区块链交易数据隐私保护机制

祝烈煌，董慧，沈蒙
北京理工大学计算机学院，北京 100081

摘要
区块链技术是一种去中心化、去信任化、公开透明的分布式数据存储技术，能够降低信任成本，实现安全可靠的数据交互。然而，攻击者可以轻易地从公开的全局账本中获得所有数据，并通过大数据分析技术挖掘用户交易规律等隐私信息。分析区块链交易数据面临的隐私泄露威胁，描述基于数据分析的攻击方法；介绍以混币机制为代表的交易数据隐私保护机制，简要描述各种混币方法的基本原理，并针对混币过程是否需要中心节点参与的问题分析不同混币机制的优势与缺陷；最后，分析了现有区块链数据隐私保护技术中存在的不足，并展望未来的发展方向。

关键词
区块链；混币机制；数据隐私保护

中图分类号：TP393 文献标识码：A doi: 10.11959/j.issn.2096-0271.2018005

Privacy protection mechanism for blockchain transaction data

ZHU Liehuang, DONG Hui, SHEN Meng
School of Computer Science & Technology, Beijing Institute of Technology, Beijing 100081, China

Abstract
Blockchain technology is a distributed data storage technology that is de-centralized, de-trusted, open and transparent. It can reduce the cost of trust and realize safe and reliable data interaction. However, attackers can easily obtain the transaction data stored in the public ledger, and may extract transaction rules and other privacy information from this data by applying big data analysis techniques. Firstly, the thread of attack of data analysis on blockchain transaction data was analyzed, and the attack methods based on data analysis were described. Then the privacy protection mechanism of transaction data which was represented by mixing mechanism was introduced, the basic principle of various mixing methods was described in brief, and the advantages and disadvantages of different mixing approaches for the problem of whether a central node was needed in the process of mixing were analyzed. In the end, the limitation of the existing technologies and envision the future directions on this topic was discussed.

Key words
blockchain, mixing mechanism, data privacy protection

1 引言

区块链技术是一种分布式的互联网数据库技术，它的去中心化、去信任化、公开透明等特点使陌生节点之间可以在不依赖于第三方可信机构的情况下建立起点对点的可信价值传递，主要优势在于能够显著降低信任成本、提升交互效率。区块链网络中没有中心服务器，系统中的每个参与节点都持有完整的数据副本，它们共同维护着数据的完整性，能够有效避免集中式服务器单点崩溃和数据泄露的风险。

然而，区块链中记录交易数据的全局账本在网络中是公开的，任意攻击者都能够获取所有交易信息，使交易者的隐私有泄露的风险。例如，比特币系统目前的交易数据大约为155 GB，包含从2009年开始运行到当前时刻的所有交易记录。对账本中的数据进行分析整理，攻击者可以获得任意一个账户对应的所有交易，还可以分析不同账户之间的交易关系图谱，即使用户采用不同的账户进行交易，攻击者也可以利用地址聚类技术分析出隶属于同一个用户的不同账户[1-5]①②。而且由于用户进行的每一笔比特币交易都将永久记录在区块链中，一旦某一笔历史交易被实名化（例如比特币交易所受到黑客攻击，导致用户账户信息泄露），则相关的所有交易记录中的交易者身份信息都将泄露。此外，随着区块链交易逐渐被应用到日常支付领域，攻击者可以利用链外信息推测区块链中账户的身份。例如，将用户的购物记录和比特币账户支付记录进行对比，分析账户的身份信息。

针对基于数据分析的隐私窃取方法，目前已出现一些隐私保护机制。主要思想是在不影响区块链系统正常工作的情况下，对公开数据中的部分信息进行隐藏，增加数据分析的难度。其中，混币是一种应用广泛的隐私保护方法。混币机制的核心思想是隐藏区块链交易双方的交易过程，使攻击者无法准确分析出不同地址之间的关联关系，从而将交易者的交易关系分散在相互无关联的地址中，增加分析交易者身份的难度。目前的混币机制主要分为中心化的混币机制和去中心化的混币机制，在执行效率、混币效果、混币费用等指标上还有提升空间，并存在拒绝服务攻击、混币过程泄密等安全问题。

混币机制能够模糊区块链交易中付款人和收款人的关系，增加攻击者通过公开账本分析用户交易规律的难度，是一种提升区块链隐私保护能力的有效机制。通过研究混币机制的原理，分析不同混币机制存在的优势和缺陷，有利于设计出性能更优的混币机制，同时为不同场景下混币机制的选择提供评价依据。

