江苏可信区块链

（电子月刊）

2020年第5期　总第5期

江苏省互联网协会

江苏可信区块链

2020年7月10日

编　　辑：刘湘生　于苏丰　张东风　王　锋
　　王梦原　葛九丽　李正豪　尹　珺
美　　工：王　亚

地　　址：江苏省南京市建邺区新城科技园创新综合体A区5号楼
联系电话：025-83343696

征稿启事

为搭建知识普及、行业交流、政府沟通，促进江苏区块链产业健康持续发展的平台，2020年3月10日起，江苏可信区块链专委会推出《江苏可信区块链（电子月刊）》，从行业动态、场景应用、技术交流、项目展示等多个视角介绍区块链行业发展的最新情况，现面向从事区块的企事业单位征集在区块链场景探索、行业赋能、产业发展、技术研发、国内外动态、投融对接等方面的稿件。欢迎从事区块链业务的企事业单位积极参与，踊跃供稿。来稿请发送邮箱：jsiaorg@126.com，联系人：李正豪，15365059600。

卷首语

6月20日，由腾讯金融研究院主办的“2020金融科技发展论坛”在北京进行直播。论坛上，中国工程院院士邬贺铨表示，5G与区块链结合，可逐步实现万物互联、万物智联、万物信联，可助力解决金融业痛点，提高效率、降低成本和风险，共同推动数字经济的发展。

5G与区块链优势互补。5G技术支撑区块链让更多的终端接入网络，数据在无线环境下传输更快、容量更大，从而促进更多的链下数据上链，为区块链网络点对点的信息传输和交换提供绝佳的基础设施服务，提升整个区块链网络的性能，极大地扩展区块链的应用范围。而区块链技术又为5G网络的优势提供一种新领域的延伸，促使5G实现真正的价值流通。

5G和区块链相互赋能。5G高速率、大宽带和低时延三大特征将提升区块链数据同步和共识算法的效率，使区块链功能最大化；而区块链技术构建的点对点去中心化网络，通过共识机制和加密算法，保障了数据的安全，并大幅度提升终端交易的效率，降低交易成本。5G和区块链的结合，取长补短，相得益彰，相互赋能。

5G和区块链结合塑造新型商业模式。5G技术支撑区块链让更多的终端接入网络，促使更多的链下数据上链，各类终端从最早的上网、到之后的上云，到现在的上链，是一种新型云网协同机制的趋势。随着海量无线终端的接入，形成新的化学反应，将在各行各业塑造出更新更多的商业模式，推动一系列相关应用场景的落地。

5G和区块链的融合，将对现实物理资产进行确权，使得通证化的物理资产上链更灵活、更自由地流转。在数据高速传输下，5G与区块链技术的强强联合使得人与人、人与物、物与物之间更高效、可靠的连接成为可能，将更有助于促进5G和区块链的快速融合。区块链有利于通过数据确权打破数据孤岛，实现共赢。作为一种相对特殊的数据传输和数据存储架构，区块链这种特殊架构及其自身的发展，将从根本上促进5G的发展，校正5G的发展方向，并丰富物联网的体系架构形式。

6月29日下午，由江苏省互联网协会主办，江苏可信区块链专委会、江苏（云与计算）华为云协办的“5G+区块链技术应用交流会”在华为南研所举行，多位5G应用与区块链企业家进行了5G应用和区块链融合发展的思想碰撞，探讨和推动5G与区块链融合发展的应用场景。希望本期电子月刊帮助您更好的理解5G和区块链的融合，《江苏可信区块链（电子月刊）》与您共同进步。

CONTENTS

目 录

一、专家特稿

孙国梓教授：区块链技术安全威胁分析（上）

孙国梓，南京邮电大学教授、江苏可信区块链专委会特聘专家

区块链概念的出现源于2008年中本聪发表了一篇《比特币:一种点对点的电子现金系统》，他在论文中提出了区块链(Blockchain)这种数据结构。作为计算机时代的先进技术，区块链应用了分布式数据存储、加密算法、共识机制、点对点传输等计算机技术，本质上是一种去中心化基础架构与分布式计算范式。

就目前而言，由于区块链技术的快速发展和进步，在不同的行业和不同的场景之下，结合区块链技术的相当一部分应用已经实现落地，而还有一部分在持续发展中。区块链技术的发展可以分为3个阶段：

区块链1．0是基于比特币的诞生而出现，此时的区块链主要用于加密货币。该层次的区块链应用增强了数字货币的具象化形式，形成了一种新型价值的数据表现形式。其通过电子数据的传输与交易完成交易介质、记账单位以及价值存储的功能。比特币就是第一个加密货币的具体实现。

区块链2．0主要用于金融服务，这一时代最大的特点就是引入了智能合约的概念，以其最简单的形式来说，是由其创建者编写以执行特定任务的程序。虽然智能合约可以在任何区块链版本上进行编码，但是以太坊是最受欢迎的选项，因为其提供了可扩展的高效处理能力。智能合约的引入使得区块链能做更多复杂的逻辑，而不是简单的点对点转账。

区块链3．0指的是其不再只为金融服务，除此之外，更多的场景也用上了区块链技术，包括政府、食品安全、媒体、司法取证等等。这个时代对区块链的认识有了更深的理解，更加认可区块链对于社会发展的价值。超级账本(Hyperledger)项目作为实现了完整权限控制及安全防护的区块链架构，是该阶段的代表技术。

当区块链技术在各行各业兴起之后，大部分专家学者们一直在探索区块链技术如何更好地融入到日常生活中。随着区块链加密货币、交易所、区块链应用等开始慢慢普及，也让很多黑客攻击者对区块链技术进行了深入研究，从区块链中找到技术漏洞作为攻击入口，以便从中获利。

近两年来，区块链在安全方面遇到了很多问题。

2019年1月25日，全球区块链数据与安全服务商派盾(PeckShield)联合多家媒体共同发布《2018年度区块链十大安全事件》，其中有2018年3月7日币安交易所遭黑客攻击，通过程序化交易拉升代币从而获利；2018年3月20日以太坊节点持续两年偷渡漏洞，攻击者利用以太坊RPC API缺陷盗取节点资产；2018年4月至5月 BEN/SMT/EDU 智能合约安全漏洞；2018年5月29日EOS节点远程代码执行；2018年7月至8月ERC20等一系列代币假充值漏洞；2018年7月至11月EOS帐户彩虹攻击;2018年8月23日 FOMO 3D游戏阻塞攻击决出大奖，破坏游戏平衡；2018年9月BTC超发漏洞；2018年8月至11月EOSDApp 等系列漏洞；2018年11月16日BCH共识破裂硬分叉。这十大安全事件只是区块链中的冰山一角，因此目前区块链的安全问题需要重视起来，减少损失。

1. 区块链概述

（1）区块链特性

区块链技术发展至今已经形成了一个较完整的技术栈。区块链被广泛地关注和研究主要是因为其本身的特性：去中心、透明性和可溯源性、开放性、不可篡改性、匿名性。

去中心化：与传统的中心化系统不同的是，区块链中并不是由某一个中心来处理数据的记录、存储和更新，而是每一个节点都是对等的，整个网络的数据维护都是由所有节点共同参与的。在传统的中心化系统中，如果攻击者攻击中心节点，就会导致整个网络的不可控，而区块链的去中心化特点提高了整个系统的安全性。

透明性和可溯源性：在区块链中所有的交易都是公开的，任何节点都可以得到一份区块链上所有的交易记录，除了交易双方的私有信息被加密，区块链上的数据都可以通过公开的接口查询，又因为区块链是以时间序列来记录数据，所以也就保证了用户可以对交易进行溯源。

不可篡改性：在区块链中所有的信息一旦通过验证共识并且写入区块链之后，数据是不可篡改的，如果想篡改数据就必须挑战 51% 以上的矿工，而这样的代价很大并且很难实现。

（2）区块链体系结构

区块链在经历长时间的演变之后，其体系结构基本已经定型，大多数的区块链底层架构由6部分组成，其中有数据层、网络层、共识层、激励层、合约层和应用层。

区块链的底层架构

数据层：主要包括数据区块、哈希函数、链式结构、Merkle树、时间戳和非对称加密等，在数据层使用时间戳来证明各个交易创建的时间，时间戳服务器对当前交易及其建立的时间和指向之前交易的哈希进行签名，这样就能反映各个交易创建的时间顺序并且这个时间是不可更改的。在区块链中每一笔交易都是公开的，

每一笔交易都显示了交易的来源和交易的去向，但只是显示双方的地址信息并不是个人的真实信息，因此在区块链中的每一个节点都可以对交易进行溯源，数据层使用的各种数据的链式结构和加密算法及时间戳技术保证了数据存储和交易的安全性。

网络层：主要包括 P2P 网络机制、传播机制和验证机制。区块链基本特性之一就是去中心化，因此任何节点之间都可以进行交易，每一个节点都有广播交易的权利，并通过特殊的验证机制使每个节点都可以对数据进行打包记账，但只有通过大部分节点才能存入区块链。采用 P2P 网络机制使得区块链的节点具有自动组网功能，目前该技术已经是非常成熟和安全的。

