面对信息化时代，稍不注意就会脱轨，所以及时的补充知识才能让我们与时俱进，今天给大家带来的是关于区块链的优缺点和区块链的优点和缺点的一篇文章，相信会给你带来较大的帮助！

首先，没有一种共识机制是完美无缺的，各共识机制都有其优缺点，有些共识机制是为解决一些特定的问题而生。

1.pow(Proof of Work) 工作量证明

一句话介绍：干的越多，收的越多。

依赖机器进行数学运算来获取记账权，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。

优点：

1)算法简单，容易实现；

2)节点间无需交换额外的信息即可达成共识；

3)破坏系统需要投入极大的成本；

缺点：

1)浪费能源；

2)区块的确认时间难以缩短；

3)新的区块链必须找到一种不同的散列算法，否则就会面临比特币的算力攻击；

4)容易产生分叉，需要等待多个确认；

5)永远没有最终性，需要检查点机制来弥补最终性；

2.POS Proof of Stake，权益证明

一句话介绍：持有越多，获得越多。

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。它是Pow的一种升级共识机制，根据每个节点所占代币的比例和时间，等比例的降低挖矿难度，从而加快找随机数的速度

优点：在一定程度上缩短了共识达成的时间；不再需要大量消耗能源挖矿。

缺点：还是需要挖矿，本质上没有解决商业应用的痛点；所有的确认都只是一个概率上的表达，而不是一个确定性的事情，理论上有可能存在其他攻击影响。例如，以太坊的DAO攻击事件造成以太坊硬分叉，而ETC由此事件出现，事实上证明了此次硬分叉的失败。

DPOS与POS原理相同，只是选了一些“人大代表”。

BitShares社区首先提出了DPoS机制。

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。类似于董事会投票，持币者投出一定数量的节点，代理他们进行验证和记账。

DPoS的工作原理为：

去中心化表示每个股东按其持股比例拥有影响力，51%股东投票的结果将是不可逆且有约束力的。其挑战是通过及时而高效的方法达到51%批准。为达到这个目标，每个股东可以将其投票权授予一名代表。获票数最多的前100位代表按既定时间表轮流产生区块。每名代表分配到一个时间段来生产区块。所有的代表将收到等同于一个平均水平的区块所含交易费的10%作为报酬。如果一个平均水平的区块含有100股作为交易费，一名代表将获得1股作为报酬。

网络延迟有可能使某些代表没能及时广播他们的区块，而这将导致区块链分叉。然而，这不太可能发生，因为制造区块的代表可以与制造前后区块的代表建立直接连接。建立这种与你之后的代表(也许也包括其后的那名代表)的直接连接是为了确保你能得到报酬。

该模式可以每30秒产生一个新区块，并且在正常的网络条件下区块链分叉的可能性极其小，即使发生也可以在几分钟内得到解决。

成为代表：

成为一名代表，你必须在网络上注册你的公钥，然后分配到一个32位的特有标识符。然后该标识符会被每笔交易数据的“头部”引用。

授权选票：

每个钱包有一个参数设置窗口，在该窗口里用户可以选择一个或更多的代表，并将其分级。一经设定，用户所做的每笔交易将把选票从“输入代表”转移至“输出代表”。一般情况下，用户不会创建特别以投票为目的的交易，因为那将耗费他们一笔交易费。但在紧急情况下，某些用户可能觉得通过支付费用这一更积极的方式来改变他们的投票是值得的。

保持代表诚实：

每个钱包将显示一个状态指示器，让用户知道他们的代表表现如何。如果他们错过了太多的区块，那么系统将会推荐用户去换一个新的代表。如果任何代表被发现签发了一个无效的区块，那么所有标准钱包将在每个钱包进行更多交易前要求选出一个新代表。

抵抗攻击：

在抵抗攻击上，因为前100名代表所获得的权力权是相同的，每名代表都有一份相等的投票权。因此，无法通过获得超过1%的选票而将权力集中到一个单一代表上。因为只有100名代表，可以想象一个攻击者对每名轮到生产区块的代表依次进行拒绝服务攻击。幸运的是，由于事实上每名代表的标识是其公钥而非IP地址，这种特定攻击的威胁很容易被减轻。这将使确定DDOS攻击目标更为困难。而代表之间的潜在直接连接，将使妨碍他们生产区块变得更为困难。

