基于区块链的高校隐私保护策略研究①

林超　沙锋
（厦门理工学院信息中心　福建厦门　351024）

摘　要 高校在日常教学管理过程中经常会涉及个人信息收集、使用及公布，数据在传输、公布的过程中可能存在隐私信息泄露，现有的中心数据库可能被攻击导致数据泄露，高校大学生经常使用互联网产品容易导致信息被收集，在大数据时代可以通过对非隐私数据关联分析来获取隐私数据。高校在做好隐私保护策略的同时应采取更先进的技术来防止信息泄露，区块链去中心化可以有效地避免中心化数据库被攻击的问题，同时区块链在身份管理上有天然优势。文章对比分析了主流区块链隐私保护技术的优缺点，发现零知识证明技术更为适合高校运用，针对零知识证明重点介绍了Hawk、Mediledger、Identity Mixer三种方案，对三种方案的身份管理和具体应用场景进行分析，选取合适的方案为高校隐私保护提供参考。
关键词 隐私保护；区块链；零知识证明

Research on Privacy Protection Strategies of Universities Based on Blockchain

Lin Chao　Sha Feng
（Information Center，Xiamen University of Technology，Xiamen，Fujian，351024，China）

Abstract Colleges and universities often involve the collection，use and publication of personal information in the daily teaching management process，there may be leakage of private information during the transmission and publication of data，the existing central database may be attacked and result in data leakage，university students often use internet products are easy to cause information to be collected，in the era of big data，private data can be obtained by analyzing non-private data. Colleges and universities should adopt more advanced technology to prevent information leakage while doing a good job in privacy protection strategies，blockchain decentralization can effectively avoid the problem of centralized database being attacked，and the blockchain

①本文系 2018 年福建省中青年教师教育科研基金项目“基于区块链的高校师生隐私保护机制研究”（项目编号：JZ180203）的研究成果之一。

has natural advantages in identity management. The article compares and analyzes the advantages and disadvantages of mainstream blockchain privacy protection technology, and finds that zero-knowledge proof technology is more suitable for universities, aiming at zero-knowledge, three solutions of Hawk, Mediledger and Identity Mixer are introduced, analyze the identity management and specific application scenarios of the three schemes, choose a suitable plan to provide a reference for privacy protection in colleges and universities.

Keywords Privacy Protection; Blockchain; Zero-Knowledge Proof

1 引言

随着移动运营商实名细则和实名认证条例的实施，互联网用户无法做到网络隐形，随之而来的是个人信息泄漏等一系列问题：黑客通过网络盗取用户信息并进行信息贩卖，不法分子利用信息进行诈骗。2015年国家发布了《非银行支付机构网络支付业务管理办法》[1]，要求支付机构在采集、存储、传输和使用客户信息时采用“最小化”原则，要求不得存储银行卡芯片或磁道信息。这个办法的出台是为了保护用户的隐私，然而随着特殊监测的需要会对网络用户进行监控以应对威胁或牺牲了用户的隐私[2]。隐私保护不仅需要监管部门加强网络管理，也需要用户加强防范，具备个人隐私保护意识，同时随着信息化的发展，各种应用爆发式增长，用户的隐私更容易被各应用服务商获取，这就需要网络管理部门制定相应的信息保护机制，同时也需要用户采取相应的措施以规避个人重要信息泄漏。总之，个人信息安全已突破了传统的安全领域，尤其在数据传输过程中面临着敏感信息的泄漏，如何兼顾数据共享服务和信息安全保护，已成了高校亟需解决的一个重要课题。

2 高校师生隐私问题

目前，各高校对个人隐私保护问题没有足够的重视，由于信息技术落后及保护意识淡薄，高校常有发生师生的隐私信息被公布到互联网上或数据泄露[3]。大学生本身就缺乏自我保护意识，尤其在没有高校个人信息保护政策的现状下，移动互联网收集信息的现象又很普遍，个人数据不经意就被人获取，不管个人是自愿的还是被迫的。虽然有的收集的并不是敏感信息，但是经过大数据技术处理可以将以前可能公开的信息或者不敏感的信息进行重组而成为隐私信息。

