区块链： 重塑经济与世界（完整图文版）

作者：徐明星等

目录

前言

2008年，一个神秘的人物，直至今日只闻其名未见其人的“中本聪”通过一篇未在任何学术期刊上公开发表的神秘论文，把比特币带到这个世界。诞生于虚拟世界的比特币代表了人类对于数学算法的一种共识，基于这种共识机制，即使没有任何政府信用背书，比特币仍然获得了世人的认可，不论是从最初几十个比特币换取一份比萨，还是2013年12月1日，比特币的单价超越一盎司黄金的价格，比特币都在向世人展示其作为价值尺度的一面。尽管比特币价格的暴涨暴跌使其减弱了在更大范围内作为货币应用的可能，但比特币向世人展示了一种不需要中介却可以实现价值传递的可能性。这种可能性就是区块链。

正如梅兰妮·斯万（Melanie Swan）指出的那样，比特币和区块链包括三个层次的内容：区块链底层技术、协议和加密数字货币。区块链技术是点对点通信技术和加密技术的结合，基于区块链技术生成的区块链本质上是一个去中心化的分布式账本数据库；在这个数据库的基础上可以开发出数目繁多的应用，这些应用通过协议层面建立共识机制实现各种功能；最后在应用层面，客户可以实现无需中间权威仲裁的点对点的交互，当然包括比特币。有人用“组织形式上的去中心化和逻辑上实现完美一致性的技术”来形容区块链技术，也有人用“下一代全球信用认证和价值互联网的基础协议之一”来阐述区块链的特点，总体而言区块链技术的应用主要包括如下内容。

一是金融产品创新。由于金融产品基础结构的主要内容就是关于参与各方权利义务的约定，货币、债券、股权等各类金融产品都可以通过协议层建立共识机制形成与传统金融产品类别相对应的创新金融产品。由于区块链形成了可以独立存在的共识机制，因此区块链技术具有自动执行协议的功能，人们将此类协议归类为智能合约。智能合约实施的基础是共识机制而非中心化的验证，使得智能合约的执行成本降到最低、执行效率大大提升。基于智能合约运行的创新金融产品具有高透明度、高安全性、高效率的显著特征。基于上述优势，区块链技术对金融行业的改变将是颠覆性的，现有金融体系中的一些角色将不再需要，金融中介的职能也将发生深刻变化。

二是金融基础设施的变革。区块链本身就是一个数据库，基于点对点的通信技术和加密技术使数据库的组织形式更具开放性和可追溯性。在区块链技术的基础上，每个数据节点都可以参与验证账本内容的真实性和完整性，相当于通过提高系统的可追责性降低系统的信任风险。这一特性使得区块链在征信、审计、资产确权等方面具有显著的优势，从而间接提高金融体系的运行效率。

三是智能物联网。由于区块链形成了独立运行的共识机制，区块链技术可以应用于物联网的数据处理和系统维护领域。比如已经有机构提出要使用区块链技术管理上百亿个物联网设备的身份、支付和维护任务。利用区块链技术，物联网设备生产商能够极大地延长产品的生命周期和降低物联网维护的成本。

四是共享经济的技术基础。区块链去中心化的共识机制使得计算服务的应用范围大大延伸。尽管电子支付技术的发展大大降低了支付的成本，但现有支付业务模式下极小金额的支付比如低于0.01元的支付成本仍然非常高。有公司正在开发一种基于区块链的微支付技术，为每个人的电脑利用闲置计算能力从事挖矿、存储等工作提供计量工具。这种计量服务正是多种共享经济的前提，将大大拓宽共享经济的深度和广度。

综上所述，区块链技术的主要优势在于基于分布式网络形成的共识机制，分布式网络使得基于区块链的应用具有明显的开放性和可拓展性，这样会使一些商业模式的门槛可以降得很低，甚至产生全新的商业模式；共识机制的独立存在使合约的执行成本降到最低，执行效率大大提升，计算服务的范围也大大提升。

全球正在掀起一股区块链的热潮。来自学术界和科技界的各种力量投身区块链的开发和创业大潮之中，也诞生了一批非常有创新意识的创业公司，成为Fintech（金融科技）中的一股重要力量；到2015年底，已经有超过20家全球顶级的金融机构、风险基金高调宣布参与各种区块链应用开发项目。当然，我们也必须要清醒地看到，区块链技术的发展不论在国际还是在国内都尚处在早期阶段，各种技术方案和商业模式等都需要进一步地探索和实践。特别是在我国，区块链作为一个全新的概念和理论，人们的认知、研究和实践刚刚起步，要想在这一领域积累优势，引领世界，还需要足够的重视，更多的投入，需要理论研究者、网络技术者、金融从业者，以及政府监管部门的积极投入和良性互动。正是在这样的大背景下，《区块链：重构经济与世界》的出版正好填补了国内关于区块链技术特点和应用分析的空白，希望此书的出版为我国区块链技术的开发应用提供一定的参考和借鉴。

