定义为使用公钥和私钥来存储、发送和接收数字加密货币的软件程序。就数字货币被视为一连串的数字签名而言，这种钱包类的数字程序里面没有钱，而是存储了比特币地址的私钥<sup>[41]</sup>。数字钱包根据终端分为四种类型：网络，桌面，离线和移动。

网络类型是用户通过浏览器进行操作的，可以在移动设备和台式机上使用。桌面类型钱包是可下载的软件程序，可为交易创建比特币地址并存储比特币地址的私钥，此类程序使用户可以完全控制操作以及隐私级别较高。硬件钱包是提供高安全性私钥存储的钱包的最有效类型，此类硬件可以看作是运行特殊软件的记忆棒。移动钱包则与台式机相似，需要在移动终端上安装相应的应用程序，以为用户提供对电子货币的高度控制，但具有基本的隐私保护<sup>[41]</sup>。

表 3.1 数字钱包分类以及特点

| 钱包类型 | 主要特点   | 代表企业                       |
|------|--|----------------------------|
| 移动钱包 | 作为智能手机程序运行，操作简单，使用灵活，但是安全性差                  | Edge; Mycellium; Coinomi 等 |
| 桌面钱包 | 作为电脑程序在计算机上使用，用户私钥存储在硬盘中，安全性较移动端好，但是仍然存在安全风险 | Jaxx Liberty; Exodus 等     |
| 在线钱包 | 网页端使用，优点是使用方便，转账效率高，但是安全性不高                  | Coinbase                   |
| 离线钱包 | 不联网的钱包，大大降低了被窃取的可能性，安全性高，但是对技术要求高，使用复杂       | Trezor                     |

资料来源：Bitcoin.com

目前数字货币钱包服务仍然面临着众多困难和存在大量不足，行业对此也没有一个统一的有效的解决办法。比如比特币钱包软件可能难以安装，并且存在

苛刻的技术要求，例如存储整个区块链的副本，截至 2015 年 3 月，比特币副本的容量为 30 GB<sup>[41]</sup>。即使目前技术手段并不要求所有参与者都需要下载整个链，但大部分的系统确实依赖某些用户下载存储这个账本链条。同时安全性也是钱包服务商们和数字货币持有者头疼的一个问题。从用户端而言，存储数字货币的终端的崩溃或黑客攻击手持数字钱包的计算机都可能会导致用户数字货币丢失。从服务商而言，黑客攻击服务商一直以来是数字钱包服务商们难以解决的重大风险。结果，许多用户或者依赖数字钱包服务，该服务将所需文件保存在共享服务器上，或者通过“纸钱包”方式物理储存数字货币的私钥。而目前，数字钱包服务商们趋向于一方面提高集中度，扩大交易所的作用和重要性，一方面添加为满足多样性用户需求的附加服务。

## 3.2 数字加密货币监管现状

### 3.2.1 世界各国监管程度

随着比特币价格的突飞猛进，众多新型的虚拟数字货币开始刺激起大众的兴趣和热情。而这也使得世界各地金融管制机构也开始关注起这种意在打破中心化的数字货币。数字货币是否会危及金融稳定，而数字货币的高度匿名性是否会为非法活动带来更大的便利性，这些都是世界各地央行所担心。大部分的中央银行机构都对虚拟货币发表了意见和看法。Jan Lansky (2018) 将世界各国对虚拟货币的监管态度分为了忽视、提醒、引导、禁止等四个级别<sup>[42]</sup>。笔者据此整理出以下各个级别的特征和大致国家：

**忽视。**持忽视态度的国家，对于数字货币并不关心，对数字货币的流通采取放任态度。因为数字货币在这些国家流通数量偏少，对于当地金融安全并不构成直接威胁，当局自然也默许其的存在和流通。截止目前，大约 150 个国家都是忽视数字货币的态度<sup>[42]</sup>。

**提醒。**对数字货币持提醒态度的国家，一方面对于数字货币在本国的流通持默认态度，另一方面又及时的警告公众注意这些新型货币的风险，包括数字货币的价值可能会意外而迅速下降，以及被他人非法盗取的技术风险。例如欧洲近 25 个国家就曾针对数字货币的相关风险发布风险警示报告。这个问题的立场实际上是世界各国当局最广泛的态度。到目前为止，比利时，巴西，塞浦路斯，丹麦，法国，希腊，匈牙利，印度，印度尼西亚，以色列，意大利，黎巴嫩，立陶宛，马来西亚，墨西哥，荷兰，新西兰，菲律宾，葡萄牙，塞尔维亚，南非，韩国，土耳其和越南都包括在此级别中。

**引导。**处于引导阶段的国家，对于数字货币的看法持中立的，一方面当局针对数字货币的使用出台相应的指导办法，帮助国民规范和安全地使用数字货币，另一方面在相关政策报告中提醒民众虚拟货币的相关风险。这个阶段的相关国家对使用指导的具体规范又不尽相同。首先，诸如在美国、加拿大、阿根廷、新加坡、捷克等五个国家，数字货币受到禁止洗钱等法律限制。其次，欧盟和瑞士都声明加密货币不能被视为商品，因而不能缴纳增值税。但是，澳大利亚、美国德国等 8 个国家认可数字货币的资产属性，但要根据现行法律征税。另一方面少数几个国家和地区，诸如英国，将虚拟货币可被视为商品，且需缴纳增值

税。甚至，波兰和西班牙主管部门，对加密货币征收所得税，以及对加密货币征收赌博税。

禁止。在该监管级别的国家，国家主管部门完全对加密货币的流通呈现负面的态度。一些国家，诸如中国、冰岛等国家，禁止国内金融机构提供虚拟货币相关的金融服务，尤其是为数字货币提供兑换服务，同时也限制国内民众使用和交易虚拟货币。另外，诸如泰国、俄罗斯孟加拉国等国家，采取更为严格的措施限制加密货币。不仅严格禁止在银行机构和人民中使用数字货币，而且可以设立严格禁令，通过严厉制裁甚至监禁来执行该禁令。

各国对于比特币的监管程度不一，但是由于数字货币的主要生产国家和流通国家集中于中国、美国和欧盟，因而这几个国家的监管措施对于数字货币的未来发展有着深远影响。

#### 3.2.2 中国监管政策

早在 2013 年，比特币就在中国市场备受关注，大量投资者开始涌入到比特币市场。而这也引起了中国监管机构的注意。为了保护投资者权益，维持金融稳定，中国人民银行禁止银行和其他金融机构进行与比特币相关的交易，同时允许个人和公司自由投资虚拟货币，但警告他们与此类交易相关的风险。此外，中央银行要求所有在线交易所向相应的监管机构提交注册，并表示将对其进行监控。

不久后，中国人民银行将该禁令扩大到支付公司。因此，美国最大的比特币交易所 BTC China 宣布，由于第三方支付提供商 YeePay 成为中央银行的关注对象，它将不再接受人民币存款。这也使比特币遭受了严重的价值损失。

在 2017 年，中国中央银行宣布打算改善对在线公司所关注问题的监管，因为数字金融的发展改善了所提供的服务及其效率，这种金融不仅包括 P2P 交易，还包括吸引资金和其他服务，这是加密货币使用带来的风险增长的一个促成因素。此后，中国人民银行发布公告，禁止银行和家庭参与发行代币筹资活动，这意味着他们不能通过 ICO 筹集资金，因为前者在中国被认为是非法的。具体中国监管政策事件如下表 3.2 所示

### 第三章 数字加密货币发展概况

表 3.2 中国监管政策事件一览

| 时间               | 事件  |
|------------------|---|
| 2013 年 5 月 12 日  | 中国人民银行发布公告表示，比特币不是货币，金融机构和支付机构不能参与与比特币相关的交易，从事比特币相关服务的网站交易需要向监管机构进行注册，中国人民银行将密切关注比特币的潜在用途洗钱。同时中国人民银行将提醒公众使用和交易比特币的风险。                           |
| 2013 年 12 月 17 日 | 在中国人民银行发布 5.12 声明后，BTC 中国不再接受人民币交易。同时中国人民银行扩大了对第三方支付提供商接受，使用或出售比特币的禁令。  |
| 2014 年 4 月 25 日  | 中国人民银行报告显示，中国人民银行已警告银行停止与虚拟货币相关的业务。   |
| 2016 年 1 月 1 日   | 中国人民银行正在进行数字货币研究，考虑发行自己的数字货币  |
| 2016 年 11 月 9 日  | 央行于 11 月 9 日发布了招募广告，内容与招聘区块链专家有关，以帮助其开发自己的数字货币。   |
| 2017 年 8 月 5 日   | 中国人民银行宣布其计划加强对中国金融服务业的监管，包括其风险评估系统宏观审慎评估中的大型在线金融业务。这些业务包括 P2P 贷方，第三方在线支付平台，众筹公司和其他金融服务。7 月，有 45 家中国金融公司同意加入名为“网联”的支付清算平台，这将使中国人民银行能够更密切地监控在线支付。 |
| 2017 年 9 月 4 日   | 中国禁止所有公司和个人通过 ICO 活动筹集资金，并重申 ICO 被视为该国的非法活动。包括中国人民银行，中国证券监督管理委员会和中国保险监督管理委员会在内的几个实体发表了联合声明，宣布了该禁令   |
| 2018 年 8 月 24 日  | 中国监管机构发出警告，禁止通过加密代币销售和交易代币非法筹集资金。该警告的目标是代币融资和加密货币市场操纵   |
| 2019 年 04 月 12 日 | 国家发展和改革委员会提议将加密货币采矿纳入其计划消除的 450 种浪费和危险活动清单。拟议的禁令将于 2019 年 5 月 7 日结束的公众意见征询期后生效。   |
| 2019 年 8 月 9 日   | 最近的一份报告指出，中国中央银行打算向七个实体发行一种国家支持的数字货币，称为 DCEP，这三个实体是三家银行，中国工商银行，中国银行和中国农业银行；阿里巴巴，腾讯和银联三大科技公司；以及中国银行协会。该数字货币旨在用于目前以中国法定货币人民币进行的付款。                |

数据来源：中国人民银行，国家发改委官网，Perkins Coie 报告

中国政府对待数字货币的监管态度不断严格，不仅禁止虚拟货币在国内的发行、交易和兑换，禁止金融机构提供数字货币相关的服务，而且将比特币的交易和登记纳入反洗钱监管。然而针对个人持有数字货币，并没有出台相关政策予

以约束。同时，数字货币在我国法律中并未有明确的法律定义，其自身法律属性也尚未界定清晰。

### 3.2.3 美国监管态度

加密货币到目前为止，一直是美国联邦政府和各州政府关注的焦点。到目前为止，在美国各个机构对虚拟货币并没有形成没有统一的看法。近年来，美国针对数字货币监管政策不断出台，一方面担心加密货币带来的金融风险，进而不断加强管控，另一方面又担忧丧失区块链技术的领导地位，不断给相关代币融资放行。

2013年，美国金融犯罪执法网络部(FinCEN)，在其发布的法规中宣布虚拟货币不符合“货币”的标准，进而不认可数字货币作为法定货币<sup>[43]</sup>。因此，根据FinCEN的规定，虚拟货币的相关服务企业应在相关部门注册获得营业执照，并接受反洗钱监管。此外，同年美国国税局(IRS)发布公告以阐明现有税收法规如何应用于与数字货币相关的交易。当局认为数字货币被视为一种资产，而不是一种货币，特别是在涉及产生外币损益的特征方面。根据这种分类，根据一般税收原则，诸如采矿，交易或持有之类的数字货币服务应履行相应的纳税义务。

然而2017年3月3日，美联储(Fed)主席杰罗姆·海登·鲍威尔(Jerome Hayden Powell)发表演讲表达了对数字货币未来前景的看好。他概述了传统支付系统及其目标，介绍了替代系统，包括分布式分类账技术，并最终上市与央行数字货币相关的潜在弊端，例如与洗钱相关的弊端，引起人们的注意，即银行可能会在用户隐私和与密码学相关的隐藏活动风险之间进行权衡。同时也表达了对数字货币将推动经济增长和改善新的经济思想和创新持开放态度。同年11月，美国商品期货交易委员会正式批准了芝加哥商业交易所集团、芝加哥期权交易所以及Cantor交易所的比特币期货上市请求。

2017年12月，美国证券交易委员会(SEC)在其官网发布了一篇文章，声称对虚拟货币和初始代币发行(ICO)进行了分析，但由于与传统证券市场相比，投资数字货币的投资者保护措施较少，欺诈的可能性大大增加。因此，SEC向公众发出警告，明确表示未向任何机构注册任何ICO业务，并建议有投资于加密货币意愿的投资者明确投资比特币风险。

在2018年初，美国当局针对ICO业务保持进一步谨慎的态度。2018年3月

美国证券交易委员会（SEC）发布《关于数字资产在线交易平台违法声明》，明确表明数字加密货币交易平台必须在美国证券交易委员会注册认证获得许可，并且向投资者传达了由美国证券交易委员会发布的 ICO 信息。同年 4 月，美国证券交易委员会指控 CentraTech 在推广代币融资时涉嫌欺诈，并叫停代币融资。

然而与联邦政府当局的谨慎形成鲜明对比的是美国各州对于数字货币的兴趣和热情，其中纽约州最为激进。早在 2015 年，纽约金融服务监管局就针对纽约加密货币业务进行了谨慎监管的规定，规定加密货币的生产、使用、交易等服务都需要获得相应的营业执照才可以经营。而截止 2019 年 5 月，比特币的营业执照已发放近 20 份。同时，纽约金融服务监管局还为了数字加密货币设立了研究与创新部，专门监管加密货币业务，同时审批数字货币营业执照。

美国对于数字加密货币的监管政策从谨慎到如今不断加强，体现了美国当局对于加密货币负面影响的担忧态度，对于数字货币的发展前景并不看好。因而对加密货币的一系列服务活动时刻保持谨慎监管态度，对涉及加密货币的代币融资业务也呈现时刻把控的态势。

#### 3.2.4 欧盟监管政策

欧盟是最早关注数字加密货币发展的国家和地区之一，早在 2012 年欧洲央行就针对加密货币发布相关报告，试图阐明数字货币的用途，同时也指出了其对于扩展线上支付的作用，加强支付系统的潜力。但是随着虚拟货币的快速发展，欧洲央行也意识到其负面影响，并向公众警示使用虚拟货币的各种风险，并将虚拟货币纳入反洗钱和反恐融资的监管。同时欧洲央行为不使得虚拟货币侵蚀其控制权，不允许欧盟内部发行数字货币。相关监管事件整理如下表。

表 3.3 欧盟相关政策一览表

| 时间               | 事件   |
|------------------|--|
| 2012 年 10 月 29 日 | 欧洲中央银行发布有关虚拟货币及其在欧盟制度下发展潜力的详细报告  |
| 2013 年 12 月 12 日 | 欧洲银行业监管警告消费者使用虚拟货币，因为（1）消费者可能会损失价值；（2）可能会从虚拟钱包中窃取金钱；（3）欧盟退款权利不受到保护；（4）价值会迅速改变；（5）可用于包括洗钱在内的犯罪活动（6）消费者可能要承担税收责任 |
| 2014 年 7 月 28 日  | 欧盟委员会表示将对虚拟货币施加反洗钱和反恐融资规则。   |
| 2015 年 1 月 11 日  | 欧洲法院裁定增值税不适用于通过交易所购买比特币。   |

