基于区块链的身份管理认证研究

董贵山 陈宇翔 张兆雷 白 健 郝 尧
(中国电子科技集团公司第三十研究所 成都 610041)

摘 要 针对网络空间中的身份管理问题,分析了通用的基于区块链的身份管理认证模型。首先,概述了身份管理的定义要求,回顾了网络空间中身份管理在区块链应用方面的早期尝试,总结了其发展经验并分析了身份管理所面临的问题,对比了区块链的优缺点及其在身份管理方面的验证项目。然后,分析了通用的区块链身份管理模型及每个模块。最后,重点对较为成熟的 ShoCard 公司的应用场景和 DIMS(Decentralized Identity Management System)做了分析对比,并对未来进行了展望。

关键词 身份管理,区块链,认证,信息安全
中图法分类号 TP316 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.11.006

Research on Identity Management Authentication Based on Blockchain

DONG Gui-shan CHEN Yu-xiang ZHANG Zhao-lei BAI Jian HAO Yao
(No. 30 Institute, China Electronics Technology Group Corporation, Chengdu 610041, China)

Abstract Aiming at the problem of identity management in network space, this paper analyzed a universal identity management authentication model based on blockchain. First, the definitionand requirements of identity management in network space were outlined, and development experience and early attempts were reviewed. Then, the advantages and disadvantages of the blockchain and some kinds of proof of concepts in identity management were analyzed. Next, based on opening analysis, a general blockchain identity management model and each module were analyzed. Finally, the mature ShoCard company's application scene and DIMS (Decentralized Identity management system) were analyzed and compared, and the prospect of the future development was put forword.

Keywords Identity management, Blockchain, Authentication, Information security

1 引言

身份管理是信息安全的关键技术之一,其包括身份的定义、建立、描述、管理、注销等。根据国际电信联盟(ITU)的归纳将身份管理分为以下几个方面[1]:用户对身份证明和账户隐私安全的保护;运营商、提供商的安全性和经济性需求;政府企业管理、公共服务需求;网络安全、公共政策需求;非政府组织隐私保护需求等。

身份管理系统(Identity Management System,IMS)的主要概念如图 1 所示。Allen[2] 提出了自主权身份(self-sovereign identity),并对身份管理系统提出了 10 项要求,这些要求描述了用户实体独立存在(Existence)、控制自己身份(Control)、直接访问自己的数据(Access)、系统逻辑的透明性(Transparency)、身份持久存在(Persistence)、轻便可移植性(Portability)、使身份尽可能被广泛使用的互操作性(Interoperability)、用户控制自己的信息(Consent)、声明揭露信息量尽可能小(Minimization)、用户权益被保护(protection)等方面。基于属性的凭证(Attribute Based Credentials,ABC)用整数代替身份信息等属性并将其存储在加密容器中。

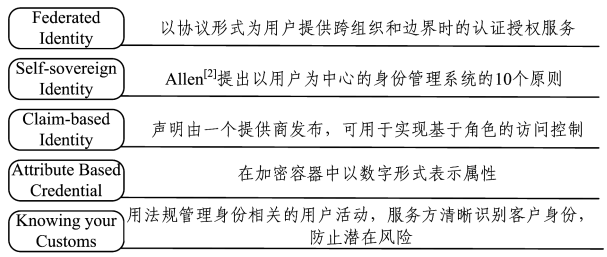


图 1 IMS 的主要概念

Fig. 1 Main concepts of IMS

身份管理在应用方面的优势体现在资源发现能力、标识符管理能力、证书管理能力、身份属性管理能力、身份模式管理能力、身份保证能力、身份管理的可互操作能力。

区块链的去中心、不可篡改的技术特点为满足 IMS 的上

到稿日期:2018-01-21 返修日期:2018-04-13 本文受国家重点研发计划项目:异构身份联盟与监管基础科学问题研究(2017YFB0802300)资助。

董贵山(1974—),男,博士,研究员,主要研究方向为信息安全;陈宇翔(1993—),男,硕士,工程师,主要研究方向为信息安全,E-mail:chenyuxiang@std.uestc.edu.cn(通信作者);张兆雷(1985—),男,硕士,主要研究方向为信息安全;白 健(1989—),男,硕士,主要研究方向为密码学;郝 尧(1971—),男,高级工程师,主要研究方向为信息安全。

述要求提供了重要手段。但对其访问、透明性、同意用户授权信息被示出、互操作等的研究仍不充分，下面将基于已有研究成果进行分析。

2　传统身份管理的发展经验与基础

终端应用的多样化使管理身份愈发重要，一个人可能会在网上因使用不同应用而具有多种虚拟身份，从而带来很多不便。即便有类似 OpenID 连接可以提供单点登录功能（Single-Sign-On）来提供便利，也没有解决完全由消费者自我管理和存储敏感信息的问题。

2.1　身份管理及信任服务

早在 1997 年微软就做了尝试[3]，用身份联盟的方法让用户用相同身份登录多个网站，但其不能记住用户喜好等不良用户体验让微软转而集中精力发展中心化身份管理系统。典型的中心化登录过程如图 2 所示。但中心化管理的缺点也是显而易见的，一旦身份提供商（Identity Provider，IDP）不可用或丢失数据，所有的商家和客户都将被影响。

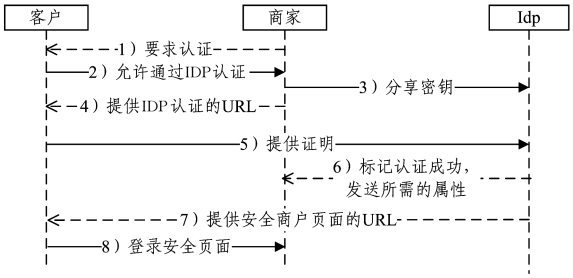


图 2　中心化登录过程

Fig. 2　Process of centralized login

2001 年成立的“自由联盟”对微软护照又做了尝试[4]，为安全断言标记语言（SAML）做出了贡献，用于在 IDP 和服务提供商之间交换认证和授权，大大推进了联盟身份的发展。但联盟的问题在于一旦认证组织不可用，用户就将得不到该组织的资源。

