第23卷 第5期 西 安 邮 电 大 学 学 报 Vol. 23 No. 5
2018年9月 JOURNAL OF XI'AN UNIVERSITY OF POSTS AND TELECOMMUNICATIONS Sep. 2018

doi：10.13682/j.issn.2095-6533.2018.05.014

# 区块链中的隐私保护技术

翟社平[1]，杨媛媛[1]，张海燕[2]，赵江明[1]

（1. 西安邮电大学 计算机学院，陕西 西安 710121； 2. 西安邮电大学 教务处，陕西 西安 710121）

**摘　要**：区块链是一种创新的应用程序模型，集成了分布式数据存储、点对点传输、共识机制、数字加密技术和其他计算机技术，具有去中心化、安全可靠和公开透明的特点。在区块链中，数字加密技术占有核心地位，用户信息以及交易数据的安全性是区块链得以推广的必要条件，密码学技术的发展推动并制约着区块链的进一步发展。本文概述了区块链基础架构，包括数据层、网络层、共识层、合约层和应用层。以比特币运行流程为例，分析区块链在隐私保护方面中仍存有在的问题，介绍这些问题现有的解决方案，其中包括混币机制、零知识证明、环签名等技术，对尚未解决的问题进行阐述，并作出展望。

**关键词**：区块链；哈希指针；比特币；混币；零知识证明

**中图分类号**：TP391.1　　**文献标识码**：A　　**文章编号**：2095-6533(2018)05-0093-08

# On privacy protection technology in blockchain

ZHAI Sheping[1], YANG Yuanyuan[1], ZHANG Haiyan[2], ZHAO Jiangming[1]

(1. School of Computer Science, Xi'an University of Posts and Telecommunications, Xi'an 710121, China;
2. Educational Administration Division, Xi'an University of Posts and Telecommunications, Xi'an 710121, China)

**Abstract**: Blockchain is an innovative application model that integrates distributed data storage, peer-to-peer transmission, consensus mechanisms, digital encryption technology and other computer technologies. It is decentralized, secure, and transparent. In blockchain, digital encryption plays a key role. The security of user information and transaction data is a necessary condition for blockchain to be popularized. The development of cryptography technology promotes and restricts the further development of blockchain. This paper outlines the blockchain infrastructure, including the data layer, network layer, consensus layer, contract layer and application layer. Taking Bitcoin operation flow as an example, this paper analyzes the problems existing in bllckchain in privacy protection, and introduces the existing solutions to these problems, including mixed coin mechanism, zero knowledge proof, ring signature and so on. The unsolved problems are expounded and prospected.

**Keywords**: Blockchain; hash pointer; bitcoin; coinjoin; zero-knowledge proof

区块链(Blockchain)是一种具有去中心化、可追溯、不可篡改、安全可靠等特性的分布式数据库，集成了P2P(Peer-to-Peer)协议、数字加密技术、共识机制、智能合约等技术，摒弃了传统中心节点维护的模式，采用多方用户共同维护的方式，实现多方间的信息监督，进而保障数据的可信度与完整性。区块链平台可以分为公有链、私有链和联盟链，公有链中所有的节点均可以自由的加入或退出，私有链严格限制参与节

**收稿日期**：2018-05-20

**基金项目**：陕西省社会科学基金资助项目(2016N008)；工业和信息化部通信软科学项目(2018-R-26)；工业和信息化部通信软科学项目(2017-R-22)；西安市社会科学规划基金(17X63)；陕西省教育厅科学研究计划资助项目(17JK0710)

**作者简介**：翟社平(1971－)：男，博士，副教授，从事语义计算研究。E-mail：zhaisheping@xupt.edu.cn
杨媛媛(1996－)：女，硕士研究生，专业方向为计算机技术。E-mail：yangyy0614@163.com

点的资格,联盟链由若干个参与机构共同管理。比特币于 2008 年被中本聪提出[1],是数字货币最成功的案例,同样也是区块链最典型的应用。此外,区块链在多个方面也拓展出了其独特的应用价值,并表现出了重塑社会的潜力。

各国政府部门高度重视区块链技术发展并积极探索区块链的全面应用。美国以太坊平台 Ethereum 基于区块链为用户提供可编程智能合约开发服务,微软公司在 Azure 云计算平台的基础上推出了 BaaS 服务等。虽然国内区块链起步较晚,但爆发的速度要比国外更快。在政策方面,2016 年 2 月,中关村区块链产业联盟成立;2017 年 5 月,中国第一个区块链标准《区块链参考架构》正式发布,区块链的基本标准得以确立;2018 年 5 月 20 日,工业和信息化部联合多个研究机构撰写的《2018 年中国区块链行业白皮书》在北京发布[2]。在技术方面,2017 年 1 月,众享比特团队发布 ChainSQL,被称为全球首个基于区块链技术的数据库应用平台;2017 年 4 月,腾讯发布 TrustSQL,提供企业级区块链基础设施和云服务。截至 2018 年 3 月底,中国以区块链为主营业务的公司数量已达 456 家。

