Ulam

新一代共识创新公链

ABSTRACT

Ulam 是继 POW、POS、DPOS、PBFT、DAG 类共识算法之后的第六个在共识算法上有重大创新的区块链项目。Ulam 共识算法的灵感来自波兰犹太人数学家斯塔尼斯拉夫·马尔钦·乌拉姆（Stanisław Marcin Ulam）的 Luck number。其利用哈希函数的特性创造出超低能耗、完全去中心化、高度稳定的区块链系统；是目前唯一一个成功打破区块链“不可能三角”的全新共识算法。Ulam 不需要进行哈希计算竞赛，可以允许低功耗的手机、智能手表、路由器等参与“挖矿”。 Ulam 设计的全新非交互式交易验证算法（NITCV），可以使 TPS 最低达到 1 万。Ulam 使用知识证明的方法构造出非交互式交易验证算法。Ulam 具有超级碎片化节点；完全去中心化；抗算力集中；49%容错率；抗量子攻击；超高 TPS；抗分叉；算法促进共识传播等八大优势，是可以替代 POW、POS、DPOS、PBFT、DAG 类共识算法的第六大共识算法。

关键词：Ulam；共识算法；随机数；区块链 3.0 ；非交互式交易证明验证

目录

项目背景

区块链这一技术到 2019 年初已经有了 10 年的历史。在这十年中区块链的技术、应用、接受度都发生了巨大的发展与变更。最早的区块链概念来源于比特币这一创造，但是经过这些年的发展，区块链已经不再专属于比特币。作为一种集计算机技术之大成的综合性技术区块链技术包括 p to p 网络、密码学、共识机制、电子签名，虚拟机等部分。其本质上是一个去中心化的分布式数据库，具有去中心化、不可篡改、可追溯等特点[1]。

经历了 2017 年和 2018 年年初的暴涨，2018 年底到 2019 初年全球的区块链公链产业正在经历着区块链历史上的第三次低谷。这个低谷的产生主要有两大原因：首先，不得不承认之前的繁华有部分泡沫的因素；其次，区块链技术应（特别是公有链技术）在应用上的短板和在大众接受度上的局限也是这次大熊市的另一个原因。目前的区块链技术之所以很难在应用层上发挥较大的作用主要原因是基础设施缺乏足够的可用性与安全性。区块链技术的核心技术是密码学和共识算法，但是目前的共识算法 POW，POS，DPOS，PBFT 和以 DAG 为结构的一些共识算法都存在着许多不可逾越的短板。这些短板可以被简要地总结为“不可能三角”，既在现存的区块链系统中不能够同时做到高度去中心化、安全稳定和高可用性。

交易速度低

交易速度或者吞吐量既 TPS（transaction per second）是一个网络系统可用性的一个重要标准。在区块链网络中 TPS 主要受到带宽的和共识机制的限制。VISA（Visa International Service Association）的 TPS 在 5000 到 8000 之间[2]。这个量级的 TPS 可以满足全球的很大一部分信用卡支付系统。可见 5000+的 TPS 是一个高可用性的区块链支付系统的基本期望值。如果要涉及到小额支付，例如微信和支付宝的日常支付，则 TPS 要比这个数字要高得多。例如，支付宝依托于蚂蚁金服自主研发的数据库 OB（OceanBase）在 2017 年时曾经打破世界纪录。其处理峰值曾达到 42,000,000TPS。虽然一般的系统不可能有支付宝如此高的使用频率，但如果考虑到区块链系统可能会应用于 IOT 设备、城市公交系统等高频交易场景，一个区块链系统需要有 10000+的 TPS 才能称之为具有高可用性或者高吞吐量。然而，这是目前几乎所有现运行的区块链公链系统都无法达到的数字。例如，比特币的 TPS 只有 7，以太坊的 TPS 只有 20，EOS 的 TPS 只有 2000 左右。况且，EOS 换取这个量级的 TPS 的代价是其极高的中心化程度和极低的鲁棒度。这一点我们将在下文予以讨论。总而言之，在目前已经运行的区块链公链系统中并没有在安全稳定的前提下达到高可用性的 TPS 的项目。这是限制区块链落地应用的最重要因素之一。

算力集中

在主流的区块链共识算法中 POW 和 POS 需要挖矿。挖矿是一种货币的发行机制，但其更是一种维持系统稳定性的筛选机制和激励机制。挖矿机制吸引矿工参与区块链网络的维护。参与者越多整个

[1] "Blockchains: The great chain of being sure about things". The Economist. 31 October 2015. Archived from the original on 3 July 2016. Retrieved 18 June 2016. The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the crypto currency.

[2] Fisher, Daniel (2015-05-25). "Visa Moves at the Speed of Money". Forbes. Retrieved 2016-05-01.

系统的去中心化程度就越高，稳定性和鲁棒度也越高。相反，如果在一个挖矿系统中算力的集中度过高，就会容易发生 51%攻击或发生硬分叉。这是因为算力集中本质上是一种中心化倾向，因此其可以破坏整个区块链网络的稳定性，让网络变得容易收到手握大部分算力的个人或组织的影响。从计算机学的角度看，算力集中将极大地损害整个系统的鲁棒度；从社会学和经济学的角度上看，算力集中将严重影响整个区块链系统的共识和其能承载的最高市值。因为大众很难去相信一个很容易被少数人操控或影响的系统可以承载他们的财富。

在比特币发明之初，中本聪认为普通的笔记本电脑或者台式机就可以担任一个比特币的节点。这样整个比特币系统就有很高的分散度和鲁棒性，人人可以参与维护网络并比较平均地分享比特币奖励。但事实上随着比特币市值的发展有一些人不断地发明新的工具去更高效地挖矿。于是就出现了更专业的 GPU 挖矿、ASIC 挖矿、甚至矿池挖矿。专业的矿池所需要的矿机价格昂贵且耗电量巨大，需要专业的团队进行运营和维护。这一发展是比特币的发明者在一开始所未曾预料到的，其极大地阻碍了大众对挖矿的参与。使得大众根本无法通过挖矿这种手段去参与比特币，无法成为比特币的节点。一方面，这种力量阻碍了比特币共识的扩张；另一方面，集中的算力使得少数人可以操控比特币的分叉，随易发动 51%攻击。虽然在大多数情况下，矿池的拥有者并没有发动攻击的动机，但历史经验表明，这种情况是的确会发生的。拥有比特币 51%左右算力的比特大陆，就成功地操控了比特币的硬分叉 BCH。[3]以 POW 为共识算法的以太坊也存在同样的问题。也曾经发生过类似的事件。本文在此不再赘述。而且，历史经验也表明正如我们所预料的那样，每次硬分叉的发生都会严重地打击大众的共识和对此系统的信心，从而导致币值的下跌。因此，算力集中也是区块链公链系统的一个重大缺陷。

高耗能

在目前所有的区块链公链系统中，最成功的是比特币系统和以太坊系统。这两个系统出现的时间很早而且使用的都是 POW 共识算法。两个系统成功的原因很多很复杂，在此本文不予深入探讨。不可否认的是，他们的成功与 POW 这一核心算法有着莫大的关系。因为 POW 共识算法是目前最能保证高去中心化和高稳定性的共识算法。而这两个特征是区块链最重要的特征。试想，如果不需要高度的去中心化和高鲁棒性，则传统的数据库就可以胜任几乎所有的应用场景，不需要区块链技术的存在。

POW 虽然可以做到比较公平和高度去中心化，但其却存在天然的缺陷，也就是极高的，无效的能耗。POW 通过让节点去寻找一个小于某数的哈希值来争夺记账权。这种方法在数学上是非常公平的。但是，随着竞争节点人数的增加，寻找这一数值的难度会变得越来越高。直到需要消耗非常多的电力，才能够获得一次记账权。据环保人士于 2018 年做的不完全统计，比特币每年消耗的电力在 33 亿千瓦左右，相当于当年全球总用电量的 0.5%。[4]而根据欧盟提供的数据，丹麦和爱尔兰两国的电力消耗总和在 2018 年只有 25 亿千瓦。也就是说为了维持比特币系统，全球每年要多消耗 2 到 3 个小国家的电力。这些消耗的电力产生的热量毫无意义，几乎百分之百被浪费掉。生产这些电力会产生大量

[3] Antonopoulos, Andreas (2017). Mastering Bitcoin: Programming the Open Blockchain (2 ed.). USA: O' Reilly media, inc. p. Glossary. ISBN 978-1491954386.

