

基于 DPoS 共识机制的区块链社区演化的可视分析方法



温啸林 李长林 张馨艺 刘尚松 朱 敏

四川大学计算机学院 成都 610065

(wenxiaolin@stu.edu.scu.cn)

摘 要 DPoS(股权授权证明)是当前主流区块链共识机制之一,独特的节点竞选机制使其形成不断演化的区块链社区。对区块链社区演化模式进行分析可以发现共识机制的潜在风险,具有十分重要的研究意义。针对 DPoS 共识机制区块链数据,提出了一种新颖的共识机制效能组合分析策略,面向区块链社区演化模式,提出了一种多角度探索的可视分析方法。首先,量化了节点排名变化前后工作完成度与投票排名的差异,对共识机制的选择效能和激励效能进行组合分析;然后,针对共识机制组合效能、节点地域分布演化和节点间差异比较等方面设计可视化视图与交互手段;最后,基于 EOS 主链真实数据设计实现基于 DPoS 共识机制的区块链社区演化可视分析系统,并通过案例研究和专家评估验证所提方法的可用性及有效性。

关键词: 区块链;DPoS;社区演化;共识机制;可视分析

中图法分类号 TP391.41

Visual Analysis Method of Blockchain Community Evolution Based on DPoS Consensus Mechanism

WEN Xiao-lin, LI Chang-lin, ZHANG Xin-yi, LIU Shang-song and ZHU Min

College of Computer Science, Sichuan University, Chengdu 610065, China

Abstract DPoS (delegated proof of stake) is one of the current mainstream blockchain consensus mechanisms, and the unique node election mechanism makes it form an evolving blockchain community. Analyzing the evolution model of the blockchain community can discover the potential risks of the consensus mechanism, which has very important research significance. For the DPoS consensus mechanism blockchain data, a novel combination analysis method of the consensus mechanism effectiveness is proposed, and a set of visual analysis methods are designed to help users analyze the evolutionary model of the blockchain community from multiple angles. First, it quantifies the difference between the degree of completion of the work and the voting ranking before and after the node ranking change and analyzes the selection efficiency and incentive efficiency of the consensus mechanism; then, it focuses on the combined efficiency of the consensus mechanism, the evolution of the geographical distribution of nodes, and the comparison of the evolutionary differences between nodes and designs visual views and interactive means; finally, it designs and implements a visual analysis system of blockchain community evolution based on the DPoS consensus mechanism based on the real data of the EOS main chain and verifies the usability and effectiveness of this method through case studies and expert evaluation.

Keywords Blockchain, DPoS, Community evolution, Consensus mechanism, Visual analysis

1 引言

近年来,区块链的运用涉及智能合约、医疗、金融、物联网、交通等多个领域。如何在决策权高度分散的去中心化系统中使各节点高效地对区块数据的有效性及其一致性达成共识,是区块链技术研究的重点。因此,工作量证明(Proof of Work, PoW)、权益证明(Proof of Stake, PoS)、委托权益证明(Delegated Proof of Stake, DPoS)等多种共识机制被相继提出,用于解决区块链中由谁来记账、如何记账、如何维护账本统一等问题。在采用 PoW 共识机制的区块链网络中

(如比特币),区块生产者由算力决定,易导致计算资源的大量浪费;在采用 PoS 共识机制的网络中(如以太坊),区块生产者由币龄决定,易导致严重的马太效应;而采用 DPoS 共识机制的区块链(如 EOS),区块生产者由普通节点票选决定,实现了快速共识验证,并解决了算力浪费和马太效应等问题。

DPoS 机制中并不是所有节点都可以成为记账节点,而是由专门的区块生产者负责记录和验证链上的交易信息。区块生产者的名额是固定的,由全部节点进行投票选举来确定。符合相应标准的节点可以作为备用节点参与竞争,其余节点

到稿日期:2020-12-11 返修日期:2021-04-23 本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。

基金项目:成都市技术创新研发项目(2019-YF05-02121-SN)

This work was supported by the Chengdu Science and Technology Bureau, China(2019-YF05-02121-SN).

通信作者:朱敏(zhumin@scu.edu.cn)

以持有的加密货币数量占总量的百分比为权重进行投票,票数较高的备选节点才能获得生产区块的资格。节点投票的权重会随着时间的延长不断减弱,因此节点需要及时调整投票方案以维持社区稳定。如果区块生产者不能胜任工作,例如,工作时限内未能及时生成区块,则会因失去大量节点的信任而降低排名,甚至失去生产区块的资格。相应地,高效工作节点的投票排名会相应增加,从备选节点中脱颖而出,成为新的区块生产者。因此,基于 DPoS 共识机制的区块链会形成一个独有的且不断演化的节点社区。同时,区块链社区也会存在如下风险:

(1)区块生产者联合操纵社区,损害社区普通节点的利益;

(2)选出不合格的区块生产者,导致社区生产能力下降。

对于区块链社区管理者等利益相关人员与共识机制的研究者而言,分析区块链社区的演化模式是检验上述风险的有效手段。可视分析能有效结合人脑智慧和机器智能,直观地呈现演化过程中的细节信息并提供灵活的交互手段用于探索和分析风险产生的原因^[1]。目前区块链可视化工作,主要研究基于 PoW 或 PoS 共识机制的传统数字货币,仅有较少的研究关注到 DPoS 这一新颖的区块链共识机制。而在对 DPoS 共识机制的可视分析中,现有的工作仅在原始数据层面进行简单的展示,不支持在各时间粒度下交互式地下钻探索,缺乏对共识机制效能的有效度量与呈现,未能将共识机制效能、节点地域分布和节点间的演化差异比较分析融合,也无法有效地探索区块链社区演化模式。因此,本文以探索区块链社区演化模式为目标,提出了一套可视分析方法,包含了共识机制组合效能分析、节点地域分布演化分析和节点间演化差异比较分析 3 个部分。该可视分析方法提供了更多维度的视

