

智能环境下金融行业面临的挑战及创新模式

北京大学 信息工程学院

朱跃生

2022年12月

北京大学

数字经济

- 以数据及数字化的知识和信息作为核心生产要素，
以数字基础设施为基石
以数字技术为关键驱动以网络为载体
以数字政府治理为保障，
- ✓ 创新运用数字技术，网络技术及智能技术，促进数据安全有序高效流转，推动数字产业化和产业数字化共同发展，实现全要素生产率提升和经济高质量发展。

数字政府治理有助于打通不同部门、不同区域、上下之间的数据壁垒，运用互联网、大数据、人工智能等技术改进行政管理和公共服务

数字经济的“四化框架”

生产要素

数据价值化



4

数据采集



数据确权



数据定价



数据交易

技术

资本

劳动

土地...

生产力

1

数字产业化



基础电信



电子信息制造



软件及服务



互联网

产业数字化

数字技术在
农业中的边际贡献数字技术在
工业中的边际贡献数字技术在
服务业中的
边际贡献

2

生产关系

数字化治理



多主体参与

3



数字技术+治理



数字化公共服务

数字经济的“四化”框架 资料来源：中国信息通信研究院

数字化/信息化/网络化/智能化 发展

融合先进信息技术的万物互联智能生态环境

- 物联网 (IoT)
- 移动计算 Mobile Communication & Computing
- 人工智能 (AI)
- 区块链 (Block Chain)
- 云计算 (Cloud)
- 大数据 (Data Science)
- 边缘计算 (Edge Computing)
- 扩展现实 (XR, Extended Reality)
- 信息安全 (Security)

I M A B C D E X S

金融科技与数字经济

FinTech将融入到数字经济的各类新业态及治理模式中

- FinTech将进一步深化供应链与金融服务合作，推进产业链运营、供应链管理、交易风险管控等领域的数字化升级
 - FinTech支撑支付、保险等金融服务无缝嵌入到各行业应用中如智慧城市的所有模块及城市生活服务中，推动城市治理数字化程度不断提高
 - 随着数字经济发展，企业数字化、产业互联网、数字城市治理等数字经济领域积累了大量数据，可进一步推动FinTech在金融服务质量及金融风险防控等方面发挥更大作用
-

- 
- 物联网及互联网成为获取金融数据及提供服务的重要途径
 - 大数据及云平台技术将在金融机构、客户营销、银行信贷风险管理、信用评估等方面，进一步提升精准性和风险预警的时效性
 - AI技术将提高金融服务自动化、智能化方面的应用更为广泛。区块链技术将在分布共享数据等丰富应用场景中，发挥防篡改、可追溯、多方协同的优势
- 

数字经济规模的测算框架

数字经济

数字产业化部分

(信息产业增加值)

数字技术创新和数字产品生产。主要包括电子信息制造业、信息通信业、互联网行业和软件服务业等。

产业数字化部分

(数字技术与其他产业融合应用)

国民经济其他非数字产业部门使用数字技术和数字产品带来的产出增加和效率提升。

数字产业化部分规模
(增加值)

产业数字化部分规模
(增加值)

=
电子信息制造业(增加值)

=
ICT产品和服务在其他领域融合渗透带来的产出增加和效率提升
(增加值)

+
基础电信业(增加值)

+
互联网行业(增加值)

$$Y = A(N_{\text{ITP}} \cdot N_{\text{OTC}} \cdot \text{Res})F[G(K_{\text{ITP}}, ETC_{\text{ITP}}), K_{\text{OTC}}, M, H, L]$$

+
软件服务业(增加值)

效率提升

产量增加

2014-2021年我国数字经济规模及占比GDP



制图：华经产业研究院（www.huaon.com）

货币 (Currency, Money)

□ 由各国政府或中央银行发行交易单位

- 用于支付商品劳务和清偿债务
- 充当交换媒介，价值、贮藏、价格标准和延期支付标准
- 与国民收入相关最大的流动性资产



□ 货币的职能-货币本质的具体体现

- ✓ **价值尺度**: 作为测量商品中包含价值量
- ✓ **流通手段**: 做为商品交换的媒介，特点是在产品交易中，产品的拥有和货币的拥有**在同一时间内**进行
- ✓ **贮藏手段**: 离开流通领域时，充当独立的价值形式和社会财富的一般代表而被储存起来
- ✓ **支付手段**: 作为独立的价值形式进行单方面活动时所执行的职能（如清偿债务、缴纳税款、支付工资和租金等）
- ✓ **世界货币**: 在世界市场上执行一般等价物的职能

数字人民币（e-CNY）



- 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，与纸钞硬币等价
- 具有价值特征和法偿性，支持可控匿名

- ✓ 数字人民币发行、流通管理机制与实物人民币一致，数字形式的法定货币，以数字形式实现价值转移
- ✓ 和纸钞和硬币等价
- ✓ 将与实物人民币长期并存
- ✓ 是央行对公众的负债，以国家信用为支撑，具法偿性
- ✓ 采取中心化管理，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，指定运营机构及相关商业机构负责向社会公众提供数字人民币兑换和流通服务
- ✓ 主要用于满足公众对数字货币的需求，助力普惠金融

《中国数字人民币的研发进展白皮书》

□ **2021年7月16日，中国人民银行发布**

《中国数字人民币的研发进展白皮书》

中国数字人民币的研发进展
白皮书

- ✓ 阐明数字人民币研发的基本立场
- ✓ 阐释数字人民币体系的研发背景、目标

愿景、设计框架及相关政策考虑

中国人民银行数字人民币研发工作组
2021年7月

研发背景

□ 数字经济发展需要建设适应时代要求、安全普惠的新型零售支付基础设施

- 随着IMABCDEXS 等数字科技快速发展，数字经济新模式与新业态层出不穷
- 新冠肺炎疫情发生以来，网上购物、线上办公、在线教育等数字工作生活形态活跃，数字经济覆盖面不断拓展，欠发达地区、偏远地区线上金融服务需求日益旺盛
- 电子支付尤其是移动支付快速发展，为社会公众提供了便捷高效的零售支付服务，在助力数字经济发展的同时，培育了公众数字支付习惯，对技术和服务创新的需求提高
- 实现高质量发展，需要更安全、通用、普惠的新型零售支付基础设施作为公共产品，进一步满足人民群众多样化的支付需求，并提升基础金融服务水平与效率，促进大循环畅通，为构建新发展格局提供支撑

研发背景（续）

□ 现金的功能和使用环境正发生深刻变化

- 现金使用率呈下降趋势，据 2019 年人民银行开展的中国支付日记账调查显示，手机支付的交易笔数、金额占比分别为 66% 和 59%，现金交易笔数、金额分别为 23% 和 16%
- 现金管理成本较高，其设计、印制、调运、存取、鉴别、清分、回笼、销毁以及防伪反假等环节耗费了大量人力、物力、财力

□ 加密货币特别是全球性稳定币发展迅猛，给国际货币体系、支付清算体系、货币政策、跨境资本流动管理等带来诸多风险和挑战

宣称“去中心化”“完全匿名”，但缺乏价值支撑、价格波动剧烈、交易效率低下、能源消耗巨大等限制难以在日常经济活动中发挥货币职能。同时，加密货币多被用于投机，存在威胁金融安全和社会稳定的潜在风险，并成为洗钱等非法经济活动的支付工具

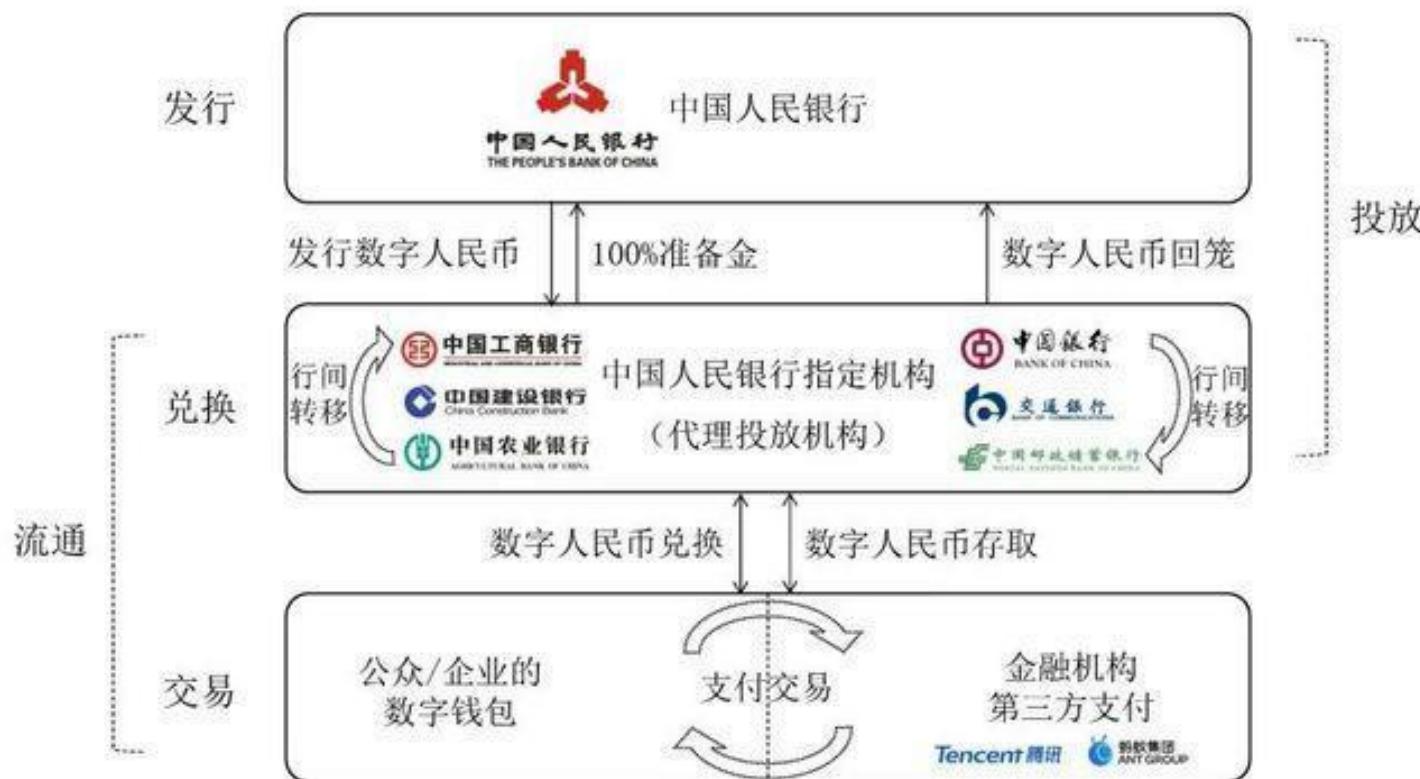
□ 国际高度关注并开展央行数字货币研发

65 个国家或经济体的中央银行中约 86% 已开展数字货币研究：美国、英国、法国、加拿大、瑞典、日本、俄罗斯、韩国、新加坡等国央行及欧央行公布了关于央行数字货币的考虑及计划，有的已开始甚至完成了初步测试

数字人民币 **VS** 电子支付工具

- 数字人民币是国家法定货币，是安全等级最高的资产
- 数字人民币具有价值特征，可在不依赖银行账户的前提下进行价值转移，并支持离线交易，具有“支付即结算”特性
- 数字人民币支持可控匿名，有利于保护个人隐私及用户信息安全

