基于 PoW 机制的区块链估值模型

王 帅, 秦 波, 陈晋川, 姬思宇, 张诗童

中国人民大学信息学院 北京中国 100872

摘要 区块链技术自诞生之日便引起了各界的关注, 随着数字经济的发展, 这类交易匿名、去中心化且技术相对安全的区块链网络技术逐渐被人们熟悉了解。区块链技术的首次出现刺激了更多功能和需求的区块链网络的产生与发展。相较于传统货币, 数字资产具有独一无二的优势。近年来, 以区块链为核心技术的数字资产价值动荡起伏, 新闻媒体争相报道也对数字资产的价值起到了推波助澜的作用。随着数字资产社区的逐渐扩大, 人们逐渐意识到了数字资产的价值所在, 但投资数字资产会面临各种风险。本文旨在以基于工作量证明(PoW)机制的区块链网络为代表, 对数字资产价值走势进行全面系统的分析。通过对数字资产获取方式的调研, 结合市场历年价格的行情分析, 以“人类行为学”和“实证主义”相结合的方式, 解析出基于 PoW 机制的区块链的价值分析方法。

关键词 区块链; 工作量证明; 价值分析
中图法分类号 TP399 **DOI 号** 10.19363/j.cnki.cn10-1380/tn.2018.05.04

Blockchain Estimation Model Based on PoW Mechanism

WANG Shuai, QIN Bo, CHEN Jinchuan, JI Siyu, ZHANG Shitong

School of Information, Renmin University of China, Beijing 100872, China

Abstract Blockchain technology has aroused the public's attention since its birth. With the development of the digital economy, such Blockchain network technologies with anonymous transactions, decentralized and relatively secure technologies ,have become increasingly familiar to people. The first appearance of Blockchain technology has stimulated the emergence and development of Blockchain networks with more functions and requirements. Digital assets have unique advantages over traditional currencies. In recent years, the value of digital assets with Blockchain as the core technology has been ups and downs, and news media rushing to report on it has also contributed to the value of digital assets. With the gradual expansion of digital asset communities, people are increasingly aware of the value of digital assets, but investing in digital assets faces various risks. This article aims to take a Blockchain network based on the proof-of-work (PoW) mechanism as a representative to conduct a comprehensive and systematic analysis of the value of digital assets. By investigating the way of acquiring digital assets and combining the market price analysis over the years, we analyzed the Blockchain value analysis method based on the PoW mechanism in a combination of “human behavior” and “positivism”.

Key words blockchain; proof of work; price analysis

1 引言

货币在推进人类文化发展中扮演着重要的角色, 是人类文明发展中各阶段的里程碑。货币的演化历史从古至今经历了: 实物货币、称量货币、纸币、电子货币和数字资产五个重要阶段。2008 年 10 月 31, 一位化名为 Satoshi Nakamoto(中本聪)的人在密码学论坛上发布了一篇名为 *Bitcoin: A Peer-to-Peer Electronic Cash System* 的区块链网络设计白皮书[1]。在 2009 年公开了区块链技术网络的实现源码, 2009 年 1 月 3 日 18 时 15 分 05 秒, 世界上第一个以区块链为技术的资产诞生, 自此进入了区块链网络新世界的大门。虽备受争议, 区块链技术的确是互联网技术发展中里程碑式的创新。

基于 PoW 的区块链数字资产并不是凭空生成的, 而是由一个个矿工利用计算机 CPU/GPU 算力不断破解一个特解难题, 即所谓的工作量证明机制(PoW), 破解成功便可以获得一定数量的数字资产作为奖励,

通讯作者: 秦波, 博士, 讲师, Email:bo.qin@ruc.edu.cn。
本课题得到国家自然科学基金面上项目（NO. 61772538）资助。
收稿日期: 2018-1-31; 修改日期: 2018-4-28; 定稿日期: 2018-05-02

这就是所谓的挖矿过程[2]。想要计算出特解难题, 就需要矿工付出相应概率的算力, 谁的算力多, 谁先计算出特解的可能性就更大。所以以工作量证明(PoW)机制参与挖矿都将会付出不小的算力成本。这也保障了基于 PoW 机制的区块链网络的蓄意破坏者须要付出大量的经济本钱为代价。后台总共会设定一定数量的特解, 所以一个基于 PoW 机制的区块链网络数字资产数量有限, 后台会调整这个特解的难度, 高效便捷地控制数字资产可被挖掘的数量, 这和现实生活中黄金开采十分相似, 地球中黄金量也是有限的。

获得数字资产有两种形式, 第一种形式便是基于 PoW 机制, 作为矿工通过算力破解特解。第二种形式是经过交易平台进行购买。破解特解是计算机算力之间的竞争, 计算机性能越好, 挖掘到数字资产的可能性就越大。然而, 在现如今庞大的挖矿市场来看, 依靠个人计算机挖矿效率就显得十分低下了[3]。所以, 为了增大挖矿效率, 除了在不断优化挖矿设备的性能之外, 联合挖矿即所谓的矿池应运而生, 挖矿由个人逐渐升级庞大到组织甚至是公司层面。

数字资产交易双方均需要“钱包”和“地址”, 过程可以类比为电子邮件之间的通信。交易双方利用手机或个人电脑, 登录某个交易平台便可以进行交易了。通过在交易平台进行网络购买是获取数字资产的一种重要渠道, 大部分购买和提现的功能均可以在交易平台实现 [4,5]。

股票、债券、期货、房地产等价格走势分析在市场中已经全面覆盖且相对成熟, 但对于基于区块链技术的数字资产市场价位的探索还尚未成熟。最近, 数字资产价值分析在不断地发展, 进行理智的分析, 了解数字资产价值涨跌的原因, 会给数字资产投资者带来十分有价值的投资信息。

对于基于区块链技术的数字资产价值分析具体指的是分析资产市场变化以及对其价格的影响因素, 但是现在存在的问题是, 现阶段我们都是基于“实证主义”对数字资产价值进行分析, 即“技术分析”。他们使用类似于股票的分析方式, 利用经济分析工具, 例如公式数学模型、趋势延长线等进行分析, 但是实际上在基于区块链技术的数字资产市场仅仅利用价格数学模型预测价格的准确度并不高[6]。

投机具有悠久的历史、这似乎是资本主义固有的。历史上来看, 投机资产中一个共同的特征是估值难度大。南海公司泡沫案和荷兰郁金香疯狂投机案等等, 都反映了人类的贪婪行为。另一方面, 也很难为资产设定一个客观的价值, 所有的投机行为都反映在时间序列的超指数增长[7]。最近, 基于区块链技术的数字资产便处于投机的风口浪尖中, 其中人类因素是数字资产价值大幅度涨跌的主要推手。仅仅利用“实证主义”进行价值评估会忽略掉人类因素, 但对基于区块链技术的数字资产的价值评估恰恰不能缺少的就是对于人类因素的分析。

文章将“实证主义”和“人类行为学”相结合, 对基于 PoW 机制的区块链数字资产进行理智全面的分析其市场变化和其价格的影响因素。首先, 我们通过调研, 对数字资产价格波动进行剖析, 总结出现阶段数字资产主要价格依据。其次, 我们对于现阶段的研究和市场现状提出对于区块链数字资产的思考和假设。最后, 通过实证分析大量数据得出回归相关结论, 并对其他基于 PoW 机制的数字资产进行检验证明。

2 数字资产价值波动分析

货币具备三个主要特性, 分别是交易媒介、存储价值和记账单位。根据经济史, 货币与权力和政治紧密相关。起初, 货币由金属制造, 其价值本质取决于金属本身的价值。后来, 货币被印在纸币上, 其价值又与黄金数量存在某种联系[8,9]。货币本身具有价值, 所以其可以充当价值的标尺。市场上对于基于 PoW 机制的数字资产价值评估是欠缺的, 我们可以将其视作一种商品, 对其价值进行评估。

