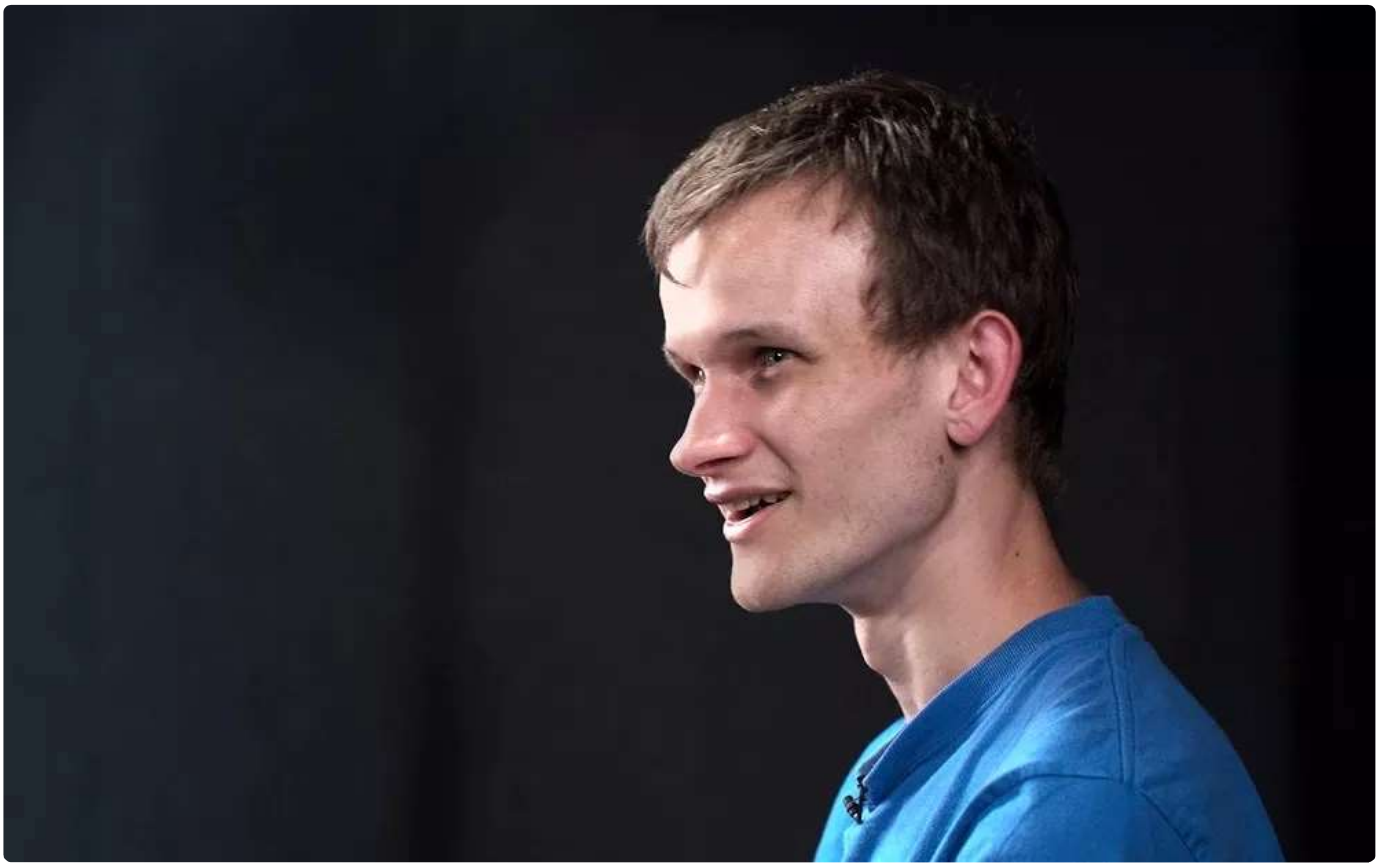
V神：区块链最关注的3大问题解决了吗？

From:Vitalik Buterin 区块链前哨 11/29



作者 | Vitalik Buterin

翻译 | 核子可乐

导语：区块链已经成为国家战略技术，各级政府和传统互联网企业纷纷布局区块链。区块链源自国外，几大加密社区一直在探索区块链新的可能性。

近日，以太坊创始人 Vitalik Buterin 发表文章介绍了加密货币在密码学、共识机制和经济三个方面经过 5 年发展后的状况、问题以及未来发展，同时也提出了当前加密领域存在的一些问题。InfoQ 本着开放、学习的精神将此文翻译出来，希望与各位同行、开发者共同学习、交流。