优点：大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证。

缺点：整个共识机制还是依赖于代币，很多商业应用是不需要代币存在的。

3.PBFT ：Practical Byzantine Fault Tolerance，实用拜占庭容错

介绍：在保证活性和安全性（liveness safety）的前提下提供了(n-1)/3的容错性。

在分布式计算上，不同的计算机透过讯息交换，尝试达成共识；但有时候，系统上协调计算机（Coordinator / Commander）或成员计算机 （Member /Lieutanent）可能因系统错误并交换错的讯息，导致影响最终的系统一致性。

拜占庭将军问题就根据错误计算机的数量，寻找可能的解决办法，这无法找到一个绝对的答案，但只可以用来验证一个机制的有效程度。

而拜占庭问题的可能解决方法为：

在 N ≥ 3F + 1 的情况下一致性是可能解决。其中，N为计算机总数，F为有问题计算机总数。信息在计算机间互相交换后，各计算机列出所有得到的信息，以大多数的结果作为解决办法。

1）系统运转可以脱离币的存在，pbft算法共识各节点由业务的参与方或者监管方组成，安全性与稳定性由业务相关方保证。

2）共识的时延大约在2~5秒钟，基本达到商用实时处理的要求。

3）共识效率高，可满足高频交易量的需求。

缺点：

1)当有1/3或以上记账人停止工作后，系统将无法提供服务；

2)当有1/3或以上记账人联合作恶，且其它所有的记账人被恰好分割为两个网络孤岛时，恶意记账人可以使系统出现分叉，但是会留下密码学证据

下面说两个国产的吧~

4.dBFT： delegated BFT 授权拜占庭容错算法

介绍：小蚁采用的dBFT机制，是由权益来选出记账人，然后记账人之间通过拜占庭容错算法来达成共识。

此算法在PBFT基础上进行了以下改进：

将C/S架构的请求响应模式，改进为适合P2P网络的对等节点模式；

将静态的共识参与节点改进为可动态进入、退出的动态共识参与节点；

为共识参与节点的产生设计了一套基于持有权益比例的投票机制，通过投票决定共识参与节点（记账节点）；

在区块链中引入数字证书，解决了投票中对记账节点真实身份的认证问题。

优点：

1)专业化的记账人；

2)可以容忍任何类型的错误；

3)记账由多人协同完成，每一个区块都有最终性，不会分叉；

4)算法的可靠性有严格的数学证明；

缺点：

1)当有1/3或以上记账人停止工作后，系统将无法提供服务；

2)当有1/3或以上记账人联合作恶，且其它所有的记账人被恰好分割为两个网络孤岛时，恶意记账人可以使系统出现分叉，但是会留下密码学证据；

以上总结来说，dBFT机制最核心的一点，就是最大限度地确保系统的最终性，使区块链能够适用于真正的金融应用场景。

5.POOL验证池

基于传统的分布式一致性技术，加上数据验证机制。

优点：不需要代币也可以工作，在成熟的分布式一致性算法（Pasox、Raft）基础上，实现秒级共识验证。

缺点：去中心化程度不如bictoin；更适合多方参与的多中心商业模式。

一、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设施，没有中心管制，除了自成一体的区块链本身，通过分布式核算和存储，各个节点实现了信息自我验证、传递和管理。

二、开放性。

区块链技术基础是开源的，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开放，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，因此整个系统信息高度透明。

三、独立性。

基于协商一致的规范和协议(类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，所有节点能够在系统内自动安全地验证、交换数据，不需要任何人为的干预。

四、安全性。

只要不能掌控全部数据节点的51%，就无法肆意操控修改网络数据，这使区块链本身变得相对安全，避免了主观人为的数据变更 。

五、匿名性。

除非有法律规范要求，单从技术上来讲，各区块节点的身份信息不需要公开或验证，信息传递可以匿名进行 。

拓展资料：

1、什么是区块链？一句话概括。

答：区块链是加密的数据库链条，即在多个时间戳/事件内交易数据加密后关联在一起，数据不可篡改可共享。

2、表现及逻辑：

a、外部操作表现形式：银行存取款汇款、记进出账、购物等。

b、内部逻辑处理（软件程序）：人为操作后数据会先加密后存储到数据库，经过程序对数据进行划分区域，比如根据事件、时间戳内发生的数据进行归类放在一起为一个区域的数据。多个事件、时间戳内发生的数据相关联就是区块链。这样加密的数据可共享，但不可篡改。

