

改进容易，颠覆难

区块链是好技术，但不是万能的，现有的金融系统历经多年形成，区块链要想颠覆颇具难度，现阶段更应着重改进效率。

文 | 本刊记者 张琴琴



王运嘉

法学博士，美国计算机博士候选人，曾担任知名跨国公司中国区一把手，后数次创业，做过专业律师，现为北京枫玉科技有限公司创始人。

比特币平稳运行七年，其底层运行技术——区块链引起了人们注意。区块链应用场景众多，它将如何改变现有金融或商业规则，也是众说纷纭。

为此，《英大金融》杂志专访到一位跨界老炮儿，有着十多年“码农”的实战经历，做过专业律师，现为北京枫玉科技有限公司创始人的王运嘉博士，请他从技术、法律以及商业模式方面解析区块链。

《英大金融》：当下，区块链备受关注，您如何看待这种火热？

王运嘉：区块链很火，主要是因为和钱靠得太近。现在依靠区块链技术发行山寨币的平台很多，炒币的更多，他们需要借这个概念的火热，让更多的人进场，将山寨币的价格拉上去，但这股炒作之风能持续多久，谁是退潮后的裸泳者，就不好说了。

《英大金融》：应该如何理性看待区块链呢？

王运嘉：关键要认识到没有一种技术是万能的。区块链是很漂亮的技术，它把多个技术无缝链接整合成一个完整的应用方案，但并没有很多人说的那么神奇。我个人认为，它可以改进效率，但很难改变业务的本质，更不可能解决所有问题。它是有一些很好的特性，但技

术特性和应用场景以及实现路径得分清楚，毕竟技术是用来解决实际问题的。许多人为了区块链而区块链，并非好事，杀鸡用牛刀或者杀牛用鸡刀，都是不合适的。

正确认识区块链

《英大金融》：提到区块链，大家会谈到它的匿名性，这一点该如何理解？

王运嘉：这里匿名和隐名的概念需要区分。法律上，匿名是带有恶意的，而隐名没有恶意，“隐名股东”，简单讲就是幕后股东，我国《公司法》是支持的。正确的说，区块链可以具有匿名性，尤其是公链，能看到账号，但不知道账号背后是谁。

《英大金融》：区块链的一大特征是去中心化，具体又是指什么？

王运嘉：准确地说，去中心有两层意思。技术层面上，整个P2P网络没有人负责，每个节点独立运行，不存在控制中心，区块链网络可以看成是一个去中心的大机器。应用层面上，它不一定是去中心的。尽管区块链账本存在于每个节点，大家都相信账本是准确且不可篡改的，但这种信任在交易环节里不足以去掉中间人，尤其是远程的实物交易，比如淘宝，一定会有第三方的存在，这个第三方是支付方，同

时也是担保方和仲裁方，比如支付宝。比特币在设计的时候引入了多重签名的功能，我在付出一笔钱的时候，我先签名，然后中间人视具体情况决定签名与否，一旦出现了纠纷，中间人来做裁判，决定钱的最终走向。

《英大金融》：系统有这样一个决策机制？

王运嘉：有，只是很少用而已。现在比特币主要用于汇款和支付，非面对面的远程实物交易场景还很少被用到，一旦涉及远程实物交易，中间人是很难被去除掉的。

《英大金融》：分布式数据库又如何体现？

王运嘉：分布式数据库也有两个层面的理解。在计算机领域，分布式是指在逻辑上它是一个数据库，但物理上数据被分别存储在不同地方。就是说，账本太大，或者数据结构太复杂，就每个节点分散存储一部分。区块链的分布式其实是一种镜像分布，也就是同步，每个节点的账本相同。其实，用户并不关心技术的实现问题，而是关心技术是否安全，账本是否准确，使用是否方便，这些才是最主要的。

不轻易改变规则

《英大金融》：在法律方面，区块链会有怎样的应用？

王运嘉：主要是存在性证明，比如防止病历、票据、选票、履历造假，也可以用于权属证明，例如版权证明，甚至于艺术品与奢侈品交易。

《英大金融》：那它是否就会替代现有的公证处？

王运嘉：不是替代，是补充或改进，替代一说多少带有敌意，但它能改进公证系统却是真的，以后也不会再有“我妈是我妈”这种让人哭笑不得的证明。重要的是，可以从技术上加强公证处或公证员的公信力，一旦被区块链公证之后，任何人都改变不了。区块链在存在性证明这个领域

的应用具有先天的优势，我个人认为，对公证系统是极好的补充。

《英大金融》：在金融领域，区块链现在可以落地的应用是什么？

王运嘉：银行间的清算、内部管控以及审计业务。前者的典型代表是 R3 联盟，后者的典型代表是德勤。

《英大金融》：区块链对清算中心会不会是一大威胁？

王运嘉：还是那句话，先不要尝试去改变这个制度，而是要在制度下改进效率。人们在过去那么多年经验总结的基础上发展出这个体系制度，不可能轻易被颠覆，尤其是在最讲究安全稳定的金融领域。现在公证需要 5 天，银行间清算需要 3 天，通过区块链将办事效率缩短到 1 天、半天甚至 1 小时，就已经非常有商业价值了，并且成本相对低廉得多。

