

报告编号: 201836000Z08D382

# 科技查新报告

项目名称: 区块链技术驱动下我国数字货币发展路径研究

委托人: 西安邮电大学 王娟

委托日期: 2018年9月7日

查新机构: 教育部科技查新工作站(Z08)

(科技查新专用章)

完成日期: 2018年9月12日



查新项目 名称	中文：区块链技术驱动下我国数字货币发展路径研究			
	英文：略			
查新机构	名称	教育部科技查新工作站(Z08)		
	通信地址	陕西省西安市咸宁西路 28 号	邮政编码	710049
	负责人	贾申利	电话	029-82667953
	联系人	时莹	电话	029-82667852-859
	电子邮箱	shiyang@mail.lib.xjtu.edu.cn		
<b>一、查新目的</b> 申报中国通信学会科技进步奖。				
<b>二、项目的科学技术要点</b> <p>区块链技术凭借去中心化、去信任化、共识机制、不可篡改等特性，在各行业中逐渐普及。该课题组在西安邮电大学、中钞（杭州）区块链研究院、北京众享比特科技有限公司等单位支持下对区块链技术驱动下我国数字货币发展路径进行研究，对区块链技术驱动下的我国数字货币发展进行研究，针对数字货币目前发展的现状和问题，从价值尺度、流通和支付功能、财富效应等多个维度，提出了区块链技术驱动下的数字货币实现技术，解决了数字货币技术难点和应用场景，为金融支付体系的应用落地提供了参考路径和技术方法：提出数字货币的发行和落地实施架构，搭建数字货币发行体系架构；提出络谱区块链登记开放平台，设计实现基于区块链的数字凭证注册、分配、转移、监管的完整方案，实现数字凭证的易用、防伪、易流通、可追溯，并设置监管机制，实现监管合规；为数字票据、信用积分管理联盟链和私有链的管理方法提供技术基础和技术支持，保障其在使用中的安全性和不可篡改性。</p> <p>络谱平台支持多种格式文件存证、数据来源可追溯、隐私保护等功能，并对监管表示友好；络谱区块链登记开放平台于 2018 年 1 月在上海票据交易所实验性生产投产。设计提出由中央银行将主权数字货币发行至商业银行业务库，商业银行受主权中央银行委托向公众提供主权数字货币存取等服务，并与主权中央银行一起维</p>				

护主权数字货币发行、流通体系的正常运行产生经济效益 374 万元。中钞络谱已与多方进行合作和探索，如中科院国家授时中心、信息产业部电子科技情报研究所、国家金融 IC 卡安全检测中心、江苏广电集团、杭州银行、中钞国鼎、西正印制、贵州食品安全云、上海仪电溯源、浙江数秦科技、杭州安存、安安专机等。该平台获得直接经济效益 563 万元，间接经济效益 1210 万元。

众享比特在区块链数据票据、积分管理、金融信贷和存证管理等领域从接入安全、通信安全、存储安全、交易安全四个维度构建去中心化的网络安全体系，通过区块链技术实现互信的数据存储和智能合约应用，为区块链驱动数字货币发展提供技术保障。已经取得 15 项软件著作权，已申请 41 项核心专利，5 项产品获得北京市新技术新产品称号，1 项技术获得中国好技术奖项，1 项产品入选中央政府采购名录，为数字货币的应用场景进行了主要工作。

### 三、查新点

1、提出区块链对数字货币发展的驱动力，设计区块链技术驱动下的我国数字货币的发行落地具体架构和监管思路；

2、提出络谱区块链登记开放平台解决方案，建立基于区块链的数字凭证注册、分配、转移、监管的完整方案；

3、为数字票据、信用积分和数字货币的身份管理、安全验证等领域剔除联盟链和私有链管理方法，保障其在使用中的安全性和不可篡改性。

### 四、查新范围要求

希望就本项目与国内相关文献进行比较是否有相同的研究报道。

### 五、文献检索范围及检索策略

#### 中文数据库检索范围

- |                    |                   |
|--------------------|-------------------|
| 1. 中国学术期刊网络出版总库    | 1915 年—2018 年 9 月 |
| 2. 中国博士学位论文全文数据库   | 1984 年—2018 年 9 月 |
| 3. 中国优秀硕士学位论文全文数据库 | 1984 年—2018 年 9 月 |



