区块链应用中的隐私保护策略研究

董贵山 陈宇翔 范 佳 郝 尧 李 枫
(中国电子科技集团公司第三十研究所 成都 610041)

摘 要 近年来,人们对身份管理系统和以用户为中心的自主权身份提出了越来越多的隐私保护需求。区块链作为解决数据隐私安全问题的重要手段,被越来越多的应用所使用。本文针对区块链应用中的隐私保护问题,首先研究了当前主流加密代币使用的隐私保护策略,包括匿名处理发送方、接收方和内容等环节,设置区块链的访问权限,创新侧链和支付通道等方法,分类存储数据等;然后分析了各隐私保护策略的效率、侧重点及应用前景,并重点分析了零知识证明对基于区块链的分布式应用的重要性;最后对智能合约、身份管理、供应链等实践领域的隐私保护策略进行介绍分析,并提出对未来方向的展望。

关键词 隐私保护,区块链应用,自主权身份,零知识证明

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.05.004

Research on Privacy Protection Strategies in Blockchain Application

DONG Gui-shan CHEN Yu-xiang FAN Jia HAO Yao LI Feng
(No. 30 Inst, China Electronics Technology Group Corporation, Chengdu 610041, China)

Abstract In recent years, more and more privacy protection requirements have been put forward for identity management systems and user-centric self-sovereign identity. As an important means to solve privacy protection problems, blockchain is used by more and more applications. Aiming at the problem of privacy protection in blockchain applications, firstly, this paper studied the privacy protection strategies of mainstream encrypted currencies, including anonymous processing of sender, receiver, content and other links, setting of blockchain access right, innovative methods such as side chain and payment channel, classified storage of data, etc. Then, the efficiency, emphasis and application prospect of each privacy protection strategy were analyzed. Specially, the importance of zero knowledge proof to distributed application based on blockchain was analyzed. Finally, this paper introduced and analyzed the privacy protection strategies in smart contracts, identity management, supply chain and other practical fields, and put forward the prospects of future direction.

Keywords Privacy protection, Blockchain application, Self-sovereign identity, Zero knowledge proof

1 引言

区块链为身份管理系统带来了颠覆性变革,成为实现自主权身份[1](Self-sovereign Identity)的重要手段。该技术能使用户获得个人数据的管理权,无需担心中心化数据库的泄露问题,并简化价值和信任传递流程,使数据记录具有可追溯、不可篡改等优势。当前也出现了多样的基于区块链的身份管理应用和平台,但区块链在逐步成为价值互联网基石的同时,也为用户的隐私保护需求带来了巨大挑战,隐私保护问题客观上制约了区块链应用的普及。

近年国外科学家对自主权身份提出的要求中也重点强调了用户身份声明泄露的信息量尽可能小(Minimization)、用户权益被保护(Protection)等[1]。当前,以比特币[2-3]为代表的公有区块链中各参与方维护公开透明的账本,每个参与方都可查看账本所有交易、发送地址、接收地址等数据。缺少隐私保护机制的缺陷,制约了区块链在身份管理和智能合约领域的应用。如何在区块链的公开透明可验证与用户隐私保护需求之间达成平衡,成为业界关注的焦点[4-5]。本文将总结现有区块链中的隐私保护策略及其优缺点和一些实践经验,以期为研发基于区块链的应用提供重要参考。

2 当前主流的隐私保护策略

2.1 隐身地址技术

在比特币[6]、以太币[7]等区块链应用中,用户地址固定不变,第三方很容易观察一个地址接收和发送交易的行为,并以

到稿日期:2018-05-14 返修日期:2018-08-16 本文受国家重点研发计划(2017YFB0802300,2017YFB0802304)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:2392827595@qq.com(通信作者);范 佳(1982-),女,博士,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;李 枫(1993-),男,硕士,主要研究方向为密码学。

此分析每笔交易的流向，从而通过地址对用户行为进行关联分析。

针对该问题的解决方法是使用收发双方事先知道的一次性地址，使第三方不能对地址的交易历史进行分析。但是，通过使用事务图分析一笔交易从发送端到一次性地址再到接收端的关系，就能破解交易流向隐私，即使在一次交易中使用多个一次性地址也不能避免该漏洞[8]。

以 CryptoNote 方案[9]为例，接收方生成一个父密钥对并公布（如图 1 所示），任何发送方都可使用接收方父密钥对生成新的一次性地址。而接收方使用父私钥扫描每个事务，以找到发给自己的事务并计算相应的一次性私钥。隐身相对早期一次性地址有了很大改进，第三方没有接收方私钥，无法通过事务图方法判断事务的目的端。

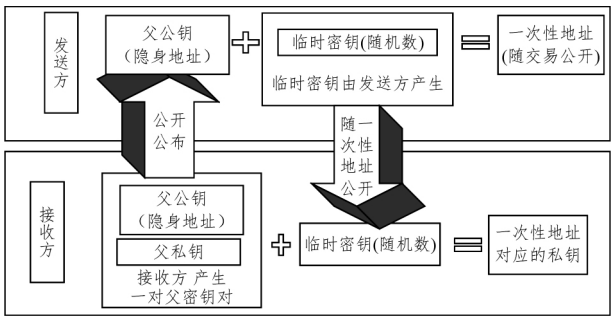

图 1 隐身地址产生一次性地址和一次性密钥的过程

Fig. 1 Process of stealth addresses generating one-time addresses and one-time keys