大学生很喜欢使用朋友圈，会在朋友圈发布个人爱好、照片、课程、家庭地址等信息，尤其喜欢将自己的生活情况发布到朋友圈，如什么时候起床，在哪里吃早餐，在哪里上课、上什么课程，在哪里自习、走哪一条路，还会附上照片，显示地址，这些信息虽然不是秘密的信息，但是经过大数据处理，就可以分析出学生所在的学校、专业、班级、年龄、作息时间、行为轨迹、家庭住址、父母职业等信息。大学生同样喜欢网络购物，网购行为容易将身份证号、手机号、银行卡号等敏感信息泄露[4]。在大数据背景下个人信息容易泄露的主要原因是我国个人信息保护法律缺乏体系，个人信息保护法律缺乏可操作性，个人隐私保护缺乏监管，个人信息保护范围缺乏清晰的界定，同时缺乏先进的隐私保护技术。因此，高校应该设立专门的信息保护部门与信息保护专员，制定师生个人信息保护策略，严格监督执行，加强宣传及采用更先进的技术手段。区块链在身份管理上有天然的优势，能有效地保护个人的隐私信息。

3 区块链隐私保护技术

区块链为身份认证管理带来了重大的变革，其去中心化特征使得用户在获得个人数据控制权的同时不必担心中心化数据库数据泄露的问题，简化了数据传递的过程，但也给用户隐私保护带来了挑战，因为区块链在分布式节点之间进行数据广播就需要公开发送地址、接收地址、交易等信息。虽然区块链地址的创建与身份无关，而且也不需要可信第三方参与，但是在区块链交易的过程中可以对其传播的轨迹进行分析从而推测出这一区块的用户身份。目前通过区块链交易进行分析推测出用户隐私信息的研究有很多，根据其分析的目的不同可以分为两类：一类是通过分析某一地址相关的交易记录来获取该地址的规律，从而推断出用户的身份；一类是通过区块交易设计中存在的知识对不同的地址进行聚类获取同一用户的多个地址。因此，很有必要采取相应的隐私保护机制尽可能地隐藏数据的信息量及其关联的知识。目前主流的区块链隐私保护技术主要有八种，下面将对其优缺点进行总结。

3.1 混合技术

混合币机制有基于中心节点和去中心化混币机制两种[5]。第一种混币过程是由第三方节点集中执行，用户先将资金发给第三方节点，第三方节点将收到的资金拆分为更小的数额分别发往不同的收款地址。由于资金经过第三方节点进行处理干扰了资金流向，使攻击者难以跟踪到用户资金流向。但是第三方会收取服务费甚至窃取资金，并且第三方知道资金的流向，其日志一旦泄露用户的权益就无法得到保障。第二种去中心化的混币过程是通过混币协议实现，去除了第三方混币服务，混币的过程是由多个用户共同完成，混币的安全不依赖于第三方，用户无须支付混币服务费。但是混币协议容易被攻击，为解决这个问题往往需要改进混币算法，从而增加了混币的计算成本，进而影响了混币的效率。

3.2 隐秘地址技术

隐秘地址技术通常是使用参与双方都知道的一次性地址，第三方没有接收到私钥无法对地址的历史交易进行分析，但是通过事务图分析发送方到一次性地址再到接收方之间的关系还是可以获取交易的流向，即使在一个交易中采取多个一次性地址也不能解决地址暴露的问题[6]。

3.3 加密技术

非对称加密技术是先用接收方的公钥对交易数据进行加密，然后将加密后的数据发送给接收方。这一方案的缺点是非对称加密算法不适合加密较大的数据量，而区块上的交易数据往往比较大。采用对称加密算法能加密大的数据量，但是对称加密算法需要秘钥协商，秘钥协商过程需要进行大量的消息广播和握手。这种方式效率比较低，同时由于区块链是个分布式系统，发送方可能在短时间内网络或者系统不能用从而导致交易无法完成。同态加密[7]方便了交易的审核且不会泄露交易的实际数额，但是全同态加密的计算开销大，效率低下。

3.4 环签名技术

环签名[8]使用其他公钥和自己公钥的密钥组进行环形签名，第三方能够验证生成的签名是环里的某个密钥签的，但是无法判断是哪个密钥签的。环签名没有设置管理员，只有环成员，环成员间也不需要合作，签名方自由选择他人的公钥加入自己的集合，集合中的成员甚至不清楚自己被加入集合。由于环签名无法提供签名者，监管起来就很困难。

3.5 离链存储技术

离链存储将数据划分为公共和隐私两部

分，公共数据存储在区块链上，隐私数据离链存储[9]在可信的第三方。区块链本身或者节点不再需要另外的访问权限，链上的交易发挥着无中心传递信任的作用，支持参与方向其他参与方在保密其交易细节的情况下进行交易。在离链存储交易信息的时候需要第三方代理维护，因此也带来了引入第三方的弊端。

