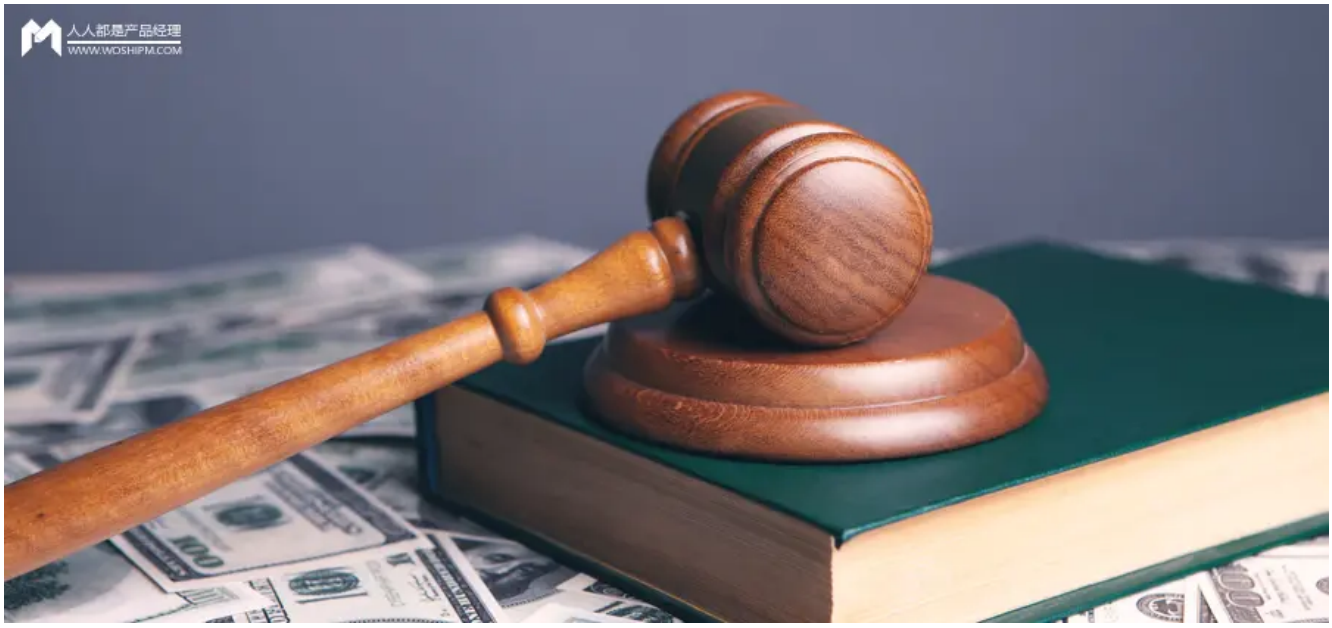
万字长文 | 一文读懂数字人民币

数字人民币是由中国人民银行发行的数字形式的法定货币，由指定运营机构参与并向公众兑换，与实物人民币等价，具有价值特征和法偿性。本文作者从数字货币、数字人民币钱包、区块链等方面，对数字人民币进行了详细的解析，一起来看一下吧。



一、央行数字货币

1. 数字人民币

数字人民币（e-CNY）是由中国人民银行发行的数字形式的法定货币，由指定运营机构参与运营并向公众兑换，以广义账户体系为基础，支持银行账户松耦合功能，与实物人民币等价，具有价值特征和法偿性，支持可控匿名。

2. 一币两库三中心

一种币指由央行背书并发行的中国法定数字货币。

两个数据库为数字货币银行库和数字货币发行库。央行数字货币的发行与流通是基于央行 -商业银行-公众的双层运营体系。发行货币时，央行将数字货币发行给商业银行的数字货币银行库，商业银行向央行缴纳 100%准备金作为数字货币发行基金，进入到央行的数字货币发行库中。

三个中心的具体结构为：认证中心，登记中心和大数据分析中心。

3. 运营机构

央行指定运营机构负责钱包运营，提供数字人民币兑换和流通服务，向央行100%缴纳准备金，帮助商业银行完善数字人民币能力。

截至2022年10月，我国共有十家数字人民币指定运营机构，包括**工行、农行、中行、建行、交行、邮储银行、招行、兴业银行、网商银行、微众银行。**

4. 受理服务机构

受理服务机构由央行数研所指定并授权，采取直连方式与数研所互联互通平台进行对接，为商户受理数字人民币交易提供技术与信息服务。一般为三方支付机构、商业银行或者聚合支付服务商。

5. 双花（double-spending）

简单而言，就是一笔钱花了两次。这个问题主要出现在数字货币的世界里，因为在这个世界你的钱只是一串数字，复制很容易。而现实世界里，纸币上有非常严格的防伪标识，很难复制，并且还有银行这样的中心化的权威机构确保你的交易唯一性，所以几乎不会出现这种问题，除非中心化机构数据出现问题。

传统现实中因为低延迟网络以及中心化管理的原因，是不会出现双花现象，无论是线下交易的现金支付或者网上支付的第三方监管交易确认，都可以避免双花问题。

6. 垫付和追缴的机制

以公交地铁乘车为例，如乘客钱包余额不足抵扣车票款项时，乘车业务系统就会存在坏账的情况。此时，业务系统就需要拥有垫付和追缴的机制。追缴机制一般通过限制乘客最多可欠款的乘车次数来控制，达到一定的欠款次数乘客无法再次使用乘车服务，直到补齐欠款；另外一种即垫付机制，一般由业务系统合作方运营机构来承担坏账金额。

