我认为，如果去中心化是区块链的价值点，那去中心化同样也是制约它发展的缺点。都说区块链去中心化，但实际上它又建立了新的中心化，在隐私和信任问题上，对于不同领域的效用是不同的，区块链技术的应用更是要考虑人性的贪婪和国家监管政策等很多方面的。

1、区块链技术下孕育出的比特币

这里没有办法非常具体的聊区块链底层的东西，我也只是从概念层面浅谈的，可能内容会有误，还望大佬指正。

区块链技术从浅层来看，就是把无数个计算机纳入到一个网络系统中，每一个计算机都是一个节点，系统会每相隔一定时间生成一个区块，一个区块中有无数个节点，因为节点是一台计算机，所以每个区块都拥有强大的计算能力。

区块链接起来就是名义上的区块链了，然后运用了一定的算术算法（比如哈希算法）在有限的区块中选出计算能力很强的少数个，给予他们记账能力。

一直在想如何通俗易懂的将区块链中的节点、区块描述出来，周末定的外卖给了我

一个启发：

区块链其实可以理解成外卖打包流程，所有的商家就是终端（计算机），也就是一个节点，商家出的餐经过贴上时间戳就是一个区块，每一个区块会按照时间顺序链接起来，形成不可逆的出餐链条，这条链条可以比喻为区块链。

有一问题就是“我作为独立的个体，为什么要拿自己计算机接入该系统呢？”。所以基于区块链技术的整个系统会有奖励机制。

比如比特币系统就约定如此：每个区块的第一笔交易进行特殊化处理，该交易产生一枚由该区块创造者拥有的新的电子货币。这样就增加了节点支持该网络的激励，并在没有中央集权机构发行货币的情况下，提供了一种将电
子货币分配到流通领域的一种方法。

每一次交易发生时，都需要进行记录，进行记录的这个节点就会获得25个比特币的奖励，这也会造成非常激烈的竞争，所以通过节点的算力来进行确认，利用哈希算法去筛选出运算能力最强的少数节点，由他们来加下这笔账，并获得奖励，这也发展成了挖矿和挖矿工，众多节点拧成一股绳，一起进行运算，平分奖励。

由于受到算法的限制，比特币的总量是有限的，总计约不到2100万个，具有稀缺性，就跟古董一样，只要有人支持它有升值价值，它就能一直流通下去，只是价格波动性很高，玩家们都是长期投资，不看重短期的涨跌，所以割韭菜的短线投资者最容易反被割。

比特币的本质就是一串代码，具有唯一性、防伪标识。它能否在市场流通完全取决于消费大众的认知、以及政府的政策。就像以前拿一头牛换3头羊、拿粮票换粮食一样，人们相互之间认可这种交易，并认可它为等值的，包括现在的硬币、纸币、银行账户和支付宝账户的数字，都是因为被人们广泛的认可为交易介质才可以流通。

硬币本质就是金属、纸币本质就是特殊处理的纸张，银行和支付宝账户的数字本身只是货币的电子记录形式，它们的等值交换和相互流通都来自于政府和人们对其交易中介价值的认可，而比特币现在确实在国内是没有价值的，但不代表未来没有实质价值，所以仍然有很多人看好比特币，持续的在进场，就和股票一样，很大投机心理，赚就赚N倍的收益，如果是想以百分之多少的收益心理投资，那基本是很难做到。

2、比特币如何对电子货币去中心化？

比特币是区块链技术在电子货币领域应用的第一胎。

它最大的优势在于在支付领域去中心化，本质是一个点对点的电子支付清算系统。比如你以前转500元给A，你的动作是发“转账500元到A的账户”给银行（或者支付宝等），金融机构（或非银行类金融机构）收到你的指令，然后执行操作，整个过程A是没办法感知的，她不知道你是什么时候支付，但是源于对银行的信任，你给A的银行转账凭证就能安心。

但是银行有可能是没办法兑付这笔款了，你转账就失败了，A也收不到钱了，这个几率很小，但不代表绝对不会发生。于是就又有人提出了P2P式的点对点支付，你直接支付给A，中间不需要金融机构来进行确认，但是信任问题怎么解决呢？

银行是一个足够信任的个体，没有了银行，就没有银行账户的账单了，也就是没有总账单了，那就需要一个账单来记录交易，账单只解决了记录问题，还是没有解决信任问题。

生活现实中总会有人承诺的事情自己忘记了，事后还不承认，如果周围人都说他承诺过，那么他就抵赖不掉了。如果这个基数足够大，我们就认为绝大部分人都是诚实的，也就是都是说的真话，那51%以上的诚实的人说的事情就是事实。

