基于区块链的数字身份应用与研究

Application and Research of Digital Identity Based on Blockchain

刘千仞，薛　淼，任梦璇，王光全（中国联通网络技术研究院，北京 100048）
Liu Qianren，Xue Miao，Ren Mengxuan，Wang Guangquan（China Unicom Network Technology Research Institute，Beijing 100048，China）

摘　要：
现有的数字身份系统多存在操作繁琐、信息易泄露、容错性低等缺点。区块链技术的弱中心化、不可篡改等特点能够较好地解决这些问题。电信运营商的手机号基本上是全用户覆盖，可以作为数字身份的标识，且具有通信功能。将针对区块链技术在数字身份领域的应用与研究展开讨论，并提出一种运营商场景下的基于区块链数字身份应用方案。

关键词：
数字身份；区块链；身份认证
doi：10.12045/j.issn.1007-3043.2019.04.018
中图分类号：TN915.08
文献标识码：A
文章编号：1007-3043（2019）04-0081-05

Abstract：
Most of the existing digital identity systems have the disadvantages of cumbersome operations，easy information leakage and low fault tolerance. The decentralization and no tampering of blockchain can solve these problems better. The mobile numbers of telecom operators cover all users basically which can be used as a digital identity and have communication capabilities. It discusses on the application and research of blockchain in digital identity，and presents a digital identity solution based blockchain under telecom operator scenes.

Keywords：
Digital identity；Blockchain；Identity authentication

引用格式：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(4)：81-85.

0 前言

随着移动互联网的普及，每个人都有若干个账号，包括网站和应用，这些账号都叫做数字身份。对应实际生活中的身份证，数字身份则是用户虚拟生活中的标识，其重要性不言而喻，用户在互联网上活动的基础是数字身份，用户通过数字身份不断与其他设备相连，这中间的所有联系、交易、数据的完整性和隐私性都必须得到最佳的保护和管理，因此只有确保用户数字身份的真实可靠，该用户后续所产生的一系列交易和活动等才会生效。随着数字身份技术和区块链的发展，人们逐渐意识到二者之间有着巧妙的联系。区块链的私钥加密、分布式存储、全程可追溯可以充分保护用户的隐私，并且用户自己掌握自己信息的处理权，可以决定谁来以什么样的目的查看和使用数据。用户的数字身份信息不断完善，可以从源头上解决区块链现存的只能保证链上存真，而无法去伪的问题，同时有效地促进区块链信息流通共享，进而提高整体的认证效率。本文主要从数字身份的发展现状及存在问题入手，探讨引入区块链技术的应用需求、场景及方案。

收稿日期：2019-03-14

1 数字身份研究现状

身份证是一组用于定义某项实体的特征数据，并具有唯一相对性。身份证的使用包括2个过程，一是认证，即国家给予的身份证明，用来证明公民的合法地位；另一是验证，利用身份证购车票、办理酒店入住等。而数字身份则是特定实体物理身份的数字版本。世界经济论坛（WEF）从使用属性的角度将数字身份定义为独特属性的集合，用于描述一个实体并确定该实体

可以参与的相关事务。

数字身份分为广义和狭义2种，狭义的数字身份就是指数字账号，广义的数字身份涉及面则非常广，因为在互联网上进行活动，不仅人需要身份，公司甚至物品也都需要身份。有了可信的数字身份，互联网上的信息传递和分享，商品交易和贸易合作才能更好地开展。

目前国家层面的数字身份是由公安部开发的eID工具，eID是一种以密码技术为基础、以智能安全芯片为载体、依托“公安部公民网络身份识别系统”签发给公民的网络电子身份标识，可以在不泄露身份的前提下在线远程识别身份。但eID只是像公民身份证号一样，是一个专属公民的编号，主要是用来认证，并且使用场景有限。现在公民的数字身份信息其实是分散的，例如支付软件存储着交易信息，聊天软件存储着社交信息，游戏软件存储着娱乐信息，这些不同属性的信息对于公民数字身份来说，就像是身体的各个部位，共同组成了最终的个体，属性越全面，身份越完整；而一个好的数字身份可以通过整合新的信息，对用户有一个全面的刻画，能够广泛应用于社会各个领域。

