区块链典型挖矿算法分析*

张成成
(西华大学计算机与软件工程学院,四川成都 610039)

摘要:区块链挖矿不仅是系统发行新币的途径,还是保障区块链系统安全稳定运行最重要的基石。而挖矿算法在设计的时候为了保证区块链免受51%攻击,则挖矿算法就必须保证不同。不同的挖矿算法消耗的主要计算机资源也不同,本文选择比特币、以太坊和Filecoin的挖矿算法为例,它们分别以消耗CPU、内存和硬盘资源为主。通过分析这三种挖矿算法的主要过程,得出区块链安全性和资源浪费之间没有两全其美的解决方案。

关键词:区块链;共识机制;比特币;以太坊;Filecoin
中图分类号:TP309 **文献标识码**:A **文章编号**:1007-9416(2017)10-0108-03

自从2009年1月3日中本聪挖出比特币的创始区块以来,区块链成为一种新的解决去中心化节点的信息同步问题的方案,其创新性不断被人们所认知[1]。这其中,最关键的是以PoW(Proof of Work,工作量证明)共识机制为基础的公有链,这些系统普遍采用不同的挖矿算法来保障整个系统的安全稳定性。安全可信是区块链的基石,在此基础上人们才能谈论区块链的其它应用。而为了保障公有链的安全性,中本聪提出了挖矿的概念。挖矿是一种通过消耗计算机资源来提高恶意节点攻击网络成本的一种方式。挖矿的中心思想起源于Hashcash机制,该机制初次提出时主要用来阻止恶意用户向邮件服务器发送垃圾邮件[2]。所有的用户向邮件服务器发送邮件的时候都要在邮件中填充一些随机字符,然后计算邮件内容的哈希值,只有当计算结果小于设定的值的时候,该邮件才能满足邮件服务器的接受条件。在这个过程中,用户为了发送一个邮件,需要消耗一点时间来找出一个随机字符,使得整个邮件能被邮件服务器验证通过。无论是合法用户还是恶意用户,都无法绕开这个过程,这在一定程度上会影响正常用户的发送速度,但是影响微乎其微。而恶意用户为了大量发送垃圾邮件,就不得不大量计算满足条件的值,这无疑会增加恶意用户的攻击成本。这就是中本聪设计比特币的时候,需要矿工计算区块头的哈希值的原因。然而,恶意节点仍然可以事先花费大量的时间来计算满足条件的随机值,然后在极短的时间内发送给邮件服务器,从而完成DOS攻击。为了防止这种情况的发生,Hashcash要求用户在邮件内容中添加一条最近的消息,例如最近一天的博彩结果等。这样恶意节点的提前运算行为就被严格限制了。而在区块链挖矿过程中,矿工计算区块哈希值的时候也必须包含前一个区块头的哈希值。这样就能严格限制恶意节点提前进行挖矿的时间。区块链挖矿的目的也是为了保障系统的安全稳定运行,本质上以每个节点的资源消耗来换取系统的高度可靠性。

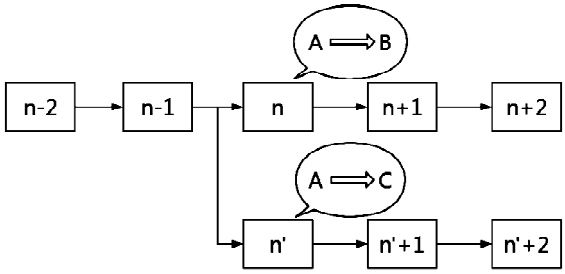

图1 区块链中的51%攻击

目前基于PoW的公有链采用的挖矿算法主要目的是为了消耗每个节点的计算机资源。计算机资源主要分为以下几大类:CPU、内存、硬盘等。那么相应的,区块链的挖矿算法也存在着以消耗这三类计算机资源为主要目的的挖矿算法。PoW共识机制的挖矿算法主要以消耗CPU和内存为主。而于今年正式发布的Filecoin则开创性的提出了一种名为时空证明(Proof-of-Spacetime)的新的共识机制。该机制的挖矿算法主要以消耗计算机硬盘资源为主。由于PoW共识机制的挖矿算法有很多,所以本文主要介绍两种具有代表性的挖矿算法。