角和更灵活的分析手段,能有效地洞察区块链社区在实际演化过程中的异常,对共识机制的选择效能和激励效能进行组合分析;还能通过展示不同时段区块生产者地域分布的演化情况,及时发现串通联合操纵社区的潜在风险。该方法不仅支持区块链社区演化模式的整体趋势分析,还可以对单个节点的演化模式及多个节点的演化差异等社区演化过程中的局部细节进行深入分析。基于该方法,研究者能更深入地发现该共识机制的优缺点,提出改进方案;利益相关人员也能及时调整管理或投资策略,增加收益。

本文的研究贡献主要有以下 3 个方面:

(1)提出了一种共识机制效能组合分析策略。将 DPoS 共识机制的效能度量划分为选择效能与激励效能,选择效能表示该共识机制是否能够选择出可靠的节点,激励效能表示节点排名既定情况下,该机制能否激励节点较好地完成本职工作,二者共同体现了共识机制的效能。本文针对社区演化过程中节点排名变化前后工作完成度与投票排名的差异,提出了节点工作完成度计算方法,并设计了结合选择效能与激励效能共识机制的组合效能分析策略。

(2)提出了基于 DPoS 共识机制的区块链社区演化的可视分析方法。针对区块链社区演化在组合效能、地域分布、节点差异等方面的特性,设计了新颖的可视化视图与交互手段,提供了一套有效的可视分析流程,从多个视角对存在的风险进行洞察,挖掘出区块链社区潜在的演化模式。

(3)设计并实现了基于 EOS 主链真实数据的可视分析系统,如图 1 所示。通过案例研究和专家评估对上述方法的有效性和可用性进行验证。结果表明,本文方法能够在实际场景下帮助用户有效地探索区块链的社区演化模式,挖掘出异常模式并分析异常原因。

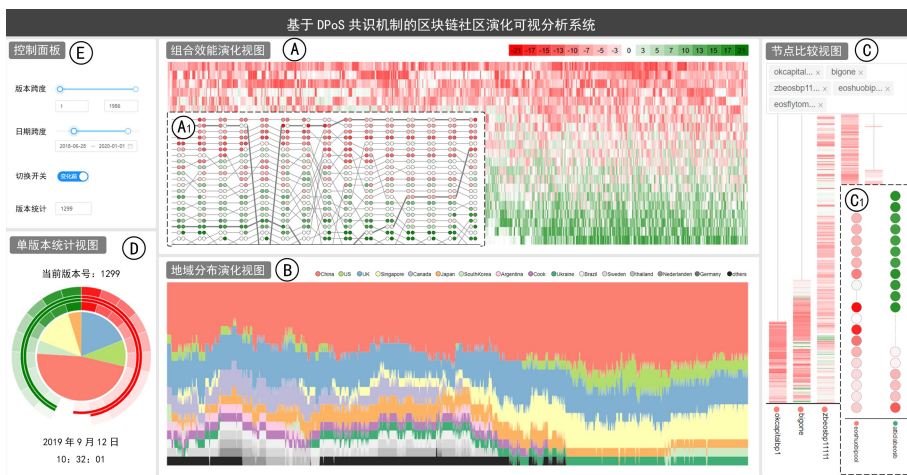


图 1 基于 DPoS 共识机制的区块链社区演化可视分析系统(电子版为彩色)

Fig. 1 Visual analysis system of blockchain community evolution based on DPoS consensus mechanism

2 相关工作

2.1 区块链共识机制研究

共识机制的优化与改进一直是区块链领域的研究热点。Zheng 等^[2]对现有的区块链技术进行了综述,总结了区块链广泛的应用场景,比较了不同区块链共识算法的差异,并指出了区块链技术未来的发展方向。Bano 等^[3]强调了区块链的核心组件是共识,讨论了区块链共识设计的各个组成部分,将

共识机制分为基于 Pow 的协议、基于 Proof-of-X 的替代协议以及混合协议,从安全性和性能的角度比较其优缺点,并且指出未来共识机制研究中交易吞吐率和交易处理的可扩展性。Zohar^[4]侧重于研究区块链激励机制,强调了以工作量证明为基础的区块链系统中激励机制的重要性,不合理的激励会使整个系统陷入危机。最新的研究中,Ferdous 等^[5]调查了现有的大部分新颖的共识算法,详细研究了共识算法中仍普遍存在的不同问题的含义,并且分析了基于不同共识算法的一

百多种加密货币,以了解其特性并分析其趋势差异。Guo 等^[6]将区块链结构按层级划分,阐明了每层区块链的核心技术原理,分析了区块链的研究进展并进行了展望。此外,文献^[5]对本文研究对象 DPoS 共识机制的相关研究进行了详尽的梳理,总结了基于 DPoS 共识机制的 5 种加密货币(EOS, Tron, Tezos, Lisk, Ark)的特点和发展。

目前,对于 DPoS 共识机制的改进研究大多通过引入新的附加机制来提升共识效率。针对 DPoS 共识机制节点投票不积极以及恶意节点勾结等现象,Tan 等^[7]引入投票激励机制来提升社区活跃度;Huang 等^[8]提出了一种基于熔断机制、信用机制和备用见证人节点的 DPoS 共识机制改进方案;Ji 等^[9]基于信任度匹配来对投票共识的过程进行优化;Chen 等^[10]在 DPoS 中引入“奖励机制”,提高了节点的投票积极性,增强了普通节点对恶意节点的贿赂抵抗性,以降低区块链网络的风险。但现有 DPoS 共识机制的改进研究发现问题角度单一,未考虑区块链社区在实际场景下的时序演化特征、共识机制效能和地域分布等信息。在分析手段方面,大多通过理论推导或模拟区块链来运行,其直观性和灵活性都存在缺陷,无法进行多角度、多层次的交互式探索。为了弥补上述不足,本文设计了高度交互的可视分析方法,考虑了共识机制的组合效能及节点地域信息的影响,分析了区块链社区演化模式,并以 EOS 主链为例证明了所提方法的有效性。