2.1 区块链数字资产价值评估和限制因素

评估区块链数字资产的价值, 我们必然要提到它的主要实现技术, 区块链技术。区块链技术的原理本质可以追溯到著名的“拜占庭将军问题”。对于互联网技术来说, 拜占庭将军问题的内在含义是, 在没有可信任第三方的情况下, 即权威节点, 网络如何快速收敛达成全网共识。区块链技术本质上很好的解决了经典的拜占庭将军问题, 达到不需任何中心节点, 即在分布式的情况下, 达成了全网的共识[10,11]。区块链技术主要解决的是在一个分布式场景中达成共识的问题。而工作量证明(PoW)机制是实现高效达成共识的主要算法和手段[12]。工作量证明(PoW)机制使得区块链交易不可杜撰且不可篡改。工作量证明(PoW)机制的核心思想是通过分布式节点(矿工)竞争计算出一个特解, 该特解是一个求解复杂困难但验证较容易的 SHA256 数学难题, 最快解出这个特解的矿工拥有该区块的记账权, 并且会获得一定数额的比特币奖励, 同时该区块也会计入到最长的区块链上[13-15]。由此可知参与 PoW 机制的矿工都将会付出不小的算力成本。

基于 PoW 机制的数字资产具有基本的价值, 即

成本。它最初的获得是利用“挖矿”, 利用计算机破解特解难题来获得数字资产, 即工作量证明(PoW)机制。如果以挖矿成本衡量该数字资产价值, 则可以根据投入的矿机费用、设备运行电费以及人力消耗来大概估计生产数字资产的大概成本。它的成本也并非一成不变, 随着矿机的性能不断优化, 运算成本是在减少的, 但是由于全球挖矿设备数量增加和技术的升级, 单位设备生产出新的数字资产的数量呈现减少的趋势。总体看来, 数字资产挖矿成本是上升的。从经济角度来看, 挖矿成本仅具有一点门槛价值, 从长远看来, 数字资产的成本因素只能作为估价的底线参考。价格主要取决于数字资产市场对于该类数字资产未来发展的总体认同。

以区块链为技术的数字资产正在逐渐进入大众的视野被人们所熟悉。但是在区块链数字资产可预见的未来, 它能够替代主流货币的可能性微乎其微, 我们假设 2100 万比特币区块链数字资产可以替代与其竞争的币种, 对该数字资产进行估值。将流通中的现金(即 M0)与 2100 万比特币区块链数字资产作比较, 可以估计出单个数字资产的价格, 但长远来看, 按照此方法对数字资产进行估值, 只能作为估值上限进行参考。

通过上述两种方式对数字资产进行估值是不准确的, 只能作为上限和下限进行参考。在现实生活中, 区块链数字资产跌宕起伏就犹如在游乐场坐过山车, 波动幅度之大, 可以让人一夜暴富, 也可以让人一贫如洗。如此大的价格波动, 为数字资产价值估计与预测带来了很大的机遇和挑战。数字资产价值较难估计主要是由于以下几点因素。首先, 数字资产价值是人们心中对该数字资产市场的认同价位, 虽然数字资产的挖矿成本可以提供一定的参考, 但是基于 PoW 机制的区块链数字资产实际的价值涨跌取决于挖矿成本和该数字资产市场两者的综合因素。而且现在某些区块链数字资产开采数量供不应求, 从短期中期来看, 舆论新闻消息对数字资产价值的影响远大于开采成本对价值的影响; 第二, 区块链数字资产属于新兴事物, 虽逐渐被大众认知, 但是却未被普遍接受。区块链数字资产的暴涨暴跌几乎都伴随着舆论新闻爆出热点事件, 而且国家相关政策的出台, 也会影响区块链数字资产价格走势, 难以预测; 第三, 区块链数字资产成为了国际投机市场的新目标新猎物, 随着投机资本的轮番坐庄, 其价格的可预测性变得更加艰难。

2.2 历史价格波动及分析

根据历史数据及相关比特币区块链技术网络的大事件, 我们可以把价格变动看作是人类对于事件结果做出的反应, 利用人类行为学对价格涨跌进行分析, 可以对数字资产市场震荡原因或发展有着深刻的理解和预测。

对区块链网络价格的分析需要结合实证主义和人类行为学, 我们将价格波动一部分原因看作为人类活动的结果。对区块链网络的需求毋庸置疑是由于人类行为活动决定的。舆论新闻是对最近人类活动行为的描述, 所以舆论新闻的发展会很大的影响人类心理进而对区块链数字资产价格产生影响。总而言之, 舆论新闻对区块链数字资产价格走势产生了突破性的影响, 舆论新闻描述了个体对数字资产市场付诸的行动和反应。舆论新闻对人类活动的报道会引起数字资产市场价格的连锁反应, 因为新闻舆论会对其他个体的行动产生影响。国家政策、安全方面和市场认可等等最有影响力的事件才会对数字资产价值产生最大程度的影响力。

为了更好地了解区块链数字资产价格波动原因, 我将分析近几年发生的几个大事件对比特币区块链价格产生的影响, 来探索影响区块链数字资产价格的因素。

2009 年到 2010 年, 区块链数字资产刚刚出现, 发展较为缓慢, 市场处于认知初期, 接受程度不高, 每个比特币价格不超过 1 美元。

2011 年 6 月, 区块链数字资产交易网站遭遇黑客攻击将 25000 比特币转进了自己的账户。由于区块链数字资产交易网络的匿名性和不可追踪性, 这笔交易始终无法追溯。这场交易网站遭遇黑客攻击事件在区块链数字资产社区引起很大轰动, 动摇了数字资产投资者的信心, 比特币价格由此一路下跌, 相较于 6 月最高价格, 跌幅在 90%以上。

2012 年, Linode 作为网站托管商, 由于其服务器的超级管理密码泄露, 使得 40000 多枚比特币失窃, 以致于它的价格一路下跌到四美元左右, 这又是一起黑客问题造成的区块链数字资产价格下跌。根据比特币区块链网络每隔四年挖矿减半的设定, 在 2012 年 11 月 28 日, 比特币区块链网络挖矿数量减半从 7200 个减至 3600 个, 由于供给减半, 数量供不应求, 使得价格上涨。

2013 年 2 月, Reddit 发出公告, 表示可以接受比特币区块链数字资产进行支付。之前, WordPress 也已宣布接受数字资产比特币支付。2013 年 3 月, 塞浦路斯爆发了严重的银行危机, 其冻结了 110 万民众的转账交易权力, 而且强制对银行账户征税, 并逐渐关闭股市和银行。区块链数字资产成为人们的资

金出路, 随着塞浦路斯经济危机爆发, 比特币数字资产价格实现了三倍涨幅。2013 年 3 月 12 日, 比特币区块链网络出现故障造成了其价格的大幅度下跌。2013 年 4 月 12 日, 在比特币数字资产出现大幅度下跌之后, 这种在线货币交易所宣布暂时停止交易。2013 年 6 月 8 日, 香港政府正式批准电子货币交易中心(GBL)允许区块链数字资产的交易业务。2013 年 12 月 5 日, 中国央行等五部委联合发布了关于区块链网络数字资产的报告通知, 旨在加强对于比特币区块链资产风险的防范控制问题, 比特币价格在此消息之后大幅度下跌 35%。2013 年 12 月 7 日, 百度公司宣布停止将比特币数字资产作为支付手段, 此消息一出, 其跌到了 697 美元。次日, 兰博基尼经销商宣布比特币数字资产可以作为支付特斯拉电动汽车的支付工具, 经此消息, 其价格回暖到 900 余美元。2013 年 12 月中旬, 中国人民银行约谈第三方支付平台, 区块链数字资产交易网站充值渠道在此之后被相继关闭, 此消息一出, 比特币数字资产单日提现数额超过 200 美元。