类比到电子支付领域，如果你转账给A这笔账单让足够多的人知道了，并且由于基数足够大，默认为大家都是诚实的，当你想反悔说自己没有转过这笔账的时候，大家就会diss你，这个就是让诚实的群众来做信任中枢，没有任何一个机构或者个人可以决定。

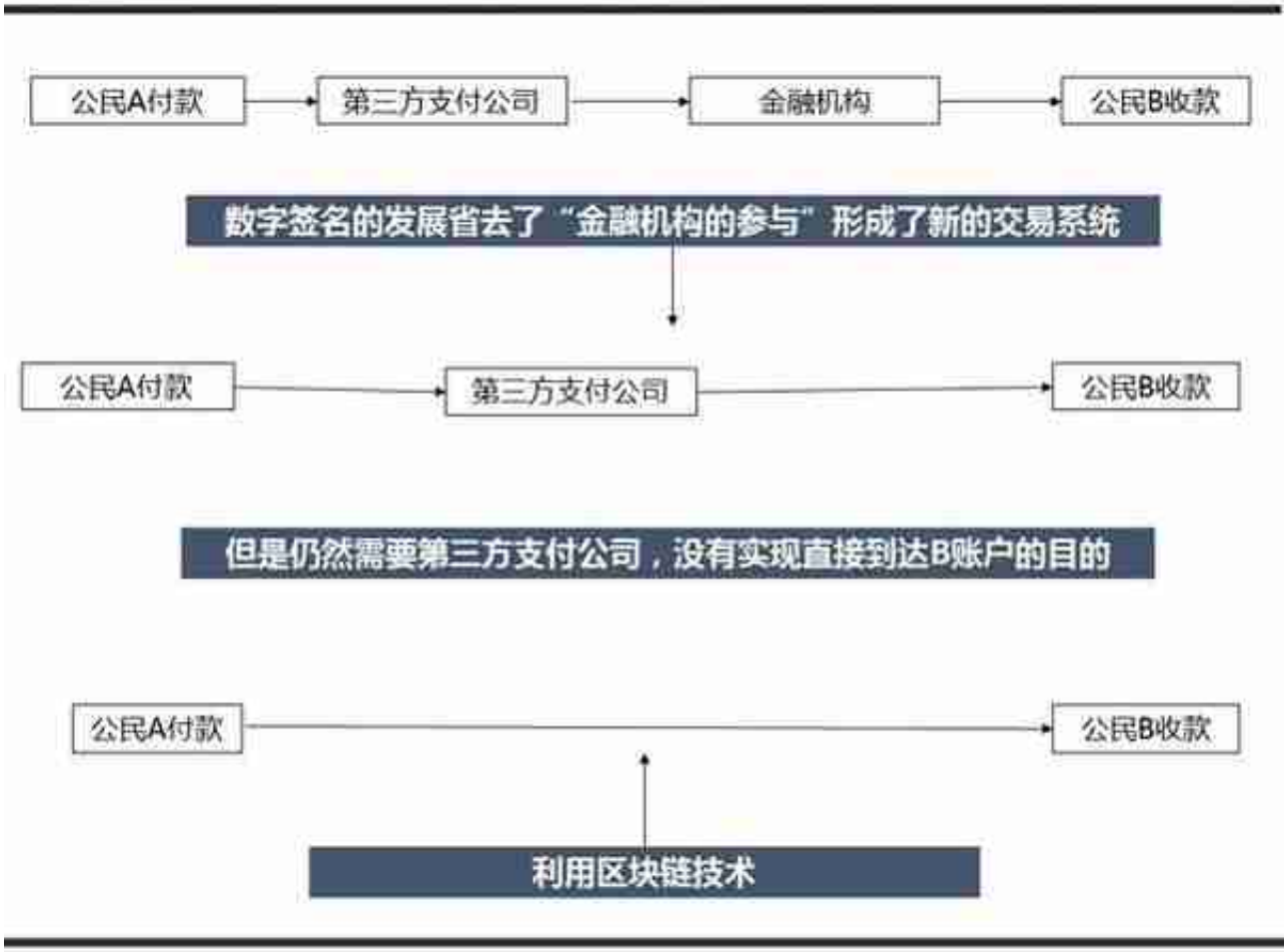
区块链的核心理念就是：人人都是诚实的，系统内的每一笔交易都记录，并且发送给每一个节点，每一个节点都拥有一个总账本，想要更改交易必须将51%的节点上的账本进行更改，这也就是去中心化。

