区块链技术下的数字身份研究——现状与挑战

邹琳，贾时雨，陈瑾，兰秋军

（湖南大学工商管理学院，湖南省长沙市，410082）

摘要：区块链技术作为继大数据、云计算、人工智能后一项新兴技术，打破了中心化管理的传统思路，从而实现去中心、去信任、防篡改的交易执行与数据存储。基于区块链技术的数字身份研究涉及身份授予、管理与验证过程，本文从当前基于区块链的数字身份研究现状角度出发，对传统方式与区块链技术下的身份管理进行了综述，身份认证方式从简单到复杂，其发展过程体现了认证需求的不断更新与信息技术的日益进步，将区块链技术应用于数字身份领域，进一步提升身份信息的安全可靠存储能力，为身份认证提供数据保障，基于此进一步提出区块链技术发展所面临的挑战与未来研究展望。

关键词：区块链；数字身份；身份管理；研究进展

中图分类号： C93　　**文献标识码：**A

0 引言

伴随着新一轮的数字化浪潮，数字化应用全方位向大众生活逐步渗透，在此过程中大量商业潜能被随之开发。作为数字化应用的先决条件，数字身份成为用户获取互联网服务的必备标识。信息化以及“互联网+”时代下，个人信息被赋予了商业价值，数字身份的内涵从“身份”本身扩展为一种“资产”，发挥其蕴含的“数字资产”商业价值。2009 年中本聪一篇关于比特币的论文《Bitcoin: A peer-to-peer electronic cash system》[1]成为区块链技术发展的开端。2020 年 4 月 20 日，我国发改委首次将区块链技术作为新技术基础设施纳入国家“新基建”范围，其去中心化、可追踪、防篡改等技术特性使其在“新基建”中可以作为价值传递媒介。作为一种去中心化大规模协同应用技术，区块链可广泛应用于数字货币、物流、医疗、供应链管理、供应链金融等多领域场景，目前最成功应用案例为比特币，该数字货币以点对点形式实现完全去中心化运行，依靠算力开发新币，并在全球范围内流通。

区块链技术在运行模式方面具备一定优势，但尚未形成完善的去中心化数字身份基础设施成为阻碍其大规模落地应用的原因之一。数字身份是连接虚拟世界与物理世界的桥梁，为实现去中心化区块链技术的大规模落地应用，将区块链技术与现实业务场景融合，应首先建立去中心化数字身份体系。数字身份作为当前互联网应用发展中一项重要环节，已有业界与学界开展了相应研究，提出了数字身份管理中关于隐私保护、密钥管理、身份更新与认证等问题的解决方案。在业界，2016 年 8 月，元界作为去中心化公有区块链项目成立，用户可通过身份账本建立身份与资产、身份与身份间联系，从而构建数字信用，将商业服务区块链化。腾讯云也致力于打造分层与跨链的高可扩展性区块链平台，其身份链提供了跨链身份注册、查询与验证功能。

数字身份已经应用于网络世界的各个领域，在网络安全保障中发挥着重要作用，本文将区块链技术与数字身份研究进展进行总结，提出现阶段发展存在的问题与挑战，并对未来技术发展加以展望。

1 数字身份概述

1.1 数字身份概念

身份伴随着每个个体的一生，它可以代表个体在个人、社会、国家层面所扮演的角色，可以包含性别、年龄、职务、国籍等属性，通过身份实现对不同个体的识别与区分。国际标准化组织将身份定义为“与实体相关的属性集”（ISO / IEC 24760-1）。通常在线下的物理世界，该身份由国家赋予其公民，但目前全球仍存在大量如难民以及极落后地区的个体无法获取公民身份。在法律层面，身份体现为法定范围内一个人权利与义务的总和[2]，伴随互联网的发展，线上虚拟世界与线下物理世界实现平行存在，数字身份将真实物理世界身份信息浓缩为数字标识码，在物理世界与虚拟世界间进行关联，身处于物理世界与虚拟世界的个体便同时具有了线下与线上的物理身份与数字身份。狭义的数字身份即个体物理身份在网络世界的映射，并以一组特定的数据进行表示。从广义角度，不仅个体拥有物理与数字身份，企业、机构以及产品、固定资产等组织与物品也可拥有其相应的身份标识，从而更好地开展网络贸易活动。M. S. Ferdous 等人[3]以数学模型的形式将数字身份进行了形式化的描述，定义了数字身份中的实体即在物理或逻辑意义上具有独特存在的物理或逻辑对象，实体集以 E 表示，实体存在或运行的环境可看做应用程序域或名称域，以 CONTEXT 表示环境集。存在于环境中的个体均具有各自可测量的属性，其属性值用于在环境中对实体进行标识，在环境 c∈CONTEXT 中，以 Ac 表示属性集，AVc 表示属性值，进一步可将属性分为标识符、部分标识符以及空标识符。

