基于区块链技术未来数字货币的可行性研究

Feasibility Study of Future Digital Currency Based on Blockchain Technology

付允纬　张晶　高华玲　叶龙祥

Yunwei Fu　Jing Zhang　Hualing Gao　Longxiang Ye

三亚学院　中国·海南 三亚 572000

Sanya College, Sanya, Hainan, 572000, China

摘　要：比特币的出现掀起了世界各国对区块链技术和数字货币研究的热潮。论文将区块链核心技术进行归纳，通过对区块链技术在政务领域、民生领域、商业等领域进行分析，利用区块链技术可以降低交易成本，提高交易效率，增加信息安全性，缩短交易流程。论文对数字货币及区块链金融领域进行了展望，未来可以深入研究区块链技术应用于金融领域的作用机理、合适场景和影响因素。

Abstract: The emergence of Bitcoin has set off a worldwide upsurge of research on blockchain technology and digital currency. In this paper, the core technologies of blockchain are summarized, and through the analysis of blockchain technology in the fields of government affairs, people's livelihood and commerce, it is found that the use of blockchain technology can reduce transaction cost, improve transaction efficiency, increase information security and shorten transaction process. In this paper, the digital currency and blockchain finance are prospected, and the mechanism, appropriate scenarios and influencing factors of blockchain technology applied in the financial field can be deeply studied in the future.

关键词：比特币；区块链；数字货币

Keywords: Bitcoin; blockchain; digital currency

基金项目：国家级大学生创新创业训练项目《基于区块链的人脸识别自由贸易港积分系统》（项目编号：202013892002）；海南省教育厅项目《基于海南旅游大数据的微博舆情分析与研究》（项目编号：Hnky2020-47）。

课题项目：全国高等院校计算机基础教育研究会计算机基础教育教学研究项目。课题名称：数据分析基础——计算机基础课程教学模式研究（课题编号：2020-AFCEC-067）。

DOI: 10.12346/emr.v4i2.5353

1 引言

区块链技术起源于比特币，最初的设计目的是解决电子支付中过度依赖可信第三方的问题。区块链将 Hash 函数、工作量证明（Proof of work,PoW）等成熟的技术进行重组，结合公私钥加密、数字签名和零知识证明等密码学技术，全新的分布式基础架构和计算范式，分析目前数字货币应用领域，展望未来数字货币的设计可行性。

2 比特币区块链的技术原理

区块链作为一种由不同节点共同参与的分布式数据库系统开放式账本系统，是按照密码学方法组成的区块链数据块，即区块链。区块链技术是在信息非对称环境下，在无信任担保的情况下，采用机器加盟算法所建立信任机制，以保证交易安全进行。主要运用了四项基础性技术：哈希预算（SHA256）、数字签名、P2P 网络及工作量证明。

哈希预算（SHA256）是由美国国家安全局研发，由美国国家标准与技术研究院（NIST）在 2001 年发布. 将任何一串数据输入到 SHA256 将得到一个 256 位的 Hash 值（散列值）。其特点是相同的数据输入将得到相同的结果。输入

【作者简介】付允纬（2011-），男，中国陕西咸阳人，在读本科生，从事区块链技术研究。

数据只要稍有变化（如一个 1 变成了 O）则将得到一个千差万别的结果，且结果无法事先预知。

数字签名，是基于椭圆曲线加密技术的公私钥来实现。公钥和私钥一般成对出现，如果消息使用公钥加密，那么需要该公钥对应的私钥才能解密；同样，如果消息使用私钥加密，那么需要该私钥对应的公钥才能解密。公钥加密保障交易信息的公开性，同时私钥解密保证了私人信息的隐蔽性。区块链技术利用非对称加密算法保证了数据的安全性。

P2P 网络，根据比特币协议，区块链采用一种无结构的 P2P 网络。P2P 网络分为有结构和无结构两种，区别在路由规则的制定方面。有结构的 P2P 网络，利用一致性哈希表（DHT）构建每个节点的路由表。无结构的 P2P 网络，节点之间路由靠广播方式. 为了避免广播风暴，一般设置一个网络 TTL，来限制广播传播的范围。