2014 年，我发表过一篇文章，也做过一场演讲，其中列举了目前数学、计算机科学以及经济学方面存在的几个棘手难题。在我看来，这些难题对于加密货币的发展成熟至关重要。五年过去，情况发生了很大变化，但是这些真正重要的问题究竟取得了多少进展？我们在哪里成功、在哪里失败，又在哪些方面发生了重要的观念转变？这些疑问正是本篇文章的核心，

我将回顾 2014 年提出的那 16 个问题，同时逐一介绍它们目前的进展状况。最后，我还整理出一份 2019 年版本的最新问题集合。

这些问题可以分为三大类：

（1）密码学。如果可解，则可通过纯数学方法解决；

（2）共识理论。对工作证明与权益证明做出的重大改进；

（3）经济。关于如何为区块链参与者提供激励要素的措施，主要集中在应用层而非协议层。这三个方向在过去五年中都取得了显著进步，当然具体进步速度仍然有快有慢。

密码学问题

1、区块链可扩展性

目前，加密货币领域面对的核心问题之一，正在于可扩展性。超大规模区块链难以建立信任：如果只有少数实体有能力运行完整节点，那么这些实体完全可以通过合谋为自己添加大量的额外比特币；其他用户由于连处理单一完整区块都做不到，因此也就无法验证某一区块是否真实有效。

问题： 建立一套类似于比特币的安全保障区块链设计方案，但其中用于保证网络正常运转的最大节点与最大交易数量之间必须具备充分次线性关系。

现状： 在理论层面已经取得重大进展，但仍有待更多实际评估。

可扩展性这一技术问题已经在理论层面上取得了重大进展。五年之前，几乎没有人考虑过分片方法。但现在，分片设计早已司空见惯。除了以太坊 2.0 之外，OmniLedger、LazyLedger、Zilliqa 以及持续发表的学术论文都在强调这种重要方法。我个人认为，虽然理论研究成果可观，但实际进展仍将渐进完成。总而言之，可以肯定的是我们已经拥有多种技术方法，可保证验证节点组安全地对单一验证者无法处理的大量数据达成共识。即使面对 51% 攻击的冲击，这类技术仍然允许客户以间接方式验证区块的全部有效性与可用性。

以下是这方面最具前景的技术成果：

- 随机采样，允许由一个小规模随机选取的委员会在统计学意义上代表完整的验证者集合：https://github.com/ethereum/wiki/wiki/Sharding-FAQ#how-can-we-solve-the-

single-shard-takeover-attack-in-an-uncoordinated-majority-model

- 欺诈证明，允许发现某项错误的个别节点集合将发现结果传播至所有节点: https://bitcoin.stackexchange.com/questions/49647/what-is-a-fraud-proof
- 监管证明，允许各验证节点以概率方式证明其已经分别下载并验证了一部分数据: https://ethresear.ch/t/1-bit-aggregation-friendly-custody-bonds/2236
- 数据可用性证明，允许客户端检测其标题所在的区块主体何时处于不可用状态: https://arxiv.org/abs/1809.09044。
- 更多相关细节信息，请参阅新的编码梅克尔树提案。https://arxiv.org/abs/1910.01247

当然，其他缓解性的措施同样所在多有，包括通过收据进行跨分片通信以及“常数”增强（例如 BLS 签名聚合）等方法。

但必须承认，目前还不存在实践层面的完全分片区块链（采用部分分片设计的 Zilliqa 最近刚刚开始运行）。从理论上讲，还存在不少与细节相关的争议，此外分片网络的稳定性、开发者经验以及降低集中化风险等问题仍没有得到很好的解决；不过好消息是，分片方法的技术可行性已经得到广泛认可。至于坏消息，目前仍有很多挑战无法单纯通过思考解决；希望目前各类正在开发的系统以及以太坊 2.0 等类似下一代区块链项目能够逐步攻克这些难题。

