Section II: 比特币前传

通向 Bitcoin 之路

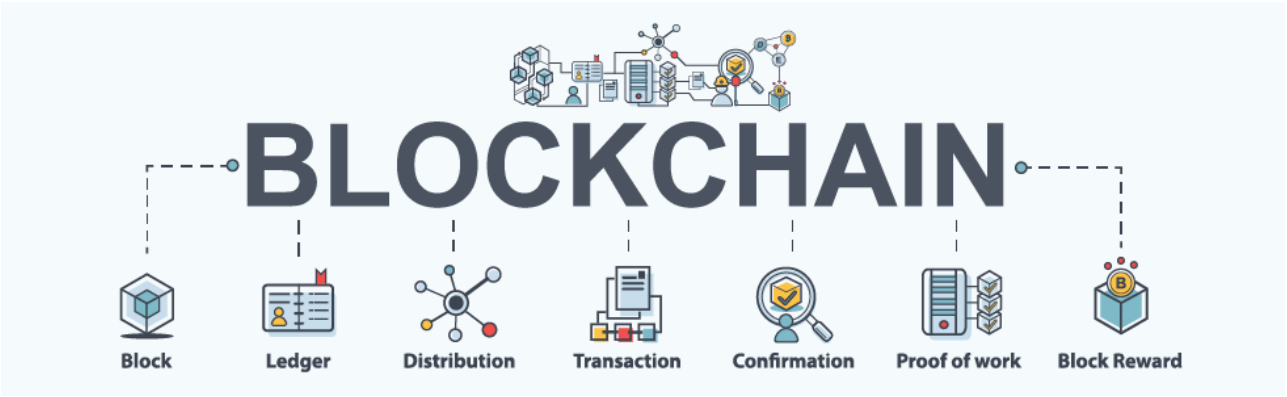
吴嘉婧 副教授

中山大学
计算机学院

Does Bitcoin matter?

- 为什么要从比特币讲起?
- 跟区块链什么关系?

- 区块链随着比特币的出现而面世;
- 区块链是载体/平台，比特币是产品



What are there before Bitcoin?

- 货币的历史
  - 历史上，很多种货币：黄金、金属币、纸币、电子现金、信用卡，PayPal
  - 经验教训
  - 理解为何Bitcoin会出现

Revisit 传统金融体系—货币发展

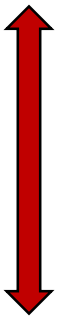
文字： 信息传递：语言→文字→印刷术→电报→互联网

(精神)

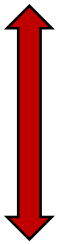
信息

(信息传递网络)

TCP/IP



楔形文字
记录生意



货币： 价值传输：大麦→黄金→纸币→移动支付→数字货币

(物质)

信用

(价值传输网络)

区块链

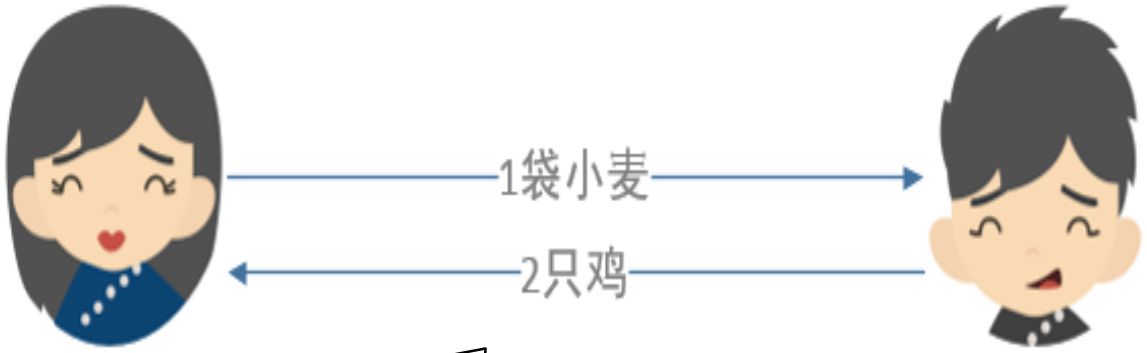
更高效交流的手段

时间：公元前3000年左右，
地点：美索不达米亚平原（伊拉克境内，古巴比伦）

Revisit 传统金融体系—货币发展

以物易物时代

- 贸易规模小
- 无统一货币
- 以物易物
- 限制
  - 时机
  - 市场规模



当且仅当：双方恰好需要对方的物品！

否则，如何解决?

Revisit 传统金融体系—货币发展

协调交易：

- 信用
- 现金

债务：需要对方的物品，先拿走用！
缺点：交易需要按照特定顺序发生

现金：需要对方的物品，直接支付！
好处：交易按照任意顺序发生

Revisit 传统金融体系—货币发展史

两种交易体系共存

- 信用体系
  - 交易不需触发的条件
  - 债务违约风险
- 现金体系
  - 精准衡量物品价值
  - 必须提前分配现金

信用体系：网络信用卡

信用卡交易

- 线上支付很方便

信用体系，什么角色不可少？

- 中介

早期，网购用户提交个人信用卡信息

- 1）to 商家 （安全？隐私？）-- 难以置信
- 2）to 中介公司：可以接受，但增加复杂度，买卖方均需开户
- 直到：中介体系SET (Secure Electronic Transaction)

信用体系：网络信用卡

90年代中期，中介体系SET (Secure Electronic Transaction)

- 1）用户无需将信用卡信息提供给商家 -- 安全,隐私
- 2）用户无需在中介公司注册账户
- 3）用户购物时，
  - 浏览器 (Tx, CreditCard) –--(加密后发送)----> 商家；
  - 商家 (你的Tx信息, 商家的Tx信息) –--(发送)---> 中介；
  - 中介解密你的Tx信息，与商家的Tx信息比对，然后批准支付

- 为什么SET体系有效?
  - 认证机制：加密后的身份 (public key) 与 现实身份连接起来
  - 强制商家、终端客户认证：complicated, & non-anonymous

信用体系：网络信用卡

90年代中期，中介体系SET (Secure Electronic Transaction)

- 一家叫 “网络现金 (CyberCash)” 公司
  - 采用了 SET 体系，推出一种小额支付系统——使用CyberCoin 数字货币
  - 2001年，网络现金公司破产，知识产权卖给威瑞信 (VeriSign,Inc.)，又转卖给 PayPal，后者使用至今

