区块链技术（1）-区块链的革命性及技术概要

2018-03-29 陈皓

区块链技术（1）-区块链的革命性及技术概要
朗读人：柴巍　15′01″ | 6.88M

才开极客时间专栏的时候，就有读者留言让我发表一下对区块链技术的一些看法。只是当时觉得区块链方面的技术一方面比较简单，感觉也没什么好说的，另一方面，我觉得还有很多更主流更能帮助大家成长的技术，所以就把区块链相关的技术文章降级处理了。

那为什么现在我又要写这个主题呢？

2010 年，我在浏览国外技术网站时，看到好多人在讨论一个叫 bitcoin 的东西，还看到有人说用几万个这个东西换了个披萨。随后，我看了一下它的白皮书，这篇不到 10 页的文档读起来还是很容易的，所以建议你读一读。

然后，我在一台电脑上尝试安装了一下，就像用 BT 或电驴下载一样，连入了这个没有服务器的 P2P 网络，下载了账本，还尝试了一下＂挖矿＂。

花了不短的时间，记下了我的比特币里的一个区块，收到了来自系统奖励的 50 个比特币。我默默地看着这个又耗硬盘空间，又非常吃 CPU 的家伙，心里想，这什么破软件，太难用了，就删

除了。（是的，这 50 个比特币也就不知道去哪了。）

记得比特币开始有价值的时候，像维基解密这样的机构为了避开被政府控制的银行，会接受比特币的捐款。2012 年的时候，比特币已经看涨了，到了 2013 年，比特币的市值已经比较高了，突破了 1000 美金。

那个时候，中国有好多人在挖矿。记得最厉害的是李笑来，他的比特币持有数量很可观，如果没有卖的话，现在就更为＂恐怖＂了。

在 2016 年的时候，我听说了个叫以太坊的东西。嗯，是区块链 + 代码的东西，又被叫作智能合约，这的确给予了区块链有更多的想像空间。还听说了这个项目是被 ICO 出来的，然后我就了解了一下 ICO。同年，我有一个高中同学，搞了个创业项目，据说是中国第一个 ICO 项目。当时筹到了 1000 万人民币，然后发个币上了二级市场。

再然后，2017 年的一天有人带我去见薛蛮子。听他说他在很短的一段时间内出手投了好多个和区块链相关的创业项目。见薛蛮子一周后，中国政府出台政策定性 ICO 非法，开始治理市场，清除所有一切和 ICO 相关的东西。

似乎市场应该就此冷静下来了。

2018 年 1 月 9 日，真格基金创始人徐小平在一个微信群里对他投资公司的 CEO 们说，区块链是一场伟大的技术革命。他要求大家＂对区块链不要有怀疑，不要有迟疑，立即动员全体员工，学习如何拥抱这场革命＂。

随着徐小平这个微信截图的流出又把区块链推到了风口浪尖。我几个关系不错的做技术的朋友也跟着入坑了……各种人，认识我的，不认识我的，全都来找我，问我区块链的事，我不想关注都不成了……

所以，我想我还是在这里写上几篇文章吧。一方面，我会很客观地把区块链的技术解释出来（不是那种天马行空完全不知所云的比喻，是实实在在的技术，我保证非技术人员都一定能看得懂），包括区块链、非对称加密、挖矿、共识机制等。

另一方面，我会结合现有的一些金融上的交易撮合的中心化标准玩法来让你来比较一下中心化和去中心化的不同。最后，我会谈一些我的观点，可能会上升到哲学层面。当然，最后还是由你自己来做判断。

下面是这几篇文章要回答的关键问题。

1. 为什么区块链技术会成为热点技术？它解决了什么问题？
2. 区块链（blockchain）究竟是个什么技术？这里，我会带你抽丝剥茧看看区块链技术，看看区块链是如何做到不可篡改、什么是＂挖矿＂，以及为什么要＂挖矿＂，全是技术干货。

