解读Cellula：致敬POW挖矿的游戏化资产发行协议

作者：Nickaqiao & Faust，极客web3

自2017年ERC-20资产风靡区块链圈以来，Web3就进入了资产发行的低门槛时代，各路项目方凭借ID0、IC0等方式肆意发行自定义代币或NFT，且大多存在强控盘或信息不透明问题，RugPull现象频发，各路镰刀俨然把IC0、ID0当做割韭菜的绝佳途径。

时至今日，常规的ID0和IC0已经充分暴露出了其在公平性上的缺陷，人们一直都希望有较为公平可靠的资产发行协议，解决新项目TGE时的诸多问题。虽然一些创意十足的项目单方面提出了自己的“公平的经济模型”，但往往没有进行通用化推广，最后这类经济模型大多沦为“具体案例”而不是“一套抽象出来的协议”。

那么，什么样的模式是更公平可靠的资产分发方式？什么样的方案能作为一套通用协议？本文将要展开介绍的Cellula为解决上述问题提供了全新视角，他们实现了一个模拟POW的资产分发层，利用虚拟工作量证明（vPOW）将资产分发过程“挖矿化”，以模拟BTC实现更公平的资产分配范式。

虽然该项目被许多人视为Gamefi，但由于其分发的游戏内奖励可以设置为任意类型的Token，Cellula理论上可以作为一个有POW效应的资产分发平台，为Web3资产发行带来了更广阔的前景和想象空间，甚至于称为“一场致敬BTC挖矿的社会实验”也不为过。



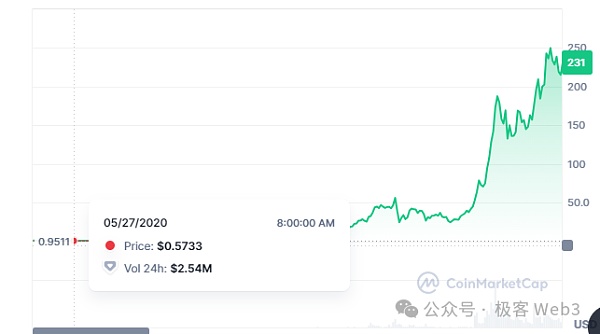
## POW和vPOW：结果不可预测的彩票抽奖

其实无论是正宗的POW还是POS，或是今天要讲的vPOW，本质都是设置一套输出结果不可预测/难预测的算法，通过输出结果来进行“彩票抽奖”。BTC矿工们要在本地构造出满足限制条件的区块，提交给网络中的全节点通过共识，才能拿到出块奖励。至于限制条件，是要让构造出的区块的Hash满足特殊要求，比如前缀是6个0。

由于区块Hash的生成结果不可预测/难预测，要构造出符合条件的区块，只能不断的变更给定算法的输入参数，这一过程需要暴力穷举，对矿工的硬件设备有很高要求。

简而言之，BTC挖矿通过SHA-256哈希算法的不可预测性/难预测性，实现了一套全网矿工在线参与的“彩票抽奖”系统，这种设计以电能为代价，确保了参与形式上的Permissionless。

此外，POW是一种更公平的资产分配方式，主流的POW公链中项目方控盘的难度比POS公链大很多，而在很多POS公链或IC0、ID0方案里，项目方强控盘的案例比比皆是。



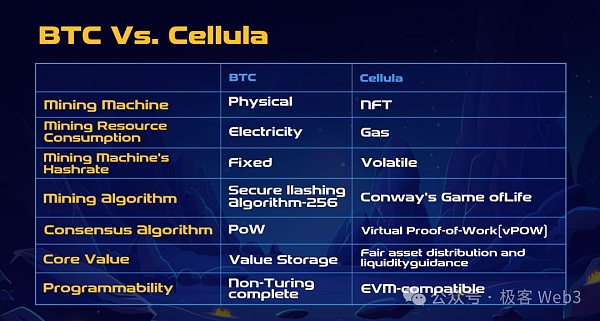
（Solana在FTX操纵下，仅在2020~2021年就暴涨了小500倍，这对后入场的Validator运行者而言极不友好）

