管理信息系统

Management Information Systems

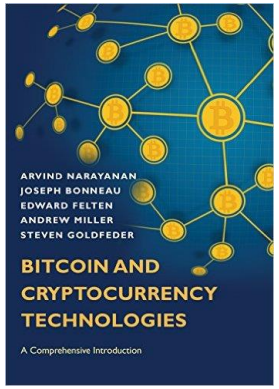
王谦 博士/副教授
南开大学商学院管理科学与工程系
wangqian70@nankai.edu.cn

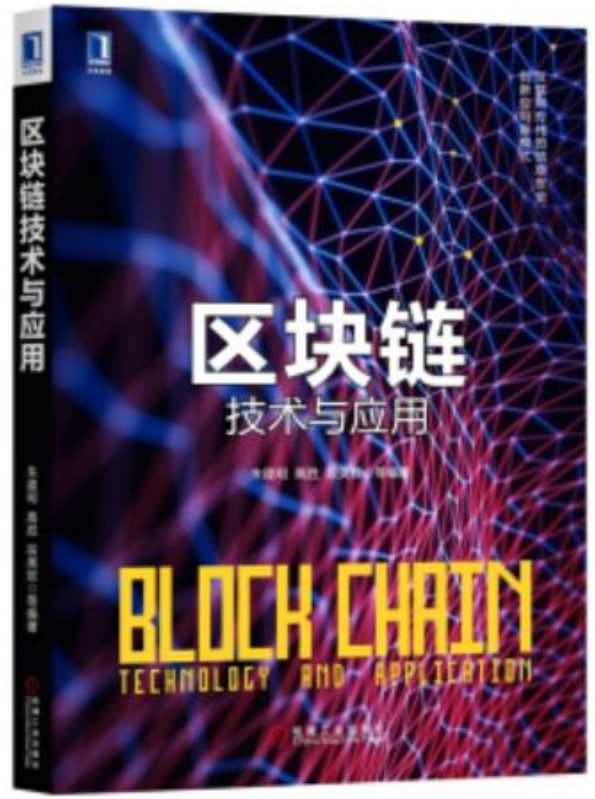
Chapter 12

区块链技术及其应用

学习目标

- 了解区块链核心技术构成
- 介绍区块链的技术特征
- 了解区块链的应用方式和应用范围





朱建明，高胜，段美姣 等编著，区块链技术与应用，机械工业出版社，2018年1月

区块链技术的影响

- 2015年以来，区块链技术引起了学术界、产业界的高度重视
  - 区块链——重塑经济与世界
  - 区块链技术有望像互联网一样彻底重塑人类社会活动形态，并实现从目前的信息互联网向价值互联网的转变
  - 互联网已经颠覆世界，区块链却要颠覆互联网
  - 区块链技术已经被视为下一代全球信用认证和价值互联网的基本协议之一
  - ……

比特币的出现

- 2008年11月
  - Satoshi Nakamoto（中本聪）发表《Bitcoin: A Peer-to-Peer Electronic Cash System》
- 2009年1月
  - 比特币发行、交易和账户管理系统开始运行
  - 创世区块（Genesis Block）
- 2010年
  - 开始流行，比特币交易所Mt.Gox在日本成立
  - https://bitcoin.org/
- 2011年~2014年：对区块链开始关注
- 2015年：区块链成为热门话题，业界开始进行深入验证与探索
- 2016年：区块链在多个行业得到更广泛的探索与应用

比特币价格走势


Market Price (USD)
Average USD market price across major bitcoin exchanges.
Source: blockchain.info
2017/12/17 08:00
USD: 19,290
USD
22,500
20,000
17,500
15,000
12,500
10,000
7,500
5,000
2,500
Mar '17
Apr '17
May '17
Jun '17
Jul '17
Aug '17
Sep '17
Oct '17
Nov '17
Dec '17
Jan '18
Feb '18

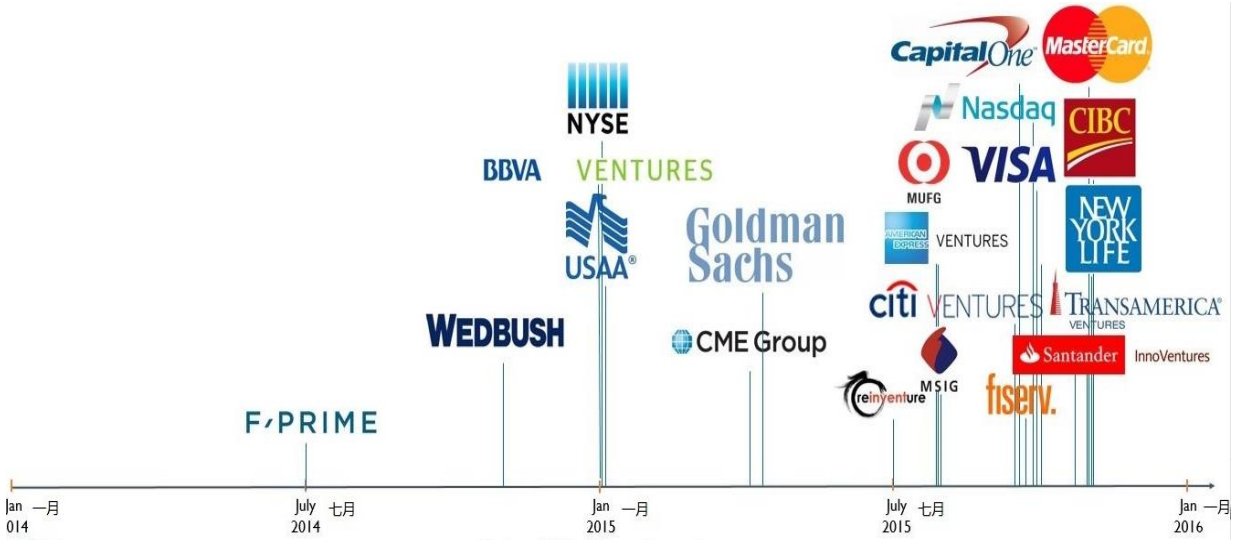
世界各国对比特币的态度

数字货币

- 2008年比特币的发明标志着数字货币技术的初步成熟，自此大量数字货币问世，数字货币市场规模不断扩大

全球数字货币已超1000种

企业大举挺近比特币与区块链创新领域



全球排名前10位的数字货币

#	名称	符号	市场总值	价格	当前发行量	交易量（24h）	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$42,469,634,391	$2583.82	16,436,762	$603,301,000	0.38%	2.73%	5.75%
2	Ethereum	ETH	$23,042,669,140	$247.37	93,152,127	$603,704,000	0.11%	1.05%	-9.61%
3	Ripple	XRP	$9,195,025,824	$0.240133	38,291,387,790 *	$100,506,000	0.08%	4.47%	-5.35%
4	Litecoin	LTC	$2,609,226,838	$50.26	51,911,482	$544,216,000	0.28%	4.43%	28.15%
5	Ethereum Classic	ETC	$1,569,021,537	$16.80	93,380,799	$82,590,000	0.72%	5.76%	-4.55%
6	Dash	DASH	$1,525,291,174	$205.69	7,415,557	$44,249,400	1.87%	2.32%	21.47%
7	NEM	XEM	$1,384,380,000	$0.153820	8,999,999,999 *	$3,676,380	0.24%	1.87%	2.16%
8	IOTA	MIOTA	$830,946,137	$0.298952	2,779,530,283 *	$2,982,940	0.69%	2.70%	-22.24%
9	Monero	XMR	$666,122,571	$45.15	14,754,951	$13,867,300	0.44%	3.02%	9.98%
10	EOS	EOS	$464,213,266	$2.33	198,958,206 *	$109,690,000	4.19%	7.54%	42.78%

全球排名前10的数字货币一览表（coinmarketcap.com，2017/07/10）

比特币与区块链技术之间的关系

应用

比特币 Bitcoin

- 全球数字货币
- 比特币交易波动性大、流动性高，受高频交易及对冲基金的喜爱

技术基础

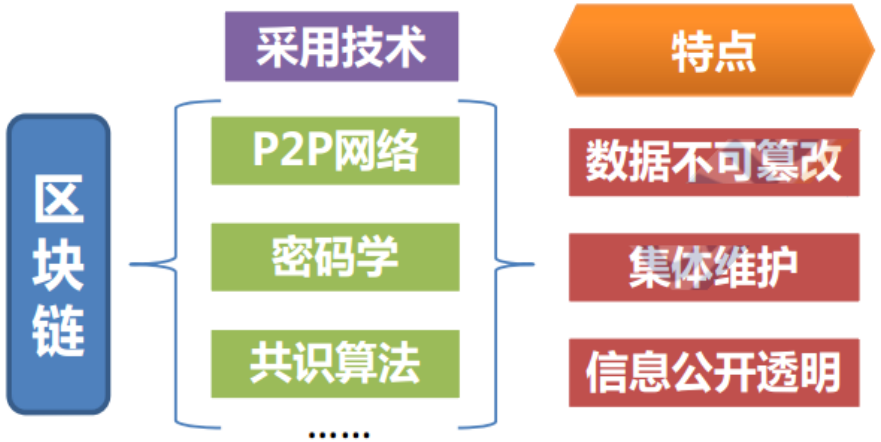
区块链 Blockchain

- 经密码加密的完备分布式总账
- 在需要第三方监管的中介网络及清算系统中发挥潜力
- 向其他需要较高信任机制的应用领域延伸

区块链是构建价值互联网的基石

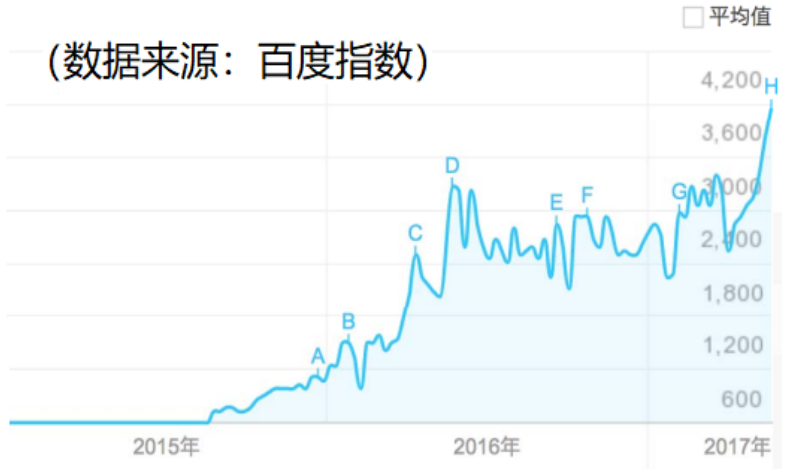
概念

➢区块链（Blockchain）是一种分布式数据库技术。在典型的区块链系统中，数据以区块（block）为单位产生和存储，并按照时间顺序连成链式（chain）数据结构。所有节点共同参与区块链系统的数据验证、存储和维护。



本质上，区块链是一种高度可信的数据库技术，提供了一种在不可信网络中进行信息与价值传递交换的可信机制。

根据百度指数来看，区块链已受到广泛关注

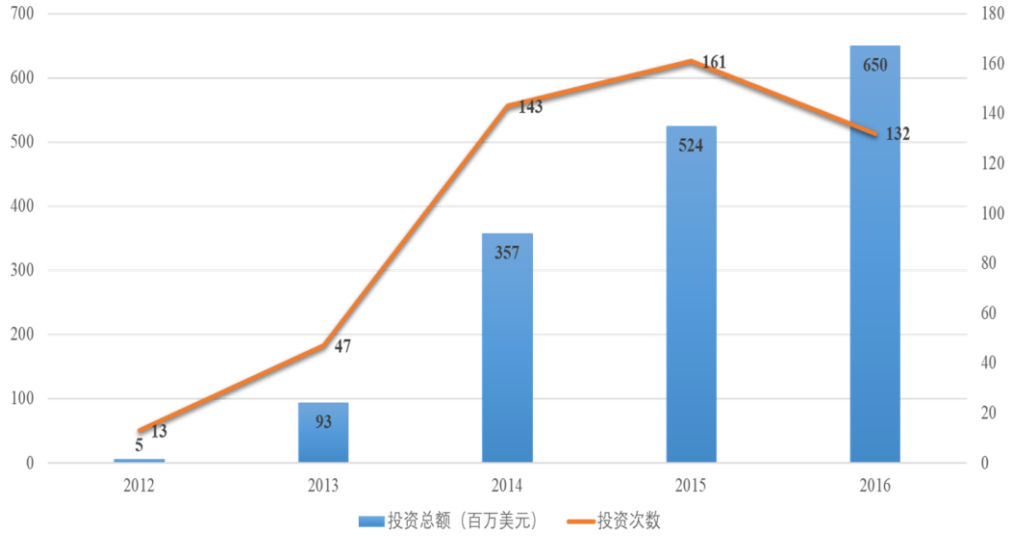


据Gartner曲线显示，区块链已经达到了**舆论炒作的巅峰**，区块链技术成熟仍需**5到10年**时间。

根据世界经济论坛调查报告预测，到2025年，全球GDP中有10%的相关信息将用区块链技术保存。

全球区块链企业快速增长

- 从区域分布来看，美国是区块链产业的领头羊，欧洲区块链产业分布密集
- 自2012年以来，全球区块链企业数量以超过65.2%的复合增长率快速增长
- 从投融资活动来看，区块链领域融资仍然保持相当高的活跃度，近三年累计融资规模11.7亿美元。其中，2016年区块链领域完成139次累计规模超过4.33亿美元的融资



