Meet Autonomous System Research

2019 年 7 月 4 日

目录

1 概要

目前，区块链行业仍处于快速发展中，并在发展中不断凝结新的共识。从共识机制、密码学、智能合约等底层技术，到上层的区块链应用（如溯源、存证、游戏等），新的技术层出不穷；与此同时，新的治理理念、新的商业模式、新的通证设计也不断涌现，这些技术创新与模式创新不断进行交叉、融合，推动着区块链行业的发展。我们认为，区块链行业的发展在一定程度上来自于社区的共识，这种共识往往是社区对某个技术、理念或模式的认可。例如，社区对 PoW 的共识使得整个行业出现了“矿场”；社区对 ICO 这一模式的认可一定程度上带来了以太坊的繁荣；社区对零知识证明相关技术的认可则带来了 ZCash、门罗币的快速发展。

我们相信区块链行业是由创新驱动的。在区块链的快速发展中，创新往往能够以最快的速度创造出最大规模的共识，更进一步的，通过创新形成的共识往往会结合资本的力量，推动整个区块链行业的发展。诚然，在传统行业，创新的作用也十分重要，但是在这些行业中，创新必须通过产品、用户体验传递给客户。也就是说，在传统行业中，从创新到产生能够维持企业发展的收益之间存在着漫长的转化过程，这一过程的漫长也使得在诸多中小企业在创新方面显得谨小慎微。而在现阶段区块链的发展中，仅仅是通过创新凝聚的社区共识，就足够为区块链团队创造足够的收益，从而使得团队在将创新性的想法转化为实际的产品方面显得从容不迫。可以认为，从未有过一个行业能够如此快速的将创新转化为企业的收益。

Autonomous System Research（ASResearch）致力于通过坚实的学术研究进行创新，并通过创新推动整个区块链行业的发展。区块链做为一个新兴行业，涉及到包括分布式系统、编程语言、虚拟机、密码学、经济学等多个不同学科中的多个不同专业。尽管理论上有着不完备性，但密码学，博弈论相关知识的引入却使得区块链系统中的共识经历了十年以上的考验。这种跨学科、跨专业的交叉性使得区块链行业的创新十分困难，相对的，将未经严格证实的创新投入实践，不仅有可能对项目方造成损失，更有可能伤害到广大社区成员的利益。因此，我们认为，通过坚实的学术研究进行创新，是区块链行业发展的重要路径。

ASResearch 由多位从事区块链研究的硕士、博士组成，拥有扎实的学术研究能力，研究工作涉及多个区块链相关的领域，并且长期从事区块链相关的研究，积累了大量区块链研究方面的经验。同时，ASResearch 积极与高校、科研院所开展合作，积极探索区块链相关的基础理论，深入理解区块链系统的各个方面。我们相信，对区块链的深入理解，是进行持续创新的基础，而持续创新正是 ASResearch 的立身之本，也是 ASResearch 对于整个区块链行业的意义所在。

2 过去的工作

2.1 区块链底层技术

2.1.1 Blockchain Runtime Environment

Blockchain Runtime Environment（BRE）的提出是为了解决区块链系统中的升级问题。目前，大部分区块链项目在系统升级过程中需要面临软分叉或硬分叉，而硬分叉则需要整个区块链系统停机维护，这不但造成了区块链项目的损失，更阻碍了区块链在实际生产环境中的大规模使用。例如，很难想象，在金融系统或工业系统中部署区块链后，这些系统需要在区块链升级时暂时停摆。

BRE 的思路是将区块链系统的协议代码以一定的数据格式放在区块链上，客户端通过不断获取链上最新的区块链协议代码，更新本地的区块链协议代码，并执行新的代码，从而实现区块链系统的自动升级。更具体来说，BRE 使用了 LLVM JIT，执行链上的 C++ 代码。BRE 在完成自动升级的基础上，更进一步的解决了不同版本的链上代码的并发执行问题，在保证正确性的前提下，进一步提高了执行性能。

