Web3.0下的区块链相关技术进展

斯雪明[1,2],潘恒[2*],刘建美[2],祝卫华[2],姚中原[2]

1. 上海交通大学区块链研究中心,上海 200030
2. 中原工学院前沿信息技术研究院,郑州 450007

摘要 区块链是Web3.0构建可信互联、价值互联的关键技术。作为一种新的去中心化基础设施,区块链自身技术也在不断发展。结合Web3.0背景,介绍了区块链的去中心化身份、智能合约、激励机制和隐私保护等相关技术进展和问题,以助力实现基于Web3.0的数据安全共享、业务流通、用户权益保障,从而达到更加公平的价值分配和价值流动。

关键词 Web3.0;去中心化身份;智能合约安全;激励机制;隐私保护

随着区块链、人工智能、无线边缘计算等技术的快速融合发展,下一代互联网Web3.0的技术研究越来越多[1]。2007年,T.O′Reilly提出Web2.0的概念[2],对比以门户网站提供静态网页浏览服务为主的Web1.0,Web2.0强调以网络为平台的连接和为用户提供互动等多种增值服务。2014年,以太坊(Ethereum,ETH)的联合创始人Gavin Wood称:现有技术已经无法适用于未来社会和技术的互动,称Web3.0为"后斯诺登网络"(post-Snowden),描绘了一个零信任(zero-trust)下的去中心化、安全、自治的网络[3]。

截至目前,Web3.0作为下一代互联网,学术及企业界对其概念仍然没有统一的认识和定义。有研究者强调其"智能化""语义化""个性化"特征[4];有研究者关注其"去中心化""安全""可信"的特征[5-6];也有研究者注重其基于数字资产化和资产数字化的价值互联特性[7];还有研究者强调其可验证性(verifiable),认为Web3.0的核心特征为应用程序的关键计算是可验证的[8]。无论对Web3.0的理解有何异同,区块链是Web3.0的核心支撑技术为普遍共识。

1 Web3.0与区块链

目前的Web2.0互联网,无论是采用传统的客户服务器架构还是云计算模式,都还是集中化处理

收稿日期:2023-06-16;修回日期:2023-07-20

基金项目:河南省重大公益项目(201300210300);河南省网络密码技术重点实验室开放基金项目(LNCT2022-A12);嵩山实验室预研项目(YYJC032022021)

作者简介:斯雪明,教授,研究方向为区块链,电子信箱:9770@zut.edu.cn;潘恒(通信作者),教授,研究方向为区块链,电子信箱:panheng@zut.edu.cn

引用格式:斯雪明, 潘恒, 刘建美, 等. Web3.0下的区块链相关技术进展[J]. 科技导报, 2023, 41(15): 36-45; doi: 10.3981/j.issn.1000-7857.2023.15.004

的分布式网络。虽然Web2.0极好地实现了用户和网络、网络与网络、用户与用户之间的连接、互动,也极大地改变了人们的生产生活方式,但随着网络应用的深入以及新一代信息技术的快速发展,现有Web2.0网络面临着诸如安全性、隐私性、透明性、真实性等多个方面的技术挑战,同时还存在着权力或利益严重聚集于第三方平台的问题[9]。因此下一代互联网——Web3.0的"去中心化"(decentralized)特点被普遍认同[5-6]。

区块链是利用块链式数据结构来验证和存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式来保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构和计算范式。

与传统分布式网络相比,区块链更多关注节点平等、不互信、存在有拜占庭节点下的异步网络以及节点如何自治、平等、安全地实现网络服务,更加接近于实际网络情况。来源于比特币的区块链技术天生强调节点平等和去中心化。通过大多数节点的共识是利用密码算法,基于智能合约的同步、严格执行及分布式账本的不可篡改记录等组合,区块链可以实现与分布式网络不同的去中心化和社会资源去中介化,解决Web2.0由于中心化所出现的信任危机、数据及隐私泄露、用户自主性差等问题,实现基于Web3.0的数据安全共享、业务流通、用户权益保障,并进一步通过区块链的加密货币或通证(token)等技术,实现更加公平的价值分配和价值流动[10-11],如图1所示。

图1　基于区块链的Web3.0环境

一个基于区块链的更加自主、安全、开放、公平的Web3.0互联网环境,首先要建立用户的去中心化身份,鼓励用户积极参与,需要保障传输及处理数据的安全和隐私,还要构建安全的去中心化应用程序(Dapp)。

Web3.0的去中心化事务处理方式是解决中心平台垄断和利益分配失衡问题的一种尝试,利用区块链的可信协作、分布式执行、数据保护、资产转移等能力进一步整合信息流、业务流和价值流,以更加标准化、更加简洁的链上智能合约来代替现有互联网应用服务,消除对中心机构的依赖。目前,区块链技术研究活跃,所涉及的共识、可扩展性、跨链、分片等技术进展很快。本文从Web3.0去中心化特征的角度介绍去中心化身份、智能合约、激励机制、隐私保护4个方面的相关进展。

