

分类号: F832

单位代码: 10335

密 级: _____

学 号: 01130547

浙江大学

同等学力硕士学位论文



中文论文题目: 基于区块链技术的数字资产交易:案例分析视角

英文论文题目: Case Analysis of Digital Assets Transaction

Based on Blockchain Technology

申请人姓名: 郑佩娜

指导教师: 王义中

合作导师: _____

专业名称: 金融学

研究方向: 互联网金融

所在学院: 经济学院

申请人单位: 上海丙晟科技有限公司

论文提交日期: 2018年9月12日

基于区块链技术的数字资产交易：案例分析视角



论文作者签名: 郑佩卿

指导教师签名: 王义中

论文评阅人 1: 隐名评阅

评阅人 2: 隐名评阅

评阅人 3: 隐名评阅

评阅人 4: _____

评阅人 5: _____

答辩委员会主席: 邹小芃 教授 浙江大学

委员 1: 钱水土 教授 浙江工商大学

委员 2: 俞洁芳 副教授 浙江大学

委员 3: 李壑 副教授 浙江大学

委员 4: 张月飞 副教授 浙江大学

委员 5: _____

答辩日期: 2018年8月23日

Case Analysis of Digital Assets Transaction Based on Blockchain

Technology



Author's signature: Zheng Peina

Supervisor's signature: Tizhang Wang

Thesis reviewer 1: Anonymous reviewer

Thesis reviewer 2: Anonymous reviewer

Thesis reviewer 3: Anonymous reviewer

Thesis reviewer 4: _____

Thesis reviewer 5: _____

Chair: Zou Xiaopeng/Professor/Zhejiang University
(Committee of oral defence)

Committeeman 1: Qian Shuitu/Professor/Zhejiang Gongshang University

Committeeman 2: Yu Jiefang/Associate Professor/Zhejiang University

Committeeman 3: Li He/Associate Professor/Zhejiang University

Committeeman 4: Zhang Yuefei/Associate Professor/Zhejiang University

Committeeman 5: _____

Date of oral defence: August 23rd, 2018

致 谢

时光荏苒，转眼间已到毕业季，学习的时光感觉如此短暂，不知不觉就这样从指间飞逝，回顾这几年的研究生生涯，蓦然回首，心中无限感怀与感激。

毕业论文的准备，从开始就读研究生课程时，就时常留意相关前沿主题，收集各方面的资料与文献开始准备，但课题的最终敲定及成文，得感谢我们的导师——王义中教授！其开放的思想，严谨的教学态度，在本人论文撰写过程中，以其渊博学识，前瞻性的思维为本人的论文提供了宝贵的意见与撰写思路。

成文过程中，课题的新颖，文献的匮乏让我对此选题一直抱有较多的不确定性，但老师的鼓励与指引，让我勇于不断探索，结合工作中的相关经验，大胆创新，认真求证，以严谨的学术研究精神对论文中的相关理论、案例进行实证，求真！正是王义中老师给予的鼓励与指导，为我们提供了宝贵的学术经验，才得以论文成文过程中少走弯路！同时，也因为老师严谨的学术精神，让我们在成文过程中不敢懈怠，做到大胆假设，小心论证。在此次论文写作过程中，连续几个月的所有周末都在闭关写作，遇到问题及时与老师沟通，当面向老师或同学们请教，让自己写作思路更加开阔，成文效率大大提升。经过这段求学旅程，让我们保持不断学习与创新的精神，在未来工作、学习过程中，都将继续指引我们未来前进的方向。

同时，要非常感谢中门家园中，各位师兄妹的帮助，如陈丽芳博士、赵庭旭师妹、还有中门的各位同门，从开题报告开始到论文完成，小到不耐其烦地为我检查细节、校验格式、协助论文打印与提交，正是因为大家的一路相协相助，才让我可以更从容地面对并解决学业过程中遇到的困难与疑惑。

最后，再次衷心地感谢老师与同学们在学业过程中给予的帮忙与指引，公司同事与领导的支持；同时，也要感谢家人在背后默默的支持与理解，在这看似漫漫求学路中，备感温暖！非常感谢！

摘要

区块链技术近年来成为备受关注的热点技术，在全球范围内有大量资本涌入，并得以蓬勃发展，这一技术受到越来越多行业的青睐，得益于其去中心化、不可篡改等特点，正在加速应用到金融、经济、货币、法律、物流、艺术等领域。虽然这一技术备受关注，但其在发展过程中仍存在标准不统一、衍生市场混乱、安全性存在威胁及难以监管等问题，以至于目前在市场还鲜有区块链和实体商业对接的落地产品。本文着重研究基于区块链技术的数字资产交易原理及其在重点行业的应用分析，以便对其他行业的应用与复制提供参考。

通过“布比（北京）网络技术有限公司”（下文简称布比）这一平台作为切为点，分析该平台将区块链技术应用于数字资产交易过程中的具体案例，研究该技术在实际应用过程中更适合应用于哪些场景，这些场景如何应用起来，未来可能面临哪些问题，该如何解决这些问题等。通过本文的分析发现：（1）从公司战略来讲，布比专注于区块链技术和产品的创新，积极申请核心专利技术，定位于基于区块链技术的数字资产交易平台，通过提供标准化接口，便于开发者或其他公司快速接入，降低行业进入门槛。（2）从公司业务发展情况来看，布比已与几十家机构合作，将区块链技术应用于商业积分、游戏交易、保险卡单、股权债券、互助保险等行业，证明区块链技术在这些行业应用的可行性。（3）从公司技术能力来讲，在经过大量业务模型，应用模型的反复试验之后，布比凭借其过硬的技术能力，解决了区块链技术本身的一些技术瓶颈，在交易性能、数据存储、节点数据同步、吞吐量方面均实现了技术突破，为行业提供了创新经验。

由上述结论得到的启示是，要加速区块链应用的落地，一方面监管层要及时制定符合现有区块链技术应用的相关法律法规，营造有利于区块链高新企业发展的创业环境；另一方面，高新企业、高校与科研机构之间可以强强联合，重点攻克区块链技术发展过程中的重难点，强化技术标准，推动区块链应用落地。第三方面，借鉴布比现有商业模式，鼓励大企业大平台加大研发力度，提供开放、高效、拓展性强的区块链底层，降低中小企业区块链开发成本，进一步推进基于区块链技术的数字资产交易的应用。

关键词：区块链；数字货币；数字资产；分布式账本

ABSTRACT

Blockchain technology has become a hot topic in recent years. There are a large number of capital influx and flourishing development around the world. This technology is favored by more and more industries. It is accelerating the application to finance, law, logistics, art and other industries, thanks to its centralization and non-tampering. However, although this technology is famous, there are still problems on inconsistent standards, chaotic derivative market, the threat of case and the difficulties of supervising and so on. As a result, there are still few blockchain cases in the market. This paper focuses on the analysis of the blockchain technology based on the principle of digital assets trading and the application of key industries, in order to provide a reference for other industries of application and replication.

In this paper, we try to analyze the digital asset trading platform based on blockchain technology, through the case of “BUBI (Beijing) Network Technology Co., Ltd.”, and discusses the blockchain technology in the foreseeable future, which scenarios are more suitable for using this technique, how to apply these scenarios, what difficulties may be encountered in the future and how to resolve them? Through the analysis of this paper we founded:

First, Bubi focuses on the innovation of blockchain technology and build the digital asset trading platform, applies for core patent technology. By providing a standardized interface, it is convenient for developers or other companies to quickly access.

Secondly, Bubi has worked with dozens of organizations to apply blockchain technology to business integration, such as game trading, insurance, equity bonds, mutual insurance and other industries, to provide the feasibility of the application using blockchain technology.

Thirdly, from the company's technical ability, after a large number of business models and the repeated test of the application model, Bubi has solved some technical bottlenecks of blockchain technology by virtue of its excellent technical ability.

In conclusion, in order to accelerate the development of the blockchain technology. On one hand, the regulatory layer should promptly laws and regulations that meet the application of the existing blockchain technology in time. On the other hand, the high and new enterprises, colleges and research institutions can strengthen the union, focus on tackling key difficulties in the development of block chain technology, strengthening technical standards and promoting the application of block chains. At last, we should encourage large enterprises to increase research and development, provide an open, efficient and expansibility blockchain, and reduce the development cost of blockchain.. And further promote the use of digital asset transaction based on blockchain technology.

KEY WORDS: Blockchain; Digital currency; Digital assets; Distributed ledger

目 录

1 绪论	1
1.1 研究背景	1
1.2 研究意义	2
1.3 研究思路	2
1.4 研究方法	3
1.4.1 文献分析法	3
1.4.2 实证分析法	3
1.4.3 案例比较法	3
1.5 研究重难点与创新点	4
1.5.1 研究重点与难点	4
1.5.2 研究的创新点	5
2 国内外研究现状.....	6
2.1 关于区块链技术的相关研究	6
2.1.1 区块链相关定义	6
2.1.2 区块链技术的特征及意义	7
2.1.3 区块链技术相关产业应用研究	8
2.2 关于 Token 经济的研究	12
2.3 关于区块链技术在数字资产交易应用方面的相关研究	14
2.3.1 数字资产定义	14
2.3.2 基于区块链技术的数字资产交易相关研究	14
2.4 国内外研究述评	17
3 理论基础.....	18
3.1 区块链技术运作基本原理	18
3.2 区块链核心技术及特点	19
3.2.1 区块链核心技术	19
3.2.2 区块链技术特点	24
4 基于区块链技术的数字资产交易现状与问题	26
4.1 基于区块链技术的数字资产交易现状	26
4.1.1 加密数字货币交易现状	26

4.1.2 非金融领域数字资产交易现状	27
4.1.3 数字资产交易平台现状	29
4.2 基于区块链的数字资产交易存在的问题	30
4.3 基于区块链的数字资产交易的意义	32
5 基于区块链技术的数字资产交易的案例分析	34
5.1 布比数字资产交易平台简介	34
5.2 布比数字资产交易平台的商业模式	35
5.3 布比数字资产交易平台的技术架构及特色	37
5.3.1 布比数字资产交易平台技术架构	37
5.3.2 布比数字资产交易平台技术特色与优势	39
5.4 布比数字资产交易平台的应用案例	43
5.4.1 商业积分	44
5.4.2 保险卡单	47
5.4.3 网络互助	49
5.4.4 游戏交易	52
5.4.5 股权债券	55
5.5 布比数字资产交易平台的其他应用案例	56
5.5.1 供应链金融	57
5.5.2 供应链溯源	59
5.5.3 公示公证	62
6 案例启示	65
6.1 案例实施成果总结	65
6.2 案例实施主要问题及建议	66
6.2.1 系统安全	66
6.2.2 技术挑战	67
6.2.3 法律风险	67
7 结论	69
参考文献	71

图表目录

表 1-1 区块链技术数字资产交易平台对比	3
表 2-1 区块链技术特征	7
图 2-1 区块链工作原理	10
图 2-2 区块链应用领域探索	10
表 2-2 区块链市场应用项目	11
图 3-1 区块链局部结构	19
图 3-2 P2P 与中心化网络模式	20
表 3-1 不同共识算法对比	22
表 3-2 非对称加密与对称加密比较	22
图 3-3 非对称加密技术会话过程	23
图 4-1 比特币 2009 年~2018 年价格走势	26
表 4-1 2016 年市值排名前四的数字货币	26
表 4-2 2018 年市值排名前四的数字货币	27
表 4-3 各区块链联盟对比	28
表 4-4 主流数字货币交易平台对比	29
图 4-2 比特币 2009 年~2018 年区块体积增长趋势	30
图 4-3 比特币 2009 年~2018 年区块平均生产间隔	31
图 4-4 比特币 2009 年~2018 年区块平均交易笔数	31
图 5-1 布比商业模式	37
图 5-2 布比技术架构图	38
图 5-3 快速交易验证	40
图 5-4 海量数据存储	40
图 5-5 高吞吐量	41
图 5-6 节点数据同步	41
图 5-7 满足多业务的区块链结构	42
图 5-8 安全私钥存取	42
图 5-9 区块链积分通兑架构	46

图 5-10 布萌数字资产平台商业积分应用架构.....	46
图 5-11 布萌数字资产平台保险卡单应用	48
图 5-12 布萌数字资产平台网络互助应用	51
图 5-13 布萌数字资产平台游戏交易应用.....	53
表 5-1 现有网络游戏与区块链游戏区别.....	54
图 5-14 布比股权债权解决方案	56
图 5-15 布比供应链金融解决方案	58
图 5-16 供应链传统独立中心认证模型	60
图 5-17 基于区块链的供应链动态多中心协同认证模型.....	61
图 5-18 布比公示公证解决方案示意图	64
表 6-1 布比区块链技术应用成果	65

1 绪论

1.1 研究背景

区块链技术具有 Trustless (去信任)、Reliable Database (数据库可靠性高)、Decentralized (去中心化)、Collectively maintain (集体维护) 等特点，近年来成为联合国、国际货币基金组织、投融资领域讨论的热点，各产业也纷纷加大投入力度。2016 年年初央行对于数字货币发行发表积极态度以后，我国注重 blockchain(区块链) 这种创新技术的金融机构日渐增多，该技术目前主要应用于数字货币。这一技术的出现是继互联网 (Internet Information) 信息之后，当前公认的新型最具潜力的，可带来翻天覆地变革的关键技术，有望引发新一轮的技术创新和产业变革，备受市场关注。

技术的发展带来了创业的黄金时代，资本市场纷纷向区块链创新公司进行投资，行业巨头们也纷纷布局，就连地方政府，也相继出台区块链创新公司的相关优惠政策，大家都争相赶上区块链这班通往未来的车。与区块链相关的商业的应用，如溯源、跨境支付、证券交易、登记、确权、智能管理等在市场中也慢慢出现。据外媒报道，从 2015 年到现在，投资到区块链相关初创公司的总金额，已经突破了 10 亿美元（数据来源：CoinBase）。其中全球十大区块链投资机构中，中国占三席，这三个投资代表为 IDG、万向区块链基金、数贝投资。2016 以来全球最大的投资项目都与区块链相关，投资金额分别在 5500 万美元和 6000 万美元，国内最大的一笔区块链项目也在 2016 年 9 月底以超过 2000 万美元的投资规模对外宣布。

区块链技术目前在市场上最成熟的应用当属比特币，及各类数字货币交易，其本质是运用计算机算法和密码学等技术创造一种去中心化的数字货币体系，实现货币的发行和交易。这一技术的应用范围远超出数字货币，它的诸多无以比拟的特性注定其具有广阔的发展前景，在我们日常生活和社会经济活动中该技术无处不在，比如证券交易及股票发行、契约、众筹、投票、知识产权保护、公益事业、电子商务、担保、跨境支付等各个方面，通过它来使中心化产生的各种负面影响得以解决。

本文选取区块链技术在数字资产交易方面的应用，不仅仅局限于数字货币交易，所以，以布比（北京）网络技术有限公司为例（下文简称“布比”），分析其在数字资产交易方面的相关产品及产出。选择“布比”作为案例分析对象，主要是因为该公司

作为区块链技术底层技术提供方，与北京比邻共赢信息技术有限公司（下文简称“比邻”）联合发布了“数贝荷包”，与阳光保险、北京农工商银行等已有合作先例，在市场中有所应证，便于我们从市场中进行取证考验。

目前，对于区块链技术在数字货币、数字资产交易的新闻及初创公司层出不穷，但真正能推向市场落地，接受市场考验的产品还很少，本文将通过对布比在数字资产交易方面的案例，多角度剖析其创新方式，以期为区块链技术应用于数字资产交易的实现方式带来更多启示。

1.2 研究意义

本文主要从区块链技术的原理分析，可能解决的问题，具体案例分析的思路进行撰写。主要研究意义，可分为以下两部分：

(1) 理论意义：区块链技术成为时下最为各金融机构、投资机构、初创企业和监管机构争相研究及投资的热门领域，联合国、国际基金组织、各大金融、投研机构也纷纷出具关于区块链相关的报告，工信部在2017年10月份也牵头国内领头企业，如万向控股、蚂蚁金服、微众银行、平安、万达、乐视等代表印制《中国区块链技术和应用发展白皮书(2016)》，对中国区块链技术的发展路径和标准化发展路径进行探讨。同时，结合各大金融、投研机构的分析报告，参考国外经济发达地区及其他国家好的经验成果，并与我国区块链技术的发展和应用现状充分结合，以实际案例来进行分析，为区块链技术的实践提供理论基础。

(2) 现实意义：本文对国内外市场中对区块链技术现状、发展态势及案例分析，从技术本身特点、优势、劣势及案例实际运用过程中可能存在的风险进行分析，结合“布比”网络有限公司在数字资产交易方面的相关落地项目进行实证分析，并提供相关建议，从而为其他企业或金融机构在运用这一技术时，具有借鉴及参考意义。

1.3 研究思路

本文研究思路主要从以下几个方面进行分析：

- (1) 根据国内外相关文献和理论，分析比较区块链技术在数字资产交易相关实现原型及可能的实现方式，为后文的分析奠定理论基础。
- (2) 选取国内外中使用区块链技术实现的相关产品、对产品在实现过程中的基本

原理，产品定位，技术应用潜在问题，分析基于区块链技术的数字资产交易发展现状、存在问题，及未来市场。

(3) 以布比网络区块链底层服务提供商及数字资产交易平台为例，以具体的基于区块链技术的数字资产交易应用案例为切入点，通过分析具体应用中技术架构、实现方式及案例应用结果，探讨和研究将来区块链技术在实际应用过程中存在的风险隐患。文章的结尾处也将会对各种类型的风险提出可行性意见和有关建议。

1.4 研究方法

因区块链这一领域较为新颖，相关文献及行业数据较为匮乏，文章撰写过程中主要运用了文献分析法、实证分析法、案例比较法。

1.4.1 文献分析法

通过查阅并整理区块链行业相关国内外文献，理清区块链技术原理，及各落地项目相关报告文献，为本文的研究奠定基础。

1.4.2 实证分析法

本文报告数据主要来源于参考文献、国内外重点刊物等渠道、各金融机构研究报告、巴比特；名词定义及相关重要结论来源于具有权威性的、影响力较大的研究机构和媒体；通过复盘应用案例实践结果、设计相关专业模型，利用具体详实的案例呈现以及各种各样的样本分析，尽可能准确地预测行业关键发展方向。

1.4.3 案例比较法

对区块链技术在数字资产交易平台方面的应用，以国内外实际落地项目 Bitshares、数贝荷包、布比进行比对分析，根据对比分析，最终选择代表性的企业作为案例分析的切入点：

表 1-1 区块链技术数字资产交易平台对比

	Bitshares	数贝荷包	布比网络
公司主体	3I 集团	北京比邻共赢信息技术有限公司	布比(北京)网络技术有限公司
成立时间	2014 年 6 月	2012 年	2015 年
成果	比特币社区有很多 DAC 项目，如 Bitshares Play, Bitshares Vote, Bitshares Music, Bitshares DNS; 涉及银行、证券交易所、博彩等	积分、卡券、信用等非货币数字资产的定制、发放、兑换、分析、管理等服务	目前已应用在商业积分、游戏装备、保险卡单、提货券、预付卡、娱乐票券等资产的数字化发行、流通。

续表 1-2 区块链技术数字资产交易平台对比

	Bitshares	数贝荷包	布比网络
产品定位	任何人无须任何技术知识，就可以在上面发行或交易包含数字货币、法币及各类金融衍生品，并且可以收取自定义资产的交易佣金。	数字资产定制管理	基于区块链技术的数字资产交易技术服务提供商
不足之处	目前的用户体验不佳，如 BTS 钱包，功能齐全，但易用性较差，想涉足的领域太为宽泛，所以导致落地的时候方向反而显得不够清晰	底层技术非自己开发，而是与布比合作	作为区块链技术提供方提供技术解决方案，没有自己的资产交易平台
技术创新	由于没有中心化服务器和管理机构，能突破许多地区法律管辖限制，实现绝对公开透明的方式来交易各类已存在的或自定义金融商品。	使用区块链作为底层架构，使区块链技术产品化，面向市场	解决了安全性问题、交易验证共识、业务可扩展性等方面具有优势，既能够满足互联网级开放式平台的要求，也可以应用于各类企业级场景。

资料来源：根据文献及网络相关资料整合

根据以上的比较分析，最终选择重点分析“布比”网络，将其作为本文的案例分析对象。布比是国内非常早就开始做区块链技术的公司，作为底层区块链服务提供商，其区块链技术稳定可用，在 15 年就有落地应用，16 年便获得 Pre-A 轮 3000 万融资，已与几十家机构合作，并有具体落地案例，平台目前已运行过千万级的用户应用，性能和安全当是有所保障。作为区块链技术研究的先行机构，将基于区块链技术之于数字资产交易的概念实现了产品化推向市场应用，且市场反映良好，具有研究及借鉴意义。

1.5 研究重难点与创新点

1.5.1 研究重点与难点

(1) 研究重点

本文研究的重点在基于区块链技术的数字资产交易应用，市场上关于数字资产交易一般会理解为狭义的数字货币交易，本文中的数字资产，泛指一切可被数字化的资产，所以，研究的范围会更为广泛一些，参考的文献、资料，涉猎案例将更为宽泛。但因篇幅有限，在研究具体应用案例时，只挑取目前有具体落地应用，且已面向市场的数字资产交易案例作为切入点，如商业积分、保险卡单、游戏资产交易、网络互助、

供应链金融等。

(2) 研究难点

虽然区块链技术目前在市场中被广泛关注，但有一个明显的障碍是相关资料缺乏，论文、学术文章、参考文献很少，而且大多集中在技术领域或是比特币交易、数字货币交易的研究，其他行业的实际落地的项目或案例很少，相关资料非常有限，本文相关文献及观点支持多数来源于各大金融机构报告、白皮书、期刊、文献报告等，因数字资产其他领域的资料匮乏，所以，也会结合本人在实际工作过程中与领导同事们的经验进行总结。以事实归纳、案例分析等方式来分析区块链在实际应用过程中可能存在的问题及风险，并提供一些借鉴参考结论是本文的重难点。

1.5.2 研究的创新点

(1) 研究内容新

本文研究的是基于区块链技术的数字资产交易，内容具有一定的创新意义。区块链技术本身就是最近几年较为热门且颇具创新的一门技术，国内外目前研究的是区块链技术有哪些技术优点，对金融行业的颠覆性研究，但区块链技术本身具有区块体积日益增大、数据确认时间过长、交易频次较低的问题，如何解决这些问题，才是当前区块链技术实现商用急需解决的问题。本文以区块链技术在数字资产交易方面的具体应用案例为切入点，研究其在实际业务场景中的技术架构、交易模式，并根据不同业务场景提供不同解决方案，这些都是全新的研究领域与研究内容。

(2) 研究视角新

国内外目前基于区块链技术既有的研究是以比特币为首的加密数字货币，缺乏关于其他非数字货币或非金融行业的基于区块链技术的数字资产交易研究。不同于现有的加密数字货币交易研究，本文以广义的数字资产交易为对象，对一切可数字化的资产的交易进行案例分析与研究，以更全面的视角，对现有的理论研究提供补充。

(3) 研究方法新

本文在研究方法方面有一定的创新意义，在选择案例分析对象时，本文采用多维度的案例与实证分析，并与布比 CEO，比邻 CEO 均有面对面交流，以调研访谈方式对区块链技术的商业模式，未来应用进行探讨，深入了解研究对象。同时，本人所在企业曾开展过基于区块链技术的数字权益交易所项目，有理论到实践的经验参考。

2 国内外研究现状

2.1 关于区块链技术的相关研究

2.1.1 区块链相关定义

区块链入门的第一书当属中本聪（Nakamoto）的《Bitcoin: A Peer-to-Peer Electronic Cash System》——比特币点对点的电子货币系统白皮书，这本书发布于金融危机爆发不久之后的2008年11月1日，虽然只有短短9页，但几乎所有关于区块链的讨论都缘起于这本白皮书。白皮书中阐述了基于P2P技术和加密技术相关的电子现金系统构架理念，即比特币系统的基本框架设计，书中没有明确提出“区块链”的字眼，但区块链目前的影响已远大于比特币。

对于区块链的定义，查看各类文献，并无明确的权威定义，主要定义如下：

狭义来讲，区块链（Blockchain）是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本（周平平、杜平宇等，2016）。数据库技术方案的可靠性，可利用去信任和去中心化的方式共同实现；系统中任意节点通过该技术方案，运用密码学的计算方法将特定时间内系统内交流的所有信息，在1个Block（数据块）上记录并运算，并生成用来校验和Chain（链接）下个Block的唯一标识（梅兰妮·斯万，2016），系统中的全部节点会共同参加，并达成共识来判断数据真实与否。

广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式（周平平、杜平宇等，2016）。

2016年，林小驰对于区块链这一概念进行如下定义：区块链技术实质上是互联网的一种协议，是去信任、去中心化的通过集体维护方式实现的数据库技术。与NoSQL数据库（非关系型）相似的技术方案统一被称作区块链，它并非是某个单一技术，区块链技术可以利用诸多架构和编程语言来实现，而且实现方法多种多样，当前普遍应用的主要有：POS机制（权益证明机制，Proof of Stake），POW机制（工作量证明机制，Proof of Work），DPOS机制（股份授权证明机制，Delegate Proof of Stake）等。

随着互联网技术的不断发展，信息交互利用 HTTP、TCP/IP 等通用协议就能完成，然而有关结算付款、资产登记等操作，因为缺少互信信息，仍需利用金融服务中介来作为记账中心或负责传递价值。区块链技术是一种不需要信用中介的电子支付系统 (Nakamoto, 2008)，利用去中心化的记账方法构建分布式账本，实现点对点价值的直接转移。区块链技术的本质是能够实现价值传递的新的互联网协议 (陈龙强, 2016)，将有可能实现去中心化的数字资产的安全转移。随着虚拟电子货币“比特币”风靡全球，区块链作为底层技术也逐渐受到各行各业特别是金融行业的关注。

