随机链白皮书

摘要

4、GDAO 的资金来源与用途

5、GDAO 官网、客户端与轻客户端

四、随机通证的发行计划与随机链的开发计划

发行数量

挖矿速度

燃烧速度与手续费

摘要

我们在日常生活中频繁接触随机数，它与信息安全、资金安全息息相关。然而随机数的安全问题并不被人重视，它往往依赖于涉及随机数的服务提供方的自身安全体系，有着被内部攻击或第三方攻击的风险。

区块链技术为我们提供了一条思路 :使用全网节点生成去中心化的随机数，这样的随机数具有极难被预测和重现的特性，从而解决了随机数的安全问题。在本文中，我们将介绍将这个想法落地实现的方法，一个提供高频稳定随机数服务的区块链产品——随机链。

随机链的基本结构由两条相互关联但作用不同的链组成，主链高速出块生成随机数，采取类 DPOS 的共识机制；辅链低速安全地整合信息，采取 POW 的共识机制。随机链通过简洁有效的设计避免冗余信息的累赘，保证产生随机数的随机性质和速度。

随机链所有使用者均默认参与 GDAO, 它包含的链上功能和链下社区将起到维护双链的正常运行、保持用户活性、为用户提供便于理解的随机数服务的作用。用户将可以通过 GDAO 官方网站、客户端、轻客户端等多种途径接触 GDAO 社区，使用随机链提供的随机数服务。

一、随机数的需求背景

1、随机数的广泛应用与伪随机数的生成

随机数在当前信息时代中的应用非常广泛。随机的意义在于，它的不可预知性和不可操控性，这可以带来公正和安全，也可以带来仿真和稳定。可以说我们每个人的生活中都经常直接使用了随机数，或者间接接触了大量利用随机数建立的应用。

真正的随机数是如理想状态下的抛硬币这样，自然存在的随机数，它具有几个特性：

第一点是统计无偏性，它在统计学上应当不存在偏差，其随机数列要满足一些统计性质。

第二点是不可预测性，就是说一个已知的任意长度的随机数列，都无法为接下来出现的随机数提供信息，或者说使我们得以预测下一个随机数。

第三点是不可重现性，意思是我们无法通过复制一个随机数（列）产生时的状态，来保证一个随机的过程产生相同的随机数。

然而，我们使用的随机数都不是真正自然存在的随机数，它们事实上都是在计算机中通过一个伪随机过程产生的伪随机数。一般的伪随机数生成过程化简后可以归纳为这样一个模式：事先确定好一个能产生“看起来”随机的结果的算法，它的结果可以想象成一个极大的“看起来”满足随机性

质的随机数表；根据一些条件的组合，如特殊密钥、时间戳等等来作为种子，利用种子来作为算法的基础值，或者说确定在随机数表中的起始位置；然后把生成次数作为加密算法中的加值，这可以想象为在随机数表中的搜索间隔，以这样的过程来生成每一个随机数。

这样生成的伪随机数不可能具有真随机数性质的第三点性质即不可重现性，因为如果复制出产生随机数时的状态——这包括随机数表或算法、随机种子生成次数等信息，就一定能产生出相同的随机数。但如果这样生成的伪随机数能够通过一些关于随机性的统计测试证明其具有统计无偏性，同时其随机数生成算法设置的足够合理使得其极难被预测，那么就可以将其视为相对安全的。对于这样的伪随机数的使用者，只要保护好随机种子，就能确保自己使用的随机数不是在其他人控制下产生的。

2、随机数的安全与现有的解决方案

随机数的安全性有两个方面。

第一点是要保证自己使用的伪随机数能满足前述的统计无偏性并且极难被预测，这通常与生成随机数算法的设计和随机种子的复杂程度有关。不过这一点并不难被保证，因为当前在很多领域已经有多种公开的优秀算法，如果使用者在安全方面足够小心，使用合适的算法和复杂的随机种子，就不会在这一点上被攻击。

第二点也是最重要的一点，就是随机种子的安全，这是本文想讨论的关键之处。如前文所述，如果同时掌握了随机数生成算法和随机种子，就等同于控制了这一系列随机数，打破了随机数的不可重现性和不可预测性，换句话说就是可以提前掌握将要生成的随机数。一般而言，为了保证随机数的公正性，生成算法都是公开开源的，那么随机种子的安全性就至关重要。