数字身份的发展经历了中心化身份、联盟身份、以用户为中心的身份以及自我主权身份阶段，逐步由中心化向去中心化模式发展，将数字身份基础设施部署于分布式环境实现分布式管理将是未来数字身份发展的一大趋势。

1.2 数字身份管理

现阶段，我们所使用的数字身份为中心化管理模式，由服务提供商向用户提供身份注册与管理服务，包括身份账号与应用一对一登录模式以及账号与应用一对多授权登录模式，如图 1、图 2 所示。数字身份管理整个流程涉及身份的注册、证明、验证、授权以及身份失效后的注销过程，证明过程为数字身份属性信息的真实性提供证据，验证阶段确认操作者确为该数字身份的拥有者，授权即为该数字身份拥有者授予该身份下的操作权限，通常此三项操作在每次用户获取网络服务前循环进行。

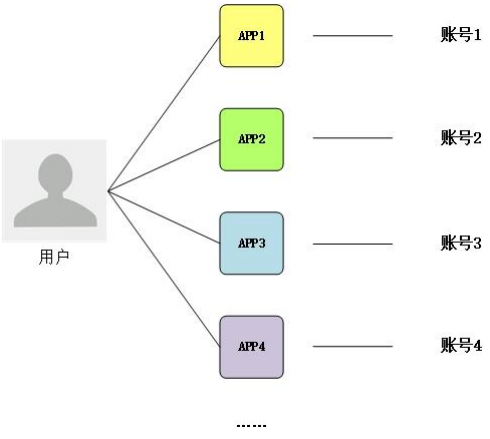

图 1　数字身份一对一登录模式

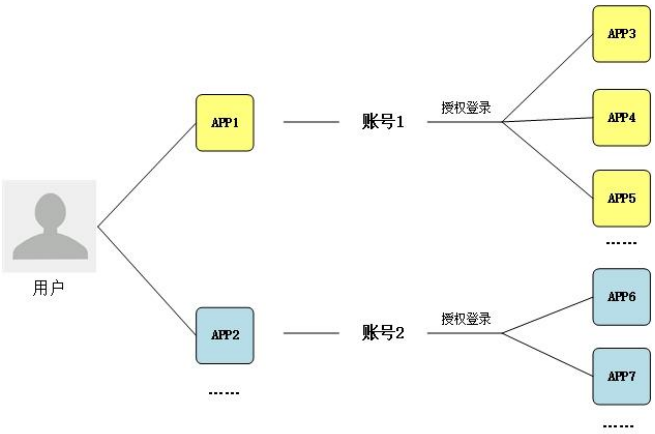

图 2　数字身份一对多授权登录模式

不同应用模式所呈现的数字身份管理具有不同特征，在中心化模式下，由第三方服务提供商授予用户身份，该身份有效范围限于提供者本身以及与该提供者建立信任关系的信任域内，此过程虽然用户可避免繁杂的身份信息管理，减轻操作负担，但反之用户丧失了对数字身份的掌控权，数据隐私难以得到保障。去中心化数字身份被认为是未来区块链技术应用落地的前提之一，以自我主权身份（SSI）为代表，用户可自行管理身份属性信息，该属性信息由认证方提供真实性认证同时附加认证方背书签名，用户数字身份中的不同属性信息可由不同认证方签名，同一属性信息也可由多个认证方签名，形式如图 3 所示，签名过程均为该属性信息的真实性提供保障。在数字身份使用阶段，依据隐私暴露最小化原则使用户向服务提供商提供满足身份认证需求的最少信息，服务提供商通过一方或多方对该身份的签名判断用户是否通过该认证，此方式打破了中心化身份模式下的信任域边界，使该数字身份具有“通用性”，免去用户管理多重身份账号的不便之处。

