

区块链金融应用研究与实践



中国银联
China UnionPay

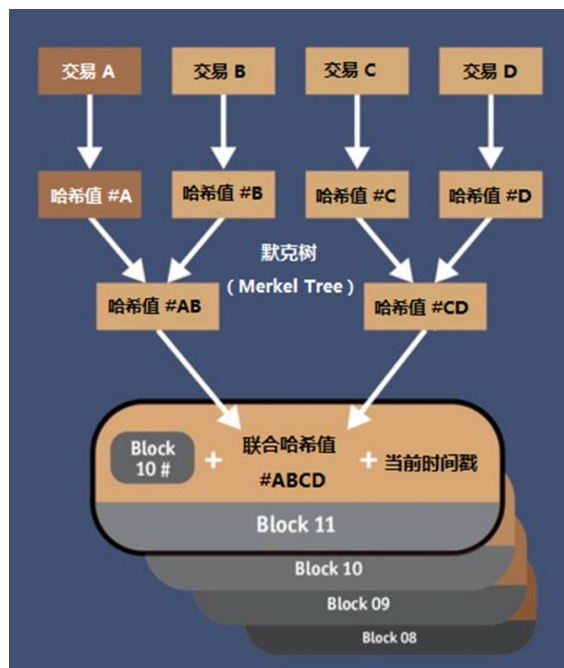
1 区块链概述

2 区块链金融应用实践

区块链与数字货币的关系

2008年中本聪在论文“比特币：一种点对点的电子支付系统”中正式提出，是基于密码学椭圆曲线数字签名算法（ECDSA）和SHA256摘要算法来实现的去中心化的点对点分布式共享账本。