4. 中国重要会议论文全文数据库	1953 年—2018 年 9 月
5. 中国专利全文数据库	1985 年—2018 年 9 月
6. 国家科技成果数据库	1978 年—2018 年 9 月
7. 重庆维普中文科技期刊数据库	1989 年—2018 年 9 月
8. 万方期刊论文数据库	1998 年—2018 年 9 月
9. 万方学位论文数据库	1980 年—2018 年 9 月
10. 万方会议论文数据库	1985 年—2018 年 9 月
11. 万方成果资源数据库	1978 年—2018 年 9 月
12. 万方专利技术数据库	1990 年—2018 年 9 月
13. 中国知识产权局中国专利数据库	1985 年—2018 年 9 月

### 中文检索词

数字货币；加密货币；区块链驱动力；发行；监管；数字存证；数字钱包；数字票据；信用积分管理；联盟链；私有链

### 中文检索式

1. 区块链 AND (数字货币 OR 加密货币) AND 驱动
2. 区块链 AND (数字货币 OR 加密货币) AND (发行 OR 监管)
3. 区块链 AND (数字存证 OR 数字钱包 OR 数字票据 OR 信用积分管理 OR 联盟链 OR 私有链)

## 六、检索结果

依据上述文献检索范围和检索式,共检索到密切相关文献 16 篇。

密切相关文献的题录和主要内容如下:

1. 张弛,贺岩,呼延雅妮,董琦,柴旖嫻.当前主流数字货币交易模式分析及发展趋势研究[J].西部金融,2018,(03):50-54.

[相关内容] 中国人民银行在 2014 年开始数字货币的研究,基于区块链和数字货币的数字票据交易平台于 2017 年成功测试运行,并正式挂牌成立了数字货币研究所。数字货币目前尚存在着线下交易应用不畅、存在隐私泄露风险,易成为洗钱、诈骗等犯罪工具,影响金融稳定与安全等诸多的问题与缺陷。本文通过研究以上问题的解决对策,对我国发展数字货币进行展望。

2. 周永林.央行数字货币及其实现模式探讨[J].金融电子化,2016,(09):35-37.

[相关内容] 数字货币提供了全新的资产持有和交换方式。其主要特点体现在以下几个方面,一是采用以加密算法为核心的区块链或分布式总账技术,使素不相识的人们可以在网络上建立信任机制,使"点对点"直接交易成为可能。二是在发行方面,没有一个中心化的机构控制和管理虚拟货币发行。三是这类虚拟货币没有任何资产担保,不和任何资产挂钩。四是在转账支付等交易环节,不需要借助银行等中间机构。

3. 王永红.数字货币技术实现框架构想[J].中国金融,2016,(08):14-16.

[相关内容] 2016 年中国人民银行正式公开表示要积极吸收国内外数字货币研究的重要成果和实践经验,做好关键技术攻关,争取早日推出央行发行的数字货币。本文就建立在区块链技术上的数字货币应用和前景展开讨论。

4. 庄雷,赵成国.区块链技术创新下数字货币的演化研究:理论与框架[J].经济学家,2017,(05):76-83.

[相关内容] 鉴于区块链技术的数字货币探索,比较分析数字货币演化历程和动因,从货币价值、发行主体、数量调节三大基本问题总结数字货币的本质、属性、锚定、信用创造四大机理。

5. 梁赓,左春,李春晓,陈胜,蒋步云,杜乐乐.基于联盟链的区块链组链方法及区块链系统:北京,CN108280646A[P].2018-07-13

[相关内容] 本发明提供一种基于联盟链的区块链组链方法及区块链系统。通过对节点进行分区,实行分区背书,分区出块,能够极大的降低共识成本,提高系统吞吐量,减少系统响应时间。

6. 李文红,蒋则沈.分布式账户、区块链和数字货币的发展与监管研究[J].金融监管研究,2018,(06):1-12.

[相关内容] 本文认为,针对金融科技的快速发展,监管者应遵循"技术中立"原则,按照金融业务本质实施监管,维护市场公平竞争;及时对金融科技/互联网金融业务进行"穿透定性",防止冒用"技术"名义违法违规开展金融业务;加强对金融机构与科技企业合作的监管,强化对信息科技风险、外包风险和其他操作风险的管控;同时,持续加强跟踪研究和监测分析,做好专业知识、人才队伍、政策措施等方面



储备。

7. 江海峰.区块链技术在金融行业的应用模式研究[D].导师: 张小茜;顾清良.浙江大学,2018.