[4] "Bitcoin Energy Consumption Index - Digiconomist". Digiconomist. Retrieved 2018-06-08.

的污染，产生极大的负外部性。这些额外产生的用电消耗以及污染仅仅是为了维持比特币系统的稳定性。如此高的维护费用远远超过了全世界任何一个计算机系统。其造成的负面影响，由全世界人民共同承担。很显然这是 POW 系统的一个重大缺陷。然而，目前并没有出现第二个能够取代 POW 并且解决高能耗问题的共识机制。DPOS，PBFT 和以 DAG 为基础的共识都有严重的中心化问题和低鲁棒性问题。他们解决了 POW 的一个缺陷，但又产生了另外一个缺陷。因此他们都不能成为 POW 完美的替代品。

中心化

正如前文所说，在很早的时候（比特币发明之初）人们就注意到了 POW 的高耗能、高污染和低吞吐量问题。并试图用新的共识算法来解决这一问题。于是很多全新的共识被提出。其中比较著名和被比较广泛使用的包括 POS，DPOS，PBFT，以 DAG 为基础的其他共识算法。POS 也需要通过寻找特定哈希值的方式挖矿，但其引入了幸运值的概念。从而大大的降低了挖矿的能耗，部分地解决了 pow 的高能耗问题。但是其幸运值系统很容易诱发马太效应，引起币的高度集中。过度集中的代币分配，会摧毁整个区块链的经济系统。这是 POS 共识算法所引发的代币集中问题。

另外一些共识机制如 Dpos，PBFT，以 DAG 为基础的共识等直接取消了挖矿的机制，因此彻底地解决了高能耗的问题。但是这些共识机制都存在超级节点。例如 EOS 的超级节点只有 21 个；PBFT 的节点基本上不能超过 100 个（通常在 7-30 个之间）；Byteball 使用 DAG 为基础的共识，其只有 12 个节点（超级节点）。这些共识算法的节点数基本都在 10 到 100 个之间。为了实现高 TPS，在实际的项目中往往采用 30 个以下的节点。如此少的节点数，整个系统甚至不能够被称为是去中心化的，或许只能够被描述为多中心化。中心化的问题很明显会带来低的鲁棒性。攻击者可以识别和预测节点，通过攻击少数几个节点来使整个系统瘫痪（例如，太少的节点数在理论上很难防御简单粗暴的 Ddos 攻击）。事实上，EOS 的系统就有被成功攻击的记录。Byteball 的节点也有因为流量压力大而瘫痪的记录。因此，一些区块链专家甚至认为这类系统并不能被称之为完全的区块链，或者应该将他们归类为区块链和传统的多中心服务器的过渡系统。这些系统解决了之前所提到的 POW 的高耗能问题，但却陷入了新的中心化问题。

量子攻击

由于 Shor 算法 ，量子计算机可以很容易地在多项式时间内分解大整数因子，从而有效地破解 RSA。Shor 算法的启用可解决离散对数问题以及今天的数字签名（例如 DSA，ECDSA 以及 EdDSA），使得它们变得无效。建立量子计算机的竞赛已经开始。像谷歌、微软、IBM、D-Wave 以及英特尔这样的公司处在了领先位置。[5]然而，截至目前，我们还未能建立一个具有数千个稳定量子位的计算机可使经典公钥密码技术变得过时。然而，该领域已经有了显著进展。一些乐观人士预测，在接下来的 10 到 20 年内，一台大型量子计算机可能能够破解非对称加密，从而破解公钥加密系统。其会带来的安全影响将是巨大的。如果 RSA 或椭圆曲线加密算法（ECC）的安全性无法得到保障，比特币和其他不抗量子攻击的区块链系统的市值将会崩溃。

[5] Quantum Information Science and Technology Roadmap for a sense of where the research is heading.

易分叉

完全开放的，去中心化的公链会有很多节点，而且节点应该是可以任意加入和退出的 。只有这种类型的系统才可以保证高鲁棒度和去中心化。以 POW 和 POS 为基础的公链系统符合这样的标准。但是这样的系统又会遇到易分岔的问题。[6]因为这样开放的挖矿机制有可能出现两个节点同时（或者几乎同时）找到随机数而获得打包权。系统很容易因此分叉。虽然不同的系统都尝试用各种方法尽量地避免孤块和分叉的出现，但是如比特币和以太坊等网络还是出现了很多的分叉，例如比特币的分叉币 BCH,BTG,B2X,BCD,SBTC,BCHC 和以太坊的分叉币 ETC。这些分叉行为使得市场上多出了很多高竞争性的 altcoin，这很大程度上削弱了原系统的总市值和大众对该系统的信心。因此分叉问题也是区块链系统需要避免的痛点。

低可用性

可用性是一个比较模糊和宽泛的概念。主要指一个区块链系统能够多大程度上运用于实际生活。比特币作为区块链 1.0，只有支付用途和价值存储用途。它的可用性是非常有限的。以太坊加入了虚拟机，做到了可编程金融。大大地提高了整个系统的可用性。但是于此同时，他们的 TPS 不足又限制了他们的可用性。以太坊的智能合约编程语言 solidity 比较小众和相对复杂这也限制了其可用性。另外，智能合约的编写往往存在很多漏洞，这些漏洞的产生也限制了区块链的可用性。最后，区块链系统往往是封闭的，缺乏与真实世界的有效交互和可信的 Oracle，这也是严重制约区块链可用性和落地应用的因素之一。

参与度不足

区块链公链项目并没有基本面作为支撑。通常来讲，其市值只取决于大众的共识。也就是说，对其认可的人数越多，关心的人数越多，安装钱包和拥有其代币的人数越多，其币值就越高。反之，其市值就越低。

在一个项目发起之初。共识往往需要项目方用真金白银建立大量的社区和召开线上线下共识大会来建立。无论项目方募到多少钱，共识的发起方和推动方往往只是发币者一方。这是一种高耗能和低效率的共识构建方式。缺乏共识导致这些项目的参与度不足，而参与度的缺失又反作用于共识。这样的负向循环使得整个公链项目的市值难以维持。这就是现在绝大多数区块链项目所面临的困局。

就整个区块链代币圈而言，也存在参与度不足的问题。因为圈外的人往往只能通过购买代币的方式进入币圈。而无论是币价上升还是下跌，缺乏共识和信仰的，刚刚加入币圈的人都有很大的冲动抛售自己手中的代币离开币圈。这就使得币圈的边界难以持续性地扩展。真正可以稳定地参与区块链的币圈的大众人数有限，这是限制整个区块链代币总市值的重要因素（甚至有可能是最重要的因素）。

[6] Thieme, Nick (4 August 2017). "Bitcoin Has Split Into Two Cryptocurrencies. What, Exactly, Does That Mean?". Slate. Retrieved 8 March 2018.