如今国民经济和社会发展各领域正在经历着数字化变革，数字信息正成为经济社会的发展动力和方向。然而数字身份要真正形成完备全面的系统还面临着许多挑战。

主要问题如下：

a）“基础设施”不完善，认证成本高。正如上面提到的，用户的数字身份信息往往多种多样，不同行业不同部门往往都有各自的数字身份系统，一个公民可能在多个系统内存在多套数字身份，造成了数据存储资源的浪费，提升使用成本，并且各个系统之间互不相通，系统之间的相互认证需要经历复杂的流程，认证成本较高。

b）隐私保护困难。谈到数据隐私，就必须提到通用数据保护条例（GDPR）。GDPR是由欧盟推出的一个目的在于遏制个人信息被滥用，保护个人隐私的法案，于2016年4月试推出，正式生效时间为2018年5月25日。根据GDPR规定：企业在收集、存储、使用个人信息时要取得用户的同意，用户对自己的个人数据有绝对的掌控权。然而，当下的情况则是用户的个人隐私数据很容易被获取，便宜出售，从而让不良利益集团有机可乘，他们利用数据分析和精准营销，定位目标用户，进而对其进行诈骗，从而使用户财产及相关的利益受损，并且相关企业业务如果涉及欧盟，还要面临2 000万欧元或全年营收4%的高额罚款。近年来用户数据泄露数据频发，屡禁不止。表1是过去1年来影响较大的泄露数据的事件汇总。

c）认证流程繁琐低效、容错性过低。用户使用不同的服务需要进行多次不同的认证，且主要通过复杂、低效的手动流程，用户体验十分不友好。并且传统的中心化身份认证依赖于单一系统的稳定性，一旦宕机或者中心化机构出现数据泄露，则影响系统响应服务，并造成信息安全事件，容错性过低。

2018年达沃斯世界经济论坛提出：一个好的数字身份应该满足5个要素。

a）可靠性：好的数字身份应具备可靠性，可以建立对其所代表的人的信任，行使其权利和自由，以证明他们有资格获得服务。

b）包容性：任何需要的人都可以建立和使用数字身份，不受基于身份相关数据的歧视风险影响，也不会面临排除身份的身份验证过程。

c）有用性：有用的数字身份易于建立和使用，并且可提供对多种服务和交互的访问。

d）灵活性：个人用户可以选择如何使用他们的数据，共享哪些数据以进行哪些交易，与谁交易以及持续多久。

e）安全性：安全性包括保护个人、组织或各种设备免遭身份盗用及滥用，不会出现未经授权的数据共享和侵犯人权等行为。

由此可见，像身份证、护照、驾驶证一样，数字身份首先需要一个强力背书机构，通常这需要依靠政府的力量来进行，并以此身份认证为基础进行扩展构建。在前文中也提到，用户的绝大多数社会行为信息基本

表1　2018年数据泄露事件统计

时间	涉及机构	后果及影响
2019-02	深网视界	泄露数据包含超过256万人的个人信息，例如姓名、年龄、性别、出生日期、身份证号、国籍、住址、雇主和过去24 h内的位置，大约有668万条记录，后果持续发酵中
2018-12	12306官网及第三方软件	泄露数据包含60余万条用户注册信息和410余万条铁路乘客信息，数据已确认真实，铁总否认泄露，原因可能来自第三方软件
2018-08	华住集团	泄露数据涉及到1.3亿人的个人信息及开房记录
2018-03	Facebook	泄露数据至少8 700万条，涉及5 000万用户，股价大跌，市值蒸发500亿美元

掌握在各类企业手中，社交、支付、购物、运动、交通信息等都分属于不同的企业，这些企业在构建用户数字身份中将会起到举足轻重的作用。而运营商由于手机号的缘故存在天然优势，一方面手机号基本能做到全用户覆盖，另一方面每个手机号都是经过实名认证的，一个手机号可以对应到一个实体人，每个人都会携带手机，这就是数字身份的最好载体，这也是运营商可以大力发展数字身份的重要原因。

2 区块链在数字身份领域应用需求

早期的身份认证主要采用口令密码的形式。用户需要在网站或者应用上进行注册并牢记自己的账号、密码，作为登录的凭证。然而每个互联网应用都有自己的认证体系和用户体系，用户在不同的互联网应用之间是无法互联互通的。因此，用户需要记住不同应用对应的账号和密码，而若设置简单或重复的密码降低记忆成本，又可能会由于密码泄露导致用户的信息安全甚至经济安全受到威胁。过多的应用导致用户账号管理困难。其中，任意一个账号信息被泄露，用户隐私将被无限扩散，导致用户一方面面临各种各样的骚扰电话和短信，另一方面存在安全隐患，导致财产损失。根据调查显示：约80%的用户不喜欢账号注册的繁琐过程；35%的在线购物者因为没有账户放弃了购物；2018年中国消费者协会发布的《APP个人信息泄露情况调查报告》显示，受访者中曾因个人信息泄露而被骚扰或侵害的人数占比高达85.2%；70%的受访者认为手机APP存在过度索取用户权限的情况；80%的受访者认为手机APP采集个人信息目的不纯，以便广告推销或者二次售卖。从这些数据中不难看出用户对于APP隐私安全问题的焦虑和担忧。

