Introduction to Block Chain

ZHAO, Peng

May 30, 2018

DLUT WilNa Lab

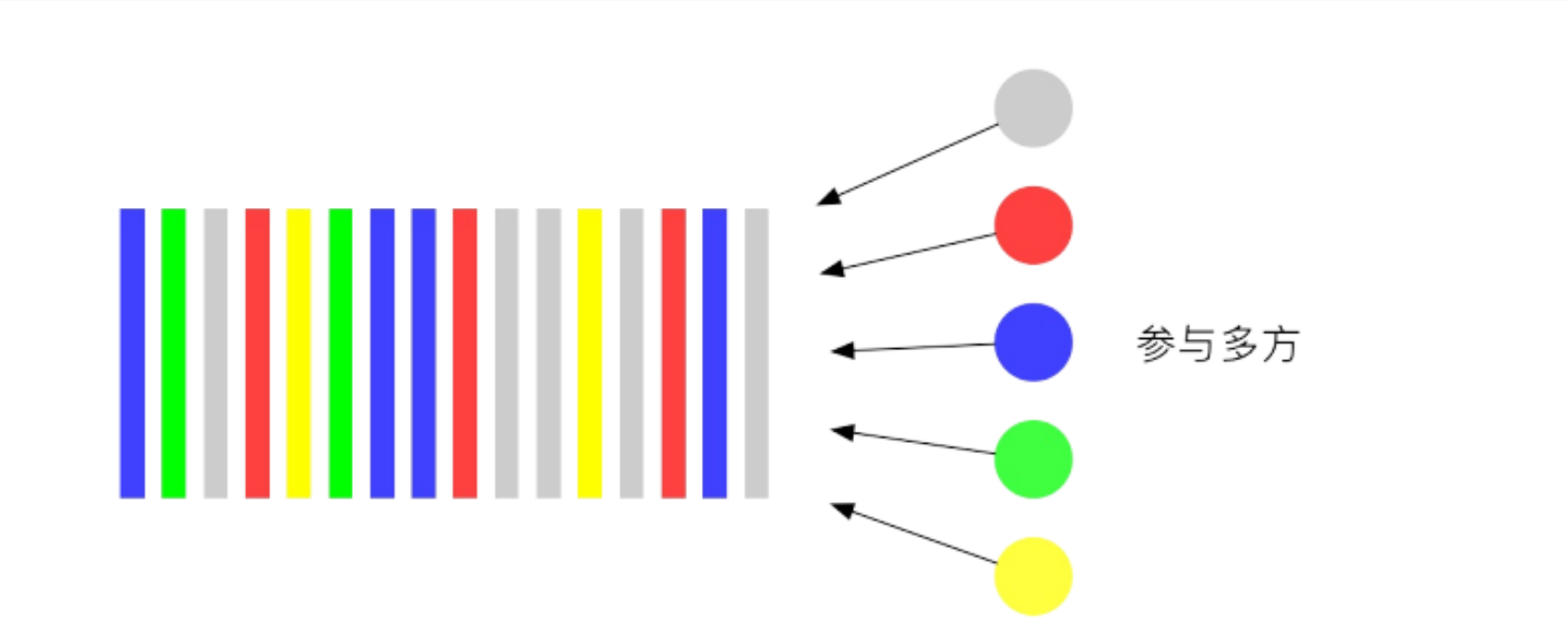
目录

账本技术

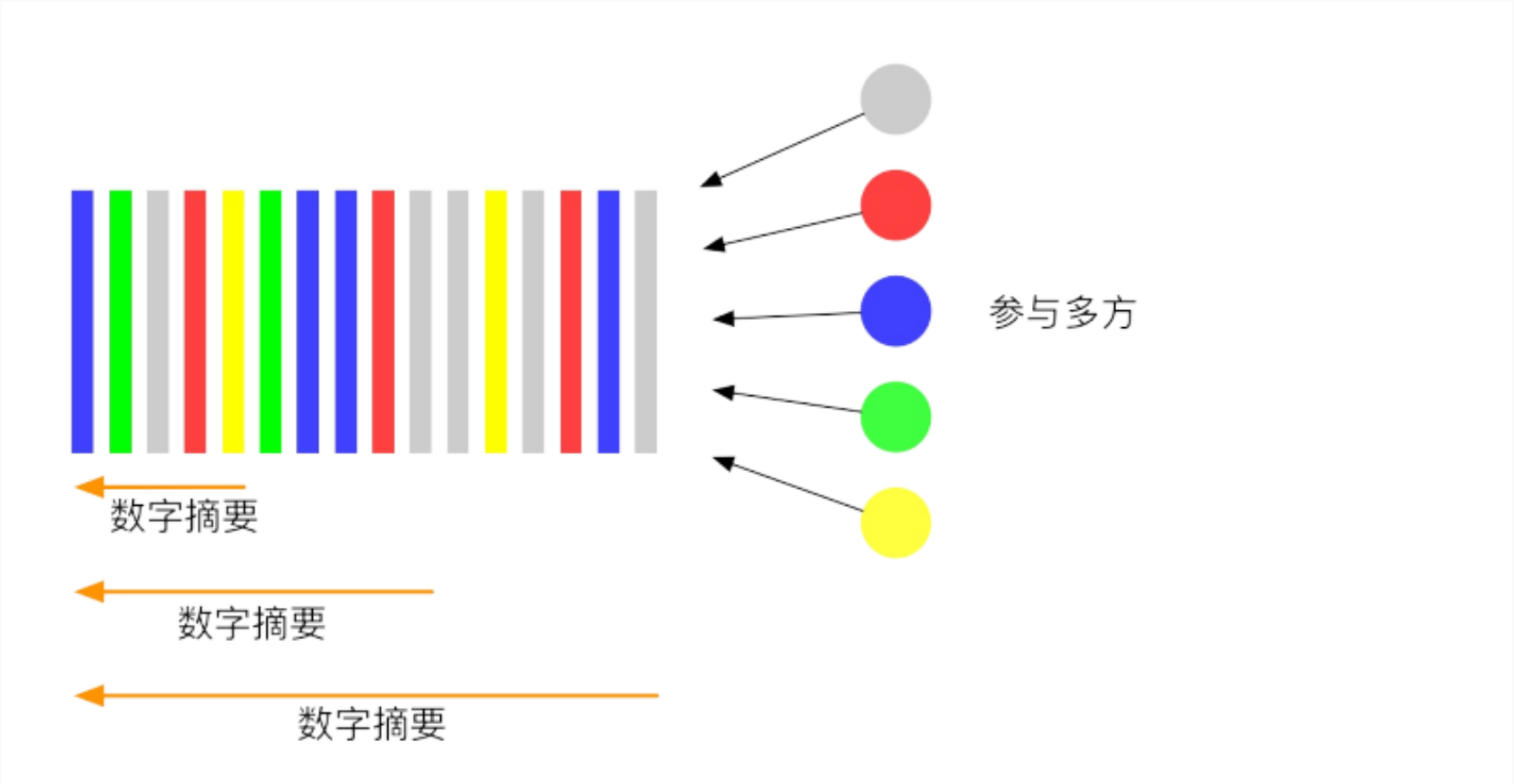
