HashDice

全球第一本写在区块链上的赌博启示录

我们生活的社会它到底长什么模样？当你觉得他黑暗时，总会有一些事情让你燃起斗志，当你为了理想奋斗时，也不时会因欺骗和背叛丧失信心，最终怎么做，全取决于你信的 “道” 。

“ 该打的仗我已经打过了
该跑的路我也跑到了尽头
老子信的道老子自己来守
背叛 争抢 没有底线
想把老子变成一只动物
no 没戏
老子宁可做一辈子披荆斩刺的小丑
也绝不会变成你们这种人渣的样子
游戏是你们的
规则老子自己来定 “

客官，请来 HashDice 的寻找你信的 “道”。

序

上帝掷骰子吗？爱因斯坦不同意哥本哈根派对于该问题的诠释，生气地说：“玻尔，上帝是不掷骰子的!” 玻尔一脸不高兴：“爱因斯坦，别去指挥上帝应该怎么做!” 谁是谁非？或许我们还无从判定，但如果要说“上帝是掷骰子的”，那么在掷骰子掷出来的世界里，我们微小若尘埃，却自命不凡、人定胜天；我们同根于动物，却高高在上、主宰万物。这就是没有自知的个体在世界在以一种“极度愚蠢”的方式在证明着自我存在。

有人说，人生无非就是一场赌博游戏。是的，人生时刻都在下注博不确定性，可掷骰子的不一定是赌徒，我们都只是挺“可爱的”一群平凡人，享受着“随机性”给我们带来的无限可能与刺激。但如果你自认为深谙随机现象，战胜人性不在话下，HashDice 将会让你明白人性中的欲望，远比规律更为复杂。

HashDice 是全球第一本写在区块链上的赌博启示录。在这里你将知道富豪的财富还有第二种来源；你也将知道人类，可能他并不是那么特别，而是与动物无甚差别。在这里你将获得最大的自由，但你也可能会因为过度的放纵而自我吞噬。赌博是资本与人性的游戏。人性，是千百年来最让人着迷又最让人捉摸不透的东西。一旦拥有通过某种带给过你安全感或实际利益的经验，你就会将此奉为真理，无论它是不是具备普遍适用性，更无论它是否只是一种单纯的概率。资本，就是资源，是地位的象征。不要认为人类已经进化到了地球生命的顶点，在高阶生命看来，人类和一般动物没有什么区别——在动物的世界里，只有利益，没有感情。资本越多，越具备游戏规则制定权，在繁衍上也能占据更大的优势。也正是因此，资本可以在很大程度上控制人性——毕竟人类终究无法脱离生物繁衍后代的本能。而赌博，正是连接人性与资本的完美桥梁。在赌的世界——HashDice 里，不存在必胜的规则可以遵循。上了赌桌，你只能信奉某种“玄学”，来博取那捉摸不定的单注概率。你可能会对无数的人不顾后果地奔赴赌场感到疑惑，那是赌博还有着它最迷人的地方——可能带来的资本暴增，以及与之相对应的社会地位的提升。但很可惜这是不可能的，千万不要挑战人性，因为真正的赌徒从来不知道止损，这也正是富豪的财富的第二种来源。没错，富豪的财富是来自工人的剩余价值。但现代社会，还有一种财富来源叫“穷人”的浪费。“穷人”的浪费又是怎么来的？就是来自于贪欲和愚昧。

人生就是一场赌博，而 HashDice 就是你上演赌博戏码的舞台，不怕你精，不怕你呆，不怕你赢，就怕你不来，只要你敢尽情地表演你的贪婪与欲望，你会活的明明白白，输的服服气气。因为 HashDice 会通过区块链持续用最公平、公正、透明、可验证的方式探索人性，给你**久赌必输的**启示，也会给你开启一条从奴役到自由的路。

目录

1. 关于 HashDice

HashDice 项目是一次基于区块链的社会化人性探索实验。我们通过设计与开发主题为“从探险者大航海到建设文明城邦”的故事背景的游戏来揭露人类在社会化活动中被个人内心的自私、贪欲、愚昧等本性反噬的现象，并将区块链的不可篡改、可追溯、公开可访问和可验证的特征融入游戏情节中来直击玩家陷入“绝境”时内心的阴暗面，再通过由浅入深的游戏情节和提供通俗易懂、可操作性强的公平验证工具来引导玩家正视自身的丑恶面，自我反省，走出困境，拥抱美好健康的生活。寓教于乐是我们的宗旨，引人入胜的游戏情节和丰富缤纷的游戏素材让玩家可高度自由发挥。游戏伊始，将会以最简单的第一视角来呈现，提供《抛硬币》、《骰子》、《过山车》等内容。随着项目的深化发展，更多的游戏内容逐步释放并将前置的内容统一到单一赌桌内的视野范围来开展。值此阶段，人与人之间的互动环节增多，伴生的是更加复杂的人际关系与生产活动，因此我们会最大限度的在游戏中对现实进行复刻，如提供庄闲转换、自由交易、竞拍、租赁、股权分红等机制，待该最小自由市场初步形成，玩家角色愈加丰富，不同的角色本性也将不断地被放大，我们将进一步丰富游戏场景，扩展玩家的原始积累和资本及地位的晋升之路，这样将更有利于我们对复杂和多样化的人性进行研究和探索。游戏的远期格局将会是以赌桌——赌场——文明城邦——哈希世界为主线来构建，在实现的路径中，玩家的视野不断开阔，并在角色不断分化的同时拥有自主的规则定制权，这将会使得游戏情景更加贴近现实，进而让玩家在与他人，与自己的博弈以及自我克制中找到自己的信奉的“道“。此外，考虑到人群的复杂性和分布的广阔性，即除了主要的“困境引导“型人群外，还设置了休闲娱乐环节来满足大众玩家需求，这也符合我们倡导积极的生活方式和为人类打开丰富的精神世界的大门之初衷。