综上所述，区块链从技术层面来讲，可简单理解为分布式的，去中心化的大型账本。在没有任何集中式清算单位或者是信用中介参与的情况下，直接点对点完成交易，实现去中心化；链上全部参与者在发生交易时，都能够通过自身账本获取交易记录，交易信息全部是公开的，并对其进行加密处理，不能够被篡改 (Joseph & Qu, 2016)。

2.1.2 区块链技术的特征及意义

对于“区块链”的出现，各大主流媒体、科技报道都透露出区块链即将要改变世界，颠覆金融业的论调，高盛在报告中更是称区块链技术将带来翻天覆地的变化。美国于 2016 年 1 月 6 日在《华盛顿邮报》发表文章，称 2016 年十大创新先进技术之一的区块链技术，将是互联网技术面世至今最为重要的研究成果，极有可能使技术创新路线发生变化。区块链利用点对点数据传输方式及分布式信息存储方法，突破了原有中介化和中心化的信息传输方式，这必将极大地影响现有传统金融行业(秦谊, 2016)。区块链具有怎样的技术特征，让大家以“颠覆”的字眼赋予厚望？

秦谊 (2016) 认为区块链的特征为可靠性和可用性、透明、记录不可篡改、数字化特征；张波 (2016) 指出区块链的技术特点为：成本低廉、安全性高、透明性强、拓展性大；荣希 (2016) 根据区块链的定义，总结了区块链的四个特征为去中心化、去信任、集体维护、可靠数据库。各主要特征描述如下：

表 2-1 区块链技术特征

序号	特征	特征描述
1	可靠性和可用性	一个区块通常是由一个开放网络中的用户群共同拥有，如果链上某个节点发生故障，并不会使链上其他节点缺少数据，其他参与者仍可在链上正常操作，对信息传输或其他金融交易不会产生影响。
2	透明特征	链上所有数据的更新都会被同步到整个区块链上。Davy Jose 和 Anton Tonev (汇丰银行分析师) 提出，区块链对于怎样在分散的体系中，对信任问题进行验证给出了最优设计，该技术解决的关键点是两个互相不认识，无须互相信任的第三方就能彼此信任。

续表 2-2 区块链技术特征

序号	特征	特征描述
3	记录无法被篡改	链上所有数据均被打上时间戳，一旦记录将无法被改动。
4	数字化特征	通过分类账或代码方式呈现链上全部资产或文件
5	去中心化	网络上所有节点之间具有相同的义务与权利，整个系统无中心化的管理机构或是硬件，节点丢失或损坏对网络整体运行不造成任何影响
6	去信任	系统运行过程中全部数据、规则公开透明，参加系统运作的所有节点之间不需要相互信任
7	集体维护	有维护权限节点中的任何人，都具有维护整个系统数据块中各个节点的权限

资料来源：根据上文相关文献整理

通过以上区块链的主要特征将区块链可带来的意义总结为四个方面：

- (1) 消除交易中介，降低交易成本；
- (2) 交易结算实时，提升交易效率；
- (3) 不可篡改性和去中心化的数据储存方式，使其成为数据和信息记录的最佳载体
- (4) 可编程的区块链使交易流程实现全自动化 (Joseph & Qu, 2016)。

2.1.3 区块链技术相关产业应用研究

有越来越多的认识，对于实现分布式分类技术俗称区块链，将对我们关于金融资产，金融行业在未来的操作带来一个根本性的转变，分布式总账的技术概念“区块链”，就像它通常所称：正席卷整个金融服务业，风险资本和投资涌入区块链相关的科技公司 (Shah& Dockx., 2016)。近年以来，只要是从事金融或投资领域相关的人，都在讨论区块链，这个被吹捧为金融时代下一个伟大的技术，成为无数主流财经报道主题，也成为中央银行、联合国等金融系统的关注重点。

2015 年是区块链讨论得特别热烈的一年，形成了区块链 1.0 到 3.0 的发展过程。区块链 1.0 本质上是对加密数字货币（以比特币为代表）的应用研究。2016 年曹磊提出，区块链对于互联网来说其作用是颠覆性的，目前具有更加深远意义的区块链 2.0 时代的大幕已开启。Blockchain2.0 被解释为在金融领域中开展区块链技术的应用，当前华尔街银行与其他金融机构合作，共同建立区块链行业标准，在 2017 年宣布推出区块链银行跨境支付平台，其目的是减少跨境支付费用，使银行清结算效率得以提升；如果说区块链 1.0 是在支付和货币领域实现去中心化，那区块链 2.0 去中心化的对象则是面向整个市场，更加宏观。区块链 2.0 将区块链技术发展为不仅只局限于加密数字货币，还包含其他各种类型的资产 (梅兰妮.斯万, 2016)。

区块链 3.0 将区块链的应用领域扩展到金融行业之外，超越货币、经济领域（周立群、李智华，2016），涵盖了我们社会经济活动的各个方面，人类在各种活动中自证信息、建立信用或获取信任，无需通过特定中间商或第三方机构，就能共享信息。区块链技术能够解决包括物流、医疗、司法等各行各业在内的信任问题，全面提升系统运行效率，像交易所也在积极尝试用区块链技术实现股权登记、股权转让等功能。区块链技术从 1.0 到 3.0 的发展，这三个阶段并非依次实现，而是共同发展，相互促进的过程。而本文要分析的数字资产交易，可理解为是基于区块链 3.0 的研究。

英国的金融领域在探索和区块链技术应用创新方面一直领先于其他国家，它着重研究汇款和智能合约领域的相关应用；欧洲重点研究银行汇款；美国则重点研究银行汇款、二级市场交易领域；日韩则重点研究银行业务领域。在金融领域之外，各国中央机构则将重点放在智能合约和认证领域方面的应用（胡乃静、周欢，2016）。针对区块链技术的合法合规，德国、法国、美国各州开展了有关立法工作，2016 年 1 月英国公布了研究报告，将在政府和金融事务中积极推动区块链技术的应用，我国为了加快数字货币方面的研究，则创建了专门研究区块链的相关单位。区块链技术将来可能在审计、股票证券、公证、票据、货币数字化、清结算等诸多领域得到广泛应用。Wyman & Chase (2016) 指出，目前的技术应用成果将是网络参与者之间数据通信的“简单应用”；第二波应用浪潮的成果是“核心交易数据”的存储系统。

金融领域中，“对于银行业，区块链作为一种高度数字化，安全防干扰的账本，可用以实现银行的核心功能：即作为价值的安全储存和转移中心（谌麟艳，2016）”。在川财证券研究所的报告中，我们可以简单地从下图分析区块链如何工作：

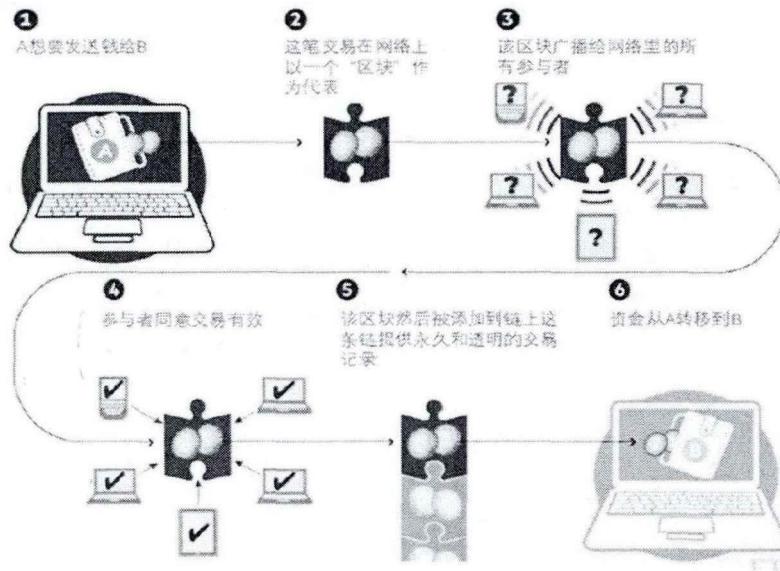


图 2-1 区块链工作原理

资料来源：金融时报、川财证券研究所

2016年初，德勤加密货币社区（德勤DC3）通过CoinDesk网站发文，在调研欧美商业社区的基础上，预测2016年区块链将走向市场，而不再仅局限于实验室。陈龙强（2016）预测，在今后的2-3年间，区块链技术可能会引发互联网金融、物联网、大数据等领域的重大且具有深远意义的变革。皮埃罗·斯加鲁菲（哈佛教授）于2015年底预测，创业者将来要关注以下10个对于社会和经济发展起到方向引领作用的领域，分别为：人工智能、基因、货币、万物互联、新型制造业、共享经济、数据、纳米技术、可穿戴设备、太空探索。根据各类资料分析及整合，对区块链可应用的领域，如下图所示：

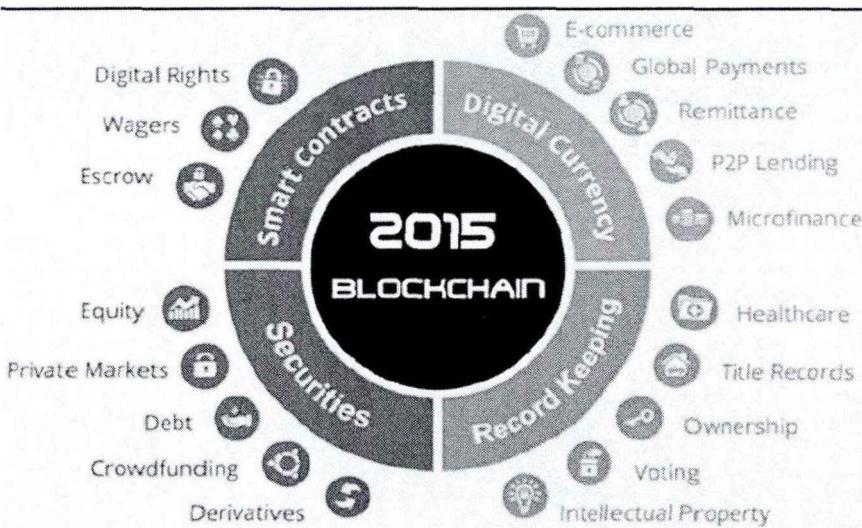


图 2-2 区块链应用领域探索

资料来源：Coindesk

工信部在《中国区块链技术和应用发展白皮书（2016）》中称，“金融机构能够在支付领域凭借区块链技术的效率和成本优势，实现了以往由于成本原因无法实现的小额跨境支付，有助于普惠金融的实现。”白皮书详解介绍了区块链技术的潜在应用，重点分析了金融领域。其他应用领域包含供应链管理、娱乐、智能制造、社会福利、教育和就业等方面。根据文献、报告及网络相关资料，将目前实际推向市场的基于区块链技术的应用汇总如下：

表 2-3 区块链市场应用项目

主要应用领域	产品名称	应用介绍
区块链与数字货币	中国比特币或数字货币主要交易平台：比特币中国、火币网、Okcoin；	排名前四位的数字货币为：比特币、以太坊、瑞波币、莱特币
	国外比特币交易平台有：BitStamp、BTC-Q	国外主要的交易平台，流动性好，口碑不错；配置了多个国家语言的版本，
区块链与跨境支付	Ripple（瑞波）	Ripple 为全球的金融结算提供解决方案，使银行间无须通过代理行，便可直接转账，及时结算，降低结算成本。实现世界首笔基于区块链技术的跨境银行间汇款，仅用 8 秒就把 1000 美元由 ATB 银行（加拿大阿尔伯塔）汇给了 Reisebank 银行（德国）
区块链与版权管理	Colu	2015 年 Colu 公司（以色列）利用区块链技术，开发了相关的终端工具和协议层，并推出数字资产平台，提供资产发行及管理服务，Colu 公司还和 Revolator 公司合作为音乐版权提供了一个注册、交易的透明可信通道
	Everledger	英国的 Everledger 与 Vastari 公司（专门从事展览和艺术品数据库服务的公司），推出了以区块链技术为基础的数据系统
	Ascribe	Ascribe 公司（德国），主要服务于艺术家们，为他们的艺术作品提供交易、注册、登记等相关服务
区块链与游戏资产交易	BitsharePlay	通过使用专利技术，提供一个聚合所有游戏的平台和一个游戏资产交易平台，使得从不同游戏中获得的代币、道具和 Play 的加密股份可相互交易
区块链与公证	Everledger	使用了区块链技术专门用于钻石认证
区块链与公益	阿里公益	蚂蚁金服率先把区块链技术尝试应用于公益事业——为我国社会救助基金会在互联网上提供捐赠平台，帮助他们实现“聆天使计划”，该公益账户被称作是“最透明的”，通过它实现的募捐过程得到社会大众的全程监督，并将募集到的 19.84 万元捐款作为儿童聋健教育、语言听力康复、调试人工耳蜗的费用

续表 2-4 区块链市场应用项目

主要应用领域	产品名称	应用介绍
区块链与数字资产交易	布比	可快速构建自己的区块链数字资产应用，目前已应用于商业积分、游戏装备、保险卡单、提货券、预付卡、娱乐票券等数字资产的发行、流通。

资料来源：根据参考文献资料整理

麦肯锡在 2016 年《中国银行业白皮书：区块链银行业规则颠覆者》的报告中详细分析了当前金融机构的痛点，对金融应用场景进行分析，同时对区块链在数字货币、跨境支付与结算、供应链金融、证券发行和交易四大领导的商业契机进行分析。只有基于大量群体参与并一起共享的区块链技术应用，才能充分体现该技术的价值；只有实现开放和互通，打破原在系统封闭才能充分发挥其优势（穆启国、陆婕，2016）”。

2.2 关于 Token 经济的研究

在互联网领域 Token 通常代表“信令、令牌”，在区块链领域则代表“通证”。Token 在区块链领域得到普遍共识，有赖于以太坊及其 ERC20 标准。以太坊上所有人以该标准为基础便可发布自己定义的 Token，该 Token 能够代表任意价值或权益。

“通证”启发和鼓励大家把各种权益证明，比如门票、积分、合同、证书、点卡、证券、权限、资质等等全部拿出来通证化（Tokenization），放到区块链上流转，放到市场上交易，让市场自动发现其价格，同时在现实经济生活中可以消费、可以验证，是可以用的东西，这是紧贴实体经济的。

现在用 Token 作为代币权益证明进行 ICO 是一个普遍的做法。由此我们也认识到，加密数字货币就是一种特殊的 Token。比特币，中本聪是想让它成为支付货币，但是现在它变成了一种数字资产，并没有发挥通货的作用。强调“代币”，名不副实，反而引发货币主权等一系列棘手难题。货币即权力，货币即政治，货币权力必须属于国家。所以 Token 可以代表任何资产，就是不能代表法币，没有国家的授权和支持，所谓“代币”只是自欺欺人。

（1）Token 的实现有三个要素：

第一个是数字权益证明，也就是说 Token 必须是以数字形式存在的权益凭证，它必须代表的是一种权利，一种固有和内在的价值（Intrinsic value）。

第二是加密，通证的真实性、防篡改性、保护隐私等能力，由密码学予以保障。

第三是可流通，说的是通证必须能够在一个网络中流动，从而随时随地可以验证。其中一部分通证是可以交易、兑换的。

事实上，通证可以代表一切权益证明，从身份证到学历文凭，从货币到票据，从钥匙、门票到积分、卡券，从股票到债券，人类社会全部权益证明，都可以用通证来代表。

人类社会的全部文明，可以说就是建立在权益证明之上的，所有的账目、所有权、资格、证明等等，全部都是权益证明。就像尤瓦尔·赫拉利在《人类简史》里说的，正是这些“虚构出来的事实”才是智人脱颖而出，建立人类文明的核心原因。如果这些权益证明全部数字化、电子化，并且以密码学来保护和验证其真实性、完整性、隐私性，那么对于人类文明将是一个巨大的革新。

(2) Token Economy

“Token Economy”，翻译过来就是“通证经济”。什么叫通证经济？就是把通证充分用起来的经济。Token 经济发生的条件：

第一，供给侧，Token 的供给充分实现高度自由和市场化，它在区块链上运行，所有机构、组织和个人均能够依靠自身服务能力和服务发布权益证明，并且任何时候均可实现交换、追溯和验证，之前在互联网中无法实现其可靠性、可信性以及安全性，现在利用 Token 每一个组织和个人现在都可以很轻松的把自己的承诺书面化、“通证化”、市场化，这是人类社会从来都没有的能力。

第二，流通速度，这是个关键。与之前的券、票、卡、积分相比，Token 在区块链上的流转速度比传统的流转方式要快数百数千倍，并且因为应用了密码学技术，其交易和流转更加可靠，摩擦与纠纷也成几何倍数地降低。如果说在传统经济时代，衡量整个社会经济发展的一个重要指标是货币流转速度，而在互联网经济时代衡量一个国家、一个城市发达程度的一个重要指标是网络流量，那么在互联网+经济的时代，通证的总流通速度将成为最重要经济衡量指标之一。当我们每个人、每个组织的各种通证都在飞速流转、交易的时候，我们的生产和生活方式将完全改变。

第三，价格发现，所有 Token 的价格在其交易及高速流转的过程中，在市场中被快速确认，通证经济就像隐形的手，与当前市场价格信息相比，要精细及灵敏数百数千倍，在所有微观领域中，发挥市场有效性或完美性的作用。

第四，通证应用，仅是其在智能合约方面的应用，就能够引发各种各样的创新，

大大超出之前互联网和计算机时代在创新方面所激发的浪潮和带来机遇的总和。基于这四点认识，我们坚信通证是将我们导向下一代互联网新经济的关键。

通证经济既能促进自由交换，又能加强监管，是市场经济的一次大升级，本质上是用密码学、用包括跨国界的开源开放超级电脑等未来信息基础设施来重新定义市场经济。人工智能，通证，区块链，这三个东西合起来，已经不是简单生产和生活方式变化的问题了，而是人类文明演进和生命存在意义改变的问题。

2.3 关于区块链技术在数字资产交易应用方面的相关研究

2.3.1 数字资产定义

什么叫数字资产？根据 MAB 智库对广义数字资产的概念描述为：“企业拥有或控制的，以电子数据的形式存在的，在日常活动中持有以备出售或处在生产过程中的非货币性资产”。从狭义上讲，数字资产指在分布式的区块链账中记录的程序——代币，可通过计算机编码实现对数字资产的控制，而资产的交换也就转换为代码的交换。

2.3.2 基于区块链技术的数字资产交易相关研究

数字资产实际上就是一切可数字化的资产，囊括了比特币、数字知识产权、数字股权、数字收益权以及各种数字货币等。数字资产实现可交易最重要的一点就是数字身份（初夏虎，2016）。区块链由算法驱动，天然支持资产数字化（陈龙强，2016）”。

本文中所指的数字资产，提广义的，一切以电子数据形式存在的，可被数字化的资产均为数字资产。在数字资产应用当中，被大众最为熟悉的当属数字货币，数字货币（Digital money）又被称为电子现金（Ecash）或货币（Emoney），视为对现实货币的模拟，涉及用户、商家和处于中心化地位的银行或第三方支付机构（中国区块链技术和应用发展白皮书，2016）。

根据各类数字资产应用特点，我们将数字资产简要地总结出如下四个特点：

（一）其呈现方式是一种虚拟资产，其存在结构不是原子或分子结构的实物体，而是以比特结构形式存在的数字代币，即大家所熟知的“Coin”。

（二）其实质只是一段代码，可通过计算机程序实现编程，在进行数字资产交换时，不过是代码间的交换。在区块链中只需根据交易规则编写出对应的智能合约，程序就可以自主实现点对点的，百分百去除中介的，无需人为处理的智能交易。

（三）它是在分布式的区块链账本中记录的资产，不像在工商部门登记的股权、

在房产部门登记的房屋产权这种实实在在的所有权，数字资产在权属确认方面还没有定论。

(四) 随着区块链技术的愈发成熟，数字技术的应用扩展，传统的实体资产也正在持续地向数字化方向发展，从而使数字资产这一概念正不断扩张到其它领域，包括文化、金融等似乎已具备了向数字资产转化的条件。虽然区块链技术还不完善，但其在多领域都显示出它的巨大潜能，在资产数字化方面更是“量身定制”版的技术(朱幼平, 2017)。

区块链的下一步发展方向是什么呢？我们判断是数字资产(曹月佳, 2016)。例如比特币、数字知识产权、数字股权、数字收益权以及各种数字货币等。若想对数字资产进行交易，最关键的便是数字化(初夏虎, 2016)。当一种数字资产拥有相应的数字身份以后，该资产便可进行转让、质押、租赁以及赠送等各种操作，凡是传统形式的金融能够实现的项目，数字金融同样全部能实现。在管理数字资产的过程中，将已经数字化的资产交给区块链处理，区块链收到交易的指令之后会将资产按指令进行转移(曹磊, 2016)。欧洲中央银行于二〇一五年二月的研究报告——《虚拟货币》一文中做了这样的定位：“数字货币是价值以数据的形式进行表现，且这种货币不是通过政府发行的，但是当具备了一定条件的时候可以用其来替代货币。”

目前市场上多数平台的数字资产交易，以数字货币交易为主。数字货币不同于法定货币，后者有国家信用为其背书，而前者的产生只需一段加密的算法，是货币的另一种存在形式，且二者之间可互相兑换的，只是兑换价格不是由政府控制，而是取决于市场中的供求关系(秦谊, 2016)。

比特币在区块链系统中稳定运行多年，这就足以说明借助计算机程序实现货币数字化是完全行得通的。英国的中央银行进行了相关研究，其结果是：基于区块链技术，由央行来发行数字货币具有可行性，此举可以使金融系统的稳定性得以增强(李峰, 2016)。从发行成本及货币安全性方面来说，传统的货币或许终将会被高科技的货币形式所取代。对于经济发展以及金融基础设施建设来说，建立新型的数字货币的流通体系，将非常有意义也非常有必要(李峰, 2016)。相比传统的货币形式，数字货币一旦得以发行不但可以使发行与流通成本极大降低，更可以借此使得经济交易活动的透明度获得有效提高，而其便利性就更不必说。而在互联网已经全面普及的大的时代背景之下，各国的中央银行完全可以运用区块链技术来开发自己的数字货币(林晓轩, 2016)。

英格兰银行最新发布的研究表明，央行发行数字货币可以促进国内生产总值(GDP)增长，由此带来的增长幅度可以达到3%，原因在于有效降低了真实汇率、货币交易成本以及扭曲性的税收；其次，CBDC（世界中心结算体系）可以加强商业圈的稳定性，这是因为给与了政策制定者使用第二个政策工具的权限，这个工具用反周期的方式控制了CBDC的质量和价格（Barrdear & Kumhof, 2016）”。

二〇一六年一月，中国人民银行专门召开了数字货币研讨会，会议达成了这样的共识：从传统货币发行及货币政策方面，数字货币的迅猛发展带给央行带来前所未有的挑战，但同时也是一种实现创新的机会。会议进行了多场景数字货币应用的研究，同时也对央行的数字货币发行战略性目标进行了明确，即尽快由中国的央行实现数字货币的正式发行（米晓文，2016）。同年二月份，中国人民银行行长周小川表示：对于推动我国经济增效、提质、升级以及金融基础设施建设来说，建立新型的数字货币的流通体系，的确很有意义，也很有必要。区块链技术将作为一种重要的技术，将用于探讨数字货币应用。他认为，目前区块链存在占用资源过多，不管是计算资源还是存储资源，结合其自身现有技术瓶颈，还应对不了金融市场中现有交易规模。

二〇一五年十一月，国际清算银行在其发布的《数字货币报告》中明确提出，区块链技术和数字货币的创新在很多领域带来了广泛的影响，特别是在支付系统及其相关服务上。这种颠覆传统的全新模式对现有商业体系的冲击结果，会促使其建立起一套完全不同的经济、金融、社会新格局。

以上文献均在不同程度上提到数字资产将是未来区块链技术的下一个发展方向。目前，数字货币还未被广泛应用和接受，或许暂时还仅仅是游离于金融主体服务项目以外、只服务于极少数用户群体的非主流产品。然而通过最近几年某些数字货币的实际运行，在去除第三方信用中介，直接以分布式总账的形式来完成点对点的交易是完全行得通的。通过以比特币为代表的各种加密数字货币的飞跃式发展，区块链技术通过了金融行业的尝试性应用的考验，也切实解决了传统金融体系中难以解决的难题，解除了对金融中介及第三方认证系统的依附，有效实现了去中心化，通过加密算法、智能合约等技术手段，确保了合约的有效与公平。“所以说，股权与债权认证、财务审计以及P2P借贷等金融项目是区块链技术未来最适合的应用领域（陈龙强，2016）”。

2.4 国内外研究述评

在国外各类金融组织、科技企业、及主要国家机构，如联合国、国际货币基金组织，美、日、英等发达国家极为关注区块链技术的应用前景，并积极探索推动区块链技术应用的落地。在中国，以北京、上海、深圳为首的城市先后成立各类区块链技术联盟，在金融科技领域率先研究孵化，并逐步向其他领域延伸展开。

通过大量文献的梳理和提炼，虽然不同学者或不同机构采用不同的分析方法、不同分析对象，但基本都得出相似结论，即区块链技术将成为开启互联网新时代的关键核心技术，很可能在全球范围内引起一场新的技术革新及产业变革。本文重点分析区块链技术在数字资产交易方面的应用，在不同行业不同应用场景中技术关注侧重点会有所不同，但基于应用的底层核心技术都同为区块链，在应用过程中均可借鉴参考。区块链技术目前最成熟的应用当属以比特币为代表的各种数字货币，在分析区块链技术应用到数字资产交易时，比特币这一数字货币所面临的相关问题，仍值得我们借鉴。

区块链技术应用于数字资产交易的研究过程中，仍存在以下不足：

(1) 关于区块链技术在数字资产交易方面的研究，目前可参考的资料及文献较少，各类文献多数集中在分析比特币的应用，或是针对数字货币的应用与发行。而广义的数字资产交易应当是包括数字货币在内的一切可被数字化的资产，在实际应用过程中，因业务场景的各不相同，其实现过程可能更为复杂。

(2) 基于区块链技术实现数字资产交易的企业较少，向市场宣布或公开的资料也很匮乏，在进行案例分析时，除了基于网上公布资料，也结合自己工作中接触的资料进行分析，相关结论及数据可能不够权威，仅作为借鉴及参考。

