第 3 章　区块链＋数字货币

3.1　数字货币概述

3.1.1　数字货币的起源与定义

1. 数字货币的起源

1982 年，戴维·乔姆(David Chaum)在顶级密码学术会议——美密会议上发表了一篇论文《用于不可追踪的支付系统的盲签名》。论文提出了一种基于 RSA 算法的新密码协议——盲签名，利用盲签名构建一个具备匿名性和不可追踪性的电子现金系统，这是最早的数字货币理论，也是最早能够落地的实验系统，得到了学术界的高度认可。1994 年布鲁斯·施奈尔(Bruce Schneier)的经典教材，就专设一节，探讨戴维·乔姆的电子现金协议。

戴维·乔姆提出的电子现金系统有两项关键技术：随机配序和盲签名。

随机配序产生的唯一序列号保证数字现金的唯一性;盲签名确保银行对该匿名数字现金的信用背书。戴维·乔姆的理论及其研发的 E-Cash 激发了研究者对数字货币的兴趣。经过近 40 年的发展,数字货币已经在戴维·乔姆理论的基础上融合了包括群盲签名、公平交易、离线交易、货币的可分割性等在内的新概念。

但戴维·乔姆当时建立的模型还是传统的银行、个人、商家三方模式。每个使用过的 E-Cash 序列号都会被存储在银行数据库中,且每次交易系统都要验证 E-Cash 序列号的唯一性,因此系统会维持一个已交易序列号的数据库,随着交易量的上升,该数据库就会变得越来越庞大,验证过程也会越来越困难。

2008 年,一位化名中本聪(Satoshi Nakamoto)的神秘人提出了一种全新的电子化支付思路——建立完全通过点对点技术实现的电子现金系统,将戴维·乔姆的三方交易模式转变为去中心化的点对点交易模式。其技术思路:把通常意义上的集中簿记分拆为约每十分钟一次的分布式簿记,簿记的权利由全网竞争选取,簿记数据按时间顺序链接起来并广播全网。任何节点均可同步网络上的全部簿记记录,均可投入计算资源参与簿记权的争夺。攻击者如果不掌握全网 51%以上的计算资源,就无法攻击这套簿记(链接)系统。通过这样的设计,以前人们隔着万水千山做不到的点对点交易,现在不依赖银行等中介机构而仅靠分布式账本就可以实现。

比特币是一个互相验证的公开记账系统,具有总量固定、交易流水全部公开、去中心化、交易者身份信息匿名等特点。其未花费过的交易输出(unspent transaction output,UTXO)的绝佳设计,解决了 E-Cash 数据库无限膨胀的问题,使数字货币技术出现新的飞跃,人们将这一前沿技术称为区块链技术。

比特币出现之后,数字货币的发烧友狂喜地发现,去中心化的数字货币

梦想竟也可以大规模实验了。于是，基于不同区块链技术创新的各种数字货币不断出现。截至 2018 年 7 月，共有近 2000 多种数字货币出现。其中，一些加密货币利用各种加密技术，对比特币进行了扩展与变型，如以太坊扩展了比特币的可编程脚本技术，致力于发展一个无法停止、抗屏蔽和自我维持的去中心化智能合约平台；达世币设置了双层奖励制网络，提供即时支付以及以混币协议 Coin Shuffle 为基础的匿名支付等增强服务；门罗币采用环签名技术隐藏交易双方地址，并吸收比特币社区发展出的机密交易技术隐藏交易金额，提供了更完善的匿名性；瑞波币允许不同的网关发行各自的借据（相当于在线债券的借据），并实现不同借据之间的自动转换；零币首次将零知识证明算法 zk-SNARK 用于保证交易发送者、接收者和交易数额的隐私性，具有较强的学术创新。

显然，数字货币以数学理论为基础，运用密码学原理来实现货币的特性。其用到的主要加密算法有对称性密码算法、非对称性密码算法及单向散列函数（哈希函数）等，常用的技术有数字签名、零知识证明和盲签名技术等。对比 E-Cash 和比特币，可以发现近 40 年来数字货币理论在支付模式和技术发展上均出现了很大的变化。

（1）支付模式从三方变为两方。这一变化是革命性的，数字货币通过先进的技术手段使得不必依赖中介就可实现点对点交易，将原有的三方支付模式变成了两方支付模式，支付行为的自主性大大加强，对整个社会具有极大的影响。