1 挖矿算法

区块链挖矿算法种类众多的原因之一就是为了防止51%攻击。在区块链中,PoW共识机制挖矿的能力与矿工所掌握的算力成正比。区块链的特性就是每个区块都指向前一个区块,这样就环环相扣,从最新的一个区块就能一次找到创世区块。但是如果一个恶意节点控制了大部分的算力,那么就可以按照下列步骤发起攻击:

(1)如下图1所示,在区块链上所有的区块都环环相扣,后面的区块包含前一个区块的哈希值。恶意节点A首先在第n个区块中进行一次交易,将一笔资金发送给B,交易数据写入到区块n中。

(2)然后掌握51%算力的恶意节点就马上从第n号区块后进行挖矿,计算新的n'区块,但是该区块不包含由A到B交易的信息,取而代之的是恶意节点A把同样一笔数额的资金发送给C的交易信息。之后其它节点就从n号区块后进行挖矿验证,而恶意节点就在n'号区块后进行挖矿。因为区块链的特点就是以区块数量最多的链作为主链,则恶意节点的算力占了绝大部分后,恶意节点所在的链则很

收稿日期:2017-09-13
*基金项目:西华大学研究生创新基金资助项目(ycjj2016072)。
作者简介:张成成(1991—),男,汉族,安徽阜阳人,硕士在读,研究方向:信息安全。

有可能成为主链。那么，A发送给B的交易的区块就彻底消失了，这样就能使得B损失了一部分资金。

正是因为51%攻击的巨大危害性，则不同的区块量系统在选择挖矿算法的时候就努力避免选择与现有区块链系统相同的挖矿算法。这样就使得其它链的矿机就无法更加高效的在新的区块链上挖矿，新的区块链的矿工算力被其它矿工绑架的概率就降低了，从而保障区块链系统的安全性。

接下来将主要介绍比特币、以太坊和Filecoin的挖矿算法。

2 挖矿算法分析

2.1 比特币挖矿算法

比特币作为最早的区块链系统，其挖矿算法采用的是SHA256散列函数，该函数属于SHA2系列。比特币的挖矿过程很简单：

(1)矿工收到用户的交易信息后，首先验证，然后构造交易的默克尔树，得到一个默克尔树根哈希值，打包进区块头中。对于矿工来说，最优的选择就是先打包手续费高的交易，这样才能保证其利益最大化。

(2)填充区块头，组成80个字节的比特币区块头。区块头的数据结构如表1所示。

(3)将80个字节的区块头信息进行双SHA256运算，得到一个32字节的哈希值。之后判断得到的结果是否小于当前区块的难度值，如果已达到，则该区块就是合法的区块。矿工把它加入到主链中，之后开始计算下一个区块。如果不小于当前区块难度值，则继续更换区块头中的随机数值，重新对区块头进行双哈希运算。

这就是比特币挖矿的完整过程。可以发现，整个挖矿过程就是不断计算做哈希运算的过程。而整个寻找合适随机数的过程是可以多个核心并行查找计算的。因此，拥有众多流处理器的GPU芯片逐渐就取代了比特币的CPU挖矿。然而，无论是CPU还是GPU，其计算过程均是将哈希运算的算法过程编译成底层指令完成计算，指令中并没有专门为哈希运算进行专门优化，无法充分发挥芯片的运算潜力。随后，FPGA(Field-Programmable Gate Array，现场可编程门阵列)通过自身强大的自定义硬件过程，使得哈希函数可以直接通过硬件编程进一步提高运算效率。而近些年，ASIC(Application-specific integrated circuit，专用集成电路)的发展促使矿工可以制作专门的硬件结构对哈希运算进行硬件定制。无疑，这种方式最大可能挖掘矿机芯片的计算潜力。