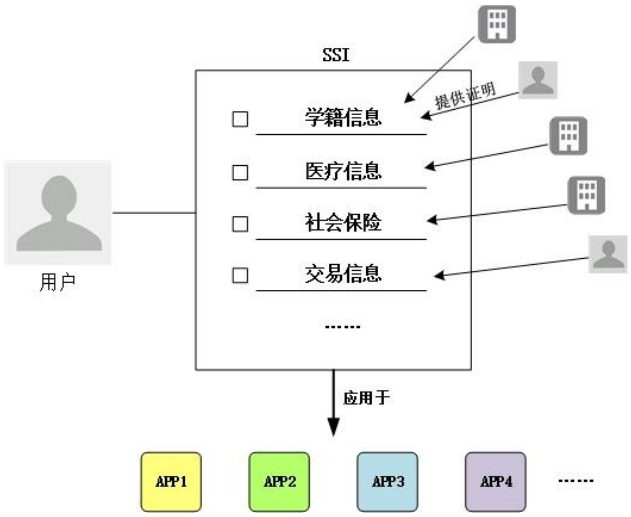

图 3　自我主权身份

1.3　数字身份特征

一个优秀的数字身份管理系统应具备以下几方面的特征：

1）安全性，用户数据可安全存储于该系统中，抵抗黑客攻击，保障用户信息在未经授权情况下不被共享或盗用。

2）灵活性，用户可通过多种设备接入该系统，无论本地或云端均可实现身份的获取与使用，同时用户可掌控其数据，规定数据使用范围、时间等。

3）可扩展，能够随业务变化提供相应技术支持，对新业务需求及时做出相应调整，满足动态变化的实际需求。

4）敏捷性，响应速度快，提供优质的用户体验。

5）隐私保护，提供隐私数据保护方案，告知用户数据使用情况，保障用户知情权，并提供隐私数据使用方式选择权。

6）可恢复，在面对人为破坏或自然灾害造成的服务中断情况，能够实现快速的故障恢复，使系统具备高鲁棒性。

在数字身份管理系统设计过程中应从管理者与用户角度充分考虑可操作性，在安全、效率、便捷性等可能造成设计需求矛盾的方面进行总体协调。

2 区块链与数字身份

2.1 数字身份管理问题

在现阶段中心化数字身份管理以及未来向去中心化身份转型的过程中，依旧面临着众多的问题与挑战，隐私保护是用户首要关注的问题，现阶段中心化模式下用户如何确定身份管理方具备数据安全存储与加密能力，并保证不将用户个人信息用于商业用途，以及暴露于网络世界的用户数据被哪些机构所收集、共享，用户对此并不具备核实能力，用户通常也不具备对自身身份进行加密所需的技术技能。其次，统一标准的基础设施建设尚不完善，用户身份信息分散存储于各个服务提供商处，一方面造成了存储资源的浪费，另外也不利于信息的互联互通，信息孤岛现象严重。最后，未形成全网下的信任体系，无法打破现存的信任域屏障，用户数字身份在多服务场景下不具备通用性，增加了用户对多重身份账户进行管理的精力支出。由于不具备全网通用性，用户需在多个服务提供商处使用各自的独立身份，该身份由中心化企业分散管理，身份的授予、撤销不受用户控制，用户是该身份的主体但不是其所有者，从而使用户丧失了原本属于自身身份的控制权。

2.2 区块链技术优势

区块链是一种按时间顺序对数据区块进行排列，以链式结构存储数据区块的数据结构，以密码学为基础保障数据的不可篡改与伪造，通过共识协议为节点建立信任从而形成的一种去中心化的数据库技术，意图构建一个更加有序、安全、稳定的新世界[4]。区块链并非一项单一技术，而是多种技术的融合，按分层架构模式可将各技术分为六层：数据层、网络层、共识层、激励层、合约层与应用层，如图 4 所示，各层执行不同任务同时相互配合，共同实现区块链现去中心化数据管理。数据层通过哈希函数、非对称加密、时间戳等技术实现相关数据的存储，保障账户安全。网络层中的 P2P 结构体现了区块链技术去中心化特点，利用传播与验证机制实现信息传递。共识层通过共识算法确保全网节点对数据一致性达成共识，激励层主要体现在公有链中，使更多正义节点自愿参与记账过程，记账节点数量的扩大同时也对整条链的安全性增加了保障。合约层与应用层均对不同应用场景提供个性化支持，实现了可编程区块链技术要求。

图 4 区块链技术架构图

区块链技术中体现的优势总结为以下几点：

1）去中心化：相较于现阶段采用的集中式管理模式，区块链中每个网络节点按区块链技术规则进行自我管理，该规则在区块链上公开透明[5]，因此在网络层面实现了系统的自治，各业务功能的实现不依赖于某个单一机构或个体，而是群体平等合作的结果，使该去中心化网络在实际运行过程中具有较好的稳健性。

2）开放性：根据区块链类型的不同，公有链、私有链、联盟链具有不同的开放性程度，依据使用场景的不同，区块链在不同范围内公开，该范围内的节点可自行加入网络并可获得该链完整的数据拷贝。

3）去信任：传统信用背书场景的可靠性建立在对背书节点的信任基础之上，受主观因素影响较大，随整个社会网络中背书节点的增加，其节点管理难度，对可靠性的判断难度均会增加，安全性随之受到影响。与之相反，区块链网络下随节点数量的增大，由算法与既定规则保障的链上操作天然地实现对恶意欺诈行为的排斥与抑制，即使在互不相识的节点间也可迅速建立信任。