3 理论基础

关于区块链最早的描述性文献，公认的当属中本聪所撰写的文章《Bitcoin: A Peer-to Peer Electronic Cash System》，不过该文献重点在于讨论比特币系统，并没有明确提出区块链的定义或概念。文中指出：区块链是用于记录比特币交易账目历史的数据结构。

在维基百科（Wikipedia）中，区块链被称为一种分布式数据库技术，通过维护数据块的链式结构，可维持持续增长的，不可篡改的数据记录。在工信部《中国区块链技术和应用发展白皮书，2016》中，把区块链定义为与点对点传输、分布式储存、共识机制以及加密算法等计算机相关技术的新型应用模式。

从技术层面来讲，区块链可简单理解为一个去中心化的分布式账本，不可以随便改动链上内容，所以实现了无需信息积分的信用建立范式。可以将区块链当作一个账本，以点对点的形式进行记账管理或者是用智能合约确保建立信用共识，就能进入这个能够确保透明、公开的数据库，省去第三方中介的介入。该数据库将历史上所有数据、交易记录以及所有处理过的信息全部包含其中。在确保公开透明的基础上，所有数据都将以加密的形式进行分布式地安全储存，将逐个形成的数据区块，以时间为轴，最终连接成区块链。

区块链技术相关应用最早出现在比特币项目中，作为比特币背后的分布式记账平台，在无集中式管理的情况下，比特币网络稳定运行八九年时间。比特币价格，更是从2013最初的13美元，到2018年4月已经一路高涨到8300美元，在全民买币热情高涨的情况下，依靠其稳定的技术架构支持了海量的交易记录，历史上也并未出现严重漏洞，这与区块链本身技术结构分不开。目前，区块链技术自身仍在飞速发展中，相关规范与标准也在进一步趋于成熟。

3.1 区块链技术运作基本原理

2016年4月高盛在《区块链：将理论付诸实践》的报告中，用一句话解释了区块链的运作原理：“交易信息（如买方、卖方、标的、价格）起始会作为一个区块存在，这些区块要被整个网络中的人认证，才会被加到链条上”。

通过对以上的解释的理解，对区块链基本原理，可下面三个基本概念开始了解：

- 一是交易：每次操作都会被记录进账本，账本的存储状态也会发生相应的改变；
- 二是区块：记录一定时间段内全部交易及对应的交易状态，并将该账本的最新状态形成共识；
- 三是链：按时间先后将区块连接在一起，完整记录账本所有状态的变化。

实现过程中，假设存在一个分布式的数据记录账本（Leger），这个账本只允许添加，不允许删除。账本底层基本结构是一个线性链表，这也是“区块链（Block Chain）”名字的来源。以比特币为例，它其实就是一本分类账，该账本分散且数据量极其庞大，账本内中每项历史交易记录都会储存在互联网中，信息不可篡改。

如图 3-1 所示，链表由一个个“区块（Block）”串联组成，后继区块记录前导区块的哈希值（PreHash）。新数据的加入，必须放到新的区块当中，而此区块是否合法，将通过计算哈希值的方式快速检验出来，任意维护节点都可提议一个新的合法区块，但必须经过一定的共识机制来对要加入的区块达成一致。

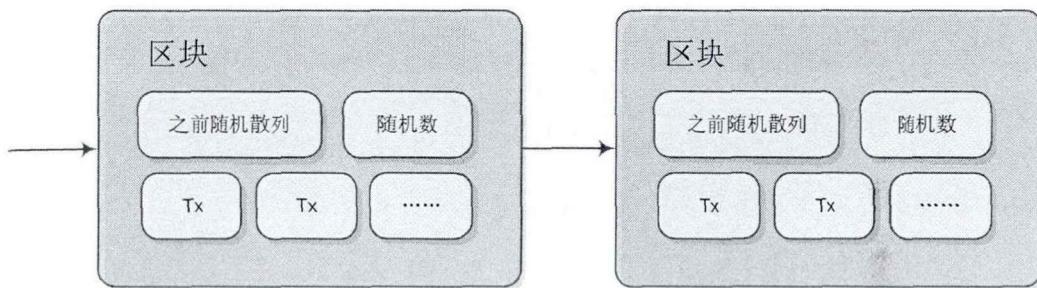


图 3-1 区块链局部结构

资料来源：Nakamoto (2008)

3.2 区块链核心技术及特点

区块链的核心技术就是数字加密技术，其在比特币的货币体系之中得到了成功的体现，区块链技术最大的优势是去中心化，使用时间戳、共识机制、加密技术、智能合作等技术，从而实现无须信用中介的点对点交易，形成了完备的分布式体系，因此完全避开传统中心化结构中，难以消除的数据安全问题，既极大地提高了交易处理效率，又有效地控制了风险。在介绍区块链应用之前，我们先厘清区块链的几个核心技术：点对点网络技术（P2P）、共识机制、多级加密技术、智能合约。

3.2.1 区块链核心技术

(1) 点对点网络协议（P2P）

如图 3-2(a) 所示, P2P 网络结构为扁平化模式, 其所有节点的地位是一样的, 没有中心服务器, 所以各节点在实现区块链系统各种功能时身份都是相同的, 这种网络协议的构架方式就是去中心化的网络基础。

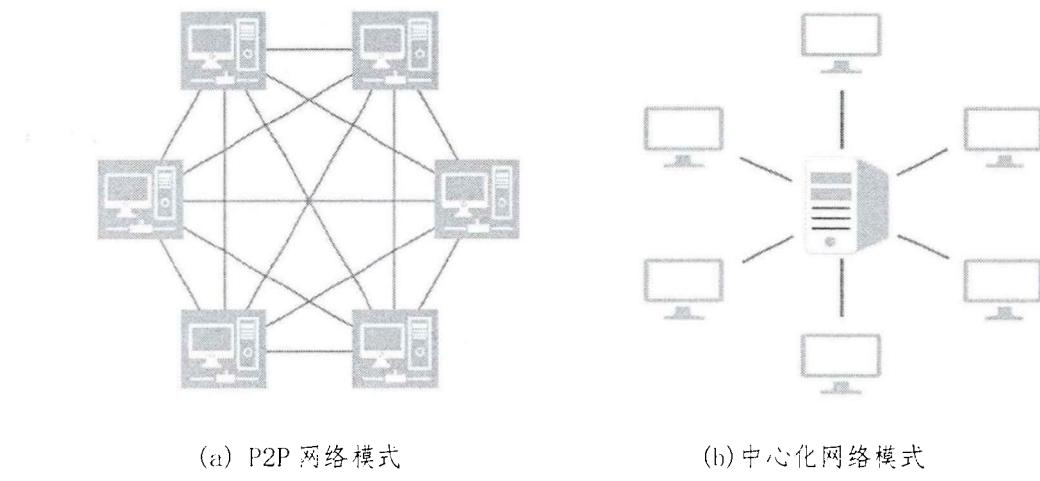


图 3-2 P2P 与中心化网络模式

资料来源:《中国区块链技术和应用发展白皮书, 2016》

在区块链系统中, 数据的传播有两种不同的方式: 即获得数据与自行发送数据。当 a 节点在接收到交易信息的时候, 将会把信息用广播的方式发送给网络内的其它节点。由于系统所用的网络模式是点对点式, 因此广播发出去的信息无法保证全部节点都顺利收到, 那么 a 节点就可以向距离较近的节点发送索要数据的申请, 通过该近距离的节点为其分发数据同时对结果进行同步处理(安庆文, 2017)。不同于中心化的网络模式, 在该网络模式中, 当节点 a 接收到邻近节点传来的消息时, 会对数据有效性进行校验, 若为无效信息, 节点 a 不做数据转发, 同时还会对传送无效信息的节点在一段时间内断开连接, 防止网络恶意攻击; 对接收到的有效信息则会将该信息向邻近节点进行广播。

在比特币出现之前, P2P 网络计算技术已广泛应用于各种应用, 如即时通讯、文件共享、软件下载、网络视频播放软件、计算资源共享等(周平平、杜平宇等, 2016)。区块链采用分布式网络模式, 通过点对点的网络协议来去除中心环节, 实现全网的安全高效。

(2) 共识机制

根据《中国区块链技术和应用发展白皮书, 2016》中的定义, 共识机制指“区块

链系统中实现不同节点之间建立信息、获取权益的数学算法”。区块链是比特币的基础技术架构，伴随比特币而生，可将区块链理解为基于互联网的去中心化记账系统。类似比特币这种去中心化的数字货币系统，要求在没有中心节点的情况下保证各节点记账的一致性，有赖于区块链技术的实现。所以，区块链的核心技术就是在没有中心控制的情况下，以一种加密算法，建立起计算机之间的互信网络，依靠技术实现了去除中介信用机构（蔡钊，2016），在没有信任基础的个体间对交易的合法性达成共识的共识技术。

共识层主要实现全网所有节点对交易和数据达成一致，防范拜占庭攻击、女巫攻击、51%攻击等共识攻击，其算法称为共识机制，因为其应用场景不同，目前常见的有以下几种共识机制：

第一种，工作量证明机制（Proof of Work-PoW）：这是我们最熟知的一种共识机制。如字面解释，PoW就是工作越多，收益越大。这里的工作就是猜数字，谁能最快猜出那个唯一的数字，谁就能做信息公示人。该算法能最大程度地解决信任问题，但缺点就是需要浪费大量算力，POW系统构建区块的过程一般称为“挖矿”（mine），在所有参与挖矿的矿工中最终每次只有一个矿工能获得记账权，其他矿工的计算都被浪费，消耗了巨大的电量（穆启国、陆婕，2016），比特币使用的就是PoW证明机制。

第二种，权益证明机制（Proof of Stake-PoS）：二〇一二年八月，Sunny King 首提 PPC，并以 PoW 运行机制进行新币的发行，以 PoS 机制确保网络运行安全，PPC 持有者具有挖矿权，并共同维护网络的安全，由股权而非算力决定。这是一种类似于股权凭证和投票系统的共识证明，也叫“股权证明算法”，由持有最多 Token 的人来公示最终信息，即权益大的节点更容易挖矿（安庆文，2017）。POS 系统构建区块的方式一般称为“铸造”（mint），以太币使用的就是 POS 机制。

第三种，运用 Practical Byzantine Fault Tolerance（简称 PBFT）实用拜占庭共识算法：这也是一种常见的共识证明，不同于前两种共识算法，PBFT 以计算为基础，也没有代币作为奖励，而是由链上所有人参与投票，少于 $(N-1)/3$ 个节点反对时就获得公示信息的权利。该算法在一九九九年由 Castro & Liskov 首次提出，在该机制下每秒的速度超过十万，Hyperledger 就是采用这种算法进行区块链项目的开发（安庆文，2017）。

第四种，股份授权证明（Delegate Proof of Stake-DPoS）原理：让每一个持有比特币的节点投票选出一百个（或其它数字）代表节点，通过这些代表节点根据相应

的算法形成区块。若代表节点不能完成区块的生成，则会取消其代表资格，再从网络中推选新代表节点。这种机制具有显著减少参与记账及验证的节点个数，从而可将速度提升至秒的优点。而其不足之处是该机制仍有赖于代币，而不少的商业用途中不必有代币。

第五种，Casper 权益证明算法（也称投注共识）原理：以太坊下一代的共识机制，每个参与共识的节点都要支付一定的押金，节点获取奖励的概率和押金成正比，如果有节点作恶押金则要被扣掉。

第六种，消逝时间量证明（Proof of Elapsed Time- PoET）原理：该共识机制由 intel 提出，其关键技术是在确保环境安全受控的前提下产生随机延时，CPU 验证其延时是否可信，最小延时者会得到记账的权限。

表 3-1 不同共识算法对比统计表

共识算法	PoS	PoW	PBFT	Casper	DPoS	PoET
性能	较高	较高	高	较高	高	高
最大允许作恶节点数量	50.99%	51.01%	32.99%	50.99%	51.01%	50.99%
去中心化程度	完全	完全	二分之一	完全	完全	二分之一
是否需要代币	需要	不需要	不需要	需要	需要	不需要
技术成熟度	成熟	成熟	成熟	没有应用	成熟	没有应用
能否防范女巫攻击	能	能	否	能	能	能
应用类型	公有链	公有链	联盟链	公有链	公有链	联盟链
需要专用硬件	不需要	需要	不需要	不需要	不需要	需要

资料来源：根据文献整理

（3）多级加密技术应用

加密算法一般分为对称加密和非对称加密，非对称简而言之即是达到安全要求与归属权检验标准进行集成至区块链内的一种加密方法。其一般是在加、解密的进程里应用到两个不是对称的密码，人们把这两个密码下定义为公钥与私钥。此种加密方式一般具备两大特征：首先是公钥能够对所有人开放，但私钥是隐密的，私钥拥有者才能使用公钥计算出对应的私钥。其次是使用公钥或私钥对数据进行加密后，只能使用其对应的密钥方可解除。

表 3-2 非对称加密与对称加密比较
(a) 非对称加密算法特点

类型	名称	计算方式	复杂度	速度	破解难度
非对称加密	RSA	基于特殊的可逆模 幂运算	亚指数级	一般	基于分解大整数的难度
	ECC SM2	基于椭圆曲线算法	指数级	较快	ECDLP 数学难题

(b) 对称加密算法特点

类型	名称	计算方式	计算耗时	速度	安全性
对称加密	AES	RIJNDAEL 算法		较快	较高
	SM1	密文迭代函数变换	32	较快	较高
	3DES	标准算法和运算逻辑	48	较慢、硬件快	较高

在区块链应用场景中，非对称加密办法能够在登录检验、数据签字以及数据加密等范围内使用。在数据完成密钥设置的环境里，信息发出人 a 使用密钥将数据设置密钥，信息接受人 b 收到数据后采用匹配的其他密钥对进行数据解除，此种办法确保了数据传输环节里的可靠性和隐密性（杨晓晨，2016）。其中信息加密场景中，主要由信息发送方 a 使用接受方 b 的公钥对信息设置密钥后传送给 b，接受人 b 再用个人的私钥将密钥解密。在实际应用中比特币是这种解密方式应用的典型代表。

数字签字的使用环节里，发出人 a 使用个人的私钥对数据设置密钥然后传输给接受人 b，b 选择 a 的公钥进行密钥解除，进而能够验证相关数据是 a 传输的。

在登录验证环节，用户的登录数据会经过私钥加密，并将登录请求传输到服务器，服务器接收到该登录请求后，将此用户的登录数据用公钥解密，同时完成验证登录。

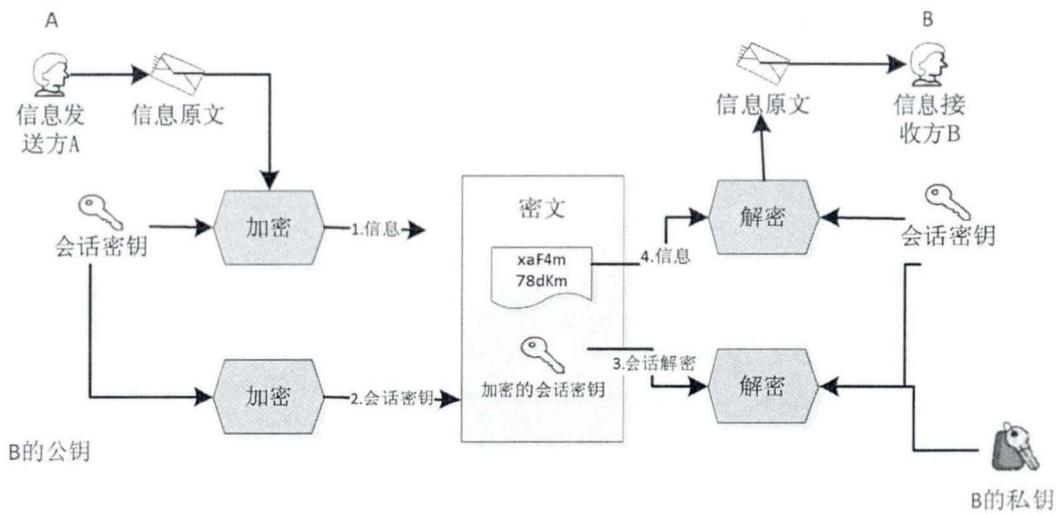


图 3-3 非对称加密技术会话过程

区块链技术最为关键的就是数据加密方式，如果加密算法遭到破解，区块链的数据安全，用户数字资产的安全性将受到挑战。区块链是加密货币数字货币的关键

技术，就像市场中流通的货币具有国家的信用保障，区块链在虚拟货币中也担负着信誉背书的作用，其在具体应用中体现为既不用真实物品质押，也不用国家或金融组织背书的信用机制，一旦脱离区块链技术，所有的虚拟货币都会失去它原有的市值，即使是比特币也不例外。

(4) 智能合约

智能合约理念的提出可追溯到 1994 年，密码学家 Nick Saab 认为智能合约的概念应当是一种用数字可以表达的允诺，协议参与者能够在其中实施被允诺的合约。然而其智能合约并没有在其当时所处的现实生活中加以执行，这是由于在那个时期网络还不具备稳定可靠的操作背景。

区块链技术的横空出世促使智能合约完成了自理论到应用的实质性飞跃，基于区块链技术，智能合约是区块链实现去中心化的应用基础。智能合约是去中心化以及去信任协议的一种，参与者能够在不需要第三方监管的基础上，主动执行协议约定，自主管理数字资产。可设想的应用场景比如：金融市场中的自动付款机制（如金融市场的限价单），一个程序或智能合约可以被设定为，当某个市场达到系统指定价格，就能触发付款行为，触发条件也可以是现实世界中的其他事件，如新闻事件、体育赛事冠军、众筹（梅兰妮·斯万，2016）。

3.2.2 区块链技术特点

Trustless 安全可靠和 Decentralized 没有中间机构管理是区块链的典型优势，加上可靠数据库（Reliable Database）、集体维护（Collectively maintain）、不可篡改、加密安全性等特征，这些特征可弥补传统金融机构高度中心化的不足，提高运作效率，降低机构运营成本，灵活更新市场规则，防止信息篡改和伪造，同时，也大大提高了系统的稳定性，减少宕机风险（长铗、韩锋，2016）。正是基于这些特点，区块链技术显露出广阔的应用前景——具有颠覆潜力。

(1) Decentralized 去中心化

学者谢伟玉和王胜 2016 年通过研究指出，在区块链体系内，不存在单一的控制组织或硬件，每个节点间的权益是对等的，各个节点和矿工均遵守同一个数据记录标准，此标准是在密码学的基础上的，不是依赖于彼此的信用，所有交易要求体系内其他参与节点同意，而不再通过信用组织担保或是第三方中介背书，同时某个节点丢失或是遭到破坏对网络的整体执行并不能产生影响。所以人们普遍认为区块链技术拥有极其

先进的完备性与健壮性。

(2) Trustless 去信任

在区块链体系中的交易规则，运作标准都是公开明确的，交易信息通过广播，信息内容众所周知，各个节点间不要求相互信任即可开展信息交换，所以在体系规定的标准区间与时间框架里，节点间不存在诈骗另外节点的可能。计算方式相互之间建立信任，各方之间建立信任的成本极低，使得原本较弱的信任关系通过算法建立强信任关系，提升效率。

(3) Reliable Database 可靠数据库

在传统的中心化网络结构中，对中心任一节点进行有效攻击便可能导致整个系统瘫痪。而区块链技术没有中心，使用分布式的数据库，令各个节点都具备一个全面的数据库复制件，拥有一模一样的账本，享有相等权利，网络中的黑客若试图篡改或破坏部分节点信息，对整个区块链系统来说并无影响，且网络里加入的节点愈多其运算功能愈强大，这个网络的信息可靠性也愈大，进而给价值的传输提供可靠架构。

(4) Collectively maintain 集体维护

区块链体系中的区块是由各个具有维护功能的节点来一同维护，同时此类有维护作用的节点是所有人都能够加入的。

(5) Open Source 开源

所谓开源就是指整个体系的代码，运作标准都是开放透明的，区块链应用遵循这一运行标准同样也应当是开源的。

(6) Anonymity 隐私保护

区块链应用中任意节点的隐私部分都是得到保护的，这是由于随意两个节点间不要求相互信任，它们也不用公布个人真实信息。以比特币为例，在比特币交互系统中，使用者无须使用自己的真实姓名，而是使用比特币的地址公钥哈希值（hashes of public keys）来作为交易标识，具备匿名性（Arvind & Joseph, 2016）。

4 基于区块链技术的数字资产交易现状与问题

4.1 基于区块链技术的数字资产交易现状

4.1.1 加密数字货币交易现状

自 2008 年以比特币为代表的数字货币面世以来，各类数字货币层出不穷，截至 2016 年 3 月，在市面上发行的虚拟货币共有 636 类，其价值总计接近 81 亿美元，此 636 类里包括价值超出 1000 万美元的 12 类虚拟货币和价值超出 100 万美元的 47 家虚拟货币。其中价值排名前四位的虚拟货币占到了价值总量的 93.29% 以上，如下表 4-1 所示：

表 4-1 2016 年市值排名前四的数字货币（2016 年 3 月 11 号数据）

类型	市场售价	价值	流通数量	价值占比	前 24 小时内完成买卖数量
比特币	421.79 美元	6449 百万美元	1529 万个	79.79%	86.30 百万美元
以太币	10.47 美元	821 百万美元	7771 万个	10.09%	24.38 百万美元
瑞波币	0.0078 美元	289 百万美元	3409102 万个	3.61%	1.79 百万美元
莱特币	3.42 美元	147 百万美元	4491 万个	1.79%	1.39 百万美元

资料来源：<http://coinmarketcap.com>

各类数字货币以比特币为首，在 2016 年后，各类数字货币如雨后春笋般不断发展壮大，掀起全民炒币的浪潮。比特币的价格，更是从 2017 年年初的 1000 美元（如图 4-1），到 9 月份时突然开始发力，在 12 月时，创下了近 2 万美元/枚的历史新高。

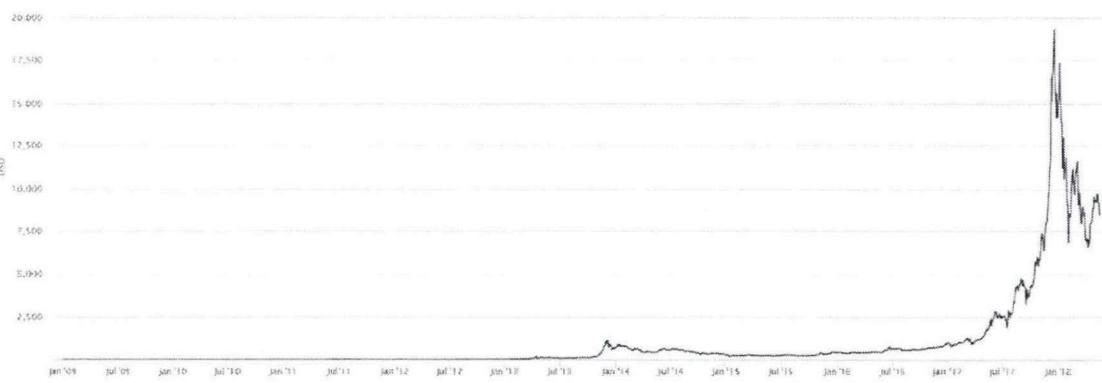


图 4-1 比特币 2009 年~2018 年价格走势

数据来源：blockchain

到了 2018 年 3 月底，据盈灿咨询不完全统计，市场上已多达 1199 种虚拟货币，

总市值约 2500 亿美元，前四大数字货币中，比特币的市值占比，从 2016 年 3 月的 79.8% 降到 2018 年 5 月份的 38.36%（如表 4-2 所示）。原因之一是国内自 2017 年 9 月人民银行严厉叫停 ICO 融资，并全面关停国内所有比特币交易所；另一原因是以外坊为代表的各类 ICO 数字货币崛起，分食市场。公众、学者和政府对币圈这些数字货币的看法差异较大，拥护者认为，他们有世界货币的特征，预示着货币制度的未来，反对者认为，该技术无法克服自身缺陷，一切繁荣皆是泡沫，终将破灭（韩裕光、孙伟等，2016）。

表 4-2 2018 年市值排名前四的数字货币（2018 年 5 月 26 号数据）

币种	价格 (美元)	市场价值 (百万美元)	可用供应量 (万个)	过去全天交易量 (百万美元)	市值占比 (%)
比特币	7576.27	129218	1705	4566	38.36%
以太坊	602.47	60049	9967	1937	17.71%
瑞波币	0.6226	24400	3918996	262	7.2%
莱特币	121.87	6910	5670	299	2.04%

资料来源：<http://coinmarketcap.com>

根据欧洲央行于 2015 年 2 月在其《数字货币》的研究报告里对虚拟货币的定义是：所谓的虚拟数字货币即是在特定状态下，能够进行与真实货币同样交易的一种数字产品，其不是各自货币管理机构发行的，仅仅是某种价值的数字表现方式。伴随相关理论分析的进步与提升，当年 11 月，世界清算组织在其《虚拟货币》的分析中对数字货币进行了更加明确的定义：其打破了传统货币的概念，依托于分布式计算方法的基础上，是一种使用了去中心化的支付系统的数字货币，作用于经济、金融及其他非金融领域，打破固有的商业运作方式实现了创新。

我国人行于 2016 年 1 月在北京举行数字资产交流会，数字货币相关专业人员依次从虚拟货币发行之整体架构、国家发行加密电子货币以及数字货币演变过程等课题开展了沟通与讨论。德勤、花旗银行以及人行的专家认为，伴随数字技术的进步和移动网络、区块链以及末端储存安全等方法的发展，世界金融领域内的交易渠道已经产生了翻天覆地的改变，会议确定了人行未来发展虚拟货币的战略规划。虚拟货币的进步同样也为人为的未来发展形成了机会和风险，也可以看出我国已认识到数字货币积极的现实意义和深远影响（曾繁荣，2016）。

