00000019不要钱

[https://xueqiu.com/5674464747/74975890](https://xueqiu.com/5674464747/74975890" \o "https://xueqiu.com/5674464747/74975890" \t "https://xueqiu.com/5674464747/_blank)

# **[转]为什么央行发行数字货币成为了一种全球性的趋势?**

Joseph T. Salerno教授在 《为什么政府讨厌现金》一文中所指出的：

我们的统治者所给出的限制现金的原因，是让社会免于恐怖分子、逃税者、洗钱者、毒品卡特尔和其他真实或想象出来的坏蛋的破坏。洪水般限制甚至禁止使用现金的实际目的，是迫使民众通过金融体系进行支付。这使得政府可以扩张自己窥视和追踪其公民最私密的财务行为的能力，以便挤干其公民的最后一元应付税款。”

[http://www.gongxiangcj.com/show-22-2063-1.html](http://www.gongxiangcj.com/show-22-2063-1.html" \o "http://www.gongxiangcj.com/show-22-2063-1.html" \t "https://xueqiu.com/5674464747/_blank)

全文

2016年1月20日，中国人民银行在其网站上公布了其召开数字货币研讨会的消息。在会上，央行要求自己的数字货币研究团队“争取早日推出央行发行的数字货币”。类似地，英格兰银行和加拿大银行等央行也正在计划或考虑发行自己的数字货币。在比特币的问世引发了私人发行、去国家化的数字货币浪潮之后，央行发行的数字货币似乎也已经成为了一种全球性的趋势。  
   
既然央行已经完全控制了货币的发行，它们为什么还要费力去开发自己的数字货币呢？  
   
好吧，这是一个有趣而又重要的问题。要回答这个问题，我们首先需要知道一些基本知识，一些数字货币101。  
   
不同于网上银行和第三方支付公司所使用的传统电子支付工具（方便传播法币的工具），数字货币是一种新技术。它是在一系列新技术的基础之上发展起来的——他们不是传输货币的工具；它们本身便是货币。其中，建立在密码学之上的数字货币也被称为加密货币。比特币就是这种这种数字货币的典范。在它横空出世之后，它又启发了许多类似的系统。一些商业银行和中央银行也开始研发自己的数字货币。根据发行者的不同，我们可以把数字货币分为三种：  
   
1、非金融机构发行的数字货币  
   
2008年11月，一个化名为中本聪的人通过发明一种名为区块链的新技术，首次设计出了一种点对点的电子现金系统，也就是比特币。2009年1月3日，中本聪完成了比特币的代码开发。由于其点对点和电子化的本质，比特币可以在两个人之间直接传递，而不需要中心化的结算机构。因此，它是一种快速、低成本、无国界的支付体系。  
   
2、商业银行发行的数字货币  
   
一些国际大型金融机构看中了数字货币低成本、快速、安全的特点，纷纷开始尝试利用其底层技术，即区块链技术，来研发它们自己的数字货币。比如，瑞银、德银、桑坦德银行和纽约梅隆银行这四家全球最大的银行就已经参与其中了。它们的数字货币类似上述的数字货币，只是其发行者有所不同。尤为值得注意的是，金融机构开发数字货币是为了满足自己快速清算交易的需求，而非通过替代央行所发行的法币来挑战金融现状。  
   
3、中央银行发行的数字货币  
   
一些中央银行，比如中国人民银行和英格兰银行，也在对数字货币进行了一番研究之后，打算推出自己的央行数字货币。在技术上，CBDC和上述两种并无二致，但由于其特殊身份，CBDC在经济上会产生更大的影响，而这也正是央行想要引入CBDC的原因。  
   
CBDC会产生至少三大影响，也就是，对政府来说，拥抱CBDC有三大原因。  
   
****创造一个去现金化的社会****  
   
政府讨厌现金，这在很大程度上就是政府希望由央行来发行数字货币的原因。  
   
对政府来说，虽然现金是其法币的原始形式，却有着一些显而易见的缺陷。与存在于金融机构里的资金相比，现金更不受政府的控制。现金一旦离开银行，就立即变得难以追踪。政府无法得知每张钞票正处于什么位置，被谁拥有，甚至不知道它是否仍然存在。这使得现金很容易被人用于贩毒、走私、逃税、洗钱甚至是资助恐怖活动。另一方面，个人所持有的现金也很容易成为窃贼或强盗的目标。  
   
更重要的是，现金会影响政府推动负利率政策的努力。当把负利率降到令人无法忍受的水平时，储户就会放弃把钱存在银行里的便利性和安全性——他们会取回自己的钱并把现金放在家里。这使得负利率政策难以实施。  
   
这也正是为什么欧洲央行决定停止发行500欧元的钞票，而前美国财长劳伦斯·萨默斯也在号召废除100美元钞票——在此之前，美国已经于1945年停止了500美元及更大面额钞票的发行。  
   
然而，只要人们还能够从银行中取出现金，不论政府如何限制现金的使用，仍然会有大量的现金游离于受政府控制的金融体系之外。这是政府不愿意看到的。但是，在一个全面使用央行电子货币的社会里，CBDC能取代传统形式的货币，并实现去现金化的目标。届时，政府将可以监控每个公民的个人账户至每一笔交易，并可以取缔所有在它们看来不合法的交易。它们也可以在出现负利率的时候阻止人们把现金取回家。人民将彻底沦为砧板上的鱼肉。正如Joseph T. Salerno教授在 《为什么政府讨厌现金》一文中所指出的：  
   
我们的统治者所给出的限制现金的原因，是让社会免于恐怖分子、逃税者、洗钱者、毒品卡特尔和其他真实或想象出来的坏蛋的破坏。洪水般限制甚至禁止使用现金的实际目的，是迫使民众通过金融体系进行支付。这使得政府可以扩张自己窥视和追踪其公民最私密的财务行为的能力，以便挤干其公民的最后一元应付税款。”  
   
****抢走比特币等私人数字货币的风头****  
   
现行的货币制度是不公正、后果严重和摇摇欲坠的，奥地利学派和其他学派的经济学家们花了很多精力来论述这一点。私人数字货币的诞生提供了一次变革货币和金融体系的改版机会。然而，各国政府也不可避免地感受到了威胁。它们嫉妒各种数字货币的风光。但碍于情面，大部分政府都不能直接宣布比特币为非法，毕竟，这有悖于它们拥护技术创新的表面立场。  
   
因此，虽然世界各国政府对数字货币的态度不一，但其区别也仅仅在于它们对比特币的拒绝程度上——没有任何一个政府在彻底地拥抱比特币。这些自大狂希望通过发行一种能被它们自己控制的数字货币，来悄悄转移掉公众对比特币的关注。  
   
结果便是，各国政府对待数字货币的立场常常十分矛盾：一方面，它们在限制比特币等数字货币的发展，另一方面，它们又在积极研究和模仿比特币开发自己的数字货币。以中国为例。2013年12月5日，“为保护社会公众的财产权益，保障人民币的法定货币地位，防范洗钱风险，维护金融稳定”，中国人民银行联合工信部、银监会、证监会和保监会，共同发布了一则通知：  
   
虽然比特币被称为“货币”，但由于其不是由货币当局发行，不具有法偿性与强制性等货币属性，并不是真正意义的货币。从性质上看，比特币应当是一种特定的虚拟商品，不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用。  
   
现阶段，各金融机构和支付机构不得以比特币为产品或服务定价，不得买卖或作为中央对手买卖比特币，不得承保与比特币相关的保险业务或将比特币纳入保险责任范围，不得直接或间接为客户提供其他与比特币相关的服务。  
   
但这绝不意味着PBoC认为数字货币是一种不好的东西，相反，在2016年的数字货币研讨会上，它们承认，实际上“……从2014年起就成立了专门的研究团队，……”，并认为“……探索央行发行数字货币具有积极的现实意义和深远的历史意义。”  
   
通过发行模仿品替换真品来偷天换日，这当然不是政府第一次这么干了。  
   
****实现对货币政策更精准的控制****  
   
央行的官员们——一帮社会工程师——对通过操纵货币政策来调控经济深信不疑。然而，每当他们的努力失败，他们便试图将其怪罪于市场。比如，他们用增加货币供应来作为一种刺激；然而，这些本应刺激实体经济的钱，却常常被“贪婪”的商人转移到金融市场，用作相反的目的。相比之下，数字货币可以帮助他们实现对货币政策更精准的控制，这不止是指它们能让“直升机上撒下来的钱”准确地飘进人们的钱包；鉴于这些数字货币是可编程的，政府甚至可以借助各种脚本来控制如何使用这些新增货币。  
   
举例来说，如果政府计划通过补贴特定农场，比如某几个玉米种植场，来扶持农业部门，他们可以直接在这些农场的账户地址里增加一笔钱，比如一亿美元，并规定这些钱只能在特定时间发送给特定化肥商，规定每家农场每年最多只能使用一千万美元，这样，他们就可以保证农场主们不会浪费这笔意外之财，并且这笔钱不会流向其他部门，比如股票市场或房地产市场。  
   
尽管这样的货币政策仍然终将失败，但在政府官员的眼里，CBDC无疑为他们提供了一种更好的工具。对他们来说，有了CBDC的帮助，他们就能更好地计划和管理经济。  
   
****结论****  
   
尽管和比特币等自由数字货币有一些相似之处，央行数字货币在本质上却和比特币所代表的东西截然相反，它有以下三个影响。（1）依靠发行央行数字货币，政府将或许能实现其建立一个去现金化社会的目标，而对大众来说，他们将要面对的财务剥削将更加严重；（2）CBDC将偷走比特币的风头并帮助政府压制数字货币革命；（3）CBDC或许会被用作一种对货币政策实现更精准控制的工具（虽然长期来看这种努力最终还是会失败）。面对这样一个即将到来的巨大威胁，自由的爱好者们应该有所警觉并尽早思考对策。（熊越/译）

[http://bastiat.mises.org/print/36483](http://bastiat.mises.org/print/36483" \o "http://bastiat.mises.org/print/36483" \t "https://xueqiu.com/5674464747/_blank)  
Joseph T. Salerno    Why Government Hates Cash

2016-09-15 21:58

自由快捷的货币意味着去中心化和高度中心化，对于后者需要有强大的有强制力的手段比如国家，有最终的暴力手段来维持信用，对于平台呢？平台的价值还剩下什么？凭什么作为中心？对于个人呢？是否参与分布式自治企业会成为新的选择？  
  
===================================================  
  
中国法定数字货币的理论依据和架构选择  
[http://iof.hexun.com/2016-09-01/185815632.html](http://iof.hexun.com/2016-09-01/185815632.html" \o "http://iof.hexun.com/2016-09-01/185815632.html" \t "https://xueqiu.com/5674464747/_blank) …  
  
  
法定数字货币会对经济和社会各个方面带来深刻影响，尤其对金融体系的影响更为深远。目前对这些影响还无法进行准确评估，但逻辑上可能出现几个结果：第一，货币结构发生变化，货币乘数增大；第二，实物货币需求持续下降，金融资产相互转换速度加快；第三，货币流通速度的可测量度有所提升，大数据分析的基础更为扎实，有利于更好地计算货币总量、分析货币结构；第四，降低KYC与AML成本，提高监管效率；第五，提供高效的共享金融环境，驱动金融创新。  
  
　　法定数字货币对金融体系还可能带来另一个重要变化，即更易引发金融脱媒，影响货币创造。由于数字货币使存款（M2-M0）向现金（M0）的转化变得十分便捷，金融恐慌和金融风险一旦产生也会加速传染，加剧对金融稳定和金融安全的破坏性。鉴于此，特定条件下必须设置适当机制加以限制。  
  
===================================================  
  
人民银行对数字货币的集中表态释放强烈信息  
  
[http://mp.weixin.qq.com/s?\_\_biz=MjM5MjkwMTc4Nw==&mid=2651451632&idx=2&sn=8652056fd5ca58c67003b117e7ba9616&scene=0#](http://mp.weixin.qq.com/s?__biz=MjM5MjkwMTc4Nw==&mid=2651451632&idx=2&sn=8652056fd5ca58c67003b117e7ba9616&scene=0" \o "http://mp.weixin.qq.com/s?__biz=MjM5MjkwMTc4Nw==&mid=2651451632&idx=2&sn=8652056fd5ca58c67003b117e7ba9616&scene=0#" \t "https://xueqiu.com/5674464747/_blank) wechat\_redirect …  
  
值得注意的是，《架构选择》一文直面了所谓“法定数字货币的运行框架”，这在《央行观察》此前的一系列文章中都有涉及，包括《人行对数字货币的态度为何变化》、《如果存准机构扩围，货币信贷将会怎样》等文章，都探讨了《架构选择》提到的第一种模式，也就是中央银行直接面向公众发行数字货币。  
  
这里面最重要的问题乃是利息。金属货币和纸币都没有利息，但银行存款有利息，这也再一次表明了银行存款本身不是法定货币，而只是一种用法定货币表明金额的随时可兑换等额法定货币的债权。在纸币时代，由于央行发行纸币之后就和纸币使用者失去了联系（来自前面提到的分布式支付结算的架构），因此央行也无从给纸币使用者发放利息。  
  
数字货币一旦付息，银行存款的根基其实就被动摇了，现在的银行间市场也就扩展到了整个社会，目前纸币只是M2一小部分的状况将要改变。不过，《架构选择》一文并没有涉及到这个问题，但人行表示自己也只是“倾向”于第二种模式，也就是维护银行存款目前的地位，这说明这方面的讨论目前大概还没有定论。毕竟，直接对数字货币付息，将大大扩展货币政策的能力，对于央行的诱惑是巨大的。

2016-09-15 22:03

DAC，全称是Distributed Autonomous Corporation，中文可以翻译为分布式自治系统。所谓DAC，就是通过一系列公开公正的规则，可以在无人干预和管理的情况下自主运行的组织系统。  
  
DAC的形态非常多，它可能是某种数字货币，也可能是一个系统或者实体机构，甚至可能是无人驾驶的汽车。作为企业，它们为客户提供有价值的服务，这种服务可以是货币传输(如比特币)、资产交易、域名服务，或者其他任意一种商业模式。  
  
以下是分布式系统的四个突出特点，活系统的特质正是由此而来：  
◆没有强制性的中心控制。  
◆次级单位具有自治的特质。  
◆次级单位之间彼此高度连接。  
◆点对点间的影响通过网络形成了非线性因果关系。  
  
   
  
  
=============================================曲双石：区块链助力企业分布式自治[http://www.ifc1000.org/2016/zch\_0620/593.html](http://www.ifc1000.org/2016/zch_0620/593.html" \o "http://www.ifc1000.org/2016/zch_0620/593.html" \t "https://xueqiu.com/5674464747/_blank)  
  
分布式自治公司不再需要依赖运营团队和技术人员的维护，而是通过设置公正公开的管理制度和运营规则，实现无人干预无人管理的自主运营。在这样分布式自治公司中，每一位员工都是参与者、贡献者，同时又是运营者、管理者，并且来去自由。任何关键人员的流失都不会对分布式自治公司造成重大影响，仍然可以平稳安全的运营。建立在分布式自治运营系统上的人力资源管理不再需要繁琐冗长的入职和离职流程……  
   
近期，区块链技术与应用引起业内广泛关注与探讨，形成一股“区块链”热潮，区块链技术究竟有哪些应用？今天早餐会深圳前海瀚德互联网金融研究院执行院长、深圳瀚德创客金融投资有限公司研究部总经理曲双石先生针对区块链在公司管理方面的应用与前景作出了深度解析。  
   
****【嘉宾简介】****  
   
****曲双石  
  
深圳前海瀚德互联网金融研究院执行院长，深圳瀚德创客金融投资有限公司研究部总经理。现中国人民大学金融学博士在读，中国人民大学国际货币研究所研究员、互联网金融研究室副主任。参与多项国家部委重大课题，撰写研究报告、发表财经评论文章及学术文章数十篇，参与编著《财政危机下的金融困局与突破》、《后金融危机时代全球国币治理的坚守与革新》。****  
   
****区块链技术蕴含的巨大能量****  
  
区块链是比特币的底层技术，是一种通过去中心化和去信任的方式让所有参与者共同维护数据库可靠性的技术方案，是一串使用加密算法生成的数据区块。区块链因为其公开透明、去中心化、去信任和不可篡改等特点，得到了银行、金融业和广泛创新领域的爆发式关注，包括花旗，摩根大通在内的众多国际巨头企业都纷纷建立了实验室研究如何在区块链上建立统一的金融生态。  
在金融业以外，区块链的应用领域也已经延伸至了公证、医疗、权益证明、共享经济、智能合约和物联网等诸多领域。区块链技术即将改变人类社会和全球经济的方方面面。  
   
****“自审计”时代****  
  
也许，若干年后，随着商业生态圈从接触，改变，到利用区块链重塑生态圈，可以实现从发起交易，到贸易复核，再到贸易确认等一系列会计入账行为的真实性，实时性，和不可逆性。股东、银行、监管机构或其他利益相关者，可以实时监控公司账本，从而减少欺诈和假账。  
  
由区块链赋予的分布式会计责任特性，使提交真实、合法、完整会计资料的责任被直接分配至整个网络所有参与员工共同行使，使传统会计模型中的第三方机构检查系统不再那么重要。企业利用区块链财务系统就完全可以自己证明会计资料的可靠性和交易的完整性。从本质上讲，区块链可以满足股东等利益相关者对于审计的公正性，有效性和准确性等所有需求，还可以弥补第三方审计在独立性、公正性、透明性和客观性方面的不足。  
   
换句话说，未来的企业也许不再需要会计师事务所的第三方审计服务，可以实现更透明，更安全，信息更真实的‘自审计’！到那时，类似安然事件的公司破产丑闻将会真正成为历史！  
   
****从自动化审计到公司管理自治****  
  
从自动化审计的实现，我们可以联想到公司管理自动化的可能。DAC（Distributed Autonomous Corporation），分布式自治系统理论，恰恰支持了这一设想。  
   
从19世纪人类创造了企业开始，过去的几个世纪中，企业发展成为了人类文明的主力，支撑了世界经济和科技文明的飞速发展，很多企业甚至富可敌国。而如今随着区块链和分布式系统的发明，企业的定义正在悄悄产生转变，贸易链流程、认证、财务系统，越来越多可以基于区块链智能合约执行的转变即将发生，这些转变可以大大减少运营摩擦，使企业交易变得更加透明和值得信赖。无单一领导模式的分布式自治公司将会被孕育，公司将一系列管理规章制度编码在区块链上，就可以实现自主运营，管理模式被离散，会计责任被分化，公司决策100%透明。  
   
