由比特币说起

区块链的前世今生及趋势

主讲人：王士勇

目 录

什么是比特币？

是一种
虚拟货币

开源
软件

P2P
网络

精密
计算

总量
2100万个

这一过程叫挖矿

获取方式详解

- 货币兑换：登录比特币中国、火币等交易平台，然后充值人民币购买，需缴纳0.4%的手续费
- 挖矿获取：多张显卡组合的专用电脑称为“挖矿机”，最低配也需上万元

- 去中心化、去信任化的货币
- 本身不会通货膨胀的货币

货币的演变

信用是传统金融行业的核心

实物货币
- 贝壳
- 牛，羊
- ……

贵金属货币
- 金
- 银
- ……

信用货币
- 纸币
- 电子货币
- 数字货币

货币的职能
- 交换媒介
- 价值尺度
- 支付手段
- 价值储藏

数字货币
- 数字美元—基于国家信用
- 比特币—依靠算法建立信用
- 其他数百种货币

比特币的市值曲线

收藏品、投资品特征明显

2015-1-12

央行等五部门：比特币不作为货币在市场流通使用

中国人民银行 | 工业和信息化部 | 中国银行业监督管理委员会 | 中国证券监督管理委员会 | 中国保险监督管理委员会

日前联合印发了关于防范比特币风险的通知

认为比特币不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用

不是由货币当局发行
不具有法偿性与强制性等货币属性
不是真正意义的货币

是一种特定的虚拟商品
不具有与货币等同的法律地位
不能且不应作为货币在市场上流通使用

现阶段，各金融机构和支付机构

不得以比特币为产品或服务定价
不得买卖或作为中央对手买卖比特币
不得承保与比特币相关的保险业务或将比特币纳入保险责任范围
不得直接或间接为客户提供其他与比特币相关的服务

比特币交易作为一种互联网上的商品买卖行为，普通民众在自担风险的前提下拥有参与的

新华社记者 曲振东 编制

新华网 WWW.NEWS.CN

比特币的技术原理

应用层		实现转账和记账功能	
激励层	发行机制		分配机制
共识层		POW	
网络层	P2P网络	传播机制	验证机制
数据层	区块数据	链式结构	数字签名
	哈希函数	梅克尔树	非对称加密

比特币的几大特征

去中心化	没有中心化的设备或者管理机构，任意节点之间的权利和义务都是对等的
去信任化	参与整个系统的每个节点之间数据交换通过数字签名技术进行验证，无需公开身份，双方匿名，无需互相信任，只要按照系统既定的规则进行，自动执行智能合约，节点之间不能也无法欺骗其它节点
共识	参与整个系统的每个节点间基于一套共识机制，通过竞争与激励计算共同维护整个区块链
公开透明	整个系统是开放的，除了交易各方的私有信息被加密外，区块链的数据对所有人公开，任何人都可以通过公开的接口查询区块链数据和开发相关应用
不可篡改可追溯	单个甚至多个节点对数据库的修改无法影响其他节点的数据库，除非能控制整个网络中超过51%的节点同时修改。区块链中的每一笔交易都通过密码学方法与相邻两个区块串联，可追溯到任何一笔交易的历史记录
集体参与	系统中的数据块由整个系统中具有维护功能的节点来共同维护
自治化	区块链中的交易可以根据事先约定，自动执行智能合约

区块链的价值

互联网与互联网金融

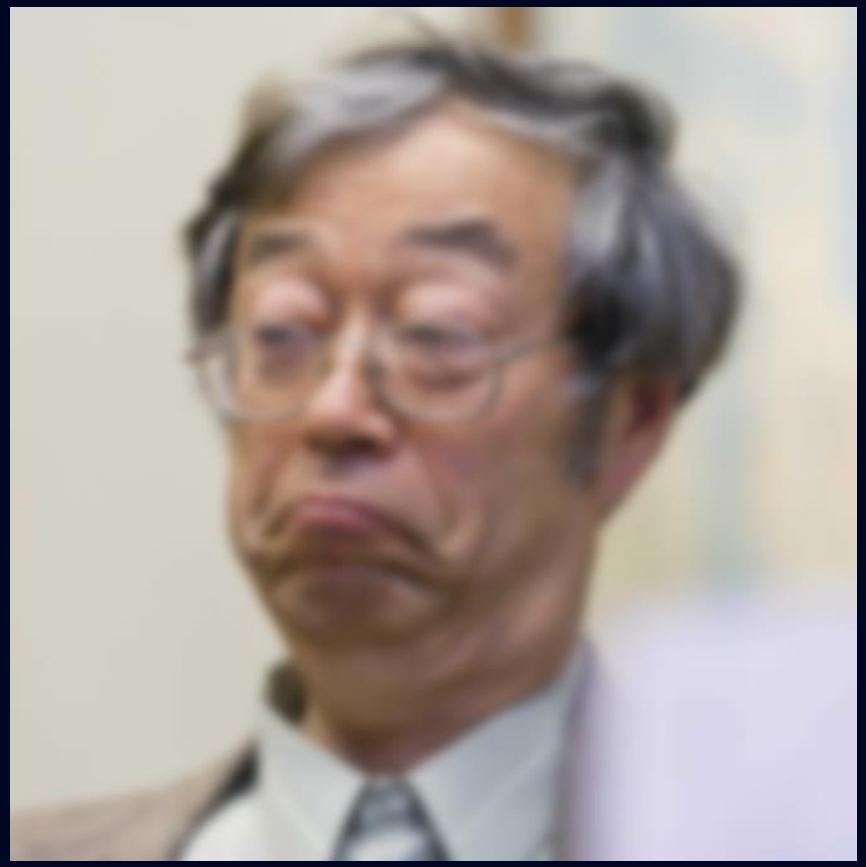
互联网核心解决的问题	信息的制造与传播
互联网未能解决的问题	价值与信用的转移
互联网金融体系的运作	政府，银行或第三方支付系统实现价值的转移
互联网金融体系的局限	信用局限在一定的机构，地区或国家的范围之内

根本问题是如何解决信用，而实现价值转移的核心是如何达成共识 → 建立一个全球性的信用共识体系，取代第三方中介，自动运行，实现“去信任”机制 → 每个国家政治，语言文化，宗教信仰不同，唯一取得共识的是数学（算法）

区块链被视为大型机、个人电脑、互联网之后颠覆式创新

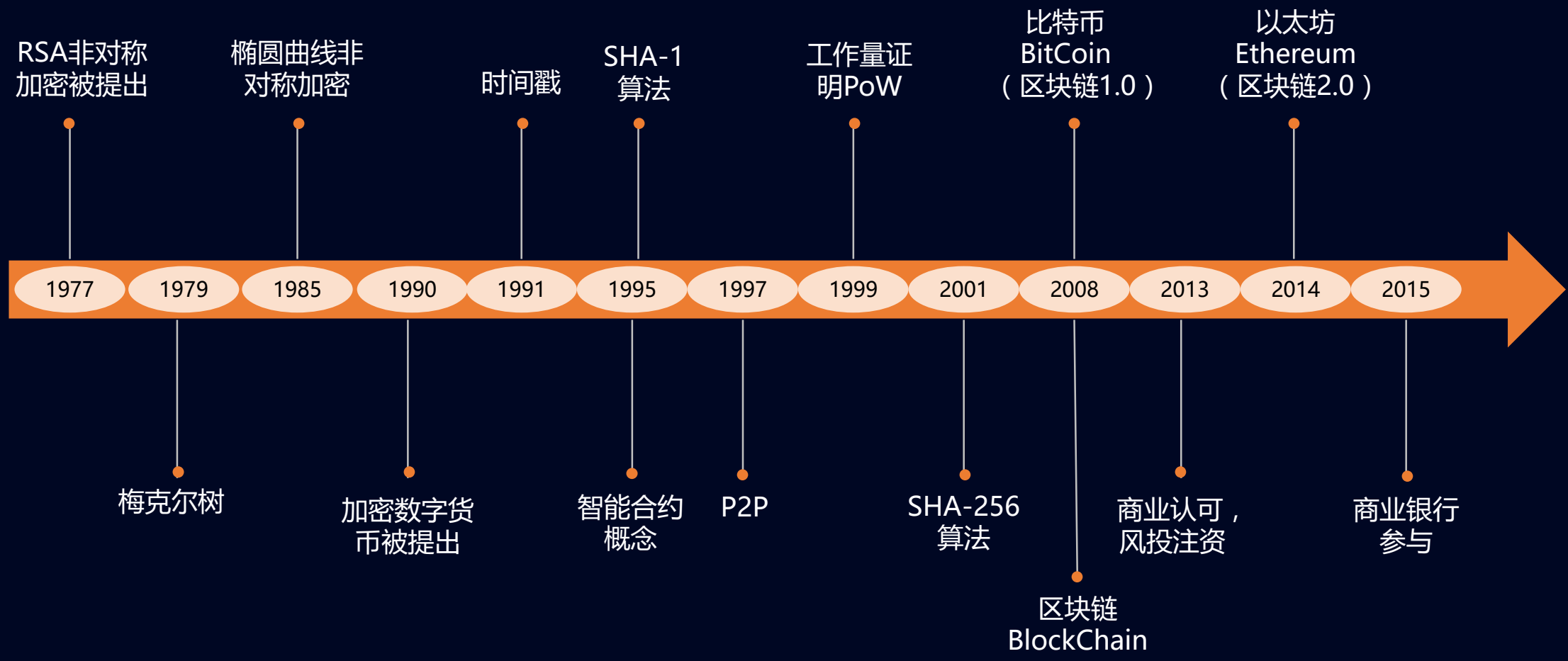
目 录

中本聪首次提出区块链的思想



2008年，中本聪在一个密码学邮件群组中发表了文章《比特币：一种点对点的电子现金系统Bitcoin: A Peer-to-Peer Electronic Cash System》，其中提到了区块链（Block Chain）的思想