3. 去中心意味着没有一个公司，没有公司就意味着没有服务器，没有服务器的软件是怎样提供服务的？这里主要会讲一下无中心化的系统是怎么运作的，是怎么达成一致的？

4. 智能合约是个什么鬼？它有什么意思？

5. 简单地谈一谈金融，你可以自行思考一下，区块链虚拟货币是否有可能取代现有的金融服务？并重组整个社会架构？

6. 最后，我会提出几个逻辑问题来让你独立思考一下＂去中心化＂的优劣，以及相关的逻辑和哲学问题。

闲言少叙，我们开始。

区块链技术的革命性

你一定看过太多的文章用各式各样的比喻来讲区块链技术是什么，以及为什么牛逼。在这里，我尝试用我的话来说明一下区块链技术的革命性。

说区块链必然要谈比特币，比特币是一种数字货币。但最令人叫绝的是，比特币号称有下面几个特性。

1. 去中心化。这意味着没有中心的服务器，不受某个人的控制，整个系统直接由用户端的电脑构成。这样的技术难度是非常大的，并不像手机 App 或是小网站一样，你想发布就发布，这需要有人来跟你一起玩。

2. 数据防篡改。所有交易纪录全量保存，并公开给所有的人，而且还被加密和校验。并不是数据不能被篡改，而是，数据被篡改的成本非常的大。（有人借此说区块链的不可篡改可以解决人类的信任问题，这个并不一定。）

3. 固定的发行量。不会像国家中央银行那样乱印钞票，造成通货膨胀。

这几个东西加在一起，就可以让那些想作弊的人，尤其是那些有权有势有钱的大公司大组织很难作恶。因为＂去中心化＂这个事，从本质上来说，造就了整个系统不再需要这些个大的公司和组织，人民可以达到真正意义上的自治，这些个大公司都会倒闭。

简单说来，相信区块链的人都相信，可以通过区块链这个技术来改变整个社会的组织形成——不再需要银行、中介机构、电商平台、支付宝等中间机构，人们可以通过一个不受任何人的控制和操作的 P2P 金融系统，进行完全自由和可信的交易。

当然，反区块链的人的观点也很明确。他们认为，所谓的去中心化看似很美好，但实则不可能。而且从目前的区块链的应用来看，也没有颠覆什么，连迹象都没有。反而，大家都在疯狂地炒作概念，没有实质的价值。像 ICO 和交易所这样的东西里面充满了大量的投机主义，泡沫非常大。

于是，这种巨大无比的争议性，把人们分割成了两种阵营，把区块链推向了火热。对此，我这几篇文章会把区块链这个技术一点一点讲解清楚，让你自己判断。

其实，对于投资机构来说，在逻辑上，我觉得他们应该感到恐慌才对，因为他们也是被革命的对象啊。如果某个事不再需要公司，人们自治，那么投资人怎么投资啊？投资的实体都没了啊，怎样有回报？

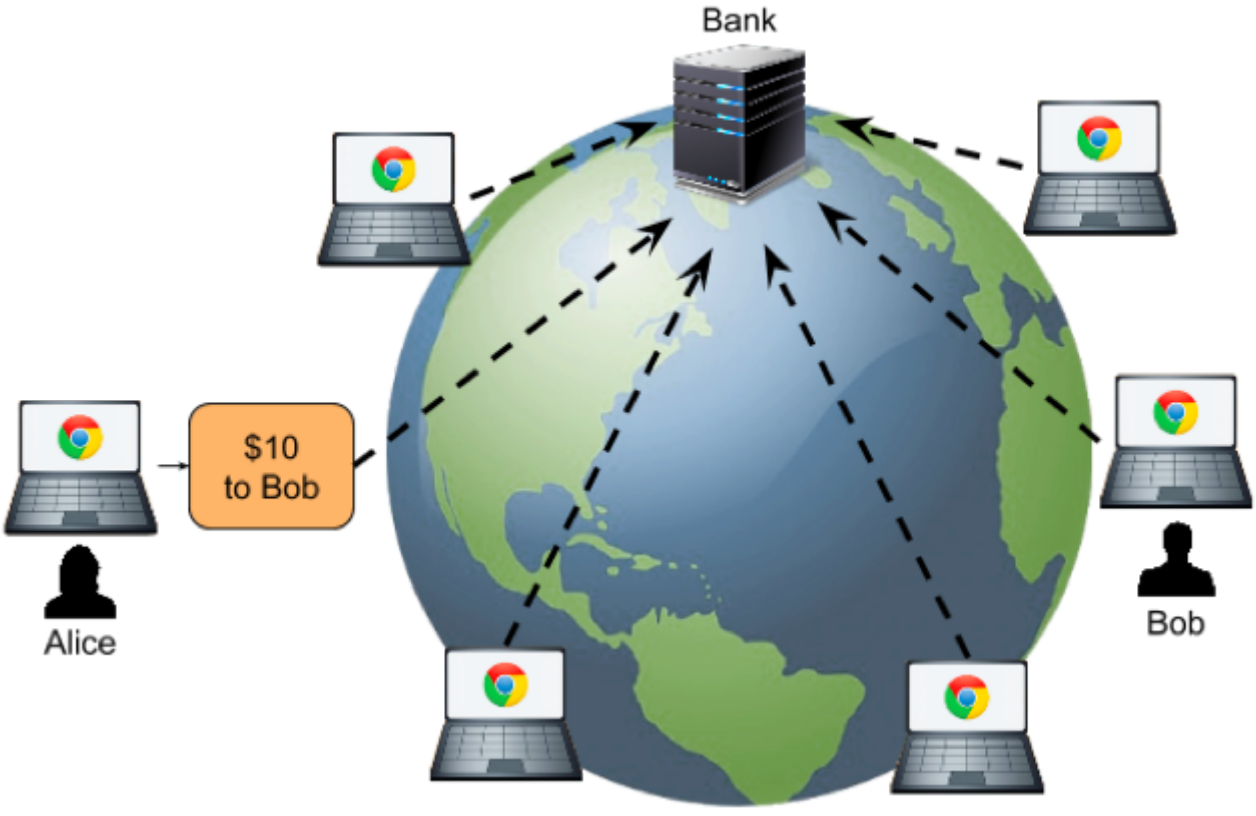
如果说，投资机构想扶植一个小公司用区块链技术把大公司干掉，那在逻辑上也说不通啊，因为如果你投资的公司也可能被别人很容易地颠覆掉，那么你怎么可能会投资呢？