### 第三章 数字加密货币发展概况

|           |  |
|-----------|--|
| 2016年2月2日 | 欧盟委员会正在对恐怖分子融资和洗钱活动进行风险评估，尤其注意虚拟货币。并且表示欧盟委员会将到2016年六月，针对设计虚拟货币的交易和兑换业务采取更严格的规则 |
| 2017年9月7日 | 欧洲中央银行总裁德拉吉拒绝了爱沙尼亚推出自己的国有数字货币“estcoin”的计划，并表示欧洲央行将不允许爱沙尼亚或任何其他欧盟成员国引入自己的货币。    |

数据来源：欧洲央行官网，Perkins Coie 报告

显然面对这种新的加密货币，与美国和中国当局和金融机构警告投资者可能面临的风险，推动加密货币监管严格化的做法不相同，欧盟内部国家即使认同加密货币可以加强非法活动这一事实，立场仍然松散，鼓励加密货币的创新开放。另一方面，欧盟的相关机构都认可数字货币可能是非常重要的风险资产，且与之相关的技术可以为当前支付系统带来的更好的提升。

### 3.3 比特币的发展现状

#### 3.3.1 比特币的发展历程

比特币是一种基于区块链技术，保证整个支付体系和虚拟货币产生和使用的点对点协议<sup>[44]</sup>。尽管在 1998 年首先描述并提出了加密货币的概念，但比特币成为该理论的第一个实践该这一概念的先行者<sup>[45]</sup>。

比特币是基于区块链的去中心化数字货币，这意味着所有交易都记录并显示在公共分布式数字总账中。它提供了相对较低的交易成本，从而在全球范围内能够提供点对点快速汇款。正如其创始人中本聪所说的，它是一种去中心化的货币，也就是说，没有任何中央机构能够通过区块链技术追寻每一个比特币持有者的个人信息并记录其交易<sup>[46]</sup>。当前，越来越多的新比特币正在通过采矿过程进入比特币网络流通，换句话说，采矿正在为整个比特币网络提供比特币的供应<sup>[47]</sup>。而比特币的价格也随着比特币的不断被挖掘走高。

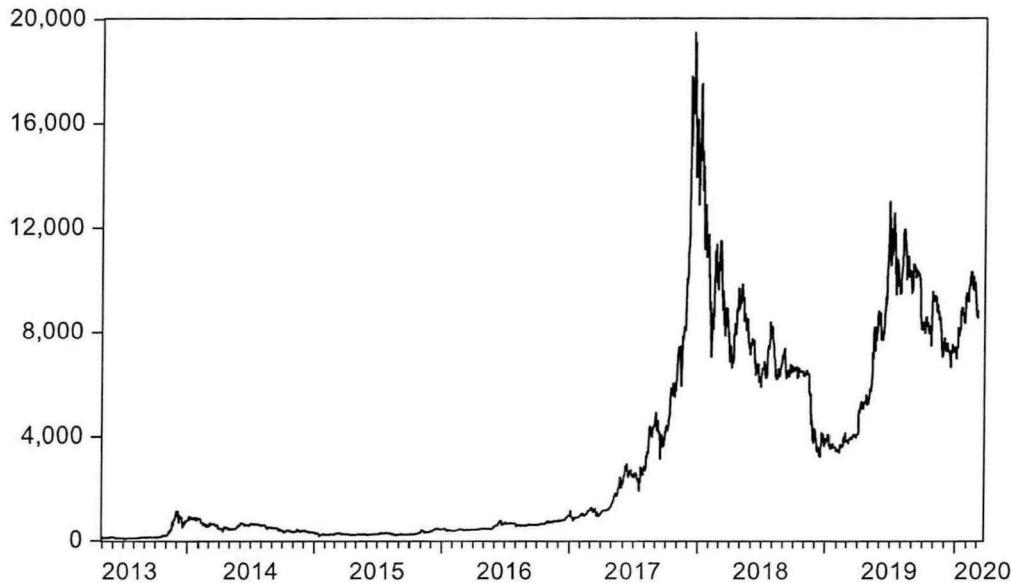


图 3.2 比特币价格走势图

比特币从 2009 年不到一分钱的价格，一度在 2017 年末暴涨接近两万美元关口，几度暴涨暴跌，吸引了大量投资者的投资热情。而从图比特币的历史价格

走势中，可以将比特币的发展归结为四个阶段：

初生阶段，即 2009 年至 2012 年。

2009 年以前，比特币都只是一个理论概念，尚未付诸于实际技术操作。2009 年中本聪发布了有关比特币的相关论文，标志着比特币的诞生。但是诞生之后直到 2010 年，比特币还没有受到市场大众的关注，2010 年，第一个比特币交易平台 Mt. gox 上线，而这也极大的推动了比特币进入交易市场。同年 5 月，一个美国人花费一千个比特币购买了两个披萨，这也是比特币首次被应用于线下商品购买，是比特币的首次商业活动。然而在这个阶段，比特币的参与者大多数都是热爱互联网且了解比特币的极客们。他们不仅热情的参与到比特币相关技术的研讨，同时使用自身的设备担当起矿工的角色，以及在交易平台上交易比特币。而这一时间段的比特币价格也没有太大的波动。

市场机遇阶段，即 2013 至 2015 年。

2013 年比特币经历了第一次价格跳跃。13 年年初比特币的价格仍然徘徊在每个比特币 12 美元的低位状态。然而 3 月受欧债危机影响，塞浦路斯政府关闭银行，这直接引发了人们对于国家央行这一货币中心的信任，比特币开始受到各国媒体和投资者关注，这助推了比特币价格的上升。同年 8 月德国政府承认比特币的货币地位，百度宣布开通比特币支付。这一系列的事件进一步助推了比特币价格暴涨。比特币价格从四月份的 205 美元直接跃升至 1009 美元，11 月直接到达 1242 美元新高。然而市场激情过后，比特币价格也迎来了一段冷静阶段。2014 年至 2015 年，各国开始针对比特币开展一系列监管规范活动。中国央行于 2013 年底发布了《关于防范比特币风险的通知》，2014 年初当时最大的比特币交易平台 Mt. gox 宣布因被盗 85 万个比特币而被迫破产清算，这一系列的事件给当时的比特币市场泼了一盆冷水，比特币市场随即进入了熊市。

主流阶段，即 2016 至 2018 年。

2016 年英国宣布脱欧，朝鲜核实验事件，特朗普当选等事件，使得世界经济不确定性增加，市场避险情绪激增。而具备避险功能，且与世界主流经济有替代关系的比特币在 13 年的暴涨过后，市场需求扩大。而世界各地投资者的涌入推动了比特币行业的各个环节建设，进一步推动了交易规模。即使部分政府不断加大监管力度，随着韩国、日本、拉美的比特币市场开始不断升温，比特币的价格从 2016 年的 400 美元暴涨到 2017 年底的 20000 美元。比特币的价格疯狂使得比特币完全进入了全球视野，同时随着比特币期货在芝加哥商品交易所上线，

比特币也正式成为了主流的投资品之一。而 2017 年暴涨之后，价格泡沫被刺破，市场开始回归理性。

产业落地阶段，即 2018 年至今。

比特币市场在 2017 年经历了市场疯狂之后，在监管层、市场认知、以及产业发展层面都开始回归理性。比特币的价格泡沫被刺破，在牛市阶段涌现出来的各种加密货币不断在市场预冷，越来越多行业链上众多因为比特币价格暴涨而造就的比特币项目也随着 2018 年的熊市开始暴雷消亡，然而 2019 年一小部分优质的企业和项目在这个产业链上初步落地，开始接受市场的检验。区块链这个比特币的底层支持技术开始被大众所熟知和接受，各国也开始落地区块链项目，布局区块链行业的未来发展，加密货币的行业发展也开始进入更迭阶段。

#### 3.3.2 比特币的应用变化

比特币虽然作为加密货币和投机性资产被大众所熟知，但是其主要的真实用途却随着加密货币行业的发展和监管层面的不断加强而不断变化。

早期阶段，比特币因其匿名性高的特点，主要被应用于丝绸之路和其它一些跨国违法犯罪活动。

在 2010 年比特币开始被应用于商业活动之后，第一个大规模使用比特币的是那些要求更多匿名性交易以及缺乏买卖规则的交易商，例如涉及毒品、麻醉药品的在线销售等。在北美市场，毒品在网络上的销售已经泛滥多年，通常是在非正式的网络公告板上以及“农夫市场”之类的网站上发布信息私下交易。此类网站还支持通过使用包括 PayPal 在内的网络支付服务商付费购买的各种毒品和违禁品<sup>[48]</sup>。而当比特币出现则与违法交易所要求的匿名性不谋而合，为此类市场交易提供更强的匿名保证。因而比特币也一定程度上助推了毒品的线上交易量。

丝绸之路匿名在线交易网站是第一家专门支持比特币交易的网站，在开始运营仅一年后，每年的交易额就达到了 1500 万美元<sup>[49]</sup>。根据 Christin 统计，丝绸之路在 2013 年的交易类目中，排名最高的是大麻，拥有 3338 个大麻销售窗口，其次是毒品，共计 2193 个毒品在售。这些商品的交易都依赖于比特币交易的匿名性。

赌博网站也是这一阶段比特币的主要使用者之一。为了保护用户隐私，并且为了向这些不便于使用正规渠道汇款的用户收费，博彩网站也大规模的使用了

比特币。例如，当时最受欢迎的单一比特币赌博游戏是 Satoshi Dice，这是一种简单的博彩游戏，如果骰子掷骰数小于玩家选择的数字，则该玩家将获胜。这项博彩服务向外披露了 2012 年约 33,000 个比特币的收入，当时平均每月增长了 78%<sup>[50]</sup>。

现阶段，比特币主要用于消费者付款，购买以及持有等用途。

比特币作为一种支付工具，也具备交易成本低的优势。信用卡和借记卡的手续费高在当时受到广大互联网商家和消费者质疑和批评，而这时比特币凭借自身支付成本低廉的优势，向大众提供了一种新的支付替代方案。而一些商家的做法也确实证实了比特币可能具有这种替代作用。美国在线零售商 Overstock.com 于 2014 年 1 月开始接受比特币付款。而这也从 Overstock 后来的财报中也反映出了良好的回馈，包括可观的收入增长，增长的平均订单量和扩大的客户群体<sup>[51]</sup>。随后，其他美国企业也增加了对比特币的支持，包括 Expedia（旅行），Newegg（电子），Foodler（餐馆交货和外卖），Gyft（数十个商人的礼品卡）和 TigerDirect（电子）。支付的优化需求倒逼着互联网商家调整其网站的支付系统以接受比特币。早期使用比特币付款的用户评论好坏参半，尽管有时会出现技术故障，难以支付，但用户节省了支付手续费，似乎对新的支付方法很满意。同时对互联网商家而言，比特币支付处理相对于各大银行支付系统是非常低廉的。例如，Coinbase（一家比特币支付处理公司）目前对每位支持比特币付款的商家收取每年不超过 1% 的费用，即每家公司不超过 100 万美元的费用，这 1% 的支付成本大大低于使用信用卡付款时商家所承担的费用。

同时，其他用户购买比特币不是为了使用比特币，而是为了持有至其升值进而获利。在 2009–2012 年期间开采的比特币中，有 60% 以上的比特币被持有一年以上，仍未被使用或花费<sup>[52]</sup>。而比特币数次价格暴涨也助推了大批量的投资者买进比特币，甚至持有其他加密货币，将其看做是一项投机性资产以等待其未来价格的暴涨，实现自身财富增长。

未来，乐观的角度看，比特币的用途将变得更加广泛，不仅可以做为通用的付款方式，主流的价值存储，而且可以为区块链技术的落地提供技术启发。而悲观的看比特币价值，其未来的发展前景将进一步受到监管限制，未来可能只作为国家的数字货币发行的启发事物。

### 3.3.3 比特币的主要特征

#### 3.3.3.1 去中心化

通常而言，无论是各国的法定货币，还是紧随比特币价格暴涨推出的各种加密货币，他们的发行和流通都依靠一个货币的权利中心。对美元而言，这个中心是美联储。美联储决定着每年美元的新投放量和旧币的销毁量，进而这个中心也影响着美元的价值。而人们持有这些美元的价值，也时刻受到美联储对市场通货膨胀和市场利率的影响。当今世界的银行体系也基本是以银行为中心，以中国为例，货币的产生和发行是由央行决定，支付转账活动也是经由银行充当信用中介完成，大部分的货币储存也是经由各类银行完成。

受金融危机的影响，比特币的设计者们基于点对点的交易机制，试图创造一个不需要货币发行中心，且完全不受货币中心影响的新型货币，以削弱通胀以及不稳定的中心政策对该货币的影响。而比特币的去中心化，狭义而言，是基于区块链技术，搭建点对点的支付网络，取代人们正常货币活动的中心。每个节点成为了高度自治的个体中心，而每个节点之间的交易不需要经由银行之类的货币中心，点对点即可完成。而点对点的交易活动的信用和安全保障则交由区块链技术的分布式账本完成。

与法定货币以及后续出现的大量加密货币相比，比特币最大的创新点是其完全去中心化的特点。而这也是比特币设计者们的初衷，也是早期使用比特币的极客们最为推崇的优点之一。去中心化特征也给比特币体系带来了众多优势。

首先，去中心化最大的好处就是避免了权力的集中，避免了一个节点权利过于集中，进而影响和控制其他节点的交易活动。其次，去中心化也可以提高计算机系统的可用性和弹性，从而避免出现因为中心故障而导致整个系统瘫痪失效。此外，它能够为用户提供了更大的隐私保护和安全保护，因为从其设计理论上说，一个窃听的对手无法通过针对任何单个点或任何单个服务器来观察整个系统中的交易。最后，去中心化也意味着每个节点都是平等的，不存在中心系统的上下级关系，也就很好的解决了节点直接的勾结问题，避免了由于单个区域勾结篡改数据的可能性。

尽管如此，比特币的去中心化理想并没有完全被实现。虽然比特币协议支持完全的权力下放（包括所有参与者充当矿工的可能性），但强大的经济力量推动着比特币集中于比特币生态系统各个级别的少数中间人。比特币行业的主要参

与者，矿工、货币兑换交易平台，数字钱包服务，支付系统等，都呈现除了不同程度的比特币中心态势。例如，曾经比特币的交易平台 MT. GOX 曾经泄露 8 万枚比特币，导致当时比特币市场价格的暴跌。而算力最强的矿池也能够在比特币产生之初对比特币的协议进行改写，进而影响整个比特币生态系统。

### 3.3.3.2 匿名性

在中心化的真实货币世界中，银行作为货币交易中心点，为了给一笔交易的完成做信用背书，必须掌握着交易双方的具体信息，包括个人住址、通讯信息、信用状况等等，以防止洗钱等非法交易行为。而比特币的交易网络是点对点的交易网络，其中交易设计并不涉及两个交易节点的个人信息。

比特币依赖于密码学的两项基本技术，即公私钥密码学用以存储和交易比特币，以及对交易的密码验证技术。标准的公私钥加密技术使任何人都可以创建公钥和关联的私钥<sup>[53]</sup>。而公钥被设计为广泛共享，私钥只能由拥有该所有权的人拥有。例如，使用公钥加密的邮件只能由拥有相应私钥的某人解密，从而允许任何人加密仅指定收件人可以阅读的邮件。同样，用私钥加密的消息只能用相应的公钥解密，从而允许指定的发件人创建可以被确认为真实的消息。

公私钥加密技术使得比特币的拥有和交易变得更加安全和高效，也使得比特币的交易匿名性更加显著。私钥在比特币当中相当于对比特币的所有权，而公钥相当于一个匿名的收款地址，也相当于计入被共享账本的密码。当甲转让比特币给乙方时候，乙方会根据这个比特币的公钥在区块链的各个节点上审核这个比特币的交易真实性，一旦确认，乙方就可以确认接收这个比特币，而这个交易也会被计入区块链的各个节点中，其他用户也只能指导一笔比特币从一个地址转让到了另一个地址。在整个交易过程中，交易双方的个人信息不需要向对方公开，也不需要任何信用中心核验各种身份信息和信用信息，保证了交易的匿名性。