2.2 区块链可视分析研究

近年来,区块链相关数据的可视分析研究逐渐活跃。Tovanich 等^[11]系统回顾了文献中或在线提出的 76 种用于区块链相关数据的可视分析工具,并将其按照目标区块链、区块链数据、目标受众、任务领域和可视化类型进行分类。调查显示,目前存在大量的网站为实时事务可视化和事务网络信息导航等提供可视化工具。然而,它们大多只是描述性的统计数据或事务细节,缺乏更深层次的分析与交互。BitCone-View^[12]是一项推测洗钱等非法活动的开创性工作,它利用定制的流程图来检测可疑的比特币交易;Dan 等^[13]将高保真可视化技术应用于大型观测设施,目的是展示出预期之外的动态事务模式,但这些先前的研究主要基于区块的内容来检测异常模式,很少涉及特定的用户或组织。针对这一点,文献^[14]采用带有图可视化的启发式聚类算法来分析区块链数据,以进行用户网络表征。Isenberg 等^[15]扩展了之前关于实体比特币交易活动的可视化探索工作,并进一步揭示了个体实体的交易历史。BitVis^[16]使用带有过滤面板的多个图形可视化来显示交易网络,以检测异常和可疑的比特币实体。针对现有研究不适合处理分析交易所间连接模式的问题,Yue 等^[17]提出了一个名为 BitExTract 的交互式的可视化分析系统,第一次尝试从交易所对交易所以及交易所对客户两个角度来探索比特币交易的演化交易模式,从区块链的应用层面去分析整个市场的变化趋势,而不仅仅是关注底层技术,为区块链可视化提供了重要思路。

总体来说,目前研究主要关注区块链事务细节分析^[13-14,18]、事务网络分析^[19-22]、异常检测^[16,20-24]、交易所分析^[17]和 P2P 网络活动分析^[25]等,缺少针对区块链社区演化模式的研究。研究对象大多为比特币,以其他加密货币为研究对象的研究(如以太坊^[19,25]和丝路币^[26])相对较少,缺少对

新颖加密货币进行可视分析的工具。本文针对基于 DPoS 这一新颖共识机制所形成的区块链社区,在事务网络分析和异常检测相关研究的基础上,提出了用于分析区块链社区演化过程、挖掘异常演化模式的可视分析方法。

3 数据与任务

3.1 数据抽象

目前,Tron,EOS 等多个区块链项目都基于 DPoS 共识机制,其中 EOS 的应用最为广泛且极具代表性。因此,本文选择基于 EOS 主链的真实数据进行研究,数据源包含区块生产者的历史排名快照数据、历史收益数据和节点信息数据。历史排名快照数据中包含每次节点排名变化时的时间戳和各节点的投票排名;历史收益数据记录了区块生产者每日生产区块的工作收益和投票奖励;节点信息数据记录了节点的账号名称、创建时间和所属地域等信息。本文将与区块链社区演化密切相关的数据属性抽取出来,如表 1 所列。

表 1 本文所用区块链的社区数据
Table 1 Blockchain community data used in this paper

属性名称	属性描述	示例
version	版本号	2
time	版本更迭时间	14 Jun 2018 at 17:41:13
name	节点名称	EOS Argentina
account	节点账号	argentinaeos
votes	收到投票总数	71 278 283
place	节点所属国家	Argentina
amount	节点每日收益	818.1132
date	收益获取日期	2018-06-17

3.2 共识机制效能组合分析策略

共识机制的效能在区块链社区演化过程中具有重要作用,较高的效能可以有效约束区块生产者及时完成工作,激励节点为社区作出贡献;而较低的效能会引发节点消极工作、串通牟利等问题。本文提出了一种共识机制效能组合分析策略,用于辅助分析共识机制效能对区块链社区演化过程的影响,策略流程如图 2 所示。

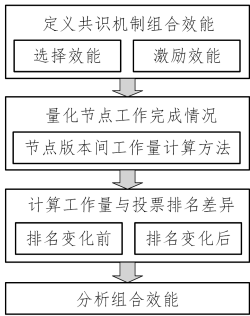


图 2 共识机制组合效能分析策略

Fig. 2 Consensus mechanism combination effectiveness analysis method

首先,定义共识机制组合效能。将 DPoS 共识机制的效能度量分为选择效能与激励效能,选择效能表示该共识机制是否能够将可靠的节点选择出来;激励效能表示节点排名既定情况下该机制能否激励节点较好地完成本职工作,对二者进行组合分析可评估共识机制的效能。排名变化前节点的工作完成度排名与实际投票排名的差异可以体现出共识机制的选择效能。差异低可以证明节点票数可以较好地匹配其工作

完成度,共识机制选择效能较高;而差异高则代表工作完成度低的节点被选择到较高的位置上,或者认真工作的节点没有得到应有的奖励,选择效能较低。排名变化后节点的工作完成度排名与实际投票排名的差异可以反映出共识机制的激励效能。差异低代表被投票选择出的区块生产者得到了足够的激励,完成了与排名相匹配的工作量;如果差异较高则反映出排名高的节点并未努力工作,区块链社区存在潜在风险。

其次,量化节点的工作完成情况。由于节点每日生产区块的收益与其工作完成度高度相关,因此,可以使用两次排名版本之间的收益数额来近似节点工作完成度。如图 3(a)所示, D_1 至 D_5 代表相邻的 5 天, V_1 至 V_6 代表节点排名的 6 个版本,版本与日期相互穿插形成多种组合方式,通常没有规律可循。一天内节点成为区块生产者的时段可能不是连续的,例如如图 3(b)中的节点在 V_3 时成为区块生产者,而在 V_4 时被剥夺生产区块的资格,在 V_5 时又重新被投票选中。两个版本之间也可能跨越多天,如图 3(c)中 V_2 和 V_3 之间包含了 D_2 和 D_3 两天。