4.1.2 非金融领域数字资产交易现状

区块链现在仍属于早期探索阶段（陈龙强，2016），金融领域是众多机构率先开拓

的领域，随着区块链技术受到越来越多的认可，其在数字加密货币的领域也得到广泛关注，资本嗅觉最为灵敏的金融巨头如：摩根大通、纳斯达克、瑞银集团、高盛集团、花旗银行等陆续成立区块链实验室。其他各类机构也纷纷成立各类区块链联盟，如 R3（全球顶级区块链联盟）、Hyperledger Project（超级账本）。国内比较出名的区块链联盟有 ChinaLedger 联盟（中国分布式总账基础协议联盟）、金链盟（金融区块链合作联盟）、China Blockchain Research Alliance（中国区块链研究联盟）。

表 4-3 各区块链联盟对比

联盟名称	成立时间	成员代表	研究领域
R3 (全球顶级区块链联盟)	2015 年 9 月	2015 年年底，R3 CEV 聚集 42 家知名银行包括巴克莱、瑞士信贷、摩根士丹利、高盛、汇丰、ING 等	区块链在金融行业的应用，为银行提供探索区块链技术的渠道以及建立区块链概念性产品
Hyperledger Project (超级账本)	2015 年 12 月	项目成员中，科技公司和金融机构各占三成，另有两成是区块链公司。而核心成员中科技公司更是占了六成以上。主要公司有：IBM、思科、因特尔、Accenture、Fujitsu、Blockchain、Hitachi 等。	能够保障各种数字化的资产买卖和记录，是分布式账本区别传统账目方式，形成跨领域的行业标准，譬如房产交易、婚姻登记、能源买卖等。
ChinaLedger (中国分布式总账基础协议联盟)	2016 年 4 月 19 日	万向区块链实验室、厦门国际金融资产交易中心、中证机构间报价系统股份有限公司、通联支付、浙江股权交易中心、招银前海金融等，11 家成员机构。	中国最具影响力的区块链联盟；开发研究分布式总账系统及其衍生技术，其基础代码将用于开源共享
金链盟	2016 年 5 月 31 日	机构汇集了 46 家金融公司，包括微众银行、京东金融、华为、恒生电子等	实现适用于金融机构的金融联盟区块链
CBRA (中国区块链研究联盟)	2016 年 1 月 5 日	由全球共享金融 100 人 (GSF100) 理事单位共同发起 (万向控股、厦门国际金融技术有限公司、乐视金融、中国保险资产管理业协会等)	打造区块链研究与交流平台

资料来源：《区块链从数字货币到信用社会》

目前各式各样的数字货币多种多样，我们耳熟能详的主要是以太坊和比特币，它们都是数字资产中的一种。当前的智能债券和智能股票包括将来人行可能发布的，由中央机构背书的虚拟货币也都是数字资产。这里所说的智能，主要是指应用区块链体系中信息无法篡改，同时能够实现计算机程序编写的优势，在区块链中进行债券、股票的记录与发行，可以让它们的信息数字化，同时借助系统定制好的智能合约开展点对点的个人买卖和清算。

区块链在虚拟货币市场的急速爆发以后，其在金融行业以及非金融行业的应用也不断拓展，来突破当前金融机制下的部分缺陷，譬如在金融领域内对中介组织的过度依赖、消费者权益保护、金融成本过高、效率较低。充分发挥区块链所具备的去信任以及去中心化的特性，能够全面实现解除金融行业在交易过程中对中介组织的过度依靠，促使协议公平公开，买卖童叟无欺，不用考虑支付对象可能发生不履行协议的隐

患，能够确保特定的事项形成时，系统自主执行协议，以保障协议公正，具备实际执行效力。所以在金融行业内区块链技术在财务清算、债券/股票发行与交易、推行商业积分等方面是最佳的不二首选。

4.1.3 数字资产交易平台现状

数字资产交易平台，目前多是以数字货币交易平台的形式存在，2018 年开始，基于区块链技术，市场上开发出了各种各样的数字货币。为了防范风险，国内在 2017 年 9 月开始对各类数字交易平台进行清理整顿，数字货币交易一度低迷，为了继续开展交易业务，各平台采用出海、开展场外交易等方式，极大加快数字资产交易平台的发展。

下面为几个主流数字货币交易平台的对比：

表 4-4 主流数字货币交易平台对比

平台名称	平台简介	交易模式	优点	缺点
Binance (币安)	全球领先的区块链资产交易平台，为全球区块链爱好者提供多币种、多语言的币币兑换服务，目前包含 Binance 区块链资产交易平台、Binance Info, Binance Labs, Binance Launchpad 等业务	币币交易； 交易手续费 0.1%。若持有 BNB，交易费用直接扣除 BNB，交易任何币种都有 50% 的折扣，即 0.05%	安全性高，采用多层、多集群系统架构；高达 140 万单/秒的高性能撮合引擎技术；币种比较多，手续费较低；充值提币速度较快	不支持法币交易； 由于用户量的猛增，服务器无法承载，稳定性受到一定影响； 已停止中国 IP 用户访问
OKEX www.okex. com	全球著名的数字资产交易平台之一，主要面向全球用户提供比特币、莱特币、以太币等数字资产的现货和衍生品交易服务	法币交易、币币交易、合约交易； 针对合约交易、币币交易各会员等级不同，手续费费率也不同	币种多，成交量大，安全性高，支持电脑端和 APP；支持人民币 OTCC 法币交易；合约交易占比平台成交额大；	用户反响比较差，评论较低；网站和 APP 偶尔会出现卡顿；已停止中国 IP 用户访问
火币网 Huobi.com	火币集团旗下服务于全球专业交易用户的创新数字资产交易平台，致力于发现优质的创新数字资产投资机会，目前提供四十多种数字资产品类的交易及投资服务，总部位于新加坡，由火币全球专业站团队负责运营	法币交易、币币交易、杠杠交易；所有交易手续费为 0.2%，持有平台币 HT，可享受手续费 5~7 折的优惠。	支持 OTC 法币交易，支持微信、支付宝、银行卡转账；注册流程简单，支持电脑端和 APP；币种多，成交量大，安全性高	经常有用户投诉 BTC 提币速度慢；客服服务滞后；支持杠杠交易，风险性较高；

资料来源：根据文献资料整理

随着比特币与区块链相继走进人们视线，与之相关的衍生物也在加速进入我们的眼

帘，ICO（Initial Coin Offering）就是其中之一。目前，ICO也没有什么官方定义，业内人士认为它是模仿证券市场 IPO（Initial Public Offering），将发行标的物由证券变为 Coin，如比特币、以太币，万事达币等。除了上面介绍的几个平台，北美区块链协会主席兰波曾说，在币圈或极客，ICO 早已不是什么新鲜事。ICO 最经典的案例便是以太坊，通过募集比特币，获得约 1 亿人民币的开发经费，构建了一个区块链底层系统，截止到 2016 年底，已有很多的金融机构及企业在以太坊上面开发了超过 200 个多区块链应用。

4.2 基于区块链的数字资产交易存在的问题

经过加密数字货币在市场中的急速爆发与发展之后，金融行业、非金融行业其他数字资产交易相关的应用也在不断拓展，以突破当前金融机制或传统商业机制中的部分缺陷，但其在发展过程中有其不可规避的一些问题，以致于在市场上，即使经过多年，也鲜有成熟应用面向市场。

（1）区块链中区块体积日益庞大

区块链技术在不断发展壮大的过程中，其网络节点中储存数据的区块体积也变得日益庞大，对计算机的运算能力与储存需求也将日益提高（长铗、韩锋，2016）。以比特币为例，其数据大小在 2016 年 1 月是 63.61GB，而到 2018 年 1 月已达到 149.27GB。如果用户使用比特币核心客户端进行数据同步，可能几天几夜都无法完成同步。且随着时间的推移，区块的数据量还在不断增加，给比特币核心客户端的运行带来很大困难。

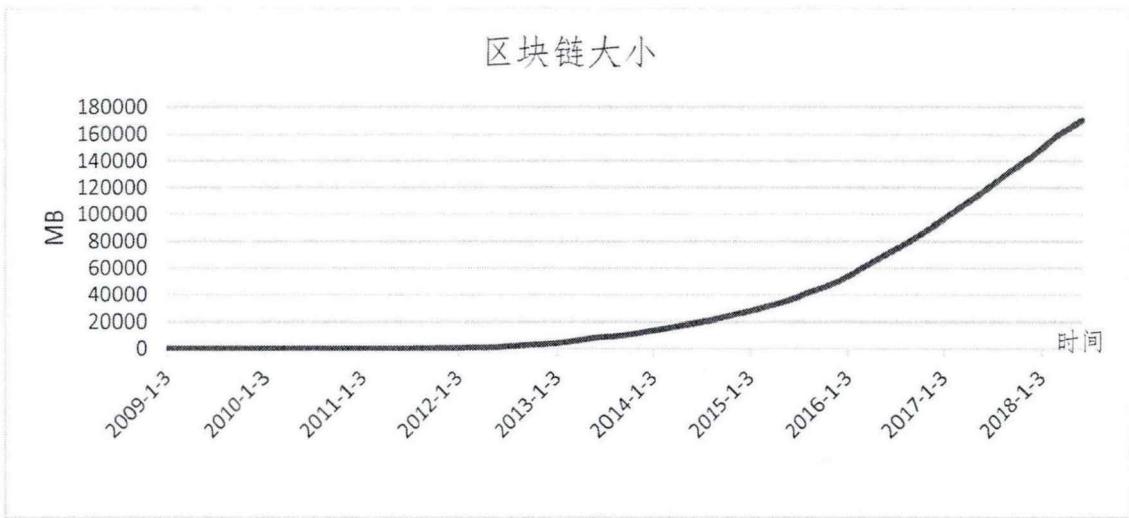


图 4-2 比特币 2009 年~2018 年区块体积增长趋势

数据来源：<https://blockchain.info>

(2) 区块链数据确认时间过长

区块链的执行问题在于速度，它需要大约 10 分钟或更长的时间去最终批准一笔交易 (Bannister, 2016)。目前的区块链交易系统，特别是金融交易系统中存在数据确认时间较长的问题，以比特币区块为例，如图 4-3 所示，当前每笔比特币交易时间大约需要 10 分钟，这对于现有金融业务，各类数字资产交易业务，尤其是当整个银行业要在全球范围内完成两个节点间的数字资产交换，而此时在若干节点的数据库里要完成这个数据的拷贝中间要消耗与等待的时间又特别长，这在当前各类交易或清算结算业务场景中，要求每秒要完成成千上万笔交易的高频交易来说，区块链目前并无法满足当前高频交易的要求。

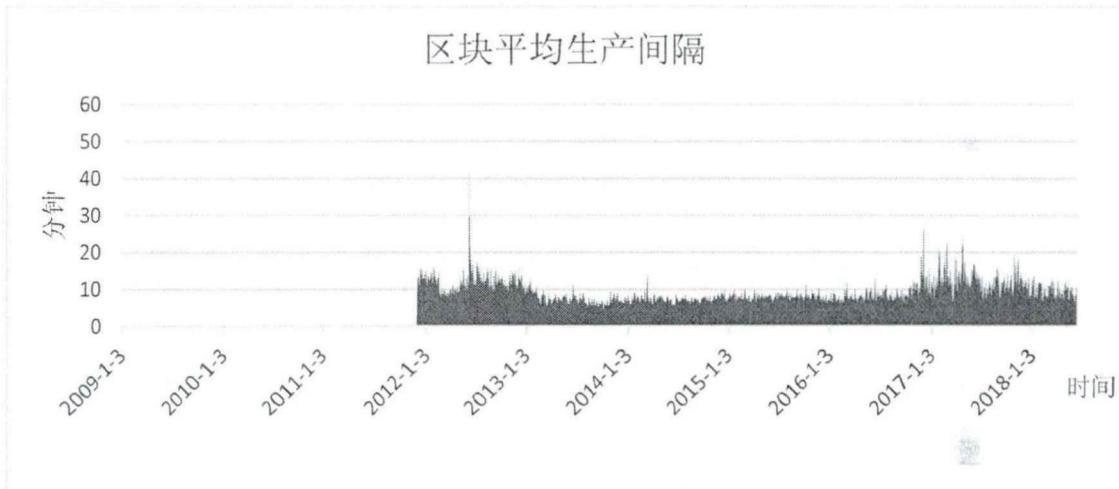


图 4-3 比特币 2009 年~2018 年区块平均生产间隔

数据来源：<https://blockchain.info>

(3) 区块交易频率过低

区块链系统交易频率较低，加之其现在挖出的资源消耗特别巨大，不仅占用极多的总算资源，也占用大量的储存资源，无法满足当前不同规模金融组织或大中型企业的资产交易或信息交换需求。如图 4-2 所示，比特币区块链每条交易平均大小为 250Byte (字节)，如果区块大小限制在 1M 以内，那么每个区块最多可容纳 4000 条交易。按 10 分钟生成一个区块的速度计算，一天能产生 144 个区块，也就是 576000 条交易，再除以一天 86400 秒，即比特币区块最高每秒处理 6.67 笔交易 (长铁、韩峰, 2016)。现在的比特币系统一秒仅可完成七个订单交易，但 VISA 要求一秒至少能快速完成上万个订单，显然区块链技术依然没有办法实现主流支付系统的交易需求。虽然用比特币不能代表所有的数字货币或数字资产，但其缺陷也侧面反映了虚拟资产交易中

所要面临的问题。

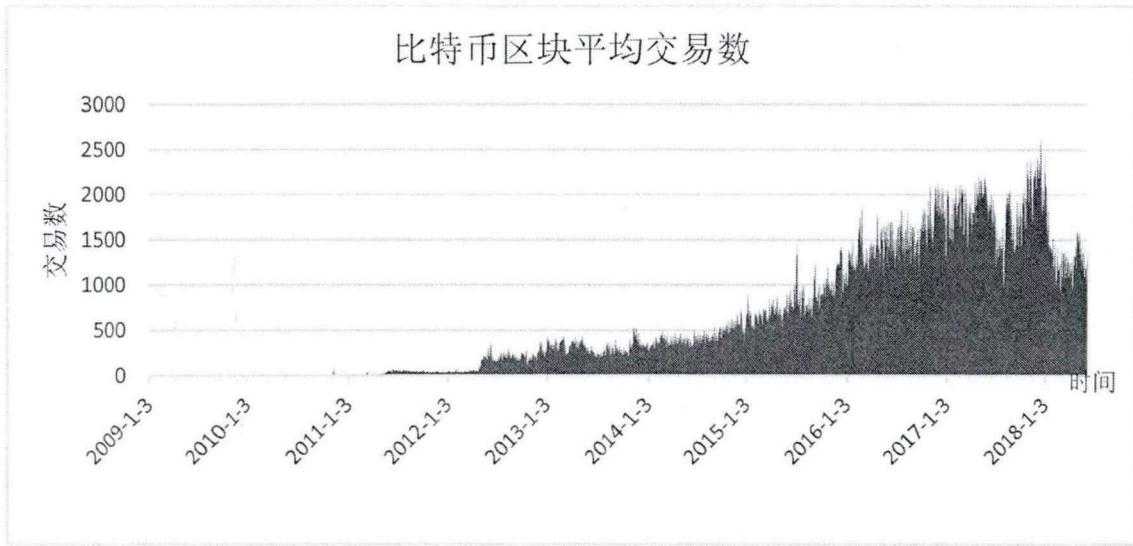


图 4-4 比特币 2009 年~2018 年区块平均交易笔数

数据来源: <https://blockchain.info>

(4) 区块链发展受到现行制度制约

从 2017 年 9 月 4 日开始，中国人民银行、网信办、工商总局、银监会等多个监管部门联合下发《关于防范代币发行融资风险的公告》，让涉及代币、虚拟货币的各种行为都变得更加谨慎，甚至相关的比特币交易所也被强行关闭，可以说，目前以比特币为首的虚拟货币交易，可能在不经意间触及到法律的灰色地带。

同时，现有金融机构、大型企业对于是否要创新，在企业内部肯定也会遇到不少阻力，因为对于任何的创新，对企业内部，既要创造经济效益，又要符合监管要求，还要与现有业务系统衔接（长铁、韩锋等，2016），其中要耗费的时间与人力、物力成本，且对现有业务造成冲击，都是企业实施创新的阻力。

除以上提到的问题，还有其他诸如交易规模、交易速率、商业模式可持续性、便利程序等问题，在当前这种情况下，市场上是否有一些落地的产品，可以较好解决以上问题的问题或进行商用？本文就从基于区块链技术的数字资产交易，在市场中的落地应用案例进行研究。

4.3 基于区块链的数字资产交易的意义

通过分析区块链关键技术的运行原理可知，该技术最突出的特点是以技术的方式

实现了无需中心机构参与的，能够稳定运行的、可靠的、去中心化系统，从数据的源头开始保障了数据的公开化，不能被篡改、可被追溯，根据具体业务场景对数字资产价值的提取只是顺理成章的事情，是数字化时代的战略选择（陈龙强，2016）。将区块链技术举一反三，应用于其他领域，其中像视频、语音及影像在内的非结构化的编码进行数字化以后，变成数字资产，也可以以资产的形式开展交易，实现价值流通。以后的实体资产如土地、汽车等也能在区块链上完成记录、明确所有权，将现在的纸质证明变为可度量的数字化资产，实现资产流通的算法化、智能化；

资产被数字化之后，在数字的世界里，将有着不受限制的扩张性、拷贝性以及能够进行多维塑造，也体现出其中潜在着的，有待于人们进一步挖掘的巨大宝矿，这一宝矿就是数字资产。其中可以包括数字化以后的债券、货币以及股票等常见资产，也可以涵盖其他无形的数字化资产，譬如品牌、信誉、版权、专利等。

资产为何要进行数字化？资产流通最便捷的办法，毫无疑问就是将资产数字化。对于公司的资产管理，资产进行数字化以后可以促进其管理费用的下降，同时提高使用效率。把保密文档以技术办法加以存储与加密，其可靠性也要极大的超过用实物形式进行保存。同时，将公司的专利、股权、品牌等资产进行数字化，作为质押获取融资，将原来企业中无形的，无法为企业带来现金流的资产全部数字化，变成资产流通，获得现金流，极大地提升的企业资金流转。大量的事实已证明数字资产是资金流通最好的方式，因为它能使资金不断流动，使资产增值并产生财富。

5 基于区块链技术的数字资产交易的案例分析

5.1 布比数字资产交易平台简介

布比（北京）网络技术有限公司（下文简称“布比”），作为国内较早研究区块链技术的公司，于 2015 年 3 月份正式成立公司，注册资本 1343 万，总部在北京，在上海、广州、深圳也有成立分公司。目前已接入几十家机构，与相关企业在商业积分、保险卡单、游戏装备、提货券、预付费卡、娱乐票券等数字资产领域，及供应链金融、股权债权、公证等领域展开合作并将区块链相关商业应用推向市场。

从公司的发展历程来看，在公司正式成立之前，其创始人蒋海是中国科学院的博士，2012 年开始就已在中科院从事区块链技术的相关研究，在区块链技术、分布式网络、密码学与信息安全方面有较深厚积累。于 2015，正式成立公司，致力于打造新一代的价值流通网络，让数字资产可在其“数字资产交易平台”中自由流通。在公司成立不久之后便融得第一笔天使轮 1000 万元，2016 年 8 月融得 3000 万的 Pre-A 融资，到 2017 年 11 月融得 1 亿元的 A 轮，从融资规模，融资速度来看，在创新科技类的初创公司中，都数得上表现亮眼。

公司主要发展历程：

- 2015 年 3 月，“布比”成立；法人代表蒋海，中国科学院博士（2010-2012），从 2012 年开始就一直从事区块链相关技术的研究和产品开发；布比平台定位于区块链技术产品服务商。
- 2015 年获 1000 万元天使轮融资；
- 2015 年 12 月，布比首个区块链商业应用案例在布比区块链平台启动。
- 2016 年，布比推出了区块链网络平台“布萌”，为用户提供场景化服务支持。据称，截至 2017 年 9 月累计用户 1200 万，月交易量超百万笔，平台中流通的资产价值已超十亿元。
- 2016 年 3 月，格格积分正式落地，基于区块链的商业积分应用面向市场；
- 2016 年 8 月完成 3000 万的 Pre-A 轮，主要由多个投资机构进行联合投资，领投机构包括招商局创投、界石创投、创新工场和启赋资本等。
- 2017 年 11 月完成 A 轮融资 1 亿人民币，由新链创投、盘古创富、联合领投。

➤ 2018年6月，布比推出商用级基础公链BUMO，获得数千万美元投资。

布比成立这么短的时间内就获得亿元融资，既得益于区块链风口，也与平台自身定位、战略布局、业务发展及过硬的技术能力息息相关。有媒体报道称，2017年8月1日，IBM（国际商业机器公司）已经公布，计划在2018年9月发布截止到目前为止的最大型的区块链商业应用项目。万向公司肖风也在去年的7月份指出，该公司为区块链创新企业准备的专项风险投资基金中的五千万美元，已经投入了两千多万美金，共有世界范围内23家创新科技企业被投资，而布比就是其中一家。

从公司战略布局来看，“布比”网络定位为区块链服务提供商，专注于区块链技术和产品的创新，已拥有数十项核心专利技术，研发出开放、高效、拓展性强的区块链底层服务平台。就采用了区块链技术的数字资产交易平台为例，布比根据具体业务场景，通过对应用层提供封装接口，方便其他企业或开发者提供快速构建上层应用，满足大规模用户数量的应用场景。

从公司业务发展情况来看，“布比”目前已接入几十家机构，面向1200万用户，有超过数十亿的资产在布比的区块链平台中流通。布比的区块链技术已广泛于数字资产、贸易金融、商业积分、电子发票、联合征信等领域，并与交易所、银行等主流金融机构开展应用试验与测试。这些应用的资产发行和流通都基于布比区块链，在数字资产可信的基础上，构建一个自由流通的数字资产网络，在该网络中资产一经发布，其后期的交易过程能够不再依靠发行者平台，资产交易从一个中心化的管理机构转化为分布式广播。布比目前在数字资产、金融、股权债券、公证领域，均有较为成熟的应用面向市场。通过这些案例的分析，参考其基于区块链的资产交易模式，为后续基于区块链的数字资产交易研究提供参考。

5.2 布比数字资产交易平台的商业模式

区块链相较于传统的互联网技术是一种新生事物，由于其还处于发展的初级阶段，而在商业领域中业务场景繁杂，用户需求多样，该技术无法满足所有要求，那么，在商用过程中可能首要解决如下问题：

(1) 可方便企业迅速完成应用对接

区块链技术虽好，但如果作为区块链技术的实施者或应用方，如果需要企业在内外部交流或实施中耗费大量的人力、物力、财力或是时间成本，那他们必然会心存顾

虑，所以，如何帮助企业或开发者快速完成区块链系统搭建或应用接入，是区块链应用平台首要考虑因素。

(2) 满足业务及用户大规模扩张需求

区块链技术发展到现在，在市场中也没有出现哪个区块链应用可以真正地适用于大交易规模或大范围客户量的商业级应用，其中的大部分还在研发中，机构或公司的用户群、交易量已达百万、千万，甚至过亿的规模，那么他们在考虑一个新技术的落地，其中一个重要指标便是看是否能与现有海量用户、交易实现平滑过度，看其是否能支持现有业务高并发、高扩展性、海量数据存储需求。

(3) 保证私钥存储安全

在金融业务中，安全是首要考虑的问题，现有区块链使用的是一串杂乱无序的公私钥，对于用户来讲并不友好，那如何在前端应用中，实现用户可以使用自己易记的用户名和密码完成登录，而在底层依旧可以利用区块链技术实现安全的稳定的、可信赖的密钥存储办法。

(4) 友好易用的运营管理体系

区块链系统是由多方共同建设维护的，对于运维或运营人员来讲，整个系统不由单方可控，提供可视化的运维管理工具，方便运维人员在该系统中进行可视化的监控管理；为运营人员提供简单易用的运营管理服务后台，方便运营客服人员进行相关营运操作也很重要。

(5) 商业隐私保护和操作权限控制

区块链一直宣称的是数据共享，信息透明，这个特点对于多数商用领域来讲反而是敏感或对立的，那么在此类分布式结构构建的多中心信任体系中，怎样完成企业所要求敏感信息过滤、用户信息保护与管理权限分配，也是在商用过程中要重点解决的问题。

基于以上问题，布比定位于为企业提供区块链解决方案，不但可以输出底层的区块链技术服务，同时也可根据企业具体业务场景，按照实际商务需求，使用布比提供的适配层进行业务封装，给上层业务提供便利，这种方法极大地减少了上层业务与区块链底层服务的对接用时，通过这种模式为其他公司或机构提供区块链解决方案。

据公开资料显示，截止 2017 年 5 月，布比平台上近十亿的数字资产在上面流通，且这些资产之间可相互打通。如 2017 年 4 月份推出的积分系统—聚分宝，在这个积分