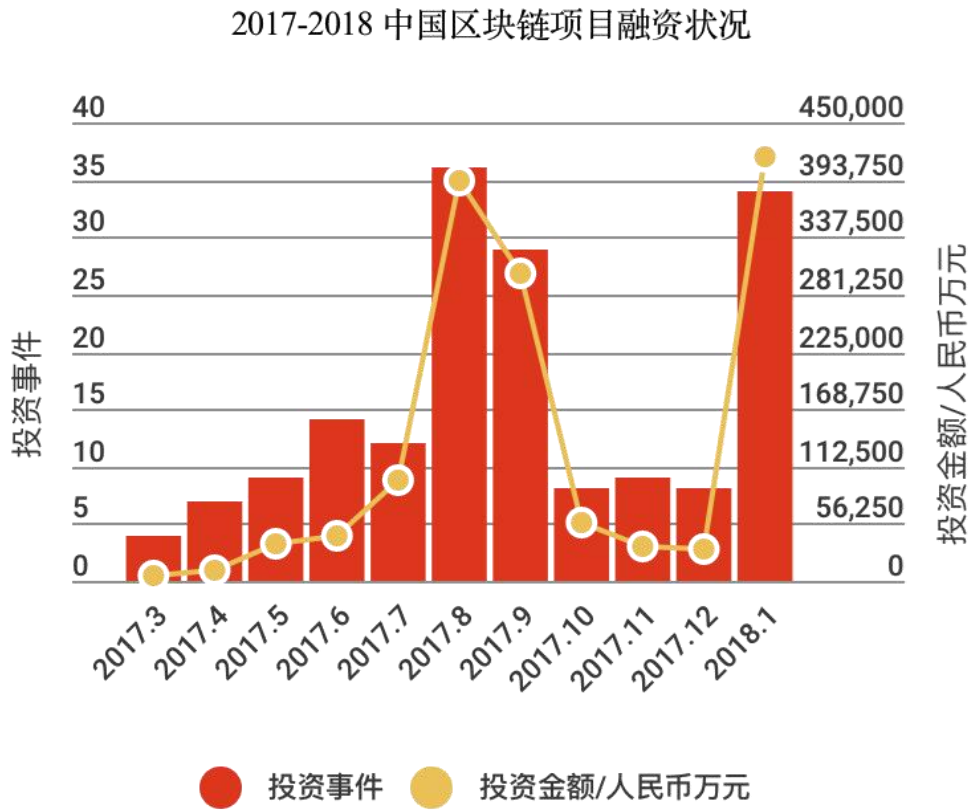
区块链引起我国政府、学术界、产业界高度关注

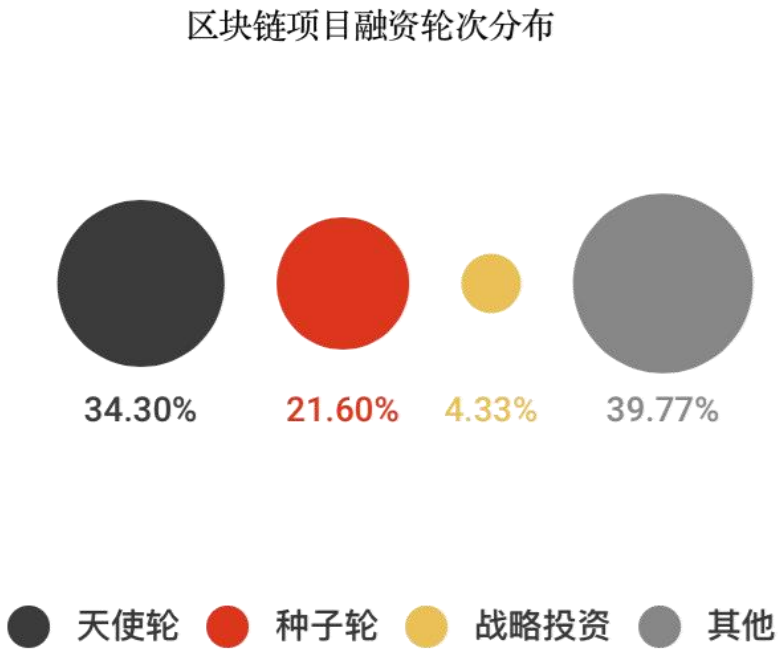
中国区块链产业发展

- 截至2016年底，中国共有105家区块链相关企业
- 从区域分布来看，区块链企业现阶段主要集中在东部地区，中西部地区也开始多点开花

中国区块链产业发展

- 2017/02至2018/01，中国区块链融资项目177个，融资金额达到143.8亿



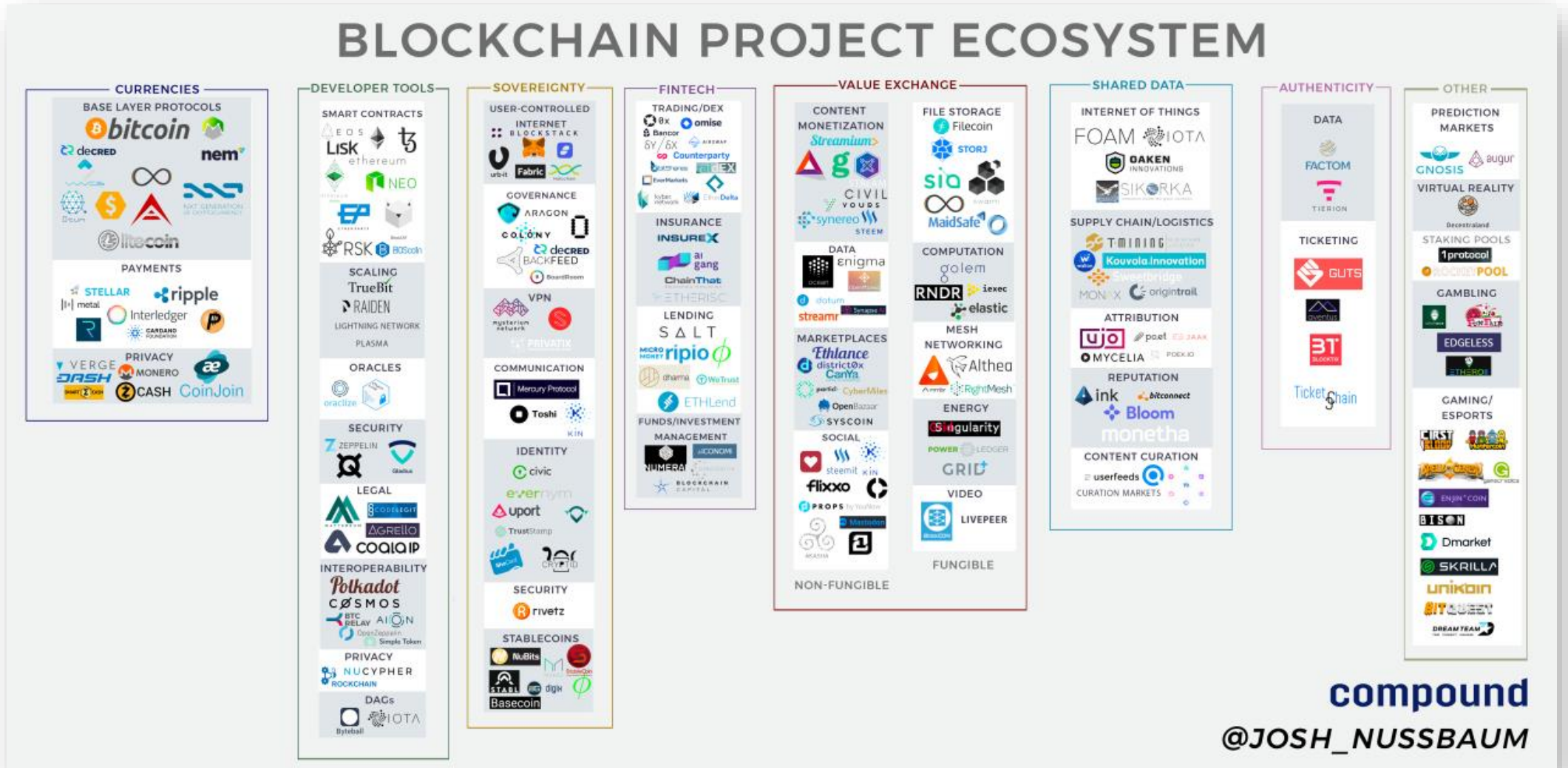


- 数据来源：鲸准

中国区块链创业企业


交易平台
OKCoin币行
安全 · 稳定 · 可信
比特币中国
BTCCHINA.COM
Huobi 火币
比特币交易网
www.btctrade.com
基础设施
矩阵元
太一
TAI
企业服务
企业级区块链解决方案
云象
YUNPHANT
onchain
Blockchain Solutions
区块链创业项目
媒体平台
巴比特
服务于区块链创新者
铅笔
CHAIN8
数字资产
www.guopai.com
果仁宝
底层技术
bumeng布萌.cn
万向区块链
WANXIANG BLOCKCHAIN
bubi布比.cn
众享比特
PeerSafe
Hyperchain

区块链生态系统


BLOCKCHAIN PROJECT ECOSYSTEM
CURRENCIES
BASE LAYER PROTOCOLS
bitcoin
decred
nem
litecoin
PAYMENTS
STELLAR
ripple
Interledger
PRIVACY
VERGE
DASH
MONERO
ZCASH
CoinJoin
DEVELOPER TOOLS
SMART CONTRACTS
EOS
Lisk
ethereum
NEO
RSK
SCALING
TrueBit
RAIDEN
LIGHTNING NETWORK
PLASMA
ORACLES
oraclize
SECURITY
ZEPPELIN
LEGAL
COALA IP
INTEROPERABILITY
Polkadot
COSMOS
PRIVACY
NUCYPHER
ROCKCHAIN
DAGs
IOTA
SOVEREIGNTY
USER-CONTROLLED
INTERNET
BLOCKSTACK
Fabric
GOVERNANCE
ARAGON
COLONY
decred
BACKFEED
VPN
COMMUNICATION
Mercury Protocol
Toshi
IDENTITY
civic
uport
SECURITY
rivetz
STABLECOINS
NuBits
Basecoin
FINTECH
TRADING/DEX
0x
omise
Bancor
Counterparty
INSURANCE
INSUREX
LENDING
SALT
ripio
ETHLend
FUNDS/INVESTMENT MANAGEMENT
NUMERAI
VALUE EXCHANGE
CONTENT MONETIZATION
Streamium
CIVIL
synereo
STEEM
DATA
enigma
streamr
MARKETPLACES
Ethlance
district0x
OpenBazaar
SYSCOIN
SOCIAL
steemit
flixxo
PROPS
NON-FUNGIBLE
FILE STORAGE
Filecoin
STORJ
sia
MaidSafe
COMPUTATION
golem
RNDR
iexec
elastic
MESH NETWORKING
Althea
RightMesh
ENERGY
Singularity
GRID
VIDEO
LIVEPEER
FUNGIBLE
SHARED DATA
INTERNET OF THINGS
FOAM
IOTA
OAKEN INNOVATIONS
SIKORKA
SUPPLY CHAIN/LOGISTICS
Kouvola innovation
origintrail
ATTRIBUTION
MYCELIA
REPUTATION
ink
bitconnect
Bloom
monetha
CONTENT CURATION
userfeeds
CURATION MARKETS
AUTHENTICITY
DATA
FACTOM
TIERION
TICKETING
GUTS
TicketChain
OTHER
PREDICTION MARKETS
GNOSIS
augur
VIRTUAL REALITY
Decentraland
STAKING POOLS
1protocol
POOL
GAMBLING
EDGELESS
GAMING/ ESPORTS
ENJIN COIN
BISON
Dmarket
SKRILL
unikoin
DREAMTEAM
compound
@JOSH_NUSSBAUM

