Bitcoin 合作式矿区挖矿研究

吕 楠
(上海海事大学 信息工程学院,上海 201306)

摘 要:比特币(Bitcoin)作为一种新型电子货币从创造之初就受到各领域学者的广泛关注,越来越的人投身到挖矿的行列。但是比特币本身的产生机制导致越多人参与,比特币产出的效率就越低。大部分比特币产出都集中在少部分的专业挖矿组织手中,个人参与者回报率极低。为了解决挖矿产出不平衡、回报率低的问题,一种合作式矿区挖矿模型通过有效整合个人参与者的计算能力,按小组形式进行合作挖矿,后将挖矿所得利益在组内重新分配,以提高个人挖矿回报率。

关键词:比特币;电子货币;矿区;挖矿
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2014)02-0039-03
doi:10.3969/j.issn.1673-629X.2014.02.009

Research on Bitcoin Cooperative Mining Area

LÜ Nan
(College of Information Engineering, Shanghai Maritime University, Shanghai 201306, China)

Abstract: Bitcoin, a new type of e-currency, has attracted researchers' attention in different fields since its birth. More and more people take part in mining activity. Due to the way of creating Bitcoin, the more people join, the lower efficiency they have. And the majority of new Bitcoins are produced by a small number of pro-mining-organizations. The rate of return of individual participants is much lower. In order to redress the imbalance of mining and raise the low rate, a cooperative mining area model, which is made of groups, is able to gather computing capability and re-assign the interests from mining, which ensures every single miner's rate could be raised.

Key words: Bitcoin; e-currency; mining area; mining

0 引 言

比特币(Bitcoin)作为一种新型 P2P 电子货币从创造之初就受到了各领域学者的广泛关注。从 2009 年 1 月至今,比特币的汇价涨幅接近 5 100 倍,今年 4 月 10 日更是涨到了 266 美元的历史高点。尽管在第二天比特币价格就回落到 155 美元,但是如此高的汇价仍然不断吸引着用户投入到比特币体系中。目前,越来越多的网站,如维基解密、Wordpress 等,表示支持比特币捐赠或交易。

比特币的概念最早在 2008 年由中本聪在文献[1]中提出。该论文将比特币描述成一种分布式的匿名数字货币。与传统虚拟货币不同的是,比特币系统不依赖于中央银行、政府的支持或者信用担保而独立存在。比特币管理交由 P2P 网络节点的分布式数据库,所有的发行、交易等都会被记录其中[2]。

比特币货币总量按照设定的速率逐步增加,并且增加速度逐渐降低。最初,比特币的预期生产速率为每十分钟 50 个,而这个速率被规定为每四年降低一半,故进入 2013 年后,产出速率已为 25 个。最终,货币总量将在 2140 年前后无限趋近于 2 100 万个,之后将不再增加。这种发行机制保证了比特币发行量不会因不良的货币政策而导致通货膨胀。值得一提的是,文献[3-4]论述了比特币的货币属性与经济学分析。

目前,获得比特币的方式主要有两种。第一种是在某些比特币交易网站通过其他货币买入,如 mtgox.com。与传统金融体系一样,这部分投资者通过比特币买入与卖出之间的汇率差获取利益。由于比特币汇价十分不稳定,并且没有涨停与跌停的限制,所以对于普通大众来说,风险过高。因此,更多的参与者主要通过第二种方式获取比特币:挖矿(Mining)。简单来说,挖矿就是计算机进行某项特定的数学计算过程,计算出结果就能够收到一定数量比特币的奖励,具体原

收稿日期:2013-05-02 **修回日期**:2013-08-08 **网络出版时间**:2013-11-29
基金项目:国家自然科学基金资助项目(61070145);中国博士后科学基金(20110490091);上海市教育委员会科研创新项目(12ZZ153)
作者简介:吕 楠(1989-),男,硕士研究生,研究方向为云计算与云存储。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20131129.0857.016.html