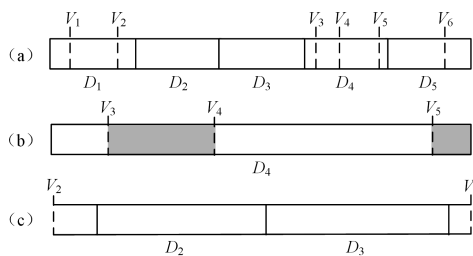


图 3 节点工作完成度计算示意图

Fig. 3 Schematic diagram of node work completion degree calculation

针对这种组合的多样性,本文提出了节点版本间工作量的计算方法,用于量化两次版本之间某个节点的工作完成情况。首先,计算节点每天生产区块的时长,如图 3(b)中的阴影部分的时间长度(单位为 s)。假设某节点第 i 天共有 k 段时间生产区块,当天第 j 段工作时长为 T_{ij} ,生产区块收益为 $Amount_i$,节点每日的平均收益 AP_i 可由式(1)求得:

$$AP_i = \frac{Amount_i}{\sum_{j=1}^k T_{ij}} \quad (1)$$

然后,假设 0h 的时间戳为 t_0 , 24h 的时间戳为 t_1 , 版本 V_q 在第 m 天的时间戳为 t_q , 版本 V_{q+1} 在第 n 天的时间戳为 t_{q+1} , 节点在版本 V_q 与版本 V_{q+1} 间的工作完成度为 W_q 。

若 $m=n$,则 W_q 可由式(2)求得:

$$W_q = AP_m \times (t_{q+1} - t_q) \quad (2)$$

若 $m < n$,则 W_q 可由式(3)求得:

$$W_q = AP_m \times (t_{q+1} - t_q) + \sum_{i=m+1}^{n-1} Amount_i + AP_M \times (t_{q+1} - t_0) \quad (3)$$

最后,计算工作量与投票排名差异来分析共识机制的组效能对区块链社区演化产生的影响。对于任意版本 V_q ,分别对所有区块生产者在排名变化前后的工作完成度 W_{q-1} 和 W_q 进行排名,得到 $rank_{q-1}$ 和 $rank_q$ 。二者与节点投票排名的差异分别代表着共识机制在版本 V_q 时的选择效能和激励效能,差异值越接近零则共识机制的效能越高,反之则证明区块链社区演化过程中存在一定的潜在风险。

3.3 可视分析任务

由上述数据特性与共识机制效能组合分析策略可知,区块链社区演化模式主要体现在共识机制效能、节点地域分布和节点间演化差异 3 个方面。因此,本文针对区块链社区演化模式的分析需求,定义了以下 3 项可视分析任务。

T_1 : 共识机制组合效能分析。共识机制的效能一定程度上能决定区块链社区的演化趋势,结合本文提出的共识机制效能组合分析策略,展示演化过程中选择效能和激励效能的变化情况,定位共识机制低效能的时间节点,有助于专家发现该机制的优劣性,从而对其进行改进。

T_2 : 节点地域分布演化分析。相同地域掌控过多的节点是区块链社区中最严重的问题之一,不仅会降低区块的生产效率,还会引发社区的信任危机。分析区块生产者在地域分布上的演化模式,一方面可以及时预防节点串通牟利问题,另一方面可以帮助专家从新的视角来评估该共识机制。

T_3 : 节点间演化差异比较分析。节点的投票排名、工作完成度、效能影响等多个属性均随时间变化情况来共同形成区块链社区演化模式的多变性和多样性,选择多个具有相似或相同属性的节点进行比较分析,有助于专家通过发现节点间演化模式的差异性来深入分析不同的演化模式形成的原因,总结出从整体上难以察觉的演化规律。

4 可视分析系统

4.1 系统概述

根据可视分析任务,本文设计并实现了一个基于 DPoS 共识机制的区块链社区演化可视分析系统。系统的用户界面如图 1 所示,包含组合效能演化视图(见图 1(a))、地域分布演化视图(见图 1(b))、节点比较视图(见图 1(c))、单版本统计视图(见图 1(d))和控制面板(见图 1(e))。可视分析的流程是,首先,从区块链社区演化模式的总览入手,在控制面板交互地设置展示的时间跨度、版本号等信息,探索比较不同时期的共识机制组合效能与地域分布的演化模式,从而发现社区中存在的潜在风险并提出假设;然后,锁定感兴趣的时段和版本,结合节点比较和单版本统计更深入地分析演化细节,分析相似或差异的原因,验证先前的假设,形成可视分析的闭环。

4.2 视图设计

4.2.1 组合效能演化视图

组合效能演化视图展示了区块链社区演化过程中共识机制的选择效能和激励效能的变化情况,对应可视分析任务 T_1 和 T_3 。

为避免视觉混淆,本文根据选定时段内的版本数量将组合效能演化视图分为全局视角和局部视角。全局视角(图 1(a))采用了显示多重变量的热区图,横轴编码节点排名变化的版本,每一列代表节点排名发生一次变化,而纵轴则表示区块链社区中区块生产者的投票排名,相同社区的区块生产者数量是固定不变的。热区的颜色编码节点工作完成度排名与投票排名的差异值,用于表示共识机制效能的强弱。

当时间跨度低于 25 个版本时,组合效能演化视图将启用局部视角(图 1 中的 A_1),将选择效能和激励效能相结合,加入单个节点的排名变化信息,为用户呈现出更多的细节。可视化布局方法如图 4 所示,坐标轴的意义与全局视角一致,

使用并排的两个圆形分别编码当前排名前后工作完成度排名与本次投票排名的差异,颜色及深度编码工作量排名与实际排名的差异程度,红色越深代表该节点在这次排名中被高估的程度越高,绿色越深代表该节点完成度排名远高于当前的实际排名。当差异值显示为白色时,表示节点工作完成度排名与实际投票排名相同,表明投票结果合理、共识机制模式效用较高。此外,该视图还引入了折线图的思想,将相同节点用直线进行连接,剥夺区块生产资格的节点则与底线相连,展示了单个节点投票排名的变化趋势。

