*约定1：LOG10(X)是指以10位底对X求对数。*

*约定2：GAIA的最小价格单位为uGAIA,换算关系如下:1000,000uGAIA = 1,000mGAIA = 1GAIA。*

*简要介绍： 整个区块链是建立在一个P2P网络上的。P2P网络上的节点和节点之间只能互相广播交易消息和区块消息。区块链地址和P2P网络中的节点是2个完全不同的概念，区块链地址是区块消息中记录的一种数据。*

## 历史

POW作为第一代共识机制解决了分布式系统中的共识问题。PoW(Proof of Work)是基于算力计价的共识机制。矿工通过解决一个复杂而无实际意义的数学问题来创建一个区块，并获得一定数量的币作为奖励。每个矿工解决问题的能力完全取决于自身的算力，为了赚取奖励，矿工会互相竞争，不断升级自己的算力，白白耗费大量的资源和能源，导致交易费用不断升高，却无益于提高交易速度。除此之外，持币者无法参与任何决策，决策权集中在少数几个矿池手中，与去中心化理念背道而驰。

PoS(Proof of Stake)是基于链上货币计价的共识机制。PoS用持币代替了算力，能够让持币者更多的参与到挖矿过程中，而且不需要计算复杂的数学问题，避免了资源和能源的浪费。已有的POS解决方案主要分为四种：基于拜占庭容错的PoS，基于链的PoS，Pow/Pos混合,基于授权的PoS(DPoS)。基于拜占庭容错的PoS容错率较低，故障节点和恶意节点不超过矿工总数的1/3，且为了达到较短的确认时间限制了验证者的数量。基于链的PoS本质上是PoW的一个货币计价改编。PoW/PoS混合只是一个过渡方案，最终仍会被一个纯粹的PoS机制所取代。基于授权的PoS通过选举代理人达成共识，牺牲了去中心化的概念，不适合公有链。在研究了已有的PoW机制和PoS机制之后，GAIA提出了一个全新的PoS方案：基于竞争的PoS(CPoS)

## CPoS

GAIA在创世区块中生成并且分配10,000亿GAIA，之后的区块创建由锻造委员会完成。为了解决PoS机制常见的富者越富问题，除创世区块外，其他区块的创建过程不再产生新币,所有收益均来自于交易费用。

锻造委员会

锻造委员会是区块链的一个基础底层模块，其中包括一个拥有创建区块权利的地址的集合。集合中的每一个地址都是一个锻造委员，每个锻造委员都有机会创建区块。为了激励锻造，成功锻造一个区块将会获得该区块中的所有交易费。

所有地址都可以申请加入锻造委员会，在加入锻造委员会时，会提交一个bls加密算法的公钥，自己保留私钥，公钥会用来验证该锻造委员产生的随机数。锻造委员会收取最少1,000GAIA作为保证金，保证金和锻造者的权益值相关，如果锻造者故意作恶，保证金会被罚没。收取保证金是为了防止节点作恶，最低限度设置为1,000GAIA是为了防止微资金地址加入锻造委员会。GAIA认为保证金较高的地址，作恶的可能性更小。如果一个保证金少于1,000GAIA的地址申请加入锻造委员会，保证金会被罚没，罚没保证金是为了防止恶意的加入申请。

锻造委员的职责是创建新的区块。锻造委员可以主动申请退出锻造委员会,该地址的保证金会被扣留256,000个区块高度。扣留保证金是一种惩罚机制，用于惩罚不能正常完成其职责的锻造委员。之所以不设置退出机制，是为了防止恶意节点，将大部分节点剔除出锻造委员会，实施长程攻击。

锻造组

所有人都可以查询到每个锻造委员的当前投票权。锻造委员首次将被按照地址的后8-bit进行分组，后两位地址即是分组编号，分组编号相同的为同一组，总共16\*16=256个组。设当前区块高度为H，则H%256=N，N号锻造组负责本轮的锻造。首次按照地址分组是为了让锻造委员尽量加入锻造委员较少的组，使得每组委员数不会相差过大。同时，由于单一用户可以拥有无限个地址，所以即使只有一个用户也能够占满256个分组。