同时 BRE 的设计有效地分散了区块链系统中 “节点” 或者 “矿工” 的权利。在诸如比特币的 PoW 共识的网络中，矿工不仅被赋予了出块的 “行政” 权利，还往往控制了系统的升级方向。在社区形成某种技术迭代的共识时，往往因为矿工的意愿或者效率的影响，导致这种共识无法得到有效的执行，在区块链系统的治理上形成了明显的权利不均衡，抑制了生态的长期有效发展。BRE 的设计为社区在达成有效共识的前提下，实现系统的迅速升级提供了有效的工具，也在系统层面有效地平衡了持币用户、开发者和矿工在生态中的话语权重。

BRE 在为区块链提供升级能力之外，更提供了通过区块链系统进行软件分发、软件更新的能力，即开发者可以开发相应的软件，与区块链有关或无关，并通过 BRE 进行分发、更新。这为区块链系统的使用场景提供了广阔的想象空间。

2.1.2 账户指数

账户指数（Account Rank, AR）的提出旨在衡量区块链地址（用户、账户）的重要度。就目前而言，大部分区块链项目仅简单的将用户的当前质押代币，或套用著名的 Page Rank 算法作为价值衡量指标。这样简单的设定存在一定的缺陷：它们或无法有效地抵抗女巫攻击，或损害了代币的流通性。

我们经过多方研究和探讨，通过全方面综合考虑各项因素，最终设计出最适合衡

量链上用户重要度的标准，账户指数[1]，其设计核心包含如下几个方面：

1. 资产中值：我们把用户一段时间内资产的中位数作为账户指数的核心变量之一：当财产中值为 x 意味着用户持有 x 个代币至少一半以上的时间，防止同样一笔资产被多个账户所利用。

2. 出入度指标：我们把用户一段时间内转账图先进行去环操作，随后分别记录转入和转出资产数量，再通过特定函数用以计算出入度指标。该指标能衡量用户的活跃度且具备反作弊功能：能证明去环操作保证了用户通过频繁转账能提升的出入度指标存在上限。

3. Wilbur 函数：Wilbur 函数 f 是账户指数的独创函数之一，满足 (a) $f(x+y) > f(x)+f(y)$，严格地抵抗了女巫攻击，(b) $\lim_{x,y\to\infty} f(x+y) = f(x)+f(y)$，防止大户的绝对统治。上述指标在进行账户指数最终计算时均使用了 Wilbur 函数。

账户指数为发现区块链世界真正价值提供了有力保证，是发展各项链上活动的根基。现已衍生出 DIP（详见??）等应用。可以预见，随着用户对链上价值需求的逐步扩大，账户指数必有更加广泛的应用场景。

2.1.3 开发者激励协议

开发者激励协议（Developer Incentive Protocol，DIP），旨在为区块链上优秀的去中心化应用（Decentralized Application, DApp）的开发者提供持续的激励（奖励）。

我们认为，目前无论是去中心化应用平台还是传统的中心化应用平台，开发者的利益没有被公平的分配：开发者获取利益的主要方式为用户购买和植入广告。相当一部分高质量免费且不含广告的应用常能带来较高的用户体验，但此部分 DApp 开发者的利益无法得到保证；另一方面，通过高质量应用来吸引用户加入为平台的主要获利方式之一，但平台获得的这一部分利益并没有直接地分配给开发者。基于以上考量，我们认为平台需要给开发者提供一定的激励以持续开发高质量的应用。

鉴于在区块链生态系统中，新的区块奖励代表了区块链系统发展中新增的价值，而出块奖励的分发决定着去中心化系统的激励方向，DIP 的主要功能为将部分出块奖励公正、公平地分配给 DApp 开发者，促进用户、区块链平台、开发者三者共生共荣的发展。

DIP 的设计主要分为两部分：给 DApp 进行排名以及给开发者发放奖励。在一定周期内，我们通过用户调用 DApp 次数的情况以及用户的账户指数对每个 DApp 给出一个排名分；最后，通过排名分计算出每个 DApp 开发者应得的奖励。