区块链作为分布式数据库的代表,其所有节点存有区块链上所有用户交易信息,这便对区块链的保密性能有着较高要求。区块链是一个去中心化的点对点网络,节点间相互不信任,不存在中心节点,因此在区块链上进行交易同样需要保证交易信息在不安全信道上的安全传输,维护交易的完整进行。为此,密码学技术在区块链中占有最核心地位。在区块链中,密码学技术保障了用户隐私和交易数据的安全性,保证数据一致性等。本文概述了区块链基础架构,包括数据层、网络层、共识层、合约层和应用层。以比特币为例,分析区块链在隐私保护方面中仍存有在的问题,介绍这些问题现有的解决方案,其中包括混币机制、零知识证明、环签名等技术,详细阐述密码学技术在区块链中如何进行隐私保护以及交易维护。

## 1 区块链体系架构

根据区块链科学研究所创始人 Melanie Swan 的观点,区块链技术已经经历了以比特币为代表的多技术组合创新的区块链 1.0 阶段,以由数字资产转移的以太坊代表的区块链 2.0 阶段。区块链技术的典型应用主要包括比特币、以太坊、超级账本等,尽管它们在具体实现上各有不同,但在整体体系架构上存在着诸多共性。如表 1 所示,区块链平台可分为五个层次:网络层、共识层、数据层、合约层和应用层。

**表 1 区块链体系架构**

| | 比特币 | 以太坊 | 超级账本 |
|---|---|---|---|
| 应用层 | 比特币交易 | 以太币交易 | 企业级区块链应用 |
| 网络层 | TCP-based P2P | TCP-based P2P | HTTP/2-based P2P |
| 合约层 | Script | Solidity/Script EVM | Go/Java Docker |
| 共识层 | PoW | PoW/PoS | PBFT/SBFT |
| 数据层 | Merkle 树 | Merkle patricia 树 | Merkle Bocket 树 |

数据层主要利用块数据结构保障数据存储的完整性,每个数据块将一段时间内接收到的数据交易封装到一个带有时间戳的数据区块中,并链接到当前最长的主区块链上存储,形成最新区块。该层涉及区块存储、链式结构、哈希算法、Merkle 树、时间戳等主要技术。其中,比特币的数据结构为 Merkle 树,以太币的数据结构为 Merkle Patricia 树,超级账本的数据结构为 Merkle Bockt 树。

共识层中主要包含共识机制,能够在决策权高度分散的去中心化系统中使得各节点高效地针对区块数据的有效性达成共识。比特币采用的共识机制为工作量证明(proof of work,PoW),以太坊采用的共识机制为 PoW 和权益证明(proof of stake,PoS),超级账本采用的共识机制为实用拜占庭容错(practical byzantine fault tolerance,PBFT)和投机拜占庭容错(speculative byzantine fault tolerance,SBFT)。

合约层主要包括的智能合约是区块链可编程特性的基础,能够自动执行合约条款的计算机化程序,以代码和数据集合的形式存储在区块链上,通过区块链节点在时间或事件的驱动下以分布式的方式执行,所有相关条款都由代码编成,能够进行

自动结算,通过签名或其他外部数据信息触发事件来执行。比特币中脚本功能有限,只能称为合约的雏形,以太坊、超级账本分别采用了不同的编程语言进行合约编写。

网络层包括各类数据传输协议以及验证机制等。区块链是典型的 P2P 网络,所有节点采用扁平拓扑结构连接,没有中心节点,任意两个节点可进行自由交易,任意节点可以随时加入或退出网络。区块链中的 P2P 协议主要用于节点间信息传输,不同的应用场景所采用的协议不同,比特币与以太坊采用 TCP 协议完成,超级账本采用 HTTP/2 协议完成。

应用层主要包括比特币、以太坊和超级账本。比特币主要是进行数字货币交易,以太坊在数字货币基础上加入去中心化应用,超级账本则不支持数字货币交易,主要是企业级的区块链应用。