****分布式自治公司会是什么样的？****  
   
分布式自治公司颠覆了人们对于传统公司的理解和想象，这样的公司是高度自治化的。分布式自治公司不再需要依赖运营团队和技术人员的维护，而是通过设置公正公开的管理制度和运营规则，就可以实现无人干预无人管理的自主运营。公司每一位参与其中的员工就好像比特币中的旷工，通过自发参与，从自身利益角度促进公司发展，同时又保障了公司的顺利运行。这样的自治管理系统使所有员工可以在去信任的环境中高效安全无摩擦的交换数据，人为的干预并不会起任何作用。  
   
在这样分布式自治公司中，每一位员工都是参与者、贡献者，同时又是运营者、管理者，并且来去自由。任何关键人员的流失都不会对分布式自治公司造成重大影响，仍然可以平稳安全的运营。建立在分布式自治运营系统上的人力资源管理不再需要繁琐冗长的入职和离职流程，区块链的共识机制使员工无需再提供任何证明和证书认证，审核流程也得以缩短。雇员薪酬与奖励系统可以公开公正运行，激励员工的同时也保障每位员工能够得到应得的公平奖励。  
   
分布式自治管理使公司的运营风险得以降低。无需维护的自治系统，减少了由于系统维护带来的技术风险，安全风险，信息泄露风险，以及因此带来的公司信誉风险。去中心化的文件存储，使公司不再依赖中心服务器，任何宕机都不再会引起重大交易风险事故，有效减少了操作风险。带有时间邮戳并公开的交易记录，保护了公司交易和账目不被篡改，保证了公司运营的客观和公正性，减少了违规操作的可能性，大大降低了安全性风险，员工道德风险，以及相应的法律风险。  
   
此外，分布式自治公司还会具有以下几个优点：  
   
****公开透明****  
  
建立在区块链上的分布式运营系统的基础是开源软件，公开公正是分布式自治公司的最基本特征。这项特征保证了在公司管理决策方面的100%透明度，去除了小团体暗箱操作的可能性。公司透明度提高的同时也提高了所有员工的大局观和参与度，每个人都能理解不同选择和背后的原因。透明度也增加了对公司的信任，因为你或许不可以完全的信任一个人或组织，却可以完全的信任数学。  
   
****去中心化****  
  
去中心化的全员参与构成了公司自治的前提。公司不再由一个高高在上的人或者若干人组成的董事会全权负责，包括运营责任和会计责任在内的所有责任被分散给所有的参与员工。公司自治系统不能够被个人或小团体完全控制，杜绝了因为管理人员的缺陷或失误而造成的公司经营不当。作为公司的投资人，客户，或其他利益相关者，可以信任公司的管理运营，相信公司不会因为少数人的失误而造成重大损失。  
   
****匿名性****  
  
由于区块链节点之间交换数据遵循固定的算法，分布式自治系统会自动判断信息是否真实有效，因此数据的交换是去信任化的，这是区块链中的共识机制。参与其中的每位员工因此也无需公开身份信息。此项底层加密技术的应用使得自治化的完全匿名企业投票成为可能，对企业信用积累和企业民主性的推行有很大帮助。  
   
****民主性****  
  
每一项公司决策的通过都必须要经过民主投票决定，包括公司分布式运营系统的核心协议和规则的制定和修改。而分布式自治的去中心化和自治的特性也决定了公司必须是一个民主投票的机构。分布式公司自治很好的调动了员工的积极性，减少了公司等级，极大地增加了自由度和灵活度。  
   
****业务连续性****  
  
由于公司的运营系统建立在区块链上，有非常高的可靠性和容错性。这个点对点的运营网络当中的每一个节点都保存着完整的数据副本，任何节点出错都不会影响到整个系统的安全运营。分布式自治系统保障了公司业务的连续性。想象一个全球性的交易平台，在没有复杂技术的情况下，不需要担心宕机的风险，也不需要担心被攻击或篡改，更不需要频繁的系统压力测试，在降低技术成本和提高信誉度方面有着多么巨大的影响。  
   
****盈利性****  
  
每一位参与公司活动的员工都可以成为公司的股东，通过自治运营和系统成长来获得收益。  
这是非常重要的，因为公司的首要目的是实现利益最大化，从而使股东获得长期收益。分布式自治公司则通过使员工获得系统发展的奖励来实现。盈利性和公司本身的价值性相关，但是，只要有利益存在，即使利润并不高，公司也会积极地自主运营下去。  
   
关于分布式自治的一切并非空谈，事实上，建立在成熟技术发展和管理模式上的第一个分布式自治系统——比特币系统已经被证实是可行的，并且已经实现了工业化。我们突然发现，站在几个世纪以来占据全球经济主体的垂直化制度公司的对面，顺应扁平化分散化制度的发展趋势，数字化革命早已经引领我们走入了新的阶段。因此我们相信在不久的将来，去中心化的自治系统模式将会带领我们创建出新型的分布式自治公司，甚至发展出一个新型的可编程经济体。分布式自治公司的构想带给了我们无限的空间和可能，而这一切的最终实现都将取决于创建者的奇思妙想。

2016-09-18 16:06

[转]这是一张区块链“淘金”地图：巨头布局、规则设计、创业冒险才刚刚开始2016-09-14 孙骋   
本文发布于《商业价值》9月刊封面报道《“淘宝”区块链》  
  
[http://mp.weixin.qq.com/s?\_\_biz=MTA2MTMwNjYwMQ==&mid=2650694856&idx=1&sn=2c077e9fa66b254418542980c15e51dc&scene=0#wechat\_redirect](http://mp.weixin.qq.com/s?__biz=MTA2MTMwNjYwMQ==&mid=2650694856&idx=1&sn=2c077e9fa66b254418542980c15e51dc&scene=0" \l "wechat_redirect" \o "http://mp.weixin.qq.com/s?__biz=MTA2MTMwNjYwMQ==&mid=2650694856&idx=1&sn=2c077e9fa66b254418542980c15e51dc&scene=0#wechat_redirect" \t "https://xueqiu.com/5674464747/_blank)  
  
1995年的互联网世界，刚从沉睡中醒来。  
  
Netscape在这一年上市，以54亿美元市值成为当时排名第一的互联网公司。它曾是世界上使用最广泛的网页浏览器，在 90 年代中期占据的市场份额超过 90%。  
  
如今Netscape已不存在，市场造就了它，也抛弃了它。当时市值排名前五位的公司还包括Web.com、Rentpath、Axel Springer，如今已被Google、Facebook、阿里巴巴、亚马逊代替。  
  
互联网在经历了资本泡沫、行业洗牌之后，朝着移动端前行；互联网的职能也从传递信息，转而成为传递价值。区块链，可谓价值传递的产物，2016年的区块链世界，和1995年的互联网是同一番景象。  
  
作为比特币的底层技术，区块链具有去中心化、不可撤销、可溯源的特征，是未来价值互联网的开端，区块链可以大大改善金融系统的效率。  
  
在这个分布式共享账本上，有多个节点，由去中心化的多方共同维护，有一个“统一共识”机制保障。互相不了解的任何人之间，可以借助这个公开透明的数据库背书的信任关系，完成端到端的记账、数据传输、认证，以及合同执行。  
  
高盛最近发布的报告认为区块链有5个典型的应用领域：共享经济、供电市场、房地产、证券交易以及金融市场。  
  
在共享经济领域，区块链可用于存储用户身份，为平台构建用户信任；在供电市场，高盛预想了一种基于区块链技术的分发网络，使得每幢建筑可以自己发电并使用区块链的识别技术在此网络上向陌生用户进行购买和销售，替代原先集中式的供电模式；将房产信息保留在区块链中，买家便可以快速、简单、低成本的核实房主的真实信息，减少房地产交易的失误，降低人工成本；在证券交易中，通过在清算与结算过程对区块链技术的使用，尤其是对股权、回购和杠杆贷款，高盛预计整个行业能够节约110亿～120亿美元的成本；此外，区块链促进金融领域的反洗钱和顾客身份审查，改善数据质量，减少可疑交易的错误识别，预计节约30亿～50亿美元的成本。  
  
****两股力量正在推动区块链浪潮，一股力量自上而下，监管层和金融机构已经着手规则的制定：****  
  
今年年初央行表示，考虑将区块链技术应用于央行数字货币中；  
  
平安集团和香港友邦保险相继加入国际区块链组织R3；  
  
中国互联网金融协会成立区块链工作小组；  
  
国内的金融区块链合作联盟5月成立；  
  
8月，工信部联合多家企业，讨论并公布了中国区块链技术与产业发展论坛未来两年的规划  
  
......  
  
从IT发展史来看，从Windows到安卓、IOS，都由大公司研发，因为研发工业标准，需要知道主要客户的需求、应用场景，这是大公司能做的，缺少大型公司参与的技术很难成为标准。目前IBM、微软等IT巨头已经参与其中。  
  
****另一股力量自下而上，创业者们试图从技术突破，打开一片天地。****  
  
作为催化剂的资本市场，期望抢占先发优势，区块链成为“新宠”。根据CoinDesk的统计，2016年一季度，区块链领域的风投总额达到1.6亿美元，较2015年四季度环比增长515%，风投平均交易规模为1140万美元。从2013年到目前，共发生186起融资与并购事件，但其中只有5起走到了C轮融资，并且投资的地域分布上相对集中在美国硅谷。  
  
优质项目很少，一些创业项目尚未有应用落地、还在谈概念，从传统VC的角度来看，并不适合早期投资，但是众多散户愿意买单。国内某号称“区块链创业”的团队通过股权众筹，累计募集近2000万资金，参与者都是散户。  
  
“错过1995年的互联网，不愿错过区块链的机会”，是很多投资人的观点，这股热情从全国各地火热召开的区块链大会、到处奔波寻找项目的投资人，可见一斑。不过区块链对投资人的知识水平要求很高，若非专业出身，恐怕很难看得明白。  
  
****规则制定者****  
在自上而下的路线中，区块链的游戏规则将在未来几年内被制定。  
  
国际货币基金组织在首份数字货币报告中指出，区块链“具有改变金融的潜力”。但目前总体还处在起跑阶段，参与者齐头并进，一时难决胜负，观望者也有可能后来居上  
  
今年6月世界银行参与主办了美联储华盛顿总部的区块链会议，90家央行代表参会，中国也参加探讨区块链和数字货币技术的应用前景。  
  
政府机构纷纷投石问路。  
  
美国政府部门一方面重点研究如何对抗区块链技术被应用于非法领域，强调区块链的安全使用；另一方面投资研发行政领域的区块链的技术应用，希望通过区块链技术提高行政管理的效率。  
  
英国就业和退休保障部试图利用区块链的技术追踪救济金的去处；印度国家支付公司和印度储备银行试图利用区块链技术解决经济和金融中大量不透明、不合规的问题；荷兰银行启动区块链数字货币的内部研发；加拿大央行正在开发基于区块链的数字化家园。  
  
****目前全球最大、成员含金量最高的区块链联盟是 R3，由花旗银行、瑞士信贷、摩根大通、高盛、汇丰银行等 42 家国际银行组成。R3 旨在制定银行业区块链技术开发的行业标准，探索实践案例，并建立银行业的区块链组织。R3 具备大型项目的研发能力，正在研究分布式账本技术在金融市场的跨界应用，参与以太坊、Eris、Chain、IBM等平台的测试。****  
  
中国平安和香港友邦保险已经加入 R3，未来将获得 R3 的内部技术支持、咨询调研服务等。这有利于在区块链发展早期，消除国内和国际的技术落差，统一技术标准，加速国内外接轨进程。  
  
放眼国内，早在今年1月，中国人民银行召开数字货币研讨会，表示从2014年起，已经成立了专门的研究团队研究数字货币技术，随后央行行长周小川表示：未来数字货币与现金将在长时间内并行、逐步替代；数字货币将作为法定货币，由央行发行并保障其安全性；央行的数字货币有可能采用区块链技术，已部署重要力量探讨其应用。  
  
企业们纷纷加入新领域。中国区块链研究联盟、金融区块链合作联盟先后成立，后者集结了微众银行、平安银行、招商银行、恒生电子、京东金融、腾讯、华为、银链科技、深圳市金融信息服务协会等等31家成员。  
  
中国区块链技术与产业发展论坛未来两年的规划，也已由工信部发布，并联合微众银行、万向、乐视金融、平安和蚂蚁金服等重点企业进行讨论。  
  
****从规划看出，各行业区块链应用将联动进行，涉及人民银行科技司、商务部电子商务和信息化司、农业部信息中心、中国电子商务协会、中国机械工业联合会这五大权威部门。****  
  
“标准”，是规划中出现最多的字眼，中国将向国际标准组织ISO/IEC JTC1提交开展区块链标准化研究建议，提前抢占位置，可见对于区块链标准制定的推进着手点，已经从国内开始转向国际。  
  
****IT巨头布局****  
IT 巨头们一直是新技术的有力推动者，区块链正好也给了创新乏力的 IT 巨头们新的机会。目前，几乎所有的 IT 巨头们都在利用技术优势着手布局。  
  
近期，IBM商业价值研究院发布了题为《全速前进——随着区块链重新思考企业生态系统和经济模式》的报告，其中提到：

全球都是基于财富创造的方法来推动人类的发展，但在人类发展的过程中，市场摩擦是财富创造的最大障碍，而人类进步的长河就是一部不断消除摩擦的历史。  
  
目前，商业中阻碍创新有三种形式的阻滞，包括信息产生和传递的阻滞，用户和网络交互过程的阻滞，以及技术和商务创新所面临的阻滞。

****而区块链的价值，就在于有效地消除、减少以上三方面的阻滞；阻滞的缓解带来成本的降低和速度的提升，从而带来产业的结构性升级，和高效、极富竞争力的规模效应。****  
  
IBM副总裁、大中华区创新事业部总经理王允臻认为，区块链的 5 个属性有助于消除市场摩擦：  
  
1、分布式而且可持续。总账会随着每笔交易的进行而更新，在所有交易之间共享，而且接近实时地在参与者之间进行选择性地复制。通过加密技术或数据分区技术确保隐私，有选择地向交易参与者授予不同的总账接触范围；交易信息和交易各方的身份都可采用掩盖技术隐藏起来。因为区块链平台并非由任何单一组织所拥有或控制，所以其持久存在并不依赖于任何单独实体。  
  
2、安全而且持久。密码能够鉴定并验证交易，并只允许参与者查看账本中与自己相关的部分。一旦同意条件，参与者就无法篡改交易记录，只能用新的交易来改正错误。  
  
3、透明而且可审计。由于一笔交易的多个参与方能够访问相同的记录，所以他们可以验证交易以及确定身份或所有权，而无需第三方中介机构的参与。每笔交易都有时间戳记，可以接近实时地进行验证。  
  
4、基于共识且可交易。所有相关的网络参与者必须一致同意交易有效。这一点通过共识算法实现。区块链可以建立交易或资产交换所依据的条件。  
  
5、经过统筹而且灵活。由于基于一个或多个条件执行的业务规则和智能合约可以内置于平台之中，因此区块链业务网络能够不断发展成熟，支持各种端到端的业务流程和各种不同的活动。  
  
“目前我们更多通过深度学习应用场景下的特定行业知识和业务逻辑，结合到PoC（Proof of Concept，电子建模中的概念验证）当中，提供原型开发，其中技术平台层面，则利用 Bluemix上建构的区块链应用开发平台，直接让开发者试水应用IBM的区块链，帮助成员从原型开发直接走向商业化部署。” 王允臻告诉钛媒体，IBM参与了 DAH 等区块链企业的投资，宣布支持由 Linux 基金会成立的超级账本项目，在新加坡建立了 IBM 区块链创新中心，未来 3 年将在金融和贸易领域推进一系列的技术试点。  
  
今年9月，IBM将发布迄今为止最大的区块链商业使用项目之一，借助区块链消除中间商而使得很多市场和功能更加高效，该项目有望在IBM全球金融部门的交易纷争中节省约1亿美金。  
  
在咨询服务、专家服务、业务设计、区块链的概念验证以及流程变革、项目实施和维护、基础架构的提供等方面，IBM都有完整的解决方案。  
  
IBM与纽约梅隆银行合作，加速证券借贷应用的设计与开发，利用区块链网络进行交易和转移资产。同时在云环境中，利用区块链安全框架，IBM帮助企业快速托管安全、防篡改的网络，并扩展至数以千计的用户，在数分钟内部署生产区块链网络，采用dashboards仪表板界面、分析和支持功能运行经过签名、认证和测试的Docker映像。  
  
王允臻认为，“现在是一个不断做大蛋糕的时候，中国的企业可以通过超级帐本这样的开源社区贡献源代码，提升国际主流技术中的话语权”。  
  
另一巨头微软则在云平台Azure上部署区块链基础工具，推出了全球首个BaaS服务，已经与多家区块链初创公司展开合作，希望在底层操作系统上对区块链提供技术平台支持。BaaS，即Blockchain-as-a-Service ，目前正式向Azure用户发布预览版。  
  
BaaS类似一种“沙盘”，合作伙伴可以在一个低风险的环境中，与不同技术互动，从智能合约到基于区块链的税务汇报服务。微软针对不同的场景，提供了一系列可复用的模板，用户可以用最简单高效的方式搭建区块链虚拟机测试环境，大大降低开发成本。  
  
包括Bitpay、MultiChain和Storj等在内的多家区块链初创公司，都已经与微软达成了合作伙伴关系，这些公司的用户可以直接在微软BaaS中找到相对应的模板。Azure BaaS是一个加强区块链技术教育环境和推进合作的平台，未来计划是规模化，希望形成“认证区块链市场”。  
  
****又一场“淘金”开始了****  
区块链的另一条路径，自下而上。  
  
在8月份在深圳由钛媒体和钛易投联合主办的区块链产业论坛上，香港中文大学教授、点亮资本合伙人劳维信进行了一场演讲。他在演讲中表示，需要把区块链、人工智能、大数据等技术放在一起看，才会对区块链有一个准确的判断。  
  
“谷歌不是第一个做搜索引擎的，所以在投资方面，追求 ‘早’是没有用的，你要看 ‘对’；其次，区块链中很多创新还没有出现，这里面的 ‘BAT’，出现不是偶然的， 需要借助以前的一些技术，而这些技术才刚刚开始，未来有更多创新将出现。区块链里的 ‘BAT’，不是那么容易找到的。”劳维信说。  
  
最后的赢家不是出发最早的选手，这个互联网法则也适用于区块链。  
  
劳维信所在的点亮资本，此前投资了国内区块链创业公司布比，近几个月内，布比将区块链技术落地应用在积分、供应链管理云平台、网贷平台等场景，帮助这些领域里的公司搭建区块链底层技术。  
  