[1]https://github.com/ASResearch/nr-report

DIP 设计的优越性在于：

1. 用户账户指数的引入天然地防止了女巫攻击，即新建大量账户来调用某 DApp 的作弊行为无法提升收益；
2. 排名分的计算我们采用所谓二阶投票模型，即用户调用不同的 DApp 能带来更多的实际排名分贡献，从本质上增大了收买用户的成本；
3. 最终奖励的计算能保证开发者复制、分裂自己的 DApp 不会获得更多的奖励。

DIP 是账户指数的首个成功应用，给大量开发者提供了持续性的奖励。具体介绍可以参见开发者激励协议紫皮书[2]。

2.1.4 共识算法

共识算法是保证区块链系统稳定、安全运行的核心。我们致力于在对现今先进的、广泛使用的共识算法进行深度理解和调研的基础上，设计并实现出具有独创性及优越性的共识算法。

共识算法的设计是一个巨大的工程，目前的工作包含以下几个方面：

共识算法调研 [3]

共识一直是分布式系统中的重要概念，而区块链的诞生更是对共识算法产生了更强烈的需求。迄今为止对比特币白皮书的引用已经超过了 5000 篇，其中大部分是共识层面的思考。这还不包括在比特币诞生之前曾获图灵奖的 Lamport 提出的拜占庭容错问题（BFT）。

我们对一系列著名的对设计新共识有帮助的专业论文进行了调研，分为如下几类：1. 对传统工作量证明的思考（PoW）；2. 对拜占庭容错问题的研究；3. 对基于随机数的权益证明 (PoS) 的研究；4. 对于非链数据结构的讨论。这一广泛的、对共识算法的调研，对设计新共识提供了重要的参考和指导意义。

共识机制设计指导 [4]

该设计指导在共识调研的基础上，进一步分析了设计新共识时需要达成的目标以及期间需要注意的问题。

该设计指导独立提出将区块提议以及一致达成两个过程分离开，分别建立系统模型，各自独立实现机制。并分别对 PoW 协议、PoS 协议、链式协议和投票协议进行了优劣性分析。

[2]https://github.com/ASResearch/dip-report
[3]https://github.com/ASResearch/consensus-survey
[4]https://github.com/ASResearch/pod_guideline

该设计指导是设计新共识算法的必备工作，在理论层面上进一步提供了指导。

TLA+ 形式化验证 [5]

所谓形式化验证是指用 TLA+ 语言实现对共识算法的形式化描述（specification）。在工程领域非常重要，尤其是分布式系统，在开发系统之前做相应的抽象描述能够帮助开发者更好的理解系统，并且能够有效发现潜在的问题，这些问题可能在测试中都难以发现。

形式化验证相当于为建造共识算法的大厦画好了图纸。目前在开源区块链项目中，只有少数共识算法有专门的形式化描述，例如以太坊[6]。我们认为，TLA+ 形式化验证为共识算法提供了真正意义上的安全性保证。

就目前的结果而言，我们的共识算法：1. 支持无准入门槛下（Permissionless）出块环境；2. 在一致性达成方面，具有很强的独创性，且能最大限度的保证系统的安全性，抵抗各种潜在的攻击；3. 能保证持续、稳定的高 TPS 及低确认时间。

2.2 通证经济设计

我们认为区块链经济体的发展离不开持币用户在整个区块链系统和生态中的参与度。某种程度上，在目前大部分的区块链系统中，持币用户和整个生态之间缺乏交互的规则和工具，所以我们从在治理的链上投票场景开始切入，提升持币用户和系统及生态的交互。

1. 设计初衷：在 onchain 的投票中，需要在投票场景中平衡票权合理分配、抗作弊、高用户参与度、票权交易流转的 “白盒” 博弈等诉求，因此我们设计了基于抗女巫攻击，带币龄和交易活跃度权重的算法，对链上投票有激励的发行协议的投票代币。

