**专 利 申 请 技 术 交 底 书**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 发明类型：发明 | | | | |
| 同日申请实用新型  请求提前公布 优先权 | | | 实审方式：新申请提 公布提  期限届满提 不提 | |
| 发明名称： 一种区块链中的随机数选取方法 | | | | |
| 发明人 | 程万鹏 | 身份证号 | | 340102199101152511 |
| 技术联系人 | 程万鹏 | 所属单位/部门 | |  |
| 电话 | 18856921285 | 传真 | |  |
| **E-mail** | trifist0115@hotmail.com | | | |

**术语解释：**

**1、本发明要解决的技术问题是什么？**

区块链技术最近日渐火热，从技术的角度上来讲，各种区块链技术实现的都是一个去中心化的，或者说是分布式的数据库系统。该系统的特点是有很多个分处与世界各地的节点，每个节点都会维护一套相同的数据库。这就导致了恶意篡改数据极其困难，数据丢失极为罕见，从而实现了一个公平透明，解决信任危机的平台。

区块链是可编程的，对于最新的区块链实现例如Ethereum或者EOS来说，几乎可以写代码（区块链的世界中称为“合约”）来记录任何事情。但是由于区块链技术本身的特点，会有一些操作实现起来比较困难，本文论述的就是其中之一——随机数的选取。

常见的平台像是PC或者服务器，他们采取的随机数获取方式是根据内置算法来计算一个伪随机数，但是这种方法在区块链的世界中行不通。正如前面所说，区块链的技术涉及到了全世界的无数节点，每个节点为了保持数据一致性，必须要求同一段代码的执行结果在自己的节点和在其他节点的执行结果一样，如果在这其中涉及到了随机过程，那么该结论则不能保证。换句话说，在区块链的世界中，需要找到一种方式，使生成随机数之前，大家都不能预测这个随机数（做到随机）。但是对于同处于系统中的各个节点，他们拿到的随机结果要一致（做到确定）。本文要介绍的就是一种符合上述规则的选取方法。

**2、详细介绍技术背景,并描述已有的与本发明最相近似的实现方案**（包括两部分：1、作为本发明基础的且帮助理解本发明公知技术内容；2、与本发明最接近的已有技术方案的说明（对于方法，应说明现有方法的步骤，对于装置，应当说明结构组成及其关系）

1.本方案技术背景

区块链技术中的区块是用来打包交易的，每个区块中会包含若干交易，且每个区块也会有个唯一标识（通过哈希算法得出）。这个标示是与该块内部的交易相关的，交易变则标识变。由于现实中的交易是发生在世界各地的，涉及到的内容以及发送者更是不计其数。由此我们可以看出，在某个特定的区块内包含的交易内容将会是随机的，由此，区块的唯一标识也会是随机的。本方案就是以这一特点为基础，来实现随机数的选取。

2.已有技术方案

A．访问外部数据方案

这一方案的代表是Ethereum中的Oraclize。它提供了一个桥梁，使链上合约可以与互联网进行交互，从而能获取到一些随机数据，包括天气、汇率、股票价格甚至宇宙微波背景辐射等，并以此作为随机源来产生随机数。

B.“投票、揭晓”方案

Randao的技术白皮书描述的就是这一方案。他的实现分为两个阶段，分别为投票阶段以及揭晓阶段。当有人需要获取随机数的时候，它会发申请给一个特定的链上合约，并且附上手续费。这时该合约会进入“投票”阶段，在这个阶段中，合约会以得到的手续费来吸引一些随机数生成者来协助生成随机数。具体方法就是每个协助者在本地生成一个随机数，取其哈希值，提交到合约中去。在“揭晓”阶段，之前参与的协助者再向相同合约发送最初生成的随机数，合约会通过取哈希来校验协助者是否作假。如果没作假，则这个随机数会记录成随机种子之一。最后，当所有协助者都揭晓之后，合约会根据合法的种子进行一系列运算来得到最终随机数，并返回给最初的调用者。

**3、以因果关系推理的方式推导出现有技术的缺点是什么？针对这些缺点，说明本发明的目的及能够达到的技术效果。**（现有技术的缺点是针对于本发明的优点来说的，本发明不能解决的缺点不必写）

1、A方案的缺点显而易见，既然区块链追求的是去中心化与信任，那么有一个中心机构来负责产生随机数明显是不妥的。A方案中，无论通过或联网获取的是天气数据或是股票数据，都无法保证数据源不会因为利益而作假。虽然选取的数据源可能足够权威并且与随机数的产生没有利益纠葛，虽然方案中提出了各种验证措施，但这都不能完全确保公正性。因为它最终依赖的还是一个权威机构，而不是一种确定的算法。

2、B方案就是为了解决A方案的问题而应运而生的。它通过严格限制随机数产生步骤来形成一种算法，使其从逻辑上就不存在造假的可能。但是它的缺点也相当明显，那就是太复杂。一个随机数的产生需要用到手续费，并且还需要一堆的协助者来进行配合。方案的维护者也要随时确保它的激励手段能吸引来一定数量的协助者，否则这个方案就无法进行下去了。

**4、本发明技术方案的详细阐述，应该结合流程图、原理框图、电路图、系统结构图进行说明**（发明中每一功能的实现都要有相应的技术实现方案；所有附图都应该有详细的文字描述；方法专利都应该提供流程图，并提供相关的系统装置）。

4.1 本部分为专利申请最重要部分，需要详细提供；

4.2 发明必须是一个技术方案，不能只有原理，也不能只做功能介绍；

4.3 对于软件、业务方法，要提供流程图；

4.4 必须结合流程图、原理框图、电路图、系统结构图等附图进行说明。

本方案是以每个区块的哈希值为基础来进行随机数生成的，由于每种区块链的具体实现并不相同，所以在针对他们的具体合约写法也不相同。这里我以Ethereum为例来进行描述：