然而这种匿名性只是有限的匿名，比特币另一个特征，即公开性，限制了比特币交易的完全匿名性。比特币的交易都由字符串完成，而这些字符串不会连接到个人的任何信息，就如带着面具做货币交易。然而，每一笔交易的完成都必须上传到区块链当中，每一个节点都会知道这一交易的完成，而且是永久性且不可被篡改。这使得每一个比特币的交易都是公开透明的，也使得每个比特币的交易可寻根溯源。这个公共账本对于监管当局而言是一个庞大的信息金矿，通过查询被用作洗钱等违法行为的比特币交易信息，就可以利用相关技术查到违法人员。例如美国当局正是利用区块链中的信息，查询到 Mt. gox 被盗取的八万个比特币

的下落。

### 3.3.3.3 内置激励性

比特币的设计创新之一在于其对激励制度的设计，这一设计激发了比特币网络内部共同维护比特币网络，保证即使没有权威中心的维护下整个网络的安全性和正常运行。

比特币内置了众多激励措施，以鼓励维护整个网络的有用行为。首先，验证区块链的矿工将获得比特币奖励。每一次交易的发生都要经由各个节点验证，而首先将十分钟内的交易验证成功并打包成一个区块的矿工就可以获得相应的比特币奖励。这也被称为出块奖励。在比特币发行之初，解决难题的矿工将获得 50 枚比特币的奖励。比特币的奖励将定期减半，以此控制比特币发行的速度和总量。预计铸造 2100 万比特币后，奖励降至零，将不再创建比特币。因此，比特币的协议设计为货币的扩张设定了可控的步伐，并且最终能够限制发行的比特币数量。

其次，第二种奖励来自于交易的手续费，这也是矿工的第二种潜在的收入来源。在发出交易信息时，买卖双方可以提出支付“交易费”，吸引更多矿工加快对交易信息的验证，这是对潜在矿工解决验证交易难题的比特币奖励。相对而言，目前的交易费用低于总交易额的 0.1%<sup>[54]</sup>。随着区块验证变得越来越困难，出块奖励也会随着比特币的供应放缓而下降，可能会出现区块验证的自动奖励低于这样做的成本的情况。未来，区块链的验证更多靠的是那些想要进行比特币交易的人支付的可选交易费用。

激励制度的设计，既解决了比特币的发行问题，保证了矿工验证区块的积极性，又有助于避免篡改区块链的欺诈行为。原则上，像比特币这样的系统可以通过多数表决通过简单的共识来验证交易，并且大多数关联用户都可以确认确实发生了给定的交易。但是随后，攻击者也可以通过创建大量假身份来对系统进行欺诈。作为回应，比特币协议使得提交假投票的成本很高。比特币协议为此设计了工作量证明，比特币实施了“一个计算周期一票”的原则代替“一个人一票”。通过这种设计，工作量证明机制会不仅能够阻止创建大量伪造身份，并且还给潜在矿工们提供了动机来参与验证区块链。

## 3.4 以太币的发展现状

### 3.4.1 以太币的发展历程

以太坊是一个基于区块链技术使用内置的图灵完备编程语言来运行智能合约的去中心化平台<sup>[55]</sup>。以太坊旨在利用和改善中本聪在比特币设计的区块链架构概念，搭建一个适合企业和个人使用的区块链平台。而以太币作为以太坊网络内部使用的货币，一方面跟比特币的区块奖励一样，作为对以太坊网络运算的奖励，另一方面也作为以太坊内部项目企业融资的手段。

以太币在币圈被称作是比特币 2.0，其对于比特币网络的改进是最富有创新性，也是广受业界关注的，因而其价格走势也随着比特币的变化而波动。

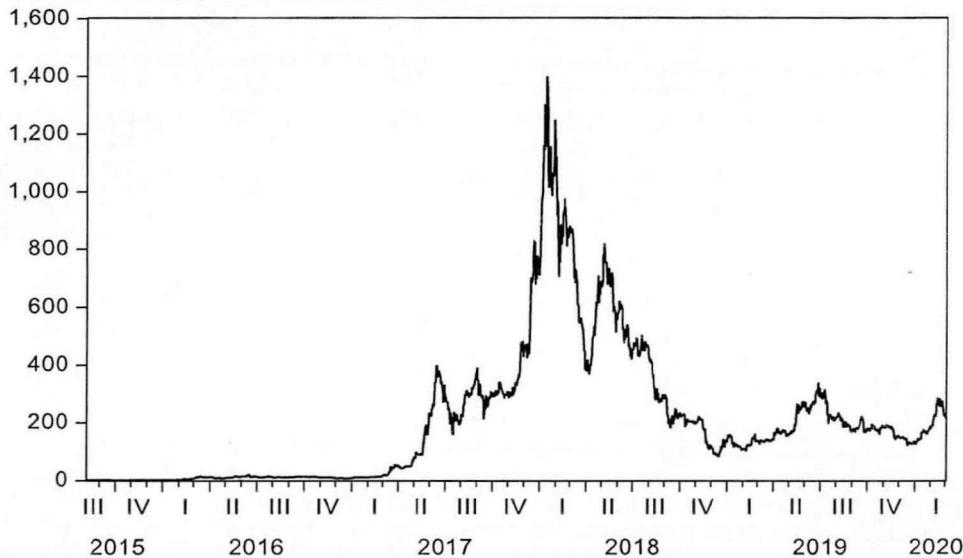


图 3.3 以太币价格走势

如图 3.3 所示，以太币的价格波动剧烈，在短短五年的时间里，以太币的价格曾经冲高至 1400 美元的价格神话，也快速跌落回几百美元区间。而从图中以太币的历史价格走势中，可以将以太币的发展归结为以下几个阶段：

初生阶段，即 2015 年至 2016 年。

以太坊团队曾于 2014 年往外公开众筹，开放短时间内的以太币预售，募集到 3 万个比特币，发售出近 6 亿个以太币，以募集到以太坊初期建设资金。然而这个时候的以太币还并没有正式在交易平台交易。直到 2015 年第一阶段的以太坊上线，同年 7 月份才开始正式在交易平台交易。这时候的数字货币被投资者广

泛关注，而作为比特币 2.0 的以太币也在这个阶段成为了加密货币的明星货币。2015 年 10 月 22 日，以太币价格还徘徊在 0.42 美元附近，随后一路上涨，并在 10 月 30 日涨至 1.16 美元，不到十天以太币价格上涨了近三倍。这个阶段的以太币由于尚未进入其开发者所宣传的实际应用阶段，价格虽然一直在震荡上行，但是并没有出现极端上涨情况。

#### 泡沫阶段，2016 年初至 2017 年末。

2016 年初，以太坊智能合约的区块链应用开始上线，以太坊走上实际应用阶段。而这时候加密货币实际热度暴涨，以太币也在这个加密货币市场狂欢的过程中，价格一度暴涨。2016 年初以太币的价格还徘徊在几美元的低位，然而 2017 年的后两个季度，以太币价格开始疯涨，一度涨至历史顶点 1400 美元一枚。这个阶段的加密货币市场充满了价格泡沫，不理性的投资者得到一个以太币应用的故事，便开始进入这个市场，疯狂购买和持有以太币。对比 2017 年初以太币价格，以太币在年末完成了近百倍的收益回报。

#### 市场冷静阶段，2018 年初至今。

2018 年加密货币市场开始回归冷静，以太币的价格也开始从历史顶点一路腰斩。2018 年 7 月 31 日，以太币价格一路回落至 142 美元，随后一直在两百美元价格区间内徘徊。这跌落的速度和幅度也让很多投资者始料不及，而当时比特币价格的暴跌也进一步刺激了以太币市场价格下跌。当市场开始冷静下来，以太币背后的以太坊扩容和性能问题也开始被不断暴露，以太坊所描绘的区块链应用未来还需要更多的新方法和更多的尝试和探索。

### 3.4.2 以太币的应用变化

以太坊的发展被设计成四个阶段，即前沿(Frontier)、家园(Homestead)、大都会(Metropolis)、宁静(serenity)。因而其整体用途变化也与其技术更新相关。

2013年以太坊创始人Vitalik Buterin发布《以太坊白皮书》<sup>[56]</sup>，标志着以太坊的诞生。2014年以太坊通过代币众筹方式，获得了大量的启动资金。如下表所示，仅仅一年之后，以太坊前沿阶段就正式投入使用。2016年以太坊进入第二阶段家园，2016年末进入第三阶段。2017年，大量知名进驻以太坊联盟，参与到以太坊生态。

表 3.4 以太坊发展事件表

| 时间       | 事件  |
|----------|---|
| 2013年末   | Vitalik Buterin 发表了《以太坊白皮书》，解释了以太坊技术框架和发展路径，标志着以太坊的诞生       |
| 2014年4月  | Gavin Wood 发表了《以太坊黄皮书》，解释了以太坊虚拟机的技术架构                       |
| 2014年6月  | 以太坊基金在瑞士设立，以促进以太坊协议和技术的开发和应用                                |
| 2014年10月 | 以太坊开放以太币预售，以募集启动资金  |
| 2014年10月 | 以太坊的出块时间缩短至12秒，标志着以太坊性能趋于稳定                                 |
| 2015年7月  | 以太坊前沿(Frontier)阶段正式发布，作为以太坊第一阶段，开发者从此可以在以太坊上开始编写智能合约和开放智能应用 |
| 2015年7月  | 以太币开始在众多交易平台交易  |
| 2016年3月  | 以太坊进入第二阶段“家园”(homestead)，开始提供智能钱包，为普通用户提供更加良好的用户体验          |
| 2016年6月  | 以太坊一个去中心化节点组织The DAO遭受黑客攻击，损失市值五千万美元的以太币                    |
| 2016年12月 | 以太坊进入第三阶段“大都会”(Metropolis)，Mist浏览器正式上线                      |
| 2017年5月  | 新增86家企业进驻以太坊联盟(EEA)，包括摩通大根、微软等企业的进驻给以太坊带来了巨大的正面效应           |

数据来源：ETHFANS 网站、笔者整理

前沿阶段是以太币初级版本的展现，开发者开始可以在以太坊挖矿，获得

以太币，同时也开始可以在以太币搭建的框架下开发各种智能合约工具和dApp（以太坊网络开发的应用）。前沿阶段的以太坊更多是开发者测试阶段，版本相对应而言比较复杂。家园阶段是以太坊的第一个正式版本，以太坊协议被优化更新，系统更加稳定，交易速度加快，普通用户也可以参与以太币挖掘。

ICO代币融资是前沿阶段和家园阶段时期以太坊的主要用途。ICO代币众筹模式在以太坊上线之初就备受币圈投资者关注，其主要思想是将传统的众筹方式放置于以太坊的区块链之中，发行相应代币，投资人以以太币购买此种代币，进而触发智能合约，进而合约将代币发放至投资者账户，在保证投资者权益的同时，促进新项目的融资进程。

截止当前，基于ERC-20标准发行于以太坊之中的ICO融资代币共有255642种，其中五个市值最大的代币融资如下表所示。以太坊代币中，市值超过一亿美金的代币有近12个，市值介于一千万美元和一亿美元之间代币有近80个。

表3.5 以太坊市值最高的五个代币

| 代币                       | 特点  | 市值(美元)        | 持有人(个)    |
|--------------------------|---|---------------|-----------|
| Tether USD (USDT)        | 数字时代的数字货币   | 6,365,155,606 | 1,142,015 |
| BNB (BNB)                | 旨在建立世界一流的加密货币交易所  | 2,400,670,789 | 313,855   |
| ChainLink Token (LINK)   | 基于区块链的中间件，充当加密货币智能合约，数据馈送，API和传统银行账户付款之间的桥梁。                  | 1,187,304,512 | 120,700   |
| Bitfinex LEO Token (LEO) | 一种实用程序令牌，旨在赋予Bitfinex社区权力，并为那些寻求最大化Bitfinex交易平台的输出和功能的人提供实用程序 | 1,017,125,144 | 1,807     |
| HuobiToken (HT)          | 火币全球是世界领先的加密货币金融服务集团。   | 850,786,860   | 10,865    |

数据来源：Etherscan网站

然而依靠以太坊发行代币融资却存在一些问题。首要问题是效率问题。以太坊在家园阶段的事务处理机制遵循时间原则，然而以太坊允许矿工设置自己合约的服务优先级，当以太坊需要处理的账户和事务数量短时间骤然增加，矿机服务碎片化容易导致大量事务延迟，进而影响合约触发和执行。其次，以太

坊内部流通的以太币同样会对 ICO 造成价格风险。此外，最为关键的问题在于对于众筹的项目没有审查和监管，因而没有解决众筹的道德风险，也让各国的监管机构对 ICO 融资产生了怀疑甚至禁止的态度。

大都会阶段，是以太坊使用区块链工作量证明协议（POW）的最后一个阶段，在这个版本，以太坊变得更加轻量级，交易更加快速安全，为进入下一个权益证明阶段奠定技术基础。

Dapp（Decentralized Application）即去中心化应用，是这一阶段以太坊的主要应用方向。过上一阶段的代币融资，众多区块链程序项目开始正式将精力放于去中心化应用开发上。这些项目通过以太坊上的智能合约，尝试用各种解决方案搭建取代中心化的应用。

截止 2019 年，以太坊 Dapp 总数已经高达 3477 个，其中涵盖了金融、物联网、智慧电网、体育博彩、游戏等多个领域。根据 Dapp 网站数据，2019 年第一季度，以太坊在整个区块链领域一度占据了近 60% 的市场份额。同时，2019 年活跃 Dapp 数高到 1129 个，活跃用户高达 143 万。下表 3.3 即部分去中心化应用。

表 3.6 以太坊部分去中心化应用

| Dapp          | 领域   | 特点                  |
|---------------|------|---------------------|
| The DAO       | 金融   | 创业投资，为以太坊应用提供去中心化融资 |
| CryptoKitties | 游戏   | 虚拟养猫游戏              |
| Fomo 3D       | 博彩   | 旁氏骗局类博彩游戏           |
| Etheropt      | 金融   | 去中心化期权交易市场          |
| Freemyvunk    | 交易平台 | 虚拟事物交易平台            |

数据来源：Etherscan 网站

宁静阶段是以太坊的最后阶段，在这个阶段为了解决工作量证明机制带来的中心化趋势，避免大算力的挖矿公司在挖矿源头控制哈希值，以太坊改用权益证明（PoS），同时将底层协议采用硬分叉，将以太坊达到完备状态。

虽然以太坊技术阶段并没有完全进入最后的宁静阶段，但是以太坊的应用空间已经在第三个阶段即大都会阶段被打开，众多的去中心化应用爱好者已经涌入以太坊开始编写去中心化应用。但是，从 ICO 融资到当前的去中心化应用，以太坊的应用变化，一直在为以太币增添着其作为以太坊内部流通货币的应用价值。未来，以太坊仍需要进一步革新技术，打开更加广阔的应用空间。

### 3.4.3 以太币的主要特征

#### 3.4.3.1 智能合约

智能合约是以太坊最为重要和突出的一个特征，指的是能够在以太坊区块链上可以自动执行的计算机程序<sup>[57]</sup>。简单而言，智能合约是完全按照创建者设置的程序自动执行的程序。图 3.1 即以太坊智能合约运作的简单流程。智能合约首先由创建者使用以太坊接受的 Solidity 和 Serpent 等编程语言编写创建，其次再将此合约部署并广播到以太坊的区块链之中，最后当触发合约条件之后将被 EVM 自动执行。

