

《计算科学导论》课程总结报告

|  |  |
| --- | --- |
| 姓 名 | 万亮杰 |
| 学 号 | 1907010305 |
| 专业班级 | 计科1903 |
| 学 院 | 计算机科学与技术学院 |

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

2020年1月3日

# **1 引言**

我们常把科学这两个字挂在嘴边，但到底什么是科学呢？百度百科给出的解释是“正确反映世界本质与规律的理论，包括正确的概念、命题、原理与理论体系；其对象是客观本质与客观规律，内容是科学本质与科学规律，形式是语言，包括自然语言与数学等人工语言。”我们是计算机专业的学生，计算机专业一直被理解成一个偏向于实际应用的专业，似乎并没有多少理论，好像与前面给出的科学的定义相距甚远，但这又是一门实实在在的科学，自有他的理论基础。与传统的“科学”不同，计算机科学的理论洋溢着现代的气息——一种现代人的意志所创造的的科学所独有的气息。他与人密不可分，他着眼于研究过程中的问题，理论知识转换为生产力的速度也极快，而且理论常常是由走的太超前的人反过来总结得出，最典型的当属“摩尔定理”。这与自然科学的研究大不相同，自然科学总是理论远超实际，理论知识转换为生产力的速度也非常缓慢，例如“从牛顿三定律被提出到第一次工业革命，之间间隔有70多年”，“法拉第发表研究成果到第二次工业革命也有三十几年。”综上所述，计算机的科学是与常规科学大不相同的，是值得单独拿出来说道说道的，计算科学导论课讲述的理论也是值得深究的。

# **2 对计算科学导论这门课程的认识、体会**

我在此之前也与大部分人一样，认为计算机就是摆弄电脑，并没有什么高深的理论，也不存在多少理论体系。学习完后我发现计算机是一门科学它是有漫长的发展史的，其间有无数人投入研究，才得以使计算机科学的理论体系趋于完善，使之成为一门真正的科学。

这是一门跨界的学科，它与数学联系十分紧密，与物理化学的关系也“相当好”，可以说计算机学科的理论基础来源于数学，计算机科学的发展离不开物理化学的长足进步。但反过来计算机的出现才使得科学研究的速度突飞猛进，数学研究彻底告别了没完没了的演算，物理化学的研究也逐渐精简，其实每一门学科都因计算机的出现而发生改变。计算机对于生活的改变就更大了，可以说现代世界没有一处可以离开计算机，计算机已经成了生活必须品，连去超市买一包口香糖也需要计算机的参与。

但这样重要的学科究竟有什么理论支撑呢？我想大部分人都说不出一个所以然来。计算科学导论这门课就是帮我们弄明白这个问题的课程。这门课程系统化的介绍了计算机的发展史，计算机的理论基础，计算机的意义与应用，详略的当地展现了一门科学的全貌，我不仅了解到了冯.诺依曼，图灵等人的功绩，我还了解到了如哥德尔，戴维.希尔伯特，罗素等人的一些趣闻，可以说这是一门内容十分丰富的课程。

同时这又是一门指导性很强的课程，它让人在学习的过程中渐渐找到发展方向，想向哪个方向发展需要什么样的知识它给的十分详细，它可能在实践性上并不强，但在理论指导上它却可以说是无懈可击。这对于偏向于实践的计算机学科来说这十分有意义，因为我们并不缺少实践性的知识，我们缺少的是理论的指导，我们需要知道的不是该怎么走路，我们需要知道的是走那一条路。

# **3 进一步的思考**

说完了对计导这门课程的认识，我来说说我的收获吧。首要的收获当然是自己的研究课题，我在此之前从未做过类似的事，我从未如此深究一件事，挖掘一样东西的内涵。这项任务让我这个总是不求甚解的人获益匪浅。

我选择了挖矿这个课题，因为我很早以前就听过这个名词，对它有一些了解，但随着课题研究的深入，我渐渐发现许多之前的见解实际上都跑偏了。实际上的挖矿要比我想的复杂得多，我已经在课上通过PPT进行了展示，但“曲有尽而意无穷”，任然有许多未讲的，我将再此补充说明，也算是展示一下计导课的收获。

首先说一说“挖矿是否有意义？”吧。要说挖矿的意义，我认为这就和鲁迅的那句经典名言一样——“意义本就是无所谓有无所谓无的，或许世上本没有路走的人多了也便成了路。”挖矿就是一个消耗大量资源来进行计算的过程，他算出的“东西”在比特币之外的领域有什么作用呢？答案是“一无是处”，并且它是一个不断重复计算的过程也谈不上对科学的发展带来贡献。一般人敢想象与比特币这样新兴的互联网相关产品有密切相关的挖矿实际上不需要任何文化水平就能干，许多文盲都可以买台矿机回来自己挖矿。这么一说好像挖矿果真是一无是处，但在比特币领域中情况又如何呢？答案是挖矿无可获缺！挖矿是维持比特币系统的基石，可以说比特币的发行流通没有一个环节离得开挖矿。是一批又一批矿工没日没夜的进行着运算让比特币可以实现上亿次的流通，也让比特币在这个过程中不断发展壮大。