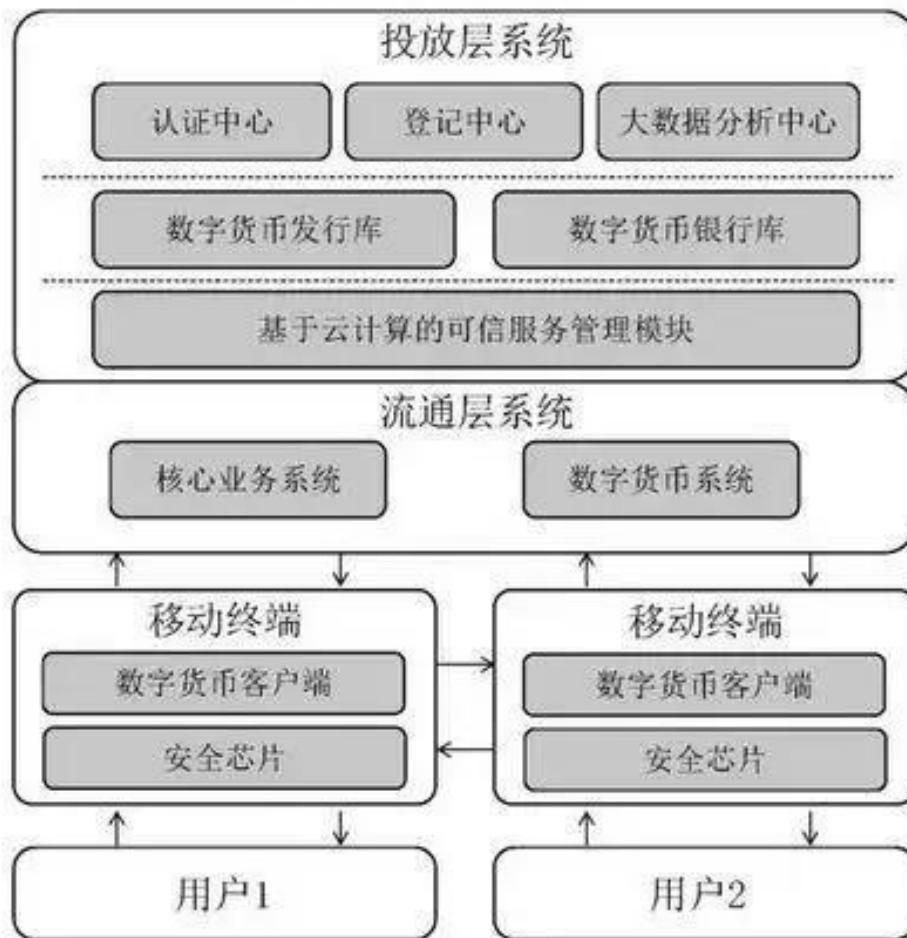
数字人民币 “双层运营体系”



数字人民币的研发/设计框架

数字人民币架构及功能模块

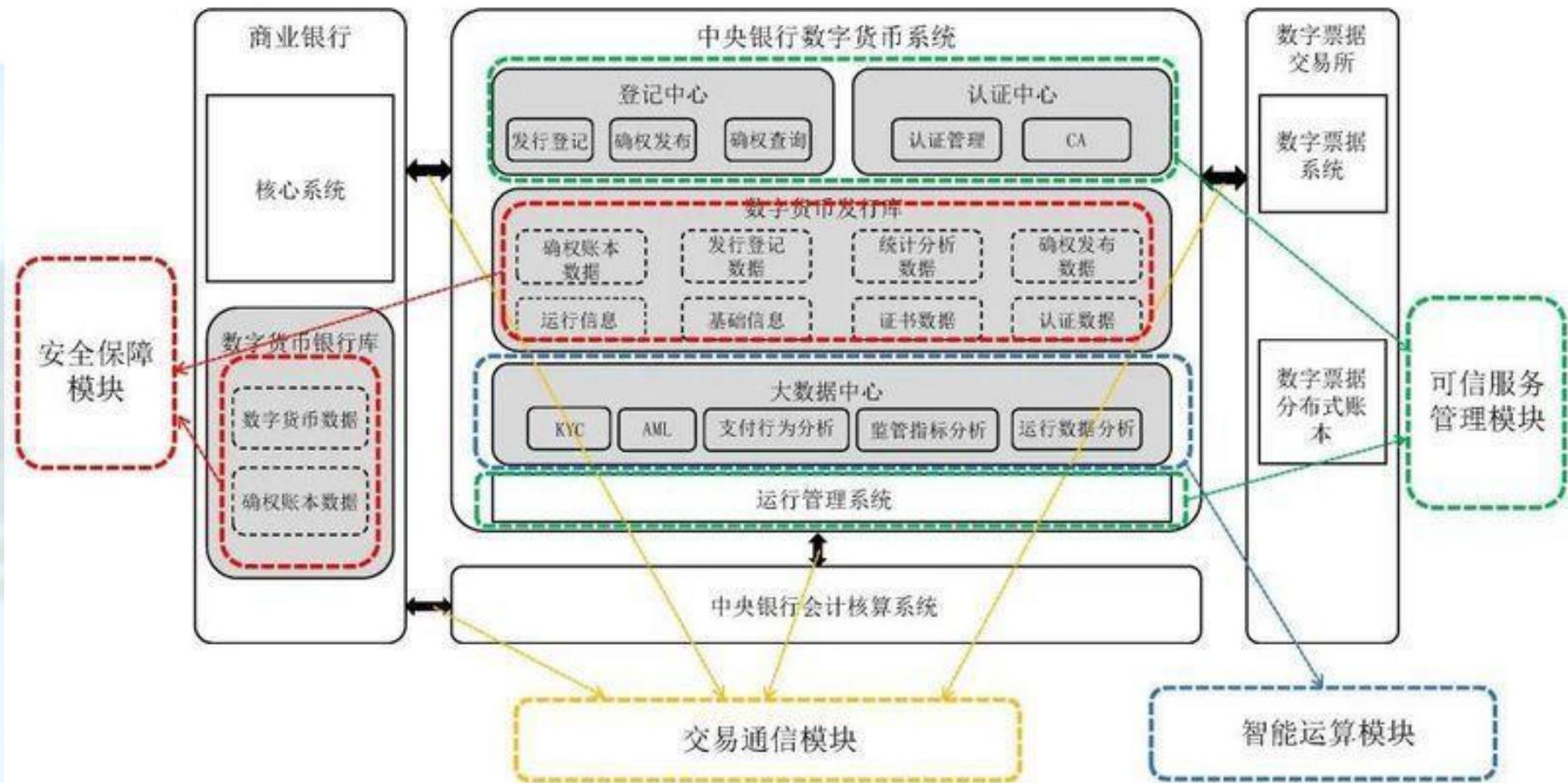
数字人民币系统简易框架



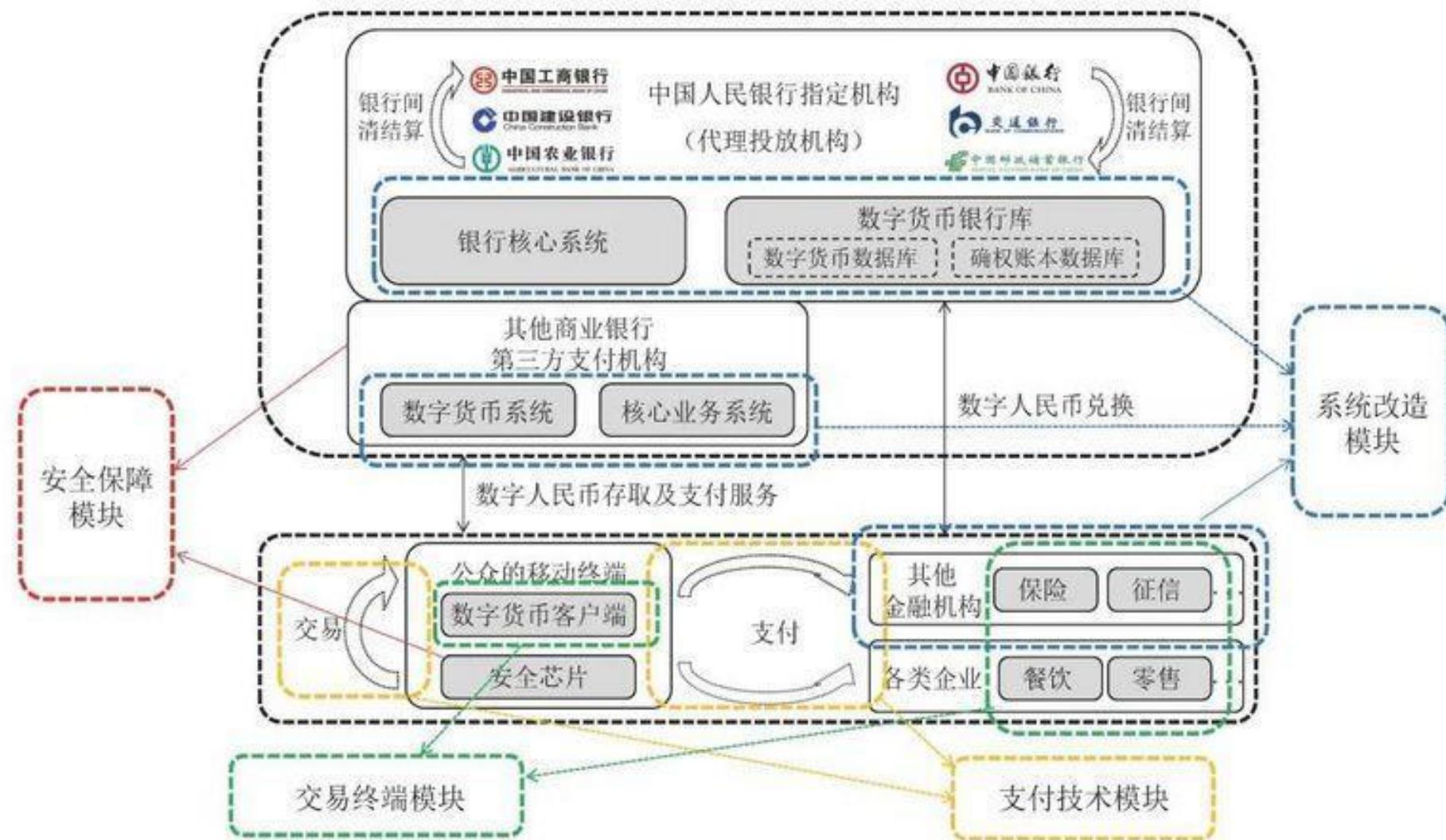
数字人民币系统功能模块



央行数字货币核心体系及功能模块



流通层及功能模块



数字人民币的技术路线

- 是一个长期演进、持续迭代、动态升级的过程，以市场需求为导向定期开展评估，持续进行优化改进
- 数字人民币系统采用分布式、平台化设计，增强系统韧性和可扩展性，支持数字人民币支付交易量的快速增长
- 综合应用可信计算、软硬件一体化专用加密等技术，以确保系统可靠性和稳健性
- 开展多层次安全体系建设，设计多点多活数据中心解决方案，保障城市级容灾能力和业务连续性，提供 **7x24** 小时连续服务
- 数字人民币体系综合集中式与分布式架构特点，形成稳态与敏态双模共存、集中式与分布式融合发展的混合技术架构

数字人民币钱包的设计

- 数字钱包是数字人民币的载体和触达用户的媒介
- ✓ 采用共建、共享方式设计移动终端 APP，对钱包进行管理并对数字人民币进行验证；
- ✓ 开发钱包生态平台，实现各自视觉体系和特色功能，实现数字人民币线上线下全场景应用，满足用户多主体、多层次、多类别、多形态的差异化需求，确保数字钱包具有普惠性。