图1示出的是数字账号过多的危害。

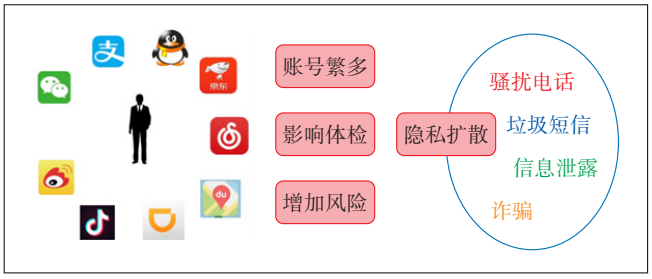

图1　数字账号过多的危害

鉴于口令密码认证方式使用不便等缺陷，支持不同系统间的统一认证技术方案应运而生。

利用社交媒体账户登录已经成为替代在线注册的主流选择。这种方式让互联网用户使用平台中现存信息来进行单点登录，比如Facebook、微信、支付宝等。主要使用的是OAuth 2.0协议。

OAuth 2.0协议关注客户端开发者的建议性，要么通过资源拥有者和HTTP服务商之间的被批准的交互动作代表用户，要么允许第三方应用代表用户获得访问的权限。协议同时为各种应用和设备提供专门的认证流程。2012年10月，OAuth 2.0协议正式发布为RFC 6749。以微信为例，第三方APP首先进行软件审核，审核通过后获取AppID和AppSecret，然后需要在微信开放平台注册开发者账号，申请微信登录且通过审核后，可开始接入流程。新用户登录该APP时，会提示微信一键登录按钮，如果用户手机没有安装微信则会提示安装微信客户端。具体步骤见图2。

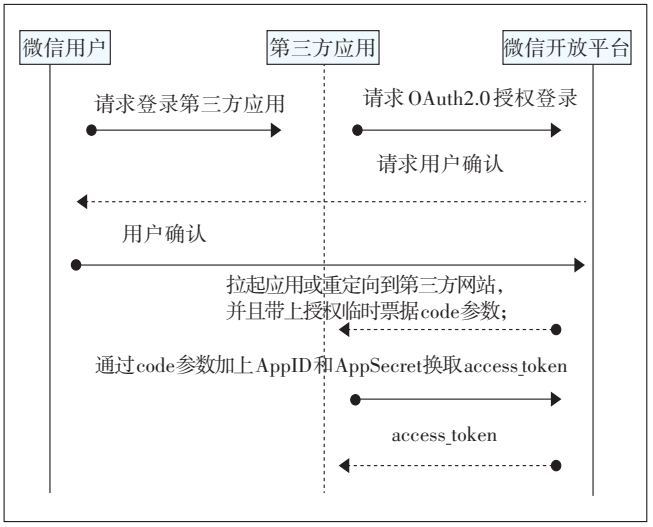

图2　微信授权登录步骤

这些步骤对于用户来说，只是简单地点几下按钮就可以完成操作，省去了注册用户的一系列流程，所以在现阶段应用非常广泛。

该方案虽然有很多优势，例如简单、开放及安全。但是该方案也存在不少弊端，例如在安全性上存在一定的漏洞。2016年11月，香港中文大学的研究人员发表文章称，“使用OAuth 2.0协议可以毫不费力地登录十亿移动LApp账户”。研究人员发现通过第三方APP开发方，错误地使用OAuth 2.0协议，能在用户不知情的情况下，被黑客远程利用。

OAuth 2.0只是其中的一个问题，用户数据如何被保护也是重中之重。企业都尽全力去保护用户个人信息，但是成本昂贵。数据显示，欧盟地区，仅英国每年的身份确认成本已经超过33亿英镑，约等于290亿人

民币。这还不包括后续由储存、保护、违约、管理等行为导致的成本追加。

并且基于社交应用的统一认证能力通常只支持用户登录，在涉及到用户信息核实的环节（如转账汇款等），都需要通过短信或者语音的方式确认用户的真实身份以及操作的合法性。这种方式不仅会影响用户的操作体验，同时可能会面临手机号码泄露带来的安全风险。

运营商掌握大量的用户信息，基于运营商提供的手机号码和个人信息进行身份验证，可以为用户提供便捷、安全的身份认证服务。但是也存在一些问题：例如如何避免用户数据流失、隐私泄露及身份盗窃；如何对接不同运营商的统一认证平台，获取移动认证服务。

