MATRIX 首席 AI 科学家邓仰东:如何用 AI 夯实区块链的底层(上篇)

邓仰东——MATRIX 首席人工智能科学家

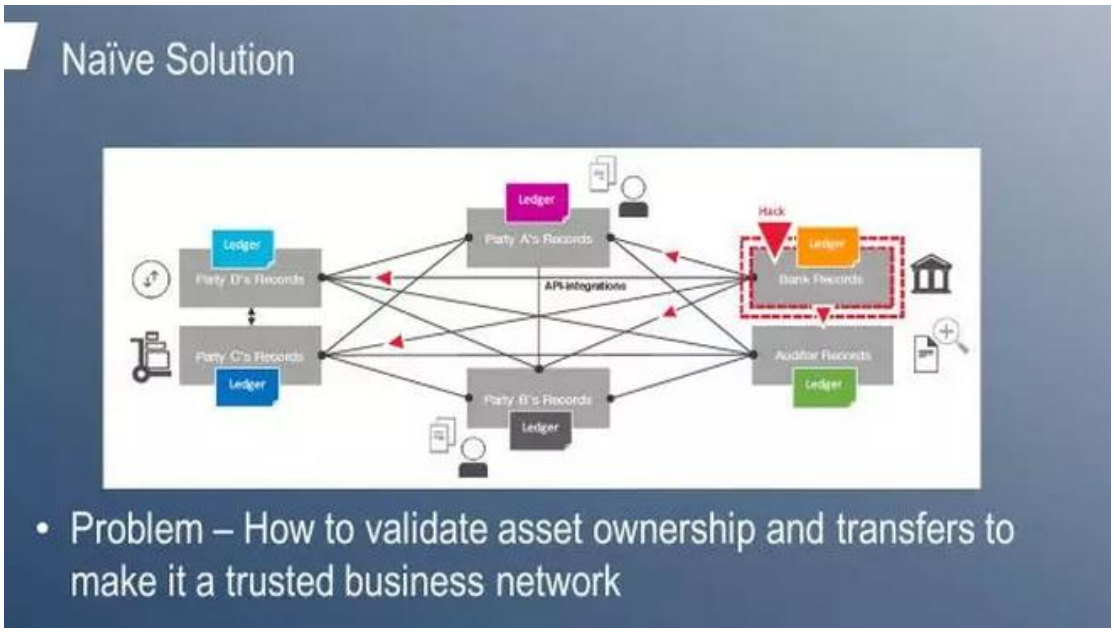
邓仰东，清华大学副教授，知名人工智能学者科学家，1995 和 1998 年在清华大学电子工程系取得学士和硕士学位，于 2006 在靠计算机及机器人专业享誉世界的卡内基 - 梅隆大学(CarnegieMellonUniversity)取得博士学位。2004 年起（博士毕业前）即已在美国 IncentiaDesignAutomation 公司担任资深工程师，2006 年 1 月加入美国 MagmaDesignAutomation 公司担任咨询级研究员，2008 年 3 月回国担任清华大学微电子学研究所副教授。现任清华大学软件学院副教授，主要研究方向为人工智能、电子设计自动化、并行算法和图形处理器架构。曾为中国高铁设计及研发了人工智能预警安全解决方案。曾带领团队在 Pascal 人工智能国际大赛上斩获第一名。邓老师将带领团队负责 MATRIX 项目中整体人工智能部分的算法设计、人工智能硬件部分的设计与研发以及下一代人工智能芯片的设计。

以一个故事开始

有一个岛在帕劳 400 公里之外一个地方，这个岛有一个特色，二十世纪他们都使用特殊的货币系统，叫石币，用石头做的钱，这个货币搬不走，有一个数值，看起来完全是自发设计的一个币，就像今天的比特币，跟那个石头某种意义上是一样的，石头有形，虚拟货币没有形。这个岛上大概三千人，所以大家的交流很快，岛上两千人都知道发生了这个事情，因此很难否认这个交易，每笔交易是不可篡改的，但是这个岛不产石头，他们要进行挖矿操作，航行 400 公里到帕劳岛上，然后把石头挖出来加工，挖完矿之后他们会用独木舟再把这个石头运过去，他们这种方式维持了很健康的很可靠的货币系统，这个故事就是说虚拟货币并不是那么虚无缥渺的事情，需要有信任就可以建立货币系统，当然里面有一些具体的机制具体怎么产生，怎么做到每笔交易的不可篡改。