1. 随机数选取的操作流程
2. 根据自己业务需要，选取一个合适的正整数n（后面会对取值做介绍），并设定可以获取最终结果的区块号为当前区块的n个区块之后。
3. 等待链上产生n个区块的时间，在第n+1个区块的时候，发起交易调用合约的接口，从而触发生成随机数的流程。
4. 合约判断当前交易所在的区块号与选取n时所在的区块号之差是否大于n。如果为真，则流程继续；如果为假，则获取失败。
5. 从当前区块的上一个区块起，连续取n个区块的哈希，分别为h1、h2、h3…hn
6. 计算种子s=f(…f(f(f(h1, h2), h3),…hn)，这里f是XOR运算。
7. 计算s对N求余得r=s mod N，最终r为区间[0,N)整数随机数。

整个操作流程图如下：

开始

选一个正整数n并令t=(当前区块数)+n

等待链上产生第n+1个区块后，外部调用合约生成随机数接口

从上一个区块起，连续取n个区块的哈希，分别为h1、h2、h3…hn

(当前区块数)>t

计算种子

s=f(…f(f(f(h1, h2), h3),…hn)

这里f是XOR运算

计算s对N求余得

r=s mod N

最终r为区间[0,N)整数随机数

结束

是

否

1. 关于流程点的原理描述
2. 对于流程1：

从区块链的实现原理来说，n的取值越大，获得的随机数遭到恶意控制的几率越小。假如n取1，那么随机数将最终由距离结果给出最近的1个区块来决定。这时候，如果某个矿工刚好有这个区块的挖掘权，那么他就可以全权控制这个随机数的产生。虽然该矿工有很大程度上跟需求随机数的合约没有利益关系，但这点并不能保证。如果需求随机数的合约刚好是一个类似于彩票的合约，那么这个矿工就可以控制开奖结果，从而使自己受益最大化。当n取值变大的时候，随机数的最终结果是跟最近连续n个区块的哈希值有关。同样是上面的例子，矿工需要连续获得最近n个区块的挖矿权才能控制最终结果，这在区块链的挖矿算法设计上基本是不可能发生的，可以保证结果不会被恶意干预。但是n的取值也不能无限大，一是n越大，需要等待的时间越长，n太大会导致体验很差。而是因为合约中的代码基本不能获取从创世区块到现在的所有区块的哈希值，像在Ethereum只能获取256个，因此它的取值只能是1到256。

1. 对于流程4、5：

在Ethereum中，每个区块的哈希值是个256位的二进制数，一般显示为一个64位的16进制数。这里我们从给出结果的交易所在的区块的前一个区块起，把取到的n个哈希值进行XOR运算，代码表示为：

1. bytes32 hash = blockhash(block.number - 1);
2. **for** (uint i = 2; i <= n; i++) {
3. hash ^= blockhash(block.number - i);
4. }
5. 对于流程6：

根据所取的随机数的范围来决定后续的操作。假如这里要取的是一个0~9的一位随机数，只需要把上一步得到的哈希值强转成无符号整型，再对10求余即可。代码如下：

1. uint8 random = uint8(uint256(hash) % 10)

这种方式得来的随机数在0~9的范围内是近似平均分布的，因为在之前的描述中说过，每个区块的哈希值是完全随机的，因此对多个哈希按位取XOR后得到的结果也是随机的。如果把它强转成无符号整型，就相当于得到了一个平均分布在1~2256之间的整数，由于2256非常大，相当于1后面77个0，因此得到的0~9中各个数字的出现概率近似是一样的。大约在每1076次选取中才会出现1次的偏差，完全可以忽略不计。

4、特殊情况说明：

在流程6中，最终产生的是左闭右开区间[0,N)直接的整数随机整数。他的偏差情况是每（2256/N）次选取中，会出现一次偏差。如果N趋近于2256，那么偏差率会增大。不过好在这个数值非常大，平时也不会经常用到，对于N的选取，使用者根据自己的业务逻辑自行判断即可。

对于确实需要很大的N或者需要取带有小数的随机数时，可以使用拆分的方法来进行选取。例如，在保留两位小数的非整数随机数选取中，可以把数字分成整数部分和小数部分，再分别用上述流程求出整数部分和小数部分的随机数，然后组合再一起即可。又例如，在超大随机数的选取过程中，可以把随机数分成每m个数字一组，然后对每一组用上述流程取随机数，最后再组合。

由于后续的处理方法不同，得到最终随机数的范围也不同。使用者完全可以根据自己的需要自行设计选取方法。例如需求带小数的部分，可以先算出一个整数随机数，再进行移位处理等等，适用范围非常广泛。

**5、本发明的关键点和欲保护点是什么？**（请提炼出本发明的技术创新点，以提醒专利代理人注意，便于其撰写权利要求书）*。*

1、从区块链中选取连续的区块哈希作为随机数的产生源，避免了只取一个哈希的时候可能带来的作假行为。相比于上述提到的两种其他实现方案，它避免了中心化嫌疑，并且实现起来简单方便，不依赖第三方协助。

2、从哈希值转变为随机数的过程，包括上面提到的对m取余并证明他们基本属于平均分布的部分。

**6、能实现本发明目的的其他替代方案**（尽量多列举可实现本发明的的其他替代方案，以便充分公开本发明）

第二大点中描述的那两个方案都可替代，但是各有各的缺点。