布比的另一家投资方万向，去年成立了一笔5000万美元的投资基金，专门投区块链创业项目，目前已经投出2000万美元，布局全球23家区块链公司，其中国内只有1家。  
  
万向控股有限公司副董事长兼执行董事、万向区块链实验室发起人肖风告诉钛媒体，在自下而上的路线里，以草根为核心的创业公司们，做出的区块链探索可能还非常初期，但恰恰是行业中比较领先的。肖风说：

“对于他们来说，没有包袱，他们不需要去考虑太多规章限制，大型公司需要考虑现实中很多的监管的需求。自下而上的这条路线可能会走得更快一点，但是明显的技术标准还没产生，这还需要时间。”

“区块链最大的价值在于数字资产的管理和交易，而不是简单地做一些结合场景的应用。” 一位 VC 机构的投资人认为。  
  
创业公司布比将区块链技术落地应用在积分、供应链管理云平台、网贷平台等场景，帮助这些领域里的公司搭建区块链底层技术。8月，布比推出了基于自身区块链的数字资产平台“布萌”，发行数字资产。  
  
这些数字资产拥有区块链技术多中心化、不可篡改的特性，数据的存储安全、可信，可以在资产流通方之间建立起多方信任，保证用户购买和使用的数字资产的真实有效性。  
  
随着互联网的快速发展，越来越多的数字资产在互联网上发行流通，比如游戏装备、预付卡、电子券、商业积分、保险卡单，这些数字资产种类繁多、价值庞大，却因为技术和商业的壁垒，大多分散在商家各自的系统里面，不能有效的在用户之间流通。  
  
布萌总经理杨帆说：“布萌拥有一套标准化协议，在布萌平台上开发的应用之间不需要对接，就可以实现布萌用户之间数据信息流、价值流互联、互通。同时，发行在布萌平台上的数字资产，可以实现点到点的传递。”  
  
布萌已经应用在商业积分、游戏币、游戏道具、预付卡、电子券、保险卡单、证券化资产、互助保险等行业和领域，阳光保险、钱香金融、多多币、数贝荷包等机构都已经加入布萌。  
  
在这个平台上，数字资产是自由流通的，其价值也是由多方共同决定的。当越来越多的应用和资产在上面流通，应用与应用之间、用户与用户之间、应用与用户之间都会发生更丰富的化学反应。  
  
在平台上，某一种数字资产得到大家认可，会带来比预期更高的价值。比如游戏中一颗宝石，只要有人愿意交换，用户可以在布萌平台上兑换成一个理财产品或者一份保险，甚至是一颗钻石。  
  
杨帆预计：平台上未来会有第三方交易所、通兑平台等机构的出现，进一步加快不同机构之间的数字资产的流通和通兑，布萌不仅仅是一个安全开放可信的数字资产平台，最终它会成长为一个由大家共同打造、维护的数字资产生态圈。  
  
在互助保障方面，借助布比区块链和数字资产平台布萌的技术，互助保障平台众托帮落地了区块链应用。众托帮拥有110万用户，通过平台发布互助计划，具有共同要求和面临同样风险的人，可自愿通过预存会费的方式加入计划，一旦成员发生计划类的风险，该计划类的所有会员将分摊不超过30万元的互助金，每个成员扣取不超过3元。  
  
但监管的真空，让互助保障行业面临系统组织者作弊、资金不透明、会员骗保等信用风险。写入布萌平台里的数据无法篡改，确保各方数据真实有效，所以众托帮用户可以查询自己的个人信息，以及不涉及隐私的其它信息，如互助计划的参与人数、他人的加入时间等等，布萌从技术上解决了信任问题。  
  
****从场景进入****  
“万事俱备，只欠场景。”  
  
8月的陆家嘴，一位投资人如此感慨道。他刚刚听完一场区块链创业路演的上半场，随着拥挤的人潮挤出大厅。  
  
如何结合自身的业务特点，从合适的场景切入，将区块链的价值最大化，是参与者们考虑的问题，这也将是上下两股力量汇聚、碰撞的地方。  
  
平安组成了区块链核心团队，专注于2件事，一是从集团内部挑出合适的业务，通过区块链去改进，二是关注国外比较前沿的创业公司，进行投资。  
  
“我从2013年就开始和马明哲总沟通区块链这件事，讲了3年，终于，今年我们召开执委大会的时候，他宣布区块链是平安集团接下来的发展重点。”中国平安集团首席创新执行官屠德言说。  
  
平安集团有20多家专业子公司，在金融、大医疗、健康领域，区块链都有潜在的应用层面。屠德言举例：平安从线下走到线上和移动端，在征信和场外交易方面，平安通过脸部识别、AI、手纹等方式，在线了解客户；平安租赁最近开始了汽车租赁和飞机租赁业务，租赁对象有不同的合作伙伴，每一个资产如何使用、如何应用，这些信息都可以记录在区块链上。  
  
前海股权交易中心建立了专门的区块链团队，试图解决非公开条件下有效、安全、多元地投资对接和交易的问题。前海股交中心总裁林凡说：

“区块链的不可复制和去中心化的储存、不可篡改性和信息化的高度透明，契合了前海股权交易中心对新型互联网的方法和方向。未来我们将交易信息、交易价值，这些目前在互联网上还无法实现，所以我们对区块链技术在金融服务的应用充满期待。”

前海股交中心面对1300万的中小微企业，这些企业规模小、运作灵活、风险较弱。接下来，非标市场和私募将首先被区块链改造：未来在场外市场挂牌的产品可能都是非标的，投资人很难在公共平台进行投资；私募产品无法公开对外销售，投资人的数量受到限制，客户需要个性化服务。  
  
蚂蚁金服将区块链应用于公益场景，在支付宝爱心捐赠平台上线的区块链公益筹款项目，将让每一笔善款可被全程追踪。  
  
在公益项目中，用户往往捐出几元到几百元不等的善款，利用区块链技术，每一笔款项的生命周期都记录在区块链上，没有人工拨付等环节，人工无法更改善款去向，用户可以持续追溯。  
  
这是一个小小的试水。蚂蚁金服希望从一个小而美的场景切入，公益需要一个平台保证捐赠的每一笔资金流开放、透明、可信任，以往公益项目也缺少合适的信任平台和配套的操作机制，其次，这个场景可以让用户更好地理解什么是区块链，算是用户教育。蚂蚁金服集团首席技术官程立说：

“对于蚂蚁金服，区块链真正的价值在于：用分布式的技术和共识算法实现一个信任机制，未来我们把云计算的强大处理能力和区块链提供的信任制度结合，希望找到合适的应用场景。”

在程立看来，区块链的创新，首先是符合监管要求，在现有的法律和监管框架下，找到业务创新点，其次是保护用户信息和资金安全信息，所以把区块链作为一种增加信任的服务，附加在现有业务基础上。  
  
“未来区块链在云端”，腾讯金融云副总经理郭锐介绍：腾讯在区块链方面也做了不少积累：一是资金处理的量级，今年春节期间，每秒15.8万笔的支付能力，每秒48.2万的帐户处理能力；二是腾讯拥有数百套分布式账户主机，面对复杂的网络，副本间账户一致性很高，所以对一致性算法、时间戳、签名机制、拜占庭将军等问题有实战经验。  
  
同时腾讯有私有链运营的基础，微信钱包、QQ支付、理财通等腾讯金融场景，加上基于私有区块链思想架构的底层账户体系，通过时间戳、链式签名、内部联盟链等机制保护用户的资金和财产安全。  
  
“通过区块链，未来我们可以提供更多的支付能力，包括反抵赖和反欺诈能力、人脸识别等，可以创建信任，不需要每个用户了解区块链链技术，就可以获得区块链的信用和保护。”郭锐说。  
  
****喧哗与骚动****  
  
区块链投资泡沫还没到来。  
  
****“目前区块链投资是一个线性、正常的发展状态，而远远没有到达到泡沫时期那种指数级上升投资的情况。我们发现，整个资本市场对区块链行业的投资越来越细分。”肖风说。****  
  
在《区块链社会》的作者龚鸣看来：许多投资机构考虑到，区块链技术在未来多个行业的发展可能性还具有极大的不确定性，目前的探索更多集中于底层架构，所以抱着观望态度，希望等待局势明确后再大举进入。  
  
区块链还处于一个知识普及的阶段，目前优秀的区块链底层技术团队全世界也没有几支，VC对区块链创业团队的投资也比较谨慎，一些团队给自己估了很高的值，但是VC不认可。  
  
于是，这些区块链创业团队创造出了 ICO的概念，不同于IPO，ICO 是Initial Coin Offering的简称，把所发行的标的物由证券变成了数字加密货币。ICO最直接的意义是：即便VC不看好，创业团队也可以在基于区块链的众筹平台上发行自己的代币，募集资金。  
  
国外的The DAO就创造了众筹纪录，在15天内众筹超过1亿美金，后来遭到技术攻击，损失了约6000万美元。国内一家区块链创业团队尚未有应用落地、还在谈概念，从传统VC的角度来看，并不适合早期投资，但是众多散户愿意买单，去年通过发行代币众筹了400多万人民币，今年二次众筹，募集了1300万资金。  
  
这些资金基本来自于早期比特币炒家，在2013年比特币价格上涨期间增加的财富。其中很多人是比特币信仰者，参与众筹时，先买比特币，再换成“小蚁币”这类代币。  
  
****就像股权众筹项目遭遇信用风险一样，这些ICO项目也有同样的问题：一是没法形成很好的信息披露方式，仅仅靠每年出一份白皮书，恐怕不能让投资者信服；二是风险定价是一个外包型定价，领头方对某一个资产做了定价，这意味着可以在外包基础上给外包方给予杠杆，难以避免利益冲突。****  
  
一位业内人士说：币圈是受益者，圈里人还持有很多比特币，他们希望把ICO和代币的游戏继续下去，获得更大利益。  
  
“区块链和比特币一定要区分开来，我么只关注真正做技术的创业者，不会考虑跟比特币相关的创业项目。”劳维信告诉钛媒体。  
  
当然，也有人对区块链投资前景并不那么看好。  
  
前上海证券交易所总工程师、中科院博导白硕质疑：“首先，开源是刚需，你要让它可信，就必须把内容晒出来，而且要让高手互相之间过招；其次，区块链理论上号称无人运行，不需要有什么服务支持，后续服务就显得非常骨感；这两边一挤压，初创公司生存有多大？”  
  
从二级市场来看，投资风险在于2点：一是目前还不具备大规模推广应用的条件，短期不会产生盈利影响；二是目前还处于研究应用早期阶段，标准还未形成。  
  
区块链不是万能的。  
  
区块链解决不了物理资金安全问题，它可以保证信息流的一致性，但需要设计非常良好的资金托管的机制才能保证安全；其次是业务流程的漏洞，区块链没有办法解决因为业务设计缺陷引入的业务级风险。  
  
现在的金融存量系统全部在一夜之间换成区块链底层架构，是不可能的，如果盲目信任的话，可能会引发巨大风险，特别是线上资产和线下的转换，存在很多的风险。  
  
对于风险，全国人大财经委委员、中国互联网金融协会区块链研究工作组组长、中国银行前行长李礼辉分析：在The DAO案例中，最终团队通过硬分叉的方式，把时间调回到受攻击以前，这样就可以把被劫持的资金返还到初始投资者的账户上，这说明区块链的技术，同样存在风险隐患，智能合约的可靠性，也必须经过专业、权威的审核和认定，预先防止漏洞。  
  
李礼辉这样看The DAO带来的启示：  
  
1、新技术开启新应用，但也会带来新的风险。  
  
应用高新技术，必须注意防范技术垄断的风险、技术性操作的风险。如果有人垄断了区块链里的智能合约编程这样一些高端的技术，你的技术不如别人，在设置编程的时候，存在某些漏洞，这些都可能为事后被攻击、盗用形成可能被利用的技术漏洞。所以，必须构建能预防道德风险的技术上的防火墙，在不同场景的区块链技术的应用中，必须对智能合约、时间戳、密钥等核心编程的安全性、稳定性、可靠性做深入分析、权威认证。  
  
2、新的技术有新的特征，风险管控要适应新的技术结构。  
  
基于区块链分布式的和不可篡改的特性，我们无法照搬现有的数据库结构下的安全控制措施来应对黑客攻击等风险事件。我们现在的数据系统，都是大中心的数据系统，这样一种系统结构下，我们采取的一些基于大数据中心的防控措施，不可能简单移植到区块链应用场景中。所以我们要针对新的技术结构，研发新的风险管控技术和应急措施。

2016-09-19 09:52

**[@一体同悲无缘大慈:](https://xueqiu.com/Die_ewige_Wiederkehr)**

[转]这是一张区块链“淘金”地图：巨头布局、规则设计、创业冒险才刚刚开始2016-09-14 孙骋 本文发布于《商业价值》9月刊封面报道《“淘宝”区块链》[网页链接](http://mp.weixin.qq.com/s?__biz=MTA2MTMwNjYwMQ==&mid=2650694856&idx=1&sn=2c077e9fa66b254418542980c15e51dc&scene=0" \l "wechat_redirect1995" \o "http://mp.weixin.qq.com/s?__biz=MTA2MTMwNjYwMQ==&mid=2650694856&idx=1&sn=2c077e9fa66b254418542980c15e51dc&scene=0#wechat_redirect1995" \t "https://xueqiu.com/5674464747/_blank)

[展开](https://xueqiu.com/5674464747/74975890)

记者也就是为写而写，还记得她写的比特币已死。[http://www.tmtpost.com/1663852.html](http://www.tmtpost.com/1663852.html" \o "http://www.tmtpost.com/1663852.html" \t "https://xueqiu.com/5674464747/_blank)

2016-11-19 10:30

[$腾讯控股(00700)$](http://xueqiu.com/S/00700" \t "https://xueqiu.com/5674464747/_blank) [$阿里巴巴(BABA)$](http://xueqiu.com/S/BABA" \t "https://xueqiu.com/5674464747/_blank)  央行研发法定数字货币  
  
中国人民银行直属单位2017年度工作人员招聘公告[http://www.pbc.gov.cn/rmyh/105208/3183358/index.html](http://www.pbc.gov.cn/rmyh/105208/3183358/index.html" \o "http://www.pbc.gov.cn/rmyh/105208/3183358/index.html" \t "https://xueqiu.com/5674464747/_blank)  
  
  
  
职位简介其他要求或  
补充说明  
  
  
  
  
  
  
主要从事数字货币及相关底层平台的软硬件系统的架构设计和开发工作。具有系统架构设计经验、区块链技术开发或应用经验、大数据平台开发经验者优先  
主要从事数字货币及相关底层平台的软硬件系统的架构设计和开发工作。具有系统架构设计经验、区块链技术开发或应用经验、大数据平台开发经验者优先  
主要研究数字货币中所使用的关键密码技术，对称、非对称密码算法、认证和加密等。  
  
  
来真格的了  
  
============================  
  
《经济通通讯社驻沪记者王嘉宁１８日乌镇专电》人行科技司副司长姚前表示，人行研究的法定数字货币不是比特币，比特币没有市场支撑，而人民币是法定货币，背后有综合国力支撑。   
　　姚前出席第三届世界互联网大会「互联网＋普惠金融」论坛时表示，人行设计数字货币仍会保持对纸币的信任，纸币仍将在相当长时间内存在。人行数字货币意在利用区块链技术，但区块链尚处于发展阶段，还未到大规模使用状体。   
　　姚前表示，个人认为「虚拟货币」不是褒义词，并称比特币矿池的中心化已经出现，约７０％矿池目前在中国，以去中心化为起点走向中心化是必然趋势。   
  
比特币死（因为不受控制），区块链活（因为国家可以把握发行权）  
============================  
  
不足值货币能够广泛交易最根本原因在于信用背书，没有足够的选择，这个宝那个金的自然只能捏着鼻子认了，好歹这么大的平台，要赖账也不是只亏我一个[不说了]  
但现在呢？  
  
现在还只是研发[大笑][能力圈]  
但研发出来了呢？[割肉]  
  
哦，还有推广，还有过渡期[不屑][护城河]  
然后呢？

2016-11-19 10:35

[http://finance.qq.com/a/20160909/019794.htm](http://finance.qq.com/a/20160909/019794.htm" \o "http://finance.qq.com/a/20160909/019794.htm" \t "https://xueqiu.com/5674464747/_blank)  
  
姚前：区块链有望像互联网一样彻底重塑人们生活方式  
  
腾讯财经讯 第二十四届中国国际金融展2016年9月8日至11日在北京展览馆举办。本届展会以“融合创新 转型升级 提质普惠”为主题，集中展示金融业“十三五”转型发展规划和各类金融机构、金融科技企业的创新成果，以及普惠金融新服务和金融IT新技术。腾讯财经全程直播本次金融展。  
  
中国人民银行科技司副司长姚前出席本次会议并发表讲话，姚前表示，一些学识认为区块链是继大经济、个人电脑、互联网、移动互联网之后的计算范式的第五次颠覆式的创新，以及下一代云计算的主形，区块链有望像互联网一样彻底重塑人们的生活方式。同时姚前也介绍了当前区块链发展中的四大优势和三大劣势。  
  
以下为嘉宾发言实录：  
  
姚前：尊敬的各位领导、女士们、先生们，大家早上好！区块链是当今金融科技领域备受关注的一个热门话题，近年来对这一技术的研究和应用呈现了爆发式的增长态势，一些学识认为它是继大经济、个人电脑、互联网、移动互联网之后的计算范式的第五次颠覆式的创新，以及下一代云计算的主形，区块链有望像互联网一样彻底重塑人们的生活方式，人民银行一直在进行研究和跟踪，今天我想谈一下区块链技术的特点和未来的趋势。  
  
区块链技术是以比特币为代表的核心技术，区块链的技术是通过时间波等技术手段，在分布式系统中实现了不依赖于某个技术中心的点对点交易，从而为数据安全、协同效率、风险控制等问题提供解决方案。区块链技术起源于2008年，目前尚未形成行业公认的区块链定义。狭义来讲，区块链是一种按照时间顺序，将数据区块以链条的方式组合成特定结构，并以密码学方式保证的不可篡改和不可伪造的去中心化共享总账。广义的区块链技术是利用加密链式区块结构来验证与存储数据、利用分布式共识算法来新增和更新数据、利用运行在区块链上的代码，来保证业务逻辑的自动强制执行的一种全新的方式。  
  
以比特币为例，一个完整的区块链系统由数据层、网络层、共识层、激励层、和约层和应用层组成，和传统的技术相比，区块链具有以下四个方面的优势。  
  
第一个优势是区块链的链长数据不可篡改，更加安全。实践证明这样一个数据库可以确保市值达百亿美元的比特币在黑客的攻击下，可以保证安全。  
  
第二个优势是异构多活，可用性强。区块链中的节点通过点对点的通信协议进行交互，在保证通信协议一致的情况下，不同节点可由不同的开发者使用不同的编程语言，基于不同的架构实现不同版本的交易，由此构成的软件异构环境确保了即便某个版本的软件出现问题，区块链的整体网络也不会受到影响，这也是区块链高可用的一个优势所在。  
  