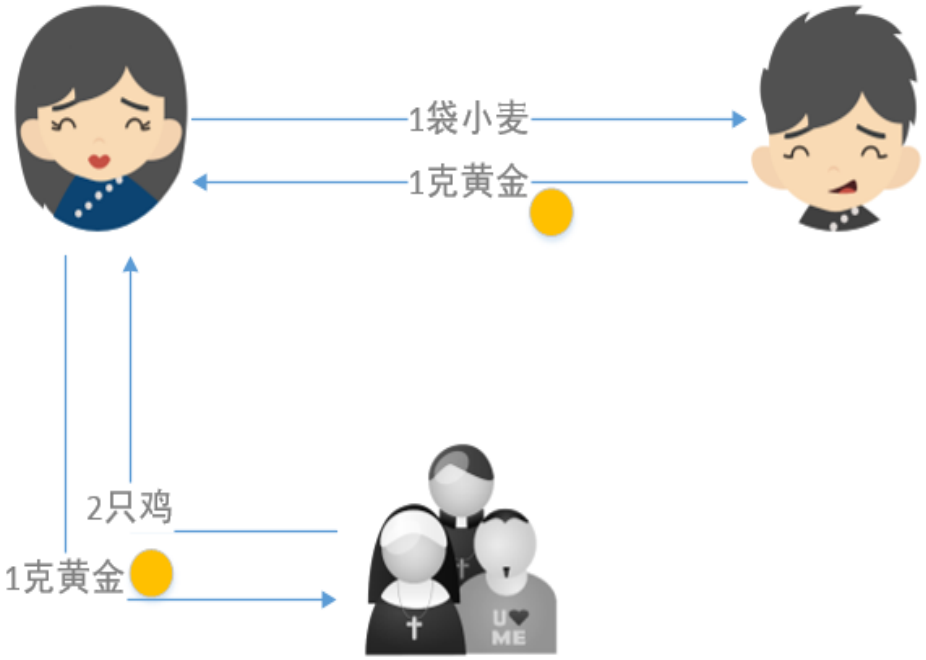
VeriSign®

全球最大网络安全认证公司：威瑞信
VeriSign(VRSN)

现金体系：实物现金

实物现金

- 开采冶炼困难
- 磨损氧化等损耗
- 故意囤积抬升金价
- 衡量标准不稳定

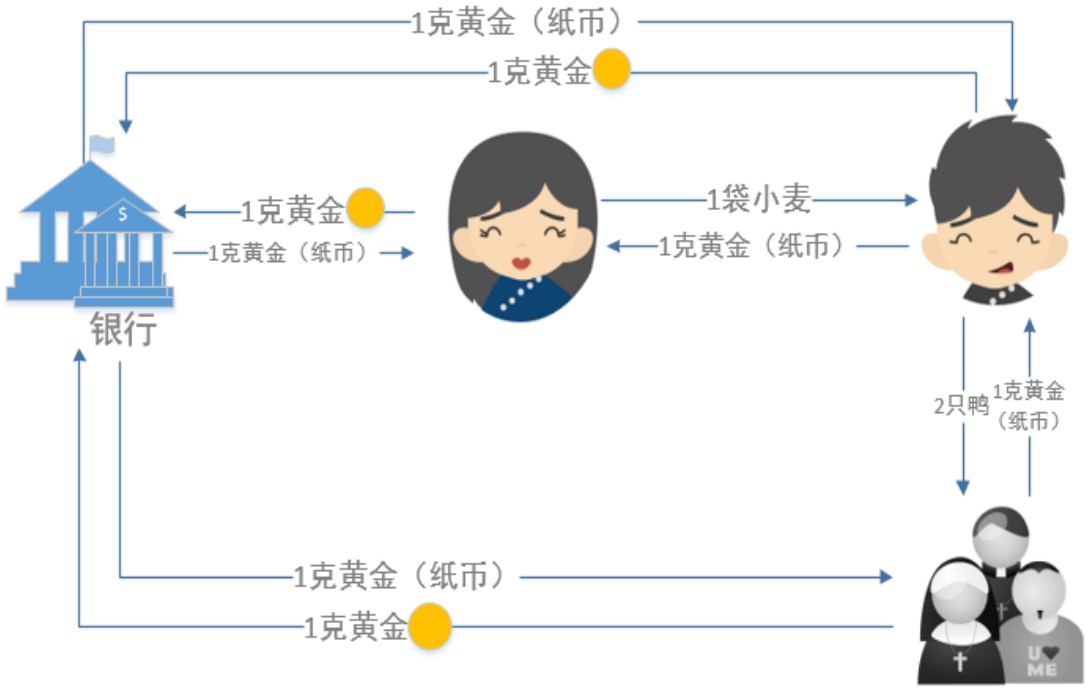


优点：
#1. 确保用户匿名性；
#2. 支持 offline trading

现金体系：符号货币

符号货币时代

- 自身价值与其代表价值差距巨大
- 易通货膨胀
- 纸币造假横行
- 日常难辨真伪



现金体系：中央系统虚拟货币时代

- 电子现金（centralized e-cash）
  - 铸造电子现金时，需要解决什么问题?
    - 防伪
    - 双重支付
    - 如何匿名

  - 为了实现可匿名支付的电子货币，解决办法?
    - 1) 为 e-cash 产生一个独特序列号;
    - 2) 不要让我看到，签名;
    - 盲签(blind signature)：铸币者不知 e-cash 行踪

