区块链最核心的形式是合约层

1、去核心化

这是区块链树立性特性，不具有任何核心机构和核心效力器，一切买卖都发生在每团体电脑或手机上装置的客户端运用次第中。

完成点对点直接交互，既糜费资源，使买卖自主化、简易化，又清扫被核心化代理掌握的风险。

2、封锁性

区块链可以了解为一种公共记账的技术计划，系统是完整封锁透明的，

账簿对一切人公开，完成数据共享，任何人都可以查账。

区块链是透明共享的总帐本，这帐本在全网公开，你拿到它的公钥，你就知道它帐外面终究是有几钱，所以任何一次的价值转换，全世界有兴味的人都能在中间看着你，转换是由矿工来帮你确认的，所以它是一个互联网共识机制。

3、不可撤销、不可窜改和加密平安性

区块链采取单向哈希算法，每个新发生的区块严酷依照时间线形次第促进，时间的不可逆性、不可撤销招致任何试图入侵窜改区块链内数据音讯的行为易被追溯，招致被其他节点的排挤，造假利息极高，从而能够限制相关不法行为。

扩展资料：

一，概念定义

什么是区块链？从科技层面来看，区块链触及数学、密码学、互联网和计算机编程等很多迷信技术效果。从运用视角来看，冗杂来说，区块链是一个散布式的共享账本和数据库，具有去核心化、不可窜改、全程留痕、能够追溯、团体维护、公激进明等特性。这些特性保证了区块链的“老实”与“通明”，为区块链发明怀疑奠定基础。而区块链丰厚的使用场景，基本上都基于区块链能够处置音讯不对称效果，完成多个主体之间的协作怀疑与一致举措[7]。

区块链是散布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型使用方式。区块链（Blockchain），是比特币的一个主要概念，它实质上是一个去核心化的数据库。

二，特征

去中心化。区块链技术不依赖额外的第三方管理机构或硬件装备，没有中心掌握，除了自成一体的区块链自身，经过火布式核算和存储，各个节点完成了消息自我考证、传递和管理。去中心化是区块链最一般最实质的特征。

封锁性。区块链技术基础是开源的，除了买卖各方的私有消息被加密外，区块链的数据对一切人封锁，任何人都可以经过公开的接口查询区块链数据和开拓相关使用，因此整个系统消息高度通明。

独立性。基于商量一致的规范和协议(相似比特币采用的哈希算法等各种数学算法)，整个区块链系统不依赖其他第三方，一切节点能够在零碎内自动平安地考证、交流数据，不需求任何人为的干预。

平安性。只需不能掌控局部数据节点的51%，就无法肆意操控矫正网络数据，这使区块链自身变得相对平安，防止了客观人为的数据变卦。

匿名性。除非有法律规范央求，单从技术下去讲，各区块节点的身份消息不需求公开或考证，信息传递可以匿名中止

重庆金窝窝剖析区块链的核心技术如下：

1-区块、链

2-散布式结构——开源的、去中心化的协议

3-非对称加密算法

4-脚本

冗杂来说，区块链是一个提供了拜占庭容错、并保证了最终一致性的散布式数据库；从数据结构上看，它是基于时间序列的链式数据块结构；从节点拓扑上看，它一切的节点互为冗余备份；从操作上看，它提供了基于密码学的公私钥管理体系来管理账户。