2. 发行方式

   (a) 发行机制和比特币类似，以 “周” 为发行单位，减半周期约为 4 年

   (b) 可通过链上转账提高地址账户指数（AR）、参与链上投票、质押等行为 “挖矿” 获得

3. 投票流程：设计了投票的基本三原则和两次投票规则及投票的监督框架，提高系统内投票作恶的成本和“共谋”的难度

[5] https://github.com/ASResearch/consensus_spec
[6] https://github.com/ethereum/eth2.0-specs

4. 参数的升级迭代：自身的参数可以进行动态调整。参数的调整和升级遵循治理过程中的“自举”及“全息”原则，即在设定初始参数占位符的基础上，为持币用户提供完整的参数升级流程和工具，由社区基于市场反馈和生态发展情况，投票决定不同时期内参数的设定。

5. 该设计的主要优点体现在：

   (a) 在生态中构建了合理的双代币经济体系，其中本币作为“良币”，刺激用户储存和保值增值。投票代币有明确的使用和流通场景及销毁规则，作为“劣币”，刺激代币的流通和使用，增加用户的参与度和生态活跃度的同时将增量价值沉淀在本币上

   (b) 用户用于投票的代币在一定限度内会以大于 1 的比例返回给用户，用以激励用户积极参与投票，同时防止了滚雪球效应。

2.3 社区治理

我们认为区块链项目，尤其是公链项目，是基于自身代币及代币的经济体展开的去中心化的开源协作组织，如何设计去中心化协作组织的治理结构和协作中复杂协作关系的博弈规则是每个公链项目需要面临的重要课题。

我们设计了社区治理结构及链上治理工具，拟解决中心化治理无法应对去中心化生态发展的需求、传统的去中心化协作中的公地悲剧及现有去中心化区块链生态中无法有效迭代升级、激励不足社区参与度低等问题。在该治理体系的设计中，我们设定了以链上公共资产为主要治理对象，以链上治理为主要手段，配合链下组织结构和监督机制的完整的治理结构。

该治理体系的设计主要包括几个方面：

1. 系统治理中的基本权利主张，即以链上“地址”为基本单位。针对地址提出三点基本主张：(a) 拥有和操作链上资产的权利；(b) 发起提案的权利；(c) 参与投票的权利；

2. 链下的组织结构和监督机制，设计了独立运行且互相制约的三会：理事会、基金会和技术委员会，分别负责拓展生态中的规模优势、效率优势和生产力组织和指导；

3. 链上协作和升级方式：设计了结合技术特点发行的治理投票代币及相对应的社区协作平台、提案流程和投票规则，及相应规则和参数的升级流程。

该治理体系的优越主要体现在:

1. 系统协作规则全息，系统中所有角色在统一的规则之下存续和发展。与此同时，迭代规则的规则也被统一的规则定义，为多重生态角色的存续和发展提供了稳定的系统基础，有效促进生态内的多重良性博弈；

2. 协作过程基于链上工具，在去中心化的组织中实现。同时辅助以链下社区组织和监督机制，丰富链上协作的维度，提高去中心化协作的效率；

3. 正向激励的协作规则，社区中的用户可以通过提高经济体贡献度、积极参与链上治理等方式，获得链上去中心化发放的原生激励，让社区成员更公平地获益，大幅提高社区参与度。

3 未来工作

ASResearch 未来的工作以研究为主，并且存在着一个主线。整体而言，得益于5G、人工智能、芯片等行业的进步，ASResearch 相信，区块链系统会在终端设备上得以大规模的部署和使用。因此，ASResearch 将会在这个方向上持续探索区块链可能的发展，包括但不限于，快速的交易确认的共识算法、高效的区块链交易存储系统、安全的智能合约等，同样的，ASResearch 也将探索更合理的通证经济设计，以及去中心化治理的理论与实践。

ASResearch 愿意向整个行业分享我们的理解，也愿意和整个行业积极合作，在实践中探索新的技术、新的模式，共同推进区块链行业的发展。