区块链隐私保护技术

刘滋润[1]，王 点[2]，王 斌[1]

（1. 中国航天科工集团第二研究院 706 所，北京 100854；2. 上海宇航系统工程研究所，上海 201108）

摘 要：从区块链定义、特点、基本概念与技术架构等方面阐述区块链技术，提出四层的技术架构。结合国内外著名的区块链项目，分析比较不同区块链共识机制的性能。分析区块链发展遇到的问题，尤其是隐私保护方面存在的问题，从数字加密货币出发，分析区块链隐私保护问题的挑战、解决方案及难点，重点对匿名币门罗币和零币使用的环签名和零知识证明进行研究。对区块链隐私保护技术进行总结与展望。

关键词：区块链；共识机制；隐私；数字加密货币；去中心化；匿名

中图法分类号：TP309 **文献标识号**：A **文章编号**：1000-7024（2019）06-1567-07

doi：10.16208/j.issn1000-7024.2019.06.012

Privacy preserving technology in blockchain

LIU Zi-run[1], WANG Dian[2], WANG Bin[1]

(1. Institute 706, Second Academy of China Aerospace Science and Industry Corporation, Beijing 100854, China;
2. Shanghai Aerospace System Engineering Institute, Shanghai 201108, China)

Abstract: To illustrate the background technology of the blockchain, various aspects of blockchain definition, characteristics, basic concepts and technology architecture were studied. A four-level architecture of the blockchain was put forward. With the famous blockchain projects at home and abroad, the performance of the consensus mechanism of different blockchains was analyzed and compared. The problems, especially the problems in privacy preserving, encountered in the development of blockchain were analyzed. From the perspective of cryptocurrencies, the challenges, solutions and difficulties of privacy-preserving in blockchain were deeply analyzed. The ring signature and zero knowledge proof in Monero and Zcash, famous anonymous cryptocurrencies, were mainly studied. The summary and prospect were put forward for the research of the future blockchain privacy-preserving technology.

Key words: blockchain; consensus mechanism; privacy; cryptocurrency; decentralized; anonymity

0 引 言

作为目前最前沿、最热门的技术之一，区块链技术引发了新一轮的技术浪潮。2008 年，中本聪（化名）发表文章——《比特币：一种点对点的电子现金系统》[1]，从此，比特币迅速进入了大众视野并在全球范围内掀起了“挖矿”热潮，它对人们传统的货币、金融观念产生强烈的冲击，具有重要的革新意义。研究发现，比特币背后的核心技术区块链技术，具有点对点、不可抵赖性、不可篡改性等特性，具有更深远的研究意义。不仅在金融领域，区块链技术在通讯、公证、医疗、工控、教育、军事等各个领域的应用都在积极的探索之中。欧美等国高度重视区块链技术研究，我国对于区块链的发展也高度重视。2016 年 12 月，区块链技术首次被列入国务院印发的《“十三五”国家信息化规划》[2]，国家在战略高度上对区块链发展进行了统筹规划，未来区块链技术的发展必将更加迅速。

在这样的背景下，本文主要介绍了区块链的基础技术和概念，并结合当下区块链发展所遇到的问题和挑战，重点对区块链隐私保护技术展开研究，限于文章篇幅和研究实际，本文从数字加密货币角度出发，分析使用区块链技术交易时，如何保护交易中的敏感信息。其中，最主要的两种技术分别是环签名技术和零知识证明技术。

收稿日期：2018-02-13；**修订日期**：2018-04-23

作者简介：刘滋润（1993-），男，江苏徐州人，硕士研究生，研究方向为信息安全；王点（1987-），男，上海人，工程师，研究方向为信息化系统建设；王斌（1981-），男，山西运城人，研究员，硕士生导师，研究方向为可信计算、网络安全。

