

区块链：互联网金融的终局

肖 风

近期的《福布斯》杂志中文网上有一篇文章说道：没听过区块链？你可能对互联网金融知之有限！

这可绝对不是标题党的作为。在互联网金融几乎都快泡沫化的中国，关于世上是否真有互联网金融的争论，居然还能像沉渣一样时不时的泛起，也难怪有人要作此提醒了。其实，我们在中国看到的任何互联网金融的技术或商业模式雏形，都发源于欧美，无一例外！只是他们不叫互联网金融，叫 FinTech，金融科技！如果美国驻华大使给你一张中文姓名的名片，你可千万不要按中文拼音去美国查人！在 FinTech 中，目前最热闹的就是区块链技术了。据报道，全球主要的金融机构甚至纳斯达克交易所，已经或马上要建立区块链实验室，以试验区块链技术在各种金融场景中的应用，花旗银行甚至在内部已经发行了自己的数字货币“花旗币”。瑞士联合银行（UBS）已经在区块链上试验了 20 多项金融应用，包括金融交易，支付结算和发行智能债券等等。

有人预言十年之后互联网金融会消失，因为届时互联网金融如同互联网一样已经融入世界，万物互联，化为无形。我一直在想象，那

个时候的互联网金融会是什么样呢？《区块链：新经济蓝图及导读》这本书也许可以帮助我们更好的找到答案。

我们都知道，信任是世界上任何价值物转移，交易，存储和支付的基础，缺省信任，人类将无法完成任何的价值交换。最初人们靠血缘和宗族来建立信任，接着人们靠宗教和道德来建立信任，后来人们靠法律和组织来建立信任，否则人类社会无法完成越来越多的各式各样的价值转移和交换。随着人类社会越来越数字化，随着互联网由传递信息，消除信息不对称的信息互联网向传递价值，降低价值交换成本的价值互联网进化。人们开始尝试通过数学算法来建立交易双方的信任关系，使得弱关系可以依靠算法建立强连接，从而去促成人类有史以来不依靠互联网技术，几乎不可能完成的价值交换活动，包括甚至更主要的是金融交换活动。

区块链就是交易各方信任机制建设的一个完美的数学解决方案，而比特币就是区块链技术的第一个伟大的应用。区块链技术原理来源于一道数学问题：拜占庭将军问题。该问题假设在东罗马帝国时期，几个只能靠信使来传递信息的围攻城堡的联盟将军，如何防止不会被其中的叛徒欺骗，迷惑从而作出错误的决策。数学家演算了一套算法，让将军们在接到上一位将军的信息之后，加上自己的签名再转给除发给自己信息之外的其他将军，大家就在这样的信息周转中，让将军们得以在不找出叛徒（找叛徒将是成本最高，效率最低的解决办法）的

情况下达成共识，从而能保证得到的信息和作出的决策是正确的。

区块链的基本结构就是这样的，人们把一段时间内的信息，数据或代码打包成一个区块，盖上时间戳，加上公私钥，与上一个区块衔接在一起，每下一个区块的页首都包含了上一个区块的信息，然后在页中写入新的信息，数据或代码，从而形成新的区块，首尾相连，从而形成了区块链。到2015年8月29号，比特币区块链上共有372016个区块，总数据容量40G，算力400P（也就是400千万次浮点计算），目前我国的天河二号超级计算机的算力也只有33P。区块链技术一是用纯数学方法来建立各方的信任关系；二是交易各方信任关系的建立完全不需要借助第三方；三是建立信任关系的成本几乎降到了零，这样共享经济的商业模式才可能在近年出现，羊毛出在猪身上的所谓互联网免费商业模式才得以成立。这也正是我所预言的区块链将帮助达成互联网金融的终极模式的核心所在。

以区块链为基础，再加以一系列建立在区块链上的辅助方法，人们正在互联网上建立一整套互联网治理机制，包括：一，工作量证明机制（要篡改区块链上的数据，需要拥有超过全网51%的算力，这使得作伪的成本会高于预期获得的利益）；二，互联网共识机制（以共识来确保正确，而无需甄别好坏）；三，智能合约机制（以程序代替合同，约定的条件一旦达成，网络自动执行合约。金融活动由交换数据变为交换代码）；四，互联网透明机制（帐号全网公开而户名匿藏，

交易不可逆转且交易由第三方“矿工”记账)；五，社交网络的互动评分机制(这使得专车司机的笑脸能换来利益而出租车司机的笑脸却不能)；六，密码学公私钥匙等这些互联网治理机制正在给经典的经济学，金融学，管理学甚至社会学带来巨大的冲击。理论结构，公司结构，金融结构甚至社会结构都面临解构与重构的命题。

区块链是互联网金融的底层技术架构。只有区块链技术的成熟，才能带来互联网金融的成熟。这是因为：

1. 它是数字世界里一切价值物的公共总帐本，任何数字资产的认证，记录，登记，注册，存储，交易，支付，流通，一个账本统统解决。
2. 它是去中心化的大数据系统，记录，传递，存储，分析，应用，一应具有。
3. 它是分布式的云计算网络，没有中心服务器，仅比特币区块链已经拥有 400P 的计算能力，而这个计算能力是由全球接入比特币系统的无数台计算机免费提供的。
4. 它是未来去中心化组织结构的基础架构。
5. 它是互联网治理机制的底层协议，前述的互联网治理机制，大部分建立在区块链上。

站在区块链的高峰上，遥想互联网金融的未来，我认为它会有如下几个特点：

1. 它是智能化的。金融交换载体由数据变为了代码，传统金融成为可编程的智能金融。

2. 它是去中心化的组织结构。点对点，端到端，P2P。

3. 它是算法驱动的金融，摩擦系数接近于零。

4. 它是一体化的系统，身份识别，资产登记，交易交换，支付结算都在区块链一个系统上一帐打通。

5. 它是实时化，场景化，7X24 小时，现实世界与虚拟世界，物理世界与数字世界无缝衔接的金融体系。

韩峰博士和数字货币界（尤其是对数字货币 2.0 有研究）的几个同仁，计划翻译出版《区块链：新经济蓝图及导读》一书，为让更多的人能够了解区块链的意义，他们精心的为每一章节都结合中国经验写了导读，这是一个富有意义的创举。正好我正在上海紧锣密鼓地筹备开设一家区块链实验室，以在中国推广区块链技术。目前中国的区块链圈子并不大，很快我们就见上面了。双方相谈甚欢，相见恨晚。当场达成以这本书为起点，以区块链实验室为支撑，未来几年出版一套区块链实验室丛书的计划。一方面借以推广这项在中国还比较陌生但未来也许会扮演终结者角色的区块链技术；另一方面也想在这可能改变历史的关键时刻，能够留下一系列的文字记录，以见证这伟大的变迁。

让我们翘首以待在区块链上浴火重生的更普惠，更智能，更实时，

更跨界的未来金融！