现金体系：中央系统虚拟货币时代

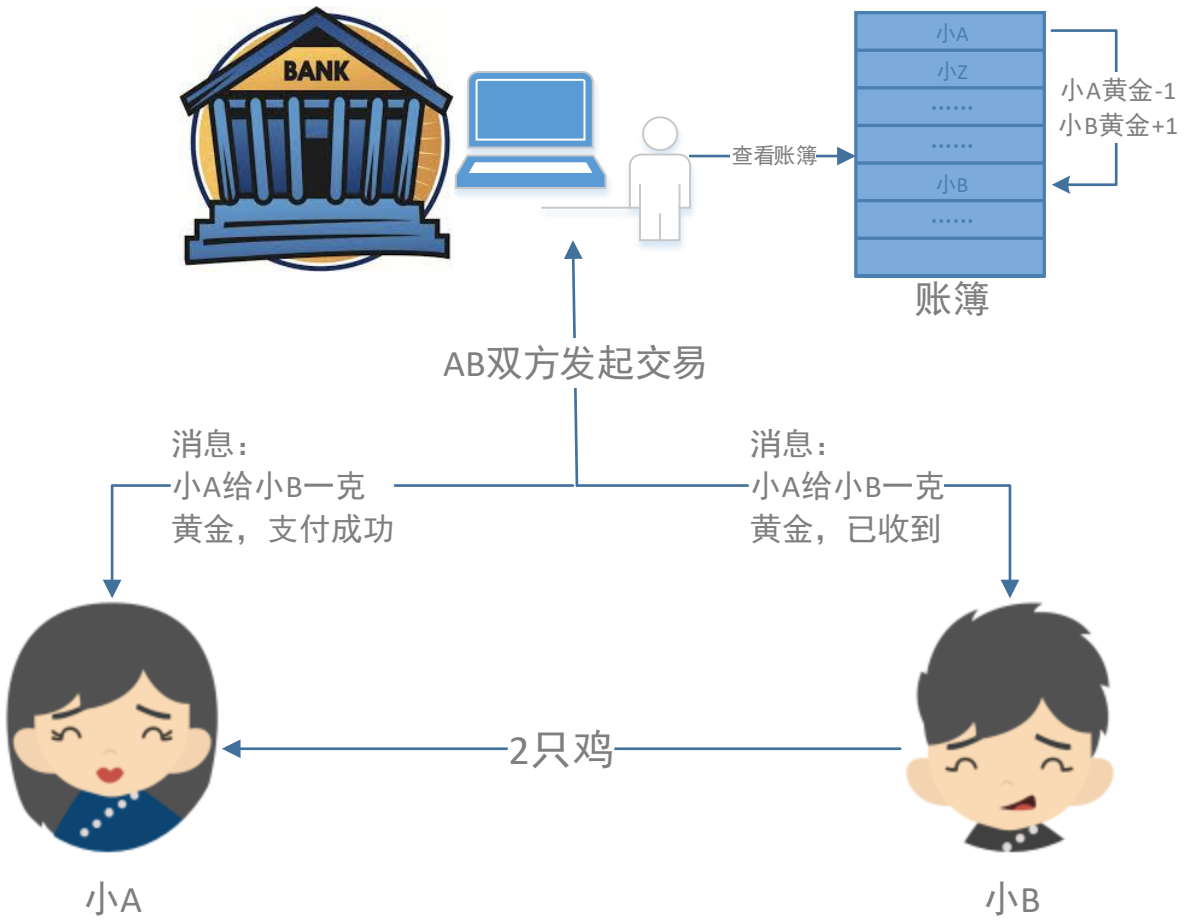
- **电子现金（centralized e-cash）**
  - 1983年，Dvaid Chaum 提出加密技术 + 现金
  - 1989年创建 Digicash 公司
  - 公司位于阿姆斯特丹，
  - 1994年5月开发e-cash网上支付

- E-cash 系统
  - 首个匿名化的数字货币密码货币
  - 1999年破产

现金体系：中央系统虚拟货币时代

电子货币的缺点

- 不可分性
- 中心化风险
- 信息不对称
- 依赖于账本持有人的信用
- 中心账本易损毁或者失窃



电子货币时代 —— 信任的难题

Peter Steiner 1993年发表于《纽约客》

- 两个互不认识的人要达成交易/协作，必须要依靠第三方：转账需要银行，支付宝，微信等信用中间机构
- 去中心化信任，how to?

Cypherpunk 密码朋克

这场去中心化的信任革命，起源于：

Cypherpunk 密码朋克

密码朋克宣言

“密码朋克”宣言甚至还使用了一些与日常交易直接相关的、非常实用的例子：

“当我在商店购买杂志并向店员递交现金时，店员无需知道我是谁。当我要求我的电子邮件服务提供商发送和接收消息时，电子邮件服务提供商不需要知道我在和谁沟通，也不需要知道我说了哪些内容，以及别人对我说了些什么，电子邮件服务提供商只需要知道在什么地方获得信息，以及我需要为这些服务支付多少费用.....因此，开放社会的因素需要匿名交易系统。到现在为止，现金一直是这个系统的重要组成部分…

…匿名交易系统不是秘密交易系统，个体用户在使用匿名系统的时候，只会在需要透露他们身份的时候，通过授权来确认—这才是隐私的本质。”

Cypherpunk 密码朋克

1970年代之前密码学
只存在美国军方系统

1970年代IBM首个
商用密码方案DES

ecash

1980年代David Chaum
创建匿名支付和电子货币

1992年Eric Hughes
开发了匿名邮件列表

1993年Eric Hughes， Tim May和
John Gilmore拟定《密码朋克宣言》
开启Cypherpunk时代

1997年Adam Back开发了Hashcash
首次引入工作量证明过滤垃圾邮件

$B-MONEY$ 1998年，Wei Dai 发布了
B-Money—交易数据维护方案

2001年Bram Cohen
开发了BitTorrent

BitTorrent

2008年中本聪发表
Bitcoin: A Peer-to-Peer Electronic Cash System

2014年，以太坊区块链出现

2010年阿桑奇
维基解密事件

Cypherpunk-Bitcoin

Bitcoin: A Peer-to-Peer Electronic Cash System

Section III

From Bitcoin to Blockchain

吴嘉婧 副教授

中山大学
计算机学院

比特币诞生

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Not me !

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

Dorian Satoshi Nakamoto
(not actually Satoshi Nakamoto)

He graduated in physics from California Polytechnic and worked on classified defense projects.