共识层：主要包括各种共识机制的算法： PoW、PoS、DPoS等。共识机制是区块链的核心技术，它主要决定谁可以记账，会影响整个系统的安全性。去中心化的特性使得区块链需要大多数节点共同参与维护整个系统的运行，遵守同一种协议规则也是必须的，PoW机制指的是完成一定的工作量才能生成一个新的区块，每个节点根据自己的计算能力进行哈希运算来争取打包区块的权利。该机制可以有效地抵御女巫攻击。

激励层：主要包括发行机制和分配机制，在区块链系统中，共识节点可以通过打包区块及通过消耗自己的计算资源成功验证和记账来获取相应的奖励。激励机制将经济因素引入区块链体系结构中主要是让节点都愿意遵守区块链的规则，惩罚不遵受规则的节点，实现系统的良性发展。

合约层：主要包括了脚本代码、算法机制和智能合约。智能合约的概念最早是在 1995 年由 Nick Szabo 提出的，智能合约就是可以运行在以太坊上的程序，以太坊就是新一代的区块链系统，其进一步完善了区块链底层中的合约层，而智能合约的出现为区块链提供了可编程的特性。智能合约的执行不需要任何信用方，只要达到智能合约的约束条件就可以自动执行。

应用层：主要包括各种应用场景和案例等。通过应用层提供用户可编程接口，允许用户自定义、发起和执行合约。例如基于以太坊的各种区块链的 DAPP 都部署在应用层。可编程货币和可编程金融也包括在应用层。

2. 区块链主要安全威胁

近年来，区块链以价值安全转移、数据安全存储为用户广泛使用。区块链底层从技术上来说有一系列加密算法和数字签名方式确保交易安全，又依赖于共识机制来产生区块，以组成一种随时间戳排序的链式结构来保证数据的不可篡改。尽管如此，目前区块链依然面临着巨大的安全威胁，基本可分为算法安全威胁、协议安全威胁、智能合约安全威胁、用户使用安全威胁和网络安全威胁5种。

（1）算法安全威胁

区块链底层本身采用了密码学算法的很多机制，例如比特币采用了 SHA256、RIPEMD160 哈希算法和椭圆曲线密码学算法，以太坊采用了Keccak256哈希算法和椭圆曲线密码学算法。除了比特币和以太坊，其他区块链同样会使用一些其他的哈希函数、加密算法和数字签名方法来保证自身的安全性。就

目前而言，这些正在使用的算法都是相对安全的，但在一些特殊情况或者面对未来发展的背景下，这些算法可能会变得不安全。主要有两个方面的安全挑战：

哈希函数：哈希函数可能会发生哈希碰撞现象，哈希碰撞指的是不同的输入数据通过同一哈希函数计算后生成了相同的哈希值，这种情况的出现取决于哈希值生成的算法。2017年7月麻省理工(MIT)研究者就发现了新型数字加密货币 IOTA 中的加密哈希函数 Curl 中存在着严重的哈希碰撞漏洞，从而导致无法保障 IOTA 的数字签名和工作量证明(PoW) 的安全性，次月IOTA 团队就将Curl 哈希算法替换成了SHA3 哈希算法。目前，MD5和SHA1 哈希算法都已经被破解，SHA256依然是安全的，但SHA256 的安全性也因为MD5和SHA1的破解而降低，Keccak256哈希算法就因此诞生，其就是SHA3哈希算法的前身。

量子计算技术：量子计算技术正在飞速发展中，该技术的成熟将会对当今密码学算法造成极大影响。现在密码学算法是安全的，主要原因是没有任何方式能短时间计算出复杂的数学难题，如果量子计算机成功诞生，其运算速度远远超过现在的计算机系统，那么目前的密码学算法对于量子计算机来说就是一个简单问题。根据对传统密码算法和量子计算技术的研究，量子计算技术对如今密码体制的威胁如表所示。

加密算法	类型	作用	理论基础	安全性威胁
AES(高级加密标准)	对称密码体制	加密	字节/字运算	破解难度减半
SHA256	哈希算法	数字指纹	—	破解难度减半
RSA	非对称密码体制	加密、数字签名	大整数分解	失效
DSA(数字签名算法)	非对称密码体制	加密、数字签名	离散对数	失效
ECDH(椭圆曲线迪菲-赫尔曼密钥交换)	非对称密码体制	加密、数字签名	椭圆曲线离散对数	失效
ECDSA(椭圆曲线数字签名算法)	非对称密码体制	数字签名	椭圆曲线离散对数	失效

量子计算技术对密码体制的威胁

因此，在量子计算技术完全成熟之前，必须有能够对抗量子计算的新型密码体制出现，否则一切运用现有密码体制的事物都将失去原有的安全性。在未来，尤其是与密码体制紧密相关的区块链技术，更

需要具备抗量子计算的密码体制来保证其安全性。

（2）共识协议安全威胁

共识协议是区块链的重要组成部分，在生成区块时需要依赖于区块链的共识机制来选择矿工打包区块。因此黑客会针对不同的共识机制，采用各种手段来破坏共识原则，以此控制整个区块链的走

向，从而让自己获利。目前主要的共识协议攻击手段有双花攻击、自私挖矿攻击(Selfish Mining)、短程攻击(Short-Range)、长程攻击(Long-Range)、币龄堆积、预计算攻击(Pre-Computation)、女巫攻击(Sybil Attack) 等。

双花攻击：双花攻击主要针对工作量证明(PoW) 共识机制，指的是攻击者通过某种方式拥有了区块链全网络上一半以上的算力，并通过其算力让区块链产生分叉，从而引导主链走向改变的攻击方法。例如，攻击者A预先准备好100个BTC，并且其拥有比特币区块链上一半以上的算力，攻击者把100个BTC投放到交易所，然后用其一半以上的算力开始挖矿，等待投放完毕后，攻击者A将交易所里的100个BTC兑现。由于攻击者A拥有一半以上的算力，可以控制比特币区块链的走向，让主链变成未包含其投放 100 个 BTC 到交易所行为的分叉链，从而使得投放行为失效，100 个 BTC 返回到攻击者手中，然而此时攻击者已经获得了 100 个 BTC 兑现的资金，这就是攻击者通过双花攻击来无偿兑现的过程。

自私挖矿：自私挖矿是指攻击者在计算出新区块的哈希值时(即发现有效区块) ，不将其发现新区块的消息广播给区块链中的其他节点，然后继续挖新区块的下一个区块，直到其他挖矿者挖到有效区块时，攻击者就把先前挖到但未广播给其他节点的所有区块公开，因为攻击者已经成功发现多个连续的区块，所以攻击者所在的链分支比其他分支更长，从而使得区块链主链走向由攻击者控制。尽管有研究者表明这种方式很难实施，但其安全隐患依旧存在。

短程攻击：短程攻击是指攻击者在区块链中提交一笔交易，在该笔交易打包到新区块时，攻击者依然在该新区块的前一个区块上进行挖矿，一旦另一个分叉的区块比包含该笔交易的分叉区块更多，那不包含该笔交易的分叉就成为了区块链主链，攻击者就达到了交易回滚的效果。常用的短程攻击是贿赂攻击，即攻击者贿赂其他挖矿者，帮他回滚交易。短程攻击的本质也是双花攻击。

长程攻击：长程攻击是短程攻击的升级版，攻击者已经拥有一大部分区块链算力资源，采用其拥有的算力资源直接让区块链产生分叉，只要长时间未被其他诚实节点发现，区块链主链走向必定会受攻击者主导。常见的长程攻击就是51%攻击。本质上依然是双花攻击，然而该攻击方式实际上更多出现了权益证明协议(PoS)共识机制，因为 PoS共识机制不通过算力来选择矿工，相比PoW共识机制消耗的资源少。

币龄堆积：通过币龄堆积的方式来进行攻击主要是针对权益证明协议(PoS) 。PoS 共识机制是根据币龄来选择打包区块的矿工，所谓币龄就是根据持有货币的量和时间计算出的一个指标数，币龄越高成为矿工的概率就越大。每打包一个区块，对应矿工的币龄都会清空。攻击者在拥有一定数量的货币后，可以通过持续拥有该数量的货币来堆积币龄，币龄足够大时，就能主导区块链区块的生成。攻击者若有足够多的货币，也可以将货币分散到多个节点，通过分布式堆积币龄来共同控制区块链走向。

预计算攻击：预计算攻击是指攻击者通过随机试错的方式来控制前一个区块的哈希值，从而更容易计算出下一个区块的哈希值。

女巫攻击：由于区块链节点随时可能加入或者退出，为了维持区块链网络数据稳定，同一份数据通常需要备份到多个分布式节点上，这就是区块链数据冗余机制。若区块链网络中存在一个恶意节点，那么同一个恶意节点可以具有多重身份，就像一个细胞可以分裂出多个细胞一样，恶意节点也可以进行分裂。那么原来需要备份到多个节点的数据被欺骗地备份到了同一个恶意节点，因为该恶意节点进行了分裂，伪装了其多重身份，这就是女巫攻击。

（3）智能合约安全威胁

进入区块链2.0时代之后，智能合约成为区块链中必不可少的一部分。在让区块链能实现更多功能的背景下，由于智能合约的编写依赖于开发人员的主观性，造成智能合约代码出现很多意想不到的漏洞，往往这些漏洞会让用户遭受巨大损失。在经历的各大安全事件和智能合约漏洞挖掘者的助力下，常见的智能合约漏洞主要被分为如下几类:

