



区块链与金融

张一锋 / 中钞区块链技术研究院

引子：电子支付的发展



金融的本质

中介

信用

区块链的概念

比特币的出现



2008年中本聪发布《Bitcoin: A Peer-to-Peer Electronic Cash System》

2009年1月3日创世区块诞生

2010年5月21日，第一笔交易达成

去中介 / 创建信任

区块链的概念

金融体系传统账本

银行A

账户	资产类型	金额
储户甲	人民币	3, 000
银行B	美元	2, 000, 000
银行C	人民币	5, 000, 000

银行B

账户	资产类型	金额
储户乙	人民币	1, 000
储户丙	人民币	70, 000
银行A	美元	2, 000, 000

银行C

账户	资产类型	金额
储户丁	人民币	2, 000
银行A	人民币	5, 000, 000

区块链概念

分布式统一账本？



登记机构	账户	资产类型	金额
银行A	储户甲	人民币	3,000
银行A	银行B	美元	2,000,000
银行A	银行C	人民币	5,000,000
银行B	储户乙	人民币	1,000
银行B	储户丙	人民币	1,000,000
银行C	储户丁	人民币	2,000,000



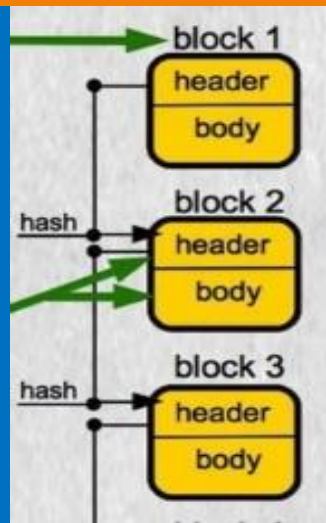
问题：

- ✓ 这个账本数据可靠吗？
- ✓ 谁来写账本？

区块链概念

链式数据结构

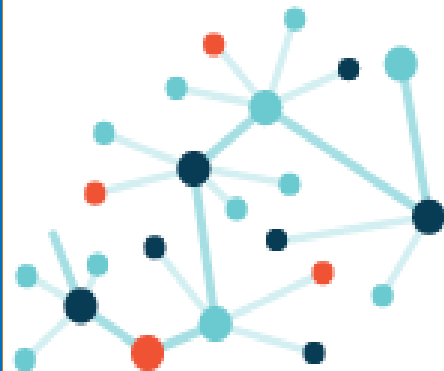
链式账本
与密码算法



区块链概念

共识机制

非中心化网络
与共识机制



区块链概念

一类采用多方共识机制来维护的完整的、不可篡改的非中心化数据库及分布式计算范式



区块链概念

区块链和智能合约



Actor



Value



Relation

区块链概念

区块链的新视角

一种人与人之间、组织与组织之间、物与物之间、甚至以上相互之间的新的协作关系



区块链的发展

区块链技术的史前期



密码学

1976年 赫尔曼的《密码学的新方向》
1977年 RSA算法（2002图灵奖）
1980年 Merkle树
1982年 拜占庭将军问题
1985年 椭圆曲线加密算法（ECC问世）



