区块链 + 智能合约

华中科技大学软件学院

郑嘉文 - 2021

什么是区块链?

数据库？去中心化分布式账本？数字货币？

定义

区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。基于时间戳的链式区块结构、分布式节点的共识机制、基于共识机制的激励机制和灵活可编程的智能合约是区块链技术最具代表性的创新点。

广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

去中心化（De-centralization）

区块链是由众多节点组成一个对等点对点（Peer-to-Peer，P2P）的网络，不存在中心化的设备和管理机构，任一节点加入，退出都不会影响系统整体的运作

去信任（Trustless）

区块链是建立在无信任的环境里的：节点可能速度慢，可能作恶，可能关机；网络可能堵塞，可能传输慢等。系统中所有节点之间通过数字签名技术进行验证，无需信任也可以进行交易。

可靠数据库 (Reliable Database)

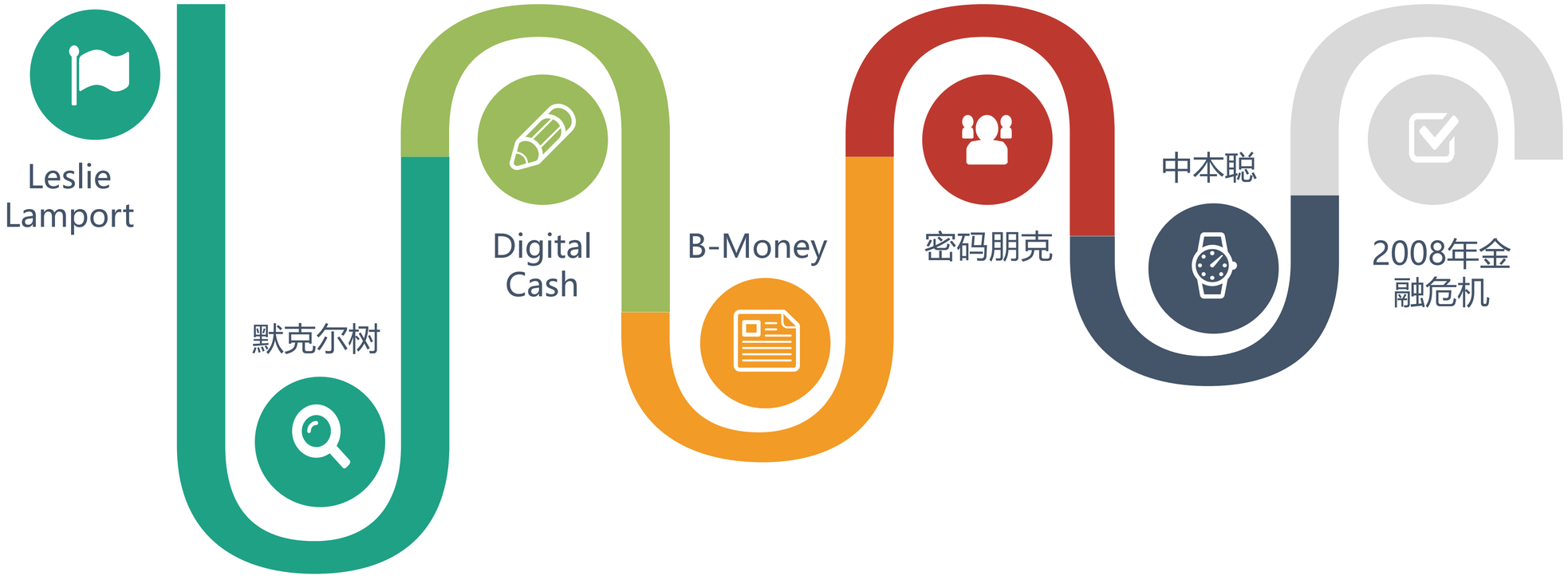
系统中每一个节点都拥有最新的完整数据库拷贝，单个甚至多个节点对数据库的修改无法影响其他节点的数据库，。

集体维护

多方存储。系统是由其中所有具有维护功能的节点共同维护的，系统中所有节点共同参与维护账本的工作。每个节点都是一个基于账本的会计系统，记录了网络上所有的交易信息。账本是不可篡改的，只能追加。