（2）技术应用出现新的飞跃。E-Cash 的两项关键技术是随机配序（随机配序产生的唯一序列号保证数字现金的唯一性）和盲签名（盲签名确保银行对该数字现金的匿名背书）。比特币则是一个互相验证的公开记账系统，其特色是把通常意义上的集中簿记分拆为约每十分钟一次的分布式簿记，簿记数据按时间顺序链接起来并广播全网，簿记的权利由全网竞争选取，以达到

去中心化的目的，标志着数字货币技术应用的新飞跃。

（3）已有的数字货币模型可为未来更为完善的数字货币系统设计提供参考。E-Cash 和比特币就像是一枚硬币的正反两面，有些关键特性可以参照研究。例如，E-Cash 每次交易都要对数字现金序列号的唯一性进行认证，而每个使用过的序列号都会被存储在数据库中，这样数据库就会变得越来越庞大，认证过程也会越来越困难。而比特币采用的 UTXO 库则可以解决 E-Cash 数据库无限膨胀问题。将来更为完善的数字货币系统设计，应该是升级版 E-Cash 和比特币的混合体。

2. 数字货币的定义

1）货币的种类

目前关于货币的衍生概念有多种，可以归为以下 4 类。

（1）法定纸币（legal currency）。日常生活中使用的为法定纸币，是央行通过国家信用背书发行的法定货币，具有法律效力。

（2）电子货币（electronic money）。经历支付方式的不断演变，人们从纸币支付到通过银行卡、储值卡、支付宝、微信以及各类电子钱包等方式支付，此类支付方式均基于电子货币账户进行资金流转，由此引出电子货币的概念。电子货币是指用一定金额的现金或存款，从发行者处兑换并获得代表相同金额的数据，或者通过银行及第三方推出的快捷支付服务，通过使用某些电子化途径将银行中的余额转移，从而能够进行交易。严格意义是消费者向电子货币的发行者使用银行的网络银行服务进行储值和快捷支付，通过媒介（二维码或硬件设备），以电子形式使消费者进行交易的货币。其本质上是法定纸币的电子化形式，是客户的银行账户的网络映射，不具备独立的发行模式和货币量要求，支付宝或微信中的电子钱包等被称为第三方支付，与银行账户相关联。

(3) 虚拟货币(virtual currency)。20 世纪 80 年代,随着网络社区的兴起,市场上出现用于社区内各种虚拟商品交易的虚拟货币,如网络积分、游戏币、社交网站发行的各类代币(如 Q 币)。虚拟货币由私人部门发行,不具备法律效力,这类货币用于虚拟的网络世界,可通过法定货币在网络空间进行购买或转让,不适用于现实场景的流通。根据欧洲中央银行定义:虚拟货币是一种未加监管,由其开发者发行和控制,被某一特定虚拟社区成员使用并接受的数字货币。根据我国现行规定,公众用法币购买的网络虚拟货币只能在某些特定平台内流通,不可跨平台使用、不可用网络游戏虚拟货币兑换人民币,也就是说虚拟货币不可赎回。

自 2008 年比特币出现以来,一般提到虚拟货币通常特指以比特币、以太币等为首的去中心化加密货币。此类虚拟货币伴随比特币价格上涨后引发的财富效应,虽然近两年有所回落,但是仍然引发许多人对各种虚拟货币狂热追捧。截至 2020 年 4 月底,市场上共有 3100 多种私人部门发行的数字货币。由于私人数字货币缺乏内在价值,诸多国际组织和政府部门将其称为虚拟货币。

(4) 数字货币(digital currency),即密码货币或加密货币。根据发行者的不同,数字货币可以分为私人数字货币和法定数字货币,比特币、以太币、瑞波币、莱特币等均可称为私人数字货币,它们并非通过政府担保,更多体现一种投资属性。由各国央行发行的数字货币才能称为法定数字货币,目前尚未出现实际使用的法定数字货币,由数字货币引出的另一新型货币名称为网络虚拟代币,此类代币相当于一种筹码或股权,曾经火热一时的 ICO(数字货币首次公开众筹)便是通过发行私有代币募集资金,代币的价值与融资的项目发展挂钩,代币形式或称呼随项目的不同可能不同。