[相关内容] 本文从区块链系统的基础模型分析入手,以比特币和以太坊区块链系统为例,自下而上将模型分为数据层,区块层,网络层,共识和激励层以及应用层五部分,并分别对于各层主要应用的基础技术和运行机制进行介绍,这其中重要的部分包括链式区块结构,哈希算法和 Merkle 树,非对称加密,P2P 网络,共识激励机制和智能合约等。

8. 张波波,张一锋.一种基于区块链的数字身份验证的方法、装置和系统:浙江,CN107888382A[P].2018-04-06

[相关内容] 本申请提供基于区块链的数字身份验证的方法,通过采用随机数,签名,各种证书的方式实现了区块链间高安全性的数字身份认证。本申请还提供了基于区块链的数字身份验证的装置和系统,具有上述有益效果。

9. 张波波,张一锋.一种基于金融 IC 卡端的数字货币交易方法及系统:浙江,CN107862607A[P].2018-03-30

[相关内容] 本发明公开了一种基于金融 IC 卡端的数字货币交易方法,该方法能够实现钱包应用同时支持数字货币与电子货币交易,并确保数字货币交易流程的高效性、安全性;本发明还公开了基于金融 IC 卡端的数字货币交易装置及系统,具有上述有益效果。

10. 李刘海,陈姝,卢小明.基于区块链的业务数据同步方法及系统、数据库系统:北京,CN106874393A[P].2017-06-20

[相关内容] 本发明提供一种基于区块链的业务数据同步方法及系统、数据库系统。本发明通过将业务数据同步至外部数据库中,由外部数据库提供查询服务,实现了对区块链中的业务数据的高效查询,从而保障了用户体验。

11. 陈姝,程双全,卢小明.日志数据库系统和同步方法:北京,CN106776894A[P].2017-05-31

[相关内容] 本发明提供一种日志数据库系统和同步方法,该系统包括同步配置单元、日志获取单元、数据同步单元和数据库执行单元。本发明将操作日志和数据分离,利用区块链技术在实现分布式存储的同时有效地保障安全性,同时可以配置不同类型数据库,无需改造节点。

12. 陈姝,程双全,卢小明.基于区块链网络的数据库写入方法及系统:北京,CN106611061A[P].2017-05-03

[相关内容] 本发明提供一种基于区块链网络的数据库写入方法及系统。本发明通过将数据库操作以数据库事务的方式在进行共识前存入数据库,并在完成共识后根据共识结果判断对该数据库事务进行提交或回退,从而实现了在共识过程保障了数据库的读写一致。

13. 徐忠,姚前.数字票据交易平台初步方案[J].中国金融,2016,(17):31-33.

[相关内容] 区块链用于票据的三种场景:可以解决链上数据真实性问题;采用区块链的分布式结构,可以消除信息不对称,实现票据价值传递的去中介化,进而消除



目前票据市场中介乱象；每张数字票据都是运行在区块链上、拥有独立的生命周期、通过智能合约编程的方式来实现的一段业务逻辑代码，利用此技术可以提高票据交易的效率，降低监管成本。如果在票据链中引入数字货币，便可实现自动实时的DVP 券款对付、监控资金流向等功能；而通过构造托管于智能合约的现金池，还可以创造出实时融资等新的业务场景。

14. 李礼辉.关于研发和试行数字票据的建议[J].金融电子化,2016,(06):7-10+6.

[相关内容] 建议抓紧研发和试行数字票据：由中国人民银行承担数字票据的统筹决策、组织研发和试行、推广工作职责；鼓励金融机构和企业参与数字票据研发和试行；现阶段先形成纸质票据、电子票据和数字票据共存的格局，通过技术手段逐步提升数字票据的市场占比；筹建数字票据交易所，承担数字票据技术核心职能；建立数字票据数据库，建立企业信用评级应用系统和票据产品评估应用系统；创新金融监管方式，利用新技术实现票据业务监管的全覆盖和硬控制。

15. 宋汉光.区块链在数字票据中的应用[J].中国金融,2018,(10):42-43.

[相关内容] 数字票据交易平台实验性生产系统使用 SDC (Smart Draft Chain, 数金链) 区块链技术，借助同态加密、零知识证明等密码学算法进行隐私保护，通过实用拜占庭容错协议 (PBFT) 进行共识，采用看穿机制提供数据监测。实验性生产系统包含票交所、银行、企业和监控四个子系统：票交所子系统负责对区块链进行管理和对数字票据业务进行监测；银行子系统具有数字票据的承兑签收、贴现签收、转贴现、托收清偿等业务功能；企业子系统具有数字票据的出票、承兑、背书、贴现、提示付款等业务功能；监控子系统实时监控区块链状态和业务发生情况。

16. 狄刚.区块链技术在数字票据场景的创新应用[J].中国金融家,2018,(05):69-71.