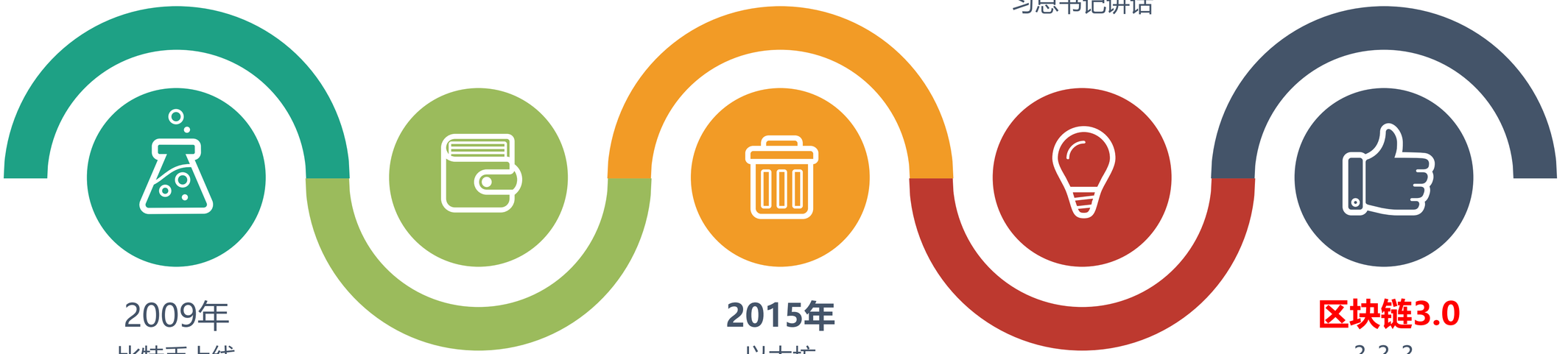
区块链历史

技术的孕育和发展阶段的重要的人和事



区块链历史

发展阶段及展望



区块链分类

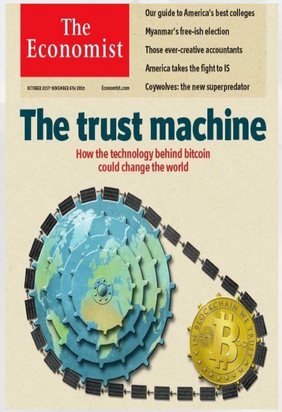
访问方式，关系

项目名称	描述	信任范围	共识速度	场景
公有链	任何人都可以参与，或者离开	任何人	慢	公开的去中心化应用
联盟链	由符合资格审查的节点控制	联盟内部	较快	产业联盟
私有链	由某个组织或者机构控制	组织内部	快	公司或者机构内部

按照链和链之间的关系，还可分为： 主链，子链，侧链

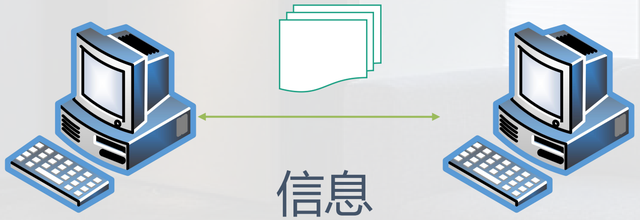
区块链解决的问题

信任



2015年10月美国著名杂志《经济学人》以封面文章发表《信任的机器》(The Promise of the blockchain: The trust machine，强调区块链是一种可以在无第三方监督的状态下建立彼此信任的技术手段，从而可作为第二代互联网“价值互联网”的基础协议。

区块链可以被视为是低成本的信任机器，是在信息不对称，不完全的环境下，在完全不信任节点间建立信任机制的技术。是价值网络，是传递价值的互联网（Internet Of Value, IOV)