基于属性的认证[5]的特点是基于数据最小化和交易事物无关联性，很好地保护了隐私。

荷兰的 IRMA[6]（I Reveal My Attribute）利用加密和 ABC 实现 DIMS（Digital Identity Manangement System）系统，比如学生属性被教育机构签名而存在于你的证件卡上。但金融等需要追溯和监管的机构可能不会加入该 DIMS。

OAuth（开放授权）[7]是在用户客户端和服务提供商之间设置了一个授权层，允许第三方网站在用户授权的前提下访问存储在服务商的各种信息，用户不会提供自己的账号密码，而是以令牌的形式提供第三方网站。用户规定了该授权层令牌的权限范围和有效期。OAuth 的体系结构如图 3 所示。

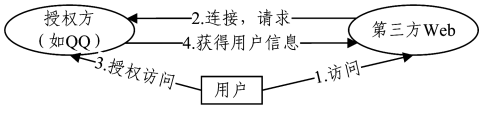


图 3　OAuth 的体系结构

Fig. 3　Architecture of OAuth

FIDO（Fast Identity Online）[8]的目的是改变目前主流的基于密码的在线身份验证技术，保证各厂商开发的强认证技术间的互操作性，逐步消除用户对密码的依赖，包括致力于“无密码体验”（生物特征）的 UAF 标准和“双因子体验”（口令和特定设备）的 U2F 标准，涉及范围如图 4 所示。除了在解决不同身份认证技术领域的“技术孤岛”问题上的优势外，FIDO 还致力于解决口令或短信验证码等传统移动端的认证方式的风险过于集中、输入不方便等问题，但距离实现广泛应用还有一定的距离。

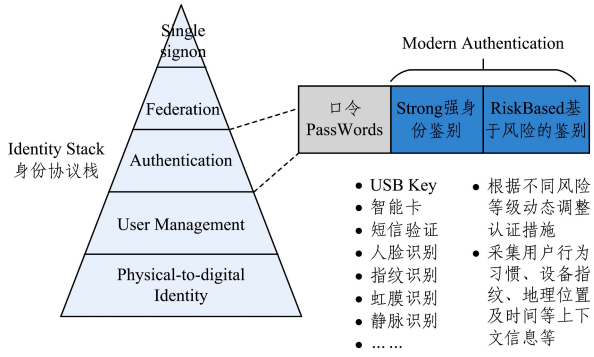


图 4　FIDO 范畴

Fig. 4　Category of FIDO

从几个案例来看，一个 DIMS 系统应满足如图 5 所示的条件。

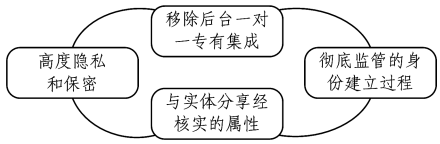


图 5　一个 DIMS 的特点

Fig. 5　Features of an ideal DIMS

在很长的时间内人们对电子身份管理系统的要求都不能得到满足，直到区块链技术的出现才得以改善。作为一个分布式账本平台（Decentralized Ledger Platform，DLP），天然的去中心结构为身份管理提供了新的解决思路，但是人们所熟知的基于比特币的区块链框架仍需诸多改进。

2.2　区块链

区块链作为比特币[9]加密货币的底层技术，最大的特点是不可变性，每个块都包含前一个块的散列，属于典型的基础设施层。其模型架构如图 6 所示。

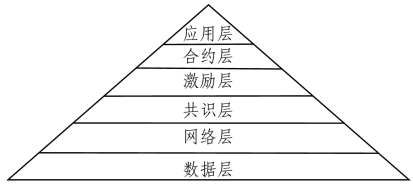


图 6　区块链模型

Fig. 6　Blockchain model

数据层封装了底层数据区块的链式结构，以及相关的非对称公钥数据加密技术和时间戳等技术，这是整个区块链技术中最底层的数据结构，是构建全球金融系统的基础，数十年的使用证明了其安全可靠，而区块链技术巧妙地将它们结合在一起。

网络层包括 P2P 组网机制、数据传播机制、数据验证机制。P2P 组网技术早期被用在 BT 这类 P2P 下载软件中，这

意味着区块链具有自动组网功能。

共识层封装了网络节点的各类共识机制算法，共识机制算法是区块链的核心技术，因为它决定了到底是由谁来进行记账，记账方式将会决定整个系统的安全性和可靠性。目前已经出现了 10 余种共识机制算法，知名的有权益证明机制(Proof of Stake，POS)、工作量证明机制(Proof of Work，PoW)、授权股份证明机制(Delegate Proof of Stake，DPoS)等。

数据层、网络层和共识层是构建区块链技术的必要元素，缺少任何一层都不能称为真正意义地使用了区块链技术。

比特币区块链对所有人公共可见、公开透明，但在身份管理应用领域出于隐私保护需求，可见的案例都将敏感数据脱离区块链(通常存于客户终端)，使区块链只起验证作用。

Onename. io[10] 允许创建区块链 ID 作为网络电子身份，验证时则采用了多个 IDP，以后可能会与社保号保险等具体电子凭证相关联。Qiy/Digital Me[11] 声称提供了以人为中心的访问、管理、分享个人数据，并提出了开发标准，但该标准仍有问题，且还未对公众使用。TrustTester 允许用户通过第三方可信平台证明他们自我披露的属性和商家交易，商家只能看到属性被可信机构验证而不知是何可信机构。SURFcontext 联盟[12] 提供教育组织间的功能来促进组织间合作，它们提供联盟身份管理服务，如果用户是这 120 家组织中某家的雇员，就可以用自己的凭据通过认证来获得商家折扣。

这些项目是先行者，不同层面的限制导致了其应用范围较小。下面以荷兰 Rabobank 的概念验证项目为例(Towards Self-Sovereign Identity using Blockchain Technology)进行详细说明[13]。

