CCTC 2017 中国云计算技术大会
Cloud Computing Technology Conference 2017
CSDN

区块链技术回顾与展望

王玮

上海乐住信息技术有限公司 CTO

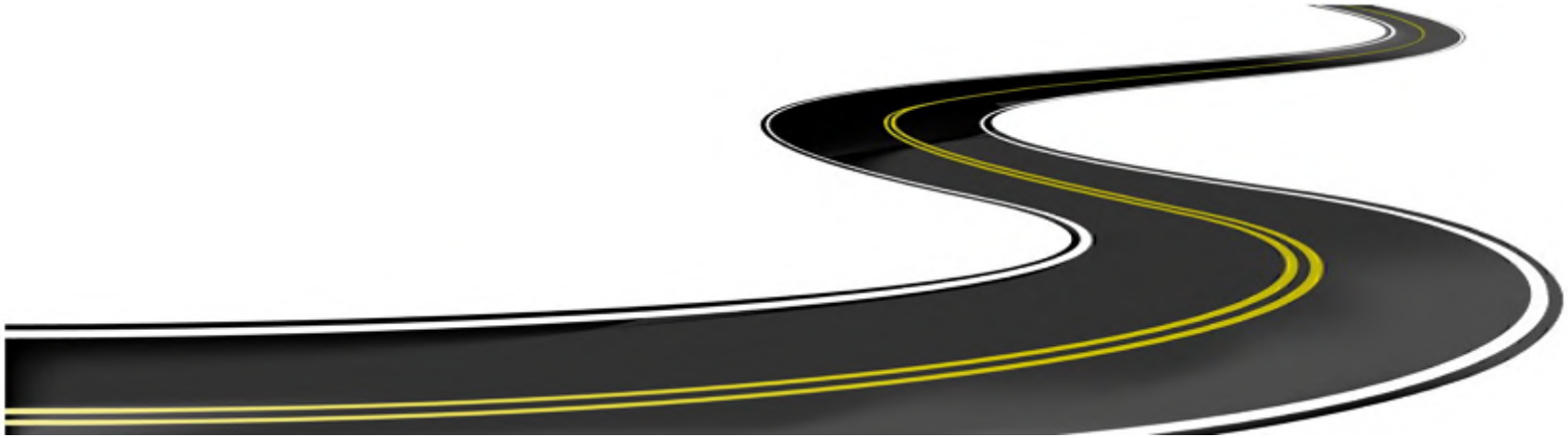
2017.5

史前纪事
区块链前传

中本魔咒
比特币横空出世

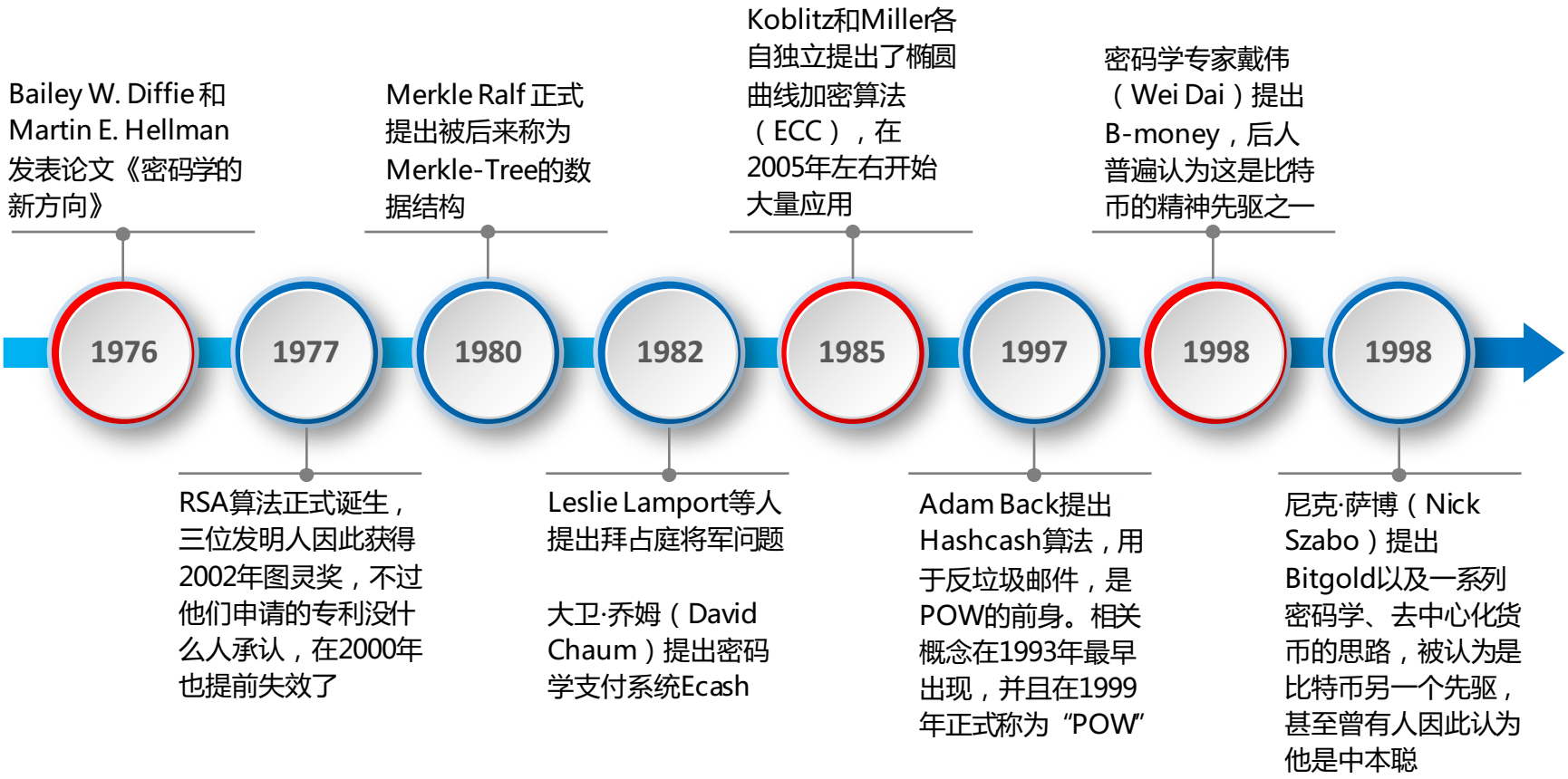
以太野望
“2.0”的雄心壮志

沧海横流
区块链大航海时代



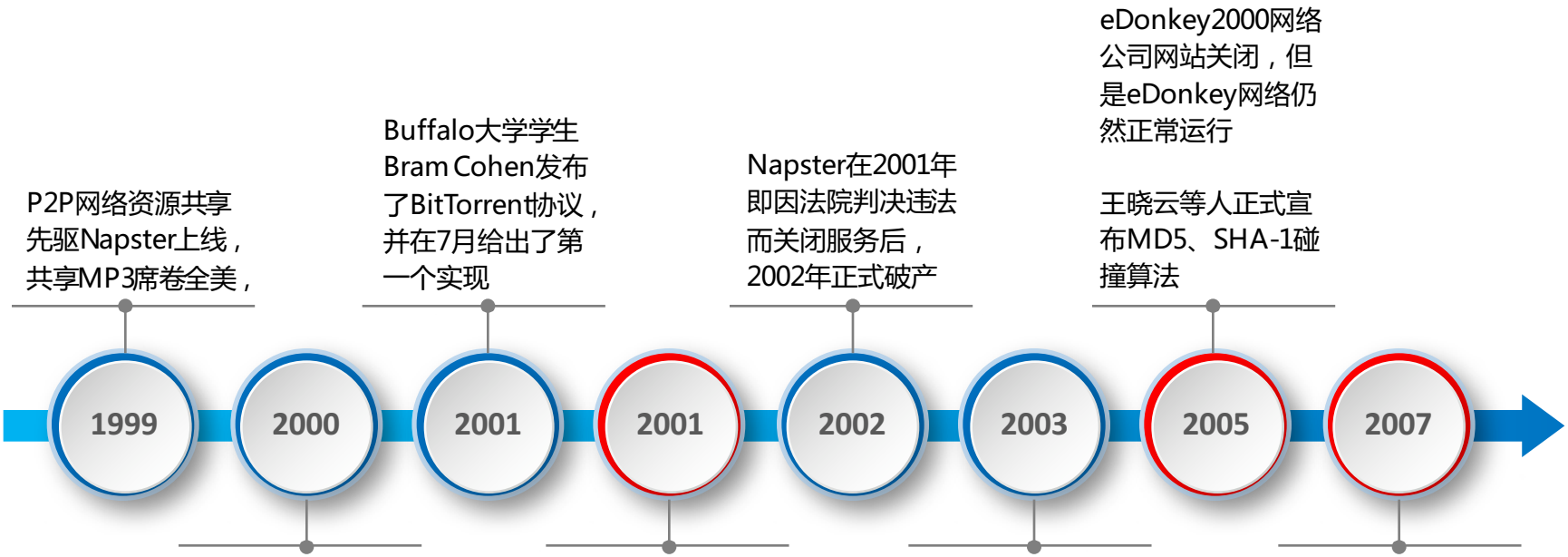
我们必须知道　　我们必将知道

史前纪事



哈耶克：《货币的非国家化》，1976

史前纪事



江山代有人才出，各领风骚三十年

中本魔咒

2008.11

中本聪发表论文《比特币：一种点对点的电子现金系统》，提出了BlockChain这种数据结构

2009.1

比特币网络正式上线，第一个版本开源客户端发表，中本聪挖出创世区块及第一笔50个比特币

2010.5

佛罗里达程序员Laszlo Hanyecz用一万比特币购买了价值25美元的披萨优惠券

2010.8

攻击者利用整数溢出的漏洞凭空创造出了1840亿个比特币，这应该是迄今为止比特币发现的唯一重大漏洞

2010.9

世界上最早的矿池Slush，发明出多节点合作挖矿的方式，并挖出了首个区块

2011.4

官方有历史记载的0.3.21版本上线，支持非常多的新特性，包括UPNP、以聪为单位等，比特币系统逐渐成熟

2012.5

Bitcoin Magazine正式发布第一篇文章，介绍比特币和密码学货币。杂志发起人之一就是后来的以太坊之父Vitalik Buterin

2013.2

Bitcoin 0.8版本发布，引入了Leveldb、新的索引机制和查询方式，以及Bloom filter方式缩减SPV节点传输量等特性

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.