区块链（比特币）的前世今生



区块链的重要成就：解决了拜占庭将军问题

拜占庭将军问题

拜占庭是东罗马帝国的首都，由于国土幅员辽阔，为了防御敌人攻击从而每个军队分割很远，将军与将军之间只能靠信差来传递消息。在战争时期，拜占庭军队内所有将军和副官必须达成一致共识，决定是否有赢的机会才会攻打敌人。但是军队可能有叛徒和敌军间谍，此时，在已知有成员谋反的情况下，其余忠诚的将军在不受叛徒的影响下如何达成一致的协议，即为“拜占庭将军问题”

拜占庭将军问题在通信领域的场景

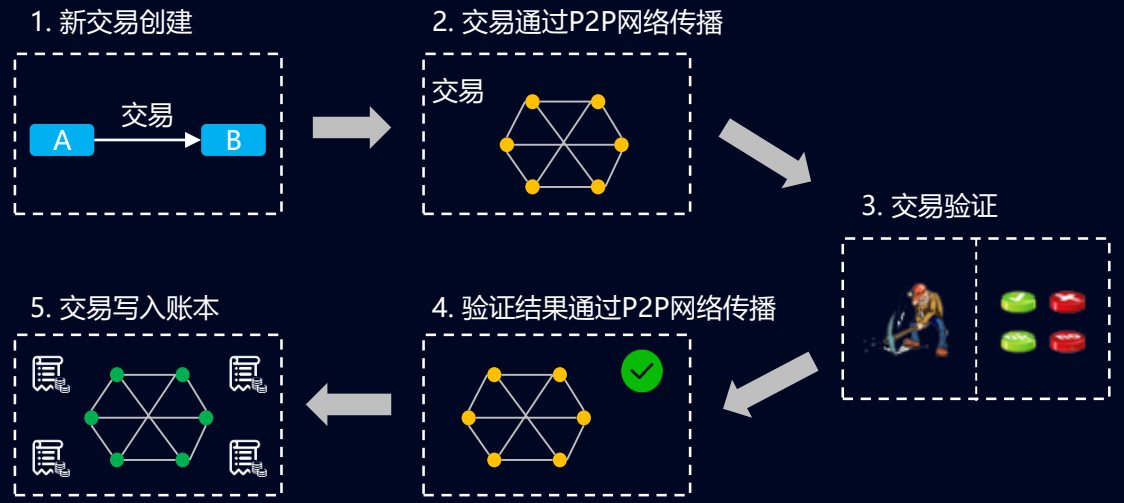
“叛变的将军”可以替换成：
一个出故障的，向其他计算机不停的发出错误信息的服务器；
一份为获取暴利而做出来的金融票据；
一个可以发出消息，做出行动的错误信息节点

交易过程（1）

第一步

所有者A利用他的私钥对前一次交易（比特币来源）和下一位所有者B签署一个数字签名，并将这个签名附加在这枚货币的末尾，制作成交易单

（B的公钥作为接收方地址）

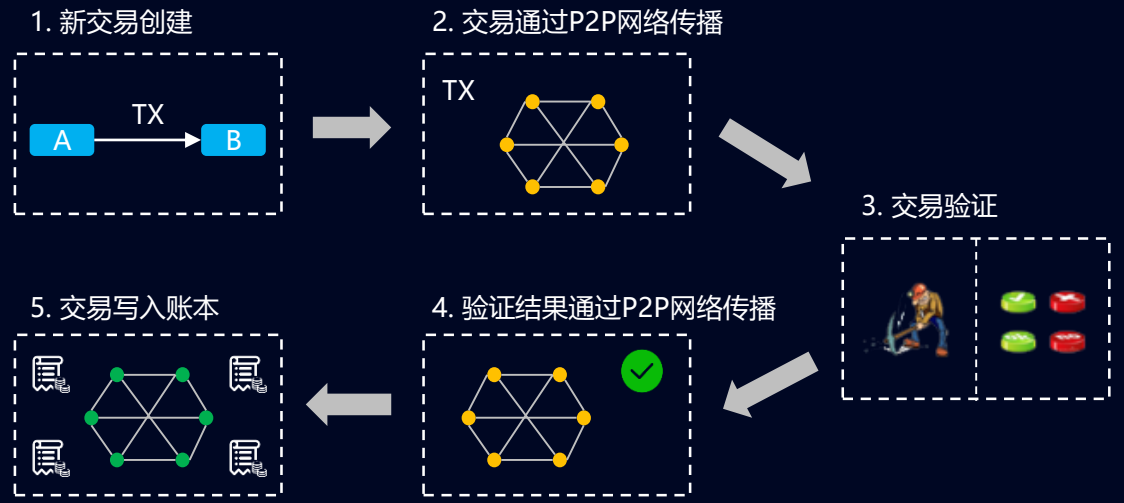


交易过程（2）

第二步

A将交易单广播至全网，比特币就发送给了B，每个节点都将收到的交易信息纳入一个区块中

（对B而言，该枚比特币会即时显示在比特币钱包中，但直到区块确认成功后才可用。目前一笔比特币从支付到最终确认成功，得到6个区块确认之后才能真正确认到帐）

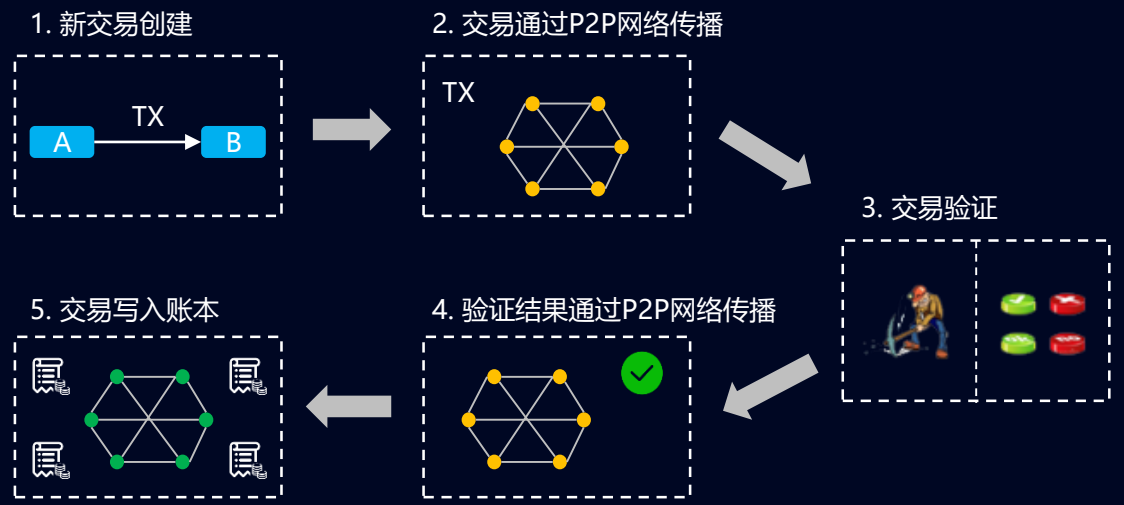


交易过程（3）

第三步

每个节点通过解一道数学难题，从而去获得创建新区块权利（争抢记账权），并争取得到比特币的奖励（挖矿）（新比特币会在此过程中产生）

（节点反复尝试寻找一个数值，使得将该数值、区块链中最后一个区块的Hash值以及交易单三部分输入SHA256算法后计算出的散列值X（256位）满足一定条件（比如前20位均为0），即找到数学难题的解。答案并不唯一）