ULAM

Ulam 是由清华大学高等研究中心团队研发的底层共识算法创新项目。Ulam 共识的灵感来自波兰犹太人数学家斯塔尼斯拉夫·马尔钦·乌拉姆（Stanisław Marcin Ulam）。斯塔尼斯拉夫·马尔钦·乌拉姆提出过 Luck number 的概念。它采用与生成素数类似的“算法”生成。清华大学密码学博士吴彦冰由此受到启发，发现利用哈希函数的特性可以创造出超低能耗、完全去中心化、高度稳定的全新共识算法。Ulam 的发明让我们意识到，达成共识竟如此简单。Ulam 不需要进行哈希计算竞赛，可以允许低功耗的手机、智能手表、路由器等参与“挖矿”。Ulam 是继 POW、POS、DPOS、PBFT、DAG 类共识算法之后的第六个在共识算法上有重大创新的区块链项目；也是全国目前唯一一个完全由中国背景团队做出的包含共识算法层重大突破的区块链项目。

Ulam 共识可以做到超级碎片化节点（任何智能手机、笔记本电脑、pad、手表等智能设备均可以参与挖矿）；完全去中心化（百万级节点）；永不产生比特币一样的算力集中化；49%恶意节点容错（目前所有共识算法中的最大容错率）；TPS 可达 10000+，确认时间 1s，超低分叉率；可以证明安全共识协议；抗量子攻击。

亮点：

- **Ulam 共识可以做到超级碎片化节点**
- **完全去中心化**
- **永不产生比特币一样的算力集中化**
- **49%恶意节点容错率**
- **超高 TPS**
- **抗分叉**
- **抗量子攻击**
- **天然促进大众共识与参与度**

共识算法

我们对于现有共识机制存在的问题重新设计出了一种新的共识机制 Ulam 共识算法。Ulam 共识算法是根据节点的幸运值来决定节点挖矿成功的概率。每个节点的幸运值是根据节点持有币的多少和持有币的时间来计算出来的一个值。每次挖矿的时候，每个节点都会根据幸运值大小的不同产生出相应个数的随机数。幸运值越大将会产生出越多的随机数。随机数通过 VRF 算法产生，保证产生的随机数是可验证的随机数。出块的时候通过时间戳上的块信息产生出可验证的随机数。挖矿节点之前产生的随机数若与此时产生的随机数相同则获得打包记账的权力。如果有多个节点同时获得有效随机数，将以幸运值长的节点获得记账权。这样可以有效地预防分叉。在节点获得记账权之后，这个

节点的幸运值将会归零。这样可以防止 Ulam 产生类似 POS 一样的高马太效应。这个挖矿过程与乐透中奖方式十分相似，每个节点的幸运值越大，产生的随机数机会越多，相当于中奖概率就会越大。Ulam 共识算法可以有效地防止矿场和矿机的出现，能减少挖矿造成的大量资源浪费。Ulam 共识算法在性能方面也能有很好的表现。从理论的角度讲，Ulam 算法的 TPS 可以达到无限大，在实际使用中可以满足金融、交易、溯源等各种场景的应用。Ulam 在实现高吞吐量的同时也保证了区块链最本质的去中心属性。我们相信基于 Ulam 共识的区块链将是下一代区块链的标准。

幸运值：Ulam 是根据节点的幸运值来决定挖矿概率的，不需要进行 hash 值的计算。 每个节点根据幸运值的大小，决定拥有的随机数的个数。节点的幸运值越大拥有的随机数越多。在每次出块的时候被选为记账节点的概率也就越高。

举例： 如果 Alice 的幸运值是 3 就会有 3 个随机数，比如 1、3、4。 Bob 的幸运值是 5 就会有对应的 5 个随机数比如 1、2、5、7、8。出块的时候会根据链上之前的信息计算出一个随机数，比如 5。因为 Bob 的随机数中出现了 5，所以 Bob 就拥有了本次的记账权并可以获得挖矿奖励。如图 1 所示。

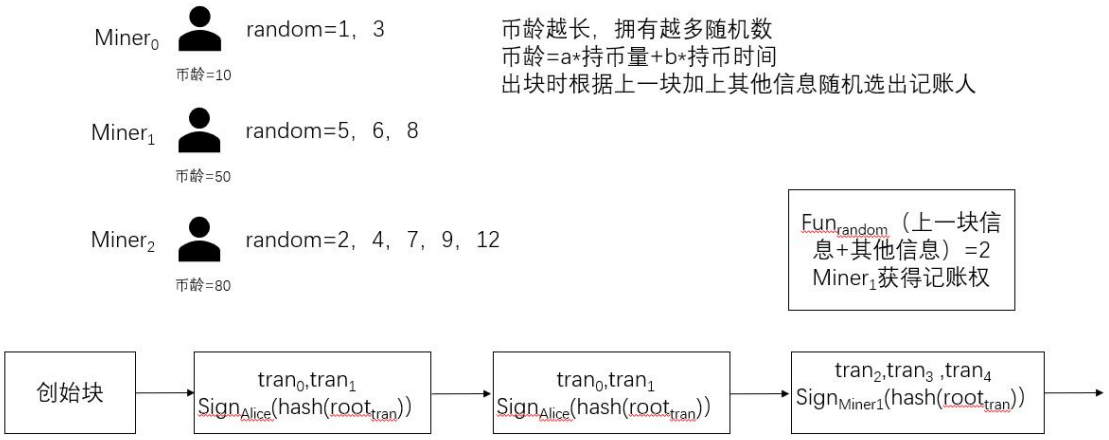


图 1,共识算法原理图

高 TPS

Ulam 设计的全新非交互式交易验证算法（NITCV），可以使 TPS 最低达到 10000。Ulam 使用知识证明的方法构造出非交互式交易验证算法。知识证明简单的来说就是证明者说服验证者相信其知道某个“知识”（信息）。一般的证明方法为构造多项式时间知识提取器提取“知识”。普通的区块链在验证交易时需要所有矿工都对区块中的交易进行验证，Ulam 的非交互式交易验证算法通过矿工打包区块后对区块内的交易验证后生成交易验证证明。其他矿工只需要验证打包节点产生的证明而不需要去验证块中的交易，这使得 TPS 大大提高。在原有的模式下，假设一个区块有 1000 笔交易，所有矿工都需要去验证这 1000 笔交易。这无疑会消耗大量的时间从而降低 TPS。而使用 Ulam 独创的非交互式交易验证算法，只需要一个矿工验证 1000 笔交易，其他矿工只需要验证打包节点生成的证明。因此，速度会比之前提高 1000 倍。非交互式交易验证算法可以使 TPS 理论上达到无限大。但是受限于网络和处理器处理的速度，目前实测 TPS 为 10000。随着网络和处理器等其他技术水平的提高，Ulam 系统的 TPS 还会有更大的提高。NITCV 的详细介绍见技术黄皮书。

抗算力集中

Ulam 不需要通过计算 Hash 原像来选出打包节点，因此在 Ulam 中并不存在算力竞赛的现象。Ulam 通过设计的算法来计算出每个节点的幸运值，从而根据每个节点的幸运值完全随机的挑选出打包节点。也就是说，一个手机充当的节点和一个超级计算机所充当的节点，当他们幸运值一样时，他们获得打包权的机会是均等的。运算能力并不能在 Ulam 算法中使节点增加获得打包权的机会。因此大众没有激励去制造和运用专业的矿机和矿池来对 Ulam 进行挖矿。因此 Ulam 系统中不存在算力集中的问题。

当然，我们不能排除，当 Ulam 的市值很高而使得 Ulam 挖矿变得非常有利可图时有人或组织建立以普通的智能设备为基础单位的矿池以追求更高的获得挖矿奖励的可能性。但是，即使发生了这种情况，Ulam 矿池主相对于散户的竞争力也远远没有目前的 POW 体系中的矿池主对于散户的竞争力大。因为在 POW 体系中，散户完全没有挖矿的能力。而在 Ulam 中，矿池并不会很大程度地影响散户挖矿的概率。况且，如果分散度足够大，大部分的挖矿能力依然会在广大散户的手中。正因为这样的预期，在 Ulam 体系中大概率不会出现大型的矿池，因为这样的矿池缺乏客观的预期收益激励。