主锻造委员

当前锻造组中投票权最高的锻造委员当选为主锻造委员，后续锻造组都倾向于验证和认同主锻造委员锻造的区块。

本组内所有的锻造委员都可以创建区块并且全网广播，其他节点收到区块后将进行验证。

为了优化不必要的计算和网络广播和建设分叉，如果主锻造委员在上一个区块产生N秒之后仍然没有全网发送新区块，则当前锻造组中投票权第2,3高的锻造委员则会立即锻造区块并广播。如果再过1S仍未产生区块，则投票权第4,5高的锻造委员则会立即锻造区块并广播。以此类推，直到锻造出新的区块。这个策略可以降低分叉的可能性，同时兼顾区块创建速度。

投票权计算

锻造委员的投票权和保证金的数值相关，设一个锻造委员缴纳的保证金为a个GAIA，则初始投票权K为LOG10(a\*0.01)\*p。P为一个在[1,4]之间的随机值，在锻造委员初次获得投票权时生成，且在投票权再次初始化时重新计算。一个新申请加入的锻造委员不会立即获得投票权，需要等待256000个区块高度以后才会获得投票权。之后每隔256个区块高度(即一轮)投票权一次性增加K。随着区块高度的增加，投票权不断累积，投票权最多增加2560个区块高度，即初始投票权K的10倍，之后不再增加。用投票权进行委员排序，如果有多个投票权最高的锻造委员，则比较锻造委员的地址值，地址值更大的排名更高。在当前分组中排名前10的锻造委员会获得额外的排名投票权，设排名为R,则排名投票权为2的(11-R)次方。总投票权为累积投票权与排名投票权之和。

每个区块都会生成一个随机值，区块高度m对应的随机值为。

为一个hash函数，让入参被唯一映射到一个[1,4]之间的值。设锻造委员地址为l，则p=。如果一个锻造委员成功将区块添加到了区块链，则该锻造委员和当前分组中投票权更高的其他锻造委员的投票权都会被重置为初始投票权（p值会重新计算），且都会被重新分组。分组依据为委员地址、当前区块高度、当前随机值三者hash的最后8-bit的值。之后随着区块高度的增加，投票权不断累积，直到最高为初始投票权K的10倍。之所以需要不断的更新分组和更新初始投票权，是为了防止恶意节点串通控制几个相连的节点进行双花攻击。

降低保证金数值和投票权的正相关程度是为了避免大额地址拥有过高的投票权。累计投票权随着区块高度增加而增加，是为了激励小额锻造委员也有机会成为主锻造委员。设置10倍的上限是为了控制小额锻造委员的数量，保证金过少的锻造委员在可信度和稳定性方面不如缴纳了大额保证金的锻造委员。排名投票权是为了降低被恶意委员联合攻击的风险。

奖励和惩罚

锻造委员的奖励由两部分组成：1.主锻造委员创建新区块将获得该区块中所有交易费。2.举报作恶锻造委员将获得该作恶地址的所有保证金。在没有双签作弊节点的情况下，锻造委员只能从交易费中获得奖励，不会获得额外的奖励。

