

大家好，今天来为大家分享区块链缺陷的一些知识点，和区块链 缺陷的问题解析，大家要是都明白，那么可以忽略，如果不太清楚的话可以看看本篇文章，相信很大概率可以解决您的问题，接下来我们就一起来看看吧！

本文目录

1. [区块链发展趋势如何](#)
2. [如何看待区块链技术的安全性？](#)
3. [属于区块链共同机制的是](#)
4. [区块链是什么，能解决什么？](#)

区块链发展趋势如何

关注天下财经，掌握财务自由。

下文为财经简讯原创，仅作参考。

首先，区块链的前世今生；

可能最能引起注意的是比特币，因为比特币价格飙涨，让全世界都为之疯狂，尤其是多年前拿几百个比特币来买汉堡的小伙伴更为抓狂。比特币基于区块链技术，所谓区块链通俗点就是一种计算机技术，相当每一个节点就是一本账本，每个节点都会记录有交集的交换记录信息，并相互通知对方。经过一系列的传递，所有节点都有了交换记录信息。相当于拿着大喇叭，所有借钱还钱的事情都告之天下，所有人都把信息记录在自己的账本上；

其次，金融行业的发展潜力；

如今银行都是以各国央行为中心，货币线上流通的记录都上报中央银行。当国家与国家进行交易时，会有外汇结算机构进行记录管理。这种模式就是所谓中心模式，所有线上的记录都由中央银行记录。这种传统模式会存在洗黑钱、监管模糊不清的情况，比如纽约、香港、伦敦这些金融中心，会产生资源不合理配置，被少部分人利用，因为这些金融中心掌握着资金的流通，如篡改、私营。如果采用区块链技术为基础，则基本属于完全公开化的模式，不会产生这些缺陷；

最后，潜力与阻力；

潜力肯定是无限的，如果采用可靠的区块链技术，大大降低全球的金融运营成本、大大提高效率和安全性。上个月Facebook想要推出libra，就是一种基于社交的区

区块链技术货币，对企业来说能提高其重要度。事情都有两面，全球央行或者既得利益者，不可能如此放弃利益，随着潮流的发展，每个国家都会自己掌握数字货币。区块链技术也可能存在缺陷或黑客攻击等问题。但如何一次生产力的提高都离不开技术的提高，都不可能存在完美的东西，只有不断完善。

如何看待区块链技术的安全性？

技术上哈希算法和RSA算法在超强算力的区块、链组合下根本无懈可击，特别是区块链比特币的庞大市值已经是简单的辅助证据。

但是我更想聊一聊共识分散化的问题

从近两年比特币的发展来看，比特币的共识在不断碎片化，最重大的一次就是BCH，但是实际上ETH、EOS都是对比特币共识的碎片化。当然每一次碎片化都做大了整个区块链市场的蛋糕。

借用一句话，公司组织高速膨胀期一切反对意见都是良药，但是什么时候会是毒药？在纯粹共识的路上区块链世界已经走得很远，我觉得是应该回头用共识为互联网为线下实体做些贡献。纯粹的共识很容易破散，结合了互联网“实业”和线下“实业”后才是坚强的共识。

技术上，越是新的产物未经安全检验无法判断安全性能。但是就像另一个回答说的：比特币、以太坊的安全性可以直接对标谷歌、亚马逊了。

属于区块链共同机制的是

在区块链系统中没有像银行一样的中心化机构，所以在进行传输信息、价值转移时，共识机制解决并保证每一笔交易在所有记帐节点上的一致性和正确性问题。区块链的这种新的共识机制使其在不依靠中心化组织的情况下，依然大规模高效协作完成运转。

除了密码学技术外，共识机制也是区块链必要元素及核心部分，是保障区块链系统不断运行的关键。

在区块链网络中，由于应用场景的不同，所以采用了不同的共识算法。目前区块链的共识机制主要有四类：1.工作量证明机制pow、2.权益证明机制pos、3.委托权益证明Dpos、4.验证池共识机制pool