罗本银行的身份管理系统架构如图 7 所示。该方案基于比特币区块链，以用户设备为中心，将用户属性经过 Issuer(发布商)验证后(验证过程包括出示身份证、驾照等信息)存储在用户终端，并在区块链上对验证的属性进行哈希处理，数字签名后将“证明”存储在区块链，系统中不存在中心数据库，当用户需要获得 Acquirer(获得方)服务时，用户在自己的终端选择获得方需要的属性，点击同意分享，实现授权(步骤 1)，并发送该属性给 Issuer，Issuer 读取用户“同意”，该“同意”触发智能合约返回区块链存储该信息的相关结果(步骤 2)，将该信息在区块链进行验证(步骤 3)后签名发回用户，用户将验证过的属性数据发送给 Acquirer(步骤 4)，查找 Issuer 所签发的证明信息，完成认证(步骤 5)。

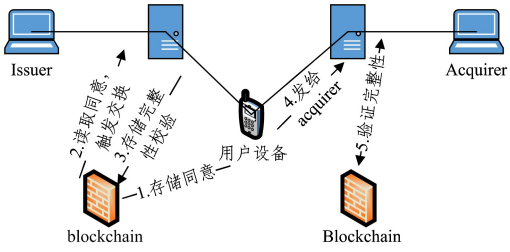


图 7 罗本银行的身份管理系统架构

Fig. 7 Rabobank's IMS architecture

该项目最大的特点是用户同意将自己的属性分享到别的域时才可以分享，符合 KYC(Know Your Customer)政策。用户完全管理自己的数据，区块链仅用于存储许可和完整性校验，借助哈希函数作为单向陷门函数的特点，在没有数据明文的情况下第三方在区块链上获得的数据无任何意义。因此实现了去中心化管理系统，用户完全拥有自己数据的主动权，也不存在中心化系统大量数据泄露的风险。

但这些早期尝试的项目的缺点也很明显，其大多使用了比特币区块链，比特币区块链中成千上万个节点都有分布式账本，每次验证需要众多节点同步数据库，花费的时间长达十几个小时，对用户认证很不友好。且比特币平台对所有人开放，没有商业理由吸引公司在该平台创建推广身份管理系统，此外，高额的软件许可费和第三方对用户行为的关联分析一定程度地泄露了隐私也阻止了这些项目的推广。

现有的 DIMS 大多处于验证阶段或针对具体应用而设计。面对生活场景中形形色色的验证，早在 2014 年就有一个名为世界公民的项目被 Chris Ellis 创造[14]，该项目是一个实际数字护照，使用区块链技术和加密程序实现，可以在线上线下验证自己的身份(见图 8)。

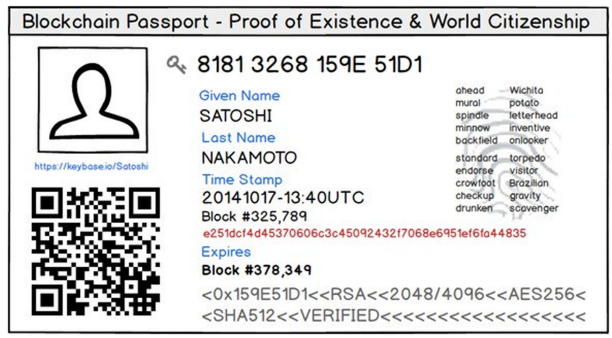


图 8 区块链身份证

Fig. 8 Blockchain identity

3 基于区块链的信任服务模型及优势

大数据时代为信任服务引入了更多的实体，如何构建网络身份的信任体系十分重要，区块链系统的弱中心化、公开透明、安全可靠为网络空间的信任服务提供了理论基础。

当前的身份管理机制在架构上面临着以下问题：各个单位的数据孤岛不能沟通、中心化管理系统的数据泄露风险高、数据认证格式和安全级别不同。针对以上问题，在身份管理中引入区块链来实现身份服务的统一与激励，在架构上通过去中心来降低数据泄露的风险，并促进多种信息和方式的融合。

从跨域、跨联盟身份管理的应用种类来看，采用的区块链模型不同于比特币为代表的公有链，任何人都可以参与记账，也不是只能在一个组织或实体内部记账的私有链，而是典型的联盟链，设定多个组织、人、公司、政府进行记账，用于产业内、联盟公司间的交易和审计等。

通过前文对国内外已有项目的分析，可以知道用户身份属敏感信息，用户和商家对系统有隐私保护的需求，而身份管理则要加强权威，从当前中心化管理系统面临的问题出发，考虑各方需求，系统架构不可完全去中心化，也不可完全中心化，因此采用跨域、跨联盟的联盟链框架。该框架可以通过交易过程中的密码学处理实现监管。区块链分布式存储、不可

篡改的特点是使用户获得数据操作主动权的重要手段，让研究人员能够在了解身份提供商、监管方、用户商家利益关系的基础上设计契合多方需求的解决方案。我们基于区块链分布式信任服务合约机制，参考 Hyperledger fabric 网络的运行机制，对通用联盟链模型进行分析（见图 9）。

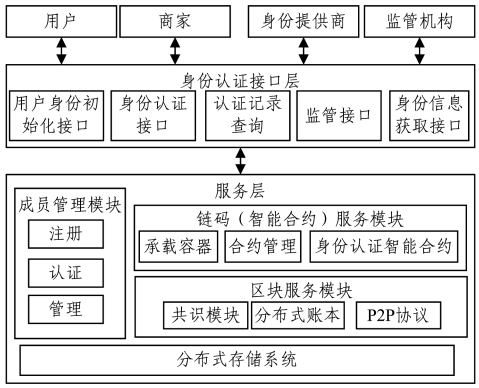


图 9　身份管理工具模型

Fig. 9　Identity management tool model

服务层提供基础区块链服务，包含 3 类逻辑结构：区块链服务模块、智能合约服务模块、成员管理模块。其通过系统中的时间或事件触发不同的模块，比如新节点加入触发成员管理模块的注册功能。

接口层为上层提供基本区块链操作接口，并设定了用户、商家、身份提供商、监管机构等几个实体，使得接口层能够为外提供基本身份认证服务，包括对商家、用户提供认证接口，对监管机构提供监管接口，同时与身份提供商接口对接，实现初始身份鉴别及登记。