但是实际上还是建立了新的中心化，也就是点对点电子支付系统的建立者，虽然目前都是要求披露所有源代码，但是仍有众多玩家并没有披露，这也是ICO电子货币被国内禁止的原因，套现跑路风险过大。

选择数字货币支付商品、账单甚至学费正在成为全球新兴的支付热潮。日本、美国、德国、澳大利亚等国家对比特币支付的立场越来越开放。2017年4月日本内阁承认比特币等虚拟货币作为授权付款工具，2013年8月德国财政部认可比特币为合法的私有资产。

从下图也能看到，比特币让人们看到了：原来电子货币的交易是可以不经过金融机

构、可以不依赖于第三方信用担保机构的。在金融领域，中心化的集权主要集中在微信、支付宝、银行等，他们拥有用户大量的交易信息，从某种程度上说是不安全的。



虽然微信和支付宝都会说自己是绝对安全的，银行也会说自己绝对安全。从Uber数据泄漏事件看，即使企业再怎么对内对外进行数据加密，数据依然有很大几率泄露的；银行说是存储货币的地方，但实际上只有少部分钱在银行账上，大部分款项都是放出去了，不是绝对安全的。

并且，无论是支付宝、微信、还是银行账户上的数字本质上是货币的记录，它是可以取现的，有纸币的形式（未来可能微信和支付宝能支持ATM机取现~），但是比特币没有实体形式，它就是在比特币网络里流通的电子货币。

这就意味着，如果商品市场允许拿比特币交易的话，比特币账户和支付宝账户是一样的，A账户减少，B账户就增加，A到B的交易就完成了。

区块链就是这笔交易的底层实现技术了，A发起交易申请，然后各个计算机（节点）开始争夺记账权（速成挖矿，每一个节点都是挖矿工），拿到记账权的节点记下

这笔账，并像系统内的全网进行传播，其他节点看到这笔交易并进行确认，确认的操作会被系统盖上时间戳，带有时间戳的交易确认就形成一个区块，当有足够多的节点都对这笔交易进行确认的时候（比特币是6笔），这笔交易就成功发生了。

比特币有自身很强大的优势，比如去中心化、开放性、不可撤销和篡改、加密安全性。利用的人人们的信任心理，人们对“集权机构”和“足够多的个体”都是信任的，个体是没有中心化的；交易账单是开放的透明的（但不会透漏个人信息，会有私钥和公钥来加密解密）；因为时间的不可逆，所以交易不可以更改和撤销，造假需要绝大多数人都不诚实，这个成本非常之高。

3、区块链的中心化和去中心化

首先我们再回顾一下区块链技术的理解：区块链本质上是解决信任问题、降低信任成本的技术方案，目的就是为了去中心化，去信用中介。

所以区块链应用的领域一定最好是具有“中央集权”式的中心化、信任失衡问题的领域，从这个角度看，目前国内大多数公司的区块链项目都只是投机倒把，只因为这其中有巨大的利润率。

当然也有实际的好的应用案例，比如：

Storj VS. Dropbox的去中心化存储

storj.io是以区块链技术为基础的不会停机的智能云存储平台，一个去中心化的基于区块链的分布式云存储系统，它能保证任何时候对用户上传到区块链的内容进行加密。若用户要从区块链上下载内容，就必须使用对应的私钥。因此，Storj网络可靠性和安全性都非常高。目前Storj的用户存储量已达到5PB。

去中心化存储是利用每一个节点（计算机）剩余的存储空间进行出租，如果贡献出租的硬盘的人数足够多，那么云存储公司将可以不需要存储设备，也会降低人员成本、数据中心成本等。而贡献存储空间的节点将获得密码学货币的回报（类似比特币）——叫“燃料”。

实际上，比特币的去中心化概念并不是独特的。我们现有的技术和社会制度就有某些去中心概念。

关于区块链去中心化的描述，这篇文章的叙述我非常认同，这里引用翻译）

电子邮件中有基于一个去中心化的协议 Simple Mail Transfer Protocol（SMTP）。每个人按 SMTP 协议标准搭建一个 SMTP 服务器，都是可以收发电子邮件的。

