大家好，感谢邀请，今天来为大家分享一下区块链 论文的问题，以及和区块链 论文推荐的一些困惑，大家要是还不太明白的话，也没有关系，因为接下来将为大家分享，希望可以帮助到大家，解决大家的问题，下面就开始吧！

本文目录

什么是“区块链”？

我不是计算机技术专家，以下对区块链的介绍来自阅读和专家朋友的评论，仅供参考。

如果要用一个词来解释区块链，那就是：分布式记账。

要理解一下这个词是什么意思，就需要先理解，传统的记账都是有一个中心的。比如银行，你从银行存款取款，通过银行借钱给别人，都是以银行为中心，所有这些交易都建立在银行的信用之上。那如果银行耍赖呢？或者更严重，国家耍赖呢？国民党在统治中国大陆的末期滥发金圆券，以及魏玛德国和津巴布韦的恶性通货膨胀，搞得货币没有卫生纸值钱，都是非常著名的例子。

金圆券

区块链针对的，就是这个问题。他们认为，去中心化的记账才是不可修改，不可抵赖的。怎么实现去中心化记账？基本的思想是，所有的用户都存储下所有的交易记录，通过数学方法，让非法修改账本变得非常困难。这样一来，就保证了账本的可靠性。

具体而言，所有用户通过穷举随机数变量，第一个得到特定要求哈希函数值（Hash）的用户将有权记账该轮交易，并获得对应的比特币奖励。以数据块（block）的形式进行传输，并以末端追加的方式将数据块连成链状（chain），因而叫做区块链（blockchain）。

听了介绍，你也许会感到这种思想很有意思，但并不像宣传得那样激动人心，那样有革命性。你的感觉是对的。实际上，区块链的基本逻辑就有些绕不过去的问题。

例如，目前完整的比特币公共账本大小已经超过150G，并以每年数十G的速度快速递增——仅仅为了支持500万用户每年3000万笔交易。如果有朝一日其处理量与目前的支付宝比肩，那每年比特币账本的大小将增加超过500T。这相当于把支付宝服务器的存储数据在所有用户的个人电脑上进行备份，——你会觉得这是个好主意吗？

又如，在传统的银行体系中，如果你把密码丢了，并没有什么了不起，向系统及时申报就是了，你的财富不会消失。但在区块链体系中，如果你把密码丢了，那么这就是个巨大的麻烦，你的货币就找不回来了。开不开心？意不意外？

区块链产品落地原理

区块链的定义业界并没有一个特别明确和唯一的回答，这里先给出个人根据所读论文而总结出的“区块链”应有特质：使用了具有"哈希链"(下文有解释)形式的数据结构保存基础数据有多个结点参与系统运行（分布式）通过一定的协议或算法对于基础数据的一致性达成共识（共识协议/算法）。

区块链靠谱吗，投资有风险吗？

区块链并不火，区块链是因比特币而火的，加密货币只是区块链+金融的成功作品。

先有比特币创造了一批财务自由，有资本入场利用空气币、山寨币怒割韭菜，现在的币圈可谓生灵涂炭，需要很长的时间来恢复元气。

而区块链只是一个技术，关于区块链是什么可以看下文。

【定义】

区块链（Blockchain）是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。该技术方案让参与系统中的任意多个节点，把一段时间系统内全部信息交流的数据，通过密码学算法计算和记录到一个数据块（block），并且生成该数据块的指纹用于链接（chain）下个数据块和校验，系统所有参与节点来共同认定记录是否为真。

区块链是一种类似于NoSQL（非关系型数据库）这样的技术解决方案统称，并不是某种特定技术，能够通过很多编程语言和架构来实现区块链技术。并且实现区块链的方式种类也有很多，目前常见的包括POW（ProofofWork，工作量证明），POS（ProofofStake，权益证明），DPOS（DelegateProofofStake，股份授权证

明机制）等。

区块链的概念首次在论文《比特币：一种点对点的电子现金系统（Bitcoin:APeer-to-PeerElectronicCashSystem）》中提出，作者为自称中本聪（SatoshiNakamoto）的个人（或团体）。因此可以把比特币看成区块链的首个在金融支付领域中的应用。

