数字货币的匿名性研究

付 烁 徐海霞 李佩丽 马添军

(中国科学院信息工程研究所信息安全国家重点实验室 北京 100093)

(中国科学院数据与通信保护研究教育中心 北京 100093)

(中国科学院大学网络空间安全学院 北京 100049)

摘 要 随着现代化信息技术的发展,数字货币已经被越来越多的人接受和认可.目前主流的数字货币在提供便捷性、不可伪造等安全性的同时,还存在不同程度的匿名性问题.一方面,数字货币应该有效保护用户的隐私;另一方面,提供匿名性的数字货币不能成为不法分子的犯罪工具.本文综述了数字货币匿名性的研究现状.首先,介绍数字货币的产生与分类,指出私人数字货币按发展历程可以分为中心化和去中心化数字货币两种;之后,本文按照数字货币的类型,阐述典型的数字货币方案,并对其安全性进行了对比和分析,重点研究了当前数字货币方案匿名性的特点和问题.最后,本文介绍了法定数字货币,定义法定数字货币的匿名性,从法定数字货币角度探讨现阶段数字货币技术的实用性并对数字货币匿名性的未来研究方向进行了展望.

关键词 数字货币;匿名性;假名性;不可链接性;区块链;法定数字货币

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2019.01045

A Survey on Anonymity of Digital Currency

FU Shuo XU Hai-Xia LI Pei-Li MA Tian-Jun

(*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)

(*Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing* 100093)

(*School of Cyber Security, University of Chinese Academy of Sciences, Beijing* 100049)

Abstract With the development of modern information technology, digital currency has been accepted by more and more people. Digital currency makes it easier to transfer funds directly between two parties in a transaction without the need of a trusted third party such as a bank or a credit card company; these transfers are facilitated through the use of public keys and private keys for security purposes. Digital currency provides a more convenient payment method, it can reduce the high cost of traditional banknotes issuance and circulation, improve the transparency of economic transactions, and reduce illegal and criminal activities such as money laundering and tax evasion. The popular digital currencies are Bitcoin, Litecoin, Ripple, etc. There are currently thousands of digital currencies in the world. The mainstream digital currency can provide convenience, unforgeability, unchangeable and other security. However, these digital currencies still have problems in privacy protection. Privacy protection includes the anonymous of the user and the confidentiality of the transaction content. On the one hand, the anonymity of digital currency should effectively protect users' privacy, for the user may not want other users know which transaction belongs to him or want to keep the transaction content especially the amount private; on the other hand, an anonymous digital currency should not be a tool for criminals, for the crim-

收稿日期:2017-08-27;在线出版日期:2018-09-07.本课题得到国家重点研发计划(2017YFB0802500)资助.**付 烁**,硕士研究生,主要研究方向为安全多方计算、数字货币、安全协议.E-mail:fushuo@iie.ac.cn.**徐海霞**(通信作者),博士,副教授,主要研究方向为安全多方计算、数字货币.E-mail:xuhaixia@iie.ac.cn.**李佩丽**,博士,助理研究员,主要研究方向为数字货币、安全协议.E-mail:lipeili@iie.ac.cn.**马添军**,博士研究生,主要研究方向为智能合约、数字货币.

inal may use the privacy protection method to protect his identity and illegal behavior. There is a lot of research work on the privacy protection of digital currency, such as Zerocoin, Zerocash, Monero etc. They provide varying degrees of privacy. This paper summarizes the research status of the private digital currency. Firstly, we introduce the generation and classification of digital currency, and point out that private digital currency is divided into two types: centralized digital currency and decentralized digital currency. Centralized digital currency has the existence of a trusted center (such as a central bank), typically represented by E-Cash. Decentralized digital currencies often use peer-to-peer (P2P) networks, and users are free to join the network to participate in the issuance and circulation of currencies. Secondly, this paper describes the typical scheme of digital currency, including E-Cash and Bitcoin. We discuss decentralized digital currency and its anonymity, analyze Bitcoin anonymity issues and typical solutions, and explore other decentralized digital currencies, including Monroe, Zerocoin, Zerocash, etc. According to the main evaluation index for the safety of digital currency, we compare these digital currency schemes from the perspective of digital fiat currency, summarizing the anonymity of these schemes and pointing out their advantages and shortcomings. Then, this paper discusses the current research status of fiat digital currency in China, defines the anonymity of legal digital currency and discusses the practicality of digital currency technology at this stage from the perspective of legal digital currency. The anonymity scheme of the current mainstream digital currency is analyzed for the enlightenment of the legal digital currency. Finally, we end up with discussing future research directions of anonymous of digital currency, which include efficient and secure consensus algorithm, innovation in cryptography technology and research on regulatory technology.

Keywords digital currency; anonymous; pseudonymity; unlinkability; blockchain; digital fiat currency

1 引 言

数字货币是金融学与计算机技术融合的产物，与传统纸质货币相比，数字货币不依赖于货币实体，而是利用密码学技术拥有防止伪造、防止二次支付等安全特性.

匿名性是数字货币的重要特性之一. 随着数字货币技术的不断发展和广泛应用，其面临的匿名性问题越来越多. 一方面，人们在使用数字货币时重视个人隐私，为了能够实现去中心化的数字货币的分布式节点的共识，交易记录会在全网公开，为用户带来账户余额信息泄露、身份位置信息暴露[1]等风险. 另一方面，私人数字货币缺乏监管，用户交易时不需要实名注册，使犯罪分子有机可乘，2017 年频繁爆发的全球性比特币勒索案件就是私人数字货币被不法分子利用的典型.

近年来，对数字货币的匿名性研究主要局限于基于区块链技术的比特币. 文献[2]首次对比特币的分布式账本进行分析，指出比特币可能存在的匿名性问题. 文献[3]对当时已发表的比特币匿名研究论文进行回顾，指出了比特币面临的匿名性挑战和问题的成因. 文献[4]介绍了几种典型的解决比特币匿名性问题的方案，针对比特币的匿名性比较这些方案的优缺点，并指出未来比特币的匿名性需要研究任意数额的交易混合. 文献[5]对比特币的安全性和隐私性问题进行了系统化的调研和深入分析. 针对用户的隐私保护问题，比较了相关技术，进行分类总结. 文献[6]则着重剖析了比特币系统，并分析系统面临的匿名性和隐私保护的挑战.

目前针对数字货币匿名性的研究工作缺少对非区块链技术的数字货币进行综合考量和对比分析. 除此之外，法定数字货币的匿名性研究还处于空白阶段.

本文对数字货币的匿名性进行综述. 按照数字货币的发展历程分析各种数字货币. 充分结合法定

数字货币的特点，综合现阶段法定数字货币的研究现状，分析各类数字货币的匿名性方法对法定数字货币的应用意义，填补法定数字货币的匿名性研究空白.

本文第 2 节介绍数字货币的产生与分类；第 3 节讨论中心化数字货币及其匿名性；第 4 节讨论去中心化数字货币及其匿名性，分析比特币的匿名性问题和典型的解决方案，探讨其它去中心化数字货币，包括门罗币、Zerocoin、Zerocash 等；第 5 节主要讨论我国法定数字货币及其匿名性，介绍法定数字货币的内涵和必要性，针对法定数字货币，分析主流数字货币技术的可行性；最后，对数字货币匿名性的未来研究方向进行总结和展望.

2　数字货币的产生与分类

金属冶炼技术的发展促进了金属铸币的诞生，纸币则依赖造纸和印刷技术的进步，数字货币的产生与发展也是以新技术的应用为前提条件的. 计算机技术、网络技术的快速发展，为数字货币的产生提供了核心保证. 网络时代的到来，更是刺激了支付工具的创新，消费者对支付的便捷性、安全性要求的不断提高也是数字货币的产生、发展的源动力.

数字货币是一种非实物货币，本身不以任何物理介质为载体[7]，具有类似于实物货币的性质，可以用来购买实物商品和服务，也可能被限制在一定范围内使用，如应用于社交网络等[8]. 数字货币以电子方式记录货币的余额，使货币形式的符号化更加彻底、更为纯粹. 与历史上出现的其他货币形式一样，数字货币的产生与发展是一定的社会经济条件和背景下的客观经济规律，是货币形式发展演变的历史的、逻辑的必然结果.

数字货币源于电子货币（E-Cash）. 1982 年，Chaum 发表了一篇题为《用于不可追踪的支付系统的盲签名》的论文[9]. 文中提出一种基于“银行—个人—商家”三方模式的货币模型，银行是一个权威的中心化机构，个人与商家之间的交易必须依赖这个中心化机构才能完成. 文章强调了模型中的中心化机构不能获知关于支付的信息，确保用户的匿名性和隐私性得到保护. 这个方案被认为是最早的数字货币系统，一经提出便引起学者的兴趣和多方研究.

2008 年，中本聪发表了一篇题为《比特币：一种 P2P 的电子现金系统》的报告①. 系统通过参与者的计算代替中心机构，变成了点对点的两方模式. 货币的各环节不依托任何实物，仅使用密码技术和校验技术来创建、分发、维护. 这种新型的电子现金系统就是比特币（Bitcoin）.

2009 年 1 月，比特币正式上线，吸引了许多技术爱好者加入比特币系统的开发和维护工作，比特币的应用也越来越广. 2014 年，关于比特币的研究报告大量出现，受到密码学和经济学领域的专家学者关注，相继产生了许多关于比特币的研讨会. 2017 年 11 月，单个比特币的价格突破 10 000 美元，保持了比特币在 2017 年的强劲上升势头，总市值接近 2000 亿美元.

比特币已经成为目前最成功的数字货币之一. 支撑比特币运行的区块链技术，由于具有去中心化、防篡改等特点[10]，也在金融、教育、物联网等领域有应用[11-12]. 在比特币热潮之下，涌现出一系列私人数字货币. 然而，私人数字货币存在许多问题，如缺少监管操作、价值波动剧烈、交易平台有安全隐患等[13-15].

面对私人数字货币的种种问题和推行数字货币的种种优势，许多国家已经开展法定数字货币的研究工作. 2015 年，英国央行首次提出中央银行数字货币（Central Bank Issued Digital Currency）的理念[16]，并联合伦敦大学学院的研究人员合作研究了 RSCoin[17-18]. 加拿大、澳大利亚、日本等国家也表示未来会推出数字化的官方货币. 我国也在 2017 年成立数字货币研究所，旨在推行我国的法定数字货币[19].

