企业内部培训
区块链技术

石恩名
广州优亿信息科技有限公司

01 区块链

区块链是什么？和其他的比起来有什么不同？

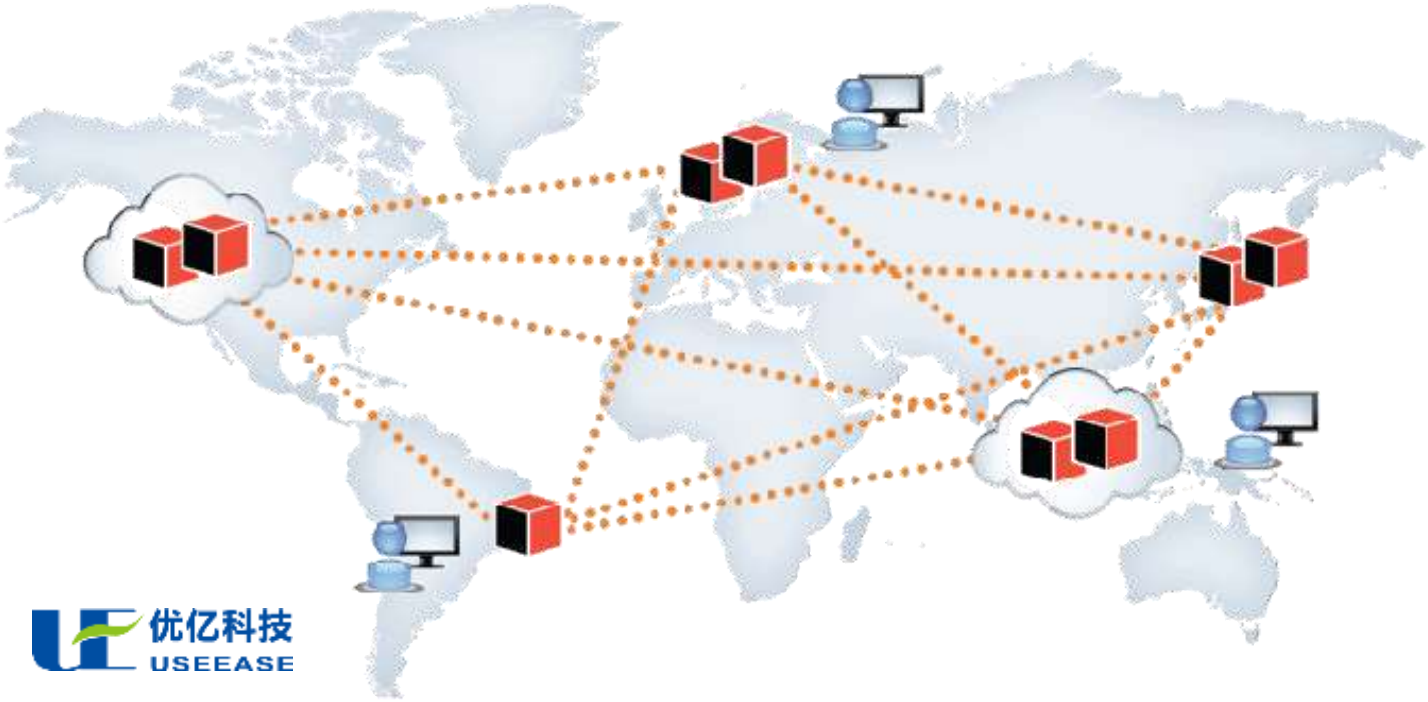
背景

传统的数据库管理系统问题：

- （1）由单一机构管理和维护， 在多方参与者协作的场景中， 因无法完全信任数据库中的数据。
- （2） 每方都需要单独构建一套承载自己业务数据的数据库， 多方数据库间的数据差异会导致繁琐的人工对账和争议。

背景

- 区块链是一种利用分布式数据存储、点对点传输、共识机制、加密算法等计算机技术构建的一种**去中心化、 不可篡改、 可追溯、 多方共同维护的**分布式**数据库**（区块链本质上看成一种数据库，任何需要保存的信息，都可以写入区块链，也可以从里面读取）
- 区块链最早起源于比特币的设计，是比特币的底层技术和基础架构。



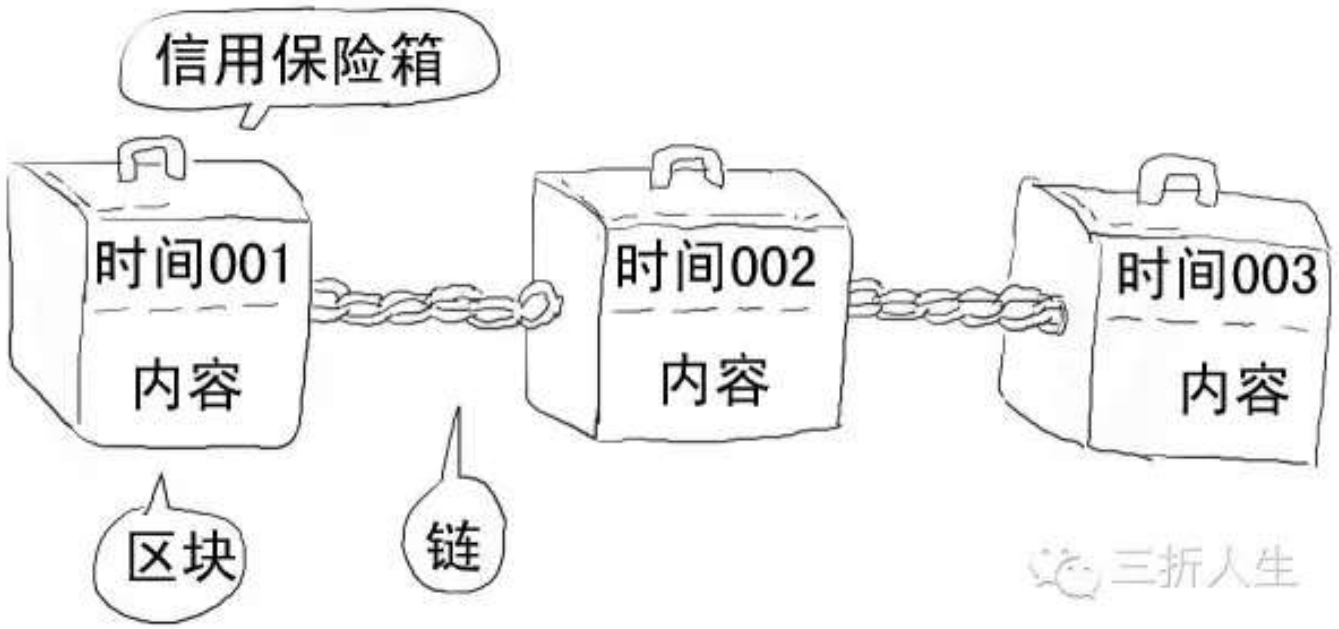
优亿科技 USEEASE

区块链基本概念

区块链，顾名思义，是由区块(Block)和链(Chain)组成的。

区块（Block）：区块很像数据库的记录，每次写入数据，就是创建一个区块。

链（Chain）：每个区块都连着上一个区块，形成链条式的数据结构记录所有的信息。



区块链基本概念

区块链技术是一种**解决信任问题、降低信任成本**的信息技术方案。通过区块链技术，互联网上的各个用户成为一个节点并相互连接起来，所有在此区块链架构上发布的内容都会在加密后被每一个节点接收并备份，换而言之每一个节点都可以查看历史上产生的任何数据。各节点将加密数据不断打包到区块中，再将区块发布到网络中，并按照时间顺序进行连接，生成永久、不可逆向的数据链，这便形成了一个公开透明的受全部用户的监督的区块链。

区块链的运作流程

运行区块链的基本流程：

1. 新的交易操作（transaction）向全网进行广播；
2. 通过共识算法（Consensus Algorithm）选择leader将交易操作写入一个区块(block)；
3. 写入区块被其他节点认可和接受。

区块链特点

区块链特点：

- （1）去中心化。
- （2）高可信。
- （3）不可篡改。
- （4）可追溯。
- （5）高可用。

区块链的三种形态

公共链：系统安全性由工作量证明或权益证明机制保证，一般需要数字货币提供交易验证激励，容易进行应用程序大规模部署，全球范围可以访问，不依赖于单个公司或辖区，匿名性强，任何参与者都可以在中写入、读取、参与交易验证（例：比特币）。

联盟链：多中心，参与人为预先根据一定特征所设定。系统内交易确认节点为事先设定，并通过共识机制确认，一般不需要数字货币提供交易验证激励。联盟链容易进行节点权限设定，拥有更高应用可扩展性。联盟链可大幅降低异地结算成本和时间，比现有系统更简单，效率更高，同时继承去中心化优点减轻垄断压力（例：全球银行加入R3)。

私有链：没有去中心，但有分布式特点，中心控制者制定可参与和进行交易验证成员范围，系统内不需虚拟货币提供奖励（例：中国银行可以联合其全球各城市分行，完成内部数据传输备份，转帐等业务。）

	共有链	联盟链	私有链
中心化程度	分布式去中心化	多中心式	单中心式
参与主体控制	任何节点可接入	预先设定具有特定特征的参与主体	由中心控制者制定参与成员
信息公开程度	账本完全公开(可匿名)	联盟内部公开(可匿名)	公司内部公开(可匿名)