区块链技术的应用

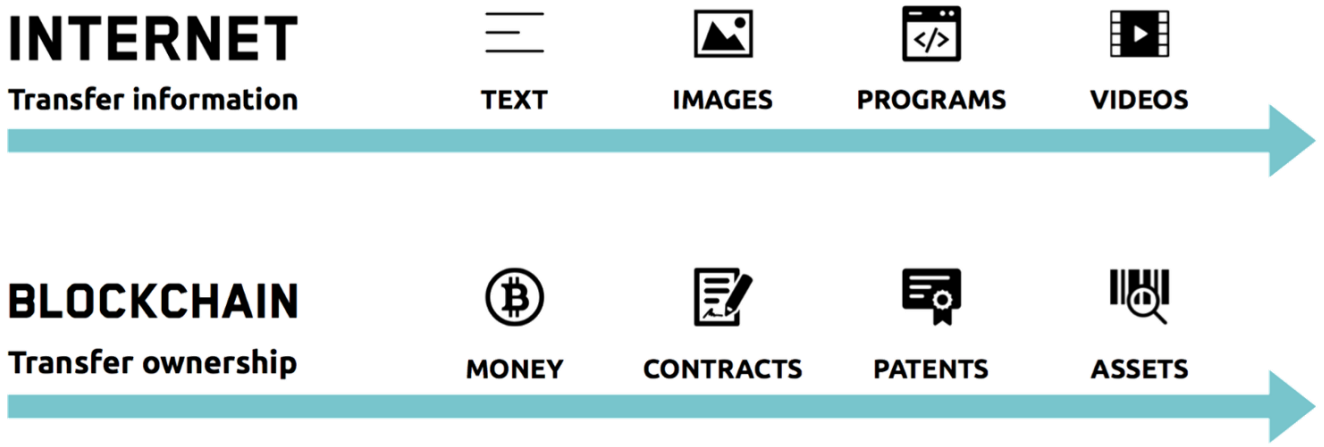

区块链
基础设施
公共平台
扩展应用
数字货币
记录保存
智能合约
数据密文存储
信息验证
积分、优惠券
电子契约防篡改
无纸化
慈善
众筹
投票
比特币及各种虚拟货币
转账
跨境支付
数字权益
博彩
托管支付


区块链
应用生态圈
金融
服务
医疗
健康
IP
版权
教育
物联网
共享
经济
通信
社会
管理
慈善
公益
文化
娱乐
支付、交易清结算、贸易金融、
数字货币、股权、私募、债券、
金融衍生品、众筹、信贷、
风控、征信
数字病历、隐私保护、健康管理
视频版权，音乐版权，软件防伪，
数字内容确权，软件传播溯源
社会公益
专利、著作权、商标保护、软件、
游戏、音频、视频、书籍许可证、
艺术品证明
代理投票、身份认证、
档案管理、公证、遗产
继承、个人社会信用、
工商管理
档案管理、学生征信、学历证明、
成绩证明、产学合作
社交、消息系统
租车、租房、
知识技能
物品溯源、物品仿伪、
物品认证、网络安全性、
网络效率、网络可靠性

12.1 区块链的概念

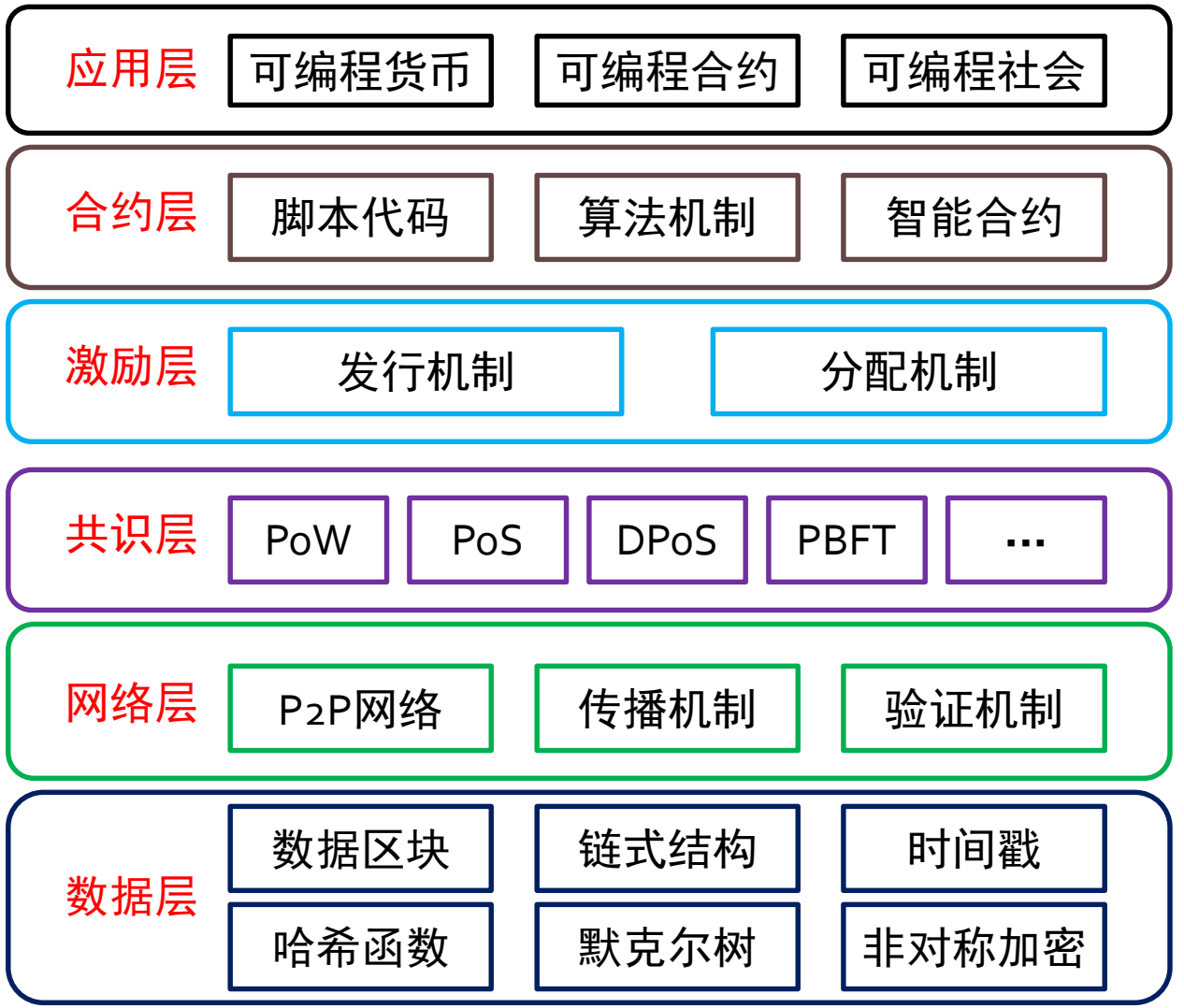
定义

- 区块链是一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式



12.1 区块链的概念

- 区块链六层参考架构

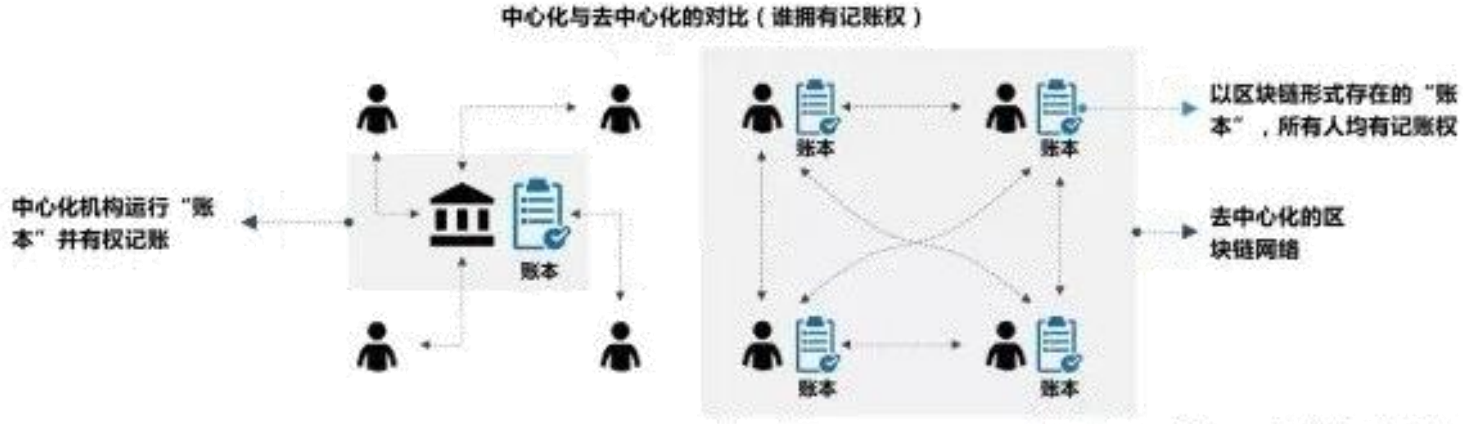


12.1 区块链的概念

区块链的特征

- 区块链实质是由多方参与共同维护一个持续增长的分布式数据库，也被称为分布式共享总账(distributed shared ledger)，其核心在于通过分布式网络、时序不可篡改的密码学账本及分布式共识机制建立彼此之间的信任关系，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，最终实现由信息互联向价值互联的进化