【通俗解释】

无论多大的系统或者多小的网站，一般在它背后都有数据库。那么这个数据库由谁来维护？在一般情况下，谁负责运营这个网络或者系统，那么就由谁来进行维护。如果是微信数据库肯定是腾讯团队维护，淘宝的数据库就是阿里的团队在维护。大家一定认为这种方式是天经地义的，但是区块链技术却不是这样。

如果我们把数据库想象成是一个账本：比如支付宝就是很典型的账本，任何数据的改变就是记账型的。数据库的维护我们可以认为是很简单的记账方式。在区块链的世界也是这样，区块链系统中的每一个人都有机会参与记账。系统会在一段时间内，可能选择十秒钟内，也可能十分钟，选出这段时间记账最快最好的人，由这个人来记账，他会把这段时间数据库的变化和账本的变化记在一个区块（block）中，我们可以把这个区块想象成一页纸上，系统在确认记录正确后，会把过去账本的数据指纹链接（chain）这张纸上，然后把这张纸发给整个系统里面其他的所有人。然后周而复始，系统会寻找下一个记账又快又好的人，而系统中的其他所有人都会获得整个账本的副本。这也就意味着这个系统每一个人都有一模一样的账本，这种技术，我们就称之为区块链技术（Blockchain），也称为分布式账本技术。

由于每个人（计算机）都有一模一样的账本，并且每个人（计算机）都有着完全相等的权利，因此不会由于单个人（计算机）失去联系或宕机，而导致整个系统崩溃。既然有一模一样的账本，就意味着所有的数据都是公开透明的，每一个人可以看到每一个账户上到底有什么数字变化。它非常有趣的特性就是，其中的数据无法篡改。因为系统会自动比较，会认为相同数量最多的账本是真的账本，少部分和别人数量不一样的账本是虚假的账本。在这种情况下，任何人篡改自己的账本是没有任何意义的，因为除非你能够篡改整个系统里面大部分节点。如果整个系统节点只有五个、十个节点也许还容易做到，但是如果有上万个甚至上十万个，并且还分布在互联网上的任何角落，除非某个人能控制世界上大多数的电脑，否则不太可能篡改这样大型的区块链。

【要素】

结合区块链的定义，我们认为必须具有如下四点要素才能被称为公开区块链技术，

如果只具有前3点要素，我们将认为其为私有区块链技术（私有链）。

1、点对点的对等网络（权力对等、物理点对点连接）

2、可验证的数据结构（可验证的PKC体系，不可篡改数据库）

3、分布式的共识机制（解决拜占庭将军问题，解决双重支付）

4、纳什均衡的博弈设计（合作是演化稳定的策略）

【特性】

结合定义区块链的定义，区块链会现实出四个主要的特性：去中心化（Decentralized）、去信任（Trustless）、集体维护（Collectivelymaintain）、可靠数据库（ReliableDatabase）。并且由四个特征会引申出另外2个特征：开源（OpenSource）、隐私保护（Anonymity）。如果一个系统不具备这些特征，将不能视其为基于区块链技术的应用。

去中心化（Decentralized）：整个网络没有中心化的硬件或者管理机构，任意节点之间的权利和义务都是均等的，且任一节点的损坏或者失去都会不影响整个系统的运作。因此也可以认为区块链系统具有极好的健壮性。

去信任（Trustless）：参与整个系统中的每个节点之间进行数据交换是无需互相信任的，整个系统的运作规则是公开透明的，所有的数据内容也是公开的，因此在系统指定的规则范围和时间范围内，节点之间是不能也无法欺骗其它节点。

集体维护（Collectivelymaintain）：系统中的数据块由整个系统中所有具有维护功能的节点来共同维护的，而这些具有维护功能的节点是任何人都可以参与的。

可靠数据库（ReliableDatabase）：整个系统将通过分数据库的形式，让每个参与节点都能获得一份完整数据库的拷贝。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库的修改是无效的，也无法影响其他节点上的数据内容。因此参与系统中的节点越多和计算能力越强，该系统中的数据安全性越高。