02 共识算法

共识算法也是一致性算法，在分布式数据库里面就已经很成熟了，那么到了区块链中，其有什么不同呢？

传统分布式数据库一致性算法

paxos算法是个分布式一致性协议，它是一种基于消息传递模型的一致性算法。Paxos算法分为两个阶段。

阶段一：寻值阶段

（a）Proposer选择一个提案编号N，然后向半数以上的Acceptor发送编号为N的Prepare请求。

(b) 如果一个Acceptor收到一个编号为N的Prepare请求，且N大于该Acceptor已经响应过的所有Prepare请求的编号，那么它就会将它已经接受过的编号最大的提案（如果有的话）作为响应反馈给Proposer，同时该Acceptor承诺不再接受任何编号小于N的提案。

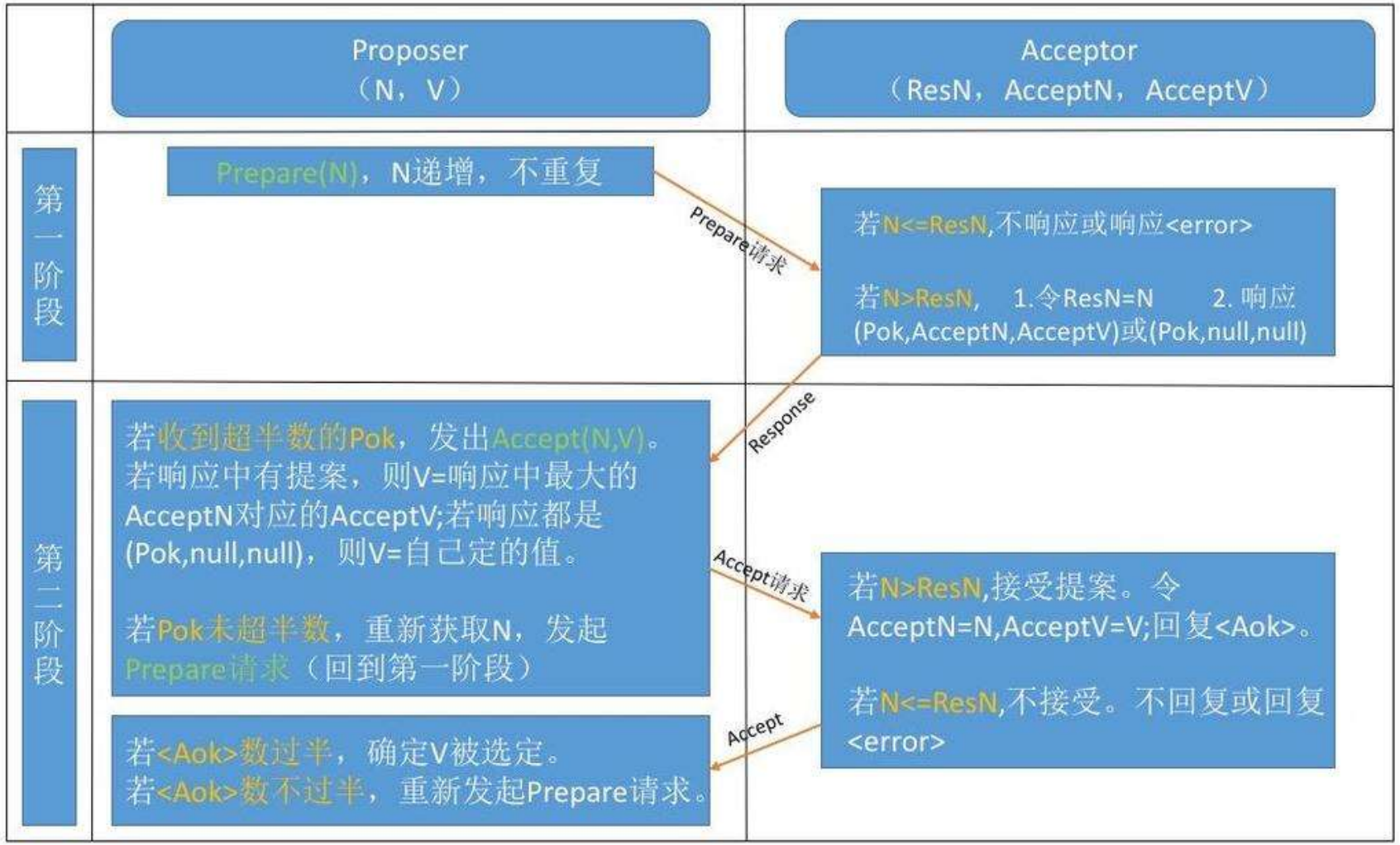
阶段二：提案阶段

(a) 如果Proposer收到半数以上Acceptor对其发出的编号为N的Prepare请求的响应，那么它就会发送一个针对[N,V]提案的Accept请求给半数以上的Acceptor。注意：V就是收到的响应中编号最大的提案的value，如果响应中不包含任何提案，那么V就由Proposer自己决定。

(b) 如果Acceptor收到一个针对编号为N的提案的Accept请求，只要该Acceptor没有对编号大于N的Prepare请求做出过响应，它就接受该提案。

Paxos算法

算法演示



Raft算法

Raft算法是一种和Paxos算法一样的分布式一致性协议。（Raft的优势就是容易理解和实现，可以少出错误~~）

Raft的工作模式是一个Leader和多个Follower模式，其安排了三种角色：

(1)Leader: 处理所有客户端交互，日志复制等，一般一次只有一个Leader.

(2)Follower: 类似选民，完全被动

(3)Candidate：候选人。

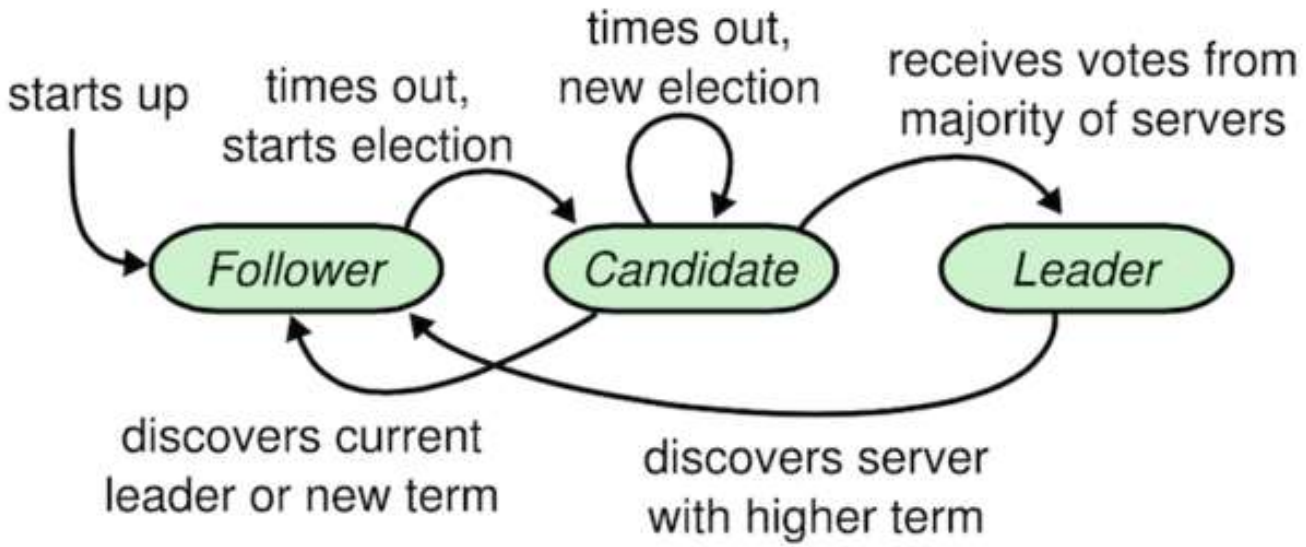


图 4：服务器状态。跟随者只响应来自其他服务器的请求。如果跟随者接收不到消息，那么他就会变成候选人并发起一次选举。获得集群中大多数选票的候选人将成为领导者。领导人一直都会是领导人直到自己宕机了。