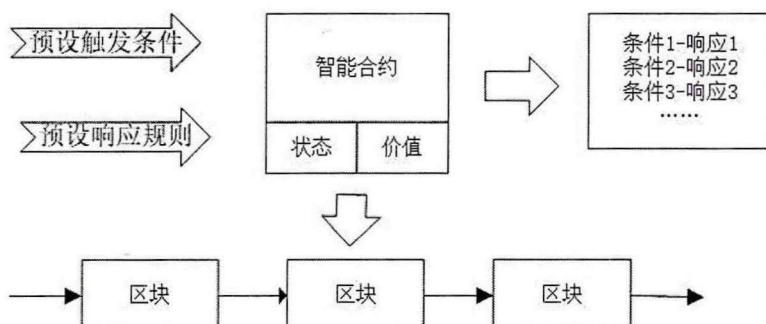


图 3.1 智能合约示意图

智能合约是以太币区别于比特币的最重要特点。比特币作为点对点的支付货币系统，其区块链技术仅仅局限于分布式的数据存储平台，不具备图灵完备性，进而也不具备进一步提升开发应用前景。然而，智能合约公开透明、不可修改、确保执行的特点，改进了比特币区块链的局限性，使得众多开发者可以在以太坊上创建智能合约，进而开发去中心化的应用，扩展了区块链技术的应用前景，提升了区块链的应用灵活性。

#### 3.4.3.2 区块多样化

比特币存在的缺陷之一是造成算力的浪费。在比特币固定十分钟的出块时间当中，一些区块链的临时分叉由于没有接入到主链上，而被主链丢弃，但是这部分也是由矿工使用大量算力得到，因而造成了算力的浪费，损害矿工积极性。

在比特币的基础上，以太币虽然将出块效率提升到了 15 秒的出块时间，但是由此也会带来更多的区块链临时分叉，进而带来更多的算力浪费。为了解决这一问题，以太币采用了 Ghost 协议和叔块奖励的做法。

叔块在 Ghost 协议中被定义为当前区块的前 2 至 7 层的区块的直接字块，由于矿工速度慢产生的没有被接入主链，但是在之后被主链发现并接入的区块。因而，如果叔块在后续的区块链中通过相应字段收入主链，叔块的矿工们也会被给予以太币奖励。反之，如果没有被后续区块收入，则仍然会被抛弃成孤儿块。

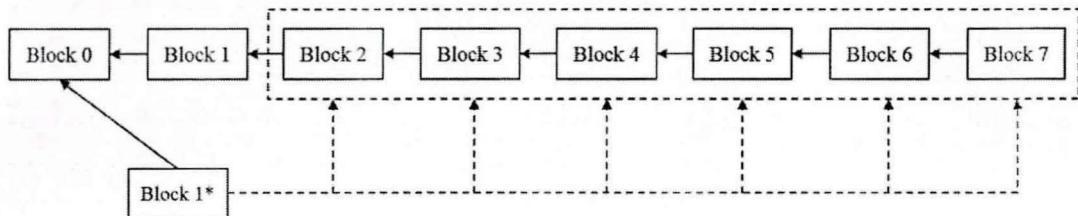


图 3.2 叔块示意图

叔块的设计一方面减轻算力浪费的问题。效率的提升使得以太币出块时间仅仅短短几十秒，由此催生了众多孤块和分叉链，叔块的设计能够将之前合法的孤块再度接入主链，提升整个主链的安全性。另一方面，叔块奖励能够降低矿池集中度的问题，降低算力大的矿池从源头控制大量以太币的情况，提升安全性。

### 3.4.4 比特币和以太币的对比分析

#### 3.4.4.1 相同之处

以太币作为想要替代比特币的存在，也承袭了很多比特币的特点和技术。两者在众多地方有着相同之处。

首先，两者都基于区块链技术，都会形成一个完整的区块链条。

与比特币一样，以太坊同样也有一条完整的区块链，而这个区块链由众多数据块拼接链条而成。而每个区块的产生和验证的过程，也由类似比特币的矿工完成。同样，每个区块的链接过程，以太币也是通过前一个区块的哈希值链接完成。正因如此，以太坊和比特币一样都具备中心化的特征。同时，双方都是一个公开透明且不需要许可的加密货币网络。也就是说，在比特币和以太币的网络中，参与者都不需要任何的机构审核，就可以自发的完成挖矿和加密货币验证的程序。

其次，以太币在前三个阶段都是采用工作量证明（PoW）机制挖矿。

比特币的矿工们获得比特币靠的是出块奖励和交易费用收取两种方式，通过最快的完成验算创造有效区块来获得比特币奖励。而以太币的前三个阶段也是同样如此，矿工通过算力解开难题，创建有效区块，获得以太币。然后两个还是有一定细微差距，以太币的工作量证明方法被称为 Rthash，它降低了挖矿过

程对硬件的门槛，使得普通的硬件挖矿成为了可能。

### 3.4.4.2 不同之处

尽管以太币承袭了比特币的众多特点和技术，以太币相比于比特币有着自身更为鲜明的特色。

首先，以太币的出块时间更加的快速和高效。

由于比特币挖矿过程对硬件算力要求很高，目前比特币的出块时间一般在十分钟左右，特别是到了新生比特币供应量减少的后期，出块时间也会进一步增加。而以太币的出块时间间隔在 14 秒左右。这个时间差距意味着，以太币系统对区块链的区块更新比比特币更快更加高效。

其次，以太币拥有更小更多样的区块。

以太币和比特币都对区块的大小有相应的限制。比特币的区块大小以字节来衡量，且每个区块被限制为 1MB。而以太币的区块大小以智能合约的复杂程度来衡量，这个限制标准也被称为“区块 GAS 上限”。每个区块的大小限制也会根据合约的复杂程度不同而有所不同。当前以太币区块中最大的区块大约为 150 万 GAS。当前，平均每个以太币区块可以容纳近 70 笔交易，而比特币区块则容纳了近 1500 笔交易。因而，以太币区块大小均在 2KB 左右。而这也降低了矿工们挖矿对硬件的要求。

同时以太币的区块也比比特币的种类更加丰富。比特币的区块中，若是有部分区块因为矿工速度慢没有被接入主链，则会被视作废块或者孤儿块。并且比特币协议不会对这部分矿工进行比特币奖励，进而这部分矿工的工作量则被浪费了。然而以太币将这部分因为矿工速度慢产生的废块称为叔块。如果叔块在后续的区块链中通过相应字段收入主链，叔块的矿工们也会被给予以太币奖励。反之，如果没有被后续区块收入，则仍然会被抛弃成孤儿块。

## 第四章 数字加密货币市场风险度量

### 4.1 数据来源

本文选取了比特币和以太币作为加密货币风险度量标的，研究 EVT-VaR 模型 GARCH-VaR 模型的比较应用，并引入规范的回测方法考察两者风险度量的准确性。

由于比特币自 2013 年才受到人们广泛关注，其价格也于 2013 年开始暴涨，故而本文选取了选取 2013 年 4 月 29 日至 2020 年 02 月 24 日以美元标价的比特币价格作为研究对象。同时选取了 2016 年 1 月 1 日至 2019 年 12 月 31 日以美元计价的以太币价格。价格数据来源于 Coinmarketcap 网。

由于数字货币的交易是全天候无间断交易，故当日收盘价取自当日晚 24 点价格，且昨日收盘价与今日开盘价格一致。比特币的收益率  $R_t$  为价格的对数收益率  $R_t = \ln P_t - \ln P_{t-1}$ ，其中， $R_t$  表示  $t$  日当日收益率， $P_t$  为当日收盘价， $P_{t-1}$  为昨日收盘价。

### 4.2 数据检验

#### 4.2.1 正态性检验

为检验比特币和以太币的收益率是否符合正态分布，本文利用收益率相对于正太分布的 Q-Q 图。Q-Q (Quantile-Quantile) 图是一种图形技术，是第一数据集的分位数对第二数据集的分位数的图，用于确定两个数据集是否来自具有共同分布。Q-Q 图上绘制了 45 度角参考线，如果两个数据集来自同一分布，则这些点将落在该参考线上。

图 4.1 中纵轴即正态分布的分位数，横轴即比特币收益率分布的分位数，红色直线代表高斯正太分布线，而蓝色散点对应着比特币收益率分布的分位数。如果蓝色散点分布越是接近直线，则其实际分布则越接近正太分布，反之则越不符合正太分布。

从图 4.1 可以明显看出比特币和以太币的收益率分布偏离了参考线，进而判断比特币收益率分布不符合正态分布。同时如表 4.1 所示，比特币收益率均值为 0.0024，序列标准差为 0.03808，偏度为 1.1392，峰值为 13.9146，远高于正态分布，具有明显的尖峰厚尾特征。以太币收益率均值为 0.001317，偏度为 -0.4005，峰度为 7.9679，同样不符合正太分布，具有明显的尖峰厚尾特征。

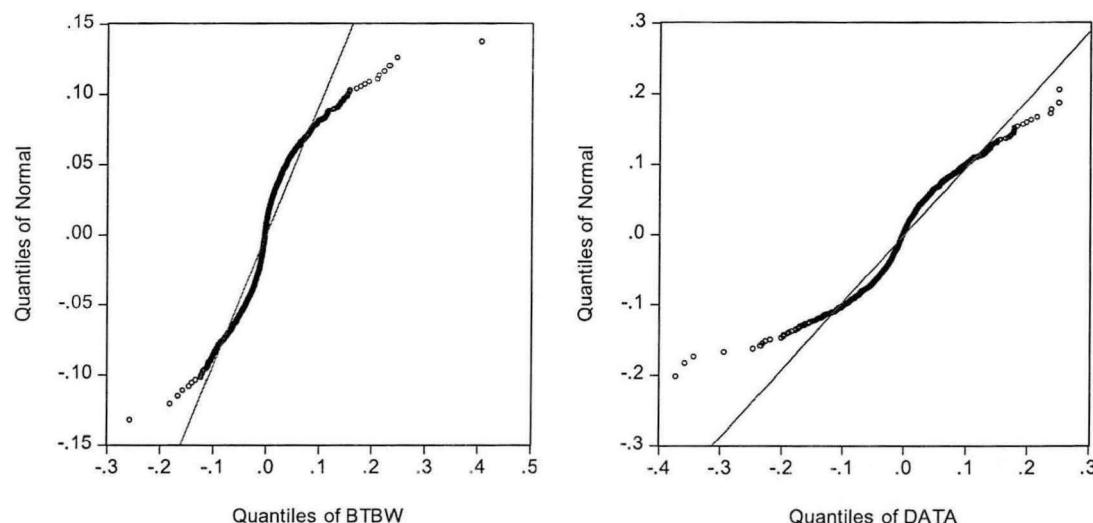


图 4.1 比特币和以太币收益率 Q-Q 图

表 4.1 比特币和以太币收益率描述性数据

|        | 均值       | 标准差      | 偏度      | 峰度      |
|--------|----------|----------|---------|---------|
| 比特币收益率 | 0.0024   | 0.03808  | 1.1392  | 13.9146 |
| 以太币收益率 | 0.001317 | 0.060015 | -0.4005 | 7.9679  |

## 4.2.2 平稳性和自相关检验

### 4.2.2.1 平稳性

本文针对比特币和以太币的收益率进行 ADF 检验。如表 4.1 显示，比特币 t 统计量为 -49.98517，以太币 t 统计量为 -16.6829，小于 1%、5%、10% 置信度下的临界值，同时两者的 P-value = 0.0，拒绝存在单位根的原假设，这表明比特币和以太币的收益率序列都是显著平稳的。

表 4.2 比特币和以太币收益率单位根检验

|                       | 比特币收益率      |           | 以太币收益率      |           |
|-----------------------|-------------|-----------|-------------|-----------|
|                       | t-Statistic | Prob.*    | t-Statistic | Prob.*    |
| ADF test statistic    | -49.98517   | 0.0000    | -16.682     | 0.0000    |
| Test critical values: | 1% level    | -3.961725 |             | -3.961725 |
|                       | 5% level    | -3.411610 |             | -3.411610 |
|                       | 10% level   | -3.127675 |             | -3.127675 |

### 4.1.3.2 自相关检验

根据下图比特币和以太币的收益率时间序列图可以初步看出，收益率序列整体是平整的，但是其波动具有从集性效应，比特币 2013 年和 2017 年两次大的波动后面也同样伴随着较为大的波动，而 2016 年附近的小波动也伴随着较小的波动。同样以太币的 2017 年波动也伴随着较小的波动。而这也反映了两个加密货币序列的相关性特征。

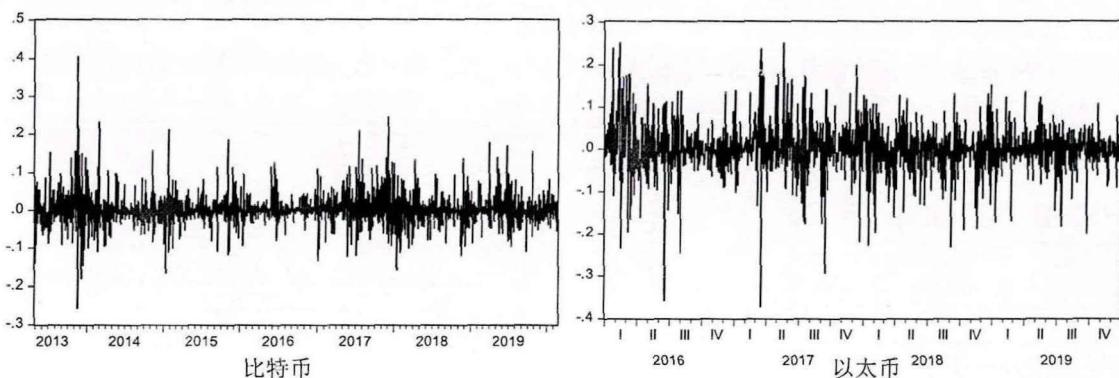


图 4.2 收益率时序图

针对两者收益率序列自相关检验，本文利用 Eviews 绘制了两者的自相关系

数图和偏相关系数图，结果如图 4.3 显示。两者的自相关系数在不同程度上均落在置信区间之外，且 Q 统计量在 95% 的置信区间均拒绝了原假设，则比特币和以太币收益率序列均具有自相关性。