7. 分级限额

指定运营机构根据客户身份事别强度对数字人民币钱包进行分类管理，根据实名强弱程度赋予各类钱包消费、转钱不同的单笔、单日交易及余额。

数字人民币钱包交易限额

钱包类型		一类钱包	二类钱包	三类钱包	四类钱包（非实名）
办理要求		手机号、有效身份证件、本人银行账户、运营机构面签	手机号、有效身份证件、本人银行账户	手机号、有效身份证件	手机号
交易限制	余额上限	无	50 万元	2 万元	1 万元
	单笔支付限额上限		5 万元	5000 元	2000 元
	日累计支付限额上限		10 万元	1 万元	5000 元
	年累计支付限额上限		无		5 万元
各运营机构可以在限额上限范围内灵活调整					

钱包限额

提升限额

消费 转钱

消费单笔限额	¥20,000
消费日累计限额	¥20,000
剩余可用	¥20,000
消费年累计限额	¥500,000
剩余可用	¥499,998.99

提示：

1.当前钱包为二类钱包，钱包限额同时受限于运营机构钱包等级及您自行设置的限额，点击“运营机构钱包限额”查询更多限额。

2.钱包限额调整后可能影响到您钱包快付的交易限额，请谨慎调整，以免影响钱包快付的正常交易。

3.注销后，使用相同钱包开立信息再次开立钱包时，日累计限额及年累计限额将继续累计。

调整消费限额

消费 转钱

转钱单笔限额	¥5,000
转钱日累计限额	¥10,000
剩余可用	¥10,000
转钱年累计限额	¥200,000
剩余可用	¥199,967.06

提示：

当前钱包为二类钱包，钱包限额同时受限于运营机构钱包等级及您自行设置的限额，点击“运营机构钱包限额”查询更多限额。

数字人民币钱包主要有四种类型：

一是按照客户身份识别强度分为不同等级的钱包。运营机构对客户进行身份识别，并根据客户身份识别强度对数字人民币钱包进行分层管理，根据实名强弱程度赋予各类钱包不同的每笔及每日交易限额和余额限额。最低权限的四类数字人民币钱包属于匿名钱包，余额限额1万元、单笔支付限额2000元、日累计支付限额5000元。仅用本人手机号码就可以开通，体现了数字人民币可控匿名的设计原则。如果要支付超过2000块钱买件东西，可以升级钱包，上传本人有效身份证件信息及绑定银行账户信息。比如，升级到二类钱包后，钱包余额上限会变为50万元，单笔支付限额升至5万元、日累计支付限额10万元。

二是按照开立主体分为个人钱包和对公钱包。自然人和个体工商户可以开立个人钱包，按照相应客户身份识别强度采用分类交易和余额限额管理；其他法人和非法人机构可开立对公钱包，并按照临柜开立还是远程开立确定交易和余额限额，钱包功能可依据用户需求定制。

三是按照载体分为软钱包和硬钱包。软钱包有移动支付APP和以软件开发工具包（SDK）提供的服务；硬钱包有IC卡、可穿戴设备、物联网设备等。比如，面向老年人推出加载健康码功能的硬钱包产品，提供安全便捷支付功能的同时，还可以便利老年人疫情防控下的日常出行。

四是按照权限归属分为母钱包和子钱包。钱包持有主体可将主要的钱包设为母钱包，并可在母钱包下开设若干子钱包，个人可以通过子钱包实现支付场景的限额支付、条件支付和个人隐私保护等功能。

8. 数字货币多边桥（mBridge）

多边央行数字货币桥是指在多个国家/地区或多个央行之间建立的一种数字货币跨境支付系统，用于实现跨国货币互换、跨境支付和结算等操作，以确保跨境支付的速度、低成本、安全、稳定和可持续性，旨在通过覆盖不同司法辖区和货币，探索分布式账本技术和央行数字货币在跨境支付中的应用。经多边央行数字货币桥连接的央行之间也可以对数字货币进行实时互换，从而使银行业服务客户和缩小功能金融提供实时资金清算。

在货币桥项目中，各国央行可实现：

1. 可通过智能合约实施跨境同步交收；
2. 兼容不同的央行数字货币系统和设计；
3. 缓解本国数字货币境外流通对他国货币主权的影响。

9. 批发型央行数字货币

央行数字货币是央行的直接负债和支付工具。批发型央行数字货币仅限于金融中介机构使用，相当于现在商业银行在中央银行的账户余额。

新加坡金管局认为，发展批发型央行数字货币很有必要，尤其是在跨境支付和结算方面。

10. 零售型央行数字货币

零售型央行数字货币相对于其他受监管数字货币（如稳定币或代币化银行存款）的独特之处在于，它将是中央银行的负债。

二、数字人民币钱包

数字人民币钱包根据多种分类方式形成了数字人民币钱包矩阵，为后续商业银行开展不同金融产品创造了条件。

1. 钱包类型

根据客户身份识别强度的不同可以将数字人民币钱包分为四类。

- 用户在默认情况下开立的是最低权限的匿名钱包，可根据需要自主升级为高权限的实名钱包，且四类钱包可以进行升级，升级后不能降级。
- 一类钱包只能带个人身份证件，前往运营机构的试点地区网点办理。

