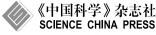
SCIENTIA SINICA Informationis

# 论文





# 基于区块链的数字内容生态价值链构建

周广猛1、姚苏2\*、李琳3、刘昕3、徐恪1,2,4

- 1. 清华大学计算机系, 北京 100084
- 2. 清华大学北京信息科学与技术国家研究中心, 北京 100084
- 3. 中国移动咪咕文化科技有限公司, 北京 100032
- 4. 鹏城实验室, 深圳 518052
- \* 通信作者. E-mail: yaosu@tsinghua.edu.cn

收稿日期: 2020-01-19; 修回日期: 2020-03-03; 接受日期: 2020-04-14; 网络出版日期: 2021-09-15

国家杰出青年科学基金 (批准号: 61825204)、国家自然科学基金 (批准号: 61932016)、北京市杰出青年科学基金 (批准号: BJJWZYJH01201910003011)、北京信息科学与技术国家研究中心 (批准号: BNR2019RC01011) 和鹏城实验室大湾区未来网络试验与应用环境 (批准号: LZC0019) 资助项目

**摘要** 随着互联网和移动终端的普及,数字内容产业正成为文化产业主要经济增长点.本文从数字内容产业面临的版权、质量和产业壁垒问题入手,分析区块链技术对于建设数字内容生态价值链的意义和优势,提出以基于区块链的数字内容平台重塑生态价值链的方案.然后分析新型平台中的关键元素、价值流转、平台架构,设计平台价值流转过程中的基础方案,最后从成本和性能角度证明联盟链适合并且可以支撑平台构建.

关键词 数字内容,价值链,区块链,价值流转,联盟链

# 1 引言

价值链概念由 Michael Porter [1] 在 1985 年第一次提出,他认为每一个企业都是进行设计、生产、营销、交货以及对产品起辅助作用的各种活动的集合.围绕产品的这些活动构成产品链,产品沿着产品链中的活动不断增值形成价值链. 2002 年,爱尔兰政府出台《爱尔兰数字内容产业发展战略》,将数字内容产业定义为创建、设计、管理和销售数字产品以及为上述活动提供技术支持的产业,涵盖网络文学、视频、音乐、游戏、动漫等多种形式.数字内容生态价值链是指围绕数字内容产品创造、生产、销售、传播和消费,以及从中获得利润的过程中形成的链式结构.具体又可以分为纵向价值链和横向价值链,纵向价值链是指从数字内容产品提供商开发创作到顾客使用产品的全过程,横向价值链是指同一产业中处于同等地位的数字内容产品服务商相互作用(例如围绕某一主体产生多种形式的衍生数字内容产品)构成的具有潜在关系的链条.图 1 是当前数字内容生态价值链的示意图,从数字内容产

**引用格式:** 周广猛, 姚苏, 李琳, 等. 基于区块链的数字内容生态价值链构建. 中国科学: 信息科学, 2021, 51: 1559-1574, doi: 10. 1360/SSI-2020-0016

Zhou G M, Yao S, Li L, et al. Digital content ecological value chain based on block chain (in Chinese). Sci Sin Inform, 2021, 51: 1559-1574, doi: 10.1360/SSI-2020-0016

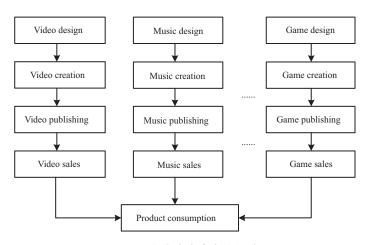


图 1 数字内容生态价值链

Figure 1 Digital content ecological value chain

品提供商的设计开发到数字内容产品服务商的发行销售再到终端设备提供商带来的产品消费,数字内容产品在其中不断增值.

根据中国互联网络信息中心《第 44 次中国互联网报告》, 截至 2019 年 6 月, 我国网民规模达 8.54 亿, 网络普及率达 61.2%, 数字文化产品在移动网民的入网时间中总占比为 53.4%. 数据表明数字文化产业正逐步发展为我国文化产业的主要增长点. 但是在发展过程中, 数字内容生态价值链的各个环节也暴露出很多问题.

- (1) 作品版权. 随着数字内容产业迅速发展, 纵向价值链上游的产品创作环节许多优秀原创作品不断涌现, 但不可忽视的是市场上也出现了大量盗版产品, 版权问题成为数字内容发展亟待解决的重要问题. 盗版猖獗主要有两个原因, 一是盗版成本低, 以电子书为例, 与纸质书相比, 电子书省去了印刷、运输以及销售成本, 而且在互联网的助力下, 数字内容流通、扩散速度飞快. 二是维权难, 这一方面由于原创者对版权登记不重视, 侵权时难以提供确实可信的证据; 另一方面由于整个维权过程手续烦琐, 原创者维权成本增加. 盗版成本低成为客观事实, 且短期难以解决. 如何使得作品版权登记迅速, 原创者维权便捷是亟待解决的问题.
- (2) 内容质量. 互联网的发展带来了信息洪流, 纵向价值链中游的产品传播环节同质化内容、暴力、色情等糟粕不断泛滥, 许多高品质的内容被淹没. 解决这一问题需要加大作品审核力度, 更重要的是形成优质创作激励机制, 例如根据作品点赞量给予原创者实质奖励, 激励原创者推陈出新, 优质内容的不断涌现是数字内容健康发展的关键.
- (3) 产业壁垒. 在数字内容发展的今天, 以知识产权多渠道变现为代表的横向价值链正成为新的发展趋势. 但是多渠道变现需要企业的强大实力支撑, 许多中小企业往往只聚焦于某一种形式的数字内容产品, 难以打破横向发展的壁垒, 造成盈利水平下降, 特别的这也限制了更多优质内容的产生. 而中小企业如果建立联盟, 由于每个个体企业都有各自的局部目标, 联盟又会面临两类企业协调问题. 一是信息共享问题, 例如哪些信息需要共享、共享信息维护、敏感信息处理等; 二是内部执行问题, 例如联盟准入、成本分摊、利益分配等. Gulati 和 Singh [2] 认为, 采用激励机制、标准操作程序和非市场计价系统等手段对企业进行激励、监督甚至适当的命令, 可以达到协调、管理和控制价值链中各企业之间关系的目的. 但是激励的公平公正公开, 协议的强制执行又成为新的问题. 不难发现企业间互不信任是产生绝大多数问题的根本原因, 仅仅依靠建立协议解决这些问题是不可靠的, 企业间互不信任最

终会使得协议毫无用武之地.