c、共享表现形式：查询个人信息、查账等。查询权限/共享权限：权限不同查询的数据不同，如银行可以查所有人信息，个人只能查个人。

3、举的例子大多不同，但逻辑处理的思路是一致的，只不过实现方法和操作不一而已。

4、区块链：具有加密数据、不可篡改数据、共享数据特点。

5、区块链技术：即用编辑的程序对数据进行加密、分区、共享等运用的技术。

开放，共识，任何人都可以参与到区块链网络，每一台设备都能作为一个节点，每个节点都允许获得一份完整的数据库拷贝，节点之间基于一套共识机制，通过竞争计算共同维护整个区块链。

去中心化、去信任机制，区块链由众多的节点共同组成一个点对点的网络，不存在中心化的设备和管理机构，节点之间数据交互通过数字签名技术进行验证，不需要信任，只需要按照设置好的规则就行，节点之间不存在欺骗不信任的问题。

交易透明，双方匿名，区块链的运行规则是公开透明的，所有的数据信息也是公开的，每笔交易都是对所有节点公开可见，由于节点之间是去信任的，因此节点不需要公开身份，每个参与的节点都是匿名的。

不可篡改，可追溯，单个节点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，区块链中的每一笔交易都通过密码学方法与两个相邻的两个区块串联，因此可以追溯每一笔交易的所有记录。

区块链正在开始一场对货币的革命。区块链应该是具有比特特性的流动性，而不再是货币特性。

根据拉德克利夫报告中指出“只有流动性才是货币政策影响经济的传导机制”，人们的支出并不受现存货币量的限制，而只是通人们预期他们能得到的货币量上述文章内容就是，这些货币可能是作为收入而获得的，也可能是通过出卖资产而获得的，抑或是借来的。区块链通过token来标记价值，所有资产都能够被极简易的在区块链上表达，资产交易所的构造和边际成本趋于零。毛球科技技术研究部认为，这是区块链的核心技术之一，它所带来的是在零边际成本场景下，流动性的爆发。

只有流动性才是区块链价值的传导机制

货币的流动性通俗来讲是指货币在流通过程中不发生损失的情况下迅速变现的能力。而随着信息化进程加剧，要求货币更具有简便、快速的交易，纸币现在流动性的变现形式已经远低于电子货币。

互联网金融时代下，“流动性”完全可以解释为“超越纸币形式表现价值的信息流”。

我们都知道，中央银行体质离开了对价值背后的信息流的控制就无法生存。因为中央银行货币政策的实质，就是控制价值信息流，或干脆说否定“信息流”。这也是几年来通货膨胀加剧的原因之一。

而电子货币之所以逐渐强于纸币的流动性特征在于，纸币价值在互联网昌盛之前，是因为它能够提供高于像黄金、白银等信息流价值。所以，电子货币的实质也就是直接的价值交换，形式载体是数字信号通过网络交换的信息。这与“流动性”的特征也就完全相符合。

虽然在上个世纪无从得知区块链的情况，但是基于流动性分析，还是准确把握了货币后世的价值特征。而现在对于区块链，人们大多数谈的都是它的技术方面，很少触及到价值内容方面。

但是，如果各央行“量化宽松被区块链追踪到利益的流向，技术马上就会“现形”为利益。

区块链是分布式的一般等价物，还是分布式的具体使用价值

区块链可以对交易的货币流动事实进行分布式的记录和计量，在基于区块链技术的分布式交易记录系统中，各节点成为独立的产品消费者，各主体平等分散决策，所有交易公开，交易节点可以匿名，保证节点账户的安全性，分散化管理无需中心服务器，规避昂贵的运维费用，降低成本。

区块链虽然形式上与货币相比，去中心化了，但它处理的流动性，仍然是基于一般等价物。

我们都知道区块链的出现基于日益严重的中心化问题，从一般等价物理论来看，一般等价物的出现是因为现存价值形式的等价物不能适应日益增长的交换需要，所以需要一种新的等价物出现，来补足现存等价物的缺点。