3.6 状态通道技术

状态通道技术是将资金托管在区块链上[10]，将交易的最终结果放在支付通道。状态通道是用户之间临时构建的支付通道，在执行交易时一方将资金存入智能合约，交易双方交换密码承诺指定资金在通道关闭时如何分配。每次使用通道时都会创建新的承诺，显示新的余额，参与方可以单方面取消通道。

3.7 安全多方计算

安全多方计算[9]要求参与方协同工作，没有一方具有访问所有数据的权限，因此隐私信息不会被泄露。但是多方计算效率低下，同时要求参与方必须是可信的。

3.8 零知识证明

零知识证明分为非交互式和交互式两种协议，允许在不泄露语句外任何信息的情况下参与的一方向另外一方证明语句是真实的。交互式零知识对系统时间和资源消耗比较大，因此常用的是非交互式零知识证明协议。zk-SNARK是比较有代表性的非交互式零知识证明[11]。

zk-SNARK采用的是同态隐藏技术，在区块链的应用当中，用户不必透露自己的信息就能验证自己想要验证的，能有效地解决信息过度分享的问题。但是zk-SNARK在执行前需要中心化产生验证密钥和证明密钥带来了信任风险，同时zk-SNARK的计算复杂度和安全性都依赖椭圆曲线的计算，每一笔交易都需要大量的内存和执行时间。

4 区块链隐私保护案例

随着区块链在智能合约、公证、审计、物流等领域的应用，通过上面的分析比较我们发现零知识证明比较适合高校信息保护。目前，去中心化的信息共享也越来越多地采用零知识证明协议。下面具体介绍几种区块链方案。

4.1 Hawk

Hawk[12]作为智能合约的零知识应用提出，其将智能合约分为公有和私有两部分。公有合约放在区块链上，私有合约不上链，通过密码协议来管理公有合约筹集、持有和分配交易资金，由可信的第三方代理各参与者执行私有合约，执行私有合约需要验证用户的权限，可信的第三方可以终止智能合约却不能影响结果。为了保证交易的安全性，公有合约会在私有合约没有被正确执行的情况下退还托管的资金，而且会要求第三方在公有合约中存入保证金以免第三方不履行合约。区块的参与方身份也对管理者隐藏，管理者仅能看到参与者在智能合约上推托的资金以及私有合约输入的指令。

4.2 Mediledger

Mediledger针对隐私问题使用了三种核心技术[13]：执行电子产品代码信息服务标准；根据业务规则执行智能合约，将单位令牌化，限定了成员所有权和时间，并通过智能合约进行保管权移交；采用zk-SNARK进行医疗隐私保护。Mediledger是基于联盟链设计的，只有被授权的制造商才允许在区块链上供应相应的序列化单元，其流程如下：

交易方甲通过API向客户端发起指令请求向交易方乙转移序列单元；交易方甲计算自己的秘钥哈希值及其身份证明作为区块事务；交易方甲生成一次转移说明的电子产品代码信息；交易方甲向交易方乙发送电子产品代码信

息及区块事务值。

交易方乙验证交易方甲的信息，并生成自己的秘钥哈希值和自己的身份证明作为自己的区块事务；交易方乙将交易发送到验证节点；验证节点上的智能合约对交易双方的身份证明进行验证，如果有效，就将事务中提交的秘钥哈希值更新到区块链上；新的哈希值就代表序列单元从交易方甲转移到交易方乙。

4.3 Identity Mixer

Identity Mixer[14]使得参与方可以实现强认证，参与方可以自主选择想要共享的属性，同时可以防止对不同认证间进行关联分析，Identity Mixer协议主要包括4个环节。

建立环节，CA产生签名秘钥并公布公钥。

注册签发环节，用户节点产生秘钥并创建注册证书请求，并在权威处注册自己的属性，通过验证以电子证书的形式签发用户属性，然后将凭证存储在用户端。

签发展示环节，在用户访问不同的应用时，访问控制策略决定了用户在展示令牌中展示哪些属性、哪些凭证或相关的属性谓词，并指定证书颁发机构公钥对用户属性进行认证。如果用户同意公示政策信息，就从最早的凭证里导出符合要求的展示令牌。

验证环节，验证方采用CA的公钥对令牌是否符合访问控制策略进行验证。

Identity Mixer 有助于避免CA对用户认证关系进行关联分析，就算是CA也无法将令牌凭证链接到原来的注册证书，也不能对用户导出的令牌进行关联性分析，而且其支持披露最小属性，没有任何多余的信息。