2) 数字货币的概念

目前,数字货币还没有一个统一的定义。在实践中,数字货币的概念非

常宽泛。如英格兰银行(BoE)认为,数字货币是仅以电子形式存在的支付手段,与传统货币类似,数字货币可以用于购买实物商品和服务。反洗钱金融行动特别工作组(FATF)认为,数字货币是一种价值的数据表现形式,通过数据交易并发挥交易媒介、记账单位及价值存储的功能,但它并不是任何国家和地区的法定货币,即没有政府当局为它提供担保,它只能通过使用者间的协议来发挥上述功能。因此,数字货币不同于电子货币,电子货币是法定货币的数字化表现,被用来进行法定货币的电子化交易。

在不同语境下,数字货币有着不同的内涵和外延。目前,狭义的数字货币主要指纯数字化、不需要物理载体的货币;而广义的数字货币等同于电子货币,泛指一切以电子形式存在的货币。

数字货币的定义分歧较大,但也有统一的部分:指一种以数字形式呈现的货币,而非纸币、硬币等实体货币,承担了类似实体货币的职能,但能够支持即时交易和无地域限制的所有权转移。

数字货币包括加密(数字)货币和央行数字货币,这也是分歧所在,我国部分权威机构认为,只有央行发行的具备法定地位的数字货币,才是真正的数字货币。中国互联网金融协会区块链研究工作组组长李礼辉在 2017 年 9 月 18 日发布的一篇文章中称:“数字货币必须具备法定地位、国家主权背书,明确发行责任主体。以比特币和以太币等为代表的虚拟货币没有国别,没有主权背书,没有合格发行主体,没有国家信用支撑,这些都不是数字货币。”

根据当前大多关于数字货币的论述,给出数字货币的概念:数字货币即数字化的货币,是一种价值的数据表现形式,以互联网为基础,以计算机技术和通信技术为手段,以数字化的形式(二进制数据)存储在网络或有关电子设备中,并通过网络系统(包括智能卡)以数据传输方式实现流通和支付功能的网络一般等价物,具有货币最为基本的交易、流通等职能。

此外，数字货币具备发行和交易成本更低、可追踪、造假成本更高等优势。因此，数字货币是未来一种趋势。而且随着区块链技术的应用，未来可能将会建立全国甚至全世界统一账本，让每笔钱都可以追溯，逃漏税、洗钱行为会在监管范围内，甚至有可能实现在刷卡机上自动扣税。

3）法定数字货币和私人数字货币

央行发行的数字货币为法定数字货币，私人发行的数字货币为私人数字货币。其中，央行发行的数字货币，是指中央银行发行的，以代表具体金额的加密数字串为表现形式的法定货币。它本身不是物理实体，也不以物理实体为载体，而是用于网络投资、交易和存储，代表一定量价值的数字化信息。

私人发行的数字货币，也称虚拟货币，是由开发者发行和控制，不受政府监管，在一个虚拟社区的成员间流通的数字货币，如比特币等。有时采用密码学技术的数字货币又称为加密货币（crypto currency）。数字货币更强调价值以数字形式表现，虚拟货币更强调价值以虚拟形式存在，而非以实物形式存在。当它们的发行和交易确认使用到密码学时，则被称为加密货币。

比较私人数字货币与法定数字货币可以发现以下不同。在内在价值上，法定数字货币以国家信用背书；私人数字货币则无信用背书。在使用范围上，法定数字货币天然具有法偿地位，在具备流通环境条件下任何人、任何机构不得拒收；而私人数字货币不具法偿性与普偿性。在价值尺度上，国家信用保证了法定数字货币计价的稳定；而私人数字货币价值不稳，公信力不强。在发行动机上，私人数字货币往往追求社会接受度最大化或利润最大化，形成一定垄断后可能会给社会带来负面性和潜在风险或损失；法定数字货币代表国家信用及社会整体利益，能维持本经济体范围内整体利益最大化。在功能上，法定数字货币除基础三大功能外，承载了更多的货币政策传导、测量、调节等功能；而私人数字货币专注于私人支付媒介作用，不考虑用于调节经济的国家功能。在业务架构上，法定数字货币具有中心化特征；而私人数字

货币则采用以加密算法为核心的区块链技术，使用较大代价处理双花、交易确认等问题，无中心化机制保障，没有运行责任兜底机构。

3.1.2 数字货币的 3 个基本问题

纵观世界货币发展史，主要经历了实物货币、金属货币和纸币 3 个传统阶段，互联网时代数字货币更大意义上是一种信用货币。货币的实际价值和名义价值逐渐分离，出现了两种对立的观点：货币金属论和货币信用论，并在关于货币的 3 个基本问题上有着不同的观点。