2.2 混合技术(Mixing)

除了一次一地址的隐身地址技术外，还有以 coinjoin[10-12]为代表的混合技术，这类技术被用于混淆资金的流向路径。比如，比特币中的混合服务 Bitcoin Fog[13-14]，从很多用户处收集比特币，并把这些比特币拆分为更小的数额后在不同时间发往不同地址，使资金流向难以跟踪。图 2 比较了有无混合服务时的资金流向，图 2(b)中当采取混合服务时，可理解为 D,E,F 各从 A,B,C 接收 1/3 个比特币，或 E 从 A、F 从 B、D 从 C 分别接收一个比特币等。越多的参与方加入，则来源和目的地的不确定性就越大。

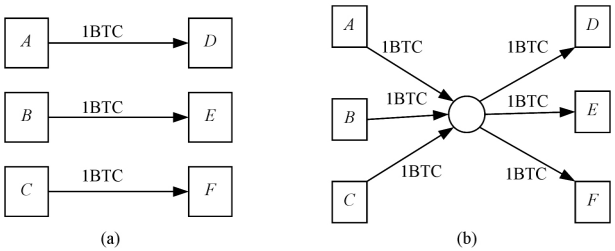

图 2 点对点交易和混合技术的比较

Fig. 2 Comparison of point-to-point transaction and mixing technology

但混合技术[15-16]通常由第三方提供，第三方会收取一些资金作为服务费甚至是窃取资金，并且其知道每笔资金的来源和去向，有可能泄露日志记录，一旦损坏用户权益，用户将难以追溯责任。

针对第三方的弊端，CoinShuffle[11,17]去除了第三方混合服务而由参与方共同协商创建交易，参与方只知道自己的输入和输出而不知道怎样解除混合。A,B,C 三方希望发起混合交易，A 用 C 的公钥加密 A 的目的地址后发送 B，B 用 C 的公钥加密 B 的目的地址后将两个消息一起发给 C，C 解密并知道 3 个目的地址，C 可设置交易，并对设置的交易签名后，发 A，B 签名确认；其他参与方只有在该设置的交易包含了正确的目的地址且没有一个参与方可以解除其他方的交易时才会签字。

对于没有第三方的混合服务，参与方越多，通信开销就越大，且可能面临没有足够用户参与而使混合不能生效的问题。

2.3 Pedersen 承诺

密码学中“承诺”[18]是一种加密机制，用户将一段数据保密，但通过提交该数据的散列值实现“承诺”，还可以在数据中添加盲因子[19]增强“承诺”抵抗穷举搜索的能力。用户需要向验证方证明数据有效时，会提交数据明文和盲因子给验证方，验证方对数据散列和去盲化处理后检查之前用户所发布的散列值是否匹配。该技术的思路与当前基于区块链的分布式身份管理的思路一致。

用户用盲因子 b 对一条消息 m 盲化处理后得到 $\mathrm{blind}(m,b)$，签名方用其私钥 k 对盲化的消息签名得到 $\mathrm{sign}(\mathrm{blind}(m,b))$，并将该消息返回用户，用户对消息进行去盲化处理后得到 $\mathrm{sign}(m,b)$。简言之，该技术允许消息被别人签名，但签名方不能看到明文信息。除了与盲签名共性外，Pederson 承诺[12]的特殊之处在于承诺可加和，即一系列承诺的加和结果等于这些数据加和后的承诺，基本思想可表达为：$C(b_1,m_1)+C(b_2,m_2)=C(b_1+b_2,m_1+m_2)$，其中 C 为“承诺”函数。

Pedersen 承诺可被用于隐藏区块链中的交易内容，Greg Maxwell[20]以保密交易（Confidential Transaction）的名义将其形式化，并在 Blockstream 的元素侧链解决方案中实现。该方案利用了椭圆曲线密码的同态可加性来证明保密交易的输入和输出的加和为零；并在此基础上引入范围证明来证明输出不是负值，否则表明发送方凭空创造了货币。“范围证明”是密码学中的一种加密机制，用于证明某个值在某个范围而不显示该值，在区块链的自治身份发展背景下[1]，该机制具有重要意义。比如，某人在买酒时证明自己大于 18 岁远比证明自己的年龄所透露的信息量小，同时也满足自主权身份最小信息量的要求。

zkLedger[21]是用于金融领域的基于区块链的分布式分类账本，使用 Pedersen 承诺让验证方确认用户资金的输出之和不大于用户资金数额，从而保护资产数额隐私。类似地，其他使用 Pedersen 承诺的方案还有保密资产（Confidential Asset）[22-23]、保密交易（Confidential Transaction）[24]等。

2.4 环/群签名

在数字签名[23,25]中，验签方必须知道该签名信息对应于哪个公钥，该特点使得数字签名的消息能够被跟踪，泄露了签名方的隐私。环签名[26]针对该需求，使用包含自己公钥与其他公钥的密钥组进行环形签名，第三方可以验证生成签名是组里的某个密钥签的，但不能判断具体是哪一个密钥所签。