第三个优势是新型协作机制，效率更高。在区块链运用之前通常有两种解决方案，第一种是在寻找共同的上级机构，由共同的信任中心对整个组织进行协调，这种方法的局限在于很难找到一个所有参与方共同认可的信任中心，对于一个中心而言，协调之下必然有优先级，不一定能够及时有效地满足所有的需求。第二种是共同由第三方机构完成协作，这种第三种机构往往能够成为各参与方的实际的权利中心，在第三方机构成立之后，如何吸纳新的会员，如何随着情况发展变化，调整各参与方的角色与权利，这些都依赖于大量的谈判和交易，区块链提供了一种不同于传统方法，以对等的方式把参与方连接起来，由参与方共同维护一个系统，通过共识机制和智能合约来表达协作规则，实现更有弹性的协作方式。因为参与方职责明确，不用向第三方机构让渡权利，无须维护第三方信任机构的成本，有利于更好地开展协作，形成更大范围、更低成本的新的协同机制。  
  
第四个优势是智能合约，更加先进。智能合约具有透明可信、自动执行、强制履约的优点，尽管如此，从1993年提出以来，智能合约始终停留在理念层面，重要原因在于长久以来没有支持可信代码运行的环境，无法实现自动强制执行，而区块链第一次让智能合约的构想成为现实。本质上讲，智能合约就是运行在区块链上的一段代码，和运行在服务器上的代码并无太大差别，唯一的区别是可信度更高。首先可信是因为智能合约的代码是透明的，对用户来讲，只要能够接触到区块链中，就可以看到编辑后的智能合约。其次可信还来源于智能合约的运行环境，除了透明，还需要保证数据的一致性和不可篡改，而这正是区块链的优势所在。  
  
因此智能合约一旦被部署到区块链上，程序的代码和数据就是公开透明的，无法被篡改，并且一定会按照预先的逻辑去执行，产生预计中的结果。如果这些代码的合约能够被认可，那么依托程序的自动化优势，不同的智能合约达到不同的目的，能够使我们加速走向更为广阔的高效的商业社会。作为近年来兴起和快速发展的新技术，区块链必然面临着各种制约其发展的问题，总体看包括三个方面的劣势。  
  
第一个是区块链的性能问题有待突破，目前来看区块链的性能问题主要体现在存储量，是系统设计时面临的最大挑战。智能合约运行时会相互调用，因此交易的处理程序特别重要，节点在验证交易的时候无法进行，只能逐笔进行，这会制约节点的处理能力。  
  
第二个劣势是在因此保护方面有待加强，传统上数据是保存在数据中心的，但是现在每个参与方都能够获得完整的数据备份，这也意味着数据是公开透明的。对于比特币而言，这样的解决方案也许够用，但如果区块链需要承载更多的业务，比如实名资产，这些信息如何保存在区块链上，验证节点在不知道具体信息的情况下如何执行合同，这就需要新型密码学方案在区块链上的应用，此外也可以规避一些隐私保护等问题。  
  
第三个劣势是升级修复机制有待探索。在公有链中，因为节点数量庞大，参与者身份不明，不可能关闭系统。此外，由于公有链不能关停，其错误修复也异常棘手，一旦出现问题，尤其是安全问题将非常致命。  
  
互联网近年来的迅猛发展，以及与物理世界的深度结合，已经根本改变了现代社会的生产生活和管理决策模式，可以预见的是，未来在中心化和去中心化这两个极点之间权衡，最大化挖掘现有区块链系统的潜力。在安全领域，虽然区块链本身的安全性经受了多年的考验，但仍需持续关注。区块链并未解决所有安全问题，对区块链的盲目信任有可能导致严重的后果，例如智能合约漏洞被利用，导致数字资产损失，监管者面临着巨大的挑战。  
  
我对区块链的理解就向大家报告到这儿，如有不当之处请大家批评指正，谢谢大家！

2016-11-28 17:26

**[@一体同悲无缘大慈:](https://xueqiu.com/Die_ewige_Wiederkehr)**

[$腾讯控股(00700)$](http://xueqiu.com/S/00700" \t "https://xueqiu.com/5674464747/_blank) [$阿里巴巴(BABA)$](http://xueqiu.com/S/BABA" \t "https://xueqiu.com/5674464747/_blank) 央行研发法定数字货币中国人民银行直属单位2017年度工作人员招聘公告[网页链接](http://www.pbc.gov.cn/rmyh/105208/3183358/index.html" \o "http://www.pbc.gov.cn/rmyh/105208/3183358/index.html" \t "https://xueqiu.com/5674464747/_blank)职位简介其他要求或补充说明主要从事数字货币及相关底层平台的软硬件系统的架构设计和开发工作。具有系统架构设计经验、区块链技术开...

[展开](https://xueqiu.com/5674464747/74975890)

终究不是一纸批文的对手  
这就缴械了  
==========================  
由央行牵头并入股的网联平台（简称“网联”），将按照新方案于近期启动，并预计于明年3月31日正式上线，届时支付机构将按照有关技术标准门槛分批接入。该平台的出现，或使支付宝和财付通退居从属地位。  
  
****“网联”是统一线上清算平台，也即网络版银联****  
“网联”也被称为网络版银联，属于线上统一清算平台，以改变第三方支付与商业银行直连及支付与清算市场不分的情况。该平台由央行牵头成立，主要是为了看清楚第三方支付的资金流向，防止赌博、贩毒、洗钱等违法犯罪活动的发生。  
此前计划由支付宝和财付通主导建设的思路，由于标准难统一、很难互相备份，加之系统建设不透明、其他支付机构有“后门”担忧（涉及机构的信息保护）等备受争议，最终被否决。  
新方案遵循“共建、共有、共享”原则，由“网联”平台的各参与方自主共建，确保统一技术标准和业务规则是平台所自建。“网联”由支付清算协会发起设立实体建设运营平台，除协会将参与实体公司出资外，央行也将入股，进而保证对“网联”这一重要金融基础设施的控制权和投票否决权。其股东总数不超过50家，募股机构在40家左右。  
  
除了央行和协会，其他任何一家第三方支付机构入股份额最高不会超过10%，投资金额不超过5000万元，以防止该平台被大型支付机构垄断。而份额的大小，将与其参与“网联”的建设程度挂钩。参与程度的评估标准包括三个方面：一是参与的产品、组件、软件；二是人员贡献；三是对平台业务规则和技术标准的反馈程度、响应程度。  
据悉，新方案的实施路线分为三步：第一步是向业内通报技术方案评审的结果；第二步是开发并募集股权；第三步是由“网联”筹备机构评估机构的投入。  
在今年4月举行的中国支付清算协会第二届会员代表大会上，就通过了由协会组织建设非银行支付机构网络清算平台的议案。“网联”主要针对持有互联网支付牌照的支付机构，这意味着以后所有的网络支付机构不再需要单独接入银行接口，只要接入平台即可。而这一平台也被认为，将改变第三方支付市场格局。  
“网联”定位于处理由网络支付机构发起的网络支付业务以及为支付机构服务的业务，支撑以电子商务等场景驱动的支付业务创新，满足基于支付账户与银行账户的网络支付跨行资金清算处理，并通过可信服务和风险侦测，防范和处理诈骗、洗钱、钓鱼以及违规等风险。  
****该平台能解决那些问题？****  
自《国家普惠金融发展规划（2016-2020)》发布以来，更好的落实普惠金融成为各大机构的共识。随着电子商务的迅猛发展，其普及性及使用的广泛性使得支付清算的管理变得尤为重要。而“网联”的出现，可以解决机构对接乱象、风控风险、信息不透明、资源浪费等问题：  
一是可以提高支付机构系统的安全性及风控水平。由于部分支付机构系统安全性及风控管理水平不同，且缺乏配套的风险保障措施，如果支付机构经营不善发生系统性风险，会对金融稳定性产生了不利影响。  
二是保证清算数据作为公共资源，而不是集中于市场垄断者手上。在一些大型第三方支付平台，存量客户规模和交易历史数据是其核心商业价值，支付与清算模式相对封闭，对其他机构具有排斥性。但竞争的关系，难以保证公平性。  
三是减少多头开发造成的资源浪费，提高交易的过程和信息的透明度。由于各银行机构业务处理平台和接口标准不一，造成多头开发、资源浪费大，一定程度上增加了开发和管理难度。另一方面，清算模式有相对的封闭性，交易处理过程和交易信息透明度低，游离于监管部门的有效监管之外，已经产生监管死角。  
四是防范诈骗、洗钱等风险。目前，虽然更大支付平台都拥有自己庞大的数据库及征信信息，但因为不是统一管理，技术、制度等方面存在漏洞，由此可能引发隐患。而由央行统一管理的“网联”，基于多年的金融管理经验，可以更好的杜绝这些风险。  
****支付宝和财付通，或由主导地位变从属地位****  
在第三方支付市场，支付宝和财付通一直处于两强的位置。但随着央行牵头并入股“网联”，支付宝和财付通或将退居从属地位。  
由易观的数据来看，第三方移动支付市场的交易规模持续增长，其中支付宝和财付通分别以55.40%和32.10%的市场份额占据第一二位。而主攻线下清算的银联仅占0.91%。  
  
在互联网支付市场中，支付宝和财付通仍然以43.39%和16.95%的市场份额排在第一二位，而银联商务以15.44%的市场份额排在第三。  
  
“网联”的到来，会让既有的第三方支付格局发生什么的变化？支付宝和财付通还能否保有既有的主导地位？  
一位业内人士表示，占市场份额大头的支付宝和财付通在未来将扮演什么样的角色，这对“网联”的成败至关重要。如果仅仅是希望这两家加入，多给他们股份即可实现；可是同时，如果这两家在整个组织中占股过多，就会形成垄断和不公平竞争。  
对此，易观支付分析师王蓬博表示，原版本中提及的“两地三中心”方案（即在杭州、深圳分别建设一个处理中心，由支付宝和腾讯建设和托管）被否定。但由于方案遵循“共建、共有、共享”原则，由“网联”平台的各参与方自主共建。拥有数据、技术、人才等方面优势的支付宝和财付通，可由此获得股权优先权。  
央行接管后，两大巨头退居从属地位的局面或许在所难免。  
另外，主攻线下清算的银联，近些年也在积极布局线上清算业务。但“网联”的入局，势必会对其形成巨大的冲击。

**[价值趋势技术派](https://xueqiu.com/jiazhi_qushi_jishu)**2016-11-28 17:33

**[@一体同悲无缘大慈:](https://xueqiu.com/Die_ewige_Wiederkehr)**

终究不是一纸批文的对手这就缴械了==========================由央行牵头并入股的网联平台（简称“网联”），将按照新方案于近期启动，并预计于明年3月31日正式上线，届时支付机构将按照有关技术标准门槛分批接入。该平台的出现，或使支付宝和财付通退居从属地位。 “网联”是统一线上清算平...

[展开](https://xueqiu.com/5674464747/74975890)

马云曾今说啥都能献给国家，这么看其实还是有小心眼的。如果真的从底层技术开始所有知识产权都愿意给国家，凭啥支付宝不能称为网联呢？

**[芒格的小学徒](https://xueqiu.com/7268811699)**2016-11-28 17:45

**[@价值趋势技术派:](https://xueqiu.com/jiazhi_qushi_jishu)**

马云曾今说啥都能献给国家，这么看其实还是有小心眼的。如果真的从底层技术开始所有知识产权都愿意给国家，凭啥支付宝不能称为网联呢？

这个“网联”是很有价值的动向，它预示了国家建设互联网2.0的基本思路，即凡涉及重要的具有战略价值的基础大数据，其底层技术必须用国家队的，民企私企不用再做占据底层技术拥数据自重的梦。

2016-12-15 11:01

“量子通信”，“量子保密通信”是两码事  
  
量子通信，是真正意义上的超距通信。你在这边干什么，平均2.25亿公里外的火星人就能马上看到。  
  
量子保密通信，就是个现有通讯加把以现有技术加上未来几十年可行技术暂时无法破解的密钥。你在这边干什么，12.5分钟后火星人才能看到，只是中途那束传递信息的光或者其他什么电磁波就算被其他人截获了，他也无法还原这段视频。  
  
所以这条，连接北京、济南、合肥、上海等城域网络的全长2000多公里的“京沪干线”量子保密通信线路。意义不在于速度，而在于安全，大规模广范围的绝对安全信息传递。[怒了]  
  
再加上央行电子货币，懂伐？  
  
再加上全球修路办厂建电厂拉电网，电力人民币？！[为什么]电力电子人民币！！！

2016-12-21 09:57

《印度时报》27日报道称，莫迪在电台讲话中号召全国人民，“学习电子经济如何运作，学习使用电子银行和银行账户的不同方式，在你的手机上学习不同银行app的有效使用，学习如何在无现金的情况下经营生意。”他还说，“我理解这一运动所带来的不便，但要治愈一个困扰我们国家70多年的顽疾，治疗过程一定不会太容易。  
  
这也是拼了[很赞]印度一亿人民跳跃进入数字货币时代可期[加油]。至于死点人，破产几家公司那根本是毛毛雨啦[抠鼻]

2016-12-21 10:25

央行参事盛松成：货币当局为什么要发行央行数字货币

2016-12-12 21:53

30

****本文作者为中国人民银行参事盛松成教授、蒋乐，授权华尔街见闻发表。本文为作者个人观点，不代表华尔街见闻立场。****

自2009年比特币问世以来，各种形式的私人数字货币发展极为迅速，国际金融机构和技术公司都纷纷投入数字货币的研发，并已取得一定进展[[1]](https://wallstreetcn.com/articles/278985" \l "_ftn1" \o ")。在这一背景下，主要经济体货币当局纷纷开始研究央行数字货币，我国也不例外[[2]](https://wallstreetcn.com/articles/278985" \l "_ftn2" \o ")。究竟货币当局为何要发行央行数字货币？仅仅是为了取代现金吗？仅仅是为了节约现金印制成本吗？显然不是。因为现金的使用比例已逐年下降，替代现金的各种电子货币逐年增长，而研究和发行央行数字货币的经济成本和社会成本是巨大的，各国央行都不可能单单为了取代现金而发行央行数字货币。

****私人数字货币倒逼货币当局开始研究发行央行数字货币****

一时间，以比特币为代表的各种私人数字货币大量涌现、迅速发展、影响极大。世界上不少经济金融学家，包括中央银行家，都受到了极大冲击，甚至有人误认为私人数字货币有可能取代主权货币。笔者早在2013年底就明确指出，虚拟货币（包括私人数字货币）本质上不是货币，不可能取代主权货币[[3]](https://wallstreetcn.com/articles/278985" \l "_ftn3" \o ")。随着时间的推移，虚拟货币的非货币本质才逐渐被人们认识。

私人数字货币使用了一系列新的技术，这些技术对金融体系的渗透力极强，甚至对现代经济金融运行带来冲击。所以，为了维护货币体系乃至整个金融体系的稳定，货币当局也必须使用同等甚至更先进的技术和设计来研究发行央行数字货币。如果任由私人数字货币无序发展，这将对货币当局政策调控和经济金融体系带来严重冲击。

第一、私人数字货币分流、替代了一部分主权货币的使用，货币政策有效性将被削弱、传导机制将被扭曲。私人货币与主权货币是此消彼长的关系。随着私人数字货币使用范围不断扩大，主权货币使用量将逐渐下降，这将降低货币当局对主权货币的控制力。同时，货币政策调控对主权货币供应和流通的影响力也将下降、不稳定，这将削弱货币政策有效性、扭曲传导机制。如果私人数字货币被普遍使用但不由货币当局发行和调控，现代经济将因此失去一个重要的调控手段，经济将因为不受货币政策调节而无法正常运行。

第二、私人数字货币价值波动大，对金融稳定带来威胁。私人数字货币没有国家信用背书，不是真正的货币，其价格极易受到市场预期影响，波动率极高，市场流动性难以得到保证。随着私人数字货币使用范围和规模的扩大，单个私人数字货币风险演变为系统性风险的概率也将上升。

第三、私人数字货币供应量相对固定，难以适应现代经济发展需要。以比特币为例，系统设定的供应量上限与不断扩大的社会生产和商品流通之间存在矛盾。若其被广泛使用，这将造成通货紧缩，抑制经济发展。这也是金本位制崩溃的根本原因。

第四、私人数字货币缺少中央调节机制，难以满足现代货币体系稳定的需要。没有集中发行和调节机构即所谓的“去中心化”是私人数字货币普遍的特征。如果私人数字货币被全社会普遍接受，而货币当局无法通过中央调节机制稳定币值，这不仅会引起经济波动，也会动摇以国家信用为基础的货币体系。[[4]](https://wallstreetcn.com/articles/278985" \l "_ftn4" \o ")

第五、私人数字货币给反洗钱、反恐怖主义融资以及资本管控带来了挑战。私人数字货币普遍存在交易匿名和资金可跨国自由流动的特征，使得不法分子易于掩盖其资金来源和投向，个人易于规避换汇额度及外汇汇出境外的管理规定[[5]](https://wallstreetcn.com/articles/278985" \l "_ftn5" \o ")，这给洗钱、恐怖主义融资及逃避资本管控带来了便利。

第六、私人数字货币增加了消费者权益保护的难度。私人数字货币价格波动大、市场参与者几乎不受监管、用户资金安全缺乏保障以及交易不透明，因此私人数字货币交易容易发生诈骗、盗窃和造假等事件。这不仅使消费者权益缺乏保障，而且增加了监管当局取证调查的难度。[[6]](https://wallstreetcn.com/articles/278985" \l "_ftn6" \o ")

因此，为了应对私人数字货币快速发展对货币主权、货币政策、金融风险以及消费者权益保护等方面的冲击，货币当局清楚地认识到，国家应尽早开始研究发行央行数字货币。未来的央行数字货币应在国家信用的支持下，不断满足社会对货币使用技术的要求，成为被广泛认可的结算支付方式，这样货币当局才能扩大主权货币的使用，减少私人数字货币对货币体系以及整个金融体系的冲击。

****货币当局发行央行数字货币具有天然优势****

品类繁多的私人数字货币由不同私人主体创造或者发行，是去中心化的，并且具有不同系统设定和交易方式，竞争非常激烈。相比而言，央行数字货币由货币当局发行和调控，是中心化的，这使得货币当局发行央行数字货币具有天然优势。

