DOI:10.19729/j.cnki.1009-6868.2018.06.003
网络出版地址:http://kns.cnki.net/kcms/detail/34.1228.TN.20181124.1856.002.html

比特币生成原理及其特点

The Generation Principles and Characteristics of Bitcoin

林成骏/LIN Chengjun
伍玮/WU Wei
(福建师范大学,福建 福州 350007)
(Fujian Normal University, Fuzhou 350007, China)

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2018) 06-0013-006

摘要: 从密码技术出发,着重分析比特币的生成和运行原理。其中,通过哈希函数的压缩性和单向性,分别描述了比特币的核心技术区块链以及工作量证明(PoW)的难度;利用数字签名的完整性和认证性分析比特币交易的验证过程。基于对比特币优缺点的分析,认为目前比特币的隐私保护和监管问题仍然突出。

关键词: 比特币;区块链;哈希函数;数字签名

Abstract: Based on the cryptographic techniques, the generation and operation principles of Bitcoin are emphatically analyzed in this paper. The blockchain (the core technology of Bitcoin) and the difficulty of power-of-work (PoW) are described respectively by using the compressibility and one-wayness of hash functions; the authentication process of Bitcoin transactions is analyzed by using the integrity and authenticity of digital signature. Finally, the advantages and disadvantages of Bitcoin are summarized. It is considered that the privacy protection and regulation are still the main problems of Bitcoin.

Key words: Bitcoin; blockchain; hash functions; digital signature

1 比特币生成背景及其意义

数字货币是一种以电子形式存在的货币,不再像虚拟货币一样局限于网络游戏,而是能够像法币一样购买真实的物品。密码货币是数字货币的重要组成之一,利用严谨的密码学原理进行货币的产生、记账和交易。自从第一个密码货币即比特币诞生后,诸如以太坊、门罗币和零币等一系列密码货币相继面世,密码货币市场呈现井喷式发展;但是密码货币在具有价值的同时,也伴随着一定的风险。分析密码货币的生成和运行原理能够让人们对数字货币有更深的理解,从而做到理性投资。

比特币是最具有代表性的密码货币之一,后续的密码货币在一定的程度上是延续比特币的技术原理。当然后续的密码货币在共识机制、交易匿名性以及数据隐私保护方面都取得了较大突破。例如:以太坊[1]利用权益证明(PoS)机制,大幅度缩减挖矿开销的计算资源;门罗币利用可链接环签名技术[2],为发送者提供匿名保护,同时可以检测双重支付;零币[3]采用非交互零知识证明机制[4]进一步提高了匿名性,实现了发送者和接收者匿名以及数据隐私,但是计算和存储开销增大。本节主要介绍比特币的生成背景和研究意义。

1.1 比特币的生成背景

比特币的诞生充满了神奇色彩,其中包含了密码学、经济学的许多前沿理论。它基于前人提出的理论基础,并充分结合了当时特殊的社会环境背景。

(1)密码学、经济学的理论基础是比特币诞生的内在条件。1976年,HAYEK [5] 在《Denationalization of Money》一书中提出只有货币非国家化才能控制货币发行量,避免因不断发行而导致货币贬值的命运。1981年,LAMPORT L [6]提出了哈希链的概念,即每轮哈希函数的输入均为上一轮输出的哈希值,从而为数据提供完整性服务,哈希链可以视为比特币的核心技术区块链雏形。1982年,CHAUM D [7]提出盲签名的思想,目的是为了构建不可追踪的密码学网络支付系统,该想法被认为是比特币设计思想的雏形。1991年,CHAUM D和HEYST van E [8]提出群签名。一位群管理员为每一位群成员发放私钥,每位群成员均可代表整个群对消息进行签名,除了群管理员外,其他实体无法得知签名人的身份,只知道签名人来自于该群。依据群签名技术,CHAUM D和HEYST van E设计出第一个密码学匿名现金系统Ecash,但是Ecash依赖于一个中心且货币不具备可分性。1987年,MERKLE R C [9]提出了一种哈希函数二叉树(即