1. 数字货币的本质问题

第一个问题是数字货币是否具有价值。货币的商品属性和债务属性是货币的两面，随着货币的演进，这两种属性的重要性也会不断发生变化：债务属性会变得更加明显，而商品属性会变得更加模糊乃至消失。当处在实物货币或贵金属货币阶段时，货币的商品属性表现相对强一点，而债务属性表现相对弱一点。当进入信用货币阶段，货币的商品属性表现逐渐消失，而债务属性表现增强，信用货币本身没有十足的价值。

数字货币本身不具有价值，本质上是一种财富价值的序列符号。数字货币的发展并没有脱离信用货币的范畴，作为一种信用货币，数字货币本质上仍是货币符号。信用货币阶段，金融机构发行的货币其实是提供金融信用。目前，数字货币主要有两种设计思路：基于“中央银行-商业银行”的数字货币本质上是组织机构信用，而基于 P2P 的数字货币本质上是个人信用。

2. 数字货币属性理论

第二个问题是谁来发行数字货币。根据货币发行主体的属性，可分为公

有属性和私有属性，即货币国家化和货币非国家化理论。从历史上看，政府很早就掌握了货币发行的权力，铸币发行国家化逐渐成为共识，形成了货币国家化理论。在铸币流通时代，因金属的稀缺性使得政府垄断货币发行权没有造成明显的影响。然而，在纸币流通阶段，纸币的发行不受贵金属储备的限制，政府为了自身财政的需要很容易超发纸币，引发货币贬值，造成通货膨胀和财富分配不公，引发经济危机和社会不满。基于经济自由主义视角，Hayek 提出了货币非国家化的设想，即废除中央银行制度，允许私人发行货币，自由竞争的过程将会发现最好的货币。

货币发行主体的争议深层次是信用保证问题。信用货币时代，货币本身不具有价值，其背后是发行者的信用问题。不同货币发行体系下，其信用保证存在着较大的差异。纯粹的政府发行法定信用货币体系，本质上是政府信用保证，由政府保证货币流通价值。以黄金等实物挂钩的信用货币体系，本质上是商品价值和政府信用的双重保证。以美元等强势货币挂钩的信用货币体系，本质上是不同主体信用的多重保证。从发行人的属性来看，主要分为公有和私有发行，本质上是法定数字货币（国家信用）与私人数字货币（私人信用）的区别。因此，数字货币的发行主体不同，其背后的信用保证不同，这也是众多虚拟货币存在较大信用风险的关键。

因信息不对称，货币发行过程中存在委托代理问题。数字货币体系将由双重委托代理逐步发展为一重委托代理问题。传统货币体系是两重信用的双重委托代理问题。传统货币流通体系是以银行为主导间接融资过程，货币发行是国家信用在金融机构之间一次配置，即一级市场中存在着一次委托代理的问题。在个体融资中，单位个体凭借自身信用到金融机构进行二次融资获得资金，即二级市场上也存在着一次委托代理问题。在 P2P 数字货币体系下是一重信用的委托代理问题。个体融资相当于以个体信用为保证，简化为私人信用之间的问题，即一次委托代理问题。

3. 数字货币发行的锚定原理和信用创造机制

第三个问题是数字货币的数量如何调节。根据货币供给的影响因素分为基础货币和派生货币能力，这一大问题可以分为两个小问题，即数字货币的基础货币发行量和数字货币的流通量。

（1）数字货币的基础货币发行量。在实物货币或金属货币阶段，货币的发行量是以实物或金属存量为依据。基于存量限制和技术水平因素，货币发行量比较稳定，实物货币或金属货币发行有了比较好的锚定物。进入信用货币高级阶段，缺乏实际价值的纸币很容易超发，货币发行过程一直存在锚定与脱锚的争议。为了维持币值稳定，人们希望纸币发行能与贵金属（或商品）挂钩而形成货币发行锚定，但政府为了自身财政需要希望纸币发行自由调控实现货币发行脱锚。历史上，政府选择过以商品存量为锚定，逐步过渡到以贵金属存量为锚定，到以强势货币为锚定。