当前有很多涉及随机数的服务，如网络通信加密、验证码、彩票，但这些服务的随机数种子都放置在服务方手中或者是由服务方提供。既然随机数的安全依赖于随机种子的安全，那么也就是说，这些涉及随机数的服务的安全就依赖于服务的提供方。如果服务的提供方被内部攻击或第三方攻击，比如网络协议漏洞、验证网站被黑客攻击数据库、彩票方形方内部人员作弊，那么随机数的安全性能就无法得到保证，用户在不知情的情况下继续使用这样的随机数将面临极大的风险。因此在现有的框架下，想要增加随机数的安全性，只能从随机数提供方的安全入手，但是并非每一个提供方在此方面都有足够的实力或有足够的重视。

3、去中心化的随机数生成

区块链技术已经快要迈入第十个年头，保证其广受关注与蓬勃发展的关键是其去中心化的特性。在我们思考随机数安全的问题时，正是区块链的去中心化特性给出了一个可能的

解决方案：链上区块一经写定即广播至全网而不可更改，每一个区块的哈希摘要都与其中包含的信息一样极难预测也无法在时间流逝后重现，如果将随机数与这些区块的哈希摘要挂钩，每一个区块对应一个新的随机数，那么这样的随机数列同样也会继承这种极难预测性与极难重现性。

其实这种解决方案同样没有跳出算法加随机种子这种生成随机数的框架。但是它的算法与区块链的技术设计挂钩，一个优秀的开源设计可以保证其安全性；随机种子与区块的生成者、区块内的交易信息和附加信息、链上的信息都相关，使得它极难被预测和重现，这也就是保证了种子的安全性。随机数的生成不再依赖于服务方持有的随机种子的安全，而是由区块链全网用户生成，算法与种子的双重安全保证使这样生成的随机数根本无法被控制或攻击，其安全性得到了极大提升。

由此可见，利用区块链的去中心化特性生成随机数确实是对于随机数安全问题的一个可能的解决方案。下文中将介绍如何将这种解决方案真正落地为一个区块链产品。

二、随机链技术设计

1、什么是随机链

我们的目标已经很明确，就是要设计一个产品，它要能够高频而稳定地生成去中心化的安全的随机数。经过上一节的讨论，这个目标可以具体化为设计一个能够高频而稳定地出块的区块链——随机链。之前的去中心化产品都不能满足这个要求，其一是因为产生随机数的速度不够或者说出块速度不够；其二就是它们结构设计的侧重点一般放在交易记账或智能合约以及侧链开发等内容上，而我们的重心是生成去中心化的随机数，对这个目标而言，过分繁杂的内容是一种累赘，它们不仅没有必要，同时还可能影响区块生成的速度和系统的安全性。

针对产品设计的目标，我们将使用 POW 与 DPOS 结合的共识机制，同时维护相互关联的两条链，它们之间的关系类似于计算机的内存和硬盘：第一条“内存链”称作主链，它是整个产品的重点，其功能就是快速出块生成去中心化的随机数，其上记录的信息很少，这是出块速度的保证；第二条“硬盘链”称作辅链，它能完成一般区块链的任务如记账、简单的合约等等，同时还会对辅链的随机数内容做整合存储和面向人类理解的翻译。在维护共识机制和双链的运作中还需要一个 GDAO 的配合。包含主链、辅链、GDAO 的这样一个整体区块链产品，就是随机链。

2、随机链 GDAO 简介

GDAO（Global Distributed Autonomous Organization），即全球分布式自治组织，是随机链作为一个区块链产品，为了保证其正常运作而设立的一个所有用户全部参与的非赢利性组织，它的功能和性质在随机链的架构中就已写定。关于 GDAO 的设定、功能和运作方式将在下一章详述，但由于在接下来的介绍过程中会多次提及 GDAO，所以在此先做简介。

3、共识机制的选择

区块链的共识机制让全网使用者能达成一致，使区块链具有了去中心化的特性。目前存在的各种共识机制各有优势和劣势，经过对于随机链的需求进行有针对性的分析设计后，在随机链中将使用到 POW 与 DPOS 共识机制。

POW（Proof of Work）即工作量证明，是经典的比特币使用的共识机制。在 POW 中，每个区块的 hash 值的最前方必须有与网络难度相关的若干个 0，这需要通过大量的尝试计算来得出，因此一个节点率先得到合理的 hash 值说明它拥有大量的算力，从而在竞争中获得了区块的产生权。接下来该节点会将得到的区块广播至全网络并得到其它节点的接受。POW 机制在最大程度上保证了去中心化，但是需要浪费大量的算力进行无意义的计算，同时需要较长的周期来达成共识，无法进行快速的出块。