2 相关知识

2.1 区块链技术概述

区块链是诞生于比特币的底层技术，最早的定义来自于中本聪在2008年发表的文章③，近年来在不断的延伸与扩展中发生了很多改变，逐渐形成了新型技术体系，且仍然在不断发展演变。通常认为区块链系统的基础架构可以按照数据层、网络层、共识层、激励层、合约层和应用层进行划分，但是随着区块链技术的发展，很多传统的模块被弱化，甚至不存在意义，例如在联盟链和私有链技术中已经不需要激励层。通过分析区块链的核心技术与发展趋势，可以将区块链技术的基础架构简化为3个层次，即网络层、交易层和应用层。

① https://en.bitcoin.it/wiki/Coinbase

② http://8btc.com/article-2027-1.html

③ https://www.bitcoin.org/bitcoin.pdf

网络层负责区块链网络的建立和各个节点之间的信息转发。交易层负责交易数据的创建、验证和存储，应用层负责提供多样化的应用服务。

其中，区块链的核心业务是在交易层中实现的，即两个“地址”之间以交易的形式进行可靠、具有公信力的数据传递。交易层的主要内容包括地址格式、交易格式、全局账本和共识机制。

区块链中的“地址”是用户为了隐藏真实身份而使用的假名，可以使用公钥并经过加密算法（例如ECC）得到。在加密算法中，公钥用于生成交易的输入地址与输出地址，私钥信息由用户自己保存，用于生成支付比特币时所必需的证明资金所有权的签名。

区块链中的“交易”对用户之间数据交互的过程进行记录，并发布于区块链网络。交易中包含输入地址、输出地址和交易内容等信息。交易内容在数字货币中代表交易的金额，在其他应用中，可能代表一个字符串或者一个证书ID。在区块链数字货币应用中，为了保证交易的可靠性，支付方必须有足够的资金进行支付，区块链交易中将采用特殊设计确保输入资金大于输出资金。例如，比特币中输入地址不仅包含付款方的账户信息，还包含此项输入资金的来源信息和签名信息，验证方可以根据输入地址信息找到资金源头，并利用签名验证发送方是否有指定资金的所有权。

全局账本是区块链的数据存储结构，用于存储所有的交易记录、合约以及相关的参数信息。全局账本通常由“区块”构成，交易信息按照一定顺序存储在区块中，同时保存这些交易的散列值、时间戳等参数，每个区块中可以存储的交易信息是有限的。区块之间按照时间关系通过区块散列连接。全局账本在系统中不是集中存储的，所有参与节点都各自维护一个本地的全局账本，邻居节点之间通过定期的信息交换使全局账本保持同步。

区块链技术的共识机制可以保证区块链网络中事务的顺序在所有节点上保持一致。常见的共识机制包括工作证明（proof of work，POW）机制[6]、股权证明（proof of stake，POS）机制④、拜占庭容错（PBFT）机制[7]等。共识机制的目的是使分布式的节点能够按照统一的规则验证交易合法性，并选出相同的一组交易作为下一个区块的数据。例如，POW机制的基本工作原理是众多竞争节点通过解决一个数学难题竞争记账权，只有被证明付出了最大工作量的节点才可以当选为记账节点，该节点有权在区块链上记录新的交易，生成新的区块。其他节点会以很小的计算代价验证此区块上的所有交易，合法的区块将被所有节点同步。通过这种机制，能够保证分布式节点中的全局账本是相同的，而且全局账本中的每一笔交易都要经过大多数节点的认可，具有较高的公信力。

④ https://bravenewcoin.com/assets/Uploads/TransactionsAsProofOfStake10.pdf

2.2 区块链交易面临的隐私泄露威胁

根据区块链技术的特点，可以分析出区块链交易具有以下特征。

- 区块链交易中包含输入地址和输出地址信息，而且每一个输入地址都指向前一笔交易，即所有输入资金都能够追溯到源头。
- 区块链交易存储在公开的全局账本中，任意参与用户都可以获得完整的全局账本。而且由于在共识过程验证节点需要检索历史交易，因此所有的交易信息不能直接采用加密等手段保护数据。

这些特征导致区块链交易数据面临隐私泄露威胁。以比特币为例，比特币交易中的地址都是由用户自行创建且与身份信息无关的，任何人无法直接通过观察交易记

录推测出交易中用户的身份信息。但是全局账本公开的交易之间存在关联关系，潜在攻击者有可能通过分析全局账本中的交易记录推测出比特币地址的交易规律，包括地址的交易频率、交易特征、地址之间的关联关系等。基于这些规律，攻击者有可能将匿名比特币地址和特定用户相关联。