类似比特币或以太币的额外的奖励会引发富者越富的副作用，而且区块的创建过程消耗的资源极低，即使只有交易费作为奖励，锻造委员已经有利可图了。

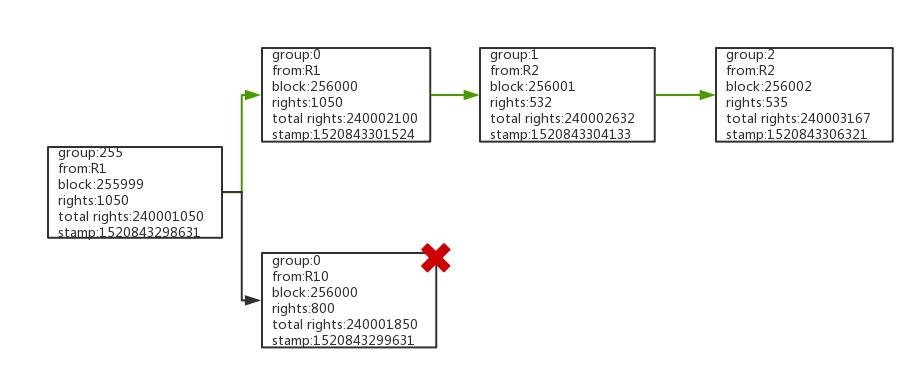
当锻造委员收到一个新的区块时，会验证区块高度、主锻造者签名、交易有效性，如果通过验证则会加入到自身的区块链上，如果没通过验证则会丢弃该区块。如果同一个锻造委员在同一个区块高度向其他锻造委员发送了两个不相同的区块，则该锻造委员被判定为作弊，将被罚没所有保证金。第一个举证该锻造委员作弊的锻造委员将获得被罚没的所有保证金。

共识机制

总投票权最高的链是主链。第N个区块的投票权等于主锻造委员在锻造该区块时的总投票权，区块链的总投票权为单个区块的总投票权之和。因为主锻造者的投票权极高，所以区块将会在极短的区块高度就达成共识，分叉将迅速被消除。