DPOS（Delegated Proof of Stake）即股份授权证明，是以比特股为代表的较新的一种共识机制。它的原理是让每一个持有者进行投票，由此产生若干位代表 ，我们可以将其理解为若干个超级节点或者矿池，而这若干个超级节点彼此的权利是完全相等的，它们将在接下来的一段时间之内轮流按照列表的顺序被委托来产生新的区块，而如果轮到某个节点时，该节点没能成功产生区块，它就会被跳过并从列表中去除。每过一段时间都会选出新的代表。DPOS 机制是在区块产生之前就达成了共识，因此可以在很快的时间内产生新的确定的区块，它很适合随机链对于高频产生随机数的需求。但它的缺点是去中心化程度稍稍不如 POW，所以在安全性上需要更加严谨的设计来进行保证。

4、交易类型

随机链上的交易类型除了在区块链中常见的生成区块的“奖励交易”和用户之间的“普通交易”之外，还有与 GDAO 相关的“燃烧交易”。通证在随机链中有使用资格的意义，因此每过一段时间会进行一定数额的扣除。每当一个用户使用与 GDAO 相关的服务或者进行“奖励交易”与“普通交易”时，GDAO 将首先检查其上一次扣除通证的时间戳，如果与当前时间戳相距一定时间以上，将会在提供服务或完成交易之前，在链上广播一个对该地址直接扣除一定数量通证而没有任何收入方的交易，这种交易就称为 “燃烧交易”。

5、双链结构

随机链中包含两条相互关联的链：主链和辅链。主链使用DPOS 共识机制，辅链使用 POW 共识机制。链上记录的信息主要有交易信息和面向人类理解的随机数翻译信息。

主链的作用是高速出块以生成随机数，它以一个很高的频率产生区块（初始速度为一秒一个）。在生成每一个区块之前首先以 DPOS 机制在候选列表中按顺位搜索在线有能力的委托节点，此候选列表由 GDAO 根据辅链的信息和投票信息共同得出。其中包含的交易信息的第一笔是对于该委托节点的“奖励交易”，其后的每一笔交易是该委托节点在当前时间段内监听到的“燃烧交易”。在验证并记录“燃烧交易”时只需验证地址对应的上次燃烧的时间戳，因此主链的交易数量并不少，但由于都是燃烧交易，因此出块速度极快。主链上每一个区块的附加信息中会简单记录由该区块的 hash 值引出的大随机数。

辅链使用 POW 共识机制，每五分钟产生一个区块（在辅链每两个区块之间约有 300 个主链区块）。辅链的作用是验证并记录当前时间段内的“普通交易”，同时将主链上当前时间段内产生的“奖励交易”和“燃烧交易”整合并记录。辅链还会对主链上产生的随机数进行整理，生成若干种基础的随机数并进行记录，以方便用户进行查找和验证。除此之外，GDAO 会记录辅链的区块在以 POW 共识机制竞争生成时进

行了区块广播的一些可信节点，作为候选列表的一部分供主链在若干时间后查找委托节点时使用。

综合起来，主链与辅链功能不同但互相紧密结合：主链记录很少信息，出块速度快，负责生成随机数并燃烧通证，它需要使用到记录在辅链上的通证燃烧时间戳，并使用由 GDAO 提供的部分来自辅链的委托节点列表；辅链记录主要信息，出块速度慢，负责记录所有交易信息同时整理主链上产生的随机数，完成随机链中对于高频性和即时性需求相对较低的工作。主链的 DPOS 共识机制在使用了结合辅链节点和投票节点两部分的委托节点列表之后变得更加安全；辅链的 POW 共识机制使得随机链去中心化的特性更加可靠。

6、智能合约与侧链

随机链的辅链将拥有智能合约功能，合约能从主链读取数据但不能向主链写入数据。为了避免过多的合约成为随机链的累赘，影响区块运行时的速度，智能合约会特化为只能使用一些关于随机数的特定功能的简单合约。

我们不认为侧链是随机链实现其产品功能的必须品，因此在初期设计中，为了使随机链能够稳定快速地运行，不会支持侧链的开发。

如有必要，复杂合约或侧链的端口可在将来与 GDAO 社区协商，通过后进行设置。

7、整体流程

在本章的最后我们将回顾随机链的整体运行流程。

主链上的区块以 M_0，M_1，M_2 记，辅链上的区块以 S_0，S_1，S_2 记。暂时假设每两个辅链区块之间恰好 300 个主链区块，M_0 与 S_0 同时出现。