图 4.3 自相关和偏相关系数图

|  |  | 比特币                           |                     |    |     |        | 以太币  |                               |                     |    |     |        |      |
|--|--|-------------------------------|---------------------|----|-----|--------|------|-------------------------------|---------------------|----|-----|--------|------|
|  |  | Autocorrelation               | Partial Correlation | AC | PAC | Q-Stat | Prob | Autocorrelation               | Partial Correlation | AC | PAC | Q-Stat | Prob |
|  |  | 1 -0.002 -0.002 0.0112 0.916  |                     |    |     |        |      | 1 -0.501 -0.501 367.06 0.000  |                     |    |     |        |      |
|  |  | 2 -0.015 -0.015 0.6022 0.740  |                     |    |     |        |      | 2 -0.015 -0.355 367.37 0.000  |                     |    |     |        |      |
|  |  | 3 0.007 0.007 0.7175 0.869    |                     |    |     |        |      | 3 0.053 -0.205 371.53 0.000   |                     |    |     |        |      |
|  |  | 4 0.026 0.026 2.4313 0.657    |                     |    |     |        |      | 4 -0.054 -0.197 375.79 0.000  |                     |    |     |        |      |
|  |  | 5 0.051 0.052 8.9997 0.109    |                     |    |     |        |      | 5 0.017 -0.163 376.21 0.000   |                     |    |     |        |      |
|  |  | 6 0.055 0.056 16.5115 0.011   |                     |    |     |        |      | 6 0.003 -0.137 376.23 0.000   |                     |    |     |        |      |
|  |  | 7 -0.007 -0.005 16.640 0.020  |                     |    |     |        |      | 7 0.002 -0.109 376.23 0.000   |                     |    |     |        |      |
|  |  | 8 -0.008 -0.008 16.800 0.032  |                     |    |     |        |      | 8 -0.004 -0.097 376.25 0.000  |                     |    |     |        |      |
|  |  | 9 -0.002 -0.005 16.806 0.052  |                     |    |     |        |      | 9 -0.015 -0.115 376.64 0.000  |                     |    |     |        |      |
|  |  | 10 0.065 0.060 27.366 0.002   |                     |    |     |        |      | 10 0.007 -0.118 376.71 0.000  |                     |    |     |        |      |
|  |  | 11 0.062 0.058 36.921 0.000   |                     |    |     |        |      | 11 0.013 -0.095 376.96 0.000  |                     |    |     |        |      |
|  |  | 12 0.001 0.002 36.925 0.000   |                     |    |     |        |      | 12 0.007 -0.062 377.04 0.000  |                     |    |     |        |      |
|  |  | 13 -0.010 -0.007 37.166 0.000 |                     |    |     |        |      | 13 -0.021 -0.075 377.64 0.000 |                     |    |     |        |      |
|  |  | 14 0.018 0.015 37.959 0.001   |                     |    |     |        |      | 14 -0.000 -0.069 377.66 0.000 |                     |    |     |        |      |
|  |  | 15 0.006 -0.003 38.055 0.001  |                     |    |     |        |      | 15 0.008 -0.054 377.77 0.000  |                     |    |     |        |      |
|  |  | 16 0.014 0.003 38.578 0.001   |                     |    |     |        |      | 16 -0.005 -0.089 377.83 0.000 |                     |    |     |        |      |
|  |  | 17 0.069 0.064 50.464 0.000   |                     |    |     |        |      | 17 0.041 -0.018 380.37 0.000  |                     |    |     |        |      |
|  |  | 18 -0.011 -0.008 50.772 0.000 |                     |    |     |        |      | 18 -0.083 -0.114 390.46 0.000 |                     |    |     |        |      |
|  |  | 19 -0.017 -0.015 51.499 0.000 |                     |    |     |        |      | 19 0.074 -0.056 398.67 0.000  |                     |    |     |        |      |
|  |  | 20 0.051 0.044 58.055 0.000   |                     |    |     |        |      | 20 -0.004 -0.016 398.70 0.000 |                     |    |     |        |      |
|  |  |                               |                     |    |     |        |      | 21 -0.038 -0.037 400.84 0.000 |                     |    |     |        |      |
|  |  |                               |                     |    |     |        |      | 22 0.034 -0.015 402.51 0.000  |                     |    |     |        |      |
|  |  |                               |                     |    |     |        |      | 23 -0.021 -0.025 403.19 0.000 |                     |    |     |        |      |
|  |  |                               |                     |    |     |        |      | 24 -0.015 -0.059 403.57 0.000 |                     |    |     |        |      |
|  |  |                               |                     |    |     |        |      | 25 0.023 -0.052 404.35 0.000  |                     |    |     |        |      |
|  |  |                               |                     |    |     |        |      | 26 0.027 0.012 405.46 0.000   |                     |    |     |        |      |
|  |  |                               |                     |    |     |        |      | 27 -0.039 -0.009 407.72 0.000 |                     |    |     |        |      |
|  |  |                               |                     |    |     |        |      | 28 0.007 -0.015 407.79 0.000  |                     |    |     |        |      |

## 4.3 GARCH-VaR 模型

### 4.3.1 滞后阶数选取

根据比特币和以太币的收益率序列的描述性分析可知，两者的收益率序列具有尖峰肥尾、非正态性、自相关性，而 T 分布相比于正太分布，更能拟合肥尾的收益率分布，故本文假设比特币收益率分布服从 T 分布。

表 4.3 GARCH 模型不同滞后阶数下的 AIC 值

| 赤池信息准则       |            |            |            |            |
|--------------|------------|------------|------------|------------|
| 阶数           | GARCH(1,1) | GARCH(2,1) | GARCH(1,2) | GARCH(2,2) |
| Bitcoin AIC  | -4.109751  | -4.011005  | -4.010850  | -4.018136  |
| Ethereum AIC | -2.969582  | -2.969343  | -2.969362  | -2.968717  |

本文根据 AIC 准则，选取 GARCH 模型的滞后阶数。AIC 准则是给定样本下，给出相对的统计模型质量的统计准则，可以用于确定多个模型中的哪个模型最有可能成为给定数据集的最佳模型。AIC 分数越低意味着模型质量越高。

根据表可知，随着 GARCH 模型的滞后阶数的增加，AIC 值也逐渐增大。当滞后阶数选取 (1,1) 时候，AIC 准则下两者的结果最小，故本文 GARCH 模型滞后阶数都选取(1,1)。

### 4.3.2 模型参数估计

根据选定的 AR(1)-GARCH(1,1) 模型，表达形式为：

$$\begin{aligned} R_t &= \mu_t + \varepsilon_t \\ \varepsilon_t &= \sigma_t e_t \\ \sigma_t^2 &= \alpha_0 + \alpha(L)\varepsilon_t^2 + \beta(L)\sigma_t^2 \end{aligned} \tag{4.1}$$

假定扰动项  $\varepsilon_t$  服从 t 分布，则 t 时刻下，VaR 表达形式为：

$$VaR_t = \mu_t + \sigma_t t^{-1}(\alpha) \tag{4.2}$$

针对本文选取的 AR(1)-GARCH(1,1) 模型进行参数估计，结果如下：

#### 第四章 数字加密货币市场风险度量

表 4.4 比特币收益率 GARCH(1,1)模型参数估计

| 变量         | 系数       | 标准差      | P 值      |
|------------|----------|----------|----------|
| $\mu_t$    | 0.001628 | 0.000667 | 0.014595 |
| $AR$       | 0.15757  | 0.02378  | 0        |
| $\alpha_0$ | 0.000056 | 0.000009 | 0        |
| $\alpha_1$ | 0.159671 | 0.018697 | 0        |
| $\beta_1$  | 0.81453  | 0.018994 | 0        |

表 4.5 以太币收益率 GARCH(1,1)模型参数估计

| 变量         | 系数       | 标准差      | P 值     |
|------------|----------|----------|---------|
| $\mu_t$    | -0.00061 | 0.001325 | 0.00338 |
| $AR$       | 0.007449 | 0.030582 | 0.00756 |
| $\alpha_0$ | 0.000333 | 0.000066 | 0       |
| $\alpha_1$ | 0.182207 | 0.027509 | 0       |
| $\beta_1$  | 0.735847 | 0.035343 | 0       |

根据表 4.5 和表 4.6 的 AR(1)-GARCH(1,1)模型的参数估计结果所示，各个变量的 P 值均小于 0.05，则认为该系数在 5% 的置信水平下是显著的。

进一步，为检验 AR(1)-GARCH(1,1)模型的拟合效果，对残差项做 ARCH 效应检验，如表 4.7 所示，两者残差 p 值均大于 5% 的置信水平，故拒绝原假设。两者的残差平方序列纯随机，表明模型拟合良好，较好的捕捉了收益率序列的异方差特性。

表 4.7 残差异方差性检验

|          | 模型     | Q-statistic | p 值      |
|----------|--------|-------------|----------|
| Bitcoin  | Lag[1] | 2.632       | 0.10473  |
|          | Lag[5] | 2.719       | 0.06058  |
|          | Lag[9] | 5.713       | 0.05938  |
| Ethereum | Lag[1] | 3.452       | 0.063186 |
|          | Lag[5] | 5.495       | 0.000135 |
|          | Lag[9] | 11.455      | 0.000251 |

进而根据估计出来的 AR(1)-GARCH(1,1)模型，计算出条件方差  $\sigma_t^2$ ，得出比特币收益率在不同置信水平下的分位数  $t^{-1}(\alpha)$ ，进而利用公式 4.2 计算两个加密货币的 VaR 值，结果如表 4.8。

表 4.8 VaR 在不同置信水平下的值

| VaR 值    | 99%       | 95%       |
|----------|-----------|-----------|
| Bitcoin  | 0.0473936 | 0.0304931 |
| Ethereum | 0.173244  | 0.099967  |

## 4.4 GARCH-EVT-VaR 模型

### 4.4.1 模型构建方法

GARCH 方法在估计 VaR 值时候，需要假设扰动项  $\varepsilon_t$  服从于特定分布，本文上述方法假设其服从于 T 分布，然而往往金融时间序列的扰动项  $\varepsilon_t$  具有比 t 分布更肥的尾部（McNeil，1998），此外本文所讨论的数字货币价格波动剧烈，日收益率往往出现大量极端值，难以被 GARCH 模型捕捉<sup>[50]</sup>。因而仅凭 GARCH 模型估计的 VaR 值往往会低估真实风险。

而极值理论 EVT 与随机变量极限观察的渐近行为有关。它为极端事件的统计建模提供了基础，并用于计算与尾巴相关的风险度量。本文将采用 POT 模型来识别超出高阈值  $u$  的极端观测值。本文为解决后尾现状和极端值，采用极值理论 EVT，拟合扰动项的尾部分布，以此整合 GARCH 和 EVT 模型估计 VaR 值。具体步骤如下：

首先，放弃之前 GARCH 模型中对于扰动项 T 分布的假设，利用极大释然估计出模型参数，进而求出条件均值  $\mu_t$  和条件方差  $\sigma_t$ ，再将残差项正太标准化，即  $Z_t = (\varepsilon_t - \mu_t)/\sigma_t$ 。

其次，利用广义帕累托分布拟合  $Z_t$  的尾部，进而根据公式 4.4 得到极值分位数  $\hat{\chi}_q$  的分布。

$$G_{\xi,\beta}(y) = \begin{cases} 1 - \left(1 + \frac{\xi y}{\beta}\right)^{-\frac{1}{\xi}}, & (\xi \neq 0) \\ 1 - e^{-\frac{y}{\beta}}, & (\xi = 0) \end{cases} \quad (4.3)$$

$$\hat{\chi}_q = u + \frac{\xi}{\beta} \left\{ \left[ \frac{n}{N_u} (1 - c) \right]^{-\frac{1}{\xi}} - 1 \right\} \quad (4.4)$$

最后，根据极值条件分位数计算 GARCH – EVT – VAR 的估计值，公式如下：

$$VaR_q = \mu_{t+1} + \sigma_{t+1} \left\{ u + \frac{\beta}{\xi} \left[ \left( \frac{n}{N_u} (1 - q) \right)^{-\frac{1}{\xi}} - 1 \right] \right\} \quad (4.5)$$

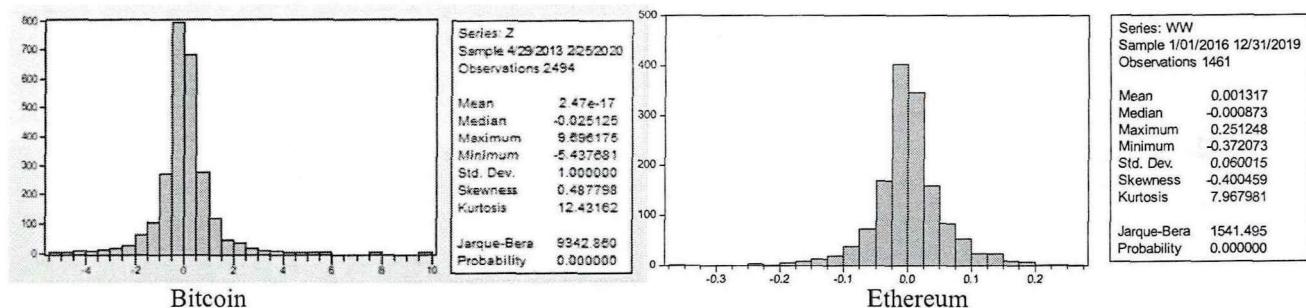
#### 4.4.2 模型应用

首先将两个加密货币的收益率 GARCH 模型的标准化残差  $Z_t$  进行描述分析，结果如下：

表 4.9 标准化残差描述性分析

|          | 均值       | 标准差      | 偏度        | 峰度       | JB 统计量   | P-value |
|----------|----------|----------|-----------|----------|----------|---------|
| Bitcoin  | 2.47E-17 | 1.01     | 0.48779   | 12.43162 | 9342.86  | 0.00    |
| Ethereum | 0.001317 | 0.060015 | -0.400459 | 7.967981 | 1541.496 | 0.00    |

图 4.4 标准化残差描述性分析



根据描述性分析结果，两者的标准化残差偏度均大于零，说明其分布为右拖尾，峰度均大于 3，说明其分布为尖峰分布。同时，JB 统计量的 P 值为 0，故在 99% 的置信水平下，两者的标准化残差  $Z_t$  不服从正态分布。

进而再对标准化残差  $Z_t$  进行 ADF 平稳性检验，结果如下表 4.10。

表 4.10 标准化残差 ADF 检验结果

|                       | Bitcoin     |        | Ethereum    |        |
|-----------------------|-------------|--------|-------------|--------|
|                       | t-Statistic | Prob.* | t-Statistic | Prob.* |
| ADF test statistic    | -51.04720   | 0.0001 | -37.1816    | 0.0001 |
| Test critical values: |             |        |             |        |
| 1% level              | -3.432779   |        | -3.432779   |        |
| 5% level              | -2.862499   |        | -2.862499   |        |
| 10% level             | -2.567326   |        | -2.567326   |        |

根据上表 4.10 的 ADF 平稳性检验结果可以看出，比特币 ADF 值为 -51.04720，以太币的 ADF 值为 -37.1816 均小于 1%、5%、10% 三种不同的显著性水平下的临界值，同时  $P\text{-value} = 0.0001$ ，拒绝存在单位根的原假设，这表明标准化残差序

列是显著平稳的。

紧接着对标准化残差的自相关性进行检验，结果如下：

根据下表 4.11 结果显示，ARCH-LM 统计量值，在 5% 的显著性水平未通过检验，接受原假设，发现其不具有 ARCH 效应，因而可以利用极值理论对其尾部分布进行帕累托分布建模拟合。

表4.11 ARCH-LM检验结果

Breusch-Godfrey Serial Correlation LM Test:

|          |               |          |                     |        |
|----------|---------------|----------|---------------------|--------|
| Bitcoin  | F-statistic   | 0.923879 | Prob. F(2,2491)     | 0.3971 |
|          | Obs*R-squared | 1.848613 | Prob. Chi-Square(2) | 0.3968 |
| Ethereum | F-statistic   | 1.41E-07 | Prob. F(2,1462)     | 0.9997 |
|          | Obs*R-squared | 1.41E-07 | Prob. Chi-Square(2) | 0.9997 |

极值理论依据选取样本方法分类成两种，一种是 BMM 方法，也就是人为将时间范围划分为块或周期，并选取变量在连续周期中所占用的最大值，进而利用广义极值分布拟合极端数据。另一类是阈值 POT 方法，将超过给定阈值的观测值作为极端数据拟合。鉴于，后者方法充分利用了样本数据，与真实数据情况更为拟合，本文选取 POT 方法。