如图 3 所示，用公钥构造环等式隐藏发送方信息，一个计算的输出是下一个计算的输入，知道密钥组中某个公钥所对

应的私钥，若验证输出 z 与最初的输入 v 相等，则能确认获得了正确的签名。

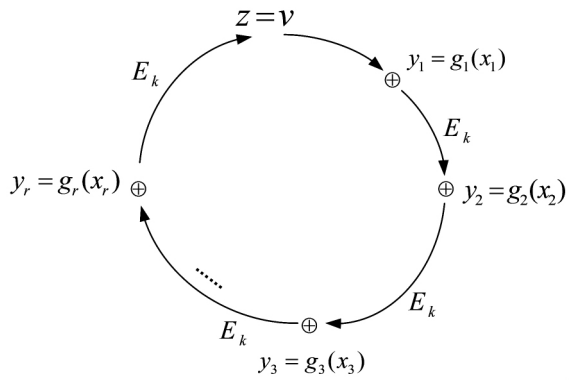

图 3　环签名

Fig. 3　Ring signature

CryptoNote[9] 除了使用上述隐身地址技术外，还使用了环签名技术，发送方选择与自己加密代币数额相同的地址的公钥来构造环签名，并采用了一次环签名策略防止双重消费。其他支持环签名的应用还有 Bytecoin、DarkNetcoin、门罗币、StealthCoin 等[13,27]。

环签名只有环成员，没有管理者，也不需环成员间合作，签名方自由选择他人的公钥加入自己形成集合，集合中的成员甚至不知道自己被包含其中。环签名在保护了发送方隐私的同时，也为监管带来了困难，这是因为无法揭示签名者。相比之下，群签名在群中设置管理员，用以在必要时撤销群签名而揭示签名人，具有更好的实际应用价值。

2.5　零知识证明

零知识证明[28] 分为交互式与非交互式两种，允许一方向另一方证明语句是真实的而不泄露语句外的任何信息。由于区块链具有去中心、多节点共识的特点，交互式零知识对系统资源和时间的消耗较大，因此一般选用非交互式零知识证明。其中，简洁非交互式零知识证明（zero-knowledge Succinct Non-interactive Arguments of Knowledge，zk-SNARK）具有代表性，被 ZeroCash[29]，Hawk[22]，Mediledger[30] 等应用采用，既保留了区块链中互不信任的个体间的共识问题，又保护了交易隐私。

zk-SNARK 最核心的技术是同态隐藏，函数 $E(x)$ 满足：给定 $E(x)$，难以找到 x；对不同输入 $x\neq y$，有 $E(x)\neq E(y)$；如果知道 $E(x)$ 和 $E(y)$，就可以计算 $E(x+y)=E(x)+E(y)$。在区块链的应用中，用户不必透露 x 和 y，就能让验证方相信自己知道 x 和 y，这在应用中有效解决了信息分享不过度的问题。

zk-SNARK 执行前需要中心化产生“证明”的证明密钥和验证密钥，在区块链去中心的系统环境中成为信任风险的来源；同时，zk-SNARK 的计算复杂度和安全性都依赖椭圆曲线运算[16]，执行一笔交易占用内存过大（3～4GB）[17]、执行时间较长（几秒到几十秒不等）[18] 等因素都制约了其在用户终端的使用。如何减少内存占用，提高计算速度，同时兼顾安全性，都成为了重要的研究课题。

相比之下，基于 Pedersen 承诺的保密资产交易[22-24] 虽然能隐藏价值，但暴露了交易之间的联系，一些方案[13,30] 在此基础上使用了标准非交互式零知识证明（Non-Interactive Zero-Knowledge proofs，NIZKs）来隐藏不同交易间的联系。

2.6　侧链和状态通道

侧链和状态通道策略都是将资金托管在区块链上，在侧链或支付通道反映交易的最终结果。侧链可理解为平行区块链[31]，同样不可篡改且永久存在。状态通道是用户间临时建立的支付通道。

执行交易时，至少一方将资金存入智能合约，以此向通道提交资金，交易各方交换密码承诺，指定智能合约中的资金在通道关闭时如何分配。每次在通道内交易时，参与方都创建新承诺，撤销旧承诺，显示新余额。各参与方可单方面触发通道关闭。

侧链本身不提供隐私保护，状态通道只为交易内容提供隐私。隐私取决于使用的策略，比如：blockstream[20] 的元素侧链使用 Pedersen 承诺；BOLT[32] 在通道添加额外的隐私层，使得接收方不能判断付款来自哪个通道；Tumblebit[33] 则在第三方混合技术的基础上分别在付款人和混合器之间以及混合器和收款人之间添加两个状态通道。

2.7　其他

与传统中心化数据库限制操作权限类似，也可限制对区块链的访问和读取权限，即仅允许授权节点连接网络并下载区块链。但该方法在去中心的区块链上又引入了可信第三方，增加了成本来源和单点故障风险，此时的区块链作为分布式数据库，任何一个节点违反出入管制或泄露都将披露区块链的所有交易细节。