2. 实验启动

目前，“下注即挖矿” 的模式风靡整个 DApp 生态，随着挖矿的规则被用户熟悉和深度体验，该模式的弊病也日渐显露，但我们依然认为它是一种较好的能够帮助新项目甚至是项目内新元素完成冷启动的方式。因此，我们也选用 “挖矿” 来打响 HashDice 这项社会化实验长跑的第一枪。从我们对现阶段市场上的项目的调研结果可知，流行 “挖矿” 模式被广为诟病的聚焦点为 “三分钟热度”，具体表现为商业嗅觉敏锐且具有丰富投资经验的 “矿工”，总是能够抢夺先机，然后在进行到第一次 “挖矿衰减” 时果断退出，从而使得获取筹码的综合成本最低。此举为止盈之上策，也是人性上的自控——戒贪。然而，如果我们常游走于 DApp 生态的各大项目之间定能察觉到最早进入的 “矿工” 几乎总是同一批人，新型垄断就此形成，自然也会就导致项目的参与后继无人。最终可观察到的现象是大部分项目上线火爆一周甚至不到一周就人走茶凉。考虑到以上恶果，我们采用逆向思维，推出与之相对的挖矿模式，即挖矿成本随着时间的推移而递减而非递增。具体的挖矿详述参见后文。

3. 关键技术概述

本小节主要概述了在区块链上进行可信随机数生成及传递的机制及其在现阶段的 HashDice 中的具体实现思路。

区块链技术由于其去中心化特性，以及交易的透明、开源等特性，在保障交易公平性方面具有极大的优势，因此其对于传统需要随机数生成器的应用场景，如彩票、博彩类应用（如扑克、麻将、抽奖等）具有颠覆性的潜力。

传统的在线博彩类游戏，由于其中心化特性，游戏平台在游戏中占据完全的优势地位，能够随意操控游戏结果。即便一些游戏平台的随机数生成器(RNG)得到第三方认证，但这些认证机构均无法保障持续的审计，玩家无从判断游戏中生成的随机数是否是公平的。然而，让玩家能够自验证随机数生成的公平性正是 HashDIce 实验成功的关键因素。如果区块链技术得到大规模应用，将彻底改变该类在线游戏的生态体系，从而让赌徒或沉迷玩家清醒地认识到博彩类游戏的零和本质（注：当存在 House Edge 时，为负和游戏），而非平台作弊或故弄玄虚。

3.1 真伪随机数

区块链的世界没有真正的随机数，但随机数却是区块链游戏之魂，至少在目前阶段如是。所以，当伪随机数让 DApp 流下第一滴血后，DApp 却无法断臂求生。潜伏的黑客们就像嗜血的鲨鱼，在嗅到腥味后迅速聚拢过来，围攻这个有着天生缺陷的猎物。

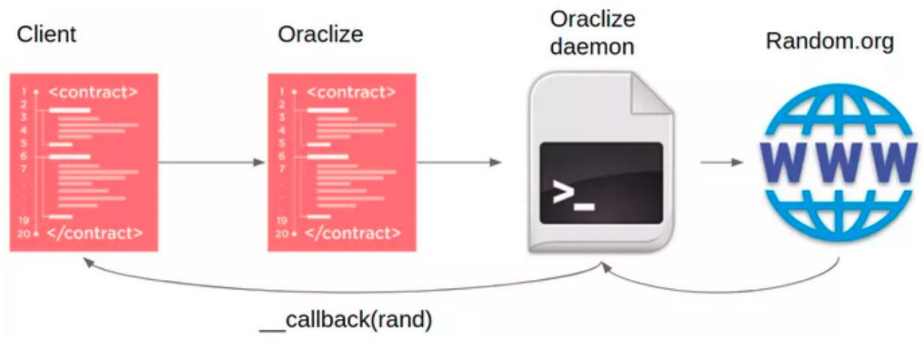
真正的随机数只存在于物理世界中，比如掷骰子的结果。最早的随机数生成器正是骰子，早在公元前 2600 年，人类就已经用四面骰来玩抛掷游戏了，迄今为止，它依然是最值得信赖的产生随机数的方法。然而，现在在计算机领域被广泛应用的随机数几乎都是由伪随机数生成算法生成，而且它的生成或多或少与单台机器的物理状态或运算状态相关，即不同机器或者说不同节点的运算结果相异。这也就说明了在区块链上生成随机数是困难的，因为区块链是一个分布式的系统，它要求各个节点的运算结果是可验证、可共识的。