收稿日期:2018-10-23
网络出版日期:2018-11-24
基金项目:中国自然科学基金(61822202,61872089)

Merkle 树），可以单独对部分数据进行验证，而无需检验所有数据，同时可以快速查询数据。1992 年，DWORK C 和 NAOR M [10]提出工作量证明（PoW）机制，用于防止垃圾邮件，邮件发送者通过一系列复杂的计算，向接收者证明邮件是值得阅读的。1998 年，SZABO N [11]将 PoW 思想应用于分布式数字货币，用户致力于解决密码学难题，正确答案需在网络中发布，且作为下一个困难问题的输入之一，从而得到一个不断增长的链条。该机制被称为“Bit Gold”，可以视为比特币体系的先驱。2001 年，NIST[12]发布了 SHA-256 算法，可以将任意长度的消息映射到 256 bit 长度的消息摘要。

（2）比特币诞生[13]的特殊社会背景。2008 年末，受美国金融危机影响，许多国家的人民陷入恐慌，一些政府为应对金融危机甚至做出过激反应，政府和银行的信誉也因此受到重创。与此同时，NAKAMOTO S [14]在 metzdowd.com 中发表了一篇名为《Bitcoin: A Peer - to - Peer Electronic Cash System》的论文，并且实际运行了其所提出的比特币理论系统，即比特币“挖掘”过程。2009 年 1 月 3 日，比特币的第一个区块问世，其中含有系统奖励的 50 枚比特币。

当代货币体系是各国法币的集合，而 2008 年金融危机暴露出法币的缺陷，让人们对当代各国货币体系产生质疑。法币具有 2 条先天缺陷：一是由政府垄断，发行的主体是国家；二是发行数量也由国家控制，自从美元与黄金脱轨，阻碍法币数量增长的机制不复存在，法币贬值的趋势很难逆转。比特币的诞生与金融危机是否有着某种关联，又是否能够为克服法币的缺陷提供新思路，这些我们不得而知。但比特币理论为我们提供了一种新的技术思想，即如何在无第三方机构的情形下构建可信机制，该思想有助于推动金融服务、公共服务、物联网（IoT）等领域的技术革新。

1.2 比特币的研究意义

从比特币出现至今，密码货币的热潮仍然存在，且对世界各国的经济活动和社会生活影响日益扩大。但是很多人只了解到比特币是一个迅速增值的密码货币，却不了解它是如何产生、如何交易；作为一个新生物，它的价值何在，存在价值的同时又是伴随着怎样的风险呢？基于此，一方面，我们要了解它的运行原理，分析它的价值和风险；另一方面，区块链作为比特币的核心技术之一，已经从单一的密码货币领域，发展到社会的各行各业，例如：在医疗健康领域，可以为病人提供隐私保护服务；在 IoT 领域，可以为用户提供产品溯源、防伪以及认证服务；在教育领域，可以为学生提供学历证明、成绩证明以及档案管理服务。然而，除了密码货币领域的应用外，区块链技术在其他领域的应用尚处于摸索阶段，相应技术理论尚未成熟。因此，了解比特币的技术原理，有助于我们今后更好地探索其在其他领域的应用。

2 比特币的密码学基础

比特币作为重要的密码货币之一，它的产生、交易和记账都依赖于严谨的密码学原理，首先介绍几个密码学的基础概念。

2.1 哈希函数

区块链是比特币的核心技术，而区块链事实上是一条哈希链，通过哈希函数串联一块块历史数据。本节主要介绍哈希函数及其相关概念。

2.1.1 哈希函数的定义

哈希又译为“散列”，哈希函数以任意长度的消息为输入，输出固定长度的消息摘要。例如：哈希函数 SHA-256 输出的哈希值为 256 bit。通常情形下，哈希函数是一类压缩函数，它的值域远小于定义域，即一个消息摘要存在多个原像与之对应。比特币系统中所应用的哈希函数还需要满足以下 3 个安全要求：