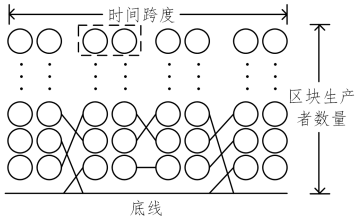


图 4 组合效能视图可视化布局(局部视角)

Fig. 4 Visual layout of combined effectiveness view (partial perspective)

4.2.2 地域分布演化视图

地域分布演化视图(图 1 中的 B)采用扩展堆叠面积图,清晰地呈现了社区演化过程中区块生产者所属地域的分布情况,对应分析任务 T_2 。

该视图的横轴与组合效能演化视图共享相同的时间跨度,纵轴的定义域映射到 $(0,1)$ 区间,用于展示区块生产者所属地域的比例分布。颜色编码代表不同的地域,如(红色,中国)、(蓝色,英国)、(浅绿,美国)等。用户对该视图进行不同时间粒度下的探索与比较,可以发现区块链社区演化过程中来自某一区域节点所占比例的变化情况,挖掘出潜在的演化模式。

4.2.3 节点比较视图

节点比较视图(见图 1 中的 C)对应可视分析任务 T_3 ,通过展示社区演化过程中单个节点受共识机制效能的影响程度、排名变化和工作完成度来比较分析节点之间的相似性或差异性,对已有假设进行验证。该视图纵轴编码表示选定时间段,横轴编码表示被选中的节点。直线区域表示节点被剥夺生产区块的资格,非直线部分的颜色和形状编码与组合效能演化视图保持一致,采用矩形和圆形分别编码全局视角(图 1 中的 C)和局部视角(图 1 中的 C_1)下节点工作完成度排名与投票排名的差异。

通过对组合效能演化视图和地域分布演化视图进行分析,发现用户可以挖掘出潜在的演化模式或异常模式,但这些模式的形成原因往往无法解释。而节点比较视图可以弥补这一不足,通过对目标时段内各个节点的表现进行交互式分析,来追溯演化模式形成的根源。

4.2.4 单版本统计视图

上述 3 个视图都使用时间轴来呈现数据的动态变化,试图从时变上挖掘出区块链社区的演化模式,忽略了截面数据对分析结果的辅助作用。为此,本文设计了单版本统计视图(见图 1 中的 D),用于呈现单个版本中组合效能演化视图和地域分布演化视图的截面数据。

设计使用嵌套式圆形布局、中心的饼图来展示当前版本区块生产者的国家分布,颜色编码与地域分布演化视图使用

相同的颜色映射,以方便用户理解;外圈以两个细环为边界并分为内圈和外圈两组,分别展示排名变化前后的数据。细环编码被高估(红色编码)、被低估(绿色编码)以及被正确评估的社区节点的比例;较宽的环形热力图用于展示详细的统计信息。

5 案例分析

本文收集并处理了 EOS 主链 2018 年 6 月主网上线至 2020 年 1 月之间的历史排名快照数据、历史收益数据和节点信息数据,包含了 1596 个节点排名更迭版本。

本文邀请了 6 位专家使用可视分析系统对 EOS 社区演化模式进行探索分析,专家包含 2 位区块链共识机制研究人员(E1 和 E2)、1 位资深加密货币投资者(E3)和 3 位可视分析研究人员(E4—E6)。

5.1 组合效能演化模式挖掘

专家们都比较关心区块链社区的整体演化情况,本系统提供的组合效能演化视图和地域分布演化视图可以从两个不同角度提供支持。专家通过控制面板与系统进行交互,将目标时间跨度设置为 2018 年 6 月至 2020 年 1 月。与此同时,组合效能演化视图和地域分布演化视图将该区间内的区块链社区演化情况进行呈现。

E1 和 E2 作为共识机制领域专家,对 DPoS 共识机制的组合效能在整体上随时间的演变情况表达出了浓厚的兴趣。实验者首先通过单击切换开关,分别观察排名变化前(图 5 中的 A)和变化后(图 5 中的 B)的组合效能演化视图。纵向观察视图后,发现二者存在共同的特征:红色主要出现在上半部分,绿色主要出现在下半部分,越靠近上下两端颜色就越深,而中间部分的颜色较浅。这表明在区块链社区演化过程中 DPoS 共识机制对节点的选择效能和激励效能都不是特别理想。从选择效能来看,该机制对排名靠前的节点出现了过于高估的现象,还相对低估了排名靠后的节点,但对于中间排名的节点选取效果表现良好;从激励效能来看,排名靠前的节点并没有完成符合其排名位置的工作,而排名靠后的节点大多都在努力完成工作。

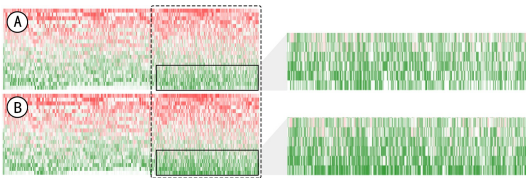


图 5 共识机制组合效能的整体演化情况(电子版为彩色)

Fig. 5 Overall evolution of the combined effect of the consensus mechanism

专家又通过横向观察视图来分析区块链社区随时间演化的模式,发现图 5 中虚线框内的区域发生了明显的颜色加深。这段时间内共识机制的效能突然降低,出现了大量的高估或低估节点工作量的情况,不能有效地将节点按照工作水平进行排名。此外,专家通过变化前后的对比分析发现,排名变化后实线框内部分的绿色要明显深于变化前,而同时段下红色变化前后的分布却较为相似。这说明在投票排名变化后排名

靠后的节点表现出众,而排名靠前的节点的工作效率几乎维持原样。该结果也在一定程度上表示 DPoS 共识机制仅对排名较低或未进入排名的节点起到了激励作用,鼓励这些节点为了获取更高的排名和收益而更努力地工作;但对于排名较高的节点来说,这种激励作用几乎没有效果。

