

量子加密货币研究进展概述

贾恒越, 武霞, 朱建明

(中央财经大学信息学院, 北京 100081)

摘要: 简述了量子加密货币的发展历史, 从方案基本模型、安全性要求、关键技术、研究进展等方面分别对不同类型量子加密货币(包括量子钞票、量子硬币、量子支票、量子比特币)进行了介绍, 最后指出未来有待进一步完善和探究的问题。

关键词: 量子加密货币; 量子货币; 量子密码; 量子不可克隆定理

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00112

Survey of quantum crypto currency

JIA Heng-yue, WU Xia, ZHU Jian-ming

(School of Information, Central University of Finance and Economics, Beijing 100081, China)

Abstract: The development history of quantum crypto currency was explained briefly, and different kinds of quantum crypto currency (including quantum bank note, quantum coin, quantum check, and quantum Bitcoin) respectively from the aspects of basic scheme models, security requirements, key technologies and research progress were introduced. Finally, the issue problems which are needed to be further improved and explored in the future were pointed out.

Key words: quantum crypto currency, quantum money, quantum cryptography, quantum no-cloning theorem

1 引言

货币在经济和金融中有着十分重要的地位, 在金融与互联网相融合的背景下, 为了提供更可靠的安全保障, 将密码算法与数字货币相结合的量子加密货币也受到了越来越多的关注。量子密码学是利用量子力学原理实现密码学任务的一门科学, 在量子密码学中, 除了众所周知的量子密钥分发之外, 还包括许多其他的应用^[1], 如量子货币 (quantum money)、有限量子存储模型、授权量子计算。

传统的数字货币已经被广泛深入地研究过, 其重点就是如何提升交易的安全性。但是数字货币有个天然的缺陷, 就是传统数字比特可以很轻易地复制。量子货币方面, 人们希望用理论上无法复制未知量子态的特点彻底杜绝伪造量子货币的可能性。量子力学的测不准原理和不可克隆原理使量子货币成为量子信息理论最早关注的领域之一, 其从理论上就保证了无法创造出伪造的数字货币。除了不可伪造性, 一个有效的交易机制还需要考虑交易是否易被验证、交易匿名性、可转账性和健壮性等。

收稿日期: 2016-08-12; 修回日期: 2016-11-29。通信作者: 贾恒越, jiahengyue@163.com

基金项目: 国家自然科学基金资助项目 (No.61309029, No.U1509214, No.61272398); 中央财经大学青年教师发展基金项目 (No.QJJ1633)

Foundation Items: The National Natural Science Foundation of China (No.61309029, No.U1509214, No.61272398), The Young Teachers Development Fund of Central University of Finance and Economics (No.QJJ1633)

20 世纪 60 年代末, 哥伦比亚大学的年轻学者 Wiesner^[2]首先想到把量子力学特性应用到防伪和版权保护需求中, 首先提出了量子货币的概念, 但其成果直到 1983 年才得到认可和发表, 如今这篇论文也被视为量子密码学的起源。1983 年, Bennett 等^[3]设计了一种只能使用一次的量子货币方案, 他们称之为量子态地铁票 (quantum state subway tokens)。在此后 20 年的时间里, 量子货币的相关研究被搁置和忽视。直到 2003 年, Tokunaga 等^[4]在 Wiesner 方案的基础上继续研究, 才有新的关于量子货币的成果公开发表, 他们尝试设计了具有不可追踪性的量子现金。此外, Mosca 和 Stebila^[5-7]于 2006 年提出量子硬币 (quantum coin) 概念并对其进行了讨论, 与之前方案中每张量子钞票都具有唯一性不同, 其特点是所有给定面额的量子硬币都是完全一模一样的。

近年来, 随着量子信息技术的不断突破和比特币的热烈讨论, Wiesner 的量子货币思想逐渐成为热点问题得到人们的关注, 其方案安全性得到了深入的研究^[8-10], Pastawski 等^[11]还考虑噪声环境影响对其方案进行了拓展。不仅如此, Georgiou 等^[12]还给出了新的量子加密货币构造方式, 其他货币形式如量子支票 (quantum cheque)、量子比特币 (quantum Bitcoin)^[13]等也陆续成为新的量子加密货币研究对象。