表1 比特币区块头字段构成

字段	大小
区块版本号	4B
前一个区块头哈希值	32B
默克尔树根	32B
时间戳	4B
区块难度值	4B
随机数	4B

但是，这些优化操作只会将算力更加集中在某几个组织手中。尤其是有了ASIC芯片之后，普通用户使用CPU或者GPU进行挖矿已经没有什么利润可言了。为了防止算力太过集中的情况发生，以太坊就提出了一种新的以消耗内存资源为目的的挖矿算法，这就是Ethash。

2.2 以太坊挖矿算法

Ethash工作过程，其实就是要求从一个巨大的数据集中随机选择若干元素，然后对其做哈希运算的运算过程。具体过程如下：

(1)生成32个字节的种子。以太坊规定每30000个区块是一个窗口，在同一个窗口期中，种子是相同的。种子的生成过程是这样的：第一个窗口期的种子是将32字节的0值做一次Keccak256运算，得到一个32字节的种子。而以后每个窗口期的种子生成方式就是将前一个窗口期的种子做一次Keccak256运算。

(2)生成不定长度的缓存。缓存的生成过程是这样的：每个缓存单元的大小为64字节，即512位。第一个缓存单元是当前窗口的种子值做Keccak512运算得到的。之后每个缓存单元都是前一个缓存单元的Keccak512值。而每个窗口期的缓存大小随着窗口期的增加而线性增大。初始大小为16MB，之后每个窗口期增加不到128KB。之后将初步得到的缓存做3个轮次的Rand Memo Hash运算。Rand Memo Hash算法将缓存的各个单元进行混淆。

(3)生成不定长度的数据集合。首先从生成的缓存中随机找出256个缓存单元，然后合并做哈希运算。这样得到的数据集初始大小为1GB，而后每个窗口期增加不到8MB。注意，在验证区块的过程中，也是同样的操作。这样就需要将缓存和数据集保存到内存中，以方便挖矿或者验证区块的时候频繁的读取数据消耗过多的时间。

(4)矿工之后就通过PoW机制进行挖矿操作。但是因为每个缓存和数据集生成时间需要消耗大量的时间，则为了防止在下一个窗口期到来的时候影响出块速度，则鼓励矿工提前计算好缓存值和数据集。

Ethash在运行过程中需要消耗大量的内存资源进行密集的查找元素计算工作。而ASIC矿机运行过程中需要竞争大量的带宽资源，这就使得采用Ethash算法的以太坊很难出现具有实用价值的ASIC矿机。实际上，当前以太坊矿工使用的芯片主要是显卡芯片，利用GPU的众多核心加快挖矿速度。

2.3 Filecoin挖矿算法

Filecoin其实存在于IPFS(Inter Planetary File System，星际文件系统)的激励层，而IPFS能够提供去中心化的数据存储和访问功能。因此，Filecoin需要大量的数据读写操作，这就要求矿工的挖矿过程进行数据读写操作。Filecoin的挖矿共分为存储挖矿和检索挖矿两部分，分别进行数据的存储和检索工作。

2.3.1 存储挖矿

存储挖矿分为四部分：抵押、接收订单、密封和证明。

2.3.1.1 抵押

抵押的主要目的是为了保证存储矿工能够为网络提供存储服务。存储矿工首先在区块链上进行一次抵押交易,该交易主要通过保存一个抵押品来抵押存储矿工的存储容量。而当存储矿工成功生成了他们提交数据的存储证明,那么存储矿工先前的抵押品就可以退回。如果存储矿工未完成相应的存储证明,那么将会失去部分数量的抵押品。一旦区块链上(分配表)出现了一个抵押交易,那么矿工就可以向存储市场提供他们的存储空间,并且可以设置一定的价格,并生成一个卖单挂到市场的订单账本中。

2.3.1.2 接收订单

接收订单的主要目的是为了从存储市场中获取存储请求。系统就会检查矿工在存储市场上的卖单是否与对应的来自客户端的买单相匹配。一旦卖单和买单想匹配,那么客户就会将自己的数据发送给存储矿工。而实际上,矿工收到的是一个个数据片。当存储矿工收到数据片后,就把数据存储到自己的硬盘中,与此同时,矿工和客户端都会签署一个交易订单,并将之提交到区块链上。