兑换系统中，平台将个人的金香黄金账户与自身已有的积分账户实现积分兑换，应用区块链完成不同数字资产间的买卖与结算。

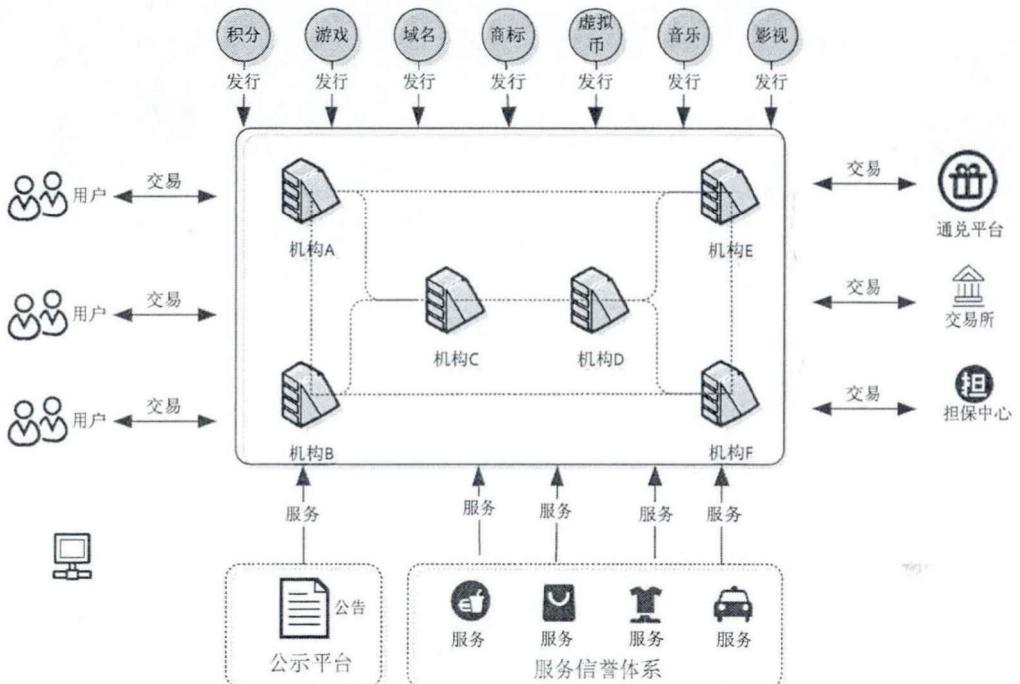


图 5-1 布比商业模式

在 2016 年 4 月份，布比作为区块链技术厂商与易诚互动旗下“比邻”合作，推出“数贝荷包”，该产品也定位为数字化资产交易平台，为客户的数字资产进行定制管理。数字资产交易是指任何可数字化的东西都可在平台上实现登记、发行；各种主体（个人、组织）也可在平台上登记、发行自己的数字资产，一旦实现资产登记，便可在平台上对数字资产进行追踪查询。

通过提供标准接口，与其他企业合作，将区块链技术在保险、积分、游戏道具、以及股权交易等范围内的数字资产中加以运用，以区块链技术为基础，致力于提高资产流动性。

5.3 布比数字资产交易平台的技术架构及特色

5.3.1 布比数字资产交易平台技术架构

Bubi Application Adaptors（布比适配层）与 BubiChain（布比区块链基础架构层）是布比区块链系统中的两个重要组成部分。使用 BubiChain 为企业提供底层基础服务，利用适配层为上层业务提供业务功能所要求的组件，为使用平台服务的业务系统提供 SDK 与 API 接口，减少因区块链的进入门槛较高，技术难度较高而引起的研发

进度慢，应用难以落地等难题。

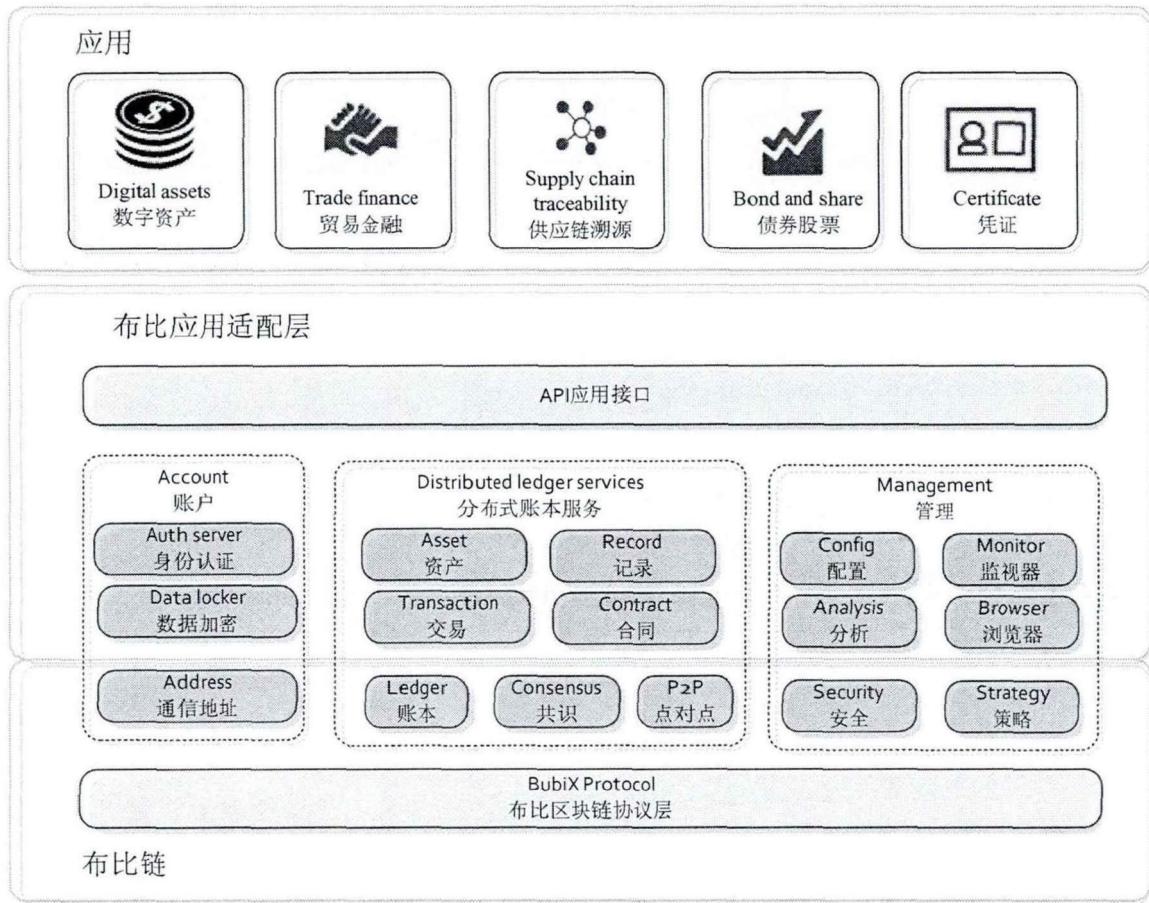


图 5-2 布比技术架构图

与普通的区块链底层服务提供商对比，布比区块链增加了 Bubi Application Adaptors 即应用适配层，公司或研发人员不用再对区块链繁杂的初级技术进行打磨，只需调用布比开发好的 API 接口，就可快速构建一个 区块链应用。目前，布比已在商业积分、游戏装备、保险卡单、提货券、预付卡、娱乐票券等数字化资产的发行及流通进行应用。针对数字资产交易，布比网络成立了“布萌”数字资产交易平台，布比链研发者之一的上海分部领导人扬帆指出，此链全力研发一种能够开展数字资产自主交易的平台，该平台中的应用使用标准化化的开发协议，平台中研发的应用不用再进行二次研发就可实现应用间的数字资产流通，满足此链中客户间的数字资产流通、价值互联以及数据流互通需求。并且，在此链中发行的数字资产能够完成点与点之间的价值流通。譬如某玩家有游戏 M 与 N 的设备，如果其不再需要 M 时，他能够把个人在 M 游戏中的装备与其他人发起交易，更换到个人需要的 N 设备。

另外，此链也能够实现不同业务领域的数字资产买卖。公司主体或研发人员采用

系统提供的业务适配层，利用平台提供的 API 接口，根据上层业务需求加以封装，就能在该平台中实现应用发布、数字资产的发行、流转与查询等功能。研发人员要做的就是注册一个布比数字资产交易平台的账号不支付任何费用就能获得平台应用的开发权限，进而拥有平台中的客户群、底层服务及平台数据等服务。链上数字资产自由流通，资产市值由链上参与的节点达成共识。

通过调查可知，现在此链在互助保险、保险卡单、企业积分、股权债券以及游戏资产交易等业务中均已得到应用。有几十家企业已参与此链，其中包括寻宝天行、众托帮、阿里云以及阳光保险等企业。而值得关注的是，寻宝天行系统中的完美世界游戏设备已经实现了使用布萌系统交换阳光保险公司的航空意外险，实现跨公司跨业务类型的资产流通。

目前，布比旗下的区块链数字资产平台——“布萌”，已发行了几千种资产，月交易笔数超百万，TPS（每秒最多处理笔数）是 3000 笔，性能还是非常优秀的（对于完全去中心化的公有链来说，TPS3000 是目前行业的共同的瓶颈）。当前社会上流通的区块链应用日益增多，然而因其技术的缺陷在商业领域中无法大规模应用，譬如人们熟知的以太币和比特币，一笔比特币交易确认时间最少需要 5 分钟，最长的甚至接近 20 分钟（杨晓晨，2016），到 2018 年交易确认时间已经至少要 10 分钟。与目前传统银行的交易确认只需秒级形成鲜明对比。

支付宝在 2014 年时 TPS 就达到了 285 万笔，区块链受限于当前分布式的记账结构，对于完全去中心化的公有链来说，要使用公有链实现大规模商用，突破 TPS3000 的瓶颈并不现实。因此在布比的区块链溯源应用基本上都采用了联盟链的设计，将原本的“一个中心”，变为“多个中心”的架构，由多个中心组成一个可信任的“生态圈”，对数据真实性背书，对交易规模化提供可能。

5.3.2 布比数字资产交易平台技术特色与优势

布比在技术方面的特色与优势主要体现在性能、扩展性、安全性和运维四个方面。通过大量的业务模型、应用模型的测试分析，布比在性能方面可达秒级交易验证，海量数据存储，高吞吐量，节点数据快速同步；在扩展性能方面可达到满足多业务区块结构、权限控制策略；同时，提供私钥存储服务，以及隐私保护方案。

5.3.2.1 性能方面

(1) 快速交易验证

通过对签名算法、账本结构、数据操作、序列化、共识机制、消息扩散等关键环节的优化，布比区块链可实现秒级快速交易验证，满足绝大部分区块链应用场景。

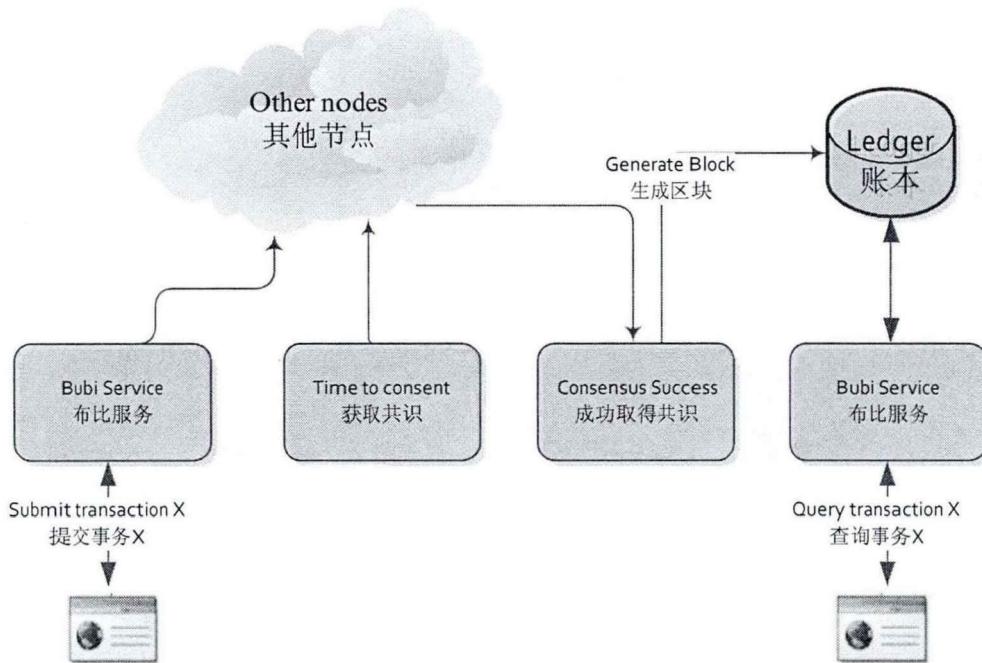


图 5-3 快速交易验证

(2) 海量数据存储

区块链复式记账模式中，系统长时间运行，历史数据不断累积。布比区块链借鉴传统金融系统中冷热数据分离存储、分表存储的机制，实现了海量数据的有效存储。离当前时间较久远的历史交易数据，非活跃的资产数据等信息可使用大数据存储平台进行存储（如 Hadoop，满足 PB 级别的数据存储）。

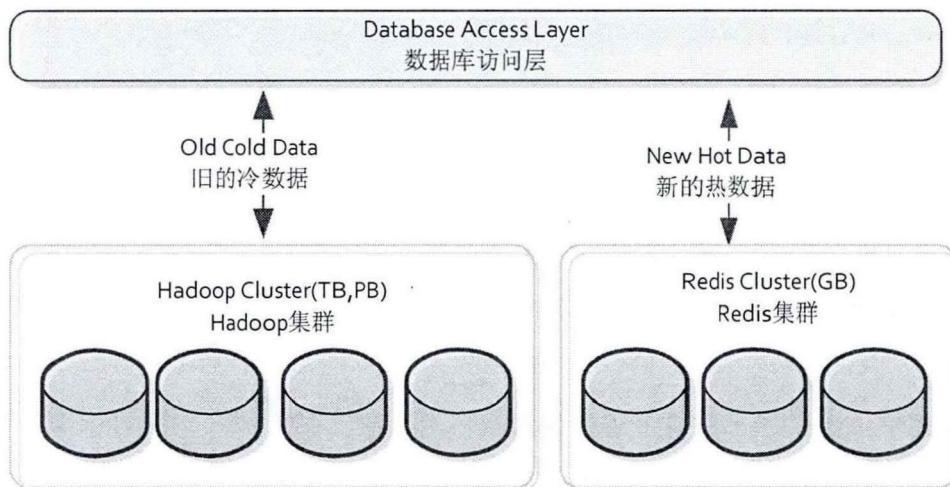


图 5-4 海量数据存储

(3) 高吞吐量

区块链的本质是一种分布式共享记账的技术，其分布式特征主要体现在分布式一致性而非分布式并发处理。为保证数据的一致性，防止拜占庭将军问题，某些特定环节只能串行执行，而无法并行。通过长期的测试与优化实践，布比区块链的处理性能已经能满足万级TPS的需求。如果再引入Off-Chain等机制，还能进一步大幅提高交易吞吐量。

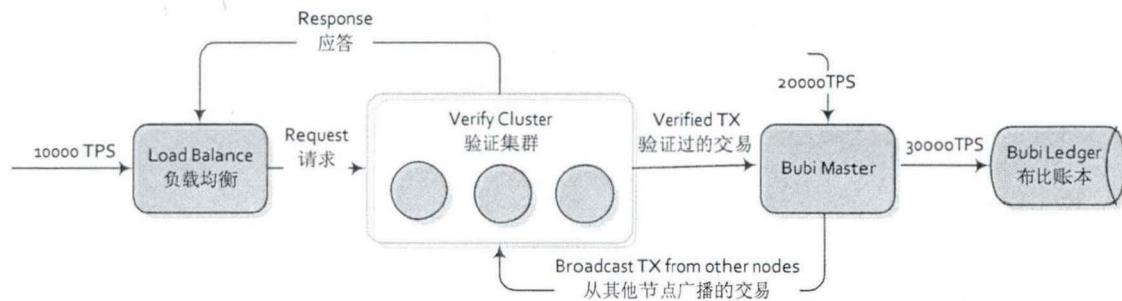


图 5-5 高吞吐量

(4) 节点数据快速同步

布比区块链支持镜像(Snapshot)机制，可以定期对本地账本制作镜像，实现便利的回滚机制，在统一共识下，可以指定镜像标签进行回滚；同时，缩短新加节点加入运转的周期，仅需同步最新镜像及少量近期交易集合，即可融入网络并参与共识验证。

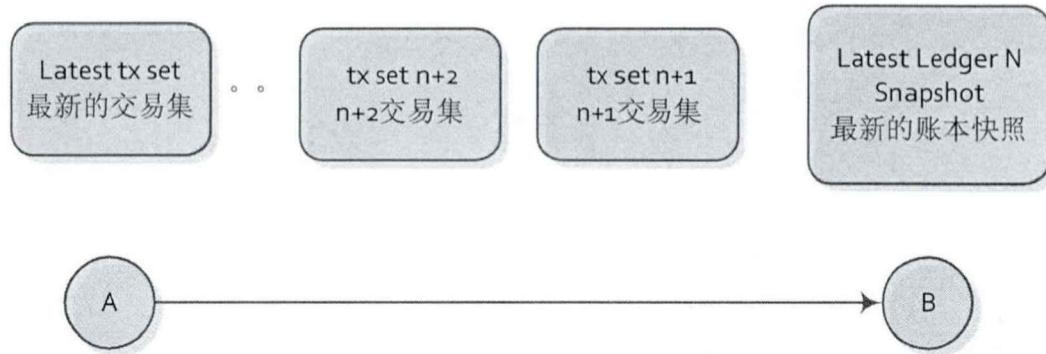


图 5-6 节点数据快速同步

5.3.2.2 扩展性方面

布比区块链的块链结构，可满足不同业务场景需求，提高系统可扩展能力，降低维护成本。可用于标记资产和资产转移，也可提供不可篡改的多维事件记录。

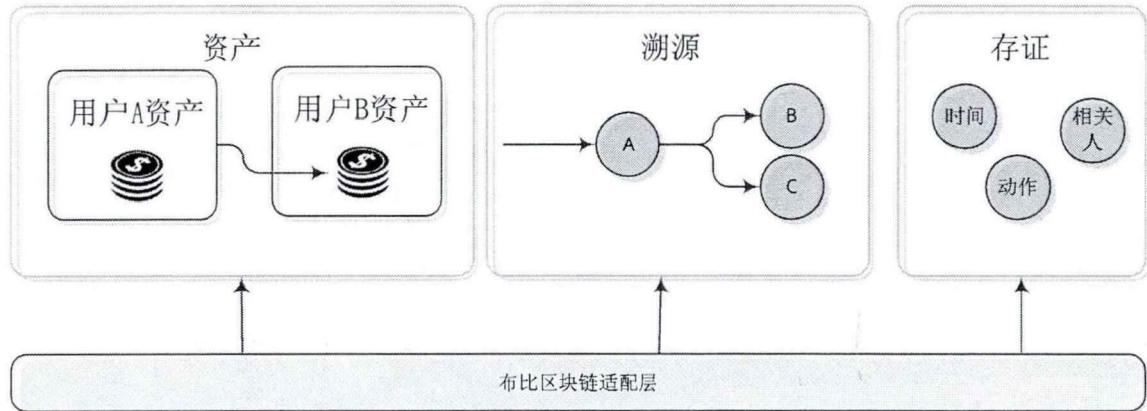


图 5-7 满足多业务的块链结构

5.3.2.3 安全方面

(1) 安全私钥存取

为了方便用户使用区块链产品服务，除了传统的客户端生成和保存机制，布比还提供网络托管存取和私钥硬件存取(U-key)两种方案。网络托管存取，即把用户名和密码通过特定算法映射成私钥并在服务端进行存储。服务器端存储的私钥均为加密数据，私钥仅能在用户端解密；硬件私钥是为了满足金融行业及物联网行业的使用需求。

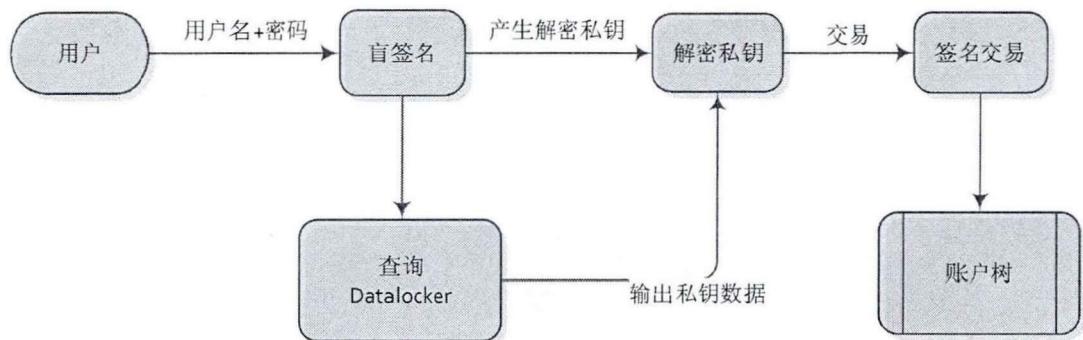


图 5-8 安全私钥存取

(2) 多重隐私保护方案

提供多重隐私保护功能。首先，区块链底层提供同态加密方式，用户所有数据均加密存储，仅用户本身可见。其次，BubiAdaptors 提供加密中间件服务，用户可根据业务需要进行选择。最后，上层应用可以在录入时对数据进行加密处理，布比负责对用户生成的加密数据进行写入和读取。

5.3.2.4 运维方面

BubiAdaptors 抽象出适用于多种业务场景的 API 接口，如：资产、溯源、存证等，供这些场景的相关业务直接使用。在新的业务场景下，布比可以基于现有的框架为用

户快速定制接口，满足业务功能需求。同时提供已封装好的，可支持多种主流开发语言（JAVA、C++、node-js、PHP）的SDK软件开发包，实现低成本快速接入。

布比提供的区块链技术服务主要有两种，一种是搭建区块链底层服务，提供标准化API接口并开放给其他企业或开发者，方便他们快速对接。另一种是配合上层应用，根据具体场景，将分布式账本内嵌到已有的应用系统中，解决行业痛点，不断优化，满足业务需求。通过对底层分布式账本的封装，降低上层应用使用门槛，在对接和使用过程中不断优化底层分布式账本和共识算法，使之趋于成熟，贴近商用。

5.4 布比数字资产交易平台的应用案例

目前区块链的应用场景，已从单一的数字货币应用，延伸到经济社会的各个领域（周平平、杜平宇等，2016），布比将区块链技术应用于商业积分、电子券、预付卡、游戏装备、保险卡单、证券化资产等数字化资产场景。所谓数字资产可以是任何数字化的资产，为资产证券化，资产数字化的发展与流通提供底层服务。相较于传统中心化系统，区块链技术对于数字资产交易，最大的优点是链上资产的流通不再依赖于发行方系统，任何有资源的渠道都可成为资产流通的渠道，由中心化的传播方式变为社会化的多方传播，极大提升数字资产流通效率。

有别于传统资产服务，各类资产证明、公证均需要第三方中间商介入，参与资产流通的角色要包含资产发行方、资产接收方、平台中介三者，资产才可完成一个流通环节。在该模式中有以下痛点：（1）资产流通依赖于在资产发行方的系统中进行使用、交易、转移，将资产流通范围限制于该系统中，平台受限、用户群受限；（2）资产流通要第三方中间商参与，资产价值越大，所依赖的大渠道中间费用越昂贵，流通成本增加。

如果数字资产的发行与流通使用区块链作为底层技术，连接资产发行方、交易者及各流通渠道，让任何形式的主体（机构/个人）均可在该数字资产网络上登记、流通自己的数字资产；支持多种数字化资产的登记、流通，实现资产登记即公示，利于数字资产的确权及追踪，有效防止资产纠纷问题，完成资产的登记、交易、确认、记账、对账、清算，提升资产流通效率。考虑到各个行业应用的可行性、成熟度和重要性及布比已落地的商业应用，本文主要列举了商业积分、保险卡单、网络互助、游戏资产交易、股权债券、供应链金融、供应链溯源、公示公证这8个场景。

5.4.1 商业积分

所谓商业积分，相信大家都不陌生，在日常各种线上线下消费场景中，人们在平常购物时，商家为了鼓励消费，会根据客户的消费水平，在客户的账户中不时奖励一些消费积分。商业积分与数字货币相似，区块链技术的安全性和去信任化，对积分持有者进行认定、确权，持有者可用自己的私钥，对积分进行消费或转让，积分流转过程链上广播、所有交易均被记录，整个过程无需第三方参与，积分消耗记录明晰。区块链技术可以使这些非金钱性的社会货币更容易被追踪、被传输、被交易，甚至于被变成金钱（梅兰妮，2016）。

现在国内外的积分业务主要有以下几种类型：

第一种：用户忠诚度积分。这种业务模式下的积分定位于提升客户忠诚度，增加用户粘性。行业大公司一般采用此类模式，如电信、银行。该模式下积分是成本中心，非盈利中心。这也是最为常见的一种积分模式。

第二种：通用积分。该模式强调的是积分的通兑和通用，通兑指商户自己发行的积分，可兑换成跨行业跨领域的“通用积分”；通用指在不同场景中均可使用。商家可将自己的积分在某平台中兑换成通用积分，此时的积分也可颇有“货币”的属性。国外做的比较好的有“Points”。

第三种：积分联盟。指不同领域的商家结成异业联盟，各加盟商共同发行一种积分，此积分可在该联盟内流通。该模式有利于提升客户忠诚度，也对联盟内各加盟商起到相互导流的作用。如英国的 Nectar（花蜜），韩国的 OKCashbag 积分计划，是国际上比较成功的积分联盟案例。

（1）行业痛点

以上几种积分模式，在国内的发展目前都不是很理想，究其原因：

首先，中心化的业务模式，限制生态系统发展。不论哪种积分模式，核心目标是吸引大量客户参与其中，构建积分系统，以确保积分消费场景的丰富及积分流通的效率。而传统的积分模式都是中心化的，天然缺失公信力，导致积分系统发展缓慢。

其次，中心化的技术架构，阻碍生态系统构建。在传统中心化的技术架构中，若要实现大量商家间的积分实时清算，相当于一个小型的“银联”跨行资金清算功能；以平安万里通为例，从 2008 年创立至 2014 年间，打通 300 多家线上主流电商积分，连接 50 万家线下商户支持积分兑换，这其间便花费了巨大的 IT 投入及时间成本。

最后，中心化的交易模式，降低积分流通效率。传统的积分交易，主要局限于用户与商家平台间的流通，用户与用户间的积分交易、转赠鲜有平台支持，导致了积分流通效率降低，流通范围受限。

国内绝大多数服务领域企业均推出了积分计划，尤其是航空、银行、通讯运营商、酒店等，都会尝试着发行平台自身积分作为用户忠诚度计划，以促进企业与客户间的交互，维护良好客情关系。这些行业领头企业的积分不管是在发行还是兑换上已经形成了一套较为成熟的体系，消费者对于这些积分也耳熟能详，但是消费者在实际使用积分的过程中满意度较低。企业为了运作这些积分系统，也需耗费较多的人力、物力。在传统中心化系统中，积分在企业内部由于技术、权限、场景受限，用户在各平台间的积分无法汇聚、流通，闲置于各个平台无法打通。内外部原因导致各企业积分利用率、活跃度不高，如何较好地平衡及运作积分系统，成为企业不得不考虑的问题。