重入漏洞:智能合约编程具有面向对象的思想，本质上一个智能合约就是一个类，因此在与区块链交互的功能操作非常复杂的情况下，通常需要进行合约调用合约的操作。一旦多个合约相互调用的关系变得复杂，就可能会出现代码重入的问题，所谓代码重入就是在某个时刻调用方法中断以致于执行其他的合约代码，该合约代码又再次调用了该发生中断方法，一直反复进入该方法。攻击者就会利用代码重入问题，让程序反复执行攻击者的恶意代码，以从中获利。在ERC20 合约中经常出现的withdraw函数就可能出现重入问题，代码如下所示:

```
function withdraw( uint _amount)  public {
    if( balances [msg. sender] > = _amount)  {
      if( ! msg. sender. call. value( _amount) ( ) )  {
        throw;
      }
    }
}
```

该代码首先对余额进行审核，再从msg．sender账户地址中转出以太币，最后修改balances数组中的余额。当函数执行到 msg．sender．call．value(_amount)( ) 时，攻击者就能通过 msg．sender 的fallback函数重复调用withdraw函数，导致msg．sender账户的以太币一直在输出，直到余额不足。

整数溢出漏洞：2018年，“清华-360 企业安全联合研究中心”ChainTrust 团队对 Etherscan 上的 390 份合约进行了完整分析，发现共有 25 个智能合约具有整数溢出漏洞。整数溢出漏洞的类型繁杂，在这 25 个合约中主要有高卖低收(underSell) 漏洞、下溢增持 (ownerUnderflow)漏洞、随意铸币(mintAny) 漏洞、超额铸币(overMint) 漏洞、超额定向分配(allocateAny) 漏洞和超额购币(overBuy) 漏洞。所谓整数溢出是由于计算机中整数具有上限和下限，如果当一个整数超过其上限或者小于其下限，那该整数

就可以从一个很大的数变成很小的数或者从一个很小的数变成很大的数，这种现象在合约进行转账的过程中很容易被黑客攻击者作为攻击点，以此实现无偿获取货币的目的。

tx. origin和msg. sender混淆漏洞在以太坊的solidity智能合约语言里，语言开发者为用户提供了tx. origin和msg. sender变量来获取账户地址。然而，很多合约开发者经常将这两个变量混淆，尽管它们的本质含义截然不同。假设当前有合约A调用合约B，合约B调用合约C，那么在合约C中的tx. origin是合约A的地址，msg. sender是合约B的地址。也就是说，tx. origin变量获取的是发送交易的最初调用方地址，msg. sender变量获取的是直接调用方的地址。若合约开发人员在开发过程将这两个变量混淆，将会发送意想不到的错误结果。

拒绝服务漏洞：拒绝服务漏洞就是攻击者通过某种手段让某些代码逻辑执行失败，以这种方式持续消耗调用合约需要的gas。例如，攻击者可能会将合约中的某些数组或者映射的大小设置成巨大，当合约对这些数据或者映射进行循环遍历时，就可能由于消耗的gas过多而执行失败；还可能某些合约在执行前，调用者必须通过一些验证，如果调用者由于某些原因无法进行验证，则无法正常调用合约；攻击者可以设定一个持续拒绝调用的合约，来阻止其他人对合约进行调用。

关键字过时：目前，solidity语言更新迭代的速度非常快，以致于很多智能合约开发者无法很快熟悉最新版本。由于最新版本可能与旧版本并不兼容，智能合约开发者可能会使用某些在新版本中过时的关键字来实现想要的效果，此时智能合约开发者可能并不知道这些关键字过时了，最终导致整个智能合约执行的效果与预期不符，甚至由于没有关键字的限制发生一些严重的错误。

未检查返回值漏洞：solidity语言提供了几种外部调用的函数方法:call()，callcode()，delegatecall()和 send()。这些函数方法具有bool返回值，然而在计算错误方面的行为与其他solidity函数方法完全不同，这些函数产生的结果并不会广播给所有人，并且不会导致当前执行中止。这些函数返回一个布尔值为false之后，继续执行接下来的代码。如果开发者并没有发现这种问题的存在，那当不满足条件返回false时，程序还会继续进行，最终得到一个无法想象的结果。

短地址/参数漏洞：2017年4月，Golem项目在一篇博文中提及发现了一个影响交易的安全漏洞。根据该帖子，当某些交易所处理ERC20令牌的交易时，没有对账户地址长度进行输入验证。这导致传送给智能合约转账函数的参数异常，以及传输金额的一系列错误问题。短地址攻击是EVM本身接受不正确填充参数的副作用。利用这一点攻击者可以通过使用专门制作的地址来进行攻击。例如某交易所具有交易功能，可以接收收件人地址和金额等信息。然后，函数接口transfer(address to，uint256 amount）使用填充参数与智能合约函数进行交互，将12位零字节的地址(预期的20字节长度）预先设置为 32字节长，Bob 要求Alice 转让他20个代币。但Bob恶意地将Alice 的地址截断以消除尾随的零，Alice使用交换接口和Bob较短的19字节地址进行交互，该接口用12个零字节填充地址，使其成为31个字节而不是32个字节，有效地窃取amount参数中的一个字节。

最终，执行智能合约代码的EVM将会注意到数据未被正确填充，并会在amount参数末尾添加丢失的字节。有效地传输256倍以上的令牌。

交易顺序依赖：在区块链中发起的交易需要经过矿工的打包才能最终记录到链上，在打包过程中，这些交易的打包顺序是具有优先级的，矿工通常会选择那些具有更高gas费用的交易优先打包。由于存在这种机制，攻击者完全可以通过支付较高的gas费用来阻碍其他低费用的交易，导致某些交易无法正常执行。

合约构造函数与合约名不一致：智能合约开发人员，可能会由于不够细心等原因，将构造函数名写得与合约名不同，这样会导致该函数不再是构造函数，能被其他人调用。这种情况的风险在于构造函数的目的通常是初始化某些合约变量，如果能被其他人调用，那合约的数据就会发生异常，即在不应该重置的时刻发生了数据重置。

时间操作/伪随机：在智能合约中，很多地方需要用到某些数据上链的时间，由于区块链并不是发起交易即上链的形式，需要经过矿工挖矿之后才能真正上链，因此数据上链时间很大一部分取决于矿工。在solidity语言中通过block. timestamp或者now来获取时间戳，可能缺乏时间的真实性。还有许多开发者，会利用block. timestamp 或者now来生成随机数，这样的行为是不妥当的，若矿工是恶意节点，那该时间戳可能会受到恶意矿工控制。

（4）用户使用安全威胁

区块链的安全性不仅仅在其本身，也有可能出现在区块链用户上。区块链用户可以分为开发者用户和普通用户，不同的用户类型会执行区块链系统中不同的功能操作。攻击者会根据用户身份进行针对性攻击，主要分为节点暴露 API 接口和钱包私钥窃取两种情况。

节点暴露 API 接口：由于目前大多数区块链平台对于开发者来说，并没有一些比较友好的区块链应用集成开发平台(IDE) 供开发者进行开发。但前不久，美国硅谷技术团队黑曜石实验室(Obsidian Labs) 发布了EOS Studio，该平台就是为EOS区块链量身定做的集成开发平台。如果这样的集成开发平台被普及，那节点暴露API的问题可能会更少地出现，就目前来说，作为开发者的区块链用户，依然需要通过各种区块链提供的API来进行开发，通常开发者用户会频繁调用这些 API来减轻开发负担。攻击者就可能会针对这些开发者节点进行攻击，通过开发者节点来控制这些API来获取区块链中一些重要信息。

钱包私钥窃取：相对于开发者用户来说，普通用户的比例更大。普通用户最频繁的操作就是登录区块链钱包进行货币交易，通常普通用户的安全意识也比较匮乏。在普通用户用其区块链钱包进行交易时，必须是以“热钱包”形式存在，也就是必须要连接到区块链中，此时该节点用户就是在线的。黑客攻击者就可能在这种时候入侵该节点用户，从而窃取该用户的钱包私钥，进一步盗取用户钱包中的货币资金。

然而离线的钱包（“冷钱包”）依然有可能被黑客攻击，黑客能通过社会工程学或一些物理攻击手段来窃取用户钱包的私钥，以达到盗取货币的目的。所以普通用户需要加强安全意识，最好的方式就是将私钥记忆在脑中或者锁进保险箱内。

（5）网络安全威胁

凡是网络都会存在病毒类的恶意程序威胁，区块链系统也是一种新型网络架构。攻击者会直接对区块链网络进行持续攻击来盗取货币资金，或者采用间接方式来敲诈拥有区块链货币的用户。主要的威胁形式有BGP路由广播劫持、伪造数字签名和勒索病毒。

BGP路由广播劫持：BGP是自治系统间的路由协议。BGP交换的网络可达性信息提供了足够的信息来检测路由回路，并根据性能优先和策略约束对路由进行决策。攻击者利用BGP路由的重定向，能利用其他矿工节点为自己挖矿。基本劫持流程：当某一矿工A连接到有效合法的矿池请求和接收任务，劫持者就开始进行攻击，在矿工A尝试连接矿池过程中，劫持者会通过一个新的BGP将矿工A的路径定向到一个恶意矿池，并维持这种定向。将第一次被劫持过的矿工连接到第二个劫持者的恶意矿池，避免重复劫持。此时攻击者就能停止攻击，矿工A就会免费作为攻击者的挖矿劳动力。