区块链技术是近年来蓬勃发展的新技术,以其去中心性、不可篡改性、公开透明性在各个领域得到广泛应用,也给数字内容生态价值链带来新的发展契机.区块链本身可以解决著名的拜占庭将军问题<sup>[3]</sup>,即在一个互不信任的分布式群体中达成共识,这可以解决数字内容产业服务商间的协调问题;区块链的不可篡改性可以为数字内容产品提供便捷可信的版权登记,降低维权成本;建立在区块链上的智能合约运行公开透明,可以用来制定相关机制,例如协调各服务商利益分配,激励原创者创作更多高质量产品等.以区块链为基础打造新型数字内容生态价值链无疑会是未来数字内容生态发展的重要方向.

本文从数字内容生态建设出发,详细论证基于区块链的新型数字内容平台的构建方法,以及新型数字内容平台(以下简称新型平台)对于重塑数字内容生态价值链的意义.新型平台基于联盟链建立,各服务商构成联盟链节点,彼此之间形成横向价值链.平台对接纵向价值链源头——原创者以及纵向价值链尾部——消费者,同时平台实现数字内容产品的传播销售环节,从而打通价值链的各个环节,形成以区块链为保障的新型数字内容价值链.新型平台利用区块链去中心化解决服务商信任问题,分布共识机制解决服务商信息共享问题,不可篡改性解决版权问题,智能合约形成复杂的业务逻辑加强生态建设,同时引入激励机制增强用户黏性.

# 2 相关工作

本节从区块链的起源出发简要介绍区块链从发展到应用的整个历程, 然后介绍区块链在各个领域的应用以及区块链和数字内容相结合的相关工作.

## 2.1 区块链技术发展

区块链起源于中本聪 2008 年发表的一篇论文"比特币:一种点对点的电子现金系统"<sup>[4]</sup>. 文章中阐述了一种不可篡改的、去中心化运行的加密货币—— 比特币, 而支撑比特币运行的技术就是区块链. 之后的 Zerocash <sup>[5]</sup> 和 Monero <sup>[6]</sup> 两种区块链架构在比特币的基础上, 引入零知识证明等技术增强交易隐私. 2013 年末, Wood <sup>[7]</sup> 提出以太坊, 它丰富了比特币的底层架构, 引入智能合约的概念解决比特币扩展性不足的问题. 2015 年, Linux 基金会发起超级账本 Hyperledger 项目, 其中 Hyperledger Fabric 是专门服务于商业联盟的联盟链架构. 与此同时, 区块链也加速在更多领域的应用尝试, 大量区块链项目开始出现 <sup>[8]</sup>.

区块链集分布式数据存储、点对点传输、共识机制、加密算法等多种技术于一身.以比特币为例,区块链由一个个区块依次连接构成,每个区块包括前一区块哈希值、交易信息等内容,区块中的交易信息由默克尔树的形式组织,如图 2 所示. 区块链的头部包含上一区块的哈希值,这一内容也被称作哈希指针,用来将区块串连成链.哈希函数对整个区块内容进行哈希得到当前区块的哈希值,"挖矿"的目标即需要找出符合要求的哈希值.矿工通过改变随机数寻找特定哈希值,所以能够在固定时间试验更多随机数的矿工,也就是算力更强的矿工更容易找到符合要求的哈希值,从而获得记账权.这一机制就是著名的工作量证明机制 (proof of work, PoW),它保证比特币的不可篡改性.具体来说,攻击者如果想篡改区块链上某区块的数据,必须在篡改数据后重新计算该区块及之后所有区块的哈希值,并生成新的最长链,成为区块链主链.完成这种攻击要求攻击者至少能拥有 51% 的算力,这在当今区块链中基本不可能实现.

区块链运行在 P2P 网络上, 网络中每个节点都保存着在区块链上进行的交易记录. 当交易产生

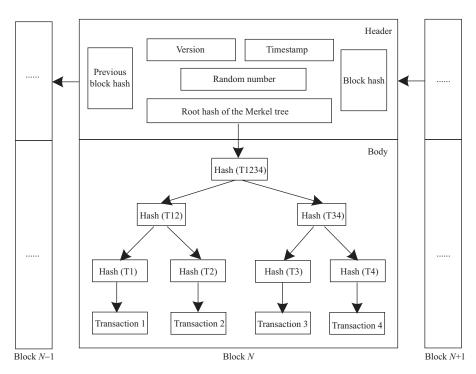


图 2 区块链数据结构

Figure 2 Data structure of the blockchain

时,区块链本身的共识机制会使得矿工开始争夺记账权,取得记账权的矿工广播生成的区块到全网接受验证,如果验证通过,所有节点更新本地节点,全网达成一致.

根据使用范围不同,区块链可以分为公有链、联盟链和私有链.公有链面向全世界任何人,是一个去中心化的系统.所有人都可以读取数据、进行交易、参与共识过程,程序开发者无权干涉用户.联盟链面向联盟中各个组织,每个区块的确认需要联盟各方达成共识.私有链写入权限仅在一个组织手里,数据读取权限受组织规定,是一个弱中心化的系统,但是达成共识时间相对较短,交易迅速,适合特定机构内部使用.

区块链最开始应用于转账交易, 智能合约的加入使得区块链步入 2.0 时代. 智能合约是执行合约条款的计算机交易协议, 本质是运行在区块链上的代码. 智能合约部署在区块链上之后, 每个节点都保存一份副本, 用户通过地址来调用运行合约. 智能合约的执行结果同样保存在区块链上, 可以作为交易的凭证. 代码执行的无歧义性、区块链的去中心性使得智能合约具有公开透明的特点. 智能合约推动经济进入智能经济时代, 人们可以通过设计特定规则的智能合约, 让物与物之间可以直接进行安全、可靠的交易, 促进经济快速增长 [9].

