



中国石油大学 (华东)
CHINA UNIVERSITY OF PETROLEUM

《计算科学导论》课程总结报告

姓 名 周国斌

学 号 1907010312

专业班级 计科 1903

学 院 计算机科学与技术学院

课程认识	问题思考	格式规范	IT 工具	Latex 附加	总分	评阅教师
30%	30%	20%	20%	10%		

1 引言

当今世界已进入信息化时代，计算机产业自产生至今，已与我们的生活有了千丝万缕的联系，成为目前世界最关注的行业之一，它的飞速发展和全球化的普及，使人们的生活发生了翻天覆地的变化，在本次报告中，我们将对计算机科学导论这门课程进行深入的探讨，对计算机大产业的一些分支产业进一步研究，本次报告的方向主要围绕区块链、比特币、挖矿展开，对于虚拟货币交易机制的安全性、比特币目前的发展情况和未来前景，以及挖矿行为对于社会发展的意义，都会在此次报告中一一进行探讨。也希望通过本次的研究报告，使我对计算机科学导论这门课程有更深一步的了解，让我对计算机这门行业的发展形势有更准确的摸索，把握世界发展的动脉。

2 对计算机科学导论这门课程的认识、体会

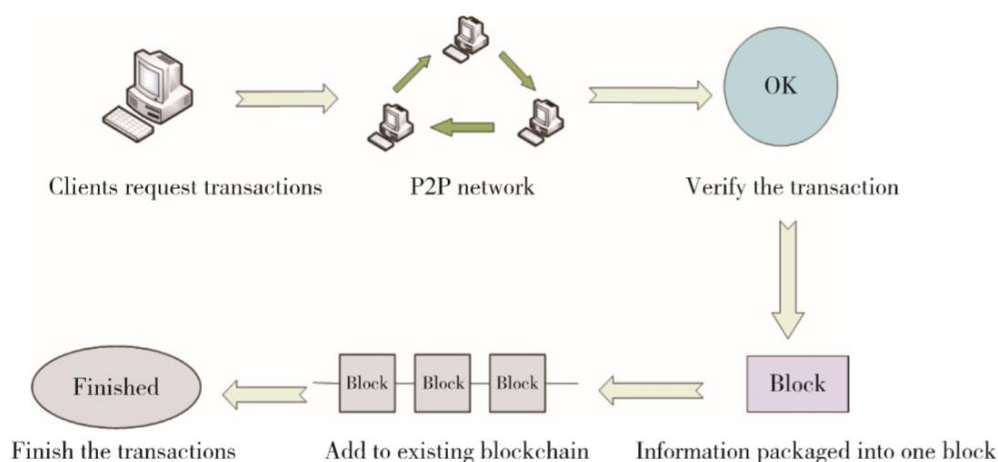
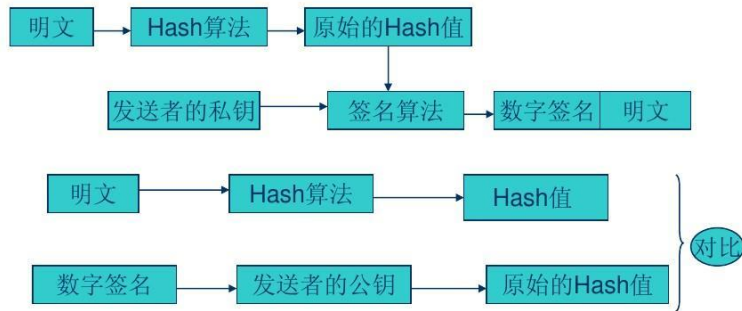