第一章
探寻区块链的源头
——“重回拜占庭”

每一个时代都有自己值得骄傲的技术，无论是晶体管、激光、互联网，还是载人航天飞机。近10年中，金融网络领域最具颠覆性、最闪耀的技术发明莫过于区块链。无论是与数字货币一道横空出世，继续发力衍生出智能合约，还是可预见的未来，不断重塑整个金融世界，都使它的夺目光芒无法掩盖。然而究其源头，我们不得不追溯到“拜占庭将军问题”和“双花问题”。后者比较简单，即如何杜绝非实体货币的再次被使用，或者是双重支付（只要引入盖时间戳的电子签名就能解决）。而前者，“拜占庭将军问题”则看起来费解且扑朔迷离，但我们又不能回避，因为它是整个区块链技术核心思想的真正根源，也直接决定了区块链技术的种种与众不同的颠覆性特质。

在某种程度上，问题比答案更重要。很难想象：如果没有“拜占庭将军问题”，没有它揭示出在人类散兵游勇的状态下，永恒的“共识”困境，那么对于这种困境的反思和探索便无法成为可能，逃离困境到达光明之地也无法成为可能。所以在我们向伟大的“答案”——区块链致以敬意之时，请不要忘记它的源头，不要忘记拜占庭。

拜占庭将军的难题

古老的“拜占庭将军问题”

让人生，让人死，让人痴迷，让人疯狂。

这就是传说中繁华与没落，绝望与救赎并存的东罗马帝国首都，拜占庭。

在2013年获得计算机科学领域最高奖项图灵奖的31年前，1972年，莱斯利·兰伯特（Leslie Lamport）搬到湾区。此时，他仍然是一个寂寂无闻的美国小伙。他充当Compass（马萨诸塞州计算机合伙人公司）西海岸计划前哨基地的先锋，不幸的是，这个分支机构最终未能落实。在长达5年的时间里，他曾是Compass总部派驻加州的唯一员工。最后，他却收到撤回东海岸的指令。于是，他决定加入斯坦福国际研究院（SRI）。在那段岁月里，SRI有一个项目，要在美国航空航天局建立容错型航电计算机系统。考虑到系统的工作性质，故障是不允许发生的。这段经历孕育了两篇旨在解决一种特殊故障的论文，由兰伯特和SRI同事马歇尔·皮斯（Marshall Pies）及罗伯特·肖斯塔克（Robert Shostak）合作完成。用计算学术语说，普通故障可能会导致信息丢失或进程停止，但系统不会遭到破坏，因为这种普通故障属于一出错就会停下来的故障类型，剩下的备份的、正常的部分照样可以运转，发挥作用。就像战场上的士兵，他们一旦受伤或阵亡就停止战斗，但并不妨碍他人继续作战。

然而一旦发生“拜占庭故障”，就会非常麻烦，因为它们不会停下来，还会继续运转，并且给出错误讯息。就像战争中有人成了叛徒，会继续假传军情，惑乱人心。当时为了解决这个问题，常常使用的技术被称为“三重模块冗余”：也就是说使用三台计算机进行万一出错的备份工作，三台独立的计算机按照少数服从多数的原则“投票”。这样，即使其中一台机器提供了错误结果，其他两台仍然会提供正确答案。但是为了证明这种方法的有效性，必须拿出证据。而在编写证据的过程中，研究人员遇到了一个问题：“错误”计算机可能给其他两台计算机发送互不相同的错误值，而后者却不会知道。这就需要使用第四台计算机来应对这个故障。

兰伯特说：“如果你使用数字签名，就可以用三台机器达成目的，因为如果‘坏了’的计算机向一台计算机发送了带签名的错误值，并向另一台发送了不同的带签名错误值，另外两台计算机就能够交换消息，以检查究竟发生了什么情况，因为两个不同的值都是签名发送的。”兰伯特还听吉姆·格雷谈论过另一个性质大体相同的问题，人们称之为“中国将军问题”。这引起了兰伯特有关司令将军和叛徒将军的联想，于是他将这个问题及其解决方案命名为“拜占庭将军问题”。