3.2 区块链的随机数生成法则

区块链的随机数生成法则的设计可能需要进行思维转换并从零开始，从而实现不同节点上的智能合约可以使用相同的随机数。我们这里将简要介绍以下 3 种：

一、让可信第三方为合约提供随机数

该方法本质上采用的是预言机(Oracle)技术。以 Oraclize(白皮书地址 http://www.oraclize.it/papers/random_datasource-rev1.pdf)为代表的预言机技术的主要作用是试图将链下的数据通过可信传递机制传输到链上，其中就包括引入链下随机数生成器产生的随机数。



预言机技术确实为将随机数引入区块链提供了一种方式，但它在可信随机数

生成及传递方面存在以下一些问题：

1.) 中心化：预言机技术所引入的随机数，从本质上而言是一种中心化机构生成的随机数，并不符合区块链技术的特性。也就是说，oraclize 事实上具备操控随机数的能力。

2.) 额外的交易成本：任何一种预言机技术都需要搭建和运营一套预言机服务平台，而运行这样一套平台是需要收取费用的，如果每请求一个随机数都需要支付一笔费用的话，这个交易成本是在区块链网络交易手续费之外额外增加的。

二、让所有节点上的合约可以采集到相同的种子，再通过伪随机算法计算出相同的随机数序列

该方案的随机数不是从合约外部引入，而是把区块链的链上信息做为种子，由智能合约根据种子生成伪随机数。然而，不同于传统伪随机数生成算法中种子的私密性，区块链上的种子几乎是“透明”的，即它是链上的区块信息，所有节点上的智能合约都能够取到，这就产生了巨大的安全隐患：

1) 其他应用程序和区块生产者也可以通过同样的方式获取区块参数（包括但不限于区块 Hash），从而可同时知道结果，进而采取相应的攻击手段。

2) 如果只是简单地使用区块 Hash 作为随机数源，由于区块链技术的特性，当前区块还没有被打包，所以只能获取当前区块之前的区块 Hash，这些区块 Hash 值对于所有节点而言都已经是已知的，要攻击这种应用是很容易的。

3) 如果攻击该应用的利益足够大，则区块生产者将产生操控区块 Hash 值的动机。就算在 POW 的区块链中，即便因此而牺牲了区块打包收益，但由于类似于以太坊这样的公链，它对叔块同样有激励，所以区块生产者的真实损失并不大。

三、通过基础合约实现伪随机数生成器，为其他合约提供一致的随机数

最契合区块链精神应属该方案，它本质上是一个由不同参与者合作生成随机数的伪随机数生成器。典型的案例是已经得到以太坊基金会支持的项目 RANDAO，他们提出了一种 Commit-Reveal 架构，用于解决可信随机数传递的问题。

在 Commit-Reveal 架构下，一笔成功的交易是这样完成的：

1) 平台生成一个随机数 Reveal，用这个随机数经过散列(Hash)处理之后生成 Commit。由于 SHA3 Hash 算法的不可逆特性，无法从 Commit 反导出 Reveal，所以 Commit 可以对外公布。

2) 用户得到一个 Commit。

3) 用户用得到的 Commit 发起一笔交易。

4) 平台向这笔交易揭示随机数，同样由于 SHA3 Hash 算法的不可逆特性，平台无法伪造一个随机数，只有真实的 Reveal 值才能得到同样的 Commit 值，该笔交易成功。

RANDAO 提供了一种在区块链上进行随机数生成及传递的有效架构，这种架构可以适用于很多应用场景。但对于一个涉及到巨大利益的博彩型应用而言，这种方式并不满足要求：由于庄家提前知道 Reveal，所以当用户投注之后，庄家在已知用户投注结果和 Reveal 的情况下，已经确切知道了开奖结果，这时庄家可以选择是否揭示随机数。也就是说，庄家具有选择性终止的权利优势，这并不符合公平原则。

在 Commit-Reveal 架构的启发下，也有人提出相互提供 Commit/Reveal 对的双重承诺揭示方案，这种方案要求用户端也提供一个 Commit/Reveal 对，最终的结果由双方提供的随机数种子混合而成。这种方式在实现上要求用户端也具备一个随机数生成器，由于大多数应用的客户端都是由应用开发者提供的，所以这种方案在实现上其实没有带来任何改进。