开源（OpenSource）：由于整个系统的运作规则必须是公开透明的，所以对于程序而言，整个系统必定会是开源的。

隐私保护（Anonymity）：由于节点和节点之间是无需互相信任的，因此节点和节点之间无需公开身份，在系统中的每个参与的节点的隐私都是受到保护。

【区块链意义之一：解决拜占庭将军问题】

区块链解决的核心问题不是“数字货币”，而是在信息不对称、不确定的环境下，如何建立满足经济活动赖以发生、发展的“信任”生态体系。而这个问题称之为“拜占庭将军问题”，也可称为“拜占庭容错”或者“两军问题”，这是一个分布式系统中进行信息机交互时面临的难题，即在整个网络中的任意节点都无法信任与之通信的对方时，如何能创建出共识基础来进行安全的信息交互而无需担心数据被篡改。区块链使用算法证明机制来保证整个网络的安全，借助它，整个系统中的所有节点能够在去信任的环境下自动安全的交换数据。更多介绍请参见《比特币与拜占庭将军问题》。

【区块链意义之二：实现跨国价值转移】

互联网诞生最初，最早核心解决的问题是信息制造和传输，我们可以通过互联网将信息快速生成并且复制到全世界每一个有着网络的角落，但是它尚始终不能解决价值转移和信用转移。这里所谓的价值转移是指，在网络中每个人都能够认可和确认的方式，将某一部分价值精确的从某一个地址转移到另一个地址，而且必须确保当价值转移后，原来的地址减少了被转移的部分，而新的地址增加了所转移的价值。这里说的价值可以是货币资产，也可以是某种实体资产或者虚拟资产（包括有价证券、金融衍生品等）。而这操作的结果必须获得所有参与方的认可，且其结果不能受到任何某一方的操纵。

在目前的互联网中也有各种各样的金融体系，也有许多政府银行提供或者第三方提供的支付系统，但是它还是依靠中心化的方案来解决。所谓中心化的方案，就是通过某个公司或者政府信用作为背书，将所有的价值转移计算放在一个中心服务器（集群）中，尽管所有的计算也是由程序自动完成，但是却必须信任这个中心化的人或者机构。事实上通过中心化的信用背书来解决，也只能将信用局限在一定的机构、地区或者国家的范围之内。由此可以看出，必须要解决的这个根本问题，那就是信用。所以价值转移的核心问题是跨国信用共识。

在如此纷繁复杂的全球体系中，要凭空建立一个全球性的信用共识体系是很难的，由于每个国家的政治、经济和文化情况不同，对于两个国家的企业和政府完全互信是几乎做不到的，这也就意味着无论是以个人抑或企业政府的信用进行背书，对于跨国之间的价值交换即使可以完成，也有着巨大的时间和经济成本。但是在漫长的人类历史中，无论每个国家的宗教、政治和文化是如何的不同，唯一能取得共识的是数学（基础科学）。因此，可以毫不夸张的说，数学（算法）是全球文明的最大公约数，也是全球人类获得最多共识的基础。如果我们以数学算法（程序）作为背书，所有的规则都建立一个公开透明的数学算法（程序）之上，能够让所有不同政治文化背景的人群获得共识。

【未来的发展】

互联网将使得全球之间的互动越来越紧密，伴随而来的就是巨大的信任鸿沟。目前现有的主流数据库技术架构都是私密且中心化的，在这个架构上是永远无法解决价值转移和互信问题。所以区块链技术有可能将成为下一代数据库架构。通过去中心化技术，将能够在大数据的基础上完成数学（算法）背书、全球互信这个巨大的进步。

区块链技术作为一种特定分布式存取数据技术，它通过网络中多个参与计算的节点开共同参与数据的计算和记录，并且互相验证其信息的有效性（防伪）。从这一点来，区块链技术也是一种特定的数据库技术。互联网刚刚进入大数据时代，但是从目前来看，大数据还处于非常基础的阶段。但是当进入到区块链数据库阶段，将进入到真正的强信任背书的大数据时代。这里面的所有数据都获得坚不可摧的质量，任何人都没有能力也没有必要去质疑。

也许我们现在正处在一个重大的转折点之上——和工业革命所带来的深刻变革几乎相同的重大转折的早期阶段。不仅仅是新技术指数级、数字化和组合式的进步与变革，更多的惊喜也许还会在我们前面。在未来的24个月里，这个星球所增长的计算机算力和记录的数据将会超过所有历史阶段的总和。在过去的24个月里，这个增值可能已经超过了1000倍。这些数字化的数据信息还在以比摩尔定律更快的速度增长。区块链技术将不仅仅应用在金融支付领域，而是将会扩展到目前所有应用范围，诸如去中心化的微博、微信、搜索、租房，甚至是打车软件都有可能会出现。因为区块链将可以让人类无地域限制的、去信任的方式来进行大规模协作。