1. 区块链是实现加密数字货币的可选技术方案之一，但加密数字货币并不一定采用区块链技术！
2. 比特币底层区块链技术有较高技术参考价值。



比特币

- ✓ 非央行统一发行
- ✓ 匿名性不可控
- ✓ 交易性能差

人行、工信部、银监会、证监会、保监会

比特币不是由货币当局发行，不具有法偿性与强制性等货币属性，并不是真正意义的货币。

比特币是一种特定的虚拟商品，不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用。

银联对区块链的理解

区块链技术是一种使用多中心化共识机制，来维护的一个完整的、分布式的、不可篡改的账本数据库技术。

两种结构

- ❖ 链式账本结构：验证与存储数据
- ❖ P2P组网结构：异构多活网络

两种算法

- ❖ 共识算法：维护节点间数据一致性
- ❖ 密码算法：保证数据传输和访问安全

一个合约

- ❖ 智能合约：编程和操作数据

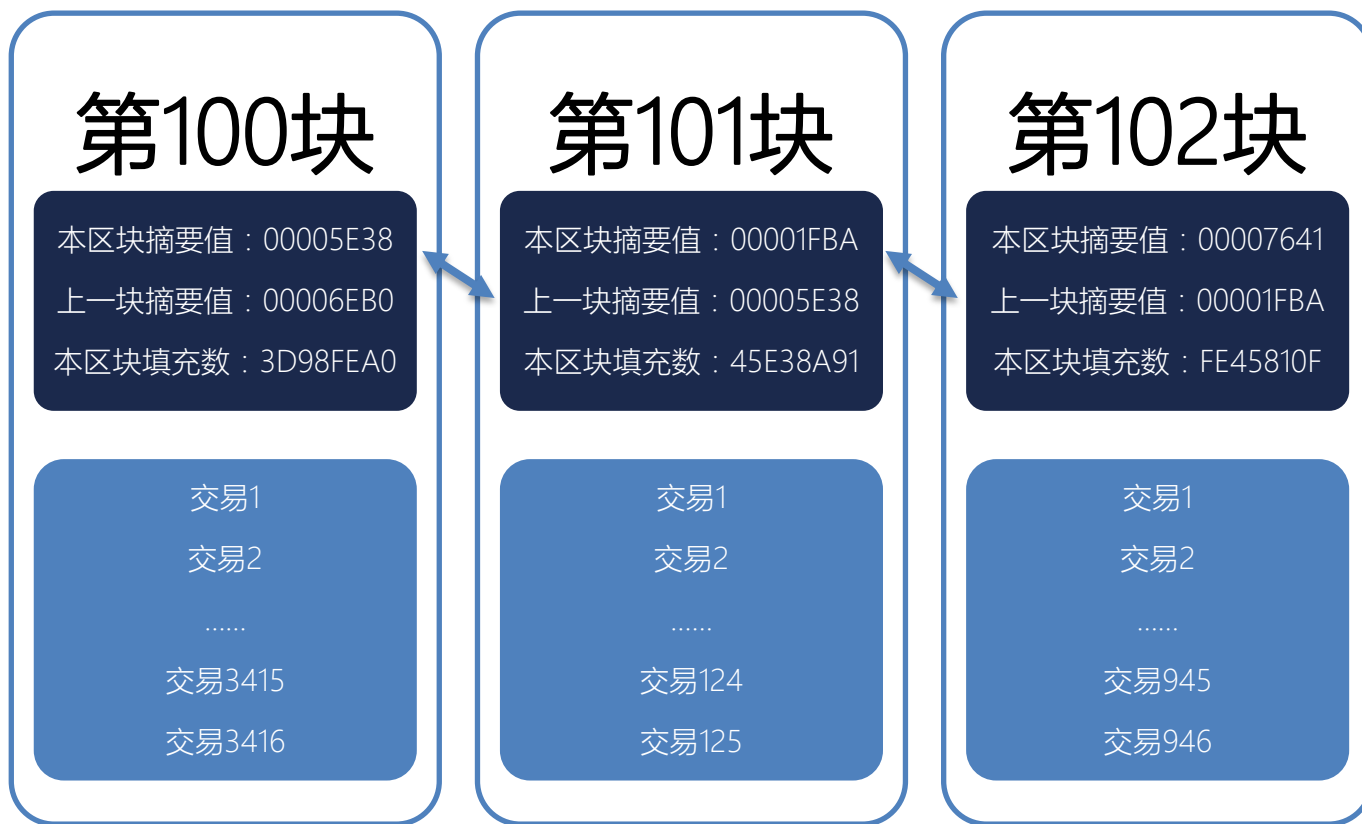
不可篡改性

集体维护性

开放性

区块链技术的链式账本结构

- ◆ 数据以区块文件形式保存
- ◆ 通过某种关联方式（比如说文件摘要）将前后区块连接起来



链式账本结构的价值

链式账本结构的比喻 – “中国字画收藏”

- ◆ 同一个字画家留存的作品通常并不多，无法抽出共性，因而无法辨识
- ◆ 收藏家会收集同时代的众多画家的作品，题字盖章，收藏家的题字和盖章可抽取共性，具备识别性
- ◆ 收藏家的题字和印章的辨识性反超字画本身，成为验真的重要判断手段



公有链、联盟链、私有链

公有链（无边界）：任何人都可以参与，容易部署应用程序，全球范围可以访问。

联盟链（有限跨主体）：有准入门槛，行业内不同主体间完成清算、结算等业务流程，可设定控制权限，具有较高的可扩展性。

私有链（主体内）：对企业、政府的内部审计与测试有用。

	公有链	联盟链	私有链
代表案例	比特币、以太坊	Fabric、Corda、EEA (以太坊联盟)	公有链、联盟链私有部署
准入控制	无	有	有
节点个数	几百到几千	4到几十	一般十个以下
交易速度	极其慢	略好	非常快
共识算法	PoW、PoS、 DPoS	拜占庭算法 (Raft、 Paxos、PBFT)	Ripple