除权限访问外，还要对所存储的数据分类。将数据分为公共和隐私两种，公共数据存储在区块链，交易细节“离链”存储在另一个带有访问控制权限的系统中。与前一种方法的区别是，区块链本身和节点不再有额外的访问权限，在区块链上存储交易的哈希值发挥了无中心传递信任的作用。“离链”[34] 存储则支持参与方向其他区块链参与方保密其交易细节的情况，使区块链能继续交换承诺和资产。在“离链”存储交易信息时需要参与方共同维护或委托第三方代理维护，此时又引入了与限制访问权限类似的弊端。

3　技术对比分析

综上所述，当前用于区块链的主流隐私保护策略包括：隐藏发送方地址的环/群签名技术，隐藏发送方地址的隐身地址技术，将交易资金混合重组以混淆资金路径的混币技术，用户认证信息展示尽可能小的 Pedersen 承诺，保护交易内容的零知识证明技术。这些策略覆盖了从发送方地址、信息内容本身、信息量大小到接收方地址再到传统访问控制权限的全方位的隐私保护。

表 1　主流隐私技术的保护环节

Table 1　Protection section of mainstream privacy technologies

技术	发送方	接收方	交易本身
隐身地址[8]	×	√	×
Pedersen 承诺[18]	×	×	√
环/群签名[26]	√	×	×
zk-SNARKs[18]	√	×	√

从表 1 可见，几种典型的密码学隐私保护策略各有侧重点，大致分为对发送方、接收方和交易本身的隐私保护，多数区块链应用将一种或几种策略组合（见表 2），能获得更好的隐私保护（见表 3）。

表 2 当前一些应用方案使用的隐私保护策略

Table 2 Privacy protection strategies used by some current application schemes

技术 \ 方案	保密交易[20]	CryptoNote[9]	门罗币[35-36]	ZeroCash[28]
隐身地址	×	√	√	√
Pedersen 承诺	√	×	√	×
环/群签名	×	√	√	×
zk-SNARKs	×	×	×	√

表 3 各区块链应用的隐私保护程度

Table 3 Degree of privacy protection of some blockchain applications

方案	发送方	接收方	交易本身
保密交易[37-39]	×	×	√
CryptoNote	√	√	×
门罗币[27,35]	√	√	√
ZeroCash	√	√	√

从表 3 可见，在门罗币和 ZeroCash 方案中，第三方不但无法判断发送方和接收方，而且也不能知道交易的具体内容。从表 1 和表 2 可见，门罗币使用了隐身地址、环签名、Pedersen 承诺来分别保护交易的接收地址、发送地址和金额；而 ZeroCash 只用了两种。从门罗币所采用的环签名的特点来看，选择若干其他用户的公钥加入签名集合，可以在一定意义上隐藏发送方的身份，但集合中成员数量有限的特点决定了对发送方提供的隐私服务也较为有限，成功与否取决于环中成员的数量和成员选取的随机性；ZeroCash 自动加密交易的原始数据，交易发送方只需用 zk-SNARK 证明其“消费能力”，交易详情不在区块链保留，第三方只知道有交易发生了，但无法知晓具体的交易参与方和内容。

不同于环签名在原有信息量基础上的叠加式隐私，zk-SNARK 透露最小信息量和零知识的特点使其具有内生的“匿名性”，完全契合自主权身份要求的信息量揭露尽可能小和用户权益被保护的要求，故受到广泛关注。

相比于完全公开透明的比特币，各加密代币不同层次的隐私保护花费了更大的计算成本。如表 4 所列，拥有最优隐私保护的 ZeroCash 除典型交易大小适中外，每笔交易产生零知识证明的计算成本也较高，当前普及到用户手机终端的难度较大，改进余地也较大（如提高算力、改进算法）。其他几种保密策略的算力消耗则是以毫秒为基准，适用于延迟低、交易大小不是限制因素的应用场景。

表 4 各区块链应用的典型交易大小

Table 4 Typical transaction sizes of some blockchain applications

区块链应用	一般典型交易大小/bytes
比特币	300
保密交易	5000
CryptoNote	1600
门罗币[27,35]	13000
ZeroCash[22]	2000

4 其他领域的区块链创新及实践经验

随着区块链从数字货币向智能合约应用、社会治理、公证、仲裁审计等更广泛的身份管理领域扩展，以零知识证明为代表的各种隐私保护技术将在去中心的信息共享中发挥更大的作用[31,40]。

4.1 Identity Mixer

IBM 的 Hyperledger[41] 联盟链平台针对企业级应用，平台的成员服务提供方（Membership Service Provider，MSP）提供了可以盲签名的零知识证明方案 Identity Mixer 凭证，为平台参与方提供基于属性的凭证（Attribute Base Credentials，ABC）[24]，平台参与方之间可以实现强认证，自主选择想要出示的属性（出示具体属性的相关谓词而不是实际值，比如证明自己大于 18 而不是具体岁数）；同时方案防止了无关方对不同认证凭证之间进行关联分析，并支持 CA 审计和撤销。

Identity Mixer 主要包含 4 个环节（如图 4 右半部分所示）。

1）建立环节（Set up）。证书权威（Certificate Authority，CA）产生签名密钥并公布公钥。

2）注册签发流程（Enrollment/Issuance）。用户节点或客户端产生密钥并创建注册证书请求；在证书权威处注册自己的属性，经过验证后用户属性以电子证书的形式签发（也称凭证，注册证书 Ecert），该凭证存储在用户终端应用中。

