

区块链技术驱动的数字资产确权机制研究^①

张婷¹ 陈乃嘉²

¹ (福建工程学院 福建 350118)

² (福州大学信息研究管理所 福建 350116)

摘要 [目的] 对区块链技术下的数字资产确权机制进行分析, 以期更好地保障数字资产确权机制的运行。[方法] 本文按照机制运行流程, 从确权方式、验证方式、安全保障这三个角度, 采用文献调查法进行研究。[结果] 该机制具有确权的唯一性、安全性和便捷性的优势。[局限] 数字资产产权人隐私保护、区块链技术的漏洞以及确权辅助软件的安全性等问题仍待解决。[结论] 应完善加密算法、加快检测技术研究、提升安全密钥技术。

关键词 区块链; 数字资产; 确权机制

Research on the Authentication Mechanism of Digital Assets Driven by Block Chain Technology

Zhang Ting¹ Chen Naijia²

¹ (Fujian University Of Technology, Fujian 350118, China)

² (Information Research and Management Institute of Fuzhou University, Fujian 350116, China)

Abstract [Objective] This paper analyzes the mechanism of digital asset confirmation based on block chain technology, in order to better guarantee the operation of digital asset confirmation mechanism. [Methods] Literature survey method. [Results] This mechanism has the advantages of uniqueness, security and convenience of confirming power. [Limitations] The privacy protection of digital asset property owner,

①本文系福建省课题基金项目“区块链技术驱动的数字资产确权机制研究”(项目编号: JAT170400)的研究成果之一。

the vulnerability of block chain technology and the security of the auxiliary software for confirming right.
[Conclusions] Improve the encryption algorithm, speed up the research of detection technology and improve the security key technology.

Keywords Block Chain; Digital Assets; the Authentication Mechanism

1 引言

随着信息的发展,数字资产必将成为资产配置中的一个举足轻重的类别,一个创设、发行、交易数字资产爆发的大机会即将来临。然而,传统的知识产权管理体系是以登记制度为核心,仅局限于对实物资产确权的传统的知识产权管理体系正在面临巨大挑战,具体表现在:随着知识产权的生产过程日渐复杂,而原有的管理体系属于静态的管理方式,很难动态地体现出知识产权复杂的形成过程;此外,在后期资产管理和流通的环节也呈现出全球化的特点,现有的登记制度较难适应这种趋势。

数字资产时代,在传统的技术已无法对数字形式的资产确权的情况下,如果采用区块链技术则可以较为轻松地应对这个难题。区块链技术号称是二代互联网的底层技术,对传统技术的升级是颠覆性的,其防篡改、可追溯等特点可以实现数字资产的确权。此外,其高效率、低成本的特点又为区块链技术下的数字资产确权机制提供了保障。

本文介绍了区块链技术并对区块链的技术驱动的数字资产确权机制进行研究,通过对该机制的研究现状、运作程序、特有优势、存在问题进行分析,进一步提出改善现状的对策,以期让区块链技术驱动的数字资产确权机制更好地运行。

2 研究概述

2.1 数字资产概念

除数字货币、数字股票、数字债券外,

数字资产的范围还包括所有数字化了的资产,比如专利、版权、创意、信用等知识文化资产^[1]。

数字资产简单来看有以下属性:(1)数字资产属于虚拟资产,以比特结构存在;(2)数字资产由计算机程序构成,可对其进行编程;(3)数字资产的内涵和外延正在迅速膨胀,金融、知识文化等领域可率先实现高度资产数字化;(4)数字货币等数字资产跨越了资产证券化的阶段,直接达到了资产货币化的阶段。

2.2 区块链技术概念

区块链技术(Blockchain)是为创造一种去中心化、分布式存储、全球统一的超级数据库系统的一整套解决方案,它起源于Satoshi Nakamoto^[2]提出的Bitcoin系统。这种去中心化、分布式存储的数据库技术具有可靠性、可信性、开放性等特性^[3-5],因此区块链技术一经提出,就引起了知识产权界、信息安全界、图书情报与信息资源管理学界的高度关注。

3 区块链技术在数字资产方面的研究现状

作为互联网领域的底层技术,区块链有望促进数据记录、数据传播及数据存储管理方式的转型。截至2017年12月,关于区块链的学术研究数量较少,相关知识产权和专利同样是一片空白。对此,笔者对区块链技术在知识产权方面的研究做一个简单的研究综述。