目前已经有许多研究通过分析区块链交易推测区块链用户的隐私信息。根据分析目的的不同，可以将这些研究分为以下两类。

第一类研究主要通过分析地址相关的交易记录，获得该地址交易的规律特征，据此推测对应用户的身份信息。由于在某一特定类型的区块链交易中会存在它特有的交易特征，攻击者可以根据地址的交易特征，对其交易发生的真实场景进行还原，从而做出用户真实身份的推测。Androulaki E等人[8]设计了一个匹配区块链地址与学生身份的模拟实验，学生以比特币作为日常交易的支付手段，并使用比特币推荐的一次性地址方法加强隐私保护，分析人员通过基于行为的聚类技术，能够以42%的准确率将学生身份和区块链地址成功匹配。Monaco J V[9]将比特币用户的交易行为进行量化，以交易时间间隔、资金流向等12项参数为依据分析用户的交易规律，经过6个月实验得到的大量数据表明，利用这种分析模型成功识别用户真实身份的精度高达62%，错误率低于10.1%。

第二类研究主要利用区块链交易设计中存在的一些潜在知识，实现对不同地址的聚类，得到同一个用户的多个地址。针对地址聚类目前主要有以下3条聚类规则。

- 对于一个具有多输入地址的交易，通常认为所有的输入地址都来自同一个用户个体或用户的集合。当用户发起一次交易时，资金可能来自于用户的多个地址，而多输入交易中用户需要对每个输入地址单独进行签名，因此大多数多输入交易的输入地址来自同一个用户。这项规则已经应用于很多研究中[1-3]，取得了很好的聚类效果。
- 同一个Coinbase交易中的多个输出地址属于同一个用户集合。随着“挖矿”难度的增加，个体“矿工”已经无法在竞争中获胜，需要成百上千的“矿工”加入“矿池”共同完成一次“挖矿”，得到的奖励会分配给参与集体“挖矿”的“矿工”。Coinbase交易表示将奖励发送给“矿工”的过程。
- 交易中找零地址和输入地址隶属于同一个用户。在一次交易中，输入地址中的总金额可能会大于用户发出的金额，因此比特币系统会为发送方自动产生一个找零地址，用于接收交易中的找零资金。找零地址与其他地址一样都有可能被系统选择成为新的交易中的输入地址，但作为输出地址的情况一般只会出现一次。由于找零地址在交易发生时是由系统重新生成的，因此一个地址不可能同时作为一次交易的输入地址和输出地址，交易的输出中也必然存在找零地址以外的输出地址。利用找零地址的这些特征，可以发现更多地址之间的关联关系。

目前已经有很多研究利用上述聚类规则，发现了比特币系统中很多地址之间的关联性。Meiklejohn S等人[4]通过使用启发式聚类方法实现了对比特币盗窃案件中相关比特币地址的识别。Zhao C[5]完成了一个全面的聚类过程，根据比特币全局账本中的全部交易数据，将35 587 286个比特币地址划分为13 062 822个用户的地址集合。

3 混币机制

完全公开的交易存储机制使区块链交

易存在隐私泄露风险，因此有必要在区块链系统中采用相应的隐私保护机制，在满足区块链共识机制的条件下，尽可能隐藏数据信息和数据背后的知识。在现有的研究中，一种广泛应用的方法是在不改变交易结果的前提下改变交易过程，使攻击者无法直接获得交易的完整信息，这种方法被称为“混币”。Chaum D[10]的文章提出了一种匿名通信技术，在通信过程中隐藏了真实的通信内容，基本思想可以通过式(1)表达：

$$C_M(Z_1,C_A(Z_0,m),A)\rightarrow C_A(Z_0,m),A \quad (1)$$

式(1)左侧为发送方发给中间人的信息，右侧为中间人将信息处理后发送给接收方的消息。发送方想要将消息Z_0和m发送给接收方的地址A，首先使用接收方的密钥C_A对消息进行加密得到$C_A(Z_0,m)$，然后将中间人的验证消息Z_1、加密后的消息$C_A(Z_0,m)$和接收方地址A进行打包，并使用中间人的公钥C_M进行加密，防止信息在发送过程中被攻击者截获或篡改。中间人收到信息后使用自己的私钥进行解密，得到Z_1，$C_A(Z_0,m)$，A，但无法解密$C_A(Z_0,m)$的内容。中间人在验证Z_1无误后，将$C_A(Z_0,m)$发送给地址A。接收方使用自己的私钥解密消息，完成此次通信。