## 2　密码技术与区块结构

哈希算法是将任意长度的消息序列映射到较短的固定长度值的函数,具有易计算性、单向性、抗碰撞性和高灵敏度等特征[3]。通常用于确保数据完整性,即验证数据是否被非法篡改,当被检验的数据发生变化时,其相应的哈希值也会发生变化,因此即使数据处于不安全的环境中,也可以依据数据的哈希值检测数据的完整性。

对区块链来说,哈希函数可以用来做区块和交易的完整性验证。在区块链中,每个区块的头部信息中会存储着前一个区块的信息的哈希值,任何用户可以比对计算得出的哈希值和存储的哈希值,来检测前一个区块的信息的完整性。

哈希指针是一种数据结构,除了包含通常的指针外,还包含一些数据信息以及与这些信息相关的密码哈希值,其中正常的指针用于取信息,哈希指针用于验证信息是否被篡改[4]。如图 1 所示,区块链即为一类使用哈希指针的链表,每个块通过使用哈希值顺序连接,根据哈希值验证区块中包含的数据是否改变,从而确保块信息的完整性。

区块链中的区块保存了全网所有数据信息,主要由包含元数据的区块头和包含所有交易数据的区块体组成[5]。区块的每个数据块通常包括区块头(header)和区块体(body)。区块头封装先前的区块哈希(prev-block),当前区块的难度目标和当前区块解随机数(nonce)、Merkle 根(Merkle-root)以及时间戳(Timestamp)等信息。

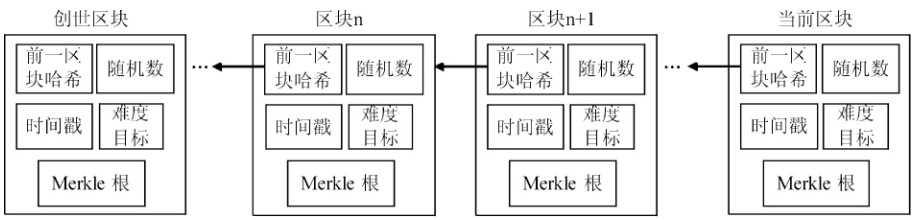


**图 1　区块链链式结构**

前一区块哈希:区块哈希是区块链的关键字段,该字段是将前一个块的数据信息进行哈希运算的结果,将链上的所有区块顺序连接,形成从创建块到当前块的最长主链。每个块不仅具有前一个块的位置信息,而且还可以根据前一区块哈希值验证区块中包含数据的完整性。

随机数(Nonce):每个数据区块的头部信息中都含有一个随机数,初始值为 0,运行比特币矿机的结点对区块整体数据进行 SHA256 运算,当随机数计算出来的 SHA256 值不满足要求时,随机数自动加一,继续进行 SHA256 运算,直到 SHA256 值比当前数据区块 SHA256 值小时,新区块产生。因此,生成新的区块的过程实际上是计算 SHA256 值,并与目标值比较的过程,比特币数据区块生成的这一过程被称为工作量证明。

时间戳:区块链技术要求获得记账权的节点必须在当前数据区块头中加盖时间戳,表明区块数据的写入时间,主链上各区块是按照时间顺序依次排列的。时间戳可以作为区块数据的存在性证明,有助于形成不可篡改和不可伪造的区块链数据库,从而为区块链应用于公证、知识产权注册等时间敏感的领域奠定了基础。

难度目标:难度目标是使整个网络的计算力大致每 10 分钟产生一个区块所需要的难度数值。难度目标由区块链网路根据过去两周的计算结果,自动重新计算未来两周的难度目标。难度目标由区块中的 SHA256 值所决定,通过控制区块头(Block Header)中的 SHA256 值应恰好落在可控范围目标区间之内来增加或减少难度目标。

Merkle 根:Merkle 树是最初由著名密码学家

Merkle 提出的哈希二叉树，用于快速验证大规模数据的完整性。Merkle 树主要是哈希二叉树或多叉树。如图 2 所示，Merkle 树通常包含区块的交易数据库，区块头的根哈希（即 Merkle 根），以及沿底层区块数据到根哈希的所有分支。Merkle 树操作过程通常将块体的数据分组，并将生成的新散列值插入 Merkle 树中。因此递归直到只留下最后一个根哈希并记录为块头的 Merkle 根，最后构造成树结构。比特币采用双 SHA256 哈希函数，即将任意长度的原始数据经过两次 SHA256 哈希运算后转换为长度为 256 位的二进制数字来统一存储和识别。