数字人民币钱包按照开户类型的不同可分为个人钱包和对公钱包，且按照相应的客户身份识别强度采用分类交易和余额限额管理；

自然人和个体工商户可以开立个人钱包，按照相应客户身份识别强度采用分类交易和余额限额管理：法人和非法人机构可开立对公钱包，并按照临柜开立或远程开立的方式来确定交易、余额限额，钱包功能可依据用户需求定制。

1）对公钱包

对公钱包是指数字人民币运营机构对公客户开立的数字人民币钱包，对公钱包按照开立方式和实名强度分为一类、二类钱包。

对公钱包特色功能：

- **代收代付**：企业开通办理数字人民币代收代付业务后，可通过企业网银、网点柜面或与邮储银行系统对接的方式，向员工个人钱包中发放工资、餐补、交通补贴、福利费等，或从签约代收业务的钱包中收取学费、党费工会费等。
- **商户数字人民币收款服务**：客户提前开立银行企业网银，完成后客户经理指导客户在企业网银开立对公钱包为开通对公钱包的合作企业（商户）提供数字人民币收款服务，在其线上、线下消费场景均可实现数字人民币支付受理，实时结算，不收取交易服务费。
- **线上缴费**：企业开通银行开放式缴费平台业务后，无须自建系统即可使用数字人民币收缴工会费、团费、党费、水电费等，资金实时到账，享受全方位的账单管理、报表对账服务。
- **约定兑回、定向兑回**：对公母、子钱包资金自动兑回至您的对公账户，可指定兑回方式、兑回频率、兑回时点，享受存款利息。
- **母子钱包多层级资金归集**：按照您与设定的方式、时间、频率，自动将子钱包中的资金归集至上一钱包中，实现多层级资金高效管理。

2）个人钱包

个人钱包：数字人民币个人钱包是自然人和个体工商户可以开立的数字人民币钱包，按照相应客户身份识别强度采用分类交易和余额管理。数字人民币钱包按照载体还可分为软钱包和硬钱包。其中，软钱包基于移动支付APP 、软件开发工具包（SDK）、应用程序接口（API）等为用户提供服务，硬钱包基于安全芯片等技术并依托 IC卡、手机终端、可穿戴设备、物联网设备等为用户提供相关服务。

3）软钱包

软钱包是指通过支持数字人民币的智能应用提供的钱包服务，可以理解为软件钱包，以App的形式存在。例如数字人民币App中的各运营机构银行的数字钱包、各运营银行App中的数字钱包等。

4）硬钱包

硬钱包是指通过柜面或电子渠道开立的存储数字人民币的实体介质，具有硬件安全单元介质的数字人民币载体。其同样具有兑出、兑回、圈存、圈提、消费、转账、查询等基本功能。例如具备 SE 安全元件的手机、NFC-SIM 卡、银行卡以及可穿戴设备等。数字人民币钱包按照权限归属分为母钱包和子钱包。其中，钱包持有主体可将主要的钱包设为母钱包，并可在母钱包下开设若干子钱包，而个人可通过子钱包实现限额支付、条件支付和个人隐私保护等功能，企业和机构则可通过子钱包来实现资金归集及分发、财务管理等特定功能。

1）母钱包

母钱包：数字人民币钱包持有主体，可将主要的钱包设为母钱包。母钱包可以管理多个子钱包。

2）子钱包

子钱包：母钱包持有主体，可在母钱包下开设若干子钱包。

个人可以通过子钱包实现支付场景的限额支付、条件支付和个人隐私保护等功能，也可以进行亲属赠予功能的管理；企业和机构可以通过子钱包来实现资金归集和分发、会计处理、财务管理等功能。

2. 钱包分级

一类钱包，需现场核验申请人身份信息，需验证有效身份证件、手机号及本人境内银行账户信息；可绑定本人境内银行账户，支持个人数字人民币钱包内数字人民币与绑定账户存款的互转；实名程度最高。

二类钱包，支持远程开立，需验证身份证件、手机号及本人境内银行账户等信息；支持个人数字人民币钱包内数字人民币与绑定存款的互转；实名程度较高。

三类钱包，支持远程开立，需验证身份证件、手机号等信息，无需绑定银行账户，实名程度较弱。

四类钱包，支持远程开立，仅验证手机号码，无需绑定银行账户，为匿名钱包。四类钱包通过绑定银行，可以升级为三类及以上实名钱包。

3. 钱包编码

在账户模式下，每个开立的钱包都会生成唯一的数字人民币钱包编号，这个钱包编号与账户所有人身份进行绑定，也是其账户模式的体现。钱包编号是用户开立数字人民币钱包的“身份标识”，类似于传统银行账户下的“卡号”，用户可以通过钱包编号进行钱包之间的“转钱”。

4. 伞形钱包

伞形钱包基于数字人民币钱包体系架构而言，在现有钱包体系的基础上叠加的一种钱包功能，主要为解决平台/商户端资金结算分账问题，避免资金占用、挪用的情况。

伞形钱包分为伞顶钱包和伞底钱包两种。伞顶钱包为对公子钱包，伞底钱包可为对公子钱包或个人钱包。平台/商户端通过向运营机构填写申请表申请伞形钱包配置，具体可根据业务需求建立不同的伞形钱包结构。