## 2.2 区块链技术研究和应用

虽然区块链技术发展时间较短,但其在性能、安全、隐私等方面都得到很多关注.性能方面, Cui 等 [10] 设计了一种基于压缩有向无环图 (DAG) 的高效、安全的区块链协议 CoDAG, 吞吐量可以达到 比特币的 164 倍,以太坊的 77 倍. Wang 等 [11] 提出的并发多链系统 Monoxide 模型,在测试环境中比比特币网络高出 1000 倍的每秒事务处理量,以及 1000 倍的状态内存容量,有望打破长期困扰区块链性能的 "不可能三角".安全方面, Gervais 等 [12] 引入一个新的定量框架,分析 PoW 共识机制下各

种共识和网络参数对区块链安全和性能的影响,并且为双花攻击和自私挖矿设计了最优的对抗策略. Apostolaki 等 [13] 从单点攻击和网络攻击两个方面提出路由攻击对比特币的影响,并给出了一些短期和长期的解决方法. 隐私方面, Kosba 等 [14] 指出现有智能合约缺乏事务隐私, 因此提出一种分散的智能合约系统 Hawk, 编译器可以为私有合约生成密码学协议, 合约各方使用诸如零知识证明之类的密码学原语与区块链进行交互, 从而不会在区块链上清晰地存储金融交易, 保留交易隐私. Cheng 等 [15] 提出 Ekiden 架构, 将 TEE 可信执行环境与区块链结合, 共识同执行分离, 解决智能合约隐私和性能的问题. 这些工作在性能、安全、隐私等方面进一步提高了区块链技术的可靠性与可用性, 也为区块链技术的应用提供了支撑.

区块链技术由于其去中心化、数据不可篡改性正被应用到许多现实场景中.基于数字货币的属性,金融领域首先引入区块链技术,用于数字票据构建、支付清算、市场预测、电子商务等. 医疗领域,区块链被用来建立安全可信的医疗数据记录 [16],如病人的电子档案. 教育领域,区块链可以作为证书认证系统,构建去中心化的全球知识库,形成知识货币等.基于区块链的存储技术将直接冲击甚至颠覆传统云计算架构,Storj,Siacoin,Filecoin等基于区块链技术的文件存储系统越来越成熟. 区块链还可以与物联网结合,区块链可以为物联网系统安全检测、分布式信任、隐私保护等方面带来新的思路.Wu等 [17] 提出一种新的区块链激励平台 SmartRetro,该平台可以激励和吸引更多的分布式检测器参与到回溯性漏洞检测中,实现自动安全反馈. 业界中国联通联合众多公司和研究机构成立物联网区块链 BOT,用以解决物联网中信息安全问题,提高物联网系统效率. 此外区块链的去中心化为传统网络带来新机遇,通过在区块链上记录网络关键信息,例如自治域号、公钥等,可以实现网络行为可追踪可验证 [18];针对多种分布式网络设备,区块链可以助力其协同工作 [19],构建去中心化可信互联网.

#### 2.3 区块链技术在数字内容领域应用

面对数字内容产业出现的诸多问题,区块链成为解决问题的重要途径.区块链可以进行版权保护,打击约束盗版现象;进行资产信息记录,实现资产的循环流通;进行透明的收入分配,解决创作者被压榨问题. Liu [20] 设计了基于 Hyperledger Fabric 的数字版权管理系统,采用 IPFS 星际文件系统解决区块链存储问题. Cai 等 [21] 为维护电影平台中电子凭证的法律有效性提出了涉及用户、发行商、广告商的多链系统,并提供了系统中链上代码开发的 5 条原则. Zhang [22] 针对数字内容系统中客户端的强交互性提出了共识协议 Dynasty,基于 Dynasty 构造了 D-Chain 区块链应用框架,以二手车交易和不动产交易两个系统证明 D-chain 在吞吐量和延迟两个方面都有较好表现.

虽然已有部分研究开始聚焦于区块链在数字内容领域的应用,但是这些研究都局限于某一层面,而且很多只是简单的功能验证,缺乏从真正的商业层次去论证平台架构以及平台内部新形态,更缺乏从宏观价值链角度理解基于区块链的数字内容平台所带来的深远意义.商业层次的新型数字内容平台设计应当遵循以下 4 项原则: (1) 支持兼顾平台的高响应和去中心化; (2) 支持便捷高效的版权保护; (3) 支持对用户实行公开透明激励; (4) 支持服务商接入构建多业务形态.基于以上原则,本文设计了基于区块链的新型数字内容平台基本模型和价值流转方式.

# 3 基于区块链的数字内容平台基本模型

本节介绍基于区块链的数字内容平台的基本模型,首先介绍数字内容平台中的关键元素,包括消费者、原创者、平台方和监管部门. 然后通过平台价值流转过程——代币在关键元素之间的闭环流转介绍平台运转. 最后介绍平台基础架构和部署架构.

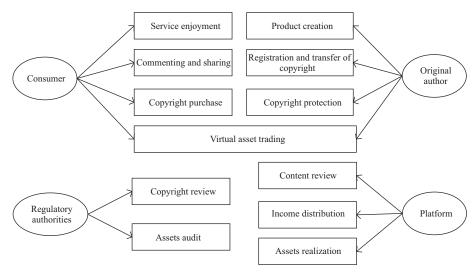


图 3 关键元素及功能

Figure 3 Key elements and functions

# 3.1 关键元素

新型平台包括消费者、原创者、平台方、监管部门 4 类关键元素, 图 3 展示了关键元素及其对应功能,下面对每种元素进行详细的功能描述.

- (1) 消费者: 数字内容平台的主要参与者, 也是数字内容平台的盈利来源. 消费者可以享用数字内容平台中的文学、视频、游戏等服务, 对服务做出评价和分享, 进而形成消费者间的社交互动. 当消费者购买内容产品或者出售游戏道具等虚拟资产时需要借助平台中的统一代币.
- (2) 原创者: 创作网络文学、视频、音乐等产品以及开发游戏的人员,是平台得以稳定健康发展的根本.平台中作品被映射成唯一的哈希值,哈希值和作品相关信息 (如作者 ID、作品标题等)被记录在区块链上,作品借助区块链机制被附加上不可篡改的时间戳,实现了版权登记.发生版权交易时,购买方和出售方以及购买时间和期限等信息也应当被记录到区块链上.当发生侵权行为时,原创者可以将区块链上的版权登记和流转记录作为证据提交,通过对接平台方管理员或监管部门进行维权.
- (3) 平台方: 运营各服务商产品, 为消费者和原创者提供业务支持. 联盟链服务商各方应就准入机制、收入分配方案等以代码形式达成一致. 为维护数字内容平台的良好运行, 平台方可以通过人工智能算法过滤劣质内容, 实现作品内容审核. 对于原创者, 平台方应根据作品带来的经济效应 (例如通过作品的评论、点赞、分享等行为估计) 给予其一定经济奖励, 对于消费者同样可以根据其时间财产 (如观看时长、游戏段位等) 实施激励来增加用户沉浸时间, 增强用户黏性. 平台通过对消费者和原创者的激励交互实现收入重分配. 最后平台方还应提供平台中代币变现接口, 实现虚拟资产和现实资产的流通.
- (4) 监管部门: 为数字内容平台提供保障. 当出现侵权行为时, 监管部门根据提供的证据进行裁决, 同时监管部门也对平台中的资产流动进行审查, 保障平台健康运行.