总体上，从价值支撑层面考虑，可以将数字货币分为私人数字货币和法定数字货币. 法定数字货币以国家信用为价值支撑，能够有效发挥货币功能，稳定货币价值. 目前，市场中大多数的数字货币均为私人数字货币. 纵观私人数字货币的发展历程，按照体系结构，可以将私人数字货币分为两类：中心化数字货币，典型代表为 E-Cash；去中心化数字货币，典型代表为比特币. 二者的主要区别在于是否存在中心节点控制货币的发行、流通等生命周期的各个环节.

数字货币作为一种货币，关系到使用者的直接利益，应该满足一定的安全性质. 数字货币的安全性包括基本安全性和可满足安全性. 为了更好的评价数字货币方案，我们将考虑数字货币的以下安全性[20]：

① Nakamoto S. Bitcoin：A peer-to-peer electronic cash system (2008). https://bitcoin.org/bitcoin.pdf

(1)不可重复交易性.货币只能消费一次,双重支付应该容易被检验;

(2)匿名性.合法用户的隐私受到保护;

(3)不可伪造性.所有人都不能伪造可花费的货币;

(4)可传递性.货币所有权转移时不需要第三方参与,且转移的过程不能被追踪;

(5)可拆分、可聚合.货币能像现实生活中一样具有可找零、可以组合支付的功能.

其中,不可重复交易性、匿名性、不可伪造性都是数字货币需要严格满足的基本性质,而可传递性以及可拆分、可聚合性能够有利于数字货币的应用,但是并不是数字货币的基本安全性.

3 中心化数字货币及其匿名性

对交易安全性和隐私性的重视,使得 Chaum 致力于实现一种可以仿真现实硬币和纸币的电子形式的货币,并提出首个中心化数字货币系统——E-Cash[9].数字货币的产生就是以匿名性为前提,各类中心化数字货币方案都是在保证匿名性的同时,探讨数字货币的其他安全性需求.

3.1 Chaum 的 E-Cash

E-Cash 系统通过盲签名算法实现.协议[9]包括一个消息提供者(Provider)和签名者(Signer),盲签名算法的目的是让签名者为消息提供者的信息签名,同时签名者不知道消息提供者发送给他的实际内容是什么.所以盲签名算法具有以下安全属性[9,21]:

(1)公开可验证性.任何知道验证算法的人都能验证签名的真伪;

(2)签名的不可伪造性.证明者只能从签名者的签名中剥离出有效签名,即使证明者请求签名者进行多个消息的签名,证明者也不能伪造其他合法签名;

(3)盲签名性.签名者并不知道所签名的消息内容;

(4)不可追踪性.在签名被接收者泄露后,签后者不能追踪签名.

利用基于 RSA 的盲签名算法,Chaum 设计了一个不可追踪的电子支付系统,系统包括"银行—个人—商家"三方,个人用户和商家在银行有自己的账户.银行具有货币发行、验证账户、修改账户余额等功能,是系统中的可信第三方机构.

在系统中进行一次匿名支付的过程主要包含以下四个步骤:签发硬币、支付硬币、收取硬币及通知用户交易结果,如图 1 所示.

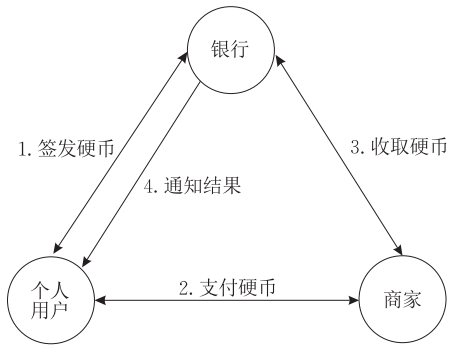

图 1 E-Cash 的一次匿名支付过程

签发硬币是银行为用户选取的硬币序列号进行一次盲签名的过程.硬币的支付、收取以及通知用户结果等环节需要验证这个盲签名.假设用户要向商家支付一元钱,详细的支付过程包括以下 8 个步骤:

(1)用户选择硬币的序列号,并对该序列号进行盲化;

(2)用户将盲化后的序列号及其对应面额发送给银行,请求银行签名;

(3)银行检查用户的账户余额,余额足够则为用户签名,并在用户的账户扣除对应金额;

(4)银行将签名结果发送给用户;

(5)用户对签名去盲,剥离出对硬币的签名;

(6)用户验证签名,若银行签名有误,交易终止,否则,用户将其发送给商家;

(7)商家首先检验签名,如果用户篡改了银行的签名,交易终止;否则,商家接受这枚硬币,并将其发送给银行进行用户二次支付的确认和账户信息的修改;

(8)银行检验签名,确认商家未篡改签名信息,并确认该枚硬币没有出现在交易账本中,防止商家二次支付某一硬币.如果检验都成立,银行在商家的账户上增加相应的金额,并通知个人用户交易完成.

上述过程包含一枚硬币的完整生命周期,在该方案中,用户和商家的每次交易都需要产生一枚新的硬币,并且由银行验证并回收硬币.所以对该系统的安全性分析如下:

(1)不可重复交易.系统将硬币序列号的签名作为支付凭证,通过查询银行维护的数据库防止货币进行双重支付,所以 E-Cash 系统具有不可重复交易的安全特性;

(2)匿名性.在签发硬币阶段,银行对于盲化之

后的硬币签名，此时银行不能得到关于用户硬币的信息，而在银行从商家处收取硬币时，商家看到的是用银行的签名而不是用户的签名，银行从商家处收取的硬币也与用户身份无关. 通过盲签名，银行无法建立硬币和用户间的对应关系，无法追踪硬币，从而保护了用户的隐私，从而保护了用户的隐私，银行和商家的勾结也不能追踪货币的使用情况，系统具有很高的匿名性；

(3) 不可伪造性. 伪造货币相当于伪造银行的签名，难度相当于分解大素数；

(4) 可传递性. 在 E-Cash 系统中，每次交易都需要银行进行货币发行和验证，所以 E-Cash 系统不具有可传递性；

(5) 可拆分、可聚合. 由于 E-Cash 系统中定义了银行能够签发硬币的面额，所以用户不能申请任意面额的货币，该系统不满足货币可拆分、可聚合的性质.

E-Cash 系统通过盲签名算法达到了很高的匿名性，适用于隐私保护要求较高的场景. 系统的匿名性也是一把双刃剑[22]：对于诚实用户具有促进作用，能够有效保护用户的信息安全；同时，匿名性会为一些犯罪行为提供便利，使犯罪分子的身份不被获知. 除此之外，在每次支付硬币时，商家和银行都要进行联机检验货币的有效性，这虽然能够防止双重支付，保障系统具有较好的安全性，但巨大的通信量和银行验证中心的瓶颈降低系统的效率.

E-Cash 的出现标志着数字货币的诞生，引发了密码学界、金融界对数字货币的兴趣. 但是该方案存在货币不可传递、不可拆分、不可聚合及交易效率低等问题，所以没有得到大规模的应用.

3.2　Juels 的可追踪 E-Cash

基于 Chaum 方案完全匿名性带来的监管问题[23]，Juels[24] 提出了一种基于“信任标识(Trustee Token)”的可信第三方追踪机制，并将该机制应用于 Chaum 的 E-Cash 系统，给出了一种简单、高效、安全的可控匿名性 E-Cash 系统.

与 Chaum 的 E-Cash 系统相比，Juels 引入可信第三方为用户产生交易所需的“信任标识”. 由于“信任标识”的规模较小，用户可以向可信第三方请求大量的“信任标识”并存储. 每个“信任标识”只能使用一次，在用户用完“信任标识”之前，用户不需要与可信第三方联系.

货币的序列号不再由用户自由选择，而是与用户的身份 ID_U 相关. 可信第三方与银行之间共享对称密钥 ω，进行“信任标识”的检验.

用户获得可信第三方的一系列“信任标识”，具体过程如图 2 所示.

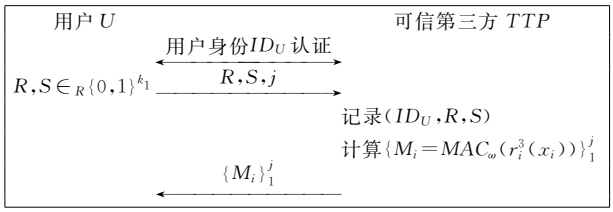

图 2　可信第三方产生信任标识的过程

(1) 用户向可信第三方证明身份 ID_U；

(2) 用户选取随机数 R 和 S，连同他想申请的“信任标识”数量 j 一同发给可信第三方，其中，R 和 S 都是带索引的伪随机数生成器的密钥种，R 用于产生盲化硬币序列号的随机数，S 则用于产生硬币序列号；

(3) 可信第三方记录用户的信息和随机数，计算“信任标识”传递给用户. 其中，$x_i=E_{PK_r}(ID_U\|s_i)$，s_i 由 S 产生，E_{PK_r} 是可信第三方公钥 PK_r 的加密函数.

在签发硬币时，用户需要将硬币的盲化信息 $r_i^3(x_i)$ 与“信任标识” M_i 一同发送给银行，由于可信第三方与银行之间共享对称密钥 ω，银行可以在验证 M_i 正确性后再对货币进行盲签名. 如图 3 所示.

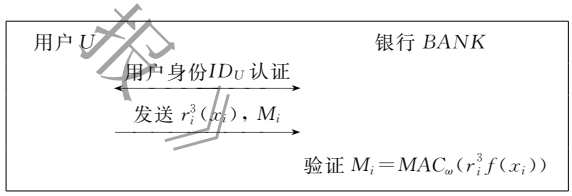

图 3　银行验证用户“信任标识”

若要追踪一枚硬币，可以将硬币 x_i 发送给可信第三方，可信第三方利用私钥解密 x_i，即可提取对应的用户身份 ID_U.

若需要追踪用户 ID_U 所有的硬币，则将 ID_U 发送给可信第三方，可信第三方可以通过查询数据库中存储的用户随机数 R 和 S 计算出用户持有的所有硬币.