2014 年第一季度, 区块链数字资产便处于降温的趋势: 2014 年 2 月 7 日, Mt.Gox 由于技术发生漏洞故障, 暂停了比特币数字资产赎回业务, 交易服务依旧会提供。此消息导致了比特币价格的下跌, 虽出现了小程度的回暖现象, 但是此事件的影响力还是特别深远。2014 年 4 月 24 日, 央行与第三方支付平台机构和商业银行进行了约谈, 希望切断关于比特币的资金链, 并且部署了对于区块链数字资产的防控工作。第二天, 支付宝发表公告, 严肃表示不会为区块链数字资产提供任何服务。2014 年 8 月 10 日, 英国财务大臣 George Osborne 发出信号表示英国想要将区块链数字资产合法化[16]。

2015 年 7 月, 人民币贬值程度很大, 投行资本转而将目光转移到区块链数字资产市场。2015 年 10 月, 投行资本进入比特币区块链数字资产市场, 通过在火币网和 OKCoin 交易平台试探盘底, 它触底反弹, 价格翻倍[17]。2015 年 10 月 22 日, 根据欧洲法院裁定, 在欧洲国家区块链数字资产应该受到与传统货币平等的待遇, 出台了免征增值税的政策。根据欧盟的法律, 法定货币之间的交易(包括纸币和硬币)是免征增值税的。瑞典政府表明, 区块链数字资产与传统法定货币不同, 不应该免征增值税, 但欧洲法院却持不同态度, 使区块链数字资产的支持者们颇受鼓舞[18]。

2016 年, 区块链数字资产市场春风得意, 越来越多的人认识到了区块链网络的价值。2016 年初, 中国央行召开了关于数字货币的研讨会, 旨在想要推出国家法定的数字货币, 研讨关于数字货币在不同场景当中的应用, 极大地鼓舞了中国数字货币的从业者和投资者, 比特币区块链资产价格也应声上扬了。2016 年 6 月 24 日, 英国脱离欧盟, 英国首相卡梅伦也宣布辞职, 造成英镑下跌, 然而比特币价格却应声上涨, 涨幅接近 20%。2016 年 7 月 10 日, 比特币区块链网络进行了第二次以四年为周期挖矿数量减半期, 导致供不应求, 价格上涨[19]。

2017 年比特币价格走势真正演绎了什么叫做过山车行情, 2017 年 1 月 11 日是全年最低价位 789 美元, 然而在 12 月 18 日达到全年最高价位 18674 美元, 高达接近 1700%的涨幅, 然而在 6 月 7 月它的行情却并不如意, 下跌了 36%。对于比特币区块链网络本身来说, 2017 年发生了极为关键的事件, 2017 年 8 月 1 日, 比特币现金区块链网络出现, 它是在比特币区块链原有主链上硬分叉产生的新一种数字资产, 分叉期间比特币行情震荡下跌, 分叉结束后, 在 9 月份市场回暖上涨。2017 年 9 月 4 日, 中国央行宣告将 ICO 定性为了不合法的金融活动, 短期时间对区块链数字资产价格造成了不小的打击[20]。

2018 年 1 月 17 日, 比特币区块链数字资产价格一度下跌高达 25%, 原因在于多国政府对数字资产增强了管控, 交易市场火爆的韩国也包含其中, 中国政府相关部门也下令关闭部分挖矿商业务[21]。2018 年预测将会受到各国政府更多的监管制约, 对于价格涨幅的影响我们拭目以待, 总而言之, 2018 年对于区块链数字资产来说, 又会让人充满期待。

2.3 区块链数字资产的主要价格依据分析

区块链数字资产行情犹如过山车一般, 我们注意到每当有与之相关热点的事件发生时, 都会导致该数字资产价格暴涨暴铁, 根据上节历史价格波动分析, 我们推断出, 在区块链数字资产发展阶段, 以下几个因素是导致区块链数字资产价格波动的主要原因:

(1) 安全性

从影响区块链数字资产价格波动的事件中, 可以看出安全问题是影响数字资产价格的首要因素, 黑客攻击区块链网络或者是交易平台的负面事件无法预测, 一旦发生如此的负面事件, 便会对数字资产价格造成很大的影响。例如 2011 年 6 月这场区块链交易网站遭遇黑客攻击事件在比特币区块链网络社区引起很大轰动, 动摇了投资者的信心, 价格由此一路下跌。2012 年, Linode 作为网站托管商, 由于其服务器的超级管理密码泄露, 使得 40000 多枚比

特币失窃, 以致价格一路下跌到四美元左右。2014 年 2 月 7 日, Mt.Gox 由于技术发生漏洞故障, 暂停了区块链数字资产赎回业务, 交易服务依旧会提供, 但导致了比特币价格的下跌。根据中国国家信息中心信息安全研究与服务中心颁布的《2013 年上半年中国信息安全综合报告》中的表示, 我国发生黑客攻击和网络诈骗的首要对象就是比特币[22]。它的总数量有限, 价值不断攀升, 由于其具有很高的匿名性, 导致一旦被盗就很难追溯, 这种特性引起了黑客的广泛关注, 由于攻击比特币区块链数字资产具有很高的回报性和难以追溯的高匿名性, 使得安全性成为引起区块链数字资产价格波动的首要因素。

黑客的攻击具有很大的负面影响且具有不可预测性。所以, 当区块链网络或交易平台遭到黑客攻击时, 数字资产价格一定会大幅度的跳水。此时, 作为正确的投资理念应该是适量买入, 随着安全漏洞的逐渐修复, 区块链数字资产价格会在未来产生回暖, 进而会使投资者产生收益。

(2) 相关政策的出台

区块链数字资产价格波动的一部分原因来自于各个国家监管层面相关政策的出台。在区块链的发展初期, 各个国家的监管部门对于区块链网络的性质和影响力还不是十分清楚, 对其监管是有缺失的。但随着近几年区块链数字资产市场的不断扩大, 区块链数字资产的影响力和交易额也在不断增加, 各国政府对区块链数字资产也产生了高度的重视。各个国家陆续出台了对区块链数字资产相关的法律法规, 国家政策动向难以预测, 这会加剧对区块链数字资产价格的敏感程度。例如, 2015 年 10 月 22 日, 根据欧洲法院裁定, 在欧洲国家区块链数字资产应该受到与传统货币平等的待遇, 出台免征增值税的政策, 使得区块链数字资产支持者受到很大鼓舞。2018 年 1 月 17 日, 比特币数字资产价格一度下跌高达 25%, 原因在于多国政府对区块链数字资产增强了管控, 交易市场火爆的韩国也包含其中, 中国政府相关部门也下令关闭了部分挖矿商的业务。

(3) 市场对区块链数字资产的认可程度

市场对区块链数字资产价值的认可程度也会不同程度的影响比特币价格的涨幅。例如, 2009 年到 2010 年, 区块链网络技术刚刚出现, 发展较为缓慢, 市场处于认知初期, 区块链数字资产接受程度不高。2013 年 12 月兰博基尼经销商宣布比特币区块链数字资产可以作为支付特斯拉电动汽车的支付工具, 经此消息其价格上涨。2016 年认识到区块链数字资产价值的人越来越多。年初, 中国央行召开了关于数字货币的研讨会, 旨在想要推出国家法定的数字货币, 研讨关于数字货币在不同场景当中的应用, 极大地鼓舞了中国数字货币的从业者和投资者, 比特币区块链数字资产价格也应声上扬。从历史行情来看, 区块链数字资产或者相关事件经过主流市场认可的时候会引发国内外媒体争相报道, 这会对区块链数字资产价格有一个显著的上行调整, 所以, 市场对区块链数字资产的认可与接收会是推动区块链数字资产价格上涨的重要因素。

(4) 四年减半的挖矿周期

按照经济学基本的供应关系法则, 如果需求量增加, 供给关系减少, 价格必然会上涨。四年比特币区块链网络挖矿数量减半是众所周知的事实, 在 2012 年 11 月 28 日, 比特币区块链网络挖矿数量减半, 从 7200 个减至 3600 个, 由于供给减半, 数量供不应求, 使得价格上涨。在 2016 年 7 月 10 日, 进入第二个以四年为周期的产量减半期时期, 导致其数量供不应求, 价格上涨。所以在区块链网络挖矿数量减半的时间段, 是值得投资者关注的, 产量供不应求, 必会导致价格上扬, 所以投资者应该在挖矿数量减半的关键时期逢低吸纳。