目前, 根据量子货币验证真伪的方式可以将其分为私钥量子货币系统和公钥量子货币系统两类。在私钥系统中, 量子货币只有银行可以对其真伪进行验证, 而公钥系统中允许任何人进行验证。现有的大部分量子货币方案都是私钥系统, 第一个公钥量子货币方案是 2009 年由 Aaronson^[14]提出的, Aaronson 等^[15,16]认为一个量子公钥方案应该有以下性质:

- 1) 存在有效的算法产生量子货币态;
- 2) 无需与货币发行银行通信, 任何人都可以验证量子货币有效性;

- 3) 任何人(除货币发行银行外)都不能复制货币。

从量子加密货币的安全性角度看, 现有方案也可以分为无条件安全的和计算安全的。在无条件安全量子货币方案中, 攻击者即使有无限的计

算时间也无法破坏系统, 如 Wiesner 的方案^[2]就是无条件安全的, 而 Aaronson^[14]、Christiano^[17]、Farhi 等^[18]提出的方案都是在计算困难假设前提下设计的。

近年来, 量子加密货币的研究取得了一定的成果, 本文分别对量子钞票、量子硬币、量子支票及量子比特币的基本思想、模型或特点进行介绍, 并对它们的研究进展进行梳理和概括。

2 基础知识

- 1) 海森堡测不准原理 (the Heisenberg uncertainty principle)

测不准原理又名“不确定关系”, 是量子力学的一个基本原理, 由德国物理学家海森堡于 1927 年提出。在微观世界中, 粒子具有波粒二象性。由于粒子具有波动性, 所以其坐标和动量不能同时取确定的值, 而是要满足一个不确定关系。

- 2) 量子不可克隆定理 (the no-cloning theorem)

量子不可克隆定理最早是由 Wootters 和 Zurek 于 1982 年提出的, 它的内容是: 一个未知量子态不能被完全克隆。该定理指出, 任何物理手段都不可能精确地复制未知量子态, 否则将会违背量子态叠加原理。它也可以看作是测不准原理的一个推论。

- 3) 量子比特 (Qubit, quantum bit)

量子比特是最简单也是最常用的量子系统, 可用一个二维 Hilbert 空间来描述它的状态。该空间的 2 个相互正交归一的基矢可记为

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ 和 } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

则二维 Hilbert 空间上的任意态矢的表达式为 $|\varphi\rangle = c_1|0\rangle + c_2|1\rangle$, 表示量子系统处于 $|0\rangle$ 和 $|1\rangle$ 的概率分别为 $|c_1|^2$ 和 $|c_2|^2$, 其中, c_1 、 c_2 是复数, 且满足 $|c_1|^2 + |c_2|^2 = 1$ 。 $|0\rangle$ 态和 $|1\rangle$ 态可以像 0 和 1 一样形成一个经典比特。但是与经典比特不同, 除了 $|0\rangle$ 和 $|1\rangle$ 这 2 个状态外, 在量子比特中还存在它们的叠加态 $c_1|0\rangle + c_2|1\rangle$ 。因此, 理论上说, 一个量子比特中可以编码无穷多的信息。

如果一组线性无关的向量 $\{|\mathbf{v}_1\rangle, \dots, |\mathbf{v}_n\rangle\}$ 能够线性表示出 n 维 Hilbert 空间上的任意向量, 则称其为该空间上的一组基。进一步地, 若其中的向量两两相互正交 (内积为 0), 且每一个的模 (即 $\sqrt{\langle \mathbf{v}_i | \mathbf{v}_i \rangle}$) 均为 1, 则这样的一组基称为完备正交基。例如, $\{|0\rangle, |1\rangle\}$ 是 C^2 的一组完备正交基, $\left\{ |+\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}, |-\rangle = \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \right\}$ 为它的另外一组常见完备正交基。

考虑复合系统, 假设粒子 A 处于 Hilbert 空间 H_A 上的 $|\phi_A\rangle$ 态, 粒子 B 处于 Hilbert 空间 H_B 上的 $|\phi_B\rangle$ 态, 则 A、B 两粒子组成的系统, 其相应的 Hilbert 空间为 $H_{AB} = H_A \otimes H_B$ 。当两粒子之间没有相互作用, 复合系统处于 $|\phi_A\rangle \otimes |\phi_B\rangle$ 态, 这种状态称为直积态 (product state)。对 2 个量子比特构成的向量空间, 其一组完备正交基为 $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ 。此外, 两量子比特组成的复合系统还有另外一组完备正交基, 即下式中的 $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ 。

$$\begin{cases} |\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \\ |\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \end{cases}$$