E-mail：1551195766@qq.com

1 区块链技术分析

1.1 区块链定义

目前，业界对于区块链还没有统一的定义，2016 年 10 月，工信部组织编纂的《中国区块链技术和应用发展白皮书》中将区块链定义为：分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。2017 年 5 月，工信部发布的《区块链参考架构》中，区块链定义是：一种对等网络环境下，通过透明和可信规则，构造不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。

本文认为，区块链是利用新思想对以往一些技术的结合形成的新模式，其核心思想是通过去中心化和去信任化的方式集体维护一个可靠的链式数据结构。

1.2 区块链主要特点

区块链具有以下主要特点。

去中心化：在区块链中事务的全过程可以不需要第三方参与，包括创建账号、创建事务、验证事务、记录事务、查询事务等等。

去信任化：区块链安全不依赖可信机构的背书，提供一种基于密码学的、低成本的可信交易。一般来说，公有链的代码是开源的，整个区块链的数据是公开的，节点间不存在互相欺骗的情况。

集体维护：所有参与节点共同维护区块链系统，包括对数据的维护、对网络架构的维护、对共识机制的维护等等。

可靠数据库：数据一旦写入区块链，只具备“增”和“查”的功能，而不具备“删”和“改”的功能，并且每一个参与节点都能取得整个区块链完整数据库的备份，因此，区块链具有不可篡改、不可伪造和不可抵赖的特性，所以区块链是可靠的。

1.3 区块链基本组成

一个完整的区块链系统包含很多技术，有作为支撑的对等网络和维护系统的共识算法，有存储数据的数据区块及其包含的时间戳、默克尔（Merkle）根、数字签名等技术，还有许多密码学加密技术与智能合约等。

P2P 网络。对等网络（peer to peer network，P2P）是一种在对等者之间分配任务和工作负载的分布式应用架构，是对等计算模型在应用层形成的一种组网或网络形式。区块链系统是建立在 IP 通信协议和分布式网络的基础上的，它不依靠传统的电路交换，而是建立在网络通信之上，而且网络中每个节点均会承担网络路由、验证数据区块等功能。

数据区块。区块链中的交易记录会存储在数据区块中，数据区块一般包含区块头和区块体两部分，区块头中封装了当前的版本号、前一区块地址、时间戳、随机数、该区块的目标哈希值以及默克尔树的根值等信息。区块体中则主要包含交易计数和交易详情。交易详情是指区块链系统的账本，每一笔交易都会被永久地记录在数据区块中。区块体中的默克尔树对每一笔交易进行数字签名，以确保交易不可伪造且没有重复交易。所有的交易通过默克尔树的 Hash 过程产生一个唯一的默克尔根值计入区块头。如图 1 所示。