- 按照客户身份识别强度分为不同等级的钱包，根据实名强弱程度赋予各类钱包不同的**单笔、单日交易及余额限额**
- 按照开立主体分为**个人钱包**和**对公钱包**
- 按照载体分为软钱包和硬钱包，可以丰富钱包生态体系，满足不同人群需求
 - 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实现数字人民币相关功能，依托 IC 卡、手机终端、可穿戴设备、物联网设备等为用户提供服务
- 按照权限归属分为**母钱包**和**子钱包**，可在母钱包下开设若干子钱包

数字人民币应用场景

□ 一种零售型央行数字货币，主要用于满足国内零售支付需求

➤ 深圳数字人民币生态体系

工商银行深圳市分行、农业银行深圳市分行、中国银行深圳市分行、建设银行深圳市分行、中国邮政储蓄银行深圳分行、交通银行深圳分行、招商银行深圳分行、微众银行（微信支付）等机构

✓ 试点范围不断扩大、应用场景越来越丰富、受理环境持续优化、使用频率逐步提高的良性发展趋势

例：2022年10月8日，深圳向个人发放1000万数字人民币红包，每个红包金额为200元，共计5万个。

数字人民币试点推进加速

□ 数字钱包

在中心化管理、统一认知、实现防伪的前提下，按照人民银行制定相关规则，各指定运营机构共建、共享方式建立移动终端APP，管理钱包并进行支付



□ 数字人民币SIM 卡



数币 SIM 卡 (SWP)

个人版数币钱包

安卓 NFC 智能机



数字人民币正式推出所面对挑战

➤ 受理终端建设

设计多样化的智能和定制化的钱包选择，改善用户体验；为所有商户设计及普及受理系统。

➤ 健全安全和风险管理机制

数字货币容易成为黑客的攻击目标，系统安全设计及开发是首要任务。必须保障在数字人民币的整个生命周期内，完善运营系统的安全管理，包括加密算法、金融信息安全、数据安全和业务连续性，以确保系统安全稳定。

➤ 设立明确的监管框架

2020年10月《中国人民银行法（修订草案征求意见稿）》虽明确“人民币包括实物形式和数字形式”，但数字人民币还需设立单独的完善的监管措施和管理办法

数字人民币安全应用

遵照《网络安全法》《个人信息保护法》《反洗钱法》《反电信网络诈骗法》等法律法规，通过一系列制度安排和技术手段确保个人信息安全，同时防范违法犯罪风险。

数字人民币防诈骗小贴士

不点击不明链接

通过官方途径获取数字人民币的权威资讯，切勿随意点击来历不明的短信链接。

谨慎转账

谨慎对待数字人民币转款，转账前，一定要认真核对转款事项。如发现上当受骗，应第一时间报警。

认准官方数币APP

数字人民币尚处试点阶段，市民下载数字人民币APP时，一定要选择官方渠道，根据银行提供的链接规范安装。

粤港澳大湾区

Guangdong-Hong Kong-Macao Greater Bay Area

□ (9+2) 城市群

- 粤 9: 广州、深圳、珠海、佛山、中山、惠州、东莞、肇庆、江门
- 特别行政区2: 香港、澳门

综合大湾区

科技+金融+产业

- 港澳与内地**不同的行政、社会、经济管理制度以及由此产生的理念及认知差异**



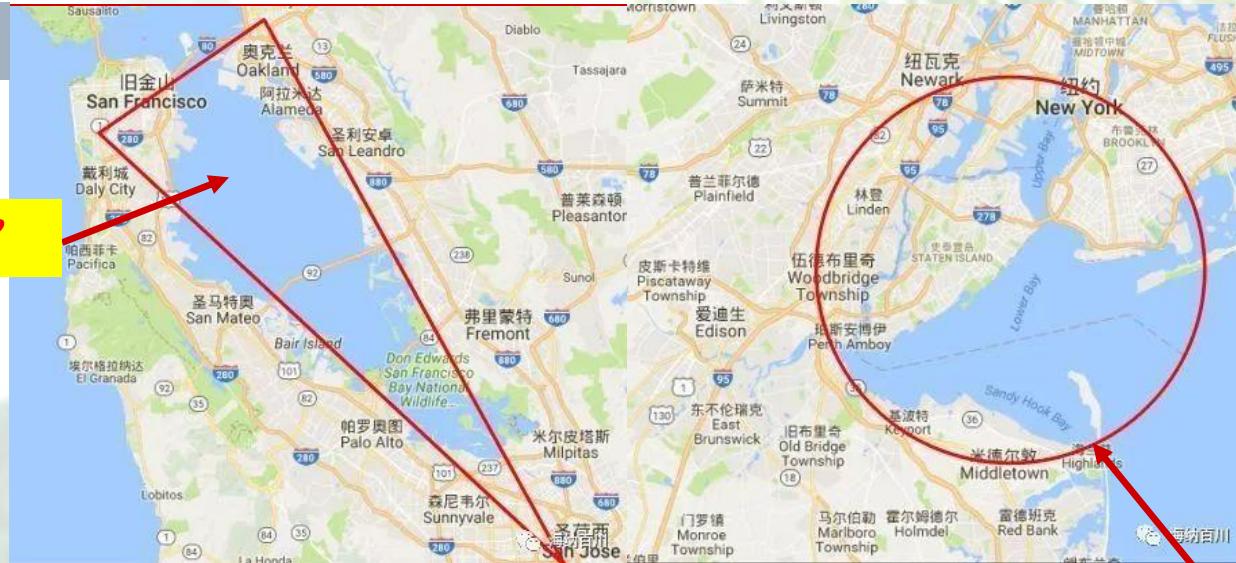
国际知名大湾区

共同点运行在同一个政治经济体制下！

➤ 美国

旧金山湾区

“高科技湾区”



纽约湾区

➤ 日本

东京湾区

“产业湾区”



“金融湾区”

粤港澳大湾区建设与挑战

□ “一国两制”框架下，充分发挥广东、香港和澳门各自优势，在制度多样性和发展水准差异性中寻求一致性，合作共赢发展，协同创新，务实推进建设。

➤ 综合大湾区

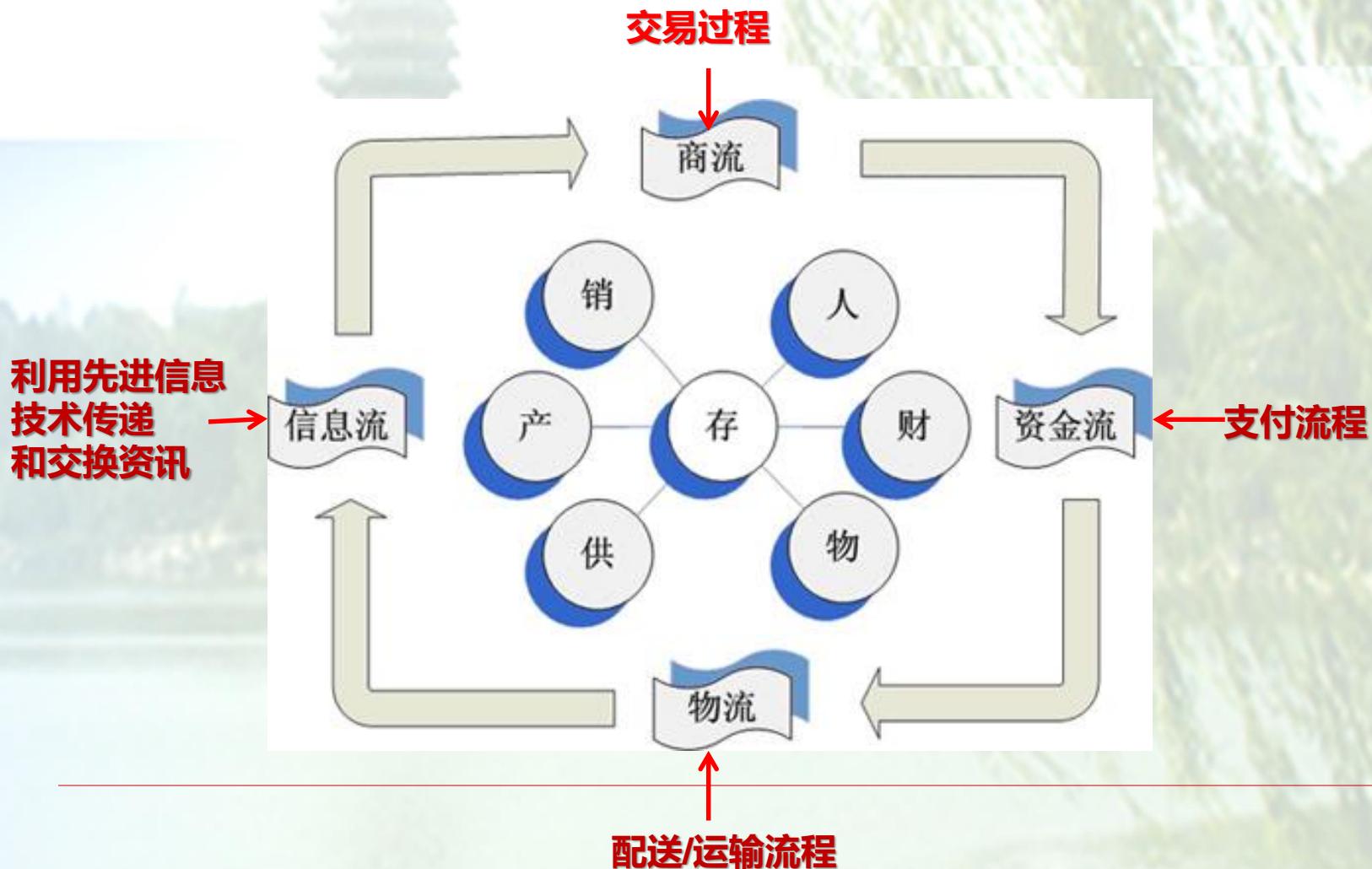
港澳（国际金融服务）+深圳（科技）+珠三角（产业）

➤ 协同创新模式

➤ **人才培养、跨境服务、科技、知识产权**

产学研用： 基础研究—场景研究—应用研究—产业推广

促进商流、物流、资金流和信息流融合发展 (“一国两制”框架下)



