國際金融论壇
INTERNATIONAL FINANCE FORUM
Since 2003

国际金融论坛 (IFF)

International Finance Forum (IFF)

全球数字货币发展报告

REPORT ON THE DEVELOPMENT OF GLOBAL DIGITAL CURRENCIES

2024

IFF20
INTERNATIONAL
FINANCE FORUM

新资本 新价值 新世界

NEW CAPITAL NEW VALUE NEW WORLD

全球金融F20 金融服务世界

Global Finance 20 (F20) Finance Serves the World

关于 IFF

国际金融论坛（IFF）是独立的、非营利、非政府国际组织，2003 年 10 月由 G20 国家以及联合国、世界银行、国际货币基金组织等相关机构及领导人共同发起成立，是全球金融领域高级别常设对话机制和多边合作机构，被誉为全球金融领域的“F20（Finance 20）”。

国际金融论坛（IFF）的目标是通过国际化、市场化、专业化的运营机制，建立全球经济、金融和公共政策领域战略对话、交流合作、实践创新、学术研究和人才培育平台，推动金融服务世界，促进全面可持续发展。

宗旨

自 2003 年创立以来，国际金融论坛（IFF）秉持和遵循“全面可持续发展 — 新资本、新价值、新世界”的宗旨，致力于打造具有战略远见、国际一流的学术智库和多边对话平台。

目标

国际金融论坛（IFF）通过公开、公平、公正的运行机制，确保独立、客观、前瞻和包容性，以促进国际金融合作与交流；通过对全球金融领域的深入研究，促进中国经济、世界经济全面可持续发展，实现以下目标：

1. 全球金融战略对话平台；
2. 全球金融交流合作平台；
3. 全球金融创新实践平台；
4. 全球金融研究智库平台；
5. 全球金融人才培养平台。

国際金融論壇
INTERNATIONAL
FINANCE FORUM

IFF2024 年
《全球数字货币发展报告》
www.iff.org.cn
www.ifforum.org

主办单位 / Host
国际金融论坛（IFF）
International Finance Forum (IFF)
UIA International Organization ID: AA2980

联合主席 / Co-chair
韩升洙 Han Seung-soo
珍妮·希普利 Jenny Shipley
周小川 ZHOU Xiaochuan

理事会 / IFF Board of Directors
埃德蒙·阿尔方戴利 阿罗约 苏丹·本·纳赛尔·苏瓦迪
Edmond Alphandéry, Gloria Macapagal Arroyo,Sultan Bin Nasser Al-Suwaidi,
陈茂波 洛朗·法比尤斯 史蒂芬·格罗夫 韩升洙
Paul Chan Mo-po, Laurent Fabius,Stephen P. Groff, Han Seung-soo,
戴青丽 梁锦松 李彤 林建海 约翰·利普斯基
Deborah M. Lehr, Antony Leung, LI Tong, LIN Jianhai, John Lipsky,
布莱恩·佩斯科 冯慧兰 珍妮·希普利 穆罕默德·希姆谢克
Bryan Pascoe, Mari Elka Pangestu, Jenny Shipley, Mehmet Simsek,
多梅尼科·西尼斯卡尔科 叶兆佳 萧志伟 中尾武彦
Domenico Siniscalco, Ip Sio Kai, Sio Chi-wai, Takehiko Nakao,
弗兰克·里斯伯曼 格里·赖斯 悉达多·蒂瓦里 让·克洛德·特里谢
Frank Rijsberman, Gerry Rice, Siddharth Tiwari, Jean-Claude Trichet,
扎法尔·乌丁·马赫默德维拉·松圭 埃里克·索尔海姆
Zafar Uddin Mahmood, Vera Songwe, Erik Solheim,
梁维特 韦浩思 大卫·赖特
Leong Vai Tac, Jose Vinals, Sir David Wright,
魏伯昂 易小准 容永祺 祝宪
Axel Weber, YI Xiaozhun,Samuel Yung Wing-ki, ZHU Xian,
周汉民 周延礼 张继中
ZHOU Hanmin, ZHOU Yanli, ZHANG Jizhong,
凯拉特·克林贝托夫 埃内斯托·塞迪略
Kairat Kelimbetov, Ernesto Zedillo,
安雅山 马志刚 让·克洛德·特里谢
Ambassador Yasser Elnaggar, MA Zhigang, Jean-Claude Trichet,

顾问委员会联合主席 / Co-Chair of Advisory Committee
约翰·利普斯基 让·克洛德·特里谢
John Lipsky, Jean-Claude Trichet

学术委员会联合主席 / Co-Chairs of Advisory Committee
安顿·马斯凯特里 赵忠秀
Anton Muscatelli, ZHAO Zhongxiu,

编委会 / Editorial Board
张继中 祝宪 林建海 宋敏
ZHANG Jizhong, ZHU Xian, LIN Jianhai, SONG Min

编辑部 / Editorial Department
庄珏 周鑫 龚思铭
Joanna Zhuang, ZHOU Xin, GONG Siming

撰稿人 / Authors
宋敏 徐瑞峰
SONG Min, XU Ruifeng

地址 / Address
中国北京市东城区东长安街 1 号东方广场 W3 座
Oriental Plaza W3, Dongcheng District, Beijing, China
邮编 / Post Code 100738
Email / info@iff.org.cn

版权声明 / Copyright Statement
本刊内容由国际金融论坛（IFF）独家拥有，未经许可， 不得转载或摘抄。
The content of this publication is an exclusive property of the IFF, and may not be reproduced or excerpted without permission

前言

在数字经济时代，数字货币的意义深远且多维，体现了其对全球金融体系、经济运作及社会生活的深刻影响。在这个伟大的时代，数字货币的全球发展正以前所未有的速度推进，标志着金融体系的一次深刻变革。数字货币不仅是技术革新的产物，也是全球经济数字化进程的重要驱动力，它对传统金融模式、货币政策、支付系统乃至国家主权货币体系产生了深远的影响。

因此，分析和总结数字货币的发展具有极其重要的意义。一方面，它帮助我们理解数字货币如何重新定义货币的本质，挑战传统的金融架构，并为全球经济带来新的机遇和挑战；另一方面，它为政策制定者、金融机构和投资者提供了宝贵的洞察，帮助他们应对技术进步带来的风险，制定出具有前瞻性的战略，以实现经济增长和金融稳定。通过对数字货币全球发展趋势的深入分析，我们不仅能够把握这一时代脉搏，还能为未来的金融创新和全球经济协调提供理论支持和实践指导。

宋敏
国际金融论坛（IFF）学术委员
武汉大学经济与管理学院原院长

Contents

目 录

01 前言

03 目录

05 第一章 全球数字货币产业的发展动能分析

1.1 数字货币产业发展的缘起 06

1.2 全球数字货币产业发展的驱动因素 08

1.3 小结 10

11 第二章 全球数字货币发展概览

2.1 全球私人数字货币产业发展现状的国别比较分析 12

2.1.1 主流原生代币的国别发展现状分析 12

2.1.2 稳定币的国别发展现状分析 18

2.1.3 平台币的国别发展现状分析 21

2.2 全球央行数字货币产业发展现状的国别比较分析 22

2.2.1 巴哈马沙元 22

2.2.2 尼日利亚电子奈拉 23

2.2.3 加拿大 Jasper 项目 23

2.2.4 欧洲央行和日本央行 Stella 项目 24

2.2.5 数字人民币 24

2.3 全球数字货币与各类新兴数字技术的融合发展新趋势 25

2.3.1 数字货币与智能合约开发 25

2.3.2 数字货币与元宇宙技术 26

2.3.3 数字货币与 Web3.0 网络技术 26

2.3.4 数字货币与人工智能技术 27

2.3.5 数字货币与资产数字化 28

2.4 数字货币的信用基础 29

2.5 小结 30

31 第三章 全球数字货币对经济体系的影响

3.1 数字货币对金融体系的影响 32
3.1.1 私人数字货币对货币国际化的影响 32
3.1.2 央行数字货币对货币国际化的影响及其国别发展经验 33
3.2 数字货币对居民消费的影响 33
3.3 数字货币对跨境贸易结算的影响 35
3.4 小结 36

37 第四章 全球数字货币产业发展的风险与挑战

4.1 数字货币的技术安全与隐私泄露风险 38
4.2 数字货币的市场波动与投机风险 39
4.3 数字货币的法律合规风险与监管不确定性 39
4.4 数字货币的可拓展性风险 39
4.5 小结 40

41 第五章 全球数字货币监管制度的国别比较分析

5.1 数字货币的司法界定 42
5.2 数字货币的非法交易监管 44
5.3 世界各国对比特币的监管制度比较 45
5.4 小结 46

47 总结

展望与政策建议 48

50 参考文献 50

第一章
全球数字货币产业的发展动能分析

第一章
全球数字货币产业的发展动能分析

1.1 数字货币产业发展的缘起

随着电子计算机的发明和信息技术的飞速发展，自 20 世纪 50 年代以来，数字技术逐渐开始以前所未有的广度和深度嵌入金融行业。1958 年美洲银行首次将电子计算机用于储蓄业务，而 1973 年成立的 SWIFT 在今天已成为全球最大的银行间电子结算网络。1980 年代以来，为满足民众逐渐增长的零售支付需求，以及基于**保护交易者隐私的需要和对现代货币体系的反思**，催生了数字货币创新研究的不断发展。而**计算机科学在密码学领域的突破，进一步催生了数字货币的发展**。

数字货币的历史发展和技术进步并不是一蹴而就的，而是**历经多次技术迭代**。1982 年，大卫·乔姆（David Chaum）提出利用盲签名技术保护用户的隐私权，基于其首次提出的数字现金（Digital Cash）概念而开发了世界上首个数字货币 DigiCash。1996 年，道格拉斯·杰克逊创立数字货币 e-gold，它与黄金 1：1 兑换，而黄金储备的准备金率为 100%。1998 年，戴伟发明 B-money，该数字货币项目在历史上首次使用了分布式记账技术。2005 年，尼克·萨博（Nick Szabo）提出 Bitgold，首次发明使用工作量证明共识机制的数字货币，从而使得保存在不同节点中数字货币的账本能够保持一致，还解决了数字货币的发行问题。2009 年，一个网名为中本聪（Satoshi Nakamoto）的网友向“ 加密货币邮件组 ”成员发送比特币白皮书，正式提出了比特币的概念，标志着基于去中心化区块链技术的数字货币技术的完善，这种数字货币也被称为加密货币，因为它没有中央服务器，也没有储备的有形资产，而是基于密码学原理确认货币所有权及确认交易。由于使用区块链技术进行分布式记账，因此也没有任何政府或个人能够关闭它们。2009 年 1 月 3 日，中本聪在芬兰的一台小型服务器挖出了比特币的首个区块，并获得 50 个比特币奖励，标志着比特币的创世区块诞生。

比特币诞生后，数字货币的发展则逐渐经历了四个发展阶段。在**初期探索阶段（2009–2013 年）**，比特币的应用主要**局限于技术爱好者和金融专业人士**，也存在着一些技术问题和法律风险。在比特币上线运行初期，比特币挖矿十分容易，使用笔记本电脑即可获得比特币奖励，因此其真实的交易价格较低。2009 年 10 月 12 日，比特币论坛中一名自称“ New Liberty Standard ”的用户通过 PayPal 向比特币开发者 Sirius 支付 5.0 美元，获得 5,050 个比特币。这是历史上第一笔有记录的比特币兑换美金交易。在 2010 年 5 月 22 日的一个历史性时刻，一个程序员使用 10,000 个比特币买了两个披萨，这一天也被定为比特币披萨日，以纪念比特币首次被用于购买现实世界中的商品，而自此之后，越来越多的数字货币交易所开始出现，投资者开始使用各种法定货币购买比特币。2010 年 12 月 13 日，中本聪最后一次登录比特币论坛，从此，再未现身。而自此至今，尚未有任何人发现中本聪的真实身份，这也是比特币和区块链技术去中心化精神的体现。2011 年 6 月 19 日，黑客通过盗取数据库的方式获得比特币交易所 Mt.Gox 管理员权限，并制造虚假卖单，将比特币价格压至 0.01 美元，Mt.Gox 和其它主流交易所宣布暂停交易 7 天。随后，数据库再次泄露，黑客通过数据库信息攻破 MyBitcoin 线上钱包，从 600 多个钱包地址中盗取了 4,019 个比特币。这一事件沉重打击了投资者对比特币安全性的信心，也引发了比特币价格的下跌。2013 年 10 月 1 日，美国联邦调查局在圣弗朗西斯科公共图书馆抓获“ 丝绸之路 ”网站的创始人，账户名“ DreadPirate Roberts ”的操纵者 Ross Ulbricht。Ross 被指控毒品交易、洗钱、黑客入侵等数项罪名。“ 丝绸之路 ”持有的接近 3 万枚比特币被缴获，另外 Ross 个人持有的 14.4 万枚比特币也被没收。

在**快速发展阶段（2013–2017 年），比特币的价格飙升**，引起了更广泛的关注。越来越多的人开始接受数字货币，并涌现出了众多的新型数字货币和相关技术，如以太坊、莱特币、区块链等。同时，数字货币在一些国家得到了一定的合法地位。2013 年 11 月 20 日，时任中国人民银行副行长易纲在一次活动上公开表示“ 比特币有启发性 ”、“ 将保持长期关注 ”，并认为“ 投资者有参与比特币交易的自由 ”。比特币在中国的热度进一步升高，每日交易量达到比特币交易所 Mt.Gox 的两倍。但随后在 2013 年 12 月 5 日，中国政府宣布比特币非货币，并禁止所有金融机构参与比特币业务，导致全球比特币价格大跌。2014 年 4 月 10 日，中国人民银行更进一步要求部分中国银行机构在 4 月 15 日前关闭部分比特币交易所的银行账户。在趋严的政策环境下，部分交易所通过海外银行、加密券系统等方式继续运营，但总体上，中国境内的数字货币交易量大幅减少。不过，在 2015 年 10 月 22 日，欧盟司法部宣布，在欧盟内部，比特币和其它加密货币的交易无需缴纳“ 增值税 ”（VAT），并认为数字货币是“ 货币 ”而非“ 商品 ”。2017 年 4 月 1 日，日本立法系统也通过法案，将日本数字货币交易所纳入 AML 和 KYC 监管，并承认比特币为一种合法的预付款工具。而且，在比特币越来越受到投资者和金融机构关注的背景下，越来越多的企业开始接受比特币付款或捐赠。2014 年 7 月 30 日，维基百科宣布开始接受比特币捐赠。2014 年 9 月 8 日，Paypal 子公司 Braintree 宣布和 Coinbase 合作，为用户提供比特币支付服务。2014 年 12 月 11 日，微软宣布将在 Windows 和 Xbox 数字商店接受比特币付款。

随着比特币暴涨和公众对其的关注度逐年增高，个体网民越来越难以独立挖出比特币。在 2010 年 8 月 16 日，挖矿难度仅为 511T。至 2021 年 5 月 21 日，挖矿难度增长至最高点 2.5×10^13T，共增长 490 亿倍，比特币挖矿活动也从早期的个人电脑挖矿转向 GPU 挖矿，甚至集中化的矿池挖矿。在 2014 年 6 月 13 日，矿池 GHash.io 的算力甚至一度占比达到 51%。不过，GHash.io 随后即发表声明称，“ 永远不会参与 51% 攻击 ”，并且承诺将通过引导矿工去其它矿池的方式，将算力占比降到 39.99% 以下。不过，随着比特币节点和交易者的不断增长，比特币区块扩容的问题也逐渐提上日程，最终，由于扩容支持方和反对方未能达成一致，2017 年 8 月 1 日，扩容争议导致比特币出现首次硬分叉，“ Segwit ”优化方案的支持者继续支持比特币，而代表更激进扩容方案的“ 大区块 ”的支持者则创造出比特币现金（BCH），并定向对原比特币持有账户进行 1：1 空投。

在随后的**泡沫破裂和监管调控阶段（2017–2020 年），数字货币市场经历了一次大规模的泡沫破裂**，比特币价格从 2017 年底的近 2 万美元暴跌至 2018 年底的约 3 千美元。同时，越来越多的国家开始对数字货币进行监管调控，以保护投资者和维护金融稳定。其中，在 2017 年 9 月 3 日，中国监管机构责令禁止其境内一切形式的 ICO（首次代币发行）。2017 年 9 月 14 日，中国监管机构责令所有境内数字货币交易所限期关闭，并停止新用户注册。至此，中国境内的各数字货币交易所，开始逐渐转移至境外。此后，在 2018 年，Facebook、Google 和 Twitter 等美国大型科技公司相继宣布禁止在其平台中投放数字货币的广告。2018 年 6 月 11 日，美国商品期货委员会（CFTC）更进一步向 Bitstamp、Kraken、ItBit 和 Coinbase 四家数字货币交易所发出传票，要求其就涉嫌市场价格操纵做出解释。不过，**在私人数字货币监管从严的背景下，数字货币和区块链的技术本身正在受到各国政府的重视**，各国政府也开始逐渐探索研发基于本国法定货币的央行数字货币。2017 年 1 月 29 日，中国央行正式成立数字货币研究所。2019 年底，中国央行“ 数字人民币 ”第一批试点城市公布，包括深圳、苏州、成都、北京、张家口等城市和雄安新区。

最后，**在恢复和发展阶段（2020 年至今），数字货币市场逐渐恢复，比特币价格再次突破历史高位**。与此同时，越来越多的**金融机构和企业开始接受数字货币**，并探索数字货币与传统金融体系的融合。此外，更多国家也开始进一步**探索发行央行数字货币**（CBDC）的可能性。尤其是新冠疫情发生以来，元宇宙和 NFT 数字藏品的爆火使得区块链概念重新步入大众视野，并进一步推动各类**新型数字货币和智能合约发展**。