2. 时间戳

问题： 在创建分布式激励兼容系统时，无论该系统覆盖在区块链之上还是本身就以区块链形式存在，都能够提供较高的时间指标准确性。所有合法用户在某一“真实”时间范围内均具有正态分布的时钟示值，标准差为 20 秒……即两个节点间的相隔时间不得超过 20 秒。这套解决方案依赖于目前的“N 个节点”概念，且可通过权益证明或者非 sybil 令牌实现（参见第 9 个问题）。系统应持续提供时间，且该时间结果应与超过 99% 的可信参与节点内部时钟保持小于 120 秒（或者更低）的差值。因为外部系统可能最终依赖于这套系统，因此无论动机如何，该系统都应保障安全以防止攻击者控制超过 25% 比例的节点。

现状： 略有进展。

以太坊实际上是个典型的幸存者，其只设定有 13 秒的出块时间，而且没有任何先进可靠的时间戳技术；具体来讲，以太坊的技术方案非常简单，即禁止客户端接受任何时间戳早于客户端本地时间的区块。但这种方法并没有经受严格的攻击测试，因此究竟是否可靠还有待观察。最近出现的网络调整时间戳提案，尝试允许客户端在无法确切知晓本地当前时间的情况下，通过确定时间共识的方式改善安全性；但这种方法同样未经测试。总体来讲，时间戳机制并不是当前研究中的主要方向。也许在权益证明（PoS）链（包括以太坊 2.0 及其他同类链）实际上线之后，问题的重要性会得到更多人的重视，相信届时情况也将有所改善。

3. 任意计算证明

问题： 创建程序 POC_PROVE(P, I) -> (O, Q) 和 POC_VERIFY(P, O, Q) -> {0, 1}。其中 POC_PROVE 执行程序 P，I 是程序 P 的输入，POC_PROVE 返回程序 P 的执行结果 O 和计算证明 Q；POC_VERIFY 取 P，O，Q 值，验证 Q 和 O 是否属于由 POC_PROVE 使用 P 得到的合法运行结果。

现状： 取得重大的理论与实践进展。

关于这个问题，基本上就是要求我们构建一个 SNARK（或者 STARK，SHARK 之类……）。问题已经顺利解决，SNARK 现在正被越来越多的人所理解及接纳，并被纳入多个区块链项目当中（包括以太坊上的 tornado.cash）。SNARK 效果拔群，既可发挥隐私保护作用（例如 Zcash 与 tornado.cash），又可作为可扩展性技术（例如 ZK Rollup、STARKDEX 以及 STARKing erasure coded data roots）。

但现有方案在效率方面仍然有所局限；我们仍然很难设计出一种易于计算的哈希函数，此外随机内存访问证明同样不好实现。另外，还有一个尚未解决的问题，即验证时间中的 O(n * log(n)) 增长到底天然受限，抑或是存在某种仅使用线性资源开销即可实现的简洁证明（类似于 bulletprrofs 防弹证明，但这种证明需要耗费线性时长进行验证）。最后，现有方案中可能包含 bug，这也是种客观存在的风险。但总体来看，这个问题只余下一些细节，基础性的难关已经基本攻克。

5. 代码混淆

问题： 问题的核心，在于创建一个混淆函数 O。在给定任意程序 P 的情况下，该混淆函数能够生成第二个程序 O(P)=Q，其中 P 与 Q 在使用特定输入的前提下将返回相同结果，但最重要的是，Q 不会披露程序 P 之内的任何信息。人们可以在程序 Q 当中隐藏密码、加密私钥或者经过改造的算法本身。

现状： 进展缓慢。

这个问题的核心就是要求找到一种对程序进行加密的方法，使得经过加密的程序能够在使用相同输入的前提下，既不影响输出结果，又确保源程序内的信息得到妥善隐藏。代码混淆的典型示例正是包含私钥的程序，其仅允许该私钥对一部分特定消息进行签名。