我们这一代人将很可能会幸运地经历人类历史上两个最让人吃惊的事件，地球上的所有人和所有机器通过区块链技术以前所未有的互信展开了空前的大规模协作，其次就是基于此真正的人工智能将被创造出来。这两个时间将会深深地改变这个世界的经济发展模式。创业者、企业家、科学家以及各种各样的极客将利用这个充裕的世界去创造能让我们震惊和快乐。

区块链的10大应用

?金融服务：在一些私募与众筹项目上，利用区块链交易流程可以缩短周期。?医疗健康：应用于医院挂号、数字病例。将这些数据记录在链上，可以保证我们的健康数据不被侵犯。?IP版权：有利于维权。利用区块链技术，把数字资产记录在链上，第三方继续使用IP版权的时候，就可以通过技术追溯到谁在用，什么时候发生的。?教育：学籍证明、档案管理、学生征信、成绩证明、产学合作等。利用区块链都可以把教育上的数据通过一种资产的方式存储在分布式的数据库当中，可以永久保留。?物联网：物品的溯源、防伪、认证，还有网络效率提升，可以把每个物品当成

一个节点进行存储流转。?共享经济：租车租房、智能硬件租赁、知识技能租赁。它可以把这些资产本身放在区块链的链条当中，对于使用权，进行流转，享受一些使用权的费用。?通信：区块链技术可以让每个人的社交ID进行确权，比如在运营商的社交数据，它可以变成一种资产进行管理。?社会管理：身份认证、档案管理、公证遗产继承、个人及社会信用等。以区块链技术进行记录，放在分布式数据库当中，永久保存。?慈善公益：可以实现整个捐助流程的阳光化。?文化娱乐：视频版权、音乐版权、软件防伪数字等。它们本身属于数字资产，容易被追诉，容易被记录，容易被进行透明化改造。

区块链并没有你想象当中的那么吊炸天，他也无法颠覆世界，只是可以让现很多传统的业务更加人性化，更加便利，更能保护隐私。

想要变现的话，区块链并不适合，因为他的开发成本太贵了。

百度推出区块链项目「莱茨狗」，有投资价值吗？

从花样不同的币，到养猫和养狗，区块链正迎来一轮热潮。眼下，BAT也开始涉足区块链市场，百度推出区块链项目“莱茨狗”。在比特币和各种币价格一路疯狂飙升后，“莱茨狗”是否值得投资呢?

先来看一下比特币为何如此火爆的。由于比特币全球的发行数量有限，而且每年都会损耗一定数量的比特币，这让比特币成为了稀缺物品，这一定程度上是比特币价格疯狂涨的原因。此外，能够在市场上流通，是比特币这个虚拟货币能够有市场价值的关键条件。如果一个虚拟货币无法在市场流通，就没有任何价值。

那么，百度的区块链项目“莱茨狗”是否有投资价值，也有两个关键的条件：

1、“莱茨狗”数量：从用户爆料的消息来看，百度区块链项目官网称，用户可以在10只形态各异的宠物狗中选择并领养。按照规定，一个百度账号可以领养两只，并首先需要下载百度钱包。不过，百度方面并没有透露“莱茨狗”是否有一个总的数量限制。

如果“莱茨狗”也像现实生活中的狗一样，能够繁殖，并且有生老病死，那么“莱茨狗”项目就很难盈利。当然了，如果百度区块链项目能够控制“莱茨狗”的繁殖速度和死亡的时间，让“莱茨狗”的数量保持在一定的区间，这个区块链还是有价值的。

2、“莱茨狗”能否进入市场交易：市场上的宠物都可以交易，那么生活在区块链中的虚拟宠物如果不能进入市场交易，这只“莱茨狗”同样没有任何的价值。在现

实生活中，宠物狗会根据品种不同，有不同的价格。区块链的“莱茨狗”是否也要有价格高低的品种呢?

由于现在百度区块链项目“莱茨狗”还有太多的未知信息，目前不好判断这一项目是否有投资的价值。不过，能够进入市场交易，并且严格控制“莱茨狗”的数量，这是百度区块链项目能否产生价值的关键因素。

END，本文到此结束，如果可以帮助到大家，还望关注本站哦！