接口层和服务层作为信任服务模型为外部应用提供基础的区块链服务，基于该模型将彻底改观现有中心化身份管理体系的现状，同时兼顾到用户隐私保护需求与监管需求。下面以注册和认证为例进行说明。

用户注册流程和认证流程分别如图 10、图 11 所示。

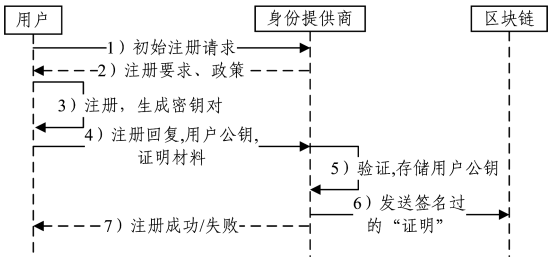


图 10　用户注册流程

Fig. 10　User registration process

1）身份提供商接到用户通过终端应用发起的注册申请。2）身份提供商选择注册要求，并将本次注册的相关政策发回用户。3）用户终端产生一对新公私钥，该公私钥对用户、身份提供商、区块链而言是唯一的。4）用户按政策要求选择属性、本人公钥及其他自由选择的属性等，将其发回身份提供商，并出示相关证明材料。5）身份提供商对用户证明材料进行验证，通过后保存用户公钥及关联用户，但不在本地保存用户数据，而是对属性数据进行哈希处理和签名处理，从而得到“证明”。6）将“证明”发送到区块链上进行加密存储。7）响应用户注册成功。

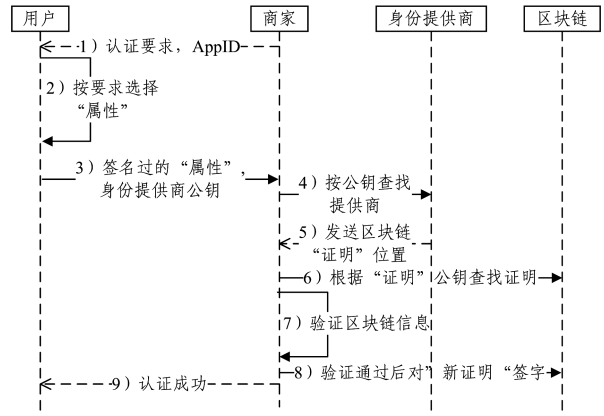


图 11　认证流程

Fig. 11　Authentication process

1）商家向用户发送随机数挑战，要求用户按政策认证所需的数据。2）用户按照认证要求的政策在终端选择之前注册时身份提供商认证过的数据属性。3）用户对挑战值签名，用公钥加密商家所需的属性材料，并提供身份提供商的公钥及关联信息发送给商家。4）商家根据提供的身份提供商信息，到身份提供商查找用户公钥、关联信息、区块链“证明”位置信息。5）身份提供商返回商家要求的信息。6）商家的终端应用自动到区块链查找“证明”信息。7）商家对用户提供的认证材料进行哈希处理，并与用身份提供商公钥签名过的区块链“证明”材料做比对，以验证认证数据的有效性。8）商家验证成功后，不在本地存储用户数据，而是对用户提供的有效数据进行哈希处理并签名，生成新的“认证”材料（带有时间戳等元数据）并发送到区块链做记录。9）返回用户认证成功信息。

在注册和认证协议中，用户、商家、身份提供商之间的信息交互都通过非对称加密技术来保证价值传输的安全性，即发送方对信息先用发送方私钥签名，再用接受方公钥加密，然后发送给接收方。接收方接收到信息后先用发送方公钥验证，再用接收方私钥解密。

认证步骤 2）体现用户对自己数据的控制和许可。信任传递通过区块链的去中心交换来承诺实现，体现在认证步骤 8）中生成本次认证的材料被商家签名记录在区块链中可供下次其他商家对用户认证时使用，几方关系如图 12 所示。

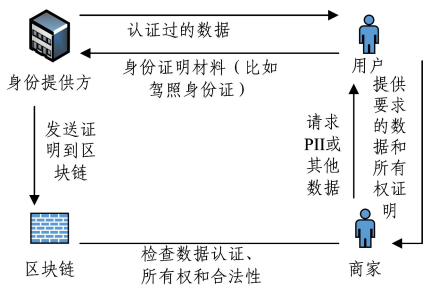


图 12　基于区块链的信任服务关系

Fig. 12　Relationship of trust service based on blockchain

由于底层区块链服务模型的支持，设计兼顾系统各参与方需求的注册、认证协议成为可能。借助区块服务模块增强

系统的可靠性、抗攻击性并实现分布式用户数据管理。借助智能合约模块定制特定场景来符合双方需求的“合同”，用代码执行法律并不遥远，可更好地保证公平性。成员管理模块维持系统各参与方有序进行，增加了系统的可扩展性。

首先，目前信任服务机制还不够成熟，基于市场需求、身份提供商及身份使用方的利益关系，以现有信任服务及身份认证为基础，结合区块链的优势特点，提出基于区块链的信任服务模型，使之提供全网统一的信任模型，支持多个身份提供商的共同接入、多种格式身份的安全认证，以及多种身份信息源认证方式的融合统一。

然后，所有的认证都是点对点发生的，用户数据存于手机终端，区块链只起到验证作用，管理机构则不用维护中心化数据库从而节约了大量成本，因为认证的真实性是由区块链上所有参与者共同验证和维护的，所以作为第三方的信用中介失去了价值。

其次，在联盟链的框架下，系统间的信息交互不再因为兼容性和互斥性导致部署成本高且连接困难，因为所有系统使用相同的技术协议，而参与方之间的认证规则也依照协议共识写入区块链作为标准，不得篡改。

最后，区块链智能合约可编程使得不同场景的管理机构根据需要使认证流程全自动化；通过在区块链嵌入预设好的认证规则，达到预定条件则自动完成，增加了用户体验并提高了工作效率。