可见上式系统中不再是 2 个子系统的直积态, 这种状态称为纠缠态 (entangled state)。上述 4 个纠缠态构成的基称为 Bell 基, 4 个基态通常被称为 Bell 态。

3 量子钞票

一般地, 一个量子钞票 (quantum bill) 方案主要包括 2 个过程: 一是银行产生有效货币的过程; 二是验证一个量子钞票是否有效的过程。

Wiesner 的量子钞票方案是第一个基于量子原理提出的量子货币方案^[2], 协议只需要单量子比特寄存器和单粒子测量即可实现。Wiesner 方案是按照以下方式执行的。

1) 货币发行。首先用 n 个量子比特来制备量子钞票, 银行从 $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ 这 4 种量子态中随机选择, 产生 n 量子比特态 $|\$_s\rangle = |k_1\rangle \otimes |k_2\rangle \otimes \dots \otimes |k_n\rangle$ 。然后, 银行给其分配一个唯一的序列号 s 。一个

量子钞票是由 n 个量子比特及其序列号组成的, 即 $(s, |\$_s\rangle)$ 。银行将量子钞票发送给客户, 并把量子钞票的制备信息及对应序列号一起安全地存储在数据库中。

2) 货币验证。收款人将量子态及其序列号发送给银行验证。银行查找序列号、检索相应的量子状态的描述, 然后验证给定的状态与附加的序列号是否一致。若一致, 则验证通过, 否则公布量子钞票无效。

因为量子钞票中量子态的制备信息是保密的, 由量子不可克隆定理可知, 除银行之外的任何人都不能进行伪造。但是它也存在不足, 即每次交易时收款人必须与银行通信才能验证货币的有效性。由货币验证方式可知, Wiesner 的量子钞票方案属于私钥的量子货币系统, 且银行还能根据每张钞票的唯一序列号对其保持追踪。2003 年, Tokunaga 等^[4]尝试对 Wiesner 量子钞票方案的可追踪性进行改进。他们通过允许钞票拥有者在银行验证之前可以修改钞票来实现不可追踪, 设计方案中特殊的修改仍可以保持钞票有效性, 但银行则无法对其进行区分。虽然 Tokunaga 等的方案具有不可追踪的特点, 但其却带来一个很明显的问题, 即一旦发现伪造货币后, 银行则需要立即作废之前所有已发行的钞票。

Wiesner 的量子钞票方案已经提出 40 多年, 由于其量子钞票附加信息只有银行知道, 所以当协议使用恰当的情况下, 是可以达到信息论安全的。但是, 如果使用不当, 则会导致钞票有可能被伪造。Lutomirski^[9]发现若银行在确认钞票无效后将钞票再还给用户, 则伪造者就可以成功地伪造出有效的量子钞票。由此可见, 即使银行返还无效量子钞票, 整个方案的安全性也会受到影响。

由上述分析可知, 仅仅是可以访问验证者, 验证者返还量子态及其有效性答复, 攻击者无需了解具体验证线路, 就可以借此交互来伪造量子钞票。然而, 公钥量子钞票方案要求验证算法公开, 伪造者也可以使用验证算法, 因此设计的难点就源于此。

关于公钥量子钞票的研究是从 1982 年开始的, Bennett 等^[3]提出公钥量子钞票思想, 并基于不经意传输协议和大整数分解困难问题首次尝试设计公钥量子货币, 该方案只允许一张钱花一次,