数字货币发行的锚定物问题变得相对重要。纸币流通时代，为了刺激经济发展和减轻政府债务，一些国家政府有超发货币的动机，特别是缺乏货币发行锚定物时这种机会更大。数字货币发行更因其无形性、无价值、低成本等特性，使得锚定问题变得更重要也更困难。信息技术容量成为新时代数字货币的较好的锚定物。基于区块链技术的数字货币设计以信息技术容量为限，采用技术锚定解决数字货币发行量问题。根据数字货币的设计规则，数字货币的获得需要通过网络“挖矿”实现，“挖矿”消耗的计算处理能量将转化为数字货币的价值，即数字货币的发行量与网络技术处理能力挂钩。科学技术是衡量一个社会生产力的重要标准，信息技术水平又是互联网时代发展的重要指标，数字货币的发行能与信息技术容量挂钩，说明数字货币发行找到了较优的锚定机制。

（2）数字货币的流通量。除了货币的基础发行量外，数字货币的流通量

主要由信用创造能力决定。货币信用创造能力是影响货币数量调节的重要因素。基础货币的发行量是显而易见的，为了应对舆论压力各国中央银行对基础货币发行比较慎重，但间接货币信用创造的影响却是较为隐蔽的。货币信用创造内生于金融交易过程，一般由中央银行发行货币，创造信用基础载体；商业银行吸收存款，同时对贷款进行定价和配置，释放出新的信用，形成货币信用循环体系。以银行主导的传统信用创造机制中，银行不仅是借款人和贷款人的媒介者，更是信用创造者，影响着货币流通量，银行过度放贷扩大信用易造成金融危机。随着金融业的不断发展，信用创造的主体不再局限于银行，包括证券公司等，形成以金融市场为核心的现代信用创造机制。

现代金融理论体系中，影子银行等非正规金融机构对货币信用创造具有重要的影响，通过金融衍生产品的创新，发挥了更强的信用创造功能，影响了货币乘数模型，最终影响宏观货币政策调控。互联网金融等新兴金融机构也可能成为信用创造或者放大的力量之一。作为金融工具的创新，数字货币一定程度上改变了传统货币的信用创造机制，其信用创造能力的衡量是后续研究的重点。

3.1.3　数字货币的主要特征

1. 数字货币的价值由供给和需求决定

与商品相比，数字货币的内在价值为零。区别于传统的电子货币，数字货币的价值只依赖于这样一种信念，即数字货币可以在未来某个时间兑换成任何商品和服务，或者是一定量的主权货币。新的数字货币的产生完全是由计算机协议决定的，不同的数字货币计划有不同的长期供给和货币创造预设规则。此外，数字货币计划倾向不以美元、欧元等主权货币计价或与其产生

关系。以比特币为例，它的价值就是按照 1 个比特币为单位进行转移的。

2. 数字货币是去中心化的货币

数字货币的基础——区块链的特点就是去中心化。区块链通过一系列数学算法建立一整套自治机制，使得人们可以不需要中介机构的帮助，就可以自由而安全地做到点对点的货币转移，并由参与者自发而公平地完成货币的发行。外部任何机构都无权利，也无法关闭它，不受任何国家、政府机构以及央行的管控。

即数字货币使用了分布式总账技术，从而允许在交易对手之间缺乏信任也不需要依赖中介的情况下，实现价值的点对点交易。实际上，分布式总账就是对价值的点对点交易信息进行复制，通过去中心化的网络分散入账后的总账更新，完成价值转移。

但实际上这只是一种理想状态，目前的不少数字货币做不到完全的去中心化，并且在该不该完全去中心化这一点上还存在着不小的争执，主要有以下两种观点。

一是有人认为，去中心化的效率实在是太低，完全去中心化是混乱的开始，还是需要中心化机构来提高效率；二是有人认为，不去中心化的数字货币是没有意义的，创造的初衷就是为了防止中心掠夺财富，数字货币最重要的就是安全性和去中心化，效率是次要。

3. 数字货币是加密的、匿名的货币

数字货币是建立在基于密码学的安全通信上的（即非对称加密、数字签名等技术），使用密码学的设计（散列函数、共识算法）来确保货币流通各个环节的安全性，确保无法进行双花。基于密码学的设计可以使数字货币只能被真实的拥有者转移或支付。