代码混淆解决方案在区块链协议当中意义重大，而且对应不少有趣的应用场景，例如如何避免恶意人士将链上的某一混淆程序复制到另一区块链环境并继续运行等等。我个人比较关注的一类应用场景，在于利用混淆后的程序替换原本包含部分工作证明的 operator。如此一来，我们就能在防止操作冲突的小工具当中消除集中化部分，从而回避掉为了确定参与节点私人行为而带来的高昂重复验证成本。

遗憾的是，这个问题相当困难，而且暂时看不到解决的希望。首先，我们需要开发新的构造函数来降低那些我们实际上并不清楚的数学对象的假设数量（例如通用密码多线性映射）；其次，我们还得想办法实现这些必要的数学对象。就目前已知的方法来看，我们距离建立起可行的安全保障机制还有很长的路要走。请参阅 https://eprint.iacr.org/2019/463.pdf 以了解这个问题的更多细节信息。

6. 基于哈希的密码学

问题： 创建一种基于哈希值随机预言机属性（而非安全假设）的签名算法，要求这种算法既具有合理的大小，又能实现与经典计算机上 160 位加密相当的安全保障水平（对于 Grover 算法，相当于 80 量子比特）。

现状： 略有进展。

自 2014 年以来，这个问题迎来了两大进展。首先是 SPHINCS，这是一种“无状态”签名方案（即使多次使用，也不必记录随机数等信息）。实际上，在五年前的问题清单发布后不久，这套方案就已经出现，能够提供大小仅为 41 kB 左右的纯哈希签名方法。接下来登场的是 STARK，签名大小基本保持在同样的水平。五年之前，我绝对没想到哈希不仅可以用来签名，还可实现通用层面的零知识证明。这样的进展令我感到欣慰，也再次证明签名大小确实是个困扰区块链的重要问题，目前其他尝试也在努力帮助证明进一步瘦身。当然，相关进展比较缓慢。

基于哈希的加密技术目前存在一大挑战，即无法解决聚合签名（例如 BLS 聚合）问题。我们虽然可以对大量 Lamport 签名使用 STARK，但效率无法令人满意。希望接下来能够出现效率更高的解决方案。（有些朋友可能好奇，能不能使用基于哈希的公钥加密？答案是否定的，任何计算成本高于平方的方法都没有可行性。）

共识理论问题

1. 抗 ASIC 工作证明

关于这个问题，解决思路在于建立一种能够处理特殊问题的高难度算法。更多关于 ASIC 的讨论请参阅：
https://blog.ethereum.org/2014/06/19/mining/

现状: 正在努力解决。

当初难题清单发布大概六个月之后，以太坊决定采用其抗 ASIC 工作证明算法，即 Ethash。Ethash 亦被称为硬内存（memory-hard）算法。在理论层面，常规计算机中的随机访问存储器已经得到良好优化，因此很难针对特殊应用做出进一步改进。Ethash 将内存访问硬性指定为工作证明计算中的必要环节，从而实现抗 ASIC。Ethash 并不是第一种硬内存算法，但它仍然带来一项重要创新：在双层 DAG 上进行伪随机查找，进而带来两种函数评估方式。首先，如果某人拥有整个（约 2 GB）DAG，则可快速计算出结果，即满足硬内存要求的“快捷路径”。第二，如果某人只拥有 DAG 中的顶层，则计算速度将相当缓慢（但仍可以快速验证结果），这种方式专门用于区块验证。

事实证明，Ethash 在抗 ASIC 方面非常成功。经过三年以及数十亿美元的采矿奖励之后，ASIC 如今虽依旧存在，但其采矿能力与成本效益至多只能达到 GPU 的 2 到 5 倍。另外，虽然已经出现了 ProgPoW 这一替代性方案，但人们开始普遍认为，抗 ASIC 算法恐怕必然具有有限的生命周期，而且抗 ASIC 本身也令 51% 攻击 的实施难度有所下降（详见 Ethereum Classic 遭受的 51% 攻击）。