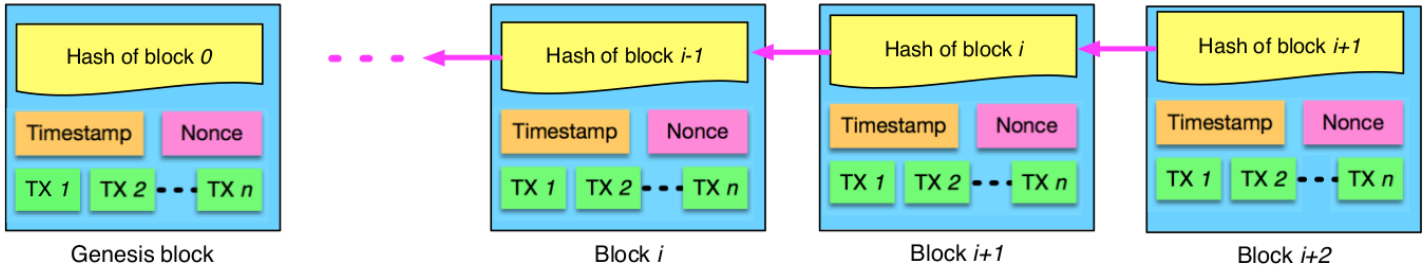
- 2009年1月，创世区块诞生。
- 一种完全基于点对点（P2P）的电子现金系统， 使得全部支付都可以由交易双方直接进行，完全 摆脱了第三方，创造了一种全新的货币体系。

比特币（BitCoin，BTC）

- 比特币（BitCoin，BTC）起源于*密码朋克*，诞生于2009年，由中本聪 **Satoshi Nakamoto** 提出
- 一种建立在计算机技术，密码学及经济学上的货币形式（加密数字货币）
- 历史上首个经过大规模长时间检验的数字货币系统，启发了后来区块链技术的发展
- 当前市场总值第一的数字货币

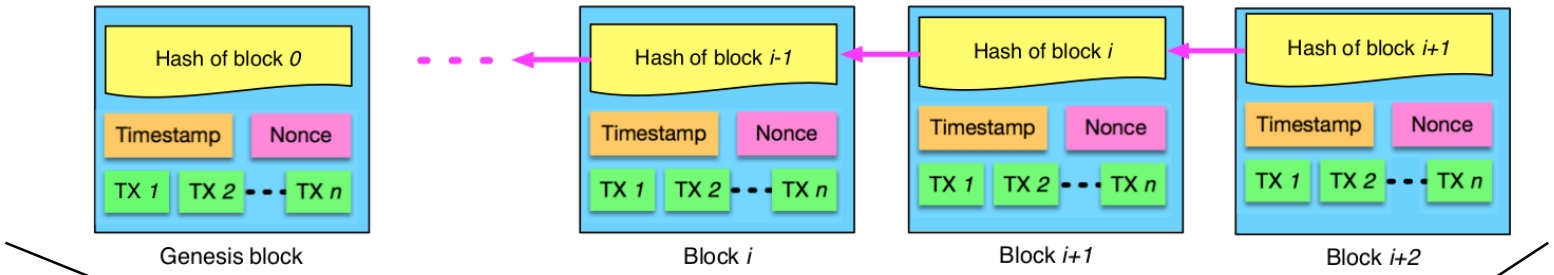
Bitcoin 的底层技术 —— 区块链初识

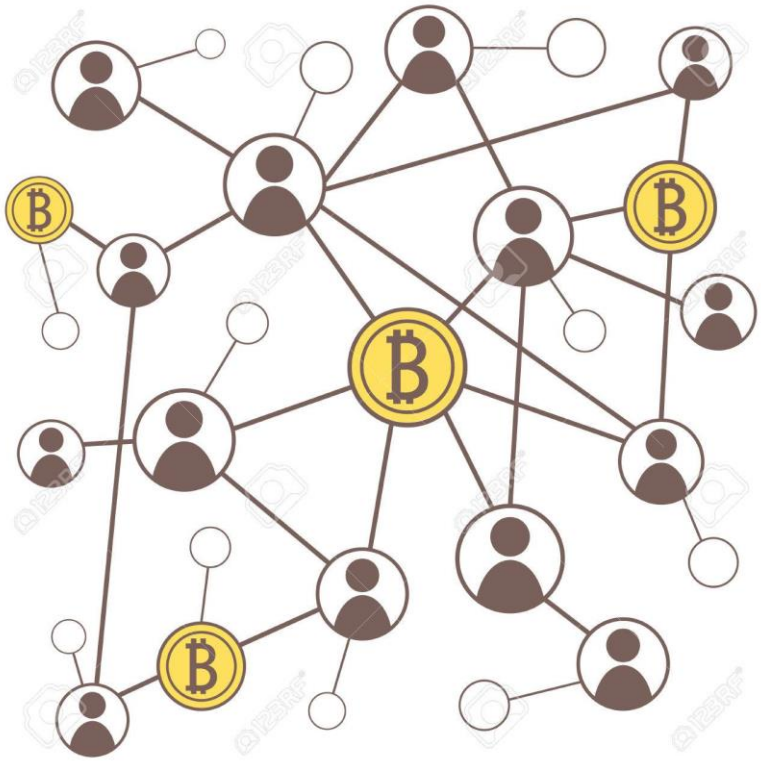
- 区块链定义
  - 按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构



  - 区块链是一个**分布式的账本数据库**
  - 网络中的每个节点都有一本完整的账本
  - 无法篡改
  - 去中心化，降低成本，提高效率

Bitcoin Network





区块链定义

- 例子：小虎队《爱》--1991年8月

向天空大声的呼唤说声我爱你

向那流浪的白云说声我想你

让那天空听得见

让那白云看得见

谁也擦不掉我们许下的诺言

- 天空、白云分布式记账节点，同时记录了“A爱B”这个信息
- 从而，让这个表白不可反悔、不能否认、修改
- 分布式账本：一笔数据，多人记录，同步保持

区块链特性

Anonymous
匿名性

Consensus
一致性

Decentralized
分布式

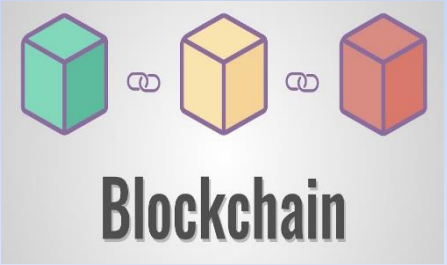
Immutable
不可篡改

生产力 vs 生产关系

- 人工智能：解放生产力
  - 剧烈地改变了人类的生活
  - 没有改变组织模式（银行柜台，移动支付）
  - 以人为中心来执行判断，做决策

- 区块链：改变生产关系
  - 它挑战和改变了人类的组织模式
  - 几十年后回头看可能发现很多机构都消失不见

意义拔高：从 农业社会 到 智能社会

	农业社会	工业社会	智能社会
生产资源			
技术手段			
生产关系			

区块链近况

- 2018年5月28日，习总书记在中国科学院第十九次院士大会、中国工程院第十四次院士大会上的讲话：

  - 以**人工智能、量子信息、移动通信、物联网、区块链**为代表的新一代信息技术加速突破应用

区块链近况

2018年7月16日，工信部苗圩部长在全国工业和信息化主管部门负责同志座谈会：

- 支持龙头企业基于云计算建立**区块链应用实验和测试平台**，发展**BaaS**服务中小企业创新，加快**丰富区块链领域应用**。指导行业组织建立公共服务平台，开展运行效率、可扩展性、容错性、安全性等测评，为企业提供政策咨询、投融资、专利保护等服务。