可以说，数字货币相比于其他电子支付方式的优势之一就在于支持远程的点对点支付，它不需要任何可信的第三方作为中介，交易双方可以在完全陌生的情况下完成交易而无须彼此信任。在数字货币中，拥有这些货币的唯一凭证就是所掌握的密钥，系统只会对密钥进行验证而不会获取其他任何信息，任何操作都是匿名的，能够保护交易者的隐私，这是非常安全的，但同时也给网络犯罪创造了便利，容易被洗钱和其他犯罪活动所利用。

4. 数字货币是不可篡改的、公开透明的货币

数字货币的本质是一个互相验证的公开记账系统，这个系统所做的事情，就是记录所有账户发生的所有交易，每个账号的交易都会记录在全网总账本(区块链)中，而且每个人手上都有一份完整的账本，每个人都可以独立统计出比特币有史以来每个账号的所有账目，也能计算出任意账号的当前余额，因此系统里任何人都没有唯一控制权，系统稳定而公平。

数字货币的交易一经确认，将被记录在区块链中，便无法撤销及改变。这意味着任何人，不管是不法分子、商家、银行，都不可以通过删除或修改交易记录的方法进行诈骗。但如果把数字货币汇给了骗徒当然也无法取回，所以在交易时要小心谨慎。

5. 数字货币可以传递价值

互联网的电子货币只能做信息的传递而无法做价值的传递，支付宝上银行在进行账户数字的加减之后，实际货币的结算可能在 24 小时，甚至一个月之后进行，价值的传递是脱离信息的，传递是滞后的，严重依赖于整个中心的运作。

数字货币网络中每笔转账，本身都是价值的转移，数字货币本身是完全虚拟的，它代表的是价值的使用权，而转账就是对价值的使用权进行再授权。

基于区块链的可溯源结构，可以找到每个“币”被发行出来的时间，价值的流转非常清晰。

6. 拥有独特的制度安排

相较传统电子货币，许多数字货币计划没有发行者、网络运作方、专业的软硬件供应商、电子货币的收单机构以及电子货币交易的清算方等第三方负责运作。但是许多数字货币计划中会有大量的中间机构提供各类技术服务。这些中间机构可以提供“钱包”服务，允许数字货币使用者转移价值，或者提供数字货币分别与主权货币、其他数字货币或资产兑换的服务。在某些情况下，这些中间机构会为其顾客存储密钥。

7. 交易费用低

现在互联网时代，在国内进行交易转账，需要给第三方平台一定的手续费用，如果是跨境转账，费用则会更多，并且还不能实时转账，需要一个等待的过程。而数字货币采用去中心化的点对点交易，不需要任何类似清算中心的中心化机构处理数据，交易处理速度更快，且不需要向第三方支付费用，其交易成本更低，交易速度更快。

3.1.4 数字货币的需求

随着金融科技水平的突飞猛进、数字货币的迅猛发展，社会对央行数字货币的呼声越来越高，其需求越来越迫切。

1. 形势发展需求

私人机构发行数字货币存在一些问题，央行发行法定数字货币具有开源

节流、提高流动性、保护用户隐私以及维护社会秩序稳定等优势。然而，如今的现实却是私人数字货币泛滥，而央行法定数字货币缺乏，不能满足经济社会发展需要。腾讯发布的《2017 年度互联网安全报告》指出，目前各种加密货币已达 1500 多种，而且不法分子利用数字货币的匿名性，使用勒索、盗窃、非法挖矿等手段获取大量不义之财。良莠不齐、虚假繁荣、乱象丛生的数字货币生态环境，给各国央行增加了压力，呼唤法定数字货币出来正本清源，引领金融科技方向。

2. 国家的现实需求

数字货币公平、公正、公开的数学算法容易取得全球共识，建立全球信用，并且依托互联网技术，可以实现全球点对点的即时支付，无疑是一些国家应对国内通货膨胀，对外突破 SWIFT 全球结算网络支付系统限制和封锁的选择。例如，2018 年 2 月委内瑞拉发行了全球第一个由政府主导的数字货币——石油币，发行总量 1 亿个，60 美元/个，只能以美元和欧元支付，主要目的是获得外汇，抵制国内严重通货膨胀。俄罗斯表示正在研究“加密卢布”，伊朗也证实将继续创建自己国家发行的法定数字货币，土耳其同样也正考虑抓紧推出其法定数字货币“土耳其币”。可以预见，随着各国法定数字货币的相继出台，势必对现有的世界货币体系格局产生影响，并逐渐推进新的货币体系形成。