我认为接下来一定会出现能够在一定程度上（中等水平）对抗 ASIC 的工作证明算法，但这种抗性较为有限，而且 ASIC 与非 ASIC 工作证明各有缺点。从长远角度来看，权益证明才是更理想的区块链共识选项。

2. 实用性工作证明

让工作证明在证明之外发挥其他作用；常见的备选方案包括 Folding@home，这是一种现成程序，用户可以将该软件下载到自有计算机上模拟蛋白质折叠结构，从而为研究人员提供治愈各类疾病所需要的大量支持性数据。

现状： 也许无法解决，但应该存在一种例外。

实用工作证明面临的主要挑战，在于工作证明算法存在以下固有属性：

- 难以计算
- 易于验证
- 不依赖于大量外部数据
- 可通过较小“分块”实现高效计算

遗憾的是，目前符合这些属性的计算任务还比较有限，而且大部分符合属性的计算任务“实用周期”太短，不足以在周期之内构建加密货币。

但还有另一种可行的例外，即零知识证明。区块链中的零知识证明（例如某一简单示例中数据的可用性）难以计算，但却易于验证。由于计算难度很高，因此如果“高结构化”计算的证明变得太容易，我们可以直接切换为验证整个区块链的状态变化——后面这种任务要求对虚拟机以及随机内存访问进行建模，因此计算成本会立刻飙升。

区块链零知识证明的存在，为用户带来了巨大的价值。如此一来，用户将不再需要直接承担链验证成本；Coda 目前就在进行这方面尝试，尽管其区块链设计非常简单，但确实针对可证明性进行了优化。这种证明能够极大提高区块链的安全性与可扩展性。换句话说，由于实际需要证明的只是区块链权益证明中的附加内容，而非完整的共识算法，所以新方案的实际计算量要远远低于现有工作证明计算量。

3. 权益证明

解决采矿集中化的另一种方法，则是彻底取消采矿活动，转而利用其他机制计算共识体系中各个节点的权重。截至目前，最流行的替代性选项当数“权益证明”——也就是将工作证明中的一 CPU 一票，转化为一代币一票。

现状： 理论获得重大进展，但仍需更多实践评估。

2014 年年底，权益证明社区发布声明，指出“弱主观性”已经成为一种必然。具体来讲，为了维护区块链经济安全，各节点在首次同步时需要额外获取近期检查点协议，并在离线数月后重新上线时，再获取一次。这是一种巨大的风险，因为在工作证明的支持者们看来，工作证明链存在明确的“头”，其由区块链客户端软件本身充当并作为数据的唯一可信来源。但是，权益证明支持者们愿意承担这种风险，因为对可信度的需求并不强烈，权益证明完全可以通过长期保证金的形式实现基本一致的效果。

目前，最有趣的共识算法在本质上类似于 PBFT（即实用拜占庭容错算法），只是利用一份动态列表替换掉固定的验证器集，意味着任何人都可以向具有锁定时间的系统智能合约内发送代币以加入这份动态列表（在某些情况下，用户可能需要等待 4 个月时间才能提取这些作

为保证金的代币）。在多数情况下（例如以太坊 2.0），这些算法会跟踪用户违反协议的行为，并通过相应罚没实现“经济最终性”。

截至目前，我们已经拥有以下几种算法（仅举几例）：

- Casper FFG:
  https://arxiv.org/abs/1710.09437
- Tendermint:
  https://tendermint.com/docs/spec/consensus/consensus.html
- HotStuff:
  https://arxiv.org/abs/1803.05069
- Casper CBC:
  https://vitalik.ca/general/2018/12/05/cbc_casper.html

以太坊 2.0 在初始阶段将采用 FFG，且目前已经取得了一定进展；Tendermint 也已经在 Cosmos 链当中运行了几个月。关于权益证明，当下仍然存在着围绕激励措施优化以及 51% 攻击应对方法等议题展开的争议。另外，Casper CBC 规范确实带来了相当具体的效率改进成果。