最短出块时间

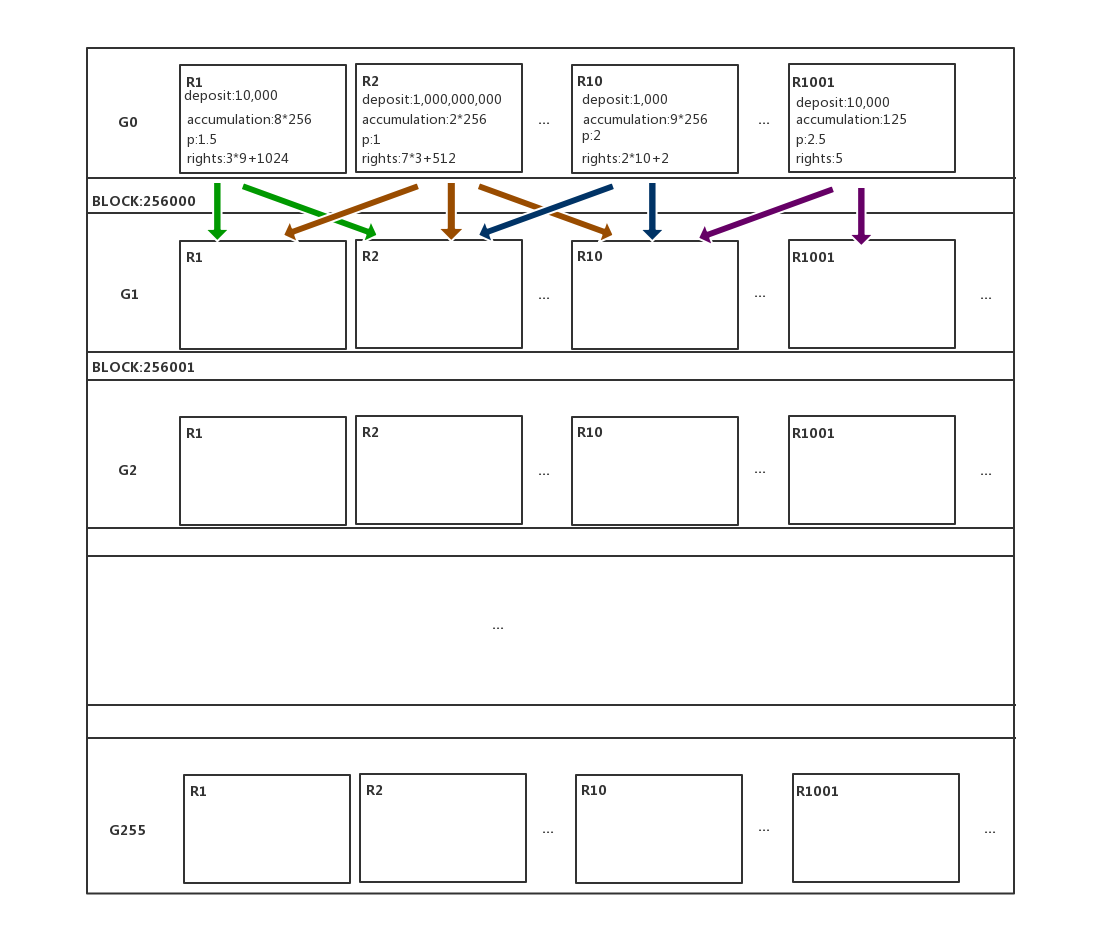
为了防止长程攻击(long-distance attack)我们在创世区块中会设定默认最短出块时间T，如果出块间隔小于T/2，则认定该区块无效。不同的侧链，可以根据需求设定不同的最短出块时间。具体过程如下：当产生一个新区块会在所有锻造者之间广播，锻造者以本机时间为准，如果新区块的时间戳大于本机时间则认为该区块无效，如果新区块时间戳和上一个区块的时间戳间隔小于T/2，也认定该区块无效，无效区块会直接被抛弃，不会被广播。之所以是T/2而不是T，是因为我们在一定程度上鼓励快速出块，也减小了锻造者本机时钟轻微误差造成的影响。例如，设定默认最短出块时间为3S，如锻造者发现两个区块的时间戳间隔小于1.5S，则认定该区块无效。