3）签发展示环节（Signing/Presentation）[29,35]。用户在访问不同应用时，访问控制策略指定了用户应在展示令牌中包含哪种类型的凭据、哪些属性或有关某些属性的谓词；还指定了（验证方信任的）证书颁发机构公钥来正确认证用户属性[42]。用户如果同意揭露访问所要求的政策信息，就从最初的凭证导出符合要求的不同展示令牌，包括：签署交易内容；证明 CA 签发的注册证书（Ecert）的有效性和所有权；揭露交易的访问控制策略所要求的属性，将令牌发给验证方，不同令牌间不能进行关联分析。

4）验证环节（Verification）。验证方使用 CA 的公钥验证令牌是否符合访问控制策略。

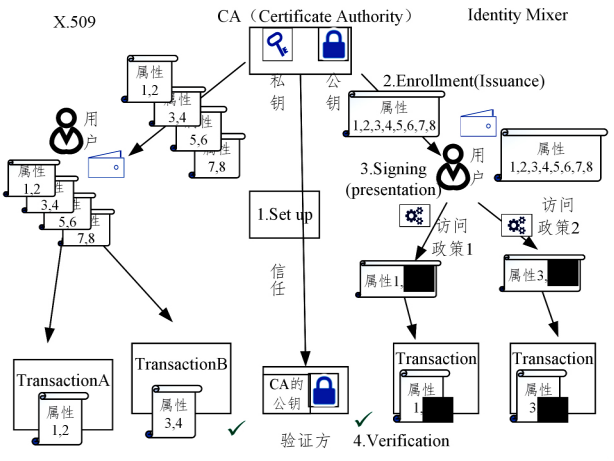

图 4 X.509 与 Identity Mixer 证书流程的比较

Fig. 4 Comparison of X.509 and identity mixer credential process

图 4 右半部分为 X.509 证书的相应工作流程，与 Identity 的详细比较如表 5 所列。传统的 X.509 证书方案在认证时会显示所有用户属性，这导致了用户信息的过度分享；且用户使用相同证书访问不同的应用，无关方可对不同认证的相同证书进行关联分析，从而造成了更多隐私泄露。当前基于区块链的自主权身份要求信息分享不过度，在满足不同的访问控制条件过程中，使用现有 X.509 证书每次都需根据不同访问在 CA 处重新签发，这提升了密钥管理的复杂性，增加了通信和存储开销。此外，该方式每次颁发的交易证书(Tcert)仍然可以由 CA 通过该用户链接其所有认证行为。

表 5　Identity Mixer 凭证和 X.509 证书的比较

Table 5　Comparison of identity mixer credential and X.509 certificate

	X.509 证书	IDMix 凭证
一组属性被数字签名	√	√
证书与私钥被密码方式绑定	√	√
相应属性的零知识证明	×	√
证书之间无关联性	×	√
最小属性披露	×	√
零知识验证证书撤销	×	√
审计权限可分配	×	√

Identity Mixer 有助于避免上述 CA 对用户认证关系的关联分析，即使 CA 也无法将网络中用户出示的令牌凭证链接到原始 Ecert，也不能对用户所导出的令牌进行关联分析，且支持最小属性披露。

基于 IDmix 凭证设计能够实现如图 5 所示的相互作用的实体关系，确保签发给用户的凭证未被撤销时，用户才能导出符合访问策略的有效令牌；检查方可有效检索和展示所呈现的令牌中的属性；令牌除了展示访问策略所需的属性外，无任何多余信息。

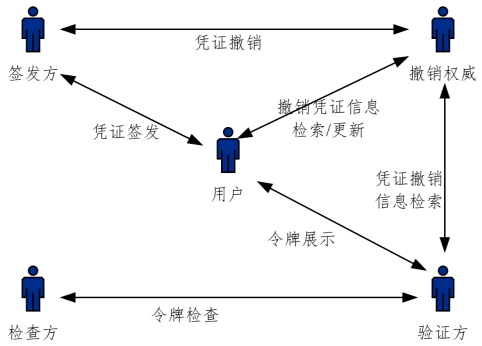

图 5　涉及隐私的 ABC 系统关系

Fig. 5　Relationship of ABC system referred to privacy

4.2　Hawk

不同于 ZeroCash 将零知识用于货币交易，Hawk[30] 作为智能合约的零知识应用被提出，通常，区块链智能合约公开透明，Hawk 方案将智能合约分为公共和私有两部分(见图 6)。公共合约在区块链公开透明，私有合约在“链下”执行，可信第三方(manager)代理各参与方操作私有合约，以密码协议方式决定公共合约如何筹集、持有以及分配资金。操作私有合约同样需要先验证用户权限，可信第三方代理私人合约的执行，可以终止智能合约但是不能影响合约结果。

