DOI:10.19729/j.cnki.1009-6868.2018.06.009
网络出版地址:http://kns.cnki.net/kcms/detail/34.1228.TN.20181106.1658.006.html

区块链的理想与现实
Vision and Reality of Blockchain

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2018) 06-0049-003

摘要: 认为区块链是互联网的又一块补丁,弥补了价值传递时的不足。去中心、匿名性和不可篡改,一起构成了区块链的三大技术支柱,这些技术特征在实际的商业应用中,还需要做很多的妥协和再平衡工作。区块链作为一种新兴的数据库技术,还处于非常早期的阶段,多个方面的技术都有待改进。

关键词: 区块链;去中心化;工作量证明(PoW);权益证明(PoS);区块链即服务(BaaS)

Abstract: Blockchain is the new patch to enhance the shortage for the Internet when transferring the value. Decentralization, anonymity and non-tampering are three technical pillars of the block chain. These technical features need to be compromised and rebalanced in practical commercial applications. It is in the very early stage as a kind of new database technology, and waiting for optimizing in several technical aspects.

Key words: blockchain; decentralized; proof of work (PoW); proof of stake (PoS); blockchain as a service (BaaS)

何宝宏/HE Baohong
(中国信息通信研究院,北京 100045)
(China Academy of Information and Communications Technology, Beijing 100045, China)

1 区块链是块补丁

互联网是一个还没有完成的科学实验,它过早离开实验室的襁褓来到了人世间。自传输控制协议(TCP)/网际协议(IP)应用的30多年以来,不断有人预言互联网会崩溃,会被新技术所替代,从IP地址耗光、垃圾信息、视频流量、路由表爆炸到安全攻击,原因不一而足;但互联网因其良好的开放性和扩展性,不断自我完善,既没有崩溃更没有被替代。

与内容分发网络(CDN)、对等网络(P2P)应用、软件定义网络(SDN)、网络地址翻译(NAT)、云计算和移动互联网等类似,区块链是针对互联网在价值传递方面的缺点,新打的一块补丁。

在传统互联网上,数据主要用来表示信息,核心要义是传播、复制和分享。随着互联网与实体经济融合的不断深化、大数据的兴起,数据正在资产化,资产正在数据化。现在的数据,很多已经是用来表示价值而不是信息了。数据表示价值,核心要义是所有权、控制和交易。

互联网与传统电话网、广播电视网类似,主要用于传递,尤其是数据信息。数字化的价值,比如货币、凭证和权益等Token,不能直接在互联网上传递,需要通过权威的中心节点做信任背书。这带来了在互联网上交易时,建立信任的成本高、效率低,以及中心节点可能造假等问题,于是就有了基于区块链的价值传递技术,希望用区块链来代替传统的中心节点,从信任机构转向信任机器。

区块链的基本思路是将价值数据按时间顺序排列成一条链,只有某数据的最后一个拥有者,才是该数据的价值拥有者。链上该数据的曾经拥有者,都只是价值的过客,是用来证明最终拥有者的。

这就是所谓的价值互联网,是互联网的又一次延展。区块链的核心是做数据管理和价值传递,只是信息技术的一个"区块",还必须与其他信息技术和场景"链"起来,才可能占据互联网世界的一个生态位。

2 区块链是一种数据库技术

传统数据库、大数据和区块链,都是用来管理数据的,都可以认为是数据库管理技术[1];但它们追求的目标不同,因此应用场景也不同。

传统数据库针对的是高价值的结构化数据,大数据针对的是海量和更多类型的数据。二者都假设,虽可能会存在数据质量等问题,但可以相信输入数据的机构以及数据管理员,相信他们不会故意捏造或篡改数据。

区块链面向的也是高价值数据,但针对的是数据机构或数据管理员,以及可能造假的问题。区块链不信

收稿日期:2018-10-16
网络出版日期:2018-11-06

任数据机构和数据管理员，不信任他/她写入的数据，除非多个相关方能够根据事先达成的协议（共识机制），集体同意录入。传统数据库为追求一致性而牺牲了效率，大数据为追求效率而牺牲了一致性，而区块链为追求更高的一致性而牺牲了更多的效率。

区块链集成了分布式网络、密码学、共识算法和智能合约等技术，采用了一种集体维护数据的思路。这带来了区块链能够防篡改的特点，但也会严重损耗性能和扩展性等。虽然通过隔离见证、分片、多链和增加块大小等手段，能够加以改善，但理论上性能和扩展性都无法与集中式的数据库技术相比。