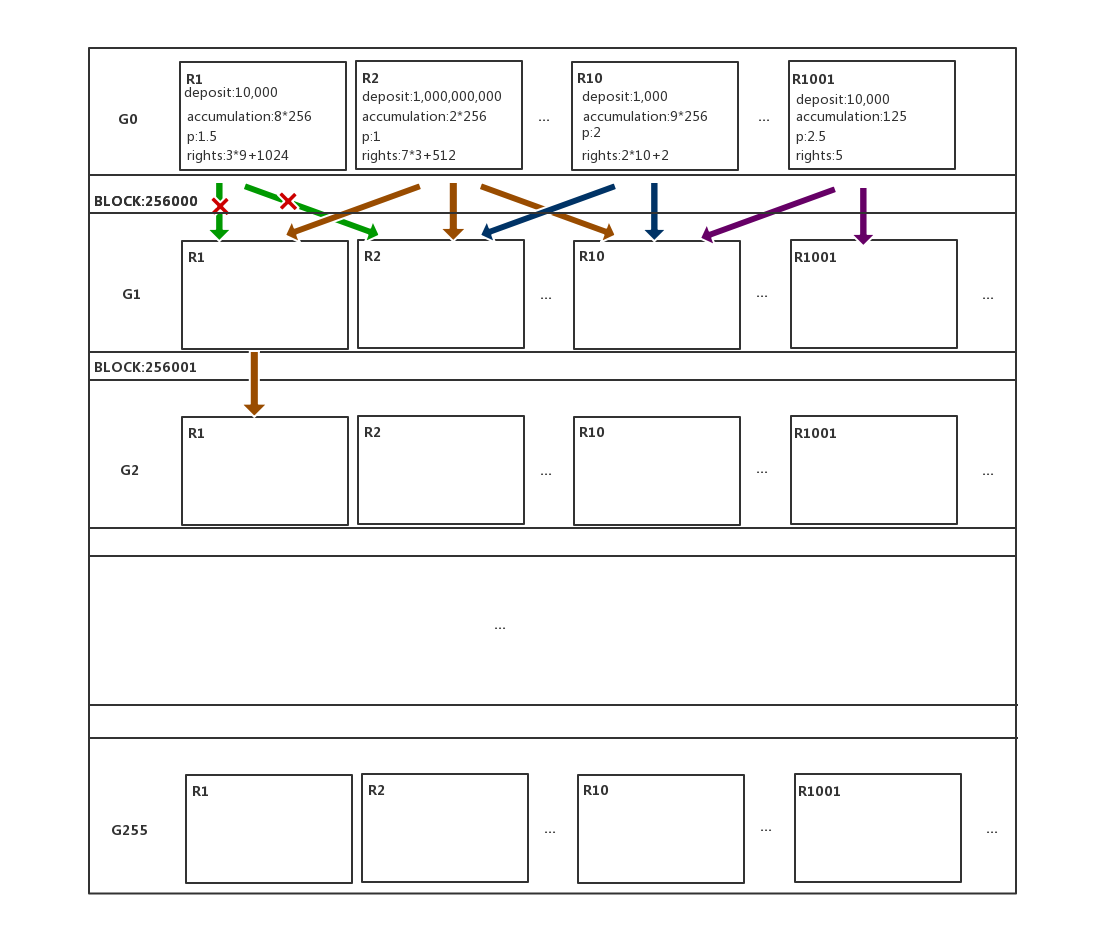
锻造过程

为了便于理解，此处只描述最高投票权锻造者和次高投票权锻造者的锻造过程和选择策略。实际情况更为复杂，但是原理相同。我们约定Rn代表分组中投票权排名第n位的锻造委员。

在区块高度255,999,所有组编号为0的锻造委员均有机会创建256,000号区块，其他分组无法创建区块。R1地址为0xdab12...00,缴纳了10,000GAIA保证金,随机值P=1.5，总共累计了2,304个区块高度(即9轮)，累积投票权为27，排名投票权为1024，总投票权为1051，设其创建的区块为B1。R2地址为0xd12e9...00,缴纳了1,000,000,000GAIA保证金,随机值P=1,总共累计了768个区块高度(即3轮)，累积投票权为21，排名投票权为512，总投票权为533，设其创建的区块为B2。虽然R2缴纳的保证金为R1的100,000倍，但是R1却获得了更高的投票权,避免了富者对投票权的垄断。所有组编号为0的锻造委员都可以将自己创建的256,000号区块进行全网广播。只有组编号为1的锻造委员们可以继续创建256,001号区块。由于总计投票权最高的链会成为主链，组编号为1的锻造委员们在理智的情况下都会在B1的基础上继续创建256,001号区块。