发展

- 单式记账法
- 复式记账法
- 数字化记账法
- 分布式记账法

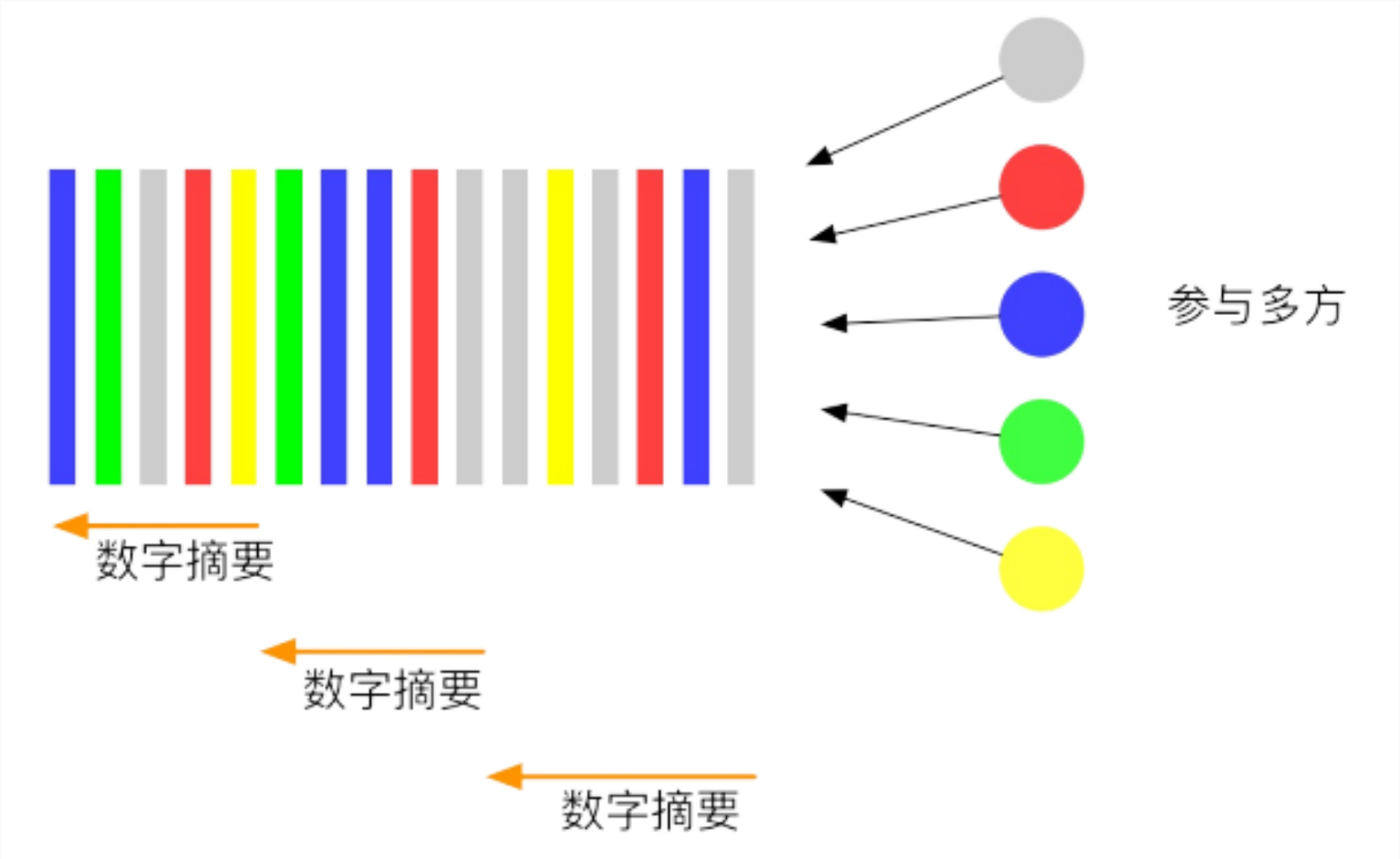
分布式记账法与区块链



分布式记账法与区块链



分布式记账法与区块链