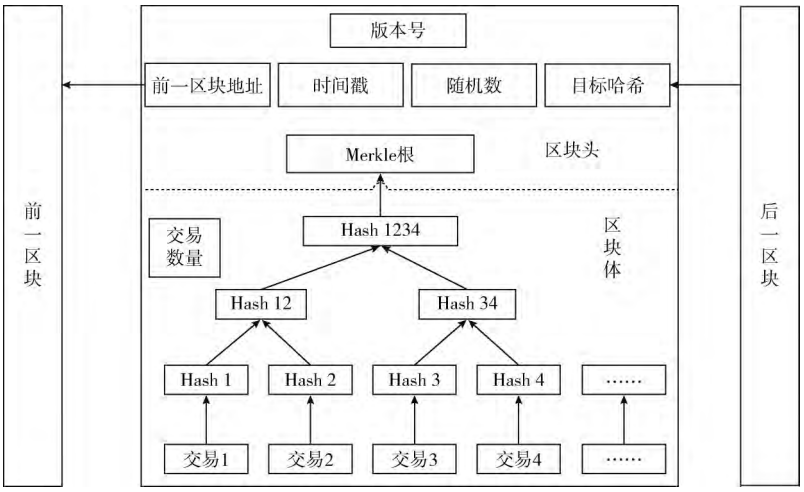

图 1 数据区块结构

1.4 区块链技术架构

为方便对区块链隐私保护的研究，考虑到数字加密货币的流通性等特点，本文将区块链技术架构抽象为 4 个层次，如图 2 所示。

数据层：包括链式结构、区块数据、数字签名、非对称加密等。

网络层：区块链节点之间通过 P2P 网络实现信息的交互。

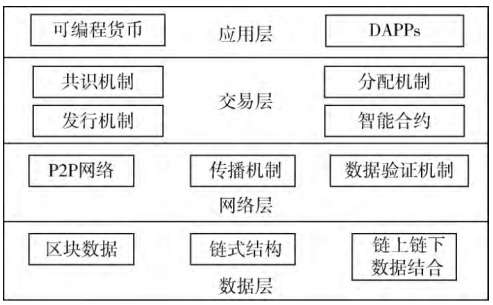

图 2　区块链技术架构

交易层：对不同的区块链地址之间的交易、合约建立一个统一的分类账，通过共识机制和激励机制保障交易的可靠性。

应用层：区块链用户通过区块链应用实现交互。

区块链共识机制是区块链使用去中心化思想解决节点间信任问题的核心所在，在区块链技术架构中具有承上启下的重要地位，区块链共识机制主要抵御两种类型的问题：

拜占庭容错。在网络中存在许多故障或连接不良的节点时必须也能够保持一致性[3]。

Sybil 攻击（女巫攻击）。即使在一个有许多伪造身份节点的网络中，也必须保持共识一致性，一般假定这些节点是为敌手所拥有。

根据不同的使用场景，不同区块链中使用的共识机制是不同的，当前比较常见的共识机制有工作量证明机制（proof of work，PoW）、权益证明机制（proof of stack，PoS）、股份授权证明机制（delegated proof of stack，DPoS）、实用拜占庭容错机制（practical byzantine fault tolerance，PBFT）、Raft 机制等，图 3 给出了几种共识机制的对比分析。

	PoW	PoS	DPoS	Raft	PBFT
场景	公链	公链、联盟链	公链、联盟链	联盟链	联盟链
记账节点	全网	全网	选出若干代表	选出一个leader	动态决定
去中心化程度	完全	完全	完全	半中心化	半中心化
存储效率	全账本	全账本	全账本	全账本	全账本+部分账本
吞吐量	约7TPS	≥25TPS	≥300TPS		≥1000TPS
响应时间	10分钟	1分钟	约3秒	秒级	秒级
容错率	50%	50%	50%	50%	33%

图 3　主要共识机制对比

注：这里的 PoW 主要是指比特币中的机制，如果是以太坊的话，虽然也是 PoW 机制，但是由于算法的不同，其吞吐量为 25TPS 左右，响应时间约 9 s。

目前，区块链平台很多，如国外的以太坊 Ethereum、IBM 的 Hyperledger Fabric、R3CEV 推出的 Corda 等，国内比较知名的有 BCOS 等，图 4 对各个区块链平台的特性简要对比。

	以太坊	Fabric	Corda	BCOS
共识机制	PoW	PBFT	BFT	PBFT、Raft
可插拔性	否	是	是	是
可扩展性	否	是	是	是

图 4　研究平台共识机制对比

1.5　数字加密货币

数字加密货币是目前区块链技术最广泛的应用场景，为方便对区块链隐私保护进行分析，本文重点从数字加密货币的角度进行分析。

在比特币和区块链之前，Chaum 在 1983 年构建了电子货币[4]。Chaum 的电子货币与现在的研究有所不同，其假设存在中央银行，货币是由银行的私钥所生产，可以利用盲签名从银行中取出这些匿名的货币。不过该方案需要这样一种假设为前提：存在一个可信的中央银行和一个中心化的密钥。现在研究的数字加密货币与电子货币类似，与法币（如人民币、欧元、美元等）相比，拥用相同的可替