那么说了这么多挖矿到底有没有用？我想这与比特币是否有用直接相关。中本聪提出的比特币是一个美好的构想，如果成形将会给世界带来巨大的福利。它可以让货币的发行和流通不在需要人的监管，完全自行运转。它可以让货币的流通变得无国界无障碍，在世界的任何一个角落都可以通过一种货币进行结算，也避免了由一国发行的货币独大，对其他国家产生不公平的现象。它更是描绘了一幅美好社会的蓝图，“人人挖矿，人人有币”的完全去中心化的美妙场景。

但现实是残酷的，有资本进驻的项目很快就会变味，事实是比特币价格大火后，无数人跟风涌入币圈，催生了许多乱象，比如“自私挖矿”，比如“中心化”，早已与中本聪的设想差了十万八千里。但希望是美好的，我们总保有币圈可以整顿好自己让这个原本美好的设想成真的希望。挖矿可能也如此，现在看不出作用，但没准假以时日，它会随比特币一块整顿好，为人造福，但如果是现在的市场又如何呢？

为了说明现在的市场，在此引用外国的两篇文献：

ABSTRACT:Abstract(#br)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.【1】

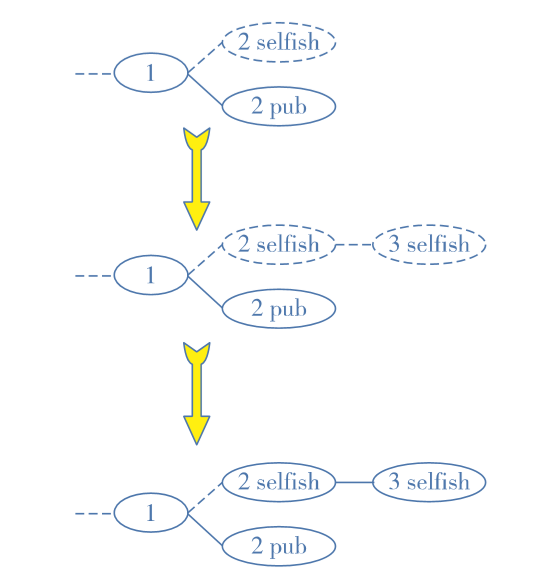
ABSTRACT:Abstract(#br)The use of crypto-currencies in financial applications is receiving increasing interest. This paper relies on a Bayesian framework that combines market-neutral information with subjective beliefs to show an application of how Bitcoin can be exploited to build diversified investment 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.【2】

可以看到现在的市场是任存在许多不足，比特币市场与主流金融市场挂钩，比特币的崩盘可能会影响到主流金融市场，主流金融市场的投资也会影响到比特币，而这两个系统本不该相通。总的来说比特币现在极不稳定，或者说一直都极不稳定，我们不建议去挖矿炒币，这是一个有着极高风险的事，而且不会对他人产生什么益处。

我刚才提到了“自私挖矿”，其实我在课上也提到了这个，但时间有限没有细讲，现在我再此补充。

在此我引用一段文献，“自私挖矿的概念是由康奈尔大学两位研究员 Eyal 和 Sirer 于 2013 年提出的，它是一种比特币的挖掘策略，是一种基于挖矿节点算力的竞争恶意节点依据“自私矿池”中区块的私密性，当一个“自私矿池”挖到新的区块，并没有根比特币共识协议立即公布该区块，从而让其余的诚实节点浪费算力去挖矿．面对区块链出现的情况，最长的那一条链被视作合法链当诚实链的长度即将接近自私链的长度时，自私矿工就会释放之前隐藏的区块从而迫使矿工的劳动作废在自私挖矿的情况下，自私矿工可以获得相对于其采用诚实挖矿 策略较多收益，而诚实矿工则会损失自己的合法收益”【3】

下面这张图就可以很好展示自私挖矿：



实际上它的原理相当复杂，但我们所要知道的就是这仅仅是挖矿的乱象之一。除此之外还有BWH攻击，FAW攻击等等等。

BWH攻击：区块截留攻击（ＢＷＨ 攻击 ）的概念 ， 攻击者加入目标标矿池只提交部分工作量证明，恶意扣留区块同时损害自己和矿池的收益。

FAW攻击：它是在区块截留攻击的基础上作了改进，攻击者发现有效区块不立即向矿池管 理者提交，当矿池外的其它矿工发现新区块时攻击者向矿池提交扣留的区块并向全网广播故意制造分叉以期望获得相应的区块收益很显然这一方法的收益是高于BＷＨ攻击的。【4】

