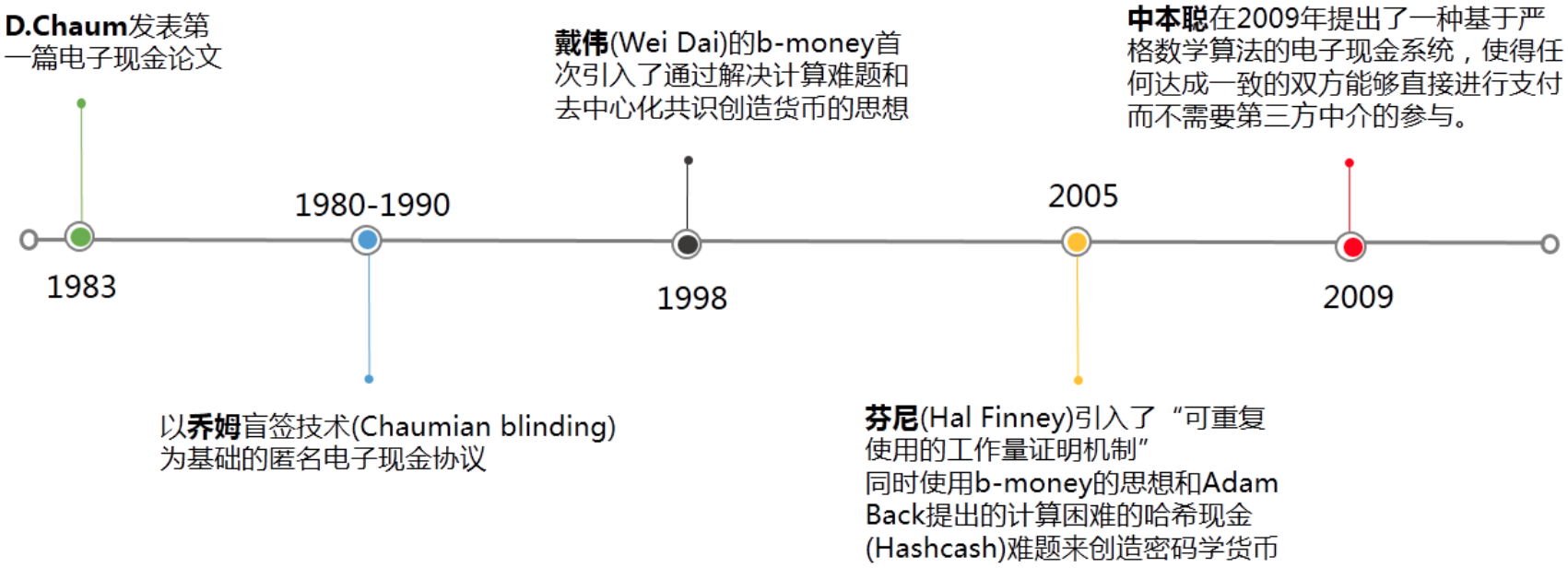
日知录 | IT大咖说 不止于技术

区块链技术对互联网基础技术的颠覆性冲击

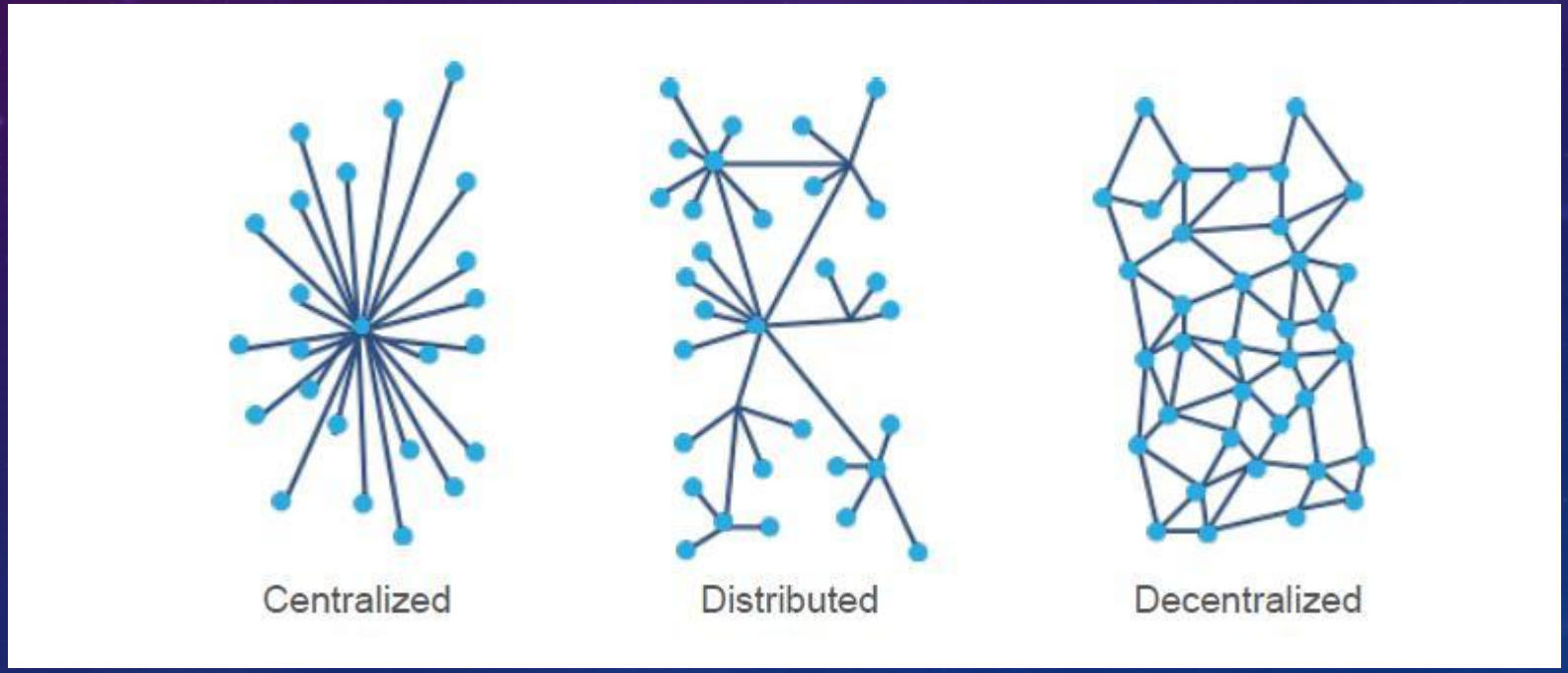
创始人：黄立峰

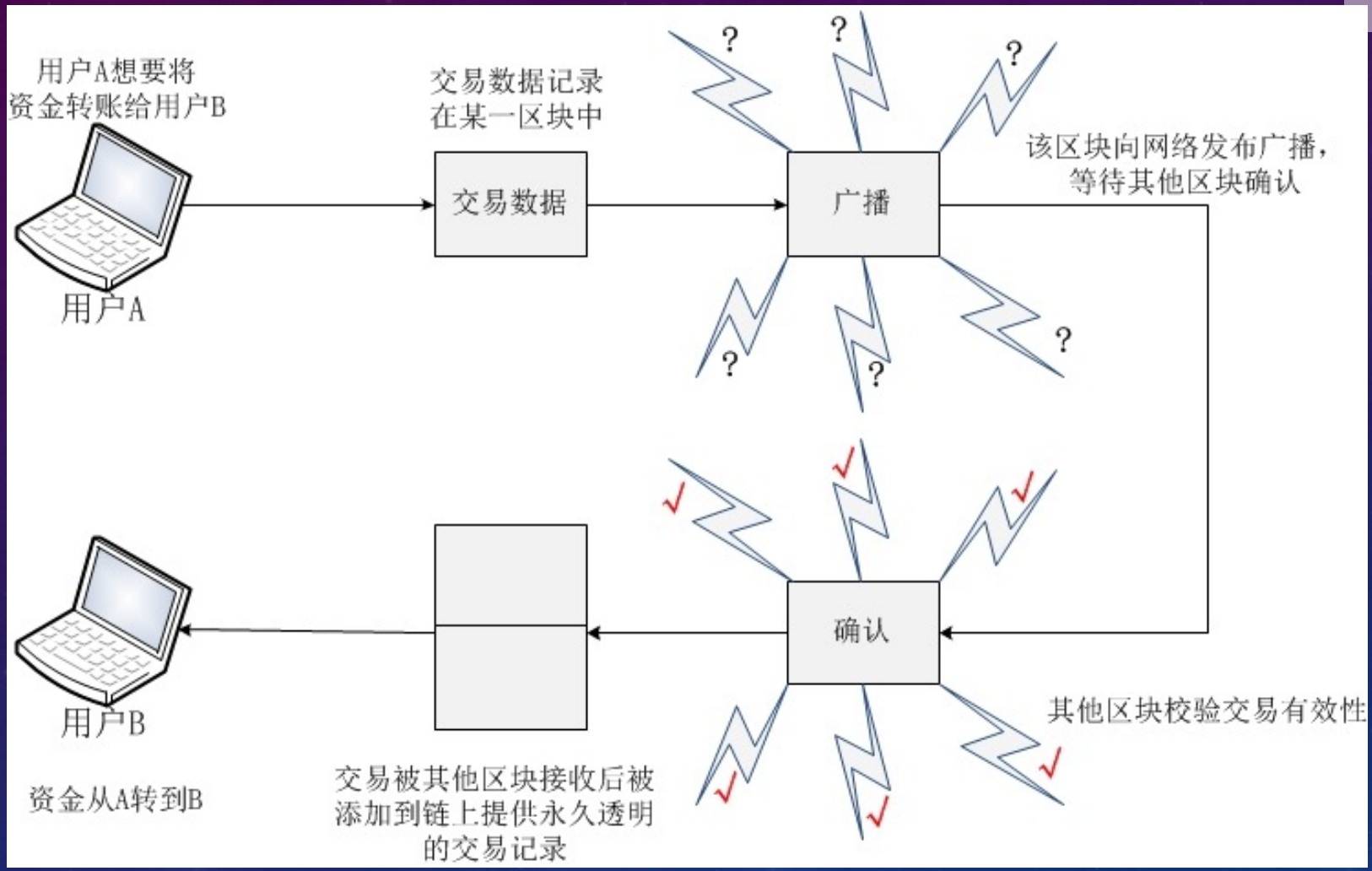
魔镜科技

区块链的起源


D.Chaum发表第一篇电子现金论文
1983
1980-1990
以**乔姆**盲签技术(Chaumian blinding)为基础的匿名电子现金协议
戴伟(Wei Dai)的b-money首次引入了通过解决计算难题和去中心化共识创造货币的思想
1998
2005
芬尼(Hal Finney)引入了“可重复使用的工作量证明机制”同时使用b-money的思想和Adam Back提出的计算困难的哈希现金(Hashcash)难题来创造密码学货币