图 1 比特币交易过程

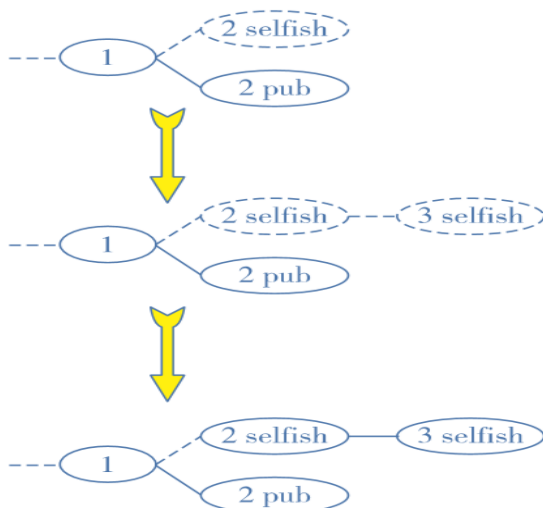
Fig. 1 Bitcoin transaction process



数字签名的流程图



BTC/CNY TOPBTC概览



对于挖矿行为的研究初衷

对于挖矿这个课题，我们小组一开始是由我先选择了这个课题，因为对于这个课题涉及到的区块链、BTC、挖矿等概念我之前都有了解过，并希望通过这次研究，能是我们小组对于这方面的知识领域都有进一步的认识，后来我们通过查找相关论文，比如江西财经大学的楼尧硕士的《加密货币币价决定与挖矿行为的探索性研究》，我们从他的论文中认识到区块链技术的一些实际应用，而 BTC 就是区块链技术应用的一个分支，BTC 是一种集合了加密计算、共识机制、点对点传输、分布式数据存储等已有计算机网络技术去中心化加密货币，BTC 出现后区块链技术作为比特币的底层技术才被广泛定义，可以说区块链技术脱胎于比特币，以至于后来到各个领域的应用。而挖矿作为 BTC 的一种现象，它的一些自身存在的问题以及它客观存在的对于社会发展的积极作用抑或是消极作用，都引得我们的深思。

关于挖矿、BTC 方面存在的问题，最主要的还是安全、利益分配问题，因为作为一种去中心化、P2P 网络技术，它的安全性饱受争议，缺少了中间机构的保障，单靠交易双方的信用作担保，显然有些天方夜谭，还有就是挖矿过程中共识机制的缺陷，在挖矿过程中产生的自私挖矿现象显然是一种非常不公平的牟利行为，攻击者通过隐藏区块的做法损害诚实矿工的利益来使自己利益最大化，这明显破坏了挖矿交易的平衡，这些我们在山东大学的韩建硕士的《比特币挖矿攻击及防御方案研究》中都做了相应了解，在后续的讨论中我们会详细阐述。最后我们想探讨的，还是对于这种炒虚拟货币的行为是否应该被视为一种合理的存在。

3 进一步的思考

在经过对于 BTC 和挖矿的系统化的了解后，我们总结出了如下几个方面的问题。第一，关于 BTC 的安全性问题，很多人可能会有所疑惑，觉得 BTC 这种虚拟货币，在 P2P 网络环境下，仅仅靠用户双方的信用制度，怎么能够维持下去呢？的确不少人觉得比特币缺少监管，市场经济波动大，风险高，而且靠着比特币交易的匿名性，使它成为一些犯罪集团的交易工具，任何地方只要有网络和基本的联网设备，都能进行交易，这也导致一些国家不认可 BTC 的交易合法性，我们国家就是禁止加密货币交易以及加密货币 ICO，并且也没有出台对口法规。当然，对于 BTC 的交易，也是存在一定安全性可言的，在《加密货币币价决定与挖矿行为的探索性研究》中就有提到“比特币的设计中每一个节点都拥有全部的交易账本信息，并且实时相互验证，如果攻击者想在这些账目中凭空创造或者掠夺本不属于自己的比特币，那么其他节点很难想相信并验证这一伪造账本，除非能成功说服所有节点，然而这种可能性概率极小。攻击者能做的只有抹除自己曾经付出的比特币，但这也不是轻易就能完成的。他必须设法将附带篡改账本的区块接入区块链主链，基于目前协议中规定等待 6 轮区块挖掘后都存在的交易方是确定的交易，又由于矿工会优先选择在最长的链上继续挖掘，因此攻击者必须快于主链挖掘到第 6 个区块，并接入主链。这种攻击成功的概率取决于攻击者算力在全球算力中的占比，占比越大成功概率越大，当攻击者占有算力超过全网算力的 50% 时，便可以随意篡改比特币的分布式账本的即时交易，比特币系统存在的这种风险被称为“51% 算力攻击”风险。”任何针对比特币的攻击方式都围绕算力争夺。为了争取挖矿奖励的矿商会通过增加挖矿设备和相互联合来增加自身算力占比。而算力过度集中于某个矿商的情况是危险的，因为掌握 51% 算力的一方具备篡改账本的能力，算力集中也意味着比特币去中心化的努力失败。预防攻击的方式是，一方面争取全网算力最大化，另一方面分散算力防止矿工联合。比特币拥有越大的全网总算力决定了其拥有更高的安全性。运用非对称加密技术也为比特币及挖矿提供了一定的安全保障。