利用这种方法，消息没有在发送者和接收者之间直接传递，而是通过中间人间接传递，使攻击者无法观察到真实发送者和接收者之间的通信行为，提高了通信的匿名性。若将消息通过多个中间人进行传递，攻击者发现双方通信关系的难度将大大增加。

数字货币中的混币机制借鉴了上述思想，通过中间人对资金进行中转，使攻击者无法直接发现交易中真实的发送方和接收方。数字货币的混币机制原理如**图1**所示。假设A和A_1是一个用户的两个数字货币地址，C是潜在攻击者，能观察到发生的所有交易。用户希望使用地址A向地址A_1转账，但是不希望潜在攻击者发现这次交易。通过采用混币机制，攻击者C无法直接观察到从A到A_1的交易过程，从而不会发现A和A_1的关联。

混币过程的执行可以由可信的第三方或某种协议实现。根据混币过程中有无第三方节点参与，将现有的混币机制分为两类：基于中心节点的混币机制和去中心化的混币机制。这两种机制在混币可靠性、混币效率和混币成本等方面各有优势和缺陷，本文将分别介绍两类混币机制的原理和特点。

4 基于中心节点的混币机制

基于中心节点的混币机制中，混币过程由第三方节点集中执行，因此也可以称为中心化混币方案。参与混币的用户首先将资金发送给第三方节点，第三方节点收到多个混币用户发来的资金后进行一系列资金分配，最终将指定金额的资金分别转移给指定的收款地址。由于资金没有直接在发送方和接收方之间传递，而是经过第三方节点的处理，对资金流向进行了干扰，因此攻击者很难发现参与用户的资金流向。

基于中心节点的混币方法原理如**图2**所示。用户希望使用地址A向地址A_1转账，但为了防止潜在攻击者C直接发现A和A_1的关系，可以首先使用地址A向第三方地址D转账，D在一段时间后向用户指定的地址A_1转账，最终实现资金在A和A_1之间的转移。在一定时间内，第三方节点可能完成了多个用户的混币过程，这在一定程度上隐藏了A和A_1的关系，使得攻击者无法在A_1、E_1、F_1中找到与A具有关联关系的地址。但是通过综合分析A、D、A_1三者在一段时间内的

交易过程，攻击者有一定概率猜测出A和A_1是一次真实交易的发送方与接收方。例如，在一定时间内D有n个输出，则攻击者找到正确交易链路的概率是$1/n$。

为了防止潜在攻击者推测出混币过程隐藏的交易关系，第三方节点在执行混币机制时需要遵循一定的限制条件，具体如下。

● A向D转账和D向A_1转账这两笔交易之间需要存在一定时间间隔t。否则，攻击者可以根据时间关系推测出真实的交易关系。

● 在时间间隔t以内，D发出的交易数量n越多，混币的效果越好，因为这将减小推测成功的概率$1/n$。

● 在一次混币过程中，各项真实交易的金额不能有明显区别。当第三方节点发出的交易中仅有一笔发送给A_1的交易金额与A发出的金额相近，那么攻击者可以由此猜测出A-D-A_1的交易链路。

● 第三方节点可以使用不同的地址作为转账的接收方和发送方，从而提升混币效果。如**图3**所示，第三方的地址D收到来自A的转账，然后通过地址E将资金转出。这种情况下，攻击者C在不知道D和D_1关系的情况下，很难推测出A和A_1的交易关系。

此类方法简单易行，不需要额外的技术改进，适用于比特币等各种数字货币。这种机制中，用户根据经验选择混币服务提供商，首先向混币服务商转移资金，并支付一定的服务费用，混币服务商收到后将资金转移给用户指定的地址。目前提供这种混币服务的网站有BitLaundry、Bitcoin Fog[⑤]、Blockchain.info等。