理将在下一节详述。参与挖矿的设备就被称为矿工(Miner)。因为比特币本身的机制限制,普通矿工获取比特币的效率非常低[5]。一份调查数据表明,在2010 年末,一台普通的个人电脑若要制造出 50 个比特币大约需要整整一年的时间。为了能够使普通矿工更有效率地参与比特币挖矿环节,文中论述一种合作式矿区挖矿模型,能够让每个参与者的劳动都能有效转化为比特币的价值。

1 Bitcoin 系统原理

为了能够更好地理解比特币系统原理,首先进行必要的名词解释[6]:

数据块链(Block Chain):数据块链就是记录了每一笔比特币交易的日志,由不断新产生的数据块链接而成。当新的数据块加入到块链中后就不会再被移走,数据块链储存了目前为止所有比特币的交易历史记录(目前约为 12 G)。

数据块(Block):每一笔比特币交易数据都会被打包成一个数据块。每一个数据块包含以下信息:数据块版本 version、上一个数据块的哈希值 prev_hash、将要写入交易记录的 hash 树值 merkle_root、更新时间 ntime、当前难度 nbits。目前,每产生一个数据块可以获得 25 个比特币。

挖矿(Mining):挖矿指通过计算一个“最小的哈希值”数学问题来产生数据块并且交易被最终确认的过程。数据块中包含的这些数据都将被用来计算这个 x 值[7]:

SHA256(SHA256(version+prev_hash+merkle_root+ntime+nbits+x))<difficult

difficult 的值会根据当前比特币的产出难度而调整,该值越小求出“最小的哈希值”就越困难,比特币的产出速度就越慢。由于哈希算法是单向不可逆的,所以想要计算 x 的值只能通过暴力搜索完成[8]。当计算出 x 的值之后客户端会向全系统广播该新数据块的信息。当至少有其他 6 个客户端在验证了该数据块合法性并接受之后,该笔交易就会被记入到数据块中,并且新产生 25 个比特币发送到某个特定地址[9]。

以上就是挖矿获得比特币的过程。由于比特币的产出速度已经被限定,所以在每个十分钟内要尽可能地先计算出有效数据块。换言之,当整个比特币系统中的计算能力越强,单一矿工计算出新数据块的难度就越大。所以在比特币系统中并不是参与者越多、全网计算能力越强产出比特币的效率就越高。恰恰相反,大部分的挖矿行为最终都成为了无效计算。为此,合作式的矿区挖矿模型能够集合零散的矿工计算能力,并且将之更加合理高效地利用起来。

2 合作式矿区挖矿

如前文所述,大部分的挖矿计算最终都是无效运算。因为挖矿的本质是一个暴力搜索求解哈希值的过程,而目标数据本身是无意义的。所以如果不能在第一时间计算出结果并且让其他客户端验证,那么这些计算都将是无效的。为了能够让这些劳动得到回报,合作式矿区挖矿应运而生。

所谓合作指的是加入每个矿区内的矿工共同计算一个数据块的哈希值,矿区的中央服务器负责将计算的区间指派给矿工。矿工不直接加入到比特币网络,而是将计算结果交由中央服务器,由中央服务器作为这些矿工的代表参与比特币网络。中央服务器将矿工的计算结果广播至比特币网络,验证通过后再把比特币返回给矿工,并从中收取一定的费用。简而言之,一个矿区内的所有矿工共同进行计算活动,矿区服务器按照劳动量将获取的比特币分派给各矿工。矿区中央服务器充当了劳资双方的媒介,并且从中抽取一定量的佣金。类似现实社会中“工头”这样的角色定位。最后资方的收入一次性首先交给工头,然后再由工头分发给每个矿工。对于矿工来说,他们并不需要知道工头将工钱存储在哪个银行,只需要向工头索要劳动所得即可。