[相关内容] 基于对数字票据及其交易特点的分析，我们初步完成了一套依托于区块链技术、以智能合约为载体的数字票据技术基础设施。每张数字票据，都是一段包含票据业务逻辑的程序代码及对应的票据数据信息，这些运行在区块链上的数字票据拥有独立的生命周期和自维护的业务处理能力，可支持票据承兑、背书转让、贴现、转贴现、兑付等一系列核心业务类型，各种业务规则可通过智能合约编程的方式来实现。

详细内容见附件。



## 七、查新结论

综合分析检索的国内密切相关文献，并与委托项目的查新点进行对比如下：

关于提出区块链对数字货币发展的驱动力，设计区块链技术驱动下的我国数字货币的发行落地具体架构和监管思路，检索到的文献 1 是委托人课题组成员关于主流数字货币的交易模式和发展趋势分析；文献 2 和 3 探讨央行数字货币的实现模式，介绍了比特币等加密货币的机制，不涉及对区块链技术特征明确的优劣势分析，以及对中央银行数字货币的属性分析，也没有从货币功能角度分析数字货币究竟应该具有哪些特征。而委托查新项目分析了区块链技术对数字货币发展的驱动力，从区块链的技术特征分析数字货币设计的基本架构，从法定货币的基本功能角度设计法定数字货币的发行机制和发展路径；文献 4 主要从提高金融创新效率和风险侧重选择的角度分析广义数字货币核心机制的设计思路，侧重于数字货币演化的视角，而委托查新项目主要是从主权法定数字货币设计的角度讨论我国数字货币发展的路径，具体针对我国的数字货币架构和数字货币生态圈，从技术视角展开相关研究。

关于提出络谱区块链登记开放平台解决方案，检索到的文献 8-12 是委托人课题组的研究成果；文献 5 涉及一种组链方法，是联盟链上的技术；文献 6 和 7 涉及金融科技领域区块链技术的应用，从国家定性、技术瓶颈和展望等角度进行了理论分析，而委托查新项目提出络谱区块链登记开放平台，设计实现基于区块链的数字凭证注册、分配、转移、监管的完整方案，实现数字凭证的易用、防伪、易流通、可追溯，并设置监管机制，实现监管合规。

关于为数字票据、信用积分和数字货币的身份管理、安全验证等领域剔除联盟链和私有链管理方法，保障其在使用中的安全性和不可篡改性，检索到的文献 13 是中国人民银行数字货币研究所的二位负责人的指南性文章，姚前负责数字货币，徐忠负责数字票据；文献 14 是中国互联网金融协会李礼辉从技术研发角度借鉴 R3 联盟的相关平台对应给出的建议；文献 15 和 16 是人民银行票据司对货币流程的梳理，是国内最早探讨央行数字票据的实现模式的文献。上述文献主要分析票据交易存在的问题和票据真实性、交易合规性等方面的问题，提出了数字票据的必要性，强调了区块链技术对数字票据的适用性，而委托查新项目在数字票据方面主要进行了相关应用场景的技术开发，从实践应用的角度攻关区块链技术的日志、存储和查询等不可篡改和真实性问题，以应用为导向开发数字钱包、数字签名等数字资产关键性认证技术。

从综合分析比较可以看出：在国内公开发表的中文文献中，与本项目查新点完全相同的未见报道。

查新员 时莹（签字）：时莹

查新员职称：馆员

审核员 陈希南（签字）：陈希南

审核员职称：副研究馆员

（科技查新专用章）

2018年9月12日

208



## 八、查新员、审核员声明

1. 查新报告中所陈述的内容均以客观文献为依据;
2. 我们按照科技查新规范进行查新、文献分析和审核, 并做出上述查新结论;
3. 我们获取的报酬与本报告中的分析、意见和结论无关, 也与本报告使用无关;
4. 本报告仅用于申报中国通信学会科技进步奖。

查新员 (签字): 时宜

2018 年 9 月 12 日

审核员 (签字):

2018 年 9 月 12 日



## 九、附件清单

16 篇密切相关文献文摘。

## 十、备注

1. 西安交通大学科技查新工作站是教育部认定的科技查新单位;
2. 本查新报告无“科技查新专用章”及骑缝章无效;
3. 本查新报告无查新员和审核员签名无效;
4. 本查新报告涂改无效;
5. 本查新报告的检索结果及查新结论仅供参考;
6. 查新报告有效期六个月。

附件：16 篇密切相关文献文摘

[1]张驰,贺岩,呼延雅妮,董琦,柴旖嫻.当前主流数字货币交易模式分析及发展趋势研究[J].西部金融,2018,(03):50-54.

