这些年虚拟货币太热了，区块链概念和虚拟货币经常成为人们茶余饭后的谈资。几个人一起泡茶聊天，聊得最多的除了房子大概就是炒币。和一些朋友聊天中发现，其实绝大多数人都是人云亦云，很多人甚至连区块链基础知识都没有，之所以这个概念热，还是因为虚拟货币炒币带来的暴富心理在作祟。当然、挖矿炒币现在在国内已经从政策层面直接禁止了，挖矿行为除了浪费能源之外并不能给我们的实体经济带来助力，潮水退去之时反而还会搞的一地鸡毛。但是区块链作为一种新型的技术应用，其在其他行业领域的应用价值还是有一定的研究价值，尚待各行各业的朋友们头脑风暴来深挖。本文，将采用尽量通俗的语言，来带你了解区块链，让你明白它的第一个应用场景虚拟货币是怎么回事，并同大家一起开拓思维看看各行各业潜在的区块链应用场景。

区块链，并不是一种技术，它是由几个传统技术叠加构建的新机制，它的杀伤力不在于技术线本身，而在于它对传统业态的颠覆，在金融领域甚至可以达到颠覆一个国家的威力。

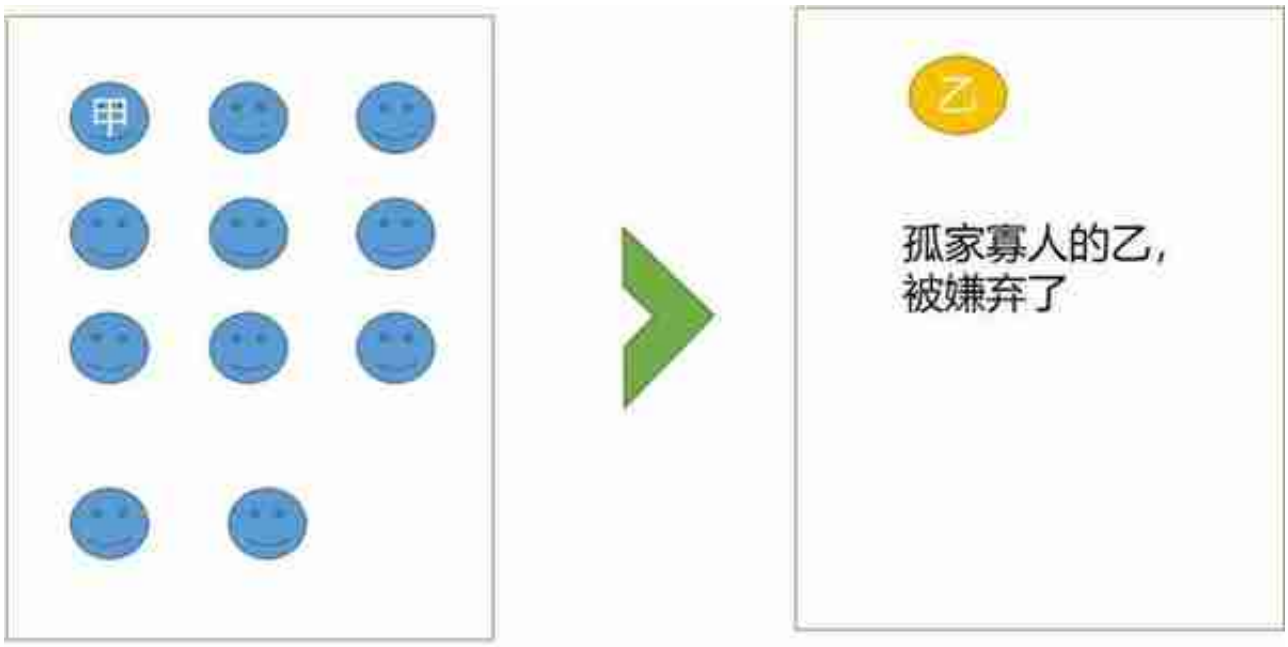
首先，我们先来看区块链的技术领域，了解区块链为什么不是新技术，而是传统技术的新架构新机制。