中本聪在2009年提出了一种基于严格数学算法的电子现金系统，使得任何达成一致的双方能够直接进行支付，而不需要第三方中介的参与。
2009

区块链的去中心化




用户A想要将
资金转账给用户B
用户A
交易数据记录
在某一区块中
交易数据
广播
该区块向网络发布广播，
等待其他区块确认
确认
其他区块校验交易有效性
用户B
资金从A转到B
交易被其他区块接收后被
添加到链上提供永久透明
的交易记录

区块数据结构

	名称	用途	大小
	神奇数	神奇数总等于0XD9B4BEF9,作为区块之间的分隔符	4字节
	区块大小	记录当前区块的大小	4字节
区块头	版本号	数据区块的版本号，用于跟踪软件/协议的更新	4字节
区块头	父区块Hash值	引用区块链中父区块的hash值	32字节
区块头	Merkel根	该区块中交易的merkel树根的hash值	32字节
区块头	时间戳	从1970年1月1日起的秒数	4字节
区块头	难度目标	该区块工作量证明的难度目标，用于矿工的工作量证明	4字节
区块头	随机数	当前区块工作量证明的参数	4字节
	交易计数	当前区块所记录的交易数	1-9字节
	交易详情	记录当前区块保存的所有交易细节	可变长

一句话介绍区块链

- 比特币背后的核心技术
- 分布式账本技术
- 可以扩展到整个互联网范围的分布式账本技术

区块链技术的构成基石

- 三大基石：p2p网络、密码学、共识算法
- 其他：嵌入式数据库、merkle tree、gossip协议

思维模式的比较

- 银行的思维模式：封闭、保守
- 区块链的思维模式：开放、透明

现有互联网有啥问题？

1. 数字化内容容易被篡改
2. 数字化内容容易被复制或窃取
3. DDoS攻击是顽疾
4. 对隐私的严重侵犯
5. 落后的安全模型：防火墙、堡垒式防御
6. 高可靠性、高可扩展性不足
7. 缺乏更加便捷的支付手段，众多互联网产业缺乏盈利途径