摘要: 基于密码学和现代网络技术的数字货币近几年来发展异常迅速,数字货币的种类持续增多,以比特币为代表的数字货币交易活跃,日本等部分国家也承认了数字货币的合法性。中国人民银行早在 2014 年就开始数字货币的研究,基于区块链和数字货币的数字票据交易平台于 2017 年成功测试运行,并正式挂牌成立了数字货币研究所。从趋势来看数字货币发展前景广阔,但就目前而言尚存在着线下交易应用不畅、存在隐私泄露风险,易成为洗钱、诈骗等犯罪工具,影响金融稳定与安全等诸多的问题与缺陷。本文通过研究以上问题的解决对策,对我国发展数字货币进行展望。

[2]周永林.央行数字货币及其实现模式探讨[J].金融电子化,2016,(09):35-37.

摘要: <正>人们把比特币等密码货币称为“数字货币”(Digital Currency),认为这类密码货币建立在一种“去中心化”的资产注册和清算机制基础之上,提供了全新的资产(包括货币)持有和交换方式。其主要特点体现在以下几个方面,一是采用以加密算法为核心的区块链或分布式总账技术,使素不相识的人们可以在网络上建立信任机制,使“点对点”直接交易成为可能。二是在发行方面,没有一个中心化的机构(如央行或私营机构)控制和管理虚拟货币发行,任何参与者都可以通过自己的努力(如比特币中的“挖矿”)获得虚拟货币,虚拟货币的发行总量一般由算法自动控制在一定范围(比特币的总量控制在 2 1 0 0 万个以内)。三是这类虚拟货币没有任何资产担保,不和任何资产挂钩,在某些人看来是没有什么“内在价值”的纯粹数字创造物,但却可以和法定货币(如美元)双向兑换,可以用于购买商品和服务。四是在转账支付等交易环节,不需要借助银行等中间机构,可以实现“点对点”(P2P)直接交易。

[3]王永红.数字货币技术实现框架构想[J].中国金融,2016,(08):14-16.

摘要: 随着互联网技术的飞速发展,数字货币受到越来越多的关注,并逐步进入了央行的视野。2016 年 1 月 20 日,中国人民银行在北京举行了数字货币研讨会,正式公开表示要积极吸收国内外数字货币研究的重要成果和实践经验,做好关键技术攻关,争取早日推出央行发行的数字货币。本期我们特约请央行、商业银行和互联网业界的资深专家,就建立在区块链技术上的数字货币应用和前景展开讨论。

[4]庄雷,赵成国.区块链技术创新下数字货币的演化研究:理论与框架[J].经济学家,2017,(05):76-83.

摘要: 鉴于区块链技术的数字货币探索,比较分析数字货币演化历程和动因,从货币价值、发行主体、数量调节三大基本问题总结数字货币的本质、属性、锚定、信用创造四大机理。基于金融创新效率和风险侧重选择不同,分析数字货币核心机制的设计思路、实践探索和未来前景,从二元间接信用创造的融合式到一元直接信用创造的重构式来实现数字货币信用模式的应用调整。结合数字货币的风险理论和监管原则,提出从单维平面到多维立体的信用风险评价体系来实现数字货币体系的有效监管,共享数字经济时代信用人格化的普惠效应。

[5]梁庚,左春,李春晓,陈胜,蒋步云,杜乐乐.基于联盟链的区块链组链方法及区块链系统:北京,CN108280646A[P].2018-07-13

摘要: 本发明提供一种基于联盟链的区块链组链方法及区块链系统。所述方法包括: 对联盟链中的所有节点按照区域进行分区; 各区域内的节点在本区域内进行背书和出块,形成支链; 各区域形成的支链向主链提交锚定请求,所述锚定请求携带的信息包括: 请求时间、当前支链编号及当前支链的哈希值; 在主链节点接收到支链的锚定请求之后,验核支链提交的签名; 在验核完成之



后,主链节点按照共识规则完成背书和出块,完成组链。本发明通过对节点进行分区,实行分区背书,分区出块,能够极大的降低共识成本,提高系统吞吐量,减少系统响应时间。

[6]李文红,蒋则沈.分布式账户、区块链和数字货币的发展与监管研究[J].金融监管研究,2018,(06):1-12.

