比特币价格从诞生时的一美元兑换1300个比特币，到2021年峰值时6.1万多美元兑换1个比特币，这期间涨了几千万倍。很多人对区块链了解甚少，今天的分享系统地介绍了区块链入门及技术运用，值得学习研读，提示自己的认知[加油]

学习目录：

1、你听过的区块链

2、现实世界存在的问题

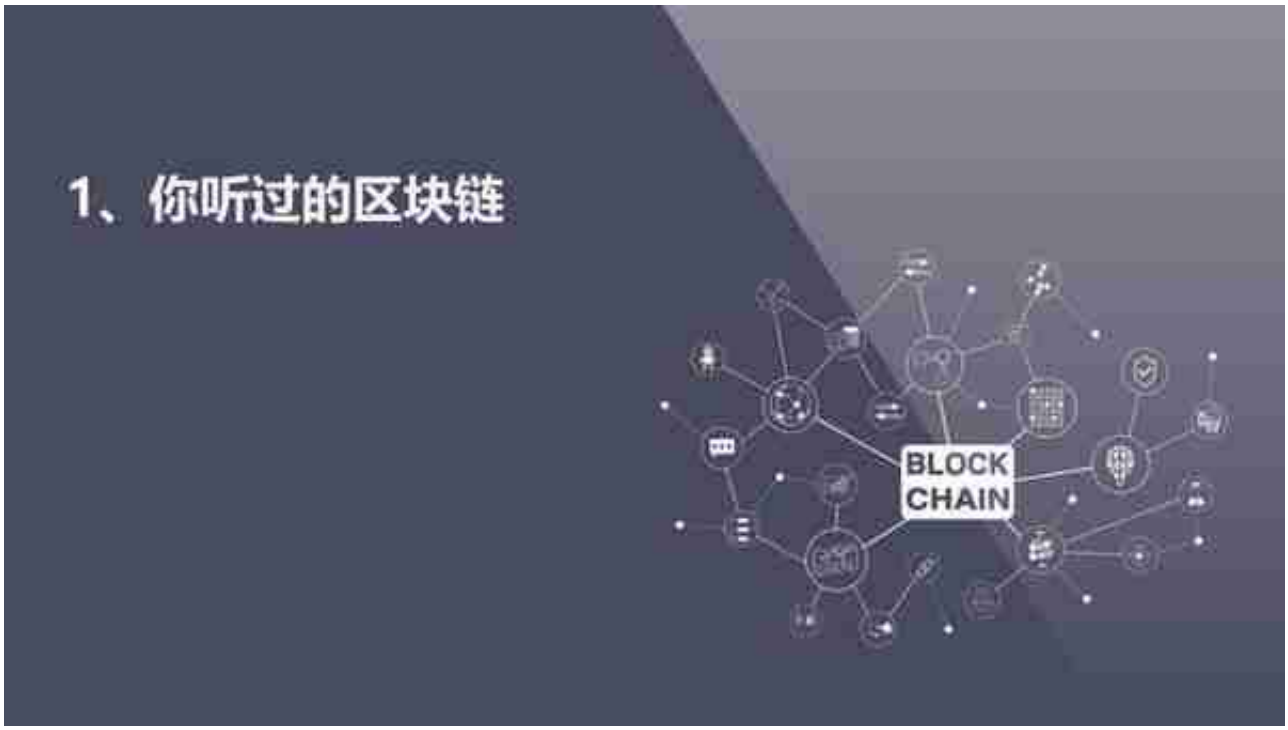
3、区块链起源及定义

4、区块链应用

5、区块链技术

资料领取方式见文末

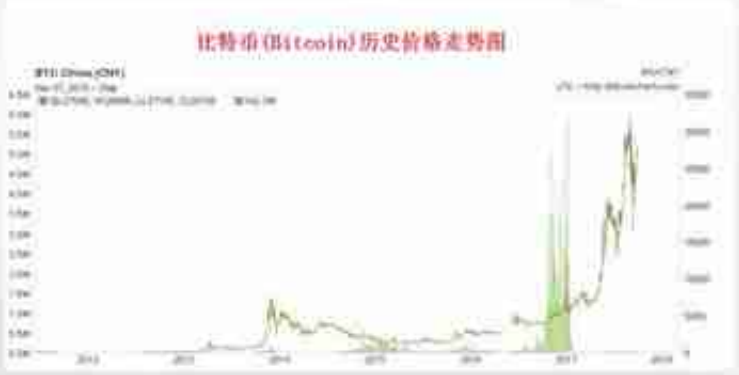

目录
1、你听过的区块链
2、现实世界存在的问题
3、区块链起源及定义
4、区块链应用
5、区块链技术


1、你听过的区块链
BLOCK
CHAIN

你听过的区块链-比特币

比特币价格从诞生时的一美元兑换1300比特币，到峰值时2万多美元兑换1个比特币。

- 去中心化
- 数量一定，上限2100万
- 本身不具备任何价值



你听过的区块链-比特币的挖矿

- 挖矿是参与维护比特币网络的节点，通过协助生成新区块来获取一定量新增的比特币。
- 当用户发布交易后，需要有人将交易进行确认，写到区块链中，形成新的区块。通过挖矿，每 10 分钟左右生成一个不超过 1 MB 大小的区块（记录了这 10 分钟内发生的验证过的交易内容），串联到最长的链尾部。