吴健^[6]探讨了基于区块链技术的数字版权

保护问题；刘伟^[7]对区块链技术如何用于知识产权服务进行了理论思考并提出了区块链知识产权服务平台架构；刘楠等^[8]提出并设计了一种基于区块链技术的大数据交换信息链，既可达到维护数据提供者合法权益的目的，又能实现对流动数据的有效管理与监控，以期在数据拥有者、提供者、中间商、用户等参与主体间顺利进行数据的信息确权、授权、交换与核算；欧洲著名知识产权咨询公司瓦力（Valea AB）^[9]从设计区块链技术的专利、商标申请数量，以及区块链对时间戳、产品认证、智能合约、知识产权审查机构五个方面分析了当前区块链技术对知识产权行业的影响。赵海军^[10]介绍了区块链技术等信息确权的基本技术与方法，这些技术与方法的有机结合与综合运用，可以实现对大数据环境下跨平台的数据信息产权归属及其权属性质的技术确认。

这些研究成果都为发展信息确权的区块链技术与方法奠定了很好的学术基础，当前亟待开展的工作是积极创造和建设大数据流通环境下数字资产确权的区块链技术机制，在大数据流通与交易实践中去检验并建立数字资产确权的区块链技术标准体系。

4 区块链技术驱动下的数字资产确权机制概述

区块链技术驱动下的数字资产确权机制的运行流程具体是：数字资产所有权人通过区块链技术，将例如比特币等数字资产的拥有时间、拥有数量、产权人等信息打包起来，形成了一个结构化的信息包，这个信息包就叫作“区块”。当这笔数字资产进行资金流动时，会产生各个交易节点，这些节点就是“链”。在需要验证数字资产所有权时，由于区块链技

术的不可篡改、不可伪造的特点，可以做到数字资产与资产人关系的一一对应，由此实现了数字资产的确权。此外，该机制还采用了非对称加密等一系列技术，保障了数字资产确权的过程的可靠性和安全性。

下面根据该机制的运作流程，分别从确权方式、验证方式和安全保障这三个角度，对该机制进行具体的分析。

4.1 产权确权方式

区块链驱动的数字资产确权机制的确权方式，主要涉及区块链技术中的“时间戳”（Timestamp）技术，这也是区块链技术最大的创新点。

在数字资产确权时，“时间戳”技术把各个数据区块依次链接起来，形成一个不可篡改、不可伪造的信息可追溯的链条式数据库^[11]，类似一个自创世以来连续不断的总体记账簿，它能反映一个数据库的完整历史。在区块链上，区块头（Header）和区块体（Body）这两部分构成了一个数据区块，时间戳被加盖在区块头中（如图1所示），用以证明当前区块体内所含的活动内容、发生数量及经过集体验证的区块创建过程中生成的所有活动记录的发生时间与行为人。借助时间戳技术，数字资产确权机制不但能实现对统一的数字资产数据库的有效管理，而且还能实现对任一时刻、任一区块上的数据内容及其产权属性与责任人的有效追踪。

数字资产产权人只要在区块链中植入时间戳，那么就等于给自己拥有的数字资产进行了产权标引，使区块链上相关数据的所有权、使用权、交易权、处置权等权属特征均具备了可追溯性。