4 应用案例介绍

由对典型的联盟链的分析可知，在基于区块链的身份管理应用中，区块链只用于去中心交换承诺、存储用户许可信息、进行完整性校验。区块链本身没有任何敏感信息，用户敏感信息都是通过验证后存储于用户终端，以实现更优的隐私保护和监管需求。当前的概念验证项目和应用案例虽不会完全契合上文通用的联盟链模型，在细节上也更为复杂，但在分析联盟链与身份管理结合的思想上是一致的，下文通过对比来加深理解。

从服务模型落实到需求上，在一个身份管理架构系统中通常会有以下角色：身份提供方，通过提供含有策略的认证模块来认证实体，比如安全断言标记语言(SAML)；Acquirer(获得方)，能够在同样的基础上设施 IDP 或请求权威机构发布的声明；Consumers(用户)，管理自己的声明。解决方案中利用 IDP 验证用户，成功后则将声明有效性存于区块链的智能合约中。

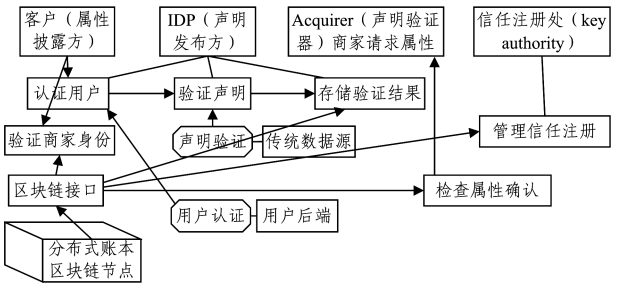


图 13 从底到上的架构

Fig. 13 Architecture from bottom to top

1)基础设施层

基础设施层作为声明的去中心化存储平台，由众多节点共同组成一个共享账本。声明的发布和撤销记录都存储于智能合约中。

2)应用层

对于每个 IDP 区块链上的智能合约，应用服务可以对用户产生认证和确认声明，可以自由部署所需要的服务。当反馈信息可以使之作出声明，IDP 就把结果写入一个区块链智能合约中。

3)业务层

声明在 IDP 处验证，用户把属性披露给商家，通过 key authority 管理信任注册。

针对比特币区块链所存在的问题，结合提出的 10 项原则[2]，我们分析对比 DIMS 和 ShoCard 应用两个相对成熟的案例。自治身份管理模型满足以下条件：

1)不依赖一个可信第三方；

2)商家能确定用户属性的有效性；

3)模型允许在必要时监管商家和用户行为。

区块链的优势在于能够大大降低信任成本、不依赖于中心化机构、信息不可伪造和篡改、自动执行智能合约等。

结合架构、协议和业务模型，用户端在 App 上用密钥对来管理身份。IDP 在区块链的智能合约中通过声明实体公钥(例如蓝牙信标)的方式来声明实体。

4.1 DIMS[15]

购买烟酒时要证明购买者的年龄大于 18 岁。目前需要物理提交政府签发的身份证给店员验证，店员可以检查身份证，但不能验证该证件是否是政府开具的。而且在验证时，顾客的其他信息如具体年龄、身份证号等不必要的信息也会泄露，且显示具体年龄远比只显示大于 18 岁敏感得多，这些问题都涉及了隐私保护问题。另外，用商家公钥加密用户，有选择性显示的声明远比直接出示身份证更安全。

用户在底层区块链平台产生公私钥对，通过多个 IDP 收集他的声明。一个实体用口令密码等在 IDP 处认证。IDP 可以分享用户要签署的信息来验证一个私钥的所有权。证明了私钥的所有权后，客户可以让可信的 IDP 存储关于他身份信息的声明。

在有隐私保护需求时，用户可以从主密钥以层次确定方式派生出密钥[16](见图 14)。只需提供从主密钥到子密钥的路径给 IDP，就可让主-子密钥关联来对同一个声明背书而不需要用户进行再次认证(见图 15)。

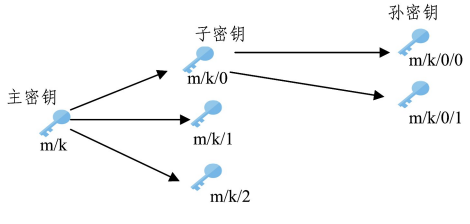
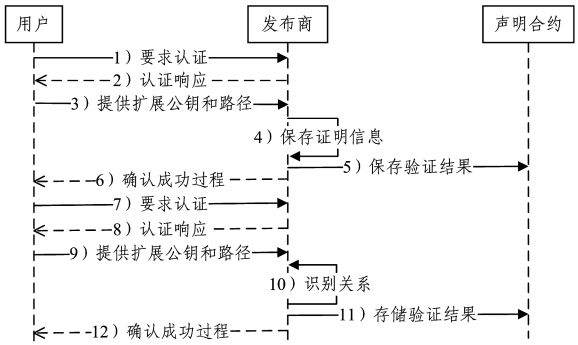


图 14 分层确定衍生密钥

Fig. 14 Hierarchical determination of derived keys

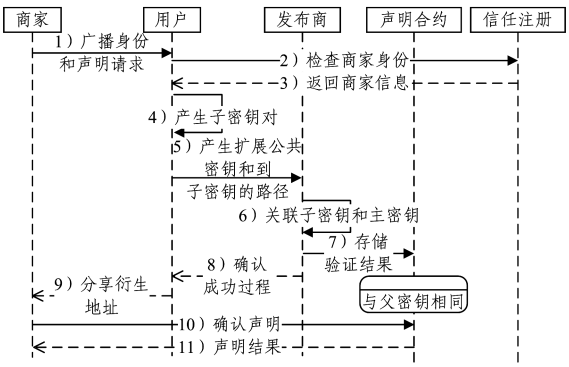


注：步骤 1）－步骤 6）建立证明所有权，步骤 7）－步骤 12）对相关密钥添加声明

图 15　属性证明协议

Fig. 15　Attribute attestation protocol

当用户需要向商家披露某个属性时，比如买烟酒时要透露是否成年，此时客户可以共享一个仅包含与年龄事务相关的声明的公钥。网上购物时，客户要先通过查看信托中心的公钥来验证商家所声明的身份。用该公钥加密就能实现只分享给该商家（Acquirer）相关声明，验证了商家身份后（见图 16 中的步骤 1）－步骤 3）），在用户端（层次算法）生成衍生密钥[16]（见图 14），把主密钥到衍生密钥的路径分享给 IDP，IDP 可以向子密钥分配相同的真值，用户之后使用衍生密钥就像使用主密钥一样。但对于不相关的第三者来说，不能确定两次事物是由同一用户发出。