（1）对任意消息 m，很容易计算出它的哈希值 $y=h(m)$；

（2）由 y 得出 m 在计算上不可行（单向性或原像稳固性）；

（3）已知消息 m，很难找出另一个消息 n 使得 $h(n)=h(m)$（抗碰撞性）。

2.1.2 哈希校验

由于哈希函数具有单向性和抗碰撞性，因此可用于检验消息的完整性，即检验消息在传送过程中是否被篡改。该过程被称为哈希校验。

效验步骤：假设 B 要发送一条消息 m 给 A，首先计算 m 的消息摘要 $y=h(m)$，并附在消息后面一起发出。A 收到消息 m' 后，检验 $h(m')\stackrel{?}{=}y$。如果相等，由于哈希函数具有强抗碰撞性，A 可在很大程度上相信消息在传送过程中没有被篡改。

2.1.3 哈希现金

哈希现金（Hashcash）最早是由 ADAM B 提出的[15]，其本质是一种 PoW 系统[10]。用户 A 要求发给他的邮件的哈希值必须包含某段特定字符串，例如：用户 A 要求邮件的哈希值的前 8 位必须是 0，否则拒绝接收该邮件。那么发给 A 的邮件正文必须添加某些随机字符使得哈希值满足该要求，这个工作是没有捷径的，计算机必须不断循环进行如下步骤：随机选取某些字符，并将其串联到邮件末尾，计算串联后的邮件的哈希值，直到哈希值的前 8 位是 0 为止。当然，计算开销取决于计算机的算力，当要求的难度提升巨大时，想要通过随意转发垃圾邮件的方式完成 A 的要求的可能性几乎为零，从而达到了防止垃圾邮件的目的。

2.2 数字签名

2.1.2 节介绍了哈希函数可以用

于检验消息是否被篡改，但是消息的接收方却无法确认消息的发送方是谁。数字签名能很好地克服该缺点，用户首先产生2把不同密钥，其中一把为私钥，需要秘密保管；另一把为公钥，需要公开发布，且他人很难从用户的公钥推算出相应的私钥。一个数字签名方案[16-17]包含3个多项式时间算法：

（1）密钥生成。输入系统安全参数（可以理解为用户所需密钥的长度），输出Alice的公钥 pk 和私钥 sk。其中，公钥是公开的，任意实体都能获得Alice的公钥，而私钥则由Alice保密。

（2）签名。Alice想以认证的形式将信息 m 发送给Bob，即Alice希望Bob能够检验消息在传送过程中是否被篡改（消息完整性）以及消息的来源（消息认证性）。算法输入Alice的私钥 sk 和消息 m，输出签名 σ。

（3）验证。Bob用Alice的公钥 pk 验证 σ 是否为消息 m 的签名。如果验证通过，算法输出1；否则输出0。

除了消息认证性和完整性外，签名还能提供不可否认性服务，即当签名人抵赖所签署过的消息时，签名 σ 可以提交给第三方仲裁机构来判定。除了上述3个多项式时间算法外，数字签名方案还需要满足一定的正确性要求：签名人所签署过的消息签名对必须以压倒性概率通过验证算法。

哈希-签名（Hash-Sign）思想是一类构造安全数字签名的重要措施，即先计算消息的哈希值，然后对哈希值进行签名。该思想有3个优点：可以抵抗无消息攻击；哈希函数可以将任意长度的消息映射成固定长度的消息摘要，于是签名算法的输入长度变成一个固定值；在证明签名方案的安全性时，可以将哈希函数模拟成随机预言器。

比特币系统所使用的签名算法为椭圆曲线数字签名算法（ECDSA）。

（1）定义1[16,18]。设定义在域 F_p（$p>3$ 且 p 是素数）上的椭圆曲线方程为：

$$y^2=x^3+ax+b \quad a,b\in F_p, \tag{1}$$

且

$$(4a^3+27b^2)\bmod p\neq 0。 \tag{2}$$

令

$$E_P(a,b)=\{(x,y)|x,y\in F_p\}\cup\{O\}, \tag{3}$$

其中，O 为无穷远点。我们称 $E_p(a,b)$ 为素数域 F_p 上的椭圆曲线。椭圆曲线 $E_P(a,b)$ 上的点数用 $\#E_P(a,b)$ 表示，称为椭圆曲线的阶。