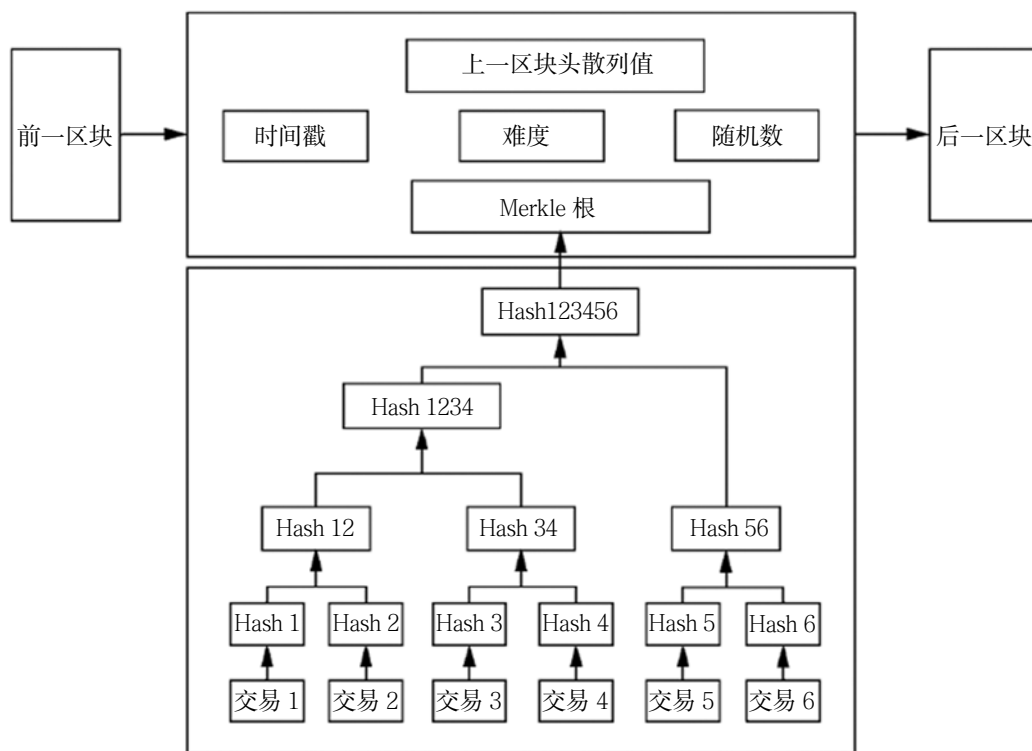


图 1 时间戳技术原理图

4.2 产权验证方式

区块链驱动的数字资产确权机制的产权验证，主要涉及区块链技术中的非对称加密技术，该技术可以实现数字资产所有权人的数字签名，有利于验证数字资产的真伪性和完整性。

非对称加密技术需要两个密钥来进行加密和解密，这两个密钥是公开密钥（public

key，简称公钥）和私有密钥（private key，简称私钥）。在数字资产的产权验证中应用的主要原理是：数字资产的产权持有人通过私钥对其数字资产进行加密，在数字资产验证前，数字资产的产权持有人可以根据需要对访问进行授权，资产验证员可以通过已授权的公钥验证该资产所有权的真实性（如图2所示）。通过非对称加密方式可以方便地实现数字资产产

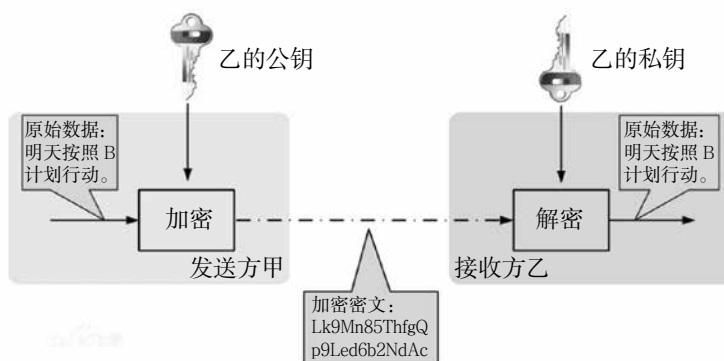


图 2 非对称加密技术原理图

权的验证,达到对于数据所有者的权利委托。

此外,在数字资产产权验证时,由于区块链技术具有统一的数据查询接口和统一的数据标准,使得在产权验证时可以不再依赖于第三方机构而实现实时的数据共享,提高了数字资产确权证明的效率。

4.3 安全保障措施

数字资产确权机制的安全性是由区块链的加密技术所保证的。区块链系统是开放的,除了交易各方的私有信息被加密外,区块链的数据对所有人公开,任何人都可以通过公开的接口查询区块链数据和开发相关应用,虽然整个区块链系统信息高度透明,但是整个分布式网络所提供的算力相当地惊人,若要篡改其中的数据,无论是从理论上,还是在实践中都较难实现。

前文所说的非对称加密技术,不仅可以应用于数字资产的数字签名,还能够对信息进行加密,在数字资产确权机制的安全保障中,具体的应用流程是:数字资产所有权人使用指定操作者的公钥对信息加密后再发送给该操作者,该操作者就可以利用自己的私钥对信息进行解密。虽然存储在区块链上的各类交易信息是公开的,但是具体参与确权或者交易的账户身份信息是加密的,只有在数据拥有者授权的情况下才可以访问到数据,保证了交易的隐私和数据的安全,该机制具备了较高的可信性。

此外,该机制中的产权信息采取分布式存储,没有中心化的特定硬件或管理机构,分布式存储的设计使区块链系统具有很好的健壮性,一个或几个网络节点发生故障不影响整个区块链系统的运行,因此该机制的区块链系统具有很高的可靠性。