法国生物学家雅克·莫诺在1970年出版的《必然性和偶然性》中提到：事物的发展存在必然性。区块链之所以被设计为一般等价物的流动性账簿，也就不言而喻了。当然，根据中国社科院信息化研究中心姜奇平“区块链与货币哲学”的观点，区块链现在仅仅是被设计为一般等价物的分布式系统，如果未来不再是一般等价物特征唱主角，那么未来的流动性将需要在利用、使用、服务应用中体现价值。所以毛球科技技术研究部认为，未来区块链不应该只在技术上体现分布不分布，更应该体现

在具体价值应用上面。

海德格尔在他的巨著《存在与时间》中提出了哲学概念：此在。这里用来形容区块链再好不过，即上帝不会甘于作记帐手段，他要活在当下与此在的目的中。意思是，区块链要长久的发展，那么就必须发展出一种情境化使用的功能，作为此在存在者，而不是昙花一现。

区块链如果不再是一般等价物，如何看待流动性

从姜奇平流动性的观点看，贝壳、货币、区块链是流动性在不同历史时期，不同价值逻辑下的不同载体。货币作为流动性，忽略掉价值的使用特征，这种使用特征从来是具体的、本地的、当下的，因而只能是分布式的。

毛球科技技术研究部认为，区块链在抓住货币这种流动性的分布式特征时，虽然早期会把它当一般等价物的记帐薄应用，但最终必然要对其进行否定之否定，发展出一种对应服务的估值功能。

目前主要有四大类共识机制：Pow、Pos、DPos、Pool

1、Pow工作量证明，就是大家熟悉的挖矿，通过与或运算，计算出一个满足规则的随机数，即获得本次记账权，发出本轮需要记录的数据，全网其它节点验证后一起存储；

优点：完全去中心化，节点自由进出；

缺点：目前bitcoin已经吸引全球大部分的算力，其它再用Pow共识机制的区块链应用很难获得相同的算力来保障自身的安全；挖矿造成大量的资源浪费；共识达成的周期较长，不适合商业应用

2、Pos权益证明，Pow的一种升级共识机制；根据每个节点所占代币的比例和时间；等比例的降低挖矿难度，从而加快找随机数的速度。

优点：在一定程度上缩短了共识达成的时间

缺点：还是需要挖矿，本质上没有解决商业应用的痛点

3、DPos股份授权证明机制，类似于董事会投票，持币者投出一定数量的节点，代理他们进行验证和记账。

优点：大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证

缺点：整个共识机制还是依赖于代币，很多商业应用是不需要代币存在的

4、Pool验证池，基于传统的分布式一致性技术，加上数据验证机制；是目前行业链大范围在使用的共识机制

优点：不需要代币也可以工作，在成熟的分布式一致性算法（Pasox、Raft）基础上，实现秒级共识验证；

缺点：去中心化程度不如bictoin；更适合多方参与的多中心商业模式

在使用共识机制，保证数据一致性时的巨大优势（共识机制则是Ripple首先提出的，数据正确性优先的网络交易同步机制，在共识网络中，无论软件代码怎么变动，无法取得共识就无法进入网络，更不要提分叉了）。

———————————————————————

PS：稍微自黑下，虽然共识机制绝对能确保任何时候都不会产生硬分叉。但是，这种机制的缺点也比较明显，那就是要取得与其他节点的共识，明显要比当前Bitcoin网络漫长的多。极端情况下，在Ripple共识机制网络中掉线的后果也是很恐怖的。

有可能你家停电一天，第二天整个系统就再也无法与其它Rippled节点取得共识了（共识机制事实上需要超过80%的节点承认了你的数据，你的提交才会被其它节点接受，否则就会被排它的拒绝连接），甚至只能清空自己全部500多GB数据重新同步才能连上其它Ripple节点。

所以目前来说，现有的Rippled端并不适合民用（商用的话影响就比较小，比如RL自己的Rippled节点托管在亚马逊云数据中心，长时间无响应是可以高额索赔的，而且那种地方除了大型灾害几乎不会断），这也是RL一直想改进的方面之一。

分享来源区视网：

“区块链是一种共享的分布式数据库技术，其优势主要突出表现在分布式去中心化、无须信任系统和不可篡改和加密安全性三个方面。”