- 每个区块的奖励一开始是 50 个比特币，每隔 21 万个区块自动减半，现阶段是12.5，最终比特币总量稳定在 2100 万个。
- 比特币采用了工作量证明 Proof of Work（PoW）的机制来实现共识

你听过的区块链-ICO

ICO，全称Initial Coin Offering，意为“首次代币发行”，可以说是以币换币：发行的是区块链项目的代币，投资者通常用市圈认知度最高的比特币或以太币去兑换。

但ICO本质上就是：通过一个还没有产品落地的项目计划，出售项目代币来筹集资金的金融行为。其基本流程是：项目方写几页白皮书，发行新的代币，出售其中一部分，以兑换价值几千万甚至上亿的比特币或以太币。

你听过的区块链-颠覆传统

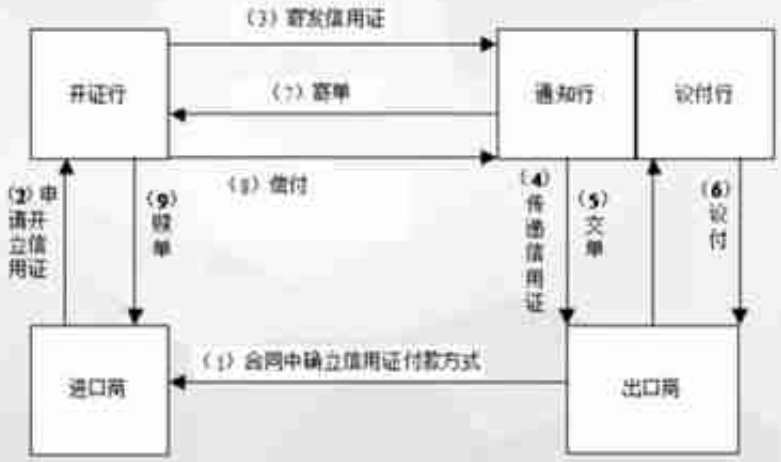
互联网（信息去中心化）已颠覆世界,区块链（信用去中心化）却要颠覆互联网

区块链时代一旦降临，就将颠覆我们现在所有的认知，我们将跨入一个全新的时代，一个不再有信任危机的时代

现实存在的问题-信任问题

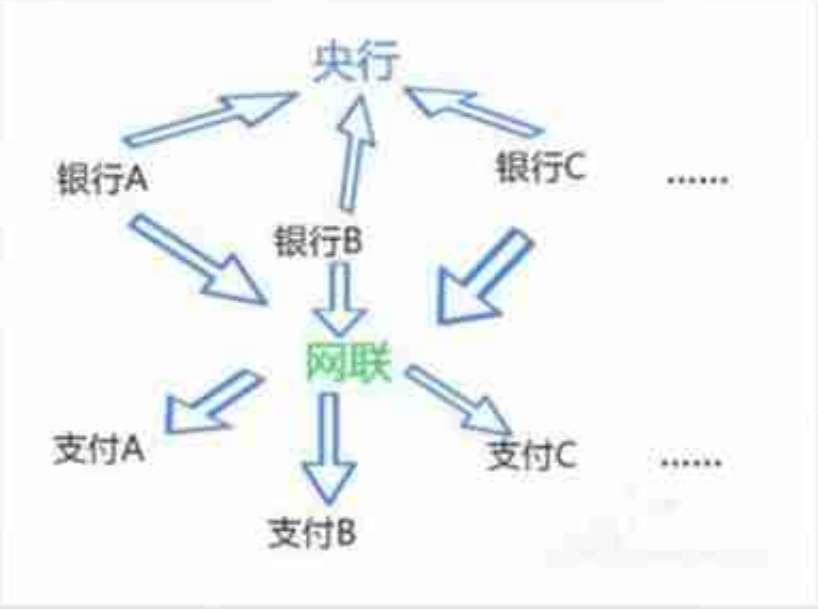
基于制度的，基于特征的和基于过程的

产品追溯
跨境交易
企业信任
.....