2　Web3.0与去中心化身份

在现有网络环境下,用户身份和个人识别信息PII(personal identifying information)由一个中心化第三方管理,用户缺少对自己数字身份和身份信息所有权的管理,导致容易出现个人隐私泄露等问题[12]。基于去中心化理念的Web3.0的发展,首先需要实现适应去中心化环境的身份管理,同时需要改进现有身份认证中对个人信息的过度泄露,加强用户对自我身份信息的管控权。因此,去中心化身份(decentralized identity,DID)作为一种新的身份认证架构和方法,将区块链的分布式账本、隐私计算等技术融入身份治理当中。

与传统身份管理不同的是,DID分离了用户身份数据的所有权和使用权。为了保障用户身份的所有权和管理权,提出了自我主权身份(self-sovereign identity)的概念和方法,强调在身份信息使用过程中用户可选择性泄露部分敏感信息,实现用户身份信息的有效管理,避免身份隐私过度泄露。

去中心化身份系统的构建方法有多种,比较通用的模型是使用代表实体的身份标识符和与之关联的属性声明凭证。2021年8月万维网联盟(W3C)发布了《去中心化身份1.0版:核心结构、数

据模型和表征》标准[8],是目前使用较为广泛的去中心化身份方法。

如图2所示,W3C标准中的DID由基础层和应用层组成。基础层主要由DID标识符(DID URL)和DID文档(DID Document)组成。DID标识符是标识用户全网唯一的数字身份的特殊字符串,DID Document是一个JSON-LD格式的数据,包含DID URL、时间戳、JSON-LD签名、加密参数、加密协议、服务端点等6部分。应用层主要是可验证凭证(verifiable credentials,VC)[10],VC提供了一种表征用户实体具有的某种属性的规范。一般情况下,DID的实体向其他实体出示自己的VC全文,以此来证明自己某些属性的真实性。但是在一些特殊情况下,出于对隐私信息的保护,并不需要出示完整的VC内容,用户可以出示可验证表达(verifiable presentation,VP)来选择性地披露信息,VP是VC持有者向验证者表明自己身份的数据。

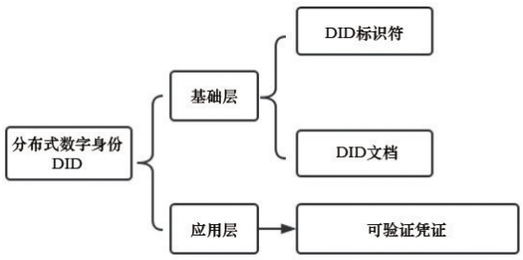

图2 分布式数字身份DID的组成模型

虽然以W3C为代表的去中心化身份,通过VC生成VP的方式,实现了在身份认证过程中选择性出示有限的PII信息,最大程度保障了用户的隐私信息,但现有的去中心化身份仍然存在不少问题,针对这些问题,去中心化身份系统研究有很多新进展。文献[13]提出了一种名为PDID(password-authenticated decentralized identities)的基于口令身份验证的去中心化身份系统,允许用户在全局命名空间中注册自己的用户名和密码对,并将其用作通用凭证,此外还可以实现向任何服务器认证用户身份的同时,不向服务器泄露任何密码信息。针对当前的加密方法将去中心化的标识符与公钥绑定,可能会引起身份窃取攻击和单个实体存在多个标识符的问题,文献[14]提出了一种基于新的加密原语——无限单向哈希链的去中心化身份模型,用户只需要一次注册,就可将用户的公钥嵌入到无限单向哈希链中,解决一个实体多个标识符的问题。文献[15]提出了具有可审计性和保密性的DID认证协议,可审计性保证系统能够检测恶意认证事件,保密性防止敌手将认证事件链接到对应的用户和服务提供商。此外,现有的DID文档高速缓存方案中的侧通道可能引起隐私问题,文献[16]提出了一种新的DID解析设计,称为Oblivira(不经意DID解析),Oblivira是一个占用空间小的安全解析代理,可以强制通用解析器在不知道请求内容的情况下解析请求。文献[17]中提出一个CanDID系统,授权最终用户管理自己的凭证,除签发证书外,CanDID的身份识别系统还可以抵抗Sybil攻击,并且允许用户将其密钥存储在CanDID委员会中,实现密钥丢失时的恢复。

3 智能合约预言机与智能合约安全

Web3.0的目标仍然是通过去中心化应用程序为用户提供网络服务。在区块链中,这些去中心化的应用程序由智能合约实现。由于智能合约部署在链上、运行在链上,智能合约的安全和链下数据的调用一直是难点。

3.1 智能合约预言机

区块链系统依靠其共识机制和密码学的相关技术,使得链上的数据难以被篡改,能够保障链上数据的真实性和可靠性,但是对于链下数据缺乏可信保障机制。智能合约预言机(Oracle)是智能合约进行链上链下数据交互的主要技术,用以保证链下数据的完整性和真实性[18]。预言机为链下数据提供了一种可信保障机制,能够实现链下数据的可信上链。基于这种特性,预言机可应用于任何需要与链下进行数据交互的Dapp。区块链预言机本质上是区块链与链下数据调用和访问的可信媒介,是一种为区块链智能合约提供可信链下数据的工具[19]。