接下来，为正确估计形态参数  $\xi$ 、尺度参数  $\beta$ ，必须先确定阈值  $u$ 。Hill(1975) 和 Pickands(1975) 提出以下估计量 ( $Q$  为正整数)：

$$\xi_h(Q) = \frac{1}{Q} \sum_{i=1}^Q [\ln x_{(T-i+1)} - \ln x_{(T-Q)}]$$

$$\xi_p(Q) = \frac{1}{\ln(2)} \ln \left( \frac{x_{(T-Q+1)} - x_{(T-2Q+1)}}{x_{(T-2Q+1)} - x_{(T-4Q+1)}} \right), Q \leq T/4$$

Hill 估计仅对 Frechet 族适用，但当它适用时，比 Pickands 估计更有效。根据 hill 方法求得比特币的阈值  $u=0.4356887$ ，以太币阈值为  $u=0.3761193$ 。

进而利用似然函数： $l(\xi, \beta, \gamma) = -N_u \ln \beta - \left(1 + \frac{1}{\xi}\right) \sum_{i=1}^N \ln \left(1 + \frac{\xi}{\beta} y_i\right)$ ，计算得到形态参数  $\xi$ 、尺度参数  $\beta$  的估计值，结果如下表 4.12。

表 4.12 广义帕累托分布计算极值参数估计

| GEV      | 形态参数 $\xi$  | 位置参数 $\beta$ | 尺度参数       |
|----------|-------------|--------------|------------|
| Bitcoin  | 0.1604574   | 0.4356887    | 0.6305954  |
| Ethereum | -0.01001534 | 0.3761193    | 0.04449277 |

最后，根据阈值和相关参数分别计算出置信水平在 99% 和 95% 的分位数  $\hat{x}_q$ ，进而利用公式 4.5，分别计算得出 VaR 值。结果如下表 4.13 所示。

#### 第四章 数字加密货币市场风险度量

表 4.13 VaR 在不同置信水平下的值

|          | 99%      | 95%       |
|----------|----------|-----------|
| Bitcoin  | 0.067291 | 0.067229  |
| Ethereum | 0.078235 | 0.0419947 |

## 4.5 Kupiec 回测检验

为了评估 VaR 值估计的质量，应该使用恰当的方法对模型进行回测。而回测是一种统计程序，可以将实际的损益与相应的 VaR 估计值进行系统比较。例如，如果用于计算每日 VaR 的置信度为 99%，预计平均每 100 天就会发生一次异常。在回测过程中，通过统计地检查在指定的时间间隔内异常发生的频率是否与选定的置信度一致，来判断模型估计得质量。

在众多回测方法中，最为常用的是 Kupiec 于 1995 年提出的基于失败率的检验方法。Kupiec 的测试也称为 POF 测试（portion of failure），用于衡量异常损失数量是否与置信度一致。在模型为“正确”的零假设下，超过 VaR 的数量遵循一个二项式分布，且可以被视作一个独立事件。当失败事件出现，则被界定为 1；而当损失值在 VaR 值之内，事件看做成功，被界定为 0。因此，执行 POF 检验所需的唯一信息是观察次数  $T$ ，例外次数  $x$  和置信度  $c$  (Dowd, 2006)。进而 POF 测试的原假设为：

$$H_0: p = p^* = \frac{x}{T}$$

其中， $p^*$  为失败概率的期望值，且  $p^* = 1 - c$ 。此时，对于 Var 值准确性的测试也就转换成对于该假设是否显著的测试。Kupiec (1995) 进而提出了似然比率检验量 LR(likelihood-ratio)：

$$LR_{POF} = -2 \ln \left( \frac{(1-p)^{T-x} p^x}{\left[1 - \left(\frac{x}{T}\right)\right]^{T-x} \left(\frac{x}{T}\right)^x} \right)$$

在模型正确的零假设下，LR 统计量服从 1 自由度的卡方分布。如果实际的 LR 统计量超过了相应置信水平下的临界值，则可以拒绝原假设，认为该 VaR 值度量模型不准确。

### 4.5.1 比特币回测结果

根据以上模型，针对 AR-GARCH 模型和 GARCH-EVT 模型，分别进行样本量为 2493 和 1900 的 POF 回测，结果如下表 4.14 及 4.15。

表 4.14 样本值为 2493 的回测结果

|        | 模型     | t-GARCH(1,1)        | Garch-EVT            |
|--------|--------|---------------------|----------------------|
| 95%置信度 | 预期失败天数 | 124                 | 124                  |
|        | 实际失败天数 | 217                 | 94                   |
|        | 失败率    | 5%                  | 4.94%                |
| LR 统计量 |        | inf(3.841)          | 0.00329(3.841)       |
|        | 模型     | t-GARCH(1,1)        | Garch-EVT            |
| 99%置信度 | 预期失败天数 | 24                  | 24                   |
|        | 实际失败天数 | 42                  | 6                    |
|        | 失败率    | 2%                  | 2%                   |
| LR 统计量 |        | 3.038403e-05 (6.35) | 4.806033e-06 (6.636) |

表 4.15 样本值为 1900 的回测结果

|        | 模型     | t-GARCH(1,1)        | Garch-EVT           |
|--------|--------|---------------------|---------------------|
| 95%置信度 | 预期失败天数 | 95                  | 95                  |
|        | 实际失败天数 | 157                 | 79                  |
|        | 失败率    | 8%                  | 4.2%                |
| LR 统计量 |        | 4.597996e-11(3.841) | 4.262736e-25(3.842) |
|        | 模型     | t-GARCH(1,1)        | Garch-EVT           |
| 99%置信度 | 预期失败天数 | 19                  | 19                  |
|        | 实际失败天数 | 32                  | 7                   |
|        | 失败率    | 2%                  | 0.3%                |
| LR 统计量 |        | 0.00029(6.635)      | 0.0014(6.635)       |

根据 LR 统计量显示当回测样本数为 2493 时，t-GARCH 模型在 95%置信度下出现了低估风险，而 GARCH-EVT 模型均在统计量临界值之内。当回测样本数为 1900 时，t-GARCH 模型与 GARCH-EVT 模型得 LR 统计均落在临界值之内，故 GARCH-EVT 模型预测效果良好。

### 4.5.2 以太币回测结果

同样根据 Kuipiec 方法，针对 AR-GARCH 模型和 GARCH-EVT 模型，分别进行样本量为 1463 和 1900 的 POF 回测，结果如下表 4.16 及 4.17。

表 4.16 样本值为 1465 的回测结果

|        | 模型     | t-GARCH(1, 1)    | Garch-EVT         |
|--------|--------|------------------|-------------------|
| 95%置信度 | 预期失败天数 | 124              | 124               |
|        | 实际失败天数 | 203              | 87                |
|        | 失败率    | 8%               | 3. 48%            |
|        | LR 统计量 | 0. 0147 (3. 841) | 0. 00784 (3. 841) |

|        | 模型     | t-GARCH(1, 1)         | Garch-EVT              |
|--------|--------|-----------------------|------------------------|
| 99%置信度 | 预期失败天数 | 24                    | 24                     |
|        | 实际失败天数 | 39                    | 7                      |
|        | 失败率    | 1. 56%                | 2. 8%                  |
|        | LR 统计量 | 3. 020129e-05 (6. 35) | 4. 956742e-06 (6. 636) |

表 4.17 样本值为 1200 的回测结果

|        | 模型     | t-GARCH(1, 1)          | Garch-EVT              |
|--------|--------|------------------------|------------------------|
| 95%置信度 | 预期失败天数 | 95                     | 95                     |
|        | 实际失败天数 | 143                    | 69                     |
|        | 失败率    | 7. 5%                  | 3. 6%                  |
|        | LR 统计量 | 3. 794352e-10 (3. 841) | 3. 256776e-24 (3. 842) |

|        | 模型     | t-GARCH(1, 1)     | Garch-EVT        |
|--------|--------|-------------------|------------------|
| 99%置信度 | 预期失败天数 | 19                | 19               |
|        | 实际失败天数 | 28                | 5                |
|        | 失败率    | 1. 47%            | 0. 26%           |
|        | LR 统计量 | 0. 00028 (6. 635) | 0. 0013 (6. 635) |

根据 LR 统计量显示当回测样本数为 1465 和 1200 时，t-GARCH 模型在 95% 置信度下出现了低估风险，其失败率均高于 GARCH-EVT 模型，因而 GARCH-EVT 模型的预测效果比前者较好。

## 4.6 实证结论

### (一) 比特币和以太币的市场风险较高

根据 GARCH-EVT 模型计算得到的 VaR 值结果, 如表 4.13 显示, 依托比特币和以太币的日间收益率计算得到的 VaR 值均呈现出较大的水平值, 表明两者的市场风险都较高。此外, 在 99% 的置信水平下, 以太币的 VaR 值高于比特币, 表明虽然以太币启发自比特币, 但是其市场风险程度却不下于比特币。

表 4.13 VaR 在不同置信水平下的值

|          | 99%      | 95%       |
|----------|----------|-----------|
| Bitcoin  | 0.067291 | 0.067229  |
| Ethereum | 0.078235 | 0.0419947 |

### (二) GARCH-GEV 模型更加适用于加密货币的风险度量

根据 Kuipiec 方法回测对比特币和以太币风险测量模型, 均发现 GARCH-EVT 模型在 99% 和 95% 的置信水平下以及不同样本水平下, 失败率更低, LR 统计落在临界值之内, 表明 GARCH-EVT 模型在计算加密货币的 VaR 值上能够获得更好的精度, 更够较好的估计风险。

## 第五章 风险成因和风险应对建议

### 5.1 数字货币市场风险成因分析

#### 5.1.1 发行机制缺乏灵活性

任何资产价格变动都离不开该资产供需关系的改变，而同样加密货币市场的供需两侧变动是影响加密货币的价格变化的重要原因之一。从供给侧来看，数字加密货币与正常法定货币最大的区别在于发行机制的差别。法定货币的发行由该国家权威中心控制，而大多数的加密货币的发行由于去中心化的设计由一套固定的发行程序控制，无法灵活调整。

首先，为了控制货币的通胀问题，众多加密货币的最大发行总量往往被限定在某一数量水平。并且为了达到这一效果，众多加密货币也设计了产能缩减的机制。

例如，中本聪对于比特币的设定是 2100 万枚比特币，以太币的发行上限是每年 1800 万枚新以太币，瑞波币最大发行量是 1000 亿枚，莱特币的总量也别设定在 8400 万枚。数字加密货币的这一总供应量限制，决定了加密货币将会缓慢地减少新产能。

以比特币为例，其发行总量被限制在 2100 万个，而出块速度在 10 分钟左右，每个区块的奖励最开始被设定在 50 个，随后每发行 21 万个区块，每个区块的奖励都将减半，以延缓比特币的发行速度。也就是说，每隔四年，比特币的产量都将减半。比特币不断下降的发行量，不仅意味着减少供应增长，而且意味着更高的采矿成本。对矿工而言，花费更高代价的算力成本，得到的比特币奖励却在每隔四年降低一半。逐步升高的挖矿成本，和不断减少的供应增长，也就很大程度上推动者比特币价格的上涨。

而从比特币的价格走势上来看，比特币的两次上涨行情也确实跟比特币的减产不谋而合。2012 年比特币第一次减产，每个区块奖励降低至 25 个比特币。而在 2013 年初比特币迎来了一次牛市行情。2016 年比特币第二次减产，出块奖励降低至 12.5 个比特币，而在 2017 年出 ICO 融资兴起带动了需求增长，这一轮

牛市也迅速开启。从经验分析的角度而言，产能有预见性的减产与比特币的价格上升或多或少存在一定的正相关关系。

其次，加密货币的生产者，即矿工们，他们的进入和退出行为独立于加密货币的供应，使得加密货币供给价格弹性几乎为零。

正常情况下，一个正常行业的供应和需求行为受到价格调节，当价格下降，部分供应者的生产成本高于收益，则会退出市场，减少行业内供给水平，推动价格回到均衡水平。然而以比特币为例，无论此时的比特币矿工数量大幅上升或者减少，出块奖励都维持在一定数量（当前出块奖励是 12.5 个比特币），并且出块时间都维持在十分钟左右，几乎不受行业内矿工数量影响。

2013 年比特币的价格暴涨，使得比特币的挖矿业务变得有利可图，进而许多企业纷纷进入比特币采矿竞赛。为了在这个采矿竞赛中获胜，众多采矿企业也纷纷装备指定 IC 芯片的强大计算机，以提高算力，在矿池中获得出块奖励。大型计算机设备和电力设施系统的投入使用，使得采矿行业类似于重型设备行业，容易进入，但由于沉没成本高昂而难以退出<sup>[58]</sup>。

当比特币价格下降一定幅度，但不是致命的幅度时候，矿工们仍将继续坚持，不会退出采矿业。更确切地说，倘若它的价格低于单位平均成本，但高于平均可变成本，矿工仍将将继续开采。因为只要收益超过可变成本，保持开采是合理的，其最终的运营损失将小于立即停止所造成的损失。根据有关比特币采矿的一些报道，许多大型采矿者在 2013 年底比特币繁荣之后进入，即使回报为负，他们仍继续运营。

倘若比特币的价格急剧下降到平均可变成本以下，所有矿工将退出采矿<sup>[58]</sup>。在 2013 年之后加入比特币采矿行业中的企业，基本拥有不相上下的算力。因而倘若比特币的价格暴跌至平均成本以下，矿工的退出将不是一个循序渐进的过程，而是突然的甚至断崖式的退出。如果比特币价格跌至阈值以下，则整个比特币系统可能会崩溃，或者比特币用户将被限制在非常少量的内部成员之间，以很小的规模交换比特币。一旦所有矿工离开比特币采矿，就没有人会从事工作证明。区块的验证将被延迟或停止。因而比特币几乎无弹性的供给曲线，使得矿工们不得不吸收比特币的任何价格变化。

总而言之，加密货币发行机制的不灵活，导致了加密货币系统的不稳定性。这来源于三个层面，第一个是加密货币为控制最大总数设计的产能定期缩减机制；第二个是加密货币供应曲线的不灵活，矿工们的收入报酬不得不吸收任何价

格变化，缺少价格稳定机制，这加剧了加密货币的价格波动；第三个来自于采矿也可持续发展的风险，在比特币价格上涨期间，矿工从事采矿活动，从而保证了比特币的供应，但是在比特币价格下跌期间，不存在诱导采矿退出的平滑方法。

### 5.1.2 市场集中度过高

从供给侧来看，不仅加密货币系统自身的不稳定性导致价格的不稳定，而且加密货币的真实市场流通量也是影响加密货币价格的重要因素。

目前，主流加密货币较高的市场集中度，成为了影响加密货币价格的重要因素之一。以比特币为例，如下表 5.1 所示，截止 2020 年 3 月 10 日，95% 的地址数量仅仅拥有 5% 的比特币数量，而大约 3% 的地址拥有接近 95% 的比特币数量。虽然比特币的交易地址可以更改，但是从其中的交易地址集中度也可以窥见比特币市场是高度集中度的。而比特币市场的少部分人持有大部分的比特币，一方面说明比特币的实际流通情况并不如预期，大部分的比特币都被少部分的人持有在手中，等待比特币的进一步升值，并不参与到真实交易当中<sup>[59]</sup>。另一方面，比特币的高度集中，使得其价格非常容易受到这些持有大量比特币的地址影响，给比特币市场造成了剧烈的价格波动。