现实存在的问题-中心问题

- 抗风险能力更强
- 平等
- 腐败与错误
- 规则简单



现实存在的问题-安全可靠问题

传输不可靠

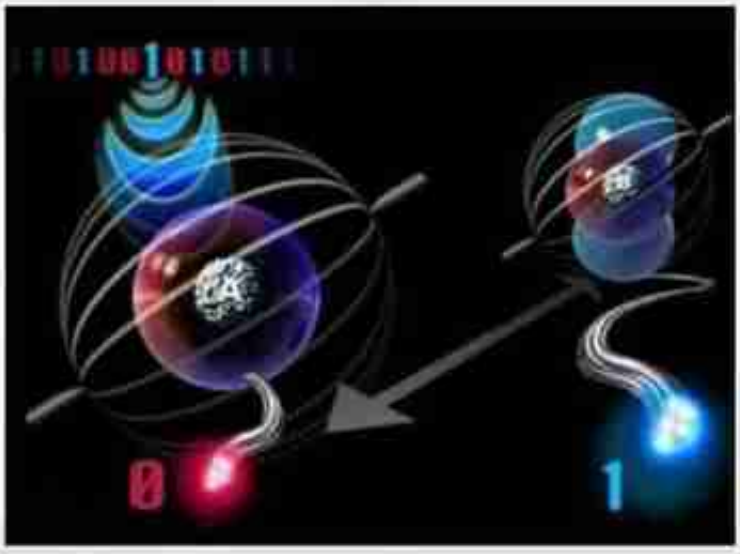
- TCP/IP协议

故意破坏

- 拜占庭将军问题

信息泄密和篡改

- 加密
- 证书
- 摘要



区块链起源-数字货币

- 货币的形态从实物货币、金属货币、代用货币、信用货币、电子货币到数字货币。货币自身的价值依托也从实物价值、发行方信用价值。
- 货币（信用卡、纸币等）需要额外系统（如银行）来完成生产、分发、管理等操作，带来很大的额外成本和使用风险，如伪造、信用卡诈骗、盗刷、转账等。
- 实现一种数字货币，保持既有货币的这些特性，消除纸质货币的缺陷，提升便携、防伪、辩伪、匿名、交易、资源、发行等方面的能力。

区块链起源-数字货币

中心化控制下的数字货币需要一个中心管控系统。
但很多时候并不存在一个安全可靠的第三方记账机构来充当这个中心管控的角色。

◆贸易两国可能缺乏足够的外汇储备；
◆网络上的匿名双方进行直接买卖；
◆交易的两个机构彼此互不信任，找不到双方都认可的第三方担保；
◆汇率的变化，可能无法连接到第三方的系统；
◆第三方的系统可能会出现故障
◆……

区块链起源-比特币

起源：

2008 年 10 月 中本聪的人提出了比特币的设计白皮书，2009 年公开了最初的实现代码

解决的问题：

■被掌控在发行机构手中；
■自身的价值无法保证；
■无法匿名化交易。

区块链起源-比特币到区块链

2014 年开始，比特币背后的区块链（Blockchain）技术受到大家关注，并正式引发了分布式记账本（Distributed Ledger）技术的革新浪潮。

人们开始意识到，记账本相关的技术，对于资产（包括有形资产和无形资产）的管理（包括所有权和流通）十分关键；而去中心化的分布式记账本技术，对于当前开放多维化的商业网络意义重大。区块链，正是实现去中心化记账本系统的一种极具潜力的可行技术。

目前，区块链技术已经脱离开比特币，在包括金融、贸易、征信、物联网、共享经济等诸多领域崭露头角。现在当人们提到“区块链”时，往往已经与比特币网络没有直接联系了，除非特别指出是承载比特币交易系统的“比特币区块链”。

区块链起源-比特币背后的技术

区块链简介-定义

≠

比特币是区块链的首个应用　　区块链是支撑比特币的底层技术

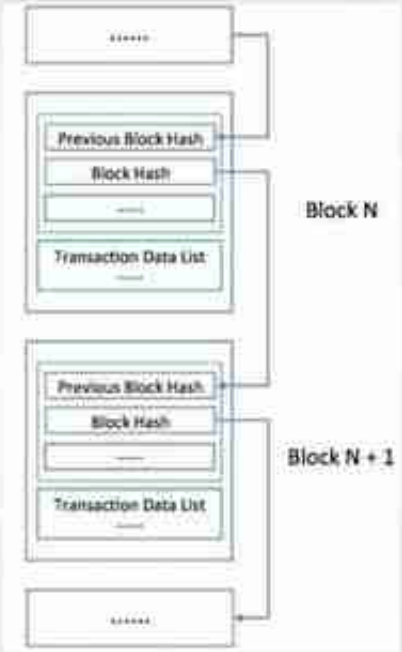
狭义	本质是一种分布式记账同步更新账本技术，以去中心化和去信任化的方式，集体维护一个可靠数据库的技术方案。
广义	一种革新和颠覆性的思维理念，去中介化，建立信任社会，实现共享