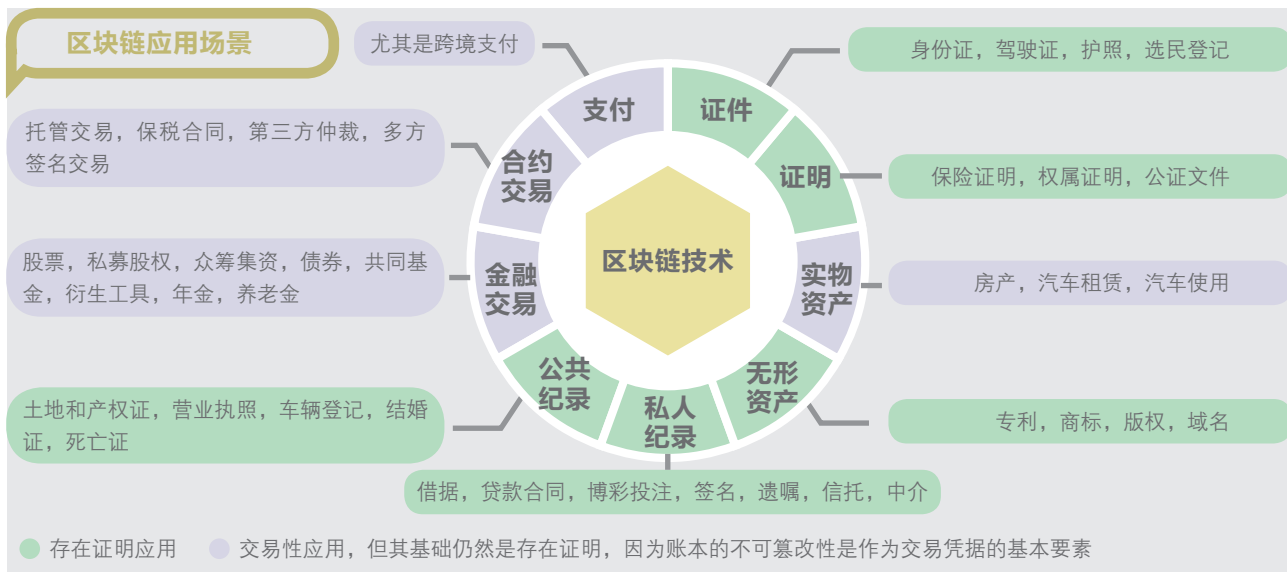
监管可以先“观望”

《英大金融》：如今区块链的火热，让人依稀想到去年大火的互联网金融。当下，监管层应该持一种什么样的态度，以避免区块链出现类似的互联网金融泡沫？

王运嘉：监管层可以先观望，无须过早干预，因为即便是运营了七年且市值最高的比特币，全球体量也不过 70 亿美元左右，不到 500 亿元人民币，很难对金融体系产生有影响的冲击。互联网金融主要是玩商业模式，它暴露出的那些问题并没有威胁到金融系统安全，反而会让人们清晰地意识到投资有风险。与互联网金融不同，区块链应用还有技术因素在里面，门槛相对较高，并且这些技术对央行未来的数字货币发行是有借鉴意义的。

《英大金融》：前段时间，区块链众筹项目 The DAO 运行几天就遭遇黑客攻击，这不是也暴露出区块链应用中技术和法律层面的

区块链是一个很漂亮的技术，它可以改进效率，但不可能解决所有问题。它是有一些很好特性，但技术特性和应用场景以及实现路径也要看清楚。



资料来源: 王运嘉博士提供

要多观察现有规则下可以改进的地方, 这就是机会, 而且越细分越好, 但一定不是实时交易的。

一些问题?

王运嘉: The DAO 作为智能合约的尝试, 是个不错的想法, 但在顶层的技术设计上出现了漏洞, 已经有很多计算机专家发文指出来, 我就不赘述了。但 The DAO 被攻击, 不完全是坏事, 因为问题在最开始就暴露出来总比在大量使用后的成熟期暴露出来要好。就法律而言, 这倒是个新的命题, 很有意思。把以太坊网络或比特币网络当作一个智能大机器, 智能合约的当事人达成合意, 形成合同, 为达到合同目的使用这个大机器, 而黑客利用这个机器的漏洞, 违反了合同主旨, 盗走了当事人的虚拟货币, 按这个思路, 法律关系就清晰了。

《英大金融》: The DAO 遭遇攻击, 究竟该追责于谁?

王运嘉: 可以参考一下 2008 年广东许霆案, ATM 机出故障开始吐钱, 许霆前后取了 17.5 万元, 一审被判无期后改判为 5 年。在中国法的语境下, ATM 出了问题不代表人就可以乘虚

而入地从里面拿钱, 更何况 ATM 机在中国法里视同金融机构的延伸。The DAO 也一样, 就是个计算机语言写的合同, 执行合同的机器出了问题, 不代表人们从中拿钱是合法的。所以, 从追责的角度而言, 在中国法的语境下, 黑客肯定是可以被追责的, 无论是民事还是刑事, 关键是得先找到他。

《英大金融》: 区块链应用前景给人很大的想象空间, 围绕区块链试图创业的公司也不少, 对此您会给些什么建议?

王运嘉: 多观察现有商业规则下可以改进的地方, 而且越细分越好, 但是涉及实时交易的, 得留个心眼, 除非是私链或联盟链。因为公链的交易速度天生就慢, 虽然可以经过其他方式改善, 但是得付出一些代价, 例如, 安全性或准确性。技术是很有层次感的, 解决一方面的问题通常以牺牲另一方面为代价, 区块链也一样。所以要围绕区块链创业, 尽量避免对交易速度或记账速度要求较高的应用场景。□