在 S_1 生成后，GDAO 整合参与竞争生成 S_1 的节点和 DPOS 机制投票得出的节点提供一个超过 300 个节点的委托列表 L_1 给主链。

从 M_{451} 开始到 M_{750}，主链以 DPOS 共识机制从 L_1 中选择委托节点，委托节点监听“燃烧交易”并获得奖励通证来完成该区块。

S_1 生成后，直到 M_{450} 生成，辅链的区块生成竞争者监听这期间的“普通交易”，并整理 M_{151} 到 M_{450} 之间的主链区块信息，打包生成区块并进行算力竞争，完成 S_2 的生成。

以上是一个流程的循环。

三、随机链 GDAO

1、为什么要有随机链 GDAO

DAO 指的是分布式自治组织。一个 DAO 能通过一系列公开公正的规则在无人管理、监督、干预的情况下自主完成一些功能。每一个区块链产品比如比特币、比特股都可以被称为一个 DAO，随机链作为一个提供特殊服务的区块链产品也是一个 DAO。

随机链在设计中并不支持复杂的智能合约功能，从而也不支持链上 DAO 的创建，所以随机链上只会存在这一个初始的 DAO。随机链在链上需要“燃烧”使用通证来保证用户活性和主链的正常运作，同时，随机链还有很多面向用户的功能要在链下完成，必须有一个去中心化的组织来持续完成这些工作，因此我们给随机链全用户参与的 DAO 特别命名为 GDAO。

2、随机链通证与 GDAO 的基本功能

通证是随机链使用者的使用凭证。只要持有通证就是随机链的用户，可以使用基本的查询功能。通证数额保持在一定额度以上的用户可以使用 GDAO 提供的全部功能。

GDAO 首先发行随机链的第一批初始通证给募资方，作为它们的使用凭证。GDAO 在随机链上还有最基本的功能需要完成，就是作为一个特殊节点广播“燃烧交易”和完

成主链 DPOS 的节点选举。这两点功能在第二章技术设计中已经详述。

3、GDAO 的社区功能

GDAO 在链下以社区的方式行使职能。随机链将成立两个社区：技术社区和用户社区。

技术社区是 GDAO 的核心组成，它是一个随机链的开源社区。它的任务包括更新随机链底层代码，以适应新的随机数生成技术或应对可能存在的攻击；在用户社区有需求的情况下，给随机链添加更多面向人类理解方式的功能，也可能添加不影响主链运行的智能合约和侧链功能；维护 GDAO 官网、客户端、轻客户端的架构，满足用户社区的需求。

用户社区是随机链大部分使用者接触到的社区。它的任务包括维持 GDAO 运营；接受用户的使用反馈并与技术社区联系，以更新随机链功能和 GDAO 官网、客户端、轻客户端的功能。

4、GDAO 的资金来源与用途

GDAO 的作用是维护随机链的正常运行发展，是一个非赢利性组织，但是为了鼓励社区成员作出贡献，需要有一部分资金用于社区成员的奖励。GDAO 的初始资金来自于初始募集资金的一部分。在随机链和 GDAO 发展稳定且初始资金消耗殆尽之后，可以通过社区全体的表决，将通证

燃烧的一部分转化为 GDAO 的收入，全部奖励给社区成员。

5、GDAO 官网、客户端与轻客户端

一般用户与 GDAO 交互有三个途径：GDAO 官网、客户端和轻客户端，这三个途径都由技术社区和用户社区共同维护。

这些交互途径的主要作用是将随机链上的随机数翻译为便于人类理解的随机数以及一些特定类型的随机数。用户将分为两个类型，第一类只能使用通证交易和辅链随机数查询、DPOS 节点投票等功能，第二类能使用 GDAO 提供的全部服务包括用户社区支持、即时的主链随机数及相关衍生随机数查询功能。成为第二类用户的条件是保持通证额度在一定限额之上或使用 GDAO 提供的客户端同步完整的随机链区块。

官网和轻客户端功能类似，只是在使用平台上的区别，用户在使用功能时将会首先通过通证额度的检测。

使用客户端将会同步完整的随机链区块，这也使得用户能接触完整的随机链功能或参与主链、辅链的区块生成。

四、随机通证的发行计划与随机链的开发计划