第二是挖矿对于社会的作用及意义。我们现存的货币体系，包括中央银行和通胀，造成了世界上的许多苦难。富人越来越富，穷人越来越穷，因此我们需要一个不同的、更好的系统。我想我们可以做得更好。比特币就是一种可能，它具备彻底变革社会的潜力。比特币作为一种基于公众总账本和 P2P 通讯的货币，解决了整个货币系统的问题。建立在区块链之上的服务和应用极大地拓展了这些可能性。它们能让政府运行更加高效、透明，但问题是，政府并不希望变得更加透明高效。世界各地的政府和金融体系都是建立在幕后操纵、资助政客和决定法律的影响力中心。当前的货币体系正符合他们的利

益，扰乱这个货币体系就意味着扰乱政府。因此，比特币是非常政治化的。在这个基于全球分布式总账的支付系统，去中心化以及把“信任”从人转移到数学上，是解决货币问题的完美方法。现在我们把重心放到挖矿上，对于挖矿，可以说是一种炒币行为，放在金融层面，可以近似等同于炒股，而这种行为，与炒股一样，对于我们社会的科技发展，没有什么促进作用，只是矿工的一种赚钱方式罢了，所以对于这种高风险、积极影响小的运转模式，我个人是持反对态度的，毕竟作为一种高投入的投资模式，所带来的设备、电力损耗是不容小看的，甚至可能会有人投入全身家当去抄虚拟货币，可以说我们不能去助长这种风险偏高的行为。

第三是 **BTC** 市场与传统金融市场的联系及 **BTC** 的投资风险，从《From financial markets to Bitcoin markets: A fresh look at the contagion effect》中 “This article studies contagion effects between traditional financial markets, represented by five equity indices and the EUR, USD, GBP, and JPY centralized Bitcoin markets. We apply a regime switching skew-normal model of asset returns that distinguishes between linear and non-linear contagion and also structural breaks in the periods. We find significant contagion effects from financial to Bitcoin markets in terms of both correlation and co-skewness of market returns. Our results also indicate that during crisis periods, risk-averse investors tend to move away from risky Bitcoin markets towards safer financial markets.” 可以看出，**BTC** 市场与传统金融市场的联系并不小，如果我们要管理好 **BTC** 市场与传统金融市场，我们势必要下些功夫在管理的机制上。而在《News and subjective beliefs: A Bayesian approach to Bitcoin investments》中 “The use of crypto-currencies in financial applications is receiving increasing interest. This paper relies on a Bayesian framework that combines market-neutral information with subjective beliefs to show an application of how Bitcoin can be exploited to build diversified investment strategies. By means of an intuitive procedure based on the Black and Litterman model, I propose to relate portfolio construction with the role of news in generating investors’ subjective beliefs, which are computed according to market reactions occurred after similar announcement events in the recent past. To test this approach, the analysis refers to an extremely volatile market phase for Bitcoin such as the interval from mid-2017 to mid-2018. Results indicate that Bitcoin can contribute to improve the risk-adjusted performances of diversified portfolios and that investors’ subjective beliefs can help to interpret the fundamental drivers of crypto-currencies’ market behaviors. This approach may also stimulate the investigation of more sophisticated strategies built according to the relationships between news and investors’ personal views on Bitcoin market dynamics.” 中看出，**BTC** 市场是一种风险极高的投资领域，而炒币更是一种大风险的行为，对于社会的积极作用更是微乎其微，综上，我们不赞同这种益处低、风险高的金融方式。