但是，使用这种方法完成混币的过程完全依赖于第三方节点，因此存在以下几点严重的缺陷。

● 额外收费和交易延迟。混币服务提供商通常会收取一定的混币费用，并且随着混币次数的增加，费用直线上升，混币时

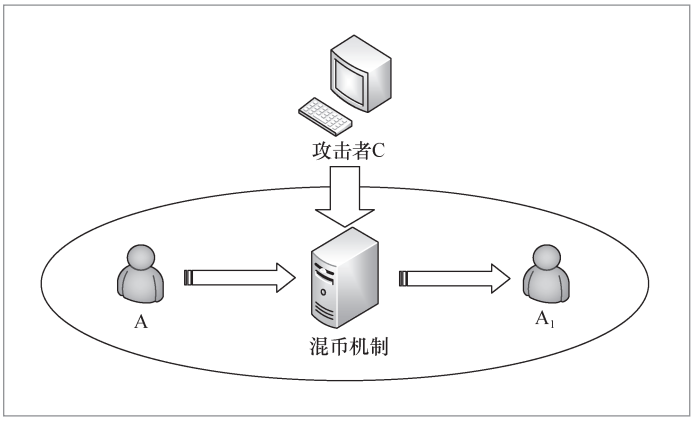

图1 混币机制原理

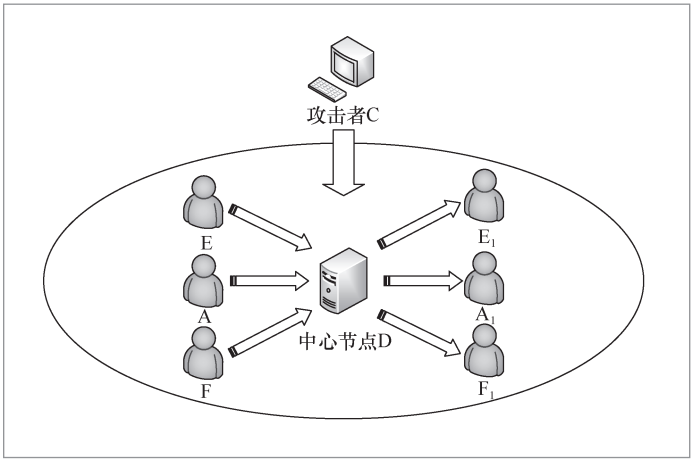

图2 基于中心节点的混币机制原理

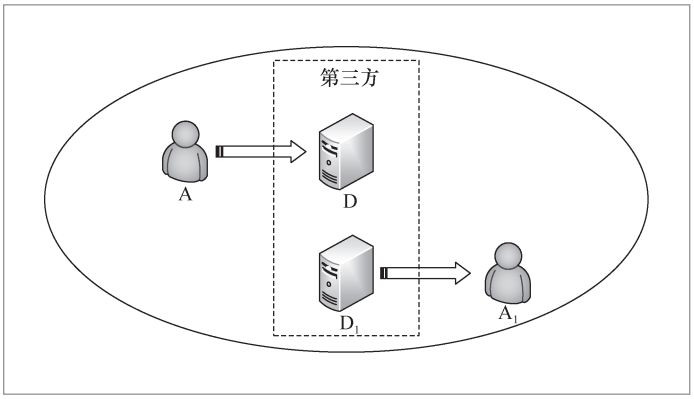

图3 第三方使用多地址的混币过程

⑤ http://bitcoinfog.info/

间也会增加。通常混币的时延为48 h，交易费用为1%~3%。

● 第三方可能偷窃资金。若在混币服务中不设置高效的监督机制，第三方节点有可能在收到用户资金后不执行约定的转账操作，偷窃用户资金，而用户无法追责。

● 第三方可能泄露混币过程。由于第三方节点掌握全部的混币过程，了解真实的交易内容，从而无法保证混币信息不被泄露。

为了保证第三方节点的可信度，Bonneau J等人[11]提出一种改进的中心化混币方案——Mixcoin。通过设置审计功能，使用户有权公布签名数据，揭露第三方节点的违规行为，混币服务商将付出失去信誉的代价。但是该方案没有从根源上解除第三方对信息泄露的威胁。Valenta L等人[12]在Mixcoin的基础上使用盲签名技术进一步优化，设计了Blindcoin方案，使第三方节点在正常提供混币服务的同时，无法得到所有交易中交易双方的真实信息，从而避免信息泄露的风险。但使用盲签名技术必然会增加混币过程中的计算量。ShenTu Q C等人[13]提出一种更加高效的盲签名混币方案，使用椭圆曲线加密算法提升计算效率。2015年上线运营的匿名数字货币达世币（Dash）⑥是一款基于比特币技术，并以保护用户隐私为目的的数字货币。达世币中所有执行混币过程的中心节点都必须支付高额押金作为担保，否则无法获得提供混币服务的权利。这种方案通过加设第三方节点违规操作应付出的代价，保护混币用户的隐私及财产安全。