第一、央行数字货币具有国家信用支撑，更容易被社会广泛接受。央行数字货币是主权货币的一种新型形态，具有和主权货币一样的法偿性和强制性。因此，社会可以像使用现有主权货币一样使用央行数字货币，无需对央行数字货币进行重新定价，更容易被社会广泛接受。而各种私人数字货币没有国家信用支撑，价格容易波动，在使用过程中则需要对其进行实时重新定价，这就是私人数字货币不会被社会广泛接受的原因。

第二、央行数字货币更有利于提高经济体系的流动性、降低交易成本。每种私人数字货币都有自己的系统设定，各系统之间面临交换和兼容的问题，这实际上增加了经济交易的复杂度。与之相比，具有国家信用支撑的央行数字货币采用统一的系统标准，交易便捷程度的提高会使交易总量上升，从而提高整个经济体系的流动性。

第三、央行数字货币有货币当局作为最后贷款人，不易发生货币挤兑危机。和其他形式的主权货币一样，货币当局是央行数字货币的最后贷款人，为货币稳定提供保障。而私人数字货币没有最后贷款人，一旦出现风险事件，货币供应商和交易平台很容易发生货币挤兑危机[[7]](https://wallstreetcn.com/articles/278985" \l "_ftn7" \o ")。

第四、央行数字货币供应量由货币当局调控，以满足现代经济发展的需要。与私人数字货币不同，一旦央行数字货币开始发行使用，货币当局便会根据经济发展需要调节央行数字货币供应量，从而保持央行数字货币的适用性，有利于现代经济的发展。

第五、货币当局能够通过中央调节机制维持央行数字货币币值稳定，保证现代经济正常运行。价值相对稳定是一种货币充当价值尺度和流通手段的前提条件，而且经济波动常伴随着币值波动，因此维持币值稳定也是现代经济正常运行的必要条件。

第六、货币当局必会通过技术手段增强央行数字货币的安全性，保护消费者合法权益。与私人数字货币截然不同，央行数字货币将会通过密码学算法保证数字货币用户安全，又要通过技术手段建立可控匿名机制，实现一定条件下的可追溯，以进一步增强央行数字货币安全性，由此保护用户交易安全[[8]](https://wallstreetcn.com/articles/278985" \l "_ftn8" \o ")。

****发行央行数字货币有利于货币政策的有效运行和传导****

与现有电子形式的本位币不同，未来的央行数字货币将可能是涉及区块链[[9]](https://wallstreetcn.com/articles/278985" \l "_ftn9" \o ")、移动支付、可信可控云计算、密码算法、安全芯片等技术的本位币。所以，未来的央行数字货币将从各方面有助于我国建设全新的金融基础设施，进一步完善我国支付体系，提升支付结算效率。更重要的是，央行数字货币最终可形成一个大数据系统，提升经济交易活动的便利性和透明度，这将有利于货币政策的有效运行和传导。

第一、央行数字货币有助于监管当局在必要时追踪资金流向，从而减少洗钱、逃漏税、逃避资本管制等行为。现有的数字货币技术不仅可以记录每笔交易，还可以追踪资金流向。与私人数字货币截然相反，监管当局可以采取可控匿名机制，掌握央行数字货币使用情况，补充现有的监测控制体系，从而增强现有制度的有效性[[10]](https://wallstreetcn.com/articles/278985" \l "_ftn10" \o ")。

第二、央行数字货币的信息优势可提高货币指标的准确性。央行数字货币形成的大数据系统，不仅有利于提升货币流通速度的可测量度，还有利于更好地计算货币总量、分析货币结构，这将进一步丰富货币指标体系并提高其准确性[[11]](https://wallstreetcn.com/articles/278985" \l "_ftn11" \o ")。

第三、央行数字货币的信息优势可以帮助监管当局更准确、更灵活地运用政策工具，追踪资金流向，以及全面监测和评估金融风险。在央行数字货币被全社会普遍接受并使用后，经济活动的透明度将大大提高，监管当局能够根据需要采集不同频率、不同机构的实时、完整、真实的交易账簿，这可为货币政策和宏观审慎政策提供巨大的数据基础。

第四、央行数字货币技术有利于货币政策的利率传导。现有的数字货币技术支持“点对点”支付结算，这可提高市场参与者的资金流动性。只有被全社会普遍接受的央行数字货币才能将这一优势辐射至不同金融市场的参与者，从而提高不同金融市场间的资金流动性和单个金融市场的市场流动性。这将降低整个金融体系的利率水平，使利率期限结构更平滑，货币政策利率传导机制更顺畅。

****综上所述，央行数字货币的创新是为了适应形势的发展、紧跟时代的步伐，保留货币主权的控制力，更好地服务于货币发行和货币政策，而不仅仅是为了取代纸币现金流通。（本文为作者个人观点，不代表供职单位意见）****

 作者单位：中国人民银行

[[1]](https://wallstreetcn.com/articles/278985" \l "_ftnref1" \o ") 例如创立于2015年9月的R3公司专门负责开发银行业区块链技术，招募的首轮团队包括了高盛、摩根、美国银行在内的42家银行。另一份公开资料显示，高盛已经开发了自己的“超级比特币”—— 一种名为SETL Coin的数字加密货币，用于交易股票、债券等资产。在同一年，被称作“华尔街女皇”的前摩根大通大宗商品全球主管Blythe Masters正在为其区块链创业公司Digital Asset Holdings融资。就在近期，区块链支付公司Ripple已经和国内一家银行达成合作，主要用于跨境支付结算。

[[2]](https://wallstreetcn.com/articles/278985" \l "_ftnref2" \o ") 我国中央银行从2014年起就成立了专门的央行数字货币研究团队。2016年2月，英国货币当局已经宣布发布央行数字货币RSCoin代码并进行测试。近两年，欧洲、美国、加拿大、日本以及荷兰等国家的货币当局纷纷开始对数字货币进行研究与实践。

[[3]](https://wallstreetcn.com/articles/278985" \l "_ftnref3" \o ") 盛松成、张璇：《虚拟货币本质上不是货币——以比特币为例》，《中国金融》，2014年第1期。

[[4]](https://wallstreetcn.com/articles/278985" \l "_ftnref4" \o ") 参见盛松成、张璇：《虚拟货币本质上不是货币——以比特币为例》，《中国金融》，2014年第1期；盛松成、翟春：《货币非国家化理念与比特币的乌托邦》，《中国金融》，2014年第7期；盛松成、蒋一乐：《央行数字货币才是真正货币》，《中国金融》，2016年第14期。

[[5]](https://wallstreetcn.com/articles/278985" \l "_ftnref5" \o ") 以比特币为例，交易和结算都是可自由跨国界的，在中国境内以人民币买入的比特币可轻松转移至外国交易平台，再以美元卖出，这是当下资本外流的一种新途径。

[[6]](https://wallstreetcn.com/articles/278985" \l "_ftnref6" \o ") 参见王信、任哲：《虚拟货币及其监管应对》，《中国金融》，2016年第17期。

[[7]](https://wallstreetcn.com/articles/278985" \l "_ftnref7" \o ") 参见王信、任哲：《虚拟货币及其监管应对》，《中国金融》，2016年第17期；徐忠、汤莹玮、林雪：《央行数字货币理论探讨》，《中国金融》，2016年第17期。

[[8]](https://wallstreetcn.com/articles/278985" \l "_ftnref8" \o ") 参见范一飞：《中国法定数字货币的理论依据和架构选择》，《中国金融》，2016年第17期。

[[9]](https://wallstreetcn.com/articles/278985" \l "_ftnref9" \o ") 区块链本质上就是交易各方信任机制建设的一个完美的数学解决方案，特点是利用数学算法建立交易双方的信任关系，不需要借助第三方，并且其数据库由所有的网络节点共享，所有人都可以共享和更新，并确认记录的交易是独一无二的（梅兰妮•斯万：《区块链-新经济蓝图及导读》，新星出版社，2016）。

[[10]](https://wallstreetcn.com/articles/278985" \l "_ftnref10" \o ") 参见盛松成、蒋一乐：《央行数字货币才是真正货币》，《中国金融》，2016年第14期；范一飞：《中国法定数字货币的理论依据和架构选择》，《中国金融》，2016年第17期；张正鑫、赵岳：《央行探索法定数字货币的国际经验》，《中国金融》，2016年第17期。

[[11]](https://wallstreetcn.com/articles/278985" \l "_ftnref11" \o ") 参见范一飞：《中国法定数字货币的理论依据和架构选择》，《中国金融》，2016年第17期。

2017-01-29 21:21

重磅：中国央行发行的数字货币已试运行，成全球首例。  
近期，中国央行关于发行数字货币动作频频，据媒体报道，央行法定数字货币的原型系统Demo有望在春节后推出。  
而在春节之前，关于数字货币的信息又有最新进展。根据财新网从多个权威渠道获悉，央行推动的基于区块链的数字票据交易平台已测试成功，由央行发行的法定数字货币已在该平台试运行，近期将成立研发中心持续完善；春节后央行旗下的数字货币研究所也将正式挂牌。  
  
这意味着在全球范围内，中国央行将成为首个发行数字货币并开展真实应用的中央银行，并率先探索了区块链的实际应用。  
  
据悉，2016年12月15日，数字票据基于区块链的全生命周期的登记流转和基于数字货币的票款兑付（DVP）结算功能已经全部实现，显示数字货币在数字票据场景的应用验证落地。目前已按计划完成了数字票据平台、数字货币系统模拟运行环境的上线部署，并与试点银行进行了网络联通。  
  
该项目的落地是由央行牵头并自主创新研发的重大金融科技成果。此举显示中国央行紧跟金融科技的国际前沿趋势，力求把握对金融科技应用的前瞻性和控制力、探索实践前沿金融服务的决心和努力。  
  
据一位参与研究的票交所人士透露，引入数字货币进行结算，可实现数字票据交易的资金流和信息流同步转移，从而实现DVP票款对付结算；同时通过区块链数字身份方案解决了不同金融机构间对用户重复KYC认证的问题等。  
  
“周小川行长希望利用数字票据平台这个项目测试数字货币、区块链以及其他成熟科技成果，并利用此项目集聚相关人才。”一位接近央行人士向财新记者表示。去年11月中旬，央行官网曾公布其直属单位招聘公告，其中招聘岗位包括从事数字货币研究与开发的人才，引发业内关注。  
  
近年随着区块链等新兴科技的兴起，法定数字货币成为各国央行的重点研究领域，英国、加拿大等多国央行都表示将涉足该领域，但目前尚无一家中央银行拿出落地的实际应用。今年初，欧洲央行（ECB）执行委员会成员伊夫•梅尔施（Yves Mersch）亦在公开场合表示，随着电子支付方式的兴起，公众对央行数字货币的需求也将增加。目前是研发央行数字货币架构的最佳时机。  
  
据了解，目前数字票据交易平台与上海票交所（下称票交所）是两个独立的交易平台。2016年12月，作为全国统一票据交易平台的票交所正式成立。两者的区别是，票交所是基于纸票电子化、ECDS电票票据交易的平台，而数字票据交易平台则是有限的参与方参与建设、测试的交易平台。  
  
前述人士透露，未来技术条件成熟时，数字票据交易平台将与票交所系统对接，最终数字票据交易平台应该是全国统一的“互联网+数字票据交易”的综合性金融服务平台。  
  
集合诸多科技亮点  
  
此次实践是法定数字货币在数字票据交易平台应用，运行范围是参与的商业银行，“将来如何应用于个人生活场景，还要继续探索。”一位参与研发该项目人士表示。  
  
据财新记者了解，该项目集合了诸多前沿科技亮点，包括数字货币、区块链、数字票据、智能合约等，自主创新研发了符合数字票据和数字货币等金融业务场景特点的底层联盟链，并在传统区块链技术基础上，对隐私保护、安全加密等设计了创新机制。在吸收区块链和智能合约等分布式技术优点的基础上，也针对其缺点和不适用性进行了特殊改造，解决了传统区块链智能合约不易升级，以及升级后繁重的历史数据迁移等问题。  
  
“在新的设计模式下可以避免类似TheDAO事件带来的风险，来解决业务逻辑升级。”前述知情人士表示。  
  
2016年6月17日发生了区块链历史上留下沉重一笔的攻击事件。区块链业界最大的众筹项目TheDAO遭到黑客攻击(被攻击前拥有1.5亿美元左右资产)，由于其编写的智能合约存在着重大缺陷,导致300多万以太币资产被分离出资产池转移给攻击者。  
  
实体货币和数字货币或长期共存  
  
2016年初，央行行长周小川在接受《财新周刊》专访时曾透露，人民银行深入研究了数字货币涉及的其他相关技术，比如区块链技术、移动支付、可信可控云计算、密码算法、安全芯片等；他还表示，未来实体货币和数字货币有可能会长期共存。  
  
其实早在2014年，央行就启动了对数字货币的研究，在周小川行长的推动下，成立了发行法定数字货币的专门研究小组，论证央行发行法定数字货币的可行性。2016年1月20日，中国人民银行数字货币研讨会在北京召开，会议明确了央行发行数字货币的战略目标，也是全球中央银行就法定数字货币的首次公开发声，引起业内诸多关注。央行认为，发行数字货币可以降低传统纸币发行、流通的高昂成本，提升经济交易活动的便利性和透明度，减少洗钱、逃漏税等违法犯罪行为，提升央行对货币供给和货币流通的控制力，更好地支持经济和社会发展，助力普惠金融的全面实现。  
  
2016年7月，央行启动了基于区块链和数字货币的数字票据交易平台原型研发工作，决定使用数字票据交易平台作为法定数字货币的试点应用场景，并借助数字票据交易平台验证区块链技术。数字货币研究所主要牵头负责底层区块链平台以及数字货币系统票交所分节点的研发任务。  
  
2016年9月，票据交易平台筹备组会同数字货币研究所筹备组，牵头成立了数字票据交易平台筹备组，启动了数字票据交易平台的封闭开发工作。  
各国央行对数字货币的青睐  
随着区块链技术的兴起，法定数字货币成为近年来各国央行的重点研究领域，各国央行正强力推行央行数字货币体系。  
除了瑞典之外，包括中国、日本、英国、加拿大、荷兰、澳大利亚、印度等国在内的全球多家央行已经陆续开启了数字货币之路。  
中国对待数字货币的态度可谓是热情主动：2014年，央行成立发行法定数字货币的专门研究小组，论证央行发行法定数字货币的可行性。2015年发布人民银行发行数字货币的系列研究报告，央行发行法定数字货币的原型方案完成两轮修订。2016年1月20日，央行召开的数字货币研讨会上，央行首次对外公开发行数字货币目标。11月，中国人民银行印制科学研究所公开招聘相关专业人员，从事数字货币研究与开发工作。2016年年底央行表示法定数字货币的原型系统Demo有望在春节后推出。  
日本央行对数字货币也表现出极大的兴趣，2016年12月份，日本央行联手欧洲央行启动了一个联合项目，研究能够作为市场基础的数字货币支持技术的潜在应用。两家央行计划在2017年公布主要研究结果。  
加拿大央行则表示在2014年起就开始密切关注两种不同类型的数字货币：一种是由央行背书的本国数字货币，另一种是没有背书的加密数字货币，如比特币。且加拿大央行的研究人员近年来也发表了多篇工作论文，探讨中央银行发行数字货币对社会福利等方面的影响。2016年年中时加拿大央行表示他们正在开发一个基于区块链技术的数字加元，据英国《金融时报》表示，这个数字货币被称为CAD-COIN。  
英国央行于2016年1月表示正在考虑是否发行央行数字货币，并于8月发表工作论文《中央银行发行数字货币的宏观经济学》，从理论上探讨了中央银行发行数字货币对宏观经济可能带来的影响，并开始招募负责推动发行基于区块链的数字化英镑的研究主管。此外，英格兰银行还发布了结合了新分布式账本技术优势和传统中心化管理货币形式的RSCoin，因此它又被称为‘混血’数字货币。该混血系统比美国停止使用金本位制度更加具有颠覆性，RSCoin的灵活性和监管性是新旧结合的最好范例。  
澳大利亚央行也是探索数字货币和区块链技术的先行者，澳大利亚储备银行在2016年2月就宣布正对数字货币和区块链支付系统进行研究，并提议全面发行数字货币澳元。

# **央行数字货币系统Demo明年要推出了，区块链真的要起飞了吗？**

[卢晓明](http://36kr.com/user/1633539537) • 2016-12-29 • 行业新闻

数字货币是大势所趋，央行已经不做不行？

区块链技术在风口上吹了一年多，央行这次系统的落地会不会给这波风口加码？

据[21世纪经济报道](http://epaper.21jingji.com/html/2016-12/29/content_53683.htm" \t "http://36kr.com/p/_self)，北京一家参与了有关区块链研究的外部咨询的公司负责人表示，央行法定数字货币的原型系统Demo有望在明年推出。此前，央行发行法定数字货币的原型方案已完成两轮修订。

这意味着，部署了至少一年的央行数字货币系统，终于要落地了。

### **先在票据领域试点，再扩大范围**

据上述区块链技术开发公司负责人表示，这个系统会现在票据领域试点，成功之后才会推广至货币领域，在该领域也同样会先小范围试点，再扩大。

票据是代表一定数量[货币请求权的有价证券](http://wiki.mbalib.com/wiki/%E7%A5%A8%E6%8D%AE" \t "http://36kr.com/p/_self)，即[货币证券](http://wiki.mbalib.com/wiki/%E8%B4%A7%E5%B8%81%E8%AF%81%E5%88%B8)，其代表一定数量货币请求权，可以在法定的范围和条件下流通。因此，它有汇兑、支付、结算和信用等基本功能。可以看到，票据虽然不是货币本身，没有法币所具有的的强制通用效力，但具有跟货币非常像的特性。

同时，今年以来相继[爆出来的数起“](http://money.hexun.com/2016-04-11/183224237.html" \t "http://36kr.com/p/_self)[票据案](http://money.hexun.com/2016-04-11/183224237.html)”，票据被伪造或挪作他用，涉及金额高达数十亿。

为了解决类似问题，央行设计了基于区块链的票据交易平台来解决这个问题，在未来两到三年内纸质票据全部退出市场。采用分布式记账的区块链技术，能够完整的纪录所有交易和所有去向，不依赖于单一的交易平台，无法篡改，保证了交易的真实；同时可以消除信息不对称，去中介化。

据中国人民银行科技司副司长兼中国人民银行数字货币研究所筹备组组长姚前表示，如果在系统中引入数字货币，就可以实现在链上直接清算，简化了票据交易流程。简单交易无需第三方的信用担保，不用担心交割问题，没有交易对手方的风险。缺点则是，因为交易中是全额清算，对参与方的资金占用较多，需要一定的措施来提高资金利用效率。（具体可以参考《数字票据交易平台初步方案》）