Raft算法

Raft算法分为两各阶段：

第一个阶段是选举领导人；

第二阶段是由领导人对其他节点对一致性的操作。

Raft算法

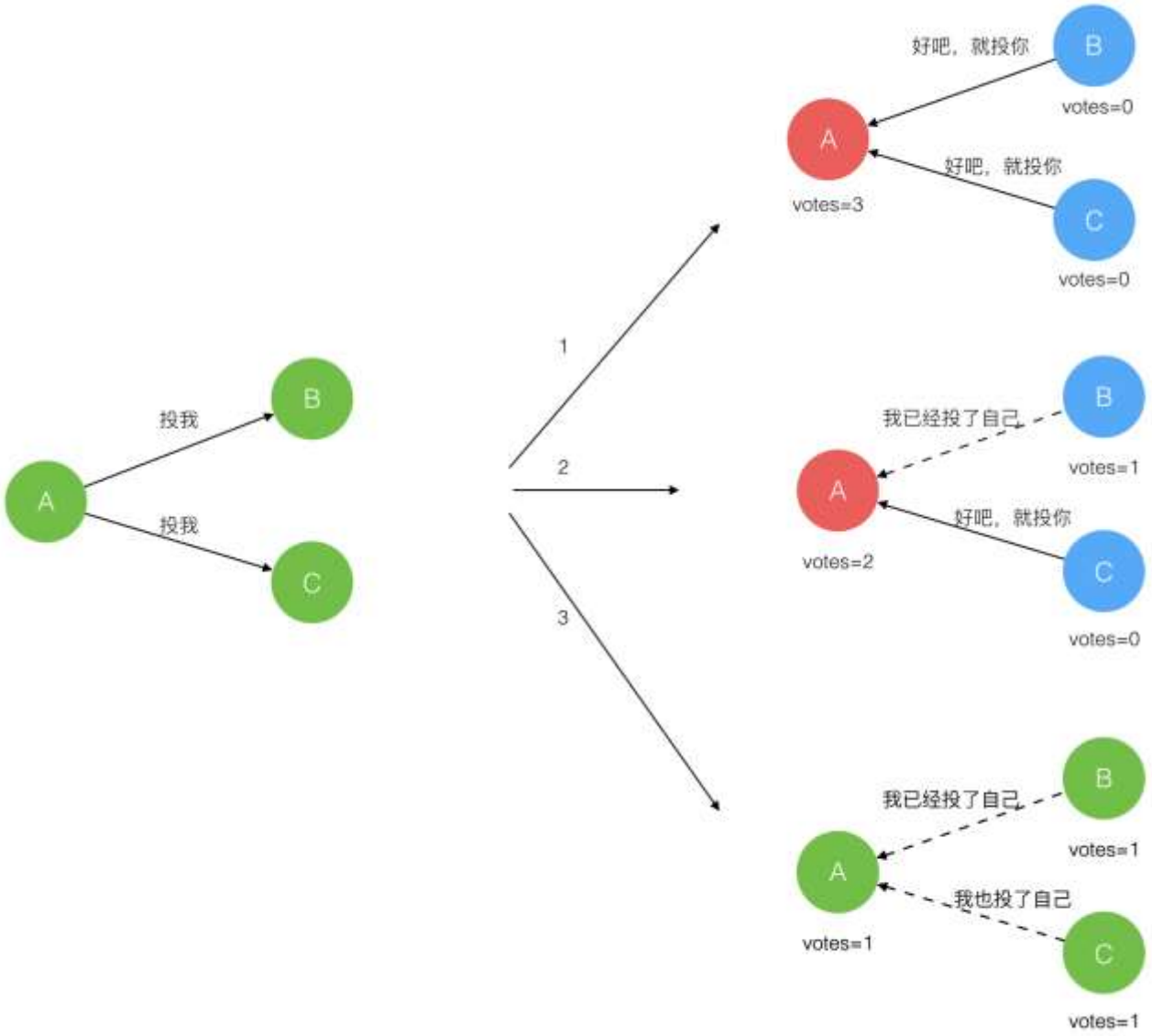
选举阶段：

（1）初始状态时所有server都处于Follower状态，并且随机睡眠一段时间，最先醒来的server A进入Candidate状态

（2）Candidate状态的server A有权利发起投票，向其它所有server发出请求，请求其它server给它投票成为Leader。

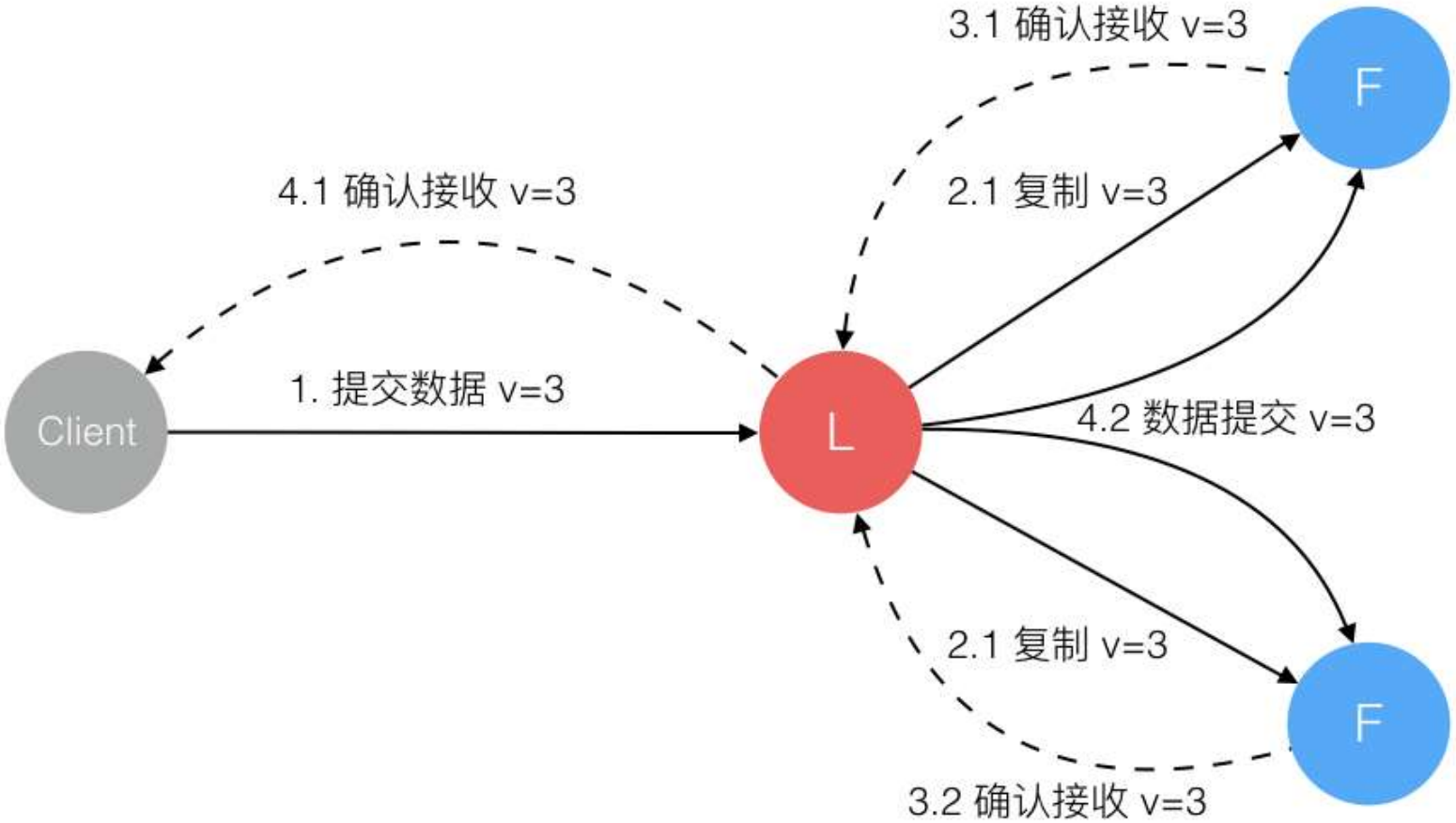
（3）当其它server收到请求后，将自己仅有的一票投给server A，同时继续保持Follower状态并重置选举计时器。

（4）当server A收到大多数（超过一半以上）server的投票后，就进入Leader状态，成为系统中仅有的Leader。



Raft算法

一致性操作阶段



区块链共识算法

传统分布式数据库主要使用 Paxos 和 Raft 算法解决分布式一致性问题， 虽然它可以解决报文可能发生丢失和延时等问题，但面对拜占庭问题的时候，决策就可能混乱，即其假定系统中每个节点都是忠诚、不作恶的。

但这对于处于公有链上的，有着大量不可信任节点的分布式数据库来说是一种灾难，会遇到各类问题，比如拜占庭问题、女巫攻击问题等。

区块链共识算法

公有链的区块链共识算法主要包括：

1. 工作量证明机制(Proof of Work, POW)
2. 权益证明机制(Proof of Stake, POS)。
3. 股份授权证明机制(Delegated Proof of Stake, DPOS)

工作量证明机制(POW)

工作量证明机制（PoW），其机制是通过**工作量**的大小来决定Leader，即工作量证明，被leader打包的区块可以获得整个网络的认可。工作量主要指算力，即计算设备每秒能进行哈希运算的次数。一台设备的算力在全网算力中所占的比重即由这台设备创建新区块(挖矿)的概率。PoW 机制可有效应对**女巫攻击**， 其依靠分布式节点间的算力竞争来保证全网区块链数据的一致性和安全性。