因此他们也称其为量子地铁票。随着量子密码和量子计算的不断发展,十多年后不经意传输协议攻击和 Shor 算法^[19]的提出对其安全性也造成了影响。

在标准不可克隆原理下,很难证明公钥量子货币安全,因为它没有考虑伪造者可以反复检测给定量子态是否为有效货币。为了构造可用的公钥量子钞票方案,Aaronson 提出了“复杂度理论不可克隆定理”。定理说明一个计算资源有限的伪造者即使可以访问货币验证器,也不能复制任意量子钞票态。在此基础上,Aaronson^[14]提出了第一个具体公钥量子钞票方案,然而这一方案很快被 Lutomirski 等^[16]证明是不安全的。在文献[16]中,作者提出了无碰撞(collision-free)量子货币的想法,即每个无碰撞的量子钞票都有一个序列号,任何人甚至货币发行银行,都不能产生具有相同序列号的2张钞票。这个功能可以防止银行发行比它声称的钱更多。银行公布所有已生产的量子钞票序列号的列表,从而可以确定银行为每张钞票只生成一个序列号。

不仅如此,研究人员还尝试利用不同的数学理论来设计新的量子货币方案。2012年,Farhi 等^[18]基于 Knot 理论提出了无碰撞且安全防伪的公钥量子货币方案^[18,20],且 Lutomirski^[20]证明了该系统的抗伪造性。Aaronson 等^[17]则基于经典隐藏子空间困难问题设计了新的量子货币系统,Pena 等^[21]对其进行了代数分析,指出无噪声情况下的方案是不安全的。

另外,量子货币验证过程采用的交互方式也逐渐受到人们的关注。Gavinsky^[22]对是否存在仅用经典通信实现验证协议的量子钞票方案进行了研究,利用新的量子密码思想——量子重构博弈(quantum retrieval games)提出了第一个仅用经典方式验证的私钥量子货币方案,且该协议可以达到信息论安全。在 Wiesner 方案的验证算法中,用户和银行之间需要3次交互,于是 Molina 等^[10]设计了一个新的仅用经典验证的量子货币方案,在其方案中验证货币有效性仅需要2次交互即可。2015年,Georgiou 等^[12]对 Gavinsky 方案进行了改进,提出一个信息论安全的私钥量子货币方案,与 Gavinsky 方案需要3轮交互相比,该方案货币验证时仅需一轮的经典通信即可。

此外,Georgiou 等还利用一次寄存器(one-time memories)作为基本工具,设计了一个新的公钥量子货币方案,此方案在随机预言模型下可达到计算安全。

4 量子硬币

量子硬币是量子加密货币的一种,由 Mosca 和 Stebila 首次提出^[5,6]。它是指所有等面额的货币都用完全相同的量子态表示,使用量子硬币一词也是与现实世界的普通硬币类似,即同一面额的不同硬币没有明显的差异。

量子硬币流通使用的基本场景如下。一个银行生产许多量子硬币并保存它们,用户通过保密量子信道从银行提取并保存量子硬币。当用户想使用量子硬币时,先利用量子信道把硬币传给交易对方。对方使用量子线路对硬币进行验证,这个过程还需要与银行进行经典通信和量子通信。最终,量子硬币存储在交易对方处直到银行回收,或作为零钱再找给其他的用户。

一个量子硬币方案由 n 量子比特态和一个量子验证线路组成,其中量子验证线路由 n 量子比特输入寄存器加上可选的附加量子寄存器、一个经典比特输出和 n 量子比特量子输出寄存器组成。Mosca 和 Stebila 认为理想的货币模型应具有以下安全特性。

- 1) 匿名性:任何人不能通过追踪货币来确定使用者或使用地点。
- 2) 不可伪造性:即使伪造者拥有一些货币和验证线路,想以不可忽略的概率伪造出能够通过验证的货币是非常困难的。
- 3) 本地验证性:在无需与银行通信的情况下,能以很高的精确率来验证货币是否有效。
- 4) 可流通性:有效货币在通过验证后不会改变,进而可以多次流通使用。

Mosca 和 Stebila 的量子硬币方案的优点是具有匿名性。在理想模型下,所有面额相同的量子硬币都应是完全相同的,没有人可以进行区分,那么硬币也就无法被追踪。同时,因为量子线路对所有需要验证的收款人都是固定的,这也为收款人提供了匿名性。他们还指出,若验证中需要通信进行交互,则可以利用匿名的经典或量子通信来保障收款人的匿名性。

