给大家普及普及区块链以及挖矿的知识吧（2019.1.4 已更新）

作者：imshf

原文链接：https://ld246.com/article/1545628892698

来源网站：链滴

前言

先介绍一下自己，其实我并不是搞技术的程序员大佬，而是一个区块链相关的运营。但是呢，自己又一些技术的东西比较感兴趣，所以也会自己整个博客什么的。以后有时间会给大家普及普及区块链以挖矿相关的知识，大家有什么问题也都可以提问，我也不是很精通，所以大家一起讨论。在黑客派发文章都是自己原创的，目前为止只在自己公众号和天涯区块链板块发过。

废话不多说，下面先说比特币。

比特币的自述

大家好，我叫比特币。My english name is BTC。

网上都说我是一种去中心化的数字货币，这个说法呢，其实说的没错，其实我就是去中心化的数字货。

我呢，来自.....

好吧，我也不知道自己来自哪个国家。就像我不知道我的爸爸中本聪是哪个国家的人一样。

哇~~~讲到这里就好想哭，我是个孤儿，我的爸爸妈妈不要我了。你们不要这样看我，就觉得我很可。哼哼，其实我现在可是身价破万的人呢。

自从我爸爸中本聪在2009年1月份把我创造出来之后，我的身价就一路狂飙，就像坐了火箭一样上涨从最开始的10000个我才能换2份披萨，到现在的一个我就可以换到500份披萨。可想而知，我现在是牛逼了。

可怜你们这些看我自述的凡人，是不可能懂我的。

虽然我爸爸中本聪抛弃我了，但是他找了加文叔叔来养我，我记得那时加文叔叔可是一把屎一把尿把拉扯大的呢。

加文叔叔你们不知道吗？加文·安德烈森啊。除了我爸爸中本聪，就是加文叔叔最厉害了。

我呢，可不是一个人。我有好多兄弟呢。我小的时候我爸爸告诉我，将来我最多会有2100万个兄弟呢所以你们别想着欺负我，不然我们兄弟一人一口口水都能淹死你了。

我爸爸当年创造我就是因为国家的货币数量不恒定，很容易引起通货膨胀。我就不同啦，我刚刚说了以后我们兄弟只有2100万个。永远也不会变的。

还有一个原因就是，用我来换东西，直接换就行，不用再像你们这些凡人一样通过银行，微信或者支宝这些第三方，而且交易过之后是不可逆的，所有人都是一样的交易方法，不可能出现交易过去更改本这种事情。

后来，我慢慢地长大了。一些国家和一些大的公司都支持用我来交易。因为我有很多优点。

1、**我是完全去中心化的，没有任何第三方可以控制我哦。**

2、**我既匿名又免税还免监管。光免税这点，就足够吸引很多大公司使用我了呢。**

3、**我是非常强壮的，没人能够让我消失。**

4、**用我来交易是跨国的，没有任何地区限制，非常方便。**

不能说太多的优点，不然你们会觉得我有点飘。神无完神嘛，我多少也会有点小缺点。

1、**要进行交易的话，交易平台大都是网站，安全性不高。**

2、**用我来交易的时间有点长。**

3、**价格波动挺大的，风险也高。**

4、**最后这点其实不算缺点，我的门槛比较高，原理又深奥，一般的凡人是理解不了我的存在的。**（像现在还是很多人说我是个巨大的庞氏骗局一样）

说完我的优缺点，觉得有点困了。

有空再给你们这些凡人继续说吧。

区块链的自述

信任

大家好~我是区块链。My english name is blockchain.

最近呢，我也是挺忙的。全世界到处都有我的身影。

我来自地球，但是具体哪个国家我也不知道，跟比特币那个家伙一样被抛弃了。

其实当比特币那家伙出生的时候，我也出生了。只不过大家都被他的金钱的外表诱惑了，没有及早的现我内在的好。

还没正式地跟大家介绍一下我自己。

我去网上看了下，都说这样说。说我是一个分布式的公共账本，将各个区块连成一个链条，实际上是种点对点的记账系统（一个总账本），每一个点都可以在上面记账（记录信息）。

但是我自己都被他们搞晕了，这么长的一句话怎么让你们搞懂我呀。

还是我自己来解释吧。

其实单独说概念没什么必要，因为即使说了，还是很多人云里雾里的，我这么跟大家说吧，我生来就为了解决信任问题的。

网上说的分布式，就是去中介化，那我的核心也是去中心化。

你们现在淘宝买东西，不都是以支付宝为中介来确保交易安全的嘛。那支付宝也就是一个中心。**我在里不是说支付宝的的坏话啊，就是说如果这个中心倒闭了或者出现了什么问题，那么会有多少损失。**