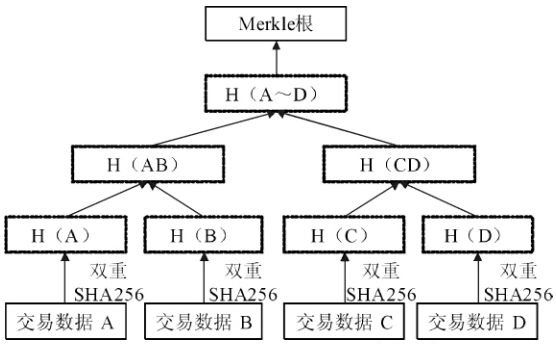


**图 2 Merkle 树**

交易列表：交易列表中保存有很多笔交易记录的详细信息，其中包括每一笔交易的生成时间、交易编号、比特币金额、付款人等信息。在数据块中，由于每一比特币支出和接收的交易是写在一起的，因此具有可追溯性。

## 3 比特币中的密码学技术

### 3.1 比特币地址

密码学的核心技术包括对称加密和非对称加密，非对称加密也称为公钥加密，可以很好地解决对称加密中密钥早期分发的问题。非对称加密算法拥有两个不同的加密密钥和解密密钥，即公钥和私钥。

私钥通常需要通过随机数算法生成，公钥通过进行不可逆算法计算得出。非对称加密算法具有公私钥分开、可在不安全信道传输的优点，同样，具有处理速度低、加密强度低的缺点，且需要基于数学问题来保证非对称加密算法的安全性。

比特币系统中的密钥对包括一个私钥，和由其衍生出的唯一的公钥，密钥对是由公钥加密生成的。在比特币交易的支付环节，收件人的地址是由一个公钥生成，称为比特币地址，即收款方[6-7]。

如图 3 所示，私钥（k）是一个数字，通常是随机选出的，公钥（K）是私钥通过椭圆曲线乘法进行加密生成，比特币地址（A）由公钥使用一个单项加密 Hash 函数生成比特币地址。

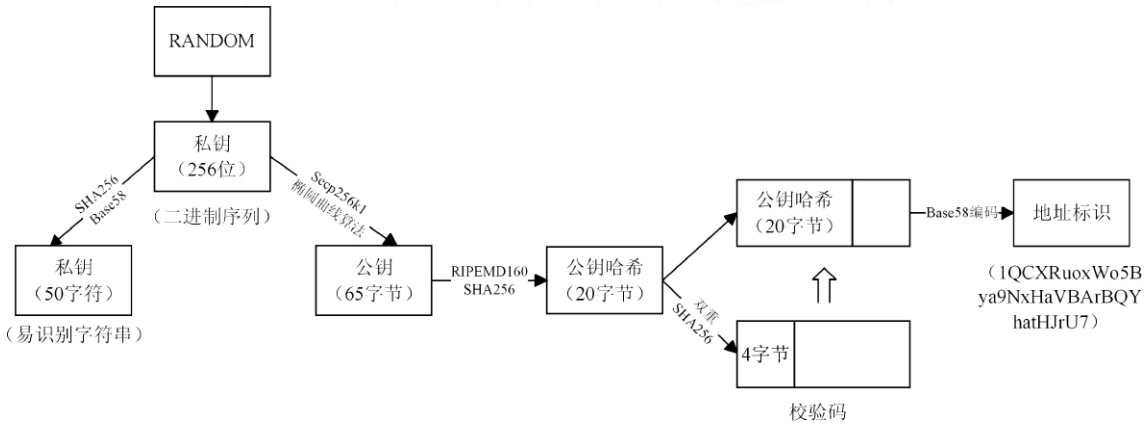


**图 3 比特币地址生成**

生成一个比特币私钥在本质上是在 1 到 $2^{256}$ 之间选一个数字，需要保证选取的结果是不可预测或不可重复的。比特币采用操作系统底层的随机数生成器来产生 256 位的随机数作为私钥，将随机生成的私钥 k 为与曲线上已定义的生成点 G 相乘，以获得曲线上的另一点，即相应的公钥 K。比特币密钥的生成点都是采用 secp256k1 标准中的生成点，一个私钥 k 乘以 G 将得到相同的公钥 K。椭圆曲线依托离散对数问题，k 和 K 之间的关系是固定的，但只能单项运算，即从 k 得到 K，从 K 难以得到 k。

用户地址的生成在不同平台上采用了不同算法，比特币采用 SHA256 与 RIPEMD160 双哈希得出比特币地址，以太坊采用 Keccak256 算法生成以太币地址。其中，比特币生成过程，以公钥 K 为输入，计算其 SHA256 哈希值，再计算哈希后数值的 RIPEMD160 哈希值，得到一个长度为 160 位的数字，作为公钥哈希，最后将公钥哈希进行 Base58 编码形成比特币地址。