1.2 全球数字货币产业发展的驱动因素

从**数字货币发展的背景**考虑其产业发展的驱动因素。首先是近年来**数字技术的进步**，尤其是密码学领域的技术突破，使得实现一种完全去中心化、没有任何中介机构管理其发行的数字货币在技术上成为可能，并通过比特币的发展为人们所熟悉，能够同时满足人们的匿名交易需求和跨境支付需求。其次，**新冠疫情的全球大流行**改变了全球经济体系的整体结构，深度影响了人们的消费习惯和日常生活方式，疫情下的各种特殊场景提升了客户需求与模式创新的适配程度，催生数字经济进一步跳跃式发展，让数字金融、数字货币以前所未有的广度和深度嵌入人们的生活中。最后，**全球化背景下生产方式的变革**，特别是新一代信息技术的发展，价值链上中高端产品供应方可通过大数据、云计算和智能技术向价值链中下游进行渗透，价值链上的数据安全也越来越重要，产业链上互联网与金融资本垄断加剧，数字技术在全球价值链中的重要性也越来越重要，数字货币作为其中的重要组成部分，也将发挥越来越重要的作用。

本报告还将从数字货币的**功能应用上分析其发展的驱动因素**。具体而言，**首先，数字货币可以用于在线支付和跨境汇款**，不仅能够缩短交易时间，还能够降低交易成本。以数字人民币为代表的央行数字货币能够实现即时到账，不仅支付体验感不亚于支付宝、微信支付，且使得用户能够直接使用央行背书的 M0 现金进行支付，绕过了金融中介机构。比特币、比特现金等私人数字货币则支付速度各异，其中比特币交易的确认速度较慢，一般需多个区块确认后方可确认交易，一般需要数十分钟，但比特币具有更高的隐私保护和最广泛的接受度，是世界范围内接受度最高的私人数字货币，且也能够通过 Lightning Network（闪电网络）等新技术实现实时到账，比特现金、莱特币等则在继续坚持 POW 共识机制的基础上，支付速度相较于比特币更快。基于 DPOS(Delegated Proof of Stake，代理权益证明) 的波场币、基于 POH（Proof of History，历史证明）的 SOLANA 等新型区块链架构数字货币则支付速度更快。其中，Solana 的每秒传输速度（TPS）为 65000，是目前活跃的公链之中传输速度最快的。

其次，**数字货币还可用于投资**，比特币通缩的性质使其价格不断上涨，各类新型数字货币的价格也经常出现数百或数千倍的上涨，从而吸引了大量投资者的关注，数字货币不同于其他所有传统投资品的特性也使其能够作为投资组合中的风险对冲工具之一发挥作用。此外，基于比特币、以太坊等数字货币衍生的各类数字资产期货、期权也可基于智能合约程序实现去中心化交易。而且，USDT 等各类稳定币的出现也使得投资者能够在外汇管制的情形下无限制跨境购买美元稳定币、欧元稳定币等，实现外币投资组合的构建。此外，利用比特币、USDT 等私人数字货币，用户还可绕过相关国家的金融监管，实现美股投资的出金入金。

此外，**数字货币还可以用于购买商品和服务**，特别是满足交易者匿名化、便利化支付的需要。用户使用数字人民币购买美团外卖、京东等数字平台的商品均可获得一定额度的优惠，并可在绕过阿里巴巴的支付宝、腾讯的微信支付等第三方私营企业的前提下，直接通过数字人民币 M0 与中央银行发生联系，实现数字支付。此外，数字货币还可实现微信支付、支付宝等第三方支付工具难以完成的商品购买。例如，美国的 Spotify、Netflix 等流媒体服务商基于版权保护因素，不支持中国大陆用户访问，因此不允许使用微信支付、支付宝等中国支付工具购买会员，从而在其平台上观看电影或听音乐。而使用比特币、USDT 等私人数字货币后，中国大陆用户即可直接向美国用户跨境购买并合租上述账号，享受上述流媒体服务。使用以太币，全球范围内任何用户均可随时在区块链中交易 NFT 数字藏品、Web3.0 中的 ENS 域名、元宇宙 Decentraland 中的数字房产等各类数字资产。

而且，**数字货币还能够作为 Web3.0 世界的基础设施**，构建新型数字产品。例如，使用以太坊网络，能够使用以太币购买 Web3.0 网络世界中的 ENS 域名，并基于以太坊智能合约实现 Web3.0 网络中的 DNS 解析，将 Web3.0 域名解析至同样基于区块链技术构建的去中心化存储服务器，并因此实现不受任何中心化机构控制的互联网访问。此外，基于以太币，还能够构建各种 NFT（非同质化代币）及元宇宙应用，并使得用户能够使用数字货币购买数字藏品，并将用户的所有权记录永久保存于区块链中。

最后，数字货币是数字经济的重要组成部分。**数字经济领域日新月异的新兴技术强劲推动了全球数字货币产业的发展，数字货币的发展也反向推动了数字经济发展**。从功能上说，构建数字货币体系是推动数字经济发展的重要力量，利用数字货币产生的流通数据对生产领域进行升级改造，进而对数字经济发展可以起到正向推动作用。同时，数字货币作为数字经济基础设施的意义已经越来越被公众所认知，数字货币是数字经济时代的发动机和数字社会的助推器。同时，数字货币不仅是推动数字经济内循环系统的润滑剂，也是推动数字经济国际化的重要推手，有利于推动跨境贸易融资，进一步推动**数字贸易**的发展。特别是，数字经济体系中，**数字供应链、数字制造**等实体产业的发展，催生了数字货币的进一步发展，区块链技术赋能下的数字货币更进一步推动了上述产业的去中介化，使用数字货币作为区块链体系中的“通证”，让原本为中心化机构控制的信息以智能合约的形式固定于区块链中，使其无法被篡改，同时强化数字经济体系中的多方协调和数据共享。

不过，**数字货币也存在一些劣势**。由于其匿名性和去中心化特点，数字货币容易被用于非法活动和洗钱等违法犯罪行为。有研究表明，大约四分之一的用户（25%）和近一半的比特币交易（44%）与非法活动有关。此外，大约五分之一（20%）的交易总额和大约一半（51%）的比特币持有，都与非法活动有关。同时，数字货币市场也存在较高的风险和不稳定性，数字货币交易所“暴雷”、“跑路”现象层出不穷，而将数字货币提取至本人钱包又将大大降低数字货币的流动性，并使得用户在此后的出金入金过程中反复支付高昂的手续费，因此数字货币投资者一般而言需要承担较大的风险。

1.3 小结

综上所述，本章从历史角度分析了数字货币发展的缘起，讨论了数字货币诞生至今不同发展阶段的特点，并同时从发展背景和功能效用两个角度讨论了数字货币产业发展的驱动因素，总结认为**数字技术的进步、新冠疫情大流行对人们消费习惯的改变、全球化背景下生产方式的变革**推动了数字货币的发展。此后，本报告从功能效用角度分析数字货币产业的驱动因素。首先，数字货币在用户端推动在线支付进一步**便利化的同时，也一定程度上保护了用户的隐私**。其次，数字货币作为**优质投资品**，正受到广大投资者的青睐。而且，数字货币可用于**跨境支付购买各类数字服务和商品**。最后，数字货币能够作为去中心化应用的基础架构元素，构建各类 Web3.0 数字生态产品。在宏观层面，数字货币的诞生**重塑了世界货币体系**，能够以前所未有的广度和深度推动国际金融架构变革，一方面对现有的**国际货币体系造成冲击**，另一方面能够为遭受金融制裁的弱小国家提供新的规避思路。

第二章
全球数字货币发展概览

第二章
全球数字货币发展概览

2.1 全球私人数字货币产业发展现状的国别比较分析

2.1.1 主流原生代币的国别发展现状分析

2.1.1.1 全球主流原生代币发展现况与技术特征的比较分析

区块链原生代币 (Native Coin) 又被叫做主链币、公链币、基础代币等，是**直接建立在特定区块**上的加密货币，也是该区块链网络的核心资产，用于支付交易费用、执行智能合约、参与共识机制等。换言之，原生代币是**具有独立主链**的数字货币，通常是在该区块链网络中的独立数字资产，具有自己的发行上限、分发方式和经济模型。目前，主流的原生代币包括比特币主网区块链上的比特币（BTC）、以太坊区块链上的以太币（ETH）、Cardano 区块链上的艾达币（ADA）、波场区块链主链上的波场币（TRX）、Cosmos 区块链上的阿童木币（ATOM）等。总而言之，不同国家采取加密货币的程度不同，根据新加坡 Triple-A 公司发布的《2024 年全球加密货币所有权状况》报告，截至 2024 年，**全球加密货币拥有率平均为 6.8%，全球加密货币用户超过 5.6 亿**，相较于 2023 年 4.2 亿的加密货币用户数量，增长了 33%。其中，有 34% 的加密货币用户属于 24-35 岁的年轻人。持有率增长最快的国家则是阿联酋，相较于 2023 年增长了 25.3%。

表 2-1 显示的是 2024 年全球各国居民加密货币持有率排名，阿联酋、新加坡、土耳其等对数字货币创新相对政策友好的国家，其加密货币持有率最高。例如，阿联酋对区块链和加密行业极为友好，其计划成为全球首个区块链政府。阿联酋法

表 2-1 2024 年全球各国居民加密货币持有率排名

国家	加密货币持有率
阿联酋	25.30%
新加坡	24.40%
土耳其	19.30%
阿根廷	18.90%
泰国	17.60%
巴西	17.50%
越南	17.40%
美国	15.50%
沙特阿拉伯	15.00%
马来西亚	14.30%
中国香港	14.30%
印度尼西亚	13.90%
韩国	13.60%
南非	12.40%
瑞士	11.50%

数据来源：新加坡 Triple-A《2024 年全球加密货币所有权状况》报告

院甚至在 2024 年的一起案件中（2024 年第 1739 号），裁决加密货币可作为有效工资支付形式。阿联酋还积极拥抱央行数字货币，阿联酋中央银行不仅发行了自己的数字货币——Govcoins，还通过其参与建设的多边央行数字货币桥，成功与

中国银行完成价值 5000 万阿联酋迪拉姆（约合 9800 万元人民币）的首笔数字迪拉姆跨境支付交易。

表 2-2 显示，不同于持有率，从持有总数来说，2023 年印度、中国、美国等**人口大国**虽然持有率排名并不高，但持有总量相对较高，分别排名全球第一、第二、第三。这可能是因为这些国家作为人口大国，同时也是数字货币投资的热土，虽然其渗透率不如阿联酋、新加坡等数字货币政策友好型国家，但总量仍然更高。

表 2-2 2023 年全球各国居民加密货币持有总量及比例排名

Country	Population	Ownership	Ownership Percentage
Country	Population	Ownership	Ownership Percentage
India	1428627663	93537015	0.065473333
China	1425671352	59134683	0.041478482
United States	339996563	52888108	0.155554831
Vietnam	98858950	20945706	0.211874656
Pakistan	240485658	15879216	0.066029784
Philippines	117337368	15761549	0.134326765
Brazil	216422446	25955176	0.1199283
Nigeria	223804632	13261259	0.059253729
Iran	89172767	12000000	0.134570233
Indonesia	277534122	12205132	0.04397705

数据来源：https://www.triple-a.io/cryptocurrency-ownership-data

不同于单独统计加密货币持有量，区块链分析平台 Chainalysis 对 2023 年世界各国加密货币采用指数进行统计，该指数相较于加密货币持有量，从更广泛的层面对加密货币的使用进行了统计。该指数将链上数据和现实世界数据结合起来，以衡量哪些国家在加密货币采用方面处于世界领先地位。全球加密货币采用指数由五个子指数组成，包括**中心化服务价值获得排名、零售中心化服务价值获得排名、P2P 交易所交易量排名 、DeFi 价值获得排名、零售 DeFi 价值获得排名**。每个子指数都基于各国对不同类型加密货币服务的使用情况，该指数对所有 154 个国家的子指数进行排名，根据人口规模和购买力等特征对排名进行加权，取每个国家在这五个排名中的几何平均值，然后在 0 到 1 的范围内对最终数字进行标准化，为每个国家提供一个决定总体排名的分数。国家的最终得分越接近 1，排名就越高。不同于前述排名，加密货币采用指数最高的为**印度、尼日利亚和越南**等发展中国家。印度加密货币增长的主要原因是金融科技的兴起和移动技术的广泛采用。印度拥有全球第二大智能手机市场，智能手机用户超过 10 亿。同时，尼日利亚也是非洲 Web3 市场扩张速度最快的国家之一，这主要是因为尼日利亚**人口众多、人口结构年轻**且对新兴事物抱有浓厚兴趣，这一切都推动了尼日利亚加密货币市场的发展。越南的数字货币参与者也格外专注于区块链的各种应用项目。《2022 年越南加密货币市场报告》披露，截至目前，越南大约有 200 个活跃的区块链项目。该报告进一步显示，越南拥有超过 1660 万加密货币持有者，成为仅次于泰国的东盟地区第二大国家，其中 31% 持有比特币。越南这些活跃的区块链项目主要关注 GameFi、DeFi、NFT、Web3、基础设施和加密钱包。从历史的角度观察，这主要是因为越南曾经遭受很多经济不稳定和通货膨胀，而传统银行无法提供良好的回报，加密货币及其他衍生的数字资产可以作为很好的**价值储藏手段**。其次，**许多在国外工作的越南人需要寄钱回家**，而使用传统的银行跨境汇款处理费很高，而用比特币等加密货币可以降低成本。最后，加密货币在越南属于一个灰色区域，没有明确的法律框架禁止或者支持，所以给了区块链活动很大空间，可以在不受任何中央机构或政府影响的情况下进行数字交易

表 2-3 2023 年全球加密货币采用指数排名

Country	Overall index ranking	Centralized service value received ranking	Retail centralized service value received ranking	P2P exchange trade volume ranking	DeFi value received ranking	Retail DeFi value received ranking
India	1	1	1	5	1	1
Nigeria	2	3	2	1	4	4
Vietnam	3	4	4	2	3	3
United States	4	2	8	12	2	2
Ukraine	5	5	3	11	10	10
Philippines	6	6	6	19	7	7
Indonesia	7	13	13	14	5	5
Pakistan	8	7	7	9	20	20
Brazil	9	9	11	15	11	11
Thailand	10	8	15	44	6	6
China	11	10	5	13	23	23
Turkey	12	11	9	35	12	12
Russia	13	12	10	36	9	9
United Kingdom	14	15	20	38	8	8
Argentina	15	14	12	29	19	19
Mexico	16	17	18	30	16	16
Bangladesh	17	18	19	33	22	22
Japan	18	22	21	49	18	18
Canada	19	25	23	62	14	14
Morocco	20	27	25	21	26	26

数据来源：Chainalysis 数据分析平台

从不同类型的数字货币的技术特征上分析，**原生代币在推动区块链项目的发展和创新方面发挥着关键作用**。区块链生态的繁荣需要吸引用户、开发者和投资者的参与，而原生币作为激励手段，可以激发这些参与者的兴趣和积极性。通过持有、使用和贡献原生币，参与者能够获得生态内部权益，推动更广泛的应用探索、技术创新和社区建设。不仅为生态系统提供了经济支持，还促进了用户和开发者的积极参与，推动了区块链项目的发展和创新。原生币的存在有助于构建健康、活跃的数字经济生态，为整个区块链行业的可持续发展做出贡献。具体而言，上述原生代币还可**基于主链所使用的共识机制**而进一步分类。

基于 POW 机制的原生代币。比特币的货币生成系统是基于 POW（工作量证明）机制，矿工通过算力竞争获得记账权，并获取交易费收入和比特币奖励。除 BTC（比特币）外，以太坊也曾使用 POW 机制，但已于 2023 年 4 月 12 日完成“上海升级”后放弃，并转向 POS 机制。此外，仍然使用 POW 共识机制的原生代币还有莱特币 (Litecoin)、比特现金 (BCH)、门罗币 (XMR)、以太坊经典（ETC）、BSV(Bitcoin Satoshi Vision)、Zcash、达世币（DASH）等。上述情况显示，仍然坚持 POW 机制的主要为比特币和以太坊等数字货币的衍生货币，以及达世币、门罗币等强调完全去中心化和用户隐私的代币。这是因为到目前为止，虽然 POW 机制相较于其他共识机制效率较低、成本较高，但仍是最能够反映区块链技术去中心化精神、实现最大程度用户匿名的技术路线。

基于 POS 机制的原生代币。POS（权益证明）是 Solana、Cardano 和 Tezos 使用的共识机制。它最早于 2011 年在比特币论坛上创建，作为工作量证明的替代品，以改善旧的共识机制的不足之处。2012 年，第一个采用权益证明的加密货币项目 Peercoin 诞生。2023 年 4 月 12 日完成“上海升级”后，以太坊 2.0 主网也已从工作证明转向权益证明。试图做到 " 更

可扩展、更安全、更可持续 "。这种方法比工作量证明方法使用的计算能力要少得多，也更环保。具体而言，PoS 算法根据持有的货币数量来确定节点在共识过程中的权重。持有更多货币的节点更有可能被选为出块节点[1]，从而获得更多的奖励。相比于 PoW，PoS 算法节约了能源消耗，提高了交易速度，但也存在财富过度集中和潜在的攻击问题。目前，使用 POS 及其衍生共识机制的代币主要有 ETH（以太币）、ADA（艾达币）、ATOM（阿童木币）、SOL（Solana 币）等。

其中，艾达币（ADA）是 Cardano 项目的产物，是基于权益证明算法 Ouroboros 开发的。而 ATOM 币作为去中心化的跨链生态系统——Cosmos 网络的基础货币，具备了多项独特的功能和特点。首先，ATOM 币以去中心化的方式进行交易和验证，避免了中心化交易所带来的安全风险。其次，ATOM 币能够实现跨链互操作，使不同区块链之间的数字资产可以进行自由流动。最后，ATOM 币采用了权益证明（Proof of Stake）共识机制，将权益抵押作为产生新区块的决策标准，提高了系统的安全性和效率。

Solana 则是一个融合了历史证明（PoH）和权益证明（PoS）的区块链。与以太币和比特币相比，它所采用的独特共识算法旨在处理“区块链三难困境”（即没有一个解决方案能够同时解决区块链中的去中心化、可扩展性和安全性三项难题）。因为花费较低，效率较高，Solana 区块链能够很好地适用去中心化发展，从钱包、DeFi、Web3 到 NFT，每秒钟可运作千余笔交易。Solana 币（SOL）是生态体系的原生虚拟货币，供给量约为 5 亿次虚拟货币。而 Solana 持有人不仅能够参加整体生态的治理，付款交易购买 Solana 主链中衍生的各类 NFT 数字藏品，还能够通过代币质押领取奖励。