当然，区块链还引入了一些数据管理之前没有过的概念，比如共识算法、智能合约和激励机制等，超出了传统数据库的概念范畴，但我们认为本质上还是数据库技术。

3 区块链的技术魔咒

去中心、匿名性和不可篡改，一起构成了区块链的三大技术支柱。因为区块链正处于从比特币实验走向市场试商用的阶段，因此这些技术特征在实际的商业应用中，还需要做很多的妥协和再平衡工作。

3.1 去中心化

比特币和区块链等希望去掉央行和交易中心等中心组织，核心理由是这些权威的中心组织可能会伪造自己的资产负债表，只能做事后审计，并且不容易发现。

但当区块链技术逐步“堕入”商业世界时，去中心化的信仰正在逐步沦丧，架构开始走向了集中。比如区块链的企业操作系统（EOS）项目，就设计了21个中心节点。事实上，如果以最典型的区块链应用，比特币和以太坊等为例做观察，就会发现已经形成了3个中心：代码中心、算力中心和财富中心。

（1）代码中心。2018年3月伦敦大学的研究人员发现：Bitcoin Core软件中所有文件的7%是由一名开发人员编写的，而以太坊中的大约20%的文件是由单一编码人员编写的。对比特币社区影响最大的最初是创始者中本聪，现在是Core小组的5个人。以太坊社区，基本由其创立者BUTEERIN V说了算。

（2）算力中心。工作量证明（PoW）和权益证明（PoS）是目前应用最为广泛的2种共识机制，分别基于算力大小和财力大小来分配记账权。PoW的基础是算力，曾经超过70%的算力由一家公司生产，集中在一个国家挖矿，这已形成了算力中心。

（3）财富中心。区块链技术的一大创新，是将激励机制内置化。PoS的基础是代币，全世界代币持有者联合起来就是财富中心。而PoW的算力，又是可以通过资本购买的。有研究表明：比特币是高度集中的，40%的比特币集中在1 000人，96.53%的比特币归属4.11%的地址。另外，PoW和PoS只是创造了所谓的数字资产，还需要做数字资产的交易，于是交易所也成了财富中心。

3.2 匿名性

在传统金融系统中，账户名是可以公开的，但账本内容是必须保密的。为储户保密指账户中的记录，不是账户号。区块链的设计反过来了，账户号是匿名的，但账本内容是公开的。区块链匿名性说的是账户名匿名，不是账户中的记录。

首先，为了交易的便利性，区块链的账户（地址）标识需要一定的稳定性和一致性。又因为所有账户的内容是公开性的，交易时的IP地址是公开的，因此实际上掩盖交易身份是非常困难的。

其次，早期的区块链应用记录的是源于母体的数字货币，区块链自产自销的是原生虚拟资产。这是一个封闭的数字价值世界，不需要与物理世界打交道就可以运转，匿名也是完全可行的。但到了区块链的2.0时代（具备智能合约和平台化等），区块链上记录和交易的不再来自区块链，而是来自物理世界的股权、版权和产权等。如果区块链上所映射的是匿名资产，从法律意义上就是无效合同。

3.3 防篡改

根据数据库理论，所有的数据库管理技术都会包含“Insert”，“Select”，“Update”和“Delete”等。但一些组织或个人把数据库所具备的“修改”能力，当作可以篡改能力来用了，导致假账频发，于是就有了区块链。它去除“Update”和“Delete”等数据库的功能，变成只能单向“Insert”和“一次性写”的数据库技术。

有人的地方就可能出现误操作，有利益的地方就可能出现欺诈；但区块链只是一种技术，认为误操作也是操作，欺诈交易也是交易，修改和篡改没什么区别。技术无法处理道德和管理层面的问题，区块链只能用下一个不可修改的操作，来弥补前一个错误操作。

区块链缺乏类似会计制度中的差错处理机制，已经带来了一些问题，例如：2016年的TheDao事件，已经让区块链陷入了程序正义还是内容正义的陷阱。

4 区块链要自证清白

不能因为一个应用系统引入了区块链，就可以相信它了。一个区块链应用系统要获得更多的信任，一是所使用的区块链要自证清白，二是区块链应用的环境也要值得信任，例如：入出链的数据和镜像关系也要自证真实性。