摘要:近年来,金融科技在全球范围内迅速兴起,以区块链为代表的分布式账户被认为是最有发展潜力的金融科技技术。作为其应用形式之一,比特币等私人数字货币快速发展,但也积累了潜在风险,引起各方广泛关注。国际组织、各国央行和监管机构均高度重视、密切跟踪研究金融科技的发展应用及其对金融稳定的影响,目前总体认为,分布式账户、区块链技术尚处于起步阶段,能否实现大规模推广并产生变革性影响,还有待观察。数字货币按照发行主体可分为私人 and 法定数字货币。对于比特币等私人数字货币,各国普遍认为其不是法定货币,并持续向投资者提示相关交易活动风险。对与私人数字货币相关的金融业务,各国要么严格限制或禁止,要么按照业务属性纳入现行监管框架,主要涉及以数字货币为基础资产的衍生品交易、为数字货币交易提供支付服务、数字货币交易平台等。此外,各国普遍认定首次代币发行(ICO)为一种公开融资活动,多数国家将其界定为证券发行行为。对于法定数字货币,各国均予以密切关注、积极跟踪研究,但多数国家尚未提出实质性的具体发行计划。本文认为,针对金融科技的快速发展,监管者应遵循"技术中立"原则,按照金融业务本质实施监管,维护市场公平竞争;及时对金融科技/互联网金融业务进行"穿透定性",防止冒用"技术"名义违法违规开展金融业务;加强对金融机构与科技企业合作的监管,强化对信息科技风险、外包风险和其他操作风险的管控;同时,持续加强跟踪研究和监测分析,做好专业知识、人才队伍、政策措施等方面储备。

[7]江海峰.区块链技术在金融行业的应用模式研究[D].导师:张小茜;顾清良.浙江大学,2018.

摘要:区块链技术起源于数字货币构想,但当前的应用研究已经延伸至金融等多个行业领域,受到多国政府、金融企业和科技巨头的关注。作为一种新兴的分布式数据库协议,区块链运用密码学技术、加时间戳的链式数据结构和分布式共识机制等技术,实现了去中心化,不可篡改、易于追溯和可编程智能合约等优势,从而为解决传统中心化机构潜在的中介成本较高和中心存储不安全等问题提供了可能的解决方案,具有广阔的应用前景。本文从区块链系统的基础模型分析入手,以比特币和以太坊区块链系统为例,自下而上将模型分为数据层,区块层,网络层,共识和激励层以及应用层五部分,并分别对于各层主要应用的基础技术和运行机制进行介绍,这其中重要的部分包括链式区块结构,哈希算法和 Merkle 树,非对称加密,P2P 网络,共识激励机制和智能合约等。目前,区块链技术仍面临诸多技术瓶颈阻碍其大规模应用,包括效率低下,存储成本高昂,共识机制资源浪费和隐私安全等问题。本文针对每一问题分析了目前可能的解决方案,例如针对效率问题的线下支付通道方案,针对资源浪费问题的权益证明机制和针对存储成本高昂的分片方案等。总结区块链技术的优势和挑战,本文提出其系统设计思路本质上是在可靠性和效率的平衡中选择性地放弃了效率这一面,从而当应用于大规模商业化场景中时将会面临诸多挑战。区块链技术的优势使其有望解决金融行业目前存在的部分痛点,在许多细分领域有着实践应用的可能。本文提出区块链技术有望在中低频交易、高信任要求、对账与中介成本较高的应用场景中首先落地,基于此以票据业务、跨境支付业务和 ABS 业务为主要关注点,并结合实例分析区块链技术对传统模式的改善情况、目前面临的挑战与应用建议。整体上看,区块链技术在金融领域的应用仍处于初级阶段,仍面临法律监管、金融市场制度建设和商业运营层面的问题和挑战。对此,本文也提出了加强行业应用标准制定和明确政策支持的建议。