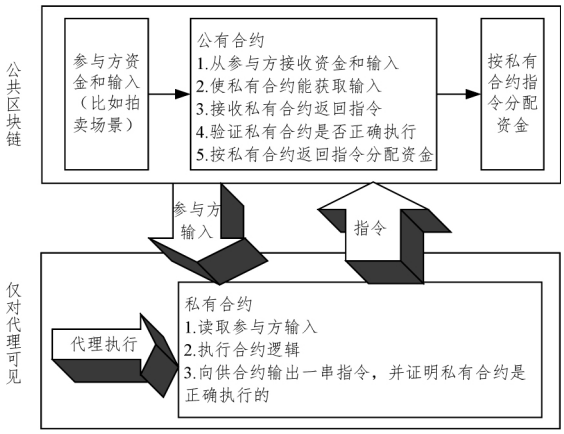

图 6　零知识用于智能合约的 Hawk 方案

Fig. 6　Hawk scheme of zero knowledge for smart contract

为了在安全上能够制衡，公共合约在私有合约未能正确执行时退还托管的资金，可信第三方也被要求在公共合约中存入保证金以防第三方代理不履行合约。

Hawk 方案将零知识证明用于智能合约，如果该方案区块链支持 ZeroCash，则参与方身份也对 manager 隐藏，此时 manager 仅能看到参与方向公共合约托管的资金及私有合约向公共合约输入的指令。

4.3　Mediledger

相比 Identity Mixer 和 Hawk 提出的零知识框架，Mediledger[22] 则针对具体问题，考虑了行业法规、制造商、批发商、分销商、服务提供商等各方的利益关系，具有较大的应用价值[24]。本节将重点分析其用区块链解决药品安全和医疗隐私问题的思路。该方案针对隐私安全问题，使用了 3 种核心技术：符合电子产品代码信息服务标准(Electronic Product Code Information Service，EPCIS)；区块链作为公开、透明、不可篡改的账本，按业务规则执行智能合约，将序列化单位令牌化，限定时间和成员所有权，并可通过智能合约移交保管权，有效避免了双花问题；使用 zk-SNARK 保护医疗隐私。

方案基于联盟链设计，只有特定产品被授权的制造商才能在区块链供应自己的序列化单元，一个序列单元(Serial Unit，SU)在参与方之间的业务转移如图 7 所示。

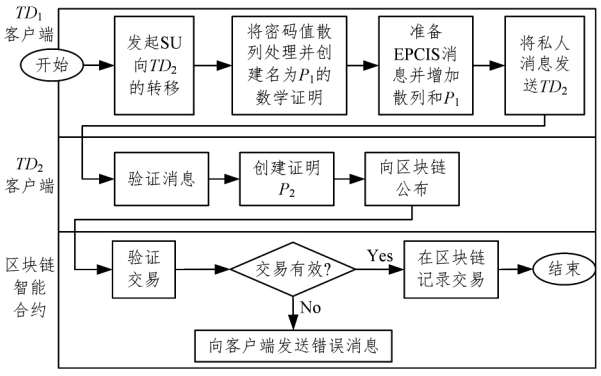

图 7　带有隐私保护的 Mediledger 方案的流程

Fig. 7　Flow of Mediledger scheme with privacy protection

交易方 TD_1 通过 API 向其客户端输入指令，请求向交易方 TD_2 转移序列单元；TD_1 计算包含自己秘密值的哈希值和 TD_1 身份的数学证明 P_1 作为区块链事务；TD_1 生成一个本

次转移说明的 EPCIS 信息；TD_1 向 TD_2 发送前两步产生的 EPCIS 信息和自己的区块链事务值。

TD_2 验证 TD_1 消息，生成自己秘密值的哈希值和 TD_2 自己身份的数学证明 P_2 作为自己的区块链事务。TD_2 将交易发送到区块链验证节点，验证节点的智能合约验证 P_1 和 P_2 是否有效，如有效，就将事务中提交的哈希值更新到区块链中。新的哈希值就表示序列单元从 TD_1 到 TD_2 的转移。

Mediledger 方案流程中的 TD_1 和 TD_2 生成各自秘密值的哈希值，体现信息分享不过度的要求，身份证明 P_1，P_2 使用 zk-SNARK 处理进一步保护隐私。

4.4 应用分析

3 种应用方案的比较如表 6 所列。从加密代币和身份管理领域的隐私保护策略使用来看，这些提高隐私需求的技术都需要扩大原始数据的存储量，并消耗更多的算力。上述每种技术都有其特定领域，各个行业需求也不相同，通常会搭配不同的隐私保护策略。目前，ZeroCash 是隐私效果最好的代币，零知识证明在自主权身份中的重要性逐渐体现，被越来越多的方案所采用[43-45]。

表 6 应用方案的比较

Table 6 Comparison of application schemes

方案	比较类			
	零知识应用特点	应用领域	数据存储	其他隐私策略
Identity Mixer	直接匿名证明[41]	企业级身份管理	用户终端	盲签名
Hawk	两级智能合约管理	涉及资金交易的场景	公开和私有两类	访问权限控制
Mediledger	zk-SNARK	医药供应链	各参与方终端	无

区块链从加密代币进入身份管理领域解决各行业的痛点时，已不再是单纯的发送方、接收方、转账金额，需要考虑行业各参与方的利益诉求、隐私保护等安全需求、行业政策法规、系统可扩展性、监管治理要求、算法策略的计算开销、通信开销和用户体验等诸多方面，依然任重道远。不同解决方案按各自的需求选择不同的隐私保护策略[46-48]，并不断有新的策略涌现，可能会在应用中形成多个相互竞争的隐私标准。