伪造数字签名：攻击者通过伪造企业的数字签名来躲避验证，并且诱导普通用户将其货币资金转给自己，从而无偿地骗取用户，让自己获利。一般分为以不可忽略的概率推算出系统的私钥和有效的通用性攻击算法两种伪造攻击方式。例如对于多重签名来说，攻击者根据身份的不同可以分为3类：签名发起者和收集者、内部的其他签名者和外部攻击者。不同身份对于搜集攻击所必备的数据信息的难易程度也是不同的，通常签名发起者最容易搜集到攻击所需数据，内部其他签名者次之，外部攻击者最为困难。假设攻击所需的必要数据就是各个签名者的数据D，通过该数据D能窃取到签名者的私钥。如果攻击者是签名发起者和收集者，那么他可以合法地接收到其他签名者的数据D；内部其他签名者在内部网络中偷听或截取数据D；外部攻击者要首先入侵内部网络然后再实施网上偷听或截取。另外，对于多重签名来说，能成功窃取签名者私钥的完全攻击还分为两类:一类是仅能伪造单个签名者的签名，另一类是既能伪造单个签名，又能伪造多重签名。后者相对于前者而言，攻击更完全。

勒索病毒：2017 年5月，全球近100个国家的微软系统计算机同时遭到名为想哭吗(WannaCry) 或想解锁吗(Wanna Decryptor) 的电脑病毒袭击。如果被感染病毒的计算机想要解除锁定，只能向对方支付所要求的比特币，否则硬盘将被彻底清空。这一场比特币勒索事件更是波及到了国内多个高校，导致高校产生巨大损失。尽管这种攻击方式并没有直接攻击区块链系统，但攻击者利用比特币的匿名性让被感染用户进行匿名转账。勒索方式不仅限于加密计算机文件，还有其他侵害计算机用户个人利益的手段。本质上就是结合区块链技术的传统网络威胁。

（本文来源于《南京邮电大学学报（自然科学版）》2019年第5期《区块链技术安全威胁分析》，作者为南京邮电大学计算机学院孙国梓、王纪涛、谷宇。已获得该期刊及孙国梓教授授权刊发。孙国梓教授：区块链技术安全威胁分析（下），请关注《江苏可信区块链（电子月刊）》第6期“专家特稿”）

二、活动路演

1.2020中国区块链技术产业发展峰会暨南京创新周鼓楼分会场开幕式成功举办

南京市政协主席刘以安致辞

6月21日，2020中国区块链技术产业发展峰会暨南京创新周鼓楼分会场开幕式成功举办。南京市政协主席刘以安，中国计算机学会区块链专委会主任斯雪明，江苏省发改委原主任、南京大学博士生导师钱志新，南京大学博士生导师、长江学者仲盛，江苏省计算机学会秘书长金莹，南京邮电大学教授孙国梓，国家超级计算长沙中心教授彭绍亮，南京博雅区块链研究院院长司华友，南京林业大学党委副书记、副校长刘中亮；南京市相关部门、大数据集团等部门负责同志；南京市鼓楼区领导刘军、洪礼来、陆敏、周文中、丁健生、高军玲、冯泉、陈海涛和区相关部门、街道主要负责同志；线上嘉宾挪威工程院院士容淳铭，挪威工程院院士、挪威奥斯陆大学教授张彦，亚洲区块链产业研究院院长陈柏珲，中国信息通信研究院云计算与大数据研究所所长何宝宏，中国人民大学法学院副院长、长江学者杨东以及一批国内外知名高校教授参加此次活动。

南京鼓楼区委副书记、区政府代区长洪礼来讲话。洪礼来说，创新是第一动力，区块链代表着互联网的未来。习近平总书记强调，“要把区块链作为核心技术自主创新的重要突破口”。鼓楼区作为南京中心城区和省会功能核心区，将全力推进 “创新名城引领区”建设，努力抢占区块链发展制高点。

鼓楼，区块链创新起步早、工作实，未来将从空间规划、专业孵化、人才培养、生态体系、平台建设、政策扶持等多方面系统推进区块链产业加快发展，将积极引入社会资本设立创投基金、产业基金，以资本赋能发展，尽快培育一批瞪羚和独角兽企业，努力为南京创新名城建设添活力、增动力。

鼓楼，区块链发展潜力大、前景广。鼓楼区将激活创新动能、专注技术驱动，共谋产业发展、加速深度融合，力争将区块链先导区建成“国家级区块链产业示范点”。

2020中国区块链技术产业发展峰会暨南京创新周鼓楼分会场开幕式结束后，2020中国区块链技术产业发展峰会主题报告和各分会场活动相继进行。此次活动聚焦国际区块链前沿技术与产业话题，专家学者、行业大咖、企业菁英等共同分享区块链技术创新与发展应用，深入探讨数据共享与可信体系建设，探索建立区块链人才培养体系，合力构建区块链技术应用和产业发展新高地。

2.“5G+区块链技术应用交流会”在华为南研所举行

“5G+区块链技术应用交流会”活动现场

6月29日下午，“5G+区块链技术应用交流会”在华为南京研究所举行。

江苏省互联网协会秘书长、江苏可信区块链专委会主任刘湘生，华为云中国区互联网行业总监李治慧，江苏省城市发展研究院副院长、江苏可信区块链专委会特聘顾问王兴亚，南京理工大学博士、教授、博士生导师、知识产权学院常务副院长、江苏可信区块链专委会特聘专家戚湧，华为云江苏行业拓展总经理曹劲，互联网行业、区块链行业、新闻媒体及华为南京研究所的专家及企业家代表共60余人参加了交流活动。

曹劲致开场辞。他表示，江苏在数字经济领域取得了令人瞩目的成绩，包括智慧城市、物联网、人工智能等诸多方面，华为从通信网络设备、ICT建设、 城市与产业智能化、教育与科技创新等全面开展，助力江苏政企智能升级，激发数字经济的新活力。在全国疫情防控和复工、复产、复学上，5G、大数据、云计算、人工智能等新技术和新应用发挥了巨大的作用，在线教育、远程办公、智慧医疗、直播带货等新消费、新业态破土而出，这些都体现出新技术和新应用给各行各业带来的巨大价值。随着科技的发展与应用创新，未来5G、云、AI、区块链的有机结合，一定会给全行业带来巨大的变革与机会。

曹劲致开场辞

戚湧作《区块链在智慧交通领域的应用》的主题报告

戚湧教授带来主题为《区块链在智慧交通领域的应用》的主题报告，他在报告中指出，随着可扩展性和效率的提高，区块链技术在社会各个领域中落地应用场景，推动现实社会向“可编程社会”转变。因此，区块链技术有可能成为“万物互联”的一种最底层的协议和秩序互联网。在智慧交通方面，借助5G技术高传输、大带宽、低延时的特性和区块链技术数据共享、隐私保护等特征能够促进先进信息技术与交通运输深度融合，实现以“数据链”为主线，加快交通运输信息化向数字化、网络化、智能化发展，为交通强国建设提供支撑。戚湧教授提出，以全国交通运输业数据作为主数据链，以区块链账本和基础数据仓库构建数据记录层，智能合约等中间件完成数据交互，从而为交通运输业数据交换共享、业务流程优化制定顶层框架，实现

交通运输全过程的数据透明化、清晰化。

本次交流会分上下两个半场。上半场中，华为云中国区互联网行业总监李治慧、苏州黑云信息科技有限公司CTO　傅朝阳、浩鲸科技河图产品市场总监李红纲分别作《5G+X共创新动能》《区块链数据协同——分布式算法共识框架》《5G消息赋能新金融科技》的交流分享。

在下半场中，江苏荣泽信息科技产品总监张辉、华为运营商5G资深专家孟凡辉、中诚区块链研究院产品总监李瀛分别带来《区块链实现政务业务高效协同》《5G加速，中国经济新动能》《区块链+城市建设供应链金融》的技术应用交流分享。

王兴亚与现场嘉宾互动交流

王兴亚院长与现场参会企业家们作互动交流。他说，江苏省互联网协会通过活动中建立平台和载体，引领江苏省互联网企业走向技术高端的对话，交流会中每一位演讲嘉宾都展示出让人眼前一亮的核心技术和应用展示。同时他认为，5G与区块链技术作为现代信息技术架构中最新的两个技术，对5G+区块链的应用探索是极具创造性与可行性的研究方向，两个技术的融合应该是一个相互碰撞的化学反应而不是简单的叠加，希望能够在不久的将来看到更多5G与区块链技术融合应用的落地场景。

刘湘生秘书长作总结讲话，他不但对在江苏从事5G、区块链产业的企业家提出了殷切的希望，更对江苏的5G、区块链相关行业企业指出了新的、可达到的方向及高度。他认为，区块链能够实现信息隐私保护、防篡改、可追溯等，5G本身在网络设备安全、用户隐私信息安全等方面的短板可以基于区块链得到弥补，因此，区块链与5G的融合应用一定有更多的应用场景。目前绝大多数的应用场景还没有借助5G的低延时、大带宽、广连接的技术特性，他建议参会企业的技术负责人可以先从某一个技术特性出发，探索与边缘计算、区块链等新兴技术的融合思路。