4）防篡改：区块链的链式结构依照时间顺序将前一区块整体数据进行哈希并按照一定规则记录于与其相连的后一区块，使二者存在相互验证关系，通常采用的共识算法需消耗大量算力资源，只有具备全网超 51%算力时才可实现伪造区块的生成速度超过真实区块，但该条件在很大程度上无法实现，从而限制了篡改链上信息的违规行为。

2.3 区块链数字身份

目前数字身份的落地应用仍面临着一些技术问题，如前文所提隐私保护、数据共享、自主控制权等，区块链技术以其防篡改、去信任、安全、去中心等特征成为虚拟网络世界下价值交换的可信媒介，由于去中心的分布式结构使链上成员处于平等地位，节点共同遵守运行规则，共同维护账本信息，使链上数据得到公共认可，因此区块链技术可成为数字身份所依靠技术之一，对数字身份技术所需的安全可靠、可用性、隐私保护、不可抵赖性等要求提供技术支持。作为开放的区块链系统平台，任何网络中的节点均可接入链上，缩短了社会距离[6]，区块链的开放性保障了每个用户均可获得区块链数字身份服务的权利。去中心化作为区块链技术的一项重要突破，保障了链上节点的平等地位，并且使节点具备自主权，由传统的被动获取身份转变为主动创建并管理身份，将主动权归还用户自身。由于身份信息的产生源

自用户，其可能带来的经济收益也应归该用户所有，借助区块链价值中介实现收益的分配。链上的数据加密以及数据广播、共享机制使身份在得到隐私保护的前提下实现了跨应用程序间的共享，打破传统模式下信任关系传递屏障，区块链技术是未来自我主权身份的一个良好基础[7]，将区块链技术与数字身份结合综合了二者的优势，成为未来研究发展的趋势之一。

3 区块链技术在数字身份领域的应用及问题

现阶段应用最为广泛的身份管理基于公钥基础设施（PKI），是一种用于保障网络信息安全的通用基础设施，可看作一系列硬件设施、人员、软件、规章等的总和，用于生成、存储、调用、吊销基于公钥密码学的公钥证书。数字证书是 PKI 体系的核心，随 PKI 体系的建立和 CA 的建设形成了较为完备的身份证书体系[8]，从而利用 PKI 实现身份鉴别、信息加密功能，保障网络信息的真实性，因此 PKI 是目前公认的保障网络身份信息安全的最佳体系。传统 PKI 不基于区块链技术，由第三方为用户授予身份，因此该模式假设第三方可信并具备符合要求的数据保护能力，该假设在通常情况下成立，但也面临着意外的黑客攻击、数据丢失风险，使第三方机构成为 PKI 体系安全保障要求中可能存在的弱点，其解决方案并非放弃 PKI 体系，而是在此基础上进行改进，由此产生了 DPKI（分布式公钥基础设施）技术，在分布式环境下，任何一个单一的机构不会对整个系统的稳定性造成很大影响，该方案去中心化形式与区块链天然契合，成为未来数字身份管理的趋势之一。区块链技术与数字身份的结合已取得了一定的研究进展，从技术问题角度可分为以下几个方面。

3.1 身份授予的真实性问题

为获取线上服务，用户凭借数字身份进行登录，当服务提供方认可该用户具备服务使用权限后便可提供服务，该前提为权威机构已通过一系列身份核验确认用户身份并将数字身份加密授予用户本人，此过程称为身份授予。

身份授予作为身份认证工作的开端，为认证提供了身份基础信息，是后续采用用户名/密码、指纹信息或 USB Key 等方法验证身份的基础。传统线下操作通常以身份证为依据，核验该人员是否人证相符，以身份证本身的真实合法性与人证比对结果作为可靠性保障，从而为需求者提供注册、登记服务，授予用户在该场景下的身份。由于身份证件信息为明文信息，包含地址、年龄等隐私数据，因此在接受核验的同时也在一定程度上泄露了个人隐私。在线上场景，获取网络服务前通常也需经过注册流程，通常由用户自行提交身份信息数据，服务提供商据此为用户授予相应身份，但身份造假问题同样存在。身份的授予也可采用线上线下相结合的方式，Daniel Augot 等人[9]所提出的线上身份授予方案便基于面对面证明以保证申请人身份的真实性。