5.2 地域演化模式探索

专家 E3 作为数字货币资深投资者,十分关心共识机制组合效能降低对区块链社区安全性产生的影响,多个节点串通牟利会严重影响普通投资者的利益。因此,在 E1 和 E2 两位专家发现共识机制效能突然降低时,E3 推测可能存在节点串通的现象,建议从地域分布上分析效能突变的原因。

专家们将关注点放到地域分布演化视图(见图 1 中的 B)上,分析社区内节点在地理分布上随时间的变化。从图中可以看出,代表中国节点的红色在整个时间区间内都占据着相当大的比例,甚至在某些时段内中国节点的比例超过了 50%;来自英国、日本、乌克兰的节点几乎在整个时间段都占有一定的比例;来自美国、新加坡、韩国的节点都是在前半部分出现较少而在 2019 年 6 月之后才开始占据一定比例;其他国家,如加拿大、13 尼德兰、巴西、德国等都是 在 2018 年比较活跃而后逐渐掉出前 21 名。

总体来说,2018 年下半年到 2019 年上半年期间排名前 21 名的超级节点的地域分布比较平均,呈现出一种百家争鸣的特点。图 6 中左图展示了 2018 年 7 月 18 日的版本统计视图,可以看出,虽然中国、加拿大和英国的节点比例相对较大,但是仍在可以接受的范围内。但从 2019 年 6 月开始前 21 名的超级节点由中国、新加坡、英国和美国几个大国统治,4 个国家加起来的比例超过 80%。图 6 中右图展示了 2019 年 8 月 19 日的版本统计视图,可以看出,中国的节点超过半数,除了日本和韩国各占了一个节点外,其他所有节点都来自上述

4 个国家。这种不协调的地域比例分布可能会产生很多安全问题,例如,同一国家节点共同约定修改区块链上的数据或者集体密谋控制投票等。因此,专家怀疑共识机制效能的突然降低与上述 4 个国家对节点的控制有关。

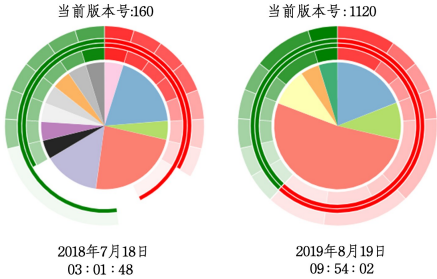


图 6 单版本统计视图比较(电子版为彩色)
Fig. 6 Single version statistical view comparison

5.3 共识机制效能突变原因分析

专家通过比较图 6 中的两个环图发现,右侧环图较为饱满且颜色较深,而左侧环图存在缺口。左侧外环绿色较多,而内环红色较多。这意味着在节点地域分布分散时,共识机制的整体效能高且激励效能高于选择效能;而节点地域分布集中时,共识机制的整体效能较低。上述分析结果虽然能在一定程度上证实区块链社区演化过程中地域分布与机制效能间存在的联系,但无法确认哪些节点导致了这种影响,因此,专家们试图对单个节点演化模式进行比较分析,从细节上进一步挖掘共识机制效能突变的具体原因。

本系统允许专家在组合效能视图中将感兴趣的节点选入节点比较视图,后者将展现出单个节点的地域信息及该时段下共识机制对其的作用效果,用于比较分析。首先,将时间跨度设置为 2019 年 6 月至 2019 年 8 月(组合效能突变的异常时段),局部视角下的组合效能视图如图 7 所示。

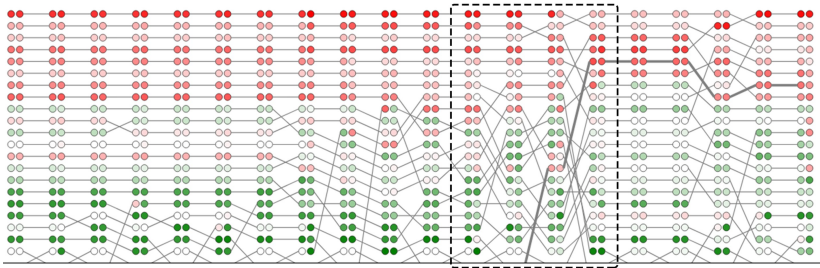


图 7 异常时段组合效能视图
Fig. 7 Combination performance view during the abnormal period

可以观察到,虚线框内存在较为强烈的排名波动,通过点击交互发现名为 newdexbp 的节点短时间内排名急速上升。将该时段排名前六的节点选入节点比较视图(见图 8 中的 A),发现除了 newdexbp 来自英国外,其余 5 个节点都来自中国,且节点颜色都为红色。专家 E1 和 E2 考虑中国节点存在串通起来非法换取选票的可能,但这无法解释 newdexbp 节点排名急速上升的原因。此时,专家 E3 发现上述 6 个节点中(包含 newdexbp 在内)有 4 个为交易所节点,推测可能交易所节点的加入才是导致区块链社区演化模式突变的根本原因。

基于上述假设,专家 E3 选择了熟知的 6 个交易所节点,

并将时间跨度扩展至全时段。此时节点比较视图(见图 8 中的 B)呈现了主流交易所节点的演化模式,除了火币网节点外,其余交易所节点刚好在社区演化模式突变后才成为超级节点,且所有交易所节点的组合效能几乎都被严重高估。根据 E3 的描述,自 2019 年 5 月 EOS 资源交易所 REX 上线,交易所节点凭借大量用户资源收揽选票,正逐渐将老一辈超级节点赶下历史舞台。结合前述分析可以验证,这种节点更新换代的方式将区块链社区演化模式引导到了错误的方向,应当对所有利益相关者敲响警钟。此发现验证了交易所节点加入导致区块链社区演化模式突变的假设,同时排除了中国节点非法获取选票的可能。