第四是 **BTC** 和挖矿目前的发展情况以及未来的前景。**BTC** 一开始由中本聪设计出来的初衷是去中心化，是希望虚拟货币的交易没有政府部门的管控，但目前情况是，由于挖矿是根据算力来评判所得收入的，导致出现了一种情况是多名矿工联合挖矿，更有甚者，已经出现了专门的挖矿公司，这就形成了一种中心化的局面，**BTC** 市场经济由各大矿场主导，这种局面没有按照中本聪设计之初发展，这或许连中本聪自己都没有想到。根据《加密货币币价决定与挖矿行为的探索性研究》中提到“加密货币挖矿市场中，矿工们生产的是几乎无差别的算力，获得的也是价值相同的代币报酬。从长期来看挖矿市场更偏向于完全竞争市场。完全竞争市场的经济学定义是，不包含任何垄断因素的市场，市场上有大量的买卖者，每个厂商提供的商品都是完全同质的，所有资源具有完全流动性，市场信息也是完全的。但是在短期内，加密货币矿商面对的是不同的电力成本、不同的挖矿设备、不同的挖矿软件和不完全的市场信息，暂把比特币挖矿市场归为垄断竞争市场。”看来要达到真正的中心化，**BTC** 市场还任重道远。

第五是挖矿中的自私挖矿。自私挖矿是比较容易盈利的。这便给加密货币的研发者提出了新的难题。如果现行的共识机制不进行相应调整，比特币等加密货币会在未来面临更多攻击。目前 **BTC** 市场还面

面临着许多潜在的威胁攻击，我们必须真正解决好 BTC 市场的现有问题，做好防范，保障在收到攻击时控制好整体金融市场的稳定性。

4 总结


通过对于《计算科学导论》这门课程的深入学习，以及我们小组对于区块链、BTC、挖矿等方面的进一步研究，我们对于当今互联网行业的发展都有了更深层次的理解，计算机由数学发展而来，从萌芽阶段开始，经过许多学者对计算机理论的不断完善，才有了如今计算机事业的蓬勃发展，并且我相信，后人将会在前人的基础之上，对计算科学进行更深入的探索。对于挖矿方面而言，我们对于它所涉及的知识有了一定程度的认知，认识到区块链、BTC 存在的现实意义，即区块链技术对于我们生活的方方面面都有着举足轻重的影响，它推动了 IOT 的发展，促进了智能家居、身份管理、智能城市等领域的发展，推广区块链技术在我们社会的应用的的确是一件有价值的事，但对于炒币这类行为，我们是不应该推崇的，我们应该理性地看待这种现象，否则，将会不利于我们社会的发展，我们可以关于 BTC 的管理出台一些政策：比特币是去中心化的应用，致使监管方的天然缺位，任何导致币价波动的行为都不会受到约束。同时比特币在设计上没能消除矿工行为和币价间的不断放大的相互影响，近几年比特币价格大涨大落让它的潜在使用者望而却步，而投机者不断涌入又进一步加重了比特币价格的不稳定性。作为标榜社区治理的比特币系统期望能通过矿工和使用者间的协议来改变现状，因此建议比特币矿工可以在挖出新币后持有一段时间，并向市场公布持有的总数。矿工在一定时间内持有比特币可以有效防止矿工在获取短期利益后减少算力投入，也避免矿工对通过“51%算力攻击”获取短期回报，同时投资者会视全网总算力的稳定情况而决定是否持有比特币。矿工持有比特币实际上是对算力——币价双向影响波动引入负反馈，算力受外部因素扰动时矿工可以选择持有更多比特币稳定投资者情绪从而减少币价波动，币价受外部因素扰动时由于矿工持有部分比特币而不会轻易撤出算力从而减少算力的波动。于矿工本身而言比特币价格稳定使得其自身收益稳定，于投资者而言价格稳定的比特币可以更放心的持有，两方都能获得更高效用。严密监控防止金融风险，加强国际联管阻止非法交易。我国十三五规划提出在新常态下转变经济发展模式，由外放型传统制造业向创新型知识密集产业发展，变中国制造到中国创造。十三五的创新要求离不开对区块链技术的应用和开发，有关部门应当密切关注技术变革，有效促进区块链技术新成果的研发。但挖矿炒币这种现象是区块链一种对科学发展并无多大积极作用的，我们现在不仅现在要从其高风险的层面考虑，更要从其对于社会的作用方面考虑，如果人们只是一味的想靠 BTC 挖矿挣快钱，会引发全社会的科技发展的怠慢，于是乎，我们的职责，是引领区块链技术、BTC 等虚拟货币技术往良性的方向发展，把握好区块链、虚拟货币的发展动向。比特币在设计上有天然的内部不稳定性，这也是造成近年来现象级的币价暴涨又崩溃的原因。交易媒介、记账单位、储存价值被普遍归纳为货币所应具备的特性，币价剧烈波动的比特币显然不具备储存价值，因此本文认为比特币不能作为一种真正的货币存在。政策建议部分，一方面提出在比特币社区治理的范畴内引入矿工持有比特币的负反馈体系，可以有效防止币价和算力的双向扩散扰动，部分解决比特币价格不稳定的问题；另一方面提出国际联合共治，有效防范突发性币价波动对经济运行造成的负面影响和涉及比特币的非法交易的存在。虽然经过十年的发展，以比特币为代表的加密货币仍是一种新兴的网络技术，距离真正的货币应用还有很长的路要走。比特币在技术上要突破交易流量限制、51%算力攻击风险以及挖矿能耗过高等问题，监管上要建立基于国际联合共治的风险防范体系，才能利于经济运行。而经济学界对此类基于区块链技术的加密货币的理论体系也亟待完善，否则不能更好的解释和预测加密货币的本质和走向。