PoW 机制将经济激励与共识过程相融合， 促使更多节点参与挖矿并保持诚信， 从而主动增强了网络的可靠性与安全性。

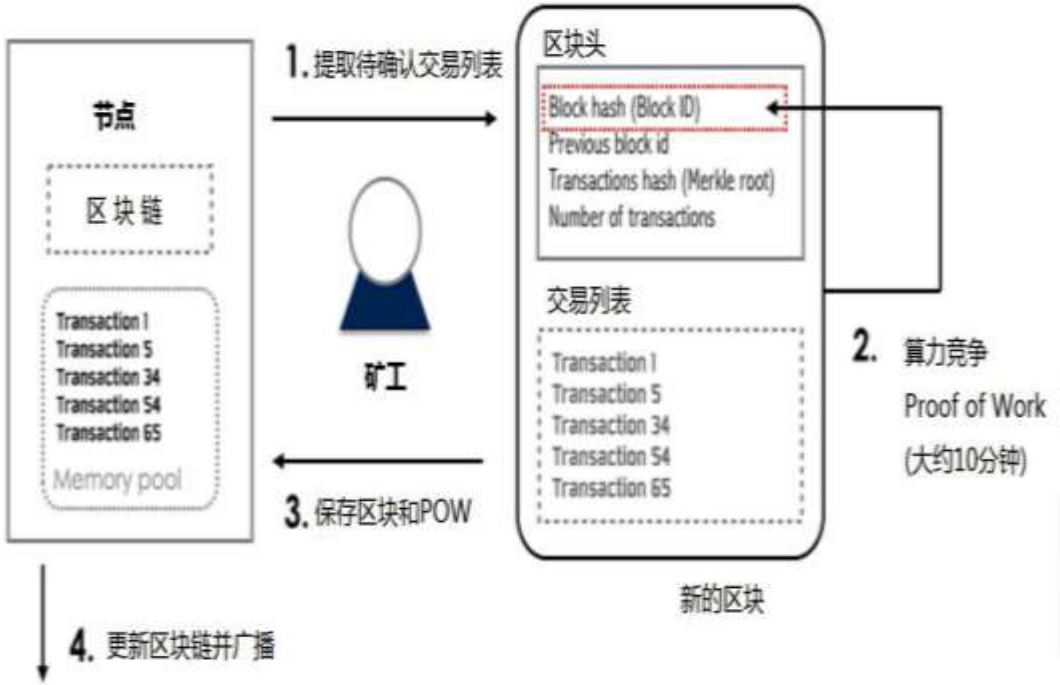
POW流程

1、每笔新交易被广播到区块链网络的所有节点。

2、为了构建新的区块， 每个节点收集自前一区块生成以来接收到的所有交易， 并根据这些交易计算出区块头部的 Merkle 根。将区块头部的随机数 Nonce 从 0 开始递增加 1， 直至区块头的两次SHA256 哈希值小于或等于难度目标的设定值为止。

3、全网节点同时参与计算， 若某节点先找到了正确的随机数， 则该节点将获得新区块的记账权及奖励， 并将该区块向全网广播。

4、其它节点接收到新区块后， 验证区块中的交易和随机数 Nonce 的有效性， 如果正确， 就将该区块加入本地的区块链， 并基于该块开始构建下一区块。



分叉问题

分叉问题：若多个区块同时被创建就会引起分叉问题。

解决方案：

（1）比特币采用确定主链，忽视分支的方法。当发生分叉时， 最长的链即花费了最多算力的链被认为是主链， 其它则被认为是分支， 分支中的所有交易会被忽略。比特币将分支结点上的区块称为孤块， 并会将其作为废块而丢弃。**一般地，比特币假定在6个区块生成以后可以确定交易。**

（2）以太坊采用GHOST协议处理。GHOST 协议认为分支上的有效区块对确认主链上的交易也有贡献， 因而没有丢弃该区块， 而是将该区块作为叔块并给予相当主块 87.5%的奖励，给予叔块的直接子块相当主块 12.5%的奖励， 矿工每引用一个叔块给予相当主块 3%的奖励。

股权证明机制(POS)

股权证明和工作量证明一样，是一种用于公有链的共识算法，其根据矿工在区块链中拥有的股权（数字货币量） 来决定其挖矿的难度。

$$H(n||h) \leqslant s(M).t$$

M 为某矿工； 函数 s 返回该矿工拥有的股权；当矿工 M 拥有的股权越多， 挖矿的整体难度就会越低， 其越容易找到合适的 n。

Casper共识算法

Casper共识是以太坊基于 PoS 机制提出。 Casper 以智能合约的方式实现，根据抵押的以太币数量和时间， 成比例的分配区块的记账权和奖励。 与 PoS 机制不同， Casper 还引入了惩罚措施， 一旦发现某个矿工作弊， 其抵押的所有以太币将全被罚没， 参与共识和出块的权利也会被取消。

基于Casper 共识的以太坊一个区块的挖矿时间为4秒，而比特币则需要10分钟。

股份授权证明机制（DPOS）

股份授权证明机制（DPOS）采用“股份投票”的方式决定谁来生成区块。它的原理是让每一个持有“股份”的人进行投票，由此产生N个超级节点或者矿池，而这N个超级节点彼此的权利是完全相等的。从某种角度来看，DPOS有点像是议会制度或人民代表大会制度。如果代表不能履行他们的职责（当轮到他们时，没能生成区块），他们会被除名，网络会选出新的超级节点来取代他们。

EOS使用DPOS共识机制

实用拜占庭容错机制（PBFT）

实用拜占庭容错机制（PBFT）是一种状态机副本复制算法，状态机在分布式系统的不同节点进行副本复制。每个状态机的副本都保存了服务的状态，同时也实现了服务的操作。在**保证活性和安全性**的前提下提供了(n-1)/3的容错性。