3.3 HashDice 的可信随机数生成及传递

3.3.1 Commit-Reveal + Tx(transaction) Hash 的结构体系

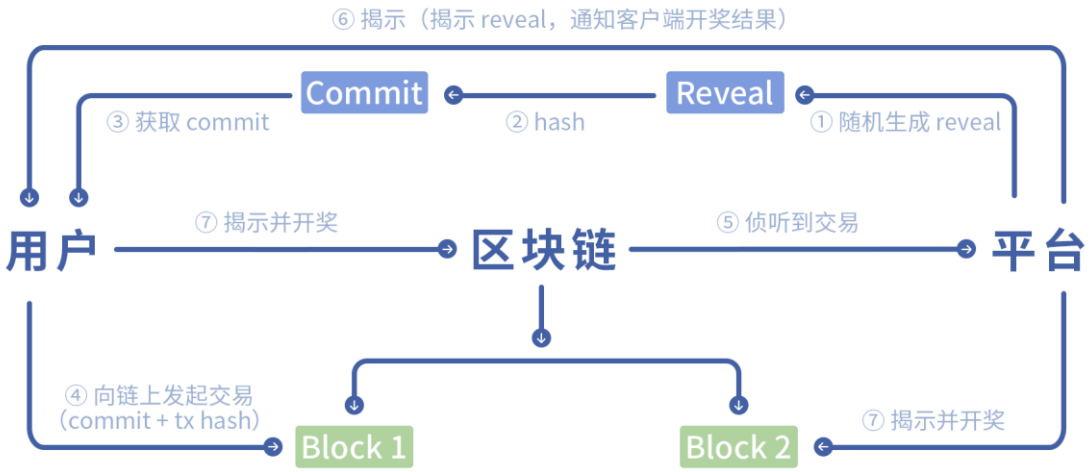
HashDice 采用的是被称为 Commit-Reveal + Tx(transaction) Hash 方式。在介绍其结构体系前，我们先简单回顾一下常用的随机数生成及传递机制：

1) Commit-Reveal 对 :它能够保证平台方可以安全地将 Commit 值公布给用户，同时能够保证平台方无法伪造 Reveal。

2）Block Hash：用户及平台方都无法操控 Block Hash 值。

3）Tx Hash：平台方无法操控 Transaction Hash 值。

从预言机引入随机数的方式，由于前文所论述的问题，我们不再考虑。那么，我们能否更进一步，让 Reveal 持有者不具备任何优势，从而失去作弊动机呢？HashDice 提出的 Commit-Reveal + Transaction Hash 方式可能是一种切实可行的方案，其交易流程如下图所示：



整个流程的链上、链下交易分为 7 步：

【第 1 步】：平台生成随机数种子 Reveal。

【第 2 步】：Hash 之后得到 Commit。

【第 3 步】：用户从平台获取经平台签名的 Commit。

【第 4 步】：用户发起投注交易，并带上 Commit。

【第 5 步】：平台监测到投注事件。

【第 6 步】：平台通知客户端开奖结果及 Reveal, Tx Hash 值。

【第 7 步】:用户和平台都可以开奖(Settle), 开奖时使用的随机数种子混合 Reveal 值和 Tx Hash 值。

该方案的关键点主要是：

1) 在监测到投注事件后，平台立即通知客户端开奖结果，用户可以验证 Commit/Reveal 对的真实性，Tx Hash 值对用户而言也是已知的，所以开奖结果是可以验证的。

2) 当客户端通知之后，用户和平台都具备开奖(Settle)能力，平台无法单方面终止开奖。

3.3.2 叔块处理逻辑

叔块(uncle Block)是以太坊的一种特性。在去中心化的区块链平台上，由于所有区块生产者都在竞争区块打包的权利，所以同时产生超过 1 个区块生产者获得区块打包的权利是不可避免的情况，在同一个区块高度不同区块生产者所打包的区块肯定是不一样的，而区块链最终只会选择其中一个区块作为主链上的区块，而其他未被主链接纳的区块则会成为孤块。

比特币对待孤块的处理方式是直接抛弃，这是因为比特币的区块产生之间的时间间隔为大约 10 分钟，所以其孤块产生比率很小，可以直接抛弃。而以太坊的区块生成之间的时间间隔为 12-15 秒，产块速度大幅度提高，同时就意味着产生孤块的比率大大提高，所以以太坊选择了不同的处理方式，并没有直接抛弃孤块，而是将这些实际并没有对主链交易状态起任何作用的区块也打包进了区块链中，这些区块被称为 “叔块” 。以太坊也对叔块打包者给予了一些激励。目前以太坊的叔块率已经超过 10%，这已成为不可忽视的问题。

叔块在大多数情况下对交易不会产生任何影响，因为它们并没有对主链上的真实交易状态做任何改变。在 Commit-Reveal + Tx Hash 的架构中，由于要使用 Tx Hash 作为一个辅助的随机数种子，叔块的问题就凸显出来 :在监测到 Commit 事件时，无从判断它到底是来自一个叔块还是主链上的区块，而等待叔块确认则需要花费几个区块的间隔时间，这对于一个即时型应用而言是难以接受的。

3.4 安全性分析

区块链应用生态崇尚开源精神，所以推向市场的 DApp 要能够经受得住各方的攻击，并提供数学上可验证的公平性。接下来我们对各种潜在的攻击方式和应对方法做简要分析：

1) 双花

对于一个已发起的交易，要进行双花攻击需要耗费成本，由于叔块比率的问题，双花攻击对于本应用而言从经济上并不可行，但这个威胁对于算力集中度很高的公链是确实存在的。

2) 选择性发布

随机数生成方可以对数据有选择性地发布，但由于结果不是由单一随机数源生成，对随机数的选择性发布没有任何意义。

3) 选择性终止

平台是否能够在开奖之前提前预知结果，并拥有有选择地进行开奖的优势？由于开奖通知的及时性，客户端可以在 Commit 交易确认之后，立即得到开奖结果并对其进行验证。