图 1 给出了合作式矿区挖矿的原理图。

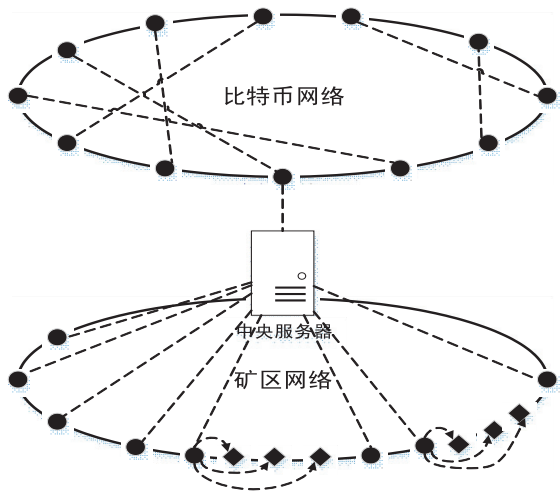

图 1 矿区网络与比特币网络

在矿区网络中,每个加入该矿区的矿工组成一个混合式的 P2P 网络。选取部分稳定节点(图中圆形节点)负责收取中央服务器指派的工作,将该工作指派给三个后继节点(图中菱形节点),由后继节点将计算结果交由圆形节点进行确认。这样的四个节点组成一个小组,圆形节点作为该小组的组长。组长将最后的确认结果,即该区间内是否能够算出新的数据块,交至中央服务器。如果该组算出了新的数据块,中央服务器就将结果广播至比特币网络进行确认。若该组未能

计算出新数据块,则从中央服务器领取新的任务。

图 2 抽象出了整个矿区的结构,最上层为矿区的中央服务器,主要负责任务的分解、指派与接收。第二层为较稳定的组长节点,负责共享任务以及后继节点结果的确认。下层为组员节点,主要负责小组中计算任务。

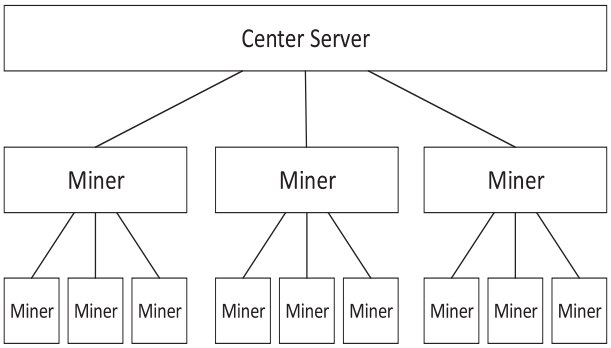

图 2　矿区结构

而图 3 给出了整个矿区的工作流程。首先,中央服务器从数据块链中得到上一个数据块、当前数据块版本等必要信息打包成一个任务(AID)。该任务会根据不同计算区间被分解成 n 个子任务(dAID),Divide(AID)。然后将每一个子任务分派给组长节点(hNID),Assign(hNID,dAID)。

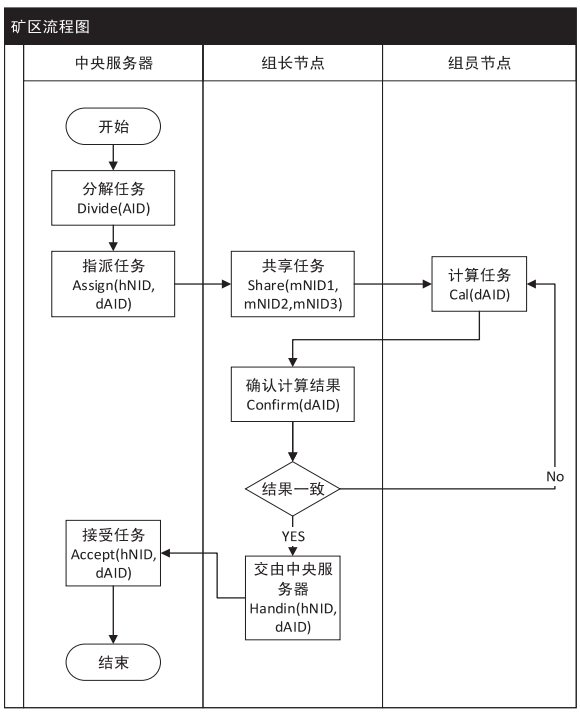

图 3　矿区工作流程

组长节点收到任务后共享给路由表中事先记录的后继节点(mNID),Share(mNID1,mNID2,mNID3)。这些组员节点收到分配的任务后开始进行挖矿操作 Cal(dAID)。计算完成后将结果返回给组长节点,由组长节点确认计算结果,Confirm(dAID)。三个结果不一致的话,再交由组员节点重新计算。若一致则上交至中央服务器,Handin(hNID,dAID)。中央服务器接受任务 Accept(hNID,dAID),将计算日志存入数据库,再将结果放入比特币系统检验。