2.1.1.2 全球比特币发展现状的国别比较分析

比特币的货币生成系统是基于 POW（工作量证明）机制，矿工通过算力竞争获得记账权，并获取交易费收入和比特币奖励。工作量证明（Proof of Work，PoW）是比特币最早采用的共识算法，也是最知名和应用最广泛的算法之一。该算法要求节点通过完成一定的计算任务（即挖矿）来确保交易的有效性。POW 机制的优势在于其安全性、完全去中心化特质和稳定性。一方面，由于 POW 代币的挖矿过程需要大量的算力，攻击者要掌控整个网络并篡改交易记录变得非常困难。另一方面，POW 代币的挖矿过程可以由任何人参与，没有中心化的控制点，就保证了网络的完全去中心化。该机制的缺陷是消耗大量的计算能力和电力资源。

鉴于比特币的匿名性质，本报告无法对世界各国普通投资者拥有比特币的数量进行统计。所以，本报告首先基于全球视角对**各国政府持有比特币数量**进行比较分析，表 2-4 显示的是各国政府持有比特币数量统计表。基于统计表分析，截至 2023 年，世界各国政府持有的比特币总量为 73701 比特币。具体而言，其中 **90.3% 的比特币掌握在美国政府手中**，总计 69,640 比特币。这主要是因为，美国联邦调查局过去总共通过其司法行动查获了 259,112 个比特币。虽然联邦调查局在联邦政府的支持下出售了 189,472 个比特币，但美国政府仍然是拥有比特币最多的政府。继美国之后，挪威持有微策略公司（MSTR）2.14% 的股份。这意味着，考虑到 MSTR 持有的 158,400 枚比特币，挪威政府间接拥有 3,390 枚比特币，占世界政府份额的 4.4%。此外，萨尔瓦多政府也在这个名单

[1] 出块节点：出块节点指负责打包交易、生产区块的区块链节点。

中，占世界政府份额的 3.2%(2,473 枚比特币)。这主要是因为该国是全球首个将比特币作为法定货币的国家。乌克兰也是一个顶级的比特币持有者，这主要是为了便于战争捐款，乌克兰政府开始接受比特币。乌克兰拥有世界政府持有的比特币数量的 0.8%(642 个比特币)。略低于乌克兰的是不丹，拥有 621 个比特币 (即 0.8% 的份额)。这主要是因为，不丹试图利用该国水力发电厂的电力为比特币挖矿机供电。委内瑞拉也持有 0.3% 的比特币，其存储在公共钱包中的比特币有 125 个。在名单的最后，则是芬兰，该国因法律原因没收了 85 枚比特币，并承诺将这笔钱捐赠给乌克兰，作为对俄战争期间的支持。

表 2-4 2024 年世界各国政府持有比特币数量统计表

Governments	BTC Holdings 2024	Share %
United States	69640	0.903
Norway	3390	0.044
El Salvador	2473	0.032
Ukraine	642	0.008
Bhutan	621	0.008
Venezuela	240	0.003
Finland	85	0.001

数据来源：https://coinweb.com/trends/which-country-owns-the-most-bitcoin/

私人数字货币的节点分为全节点、轻节点和 SPV 节点。全节点是指包含全部交易信息的完整区块链的节点。轻节点仍需下载全部数据进行解析，获取与自身相关的交易数据，但无须本地保存全部数据。SPV 节点不需要下载新区块的全部数据，只需要保存区块头部信息。不同于比特币挖矿，下载全部区块链历史数据并成为比特币全节点并不会产生任何收益，对用户唯一的益处是使用全节点进行比特币交易活动安全性最高，因此某种程度上反映了该国针对数字货币的匿名化交易需要程度。此外，比特币全节点用户相当于担任了比特币交易验证系统中某种“志愿验证者”的角色，可以为其它轻节点或 SPV 节点用户提供数据验证及下载服务。虽然目前历史区块全部数据高达数百 GB，需要较长时间才能完全同步，但比特币全节点的存在是比特币系统去中心化的保障，而如果比特币全节点全部被某一个体垄断，将可能发生数据篡改等问题。因此，比特币全节点数量，在某种程度上，可以反映该国数字货币用户对于维持比特币系统去中心化特征的意愿。目前，比特币全节点数量在不同国家差异较大，表 2-5 显示的是 2024 年 7 月 24 日不同国家的比特币全节点数量，其中 n/a 表示节点所在国家或地区未知，其中美国仍然是全球比特币全节点数量最多的国家，其次分别是德国、法国、荷兰等欧洲国家。而传统上比特币挖矿活动较多的中国反而排名在第 10 名以外，表 2-3 中使用数字货币较多的越南、印度等国全节点数量也较少。**这一现象说明，美国的比特币匿名化需要和维持比特币系统去中心化特征的需求仍然最高**。

表 2-5 2024 年 7 月 24 日世界各国比特币全节点数量统计表

国家	比特币全节点数量
1. n/a	12029
2. United States	1771
3. Germany	1760
4. France	432
5. Netherlands	334
6. Finland	305
7. Canada	283
8. United Kingdom	221
9. Singapore	213
10. Switzerland	164

数据来源：本报告使用比特币全节点客户端收集整理

2.1.1.3 全球以太坊发展现状的国别比较分析

以太坊作为目前总市值仅次于比特币的数字货币，其吸引投资者关注的原因在于：首先，以太坊**引入了智能合约的概念**，允许开发者编写和部署可自动执行的合约代码。这使得以太坊不仅仅是一个数字货币，还成为了一个去中心化应用（DApp）的开发平台。智能合约可以用于构建去中心化金融（DeFi）、数字资产发行、供应链管理、投票系统等各种应用。其次，以太坊**拥有一个庞大而活跃的开发者社区**，以及众多的项目和应用，形成了一个庞大的生态系统。这些包括 DeFi 应用，如去中心化交易所（DEX）、借贷平台，NFT 市场，以及各种基于区块链的游戏和社交平台等。而且，以太坊的设计目标之一是去中心化和开放性。任何人都可以加入以太坊网络，并参与节点运行、开发 DApp 或参与社区治理。这种开放性增加了创新的可能性，并且使得任何人都能在平等的条件下访问和使用以太坊的功能。此外，以太坊的底层技术架构经过多年的发展和改进，具备**较高的安全性和稳定性**。尽管有过一些安全漏洞和网络拥堵的事件，但以太坊团队和社区通过升级和改进持续增强了平台的健壮性和安全性。最后，以太坊**智能合约遵循开放的标准**，如 ERC-20 和 ERC-721 等，这些标准促进了各种代币和数字资产的互操作性和流动性。这也使得以太坊成为了全球范围内最流行的数字资产发行平台之一。

从全球国别发展现况分析，表 2-6 显示，根据截至 2024 年 7 月 25 日的数据，目前**美国拥有最多的以太坊节点数量**，其次是**德国、韩国、加拿大、英国、法国等国**。不同于前述加密货币持有率和持有量排名，上述国家在比特币和以太坊节点数量上居多的原因应当是多方面的。首先，这些国家在**信息技术、互联网基础设施和高速网络连接**方面处于领先地位。拥有先进的技术基础设施使得运行和维护加密货币节点变得更为容易和可靠，特别是比特币和以太坊臃肿的区块数据使得其需要高速网络和大容量硬盘方能维持运行全节点。其次，美国和上述欧盟国家拥有发达的金融体系和深厚的经济基础。这些条件使得个人和机构更倾向于投资和参与加密货币市场，从而促进了节点数量的增长。而且，**比特币与以太坊全节点不同于挖矿活动能够带来收益，全节点用户仅仅是为了维持比特币与以太坊系统的去中心化特征，或个人研究开发需要而志愿下载全节点客户端并加入主网**，这些国家拥有活跃的技术社区和大量的软件开发者、工程师以及对新技术和创新感兴趣的个人。他们的参与推动了比特币和以太坊网络节点的数量增加，因此全节点数量的排名**与加密货币持有率、持有量的国别排名有所不同**。此外，在这些国家，对加密货币的**法律法规和监管较为宽松或明确**，这有助于鼓励更多个人和企业在该国运行和管理加密货币节点。最后，这些国家的大学和研究机构在区块链技术和加密货币领域有着广泛的研究和教育活动，这种学术支持和知识积累也促进了节点数量的增长。

表 2-6 2024 年全球主要国家以太坊全节点数量统计表

排名	国家	全节点数量（比例）
1	美国	1,977 (48.56%)
2	德国	498 (12.23%)
3	韩国	149 (3.66%)
4	加拿大	141 (3.46%)
5	英国	141 (3.46%)
6	法国	107 (2.63%)
7	荷兰	87 (2.14%)
8	伊朗	75 (1.84%)
9	新加坡	68 (1.67%)
10	捷克	67 (1.65%)

数据来源：本报告使用以太坊全节点客户端收集整理

2.1.2 稳定币的国别发展现状分析

比特币价格的波动性表明它无法提供货币的核心功能，所谓的稳定币试图弥补这一缺陷，但能否成功扩容并保持稳定，值得怀疑（Eichengreen，2019）。目前稳定币主要包括 USD Tether（USDT）、USD Coin（USDC）、DAI 等，其中泰达币和 USDC 占据最高的市场份额，且分别在数字货币市值总榜中排名第三、第七，大有不相上下之势，这主要是因为**USDT 目前避开美国市场，而 USDC 对纳入美国政府监管框架相对积极**。目前，美国众议院共和党议员 Patrick McHenry 起草的稳定币法案已在众议院金融服务委员会获得通过。众议院的法案较为简短，赋予州政府较大权力，而参议院的法案则更为详尽，平衡了州政府和美联储的权力。参议院的法案不仅明确了谁可以发行锚定美元的稳定币，还涉及了发行方合并或破产时的处理方式。该法案提出，如果稳定币发行方破产，应由联邦存款保险公司 (FDIC) 接管，以保护储户利益。草案同时鼓励多家机构包括银行参与稳定币的发行，对于发行量小于 10 亿美元的稳定币，所受的监管不会像银行那样严格。而对于发行量超过 10 亿美元的稳定币，法案要求实施与银行相同的严格监管。**两份草案都对 USDT 持有排斥态度，尤其是参议院的草案，明确禁止美国公司持有或使用 USDT**。

因此，新规实施将对 USDC 相对有利，USDC 的发行方——Circle 的 CEO 本身也一直在积极推动国会出台监管法案，强调 USDC 的全额保证金制度，且与商业银行的部分准备金制度相比，USDC 能够提供全额保证金，100% 兑付美元，不担心挤兑。不过，从这个角度观察，也可得出结论，美国市场的影响较大，美国政府对不同类型稳定币的监管态度，将深度影响稳定币全球市场走势。

同时，稳定币发行方的公司注册地点也对其市场走势影响较大。表 2-7 为全球总市值排名前十的稳定币总部所在地，显示**稳定币发行方一般将发行实体总部设置于美国或其他一些数字货币政策较为宽松、具备避税天堂特点的国家或地区**。将总部设置于美国主要是为了符合美国监管政策要求，并获得**更高的关注度和技术支持**，设置于美国以外的部分国家或地区则是为了**规避监管**，实现稳定币的真正去中心化。

例如，泰达币由一家名为 Tether Limited 的公司发行，该公司最初注册于马恩岛，后迁至中国香港，现总部位于巴哈马，但其实际运营团队却与美国加密货币交易平台 Bitfinex 有着千丝万缕的联系，但实际注册地均被认为是离岸银行业务的避税天堂。相比之下，USDC 发行人 Circle 受美国管辖，因为它的总部位于马萨诸塞州波士顿。USDC 发行人 Circle Internet Financial2024 年初还进一步宣布，计划在首次公开募股前，将其法律基地从爱尔兰共和国迁往美国。总而言之，USDC 将其各类实体机构设置于美国境内，主要是因为该公司始终将**稳定币业务合规性置于公司发展首位**。USDC 将自己打造为完全受监管、透明的稳定币的战略，可能会促使 Tether 尝试重塑其公众形象。

DAI 是目前去中心化稳定币龙头 Maker DAO 于 2017 年正式发行和管理。MakerDAO 是去中心化金融 (DeFi) 项目，总部位于美国旧金山，创始人为 RuneChristensen。First Digital (FDUSD) 则是以储备金提供支撑的稳定币，由总部位于香港的金融公司 First Digital Limited 的子公司发行。USDD 则由总部位于新加坡（波场在发展早期为旧金山与北京双总部）的波场基金会发行，创始人为中国人孙宇晨。孙宇晨将 USDD 发行方总部设置于新加坡而非美国，正是为了规避监管。2024 年 4 月，美国 SEC 修改对 Tron 创始人孙宇晨的诉讼，称其在美国多地频繁出行，从而使得法院具备相应管辖权。SEC 指控孙宇晨及其公司通过 Tron 和 BitTorrent（BTT）代币销售未注册证券，并进行操纵性洗钱交易。SEC 称，孙宇晨在 2017 年至 2019 年间在美国度过超过 380 天，旅行目的地包括纽约、波士顿和旧金山等地。孙宇晨则反驳称，代币销售完全在海外进行，避免了美国市场，因此 SEC 无权对其及总部位于新加坡的 Tron 基金会施加管辖。PYUSD 则在发行中得到 Paypal 的背书支持，在 PayPal 旗下的 Venmo 支付应用程序上提供。该稳定币建立在以太坊之上，由 Paxos Trust Company 发行，公司总部位于纽约，为客户提供受监管的区块链基础设施。此外，Edelcoin AG 宣布推出 Edelcoin (EDLC)，Edelcoin 是一种由一篮子贵金属和贱金属支持的稳定支付代币，比单一的基于法定或金属的稳定币具有更高的稳定性，并且具有与其他数字货币相同的多功能性。

表 2-7 2024 年全球稳定币总市值排名

总排名	币种	总市值	流通总量	总部
3	Tether	$114,397,689,330	114,419,695,894 USDT	巴哈马
7	USDC	$34,045,254,012	34,050,433,983 USDC	美国波士顿
19	DAI	$5,347,781,372	5,347,888,596 DAI	美国旧金山
46	First Digital USD	$2,019,998,217	2,021,456,516 FDUSD	中国香港
90	USDD	$737,947,349	738,651,979 USDD	新加坡
124	TUSD	$495,734,749	495,201,533 TUSD	美国旧金山
149	PYUSD	$349,644,031	349,835,043 PYUSD	美国纽约
201	EDLC	$6,203,301,740	5,516,931,200 EDLC	瑞士
202	USDe	$3,399,038,489	3,400,785,672 USDe	不详
207	FRAX	$647,179,176	649,434,271 FRAX	不详

数据来源：本报告手动收集整理（数据统计截至 2024 年 7 月 25 日）

除美国外，**中国香港地区也积极拥抱稳定币发展机遇**。2024 年 7 月 18 日，香港金管局公布了稳定币发行人“沙盒”参与者。除香港本土圆币、渣打成为首批参与企业外，内地互联网企业京东也位列其中，具体包括五家公司，分别为京东币链科技（香港）有限公司、圆币创新科技有限公司，及渣打银行（香港）有限公司、安拟集团有限公司、香港电信有限公司。

不过，上述企业均仅计划发行港元稳定币。香港作为中国资金进出的“安全阀”，发展港元稳定币产业不仅有助于香港进一步巩固其作为国际金融中心的地位，也可能对全球金融生态系统产生重要影响，进一步巩固港元在国际贸易体系中的地位。不过，发行过程中离岸人民币稳定币的缺位，使其仍然仅是一次数字货币产业创新发展的试水。如果未来能够随着产业的发展推进，推动**人民币稳定币在港发行**，香港作为全球最大和最重要的离岸人民币业务中心，必将能够在数字化浪潮中，进一步**推动人民币国际化发展，和数字资产的人民币计价**。

当然，从目前主流稳定币的**挂钩币种**上分析，以目前交易量最大的泰达币（Tether）为例，该币目前分为美元泰达币、欧元泰达币、人民币泰达币、费城金银指数泰达币和泰达黄金等。表 2-8 显示的是全球不同币种类型泰达币流通量统计表。根据 2024 年 7 月 24 日最新公布的**泰达币透明度报告**，目前正在流通的泰达币中，最多的仍然为泰达美元，显示**美元锚定的稳定币仍然占据最高的市场地位**，其次分别是泰达欧元、泰达人民币、泰达墨西哥比索、泰达黄金等，稳定币市场呈现出美元独大、多极化格局共存的局面。

表 2-8 全球不同币种类型泰达币流通量统计表

货币种类	净流通量
泰达美元	114,419,695,893.83 美元
泰达欧元	30,618,610.07 欧元
泰达人民币	20,503,468.90 人民币
泰达墨西哥比索	19,562,400.00 比索
泰达黄金	246,524.33 盎司

数据来源：https://tether.to/en/transparency/?tab=usdt

从具体技术角度分析，泰达币（Tether）没有自己的区块链网络，而是在既有的区块链网络中，通过在交易附加信息中添加的方式发行代币和记录交易信息。泰达币主要基于比特币的 omni 协议、以太坊的 ERC-20 协议和波场币的 TRC-20 协议发行和记录交易信息，使用不同协议发行的泰达币之间互相不可转账。基于比特币 omni 协议的泰达币的最早发行，始于 2014 年 11 月，由于支付效率低下，交易量逐渐被 2018 年和 2019 年上线的 ERC20-USDT 和 TRC20-USDT 超越。以比特币 omni 协议为例，具体算法为，泰达币首先将交易信息记录于存储比特币锁定脚本中以 OP_Return 开头的“ 备注信息 ”中，而存储泰达币交易记录的比特币网络中的比特币交易金额，除矿工费外一般仅向收款方支付比特币防尘机制规定的最小粉尘阈值 546 聪（0.00000546 个比特币）。由于备注信息在比特币区块中同样具有不可篡改性，因而交易信息存储于备注信息中完全可以防止泰达币的双花问题。泰达币的这一机制使其同时做到了发行层面的中心化和交易验证层面的去中心化。