为实现数字身份与物理身份的关联，可通过线下已存在的实名体系为线上身份授予提供依据，Jong-Hyouk Lee[10]提出基于区块链的 ID 即服务方案，基于现存移动通信服务的实名认证，用户可在 BIDaaS 提供方处获取虚拟 ID，该虚拟 ID 即为用户线上数字身份，其真实性建立在实名制移动通信基础之上，解决了身份授予的信息真实性问题。通过数学模型进行运算也可作为数字身份真实性的保障之一，Chao Lin 等人[11]将现实场景中个体间的联系通过网络图进行表示，顶点代表个体，连接顶点的边代表二者间的联系，在顶点进行动态变化时，所提出的传递封闭无向图身份认证方案 (TCUGA) 仍然可以提供身份证书的授予、查询功能，此外对于两顶点间不存在直接关联的情况，可通过其他共同与该点有联系的路径实现关联，进而为其授予合法身份，即通过分布式的网络结构下所产生的信任关系为用户提供身份真实性的保障。Chao Lin 等人[11]TCUGA 方案的实现以区块链作为技术支持，节点的动

态变化可通过区块链实现低成本的高效广播，利用智能合约实现算法过程的独立自主，并最终将用户身份信息进行安全可靠存储。

为实现去中心化的身份授予，同时保障对身份真实性的认可，谭海波等人[12]提出在联盟链上用投票方式使用户获取身份注册权限，该方案下，申请者为加入该共享联盟链，须获得链上半数以上联盟成员投票认可，该申请者基于椭圆曲线算法为自身生成公私钥对，并秘密保存私钥，通过可靠信道将公钥及其身份信息发送至联盟链上所有成员，并委托某一成员发起“身份创建投票合约”，链上成员通过该合约参与投票，赞成票数过半时“数字身份控制合约”自动保存该申请者公钥并创建身份标识(SC-ID)，从而完成身份注册流程。

3.2 隐私保护问题

数字身份的使用一方面为用户提供了便利的网络服务获取权限，但随着网络服务的数量与范围逐步增长，互联网上积累了大量的个人和敏感信息[13]，其包含内容十分广泛，一言一行均可能记录在内[14]，大数据在为商业、社会带来便利的同时也蕴藏着巨大的风险[15]，过多身份信息的线上存储，用户的个人隐私数据很容易被获取[16]，隐私数据的泄露风险，不同应用间的身份关联，用户习惯推测等问题也引发了对数字身份隐私保护问题的思考。

在某些应用场景下，用户并非必须使用其真实身份，利用伪身份的同时保障伪身份与真实身份在一定条件下可关联可作为数字身份的应用之一。Arun Thapa 等人[17]设计出分布式在线社交网络（DOSN）下的安全与隐私拍卖模型（SPA），由可信第三方（TTP）为拍卖参与者授予公共/私有伪身份，利用 TTP 私钥为用户公共伪身份签名后生成用户证书，证书与私有伪身份经用户公钥加密后由 TTP 发送至用户，此后用户便可以公共伪身份进行价格投标，在不同拍卖场景下使用不同身份以避免真实身份信息的泄露，利用私有伪身份提供与公共伪身份间的关联证明。从而保障了在不暴露真实身份的情况下参与拍卖活动，但在必要时也可通过一定权限下的解密操作获取该伪身份的真实对应关系，由于该方案存在 TTP，是中心化管理的案例，因此可将该方案运用于区块链场景，利用去中心化的方式对该方案进行改进部署。

身份隐私保护的另一途径为避免身份的关联，包括同一身份在不同应用间的关联以及同一应用下交易双方身份的关联。伪身份的使用可为同一用户在不同应用中提供非关联的身份，避免攻击者的关联分析。对于交易双方的身份关联问题，吴进喜等人[18]在区块链公平合约签署的基础上进一步提供了避免身份关联的身份混淆方案，引入半诚实可信的第三方提供中间服务，签署方分别与第三方签署该协议，以秘密因子保障合同隐私性，以保证金约束各方行为，待该合同被正确记入链上后各方可赎回保证金，第三方获取服务费。同一合同的签署方可任意选择第三方实现身份混淆，避免了签署方直接对接产生身份的暴露与关联，一定程度上解决了线上身份的隐私保护问题。

3.3 自我主权问题

现阶段用户所获取的数字身份通常依赖于大型身份提供商，如 Facebook、腾讯等，或在每个服务提供商处创建新的数字身份，数字身份的掌控权由供给方持有，形成以服务提供商为中心的数字身份体系。在分布式管理思路下的自我主权身份（SSI）以用户为中心，声明发布方以及身份验证方围绕用户提供身份证明与验证功能，实现用户自主控制其身份的要求。不受中心化方式管理的身份系统地址分配面临 Zooko 三角矛盾，几乎不可能同时实现分布式分配标识符、安全（无冲突）以及人类可读。uPort 针对非人类可读地址问题设计了