“我记得，与我的朋友怀特·迪菲（White Duffy）坐在伯克利的一间咖啡馆里，当时他描述了一个构建数字签名的问题。”兰伯特回忆说，“他说：‘如果能办到的话，会非常有用。’我说：‘这听起来并不很困难。’于是在一张餐巾纸上，我为他勾画出了第一种数字签名算法。虽然当时并不很实用，但目前已经变得切实可行。”只可惜那张餐巾纸已经消逝在时间的流沙中。在后来1982年正式出版的拜占庭将军论文的序言中，他这样写道：

“我一直觉得正是因为通过用一组围坐在圆桌旁的哲学家来表述，Dijkstra（迪克斯塔）的‘哲学家就餐问题’才变得如此让人关注（比如在理论界，它可能比‘读者/作者’问题都引人注目，尽管读者/作者问题可能更具实际意义）。我认为Reaching Agreement in the Presence of Faults（达成共识的缺陷）中所描述的问题十分重要，值得计算机科学家们去关注。‘哲学家就餐问题’使我认识到，把问题以讲故事的形式表达出来更能引起人们的关注。在分布式计算领域有一个被称作‘中国将军问题’的问题。在这个问题中，两个将军必须在进攻还是撤退上达成一致，但是相互只能通过信使传送消息，而且这个信使可能永远都无法到达。我借用了这里的将军的叫法，并把它扩展成一组将军，同时这些将军中有些是叛徒，他们需要达成一致的决定。同时我想给这些将军赋予一个国家，同时不能得罪任何读者。那时候，阿尔巴尼亚还是一个完全封闭的国家，我觉得应该不会有阿尔巴尼亚人看到这篇文章，所以最初的时候这篇论文题目实际是The Albanian Generals Problem（阿尔巴尼亚将军问题）。但是Jack Goldberg（杰克·古登博格）后来提醒我，在这个世界上除了阿尔巴尼亚之外还有很多阿尔巴尼亚移民，所以建议我换个名字。于是就想到了这一更合适的叫法——Byzantine generals（拜占庭将军）。”

写这篇论文的最主要目的是将拜占庭将军这个叫法用在这个问题上。基本的算法文章在1980年的论文中就已经出现了。

起源：拜占庭位于现在土耳其的伊斯坦布尔，是东罗马帝国的首都。由于当时拜占庭罗马帝国国土辽阔，为了防御敌人每个军队都分隔很远，将军与将军之间只能靠信差传消息。在战争时期，拜占庭军队内所有将军和副官必须达成一致共识，决定是否有赢的机会才去攻打敌人的阵营。但是，军队可能有叛徒和敌军间谍，左右将军们的决定，扰乱军队整体的秩序。在达成共识的过程中，有些信息，往往并不代表大多数人的意见。这时候，在已知有成员谋反的情况下，其余忠诚的将军在不受叛徒的影响下如何达成一致的协议，就是“拜占庭将军问题”。

两军问题：军队与军队之间分隔很远，传递信息的信差可能在途中阵亡，或因军队距离不能在得到消息后即时回复，发送方也无法确认消息确实丢失的情形，导致不可能达到一致性。在分布式计算上，试图在异步系统和不可靠的通道上达到一致性是不可能的。因此对一致性的研究一般假设信道是可靠的，或非异步系统上运行。[1]

“拜占庭将军问题”在通信领域的意义

“拜占庭将军问题”并非如传说中那样，源于公元5世纪的东罗马战场，而是产生于1982年一位美国计算机科学家的头脑当中。因此，我们不会使用任何1982年之前的案例来描述这个问题在古老年代的意义，因为再往前追溯，它并未真正、严肃地被提出并加以审视。

在原始的战争年代，将军与将军、将军与下属间只能采用原始的方式——“出行靠走，通讯靠吼”的口头传输。这对应兰伯特论文提出算法中的第一部分的口头消息算法，简称OM（m）算法。这种情形，真伪很难辨别，只有当叛徒的总数不超过将军总数的1/3，成为一个特殊的“拜占庭容错系统”时，才能在很大的消息验证代价后，实现最终的一致行动。这个结果非常令人惊讶，如果将军们只能发送口头消息，除非超过2/3的将军是忠诚的，否则该问题无解。尤其是，如果只有三个将军，其中一个是叛变者，那么此时无解。但这样的错误，这样的有意、无意的“叛徒”却可能经常出现。无论是我们把“叛变的将军”替换成以下哪种，该问题都成立。

- 一个出故障的，向其他计算机不停发出不同错误信息的服务器；
- 一份为获取暴利而做出来的金融票据；
- 一份失效的医疗纠纷合同；
- 一份含混不清的保单；
- 一个可以发出消息，做出行动的错误信息节点。