物联网+”发展与应用

在互联网基础上延伸扩展起来的网路

利用传感设备及网路技术，通过感知、识别、
以及网路连接

物物相连：在物与物间进行通信和信息交换，
利用智能技术，实现智能化识别、定位、跟踪、
监控和**安全管理**

事物：联事件，联人，联物，联数据



➤ 基于IoT的感知/移动支付

如：生物识别、NFC、ETC

➤ 基于IoT的即时动态掌控贷

款企业的运营过程：

采购管道、生产过程、

成品积压、销售情况...等，

及时调整贷款进度和额度，

贷前调查、贷中管理、

贷后预警，降低违约风险，

提高风控水准

移动计算 Mobile Computing

利用电脑或智慧终端机设备，在无线移动环境下实现数据传输及信息处理和资源分享

在飞行器、列车、车辆、行走等移动环境中，利用移动通信网和卫星通信产生的“物”联资料很丰富。各种各样的应用场景，将产生联人联物的大量数据。



移动金融

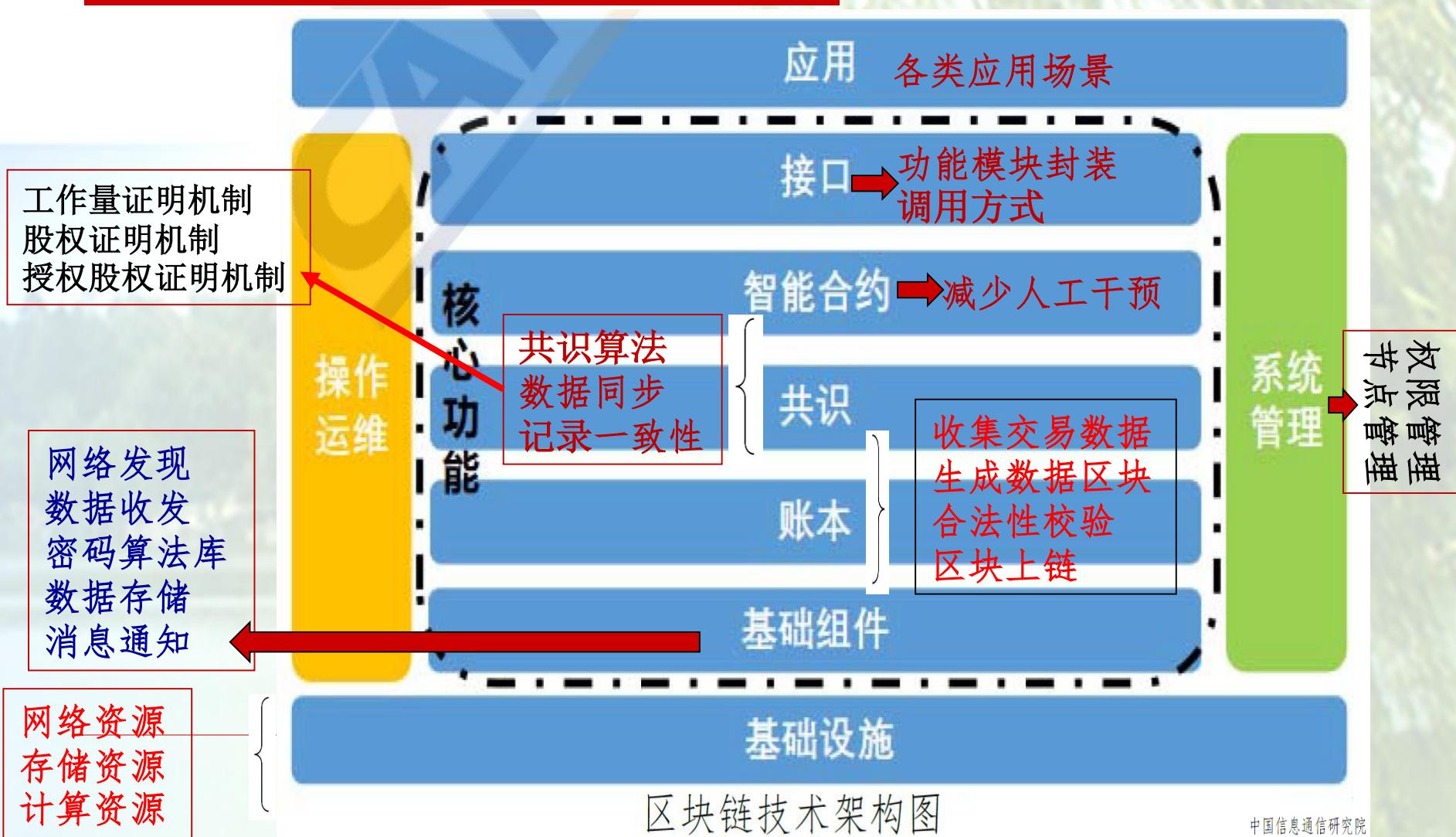


- 移动银行
- 移动掌上生活
- 移动理财投资
- 移动支付
- 移动信贷

区块链在金融行业应用

类型	政府	金融	工业	医疗	法律	版权
价值转移		数字票据 跨境支付 应收账款 供应链金融	能源交易	医疗保险		
存证	电子发票 电子证照 精准扶贫	现钞冠字号 溯源 供应链金融	防伪溯源	电子病历 药品追溯	公证 电子存证 网络仲裁	版权确权
授权管理	政府数据 共享	征信		健康数据 共享		版权管理

支撑区块链技术的基础架构



口 基于密码学原理

- ✓ 利用散列方法 (hashing) 对交易加上时间戳 (timestamps)
- ✓ 将它们合并入一不断延伸的基于散列的工作量证明链 (proof-of-work) 作为事务记录，保证记录具不可更改特性以及可溯源

口 采用共识算法对数据达成共识

- 各参与方按事先约定规则存储信息并达成共识
通过共识机制选出记录节点，由节点决定最新区块数据
- 多方参与最新区块数据的验证、存储和维护，数据一经确认，难以删除和更改，只能进行授权查询操作
- 任何达成一致的双方可直接进行支付，不需第三方中介参与

散列算法（哈希）



算法模型示意

✓ 散列算法的用途不是对明文加密，
而是防止对原文的篡改

固定长度值 (输出)

固定长度值

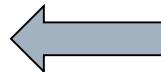
消息

散列函数

散列值

消息任何一位或多位的变化将导致该散列值变化！

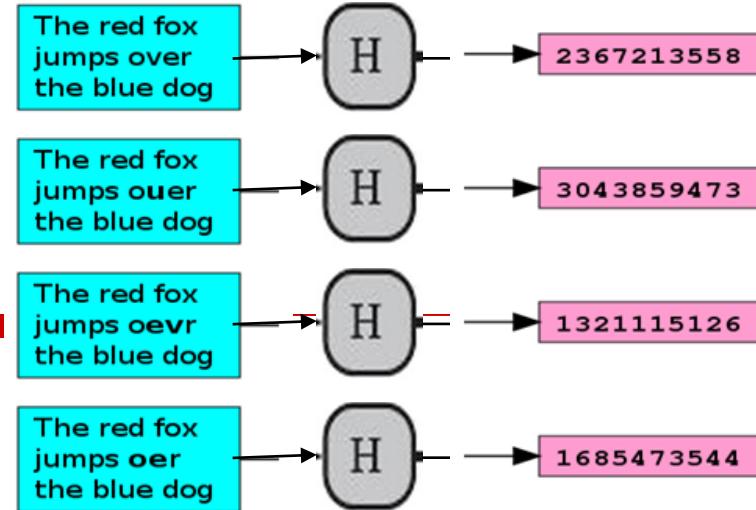
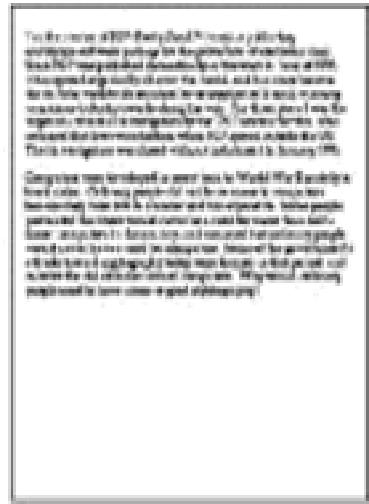
无穷大
消息集合



真正的原文
只是其中一份

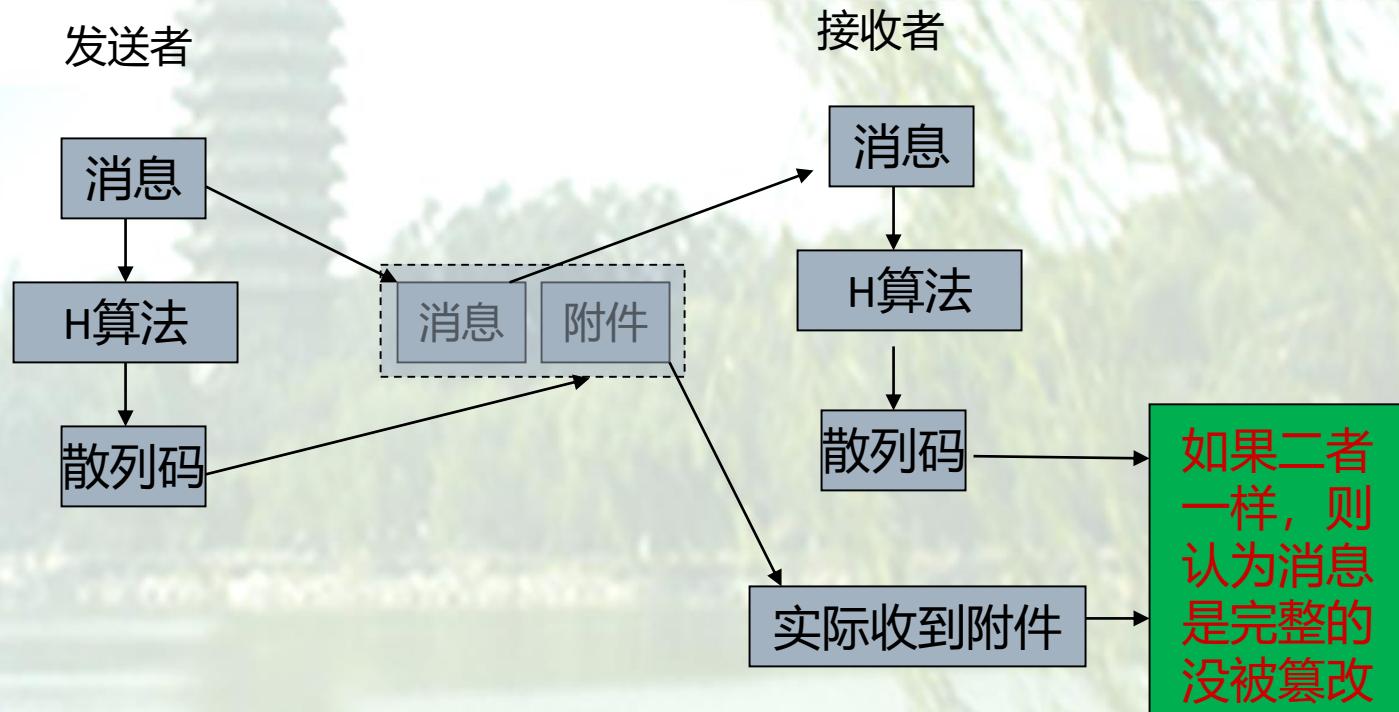
散列 (哈希) 算法

MD5, SHA1, SHA2, SHA3, SM3



" "	→ H → d41d8cd98f00b204e9800998ecf8427e
"a"	→ H → 0cc175b9c0f1b6a831c399e269772661
"abc"	→ H → 900150983cd24fb0d6963f7d28e17f72
"abcdefghijklmnpqrstuvwxyz"	→ H → c3fcfd3d76192e4007dfb496cca67e13b
"ABCDEFGHIJKLMNPQRS TUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"	→ H → d174ab98d277d9f5a5611c2c9f419d9f