比如，Solana币价在FTX和SBF操纵下，曾在2019~2021年暴涨近1000倍，而很多Solana验证节点运行者是其早期投资人，它们获得筹码的成本近0，这严重打破了资产分发上的公平性。虽然POW当中项目方也有控盘的空间，但程度往往要比在POS中轻得多。

问题在于，POW的模式往往被应用于底层公链而非DAPP的资产发行层，我们能否以一套链上可实现的方案，模拟出POW的效果？如果能，就可以实现一套比IC0、ID0等强控盘方案更公平可靠的资产分发协议，搭配一些游戏场景，可以做出一些有意思的Gamefi（当然实际用途不仅限于游戏，还可以为其他项目提供一套公平的资产分发方案）。

所以关键是，如果我们要在链上资产发行层模拟出POW的效果，该怎么做呢？在本文介绍的Gamefi项目Cellula中，通过引入著名的“康威生命游戏”算法，为链上虚拟的数字实体（称为“BitLife”）分配算力。说白了像是让一帮人在自己的培养皿中繁育细胞集群，随着时间推进，谁的培养皿中存活细胞越多，折算后得到的挖矿算力越高，越可能获得挖矿奖励。

简而言之，Cellula把传统POW的哈希计算，换成了另一种结果不可预测/难预测的计算方式，替换了“Proof of Work”中的“Work”形式。在Cellula的思路下，关键在于如何获得存活细胞数更多的培养皿（BitLife），而推演BitLife的状态变化需要耗费计算资源，本质是把BTC挖矿执行的哈希算法变为推演康威生命游戏的特定算法，这被称为vPOW（Virtual POW）。

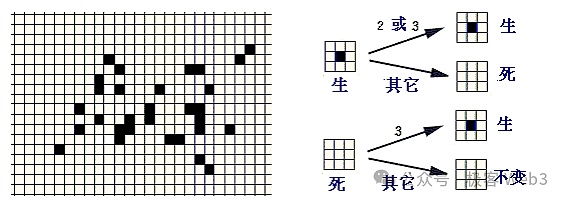


下面让我们对vPOW的机制设计展开更深入的解析，不得不说，这里的很多细节非常有趣，可以说Cellula在做的事情之一，是通过链上NFT交易链条来模拟BTC的矿机产业链模型。

## vPOW的核心：康威生命游戏与BitLife

在对Cellula的机制设计展开解读前，让我们先来看看vPOW最重要的核心——“康威生命游戏”，它最早可追溯到冯诺依曼于1950年提出的“细胞自动机”概念，而后数学家约翰·康威在1970年正式提出“康威生命游戏”，用算法模拟自然界生命的演化规律。

假设我们有一个培养皿，将其按照二维坐标划分出一堆小方格，然后我们对培养皿进行“初始设置”，让一些活细胞占据部分方格，此后这些细胞的生死状态将随时间演化，逐渐呈现出形态复杂的细胞集群（大家可以想像霉菌是怎么繁殖的）。这本质是一个二维格子游戏，规则非常简单：



每个细胞有两种状态：存活/死亡，就像扫雷游戏一样，每个细胞和自己周围八个方格上的细胞会产生互动（如图，黑色为存活，白色为死亡）；

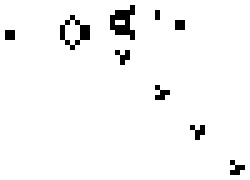
假设某细胞存活，但周围8格内存活细胞小于2个（0或1），则该细胞进入死亡状态；

某细胞存活，且周围有2个或3个存活细胞时，该细胞仍保持存活；

细胞为存活状态，周围有超过3个存活细胞时，该细胞进入死亡状态（模拟生命数量过多而争抢资源的场景）；

当前细胞为死亡状态，但周围有3个存活细胞时，该细胞转入存活状态（模拟细胞增殖)

所以很简单，在二维培养皿中给定细胞状态的初始模式，然后按照上述规则，细胞状态会随时间推移，不断地演化迭代，产生千变万化的结果。你甚至能用康威生命游戏模拟出计算机的效果。



比如说，培养皿中每个细胞的生/死，对应着二进制的0/1，你可以把细胞初始状态视为“输入参数”，每个细胞的生死（0或1）代表输入数据，之后细胞状态会按照初始模式开始演变，每一轮状态变化就相当于计算过程中的一步操作，经过一段时间后得到的状态，可以看作“输出”。