大约上述文章内容概念过于笼统，我来举个例子，你就好了解了。

你可以想象有 100 台计算机散布逝世界各地，这 100
台机器之间的网络是广域网，并且，这 100 台机器的具有者相互不怀疑。

那么，我们采用什么样的算法（共识机制）才干够为它提供一个可怀疑的环境，并且使得：

节点之间的数据交流进程不可窜改，并且已生成的历史记载不可被窜改；

每个节点的数据会同步到最新数据，并且会考证最新数据的有效性；

基于少数遵从少数的准绳，局部节点维护的数据可以客观反映交换历史。

区块链就是为了处置上述效果而发生的技术计划。

二、区块链的核心技术组成

不论是公链还是联盟链，至少需求四个模块组成：P2P
网络协议、分布式一致性算法（共识机制）、加密签名算法、账户与存储模型。

1、P2P 网络协议

P2P 网络协议是一切区块链的最底层模块，负责买卖数据的网络传输和广播、节点发觉和维护。

一般我们所用的都是比特币 P2P 网络协议模块，它遵照肯定的交互准绳。比如：初次衔接到其他节点会被央求依照握手协议来确认外形，在握手之后末尾央求 Peer 节点的地址数据以及区块数据。

这套 P2P 交互协议也具有自己的指令集合，指令体往常在消息头（Message Header) 的 命令（command）域中，这些命令为下层提供了节点发觉、节点获取、区块头获取、区块获取等功用，这些功用都是十分底层、十分基础的功用。假定你想要深化了解，可以参考比特币开拓者指南中的 Peer Discovery 的章节。

2、分布式一致性算法

在模范分布式计算范围，我们有 Raft 和 Paxos
算法家族代表的非拜占庭容错算法，以及具有拜占庭容错特性的 PBFT 共识算法。

假定从技术演化的角度来看，我们可以得出一个图，其中，区块链技术把原本的分布式算法中止了经济学上的拓展。

在图中我们可以看到，计算机应用在最末尾多为单点应用，高可用便利采用的是冷灾备，事前展开到异地多活，这些异地多活能够采用的是负载平衡和路由技术，随着分布式系统技术的展开，我们过渡到了 Paxos 和 Raft 为主的分布式系统。

而在区块链范围，多采用 PoW 义务量证明算法、PoS 权益证明算法，以及 DPoS 代理权益证明算法，上述文章内容三种是业界主流的共识算法，这些算法与模范分布式一致性算法不同的是，它们融入了经济学博弈的概念，下面我区分冗杂引见这三种共识算法。

PoW： 一般是指在给定的约束下，求解一个特定难度的数学效果，谁解的速度快，谁就能取得记账权（出块）权益。这个求解进程经常会转换成计算效果，所以在比拼速度的状况下，也就变成了谁的计算方法更优，以及谁的装备功用更好。

PoS： 这是一种股权证明机制，它的基本概念是你发生区块的难度应当与你在网络里所占的股权（一切权占比）成比例，它完成的核心思绪是：使用你所锁定代币的币龄（CoinAge）以及一个小的义务量证明，去计算一个手段值，当满意手段值时，你将能够获取记账权。

DPoS： 繁杂来理解就是将 PoS 共识算法中的记账者转换为指定节点数组成的小圈子，而不是所有人都可以参与记账。这个圈子能够是 21 个节点，也有能够是 101 个节点，这一点取决于想象，只需这个圈子中的节点才干取得记账权。这将会极大地提高系统的吞吐量，由于更少的节点也就意味着网络和节点的可控。

3、加密签名算法

在区块链范围，应用得最多的是哈希算法。哈希算法具有抗碰撞性、原像不可逆、难题友好性等特征。

其中，难题友好性正是众多 PoW 币种赖以具有的基础，在比特币中，SHA256 算法被用作任务量证明的计算方法，也就是我们所说的挖矿算法。

而在莱特币身上，我们也会看到 Scrypt 算法，该算法与 SHA256 不同的是，需求大内存支持。而在其他一些币种身上，我们也能看到基于 SHA3 算法的挖矿算法。以太坊使用了 Dagger-Hashimoto 算法的改良版本，并命名为 Ethash，这是一个 IO 难解性的算法。