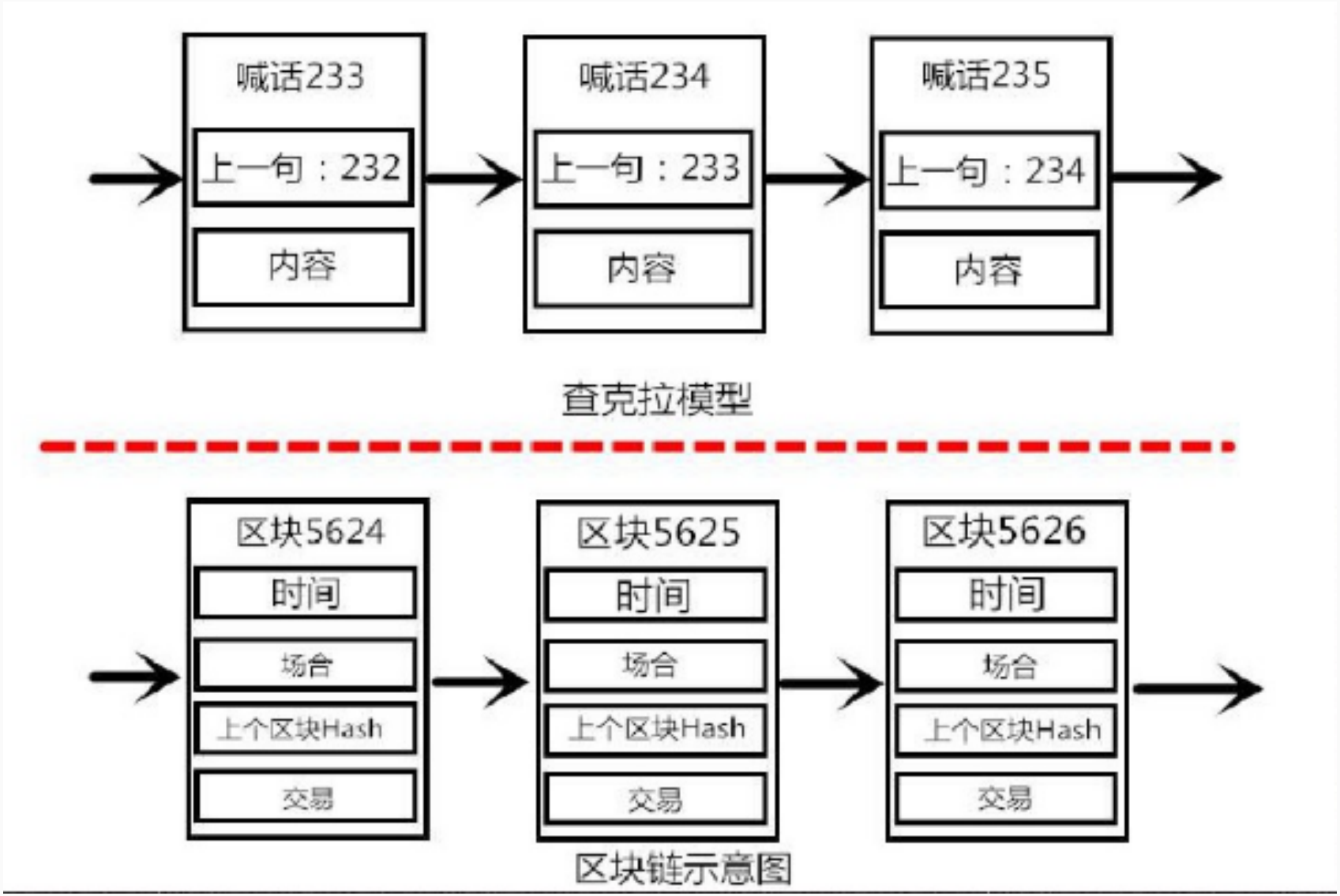


区块链

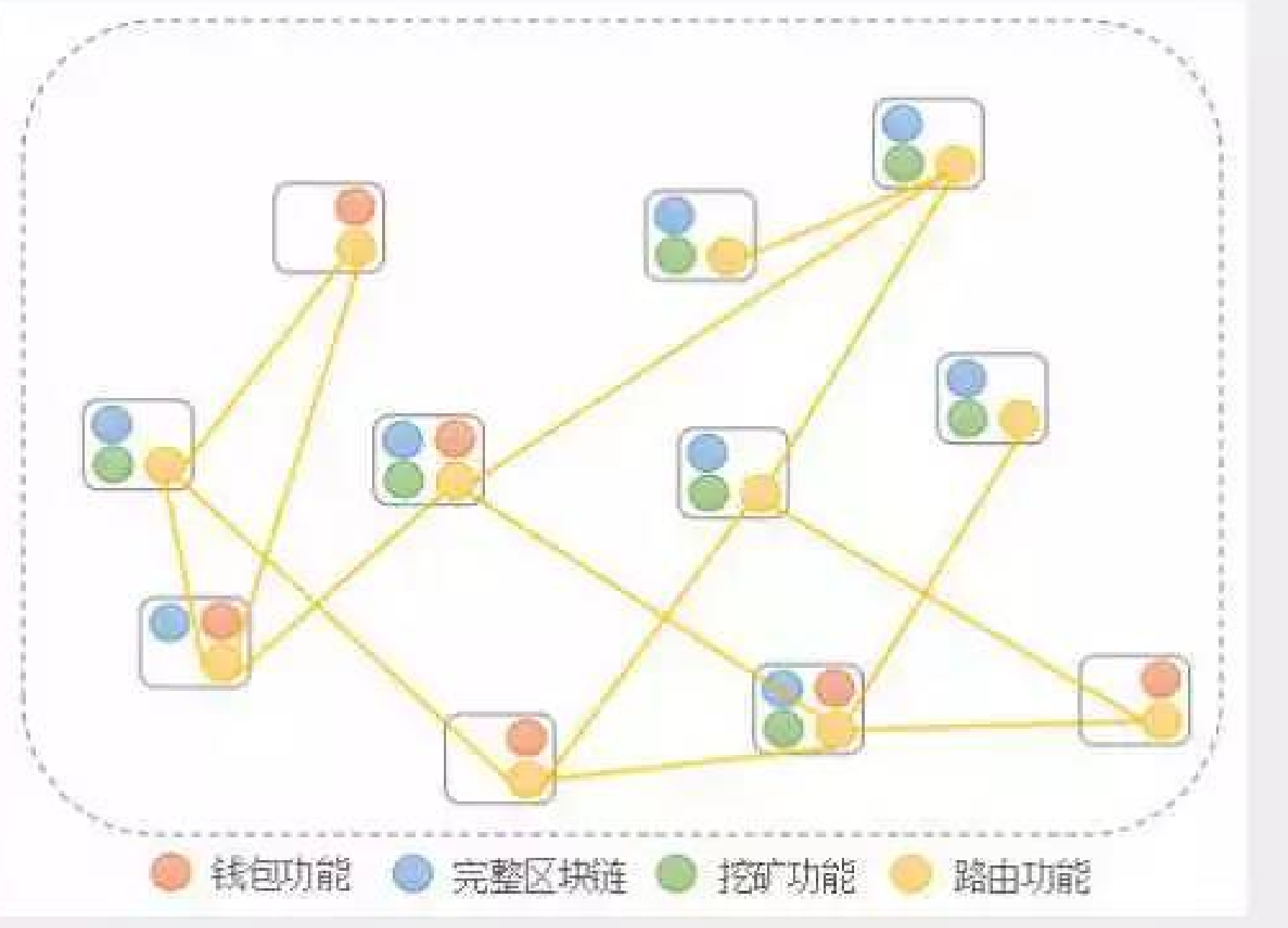
定义

- 区块链是一个分布式账本，一种通过去中心化、去信任的方式集体维护一个可靠数据库的技术方案
- 交易 transaction
- 区块 block
- 链 chain

结构


喊话233
上一句：232
内容
喊话234
上一句：233
内容
喊话235
上一句：234
内容
查克拉模型
区块5624
时间
场合
上个区块Hash
交易
区块5625
时间
场合
上个区块Hash
交易
区块5626
时间
场合
上个区块Hash
交易
区块链示意图

网络



优点

- 分布式容错性: 分布式网络极其鲁棒，能够容忍部分节点的异常状态
- 不可篡改性: 一致提交后的数据会一直存在，不可被销毁或修改
- 隐私保护性: 密码学保证了数据隐私，即便数据泄露，也无法解析。