### **数字货币具体体系构想**

可以看到，数字货币的引入主要是出于安全和提高效率的考虑。

在今年年初的中国人民银行数字货币研讨会上，会议就表示，发行数字货币可以降低传统纸币发行、流通的高昂成本，提升经济交易活动的便利性和透明度，减少洗钱、逃漏税等违法犯罪行为，提升央行对货币供给和货币流通的控制力，更好地支持经济和社会发展，助力普惠金融的全面实现。

据报道，[央行早在2014年就成立专门研究团队](http://news.xinhuanet.com/fortune/2016-01/22/c_128655193.htm)。此前，央行发行法定数字货币的原型方案已完成两轮修订。

至于这套体系的具体核心要素，姚前今年8月曾在《中国金融》中[撰文介绍过](http://business.sohu.com/20160831/n467038768.shtml" \t "http://36kr.com/p/_self)，具体而言，该体系包括以下几项主要构成要素：

央行数字货币私有云：用于支撑央行数字货币运行的底层基础设施。

数字货币：由央行担保并签名发行的代表具体金额的加密数字串。

数字货币发行库：人民银行在央行数字货币私有云上存放央行数字货币发行基金的数据库。

数字货币商业银行库：商业银行存放央行数字货币的数据库，可以在本地也可以在央行数字货币私有云上。

数字货币数字钱包：指在流通市场上个人或单位用户使用央行数字货币的客户端，此钱包可以基于硬件也可以基于软件。

认证中心：央行对央行数字货币机构及用户身份信息进行集中管理，它是系统安全的基础组件，也是可控匿名设计的重要环节。

登记中心：记录央行数字货币及对应用户身份，完成权属登记；记录流水，完成央行数字货币产生、流通、清点核对及消亡全过程登记。

大数据分析中心：反洗钱、支付行为分析、监管调控指标分析等。

现在，中国的电子支付已经十分普遍了，在用户体验上跟数字货币非常接近。法定数字货币的引入，可能会一定程度上会降低对第三方支付机构作为支付转接机构和支付通道的依赖，但具体要看数字货币最终落地的方案。

### **区块链行业即将起飞？**

当然，这个消息最利好的，还是区块链行业。

向来对政策变动十分敏感的股民们先来了个[快速反应](http://money.163.com/16/1229/10/C9EQNNAH002580S6.html)，今日早盘，区块链概念股走强，飞天诚信率先涨停，赢时胜、御银股份和恒生电子等走高，这些公司都开始部署或者研究区块链技术。

不过，从实质上来说，央行数字货币的推出，对行业有没有推动作用？

OKCoin币行网副总裁段新星表示：“在技术领域创新中国走向国际前沿，政府的高度重视也有利用区块链技术的发展和更好的应用于实际场景中。在未来区块链一定能最大程度上的造福与人类。

维优元界创始人初夏虎则认为，这虽然是个利好，但谈不上鼓励和刺激，因为数字货币是大势所趋，央行已经不做不行。

确实，随着区块链技术的兴起，不仅中国，英国、加拿大等国家的央行都表示将涉足该领域，并提出了自己方案。同时，不少创业公司也已经开始了在数字货币和基于区块链跨境结算，这样的系统与其掌握在第三方手中，基于安全的考虑，央行有必要推出官方的系统。

初夏虎还表示，央行的举措只是说明了这确实是个趋势，对于行业本身来说，区块链技术的应用就像是“1万米的长跑，你只跑了100米，你接着跑就好了”。他相信，区块链行业即将起飞。

=======================  
印度巴基斯坦委内瑞拉那些只是废个旧钞，中国是直接废纸币啊，其实现在也差不多了，不是支付宝就是微信，再不刷卡，我都经常兜里不揣钱就去逛街[可怜]

2017-04-30 08:51

无现金时代支付入口争夺升级 银行主动向移动端迁移2017年04月30日00:20 经济观察报  
  
　“无卡无现金”时代支付入口争夺升级  
　　李意安  
　　支付圈最近发生了两件大事：4月17日，交行首次推出“手机信用卡”产品，成为业内第一家信用卡产品全面迁移至移动端的银行，从信用卡的发行审核到使用，全生命周期均在线上进行；紧随其后，4月18日，在蚂蚁金服主导下，首批15家联盟成员一起在杭州成立了全球首个无现金联盟，蚂蚁金服同时宣布，未来两年将提供60亿元来帮助联盟成员推进无现金进程。  
　　从市场反馈来看，二者双双首战告捷：手机信用卡在两个月的试运行中，先后获得83.3万的客户申请，30秒内81%的客户得到批核，三分钟内的处理率达到99%，批核率高达到70%，甚至高于传统实体信用卡的批核率；而无现金联盟成立之后，一天内就获得了超过1000家企业的申请加入，其中零钱支付比例最高的地方——菜市场显得尤为积极。  
　　在某种意义上，这看似风马牛不相及的两件事件正向着同一个目标推进——前者试图消灭实体信用卡，后者试图消灭现金。当信用卡和现金都消失，账户就成为了唯一的支付入口，产业升级由此实现。“支付是刚需，随着实体信用卡和现金逐步被取代，各家机构从支付方式之间的竞争逐步转变为对支付入口的争夺，这意味着支付的竞争形态已经发生了变化。在此背景下，银行们也逐渐开始意识到了自建账户的重要性，并尝试主动向移动端迁移。”一位第三方支付副总裁告诉经济观察报，一场看不见硝烟的入口争夺战已经拉开序幕。  
　　“无现金+无卡”时代  
　　蚂蚁金服相关负责人告诉经济观察报，出于对低碳运营和提升商业效能的愿景，未来两年，蚂蚁金服将提供60亿元来帮助联盟成员推进无现金进程，希望用五年的时间推动中国社会进入无现金时代。  
　　无独有偶，早在2015年，微信支付就曾发起过一个“无现金日”的概念。当年9月，微信支付牵头，和10家银行、全国11个行业的8万门店一起在8月8日发起了全球首个“无现金日”。微信支付也自此确定了面向服务商全面开放的策略以及自身“连接器”的角色定位：只做基础方案，将市场留给第三方开发者、服务商、系统商。  
　　因而，事实上，对‘无现金’喜闻乐见的人除了微信、支付宝，也包括商家、服务商，甚至银行。多方推动下，无现金的趋势已然不可逆。  
　　“在一二线城市，把现金和信用卡作为备用选项已经成为许多消费者的常态。对大多数银行而言，已经接受了‘无卡’、‘无现金’的趋势，因此，许多银行也在主动进行一些策略上的调整和产品上的优化。交行的这款手机信用卡产品以及之前京东白条与银行的合作产品都可以看做一种尝试的路径。”一家股份制商业银行信用卡中心的产品经理告诉经济观察报，而真正敏感的核心关键点在线下刷卡转移到线上扫码的过程中，支付入口将成为兵家必争之地。“无现金意味着所有支付都从线上走，对银行而言，流量入口到底是自己的场景，还是第三方的场景，区别很大。对信用卡中心来讲，当然还是希望这些消费直接来自自己的应用场景，而非来自支付宝、微信等体系。这也是银行卯足力气要做自己的‘无卡产品’的原因。”  
　　上述产品经理认为，通过自身场景所获取的流量能给银行带来更强的主动性：“一方面可以明确看到用户的具体消费金额、商户编码，更有利于风控，另一方面，也更有利于大数据的累积和精准推送。但现阶段而言，无论是支付宝还是微信，对于用户商户编码等用户消费信息都是不对银行开放的。”  
　　而交行信用卡中心总经理王卫东则补充认为，无实体卡片的“手机信用卡”亦是应对行业同质化竞争的一种产品策略。  
　　“信用卡行业经过这么多年的发展，内部的竞争也越来越激烈，这俨然已经是一片红海，同质化是客观存在的现象。通过这次‘手机信用卡’的创新，信用卡中从一个发卡商的职能蜕变为一个信用卡的帐户提供商、一个消费信贷的提供商、一个移动互联网平台的提供商、一个移动支付的提供商。”王卫东表示，“传统信用卡通常要经过两个礼拜的审核周期才能把卡寄给用户，激活后才能使用。而纯线上手机信用卡可以在申请之后可以极速发卡，秒发秒用。而且本身就是一个账户，同时这个账户上还给你一笔贷款。这个手机上的虚拟卡可以绑定交通银行(6.020, 0.00, 0.00%)的买单吧支付、银联的云闪付、支付宝、微信、Applepay、华为pay、小米pay等等，实体信用卡拥有的功能它全有。”  
　　王卫东向经济观察报表示，未来随着存量信用卡的逐步到期，不排除将实体信用卡全面虚拟化的可能。  
　　卡中心必选项：强化APP入口  
　　“无卡时代，真的到来了。”在“手机信用卡”发布的当下，王卫东如此感慨。  
　　而事实上，尽管在手机端发行信用卡全线产品的银行并不多，但拥有信用卡独立APP的银行已经不在少数。除交行以外，中行、招行、中信、浦发、民生、平安、光大等都已经用了信用卡的独立APP。  
　　就在不久前，银联总裁时文朝就曾撰文指出：未来将“很快将看不到实体的卡片”。“从有卡到无卡，反映的是从以卡片为基础深化到以账户为基础的支付内涵的变化。“支付的移动化会越来越普及，也将越来越深化。手机早就超出便携式即时通讯工具的范畴，成为个人信息处理系统终端，真正成为人的体外器官，须臾不愿离身。在下个浪潮到来前，围绕这个终端去分食‘国民总时间’是各类商业行为考虑的出发点，支付也概莫能外。这已是个现实性的趋势。”  
　　王卫东告诉经济观察报，在这款产品发行之前，交行和包括Visa、万事达和银联在内的多家卡组织进行了沟通，信用卡业务向移动端的迁移已经成为行业共识。  
　　王卫东认为，和传统的互联网平台相比，银行的信用卡中心依然具备优势。“互联网企业最渴求的是流量，为了流量不惜血本地烧钱，而我们已经坐拥5300万个信息健全、数据完整、经过风控把关的、有粘性的用户。同时具备一定的品牌积累，信用卡最知名的品牌‘最红星期五’拥有广泛的拥趸，并且融入了相当的金融场景，覆盖一百多个城市的热门商圈，，包括加油、超市、餐饮在内的五万多家商户优惠。因此，交行买单吧app上线一年多，我们就累计了2300万的客户。”  
　　在王卫东看来，强化APP入口的策略在于用户体验做减法的同时，风控策略要做加法。“从底层技术来讲，因为这种改变，我们的底层风控现在是13，277个策略规则、745个征信字段运用、32个评分卡模型、并且跟人民银行征信系统、公安部的身份信息系统等15家外部主流数据源进行合作。基于这个策略系统进行实时发卡、信用卡额度和消费信贷的审批。”  
　　事实上，如果仅仅观察信用卡市场的规模体量，这个蛋糕一直在膨胀。2016年末，全国信用卡累积发卡是6.3亿张，16年比15年发卡增长的速度是18.9%，而过去五年当中，它的复合增长率是18.2%。全国信用卡交易金额去年的增长是16.8%，全国信用卡行业的授信总额，去年已经达到9.14万亿，同比前一年增长是29.1%。另一方面，根据iResearch艾瑞咨询统计数据显示，2016Q4第三方移动支付市场份额中，支付宝与财付通共占据92.0%份额，其中支付宝占比55.0%，财付通占比37.0%。  
　　“虽然看上去支付宝和微信垄断了很大的市场，但是目前扫码付等移动支付产品的交易贡献主要还是来自一二线城市，在三四线城市甚至更偏远的地方，还有大量的长尾市场等待挖掘。这是一个数十万亿计的市场。随着市场的逐步发展和渗透，相信会有越来越多的参与方加入，包括银行，这是一种健康的发展态势。蛋糕在变大，大家都在增长，即使未来支付宝、微信的市场份额出现了下降，也是十分正常的现象。”一位接近支付宝的人士告诉经济观察报。

2017-04-30 08:56

中国离无现金社会还有多远？  
商业周刊/中文版2017-04-23  
　撰文：孟添（上海大学科技金融研究所副所长、上海市互联网金融行业协会副秘书长）  
　　五年后，中国是能够实现无现金社会的  
　　因为“天时、地利、人和”已皆俱  
　　2017年两会，大家对无现金社会议论纷纷。人大代表也有相关提案提出。支付宝表示“五年推动中国进入无现金社会”，而福耀玻璃集团掌门人曹德旺认为“需要一两百年。”对此讨论，我认为五年后，中国是能够实现无现金社会的。  
　　首先，要对无现金社会有一个认识。无现金社会并不是消灭现金，而是将无现金作为主流支付方式的社会。其内涵也非常丰富，无现金包括互联网支付、银行卡、二维码支付、NFC（近场支付）等各类支付工具的应用。在不久的将来，中国能够实现无现金社会，因为“天时、地利、人和”已皆俱。  
　　“天时”  
　　所谓“天时”，无现金社会是符合历史潮流的。孙中山先生说过“历史潮流浩浩荡荡，顺之者昌，逆之者亡。”从历史发展的角度看，货币的形态本身就一直在不断变化演进。随着新技术不断发展，无现金社会是货币形态演变的必然趋势。就好像铜钱替代贝壳，纸币替代银元，最终电子货币将替代纸币成为货币目前能够预知的最终形态。  
　　实际上，许多国家的央行都在关注与研究电子货币。2016年11月，瑞典央行称考虑在两年内作出是否发行“电子克朗”的决定，并对禁止流通实物现金进行评估，可能成为全球第一个完全使用“数字现金”的社会。根据瑞典央行的数据，该国非现金交易平稳增长，比过去10年高出10%，达到了92%的高峰。  
　　  
印度日前宣布废除500和1000元卢比纸币，民众排长队取钱  
　　印度同样也在不遗余力地推广“无现”交易。尽管目前现金交易在印度仍然是主流，印度财政部推出一揽子涉及民生领域的优惠政策，鼓励民众使用电子支付的方式。印度领导人在社交网站上发文称，数字交易有望终结腐败，希望更多人转向数字交易。英国央行也表示，正在研究考虑是否由央行来发行数字货币，目前研究工作还处于初级阶段。美联储正在不断深入分析数字货币，研究其特性、影响、背后的技术支持等。新加坡正在适用于跨境交易的电子货币试验项目。2016年，中国人民银行印制科学研究所开始招募数字货币研发人员。全球各国的无现金社会都在加速发展。数据显示，在2008年至2012年间，全球现金交易数额为11.6万亿美元，增幅仅有1.75%；而同期的非传统支付方式交易数额增加近14%。这个历史潮流已经滚滚涌来，势不可挡。  
　　“地利”  
　　所谓“地利”，非银行支付机构的“鲇鱼效应”使得中国在无现金支付领域拥有了活跃的市场主体，这大大加快了相关技术更迭与无现金化的速度。西方发达国家由于拥有成熟与完善的金融体系，银行与相关金融机构日趋保守，在无现金支付方式上主要停留在银行卡支付，其他移动支付创新乏善可陈。而随着中国移动互联网的飞速发展，第三方支付机构的迅猛壮大。目前中国人民银行发放了267张支付牌照。2010年以来，中国第三方支付市场的交易规模保持50%以上的年均增速迅速扩大，高速发展的7年，已经成为全球的领跑者。2016年中国第三方支付总交易额为57.9万亿人民币，相比2015年增长率为85.6%。其中移动支付交易规模为38.6万亿元，约为美国的50倍。第三方支付市场已成为中国互联网金融领域最为成熟的行业，并作为基础服务广泛应用于各行业。  
　　  
　　特别是第三方互联网支付机构的异军突起，支付宝、财付通已经占据70%市场份额。而银行卡收单业务也在被第三方支付不断蚕食。根据中国银联统计数据，2014年起第三方机构的线下交易量已经超过银行，收单业务的优势已经朝着第三方机构的移动端快速转移，几乎所有市场主要银行都出现了收单商户数、交易量和收益的滑坡。在互联网支付领域，非银行支付机构已经成功逆袭，正倒逼银行机构积极应对与寻求创新。而金融机构的反击也大大加速了整个市场的发展。  
　　最有代表的例子是2015年12月12日，银联联合20多家商业银行推出“云闪付”移动支付品牌。此后，在此品牌下陆续推出ApplePay、SamsungPay等支付产品。不同于第三方支付机构的二维码支付，这种基于NFC、HCE和Token技术的支付方式，依靠安全便捷的支付体验、庞大的苹果等品牌手机用户群、不断完善的非接受理环境也在大大加快中国无现金化的速度。  
　　“人和”  
　　所谓“人和”，中国网民众多，具有广大的市场空间与普惠需求，基于互联网的移动支付消费习惯与认同容易形成，这是无现金社会快速发展的市场基础。早在2012年，中国成为全世界第一个国家移动互联网网民大于PC互联网网民的国家，截至2016年12月，中国网民规模达7.31亿，全年共计新增网民4299万人。互联网普及率为53.2%，较2015年底提升2.9个百分点。手机网民规模达6.95亿，较2015年底增加了550万人。  
　　网民中使用手机上网人群的占比由2015年的90.1%提升至95.1%，提升5个百分点，网民手机上网比例在高基数基础上进一步攀升。预计2017年规模将达7.72亿，互联网普及率将达55.9%；手机网民规模达7.39亿，网民中使用手机上网人群的占比由2016年的95.1%提升至97.8%。数据显示，2016年中国移动支付业务共发生257.1亿笔，同比增长85.82%，移动支付金额也达到157.55万亿元；网上支付业务依然是非现金类支付的主力军，共发生461.78亿笔，同比增长26.96%，金额更是达到2084.95万亿元。基于这样的群众基础与用户习惯，无现金作为主流支付方式指日可待。  
　　  
　　综上所述，中国在不久的将来能够实现无现金社会。特别在五年后，将是一个引爆点。因为到2022年，00后（2000年至2009年出生的人）将步入社会开始工作，85后（即1985年至1989年出生的人）已经工作15年，和90（1990年至1999年出生的人）一起，当他们开始逐步成为主流人群，他们习惯的无现金支付方式将成为主流的支付方式，他们对无现金化的认同将成为社会的主流认同。  
　　“东风”  
　　那么，中国实现无现金社会是否存在障碍？有人认为，电子支付的风险是推行无现金支付的一大障碍。也有人认为，中国疆域辽阔，发达地区和欠发达地区在无现金支付方面的差距将是推行无现金社会的又一大障碍。  
　　从风险管理的角度看，任何的创新都不可避免地伴随着风险，对于颠覆式的创新，我们要给予更多的宽容与鼓励，同时也要做好监管坚守底线。关键不在于有没有风险，而是有没有识别与控制风险的能力与技术。金融的本质就是风控，所以存在风险不应成为推行无现金支付的阻碍。随着移动支付的不断发展，传统的一些监管方式也正在向技术型监管转型。当下，我们更需要对推进“无现金社会”建设加深理解，统一认识，达成共识，形成标准。  
　　从地区差异的角度看，只要加大在不发达地区基础设施建设的力度，逐渐培养消费者支付习惯，不发达地区推进无现金支付的效应会比发达地区更快，西藏连续五年移动支付渗透率全国第一就是最好的例子。国外移动支付发展最快的也在非洲、南美等地区。不发达地区的这种发展是跨越式的。因为原来比较薄弱，在接受新技术与新变革时反而更容易适应。  
　　  
　　中国要进入“无现金社会”，天时、地利、人和皆在，只欠东风。这东风就是，无现金社会的早日实现需要政府进一步加强引导，推进基础设施建设，做到创新与规范的平衡，构建行业健康发展的生态圈，形成有序竞争的行业格局。市场的力量是巨大的，但在金融领域更要注重有序。  
　　无现金社会的实现将对中国的发展意义重大，最直接的好处是给人们的生活带来便捷性，可以大大提高效率。比如在公共服务、社会保障领域实现移动支付，就可以真正让群众少跑路少排队。然而，重大的意义莫过于数据的有效积累。  
　　不同场景下大数据的积累，如果结合人工智能进行相关分析与运营，能够带来巨大的无法预见的价值。同时这样的积累也为打通整个社会条块分割的数据源提供了条件。如果能够结合区块链技术，特别是在公有链方面，对国内整个征信体系的建设具有重要价值，比如实现电子化交易记录的不可逆与可追溯，精准打击各类经济犯罪、反洗钱活动等。此外，征信成本居高不下是中国中小企业融资难、融资贵问题长期以来无法解决的症结所在，而无现金社会或许能够带来一丝新的曙光。  
　　（本文内容不代表彭博编辑委员会、彭博有限合伙企业、《商业周刊/中文版》及其所有者的观点。）  
　　编辑：马珊珊、格根坦娜