积分本质上也是一种数字资产，以商家自身的服务或产品作为价值背书。但很多时候，这些积分零散分布在各个账户之中、数量少、价值低、使用规则复杂、核销过程繁琐，使得这些积分，只能在账户中变得非常鸡肋。

商家设计积分的初衷是为了吸引消费者的二次或多次回购，为了促进忠诚度的提升，消费者也期待通过这些积分得到一些优惠，但目前散落在各个商家系统中的积分，不一定可以给商户带来消费者的二次消费，且还要费时费力建立积分发行与兑换体系，花费巨大却可能达不到营销效果，在现有传统的积分体系中，并不能很好地满足双方现有需求。

（2）基于区块链技术的解决方案

基于以上场景，布比旗下的数字资产交易平台“布萌”，让商家可以用平台提供的接口，在接入积分发行系统时省时省力，不需要商户自己再去重头开始设计一套积分管理系统，大大降低区块链应用接入门槛。

用户也可将积分自由转赠，激活积分消费，为商家带来流量。图 5-9 为我们展示了区块链积分通兑架构，各企业以联盟链的形式在链上完成积分发行、后续积分可在链上自由流通，积分流通由单中心控制变为社会化传播。

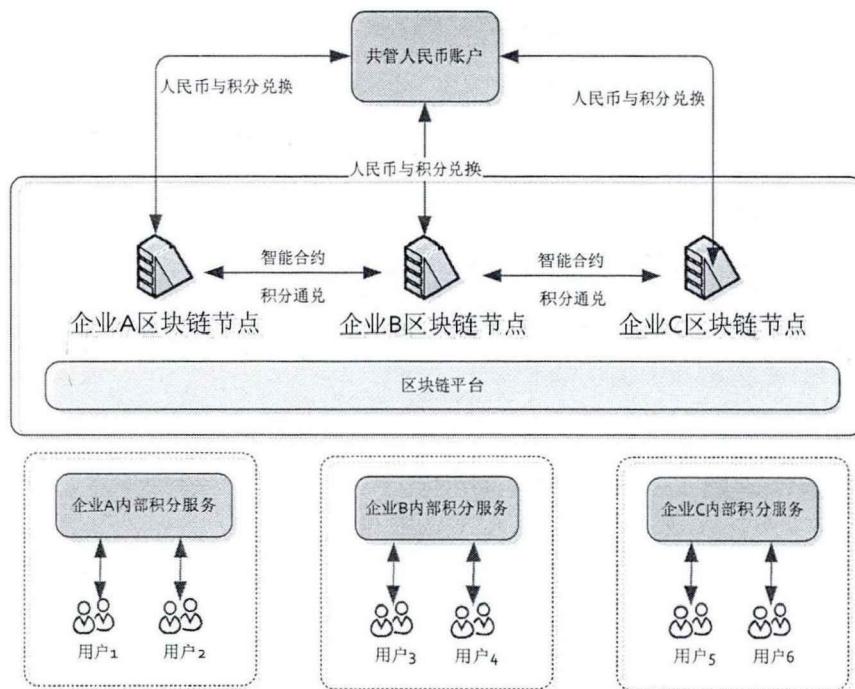


图 5-9 区块链积分通兑架构

布比作为底层技术的服务提供商与“比邻共赢（Belink）”合作，在比邻旗下产品“数贝荷包”平台上，为商户提供数字资产的定制管理服务，为企业发行并管理积分、卡券等数字资产。对于个人用户而言，用户直接通过关注平台微信服务号就能轻松查询、使用、交易、转赠积分或卡券，降低用户使用门槛，企业也可极大地降低积分系统搭建所需耗费人力及物力。

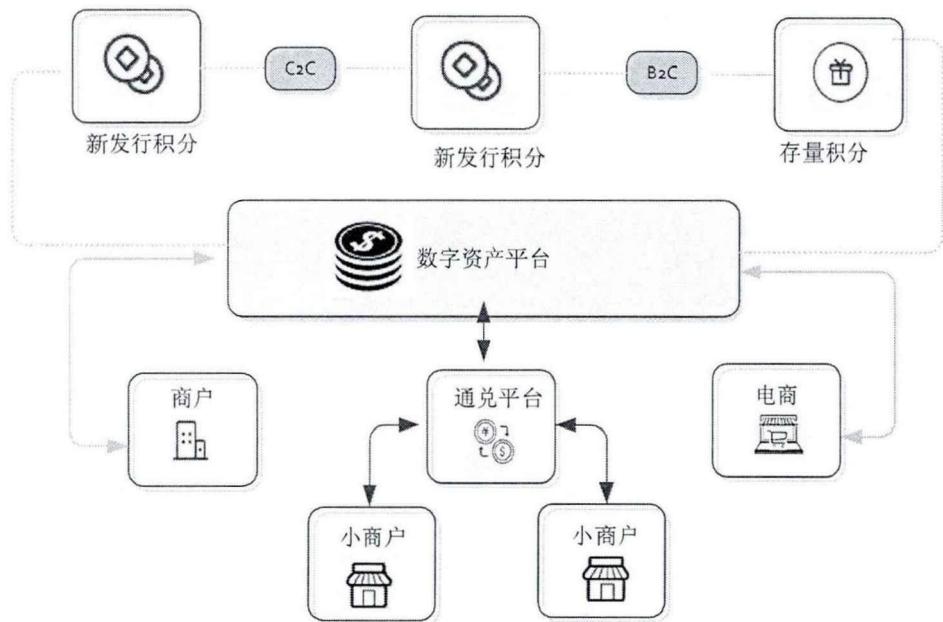


图 5-10 布萌数字资产平台商业积分应用架构

为将区块链技术更好地在商业积分领域落地，布比在 2016 年联合比邻共赢（Belink），携手国内知名保险机构——“阳光保险”开展了长期的战略合作，合作内容主要围绕着区块链技术应用展开，在 2016 年第一季度，双方尝试性地将传统保险业务架构在区块链上，发行了具有区块链技术属性的积分“阳光贝”，用以活跃阳光保险积分体系的用户流通率及使用率。

利用区块链技术“交易即结算”的特性，数贝荷包与阳光保险合作解决了积分在集团内各部门间的结算，及用户间多账户相互流通、变现的问题，成为国内较早的区块链积分应用，让原来沉淀在用户手中的积分更好地流通，据相关数据反馈显示，自该积分应用上线以来，阳光保险的积分利用率同比上升了 50%，为企业、用户及业务发展，提供良好的技术支持。目前“数贝荷包”已相继接入阳光保险、北京农商银行、安华农业保险等大型银保机构，在基于区块链技术的商业积分应用中走在市场前列。

基于区块链技术的商业积分应用，本质上要解决的问题是，构建一个去中心化的积分资产发行、流通及交易体系。体系内任何机构只要设置承兑条件，便可发行积分。积分拥有者可自由挂单买卖积分。一切交易都在去中心化的体系内进行。利用区块链“多方发行，自由流通”的特性，实现积分跨平台自由流通，积分总量恒定，交易准确透明，实现积分的自由兑换与交换。

5.4.2 保险卡单

保险卡单属于保险合同中的一种，相对于传统保单，更方便快捷，具有保险其间短，保费低的特点，常见的保险卡单有意外险、乘意险。传统的保险业态中主要由保险公司、保险经纪人、投保人组成，随着社会的不断发展，保险公司险种、交易规模、保单数量、参保主体越来越多元化，传统保险业务逐渐表现出较大的局限性。

对于消费者而言，区块链的航空保险卡单与传统渠道销售的保险卡单主要区别在于卡单销售理赔全程可追溯，信息不可篡改的特性，意味着信息一旦提交，任何人都无法通过篡改其他权益人已认可的数据来进行重新交易，中间渠道商想篡改保险价格，保单重复销售也将无法实现。

（1）行业痛点

保险卡单的数字化在互联网飞跃的今天，逐渐进行了人们的视野和日常生活，相当部分的保险卡单在售卖过程中必须依托于某一场景或渠道，譬如大家熟知的航空意外险，就要借助于旅游网站，保险出售方把保单的销售权赋给了渠道代理商，这就要

求代理商与保险发行方进行系统对接，无疑加大了人力和时间成本。航空意外险一直是保单造假的重灾区，因为航空意外险只有在飞机发生意外时，才会出现理赔，所以，大多数情况下客户即使买到假的保单也不容易发现。

另外，航空意外险大多是通过代理商进行售卖，成本几元，但经过渠道加价，到消费者手里，就可能变成几十元。且数字化保单造假成本低，代理商销售保单时，保险发行方较难监管，容易存在假保单，或重复销售等行为。

(2) 基于区块链技术的解决方案

区块链是按区块链生成顺序相连而成的链式结构，用密码学的技术保证数据不可篡改不可伪造，同时又是一个去中心化的分布式账本数据库，相比于传统的中央数据库，区块链具有安全、透明及高效的优点。

布比在和保险机构合作的业务模式中，保险卡单在区块链平台上交易、流转，保障了交易的有迹可寻，安全透明，严禁虚假保单存在。渠道代理商，只要实现与“布萌”的对接，一次对接就可以享有该平台所有保险卡单的销售资源，极大地简化了中间环节，节约了人力、物力。在2016年7月，“数贝荷包”与阳光人寿合作，成功地将传统的保险卡单数字化，阳光人寿推出“飞常惠航空意外险卡单”并构架在“数贝荷包”平台上。“飞常惠航空意外险卡单”被设计为可自由转赠的一款保险产品，在微信平台中用户可自由分享，加入了社交属性，改变了长久以来保单仅能购买自用，不能分享或转赠的境况，极大提升了保险的流通。

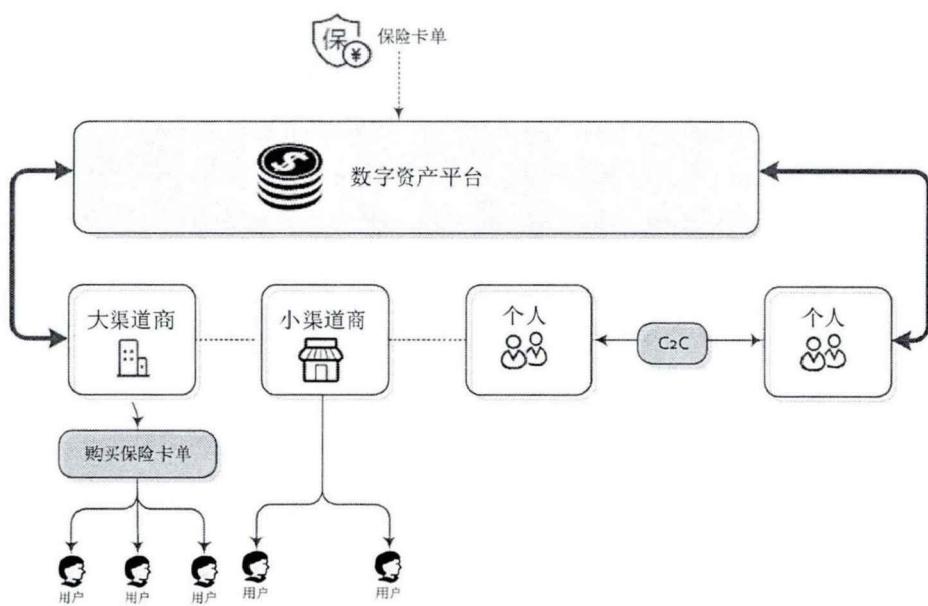


图 5-11 布萌数字资产平台保险卡单应用

使用区块链技术进行保险卡单销售较之于传统保险卡单销售主要有以下区别：

第一，卡单销售流转全程记录可追溯，确保数据真实性。创新型的基于区块链的保险卡单销售，基于区块链技术不可篡改，可追溯，可回溯到卡单销售源头，客户流转，客户理赔等全过程。参与方不仅能查验卡单真伪，也确保了卡单的真实性和唯一性。

第二，卡单销售直达用户，去掉中间商，售价更便宜。基于区块链安全可信的技术基础，卡单在平台与用户之间，用户与用户之间自由转移、赠送，去除航空公司、第三方网站、渠道中间商等环节，保险直达终端用户，节省中间费用，让惠于用户，保险价格费用降低，也可更好地提升用户的购买率及复购率，实现良性循环。

第三，保单自由转赠，提升卡单流通率及使用率。传统航空保单与机票一起购买，价格一般为几十元，购买时，只需勾选，是否已在保险公司承保，保险条款可能都不甚了解。而基于区块链的这种创新型保险卡，用户在微信端直接输入被保人及航班信息，便可投保成功，保险相关条款，理赔过程在手机端便可一目了然。相比对传统保单在保存、赠送、转让时诸多不便的问题，布比的这种创新型保单，可一次性以 60 元购买 20 人次的保单，平均 3 元一份保单，便可获得 200 万元的保障，与市面上普遍 30 元一份保单的价格相比，有极大的价格优势，同时用户可将这些保单随时随地地发送给即将出行的亲友或客户，导游或团体也可直接将保单群发给团友们，提升了保单的流通效率并赋予了保险卡单的用户社交属性。

区块链与保险行业的结合，另外一个方向是自动理赔，通过区块链的智能合约技术，保险公司可以无须等待投保人申请理赔，系统便可自动赔付。如航空延误险、航空意外险，通过调用航空公司或机场 API 接口，智能合约可自动判断某航班是否发生延误或意外，根据延误情况或意外情况自动触发理赔行为，无须用户主动干预。

5.4.3 网络互助

网络互助是一些有着相同风险要面对的群体，他们为了能有效地抵御风险，提前交出一定的补偿损失的分摊金的保险方式。在保监会 2015 年颁布《相互保险组织监管试行办法》后，相互保险获得了空前关注，众托帮、斑马社、康爱公社、水滴互助、夸克联盟、轻松互助、同心互助、17 互助等上百家网络互助平台，如雨后春笋般横空出世，为传统保险行业注入新的活力。

(1) 行业痛点

传统保险行业中，以重大疾病为例，投保人保额在5-10万元之间，但在现实生活中，因要缴纳的保费金额太高，投保人对风险意识不足，或经济不允许，没有购买足够的保险，在遇到有重大疾病的时候，就不能得到重疾险的相应补偿，这必然将蒙受经济上的损失，多年的积蓄可能就因病付之东流。

网络互助的保险具有很多优势，表现在购买流程简单、可选择性多、费用低等，在宣传、监管力度不够的情况下，人们还不能很好地看到该保险与现有各类保险的区别及优势。慈善机构要获得持续支持，就必须具有公信力，而信息透明是获得公信力的前提（周平平、杜平宇，2016）。公益慈善机构经常爆发出一些像“郭美美”之类的“黑天鹅事件”，极大地影响地民众对于公益慈善机构的信任度，由于行业内发生过使人们集体受骗的事件。如今怎样提高平台的安全系数，增加客户的信任度，使平台的信誉不再受到质疑，成为平台今后发展的首要任务。

（2）基于区块链技术的解决方案

布萌通过将用户信息，保费缴纳记录、保险交易状态等数据纳入区块链中，并和互助平台众托帮联手，就是要运用这个平台的技术优势来对平台的信息有个公正、公开的保障。在客户有理赔需求时，被保险人、医疗部门、鉴定部门、平台在填写有关理赔材料时，都会校验各自私钥，这样让伪造现象没有立足之地，使整个理赔过程公正、合规。

一个平台的安全，能使客户增强依赖感，进而对购买一个新的险种起到了推波助澜的作用。根据众托台官网实时数据显示，截止到2018年5月份，已有966万用户加入众托帮平台。以“抗癌互助医疗计划”为例，用户只需预存10元便可以获得这个计划的保障，和众多参与者构成抗癌社群，这个团体里如果有一个人得病，其他人就拿出三元或更多的资金给予资助。这样积沙成塔，在自身意外得病的情况下，别人也会不遗余力地伸出援手，以此达到互助的目的。网络互助根植于传统保险，采用创新的区块链技术，可对传统保险业进行“去中心化”改造，解决用户信任、控制潜在风险。

在整个公益流程中，如图5-12所示，用户的参保记录、出保申请、鉴定记录、医疗证明、提款记录，均可存储在区块链上，在满足隐私保护及法律法规的前提下，也可以选择性地向公众公开。为了让整个公益环节更加透明，具备权威性，鉴定机构、医疗机构、银行、监管审计机构，也可以以联盟链的形式，作为区块链系统中的节点，加入到整个公益链中，接受公众和社会监督，使得整个公益系统更加客观，透明，可

信。

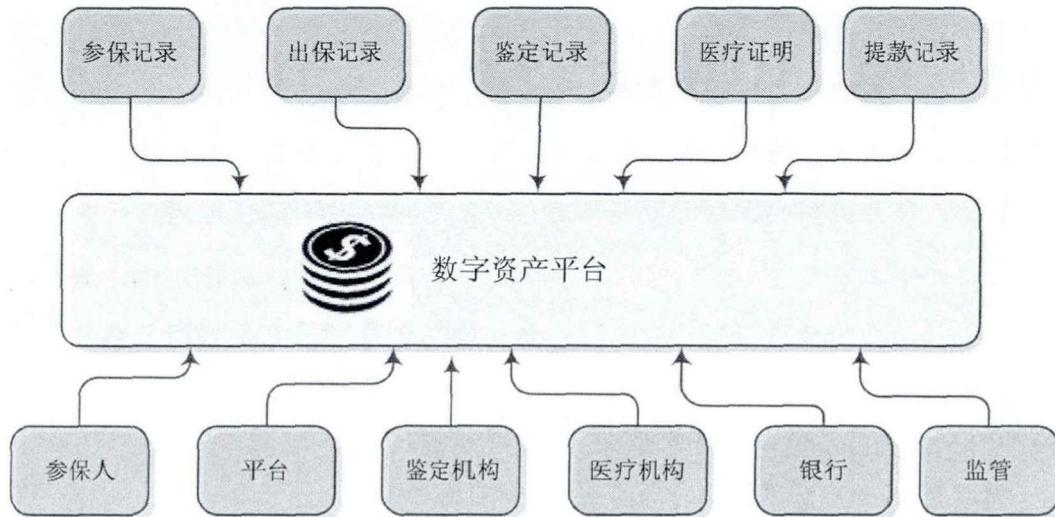


图 5-12 布萌数字资产平台网络互助应用

除了布比，“水滴互助”背后也是使用了区块链技术，来实现网络互助模式，在没有资金池的情况下，实现点对点的互助形式，且在公司在 2016 年 5 月，刚拿到 IDG(美国国际数据集团)、真格、腾讯等机构 5000 万美元的融资。

关于区块链在公益方面的应用，“支付宝”发起的公益项目也曾名噪一时，在 2016 年，在支付宝平台发起了一项为听障儿童捐赠的活动。这个活动的新颖之处是在完成捐赠后，在浏览款项去向时有意外的发现，和传统捐赠平台不同的是查看界面增加了爱心传递是通过哪个界面，其所有的爱心传递记录均被记在区块链上。从中不难看出，用户将能够清晰地查询到自身的所捐赠款项从支付宝进入到受助者账户的整个流程。

在国内的公益活动中，发挥大平台大企业的优势，开发一个技术顶尖、透明、公开的平台和运行体系，这样才能使爱心最大限度发挥出来。区块链以其自身不可篡改的独特的分布式账簿记录功能，得到人们的青睐并寄予厚望，它的共识机制和 P2P 分布式技术体系，解决了公益慈善行业中一直存在的公信力问题，在公益行业中开辟了全新的一小领域。

蚂蚁金服 CTO 程立表明，支付宝平台上，有的用户在捐出小额款项以后，这些捐赠资金离开支付宝以后，后续被如何流转，就如石沉大海。借助区块链平台，就如同一家管理投递捐款的网络邮局。如果把每笔捐款都比作包裹，在包裹所经之处都要被印上邮戳，这些邮戳处于公开、透明状态，可被一一查找。用户的捐款到达平台后，这些款项后期的流转都会自动地在区块链上得以记录并呈现，并且在任何条件下都纂

改不了，发挥区块链技术无可比拟的优势，

区块链公益账户与普通公益账户本质上最大的区别在于，区块链公益账户是利用分布式技术和共识算法来重构该行业的信任机制，把控制账本的权利由过去的指定方转化为公之于众，让每个捐款人都了然于心，发挥区块链分布式账本的作用。众人都有权记录账目，公开透明，捐款记录在节点中广播后得到共识，便将永久存在，不能改动，为了审讯和监督打开了方便之门。其次，通过智能合约，把互助的“共识”用户程序写入系统，当满足理赔规则时，智能合约自动执行，节省了核保、提交投保证明等一系列环节，简化理赔环节，节省人力。在区块链上存储数据，高度透明，不可篡改，天然适用于公益场景。

5.4.4 游戏交易

根据《2015年中国游戏产业报告》中的数据显示，2015年游戏市场销售收入达1407亿人民币，若加上历年游戏销售累计，整个游戏市场闲置游戏资产规模可观。2014年，整个游戏交易市场份额为400亿元人民币，游戏交易市场中常见的流动资产都是虚拟的，被大家所熟知的游戏资产有：（1）游戏装备（2）游戏账号（3）游戏金币（4）游戏道具等。很多玩家都做着游戏的交易活动，这些虚拟活动在平台上成功完成交易，平台做一定的寄售交易、担保交易，在交易完成后向卖方收取一定服务费，作为平台利润来源。传统游戏行业是基于HTTP协议下的中心化数据存储结构，而在去中心化的区块链技术体系中，玩家将拥有虚拟资产的所有产权，开发者或游戏厂商也将无法随意更改游戏账号。随着区块链技术的出现和不断成熟，虚拟资产去中心化存储、游戏规则去中心化制定，从技术层面变得越来越有可能实现。

（1）行业痛点

我国如今的游戏交易平台主要有两种模式：（一）如淘宝游戏、5173这类以端游游戏资产交易为主要内容的平台；（二）像魔游游、交易猫这种以手游游戏资产交易为主的平台。此类平台存在的主要弊端是交易手续费较高、平台上骗子较多、存在虚假交易、用户权益受到侵害时，得不到有效保障。

目前游戏行业中，最常见的安全问题当属玩家自身游戏账号被盗、或是游戏玩家间互相作弊；账号被盗后，玩家账号中的相关游戏资产可能会被转卖、转移，给玩家造成一定的经济损失。玩多过后通过账号申诉、客服介入等方式去追回，往往都已滞后，能追回的，可能少之又少，虽然各游戏平台采取一系列措施去保证用户的安全性，

但盗号、玩家间作弊仍不能很好地从根源上去解决。

在区块链技术成熟之前，网络游戏使用的是中心化的服务器来对数据进行处理和存储，所以这一中心化的结构在游戏中直接表现为：游戏规则由游戏厂商来制定，他们可以任意更改、创造、毁灭游戏中的任一内容。游戏场地由厂商提供，玩家依赖于厂商提供的场地。游戏账号存在于游戏厂商服务器上，不归游戏玩家所有，所有权归游戏厂商。游戏道具绑定于某个游戏账号，同样依附于厂商服务器，无法转移。由此看出，在中心化的游戏生态系统中，游戏玩家高度依赖于游戏厂商，面对游戏中一些霸王条款或不公，也表现得无能为力。

(2) 基于区块链技术的解决方案

基于以上背景，游戏公司借助于布萌旗下的布萌区块链数字资产交易平台，将游戏经济体系中涉及的代币等虚拟资产当作数字资产在区块链平台中进行流通。

如图 5-13 所示，在整个游戏生态中，各游戏公司，利用平台提供的 API 接口，使得不同服务器、不同游戏间的道具可在数字资产平台中流通；用户与用户之间可在平台中实现游戏资产的自由转移和交易，无须中间商，去除中间费用，可大幅提升游戏资产流通的便利性，及用户活跃度，从而提高用户充值率，实现游戏资产流通。在长期交易过程中，为整个游戏生态建立起可靠的信誉体系，维持游戏社会稳定。

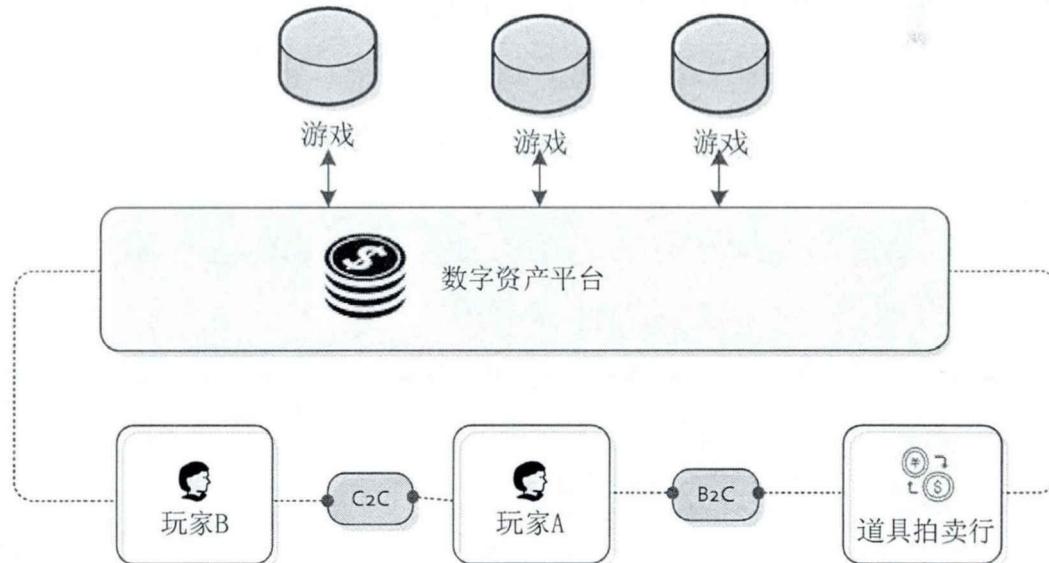


图 5-13 布萌数字资产平台游戏交易应用

与现有网络游戏相比，区块链游戏中游戏玩家与游戏厂商间的关系将发生根本性的改变。如表 5-2 所示，在区块链游戏平台上，游戏资产就是玩家自己的数字资产，归玩家所有，玩家可根据自身喜好购买游戏道具，且在平台中可自由出售、转让；当