[8]张波波,张一锋.一种基于区块链的数字身份验证的方法、装置和系统:浙



江,CN107888382A[P].2018-04-06

摘要:本申请提供的基于区块链的数字身份验证的方法,包括:接收到应用方证书生成指令时,获取第一随机数,使得应用服务器利用第一随机数生成应用方证书;获取应用方证书和安全因子,根据应用方根证书中的公钥验证应用方证书是否有效;若是,则利用安全因子生成钱包证书;接收到输入的口令后,获取第二随机数,根据第二随机数和口令计算出摘要值,并验证摘要值是否正确;若是,对交易信息和安全因子利用钱包服务中的私钥进行签名,使得应用服务器利用签名验证钱包证书是否合法且是否有效。通过采用随机数,签名,各种证书的方式实现了区块链间高安全性的数字身份认证。本申请还提供了基于区块链的数字身份验证的装置和系统,具有上述有益效果。

[9] 张波波,张一锋.一种基于金融 IC 卡端的数字货币交易方法及系统:浙江,CN107862607A[P].2018-03-30

摘要:本发明公开了一种基于金融 IC 卡端的数字货币交易方法,包括:终端向 IC 卡端发送钱包应用选择指令;终端接收 IC 卡端发送的交易数据的发送请求;终端通过发送请求判断是否为数字货币交易;如果是,终端向 IC 卡端发送交易数据,以便 IC 卡端判断交易类型并生成验证数据;其中,交易数据包括应用扩展标识以及终端交易属性;终端接收 IC 卡端发送的验证数据;终端对接收到的验证数据进行验证;验证通过后,终端进行交易过程。该方法能够实现钱包应用同时支持数字货币与电子货币交易,并确保数字货币交易流程的高效性、安全性;本发明还公开了基于金融 IC 卡端的数字货币交易装置及系统,具有上述有益效果。

[10] 李刘海,陈姝,卢小明.基于区块链的业务数据同步方法及系统、数据库系统:北京,CN106874393A[P].2017-06-20

摘要:本发明提供一种基于区块链的业务数据同步方法及系统、数据库系统,该方法包括:提供业务合约接口供调用以编辑业务数据;根据所述业务数据生成交易信息并提交交易;将所述交易信息发送至当前区块链网络中参与共识;接收返回的共识结果信息,若所述交易信息通过共识,则将所述交易信息实时同步至预配置的外部数据库,以供所述外部数据库同步所述业务数据并提供业务数据查询服务。本发明通过将业务数据同步至外部数据库中,由外部数据库提供查询服务,实现了对区块链中的业务数据的高效查询,从而保障了用户体验。

[11] 陈姝,程双全,卢小明.日志数据库系统和同步方法:北京,CN106776894A[P].2017-05-31

摘要:本发明提供一种日志数据库系统和同步方法,该系统包括同步配置单元、日志获取单元、数据同步单元和数据库执行单元。同步配置单元配置用于获取待同步的数据对象名称以配置同步名称列表。日志获取单元配置用于进行交易,生成交易信息并参与共识,将通过共识的交易信息存入本地区块链。其中,交易信息包括数据库操作日志。数据同步单元配置用于根据同步名称列表在本地区块链中查找对应的数据库操作日志,根据查找到的数据库操作日志确定数据同步操作。数据库执行单元配置用于对预定的数据库执行数据同步操作。本发明将操作日志和数据分离,利用区块链技术在实现分布式存储的同时有效地保障安全性,同时可以配置不同类型数据库,无需改造节点。

[12] 陈姝,程双全,卢小明.基于区块链网络的数据库写入方法及系统:北京,CN106611061A[P].2017-05-03

摘要:本发明提供一种基于区块链网络的数据库写入方法及系统,该方法包括:接收包括数据库操作的交易信息;根据所述数据库操作创建数据库事务,并将所述数据库事务存入本地数据库;将所述交易信息发送至当前区块链网络中参与共识;接收返回的共识结果信息并判断所述交易信息



是否通过共识:是,则在所述本地数据库中提交所述数据库事务;否,则在所述本地数据库中回退所述数据库事务。本发明通过将数据库操作以数据库事务的方式在进行共识前存入数据库,并在完成共识后根据共识结果判断对该数据库事务进行提交或回退,从而实现了在共识过程保障了数据库的读写一致。

[13]徐忠,姚前.数字票据交易平台初步方案[J].中国金融,2016,(17):31-33.