由于系统仅仅在 Chaum 方案的基础上引入了“信任标识”，货币的生命周期没有发生变化，所有额外的交互都在货币产生之前，所以系统仍然具有不可重复交易、不可伪造的安全性. 系统的匿名性则受可信第三方的影响，如果可信第三方是诚实的，银行和用户依然无法追踪货币，只有第三方能够追查用

户身份或货币的所属者.但是该修改方案显然带来了可信第三方的效率和安全问题.

3.3 Foteini 的可传递 E-Cash

除了匿名监管问题,Chaum 的 E-Cash 系统的另一个局限性在于,每笔交易必须通过银行辅助完成,这无疑增加了银行的工作量.而且,人们希望交易可以在用户之间直接进行.所以,基于以上现实需求,Foteini 等人提出了可传递的 E-Cash 系统[25].系统的主要技术方案是可延展签名[26],货币传递的过程中不需要可信第三方参与,是第一个有效、完全匿名且可传递的 E-Cash 系统.

可延展签名允许参与者通过消息 m 的签名计算消息 m' 的签名.可延展签名方案除了具有不可伪造性、公开可验证等基本属性,还具有 m' 签名结果不会暴露 m 的任何额外信息的安全性[26].

在 Foteini 的系统中,每枚硬币都有双重支付标签防止出现重复交易.除此之外,Foteini 为货币增加了转移次数属性,用户 S 将硬币传递给 R 的过程就是利用签名方案的可延展性产生新签名的过程.利用新的签名构造硬币,使得硬币不会暴露用户的身份信息,而且该转移过程只需要发送者和接收者两人参与.对该方案的安全性分析如下:

(1)不可重复交易.系统为每个硬币增加了双重支付标签,硬币传递的过程中检验标签是否出现,防止双重支付;

(2)匿名性.该方案的匿名性达到了观察后接收、花费后观察以及花费后接收完全匿名性①,即考虑一个控制银行的敌手,敌手不能将观察到的诚实用户的硬币与新接收的硬币联系起来;敌手不能将自己在之前花费过的硬币与新观察到的诚实用户的硬币联系起来;当银行是诚实的,敌手不能识别出一枚硬币是否是自己曾花费过的;

(3)不可伪造性.系统通过可扩展签名方案的强不可伪造性,保证了货币的不可伪造性;

(4)可传递性.该方案主要解决传统 E-Cash 的可传递性问题,具有可传递性;

(5)可拆分、可聚合性.该方案依然没有解决 E-Cash 的组合支付及找零问题.

Foteini 的方案是 E-Cash 系统的重要革新之一,解决了中心化数字货币普遍存在的货币不可传递的问题.但是,该方案的货币依然不可拆分、不可聚合,货币的价值自产生之后不会改变,极大地限制数字货币的流通.在匿名性方面,该方案依然是完全匿名的数字货币方案,存在监管困境.

3.4 中心化数字货币系统对比分析

对上述三种中心化数字货币系统,按照技术特点、安全特性进行比较,结果如表 1 所示.

表 1 中心化数字货币系统对比

性质	系统		
	Chaum	Juels	Foteini
技术特点	盲签名	信任标识	可扩展签名
不可重复交易性	√	√	√
匿名性	完全匿名性	可控匿名性	完全匿名性
不可伪造性	√	√	√
可传递性	×	×	√
可拆分、可聚合	×	×	×

通过表 1 可知,在匿名性方面,Chaum 和 Foteini 的方案匿名性较高,即使银行参与也无法追踪用户或硬币,Juels 的方案则引入可信第三方用于用户身份和货币的追踪.

除此之外,中心化数字货币系统因为有银行参与货币的发行和流通环节,能够实现数字货币的不可重复交易和不可伪造性.但这类系统普遍存在货币不可传递、不可拆分、不可聚合问题,不利于进行大量交易.

4 去中心化数字货币及其匿名性

去中心化数字货币往往采用对等(P2P)网络,用户可以自由地加入网络参与货币的发行和流通[27].系统中的用户可以创建多个地址保护个人信息.所以,我们采用以下衡量标准评价这类数字货币的匿名性:

(1)假名性.用户使用数字货币时不会直接暴露真实身份;

(2)不可链接性[28].用户地址的不可链接性,即敌手难以将同一用户的不同地址链接起来.多个交易的不可链接性,即敌手难以将同一用户的不同交易链接起来.交易输入输出的不可链接性,即敌手难以将一笔交易的发送方和接收方链接起来.

通过这个标准,本节主要分析比特币的匿名性问题及匿名性保护方案.并比较其他针对匿名性和用户隐私提出的数字货币,包括门罗币、Zerocoin、Zerocash 等等.

4.1 比特币的匿名性

比特币是第一个去中心化数字货币,也是目前

① Antonopoulos A M. Master Bitcoin. 2015. https://github.com/bitcoinbook/bitcoinbook/releases/tag/Edition1Print1

最受欢迎的数字货币之一[29]. 比特币基于密码学原理而不基于信任，使得任何达成一致的双方，能够直接进行支付，从而不需要第三方中介的参与. 比特币的去中心化主要通过链式存储结构和工作量证明机制[30-31]实现.

比特币系统采用基于国际互联网的 P2P 网络架构，该网络具有去中心化、开放性的特点. 任何用户都可以随时加入比特币网络中，参与货币的发行、流通，进行比特币的交易.

由于用户可以产生任意数量的地址，加入网络和创建地址的过程不需要实名认证，所以系统满足假名性.

传统的数字货币用序列号作为货币的唯一标识，比特币没有货币实体，而是通过未使用的交易输出(Unspent Transaction Output)，即 UTXO，来构造新的交易.

比特币交易指明了一定数额的货币流向，可以包括一个或多个输入地址和输出地址. 每笔输入都是一个有效的 UTXO. 发送方对输入地址的交易和接收方公钥进行数字签名，并将这个签名附加在末尾，即可产生一笔交易. 而其他人通过对签名进行检验，就能够验证该链条的所有者.

为了防止交易的双重支付，传统的数字货币方案引入可信第三方检验每一笔交易，并在每一笔交易结束后，回收货币重新发行. 这种方案使得整个系统完全依赖于这一可信第三方.

比特币采用的解决方法是，将这笔交易公开，让全网所有节点共同验证交易，从而代替可信第三方. 为了实现这一点，全网的所有节点都需要拥有一条共同的历史交易序列.

系统采用区块这一数据结构记录和确认交易信息. 每个区块包括区块头和区块体两部分. 区块头记录了前一区块的哈希值，当前区块的时间戳及 Merkle 树根等信息. 交易数据会通过 Merkle 树的哈希过程生成唯一的 Merkle 树根值记录在区块的区块头，这样的存储结构便于交易信息的查询和校验，也有利于空间回收. 比特币的区块结构如图 4 所示.

为了构造区块，比特币系统采用一个类似于哈希现金中的的工作量证明机制. 在区块中增加一个随机数区域，这个随机数要使得该区块的哈希值满足头部具有目标多个 0. 产生区块的节点需要反复尝试来找到这个随机数，这一过程通常被称为“挖矿”. 由于此后的区块是链接在该区块之后的，所以想要更改该区块中的信息，就需要重新完成之后所有区块的工作量. 所以，工作量证明机制能够防止区块被

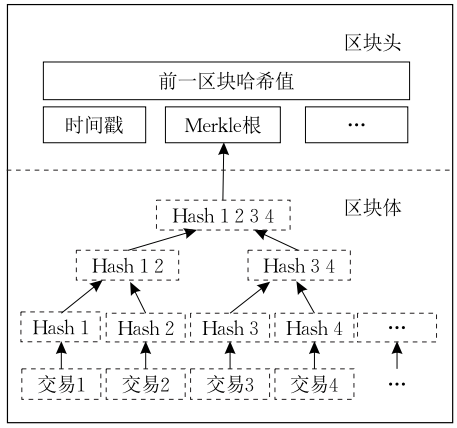

图 4　区块的数据结构

篡改，形成有效的区块链条，即区块链.

由于区块链公开了所有交易信息，包括交易的面额，交易的输入地址和输出地址. 所有人都能够观察、分析区块链中的数据. 所以，学者对比特币是否能实现不可链接性、不可链接性达到了怎样的程度进行了深入分析.

最初针对比特币的分析主要基于两点假设：交易的所有输入地址属于同一个真实用户[32]；有多个输出的交易可能存在找零地址，即多个输出中有一个地址属于交易的发送方[33].

这些假设符合现实生活中交易. 假设用户想要购买商品，交易单位用 BTC 表示，即比特币. 商品的价格为 8BTC，用户拥有三个地址，对应交易金额为 5BTC、3BTC 和 6BTC. 用户只能利用多个地址进行的组合支付，如图 5 所示.

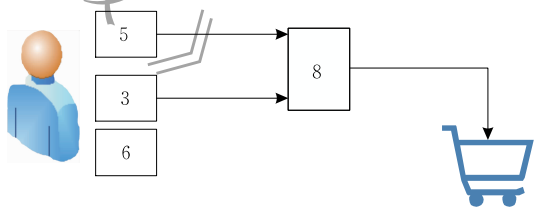

图 5　结合多个输入地址的比特币交易

这种情况满足对于比特币的第一点假设.

另一方面，拥有三个比特币地址，对应金额分别为 5BTC、3BTC 和 6BTC 的用户想要购买 8.5BTC 的商品，由于比特币交易无法直接拆分，用户需要组合 3BTC 和 6BTC，并返回自己 0.5BTC. 所以这笔支付交易有两个输出，如图 6 所示.

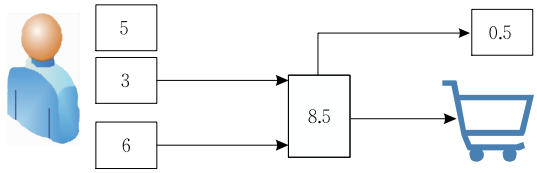

图 6　存在找零地址的比特币交易

虽然不能直接将输出值更小的地址视为找零地址，但是比特币钱包会为用户产生新地址用于找零，进一步分析区块链并确认找零地址十分容易.