(5) 硬分叉和其他数字资产

2017 年 8 月 1 日, 比特币现金区块链网络出现, 它是在比特币区块链原有主链上硬分叉产生的新一种数字资产, 分叉期间比特币数字资产行情震荡下跌, 分叉结束后, 在 9 月份市场回暖上涨。硬分叉短期会使区块链数字资产市场震荡下跌, 但长期看来趋势是上涨的, 因为硬分叉解决了区块链的性能问题, 更多人会接受分叉前后的区块链网络, 而且分叉前数字资产的持有者能得到相同数量的分叉资产。分叉的数字资产是镜像原来区块链而来的, 却与之前有着不同的协议, 新的分叉数字资产分化了资金流和市场关注度, 所以短期内会导致区块链数字资产价格下跌, 由于价值的稀释。硬分叉对区块链数字资产带来的影响是短期的, 从长期看来其价格还是会上升, 硬分叉可以看作区块链数字资产价格上扬的减速带[23]。

由于比特币区块链网络技术本身开源的性质, 不断有其它区块链数字资产发行上市, 例如以太坊等。它的思想和技术来源于中本聪的首个区块链网络, 可以说是首个区块链数字资产的超发。其它数字资产层出不穷, 首个区块链数字资产并没有绝对的技术优势由于其开源性质, 市场只看到它的价格高, 挖矿难度大, 其它的数字资产价格较为便宜, 比较容易投机操纵, 所以其它区块链数字资产的存在必

定会分摊市场, 影响比特币区块链资产的价格。

综上所述, 无论是安全性问题、国家政策出台、市场认可程度、四年挖矿减半、分叉和其它数字资产等因素, 均会引起国内外媒体的大肆报道, 区块链数字资产会因此逐步进入公众的视野, 人们对于区块链网络的关注度也会随之增加。

3 PoW 机制的区块链估值

上一章节分析了数字资产价格的影响因素, 成本、安全性、国家政策管制、市场认可程度、四年挖矿数量减半规律、分叉和其它数字资产等等均会对数字资产价值造成不同程度的影响。本章将利用实证主义, 分别对成本和安全性、国家政策管制等其他影响因素进行数据上的分析, 做出数学回归拟合模型分析。

3.1 挖矿计算难度和数字资产价值的相关性

考虑到数字资产的价值问题, 成本是首先需要想到的影响因素。首个区块链数字资产最初的获得的方式是利用计算机破解特解难题, 即我们所说的基于工作量证明(PoW)机制进行挖矿。所以我们可以根据投入的矿机费用、设备运行电费以及人力消耗来大概估计生产单位数字资产的大概成本。矿机和人力的投入属于固定消费, 而平均生产单位数字资产的电量主要与破解特解的计算难度和自身算力有关, 其中将自身算力视为恒定, 因此破解特解的计算难度变化可以直接反映出区块链数字资产成本的变化趋势。

为了证明区块链数字资产价格是否与挖矿计算难度有一定的相关性, 我们选取 Investing.com 提供的比特币区块链网络价格历史数据和“比特范”提供的历史挖矿计算难度数据, 对 2014 年 9 月 21 日到 2018 年 1 月 7 日这段时间进行分析。数据是以周为单位的, 如图 1 所示, 我们可以看到价格走势与计算难度走势基本相同, 且大体上呈现上升趋势。

根据梅特卡夫定律, 随着用户数量的平方数增加, 网络的有用性随之增加。换而言之, 网络的价值为$V = K \times N^2$(K为价值系数, N为用户数量), 即网络的价值与联网用户数量平方成正比, 例如电话网络与电话用户数量平方成正比关系[24,25]。

由于全球各地对于投入的挖矿设备在数量上以及技术上都在不断的提升, 导致了单位运算能力的设备能够挖掘出的区块链数字资产数量呈现逐步减少的态势, 所以单位比特币区块链网络数字资产的实际开发成本是在快速上升的, 图 1 可以很好的证明这点。

图 1 价格与计算难度走势

Figure 1 Trends in price and calculation difficulty

类比梅特卡夫定率, 我们做出假设并验证, 网络参与挖矿的矿工数量越多, 挖矿计算难度就越大, 该区块链网络的价值就越高。所以我们猜想挖矿计算难度的平方与区块链数字资产价格之间呈线性关系, 所以我们将比特币区块链网络历史价格与历史挖矿计算难度的平方绘成散点图, 如图 2 所示, 可以看出价格与计算难度平方存在一定的线性关系, 所以我们对两个变量进行回归分析, 进一步对两者关系进行验证。

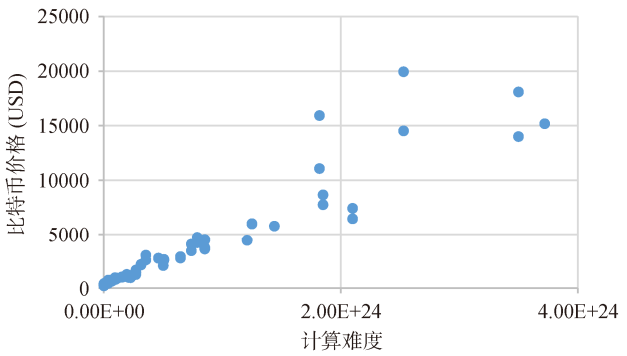

图 2 价格与计算难度平方散点图

Figure 2 The scatter plot of price and calculation difficulty squared

由表 1 可知, 相关系数 *Multiple R*, 衡量的是价格与挖矿计算难度平方两者之间的相关程度, *R* 等于

0.9526, 说明价格与挖矿计算难度平方相关程度很高, 且呈正相关关系。可决系数 *R Square,* 用来度量拟合优度, 其值 R^2 等于 0.9075, 表明挖矿计算难度平方这个变量用来解释价格的能力为 90.75%, 拟合效果较强。调整 *R* 平方判定系数 *Adjusted R Square*, 其值等于 0.9069, 说明挖矿计算难度平方可以说明价格的 90.69%, 价格的 9.31%需要其他因素来说明。表 2 表示通过 *F* 显著性统计量, 即 *Significance F* 来判定价格与挖矿计算难度平方回归模型的回归效果, 价格与挖矿计算难度平方分析中的 *P* 值等于 $8.69153*10^{-90}$, 远小于显著性水平 0.05, 说明关于价格与挖矿难度平方回归模型的回归效果较为显著。由表 3 可知, 挖矿计算难度平方的 *P* 值为 $8.69*10^{-90}$, 远小于显著性水平 0.05, 说明挖矿计算难度平方这个变量的回归系数十分显著, 挖矿计算难度平方与价格存在相关性[26-29]。

由上述回归分析, 我们基于工作量证明(PoW)机制, 进而分析证明了挖矿计算难度的平方与价格具有显著的线性关系。

表 1 价格与计算难度平方回归统计表

Table 1 Regression statistics of price and calculation difficulty squared

回归统计	
Multiple *R*	0.952614598
R Square	0.907474572
Adjusted *R* Square	0.906930305
标准误差	1005.821129
观测值	172

表 2 价格与计算难度平方方差分析表

Table 2 Variance analysis table of price and calculation difficulty squared

	df	*SS*	*MS*	*F*	Significance *F*
回归分析	1	1.69E+09	1.69E+09	1667.333	8.69153E-90
残差	170	1.72E+08	1011676		
总计	171	1.86E+09			

表 3 价格与计算难度平方方差回归参数表

Table 3 Variance regression parameter table of price and calculation difficulty squared

	Coefficients	标准误差	t Stat	P-value	Lower 95%	Upper 95%	上限 95.0%
Intercept	308.4625265	84.21168	3.662942	0.000333	142.227263	474.6978	474.6978
X Variable 1	4.74782E-21	1.16E-22	40.83299	8.69E-90	4.51829E-21	4.98E-21	4.98E-21