为了满足理想的量子硬币安全要求,量子

硬币的有效性验证是其体制设计时需要重点考虑的问题。在量子硬币的使用中,不能简单地在不受保护的形式下公开提供一个量子验证线路。量子线路有可能会被分解,从而找到有效方法来伪造硬币。因此,文献[6]中分别基于黑盒假设^[23]和盲量子计算^[24,25]提出了2种实现验证线路的方法。

黑盒假设,即假设验证线路是一个黑盒,安全性取决于复杂度理论假设。Mosca 和 Stebila 首先在黑盒预言模型下实现量子硬币的验证线路,设计了一个不可伪造的量子硬币方案,此方案允许硬币流通任意次数。验证线路黑盒的使用意味着硬币可以本地验证而不需要与银行任何经典或量子的通信。对黑盒计算的经典技术是物理地防止篡改硬件,但是对量子计算中的对应情况还并不是很清楚。Mosca 和 Stebila 将复杂度不可克隆原理应用到量子硬币中,对其安全性进行分析,如果一个伪造者可以访问量子硬币系统的验证黑盒,但不能了解其内部,则无法在任何合理时间内获得比他起始时更多的硬币。

盲量子计算是指一方让另一方代表他执行计算,但计算结束后计算执行者不能获得关于输入态、输出态或所执行操作的相关信息,其安全性属于信息论安全。基于盲量子计算的量子硬币方案,验证者需要通过一种混淆验证与银行进行交互。通过交互,验证者仅能知道量子硬币的有效性。然而,基于盲量子计算的量子硬币需要与银行进行通信,对在线量子通信具有较强的依赖性。

上述量子硬币协议都是私钥量子货币系统,目前还没有公钥量子硬币相关研究成果。此外,在量子硬币协议设计中如何减少盲量子计算的通信和计算量是值得进一步研究的问题。另外,如果银行正确地发行量子硬币,其本质上应是匿名的,但是目前还没有一个机制能让用户的系统验证硬币确实是银行正确发行的,因此这也是一个有待解决的问题。

5 量子支票

量子支票的思想是由 Moulick 等^[13]于 2016 年提出的,他们定义了量子支票应满足的基本性质,并对量子支票的实现方案进行了研究。假设 Bank 是可信中心银行, Alice 是银行客户。Bank 可有若干个支行,它们与 Bank 通过安全的经典

信道相互连接。在交易发生时, Alice 通过签署支票给交易方 Abby 付款, Abby 拿到支票后再与 Bank (或其分行) 验证支票有效性从而进行兑现。Moulick 等认为理想量子支票方案应满足以下要求。

- 1) 可验证性: 可信银行 (或其任何分行) 必须能够验证支票的真实性。
- 2) 不可否认性: 支票拥有者在签发支票后不能否认他签发过的支票。
- 3) 不可伪造性: 任何攻击者不能以支票拥有人名义伪造支票。
- 4) 不可重用性: 任何人不可以多次使用同一支票去提取现金。

在上述条件下, Moulick 和 Panigrahi 基于量子单向函数^[26]、Fredkin 门 (可借助附加粒子非破坏性地比较 2 个量子态) 及数字签名等密码工具提出了第一个量子支票方案, 该方案包括 3 个部分。

- 1) 生成算法: 输入安全参数后, 生成“支票本”及支票拥有者密钥。
- 2) 签发算法: 支票拥有人输入密钥和需要签发的额度, 产生有序组 $\chi = (id, \$, \rho_s)$ 称为支票, 其中, id 和 $\$$ 是用于描述发行者身份和签署金额的经典信息, ρ_s 表示量子支票态。
- 3) 验证算法: 输入密钥、待验证的支票 χ , 判断其是否有效。

Alice 与 Bank 共享 n 个 GHZ 态和与每个纠缠态对应的唯一的经典比特序列号, 双方共同产生一串经典比特密钥并选取一个安全的数字签名算法。Alice 把数字签名中所使用的公钥发给 Bank, 自己保留私钥。Alice 根据支票额度及自己选取的随机数利用量子单向函数来制备 n 个量子态 $|\psi^{(i)}\rangle$ ($1 \leq i \leq n$), 1 个 $|\psi^{(i)}\rangle$ 和 1 个 GHZ 态一组, 然后再依据序列号对每组的 $|\psi^{(i)}\rangle$ 和共享 GHZ 态的一个粒子进行 Bell 测量并执行一个么正操作, 将一个粒子和个人信息、支票面额、序列号、数字签名、随机数等必要的经典信息一起作为签署的支票发送给 Abby。Abby 兑现时将支票交给 Bank, Bank 对其进行测量、纠错后, 检测收到量子态与期望量子态的保真度。若测试结果在安全参数容许范围内, 则支票验证通过; 否则, 银行将拒绝接收支票, 终止交易并销毁支票。