刘湘生作总结讲话

刘湘生认为，未来5G+区块链的应用必定会在江苏出现更多的应用场景，他鼓励企业家们积极跟上5G与区块链国家战略发展的步伐，把握住5G与区块链融合发展的机会，希望5G和区块链相关的企业打破成见与割裂，共同探索技术、场景的融合，将区块链的技术特性融入到5G的产业生态中发展。

本次交流会活动由江苏省互联网协会主办，江苏可信区块链专委会、江苏（云与计算）华为云协办，新华报业传媒集团、中国江苏网、荔枝网、新华网、龙虎网省市媒体作支持单位，南京天泽广告传播有限公司策划。（李正豪）

3.2020南京“区块链与产业互联融合应用论坛”顺利举办

6月18日，作为2020南京创新周的高端论坛之一，由江北新区管委会主办的“科技赋能 · 链动未来”区块链与产业互联融合应用论坛在江北新区成功举办。江北新区管委会副主任陈潺嵋，南京市大数据管理局副局长何军，南京市地方金融监督管理局副局长陈新颜，中国工程院院士、北京邮电大学教授张平，工业和信息化部原副部长、中国信息化百人会学术委员会主席杨学山，华为中国区块链高级专家周俊等数百名来自政府、学界和企业界代表现场或线上出席本次论坛。荣泽科技作为协办单位出席本次论坛。

江北新区管委会副主任陈潺嵋发表致辞

江北新区管委会副主任陈潺嵋在致辞中表示，区块链技术的集成应用在新的技术革新和产业变革中起着重要作用。

活动现场，江北新区自贸区综合协调局局长张乐对日前发布的《江北新区（自贸区）促进区块链产业发展若干政策措施》做了深度解读。该政策对新区区块链企业给予落户、经营、应用、培训、金融等各方面的扶持，基本覆盖了区块链产业的各个环节，切实推进新区区块链的技术发展和场景应用。

国家工信部原副部长、北京大学教授杨学山先生做了《以事务为中心看新基建、数字化转型和智能化》的主题报告。杨学山表示，信用体系是数字化转型和新型技术设施中的重要组成部分，以事务为中心，将网络、数据、技术手段、标准制度连接起来，提供了新的基础设施和社会服务。经济社会的发展，对于承担具体事项的机构/企业来说，要有工业技术和信息技术融合一体的新技术体系。企业要将一个个环节和一个个过程中显性化、结构化、标准化的数据和知识转变为企业的组织知识和组织能力，累计到软件和系统中，形成可重用的企业新型基础设施，来提高企业的可持续发展能力以及核心竞争力

中国工程院院士张平围绕《新基建中的使能技术》展开，他认为区块链技术是非常有价值、有前景的一种应用技术，在新一轮的区块链发展浪潮下，区块链的产业发展更需要厘清相关问题、深度挖掘其存在和发展的价值，更好地为城市的经济产业发展做出更大贡献。

江北新区科技创新局局长聂永军发布了江北新区数据DNA计划，启动了数据开放平台“引链”。该平台旨在保护数据安全隐私的前提下，鼓励企业、社会组织和个人对公共开放数据进行增值再利用，重点以企业服务、科技创新、知识产权、金融服务、医疗健康、市场监管、民生服务等领域开放应用为牵引，打造数据开放融合生态体系，用数据实现兴企惠民。江北新区科技型企业将根据数据资

。

源开放清单，结合各自业务需求，定制数据应用合作场景，在保护数据安全隐私的前提下，通过部分开放应用的先行先试，唤醒政务数据，推动更多领域数据开放，逐步形成国内领先的，以数据为关键生产要素的创新生态体系。

在 圆桌论坛环节，针对“数字化转型在哪些环节需要区块链技术”、“区块链技术助力数字化转型的机理”、“区块链推动数字化转型的成功案例”嘉宾展开讨论与分享。荣泽科技董事长、总经理钟晓就区块链技术如在企业数字化转型中如何应用和落地分享了三个观点：第一，首先要形成对区块链新技术的共识，而且要有目标、有重点地去形成共识；第二，区块链技术不是孤立的，作为新基建中的“新基建技术”，它必须与其他先进的技术相融合，才能在各个行业更广泛的应用和落地。业务场景驱动，同时加强技术含量并持续改进，才能更好地助力数字化转型；第三，区块链技术必须要依托金融、物流、制造业、农业等产业，只有依托产业才会有生命力。

4.“2020一路同行精品路演系列沙龙”（第三场）活动成功举行

“2020一路同行精品路演系列沙龙”第三场活动现场

6月24日下午，“2020一路同行精品路演系列沙龙”（第三场）活动在南京市建邺区金财大楼一楼会议厅举行。

江苏省互联网协会秘书长刘湘生、南京建邺区江东商贸区党工委书记、管委会主任郑知邦、七星投资集团副总经理、华亚创投总经理马霞薇、清华大学大数据研究中心副主任卜晓军作为路演点评嘉宾出席本次活动，路演方、投资人、企业代表近50人参加了路演沙龙。

南京建邺区江东商贸区党工委书记、管委会主任郑知邦致开场辞。他表示，江东商贸区始终坚持市场导向，在建邺区中率先探索园中园的运作模式，以优质服务引领园区创新发展，致力构建创新生态体系，为企业发展提供强有力的政策支持，吸引直投基金、创投机构为园区企业的创新发展提供全生命周期的金融支撑。

郑知邦致开场辞

南京翼太源信息科技公司CMO顾晏作《区块链证书发行查询解决方案项目》的主题路演。顾晏提出，签书区块链电子证书服务平台是一个一站式的证书服务平台，现了证书的完全电子化，将“最多跑一步”提升为“一步不用跑”，同时区块链技术将实现证书的保真与多方确认，降低证书行业的

顾晏作《区块链证书发行查询解决方案项目》的主题路演

信任成本。签书还可以支持定制化，发证机构可以根据自己的业务需求定制电子证书服务。签书底层采用自主研发设计的，国产可控的区块链底层平台，具有高可用性，高定制化，低成本的优势，可以根据不同发证机构的不同需求做具体的定制化操作。同时，签书区块链电子证书服务平台还融合了阈值签名和零知识证明等先进技术，以实现证书在区块链上的多方“盖章”确认，同时保护相关方的隐私。

此外，苏州思达通教育投资有限公司总裁曹笋、江苏瑞丰信息技术股份有限公司副总经理吴胜誉、清数云医科技有限公司副总裁张超作为路演嘉宾参加本次沙龙，南京农纷期电子商务有限公司副总裁袁冬梅、苏州黑云信息科技公司CEO谢绍蕴、智通三千投融资总监叶飞分享各自企业的商业模式。

马霞薇进行路演点评

七星投资集团副总经理、华亚创投总经理马霞薇对参与路演的四家企业分别做了详细的指导和点评。她认为，参与路演的企业项目都非常优质，确实在针对性地解决社会中的一些痛点问题，部分企业项目在细化后可以实现全面铺设推广。同时她建议，资本方除了资金的介入，更重要的是实现资源的对接，帮助企业补足自身短板，将企业项目的细节夯实，使企业能够在资源支持、市场配置以及相适应匹配的专业性资本方指导下快速发展壮大。

清华大学大数据研究中心副主任卜晓军对参与路演的四家企业分别做了点评。他认为，参与路演企业都是和目前数字经济的发展趋势相结合，紧扣南京创新周的主题，为行业提供细化垂直的服务。他建议企业既要大胆开拓也要如履薄冰，可以适时对标已成熟的商业模式，将商业模式和资金流与信息流相结合，确保盈利模式在高价值方向上实现突破，让企业在一到一百的发展阶段走的更加平稳。

卜晓军进行路演点评

刘湘生作总结致辞

刘湘生秘书长做了“2020一路同行走向美好”的总结致辞，致辞表示，江苏省在垂直领域具有大量的数据平台，这些数据平台就是互联网行业所沉淀的资源池。目前，国家已将数据要素定义为资产，大数据平台型企业必将迎来高速的发展期。尽管受疫情影响，我们正在经历资本寒冬，面临融资难、融资贵、融资慢等问题，但我相信，只要企业能够抓住社会发展的趋势，服务于

整个社会，商业模式能够被市场所认可接受，就一定能够发展壮大。同时，互联网协会秘书长刘湘生建议，创业需要依据互联网的思维去完成平台化的战略，盈利模式要依照互联网思维去设计，互联网的思维是开放共享，唯有如此才能实现企业指数级的增长发展。最后，希望协会能够与企业及资方一路同行，共同走向美好。

本次路演活动由江苏省互联网协会、南京建邺区江东商贸区主办，七星创新集团、江苏省股权投资中心协办，众赞金服、南京天泽广告传播有限公司策划。（李正豪）

三、高端访谈

王鼎博士专访：发展区块链 赋能新基建

王鼎：博士，现任启迪控股高级副总裁、启迪数据资产研究院院长、启迪数字集团董事长、启迪区块链集团董事长。

4月20日，国家发改委举行例行新闻发布会，明确了新基建最新范围，将“区块链”纳入信息基础设施之中。在5月召开的全国“两会”上，“区块链”也成为代表委员热议的话题。近日，就“区块链”发展现状、面临挑战、存在痛点、主要作用、政策建议等问题，启迪数据资产研究院院长王鼎博士接受中国电子报等国内知名媒体采访。