（2）构建素数域上椭圆曲线的运算法则[16,18]。$E_P(a,b)$ 上的点按如下加法法则构成一个Able群：

1）$O+O=O$，O 可以视为零元；

2）$\forall P=(x,y)\in E_P(a,b)\backslash\{O\}$，$P+O=O+P=P$；

3）$\forall P=(x,y)\in E_P(a,b)\backslash\{O\}$，$P$ 的逆元为 $-P=(x,-y)$，满足 $P+(-P)=O$；

4）2个非零元的不同点相加，设0，$P_2=(x_2,y_2)\in E_P(a,b)\backslash\{O\}$，且 $x_1\neq x_2$，若 $P_3=(x_3,y_3)=P_1+P_2$，则 $(x_3,y_3)=(\lambda^2-x_1-x_2,\lambda(x_1-x_3)-y_1)$，其中 $\lambda=\frac{y_2-y_1}{x_2-x_1}$；

5）倍点原则，设 $P_1=(x_1,y_1)\in E_P(a,b)\backslash\{O\}$，且 $y_1\neq 0$，若 $P_3=(x_3,y_3)=P_1+P_1$，则 $(x_3,y_3)=(\lambda^2-2x_1,\lambda(x_1-x_3)-y_1)$，其中 $\lambda=\frac{3x_1^2+a}{2y_1}$。

（3）ECDSA[18]。首先考虑等式：$K=kG$，若已知 k 和 G，则由加法法则易得 K；但若只给定 G 和 K，求 k（K 关于基底 G 的对数）在一些椭圆曲线上是困难的，该问题即为椭圆曲线上的离散对数问题。为了使该问题足够困难，椭圆曲线需要满足以下条件：$\#E_P(a,b)$ 有一个大的素因子 n，满足 $n\geq 2^{160}$ 且 $n\geq 4\sqrt{q}$。接下来我们介绍具体的签名算法。

1）密钥生成。算法输入安全参数 1^{160}，随机选取整数 $k\in[1,n-1]$，基点 $G\in E_p(a,b)$，计算 $K=kG$。算法输出公钥 K，私钥 k。

2）签名。算法输入签名人私钥 k 和消息 m，然后进行如下步骤：

（a）随机选取整数 $d\in[1,n-1]$；

（b）计算 $dG=(x_1,y_1)$ 和 $r=x_1 \bmod n$。如果 $r=0$，返回步骤a；

（c）计算 $s=d^{-1}(H(m)+kr)\bmod n$。如果 $s=0$，返回步骤a；

（d）输出 m 的签名 $\sigma=(r,s)$。

3）验证。算法输入签名人公钥 K，签名 σ 和消息 m，然后进行如下步骤：

（e）验证 $r,s\in[1,n-1]$；

（f）计算 $u_1=H(m)s^{-1} \bmod n$ 和 $u_2=rs^{-1} \bmod n$；

（g）计算 $X=u_1G+u_2K=(x_1,y_1)$，如果 $X=O$，算法输出0；否则，继续计算 $v=x_1 \bmod n$；

（h）若 $v=r$，算法输出1；否则，算法输出0。

3 比特币原理

本节主要介绍比特币的生成以及交易原理[14,19]。

（1）比特币地址。现实中，人们想进行存钱、转账等一系列操作，首先得前往银行开个账户，然后领取银行分配的一串数字帐号（银行卡号），帐号的密码由用户设定。而在比特币体系中，账户不需要由中心机构来开设，用户首次使用比特币时只需下载客户端。用户的公私钥对由签名方案的密钥生成算法产生，公钥即为比特币地址，私钥由用户储藏在钱包文件中。事实上，比特币系统具有去中心化和弱匿名性的特点，去中心化是由于比特币的生成和交易过程没有中心机构参与；弱匿名性是指比特币系统采用的是假名技术，用户的公钥无法与其现实生活中的身份相联系。但是该技术无法为用户提供地址不可关联性服务和交易金额的机密性服务。地址不可关联性指的是：任意给定2个公钥地址，敌手无法在多项式时间内判断2个地址是否属于同一个用户。这些更强的匿名性可以由零知识证明或环签名技术实