分类

- 公有链
- 联盟链
- 私有链

比特币

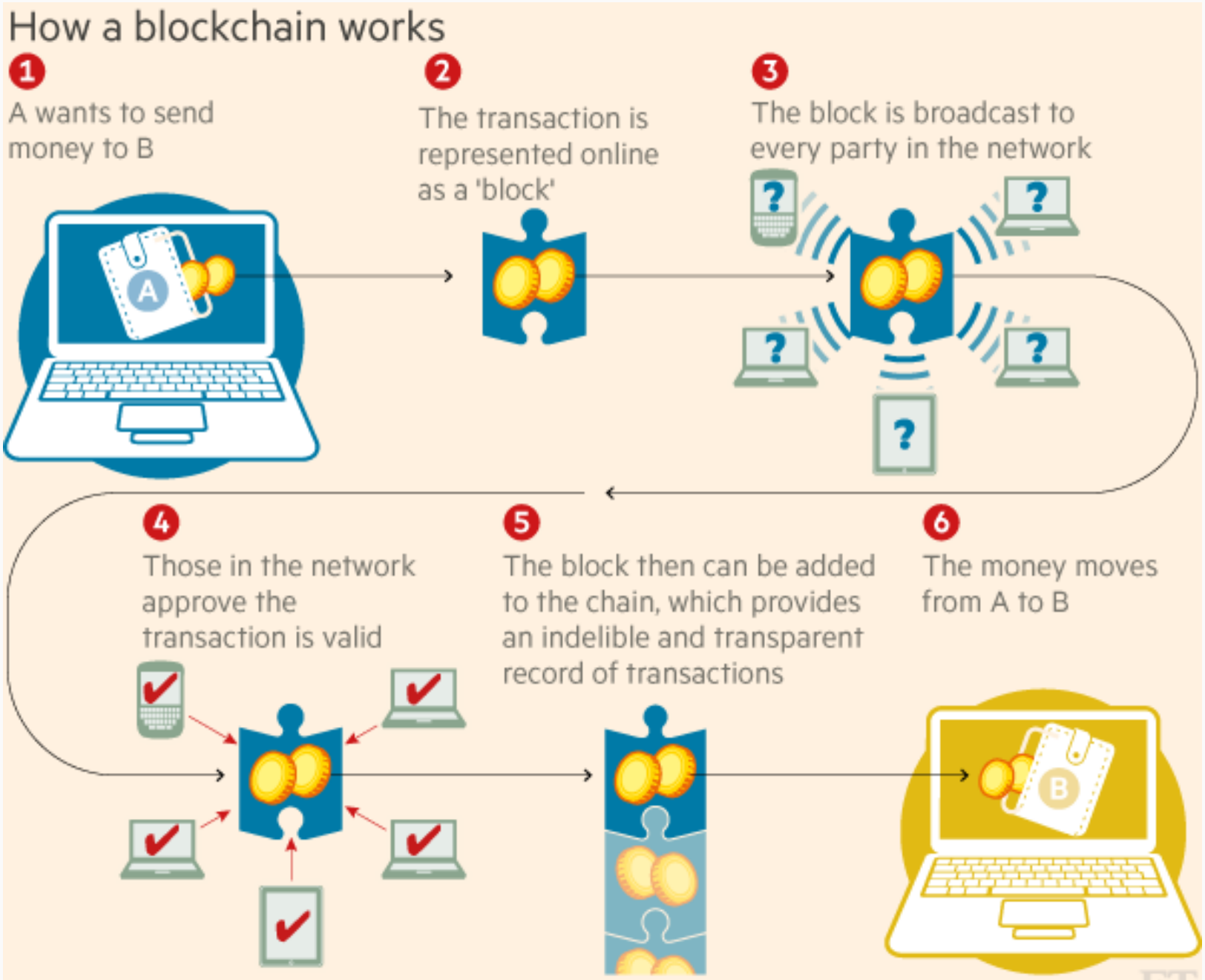
吐槽

- 比特币就是个骗局，任何一个程序员都可以再造出更多的比笨币，比傻币，比蠢币，
- 这种凭空造出来，完全没有实体的虚拟币怎么可能有价值？
- 没有政府背书担保，怎么可能有信用当货币？你这是疯了吧！

概念

- 是基于区块链技术的一种数字货币实现
- 2008 年 11 月 1 日，中本聪发布比特币白皮书:《Bitcoin: A Peer-to-Peer Electronic Cash System》(《比特币: 一种点对点的电子现金系统》)
- 2010 年 5 月 21 日，第一次比特币交易: 佛罗里达程序员 Laszlo Hanyecz 用 1 万 BTC 购买了价值 25 美元的披萨优惠券。这是比特币的首个兑换汇率:1:0.0025 美金。1:45478.02RMB

交易流程


How a blockchain works
1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
A
B

挖矿

- 收益：固定奖励 (50,1/2 per 4, 12.5) 和小费
- 形式：抢答问题
- echo transactions+value+previous | md5sum
- e24c79c0cc25b78de7f593f58fee4587