### 3.2　比特币交易

数字签名系统包含签名算法和验证算法;签名算法对消息进行一定运算,从而生成一个由签名密钥控制的数字签名,签名者掌握签名密钥以及签名算法的具体流程,因此签名密钥、签名算法的安全性得以保证。验证算法通过验证所接收消息的数字签名进而验证消息的有效性,验证算法和验证密钥全网公开,任何消息接收者都可以查看和使用,即全网所有人都可以使用其对所接收的消息进行有效性验证。

在以区块链为底层技术的密码货币系统中,数字货币所有者将该数字货币的上一个交易单内容和下一个拥有者的地址进行哈希计算,将使用自己私钥对信息进行数字签名后的数据附加在交易列表的最后,发送给接受者[8]。接受者需要对所接受的信息进行签名验证,以证明上一位拥有者的信息,进而验证该交易的拥有者。区块链中每笔交易同时记录该货币当前的所有者、前一所有者、下一所有者。因此可以实现货币的全程可追溯,有效避免了双重支付、虚假交易等问题[9]。

如图 4 所示,用户 2 与用户 3 进行付款交易,当用户 2 需要向用户 3 支付 10 个比特币时,首先要在交易单上记录金额和该比特币的来源。用户 2 的 10 个比特币来自于用户 1,因此,完成用户 2 对用户 3 的支付交易,需要记录比特币的来源、支付的金额、以及用户 2 的数字签名。

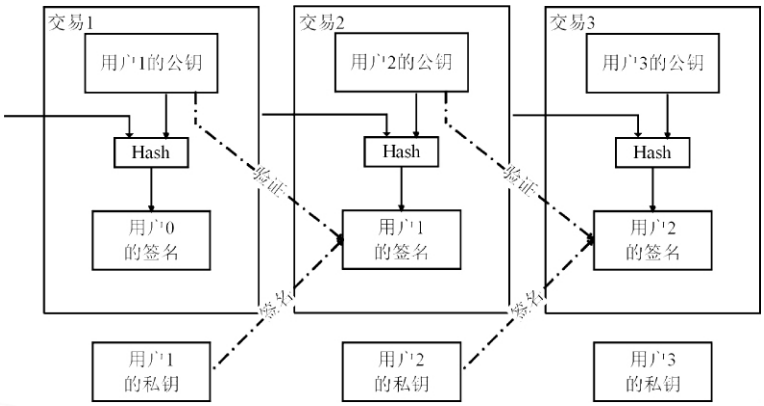


**图 4　交易的签名和验证**

在交易认证过程中,签名主要由付款人来完成,交易的付款人首先对上一笔交易的交易数据信息进行哈希运算得到其哈希值,付款人使用自己的私钥对该哈希值进行加密,加密后的数据将作为上一交易数据信息的数字签名与上一交易数据同时发送给接收方。接收方收到信息之后,将对交易的合法性进行验证,使用与上一步相同的哈希函数从接收的交易数据信息得到哈希摘要,之后利用付款人的公钥对上一步附加的数字签名进行解密得到另一哈希摘要。通过对两个摘要进行对比,可确保交易单有效性,若二者内容相同,接受方就能确认交易单有效。

### 3.3　共识机制

共识机制用于确定区块链网络中的记帐节点,并用于确认交易信息,保证各区块数据的一致性同步。早期的比特币区块链使用了工作证明机制,该机制严重依赖节点算力来确保比特币网络分布式记账的一致性。随着区块链技术的发展和各种竞争性货币的出现,研究人员提出了各种机制,可以在不依赖计算能力的情况下达成共识。例如,股权证明、委任权益证明(delegated proof of stake, DPOS),以及一些分布式一致性算法,如 PBFT, Raft 等算法,这些共识机制各有利弊,应用场景也各不相同。

PoW 机制依赖分布式节点之间的计算能力竞争,确保整个网络区块链数据的一致性和安全性。每个节点贡献自身算力,通过类似暴力破解的方法寻找一个合适的随机数,使得区块头元数据经过 SHA256 运算后得到的哈希值小于区块头中难度目标值,即

$$H(n \parallel h) \leqslant t, \tag{1}$$

其中 $H$ 为 SHA256 哈希函数;$n$ 为随机数;$h$ 为区块头部数据,主要包含前块哈希、Merkle 根等内容;$t$ 为难度目标,$t$ 值越小,$n$ 值越难找到;第一个寻找到随机数的节点则可获得新区块的记账权。以比特币网络为例,PoW 的共识流程如下。