2017年,基于以太坊的第一个去中心化预言机Chain Link被提出[20],通过在链下采用多数据源

及多预言机节点的方式获取源头数据,提高源头数据采集的可信性。2019年,国内去中心化预言机Dos Network白皮书发布[21],从预言机节点选择的角度出发,基于可验证随机函数实现去中心化网络中工作节点的随机选取,并通过门限签名技术实现数据验证。预言机工作角色主要由链上用户智能合约即区块链智能合约、链上预言机智能合约及链下的外部数据源3个部分组成。

目前智能合约预言机也有较多研究进展。文献[22]提出了一种基于门限聚合签名的区块链预言机数据传输模型,该模型将签名与数据聚合到一个预言机上,与链上智能合约进行单次交互,减少区块链存储空间开销和通信负载。文献[18]研究了基于分布式预言机的链下数据源可信评估激励技术,提出了基于分布式预言机的可信数据上链技术。针对提高车联网中的用户身份安全可信问题,文献[23]提出了一种基于区块链预言机的车联网可信身份注册方案。该方案使用智能合约、分布式预言机、机器学习算法等技术构建预测模型,可以保证车联网用户在注册阶段的可信。文献[24]提出了一种基于预言机和零知识证明的区块链数据上链方案,该方案能够提高数据源的可信性并增强数据的隐私安全性。

3.2　智能合约安全

智能合约是存在于区块链上以代码形式定义的承诺,一经部署,很难修改。基于区块链的Web3.0应用,最终是以智能合约的形式实现的,而且可能会涉及一些代币交易,因此保证智能合约安全非常重要。

3.2.1　智能合约漏洞分类

作为应用最为广泛的主流区块链系统,以太坊上的智能合约漏洞最为典型和丰富。表1以以太坊为例,总结了智能合约编写、编译、区块链交易驱动3个阶段共14种类型的漏洞。

在智能合约的编写阶段,高级语言是主要的工具。在开发者利用高级语言对智能合约进行编写时,安全漏洞主要由高级语言设计模型本身和开发者编程能力参差不齐的问题导致。在编译完成之后,虚拟机是智能合约字节码的执行器。在以太坊环境下,虚拟机层面上智能合约的安全威胁存在于智能合约字节设计规范和运行机制本身的缺陷等。智能合约在区块链平台运行时,由于区块链本身的特性,也会产生如时间戳和事务顺序依赖等安全风险。

表1　常见智能合约漏洞分类

智能合约运行阶段	常见安全漏洞	备注
编写阶段	整数溢出 拒绝服务漏洞 可重入漏洞 权限控制漏洞 异常处理漏洞 类型混乱漏洞 未知函数调用漏洞 以太冻结漏洞	与高级语言设计模式、用户编写等有关
编译阶段	以太丢失漏洞 短地址攻击 调用栈溢出漏洞 Tx.Origin漏洞	与智能合约字节执行器有关
区块链交易驱动阶段	时间戳和事务顺序依赖 区块参数依赖	与区块链本身的特性有关

3.2.2　智能合约漏洞检测

智能合约具有不可更改性,一旦部署在区块链上就不能进行修改,只能进行升级,但是升级智能合约又是困难和繁琐的,所以在部署智能合约上链之前,对其进行漏洞检测是非常重要的。

文献[25]将已有的智能合约漏洞检测技术分为基于模糊测试、基于污点分析、基于符号执行、基于形式化验证、基于机器学习等若干种,前3种是最常用的检测技术,其中模糊测试因高效多产的漏洞发觉能力而应用广泛,缺点包括漏洞定位复杂、测试用例生成低效等[26-27];污点分析是检测合约鲁棒性和漏洞挖掘的关键技术,其缺陷包括信息流分析不全面造成的过污染和欠污染,以及在污染传播的过程中内存存储信息的处理等问题[28];符号执行通过探索程序中所有可执行路径,发现安全漏洞,但存在路径约束求解难和路径爆炸等问题[29]。综上所述,智能合约漏洞检测技术已经取得了巨大进步,但由于智能合约出现的时间比较短,发展迅速,还没有形成专门漏洞库。因此,仍然需要持续研究以确保智能合约的安全。

4 Web3.0与激励机制

Web3.0的去中心化特征支持用户在无中心化第三方机构的情况下进行沟通和交易,可以让用户拥有更大的数据控制权,实现用户创造数据、拥有数据、控制数据和基于区块链协议的自动公平利益分配。由于Web3.0下系统的自治和用户的平等性,要保证Web3.0的正常运转,必须设计适当的激励机制。

现阶段激励机制主要通过使用代币或者积分的形式提高用户参与的积极性。比特币作为最经典的区块链系统,采用代币的方式激励矿工挖矿。同时在一些其他的区块链系统中,也使用了代币奖励的方式激励用户参与。文献[30]根据用户的私有数据估值进行代币奖励,激励用户提供私有数据参与联邦学习训练。文献[31]鼓励用户将自己的信息分享给其他用户来赚取积分,用积分获取更多信息促进信息共享。文献[32]采用资源包作为奖励,激励用户不断参与训练来获取积分,使用积分去兑换资源包。区块链技术采用通证来激励节点不断参与工作,其工作方式与上述的激励方式类似,可以在不同的场景下将上述方式应用到区块链中。奖励能够刺激用户工作的积极性,但也存在奖励分配公平性的问题,因此在进行最终的奖励之前,还需要根据不同实体的贡献大小进行等级评定,根据评定结果进行奖励分配。