而这里，每一个错误节点可以做任意事情：不响应；发送错误信息；对不同节点发送不同决定；不同错误节点联合起来攻击其他节点等。没准会出现比这更严重、更荒谬的错误。

如果说“叛变的拜占庭将军”是我们社会中各种类型的信息节点的隐喻，那么“拜占庭将军问题”所描述的情景，这样一个进攻／撤退命令极难验证真伪的中世纪战场，则无疑是我们当今越发缺乏中心化的、难以判别信息与产生信任的社会的极度悲观的隐喻。

用算法解决难题——区块链技术的雏形

构造出一个完美的、可以解决问题的“拜占庭容错系统”是一个不小的挑战。而且构造出来以后，其是否真的有效，能否经得起时间的考验与各方的质疑，这些

都关乎着这个系统未来的命运与其创造群体的声誉。

2008年冬季，美国MIT（麻省理工学院）的密码学及密码学政策战略的邮件讨论组中，一位澳大利亚的企业家James A Donald（詹姆斯·A. 唐纳德）就对一位声称构造出了一个点对点的、不需要第三方权威认证的e-cash（电子现金）支付系统提出了质疑。而他的理由就是：对方设计的P2P系统不能够解决“拜占庭将军问题”。

在邮件中他挑剔地说道：“我们的确真的非常非常需要这个系统，但我所担忧的并不是信任的问题，而是如何获取一个全局共享的图景，借由此点而获取一致性的问题。每个人都知道X，这并不足够。我们需要让每个人都知道‘每个人都知道X’。而每个人都知道‘每个人都知道X’就是‘拜占庭将军问题’中，分布式的数据处理最难解决的问题。尤其是当X是非常庞大的数据时……”言下之意，他并不清楚或不确信这个去中心化的系统，如何解决拜占庭将军的难题。

仅仅在一天之后，他就收到了原作者的回复，一封简洁、优雅的邮件解释了在这个系统中，破解“拜占庭将军问题”的算法。[2]

“工作量证明链”（proof-of-work chain）正是我解决“拜占庭将军问题”的方案。我将在那个语境中对它进行重新表述。

一群拜占庭将军，人手一台电脑想用字符串模式匹配的方法，暴力破解国王的Wi-Fi密码，当然他们已经事先获取了组成密码的字符串的长度。一旦他们开始模拟网络发送数据包，他们必须在一个限定的时间内完成破解工作，并清除服务器和电脑上的记录，否则他们就会被发现，那就麻烦了。只有当绝大多数将军在同一时间发起攻击和破解，这样才能有足够的CPU（中央处理器）和计算能力在短时间内完成破解工作。

他们并不特别在乎什么时候开始攻击，只要他们全部同意就好。一开始的时候，大家决定这样搞：任何人觉得时机到了都可以宣布一个攻击时刻。而且，不论是什么时候，只要是第一个被听到的攻击时刻，就将被确定为官方的攻击时刻。这样的话问题又来了，因为网络传达有延迟和干扰，如果有两个将军差不多同一时间公布了两个不同的攻击时刻，那么有的人会最先听到其中一个将军发布的攻击时刻，而又有些人则会最先听到另外一个将军发布的攻击时刻。

他们使用一个“工作量证明链”来解决这个问题。当每个将军接收到任何表达形式的第一个攻击时刻时，他都会设置他的计算机来求解一个极其困难的“工作量证明”问题，对这个问题的解答是一个哈希（Hash）散列，里面也将包含着这次的攻击时刻。由于这个“工作量证明”问题，非常难解，一般而言，就算所有人收到这个问题后同时求解，也至少需要10分钟才能产生解答。一旦一个将军解出了“工作量证明”，他将会把这个算出来的“工作量证明”向整个网络进行传播，每一个接收到的人，将在他们当前正在做的“工作量证明”计算的散列中附加上刚刚被求解出来的那个工作量证明。如果任何人正在计算他收到的其他的一个不同的攻击时刻，他们将会转向新的更新后的“工作量证明”计算当中，因为他现在的“工作量证明链”更长了。

两个小时后，将有一个攻击时刻被散列在一个有12个“工作量证明”的链中。每个将军只要通过验证（这条工作链的）计算难度，就能估算出平均每小时有多少CPU算力耗费在这上面，也就会知道：这一定是在分配的时间段内，绝大多数将军的计算机共同协作才能生成的结果。如果“工作量证明链”中展示出来的算力足够强大，可以破解国王的Wi-Fi密码，那么他们就可以在一致同意的时间内安全地展开攻击。

同步、分布式数据库和一个一致的、全局性的视野的问题如何解决？“工作量证明链”就是答案。

我们可以看到这封邮件解决了下面几个问题：

（1）引入一个困难的、需要10分钟求解的工作量计算，限制了网络中每个时刻中被提出的进攻时刻数目。

（2）将所有求解出的“工作量证明”都逐一加入，形成一个越来越长的链条，一个记录着所有“参与着攻击时刻哈希计算的将军、计算的‘工作量证明’、关于‘工作量证明’的计算的总体名录”。