区块链近况

进入国家规划

多地地方政府，采用多种方式引导和支持区块链技术和产业的发展

2016年12月，区块链列入国务院《“十三五”国家信息化规划》	2017年1月，工信部《软件和信息技术服务业发展规划(2016-2020年)》	2018年3月，工信部《2018年信息化和软件服务业标准化工作要点》	2018年5月，24个省市或地区发布了区块链政策及指导意见

2019年10月25日，中央政治局18th集体学习

学习进行时 新华通讯社出品

第一头条 | 讲习所 | 近平日历 | 近平STYLE | 专家库 | 报道集

新华网 > 高层 > 正文

www.news.cn 新华网 NEWS www.xinhuanet.com

让新闻离你更近

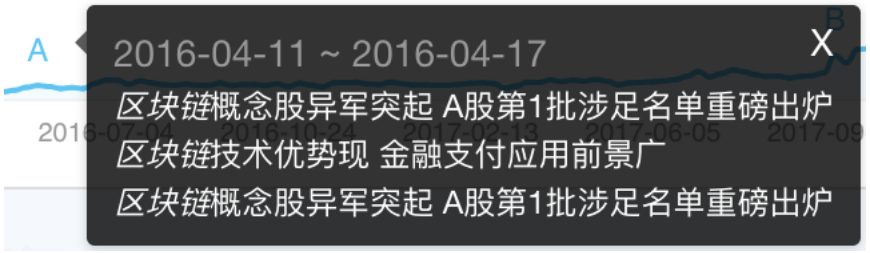
习近平在中央政治局第十八次集体学习时强调 把区块链作为核心技术自主创新重要突破口 加快推动区块链技术和产业创新发展

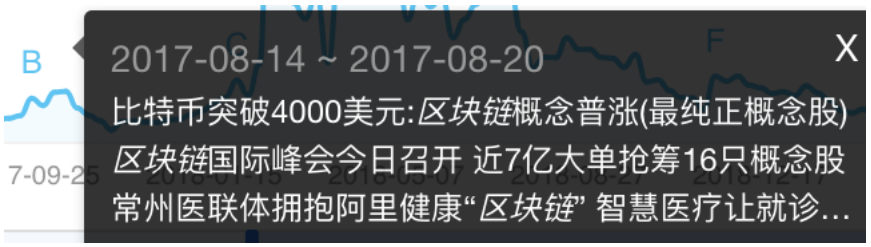
2019-10-25 18:14:26 来源： 新华网

区块链热度

百度指数


搜索指数
对比时间段
2015-08-03 ~ 2020-09-05
自定义
PC+移动
全国
区块链
新闻头条
平均值
100,000
80,000
60,000
40,000
20,000
A
B
C
D
E
F
G
H
I
2015-11-23
2016-03-14
2016-07-04
2016-10-24
2017-02-13
2017-06-05
2017-09-25
2018-01-15
2018-05-07
2018-08-27
2018-12-17
2019-04-08
2019-07-29
2019-11-18
2020-03-09
2020-08-31

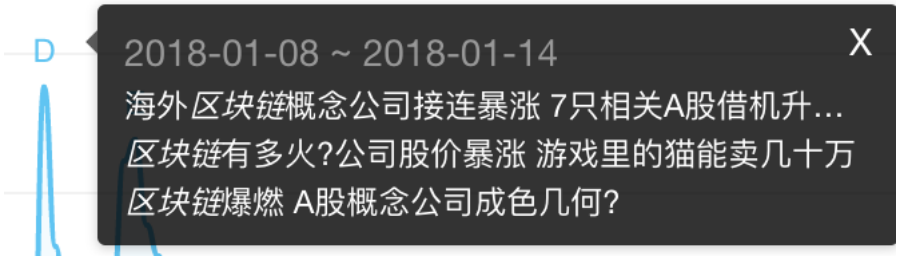

A
2016-04-11 ~ 2016-04-17
X
区块链概念股异军突起 A股第1批涉足名单重磅出炉
区块链技术优势现 金融支付应用前景广
区块链概念股异军突起 A股第1批涉足名单重磅出炉

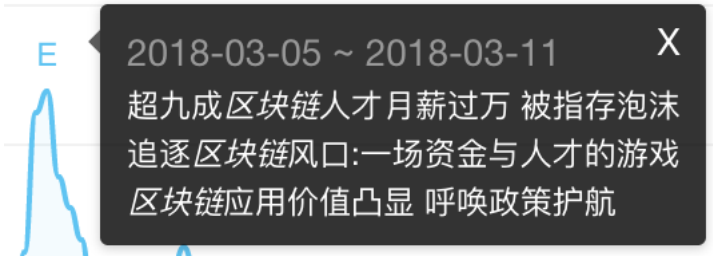

B
2017-08-14 ~ 2017-08-20
X
比特币突破4000美元:区块链概念普涨(最纯正概念股)
区块链国际峰会今日召开 近7亿大单抢筹16只概念股
常州医联体拥抱阿里健康“区块链” 智慧医疗让就诊…

区块链热度

百度指数


2019-10-28 ~ 2019-11-03
区块链迎政策利好 成核心技术创新重要突破口
深圳区块链电子发票突破1000万张
刷屏的区块链究竟是什么?你想知道的都在这里!
搜索指数
区块链
全国
新闻头条
平均值
100,000
80,000
60,000
40,000
20,000
A
B
C
D
E
F
G
H
I
2015-11-23
2016-03-14
2016-07-04
2016-10-24
2017-02-13
2017-06-05
2017-09-25
2018-01-15
2018-05-07
2018-08-27
2018-12-17
2019-04-08
2019-07-29
2019-11-18
2020-03-09
2020-08-31


D
2018-01-08 ~ 2018-01-14
海外区块链概念公司接连暴涨 7只相关A股借机升...
区块链有多火?公司股价暴涨 游戏里的猫能卖几十万
区块链爆燃 A股概念公司成色几何?