⑥ https://www.dash.org/

中心化混币方案的本质是单纯地将一笔资金在多个地址中进行多次转移，实现简单，易于操作，混币过程不需要其他的技术支持，在区块链技术下的各类数字货币系统中具有极高的适用性。但是，现有的中心化混币方案普遍存在时延问题。大多数改进方案通过增加第三方违规的代价来防止盗窃和信息泄露的发生，不能从根本上杜绝违规行为的发生，采用盲签名等密码学技术的混币方案会增加计算代价，并且由第三方执行混币过程必然会带来额外的服务开销。笔者从是否需要混币费用、是否存在盗窃风险等方面对现有的中心化混币机制特征作出对比分析，见**表1**。

5 去中心化的混币机制

去中心化混币方案的混币过程通过混币协议实现，不需要第三方节点参与。最早的去中心化混币方案是由 Gregory Maxwell在比特币论坛上提出的CoinJoin机制。CoinJoin机制核心思想是通过将多个交易合并成一个交易的方法，隐藏交易双方输入输出的对应关系。如**图4**所示，当一笔交易中只有一个输入地址与一个输出地址时，攻击者可以直接观察到交易双方的关联关系，而在CoinJoin机制下，若干笔单输入—单输出交易被合并为一笔多输入—多输出交易，交易的双方由两个单独的地址变为两个地址的集合。对于一个多输入—多输出交易，潜在攻击者无法通

表1 基于中心节点混币机制特征对比

混币机制	混币费用	额外开销	盗窃风险	混币过程泄露风险
Mix	有	时间开销高	高	高
Mixcoin	有	时间开销高	中，支持审计	高
Blindcoin	有	计算开销高	中，支持审计	低，使用盲签名
Dash	有	需要额外押金	中，具备惩罚机制	高

2018005-7

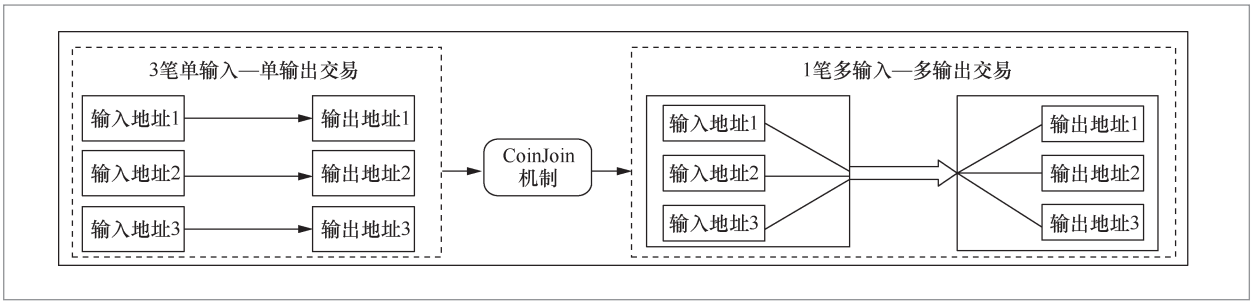

图 4 CoinJoin 机制示意

过观察交易信息确认输入和输出之间的对应关系。一般情况下，CoinJoin机制需要第三方服务器撮合所有混币申请方进行签名。CoinJoin交易中，每个用户独立分散地完成签名，只有提供了所有签名并进行合并，交易才能被判定合法，并被网络接收。这种去中心化的混币机制免除了第三方服务提供者的参与，混币过程是在所有混币用户的共同参与下完成的，从而有效避免了第三方盗窃与泄露混币信息的风险。CoinJoin是去中心化混币机制的基础，其思想被运用在多种匿名比特币协议中，例如Dark Wallet⑦、CoinShuffle⑧和 Join Market。

CoinJoin机制对所有用户交易的匿名性提供了强大的保障。即使只有部分用户使用这种协议，攻击者也会因无法准确识别全局账本中使用该协议的交易，而无法使用第2.2节中介绍的分析方法。这种不依赖第三方节点的混币机制能够从根源解决中心化混币方案中存在的资金偷窃、混币费用等问题。但是，由于没有第三方参与混币的组织与执行，混币用户往往需要自行组织协商，并完成混币过程，从而暴露出以下问题：

- 依然需要第三方节点协助完成寻找混币用户的过程，因此仍不可避免中心化混币中的一些威胁；
- 参与混币的用户在协商的过程中可能暴露自己的混币信息，无法保证所有混币参与方守信；
- 在执行混币过程中，如果由于部分节点违规操作导致混币失败，攻击者有可能趁机发起拒绝服务攻击；
- CoinJoin方案形成的多输入多输出交易将记录在全局账本中，用户无法抵赖其曾经参与过混币。