摘要: <正>票据作为一个集交易、支付、清算、信用等诸多金融属性于一身的非标金融资产,市场规模大、参与方众多、业务复杂,是区块链的一个极佳应用场景。目前票据业务主要存在三方面问题:一是票据的真实性,市场中存在假票、克隆票、刑事票等伪造假冒票据;二是划款的即时性,即票据到期后承兑人未及时将相关款项划入持票人账户;三是违规交易,即票据交易主体或者中介机构,存在一票多卖、清单交易、过桥销规模、出租账户等违规行为。与此相对应,区块链用于票据场景也主要有三种。首先,可以解决链上数据真实性问题。从票据发行即对全网所有业务参与方广播,当检验数字票据信息是否被转让或者篡改时,区块链可以提供无可争议的一致性证明。其次,采用区块链的分布式结构,可以消除信息不对称,实现票据价值传递的去中介化,进而消除目前票据市场中介乱象。最后,每张数字票据都是运行在区块链上、拥有独立的生命周期、通过智能合约编程的方式来实现的一段业务逻辑代

码,利用此技术可以提高票据交易的效率,降低监管成本。如果在票据链中引入数字货币,便可实现自动实时的 DVP 券款对付、监控资金流向等功能;而通过构造托管于智能合约的现金池,还可以创造出实时融资等新的业务场景。

[14]李礼辉.关于研发和试行数字票据的建议[J].金融电子化,2016,(06):7-10+6.

摘要: <正>当前,区块链已经得到金融机构的关注。国际货币基金组织(IMF)在首份数字货币报告中指出区块链"具有改变金融的潜力",英国政府发行的《分布式账本技术:超越区块链》提出将优先在传统金融行业应用区块链技术,英国央行已在考虑发行数字货币,纳斯达克借助区块链建立私人股权交易平台 Linq,花旗、汇丰、富国等银行加入 R3 区块链联盟并设置自己的研究实验室,德勤借助基于区块链的 Rubix 平台提供咨询和审计。票据是便捷的支付结算工具和融资工具,也是重要的货币政策工具。2009 年,我国推出电子票据,纸质票据与电子票据并行。我国票据业务发展迅速,规模巨大。现行票据的主要缺陷,在于难以有效管控和防范风险。票据造假,“一票多卖”,票据变成融资套利工具和规避金融监管的“掩体”。票据业务监管效率低、成本高。国务院《推进普惠金融发展规划》明确指出:“金融基础设施是提高金融机构运行效率和服务质量的重要支柱和平台,有助于改善普惠金融发展环境,促进金融资源均衡分布,引导各类金融服务主体开展普惠金融服务。”应用区块链技术构建全新的数字票据,可能形成新的技术优势:成本较低,风险较小;数据完整,信息透明;智能化管理和监控。这将提升金融基础设施的服务功能,有利于推进普惠金融发展。建议抓紧研发和试行数字票据:由中国人民银行承担数字票据的统筹决策、组织研发和试行、推广工作职责;鼓励金融机构和企业参与数字票据研发和试行;现阶段先形成纸质票据、电子票据和数字票据共存的格局,通过技术手段逐步提升数字票据的市场占比;筹建数字票据交易所,承担数字票据技术核心职能;建立数字票据数据库,建立企业信用评级应用系统和票据产品评估应用系统;创新金融监管方式,利用新技术实现票据业务监管的全覆盖和硬控制。

[15]宋汉光.区块链在数字票据中的应用[J].中国金融,2018,(10):42-43.

摘要: <正>票据市场是中国发展最早的金融子市场之一。经过多年的建设和发展,作为有效连接货币市场和实体经济的重要通道,票据市场已成为金融市场体系的重要组成部分。上海票据交易所(以下简称“票交所”)是经国务院同意设立、中国人民银行指定的全国性票据报价交易、托管登

记、清算结算、信息查询和票据风险监测平台,是中央银行实施货币政策再贴现和公开市场操作的重要金融基础设施。自成立以来,票交所始终聚力前沿科技,以科技创新带动业务创新,以科技进步推动票据市场提质增效,努力推动票据市场更好的发展。

[16]狄刚.区块链技术在数字票据场景的创新应用[J].中国金融家,2018,(05):69-71.

摘要:<正>区块链技术是一种以分布式为特征,以密码学为基础,提供数据可信和业务可信的全新的金融基础设施的底层核心技术。该技术可以为金融业务提供无需第三方中介的业务流程公开、信息证明公示以及资产流转记录可查的高效的技术支持,显著降低金融业务复杂度和成本,提升共享信息的便利性,营造多方互信的协作机制,重构金融基础设施形态,有效解决金融行业数据孤岛和数据寡头的问题,促进金融业务创新。