玩家想离开游戏，玩家可以随意转让道具，无须游戏厂商同意审核，不会因为道具不可出售而带来经济损失。

表 5-1 现有网络游戏与区块链游戏区别

内容	现有网络游戏	区块链游戏
规则	游戏厂商制定	开发者写成智能合约
	厂商可随时更改	开发者无权更改
	数据存储在中心化服务器中	存储于区块链上
场地	厂商中心化的服务器	区块链上，开发者无权控制
	存储在中心化服务器上	存储在区块链上
	所有权归游戏厂商所有	所有权归游戏玩家所有
	玩家只有使用权	玩家可随意转让、出售
	随时可以封玩家账号	开发者无权封号或对账号做其他限制操作
	道具随意滥发、更改	道具发放按智能合约规定进行
	道具转让需厂商同意	玩家可随意转让道具

资料来源：根据文献资料整理

可以设想的基于区块链的游戏行业，是游戏道具最初由开发者或游戏厂商制作，但后续的游戏开发可交给玩家或社区，代码开源。如 17 年底以太坊上的 CryptoKitties（区块链养猫），游戏源代码及游戏规则完全公开在以太坊网络上，所有玩家均可看到，正因为玩家的深度参与与紧密互动，CryptoKitties 的玩家社区从游戏发售之初至今都非常活跃，以至于有段时间还造成以太坊网络堵塞。区块链游戏区别于传统网络游戏的核心差异在于规则和数据的高度透明，不可篡改，玩家拥有游戏虚拟资产，即数字资产的所有权。社区建设、社群的存在将可为游戏的成败提供可能。

除了游戏本身基于区块链技术的开发，像布比这样的数字资产交易平台，可以提供基于区块链的游戏道具交易平台，因为游戏本身最值钱的就是道具本身。游戏道具交易一直是游戏中利润率颇为可观的生意。国内比较知名的平台包括了上文提到的 5173（公司已被 15 亿元收购）、交易猫等。在国外，有 2014 年底问世的 Opskins，它是全球最大的皮肤交易平台，每月拥有 1000 万个独立用户，交易手续费在 10% 左右，2017 年第一季至第二季度营业额达 2.5 亿美元左右。乐观的市场预期，丰厚的利润，也使得这一领域涌了不少资本，如 GameFlip、Wax、DMarket、Nexium 等。GameFlip、Wax 此前就在做道具交易平台，希望通过区块链技术，解决游戏道具出售中的信任问题。DMarket 则希望打造基于区块链的跨游戏道具交易平台，为游戏开发者提供跨游戏交易的 API，所有游戏中的虚拟物品实行一键出售、一键交易或一键评估。它们基于区块链的数字资产交易模式与布比在游戏资产交易方面的思路相似，可互相借鉴参考。

5.4.5 股权债券

许多金融类的资产，把关注的目光投向了区块链，因为它公开透明、无法篡改的技术特性，能提供一种摈弃第三方金融中介的创新体系，对于金融系统的完备性有长足的发展空间，例如债券、股权、基金、票据都能纳入区块链的分布式账本里，在链上展开数字资产的交易活动实现价值流通。（张孝荣，杨思磊，2017）。

（1）行业痛点

中国的股权交易市场在近年来发展迅速，据《2017年中国股权投资市场回顾与展望》的报告中显示，中国2017年股权投资市场募资总额近1.8万亿，且整个股权投资市场目前尚处于初级发展阶段，股权基金规模暴增，但由于股权、期权上市概率低、时间长，传统IPO、并购的退出方式无法满足股权持有者对于流动性的需求。股权的持有者，不管是企业创始人、投资者还是员工，都十分希望能在公司上市前有机会将持有股份变现流通。

（2）基于区块链技术的解决方案

布比区块链官网中显示，平台已将区块链技术应用于众筹平台、区域股权交易中心、区域金融资产交易中心、私募管理平台。应用区块链技术将股权、债券进行资产的数字化、证券化，将有助于完善登记与流转服务，尤其是区块链构建的多中心体系，能够大幅地提升资产跨域流通的效率，降低交易成本，使得管理更安全、高效、可信、低成本、合规。

如图5-17所示，对于项目公司及股东而言，股权（债券）从登记到执行，数据信息连续记录在区块上并形成唯一的数字凭证，保证信息真实完整性；可追溯特性能够对更新情况实时追踪。对于股权交易中心、众筹平台等交易平台而言，通过跨域的多中心化信任，使不同组织按分布式的方式相互协作变成可能，更低的成本匹配供需，便于加密证券化资产的转让与交易。对于监管机构而言，运行的节点可以拥有对数据的广泛访问权，增强的信息披露记录，易于监管并满足合法合规性要求。

基于区块链技术的股权（债券）交易平台，可实现股权信息在线登记，股权激励方案在线自主设计，员工期权在线签章授予，股权激励计算在线管理等功能，将股标（债券）从登记到执行的所有数据信息以时间链的形式在区块链上呈现，并形成唯一的数字凭证，确保信息的真实度与完整性，帮助企业建立端到端的信用体系，为投资人、投资机构提供一个高效、可信的资产流通环境。

在实现方式上，股权交易更多地是在联盟链（Consortium Blockchain）中进行，因为公有链公开透明非安全性保障，而私有链又有强中心化特性，采用联盟链的方式，只有一部分指定的节点，指定的部分人才可追溯平台中的所有交易信息，既保证了弱中心化的集体维护，又尽力维护了信息的隐私。

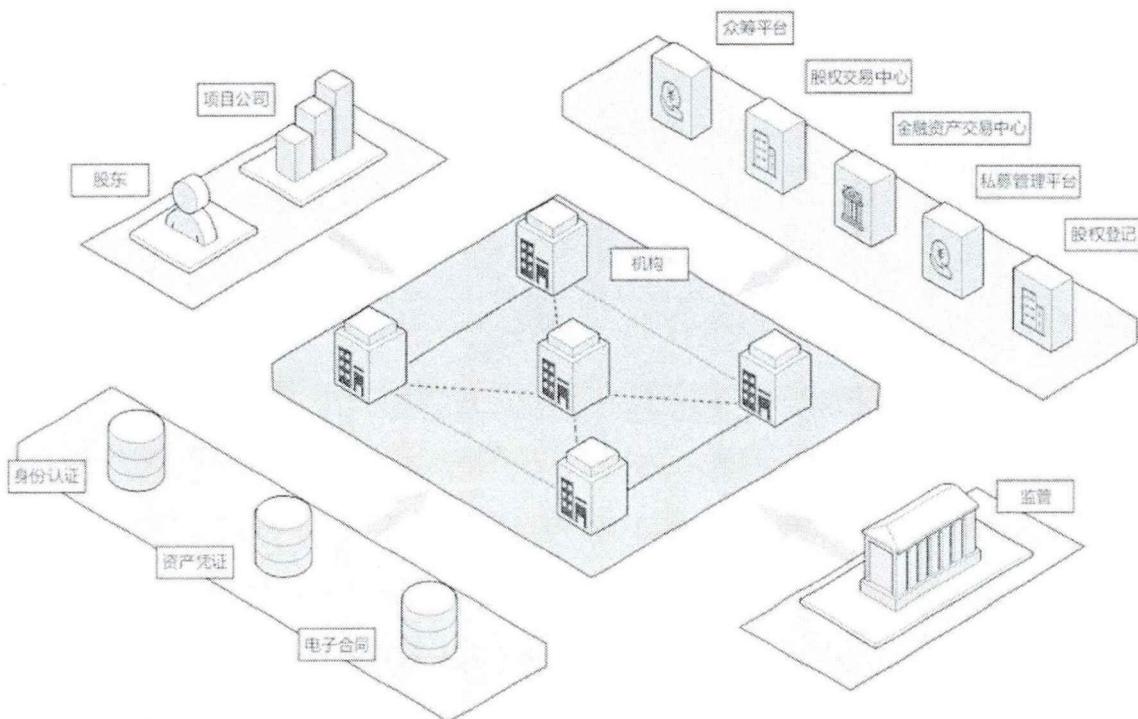


图 5-14 布比股权债权解决方案

资料来源：布比官网

就在最近 2018 年 3 月，摩根凯瑞资本（Morgan Creek Capital Management LLC）宣布收购 Full Tilt Capital LLC，成立 5 亿美元的区块链基金，旨于将企业股权和债权转换为数字货币，实现资产流通。凭借区块链技术构建安全、可信的股权资产管理平台，将可很好地解决股权（债券）交易过程中的信息不透明、交易不可信问题。

5.5 布比数字资产交易平台的其他应用案例

除了上文提到的数字资产交易，布比在其他领域也均有涉及，虽然以下应用不能准确地归类为数字资产交易，但在当前市场商业级应用中也表现抢眼，对区块链应用落地与实践具有较高的借鉴意义，所以，本文也对这类应用做简要分析。

5.5.1 供应链金融

供应链金融，根据MBA智库中的解释，供应链金融是指一种需银行充当金融中介的融资方式，以银行为媒，充当大型企业和中小微企业关系的枢纽，将他们联合起来，而后研发出可被双方灵活使用的金融类产品和服务的形式。一个商品的供应链周期从最初的购买原料开始，到产品加工最后制成商品，再由渠道代理或分销商卖出去，不可或缺的参与主体有：（1）供货商（2）加工商（3）分销商（4）消费者，它们构成了一个完整的供应链路。

（1）行业痛点

供应链金融主要是给中小企业或小微企业提供综合的金融解决方案，此类业务在中国大陆虽然已推行十多年，但因为供应链上的信息不透明，制约了该业务的发展（周立群、李智化，2016）。在当前的供应链环境中，中小企业存在融资难、融资贵的问题，根据《中小微企业融资缺口报告（上）：全球缺口有多大》报告显示中国40%的中小企业存在信贷困难，或是完全无法从正规金融机构获得外部融资，或是达不到正规金融体系的融资要求。

加之，在整个供应链体系中，有着强大资金后援、实力强劲的龙头企业，凭借其自身优势，对上下游的合作企业在价格、交货等交易条款方面往往又不够人性化，如账期拉长、价格压低、交货时间缩短等严苛要求。中小企业受到打压，发展受到桎梏，而这些没有话语权的企业，恰恰是大多数的中小企业，最终可能导致这些中小企业资金链断裂，造成整个供应链的失衡。

（2）基于区块链技术的解决方案

在整个供应链金融体系中，是典型的多主体参与、信息不对称、信用机制不完善的场景，区块链技术的出现与其有天然的适用性。

布比面对整个供应链中存在的金融问题，使用区块链技术应用于消费金融理财、仓单质押融资、应收账款融资、票据托管贴现、大宗商品交易等场景。通过区块链技术的共享账本为记账依据，充分实现信息、资金、物流统一；以核心企业的信用（核心企业到期付款的能力）为保障，并作为整个产业链条下第一还款来源，风险可控；设立拆分、流转的收益分配机制，鼓励应收资产逐级流转，满足不同场景、不同参与方资金诉求。

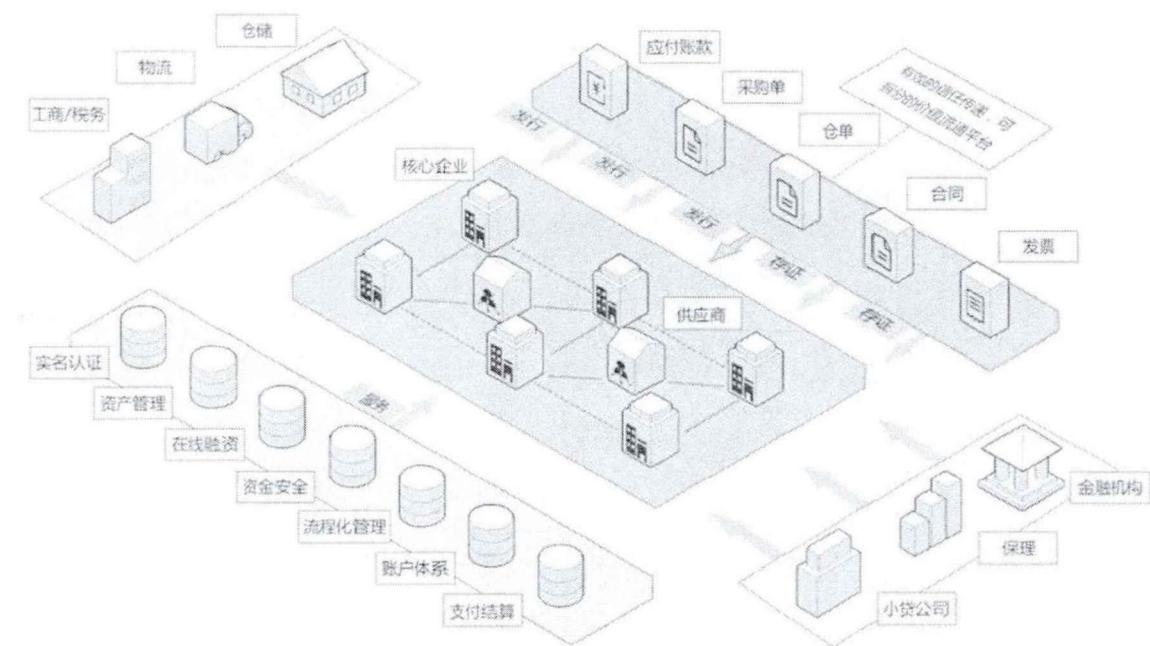


图 5-15 布比供应链金融解决方案

资料来源：布比官网

为满足该应用场景，布比发布了“壹诺金融”供应链金融平台，将区块链技术与供应链金融结合，将传统企业贸易过程中的内销行为，用区块链技术转换为一种可拆分、可流转、可持有到期、可融资的区块链凭证。平台提供实名认证、资产管理、在线融资、资金管控等服务。满足各参与方在业务层面的作业管理要求。

对于产业链上游核心企业，他们处于产业链的中心位置，他们的信用往往只能覆盖到与其有直接贸易往来的一级供应商或一级经销商，无法传递给更需要金融服务的上下游中小企业。通过自身信用价值传递，打破信息不对称，解决产业链下游中多级供应商融资难、融资贵的问题，降低产业成本、优化资金配置。

对于中小企业来讲，基于核心企业信誉，打造商业银行、保理公司、物流、仓储等多主体参与的平等协作平台，保证流转中的信用传递，实现多级供应商享受低成本的金融服务。

对于金融机构而言，布比将数据授权共享，打通链中参与主体各层间的交易关系，降低机构间信用协作风险与成本，可更好地获取到业务量多，风险可控，议价空间更大的投资资源。

在传统的贸易融资中，商票、银票流转困难且不可拆分，应收账款、预付账款、

库存等更是如此，借助区块链平台，将此类资产进行数字化，在区块链平台中登记，因其已转为数字化资产，且可拆分，流通将更加便捷，方便企业根据自身需求转让或抵押，加速资产的流通，为企业创造现金流支持。

在一个完整的供应链金融生态中，最理想的状态是将所有参与主体上链，形成数据共享的合作，但在商业落地过程中，很难一下就把所有相关资源及主体整合上链，可从关键企业或主导者自身资源切入，将整个供应链金融生态逐渐做大做强。

5.5.2 供应链溯源

“溯源”顾名思义，就是追踪记录有形商品或无形信息的流转链条（长侠、韩锋等，2016）。通过对每一次信息流转进行登录，可对商品产地进行追溯、防伪鉴证，根据溯源信息优化整个供应链环节，基至于提供供应链金融服务。供应链平台很适合用区块链技术作为监管或认证手段。（周平平、杜平宇，2016）。现代供应链虽然也善于利用数据，但是缺乏信任。纵观历史，组织间、公司间、人与人之间的不信任（包含担心信息可能落入竞争者手中）严重阻碍于信息资源的共享。反过来，即使信息真的实现了共享，数据通常并不完全可信。

（1）行业痛点

首先，传统的溯源系统，使用中心化的账本模式，整个供应链系统中的参与者将供应链环节中的产生的各类信息分散、孤立地记录和保存在各自的系统内，信息封闭不透明。导致链条上各参与方信息不对称，在出现相关事项或状况时，彼此难以准确获取事态信息，指出问题之所在，影响供应链效率。

其次，在传统中心化的模式下，源头企业、渠道商都是整个链路中的利益相关者，信息由哪一方来进行保存与维护都存在不可信，因为当账本中存储的信息不利于利益相关者时，账本会存在篡改或账本被该中心化机构毁坏的情况，账本信息是否可信存疑。

最后，因为整个链条中的信息不透明，当供应链中各参与方出现纠纷时，举证或追责将变得费时费力，要利益相关者出具对自己不利的证据，在某些情况下将变得不可行。

供应链交易过程涉及到供应商、工厂、销售渠道、客户等多个交易主体，需将原材料到成品产出并实现交易整个链条串起，要在各交易主体之间进行交易行为的认证，实现整个交易过程有据可查。如图 5-15 所示，在传统的交易当中，通常会与某一权威的第三方中心机构合作，实现交易行为认证，。

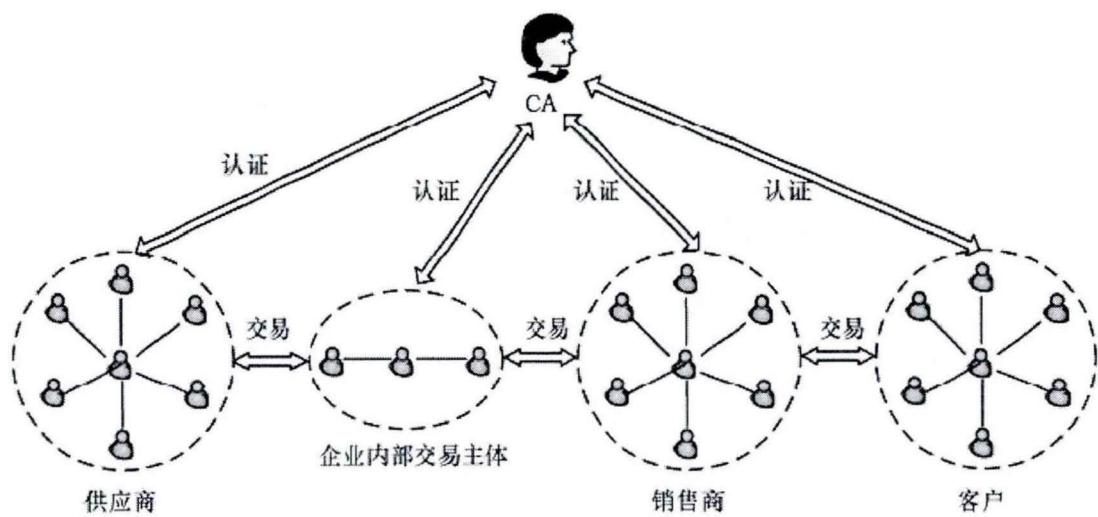


图 5-16 供应链传统独立中心认证模型

资料来源：《供应链的可信溯源查询在区块链上的实现》

（2）基于区块链技术的解决方案

区块链分布式账本，可以创建永久的透明的资产相关交易记录，进而建立一个牢不可破的信任链。每条记录都有时间戳，可追踪过往发生的所有事件。要访问区块链上的数据记录，只有授权者才可访问，参与者可以是特定部分的参与者，也可以是所有参与者。数据所有权和访问权可以是匿名的，但可在需要身份验证的合作伙伴间安全地进行识别。简而言之，可同时广泛地共享并保护数据记录。

区块链去中心化的特性使其不用依托于第三方中间机构为认证方，它的多中心认证方式让各个交易参与者都具有认证资格来参与交易行为认证。从图 5-16 中可以看出，供应商、企业内部交易主体、销售商、客户中的任一交易主体都可对交易行为进行证明，任一交易方有要更改记录的不良企图时，会有另外多个交易方拿出证据使其无以遁形，并能把它驱逐出供应链系统。如果销售商想欺骗客户时，客户本身就在链上除了用自己的能力，再联合一些交易方，形成合力，证明其确有欺诈行为时，也可将销售商屏蔽于供应链系统之外。同理，客户假如想对销售商瞒天过海，在交易中的非法过往，将会在链上被留存与记录，严重者将会受到取消交易资格的惩罚。

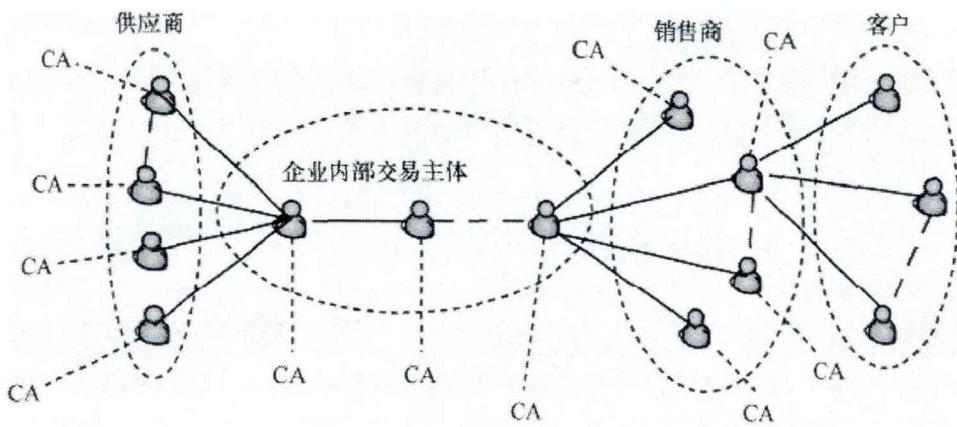


图 5-17 基于区块链的供应链动态多中心协同认证模型

资料来源：供应链的可信溯源查询在区块链上的实现。

布比目前已将区块链技术应用于食品、药品、消费品、艺术品等领域的溯源工作，特地上线了对应的溯源平台“物链”。该平台运用区块链多中心信用、安全、可靠、高效、低成本的特点，为企业制造商、电商、各级分销商、零售商、消费者、仓储、物流、提供供应链溯源服务，产品可双向追溯、辅助防伪。做到供应链关键信息实时采集、共享，提升流通效率，实现多方共赢的有机市场运行体系。

在区块链上跟踪货物来源可降低风险，提高生产和分销质量，制造商可了解他们收到的原料是否符合生产要求，采购者可确定商品的运输是否条件适宜，从而减少浪费、损耗和瑕疵，也可减少欺诈、盗用和假冒伪劣行为。

除了布比，国内市场上目前已有不少公司积极开展区块链溯源的相关应用，如：阿里巴巴旗下的“天猫国际”，截至去年底，大胆引入了国际上近七十个国家的约 4100 种商品 16400 个海外品牌，这些商品利用区块链技术来进行全球原产地追踪，再辅以大数据寻根溯源，对引进的品类进行全方位追踪，最早记录可始于原材料生产、加工、检验、出厂、运输、海关检验检疫等信息都了如指掌，让用户对产品质量得以放心，有证可查。

再如：2017 年底，众安保险与顺丰优选合作运营的区块链“步步鸡”，在顺丰优选的 APP 中首先出售，购买者，只要登陆手机 APP 或顺丰网站，就能成功购买。购买者在收到产品时，可以用手机查询，就能一览无遗地看到商品的全部信息：鸡的品系、养育人厂、成长足迹、出栏时间等，商品的详细信息呈现于区块链中，真实可信，解

决了商品的信任问题。

在国外，英国初创公司 Provenance，通过将 RFID 标记（Radio Frequency Identification，射频识别）与区块链结合，对海鲜商品进行验证，从海鲜捕获地印度尼西亚海岸开始，一路追踪到其被运输到行业中要求最严苛的采购者——日本寿司商人手中，满足客户对商品的高品质要求。同样，在英国的 Everledger 因向比特币区块链上传 98 万个钻石规格信息而闻名。2016 年 9 月，Everledger 的首席执行官兼创始人 Leanne Kemp 推出了该公司新构建的平台，通过金伯利进程认证流程对钻石进行数字认证。Everledger 基于 IBM Bluemix 上的 IBM Blockchain 高安全性业务网络构建，并通过云提供，在过去的一年中开发了一个全球数字账本，用于追踪和保护全球奢侈品。IBM 基于云的区块链解决方案可以防止未经授权的访问和篡改，通过抵御内外部威胁，保护数据，确保切入点和网络完整性，满足钻石业严格的安全要求。

现在中介机构在整个供应链中扮演的最重要角色，为上下游建立信任关系，从认证商品是否安全、合规，到融资和执行货物买卖付款，值得信赖的中介机构可降低双方交易风险，但他们在中间必然也会蚕食利润。使用区块链溯源技术可清晰地掌握中间各环节关键信息，及时揭示商品/资产的位置、所有者、处理人，及商品/资产状况。利用这些可靠的实时数据，对于商品的流转、库存、交货时间也都可以做到更加准确的预估与调配，更好地管理整个供应链的上下游及各个环节，从而及时规划流程、库存管理、纠纷解决、减少浪费及质量控制。链上各角色之间的问责机制、信任感也可进一步得到保障，区块链技术的出现也将慢慢地取代中介机构这一角色。

对于未来的奢侈品行业，高端葡萄酒等，以上几个公司的成功案例对于保护商品来源和真实性会带来重要的影响，创建永久记录来保护商品真实性，与供应商的合作，将会确保在路通环节上做出保障。许可型账本对访问权限严格控制，区块链状态的读取和修改，严格限制于几个用户，去中心化的同时维护确保信息的真实与准确。这些成功案例预示着在未来区块链领域也会更多结合被应用。

5.5.3 公示公证

根据 Wiki(维基百科)的含义，公证是由于法人、自然人或组织机构发起的，公证机构按照相关的法定程序对民事行为、事实、文书进行事实认证、合法认证并出具认证结论的活动。换句话说，公证是有关机构对一些事物提供保证和证明，这些事物可以包括文件、发明、交易、合同、身份等内容。

而网络公证在MBA智库中这里指的是借助于网络，通过存在于网络中的公证机构对网络上的文件、交易、身份等做强化性的证明和认可，同时可对证据做出保全，行使法律监督行为，做出具有法律效应的认证活动。