## 3.2 平台运转

## 3.2.1 平台机制

新型平台相比于传统数字内容平台更加具有安全保障和法律效力, 主要基于以下 3 个机制:

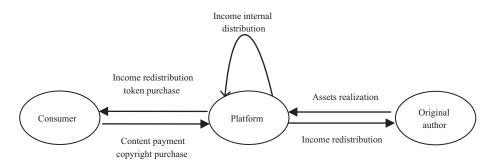


图 4 价值流转过程

Figure 4 The value transfer process

- (1) 信息共享机制. 区块链每个节点通过共识机制维护统一的账本, 用户的行为数据以及产生的价值直接记录在账本上. 联盟链上的每个企业维护一份账本, 可以保证所有企业数据共享, 解决企业因互不信任导致信息无法共享的问题. 不同业务可以采用不同的通道, 通道内数据只对参与该通道的节点可见, 在实现数据共享的同时实现数据保护.
- (2) 版权保护机制. 区块链保证数据的不可篡改性, 原创者登记作品, 区块链上立即增加一条不可篡改的、带有时间戳的交易信息, 版权流转过程也会作为交易记录在区块链上. 区块链上的信息记录可以解决维权中取证难的问题.
- (3) 合约机制. 现实中的合同在具体操作时常常面临合同语句歧义, 强制执行合同代价昂贵等问题. 但平台的某些场景需要合同的强制约束, 例如多家企业如何协同发展, 如何给予消费者和原创者一定收入激励等问题. 区块链上部署智能合约相当于签订了现实中的合同, 智能合约表现为代码形式, 代码的解释是唯一的, 避免自然语言歧义的问题, 而且代码是受系统控制自动执行的, 整个过程对于合约当事人公开透明.

#### 3.2.2 价值流转

价值流转是指伴随用户在平台中的活动, 代币在平台各个关键元素之间进行流转, 进而形成循环、健康的数字内容生态. 价值流转体现了平台运转过程, 价值流转基于下面两个前提.

- (1) 用户群体统一. 联盟链使得多家服务商共存, 用户只需要注册一个账号即可对接生态中的所有服务. 用户群体统一一方面降低平台准入门槛, 用户通过一个账号可以享受丰富服务, 提高了用户留存率; 另一方面平台可以根据用户多样行为, 提供更加符合用户需求的产品.
- (2) 流通资产统一. 平台中流通代币统一, 用途涵盖产品消费、平台收入重分配等活动. 而且游戏道具等虚拟资产可以按照一定方式与代币进行换算, 打破了虚拟资产后续价值流转的僵局, 实现价值流转的闭环回路.

价值流转过程如图 4 所示,原创者通过创作开发数字内容产品获得代币资产,消费者通过付费享受数字内容产品,包括浏览资讯、阅读、听音乐、看视频、玩游戏等.平台方资产交易接口提供现实资产与虚拟资产互换功能,消费者通过接口购买代币用于消费,原创者通过接口变现代币资产.平台方通过对原创者和消费者进行一定的行为激励,实现平台收入的重分配.

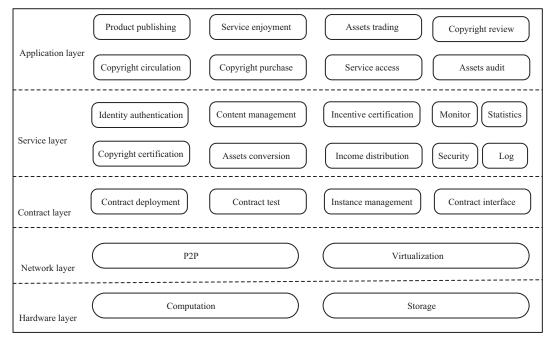


图 5 数字内容平台基础架构

Figure 5 The fundamental architecture of digital content platform

## 3.3 平台架构

#### 3.3.1 基础架构

根据平台的业务流程,基于区块链的数字内容平台基础架构如图 5 所示,分为硬件层、网络层、合约层、服务层、应用层 5 部分.

- (1) 硬件层包括计算和存储两部分, 是平台最底层的硬件资源. 算力是区块链运行的基础, 计算硬件一方面为"挖矿"提供算力支持, 另一方面支持平台业务处理. 存储是指存储平台数据的硬件资源, 由于区块链存储性能有限, 一些重要信息 (如账户信息、交易信息等) 需要存储到区块链上, 其余信息可以采用常见的关系型数据库本地存储.
- (2) 网络层包括 P2P 和虚拟化两部分, P2P 分布式网络用于在节点间传送数据形成分布式账本.虚拟化是指通过网络功能将计算、存储虚拟化,提供虚拟执行环境 (例如以太坊中的 EVM), 为上层服务提供接口.
- (3) 合约层包括智能合约的测试、部署、管理功能,同时提供用于硬件层账本数据存储的接口. 部署的智能合约是平台各方协作的基础,合约涵盖服务商准入、版权保护、收入分配、虚拟资产交易等场景. 智能合约执行过程对当事双方都透明公开.
- (4) 服务层包括支撑应用层多项应用的后台接口. 具体包括身份认证、版权认证、内容管理、资产转换、激励认证、收入分配服务, 以及保障平台运行的监测、统计、日志、安全服务. 其中内容管理包括内容的登记、存储, 以及平台方参与的内容推荐、审核等; 资产转换包括虚拟资产间的交易、虚拟资产同现实资产的转换; 激励认证根据激励机制对原创者和消费者进行激励条件的验证, 从而触发智能合约实现收入分配.
  - (5) 应用层包括面向平台使用者的接口. 用户可以注册登录进入平台, 享受平台中的数字内容服

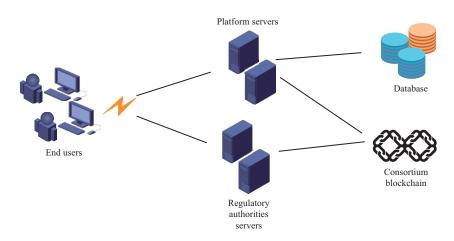


图 6 (网络版彩图) 数字内容平台部署架构

Figure 6 (Color online) The deployment framework of the digital content platform

务,或者作为原创者提供优质作品,进行版权管理.平台方还可以接入新的数字内容业务,丰富数字生态.监管部门可以进行版权审查和资产审计,维护平台运行.