2.3.1.3 密封

密封的目的是为未来的证明准备数据片。存储矿工的存储空间被分为几个扇区,每一部分都包含分配给矿工的数据片。网络通过分配表对每个存储矿工的各个存储扇区进行跟踪。当一个存储扇区存储满了之后,该扇区就会被密封。密封操作过程很慢,它需要依次将一个扇区的数据转换保存为一个副本。而每个数据的物理拷贝都与存储矿工的公钥相关联。

2.3.1.4 证明

存储矿工需要证明他们存储了提交的数据片。当存储矿工被分配到一个数据的时候,他们必须重复生成数据副本证明,以此来保证存储矿工确实保存了数据。该证明将推送到区块链中,并被全网验证。

2.3.2 检索挖矿

检索挖矿分为两部分:接收订单和发送。

2.3.2.1 接收订单

索引矿工从索引市场中获取数据请求。索引矿工通过向网络中传播卖单来宣布他们的数据片。他们设置一个价格,然后添加一个卖单到市场的订单账本中。然后,索引矿工检查他们的订单是否与对应的客户买单相匹配。

2.3.2.2 发送

一旦订单匹配,索引矿工将会发送他们的数据片给客户端。客户端收到数据片后,矿工和客户端签署一个交易订单并提交到区块链中。

3 结语

区块链,尤其是公有链中,为了保障系统的安全性,容错率达到50%的PoW共识机制似乎是个好的选择。但是它也带来了严重的能源浪费问题。这个能源能源浪费问题包含两个方面,一个指能源浪费,一个指矿机的浪费。能源浪费指的是矿工需要消耗大量的电力来进行挖矿。以比特币为例,当前的比特币网络全网算力为5000PH/S,而阿瓦隆即将发布的Avaon741矿机单机算力为8TH/S,所用功率为1150瓦,即使全网矿机全部更换为最新矿机,全网一天仍要消耗约1700万度电力能源。无疑,这是一种巨大的能源浪费。

矿机浪费指的是废旧的矿机无法二次利用。以比特币ASIC矿机为例,该种矿机通过对底层的硬件进行定制优化,使其做哈希运算速度明显高于显卡矿机,但是正因为这一点,所以导致了比特币ASIC矿机在挖矿淘汰后就无法二次利用。而以太坊挖矿主要以显卡为主,其挖矿淘汰后仍然可以被个人电脑收购使用。同样,Filecoin矿机挖矿淘汰后仍然可以被普通用户加以利用,这和以太坊一样,均在一定程度上减少了能源浪费。

然而,通过以上三个典型算法的说明,我们发现区块链中的挖矿算法既要保证系统的安全,又要尽可能的降低能源浪费,这是个很难同时满足的要求。这同时也说明了,区块链系统的安全性是需要以一定的能源浪费为代价的。

参考文献

[1]Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [J]. Consulted, 2008.

[2]Back A. Hashcash - A Denial of Service Counter-Measure[C]// USENIX Technical Conference.2002.

Analysis of Typical Mining Algorithm of Blockchain

Zhang Chengcheng

(School of Computer and Software Engineering, Xihua University,Chengdu Sichuan 610039)

Abstract: Block chain mining is not only a way for system to issue new coins, but also the most important cornerstone for ensuring the safe and stable operation of the block chain system. A mining algorithm must be designed differently for preventing block chain from 51% of attacks. Different mining algorithm would consume different major computer resources. The paper takes mining algorithms of Bitcoin, Ethereum and Filecoin as examples, which mainly consume resources of CPU, memory and disk respectively. Through analyzing the major process of such three mining algorithms, the paper comes to conclusion that there is no solution satisfying both safety of block chain and effective resources consumption.

Key Words: Blockchain;Bitcoin;Ethereum;Filecoin