点对点传输

电骡网络，又称作为DHT (Distributed Hash Table)，分布式哈希表，标志成熟的点对点网络技术的问世。

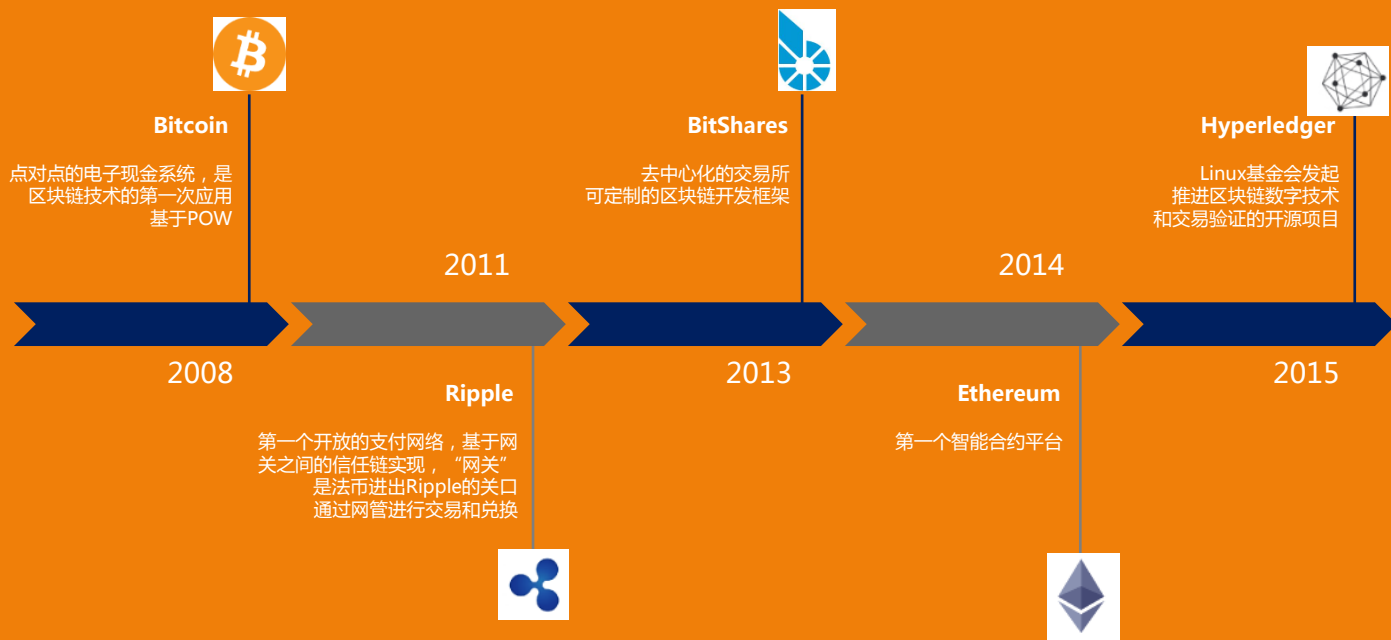
Hash Cash

双花问题

1997年 哈希现金（Hash Cash）算法机制问世。解决去中心化系统的双花。
2004年 “可复用的工作量验证”机制问世。成为比特币POW机制的前身

区块链的发展

区块链发展历程



区块链的金融应用

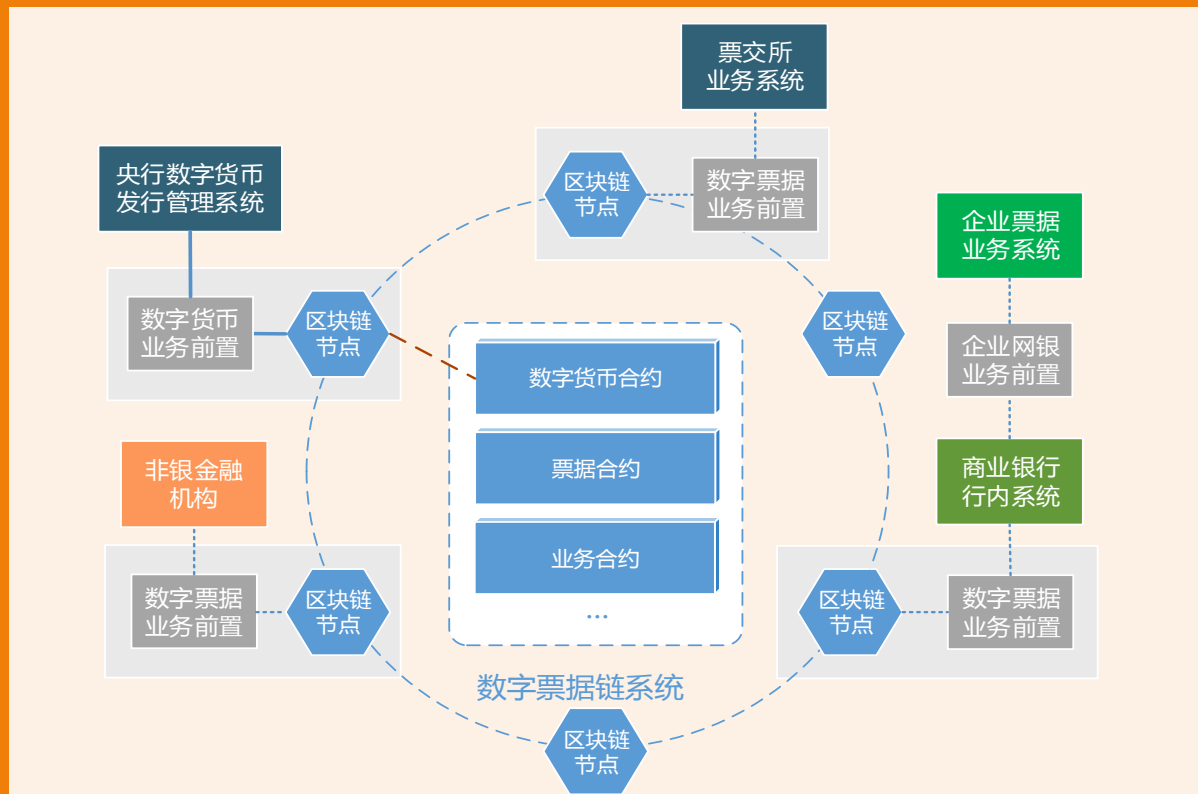


案例分析-数字票据

银行承兑汇票		2	BB 01
出票日期 贰零零捌 年 捌 月 贰拾壹 日			
出票人全称 中国 鲁国河南有限公司	收款人 全称 深圳市 电子科技有限公司		
出票人账号 170200170101016888	账号 4430 6636 4018		
付款行全称 工行	开户银行 工行深圳分行		
出票金额 人民币 伍拾伍万 元 正	亿 千 百 十 万 千 百 十 元 角 分		
汇票到期日 贰零零捌 年 壹 月 贰 拾 壹 日	付 行 号		
承兑协议编号 2008-071-10	付 行 地 址		
本汇票请行承兑，到期无条件付款。		本汇票已承兑，到期无条件付款。	
财务专用章		承兑行章	
出票人签章		承兑日期 年 月 日	
备注：		复核 记账	