# 3.3.2 部署架构

完全去中心化平台中所有代码应运行在联盟链上,但是区块链本身存储和处理性能有限,这种方式会限制平台性能.为满足兼顾平台高响应和去中心化的原则,新型平台仍需结合传统的客户端服务器架构.但是需要进一步区分核心代码(如版权的登记、资产的转移)和核心数据(如作品信息、用于实行用户激励的作品点赞量等),核心代码和数据的存储转移到区块链中.

本文提出的新型平台部署架构如图 6 所示, 终端用户访问平台方服务器, 平台方服务器完成对用户请求的处理. 平台将重要操作数据记录到联盟链中, 其余非核心数据 (例如用户登录 IP 等) 记录到数据库中. 这样一方面减轻区块链处理负担, 另一方面也加快平台响应速度. 联盟链节点包括各内容产品服务商, 同时为保证平台在其中不作弊, 可以接入第三方监察机构作为平台监管部门, 例如公证处. 区块链本身的共识机制决定各个节点都会保存链上数据, 保证一方难以篡改链上数据.

为保障一定的去中心化, 平台必须为终端用户提供服务接口, 使其可以访问联盟链中涉及自身的数据, 例如用户作品版权信息, 作品点赞量等, 这一接口可以由监察机构的服务器代为运行. 用户若存疑也可进行自测监督, 例如点赞自己作品后去区块链上查询该记录是否出现. 一旦出现纠纷, 监察机构可以直接调取联盟链数据介入调查.

# 4 基于区块链的数字内容平台价值流转方案设计

从图 4 可以看到整个平台中价值流转的路径包括: 消费者购买代币、消费者对内容产品付费、原创者变现代币、平台给予原创者激励和平台对消费者进行激励. 其中前 3 种流转是代币的简单传递行为,不需要方案设计. 后两种属于收入分配问题,平台方需要设计合理的方案激励消费者的产品投入以及原创者的作品创作,这是平台生态能够健康平稳发展的基础.

对于消费者和原创者的激励需要针对二者的行为特征进行,消费者的主要行为特征包括游戏在线时长、视频观看时长、文章评论、游戏通关等,原创者行为特征包括创作时长、作品被评论、作品被点

赞等. 宏观来看, 消费者和原创者的行为特征大体可以分为离散的和连续的行为特征, 因此本文提出一种跨业务的结合离散和连续行为特征的激励机制, 对消费者和原创者给予代币奖励.

首先需要在时间维度上划分时间间隔  $\Delta t$ , 通过特定函数在时间间隔上的积分计算时间激励, 根据事件是否在  $\Delta t$  内发生映射到相应函数上获得事件激励, 结合时间激励和事件激励获得相应代币奖励. 具体步骤如下:

(1) 根据当前用户 u ( $u \in U$ ) 在业务 b ( $b \in B$ ) 上的持续时长  $t_{u,b}$  ( $t_{u,b} \in T$ ) 计算出当前用户所在的映射区间 n:

$$n = |t_{u,b}/\Delta t|. \tag{1}$$

由实际协调平台和用户利益后确定的分配函数  $\mathrm{Time}_b(t)$  ( $\mathrm{Time}_b(t) \in F_{\mathrm{time}}$ ), 计算该业务上的时间 激励:

$$rate\_time_{u,b} = \int_{n\Delta t}^{(n+1)\Delta t} Time_b(t) dt.$$
 (2)

计算用户 u 的总时间激励:

$$rate\_time_u = \sum_{b \in B} rate\_time_{u,b}.$$
 (3)

(2) 根据用户 u 在当前时间段  $\Delta t$  内, 事件 e ( $e \in E$ ) 是否发生及对应的事件 – 激励映射函数  $Event_e(t)$  ( $Event_e(t) \in F_{EVENT}$ , 函数定义域为  $[0, \Delta t]$ ), 计算事件发生对应的事件激励.

首先检测用户 u 在当前时间间隔  $\Delta t$  内是否发生事件 e. 由实际协调平台和用户利益后确定的事件激励映射函数, 计算事件激励:

$$rate\_event_{u,e} = \int_0^{\Delta t} Event_e(t) dt.$$
 (4)

计算总事件激励:

$$rate\_event_u = \sum_{e \in E} rate\_event_{u,e} \times I_i,$$
(5)

其中  $I_i$  取值如下所示:

$$I_i = \begin{cases} 1, & e \text{ 发生,} \\ 0, & e \text{ 未发生.} \end{cases}$$
 (6)

(3) 计算总激励, 并将其映射到代币. 当前  $\Delta t$  时间内的总激励计算如下所示:

$$rate_u = rate\_time_u + rate\_event_u. (7)$$

根据实际协商确定的激励 - 代币映射函数 Reward, (rate), 代币值计算如下所示:

$$Token = Reward_u(rate_u). (8)$$

(4) 当前  $\Delta t$  时间结束后, 回到步骤 1, 重新计算活跃用户的激励.

图 7(a) 展示了时间激励示意图, 图 7(b) 展示了事件激励示意图, 图 7(c) 展示了事件激励和时间激励叠加示意图.

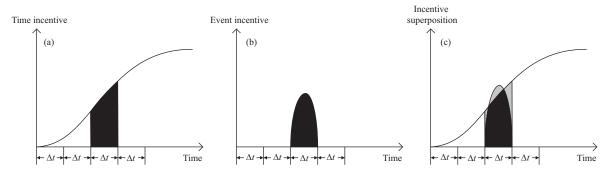


图 7 激励示意图. (a) 时间激励; (b) 事件激励; (c) 时间事件激励叠加

Figure 7 Incentive diagram. (a) Time incentive; (b) event incentive; (c) time incentive and event incentive

# 5 区块链可行性分析

本节对区块链构建数字内容平台的可行性进行分析, 首先以主流公有链以太坊为例, 从交易成本方面阐述公有链不适用于新型平台构建的原因, 然后以主流联盟链 Fabric 为例, 论证联盟链在处理性能方面已经可以支撑新型平台运行.