3.2 搜索量数据和数字资产价格的相关性

实际上, 区块链数字资产的涨跌是成本信息结合市场信息形成的。从短期和中期来看, 新闻媒体爆出利好和利空消息对数字资产持有人或者是投资者心理影响很大。每次区块链数字资产暴涨暴跌几乎都伴随热点事件的出现。这些热点事件基本包含了上一章分析的影响数字资产价格的行为(安全、政策出台、市场认可程度、四年减半挖矿规律、硬分叉及其它数字资产等等), 人类行为无疑可以决定对区块链数字资产的需求, 新闻媒体报道是对最新个体活动的描述。所以影响价格的很大因素是这个新闻媒体内容的发展态势。Robert Shillerr 认为, 区块链数字资产价格的走势特别符合投机泡沫的定义, 人们争先恐后的持有某类数字资产, 希望通过增值获取财富, 区块链数字资产投资逐渐被人们所熟悉与了解, 新闻媒体在其中很大程度上起到了推波助澜的影响[30]。新闻媒体对大众心理影响的最直接反应可以体现在公众对于这一事物的关注度。所以, 我们假设新闻媒体对区块链数字资产相关事件的报道会引起公众的注意力, 从而间接引起区块链数字资产价格的变化。我们将对这一现象进行验证。

公众注意力是一个抽象的概念, 幸运的是, 搜索引擎给我们提供了很多量化信息, 具有代表性的 Google Trend(谷歌趋势)提供了特定关键词的搜索与点击热度数据。所以我们下载了 Google Trend 对于关键词‘Bitcoin’的搜索量数据(以周为周期, 已标准化 0-100 数值比例), 间接反映比特币区块链网络的价值所在。我们选取 2014 年 9 月 21 日到 2018 年 1 月 7 日这段时间的比特币价格与‘Bitcoin’的搜索量进行分析。数据是以周为单位的, 如图 3 所示, 我们可以看到价格走势与‘Bitcoin’的搜索量基本相似, 大体呈上升趋势。

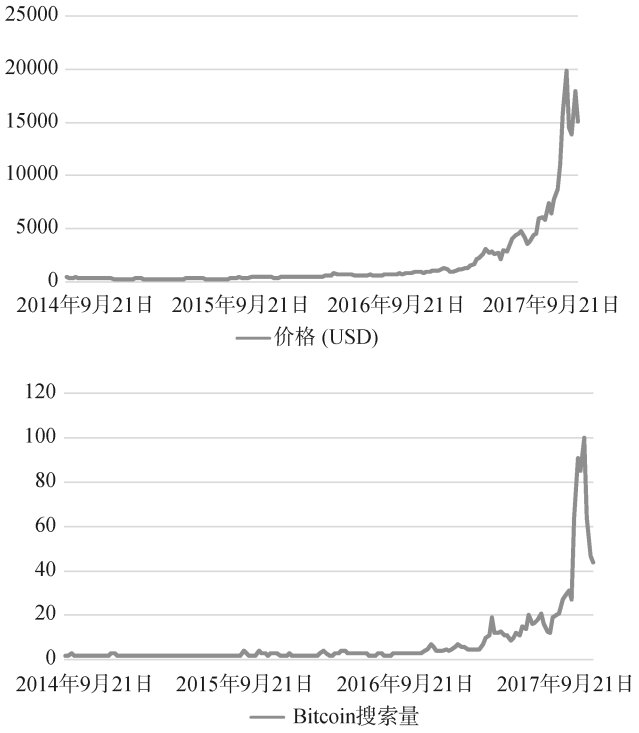

图 3　价格与搜索量走势

Figure 3　Trends in price and search volume

我们假设搜索量与其价格之间呈线性关系，我们将历史价格与历史‘Bitcoin’搜索量绘成散点图。如图 4 所示，可以看出价格与搜索量存在一定的线性关系，所以我们对两个变量进行回归分析，进一步对两者关系进行验证。

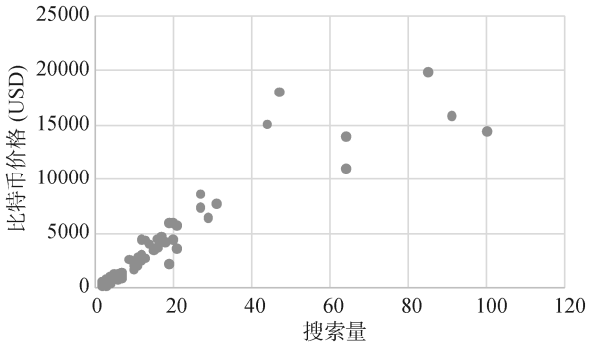

图 4　价格与搜索量散点图

Figure 4　Scatter plot of price and search volume

由表 4 可知，相关系数 *Multiple R*，衡量的是价格与搜索量两者之间的相关程度，*R* 等于 0.9426，说明价格与搜索量相关程度很高且呈正相关关系。可决系数 *R Square*，用来度量拟合优度，其值 R^2 等于 0.8884，表明搜索量这个变量用来解释价格的能力为 88.84%，拟合效果较强。调整 *R* 平方判定系数 *Adjusted R Square*，其值等于 0.8877，说明搜索量可以说明价格的 88.77%，价格的 11.23%需要由其他因素来说明。表 5 表示通过 *F* 显著性统计量，即 *Significance F* 来判定价格与搜索量回归模型的回归效果，价格与搜索量分析中的 *P* 值等于 $7.27*10^{-83}$，远小于显著性水平 0.05，说明关于价格与搜索量的回归模型的回归效果较为显著。由表 6 可知，搜索量的 *P* 值为 $7.27*10^{-83}$，远小于显著性水平 0.05，说明搜索量这个变量的回归系数十分显著，搜索量与价格存在相关性。

表 4　价格与搜索量回归统计表

Table 4　Regression statistics for price and search volume

回归统计	
Multiple *R*	0.942552
R Square	0.888404
Adjusted *R* Square	0.887747
标准误差	1104.626
观测值	172

表 5　价格与搜索量方差分析表

Table 5　Analysis of variance of price and search volume

	df	*SS*	*MS*	*F*	Significance *F*
回归分析	1	1.65E+09	1.65E+09	1353.348	7.27E-83
残差	170	2.07E+08	1220198		
总计	171	1.86E+09			

所以，由上述回归分析，搜索量与价格具有显著的线性关系。因为搜索量与用户相关，根据梅特卡夫定律，网络价值与参与入网络的用户数量的平方成正比关系。我们做出假设，测试搜索量平方与比特币区块链网络价格的回归关系。如图 5 所示，可决系数 *R Square* 等于 0.6603，对于估值模型的拟合效果不佳。所以搜索量与价格的线性关系更明显。

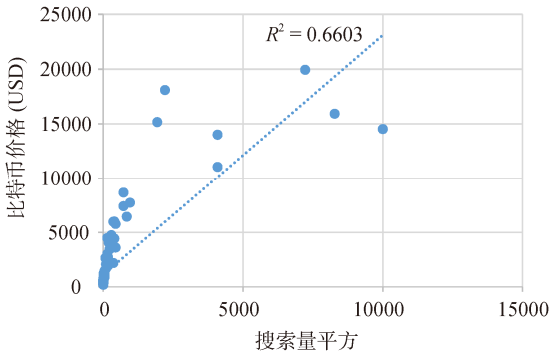

图 5　价格与搜索量平方散点图

Figure 5　Scatter plot of prices and search volume squared

表 6　价格与搜索量方差回归参数表

Table 6　Variance regression parameters for price and search volume

	Coefficients	标准误差	t Stat	P-value	Lower 95%	Upper 95%	下限 95.0%	上限 95.0%
Intercept	76.21922	95.45635	0.798472	0.425711	–112.213	264.6516	–112.213	264.6516
X Variable 1	210.2274	5.714584	36.78788	7.27E-83	198.9467	221.5081	198.9467	221.5081