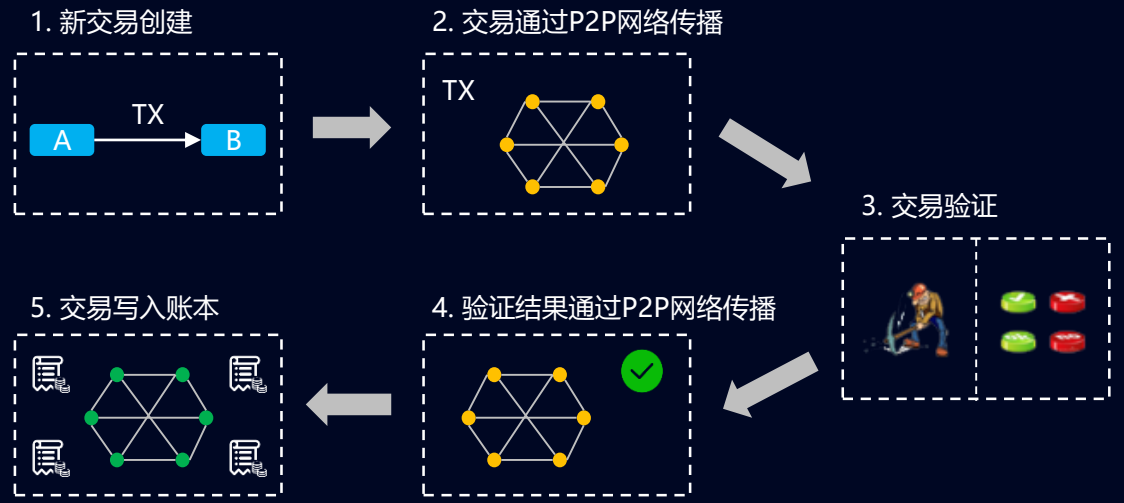


交易过程（4）

第四步

当一个节点找到解时，它就向全网广播该区块记录的所有盖时间戳的交易，并由全网其他节点核对

（时间戳是用来证实特定区块必然于某特定时间确实存在的。比特币网络采取从5个以上节点获取时间，然后取中间值的方式作为时间戳）

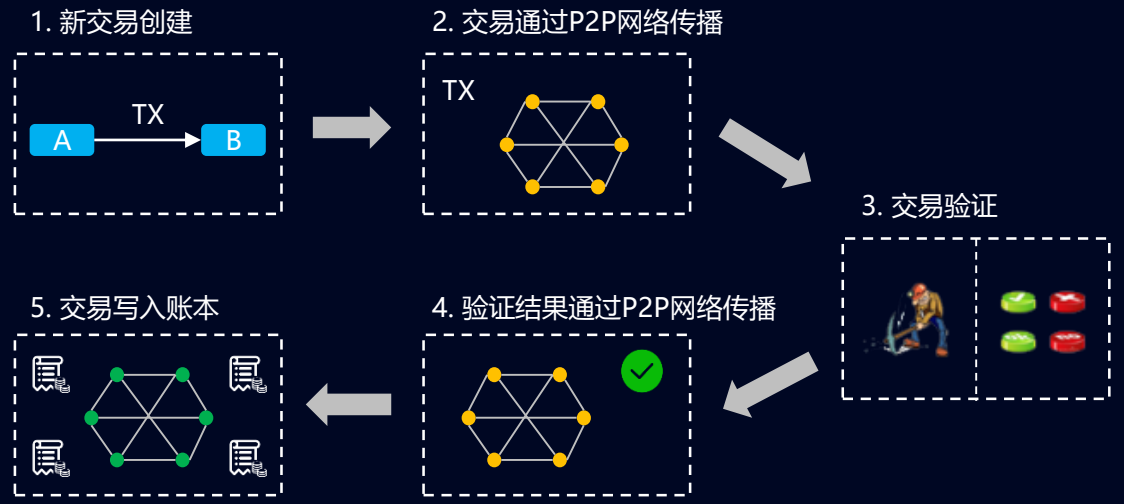


交易过程（5）

第五步

全网其他节点核对该区块记账的正确性，没有错误后他们将在该合法区块之后竞争下一个区块，这样就形成了一个合法记账的区块链

（每个区块的创建时间大约是10分钟。随着全网算力的不断变化，每个区块的产生时间会随算力增强而缩短、随算力减弱而延长。其原理是根据最近产生的区块的时间差（约两周时间），自动调整每个区块的生成难度，使得每个区块的生成时间维持在10分钟左右）



最初的比特币是从哪里来的

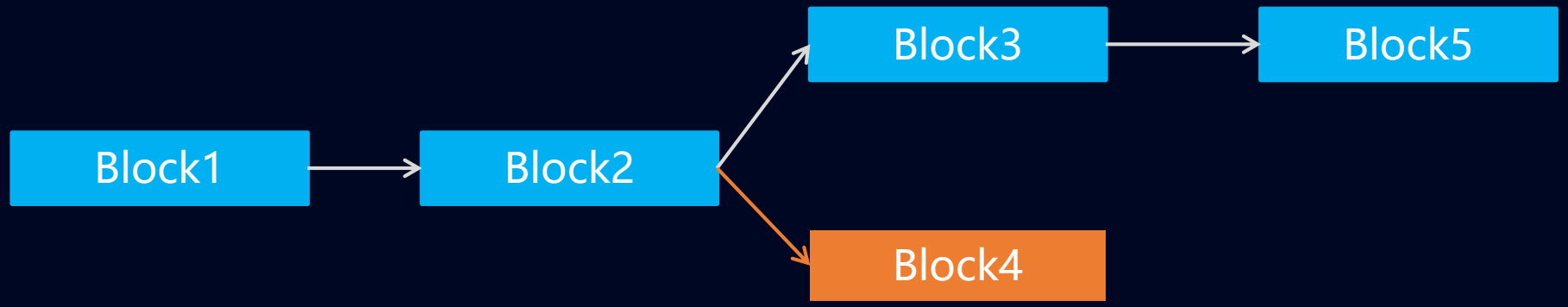
1. 最初的比特币是由系统奖励给抢到记账权记录区块的矿工的
2. 每一个区块在生成的时候就会在生成这个区块的矿工账户上生成一定数量的新的比特币作为奖励
3. 区块链上记录了所有的比特币交易记录
4. 只需要追溯所有与账户相关的历史交易就能知道这个账户上到底有多少余额
5. 余额不足时，矿工就会拒绝记录交易
6. 每个比特币账户都有公钥和私钥，发起交易时用私钥对交易信息签名，矿工收到信息后用公钥验证签名，验证通过则是本人，否则为冒名顶替

如何判断以谁的记录为准

（如何决定由哪个矿工生成下一个区块）

1. 共识机制：工作量证明（PoW）
2. 设计一个数学问题，该数学问题会耗费大量的计算机CPU时间才能得出答案，同时每一次得出的结果都会作为下一次计算的初始条件进行再次计算
3. 全世界的矿工一起来计算这个问题，谁先得出答案，他就可以用这个答案生成一个新的区块，再广播到网络中
4. 收到这个新区块数据的矿工会立即停止当前的计算，用新区块里的数据重新进行下一次计算
5. 矿工产生的区块一旦被网络接受，他就能获得一笔比特币作为报酬

叉链（出现不一致了，如何裁决）



- 同一时间段内全网不止一个节点能计算出随机数，即会有多个节点在网络中广播它们各自打包好的临时区块（都是合法的）
- 某一节点若收到多个针对同一前续区块的后续临时区块，则该节点会在本地区块链上建立分支，多个临时区块对应多个分支。该僵局的打破要等到下一个工作量证明被发现，而其中的一条链条被证实为是较长的一条，那么在另一条分支链条上工作的节点将转换阵营，开始在较长的链条上工作。其他的短分支将会被网络彻底抛弃
- 比较分叉的长短，存长弃短

交易多久之后可以到账、是否真的无法篡改？

- 六度空间理论
- 交易发生后比特币就会即时显示在接收方的比特币钱包中，但直到区块被确认成功后才可使用
- 一笔比特币从支付到最终确认成功，需要得到**6个节点**（除自身之外其他5个节点）确认之后才能真正确认到帐，到账之后就不可篡改

是否真的无法篡改

- 可以篡改，代价会随着全网算力的增强而变大，随算力的减弱而变小
- 控制全网51%算力的人可以篡改

安全问题

公开的P2P网络，是否会受到攻击

- 粉尘攻击：大量的微小交易，造成区块拥堵。（每个块只能包含1 MB 的交易记录）
- 女巫攻击：在网络中，恶意实体模仿多个身份，通过控制系统的大部分节点来削弱正确数据冗余备份的作用

如何避免记假账

- 不同于传统的单中心或单节点记账方案，没有任何一个节点可以单独记录账目，从而避免了单一记账人被控制贿赂而记假账的可能性
- 非对称密钥对交易信息签名，并广播
- 共识机制+分布式节点的验证确认机制（6个）

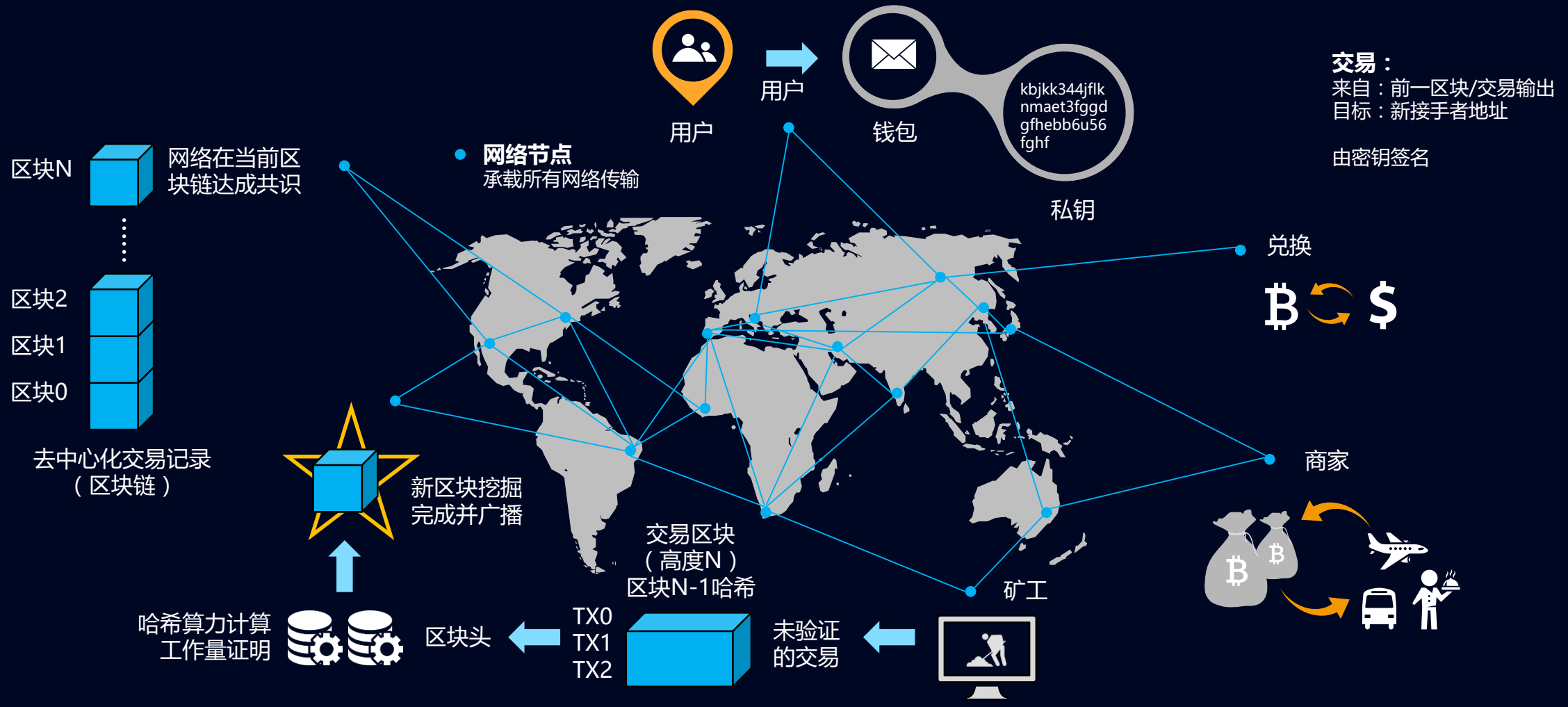
如何避免“双花”