4. 存储证明

解决共识问题的第三种方法，在于使用算力与代币之外的其他稀缺性计算资源。目前，这方面的替代性方案主要有存储与带宽两种选项。在原则上，我们无法为带宽的提供或者使用给出事后密码学证明，因此带宽证明只能算是社会证明中的一个子集，我们将在后续问题中进一步讨论。与之对应，存储证明则可通过计算方式实现，其主要优势在于可完全抵御 ASIC 攻击。目前，磁盘驱动器这类存储资源似乎是最好的选择。

现状： 已经取得一定理论进展，但仍有很长的路要走，同时需要大量实践层面的评估。

目前已经出现了不少采用存储证明协议的区块链，包括 Chia 与 Filecoin。但这类算法仍然没有经过大规模的实践测试。我个人比较关注其中的集中化问题：这类算法到底是由众多提供存储容量的散户主导，还是由少数大型矿场主导？

经济问题

1. 稳定币

比特币面临的主要问题之一，在于其与法定货币之间的兑换价格波动过大……问题是：如何构建一种以稳定汇率兑换法定货币的加密资产。

现状： 略有进展。

MakerDAO 目前已经正式上线，且稳定运行了近两年时间。作为其潜在抵押资产的以太币价值已经下跌了 93%，但 MakerDAO 仍然不受影响，且目前发行的 DAI 稳定币总值已经超过 1 亿美元。目前，MakerDAO 已然成为以太坊生态系统中的一大支柱，不少其他以太坊项目已经或者正在与之集成。此外，UMA 等其他合成代币项目也表现出迅猛的发展速度。

但是，虽然 MakerDAO 系统在形势严峻的 2019 年当中幸免于难，但未来其仍可能面临更多挑战。此前不久，比特币价格在两天之内下跌了 75%；同样的情况有一天也可能会发生在以太币或者任何其他抵押资产之上。与此同时，针对区块链底层的恶意攻击也有可能全面肆虐，对这种情况的预期进一步导致加密货币价格下跌，最终形成恶性循环。另外一个重大挑战，在于 MakerDAO 这类系统的稳定性由非公开预言机决定。目前，确实存在不少新的预言机探索尝试（详见第 16 个问题），但人们尚不清楚这些新方案能否顶得住巨大的经济压力。就目前来看，由 MakerDAO 控制的抵押品在价值上仍低于 MKR 代币；如果这种关系发生逆转，那么 MKR 持有者有可能以集体方式“洗劫”MakerDAO 系统。虽然理论上存在不少能够防止此类攻击的方法，但全都缺少现实层面的测试。

2. 公共项目的去中心化问题

“公共项目”是经济体系中的常见挑战之一。例如，假设某个科研项目需要耗资 100 万美元方可完成，且已知如果研究顺利结束，那么产生的成果可帮助 100 万民众各节约 5 美元。总体来讲，这一公共项目虽然拥有明确的收益，但从任何个人角度来看，为其做出贡献都不符合利益诉求……目前，大部分公共项目都包含附加的假设与要求：存在一种完全可信的预言机，用于判断某一公共项目是否已经完成预期任务。（这实际上是一种错误的假设，但与本次主题无关，因此不做具体讨论。）

现状： 略有进展。

关于公共项目的资金筹集问题，主要可分为两大类：首先是资金问题（公共项目从何处获得资金）；其次是倾向聚合问题（如何确定哪些属于真正的公共项目，哪些实际上属于归个人所有的私有项目）。这里我们假设已经解决了后一个问题，因此集中精力探讨前一个问题。

总体而言，目前这一领域并没有出现新的重大突破。解决方案分为两类，其一在于尝试提取出个人贡献，并据此为人们提供社会性奖励。当前不少慈善活动就遵循这一思路，也有 Peepeth 抗疟疾捐赠徽章等通过心理满足感与成就感解决问题的方案。其二是从具有网络效应的应用当中收集资金。在区块链领域中，解决问题的方法主要有以下几种：

- 发行代币
- 在协议级别收取交易费用（例如通过 EIP 1559 收费）
- 从某些二层（Layer-2）应用程序当中收取部分交易费（例如 Uniswap，某些规模化解决方案，包括在以太坊 2.0 的执行环境中收取租赁费用等）
- 收取其他费用（例如 ENS 注册费）