针对CoinJoin机制的缺陷，出现了很多改进方法。Ruffing T等人[14]提出一种完全去中心化的比特币混币协议——CoinShuffle，在CoinJoin的基础上增加了将输出地址洗牌的机制，使混币参与者无法得到自己以外的交易地址关联关系。但是该方案在执行混币过程时要求所有参与者同时在线，容易遭受拒绝服务攻击。Bissias G等人[15]提出一种基于区块链广告匿名寻找混币参与者的去中心化混币协议——Xim，随着混币参与用户数量的增加，攻击者发动攻击的代价也会线性增加，从而有效避免拒绝服务攻击。CoinParty[16]中由安全多方计算模拟可信第三方，即使在部分混币参与节点恶意操作或失效的情况下，混币过程依然有效。门罗币（Monero）⑨的混币机制中采用了环型加密匿名技术，使混币参与用户无需与其他参与节点进行交流，可自行参与混币，为去中心化混币机制中常见的拒绝服务攻击、混币用户泄露信息等问题提供了有效

⑦ https://www.wired.com/2014/04/dark-wallet/

⑧ http://insidebitcoins.com/news/coinshuffle-aims-to-improve-privacy-in-bitcoin/29269

⑨ https://getmonero.org//knowledge-base/about

的防御措施。

去中心化混币机制取消了第三方混币提供者的参与，通过混币协议使混币过程在多个用户的共同参与下完成。因此混币过程的安全不依赖于第三方节点的可信度，用户也无需为混币服务花费额外的费用。但是，很多去中心化混币方案具有很高的遭受攻击的风险，该问题通常需要以改进算法的方式解决，因此也增加了混币机制的计算成本，影响混币服务的效率。针对混币机制中是否需要混币费用、是否存在盗窃风险等特征，笔者对现有的几种典型去中心化混币机制进行了对比分析，见**表2**。

6 未来研究方向

由于传统的基于混币机制的隐私保护方案实现简单，不会对区块链原有的共识机制产生影响，在现有的区块链应用中得到了推广。但区块链的混币机制中依然存在一些缺陷。在区块链技术持续发展的同时，还需要对混币机制做进一步的研究。

如果不借助其他隐私保护技术，混币机制的隐私保护效果十分有限，分析人员仍然可以使用特定的分析方法发现交易中隐藏的信息。因此，有必要通过采用密码学算法保证混币的安全性，例如零知识证明机制和同态加密机制。但引入加密机制需要对底层协议进行大幅改动，并需要消耗更多的计算资源，影响区块链应用的效率。虽然已经出现一些扩展方法对原本效率不高的安全混币机制进行了改良，使计算量大大减小，例如Pinocchio Coin[17]和ZeroCash[18]有望显著降低Zerocoin的证明规模和计算成本，但这些方案及扩展的改良方案都需要对区块链系统做出重大修改，从而无法落实到实际应用中。因此希望隐私保护机制在保护系统安全的同时尽量避免对系统做出改动。然而，现有的一些能够直接部署在区块链上的机制（如CoinShuffle）往往不具有足够的安全性，存在着遭受攻击的风险。

在未来的研究中，需要使用一种更加安全高效的加密方案为混币机制的执行提供保障。密码学算法保护下的混币机制需要充分考虑区块链服务器在计算性能和存储性能上的缺陷，同时还需要重点考虑如何避免或者减少对区块链底层协议的修改，使安全高效的混币机制更容易得到落实与推广。

7 结束语

本文介绍了区块链技术中用于保护交易数据隐私的混币机制。首先，从隐私保护中面临的威胁出发，说明了混币机制的核心思想和应用场景；其次，对混币机制的基本原理进行了详细的阐述；最后，分别从基于第三方节点的混币方法和去中心化的

表 2 去中心化混币机制特征对比

混币机制	混币费用	特殊需求	盗窃风险	拒绝服务风险
CoinJoin	无	无	无	高
CoinShuffle	无	需要参与者同时在线	无	高
Xim	有	无	无	低
CoinParty	无	无	无	低
Monero	无	环签名导致额外计算开销	无	低

2018005-9

混币方法的角度，详细地分析了两类混币方法的优势与缺陷，总结了现有混币方案作出的改进，并展望了混币机制未来可能的研究方向。

参考文献：

[1] REID F, HARRIGAN M. An analysis of anonymity in the Bitcoin system[C]//The 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust, October 9–11, 2011, Boston, USA. Piscataway: IEEE Press, 2011: 1318–1326.