4.1 基础设施

区块链不是天然值得信任的。在许可链（比如联盟链和私有链）中，用户的授权和访问控制，需要由值得信任的管理员来执行。虽然无需许

可的公有链中，去掉了管理员这个角色。但无论是公有链、联盟链和私有链，都还需要信任自己的组成部分[2]：

（1）必须信任所选用的加密技术。但是，加密算法或实现可能会有缺陷，智能合约也可能会有漏洞。

（2）必须信任所运行的软件。要祈祷程序员是个天才，所开发的软件没有BUG。

（3）必须相信用户之间不会共谋。如果一个群体或个人控制了PoW系统中51%的算力，或者PoS系统中51%的投票权，整个区块链的防篡改根本就不成立了。

（4）必须相信节点的中立性。要假设节点会公平地接受和处理每笔交易，类似于“网络中立”的法律原则，但“链中立”但还没形成标准和法律制度。

4.2 应用环境

区块链应用要依存于外部环境和整个生态。环境中的一些不可信因素，也必然会被带入到区块链的生态系统中。区块链具有防篡改能力，但只是数据已经在链上的时候。在数据写入链之前，在数据离开区块链之后，是否被篡改了，区块链都是无能为力的。

不像区块链的虚拟币是一个闭环应用，区块链上的数据在一些溯源、存证等非闭环的应用场景下，虽然是不可篡改的，但链上的数据与物理世界物品的“关联关系”不能上链，区块链可以防止篡改数据，但无法防止篡改映射关系。

5 区块链发展趋势展望

区块链技术还在持续演进中，扩展性有待进一步提升，性能还无法满足高频交易的需要，对共识算法还没有共识，智能合约的“智商”还有待提升，新业务模式还在探索中。总的来看，区块链技术演进趋势呈现如下几个特点[3]。

（1）架构方面：公有链和联盟链融合持续演进。联盟链是区块链现阶段主要的落地方式，但相对于公有链而言，扩展性、隐私胡和社区激励还有待完善。随着应用场景趋于复杂，公有链和联盟链的架构模式开始走向融合：以面向大众的公有链做基础设施，通过隔离和加密等手段，面向企业构建基于公有链的联盟链。这种模式与业界之前的虚拟专用服务器（VPS）、虚拟专用网（VPN）、虚拟专用数据库（VPD）和虚拟专用云（VPC）等非常相像，因此可以称为“虚拟专用链（VPB）”。

（2）部署方式：区块链即服务（BaaS）加速演进。区块链的实现可以是基本传统IT的，也可以是基于云计算的。现在，越来越多的区块链开发者和用户意识到了新兴的云计算带来的好处。基于云计算搭建BaaS，不仅可以带来快速开发、敏捷部署和成本较低等优势，还可以让区块链企业将重点转向面向垂直行业，以更好地对接用户。

（3）技术层面：跨链及高性能的需求日益凸显。不同的区块链适用于不同的应用场景，跨链技术可以让区块链适于更加复杂的场景，以实现多个区块链之间的价值转移、存证和授权管理等，如金融质押、资产证券化、溯源防伪和征信等。目前典型的跨链技术，如公证人机制（Notary schemes）、侧链/中继（Sidechains/relays）、哈希锁定（Hash-locking）、分布式私钥控制（Distributed private key control）。

（4）共识方面：共识机制从单一向混合方式演进。导致区块链性能降低的重要因素之一是共识算法。PoW、PoS、股份授权证明（DPoS）和拜占庭容错等，各据优势，各有最适用的场景。为提升效率，需在安全性、可靠性、开放性等方面进行取舍，根据场景切换共识机制成了新趋势，并且将从单一的共识机制向多类混合的共识机制演进，运行过程中支持共识机制动态切换，或系统根据当前需要自动选择相符的共识机制。

（5）智能合约方面：可插拔和易用性成为关注的重点。更具体而言：一是可插拔的执行环境架构，二是明示化的调用关系，三是可链外存储的合约代码，四是低耦合度的设计，五是完整安全的防护体系。

参考文献

[1] 何宝宏.别拿着区块链找钉子[EB/OL].(2018-05-20)[2018-00-00]. https://mp.weixin.qq.com/mp/profile_ext?action=home&__biz=MzAxMjIyMjYxOA==&scene=126&subscene=0#wechat_redirect

[2] ROBACK E. U.S. Department of Commerce [R]. USA:National Institute of Standards and Technology, 1990. DOI:10.13039/https://doi.org/10.13039/100000161

[3] 中国信息通信研究院. 区块链白皮书(2018年) [R]. 北京: 中国信息通信研究, 2018

作者简介

何宝宏，毕业于中国科学院计算技术研究所，获计算机博士学位，目前担任中国信息通信研究院云计算与大数据研究所所长；从事互联网研究20余年，现主要研究方向为互联网技术哲学；出版《互联网的基因》等书。