超低耗能

Ulam 的挖矿机制采用哈希随机数生成，不需要寻找特定的哈希。因此，一台超级计算机和一台普通的智能手表手机找到正确的随机数的概率是一致的（不考虑币零的情况下）。从而，成功地做到了超低能耗。因为用专业的矿机或者计算机用来挖 Ulam 不会有任何的优势。因此 Ulam 的参与者必定是普通的用户用的笔记本电脑、台式机、智能手表、手机、平板电脑等设备。实测表明 Ulam 挖矿所需要的能耗不会超过这些智能设备日常能耗的 5%（如果这些设备被用于 3D 建模，运行大型 3D 游戏等则这个百分比会更低），几乎可以忽略不计。因此，Ulam 挖矿几乎不需要消耗节点的额外能耗，节能环保。其可以完美地解决 POW 的高耗能和高污染问题。

完全去中心

因为专业的矿机在进行 Ulam 挖矿时并没有优势，所以在 Ulam 的生态系统中将不会有专业矿机的出现。而大众会用自己日常的设备比如手机、笔记本电脑、台式机、Pad、智能手表等进行挖矿。由于参与的门槛低，大众就可以高度参与 Ulam 节点的运行。因此即使有 Ulam 的矿主用大量的手机建立 Ulam 矿池，这些矿池对于大众来说也不会有不可逾越的绝对优势。也就是说，Ulam 的硬件生态系统将可以做到完全去中心化。

目前比特币和以太坊之所以会在挖矿能力上中心化是因为矿机、矿池、电费价格高昂。普通人没有办法参与。而决定要通过挖矿来赚钱的人们有强烈的动机去不断的扩大矿池，以降低自己的单位矿机的电费成本、管理成本、储存成本。这就使得以 POW 为基础的挖矿体系会有天然的马太效应使得算力集中化。然而，如果普通的智能设备都可以挖矿，则大众可以零门槛参与。分散的挖矿比集中的挖矿需要更低的场地成本、电费成本、管理成本以及运营成本。因此，集中式挖矿相对于大众分散式挖矿将不会有太大的优势。失去了 POW 的天然算力集中的刺激，Ulam 的节点将可以完全分散在大众的用户之中。目前，全球的手机、电脑、pad 等智能设备的数量超过 100 亿台。Ulam 将是人类历史以来最分散，最去中心化的计算机系统。

算法促进参与

区块链公链项目的市值主要取决于大众的共识，而共识又主要取决于参与的人数和大众的信心。绝大多数项目的共识需要通过大会、线下活动、网上宣传来获得。这种方法效率很低，没有病毒传播的效果。一旦项目方停止投入真金白银，这样的项目往往就会冷却下来。或者一但币价剧烈下跌，大众就会对该项目失去信心。Ulam 在算法上解决了这个问题。Ulam 的挖矿机制与幸运值有关。具体的说，一台挖矿设备能获得 Ulam 的一次记账权的概率不是取决于这台设备的算力而是取决于运气与幸运值。幸运值与挖到 Ulam 的概率正相关。而幸运值又与持币数量和持币时间正相关。因此，Ulam 的共识机制有鼓励用户持有 Ulam 的作用。在币价上升后，持币者有激励不会一次性卖出自己所有的持仓，而会留下一部分继续挖矿。在币价下跌时，持币人有动力不会一次性全部割肉卖出，而会留下一部分继续挖矿。因为挖矿之所得可以弥补币价下跌所带来的损失。而对于完全没有币的新用户，他们有动力购买一定数量的 Ulam 用于挖矿。这样，Ulam 在算法上实现了鼓励新用户进入，老用户持仓。并在涨跌中赋予持币者信心的作用。而这些作用都是 Ulam 天然具备的，不需要项目方持续投入法币和人力进行共识的建立与维护。

抗量子攻击签名算法

NTRU(Number Theory Research Unit)算法是 1996 年由美国布朗大学三位数学教授发明的公开秘密体制 。这是一个基于多项式环 （其中 N 是一个安全参数）的密码体制。它的安全性依赖于格中最短向量问题（SVP）。相对于离散对数或大数分解等公开秘密体制来说，它有许多优势。在安全性方面，NTRU 算法具有抵抗量子计算攻击的能力，而 RSA 和 ECC 算法是无法抵抗量子计算的。当前，对于用什么公钥密码来替代正在大量使用的 RSA 和 ECC，主要有以下互相竞争的技术解决方案：NTRU 公钥密码体制、McEliece 公钥密码体制、MQ 公钥密码体制。

McEliece 公钥密码体制的安全性基于纠错码问题，安全性强，但计算效率低。MQ 公钥密码体制，即多变元二次多项式公钥密码体制（Multivariate Quadratic Polynomials in Public Key Cryptosystem），基于有限域上的多变元二次多项式方程组的难解性，在安全性方面的缺点比较明显。相比之下，NTRU 公钥加密体制算法简洁、计算速度快、占用存贮空间小。

- **密钥的生成**

  随机生成 2 个多项式 $f \in R_f, g \in R_g$，其中 f 必须满足在模 p 和模 q 的情形下均有乘法逆元。如果参数选择合适，大多数的 f 都有逆元，而且可以通过改进欧几里得算法很容易找到这些逆元。用 F_p, F_q 分别表示这两个逆元，

  即

  $$F_q \otimes f \equiv 1 \pmod{q}$$

  $$F_p \otimes f \equiv 1 \pmod{p}$$

然后，计算

$$h \equiv F_q \otimes g \ (\mathrm{mod}\, q)$$

多项式 h 即为公钥，私钥为 f ，实际上 F_p, F_q 也必须保密。

- **加密算法**

假设要加密的消息 $m \in R_m$ ，随机选取多项式 $\phi \in R_\phi$ ，然后利用公钥 h 进行如下运算

$$e \equiv p\phi \otimes h + m \ (\mathrm{mod}\, q)$$

多项式 e 为消息 m 对应的密文。

- **解密算法**

收到密文 e 后，可利用私钥 f 进行解密。 F_p 必须预先计算。解密首先计算

$$a \equiv f \otimes e \ (\mathrm{mod}\, q)$$ 其中选取多项式 a 的系数在区间 $[-q/2, q/2]$ 内。然后通过如下计算恢复明文：$F_p \otimes a \ (\mathrm{mod}\, p)$ 。

- **解密算法的工作原理**

多项式 a 满足：

$$\begin{aligned} a \ &\equiv f \otimes e \ \equiv f \otimes p\phi \otimes h \ + f \otimes m \ (\mathrm{mod}\ q) \\ &= f \otimes p\phi \otimes F_q \otimes g \ + f \otimes m \ (\mathrm{mod}\ q) \\ &= p\phi \otimes g \ + f \otimes m \ (\mathrm{mod}\ q) \end{aligned}$$

对于最后一个多项式 $p\phi \otimes g \ + f \otimes m$ ，如果参数选择合适，这个多项式的系数都可以限制间 $[-q/2, q/2]$ 内，因此，这个多项式在所有系数模 q 的情形下不会改变。这意味着将 $f \otimes e \ (\mathrm{mod}\, q)$ 的所有系数都选取在区间 $[-q/2, q/2]$ 内，的确可以得到正确的 $a = p\phi \otimes g \ + f \otimes m \in Z[X]/(X^N - 1)$ 。

将多项式 a 进行模 p 约化，可得到 $f \otimes m \ (\mathrm{mod}\, p)$ ，然后用 F_p 去乘上述多项式即可得到相应的明文消息 $m \ (\mathrm{mod}\, p)$ 。