相关的逻辑问题，我们会放在最后来讨论，还是先看一下区块链的技术。下面会有非常详细的技术细节，如果你不关心技术细节，那么可以只看＂技术概要＂一节。

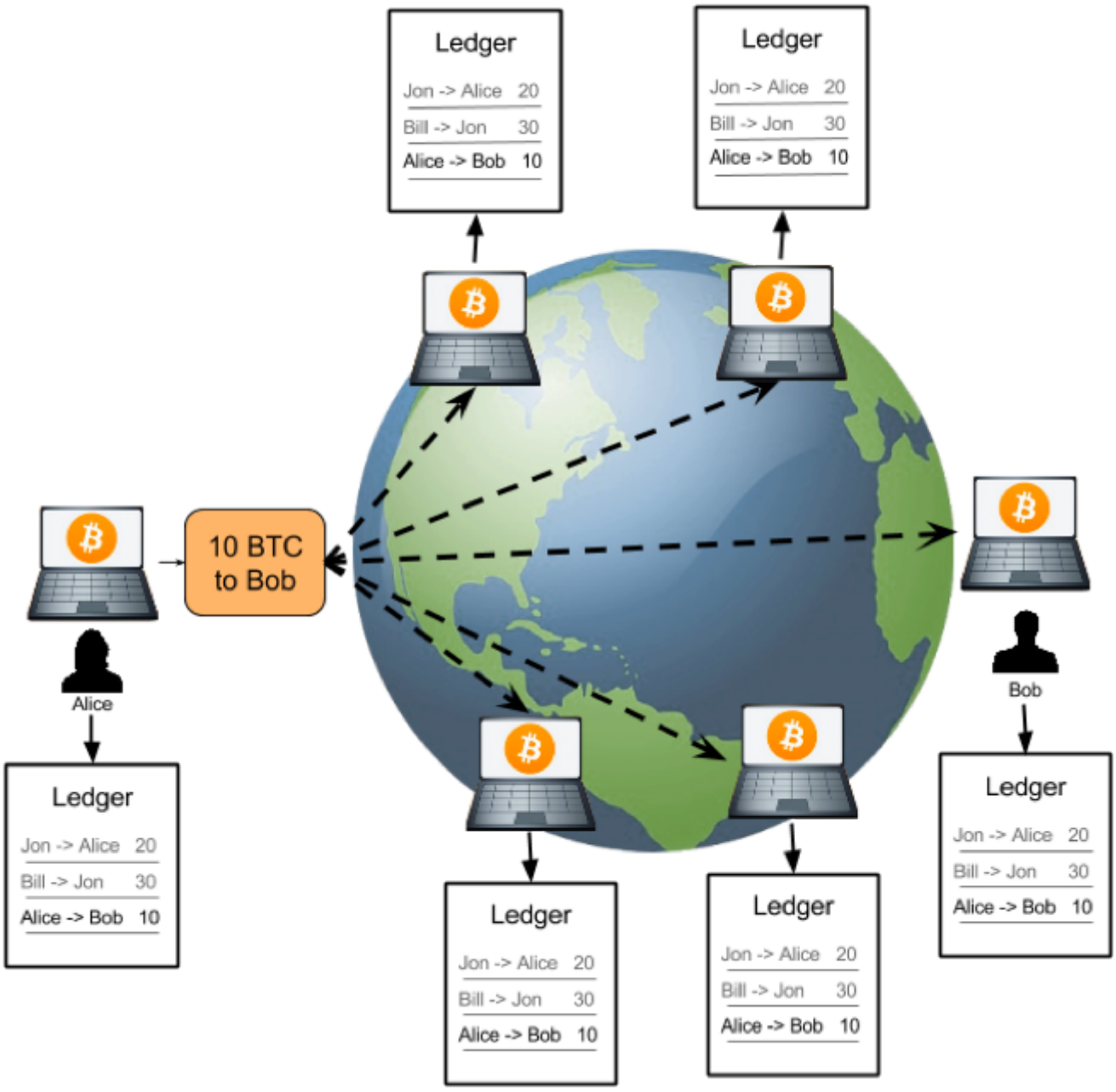
技术概要

首先，我们先看一下中心化和去中心化的业务流是什么样的。

下面的图给出了＂传统中心化＂和＂去中心化＂的对比。



中心化结构（大家都将记账权交给银行）



去中心化的交易

去中心化的比特币交易处理流程如下。

- 首先，需要交易的用户把交易传到网络中。
- 然后，网络上有些机器叫记账结点，它们通过比拼计算力的方式竞争记账权。这也叫 " 挖矿 "。