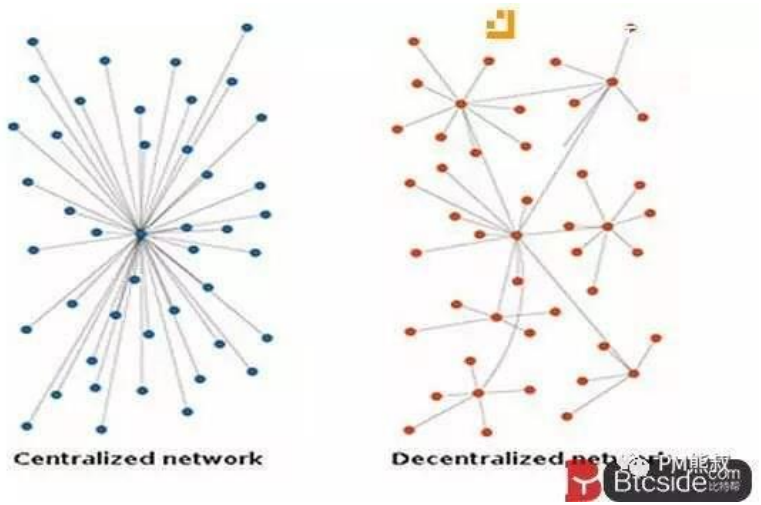
12.1 区块链的概念

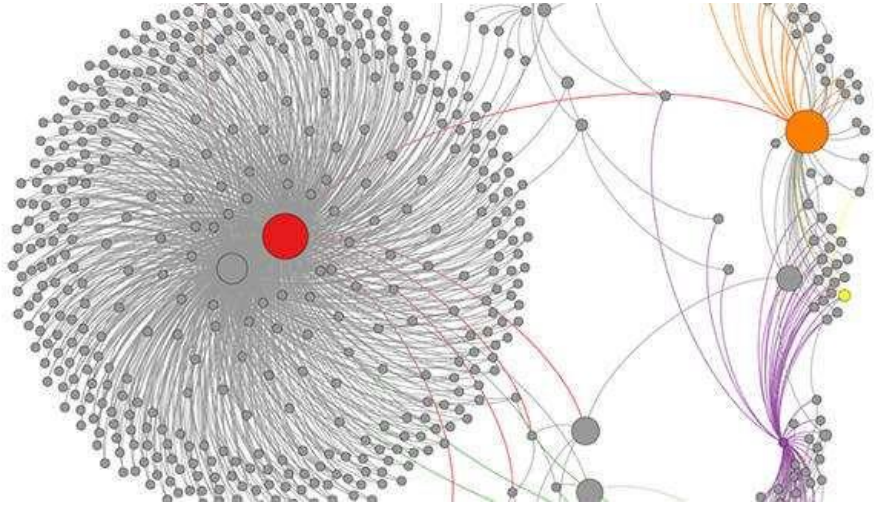


❋ 区块链的特征

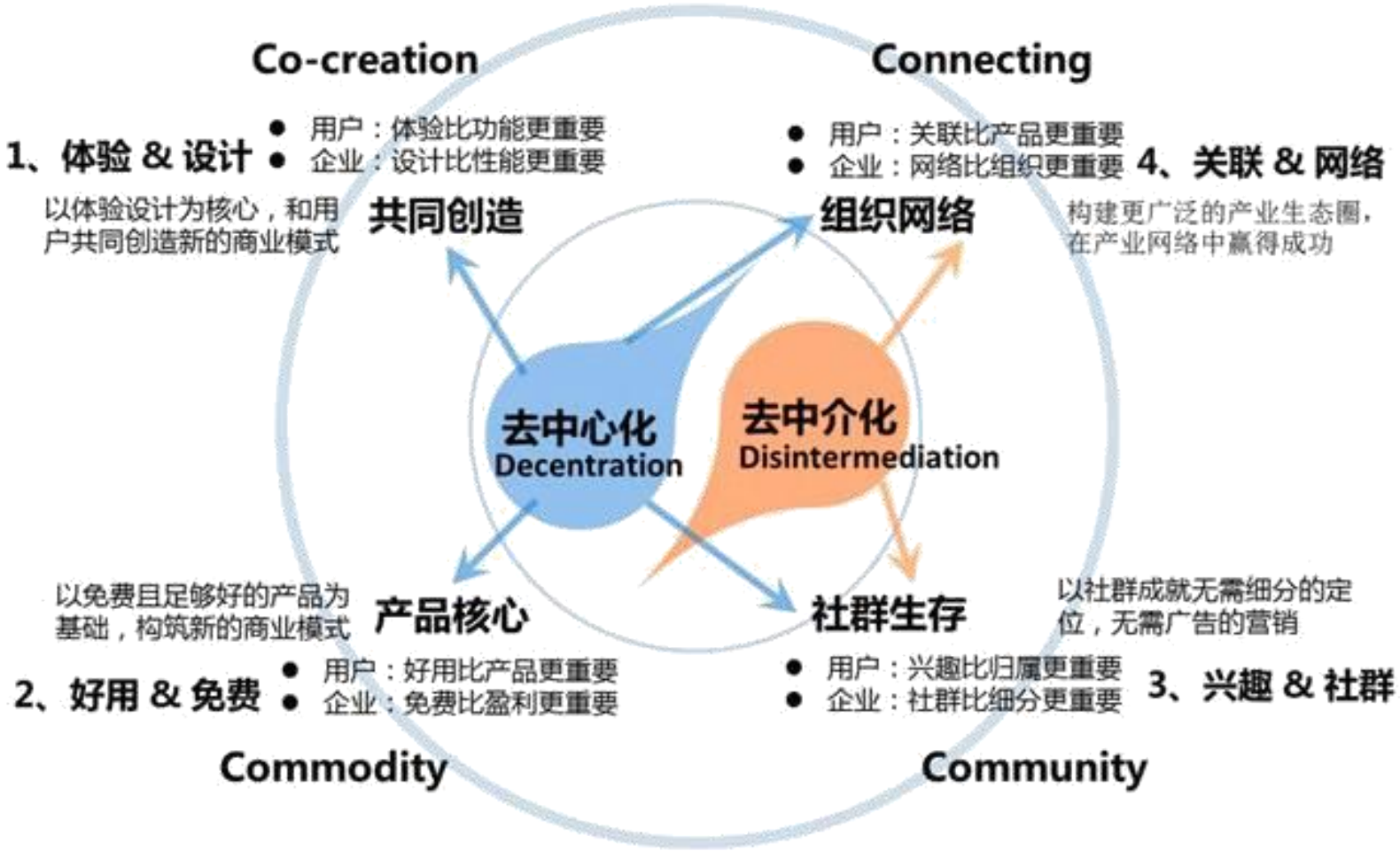
① 分布式结构

– 区块链构建在分布式网络基础之上，账本并不是集中存放在某个服务器或数据中心，也不是由第三方权威机构来负责记录和管理，而是分散在网络中的每一个节点，每一节点都有一个该账本的副本，所有副本同步更新，体现了去中心化的特点





12.1 区块链的概念

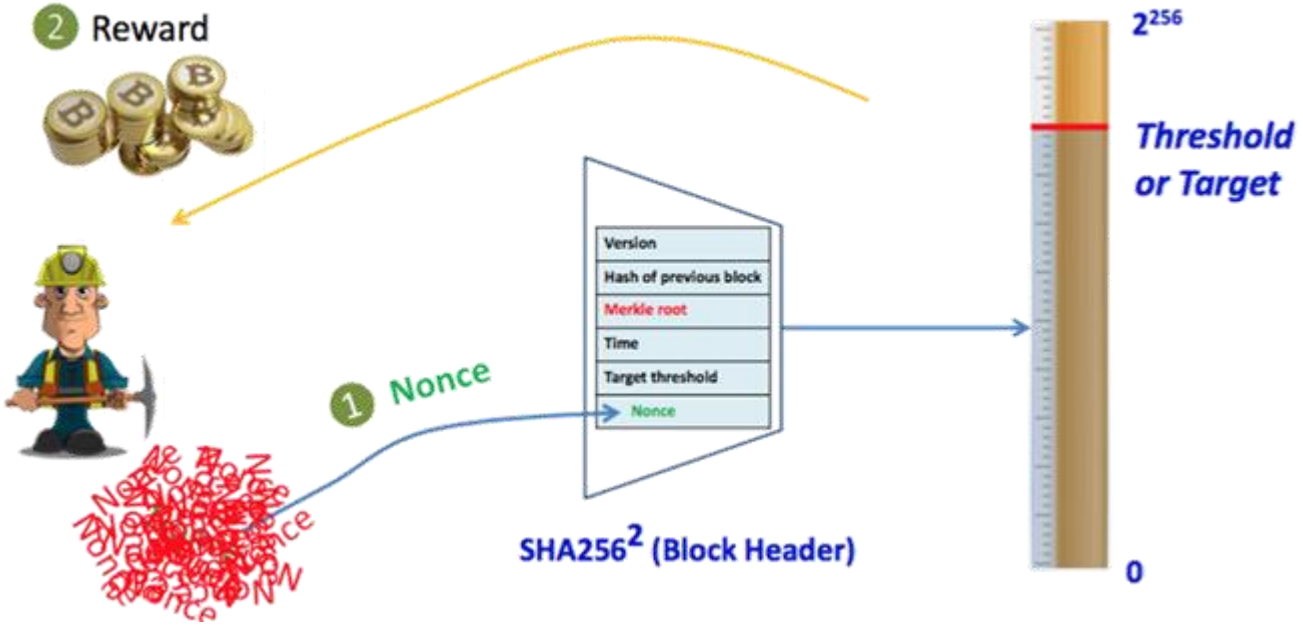

Co-creation
Connecting
1、体验 & 设计
用户：体验比功能更重要
企业：设计比性能更重要
以体验设计为核心，和用户共同创造新的商业模式
共同创造
组织网络
用户：关联比产品更重要
企业：网络比组织更重要
4、关联 & 网络
构建更广泛的产业生态圈，在产业网络中赢得成功
去中心化
Decentration
去中介化
Disintermediation
以免费且足够好的产品为基础，构筑新的商业模式
产品核心
社群生存
以社群成就无需细分的定位，无需广告的营销
2、好用 & 免费
用户：好用比产品更重要
企业：免费比盈利更重要
用户：兴趣比归属更重要
企业：社群比细分更重要
3、兴趣 & 社群
Commodity
Community

12.1 区块链的概念

❋ 区块链的特征

② 建立信任

– 区块链技术通过数学原理和程序算法，使系统运作规则公开透明，实现交易双方在不需要借助第三方权威机构（如央行等）信用背书下通过达成共识建立信任关系



12.1 区块链的概念

区块链的特征

③ 公开透明

– 区块链对任何可以上网的人是开放的、透明的。任何人都可以加入区块链，也能查询区块链上的区块记录；同时所有用户看到的是同一个账本，能看到这一账本所发生和记录的每一笔交易

交易记录 比特币交易的相关信息

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK

1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA 0.015 BTC

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK 0.0845 BTC

0.0995 BTC

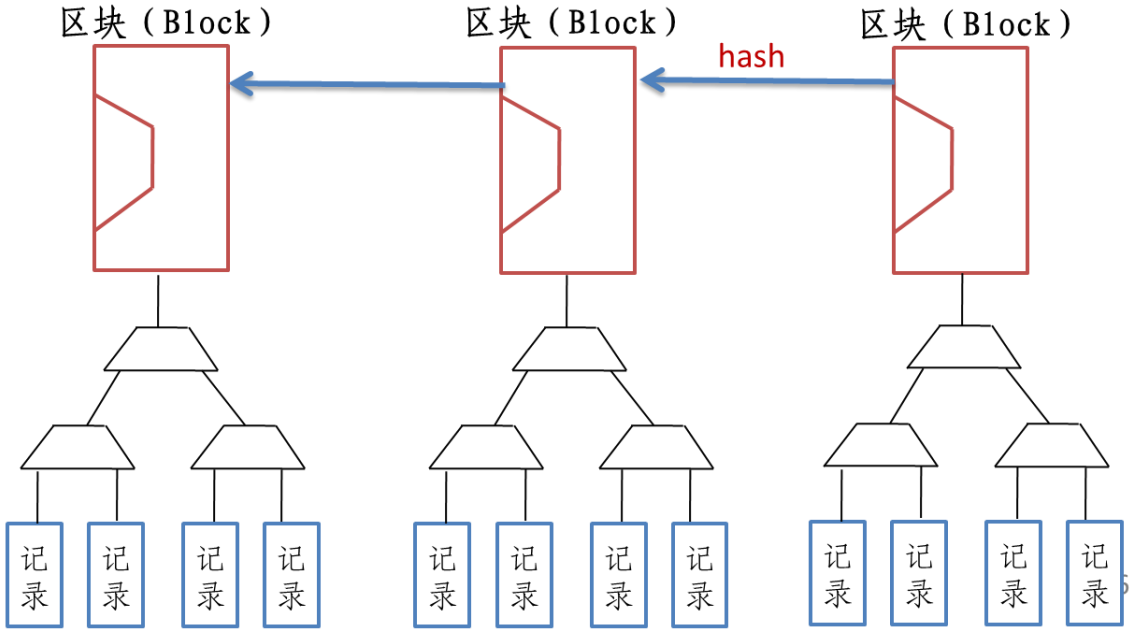
概览		转入与转出	
数据量	258 (字节)	转入总额	0.1 BTC
接收时间	2013-12-27 23:03:05	转出总额	0.0995 BTC
接纳区块	277316 (2013-12-27 23:11:54 + 9 分钟)	交易费	0.0005 BTC
确认	74648 确认	估计交易金额	0.015 BTC

12.1 区块链的概念

区块链的特征

④ 时序且不可篡改

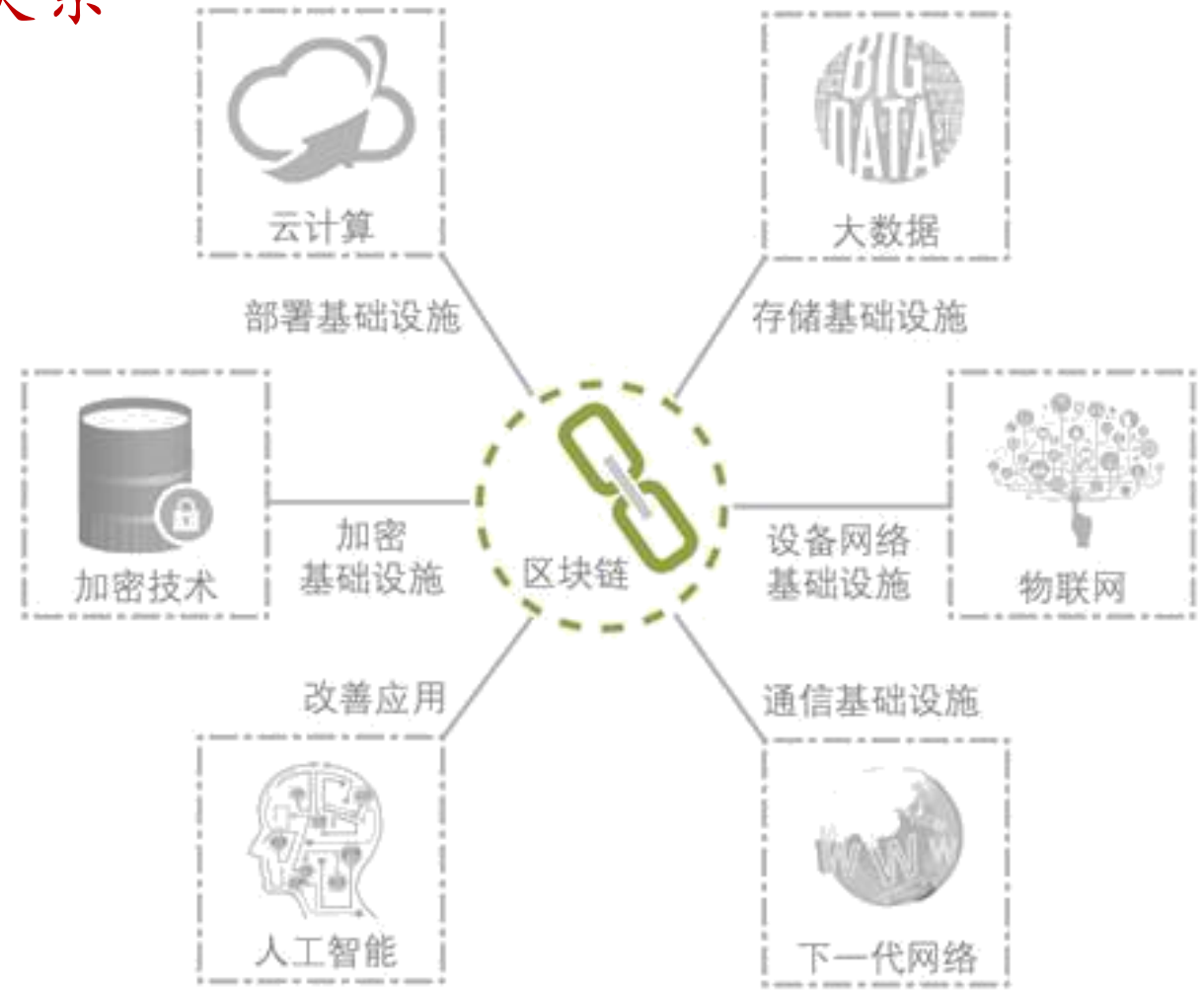
– 区块链采用带有时间戳的链式区块结构存储数据，具有极强的可追溯性和可验证性；同时，由密码学算法和共识机制保证了区块链的不可篡改性