区块链系统也跟其他系统一样，架构上有很多层次，例如数据层、网络层、激励层、共识层
、合约层和应用层
等等分层架构，各分层是不同的技术
线负责。
区块链两大最核心特点，是防篡改和去中心化，相应的核心技术也就是密码学和p2p技术。
密码学，主要应用于区块链数据块的加密机制，负责安全部分。P2P技术，指的是点对点数据传输技术（不是前几年曾经火过一阵子的那个坑蒙拐骗大家钱财的融资平台），主要负责区块链数据的复制传播。这些技术都不是新技术，都是几十年前就有的。P2P技术在十几年前WINDOWS XP年代曾经有红火过很多软件，典型的像电驴emule、BT，还有当年的pplive、暴风影音等音视频软件，但是因为涉及音视频版权问题，很多应用都已下架。加密算法和P2P技术作为核心技术本身，在安全、服务器等很多技术领域仍然大放光彩。在区块链体系中，因为没有中心服务器集中存储数据，p2p技术就是整个体系运行的基石，来确保每一节点及时通过网络传输获取到一致的数据链，保障了整个系统的数据一致性。

下面，我们来看看区块链的数据区块组成和运行机制。

区块链数据加密的部分，主要是通过层层加密运算生成hash值二叉树来构建，这个就是区块链的数据块实现方式，下面我用插图来做一下概览，为了让大家看得懂，

这个链块的构成我做了一定简化，和实际技术实现会有一些差异，但是更容易理解。




换句话说，除非乙能够黑掉网络上一半以上的节点，也就是发生了“51%攻击”，把当时区块1的数据篡改掉，否则他想耍赖是不行的。说到这里，可能有人要问了，那如果一个人真的能够黑掉50%以上的网络节点呢，这样也不是很安全嘛。这里跟大家说实际场景中要实现的两个天大的难度，第一个在记账修改数据整个事情上，你是算力要强到抢到记账权也就是修改权；第二个就是你要实现51%攻击就要破解掉这51%节点电脑的加密私钥，而这几乎是不可能完成的；要完成以上两个难度的任务，你要付出的代价可能几十亿美元都不见得有结果。除非整个区块链网络上的51%的人跟你一起修改了数据，但是这种情况下，这个区块链本身就已经废掉了，区块链构想的原则是“网络上的人是诚实的”，如果大家都要集体犯罪，那就没有存在的必要了吧。分布式架构之所以被追捧，一个很重要的原因也是源于大家对中心节点的不信任，如果分布式节点的多数人也不可信任，那还不如回到中心权威模式。

通过以上内容，我们知道，区块链的价值所在，正是其分布式体系具有不可篡改、可追朔的安全特征。这决定了区块链数据必然是很好的信用数据，对于我们构建诚信社会是非常有帮助的。目前我们有很多的机构和个人都在区块链应用场景方面深挖，希望能贡献自己的一份力量。

题外话：有人问，既然区块链这么好，为什么要禁止挖矿和虚拟货币交易呢，这里面涉及深重的社会问题。我列举几个供大家揣摩：1、虚拟货币的挖矿行为，需要耗费大量设备和显卡以及最重要的电力资源，并没有给人民的生活带来美好，财富

都在向矿厂转移。连我们最与世无争的游戏宅男们，也都因为炒到天价的显卡买不起而享受不到游戏的乐趣。2、全球碳排放控制，不能允许这种空耗资源的行为，我们现在连工厂都拉闸限电了，更不用说对虚拟矿厂了。3、货币是以一个国家的信用为背书的，只有国家才有货币发行权，如果人人都可以搭建发行自己的一套虚拟货币，那置国家人民于何地，这是对国家对人民的财富掠夺；目前只有一些信用破产的小国以及掌控了话语权的米国才在推行各种虚拟货币，背后原因大家想想。4、社会会形成炒币氛围怪圈，整个社会风气全部为之一变，到处都是虚拟货币诈骗，到处都由实入虚，没人再安居乐业没人再共建美好家园了。