通过上述假设可以初步构建比特币用户网络.将比特币用户网络进一步联系外部的互联网资源(如社交网络、论坛等用户信息)，有获得用户真实身份的可能.例如，用户在论坛中公开自己的比特币地址，如果这个用户对应的论坛账户信息被盗取，比特币地址对应的真实身份就不言而喻了.

通过分析区块链的交易信息，敌手可能将同一用户的不同地址链接起来，从而将这些地址涉及到的交易链接起来.敌手还有能力将同一笔交易的输入输出链接起来.所以，比特币系统不具有交易输入输出的不可链接性、不具有用户地址的不可链接性以及多个交易的不可链接性.

之后，对于比特币的分析，学者进行了实验认证[34]，用更直观的图表展现比特币的地址、交易分布，证实了比特币不可链接性存在的安全隐患.

此外，区块链的公开账簿有利于敌手识别用户的具体使用习惯[35].学者基于对比特币交易的两点假设，利用自己的比特币地址向已知服务(矿池、外汇网站等)进行支付，确认服务商的地址，观察服务商的未来交易，实现大型比特币交易的追踪.Spagnuol[36]设计了一个自动化区块链信息分析工具——BitIodine，并在实际使用情况中测试：根据美国联邦调查局的描述，利用 BitIodine 工具，找到杀手 Dread Pirate Roberts 的一笔交易.

虽然对比特币分析方法有利于打击犯罪，在现实生活中具有积极意义.但是在本质上，这些分析结果表明比特币系统的不可链接性存在问题.比特币系统的匿名性实际只实现了假名性.采用数字货币系统的安全性标准对比特币系统进行分析，分析结果如表 2 所示.

表 2 比特币系统的安全性分析

性质	满足	技术	说明
不可重复交易	√	工作量证明 数字签名	诚实节点算力大于全网的 50%
匿名性	部分满足	产生任意数量的 ID； 区块链数据公开	只做到假名性，不具有不可链接性
不可伪造性	√	工作量证明 数字签名	诚实节点算力大于全网的 50%
可传递性	√	交易	货币没有具体面额
可拆分 可聚合	√	交易	用户自定义交易

与中心化数字货币相比，比特币通过交易的方式实现了数字货币的传递、拆分及聚合.但是，比特币的不可链接性问题亟需解决，学者针对这类问题设计了许多应用于比特币系统之上的保护方案.

4.2 基于比特币的混合方案

1981 年，Chaum[37]首次提出了混合网络的概念，并给出基本的混合协议.混合协议可以为任意通信系统提供保护.参与混合协议的用户将消息加密，并通过一系列可信混合器传送.这些混合器将消息进行解密和随机置换，再按照一定的规则发送给接收方.这一系列的置换使得追踪某个具体消息变得十分困难.

比特币独特的脚本语言可以让用户自定义交易规则，具有多个输入的交易可以进行相互独立的签名.这一特性使混合协议可以应用在比特币系统中.用户之间采用混合协议将多笔交易混合为一个多输入、多输出的交易，交易混合的结构如图 7 所示.

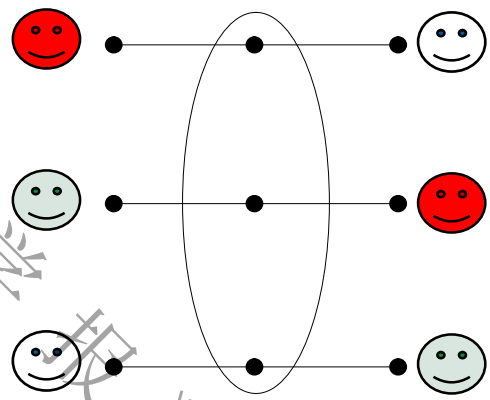

图 7 比特币交易的混合

每个用户将两个地址作为交易的输入输出发送给混合器.混合器置换这三个用户的地址，形成一笔交易.为了使交易有效，参与混合的所有用户都应提供混合交易的有效签名.即使有敌手拒绝服务，不对交易签名，也只是导致混合失败，敌手不会偷到其他用户的比特币.

其他用户即使获得这笔交易，也不能确定交易的输出地址与输入地址的对应关系.从而割裂交易的输入输出，显然，Reid 和 Harrigan[32]、Androulaki 等人[33]的假设无法分析此类交易.

最早的比特币混合方案是 Barber 等人[38]提出的二方混合.之后，Bissias 等人提出了一个名为 Xim[39]的系统，将两方混合协议设计为一个多轮协议，增强匿名性.同时，系统允许用户寻找匿名合伙人，使混合过程更加灵活.

利用混合方案保护比特币匿名性的技术日渐成

熟，混合方案也从最初的中心化混合发展为去中心化的混合，典型的混合方案包括 Mixcoin、Coinjoin①、CoinShuffle 以及 CoinShuffle++，这些方案的效率越来越高，实用性越来越强，逐渐得到了人们的广泛应用.

4.2.1　中心化的混合——Mixcoin

Mixcoin[40] 是最初的比特币中心化混合系统，混合协议有许多的限制：协议固定了混合的交易额，不允许用户进行交易货币的数量选择搭配. 由于需要第三方的参与，系统引入问责机制(accountability). 在混合之前，每个用户会获得混合器的签名作为担保，通过这个签名公开验证混合器的行为，发现混合器的恶意操作. 但是这种问责机制只能做到事后补救，如果混合器不在意自己的声誉，混合器可能存储用户的混合的信息并进行恶意公开. 为了减少恶意的混合器的影响、防止混合器之间合谋，可以采用多个不同混合器进行混合.

考虑到交易的混合费变化会影响用户的匿名性，作者提出了随机混合费用机制. 用户要混合的交易金额及混合费用是否收取，由一些预定义的混合器决定. 采用随机混合费用机制，使得混合费用不作为交易金额的一部分，混合的输入地址与输出地址具有相同的值.

假设参与混合的用户足够多，经过混合，敌手难以链接混合交易中同一用户的输入地址和输出地址，也难以将这一笔混合交易的发送方和接收方链接起来. 若每个用户在交易之前都进行一次混合协议，敌手将难以链接同一用户的不同交易. 所以，采用这一混合协议能够实现比特币的不可链接性，利于保护交易地址.

但是这种混合方式有很大的局限性，而且受混合器的影响很大：所有参与混合的交易金额必须一致，否则敌手能够通过交易金额发现输入输出地址之间的对应关系. 混合器必须足够诚实：一方面，混合器不能记录用户参与混合的输入输出，混合器不应该询问用户的身份信息；另一方面，系统需要防止混合器偷币.

鉴于中心化混合对混合器的要求很高，逐渐产生了去中心化的混合方案.

4.2.2　去中心化的混合——Coinjoin

Coinjoin 是最早的比特币去中心化混合系统. 用户能够自发寻找混合参与者，共同创建一个包含所有输入的比特币交易.

一个 Coinjoin 交易结构的例子如图 8 所示. 其中三个同样的输出是 Coinjoin 的结果，输入的比特币值大于输出的比特币值，两者之差是本次交易的交易费用.

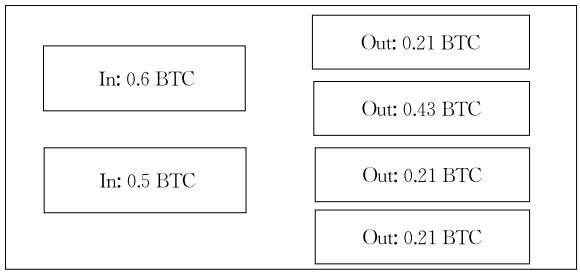

图 8　Coinjoin 混合交易示例

与图 7 相比，Coinjoin 系统不需要混合器进行交易的置换. 用户需要自发地寻找想要参与混合的用户，产生 Coinjoin 交易.

在比特币的不可链接性方面，本质上，Coinjoin 与 Mixcoin 的混合方式相似，Coinjoin 也能实现三层含义的不可链接性.

与 Mixcoin 协议相比，Coinjoin 通过一个 P2P 的混合协议自发的进行混币操作，这与比特币系统的架构更加切合. 而且 Coinjoin 混合协议还有以下优点：首先，它没有自举问题，用户不必等待中心化的混合器出现，混合可以自发进行、随时进行；其次，在去中心化的混合中不会有偷币的情况出现，协议能确保用户的输入金额与输出金额相等.

Coinjoin 虽然能够防止偷币，但是发生偷币后无法避免同一敌手再次破坏混合，为了解决这一问题，产生了更好的混合系统——CoinShuffle.

4.2.3　CoinShuffle

CoinShuffle[41] 系统的灵感源于 Coinjoin，最大的技术创新是引入纠察机制，每次混合失败都能找到恶意节点，用户可以避开恶意节点进行下一轮操作.

系统假设每个用户已经拥有比特币地址，用户发送消息前会利用地址对应的私钥签名. 混合固定的操作顺序，系统假设用户操作顺序公开已知，用户已经协商好要混合的交易数额.

该协议遵循 Coinjoin 范式：一组用户共同创建一个混合交易，并且每个用户可以独自确认自己不会丢失金钱，一旦受到欺骗，用户拒绝对交易进行签名.

CoinShuffle 协议的系统架构如图 9 所示.