如果该数据块在比特币系统中经过确认并且中央服务器获得了比特币,那么参与该数据块挖矿的矿工节点无论是否是计算出该数据块的小组都将得到相应的劳动分成。这么做的好处就是,只要参与挖矿的矿工都能够让自己的劳动变成有效劳动。不存在没有计算出数据块之前的计算就变成无效计算的情况。通过集体劳动让利益分配更平衡。

3　分析与改进

比特币从诞生到壮大一直受到学者的各种质疑,甚至有学者提出由于先前加入比特币体系的用户更加容易获得比特币,所以将之定义为一个彻头彻尾的“庞氏骗局”。实际上,比特币是一套建立在信用机制上的货币系统[10]。而合作式矿区挖矿模型中的矿区实际上充当了该矿区内“中央银行”,扮演了传统货币体系中国家信用的角色[11]。该服务器负责整个矿区的利益分配,如何保证中央服务器,亦即整个矿区的信用,如何吸引更多矿工的加入,是有一定难度的。同时,矿区的结构与比特币系统体系所提倡的去中心化理念也是相背的[12]。

第二,不同的矿工计算能力必然有所不同,如何保证计算能力相近的矿工节点被分配到一个小组中,从而避免了计算较快的节点需要等待较慢节点确认结果的可能。目前一种可行的解决思路是,每个矿工节点在加入矿区之前会首先进行能力测试,并将之记录下来。随后再将计算能力相近的节点组成一个小组。

第三,大部分个人用户参与挖矿主要是想利用计算机剩余能力进行闲时挖矿。比如,平时在办公时利用显卡的并行计算能力参与挖矿,只要不是运行大型的 3D 游戏或者对显卡运行有较高负载的程序,挖矿计算不会影响计算机的正常使用。那么如何保证这些节点能够稳定地在矿区中挖矿也是尚需解决的问题。

4　结束语

比特币作为一套基于密码学理论的新型货币体系有着较高的理论完整性与实际可操作性,正在被越来越多的投资者与企业所接受。但是由于比特币本身限定,随着时间的推移,更多矿工的加入,比特币产出的效率只会越来越低。大部分的计算都将成为无效计算。

合作式矿区挖矿形式通过计算能力的聚集与利益的重分配,在一定程度上解决了传统挖矿效率低的问

(下转第 45 页)

对于测试函数 3,迭代结束后,得到 200 个有效解,曲线如图 4 所示。

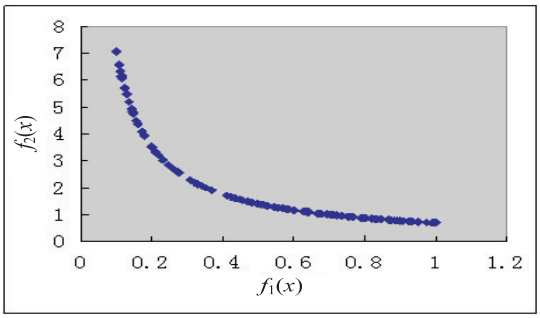

图 4　该算法对 Deb 函数求得的 Pareto 前端

5　结束语

文中的主要改进是全局最优值和个体最优值的选择策略与文献[1,12]中不同。由上面 3 个测试函数所得的曲线可以得出:改进的算法,可以正确地绘制出测试函数的曲线,与文献[1,12]相比,分布性和多样性都不差,说明文中的改进算法可行。

参考文献:

[1] Coello C A C, Pulido G T, Lechuga M S. Handling multiple objective with particle swarm optimization[J]. IEEE transaction on evolutionary computation,2004,8(3):256-279.

[2] Parsopouos K,Vrahatis M. Particle swarm optimization method in multiobjective problems[C]//Proc of 2002 ACM symposium on applied computing. Madrid:[s. n.],2002:603-607.

