Zcash挖矿算法深度解析

雷盈 2016-11-25 10:57发布在 竞争币 34934

相比于比特币，Zcash在挖矿算法方面进行了修改。比特币使用的挖矿算法是SHA256， Zcash则使用的是Equihash。Equihash算法由Alex Biryukov 和 Dmitry Khovratovich联合发明，其理论依据是一个著名的计算法科学及密码学问题——广义生日悖论问题。

笔者希望通过尽可能通俗的语言论述Zcash是如何运用Equihash算法实现挖矿进程的。

接下里讲解Zcash挖矿的一般过程。注：笔者目前仍无法完全脱离代码进行讲解。

<ignore_js_op>

①构建区块头 执行挖矿算法之前，首先要构建一个区块头。Zcash的区块头（Block header）结构如下,这一结构与比特币的区块头类似，差异在于随机数的位数。

<ignore_js_op>

32-bit	nVersion	//版本号，32位
256-bit	hashPrevBlock	//前一区块头的hash，256位
256-bit	hashMerkleRoot	//交易记录的hash树的值，256位
256-bit	nNonce	//随机数，比特币32位，Zcash256位
32-bit	nTime	//更新时间，32位
32-bit	nBits	//当前运算难度，32位

图1 Zcash的Block header

nVersion，区块版本号，升级时改变。 hashPrevBlock，从前一区块获得。 nBits，由全网算力决定，每产生一个新块都调整一次难度（比特币每2016个区块调整），算法为DigiShield v3/v4。 nTime，基本取机器当前时间轴。 hashMerkleRoot，本字段允许矿工自行调整，变化来自于对包含进区块的交易进行增删，或改变顺序，或者修改Coinbase交易的输入字段。 nNonce，Zcash提供2^256种可能取值，而比特币提供2^32种。 一般来讲，hashMerkleRoot和nNonce是发挥挖矿自由度的地方。

1. 选择待确认的交易，因为矿工可以从交易中获得手续费，所以一般构建区块时会选择尽可能多的交易，但是不能超过容量上限（2M）。
2. 确定Coinbase，这里记录假如该区块构建成功，矿工将获得的收益（手续费+奖励）。
3. 构造Merkle树（集合交易信息），生成随机数V，写入其他参数
4. 构建如图1所示的Block header。

②转化为一个广义生日悖论问题

我们通常把比特币的“挖矿”过程比作解一道算法题。而这道算法题的题目就是通过对Block header 的函数处理给出。 比特币的算法：对Block header的参数进行两次SHA256运算，得到一串256位的字符串，让它与一个预期值target进行比较，如果这个值小于target，则挖矿成功，即SHA256（SHA256（Block header））<target，否则调整Block header（修改随机数或者Merkle树），再重复上述运算。 Zcash的算法：同样是在构建完Block header以后， Zcash不是做一个不等式判断，而是以Block header作为输入，将挖矿问题转化为一个“广义生日悖论问题”。

什么是广义生日问题?

用计算机语言定义广义生日悖论： 随机生成一个由N个“n位字符串{Xi}”组成的列表L,

<ignore_js_op>

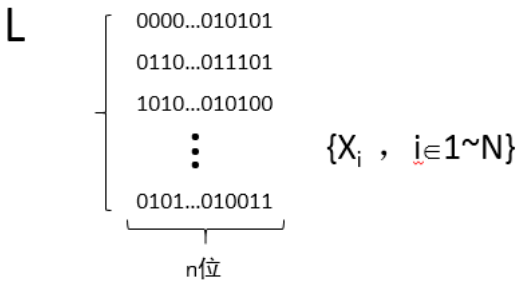

图2

要求在这些字符串中找到2^k个特定的{Xij}，使得：

<ignore_js_op>

$$X_{i_1} \oplus X_{i_2} \oplus \cdots \oplus X_{i_2{}^k} = 0 \quad （\oplus: 异或符号）$$

通俗的表达：从该列表L中找到2^k个完全相等的元素，即找到2^k个碰撞元素。

注:限于篇幅，本文只讲结论，若读者感兴趣，可自行查找“生日问题相关内容”

如何处理Block header得到一个“生日问题” Zcash内有一个专门的哈希函数Equihash Generator。Equihash Generator的功能是将一个输入和一个索引映射到一个长度为n位的输出。 令i ∈ {1 .. N}，把生成的区块头（Block header）以及整数n、k作为输入，其中 n、k的值由官方给定，通过<ignore_js_op>