现，本文不进行展开。

（2）点对点（P2P）网络。NAKAMOTO S[14]曾说过："比特币是一种P2P的现金支付系统。"这种P2P结构的特点是：中心平台不是必要条件，每一台电脑都是一个独立体，独立体间通过互联网相互连接，最终形成密密麻麻的网络节点图。因此P2P网络一旦启动就无法停止下来，除非所有实体都退出该网络。

3.1 比特币的交易流程

3.1.1 比特币交易链条

比特币不是基于账户的密码货币，而是基于交易的密码货币。在基于账户的货币中，我们可以通过账户直接查询余额；但在比特币系统中，我们需要通过未花费交易输出（UTXO）来统计该地址余额。

每一笔交易都是由交易输入和交易输出构成。交易输入里面的字段主要是脚本签名（包含本次交易的签名和付款人公钥）、UTXO的索引，该字段表明了付款人信息和付款人的金额来源。其中，数字签名使用ECDSA，付款人先将本次交易关键数据（例如：UTXO索引、交易金额和收款人公钥）作为哈希函数的输入，计算相应的哈希值，再使用私钥对哈希值签名；交易输出里面的字段主要是脚本公钥（包含若干个脚本指令和收款人公钥地址的哈希值）、地址和金额。该字段主要表明收款人的地址和收款金额。

3.1.2 比特币交易步骤

（1）验证本次交易是否是可支付的。比特币的所有交易记录提供了比特币UTXO查询，只有当本次交易的UTXO对应的金额大于或等于收款金额时，该笔交易才是可支付的。

（2）用私钥签署这笔交易，并将签名放置在交易的脚本签名中。

（3）将该交易单广播出去，寻求其他实体的认可。所有合法的比特币交易最终都会被封装在历史区块之中。

但是上述转账过程存在一个问题：收款人很难确认比特币所有者是否对该比特币进行双重支付。

3.1.3 双重支付

（1）无双重支付的情形。假设A有1枚比特币，要将其转给B。A首先构造一笔交易Tx1：使用私钥签署该笔交易，并将交易单Tx1广播出去。其他实体收到信息后，通过UTXO索引计算A是否有能力支付1枚比特币，如果有能力支付，则认为此次交易是合法。最后，A的钱包地址减少1枚比特币，B的钱包地址增加1枚比特币。

（2）有双重支付的情形。如果A利用同一个UTXO构造2笔交易（Tx1：从A地址转1枚比特币给B地址；Tx2：从A地址转1枚比特币给C地址），并用私钥分别签署这2笔交易。由于消息传送具有随机性与先后性，有些实体先收到第1条交易，而有些实体会先收到第2条交易，那么比特币系统会以哪条交易为准？

3.2 挖矿

挖矿是比特币系统的工作机制，能很好地解决双重支付的问题，本节主要介绍挖矿的流程。

3.2.1 区块及其作用

区块的主要成分包括：前一个区块的哈希值、难度值、当前区块所有交易的Merkle根节点的哈希值、时间戳（区块的创建时间）和随机数。值得注意的是：上述成分中出现2个哈希值，它们使用相同的哈希函数SHA256(SHA256( ))（使用2次SHA256算法），区别在于函数输入不同。第1个哈希值是前一个区块创建者挑战PoW成功后的结果，区块中的随机数为创建区块的实体随机选取，目的是为了找到满足PoW要求的随机数，具体将在3.2.2节介绍；第2个是Merkle根节点的哈希值，实体将收集到的交易放置在树状结构的最底层，每笔交易都视为一个叶子节点，开始构建Merkle树：首先计算每笔交易的哈希值，然后从下往上依次将每2个哈希值作为哈希函数的输入（每个树节点依然使用SHA256(SHA256( ))算法），计算出上一层哈希值，直到计算出最顶层的哈希值，即Merkle根节点的哈希值。Merkle树有2个优点：可以单独取出一个分支，对数据进行验证；可以依据树状结构快速查询到一笔交易。