4) 重入

这里指的重入不是常见安全问题中的通过回调函数重入，而是多次使用同一个 Commit/Reveal 对进行重复投注，要消除该问题需要注意以下几点：

a) 不能在不同版本合约之间，使用同一个签名地址。

b) 一旦某个 Commit/Reveal 对被使用，它将被记录在合约中，不能被再次使用。

5) 区块生产者篡改结果。

负责区块打包的区块生产者是否有能力篡改或操控结果呢？首先，由于我们从外部引入了一个 Reveal 随机种子，区块生产者不能够通过操控区块参数来控制结果。其次，区块生产者不能够随意选择区块中打包的交易，任何一个交易的变更都会造成区块 Hash 值的变化，从而影响区块生产者打包权利的工作量计算，所以如果区块生产者要改变打包的交易，等同于放弃了该区块的打包权利，除非利益足够大，否则对于区块生产者而言经济上不划算。

6) 区块生产者与平台方勾结

对于算力高度集中的区块链平台而言，这确实是一个问题，而对于算力分布去中心化程度很高的区块链平台而言，要做到这一点从经济上而言完全没有可行性。

7) 拒绝服务(DDoS)

很多 DApp 项目本身都无法避免本身的 DDoS 风险，黑客通过发送大量高 gas price 的交易，可以短时间阻塞，从而造成正常交易无法被打包。在这种游戏逻辑下，交易的可靠性是关键因素，而 DDoS 攻击是致命的。HashDice 将提供一种在阻塞的情况下，在限定时间内如果没有完成交易，用户可以回撤其资金的机制。

8) 其他安全事项

对于一个代码开源、运行透明的区块链应用而言，安全问题远不止上述这些概要的内容。已知的安全问题还包括溢出、回调重入、错误地使用 this.balance、短地址攻击、底层调用的状态检查等各种类型的攻击，这些攻击方式以及应对方法是通过大量的开源代码暴露和总结出来的。所以，我们认为，选择一个受众群

体较大的区块链平台，对于开发一个可用的分布式应用也是非常重要的，这是我们目前选择在波场和以太坊上进行开发的重要原因。

4. 应用生态的构建

HashDice 团队希望能够吸纳更多的生态共建者和合作伙伴广泛地参与到这场社会化人性探索实验的活动中，共同构建一个公正透明，颇具启示性的游戏生态。因此，团队自身在给项目内容持续输血的同时也推出了深度孵化服务和 UGC 体系来推动项目的发展。

4.1. 深度孵化

围绕着游戏生态，有很多专业化的团队能够提供非常有效的内容和产品来帮助玩家选择和玩法，提供多维度评估等，构建生态上的深度交互，让生态更有活力，让本次实验更加有效和有意义。因此，我们会与专业的游戏服务团队建立合作或深度孵化有创意和高质量的游戏团队。

4.2. UGC 体系

大量的 UGC（User Gernerated Content）是对实验的正反馈。在 HashDIce 项目开展过程中，优质的 UGC 内容的生产者会获得相应的激励，而且 UGC 内容本身将极大地提升社区活跃度，促进社区发展，并对需要更多信息的人提供价值。

在 HashDIce 的生态系统中，用户可以帮忙更新和维护游戏的相关信息（如提供更易懂的玩法和简介，游戏项目的更新消息等），也可以发表自己的游戏体验和感想，抑或产出深度分析或科普。所有的优质内容将经由系统的推荐机制进入到所有玩家的阅读视野，其他玩家也可以通过点赞、评论、赏金等机制产生次级 UGC 完成互动。

该部分所提到的奖励机制均通过项目发行的 Token 实现。具体的 Token 发行计划参见后文。

5. Token 的发行与生态

我们认为未引入 Token 模型的区块链项目将是无源之水。为了让 HashDice 能够持续长存，我们将发行用于在 HashDIce 生态内流通的 HDT，并为此设计了优秀的经济模型。此外，根据游戏的初始设置，我们还将预先出售部分 HDT 来支撑游戏中的奖池以及用于运营与推广。

5.1 代币发行方案

HDT 的发行总量为 100 亿，且永不增发。其分配图如下：

代币分配方案		
项目	百分占比	HDT 分配
私募	**5**	**500,000,000**
团队激励	10	1,000,000,000
推广运营	10	1,000,000,000
探险者挖矿 A	8	800,000,000
探险者挖矿 B	8	800,000,000
矿山深处奖池	4	400,000,000
调整挖矿(夺宝奇兵)	20	2,000,000,000
创世奖池	10	1,000,000,000
大航海基金	25	2,500,000,000
总量	100	10,000,000,000

私募计划：私募计划共筹集 **6,250,000** TRX，未筹满部分进入“矿山深处奖池“。

5.1.1 规则释义与名词解释：

下注中奖筹码设置原则：下注筹码与奖金的类型尽可能保持一致。

挖矿解释：“投注即挖矿”。举例，当调整胜率为 95%时对应的赔率为 1.032，每下注 1 TRX 或者 1 VENA 将得到若干 HDT。而以 HDT 作为筹码下注不属于挖矿范围，但会向该类下注的玩家定期空投糖果或增加其质押分红的权重。