5 区块链技术驱动下的数字资产确权机制分析

5.1 数字资产确权机制的特有优势

基于以上对数字资产确权机制的分析,可以得出数字资产确权与实物资产确权相比具有一定的优势,具体表现在以下三方面。

(1) 数字资产确权的唯一性

区块链技术以“时间戳(Timestamp)”的方式把各个数据区块依次链接起来,形成一个不可篡改、不可伪造的信息可追溯的链条式数据库。借助时间戳,它不但能实现对这种全球统一数据库的有效管理,而且还能实现对任一时刻、任一区块上的数据内容及其产权属性与责任人的有效追踪。区块链技术的不可篡改性和实时跟踪的特点,能有效地避免实物资产确权的易丢失、易出错的缺陷,降低了数据的维护成本。

(2) 数字资产确权的安全性

区块链采用非对称加密和授权技术,存储在区块链上的各类信息是公开的,但是具体参与交易的账户身份信息是加密的,只有在数据拥有者授权的情况下才可以访问到数据,保证了交易的隐私和数据的安全,具备了较高的可信性,保障了数字资产在确权后交易的安全性,避免了传统的实物资产登记可能因为自然灾害等因素造成确权的不安全性。

(3) 数字资产确权的便捷性

依赖于可靠、不可篡改的数据库,区块链将彻底改变资产信息的登记与验证方式,各类数据信息和社会活动将不再依靠第三方个人或机构来获得信任或建立信用,全网的多方验证形成了数据信息的“自证明”模式,就相当于“数字身份证”。由于不再依赖于第三方机构管理和提供的数据信息,使得数字资产主权的证明更加便捷。

5.2 数字资产确权机制存在的问题

基于以上对数字资产确权机制的分析,也可以看出数字资产确权机制存在的一定问题,具体表现在以下三方面。

(1) 数字资产权人的隐私问题

随着区块链技术的不断发展和广泛应用,其面临的隐私泄露问题越来越突出。相比于传统的中心化结构,区块链机制不依赖特定中心节点处理和存储数据,因此能够避免集中式服务器单点崩溃和数据泄露的风险,但是为了在分散的区块链节点中达成共识,区块链中所有的记录必须公开给所有节点,这将显著增加隐私泄露的风险^[12]。区块链技术下的数字资产确权机制虽然具有匿名性,但是交易记录却完全公开,在数字资产确权中,分析人员通过分析数字资产的确权信息、交易数据可以获得用户的交易规律,甚至可以以此推算出用户的身份信息和位置信息,后果十分严重。

(2) 区块链新型技术仍有待完善

2016年6月,发生了黑客攻击TheDAO项目中智能合约的事件,也让更多人认识了智能合约还有漏洞。智能合约仍属于一项新技术,需要懂代码的监管者持续进行考核校验,并能预知程序执行后可能会产生的后果。TheDAO项目属于公共契约范畴,它更像一个公募基金,参与人数众多且不特定,整个“基金”的募集和管理的过程均由计算机程序执行,基金的募集、管理、赎回等流程都包含在一个被编程的智能合约之中。这样复杂的流程,稍有不慎就会出现漏洞,也给数字资产确权的安全性造成了威胁。

(3) 数字资产确权辅助软件的安全性问题

区块链技术本身的安全性很高,采用非对称密钥机制,保证了安全性和有效性,但是对

私钥的使用和保存状况却令人堪忧,即使256 bit 的私钥表现成50个字符长度形式,依然难以记忆,使用其他软件进行辅助交易是必然的选择,但这类软件的安全性就值得商榷,交易网站或者个人的比特币被盗的消息络绎不绝,使用安全问题需要引起人们的重视。

5.3 数字资产确权机制的完善建议

(1) 完善加密算法,避免机制安全漏洞

针对该机制的区块链安全漏洞的问题,建议应采用合适的访问控制策略,防止恶意节点接入和监听网络,从根本上增强网络层的保护能力。此外,可以采用传统的中心化架构中成熟的安全措施,针对公有链网络,重点研究异常节点检测的方式,及早发现和屏蔽恶意节点,此外还需研究在效率、性能、易用性方面更好的匿名通信机制,替代现有的匿名通信方案;另外,有必要研究采用密码学算法保证数字资产确权的安全性,基于加密的保护方案应该充分考虑区块链服务器在计算性能和存储性能上的缺陷,设计通用性更高的加密方案。