- 用户将同一笔资金提交了两次交易，系统没有识别并认可了这两次交易
- 恶意用户攻击系统，对账本进行控制，让系统接受了两次交易，或者直接修改账本

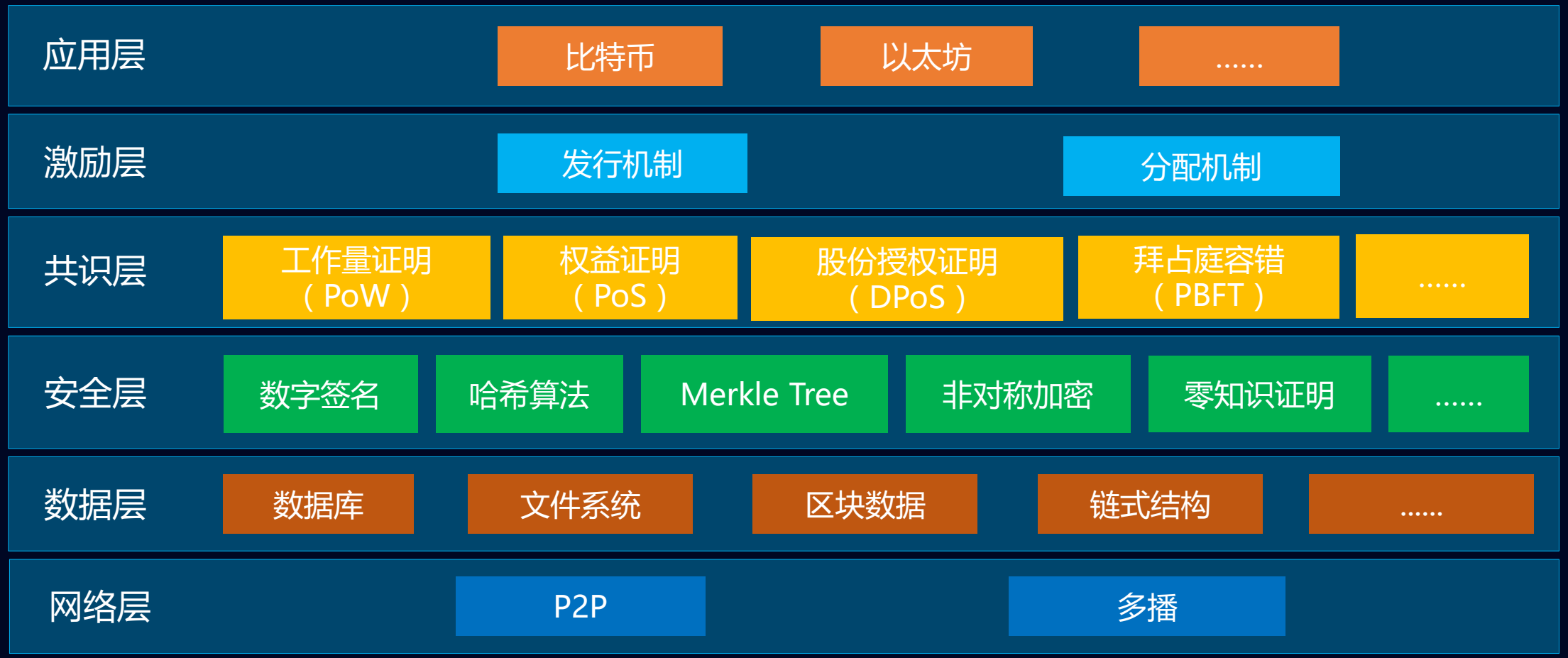
如何避免“双花”

- UTXO机制确保不会发生“双花”，检查本笔交易相关的UTXO是否被其他交易花费
- 共识机制+分布式节点的验证确认机制（6个）

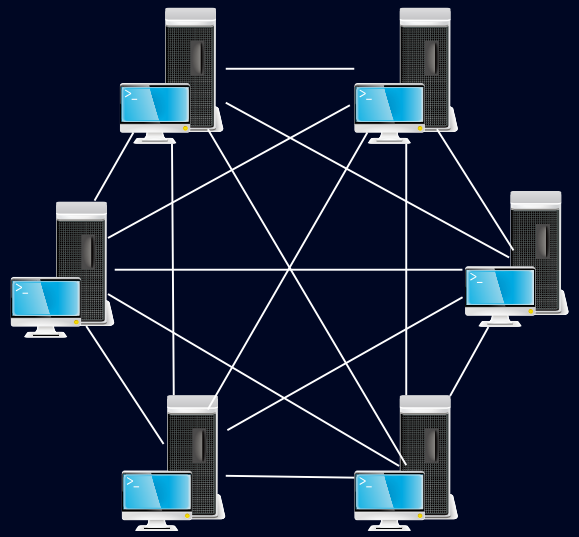
回顾一下比特币的应用架构



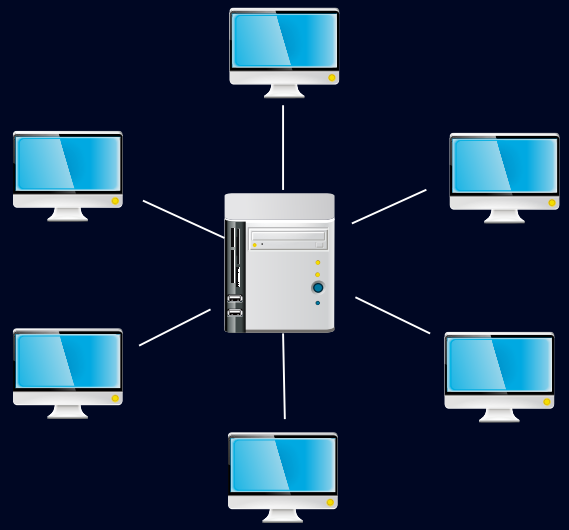
区块链技术架构


应用层
比特币
以太坊
……
激励层
发行机制
分配机制
共识层
工作量证明（PoW）
权益证明（PoS）
股份授权证明（DPoS）
拜占庭容错（PBFT）
……
安全层
数字签名
哈希算法
Merkle Tree
非对称加密
零知识证明
……
数据层
数据库
文件系统
区块数据
链式结构
……
网络层
P2P
多播

区块链技术架构



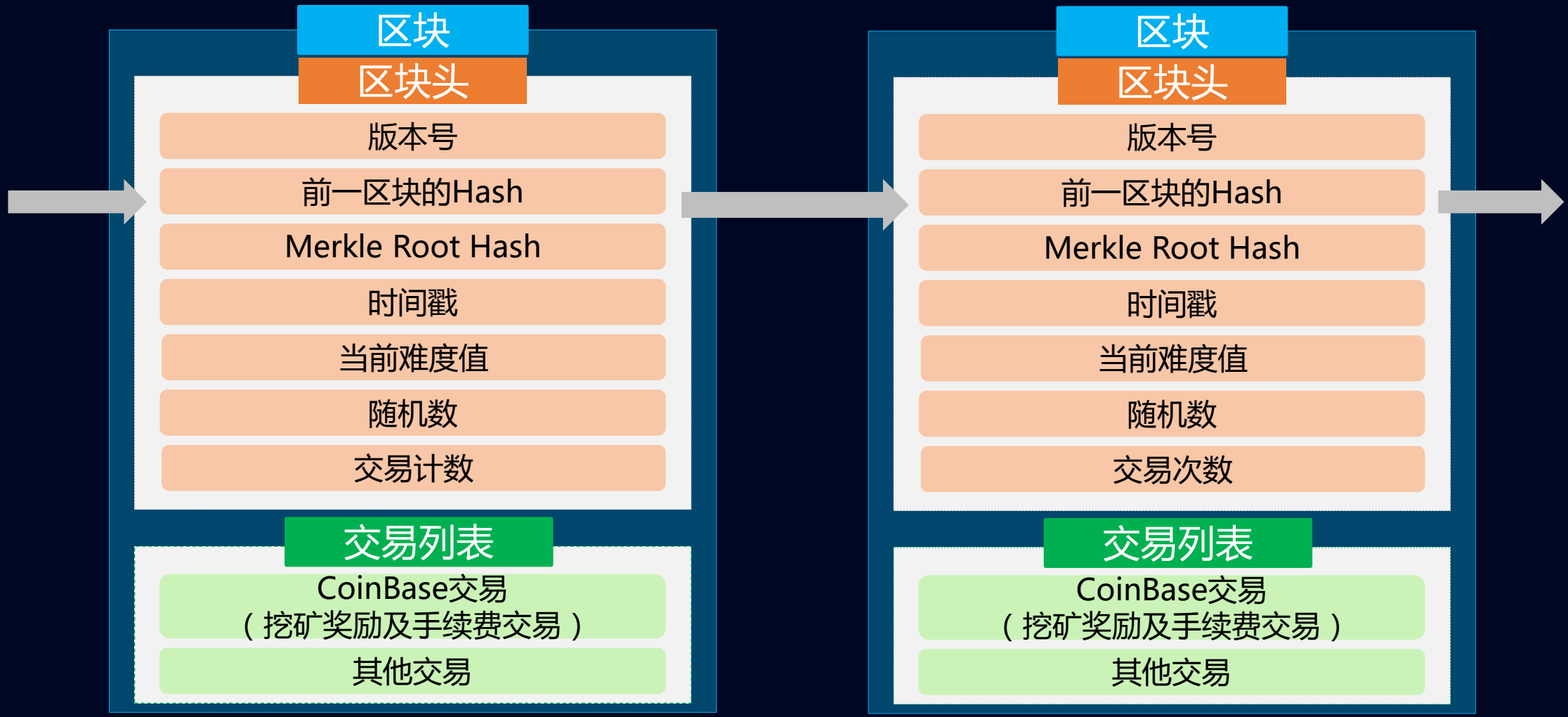
P2P网络模式



中心化网络模式

- P2P网络也称点对点网络，端对端网络，是构建在互联网上的一种连接网络
- 不同于中心化网络模式，P2P网络中各节点的计算机地位平等，每个节点有相同的网络权力，不存在中心化的服务器。所有节点间通过特定的软件协议共享部分计算资源、软件或者信息内容
- P2P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