（3）基于这条长链得出安全的进攻时刻的答案。

最后，请各位读者注意这封解释邮件头上的内容：

日期：2008年11月14日06:56:55（GMT+8）

邮件作者的签名：Satoshi Makamoto

区块链之父——中本聪

神秘的中本聪，神秘的论文

上一节中，用“国王的Wi-Fi”解释“拜占庭将军·难题”算法的邮件作者，名叫Satoshi Makamoto，如果你对这个英文名字感到陌生，不妨看看其他几个译名：

日语翻译：中本哲史；

汉语翻译：中本聪。

比特币圈内的人一定都知道他的大名：一个匿名者、一个爱收集火车模型的天才黑客。人们关注他的理由还有很多：不仅因为他发明了比特币，还因为传言他拥有一笔类似尼伯龙根宝藏一样的海量比特币财富，以及其他诸多不为人所知的内容。然而，所有寻找中本聪的努力都以：

• 相同的方式开始（我们找到了！）；

• 相同的方式高潮（看似可靠，但并不有力的证据引发坊间的热议）；

• 相同的方式落幕（被怀疑或证明不是）。

无论是《新闻周刊》《纽约时报》，还是《连线》杂志近来出现的寻找中本聪的数次“乌龙”，让人们甚至开始计数，“这是第12次还是第13次发现‘真正’的中本聪了？”

他的最近一次露面是沉寂多年后的又一封声明：2015年12月在Linux基金会的比特币开发者群组中：

邮件标题：“Not this again.”（这次你们仍然没猜对）

正文：“I am not Craig Wright. We are all Satoshi.”（我不是克雷格·赖特，我们都是中本聪）

这次媒体炒作源于2015年12月8日，《连线》刊文认为克雷格·斯蒂文·赖特（Craig Steven Wright）即中本聪，并列举了部分掌握的“可靠”证据，包括猜测在一段可能要发言的视频中所要说的话和内容。之后数小时，澳洲警方突袭并搜查了他的家，但警方称此次搜查是和税务相关，与比特币没有联系。《卫报》援引路透社记者称，赖特的办公室也遭到了搜查。

然而这次搜查之后，中本聪的声明并没有得到开发者群体的广泛关注。事实上，自2014年9月起，就有确定的网络证据显示：部分中本聪的邮箱账户已经“有意无意”地被盗。甚至，盗取者本人对此也供认不讳，并颇为得意地提醒：中本聪先生保密工作没有做够，为安全起见请赶紧逃离，以防被抓捕。在揶揄的同时，仍然不忘记来一句Thank you for inventing Bitcoin（多谢你发明了比特币）。

下图是2014年中本聪的邮箱因长期荒废等原因被黑客盗用，从此更难有任何可信的渠道证明任何发表声明的是其本人。

图1-1　中本聪邮箱账户被盗，并用中本聪账户发表声明

资料来源：http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?id=2003008%3ATopic%3A9402&page=4#comments

这看起来似乎是一件非常滑稽的事，多么地矛盾！中本聪的密码学造诣十分精湛，许多曾经被认为是冗余设计的错误，后来都被证明是正确的。比如，精心挑选的Koblitz（科布利茨）曲线，避开了美国国家安全局在加密标准中暗藏的后门；比如，在椭圆曲线数字签名算法加密的基础上，再哈希两次，足以应付量子计算机的威胁。这粗心的与精密的居然是同一个人。

2008～2011年的网络讨论中，中本聪的一言一行也伴随着比特币概念的成型与实现，当然还有那篇著名的并未发表在任何学术期刊上的“神秘的论文”。论文的简介如下：

“本文提出了一种完全通过点对点技术实现的电子现金系统，它使得在线支付能够直接由一方发起并支付给另外一方，中间不需要通过任何的金融机构。虽然数字签名部分解决了这个问题，但是如果仍然需要第三方的支持才能防止双重支付的话，那么这种系统也就失去了存在的价值。我们在此提出一种解决方案，使现金系统在点对点的环境下运行，并防止双重支付问题。该网络通过哈希散列对全部交易加上时间戳（timestamps），将它们并入一个不断延伸的基于随机散列的工作量证明的链条作为交易记录，除非重新完成全部的工作量证明，形成的交易记录将不可更改。最长的链条不仅将作为被观察到的事件序列（sequence）的证明，而且被看作是来自CPU计算能力最大的池（pool）。只要大多数的CPU计算能力都没有打算合作起来对全网进行攻击，那么诚实的节点将会生成最长的、超过攻击者的链条。这个系统本身需要的基础设施非常少。信息尽最大努力在全网传播即可，节点（nodes）可以随时离开和重新加入网络，并将最长的工作量证明链条作为在该节点离线期间发生的交易的证明。”