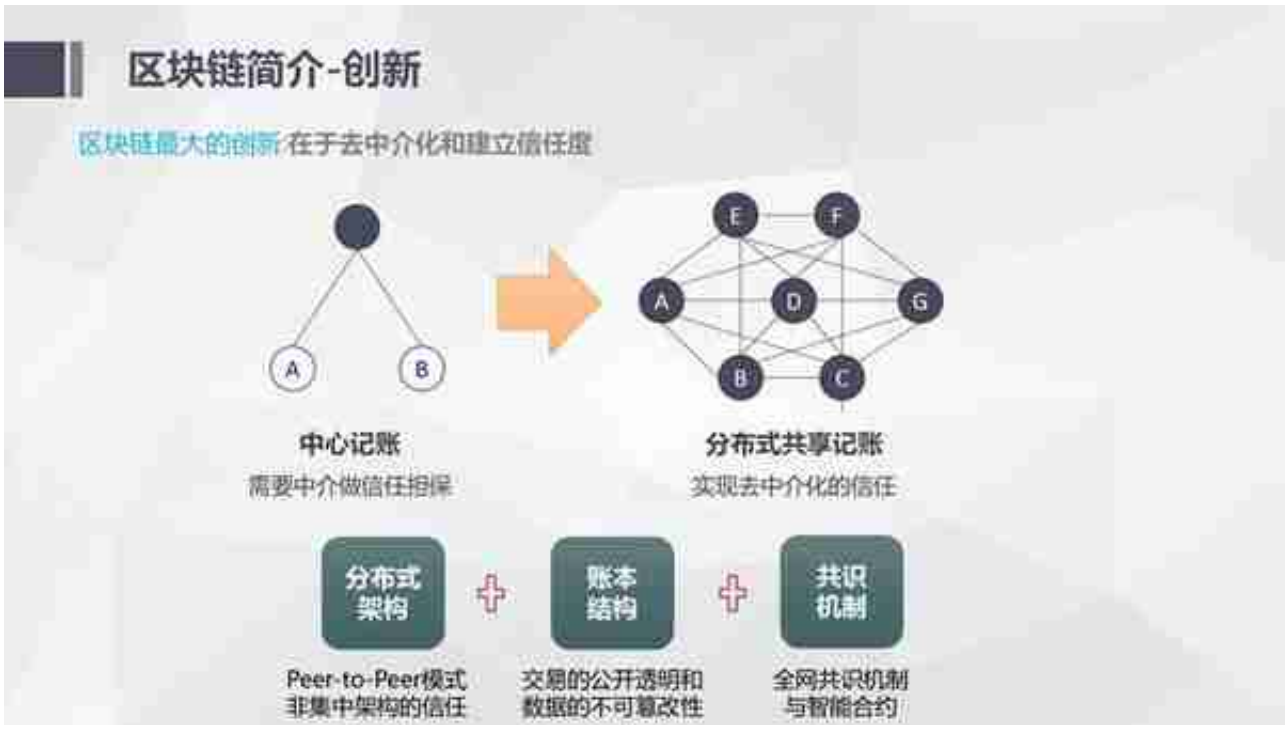
区块链简介-结构

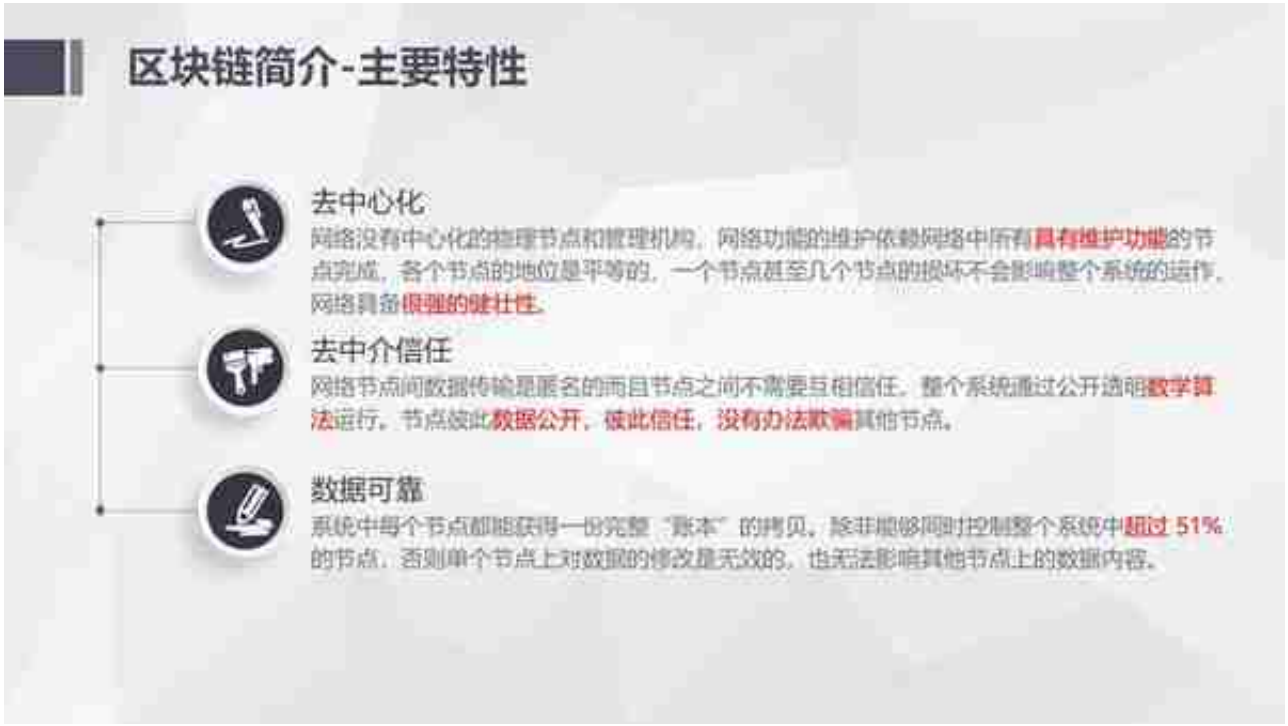
交易（Transaction）：一次操作，导致账本状态的一次改变，如添加一条记录；

区块（Block）：记录一段时间内发生的交易和状态结果，是对当前账本状态的一次共识；

链（Chain）：由一个个区块按照发生顺序串联而成，是整个状态变化的日志记录。




区块链简介-创新
区块链最大的创新在于去中介化和建立信任度
A
B
E
F
A
D
G
B
C
中心记账
需要中介做信任担保
分布式共享记账
实现去中介化的信任
分布式架构
账本结构
共识机制
Peer-to-Peer模式
非集中架构的信任
交易的公开透明和
数据的不可篡改性
全网共识机制
与智能合约


区块链简介-主要特性
去中心化
网络没有中心化的物理节点和管理机构，网络功能的维护依赖网络中所有具有维护功能的节点完成，各个节点的地位是平等的，一个节点甚至几个节点的损坏不会影响整个系统的运作，网络具备很强的健壮性。
去中介信任
网络节点间数据传输是匿名的而且节点之间不需要互相信任，整个系统通过公开透明数学算法运行，节点按此数据公开，彼此信任，没有办法欺骗其他节点。
数据可靠
系统中每个节点都能获得一份完整“账本”的拷贝，除非能够同时控制整个系统中超过51%的节点，否则单个节点上对数据的修改是无效的，也无法影响其他节点上的数据内容。

区块链简介-分类

A 公共区块链

网络中的节点可任意接入，网络中数据读写权限不受限制，任何人都能参与共识过程，比特币属于典型的公有链。