注：步骤 1）－步骤 3）是商家身份鉴别，步骤 4）－步骤 11）是声明验证

图 16　商家声明验证

Fig 16　Verification of merchant's declaration

此时完成了派生密钥的声明，把这个密钥和带有声明真值的智能合约的位置分享给商家，商家则能验证声明是由信任机构出具的（见图 16 中的步骤 4）－步骤 11））。

由权威部门管理信任注册与客户声明被 IDP 验证相似。实体属于特殊组织（如本地银行），可以向权威部门证明（中央银行）自己私钥的所有权，中央银行则把这个信息添加到信任注册表（也是智能合约的一种），该过程类似图 15 中的步骤 1）－步骤 6）。

4.2　ShoCard

4.2.1　ShoCard 首次认证

ShoCard[17]较早涉足区块链身份管理领域，相对成熟，形成了自己的落地产品，最典型的是与 SITA 航空合作的基于区块链的数字身份认证 APP。人们在跨国旅行时，在机场安检的过程中要不断出示护照、登机牌、面部核验等信息，这些信息组成的数字身份是个人与服务商互动的关键，服务流程如下。

1）注册环节。用户在终端下载 APP 后自动生成 ShoCardID 和关联公私钥对，用户使用该 APP 对身份证件（如护照、驾照等）拍照，APP 会读入证件上的元数据（如姓名、号码等），加密并存储在本地终端 APP。读取的数据经过密码学处理（如哈希、加密等）创建验证字段后发到区块链，同时对姓名、护照号等元数据哈希处理，再用存储在 APP 的私钥签名后发送到成员接口服务器用于记录区块链的验证字段。

2）完成注册后，首次认证（见图 17）。

①客户向商家出示物理身份证明（见护照等），商家检查是否是客户本人。该步骤与正常安检基本相同。

②步骤①通过后，用户可通过 APP 出示二维码，商家扫码连接到成员管理服务器。

③商家在成员管理服务器中查询并获取指向客户在区块链的记录，验证所有权，包括：用户出示的 ShoCardID 与记录是否一致、电子信息与物理证件是否一致、商家机器对用户面部进行识别的结果与证件记录是否一致。

④所有权验证完成，商家请求成员服务器对客户验证通过，成员服务器生成认证证书，证书包括 ShoCardID、证件照片、认证通过令牌。对证书进行哈希处理签名后得到“证明”并发送到区块链存储，并在服务器存储索引“证明”的位置。

⑤成员管理服务器向客户颁发认证通过证书。

⑥客户 APP 收到证书后对其加密并存储到本地，可用于对以后有相同要求的商家进行认证。此时用户终端 APP 包含的信息（安全加密消息或安全信封）有：指向成员服务器的指针和区块链相应记录、用于面部识别对比的证件照、首次认证的证书（令牌）、指向证书验证记录的指针。

⑦先对终端 APP 的“安全加密消息”进行整体签名，再用对称密码加密发送成员管理服务器（用户终端也有备份）以供以后检索，其中对称密钥存储于本地终端。

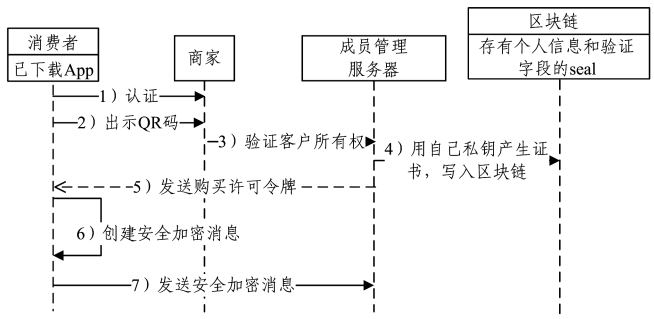


图 17　客户的第一次认证

Fig. 17　Customer's first authorization

4.2.2　第二次及以后认证

当用户到了不同地区，用户终端（可以无网络）的认证过程如下（见图 18）。1）商家要求认证。2）用户出示二维码和对称密钥给商家。3）商家通过扫描二维码来连接到成员管理服务器以查询区块链上的相关资料（上传资料包含第一次认证结果，其他相同）。4）区块链和成员管理服务器将相关资料返回给商家。5）商家收到资料后，APP 自动执行以下操作：用户公钥验证安全加密信息和区块链元数据；验证物理证件照片等信息并与安全加密消息进行对比；用前一用户公钥来验证证书、证书对应区块链的记录和证件照，以及上一商家的许可令牌。6）与用户肖像进行比对。7）通过验证。