数字票据-架构



数字票据-DVP

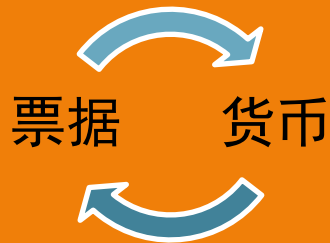
非DVP

传统中心化系统各自独立
交易后，再通过对账完成
最终交易



DVP

区块链使用统一账本，直接
锁定交易资源，不依赖外部
系统，确保交易的原子性



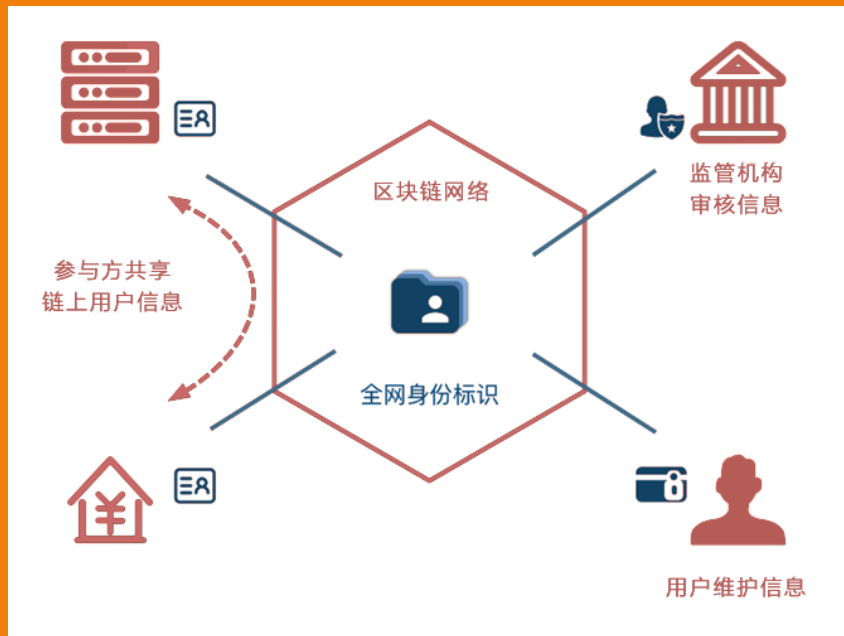
数字票据-交易所

- 不再需要一个中央对手方
- 任何两个节点之间，可以直接进行交易



数字票据-KYC

- 通过全局KYC能力，避免了大量重复认证、验证的社会资源浪费，同时提高了诚信信息的透明度，可以帮助用户降低改变服务商时的成本



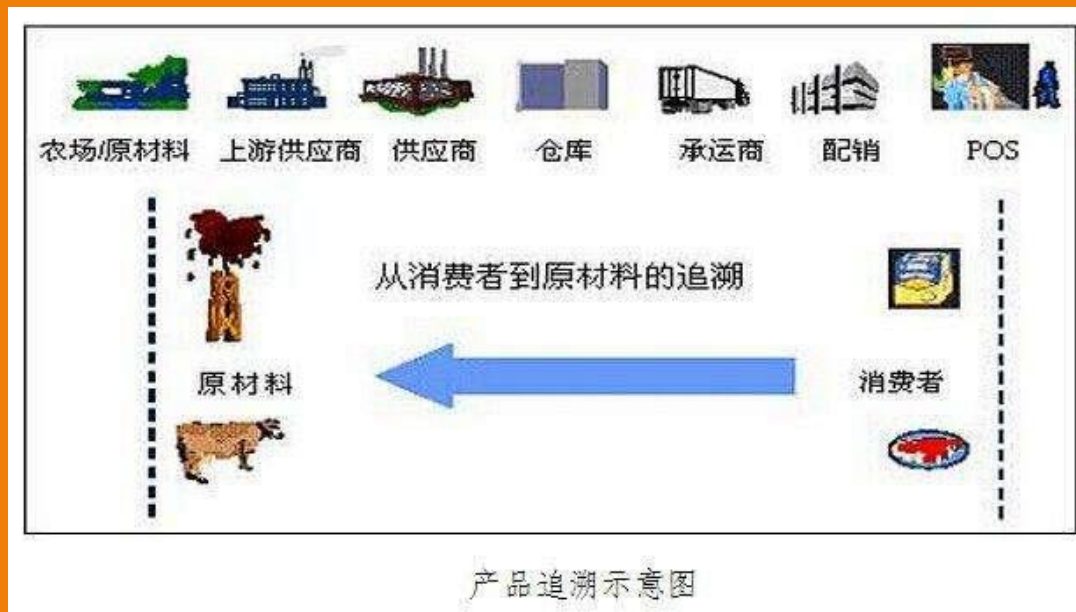
公益基金



资金清算



供应链溯源



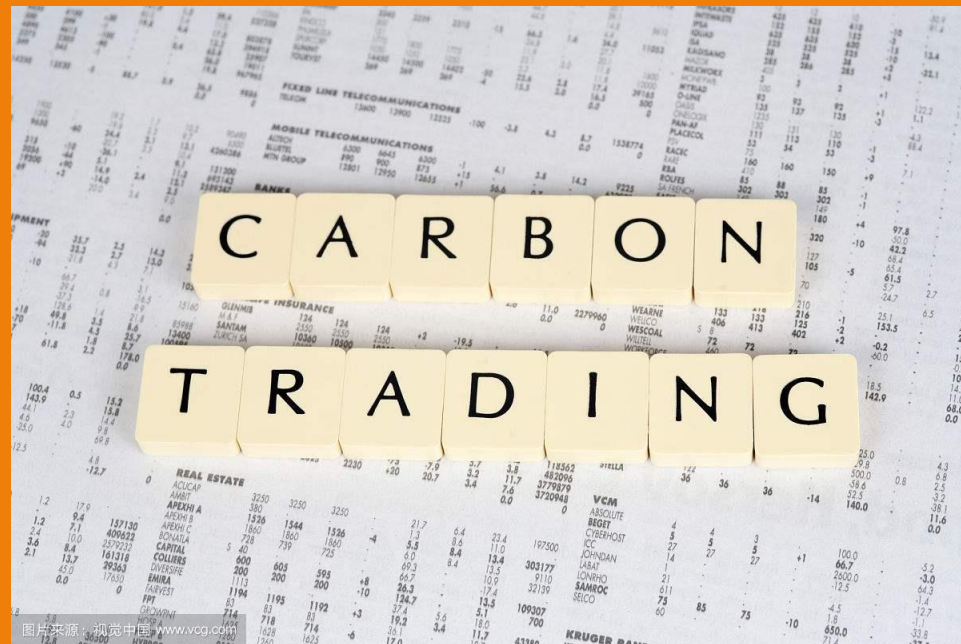
跨境支付



数字门票



分布式交易所



图片来源：视觉中国



P2P监管



区块链是一个复杂的概念

**The first five times you think
you understand it, you don't.**

—— Dan Kaminsky