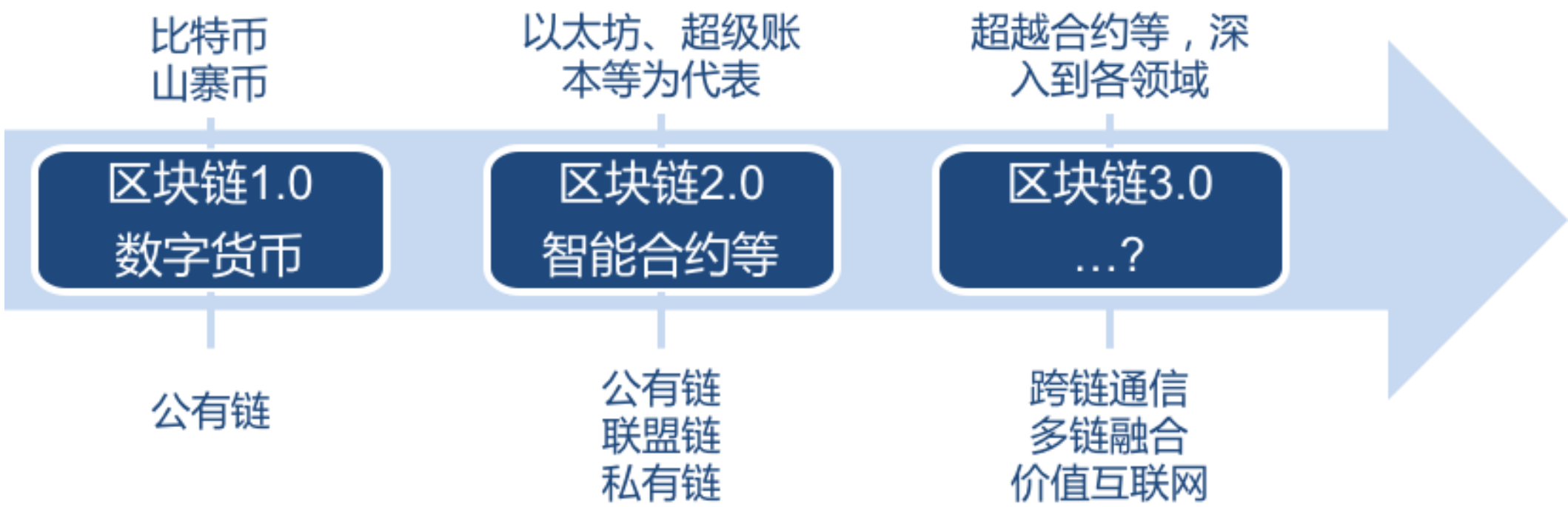
12.1 区块链的概念

- 区块链与新一代信息技术的关系

“十二五”确立的七大战略性新兴产业



12.2 区块链技术演化发展



12.2 区块链技术演化发展

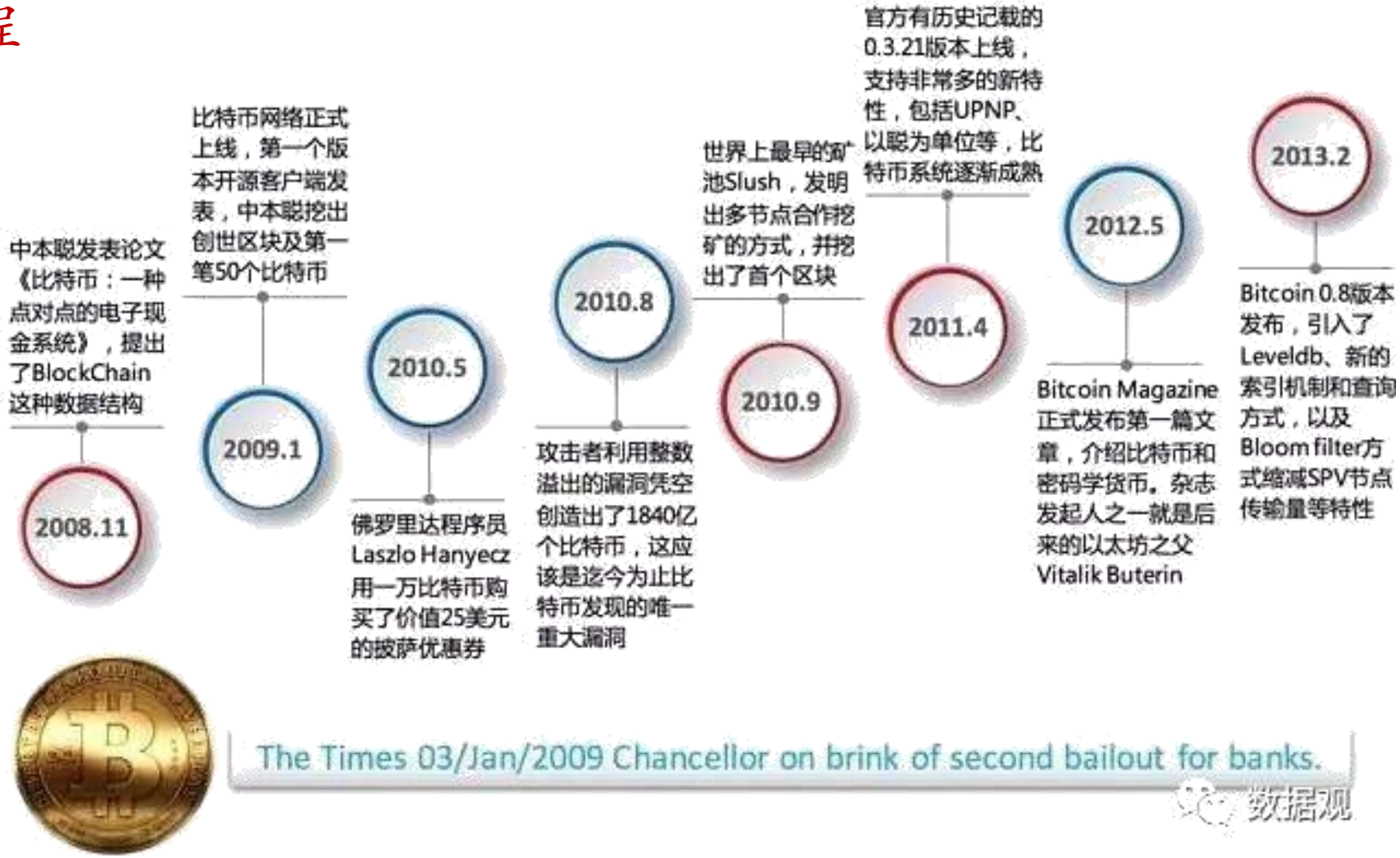
区块链1.0

工作原理

- 通过共识层的工作量证明生成新区块，并通过网络层向全网广播
- 经全网节点验证通过后，将奖励分配给相关节点，并将新生成的区块与之前区块通过哈希方式链接在一起
- 若要修改某个历史区块中的交易内容，则必须将该区块之前的所有区块的交易记录及密码学证明进行重构，而当区块达到一定的高度时几乎难以篡改

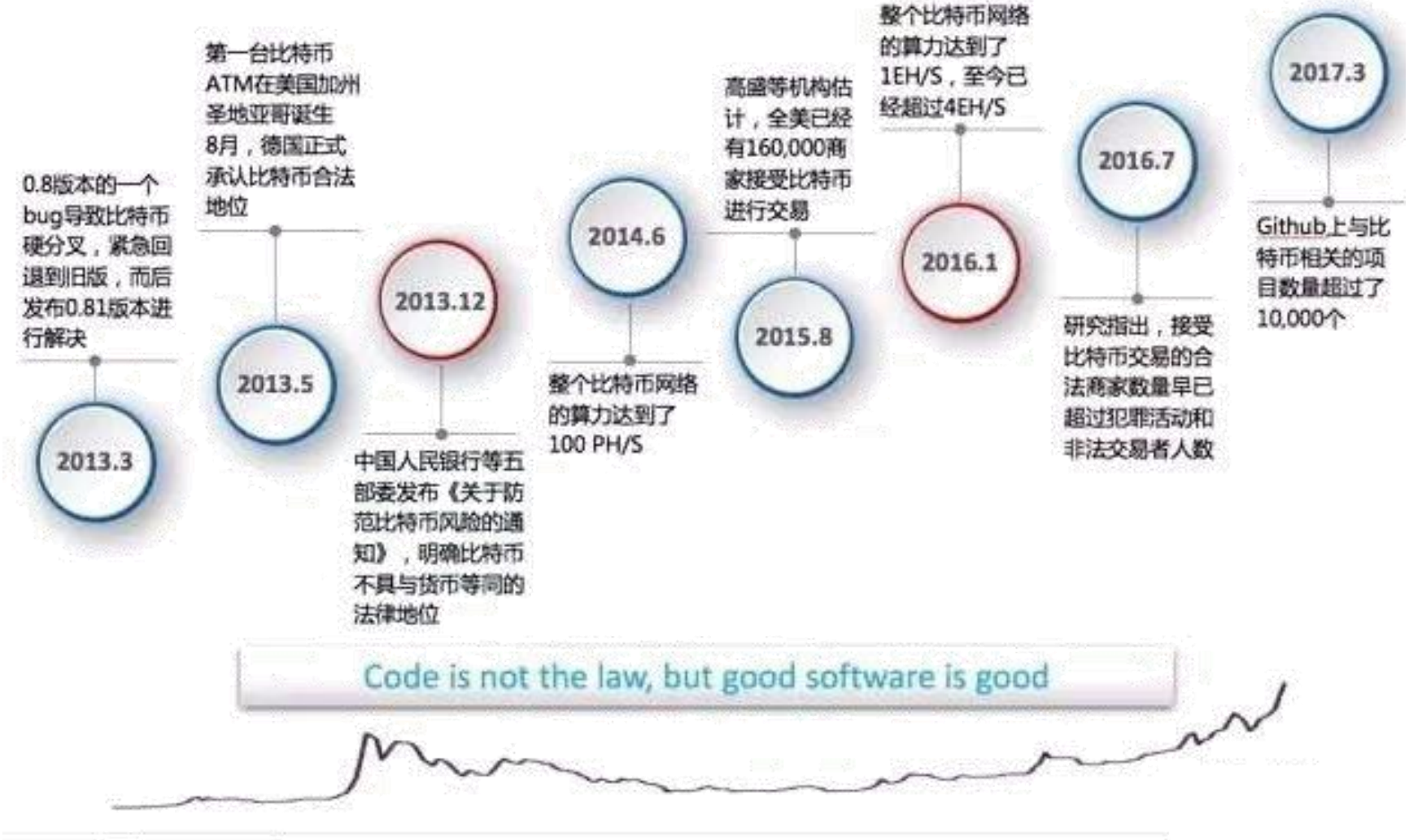
12.2 区块链技术演化发展

- 比特币发展历程



12.2 区块链技术演化发展

- 比特币发展历程



12.2 区块链技术演化发展

区块链2.0

- 区块链2.0是以以太坊（Ethereum）为代表的智能合约，是超越以比特币为代表的区块链1.0数字货币之外，在经济、市场和金融全方面的应用，包括股票、债券、期货、贷款、抵押、产权、智能财产等
- 若将区块链1.0看作“全球账簿”，区块链2.0则可看作“全球计算机”，其实现了区块链系统的图灵完备，可以在区块链上传和执行应用程序，并且程序的有效执行能得到保证，在此基础上实现了智能合约的功能