结束语 本文分析对比了当前区块链应用的主流隐私保护策略。首先，对各种主流加密代币中使用的隐私策略进行介绍，并将这些策略分为发送方、接收方、交易本身、零知识证明、传统访问控制、侧链和支付通道等创新类方法进行对比分析。其次，分析零知识证明对基于区块链的分布式应用的重要性，相比一些解决方案同时使用环签名、隐身地址等技术达到保护发送方、接收方或交易隐私的效果，零知识具有存储空间小、透露信息量小、全方位隐私保护等天然优势。然后，对 Identity Mixer，Hawk，Mediledger 等身份管理、具体场景的应用方案进行阐述和对比分析。最后，针对区块链应用中的隐私安全问题，分析了未来的应用方向。

参 考 文 献

[1] ALLEN C. The Path to Self-Sovereign Identity [EB/OL]. (2018-03-14) [2018-05-10]. http://www.coindesk.com/path-self-sovereign-identity/.

[2] MOSER M. Anonymity of bitcoin transactions [EB/OL]. http://xueshu.baidu.com/s?wd=paperuri%3A%2805b83a0935a0aed4f1fbb6a1fa94dc68%29&filter=sc_long_sign&sc_ks_para=q%3DAnonymity%20of%20Bitcoin%20Transactions&sc_us=8079223010421678528&tn=SE_baiduxueshu_c1gjeupa&ie=utf-8.

[3] LIN I C, LIAO T C. A survey of blockchain security issues and challenges[J]. IJ Network Security, 2017, 19(5): 653-659.

[4] DORRI A, KANHERE S S, JURDAK R. Blockchain in internet of things: challenges andsolutions[EB/OL]. [2018-05-10]. http://xueshu.baidu.com/s?wd=Blockchain+in+internet+of+things.

[5] LI X, JIANG P, CHEN T, et al. A survey on the security of blockchain systems, Future Generation Computer Systems[EB/OL]. [2018-05-10]. http://www.sciencedirect.com/science/article/pii/S0167739X17318332.

[6] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. [2018-05-10]. http://bitcoin.org/bitcoin, 2009.

[7] Ethereum White Paper. A next-generation smart contract and decentralized application platform [EB/OL]. (2015-11-12). https://github.com/ethereum/wiki/wiki/White Paper.

[8] HEARN M. Merge avoidance: Privacy enhancing techniques in the bitcoin protocol [EB/OL]. [2018-05-10]. https://www.coindesk.com/merge-avoidance-privacy-bitcoin/.

[9] BERGAN T, ANDERSON O, DEVIETTI J, et al. CryptoNote v 2.0[EB/OL]. [2018-05-10]. https://cryptonote.org/whitepaper.pdf.

[10] ANDY G. Dark wallet is about to make bitcoin money laundering easier than ever[EB/OL]. [2018-05-10]. https://www.wired.com/2014/04/dark-wallet/.

[11] Belcher. Joinmarket-Coinjoin that people will actually use[EB/OL]. [2018-09-09]. http://bitcointalk.org/index.php?topic=919116.0.

[12] ZIEGELDORF J H, GROSSMANN F, HENZE M, et al. CoinParty: Secure multi-party mixing of bitcoins[C]// Proc of the 5th ACM Conf on Data and Application Security and Privacy. New York: ACM, 2015: 75-86.

[13] CAMENISCH J, LYSYANSKAYA A. Signature Schemes and Anonymous Credentials from Bilinear Maps[M]// Advances in Cryptology -CRYPTO 2004. Berlin: Springer, 2004: 56-72.

[14] Bitcoin Fog. Accessing bitcoin fog[EB/OL]. [2018-09-09]. http://bitcoinfog.info/.

[15] BitLaunder. BitLaunder's mixer vs "major exchanges" mixer [EB/OL]. [2018-09-09]. http://bitcoin.stackchange.com/questions/25722/bitlaunders-mixer-vs-major-exchanges-mixer/25753.

[16] BONNEAU J, NARAYANAN A, MILLER A, et al. Mixcoin: Anonymity for bitcoin with accountable mixes[C]// Proc of the 18th Int Conf on Financial Cryptography and Data Security Finacial. Barbados: Financial Cryptography, 2014: 486-504

[17] KYLE T. CoinShuffle aims to improve privacy in bitcoin[EB/OL]. [2018-09-09]. http://insidebitcoins.com/news/coinshuffle-aims-to-improve-privacy-in-bitcoin/29269.

[18] PEDERSEN T P. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing[C]// International Cryptology Conference on Advances in Cryptology. Springer-Verlag，1991：129-140.

[19] CHAUM D. Blind Signatures for Untraceable Payments[M]// Advances in Cryptology. US：Springer，1983：199-203.

[20] MAXWELL G. Confidential Transactions[EB/OL]. https://people. xiph. org/ ~greg/confidential _values. txt.

[21] NEHA N，VASQUEZ W，VIRZA M. zkLedger：Privacy-Preserving Auditing for Distributed Ledgers，IACR Cryptology ePrint Archive [EB/OL]. [2018-05-10]. https://eprint. iacr. org/2018/241.