区块链的技术特性

- 不可篡改
- 数据共同管理
- 无中心或弱中心、自证其信

区块链的商业特性

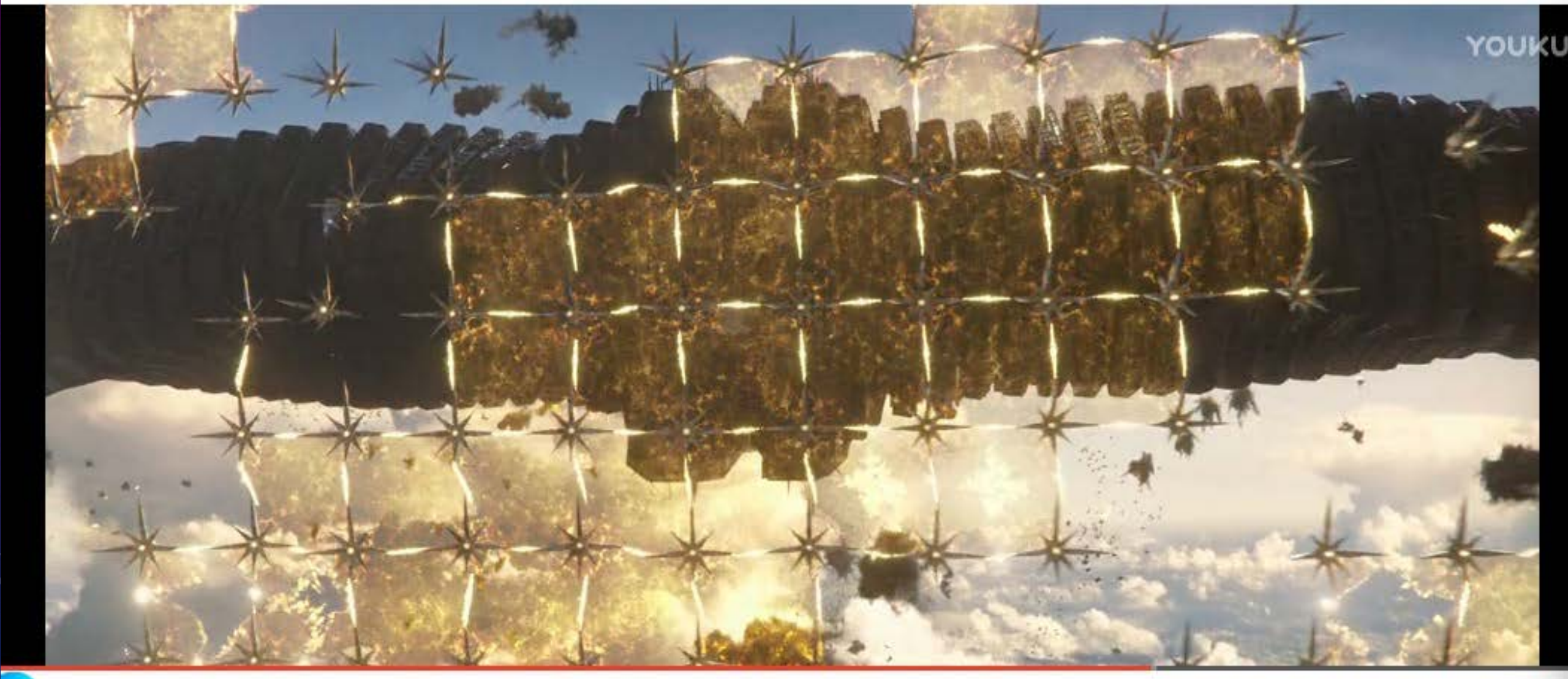
- 构建信用、信任的基石
- 去中心、去中介，自证其信
- 构建银行的It基础设施
- 数字资产的确权
- 隐私保护的曙光
- 安全模型的变迁

安全模型的变迁

- 大公司的要塞防御
- 谷歌的no trust模型

单点防御

网状防御



现有区块链技术的不足

- 并发性不足
- 延时长
- 隐私保护不足
- 浪费能源
- 公平与效率的平衡

区块链与人工智能的关系

- 区块链就是用机器来决定钱的归属，其意义远大于机器赢了一盘棋重要的多
- 不可篡改性是防止AI越界的最根本条件

信鏈

- 区块链BAAS(Block Chain As Service)平台
- 创新的共识算法：对用户贡献的存储和带宽进行激励
- 解决现有区块链技术面临的各种问题
- Slogan：用区块链连接全世界，保护每个人的数据所有权

个人自我介绍

- 15年It工作经验，技术极客，善于思考（技术与哲学结合）
- 整个职业生涯就是在为区块链做准备：华为、快播、人脸支付
- 区块链大学：区块链技术社区（qkldx.net）
- 微信：18612986682，网名：飞骐

- Thanks

飞骐

北京 海淀

日知录 | IT大咖说 不止于技术