**简单谈谈究竟什么是“区块链”技术**

今年9月，13家顶级银行，包括汇丰银行、德意志银行等，已经加入了一个由金融技术公司R3领导的组织。R3公司将会利用区块链技术作为框架。宣布加入的13家银行是：花旗银行、美国银行、摩根斯坦利、德国商业银行、法国兴业银行、瑞典北欧斯安银行、纽约梅隆银行、三菱UFJ金融集团、澳大利亚国民银行、加拿大皇家银行和多伦多道明银行。由此总计22家银行加入财团。此前，另外9个银行已经签署了R3的初创协议，这代表着首次，银行之间对于如何利用区块链——支撑比特币的技术——用于金融层面达成了共识。

　　今年10月，首届全球区块链峰会“区块链—新经济蓝图”在上海举办。有来自央行金融研究所、央行征信中心、上海证券交易所、陆金所、德勤会计事务所等全球约200位包括银行、支付、证券、大宗商品等金融行业及其他对区块链技术应用前景有兴趣的行业专业人士参加。议主办方为万向区块链实验室（WanXiang Blockchain Labs），会议上还将进行区块链技术投资基金成立仪式。中国万向控股有限公司将设立一支5000万美元的专门投资有商业前景的区块链应用技术项目的基金，用于在全球范围内投资区块链商业应用相关的各类项目，包括区块链技术商业应用早期项目（天使投资，种子基金）与中后期的项目投资。

　　10月中旬，根据来自与中华人民共和国国家互联网信息办公室（Cyberspace Administration of China，CAC）的文件中再次提到了区块链技术，“虽然有人认为比特币及其区块链技术还不够稳定，但也无法忽视其对于支付带来的革命性变化。究其根源，是互联网和新技术发展带来了分布式支付清算机制的拓展，进而可能推动分布式金融交易创新。”

　　那到底什么是“区块链”技术呢，作为一个长期研究区块链的行业前沿人士，谈一下我个人的看法。

　　一、定义

**区块链（Blockchain）是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。该技术方案主要让参与系统中的任意多个节点，通过一串使用密码学方法相关联产生的数据块（block），每个数据块中包含了一定时间内的系统全部信息交流数据，并且生成数据指纹用于验证其信息的有效性和链接（chain）下一个数据库块。**

　　区块链是一种类似于NoSQL（非关系型数据库）这样的技术解决方案统称，并不是某种特定技术，能够通过很多编程语言和架构来实现区块链技术。并且实现区块链的方式种类也有很多，目前常见的包括POW（Proof of Work，工作量证明），POS（Proof of Stake，权益证明），DPOS（Delegate Proof of Stake，股份授权证明机制）等。

　　区块链的概念首次在论文《比特币：一种点对点的电子现金系统（Bitcoin: A Peer-to-Peer Electronic Cash System）》中提出，作者为自称中本聪（Satoshi Nakamoto）的个人（或团体）。因此可以把比特币看成区块链的首个在金融支付领域中的应用。

**二、特征**

　　结合定义区块链的定义，需要有这四个特征我们才能认为：**去中心化（Decentralized）**、**去信任（Trustless）**、**集体维护（Collectively maintain）**、**可靠数据库（Reliable Database）**。并且由四个特征会引申出另外2个特征：**开源（Open Source）**、**匿名性（Anonymity）**。如果一个系统不具备这些特征，将不能视其为基于区块链技术的应用。

**去中心化（Decentralized）**：整个网络没有中心化的硬件或者管理机构，任意节点之间的权利和义务都是均等的，且任一节点的损坏或者失去都会不影响整个系统的运作。因此也可以认为区块链系统具有极好的健壮性。

**去信任（Trustless）**：参与整个系统中的每个节点之间进行数据交换是无需互相信任的，整个系统的运作规则是公开透明的，所有的数据内容也是公开的，因此在系统指定的规则范围和时间范围内，节点之间是不能也无法欺骗其它节点。

**集体维护（Collectively maintain）**：系统中的数据块由整个系统中所有具有维护功能的节点来共同维护的，而这些具有维护功能的节点是任何人都可以参与的。

**可靠数据库（Reliable Database）**：整个系统将通过分数据库的形式，让每个参与节点都能获得一份完整数据库的拷贝。除非能够同时控制整个系统中超过51%的节点，否则单个节点上对数据库的修改是无效的，也无法影响其他节点上的数据内容。因此参与系统中的节点越多和计算能力越强，该系统中的数据安全性越高。