伞形钱包应用案例：

招商银行无锡分行成功为国联财务公司党支部实现数字人民币党费缴纳，数字人民币缴费金额直接发放到企业清算账户。

招商银行App数字人民币缴费创新性提出“伞形钱包”方案。所谓“伞形钱包”包括“伞顶”和“伞底”两个部分：为生活缴费场景开通了专用钱包作为“伞顶”，为每个缴费商户开立一个缴费收款专用钱包作为“伞底”，用户在数字人民币支付后，“伞形钱包”方案有效降低了商户开通数字人民币支付的门槛。

商户无需至招行网点开立对公数字人民币钱包，只要与招行签订协议授权即可开通。另一方面，系统自动将银行卡资金和“伞底”钱包资金按照商户清算要求，统一并账转入商户收款账户，数字人民币支付和银行卡支付交易将在一个对账单中体现。

5. 钱包账户模式-基于账户（account-based）

账户模式以广义账户体系为基础，是数字人民币账户体系的体现，表现形式为用户在运营机构开立的数字人民币软钱包。运营机构以账户形式记载数字人民币的价值，并建立与使用者身份与账户中数字人民币价值间的关联关系，确立使用者对于数字人民币价值的所有权。

6. 钱包账户模式-基于准账户（quasi-account-based）

准账户模式同样是以账户形式记载数字人民币的价值，但不建立使用者身份与账户中数字人民币价值间的关联关系。也就是说，准账户模式的数字人民币产品针对不特定身份使用者发行，发行时是非实名的，发行后可根据用户身份进行绑定实名。

用户在准账户钱包如不慎丢失，可申请挂失。准账户模式的硬钱包，根据数字人民币硬钱包的技术规范进行开发，也具有唯一硬钱包编号，但其币串储存在运营机构的后台服务器系统中。准账户硬钱包是用户软钱包的下属子钱包，在交易时只支持单离线支付，关联后可申请挂失。

7. 钱包账户模式-基于价值（value-based）

价值模式指可以支持用户使用“双离线”支付下的“硬钱包”，通过芯片和算法来实现两个钱包之间的币串交换，币串储存在硬钱包的载体中，用户通过占有和控制相应的载体享有数字人民币的所有权。包括IC卡、手机终端、可穿戴、SIM卡、物联网设备等多种形态。支付时，收付双方可直接在无网络的情况下实现点对点的价值转移。

数字人民币支持“双离线”支付，采用NFC技术来实现，需收付双方设备具备内置安全芯片的硬件钱包功能，可以满足公交地铁出行、停车场、山区甚至是地理灾害等特殊环境下的支付需求，不通过互联网也可以直接进行离线交易，为公民提供便利的支付体验。双离线支付是数字人民币创新场景的一个重要方向，彻底脱离了网络对移动支付行为的约束。

8. 可控匿名性

数字人民币的可控匿名体现在：

- 一是应符合日常小额现金支付的习惯，确保相关支付交易的保密性。
- 二是应明确匿名对象，确保消费者使用数字人民币进行交易时，其个人信息不被商户和其他未经法律授权的第三方获取。
- 三是应加强个人信息的使用和保护，确保运营机构收集的客户基本信息、产生的交易和消费行为信息不会被泄露。

9. 可编程性

数字人民币通过加载不影响货币功能的智能合约实现可编程性，使数字人民币在确保安全与合规的前提下，可根据交易双方商定的条件、规则进行自动支付交易，促进业务模式创新。

10. 双离线支付

双离线支付，即使手机没信号，依然可以使用。只要手机安装了数字人民币的钱包，不需要网络，也不需要信号，手机没电的情况下，两个手机相互碰一碰就能实现转账或支付。

双离线支付核心指的是介质和受理终端都离线的情况下完成业务的一个过程，最典型的就是支付业务和核实身份。对支付业务来说，它通过交易完成之后的延期请款来完成闭环交易的过程，核心是实现了快速的核身和支付的一种技术方案。

它的业务机制有两个核心要点。一个是业务机制上面有两个特征，包括了核身和支付；另外一个就是终端和介质之间有一个信任机制。

在交易安全机制方面有三个维度：

1. 风控的额度，就是双离线之后的交易的额度；
2. 会有垫付和追缴的机制；
3. 信用体系。

实际上码和脸在双离线场景下它本质是一个先享后付的过程，解决的是用户体验的问题。适用的场景是：大量人群快速短时内完成核身或小额支付的场景，在网络不畅或信息化环境异常时，也要求保障交易的成功率，否则将可能引发群体事件的场合，典型的如：公交、校园食堂消费；以校园食堂为例：12点下课，几万人集中在1个小时内完成就餐，如果不支持双离线交易，要么引发群体事件，要么就是学校免费让学生吃饭，学校买单；校园场景双离线特点在于校园核身，必须是校园身份，这是封闭环境和开放环境（比如公交）的差异；核身要求必须学生或者老师的身份才能消费，它是特定场景特定策略。

目前有两个正在上线的实现路径，还有两个未来的技术方向，目前已经实现了卡、码和脸的双离线的核身和支付，主要是合约记账加上运营方资金兜底的一个路线。

在资金兜底路线上面又有两条路线。一个是学校许可学生授信的信用额度，在离校的时候进行管控；另一个就是基于营销策略的资金路径。

当前在研究的一个技术方向是物联网边缘计算。通过边缘计算，增强风控能力；风控共性除了交易行为之外（限额、限场景、透支风控额度等），基于物联网，通过同一个场所交易地点，在边缘计算网关，完成核销脱机风控余额，增加双离线的风控效果。