[2] LIAO K, ZHAO Z, DOUPE A, et al. Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin[C] //The Symposium on Electronic Crime Research, June 1–3, 2016, Toronto, Canada. Piscataway: IEEE Press, 2016: 1–13.

[3] RON D, SHAMIR A. Quantitative analysis of the full Bitcoin transaction graph[C]//The 17th International Conference on Financial Cryptography and Data Security, April 1–5, 2013, Okinawa, Japan. Heidelberg: Springer, 2013: 6–24.

[4] MEIKLEJOHN S, POMAROLE M, JORDAN G, et al. A fistful of bitcoins: characterizing payments among men with no names[C]//The 13th ACM Internet Measurement Conference, October 23–25, 2013, Barcelona, Spain. New York: ACM Press, 2013: 127–140.

[5] ZHAO C. Graph–based forensic investigation of Bitcoin transactions[D]. Iowa: Iowa State University, 2014.

[6] DWORK C, NAOR M. Pricing via processing or combatting junk mail[C]//The 12th Annual International Cryptology Conference on Advances in Cryptology, August 16–20, 1992, Santa Barbara, USA. Piscataway: IEEE Press, 1992: 139–147.

[7] CASTRO M, LISKOV B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398–461.

[8] ANDROULAKI E, KARAME G O, ROESCHLIN M, et al. Evaluating user privacy in Bitcoin[C]// The 17th International Conference on Financial Cryptography and Data Security, April 1–5, 2013, Okinawa, Japan. Heidelberg: Springer, 2013: 34–51.

[9] MONACO J V. Identifying Bitcoin users by transaction behavior[C]//The SPIE DSS, April 20–25, 2015, Baltimore, USA. Baltimore: SPIE, 2015.

[10] CHAUM D. Untraceable electronic mail, return addresses and digital pseudonyms[J]. Communications of the ACM, 2003: 211–219.

[11] BONNEAU J, NARAYANAN A, MILLER A, et al. Mixcoin: anonymity for Bitcoin with accountable mixes [C]//The 19th International Conference on Financial Cryptography and Data Security, January 26–30, 2015, San Juan, Argentina. Barbados: Financial Cryptography, 2014: 486–504.

[12] VALENTA L, ROWAN B. Blindcoin: blinded, accountable mixes for Bitcoin[J]. Financial Cryptography and Data Security, 2015: 112–126

[13] SHENTU Q C, YU J P. A blind–mixing scheme for Bitcoin based on an elliptic curve cryptography blind digital signature algorithm[J]. Computer Science, 2015.

[14] RUFFING T, MORENO–SANCHEZ P, KATE A. CoinShuffle: practical decentralized coin mixing for Bitcoin[M]//Computer Security –ESORICS 2014, Heidelberg: Springer, 2014: 345–364.

[15] BISSIAS G, OZISIK A P, LEVINE B N, et al. Sybil–resistant mixing for Bitcoin[C]//The 2015 ACM Workshop on Privacy in the Electronic Society, November 3, 2014, Scottsdale, USA. New York: ACM Press, 2014: 149–158.

[16] ZIEGELDORF J H, GROSSMANN F, HENZE M, et al. CoinParty: secure multi –party mixing of Bitcoins[C]//The 5th ACM Conference on Data and Application Security and Privacy, March 2–4, 2015, San Antonio, USA. New York: ACM Press, 2015: 75–86.

[17] DANEZIS G, FOURNET C, KOHLWEISS M, et al. Pinocchio coin: building zerocoin from a

succinct pairing–based proof system[C]// ACM Workshop on Language Support for Privacy–Enhancing Technologies, November 4, 2013, Berlin, Germany. New York: ACM Press, 2013: 27–30.

[18] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payments from Bitcoin[C]//The 2014 IEEE Symposium on Security and Privacy, May 18–21, 2014, Berkeley, USA. Washington: IEEE Computer Society, 2014: 459–474.

作者简介

祝烈煌（1976-），男，博士，北京理工大学计算机学院教授、副院长、博士生导师，网络与信息安全研究所所长，主要研究方向为密码算法与安全协议、区块链技术、大数据隐私保护等。

董慧（1993-），女，北京理工大学计算机学院硕士生，主要研究方向为区块链应用与隐私保护。

沈蒙（1988-），男，博士，北京理工大学计算机学院讲师、硕士生导师，主要研究方向为数据安全共享与隐私保护。

收稿日期：2017-12-14

2018005-11