B 私有区块链

网络中的节点被一个组织控制，写入权限仅限在一个组织内部，读取权限有限对外开放，全球 42 家银行组建的区块链联盟 R3 CEV 就是私有链。

C 联盟区块链

介于公有链和私有链之间，公开节点：网络中的节点部分可以任意接入，授权节点：则必须通过授权才可以接入的区块链，比如清算。

区块链简介-发展

可编程货币

货币与交易，即应用中与现金有关的加密数字货币,如货币、转账、汇款和数字支付系统等

■ 区块链1.0

可编程经济

智能合约，如股票、债券、期货、贷款、智能资产和智能合约等更广泛的非货币应用

■ 区块链2.0

可编程社会

自治与管理，在政府、健康、科学、文化和艺术方面有所应用，甚至最终实现去中心化自治社会的终极效果

■ 区块链3.0


4、区块链的应用
BLOCK
CHAIN


区块链应用-商业价值
分布式
容错性
技术特
性
隐私保
护性
不可篡
改性
可信任性
业务特性
增强安全
降低成本
成本

区块链应用-银行金融领域

区块链技术可以为金融服务提供有效可靠的所属权证明和相当强的中介担保机制：

◆加拿大央行开发基于区块链技术的数字版加拿大元（名称为 CAD 币），以允许用户可以使用加元来兑换该数字货币。经过验证的对手方将会处理交易，如果需要，银行将保留销毁CAD币的权利。

◆英国银行已经实现了基于分布式账本平台的数字化货币系统。RSCoin 目标是提供一个由中央银行控制的数字货币，采用了双层链架构、改进版的 2PC 提交，以及多链条之间的交叉验证机制。因为主要是央行和下属银行之间使用，通过提前建立一定的信任基础，可以提供较好的处理性能。