最后我们来看一看各国法律对此的态度：

中国：

目前比特币在中国是被禁止交易和挖矿的，2017 年 9 月 4 日中国人民银行等七部委联合下发《关于防范代币发行融资风险的公告》，内容指出大量涌现的 ICO （首次代币发行）活动涉嫌非法，其严重扰乱了经济金融秩序，要求各类代币发行活动应当立即停止，国内数字货币交易也所被勒令关停。尽管目前国内己停止比特币场内交易，但风险仍然没有消失，境外交易所仍在进行人民币兑换业务，扰乱人民币金融与外汇市场；在重重监管下，场外交易与项目“出海”或将成为新的潜在风险，给后续监管进一步增加了难度。香港和台湾对加密货币实行严格监控，2018 年 4 月，中国台湾当局宣称，将推行基于现有反洗钱法规的加密货币监管规定。台湾地区法务部门发言人邱太三称，为避免比特币等加密货币成为洗钱方式，将对加密货币进行监控，预计于 2018 年 11 月底以前完善好相关法规。

日本：

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

欧盟：

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

美国：

虽然美国各州对加密货币监管规定都有不同，但近年来总体上趋于严格。美国商品期货交易委员会（CFTC）将比特币看做大宗商品，并宣称其监管对象包含洲际贸易中涉及比特币的操纵和诈骗等行为以及与比特币直接挂钩的大宗商品期货交易。【5】

# **4 总结**

总的来说，我们不建议挖矿不仅是从风险上考虑，更是从社会意义上考虑，现在的数字货币更像是一件半成品，不仅不会给社会带来多少益处，而且许多恶性的行为还会增加社会的不稳定因素，可能还需要很长时间的发展才能真正完善。现如今比特币市场常与金融界挂钩，或者说比特币市场已融入金融市场，许多的问题在滋生，各国对此态度也不尽相同。挖矿作为比特币最重要的一部分在各个地区反倒不断扩张，究其原因，可能是因为它的无门槛吧，它只需要买一台矿机，按照比特币平台的指导运行程序就行了，然后就可以碰运气等着比特币进账。比特币矿场在各国野蛮生长，各种大的矿场扎根在电力便宜的地区，美国的密西西比河周围的水电站，中国四川云南电站周边都有大的矿场。这样的结果就是导致比特币越来越中心化，就比如中国的算力已经占到世界的70%，也就是说世界上70%的比特币都是由中国发行，而我们知道比特币的算力达到51%就可以影响整个比特币市场，所以现在的市场还和中本聪设想的一致吗？答案当然是否定。越来越多的币集中在少数人手中，不断有人进驻比特币市场炒币导致币值不稳，矿难时有发生，有人甚至说“比特币价格大起大落才正常”，这是什么样畸形的市场？所以，对于以比特币为首的数字货币，大家不要过于狂热，最好只是把它当成区块链技术的一项应用，对此有所了解就行，但也不要完全否定它，毕竟希望是有的，它也可以说是一项发展好了就可以造福于社会的项目，我们可能还是要保持审慎的态度，理智地对待它。