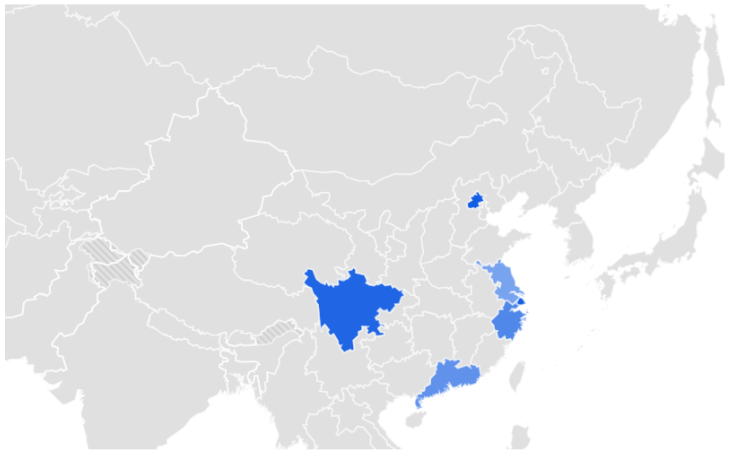

E
2018-03-05 ~ 2018-03-11
超九成区块链人才月薪过万 被指存泡沫
追逐区块链风口:一场资金与人才的游戏
区块链应用价值凸显 呼唤政策护航

区块链热度

Google Trends

Interest by subregion

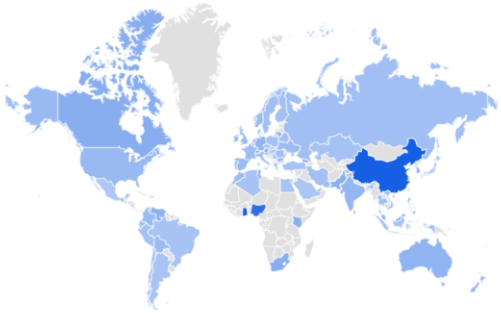
Subregion



1	Beijing	100
2	Shanghai	98
3	Sichuan	92
4	Zhejiang	61
5	Guangdong	51

Interest by region

Region



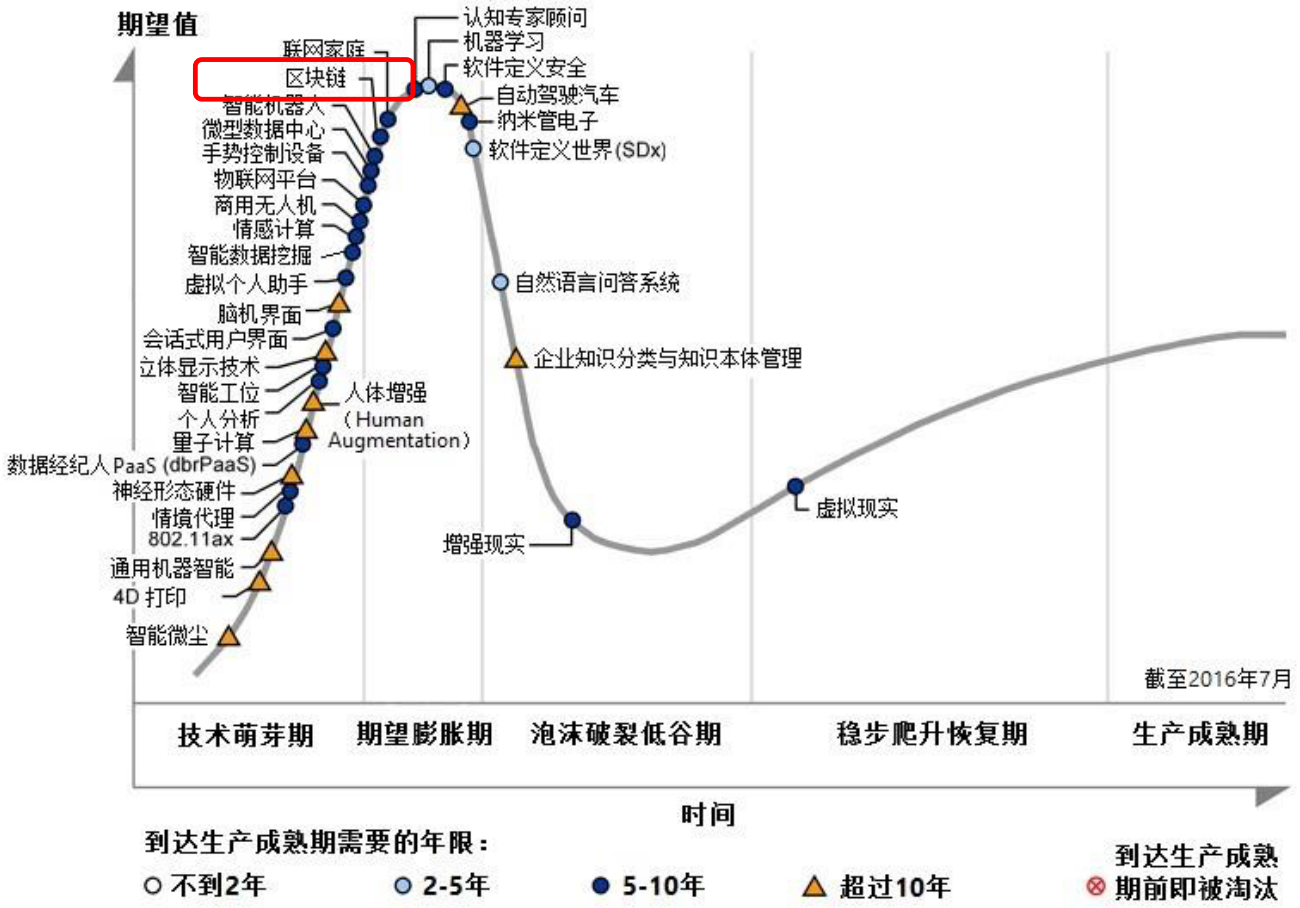
1	Ghana	100
2	China	98
3	Malta	89
4	St. Helena	86
5	Nigeria	83