文献[33]在移动人群感知的场景下,设计了一种基于数据质量的分配方法,以鼓励客户提交高质量的数据。文献[34]基于众包的室内导航系统场景设计了一种根据用户提供的数据权重为标准的贡献量测量方法。文献[32]在联邦学习中,提出了一种基于夏普利值(Shapley value)的贡献指数,通过本地数据集、机器学习算法和测试集等多个因素来评估实体的实际贡献指数。文献[35]提出一种基于等级驱动拍卖的新型激励机制,根据用户资源的大小进行计算,资源越丰富、层次越高、其贡献量相应也会越多。Web3.0中需要不同实体之间协同工作,而公平公正地计算贡献量是保证实体不断工作的前提。

5 Web3.0与隐私保护

Web3.0与Web2.0的重要区别在对数据安全和隐私的保护上。Web3.0以用户为中心,赋予了用户数据自主权,使用户可以在交易和数据流通中真正获益。因此,如何保护交易与数据共享过程中的用户隐私就成为了需要研究的课题。目前,基于区块链的隐私保护方案的研究热点包括零知识证明、同态加密、差分隐私、可信执行环境、联邦学习等技术,如表2所示。

5.1 零知识证明

零知识证明(zero knowledge of proof,ZKP)技术是一种重要的隐私保护技术,由S.Goldwasser等在20世纪80年代初提出[36],是指证明者在不向验证者提供任何有用的信息的情况下,使验证者相信某个论断是正确的。ZKP技术因其良好的可靠性、完备性和零知识性,有望被广泛应用于区块链等潜在的Web3.0场景,保证数据的有效性的同时不泄露敏感信息。

交互式零知识证明常被应用于区块链的隐私保护、区块链的扩容及区块链跨链等方面。文献[37]中提出了ZeroCoin强匿名性加密货币,实现了

表2 区块链主要隐私保护方法

隐私保护方法	定义
零知识证明	一种交互式的证明协议,其中一个证明者可以在不泄露关于某个陈述任何信息的情况下,向另一个验证者证明该陈述的正确性
同态加密	一种加密技术,允许在密文上执行计算并得到加密后的结果
差分隐私	一种高效的隐私保护技术,通过在数据中加入随机噪声的方式进行数据保护
可信执行环境	一种在硬件层面提供隐私保护的解决方案
联邦学习	机器学习领域中的一种隐私保护计算方案

内部不可链接性,防止用户交易地址被暴露。文献[38]在区块链上提出了一个基于零知识证明的联邦学习(ZKP-FL)方案,对于局部数据的计算和局部模型参数的聚合都采用了零知识证明,目的是在不需要局部数据明文的情况下可验证计算过程。文献[39]中提出的ZK-Rollup方案是一种针对区块链的Lay2层扩容方案,链下进行复杂计算和零知识证明的生成,链上进行证明的校验并存储部分数据保证数据可用性;文献[40]中提出的Coda项目使用递归组合的简洁非交互式证明技术,使验证时间缩短至200 ms,适用于轻量级客户端。文献[41]将零知识证明技术应用在跨链领域,提出ZK-Router协议(zk-based cross-chain router protocol),协议是在目标链合约内无信任的验证,利用零知识证明认证源链的共识机制,引申出跨链基础设施ZK-Router,具有无信任依赖、链上轻计算、通用、低延迟、无资产抵押的显著优势。

5.2　同态加密

同态加密(homomorphic encryption,HE)是一种对密文进行运算等效于对明文进行相应运算的技术。经过多年的研究,成熟的同态加密算法已有很多,大致可分为部分同态加密和全同态加密,如ElGamal算法(乘法同态性)、Paillier算法(加法同态性)和BFV方案(全同态性)。文献[42]结合Paillier算法和ElGamal算法提出了同态加密算法Pail-Gamal,不仅支持第三方监管所有密文,还支持将密文的合法性检测放在链下进行,减少链上交易数据。文献[43]将区块链技术和BFV全同态加密算法相结合,把加密后的选票存储在区块链上,保证了选票的不可篡改性。可见,同态加密技术不仅能够提高交易的可监管性和高效性,还能抵抗量子计算攻击,非常适用于未来Web3.0的大规模交易场景。

在数据共享方面,监督方管理成员私钥量过大,极易出现合谋攻击。为此,文献[44]提出了一种使用单密钥同态加密构造多密钥同态加密的方案,减短密钥尺寸的同时提高了加密运算效率。文献[45]将同态加密与群签名技术、密钥共享算法结合,使群管理员和监管机构分别生成仅群成员可见的部分私钥,解决了单一群管理员权力过大的问题。

除了用户交易和数据共享方面,同态加密技术还运用于机器学习和多方安全计算等领域。文献[46]提出了一种基于部分同态加密和联邦学习的多方隐私保护机器学习框架PFMLP,使学习方只能通过同态加密来传输加密的梯度。文献[47]利用同态加密、秘密共享和零知识证明构建了一个可公开验证的安全MPC协议,该协议由链上计算和链下预处理2个阶段组成,增强了隐私机密性。