工作量证明机制（PoW），工作量是信任产生的基础。在区块链中，通过解决一个数学难题来证明自己的工作量。这个数据难题就是对一个数字串进行两次 SHA256 运算，如果得到的数小于一个指定的值就算是成功。否则，要通过不断地尝试试错（学术上叫暴力破解）来求解这个数。

3 区块链的分类及意义

区块链可以分为公有链、私有链与联盟链。公有链具有自由加入和退出的机制，信息开放程度高，代表为比特币、以太坊。联盟链是通过授权加入和退出，私有链为私有机构单中心网络。公有链、联盟链、私有链在开放程度上是递减的，公有链开放程度最高、最公平，但速度慢、效率低；联盟链、私有链的效率比较快，但弱化了去中心化属性，更侧重于区块链技术对数据维护的安全性。

区块链不仅是技术上的重大创新，更是人类组织结构上的重大创新，区块链首次在组织分散的前提下实现了行动的统一，理论上实现了数据传输中的数据自我证明，从深远意义上讲，这超越了传统和常规意义上需要依赖第三方的信息验证模式，降低了建立全球信用体系的成本。

4 区块链的应用领域

4.1 在政务方面

政府数据共享，通过构建专属的私有链，解决数据共享监管弱、数据关联风险较大等痛点。在政务数据库建设中采用区块链技术，构建分布式数据库或去中心化数据库，将大大减少交易环节，降低交易成本，缓解政务服务参与者之间的信息不对称，提高分工协作的效率。区块链的可追溯性在“数字政府”的监管平台中应用区块链技术，将被监管对象的所有信息都记录在案，能够准确高效地监测和追溯监管对象的实时状况。基于区块链技术的“数字政府”治理架构，能利用哈希函数和非对称加密等算法对隐私保护或涉密数据进行加密来确保数据的安全性，并能在数据共享交换过程中确保其完整性 [1]。

4.2 在民生方面

精准扶贫方面，区块链技术可以使捐赠的环节更加透明，其原因在于区块链上的交易可以点对点完成，机构可以直接将钱捐赠给指定的人或机构，无需转手多家银行和机构，且每一次捐赠都会直接记录在分布式账本数据库中，记录公开透明，可查询且不可篡改，也可以通过账本追溯捐款去向。利用区块链技术去中心化、不可篡改、可追溯、共识信任等技术特性结合指纹识别技术实现扶贫对象的识别和退出、以及基金管理。

个人医疗健康数据，解决数据分散、不完整、共享难的痛点；阿里健康与常州市合作“医联体 + 区块链”试点项目，该项目将区块链应用于医联体底层技术架构体系中，实现医疗机构之间的安全、可控的数据互联互通，用低成本、高安全的方式，解决长期困扰医疗机构的信息孤岛和数据安全问题。

在智慧出行中，利用区块链的数据完整性和不可篡改性建立一个车辆管理系统公有链，即可以进行车辆管理，同时也能进行二手车的售卖等。与传统的车辆管理不同，所有车辆都需要在这个公有链下进行注册，才能在智慧城市的道路上行驶，区块链的智能合约技术用来提醒用户对车辆及时进行检测，从而减少交通事故的发生，保护用户的安全。

4.3 在商业方面

传统的票据形式难以满足改革和创新的要求，票据区块链在一定程度上克服了传统票据存在的一系列缺陷。可以有效防范票据市场风险的同时，更好的解决双方内控不足、贸易真实和违规交易的问题。数字票据是基于区块链的底层架构和加密算法进行研发的，可以显著降低运营成本，提高运作效率。

小微企业信用认证，利用区块链与大数据技术，还原小微企业行为特征、风险画像、信用水平。减少小微企业信用风险一方面，由于区块链上的存储信息具有不可伪造、无法篡改的特性，通过这一技术能够保证所有交易信息的安全与真实可靠。另一方面，做到全程实时进行监控，从而避免出现信息造假的情况，保证业务的公开透明。多方资源共享在开放架构的基础上，该平台能够获取银行等外部主体的数据资源，借助大数据等技术手段，构建形成更加完整的供应链金融网络，多维度地考察中小企业的信用状况 [2]。