创世奖池：由于游戏中设置了以 HDT 为筹码下注以及下注中奖原则，我们需要设立 HDT 的初始奖池。

探险者挖矿：探险者挖矿即创世挖矿，用于冷启动。

夺宝奇兵：夺宝奇兵属于调整挖矿。HashDice 采用非连续挖矿模式进行，为了保护投资者利益以及平台追求稳定、长期、真实的游戏流水的愿景，团队会根据新游戏本身以及二级市场价格的情况开启属于该新游戏下挖矿模式。在启动新游戏挖矿时，该部分锁定。

大航海基金：HashDice 的设计哲学遵循“涟漪现象”，先以个体与赌桌交互为最小单位的一个中心点，围绕中心点的蓄能爆发逐步扩散，我们相信中心点能量越大，影响范围更广，期盼影响至不可触及的边界。在此过程中，我们会高度顺应与契合人类本生的情感需求，由人机对战发展至 PvP，甚至扩充至更加复杂的模式，当然我们也将“邓巴数”理论应用于该设计环节之中，使玩家获得最真实和最有实际意义的游戏体验。因此，大航海基金则是每一圈涟漪能量环的基建基金，也是涟漪扩散的加油站。

5.2 探险者挖矿

在 HashDice 中，探险者挖矿采用竞争挖矿的模式。游戏中设置有 AB 两座矿山。用 TRX 下注即挖 A 矿，用 VENA 下注即挖 B 矿。挖矿设置细节如下：

1) 探险者挖矿总量 20 亿 HDT，分为三个阶段（参见 5.2.3）开采，并将 AB 两座矿山设置成对照形式来进行竞争挖矿。
2) A、B 两座矿山中，每座矿山各有总量 8 亿 HDT。即共有 16 亿 HDT 待通过下注挖矿来开采。
3) A、B 两座矿山底部额外贮藏总量为 4 亿的 HDT，但分布比例未知。如果 A 矿先被开采完，则 A 矿底部额外贮藏的 HDT 将按照挖矿量权重分配给开采 A 矿矿工，则 B 矿底部额外贮藏的 HDT 直接销毁。相反，如果 B 矿先被开采完，则 B 矿底部额外贮藏的 HDT 将按照挖矿量权重分配给开采 B 矿矿工，则

A 矿底部额外贮藏的 HDT 直接销毁。

4) 如果 A 矿先被开采完，B 矿除去 B 矿底部额外贮藏的 HDT 之外，剩余未被开采完的 HDT 将按照挖矿量权重分配给开采 B 矿矿工。相反，如果 B 矿先被开采完，A 矿除去 A 矿底部额外贮藏的 HDT 之外，剩余未被开采完的 HDT 将按照挖矿量权重分配给开采 A 矿矿工。**（该部分有 3 个月的锁定期，每月释放 1/3）**

5) 通常我们所谓的开启挖矿模式是将胜率调整为 95%, 其对应的赔率为 1.036 (赔率以实际上线产品为准)。即每下注 1 TRX 或者 1 VENA 将得到若干 HDT。

投注胜率	投注回报率	投注期望	单位亏损
0.95	1.036	0.9842	0.0158

即:每投注 1 单位 TRX 或者 VENA，预期亏损 0.0158 单位(挖矿成本)。

5.2.1 分级挖矿模式

探险者挖矿分为三阶段：

【第一阶段】：与宝藏（HDT）偶然邂逅的懵懂。（挖矿比例 10%）

【第二阶段】：轻车熟路下的疯狂夺宝。（挖矿 HDT 比例 65%）

【第三阶段】：探险者们的最后冲刺（挖矿 HDT 比例 25%）

第一阶段完成后会统计矿工的工作量证明，第一阶段工作量越多，工作等级越高,第二阶段将获得更多的挖矿加成，即挖矿成本更低。工作量证明共分为 10 等级，等级及加成对应如下表，如果矿工没有参与第一阶段的挖矿，则获得的工作量奖励为 0。所以，第一阶段的挖矿非常重要！

工作证明等级	人数占比	第二阶段加成
level1	5%	2%
level2	10%	4%
level3	15%	6%
level4	20%	8%
level5	20%	10%
level6	15%	12%
level7	10%	14%
level8	2%	16%
Level9	2%	20%
Level10	1%	25%

第二阶段的挖矿模型：

$$\mathrm{HDT} = \mathrm{TRX} * \frac{1}{1 + e^{1-\frac{2*mined}{total}}} * (1 + Reward\ ratio)$$