$X_i = \mathrm{EquihashGen}_{n,k}(\text{Block header}, i)$

的函数过程，可以生成一个由N个“n位字符串{Xi}”组成的列表L。

<ignore_js_op>

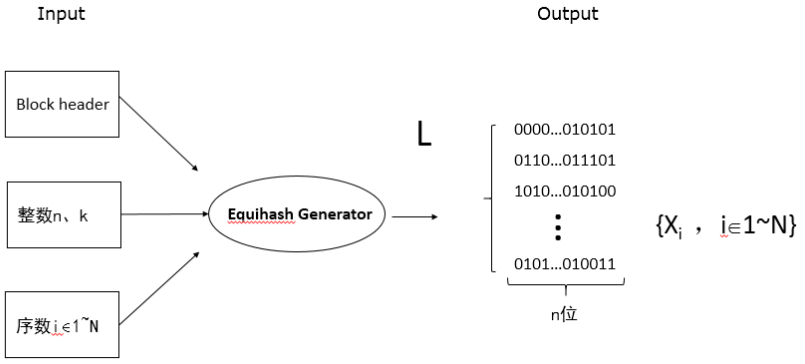

图3

③ “广义生日悖论”的解法 用于解决“广义生日问题”，数学界提出了许多著名的算法，密码学家Wagner的算

理论上，为了公平起见，用于“工作力证明”的算法必须是对于该问题的最优算法，因为假如这个算法不是最优的，那么可能有人会发明并暗地里使用更优秀的算法挖矿，则在同算力条件下他的挖矿成功概率就会大于其他人。但是若是仔细考察“OptimisedSolve”算法，不难发现它还是存在优化的可能性的。具体如何实现优化，本文不展开思考，笔者的后续文章会就这一点进行单独讨论。
限于篇幅，不详细介绍“OptimisedSolve”算法的原理，若有兴趣，可以参考文献:《Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem》

求解过程:

把从Block header派生出的列表“n位字符串”列表L当做“生日问题”的条件，运用改良的算法“OptimisedSolve”，即可从L中找到2^k个完全相等（碰撞）的{Xij}，使得:

<ignore_js_op>

$$X_{i_1} \oplus X_{i_2} \oplus \cdots \oplus X_{i_2^k} = 0$$

具体过程如图4所示

<ignore_js_op>

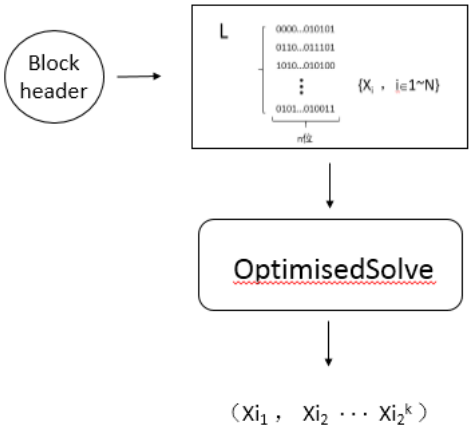

图4

④难度调整（Difficulty filter）
到第③步为止，“生日问题”已经被解决了。但是并不是说谁先构造并解决了一个“生日问题”谁就取得了“挖矿”的胜利，若单纯以生成并解决一个“生日问题”作为胜利条件，则有可能出现以下几个问题:
1.从概率学的角度，生成的列表L中可能不存在2^k个完全相等的值，即碰撞的个数少于2^k。这会导致有的“矿工”构造出来的“生日问题”是无解的，所以当出现这种情况时必须重构一次“生日问题”。
2.单纯的使用“OptimisedSolve”导致“挖矿”难度难以被控制，因为该算法的运行时间服从泊松分布。
3.在内存足够多的情况下，可以使用更复杂的技术迭代产生多个摊销成本更低的解决方案，即运行这样的算法会让单位内存的运行成本降低，有悖于公平“挖矿”的理念。
（Zcash希望实现公平“挖矿”，即群众参与挖矿，而不是矿池垄断挖矿。）

所以，和比特币一样，Zcash也应用了一个叫做Difficulty filter的难度调整算法。

Difficulty filter（记为H）是一个被用来调整工作证明的时间和内存要求的算法。得出“生日问题”的碰撞解{Xij}之后，还要进行Difficulty filter环节的检验。检验通过才能算是“挖矿”成功。具体过程如图5所示。