美元泰达币（USDT）既不通过矿工挖矿生成，也不额外生成货币，而是采用中心化的方式以 100% 准备金发行数字货币。用户可以通过 SWIFT 电汇美元至 Tether 公司提供的银行帐户，或通过 Bitfinex 交易所换取 USDT。赎回美元时，反向操作即可。不过，用户通过 Tether 官网将 USDT 换为美元有一定限制。根据 Tether 公司 2018 年 11 月 27 日公布的公告，个人用户通过 Tether 公司官网赎回法币有 10 万美元的金额要求，且需支付一定的手续费。而大部分中小用户需要通过交易所交易泰达币。

泰达币在采用 omni 协议、ERC-20 协议和 TRC-20 协议时，**验证速度依次递增，安全性和手续费依次递减**。安全性依次递减主要是因为不同于比特币十余年的运行历史与不断修订，波场币 TRC-20 协议历史较短，未来可能存在较大漏洞，波场币运营方甚至以 1000 万美元悬赏开发者发现波场币的漏洞。因此一般大额**转账使用 omni 协议，中等额度使用 ERC-20 协议，小额转账使用 TRC-20 协议。**

更进一步分析，虽然上述协议各有差异，但用户偏好也在不断变化。表 2-9 显示的是泰达美元在各区块链主网流通量排名。根据 2024 年 7 月 23 日最新公布的泰达币透明度报告，目前泰达美元在波场网络（Tron）中的流通量最高，为 603 亿美元，其次为以太坊中发行的泰达美元，高达 506 亿美元，而传统的比特币网络 Omni 中发行的泰达美元，仅 1.3 亿美元，远远落后于其他各类新兴区块链协议，如 Avalanche、Solana 等，说明**稳定币用户对支付速度敏感度最高，更倾向于使用在波场网络和以太坊网络中使用稳定币，并不热衷于隐私保护程度最高的比特币 Omni 网络**。

表 2-9 泰达美元在各区块链主网流通量排名

主网	净流通量
Tron	60,318,181,182.30
Ethereum	50,657,945,368.29
Avalanche	1,259,646,866.15
Solana	731,256,391.97
Ton	619,674,501.59
Near	253,999,998.00
Celo	188,100,000.80
Omni	130,009,681.25
Cosmos	103,500,000.11
EOS	72,650,283.65
Tezos	37,277,929.64
Polkadot Asset Hub	22,997,725.05
Algorand	13,017,596.75
Liquid	10,211,849.00
SLP	986,524.74
Kusama Asset Hub	239,994.54

数据来源：https://tether.to/en/transparency/?tab=usdt

2.1.3 平台币的国别发展现状分析

平台币是由数字资产交易平台发行的数字货币。目前，主流的平台币包括币安交易所发行的币安币、火币交易所发行的 HT、OKEX 交易所发行的 OKB 等。平台币主要包括积分和股票两种性质，作用主要包括**手续费优惠、分红、平台币自身增值、参与社区决策、空投其它币种、辅助上币**等。换言之，数字货币交易平台在自身的不断发展壮大中，已不满足于通过收取数字货币交易中介费赚取收益，而是进一步利用平台本身的高关注度和高访客数量，利用自身优势试图构建全新的数字货币体系，从而带来更高流动性[2]。根据《福布斯》杂志的统计[3]，截至 2022 年 11 月，全球超过 16 家加密货币和 DeFi 交易所创建了其平台币[4]，这些代币的总市值超过 620 亿美元。这些平台币为持有者提供交易所福利，如交易费用折扣、优惠保证金贷款条款等，同时也使得货币发行者能够逐步在数字货币市场交易中占据主导权，利用自身交易规模优势吸引投资者使用自身平台币作为中介货币，从而试图挑战美元作为数字货币市场中价值锚定工具的地位。其中，平台币中最成功的是中国首富赵长鹏创立的币安币，市场总额达到 459.77 亿美元。表 2-10 显示，这些平台币**部分远程办公，除部分总部位于新加坡、美国、日本等发达国家外，其余均位于塞舌尔、巴哈马、开曼群岛等对数字货币交易所政策友好或税收优惠政策较多的国家**。其中币安、OKX、火币、Gate.io（芝麻开门）等交易所均为中资背景、原总部位于中国的交易所，在中国数字货币监管政策收紧后转移总部至海外或改为无总部远程办公。

[2] 例如，在 OKB、币安等平台将其它数字货币兑换为平台发行的私人数字货币如币安币、OK 币等时，能够减免一定比例的手续费。

[3] 数据来源：https://www.forbes.com/sites/ninabambysheva/2022/11/14/the-looming-62-billion-crypto-contagion/

[4] Coinbase 和 Kraken 没有发行平台币的原因或是因为他们担心平台币可能会被 SEC 视为证券

表 2-10 2022 年主流平台币所在地及市场总额排名

交易所	代币标志	总部所在地	市场总额（百万美元）
Binance（币安）	BNB	无，远程办公	45977
OKX	OKB	塞舌尔	4651
Uniswap **	UNI	美国纽约	4188
Crypto.com	CRO	新加坡	2024
Tokenize Xchange	TKX	新加坡	803
Huobi（火币）	HT	塞舌尔	699
Kucoin	KCS	塞舌尔	693
Whitebit	WBT	立陶宛	682
PancakeSwap **	CAKE	日本	590
BTSE	BTSE	英属维京群岛	562
Gate.io	GT	无，远程办公	538
Synthetix Network	SNX	澳大利亚	392
FTX	FTT	巴哈马	262
MEXC Global	MX	塞舌尔	87
Bidget	BGB	新加坡	27
BitMart	BMX	开曼群岛	16

数据来源：https://www.forbes.com/sites/ninabambysheva/2022/11/14/the-looming-62-billion-crypto-contagion/?sh=1aa5c1a61c39

2.2 全球央行数字货币产业发展现状的国别比较分析

央行数字货币分为零售型和批发型，批发型央行数字货币仅面向央行与金融机构而不面向公众（Bech and Garratt，2017）。但在技术设计方面，越来越多的央行正在考虑“混合”或“中间”架构，其中央行数字货币是对央行的类似现金的直接债权，而私营部门管理所有面向客户的活动 (Auer et al., 2020)。发行央行数字货币时，一些基于“代币”，另一些基于“账户”，还有一些使用两者的组合 (Lee et al., 2020)。目前，已有近 50 家央行已经推出了央行数字货币（CBDC）的设计或原型（Auer & Boehme, 2021）。世界上超过三分之一的受调查央行表示，发行 CBDC 是一种中期可能性 (Boar et al., 2020)。**66 项零售型央行数字货币项目和 25 项批发型央行数字货币项目中，大部分项目仍处于研究或试运行阶段，其中仅有巴哈马、尼日利亚和东加勒比央行已正式发行央行数字货币，均为零售型央行数字货币**。批发型央行数字货币项目，目前进展较快的包括加拿大 Jasper 项目和欧洲央行的 Stella 等。

2.2.1 巴哈马沙元

2020 年 10 月，巴哈马央行宣布，10 月 20 日起正式推出央行数字货币——“沙元”（Sand Dollar），使其成为世界上首个正式发行央行数字货币的国家。沙元的发行机制是，通过与巴哈马元 1:1 兑换支持，而巴哈马元又与美元挂钩。为避免通货膨胀，巴哈马中央银行只会在需求增加时铸造新的沙元，在铸造新的沙元后将删除等量物理巴哈马元的流通。沙元的技术解决方案由交易提供商 NZIA 提供，NZIA 为此开发了一种新的专用于央行数字货币的分布式无线支付系统，该系统由模块化设计组成，集成了混合无线通信网络、区块链硬件节点、边缘处理能力和“Cortex”分布式账本，能够与现有的银行系统协同工作，为现有的集中式支付网络提供用于替代的分布式支付网络辅助。

为什么作为加勒比地区一个岛国的巴哈马，领先于世界各主要经济体首先正式发行央行数字货币？英联邦秘书处 2020 年发布的《英联邦国家数字经济状况》报告显示，巴哈马目前的互联网普及率达到 90%，在英联邦国家中位居第四，仅次于加拿大、澳大利亚和新西兰。而根据巴哈马央行数字货币项目“沙元”的项目主页介绍，巴哈马央行 2019 年夏在巴哈马埃克苏马（Exuma）区进行了央行数字货币试点，试点项目的调查结果显示，大约 96% 的埃克苏马受访居民拥有移动设备，大约 40% 的受访者使用这些设备来执行某些形式的账单支付或网上银行交易。近三分之二的受访者表示愿意在未来使用移动设备进行支付或商业交易。巴哈马中央银行行长 John A. Rolle 在接受《华尔街日报》采访时表示，“巴哈马在多里安飓风过后所经历的基础设施破坏，使得在某些情况下，银行需要一年多的时间才能重建实体分支机构。然而，如果拥有一个人人都可以访问的电子支付基础设施，那么这就像重新启动通信链接一样简单。”**综上所述，高度发达的数字经济、互联网普及率与居民使用电子支付的高意愿，是巴哈马央行数字货币项目进展远远快于世界各主要经济体的基础，而巴哈马国家由分散式群岛组成的特性，更进一步增大了该国发行央行数字货币的需要。**

2.2.2 尼日利亚电子奈拉

2021 年 10 月 25 日，尼日利亚总统宣布正式推出央行数字货币项目电子奈拉（eNaira），使其成为世界上第二个正式发行央行数字货币的国家。电子奈拉基于开源的分布式账本项目 Hyperledger Fabric 进行构建，并支持尼日利亚央行采用双层模型架构。为保障包容性，电子奈拉使用基于账户的央行数字货币模型。为解决潜在的经济美元化问题，尼日利亚电子奈拉已经将与其它国家央行数字货币未来的互操作性纳入设计之中。

为什么非洲小国尼日利亚如此急切地发行央行数字货币？根据 Coin Dance 数据库，过去五年内，在 Paxful 交易平台上的比特币交易额，尼日利亚高居世界第二，仅次于美国，而加密货币泛滥的原因在于持续性的通货膨胀。Trading Economics 数据显示，尼日利亚奈拉通货膨胀率始终维持在 10% 以上。居民为对抗通胀使用加密货币作为交易货币的现象又进一步加重洗钱、毒品、枪支交易等违法行为泛滥。**因此，尼日利亚央行推出央行数字货币的主要目的就是为了对抗加密货币风险，维护金融安全，遏制非法交易。**

2.2.3 加拿大 Jasper 项目

不同于满足普通居民交易需求的巴哈马沙元与尼日利亚电子奈拉等零售型央行数字货币，加拿大 Jasper 项目是较早开展的批发型央行数字货币项目，也是发达国家央行数字货币进展最快的项目之一，已经进入试点阶段。Jasper 项目在不同阶段使用了不同的区块链技术，从 2017 年至 2018 年，加拿大央行的批发型央行数字货币项目 Jasper 分别在第 1-4 阶段，对利用区块链技术进行大额银行间支付结算进行初步调查，对分布式账本技术在高价值银行间支付清算和结算方面的效率进行测试，探索将央行数字货币与其他资产整合的潜在好处、实验开发跨境跨货币结算系统。Jasper 项目的第 1 阶段和第 2 阶段测试，分别运行于以太坊和金融科技公司 R3 开发的金融领域交易平台 Corda。由于以太坊的公有链性质，Japser 项目认为第 1 阶段测试存在隐私泄露的重大风险。而与比特币、以太坊等公有链系统不同，第 2 阶段的 Corda 系统采用许可链技术，即数据并非全网可见，而是只有在合约范围内的合法参与主体才可见。而且，Corda 中每个节点所有者都要经过 KYC 流程获取身份证书才能加入网络。因此，在第 2 阶段测试中，Jasper 项目报告对许可链技术做出了较高评价，认为虽然就核心运营成本而言，独立的分布式账本系统不太可能像集中支付系统那样有利，但是由于能够与更广泛的金融市场基础设施进行整合，所以区块链技术可以提高金融系统的效率。

2.2.4 欧洲央行和日本央行 Stella 项目

Stella 项目是欧洲央行和日本银行开展的批发型央行数字货币联合研究项目，截至目前共进行了四个阶段的实验。第一、三阶段实验使用 Hyperledger Fabric，第二阶段使用 Corda 作为技术支持。第一阶段，使用分布式账本技术（DLT）来处理大规模支付。第二阶段，在 DLT 环境中测试证券结算。第三阶段，应用 DLT 相关技术，提高跨境支付效率。2020 年 2 月 12 日，欧洲央行和日本央行发布第四阶段联合报告，探讨了隐私增强技术 (PET) 解决分布式账本技术（DLT）应用于金融领域可能存在的隐私问题（例如限制第三方对信息的访问），以确保央行数字货币能够在确保机密性的情况下也可以有效地进行审计。

2.2.5 数字人民币

央行数字货币研发领域，中国是目前**较早明确表示将央行数字货币投入试运营**的国家之一。2014 年，中国人民银行成立了法定数字货币研究小组，开始对发行框架、关键技术、发行流通环境及相关国际经验等进行专项研究。2016 年，中国人民银行成立数字货币研究所，完成法定数字货币第一代原型系统搭建。2017 年末，人民银行开始组织商业机构共同开展法定数字货币 DCEP 项目研发试验。2022 年 1 月 4 日，数字人民币（试点版）App 上架各大应用商店。 2022 年 1 月 7 日，京东、美团、饿了么、天猫超市、滴滴出行等 49 家平台已接入数字人民币系统。

目前，数字人民币已经进入了多个试点阶段，在**多个城市和地区进行推广测试**。这些试点包括了不同场景的应用，如零售支付、公共交通、政府服务等。试点范围涵盖了大城市和中小城市。同时，数字人民币的使用体验不断优化，包括了线上线下支付、离线支付等功能。用户可以通过数字人民币钱包进行各种交易，如购物、转账、支付公共服务费用等。

在技术平台层面，数字人民币的技术平台不断完善，具备了安全、可靠的技术基础。包括了区块链技术在内的一些新兴技术被用于保障交易的安全和透明度。相关法律和政策框架也在逐步完善，以支持数字人民币的推广和使用。中国政府对数字人民币的发展持积极态度，并出台了一系列政策来规范其应用。各大商业银行和金融机构已经开始参与数字人民币的相关业务，包括发行、兑换和交易等方面。这有助于数字人民币在金融系统中的全面融入。

同时，中国在数字人民币方面的探索也引起了国际关注。中国与其他国家和地区就数字货币的标准和政策进行了交流合作，推动了国际数字货币的发展讨论。

此外，在技术层面，虽然数字人民币在技术层面使用了与比特币类似的数字证书体系、数字签名、安全加密存储等技术，但与以比特币为代表的私人数字货币存在以下差异。首先，与比特币不同的是，数字人民币采用**有限匿名的方式**。在真实应用场景中，数字人民币账户地址是匿名的，但在数字人民币后台系统中，所有者标识可以关联到真实用户的实名，具体关联由数字货币系统建立所有者标识到真实用户的对应关系。中国人民银行数字货币研究所在其专利“数字货币的支付方法和支付系统”（专利号：CN201710493136）中即指出，“虽然数字货币本身所有者标识是匿名的，但数字货币系统后台能够做到实名”。因此，央行数字货币相较于比特币，能够在实现金融便利化和有限匿名的同时，更好地遏制利用数字货币开展违法交易。

其次，在算法上，比特币主要使用椭圆曲线数字签名算法 (ECDSA) 对交易信息进行签名和验证，而数字人民币使用**国产椭圆曲线公钥密码算法标准 SM2 对交易信息进行签名和验证**。比特币主要使用美国国家安全局 (NSA) 研发的哈希函数 SHA256 作为信息摘要算法，而数字人民币主要使用**国产哈希算法标准 SM3**。因此数字人民币使用基于椭圆曲线密码学和密码杂凑函数自主研发的国产加密算法，能够更好地保障央行数字货币系统的的安全性。此外，SM2 算法相较于椭圆曲线数字签名算法 (ECDSA)，加入了较多检错功能，从而能够进一步提高数据完整性和系统安全性。SM3 算法则在 SHA256 算法的基础上进一步复杂化设计，例如压缩函数的每一轮都使用 2 个消息字，从而提高其安全性。

最后，比特币的签名信息全网广播，可由全网任意全节点验证。而数字人民币的签名信息仅由收款方和服务商系统验证。而被授权验证的服务商系统属于许可链中的被授权节点。因此，数字人民币没有采用比特币完全开放式的公有链，而是采用了类似分布式账本平台 Corda 的**许可链体系**，该数据库的特点是，交易无需全网广播；共识机制仅存在于负责验证交易的节点之间；没有区块的概念，后续交易直接指向前序交易。

2.3 全球数字货币与各类新兴数字技术的融合发展新趋势

2.3.1 数字货币与智能合约开发

基于数字货币区块链技术的智能合约开发，是数字货币与各类新兴数字技术交互融合的基础。以太坊是首个支持智能合约的区块链平台，基于其**可编程性、丰富的生态系统和可持续的升级能力**。在以太坊虚拟机中，任何人都可以**编写合法的脚本以执行任意逻辑**。目前，基于以太坊等新型数字货币的各类数字经济产品，包括各类**去中心化应用**，如去中心化交易所、去中心化身份验证、去中心化投票等，以及各类资产代币化，如房地产、股票、金属等资产，在以太坊中进行代币化后将可以在区块链上交易。基于以太坊平台，还可以实现在区块中进行供应链管理，以提高透明度和效率，并帮助企业更好地监控和管理供应链。根据 Dappros 发布的 2023 年区块链与 Web3.0 开发者统计报告（见表 2-11），**目前拥有最多区块链开发者的国家是美国，其次是印度、英国和加拿大。其中，区块链开发者又可进一步细分为以太坊开发者、Hyperledger 开发者、Solidity 开发者、NFT 开发者、Web3 开发者等**。其中以太坊开发者是指在以太坊主链上开发智能合约程序，以发行衍生代币或各种以太坊合约程序为目的的开发者，Hyperledger 则是目前最主流的许可链开发平台，主要用于需要保证数据安全、不能完全去中心化的区块链应用，如央行数字货币等。Solidity 则是目前以太坊智能合约程序编写所需要的语言。NFT 则是非同质通证开发，以近年来热门的数字藏品为主。