针对传统身份认证的一系列问题，本文从区块链技术的角度提供一种新的思路，区块链是一种由多方共同维护，以块链结构存储数据，使用密码学保证传输和访问安全，能够实现数据一致存储、无法篡改、无法抵赖的技术体系。通过多方参与的分布式账本技术，可实现运营商之间的合作机制；通过密码学原理的非对称加密、智能合约以及零知识证明的方式，保护个人隐私数据不被泄露盗取；通过将数据使用的决策权归还给用户，解决了用户身份数据使用的合法合规性问题，同时也提供了对接用户、运营商和需求方的创新性思路。

3 基于区块链的数字身份应用

通过区块链构建数字身份系统，设计思想是采用弱中心化的“公治”式机制。在该系统中，所有业务系统像原来一样，各管各自的用户账户，但会通过联盟链的形式来彼此鉴权和认可对方的登录请求，并授权访问对应的用户数据。

运营商利用算法为实名认证用户创建数字身份，与此身份相关联的私钥安全地存储在用户的eSIM上，公钥存储在所有节点上。然后用户使用自己的私钥添加数字签名，登录时将数字签名等摘要信息上链进行验证，如图3所示。

所有运营商用户数据信息生成摘要（公钥、数字签名等）放在链上，其他的软件需要身份认证的时候访问链进行认证，对其他软件来说，用户是匿名登录，保护了用户隐私，避免了用户信息泄露。第三方开启授权认证时可以通过授权平台对授权信息进行查询，通过智能合约技术实现对数据信息的查询，通过链完成验

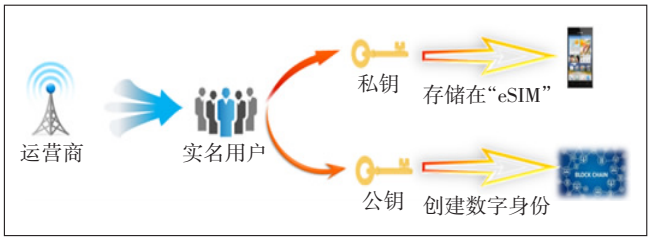

图3　运营商数字身份原理

签过程，直接获取认证结果。以此构成一个联盟链，所有加入链中的企业可以互相达成可信机制，具体流程如图4所示。

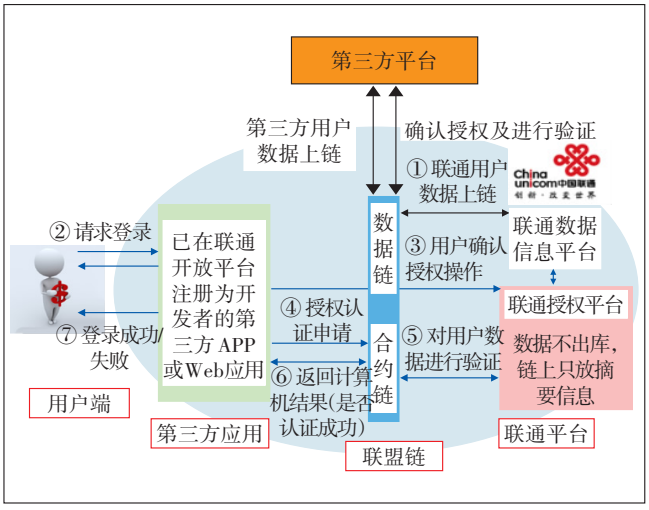

图4　数字身份流程

a）运营商将自有实名认证的用户数据库，通过算法进行加密，生成公钥和私钥对，利用公钥生成数字签名。其中，公钥和数字签名上链进行存储。私钥存储在用户本地，即eSIM卡上。

b）用户请求登录在运营商开放平台注册过的第三方APP或者Web应用。

c）第三方APP或者Web应用将用户请求信息发送给运营商授权平台，授权平台提示用户，获取用户授权登录信息，在此基础上提示用户信息使用范围，是否允许第三方使用用户信息（该步骤不影响用户后续登录操作）。