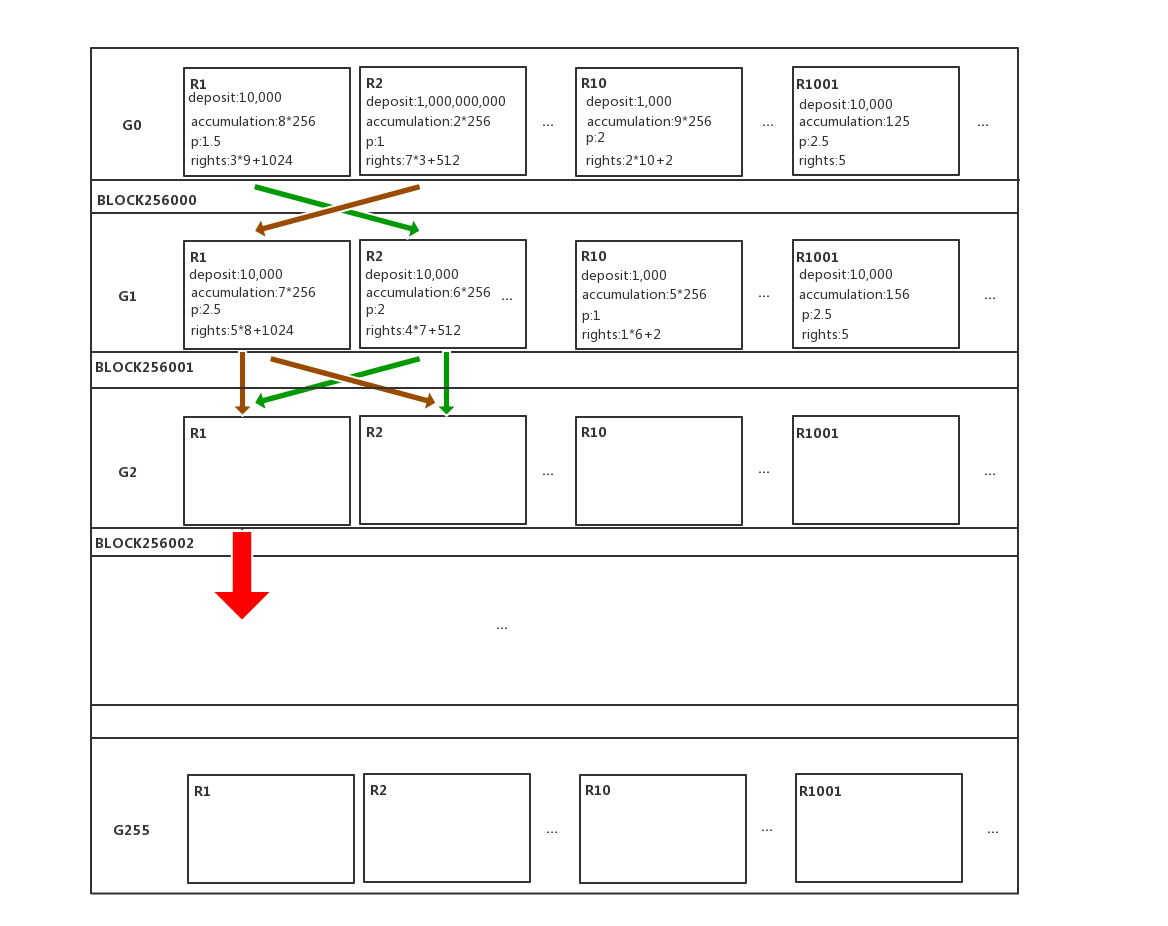


现实世界的网络环境极为复杂，投票权最高的投票委员有可能没有向下一个锻造分组发生新的256,000号区块。G1分组锻造委员的最优策略是：等待G0分组R1一段时间，如果仍无响应，则接受R2创建的区块。愿意等待的时间和G1分组锻造委员自身的总投票权相关。自身总投票权越低的节点愿意等待的时间越长，因为这是在256,001区块高度打败同组更高投票权投票委员的唯一方法。G1分组中R1会等待一段相对较短的时间，然后接受G0分组R2创建的区块。因为自身投票权最高，即使接受了投票权较低的区块，仍然有较大机会胜出。

