李赫：从歪曲的比特币谈区块链应用及误区

原文地址：<http://www.wanbizu.com/blockchain/201701098708.html>

区块链源于IT技术，但主要应用于金融等非IT行业。由于行业的专业性和技术的复杂性在区块链应用时共存，导致出现了两个世界：一个是程序员的世界，这里的人在大肆谈论着去中心化、价值传输网络、第五范式，但是却不懂行业特点和细节，应用很难具体落地;另一个是行业人士的世界，这里的人熟悉合规处理，清楚行业流程，却被区块链的概念弄得晕头转向。本文总结了一些常见的区块链应用问题，对其加以分析，并提出一些体会和建议，希望能对区块链应用有所启发。

**一、被歪曲的比特币**

　　比特币在互联网上经常被网友称之为货币，很多人狂热地崇拜它，认为比特币的去中心化和总量限制避免了通货膨胀，是未来经济的希望，甚至呼吁央行使用比特币，那么比特币真的如网友所说的这样么?

**（一）比特币能否用于经济体系？**

　　货币是推动经济发展和社会进步的重要力量，是经济体系的血液，在信用货币制度下，流通中的货币数量要和经济总量及流通效率相匹配，否则会对经济发展产生反作用，因此货币总量要随着当前的经济情况做出适当的调整。

　　假如总量不变的比特币作为货币应用于真实的经济体系，固然不会产生通货膨胀，但是随着经济的发展，社会对货币流通总量的需求也会增长，由于比特币总量不变，就会发生社会需求大于货币供给的情况，表现为比特币的购买力会越来越高，相对于商品，就是价格的下跌，引起企业利润减少，导致员工工资下降，从而抑制消费，消费的抑制引起商品价格持续下跌，企业利润进一步减少，然后又引发新一轮的生产减少，投资下降。如此循环，经济学称之为螺旋式通货紧缩。最终结果就是：比特币如果作为货币，经济会因此而逐步停滞。

**（二）比特币是什么？**

　　既然比特币无法当作货币，那么是中本聪错了么?这里就又出现了另一个曲解：中本聪从来没有说过比特币是货币。

　　在经济学中，货币英文“Currency”，现金英文“Cash”，是完全不同的两个概念，基础货币包含准备金、现金等多种形式，现金只是货币的一部分。首先看中本聪白皮书的英文原文标题：“Bitcoin: A Peer-to-Peer Electronic Cash System”，再看最后一章的结论：“We have proposed a system for electronic transactions without relying on trust”。白皮书始终说比特币是一个电子现金系统，并且结论也明确说实现的是一个不需要信任中介的电子现金系统，全文没有使用“Currency”这个词。电子现金系统上世纪90年代就已出现，广泛应用于银行业，比如Mondex、Cybercash等系统，他们都与比特币一样实现了匿名性、密码学安全、不可重复花费等特点，不同的是比特币实现了不需要第三方信任中介的点对点交易。

**二、区块链应用特点**

　　从比特币的例子可以看出，区块链应用目前普遍存在两个问题，一是行业知识不足，二是对区块链技术产生误解和夸大，同样的问题也存在于对智能合约的理解上面。

**（一）智能合约到底是什么？**

　　智能合约又叫智能合同，在很多文章中，都有对其的描述，比如数字承诺、自动化智能、自金融、代码即法律等等，说法丰富多彩，但最后的结果是导致很多初学者对智能合约越来越迷茫。剥开智能合约的层层包装，本质上它就是一个程序，唯一不同的是这个程序运行在区块链上，你可以使用现有的程序语言比如JAVA语言编写，当然像传统IT系统一样，不同的区块链也可以自定义自己的编程语言和编译器，比如以太坊自己定义了Solidity语言作为他的智能合约编程语言。

**（二）智能合约与传统** **IT** **程序的区别**

　　为什么同样是程序，运行在区块链上的叫智能合约?因为智能合约运行时继承了区块链的特性，从而可以实现传统IT程序一些不能实现的功能，使其特性类似于纸质合同，当不同的节点运行智能合约时，就好像他们之间执行了一个可信任的合同一样，因此称之为智能合约。与传统的IT程序相比，智能合约有以下四个特点：