1.工作量证明(ProofofWork，简称POW):

可简单理解为一份证明，证明你做过一定量的工作。通过查看工作结果，就能知道你完成了指定量的工作。区块链共识算法用的最多的就是POW。比特币和以太坊都是基于POW的共识机制。

例：比特币在区块的生成过程中使用的就是POW机制，简单理解就是大家共同争夺记账权利，谁先抢到并正确完成记账工作，谁就得到系统的奖励，奖励为比特币，也就是所谓的“挖矿”。矿工（参与挖矿的人）通过计算机的算力去完成这个记账工作，这个拥有计算能力的专业计算机就是所谓的“矿机”。

优点：

- ①完全去中心化，节点自由进出，避免了建立和维护中心化信用机构的成本。
- ②只要网络破坏者的算力不超过全网总算力的50%，网络的交易状态就能达成一致，并不可篡改历史记录。
- ③投入越多算力，获得记账权概率越大，越有可能产生新的区块奖励。

缺点：

- ①目前比特币挖矿造成大量的算力和能源浪费。
- ②挖矿的激励机制也造成挖矿算力的高度集中
- ③结算周期长，每秒最多结算7笔交易，不适合商业应用。

2.权益证明(Proof of Stake, 简称POS):

通过持有Token（代币）的数量和时长来决定你获得记账的机率，类似于股票的分红制度，持有股权越多的人就能够获得更多的分红。Token相当于区块链系统的权益。目前有很多数字资产用pow发行新币。

优点：

- ①降低了PoW机制的资源浪费。
- ②加快了运算速度，也可以理解为工作量证明的升级版

缺点：

①拥有币龄越长的节点获得记账权的几率越大，容易导致马太效应，富者越富，权益会越来越集中,从而失去公正性。

3.委托权益证明(DelegatedProofofStake，简称DPOS):

是基于POS衍生出的更专业的解决方案，类似于董事会投票，指拥有Token的人投票给固定的节点，选举若干代理人，由代理人负责验证和记账。不同于POW和POS的全网都可以参与记账竞争，DPOS的记账节点在一定时间段内是确定的。

为了激励更多人参与竞选，系统会生成少量代币作为奖励。比特股就采用该方式。

优点：

相较pow，dpos大幅提高区块链处理数据的能力，甚至可以实现秒到账，同时也大幅降低维护区块链网络安全的费用。

缺点：

去中心程度较弱，节点代理是人为选出的，公平性相比POS较低，依赖于代币的增发来维持代理节点的稳定性。

4.验证池共识机制Pool

这是一种基于传统的分布式一致性技术，加上数据验证的机制，是目前行业链大范围在使用的共识机制；

优点：不需要依赖代币也可以实现秒级共识验证；

缺点：去中心化程度弱，更适合多方参与的多中心商业模式；

总结：每一种共识机制都不能同时满足安全、效率、公平。去中心程度越弱，安全性就越低，区块链的速度就越快；去中心化程度越强，安全性就会越高，区块链的速度就会越慢。POW完全去中心化，但运行效率太低。POS提高了效率，但却降低了公平与安全。DPOS有强烈的中心化特性，却在短期内效率最高。目前行业区块链大范围使用Pool共识。

区块链是什么，能解决什么？

区块链是什么

区块链本质上是一个去中心化数据库。是一种分布式数据存储，点对点传输，共识机制，加密算法等计算机技术的新型应用模式。

举个例子：

比如说小明找大康借一百块钱，但大康怕他赖账，于是就找来村长做公证，并记录下这笔账，这个就叫中心化。但如果，你不找村长，直接拿个喇叭在村里大喊“我大康借给小明一百块钱！请大家记在账本里”，这个就叫去中心化。