11. 支付即结算

数字人民币相比现钞可提高流通过程中的透明度与流通效率，支付即结算，从而有效提升企业支付清结算的效率和央行对资金流动的监控。

12. 数字人民币消费红包

数字人名币消费红包是指用于在特定商家的实体店或者网上消费场景，可以抵扣部分购买金额的红包。消费红包具有有效期，过期后会被回收。

13. 银银合作

银银合作是数字人民币试点发展阶段，同业银行之间的一种合作探索。一方面是帮助非运营机构银行能够接触到数字人民币生态体系，另一方面也是运营机构银行快速拓展数字人民币应用场景和用户覆盖的一种方式。

14. 直连模式

运营机构银行直接对接合作银行，向合作银行输出数字人民币钱包的开立管理和使用能力，在合作银行的自有渠道以实现开通。运营机构代理合作银行与央行进行资金结算，使用运营机构银行自身的数字人民币额度。

直连模式下，合作银行能够在自有渠道实现数字人民币个人钱包的功能，同时还能对接实现合作银行客户对公钱包、商户受理的功能。

15. 间连模式

间连模式，又称为“钱柜模式”。合作银行在运营机构开立金融机构数字钱包作为“钱柜”，使用自有资金向央行的准备金账户预先兑换一定数量的数字人民币存入钱柜，作为资金池向客户提供数字人民币的兑换流通服务，使用独立于运营机构以外的数字人民币额度。

间连模式下，通过接入互联互通平台，支持合作银行在共建的“数字人民币”App渠道实现各运营机构“个人钱包”绑定合作银行的银行账户并进行数字人民币的兑换等功能。这类模式的主要特征在互联互通平台中会有所体现，例如很早之前建行的数字人民币钱包即支持了中信银行的银行卡绑定。

16. 混合模式

混合模式，即上述两种模式的结合。直连与间连模式并行，合作银行在运营机构开立“钱柜”，同时又与运营机构保持直连系统对接。这类模式理论上而言应该是最完美的，即可以在数字人民币App中有体现，还能最大程度地发挥自身渠道的入口优势，为其增加流量。

间连模式下对接互联互通平台两种接入形式：

1）直通模式

即合作银行直接和央行数字货币研究所协商，直接接入数字人民币互联互通平台。这种模式是数字人民币在前期试点阶段，2.5层银行创新的一种积极尝试，而且彼时类似于“城银清算”“农信银”的一点接入平台还没有建立完善。例如最早支持数字人民币六大行以外绑卡的中信银行、招商银行（招行如今又成了2层运营机构）即是这种模式。

2）代理模式

即合作银行通过接入“城银清算”“农信银”等官方接入平台，然后再“一点接入”互联互通平台。这种模式可能是间连模式下未来中小银行进行数字人民币业务创新的主流。

三、货币相关的概念

1. 法定货币

法定货币（Legal tender），是指不代表实质商品或货物，发行者亦没有将货币兑现为实物义务；只依靠政府的法令使其成为合法通货的货币。法定货币的价值来自拥有者相信货币将来能维持其购买力。货币本身并无内在价值（Intrinsic value），也就是说，当纸币产生之后，法定货币实质上就是法律规定的可以流通的纸币。

2. M0、M1、M2

M0，M1，M2是货币供应量的三个定义，分别表示流通中的现金，狭义货币与广义货币。

通俗解释如下：

- M0指的是流通中的现金。
- M1指的是M0加上商业银行体系的支票存款。
- M2指的是M1加上商业银行的定期存款和储蓄存款。

3. 无限法偿性

无限法偿是指在货币流通条件下，国家对主币在法律上所赋予的无限支付能力。即每次支付的数额不受限制，任何人都不得拒绝接受。

金属货币流通时期，由于主币的名义价值与内在价值相符，而辅币的名义价值则大大高于内在价值，故国家规定主币为无限法偿货币，辅币为有限法偿货币。纸币流通时代，主币和辅币均为价值符号，都凭国家赋予的权力流通，故都是无限法偿货币。

4. 稳定币

一种旨在针对特定资产或一篮子资产保持固定价值的加密资产。

稳定币（Stablecoin）是通过与法定货币、主流数字货币、大宗商品等财产锚定，或通过第三方主体调控货币供应量的方式，实现货币价格相对稳定的区块链数字货币。目前，根据锚定对象与运行机理的不同，稳定币可分为链下资产支持型稳定币（Off-chain-backed Stablecoin，以下简称为“链下型稳定币”）、链上资产支持型稳定币（On-chain-backed Stablecoin，以下简称为“链上型稳定币”）以及算法型稳定币。

5. 证券代币（SECURITY TOKENS）

在其发行、营销、转让、交易、存储的辖区符合“证券”定义的加密资产。通俗地说，证券型代币必须与资产挂钩，例如现金、股份、固定收益资产、不动产、大宗商品等。它们是数字资产（代币）与传统金融产品的交汇点——一种改进旧事物的新技术，如果我们把比特币这样的加密货币称之为“可编程货币”，那么证券型代币则可以被称为“可编程所有权”版本的代币，也就是其所有权下的任何资产都可以并将被代币化（包括公开募股和私募股权、股票、债务、不动产、商品等）。