12.2 区块链技术演化发展

- 以太坊发展历程

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

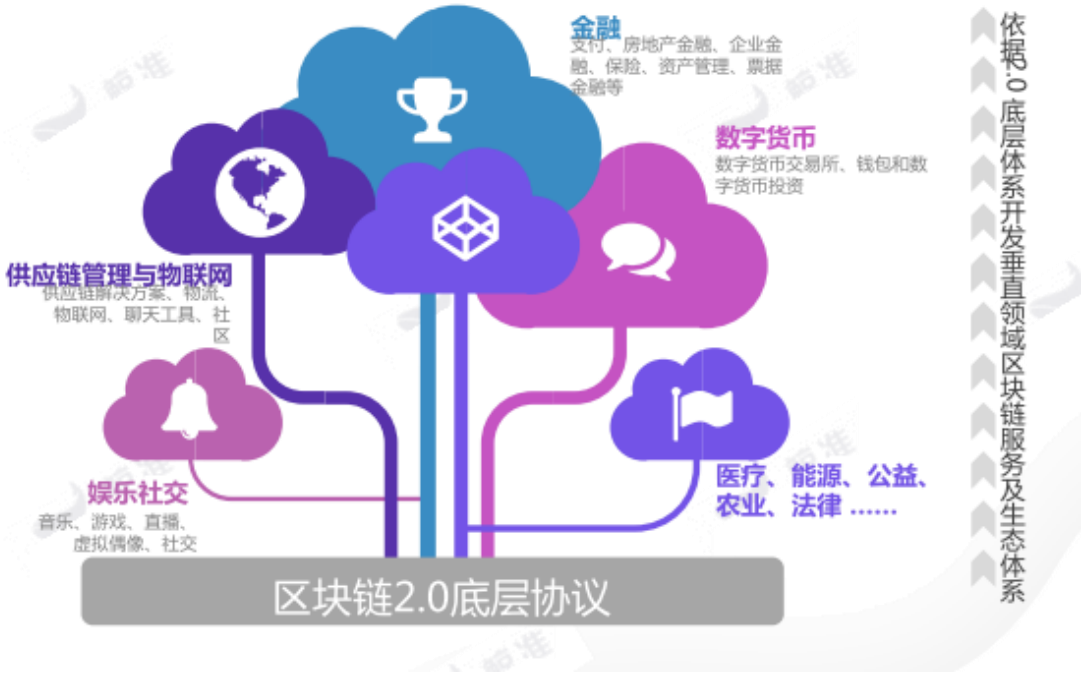
2016.3 Homestead版本发布

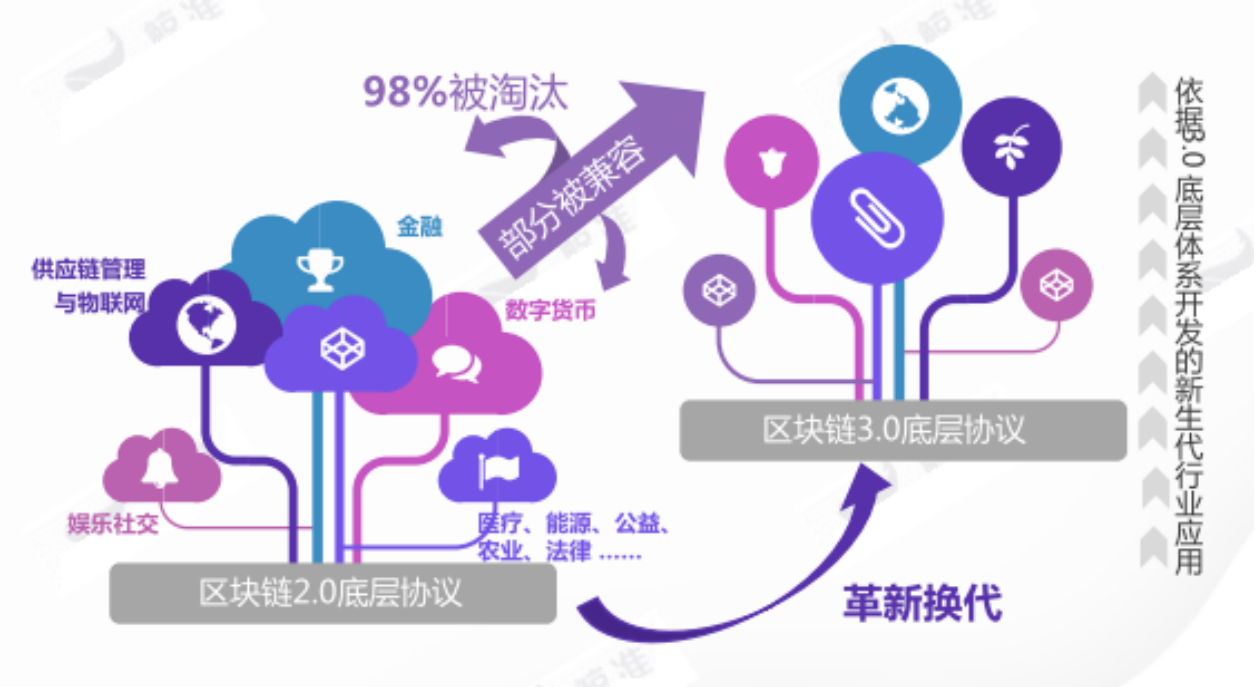
同年6月，著名的The DAO被攻击事件发生，以太坊硬分叉，出现了ETC和ETH并行

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

12.2 区块链技术演化发展





12.2 区块链技术演化发展

- 区块链技术的局限性
  - 政府监管挑战
  - 运行安全风险
  - 系统效率问题
  - 可扩展性问题
  - 隐私泄露风险

12.2 区块链技术演化发展

区块链技术发展趋势

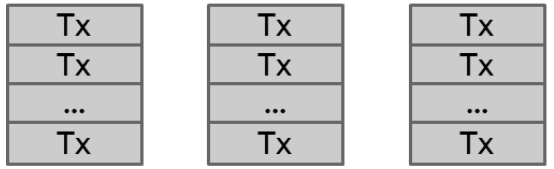
- 区块链行业应用加速推进，从数字货币向非金融领域逐步扩展
- 企业应用是区块链的主战场，联盟链/私有链将成为主流
- 应用催生多样化的技术方案，区块链性能将不断得到优化
- 区块链与云计算的结合越发紧密，BaaS（BlockChain-as-a-Service）有望成为公共信任基础设施
- 区块链安全问题日益凸显，安全防护需要技术和管理全局考虑
- 区块链的跨链需求增多，互联互通的重要性凸显
- 区块链竞争日益激烈，专利争夺成为竞争重要领域
- 区块链投资持续火爆，代币众筹模式累积风险值得关注
- 区块链技术与监管存在冲突，但矛盾有望进一步调和，区块链技术未来将逐步适应监管政策要求，逐步成为监管科技（RegTech）的重要工具
- 区块链虽在数学上具有完备性，但也存在安全问题，未来还需要从工程和管理等层面加强安全，也需要标准提升可信程度

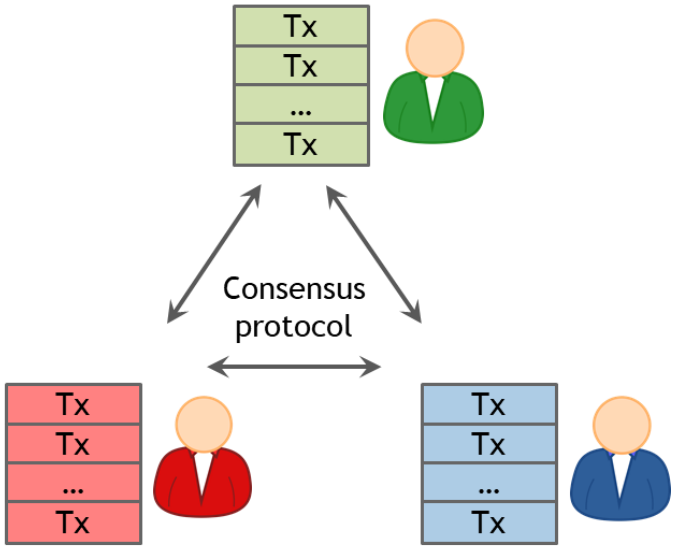
12.3 分布一致性

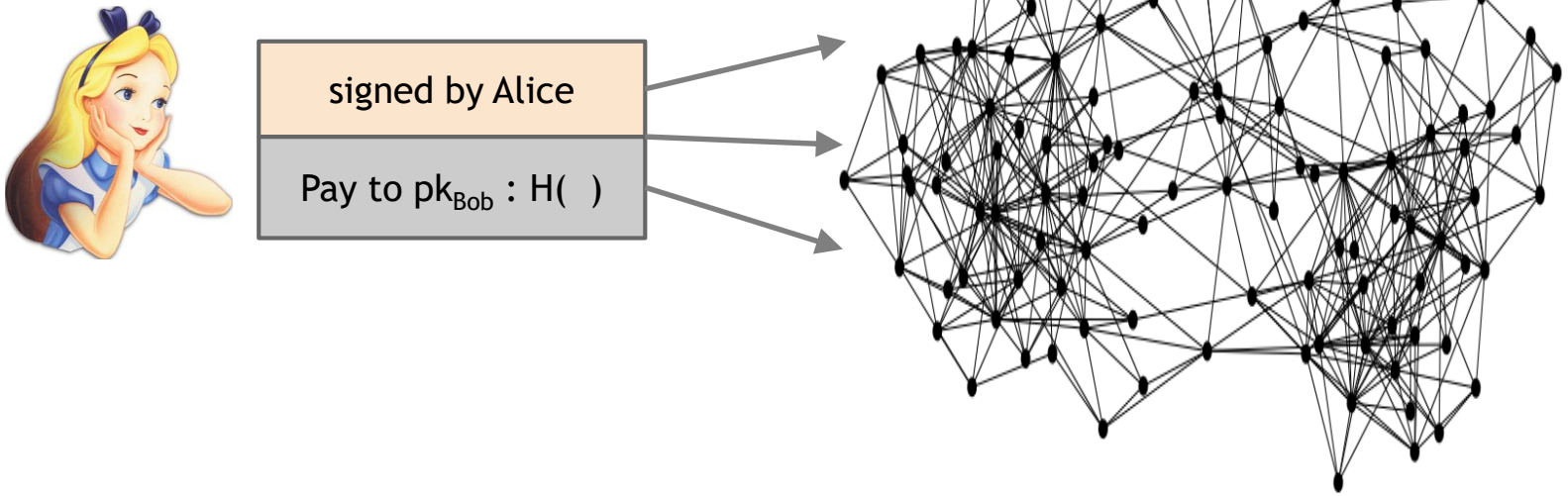
- 伴随"去中心化"出现的问题
  - 谁来维护交易账本?
  - 谁有权验证交易是否合法?
  - 谁发行新的比特币?
  - 谁决定系统规则改变?
  - 比特币如何获得交易价值?

12.3 分布一致性

- 比特币是Peer-to-Peer系统







12.3 分布一致性

分布一致性

- 存在n个节点，其中有一些节点可能是错误的、不合法的或恶意的（faulty or malicious）。一个分布式共识协议（Distributed consensus protocol）需要满足下列两个条件：
  - 所有诚实节点最终达成一致
  - 最终决定是由诚实节点生成的

12.3 分布一致性

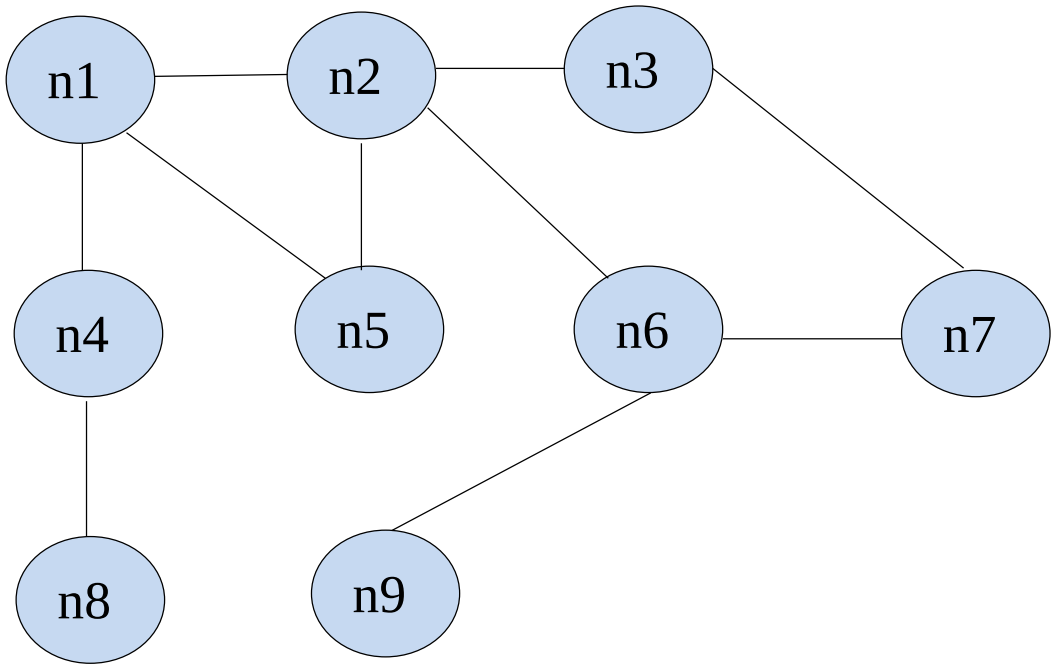
对等网络

- 对等网络（Peer-to-Peer，简称P2P）是一种分布式网络，网络的参与者共享它们所拥有的CPU、存储等硬件资源
  - P2P网络中各节点的计算机地位平等，每个节点既是资源提供者（服务器），又是资源获取者（客户端）
  - 所有节点间通过特定的软件协议共享计算资源、软件或者信息内容
  - 共享资源能被其它对等节点直接访问而无需经过中间实体