供应链金融是区块链技术重要应用领域，供应链金融领域存在信息真实性无法辨别，无法鉴别核心企业是否与上下游企业合谋造假、虚构交易诈取贷款等。通过区块链技术多个利益相关方可以提前设定好规则，实现数据的互通和信息的共享。采用智能合约将降低人工监督成本，并在独立于第三方的前提下也可自动执行，紧密对接业务流程节点，简化运作程序。

5 未来数字货币的可行性设计

5.1 法律准备

数字货币的发行首要原则是保证金融稳定，因此赋予数字货币法偿性。在数字货币发行前，在法律层面明确数字货币是人民币的一种表现形式，同时赋予数字货币无限支付能力，凭其法律效力强制流通使用，和现行流通的纸币、铸币一样是无限法尝货币，同样适用于《中国人民银行法》第十六条和《中华人民共和国人民币管理条例》第三条规定。从长远看，对数字货币另行立法更为可取[3]。

5.2 发行主体

中国数字货币的发行主体应为中国人民银行，数字货币内在价值由国家信用做保证，代表中国国家形象，通过互联网在全国乃至世界行使货币职能。企业基于企业信用或者数字货币沉淀，发行用于电子支付的虚拟货币等等，应规定于常规的电子货币范畴。

5.3 流通网络及数字签名

流通网络应由互联网、移动通讯网及末端支付渠道组成。数字货币应该自带数字签名，允许流通环节中各计算机节点记录和安全验证。允许面对面在线或单离线和离线支付操作。

5.4 结算采用分布式记账系统

数字货币的分布式记账网络应该只由国家统一组件的骨干计算机网点组成，也就是说，数字货币的支付、结算的验证等只由固定的计算机网点完成。云计算、云存储技术有利于搭建这种骨干计算机网点。数字货币本身不局限于特定技术；从竞争择优的角度，也需要在优化演进过程中充分比较多种技术路线。因而，技术上央行数字货币体系应该是一种包容性的架构，既能体现成熟技术的稳定性，又要能够保持一定的技术先进性。

5.5 支付账号与数字钱包

数字货币体现出货币的储藏功能。数字钱包只是对对应的交易情况进行验证和登记，没必要参与验证或记录整个网络的交易，以体现快捷、便利的功能，避免无必要的重复计算。数字货币应具备电子货币便捷支付的优点，而且要发展安全可靠的离线支付功能，才能充分保证数字货币的信誉，减少对纸币的依赖。

5.6 风险提示

法定数字货币一经问世，货币结构将发生显著变化，货币乘数也将迅速增大，金融脱媒甚至“去中心化”的可能性加大。因此，数字货币的“隐形性”，金融恐慌更易传染，金融风险更易爆发，对金融安全乃至社会稳定的破坏性将更难预测与把控。因此，通过大数据进行数字货币宏观运行分析、对骨干分布计算网点进行实时管理以及对数据钱包实行微观监测，中央银行闭环式审慎管控数字货币生产、发行、流通、回笼全过程，则十分必要，也切实可行[4]。

6 结语

区块链技术的诞生为社会中实体货币虚拟化提供了可能，同时货币自身的价值依托也不断地发生演化，从最早的实物价值到今天对科学技术和信息系统的信任价值。未来与人工智能、大数据采集和分析等领域要深度的结合，建立一个虚拟空间的真实社会，一个高效、开放、共享的高度信任的社会。

参考文献

[1] 王玮.区块链的意义与数字货币应用中的难点思考[J].财富时代,2019(11):10-11.

[2] 张鹏,罗新星.一种基于区块链数字代币的有限溯源方法[J].系统工程理论与实践,2019(6):1469-1478.

[3] 伍旭川.区块链技术的特点、应用和监管[J].金融纵横,2017(4):19-23.

[4] 张晶.企业采购成本数据分析与控制[J].数字技术与应用,2021(4):198-200.