记者：您认为目前中国区块链基础设施的发展现状如何？

王鼎：当前，我国区块链基础设施正处于高速发展阶段，技术集成创新能力逐步提升，产业和市场基础日益坚实，新产品、新应用、新模式不断涌现。区块链基础设施的开放性、通用性、使能性进一步显现，推动构建支撑数字经济和智慧社会发展的全新网络环境和价值交换体系。我认为主要有4个明显特征:

一是技术创新步伐加快。存储加密、共识算法和跨链协作等关键技术研发速度加快，共识机制从单一算法向混合共识方向演变。区块链与云计算、人工智能、大数据融合创新更加活跃，企业依托云服务资源加快部署Bass平台，区块链基础设施化特征更加明显。启迪区块链加快智能合约、数据沙盒、加密算法、可信交换技术、数据质量管控等群体性技术集成，研发了新一代数字融合基础设施（TDI），为打破数据孤岛，实现数据全链贯通，打造数据价值交互体系奠定了基础。

二是应用场景日益丰富。据不完全统计，目前全国已建或在建产业园区达20余个，区块链企业已超过1000家。越来越多的金融机构在跨行（境）支付、资产管理、供应链金融等业务活动中采用区块链

技术，数字人民币体系（DC/EP）的研发工作稳步推进。除数字资产管理和交易外，区块链在政务数据交换、物联网、智能制造、数字版权、产品溯源等领域应用场景更加丰富多元，在促进数据开放利用、推动要素高效流动、降低社会交易成本方面的作用已经显现，为构建有序的数字经济体系提供了坚实支撑。

三是产业生态正在形成。近年来，区块链市场热度较高，一批初创企业迅速崛起，形成了集聚发展的态势。互联网企业、新兴科技企业在硬件产品、加密算法、人工智能、平台服务等领域不断发力。各地也纷纷布局区块链相关产业，推进产学研用多方协作，涌现出一批面向应用的创新实验室、技术研发平台和开放式产业联盟，涵盖底层基础设施、应用支撑平台、行业应用开发以及周边配套服务的产业链初步形成。我国区块链专利申请数量已位居全球第一。

四是政策环境不断优化。习近平总书记在中央政治局第十八次集体学习时明确指出，把区块链作为核心技术自主创新的重要突破口，加快推动区块链技术和产业创新。为抢抓区块链发展的重大战略机遇，近两年来，全国各地密集出台相关政策，截至2019年底，全国发布区块链相关政策约290项。今年5月，浙江省宁波市发布《加快区块链产业培育及创新应用三年行动计划（2020-2022）》，广东省广州市出台《推动区块链产业创新发展的实施意见（2020-2022年）》，贵州省政府印发《关于加快区块链技术应用和产业发展的意见》。这些政策围绕提升区块链技术创新能力、推进“建链上链用链”、促进区块链从点到线在更多领域深化应用、探索创新区块链监管模式等方面，加强了政策引导和组织领导，加了大财政金融扶持、标准研制和人才引培，为区块链新基建赋能赋智奠定了良好的发展环境。

记者：目前，区块链作为新基础设施，将面临哪些挑战？其中的主要痛点在哪里？

王鼎：当前区块链热度虽高，但是区块链作为新基建仍面临不小挑战，主要有3个方面的表现：

一是需要树立对于区块链客观、理性的价值认知。区块链是分布式数据存储、点对点传输、加密技术、共识算法等多技术集成应用的结果，在数字资产管理与交易方面有着天然优势。由于公众对其颠覆式创新的预期和强金融属性的高度关注，造成区块链短期价值高估，甚至有形成泡沫的风险。但从长期发展看，其影响不不容小觑。区块链技术在实现信息化条件下的价值交互、构建新型社会信任体系、塑造数字经济发展新范式、催生新型价值创造方式等方面存在长期的商业机遇，其生命力将随着应用的普及而逐步凸显。

二是区块链作为新技术基础设施的就绪度较低。区块链技术仍是一项需要持续迭代完善的技术，分片、跨链、侧链等共性关键技术和共识机制、经济激励模型等仍处于试验测试阶段。标准统一、协作互认的区块链底层技术平台尚未形成，作为基础设施架构体系也不够清晰，与5G、云计算等新基础设施相比，区块链技术广泛应用和规模普及还有很长的路要走。

三是产业发展环境还需要进一步改善。从区块链应用来看，由于与现有监管体系的适应性等问题，目前鲜有与行业业务深度融合的大规模商用案。如何优化监管框架、增强监管政策弹性，妥善平

衡技术创新和风险管控的关系，是未来政策设计的关键环节。同时，区块链技术在规模应用、标准制定、人才储备方面还存在短板，这些问题，也需要在发展中协调解决。

记者：区块链作为基础设施，对经济、对产业及产业上下游有哪些带动作用？

王鼎：一是区块链为充分挖掘数据价值提供了使能工具。当前，我国跨部门、跨层级、跨地域间的数据碎片化严重，基础数据尚未互联互通，整合共享效率亟待加强，难以形成完整的数据链和全景数据，数据的要素作用难以充分发挥。启迪区块链通过对智能合约、数据沙盒、加密算法、可信交换技术、数据质量管控等群体性技术集成，可建立一套数据采集、存储、管理、分析、使用策略，实现数据全链贯通，让数据真正产生价值。

二是推动信息基础设施从计算资源供给向数据价值交互转变。区块链、智能合约、数据沙盒等技术发展，进一步丰富了数据基础设施的内涵，为数据安全可信交换、数据价值度量与传递，以及对数据进行全生命周期的管理治理都提供了新的工具。新型数据基础设施将为数据所有者（数据主体、数据生产）、管理者（数据传输、算法管理、数据治理）与使用者（数据应用），构建起实时精准、可信交换、全程全景、完整可溯的数据支持体系，这不仅意味着数据采集、传输、处理、应用和安全的能力会更强，也意味着为数据赋值、为管理赋权、为应用赋能将成为现实，以数据为核心要素的数字经济将得到蓬勃发展。

三是有利于形成数字经济新的价值空间。区块链正从底层与现有互联网基础架构融合集成，引导传统互联网从信息传递向价值交互转变，从6个层次拓展数字经济价值空间。在第一层，区块链与数据中心、4G/5G等集成融合，提升数字经济基础设施建设能力；在第二层，区块链与数据和网络集成应用，提升数据接入和利用能力；第三层，基于区块链和可信交换平台，提升经济社会基础信任能力；在第四层，通过构建共识算法和激励体系，塑造资产的数字化传递和交易能力；在第五层，通过智能合约和DAPP,培育形成产业链价值网络空间构筑能力；在第六层，构建产业价值运行和资源循环体系，形成健康良性发展生态体系。

记者：区块链作为新基建应该如何来建设？对于政策有哪些建议？

王鼎：三点个人建议：

第一，加快顶层设计，提高区块链基础设施的就绪度。一是出台国家层面的指导性文件，进一步明确区块链创新发展与应用的路径，引导各地遵循技术发展规律，科学规划布局区块链产业，着力解决基础研究、技术创新和市场应用衔接不畅的问题。二是加大对基础研究平台、共性关键技术平台的投入，探索建立重大基础理论、共性关键技术溢出的后向激励机制，引导产学研用围绕核心技术突破同向发力。三是研制统一的区块链底层技术平台参考架构，构建不同层级的共性能力平台。

第二，以协同创新牵引区块链规模应用。一是支持搭建核心技术研究与多种类技术融合的应用创新平台，研究区块链与人工智能、大数据、云计算等新一代信息技术的协作关系，通过技术组合效

应，形成综合性解决方案和技术支持体系。二是依托科研院所、重点企业，组织实施区块链领域创新能力建设工程，汇聚产学研用各方力量，打造一批区块领域技术创新平台，在全国构建点线面结合的创新网络，推动区块链技术在经济社会各领域的深度应用。

第三，完善区块链应用支撑体系。一是开展区块链技术应用标准体系建设，制定区块链技术统一术语、参考架构、评价体系等基础标准，确定区块链灵活性、可扩展性、延时、数据架构、可审计性、监管等内容，依托标准引导产业技术创新。二是推动区块链与实体经济融合，面向产品溯源、存证取证、数据共享、版权保护等重点领域，支持骨干企业打造一批可复制、可推广的典型案例，丰富行业应用，促进供需对接。三是构建区块链基建运行监测体系，实现有效管理和精准服务，推动数字基建高质量发展。四是推动高校与区块链企业合作，设置区块链专业课程，采用企业导师和高校导师轮流授课的方式，培育区块链专业人才。

（王鼎博士授权本刊发布）

四、江苏动态

1.江苏省科技厅江苏省工业和信息化厅联合发布《关于加快推动区块链技术和产业创新发展指导意见》

日前，为抢抓全球新一轮科技革命和产业变革的重大机遇，充分发挥江苏区块链产业基础较好、数据资源丰富、应用场景广阔的优势，加快推动江苏省区块链技术和产业创新发展，江苏省科技厅江苏省工业和信息化厅联合发布《关于加快推动区块链技术和产业创新发展指导意见》（简称《意见》）。