d）第三方APP或者Web应用获取用户授权之后，开始上链进行验证申请。

e）利用用户授权，在链上匹配对应公钥和数字签名，同时在运营商数据库内部进行匹配。

f）将匹配的结果反馈给第三方APP或者Web应用。

g）根据反馈的结果对用户的登录请求进行回应，

匹配成功则登录成功，否则就登录失败。

h）只要加入联盟链中的企业都可以共享认证用户，假设第三方企业也有自己的认证用户数据库，则这些用户可以直接登录联盟链中的其他应用，原理和流程同上述方式。

本方案最终为用户生成一个唯一的数字身份，可以用来登录所有联盟链内的应用。利用区块链技术为加入联盟链中的合作伙伴之间达成实名认证用户互通。

4 区块链在数字身份领域的场景及意义

运营商为用户创建的数字身份，在条件允许的情况下，可以用来打造基于区块链技术的身份认证平台，结合eID，可以提供诸如统一身份认证、信息校验、免密登录等服务。并且该数字身份不仅可以用来进行第三方合作伙伴验证。还可以用于政府、金融、民生、医疗、交通等多个领域，形成电子政务链、在线医疗链、健康保险链等。在保护用户隐私的同时，极大地方便了用户，同时也符合网络实名制的要求，利于互联网安全机制的建立。

5 总结

将区块链技术应用于数字身份，归结起来有如下优势。

a）数据真实有效。基于区块链不可篡改、全历史的特性，区块链可以充分保障链上所有数据的真实可信。对于数字身份来说，为确保上链数据无虚假，这一部分需要在数据上链之前出具政府权威认证的信用背书，对于运营商来说，现拥有的所有用户都是实名用户，再把这些数据上链，从而确保链上数据是真实有效的。上链之后，每一个数据都是在所有节点的共同监督下被真实完整地记录下来，证据充分且可追溯。系统对所有链上用户透明，所有参与者都有可能获取他人已授权的信息。

b）数据安全及隐私保护。区块链的签名私钥、加密技术、安全多方计算等技术，可以有效保障用户隐私安全。数据使用权都在用户自己手上，而不是像现在这样，在各种企业手中，这就保证了用户隐私不会被其他任何人随意使用。并且在交易过程中，双方的隐私都可以通过脱敏技术得到很好的加密处理，外人对其交易行为的了解只限制于过程表面，交易双方的信息都是加密的。在隐私保护下的前提下，区块链可为数据开放提供解决方案，让数据真正放心地流动起来。

c）数据流通及共享。目前不同的互联网平台以及各个业务系统之间依然是相互独立的，核心数据是各自的立足之本，轻易不会外泄。通过区块链技术，搭建基于各个平台和业务系统之间的联盟链体系，并采取相应的智能合约、共识机制以及激励机制，从而有效地驱动企业去“共享数据”，实现优势互补，使数据价值利用最大化，进一步促进行业信息流通和整合。区块链提供的可追溯路径，可以有效破解数据确权难题，有利于建立可信任的数据资产交易环境。

对于数字身份而言，要想保证绝对安全仅靠某一种技术是无法实现的，而是需要多种技术进行优势互补，形成软硬一体的完备解决方案。虽然区块链的分布式账本是安全级别较高的技术，理论上账本不会轻易受到破坏或者篡改，但不法分子会将攻击重点转向用户和设备，因此需要提升上链前的安全措施，例如加大对区块链参与者的身份验证，提升设备和执行环境的安全性。随着技术的发展，这些安全优先事项一旦得到有效解决，区块链技术必将充分发挥其潜力，成为数字身份的坚强护盾。

参考文献：

[1] 中国信息通信研究院. 可信区块链推进计划[EB/OL].[2018-10-12]. http://www.trustedblockchain.cn/.
[2] 邵奇峰，金澈清，张召，等. 区块链技术：架构及进展[J]. 计算机学报，2018，41(5)：3-22.
[3] 曹黎军，彭鹏，江泽武. 数字身份：区块链时代的基石[EB/OL].[2018-10-12]. https://www.jinse.com/blockchain/203083.html.
[4] 彭永勇，张晓韬. 基于区块链应用模式的可信身份认证关键技术研究[J]. 网络安全技术与应用，2018(2).
[5] 叶纯青. 区块链与保护数字身份安全[J]. 金融科技时代，2016(12)：92-93.
[6] 蔡维德，郁莲，王荣，等. 基于区块链的应用系统开发方法研究[J]. 软件学报，2017，28(6)：1474-1487.
[7] 陈龙强. 区块链技术：数字化时代的战略选择[J]. 中国战略新兴产业，2016(6)：56-58.
[8] GSMA. Blockchain- Operator Opportunities[R/OL]. [2019-01-09]. https://www.gsma.com/newsroom/all-documents/ig-03-blockchain-operator-opportunities-v1-0/.

作者简介：
刘千仞，工程师，硕士，主要从事区块链及数据分析工作；薛淼，高级工程师，博士，主要从事区块链标准及应用研究工作；任梦璇，工程师，硕士，主要从事区块链及数据分析工作；王光全，教授级高级工程师，学士，主要从事高速光纤通信技术及应用研究工作。