# 5.1 公有链成本分析

目前主流的公有链是以太坊,本小节以以太坊估算构建新型平台的成本. 以太坊中交易执行的成本主要是交易消耗的 Gas, 节点在上传交易时需要提供 GasPrice,表示节点愿意为每 Gas 支付多少的以太币,节点愿意支付的 GasPrice 越高,交易越会被提前打包. 一笔交易的成本计算方式为 GasPrice × GasUsed.

表 1 是以太坊官方网站<sup>1)</sup> 某天对全网 GasPrice 的统计. 因为 GasPrice 过小会影响交易确认时间, 参考表 1 后本文取 10 Gwei 作为成本计算标准. 2016 年以太坊由于 The Dao 事件发生分叉, 新链中代币为 ETH (Ethereum), 旧链中代币为 ETC (Ethereum classic). 当天以太币与人民币的兑换大约为 1 ETH = 1570 RMB, 1 ETC = 34 RMB.

本文实现简单的版权合约 WorkCopyrights<sup>2)</sup> 用以作品版权登记和流转, 同时根据 ERC20 标准实现代币合约 simpleToken, 记录作品点赞量用以激励原创者 (这里以点赞量记录作为平台和区块链众多激励交互行为的代表). 合约中交互操作单次的 GasUsed 和成本如图 8(a) 所示.

根据 QuestMobile 《2019 中国移动互联网春季报告》, 视频网站爱奇艺日活跃用户量在一亿左右, 音乐网站 QQ 音乐日活跃用户量在 700 万左右, 本文取 5000 万作为新型平台的日活量进行估算. 版权合约和代币合约部署只需一次, 带来的交易成本可以忽略不计, 主要的交易成本集中在用户和区块链频繁的交互行为中. 按照每日版权登记 10 万次, 版权流转 1 百万次, 转账 1 千万次, 点赞记录 1 亿次进行估算, 各项操作的总成本如图 8(b) 所示. 以 ETH 估算每日交易总成本约为 7915 万, 以 ETC 估算日交易总成本约为 172 万.

本小节只列举了基本交互方式产生的费用,实际中平台业务逻辑更复杂,即使公有链代币与人民币兑换比率再低,合约交易成本也是平台运营者难以忍受的.因此采用公有链作为底层区块链在经济成本上是不可行的.联盟链本身没有交易费用,作为新型平台底层区块链的实现更加合适.但联盟链

<sup>1)</sup> 以太坊官方网站: https://ethgasstation.info.

<sup>2)</sup> 代码见 https://github.com/zhou-code/valuechain.

表 1	某天以太坊全网	GasPrice(	Gwei'	) 统计

Table 1 GasPrice statistics of the whole network of Ethereum someday

GasPrice	[0, 1]	(1, 4]	(4, 20]	(20, 50]	> 50
Proportion (%)	9	29	44	16	2

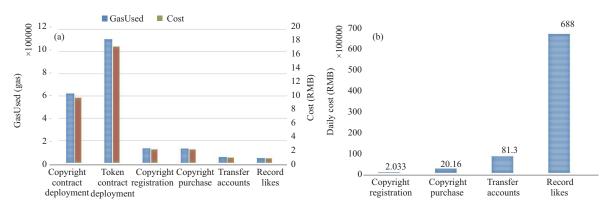


图 8 (网络版彩图) 交互操作的 GasUsed、成本以及总成本 (ETH). (a) 各项交互操作的 GasUsed、成本; (b) 各项交互操作日成本

Figure 8 (Color online) The GasUsed, cost and total cost of interactions with blockchain (ETH). (a) The GasUsed and cost of interactions; (b) daily cost of interactions

性能是否能满足新型平台智能合约的需求仍需实验验证,下面对联盟链合约处理性能进行分析.

#### 5.2 联盟链性能分析

目前主流的联盟链是超级账本 Hyperledger 项目中的 Fabric, 本小节对 Fabric 运行数字内容平台 合约的性能进行分析.

Fabric 中的智能合约称为链码, 运行在不同的通道中. 不同通道之间彼此独立, 通道建立时需要指定可以参与该通道交易的节点, 通道中的交易、数据只对通道内的节点可见, 实现了不同业务场景下业务隔离. Fabric 中节点参与不同的业务, 加入不同的通道, 形成面向业务的多条通道, 也就是联盟链中的"多链". Fabric 由有限节点组成, 节点在交易执行中可以承担多种角色, 例如证书分发节点、排序节点、背书节点等. 交易确认的整个流程为: 客户端提交交易提案到背书节点, 收到背书节点的提案答复并验证后, 封装提案为交易提交给排序节点, 排序节点将交易广播给所有节点, 所有节点更新状态数据库, 同时打包成区块追加到区块链上.

Hyperledger Caliper 是超级账本项目中测试区块链平台性能的框架. Caliper 提供多种测试方式以及对多种参数的监控,用户需要编写待测试的智能合约、网络配置以及测试流 (测试函数和测试数据流等). 本小节利用 Caliper 对 Fabric 中合约性能进行测试. 与 5.1 小节一致,待测试合约包括代币流转合约和版权合约. 代币流转合约包括新建账户、转账、存取款等功能,版权合约包括登记、查询、转让等功能. 合约功能确定后,测试不同网络配置下的合约处理性能.

实验运行在 Ubuntu16.04 的系统中, CPU 型号是 4-coreIntel(R) Xeon(R) CPU E3-1220 v5 @ 3.00 GHz, 内存 32 G. 测试的 Fabric 版本为 v1.4.0, Caliper 的版本为 v0.2.0. 采用的测试模式是 fixed-backlog, unfinished\_per\_client 参数值为 0, 目的是希望得到平台在不积压交易且交易都能成功执行时所能支持的最大 TPS, 即联盟链在稳定运行时交易的 TPS.