- 获得记账权的结点，会把待记账的交易进行计算打包，并向全网广播。收到新的记账包的结点会对其进行验证，验证通过后加入自己的区块。

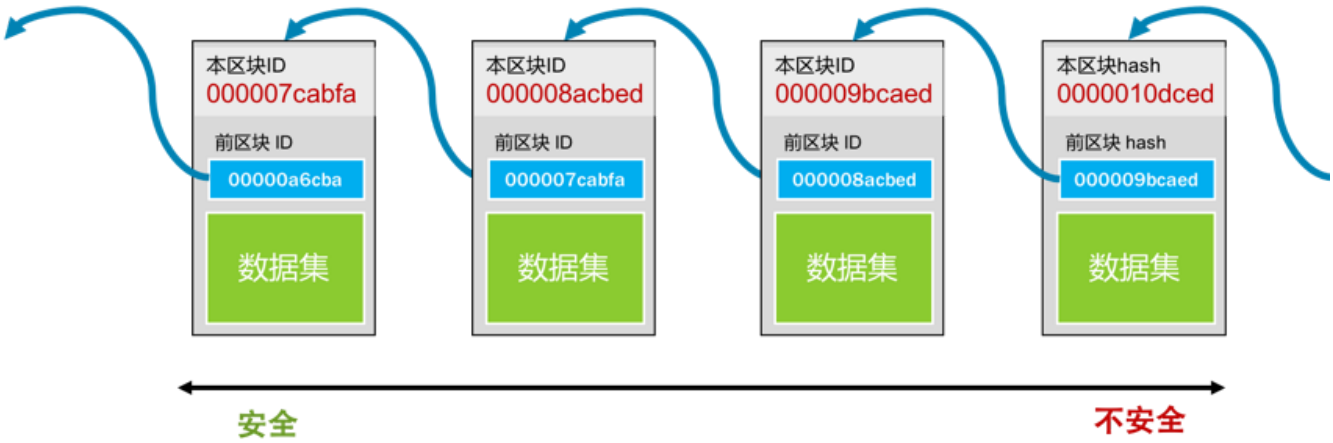
注意，整个比特币的世界是没有服务器的，其完全是靠大家用自己的电脑拼出来的一个分布式系统。既然这些电脑都是大家自己的，所以这种 P2P 的去中心化网络有一个前提假设——" 网络中的任何结点都是不能信任的，它们中的任何一个都可能会作恶 "。

基于这个前提假设，这个分布式的账本系统就需要有如下的设计：任何人都可以拿到所有的数据。所以，数据要能很容易被验证是合法的没有被修改过的，而且也要是很难被人修改的。