3.3　多变量的数字资产估值回归分析

根据以上单变量分析, 我们将基于 PoW 机制的挖矿计算难度和搜索量作为自变量, 以挖矿难度平方和搜索量作为检测因子, 将比特币区块链数字资产价格作为因变量进行多变量回归拟合分析。由表 7 可知, 相关系数 *Multiple R* 等于 0.9839, 表明自变量与因变量之间相关程度很高且呈正相关。可决系数 *R Square* 等于 0.9681, 挖矿难度平方与搜索量测定价格的拟合效果很高。调整 *R* 平方判定系数 *Adjusted R Square* 其值等于 0.9677, 说明两个自变量能说明因变量比特币价格的 96.77%, 3.23%要由其他因素来解释。表 8 通过 *F* 显著性统计量, 即 *Significance F* 来判定多变量回归模型的回归效果, 分析的 *P* 值等于 $4.2*10^{-127}$, 远小于显著性水平 0.05, 说明多变量回归模型的回归效果较为显著。由表 9 可知, 挖矿计算难度平方的 *P* 值为 $8.98*10^{-48}$, 搜索量的 *P* 值为 $7.06*10^{-41}$ 远小于显著性水平 0.05, 说明两个自变量的回归系数显著。所以这个模型的预测能力是通过检验的。

表 7　多变量回归统计表

Table 7　Multivariate regression statistics

回归统计	
Multiple R	0.983899
R Square	0.968057
Adjusted R Square	0.967679
标准误差	592.7365
观测值	172

表 8　多变量方差分析表

Table 8　Multivariate variance analysis table

	df	*SS*	*MS*	*F*	Significance *F*
回归分析	2	1.8E+09	9E+08	2560.807	4.2E-127
残差	169	59375876	351336.5		
总计	171	1.86E+09			

表 9　多变量方差回归参数表

Table 9　Multivariate variance regression parameters table

	Coefficients	标准误差	t Stat	P-value	Lower 95%	Upper 95%	下限 95.0%	上限 95.0%
Intercept	81.36343	51.22201	1.588447	0.114054	–19.754	182.4808	–19.754	182.4808
X Variable 1	2.72E-21	1.32E-22	20.52834	8.98E-48	2.46E-21	2.98E-21	2.46E-21	2.98E-21
X Variable 2	106.1085	5.926864	17.90297	7.06E-41	94.40823	117.8087	94.40823	117.8087

综上, 我们以挖矿计算难度 x_1 和搜索量 x_2 作为自变量, 比特币区块链数字资产价格 *Y* 作为因变量得出多变量回归线性方程。即:

$$Y = 2.72*10^{-21}x_1^2 + 106.1085x_2 + 81.3634 + \mu$$

我们为回归方程添加了随机扰动项 μ, 其中随机扰动项包括挖矿计算难度和搜索量两个自变量中被忽略的因素影响、两个自变量观测值的观测误差影响、模型关系设定误差的影响和其他随机因素的影响。

3.4　其他区块链数字资产估值分析方法检验

受到首个区块链网络的启发与影响, 且由于其本身具有的开源性质, 其他的区块链数字资产层出不穷的地衍生出来。大部分基于公有链的或者是数字资产均是基于工作量证明(PoW)机制实现全网共识, 例如现如今发展较好且比较有代表性的莱特币区块链网络(Litecoin)和以太坊(Ethereum)均是基于工作量证明(PoW)机制进行挖矿。本节我们将通过对 Litecoin 和以太坊这两个当下具有代表性的区块链数字资产的价格进行分析, 验证上述归纳的资产估值分析方法是否同样适用于其他数字资产的分析。即首先根据主流的新闻媒体报道分析影响数字资产价格的主要依据, 其中包括安全性事件、国家政策、市场认可、每四年减半挖矿周期、分叉和其他数字资产产生等因素, 进而基于工作量证明(PoW)机制, 利用挖矿计算难度和数字资产关键字搜索量为自变量, 数字资产价格作为因变量, 分析自因变量之间的回归关系的方法。

通过首个区块链数字资产的启发, 衍生出来了一种新型的数字资产, 叫作莱特币(Litecoin)。它可以使用户即时付款给世界上的任何人。它与首个区块链网络具有相似的技术原理, 但与之前相比不同的是, 第一, 莱特币区块链网络平均 2.5 分钟就可以处理一个块, 快于处理速度为大约 10 分钟的比特币区块链网络 4 倍, 所以它具有更高效的交易速度; 第二, 莱特币区块链网络预计总量为 8400 万个, 几乎是首个区块链数字资产的四倍; 第三, 其在工作量证明(PoW)算法中运用了由 Colin Percival 提出的 scrypt 加密算法, 使得此数字资产的挖掘更为容易, 即挖矿计算难度小[31]。

根据之前对基于 PoW 机制的区块链数字资产估值分析, 我们知道影响其价格的主要因素为挖矿成本、安全性、国家政策、市场认可程度、四年挖矿减半周期、分叉及其它数字资产出现等因素。我们将挖矿计算难度和数字资产关键字搜索量作为自变量, 以挖矿难度平方和搜索量作为检测因子, 将数字资产价格作为因变量进行多变量回归分析检测。得出挖矿难度和搜索量与该数字资产价格具有显著的线性关系, 并得到基于 PoW 机制的区块链数字资产的多元线性回归拟合方程。同理, 我们选取 Investing.com 提供的莱特币区块链网络价格历史数据和“比特范”提供的历史挖矿计算难度数据, 对 2016 年 8 月 28 日到 2018 年 1 月 14 日这段时间进行分析。数据是以周为单位的, 将挖矿难度和‘Litecoin’搜索量(以周为周期, 已标准化 0-100 数值比例)作为自变量, 以挖矿难度平方和搜索量作为检测因子, 价格作为因变量进行多变量线性回归检测, 证明上一节归纳的区块链数字资产估值的分析方法是否适用于其他数字资产价格分析。

由表 10 可知, 相关系数 *Multiple R* 等于 0.9473 表明自变量挖矿难度平方和搜索量与因变量价格之间正相关程度很高。可决系数 *R Square*, 等于 0.8974, 说明挖矿计算难度平方和搜索量可以说明价格的 89.74%, 拟合效果佳。调整 *R* 平方判定系数 *Adjusted R Square*, 其值等于 0.8944, 说明两个自变量能说明因变量价格的 89.44%, 价格的 10.56%要由其他因素来解释。表 11 表示通过 *F* 显著性统计量, 即 *Significance F* 来判定价格与挖矿计算难度平方和搜索量回归模型的回归效果, 分析的 *P* 值等于 $2.5*10^{-35}$, 远小于显著性水平 0.05, 所以此多变量回归模型的回归效果显著。由表 12 可知, 挖矿计算难度平方的 *P* 值为 $1.54*10^{-26}$, 搜索量的 *P* 值为 $9.5*10^{-5}$, 均远小于显著性水平 0.05, 说明回归系数显著。由此得出结论本文分析归纳的区块链数字资产估值的分析方法适用于莱特币区块链数字资产价格分析。

表 10 多变量回归统计表

Table 10 Multivariate regression statistics

回归统计	
Multiple R	0.947286
R Square	0.897352
Adjusted R Square	0.894419
标准误差	22.14261
观测值	73

表 11 多变量方差分析表

Table 11 Multivariate variance analysis table

	df	*SS*	*MS*	*F*	Significance *F*
回归分析	2	300031	150015.5	305.9697	2.5E-35
残差	70	34320.68	490.2954		
总计	72	334351.7			

表 12 多变量方差回归参数表

Table 12 Multivariate variance regression parameters table

	Coefficients	标准误差	t Stat	P-value	Lower 95%	Upper 95%	下限 95.0%	上限 95.0%
Intercept	18.36413	2.863315	6.413589	1.44E-08	12.65342	24.07483	12.65342	24.07483
X Variable 1	1.74E-11	1.02E-12	16.9909	1.54E-26	1.53E-11	1.94E-11	1.53E-11	1.94E-11
X Variable 2	0.95038	0.229479	4.141466	9.5E-05	0.492698	1.408061	0.492698	1.408061