只要布置适当的初始模式，康威生命游戏能在经过若干代演变后，输出特定结果。由于初始模式千变万化，可以利用其特性模拟出彩票抽奖的效果。我们可以设置限制条件，每个玩家随机选择一批初始模式，经过100代演化后，输出结果满足xx特征的培养皿主人有资格获取奖励，这样就和BTC挖矿的思路比较接近了：

“系统先限定哪类输出结果符合要求，参与者向给定算法输入随机的初始值，尝试得到符合要求的输出结果”。由于待尝试的初始输入参数非常多（几乎是天量），你必须要付出很大努力才能撞大运中奖，这正是工作量证明的逻辑：矿工必须要付出一定工作量才能获取奖励。

在理解了Cellula和康威生命游戏的基本思想后，我们再看他具体的细节设计。Cellula把前面说的“培养皿”分为9\*9=81个方格，每个方格上的细胞有生/死两种状态(对应二进制的0和1），这样一来，按照排列组合，培养皿中的细胞初始状态有2^81种，这个数字等于1万亿的平方（基本是个天文数字）。

然后，玩家要做的是对培养皿的初始模式（输入参数）进行选择。BitLife充当了培养皿的实体（实际是个NFT），包含81个方格，每个方格上放置一个细胞（可能有生/死两种状态，空置的方格等价于死细胞）。然后，BitLife中每3\*3=9个相邻方格构成一个BitCell，每个BitLife由2~9个BitCell拼接而成（如果你构造的Bitlife不足9个Bitcell，有些地方就被空置，默认都是死细胞）。

按照排列组合，BitCell（3\*3方格）有2^9种初始模式，玩家要做的就是随机挑选不同模式的多个BitCell组合起来，构造出一个BitLife。简单来解释，就是为自己的培养皿随便找一个初始模式，然后前面讲过，不同的初始模式总计有2^81种，是个天文数字。所以留给参与者的选择空间非常大，这就和BTC挖矿里用SHA-256的场景有点像。



BitLife的细胞状态会随着区块高度的增加而变化。Cellula按照不同区块高度下BitLife的状态来分配算力。给定一个区块高度，包含的存活细胞越多的BitLife拥有的算力越高，这就相当于创造了一种虚拟矿机。

这里举个具体的例子，Cellula参与者要在链下穷举BitLife的2^81种初始模式，预测每种模式演化后的状态，然后看能否符合奖励系统的要求。假设现在的区块高度为800，而系统提出要求：区块高度为1000时，存活细胞数最多的BitLife能获得最多的奖励，那么参与者的目标会很明确：

在区块高度为800时，我要获取某个模式的BitLife，该模式的BitLife在区块高度为1000时，能比其他BitLife有更多存活细胞。

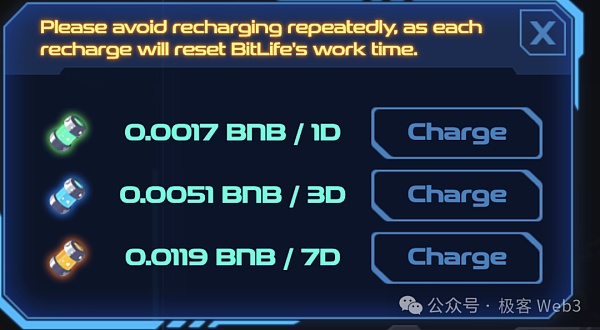
这其实就是Cellula的核心玩法，你的目标就是自己构造/从别人手上买到最有可能获得挖矿奖励的BitLife，这种模式就相当于允许普通散户/高级散户自己研发矿机，然后你可以把自己造的矿机卖给别人，可以购买别人的矿机来挖矿。如果你要自己造矿机，那就要在链下自行推演出不同模式的BitLife的状态演化，这会耗费计算资源；如果你要买别人的矿机，其实就是买不同初始模式的Bitlife，你要自行判断这些BitLife未来的状态变化，所以你还是要在链下自行计算。这其实是整个Cellula游戏设计中非常有趣的一个点。