表 2-11 世界各国区块链开发者数量排行表

排名	国家	区块链	以太坊	Hyperledger	Solidity	NFT	Web3
1	美国	6493	1545	280	1902	1077	1031
2	印度	5469	1915	660	2286	657	979
3	英国	1459	274	58	317	162	144
4	加拿大	1229	354	64	407	231	245
5	巴基斯坦	1132	423	73	541	270	269
6	法国	1057	233	59	349	185	121
7	尼日利亚	940	181	16	296	119	135
8	越南	866	171	27	327	117	96
9	德国	862	205	63	223	69	84
10	西班牙	791	209	79	273	101	103
11	土耳其	690	103	20	237	81	87
12	新加坡	657	145	24	192	112	86
13	意大利	647	95	19	145	84	59
14	中国	581	99	17	115	60	57
15	荷兰	570	95	31	110	44	33
16	阿联酋	533	168	46	194	93	95
17	巴西	528	140	41	188	83	77
18	韩国	507	69	11	108	66	30
19	澳大利亚	499	100	15	111	56	50
20	伊朗	498	94	10	171	39	60

数据来源：https://www.dappros.com/202303/worldwide-blockchain-and-web3-developers-statistics-2023/

2.3.2 数字货币与元宇宙技术

私人数字货币还广泛用于元宇宙世界的构建和结算。用于**元宇宙世界货币结算**的数字货币被称为元宇宙币，主要有SLP、TLM、CHR、SAND、AXS、MANA六种。目前最知名的元宇宙项目Decentraland和The Sandbox分别使用自行发行的私人数字货币MANA和SAND结算元宇宙土地购买、道具购买等数字资产交易活动。Decentraland和The Sandbox中的所有数据均以智能合约的形式存储于以太坊公链中，而**区块链不可篡改的特性保证了元宇宙世界中的数字资产产权确认不受任何中心化机构的控制**。基于上述原因，元宇宙投资正在逐渐引起各大金融机构的重视。2022年7月，伊斯兰银行Warba宣布进军元宇宙世界，并在元宇宙中购买两块土地。2022年9月，新加坡最大商业银行星展银行也宣布，在元宇宙中购入虚拟土地进行开发。世界范围内，NFT投资者正使用元宇宙币打破时空壁垒，在元宇宙数字世界实现货币的自由兑换和流通。根据Finder于2022年对超过28000名世界各国受访者进行的NFT持有率调查（见表2-12），**持有率较高的国家主要为菲律宾、泰国、马来西亚等发展中国家。而70.6%的受访美国公民不知道NFT是什么，且只有2.8%的人拥有NFT，说明虽然NFT技术发源于美国，但当下主要交易者已转向发展中国家。**

表2-12 世界各国NFT持有率排行表

排名	国家和地区	拥有至少一个NFT	计划购买NFT	预期持有率
1	菲律宾	0.32	0.095	0.415
2	泰国	0.266	0.079	0.345
3	马来西亚	0.239	0.105	0.344
4	阿联酋	0.234	0.115	0.349
5	越南	0.174	0.1162	0.291
6	尼日利亚	0.137	0.217	0.354
7	巴西	0.121	0.099	0.22
8	中国香港	0.107	0.104	0.211
9	委内瑞拉	0.106	0.135	0.241
10	秘鲁	0.099	0.145	0.244

数据来源：https://www.finder.com/nft-statistics

2.3.3 数字货币与Web3.0网络技术

数字技术发展的基石是Web2.0，即基于中心化的服务器的信息技术创新，而即将到来的Web3.0时代，**以区块链技术为基石，以去中心化为特征，而数字货币执行该系统中的信息媒介和价值交换功能**。从具体的产品角度分析，Web3.0的代表性产品Ethereum Name Service（ENS）是Web3.0时代数字经济发展的基础服务之一，虽然基**于ENS域名和IPFS分布式存储系统**并进行DNS解析后，能够搭建**“永不停机、去中心化且无法屏蔽的服务器”**，但是在上述Web3.0体系中，ENS域名的解析信息存储在以太坊的智能合约中，租用域名需要向以太坊中ENS官方支付一定以太币作为费用，而每次解析均需要消耗一定量的以太币作为gas费。目前，根据Built With统计的全球IPFS网站列表（见表2-13），截至2023年7月11日，目前现有4843个基于区块链IPFS存储技术搭建的Web3.0网站，其中除部分以io域名结尾以及所在地不明的网站外，**美国拥有最多的Web3.0网站，其次是中国和荷兰**。

表2-13 世界各国使用IPFS搭建的Web3.0网站数量排名

国家	数量
美国	1664
中国	111
荷兰	44
科科斯群岛	36
印度	34
芬兰	33
英国	27
德国	26
法国	22
加拿大	22
俄罗斯	20
巴西	16
印度尼西亚	15
瑞士	13
意大利	11
根西岛	9
西班牙	8
新加坡	8
墨西哥	8
澳大利亚	7

数据来源：https://trends.builtwith.com/websitelist/IPFS

不过，作为Web2.0域名替代品的ENS域名，虽然炒作价格不断上涨，目前仍仅处于概念阶段，生态发展缓慢，仅Brave浏览器等少数浏览器工具可以直接访问ENS域名，目前ENS域名和IPFS分布式存储系统配合后，仅可用于静态网站建设，尚不适用于当前数字经济快速发展的生态，以至于ENS域名管理机构向Web2.0时代的域名管理机构ICCAN求助，且每次DNS解析均需要收取高额的解析费用。

2.3.4 数字货币与人工智能技术

数字货币与人工智能技术，是相互发展、共同促进的关系。人工智能技术不仅能够**分析大量的区块链元数据和数字货币交易数据**，提供更精准的市场预测和技术架构改进方案。而且，区块链技术赋能下的智能合约还可以通过人工智能技术**进行更复杂的逻辑判断和自动执行**，提高区块链的效率和灵活性。此外，人工智能技术可以通过分析大数据流和交易模式来**检测潜在的欺诈行为**[5]，提高区块链上交易的安全性和可信度。

从央行数字货币的角度观察，首先，人工智能技术可用于监控央行数字货币交易活动，检测异常或可疑的交易模式，以**防止欺诈和非法活动**。此外，人工智能技术可以用于开发更智能化的央行数字货币支付系统，**提升用户体验和支付效率**。而且，人工智能技术还能够进一步增强央行数字货币中所使用的**区块链系统的效率和安全性**，使其智能合约的执行可以通过人工智能技术进行更复杂的条件判断和自动化执行，提高整体系统的灵活性和响应能力。最后，人工智能技术还可以帮助央行进行政策制定和决策支持。通过分析大数据、预测经济走势和货币需求，人工智能可以为央行提供更准确的决策依据，帮助优化货币政策和经济管理。

目前，已有较多人工智能技术赋能下的私人数字货币。表2-14显示，总市值最高的人工智能数字货币分别为NEAR、ICP、FET等。2023年11月，NEAR官方发布了NEAR Tasks

[5] 例如，Coinbase使用Amazon SageMaker开发机器学习算法来进行图像分析，打击诈骗行为。该交易所所使用的面部相似性算法能够自动从上传的身份证中提取面部特征，然后将这些面部特征与已上传的其他身份证的面部特征进行比较。诈骗者通常会将同一张照片放在多个身份证件上，否则他们必须在身份证上的几个位置编辑面部照片。而通过这种面部相似性算法，Coinbase可以快速发现这些伪造的证件。

以进行人工智能模型的的训练和改进。NEAR Task 是基于区块链的人工智能标注平台，模型训练需求方（Vendor）可以在平台发布任务请求，并上传基础数据素材，用户（Tasker）可以参与进行任务答题，为数据进行文本标注和图像识别等人工操作。任务完成后，平台会给用户 NEAR 代币奖励，而这些经过人工标注的数据会被用于训练相应的 AI 模型。

表 2-14 2024 年全球人工智能数字货币总市值排名

排名	货币	价格	总市值
19	NEAR	US$5.68	US$6,254,569,717
27	ICP	US$9.54	US$4,456,422,096
32	FET	US$1.20	US$3,023,913,830
42	RENDER	US$6.04	US$2,366,063,147
43	TAO	#######	US$2,330,659,380
56	GRT	US$0.19	US$1,783,697,943
100	AKT	US$3.08	US$746,024,074
131	AIOZ	US$0.48	US$530,358,550
173	AGIX	US$0.57	US$359,013,041
179	ARKM	US$1.37	US$331,613,532

数据来源：本报告手动收集整理（数据统计截至日期为 2024 年 7 月 25 日）

2.3.5 数字货币与资产数字化

去中心化金融（英语：Decentralized finance，俗称 DeFi）是一种创建于区块链上的金融，它不依赖券商、交易所或银行等金融机构提供金融工具，而是利用区块链上的智能合约（例如以太坊）进行金融活动。DeFi 的愿景是将一切都**数字资产化，使其自由开放地在全球市场上进行交易**，而 DeFi 代币则是这些去中心化金融交易所或项目发行的代币，代币的持有者可从平台生态发展中获得收益。目前，DeFi 币主要包括抵押借贷、去中心化平台、衍生品平台三种。抵押借贷协议中最知名的是 Maker DAO，它是基于以太坊区块链的去中心化的自治组织和智能合约系统，包含稳定币 DAI 和治理代币 MKR 两种。去中心化交易平台（DEX）包括 dYdX、Uniswap 等。Chainalysis 于 2021 年发布的报告根据世界各国链上 DeFi 协议接收总额、链上 DeFi 存款数量、链上 DeFi 协议零售接收总额进行综合评分，并计算出各国 DeFi 采用指数（见表 2-15），发现世界各国**数字货币交易量排名与 DeFi 协议采用指数排名并不完全重合，而具备一定的差异性**。

本报告认为，美国在去中心化金融（DeFi）领域的采用率最高，主要因为几个因素。首先，美国拥有全球最成熟的金融市场和强大的技术基础设施，这为 DeFi 平台的创新和推广提供了坚实的土壤。其次，美国的风险投资环境非常活跃，许多科技公司和创业者在这里寻找资金支持，推动了 DeFi 项目的快速发展。此外，美国的金融法规虽然相对严格，但也促使许多公司和机构在合法合规的框架下开发创新产品，进一步推动了 DeFi 的应用和普及。最后，美国的科技文化和金融意识也使得投资者和消费者对新兴的金融技术充满了热情和接受度，这使得 DeFi 产品在这里得到了广泛的尝试和应用。

本报告认为，越南在去中心化金融（DeFi）领域的采用指数排名第二，主要是由于几个关键因素。首先，越南的金融服务传统上以现金交易为主，金融科技和数字货币的普及为用户提供了更便捷的金融服务，吸引了大量对 DeFi 感兴趣的用户。其次，越南年轻人口众多，科技接受度高，数字货币和 DeFi 产品的创新和灵活性符合这一群体的需求。再者，越南政府对区块链技术和数字货币表现出积极的态度，推动了相关技术的应用和发展。最后，越南的高通货膨胀率和金融系统的局限性使得人们对去中心化的金融解决方案有更高的需求，DeFi 产品在提供更高的透明度和金融自由度方面显得尤为吸引人。这些因素共同推动了越南对 DeFi 产品的广泛采用。

总而言之，本报告认为 DeFi 协议打破了世界各国货币交易的壁垒，推动了世界各国的货币国际化。首先，在中国 P2P 平台相继被关停、美国的 Lending Club 等 P2P 平台需要上传社保账号进行 KYC 认证的大背景下，基于 DeFi 协议的区块链借贷，**能够打通跨国借贷的壁垒**。其次，币安、OKex 等中资背景的数字货币交易所均要求中国公民上传身份证及人脸识别后方可交易，且在数字货币存入及取出时需要缴纳高额手续费，还存在一定的“平台跑路”风险，而基于 DeFi 协议的去中心化交易所，基于智能合约进行币币兑换，**风险与交易成本均有所降低，有利于提高数字货币的流动性**。

表 2-15 2021 年世界各国 DeFi 采用指数排名

排名	国家	DeFi 采用指数
1	美国	1.00
2	越南	0.82
3	泰国	0.68
4	中国	0.62
5	英国	0.60
6	印度	0.59
7	荷兰	0.55
8	加拿大	0.52
9	乌克兰	0.49
10	波兰	0.46
11	法国	0.46
12	澳大利亚	0.41
13	土耳其	0.40
14	瑞士	0.38
15	俄罗斯	0.36
16	阿根廷	0.34
17	巴西	0.32
18	葡萄牙	0.31
19	中国香港	0.30
20	多哥	0.30

数据来源：https://blog.chainalysis.com/reports/2021-global-defi-adoption-index/

2.4 数字货币的信用基础

虽然数字货币产业发展迅速，同时在和各类新型数字技术交叉融合发展中展现出独有的特性，但目前仍有部分批评者对数字货币，特别是私人数字货币或加密货币的价值，及其背后的信用基础有所质疑。巴菲特于 2020 年在接受 CNBC 采访时认为，“加密货币基本没有任何价值，他们不生产任何产品[6]”。2023 年，美国总统拜登向国会提交的年度经济报告也对数字资产的好处提出了重大质疑，并对加密资产的价值提出质疑。他在报告中提出，“事实上，迄今为止，加密资产似乎并没有提供任何基本价值的投资，也不能作为法定货币的有效替代品，改善金融包容性或提高支付效率；相反，他们的创新主要是为了支持加密资产的价格而人为地制造稀缺性——而且其中许多没有基本价值[7]”。

央行数字货币由中央银行发行，信用基础来源于国家信用背书，与国家法定货币价值等同，且能够进一步推动法定货币的便捷化、数字化。而私人数字货币基于密码学算法发行，其中稳定币类似于不受监管的银行，一般具有一定的储备资产支撑其币值兑换汇率稳定，其信用基础来源于币值稳定及其背后所挂钩的资产价值。

而没有准备金的私人数字货币，在背后大多没有实物资产支撑，其信用基础有所不同。本报告认为，比特币、以太坊

[6] Warren Buffett: Cryptocurrency ‘has no value’ – ‘I don’t own any and never will’, https://www.cnbc.com/2020/02/24/warren-buffett-cryptocurrency-has-no-value.html

[7] White House blasts digital assets in new report, sees little value in crypto, https://www.theblock.co/post/221815/white-house-blasts-digital-assets-in-new-crypto-report?modal=newsletter

等背后大多没有实物资产支撑的私人数字货币，其信用支撑主要来源于以下几个方面：首先，私人数字货币的信用基础来源于**技术驱动的稀缺性**，比特币总量上限 2100 万枚，且比特币“挖矿”产量每 4 年减半，因此比特币是一种倾向于通货紧缩、越来越稀缺的货币。比特币诞生的历史背景即是 2008 年金融危机以来，美国超量化宽松政策所导致的货币贬值。部分学者认为，比特币一定程度上具备黄金的特征，可以被认为是“数字黄金”或“黄金 2.0”（Baur & Hoang, 2021）。不过，虽然比特币与黄金、白银等商品货币一样有一定的货币特征，但是不同于央行数字货币，无法进行货币政策调控。而且，以比特币为代表的私人数字货币也与黄金存在一定的差异性。因为比特币相较于黄金，可以进一步细分的程度更高。一个比特币被细分为 100,000,000 个聪，这意味着每个聪相当于比特币的十亿分之一。所以和黄金不同，比特币也不一定通货收缩，仍然可以满足交易需要，仅仅是计量单位会不断收缩，即比特币存在内生的货币供给。

其次，本报告认为私人数字货币的信用基础还来源于**投资者和使用者的信仰**。换言之，已经有足够多的投资者和交易者加入到私人数字货币。奥地利学派的鼻祖 Carl Menger 认为，货币可以在没有政府干预的情况下进化。他提出，货币单位是从一个过程中自发产生的，在这个过程中，经常交易的商品逐渐成为一种普遍接受的交换媒介（Menger, 1892）。这种社会协调不需要任何正式的决策或立法决定，而是可以由已经存在的需求引发。此外，还有很强的网络效应。使用特定交换媒介的市场参与者越多，这种媒介提供的效用就越大；也就是说，交换媒介的主导地位具有自我强化效应 (Kiyotaki, N., & Wright, R., 1989; Kiyotaki, N., & Wright, R., 1993)。换言之，被最广泛接受和最能长期保持价值的商品将成为货币。货币之所以有用的最重要的原因在于，只要别人觉得它有用，只要别人愿意接受它，它就起作用了。更进一步，从博弈论的视角，如果一种商品有足够多的支持者信仰，它将成为一种货币。哈耶克在《货币的非国家化》中，也提出反对国家控制货币发行，支持转而由私人发行货币。这一论断也为上述私人数字货币的价值提供了理论支撑。

从货币的三大职能分析，显然以比特币为代表的私人数字货币能够较好地适合网络时代，满足支付手段功能，交易者不再需要像纸币一样当面交易，也不再需要类似于电子支付需要一个中心化的中介机构确定核对数字化支付指令，而是能够在一个去中心化的系统中实现匿名化支付需要。不过，从财富存储和价值尺度的角度分析，以比特币等没有准备金支撑的私人数字货币价格波动过大，无法用于长期价值存储，也难以用于衡量真实世界的商品价格。而稳定币能够较好地满足上述需要。

2.5 小结

综上所述，本章基于全球视角对私人数字货币、央行数字货币、数字资产的发展现状进行了国别比较分析，还进一步讨论了数字货币与各类新兴数字技术的创新融合发展。具体而言，在私人数字货币部分，本章首先对比特币、以太坊等主流原生代币的国别发展现况进行了分析，并解读了不同国家采用数字货币程度不同的背后原因。此外，本章还对稳定币的国别发展现状进行了分析，探讨了总市值前十的稳定币总部所在国的差异及其背后因素，讨论了美国稳定币监管政策的动态和中国香港地区发展稳定币产业的潜力及其未来发展趋势对人民币国际化的潜在影响。最后，本章还进一步对主流平台币的技术特征、发行机构所在国的差异及其背后因素进行了讨论。在央行数字货币部分，本章进一步对目前主流的央行数字货币的进展及其发行背后的动机进行讨论。在数字资产部分，本章则进一步介绍了 DeFi 协议的特点，分析了各国 DeFi 采用指数存在差异的原因。最后，本章对各类新兴数字技术或数字货币所衍生的技术应用场景，如智能合约、元宇宙、Web3.0、人工智能等赋能数字货币创新产业发展的具体途径和动能进行了国别比较分析，对这些技术融合领域发展较好的国家和地区进行了总结分析。