3. 提升金融服务水平的需求

数字货币采用数学算法发行、分布式记账、共识机制、非对称加密算法、智能合约，由此形成了总量控制、去中心化、点对点、不可篡改、匿名、加密、可编程等特性，与传统货币和支付手段相比有很多自己的优势。例如，与支付宝等电子支付货币相比，因为其不需要第三方参与，交易更加便捷、成本更加

低廉，而且更能保证数据安全和个人隐私，保证交易信息安全。另外，其低成本、高效率、智能化的特性，可以切实降低企业支付结算成本，提升偏远山区金融服务水平，打开普惠金融、金融精准扶贫新局面。

4. 中国人民银行数字货币 DC/EP 试点

DC/EP 中的 DC 是 Digital Currency，译为数字货币，而 EP 是 Electronic Payment，译为电子支付。DC/EP 这一概念最早在 2014 年提出，于“2019 外滩金融峰会”上首次亮相。

我国 DC/EP 有以下 4 个特性。

（1）法定货币，不可拒收。法定货币是指，它由中国人民银行发行，身份地位与传统货币一样，具有法定效力，是一种数字化形态的人民币。不可拒收是指，在我国法制管理范围内，DC/EP 是绝对可以承担“一般等价物“的流通功能，任何人和机构不可拒收，即在我国法制管理范围内可以收人民币的地方就必须可以收 DC/EP。

（2）安全性。DC/EP 基于国家强大的技术与信用保障，让所有的消费支付流向都有更加精确与全面的跟踪记录，公民身份信息与钱包牢牢绑定，被盗刷的风险将不存在。相对纸币而言，也解决了携带纸币意外遗失、被偷盗抢劫，以及收到假币的风险。

（3）便捷性。无需网络的支付手段能让全体人民生产、生活更加方便快捷。此外，无需纸币的货币发行方式能有效减少国家人力、物力成本。

（4）可跟踪回溯性。DC/EP 基于我国强大的技术与信用保障，让所有的消费支付流向都有更加精确与全面的跟踪记录。所有的数据直接保存在央行的服务器上，央行可以随时看到每个人或机构的每笔费用的详细记录。

2020 年 4 月 16 日，我国央行数字货币在雄安、深圳、成都、苏州 4 座城市

正式开展试点工作。如果试点实验顺利进行，我国央行将会加快全国推广步伐，让更高度的数字时代提前来临。

3.1.5　中央银行发行数字货币面临的挑战

目前，虽然说区块链技术在不断地发展且日趋完善，但是真正要把区块链技术应用于商业特别是金融业，这其中还存在着许多的问题。其中，最大的 3 个问题：安全性、应用范围和隐私保护。

1. 安全性

区块链目前面临最严峻的问题仍然是安全性。自比特币问世以来到目前为止，其遭受到黑客的攻击导致的被盗事件时有发生，因此基于区块链技术的数字货币在技术面上尚未成熟。虽然实际系统中攻击一次需要的成本投入远远超过成功攻击后的收益，但受到攻击的威胁始终存在。

2. 应用范围

央行发行数字货币，第二个核心问题是应用范围。目前讨论的数字货币，主要指替代现金支持自然人之间的小额交易。但以现有的技术手段而论，要做到这一点完全不需要数字货币，支付宝或者微信就足够了。关键的问题是，一旦央行对外发行数字货币，企业法人和金融市场这两个更大的应用层面是否也需要引入？这些机构与自然人账户发生往来时，应该接受还是拒绝数字货币呢？

答案很显然是否定的。因为现有的支付清算系统中，企业法人和金融市场参与者都是受到严格管制的，其账户实行严格的实名制管理。支付系统中的管理员（例如，开户银行和中央银行）在后台可以看到数据全貌。这种架

构，目标是整个社会的数字化管理，包括但不限于应对税收征管、反洗钱、应急处理等各种挑战。显然，不记名且点对点的数字货币是一个异端，会让整个系统乱套。

3. 隐私保护

在区块链中，参与者都拥有一份完整的数据备份，所有交易的信息都会在全网公开，这是区块链在解决信息不对称领域所具有的优势。这一点对于区块链使用方是不利的。用户不愿意公开自己的账户隐私，商业机构也不会将商业机密公开共享给同行。如何实现隐私保护是一个难题。