其中：$Reward\ ratio$为第一阶段根据工作量的加成比例。

5.2.2 挖矿数学模型

探险者挖矿通用模型：

$$HDT = trx * f(x)$$

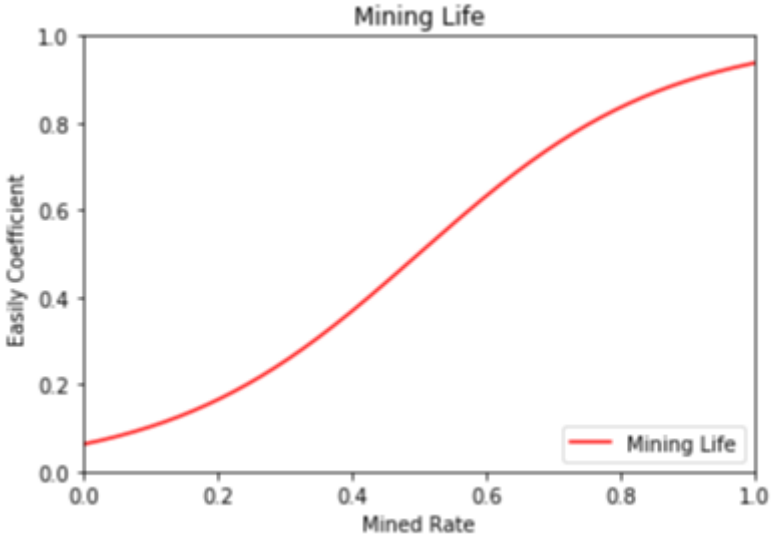
其中 $f(x)$ 表示挖矿容易程度，$f(x)$ 为单调递增函数，越到后期挖矿越容易。$f(x)$ 是依据函数原型为 sigmoid 的函数 $F(x)$ 演变而来。

$$F(x) = \frac{1}{1+e^{-x}}$$

全周期的挖矿通用数学模型：

$$\mathrm{HDT} = trx * \frac{\beta}{1+\alpha^{1-\frac{2*\mathrm{min}ed}{total}}}$$

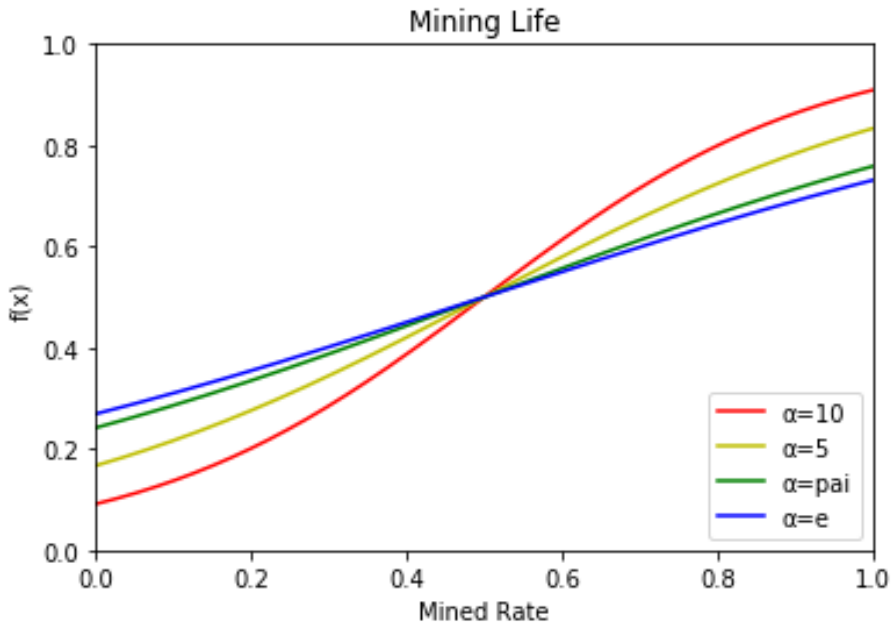
其中α和β为可调参数，挖矿容易程度图为：



5.2.3 模型参数分析

1）参数α

在参数β一定的情况下，参数α决定了挖矿容易程度的增长速度，α值越大，挖矿容易程度增长越快，同时初始挖矿难度和结尾挖矿难度差距就越大，反之亦然。



2）参数β

在参数α确定的情况，参数β决定了投入一个 trx 产出 HDT 的比例。参数β值越大，挖矿越容易，反之亦然。

最终，我们取参数$\alpha=e$，参数$\beta=1$进行海量数据的模拟来确定了探险者挖矿的模型：

$$\mathrm{HDT}=trx*\frac{1}{1+e^{1-\frac{2*\min ed}{total}}}$$

其中：HDT 表示获得的 HDT 数量

TRX 表示投注的 TRX 数量

Mined:表示被已经被挖出的数量

Total:表示矿山的总量

5.3 探险者挖矿的背景故事

既然人生是一场赌博，那么谁也不知道下一刻会发生什么。在大航海时代，探险者们的出海同样如此，前方等待的是财富还是死亡，我们未能预测，但我们愿意放手一搏，证明此生我们真正来过。