第三章
全球数字货币对经济体系的影响

第三章
全球数字货币对经济体系的影响

3.1 数字货币对金融体系的影响

3.1.1 私人数字货币对货币国际化的影响

比特币等私人数字货币去中心化与难以监管的特征使其成为跨国虚拟经济的最佳媒介，常搭配比特币混淆器等高匿名工具用于走私、毒品贩卖、人口拐卖等线下非法交易黑市。不过，**比特币币值波动的特征使其在合法的虚拟经济中，反而不具备优势**。因此，USDT（美元泰达币）等稳定币能够在满足数字货币交易去中心化需求的同时，保障交易双方的**币值稳定性**，从而在各种虚拟商品的购买中，成为主流，如各类 NFT 艺术品购买、虚拟号码购买、数字平台会员购买、教育邮箱购买等。而上述数字商品使用美元计价的 USDT 购买的主流现实情况，又进一步加大了在新一代去中心化数字经济体系中**美元作为锚定货币的既有地位**。Tavabi et al（2019）使用爬虫技术爬取 80 多个暗网论坛的语料库，并基于人工智能方法，使用潜在狄利克雷分配 (LDA) 算法和非参数 HMM 算法进行建模统计后发现，84.7% 的暗网用户是男性，仅 9.4% 的暗网用户是女性。此外，他还对世界各国的每日平均暗网用户数量进行了统计（见表 3-1），发现**美国拥有最多的暗网用户数量及比例，其次是德国和印度**。值得注意的是，统计表中并未包含中国的数据，本报告认为，这可能是因为该研究者仅统计了英文语料库，而尚未对中文暗网论坛的语料数据进行分析统计。

不过，随着欧元、人民币等货币的逐渐崛起，发行 USDT 的 Tether 公司也发行了相应的欧元泰达币（EURT）、离岸人民币泰达币（CNHT）、墨西哥比索泰达币（XMNT）等。根据 Tether 公司 2023 年 7 月最新发布的透明度报告（见表 3-2），目前 USDT 总流通量为 833 亿美元，而欧元泰达币和离岸人民币泰达币仅为 3638 万欧元和 2050 万人民币，发行量相较于 USDT 远远不及，**仅可作为稳定币交易的补充，尚未能够对数字货币交易市场中美元作为锚定货币的既有格局带来挑战**。此外，美元泰达币在波场的 Tron 网络、以太坊的 Ethereum 网络、Solana 网络、比特币的 Omni 网络等**众多区块链主链上均有发行，具有最高的兑换兼容性**。

表 3-1 世界各国每日访问暗网平均用户数量统计表

国家	每日平均用户数量
美国	467,982(19.69 %)
德国	283,997(11.95 %)
印度	102,554(4.32 %)
印度尼西亚	92,715(3.90 %)
法国	91,667(3.86 %)
俄罗斯	89,891(3.78 %)
芬兰	85,092(3.58 %)
荷兰	69,416(2.92 %)
英国	61,458(2.59 %)
埃及	50,612(2.13 %)

数据来源：Tavabi et al（2019）研究论文

表 3-2 泰达币各币种流通量排行表

货币种类	USDT	EURT	CNHT	XMNT
Tron 网络	$43,118,788,997	无	无	无
Ethereum 网络	$38,301,860,819	€ 36,385,896	¥5,503,468	$19,562,400
Solana 网络	$859,056,690	无	无	无
Omni 网络	$237,944,877	€ 1,443.99	¥15,000,000	无
其他	$860,414,101	无	无	无
发行总量	$85,820,856,434	€ 36,387,340	¥20,503,468	$19,562,400

数据来源：泰达币官方

3.1.2 央行数字货币对货币国际化的影响及其国别发展经验

不少学者认为，央行数字货币的推行能够推动该国的主权货币国际化。Cong & Mayer（2022）基于两国博弈模型对法定货币、加密货币和央行数字货币的动态全球竞争进行模拟发现，通过推出央行数字货币，**弱势货币可能会挑战强势货币的主导地位**。如果它对强势货币的主导地位构成威胁，那么弱势国家发行央行数字货币也会增加强势国家推出央行数字货币的动力，从而产生央行数字货币发行的战略互补性。美国战略与国际研究中心 2022 年 4 月的研究报告也同样指出，中国的数字人民币计划强化了美国、欧盟、日本等国政府对央行数字货币的兴趣 。此外，美国拜登政府正在加强对中国数字人民币计划的审查，因为担心该计划可能会推翻美元作为全球主要储备货币的地位。Shen(2022) 更进一步利用平滑转换自回归（STAR）模型和非线性时变参数随机波动向量自回归（TVP-SV-VAR）模型，实证分析了数字人民币、人民币国际化和国际货币体系发展之间的关系。结果表明，数字人民币与人民币国际化之间的关系是时变的，在不同的经济情况下，上述关系存在显著差异。**数字人民币可以促进人民币国际化，从而有助于国际货币体系的多样化**。

从技术原理维度分析，本报告认为，数字货币能够促进货币国际化的原因在于，首先数字货币跨越时空的特性使得跨境支付结算更加便捷。相较于传统纸质货币，数字货币能够以更快更高效的速度完成结算，因此有利于其推广。其次，若数字货币使用区块链技术，其去中心化的特征将使其在治理结构上更加民主，还能够基于跨链技术展开币币结算，绕开 SWIFT 等中心化结算机构，从而获得更高的国际认可。最后，基于人工智能、大数据等技术，区块链能够更加高效、及时地调控货币供给，从而具备相较于传统货币更高的稳定性。

3.2 数字货币对居民消费的影响

从私人数字货币的角度观察，为提高数字货币的交易与支付便捷性，各类私人数字货币的移动支付工具也不断涌现，使得使用私人数字货币消费也越来越便利。出现这些工具的原因是，使用全节点接收和发送数字货币对普通用户而言存在一定难度，因而数字货币移动钱包应用程序不断涌现。而数字货币的数字支付工具分为中心化与去中心化钱包。中心化的数字货币钱包包括各种交易所钱包，如 Coinbase 钱包、Okex 钱包等，可用于交易所内快速币币交易以及与法币快速兑换，适用于短线数字货币投资者和中心化数字货币衍生品交易，交易所内交易手续费一般较低，但安全性也相对较低。因此，目前基于开源代码的去中心化钱包是私人数字货币大额长期存储的主流。目前以太坊钱包以 Metamask 为主，可以与 opensea 等各类 NFT 市场快速连接登录。其它通用型数字货币钱包包括 imtoken, tokenpocket 等，支持不同种类的数字货币。因此，在上述私人数字货币钱包的加持下，用户可以快速便捷地在保证匿名性的同时，便捷地消费。**在 APEXTO 平台，用户可以便捷地使用比特币购买挖矿服务器，在 Bamboo Card 平台，用户可以便捷地购买数字货币礼品卡**。

从央行数字货币的角度观察，央行数字货币本质上是现金的有效替代，一个国家的现金使用水平和趋势将影响对中央银行数字货币（CBDC）的需求。在现金使用量已经非常低的国家，对数字货币的需求将会疲软。在现金使用量非常高的地方，由于缺乏现金替代品，需求将会更强 (Khiaonarong and Humphrey, 2019)。相较于实物现金，央行数字货币存在明显优势。因为实物现金的存在对利率规定了一个下限，这使得负利率货币政策往往缺乏有效性。而中央银行数字货币的使用将有可能克服这一下限（Grasselli and Lipton, 2019）。此外，央行数字货币不仅可作为经济体储备政策的有效补充（Stevens, 2021），还将能够扩大农村地区获得现金和银行服务的能力（Alonso, 2020）。

新冠病毒的大流行进一步凸显了零售支付市场的低效率和央行数字货币的潜在益处（Cheng et al., 2021）。具体而言，如果 CBDC 被广泛接受用于交易，买家将持有更多的央行数字货币，增加买卖双方之间的交易量，进而导致更高的消费 (Keister and Sanches, 2019)。但是，个人对支付方式的偏好是异质的，不能完全由收入和年龄等人口特征来解释。为了在理论框架中充分理解引入央行数字货币对宏观经济和微观经济的影响，必须首先了解消费者的支付选择，因为央行数字货币将首先扩大家庭可用的支付和储蓄选择 (Koulayev et al, 2016)。

从中国的视角观察，2021 年 7 月 16 日，中国央行发布《中国数字人民币的研发进展白皮书》，央行数字货币发展正式进入发展的快车道。2020 年，中国的数字支付规模已达 249 亿元，**能够满足大部分普通用户的居民消费需要，因此部分批评者认为央行数字货币属于重复创新**。但央行数字货币与传统的数字支付仍然存在较大差异。支付宝和微信支付主要分为余额支付与快捷支付。余额支付的流程是，用户资金从银行个人账户转至支付宝或微信支付相应账户后再进行消费。而快捷支付则是资金通过银行中转。二者均需通过银行或金融机构中转，而数字人民币属于 M0，无需通过银行。因此数字人民币可靠性高于数字支付，不存在银行或机构挤兑风险，且数字人民币具有无限法偿性质，任何人不得拒绝接受，使得数字人民币未来的流通性和便捷性必然高于数字支付，也将更进一步推动居民消费。

而且，数字人民币主要采用国产加密算法 SM2 进行签名验证，而支付宝和微信支付在交易过程中使用美国国家安全局研发的 RSA 算法进行签名验证。数字人民币数据存储于中国人民银行授权的分布式账本，而微信支付和支付宝属于存储于中心化的私营企业服务器。2015 年 5 月 27 日，杭州市政建设工程导致四条大对数光缆中断，造成部分支付宝用户服务不可用。而数字人民币由于采用多个央行数字货币确权信息副本以供查询，从而能够有效防止上述宕机风险。因此，微信支付和支付宝的算法安全性与数据存储安全性也低于数字人民币。综上所述，**央行数字货币将给居民日常消费带来革命性变化，带来与微信支付、支付宝等传统数字支付工具完全不一样的体验**。

3.3 数字货币对跨境贸易结算的影响

央行数字货币即使只用于国内用途，也将超越国界。这使得不同央行发行的数字货币的协调工作至关重要，如果协调成功，央行数字货币将可能会被用来提高跨境支付的效率 (BIS Innovation Hub, 2021）。Auer 等（2021a）认为，发行央行数字货币（CBDC）可以缓解当前跨境支付的摩擦。具体而言，通过互操作中央银行数字货币（CBDC），形成多 CBDC（mCBDC）安排，将能够改善跨境支付效率低下的问题（Auer et al., 2021c）。Carstens(2020) 也认为，区块链技术应用于央行数字货币能够降低跨境支付的成本。

从具体技术角度分类分析不同类型数字货币对跨境贸易结算的影响。首先，以比特币为代表的传统私人数字货币具备完全去中心化的特征，在使用“混币”等方法进行的交易理论上可不受任何外部实体控制，并实现完全匿名化。目前，比特币在俄罗斯、朝鲜、伊朗等受美国为首的西方国家制裁的国家的进出口贸易结算，以及毒品、洗钱、恐怖主义等非法活动的跨境贸易结算中被广泛使用。但由于其运行不受政府控制，比特币等各类私人数字货币的发展并没有得到大多数国家的支持。此外，比特币币值的剧烈波动也使其不利于广泛用于合法的跨境贸易结算中，反而可能因比特币币值波动导致贸易公司出现巨额损失。

鉴于比特币在跨境贸易结算中的缺陷，币值稳定的加密数字货币——稳定币逐渐步入视野，稳定币一般基于智能算法或等价抵押物维持币值与法定货币的兑换比例，主流的稳定币包括 USD Tether（USDT）、USD Coin（USDC）、Binance USD（BUSD）等。其中，美元泰达币（USDT）**既不通过矿工挖矿生成，也不额外生成货币，甚至没有自己的主链，而是在以太坊、Sonala 等第三方区块链中，基于智能合约编程，采用中心化的方式以 100% 准备金发行数字货币**。用户可以通过 SWIFT 电汇美元至 Tether 公司提供的银行帐户，或通过 Bitfinex 交易所换取 USDT。赎回美元时，反向操作即可。目前，稳定币已广泛用于 Web3.0 世界的各类金融资产交易。 然而，稳定币用于跨境结算虽具备一系列优点，但其去中心化程度不如比特币[8]。此外，在国际贸易货币体系中，美元和欧元属于相对强势货币，而发行稳定币的科技公司大部分为西方国家的科技公司，稳定币也大多以美元作为锚定，美国将是稳定币运营模式下的赢家。从本质上看，稳定币是以国际强势货币为基础的信用衍生数字货币，同样存在国际强势货币驱逐本地弱势货币的问题，**以稳定币作为跨境贸易的结算货币，可能将进一步强化美元的优势地位**。

最后，目前新兴的多边央行数字货币桥（m-CBDC Bridge）项目也正通过各国央行在统一共享的标准“走廊网络”中发行存托凭证方式，替代本国数字货币的境外发行。境外使用国则以占有存托凭证为依托，在本国对应派生外币数字货币或信用货币。**在跨境贸易结算中使用多边央行数字货币桥，**

[8] 例如，泰达币官方可基于交易方是否存在违法行为，封禁特定泰达币用户所持有的稳定币。

可实现本国数字货币的境内外物理隔离，同时便于数字外币的境内监管，解决强势货币驱逐弱势货币的困扰，降低数字货币跨境运营的系统风险。“走廊网络”的存托凭证依托同一个分布式账本，无须通过复杂的代理行网络，可实现点对点的实时交易，显著提高结算效率。同时，“走廊网络”也支持以现有清算系统接入，给未推出数字货币的国家提供便利，适用范围得到扩展。这种模式不仅可以绕开受美国控制的 SWIFT 体系，且能对弱势货币国家的主权形成保护，有助于实现互惠互利的国际金融合作。不过，**该项目难点在于需要各国央行广泛参与并协同制定相关标准，否则可能会出现“多桥并行”的格局，从而限制项目的通用性**。

3.4 小结

综上所述,本章基于全球视角对私人数字货币和央行数字货币对货币国际化的影响进行了研究，具体而言，私人数字货币的匿名性质有益于跨国非法交易，而央行数字货币的推行能够推动该国的主权货币国际化。随后本章还进一步基于国别视角,对私人数字货币应用于暗网交易时,暗网交易中各国用户交易量的比例进行了统计分析，并讨论了各国暗网交易量存在差异的原因。最后，本章还进一步基于既有文献讨论了数字货币对于居民消费和跨境贸易结算的影响。

第四章
全球数字货币产业发展的风险与挑战

第四章
全球数字货币产业发展的风险与挑战

4.1 数字货币的技术安全与隐私泄露风险

虽然经过多年的发展，比特币等传统数字货币基于密码学原理的安全性已得到验证，但随着数字技术日新月异的发展，**数字货币的技术安全风险隐患仍然存在**。比特币的交易验证系统高度依赖于密码学的安全性，具体原理是对交易信息进行哈希运算得到交易摘要后，数字货币发送方使用私钥和椭圆曲线数字签名算法（ECDSA）对交易摘要进行加密后广播，随后全网中的任意全节点均可使用发送方公钥对加密后的交易摘要进行解密，并验证解密所得交易摘要是否与前述交易摘要相同，从而判定交易信息是否确是由拥有私钥的发送方发出。比特币主要使用椭圆曲线数字签名算法（ECDSA）对交易信息进行签名和验证，主要使用美国国家安全局（NSA）研发的哈希函数 SHA256 作为信息摘要算法。

然而，**近年来随着量子计算机的出现，Shor 算法[9]被认为可用于通过在假设的量子计算机上计算离散对数来破解比特币中的椭圆曲线密码学**。其中，使用 Shor 算法破解 RSA 算法需要 4098 个量子位和 5.2 万亿个 Toffoli 门才能获得 2048 位 RSA 密钥，这表明 椭圆曲线加密函数比 RSA 更容易成为量子计算机的目标。不过，所有这些数字都大大超过了任何曾经建造的量子计算机，并且估计这些计算机的创建需要十年或更长时间。理论上，一台 4000 qubit 的量子计算机可以在几秒钟内破解比特币的加密。

针对量子计算机对数字货币系统的可能破坏，密码学家提出全新的**格基密码学**，其主要目标是提供一种在量子计算机出现时仍然安全的加密和签名方案。它利用了格的结构和性质，这些结构可以看作是高维空间中的向量组成的网格。这些向量可以用来表示一些复杂的数学问题，这些问题在传统计算机上难以解决，在量子计算机上也是计算困难的。不过，清华大学助理教授陈一镭也在 eprint 发表工作论文[10]，进一步提出破解格密码的量子算法。总而言之，**数字货币的密码学算法与量子攻击算法正在互相攻防**。

从隐私泄露风险的视角观察，当下各类私人数字货币的匿名性使得其成为了一些非法活动的工具，例如洗钱、走私等。因此，隐私保护也是数字货币领域内一个备受关注的问题。虽然通过混币等技术，比特币理论上能够做到在隐私世界中的完全匿名，但鉴于区块链公链的技术特征，**一旦使用者的比特币地址公开或与真实世界身份相关联，其所有交易记录则完全公开**。

此外，一些新兴的数字货币项目，例如由 ChatGPT 创始人 Sam Altman 资助并由 Alex Blania 运营的 Worldcoin，其免费空投数字货币的附加条件是，为了加入 Worldcoin 的数字货币系统，用户必须交出眼球以供扫描采集信息。Worldcoin 使用眼球扫描来生成他们称之为“人格证明”的记录，根据该项目，这种凭证在未来将有许多未指定的应用。然而，眼球隐私数据高度敏感，涉及个人种族、个人健康、遗传信息等诸多高度敏感信息。