5.3　差分隐私

在Web3.0中,数据的去中心化和开放性往往会导致数据的隐私泄露。差分隐私(differential privacy)是一种通过在数据中添加噪声来保护用户隐私的技术。将差分隐私技术应用到Web3.0中,可以更好地保护用户的隐私,提高用户的信任度。

Web3.0的智能交互离不开机器学习,然而在机器学习中模型训练过程可能会暴露用户的隐私。许多研究者开始将差分隐私的保护方案与机器学习结合,文献[48]提出了一种新的差分隐私框架,该框架在客户端上传数据之前添加人工噪声,有效地保护了客户端数据的隐私。此外,文献[49]关注分布式机器学习场景,将随机噪声扰动应用在学习者对分布式数据库的差分梯度查询响应中,开发了分布式隐私数据机器学习的差分隐私梯度下降算法。

安全多方计算(secure multi-party computation,SMPC)是一个密码学原语,常被用于分布式隐私数据学习的场景,该技术能够使Web3.0中的各个节点之间在不暴露隐私的情况下,互联合作创造更多的价值。Dwork等[50]首次指出SMPC可以很好地与差分隐私结合,例如通过安全计算和加性噪声可以很容易地实现差分隐私求和。Zhou等[51]提出一种SMPC协议,该协议分别对链上计算与链下预处理2个阶段提供隐私保护,并将其作为共识算法的一部分。

在Web3.0中,社交网络分析可以帮助分析和优化去中心化应用的用户体验和社区建设。但是目前一般的社交网络分析中仍存在隐私泄露的问题,利用差分隐私能够有效保护数据安全。Qin等[52]提出的方案基于分组和迭代的方法,方案中迭代分组的方法适当地保留了社交网络中的结构信

息,每轮迭代中添加的噪声也能够提供一定的隐私保护。Sun等[53]提出了一种新的去中心化差分隐私机制,该机制要求每个参与者不仅要考虑自己的隐私,还要考虑其邻居的隐私,在此基础上计算整个网络的最小噪声尺度。在此框架中,差分隐私起到了至关重要的作用。

5.4 可信执行环境

可信执行环境(trusted execution environment,TEE),是一种由硬件和软件相结合实现的安全计算环境,可以提供硬件加密、安全存储空间和隔离机制等功能,其目的是在不受信任的主机操作系统中提供安全的执行条件,从而保护敏感数据和代码不受攻击和不被泄露[54]。区块链系统是公开透明的,其中智能合约的执行不受保护,用户隐私信息容易泄露。因此,将TEE与区块链技术结合,可提高区块链应用的安全性,避免智能合约执行环境被攻击和操纵[55]。文献[56]提出一种基于SGX的轻量Fabric链码可信执行环境构建方法及E-Fabric架构,将智能合约的执行部署在可信执行环境中,搭建支持原生Go语言的可信镜像和容器,为链码创建可信执行环境并通过远程认证协议验证链码是否可信。然而,如果TEE中的内存访问模式存在泄露问题,智能合约的执行仍然可能被破坏。为此,文献[57]提出了一个新的通用框架SECAUCTEE,允许智能合约在基于Intel SGX的TEE上运行,并通过实现不可知执行和端到端加密服务,避免了内存访问模式泄露问题。由于区块链中存储了大量的敏感数据且数据量在不断增加,因此需要更加高效的内存管理技术来实现更高效和更安全的数据管理。文献[58]提出了一种轻量化的代码迁移方案,可以有效降低系统中内存换页的开销,避免内存利用率不足的问题。

5.5 联邦学习

联邦学习(federated learning)是一种分布式机器学习技术,在不暴露用户原始数据的情况下,对模型进行训练和优化。联邦学习可以将模型训练过程分布在多个设备或节点上,通过加密和数据分割技术来保护用户数据的隐私和安全。Web3.0中,联邦学习可以作为数据隐私保护和智能决策的核心技术,为用户提供更加开放和自由的数字经济和数字社会体验。

在Web3.0中,数据的价值往往需要通过数据共享来体现,如在医疗保健领域和智能制造领域中都涉及到大量敏感数据的共享,因此数据共享必须具备足够的安全性和隐私保护机制。关于数据共享过程中隐私保护的研究,有许多成果:文献[59]提出利用FedXGBoost算法、区块链技术和智能合约的解决方案,解决了联邦学习数据共享中的可扩展性、隐私保护和可靠性等问题,有效应对了Web3.0中数据共享的隐私保护挑战;文献[60]提出了一个基于区块链的ESB-FL框架,该框架使用一种非交互式的指定解密函数加密方案和区块链结合,在确保隐私保护的同时保持较高的效率、准确性和安全性;文献[61]提出将联邦学习与Hyperledger Fabric企业级区块链进行集成来提高联邦学习客户端之间的可见性和安全性,通过跟踪客户端的更新以保护全局模型免受恶意更新的影响;文献[62]等使用区块链作为联邦学习的底层分布式框架,并且采用了同态加密和Multi-Krum技术来实现密码文本级的模型聚合和过滤,保证了本地模型的可验证性;文献[63]提出使用联邦学习和区块链技术保护电子健康记录隐私,该方案基于CNN的安全分类模型,对可用数据集进行正常和异常用户的分类;文献[64]提出了一种基于公有链和私有链的隐私保护可搜索加密方案,采用智能合约进行二次验证,保证数据隐私和访问控制验证的正确性;文献[65]基于联邦学习和差分隐私技术构建了一个用于阿尔茨海默病早期检测的异步隐私保护聚合框架,该框架允许多个医疗机构参与方对更新后的梯度进行本地加密,通过将加密后的梯度在云端聚合,确保模型数据在聚合过程中的保密性。