标志着区块链 2.0 时代的以太坊(Ethereum)将区块链技术引入到了一个全新的智能合约领域。以太坊通过一套图灵完备的脚本语言(EthereumVirtual Machinecode, 简称 EVM), 可以使用户在其之上搭建应用[32]。以太坊也是基于工作量证明(PoW)机制, 可以在区块链上实现应用程序的上传和执行, 而且对程序的有效执行起到了保障作用, 即实现了智能合约功能。以太坊可以触及到多种金融行业领域的应用, 例如, 资产交易、众筹、借贷(P2P)以及保险等等方面。以太坊其实是一种基于信任的区块链技术, 在不需要权威可信任节点背书的情况下, 全网可以达到共识, 通过智能合约执行各种事务, 减少了人

为的中间参与风险与成本[33]。

根据之前对基于 PoW 机制的区块链数字资产价格分析, 我们知道影响区块链数字资产价格的主要因素为挖矿成本、安全性、国家政策、市场认可程度、四年挖矿减半周期、分叉及其他数字资产出现等因素。我们将挖矿计算难度和该资产搜索量作为自变量, 以挖矿难度平方和搜索量作为检测因子, 将数字资产价格作为因变量进行多变量回归分析检测。得出挖矿难度和搜索量与相应数字资产价格具有显著的线性关系, 并可以通过回归分析得到有关数字资产价格的多元线性回归方程。同理, 我们选取 Investing.com 提供的以太坊价格历史数据和“etherchain.org”提供的历史挖矿计算难度数据, 对 2016 年 3 月 1 日到 2018 年 1 月 21 日这段时间进行分析。数据是以周为单位的, 将挖矿难度和‘ETH’搜索量(以周为周期, 已标准化 0-100 数值比例)作为自变量, 以挖矿难度平方和搜索量作为检测因子, 以太坊区块链网络价格作为因变量进行多变量线性回归检测分析, 证明上一节归纳的区块链数字资产估值的分析方法是否适用于其它数字资产价格分析。

由表 13 可知, 相关系数 *Multiple R* 等于 0.9345 表明自变量挖矿难度平方和搜索量与因变量以太坊价格之间相关程度很高, 且呈正比例相关。可决系数 *R Square*, 等于 0.8733, 说明挖矿计算难度平方和搜索量可以说明价格的 87.33%, 拟合效果较好。调整 *R* 平方判定系数 *Adjusted R Square*, 其值等于 0.8706, 说明两个自变量能说明因变量价格的 87.06%, 价格的 12.94%要由其他因素来解释。表 14 表示通过 *F* 显著性统计量, 即 *Significance F* 来判定价格与挖矿计算难度平方和搜索量回归模型的回归效果, 分析的 *P* 值等于 $2.44*10^{-43}$, 远小于显著性水平 0.05, 所以关于以太坊的多变量回归模型的回归效果显著。由表 15 可知, 挖矿计算难度平方的 *P* 值为 $2.74*10^{-7}$, 搜索量的 *P* 值为 $3.81*10^{-33}$, 均远小于显著性水平 0.05, 说明回归系数显著。由此得出结论本文分析归纳的区块链数字资产估值的分析方法适用于以太坊区块链数字资产价格分析。

表 13 多变量回归统计表

Table 13 Multivariate regression statistics

回归统计	
Multiple R	0.93449
R Square	0.873271
Adjusted R Square	0.870603
标准误差	89.32411
观测值	98

表 14 多变量方差分析表

Table 14 Multivariate variance analysis table

	df	*SS*	*MS*	*F*	Significance *F*
回归分析	2	5223188	2611594	327.3168	2.44E-43
残差	95	757985.7	7978.797		
总计	97	5981174			

表 15 多变量方差回归参数表

Table 15 Multivariate variance regression parameters table

	Coefficients	标准误差	t Stat	P-value	Lower 95%	Upper 95%	下限 95.0%	上限 95.0%
Intercept	–144.508	15.56299	–9.28537	5.57E-15	–175.404	–113.612	–175.404	–113.612
X Variable 1	2.76E-29	4.98E-30	5.535591	2.74E-07	1.77E-29	3.75E-29	1.77E-29	3.75E-29
X Variable 2	10.6053	0.575219	18.437	3.81E-33	9.463352	11.74726	9.463352	11.74726

4 小结

传统的法定货币(纸币)的价值所在来源于国家的信用背书, 通过国家信用解决不信任问题, 然而区块链数字资产由于其去中心化的机制, 没有第三方信用背书, 但其价值是的确存在的。首先基于 PoW 机制的区块链数字资产的基本价值来源于其挖矿价值, 其中包括矿机投入费用、消耗电量和人工费用, 成本保证了区块链数字资产的基本价值, 可以作为区块链数字资产估值的下限。其次, 对于黄金来说, 除了其基本的成本价值, 黄金的价值还建立在公众对黄金的共识认可程度, 并且难以打破, 类比到区块链数字资产的价值, 随着区块链数字资产市场的逐渐庞大和逐渐形成的用户系统, 人们对于区块链数字资产的共识价值逐步加深。

综合文章, 对于区块链数字资产价格估计的分析, 我们应该结合“人类行为学”和“实证主义”的方式, 首先根据主流的新闻媒体报道分析影响区块链数字资产价格的主要依据, 其中包括安全性事件、国家政策、市场认可、每四年减半挖矿周期、分叉和其它数字资产等因素, 进而基于工作量证明(PoW)机制, 利用挖矿计算难度和关键字搜索量为自变量。根据文中提出的分析方法对区块链数字资产的价格进行预测判断, 全面综合的对区块链数字资产的价

格走势进行分析, 理智投资。

本文以首个区块链数字资产为主要研究对象, 通过对其获取方式和发展历程全面深入的调研, 提出了通过以“人类行为学”和“实证主义”相结合的方式, 对区块链数字资产估值分析的方法。旨在让更多的人理智走进区块链数字资产、在这个如过山车般行情的投资市场中走的更远更踏实。

参考文献

[1] Jia Liping. “Theory, Practice and Impact of Bitcoin.” International Finance vol. 12, pp. 14-25, 2013.
(贾丽平. “比特币的理论、实践与影响.” *国际金融研究* 2013, 12: 14-25.)

[2] Luo Qiang, and Zhang Rui. “Bitcoin.”Machinery Industry Press, 2014.
(罗强, 张睿. 比特币. 机械工业出版社, 2014.)

[3] Sun Jiayin, “Study on the Nature and Pricing and Regulation of Bitcoins [Master Dissertation] ”, Shanghai Jiao Tong University, 2014.
(孙佳音, 比特币的性质、定价与监管研究[硕士学位论文], 上海交通大学, 2014.)

[4] “Bitcoin (virtual currency)” Sogou, http://baike.sogou.com/v44342252.htm?fromTitle=%E6%AF%94%E7%89%B9%E5%B8%81, January.2018.
(比特币(虚拟货币)-搜狗百科 http://baike.sogou.com/v44342252.htm?fromTitle=%E6%AF%94%E7%89%B9%E5%B8%81, January. 2018.)

[5] X Li and C A Wang, “The technology and economic determinantsof cryptocurrency exchange rates,” Elsevier Science Publishers, 2017.

[6] “Talk about bitcoin price analysis method, how to carry on theappropriate bitcoin price analysis,”play the currency Family,http://www.wanbizu.com/baike/201407291143.html,January, 2018.
(“谈比特币价格分析方法,如何进行恰当的比特币价格分析”玩币,http://www.wanbizu.com/baike/201407291143.html, January, 2018.)

[7] J.A. Feigenbaum, P.G.O. Freund, “Discrete scale invariance in stock markets before crashes,” *International Journal of Modern Physics B*, vol. 10, pp. 3737-3745, 1996.