公证的本质是为了向公众证明某种结果、关系或状态的真实存在，传统的公示公证方式需要第三方机构背书，且证明过程又稍显烦琐、复杂、低效。利用区块链技术去信任、信息不可篡改的特点，将这些信息登记于区块链上，达成共识链条，相对于传统的公示公证方式，在安全性和有效性上得到极大提升，提高信息公示的公信力。

(1) 行业痛点

在现有传统的公证体系中，一般由公证机关行使公证职能，即需要一个专门的第三方机构来提供信用背书，这其中需花费高昂的时间、人力、财力及制度成本，像各种证书的公证，如学位证书、房产证、结婚证、驾驶证，经常有公证需求，而整个公证过程，手续繁琐，效率低下。

现有各国公证中心保管公证文书的方式可能是在带有日期的材料上盖章，拍照载入系统，这些纸质或电子资料非常有可能遭到系统攻击，或时间较久而丢失。对于信息的公示，公信力是核心。即使是在当前的大数据时代，也并没有解决公信力的问题，因为数据完全受控于系统管理者。

(2) 基于区块链技术的解决方案

为了提供公示服务，布比打造了区块链公示公证平台服务商“数链”，基于区块链技术，为慈善组织、政府机构、物业公司，提供进出账公示服务，将资金使用流向透明公开化，促进公共事业发展，为政府、企业提供招投标公示服务，提高招投标信息对称，防止滋生腐败，降低成本。

公示的本质就是通过将信息公开化获得大众群体的确认及共识，这与区块链达成共识后不可篡改的本质具有异曲同工之处。在链上的各种招投标公示文件将生成唯一的散列值记录到区块链上，打上时间戳记录到公证系统中，区块一旦生成，文件信息将无法篡改，文件完整地记录着事件所对应的时间、人物、内容，可供追溯；且各文件是分布式的记账结构，某些节点的破坏并不会影响数据的完整性，只要有一个以上的节点存在，被认证过的数据便可被完整追溯。公示公证文件存在的真实性与完整性在区块链平台中因其分布式、多中心化的特性得以保障。

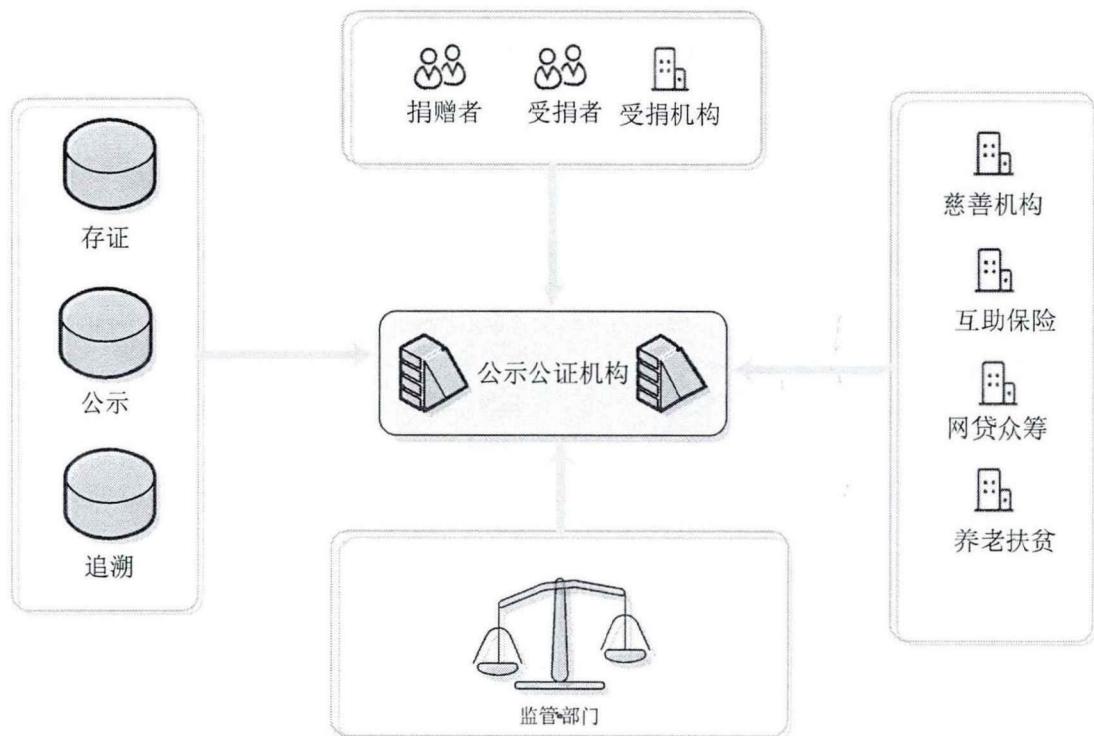


图 5-18 布比公证公证解决方案示意图

区块链应用于数字公示领域，相比于中心化网络系统，优势在于：公示内容一旦在区块链上发行，就不能再次被修改或者删除，受限于区块链的协商机制和多节点设计，作为平台也无法再修改和删除公示内容；相比于传统纸质加印章的公示方式，基于区块链的数字公示提供了更难复制和更容易鉴定真伪的安全机制；而相比于纸质实物公示的方式，其传播成本更低，更容易分发和保存。

6 案例启示

6.1 案例实施成果总结

布比作为区块链的新兴服务平台本身就是一个复杂的系统工程，在当今行业热潮中并没有因为 ICO 的火热便转型去做 ICO，而是将平台定位为“让数字资产自由流动起来”务实前进，目前已是行业内较为优秀的区块链服务公司，在同行业中做出显著成绩。

自 2016 年 8 月布比入驻微软加速器以来，成为该孵化器中区块链公司之一，整合微软加速器资源，推动中国区块链技术的快速发展。在短短一年当中，在前文介绍的多个领域中，均已孵化出较为成功的产品，并在市场中接受检验。

如表 6-1 所示，布比目前已在区块链多个领域中孵化出对应的区块链产品应用，第一个领域就是数字资产交易，截止到 2018 年 5 月份在数字资产交易平台中已累计用户超 1400 万，与国内十几家银行及保险公司合作，如华安保险、阳光保险等，另外有 1000 多家商户也会逐渐接入该系统。

第二个领域是供应链，将供应链生态中的上下游打通，把大企业的信用释放出来，为小企业背书，让中小企业在这个生态链中可享受到大企业的信用背书，降低融资难度及融资成本。建立的壹诺供应链金融平台在 2016 年 5 月便完成了数百万的天使轮，并与钱香金融合作，钱香金融以该平台提供的区块链底层服务，截至到 2018 年 5 月已累计交易 32 亿人民币。

第三个领域是公示公证，与众托帮、斑马社、中国红十字基金会合作，将区块链技术与公益结合，发挥其去中心化、可追溯、数据不可篡改的特性，所有公益资金流向透明，解决了公益中会员与会员间的信任问题。截止到 2018 年 5 月，众托帮中已有 967 万的用户加入，让公益慈善更加公开透明。

表 6-1 布比区块链技术应用成果

应用领域	服务平台	合作企业	成果	业务
数字资产	布萌	华安保险、阳光保险、格格积分、云商租赁、好哥哥、芸券	截止 2018 年 5 月 28 号，用户累计已超过 1436 万，24 小时交易笔数达 14.82 万笔	积分、优惠券、游戏装备、理财券、提货券、电子保单；

续表 6-2 布比区块链技术应用成果

应用领域	服务平台	合作企业	成果	业务
金融	壹诺供应链金融平台	钱香金融	截止 2018 年 5 月，钱香金融累计交易 32 亿元	票据、仓单、应收账款、征信、消费金融等；
股权债券	金股链	青岛港航联合商品贸易场有限公司等	2016 年 8 月获得 500 万天使融资	股权、债券，这两点目前在国内做的比较复杂；
公证公证	数链	众托帮、斑马社、人人互助、中国红十字会	截止 2018 年 5 月，已有 967 万的用户加入众托帮	公益慈善、供应链溯源、权属登记、社区治理、政务公开

资料来源：根据布比官网及其他资料整理

第四个领域是股权债券，这两个领域在国内用起来相对较为复杂，目前布比是建立了金股链平台，将股权债券相关应用场景进行落地。旨于利用区块链技术加密股权、债券等证券化资产，并为相关机构提供身份认证、资产凭证、电子合同服务。

根据中投顾问发布的《2016-2020 年区块链技术深度调研及投资前景预测报告》，在报告中着重分析了区块链技术在支付、数字货币、金融、医疗、物联网及包含公证类、数字版权、智慧政府、自治社会等领域，与布比正在研究与应用的领域不谋而合，随着技术的发展，这些应用也趋于成熟更好地服务市场。

6.2 案例实施主要问题及建议

区块链技术在某些行业中已开始走向市场进行应用，利用其分布式的记账模式展开交易，重新构建了信任机制，简化了交易过程，节约了人力和物力，让市场运作效率得到了有效的提升，开辟了价值流通网络的先河（陈龙强，2016）。通过区块链技术可以解决在虚拟经济体系中的信任问题，数字资产被高度数字化，在流通过程中有迹可寻，能被追溯，交易过程根据发生时间被记录，来源与去处都公开、透明。但因为该技术现在还处于初级阶段，大家都处于摸索状态，所以，在应用落地过程中不可避免地，要面临着一些通用问题。

6.2.1 系统安全

首先，布比是一个提供区块链底层服务的平台，从技术特点来看，区块链是可靠的、安全的、值得信赖的技术，在实际运用中却可能因开发者或调用企业运用不当而差强人意，平台的底层服务由相关企业或开发者自行调用，他们在开发过程中可能存在

在技术不成熟、业务逻辑设计不严谨，而存在一些没被发现的漏洞与安全问题，许多数字货币交易平台就因系统漏洞遭遇黑客攻击，导致用户或平台损失惨重。

其次，在区块链运作体系中，验证客户身份的唯一标识是私钥，如果用户丢失密钥数字资产无法找回。在常见的业务模式中，应该把私钥和客户的真实身份互相捆绑，而且不是由客户，而是由运作方来管理私钥。因此，密钥的安全性、可靠性就成了商业运作过程中的重中之重，要切实加以重视。安全性问题，不单单是由区块链技术自身能完成的，它也要结合具体业务场景，借助于内外部的技术力量得以解决。

6.2.2 技术挑战

在传统货币银行学中存在“不可能三角”也称为“三元悖论”（陈一稀，2016），在数字货币经济学中也存在不可能三角的问题，即在数字资产交易中不可能同时满足“去中心化、低能耗、安全”这三个要求。为了追求去“中心化”和“安全”，则无法实现“高效低能”；追求“高效低能”和“安全”则无法完全“去中心化”；追求“高效低能”和“去中心化”，则必须牺牲“安全”。在实际应用过程中要充分考虑系统的整体性，根据业务场景，平衡好这个“不可能三角”的关系。

对于完全去中心化的公有链来说，TPS3000（每秒最多处理笔数）是目前行业的共同的瓶颈，为解决这一瓶颈，布比采用联盟链的形式，将原本的“一个中心”，变为“多个中心”，虽然布比现在已能达到月交易笔数超百万，对交易规模化提供可能，但要达到像支付宝在2014年时TPS就达到285万笔的记录，区块链技术尚有很长的路要走。

6.2.3 法律风险

数字资产最大的问题是法律保护问题，像比特币因其强隐藏性，在贩毒、军火交易、支付绑架赎金等方面被广泛应用。如：2017年在世界上造成巨大影响的勒索病毒事件，犯罪分子把比特币作为赎金，想按图索骥地找到他们有相当难度。当前的法律条文中没有将数字货币和比特币当作一种资产，有关的政府机构认定只它们为虚拟商品。同时为了防范风险，央行在2017年发布了“关于防范代币发行融资风险的公告”，对60家ICO平台开展整顿工作，给数字货币交易平台带来重大打击，为了规避这些法律灰色地带，布比暂时也没有开发“加密数字货币交易”的相关应用。

同时，区块链技术的首要特点是去中心化，对中央银行机构，及传统金融企业是一个颠覆性的冲击，会导致相关国家机构和部门持谨慎态度，对区块链应用的落地与普及产生疑虑。去中心化这一技术突破，规避了传统中心化结构的束缚，但正因为其

去中心化，所以没有明晰的参与主体，造成了监督和管理上的困难。

2016年我国出台的民法总则中，对新兴的民事客体（如数据信息、虚拟财产）作了规范，在法律法规上真正确定了知识产权、商标权等无形资产的所有权，制定专项法律加以保护。但是仍有为数不少的无形资产尚未在法律法规中得到确权，数字资产要获得有效的法律保护将是一个长期且艰难的过程。监管机构在面对此类新兴技术时，应当保持密切关注，并做好积极应对措施，制定相关标准规范，更好地支持此类科技创新产品可被合理地落地应用。

以上问题，布比作为市场的先行者，目前可能还无法完全克服，虽然有些产业已投入使用区块链技术，但并不代表要推翻原有的市场体系，而是在试图更新，整合到现有系统中。各大产业对区块链技术的应用，目前更多是在论证、试验阶段，离真正投入市场进行大规模商用还有一段距离。若能有效地规避并解决以上问题，相信在不远的将来，区块链技术落地项目的数量及质量有望迎来新的阶段。

7 结论

区块链技术从 2008 年的比特币启蒙时代开始发展到现在，近 9 年的时间经历了不断的发展与探索，但目前仍处于理论验证阶段，其真正进入高速发展期，是从 2016 年开始，但主要都集中在加密数字货币交易领域（以比特币为代表），数字货币交易方面的技术已相对成熟，而在智能合约和分布式账本方向的具体应用尚处于初步实践阶段，在非金融领域更是全新领域，布比在数字资产交易方面的应用与探索基本也是处于从启蒙到高速发展的状态。要将区块链技术从理论到实践，建立一个商业级的，符合各类业务场景的基于区块链技术的数字资产交易应用，还要面临诸多挑战。

本文剖析了区块链的相关核心技术，包括其定义、运作原理、核心技术，并对区块链技术在数字资产交易方面的案例，进行深入分析。通过本文的研究，读者可以对区块链的相关核心技术形成整体上的认识，并对区块链在数字资产交易（而非仅局限于数字货币应用），甚至是整个信息科技产业中的位置和发展趋势形成更清晰的认知。

通过对布比基于区块链技术的数字资产交易应用案例进行实证分析，研究基于区块链技术下的各类数字资产交易行业痛点、并提供对应解决方案，得出以下结论：

(1) 一切可被数字化的资产均可在区块链中交易

一切可被数字化的资产，均可以通证化（Tokenization），以 Token 的方式代表任何权益与数字资产，并放到区块链上进行流通。如商业积分、保险卡单、游戏资产、股权债权、合同、证书等。

(2) “不可能三角”，安全第一

区块链在应用过程中存在的“不可能三角”问题，在业务应用当中，特别是资产交易过程中，“安全性”是首要考虑因素。布比作为区块链底层服务平台，提供标准化的、定制化应用接口，根据具体业务场景开发者与合作机构，可自行开发满足其业务需求的商业应用，极大地降低了行业的进入门槛。

(3) 职能部门牵头开展应用示范

为了加速区块链数字资产交易的应用，监管部门可起牵头作用，带领大中型企业联合高校、科研机构、金融机构进行产研合作，重点攻克区块链技术中的重难点，并加速技术标准化进程，为发展优秀的区块链创新企业提供指导意见，并出具相关政策扶持，开展应用示范，营造良好的区块链应用发展氛围。

(4) 监管机构一同上链，解决监管盲区

因区块链技术的去中心化特点，与互联网传统的中心化交易模式有较大区别，监管机构或传统金融机构对该技术的应用与推广持顾虑态度。如果能结合区块链自身的技术优势，比如账本共享、应用快速对接、消息实时传输等特点，让上级监督部门作为区块链中的某一节点加入链中，由传统的行政强制，转化为参与主体，使其获得了最真实、可靠的数据。对区块链技术加以正确利用和管理，强化政府的行政职能，采用一些智能化监督机制，能最大程度地使监控成本下降，使监管职能切实落到实处，相较于传统的数据监管方式将取得重大突破。

区块链技术的基本思想虽然起源于比特币，但发展到今日，区块链并不仅仅局限于比特币，在技术方面的研究更侧重于除数字货币之外的应用。区块链技术在其发展上有一定的局限和安全隐患，但它在现有的应用领域，如开源社区中发起的开放的“以太坊”和“超级账本”项目，各类溯源应用，跨境汇款等，再加上布比在各领域中的落地应用分析，充分证明了区块链的价值。

在一切可数字化的资产及场景中利用区块链技术实现去中心化、程序化及自动化存储、交易。其应用领域可包含（但不仅局限于）上文提到的：商业积分、保险卡单、网络互助、游戏资产交易、股权债券、供应链金融、供应链溯源、公示公证等诸多领域。毫无疑问的是，区块链技术在已经落地的领域，确实带来了生产力提升，解决了现有业务场景中所存在的问题。未来一段时间内，随着区块链技术的不断成熟，将为我们新一代信息技术及经济社会转型提供技术支撑。有理由相信，随着更多商业应用场景的出现，区块链技术将在未来金融和信息技术等领域占据越来越重要的地位。

参考文献

- [1] Batlin A, Jaffrey H, Murphy C, et al. Building the trust engine, How the blockchain could transform finance (and the world) [R]. UBS , 2016: 9-14.
- [2] Scott, B. How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance? [R]. United Nations Research Institute for Social Development. 2016(12):11-17.
- [3] He D, Habermeier K, Leckow R, et al. Virtual Currencies and Beyond:Initial Considerations[R]. IMF, 2016(1):7-37.
- [4] Crawford,S.&Piesse, D. Blockchain technology as a platform for digitization, Implications for the insurance industry [R]. Ernst & Young Global Limited, 2016:4-11.
- [5] Morini, M. From “Blockchain hype” to a real business case for Financial Markets [R]. Bocconi University and Banca IMI, 2016.
- [6] Kraft, D. Difficulty control for blockchain-based consensus systems. Peer-to-Peer Networking and Applications[R].2016:397-413.
- [7] Fanning, K. Blockchain and Its Coming Impact on Financial Services[J]. Corp. Acct. Fin, 2016, Vol.27 (5):53.
- [8] Shah S, Dockx A, Baldet A, et al. Unlocking Economic Advantage with Blockchain --A guide for asset managers[R]. J.P Mogan. 2016:3-18.
- [9] Huckle S, Bhattacharya R, White M, et al. Internet of Things, Blockchain and Shared Economy Applications[J].Procedia Computer Science, 2016, Vol.98:1-6.
- [10] Swan, M. Blockchain thinking:the brain as a decentralized autonomous corporation[J]. IEEE Technology and Society Magazine . 2015(12):41-52.
- [11] Yanovich Y., Mischenko P.& Ostrovskiy A. Shared Send Untangling in Bitcoin White Paper [R]. Bitfury Group, 2016.
- [12] Joseph L.N., John Qu&Feng Han . 区块链--银行业游戏规则的颠覆者[R]. 麦肯锡大中华区.2016(05).
- [13] 安庆文. 基于区块链的去中心化交易关键技术研究及应用[D]. 硕士学位论文, 东华大学, 2017: 11-15.
- [14] 鲍烨童. 哈佛教授谈未来经济的十个重要领域[J]. 中关村. 2016 (02) : 80-85.
- [15] 蔡凯龙. 美国关于区块链的研究和教学[J]. 新经济. 2016 (19) : 86-87.

- [16] 蔡钊. 区块链技术及其在金融行业的应用初探[J]. 中国金融电脑. 2016(02): 30-34.
- [17] 曹月佳, 承安. 区块链的发展方向是数字资产[J]. 国际融资. 2016(11)34-35.
- [18] 陈龙强. 区块链技术: 数字化时代的战略选择[J]. 中国 VC/PE 评论. 2016(11)56-58.
- [19] 长铗, 韩锋. 区块链: 从数字货币到信用社会[M]. 中信出版社: 2016: 69-73.
- [20] 陈一稀. 区块链技术的“不可能三角”及需要注意的问题研究[J]. 浙江金融. 2016(02): 17-19.
- [21] 冯珊珊. 区块链: 信用背书大数据时代的可能性[J]. 首席财务官. 2016(06): 14-17.
- [22] 【英】弗里德里希·冯·哈耶克. 货币的非国家化[M]. 新星出版社, 2007: 54-57.
- [23] 谷勤. 区块链技术在金融业的应用探析[J]. 金融科技时代. 2016(11): 39-42.
- [24] 龚鸣. 从证券的角度开始讲: 区块链为什么能成为一种颠覆性的技术[J]. 新经济 New Economy. 2016(19): 84-86.
- [25] 郝延山, 龙晏明. 联盟链技术在资产证券化场景的应用探索[J]. 清华金融评论, 2017(04): 39-41.
- [26] 黄芳芳. 数字资产时代已至? [J]. 经济. 2016(33): 30-35.
- [27] 黄锐. 金融区块链技术的监管研究[J]. 学术论坛. 2016(10): 53-58.
- [28] 杰基海兰, 阿琼卡帕尔. 区块链: 颠覆还是服务[J]. IT 经理世界. 2016(09): 20-22.
- [29] 李钧, 龚明. 数字货币: 比特币数据报告与操作指南[M]. 电子工业出版社, 2014(1): 10-12.
- [30] 李群. 区块链技术不是阳光雨露, 巨大的风险隐含其中[J]. 商. 2016(13): 169.
- [31] 李焱焱. 国际比特币跨境支付的发展与中国未来应用的前景[J]. 对外经贸实务. 2015(09): 54-56.
- [32] 李莹, 陈左, 周昆平. 把握基于区块链技术的互联网金融新模式[N]. 上海证券报. 2016-5-18 (08).
- [33] 刘秋万. 区块链技术发展与银行业应用[J]. 金融电子化. 2016(06): 11-13.
- [34] 林晓轩. 区块链技术在金融业的应用[J]. 中国金融. 2016(08): 17-18.
- [35] 何广锋, 黄未晞. 区块链技术本质以及对金融业的影响[J]. 清华金融评论. 2016(04): 102-106.
- [36] 刘德林. 区块链智能合约技术在金融领域的研发应用现状、问题及建议[J]. 海南金融. 2016(10): 27-31.

- [37] 谌麒艳. 区块链: 金融业即将面临的一场革命? [J]. 银行家. 2016(07): 14-16.
- [38] 马殊玥. 数字货币下的区块链技术发展研究 [N]. 金融时报. 2016-4-11(10).
- [39] 梅海涛, 刘洁. 区块链的产业现状、存在问题和政策建议 [J]. 电信科学. 2016(11): 134-138.
- [40] 穆启国, 陆婕. 区块链技术调研报告之二: 区块链技术进化论 [R]. 成都: 川财证券研究所, 2016: 6-7.
- [41] 秦谊. 区块链技术在数字货币发行中的探索 [J]. TSINGHUA Financial Review. 2016(05): 19-22.
- [42] 荣希. 区块链技术在资产证券化中的应用设想 [J]. 金融证券. 2016(03): 153-154.
- [43] 商瑾. 区块链技术在金融领域的应用与局限 [J]. 债券. 2016(9): 59-62.
- [44] 宋湘燕, 黄珊. 区块链技术在商业银行的应用前景 [N]. 金融时报. 2015-12-21(012).
- [45] 孙建钢. 区块链技术发展前瞻 [J]. 中国金融. 2016(8): 23-24.
- [46] 王永利. 央行数字货币的意义 [J]. 中国金融. 2016(8): 19-20.
- [47] 王晟. 区块链式法定货币体系研究 [J]. 经济学家. 2016(9): 77-85.
- [48] 吴仲, 邢治俊, 陈富节等. 浅析区块链在金融领域的应用和挑战 [J]. 科技经济导刊. 2016(28): 253.
- [49] 夏新岳. 基于区块链的股权资产购买和转赠设计与实现 [D]. 硕士学位论文, 内蒙古大学, 2016: 7-12.
- [50] 谢伟玉, 王胜. 区块链技术: 颠覆式创新——区块链和数字货币系列报告之一: 入门指南 (上) [R]. 上海: 申万宏源研究所, 2016.
- [51] 姚国章, 吴春虎, 余星. 区块链驱动的金融行业发展变革研究 [J]. 南京邮电大学学报. 2016(05): 1-9.
- [52] 益言. 区块链的发展现状、银行面临的挑战及对策分析 [J]. 金融会计. 2016(04): 46-50.
- [53] 袁勇, 王飞跃. 区块链技术发展现状与展望 [J]. 自动化学报. 2014(04): 481-494.
- [54] 张波. 国外区块链技术的运用情况及相关启示 [J]. 金融科技时代. 2016(05): 35-38.
- [55] 赵衍琛, 陈丽如. 基于区块链技术的数字货币与传统货币辨析 [J]. 企业导报. 2016, (19): 188.

- [56] 张泽云. 虚拟货币发展的潜在影响及其监管问题初探 [D]. 硕士学位论文, 浙江工商大学, 2015.
- [57] 张孝荣, 杨思磊. 腾讯区块链方案白皮书 [R]. 腾讯 FiT (支付基础平台与金融应用线)、腾讯研究院. 2017: 20-25.
- [58] 曾繁荣. 基于分布式账本技术的数字货币发展研究 [J]. 西南金融. 2016(05): 63-68.
- [59] 周立群, 李智华. 区块链在供应链金融的应用 [J]. 信息系统工程. 2016(07) 49-51.
- [60] 周平平, 杜平宇等. 中国区块链技术和应用发展白皮书 (2016) [R]. 北京: 工业和信息化部信息化和软件服务业司. 2016: 6-23.
- [61] Buterin V. Ethereum White Paper: A next generation smart contract & decentralized application platform [EB/OL]. 2015.
<https://github.com/ethereum/wiki/wiki/WhitePaper>.
- [62] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. [2008-10].
<https://bitcoin.org/bitcoin.pdf>.
- [63] 布比 (北京) 网络技术有限公司. 布比区块链产品白皮书 [EB/OL]. [2016-08].
<http://www.bubi.cn/bubichain-white-paper>.