显著特点

为什么说要去中心化呢，因为毕竟所有的交易、数据、信息都集中在一个公司或者机构，那是多么危的一件事情。一个国家都有可能覆灭，更别说一个公司了。

接下来我说一下公共记账本，公共的意思很明显，就是所有人都可以参与记账。因为所有人都可以参记账，所以就保证了数据以及信息的公平性、真实性和不可篡改性。

打个比方，在一个100人的村子，张三买了李四家一头牛，向他支付1万元。普通的做法是，他可以告中间人村会计赵六（总记账人），将自己账下1万元转到李四账下。

但在我这里，张三无需再通过总记账人赵六，而是直接将自己账本的1万元记到李四账本；同时这笔易信息也会传到全村（即我的整个系统）。当村里其他人知道并确认了这笔交易，交易才算最终完成。

因为这笔交易被加密处理，只有李四才能收到这1万元，而其他98人只能在账户内看到有这笔交易信，但无法看到这笔信息是转给谁的。此外系统可以完整记录交易过程，整个交易可以溯源。

假如张三把这1万元误转给了王五，因为交易被加密，王五在没有密钥的情况下无法得到这笔转款。

另外，如果张三转完这1万元后又重复转给李四1万元，因为其他98人已经收到过相同信息便不会再确，这种情况下交易便不会成立。

还有一种情况，张三发起1万元转款后突然后悔，想私自把转的1万元改成100元，他需要将其他98人户内的信息都要由1万改成100元。

如果全网节点足够大，这样的修改是需要极高成本（远高于交易成本），理论上这种修改是不能实现。

这个例子说明了我的几个重要特点：**完全点对点，没有中间方；信息加密，注重隐私；交易可追溯；有节点信息统一，交易不可篡改**（修改一个节点信息，需要其他节点共同修改）。

人无完人

其实这些特点也是我的优点，也是为什么现在所有国家都在研究我的原因。甚至是有些大学里已经开了关于我的课程。

我还是低调地来总结一下我的优点吧。

第一，我是加密的，非常安全，所有的数据信息等都是任何人无法得到的。

第二，我可以用token机制来解决利益分配问题。

第三，我最大的优点就是可以解决信用问题。

第四，我的所有数据信息都是不可逆的，不可被篡改的。

当然了，世间万物，有阴必有阳，有利必有弊。所以我还是有一点不足之处的。

第一，效率问题，目前来说我所能够进行交易的效率还不是很高，不能够满足你们日常需要的场景。

第二，能耗问题，以比特币那家伙为例，要制造出一个它，需要耗费很多的电力，据数据预测，2020比特币挖矿耗电量将和全球耗电量持平。

第三，博弈问题，我虽然说是去中心化的，但是这个点淡化了国家监管的概念，可能会导致有人利用做非法的事情。

当然了，任何事物都不可能是完美的，比我的前面那些优点，这些缺点就显得不那么重要，也很期待术人员能在后期的技术发展中能将这些缺点的影响降到最低。

小结

那至于我的用处，那可就大了，从金融到游戏，从招聘到租赁，各行各业都可以与我结合起来，变得

以前更加的方便更加的安全。

你们肯定听过“互联网+”模式，就是说互联网结合一些传统的行业，这种新的模式在前几年非常火，就连大学里也在教。

那现在已经是“区块链+”模式的时代了，就是我与互联网行业或者传统行业相结合，各自发挥各自优点，让社会人民的生活过得更美好。

当然，在我的前期，竞争肯定是非常激烈的，就像互联网早期，死掉多少创业公司，才成就了现在的些大公司。

所以并不是谁先进场就能够胜利，胜利的往往都是能笑到最后的人。

区块链的起源

持续不定期更新，未完待续……