① Maxwell G. Coinjoin: Bitcoin privacy for the real world. Post on bitcoin forum. https://bitcointalk.org/index.php?topic=279249

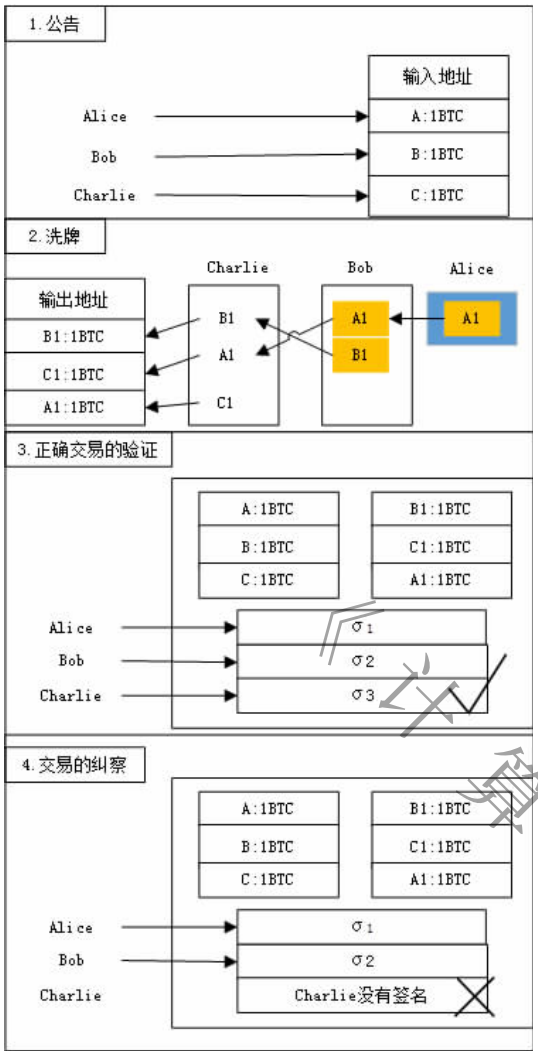

图 9 CoinShuffle 系统架构

协议包含 4 个步骤：公告(announcement)、洗牌(shuffling)、正确交易的验证(Transaction Verification)及错误的纠察(Blame). CoinShuffle 系统的流程如下：

(1) 公告. 公告阶段发生在混合之前，用户生成一个新的临时加密-解密密钥对并广播；

(2) 洗牌. 用户创建一个新的比特币地址作为混合交易的输出地址. 之后，用户采用一个解密混合网络，打乱刚生成的输出地址，得到输出地址集合，由最后一个用户广播这个集合；

(3) 正确交易的验证. 用户验证自己的输出地址在集合中. 如果存在，用户创建混合交易，对交易签名后广播. 用户在收到所有其他用户的签名后，能够创建一个完全签名版本的混合交易，将这笔交易发布到比特币网络；

(4) 错误的纠察. 在前面阶段的每一步，用户都能检查其他用户是否遵守协议. 一旦存在非法操作，协议进入纠察阶段，识别行为异常的用户. 行为不端的用户会在随后协议的运行中被排除.

与 Coinjoin 相比，在 CoinShuffle 系统中，偷币行为会在第一时间被发现，攻击者不能偷取或破坏诚实用户的货币，系统具有可验证性. 系统还具有健壮性，恶意参与者会在纠察阶段被找到排除，只要通信连接可用，即使存在恶意的参与者，协议最终也会成功.

然而，在 CoinShuffle 系统中，最好情况下的通信轮数和参与者的个数呈线性相关，最坏情况下的通信轮数与参与者个数的平方相关. 作者对系统性能进行的实验分析结果表明，50 个用户产生一个混合交易需要大约 3 min，系统的效率较低，与比特币每秒 7 笔的吞吐率相比，该方案降低了交易速度.

4.2.4 CoinShuffle++

为了解决 CoinShuffle 系统的通信效率问题，Ruffing 等人进行了更深入的研究，设计了一个点对点(P2P)的匿名通信协议[42].

作者基于 DC-net(Dining Cryptographer net)协议设计新的 P2P 混合方案. DC-net 协议思想是：两个参与者 p_1 和 p_2 共享密钥 k，用户 p_1 想要匿名发布消息 m，于是 p_1 发布消息 $M_1=m\oplus k$，p_2 发布消息 $M_2=k$. 观察者可以计算 $M_1\oplus M_2=m$，但是不知道 m 由谁发出. n 个参与者两两之间进行上述操作，就能隐藏消息 $m_1,m_2,\cdots,m_n$ 的来源.

基于以上构造的 DC-net，作者设计了 DiceMix 协议. 并将 DiceMix 协议和 Coinjoin 结合，设计了能够应用于比特币系统的 CoinShuffle++协议.

该方案与 CoinShuffle 的主要区别在于地址的混合方式不同，用 DiceMix 协议代替 CoinShuffle 的解密混合网络，不需要复杂的加解密运算，所以系统能够达到与 CoinShuffle 相同的安全目标，同时又具有更高的通信速度. CoinShuffle++协议在最好情况下，只需要常数轮通信，在最坏情况下(假设存在 f 个恶意参与方)也只需要 $4+2f$ 轮通信. 在有 50 个参与方的场景下，CoinShuffle++在 8 s 内就可以完成混合交易. 所以 CoinShuffle++系统具有更高的实用性.

4.2.5 混合方案的对比

从中心化到去中心化，从安全性到混合效率的提高，比特币混合方案的发展日趋成熟. 对上述比特币混合方案的对比情况如表 3 所示.

表 3　比特币混合方案对比

混合方案	分类	技术	方案总结
Mixcoin	中心化混合	问责机制；随机交易费用	优点：不可链接性，兼容；缺点：不能自定义混合金额，安全性受混合器影响，需要混合费用，有被偷币的风险
Coinjoin	去中心化混合	匿名通信 Tor 交换地址信息	优点：不可链接性，兼容，防止偷币，无额外的混合费用；缺点：不能自定义混合金额，敌手会终止混合
CoinShuffle	去中心化混合	公钥加密方案；解密混合网络	优点：不可链接性，兼容，防止偷币，无额外混合费用，能纠察敌手；缺点：不能自定义混合金额，效率较低
CoinShuffle++	去中心化混合	DC-net 协议；DiceMix 协议	优点：不可链接性，兼容，防止偷币，无额外混合费用；纠察敌手；效率更高；缺点：不能自定义混合金额

总体上，采用混合的方法与比特币系统兼容；混合方案可以保护比特币的交易地址，实现不可链接性.

但是，所有的混合方案都无法解决一个问题：不能自定义混合的金额，所有参与混合的用户必须进行相同金额的交易，这是由区块链公开交易金额导致. 此外，混合方案存在开销问题，系统需要消耗更多的计算机资源和通信资源实现混合.

鉴于采用混合方案保护比特币系统具有一定的约束，许多学者从数字货币的发行或流通等环节修改比特币方案，从而提出了不同的去中心化数字货币解决匿名性问题，门罗币（Monero）、Zerocoin、Zerocash 是其中最典型的三种.

4.3　门罗币

门罗币（Monero）关注隐私性（privacy）、去中心化（decentralisation）和扩展性（scalability），系统基于 CryptoNote 协议和相关代码，主要采用环签名算法[43]和一次性随机地址技术解决数字货币的匿名性问题.

环签名同群签名[44-46]一样，也是一种模糊签名者的签名方案，与群签名不同的是，环签名中的小组成员没有管理员，不会因为管理员的陷门信息暴露出具体的签名者[47].

在环签名系统中，所有可能的成员构成一个环，每个成员都有自己的私钥和公钥，签名者用自己的私钥和其他所有环成员的公钥生成签名.

环签名最重要的安全性是无条件匿名性，当环成员个数为 n 时，敌手不会以大于 $1/n$ 的概率识别产生环签名的真正签名者.

在门罗币中，用户可以混合一系列具有相同面额的交易，通过环签名技术，混合过程中不需要其他参与者的签名，从而在交易的多个输出中隐藏自己的真实身份. 这样，敌手难以将一笔交易的输入地址与输出地址链接起来，实现了交易交易输入输出的不可链接性.

采用环签名技术能够保护单个交易的不可链接性，但是还不足以保护用户多个地址的关系以及多个交易之间的关联. 针对这个问题，门罗币提出了一次性随机地址的解决方案.

一次性随机地址源于 Diffie-Hellman 的交换协议[48]. 交易的发送方利用接收方的地址和一个随机数为接收方产生一次性随机地址. 由于随机数只由发送方掌握，其他人无法发现随机地址和接收方之间的关系. 随机数也保证了随机地址互不相同，随机地址间没有任何联系.

通过环签名和一次性随机地址两种技术，门罗币实现了不可链接性的三层含义. 然而，在实际应用时，学者依然发现门罗币存在匿名性问题.

门罗币在设计之初没有规定交易的输出面额，后来，门罗币开发者定义了门罗币的输出面额[49]为 $A\times 10^B$，其中 A 是整数，且 $1\leq A\leq 9$，$b\geq -12$. 之前不符合面额范式的交易就难以进一步与其他交易混合[50].

鉴于混合方案的局限性，学者对于数字货币的匿名性研究逐渐从混合转向引入其他密码学技术，匿名性解决方案不再仅仅针对地址，而是为用户提供普通货币和匿名货币的转换.

4.4　Zerocoin

Zerocoin[51]是霍普金斯大学的 Miers 等学者基于零知识证明技术提出的比特币扩展方案，系统需要利用基础货币 Basecoin 产生 Zerocoin.

系统中的 Basecoin 与比特币系统具有相同的结构，是用户进行交易的基础货币. 如果用户有隐私保护的要求，则需要将 Basecoin 转换为 Zerocoin. Zerocoin 系统利用的密码学技术主要是零知识证明，每个 Zerocoin 作为用户拥有未花费的基础货币的证据，使得货币转换过程能够切断新货币与老货币之间的联系.

Zerocoin 的产生过程与比特币有很大差别：用户需要拥有对应金额的 Basecoin，而且系统要求所有用户能够访问一个公告板.

由于 Basecoin 与比特币结构相同，区块链充当了公告板的角色. 用户 Alice 产生一枚 Zerocoin 后会将硬币的承诺和对应金额公开.

所有的 Zerocoin 都是这样产生，每次铸币后，区块链上都会出现新的硬币. 所以，区块链上会有所有未花费的 Zerocoin 对应的承诺集合. 用户花费 Zerocoin 时则需要证明自己拥有集合中的一个元素，用户通过产生一个非交互的零知识证明 π，证明：

(1) 用户知道硬币的承诺在公告板中；

(2) 用户知道公开承诺的随机数.

其他用户验证 π 的正确性并检验硬币是否在其他交易中出现过，避免双重支付. 若这两个条件都满足，则交易成功.

Zerocoin 应用 Fiat-Shamir 的启发式算法[52]将 Schnorr 等人的零知识证明方案[53]转换为一个非交互的零知识证明，使得任意概率多项式敌手区分两枚不同 Zerocoin 的概率是可忽略的，实现了货币的不可链接，避免敌手通过货币实现用户身份的追踪.