稳定性

女巫攻击

Sybil 攻击是指利用社交网络中的少数节点控制多个虚假身份，从而利用这些身份控制或影响网络的大量正常节点的攻击方式 。Sybil 攻击最早出现于无线通信领域中。Douceur 第一次在点对点网络环境中提出，他指出这种攻击将破坏分布式存储系统中的冗余机制。后来 Karlof 和 Newsome 等都指出 Sybil 攻击对传感器网络中的路由机制同样存在着威胁。在区块链中也存在 Sybil 攻击。Ulam 是根据幸运值累加来进行挖矿的。而幸运数的产生需要依赖上一个节点的信息。因此，即使一个恶意节点可以造出许多地址，但是造出的地址都是没有幸运值的。因为哈希函数的特性使得攻击者不可能伪造出由上一个节点信息所生成的随机数，所以不可能对 Ulam 系统进行 Sybil 攻击。

51%攻击

区块链分叉时选择最长的链做为正确链是比特币的一种预防分叉的规则。不同的系统这种选择的机制会略有差异，但是总体的原理都比较相似。链的生成速度与计算能力直接相关，当攻击者掌握 51%的计算能力，就能够任意选择他希望区块的分叉，从而可以实现双花攻击。这在 POW，POS 上都是可以类似实现的。因此，这种攻击方式被称之为 51%攻击。Ulam 生成块时不依赖算例的大小，是完全随机选出的打包节点。因此不存在 51%的算力的概念。由于 Ulam 出块时间是固定的，所以在攻击者意图产生双花时系统可以很容易识别其第二次无效交易。因此 Ulam 可以有效防止双花的产生。

DDOS 攻击

DDOS（Distributed Denial of service）攻击是指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力。[7]其主要的原理是通过运算和带宽的过载使得服务器瘫痪从而达到攻击的目的。这种攻击方式很原始和粗暴，但是往往很难防御。Ulam 主要从三个方面防止 Ddos 攻击。

- **NITCV ：**Ulam 通过独创的非交互式交易验证（NITCV）来对交易进行检查和验证。NITCV 使得节点所需要处理的信息量和系统所依赖的带宽大大减小因此可以一定量的减小 DdoS 攻击的发生。

- **随机节点打包：**Ulam 下一个打包的节点完全是随机产生的，因此攻击者无法找到下一个应该攻击的节点。即 Ddos 攻击者无法找到狙击的目标。这样一来，对 Ulam 实施 Ddos 攻击几乎是不可能的。

- **高度其中心化：**即使攻击者不能确定一个可攻击的节点，其依然可以选择大面积攻击，即一次性攻击多个节点。但是正如前文所述，Ulam 的节点可以是手机、手表、平板电脑。未来，Ulam 系统将拥有成千上万甚至上百万个节点。这又使得大面积攻击的难度指数级增长。综合以上的三个方面，Ulam 系统可以完美地防御 Ddos 攻击。

量子攻击

[7] "Understanding Denial-of-Service Attacks". US-CERT. 6 February 2013. Retrieved 26 May 2016.

Ulam 使用的基于格基困难问题的抗量子计算机攻击算法 NTRU。NTRU 公钥密码体制和实现方法，并对其安全性进行了研究。NTRU 算法被公认为是公开密钥体制中最快的算法。[8]通过对 NTRU 的安全性分析和比较来看，它对系统要求极低，不需要较高的计算机能力以及较复杂的硬件设备。它高速、低需求、易实现、快速而安全的特性使得它适合于安全性要求高、体积、成本、内存及计算能力等受限的电子设备。因此其必将在诸如智能卡、移动通信系统、保密数据网、电子商务、电子现金和微型支付系统及认证系统等业务方面发挥重要作用。它完全有可能在公钥密码体制中占有重要地位，去代替现在非常流行的 ECDSA 密码体制。

延时攻击

延时攻击是指攻击者可以掌握网络中网络数据包的延时，通过延时转发区块来对区块链产生分叉，之后进行双花等攻击。Ulam 出块的时间是固定的，所以在安全的网络环境下不会产生延时攻击。当然，如果网络环境封闭，其时间体系也有可能被操控。但是，由于 Ulam 是高度去中心化的。在高度跨硬件平台，跨国界的情况下，要操控整个网络的时间体系或传输速度是几乎不可能的。其难度超过了任何个人甚至任何国家的能力。因此可以认为 Ulam 对延时攻击是安全的。

同构链

同构在数学中表示两个图形存在某些性质相同，但是表现显示不通，并且存在映射关系。同构链是基于 ULAM 主链开发的侧链，使用 ULAM 共识运行出块，可以看成是一个独立的公链。同构链是和 ULAM 主链单向连接的，采用单向锚定，安全性可以由 ULAM 主链保证，同构链发生问题不会影响到 ULAM 主链。同构链也有共识机制，有独立的节点。同构链与 ULAM 主链具有相同的性质，但是在某些地方存在不同，同构链可以根据不通行业的需求来改变或者添加相应的功能和数据块。

同构链的优势：

1. 用 ULAM 主链的共识——随机数，低能耗，转账速度快，TPS 高
2. 完全去中心化，不可篡改，分布式账本，共识信任机制，开放性，匿名性
3. 自行设置激励机制
4. 基于同构链发行 DAPP
5. 基于同构链制作自己的智能合约
6. 解决行业痛点

[8] Robertson, Elizabeth D. (August 1, 2002). "RE: NTRU Public Key Algorithms IP Assurance Statement for 802.15.3" (PDF). IEEE. Retrieved February 4, 2013.

ULAM 同构链架构如下图：

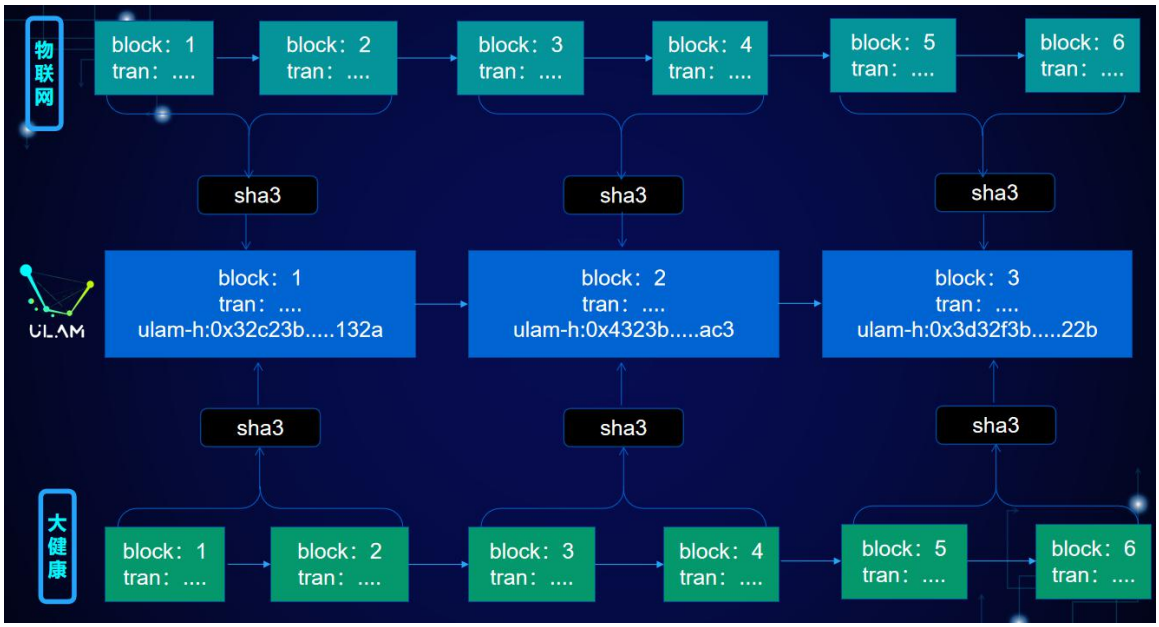


图 2：ULAM 同构链结构

生态系统

虚拟机

Ulam 虚拟机（Ulam Virtual Machine，简称 UVM），作用是将智能合约代码编译成可在以 Ulam 系统上执行的机器码，并提供智能合约的运行环境。它是一个对外完全隔离的沙盒环境，在运行期间不能访问网络、文件，即使不同合约之间也有有限的访问权限。