协议假设 Alice 和 Bank 是诚实的, 量子态可

以被存储在量子寄存器中或一直在量子网络中处于传输状态。Moulick 等对协议的安全性进行了简要的分析,依照协议步骤,一个可信银行的任何合法客户都可以签发支票,且在量子力学原理保障下支票不会被伪造和篡改,支票的有效性由可信银行(或下属分行)进行验证。该协议的安全性除依赖量子信息的基本定律外,还与协议选用的数字签名协议、量子单向函数等密码工具的安全性紧密相关。

6 量子比特币

比特币^[27]自 2008 年提出以来受到了极大的关注,与传统的实体货币发行规则不同,比特币是完全依照事先规定好的规则产生新的货币,这种货币能够有效地避免以往实体货币的物理版权伪造,同时基于密码技术也可以有效地防止数字化信息伪造。这种加密货币基于密码学方法和区块链技术,使货币的发行和交易实现了去中心化。

2016 年 4 月,瑞典林雪平大学的 Jogenfors^[28]把量子力学基本原理与比特币设计思想结合提出了第一个去中心化的分布式量子货币系统——量子比特币方案。该系统是基于公钥密码技术的,其方案由 3 个算法组成。

1) 密钥生成算法:输入安全参数 n ,随机生成一个公私钥对。

2) 货币发行算法:输入安全参数 n 和私钥,产生一个量子比特币。

3) 货币验证算法:输入待验证的量子比特币和公钥,验证其是否有效。

量子比特币协议以经典的分布式账簿方案和经典的数字签名方案作为基本工具,方案设计采用隐藏子空间的 mini 方案模型。基于 mini 方案模型不仅为完整协议设计提供方法思路,同时对简化协议安全性证明也有十分重要的作用,这一研究方式在文献[12,16~18]中也被使用过。

Jogenfors 先设计出仅能产生或验证一个量子比特币的 mini 方案,在 mini 方案的基础上再利用区块链技术扩展得到完整的量子比特币方案。交易双方可以通过适当的信道,以传输量子比特币态方式,进行量子比特币转账,并把信息记录在公开的区块链中。交易结算立即生效,无需等待矿工们的确认,而且量子比特币

就像普通的硬币和纸币一样能够被多次重复使用,直至衰减耗尽。

文献[28]还给出了正式的抗伪造性安全证明,量子比特币对用量子计算机做任何伪造货币的行为有天然的免疫力。因而协议理论上是无条件安全的,相应的安全性证明是基于标准的攻击者复杂性假设的。

与经典比特币协议相比,量子比特币还具有以下优势。

1) 量子比特币交易是即时的。经典比特币交易必须由他人验证,而验证时间往往比较长,因此比特币交易比较慢,而量子比特币交易仅需要接收者读取区块链的一个最近的副本即可。

2) 量子比特币交易是可本地完成的。经典比特币交易需要与互联网进行双向通信,而量子比特币的交易则可以在很遥远的地方甚至在太空执行,不需要网络访问。只读区块链访问方式使用户可以只存储本地离线区块链副本即可。假定接收量子比特币已经在本地区块链副本中验证过,那么用户只需要读取本地离线的区块链副本即可完成交易。

3) 量子比特币具有更好的可扩展性。Nakamoto 最初提出比特币时估计的全局限制为每秒 7 次交易。相比之下,量子比特币的本地交易操作意味着对交易的速率没有上限。尽管其挖矿速率受量子碎片和量子比特币区块链的容量限制,但仅在挖矿过程中存在性能限制显然比在交易速率上存在瓶颈要好的多。

4) 量子比特币交易具有匿名性。本地交易操作仅有交易的双方才知道没有记录,因而具有匿名性。本质上,除了普通纸币和硬币是由法定银行发行的以外,量子比特币的交易与普通纸币、硬币的交易是类似的。而对于经典的比特币,所有交易都记录在区块链中,允许任何人复制数据,从而可以追踪交易过程,进而可以消除比特币用户的匿名性。