在区块领域之外，这个问题早已是老生常谈，解决方案包括：政府税收；企业或其他组织性收费等。

3. 信誉系统

问题： 设计一套形式化的信誉系统，包括一项信誉评分 rep(A,B)->V，其中 V 表示从 A 的角度出发衡量出的 B 信誉情况；一种用于确定一方在多大程度上信任另一方的概率机制；以及根据某种进行中或者已经结束的交互记录，对信誉评分进行更新的机制。*

现状： 进展缓慢。

自 2014 年以来，信誉系统的进展非常有限。其中最值得一提的成果，也就是利用代币注册表建立一套可信实体 / 对象管理列表；Kleros ERC20 TCR（一份合法的 ERC20 代币管理注册表）就是其中一例；再就是 Uniswap（http://uniswap.ninja）替代接口，以此为后端获取代币、单号以及徽标列表。目前还没有出现任何真正具有主观多样性的信誉系统，这可能是因为目前广泛存在于区块链之上的人群“社会关系图”还没有积累到足够的信息。如果未来一段时间内在某些理由的驱动下，此类主观评判信息开始出现，那么此类信誉系统仍有可能迎来快速发展。

4. 卓越证明

这是个有趣而且尚未得到广泛关注的问题，即解决代币的实际分配难题（不可能每位采矿参与者都能轻松获得代币）。这种分配原则应当有益于社会，同时在设计层面强调参与者的创造性尝试与天赋。例如，我们可以提出一种“证明证明（proof of proof）”货币，用以奖励那些证明了某些高难度数学定理的参与者。

现状： 没有进展，也没有人关注。

目前最流行的代币分配方式仍然是——空投。一般来讲，代币会在项目启动之初根据各参与者的此前持币时进行分配，要么遵循其他一些指标（例如握手空投）。但是，目前还没有出现任何针对参与者创造力的验证方法；当然，考虑到目前 AI 技术的进展，设计出这样一种只有人类能够做到、而计算机只能加以验证的任务，可能确实太难了。

5. 去中心化贡献度

遗憾的是，除了刺激公共项目的推进之外，中心化方法还能解决另一个独特的难题：明确哪些公共项目具有价值，而后确定应付出工作量实现这些公共项目。此项挑战关注的又是后一个问题。

现状： 略有进展，但侧重点亦有所改变。

近年来，在确定公共项目价值贡献方面，最新进展仍然无法将之前提到的确定任务与确定完成度这两点区分开来。之所以如此，是因为二者在实践层面上确实盘根错节、难以剥离。某些团队负责的工作往往存在不可替代性且相当主观，因此最合理的方法是将任务重要性与项目完成度视为统一的整体，并使用相同的技术对二者加以评估。

幸运的是，这方面确实获得了不小的进展，特别是二次融资机制的出现。二次融资允许个人向项目捐款，且利用公式将捐赠人数、捐款数额纳入计算，从而实现项目融资的完美协调。（这里的「完美」，是指既保障每一位捐赠者的利益，亦不会令项目成为少数人的专属、大多数人的悲剧。）在进行项目捐赠时，应捐数额与实捐数额之间的差额，将由某个集中资金池以补贴形式提供给项目方（关于集中资金池来源，请参阅第 11 个问题）。需要注意的是，这种机制强调满足某些社群的价值主张，而非满足某些特定目标（无论是否符合部分群体的主张）。由于价值问题往往相当复杂，因此这种方法在处理其中的未知因素时往往更为稳定有效。

在实践当中，二次融资机制已经在最近的 gitcoin 二次融资活动中获得了巨大成功。此外，二次融资以及其他类似机制也保持着良好的发展势头，例如限制成对有界二次融资中的串通活动等。此外，人们还在票选反贿赂技术的规范化与实施方面做出大量努力，旨在禁止用户向第三方证明自己的投票内容，从而预防共谋与串通攻击。

6. 抗女巫攻击系统

这个问题与信誉系统也有一定关联，同时也是建立“唯一身份系统”时面临的主要挑战。抗女巫攻击系统是一种能够生成通证，并利用该通证证明其身份不属于女巫攻击组成部分的系统。在这方面，我们当然希望实现方式比「一块钱一票」更科学一些……比如一人一票。*