UVM 特点：

- UVM 是一种基于栈的虚拟机（区别于基于寄存器的虚拟机），用于编译、执行智能合约。
- UVM 是图灵完备的（图灵完备是指：具有无限存储能力的通用物理机器或编程语言，简单来说就是可以解决一切可计算的问题）。
- UVM 是一个完全隔离的环境，在运行期间不能访问网络、文件，即使不同合约之间也有有限的访问权限。
- 操作数栈调用深度为 1024。
- 机器码长度一个字节，最多可以有 256 个操作码。

指令：

文件 opcodes.go 中定义了所有的 OpCode，该值是一个 byte，合约编译出来的 bytecode 中，一个 OpCode 就是上面的一位。opcodes 按功能分为 9 组（运算相关，块操作，加密相关等）。

指令函数集：

jump.table.go 中定义了四种指令集合，每个集合实质上是个 256 长度的数组，指令集分为了四种，分别是 frontier Instruction Set、home stead Instruction Set、byzantine Instruction Set、Constantinople Instruction Set（荒地，农庄，拜占庭，君士坦丁堡）；应该是对应了 UVM 的四个发展阶段。指令集向前兼容。

解释器：

interpreter.go 中有解释器的入口函数 run，根据用户给定的输入数据，循环对智能合约中的代码进行解析，翻译成对应的指令函数集中的函数，并运行。

Gas 计算：

gas_table.go，gas.go,根据不同的运算，计算消耗的 gas，具体的方法都定义在 gas_table 里面。

智能合约：

contract.go，合约是 UVM 智能合约的存储单位也是解释器执行的基本单位，包含了代码，调用人，所有人，gas 相关的信息。contracts.go ，包含了一些 UVM 预先编译好的一些合约，例如 ucrecover、sha256hashripemd160hash。

Memory：

emory.go，内存用于一些内存操作（MLOAD,MSTORE,MSTORE8）及合约调用的参数拷贝（CALL，CALLCODE）。内存数据结构，维护了一个 byte 数组，MLOAD，MSTORE 读取存入的时候都要指定位置及长度才能准确的读写。

Stack：

stack.go，UVM 中栈用于保存操作数，每个操作数的类型是 big.int.执行 opcode 的时候，从上往下弹出操作数，作为操作的参数。

Statedb：

go-Ulam/core/state/statedb.go，合约本身不保存数据，合约及其调用类似于数据库的日志，保存了合约定义以及对他的一系列操作，只要将这些操作执行一遍就能获取当前的结果，但是如

果每次都要去执行就太慢了，因而这部分数据是会持久化到 stateDb 里面的。code 中定义了两条指令 SSTORE SLOAD 用于从 db 中读写合约当前的状态。

Log：

logger.go，对 uvm 运行过程，对 memorty，stack，statedb，还有一些信息的记录。

下图是 UVM 的逻辑结构图：

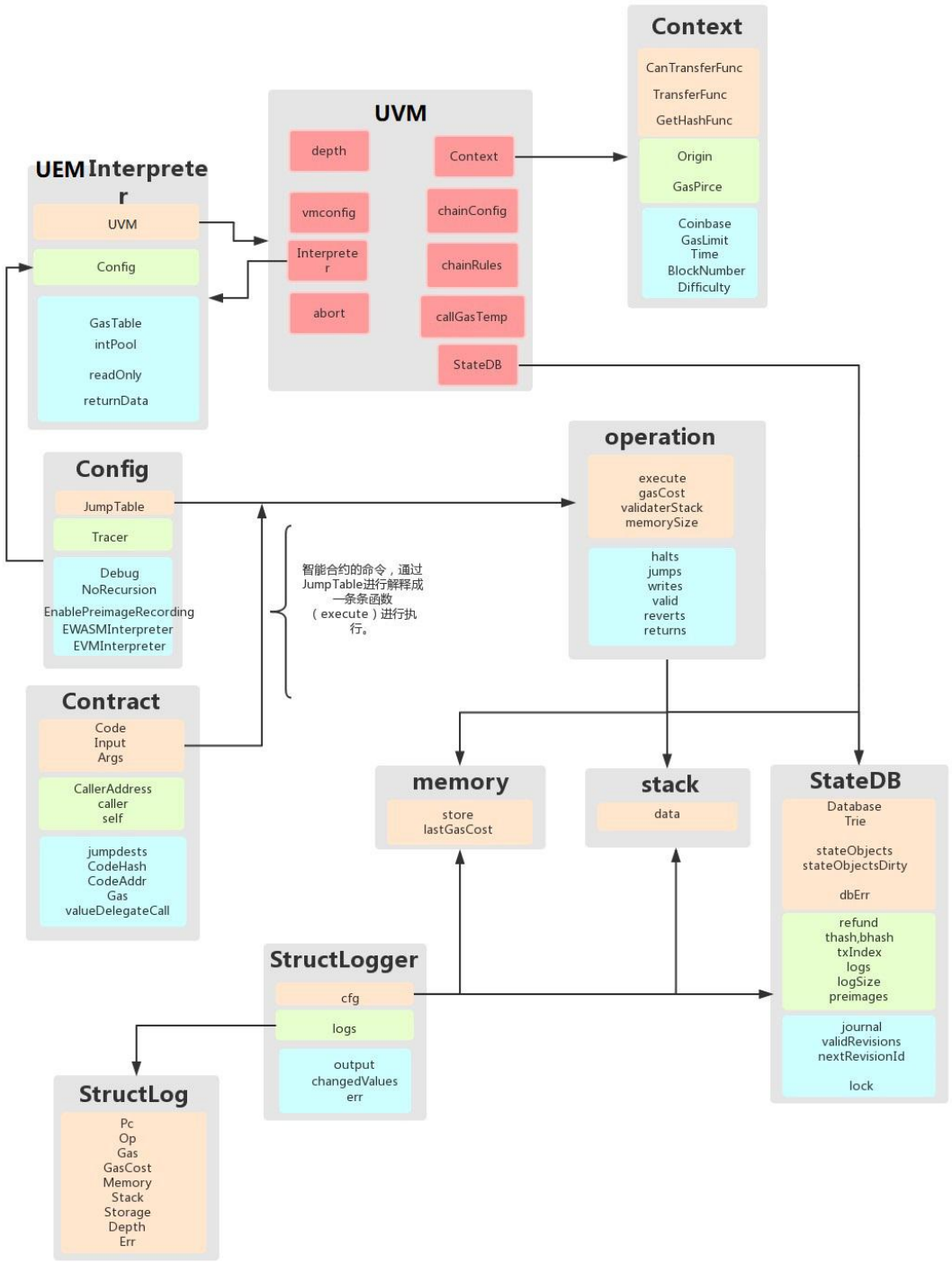


图 3：UVM 结构图

API

获得账户信息 GET： ulamchain.io:6000/account

获得区块信息 GET：ulamchain.io:6000/block

获得交易信息 GET：ulamchain.io:6000/get/transaction

提交交易 POST：ulamchain.io:6000/new/ transaction

智能合约

智能合约是 1994 年由密码学家尼克萨博（Nick Szabo）最先提出的理念，几乎与互联网同龄。根据 Nick Szabo 的定义：当一个预先编好的条件被触发时，智能合约执行相应的合同条款。区块链技术给我们带来了一个去中心化的，不可篡改的，高可靠性的系统，在这种环境下，智能合约才大有用武之地。Ulam 具备独立的智能合约体系：Ulam Contract。