[22] The MediLedger Project 2017 Progress Report. Charter [EB/OL]. [2018-05-10]. http://www. authorstream. com/jdonahue123/The-MediLedger-Project-2017-Report/.

[23] 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/.

[24] MENDLING J，WEBER I，AALST W V D，et al. Blockchains for business process management-challenges and opportunities [EB/OL]. [2018-05-01]. https://www. researchgate. net/publication/316076240_Blockchains_for_Business_Process_Management_-_Challenges_and_Opportunities.

[25] MAN H A，SUSILO W，YI M. Constant-size dynamic k -TAA [C]// International Conference on Security and Cryptography for Networks. Berlin：Springer，2006：111-125.

[26] Rivest R L，Shamir A，Tauman Y. How to Leak a Secret[M]// Advances in Cryptology — ASIACRYPT 2001. Berlin：Springer，2017：552-565.

[27] MONERO. A note on chain reactions in traceability in cryptoNote2. 0[EB/OL]. [2018-09-09]. https:// getmonero. org/knowledge-base/about.

[28] BEN-SASSON E，CHIESA A，GENKIN D，et al. SNARKs for C：verifying program executions succinctly and in zero knowledge[M]// Advances in Cryptology (CRYPTO2013). Berlin：Springer，2013：90-108

[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] KOSBA A，MILLER A，SHI E，et al. Hawk：The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts [C]// Security and Privacy. IEEE，2016：839-858.

[31] YUAN Y，WANG F Y. Parallel blockchain：concept，methods and issues[J]. Acta Automatica Sinica，2017，43(10)：1703-1712. (in Chinese)
袁勇，王飞跃. 平行区块链：概念、方法与内涵解析[J]. 自动化学报，2017，43(10)：1703-1712.

[32] GREEN M，MIERS I. Bolt：Anonymous Payment Channels for Decentralized Currencies[C]// ACM Sigsac Conference on Computer and Communications Security. ACM，2017：473-489.

[33] HEILMAN E，ALSHENIBR L，BALDIMTSI F，et al. Tumble-Bit：An Untrusted Bitcoin-Compatible Anonymous Payment Hub[C]// Network and Distributed System Security Symposium. 2017.

[34] JOSEPH P，THADDEUS D. The bitcoin lightning network：Scalable Off-Chain instant payments[EB/OL]. [2018-09-09]. http://lightning. network/lightning-network-paper. pdf.

[35] SUN S F，MAN H A，LIU J K，et al. RingCT 2. 0：A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero[C]// European Symposium on Research in Computer Security. Cham：Springer，2017：456-474.

[36] Monero. What is Monero？[EB/OL]. [2018-09-09]. https://getmonero. org/get-started/what-is-monero/.

[37] CHAIN I. Confidential assets[EB/OL]. [2018-05-10]. https://blog. chain. com/hidden-in-plain-sight-transacting-privately-on-a-blockchain-835ab75c01cb.

[38] AXWELL M. Confidential transactions [EB/OL]. [2018-05-10]. https://people. xiph. org/ ?greg/confidential_values. txt.

[39] Confidential assets [EB/OL]. [2018-05-10]. https://www.grin-forum. org/t/confidential-assets/1217.

[40] ZYSKIND G，NATHAN O，PENTLAND A S. Decentralizing Privacy：Using Blockchain to Protect Personal Data [C]// 2015 IEEE Conference on Security and Privacy Workshops (SPW). 2015：180-184.

[41] Hyperledger. Project Charter[EB/OL]. [2018-05-10]. https://www. hyperledger. org/about/charter.

[42] CAMENISCH J，DRIJVERS M，LEHMANN A. Anonymous Attestation Using the Strong Diffie Hellman Assumption Revisited[C]// International Conference on Trust and Trustworthy Computing. Springer International Publishing，2016：1-20.

[43] LIANG X，ZHAO J，SHETTY S，etal. Towards data assurance and resilience in IoT using blockchain[C]// 2017 IEEE Military Communications Conference (MILCOM). IEEE，2017：261-266.

[44] KORPELA K，HALLIKAS J，DAHLBERG T. Digital supply chain transformation toward blockchain integration[C]// Proceedings of the 50th Hawaii International Conference on System Sciences. 2017.

[45] PARK J H，PARK J H. Blockchain security in cloud computing：Use cases，challenges，and solutions[J]. Symmetry，2017，9(8)：164.

[46] DORRI A，STEGER M，KANHERE S S，et al. Blockchain：A distributed solution to automotive security and privacy[J]. IEEE Communications Magazine，2017，55：119-125.

[47] TOSH D K，SHETTY S，LIANG X P. Security implications of blockchain cloud with analysis of block withholding attack[EB/OL]. [2018-05-10]. https://www. researchgate. net/publication/317182715_Security_Implications_of_Blockchain_Cloud_with_Analysis_of_Block_Withholding_Attack.

[48] RUFFING T，MORENO-SANCHEZ P，KATE A. CoinShuffle：Practical Decentralized Coin Mixing for Bitcoin[C]// European Symposium on Research in Computer Security. New York：Springer-Verlag，2014：345-364.