12.3 分布一致性

对等网络

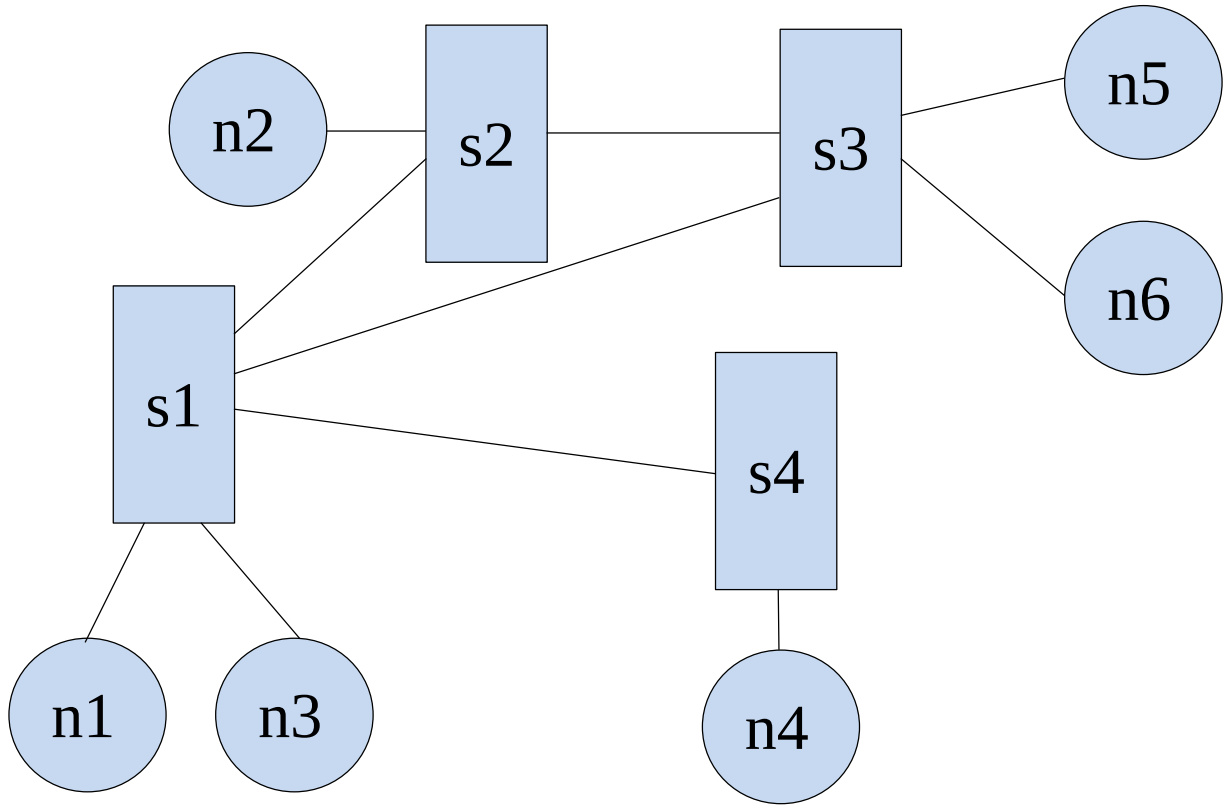
- 全分布式P2P
  - 每个节点的功能完全对等，既为客户端又为服务器，节点间的连接是任意的，其拓扑结构没有规则的几何形状



12.3 分布一致性

对等网络

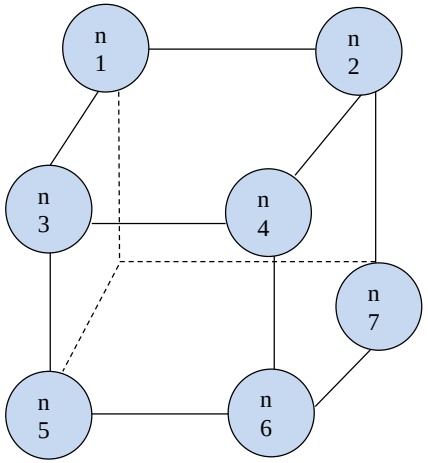
- 混合式P2P
  - 节点分为超级节点（super）和普通节点（normal）两种类型



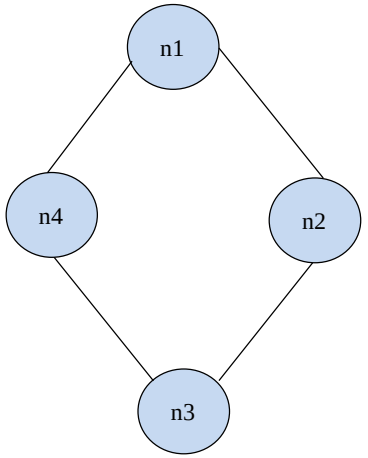
12.3 分布一致性

对等网络

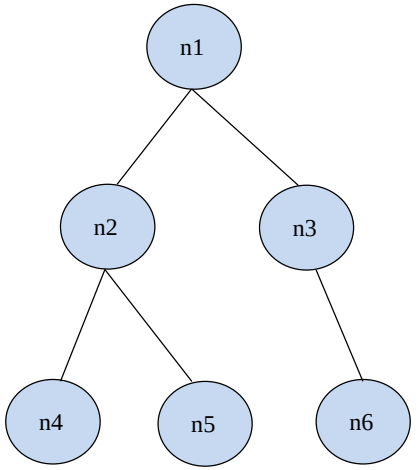
- 结构化P2P
  - 节点按一定的规则选择邻居节点并进行连接，所形成的拓扑结构为规则的几何形状，如立方体结构、环状结构、树状结构等



立方体结构



环状结构

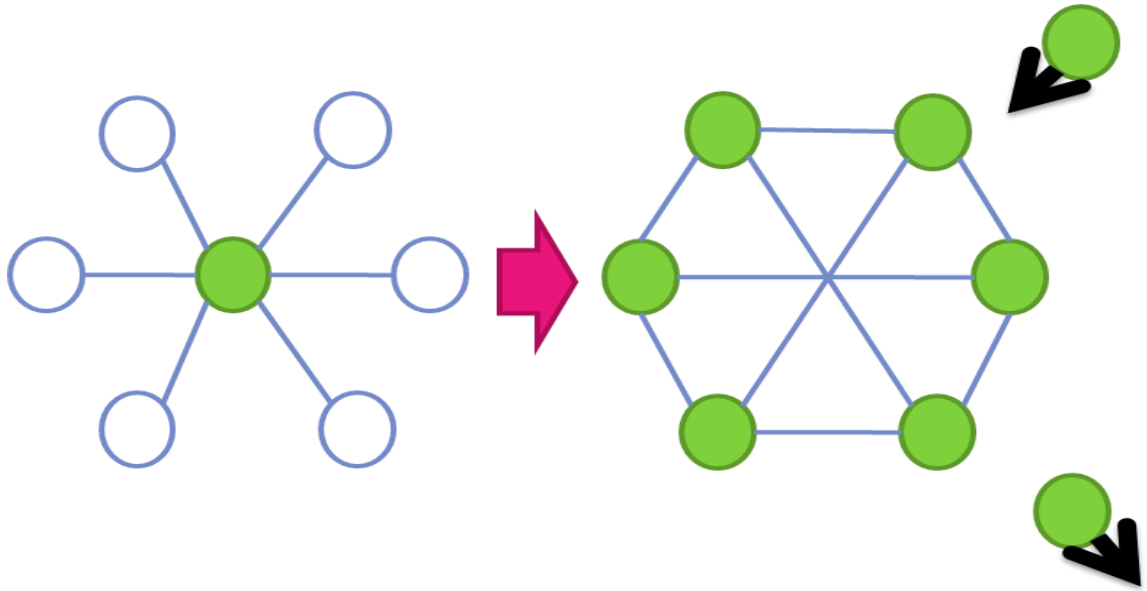


树状结构

12.3 分布一致性

对等网络在区块链中的应用

- 对等网络技术是区块链系统连接各对等节点的组网技术，是构成区块链技术架构的核心技术之一
  - 公有链可采用全分布式P2P结构
  - 联盟链和专有链可采用混合式P2P结构



12.3 分布一致性

分布一致性协议

- 区块链采用的是分布式架构，而一致性是分布式系统的基础研究问题，也是区块链系统的基础研究问题。
  - 分布式系统对一致性的要求是：数据和其副本达到完全相同的状态
  - 一致性协议定义了在一个分布式系统中哪些操作被认为是正确的，或者是定义了以何种顺序执行操作可以保持分布式系统中数据的正确性

12.3 分布一致性

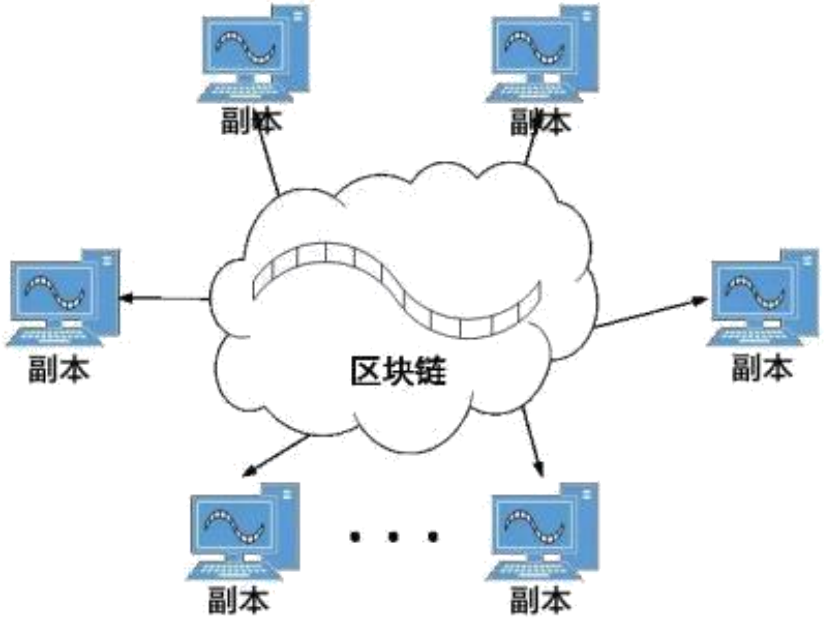
分布一致性协议

- **以客户为中心**的一致性协议从系统外部服务请求发起者的角度来考虑一致性问题。系统是一个只对外部提供服务接口、完全屏蔽内部实现细节的黑盒
- **以数据为中心**的一致性协议关注分布式系统的内部状态，即副本之间的进程同步问题和操作的执行顺序问题。这种视角假设并发进程可能同时修改副本，系统需要在这种情况下保持一致性

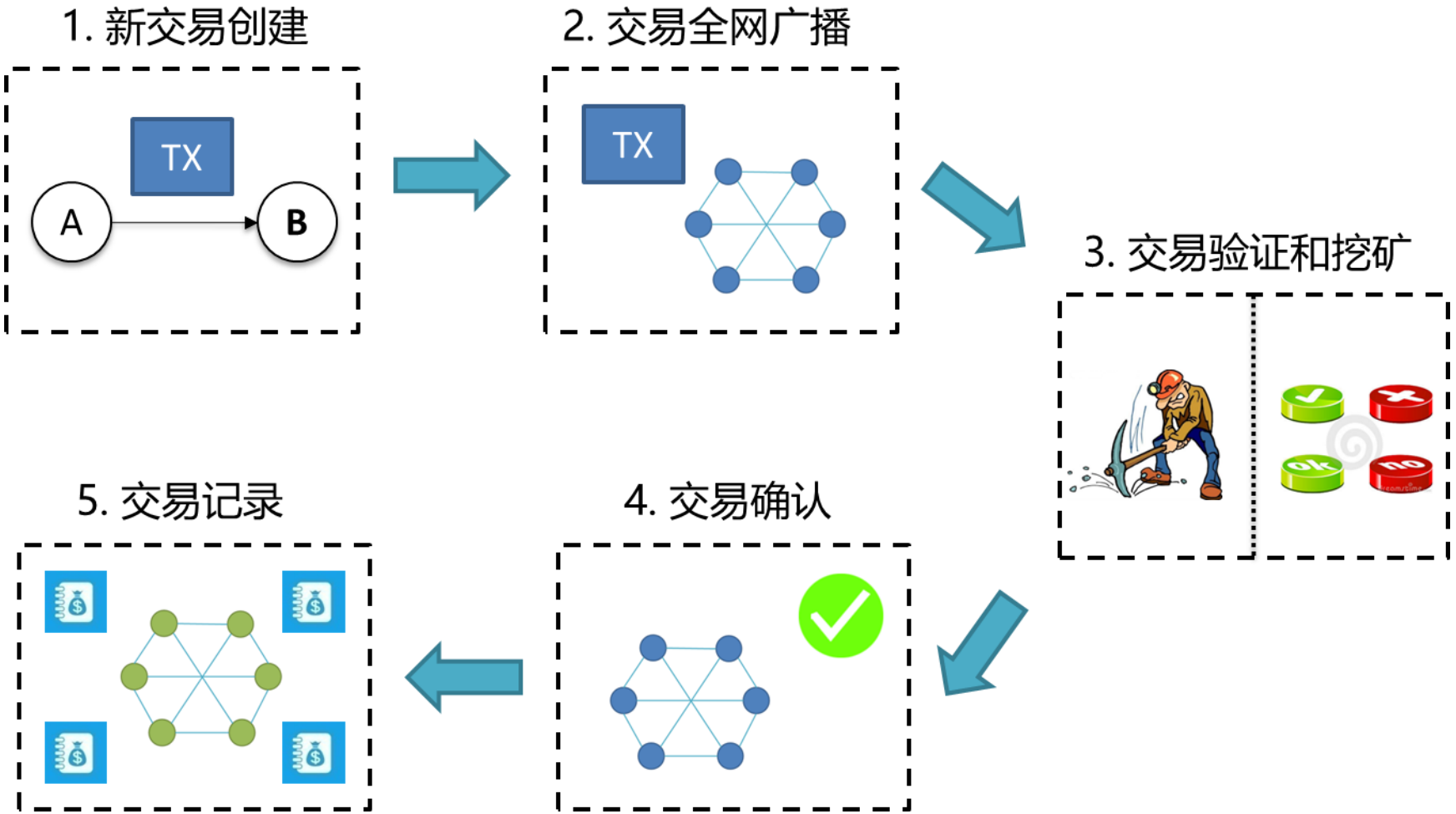
12.3 分布一致性

区块链中的一致性

- 区块链中的一致性是通过网络中成千上万个独立节点异步交互而达到的，它是比特币中不依赖于中心机构的交易、支付和安全模型的实现基础
- 区块链中的一致性来自于节点上独立执行的四种过程的相互作用
  - 每次交易的独立验证
  - 挖掘节点独立地集成交易到新区块中
  - 每个节点对新区块独立验证并组装成区块链
  - 每个节点基于工作量证明独立地选择具有最多计算量的区块链