代性和匿名性保证，但不需要中心化的发证机关。

随着 2008 年比特币白皮书的发布，比特币的成功激励了许多其它数字加密货币的出现，有些是基于比特币的基本结构（如，莱特币、达世币等），而有些则是完全独立设计的（如，门罗币、Zcash 等）。数字加密货币可以理解为区块链技术加上相应的令牌或货币，其交易需要被验证并以区块的形式存储在底层的区块链中[5]。

2 区块链存在问题

尽管区块链在许多方面优势十分显著，但是它还存在许多问题，如：

51%攻击威胁。敌手可能以盗窃或颠覆共识算法的形式实施攻击。如果恶意一方控制网络 51%或更多的节点或者算力，区块链历史将被改写。此外，控制网络 25%左右的哈希功率也可能对系统造成其它攻击[6]，甚至，文献[6]认为，任意规模的组织都可能会对区块链网络产生威胁。

资源浪费[7]。为了防止“双花攻击”和其它区块链欺骗行为的发生，工作量证明机制的算力代价很高，因此使用 PoW 机制的区块链需要消耗非常多的能源。

吞吐量小。比特币的交易率峰值目前为 7 次/s 交易(TPS)。相比之下，信用卡 VISA 平均每秒约 2000 次交易，峰值吞吐量为 24000TPS[8]。

货币价值波动极大。数字加密货币价值是由市场决定的，而新技术的不确定性往往导致较高的波动性。以比特币为例，从最初的约 0.003 美元到最高突破两万美元，考虑到其仅仅出现短短几年时间，这种情况是历史上所罕见的。

区块链中不存在中心化的可信第三方，因此在设计安全协议时还存在隐私保护的问题[9]，近几年的研究结果表明，由于区块链数据的公开性，通过对大量交易的数据进行分析，已经出现了许多去匿名的方案，区块链的隐私保护问题形势十分严峻。本文将对该问题进行详细的分析与研究。

3 区块链隐私保护技术

由于区块链上的数据无法删除和篡改，当用户发现部分地址或交易信息泄露时已经为时已晚，无法采取挽救措施，因此与传统领域相比，区块链的隐私保护问题更加重要。对区块链的隐私保护必须采取事前防御的策略，即从方案的制定上、协议上、算法上对用户隐私进行高度重视与保护[10]。

3.1 区块链隐私保护定义

在信息系统中，隐私一般是指数据拥有者不愿意被披露的敏感信息，如敏感数据或者数据所表征的特性。在比特币白皮书中简要说明了区块链隐私模型，并与传统金融安全模型进行了对比。为了在分布式的节点间实现数据同步和共识，区块链必须公开一些信息，比如公开地址、交易内容等等。尽管区块链的地址表面上是用户创建、与用户身份无关，在这个过程也不需要可信第三方参与，但是，当区块链用户使用地址进行区块链交易或其它业务时，对网络层区块链交易的传播轨迹进行分析可能会推测出该地址对应的真实身份。因此，必须考虑到隐私保护的问题，需要对链中的敏感信息进行处理，防止隐私泄露。

《区块链参考架构》中对隐私保护的描述为：

由于区块链技术为所有的参与节点提供了公共账本，这给业务的使用者和提供者带来了额外的隐私挑战。隐私保护活动具体包括：

（1）识别区块链服务的隐私构成；

（2）制定区块链服务隐私保护策略；

（3）执行具体的区块链隐私保护活动，对构成隐私的事务相关的相关方身份和事务细节的保护，具体的保护对象包括并不限于数据存储、数据传输和数据应用；

（4）定期审核区块链隐私保护策略和隐私保护活动的具体效果，必要时对隐私保护策略进行修订，并按照新的策略执行隐私保护活动。

本文认为，区块链隐私保护就是通过引入一些隐私保护算法、协议或其它策略，在区块链中保护身份隐私和交易隐私。保护身份隐私就是要尽量减小用户身份与区块链地址之间的相关性，保护交易隐私是指保护区块链存储的交易记录及潜在信息（如交易金额、反映的用户消费水平和生活习惯等等）。