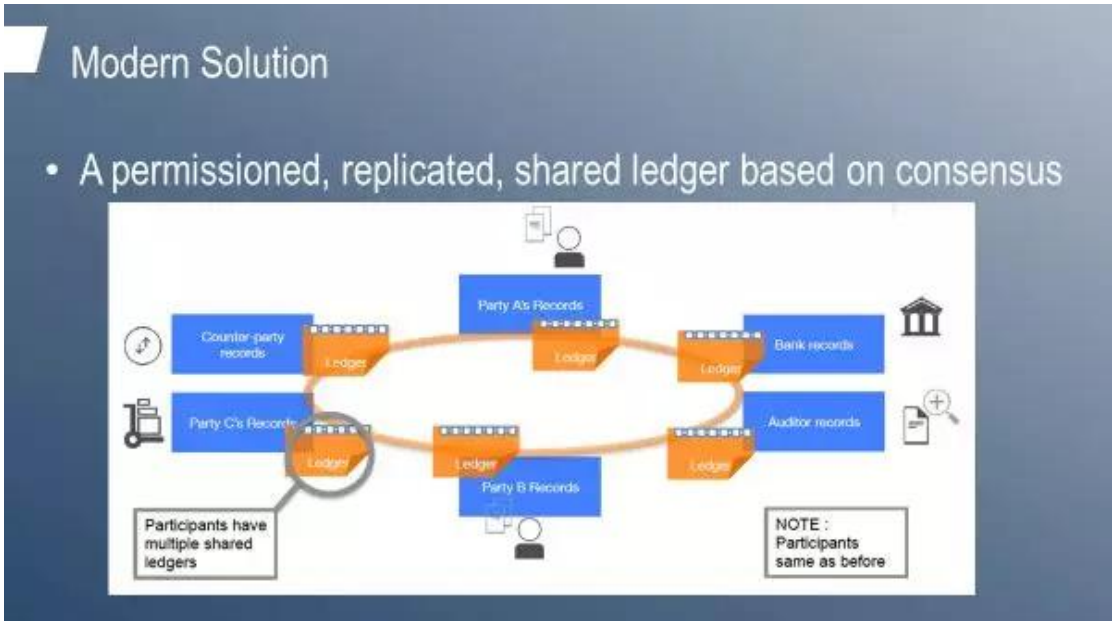
区块链的本质

区块链是什么样的东西，今天进行各种各样的商业行为，一般会在网络上进行，没有孤立进行商业行为，实际上在商业网络进行货币或者资产的转移。在进行资产转移的时候，要涉及到每次资产转移要涉及到三个要素，第一个要素是参与者，要涉及一个或者两个或者更多的参与者，资产转移过程中今天社会通常用合同界定两个人的行为，合同可以很简单。既然要有资产转移，那么涉及到账本，随便交易发生了需要记录下来，双方不能否认，账本起这个作用，说到这里基本上区块链基本要素都已经具备了，区块链就是一个分布式的账本，这个账本可以相信不容易被某些人恶意篡改，不能说绝对不可篡改，但是不容易被篡改，不容易到什么程度，基本上可以相信是不可篡改的，这个账本记录的是每个商业网络上发生各种行为，各种资产的转移的行为。



区块链是中本聪 2009 年的时候出了白皮书建立起来的，区块链是这样一个思想，还是一个一个网络，这个网络很多的节点，大家都有一个账本，分布式的账本，这些账本内容应该说是具有共识的，每笔交易通过共识方式的写到账本上，对网络上最简单的比如说必须有 51%的节点账本都是一样的，才能承认这个交易是真正发生的，比

如说有人恶意篡改账本也是可能的，但是要和 51%网络节点去共谋才能达到修改的目的，是非常困难的，通过这个方法能够达到了账本是可信的，不容易被篡改的，所以区块链就是这样的，涉及到一些共识的机制，总体来说区块链本身的引入并没有引入很多新的技术，应该是说对比较传统的技术很完美很漂亮的这样一个集成，使得这样一个机制就可以实用。