区块分为区块头和区块体2部分：区块头包含前一个区块的哈希值、难度值、Merkle根节点的哈希值、时间戳和随机数；区块体包含当前区块的所有交易。

区块链就是按创建的时间顺序进行排列的区块链条，它完美地实现了一个牢不可摧且永不停息的比特币交易数据库。

比特币系统大约每10 min产生一个区块，该区块包含这10 min内未确认的交易以及前一个区块（银行的系统如果崩溃将导致其所有数据都失去了，但是比特币系统则不同，每个节点在工作时都得下载一个最新区块，该区块就包含历史全部记录，故在比特币世界中只要还有一个节点在运作，那么它的历史数据就不会丢失，因此可以视比特币系统亦或者区块链为分布式记账），因此从第一个区块问世至今就形成了一条完整的区块链。区块有2点作用：收集交易记录；做存在证明和防篡改，因为区块的哈希值施加了时间戳，一方面能证明区块的存在时间，另一方面由哈希函数的抗碰撞性知区块被篡改的概率可忽略。

3.2.2 PoW

在介绍哈希函数时已经阐述了Hashcash，Hashcash设定特定的哈希值开头作为实体的挑战目标，而实体则不断尝试不同的随机数，以期得到

满足要求的哈希值。在比特币区块的建设过程中引入一个类似Hashcash的规则，即PoW机制，它的本质是为了防止低算力的实体随意或恶意发布区块。此时，哈希函数的输入为区块头，输出是一个256 bit的哈希值。比特币系统会把每个区块完成的时间控制在10 min左右。如果难度低于10 min，系统就自动调高难度值，增加哈希值开头0的位数；如果难度高于10 min，就适当减少哈希值开头0的位数，以调低难度值。这是比特币系统默认的一个规则：维持10 min产生一个区块。这个PoW的过程被称为挖矿。

挖矿的本质是争夺记账权，实体（矿工）收集、检验和确认过去一段时间内发生的交易。当找到一个符合PoW机制的哈希值，矿工就能够将自己封装的区块广播出去，让其他矿工验证该区块。如果有矿工接受该区块并以它为基础继续挖下一个区块，那么该区块中的所有交易单就获得一次确认。每延长一个区块就等价于该区块中的交易多了一次确认。若得到6次确认，那么该区块就获得全网的认可，封装到历史区块中。矿工挖矿的具体流程如下：

（1）下载一个最新区块（其中包含所有历史交易记录），计算出它的哈希值；

（2）收集尚未被确认的交易单并使用签名技术校验交易单的有效性，把有效的交易单纳入新的区块；

（3）选取一个随机数（这是为了满足PoW机制的要求）；

（4）将第（1）—（3）步产生的数值作为SHA-256(SHA-256( ))算法的输入，得到一个256 bit的二进制数，并检查这个数是否符合PoW机制的要求；

（5）如果满足PoW要求，则向全网广播新区快。若其他矿工接受本区块，就会在该区块末尾继续进行挖矿工作以延长区块链。若不符合PoW要求，则重复第（2）—（5）步，直到符合要求或者接收到其他矿工发布的新区块。

在比特币世界中每10 min会产生新增比特币奖励给成功建立新区块的矿工，每个区块的奖励在最初的4年中是50个比特币（4年大概产生21万个区块），之后的4年每个区块是25个比特币，依次类推下去，最终系统只能产生2 100万个比特币[20]。同时，新区块的建立者会获得每笔交易所产生的交易费用。