3.2 区块链隐私保护面临的挑战

目前，对于区块链隐私保护的研究还存在许多困难与挑战，例如，存在许多去匿名技术：多输入、变换地址、IP 关联分析、使用中心化服务等等[11]。从数字加密货币的角度出发，区块链隐私保护面临的主要挑战有：

（1）推测交易者身份：在数字货币交易中，以比特币为例，如果两笔交易的接收地址相同，则该两笔交易的接收方为同一人，因此每次交易中应当使用不同的接收地址。对于发送方，其输入往往是分布于不同的交易输出中，但是当进行大额交易时，需要将多个交易输出合并作为一个输入，此时可以推断这种多输入交易的输入为同一人所有。

由于区块链数据的公开性，每一笔交易都公开广播和大量复制，所以即使是在交易提交数年之后，任何潜在的标识信息都可能被挖掘出来，针对交易图关联分析，可以推测潜在的信息，甚至推断交易者身份。

（2）暴露交易金额：在比特币交易中，输入地址、输出地址和交易金额都是公开的，以方便矿工对交易的合法性进行验证。不过，实际生活中，许多情况下交易双方不希望公开交易的具体数额，因此，在保障矿工能够对交易合法性进行判定的同时怎样隐藏交易金额，提出了一种挑战。

4 区块链隐私保护实现

在区块链中实现隐私最常考虑的几种方式如下：

同态加密（homomorphic encryption，HE）。使用同态加密可以方便交易的审核，而且不会泄露交易的实际数额。但全同态加密目前是非常低效的，因为它的计算开销极大（10 亿数量级）、密钥占用空间达 25 GB。一些数字加密货币，如门罗币使用机密交易（CT）来隐藏交易的金额，它使用加法同态加密，具有较少的计算开销[12]。

混合服务。货币可以使用第三方服务器实现混合，如 CoinJoin 方案，它是唯一一个不需要对比特币协议进行修改就能实现混合的解决方案，因此它的应用十分广泛。例如 SharedCoin，它是由 blockchain. info 推出的一种比特币冲洗服务[13]，基于 CoinJoin 协议对比特币交易进行混淆，通过同时创造大量的输入交易和输出交易，并增加交易的重复次数来使比特币地址变得更加难以追踪，但是有研究发现，通过工具分析数据特征，还是可以发现原来交易的输入和输出地址。此外，所有参与方都可以执行混合合约的一部分，从而消除对可信服务器的需求，例如 JoinMarket，混合请求通过互联网中继通信（IRC）广播。

隐私货币设计。例如，在进行交易的时候，执行一些混合的操作，一般情况下不允许使用只带有一个输入的交易。这些数字加密货币可以利用零知识证明的方式进行交易，比如 ZCash 就是这样做的[14]。

调整访问结构。为增强区块链的隐私性，可以通过隐藏元数据，或有通过访问控制机制确定交易只对某些特定人员可读。

追踪叛逆者。该举措是为了实现对破坏他人隐匿性的当事人进行惩罚，进而增强方案的匿名性，因为惩罚机制大大降低了参与方实施破坏的意愿。

广播加密。为接收者提供了高度匿名性，因为群中的每个用户都接收加密消息，但只有具有正确权限或密钥的用户才能解密。广播加密也是完全抗合谋攻击的[15]。

安全硬件。可以用于限制用户的操作，例如硬件可以在输出交易之前实施混合操作，或者像在盲签名中那样用于提高随机性[4]。

中间人。例如，中间人从一个交易所中存入和提取货币，可以消除“可追溯性”属性。

安全多方计算。这使得参与方协同工作，没有一个人有访问所有的数据的权限，因此没有人可以泄露秘密信息。但是，效率低下问题突出，而且要求各方必须是可信的[15]。

离链存储。在区块链中离链存储敏感数据将提高区块链的隐私性，只有在需要访问这些数据时才将其上链[15]。在进行离链存储时要选择可信的存储主机，或者将数据分割，并存储在多个节点上。