◆ 中国邮储银行布携手 IBM 推出基于区块链技术的资产托管系统，为中国银行业首次将区块链技术应成功用于核心业务系统。

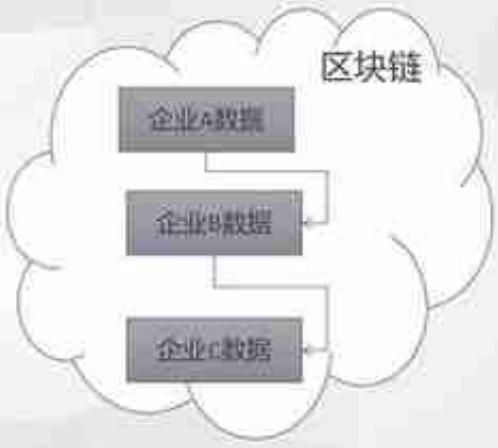
区块链应用-支付领域

Abra	• 区块链数字钱包，无需银行账户，实现不同币种的兑换
Bitwage	• 基于比特币区块链的跨境工资支付平台
BitPOS	• 低成本的快捷线上支付
Circle	• 由区块链充当支付网络，允许用户快速进行跨币种的快速汇款
Ripple	• 实现跨境的多币种低成本实时交易，引入了网关概念（类似银行）

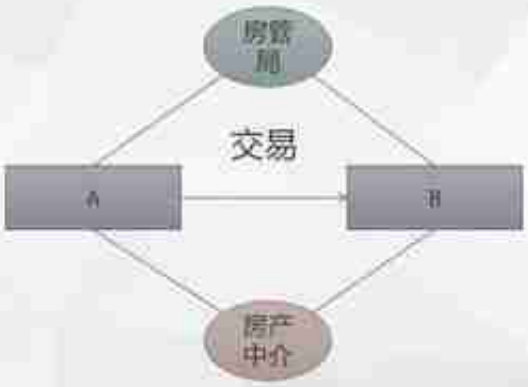
区块链应用-证券领域

Nasdaq Linq	• 美国纳斯达克证券交易所推出区块链平台，面向一级市场的股票交易流程。通过该平台进行股票发行的的发行者将享有“数字化”的所有权。
BitShare	• 推出基于区块链的证券发行平台，号称每秒达到 10 万笔交易。
DAH	• 为金融市场交易提供基于区块链的交易系统。获得澳洲证交所项目。
Symbiont	• 帮助金融企业创建存储于区块链的智能债券，当条件符合时，清算立即执行。
Overstock.com	• 推出基于区块链的私有和公开股权交易“T0”平台，提出“交易即结算”的理念，主要目标是建立证券交易实时清算结算的全新系统。
“SETLcoin”	• 高盛为这种新虚拟货币申请专利，用于为股票和债券等资产交易提供“近乎立即执行和结算”的服务。

区块链应用-征信

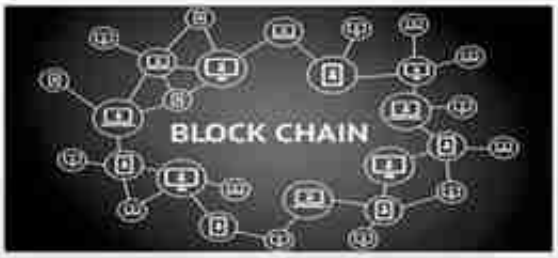


区块链应用-权属管理



1，物品的所有权是写在数字链上的，谁都无法修改

2，智能合约，确保合同准确执行



区块链应用-物联网

2017年3月，中国联通联合众多公司和研究机构在ITU-T SG20成立了全球首个物联网区块链（BOT，Blockchain of Things）标准项目，定义了去中心化的可信物联网服务平台框架。

区块链应用-其他

BitMessage
- 基于区块链的安全可靠的通信系统。

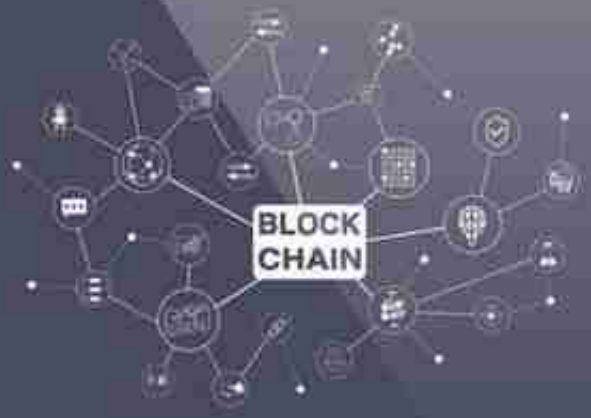
GemHealth
- 医疗数据的安全管理，已与医疗行业多家公司签订了合作协议。