总体而言，我们的研究结果是支持区块链技术的发展的，而它在挖矿炒币方面的应用，我们并不提倡，无论什么计算机科学技术，我们都应该引领它向促进人类社会的发展方向发展，这是从事计算机行业工作者身上的一副重任。

5 附录

Github

github.com/CobainChou



Set status

CobainChou

Edit profile

Joined 11 hours ago

Overview Repositories 1 Projects 0 Packages 0 Stars 0 Followers 0 Following 0

Popular repositories

Batcave

3 contributions in the last year

Contribution settings

Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

ion

ted

i

Learn how we count contributions.

Less More

Contribution activity

2020

January 1, 2020

Created 1 commit in 1 repository

CobainChou/Batcave 1 commit

观察者


观 风闻

输入感兴趣的内容...

首页 话题 发帖

私信 提醒

用户头像



CobainChou

文章 0 回复 0 被回复 0 收藏 0 赞 0 关注

已发布 0 草稿箱 0

没有更多数据了

关注 0 粉丝 0

个性签名

性别: 男

生日: 保密

所在城市: 保密

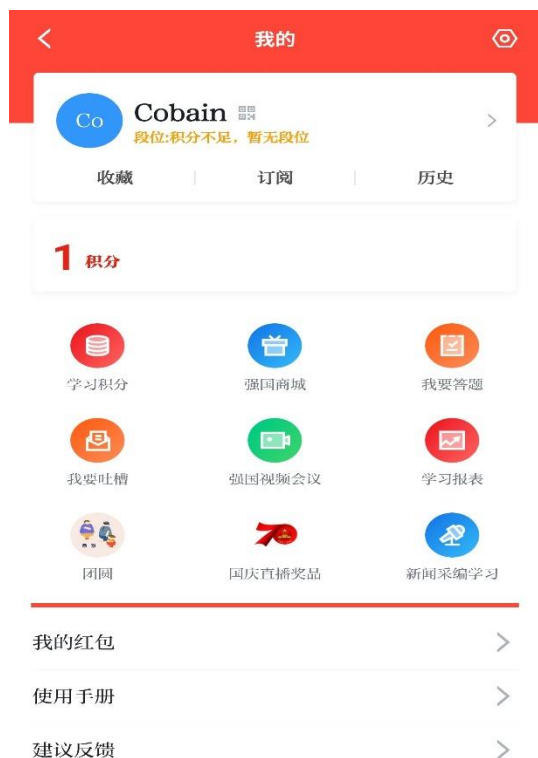
职业:

教育背景:

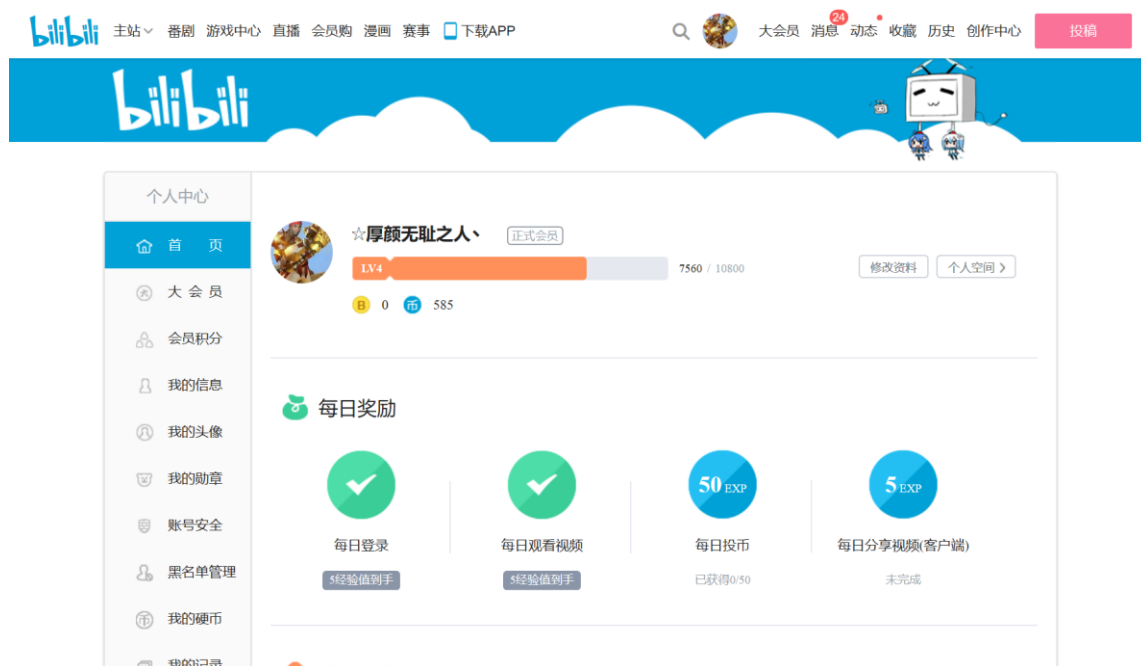
我的账户

修改个人信息

学习强国



哔哩哔哩



blog.csdn.net/qq_45790204

博客园

cnblogs.com/CobainChou/

小木虫

muchong.com/bbs/space.php?uid=20260566

9

参考文献

- 【1】 娄尧，俞国平，《加密货币币价决定与挖矿行为的探索性研究》，2019.6
- 【2】 洪 阳 ， 王 立 松 ， 葛 春 鹏 ， 《 比 特 币 平 台 挖 矿 策 略 及 其 收 益 综 述 》，
DOI:10. 13878/j. cnki. jnuist. 2019. 05. 004
- 【3】 韩建，徐秋亮，《比特币挖矿攻击及防御方案研究》，2019.5.20
- 【4】 Department of Management; Economics and Industrial Engineering of Politecnico di
Milano; Italy, News and subjective beliefs: A Bayesian approach to Bitcoin
investments
- 【5】 Roman Matkovskyy; Akanksha Jalan; Department of Finance and Accounting; Rennes
School of Business; 2 Rue Robert d' Arbrissel; 35000 Rennes; France; From financial
markets to Bitcoin markets: A fresh look at the contagion effect