中本魔咒

2013.3

0.8版本的一个bug导致比特币硬分叉，紧急回退到旧版，而后发布0.81版本进行解决

2013.5

第一台比特币ATM在美国加州圣地亚哥诞生
8月，德国正式承认比特币合法地位

2013.12

中国人民银行等五部委发布《关于防范比特币风险的通知》，明确比特币不具与货币等同的法律地位

2014.6

整个比特币网络的算力达到了100 PH/S

2015.8

高盛等机构估计，全美已经有160,000商家接受比特币进行交易

2016.1

整个比特币网络的算力达到了1EH/S，至今已经超过4EH/S

2016.7

研究指出，接受比特币交易的合法商家数量早已超过犯罪活动和非法交易者人数

2017.3

Github上与比特币相关的项目数量超过了10,000个

Code is not the law, but good software is good

以太野望

2013.11 — Vitalik Buterin发起Ethereum项目，并在12月发布了以太坊白皮书的首个版本

2014.2 — Vitalik在迈阿密比特币会议上公布以太坊项目，吸引众多高手加入核心开发团队，并于3月发布了POC3

2014.4 — Gavin Wood发布了以太坊黄皮书（EIP-150），全面定义了EVM规范

2014.7 — 7.24日以太坊正式开始预售，总计发售了60,102,216个以太币，募集了31,531个比特币

2014.10 — POC6发布。这是一个具有重要意义的版本，亮点之一是区块链速度。区块时间从60秒减少到12秒，并使用了新的基于GHOST的协议

2015.7 — 以太坊发布第一个正式版本，也就是Frontier阶段版本，这个版本尚不完善，但标志着以太坊的正式运行

2016.3 — Homestead版本发布