Storj
- 基于比特币区块链的安全的数据分布式存储服务。

Tierion
- 确保数据安全记录。

Twister
- 去中心化的“微博”系统。

5、区块链技术




区块链技术-关键技术及挑战
密码学技术
分布式共识
处理性能
扩展性
系统安全
数据库和存储系统
可集成性


区块链技术-核心技术分解
分布式系统
密码学与安全
区块链

区块链技术-分布式系统：一致性

存在如下的问题：

1，节点之间的网络通讯是不可靠的，包括任意延迟和内容故障；
2，节点的处理可能是错误的，甚至节点自身随时可能宕机；
3，同步调用会让系统变得不具备可扩展性

理想的分布式系统一致性应该满足：

1，可终止性（Termination）：一致的结果在有限时间内能完成；
2，共识性（Consensus）：不同节点最终完成决策的结果应该相同；
3，合法性（Validity）：决策的结果必须是其它进程提出的提案。

区块链技术-分布式系统：共识算法

区块链技术-分布式系统： Paxos

Paxos 是第一个被证明的共识算法，其原理基于两阶段提交 并进行扩展。

proposer：提出一个提案，等待大家批准为结案。往往是客户端担任该角色；

acceptor：负责对提案进行投票。往往是服务端担任该角色；

learner：被告知结案结果，并与之统一，不参与投票过程。可能为客户端或服务端。

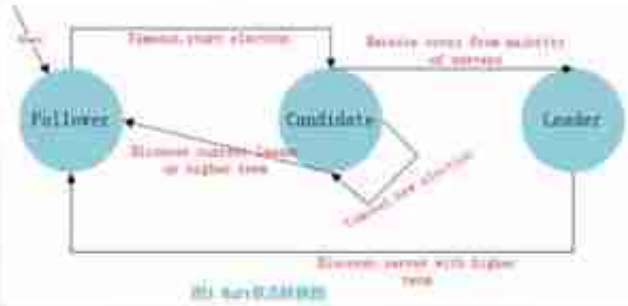
区块链技术-分布式系统： Raft

Raft 算法是Paxos 算法的一种简化实现。

Leader（领导者）：负责日志的同步管理，处理来自客户端的请求，与Follower保持这heartBeat的联系；

Follower（追随者）：刚启动时所有节点为Follower状态，响应Leader的日志同步请求，响应Candidate的请求，把请求到Follower的事务转发给Leader；

Candidate（候选者）：负责选举投票，Raft刚启动时由一个节点从Follower转为Candidate发起选举，选举出Leader后从Candidate转为Leader状态；



区块链技术-分布式系统： 拜占庭错误

对于拜占庭问题来说，假如节点总数为 N，叛变将军数为 F，则当 时，问题才有解，即 Byzantine Fault Tolerant (BFT) 算法。

1999 年提出的 Practical Byzantine Fault Tolerant（PBFT）是第一个得到广泛应用的 BFT 算法。只要系统中有2/3的节点是正常工作的，则可以保证一致性。

PBFT 算法包括三个阶段来达成共识：Pre-Prepare、Prepare 和 Commit。

PoW（Proof of Work）算法是限制一段时间内整个网络中出现提案的个数（增加提案成本），另外是放宽对最终一致性确认的需求，约定好大家都确认并沿着已知最长的链进行拓宽。系统的最终确认是概率意义上的存在。这样，即便有人试图恶意破坏，也会付出很大的经济代价（付出超过系统一半的算力）。

区块链技术-分布式系统： FLP不可能原理

FLP 不可能原理：在网络可靠，存在节点失效（即便只有一个）的最小化异步模型系统中，不存在一个可以解决一致性问题的确定性算法。

Fischer, Lynch 和 Patterson 三位作者于 1985 年发表论文，不要浪费时间去为异步分布式系统设计在任意场景下都能实现共识的算法。

科学告诉你什么是不可能的；工程则告诉你，付出一些代价，我可以把它变成可能。

一致（Agreement）	• 每个正确的执行过程应该在相同的值上达成一致；
完整（Integrity）	• 每个正确的执行过程最多只能决定一个值。如果它决定了某个值的话，这个值一定是被某个执行过程提出的；
终止（Termination）	• 所有的执行过程最终会做出一个决定；
正确（Validity）	• 如果所有正确的执行过程提出了相同的值V，那么所有正确的执行过程都会决定值V。

区块链技术-分布式系统： CAP原理

分布式领域CAP理论
◆Consistency(一致性), 数据一致更新，所有数据变动都是同步的
◆Availability(可用性), 好的响应性能
◆Partition tolerance(分区容错性) 可靠性