应用

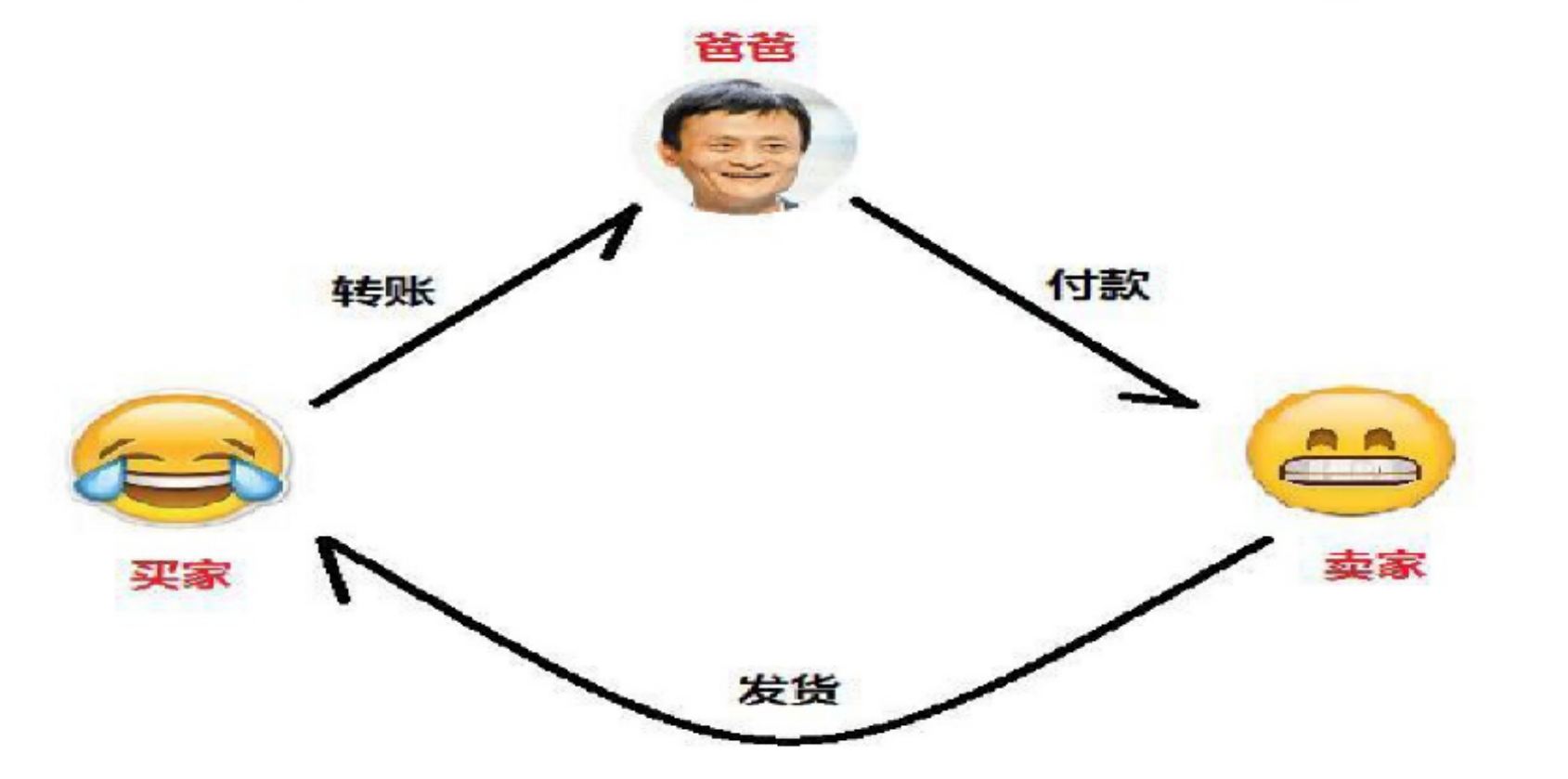
应用

- 加密数字货币：比特币，以太坊，瑞波币
- 支付汇兑：简便，免费 (跨国)
- 公证防伪：公证通（factom）、Monegraph、Stampery
- 智能合约：彩色币、闪电网络、侧链
- 物联网：ADEPT、Filament、Tilepay、Slock.it（slock-it）
- 身份验证：BlockScore、Shocard、LaunchKey、BitNation
- 预测市场：Augur、Truthcoin、Futarchy
- 资产交易：比原链（bytom）、量子链（qtum）、Medici
- 电子商务：OpenBazaar、Eris、BitXBay、Bitmarkets
- 社交通讯：Gems、Codius、比特信（bitmessage）、Twister
- 文件存储：MaidSafe、Enigma、Filecoin、公证通（factom）
- 数据 API：Coinalytics、Blocktrail、BlockCypher
- 其它：DECENT、亿书、好扑区块链、Energo、天算
- 银行结算：R3CEV、Corda
- 区块链金融：iCube