# **5 附录**

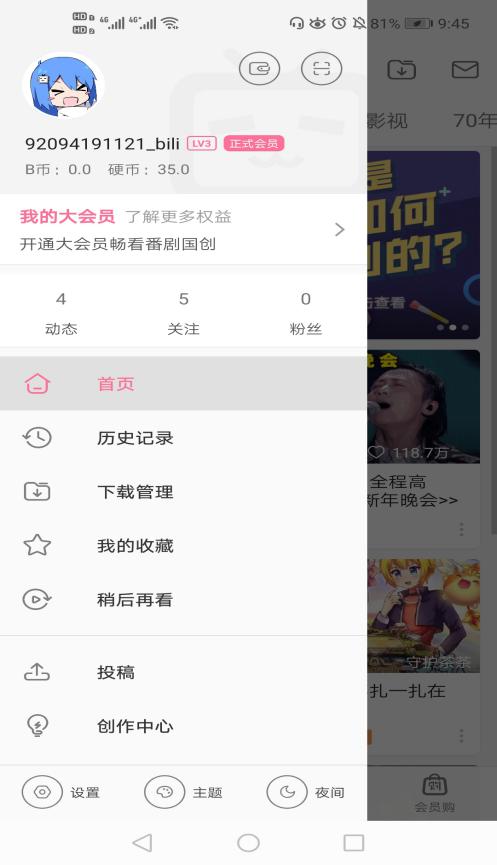
## **观察者**



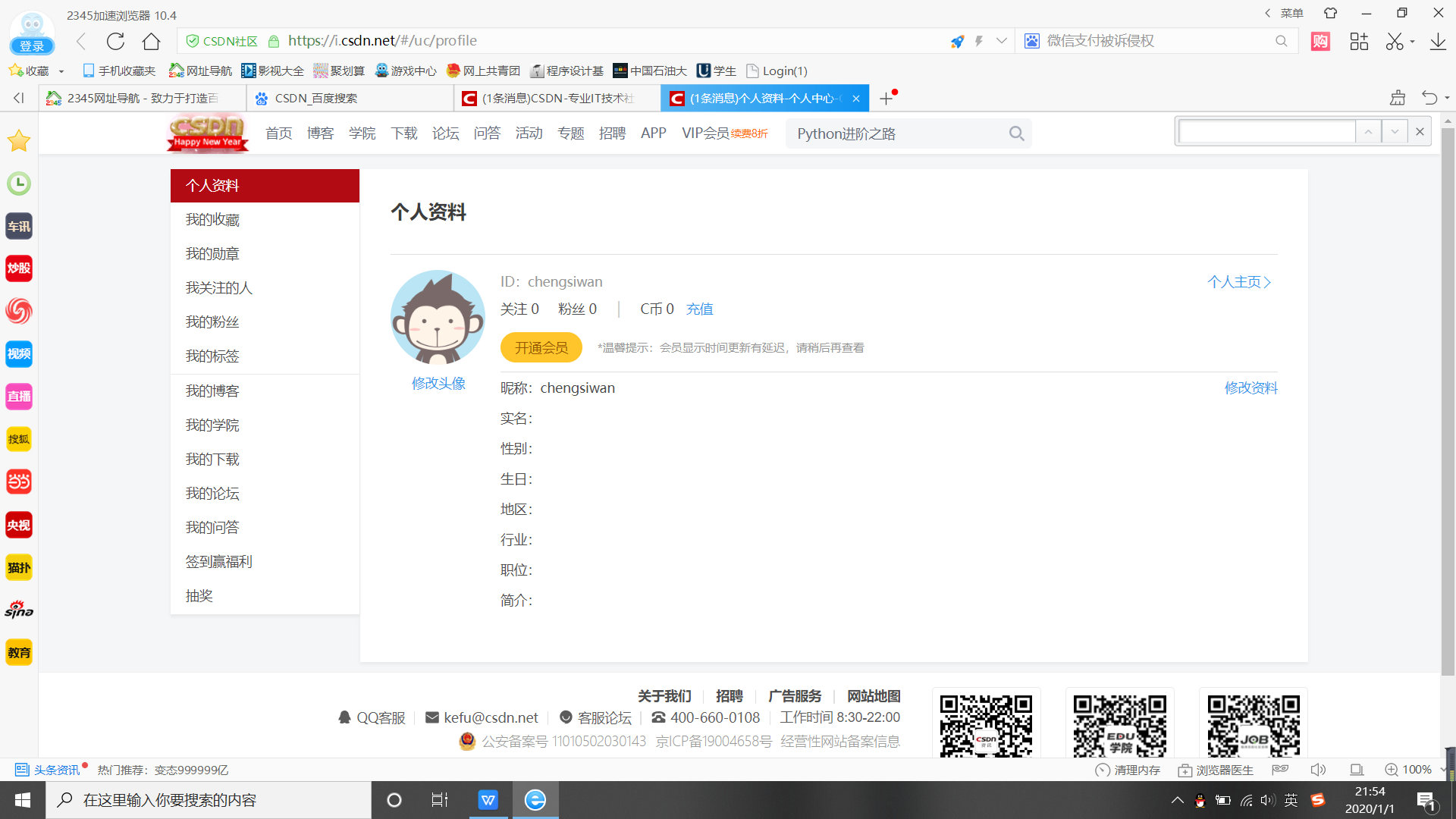
## **学习强国**



## **哔哩哔哩**



## **CSDN**



## **博客园**



## **小木虫**



# **参考文献**

# 【1】From financial markets to Bitcoin markets: A fresh look at the contagion effect

Roman Matkovskyy; Akanksha Jalan;

Department of Finance and Accounting; Rennes School of Business; 2 Rue Robert d’Arbrissel; 35000 Rennes; France;

【2】News and subjective beliefs: A Bayesian approach to Bitcoin investments

Andrea Flori;

Department of Management; Economics and Industrial Engineering of Politecnico di Milano; Italy

【3】《比特币平台挖矿策略及其收益综述》 洪阳 王立松 葛春鹏

【4】《比特币挖矿攻击及防御方案研究》 韩健

【5】《加密货币的币价决定于挖矿行为的探索性研究——以比特币为例》

楼尧