[8] Bariviera A F, Basgall M J and Hasperué W, “Some stylized facts of the Bitcoin market,” *Physica A Statistical Mechanics & Its Applications*, vol. 484, pp. 82-90, 2017.

[9] Dyhrberg A H. “Bitcoin, gold and the dollar – A GARCH volatility analysis,” *Finance Research Letters*, vol. 16, pp. 85-92, 2015.

[10] Castro M, Liskov B. “Practical byzantine fault tolerance and proactive recovery,” in Proc. ACM Symp. Computer Systems (CS’20),pp. 398-461, 2002.

[11] Fan Jie, Yi Le-Tian and Shu Ji-Wu, “Research on the technologies of Byzantine system,” Journal of Software, vol.24, no. 6, pp. 1346-1360 (in Chinese), 2013.
(范捷, 易乐天, 舒继武. “拜占庭系统技术研究综述”, *软件学报*, 24(2013):1346-1360.)

[12] Bentov I, Lee C, Mizrahi A and Rosenfeld M, “Proof of activity: extending Bitcoin’s proof of work via proof of stake,” in Proc. ACM Symp, SIGMETRICS Performance Evaluation Review, (SIGMETRICS’42), pp. 34-37, 2014.

[13] “Consensus in Bitcoin: one system, many models,” https://freedom-to-tinker.com/blog/randomwalker/consensus-in-bitcoin-one-system-many-models/, December, 2014.

[14] Huberman G, Leshno J D and Moallemi C C, “Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System,” Social Science Electronic Publishing, 2017.

[15] Chen Hao, “Economic Analysis of Bitcoin [Master Dissertation],” Zhejiang University, 2015.
(陈豪.比特币的经济学分析[硕士学位论文]. 浙江大学, 2015.)

[16] “The United Kingdom may be bitcoin as legal currency,” inance Tencent, http://finance.qq.com/a/20140810/010218.htm, January, 2018.
(“英国或将比特币列为合法货币,” 财经腾讯网 ,http://finance.qq.com/a/20140810/010218.htm, January, 2018.)

[17] “Bitcoin market and investment bank's lurking funds,” play currency family, http://www.wanbizu.com/jingyan/201606127038.html, January, 2018.
(“比特币盘面与投行潜伏资金,” 玩币族, http://www.wanbizu.com/jingyan/201606127038.html, January, 2018.)

[18] “The European Court of Justice ruled that Bitcoin transactions should be tax-free and that opaque transactions lead to worries,” Xinhua Website, http://news.xinhuanet.com/world/2015-10/24/c_128351420.htm, January, 2018.
(“欧洲法院裁定比特币交易免税, 不透明交易引担忧,” 新华网, http://news.xinhuanet.com/world/2015-10/24/c_128351420.htm, January, 2018.)

[19] “10 coins community events in 2016!” https://www.btctrade.com/bitcoin/1323.html, January, 2018.
(“2016 年 10 大币圈事件！” https://www.btctrade.com/bitcoin/1323.html, January, 2018.)

[20] “How bitcoin is crazy in 2017? Analysis ofroller coaster-like market and heavy events,” Huitong website, http://finance.sina.com.cn/money/forex/hbfx/2017-12-31/doc-ifyqchnr7874160.shtml, January, 2018.
(“比特币 2017 年如何疯狂？细数过山车行情及重磅事件,”汇通网 http://finance.sina.com.cn/money/forex/hbfx/2017-12-31/doc-ifyqchnr7874160.shtml, January, 2018.)

[21] “regulation of multiple countries become more stringent, bitcoin plummeted 25% within a day,” Foreign media, http://www.cankaoxiaoxi.com/finance/20180118/2252326.shtml, January, 2018.
(“多国监管收紧,比特币一天内暴跌25%,” 外媒, http://www.cankaoxiaoxi.com/finance/20180118/2252326.shtml, January, 2018.)

[22] “China's Information Security Comprehensive Report for the First Half of 2013,” Rising Website, http://www.rising.com.cn/about/news/rising/2013-07-10/14047_3.html, January, 2018.
(“2013 年上半年中国信息安全综合报告,”瑞星网, http://www.rising.com.cn/about/news/rising/2013-07-10/14047_3.html, January, 2018.)

[23] “How does the hard fork affect the value of bitcoin storage?” Babbitt, serving blockchain innovators, http://www.8btc.com/hardfork-affect-bitcoins-usefulness-store-value, January, 2018.
(“硬分叉会如何影响比特币的价值储存有用性?” 巴比特,服务于区

块链创新者, http://www.8btc.com/hard-fork-affect-bitcoins-usefulness-store-value, January, 2018.)

[24] Tang Qi. "Mettkafe's Law in Network Economy and Its Applications." Journal of Wuxi Institute of Technology, vol. 5, no. 3, pp.78-80, 2006.
(唐麒. "浅谈网络经济中梅特卡夫法则及其应用." *无锡职业技术学院学报*, 5(2006):78-80.)

[25] Alabi K, "Digital blockchain networks appear to be following metcalfe's law, " Electronic Commerce Research & Applications,2017.

[26] Chatterjee., "Case Study Regression Analysis, " Machinery Industry Press, 2013.
(查特吉, "例解回归分析," 机械工业出版社, 2013.)

[27] Zhang Shanfeng, "Regression analysis of financial projections using EXCEL, "Office Automation: Integrated, vol. 10, pp. 44-45, 2010.
(张山风, "利用 EXCEL 进行财务预测的回归分析, "*办公自动化: 综合版* , 10(2010):44-45。)

[28] Balcilar M, Bouri E and Gupta R, "Can volume predict Bitcoin returns and volatility? A quantiles-based approach, " Economic Modelling, vol. 64, pp. 74-81, 2017.

[29] Hayes A S, "Cryptocurrency value formation: An empirical study-leading to a cost of production model for valuing bitcoin, "Telematics& Informatics, 2016.

[30] Ling Qing, "Technical Principle and Economic Analysis of Bitcoins [Master Dissertation], "Fudan University, 2014.
(凌清, 比特币的技术原理与经济学分析[硕士学位论文], 复旦大学, 2014.)

[31] He Hongliang, "Litecoin and Scrypt Algorithm, "Economic Practice, 2016.
(何洪亮, "莱特币与 Scrypt 算法, " *经贸实践*, 2016.)

[32] "Ethereum"Baidu Encyclopedia, https://baike.baidu.com/item/%E4%BB%A5%E5%A4%AA%E5%9D%8A/20865117?fr=aladdin, January, 2018.
("以太坊"百度百科, https://baike.baidu.com/item/%E4%BB%A5%E5%A4%AA%E5%9D%8A/20865117?fr=aladdin, January, 2018.)

[33] Lee Hyuk, "A Tentative Approach to Ethereum Based on Blockchain 2.0." China Financial Computer, vol. 6, pp.57-60, 2017.
(李赫等, "基于区块链 2.0 的以太坊初探," *中国金融电脑* 6 (2017):57-60.)

王帅 2017 年在北京林业大学网络工程专业获得本科学位。现在中国人民大学软件工程专业攻读硕士学位。研究领域为信息安全、区块链、数字货币。Email: 944909511@qq.com

陈晋川 现任中国人民大学信息学院副教授,主要研究领域为分布式数据管理技术以及区块链技术。Email: jcchen@ruc.edu.cn

张诗童 2017 年在南开大学数学科学学院应用数学专业获得本科学位。现在中国人民大学软件工程专业攻读硕士学位。研究领域为信息安全、区块链、数字货币。Email: 644254041@qq.com

秦波 现任中国人民大学信息学院讲师, 主要研究领域为云计算安全、信息网络安全、数据安全与密码学等。Email: bo.qin@ruc.edu.cn

姬思宇 现在于中国人民大学信息学院攻读信息安全学士学位。研究领域为信息安全、区块链、数字货币。Email: jisiyu96@126.com