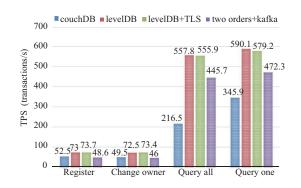


图 9 (网络版彩图) 多种条件下版权合约各交易 TPS Figure 9 (Color online) Transaction TPS of the copyright contract under various conditions

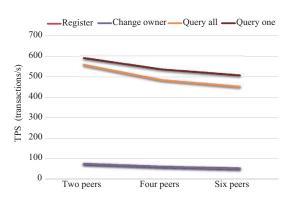


图 10 (网络版彩图) 不同 peer 节点数下的版权合约 交易 TPS

Figure 10 (Color online) Transaction TPS of the copyright contract with different numbers of peer nodes

图 9 的网络拓扑是两个证书分发节点;一个排序节点 orderer, 排序机制为 solo 模式; 两个组织,每个组织各有一个对等节点 peer. 图 9 展示了分别使用 levelDB 和 couchDB 数据库, 以及在使用 levelDB 数据库下启用 TLS 安全传输协议的版权合约各交易平均 TPS 情况. 整体来看, 登记、转让交易由于涉及到对区块链的写操作, TPS 在 70 笔/s 左右. 版权查询交易只涉及对区块链的读操作, TPS 较高,在 600 笔/s 左右,且查询单笔交易和多笔交易的性能变化不大. 此外图 9 显示 Fabric 中数据存储使用 levelDB 比 couchDB 性能更好,而且在服务器端采用 TLS 后,对各个交易的性能影响都不大. 因此后面的测试中我们都采用 levelDB 数据库以及不开启 TLS 通信.

不同的排序机制以及平台联盟链中节点数的数量都会影响交易的确认速度. 因此接下来主要测试不同节点数和排序机制下的 Fabric 合约处理性能. Fabric v1.4.0 中支持两种共识算法,一种是单节点共识 solo,另一种是分布式消息队列 kafka. kafka 由排序节点、kafka 集群和 zookeeper 集群组成,可以提供交易排序服务并具备额外的崩溃容错能力. 排序节点相互之间不通信,只与 kafka 集群通信, kafka 集群与 zookeeper 相互连接. 图 9 也展示了 kafka 机制下的 TPS. 其中 kafka 模式下包含两个排序节点,4 个 kafka 节点,3 个 zookeeper 节点,而 solo 模式(图 9 中标注 levelDB 的数据)下只有一个排序节点,其余节点配置二者相同. 从图中可以看到由于节点增多, kafka 模式下合约执行性能下降较为明显,但是仍能保持写操作在 50 笔/s 左右,读操作在 450 笔/s 左右. 以 5.1 小节日活量估算,版权登记 TPS 需求为 1 笔/s,版权转让 TPS 需求为 10 笔/s,版权查询 TPS 需求为 100 笔/s,对比得到 Fabric 性能完全可以满足实际中版权登记、转让、查询需求.

对等节点需要对交易进行背书,因此对等节点数越多,一笔交易需要等待背书的节点数越多,交易 TPS 越低. 图 10 展示了对等节点 peer 数量对交易处理性能的影响,从中可以看到随着 peer 数量增多 TPS 下降,但下降幅度逐渐变小.表 2 是不同 peer 节点数下交易平均时延统计,可以看到查询交易 (读操作) 时延基本没有太大变化,登记、转让交易 (写操作) 时延上升,但是上升幅度逐渐变小.这些表明实际中联盟链节点数增加对 Fabric 合约处理性能不会产生很大影响.

同时我们也测试了代币流转合约. 合约包括创建账户、存款、取款、转账、余额查询等功能, 其中前 4 个是对区块链的写操作, 延时较大, TPS 较低, 余额查询属于读操作, 其延时较低, TPS 较高. 表 3 直接以读写操作形式展示了合约性能测试的结果, 写操作的 TPS 在 65 笔/s 左右, 读操作 TPS 在 630 笔/s 左右. 根据 5.1 小节的日活量估算, 转账 (写操作) 的 TPS 需求在 100 笔/s, 余额查询 (读查

#### 表 2 不同 peer 节点数下版权合约交易平均时延 (单位: 秒)

Table 2 Average transaction latency of the copyright contract with different numbers of peer nodes (Unit: s)

Function	Two peers	Four peers	Six peers
Register	0.48	0.58	0.64
Change owner	0.46	0.59	0.66
Query one	0.05	0.05	0.07
Query all	0.05	0.06	0.07

#### 表 3 代币流转合约性能测试结果

Table 3 Performance of the value transfer contract

Function	Max latency (s)	Min latency (s)	Avg latency (s)	Throughput (TPS)
Write	1.05	0.13	0.54	65.5
Read	0.23	0.01	0.04	631.3

询) TPS 需求在 1000 笔/s, 对比得到 Fabric 能满足实际中代币流转的基本需求.

从两组合约的多组测试中可以得出,决定 Fabric 中合约交易 TPS 的关键因素是交易的类型,即读操作密集型还是写操作密集型,此外是合约功能的复杂性. 在本文的实验环境下,多次变换网络配置,读操作交易 TPS 仍能稳定在 550 笔/s 左右,写操作交易 TPS 在 55 笔/s 左右,与平台合约需求相比,Fabric 可以满足基本的平台合约需求. 考虑到实验环境采用一台机器模拟所有节点,实际应用中多台机器可以使合约交易处理性能进一步提高. 而且对于像记录作品点赞这类频繁写操作,实际中可以采用一些折衷方法,例如累积到不同数量进行记录. 在实际部署环境中,随着机器性能提升、网络环境优化、交易排序优化等,联盟链性能也会进一步提高,因此联盟链适合而且可以支撑构建新型平台.

# 6 总结展望

本文针对数字内容产业发展中出现的企业协调、信息共享、版权保护等问题,结合区块链的去中心化、数据不可篡改等特性,提出以基于区块链的数字内容平台重塑数字内容价值链的方案.首先分析了新型数字内容平台中关键元素、价值流转、平台基础架构和部署架构,然后设计平台价值流转激励机制.最后从成本角度,阐述联盟链相比于公有链更适合构建新型平台的原因;从性能角度,论证联盟链的性能足以支撑新型平台的运行.区块链作为数字生态建设的底层设计可以解决其发展中的诸多问题,真正实现健康可信的数字生态.但是区块链本身在资源消耗、计算效率、安全保证等方面仍存在问题,而且区块链加数字内容这种结合方式的共识机制以及网络通信等也需进一步优化.下一步需要针对这些问题展开研究,实现真正高效可信的数字内容生态价值链.