而且，大部分私人数字货币交易所，为满足监管机构合规要求，已要求注册用户进行 KYC 验证后方可进行数字货币交易或购买。如币安、OKex 等中资数字货币交易所，均需要用户在摄像头前持有本人身份证件进行**人脸识别验证**。Coinbase 等美资数字货币交易所，则一般也需要用户输入个人的社会安全号码 (SSN) 。相较于上述中心化、高度侵犯隐私的交易所，不需要任何个人认证信息、使用智能合约技术确保交易安全的 P2P 去中心化交易所，如 LocalBitcoins 等，则纷纷在各国监管机构打击下关闭。当下，除在部分数字货币交易合法的国家的街头 OTC 平台使用现金购买外，**匿名购买私人数字货币的渠道已越来越少，大部分用户一旦进入数字货币市场，其真实身份即被监管机构锁定**。

[9] 在经典计算机上，质因数分解是一个非常困难的问题，特别是对于非常大的整数。然而，彼得·肖尔的 Shor 算法却可以在量子计算机上以多项式时间复杂度完成质因数分解。具体而言，Shor 算法的时间复杂度是 O((log N)^3)，其中 N 是要分解的整数的位数。这意味着，对于足够大的整数 N，Shor 算法在量子计算机上能够以极快的速度完成质因数分解，而经典计算机则无法在合理的时间内完成相同的任务。

[10] Quantum Algorithms for Lattice Problems, https://eprint.iacr.org/2024/555.pdf

4.2 数字货币的市场波动与投机风险

相较于传统货币，数字货币还具备高度的市场波动性风险与投机风险。私人数字货币与股票等背后有实体经济支撑的投资品不同，往往**仅仅依靠其稀缺性和技术特征支撑其价格**。例如，比特币在 2020 年经历了从约 $5,000 上涨至超过 $20,000，随后又在 2021 年达到近 $69,000 的高峰，然后又在几个月内暴跌至 $30,000 以下，2024 年以来，随着比特币挖矿收益减半的到来，比特币又快速上涨至 $70,000 以上。使用比特币作为该国法定货币的萨尔瓦多，也因为比特币币值的高度波动性，导致其货币体系稳定性受到一定程度影响。此外，2022 年 5 月，号称与美元挂钩的稳定币 TerraUSD 与姐妹代币 Terra（即 LUNA）双双崩盘，造成高达 400 亿美元损失的加密货币领域大崩盘事件。上述案例均说明私人数字货币币值可能存在高度波动性。

4.3 数字货币的法律合规风险与监管不确定性

首先，全球对数字货币的**监管政策存在显著差异**。一些国家对数字货币采取支持和促进的态度，如瑞士和新加坡；而另一些国家则采取严格监管甚至禁止的立场，如中国和印度。不同的法律框架导致了跨国运营的复杂性和不确定性。

此外，数字货币交易平台和服务提供商必须遵守所在国的法律法规，包括反洗钱（AML）、了解客户（KYC）等合规要求。例如，美国的 FinCEN 规定数字货币交易所需要进行严格的 KYC 和 AML 程序，否则可能面临罚款或运营禁令。而且，**数字货币在各国的法律地位也不尽相同**，有的国家将其视为货币，有的视为资产或证券。这种分类上的差异会影响税收、交易和法律诉讼等方面的处理方式。例如，美国证券交易委员会（SEC）将某些数字货币视为证券，因此受《证券法》监管。

从**交易合法**性的视角观察，在某些国家，数字货币的交易可能处于法律的灰色地带，甚至可能被视为非法活动。例如，中国在 2021 年宣布全面禁止数字货币交易和挖矿活动，导致相关企业和投资者必须迅速调整策略。从**合规成本**的视角观察，合规要求增加了交易平台和企业的运营成本，包括合规人员的聘用、合规系统的建设、持续的法律咨询等。尤其是在多国运营的情况下，不同地区的合规要求可能互相冲突，进一步增加了运营复杂性和成本。

基于上述分析，数字货币还面临各类**监管不确定性风险**。例如，监管政策的突变风险，即政府和监管机构可能会根据市场变化、社会影响和安全问题突然调整对数字货币的政策。这些调整可能导致市场剧烈波动，投资者和企业的策略需要迅速调整。例如，2018 年韩国政府突然加强对数字货币交易的监管，导致市场大幅波动。

此外，**新法规的出台**可能要求数字货币企业和交易平台进行重大的业务调整。例如，欧盟的《加密资产市场法案》（MiCA）将对数字货币市场带来广泛的影响，包括增加合规负担和透明度要求。而且，**执法力度不确定性**也是重要的风险因素之一，因为即使法律法规已经出台，其执行力度和方式也可能存在较大差异。这种执行上的不确定性会导致企业在合规上的困惑和风险。例如，印度虽然讨论数字货币监管多年，但执行细则仍然不明确，给市场参与者带来了困扰。

最后，数字货币还存在**跨境监管冲突和跨国协调的不足**。例如，美国和欧盟的数字货币法规可能存在冲突，企业必须遵循多重监管要求，增加了合规难度和法律风险。而且，目前全球尚未形成统一的数字货币监管标准，不同国家的监管政策各异，给跨国交易和投资带来了复杂性和风险。国际合作和协调的不足，使得数字货币市场面临不同国家政策变化带来的不确定性。

4.4 数字货币的可拓展性风险

比特币的货币生成系统是基于 POW（工作量证明）机制，矿工通过算力竞争获得记账权，并获取交易费收入和比特币奖励。该机制主要通过 SHA256 函数实现。SHA256 不论输入的数字信息长度多少，最后均会输出长度固定 256bit 的字符串。且若输入的信息稍有不同，它们几乎必然对应到不同字符串。因此，比特币的发行机制为，矿工使用 SHA256 函数对包含有自身获得比特币奖励和手续费的一系列全网交易信息进行运算，若某位矿工能首先使得输出的字符串前 N 位字符为 0，则该矿工获得记账权，包含矿工奖励的交易信息被加入到新的区块内。N 由全网算力决定，比特币网络每 2016 个区块产生后调整一次，以确保系统平均每 10 分钟产生一个区块。

因此，基于上述分析，比特币 POW 机制**存在耗电量大、验证过程复杂、交易成本高、记账拥挤等问题**。在比特币运行早期，部分程序员使用普通个人电脑的算力即能赢得记账权，并挖矿获取大量比特币。但随着比特币价格的上涨和更多投资者的进入，比特币挖矿难度逐年攀升，2010 年 8 月 16 日仅为 511T。至 2021 年 5 月 21 日，增长至最高点，共增长 490 亿倍（图 5）。根据剑桥大学综合计算矿机综合效率

和综合电力效率而估算出的当前算力水平下比特币挖矿年电力消耗量 CBECI（Cambridge Bitcoin Electricity Consumption Index，剑桥比特币电力消耗指标），比特币年耗电估值从 2014 年 12 月 1 日的 2.12TWH 增长至 2021 年 5 月 13 日最高点的 143.85TWH，增长了 67.85 倍。

此外，比特币有限的区块大小限制了将智能合约应用于比特币，导致其可拓展性有限。传统区块链（如比特币）的区块大小和生成速度有限，通常比特币的区块大小为 1MB，平均每 10 分钟生成一个新区块，这意味着每秒只能处理大约 3 到 7 笔交易。这种限制导致在交易量激增时，网络处理能力不足，形成交易积压。与其相对的是，以太坊可拓展性更高，处理速度更快。目前，以太坊的 tps 约为 15-20。这意味着以太坊每秒最多能处理约 15-20 个交易。但数字货币存在的**不可能三角**[11]，使得在保障安全性的同时，处理速度越快、拓展性越高的数字货币，其去中心化程度也越低。例如处理速度相较于以太坊更快、可拓展性更高的 Solana，虽然任何人都可以运行 Solana 节点，但由于 Solana 需要高性能硬件，验证者通常会从私营数据中心租用服务器来运行其节点，因此大多数区块链上的大部分计算都是在大型数据中心的私人服务器上完成的，也导致 Solana 的去中心化程度不如比特币及以太坊，一定程度上存在大型节点过度控制的问题。

4.5 小结

本章从技术安全与隐私泄露风险、市场波动与投机风险、法律合规风险与监管不确定性、可拓展性风险四个角度对**数字货币产业发展的风险**进行了总结分析。首先，对于技术安全与隐私泄露风险，随着数字技术日新月异的发展，数字货币的技术安全风险隐患仍然存在，且数字货币的密码学算法与量子攻击算法正在互相攻防，而一些新兴数字货币项目和数字货币交易所需要在认证环节中进行人脸识别验证，导致存在隐私泄露的风险。其次，对于市场波动与投机风险，私人数字货币与股票等背后有实体经济支撑的投资品不同，往往仅仅依靠其稀缺性和技术特征支撑其价格，数字货币币值存在高度波动性。此外，对于法律合规风险与监管不确定性，全球对数字货币的监管政策存在显著差异。一些国家对数字货币采取支持和促进的态度，如瑞士和新加坡；而另一些国家则采取严格监管甚至禁止的立场，如中国和印度。不同的法律框架导致了跨国运营的复杂性和不确定性。最后，对于可拓展性风险，比特币 POW 机制存在耗电量大、验证过程复杂、交易成本高、记账拥挤等问题，比特币有限的区块大小还进一步限制了将智能合约应用于比特币，导致其可拓展性有限，也使得数字货币领域的不可能三角持续存在。

[11] 区块链不可能三角是以太坊创始人 Vitalik Buterin 提出的一个理论，指的是区块链网络无法同时实现安全性、去中心化和可扩展性。

第五章
全球数字货币监管制度的国别比较分析

第五章 全球数字货币监管制度的国别比较分析

5.1 数字货币的司法界定

如何界定私人数字货币的性质是数字货币监管的重点。在司法实践中，中美两国对私人数字货币的定位存在一定差异。2013 年，中国人民银行、工业和信息化部、中国银行业监督管理委员会发布《关于防范比特币风险的通知》，提出“**比特币应当是一种特定的虚拟商品，不具有与货币等同的法律地位**，不能且不应作为货币在市场上流通使用”[12]。与中国的监管政策不同，美国在不同判例中将数字货币分别定义为证券和货币[13]。

在美国司法实践中，判定数字货币是否是证券主要根据 Howey 测试，豪威测试是美国最高院在 1946 年的一个判决（SEC v. Howey）中使用的一种判断特定交易是否构成证券发行的标准。如果被认定为证券，则需要遵守美国 1933 年证券法和 1934 年证券交易法的规定。Howey 测试指出，投资合同是指合同、交易或计划，其中一个人将其资金投资于一家共同企业，并期望仅从发起人或其他人的努力中获得利润。第九巡回法院“将 Howey 的定义提炼为三部分测试，要求 (1) 投资 (2) 共同企业 (3) 并期望通过他人的努力产生利润。”

在美国司法实践中，判定数字货币是货币主要是因为有益于判定数字货币相关的洗钱非法行为[14]。在美国政府诉哈蒙案 [United States v. Harmon, 2021 U.S. Dist. LEXIS 73504, 2021 WL 1518344] 中，法院在仔细研究“货币”一词的普通含义以及哥伦比亚特区货币传输法（District of Columbia's Money Transmitters Act，MTA，哥伦比亚特区地方法典编号 D.C. Code § 26-1023）的法定历史和结构后，认为“比特币符合 MTA 下的货币定义条件”，因为虽然 MTA 从未定义“货币”的概念。但当法规未提供定义时，法院通常赋予法规术语其通常含义。首席法官 Beryl A.Howell 认为，一般术语“货币”通常表示交换媒介、支付方式或价值储存，而比特币就是这些东西。此外，MTA 将资金转移定义为“从事接收资金以进行转移或在美国境内转移资金的业务，或通过任何和所有方式转移到国外地点，包括但不限于支付工具、电汇、传真或电子转账。”

美国法院在上述两个判例中分别将两种数字货币——比特币视为货币、ABTC 代币视为证券。二者将极大地强化了美国政府对数字货币的监管。由于美国的司法体系主要为判例法，因此上述判例将为今后美国数字货币创新监管带来极大影响。针对利用数字货币项目非法集资，美国法院主要利

[12] 例如，杭州互联网法院在《陈某诉浙江某通信科技有限公司网络购物合同纠纷案》中，依据上述公告确认了比特币的商品属性，并确认适用于《消费者权益保护法》中所述的商品七天无理由退货制度。

[13] 例如，在美国证监会诉 NAC 基金会案 [SEC v. NAC Found., LLC, 2021 U.S. Dist. LEXIS 4079, 2021 WL 76736] 中，区块链开发公司 NAC 基金会及其首席执行官 Marcus Rowland Andrade 通过“首次代币发行”（“ICO”）成功筹集了数百万美元。美国政府因此随后采取了两项执法行动：对 Andrade 进行电汇欺诈和洗钱的刑事起诉，以及由美国证券交易委员会（“SEC”）提起的民事诉讼，指控欺诈性和未注册的数字证券销售违反了 1933 年证券法和 1934 年证券交易法，而后者的法律依据是被告 ICO 代币符合 Howey 测试的三项原则。

[14] 例例如，美国政府诉哈蒙案 [United States v. Harmon, 2021 U.S. Dist. LEXIS 73504, 2021 WL 1518344] 中，被告被指控串谋洗钱，非法转移涉及刑事犯罪的资金，以及经营无牌汇款业务。被告涉嫌在 2014 年至 2017 年间经营在线服务 Helix 以作为比特币混淆器（Bitcoin Tumbler）。该混淆器使得客户发送至 Helix 的比特币的识别信息被剥夺，从而隐藏比特币的来源及所有者。法院认为，被告在没有许可证的情况下从事损益资金额度与识别确认法（美国法典编号：26 U.S. Code § 1001）第（10）款中定义的汇款业务，违反了哥伦比亚特区货币传输法（District of Columbia's Money Transmitters Act，MTA，哥伦比亚特区地方法典编号 D.C. Code § 26-1023）。被告则试图驳回非法货币传输的指控，辩称比特币不是 MTA 定义下的“货币”，并且比特币混淆器也不是《禁止无证货币传输业务法》（美国法典编号：18 USCS § 1960）定义下的货币传输业务。法院则在仔细研究“货币”一词的普通含义以及 MTA 的法定历史和结构后，认为“比特币符合 MTA 下的货币定义条件”

用上述判例中的 Howey 测试对数字货币是否为证券进行认定。现行的数字货币中，比特币、以太坊已被美国证监会认定为不属于证券，因而不需要接受美国证监会的监管，而包括 Telegram、Block.one 在内的众多区块链公司的 ICO 仍难逃被界定为证券的命运，被迫妥协或进行和解。不同于美国区别对待不同形态数字货币的做法，中国目前主要采取“一刀切”的做法。2017 年 9 月，中国人民银行、中央网信办、工业和信息化部等发布《关于防范代币发行融资风险的公告》，明确指出“本公告发布之日起，各类代币发行融资活动应当立即停止”。例如广东省高院 2020 年“郝铃声等集资诈骗案”的判决即是根据《中华人民共和国刑法》第一百七十六条和上述公告，将被告人发行的“LCC 影视区块链虚拟货币”以及“PTO 珠宝区块链虚拟货币”视为集资诈骗。禁止一切代币发行活动虽然能够短期内遏制利用数字货币开展的非法集资活动，但实际上，基于区块链技术的数字资产创新项目与数字货币项目之间存在一定相似性与易混淆性，使得对区块链创新项目监管容易出现偏差。例如，蚂蚁金服区块链部门负责人张辉 2019 年 5 月 2 日在出席第三届“区块链商业峰会”（BoB）时提到，蚂蚁金服正在探索如何以“某种形式的代币”（some form of a token）在区块链上发行数字资产。但随后蚂蚁金服又辟谣称张辉所说的“some form of token”不是代币。因此，在现阶段应尽快制定类似于美国 Howey 测试的类似数字货币、数字资产判定标准，使得相关法律法规的实施既不阻碍区块链金融创新，同时又能有效防范有关个体利用数字货币开展非法集资活动。

在中国司法实践中，目前尚未有涉嫌提供比特币混淆器服务的相关案例，相关法律法规较为缺失。比特币作为交易信息完全公开的数字货币，其匿名性主要依靠比特币混淆器实现。在打击利用比特币进行非法交易的过程中，比特币混淆器是重要的一环。根据《中华人民共和国反洗钱法》规定，“本法所称反洗钱，是指为了预防通过各种方式掩饰、隐瞒犯罪所得及其收益的来源和性质的洗钱活动，遏制相关违法犯罪活动，依照本法采取相关措施的行为”。因此，若仅将比特币视为虚拟商品，或不单独出台针对数字货币混淆器的专门法律，将难以根据《反洗钱法》对经营比特币混淆器业务的个体加以法律制裁。目前，仍处于运营状态的主流比特币混淆器包括使用俄罗斯主机运营商 REG.RU LLC 注册的 Kutbit，利用西班牙后缀域名 es 注册的 Coinmixer，澳大利亚海外领地科科斯群岛后缀域名 cc 注册的 Bitblender 和在香港域名服务商“时代互联国际有限公司”注册的 Chipmixer。因此，本报告建议在比特币混淆器领域应加强国际司法合作，同时中国立法部门应尽快出台相关法规，完善打击利用比特币混淆器进行洗钱活动的法律。

5.2 数字货币的非法交易监管

由于比特币在混淆器的帮助下实现的匿名性，比特币被大量用于勒索软件、毒品交易、性犯罪和恐怖主义犯罪等违法活动交易。针对利用数字货币开展违法活动交易，中美两国均根据相应法律和判例进行了严厉打击。大量黑客利用勒索软件对用户数据进行窃取或加密，并要求被勒索用户支付比特币赎金。由于比特币在混淆器的帮助下实现的匿名性，对勒索攻击行为人的追溯一般难以实现。目前中国尚未有针对勒索软件开发者提起诉讼的案例。但在美国的司法实践中，除少数案例最终抓捕到勒索软件开发者外，还有许多案例为受害者起诉相关服务器或电脑供应商因程序漏洞导致数据泄露[15]。