基于上述挖矿过程可知：双花意味着需要广播同一笔比特币的2次不同交易单。矿工在收集时只会将其中一个封装在自己的区块中，从而能够有效地防止双花。

3.2.3 区块链的延长和交易的最终确认

每笔比特币交易只有获得6次确认，才能认定为有效。在挖矿过程中，同一段时间会生成很多有效区块，不同有效区块中的元素除前一个区块的ID是相同外，其他元素几乎都不同，例如：交易单集合就是不同的。若1个节点收到2个有效区块，则将这2个区块都放在主区块链的后面，并形成一个Y型分叉，后续收到的区块则基于这2个区块产生，使区块链延伸下去。矿工始终选择最长的分支成为主区块链的一部分，并继续工作以延长区块链。一般包含这个交易的区块出现后，还需等待5～6个后续的区块生成，才能确定该区块是否进入主区块链，从而最终确认区块中的交易是否有效。可见比特币的交易所需时间比较长。

4 比特币的主要特点

比特币的本质和大多数虚拟货币一样，由一堆代码组成，但同时它也具有许多传统虚拟货币不具备的优点[21-23]。

（1）去中心化思想，发行数量固定。法币的发行受政府与中央银行约束；但比特币不同，它采用区块链技术和非对称密码技术，发行不受央行约束，而且比特币的发行具有上限，从而避免一些因为人为决策因素而导致的货币贬值。

（2）交易成本低廉。比特币的交易不需要中介机构，交易成本低廉（但对小额交易而言，成本较高）。同时，比特币中的用户采用的是假名，国家很难收取比特币的交易税。

（3）货币不可伪造，无法双重支付，交易不可逆转。系统中的每个区块都有记录可查，想要伪造比特币几乎不可能。区块链会不停地延长，一旦交易被全网接受并装入历史区块后是不可撤销或逆转的。同时，比特币的PoW机制能很好地防止双重支付现象。

（4）全球化转账支付。比特币的交易效率相对与中国境内的同行或跨行转账效率慢，这是因为中国的银行都有一个可信任的第三方（央行），因此交易双方的身份认证很便捷；但比特币具有一个显著的优势：可打破国界进行全球化转账支付，且该效率比目前法币的跨国转账效率高。法币进行跨国转账时，两国的银行中间缺少一个可信赖的第三方，造成双方的身份认证十分漫长。

（5）开源。比特币的原理和技术都是公开的，还有其软件代码也是基于开源协议发布的，莱特币就是基于比特币协议产生。

与此同时，比特币的缺点也是显而易见。

（1）在比特币世界中，私钥代表一切，一旦私钥泄漏或遗忘，意味着你的比特币财富也将失去，且他人无法帮你找回丢失的比特币。

（2）比特币无央行发行，无政府部门为其交易和安全保驾护航，这也是人们对比特币信心不足的主要原因之一。

（3）比特币的系统虽然很健壮，但它的交易平台（通常是一个网站）是脆弱的，易遭受黑客攻击，例如：Mt.Gox曾是世界最大的比特币交易

平台，但被恶意攻击，于2014年2月28日宣布破产，比特币的行情大跌。

5 结束语

文中，我们主要介绍比特币系统中涉及的相关密码技术，包含签名、哈希函数以及区块链技术。尤其是区块链技术，以链状结构存储数据，以密码技术为数据传输提供机密性和认证性服务，从而形成一条分布式存储、无法篡改、永无止息的数据库。但比特币等诸多数字货币在一定程度上具有匿名性，使得监管问题日益严峻，如何在保护实体隐私的同时实施有效的监管是数字货币领域的一大挑战。另一方面，由于区块链技术能摆脱第三方机构制约，使得它不再局限于数字货币领域。目前，区块链技术在金融服务、公共服务和IoT等领域的应用尚处于探索阶段，有待进一步发掘。