**开源（Open Source）**：由于整个系统的运作规则必须是公开透明的，所以对于程序而言，整个系统必定会是开源的。

**匿名性（Anonymity）**：由于节点和节点之间是无需互相信任的，因此节点和节点之间无需公开身份，在系统中的每个参与的节点都是匿名的。

**三、区块链意义之一 ：解决拜占庭将军问题**

**区块链解决的核心问题不是“数字货币”，而是在信息不对称、不确定的环境下，如何建立满足经济活动赖以发生、发展的“信任”生态体系。**而这个问题称之为“拜占庭将军问题”，也可称为“拜占庭容错”或者“两军问题”，这是一个分布式系统中进行信息机交互时面临的难题，即在整个网络中的任意节点都无法信任与之通信的对方时，如何能创建出共识基础来进行安全的信息交互而无需担心数据被篡改。区块链使用算法证明机制来保证整个网络的安全，借助它，整个系统中的所有节点能够在去信任的环境下自动安全的交换数据。关于解决拜占庭将军的细节问题请参见相关论文。

**四、区块链意义之二：实现跨国价值转移**

　　互联网诞生最初，最早核心解决的问题是信息制造和传输，我们可以通过互联网将信息快速生成并且复制到全世界每一个有着网络的角落，但是它尚始终不能解决价值转移和信用转移。这里所谓的价值转移是指，**在网络中每个人都能够认可和确认的方式，将某一部分价值精确的从某一个地址转移到另一个地址，而且必须确保当价值转移后，原来的地址减少了被转移的部分，而新的地址增加了所转移的价值。**这里说的价值可以是货币资产，也可以是某种实体资产或者虚拟资产（包括有价证券、金融衍生品等）。而这操作的结果必须获得所有参与方的认可，且其结果不能受到任何某一方的操纵。

　　在目前的互联网中也有各种各样的金融体系，也有许多政府银行提供或者第三方提供的支付系统，但是它还是依靠中心化的方案来解决。所谓中心化的方案，就是通过某个公司或者政府信用作为背书，将所有的价值转移计算放在一个中心服务器（集群）中，尽管所有的计算也是由程序自动完成，但是却必须信任这个中心化的人或者机构。事实上**通过中心化的信用背书来解决，也只能将信用局限在一定的机构、地区或者国家的范围之内**。由此可以看出，必须要解决的这个根本问题，那就是信用。所以价值转移的核心问题是**跨国信用共识**。

　　在如此纷繁复杂的全球体系中，要凭空建立一个全球性的信用共识体系是很难的，由于每个国家的政治、经济和文化情况不同，对于两个国家的企业和政府完全互信是几乎做不到的，这也就意味着无论是以个人抑或企业政府的信用进行背书，对于跨国之间的价值交换即使可以完成，也有着巨大的时间和经济成本。但是在漫长的人类历史中，无论每个国家的宗教、政治和文化是如何的不同，唯一能取得共识的是数学（基础科学）。因此，可以毫不夸张的说，**数学（算法）是全球文明的最大公约数，也是全球人类获得最多共识的基础**。如果我们以数学算法（程序）作为背书，所有的规则都建立一个公开透明的数学算法（程序）之上，能够让所有不同政治文化背景的人群获得共识。

**五、未来的发展**

　　互联网将使得全球之间的互动越来越紧密，伴随而来的就是巨大的信任鸿沟。目前现有的主流数据库技术架构都是私密且中心化的，在这个架构上是永远无法解决价值转移和互信问题。所以区块链技术有可能将成为下一代数据库架构。**通过去中心化技术，将能够在大数据的基础上完成数学（算法）背书、全球互信这个巨大的进步。**

　　区块链技术作为一种特定分布式存取数据技术，它通过网络中多个参与计算的节点开共同参与数据的计算和记录，并且互相验证其信息的有效性（防伪）。从这一点来，区块链技术也是一种特定的数据库技术。互联网刚刚进入大数据时代，但是从目前来看，大数据还处于非常基础的阶段。**但是当进入到区块链数据库阶段，将进入到真正的强信任背书的大数据时代。**这里面的所有数据都获得坚不可摧的质量，任何人都没有能力也没有必要去质疑。

　　也许我们现在正处在一个重大的转折点之上——**和工业革命所带来的深刻变革几乎相同的重大转折的早期阶段**。不仅仅是新技术指数级、数字化和组合式的进步与变革，更多的惊喜也许还会在我们前面。在未来的24个月里，这个星球所增长的计算机算力和记录的数据将会超过所有历史阶段的总和。在过去的24个月里，这个增值可能已经超过了1000倍。这些数字化的数据信息还在以比摩尔定律更快的速度增长。区块链技术将不仅仅应用在金融支付领域，而是将会扩展到目前所有应用范围，诸如去中心化的微博、微信、搜索、租房，甚至是打车软件都有可能会出现。因为区块链将可以**让人类无地域限制的、去信任的方式来进行大规模协作**。

　　我们这一代人将很可能会幸运地经历人类历史上两个最让人吃惊的事件，地球上的所有人和所有机器通过区块链技术以前所未有的互信展开了空前的大规模协作，其次就是基于此真正的人工智能将被创造出来。这两个时间将会深深地改变这个世界的经济发展模式。创业者、企业家、科学家以及各种各样的极客将利用这个充裕的世界去创造能让我们震惊和快乐。