消息鉴别一般机制



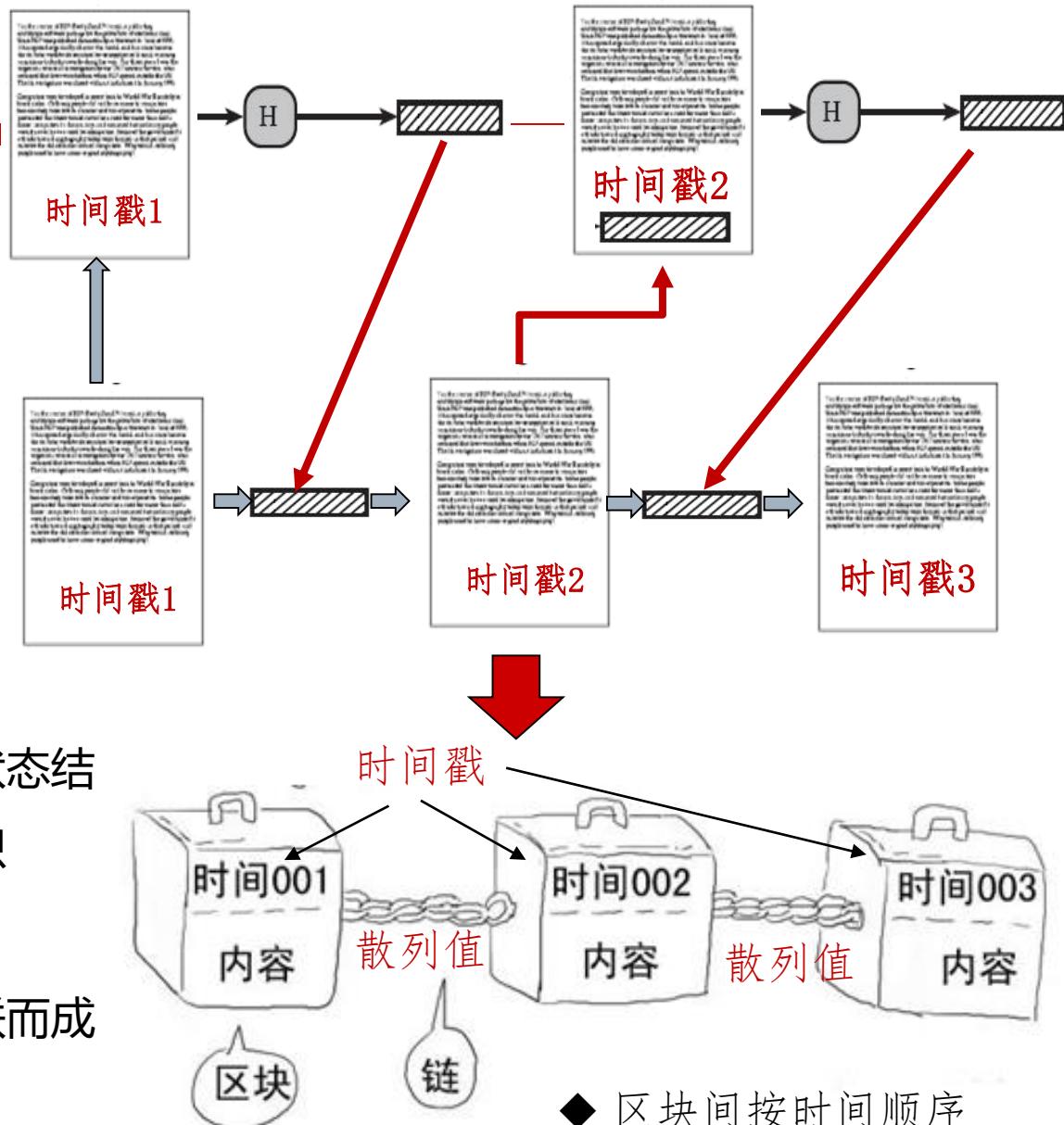
防止金融信息被篡改

信息与区块链示意图

◆结合密码学算法

- 区块（Block）为单位构成工作量证明的数据链
- 构成链式（Chain）数据结构

- 区块
记录一段时间内发生的交易和状态结果，对当前账本状态的一次共识
- 链
将一个个区块按照发生顺序串联而成整个状态变化的日志记录



区块链关键技术点

✓ 数据可信

→ 密码学算法

完整性检验
数字签名
时间戳
随机数
密码算法

→ 不可篡改

✓ 共识机制

→ 智能合约 → 链式结构

✓ 分布式数据存储

- 多方共同维护
- 密码学保证不可篡改传输和访问安全
- 一致存储、难以篡改、防止抵赖
(分布式账本)

✓ 点对点传输



区块链特征

➤ 一种带时间戳的新型数据库

需求：数据真实、有效、不可伪造、难以篡改

➤ 一个跨主体、多方写入的应用场景

需要：保证多个主体之间数据的一致性

➤ 在不可信的环境中建立基于数学的信任

需求：数据可信（密码学算法、数字签名、随机数）、结果可信（智能合约、公式算法）和历史可信（链式结构、时间戳）

一种“机器中介”，适用于协作方不可信、利益不一致或缺乏权威第三方介入行业



区块链特色

➤ 复式记账 演进》》分布式记账

传统系统由会计各自记录，存在多个不同账本

区块链变成“全网共享”分布式账本，参与记账的各方通过同步协调机制，保证数据的防篡改和一致性，规避复杂的多方对账过程

➤ “增删改查”演进》》“增查”操作

传统数据库具有增加、删除、修改和查询操作

区块链只增加和查询操作，通过区块和“块链式”结构，加上时间戳进行凭证固化，形成环环相扣、难篡改的可信数据集合



区块链特色

➤ 单方维护 演进》》多方维护

数据库单方维护系统，对数据记录具有高度控制权

区块链引入分布式账本，多方共同维护，数据的写入和同步不局限在一个主体范围之内，通过多方验证数据、形成共识，再决定哪些数据可以写入

➤ 外挂合约 演进》》内置合约

资金流和商务信息流是两个不同的业务流程，商务合作签订的合约在人工审核、鉴定后，再通知财务进行打款，形成相应的资金流

区块链采用智能合约，基于事先约定规则，通过代码独立执行、协同写入，形成信息流和资金流整合的“内置合约”