**A.数据透明**

　　因为区块链上所有的数据都是公开透明的，因此智能合约的数据处理也是公开透明的，运行时任何一方都可以查看其代码和数据。

**B.不可篡改**

　　因为区块链本身的所有数据不可篡改，因此部署在区块链上的智能合约代码以及运行产生的数据输出也是不可篡改的，运行智能合约的节点不必担心其他节点恶意修改代码与数据。

**C.永久运行**

　　支撑区块链网络的节点往往达到数百甚至上千，部分节点的失效并不会导致智能合约的停止，其可靠性理论上接近于永久运行，这样就保证了智能合约能像纸质合同一样每时每刻都有效。

**D.互相校验**

　　继承区块链对每笔交易都要进行全网所有节点验证的特性，智能合约如**图** **1** 所示，也是所有节点同时运行同一代码并对结果进行互相校验，只有大部分节点输出结果一致时，才将输出写入区块链中作为正式数据，因此恶意修改部分节点的智能合约运行输出并不会影响全网最终的运行结果，有效实现了数据一致性。

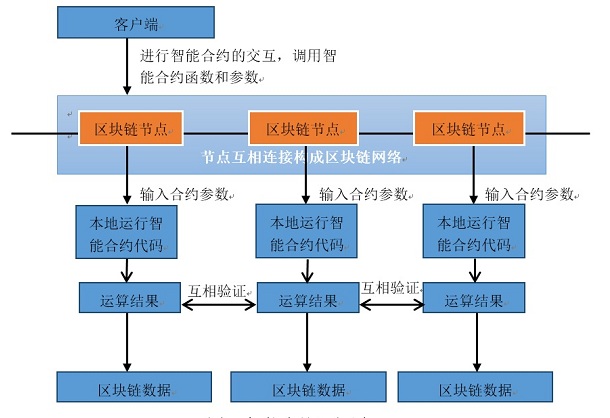


　　图1 智能合约运行原理

**（三）区块链应用注意事项**

　　根据网络常见的对区块链应用的误解，总结了以下几点应用的注意事项。

**A.区块链实现的不是性能的提升，而是业务模式的改变，相反性能大幅度下降。**

　　区块链目前所使用的都是已有的技术，通过对这些技术重新组合，以大量消耗存储资源、CPU资源和网络资源，降低整体系统性能为代价，在密码学的基础上，实现了点对点网络的可信交易，从而在业务模式中去掉信任背书的第三方，扁平化整个应用场景，实现了业务模式的创新。

**B.区块链的核心不是去中心化而是去中介化。**

　　区块链应用的目的是降低成本，优化业务流程，它只是商业活动的一种技术工具，其本质是去掉应用场景中信用背书的中介。完全去中心化不但不会促进经济发展反而会阻碍，尤其是金融业，需要一个强有力的中心进行监管，否则会导致各种违法违规行为出现，前几年P2P行业的大量集资诈骗事件就是很好的例子。同时，如果在区块链应用时没有去掉一个已存在的中介，那么这种应用场景很有可能是一个伪应用。

**C.区块链能实现的，现在有IT系统都能实现。**

　　区块链与人工智能、纳米技术等科技创新不同，**本质是现有技术的重构**，因此在区块链众多的应用场景中，现有IT系统都是已经或者可以实现的，只是成本较高，效率较低。

**D.只能实现对区块链内部自己产生的信息建立信任，对外界引入区块链的信息无法信任。**

　　外界输入区块链的信息是由人来操作的，不存在密码学基础，也无法产生信任关系。

**E.区块链应用并不一定需要代币。**

　　目前公有链的共识算法，例如POS、POW等实际上是一种经济博弈机制，因此需要代币明确经济权益。但是在企业应用中，通过使用PBFT等共识算法，由数学算法来实现各节点的共识，因此并不需要代币。

**三、区块链的应用误区实例**

　　从几个伪应用和不合规应用来看区块链应用的特点。

**（一）区块链的伪应用**

**A.使用智能合约实现保险自动理赔**

　　一些文章写到用智能合约的公开透明、不可篡改实现保险理赔的自动化处理，事实上智能合约无法实现理赔自动化，在这个应用场景中，并没有实现去中介化，智能合约只是实现了普通程序的功能，属于伪应用。保险业一直致力于保险理赔自动化的发展，一方面可以实现较好的用户体验，另一方面可以大幅节省运营成本，目前的IT系统已经能够满足技术要求，其主要的困难是存在理赔欺诈，反欺诈必须靠保险公司人工查勘。