Gartner新兴技术成熟度曲线-2016

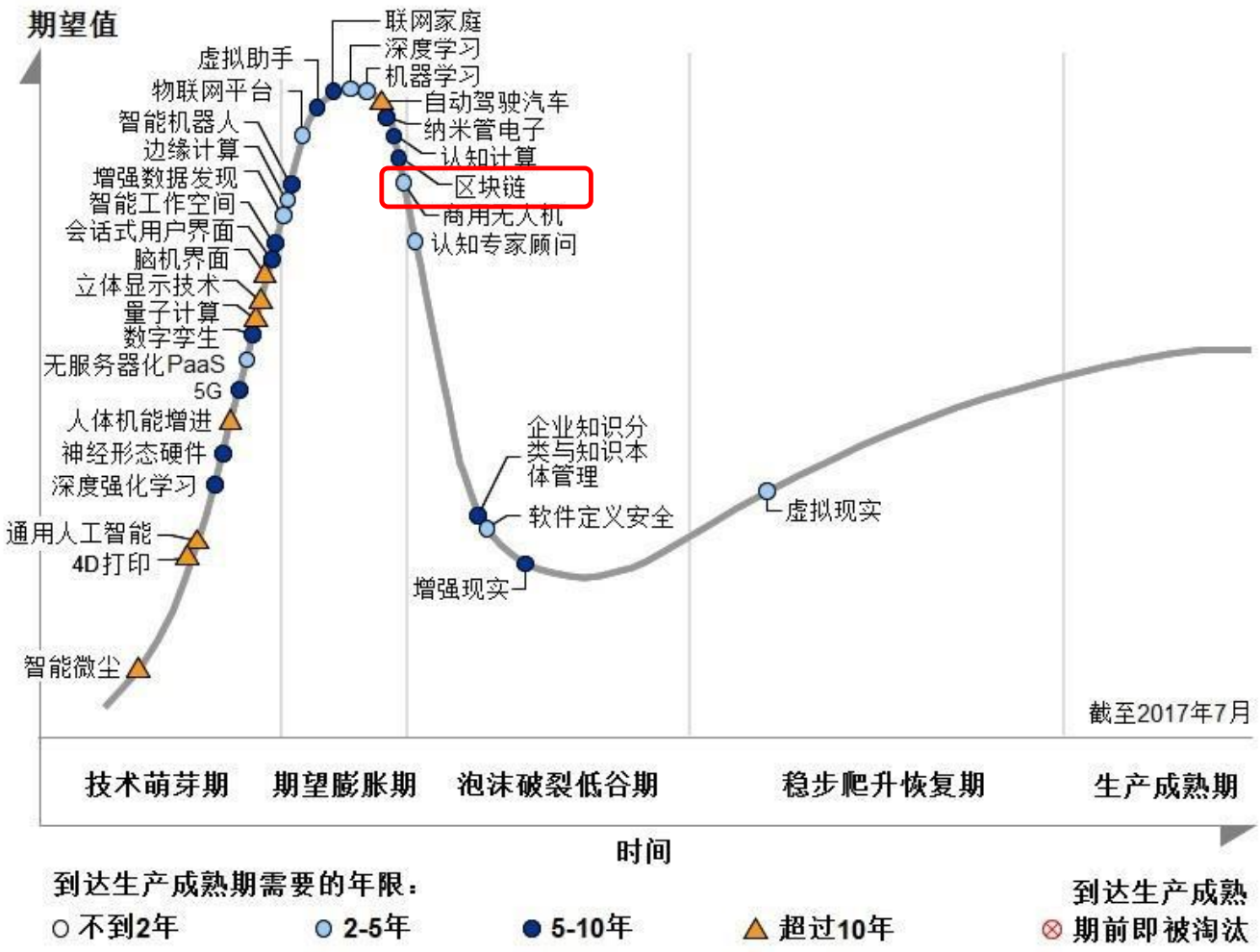
在 Gartner 技术成熟度曲线: 新兴科技技术成熟度曲线

它集逾两千种科技的大成，凝聚独到的见解，并以简洁明了的方式呈现出 29 项新兴科技技术和趋势。

该技术成熟度曲线重点关注了那些有望在未来五到十年内拥有高度竞争优势的科技

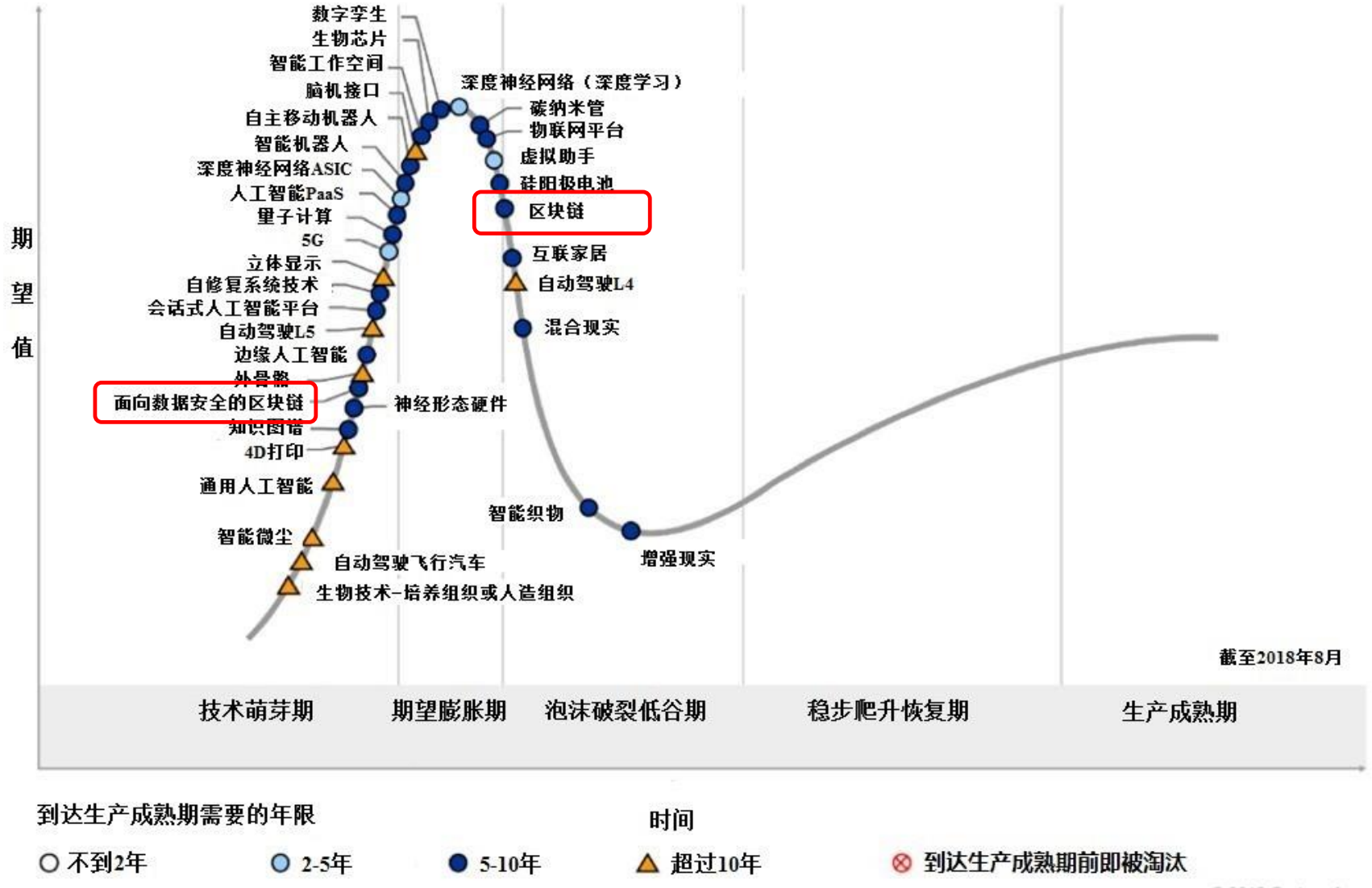


Gartner新兴技术成熟度曲线-2017