5) 量子比特币的交易是免费的。经典比特币交易通常需要支付少量费用给矿工,以防止垃圾交易,并为矿工提供额外的激励,在比特币的通货膨胀控制方案下预计这些费用可以维持挖矿到 2140 年。然而,量子比特币交易是本地交易,无需付费,即便受同样通货膨胀控制达到流通货币限额,用户仍可以继续进行交易。

6) 量子比特币的区块链更小,并以更可预测的速度增长。本质上,添加到区块链的数据永远不能删除,截至2016年3月,比特币区块链的大小已超过60 GB。这种大尺寸使它难以在较小的设备上执行完整的比特币实现。量子比特币也有一个不断增长的区块链,但它只记录新发行的货币,即在开采新货币时增长,故能极大地减少占用空间并增加效率。

7) 量子比特币是一种理想的分布式公开可认证的支付系统,是量子力学的一个具体应用。在量子比特币的设计中,货币不需要有一个中央权威机构发放,而且只要在实验环境中能够制备、存储、测量和重构低噪声的量子态,量子比特币就可以马上投入使用。不可克隆定理从理论上提供了防复制的保证,而且基于区块链技术使研究人员能够以分布和民主的方式创造货币。量子比特币是一个具有安全性、与本地交易结合的分布式支付系统,像2008年诞生的比特币一样,该方案的提出给加密货币的发展带来新方法和新思路。

7 结束语

近年来,量子加密货币的研究受到越来越多的关注,本文对现有量子加密货币相关文献进行了较全面的梳理,对多种类型的量子加密货币方案的研究进展和现状进行了综述。总体来说,当前对量子加密货币方案其性能研究主要是从以下几个方面进行扩展的。由私钥加密货币设计转向公钥加密货币方案设计;验证过程由量子通信转化为经典通信;逐步降低验证过程所需交互次数。从安全性角度,其研究主要包括基于量子力学基本原理构建信息论安全的方案、基于不同的数学难题构建计算安全方案、基于数字签名等密码学基本协议安全性的方案。此外,量子比特币的提出也将之前量子加密货币的权威中心式模型拓展到去中心化分布式模型下。

虽然量子加密货币在安全性上有天然的优势,但方案设计使用不当也会带来安全问题,其很多研究还处于刚刚起步阶段,因此存在很多有待完善或解决的问题,如量子硬币的构造需要一个黑盒验证线路,尽管关于经典线路的黑盒有一些研究成果,但对量子线路的情况目前还没有相

关研究成果;减少基于盲量子计算验证的量子硬币的通信和计算量也是值得进一步研究的问题;量子加密货币方案的安全性证明还有待完善和深入;尝试用不同的数学理论来设计安全可靠的公钥量子加密货币方案等。

参考文献:

- [1] BROADBENT A, SCHAFFNER C. Quantum cryptography beyond quantum key distribution[J]. *Designs, Codes and Cryptography*, 2016, 78(1): 351-382.
- [2] WIESNER S. Conjugate coding[J]. *ACM Sigact News*, 1983, 15(1): 78-88.
- [3] BENNETT C H, BRASSARD G, BREIDBART S, et al. Quantum cryptography, or unforgeable subway tokens[C]//*Advances in Cryptology(CRYPTO '82)*. 1982:267-275.
- [4] TOKUNAGA Y, OKAMOTO T, IMOTO N. Anonymous quantum cash[C]//2003.
- [5] MOSCA M, STEBILA D. A framework for quantum money[J]. Poster at Quantum Information(QIP). 2007.
- [6] MOSCA M, STEBILA D. Quantum coins[J]. *Error-Correcting Codes, Finite Geometries and Cryptography*, 2010, (523): 35-47.
- [7] MOSCA M, STEBILA D. Unccloneable quantum money[EB/OL]. <http://www.iqst.ca/events/cqisc06/papers/Mon-1130-Stebila.pdf>.
- [8] NAGAJ D, SATTATH O, BRODUTCH A, et al. An adaptive attack on Wiesner's quantum money[J]. *Procedia Environmental Sciences*, 2014, 19(6):446-455.
- [9] LUTOMIRSKI A. An online attack against Wiesner's quantum money[EB/OL]. <https://arxiv.org/pdf/1010.0256v1.pdf>.
- [10] MOLINA A, VIDICK T, WATROUS J. Optimal counterfeiting attacks and generalizations for Wiesner's quantum money[M]. Berlin:Springer, 2012.
- [11] PASTAWSKI F, YAO N Y, JIANG L, et al. Unforgeable noise-tolerant quantum tokens[C]//*The National Academy of Sciences*. 2012: 16079-16082.
- [12] GEORGIOU M, KERENIDIS I. New constructions for quantum money[C]//*The 10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015)*. 2015: 92-110.
- [13] MOULICK S R, PANIGRAHI P K. Quantum cheques[J]. *Quantum Information Processing*, 2016, 15(6): 1-12.
- [14] AARONSON S. Quantum copy-protection and quantum money[C]//*IEEE Conference on Computational Complexity(CCC 2009)*. 2009:229-242.
- [15] AARONSON S, FARHI E, GOSSET D, et al. Quantum money[J]. *Communications of the ACM*, 2012, 55(8): 84-92.
- [16] LUTOMIRSKI A, AARONSON S, FARHI E, et al. Breaking and making quantum money: toward a new quantum cryptographic protocol[C]//*Innovations in Computer Science (ICS 2010)*. 2010: 20-31.
- [17] AARONSON S, CHRISTIANO P. Quantum money from hidden subspaces[C]//*The Annual ACM Symposium on Theory of Computing*. 2012:41-60.
- [18] FARHI E, GOSSET D, HASSIDIM A, et al. Quantum money from

- knots[C]//Innovations in Theoretical Computer Science Conference. 2012:276-289.
- [19] SHOR P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//The Symposium on Foundations of Computer Science, IEEE Computer Society. 1994:124-134.
- [20] LUTOMIRSKI A. Component mixers and a hardness result for counterfeiting quantum money[EB/OL]. <https://arxiv.org/pdf/1107.0321.pdf>.
- [21] PENA M C, FAUGÈRE J, PERRET L. Algebraic cryptanalysis of a quantum money scheme the noise-free case[M]. Berlin: Springer, 2015.
- [22] GAVINSKY D. Quantum money with classical verification[C]//The 11th International Conference on Quantum Communication. AIP Publishing. 2011:135-140.
- [23] BARAK B, GOLDBREICH O, IMPAGLIAZZO R, et al. On the(im) possibility of obfuscating programs[C]//Advances in Cryptology — CRYPTO 2001. 2001:1-18.
- [24] CHILDS A M. Secure assisted quantum computation[J]. Quantum Information & Computation, 2005, 5(6): 456-466.
- [25] BROADBENT A, FITZSIMONS J, KASHEFI E. Universal blind quantum computation[C]//The Annual Symposium on Foundations of Computer Science. 2008: 517-526.
- [26] BUHRMAN H, CLEVE R, WATROUS J, et al. Quantum fingerprinting[J]. Physical Review Letters, 2001, 87(16): 175-196.
- [27] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. http://wenku.baidu.com/link?url=sizMroqiQwU4R4KOo80ujYJtuMv4Iq-6uaD7ycOwigHaPz9nkKhSbM0U_1ijZ0n6Syo1gZ5b009t8Ix3waazzbDCo4ttyQ2sMAkGauL19wi.
- [28] JOGENFORS J. Quantum Bitcoin: an anonymous and distributed currency secured by the no-cloning theorem of quantum mechanics[EB/OL]. https://www.researchgate.net/publication/299749136_Quantum_Bitcoin_An_Anonymous_and_Distributed_Currency_Secured_by_the_No-Cloning_Theorem_of_Quantum_Mechanics.

作者简介:



贾恒越 (1983-), 女, 内蒙古海拉尔人, 中央财经大学讲师, 主要研究方向为量子信息、量子密码协议设计。



武霞 (1987-), 女, 山东临沂人, 中央财经大学讲师, 主要研究方向为量子信息。



朱建明 (1965-), 男, 山西太原人, 中央财经大学教授、博士生导师, 主要研究方向为信息安全、经济信息分析。