数据层—区块与区块链


区块
区块头
版本号
前一区块的Hash
Merkle Root Hash
时间戳
当前难度值
随机数
交易计数
交易列表
CoinBase交易
（挖矿奖励及手续费交易）
其他交易
区块
区块头
版本号
前一区块的Hash
Merkle Root Hash
时间戳
当前难度值
随机数
交易次数
交易列表
CoinBase交易
（挖矿奖励及手续费交易）
其他交易

数据层—交易（UTXO）

版本（比特币协议的协议号）

交易支出（输出Tx_out）量统计

交易付款方（输出Tx_out）地址详情列表

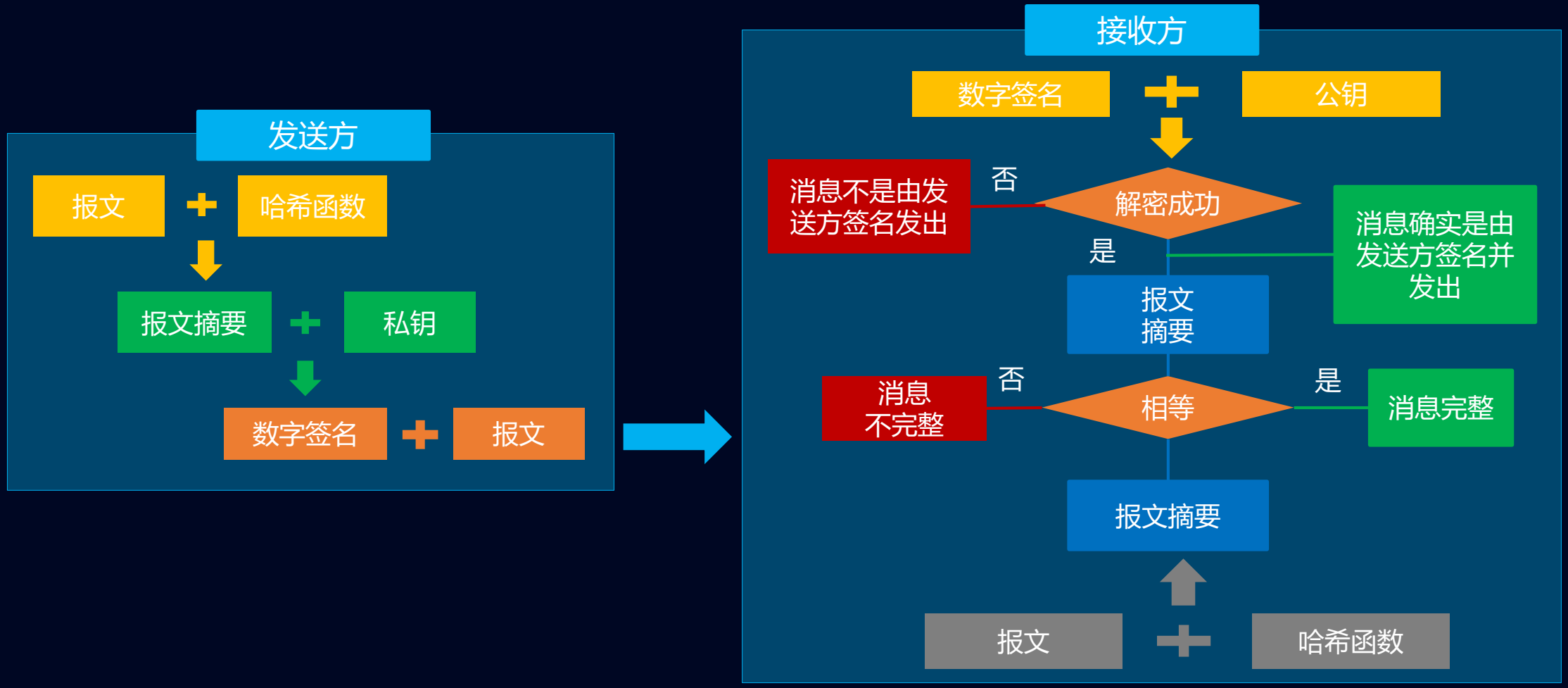
交易收入（输入Tx_in）量统计

交易收款方（输入Tx_in）地址详情列表

锁定时间戳

- UTXO（Unspent Transaction Outputs）是未花费的交易输出
- 链条的源头都是挖矿奖励，末尾则是当前未花费的交易输出。所有的未花费的输出即整个比特币网络的UTXO
- 比特币规定每一笔新的交易的输入必须是某笔交易未花费的输出，每一笔输入同时也需要上一笔输出所对应的私钥进行签名，并且每个比特币的节点都会存储当前整个区块链上的UTXO，整个网络上的节点通过UTXO及签名算法来验证新交易的合法性
- 交易主要的两个单元字段就是交易的输入与输出。输入标识着交易的发送方，输出标识着交易的接收方及对于自己的找零，交易的手续费则是输入的总和与输出的总和之差
- 交易输入三种类型：标准输入（Standard TxIn）,花费挖矿奖励（手续费收入）（Spend CoinBase TxIn ），产生挖矿奖励（挖矿奖励）（CoinBase Generation TxIn ）
- 交易输出类型两种类型：标准交易输出（Standard TxOut）,挖矿奖励输出（手续费支出）（CoinBase TxOut）

安全层—数字签名


发送方
报文
哈希函数
报文摘要
私钥
数字签名
报文
接收方
数字签名
公钥
消息不是由发送方签名发出
否
解密成功
消息确实是由发送方签名并发出
是
报文摘要
消息不完整
否
相等
是
消息完整
报文摘要
报文
哈希函数

安全层—梅克尔树

- 一种哈希二叉树，使用它可以快速校验大规模数据的完整性。

  在比特币网络中，Merkle 树被用来归纳一个区块中的所有交易信息，最终生成这个区块所有交易信息的一个统一的哈希值，区块中任何一笔交易信息的改变都会使得使得 Merkle 树改变

- 非叶子节点value的计算方法是将该节点的所有子节点进行组合，然后对组合结果进行hash计算所得出的hash value

安全层—零知识证明

证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的

零知识证明实质上是一种涉及两方或更多方的协议，即两方或更多方完成一项任务所需采取的一系列步骤

证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息

共识层

PoW	● 所有节点都可以进行数学运算来解题从而获取记账权 ● 资源消耗相比其他共识机制高、可监管性弱，同时每次达成共识需要全网共同参与运算，性能效率比较低，容错性方面允许全网50%节点出错
PoS	● 主要思想是节点记账权的获得难度与节点持有的权益成反比 ● 相对于PoW，一定程度减少了数学运算带来的资源消耗，性能也得到了相应的提升，但依然是基于哈希运算竞争获取记账权的方式，可监管性弱。该共识机制容错性和PoW相同
DPoS	● 与PoS的主要区别在于节点选举若干代理人，由代理人验证和记账 ● 其合规监管、性能、资源消耗和容错性与PoS相似
PBFT	● 是一种采用许可投票、少数服从多数来选举领导者进行记账的共识机制，领导者节点拥有绝对权限，但该共识机制允许拜占庭容错 ● 该共识机制允许强监管节点参与，具备权限分级能力，性能更高，耗能更低，该算法每轮记账都会由全网节点共同选举领导者，允许33%的节点作恶，容错性为33%

激励层

获得记账权的节点将获得一定的奖励，作为CoinBase交易支付给该节点

大概每10分钟发行一次。随着全网算力的不断变化，每个区块的产生时间会随算力增强而缩短、随算力减弱而延长。每2周自动调整每个区块的生成难度，使得每个区块的生成时间是10分钟

自2009年开始，奖励每4年减半，头 4 年，将会产生总额为 10,500,000 BTC 的比特币，最近一次减半发生在2016年7月9日

限量发行，到2140年全球总共会发行2100万比特币（上限），现在一共有1620万的流通比特币（价值为160亿美金）

应用层

比特币

- 区块链 1.0 的代表产品
- 数字货币
- 类似黄金一样的常规货币替代物，通常用来作为支付交易的媒介以及价值储存的手段
- 实现转账与记账功能

以太坊

- 区块链 2.0 的代表产品
- 智能合约
- 创建一个基于智能合约以及去中心化技术的分布式应用软件开发平台，使开发人员可以建立并运行分布式应用程序
- 以太坊虚拟机（EVM）
- 分布式应用（DAPP）
- 脚本代码