区块链分类（按应用场景分）

➤ 联盟链

只允许认证后的机构参与共识，交易信息根据共识机制进行局部公开；
根据一定特征所设定的节点能参与、交易，共识过程受预选节点控制

➤ 私有链

只适用于限定的机构之内

写入权限在一个组织手里，读取权限可能会被限制

➤ 公有链

允许任一节点加入，不对信息传播加以限制，信息对整个系统公开
任何人都能读取区块链信息，发送交易并能被确认，参与共识过程，
比特币是公有链的代表

区块链行业应用（美国）

（斯坦福大学《区块链项目研究报告》）

民主、政府



土地登记



慈善、捐助



健康



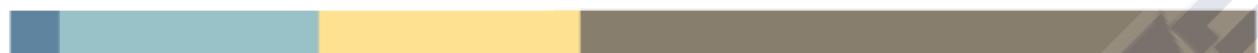
农业



金融科技



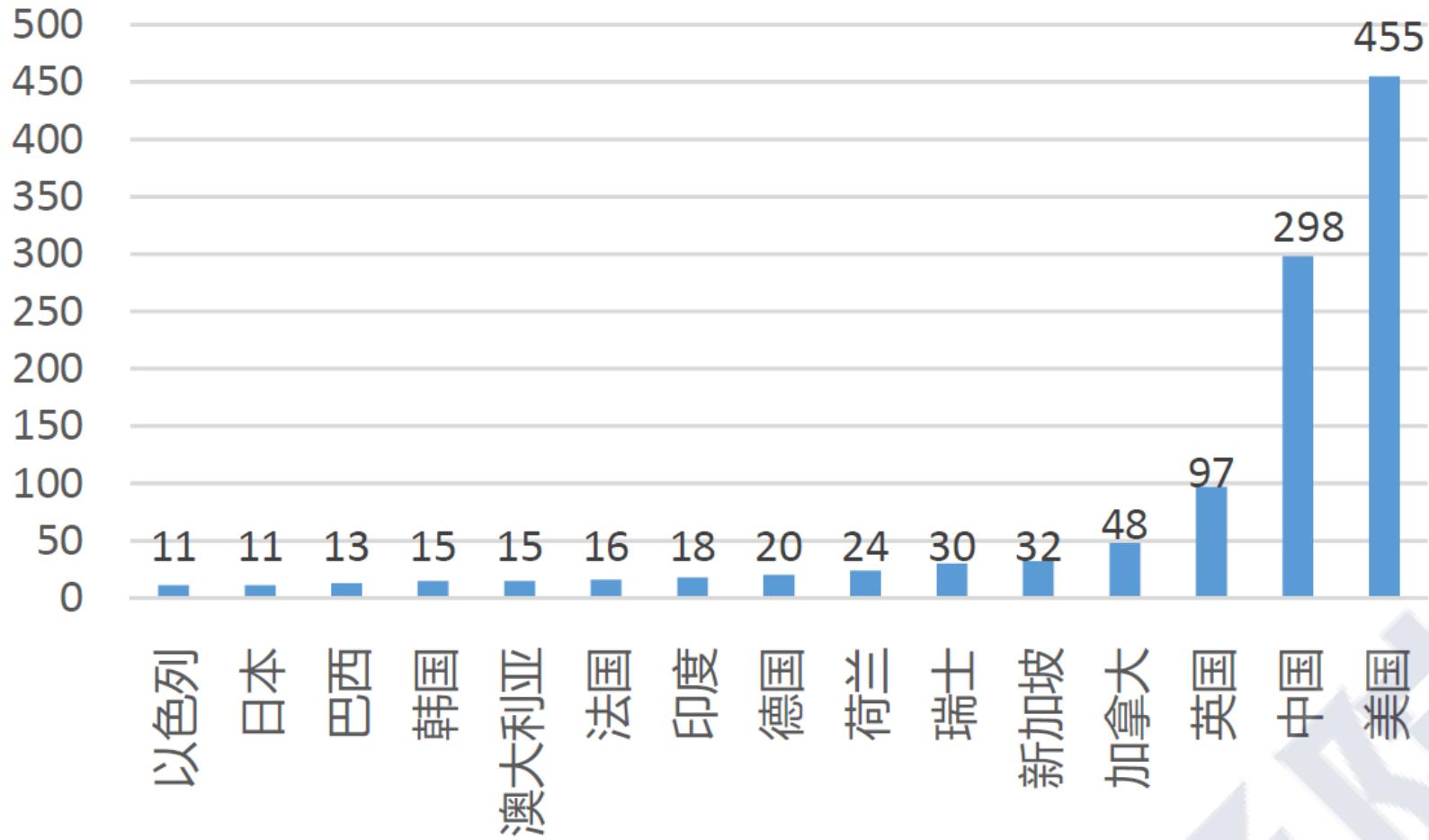
能源、气候、环境



Time Frame for Proof of Impact

- 0–6 months
- 6–12 months
- 1–2 years
- 2+ years
- Unknown

各国区块链企业分布



区块链应用前景

1

需求：

金融、医疗、公证、通信、供应链、功能变数名称、投票等领域都在尝试利用区块链技术

2

投资：

风投热情高，投资密度大，资金供给逐步上升，充足资金有望推动技术发展

3

应用：

一种市场工具，说明节约交易成本、管理成本，提高安全性，去除中间机构，公司业务模式转移

4

技术：

促进数据记录、数据传播、数据存储方式转型，有望改变互联网底层基础协定

5

社会结构变迁：

可融合经济和法律，改变社会监管模式及社会组织形态，走入分散式自治社会

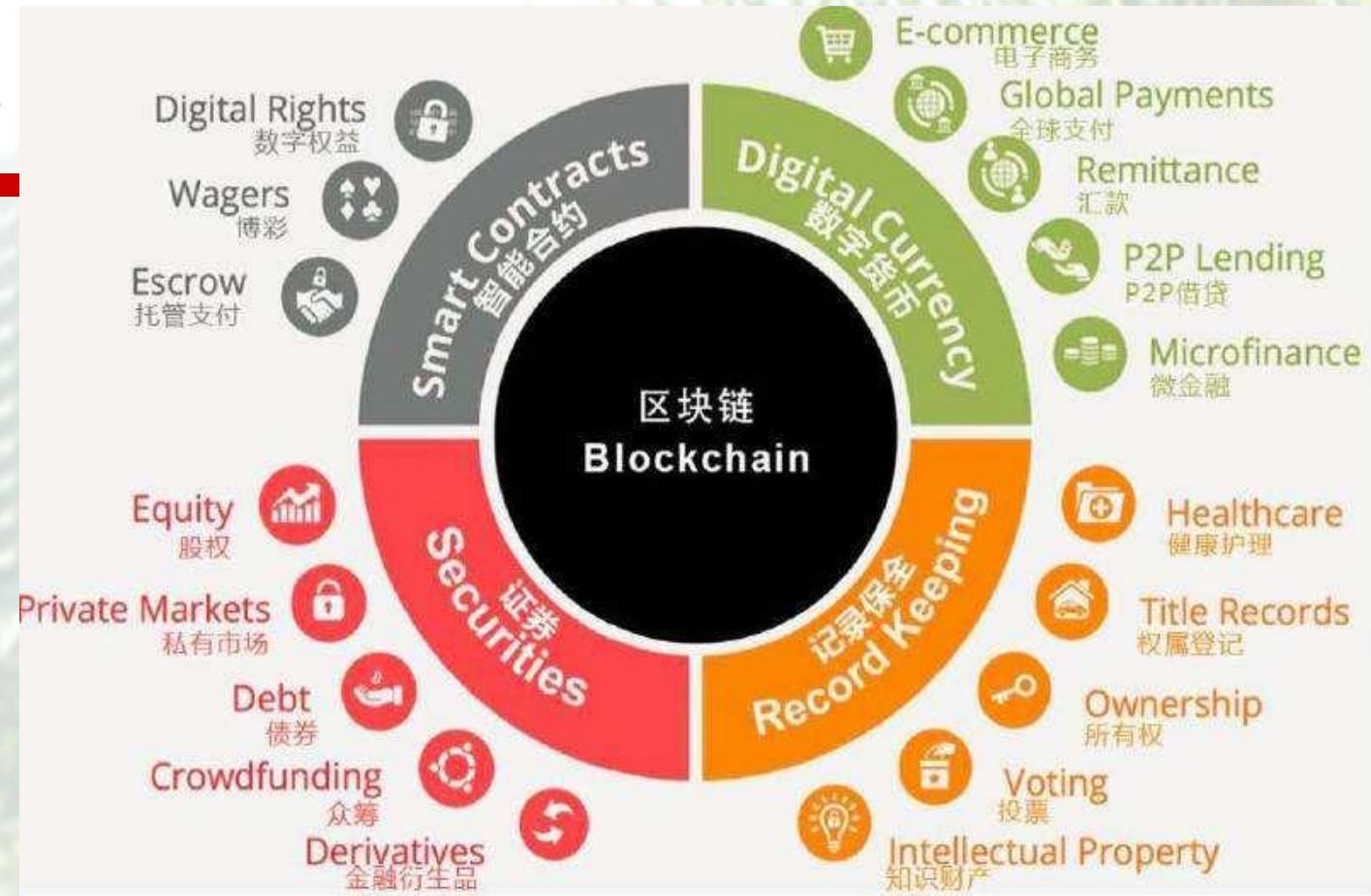
区块链应用场景

- 金融服务

- 权属管理

- 资源分享

- 降低交易成本
- 降低管理成本
- 降低管控风险



通过采用**数据加密、时间戳记、分散式共识和经济激励**等手段，在无需互相信任的分散式系统中实现点对点交易、协调与协作



融合先进资讯技术智能环境下互联网+，智能+

“互联网+，智能+” = “互联网+ 智能+各行各业”

北京大学

互联网+ 智能+金融

- ✓ 2017年6月中国人民银行颁布《中国金融业信息技术十三五发展规划》

利用信息技术持续驱动金融创新，促进金融业合理利用新技术，建设云计算、大数据应用基础平台及互联网公共服务可信平台，研究区块链、人工智能等热点新技术应用，实现新技术对金融业务创新有力支撑和持续驱动，促进金融创新发展，稳步推进系统架构和云计算技术应用研究

- ✓ 2017年7月国务院发布《关于印发新一代人工智能发展规划的通知（国发〔2017〕35号）》

明确指出人工智能已成为国际竞争的新焦点，是引领未来战略性的技术，世界主要发达国家把发展人工智能作为提升国家竞争力、维护国家安全的重大战略

传统金融统计方法与预测策略已不适用金融大数据发展需求。迫切需要在FinTech中，建立智慧金融科技创新云服务平台，使用大数据+人工智能实现金融大数据统计、智能分析、价值关联及预测，以及提供安全保障及隐私保护

国家新一代人工智能开放创新平台

(2017年11月至今)

- 依托百度：“自动驾驶”
- 依托阿里云：“城市大脑”
- 依托腾讯：“医疗影像”
- 依托科大讯飞：“智能语音”

- 依托商汤：“智能视觉”

- 依托上海依图：“视觉计算”
- 依托明略科技：“营销智能”
- 依托华为：“基础软硬件”
- 依托中国平安：“普惠金融”
- 依托海康威视：“视频感知”
- 依托京东：“智能供应链”
- 依托旷视：“图像感知”
- 依托360：“安全大脑”
- 依托好未来：“智慧教育”
- 依托小米：“智能家居”



金融科技 (FinTech)

➤ 融合先进信息技术的金融科技



IMABCDEXS



金融业

- ✓ 2015年国务院颁布《关于积极推进“互联网+”行动的指导意见》明确提出“互联网+普惠金融”发展方向

将互联网与银行、证券、保险、基金等进行融合创新，提供丰富、安全、便捷的金融产品和服务，满足不同层次实体经济的投融资需求，促进互联网金融的健康发展

- ✓ 2016年中国银监会颁布《中国银行业信息科技十三五发展规划监管指导意见》

以互联网、大数据、云计算等为代表的新兴技术与传统金融加速融合，既为银行业改革发转型带来了新的动力，也对银行业的传统优势领域形成一定压力，信息科技成为银行业金融机构抵御风险和增强竞争力的关键’

支付结算与清算服务

- 移动支付/P2P汇款/数字货币/数字交易所/外汇批发

社会

- 高频量化交易/程序化跟单交易/互联网证券/智能投融/智能投研



金融市场基础设施服务

- 大数据技术 (大数据分析、机器学习、预测模型)
- 分布式账本技术 (区块链、智能合约)
- 云计算技术
- 人工智能技术 (智能技术机器人、自动化财务、算法技术)
- 安全技术 (身份认证)
- 移动互联网/物联网技术
- 门户与数据聚合
- 生态系统 (基础架构、开源技术、APIs)

信贷、存款以及资金筹集

- 众筹/P2P网贷/移动银行/征信

图 金融科技的应用领域范围 资料来源：巴塞尔委员会

金融科技的发展

□ 第一阶段

科技行业的少数成果应用在金融领域，通讯技术与信息技术的发展使国际贸易、国际金融更加便捷，科技进步推动金融市场全球化

□ 第二阶段

科技扩大金融业的经营范围，改变金融业工作方式，通过IT 软硬体实现传统金融机构办公和业务的电子化、自动化，提升了金融机构工作效率，产生了信贷系统、清算系统等现代化产品

□ 第三阶段

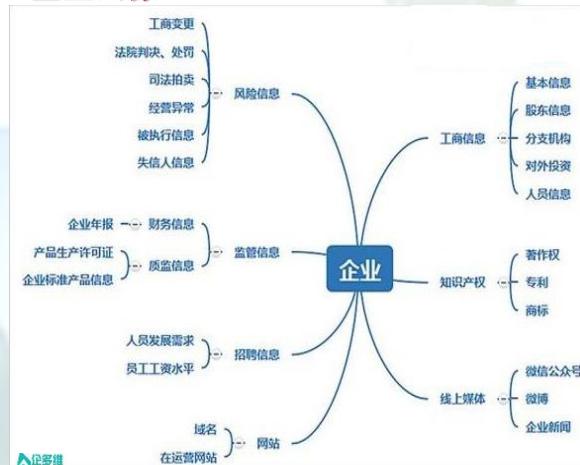
互联网金融阶段，依托互联网技术与信息通讯技术。提供金融服务或者与金融机构合作推出金融服务。搭建线上业务平台，利用互联网或者移动终端管道汇集海量的用户信息，实现金融业务中的资产端、交易端、支付端、资金端任意组合的互联互通

□ 第四阶段

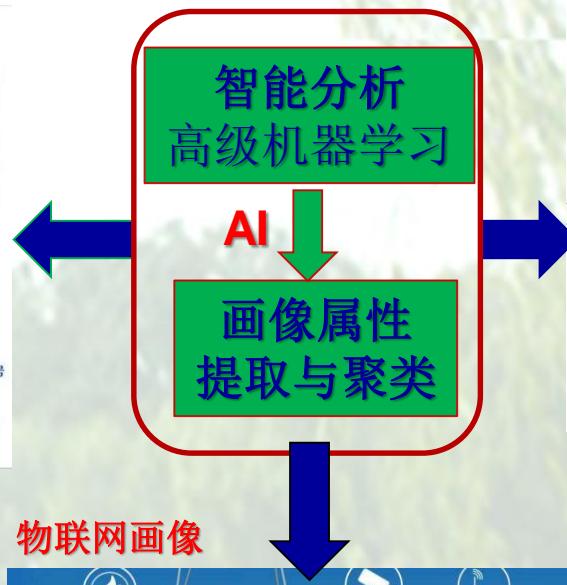
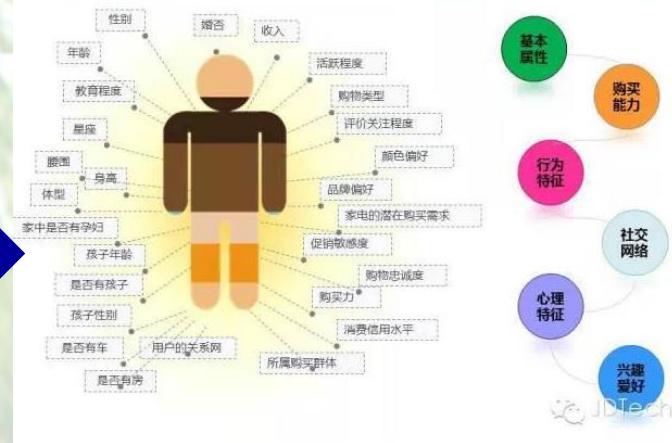
通过大数据、云计算、人工智能、区块链新的IT技术改变传统的金融信息采集来源、风险定价模型、投资决策过程、信用中介角色，可大幅提升传统金融的效率

大数据特征分析提取与人工智能

企业画像



用户画像



物联网画像



物体属性

金融业用户画像体系：银行版

支持应用场景

36大数据 (36dsj.com) 公众号: dashuju36

表征用户角色

第一维 · 标签应用深度

贴近生活
各种数据

预测标签

事实标签

虚拟代表
实际用户



ArchSummit 全球架构师峰会

信息集合: 用户社会属性、生活习惯和消费行为等信息
》勾画目标用户、联系用户诉求
》使用者属性、行为与关联

传统金融 → 智能金融

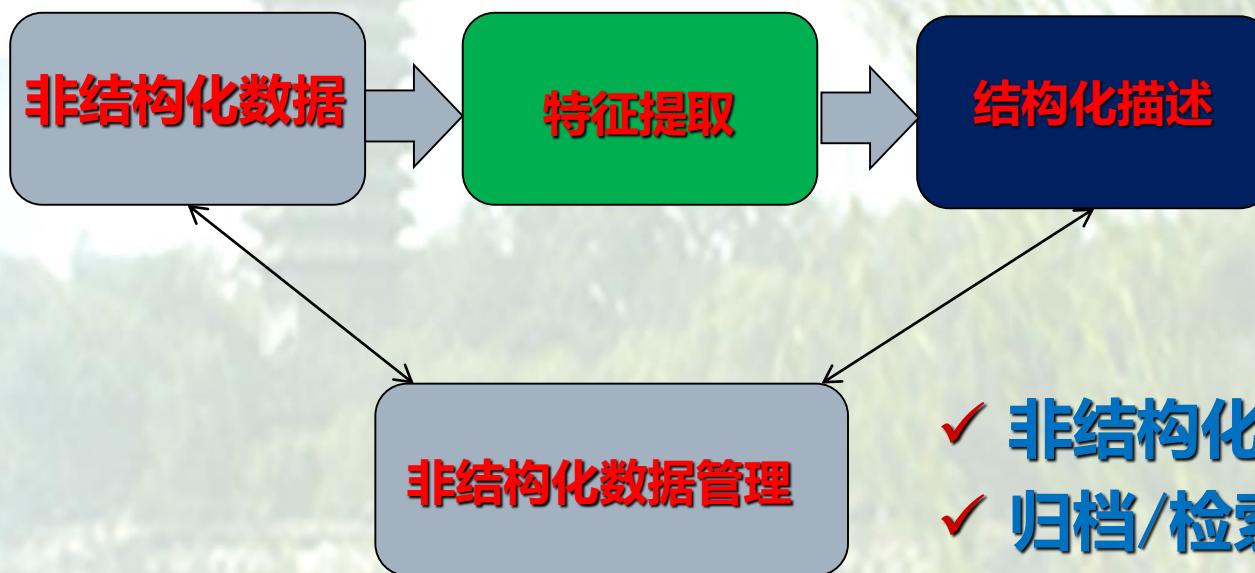
口 传统金融系统

- ✓ 数据收集和处理的方式原始
客户身份数据、资产负债情况数据、交易信息数据等
- ✓ 非结构化数据多
视频、音讯、纸质档等，难与标化和理解，需转换成可分析的结构化数据
- 人工智能技术发展，为海量金融数据的分析提供技术支持
深度学习、电脑视觉、自然语言处理
提升金融企业工作效率，进一步降低成本
- ‘人工智能+金融’应用的探索实践，摩根大通、花旗银行、招商银行、亚马逊、谷歌，蚂蚁金服、百度、京东金融等探索人工智能技术应用