(1) 广播阶段:网络中节点打包交易并且将新交易广播至全网。

(2) 节点计算阶段:全网每个单节点收集过去 10 分钟的所有交易,以 Merkle 树形式组织从而计算出 Merkle 根填入区块头。同时节点将区块头的 Nonce 值从 0 依次递加 1,直至区块头的两次 SHA256 哈希值小于或等于当前网络中的难度目标值。

(3) 新区块生成:第一个找到正确随机数的节点阔的新区块的记账权,同时获得挖矿奖励,该奖励包含该区块中所有交易的交易费以及新区块的区块奖励。节点打包区块后,向全网广播新区块。

(4) 验证阶段:网络中其他节点接收到新区块后首先验证其正确性及有效性,通过数字签名验证交易的有效性,同时计算随机数的正确性。验证无误后,节点将该新区块加入本地区块链中,并基于该块构建下一区块。

### 3.4 隐私保护现存问题

区块链技术中存储交易信息的全局账本是公开的,任何加入区块链网络的节点都可以获得完整的副本。通过分析全局账本中的交易记录,潜在攻击者有可能对用户的交易隐私和身份隐私带来威胁[10]。交易隐私威胁指包含交易详情的一些潜在威胁,例如攻击者通过对一系列交易记录进行深层次分析获得一些有价值信息,包括特定账户的资金余额、交易详情、关联账户、资金流向等。身份隐私威胁主要是指交易者身份泄露的潜在威胁,攻击者在分析交易数据的基础上,可以通过结合一些背景知识获得交易者的身份信息。

为了对抗这种攻击,目前的保护措施主要包括混币(coinjoin)、环签名(ring signature)、零知识证明(Zero-Knowledge Proof)等[11]。达世币(Dash)采用混币措施,由混币节点将多笔交易合并为一笔交易,进而隐藏付款地址与收款地址之间的关系。门罗币(Menero)采用环签名,它认可验证签名,不可知晓签名者身份,进而隐藏交易发送者的身份信息。零币(Zerocash)采用零知识证明,在不泄露交易信息以及额外信息的条件下,向验证者证明交易的正确性。

## 4 数字货币中的其他密码学技术

### 4.1 混币机制

混币机制在数字货币中加入可信第三方,将所有交易的输入与输出地址打乱,进而实现货币的混合。在混币机制中,存在三个角色:混币提出方、混币制定的接收方、系统中的可信第三方。具体的混币过程首先由混币提出者将货币发送给可信第三方,可信第三方通过相应算法进行混币,然后将混币后的数字货币发送至提出方设定好的接受方。由此,混币机制可以用以下公式表示为

$$C_M(Z_1,C_A(Z_0,m),A)\rightarrow C_A(Z_0,m), \quad (2)$$

公式(2)的左侧表示混币提出人向可信中间人发送的信息,右侧表示可信第三方经过处理之后想接收方发送的信息。混币提出人的最终目的是将消息$(Z_0,m)$发送给接收方的地址 A,首先将消息$(Z_0,m)$用接受者 A 的密钥 $C_A$ 进行加密,得到$C_A(Z_0,m)$,接下来在加密的信息上加入可信第三方的验证消息 $Z_1$ 和接收方地址 $A$,对添加后的信息采用可信第三方的密钥 $C_M$ 进行加密,得到$C_M(Z_1,C_A(Z_0,m),A)$,可以有效避免消息在不安全信道上传输时被截获或篡改。可信第三方收到信息后,首先采用自己的密钥对消息进行解密,可以得到$Z_1,C_A(Z_0,m),A$,但仍然无法获得 $Z_0,m$。可信第三方解密后需要验证 $Z_1$ 是否正确,判断无误后,将 $C_A(Z_0,m)$发送给接收方 A。接收方采用自己的密钥进行解密,获得 $Z_0,m$,完成此次通信[12]。

此类混币机制称为基于中心节点的混币机制,由可信第三方完成混币的过程,首先混币的提出者将数字货币发送给可信第三方节点,可信第三方可以收取多个用户发来的资金,将所收到的资金进行分配,最后根据混币提出方指定的金额和地址进行货币转移。混币机制避免了资金直接由发送方到达接收方,对资金的流向形成了干扰,进而避免攻击者通过资金流向获取隐私信息。