区块链应用的技术架构

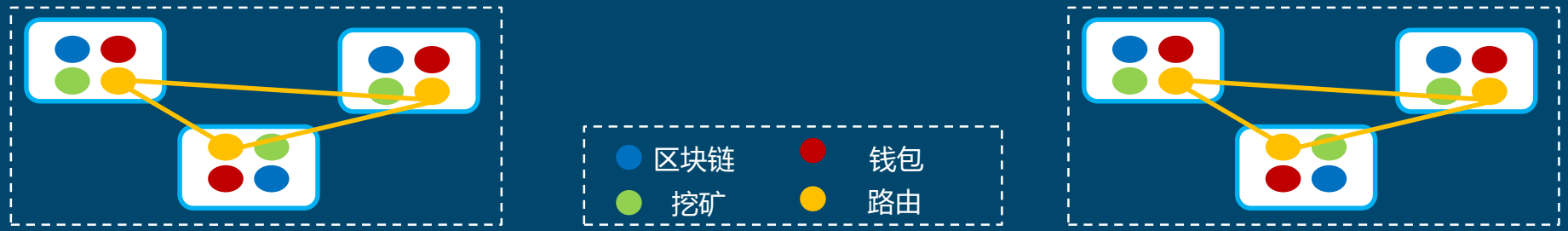
应用层

智能合约 | 数字资产与交易 | 身份识别与认证 | 自治组织 | ……

BAAS

比特币 | 以太坊 | ……

区块链网络层



基础技术层

P2P	时间戳	PoW	Merkle Tree	地址
SHA-256	椭圆曲线算法	RIPEMD-160	Base58	……

目 录

优势

达成共识 不可篡改 永久追溯	● 参与方都是区块链网络中的一个节点，整个业务过程的每个环节都形成了一个数据区块记录，该区块不可篡改且完整可追溯，便于监管与审计 ● 参与方不必担心某一方篡改合约，数据或其他信息不对称问题而导致利益损失
提效降本	● 减少中间环节，简化优化业务流程 ● 自动化执行合约，减少人工环节 ● 降低资源的闲置 ● 数字化，节约实物资源
安全可靠	● 分布式架构，避免单点故障 ● 分布式存储，数据安全 ● 集体参与，多方验证，降低风险
自动智能	● 智能合约，基于可信的不可篡改的数据，自动化执行一些预先定义好的规则与条款（脚本程序）
业务创新	● 基于区块链提供的可信可靠的数据与环境，金融，供应链，制造，医疗，教育等各行各业都可以优化现有的业务，扩展新的业务

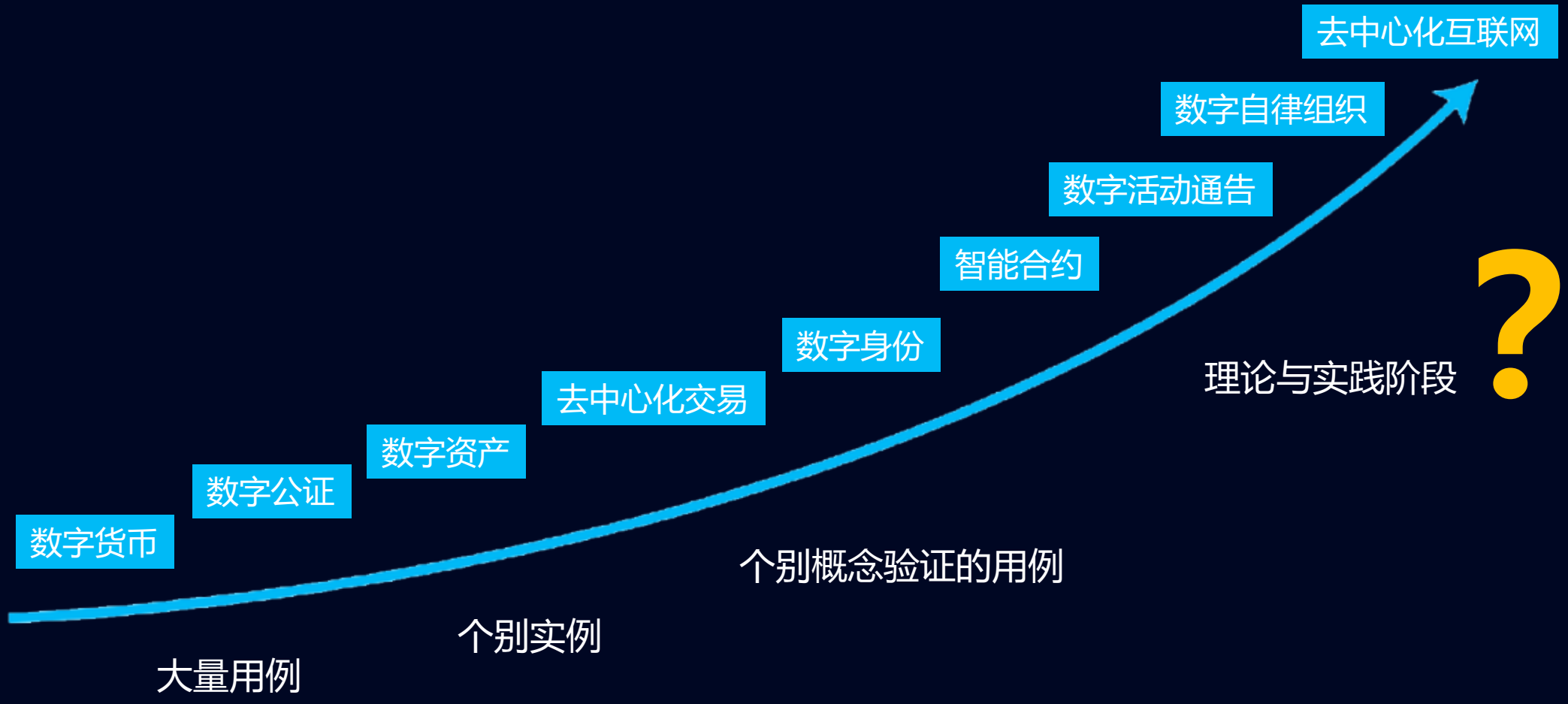
目前存在的问题

1. 技术的挑战（吞吐量，高并发，一致性，可伸缩性，模块化，标准化等）
2. 存在延迟，处理一笔交易需要10分钟
3. 容量与带宽的瓶颈
4. 安全性需要进一步提升，目前区块链上传输和存储的数据都是公开可见的，商业秘密与个人隐私
5. 用户体验，区块链的可交互性
6. 商业模式的挑战
7. 政府的监管态度与法律法规的不确定性