6. 普惠金融

指个人和企业能够以一种负责任和可持续的方式获得满足其需求的有用且可负担的金融产品和服务（如交易、支付、储蓄、信贷和保险）。

联合国于2005年提出的金融服务概念，意指普罗大众均有平等机会获得负责任、可持续的金融服务；又称包容性金融，其核心是有效、全方位地为社会所有阶层和群体提供金融服务，尤其是那些被传统金融忽视的农村地区、城乡贫困群体、微小企业。近年来，随着科技与环境的快速演变，“金融科技”成为推展普惠金融的重要力量。

小微企业、农民、城镇低收入人群、贫困人群和残疾人、老年人等特殊群体是当前我国普惠金融重点服务对象。

7. 实用代币（UTILITY TOKENS）

指赋予持有人权利，可从发行机构或发行网络获取当前（或未来）的某种产品或服务的加密资产。

实用代币比硬币有更广泛的功能，因为它们通过授予用户获得未来服务或产品的机会，以不同的方式为投资者提供价值。例如，一家新成立的公司可以设置首次代币发行，并向投资者出售实用代币，投资者可以在以后使用它们来购买公司的产品和服务。

8. 私人数字货币

私人发行的数字货币，也就是虚拟货币，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，比如我们通常知道的比特币。简单说呢，数字货币与传统货币类似，可以用于购买实物商品和服务。

四、区块链相关概念

1. 区块链

区块链是一个共享的、不可篡改的分布式账本，旨在促进业务网络中的交易记录和资产跟踪流程。资产 可以是有形的（如房屋、汽车、现金、土地），也可以是无形的（如知识产权、专利、版权、品牌）。几乎任何有价值的东西都可以在区块链网络上跟踪和交易，从而降低各方面的风险和成本。如果要修改区块链中的信息，必须征得半数以上节点的同意并修改所有节点中的信息，而这些节点通常掌握在不同的主体手中，因此篡改区块链中的信息是一件极其困难的事。

相比于传统的中心化网络机制，区块链具有如下三大核心特点：一是数据难以篡改、二是去中心化、三是共识机制。基于这三个特点，区块链所记录的信息更加真实可靠，可以帮助解决人们互不信任的问题。

2. 智能合约

智能合约（英语：Smart contract ）是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。智能合

约概念于1995年由Nick Szabo首次提出，智能合约的目的是提供优于传统合约的安全方法，并减少与合约相关的其他交易成本。

智能合约只是存储在区块链上的程序，在满足预先确定的条件时会运行这些程序。 它们通常用于自动执行协议，以便所有参与者都可以立即确定结果，而无需任何中间人参与，也不会浪费时间。 它们还可以自动完成工作流程，在满足条件时触发下一个操作。

3. 分布式账本

分布式账本也称为共享账本，是一种可在网络成员之间共享、复制和同步的数据库。分布式账本记录网络参与者之间的交易，比如资产或数据的交换。这种共享账本降低了因调解不同账本所产生的时间和开支成本。

分布式账本的特点：

- 去中心去信任：多份数据分布保存在各个节点，没有中心化或第三机构负责控制数据。
- 集体维护数据一致：参与者以公钥作为身份标识，各节点独立校验数据合法性，各节点共识决定写入哪些数据。
- 数据可靠难以篡改：数据在区块中，各节点保存全部区块。可定制数据访问权限，块间的链式关联防止篡改数据。

4. 非对称加密

非对称式密码学（英语：Asymmetric cryptography）也称公开密钥密码学（英语：Public-key cryptography），是密码学的一种演算法，它需要两个密钥，一个是公开密钥，另一个是私有密钥；公钥用作加密，私钥则用作解密。使用公钥把明文加密后所得的密文，只能用相对应的私钥才能解密并得到原本的明文，最初用来加密的公钥不能用作解密。由于加密和解密需要两个不同的密钥，故被称为非对称加密；不同于加密和解密都使用同一个密钥的对称加密。

公钥可以公开，可任意向外发布；私钥不可以公开，必须由用户自行严格秘密保管，绝不透过任何途径向任何人提供，也不会透露给被信任的要通讯的另一方。基于公开密钥加密的特性，它还能提供数位签章的功能，使电子文件可以得到如同在纸本文件上亲笔签署的效果。

5. 共识机制

共识机制就是为了解决在分布式记账系统中如何达成一致的问题。共识机制也是所有节点都必须要遵守的一种**规则**。交易的记账权是需要竞争才能获得的，即通过挖矿来计算一个复杂的数学问题，通过提高数学题的难度，可增加所需计算量，这种计算量构建了一个工作量证明机制。

如果想要修改某个区块的交易信息，就必须完成该区块和其之后连接区块的所有工作量，这大大增大了篡改数据的难度。除非拥有系统51%以上的算力，而目前是不可能的。全网认可最长的链，因为最长的链包含了最大的工作量，这笔交易就被最终验证。

6. 去中心化金融（Defi）

指一系列另类金融市场、产品和体系，它们使用加密资产和所谓“智能合约”的软件，以分布式账本或类似技术构建。不同于过去中心化的传统金融需要许多中介机构如银行、保险业者、证券交易所的参与，并且对本人进行身份认证，才能让客户进行买卖交易、抵押借贷、保险赔付等金融商品的购买及使用；DeFi 利用了区块链的技术，完全解决了身份认证的麻烦以及因为中介机构参与而产生的额外成本支出这两个问题，同时也在这个基础上，逐渐发展出有别于传统金融的金融商品，而开始受到追捧。