在理解了游戏的核心机制后，我们再来看其他细节：其实BitLife中的活细胞可以溢出到初始的9\*9格子外，存活的细胞数可以远大于9\*9个，没有边界限制。如图所示，如果某个BitLife包含的活跃细胞数不断增多，其分配到的挖矿算力也会越来越高，而如果BitLife的初始模式选择不当，活细胞数越来越少，算力也会越来越低。





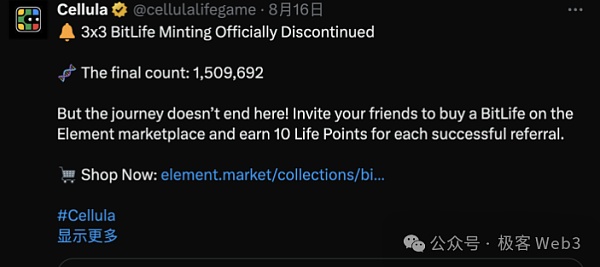
然后，系统会每隔5分钟分发一定的挖矿奖励（游戏里称为能量点），根据每个BitLife在网络中的算力份额来分配。



在Cellula中，玩家合成BitLife的过程，就是一个“制造”新矿机的过程。我们前面曾提到，BitLife的实体是一个NFT，BitLife在链上被mint出来后，要进行“充电”操作才能启动挖矿，单次充电有效期为1天、3天和7天，需要支付一笔小额手续费，且到期后需要继续充电。

这里要说下，为了鼓励用户多去对BitLife进行充电，Cellula设置了一个“充电抽奖”功能，你每次发起充电操作时都可能被选中，获得一些额外奖励（就是说这个奖励和挖矿奖励独立开）。这块的设计我们会在后面Analysoor算法的部分简单介绍下。

按照Cellula官方的规则，目前包含3\*3个Bitcell（也就是包含81个小方格）的BitLife铸造已经停止，玩家们一共铸造了150多万个此类BitLife，未来新用户可以在二级市场购买BitLife并进行充电挖矿。按照官方的解释，限量铸造是为了维持游戏生态的稳定，防止有科学家无限的铸造BitLife NFT导致矿机价值缩水。

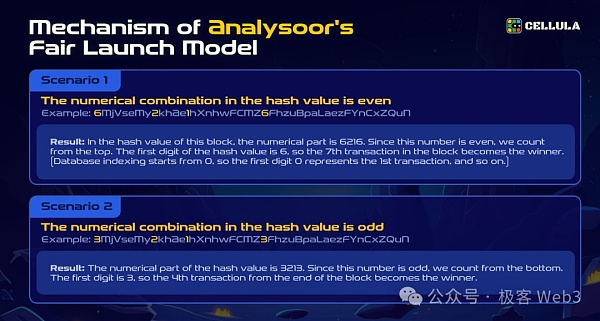


而且在未来，Cellula将引入类似于矿机制造商的角色，这个角色基于许可制，要质押代币、公示销售渠道、具有一定社区规模和影响力等，这些制造商将负责铸造和销售包含4x4个BitCell的BitLife，也就是包含16\*9=144个小方格。制造商可以铸造的BitLife量，将受到其质押代币量的限制。

在此我们大致把vPOW涉及的核心概念通俗解释了一遍。vPOW的本质是基于给定规则的计算模型，参与者可以通过优化策略来参与竞争，通过游戏化的方式进行资产发行与分配。Cellula模拟了BTC矿机市场的运作形式，替换了工作量证明中的计算任务形式，由于挖矿算力的分配方式可以动态调整，任何模式的BitLife都未必是全局最优的，今天细胞存活数最多的BitLife，明天就可能被其他BitLife超越，这会导致复杂的涌现现象和动态的策略。

## Analysoor抽奖算法和VRGDAs指数定价曲线

在前面我们主要针对康威生命游戏及Cellula的核心机制进行了展开式的解读，下面我们再来考察下游戏中包含的其他设计。上面我们提到Cellula有个充电抽奖环节，这里用到了名为Analysoor的随机数输出算法，它把区块哈希作为随机数生成器的输入参数，抽出每个区块里参与充电者中的赢家，引入了一种彩票制度。