《意见》的基本原则是科技引领，重点突破；系统谋划，统筹布局；应用带动，开放创新；安全可控，规范发展。

《意见》的发展总目标是：区块链基础层、技术层和应用层实现全链条突破，技术创新能力处于国际先进水平，形成涵盖核心技术、关键系统、支撑平台和集成应用的完备产业链和高端产业群，畅通区块链创新链、应用链、价值链，为构建自主可控现代产业体系提供重要引擎，为建设科技强省、制造强省、网络强省奠定坚实基础。近期目标，通过3年左右努力，部分领域关键核心技术取得重大突

破，集聚一批高水平人才队伍和创新创业团队，建成若干国内一流的创新创业平台载体，区块链产业规模、技术创新能力和示范应用水平处于全国前列：区块链理论与技术体系初步建立；区块链产业竞争力居于全国前列；区块链发展环境和创新生态不断优化。

《意见》的重点任务是，一是强化区块链科研前瞻布局:强化前沿理论与应用基础研究，强化关键共性技术攻关，强化创新平台载体建设，强化人才智力支撑；二是推动区块链产业集聚发展：着力培育区块链新兴业态，着力培育壮大区块链企业，着力推动区块链技术在产业园区应用发展，着力推动区块链领域军民融合，着力加强区块链应用管理；三是加快区块链多领域多场景示范应用：区块链＋先进制造，区块链＋移动通信，区块链+物联网，区块链+数字医疗，区块链+现代物流，区块链+通信信息安全，区块链+金融，区块链+智慧农业，区块链+政务服务。

在保障措施方面，《意见》要求，一要加强统筹协调，二要加强政策扶持，三要加强国际合作，四要加强宣传引导。

2.苏州市长李亚平专题调研苏州市区块链产业发展情况

6月16日，苏州市委副书记、市长李亚平专题调研全市区块链产业发展情况。近年来，苏州积极推动区块链技术和产业发展，不断做强区块链技术的研究和应用。截至5月底，全市集聚区块链相关企业超过60家，区块链相关技术应用企业已达178家。在中央网信办公布的区块链信息服务备案项目中，苏州完成备案10个项目，占全省的28.6%。李亚平指出，要深入学习贯彻习近平总书记关于区块链的重要讲话精神，主动对标先进城市，立足苏州产业特点，走出一条特色化、专业化、市场化的区块链发展道路，努力实现从“先发”走向“领先”。李亚平要求，积极抢抓先机，加强政策引导，强化区块链技术和产业发展的规划布局。要发挥龙头企业的示范带动作用，加大政府统筹力度，支持骨干企业打造一批可复制、可推广的典型案例，打造区块链产业发展高地。要以金融领域为突破口，打造数字货币先行区。李亚平强调，要勇于创新，加速应用落地，着力构建区块链产业生态，推动区块链产业集群化发展，充分发挥区块链技术优势，推动更多看得见摸得着的应用场景落地。要加快推动区块链技术和产业创新发展，依托区块链技术赋能经济社会高质量发展。

3.集聚政产学研要素，赋能经济发展 无锡成立区块链产业联盟

6月23日，无锡市区块链产业联盟成立大会暨第六届“i创杯”互联网创新创业大赛在无锡高新区举办。联盟旨在以无锡区块链技术与应用的创新发展需求为基础和纽带搭建政产学研合作交流平台，提升无锡在区块链领域的知名度和影响力。

无锡拥有不少具备区块链技术核心能力，特别是底层关键核心技术，并参与多项相关国际和国家

标准研制的高新技术企业，恒为信息科技、中城智慧科技等一批区块链企业成功获国家网信办备案。2020年4月，工信部发布全国区块链和分布式记账技术标准技术委员会名单，恒为信息科技成为第一届委员会成员单位。无锡区块链创新创业日益活跃，已经形成良好的发展态势，在物联网、电子政务、产品溯源等领域涌现出一批有技术竞争力的企业。

无锡市副秘书长周浩明在会上发言表示，此次联盟的成立正当其时，对促进全市新经济发展也具有重要意义。未来要通过联盟的发展，进一步加大区块链企业的引进和培育；通过联盟的平台，进一步促进大家抱团发展，优势互补；通过联盟的努力，进一步加快以物联网为龙头的新一代信息技术产业发展。

无锡市区块链产业联盟由无锡市信息化协会、江苏恒为信息科技有限公司联合无锡市高校、科研机构和社会企业共同发起成立。联盟首批成员单位共61家，江苏恒为信息科技有限公司任会长单位，中国移动江苏公司无锡分公司、红豆集团有限公司、江苏中城智慧科技有限公司等15家单位当选副会长单位，无锡市财政局、江苏才标信息科技有限公司、无锡开云信息技术有限公司等45家单位任理事单位。

江苏省工业和信息化厅大数据产业处张北虹处长、无锡市人民政府周浩明副秘书长，以及无锡市委网信办、市工业和信息化局等部门有关领导出席本次大会，与联盟首批成员单位企业负责人及代表共同见证联盟的成立。

在未来发展中，联盟将围绕区块链技术研究、成果转化、应用推广、标准制定、教育培训、检测认证和产业发展等方面，提升联盟成员的研发设计和生产服务水平，构建无锡市区块链技术产业生态，促进区块链与经济社会各领域的深度融合，赋能无锡社会经济的高质量发展。

会议同期还进行了“i创杯”区块链专场路演，20个入围项目均是来自于全国各地基于区块链技术创新和行业应用的优秀代表。最终，自主安全可控的高性能区块链底层核心平台、基于区块链技术的疫苗追溯服务系统、基于跨链技术的服务集成和治理枢纽和可信认证基础设施与应用赋能平台4个项目脱颖而出，进入无锡总决赛，并取得省级比赛资格。

4.全国首个区块链医疗应用落地苏州昆山市

日前，苏州昆山市药事管理服务平台依托苏州移动区块链、大数据、云计算技术，在国内率先实现医疗机构电子处方向社会零售药店开放，实现就诊配药信息全程互享互通，全网支付，搭建病患、医师、药师以及相关监管人员之间的多元化购药监管平台。

在药事管理服务平台，患者可直接查询三年内在昆山本地医院就诊记录和处方信息，其中处方单可溯源追踪，并详细展示门诊信息、药品信息及处方来源。首次使用药事管理服务平台的昆山市民许女士说：“以往都是纸质信息，时间长了保存得难免不够完整，现在在智慧昆山APP上面，进入

药事服务管理平台，就可直接查询信息，并且还可以直接在上面买药，非常方便。

利用区块链技术，平台将患者的诊疗记录加密存放，保障患者隐私的同时，促进医疗信息的共享，创造安全、可信和便捷的医疗记录，具有高度的完整性和可信性，保证了数据的有效性和安全性，使得医院和医院之间能够实现连接并且及时无缝分享信息，而无需担心信息被泄露或者被篡改，保障了患者用药的安全性和可靠性，有利于提升医患关系。昆山市卫生计生信息中心主任金健表示：“通过对共享电子处方进行数据上链，处方不可篡改且全程可追溯，我们监管部门更加‘心里有数’了，解决了电子处方共享防伪性低、容易篡改、责任界定困难的三大难题。而区块链的引入更增加了我们平台的安全保障，服务监管溯源可靠，百姓就医配药更放心，提升了健康服务获得感。

区块链医疗应用促进了医疗服务与医疗模式的转变，在人工智能、大数据分析、物联网等技术的协同下，全新的远程医疗护理、疾病预测、按需服务、精准医疗将成为可能。后续苏州移动将进一步探索5G+区块链的创新应用研究，并积极推动在教育、医疗健康、食品安全等民生领域和政务领域的应用，助力信息化建设与数字经济发展。”

五、国内讯息

1.北京布局区块链产业“四大高地”赋能经济发展

北京市人民政府办公厅日前发布印发《北京市区块链创新发展行动计划（2020—2022）》的通知，力争率先形成区块链赋能经济社会发展的“北京方案”。

计划提出将原创引领与需求驱动相结合、系统布局与动态调整相结合、即期投入与持续支持相结合，预计到2022年，把北京初步建设成为具有影响力的区块链科技创新高地、应用示范高地、产业发展高地、创新人才高地，建立区块链科技创新与产业发展融合互动的新体系。

计划共设定4类重点任务，20项具体任务，包括打造区块链理论与技术平台、建设落地一批多领域应用场景、培育融合联动的区块链产业、建设领先的区块链人才梯队等。

在强化区块链基础研究和关键核心技术攻关方面，北京将支持在高性能计算、可信芯片、众智科学等重点领域开展研究，突破区块链共性理论问题。在场景建设方面，将推动政务服务“数据共享，业务协同”以及促进金融服务“多方互信，降本增效”等。

在培育区块链产业方面，北京将围绕构建区块链一体化产业链体系，打造具有全球影响力的创新型领军企业，为中小型创新企业提供应用场景支持，促进产业链上下游协同发展。

2.浙江省区块链专业标准化技术委员会正式成立

7月5日上午，在由杭州市余杭区政府指导，杭州未来科技城管委会、巴比特主办的“拥抱产业新浪潮——2020杭州区块链国际周”现场，浙江省区块链专业标准化技术委员会（以下简称区块链标技委）揭牌成立。区块链标技委由浙江省经信厅标发起，是浙江省市场监管局领导下的区块链行业的地方标准化组织，同时也是国内首家区块链领域标准化技术委员会。标技委的秘书处设在浙江省数字经济学会，主任由浙江大学计算机学院院长陈刚教授担任，浙江大学、蚂蚁金服、趣链科技、巴比特等机构专家担任委员。据悉，目前区块链标技委正在联合趣链、数秦、泛链以及巴比特推进基于区块链身份认证（DID）的标准化试点项目。