但是，Zerocoin 系统具有一定的局限性. 一方面，使用 Zerocoin 不能有效的拆分和组合，用户在产生 Zerocoin 时需要考虑铸币面额；另一方面，Zerocoin 不隐藏交易金额和交易的接收地址，如果交易面额唯一，其他用户就能够将这枚 Zerocoin 关联到原始硬币上，从而再次破坏该用户的不可链接性.

4.5 Zerocash

鉴于 Zerocoin 存在的种种问题，Eli 等人提出了一种新的数字货币方案——Zerocash[54]. 在 Zerocash 中，用户同样可以在 Basecoin 和 Zerocash 之间转换.

Zerocash 最初是在比特币交易的区块链主链上增加的侧链，这条侧链使交易的发送方对货币进行拆分再组合，从而达到匿名交易的目的. 随着 Zerocash 的技术日渐成熟，目前，Zerocash 已经不再以比特币侧链的形式被使用，而是开发出一种新的数字货币.

Zerocash 在许多方面与比特币相同：都是基于账本结构，货币产生采用工作量证明机制，有 2100 万的总量上限，不同的是，Zerocash 更注重用户的隐私保护.

Zerocash 的功能通过两类交易实现：铸币(mint)交易和熔币(pour)交易. 与比特币相同，Zerocash 也采用区块链作为去中心化的交易账本，产生的交易会被广播并附加到区块链上.

铸币交易用于产生 Zerocash. 用户将指定数量的 Basecoin 转换为相同金额的 Zerocash. 交易通过基于 SHA-256 散列函数的承诺方案隐藏 Zerocash 的价值和用户的地址.

熔币交易为用户提供私密支付. 一般来说，一个熔币交易最多有两枚输入硬币和两枚输出硬币，交易采用一个零知识证明，证明以下信息：

(1) 用户拥有这两个输入硬币；

(2) 每枚输入硬币都在以前的铸币交易的或熔币交易中出现；

(3) 交易前后，硬币的总价值相等.

熔币交易在花费输入硬币时只显示硬币的序列号，不显示硬币面额或地址等其他信息，从而将输入硬币匿名转换为输出硬币.

由于 Zerocash 交易隐藏价值和地址，所以敌手无法获得他人的账户余额.

与 Zerocoin 不同的是，Zerocash 的熔币交易使货币能够以任何方式拆分或合并保留. Zerocash 支持用户直接付款，在交易过程中隐藏相应交易的支付来源、去向和交易金额，为用户提供更高的隐私保护.

系统能达到账本的不可区分性(Ledger Indistinguishability)，敌手不能区分两个不同的账本，不能通过账本获得公开信息之外的任何内容. 敌手无法从账本中分析出额外信息，就无法链接任何交易，所以 Zerocash 能够达到很好的不可链接性，被认为是目前匿名性最好的数字货币.

在效率方面，由于 Zerocash 采用的 zk-SNARK 证明大小不超过 300 字节，可以在几毫秒的时间内得到验证. 所以 Zerocash 的交易数据小于 1 KB，验证时间小于 6 ms. 但是 zk-SNARK 算法生成证明的过程非常缓慢[55]，通常需要 1 min 才能生成新的证明，是 Zerocash 的效率瓶颈.

4.6 去中心化数字货币的比较

我们从方案的技术方法、优点和缺点三个方面对去中心化数字货币的匿名性进行对比分析. 分析结果如表 4 所示.

表 4 去中心化数字货币匿名性对比

数字货币	方法	优点	缺点
比特币	区块链	具有假名性	不具有不可链接性
门罗币	区块链；环签名；一次性随机地址；去中心化混合	实现不可链接性；无混合费用；混合不需要其他用户参与	存在与混合方案相同的由交易面额引发的问题；
Zerocoin	区块链；零知识证明；货币转换	通过货币转换实现用户地址和交易的不可链接性	Zerocoin 不能有效地拆分和组合；不隐藏交易金额
Zerocash	区块链；zk-SNARKs；货币转换	交易的验证效率高；匿名性强	zk-SNARKs 产生证明的速度慢，是系统的效率瓶颈

上述数字货币普遍结合区块链结构和密码学技术解决匿名性问题.通过设计独特的交易结构并采用区块链作为账本,可以实现货币的转移、拆分和聚合.然而,由于上述方案都是在比特币系统的基础上进行加固,随着安全性的提升,系统的效率必然受到影响.

5　法定数字货币及其匿名性

5.1　法定数字货币的内涵及意义

数字货币的发展正在改变着我们的现实社会,受数字货币的启发,各种第三方支付机构也在大力推广"无现金社会",支付宝、微信支付、银联云闪付等服务已经渗透到日常生活的方方面面.这类服务的成功也体现了研究法定数字货币的紧迫性.国家必须在发行法定数字货币上占据主动权.

随着互联网、区块链等技术的飞速发展,从全球范围看,推行数字货币成为大势所趋,数字货币也成为未来数字金融的必然选择.央行发行的数字货币与私人数字货币的本质完全不同,央行数字货币是由中央银行发行和调控的,具有国家信用支撑,能够维持由国家信用支撑的现代货币体系的稳定.

目前,许多国家对数字货币采取积极的态度,委内瑞拉政府发行了全球首个法定数字货币——"石油币",引起广泛关注.石油币发行总量约1亿枚,每一枚石油币以委内瑞拉的一桶石油储备作为背书.与此同时,还有不少国家处于法定数字货币的研究阶段.英国央行委托伦敦大学负责研发的数字货币RSCoin,是首个由央行提出的数字货币体系,现已进入初步测试阶段.加拿大央行正在进行一项名为"Jasper"的实验项目,旨在探索创建一种使用数字货币技术的支付系统,最终将推出加拿大电子版加元CADCoin.俄罗斯央行也成立了研究区块链技术和分布式账簿的金融科技和研发部门.其他如美国、瑞典、新加坡、日本、荷兰、澳大利亚等国的中央银行纷纷表示将对法定数字货币的制度设计和关键技术进行探索研究.

法定数字货币由中央银行指导发行,属于现金(M0)范畴[56].在价值维度上,法定数字货币是信用货币[57],以国家信用作为价值支撑,是中央银行对公众发行的债务.法定数字货币的技术本质是加密货币①,依托密码学技术维护系统安全.在实现维度上,法定数字货币是算法货币[57],在保证安全的前提下,赋予货币更多的功能.法定数字货币在应用维度上是智能货币[57],与传统的支付方式相比具有更多元的应用场景.

与纸质货币相比,数字货币没有货币实体,发行法定数字货币能够有效降低印刷成本和存储成本,避免纸币存在的运输风险[58-59];除此之外,法定数字货币能降低用户收到假币的概率,减少用户去银行兑换纸币的环节;最重要的是,发行法定数字货币有利于构建信息化社会,数字货币能够提供货币的精准定位,监管机构可以更加清晰地了解和追踪资金的具体流向,防范洗钱和腐败,方便国家进行货币调控,为普惠金融提供便利[60].

随着私人数字货币的快速发展,其底层的支撑技术可以说是日新月异,这也为法定数字货币的研究起到了促进和借鉴作用.但是私人数字货币的缺陷也很明显,除了上文提到的匿名性方面的问题,效率或者说吞吐率也是饱受诟病的一个方面.例如比特币的工作量证明机制,使得系统生成一个区块的时间保持在十分钟左右,意味着系统每秒钟进行约7笔交易.比特币之后提出的私人数字货币尽管在效率方面有所改进,但是距离满足法定数字货币的交易规模还存在巨大差距.以2017年"双11"为例,淘宝网仅通过支付宝完成的交易笔数就达到14.8亿笔,平均每秒进行17 129笔交易,交易高峰达到25.6万笔/秒.7笔/秒的吞吐率与我国的现实交易要求相距甚远,这就导致对于法定数字货币,比特币等数字货币技术只能有选择地部分借鉴,需要新的设计思路,以达到监管、匿名、高效三者之间的平衡.

不仅研究法定数字货币具有现实意义,解决法定数字货币的一系列安全问题也能够推进密码学的发展[61].作为法定数字货币,所面对的不仅仅是普通的使用者,还要应对不法分子对货币的攻击行为.货币发行、流通、回笼的各个环节,都需要依靠密码学技术.随着量子计算机的不断发展,如何利用密码学技术,甚至探讨新的密码学技术来安全维护数字货币系统,都必将对密码学提出更高要求,为密码学带来革命.因此,法定数字货币设计与实现的研究工作具有很重要的意义.

5.2　法定数字货币的匿名性需求

法定数字货币作为一种具有法定地位的货币,应有效代替现金,实现安全存储、安全交易、匿名流

① Committee on Payments and Market Infrastructures. Digital currencies. Bank for International Settlements. 2015. https://www.bis.org/cpmi/publ/d137.pdf

通等需求[62].

匿名性是法定数字货币的设计和构建须慎重考虑的重要因素之一.作为可流通的货币,相关信息除了货币的使用者以及法定机构外,任何参与方不能获悉拥有者或者货币过去的使用者的身份信息,确保交易过程中的匿名性.在对数字货币的监管制度中,匿名性也非常重要.为了兼顾反洗钱、反恐怖融资等需求,法定数字货币的开发应与监管相协调,在实现匿名的同时,又在一定条件下允许执法机关把坏人抓出来[63].所以,我国法定数字货币的匿名性要求满足"前台自愿、后台实名"的可控匿名性.

5.3 现行技术与法定数字货币的匿名性

为了实现国家信用,法定数字货币的发行必须由国家主导,这与中心化数字货币的思想相契合.法定数字货币系统中存在中央银行控制货币的发行量,为每枚货币负责.

由于法定数字货币的匿名性需求为"前台自愿,后台实名",货币在流通的过程保持匿名,但是在货币系统中存在执法部门在监控货币的流通情况,所以,本质上,法定数字货币是可追踪的货币.

许多经典 E-Cash 方案难以实现货币的追踪:Chaum 的方案以匿名性为出发点,即使银行与商家勾结也无法追踪货币;在 Foteini 的方案中,敌手无法建立任意硬币之间的关联,也不能获知硬币的使用者身份.这样的匿名性与法定数字货币的需求相悖,显然不能应用于法定数字货币.