下面从数字加密货币角度，介绍两种具体的区块链隐私保护实现方案。

4.1 门罗币与 CryptoNote

门罗币给自己的定义就是一个匿名的数字加密货币，其采用 CryptoNote 协议，通过“多层可链接自发匿名群签名（M-LSAGS）实现混合。

门罗币的发行为用户提供更强的隐私性，通过使用隐蔽地址（stealth address）来隐藏交易数据和关键画像，以防止双花攻击[16]。门罗币在混合协议中使用环签名，门罗币中每笔交易都使用环签名方案生成一个关键画像，关键画像是针对给定用户的私钥执行单向函数的结果。画像中包含的信息可以让第三方知道该交易已被正确地形成而且没有试图双花攻击。在门罗币中，环签名与隐蔽地址相结合使用，隐蔽地址是一次性使用的地址，且与任何用户不相关。货币的接收方通过使用私有的“viewkey”可以确认它们的存储位置，然后使用私人的“消费密钥”来形成一个环签名将这笔货币花费。不过，CryptoNote 中引入环签名会对可扩展性产生不利影响[17]。

隐蔽地址是由比特币开发者 Peter Todd 提出，并广泛应用于比特币中。其实现思路如下：传统上使用一个地址是很容易跟踪的，而如果使用很多地址，用户必须记住多个不同的存储私钥。隐蔽地址允许用户使用多个地址，但实际使用时只有一个，因为在这个过程中使用服务器处理多个账户，以改善用户体验、防止伪造货币并提高用户的隐私性。

Greg Maxwell 首次提出机密交易（confidential transactions）用于隐藏交易金额，但不隐藏发送方或接收方地址。这是通过加法同态加密实现的，交易占用空间约 5 KB 大小，证明占用 2.5 KB。门罗币将环签名与机密交易相结合，形成机密环交易（ring confidential transaction）[12]。门罗币通过硬分叉实现机密环交易，可以实现隐藏交易的金额、来源和目的地。同时，可以大大提高链式分析的难度[18]。

门罗币还引入了新的椭圆曲线算法，将输出的分布散列到椭圆曲线上，这在以往任何研究论文中都没有出现过，不过门罗币研究团队认为这是一种安全的哈希函数[12]。然而，目前没有分析能够表明该函数的输出是否是随机均匀分布的，或者该实现过程是否是单向的，因此，一般将其视为一种随机函数。门罗币的椭圆曲线加密以爱德华兹曲线为基础，爱德华兹曲线速度快，而且在特定的定义中，如 Curve25519，其安全级别更高。

4.2 ZCash 与 zk-SNARKs

2013 年，约翰·霍普金斯大学的研究人员设计了 Zerocoin 协议，该协议可以提供内置的不可链接性[19]。Zerocoin 的设计是为了应用于比特币区块链系统，通过一系列的过程将交易的起源隐藏起来，例如通过铸币将比特币转

化为 ZeroCoin，以与透明的比特币交易相混淆。ZeroCoin 是对比特币的一种拓展，但由于该方案的效率问题和缺陷，往往不被使用。使用 ZeroCoin 时每花费 1 个货币需要一个 25 KB 的证明，总的交易大小达 49 KB。该交易还只存在于单一的面额，不能实现金额的任意切分，因此往往需要计算许多复杂的证明；ZeroCoin 不支持非交互交易而且零知识证明的时间过长。

针对这些问题，2014 年 Ben-Sasson 等提出了 ZeroCash 方案[20]。ZeroCash 使用简洁的非交互式零知识证明（zk-SNARKs）保护交易金额、发送方和接收方地址。zk-SNARKs 要求发送方以零知识的方式产生一个证明，证明其具有花费金额大于或等于交易的价值的能力。除了简洁的特性，zk-SNARKs 具有非常好的完整性和计算可靠性的特性，它的零知识证明是多项式时间的。