参考文献
[1] BUTERIN V. Ethereum: A Next Generation Smart Contract and Decentralized Application Platform [EB/OL]. [2018–10–23]. https://github.com/ethereum/wiki/wiki/White–Paper
[2] LIU J K, WEI V K, WONG D S. Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups [C]// Information Security and Privacy: 9th Australasian Conference, (ACISP 2014). Berlin: Springer, 2004: 325–335. DOI: 10.1007/978–3–540–27800–9_28
[3] BEN–SASSON E, CHIESA A, GARMAN C, et al. Zerocash: Decentralized Anonymous Payments from Bitcoin[C]// 2014 IEEE Symposium on Security and Privacy. USA: IEEE, 2014: 459–474. DOI: 10.1109/SP.2014.36
[4] BEN–SASSON E, CHIESA A, GREEN M, et al. Secure Sampling of Public Parameters for Succinct Zero Knowledge Proofs[C]// 2015 IEEE Symposium on Security and Privacy. IEEE: USA, 2015: 287–304. DOI:10.1109/SP.2015.25
[5] HAYEK F A. Denationalization of Money [EB/OL].[2018–10–23]. https://mises–media.s3.amazonaws.com/Denationalisation%20of%20Money%20The%20Argument%20Refined_5.pdf?file=1&type=document
[6] LAMPORT L. Password Authentication with Insecure Communication [J]. Communications of the ACM, 1981, 24(24): 770–772. DOI: 10.1145/358790.358797
[7] CHAUM D. Blind Signatures for Untraceable Payments [C]// Advances in Cryptology: Proceedings of CRYPTO '82. Berlin: Springer, 1982
[8] CHAUM D, HEYST van E. Group Signatures [C]// Advances in Cryptology – EUROCRYPT' 91, Workshop on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1991: 257–265. DOI: 10.1007/3–540–46416–6_22
[9] MERKLE R C. A Digital Signature Based on a Conventional Encryption Function[C]// Conference on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1988: 369–378
[10] DWORK C, NAOR M. Pricing via Processing or Combatting Junk Mail[C]// CRYPTO '92 Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer, 1992: 139–147. DOI: 10.1007/3–540–48071–4_10
[11] SZABO N. Bit Gold[EB/OL].[2018–10–23]. https://en.wikipedia.org/wiki/Nick_Szabo#Bit_gold
[12] NIST. Descriptions of SHA–256, SHA–384 and SHA–512[EB/OL].[2018–10–23]. http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256–384–512.pdf
[13] 李钧, 长铗. 比特币[M]. 北京: 中信出版社, 2014
[14] NAKAMOTO S. Bitcoin: A Peer–to–Peer Electronic Cash System [EB/OL]. (2009–02–08)[2018–10–23]. https://bitcoin.org/bitcoin.pdf
[15] ADAM B. A Partial Hash Collision Based Postage Scheme [EB/OL].[2018–10–23]. http://www.hashcash.org/papers/announcetxt
[16] KATZ J, LINDELL Y. Introduction to Modern Cryptography [M]. Florida: CRC Press, 2007
[17] DIFFIE W, HELLMAN M E. New Directions in Cryptography [J]. IEEE Transactions on Information Theory, 1976, 22(6): 644–654. DOI: 10.1109/TIT.1976.1055638
[18] JOHNSON D, MENEZES A, VANSTONE S. The Elliptic Curve Digital Signature Algorithm (ECDSA)[J]. International Journal of Information Security, 2001, 1(1): 36–63. DOI: 10.1007/s102070100002
[19] FRANCO P. Understanding Bitcoin [M]. Britain: John Wiley & Sons, 2014
[20] 于江. “新型货币比特币”:产生,原理与发展[J]. 吉林金融研究, 2013, (5): 17–19. DOI: 10.3969/j.issn.1009–3109.2013.05.005
[21] 罗强, 张睿. 比特币[M]. 北京: 机械工业出版社, 2014
[22] 张超. 新型虚拟货币比特币的发展现状及其对现实经济和金融影响的研究[J]. 时代金融, 2013, (5): 291–293
[23] 刘宁, 沈大海. 解密比特币[M]. 北京: 机械工业出版社, 2014

作者简介

林成骏，福建师范大学数学与信息学院在读硕士研究生；研究方向为格密码与同态签名。

伍玮，福建师范大学数学与信息学院副教授；研究方向为密码学；主持国家自然科学基金项目2项，参与教育部留学回国人员基金等科研项目；获得福建省自然科学优秀学术论文三等奖；已发表学术论文60余篇。