目 录

区块链的发展趋势

区块链技术在快速演变，新的性能在不断结合创造更强有效的解决方案



部分国家和地区对区块链的态度

英国政府：区块链及分布式账本技术有着颠覆性潜力

美国特拉华州：区块链技术简化企业注册成本

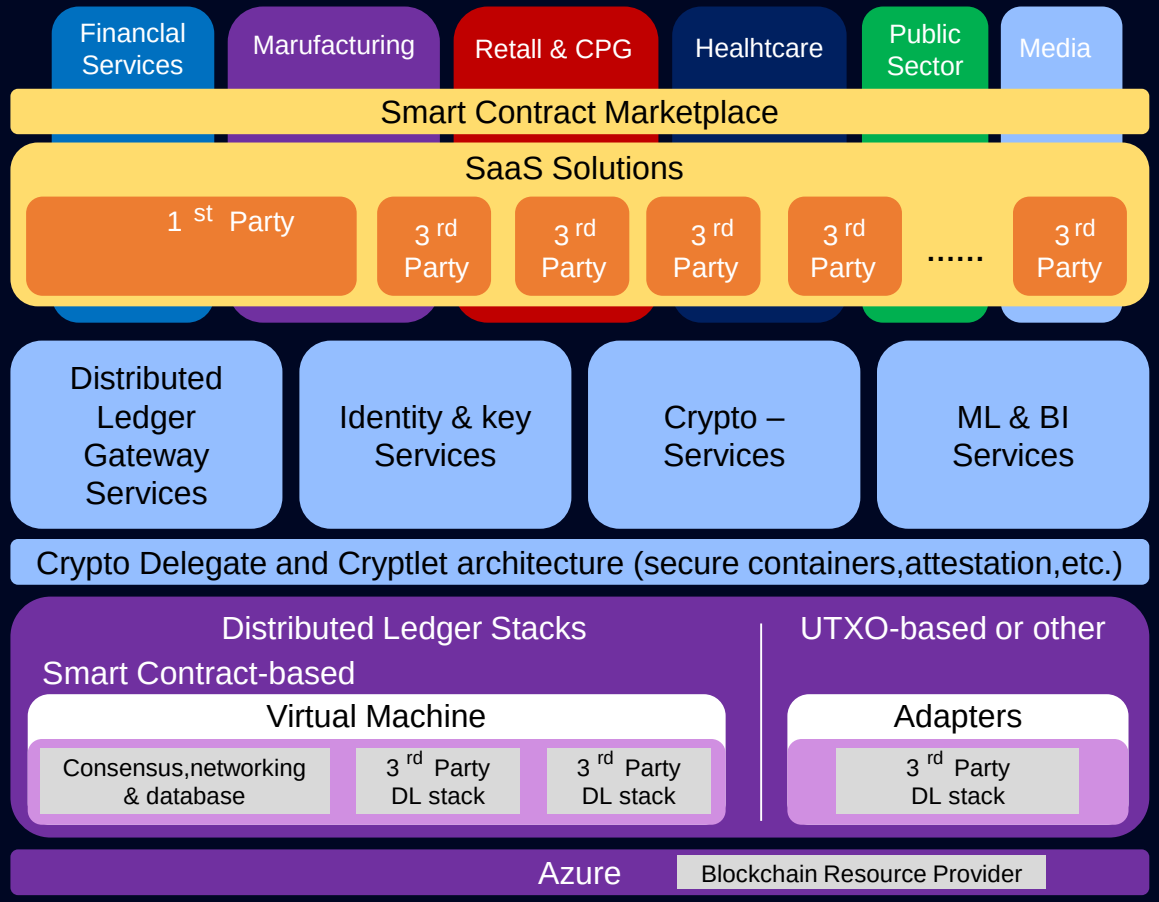
俄罗斯央行：研究区块链在金融领域的潜在应用

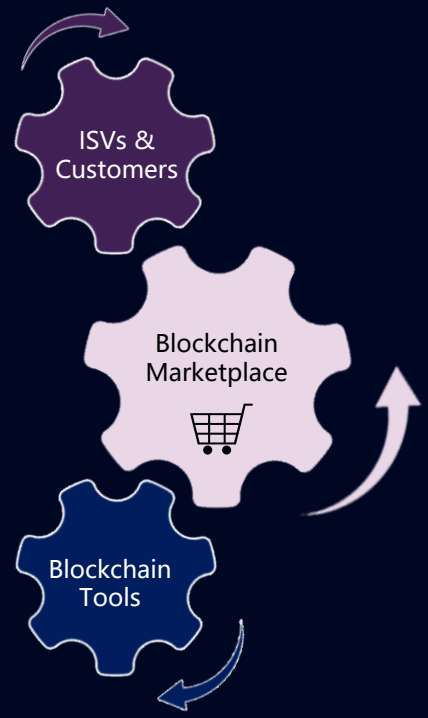
欧洲证券及市场管理局：区块链技术可改进交易后流程

新加坡政府：银行应持续关注技术变革

香港特区政府：希望推动金融科技在香港金融服务业的发展

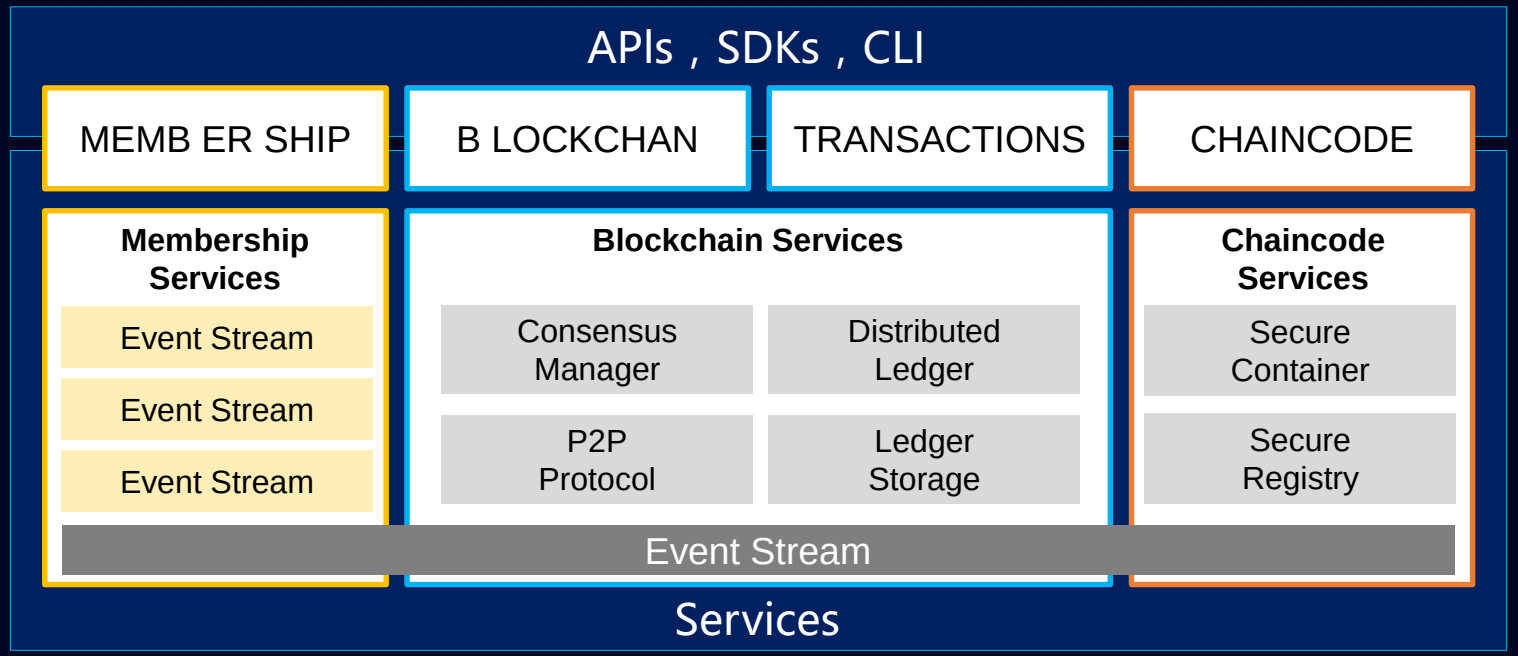
开源社区—微软开源区块链平台Bletchley





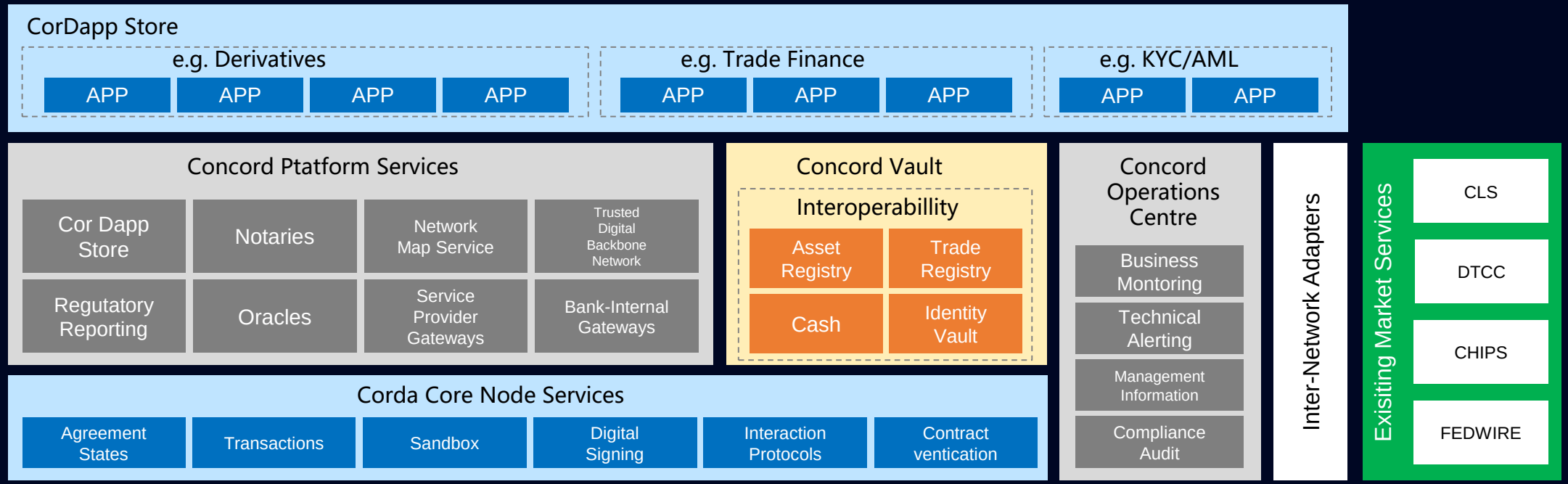
- 构建新的开放性平台，提供高可用、稳定的服务
- 整合身份管理，密钥管理，隐私管理，安全管理，运营管理和协作管理
- 适用于金融服务、医疗行业和政府部门