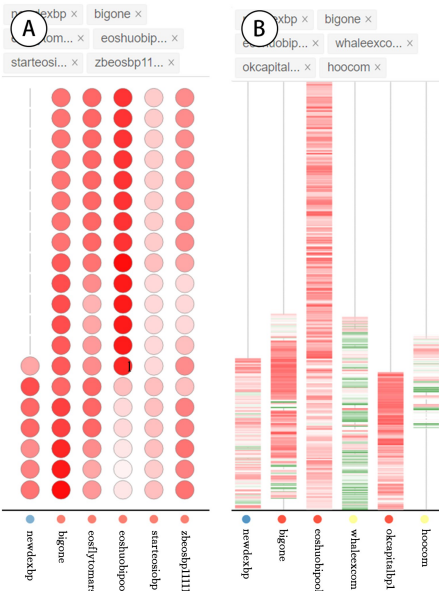


图 8 节点演化比较分析(电子版为彩色)

Fig. 8 Comparative analysis of node evolution

6 专家评估与建议

为了评估本文提出的可视分析方法,在 6 位专家使用可视分析系统探索区块链社区演化模式的过程中,记录了其对未来改进的意见和建议,并在分析完成后又集中收集了用户反馈。

首先,区块链领域专家们一致表示本文提出的方法具有实际意义。相比以往区块链节点数据的分析方法,使用本文方法可以更加简便快捷地发现容易被忽略的异常演化模式并分析其产生的原因。E1 表示对节点组合效能分析的方法新颖且实用,结合组合效能视图的展示与交互可以深刻理解演化过程中共识机制的表现情况,可以指导专家发表关于 DPoS 共识机制改进的新见解。E2 认为将单个节点的信息嵌入到组合效能视图中起到了辅助分析的作用。E3 表示依靠本文分析方法得出的 2019 年 6 月效能突变的引发原因对投资者选择数字货币交易所具有指导意义。

同时,专家们也给出了对本文方法的修改建议。E2 希望可以不仅考虑排名前 21 的超级节点,未竞选成功的备选节点的演化模式也同样值得研究。E4—E6 从视图设计和交互角度,首先肯定了组合效能视图和节点比较视图嵌入更多信息的做法,但颜色映射存在不足,采用不同深度编码并不能有效区分节点的效能差异。此外,与组合效能视图交互时,选中多个节点会发生重叠现象,引起视觉混淆,不易于用户理解。

7 用户评估

案例分析与专家评估已初步验证了本文提出的可视分析方法的有效性,为了更加客观地对本文方法的有效性和可用性进行全面评估,本文采用用户评估来分析缺乏经验的普通用户对可视分析系统的使用体验。

7.1 评估成员构成

本文的用户评估环节邀请了 15 位成员参加,其中包括 6 名女性和 9 名男性,年龄都处于 21~26 岁(均值为 22.67,方差为 1.69)。参与者均为对数字货币和区块链感兴趣,或有

数字货币交易经验的在校大学生。图 9 给出了用户通过李克特量表对数据分析、区块链相关知识和数据集掌握程度的自评报告。

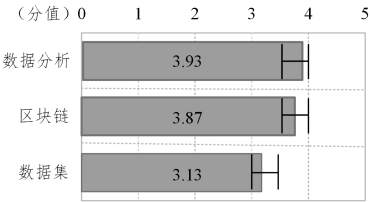


图 9 成员知识背景统计

Fig. 9 Statistics of member knowledge background

7.2 评估设计

用户评估分为 4 个阶段:第一阶段,用户需花费 30 min 熟悉问题背景并自由探索数据集,保证其了解数据特性;第二阶段,要求用户使用传统区块链浏览器中的可视化工具分析 3.3 节中的 3 个任务(T_1-T_3),每个任务用时 5 min;第三阶段,用户需花费 10 min 学习可视分析系统的各部分含义及操作方法,然后在与第二阶段相同时间内使用系统分析相同的任务;第四阶段,采用问卷调查并从有效性和可用性两方面判断用户对系统的使用体验,问卷内容如表 2 所列。

表 2 问卷内容

Table 2 Questionnaire content

类别	序号	内容
有效性	Q_1	共识机制组合效能分析是否达到效果?
	Q_2	节点地域分布演化分析是否达到效果?
	Q_3	节点间演化差异比较分析是否达到效果?
可用性	Q_4	可视分析系统的视图设计是否易于理解?
	Q_5	可视分析系统的交互操作是否易于使用?
	Q_6	可视分析系统是否优于传统分析手段?

7.3 评估结果与讨论

用户的评估结果如图 10 所示,左图展示了在第二阶段和第三阶段中用户分析 3 个任务的用时。对比两种分析方式的用时差异可知,本文方法能有效缩减用户得到见解的时间成本,提高了分析效率。右图使用李克特五级量表统计了用户问卷调查的结果。在有效性方面,系统对分析任务的支持程度获得了较高的分数,尤其在组合效用分析中表现优异;在可用性方面,用户一致认为系统的使用体验良好,与传统分析手段相比其更易于理解与分析,但交互操作仍有提升空间。

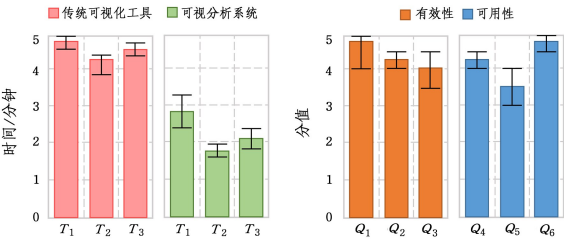


图 10 评估结果

Fig. 10 Evaluation results

结束语 由于 DPoS 共识机制的特性,所有基于该共识机制的区块链都会形成独有的区块链社区。本文基于 DPoS 区块链社区的相关数据,提出了一种新颖的节点组合效能分析策略,设计了完整的区块链社区演化可视分析流程并且实现了相应的可视分析系统。最后,本文邀请了来自区块链共识机制研究、数字货币投资和数据可视化 3 个领域的 6 位