7. 数字资产

使用分布式账簿或类似技术发行或承载的数字工具。其不包括数字形式的法定货币。数字资产的广义定义为在加密安全的分布式账本或财政部门指定的任何类似技术上记录的任何价值的数字表示形式。数字资产包括（但不限于）：

- 可兑换的虚拟货币和加密货币
- 稳定币
- 不可替代的代币（NFTs）

数字资产不是真实货币（又称“法定货币”），因为数字资产硬币和纸币，也并非由政府的中央银行以数字方式发行的。

与真实货币等值的数字资产，或作为真实货币的替代品，被称为可兑换虚拟货币。

加密货币是可兑换虚拟货币的一个实例，可以用于支付商品和服务款项，在用户之间进行数字交易，并兑换成真实货币或数字资产。

8. 加密资产

也称为“加密货币”，是一种主要依赖于密码学和分布式账本技术（或类似技术）的私人部门数字资产。加密资产可以提高支付和转账效率，它们的匿名性特征可能会带来洗钱及恐怖活动融资的风险。加密资产活动可分为涉及资产发行和分配的基础市场活动、次级市场活动，以及边缘市场活动三种类型。

9. 电子钱包（E-MONEY）

一种存储的货币价值或预付款产品，其中，消费者的资金或价值（其可用于多种用途）的记录被存储在预付卡或电子设备（如计算机或电话）上，并作为一种支付工具被发行人以外的其他方所接受（可用于多种用途）。这种储存的价值代表了对电子钱包提供商的债权，电子钱包提供商需在对方要求时全额偿还。

五、数字人民币是什么

1. 概念与主要特征

数字人民币是央行发行的数字形式的法定货币，由指定运营机构参与运营，以广义账户体系为基础，支持银行账户松耦合功能，与实物人民币等价。根据央行披露的信息，数字人民币主要有以下几个特征：

- 数字人民币是央行发行的法定货币，体现为央行对公众的负债，以国家信用为支撑，具有法偿性。
- 数字人民币采取中心化管理、双层运营架构，央行在运营体系中处于中心地位，负责指定运营机构的商业银行发行数字人民币并进行全生命周期管理，后者则负责向社会公众提供数字人民币兑换和流通服务。
- 数字人民币定位于现金类支付凭证（M0），与实物人民币长期并存。在未来的数字化零售支付体系中，数字人民币和指定运营机构的电子账户资金具有互通性，共同构成现金类支付工具。
- 数字人民币是一种零售型央行数字货币，主要用于国内零售支付需求。

2. 主要优势

数字人民币无兑换、交易、转账手续费外，最大优势是不依赖银行账户便可以独立存在、进行价值转移，即其具有支付即结算、支持离线交易和可控匿名（小额匿名与大额可溯）等优势，使得其在一定程度上摆脱了实体银行账户、避免了网络通信费中间清算收费以及个人隐私保护等问题。具体来看：

用户通过下载“数字人民币（试点版）App”，并输入手机号、验证码、设置登录密码，选择运营机构后就可以完成等级为“四类钱包”的注册，绑定银行卡后则相应升级为“二类钱包”（即数字钱包内的数字人民币与绑定银行卡账户内存款可以互转），通过App上的付款码和收款码就能完成交易。其中：

- 数字人民币钱包支持NFC功能的手机通过在线、离线两种模式，靠近POS终端NFC区域、或与另一台NFC手机轻轻“碰一碰”（苹果手机暂不支持POS终端和手机终端），即可安全便捷的支付。在手机无电无网的情况下也可以完成交易！
- 在转账功能上，仅需在App内输入收款人手机号或钱包编码后，再输入金额和支付密码即可成功转账。
- 在数字人民币钱包内还可添加“子钱包”开通钱包快付功能，绑定京东、饿了么、美团等商户，就可相应的商户App内使用数字人民币付款。微信视频号、小程序可以使用数字人民币支付啦

此外，除上文提及的“数字人民币（试点版）App”外，用户还可以通过指定运营机构手机银行App开通数字人民币钱包，非指定运营机构的商业银行亦可以通过与指定运营机构合作，向客户提供数字人民币服务。

这意味着没有银行账户的社会公众也可以通过数字人民币享受基础金融服务，短期来华的境外居民可以在不开立中国内地银行账户的情况下开立数字人民币钱包，满足在华日常支付需求。

2. 试点地区：共涉及17省（市）地区

目前数字人民币试点地区已历经四批。具体来看：

1. 2020年4月，数字人民币先行在深圳、苏州、雄安、成都、冬奥场景等“4+1”地区进行封闭测试。
2. 2020年10月，央行新增上海、海南、长沙、西安、青岛、大连6个地区，使得数字人民币试点地区扩展至“10+1”地区。
3. 2022年3月，央行启动数字人民币第三批试点地区，将天津、重庆、广州、福州、厦门、浙江省承办亚运会的六个城市作为试点地区，同时明确北京市和张家口市在2022年北京冬奥会、冬残奥会场景试点结束后转为试点地区。
4. 截止到2022年12月16日，数字人民币试点地区已扩展至17个省市和地区，全部的试点地区包括：北京、天津、河北省、大连、上海、江苏省、浙江（杭州、宁波、温州、湖州、绍兴、金华）、福建（福州、厦门）、山东（济南、青岛）、长沙、广东省、广西（南宁、防城港）、海南省、重庆、四川省、云南（昆明、西双版纳）、西安。