<ignore_js_op>

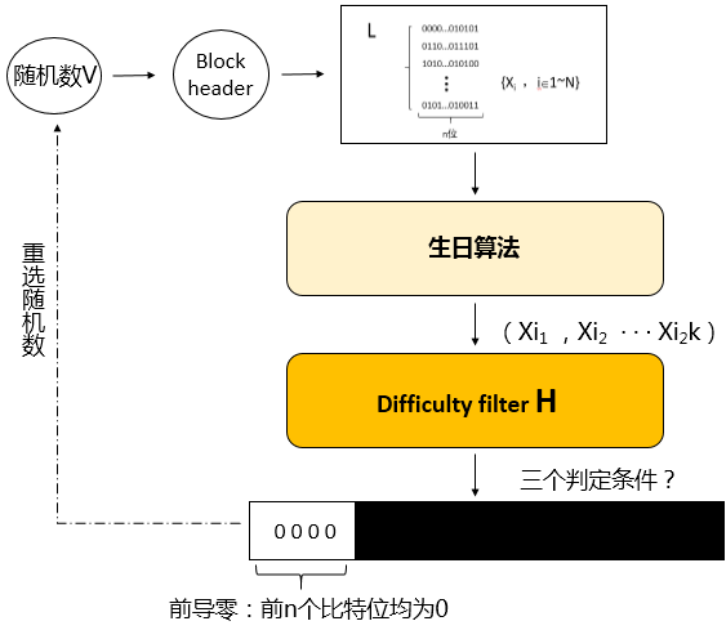

图5

1）Difficulty filter的三个判断条件

注：H（S）表示输入S 经过Difficulty filter H这一算法过程输出的结果. -生日算法条件：<ignore_js_op>

$$H(I||V||x_1) \oplus H(I||V||x_2) \oplus \cdots \oplus H(I||V||x_{2^k}) = 0,$$

-难度算法条件：<ignore_js_op>

$$H(I||V||x_1||x_2||\ldots||x_{2^k})$$

的结果有d个前导零

-绑定算法条件：<ignore_js_op>

$$H(I||V||x_{w2^l+1}) \oplus \ldots \oplus H(I||V||x_{w2^l+2^l})$$

的结果有n*l/(k+1)个前导零，这对于所有满足条件的w、l均成立。

注;前导零的个数指的是一串二进制数前若干位为零的位数（见图5）。

-生日算法条件表示用来确定上一过程获得的解是否是满足条件的碰撞； -难度算法条件用来确定当前难度是否合理，并成为难度调整的依据； -增加一个绑定算法可以防止有人发明某种算法：该算法使用足够多内存摊销成本，使单位内存成本降低。 （这里只讨论结论，具体算法限于篇幅不展开讨论）

2）判断过程

如果某矿工构造的“生日问题”能找到2^k个碰撞解，并且经过难度 调整算法以后仍满足三个条件，则这个“矿工”挖到了“矿”，即此人成功建成一个新区块。 如果不能找到足够数目的解，或者无法全部满足三个条件，则“挖矿”失败，此时矿工需要修改随机数，从头开始，重新开始新一轮的“挖矿”。 同样的，这一过程也会成为Zcash挖矿难度调整的依据，每生成一个新块，都会进行一次难度调整。

④总结

Zcash挖矿的一般过程即先构造输入条件（区块头以及各项参数），通过特定函数将输入条件转化成“广义生日问题的一般形式”，用优化算法解析该问题并对获得的解进行难度判断，同时满足算法条件和难度条件则判定“挖矿”成功，否则调整随机数重新运算。

本文为雷盈特邀作者Carlos撰稿，作者钱包地址：15s9WUHtPLAdSqvYaFYniE3k1wFGUoHDF8

雷盈（公众号:RadarWinChina）是上海区块链标杆企业，为区块链全产业链提供技术与咨询服务。

文章标签： Zcash

推荐资讯

巴比特专栏 | 零基础了解以太坊：以太坊智能合约的运作原理

7163 1

拉了盘就跑？12月ICO项目方的ETH抛售量创18年月度记录

16121 0

熊市也能买买买，这些公司都参与了今年的并购狂潮

40488 1

评论（1）

登录 账号发表你的看法，还没有账号？立即免费 注册

比特币导师 2017-11-23

BTG用的挖矿算法是和Zcash一样的Equihash算法，了解这个算法的优点可以读一读这篇文章：Zcash挖矿算法深度解析 http://t.cn/R0HKhMH

0 赞 回复 0 踩