**B.使用区块链技术保证海淘奶粉的真实性**

　　一些文章写到使用区块链创造信任的能力，保证海淘奶粉整个链条的真实可信，杜绝假货。事实上，海淘奶粉甄别假货的唯一方法是从唯一中心——奶粉生产厂商去验证，不可能实现去中心化的验证，同时海淘奶粉在销售中的流转信息，也是由人工输入到区块链上的，区块链无法保证其真实性。

**（二）区块链的不合规应用**

　　区块链在网络互助的应用是对合规性的一个挑战。**网络互助**是近年来兴起的一种新的类保险形式，通过使用区块链技术，可以大大增加信息的透明度、对称性和安全性，有效增加网络间人与人的互信。但是网络互助不符合保监会对相互保险的监管要求，因此不能自称保险。保监会对保险企业在偿付能力、资金运用、信息披露、组织形式等方面有着严格的规定和监管，从而充分保障投保客户的权益，即使保险企业倒闭，客户所持有的保单依然可以继续有效履行到合约期满。而缺乏监管的网络互助风险很大，需要面对资金池、偿付能力不足、甚至倒闭等各种问题。

**四、正确对待区块链技术**

　　Gartner是全球最大的IT行业分析和咨询服务企业之一，新兴科技技术成熟度曲线报告是Gartner的特色年度报告，旨在为企业战略师、首席创新官、研发团队负责人等提供关于技术与趋势的一种跨行业观点。2016年度新兴科技技术成熟度曲线显示，如**图** **2** ，业界对区块链的期望值已经接近顶峰，大大超过了区块链目前的实际能力，未来会有一个逐渐冷静的过程。

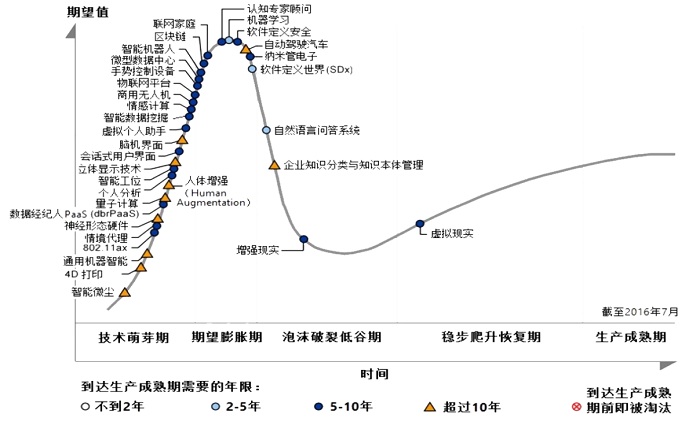


图2 Gartner2016年度新兴科技技术成熟度曲线

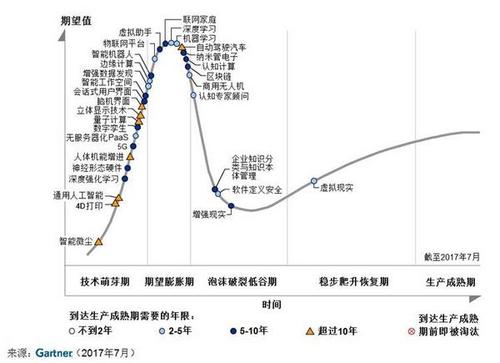


图3 Gartner2017年度新兴科技技术成熟度曲线

　　总体来说，笔者认为对待区块链可以用3个词概括：冷静、专业、坚持。

**冷静**

　　区块链技术目前处于早期阶段，还不成熟，并没有离奇到网络小说中那般神奇，更不是无所不能的全能技术。它只是一个工具，能改造部分应用场景，但我们不能去神化它，因为神话神化除了带来欺骗不会有任何好的结果。任何一种技术都有它客观存在的、不可逾越的限制，重要的是我们如何去利用好它。

**专业**

　　区块链技术的应用，不仅需要IT知识，更需要丰富的行业知识，只有深入了解行业内具体情况才能实现应用落地，没有坚实的行业知识基础的应用往往会变成伪应用或不合规应用。

**坚持**

　　虽然目前区块链还有诸多的问题，但是风险和挑战只是区块链技术走向不断成熟的垫脚石，这是任何一项新技术的必经过程，只要按照科学的方法循序渐进，区块链必然有着广阔的前景和美好的未来!