但是现实中，例如 Google gmail 这样的中心化邮件服务提供商占据了电子邮件服务的绝大部分。一个被设计为去中心化的服务，最终实现却相当中心化。

市场经济可以认为是一个去中心化的经济制度。价格，生产，消费由各个市场主体博弈决定。而计划经济则是一种中心化的经济制度。国家计划委员会负责确定各类商品的价格和产量。我国逐步减少计划经济这一中心化经济制度在我国经济中的比重，到现在我国已成为了一个相当市场化的经济体，而这期间我们实现了三十多年的高速经济发展。

还有相当多的例子可以说明，中心化和去中心化并不绝对是谁优谁劣。在一些特定的场景中，中心化有其优势，在另外一些例子中去中心化有更高的效率。在更多的例子中，一个庞大的系统既有中心化的部分，又有去中心化的部分。

当我们谈起来到比特币时，我们都认为它是一个去中心化的系统。比特币确实被设计为一个去中心化的系统。但在比特币生态系统中，我们也能看到相当多的中心化子系统。

比特币交易所是进行比特币和各种货币兑换的地方，这些比特币交易所是中心化的。当我们要在比特币交易所交易我们的比特币时，我们需要将比特币发送给交易所的我们的账户上。这时，我们的比特币的控制权其实已经交给了交易所。这是因为需要由交易所撮合交易，并在交易所内部结算。中心化的设计使得交易撮合效率更高。

矿池是比特币矿工为了使挖矿收益更为稳定而结成的共同挖矿团体。现在单人挖矿已经不太可能挖出比特币了。由于全网的算力增涨很快，单个矿工挖得比特币的概率越来越低。当然，并不是没有可能，只是概率很低。这意味着单个矿工需要很长时间才能挖到比特币。

而加入矿池，可以按自己贡献的算力，从整个矿池的每份收益中分得一定比例。这样就能使收益在时间上分布更为均匀。不至于出现挖了5年才挖到一块矿的情况。这和联合买彩票是一个道理。矿池是中心化的概念。矿池内矿工的计算证明需要先提交给矿池经理，矿池收益会先打入矿池经理的比特币地址，再由矿池经理分配收益。

在实践中，中心化和去中心化并没有绝对的对和错。制度和技术上保证各种可能性，让市场自由发展，在不同的场景下会自然而然出现合适高效的的技术选择。

我们不可能要求每个电子邮件用户都架设电子邮件服务器。对于普通用户，让渡一部分隐私和忍受一些广告，换取免费便捷的邮件服务是合理的选择。但是技术上应该保证用户拥有架设自己邮件服务器的可能性。如果用户非常在意自己的隐私和安全，并愿意为隐私和安全付出代价，那么他们就可以架设自己的邮件服务器。

比特币实践中，比特币交易所、矿池这类中心化机制或者机构的出现，都是因为在某些应用场景下，效率变得更为重要。比特币用户愿意让渡一部分权力给中心机构，选择信任中心机构。而且这些中心机构也不是垄断的，用户具有选择中心机构的权力。这使得整个比特币的生态系统的运行效率更高。比特币本身设计是去中心化的，过度的中心化常常会引起比特币社区的警惕和担忧。

为什么要去中心化？去中心化的原因在于某些制度和系统的中心化趋势趋于严重，而且没有制衡和监管。人们被强迫屈服于中心化的制度设计。例如，现代金融体系是非常中心化的，而现代金融体系的部分弊端就源自其中心化的制度结构。

政fu和央妈控制了货币发行权。每次超发货币制造通货膨胀都是对社会财富的一次掠夺。通货膨胀使人们手中的财富缩水，最终受益的都是政fu，而受害的都是大众。而且这种状况的出现并非出自人们的自愿，而是政fu通过法律获得法定垄断权力。

人们的金融行为严重依赖银行。而其实人们存在银行的存款并不绝对安全。这是因为现代银行都实行部分准备金制度。人们将钱存于银行，银行并没有将钱全部安全地保存起来，而是将其中绝大部分用于放贷，银行并不承诺能兑现储户的所有取款要求。

比特币成功的最大原因是它在技术上成功实现了数字货币的去中心化。而去中心化这一特性对现代金融货币体系是有积极意义的。比特币展示了一种不为任何中心机构所控制的，无法恶意制造通货膨胀的数字货币的可能性。这种去中心化设计提供了对现代金融货币体系进行改革的技术上的可能性。