2008年11月1日深夜2：10，当时的中本聪也许是怀着欣喜之情，发出了题为“Bitcoin P2P e-cash paper”（比特币P2P电子现金论文）的邮件。在邮件中他给出了含有上述见解的论文的链接，重述了比特币的五个主要特性：

（1）可以用点对点的网络解决双重支付（双花）问题；

（2）没有类似铸币厂一级的第三方的信任机构；

（3）使用者可以完全匿名；

（4）可以用哈希现金形式的“工作量证明”来制造新的货币；

（5）用于制造新货币的“工作量证明”机制同样可以用来预防双重支付。

一个伟大的社会实验从此开始！然而直到今天，世界上仍然没有人能找到他。即使加州大学洛杉矶分校金融学教授Bhagwan Chowdhry（巴格·乔杜里）已提名他为2016年诺贝尔奖经济学奖的候选人，或是瑞士小镇上的瑞信银行打出招牌：“欢迎来到达沃斯，中本聪！”

他的一生就像一个谜团，出现、闪耀、隐逸于茫茫人流。也许正如康奈尔大学教授萨若所评论的那样：重要的是中本聪的实际遗产。我们的银行基础设施已经过时了，自千年虫爆发重写代码以来就再未更新过。金融体系的透明度和可审计性极低。银行零售业自1959年以来鲜有创新，直到几年前才有所改观。即使在今天，银行依然为我们的钱提供残旧、难用的接口。我不会宣称比特币那样的虚拟货币是最终的解决方案，或者甚至是目前可靠的解决方案之一。即使最近有规划进行改进，比特币也不能扩展到世界各地，而且它在安全上面临着很大的困难。但它确实带来了一些新的技术思路，可以丰富我们的国际社会；这些思路中的一部分是中本聪发现的，另一部分是中本聪的前人发现的。负责任的媒体需要放下毫无意义的寻人工作，把精力集中在比特币这种技术和它带来的启示上。这才是真正该做出的行动。

波动的价格，轰动的交易

从横空出世到渐入佳境，从默默无闻到妇孺皆知，比特币一路走来，价格的波动也一路备受争议。在看过了无数类似《十问比特币：3年翻25000倍》这样骇人听闻的新闻标题之后，人们的心脏承受能力也越来越强。25000倍，这是事实吗？

图1-2　比特币兑换美元价格

资料来源：https://blockchain.info/zh-cn/charts/market-price?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address

比特币兑换美元价格在2014年1月达到峰值1120美元左右。一般读者显然忽略了一个基本的数学常识：如果一定要选用0作为除数，进行对比，则很容易得到一个近乎无穷大的结果。25000倍似乎也并不算离谱。我们不妨选用漫长的0值时期后非常早的一个点：中本聪依然频繁出现的2010年的某一个点，以0.0619美元作为基准，做一下计算：18093倍，依然不小。

2016年2月25日比特币的价格是424美元，虽然波动已经平缓，但相对于两年前顶峰时期的1120美元，也仅是那时的37.8%。其实从2011年第一次“比特币－比萨饼”的公开交易兑换至今，比特币兑换美元价格经历了无数次的暴涨暴跌。

表1-1　2010～2015年比特币兑换美元价格

数年间持续反复的涨跌后，大众终于接受了比特币这样的新常态，每日交易的次数也在震荡中逐步攀升，趋于27.5万笔／日（数据源于区块链网站）。

图1-3　比特币每日交易数

资料来源：https://blockchain.info/zh-cn/charts/n-transactions?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=

核心开发成员埃米尔·塔吉（Amir Taaki）的评论中引用了业界周知的Hype Cycle（炒作周期）来解释这一经济现象：“你可以说，比特币遵循了市场研究机构Gartner（高德纳）的‘炒作周期’规律，即一种理论上的技术从被采用到成熟的曲线。这个周期始于技术萌芽期，然后经历期望膨胀期、幻觉破灭谷底期、复苏期和生产力成熟期四个阶段。”根据这一理论，比特币正在走出幻觉破灭谷底期，人们开始珍视可靠的代码，抛弃人为因素和围绕这种因素的动荡。