实用拜占庭容错流程

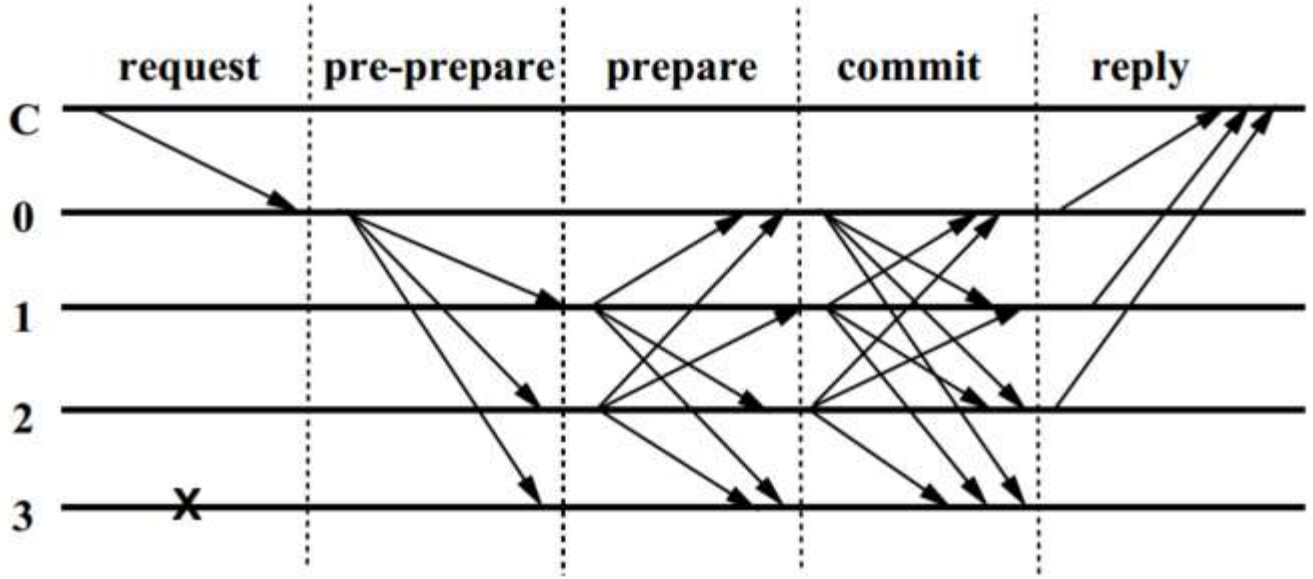
PBFT算法流程：

1.客户端向主节点发送请求调用服务操作

2.主节点通过广播将请求发送给其他副本

3.所有副本都执行请求并将结果发回客户端

4.客户端需要等待f+1个不同副本节点发回相同的结果，作为整个操作的最终结果。



总结

（1）公有链的共识算法，均需要“代价”作为支撑，比如工作量、股权。

（2）对于私有链来说，其和传统的分布式数据一样，采用paxos算法和Raft 算法即可。

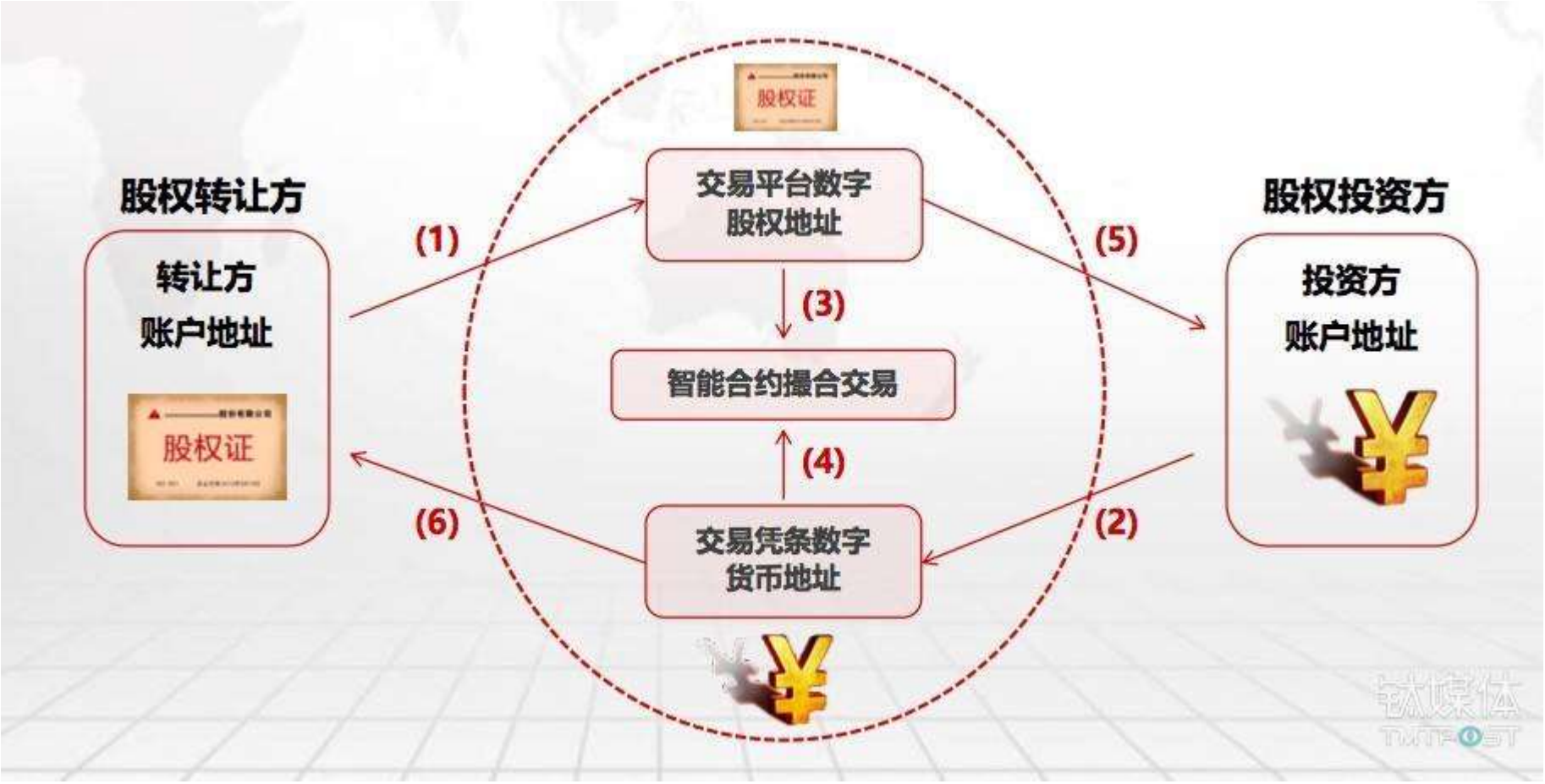
（3）“因地制宜”最重要，根据不同的场景采用不同的共识算法解决问题。

03 智能合约

智能合约是用程序语言编写的商业合约， 在预定条件满足时， 能够自动强制的执行合同条款， 实现“代码即法律” 的目标。

智能合约

智能合约是用程序语言编写的商业合约， 在预定条件满足时， 能够**自动强制的执行**合同条款， 实现**“代码即法律”** 的目标。



智能合约

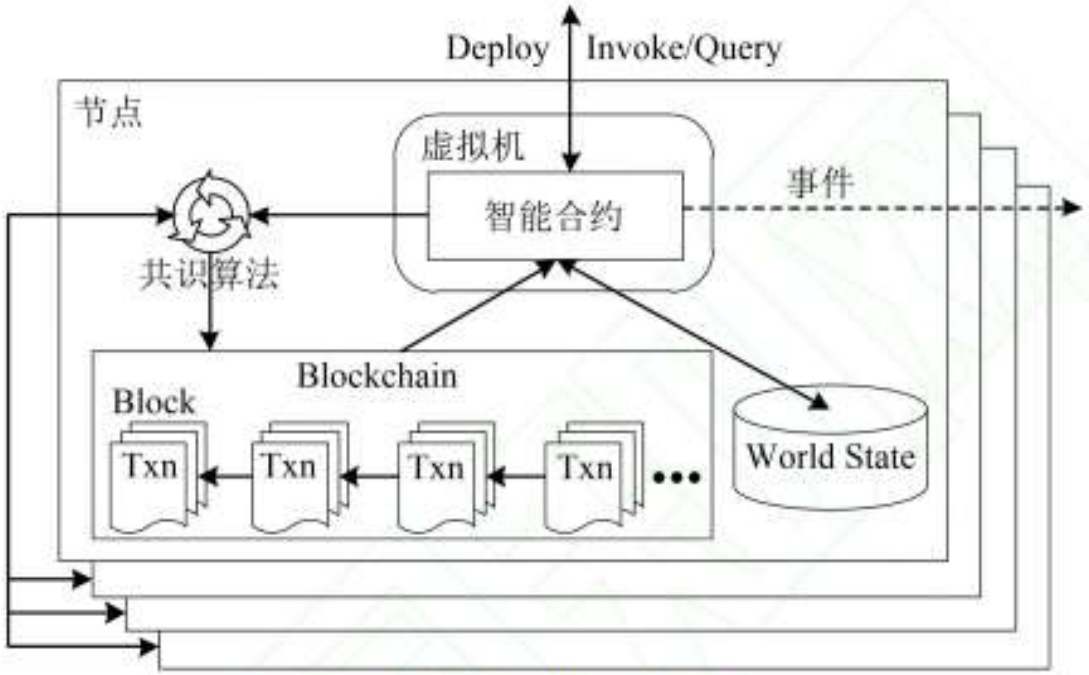


图 6 智能合约的运作机制

（1）依照商业逻辑编写完智能合约代码后， 需要将其发布到区块链网络节点上。

（2）调用涉及到修改操作， 需要先在全网达成共识， 之后修改操作会被记录在区块链，修改结果会被存在状态数据库。调用查询操作，则无需共识， 也不需被记录在区块链上。

（3）智能合约支持合约内部事件的注册与通知机制，外部应用与智能合约间的关系非常类似于传统数据库应用与存储过程间的关系， 存储过程运行于数据库管理系统之中， 访问关系数据库数据， 而智能合约运行于区块链系统之中， 访问区块和状态数据。

04 可扩展性

区块链想要真正做到更深度化的应用和普及，关键就是要解决交易的吞吐量和交易的速度问题

可扩展性

区块链（公有链）的**吞吐量和交易速度**一直是区块链发展和应用的关键技术瓶颈。

币价创新高的背后：比特币网络严重拥堵，高峰期有逾10万笔交易未确认

Wendy 2017-02-24 15:01 发布在

2月22号，比特币网络中的交易队列（mempool），达到了历史新高。过10万笔交易没有确认，大多数人都迟”。

以太坊区块链出现拥堵 罪魁祸首竟是“云养猫”