金融非结构化大数据的结构化描述

化解为结构化数据



- ✓ 非结构化数据处理引擎
- ✓ 归档/检索引擎
- ✓ 描述与分类与聚类

主要业务

- 基于移动互联网技术的金融服务 (I/MS)
 - 基于人工智能的金融服务 (A/E/S)
 - 基于区块链的金融服务 (B/S)
 - 基于云计算的金融服务 (C/E/S)
 - 基于大数据的金融服务 (D/S)
 - 基于安全技术的金融服务 (S)
-

“互联网+普惠金融”

□ 互联网+金融模式

- 1) 互联网公司做金融
- 2) 金融机构互联网化
- 3) 互联网公司和金融机构合作

- 智能化征信
- 智能化风控
- 智能化投顾
- 智能投资

智能征信

□ 传统征信

- 依赖于信用卡、收入、还款行为等信息
- 高信息密度数据来源单一，时效性、覆盖率、场景触达率受限制

- ✓ 利用金融云平台，更精准更快捷地整合结构性/非结构性的多元化信用数据
- ✓ 与多家征信机构合作，针对性更强地与客户群体建立“粘性效应”
- ✓ 利用大数据分析挖掘客户交易数据间交互性和相关关系，对客户信贷记录、违约记录、偿还情况及各种消费情况、资产情况进行分析和筛选，评估客户还款能力和还款意愿，全面评估客户信用和深入测评业务风险，决定贷款授信，增强征信能力

智能风控

- ✓ 利用经验积累及机器学习理论，通过智能分析及检测方式，提前感知风险
- ✓ 根据修复策略，自我调整地可靠安全管理风控

智能投顾

- ✓ 对证券、保险、股指期货、银行帐单等数据，利用智能分析演算法对数据进行分析，为投资者优化组合投资，提供投顾服务，实现收益最大化

智能投资

- ✓ 人工智能量化投资平台 让金融投资更加“智慧”

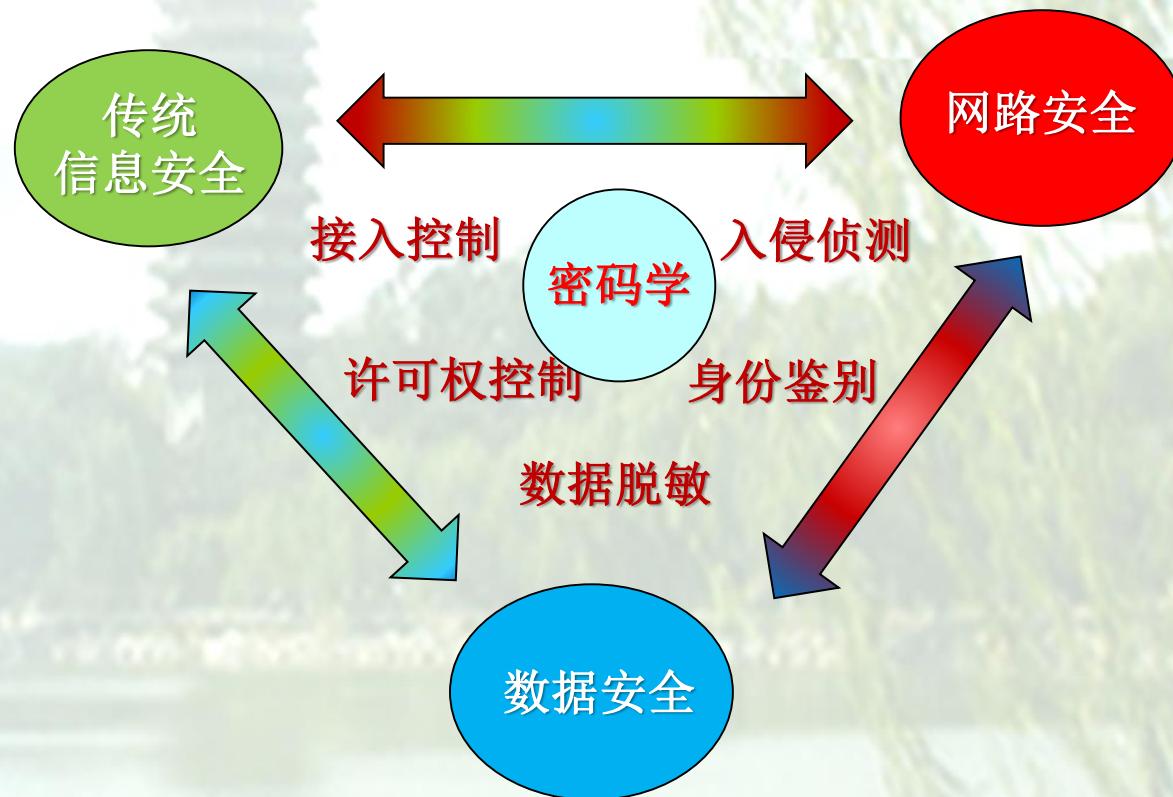


面对挑战



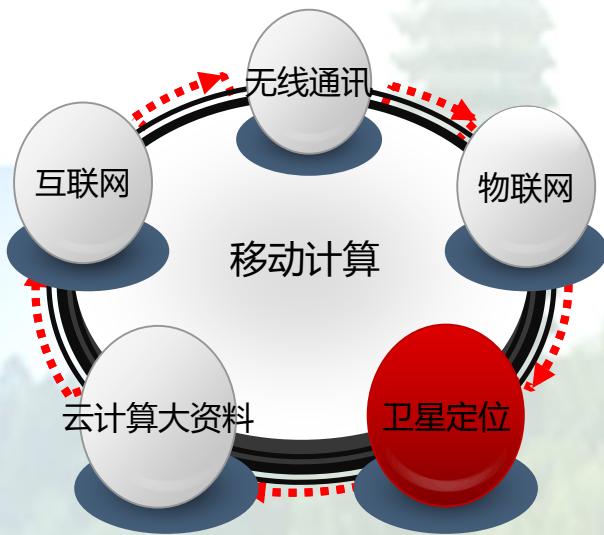
- 金融科技人才不足
- 协同模式不完善
- 核心技术缺乏
- 数据安全及隐私保护体系未健全

信息/网路/数据安全的共异性



保密性 完整性 可靠性 不可抵赖性 合法性 可用性 真实性 可控性 准确性

移动计算系统的隐私泄露与保护



基于位置服务 (LBS, Location-Based Services)

融合GPS定位、移动通信、导航等技术，提供与空间位置相关的综合信息，为使用者提供定位、追踪和敏感区域警告等服务。如Google地图，百度地图，通过位置服务提供者务、医疗、工作和生活的各种服务。