现状: 略有进展。

目前已经有不少尝试解决人类特有问题的方案，我能够想到的包括（但不限于）：

- HumanityDAO: https://www.humanitydao.org/
- Pseudonym parties: https://bford.info/pub/net/sybil.pdf
- POAP ("proof of attendance protocol"): https://www.poap.xyz/
- BrightID: https://www.brightid.org/

随着人们对于二次投票以及二次融资等技术的愈发关注，反女巫攻击系统的市场需求也日趋旺盛。希望当下以及未来的技术进展能够切实满足这些需求。

7. 去中心化成功指标

问题： 提出并实施一种分布式方法，用以衡量现实场景下的数值变量……该系统应当能够衡量人类目前可达成大致共识的任何数值属性（例如资产价格、温度、全球二氧化碳深度等）。

现状： 略有进展。

这一点目前被统称为“预言机问题”。分布式预言机的最大规模已知实例为 Augur，其已经处理涉及数百万美元的下注结果。Kleros TCR 等代币管理注册中心也属于这个范畴。但是，此类系统仍未针对分叉机制进行实际测试，例如衡量某个极具争议的问题或者衡量是否发生了 51% 攻击。另外，区块链之外也有人在进行预言机问题研究，即“同行预测”。

另一大迫在眉睫的挑战在于，人们希望依靠这类预言机系统指导资产转移，而相关资产的总数额要远远大于系统内的原生代币。在这种情况下，代币持有者在理论上确有动机合谋提供错误答案以窃取这部分资产。一旦发生这类状况，系统必然分叉，而原始系统中的代币很可能变得毫无价值。但是，原始系统中的代币持有者仍可通过窃取到的资产获得回报。稳定币（参见第 10 个问题）在这方面就存在着巨大的风险。解决这类问题的方法之一，是建立起一套与之对应的系统，假设确实存在始终抱有利他心态的数据提供者并据此建立识别机制；

此外，放慢系统的运行速度，确保恶意数据提供者在操纵预言机系统投票时，依赖该预言机的用户仍有时间有序退出。无论如何，预言机技术的下一步发展方向必将成为区块链领域的重要议题。

更多新问题

已经 2019 年了，如果要重新整理出这么一份难题清单，那么除了上面这 16 条或保持原样、或侧重点有所变化的老问题之外，我还要加入几条新问题。例如：

- 加密混淆: 参见第 4 个问题。
- 后量子时代下的加密工作: 同时基于哈希与抗量子算法的“结构化”数学对象，包括椭圆曲线等值线、格密码等……
- 反共谋基础设施: 正在逐步开展与完善，包括增加针对节点运营方的隐私保护，以尽可能实用的方式增加多方计算等。
  https://ethresear.ch/t/minimal-anti-collusion-infrastructure/5413
- 预言机: 与第 16 个问题相同，但不再强调“成功指标”，而更多侧重于一般性的“实际数据获取”问题。
- 人类特有验证（或者从更现实的角度讲，人类半特有验证）：与第 15 个问题相同，但强调“绝对”解决方案：通过两轮验证的难度要比通过一轮高得多，而且即使全部通过，也无法同时获得多个验证身份（且具有潜在危害）。
- 同态加密与多方计算: 实用性仍有待持续改进。
- 去中心化治理机制: DAO 很酷，但目前的 DAO 仍然比较原始，我们还能做得更好。
- 对 51% 工作证明攻击的完备响应能力: 目前正在改进与完善。
  https://ethresear.ch/t/responding-to-51-attacks-in-casper-ffg/6363
- 更多公共项目资金来源: 理想的做法是对具有网络效应的系统内拥塞资源收费（例如交易费用），但在去中心化系统中，这类举措需要具备公共合法性；因此，这是一种社会问题，有望通过技术方式得到解决。
- 信誉系统: 与第 12 个问题相同。

总的来看，基础层面的问题解决起来比较缓慢，但仍在逐步推进；与之相对，应用层的问题才刚刚起步。

原文链接：

https://vitalik.ca/general/2019/11/22/progress.html

今日荐文