表 5.1 比特币地址以及余额集中度

| 层级           | 地址数（个）  | 占比（%）    | 比特币数量      | 占比（%）    |
|--------------|---------|----------|------------|----------|
| 0-0.0001     | 2453419 | 8.20     | 11.97      | 0.000065 |
| 0.0001-0.001 | 5383590 | 18.00    | 277        | 0.0015   |
| 0.001-0.01   | 6940304 | 23.20    | 2996.61    | 0.0164   |
| 0.01-0.1     | 7278869 | 24.34    | 172103.39  | 0.94     |
| 0.1-1        | 2120782 | 7.09     | 748649.34  | 4.09     |
| 1-10         | 564695  | 1.89     | 1699299.92 | 9.29     |
| 10-100       | 129539  | 0.43     | 4527417.14 | 24.77    |
| 100-1000     | 12510   | 0.042    | 3533367.63 | 19.33    |
| 1000-10000   | 1895    | 0.0063   | 4766348.18 | 26.08    |
| 10000-100000 | 102     | 0.000341 | 2272582.83 | 12.43    |
| > 100000     | 3       | 0.00     | 523860.39  | 2.9      |

数据来源：BTC.com、Bitinfocharts

而其他的加密货币市场也是如此，受到加密货币稀缺性和价格上升预期影响，根据 IntoTheBlock 研究报告显示，截至 2019 年 10 月，154 个地址拥有近

40%的以太币，128个地址占有近47%的莱特币。

一方面，对于加密货币的投资者而言，保持所持货币的稀缺性是实现该加密货币升值的重要方法之一。对这些投资者而言，拥有更多的加密货币，意味着能在流动性缺乏的交易市场，更大程度上影响加密货币价格的变化。另一方面，加密货币的基尼系数越高，对中小投资者而言，市场风险也就越大。

### 5.1.3 投机需求旺盛

加密货币的价格变化深层次原因仍然归结于加密货币供需两侧的变化，而大多数加密货币的供给是可预见的和相对稳定的，因而加密货币的价格很大程度上取决于需求侧因素。加密货币的需求是指投资者基于某种需要，对加密货币的需要量。当下加密货币的需求主要来自两个方面：应用需求和投机需求。这两个需求对于加密货币价格的影响程度和影响方式都各有不同。

应用需求是加密货币最基本的需求，也是加密货币中最为稳定的需求因素之一，它取决于加密货币的技术落地情况，也取决于整个加密货币市场环境。加密货币最基础的应用是作为支付工具，通过点对点方式，绕开权威中心，利用区块链给双方信用背书，降低交易的信息成本和交易的手续费。例如，美国在线零售商 Overstock 于 2014 年开始接受比特币付款，同时接入 coinbase 的比特币支付服务。Overstock 只需要每笔支付给 coinbase 平台 1% 的手续费，却不仅降低了传统银行支付的支付成本，而且获得了增长的平均订单量和扩大的客户群体<sup>[51]</sup>。随后，其他美国企业也增加了对比特币的支持，包括 Expedia（旅行），Newegg（电子），Foodler（餐馆交货和外卖），Gyft（数十个商人的礼品卡）和 TigerDirect（电子）。

此外，以太币的智能合约，也是加密货币另外一个应用需求方向。当前的加密货币大多数都是基于区块链技术，所有交易信息会被记录在区块内，公开透明且难以篡改。而以太币将记录至区块的信息拓展到提前设定的合约信息。智能合约一旦被记录至区块内，则合约内的所有用户会被区块链平等对待，自动运行相应程序而不受人为干扰，保证了合约履行的自动化和不被篡改。例如，苏格兰皇家银行用以太坊的分布式记账和智能合约平台创建了一个结算交割机制。

尽管应用需求是加密货币最为基础性的需求，然而技术的尚不成熟却限制着加密货币的实际落地应用。比特币的支付应用，当前正因为接纳用户少，确认

时间过长以及安全性不足等缺陷，难以被大范围落地使用。而以太币的智能合约应用也存在着技术门槛和缺陷，例如以太币的智能合约仍然对于编写者的技术要求交稿，倘若智能合约的编写一开始出现错误，则后续执行也会存在漏洞。因而，目前针对加密货币的应用需求仍然只是加密货币需求的冰山一角。

不可否认，投机需求是目前加密货币最为旺盛的需求。

在凯恩斯的货币需求理论中，货币的需求被分为了交易需求，谨慎需求和投机需求。而法定货币具备以上交易需求是因为国家的信用背书使得法定货币具备一定的交易价值，能够被兑换成一个等值的产品或者服务，并且这个价值还随着国家信用的变化而变化。这也是加密货币的货币属性被广泛质疑的原因，其去中心化的特点使得其不具备任何国家或者权威机构的信用背书，其价值也就无法跟任何信用机构相挂钩，只能依赖于其未来的应用落地愿景。然而，加密货币的去中心化设计目前由于技术原因难以实际落地，同时也抵触了权威中心的核心利益，并且其价格不断剧烈波动，都影响其能够作为一个货币的真实性。然而加密货币市场仍然有众多投资者趋之若鹜，这大部分都是由于投资者的投机需求引发导致。

现阶段，以比特币为例，市场上的投机行为主要有三种类型，一是利用比特币短期的价格波动在交易平台上的不断的低买高卖，以获取短期的价差收益。例如在 2010 年底至 2013 年底这个时间段，比特币市场的日均换手率高达 41%，意味着这个时间段近一半的比特币都在交易平台被交易还手，反映了投资者较强的短期投机心理<sup>[60]</sup>。二是，投资者在不同交易平台利用比特币不同的价格差别套利。三是，囤积大量比特币，博取未来某一时间比特币的高额回报率。此外，根据《全球比特币发展研究报告》（2017）数据显示，80.77% 的比特币投资者以短期盈利为目的，仅 13.81% 的用户选择长期持有。狂热的投机，让比特币甚至被认为是一个旁氏骗局，是一次投资者的集体妄想<sup>[61]</sup>。

然而，比特币的投机需求旺盛却对整个比特币市场产生了众多负面影响。首先，比特币的投机活动极大的放大了市场波动，降低了比特币的市场信任。比特币市场发展初期，整个市场的流动性不足，而比特币市场的集中度高，容易受到比特币大额持有者们的操控。其次，投机活动使得资本过于狂热，损害了比特币经济的健康发展。投资者对比特币的投机脱离了对加密货币技术应用的思考和投资，占用了本应该用来投资于正常比特币应用的资源，从而破坏了市场环境和经营环境，阻碍了比特币技术的正常发展。

目前，加密货币的技术应用缺陷限制了加密货币的应用需求的满足，而加密货币的市场价格却进一步助长着投机需求的旺盛。

#### 5.1.4 政策环境的变化

政策环境的变化是影响比特币市场风险的重要外部因素。

当前数字货币的交易节点主要分布在美国、中国、欧盟以及日本等国家，这些国家对于数字货币的态度以及出台的相关政策对于数字货币的价格有着更为直接的影响。在数字加密产生初期，监管的宽松为加密货币价格打开了上升空间。以比特币为例，在2010年至2013年比特币第一次价格牛市阶段，各国对于新生的比特币了解尚浅，没有表明对于比特币的监管态度，因而这一阶段监管的确实助长了比特币价格的飞速上涨。而后由于各国监管开始加强，需求被政策压制，价格一段时间内都被腰斩。

数字货币的价格对于诸如中国、美国、欧盟等主要国家的监管政策反应敏感，当政策趋向于加强监管或者否定加密货币，加密货币的价格在短期内会立即下跌。当政策释放出利好消息，加密货币价格会在短期内上升。以比特币为例，从表中可以看出，当政策当局承认比特币地位，或者释放出善意时候，比特币当日的上涨幅度一般会超过5%；当负面消息被释放，比特币当日下跌幅度也较为剧烈。

表 5.1 政策变动影响比特币价格

| 时间          | 事件                        | 价格变化    |
|-------------|---------------------------|---------|
| 2013年5月15日  | Mt.gox 交易平台银行账户遭美国国土安全局冻结 | -4.21%  |
| 2013年8月14日  | 印度央行宣称，暂不管制比特币            | 6.68%   |
| 2013年8月19日  | 德国承认比特币作为金融资产的合法地位        | 4.5%    |
| 2013年12月5日  | 中国发布《关于防范比特币风险的通知》        | -6.74%  |
| 2013年12月17日 | 支付宝关闭比特币交易通道              | -14.42% |
| 2014年1月10日  | 新加坡承认比特币的合法地位             | 7.78%   |
| 2014年2月10日  | 俄罗斯全面禁止比特币流通              | -6.64%  |

数据来源：blockchain 网站

## 5.2 风险应对建议

### 5.2.1 宏观监管层面

#### 5.2.1.1 建立风险预警机制

针对加密货币价格波动大，市场风险较高的特点，相关部门应当根据比特币、以太币等主要加密货币的特点，展开相对应的技术研究和监管办法研究，完善对于加密货币交易的跟踪系。同时，建立风险跟踪机制，根据加密货币的相关特征，打造动态的跟踪体系，并且根据监测结果对各类风险进行预判。例如，可以从比特币价格变动、以及价格影响因素变动建立完整的监测系统<sup>[60]</sup>。进而，通过规范信息披露制度，及时的向公众预警加密货币的相关风险，做到防范于未然。

#### 5.2.1.2 差异化原则监管

加密货币的发展并不是一无是处，比特币的点对点支付对于降低支付成本具有启发意义，而以太币的智能账本技术也对于新型信用体系的架构有较大的技术意义。而国家监管层面也同样要根据加密货币的优势和劣势，实行差异化监管，既要严格防范加密货币引发的市场风险，也要给予加密货币创新技术发展的空间；既在大环境下保证金融环境的稳定有序，又不以高标准严监管扼杀技术创新。差异化对待加密货币市场，兼顾金融安全与创新。

就加密货币的市场风险管理而言，可以就中心化和非中心化货币差异化监管，将数字货币与区块链技术差异化监管<sup>[62]</sup>。首先，数字货币目前可以根据其中心化特质分为中心化货币和非中心化加密货币。例如，央行发行的数字货币DEPC可以直接纳入已有的金融监管体系；比特币等去中心化货币则作为私有金融资产，纳入金融资产的监管范围，对于该资产的生产平台、交易平台、资金流向采取更加严格的监管政策，保护投资者权益。其次，比特币虽然作为加密货币被投资者所青睐，但是不能忽视其底层技术即区块链技术的价值和技术意义，区块链对于重塑信用体系，降低信用成本具有重要意义。因而，在针对加密货币的监管当中，不能简单粗暴的全面否定，应该对其有价值的底层支持技术从监管中剥离出来，鼓励技术创新，才能在未来的技术发展中不落下风。

#### 5.2.1.3 建立国际合作机制

加密货币作为一个去中心化货币，一个很重要的特质是可以在全球网络流通。加密货币的国际化流通，也就意味着加密货币风险也是全球蔓延性质的。并

且加密货币的技术更迭迅速，仅仅依靠少数监管部门很难做到动态监管。因而，应该建立国际合作机制，与世界各国合作，共同防范加密货币风险。

#### 5.2.1.4 严防加密货币犯罪行为

在比特币价格飞涨的同时，越来越多的加密货币从市场中涌现。诸如狗狗币、悬赏币等加密货币仅仅是对比特币的模仿，甚至仅仅是利用加密货币概念非法融资。而另一类加密货币，例如以太币，是对比特币的改进，在技术应用上更加复杂。而复杂的加密货币技术对于我国监管机构打击加密货币犯罪提出了更高的技术挑战。

当前，打击加密货币犯罪主要应该集中在三类事件。

一是针对加密货币产业链的攻击行为。例如针对加密货币的盗窃行为，对矿池的攻击以及针对交易平台对于加密货币价格操纵行为。由于加密货币的新颖性，以及相关负责机构和管辖权的责任划分不明确，加密货币技术又相对复杂，程序不确定性以及资源有限，执法部门通常难以预防或解决这些犯罪。

第二，利用加密货币的洗钱行为。以比特币为例，比特币洗钱可能会变得越来越难追踪，尤其是当资金通过混合器进行流动时，混合记录对公众是隐藏的，可能无法提供给执法人员。这些新的特征可能会帮助肇事者掩盖犯罪行为。而新的加密货币设计未来可能会针对洗钱这一目的，设计匿名性和不可追踪性更强的加密货币。

最后，利用加密货币概念非法集资行为。比特币的价格飞涨过程中，越来越多新生加密货币涌现在市场当中。其中不乏通过加密货币概念非法集资的行为。例如，2018年初一家迪拜公司发行阿里巴巴币，众筹近350万美元。虽然我国已明确禁止代币融资的行为，但是仍然要警惕利用加密货币或者是区块链概念非法集资的犯罪行为。

目前，加密货币市场规模越来越庞大，加密货币技术愈加复杂，我国明确相关机构和部门的监管职责，必要时成立专门监管部门，加强技术培训，严防加密货币的犯罪行为。

## 5.2.2 微观参与者层面

### 5.2.2.1 投资者层面

个人投资者，尤其中国投资者，是目前加密货币市场的参与主体，也是当前加密货币市场主要的需求方，因而个人投资者对于加密货币的供需也将影响加密货币的价格波动。对于加密货币的个人投资者而言，提升个人投资者的参与素质，正确认识加密货币市场变得尤为重要和关键。

首先，个人投资者在进入加密货币市场前，应当对加密货币本质和市场环境进行深入了解。工欲善其事必先利其器，投资者在选择投资标的的时候，应该回归理性，先了解加密货币的相关理论，辩证的看待加密货币。不仅应该认识到加密货币作为数字货币难以应用落地、投机性强、价格波动剧烈等不利因素，也应该认识到其底层区块链技术却具有很强的应用前景。投资者只有更加客观辩证的看待加密货币，才能在系统性认识下，做出理性的投资决策。

其次，投资者应当提高风险防范意识，做好相关的风险管理措施。加密货币市场一个显著特征就是价格波动剧烈，市场风险大，市场投机性严重。伴随着数字货币的价格风险，还有加密货币的技术风险、监管风险等等。面对这些风险，投资者更应该在进入市场前，做好相应的风险准备，提高风险抵御能力。当投资者进入加密货币市场，不仅应该选择资质良好的加密货币平台以提高抵御技术风险能力，同时应该做好风险管理，避免投入过多资金在加密货币市场。

### 5.2.2.1 加密货币企业层面

自 2013 年比特币热以来，越来越多的企业就加入到加密货币的产业链当中。无论是各大挖矿企业，还是各种线上交易平台，亦或者是各种区块链科技公司，都如同雨后春笋般迅速出现在加密货币行业中。而这一大批加密货币企业不仅仅是推动加密货币价格飞涨的背后因素，也是加密货币市场不稳定因素的来源。无论是交易平台遭受黑客攻击倒闭，还是区块链公司非法集资暴雷，都会对当前的加密货币市场造成负面影响。因而，对加密货币企业而言，更应当汲取历史教训，规范自身发展，提升自己的科技创新能力，方能更好应对加密货币的市场风险，才能获得更加长远的发展。

对加密货币的采矿企业而言，应当积极顺应监管要求，积极加强技术转型和升级，同时应当积极承担企业的社会责任，平稳加密货币的价格，减少因价格波动带来的不必要损失。当前各国都在积极加强加密货币的监管措施，2018 年我

国就要求国内各加密货币挖矿企业有序退出挖矿业务，美国也将除了比特币和以太币以外的代币约束为有价证券，将其整个产业链都纳入现行金融条例约束。此外，随着加密货币的稀缺性受到国家主权性数字货币的挑战，加密货币的产能下降也进一步推升挖矿成本，挖矿企业的利润率在不断下降。对挖矿企业而言，一方面只有顺应监管趋势，主动增强企业营运透明度，有序淘汰落后产能企业，才能进一步生存于市场当中；另一方面，加强技术创新和方向转型，做好技术保护以避免黑客攻击，同时利用技术创新为企业发展赋能，积极寻求新的发展方向。