可行命名层，使以太坊智能合约地址作为用户身份标识符的非可读 uPort ID 映射为可读形式，Blockstack[19]也采用了相类似的映射方法实现可读性。

Md Sadek Ferdous 等人[20]使用数学模型对自主身份的概念提供了一个正式的定义，在该自主身份中，用户是身份管理的中心，一个自我主权身份应是可移植的，从而保证跨多个应用间身份的互操作性，该身份由用户或团体提出声明，包含声明者有关的身份事实。该自我主权身份所具有的三个主要特性为：对可移植身份的自主管理、基于用户许可的属性披露和身份的互操作性，另外还具备存在性、可控性、访问权、透明性、长期有效性、可移植性、互操作性、许可性、隐私披露最小化和安全性这十种特性。

在自我主权身份概念中，可验证声明为用户提供身份信息的具体描述，是 SSI 的核心部分[21]，声明发行者为用户签发声明，并通过非对称加密算法进行签名确保声明确由该发行者发布，保障声明的可信度。一个用户主体可对应多个不同领域身份声明，同一声明也可由不同证明者授予证明。用户可向服务提供商提供其拥有的可验证声明，验证方可通过单一证明或汇总一个声明关联的多方证明验证该用户身份，形成更完整用户画像从而建立信任。

3.4 跨域问题

用户所获取的数字身份可作为其在网络世界的通行证书，经核验后可使用户获得其权限范围内多种类型的网络服务。通常，不同类型的服务由各服务提供商主体独立运行，之间缺乏安全有效的信息共享渠道[22]，从而形成信息的“孤岛”，具有各自相对独立的信任域，而同一用户在获取多项不同类别服务的过程中，单一域的认证结果无法迁移至多域，因此用户需访问不同信任域以获取相应域下的访问权限，频繁的信息交互引发对跨域认证的需求。

PKI 体系提供的跨域认证方案其核心即解决信息网络空间中的信任问题，PKI 结构一般为多层次树状结构，包含多种认证机构（CA）以及终端实体等，CA 也呈分层组织形式，顶层由政策批准机构（PAA）创建 PKI 整体架构的方针、政策，其地位相当于根 CA，PAA 下属政策 CA（PCA）对 PAA 政策进行行业或地区的细化，CA 作为 PCA 的下属级别直接面向用户提供证书服务，PCA 管理 CA 间的交叉认证。建设一个完整的跨多领域、多地区 PKI 体系是一项庞大的工程，其建设与维护成本较高。此外，通过多级证书链连接不同信任域进行证书传递，公钥算法签名与计算开销也成为影响跨域认证效率的问题之一。基于身份的密码体制（IBC）以用户自定义字符串作为公钥，解决了通过证书绑定公钥与身份模式下证书的传递开销问题。高阳等人[23]将信任与基于身份的密码体制（IBC）进行结合，提出了一种基于信任的用户跨域访问信息服务实体（information service entity ， ISE）资源的算法。用户在域内完成身份注册，跨域认证时由域代理基于信任模型计算域代理间的相似性与欧氏距离得到域间信任值，以得分结果判断跨域身份是否可信，但存在信任模型、评分标准随研究者主观变动的问题。针对 PKI 体系跨域认证效率问题，周致成等人[24]设计出基于区块链技术的高效跨域认证方案，基于原有 PKI 体系，以区块链节点形式设置根 CA 服务器、认证服务器，区块链 CA（BCCA）信任模型提供跨域认证方法，不同域的根 CA 经许可后加入联盟链，同时根 CA 证书哈希值记录于链上，产生跨域认证需求时即可通过比对证书哈希值进行判断。减少公钥验证签名、验签次数，从而提升跨域认证效率。马晓婷等人[25]针对跨域（PKI 域和 IBC 域）认证问题，进行了基于区块链的跨域异构认证方案设计，在 IBC 域设置区块链域代理服务器，并参与国密算法 SM9 的密钥生成计算过程，IBC 域区块链域代理服务器与 PKI 域区块链证书服务器共同构成联盟链，链上各节点保持相互怀疑，通过周期性相互认证保障该链的安全可信，从而提供不同域间的相互认证服务。

4 区块链数字身份所面临的其他问题

（1）公众感知问题

2019 年 10 月 24 日在有关区块链技术发展现状和趋势进行的第十八次集体学习中，国家提出将区块链作为核心技术自主创新的突破口，加快推进区块链技术的发展。现阶段我国仍处于区块链技术的初级研究阶段，各项应用技术有待逐步推进与完善，关于区块链数据累积与存储、共识机制的安全性与算力消耗等问题均需要进一步研究。同时区块链作为一种去中心化系统，不同于现阶段所熟悉的中心化管理方式，在对该技术的宣传、培训方面仍需投入大量精力，从而实现现有模式与去中心化模式的对接与转移，为使公众接受去中心化的思想并采用区块链技术仍需要一定的过渡时间。