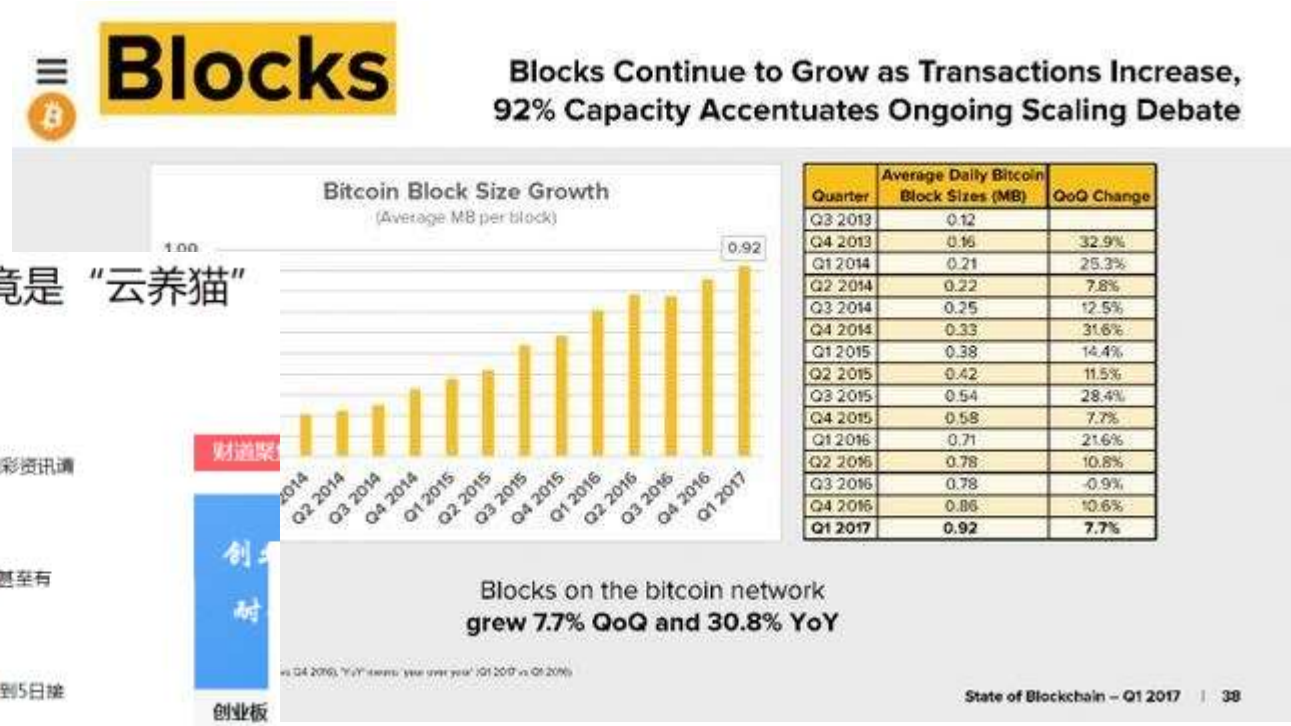
2017-12-05 22:03:00 华尔街见闻

本文来自华尔街见闻（微信ID：wallstreetcn），编辑刘怡心。更多精彩资讯请登陆wallstreetcn.com，或下载华尔街见闻APP。

一款上线不久的“吸猫”游戏，竟然令以太坊区块链在近日显著拥堵，甚至有些“不堪重负”。

12月3日开始，以太坊待处理交易几乎直线上升，从此前的不到5000，到5日接近凌晨6点触及2万关口。

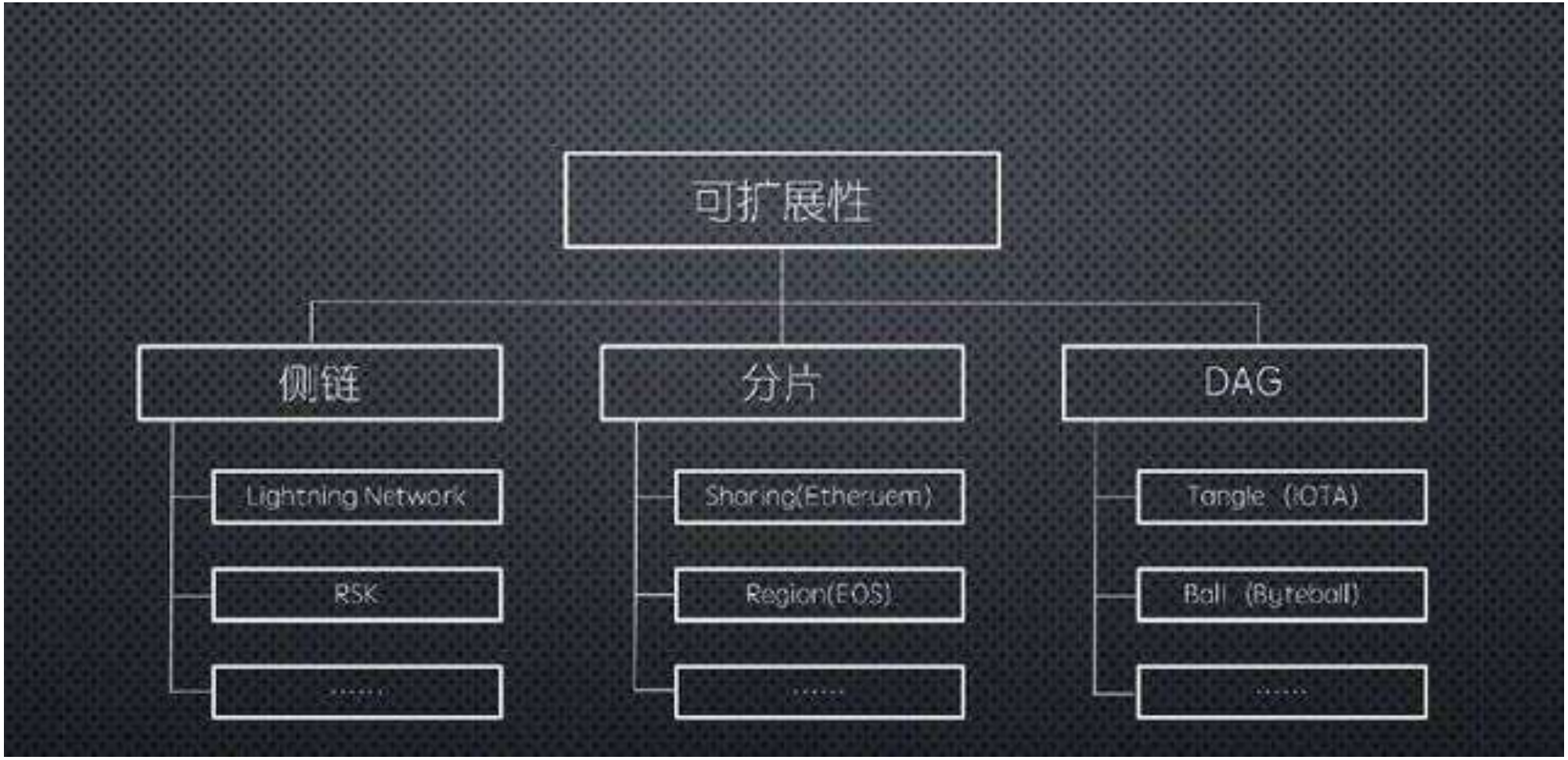
这个聚众云吸猫的游戏名为Cryptokitties，是基于以太坊平台运行的。用户在游戏中可以养大、买卖并繁育“电子宠物”小猫，每只小猫和繁衍的后代都是独一无二的。



优亿科技 USEEASE

可扩展性

现有的主流的可扩展性解决方案可分为三种**侧链**技术(SideChains)、**分片**技术(Sharing)和**有向无环图（DAG）**。



侧链

侧链（Side Chains）是通过在外部搭建一个新的交易通道嫁接到主链，从而解决扩容问题。

侧链的一个典型就是比特币的**闪电网络**（Lighting Network）：A和B两人可以把比特币放到一个多重签名钱包中锁定（链下），然后进行交易签名更改双方各自能取回的比特币数量。交易参与方可以随时关闭交易通道，最后一笔经过签名且包含最新余额动态的交易最终将会被广播并写入比特币区块链。

分片

分片其实是一种传统数据库的技术，它将大型数据库分成更小、更快、更容易管理的部分。分片技术可以理解为在将主链在内部进行切分。

现在用了分片技术的主要有以太坊的sharing和EOS的Region。

以太坊分片机制介绍

以太坊依据账户地址将全网划分为多个相对独立的分片， 每个分片内维护一条独立子链， 用户可自行选择在哪个分片执行自己的交易， 每个节点根据自身的计算和存储能力选择加入一到多个分片， 并处理和存储这些分片上的交易。

全网节点分工配合以覆盖到所有分片， 如果需要访问本节点没有的交易数据， 则利用轻客户端技术从其它分片节点读取。 全网节点可并行的处理和存储不同的交易数据， 使得全网交易处理能力不再受限于单一节点， 单一节点也不需处理、 存储全部数据。

有向无环图

有向无环图（Directed Acyclic Graph，DAG）是一种数据结构，不同于传统区块链的底层数据结构Blockchain设计，其通过数据单元之间的引用来完成交易的确认。

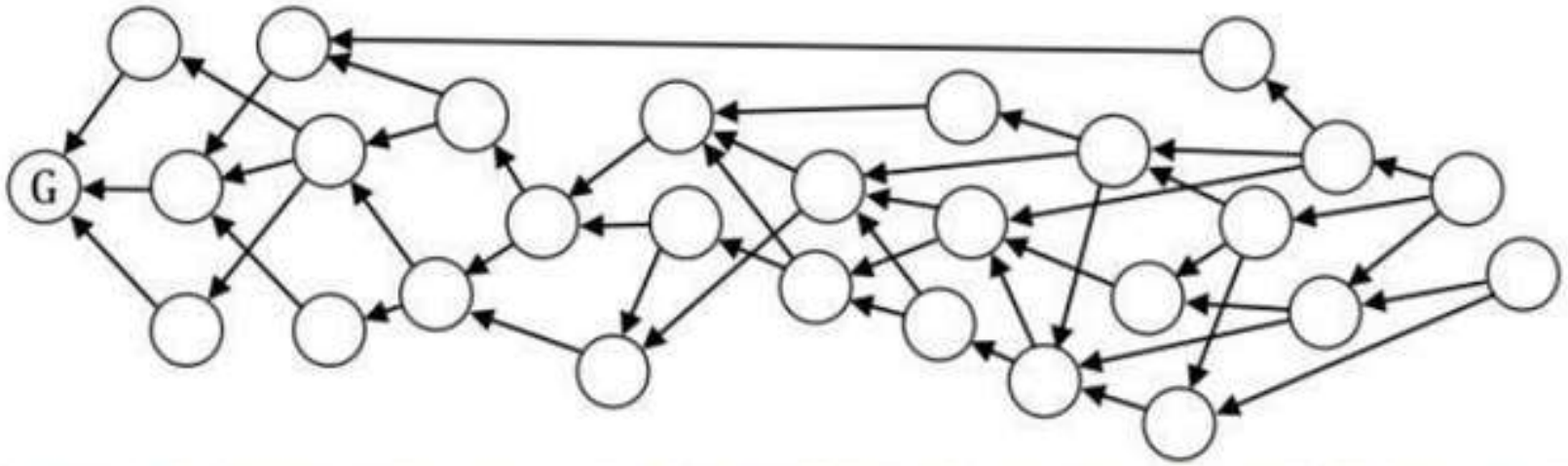


Figure 1. Storage units connected into a DAG. Arrows are from child to parent, G is the genesis unit.