基于这个设计，比特币使用了两个比较大的技术：" 区块链技术 "和" 工作量证明共识机制 "。

区块链

第一个技术就是区块链，区块链又叫 blockchain，其中有一个一个的区块，每个区块中包括着一组交易信息，然后，每一个区块都会有一个 ID（或是一个地址），这些区块通过记录前一个区块的 ID 来形成一条链。文本中的图有助于你形象地理解这一概念，感兴趣可以看看。



但需要注意下面这几个方面。

- 每个块的 ID 都是通过其内容生成的，所以，只要是内容有一丁点儿的变化，这个 ID 都会完全不一样。
- 而生成 ID 的内容中还包括上一个块的 ID。于是只要上一个块的内容变了，其 ID 也要跟着变（不然就不合法了），那么后面指向这个块的 ID 也要变。于是，后面指向这个块的 ID 也要重新计算，而变成另一个，这样就会形成一个连锁效应——一个块被修改，后续的所有块都要跟着一起改。于是导致了修改成本的提升。
- 这种一处改，处处改的方式，并不代表不能篡改，而只是让修改面比较大，让你的改动麻烦一点。
- 越旧的区块的篡改会造成越大面积的修改，于是越旧的区块就不容易篡改，就越安全。反之，越新的区块就越不安全。

而真正让区块链做到非常难篡改的是工作量证明的共识机制。

工作量证明共识机制

我们知道，分布式网络的数据一致性是最难的问题了，在这种去中心化的网络集群下就更难了。其中最大的本质差别是，一个公司内的分布式系统中的结点是被假设成可信任的，而在去中心化

的网络下，结点要被假设成不可信任的。想象一下，在一堆不可信的结点上做一致性是不是一件很难的事？

这里，需要解决几个与＂数据一致性＂相关的问题。

- **以谁的数据为准？**任何结点都可以修改自己所下载的账本，也就是任何一个人都可以伪造账本。那么，谁的数据才是对的？**在去中心化的网络下，我们只能认为，大多数人认识的数据是对的。**只要我控制了一半以上的结点，那么我让这＂大多数人＂伪造同一份账本，那么相当于整个账本都被我修改过来了。**因为在没有服务器的去中心化的网络下，所谓的真理只不过是大多数人同意的东西。**

- **＂大多数人＂的问题。**是人数吗？在网络世界里，我可以用程序模拟出无穷多的＂人＂出来投票，所以，用人数来解决去中心化的问题，在分不清是人还是狗，是生物还是程序的计算机世界里，是一件很愚蠢的事。

- **意见分歧问题。**如果在同一个时刻，有多个人都在告诉其它人，这账应该这么记。比如说，有人说，左耳朵转了 10 块钱给了耗子叔，有人说，左耳朵转了 20 元给了耗子叔，还有人说，左耳朵没有花钱，是陈皓花的钱。而且，他们的数据都合法，那么，整个网络应该听谁的？

是的，这种没有人组织的玩法真是乱啊。

为了解决这几个问题，比特币使用了 Proof-of-Work 工作量证明机制，也就是＂挖矿＂。所谓的＂挖矿＂其实就是用大规模的计算来找到一个符合系统要求的区块 ID。要找到符合条件的区块 ID 只能通过暴力穷举的方式，所以要付出大量的系统计算资源和电力。

这样一来，我们用这种＂极度消耗计算力＂的方式来提高成本，从而有效地遏制或解决下面几个问题。

1. **修改几乎变得不可能。**试想，如果生成一个区块需要大量的长时间的计算力。也就是在世界上最好的电脑集群下计算 10 分钟才能打好一个包，那么，当我们要去修改数据内容的时候，这个过程也是一样的。前面说过，如果你要伪造一个块，那么你就要修改后面所有的块，修改一个块的成本如此之高，那么修改整个链的成本也就非常之高了。

2. **能掌握 51% 的算力的人也变得几乎不可能。**除了伪造一条链的成本很高，还要控制大多数人的算力，这意味着，是一个非常大的金钱的投入。这两个难度加起来，几乎不太可能。

3. **解决分歧。**一方面，这么大的工作量找出来的区块 ID，已经有效地降低了大家有意见冲突的概率。另一方面，就算是出现了合法冲突的区块（同时出现了多个合理的区块，即区块链出现分支／分叉），**也就是多个合法的账本。**而因为挖矿的成本太高，导致要同时跟进多个