根据本次更新的情况，我们注意到：一方面，试点地区由深圳、苏州、雄安、成都4个单点城市，进一步扩展至广东、江苏、河北、四川全省；另一方面，增加了山东省济南市、广西壮族自治区南宁市、防城港市和云南省昆明市、西双版纳傣族自治州等5个市（州），作为新的试点地区。

此次数字人数字人民币民币试点区域的扩大，意味着我国央行数字人民币在前三批试点的基础上继续稳妥有序推进，为最终走向全国推广奠定更扎实的技术和应用基础。

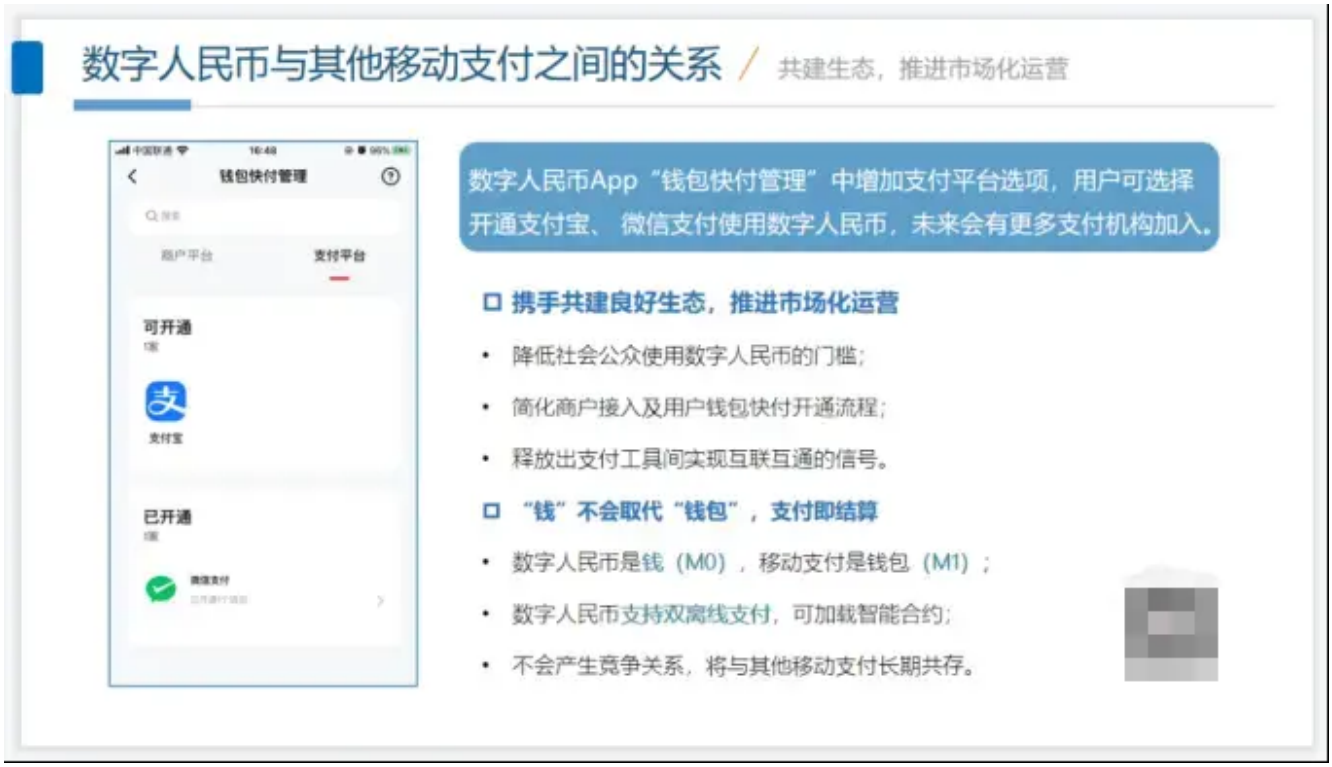
3. 指定运营机构10家

目前数字人民币的指定运营机构共10家，分别为工行、农行、中行、建行、交行、邮储银行、招商银行、兴业银行以及网商银行（支付宝）、微众银行（微信支付），即包括全部国有六大行、股份行中的招行与兴业银行以及网商银行、微众银行两家互联网银行。

4. 数字人民币与第三方支付有一定差异

数字人民币与支付宝、微信支付等第三方支付工具存在一些差异，数字人民币等同于现金，支付宝、微信支付则为装钱的工具或载体，即钱包。主要体现在第三方支付工具资金存放于第三方支付机构，并由机构向央行缴存准备金；第三方支付工具没有网络难以完成支付（即支付后需等待第三方支付机构统一结算）；以及第三方支付工具需要实名认证且第三方平台会获得消费者身份信息和支付数据等等。

除了差异之外，数字人民币与其他移动支付之间也有一定的关系。我发现数字人民币App“钱包快付管理”中已经增加支付平台选项，用户可选择开通支付宝、 微信支付使用数字人民币，相信未来会有更多支付机构加入。



作者：沐沐；整理：闻道、喵喵、峰峰；公众号：沐沐讲数币，数字人民币支付产品专家。