定理：任何分布式系统只可同时满足二点，没法三者兼顾。

忠告：架构师不要将精力浪费在如何设计能满足三者的完美分布式系统，而是应该进行取舍。

区块链技术-分布式系统： ACID 和BASE

ACID:
- Atomicity(原子性)
- Consistency(一致性)
- Isolation(隔离性)
- Durability(持久性)

BASE模型反ACID模型，完全不同ACID模型，牺牲高一致性，获得可用性或可靠性：
·**Basically Available**基本可用。支持分区失败(e.g. sharding碎片划分数据库)
·**Soft state**软状态 状态可以有一段时间不同步，异步。
·**Eventually consistent**最终一致，最终数据是一致的就可以了，而不是时时高一致。

BASE思想的主要实现有：1.按功能划分数据库;
2.sharding碎片

区块链技术-分布式系统： 可靠性指标

指标	概率可靠性	每年允许不可用时间	典型场景
一个九	90%	1.2 小时	不可用
二个九	99%	3.6 天	普通单点
三个九	99.9%	8.6 小时	普通企业
四个九	99.99%	51.6 分钟	高可用
五个九	99.999%	5 分钟	电信级
六个九	99.9999%	31 秒	极高要求
七个九	99.99999%	3 秒	N/A
八个九	99.999999%	0.3 秒	N/A
九个九	99.9999999%	30 毫秒	N/A

如何提升可靠性，有两方案：**一是让系统中的单点变得更可靠；二是消灭单点。**

区块链技术-密码学与安全：HASH及摘要

Hash （哈希或散列）算法能任意长度的二进制值（明文）映射为较短的固定长度的二进制值（Hash 值），并且不同的明文很难映射为相同的 Hash 值。

目前流行的 Hash 算法包括 MD5、SHA-1 和 SHA-2。

数字摘要是 Hash 算法最重要的一个用途，解决确保内容没被篡改过的问题（利用 Hash 函数的抗碰撞性特点）


区块链技术-密码学与安全：加解密算法
DES
3DES
AES
RSA
Diffie-Hellman 密钥交换
ElGamal
椭圆曲线算法(ECC)


区块链技术-密码学与安全：数字签名
数字签名用于证实某数字内容的完整性（integrity）和来源
A 先对文件进行摘要，然后用自己的私钥进行加密，将文件和加密串都发给 B。B 收到后文件和加密串，用 A 的公钥来解密加密串，得到原始的数字摘要，跟对文件进行摘要后的结果进行比对。
HMAC
盲签名
多重签名
群签名
环签名

区块链技术-密码学与安全：PKI

PKI 是建立在公私钥基础上实现安全可靠传递消息和身份确认的一个通用框架

- CA（Certification Authority）：负责证书的颁发和作废，接收来自 RA 的请求，是最核心的部分；
- RA（Registration Authority）：对用户身份进行验证，校验数据合法性，负责登记，审核过了就发给 CA；
- 证书数据库：存放证书，一般采用 LDAP 目录服务，标准格式采用 X.500 系列。

数字证书用来证明某个公钥是谁的，并且内容是正确的，数字证书就是像一个证书一样，证明信息和合法性。由证书认证机构（CA）来签发，数字证书内容可能包括版本、序列号、签名算法类型、签发者信息、有效期、被签发人、**签发的公开密钥**、**CA 数字签名**、其它信息等等

区块链技术-以太坊

以太坊（英语：Ethereum）是一个开源的有智能合约功能的公共区块链平台。通过其专用加密货币以太币（Ether，又称“以太币”）提供去中心化的虚拟机（称为“以太虚拟机”Ethereum Virtual Machine）来处理点对点合约。

以太坊（Ethereum）目标是打造成一个运行智能合约的去中心化平台（Platform for Smart Contract），平台上的应用按程序设定运行，不存在停机、审查、欺诈、第三方人为干预的可能。

以太坊区块链的特点主要包括：

1. 单独为智能合约指定编程语言 Solidity；
2. 使用了内存需求较高的哈希函数：避免出现算力矿机；
3. uncle 块激励机制：降低矿池的优势，减少区块产生间隔为 15 秒；
4. 难度调整算法：一定的自动反馈机制；
5. gas 限制调整算法：限制代码执行指令数，避免循环攻击；
6. 记录当前状态的哈希树的根哈希值到区块：某些情形下实现轻量级客户端；
7. 为执行智能合约而设计的简化的虚拟机 EVM。

区块链技术- Fabric介绍

Hyperledger（超级账本）项目是首个面向企业的开放区块链技术的重要探索。在 Linux 基金会的支持下，吸引了包括 IBM、Intel、摩根等在内的众多科技和金融巨头的参与，fabric 是其核心项目。

Fabric是为企业构建的领先的开源、通用区块链结构

区块链技术- Fabric应用