一、区块链技术的含义

区块链（BlockChain）技术是一种使用去中心化共识机制去维护一个完整的、分布

式的、不可篡改的账本数据库的技术，它能够让区块链中的参与者在无需建立信任关系的前提下实现一个统一的账本系统。区块是公共帐本，多点维护；链就是盖上时间戳（Timestamps），不可伪造。区块链本质上是一个注重安全和可信度胜过效率的一项技术。

目前所有的系统背后都有一个数据库，也就是一个大账本。那么谁来记这个账本就变得很重要。现在就是谁的系统谁来记账，各个银行的账本就是各个银行在记，支付宝的账本就是阿里在记。但现在区块链系统中，系统中的每个人都可以有机会参与记账。在一定时间段内如果有新的交易数据变化，系统中每个人都可以来进行记账，系统会评判这段时间内记账最快最好的人，将其记录的内容写到账本，并将这段时间内账本内容发给系统内所有的其他人进行备份。这样系统中的每个人都有一本完整的账本。

因此，这些数据就会变得非常安全。篡改者需要同时修改超过半数的系统节点数据才能真正的篡改数据。这种篡改的代价极高，导致几乎不可能。例如，比特币运行已经超过7年，全球无数的黑客尝试攻击比特币，但是至今为止没有出现过交易错误，可以认为比特币区块链被证明是一个安全可靠的系统。因此可以认为，区块链技术就是一个全民参与记账的方式，它将带来的是记账方式的革新。

二、区块链的技术优势

1、分布式去中心化

由于区块链中每个节点和矿工都必须遵循同一记账交易规则，而这个规则是基于密码算法而不是信用，同时每笔交易需要网络内其他用户的批准，所以去中心化的交易系统不需要一套第三方中介结构或信任机构背书。

而在目前，不管是传统的交易系统，还是第三方交易系统，都是基于中央账簿的体系中，中央账簿就扮演着信息保管员的角色，每笔交易需要第三方中介或者信任机构背书，这属于中心化的交易网络。

2、无须信任系统

区块链网络中，通过算法的自我约束，任何恶意欺骗系统的行为都会遭到其他节点的排斥和抑制，因此，区块链系统不依赖中央权威机构支撑和信用背书。

传统的信用背书网络系统中，参与人需要对于中央机构足够信任，随着参与网络人数增加，系统的安全性下降。和传统情况相反，区块链网络中，参与人不需要对任何人信任，但随着参与节点增加，系统的安全性反而增加，同时数据内容可以做到

完全公开。

3、不可篡改和加密安全性

区块链采取单向哈希算法，同时每个新产生的区块严格按照时间线形顺序推进，时间的不可逆性导致任何试图入侵篡改区块链内数据信息的行为都很容易被追溯，导致被其他节点的排斥，从而可以限制相关不法行为。

区块链的三大特征

相比于传统的中心化方案，区块链技术主要有以下三个特征：

1、区块链的核心思想是去中心化

在区块链系统中，任意节点之间的权利和义务都是均等的，所有的节点都有能力去用计算能力投票，从而保证了得到承认的结果是过半数节点公认的结果。即使遭受严重的黑客攻击，只要黑客控制的节点数不超过全球节点总数的一半，系统就依然能正常运行，数据也不会被篡改。

2、区块链最大的颠覆性在于信用的建立

理论上说，区块链技术可以让微信支付和支付宝不再有存在价值。《经济学人》对区块链做了一个形象的比喻：简单地说，它是“一台创造信任的机器”。区块链让人们在互不信任并没有中立中央机构的情况下，能够做到互相协作。打击假币和金融诈骗未来都不需要了。

3、区块链的集体维护可以降低成本

在中心化网络体系下，系统的维护和经营依赖于数据中心等平台的运维和经营，成本不可省略。区块链的节点是任何人都可以参与的，每一个节点在参与记录的同时也来验证其他节点记录结果的正确性，维护效率提高，成本降低。

一句话概括，区块链触动的是钱、信任和权力，这些人类赖以生存的根本性基础。

相信经过小编对区块链的优缺点和区块链的优点和缺点的介绍，你对区块链的优缺点了解更加地透彻了，感谢你对我们地支持与关注！