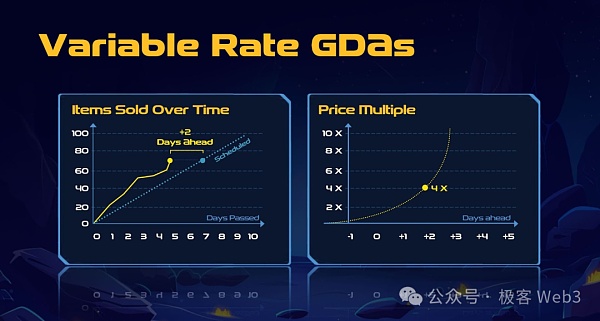


比如在Analysoor的设计中，当前BNB Chain的区块哈希为6mjv....的一长串字符串，里面包含4个数字：6、2、1、6。按照这几个数字在字符串中的排序，第一个数字是6，最后一个数字是6，为偶数，将从前往后计数。提取出来的数字是从0开始计数的，于是数字6对应的交易排序是7，就从当前区块里把第7个充电玩家视为中奖者。当然具体的设计可以更灵活，这里只是举个例子。上述随机性的抽奖算法可以有效激励玩家多充电，调动游戏内生态的活跃度。

此外，在Cellula的整个交易模型中，有一个问题：某种模式的BitLife一旦被某个大佬Mint出来，其采用的BitCell组合方案会被公开，其他人也可以“跟风”，按照相同的组合方案去mint BitLife，最后很容易引发一堆人跟风的现象，严重影响游戏结果的随机性。为此，Cellula引入了可变速率渐进荷兰拍卖（VRGDAs），这是由Paradigm开发的定价算法，会动态调整价格——当铸造量超预期时抬价，铸造量不及预期时降价。

假设初始预期是每天铸造10个A类NFT，起始价格为1个CKB。本来到了第5天，预期人们共计铸造50个A类NFT，但因为很多人跟风，铸造量达到70个，这相当于原计划到第7天实现的目标。为了限速，要通过指数定价曲线快速提高铸造价格，单价涨到4个CKB来抑制铸造行为。

如果到第15天，只铸造了120个（原计划此时铸造共150个），没有达到预期销量，这时会下调价格，刺激铸造量。



在上述场景中，当某类BitLife在短时间内被大量铸造时，该类NFT的铸造价格会指数级增长，这种剧烈的价格上涨可以有效的防住科学家。

## 总结：从玩家博弈的视角看待Cellula

在讲完了Cellula的全部核心设计后，我们不妨从玩家的博弈视角来看待这一脑洞大开的游戏机制。首先，在vPOW中有很多参与方，每个参与方的策略都不同，以一级发行市场为例，一个”科学家“可以写代码，组合不同的BitCell去找到算力更高的BitLife，获取更高的挖矿收益，同时会存在一些MEV玩家，他们监听链上的铸造事件，当发现某个NB的科学家铸造了某类型的BitLife时，他们也会跟风大量铸造。

但由于VRGDAs指数型定价算法的存在，单一类型的BitLife铸造价格可以指数级增长，这样可以有效的防住科学家（反女巫），当然也会对BitLife/矿机进行定价，如果某类矿机的算力高，它的铸造/生产价格也会很高，后面流通在二级市场的价格会参考生产价，进而传导到整个供应链当中。

类比BTC矿机的发行过程，科学家发现某类型BitLife的算力高，就好像矿机公司研发出新的芯片，MEV玩家跟风铸造，就好像一级经销商完成矿机的定价，而后的二级市场交易就类似于散户从经销商手中购买设备。

不同的是相比现实世界的矿机研发，科学家发现新的BitLife的速度会快很多，而且任何人都可以参与到BitLife的状态推演中，很大程度上相当于降低了矿机的研发权力，“人人都有机会成为科学家”，这对于大多数人而言是更为友好的，也是现实中矿机生产链条中不可能出现的。

而对于项目方本身而言，采用POW式的资产分发方案本身就削弱了他的权力，所以，无论是科学家还是项目方，亦或是普通玩家，都无法单方面控制市场。在矿机铸造环节以及发行环节，就产生了这三方的博弈，没有一方能够完全垄断市场，这可以形成一种动态的平衡。

总体而言，相比于BTC矿机产业链，Cellula的方案是一种更有趣的社会实验。