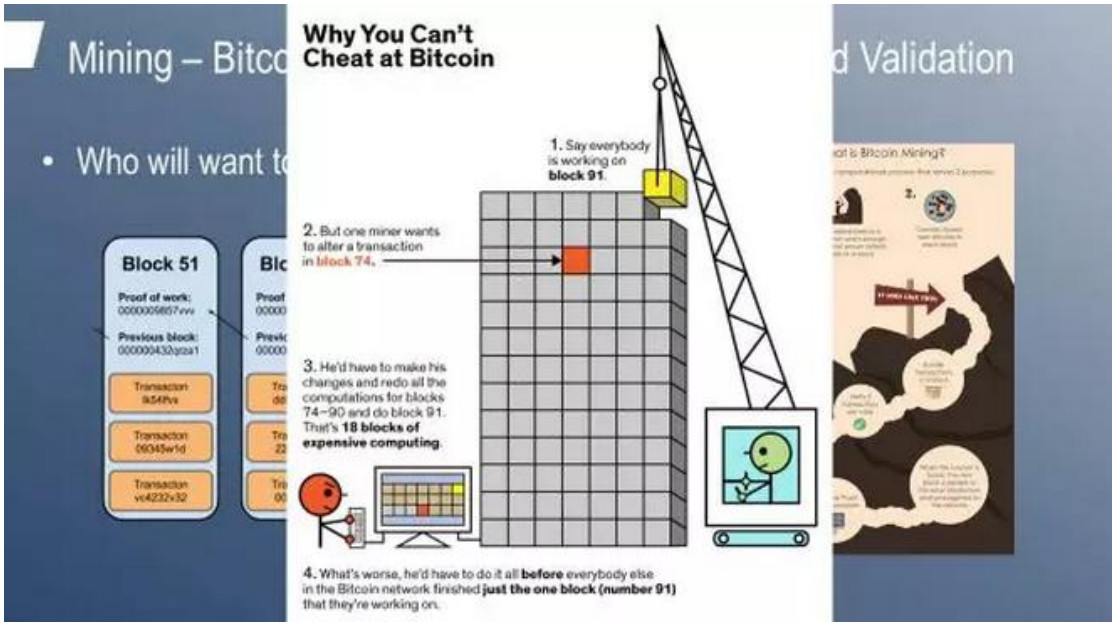


比特币，区块链第一个成功应用

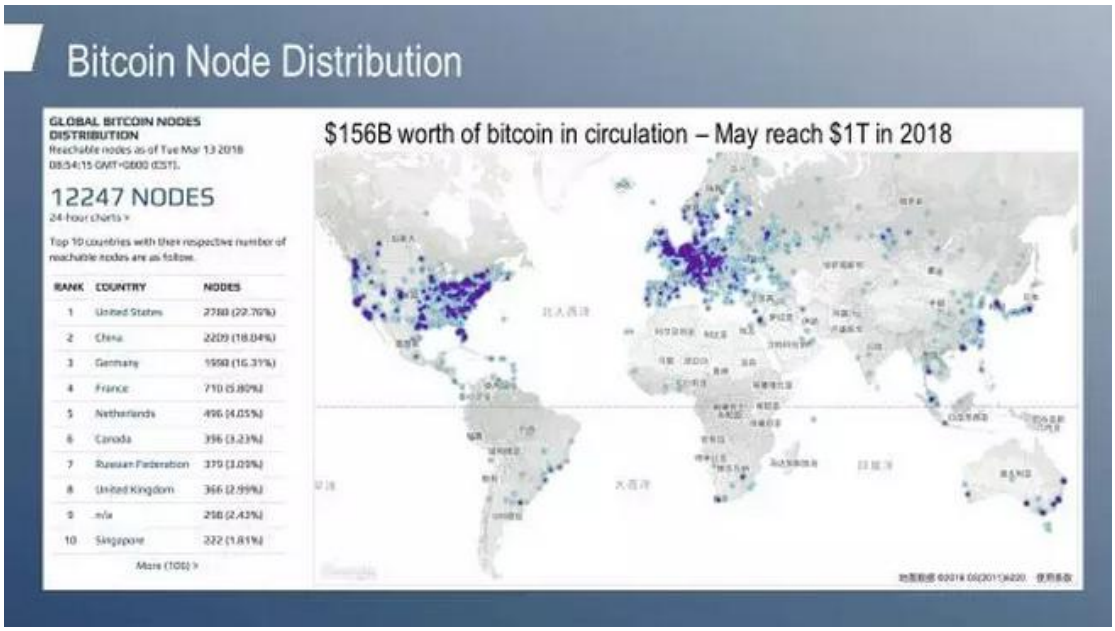
第一个区块链就是比特币网络，当时大家还没有认识到区块链还有别的功能，大家想就用区块链来维持一个虚拟货币就是比特币，实际上比特币并不等同于区块链，但是区块链是比特币的基础，比特币还有一个特点要进行挖矿的操作，挖矿是什么意思呢，大家在网络上要进行交易，之后记到账本上，有很多的交易发生了，一笔一笔打成一个列，一部分可以打成一个块，若干条这样放在块里存储下来，就是交易的链。每笔交易会同时发到网络很多节点，每个人进行验证，为什么给你验证？区块链有一个挖矿机制，每个人都可以把现在已经发生的交易打成列，可以给它一定的奖励，比如说奖励几个币，大家有意愿帮助这个活动，后来就进行挖矿操作，算哈希值，通过检查