#### 参考文献 -

- $1\quad \text{Porter M E, Millar V E. How information gives you competitive advantage. Harvard Business Rev, 1985, 63: 149–160}$
- 2 Gulati R, Singh H. The architecture of cooperation: managing coordination costs and appropriation concerns in strategic alliances. Administrative Sci Q, 1998, 43: 781–814
- 3 Lamport L, Shostak R, Pease M. The Byzantine generals problem. ACM Trans Program Lang Syst, 1982, 4: 382-401
- 4 Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. 2009. https://bitcoin.org/bitcoin.pdf
- 5 Sasson E B, Chiesa A, Garman C, et al. Zerocash: decentralized anonymous payments from bitcoin. In: Proceedings of IEEE Symposium on Security and Privacy, San Jose, 2014. 459–474

- 6 van Saberhagen N. CryptoNote v 2.0, 2013
- 7 Wood G. Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 2014, 151: 1–32
- 8 Shao Q F, Jin C Q, Zhang Z, et al. Blockchain: architecture and research progress. Chin J Comput, 2018, 41: 969–988 [邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展. 计算机学报. 2018, 41: 969–988]
- 9 Xu K, Yao W B. Cyber intelligent economy and blockchain. J Guangdong Univ Tech, 2018, 35: 1–9 [徐恪, 姚文兵. 赛博智能经济与区块链. 广东工业大学学报, 2018, 35: 1–9]
- 10 Cui L, Yang S, Chen Z, et al. An efficient and compacted DAG-based blockchain protocol for industrial Internet of Things. IEEE Trans Ind Inf, 2020, 16: 4134–4145
- 11 Wang J, Wang H. Monoxide: scale out blockchains with asynchronous consensus zones. In: Proceedings of USENIX Symposium on Networked Systems Design and Implementation (NSDI), Boston, 2019. 95–112
- 12 Gervais A, Karame G O, Wüst K, et al. On the security and performance of proof of work blockchains. In: Proceedings of the ACM Conference on Computer and Communications Security, Vienna, 2016. 3–16
- 13 Apostolaki M, Zohar A, Vanbever L. Hijacking bitcoin: routing attacks on cryptocurrencies. In: Proceedings of IEEE Symposium on Security and Privacy, San Jose, 2017. 375–392
- 14 Kosba A, Miller A, Shi E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts.
  In: Proceedings of IEEE Symposium on Security and Privacy, San Jose, 2016. 839–858
- 15 Cheng R, Zhang F, Kos J, et al. Ekiden: a platform for confidentiality-preserving, trustworthy, and performant smart contracts. In: Proceedings of IEEE Symposium on Security and Privacy, San Francisco, 2019. 185–200
- 16 Xue T F, Fu Q C, Wang C, et al. A medical data sharing model via blockchain. Acta Autom Sin, 2017, 43: 1555–1562 [薛腾飞, 傅群超, 王枞, 等. 基于区块链的医疗数据共享模型研究. 自动化学报, 2017, 43: 1555–1562]
- 17 Wu B, Li Q, Xu K, et al. SmartRetro: blockchain-based incentives for distributed IoT retrospective detection.
  In: Proceedings of IEEE International Conference on Mobile Ad Hoc and Sensor Systems, Chengdu, 2018. 308–316
- 18 Xu K, Xu S S, Li Q. Blockchain-based decentralized trusted Internet infrastructure. Commun China Comput Federation, 2020, 16: 29–34 [徐恪, 徐松松, 李琦. 基于区块链的去中心化可信互联网基础设施. 中国计算机学会通讯, 2020, 16: 29–34]
- 19 Wu B, Xu K, Li Q, et al. Toward blockchain-powered trusted collaborative services for edge-centric networks. IEEE Network, 2020, 34: 30–36
- 20 Liu X. Design and implementation of digital copyright management system based on blockchain. Dissertation for Master's Degree. Dalian: Dalian University of Technology, 2019 [刘学. 基于区块链的数字版权管理系统的设计与实现. 硕士学位论文. 大连: 大连理工大学, 2019]
- 21 Cai W D, Yu L, Wang R, et al. Blockchain application development techniques. J Softw, 2017, 28: 1474–1487 [蔡维德, 郁莲, 王荣, 等. 基于区块链的应用系统开发方法研究, 软件学报, 2017, 28: 1474–1487]
- Zhang G R. Research on blockchain technology based on digital content protection. Dissertation for Master's Degree. Shenzhen: University of Chinese Academy of Sciences, 2018 [张耕瑞. 基于数字内容保护的区块链技术研究. 硕士学位论文. 深圳: 中国科学院大学, 2018]

# Digital content ecological value chain based on block chain

Guangmeng ZHOU<sup>1</sup>, Su YAO<sup>2\*</sup>, Lin LI<sup>3</sup>, Xin LIU<sup>3</sup> & Ke XU<sup>1,2,4</sup>

- 1. Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China;
- 2. Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing 100084, China:
- 3. Miqu Culture Technology Co., Ltd., China Mobile Communications Group Co., Ltd., Beijing 100032, China;
- 4. Peng Cheng Laboratory (PCL), Shenzhen 518052, China
- \* Corresponding author. E-mail: yaosu@tsinghua.edu.cn

Abstract With the popularity of the Internet and mobile terminals, the digital content industry is becoming the main economic growth point of the cultural industry. Starting from the copyright issues, quality issues and industry barriers faced by the digital content industry, this paper analyzes the advantages and significance of the blockchain technology in the construction of the digital content. Then reinventing the digital ecological value chain through a blockchain-based digital content platform is proposed, and the key elements, the value transfer method and the system architecture of the new platform are analyzed. Then the basic program design of the value transfer process of the platform is given. Finally, experimental analysis proves that the consortium blockchain is suitable and can support the construction of the platform from the perspective of cost and performance.

Keywords digital content, value chain, blockchain, value transfer, consortium blockchain



Guangmeng ZHOU was born in 1997. He is currently pursuing his Ph.D. degree in School of Computer Science and Technology at Tsinghua University, China. His main research interests include collaborative learning, network security and blockchain.



Su YAO received his Ph.D. degree from National Engineering Laboratory for Next Generation Internet Interconnection Devices, Beijing Jiaotong University. Since 2017, he has undertaken postdoctoral research in Tsinghua University. He joined Beijing National Research Center for Information Science and Technology in 2020 and severed as a research assistant. His research interests include future network architecture, network security, and space and block-chain.



Xin LIU is the Chairman of Migu Culture Technology Co., Ltd. He has more than 20 years of experience in the mobile communications and Internet industries. He directs the business of Migu Culture Technology Co., Ltd, including platform development, big data, product design, and 5G.



Ke XU was born in 1974. He received his Ph.D. from Department of Computer Science and Technology of Tsinghua University, Beijing, China, where he serves as a full professor. He has published more than 100 technical papers and holds 20 patents in the research areas of next generation Internet, P2P systems, Internet of Things (IoT), and network virtualization and optimization.