对加密货币交易平台而言，汲取历史教训，提升交易平台进入门槛，完善平台交易的安全性和透明度，并且积极纳入监管框架，才能更好地防范加密货币市场风险。目前，大部分的加密货币交易都是通过各种交易平台完成交易和兑换，而这也使得交易平台成为众多加密货币投机者的首选。对于平台而言，MT.Gox被黑客攻击至破产和BTC-e洗钱事件，为各大交易平台敲响了警钟。因此，为防范市场风险，一方面交易平台应该汲取历史教训，提升平台的技术手段，提高对投资者的交易保护，防范黑客入侵的再次发生，另一方面，交易平台应当加强对平台内投资者的风险提醒，提升投资者的风险防范意识，并且提高投资者准入门槛，引导加密货币投资者回归理性。此外，交易平台仍需要积极承担社会责任，积极纳入监管体系，提升从业人员素质，以帮助平稳加密货币价格波动，助力市场回归理性。

对区块链科技公司而言，回归行业初心，专注区块链技术的应用落地，避免以区块链概念进行非法集资，才能促进整个行业的良性发展，让加密货币的价格回归价值。区块链作为比特币的底层技术，一直被投资加密货币市场的投资者所青睐。但是区块链行业基础设施差，落地项目少之又少，众多曾经红极一时的区块链公司都逐渐退出市场，而以太坊的应用大多都是ICO融资，没有真正的将区块链技术引导至实际落地。因而，对于区块链科技公司而言，回归行业初心，放弃概念性炒作，走上创新应用的道路，才是目前区块链技术公司的当务之急，才能汲取之前行业教训，平稳市场发展。

## 第六章 结论与展望

### 6.1 结论

本文联系当前热点事件加密货币，以当前市场上份额占比前两位的比特币和以太币为案例，详细解构了加密货币的交易原理、特征、产业链发展以及发展过程，展现了加密货币发展的影响和风险。同时尝试结合 GARCH 方法和极值理论，优化对加密货币的市场风险度量方法，直观的展现加密货币市场风险大小。进而通过供需两侧分析市场风险形成原因，并对此提出监管建议。本文最终得出以下主要结论。

加密货币的产生和发展近十年之后，其已经形成了一个完整而又庞大的产业链条，投资者的趋之若鹜使得这个产业成长速度惊人。而加密货币产业的发展也会推动下一阶段产业结构的转型，未来或将提供新的支付工具。

通过以太币和比特币的发展以及特征对比，发现以太币改进了比特币诸多缺陷，将区块链技术从原有的数据分部存储应用扩展到自由搭建应用平台，提升了区块链技术的应用场景，扩充了以太币的实用价值。然而，数字加密货币的固有缺陷，仍然为价格风险留下了隐患。

在加密货币市场风险度量方面，比特币和以太币的价格波动剧烈，传统的 GARCH 方法估计出来的 VaR 值难以捕捉到价格波动的极端情况。在结合极值理论的 POT 方法以及 GARCH 方法之后，估计出来的 VaR 值在回测检验中表现更加良好。因而 GARCH-EVT 方法估计比特币市场风险的精确度更高。

同时，通过风险度量发现，比特币确实存在较高的市场风险。造成比特币市场风险加剧的原因主要是，加密货币供给端的供给机制不灵活，市场集中度过高以及定期减产的固有属性，以及需求端的应用需求难以满足和投机需求旺盛共同导致的。而外部来看，各国的政策变化也是加剧加密货币市场风险的要素之一。

综上，数字加密货币的发展在近十年间迅速发展，而这背后是不断涌现出来的新的技术概念和新的技术愿景对市场的吸引。众多投资者的不理性以及加密货币自身存在的缺陷造就了加密货币币值的不稳定，造成了其较大的市场风险。因而无论是政府、加密货币行业以及投资者都需要保持理性，做好相关风险应对。

## 6.2 研究展望

本文以加密货币的市场风险为研究对象，通过展现比特币和以太币发展的产业链，分析加密货币的市场风险，同时基于极值理论度量加密货币的市场风险大小，进而针对其市场风险探求其背后的风险成因。但是本文研究仍然存在众多不足之处需要改进和扩展。

首先，本文尝试结合机制理论和 GARCH 方法计算比特币和以太币的 VaR 值以度量加密货币的市场风险大小。虽然回测结果显示该方法度量效果良好，但是比特币和以太币仅仅作为加密货币的其中两种，难以完全代表加密货币，进而仅以两种加密货币数据难以说明这个模型完全适用于加密货币市场风险度量。因而，后续仍然需要以更多种类的加密货币数据衡量该类模型的适用性。

其次，针对市场风险的成因方面，本文不仅从加密货币的供需两侧角度，而且从主观角度审视加密货币，探究其中风险成因。然而在成因探究方面，更多采用定性分析和文献分析方法，并没有采用定量分析方法，缺乏一定说服力。因而，后续仍需要以更加客观的定量分析方法探究数字加密货币市场风险的真实成因。

最后，本文主要针对加密货币的市场风险进行分析，主要聚焦于非法定的数字加密货币，并没有将目前各国正在努力推进的法定数字加密货币纳入分析范围。今后法定数字货币必然将在市场掀起新的浪潮，因而未来仍需要对于法定数字货币展开更多的讨论和思考。

## 致谢

时光荏苒，恍惚间研究生生涯接近尾声。回想起初入南大时候，还只是一个懵懂少年，恍惚间已经在学校度过了近七年时间，少年也早已在岁月中磨砺长大。此时，百感交集，但唯有感激之情最甚。

首先，最为感激的是我的导师，王玉帅老师。初见老师，是在本科金融学课堂，王老师以其启发性的教学内容、富有激情的教学方式，引导着我们打开金融学的知识大门。何其幸运，能够在研究生期间再次遇见老师，在老师的指导下完成研究生生涯。研究生期间，老师不仅在学业上对我指导有加，而且在生活上对我关怀备至。老师于我，亦师、亦兄、亦父。

其次感谢我的父母，在我求学路上的大力支持，包容我的任性，认可我的选择。最后，感谢经管学院的老师们，感谢金融专硕的同学们，感谢大家让我在这个城市有家般的温暖和深深的归属感，让我以南大学子而骄傲。

## 参考文献

- [1] 周光友,施怡波.互联网金融发展、电子货币替代与预防性货币需求[J].金融研究,2015,05:67-82.
- [2] 谢平,刘海二.ICT、移动支付与电子货币[J].金融研究,2013,10:1-14.
- [3] 李志杰,李一丁,李付雷.法定与非法定数字货币的界定与发展前景[J].清华金融评论,2017,04:28-31.
- [4] 戴文桥.我国数字货币发展、应用与监管问题[J].合作经济与科技,2020,04:74-75.
- [5] Wallace B . the rise and fall of bitcoin[J]. Wired, 2011, 19(12):99-100.
- [6] Grinberg R. Bitcoin: An innovative alternative digital currency[J]. Hastings Sci. & Tech. LJ, 2012, 4: 159.
- [7] Melanie Swan. Blockchain: Blueprint for a New Economy[M]// Blockchain : blueprint for a new economy. O'Reilly, 2015.
- [8] Surda P. Economics of Bitcoin Is Bitcoin an Alternative to Fiat Currencies and Gold[J]. 2012.
- [9] Yermack D. Is Bitcoin a real currency? An economic appraisal[M]//Handbook of digital currency. Academic Press, 2015: 31-43.
- [10] Hanley B P. The false premises and promises of Bitcoin[J]. arXiv preprint arXiv:1312.2048, 2013.
- [11] Van Alstyne M. Why Bitcoin has value[J]. Communications of the ACM, 2014, 57(5): 30-32.
- [12] Hofert E. Regulating virtual currencies[R]. IMFS Working Paper Series, 2019.
- [13] 庄雷, 郭宗薇, 郭嘉仁. 数字货币的发行模式与风险控制研究[J]. 武汉金融, 231(03):58-64.
- [14] Van Valkenburgh P. Framework for Securities Regulation of Cryptocurrencies[J]. Coin Center, 2017.
- [15] Hughes S J, Middlebrook S T. Regulating cryptocurrencies in the United States: Current issues and future directions[J]. William Mitchell Law Review, 2014, 40(813).
- [16] Nakamoto S. A peer-to-peer electronic cash system[J]. Bitcoin.-URL: <https://bitcoin.org/bitcoin.pdf>, 2008.
- [17] 曾莹莹. 比特币价格行为机理及其影响[J]. 合作经济与科技, 2019(18).
- [18] 邓伟. 比特币价格泡沫: 证据, 原因与启示[J]. 上海财经大学学报, 2017, 19(02): 50-62.
- [19] 闫方玲, 谢敏, 任雪瑶, 等. 影响比特币价格因素的探索性分析[J]. 智库时代, 2018 (30): 149.
- [20] Kalyvas A, Papakyriakou P, Sakkas A, et al. What drives Bitcoin's price crash risk?[J]. Economics Letters, 2019: 108777.
- [21] Wood G. Ethereum: A secure decentralised generalised transaction ledger[J]. Ethereum

## 参考文献

- project yellow paper, 2014, 151(2014): 1-32.
- [22] Atzei N, Bartoletti M, Cimoli T. A survey of attacks on ethereum smart contracts (sok)[C]//International conference on principles of security and trust. Springer, Berlin, Heidelberg, 2017: 164-186.
- [23] Grishchenko I, Maffei M, Schneidewind C. A semantic framework for the security analysis of ethereum smart contracts[C]//International Conference on Principles of Security and Trust. Springer, Cham, 2018: 243-269.
- [24] 刘刚, 刘娟, 唐婉容. 比特币价格波动与虚拟货币风险防范——基于中美政策信息的事件研究法[J]. 广东财经大学学报, 030(3):P.30-40.
- [25] 练雅祺. 虚拟货币的风险及其防范——以比特币为例[J]. 时代金融, 2019(06):57-58.
- [26] Trucios C. Forecasting Bitcoin risk measures: A robust approach[J]. International Journal of Forecasting, 2019, 35(3): 836-847.
- [27] Nica O, Piotrowska K, Schenk-Hoppé K R. Cryptocurrencies: Economic benefits and risks[J]. University of Manchester, FinTech working paper, 2017 (2).
- [28] 郭文伟, 刘英迪, 袁媛, 等. 比特币价格波动极端风险, 演化模式与监管政策响应——基于结构突变点 CAViaR-EVT 模型的实证研究[J]. 南方金融, 2018, 1(10): 41-58.
- [29] Zhai Y, Zhao F. A Comparative Study of the Risk Measurement of the Bitcoin Market Based on the GARCH-T Model and the GEV Model[J]. 2019.
- [30] Troster V, Tiwari A K, Shahbaz M, et al. Bitcoin returns and risk: A general GARCH and GAS analysis[J]. Finance Research Letters, 2019, 30: 187-193.
- [31] Kohn A, Tansel A U. THE FUTURE OF VALUE: FROM BITCOIN TO CENTRAL BANK DIGITAL CURRENCIES[J].
- [32] Northeastern Association of Business, Economics and Technology, 2018: 189. Williams M T. Virtual currencies—Bitcoin risk[C]//world bank conference, Washington, DC. 2014, 21.
- [33] Bryans D. Bitcoin and money laundering: mining for an effective solution[J]. Ind. LJ, 2014, 89: 441.
- [34] Wood G. Ethereum: A secure decentralised generalised transaction ledger[J]. Ethereum project yellow paper, 2014, 151(2014): 1-32.
- [35] Philippe J. Value at risk: the new benchmark for controlling market risk[J]. Chicago: Irwin Professional, 1996.
- [36] Linsmeier T J, Pearson N D. Risk measurement: An introduction to value at risk[R]. 1996.
- [37] Engle R F. Autoregressive conditional heteroscedasticity with estimates of the variance of United Kingdom inflation[J]. Econometrica: Journal of the Econometric Society, 1982: 987-1007.
- [38] McNeil A J. Calculating quantile risk measures for financial return series using extreme value theory[R]. ETH Zurich, 1998.
- [39] Scheinert C. Virtual currencies: Challenges following their introduction[M]. EPRS, European Parliamentary Research Service, Members' Research Service, 2016.
- [40] Brandvold M, Molnár P, Vagstad K, et al. Price discovery on Bitcoin exchanges[J]. Journal

## 参考文献

- of International Financial Markets, Institutions and Money, 2015, 36: 18-35.
- [41] Bal, A. & Lee, D. K. Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data[J]. Amsterdam: Elsevier, 2015.
- [42] Lansky J. Possible state approaches to cryptocurrencies[J]. Journal of Systems Integration, 2018, 9(1): 19-31.
- [43] Network F C E. Application of FinCEN's regulations to persons administering, exchanging, or using virtual currencies[J]. United States Department of the Treasury, 2013.
- [44] Böhme, R., Edelman, B., Christin, N. & Moore, T. Bitcoin: Economics, Technology, and Governance[J]. The Journal of Economic Perspectives, 2015, 29, 213-238.
- [45] Kelly B. The bitcoin big bang: how alternative currencies are about to change the world[M]. John Wiley & Sons, 2014.
- [46] Franco P. Understanding Bitcoin: Cryptography, engineering and economics[M]. John Wiley & Sons, 2014.
- [47] Nakamoto S, Bitcoin A. A peer-to-peer electronic cash system[J]. Bitcoin.–URL: <https://bitcoin.org/bitcoin.pdf>, 2008.
- [48] Kim H K. Bitcoin regulation: legal and regulatory issues of the virtual currency system[J]. The Korean Journal of Securities Law, 2014, 15(3): 377-431.
- [49] Moore T, Christin N. Beware the middleman: Empirical analysis of Bitcoin-exchange risk[C]//International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013: 25-33.
- [50] Bouoiyour J, Selmi R. Bitcoin: A beginning of a new phase[J]. Economics Bulletin, 2016, 36(3): 1430-1440.
- [51] Sidel R. Overstock CEO sees Bitcoin sales rising more than expected[J]. Wall Street, 2014.
- [52] Meiklejohn S, Pomarole M, Jordan G, et al. A fistful of bitcoins: characterizing payments among men with no names[C]//Proceedings of the 2013 conference on Internet measurement conference. 2013: 127-140.
- [53] Diffie W, Hellman M. New directions in cryptography[J]. IEEE transactions on Information Theory, 1976, 22(6): 644-654.
- [54] Möser M, Böhme R, Breuker D. An inquiry into money laundering tools in the Bitcoin ecosystem[C]//2013 APWG eCrime Researchers Summit. Ieee, 2013: 1-14.
- [55] Buterin V. Ethereum white paper[J]. GitHub repository, 2013, 1: 22-23.
- [56] Buterin V. What proof of stake is and why it matters[J]. Bitcoin Magazine, 2013, 26.
- [57] Atzei N, Bartoletti M, Cimoli T. A survey of attacks on ethereum smart contracts (sok)[M]//Principles of Security and Trust. Springer, Berlin, Heidelberg, 2017: 164-186.
- [58] Mitsuru I, Kitamura Y, Tsutomu M. Is Bitcoin the only cryptocurrency in the town[J]. Economics of Cryptocurrency and Friedrich A. Hayek. No. 602. Institute of Economic Research, Hitotsubashi University, 2014.
- [59] Ron D, Shamir A. Quantitative analysis of the full bitcoin transaction graph[C]//International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013: 6-24.

## 参考文献

---

- [60] 许波. 比特币市场风险研究[D]. 浙江工业大学, 2014.
- [61] Yermack D. Is Bitcoin a real currency? An economic appraisal[M]/Handbook of digital currency. Academic Press, 2015: 31-43.
- [62] 张建. 风险管理视角下的数字货币监管[D]. 华中科技大学, 2017.