（2）数字身份应用问题

无论集中式数字身份授予与去中心化的自我主权身份，均存在对用户身份真实性提供证明的签名方，通常由具有权威性的机构、公司进行提供，如公安系统、医疗系统以及大型企业等，此类组织一般具有一定的规模，其数据较为可靠，同时具备一定的数据安全保护能力，可为用户授予其合法身份。同时对于非大型权威机构，例如社区、学校社团等，其成员也存在身份证明需求，传统开具纸质凭证并签名盖章的方式受时间、空间限制，难以满足数字化时代工作效率，但该小型团体不具备完善的身份系统，数字化要求与可靠性要求均难以满足。因此未来研究可将非大型权威机构身份授予与认证可靠性问题纳入研究范围，通过信任模型，在身份发布方与认证方间建立信任关系。

其次，同一用户可具备多重数字身份，针对不同应用场景，同一身份应能够在不同服务提供商处迁移使用，并且实现用户操作的方便快捷。对于使用专有外置设备如 USB Key 辅助身份认证的方式给通常给用户带来了诸多不便，随身携带专有设备在生活中基本无法实现，而使用与用户时刻关联的生物特征如指纹、虹膜作为认证途径则对检测设备的便携与可靠提出要求。智能移动通讯设备作为日常必不可少的工具之一，其智能性与便携性使其成为数字身份认证的可行工具之一。身份信息存储于智能设备，一方面使身份在不同应用间的迁移更加快捷，但反之，设备的丢失意味着存储于设备中的身份信息面临泄露风险，用户体验的便捷性与用户数据的安全性二者之间产生了一定的矛盾关系。

（3）规范标准问题

在去中心化的区块链系统中，不存在处于领导地位的任一节点，所有网络中的节点平等地依据规则执行操作，因此可打破国界的限制，形成在全球范围内均可平等使用的大型网络系统，但现阶段仍缺少全球统一的区块链标准以及立法等规范。在跨国家、地区合作，跨领域、机构合作的情况下仍需统一的规范机制。

5 总结、建议与展望

数字社会中，信息以二进制表示在计算机网络环境下传递，一方面信息的传递速度大大增加，但同时由于网络的虚拟性，难以确定信息的发布源与信息使用者的真实身份，为网络安全带来了一定的隐患。现阶段中心化数字身份的应用与发展已出现了一定的瓶颈，其主要问题产生于用户对数字身份的控制权不足，由第三方授予、管理身份的模式存在信息泄露、收益归属、身份丢失等实际问题，因此可将区块链技术与数字身份二者融合，身份数据链上存储有效防止数据篡改，非对称加密算法提供隐私与签名等安全保障，链上数据共享利于身份的迁移使用，简化价值和信任传递流程[26]，去中心化模式使用户拥有数字身份的所有权。

新技术的结合可为传统技术难题提供不同解决思路，现阶段我国处于区块链数字身份研究的初级阶段，新技术的探索难免会遇到各种问题与困难，从而产生新的研究问题。

区块链技术的普及其前提为区块链基础设施的完善，当硬件设施达到应用标准后，如何将原有系统顺利转移至区块链架构，保障原有数据的安全与可用，同时该过程的资金成本、时间成本均应控制在合理范围之内，达到既高效又可靠的系统对接。作为未来身份管理主要技术的自我主权身份如何通过不同渠道为用户提供身份的证明，形成包含多方位的用户画像，建立关于用户自身的声誉体系，在面对不同应用场景时，可为验证者提供验证所需关联度最强但同时最少量的身份信息，以及该过程如何利用数学模型进行量化与评价。最后对数字身份管理的整个过程进行记录与监控，通过选定指标与机器学习方法的结合设计欺诈、犯罪监控模型，及时发现异常信息并提早进行干预。以上研究问题在未来区块链数字身份的应用中均值得引起学者的关注。

数字身份已经融入了日常的工作、生活，潜移默化地改变着我们的网络习惯，在未来，数字身份将是一项极具潜力的研究方向。本文对数字身份及区块链在该领域的应用研究进行了综述，期望对于公共服务、金融、网络服务等应用场景数字身份的管理与使用提供参考。

参考文献

[1] S Nakamoto. Bitcoin: a peer-to-peer electronic cash system[OL]. 2009.https://bitcoin.org/bitcoin.pdf

[2] 张婧羽，李志红.数字身份的异化问题探析[J].自然辩证法研究，2018，34(09): 45-49.

[3] M S Ferdous, G Norman, R Poet, et al. Mathematical Modelling of Identity, Identity Management and Other Related Topics[C]. Glasgow Scotland UK: ACM, 2014.9-16.

[4] 田道坤，彭亚雄.在区块链中基于混合算法的数字签名技术[J].电子科技，2018，31(07): 19-23.

[5] 刘敖迪，杜学绘，王娜，等.区块链技术及其在信息安全领域的研究进展[J].软件学报，2018，29(7): 2092-2115.