达世币是一种较常见的数字货币,采用了中心化的混币机制。达世币的可信第三方节点在混币过程中需要交纳一定金额的押金,一旦主节点进行非法操作,押金即被没收,避免混币节点存在破坏行为,提升可信第三方节点的可信度。除此之外,达世币还引入了链式混合和盲化的思想,链式混合是指用户交易时可以随机自主的选择多个主节点进行混合。盲化技术是指用户不需要将输入和输出发送到交易池,而是指定主节点将输入和输出传递到另一主节点。因此,对于主节点而言很难获得用户的真实身份,避免了中心节点被破坏而泄露用户隐私信息的问题。

### 4.2 零知识证明

零知识证明是由 Goldwasser 等在 1989 年提出

的,是一种两方协议或多方协议,参与人包括证明者和验证者,零知识证明可以实现证明者在不透漏任何隐私信息的情况下,验证者可以判断某个消息的有效性,实现有效证明。零知识证明的原理可以用描述为:对于语言 L,令$\langle P,V\rangle$是其交互证明系统。如果对于每个概率多项式时间交互机 $V^*$,都存在一个概率多项式时间算法 $M^*$,使得$\{\langle P,V^*\rangle_{(x)}\}_{x\in L}$和$\{M^*(x)\}_{x\in L}$总体是计算不可区分的,则称$\langle P,V\rangle$是计算零知识的。

2013 年提出 Zerocoin 概念,是一种较为常见的数字货币,采用了零知识证明技术,可以实现完全匿名的数字货币[13]。Zerocoin 中的匿名集合中包括现有的所有 Zerocoin,Zerocoin 系统可以通过“铸币”方法使比特币转换成 Zerocoin。用户进行 Zerocoin 交易时,首先通过零知识证明算法证明自己的 Zerocoin 存于系统中并且没有已经被花费。但零币扔然存在许多问题,例如 Zerocoin 无法由比特币系统生成;Zerocoin 的货币金额不可任意切分 Zerocoin 不支持非交互交易,并且零知识证明过程过于繁琐。为此许多新的方案被提出,SASSON 等人提出了 Zerocash 方案最为典型。

Zerocoin 技术在比特币主链上增添了一条侧链,进而实现了隐私保护。当交易被提出时,会被拆分成多个规模较小的交易,并发送到全网中,在交易接受者地址之前多个交易会被合并成原交易。Zerocash 技术则采用承诺函数将信息进行封装,其中包括交易的发出者、接受者、金额等,在验证的过程中,采用了零知识证明技术,可以有效的保护交易发出者、接受者的地址信息以及交易的具体金额。由此可见,采用 Zcash 进行交易时,需要采用公私钥对进行验证。

但 Zcash 仍然存在许多不足,在 Zcash 发送交易的参数初始化时存在中心化的问题,很大的对去中心的特点以及用户的隐私保护造成了影响。零知识证明过程过于繁琐,证明生成过程的效率过低,需要消耗大量时间,严重影响了数字货币的高效性。

### 4.3　环签名

环签名是一类只有环成员,没有管理者的数字签名方案,具有无条件匿名性,正确性和不可伪造性三个特性。具有较高的安全性,攻击者根据所获取的消息无法判断当前签名是由哪位生成,当攻击者拥有环成员私钥的情况下,也难以进行破解。同时,签名可被所有其他环成员验证真实性,其他成员无法伪造该签名者的签名,攻击者也无法对某个消息伪造签名。

门罗币采用了大量密码学技术实现隐私保护,最为核心的是基于换签名的混币机制。该混币机制是去中心化的混币操作,没有第三方的存在,有效的避免了中心节点被破坏等问题。此外,门罗币中也采用了隐藏地址技术,可以实现地址的隐藏,交易的发送者采用隐藏地址技术生成临时地址,全网上的所有用户需要对该条交易信息进行验证,进而判断该条交易是否是发送给自己,并且只有交易的接受者才能解密该条消息。利用隐藏地址技术,全网的用户都可以看到该条交易,并对交易的有效行进行验证,并且无法确认交易的接受者[14]。

此外,环签名技术也可以实现不可追踪性,交易发送者利用随机数生成器生成私钥,使用椭圆曲线加密算法生成对应公钥,同时得到与之对应的密钥镜像。一个密钥镜像对应一个签名,其目的是判断签名的唯一性和不可复制。交易发送者在所有的交易列表中随机选取 $n$ 个交易,与自己的公钥组成 $n+1$ 个交易集合 $T$。利用 $T$、随机数集合、私钥以及非交互式挑战最终得到最后的签名。