区块链技术的应用场景概览

基于区块链的应用场景也是形形色色，层出不穷。



1 区块链概述

2 区块链金融应用实践

摩根士丹利的区块链预测曲线

2014-2016:区块链价值的评估阶段：

银行以及其他金融基础设施中介机构，共同探讨区块链的机会并评估其对于金融行业的价值。
期间，R3和Linux Hyperledger 基金会成立。

2016-2018: 原型验证 (POC) 阶段：

金融业用特定的资产/业务，如跨境汇款等进行区块链试点

2017-2020: 共享基础设施 (网络) 形成阶段：

POC原型得到验证，提供开放接口和账本API给外部用户。
通过人工的减少以及基础设施成本分摊降低成本。

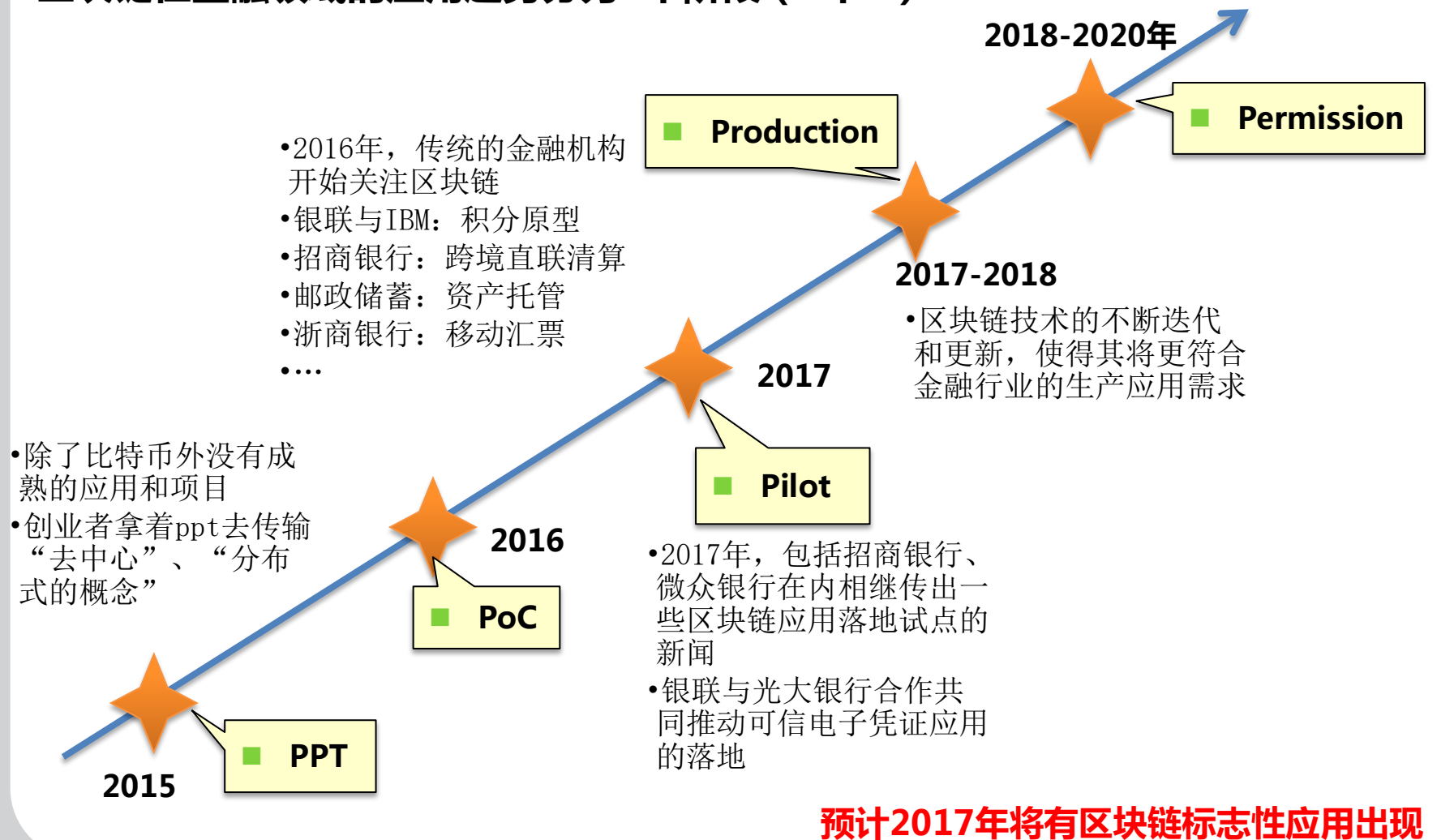
2021-2025:扩张阶段：

更多的金融资产/业务转移到区块链上。



区块链在金融领域的应用趋势

区块链在金融领域的应用趋势分为5个阶段（5个P）：



区块链在金融行业的机遇

区块链技术将在信用、价值流通、风控与监管方面，为金融服务提供更好的解决方案

金融业务核心

信用

区块链有数据防丢失和不可篡改的特性，非常适合于记录信用