探险者们扬帆出海，惊现 A 和 B 两座矿山，摇身一变成为了矿工。AB 两矿充满了神秘感，这就使其更具诱惑力。矿工们从搁浅的漂流瓶中的纸卷得知了 A 和 B 两座矿山底部有 4 亿的宝藏 HDT，和若干 VENA 和 TRX，但令人疑惑的是纸卷中对 A 和 B 矿中宝藏 HDT、VENA、TRX 的分布情况只字未提。于是矿工们对于挖矿的选择无疑又是一次豪赌。对，当矿工们下定决心参与这一次豪赌时，纷纷陷入了沉思，他们幻想着财富自由的那一天，沙滩，美女，海鸥，还有曾经的老船长。嗯，一幅美好而没有尽头的画卷瞬间在脑海中顺滑铺展，然而贪婪与私心在此刻喷薄而出，每个人都想将宝藏据为己有而考虑去独立挖一条通往财富自由的隧道，嘀嗒一声，矿工们从梦中突醒，面面相觑，发现早已垂涎三尺，后知后觉刚才的嘀嗒声是自己的口水拍打在靴子上的迸溅声。梦醒之后，一场浩浩荡荡的创世挖矿革命就拉开了序幕，可以想象一座金灿灿的宝矿，在人性的贪婪驱使下最后会千苍百孔，在阳光的散射下，我们似乎还能沉醉在丁达尔效应的光景之中。

可是擅长航海的探险者们并不擅长挖矿，邂逅了宝藏的他们却表现出一副懵懂的模样。由于缺乏挖矿经验且没有提前准备装备，只能就地取材，因此矿工们的挖矿产出较低，纷纷抱怨着挖矿难呀，挖矿难。尽管如此，矿工可没有气馁，他们在挖矿实践中总结经验，并在区块链上面记录着自己的日常，这可是工作量的证明，也是璀璨的功勋章。

日子一天一天过去，矿工们翻看着自己的日常记录有了很多感悟，觉得是时候返航休整了。休整期间，矿工们锻造精良的挖矿装备，并在坊间分享着自己暴富的经历来满足自己的虚荣心，于是吃瓜群众们也心动不如行动，毅然加入了淘金大军。当再次来到矿山前，老矿工们都不约而同的选择了自己之前走过的路，在之前的深度下继续开采，这些矿工们早已轻车熟路，但由于天赋各异，这次的挖矿产出因第一次累积的工作量证明的不同而有着不同的产出系数，而初出茅庐的矿工在坊间聆听故事之余也在出发前做好了些许准备，他们选择前辈走过淘金之路（挖矿隧道）从捡漏开始奋起直追，由于还是缺乏挖矿经验，因此他们的挖矿产出要比有过工作量证明的矿工产出要低，但新入场的矿工们的产出系数相同，

得益于有了精良的装备，新入场的矿工第一次挖矿就币老矿工第一次挖有着更高的产出。

在挖矿的漫长岁月里，矿工们的挖矿利器在时间的洗涤和与矿石的摩擦中早已成为了钝器，于是他们又返程休养生息，修复装备再造利器。可想而知，这一次的矿山开采已经让依旧幸存的矿工们赚的盆满钵满，而去还传言着矿山底部还蕴藏着丰厚的宝藏且离那一刻不远了。眨眼儿的功夫，流言传遍大街小巷，人们抵挡不住金钱的诱惑，宁可信其有不可信其无，磨刀霍霍在小镇后山就开始集体训练各种挖矿淘金技巧，没过多久就人人身怀绝技，夺取宝藏势在必得。由于全民的系统性训练，大家的挖矿经验已经十分丰富并且技能水平相差无几，于是在疯狂淘宝的最后阶段，大家的挖矿产出却是惊人的相似。不仅如此，就如牛顿所言，“他可计算宇宙，却无法计算人类的恐惧与贪婪“，矿工们的大脑已被矿山底部的宝藏封闭，在触手可及之时已然忘却所谓的疲惫。”得到“和”失去“就在一瞬间，因为大家都知道 A 和 B 两座矿山毗连，底部相互支撑。无论哪做矿山先被开采到纵深底部都会因受力不均导致邻矿塌方，只能眼睁睁看着眼前的宝藏灰飞烟灭。让煮熟的鸭子飞走，想必没有矿工会放手，那么最终阳光下矿山轰然倒塌的壮丽景色究竟会是怎样？只能拭目以待，大航海时代的“淘金热”的升腾，或许我们只能屏住呼吸，扬起双手，透过指缝间的那狭小的视线窥视着它在巨震后的上空不断扩散。

5.4 HDT 权益

我们将 HashDice 项目收□ 的 20%进入奖池，而其中的 60%将用于对持币玩家进□ 质押分红，玩家通过抵押 HDT，每 24 小时，均可分享平台的利润。

参与分红的 Token 可以是挖矿、预售、□ 户奖励、合作方的 Token 以及释放给团队的部分等。

6. 联系我们

Telegram: t.me/hashdice

Discord: https://discordapp.com/invite/Cn6rnUw

Twitter: https://twitter.com/hashdice1?s=09

Email: hashdice@hotmail.com

7. 法律及免责声明

1） 我们搭建游戏平台来推动一场社会化人性探索试验，但不劝导游戏用户参与任何游戏，在未取得相关许可的情况下，严禁 18 周岁以下玩家参与本次实验。
2) 我们遵守相关国家和地区的法律法规，不向禁止区块链项目的国家和地区提供任何游戏服务。
3) 我们不做任何形式的承诺，持有 HDT 尽管能公平获得平台的相关权益，但我们不承诺其升值空间。
4) 参与游戏可能会面临损失，如□ 法承担，请勿参与游戏。
5) 本□ 文件的解释权归 HashDice 项目团队所有。