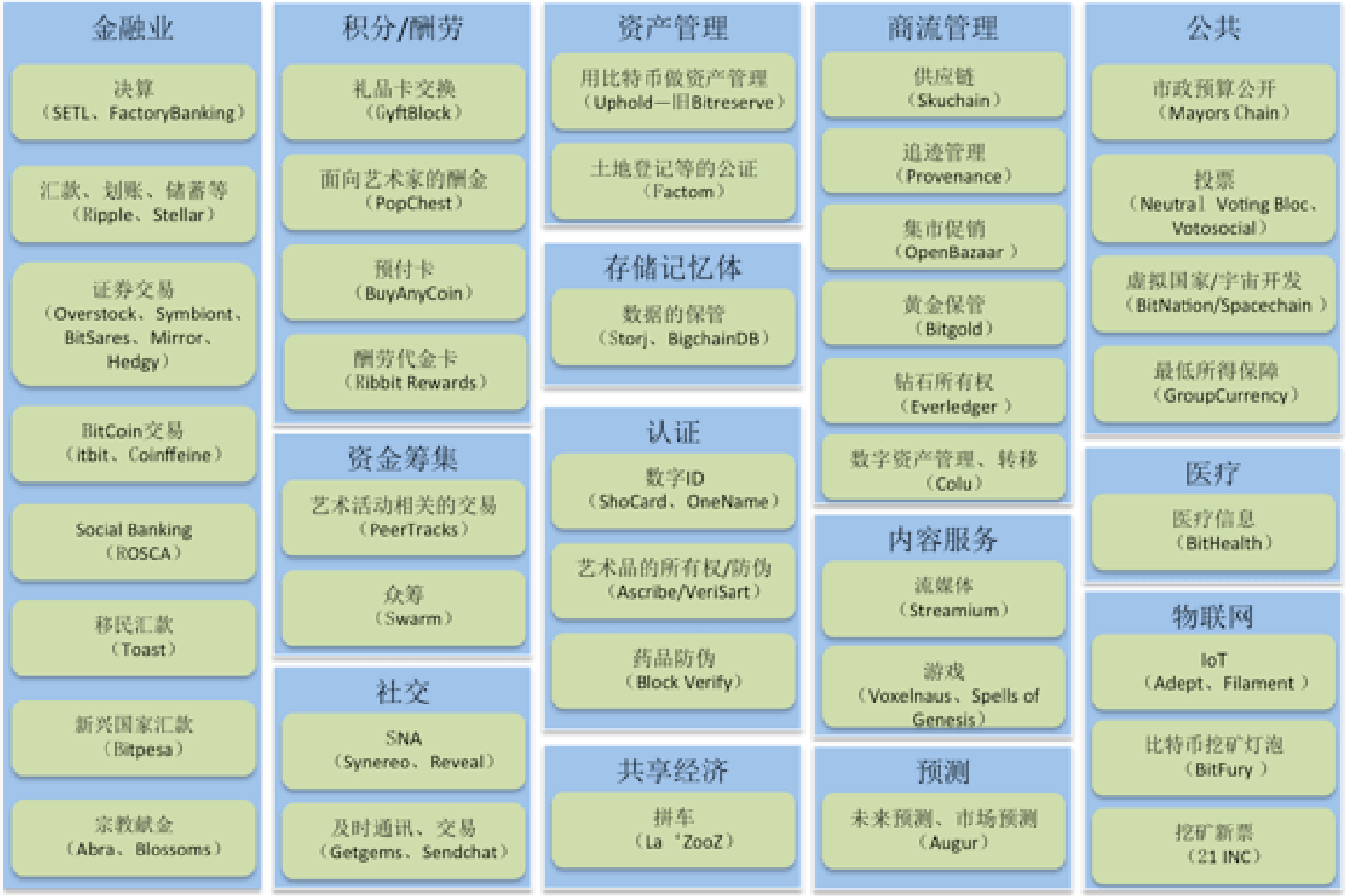
研究方向

- 区块链记录内容和交换对象的拓展：价值信息，财产的所有权、服务的受与权（所有权、使用权）的转移和证明
- 共通维护机制的改进和高性能化：处理时间、区块的大小、算力的浪费
- 网络参加的限制和参加者信赖度的提高：加入审查，提高效率

Centralization



Applications



谢谢