4.4 方案比较分析

对3种应用方案进行比较，如表1所示，从身份管理和加密代币的隐私保护策略来看，提高隐私保护一般都需要扩大数据的存储，同时会消耗计算力。这3种方案都有其特定的应用领域，且会根据行业的需要搭配不同的隐私策略，零知识证明策略现被越来越多的方案采用，代币Zerocash是目前隐秘效果最好的。区块链目前更多地被应用于身份管理，需要考虑行业的政策法规、参与各方的诉求、系统扩展性、计算开销、监管要求、通信开销、隐私保护及用户体验等要求。通过比较分析可以发现，针对高校的应用场景比较适用的是Identity Mixer方案。

表 1　三种应用方案比较

方案	零知识证明	数据存储	应用领域	其他隐私策略
Hawk	智能合约管理	公有和私有	资金交易场景	访问权限控制
Mediledger	Zk-SNARK	各参与方	医药领域	无
Identity Mixer	匿名证明	用户端	企业级身份管理	盲签名

5　结束语

移动互联网的兴起为生活带来便捷的同时，也给个人信息保护带来了挑战，尤其在大数据时代，可以通过对非隐私数据进行关联分析获取个人的隐私数据。而高校大学生很喜欢使用互联网产品，更容易将自己的信息暴露出去。高校在做好隐私保护策略的同时，更应采用更为先进的技术来防止隐私信息泄露，而区块链在身份管理上有其特有的优势。本文对比分析了当前主流的区块链隐私保护技术，

总结分析了各类技术的优缺点，零知识证明具有存储量小、最小量信息透露、全方位隐私保护的特点，较适合高校师生隐私信息保护。针对零知识证明，本文重点介绍了Hawk、Mediledger、Identity Mixer三种常用的方案，对其身份管理及具体应用场景进行介绍和分析，选取Identity Mixer作为高校隐私保护方案，为未来高校隐私保护提供参考。

参考文献

[1] 银行专家. 非银行支付机构网络支付业务管理办法[OL].[2015-12-28].http://www.gov.cn/gongbao/content/2016/content_5061699.htm.

[2] 梁春阳. 我国网络舆情研究文献计量分析[J]. 图书馆理论与实践，2015，2：44—49.

[3] 赵海平，赵安琪，付少雄. 高校个人信息保护政策研究及启示——以2019年QS世界大学排名前100名高校为例[J]. 图书馆杂志，2019，38(8)：28—33.

[4] 付卓婧. 大数据时代高校学生信息隐私保护机制研究[J]. 青年时代，2017，35：77—78.

[5] 祝烈煌，董慧，沈蒙. 区块链交易数据隐私保护机制[J]. 大数据，2018，4(1)：50—52.

[6] HEARN M. Merge Avoidance：Privacy Enhancing Techniques in the Bitcoin Protocol[EB/OL].[2018-05-10]. https://www.coindesk.com/merge-avoidance-privacy-bitcoin.

[7] 刘滋润，王点，王斌. 区块链隐私保护技术[J]. 计算机工程与设计，2019，40(6)：1571.

[8] YUAN C，XU M X，SI X M. Research on a New Signature Scheme on Blockchain[EB/OL].[2018-05-10]. https://www.hindawi.com/journals/scn/2017/4746586/.

[9] SASSON E B，CHIESA A，GENKIN D，et al. SNARKs for C：Verifying Program Executions Succinctly and in Zero Knowledge[M]//Advances in Cryptology-CRYPTO. Berlin：Springer，2013：92—106.

[10] GREEN M，MOERS I. Bolt：Anonymous Payment Channels for Decentralized Currencies[C]//ACM SIGSAC Conference on Computer and Communications Security. ACM，2017：473—488.

[11] SASSON E B，CHIESA A，GENKIN D，et al. Zerocash：Decentralized Anonymous Payments from Bitcoin[C]//Security and Privacy. IEEE，2014：551—473.

[12] KOSBA A，MILLER A，SHI E，et al. Hawk：The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts[C]//Security and Privacy. IEEE，2016：840—856.

[13] MENDING J，WEBER I，WIL VDA，et al. Blockchains for Business Process Management-Challenges and Opportunities[EB/OL].[2018-01-23]. https://www.researchgate.net/publication/316076240_Blockchains_for_Business_Process_Management_-_Challenges_and_Opportunities.

[14] Hyperledger. Project Charter[EB/OL].[2018-05-10]. https://www.hyperledger.org/learn/white-papers.