6 结论

区块链技术可以为Web3.0提供包括去中心化、用户自主、通证化数字资产、隐私保护、安全可信等多种特征的技术基础支撑。未来技术愈发呈现综合融通的趋势,Web3.0将会是最新通信、计

算、存储技术的综合体。而区块链技术本身就是密码、对等网络、分布式共识、程序设计等各种技术的综合。除了区块链技术本身可以作为Web3.0的底层支撑之外,区块链各种技术的巧妙组合方式也可以作为发展Web3.0技术的借鉴。Web3.0的发展与区块链技术的发展也将相互促进,Web3.0为区块链技术提供更多的应用场景和需求,而区块链技术的发展也为下一代互联网的创新提供保证。

参考文献(References)

[1] Lin Y J, Gao Z P, Du H Y, et al. A unified blockchain-semantic framework for wireless edge intelligence enabled Web 3.0[J]. arXiv Preprint, 2022: 2210.15130.

[2] O′Reilly T. What is Web 2.0: Design patterns and business models for the next generation of software[J]. International Journal of Digital Economic, 2007, 65(1): 17-37.

[3] Wood G. Dapps: what Web 3.0 looks like, Apr 2014[EB/OL]. [2023-05-20]. http://gavwood.com/dappsweb3.html.

[4] Hendler J. Web 3.0: The dawn of semantic search[J]. Computer, 2010, 43(1): 77-80.

[5] Zarrin J, Wen Phang H, Babu Saheer L, et al. Blockchain for decentralization of internet: Prospects, trends, and challenges[J]. Cluster Computing, 2021, 24(4): 2841-2866.

[6] Alabdulwahhab F A. Web 3.0: The decentralized web blockchain networks and protocol innovation[C]//2018 1st International Conference on Computer Applications & Information Security (ICCAIS). Piscataway, NJ: IEEE, 2018: 1-4.

[7] Avrilionis D, Hardjono T. From trade-only to zero-value NFTs: The asset proxy NFT paradigm in Web3[J]. arXiv Preprint, 2022: 2205.04899.

[8] Liu Z, Xiang Y, Shi J, et al. Make Web 3.0 connected[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 19(5): 2965-2981.

[9] Weyl E G, Ohlhaver P, Buterin V. Decentralized society: Finding Web3′s soul[J]. Available at SSRN 4105763, 2022.

[10] Web3.0前瞻研究报告(2022年)[R/OL]. [2023-06-11]. http://www.trustedblockchain.cn/#/result/result/resultDetail/2cc84f5277fe4e2689f42c947c18ebdd/0.

[11] Qin R, Ding W W, Li J J, et al. Web3-based decentralized autonomous organizations and operations: Architectures, models, and mechanisms[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 53(4): 2073-2082.

[12] Gilani K, Bertin E, Hatin J, et al. A survey on blockchain-based identity management and decentralized privacy for personal data[C]//2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). Piscataway, NJ: IEEE, 2020: 97-101.

[13] Szalachowski P. Password-authenticated decentralized identities[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 4801-4810.

[14] Park C S, Nam H M. A new approach to constructing decentralized identifier for secure and flexible key rotation [J]. IEEE Internet of Things Journal, 2021, 9(13): 10610-10624.

[15] Alangot B, Szalachowski P, Dinh T T A, et al. Decentralized identity authentication with auditability and privacy [J]. Algorithms, 2022, 16(4): doi: 10.3390/a16010004.

[16] Huh S, Shim M, Lee J, et al. Did we miss anything? Towards privacy-preserving decentralized ID architecture [J]. IEEE Transactions on Dependable and Secure Computing, 2023(1): 1-18.

[17] Maram D, Malvai H, Zhang F, et al. Candid: Can-do decentralized identity with legacy compatibility, sybil-resistance, and accountability[C]//2021 IEEE Symposium on Security and Privacy (SP). Piscataway, NJ: IEEE, 2021: 1348-1366.

[18] 田潇, 杨国忠, 钟晓, 等. 基于门限签名的预言机数据源评估激励机制研究[J]. 电子技术与软件工程, 2022(5): 248-252.

[19] 毕丹阳, 张钰雯, 毕雅晴. 基于预言机的可信数据上链技术[J]. 信息通信技术与政策, 2021, 47(9): 79-84.

[20] ChainLink white paper[EB/OL]. [2021-05-10]. https://link.sm artcontract.com/whitepaper.

[21] Dos network white paper [EB/OL]. [2021-05-10]. https://www.dos.network.