专家及15位缺乏经验的普通用户共同对系统进行评估,验证了本文提出的可视分析方法的有效性和可用性。

未来工作主要包含以下3个方面:1)目前仅考虑了节点的排名、工作量、地域等信息,未来可以将节点类型作为参考,并关注备选节点的演化模式,提高分析的全面性;2)从可视化和交互设计方面改进可视分析原型系统,如采用区分度更大的颜色区间映射节点效能差异和加入自适应布局算法等,优化用户操作体验;3)目前系统仅针对历史数据进行分析,未来可以考虑接入实时数据接口,实时分析区块链社区的演化模式,以便于更及时地洞察异常。

参考文献

- [1] 陈为,沈则潜,陶煜波.数据可视化(第2版)[M].北京:电子工业出版社,2019.
- [2] ZHENG Z, XIE S, DAI H N, et al. Blockchain Challenges and Opportunities: A survey[J]. International Journal of Web and Grid Services, 2018, 14(4): 352-375.
- [3] BANO S, SONNINO A, Al-BASSAM M, et al. SoK: Consensus in the Age of Blockchains[C]// Proceedings of the 1st ACM Conference on Advances in Financial Technologies. 2019: 183-198.
- [4] ZOHAR A. Securing and Scaling Cryptocurrencies[C]// Twenty-Sixth International Joint Conference on Artificial Intelligence. 2017: 5161-5165.
- [5] FERDOUS M S, CHOWDHURY M J M, HOQUE M A, et al. Blockchain Consensus Algorithms: A Survey[J]. arXiv: 2001. 07091, 2020.
- [6] GUO S T, WANG R J, ZHANG F L. Summary of Principle and Application of Blockchain[J]. Computer Science, 2021, 48(2): 271-281.
- [7] TAN S P, YANG C. Research and Improvement of Blockchain's DPoS Consensus Mechanism[J]. Modern Computer (Professional Edition), 2019(6): 4.
- [8] HUANG J C, XU X H, WANG S C. Improved Scheme of Delegated Proof of Stake Consensus Mechanism[J]. Journal of Computer Applications, 2019, 39(7): 2162-2167.
- [9] JI Y X, HUANG J H, WANG Z, et al. Improved PBFT Consensus Algorithm Based on Trust Matching[J]. Computer Science, 2021, 48(2): 303-310.
- [10] CHEN M R, LIN Y, LAN W, et al. Improvement of DPoS Consensus Mechanism Based on Positive Incentive[J]. Computer Science, 2020, 47(2): 269-275.
- [11] TOVANICH N, HEULOT N, FEKETE J D, et al. Visualization of Blockchain Data: A Systematic Review[J]. IEEE Transactions on Visualization and Computer Graphics, 2019, 27(7): 3135-3152.
- [12] BATTISTA G D, DONATO V D, PATRIGNANI M, et al. Bitconeview: Visualization of Flows in the Bitcoin Transaction Graph[C]// Visualization for Cyber Security. IEEE, 2015: 1-8.
- [13] DAN M G, BIRCH D, AKROYD D, et al. Visualizing Dynamic Bitcoin Transaction Patterns[J]. Big Data, 2016, 4(2): 109-119.
- [14] GAULDIE D, LANGEVIN S, SCHRETLEN P, et al. Louvain Clustering for Big Data Graph Visual Analytics[C]// IEEE Vi-week 2013. IEEE, 2013.
- [15] ISENBERG P, KINKELDEY C, FEKETE J D. Exploring entity behavior on the bitcoin blockchain [C]// VIS 2017-IEEE Conference on Visualization. 2017: 1-2.
- [16] SUN Y, XIONG H, YIU S, et al. BitVis: An Interactive Visualization System for Bitcoin Accounts Analysis[C]// 2019 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, 2019: 21-25.
- [17] YUE X W, SHU X, ZHU X, et al. Bitextract: Interactive Visualization for Extracting Bitcoin Exchange Intelligence[J]. IEEE Transactions on Visualization and Computer Graphics, 2018, 25(1): 162-171.
- [18] CHAWATHE S. Monitoring Blockchains with Self-Organizing Maps[C]// 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018: 1870-1875.
- [19] NORVILL R, PONTIVEROS B B F, STATE R, et al. Visual Emulation for Ethereum's Virtual Machine[C]// NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2018: 1-4.
- [20] AHMED M, SHUMAILOV I, ANDERSON R. Tendrils of Crime: Visualizing the Diffusion of Stolen Bitcoins[C]// International Workshop on Graphical Models for Security. Springer, Cham, 2018: 1-12.
- [21] BISTARELLI S, SANTINI F. Go with the-Bitcoin-Flow, with Visual Analytics[C]// Proceedings of the 12th International Conference on Availability, Reliability and Security. 2017: 1-6.
- [22] OGGIER F, PHETSOUVANH S, DATTA A. BiVA: Bitcoin network visualization & analysis[C]// 2018 IEEE International Conference on Data Mining Workshops (ICDMW). IEEE, 2018: 1469-1474.
- [23] KUZUNO H, KARAM C. Blockchain explorer: An Analytical Process and Investigation Environment for Bitcoin[C]// 2017 APWG Symposium on Electronic Crime Research (eCrime). IEEE, 2017: 9-16.
- [24] KINKELDEY C, FEKETE J D, BLASCHEK T, et al. Visualizing and Analyzing Entity Activity on the Bitcoin Network[J]. arXiv: 1912. 08101, 2019.
- [25] BOGNER A. Seeing is Understanding: Anomaly Detection in Blockchains with Visualized Features[C]// Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers. 2017: 5-8.
- [26] ZHONG Z, WEI S, ZHAO Y, et al. SilkViser: A Visual Explorer of Blockchain-based Cryptocurrency Transaction Data[J]. arXiv: 2009. 02651, 2020.



WEN Xiao-lin, born in 1998, postgraduate, is a member of China Computer Federation. His main research interests include information visualization and visual analytics.



ZHU Min, born in 1971, Ph.D, professor, Ph.D supervisor, is a member of China Computer Federation. Her main research interests include information visualization, visual analytics and bioinformatics.