随着 ZeroCash 协议的不断完善，ZCash 已经发展成为一个独立的数字加密货币。ZCash 中用户具有更大的自主性，可以选择是否对交易进行加密[5]。ZCash 在包含所有以前的交易信息的默克尔树上使用 zk-SNARKs。如果使用不当，这可能会泄漏有关最新交易的信息，因为交易将出现在最新的一个集合中而不是之前的。为了防止这种情况，默克尔树大小是固定的，为 2^{64}。如果 ZCash 平均每秒产生 1000 笔交易，这将花费 292 000 000 年时间将默克尔树填满。

目前，证明的产生在计算上还比较昂贵，生成一个密钥对需要花费几分钟的时间，生成零知识证明更加困难（至少 3 分钟）[21]，但这是一个活跃的研究领域。需要强调，这些证明的验证是非常有效的，而且签名的大小非常小——签名占用大约 322 字节，验证的时间大概为几毫秒（约 8.5 ms）[22]。

以上几种方案以及门罗币的一些特性，总结见表 1。

表 1 几种区块链方案的隐私特性

	ZeroCoin	ZeroCash	ZCash	Monero
出现时间	2013	2014	2016	2014
隐藏来源	是	是	是	是
隐藏接收方	否	是	是	是
隐藏交易金额	否	否	自主选择	是

简洁的属性使这些方案可以很快产生证明，而且与其它零知识证明相比，占用空间“小”、验证很快[20]。然而，与其它的区块链交易相比，证明以及交易占用的空间依然是非常大的。在表 2 中，我们比较基于 zk-SNARKs 的数字加密货币以及 SNARKs 的性能和成本。

目前所有基于 zk-SNARKs 的方案需要一个可信的安装阶段，否则构建系统时使用的秘密信息可能会被不可信方用于伪造交易或创造假的货币。为减轻可信安装阶段的必要性，可以考虑使用多方设置方案。与使用一个可信方相比，使用 N 个参与方的安全性更高，因为 N 方中只需要一方是可信的就可以了。

表 2 不同区块链交易性能比较

	SNARKs for C	ZeroCoin	ZeroCash	以太坊
交易占用空间（字节）	322	约 49000	996	65
安全级别/bit	N/A	80/128	128	128
密钥生成时间/min	20	7.8	5	/
证明时间/min	22	3	1	/
验证时间	4.68 s	0.45 s	5.4 ms	/

5 结束语

随着比特币的兴起，底层的区块链技术越来越引起学术界的广泛关注，在注意到区块链固有的安全特性之外，还应当认识到其存在的隐私保护问题。本文主要结合数字加密货币对此展开研究，对其底层的技术、协议、机制进行分析，期望对未来的研究提供有价值的参考。未来，应加强联盟链和私有链研究、离链支付保护研究和安全加密技术研究，还需要对具体的技术实现与优化进行详尽的研究和设计，并能够从数字加密货币迁移到通用的区块链技术中。

参考文献：

[1] Rajput U，Abbas F，Hussain R，et al. A simple yet efficient approach to combat transaction malleability in bitcoin [C] // International Workshop on Information Security Applications. Cham：Springer，2014：27-37.

[2] WANG Hao，SONG Xiangfu，KE Junming，et al. Block chain in digital currency and its privacy protection mechanism [J]. Netinfo Security，2017 (7)：32-39 (in Chinese). [王皓，宋祥福，柯俊明，等. 数字货币中的区块链及其隐私保护机制 [J]. 信息网络安全，2017 (7)：32-39.]

[3] Baghban H，Moradi M，Hsu C H，et al. Byzantine fault tolerant optimization in federated cloud computing [C] //IEEE International Conference on Computer and Information Technology. Nadi：IEEE，2017：658-661.