Ulam Contract 包括以下特性：

- 确定性
- 高性能
- 拓展性

其合约类型包括：

- 验证合约
- 函数合约
- 应用合约。

从性能角度来说，Ulam 采用了轻量级的 UVM（Ulam Virtual Machine）作为其智能合约的执行环境，其启动速度非常快，占用资源也很小，适合像智能合约这样短小的程序。通过 JIT（即时编译器）技术对热点智能合约进行静态编译和缓存可以显著提升。ULAM 虚拟机的指令集中内建提供了一系列的密码学指令，以优化智能合约中用到密码学算法时的执行效率。此外，数据操作指令直接对数组及复杂数据结构提供支持。这些都会提升 Ulam 智能合约的运行性能。

Ulam 智能合约实现可拓展性的方法是通过高并发和动态分区的形式，结合其低耦合的设计完成的。低耦合合约程序在一个虚拟机（Ulam 虚拟机）中执行，并通过交互服务层与外部通信。因此，对智能合约功能的绝大部分升级，都可以通过增加交互服务层的 API 来实现。

应用场景

Ulam 生态中将包括 Ulam 主链，Ulam 钱包区块链浏览器，虚拟机以及智能合约系统。由于去中心化，高 TPS 和安全性的实现。Ulam 生态将可以应用于多场景的落地，真正地将区块链落地应和改变世界。

- **大健康产业：**基于 Ulam 的架构可以设计并发行众多医疗币以及医疗区块链平台。开发者可以在该数据链上打造大健康数据平台，平台上的利益相关者包括个人用户、健康魔盒集成方、医疗服务提供方、医疗数据消费商、投资者、Ulam 平台。健康魔盒作为医疗数据链的核心与流量入口。

- **物联网：**基于 Ulam 的架构设计并发行多种物流币。通过区块链特有的分布式资产交易记录和数据不可篡改的特性，Ulam 可以有效地在以下四种业务场景赋能物流产业：快递保价、公益活动、行业黑名单共享、快递安全监管， 进一步完善流服务。

- **交通出行：**Ulam 可协助汽车厂商或共享汽车平台部署区块链工具，帮助所有者追踪汽车维修历史、车辆行驶行为、以及其他相关数据可以利用手机应用实现车辆的上锁/解锁，获得临时访问权限可以通过数字钱包与积分，鼓励租赁或借用车辆的司机每周记录其里程并换取积分。

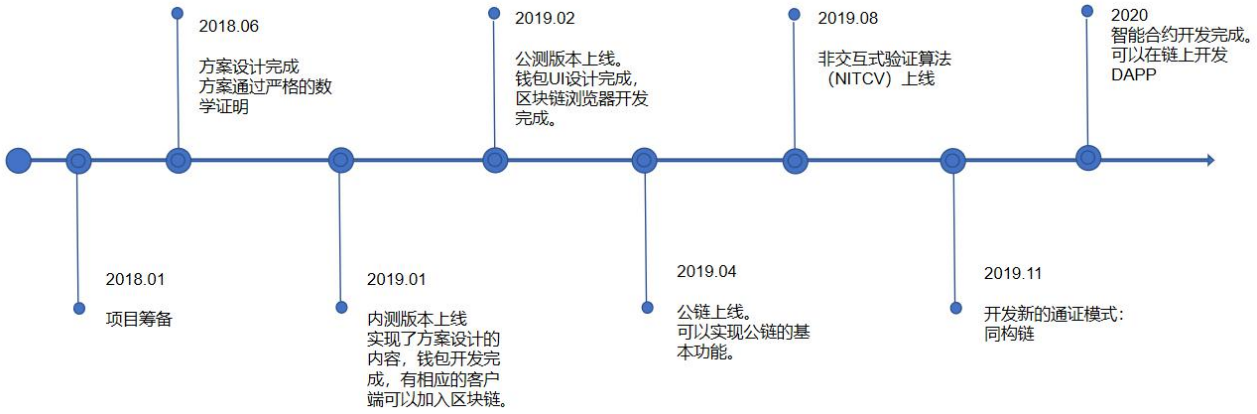
- **游戏：**基于 Ulam 的架构设计并发行游戏币。游戏开发者可以在该平台链上开发游戏，游戏运营方可以依托 Ulam 进行游戏运营。平台上的相关者包括：游戏开发及运营者、游戏玩家、 Ulam 游戏平台、投资者、下游直播平台和赛事运营方等。

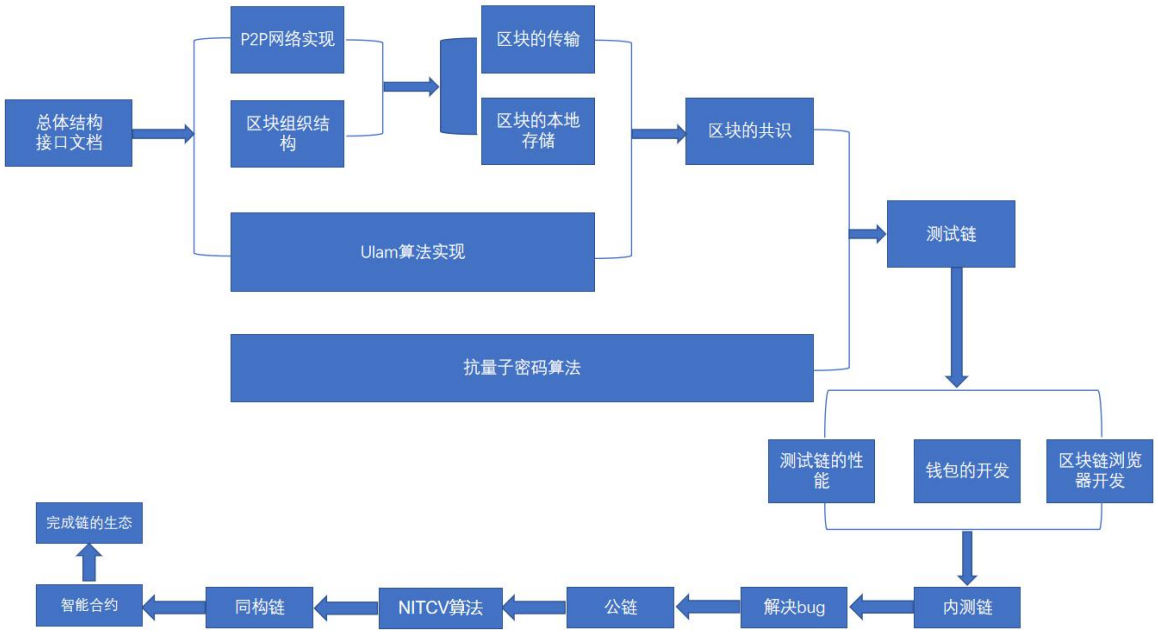
- **共享经济：**基于 Ulam 现有的架构设计属于个性化的共享经济平台。共享经济的特质之一就是去中介化。传统共享经济在发展的过程中已经从去中介化延伸为去小中介化。虽然交易过程中降低了中介耗费的成本，但是远没有达到共享经济的理想状态。而 Ulam 的高可用性和安全性可以为实现真正的共享经济提供基础设施。

团队介绍

吴彦冰：Ulam 发起人；清华大学高等研究院（数学）博士；师从王小云院士。曾破解韩国标准加密算法 LEA；提出了新的密码学破解方法。在区块链领域有两篇相关论文和两个相关专利；设计过既是匿名又便于监管的数字货币系统。做过相关的项目包括信贷工厂平台、基于智能合约的可搜索对称加密系统设计与实现、基于区块链的信贷工厂平台、以太坊侧链开发等。

