鉴于我对区块链的关注，以及很多关注我的朋友们，并不是很清楚区块链的本质和潜力点，所以今天在地铁里疏离了一下，并分享给大家。

你见过钱吗？

你见过钱吗？我相信你是没见过真正的钱的。

这是钱吗？

后来，铁又被当成了钱，然而历史总是惊人的相似，铁很快就被逐出了货币圈，成为了军事、建筑领域的新规。

但是，从原始社会到现在，中华上下五千年，朝代更替、国家分合，我们的真钱的实体一变再变。

> 迄今为止，能称为“真钱”的只有黄金。

为什么黄金成为货币圈的常青树呢？

关键的一点，以我们当下的科技水平，我们无法“无中生有”变出黄金，任何国家or组织，无法随意地产生黄金。

黄金是如何产生的？45亿年前，地球还是个大火球。宇宙中无数的小天体携带着黄金奔向了地球，地球将其融化成为“熔浆”，成为了地心。

根据估计，这些黄金总量为48亿吨。而迄今为止，47亿吨还在地核内，8600万吨在地幔里，而分布到地壳的黄金总数不到1亿吨。即便如此，我们想要从金矿中把黄金提取出来，也要花费很多力气。

如果你想获取黄金，有两种办法：

- 进入地核，从近万度高温的溶液里，将黄金熔浆捞出来。
- 在火山、地震的作用下，把黄金喷到地壳上来。不过同时，我们人类大概率会步恐龙后尘。

黄金是“真钱”，但它不容易携带，也不容易切割、交易，所以各国政府便用钞票，基于国家信任基础上的货币，让我们绝大部分人误以为“钞票就是钱”

真钱的特质

靠神明，明显是不太靠谱，所以我们还有另外一条路——靠自己。

这个自己，并不是个体的你自己，而是自己的群体，或是说群体的绝大多数。只要群体内都认可、都信任就可以成为“真钱”。

我们仔细分析一下，真钱有哪些特质？

1. 没有发行机构，发行数量不可能被操纵

用术语说，就是“完全去中心化”，它不能被任何人、组织或是国家操控。

2. 有总量

真钱的总量，不能像铁那么多，也不能像钻石那么稀少。有一个适度的量。

3. 能匿名、保存方便

不能像现在的支票一样，能追踪出使用者。我们需要隐私。

4. 容易合并、分割使用，且不容易损坏

术语就是，有很好的“健壮性”。

5. 可以交易、跨国界流通

可以流通，可以买卖，操作方便。

6. 无法造假，具有专属所有权

我的就是我的，不能莫名其妙变成你的。

以上六条，黄金满足大多数，但流通使用起来并不容易。而比特币，便是号称能达到“真钱”的所有特质。

我们来逐一对比下：

特质	比特币
去中心化	没有发行机构，只能通过大量的计算产生
有总量	数量不会超过2100万个
能匿名，保存方便	基于密码学的匿名性
健壮性	容易转移、支付
流通性	在网络部落中，都可以交易
专属所有权	基于密码学，确保只有真正的拥有者才可以交易

这是比特币。比特币最核心的技术——区块链又是什么？

官方的解释想必大多数人是看不懂的.

> 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...

即便是通俗的解释，如：

> 数据库就是一个账本，读写数据库就是记账行为，区块链就是分布式账本...

对于大多数人，是一头的雾水。下面，不会涉及到任何的数据库、密码学、算法原理及网络的知识，来说一说什么是区块链。

> 计算机并不是新颖的技术，而是现实生活的复刻。

拿我们中国传统认知里的“家谱”为原型，我们来复现一下区块链。

家谱与区块链

1. 家谱的维护，是去中心化的

你家的家谱，像户口本一样谨慎存放着。它的复刻本，在你的七大姑八大姨家，每家都有一份，而且内容完全一样。

每次有新成员加入，更新家谱时，有族长带领大家开家族会议，共同修订、补充新版本。

如果你自己偷偷修改了，是不会得到家族承认的，甚至会被给予家法处置。

2. 家谱是公开的，拥有开放性

家谱是可以完全公开的，上面记载着祖先们的光荣事迹，就像一部博物馆。

3. 同族信任的自治性

作为家族的成员，如果你在他乡遇到陌生人，发现他竟然也是你们家族的成员，你们绝对不会怀疑家谱内容的真实性，而是双双举杯欢饮达旦。

4. 信息不可篡改

如果要想改动，需要经过家族大会的同意，个人是无法改动所有复刻版的家谱的。仅用“少数服从多数”原则，就能轻松发现个人的篡改。

所以，家谱数据的稳定性和可靠性都极高。

5. 匿名性

对于改动家谱时，是谁抄上去的，并不重要。每次修改和补充的内容，是家族会议讨论的结果，到底是大街上哪位写字先生帮忙增删内容的，后人不得而知。

区块链中的每次交易，到底是谁完成的，我们也不关心。

6. 历史可追溯性

这是家谱的基本功能，你的父亲、爷爷、爷爷的父亲、爷爷的爷爷...都能在家谱上查的清楚明白。

就像区块链中，通过任意一个区块，都可以追溯到与之相关的区块，了解整个信息的演变过程。

区块链的实现

有个人叫中本聪，打算生养2100万个儿子，都叫他们比特币。

- 儿子可能会死掉：比特币被用掉或是转移；
- 儿子会有儿子，也就是孙子：通过转移获得的比特币
- 孙子也会死掉：比特币被第二次转移
- ...
- 恋爱循环了

为了避免家族混乱，中本聪建立了一个家谱。

【问题一：家族人口的数量是如何确定的？】

就像一个一元一次方程，有1个解；
二次方程，有2个解；
三次方程，有3个解；
...
找规律，N次方程，有N个解。

每个解就是一个一个儿子。理论上，这个养儿子的方程，有N个解。

【问题二：如何知道哪个是你的儿子？】

和解方程一样，求解很难，验证很简单。带入一下就ok了!

等式两边相等，就对了。

茫茫人海中，你无法知道哪个人是你的儿子，但你能很容易知道某个人是不是，去做亲子验证就可以了。

【问题三：挖矿】

现在很容易理解这个行话了。每个儿子都是“金儿子”，所以我们都抢着领养，领着就和从地壳内捞出金子一样了。

那要如何才能领养成功呢？理论上，按照预先设计的程序，大约每10分钟，允许有50个娃娃被领养，直到100年后，金娃娃们被全部领养。

【问题四：花钱买儿子】

我们没有时间和精力去领养的话，可以买别人的啊，所以儿子辈中的孙子辈就诞生了。

这个家族成员的人，有一个特质：

- 每个人死亡的同时，都会立即转世成为下一辈的成员
- 并且家族会马上修订家谱
- 并且这个人会验证家族修订家谱成功后，才会咽气

同样的，每个人在出生前，也要验证完家谱的正确性后，才开始成为新生儿。

总结

1. 比特币作为货币时，是有限制的

只能确保在比特币虚拟部落中，不会出现通货膨胀。

也就是说，还有其他的币，所以不要迷信某种特定数字货币。

2. 区块链是数字货币的核心，但绝不仅限于此

当下，区块链已在艺术、法律、保险、房地产等行业得到广泛重视，今后还将在更

多领域大放异彩。

3. 区块链，是建立一种信任，基于和神明比肩的群体信任

以上。