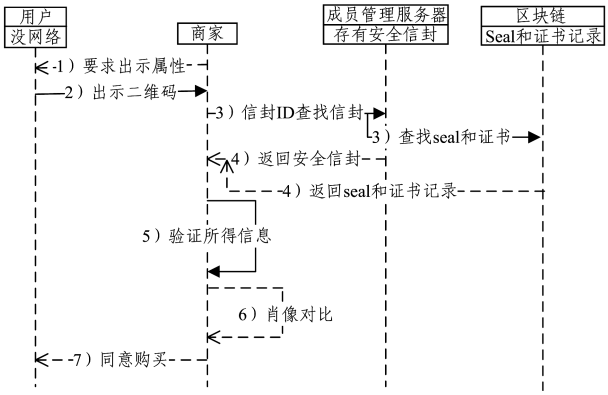


图 18 客户第二次(及以后)认证

Fig. 18 Customer's second (and later) certification

ShoCard 是早期尝试区块链身份管理的公司并发展至今,其认证和注册流程具有代表性。其技术思路形成共识,即用户终端存储个人数据,区块链作为去中心的交换承诺,保证信息的有效性和完整性。其他公司方案都在此技术共识基础上加入了自己的特点,比如:Uport[18] 身份依托于以太坊,在该技术路线上的创新是去除了身份提供商 IDP,用分级的智能合约方式实现以用户为中心的账号管理和依托账号管理实现非区块链应用身份的关联,具有很好的兼容性,并被后来国内的 IDHub[19],SelfKey[20] 等方案所借鉴;Civic[21] 在该技术思想上引入了通证激励机制,身份管理中的通证可以表示比加密货币更高维度的价值,如身份权证、积分、信用、服务、资产等。可见基于区块链的身份管理还在不断地发展中,但已经形成了一些技术路线的共识,以期提供更好的服务。

5 对比分析

通过重点分析两种用例可以看到,在区块链应用中,用户敏感信息都存于手机终端,但场景不同,在进入商店买酒时客户通常要提供身份证、驾驶证等,但他们不希望把名字、地址等展示出来,此时仅选择特定属性分享即可,且不同场合要查验的信息有所不同。而对于跨地区旅行,安检每次查验的信息较多且差异变化小,验证信息较为全面。

由表 1 可知,DIMS 和 ShoCard 都满足了分布式身份管理系统的主要性能指标,不依赖可信第三方,商家可确定用户属性有效及监管要求。但是在用户体验上有所差别,DIMS 在隐私保护方面具有优越性,且由于应用场景相对简单而不需每次查验物理证件。

表 1 DIMS 方案和 ShoCard 方案的对比

Table 1 Comparison of DIMS and ShoCard

	不依赖可信第三方	商家能确定用户属性有效	监管	检查物理证件	隐私保护(无关联和不可追踪)
DIMS	√	√	√	×	√
ShoCard	√	√	√	√	×

DIMS 使用密钥衍生技术,对用户来说可以每次使用不同的一次性公私钥(从主密钥衍生),对此参考 CryptoNote2.0 方案,引入跟踪密钥,截断地址帮助监管机构在必要时追溯责任,使得认证具有良好的隐私保护。在第三方看来:认证事物具有不可追踪性,所有网络中的成员都可能是被认证的一方;所有的认证方也无关联性,任意两次认证事物不能确定是在同一认证方认证。

理论对比 DIMS 更具优势,ShoCard 对用户使用体验较为繁琐,隐私保护也有所欠缺,但由于其率先实践,积累了很多实践经验。

如图 19 给出了金融和公司的身份管理用例,但值得注意的是金融机构往往更加倾向于选择使用私有链技术,参与节点的资格会被严格限制。由于参与节点是有限的和可控的,因此私有链往往有极快的交易速度、更好的隐私保护、更低的交易成本,不容易被恶意攻击,并且能做到身份认证等金融行业必需的要求。相比于中心化数据库,私有链能够防止机构内单节点故意隐瞒或者篡改数据,即使发生错误,也能够迅速发现来源。

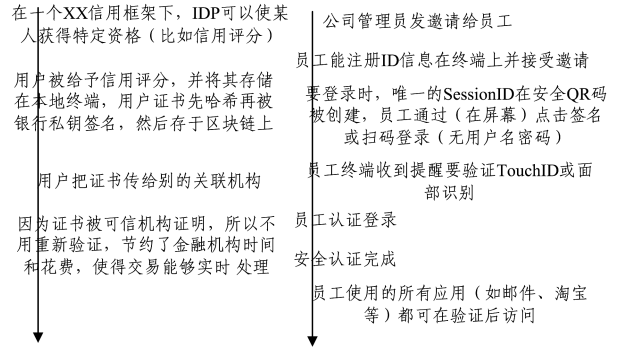


图 19 金融和公司的身份管理用例

Fig. 19 Identity management comparison of financial and corporate use cases

通常应用于企业政府的身份管理会选择联盟链,私有链和联盟链之间的设计隐私权限会有不同,联盟链中的权限设计要求往往会更为复杂。无论是哪种链都没有绝对优劣,往往需要根据不同的应用场景来选择适合的区块链类型,不同方案的侧重点也有所不同(见图 20),年龄证明侧重便捷性,机场安检侧重安全性,因此流程设计有简略和繁琐的差别。

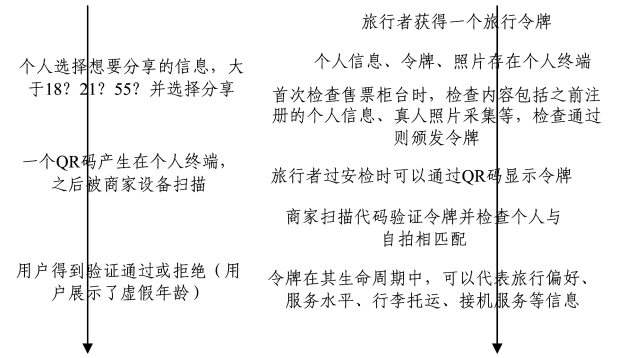


图 20 用户年龄证明和机场安检场景的比对

Fig. 20 Comparison of user's age proof and airport security check

结束语 学者们纷纷提出区块链的应用场景设想,比如设备寿命管理、工作绩效激励、供应链物流、资产证券化、数据版权保护等,各种应用的本质都会涉及身份管理,在陌生的环境中,区块链为互不了解的节点间建立了可靠信任,由此也把区块链称为价值互联网的曙光。

首先,从全篇的分析可以看出,由于应用场景和需求的不

同，基于区块链的身份管理持续发展，不断有新功能或插件应用加入进来。比特币使用公有链，金融机构使用私有链技术（写账本的权限由单一组织享有），企业、政府则多考虑联盟链技术。

其次，随着身份管理应用场景的需求逐渐复杂，其区块链技术变得越来越复杂，其特点是系统内不同的节点有不同的权限，有的节点只能查看部分区块链数据，有的节点能够下载完整的区块链数据，有的节点负责参与记账。这可能会使得私有链、联盟链、公有链的边界逐渐模糊。

最后，从区块链本身的特点及相关实践来看，身份管理是真正的受益者，因为可以帮助建立单一客户视图并简化节点加入和管理，这是一个技术范式，与关系数据库类似，即有多种实现方式，每种实现都有各自的优缺点，私有链和公有链的不同风格也是如此。挑战与机遇并存，区块链的发展将会给公司、政府、金融等各行业的中心化身份管理系统带来冲击，在降低成本以及提高可靠性、安全性方面具有深远影响。

参 考 文 献

[1] ITU-T X. 1250《Enhancing Trust and Interoperability in global identity management》[EB/OL]. [2018-08-19]. http://www.zbgb.org/129/StandardDetail2192142.htm.