传输价值的代币

2016年中国人民银行行长接受财新传媒的采访中罕见地对区块链和数字货币进行了表态：“从历史发展的趋势来看，货币从来都是伴随着技术进步、经济活动发展而演化的，从早期的实物货币、商品货币到后来的信用货币，都是适应人类商业社会发展的自然选择。作为上一代的货币，纸币技术含量低，从安全、成本等角度看，被新技术、新产品取代是大势所趋。特别是随着互联网的发展，全球范围内支付方式都发生了巨大的变化，数字货币发行、流通体系的建立，对于金融基础设施建设、推动经济提质增效升级，都是十分必要的。”我们不难发现，中国人民银行已经完全意识到了数字货币是新时代发展的必然，而区块链则是一种可选项。

国际货币基金组织（IMF）与各国央行撰写的《数字货币》报告中提出了一种代表绝大多数央行的典型看法。国际清算银行下属组织CPMI（支付与市场研究委员会）指出，比特币隶属于数字货币的一种，可以从以下三个维度来看待这种数字货币。

第一，它是一种资产，这一点如同其他很多货币一样，可以被用来作为支付的手段，但同时并不与一种主权货币必然相联系，没有任何实体、任何官方权威的背书（这一点与QQ币、网络虚拟币不同）。

第二，它并不具有内在固有的价值，因此它应有的价值取决于愿意接受它、使用它的人们，取决于这些人们对于它未来（可以兑换的商品、服务、货币）的信心。

第三，目前参与其中的第三方机构大都由“非银行组织”构成，这些组织在开发和维护数字货币和分布式账本技术上非常活跃。

在比特币开发和部署时需要考虑的因素中，这份报告同样提到网络效应（network effect），如同电话、手机第一次走入人们的世界，使用的人群越多，它的价值也随之越大。当越来越多的人采用比特币的时候，它的价值也会越大。而这源于它固有的优势：

（1）最初设计上考虑到了方便、全球可达、全球跨国界的使用；

（2）廉价。（各国央行也承认至少在某些交易的场合，对于用户来说，它提供了一种更加方便和廉价的方法）

在各国央行看来也有悲观的一面，它也存在着安全和信任主体缺失的缺点。但这些都不妨碍比特币作为一种传输价值的代币或传输价值的语言继续发挥作用。

然而在自由主义者眼中，比特币显然走得更远，它不仅可以被作为一种安全可靠的存储和转移法币价值的机制，更是一种互联网协议上的价值操作方法（Value over IP）。比特币以一种全新的方式取代物权法中的传统产权链，以一种可识别的安全方式保护使用者的资产利益，并提供一套透明的规则和执行机制以便所有参与者在记账上受到平等对待。所有这些比特币完成的功能都不需要依赖金融、监管或司法部门，比特币本身就是法律的代码。这一点尤其在缺乏完善的金融系统、法制失灵、无法保证公民财产权稳定的地方，体现得淋漓尽致。

使用Kipochi钱包的肯尼亚人不仅可以如愿地使用比特币的全球性金融体系，而且还可以把比特币兑换成M-Pesa以便完成当地的交易和购物。新时代里远下南洋掘金的菲律宾、马来西亚华裔可以通过OKlink将东南亚货币以低廉的手续费用转回中国大陆的家中。

在政府和私营部门已经失败的地方，开源开发已经在比特币身上找到了解决办法。我们回首它诞生的历史也会发现，比特币在2008年开始的国际金融危机中，在普遍的泡沫和对威权信任的丧失中诞生，可以说不只是比特币开发者造就了比特币，而是这个时代造就了比特币。

区块链到底是什么

比特币的传奇尚未落幕，另一个传奇就已经开启：2015年7月，高德纳发布了新一年的技术成熟度曲线图。从图中可以清晰地看到：比特币所代表的加密货币（cryptocurriencies）和虚拟货币交易（Cryptocurriencie Exchange）逐渐从2014年炒作的顶峰期跌落到大众普遍失望的谷底。

图1-4　高德纳2015年新兴技术成熟度曲线

资料来源：http://www.gartner.com/newsroom/id/3114217
中文版链接：https://www.zhihu.com/question/21314303

然而，出乎意料的是，整个产业并未衰落。截至2016年2月19日，全球比特币相关产业投资额度仍然逐渐升温，突破10亿美元。这其中以完成两轮融资的OKcoin为首的7家中国公司也格外引人注意，带领着中国区块链产业的发展。这也显示了资本与市场的整体乐观。正如中国古人所说的，“阴极阳生”。一种新的技术让投资者和业界再次看到了曙光，那就是Blockchain（区块链）。这是一个并不常见的现象。一般而言，当一项技术衰退的时候，除非它的生命周期非常长，能极大地激励人类的期待和梦想，比如人工智能，它能极大地勾起科研界、技术界的梦想。从20世纪60年代，从海曼·明斯基（Hyman Minsky）时代一直发展到今天的阿尔法狗时代。但大部分创新技术一跌下去就被淘汰了。比特币、加密货币这种技术之所以能硬挺到今天，非常重要的因素就是背后的区块链技术又再次把它拉动了起来。