[22] 刘炜, 郭灵贝, 夏玉洁, 等. 基于门限聚合签名的区块链预言机数据传输模型[J]. 郑州大学学报(理学版), 2023, 55(4): 23-29.

[23] 张晴晴, 田潇, 田锦, 等. 基于区块链预言机的车联网可信身份方案研究[J]. 信息安全研究, 2023, 9(2): 120-126.

[24] 管驾浠, 马兆丰, 叶可可, 等. 基于预言机和零知识证明的区块链数据上链方案[J]. 信息安全与通信保密, 2022(10): 25-37.

[25] 董伟良, 刘哲, 刘逵, 等. 智能合约漏洞检测技术综述[EB/OL]. [2023-06-11]. http://www.jos.org.cn/1000-982-5/6810.htm.

[26] Kolluri A, Nikolic I, Sergey I, et al. Exploiting the laws of order in smart contracts[C]//Proceedings of the 28th ACM SIGSOFT International Symposium on Software

Testing and Analysis. New York: Association for Computing Machinery, 2019: 363-373.
[27] Zhang Q, Wang Y, Li J, et al. Ethploit: From fuzzing to efficient exploit generation against smart contracts[C]// 2020 IEEE 27th International Conference on Software Analysis, Evolution and Reengineering (SANER). Piscataway, NJ: IEEE, 2020: 116-126.
[28] Schwartz E J, Avgerinos T, Brumley D. All you ever wanted to know about dynamic taint analysis and forward symbolic execution (but might have been afraid to ask)[C]//2010 IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE, 2010: 317-331.
[29] Coward P D. Symbolic execution systems: A review[J]. Software Engineering Journal, 1988, 3(6): 229-239.
[30] Hu R, Gong Y. Trading data for learning: Incentive mechanism for on-device federated learning[C]//GLOBECOM 2020-2020 IEEE Global Communications Conference. Piscataway, NJ: IEEE, 2020: 1-6.
[31] Lyu L, Yu J, Nandakumar K, et al. Towards fair and privacy-preserving federated deep models[J]. IEEE Transactions on Parallel and Distributed Systems, 2020, 31 (11): 2524-2541.
[32] Song T, Tong Y, Wei S. Profit allocation for federated learning[C]//2019 IEEE International Conference on Big Data (Big Data). Piscataway, NJ: IEEE, 2019: 2577-2586.
[33] Yan X, Ng W W Y, Zeng B, et al. P2 SIM: Privacy-preserving and source-reliable incentive mechanism for mobile crowdsensing[J]. IEEE Internet of Things Journal, 2022, 9(24): 25424-25437.
[34] Xie L, Luan T H, Su Z, et al. A game-theoretical approach for secure crowdsourcing-based indoor navigation system with reputation mechanism[J]. IEEE Internet of Things Journal, 2021, 9(7): 5524-5536.
[35] Liang X, Yan Z, Kantola R. GAIMMO: A grade-driven auction-based incentive mechanism with multiple objectives for crowdsourcing managed by blockchain[J]. IEEE Internet of Things Journal, 2022, 9(18): 17488-17502.
[36] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof-systems[J]. SIAM Journal on Computing, 1989, 18(1): 186-208.
[37] Miers I, Garman C, Green M, et al. Zerocoin: Anonymous distributed E-Cash from Bitcoin[C]//IEEE. 2013 IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE, 2013: 397-411.
[38] Xing Z B, Zhang Z J, Li M, et al. Zero-knowledge proof-based practical federated learning on blockchain[J]. arXiv Preprint, 2023: 2304.05354.
[39] Gluchowski A. Zk rollup: Scaling with zero-knowledge proofs[EB/OL]. [2023-06-11]. https://pandax-statics.oss-cn-shenzhen. aliyuncs. com/statics/1221233526992813.pdf.
[40] Bonneau J, Meckler I, Rao V, et al. Coda: Decentralized cryptocurrency at scale[J]. Cryptology ePrint Archive, 2020. https: //eprint.iacr.org/2020/352.
[41] Chang X, Luo X, Xu G C, et al. ZkRouter: 无信任、通用跨链基础设施[EB/OL]. [2023-05-24]. https://drive.google.com/file/d/1lijlXhSE0jayn2PoR6ZHgsuAdHrrg36_/view.
[42] 杨敏, 徐长通, 夏喆, 等. 一种高效且可监管的隐私交易方案[J]. 武汉大学学报(理学版), 2023, 69(1): 39-50.
[43] 杨亚涛, 刘德莉, 刘培鹤, 等. BFV-Blockchainvoting: 支持BFV全同态加密的区块链电子投票系统[J]. 通信学报, 2022, 43(9): 100-111.
[44] 李文卿, 马锐, 张文涛. 基于共用密钥的高效多密钥同态加密方案研究[J]. 计算机工程与科学, 2023, 45(2): 252-260.
[45] 张学旺, 张豪, 姚亚宁, 等. 基于群签名和同态加密的联盟链隐私保护方案[J]. 信息网络安全, 2023, 23(3): 56-61.
[46] Fang H, Qian Q. Privacy preserving machine learning with homomorphic encryption and federated learning[EB/OL]. [2023-06-11]. http://dx.doi.org/10.3390/fi13040094. doi:10.3390/fi13040094.
[47] Zhou J, Feng Y, Wang Z, et al. Using secure multi-party computation to protect privacy on a permissioned blockchain[J]. Sensors, 2021, 21(4): 1540.
[48] Wei K, Li J, Ding M, et al. Federated learning with differential privacy: Algorithms and performance analysis [J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 3454-3469.
[49] Wu N, Farokhi F, Smith D, et al. The value of collaboration in convex machine learning with differential privacy [C]//2020 IEEE Symposium on Security and Privacy (SP). Piscataway, NJ: IEEE, 2020: 304-317.
[50] Dwork C, Kenthapadi K, McSherry F, et al. Our data, ourselves: Privacy via distributed noise generation[C]// Advances in Cryptology-EUROCRYPT 2006: 24th Annual International Conference on the Theory and Applications of Cryptographic Technique. Berlin Heidelberg: Springer, 2006: 486-503.
[51] Zhou J, Feng Y, Wang Z, et al. Using secure multi-party computation to protect privacy on a permissioned blockchain[J]. Sensors, 2021, 21(4): 1540.
[52] Qin Z, Yu T, Yang Y, et al. Generating synthetic decentralized social graphs with local differential privacy[C]// Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. NewYork: Association for Computing Machinery, 2017: 425-438.
[53] Sun H, Xiao X, Khalil I, et al. Analyzing subgraph statis-