[2] Christopher Allen. The Path to Self-Sovereign Identity[EB/OL]. [2018-08-19]. http://www.coindesk.com/path-self-sovereign-identity.

[3] MSN Historical Timeline: A brief history of milestone events in the life of MSN from the past ten years [EB/OL]. [2018-08-19]. http://www.microsoft.com/presspass/press/2002/nov02/11-08MSN8GlobalTimeLine.mspx.

[4] STAAIJ R V D. Handboek identity & access management[M]. Netherlands: Academic Service, 2014.

[5] KONING M, KORENHOF P, ALPÁR G, et al. The ABC of ABC: an Analysis of Attribute-Based Credentials in the Light of Data Protection, Privacy and Identity[C]// Proceedings of the 10th International Conference on Internet, Law & Politics. 2014: 357-372.

[6] ALPÁR G, JACOBS B. Credential Design in Attribute-Based Identity Management[M]. Wolf Legal Publishers, 2013: 189-204.

[8] 胡可欣. FIDO UAF 认证协议的安全性研究[D]. 合肥：中国科学技术大学，2016.

[9] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. [2018-08-19]. https://bitcoin.org/bitcoin.pdf.

[10] OneName: The Bridge Between Physical & DigitalIdentity | Blockchain for the Billions on WordPress.com. [EB/OL]. [2018-08-19]. https://rywalk.wordpress.com/2015/02/13/onename-the-bridge-between-physical-digital-identity.

[11] Qiy Foundation | Technology[EB/OL]. [2018-08-19]. https://www.qiyfoundation.org/qiy-scheme/what-is-a-scheme/technology.

[12] SURF | Op SURFconext aangesloten diensten[EB/OL]. [2018-08-19]. https://www.surf.nl/diensten-en-producten/surfconext/op-surfconext-aangesloten-diensten/index.html.

[13] ANDREW M, et al. PoC KYC on blockchain with Tradle. Tech. rep. Utrecht: Rabobank Nederland, [EB/OL]. [2018-08-19]. https://www.newsbtc.com/2015/08/24/tradle-integrating-blockchain-technology-with-kyc-requirements.

[14] Estonia's new e-residents are surpassing the country's birth rate [EB/OL]. [2018-08-19]. https://thenextweb.com/eu/2017/07/25/estonias-new-e-residents-surpassing-countrys-birth-rate.

[15] DJURI B. Towards Self-Sovereign Identity using Blockchain Technology [EB/OL]. [2018-08-19]. http://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf.

[16] BERGAN T, ANDERSON O, DEVIETTI J, et al. CryptoNote v 2.0[EB/OL]. [2018-08-19]. https://cryptonote.org/whitepaper.pdf.

[17] TRAVEL identity of the future[EB/OL]. [2018-08-19]. https://shocard.com.

[18] uPort The Wallet is the New Browser - Medium [EB/OL]. [2018-08-19]. https://medium.Com/@ ConsenSys/uport-the-wallet-is-the-new-browser-b133a83fe73%7B%5C#%7D.1l0vsfq2p.

[19] IDHub 数字身份白皮书[EB/OL]. [2018-08-19]. http://www.idhub.network.

[20] SelfKey[EB/OL]. [2018-08-19]. https://selfkey.org/wp-content/uploads/2017/11/selfkey-whitepaper-en.pdf.

[21] Civic WHITEPAPER[EB/OL]. [2018-08-19]. https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf.

[22] ANTONOPOULOS A M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies[M]. USA: O'Reilly Media, Inc., 2014.

[23] Hyperledger. Project Charter[EB/OL]. [2018-08-19]. https://www.hyperledger.org/about/charter.

[24] ANONYMOUS. New kid on the blockchain[J]. New Scientist, 2015, 225(3009): 7.

[25] SWAN M. Blockchain thinking: the brain as a decentralized autonomous corporation[J]. IEEE Technology and Society Magazine, 2015, 34(4): 41-52.

[26] ETHEREUM White Paper. A next-generation smart contract and decentralized application platform [EB/OL]. [2018-08-19]. https://github.com/ethereum/wiki/wiki/White Paper.

[27] Merkle R C. Protocols for Public Key Cryptosystems[C]// 1980 IEEE Symposium on Security and Privacy. IEEE, 2014: 122-122.

[28] ALLISON I. Ethereum's Vitalik Buterin explains how state channels solve privacy and scalability[EB/OL]. [2018-08-19]. http://www.ibtimes.co.uk/ethereums-vitalik-buterin-explains-how-state-channels-address-privacy-scalability-1566068.

[29] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: Decentralized Anonymous Payments from Bitcoin[C]// Security and Privacy. IEEE, 2014: 459-474.

[30] DAVID B. Blockchain revolution. Amsterdam[EB/OL]. [2018-08-19]. http://www.slideshare.net/15Mb/blockchain-revolution.

[31] DAVID B. Identity is the new Money[EB/OL]. [2018-8-23]. http://www.dgwbirch.com/words/book-identity-is-the-new.html.

[32] Scalability - Bitcoin Wiki[EB/OL]. [2018-08-19]. https://en.bitcoin.it/wiki/Scalability.

[33] Building trust in government[EB/OL]. [2018-08-19]. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?Htmlfid=GBE03801USEN&.