账本是不可能的，所以矿工们只能赌跟其中一个。大多数人所选择的那一个分支的链就会越来越多，于是另外一边也就无人问津，从而作废了。

你别看 Proof-of-Work 成本这么高，还这么耗电不环保，但是，这是目前去中心化系统中最安全的玩法。（其中的相关细节可以查看后面的＂挖矿＂和＂去中心化的共识机制＂。）

好的，上面就是区块链的相关技术概要。如果想了解相关的技术细节，你可以继续看后面的内容。如果不感兴趣，可以选择跳过。

文末给出了《区块链技术》系列文章的目录，希望你能在这个列表里找到自己感兴趣的内容。

- 区块链技术（1）- 区块链的革命性及技术概要
- 区块链技术（2）- 区块链技术细节：哈希算法
- 区块链技术（3）- 区块链技术细节：加密和挖矿
- 区块链技术（4）- 去中心化的共识机制
- 区块链技术（5）- 智能合约
- 区块链技术（6）- 传统金融和虚拟货币

精选留言

左耳朵 55

剧透一下，别看这篇文章标题中有“革命性”的字眼，后面会反转的……😊

2018-03-29

左耳朵 52

对了，一定会有人问我当年删掉那50个比特币后悔不？

不后悔啊，因为这种快钱会让我有“错觉”，会让我错误地感觉到自己有很NB的挣钱能力，然而，自己靠的只不过是运气而已，根本不是靠实力。最糟糕的是，这种挣快钱的感觉会让我觉得其它任何工作和事业都是SB，因为相比起来，其它挣钱的方式太辛苦太慢，都不会让我再有兴趣，然后，我就会因此进入“赌徒心态”的世界，万劫不复。

（你可以认为这是我的“酸葡萄心理”吧，哈）

2018-03-29

helloworld 5

区块链里面没有什么新技术，是各种技术的组合，解决了去中心化的数据确权问题。

2018-03-30

周楷雯Kevin 4

牛逼啊

2018-03-29

iDev_周晶 4

语言一如既往的精炼 醍醐灌顶 期待后面的几篇

2018-03-29

木刀 2

从技术层面看，区块链和之前存在的IT技术之间没有显著的壁垒，简单来说是一个特殊方式加密的分布式数据库，并无革新性的进步；
但从价值观层面看，它们则有根本性的不同——以前所有的技术都旨在提高效率，区块链牺牲效率，引入激励机制和共识机制。区块链的共识，并不单单是技术上的公共账本共识，更是对区块链价值介质的共识。

2018-03-31

大雄 2

http://www.bilibili.com/video/av12465079?share_medium=android&share_source=copy_link&bbid=58AF5121-82EC-4A4E-B5D6-C2249CF325BB23666infoc&ts=1522341717868
也分享一篇bili上的比特币视频

2018-03-30

启能 2

2018-03-29

stone 1

如果为了做到数据一致性，采用bof方式穷举，那性能是如何保证实现的？

2018-03-30

大雄 1

期待与传统金融的对比

2018-03-30

i 1

悬念好多，期待耗子哥后文。

2018-03-29

阿亮 1

耗子哥终于开始讲区块链了，期待后面的反转

2018-03-29

吴天 1

很棒 正是我想要了解的 确实没理解到这种去中心分布式数据库怎么应用到实际？革命性在哪里

2018-03-29

stone 1

2018-03-29

云学 1

这个专栏买的太值了，还能学到区块链，意料之外，希望多些几篇把区块链讲透彻，谢谢

2018-03-29

darren 0

第三个问题，不会。不同的分支看到的未确认的交易集是不一样的。

分叉的以后的区块，他们上面的数据应该一样吧，

2018-05-08

徐俊 0

为什么是对区块头做两次 SHA-256 的 hash 求值？

二次hash可以避免hash字符串相同

2018-04-23

fsj 0

区块链果然是热点，第一篇的留言这么多

2018-04-16

Randy 0

有不同声音的时候，即区块链出现分叉时，所有的矿工只能选择其中一个分支（因为没人有算力可以同时发出两个不同的声音
这句没懂啊，从概率上说大家选择分叉1和分叉2的几率是一样的，会不会很长一段时间内同时存在两个区块链呢

2018-04-14

q

0

耗子叔能推荐一些不错的国外技术论坛么

2018-04-10