当然，除了挖矿算法，我们还会使用到 RIPEMD160 算法，次要用于生成地址，众多的比特币衍生代码中，绝大局部都采用了比特币的地址想象。

除了地址，我们还会使用到最核心的，也是区块链 Token 系统的基石：公私钥密码算法。

在比特币大类的代码中，根本上使用的都是 ECDSA。ECDSA 是 ECC 与 DSA 的区分，整个签名进程与 DSA 相似，所不一样的是签名中采取的算法为 ECC（椭圆曲线函数）。

从技术上看，我们先从生成私钥末尾，其次从私钥生成公钥，最后从公钥生成地址，上述文章内容每一步都是不可逆进程，也就是说无法从地址推导出公钥，从公钥推导到私钥。

4、账户与买卖模型

从一末尾的定义我们知道，仅从技术角度可以以为区块链是一种分布式数据库，那么，少数区块链终究使用了什么类型的数据库呢？

我在想象元界区块链时，参考了多种数据库，有 NoSQL 的 BerkelyDB、LevelDB，也有一些币种采用基于 SQL 的 SQLite。这些作为底层的存储装备，多以轻量级嵌入式数据库为主，由于并不触及区块链的账本特性，这些存储技术与其他场所下的使用并没有什么不同。

区块链的账本特性，普通分为 UTXO 结构以及基于 Accout-Balance 结构的账本结构，我们也称为账本模型。UTXO 是“unspent transaction input/output”的缩写，翻译过去就是指“未破费的交易输入输入”。

这个区块链中 Token 转移的一种记账形式，每次转移均以输入输入的方式出现；而在 Balance 结构中，是没有这个形式的。

从技术的角度，架构的角度，用深入的言语来跟自己讲讲，我对区块链的一些理解。

终究啥是区块链？Block chain，一句话来说，区块链是一个存储系统，存储系统更细一点，区块链是一个没有管理员，每个节点都具有部分数据的分布式存储系统。

那稀有的存储系统，是什么样子的呢？

如上图所示，底部是数据，下面可以写入数据。一个空间存储数据，一个软件管理数据，提供接口写入数据，这就是存储系统。比如MySQL就是最稀有的存储系统。

一般的存储系统，繁杂具有什么效果呢？至少有两个罕见的成绩

第一个是非高可用的问题，数据具有一个中央很风险。用技术的话说，就是数据不高可用。

第二个问题是，它具有写入的单点，写入点只需一个。用技术的话说，就是它是一个单点控制。

那一般的存储系统一般是如何处置这两个问题的呢？

首先看一下如何保证高可用？

普通的存储系统一般是用“冗余”的方式来处置高可用问题的。图上图所示假设能够把数据复制成几份，冗余到多个中央，就能够保证高可用。一个中央的数据挂了，另外的地方还存有数据，例如MySQL的主从集群就是这个原理，磁盘的RAID也是这个原理。

这个地方需要强调的两点是：数据冗余，经常会引发一致性的问题

1、例如MySQL的主从集群中中其实读写会有延时的，它其实就是有一个短的时间内读写不一致。这个是数据冗余，带来的一个反作用。

2、第二个点是数据冗余经常会降低写入的效率，由于数据同步也是需要消耗资源的。你看单点写入，假设加了两个从库之后，其实写入的效率会受影响。普通的存储系统，就是采用冗余的方式，保证数据的高可用的。

那么第二个问题，普通的存储系统，能否多点写入呢？

答案是可以的，比如说以这个图为例：

其实MySQL的话可以做一个双主的主从同步，双主的主从同步，两个节点，同时可以写入。假设要做多机房多活的数据中心，其实多机房多活也是停止数据同步的。这里要强调的是多点写入，经常会引发写写抵触的一致性问题，以MySQl为例，假定有一个表的属性是自增ID，那么往常数据库中的数据是1234，那么其中一个节点写入，插入了一条数据，那它能够变成5了，然后这5条数据，向另外一个主节点停止数据同步，同步完成之前，假设另外一个写入节点，也插入了一条数据，也生成