与之相反,Juels 的 E-Cash 系统通过引入可信机构为用户颁发"信任标识",通过银行和可信机构实现对货币和用户的追踪.直觉上,Juels 的方案满足法定数字货币的可控匿名性需求.但是,该方案存在局限性:与 Chaum 的 E-Cash 系统相同,Juels 的方案需要银行参与货币的流通,货币不满足可传递性;虽然"信任标识"的规模很小,但是每次交易都需要一个新的"信任标识",对于我国庞大的货币交易量,该方案显然是不现实的.

去中心化数字货币能够解决上述可传递问题:通过区块链结构实现节点的分布式共识,从而替代银行参与每笔交易验证.虽然这类数字货币没有中心机构,但是引入中心参与货币的发行是可行的.但是,法定数字货币不能仅仅通过在该类数字货币中引入中心机构发行货币实现.

对于比特币,系统是完全开放的,任何人都能参与交易的验证,用户虽然由地址标识,经常使用相同地址、多个地址间的频繁交易等都会破坏用户的匿名性,通过区块链将用户的身份暴露,破坏了数字货币"前台自愿"的匿名性.

混合、门罗币、Zercoin、Zerocash 等方案虽然能够保护用户的隐私,但是无法实现"后台实名"的可控要求.而且,这些方案都是在比特币区块链的基础上进行设计,都存在一个共同的问题——吞吐率低.比特币的工作量证明机制的自动调节使得系统生成一个区块的时间保持在十分钟左右,意味着系统每秒钟进行约 7 笔交易.我国的用户规模已达 14 亿,从而造成交易数量极为庞大,2017 年淘宝网双 11 的交易峰值即达到 25.6 万笔/s.7 笔/秒的吞吐率与我国的现实要求相距甚远.

因此,法定数字货币的匿名性方案设计的重点是"后台实名".现阶段,考虑货币流通"可控性"的私人数字货币方案少之又少,私人数字货币由于缺乏国家信用做支撑,用户会更在意隐私的保护,从而偏向于使用匿名性更强的数字货币,所以私人数字货币的开发者为了迎合市场及用户需求会避免货币的可追踪.法定数字货币作为国家的信用货币,国家为了维护用户的安全对货币实施监管无可厚非,所以,"后台实名"的安全性需要研发人员的创新和尝试,"后台实名"的匿名性要求也是法定数字货币的开发者的重要的挑战之一.

除此之外,法定数字货币匿名流通的实现对于货币的可传递性、吞吐率都提出更高的要求,安全、高效的流通是实现法定数字货币"前台自愿"的基石,是法定数字货币可控匿名性的重要前提之一.

6 展 望

根据目前的数字货币匿名性研究现状,从以下几个方面对未来的研究工作进行展望:

(1)高效安全的共识算法.安全、高效的流通是数字货币的重要前提,交易验证速度慢、可扩展性差等问题会极大影响系统的效率,影响货币的匿名流通.所以,在实现数字货币匿名性的同时又不影响用户的交易效率,需要更为高效安全的共识算法.共识算法的核心在于如何在分布式系统中取得一致,而且这种一致性要蕴含随机性,并且所达成的一致性结果是可以被快速验证的.从而可以看出,这种一致性是计算困难性所带来的随机性导致的,所以密码学研究团队提出好的共识算法也就不足为奇了.针对法定数字货币,需要在我国货币交易的极高体量压力下,设计支持可控监管功能的高效共识,兼顾系

统的效率和安全；

(2)密码学技术的创新. 随着量子计算机和数据分析技术的发展，传统密码学技术的安全性受到越来越大的威胁. 数字货币尤其是法定数字货币，涉及到未来国家安全. 对于数字货币全生命周期的各个阶段如发行、流通、回笼机制都有极高的安全性要求，这些安全性的保障离不开数字签名、加密算法的支持，而匿名性是各阶段中共性的要求. 所以为了实现数字货币的匿名性，有必要研究更加高效、安全的密码学技术；

(3)监管技术的研究. 对于法定数字货币来说，要在可监管的基础上实现用户的隐私保护，否则就是对非法行为的放任和纵容，可监管是法定数字货币发行的必要条件. 由于法定数字货币目前仍处于研发阶段，因此要研究预设式监管方案设计，将监管与用户的身份管理和交易流程相结合，对于非法操作，可恢复数据内容(作为证据)及相对应的各参与方身份(用作处罚)；同时也要设置应急响应机制，以实现监管部门对于数字货币交易过程中的治理和纠错等功能.

7　结　论

本文从数字货币的匿名性角度出发，对中心化及去中心化数字货币方案进行深入分析和比较，分别指出它们的优势及不足. 进一步讨论了我国法定数字货币的研究现状，分析当前主流数字货币的匿名性方案对法定数字货币“前台自愿，后台实名”的启示. 法定数字货币的研发、设计和推广是国家的重要战略部署，这项工作不是一蹴而就的，真正实现法定数字货币必将是一个漫长的过程. 开展并部署我国的法定数字货币、实现我国法定数字货币的可控匿名性还需要多方面、全方位的深入研究.

参　考　文　献

[1] Au M H, Liu J K, Fang Junbin, et al. A new payment system for enhancing location privacy of electric vehicles. IEEE Transactions on Vehicular Technology, 2014, 63(1): 3-18

[2] Reid F, Harrigan M. An analysis of anonymity in the Bitcoin system//Proceedings of the IEEE Third International Conference on Privacy, Security. Boston, USA, 2013: 197-273

[3] Herrera-JoancomartíJ. Research and challenges on Bitcoin anonymity//Proceedings of the Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance. Wroclaw, Poland, 2014: 3-16

[4] Maurer F K. A survey on approaches to anonymity in Bitcoin and other cryptocurrencies. Lecture Notes in Informatics. Bonn, Germany, 2016: 2145-2160

[5] Conti M, Kumar E S, Lal C, Ruj S. A survey on security and privacy issues of Bitcoin. IEEE Communications Surveys & Tutorials, 2017, 20(4): 3416-3452

[6] Wang Hao, Song Xiang-Fu, Ke Jun-Ming, et al. Blockchain and privacy preserving mechanisms in cryptocurrency. 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. 信息网络安全，2017，(7)：32-39)

[7] Shi Wan-Rong, Wang Wen-Tao, Meng Hui-Yan. The generation and development of digital currency. Financial Perspectives Journal, 2016, (7): 25-32(in Chinese)
(施婉蓉，王文涛，孟慧燕. 数字货币发展概况、影响及前景展望. 金融纵横，2016，(7)：25-32)

[8] Allaham M, Altarawneh H, Abdallat N. Development of electronic money and its impact on the central bank role and monetary policy. Issues in Informing Science & Information Technology, 2009, 6(1): 339-349

[9] Chaum D. Blind signatures for untraceable payments// Chaum D, Rivest R L, Sherman A T, eds. Advances in Cryptology. Boston, USA: Springer, 1983: 199-204

[10] Yuan Yong, Wang Fei-Yue. Blockchain: The state of the art and future trends. Acta Automatica Sinica, 2016, 42(4): 481-494(in Chinese)
(袁勇，王飞跃. 区块链技术发展现状与展望. 自动化学报，2016，42(4)：481-494)

[11] Xie Hui, Wang Jian. Study on block chain technology and its application. Netinfo Security, 2016, (9): 192-195(in Chinese)
(谢辉，王健. 区块链技术及其应用研究. 信息网络安全，2016，(9)：192-195)

[12] Wang Ji-Ye, Gao Ling-Chao, Dong Ai-Qiang, et al. Blockchain based data security sharing network architecture research. Journal of Computer Research and Development, 2016, 54(4): 742-749(in Chinese)
(王继业，高灵超，董爱强等. 基于区块链的数据安全共享网络体系研究. 计算机研究与发展，2016，54(4)：742-749)

[13] Christin N. Traveling the silk road: A measurement analysis of a large anonymous online. arXiv: 1207.7139v1, 2012

[14] Deng Wei. Bitcoin price bubbles: Evidence, causes and implications. Journal of Shanghai University of Finance and Economics, 2017, 19(2): 50-62(in Chinese)
(邓伟. 比特币价格泡沫：证据、原因与启示. 上海财经大学学报，2017，19(2)：50-62)

[15] Croman K, et al. On scaling decentralized blockchains// Clark J, Meiklejohn S, Ryan P, eds. Financial Cryptography and Data Security(FC2016), Christ Church, Barbados, Lecture Notes in Computer Science, vol 9604. Berlin, Germany: Springer, 2016: 106-125

[16] Tsai Wei-Tek, Zhao Zi-Hao, Zhang Chi, Yu Lian. Discussion on the Central Bank Issued digital currency RSCoin of England. Financial Computerizing, 2016, (10): 78-81(in Chinese)

(蔡维德，赵梓皓，张弛，郁莲. 英国央行数字货币 RSCoin 探讨. 金融电子化，2016，(10)：78-81)

[17] Danezis G，Meiklejohn S. Centrally banked cryptocurrencies //Proceedings of the 23rd Annual Network and Distributed System Security Symposium (NDSS 2016). San Diego，USA，2016：21-24

[18] Yao Qian. The Central Bank's digital currency：An introduction to the RSCoin system. Financial，2017，(13)：20-22 (in Chinese)
(姚前. 中央银行加密货币——RSCoin 系统之分析. 财经，2017，(13)：20-22)

[19] Yao Qian. Prototype of China's digital fiat currency. Chinese Financial，2016，(17)：13-15(in Chinese)
(姚前. 中国法定数字货币原型构想. 中国金融，2016，(17)：13-15)

[20] Okamoto T，Ohta K. Universal Electronic Cash. International Cryptology Conference. Berlin，Germany：Springer，1991：324-337

[21] Feng Deng-Guo. An overview of digital signature techniques. Information Security and Communications Privacy，1996，(3)：15-22(in Chinese)
(冯登国. 数字签名技术概述. 信息安全与通信保密，1996，(3)：15-22)

[22] Solms S V，Naccache D. On blind signatures and perfect crimes. Computers & Security，1992，11(6)：581-583