- iOS按照时间顺序记录使用者的位置座标信息
- Android提供位置服务的API，获取当前经纬度的信息，追踪设备的移动路线，或设定敏感区域特定警报信息

例：数据脱敏

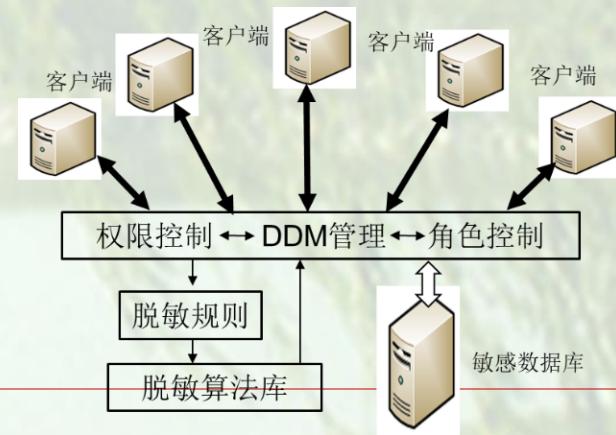
➤ 数据交互安全与脱敏技术

- 可逆脱敏（可恢复）：脱敏后的数据可还原成脱敏前的原数据
- 不可逆脱敏（不可恢复），脱敏后的数据不能还原成脱敏前的原数据

✓ 静态数据脱敏技术



✓ 动态数据脱敏技术



人工智能安全应用

口 人工智能创新性应用

数据分析、知识提取、自主学习、智慧决策、自动控制等能力，在网路防护、信息管理、信息审查、智慧安防、金融风控、舆情监测等网路信息安全和社会公共安全领域

✓ 网路防护

利用AI算法开展入侵侦测、恶意软体检测、态势感知、威胁预警等技术和产品研发

✓ 信息管理

利用AI技术实现对资料分级分类、防泄漏、泄露溯源等资料安全保护目标

✓ 信息审查

利用AI技术辅助人类对表现形式多样，数量庞大的网路不良内容进行快速审查

✓ 智能安防

利用AI技术推动安防领域从被动防御向主动判断、及时预警智能化

✓ 金融风控

利用AI技术提升信用评估、风险控制等效率和准确度，进行金融交易监管

✓ 舆情监测

利用AI技术加强国家网路舆情监控能力，提升社会治理能力，保障国家安全

金融科技智能安全

多模态/多因子信息的安全识别与鉴别



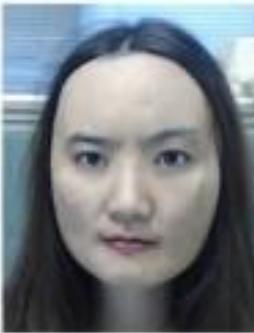
✓ Real Face



✗ Prints Attack



✗ Replay Attack



✗ 3D Mask Attack

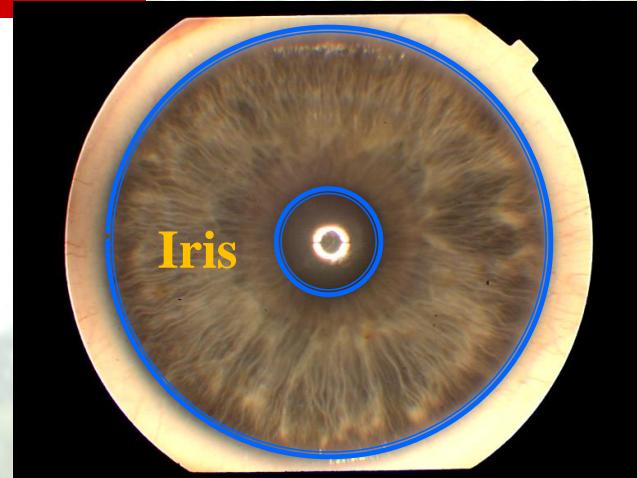
3D打印人脸套



多模态/多因子信息的安全识别与鉴别

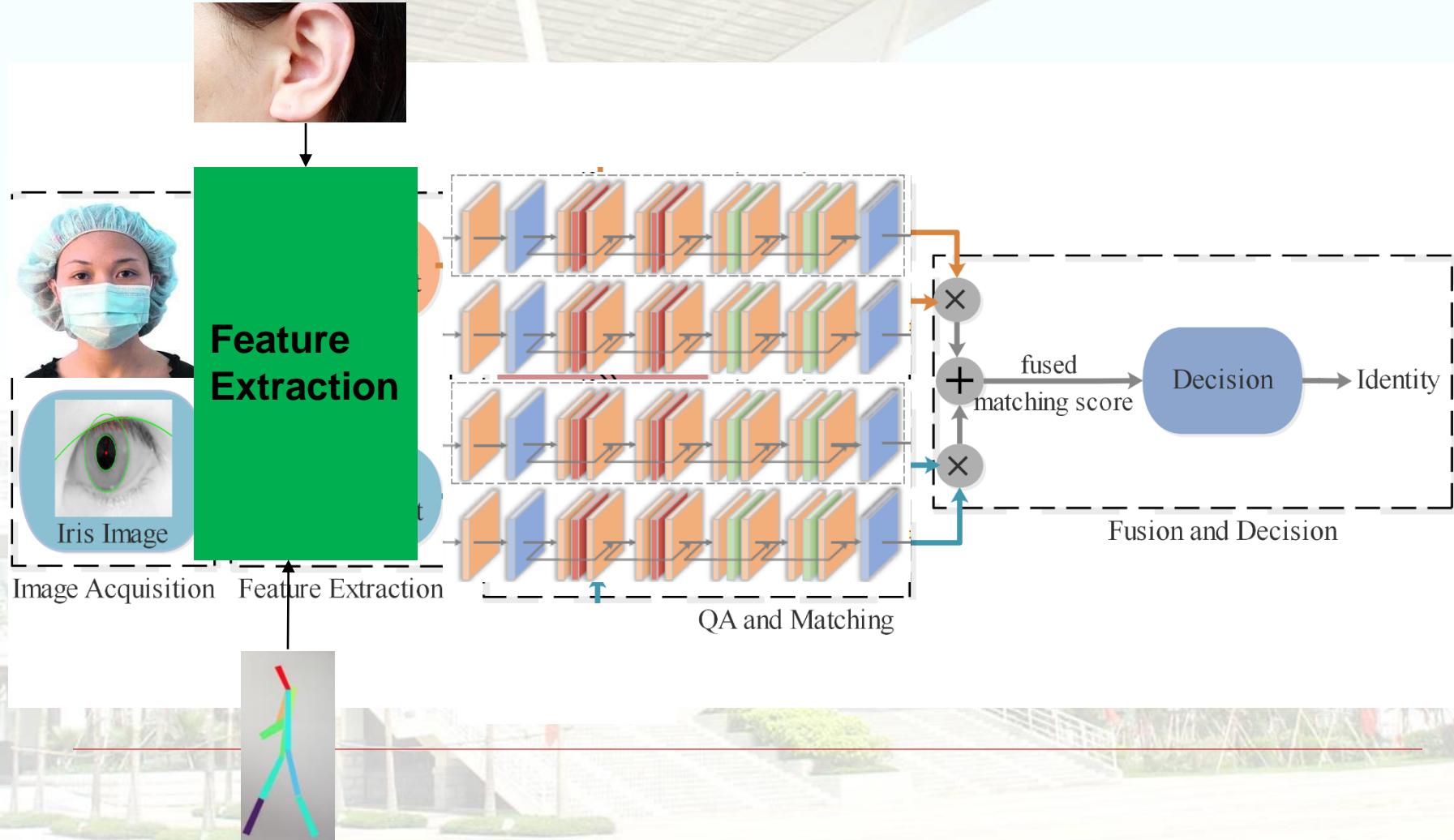


虹膜与人脸识别- 支付及信贷



疫情场景下的智能安全

虹膜/人脸/人耳/形态等特征融合安全识别与鉴别



虹膜与人脸融合安全识别与鉴别

A Robust Single-sensor Face and Iris Biometric Identification System based on Multimodal Feature Extraction Network

Zhengding Luo, Qinghua Gu, Yuesheng Zhu, Zhiqiang Bai
Communication and Information Security Lab
Shenzhen Graduate School, Peking University, China
Emails: {luozd, guqh, zhuy, baizq}@pku.edu.cn

Abstract—Joint face-iris identification can integrate complementary information from face and iris to fulfill the requirement of performance improvement and security. However, most of the current face-iris multimodal biometric systems acquire face and iris with different sensors which brings about the increase of capturing complexity and device cost. Besides, they are limited by the identification performance degradation under non-ideal scenarios. In order to address these problems, a robust single-sensor face and iris biometric identification system based on multimodal feature extraction (MFE) network is proposed. Only a single sensor is needed to obtain face and iris images in the proposed system, with the goal of improving recognition performance while minimizing sensor cost and acquisition time. The MFE network is designed as a general network module to extract both face and iris features and it is trained with a triplet framework to reduce intra-class variations and enlarge inter-class variations. Our experimental results on CASIA-v4-distance and FRGC v2.0 non-ideal datasets show that the proposed system achieves better identification performance in terms of Equal Error Rate (EER) and False Reject Rate (FRR), etc. compared with other unimodal and multimodal biometric systems.

Index Terms—multimodal biometrics, face and iris recognition, non-ideal biometrics, deep learning, a single sensor

I. INTRODUCTION

Traditional identification techniques include password-based schemes and token-based schemes. However, these schemes are vulnerable to attacks when the passwords are divulged or the tokens are stolen. Biometric recognition refers to automatic identification using certain physiological or behavioral traits associated with an individual. These biometric traits include face, fingerprint, iris, palmprint and voice, etc. which have an edge over traditional identification approaches because they cannot be stolen or shared [1]. But unimodal biometric systems are limited by some inherent drawbacks such as lack of uniqueness, restricted degrees of freedom, non-universality, sensitivity to noisy data, vulnerability to spoofing and unacceptable error rates [2]. Multimodal biometrics can fuse information from multiple modalities to overcome the limitations of single modality and enhance discriminant ability [3]. Apart from that, multi-biometric systems increase the resistance to spoofing attacks by making it difficult to spoof multiple modalities simultaneously [4].

Among biometric traits, face and iris have received significant attention because of many outstanding characteristics.

Face recognition is the most natural and acceptable way in biometric recognition, whereas photographs, videos, 3D masks and other spoofing ways make face recognition less reliable [5] [6]. Iris is one of the most promising biometric traits due to its unique textures, which is stable until the end of human life unless there are accidents [7]. Iris images are usually acquired within a short distance under near-infrared illumination [8]. However, iris recognition may suffer from identification performance degradation when image acquisition is not constrained strictly. Therefore, the pros and cons of face and iris can complement each other to enhance the overall recognition performance and security [9].

While research into face-iris multimodal biometrics has achieved a large increase over recent years, many related experiments are based on **chimeric datasets** (i.e. face modality and paired iris modality come from different users) due to a lack of available **real-user datasets** (i.e. face modality and corresponding iris modality come from the same person) [10]. The independent acquisition of each modality from different sensors may increase sensor cost, data acquisition time and the risk of spoofing in chimeric datasets. It is much more desirable to acquire multiple modalities from a single sensor for security and usability reasons in practice [11], [12]. In addition, since iris images can be extracted from face images without incurring additional hardware cost as shown in Fig. 1, it is economical and convenient to obtain face and iris samples using a single sensor device.

It is common and unavoidable to deal with some noisy factors such as off-angles, reflections, illumination changes and blurred images under less-constrained or non-ideal scenarios. These noisy factors result in the recognition performance drop and lack of security in face-iris multimodal biometric systems. Therefore, development of a robust face-iris multimodal biometric system is highly desirable. The key contributions of this paper are summarized as follows: (1) We propose a face-iris multimodal biometric system combining information from face and iris to enhance the limited discriminant ability of unimodal biometrics. Besides, the proposed system exhibits superior robustness under non-cooperative environments. (2) A **multimodal feature extraction (MFE) network** is developed to extract face and iris features in our system. The MFE network is a modality-general network and it is trained with a triplet

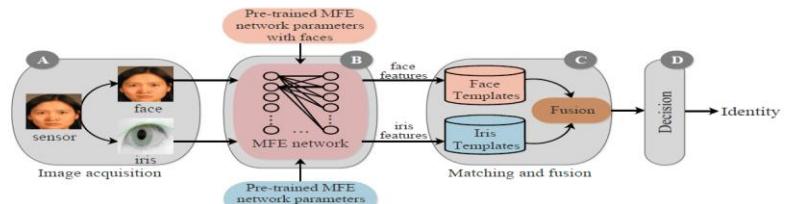


Fig. 2. Diagram of the proposed system consisting of four modules. (A) Image acquisition: face and iris are obtained by a single sensor. (B) Feature extraction: a general MFE network module used for face and iris feature extraction with pre-trained parameters. (C) Matching and fusion: generation of matching scores and face-iris fusion at score level. (D) Decision: identity determination by comparing the fused score with a threshold value.

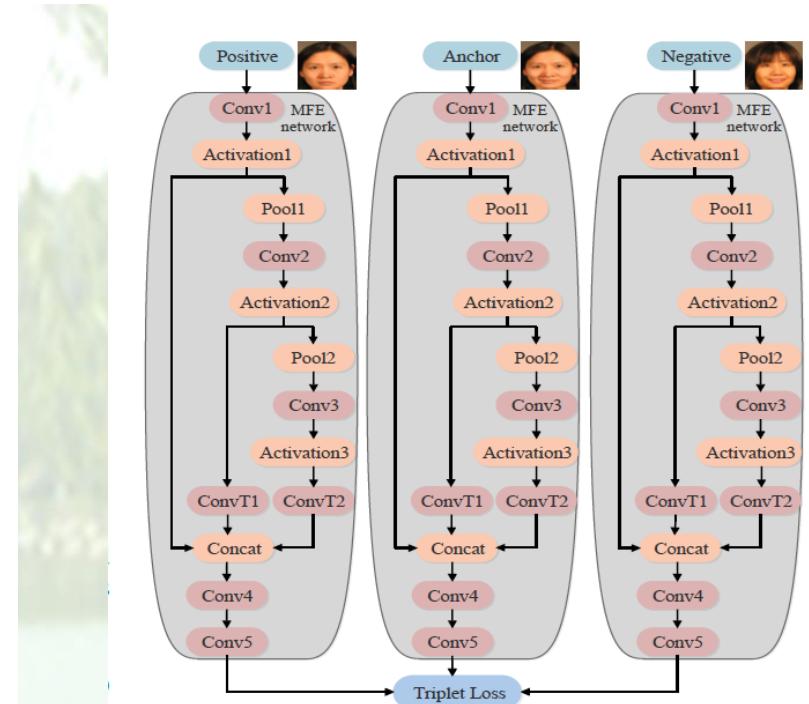


Fig. 3. Triplet training architecture for the MFE network. Positive, anchor and negative represent the input of three identical MFE networks which share the same parameters during training. The structure aims to reduce the distance of genuine pairs (positive-anchor) and enlarge the distance of imposter pairs (anchor-negative). The MFE network trained with this scheme can achieve a more distinct separation between intra-class and inter-class distribution.

面向金融科技应用应用场景的智能分析处理

□ 手写字和数学公式的智能检测与识别（OCR + AI）

对图片中的字母、手写字、表格、数学公式等字符进行智能检测和识别