2017-04-30 09:20

这文重点说的是，M0的占比会越来越低，因为“无现金”，而替代路径：如果银行卡成为主流的电子支付手段，对应的应该是M1；如果第三方支付账户中的货币基金，如余额宝、零钱宝等成为主流的支付工 具，则对应的是M2中的非存款类金融机构存款；如果信用卡和蚂蚁花呗、苏宁任性付等消费金融产品成为主流的支付工具，则并不在央行的货币统计口径之中。  
这样就会造成大量的表外，造成恶性通胀等问题，但并非无解，答案就是区块链数字货币，因为其不可篡改性（国家级要篡改控制超过51%的节点想也不可能，或者说有能力做的国家或组织不会傻到去做，真做了就是开战的代价）和可追溯性。当然届时可能又产生出新的问题，新的风险，但总体是利大于弊的。  
  
===================================================

http://www.sohu.com/a/137077029\_398806

# **无现金社会的潜在挑战，央妈准备好了么？**

2017-04-28 22:13

今天与时代财经的一位朋友讨论无现金社会的问题，谈到欧洲政府部门也在力推无现金社会的到来，看来，在全球范围内，无现金社会已经成为一种共 识。这里就自然衍生出一些问题，随着现金使用比例的下降，社会的货币供应结构会发生怎样的变化？对央行的货币政策又会产生怎样的影响？对普通人而言，除了 支付手段的便捷化和多样化以外，无现金社会还有其他的显著影响吗？

不妨逐一来看一下。

1、无现金社会，可能会是央行货币统计口径失效

谈到货币供应，一般有三个概念，分别为M0、M1和M2，三者的关系如下：

M0=流通中的现金，

M1=M0+单位活期存款，

M2=M1+定期存款+储蓄存款+非存款类金融机构存款+住房公积金存款。

一般认为，M0是狭义的货币供应；M1是现实的货币供应，可直接用于支付；M2是潜在的货币供应，因为其中的定期存款和储蓄存款不能进行即时的购买力。

在无现金社会中，M0的占比会越来越低，该指标也就越来越不重要。那谁的占比会增加呢？M1还是M2？

关键是替代性的支付工具是谁？如果银行卡成为主流的电子支付手段，对应的应该是M1；如果第三方支付账户中的货币基金，如余额宝、零钱宝等成为主流的支付工 具，则对应的是M2中的非存款类金融机构存款；如果信用卡和蚂蚁花呗、苏宁任性付等消费金融产品成为主流的支付工具，则并不在央行的货币统计口径之中。

基于目前的趋势来看，包括信用卡在内的消费金融产品成为主流支付工具的概率更大，而此类工具并未被统计到央行货币口径之中，会使货币统计口径与社会中的真实购买力脱节，统计口径小于真实购买力。

举个例子，央行统计的即时购买力M1有50万亿元，而考虑到大量的消费金融产品（尤其是其分期功能）的存在，社会真实的购买力可能在60万亿元左右，这种真实货币供应的增大可能会带来潜在的通胀风险。

2、央行数量型货币政策的挑战

央行的货币政策，大致分为调整利率的价格政策和调整货币供应量的数量政策类。央行调整货币供应量，一般通过调整基础货币和货币乘数两个手段进行，其主要媒介 是存款性金融机构，影响的主要是银行存款。而在无现金社会中，真实的购买力隐藏在消费金融产品而非银行存款中，便会导致央行的数量型工具在特定情境下失去 效果。

3、对普通人还有哪些影响？

对普通人而言，无现金社会的直接影响在于支付的便捷性和多样性。但也有潜在风险，那便是若央行不能正确应对无现金社会对于货币供应统计和货币政策传导的挑 战，那么这种挑战便会传导至普通民众身上，不仅带来通胀问题，还会因货币政策的失调影响资产价格，届时，你的股票或房产价格也许会坐过山车。

综上，无现金社会的到来，不仅仅是支付工具的普及和安全性本身的问题，还涉及到央行货币政策的基础性调整和变革，是一个循序渐进的过程，是一个全盘推进的过程，很难一蹴而就的。

2018-01-14 09:31

调整观点，国家信用担保的数字货币不是最优选，但远比基于共识的去中心电子货币靠谱，ico全扯蛋，btc和其他几个主流币种现有机制对于蠢货和坏人的制约太少，但不妨碍（可能有人）炒了赚钱。  
一句话，“不要钱”这是个以实具名的过程，光靠好人和和气气是推动不了的，真正的超国家的信用交易单位必须有超国家的强有力的某种信用体作为背书。触动利益比触动灵魂更难，中间必见血火，拭目以待[跪了]。

2018-01-17 09:31

如何发行自己的虚拟币，10分钟搞定ICO，走上人生巅峰

================================

https://zhuanlan.zhihu.com/p/32796998



# **10分钟搞定ICO**

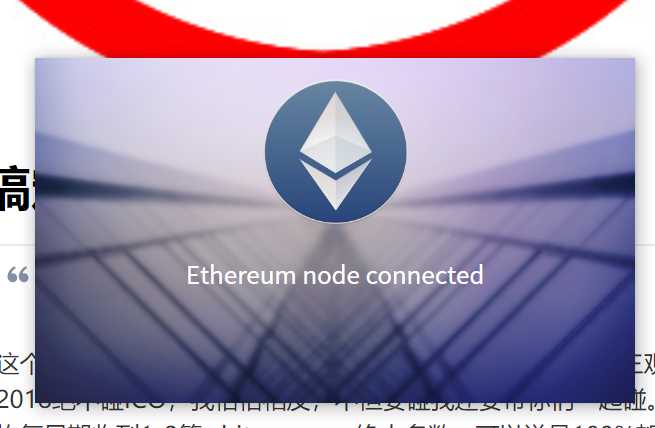
[IMG_257](https://www.zhihu.com/people/liu-yi-jie-84)[刘易杰](https://www.zhihu.com/people/liu-yi-jie-84" \t "https://zhuanlan.zhihu.com/p/_blank)

7 天前

我本来是不想写这个的，昨天看了曹政的文章《不要试图挑战人性》，感触挺深的，曹大说他2018绝不碰ICO，我恰恰相反，不但要碰我还要带你们一起碰。ICO现在简直是太火了，我平均每星期收到1-2篇whitepaper，绝大多数，可以说是100%都是忽悠人的，我不当韭菜也会有别人被收割，莫不如我今天就给你们指条路——干嘛参与别人的ICO啊？你可以自己搞啊！

废话不说，首先去以太坊下载一个钱包。[Ethereum Project](http://link.zhihu.com/?target=https://ethereum.org/" \t "https://zhuanlan.zhihu.com/p/_blank)

下载完了安装，你的界面应该是这样的：

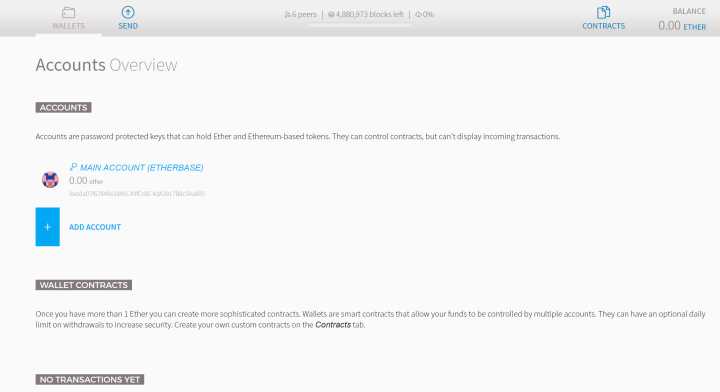


官方的这个钱包bug非常多！经常打不开，而且和网络sync区块链的时候经常会有各种各样的问题……不过，如果你能侥幸安装成功并且同步成功。

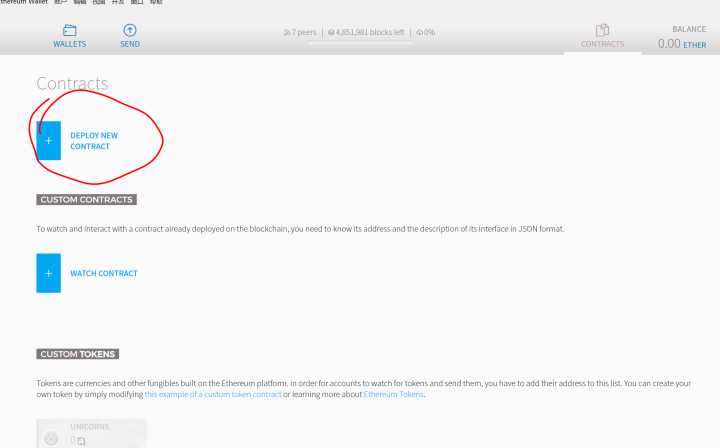
恭喜你，你已经成功克服了你ICO道路上最大的技术难关，胜利在望，会所嫩模在向你招手！



好，打开钱包，界面应该是下面这样：



看到右上角那个“CONTRACTS"按钮了吗？轻轻点一下：



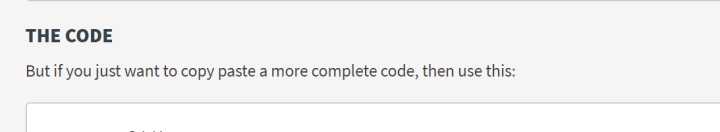
再点这个Deploy New Contract:

然后，打开这个网站：[Create a cryptocurrency contract in Ethereum](http://link.zhihu.com/?target=https://www.ethereum.org/token" \t "https://zhuanlan.zhihu.com/p/_blank)

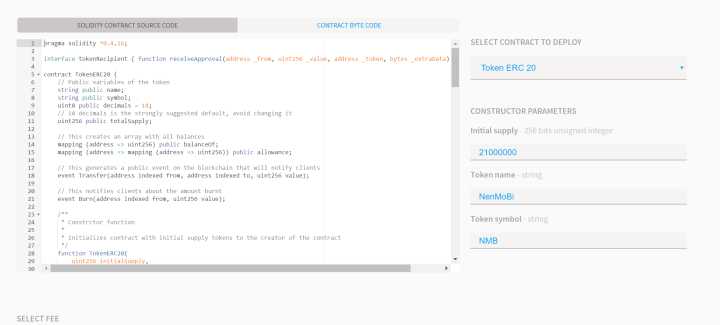
不懂英文？没问题

看不懂代码？无所谓

看到**THE CODE**了吗？



把下面的代码copy下来，然后粘贴到你的以太坊钱包里，再右边下来菜单里面选那个Token ERC 20 ，你会看到的界面大概是这个样子：



这个时候系统会让你输入三个参数：

Initial Supply:你要发行多少个币呢？ 我填了2100万个，致敬比特币嘛！

Token Name:咱发行的币叫什么名字呢？我本来想叫刘易杰币……后来一想这太不中本聪了……不忘初衷，ICO骗钱为的就是会所嫩模，就叫嫩模币吧！

Token synbol：就是币的符号，比如比特币是BTC，以太坊是ETH，咱们嫩模币当然是NMB了！

然后下面有个蓝色的deploy,点了这个deploy,嫩模币就正式发布了————这里有个条件，就是钱包里要有少量的ETH，作为执行合约的Gas，大概是0.00几个ETH就够了，也就几美元到几十美元的事儿。

好了。

完成了。

如果你完成了如上所说的步骤的话，那么你成功的在这个世界上，基于以太坊网络，创造了一种新的加密货币————如果这破玩意儿能称为加密货币的话……

我大概解释一下啊这玩意儿是啥：以太坊网络和只能合约，支持一个use case就是用户可以通过以太坊来发行自己的"Token", Token是什么呢？你可以理解为现实生活当中的“积分”，对，比如加油站洗车店会员卡积分，楼下发廊Tony老师让你办的冲2000送1000的美发会员卡，奶茶点送你的盖满10个张送一杯的集戳卡，幼儿园老师给小朋友的小红花……

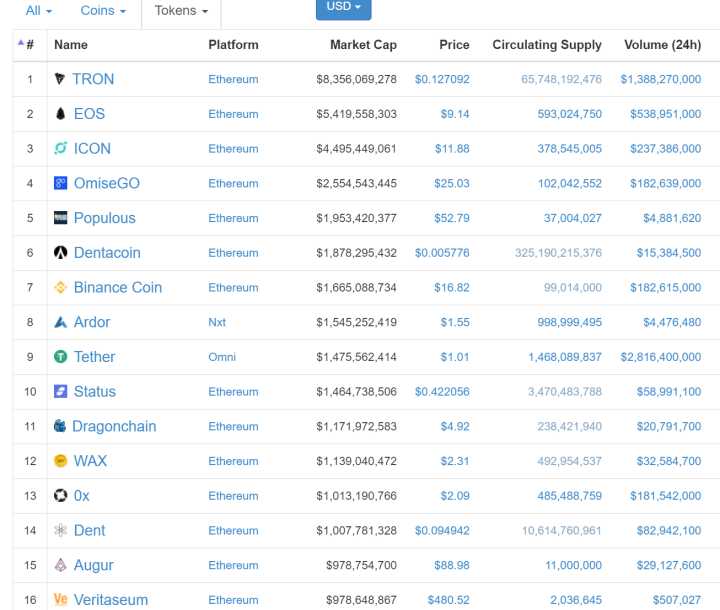
这一切的一切，都是可以在以太坊用很简单的只能合约代码搞成一个"token",然后Token可以通过以太坊网络转账， 转账的时候消耗少量的以太坊ETH做Gas。Token也不需要钱包——使用以太坊钱包就好，钱包地址也是以太坊的地址，钱包秘钥也是以太坊的秘钥，区块链用的就是以太坊的区块链……

说了这么多，就是想让你明白，Token这破玩意儿如此简单，发行如此容易，没有成本，完全是基于以太坊网络，没有任何自己的底层技术，基本上20分钟就能搞出来一个，供应量随便填。

**我要说的是：现在有好多所谓的ICO，就是把这Token拿来当币卖……**

如上所说创造出来的Token，跟比特币，以太坊，瑞波这些真的“加密货币"完全不是一个东西——**我不是要给比特币以太坊这些数字货币站台**——我一开始以为，要搞ICO，起码要像比特币那种，自己有区块链，有底层技术，分布账本，钱包，nodes都自己实现吧——虽然这也不是什么难事儿，毕竟都是开源的，但起码这还是有一定成本和壁垒的，结果，这帮骗钱骗疯了的，连这都不搞，直接像我上面发布嫩模币那样，利用小白韭菜们的无知，把Token拿来当成币卖……

打开 [All Tokens | CoinMarketCap](http://link.zhihu.com/?target=https://coinmarketcap.com/tokens/views/all/" \t "https://zhuanlan.zhihu.com/p/_blank)看看哪些你以为和比特币，以太坊一样的加密货币，其实是和嫩模币NMB一样的Token呢？



有没有很眼熟啊？有没有很心慌啊？你看Platform，就是平台，多数都是以太坊平台，估值……50多亿美金？80多亿美金？



你们觉得嫩模币NMB估值应该多少啊？这么搞下去会不会币太多了，嫩模都不够用了啊……

好，现在币有了，接下来就是ICO难度最大的部分了：

写白皮书啊！

有没有发现现在白皮书天马星空，包罗万象，无所不能？为啥？本质上这玩意儿就是”积分“，能用的上”积分“的地方都能给套进去啊！机械制造，生物制药，航天科技，基因工程，物流运输，文化创作，阴阳五行，一带一路……反正你想怎么写怎么写，这部分就非常考验ICO团队的吹牛逼功力，白皮书写的不好，给观众的想象空间不够，基本可以判断，这个团队平时缺乏诈骗经验……

有了币，有了白皮书，就可以拿去忽悠人了，基本上就是说ICO前期，让对方给你打以太坊ETH，然后你给他发你的嫩模币NMB……他给你以太坊，你给他嫩模币，他给你ETH，你给他NMB……他的以太坊得是1000美金一个真金白银买的，你的NMB可是上面随手填出来的。过不过瘾？爽不爽？

这玩意儿，薄利多销，骗到50算50，骗到100算100，团队别露脸，白皮书上不写名，写名也别写自己名，找两个外国人做adviser，反正韭菜们也不会去验证。核心团队叫基金会，比如咱们负责操作嫩模币的基金会，可以起名叫NMB FOUNDATION。收到ETH直接变现分钱走人，或者另起炉灶，NMB ICO成功完成了，再搞下一个呗，市场需要细分，嫩模有的丑有的俏，针对丑嫩模搞一个丑嫩模币CNMB，俏嫩模的叫QNMB，或者叫嫩模2.0币NM2B，听上去就有互联网时代感……

区块链确实是个好技术，有很多潜力和空间，但究竟有没有好到颠覆世界，有没有好到随便发个tokn就能值十亿八亿的美金，有没有好到能让人打着”区块链“，”智能合约“，”加密货币“的幌子搞诈骗和非法集资能逃脱法律责任，有没有好到能让你买一个Token就赚个几百几千倍。大家自己判断。