3.2 基于区块链的数字货币

3.2.1 区块链与数字货币

1. 区块链在数字货币发行上的优势

区块链＋数字货币，将开启全球数字货币时代。区块链技术最早应用于比特币，尽管比特币天然不是法定货币，但却为法定货币由纸币进入电子货币后的数字货币时代奠定了技术基础和应用示范，目前各国央行都在加紧研究法定数字货币。

区块链技术的应用，带给数字货币诸多优势。

（1）极大降低了交易成本。第三方支付机构在支付过程中承担着一定的背后通道成本、系统管理与优化成本、电费、广告费等多种成本费用。数字

货币的交易无须经过第三方金融中心来交易，可以有效避免背后通道支付成本，降低系统管理与优化、电费、广告费等成本。

（2）极大提高了安全性。数字货币采用分布式账本技术，黑客无法通过对单一中心节点进行攻击而造成系统崩溃等重大安全问题，能够实现替代第三方支付虚拟账户充当电子支付媒介。区块链技术是制造信任的机器，区块链上的每笔交易都可以被追溯，这样既可以实现全流程的安全管理，又为监管部门完成实时、高效的监管工作提供了技术支撑，能够有效防范洗钱等违法行为。

（3）提高了服务品质。分布式系统比单机系统更可靠。主要表现为以下 3 方面：①可用性，即系统在一些异常发生时仍可维持正常服务的能力；②安全性，即必须保证文件和其他资源不被非法使用的能力；③容错性。

2. 数字货币系统应兼收并蓄包括区块链在内的各种成熟技术

数字货币系统以及前端应用的建设必须基于难以篡改和不可伪造的铸币（登记）中心，需要有高效率、高弹性、高安全性、层级化的铸币（登记）分中心，需要有货币流通全生命周期的全息记录，并在此基础上支撑全新的智能化商业应用。

如何实现各铸币（登记）分中心所服务的商业网络之间的数据一致性需求，区块链可以提供全新思路的借鉴，例如共识算法和智能合约。但是，不宜对这种借鉴的“拿来主义”生搬硬套，必须根据实际业务需求进行应用层面的改造。同时，系统建设者不宜拘泥于任何技术，要有长期演进的技术理念。

因此除了区块链技术，还需要关注其他正在竞争和发展中的安全技术、可信技术，例如，可信可控云计算，特别是芯片技术。在数字世界里对用户而言最重要的就是密钥，其安全管理存储对于终端交易安全至关重要。为实现数字货币交易过程中的端到端的安全，数字货币在后台云端可利用可信技

术，前台可利用芯片技术，传输过程可利用信道安全技术。

3. 区块链使价值的点对点传播成为可能

货币在发行流通中只是在账户上进行数字的加减，数字货币可以发挥数字的本质特性，对人类货币史的发展具有重要意义。当前，如需发行数字货币，点对点的发行系统是非常值得研究和探索的。区块链这种天然的分布式技术，必定会成为未来数字货币发行的主流方向，甚至是唯一方向。区块链是一种让人们在无须信任的情况下，通过共享的事件记录或日志达成共识的技术。这个共享的事件记录或日志分布式存储于整个网络中，并由所有参与方进行验证，由此避免了对第三方信用的需求。

现在的信息互联网需要向价值互联网转变。货币的本质是交易便利性，只包含信息而没有价值的点对点传播无法满足交易便利性的要求。只有实现价值点对点传递，经济交易和整个社会、企业组织才能成为一种新形态。

整个社会经济系统是商品与服务的设计、生产、交易与物流的整合运行。所有经济活动都可以理解为一个契约过程，即合同交换过程。实质上，合同交换是产权交换，整个经济过程就是一个所有权或产权证明的转移过程。在数字经济中，这些所有权证明将被数字化，以数字形态转移。这与信息社会的信息转移没有本质区别。然而，目前在产权转移时需要复杂的签约过程，产权转移和资金转移过程相互割裂，无法实现价值的点对点转移。此时，区块链第一次使价值的点对点转移成为可能。

虽然像支付宝、微信的红包系统，看起来像是价值的点对点传播，但是它们并没有改变整个价值形态的转移系统。它们其实是构建于现有银行账户基础上的，在各个银行之间开一个大账户，然后把各个消费者的银行账号挂在它的大账户上。大账户又跟各个银行来对应，以便在内部做到点对点转移。实质上，它们并没有真正改变整个银行系统，更谈不上货币发行系统。