这个哈希值很容易认证这个有没有被篡改过，记账的操作，最后还要进行挖矿，要把刚才算出来的哈希值算到预值之内，前面要变成 0，就把哈希值再哈希一次，一直迭代的哈希一直到满足这个值为止，这个时候挖矿结束了，如果同时很多人完成任务，谁打成的列最长就把这个发给谁，有点像是挖金矿，要钻一个很深的洞把金子拿出来，这个行为很像挖矿，这是挖矿的概念。

为什么要进行这样一个操作呢，实际上就是说要打成一条链之后，某人要篡改这笔交易，那么要把后面的块全部拿掉，取出这个块篡改内容才能完成篡改动作，有很多人在进行挖矿操作，要想篡改是非常困难的，是这样一个概念。



由于是 2018 年初的数据，那天的数字是全国比特币网络有（12477）个节点，不过不一定是挖矿的节点，实际会有一个程序能够接受这些交易，参与这些交易的认证工作，但是并不一定是矿工。美国有 2000 多个，中国是 2200 多个，排名第二。



智能合约

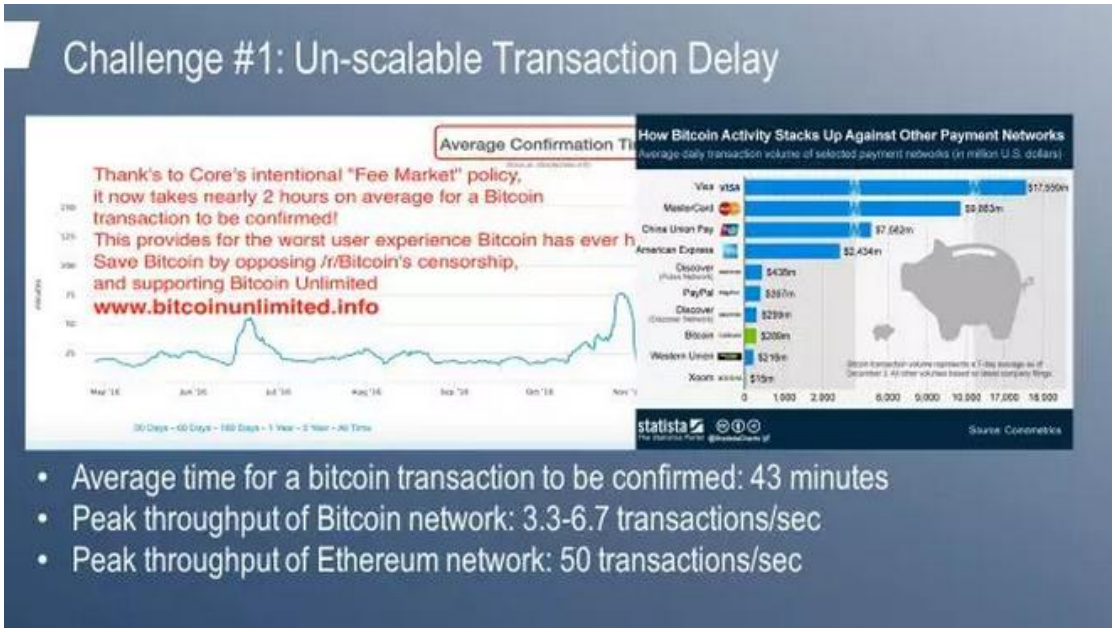
比特币没有智能合约概念，比特币只能支持两个人点对点交易，一般是一次性把资产转移发生了，交易活动中经常有复杂的商业行为，商业通过合同来界定的，所以在