了一条这个自增id为5的数据。那么，生成之后，往另外一个节点同步，然后同步数据抵达之后会与外地的这两条5抵触，就会同步失利，会引发写写的一致性冲突问题。这个多点写入的话都会出现这个问题。

多点写入，如何保证一致？

维新“天鹅大咖课”给你更多的技术干活

区块链运作的7个核心技术引见 2018-01-15

1.区块链的链接

望文生义，区块链即由一个个区块组成的链。每个区块分为区块头和区块体（含交易数据）两个部分。区块头包括用来实现区块链接的前一区块的哈希（PrevHash）值（又称散列值）和用于计算挖矿难度的随机数（nonce）。前一区块的哈希值实际是上一个区块头部的哈希值，而计算随机数规则决议了哪个矿工可以获得记载区块的权益。

2.共识机制

区块链是随同比特币出世的，是比特币的基础技术架构。可以将区块链理解为一个基于互联网的去中心化记账系统。类似比特币这样的去中心化数字货币系统，恳求在没有中心节点的状况下保证各个老实节点记账的一致性，就需要区块链来完成。所以区块链技术的核心是在没有中心掌握的状况下，在相互没有疑心基础的团体之间就交易的合法性等达成共识的共识机制。

区块链的共识机制目前主要有4类：PoW、PoS、DPoS、分布式一致性算法。

3.解锁脚本

脚本是区块链上实现自动验证、自动实施合约的主要技术。每一笔交易的每一项输出严酷意义上并不是指向一个地址，而是指向一个脚本。脚本类似一套规则，它约束着接收方怎样才干花掉这个输出上锁定的资产。

交易的合法性验证也依赖于脚本。目前它依赖于两类脚本：锁定脚本与解锁脚本。锁定脚本是在输出交易上加上的条件，经过一段脚本言语来实现，位于交易的输出。解锁脚本与锁定脚本相对应，只要满意锁定脚本恳求的条件，才干花掉这个脚本上对应的资产，位于交易的输入。经过脚本言语可以表达很多灵敏的条件。注释脚本是经过类似我们编程范围里的“虚拟机”，它分布式运转在区块链网络里的每一

个节点。

4.交易规则

区块链交易就是形成区块的根本单位，也是区块链负责记载的实际有效形式。一个区块链交易可以是一次转账，也可以是智能合约的布置等其他事务。

就比特币而言，交易即指一次支付转账。其交易规则如下：

1）交易的输入和输出不能为空。

2）对交易的每个输入，如果其对应的UTXO输出能在以后交易池中找到，则拒绝该交易。由于以后交易池是未被记载在区块链中的交易，而交易的每个输入，应当来自确认的UTXO。如果在以后交易池中找到，那就是双花交易。

3）交易中的每个输入，其对应的输出必需是UTXO。

4）每个输入的解锁脚本（unlocking ）必需和相应输出的锁定脚本（locking ）独自验证交易的合规性。

5.交易优先级

区块链交易的优先级由区块链协议规则决议。关于比特币而言，交易被区块包括的优先次第由交易广播到网络上的时间和交易额的大小决议。随着交易播送到网络上的时间的增加，交易的链龄增加，交易的优先级就被提高，最终会被区块包括。关于以太坊而言，交易的优先级还与交易的公布者甘愿支付的交易费用相关，公布者甘愿支付的交易费用越高，交易被包含进区块的优先级就越高。

6.Merkle证明

Merkle证明的原始应用是比特币系统（Bitcoin），它是由中本聪（Satoshi Nakamoto）在2009年描画并且发明的。比特币区块链使用了Merkle证明，为的是将交易存储在每一个区块中。使得交易不能被窜改，同时也复杂验证交易能否包含在一个特定区块中。

7.RLP

RLP（Recursive Length Prefix，递归长度前缀编码）是Ethereum中对象序列化的一个主要编码方式，其手腕是对恣意嵌套的二进制数据的序列停止编码。