12.4 比特币如何交易



12.4 比特币如何交易

比特币交易

- 比特币交易的本质是一个包含交易发送方、接收方、资产转移相关信息的数据结构，包含了一笔资金从初始点（输入值）转移至目标地址（输出值）的信息

字段	大小	描述
版本	4字节	明确这笔交易参照的规则
输入数量	1-9字节	交易输入（TxIn）列表中交易的数量
输入列表	不定	一个或多个交易输入
输出数量	1-9字节	交易输出（TxOut）列表中交易的数量
输出列表	不定	一个或多个交易输出
锁定时间	4字节	一个UNIX时间戳或区块号

12.4 比特币如何交易

比特币交易

- 比特币交易中每一笔交易的输入必然是之前某笔交易未花费的输出（UTXO，Unspent Transaction Outputs），同时每一笔输入也需要上一笔输出所对应的私钥进行签名
- 交易构成了一个链式结构，所有合法的比特币交易都可以追溯到前一个或多个交易的输出
- 比特币可以被分割成表示八位小数的“聪”，一个UTXO可以是一“聪”的任意倍
- Coinbase交易

12.4 比特币如何交易

交易记录 浏览比特币交易的相关信息

7c402505be883276b833d57168a048cfdf306a926484c0b58930f53d89d036f9

1AnLpMkAmf7jy2BNkP3oYw1phzhNuLws7M (0.32 BTC - 输出) → 1GJYiog3ato17SSTFCCdkZ44H6LdkW9j1V - (已使用) 0.319 BTC

0.319 BTC

概览	
大小	224 (字节)
接收时间	2013-08-05 18:45:14
在区块内	250399 (2013-08-05 19:01:11 + 16 时间)
确认	226072 确认
播报方IP地址	70.69.229.109 (whois)
可视化	浏览树状图

输入与输出	
输入总额	0.32 BTC
输出总额	0.319 BTC
交易费	0.001 BTC
每字节费用	446.429 sat/B
预计比特币成交	0.319 BTC
脚本	隐藏交易脚本 & Coinbase信息

输入脚本

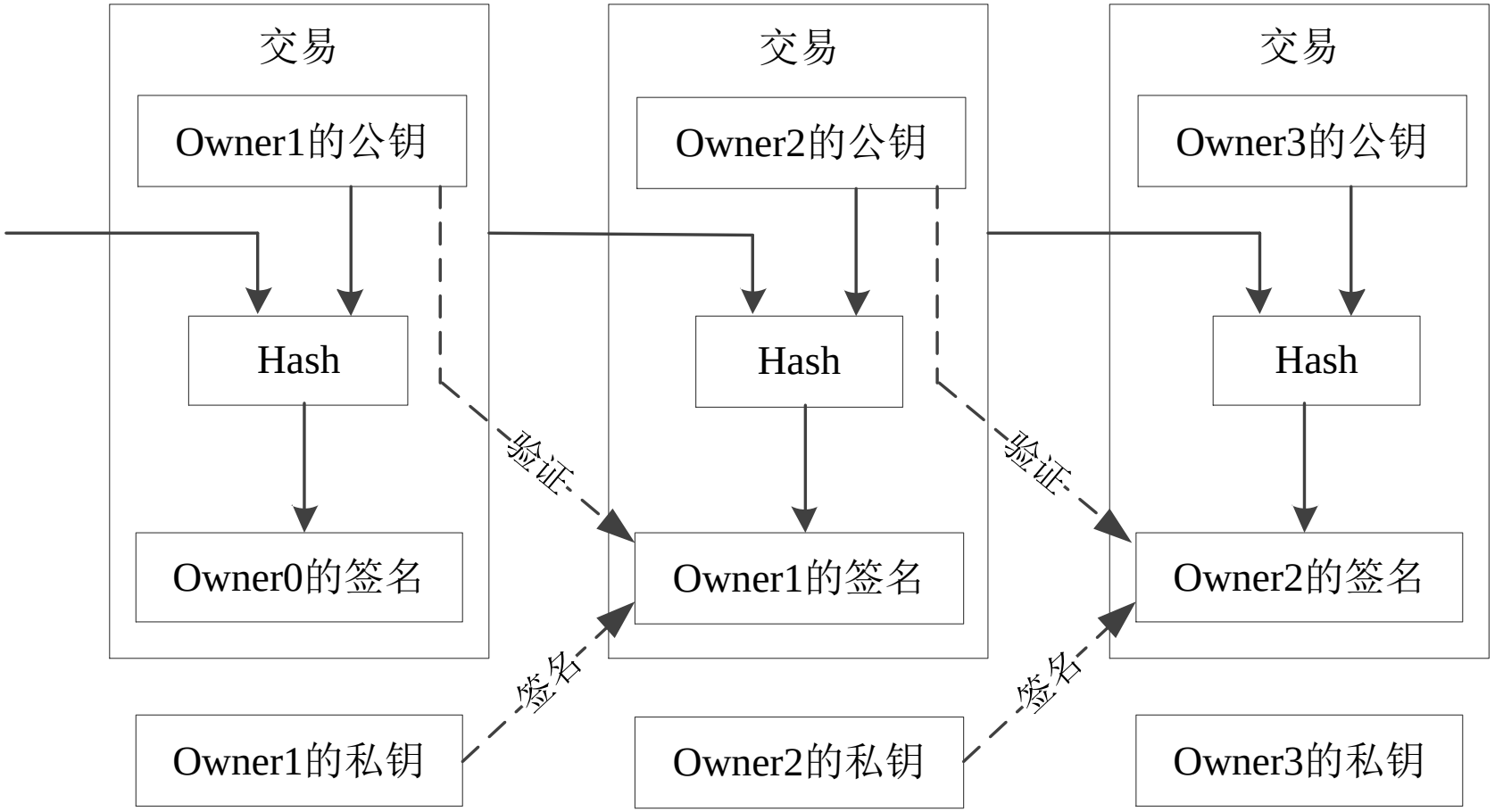
304502205014856cdf89da70ad9a4f223bac4e5477da5c6cb69ef2b9f8b5f8548e21307e0221009bfe2698f1eb1c561f41981d8e78c11d9e685a70e682f144ee6c8ab5ecb0497c01
042b2d8def903dd62d0c4161ed8d4ccfa5967e11a28e65cb141235b7c27d8ef6aa3bd63be077323cf3d7e0e8895b264b94feb4b40478b431da6f45dfc8e1004f62 确认

输出脚本

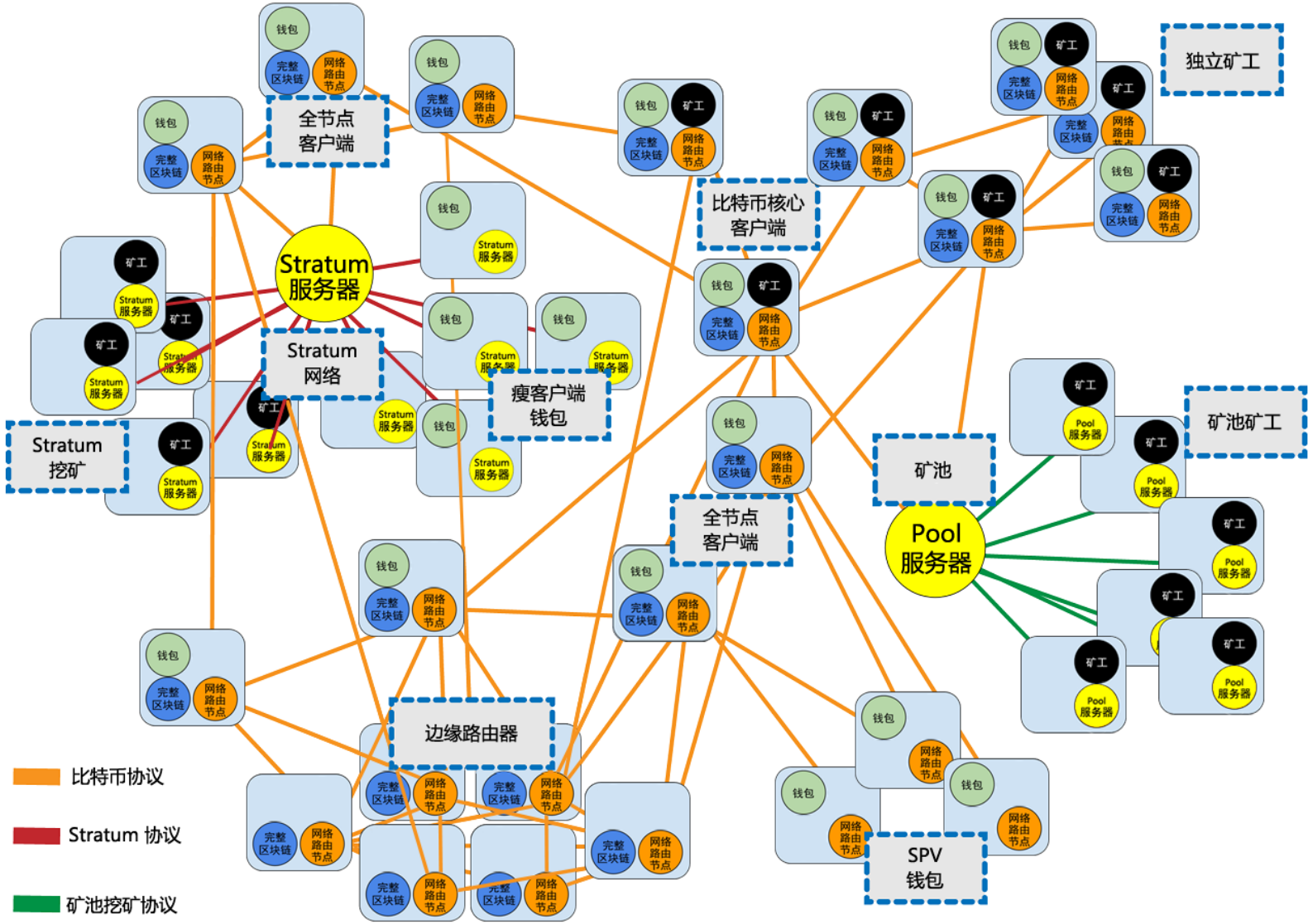
OP_DUP OP_HASH160 a7db6ff121871c65a8924b8e40f160d385515ad7 OP_EQUALVERIFY OP_CHECKSIG 确认

12.4 比特币如何交易

- 比特币交易链

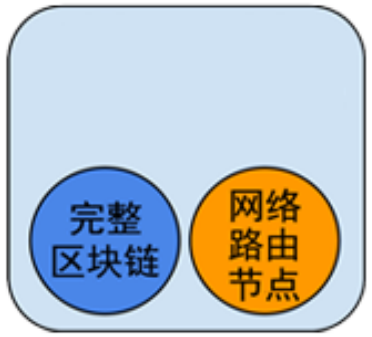


12.4 比特币如何交易


钱包
完整区块链
网络路由节点
矿工
全节点客户端
独立矿工
比特币核心客户端
Stratum服务器
Stratum网络
瘦客户端钱包
Stratum挖矿
矿池
矿池矿工
Pool服务器
全节点客户端
边缘路由器
SPV钱包
比特币协议
Stratum 协议
矿池挖矿协议

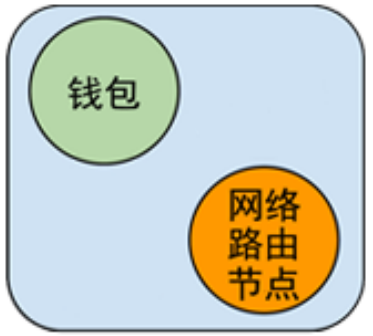
12.4 比特币如何交易

(1) 比特币核心



(2) 完整区块链节点

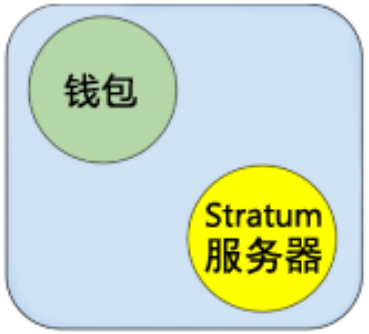
(3) 独立矿工



(4) 轻量(SPV) 钱包

(5) 矿池协议服务器

(6) 挖矿节点



(7) 轻量Stratum钱包

The End