DAG流程

（1）客户端自主异步地提交一个数据单元，客户端采用点对点互相校验

（2）通过数据单元之间的引用来完成交易的确认，后面发生的单元去引用前面的单元。

（3）数据单元间通过引用关系链接起来，从而形成具有半序关系的DAG

（4）通过特定的方法选择“主链”，“主链”确立了，才把“双花”检测出来剔除，在确定“主链”以前它是一个并行验证的操作，而且是并行往数据结构上放。（“主链”的选择采用共识算法进行确定）

有向无环图

目前采用DAG作为存储结构的代表项目有dagcoin、Byteball、Iota。

	IOTA	Byteball	TrustNote
代币	IOTA	Byte	TTT
市值	140亿美元	4亿美元	–
共识机制	PoW权重累加	12名公证人	TrustME-PoW/BA
智能合约	不支持	声明式合约	高级声明式合约
奖励机制	无	交易引用和公证	交易引用和挖矿
节点分类	全节点 轻节点	全节点 轻节点	超级节点 全节点 轻节点 微节点
交易费	无	有	有
双花问题	PoW权重比较	MainChain定序	MainChain定序
低交易量问题	中心化的协调者	弱中心化的公证人	TrustME公证节点

优亿科技 USEEASE

05 案例和应用

区块链的应用广泛，可以利用区块链的不可篡改、防抵赖等特性解决之前难以解决的问题。

业务架构

优亿科技
USEEASE

区块链各领域应用

领域	案例	服务商/应用商	时间
跨境支付	Visa B2B Connect	Visa、Chain	2017年（计划）
保险	LenderBot	Stratumn、Deloitte、Lemonway	2016年
证券	Linq	纳斯达克、Chain	2016年
物联网	ADEPT	IBM、三星	2015年
物联网	汽车租赁	Visa、DocuSign	2015年
文化	Ujo Music	Ujo Music	
教育	BitProof	BitProof、Holberton School	
房地产	Ubitquity	Ubitquity	
医疗	Guardtime	Guardtime、爱沙尼亚电子卫生基金会	
慈善	BitGive	BitGive基金会	2015年
供应链	Provenance	Provenance	

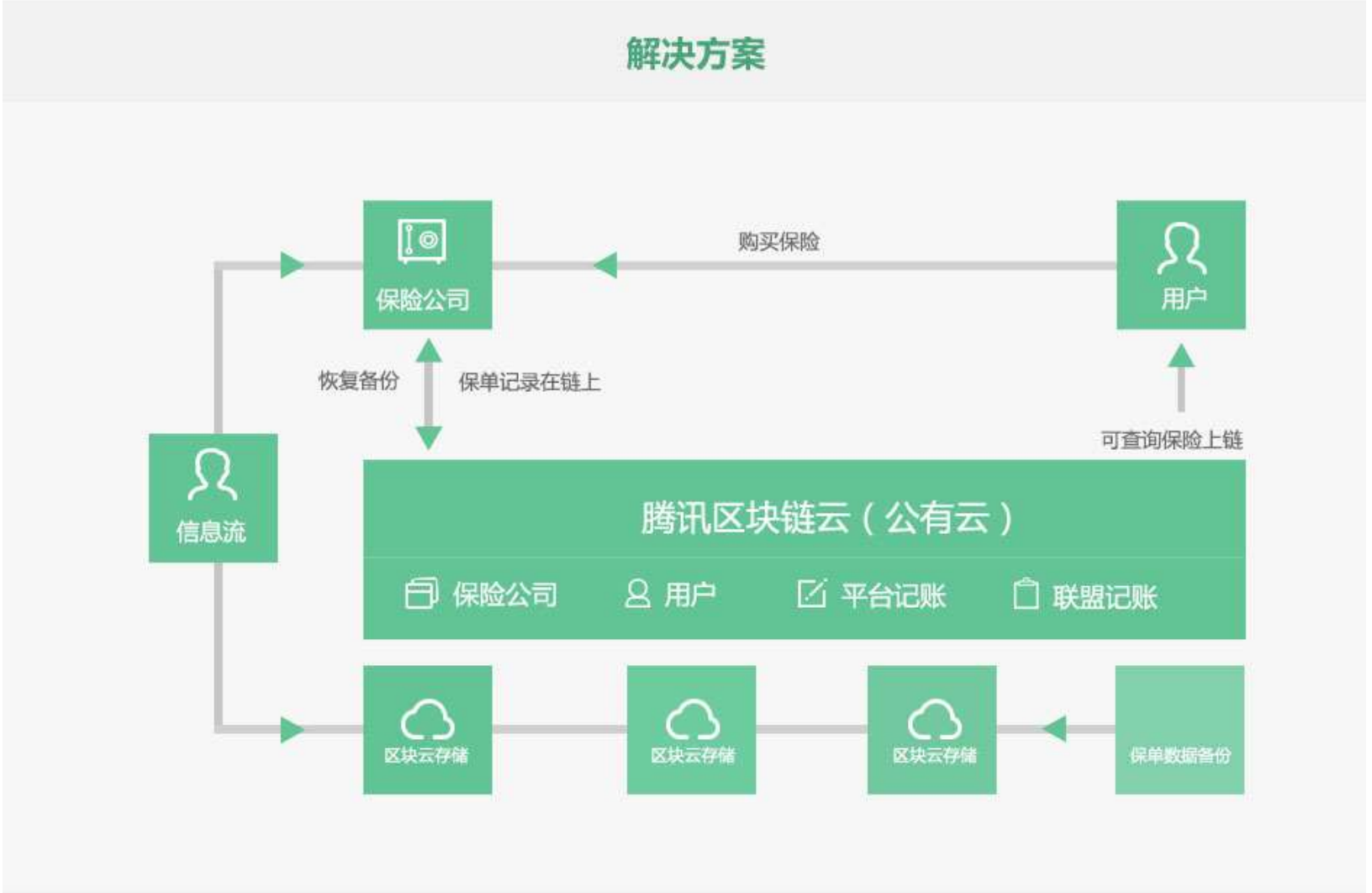
区块链应用场景——腾讯云


区块链场景应用:
数字资产
鉴证证明
共享账
解决方案
以腾讯微黄金红包为例
FiT
购买黄金（资产发行）
申请提现（资产兑付）
用户
发送红包（资产转让）
用户
恢复备份
可查询黄金红包记录上链
腾讯区块链云（公有云）
FiT
用户
银行
联盟记账
区块云存储
区块云存储
区块云存储

区块链应用场景——腾讯云

区块链场景应用：

数字资产　鉴证证明　共享账

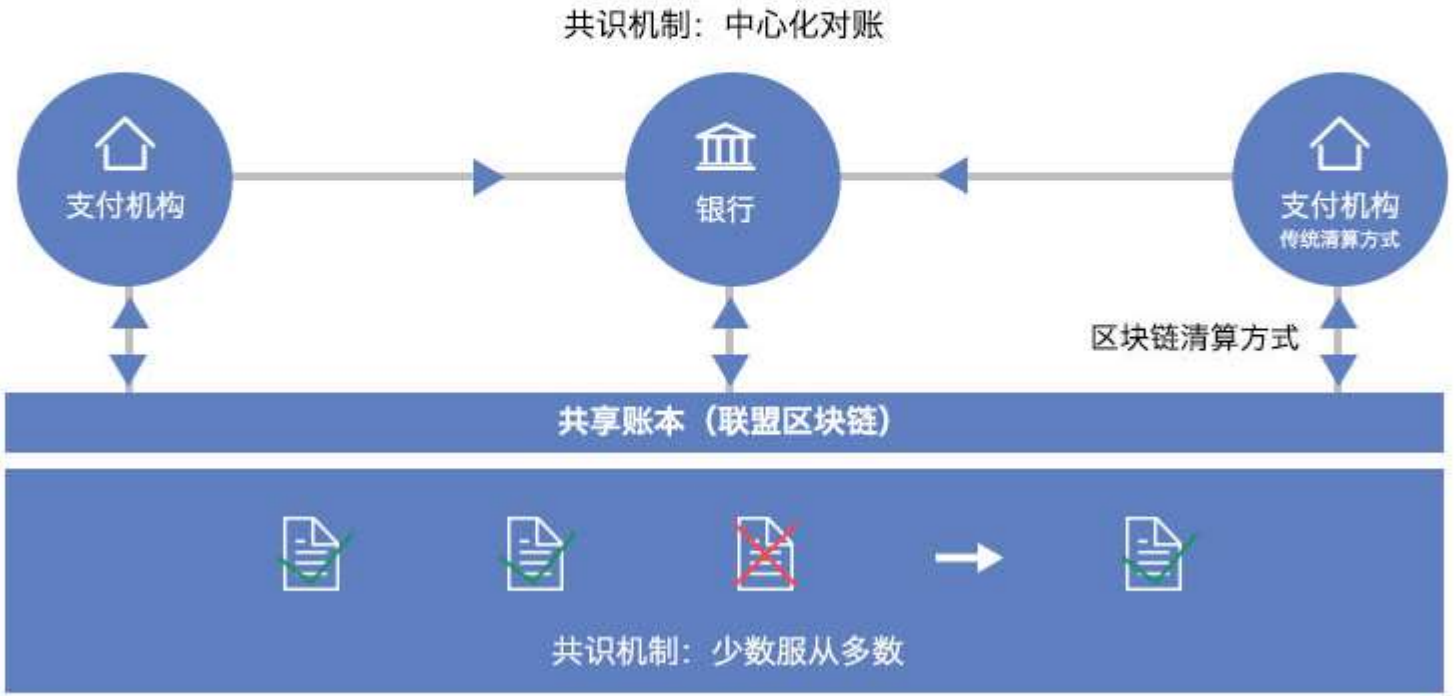


区块链应用场景——腾讯云

区块链场景应用：

数字资产　鉴证证明　共享账

解决方案



联盟链发展

中国区块链三大联盟			
	金链盟	中国分布式总账基础协议联盟 (China Ledger)	中国区块链研究联盟 (CBRA)
设立目标	在3至5年内研发一条或多条金融区块链，推出多种广受欢迎的区块链终端应用，制定一批高水平联盟标准，申请一批区块链专利技术。	1.聚焦区块链资产端应用，兼顾资金端探索；2.构建满足共性需求的基础分布式账本；3.精选落地场景，开发针对性解决方案；4.基础代码开源，解决方案在成员间共享。	打造区块链技术的研究与交流平台；打造政策沟通平台，厘清区块链技术在现有监管模式与货币政策操作中的定位;打造区块链技术的市场应用平台，推动具体应用规则的规范化、标准化，进行项目落地与路演，形成区块链研究领域具有高端学术品味和较强国际影响力的中国特色新型智库。
成立地点	深圳	上海	北京
设立时间	2016.5.13	2016.4.19	2016.1.5