[6] 杨慧琴，孙磊，赵西超.基于区块链技术的互信共赢型供应链信息平台构建[J].科技进步与对策， 2018，35(05): 21-31.

[7] DV Bokkem,R Hageman,G Koning, et al.Self-sovereign identity solutions: The necessity of blockchain technology[J].arXiv preprint arXiv,2019,1904.12816.

[8] 刘知贵，杨立春，蒲洁，等.基于 PKI 技术的数字签名身份认证系统[J].计算机应用研究，2004，(9):158-160.

[9] D Augot , H Chabanne , O Cl é mot, et al., William George.Transforming face-to-face identity proofing into anonymous digital identity using the Bitcoin blockchain[C]. Calgary CANADA:IEEE,2017.25-34.

[10] A M ü hle, A Gr ü ner, T Gayvoronskaya, et al.A survey on essential components of a self-sovereign identity[J].Computer Science Review,2018,30: 80-86.

[11] JH Lee.BIDaaS: Blockchain Based ID As a Service[J].IEEE Access,2018,6: 2274-2278.

[12] Lin C, He D, Huang X, et al. A New Transitively Closed Undirected Graph Authentication Scheme for Blockchain-Based Identity Management Systems[J]. IEEE Access, 2018,6: 28203-28212.JI X G, DENG Y Y, WANG P. Characters of atmosphere pressure, pure oxygen fixed bed gasification of seven kinds coal[J]. Clean Coal Technology, 2004, 25(4): 50-52.

[13] 周艺华，李洪明.基于区块链的数据管理方案[J].信息安全研究，2020，6(1): 37-45.

[14] 王德夫.大数据时代下个人信息面临的新风险与制度应对[J].西安交通大学学报:社会科学版， 2019，39(06):123-132.

[15] 邱仁宗，黄雯，翟晓梅.大数据技术的伦理问题[J].科学与社会，2014，4(01): 36-48.

[16] 刘千仞，薛淼，任梦璇，等. 基于区块链的数字身份应用与研究[J]. 邮电设计技术，2019，518(04):87-91.

[17] 谭海波，周桐，等.基于区块链的档案数据保护与共享方法[J].软件学报，2019，30(9): 2620-2635.

[18] A Thapa, W Liao, M Li, et al. SPA: A Secure and Private Auction Framework for Decentralized Online Social Networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2016, 27(8): 2394-2407.

[19] 吴进喜，高莹，张宗洋，等.基于区块链的多方隐私保护公平合同签署协议[J].信息安全学报，2018，3(3): 8-6.

[20] M Ali,J Nelson,R Shea, et al. Blockstack: A Global naming and storage system secured by

blockchains[C]. Denver, CO:USENIX Assoc,2016. 181-194.

[21] MS Ferdous,F Chowdhury,MO Alassafi.In Search of Self-Sovereign Identity Leveraging Blockchain Technology[J].IEEE Access,2019,7: 103059-103079.

[22] 谭海波，周桐，赵赫，等.基于区块链的档案数据保护与共享方法.软件学报，2019，30(9):2620-2635.

[23] 高阳，马文平，刘小雪.基于信任的服务实体跨域认证方案[J].系统工程与电子技术，2019，41(2): 439-444.

[24] 周致成，李立新，李作辉.基于区块链技术的高效跨域认证方案[J].计算机应用，2018，38(2): 316-320，326.

[25] 马晓婷，马文平，刘小雪.基于区块链技术的跨域认证方案[J].电子学报，2018，46(11): 2571-2579.

[26] 董贵山，陈宇翔，范佳，等.区块链应用中的隐私保护策略研究[J].计算机科学，2019，46(5): 29-35.

Research on Digital Identity Based on Blockchain Technology: Status and Challenges

ZOU Lin，JIA Shiyu，CHEN Jin，LAN Qiujun

(Department of Business Management, Changsha/ Hunan, 410082)

Abstract：Blockchain technology, as an emerging technology following big data, cloud computing, and artificial intelligence, breaks the traditional thinking of centralized management, thereby achieving decentralized, trustless, tamper-proof transaction execution and data storage. The research of digital identity based on blockchain technology involves the process of identity granting, management and verification. From the perspective of the current research status of digital identity based on blockchain, this article summarizes identity management under traditional methods and blockchain technology. Identity authentication methods range from simple to complex. Its development process reflects the continuous updating of authentication requirements and the increasing progress of information technology. The application of blockchain technology in the field of digital identity further improves the safe and reliable storage capacity of identity information and provides data protection for identity authentication. Based on the above research, the challenges faced by the development of blockchain technology are further proposed, and future research is prospected.

Keywords: Blockchain; Digital Identity; Identity Management; Research Progress