tics from extended local views with decentralized differential privacy[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: Association for Computing Machinery, 2019: 703-717.
[54] Sabt M, Achemlal M, Bouabdallah A. Trusted execution environment: What it is, and what it is not[C]//2015 IEEE Trustcom/BigDataSE/Ispa. Piscataway, NJ: IEEE, 2015, 1: 57-64.
[55] Lind J, Eyal I, Kelbert F, et al. Teechain: Scalable blockchain payments using trusted execution environments[J]. arXiv Preprint, 2017: 1707.05454, 2017.
[56] KELEKET GOMA Christy Junior Yannick, 易文哲, 王鹃. 一种基于SGX的轻量Fabric链码可信执行环境构建方法[J]. 信息网络安全, 2022, 22(7): 73-83.
[57] Desai H, Kantarcioglu M. SECAUCTEE: Securing auction smart contracts using trusted execution environments [C]//2021 IEEE International Conference on Blockchain (Blockchain). Piscataway, NJ: IEEE, 2021: 448-455.
[58] 李明煜, 夏虞斌, 陈海波. 面向SGX2代新型可信执行环境的内存优化系统[J]. 软件学报, 2022, 33(6): 2012-2029.
[59] Zhou Z, Tian Y, Xiong J, et al. Blockchain-enabled secure and trusted federated data sharing in IIoT[J]. IEEE Transactions on Industrial Informatics, 2023, 19(5): 6669-6681.
[60] Chen B, Zeng H, Xiang T, et al. ESB-FL: Efficient and secure blockchain-based federated learning with fair payment[J]. IEEE Transactions on Big Data, 2022, doi: 10.1109/TBDATA.2022.3177170.
[61] Mothukuri V, Parizi R M, Pouriyeh S, et al. FabricFL: Blockchain-in-the-Loop federated learning for trusted decentralized systems[J]. IEEE Systems Journal, 2022, 16(3): 3711-3722.
[62] Wang N Y, Yang W T, Wang X D, et al. A blockchain based privacy-preserving federated learning scheme for Internet of vehicles[EB/OL]. [2023-06-11]. https://www.sciencedirect.com/science/article/pii/S235286482200011-34.
[63] Alzubi J A, Alzubi O A, Singh A, et al. Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning[J]. IEEE Transactions on Industrial Informatics, 2022, 19 (1): 1080-1087.
[64] Du R Z, Ma C X, Li M Y. Privacy-preserving searchable encryption scheme based on public and private blockchains[J]. Tsinghua Science and Technology, 2022, 28(1): 13-26.
[65] Li J C, Meng Y, Ma L C, et al. A federated learning based privacy-preserving smart healthcare system[J]. IEEE Transactions on Industrial Informatics, 2022, 18 (3): 2021-2031.

Progress of Blockchain related Technologies in the Web 3.0

SI Xueming[1,2], PAN Heng[2*], LIU Jianmei[2], ZHU Weihua[2], YAO Zhongyuan[2]

1. Blockchain Research Center, Shanghai Jiao Tong University, Shanghai 200030, China
2. Frontier Information Technology Research Institute, Zhongyuan University of Technology, Zhengzhou 450007, China

Abstract Blockchain is the key technology for Web 3.0 to build trusted interconnections and value interconnections. As a new decentralized infrastructure, the technology of blockchain is also constantly evolving. Combined with the background of Web 3.0, the technological progress and existing problems of blockchain are introduced in this paper, such as decentralized identity, smart contract, incentive mechanism, and privacy protection. They help to realize the technologies in Web 3.0, such as the data security sharing, business circulation and rights guarantee of users, so as to achieve the goal of more fair distribution and flow of the value.

Keywords Web 3.0; decentralized identity; smart contract security; incentive mechanism; privacy protection

（责任编辑　王微）