R3CEV — 金融企业的区块链大联盟

- 2015年9月由R3发起的区块链联盟，目前已有42家全球主要金融机构加入。
- 采用联盟策略，R3的使命是引导各成员银行在涉及区块链和分布式帐本技术的工程、实验以及研究项目上进行协作。重量级银行的加入赋予了R3较强的权威性。
- 提供区块链技术的五家厂商分别为Chain，Ethereum，Eris Industries，IBM，Intel。云基础设施由Amazon，IBM和Microsoft Corporation提供。
- 2016年4月，R3公布了其区块链技术测试的八大核心领域，分别为互操作性、支付、结算、金融交企业债券、回购、掉期和保险。
- 目前加入R3的中国公司有中国平安、招商银行、中国外汇交易中心、民生银行。

区块链技术在国内的发展：金链盟

6月1日,中国区块链合作联盟“金链盟”在深圳成立

金链盟由微众银行倡议，联合平安银行、招商网络、恒生电子、赢时胜、四方精创、京东金融、深圳市金融信息服务协会等25家机构共同发起，腾讯、华为、山东城商行合作联盟等6家机构作为成员单位加入。联盟目标在3到5年内研发出1条或多条供所有联盟单位使用的区块链，并以此为基础部署区块链应用。

区块链技术在国内的发展：ChinaLedger

2016年4月19号，专注于分布式账本及其衍生技术研究的中国分布式总账基础协议联盟ChinaLedger在北京正式成立。

ChinaLedger联盟的主要工作任务是共同合作研究区块链技术，结合中国政策法规和中国金融行业独特的业务逻辑，以使得符合中国的政策法规、国家标准、业务逻辑和使用习惯。此外，将来ChinaLedger联盟的区块链底层技术协议将会是开源的，各界可以在这个基础协议上搭建具体的应用场景。

发起单位：

中证机构间报价系统股份有限公司、中钞信用卡产业发展有限公司北京智能卡技术研究院、浙江股权交易中心、深圳招银前海金融资产交易中心、厦门国际金融资产交易中心、大连飞创信息技术有限公司、通联支付网络服务股份有限公司、上海钜真金融信息服务有限公司、深圳瀚德创客金融投资有限公司、乐视金融、万向区块链实验室等十余家单位组成。万向区块链实验室是ChinaLedger联盟的秘书处。

除11家发起人单位以外，ChinaLedger联盟也邀请了英国瑞银高级创新经理Alex Baltin、加拿大多伦多交易所首席数字官Anthony Di Iorio、以太坊创始人Vitalik Buterin、比特币核心开发者Jeff Garzik作为联盟海外技术顾问。

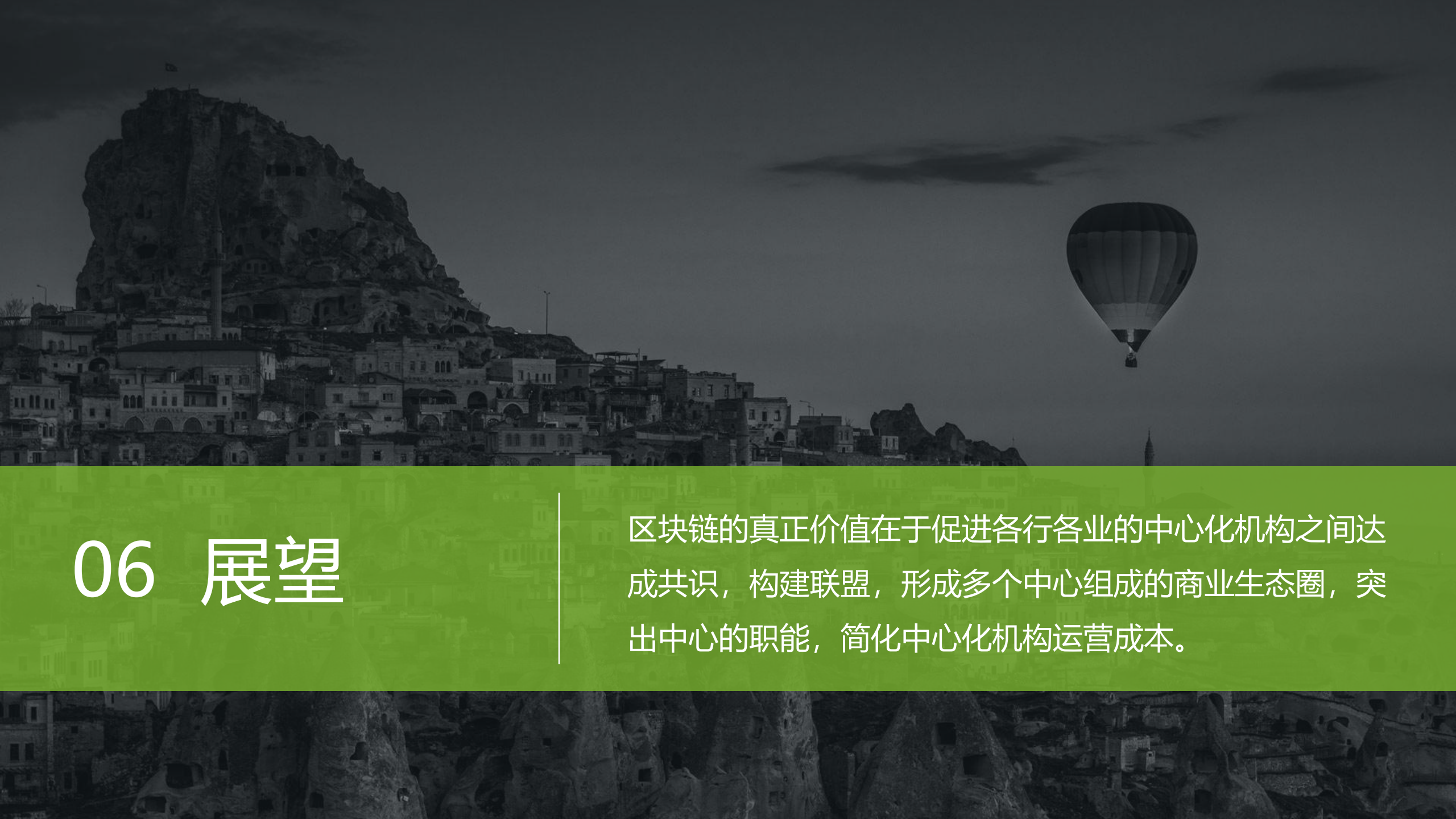
在区块链技术向各个领域特别是金融领域迅速渗透的新形势下，各国的金融机构、资本市场、信息技术领域都面临着巨大的挑战和机遇。利用区块链技术打造价值互联互通的基础设施，已经被全球很多国家提到战略的高度。由全球性的金融机构组成的跨境区块链联盟已经在积极行动并推出了阶段性成果。

区块链技术在国内的发展：银行间市场区块链技术研究组

2016年8月12日,经全国金融标准化技术委员会批复，银行间市场技术标准工作组区块链技术研究组于近日在上海成立。继中国分布式总账基础协议联盟、中国互联网金融协会区块链研究工作组后，区块链技术研究组成为了国内第三个区块链组织。

区块链技术研究组当前的工作重心将集中在银行间市场区块链技术、监管及法律框架的前瞻性研究以及与R3等国际区块链联盟的联系上。区块链技术研究组的成立将对区块链技术在银行间市场基础设施和应用服务的规划和建设产生深远影响。

成员单位：涵盖银行间市场中介机构、市场成员和科研机构；包括中国外汇交易中心、上海黄金交易所、上海清算所、中国国债登记公司、中国银行间市场交易商协会、中国银联、工商银行、农业银行、交通银行、浦发银行、上海银行、汇丰银行、花旗银行、平安保险、中信证券、道富银行、中国金融电子化公司、复旦大学、浙江大学19家机构。



06 展望

区块链的真正价值在于促进各行各业的中心化机构之间达成共识，构建联盟，形成多个中心组成的商业生态圈，突出中心的职能，简化中心化机构运营成本。

展望

区块链虽有去中心化的特性，但很多线上业务的纠纷无法离开中心来解决。因此**区块链的真正价值在于促进各行各业的中心化机构之间达成共识，构建联盟**，形成多个中心组成的商业生态圈，这样的生态系统突出了中心的职能，大大简化了中心化机构运营成本。


Thanks for
your attention!