[4] Kraft D. Difficulty control for blockchain-based consensus systems [J]. Peer-to-Peer Networking and Applications，2016，9 (2)：397-413.

[5] Luis Gomez Quintana. Creating a tokenized fund in the ethereum blockchain [D]. Tampere：Tampere University of Applied Sciences，2017.

[6] Eyal I，Sirer E G. Majority is not enough：Bitcoin mining is vulnerable [C] //International Conference on Financial Cryptography and Data Security. Berlin：Springer，2014：436-454.

[7] Yli-Huumo J，Ko D，Choi S，et al. Where is current research on blockchain technology?-A systematic review [J]. Plos One，2016，11 (10)：e0163477.

[8] Sompolinsky Y，Zohar A. Secure high-rate transaction processing in bitcoin [M] //Financial Cryptography and Data Security. Berlin：Springer，2015：507-527.

[9] TIAN Haibo，HE Jiejie，FU Liqing. A privacy preserving fair contract signing protocol based on public blcokchains [J]. Journal of Cryptologic Research，2017，4 (2)：187-198 (in Chinese). [田海博，何杰杰，付利青. 基于公开区块链的隐私保护公平合同签署协议 [J]. 密码学报，2017，4 (2)：187-198.]

[10] Kosba A，Miller A，Shi E，et al. Hawk：The blockchain model of cryptography and privacy-preserving smart contracts [C] //Security and Privacy. San Jose：IEEE，2016：839-858.

[11] Conoscenti M，Vetrò A，Martin J C D. Blockchain for the internet of things：A systematic literature review [C] //Computer Systems and Applications. Agadir：IEEE，2017：1-6.

[12] 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.

[13] Bonneau J，Narayanan A，Miller A，et al. Mixcoin：Anonymity for bitcoin with accountable mixes [C] //International Conference on Financial Cryptography and Data Security. Berlin：Springer，2014：486-504.

[14] Sasson E B，Chiesa A，Garman C，et al. Zerocash：Decentralized anonymous payments from bitcoin [C] //IEEE Symposium on Security and Privacy. San Jose：IEEE，2014：459-474.

[15] Ben-Sasson E，Chiesa A，Genkin D，et al. SNARKs for C：Verifying program executions succinctly and in zero knowledge [M] //Advances in Cryptology-CRYPTO. Berlin：Springer，2013：90-108.

[16] Courtois N T，Mercer R. Stealth address and key management techniques in blockchain systems [C] //International Conference on Information Systems Security and Privacy. Porto：SciTePress，2017：559-566.

[17] Ruffing T，Moreno-Sanchez P. ValueShuffle：Mixing confidential transactions for comprehensive transaction privacy in bitcoin [M] //Sliema：Financial Cryptography and Data Security，2017：133-154.

[18] Kumar A，Fischer C，Tople S，et al. A traceability analysis of monero's blockchain [C] //European Symposium on Research in Computer Security. Cham：Springer，2017：153-173.

[19] Miers I，Garman C，Green M，et al. Zerocoin：Anonymous distributed E-cash from bitcoin [C] //Security and Privacy. Berkeley：IEEE，2013：397-411.

[20] Ben-Sasson E，Chiesa A，Green M，et al. Secure sampling of public parameters for succinct zero knowledge proofs [C] //Security and Privacy. San Jose：IEEE，2015：287-304.

[21] Bergquist J，Laszka A，Sturm M，et al. On the design of communication and transaction anonymity in blockchain-based transactive microgrids [C] //The Workshop on Scalable & Resilient Infrastructures for Distributed Ledgers. Las Vegas：ResearchGate，2017：1-6.

[22] Benhamouda F，Camenisch J，Krenn S，et al. Better zero-knowledge proofs for lattice encryption and their application to group signatures [M] //Advances in Cryptology-ASIACRYPT. Berlin：Springer，2014：551-572.