表1-2　中国区块链产业投资列表（2016年2月19日更新）

比特币与区块链是父与子关系吗

对于比特币与区块链，有两种常见的错误概念，在业界广为传播：

错误观念1：比特币与区块链是父与子的关系；

错误观念2：区块链是比特币的一个意外发现和生成物，带来出乎大家所料的惊喜，之前没有人料到这一切。

事实上，作为比特币实现的底层技术，区块链的产生是伴随着比特币一道出现的，称之为父与子的关系极其不准确。其次，与其说意外，倒不如说是“蓄谋已久”。早在2010年，在后来的比特币核心开发者Gavin Anderson（盖文·安德森）的讨论帖中，中本聪就指出自己为什么在比特币初始代码版本wallet.dat中嵌入一种非常简单的脚本（Gavin发现后曾一度陷入紧张不安中）。

中本聪说：“我很多年前就已经在思考，是否可以让（比特币）支持多种交易类型，包括：托管交易、债券合同、第三方仲裁、多重签名等。如果比特币未来能够大规模发展，那么这些交易种类都将是我们未来想探索的，但是在一开始设计时就应该考虑到这些交易，这样奖励才能够实现。”

事实上，正如后来的研究者分析发现，这些结构的应用早已超出了数字货币，甚至可以扩展到任何类型的交易方式，例如各种基于智能合约的应用。其实可以套用设计中的专门术语说，“区块链”是比特币的“可供性”，这种载体提供了一种更为广阔的交互的可能性。

中本聪版本的第一版“比特币区块链”的基础协议非常简单：通过盖时间戳，各方一同记账、一同公证，每10分钟确认一次，形成记录全网这10分钟所有正确的一个账本数据库“区块”，然后每个合法的区块连成一个个链条，形成分布式的、大家一致同意的账本数据库，这就是“区块链”。

图1-5　区块链示意图

资料来源
https://camo.githubusercontent.com/e8e2a0c15c17b066e7f17056f7697819b9a1aa33/687474703a2f2f766974616c696b2e63612f6696c65732f626c6f636b5f706963747572652e706e67

区块链本质上是一个去中心化的分布式账本数据库，是比特币的底层技术，和比特币是相伴相生的关系。区块链本身其实是一串使用密码学相关联所产生的数据块，每一个数据块中包含了多次比特币网络交易有效确认的信息。

每当有加密交易产生时，网络中有强大运算能力的矿工（Miner）就开始利用算法解密验证交易，创造出新的区块来记录最新的交易。新的区块按照时间顺序线性地被补充到原有的区块链末端，这个账本就会不停地增长和延长。

通过复杂的公共钥匙和私人钥匙的设置，区块链网络将整个金融网络的所有交易的账本实时广播，实时将交易记录分发到每一个客户端，同时还能保证每个人只能对自己的财产进行修改。当然，账本里也有别人的交易记录，虽然可以看到数值和对应的交易地址（基本上这是由一段冗长的乱序字母和数字组成），但是如果不借用其他技术手段也根本无法知道交易者的真实身份。

如果从不同的技术角度来剖析，我们可以这样看待区块链：它是一种数据库、一种分布式系统，也是一种网络底层协议。

（1）数据库。区块链是一种公共数据库，它记录了网际间所有的交易信息，随时更新，让每个用户可以通过合法的手段从中读取信息，写入信息。但又有一套特殊的机制，防止以往的数据被篡改。

（2）分布式系统。区块链是一种分布式系统，它不存储放置在某一两个特定的服务器或安全节点上，而是分布式地存在于网络上所有的完整节点上，在每一个节点保留信息备份。

（3）网络底层协议。区块链是一种共识协议，基于这种协议，可以在其上开发出数目繁多的应用。这些应用在每一时刻都保存一条最长的、最具权威的、共同认可的数据记录，并遵循共同认可的机制进行无须中间权威仲裁的、直接的、点对点的交互信息。

层出不穷的其他数字货币

由于区块链最先被应用于数字货币——比特币，所以各方的开发设计者很容易想到，运用或改造这种区块链技术（加密算法、处理时间、区块大小等）可以造出新的数字货币，我们不妨称之为1.0时代。1.0时代中各种数字货币层出不穷，截至2016年2月28日，统计显示已知的有688种，从分文不值到估值上亿美元。我们简要介绍除比特币以外排名靠前的三种。

表1-3　全球排名前十位的数字货币

资料来源：http://coinmarketcap.com/