同年6月，著名的The DAO被攻击事件发生，以太坊硬分叉，出现了ETC和ETH并行

2017.? — 以太坊将于2017年正式发布Metropolis，将是POW最后一个阶段，或许将是造币的最后一个阶段

区块链2.0　世界的计算机

沧海横流

2011.10 莱特币诞生，作为比特币的复制者，主要区别在于采用scrypt替代SHA-256

2012.9 当前Ripple的前身OpenCoin成立，发布新版Ripple协议，并且发行了瑞波币。后来专注于银行间转账市场

2013.8 德国正式承认比特币合法地位，成为承认比特币/密码学货币的第一个国家

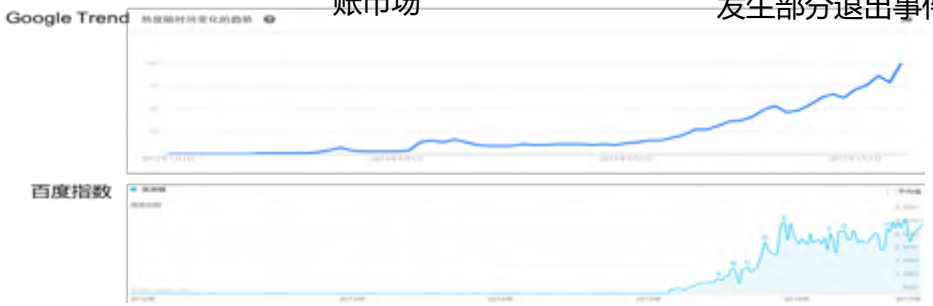
2015.9 R3 CEV正式成立，目标是制定银行区块链技术开发的行业标准，已有超过40家金融机构加入；日后又发生部分退出事件

2015.11 纳斯达克完成了基于区块链平台LINQ的首个证券交易，发行了Chain公司股票

2016.1 中国人民银行在北京召开数字货币研讨会，旨在重点部署数字货币及区块链技术研究。着手进行主权数字货币的研究与发行

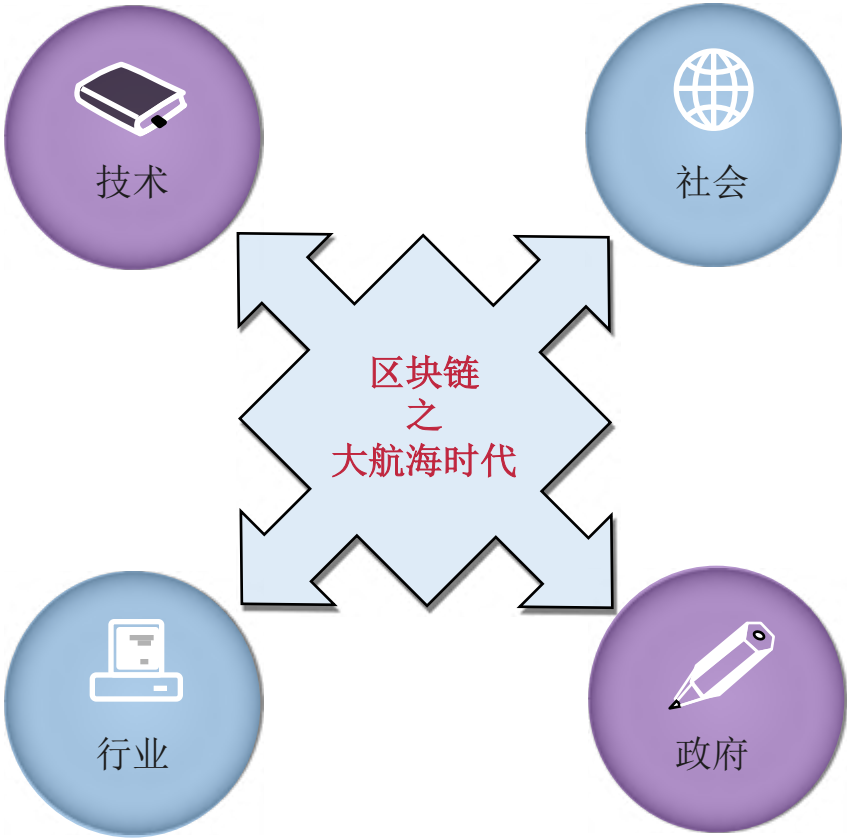
2016.3 IBM正式开源OpenBlockChain，并以此为基础成立了HyperLedger项目

2017 据统计，截至2017年4月底，全球总共455家区块链公司累计获得融资额为19.47亿美元，在获投公司数量上中国共有61家位列全球第二



沧海横流

- 以太坊、Hyperledger、Corda、ZCash，以及国内相关区块链技术层出不穷
- POW、POS/DPOS、POET、ZK、PBFT等共识机制日渐成熟
- 比特币全球算力在2017年5月达到4 ExaHash/S
- 莱特币率先实现了隔离见证