ROADMAP



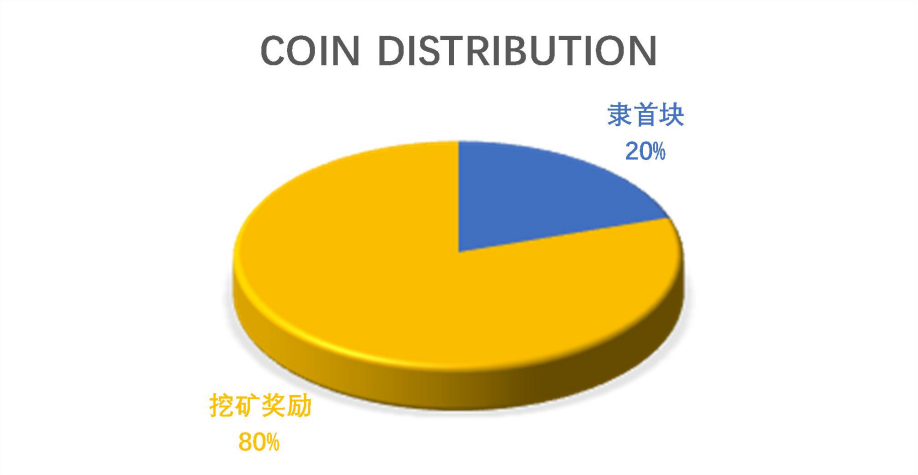


总体开发流程

燃料

ULAM 中的燃料用于同构链、智能合约、资源转移、数据上链中使用，燃料用于奖励 ULAM 上的拓荒者。

ULAM 燃料的总量为 1414213562，可拆分至小数点后 18 位。80%用于拓荒者进行开垦，8 年开垦完；20%属于初始燃料并写进隶首块中。1414213562 是 √2x1000,000,000 的近似值。√2 是人类发现的第一个无理数。



隶首是第一个发明数学和第一发明记账的人，区块链诞生的最初目的也是为了记账，为了记住和致敬这位伟大的数学家，Ulam 团队选用“隶首块”这个词来称呼 Ulam 区块链中的第一个区块。

大约公元前 5 世纪，当时的毕达哥拉斯学派重视自然及社会中不变因素的研究，把几何、算术、天文、音乐称为"四艺"，在其中追求宇宙的和谐规律性。他们认为：“万物皆数”；“人们所知道的一切事物都包含数；因此，没有数就既不可能表达，也不可能理解任何事物”。毕达哥拉斯学派所说的数仅指整数，而分数是被看作两个整数之比，他们相信宇宙万物总可以归结为简单的整数和整数之比。毕达哥拉斯学派的一项重大贡献是证明了毕达哥拉斯定理（在中国叫勾股定理）。毕达戈拉斯的一个学生西伯斯他勤奋好学，善于观察分析和思考。他研究了这样的问题：“边长为 1 的正方形，其对角线的长是 √2”。他根据毕达戈拉斯定理，发现 √2 不能用整数或整数之比（即现在所说的有理数）表示。也就是找不到一个数（指整数或整数之比，即有理数）使它平方后等于 2，即正方形的对角线和边的不可公度性（所谓线段的可公度性是指：对于两条给定的线段，能找到某第三条线段，以它为单位线段能将给定的两条线段划分成整数段）。这一悖论直接触犯了毕氏学派的根本信条，导致了当时认识上的"危机"，从而产生了人类历史上第一次数学危机。发现 √2 的西伯斯不但没有得到荣耀，反而因此被毕达哥拉斯的门徒重罚和追杀。最后西伯斯在逃跑的途中被毕达哥拉斯的门徒残忍地杀害。但是，正是这次危机将数学这门“上帝的语言”带向了另一个时代。西伯斯的名字也因此永远被历史铭记。

√2 是第一次数学危机的引发者。Ulam 选用这个数字作为发行量一则为了致敬人类历史上的第一次数学危机和变革的开始；二则也希望 Ulam 这一全新的共识可以像 √2 一样引发区块链领域的一次变革。

免责声明

本文档只在于传达信息之用，并不构成买卖 Ulam 股份或证券的相关意见。任何类似的提议或征价将在一个可信任的条款下并在可应用的证券法和其它相关法律允许下进行，以上信息或分析不构成投资决策或具体建议。本文档不构成任何关于证券形式的投资建议，投资意向或教唆投资。本文档不组成也不理解为提供任何买卖行为，或任何邀请买卖任何形式证券的行为，也不是任何形式上的合约或者承诺。

- 参与项目则代表参与者已达到年龄标准，具备完整的民事行为能力。投资者一旦参与投资即表示了解并接受该项目的风险，并愿意为此承担相应结果和后果。

- Ulam 团队将不断进行合理尝试，确保本白皮书中的信息真实准确。开发过程中，平台可能会进行更新，包括但不限于平台机制、Coin 及其机制、Coin 分配情况。本文档的部分内容可能随着项目的进展在新版白皮书中进行相应调整，团队将通过在网站上发布公告或新版白皮书等方式，将更新内容公布于众。请参与者务必及时获取最新版白皮书，并根据更新内容及时调整自己的决策。Ulam 明确表示，概不承担参与者因(i)依赖本文档内容、(ii)本文信息不准确之处，以及(iii)本文导致的任何行为而造成的损失。

- 团队将不遗余力实现文档中所提及的目标，然而基于不可抗力的存在，团队不能做出完全承诺。

- Ulam 的增值与否取决于市场规律以及应用落地后的需求，其可能不具备任何价值，团队不对其增值做出承诺，并对其因价值增减所造成的后果概不负责。

- Ulam 平台遵守任何有利于区块链行业健康发展的监管条例以及行业自律申明等。参与者参与即代表将完全接受并遵守此类检查。同时，参与者披露用以完成此类检查的所有信息必须完整准确 。

- ULAM 燃料仅为 ULAM 公链上的运行资源，不具有货币属性，不与货币进行兑换

- 其他

Ulam 明确表示不承担任何参与项目造成的直接或间接的损失，包括：

1.因为用户交易操作带来的经济损失；

2.由个人理解产生的任何错误、疏忽或者不不准确信息；

3.个人交易各类区块链资产带来的损失及由此导致的任何行为。

引用

[1] "Blockchains: The great chain of being sure about things". The Economist. 31 October 2015. Archived from the original on 3 July 2016. Retrieved 18 June 2016. The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the crypto currency.

[2] Fisher, Daniel (2015-05-25). "Visa Moves at the Speed of Money". Forbes. Retrieved 2016-05-01.

[3] Antonopoulos, Andreas (2017). Mastering Bitcoin: Programming the Open Blockchain (2 ed.). USA: O' Reilly media, inc. p. Glossary. ISBN 978-1491954386.

[4] "Bitcoin Energy Consumption Index - Digiconomist". Digiconomist. Retrieved 2018-06-08.

[5] Quantum Information Science and Technology Roadmap for a sense of where the research is heading.

[6] Thieme, Nick (4 August 2017). "Bitcoin Has Split Into Two Cryptocurrencies. What, Exactly, Does That Mean?". Slate. Retrieved 8 March 2018.

[7] "Understanding Denial-of-Service Attacks". US-CERT. 6 February 2013. Retrieved 26 May 2016.

[8] Robertson, Elizabeth D. (August 1, 2002). "RE: NTRU Public Key Algorithms IP Assurance Statement for 802.15.3" (PDF). IEEE. Retrieved February 4, 2013.

其他

官方网站：www.ulamchain.io

电子邮箱： contact@ulamchain.io