开源社区—Linux基金会开源区块链项目Hyperledger



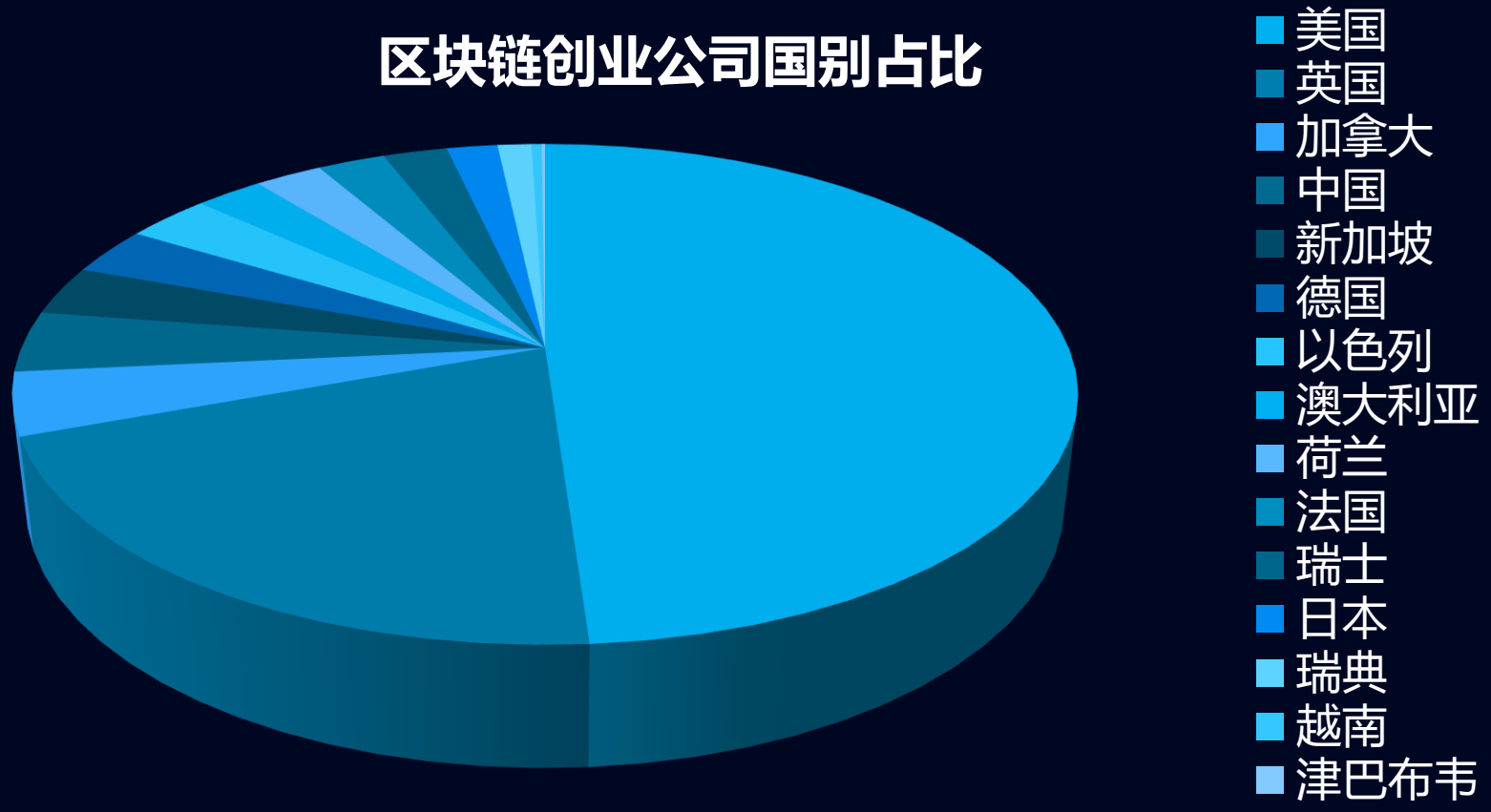
- 2015年12月，Linux基金会牵头，联合30家初始成员（包括IBM、Accenture、Intel、J.P.Morgan、R3、DAH、DTCC、FUJITSU、HITACHI、SWIFT、Cisco 等），共同发起Hyperledger项目
- 超过80家企业和机构加入Hyperledger项目，目前包括13家来自中国的公司，包括华为、三一重工等
- HyperLedger项目汇集了金融、银行、物联网、供应链、制造等各界专家。目的是打造一个跨领域的区块链应用平台，企业级开源区块链解决方案

开源社区—R3区块链联盟开源区块链平台R3 Concord



- R3CEV（Crypto 2.0, Exchanges, Ventures) 是一家总部位于纽约的区块链创业公司，由其发起的R3区块链联盟，至今已吸引了42家巨头银行的参与，其中包括美国银行、花旗银行、摩根大通、汇丰银行等，中国已经有平安集团，民生银行和招商银行等机构加入该联盟
- Concord上层支持金融衍生产品、贸易融资等业务，中间层提供公共服务，其中Vault是Concord的区块链。Corda是Concord的底层基础平台
- Corda将开源给Hyperledger

区块链全球创业公司情况



区块链在国内的发展—联盟组织不断涌现

联盟名称	创立时间	描述
亚洲区块链协会（DACA）	2015年7月	极具行业影响力的“政社产学研媒投”区块链协会，是区块链界版的“亚洲企业家俱乐部”
中国区块链研究联盟	2016年1月5日	全球共享金融100人论坛在北京宣布成立“中国区块链研究联盟”
中关村区块链产业联盟成立	2016年2月3日	全球首家专注网络空间基础设施创新的中关村区块链产业联盟在京成立
中国分布式总账基础协议联盟ChinaLedger	2016年4月19日	中证机构间报价系统股份有限公司等11家机构共同发起
金融区块链合作联盟	2016年6月1日	微众银行、平安银行、京东金融等25家企业发起，腾讯和华为等6家机构作为成员单位加入
中国互联网金融协会区块链研究小组	2016年6月15日	中国互联网金融协会领导下的专项研究组织
陆家嘴区块链金融发展联盟	2016年10月9日	在中国银监会上海监管局、上海市经信委、上海陆家嘴金融城发展局的指导下，上海市互联网金融行业协会、上海金融业联合会、中国金融信息中心等13家机构共同发起成立

区块链在国内的发展—大型企业机构开始试水

银联构建区块链
电子凭证系统

微众银行运用区块链
实现联合贷款

SWIFT推出
区块链概念验证

央行成立
中国数字货币研究所

蚂蚁金服上线
区块链公益筹款项目

……

区块链的类型

无官方组织及管理机构，无中心服务器，参与的节点按照系统规则自由接入网络、不受控制，节点间基于共识机制开展工作。任何人都能参与公有链的共识流程，任何人都可以读取公有链上的数据，任何人都可以发起交易，只要验证通过就可以纳入公有链

公有链

私有链

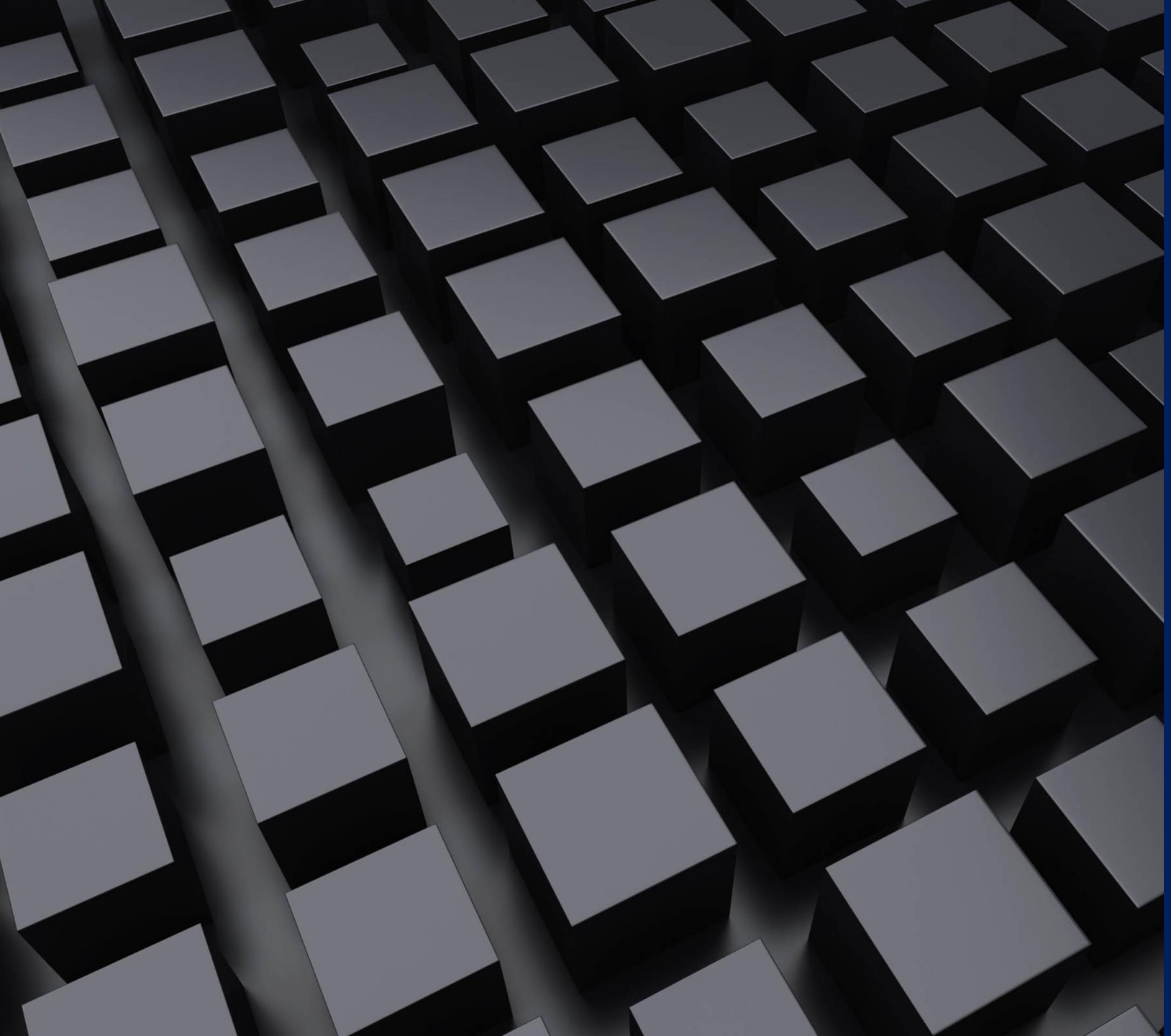
建立在某个企业内部，系统的运作规则根据企业要求进行设定，修改甚至是读取权限仅限于少数节点，同时仍保留着区块链的真实性和部分去中心化的特性。所有许可和认证都被单一个体或组织掌握，其公开程度完全取决于私有链的所有者

由若干机构联合发起，介于公有链和私有链之间，兼具部分去中心化的特性。所有许可和认证都被预选的节点或组织掌握，其公开程度取决于联盟链的共同所有者的绝大多数

联盟链

区块链应用生态圈


区块链
应用生态圈
金融
服务
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
医疗
健康
数字病历、隐私保护、健康管理
IP
版权
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
教育
档案管理、学生征信、学历证明、成绩证明、
产学合作
物联网
物品溯源、物品防伪、物品认证、网络安全性、
网络效率、网络可靠性
共享
经济
租车、租房、知识技能
通信
社交、消息系统
社会
管理
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
慈善
公益
社会公益
文化
娱乐
视频版权，音乐版权，软件防伪，数字内容
确权，软件传播溯源



THANKS

王士勇

2017年7月22日