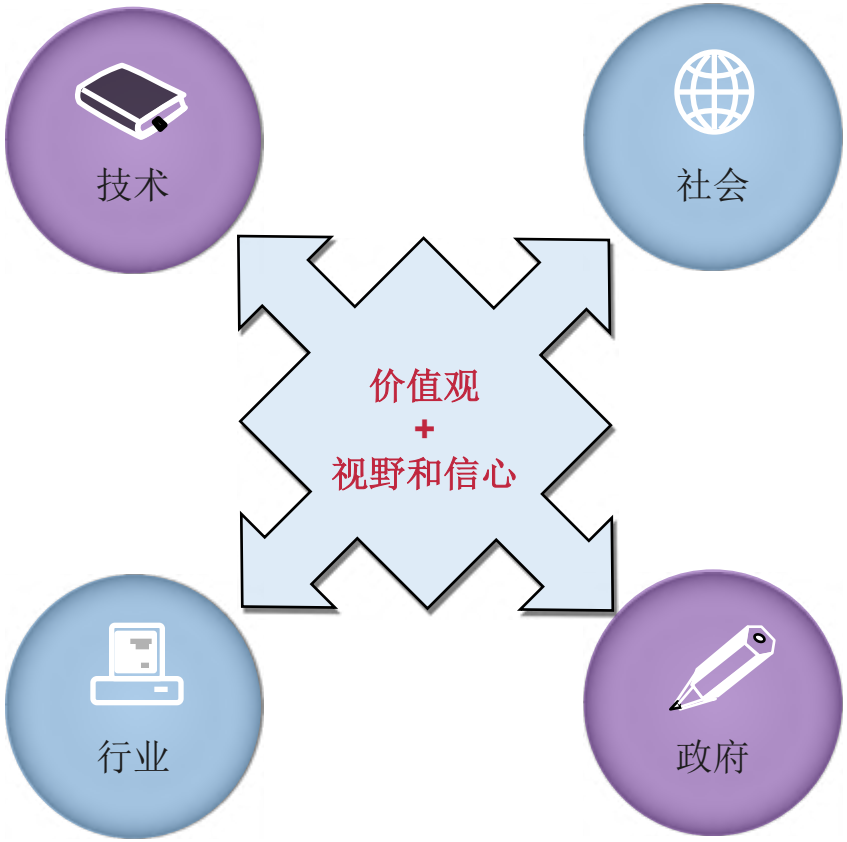
- 截止2016年3月，初步估计全球共有656种数字货币
- 截止2017年4月，数字货币总市值接近300亿美元，其中比特币占80%
- 全球数千万商家有可能直接或间接通过比特币进行交易
- 区块链相关学术论文已经达到近20,000篇

- 区块链在全球范围内票据、证券、保险、供应链、存证、溯源、知识产权等十几个领域均有大量POC应用，某些已经走入实践
- 国际、国内多家互联网金融企业、银行及各类企业宣布推出自己的区块链项目

- 全球已经有至少十几个国家正式承认比特币合法地位，部分国家承认其作为货币的属性
- 中国央行虽然禁止比特币作为货币兑换，但是率先宣布研究和发行数字货币
- 中国工信部指导下公布了《区块链和分布式账本技术参考架构》标准

我们必须知道 我们必将知道

- 目前主流共识算法的异同，如何选择？
- “零知识证明”会是新的杀手级技术吗？
- 现在需要学习区块链吗，人才缺乏问题如何解决？
- 隔离见证对区块链类系统的设计会有什么启发和影响？
- 跨链交易最佳实践是什么？
- 央行数字货币会采用什么样的技术方案？



- 央行的数字货币会长什么样，对我们日常生活有什么影响？
- 区块链应用适合普通老百姓使用吗，面向C端的区块链应用如何解决安全性、可靠性等问题？
- 区块链将会是下一代互联网还是另一个昙花一现的“Buzz word”？

- 什么样的应用真正适合区块链，如何辨别伪应用？
- 以太坊与HyperLedger，竞争还是结合？
- **现在都有哪些典型的区块链项目，应该如何入手？**
- R3这个“无链之链”会被金融界和区块链界接受吗？
- 线下资产搬到链上的“正确姿势”是什么？

- 区块链应用如何在匿名与监管之间达到有效平衡？
- 政府如何通过区块链技术提升社会公共事业的公信力、可靠性？
- 各国政府对虚拟货币的长期态度如何？

共同参与

区块链大航海时代

我们必须知道 我们必将知道