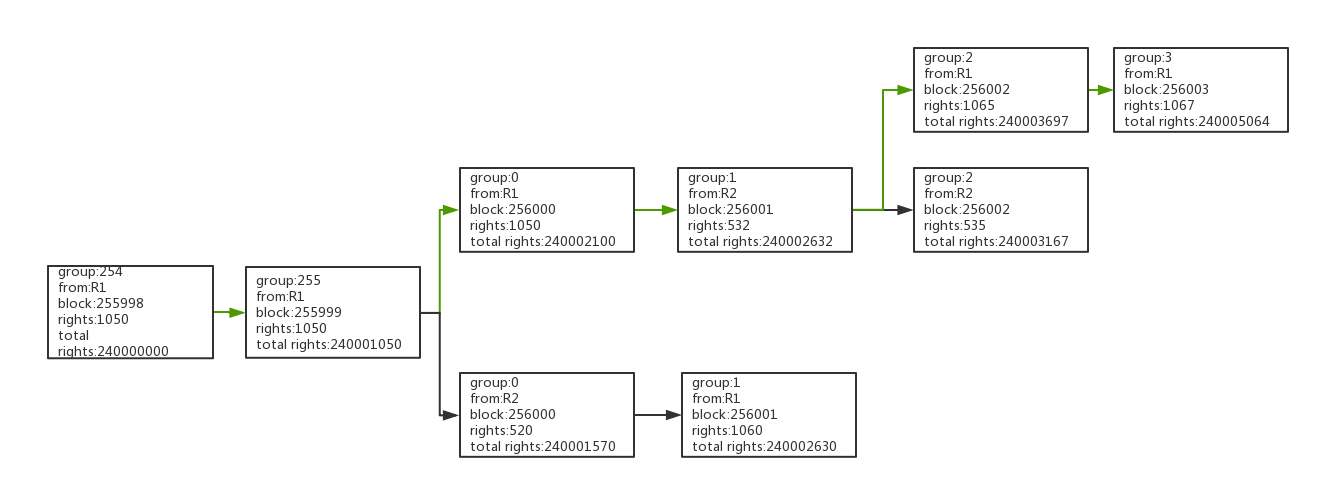


由于总投票权和分组、保证金、累积区块高度、排名投票权、地址五者相关，使得锻造委员难于串通作弊，但不排除由于网络原因或者其他未知原因导致的，最高投票权锻造者接受了上一个区块的次高投票权的锻造者创建的区块，如图所示。

G1分组中的R1接受了G0分组R2创建的256,000号区块，而G1分组中的R2接受了G0分组R1创建的256,000号区块。G1分组中的R1和R2都会向G2分组的锻造者提交区块。G2分组中的R1选择总投票权最高的链继续锻造。



基于cPoS机制，分叉总是能在较短的区块高度被消除，如图所示。在区块高度256,000和区块高度256,001产生了分叉,而G2分组的最高投票权锻造者选择了其中一条链，该链的总投票权显著增大，有极高概率胜出。G3分组的锻造者会基于该链继续创建区块。



可验证性随机

每一个区块都有一个随机值，随机值由当前区块的锻造者产生。锻造者拥有一把特殊的bls私钥，用于生成随机数，而对应的bls公钥在锻造者申请加入锻造委员会时公布。设当前区块高度为m，随机值为，上一个区块随机值为，BLS为签名算法,则，即使用上一个区块的随机值和当前区块高度来生成新的随机值。锻造者在当前区块高度，同时公布旧bls私钥和随机值，以及新的bls公钥。由于所有人都提前获得了旧的bls公钥，所以都可以对随机值进行验证，确保随机值的确是由旧bls私钥生成的。由于旧的私钥已经被知晓，所以锻造者需要更换新bls私钥，并公布新bls公钥。在随机数生成过程中没有加入交易信息等可人为控制的信息，是为了确保锻造者不会人为筛选交易，以获得对自己更有利的随机结果。

我们无需保证初始随机源的随机性，非随机的初始随机源，只会对最初的几个区块产生影响，对于后续区块，即使初始随机源是非随机的，后续产生的随机数仍然是随机的。

由于锻造者提前知道了锻造结果，这种方案对锻造者有一定优势，但是可以通过应用层的再次随机抵消这种优势。

参考文档：

http://blog.csdn.net/AAA123524457/article/details/52837289

http://blog.liqilei.com/bai-zhan-ting-gong-shi-suan-fa-zhi-pbftjie-xi/

http://chainx.org/news/index/detail/id/14.html

https://www.zhihu.com/question/52254063

http://ethfans.org/posts/consensus-compare-casper-vs-tendermint

https://www.leiphone.com/news/201706/JfsBmaf6Y0ZtV11R.html

https://www.cardanohub.org/zh/academic-papers-3/

https://iohk.io/research/papers/#9BKRHCSI

https://iohk.io/research/papers/#XJ6MHFXX

https://188bz.com/64342.html

https://bitshuo.com/topic/5a505639ecc0ff3642836274

https://wiki.chainnova.com/pages/viewpage.action?pageId=3997804