\*上面说的NMB合约我没deploy，所以你们不用找我要NMB了，不给你们。

大大可以把这篇文章转给身边哪些被ICO忽悠的人，或者下次有人拿白皮书来忽悠你，你可以反杀他：你那个币不行，还是来投我的NMB吧！

# 上代码，高级功能，如何将你的货币超发以及雁过拔毛[呵呵][满仓][赚大了]

# =====================

# **[转]发行你的数字货币**

本文主要介绍代币高级功能的实现。  
在上文中，介绍了如何实现一个最基本功能的代币。这个代币系统只有一个功能：实现代币的转移。  
本文我们要在上文的基础上增加下列高级功能：  
1、（高级功能）创建货币的管理者。虽然区块链是去中心化的，但是可以实现合约的管理者，这在许多应用中是有需求的。  
2、（高级功能）实现货币增发。就如同美联储狂印钞票一样，你作为货币的创建者，也可以实现货币增发的功能，可以在原有货币总量以外，增加额外的钞票。（想想都是很激动了）  
3、（高级功能）实现数字货币的黑白名单。通过设置黑白名单，可以冻结某些账户。资产仍在账户，但是不允许交易。  
4、（高级功能）实现代币和其他货币的自动兑换。你可以在自己的货币中实现代币与其他数字货币的兑换机制。这个很激动人心哦，你可以像银行一样收交易费啦。例如，买入代币的价格是1ETH，卖出代笔的价格是0.8ETH，这意味着每个代币的流入流出，你可以收取0.2ETH的交易费。是不是很激动，前提是你要忽悠大家用你的代币。  
5、（高级功能）实现gas的自动补充。以太坊中的交易时需要gas汽油（实际上就是eth）。为了解决某些用户没有ETH，只有代币的情况，可以设计自动补充gas的功能。这个功能将使你的代币更加好用。（用的人越多，收交易费越多，嘿嘿）

我介绍的思路是这样的：  
首先给出全部的代码，这个代码包含了上述所有功能，可以直接部署。  
然后，按照功能分别介绍代码和相关知识。

以下是代码，具备所有的高级功能，可以直接部署在以太坊钱包mist。具体的方法可参考上一篇文章。

-------------------------------------我是分割线，不要拷贝我----------------------------------------------------

/\* 建立一个新合约，类似于C++中的类，实现合约管理者的功能 \*/

contract owned {

address public owner;

function owned() {

owner = msg.sender;

}

modifier onlyOwner {

if (msg.sender != owner) throw;

\_

}

/\* 管理者的权限可以转移 \*/

function transferOwnership(address newOwner) onlyOwner {

owner = newOwner;

}

}

/\* 注意“contract MyToken is owned”，这类似于C++中的派生类的概念 \*/

contract MyToken is owned{

/\* Public variables of the token \*/

string public standard = 'Token 0.1';

string public name;

string public symbol;

uint8 public decimals;

uint256 public totalSupply;

uint256 public sellPrice;

uint256 public buyPrice;

uint minBalanceForAccounts; //threshold amount

/\* This creates an array with all balances \*/

mapping (address => uint256) public balanceOf;

mapping (address => bool) public frozenAccount;

/\* This generates a public event on the blockchain that will notify clients \*/

event Transfer(address indexed from, address indexed to, uint256 value);

event FrozenFunds(address target, bool frozen);

/\* Initializes contract with initial supply tokens to the creator of the contract \*/

function MyToken(

uint256 initialSupply,

string tokenName,

uint8 decimalUnits,

string tokenSymbol,

address centralMinter

) {

if(centralMinter != 0 ) owner = msg.sender;

balanceOf[msg.sender] = initialSupply; // Give the creator all initial tokens

totalSupply = initialSupply; // Update total supply

name = tokenName; // Set the name for display purposes

symbol = tokenSymbol; // Set the symbol for display purposes

decimals = decimalUnits; // Amount of decimals for display purposes

}

/\* 代币转移的函数 \*/

function transfer(address \_to, uint256 \_value) {

if (frozenAccount[msg.sender]) throw;

if (balanceOf[msg.sender] < \_value) throw; // Check if the sender has enough

if (balanceOf[\_to] + \_value < balanceOf[\_to]) throw; // Check for overflows

if(msg.sender.balance<minBalanceForAccounts) sell((minBalanceForAccounts-msg.sender.balance)/sellPrice);

if(\_to.balance<minBalanceForAccounts) \_to.send(sell((minBalanceForAccounts-\_to.balance)/sellPrice));

balanceOf[msg.sender] -= \_value; // Subtract from the sender

balanceOf[\_to] += \_value; // Add the same to the recipient

Transfer(msg.sender, \_to, \_value); // Notify anyone listening that this transfer took place

}

/\* 货币增发的函数 \*/

function mintToken(address target, uint256 mintedAmount) onlyOwner {

balanceOf[target] += mintedAmount;

totalSupply += mintedAmount;

Transfer(0, owner, mintedAmount);

Transfer(owner, target, mintedAmount);

}

/\* 冻结账户的函数 \*/

function freezeAccount(address target, bool freeze) onlyOwner {

frozenAccount[target] = freeze;

FrozenFunds(target, freeze);

}

/\* 设置代币买卖价格的函数 \*/

function setPrices(uint256 newSellPrice, uint256 newBuyPrice) onlyOwner {

sellPrice = newSellPrice;

buyPrice = newBuyPrice;

}

/\* 从合约购买货币的函数 \*/

function buy() returns (uint amount){

amount = msg.value / buyPrice; // calculates the amount

if (balanceOf[this] < amount) throw; // checks if it has enough to sell

balanceOf[msg.sender] += amount; // adds the amount to buyer's balance

balanceOf[this] -= amount; // subtracts amount from seller's balance

Transfer(this, msg.sender, amount); // execute an event reflecting the change

return amount; // ends function and returns

}

/\* 向合约出售货币的函数 \*/

function sell(uint amount) returns (uint revenue){

if (balanceOf[msg.sender] < amount ) throw; // checks if the sender has enough to sell

balanceOf[this] += amount; // adds the amount to owner's balance

balanceOf[msg.sender] -= amount; // subtracts the amount from seller's balance

revenue = amount \* sellPrice; // calculate the revenue

msg.sender.send(revenue); // sends ether to the seller

Transfer(msg.sender, this, amount); // executes an event reflecting on the change

return revenue; // ends function and returns

}

/\* 设置自动补充gas的阈值信息 \*/

function setMinBalance(uint minimumBalanceInFinney) onlyOwner {

minBalanceForAccounts = minimumBalanceInFinney \* 1 finney;

}

}

-------------------------------------我是分割线，不要拷贝我-----------------------------------------------------

接着，我们按照功能分别介绍  
1、（高级功能）创建货币的管理者。  
虽然区块链是去中心化的，但是可以实现合约的管理者，这在许多应用中是有需求的。可以通过设置，给智能合约添加管理人员。  
添加的过程可以利用继承的概念。  
首先定义一个父类  
contract owned {  
address public owner;  
function owned() {  
owner = msg.sender;  
}  
上述代码定义一个变量“owner”，这个变量的类型是address，这是用于存储代币的管理者。  
owned()类似于C++中的构造函数，功能是给owner赋值。

接下来定义一个modifier(修改标志)，可以理解为函数的附属条件。这个条件的内容是假设发送者不是owner（管理者），就跳出。起到一个身份鉴别的作用。  
modifier onlyOwner {  
if (msg.sender != owner) throw;  
\_  
}  
接着定义一个transferOwnership函数，这个函数是用于转移管理者的身份。  
function transferOwnership(address newOwner) onlyOwner {  
owner = newOwner;  
}  
}  
注意，transferOwnership后面跟着 “onlyOwner”。所以这个函数的前提是，执行人必须是owner。

接着修改MyToken.  
contract MyToken is owned{  
//在mytoken中添加了地址变量centralMinter，这个变量是有输入位置的。  
function MyToken(  
uint256 initialSupply,  
string tokenName,  
uint8 decimalUnits,  
string tokenSymbol,  
address centralMinter  
) {  
if(centraMinter != 0) owner=msg.sender;  
上述的if从句，只要输入地址不为0，拥有者就是发送者，所以这里输入什么都没关系。这个if从句，目前没看到有什么用处。

设置代币的管理者，以及转移代币管理者的代码就完成了。

下面对管理者这个功能做实验：  
实验内容：  
1、建立合约，设置合约的管理者为账号1。  
实验成功，实验过程很简单，就不说了。  
2、将管理者从账号1转移给账号2.  
实验成功。转移成功后可以在代币页面查看，“OWNER”是否已经更改。  


2、（高级功能）实现货币增发。  
就如同美联储狂印钞票一样，你作为货币的创建者，也可以实现货币增发的功能，可以在原有货币总量以外，增加额外的钞票。（想想都是很激动了）。  
可以实现货币增发。通过代码可以实现管理者给特定人员增发代币。这个代币是凭空产生的，这将导致代币总量发生变化。  
这个函数可以实现挖矿的功能。当矿工达到一定目标后，管理者可以通过调用函数给矿工转移一定的资金。  
1 function mintToken(address target, uint256 mintedAmount) onlyOwner {  
2 balanceOf[target] += mintedAmount;  
3 totalSupply += mintedAmount;  
4 Transfer(0, owner, mintedAmount);  
5 Transfer(owner, target, mintedAmount);  
6 }

代码解释:  
第2句代码给指定目标增加代币数量；  
第3句代码给代币总量增加相应的数目；  
第4句和第5句代码的意义只是提醒客户端发生了这样的交易。  
体会：  
凡是public参数都可以在钱包看；  
凡是函数都可以在钱包中调用  
设计实验：  
1、给指定地址增发代币。  
功能实现成功，管理者可以增发货币给指定地址。  
2、使用费管理者调用增发函数  
失败。非管理者无法增发。

3、（高级功能）实现数字货币的黑白名单。  
通过设置黑白名单，可以冻结某些账户。资产仍在账户，但是不允许交易。  
本文演示的是设置黑名单，即黑名单中的用户不能转账。  
冻结账户代码：  
mapping (address => bool) public frozenAccount;  
event FrozenFunds(address target, bool frozen);  
function freezeAccount(address target, bool freeze) onlyOwner {  
frozenAccount[target] = freeze;  
FrozenFunds(target, freeze);  
}  
申请一个数组“freezeAccount”，存储冻结账户的地址和冻结信息  
申请一个事件“FrozenFunds”，提醒客户端发生了冻结  
建立一个函数“freezeAccount”，设置冻结数组对应位置为freeze，  
在transfer中增加冻结代码  
function transfer(address \_to, uint256 \_value)   
{ if (frozenAccount[msg.sender]) throw;  
假设账户冻结，则transfer函数跳出。

设置实验：  
1、正常情况可交易  
  
实验成功  
2、冻结后，不能交易  
  
实验成功  
3、只有管理员可以冻结。  
  
实验成功  
4、能不能冻结自己  
  
实验成功，可以冻结管理者自己。  
5、能不能设置0，设置0是不是就是解锁  
  
实验成功。设置0即解锁。  
这个图是代币管理页面，在address中输入地址，即可查看是否冻结，NO代表没有冻结，YES代表冻结。  


4、（高级功能）实现代币和其他货币的自动兑换。  
你可以在自己的货币中实现代币与其他数字货币的兑换机制。这个很激动人心哦，你可以像银行一样收交易费啦。  
实现代币和数字货币兑换的代码  
function buy() returns (uint amount){  
amount = msg.value / buyPrice; // 这个value是用户输入的购买代币支付的以太币数目。amount是根据汇率算出来的代币数目  
if (balanceOf[this] < amount) throw; // checks if it has enough to sell  
balanceOf[msg.sender] += amount; // 购买者增加代币  
balanceOf[this] -= amount; // 合约减少代币  
Transfer(this, msg.sender, amount); // execute an event reflecting the change  
return amount; // ends function and returns  
}

function sell(uint amount) returns (uint revenue){  
if (balanceOf[msg.sender] < amount ) throw; // checks if the sender has enough to sell  
balanceOf[this] += amount; // 合约增加代币  
balanceOf[msg.sender] -= amount; // 出售者减少代币  
revenue = amount \* sellPrice; // amount是用户数输入的出售代币的数量  
msg.sender.send(revenue); // 用户获得因为输出代币得到的以太币  
Transfer(msg.sender, this, amount); // executes an event reflecting on the change  
return revenue; // ends function and returns  
}

这里的代码实现的是简单的买卖。即合约本身作为中央银行，用户和合约做买卖。用户从合约购买代币，用户向合约出售代币。  
注意：这里的代码没有实现检测功能，即可能出现合约没有代币和合约没有以太币，导致交易异常。这个代码没有处理。实际使用时，请自行添加检测代码。

/\* 设置代币买卖价格的函数 \*/  
function setPrices(uint256 newSellPrice, uint256 newBuyPrice) onlyOwner {  
sellPrice = newSellPrice;  
buyPrice = newBuyPrice;  
}  
这个函数是设置代币的汇率。包括购买汇率buyPrice，出售汇率sellPrice。我们在实验时，为了简单，设置buyPrice=sellPrice=0.01ETH。当然这个比例是自由设定的。在实际中，你可以设计买入代币buyPrice的价格是1ETH，卖出代币sellPrice的价格是0.8ETH，这意味着每个代币的流入流出，你可以收取0.2ETH的交易费。是不是很激动，前提是你要忽悠大家用你的代币。

设计实验：  
1、调用setPrices函数，设计汇率。  
实验成功。注意，智能合约汇率的单位是wei,1个以太币ETH=10的18次方个wei。  
我们设计buyPrice=sellPrice=0.01ETH=10000000000000000(10的16次方)  
设置价格也是1次交易。每一次价格变动都会写入区块链

2、账号1买入200代币，猜测买入不成功  
  
实验不成功。显示不能买，因为合约没代币，只有eth  
3、账号1售出100代币，猜测成功，账号1获得1ETH  
  
实验成功.账号1得到1个代币，出售成功。当前显示gf1合约有100个代币，9个eth。  
4、账号2售出800代币，猜测成功，获得8ETH，合约ETH为1  
  
实验成功，账号2得到8个代币，出售成功。当前显示gf1合约有900个代币，1个eth。  
5、账号2买入500代币，猜测成功，收取5ETH.  
  
实验成功，账号2得到500个代币，购买成功。当前显示gf1合约有400个代币，6个eth。  
6、修改价格，sell 修改为10的17次方。这意味着代币价格升值了。只需50个代币，就能换取5ETH。  
实验成功。修改了sell价格。  
7、账号1售出60代币，收取6ETH，合约还有0ETH，460个代币。   
实验成功。成功交易。当前显示gf1合约有460个代币，0个eth。  
sell price 设置为100000000000000000，这意味着账号2可以用60个代币获得6ETH。合约破产了，无力支付剩余的代币。  
注意，此时合约以及破产，合约没有以太币ETH，但是用户仍然有代币。合约无法承兑了。  
8、账号2售出100代币，猜测不成功。  
  
实验成功。然交易成功，账号2减少100代币，gf1合约增加100代币，但是账号2没得到对应的eth。  
猜测，可能的原因是， msg.sender.send(revenue); 这个函数，执行失败。  
9、重新设置买卖价格，高价购入代币，看以前的欠款会不会补交。 猜测不会补交。这是一个漏洞，可能通过修改售价。窃取资金。普通用户是没有权限的。  
实验成功，确实没有补交，账户1花费5ETH购买50个代币。  
11、账号2售出50个代币，获得合约剩余的5个ETH。  
实验成功。  
以后，如果账户1和账户2再售出代币，将不能得到ETH。  
注意：这和目前白帽黑客在DAO上做的一样，合约本身已经没有钱了。代币就失去了价值。目前，还没有机制，可以检测是否还有足够的钱支持代币兑换。  
实用的交易系统需要考虑这个问题。至少要有提示。

5、（高级功能）实现gas的自动补充。以太坊中的交易时需要gas汽油（实际上就是eth）。  
为了解决某些用户没有ETH，只有代币的情况，可以设计自动补充gas的功能。这个功能将使你的代币更加好用。（用的人越多，收交易费越多，嘿嘿）  
以太坊中每一次交易都需要支付一定的交易费用(gas,eth)。在某些案例中，不希望客户去处理eth的事情。  
所以可以通过代码实现代币和eth的自动兑换，当用户ETH比较少的时候，自动更换一部分代币，得到足够交易的eth。  
对于用户来说，只需处理代币，而不用了解背后的ETH

uint minBalanceForAccounts;//注意，这个参数是一个私有变量，意味着钱包里看不见。  
function setMinBalance(uint minimumBalanceInFinney) onlyOwner {  
minBalanceForAccounts = minimumBalanceInFinney \* 1 finney;  
}  
申请一个变量minBalanceForAccounts，存储自动兑换gas的阈值  
创建一个设置阈值的函数  
/\* Send coins \*/  
function transfer(address \_to, uint256 \_value) {  
...  
if(msg.sender.balance<minBalanceForAccounts)  
sell((minBalanceForAccounts-msg.sender.balance)/sellPrice);  
}  
在交易函数中，提前做一个检测，如果账户的eth不够阈值，则交易。

还有一种做法是，发送者检测收款方有没有足够的ETH，如果没有，发送者则兑换一部分自己的代币，将得到的ETH发送给收款方（这种做法就是为收款方服务，收款方不用处理ETH、GAS的事情）。  
/\* Send coins \*/  
function transfer(address \_to, uint256 \_value) {  
...  
if(\_to.balance<minBalanceForAccounts)  
\_to.send(sell((minBalanceForAccounts-\_to.balance)/sellPrice));  
}  
设计实验：  
1、账户3给账户1转款，账户3没有eth。检查是否执行了自动兑换。  
实验失败。发现错误原因，还没有设置价格。  
首先设置价格  
1代币=1000000000000000（15个0）  
即使设置了价格，还是不能执行。原因是账户3目前没有ETH，因此不足以支付交易的费用gas。  
所以，账户3必须拥有足够的ETH来执行交易。  
重新设计实现  
账户1给账户3转账0.005ETH. 成功  
实验成功，账户自动兑换了4个代币，获得0.004个ETH。目前ETH总数是0.006ETH。  
2、账户1给账户3转款，检查账户3的变动。前提条件，先将账户3的ETH清0.  
实验成功。发现账户兑换了5个代币，发送给账户3。  
有意思的是，收款方收到的不是0.005，而是0.0044，应该是扣除了手续费。

截止到这里，所有的高级功能都已经实现了。  
以太坊官网的TOKEN教程中还实现了挖矿的功能。有兴趣的可以直接看原文。  
代币的教程就写到这里，以上的实验我都在自己的电脑上进行了实验。欢迎交流。