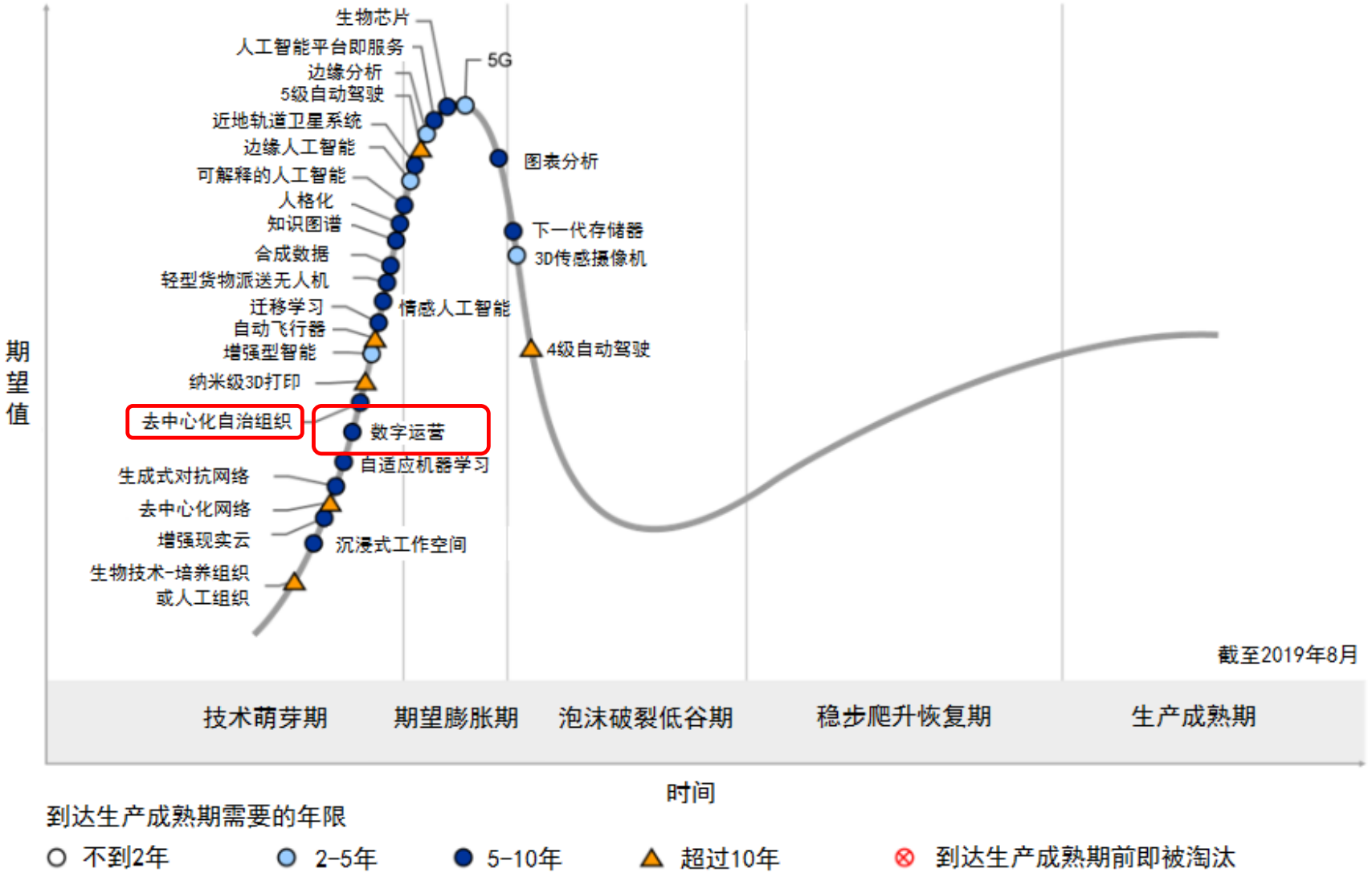


来源：Gartner（2017年7月）

Gartner新兴技术成熟度曲线-2018



Gartner新兴技术成熟度曲线-2019



Gartner Hype Cycle for Emerging Technologies, 2019

gartner.com/SmarterWithGartner

Source: Gartner

Gartner

Gartner新兴技术成熟度曲线-2020