信息

互联网在节点间传递信息

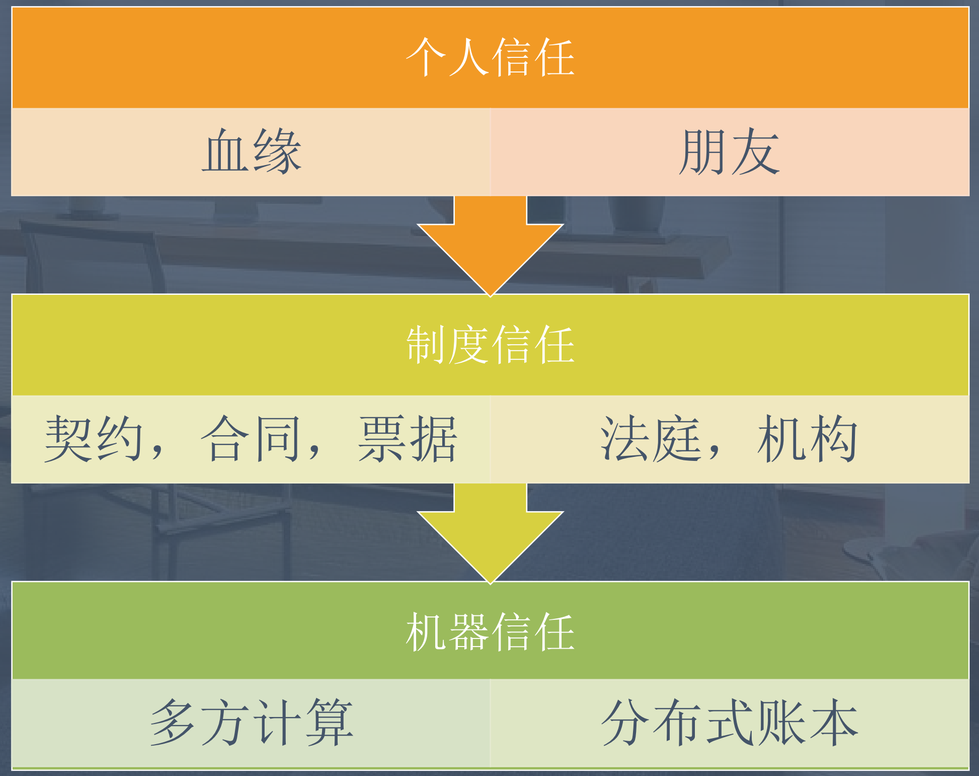
信任

区块链交换的是价值，是价值网络，是在不信任节点间建立信任关系，传递的是信任。是信任机器

互联网在节点间传递信息

缺乏信任而产生的怪象

押金，质押，帐期对账，书面合同，公证...



区块链技术概述

区块链技术是一个涉及多学科，多领域的技术家族

学科名	技术示例
计算机分布式系统共识	PoW， PoS， Paxos …
计算机网络	P2P，Kademlia， Gossip…
计算机密码	对称加密，不对称加密，哈希函数，默克尔树 …
计算机容错	拜占庭容错…
图论	有向无环图（DAG）…
博弈论	纳什均衡，囚徒困境…
社会学	公地悲剧，帕累托改进…
经济学	激励模型，经济模型…
概率论	奥卡姆剃刀…

区块链技术不是一个单项技术的创新，而是已有的多学科技术交叉混合的集成式创新

区块链技术应用

大范围应用的，比较成熟的领域

去中心化身份

学生证，医师证，身份证...

存证确权

电子合同，电子证据，电子处方...

溯源

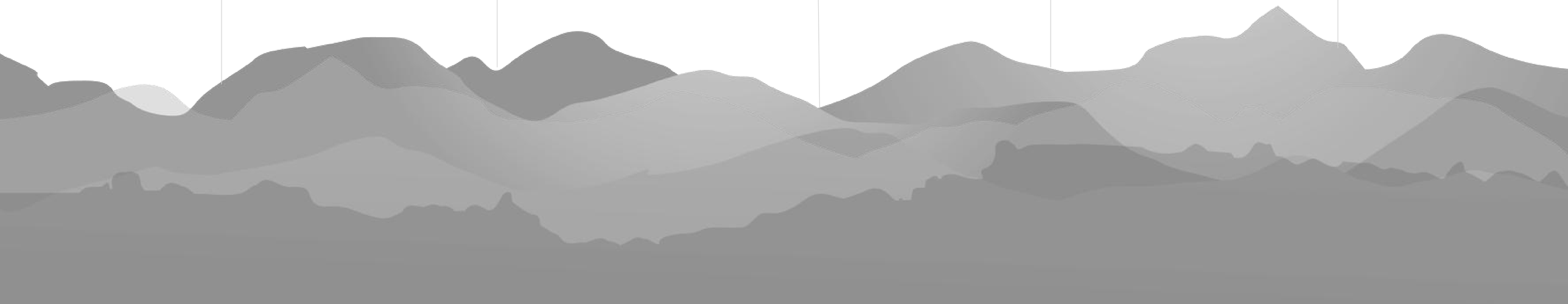
版权保护，产品防伪...

支付

支付，转账，兑换...

金融

借贷，DEFI...



区块链技术应用

正在探索将区块链应用于各行各业的“区块链+”模式

区块链+能源

通过区块链，将能源进行编码，并合理分配，保证所有的能源都实现有效利用和价值最大化

区块链+教育

区块链技术可以加强全球教育机构的数字版权保护、教学服务增值，大幅提升教育资产在链上交易流通性能

区块链+艺术

通过区块链技术能很好的记录商品的生长过程，流转运输过程，解决农产品安全问题

区块链+农业

通过区块链技术能很好的记录商品的生长过程，流转运输过程，解决农产品安全问题

区块链+医疗

解决在医疗行业存在的医疗信息不互通、医疗资源分布不均衡、医疗需求不能满足等问题

链改 就是对现有的商业模式，通过应用区块链技术进行改造，以改进生产关系，提高协作效率

币改 就是对现有的业务加入通证机制，起到激励，加速流通的作用

区块链技术面临的挑战

区块链技术目前还处在襁褓期

量子攻击

区块链的加密算法能否经受量子计算机攻击?

交易效率

目前公链的TPS普遍不足，如何提高区块链的效率?

智能合约

如何应对智能合约的漏洞问题?

法律法规

国家监管政策法规不清晰，不明朗。而且国家间，政府间政策都不一致

既见君子，云胡不喜

电话 **13240946967**
邮箱 zy731@hotmail.com
微信 **gavinzheng731**
博客**https://my.oschina.net/gavinzheng731/**

谢谢聆听

Q&A

郑嘉文