性犯罪和毒品犯罪中往往使用比特币交易。曾经最大的以比特币交易的暗网市场“丝绸之路”中，大部分交易与儿童色情或毒品犯罪有关[16]。由于国际社会对恐怖主义活动资金的打击，比特币也日渐称为恐怖主义活动中常用的主流交易和捐款方式[17]。针对利用比特币等数字货币筹集资金以用于恐怖主义犯罪，中国等发展中国家目前立法与监管均相对缺失。境内恐怖主义团体利用比特币开展筹款的活动较为猖獗。例如，香港个别违法 Telegram 频道利用比特币筹款为逃亡海外的香港暴恐分子提供资金。针对此类违法犯罪行为，各国执法机关应学习美国经验，加大互联网卧底巡查，并依法没收暴恐分子违法资金。

当前，中国政府有关部门对数字货币、ICO 等金融类区块链活动进行了严厉打击。2021 年 9 月发布的《中国人民银行等关于进一步防范和处置虚拟货币交易炒作风险的通知》明确了虚拟货币相关业务活动属于**非法金融活动**，要求“金融机构和非银行支付机构不得为虚拟货币相关业务活动提供服务”，似乎已经在源头上完全斩断了境内企业和普通投资者参与数字货币交易的可能性。但实际上，上述监管策略没有对境内法人参与金融类区块链活动造成任何影响，反而进一步吸引了国内更多企业和普通投资者的关注。这也是中国人民银行在发布上述所谓“史上最严格”加密货币监管公告后，比特币价格曾一度大跌但随后又迅速回弹甚至反而在 2021 年 11 月历史性达到史上最高位的主要原因。本报告发现，三大交易所币安、火币和 OKex 中，OKex 未清退中国大陆用户，而仅需输入姓名和身份证号码进行认证后，即可进行每笔限额 2000 元人民币的数字货币购买，而 OKex 仅要求用户在 C2C 交易中使用微信支付或支付宝购买数字货币时保持微信支付姓名与认证姓名一致，即可完成交易。换言之，鉴于微信支付转账一般仅向对方显示姓名部分字符，若不法分子试图利用数字货币转移资产至境外或从事不法活动，完全可以使用多个与自己姓名类似的身份证进行账号认证，并多次少量购买后完成匿名性质的巨额资金转移。而币安和火币虽然声称将清退中国大陆地区用户，但普通用户仍可使用海外虚拟手机号码注册、注册海外离岸公司账户进行机构认证等操作规避监管，因此币安和火币中使用微信支付、支付宝及中国大陆地区银行卡购买数字货币的人民币交易区仍然交易异常活跃。而芝麻开门、Paxful、Local Cryptos 和 Local Bitcoins 等交易所，不仅存在人民币交易区，且认证门槛更低。部分交易账号甚至黑钱涌动，具体而言交易门槛越低，相应交易价格越高，存在所谓“**洗钱溢价**”的现象。

[15] 例如在 Blackbaud 数据泄露诉讼案 [In re Blackbaud, Inc., 2021 U.S. Dist. LEXIS 123355, 2021 WL 2718439] 中，原告声称，从 2020 年 2 月 7 日到 2020 年 5 月 20 日，网络犯罪分子精心策划了对 Blackbaud 系统的两部分勒索软件攻击（“勒索软件攻击”）。网络犯罪分子首先渗透到 Blackbaud 的计算机网络，复制原告的数据，并持有它以索取赎金。然后他们试图但未能阻止 Blackbaud 在 2020 年 5 月被发现后访问其自己的系统。Blackbaud 最终支付了以未公开数量的比特币支付赎金，以换取网络犯罪分子先前访问的任何数据将被永久销毁的承诺。被告 Blackbaud 争辩说，法院对原告的索赔缺乏事物管辖权，特别是声称未能充分声称他们的伤害可追溯到 Blackbaud 的行为。但最终的判决中，法院拒绝了 Blackbaud 的动议并判决 Blackbaud 对数据泄露负有责任。

[16] 在美国政府诉 Salaam 案 [United States v. Salaam, 2021 U.S. Dist. LEXIS 103119, 2021 WL 2217066] 中，被告 Salaam 曾试图通过比特币从美国色情分类信息网站 backpage.com 购买广告服务，以推广其非法的儿童色情服务和儿童色情制品。美国政府诉 Hagan 案 [United States v. Hagan, 766 Fed. Appx. 356, 2019 U.S. App. LEXIS 8839, 2019 FED App. 0144N (6th Cir.)] 中，Hagan 被控利用比特币通过“暗网”从各种海外供应商处大量购买毒品并分销给其它顾客。2020 年浙江省温州市中院“姜振泉走私毒品案”中，被告姜振泉通过比特币支付毒资向境外卖家订购毒品。2021 年浙江省诸暨市人民法院“谢彭等贩卖毒品案“中，被告通过 telegram 软件联系毒品订单，以比特币形式收取毒资向浙江各地买家出售在云南租赁土地种植的大麻。。

[17] 美国政府诉 155 虚拟货币资产案 [United States v. 155 Virtual Currency Assets, 2021 U.S. Dist. LEXIS 69035, 2021 WL 1340971] 中，美国政府声称通过在 Telegram、Facebook 等社交媒体平台卧底，发现了 155 个比特币地址与为外国恐怖主义组织 (FTO) 的实体募款有关。因此美国政府认为这些资金募集计划违反了《跨国恐怖主义法案》（美国法典编号：18 USCS § 2332b），并可根据《民事没收法》（美国法典编号：18 U.S. Code § 981）(a)(1) 与 (G)(i) 条款予以没收。法院引用美国政府诉 Harmon 的判例 [United States v. Harmon, 474 F. Supp. 3d 76, 80 (D.D.C. 2020)] 而将比特币视为去中心化的虚拟货币，因而将上述 155 个比特币地址所拥有的比特币视为资产，并判决予以没收。

5.3 世界各国对比特币的监管制度比较

美国监管机构，如证券交易委员会（SEC）和金融犯罪执法网络（FinCEN），在比特币的合法性、监管和税收方面建立了相对明确的框架。例如，SEC 将一些数字货币视为证券，并对相关产品进行严格监管。FinCEN 则要求数字货币交易所遵守反洗钱（AML）和了解客户（KYC）政策。此外，美国拥有庞大的加密货币交易市场， Coinbase、Kraken 等交易平台在全球具有重要影响力，且美国企业在比特币支付、借贷和区块链技术应用方面不断创新。然而，监管的不确定性和合规成本依然是挑战，尤其在税收处理和新产品审批方面。

欧盟对比特币的态度逐渐由谨慎转向支持，努力在促进创新和保护消费者之间找到平衡。欧盟通过《第五反洗钱指令》(5AMLD) 要求加密货币交易所和钱包提供商遵守严格的 KYC 和 AML 规定。此外，《加密资产市场法案》（MiCA）旨在为整个欧盟区内的加密资产提供统一的监管框架，促进市场的稳定和增长。一些欧盟国家，如德国，在比特币的法律地位和税收政策方面相对明确，并成为了加密货币和区块链技术发展的中心。瑞士的“加密谷”（Crypto Valley）吸引了大量的区块链初创公司和投资者，推动了本地经济和技术创新。

亚洲国家对比特币的态度较为多样化。日本在 2017 年成为第一个将比特币合法化并作为支付手段的国家。日本金融厅（FSA）对加密货币交易所进行严格监管，以保护投资者利益和防止犯罪行为。韩国对加密货币采取了积极的监管态度，虽然早期曾考虑禁止，但最终选择了加强监管来确保市场透明和稳定。韩国还积极推动区块链技术在金融和公共服务领域的应用。然而，中国对比特币的态度最为严格，自 2021 年起全面禁止了加密货币交易和挖矿活动，导致许多矿工和交易所迁出中国。尽管如此，中国仍在积极推动央行数字货币（DCEP）的开发和测试，并将其作为全球支付体系中的关键创新。

拉美和非洲地区的比特币发展则主要受到经济环境和金融基础设施的影响。在拉丁美洲，一些国家如阿根廷和委内瑞拉，由于本地货币贬值严重，比特币成为了民众对抗通货膨胀和保护财富的重要工具。此外，2021 年萨尔瓦多成为全球第一个将比特币作为法定货币的国家，旨在促进金融普惠

和减少国际汇款成本。尽管这一举措备受关注和争议，但它标志着比特币在主权货币体系中的重要尝试。

在非洲，尤其是尼日利亚和南非，比特币的接受度也在上升，主要因为它提供了传统银行体系难以覆盖的金融服务。许多非洲国家民众利用比特币进行跨境汇款和支付，这不仅提高了金融包容性，还降低了交易成本。然而，监管环境相对滞后，许多国家尚未建立明确的政策框架。

在中东，比特币的发展受到各国政策和社会文化的影响。例如，阿联酋积极探索区块链和加密货币的应用，并逐步形成了支持创新的监管框架。迪拜国际金融中心（DIFC）和阿布扎比全球市场（ADGM）都制定了相关法规，以吸引全球区块链企业。然而，沙特阿拉伯和伊朗等国对加密货币则持谨慎态度，主要关注其潜在的金融稳定风险和对现有货币体系的冲击。

5.4 小结

本章首先将中美两国在法条和司法实践中对数字货币的司法界定进行了对比分析，同时由于比特币在混淆器的帮助下实现的匿名性，比特币被大量用于勒索软件、毒品交易、性犯罪和恐怖主义犯罪等违法活动交易。本章进一步就中美两国对数字货币非法交易监管的方式和法律途径进行了总结。最后，本章更进一步对世界各国的比特币的监管制度进行了比较。

总结

总结

展望与政策建议

本报告从历史和功能效用两个角度深入分析了数字货币的发展历程及其驱动因素，指出数字技术进步、生产方式变革和全球化背景是推动数字货币发展的关键因素。在用户端，数字货币不仅便利了在线支付和保护了隐私，还吸引了投资者，并支持跨境支付和数字服务购买，作为 Web3.0 生态系统的基础设施有着重要作用。宏观层面上，数字货币重塑了全球货币体系，对国际金融架构产生了深远影响，同时为面临金融制裁的国家提供了新的规避方案。

本报告还对私人数字货币、央行数字货币和数字资产的国别发展现状进行了比较分析，并探讨了数字货币与新兴数字技术的融合，特别是智能合约、元宇宙和人工智能等技术如何推动数字货币产业的发展。在私人数字货币方面，本报告分析了比特币、以太坊及稳定币的发展现状，并探讨了各国对这些货币的采纳程度和监管政策差异，尤其是美国与中国香港的稳定币监管动态及其对人民币国际化的潜在影响。央行数字货币部分探讨了主流央行数字货币的发展动机，而数字资产部分则介绍了 DeFi 协议的特点及各国采用差异。进一步分析集中于私人数字货币与央行数字货币对货币国际化的影响，指出私人数字货币的匿名性质有助于跨国非法交易，而央行数字货币则有助于推动主权货币的国际化。同时，本报告还就数字货币对居民消费和跨境贸易结算的影响进行了探讨。

在风险分析方面，本报告总结了技术安全与隐私泄露、市场波动与投机、法律合规与监管不确定性、以及可拓展性等四大风险，其中包括数字货币在隐私泄露、价格波动、全球监管差异和技术可拓展性方面的问题。最后，本报告对中美两国在数字货币司法界定、非法交易监管及全球比特币监管制度进行了比较分析，揭示了不同国家在数字货币领域的监管实践和法律途径。

展望未来，全球数字货币产业将继续经历深刻的变革和扩张。数字技术的不断进步和全球化背景下的经济变革将进一步推动数字货币的创新和应用。随着央行数字货币的逐步推出，主权货币的国际化进程将加快，可能会在全球货币体系中形成新的格局。这将促进跨境支付的效率提升，同时增强金融系统的包容性和安全性。私人数字货币和稳定币将在支付、投资和跨境交易中扮演越来越重要的角色，尤其是在数字资产和 DeFi 领域的应用将不断拓展。

然而，这些发展也将伴随技术安全、隐私保护、市场波动和法律监管等方面的挑战。随着各国监管框架的逐步完善和全球合作的加强，数字货币行业的风险管理将得到改善，同时技术的可拓展性和合规性也将得到提升。未来，数字货币与新兴技术如人工智能、智能合约、元宇宙等的融合将可能引领新一轮的技术革命，推动经济和社会的全面数字化转型。因此，全球数字货币产业的发展将不仅改变金融市场的格局，还将深刻影响国际经济体系的结构和全球经济的动态。

本报告认为，从数字货币产业政策的角度，未来数字货币会出现原生代币、稳定币、央行数字货币长期共存的局面。比特币等私人数字货币中虽然存在大量非法交易，且不受监管部门控制，但只要有需求就会持续存在，难以被彻底消灭。而一部分稳定币会逐渐向监管部门靠拢，在纳入监管框架之后逐步进入全球数字支付体系。各大经济体，**应积极研发以自己货币为基础的稳定币或央行数字货币**，以拥抱数字时代新的发展需要，同时在数字经济新时代积极拓展本国货币在元宇宙世界、区块链世界中的支付比例，使其成为各类数字资产的锚定货币。基于智能合约技术调控央行数字货币发行，并将其与数字资产投资、跨国央行数字货币桥结合，拓展数字货币全球化。同时，还应当积极探索数字货币在数字经济与实体经济中的应用，推动元宇宙、数字制造、数字供应链等产业高质量发展。

从监管政策的角度，本报告认为各国监管机构“**堵不如疏**”，应该采取**引导而非完全禁止**的监管政策，保护普通投资者合理的投资需求，遏制跨境资本流动需求，严厉打击使用数字货币进行违法犯罪的需求。具体而言，监管部门应积极使用大数据技术与人工智能技术，监测私人数字货币流向，并与数字货币交易所合作共享 KYC 数据，实现一定程度的私人数字货币“监管后台实名化”，使得在满足投资者投资需求的同时，防范可能出现的各类私人数字货币实施洗钱等 违法犯罪风险。

总而言之，从数字货币产业发展的有利因素角度，随着全球数字经济和各类数字货币衍生产业的不断发展，以及数字货币和各类新兴数字技术的创新融合，都一定程度上推动了数字货币产业的可持续发展。但私人数字货币在**监管政策方面的不确定性**，以及各国在发展央行数字货币过程中**争夺货币国际化主导权**，都给未来数字货币产业发展带来较多不确定因素，需要政策制定者**加强国际协调合**作。

参考文献

[1].Eichengreen, B.(2019), “From commodity to fiat and now to crypto：What does history tell us?”, NBER Working Paper, No.25426.

[2].Bech, M.L. & R.Garratt(2017), “Central bank cryptocurrencies”, BIS Quarterly Review 22(3): 55-70.

[3].Auer, R. et al(2020), “Rise of the central bank digital currencies: Drivers, approaches and technologies”, BIS Working Papers, No.880.

[4].Lee, A. et al (2020), “Tokens and accounts in the context of digital currencies”, FEDS Notes, 2020-12-23.

[5].Auer, R. & R.Boehme(2021), “Central bank digital currency: The quest for minimally invasive technology”, BIS Working Papers, No.948.

[6].Boar, C. et al(2020), “Impending arrival - A sequel to the survey on central bank digital currency”, BIS Papers, No.107.

[7].Baur, D. G., & Hoang, L. (2021), “The Bitcoin gold correlation puzzle”, Journal of Behavioral and Experimental Finance, 32, 100561.

[8].Menger, Karl. "On the origin of money." The Economic Journal 2.6 (1892): 239-255.

[9].Kiyotaki, N., & Wright, R. (1989). On money as a medium of exchange. Journal of political Economy, 97(4), 927-954.

[10].Kiyotaki, N., & Wright, R. (1993). A search-theoretic approach to monetary economics. The American Economic Review, 63-77.

[11].Tavabi, N., et al (2019), Characterizing activity on the deep and dark web. arXiv. https://arxiv.org/abs/1903.00156

[12].Cong, L.W. & S.Mayer(2022), “The coming battle of digital currencies”, The SC Johnson College of Business Applied Economics and Policy Working Paper Series, 2022-04.

[13].Shen, C.(2022), "Digital RMB, RMB Internationalization and Sustainable Development of the International Monetary System" Sustainability 14, no. 10: 6228. https://doi.org/10.3390/su14106228

[14].Khiaonarong, T. & D.Humphrey (2019), “Cash use across countries and the demand for central bank digital currency”, IMF Working Papers, No.19/46.

[15].Grasselli, M.R. & A.Lipton(2019), “On the normality of negative interest rates”, Review of Keynesian Economics 7(2):201-219.

[16].Stevens, J.(2021), "Money creation in the modern economy: an appraisal", Review of Keynesian Economics 9(1):43-60.

[17].Alonso, S. et al(2020), "Detection of financial inclusion vulnerable rural areas through an access to cash index: solutions based on the pharmacy network and a cbdc. evidence based on vila (spain)", Sustainability 12(18):1-33.

[18].Cheng, J. et al(2021), “Preconditions for a general-purpose central bank digital currency”, FEDS Notes, 2021-02-24-1.

[19].Keister, T. & D.R.Sanches(2019), “Should central banks issue digital currency?”, Federal Reserve Bank of Philadelphia Working Paper, No.19-26.

[20].Koulayev, S. et al(2016), "Explaining adoption and use of payment instruments by us consumers", The RAND Journal of Economics 47(2):293-325.

[21].BIS Innovation Hub(2021), "Central bank digital currencies for cross-border payments", https://www.bis.org/publ/othp38.htm.

[22].Auer, R. et al(2021a), “Permissioned distributed ledgers and the governance of money”, BIS Working Papers, No.924.

[23].Auer, R. et al(2021c), "Multi-CBDC arrangements and the future of cross-border payments", BIS Papers, No. 115.

国际金融论坛（IFF）

国际金融论坛（IFF）是非营利独立的、非营利、非政府国际组织，2003 年 10 月由 G20 国家以及联合国、世界银行、国际货币基金组织等相关机构及领导人共同发起成立，是全球金融领域高级别常设对话机制和多边合作机构，被誉为全球金融领域的“ F20（Finance 20）”。

国际金融论坛（IFF）的目标是通过国际化、市场化、专业化的运营机制，建立全球经济、金融和公共政策领域战略对话、交流合作、实践创新、学术研究和人才培育平台，推动金融服务世界，促进全面可持续发展。

国際金融論壇

INTERNATIONAL FINANCE FORUM

Since 2003

IFF 微信公众号
微信号：IFFweixin

www.iff.org.cn
www.ifforum.org