[3] Hu X,Eberhart R. Multiobjective optimization using dynamic neighborhood particle swarm optimization[C]//Proc of IEEE congress on evolutionary computation. Honoluu,Hawaii,USA:[s. n.],2002.

[4] Hu X, Eberhart R C, Shi Y. Particle swarm with extended memory for multiobjective optimization[C]//Proc of IEEE swarm intelligence symp. Indianapolies, IN, USA:[s. n.], 2003:193-197.

[5] Raquel C R,Naval P C. An effective use of crowding distance in multiobjective particle swarm optimization[C]//Proc of congress on evolutionary computation. Washington DC,USA: ACM Press,2005:257-264.

[6] Zitler E. Evolutionary algorithm for multiobjective optimization:Methods and application[D]. Zurich:Swiss Federal Institute of Technology,1999.

[7] 李　宁,邹　彤,孙德宝,等. 基于粒子群的多目标优化算法[J]. 计算机工程与应用,2005,41(23):43-46.

[8] Kennedy J,Eberhart R C. Particle swarm optimization[C]// Proceeding of 1995 IEEE international conference on natural networks. Piscataway,USA:[s. n.],1995:1942-1948.

[9] Schaffer J D. Multiple objective optimization with vector evaluated genetic algorithms[C]//Proc of the first int'l conf on genetic algorithms. Lawrence Erlbaum:[s. n.],1985:99-100.

[10] Kita H,Yabumoto Y,Mori N,et al. Multi-objective optimization by means of the thermo dynamical genetic algorithm [C]//Proc of parallel problem solving from nature-PPSN. Berlin,Germany:Springer-Verlag,1996:504-512.

[11] Deb K. Multi-objective genetic algorithms:Problem difficulties and construction of test problems[J]. Evolutionary computing, 1999,7:205-230.

[12] 张利彪,周春光,马　铭,等. 基于粒子群算法求解多目标优化问题[J]. 计算机研究与发展,2004,41(7):1286-1291.

(上接第 41 页)

题,至少让一些潜在的无效运算也能收获劳动成果,平均分配了劳动与利益的转化效率。但同时也存在一些诸如节点分组、信用保证等尚未解决的问题,需要依靠将来的工作来完善这一模型。

参考文献:

[1] Nakamoto S. Bitcoin:A peer-to-peer electronic cash system [EB/OL]. [2013-04]. http://bitcoin. org/bitcoin. pdf.

[2] Wikipedia. Bitcoin[EB/OL]. [2013-04]. https://en. wikipedia. org/wiki/Bitcoin.

[3] 洪蜀宁. 比特币:一种新型货币对金融体系的挑战[J]. 中国信用卡,2011(10):61-63.

[4] 崔屹东,郑晓彤. 对新型货币比特币的经济学分析[J]. 现代经济信息,2012(9):9-9.

[5] Barber S, Boyen X, Shi E, et al. Bitter to better - How to make bitcoin a better currency[C]//Proc of financial cryptography and data security. [s. l.]:[s. n.],2012:399-414.

[6] Vocabulary[EB/OL]. [2013-04]. http://bitcoin. org/en/vocabulary.

[7] 比特币是怎么生成的? [EB/OL]. [2013-04]. http://www. zhihu. com/question/20586821.

[8] 徐金福. Hash 函数 HAS-160 和 MD5 潜在威胁的分析[D]. 济南:山东大学,2007.

[9] 郑书雯,范　磊. 基于 P2P 网络 Bitcoin 虚拟货币的信用模型[J]. 信息安全与通信保密,2012(3):72-75.

[10] Reid F, Harrigan M. An analysis of anonymity in the bitcoin system[C]//Proc of security and privacy in social networks. [s. l.]:[s. n.],2013:197-223.

[11] 董　昕,周　海. 网络货币对中央银行的挑战[J]. 经济理论与经济管理,2001(7):21-25.

[12] 董　璐,唐潇霖. 虚拟货币的前景和风险[J]. 互联网周刊,2005(32):58-60.

Bitcoin合作式矿区挖矿研究

作者： 吕楠， Lü Nan
作者单位： 上海海事大学 信息工程学院,上海,201306
刊名： 计算机技术与发展
ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2014(2)