以前村长德高望重，掌握全村的账本，大家都把钱存在他这里，这是过去大家对中心化的信任。现在，大家都担心村长会偷偷挪用大家的钱，怎么办呢？于是大家就给每个人都发了一本账本，任何人之间转账都通过大喇叭发布消息，收到消息后，每个人都在自家的账本上记下这笔交易，这就叫去中心化。有了分布式账本，即使老孔或老周家的账本丢了也没关系，因为老朱、老杨等其他家都有账本。

区块链有什么特点：

去中心化：因为区块链的去中心化，它可以帮助点对点交易，因此，无论你是在交易还是交换资金，都无需第三方的批准。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。去中心化是区块链最突出最本质的特征。

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。开放性比较少被提到，但它也很重要，甚至可以说开放性是去中心化特性的保证之一。

安全：不受任何人或实体的控制，数据在多台计算机上完整复制（分发），攻击者无单一的入口点。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。

不可篡改：信息通过密码学技术进行加密，一旦进入区块链，任何信息都无法更改。

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。区块链的匿名性特点，在一定程度上很好地保护了用户的隐私。但是区块链的匿名性也颇具争议，因为它在人们交易、隐私方面起到了重要的保护作用，也为一些违法犯罪行为提供了“保护伞”。

区块链应用领域

金融领域

区块链在国际汇兑、信用证、股权登记和证券交易所等金融领域有着潜在的巨大应用价值。将区块链技术应用在金融行业中，能够省去第三方中介环节，实现点对点的直接对接，从而在大大降低成本的同时，快速完成交易支付。

首先是因为区块链的去中心化特性带来的优势。在传统的金融机构，如银行，老王想给小张转一笔钱，他需要先通过中心机构银行的确认才能把钱转到小张手中，而在区块链网络中，老王不需要通过银行就能把钱转给小张，这不仅提高了交易的效率，还在一定程度上节约了交易的成本。

目前火爆的defi，就是去中心化金融，虽然现在还在初始阶段，各方面都还不够成熟，但相比2017年的1-C-0空气，已经有了一定的落地。

物联网和物流领域

区块链在物联网和物流领域也可以天然结合。通过区块链可以降低物流成本，追溯物品的生产和运送过程，并且提高供应链管理的效率。将物流和供应链行业带入现代化将在全球范围内产生广泛影响。通过降低整体成本并允许物流流程中的实体与更多的个体代理商合作，整个物流将会有全面的改进。这些效率的提高最终将导致在流程的每个阶段节省成本。该领域被认为是区块链一个很有前景的应用方向。

公共服务领域

区块链在公共管理、能源、交通等领域都与民众的生产生活息息相关，但是这些领域的中心化特质也带来了一些问题，可以用区块链来改造。比如，对于普通企业来说，往往最难的就是去政府部门办事，不但需要各种证明文件，而且还需要跑多个部门，不同的部门要求还不一样。主要原因就是原先各个政府部门的数据都是孤立的，彼此不共享，但如果都能在信息高度安全的基础上“上链”，数据实现共享，则办事人就能实现只需在一个部门内解决多数问题。因为所有办事流程交付给智能合约后，后面就可以自动处理并流转，所谓“一网通办”并不再是梦想。

数字版权领域

通过区块链技术，可以对作品进行鉴权，证明文字、视频、音频等作品的存在，保证权属的真实、唯一性。作品在区块链上被确权后，后续交易都会进行实时记录，实现数字版权全生命周期管理，也可作为司法取证中的技术性保障。拿一首歌曲来

说，如果原作人申请了该歌曲的版权，但是由于中心化机构存在存储不安全、不公开透明以及易被利益驱使的缺陷，版权可能被他人进行篡改，这样很可能损害了歌曲原创者的权益，而如果说该歌曲的数字信息及版权信息记录在了区块链上，借助区块链的公开透明以及防篡改性等优势，就能很好地避免版权信息被恶意篡改的情况发生了。

保险领域

在保险理赔方面，保险机构负责资金归集、投资、理赔，往往管理和运营成本较高。通过智能合约的应用

文章到此结束，如果本次分享的区块链缺陷和区块链缺陷的问题解决了您的问题，那么我们由衷的感到高兴！