价值流通

点对点组网交易，交易由整个网络确认，去除中介，加快流通

风控

共享账本，自主风控，风控信息源多

监管

监管方自主参与到网络中直接监管，无需依赖受监管机构开放度

区块链优势

区块链在金融行业的挑战

区块链技术在金融行业运用尚在早期阶段，并不成熟，需要在政府及产业界的协作支持下努力克服一系列技术、业务、应用场景、标准层面的挑战，方能实际发挥价值

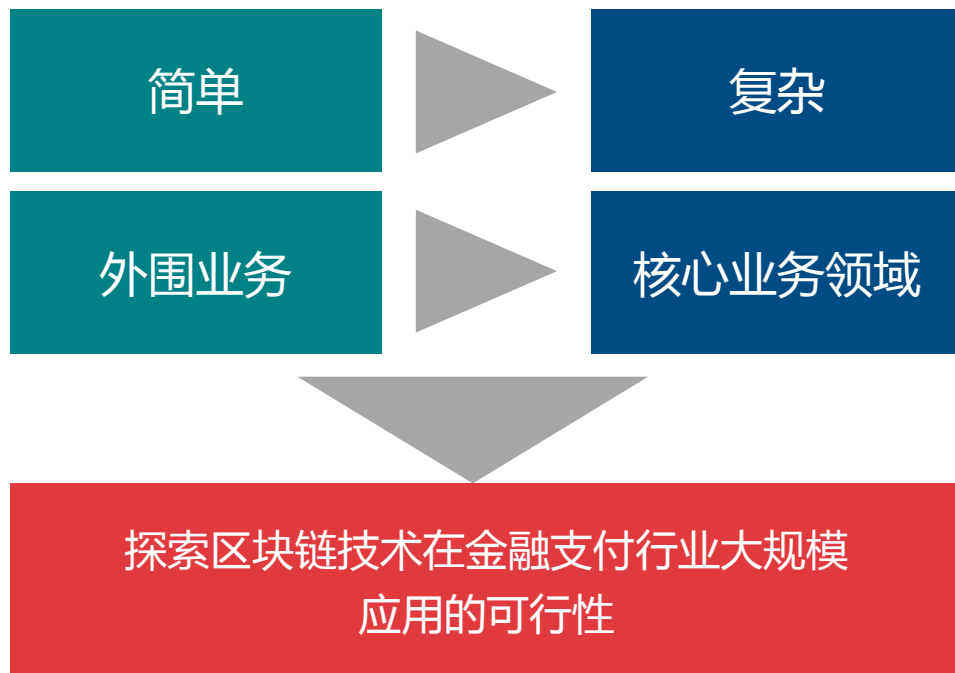


区块链技术与应用研究策略

区块链应用实践

目前，区块链潜在应用场景特点：

- 非实时性业务
- 轻量级信息存储
- 交易吞吐量较小
- 信息敏感度较低



区块链金融应用



基于区块链跨境汇款查询应用



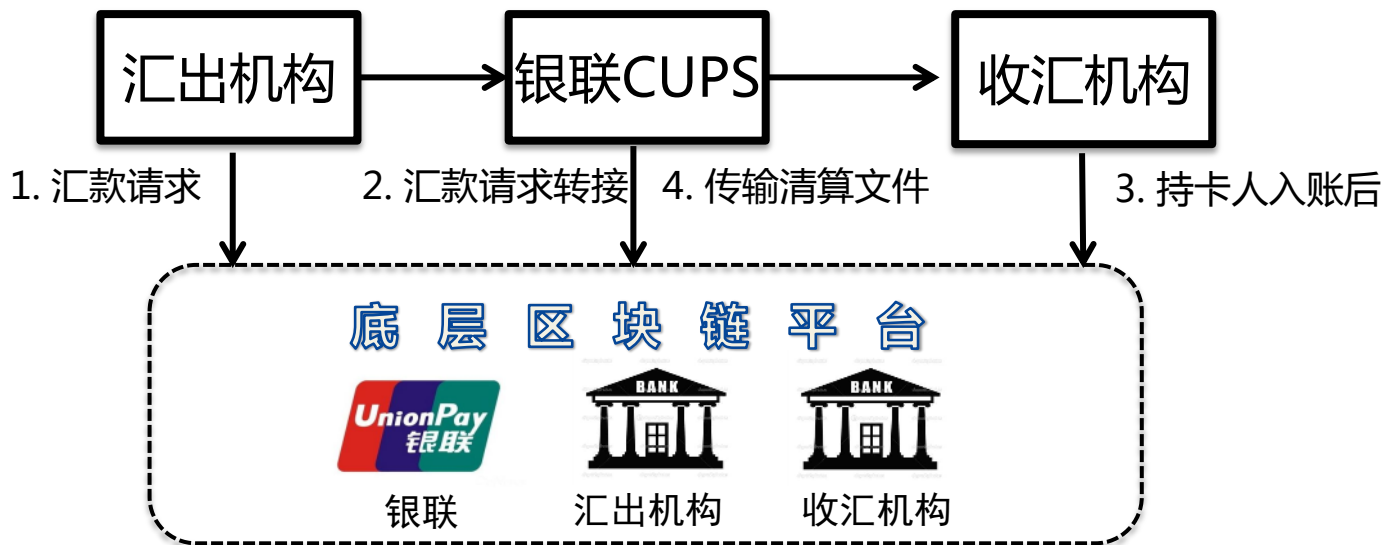
境外用户向境内银联卡持卡人汇款

痛点所在



汇出机构至汇入机构信息不对称

基于区块链的解决方案设计：



基于区块链的保单存证及理赔应用

痛点：传统的保单理赔从报价到投保申请、从承保到合规审核、从出单再到第一时间损失通知等等，每个环节都需要人工参与，导致流程复杂、耗时长，并且运营成本高昂。



数据存证

0x189414acac4b457ad40bc55f
6feeb1c735915a12



私钥签名

0xa563b9f7ba166e79ebae0f48
e5bea2324c421c7693b94cbc2
6eed839bef0f8f8

写入区块



数据存证

将航空意外险需要的文件（机票、个人身份信息、保单等）上传



自动理赔

理赔时基于预设条件进行资金划拨的行为，银联的贷记业务可作为自动理赔的支付通道



SMART CONTRACT



- 智能合约可以自动监测保单执行的情况，一旦触发理赔要求，无需投保人申请理赔，保额将自动赔付。
- 极大地提高客户满意度，减少保险公司的人力理赔成本。

区块链技术应用总结——可信区块链商业网络生态系统

金融服务

支付、普惠金融
对账、清算、结算
资产数字化
资产托管等

增值服务

银行卡积分服务
行业积分服务
电子凭证无纸化等

数据服务

数据确权
数据交易
数据真实性、可追溯等

供应链

电子信用证
应收账款
动产质押
电子票据等

...

应用场景



谢 谢 ！