[23] Zhang Ni. The Research of Electronic Cash Payments Systems and Its Key Techniques[M. S. dissertation]. Information Engineering University，Zhengzhou，2005(in Chinese)
(张妮. 电子现金支付系统及其关键技术的研究[硕士学位论文]. 中国人民解放军信息工程大学，郑州，2005)

[24] Juels A. Trustee tokens：Simple and practical anonymous digital coin tracing//Franklin M，ed. Financial Cryptography. Lecture Notes in Computer Science 1648. Berlin，Germany：Springer，1999：29-45

[25] Baldimtsi F，Chase M，Fuchsbauer G，et al. Anonymous transferable E-Cash//Proceedings of the IACR International Workshop on Public Key Cryptography. Berlin，Germany：Springer，2015：101-124

[26] Chase M，Kohlweiss M，Lysyanskaya A，Meiklejohn S. Malleable signatures：New definitions and delegatable anonymous credentials//Proceedings of the IEEE Computer Security Foundations Symposium. Vienna，Austria，2014：199-213

[27] Canard S，Gouget A，Traor'e J. Improvement of efficiency in (unconditional) anonymous transferable E-Cash//Tsudik G，ed. Financial Cryptography 2008. Cozumel，Mexico，2008：202-214

[28] Narayanan A，Bonneau J，Felten E W，et al. Bitcoin and Cryptocurrency Technologies：A Comprehensive Introduction. New Jersey：Princeton University Press，2016

[29] Liu Li. The development，influence and supervision of digital currency. Money China，2016，(12)：17(in Chinese)
(刘莉. 论数字货币发展状况、影响及监管. 财经界，2016，(12)：17)

[30] Dwork C，Naor M. Pricing via processing or combatting junk mail//Proceedings of the International Cryptology Conference on Advances in Cryptology. Santa Barbara，1992：139-147

[31] Back A. Hashcash — A denial of service counter-measure//Proceedings of the USENIX Technical Conference. Monterey，USA，2002：1-10

[32] Reid F，Harrigan M. An analysis of anonymity in the Bitcoin system//Proceedings of the IEEE Third International Conference on Privacy，Security. Boston，USA，2011：1318-1326

[33] Androulaki E，Karame G O，Roeschlin M，et al. Evaluating user privacy in Bitcoin//Proceedings of the International Conference on Financial Cryptography and Data Security FC2013. Okinawa，Japan，2013：34-51

[34] Ron D，Shamir A. Quantitative analysis of the full Bitcoin transaction graph//Sadeghi A R，ed. Financial Cryptography and Data Security. Berlin，Germany：Springer，2013，7859：6-24

[35] Meiklejohn S，Pomarole M，Jordan G，et al. A fistful of Bitcoins：Characterizing payments among men with no names//Proceedings of the 2013，Conference on Internet Measurement Conference. London，UK，2013：127-140

[36] Spagnuolo M. BitIodine：Extracting intelligence from the Bitcoin network//Proceedings of the Financial Cryptography and Data Security. Barbados，2014：452-463

[37] Chaum D. Untraceable electronic mail，return addresses，and digital pseudonyms. Communications of the ACM，1981，24(2)：84-88

[38] Barber S，Boyen X，Shi E，Uzun E. Bitter to better — How to make Bitcoin a better currency//Keromytis A D，ed. Financial Cryptography and Data Security (FC2012). Bonaire，the Netherlands，2012：399-414

[39] Bissias G，Ozisik A P，Levine B N，Liberatore M. Sybil-resistant mixing for Bitcoin//Proceedings of the 13th ACM Workshop on Privacy in the Electronic Society (WPES 2014). New York，USA，2014：149-158

[40] Bonneau J，Narayanan A，Miller A，et al. Mixcoin：Anonymity for Bitcoin with accountable mixes//Christin N，Safavi-Naini R，eds. Financial Cryptography. Barbados，2014：481-499

[41] Ruffing T，Moreno-Sanchez P，Kate A. CoinShuffle：Practical decentralized coin mixing for Bitcoin//Proceedings of the Computer Security (ESORICS 2014). Wroclaw，Poland，2014：345-364

[42] Ruffing T，Moreno-Sanchez P，Kate A. P2P mixing and unlinkable Bitcoin transactions. Network and Distributed System Security Symposium. San Diego，USA，2017：43-58

[43] Rivest R L，Shamir A，Tauman Y. How to leak a secret//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Gold Coast，Australia，2001：552-565

[44] Bellare M, Micciancio D, Warinschi B. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions//Proceedings of the Advances in Cryptology (EUROCRYPT 2003). Warsaw, Poland, 2003: 614-629

[45] Camenisch J, Stadler M. Efficient group signature schemes for large groups//Proceedings of the Advanced in Cryptology. Santa Barbara, USA, 1997: 410-424

[46] Chaum D, Heyst E V. Group signatures//Proceedings of the Advances in Cryptology (EUROCRYPT'91). Brighton, UK, 1991: 257-265

[47] Liu Biao. Research and Application of Ring Signature Scheme [M. S. dissertation]. Xidian University, Xi'an, 2012 (in Chinese)
(刘彪. 环签名算法研究与应用[硕士学位论文]. 西安电子科技大学, 西安, 2012)

[48] Diffie W, Hellman M. New directions in cryptography. IEEE Transactions on Information Theory, 1976, 22(6): 644-654

[49] Mackenzie A, Noether S. Monero Core team: Improving obfuscation in the CryptoNote protocol. Research Bulletin MRL-0004, Monero Research Lab, Germany, January 2015

[50] Kumar A, Fischer C, Tople S, et al. A traceability analysis of Monero's Blockchain//Proceedings of the European Symposium on Research in Computer Security. Barcelona, Spain, 2017: 153-173

[51] Miers I, Garman C, Green M, Rubin A. Zerocoin: Anonymous distributed E-Cash from Bitcoin//Proceedings of the 2013 IEEE Symposium on Security and Privacy. San Francisco, USA, 2013: 397-411

[52] Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems//Proceedings of the Advances in Cryptology (CRYPTO'86), Santa Barbara, USA, 1986: 186-194

[53] Schnorr C P. Efficient signature generation by smart cards. Journal of Cryptology, 1991, 4(3): 161-174

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

[55] Zhu Lie-Huang, Gao Feng, Shen Meng, et al. Survey on privacy preserving techniques for blockchain technology. Journal of Computer Research and Development, 2016, 54(10): 2170-2186(in Chinese)
(祝烈煌, 高峰, 沈蒙等. 区块链隐私保护研究综述. 计算机研究与发展, 2016, 54(10): 2170-2186)

[56] Fan Yi-Fei. Theoretical basis and structural selection of China's digital fiat currency. China Finance, 2016, 17: 10-12(in Chinese)
(范一飞. 法定中国数字货币的理论依据和架构选择. 中国金融, 2016, 17: 10-12)

[57] Yao Qian. Understanding central bank digital currency: A systemic framework. Scientia Sinica Informationis, 2017, 47: 1592-1600(in Chinese)
(姚前. 理解央行数字货币: 一个系统性框架. 中国科学: 信息科学, 2017, 47: 1592-1600)

[58] Qiu Xun. Digital currency issue of China: Method, problems and policy. Southeast Financial, 2017, (3): 14-20(in Chinese)
(邱勋. 中国央行发行数字货币: 路径、问题及其应对策略. 西南金融, 2017, (3): 14-20)

[59] Zhou Yong-Lin. Discussion on Central Bank digital currency and its realization. Financial Computerizing, 2016, (9): 35-37 (in Chinese)
(周永林. 央行数字货币及其实现模式探讨. 金融电子化, 2016, (9): 35-37)

[60] Li Gen. Discussion on the current situation and development of digital currency. Business, 2016, (10): 173-173(in Chinese)
(李根. 论数字货币的现状影响因素及发展趋势. 商业, 2016, (10): 173-173)

[61] Qin-Bo, Chenli Chang-Hao, Wu Qian-Hong, et al. Bitcoin and digital fiat currency. Journal of Cryptologic Research, 2017, 4(2): 176-186(in Chinese)
(秦波, 陈李昌豪, 伍前红等. 比特币与法定数字货币. 密码学报, 2017, 4(2): 176-186)

[62] Wang Yong-Hong. Implementation Framework of Digital Currency Technology. Chinese Financial, 2016, (12): 15-17 (in Chinese)
(王永红. 数字货币技术实现框架. 中国金融, 2016, (12): 15-17)

[63] Yao Qian. Consideration of China's digital fiat currency. Chinese Financial, 2016, (12): 26-27(in Chinese)
(姚前. 中国版数字货币设计考量. 中国金融, 2016, (12): 26-27)

FU Shuo, M. S. candidate. Her research interests include secure multi-party computation, digital currency, secure protocol.

XU Hai-Xia, Ph. D., associate professor. Her research interests include secure multi-party computation, digital currency.

LI Pei-Li, Ph. D., assistant professor. Her research interests include digital currency, secure protocol.

MA Tian-Jun, Ph. D. candidate. His research interests include smart contract, digital currency.

Background

The research of this paper belongs to the field of digital currency. Digital currency is distinct from physical currency. It exhibits properties similar to physical currencies, but allows for instantaneous transactions and borderless transfer-of-ownership. Like traditional money, these currencies may be used to buy physical goods and services, but may also be restricted to certain communities such as for use inside an on-line game or social network. Inspired by the private digital currency, many countries are working on digital fiat currency.

In this paper, we mainly discuss the anonymous of digital currency, which is the basis of the study of digital fiat currency. At present, there is no national solution to the anonymous of digital fiat currency. However, the international solution to the anonymity of other digital currencies including: mixnet, blind signatures and zero knowledge proof.

In mixnet, the value of transactions must be uniform. Schemes applying cryptographic tools will achieve higher anonymity, anyone can not link others' transactions or addresses. As regulatory issues should be considered in the design of digital fiat currencies, these schemes are not applicable to the anonymity of the digital fiat currency.

On the basis of the research of anonymity solution, this paper proposes an anonymous framework for digital fiat currency. This framework can provide ideas for country while designing the digital fiat currency. To help the monetary sovereignty to control digital fiat currency. Helping our country to take the initiative in the digital fiat currency field.

This work is supported by the National Key R&D Program of China (2017YFB0802500).