## 5　结语

在区块链备受关注的如今,数据安全和隐私保护受到了严峻的挑战,先进的密码学技术可有效解决此类问题,但仍存在存在薄弱环节。私钥的生成是采用计算机系统中的随机数生成器生成,称为伪随机,具有一定规律性,存在被破解的威胁。SHA-2 算法目前虽然并没有有效的方法破解此系列算法,但是一旦被破解,区块链中所有数据的隐私和安全将不复存在。数字加密技术贯穿区块链系统,是区块链系统的核心技术,密码学的研究对区块链的发展将起到决定性作用。

现有的数字货币应用已较为成熟,例如比特币、零币、门罗币等。但区块链在其他领域的研究才刚刚开始。区块链作为一种新的网络技术,仍需要研究人员进行相关应用的研究,为区块链的进一步应用提供技术基础。

## 参 考 文 献


[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[Z/OL]. [2018-05-10]. https://bitcoin.org/bitcoin.pdf.

[2] 工业和信息化部信息中心. 2018 中国区块链产业白皮书[EB/OL]. (2018-05-21)[2018-05-10]. http://www.cbdio.com/BigData/2018-05/21/content_5718003.htm.

[3] SHEN Y, WANG G. Improved preimage attacks on RIPEMD-160 and HAS-160[J/OL]. Ksii Transactions on Internet & Information Systems, 2018, 12(2):727-746[2018-07-18]. http://doi.org/10.3837/tiis.2018.02.011.

[4] 王化群, 吴涛. 区块链中的密码学技术[J/OL]. 南京邮电大学学报(自然科学版), 2017, 37(6):61-67[2018-05-18]. http://www.cnki.com.cn/Article/CJFDTOTAL-NJYD201706011.htm. DOI:10.14132/j.cnki.1673-5439.2017.06.010.

[5] 袁勇, 王飞跃. 区块链技术发展现状与展望[J/OL]. 自动化学报, 2016, 42(4):481-494[2018-07-18]. http://www.wanfangdata.com.cn/details/detail.do?_type=perio&id=zdhxb201604001. DOI:10.16383/j.aas.2016.c160158.

[6] BENCIC F M, ZARKO I P. Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph[Z/OL]. (2018-04-26)[2018-05-18]. http://arxiv.org/pdf/1804.10013.

[7] 翟社平, 李兆兆, 段宏宇, 等. 区块链关键技术中的数据一致性研究[J/OL]. 计算机技术与发展, 2018, 28(8):94-100[2018-05-18]. http://epub.cnki.net/kns/brief/result.aspx? dbPrefix=CJFQ doi:10.3969/j.issn.1673-629X.2018.09.020.

[8] 孙国梓, 冒小乐. 基于区块链技术的电子数据存整系统[J/OL]. 西安邮电大学学报, 2018, 23(4):78-83[2018-07-18]. http://dx.doi.org/10.13682/j.issn.2095-6533.2018.04.013.

[9] 安庆文. 基于区块链的去中心化交易关键技术研究及应用[D/OL]. 上海:东华大学, 20171-60[2018-05-17]. http://epub.cnki.net/kns/brief/result.aspx?dbPrefix=CDMD.

[10] 翟社平, 段宏宇. 区块链技术:应用与问题[J/OL]. 西安邮电大学学报, 2018, 23(1):1-13[2018-07-18]. http://dx.doi.org/10.13682/j.issn.2095-6533.2018.01.001.

[11] 陈捷, 高英. 区块链在物联网隐私保护中的应用[J/OL]. 物流技术, 2018, 37(7):33-38[2018-05-18]. http://epub.cnki.net/kns/brief/result.aspx? dbPrefix=CJFQ. DOI: 10.3969/j.issn.1005-152X.2018.07.008.

[12] ZYSKIND G, NATHAN O, PENTLAND A. Decentralizing Privacy: Using Blockchain to Protect Personal Data[C/OL]//IEEE Security and Privacy Workshops. [S.l]: IEEE Computer Society, 2015:180-184[2018-05-17]. https://ieeexplore.ieee.org/document/7163223. DOI: 10.1109/SPW.2015.27.

[13] 苑超. 区块链隐私保护关键技术研究[D/OL]. 郑州: 战略支援部队信息工程大学, 2018:1-55[2018-05-17]. http://epub.cnki.net/kns/brief/result.aspx? dbPrefix=CDMD.

[14] 祝烈煌; 董慧; 沈蒙; 区块链交易数据隐私保护机制[J/OL]. 大数据, 2018(5): 46-56[2018-05-17]. http://epub.cnki.net/kns/brief/result.aspx? dbPrefix=CJFQ. DOI: 10.11959/j.issn.2096-0271.2018005.


[责任编辑:陈文学]