2003 年又设计了第二个，即以太坊，引入了智能合约的概念，每个节点上要跑一个虚拟机，虚拟机可以执行程序，其实就是程序化的合同，界定是每次交易或者一系列交易规则性的行为叫智能合约，发生交易上传合同把合同执行起来，然后根据各种条件自动完成各种交易过程，使得复杂的商业行为在区块链完成，也是非常重要的发明，所以今天某种意义上，比特币有点像黄金，把它很多情况保值，另外一方面进行交易。

智能合约有些特性，首先有自主性，这里面两个人之间可以通过在智能合约的指导下完成非常复杂的商业行为，不需要公司、律师和其他国家的干预，第二点是可信，区块链可以交易是可信的，第三点有备份，分布式的账本，丢失了一个账本，一些记录没有关系，可以通过分布账本恢复，再就是经济，比如这里生产各种各样的产品，进行消费然后进行交易，以前通过公司转移，有经济学的一些理论，公司通过信任降低了交易成本，今天通过区块链的行为，不需要公司和管制机构可以达到可信的交易是非常重要的思想，精确界定了商业行为，想随便赖帐是很难做到的。

目前区块链存在的问题

第一个问题，交易速度比较慢，很难做到微信和支付宝那样进行交易，比特币交易时间是几十分钟这样的量级，同时能够处理的交易数也是有限的，比特币每秒完成 3.3 笔到 6.7 笔，以太坊好一些，这是过去平均交易时间变化的情况，平均交易时间越来越长，这是比特币的情况。因为它交易比较慢，同时处理的流水比较低，造成的局面像以太坊和比特币不能达到支付宝或者是微信这样的交易量。



另外一方面，对一般用户来说这是一个问题，以前在商业行为中写合同，有了智能合约以后改变了，变为写代码，你得会写智能合约程序，然后才能进行商业行为，这个对于大部分来说还是很突出的问题，父母他们很难使用智能合约进行商业行为了。

第三个问题是安全信用问题，智能合约是分布式的程序，在很大不可靠的网络上同时分布式的运行很多拷贝的程序，造成一个问题很容易受到攻击，本身和钱是有关系的，比特币或者是以太坊，很多人想对它进行攻击，本身因为分布式的环境也造成很多攻击的行为，最典型 2016 年的时候在以太坊上面，当时盗到了 6 千万美元。

智能合约安全性，这不是新的问题，只要有智能合约就有安全性的问题，这个故事是说在土耳其的西边有一个城市，在古代具有非常重要的战略地位亚洲之门，亚历山大大帝他确实先占领这个城市，从这里打到了印度，有一个圣物是一个牛车，建城得到牛车的帮助，他们绑在庙里面，用一个结，一般人很难解开，后来他们说谁能解开就可以成为这个城市的主人，这个结其实就是一个智能合约，但是另外一方面亚历山大大帝拔剑就把这个砍掉了，本身这个意义不去讨论，单独看智能合约暴力攻击面前是非常脆弱的，这个问题直到今天也没有办法解决，今天使用区块链进行交易的时候，以太坊也很容易受到攻击，攻击各种各样，代码写错了顺序，应该是付钱扣掉然后再转移，写反了，同时有很多的拷贝在运行，就把钱转到别人的账号去，一般写数据总有漏洞，这个问题很难去克服。

第四个问题是整个区块链，尤其比特币最被人诟病的就是挖矿，很多人认为就是资源的浪费整个挖矿用的电力是以这样一个指数趋势不断增长，今天大概所有比特币，挖比特币所用的电力相当于两百多个国家加起来的和比特币挖矿是一样的，所以也是一个很惊人的数字，所以很多国家对挖矿电力进行控制，这也是必须要解决的问题。