(2) 加快检测技术研究,保障产权人隐私安全

针对该机制的数字资产产权人隐私保护问题,建议除了行政手段外,有必要研究针对性的监管技术,检查和遏制利用区块链技术进行的非法活动。目前已经出现了很多专门从事区块链监管科技的公司和研究机构,例如,美国纽约的Chainalysis开发了用于打击网络犯罪活动的工具,已经检查了价值150亿美金的比特币交易^[13]。美国桑迪亚国家实验室受美国政府支持开发分析工具,这种工具将帮助执法部门将数字资产交易去匿名化^[14];英国伦敦的区块链情报公司Elliptic为全球企业和法律机构提供数字资产监控的技术支撑;加拿大公司Blockchain Intelligence Group开发了QLUE

来帮助世界各地的执法机构通过识别和追踪数字资产来打击涉及比特币的金融犯罪交易^[15]。此外在研究数字资产确权的隐私保护技术的同时,也应该关注如何对滥用区块链技术的非法行为进行监管。

(3) 提升安全密钥技术,开发多样验证方式

针对数字资产确权辅助软件的安全性问题,建议在应用层除了提升用户的安全意识、增强区块链服务商的安全能力外,重点是要研究钱包的密钥保护技术,开发使用方便、安全可靠的钱包程序,钱包密钥直接关系到账户的安全,可以研制无密钥的密码算法和代码混淆技术,防止恶意用户通过反汇编等方法提取密钥信息,可以研究基于口令、硬件以及生物特征等多因素认证机制,增强私钥的安全性,有效地避免辅助交易软件所带来的安全隐患。

6 小结

本文对区块链技术驱动的数字资产确权机制进行了初步的研究:首先,通过概念介绍和研究综述的方式概述了该机制的研究现状;其次,根据机制的运作流程,从确权方式、验证方式和安全保障三个角度对该机制进行了分析,在分析的基础上,归纳总结了与实物资产相比的区块链数字资产确权机制的特有优势,并对其存在的问题进行剖析,最终提出解决该机制问题的对策。

本文主要从理论角度对数字资产确权机制进行研究,而实践中更为具体的研究还有待加强。数字资产确权机制未来会面临诸多例如技术和政策等考验,这些也成为未来研究中需要继续思考的问题。

参考文献

- [1] 不了解资产数字化? 一边玩去[EB/OL]. [2017-07-11].http://www.sohu.com/a/156324489_470007
- [2] Satoshi Nakamoto.Bitcoin: A Peer-to-Peer Electronic Cash System[EB/OL]. [2017-12-04].<https://bitcoin.org/bitcoin.pdf>.
- [3] Swan M.Blockchain: Blueprint for a New Economy[M].Sebastopol, CA: O'Reilly Media, 2015.
- [4] 袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2016,42(04):481—494.
- [5] 沈鑫,裴庆祺,刘雪峰.区块链技术综述[J].网络与信息安全学报,2016,2(11):11—20.
- [6] 吴健.去中心化数字版权保护技术初探[J].西部广播电视,2016,(12):210—213.
- [7] 刘伟,蔺宏宇.区块链技术原理及基于区块链技术的知识产权服务浅析[J].产权导刊,2016,(11):65—69.
- [8] 刘楠,魏进武,刘露.大数据交换信息链[J].电信科学,2016,32(10):130—136.
- [9] Valea AB. Blockchain Technology Expected to Strongly Impact the IP Industry [EB/OL]. [2017-12-24].<https://www.lexology.com/library/detail.aspx?g=a1461135-598b-4c3c-811c-73ac70c3f67b>
- [10] 赵海军.大数据环境下的信息确权方法探究[J].图书情报导刊,2017,2(09):40—47.
- [11] 林小驰,胡叶倩雯.关于区块链技术的

- 研究综述[J].金融市场研究, 2016, (02): 97—109.
- [12] Au M H, Liu J K, Fang Junbin, et al. A new payment system for enhancing location privacy of electric vehicles[J]. IEEE Trans on Vehicular Technology, 2014, 63 (1): 3—18.
- [13] Chainalysis. Protecting the integrity of digital assets [EB/OL]. [2017-12-25]. <https://www.chainalysis.com/>
- [14] Sandia. Beating bitcoin bad guys [EB/OL]. [2017-12-25]. <https://www.sandia.gov/news/publications/labnews/articles/2016/19-08/bitcoin.html>
- [15] Blockchaingroup. Blockchain intelligence group [EB/OL]. [2017-12-25]. <https://Blockchaingroup.io/>