3.河北印发《河北省区块链专项行动计划（2020-2022年）》

河北省委网信办近日印发《河北省区块链专项行动计划（2020-2022年）》。《行动计划》提出，加强区块链技术集成创新发展，推动区块链产业与实体经济融合发展，推进区块链技术广泛运用，构建区块链健康发展生态环境，加强区块链技术应用的监督管理。《行动计划》明确了河北省区块链技术及产业应用发展目标。到2022年末，河北省区块链相关领域领军企业和龙头企业达到20家，培育一批区块链应用产品，力争打造出1-3个全国知名区块链品牌，形成3个具有区域影响力的区块链产业集聚园区，区块链产业竞争力位居国内前列。

4.广州打造全国首个区块链发展先行示范区

日前，广州正式获工信部批复创建区块链发展先行示范区，成为全国首个获批创建区块链发展先行示范区的城市，这标志着广州在发展区块链产业的道路上又迈出了重要的一步。

在发展区块链产业的道路上，广州将区块链作为自主创新突破口，加快“建链、上链、用链”,坚持将区块链产业发展作为服务实体经济应用场景的重要推手，从金融、物流、政务、知识产权、工业互联网等方面，不断增强区块链技术与传统经济各个领域的深度融合，构建经济高质量发展新引擎。

广州把区块链作为核心技术自主创新的重要突破口，力争打造成为国内区块链产业集聚区、创新引领区、应用先行区。努力培育一批具有安全稳定区块链产品的行业重点企业，覆盖产业链各个环节，逐步形成“基础底链+BaaS平台+应用开发+行业应用”区块链全产业链集群发展格局。

广州正在推进形成“一核多区”的发展布局，加快提升自主可控的创新能力，构建自主可控的区块链底层平台。实施重点领域研发计划，围绕区块链产业重点领域组织实施重大科技专项；实施高新技术企业树标提质行动，支持区块链企业壮大为行业标杆企业；支持区块链企业建设工程技术研究中

心、重点实验室、技术中心、院士工作站等研发机构正在不断努力构建开放共享的产业生态。支持有条件的区先行先试，加快区块链和人工智能、大数据、物联网等前沿信息技术的深度融合，在政务、金融、产业以及教育等领域开放一批区块链应用场景，形成一批可复制推广的商业模式，推出一批区块链规则和标准体系。组织开展区块链行业应用场景示范工程，遴选一批区块链成熟应用并推广示范。

5.深圳成立首个区块链标准化测评工作站

深圳区块链行业将加快标准化发展。6月11日，第四届中国区块链开发大赛暨区块链国家标准及系统测试标准广东研讨会在深圳举行，首个可专业进行国家标准申报测试的区块链标准化测评工作站在深圳率先成立。

2016年9月，国际标准化组织（ISO）成立了区块链和分布式记账技术委员会（ISO／TC307），负责制定区块链和分布式记账技术领域的国际标准。2017年3月，中国电子技术标准化研究院承担ISO／TC307国内技术对口单位。2019年12月，工业和信息化部组织筹建全国区块链和分布式记账技术标准化技术委员会，秘书处承担单位为中国电子技术标准化研究院。目前，中国电子技术标准化研究院负责对区块链系统进行是否符合区块链标准的软件测试，测试通过后，颁发相关证书。

中国电子技术标准化研究院区块链研究室主任李鸣介绍，中国电子技术标准化研究院从2017年开始，每年举办1次中国区块链开发大赛，推动中国区块链技术发展。目前，第四届中国区块链开发大赛正处于报名阶段，正式比赛将在7月中旬进行。

当天亮相的区块链标准化测评工作站由深圳电标测试技术有限公司负责组织，面向广东地区的企业，接受区块链系统的测试申报，以及相关技术服务。同时，将积极申报深圳区块链标准测试公共技术平台，为广东乃至全国、全球的区块链产品，提供基于标准的测试技术服务。

六、国际简讯

1.中国专利保护协会：美韩中位居全球区块链授权专利数前三

“中国专利保护协会”7月1日发布《2020年区块链领域全球授权专利报告》。报告显示，截至2020年5月14日，区块链领域在全球范围内共有3924件授权专利，其中获得专利数最多的是美国，占39%，韩国其次，占21%，中国排名第三为19%。

在全球已获得授权的区块链专利排名中，阿里巴巴（含支付宝）以212件区块链授权专利数位列全球第一，接近第二名IBM（136件）和第三名Coinplug（107件）之和。此外，腾讯（含前海微众银行、财付通）排名第九，拥有42件授权专利。

2.Libra将会和CBDC共存，并在国家数字货币间搭建桥梁

美东时间6月24日，在哈佛大学肯尼迪政府学院的贝尔弗中心智库展开了一场由中心主任Aditi Kumar主持的关于数字货币的研讨会。Libra协会副主席和政策交流总监 Dante Disparte 表示，数字货币的出现并不会将传统的金融模式排除，单一稳定币的模式会增加应用场景，但没有放弃多币种质押的Libra设计，而且在积极尝试和IMF、FSB以及其他监管机构积极沟通，并希望更多国际机构加入共同促进跨国结算。

他还指出，Libra会遵守当地国家的资本管制，并致力于服务占世界人口50%以上的那些高通胀法币国家。Libra寻求遵守国际法规，但并不会用于为美国政府执行外交制裁的工具。当说到和央行数字货币的关系，Dante认为Libra将会和CBDC共存，并在国家数字货币间搭建桥梁。

3.世界经济论坛拟利用区块链技术治理政府部门腐败活动

世界经济论坛（WEF）希望利用区块链技术使政府公共部门的腐败活动更加困难。WEF区块链项目负责人Ashley Lannquist表示：“腐败对区块链来说是一个‘高潜力’的空间，因为你真的可以从分权中获益。例如记录很难删除或审查。”WEF正在与哥伦比亚政府合作，以查看基于区块链的透明度是否可以帮助防止腐败。Ashley Lannquist负责的一份报告指出，黑暗交易困扰着许多国家的公共部门，但提高透明度、公共问责制和适当的文件是解决办法。区块链就是一种解决方法。

4.泰国央行将开发CBDC去中心化支付系统原型

泰国中央银行宣布了一项开发商业去中心化支付系统原型的项目，成为最新加入央行数字货币(CBDC)行列的货币监管机构。泰国央行CBDC（央行数字货币）的原型将基于Inthanon项目，这是一个由泰国央行与该国八大商业银行合作发起的分布式账本项目。公告称，该项目的范围将包括进行可行性研究，以及开发一个流程整合CBDC与企业的创新平台。新的原型项目定于下个月开始，预计将持续到今年年底，届时泰国央行将公布该项目的总结和结果。

七、业界声音

1.互联网巨头，一个假想的区块链未来

有关区块链的讨论和探索仍在继续，但是，它的发展方向逐渐明朗却是一件非常肯定的事情。越来越多的区块链玩家经历了早期的狂热追捧之后，开始较为理性地看待区块链并且试图找到真正适合自己的区块链的发展道路。避开发币或者ICO的雷区，当区块链真正回归到一种技术的状态，成为人们的共识。

当区块链被看成是一种前瞻性的布局，以维持互联网巨头本身的市场地位的时候，它的本质其实已经发生了偏移。因为按照我们对于区块链的认识和看法，所谓的区块链技术并不是仅仅只是进行简单的缝缝补补，而是要真正改变业已形成的固定的体系，特别是现在已经形成的一个又一个的互联网中心。

对于互联网巨头们来讲，经历了PC时代和移动互联网时代的发展之后，它们其实已经建构，并且已经形成了名符其实的中心。在电商领域有阿里、京东为代表的电商中心；在社交领域有腾讯为代表的社交中心；在外卖领域有美团为代表的外卖中心……这些中心已经建构了一个相当成熟的生态圈，在每一个中心之外，我们都可以看到一个有机运行的体系。这个庞大的运行体系，其实就是我们所说的中心化。

区块链技术要做的并不是对中心化进行优化，从而来巩固这些中心化平台的市场地位，它要做的是颠覆这些大型的中心，通过激活这些中心化体系内不同个体的力量来建构一个去中心化的运行体系和系统。这需要互联网巨头们有一种自我革新的勇气，才能取得效果。如果仅仅只是区块链看成是一个优化的技术，最终所谓的区块链技术其实早就已经背离了它的本质，从而进入到了一个发展怪圈之中。

从这个角度来看，互联网巨头们对于区块链的看法从一开始其实就已经错了，他们并不愿意放弃自身业已形成的强大的资源优势，而仅仅只是想方设法地来巩固他们业已形成的优势地位。此刻，区块链技术不再是一种颠覆性的存在，而是变成了互联网巨头的附庸。可想而知，这样的区块链技术或许就连它一半的功力都无法发挥出来，仅仅只是变成了互联网巨头们维持自身地位的一种方式和手段。

虽然互联网巨头们有自身的技术、资本、场景等诸多方面的优势，但是，他们对于区块链的定位最终决定了他们并不能够真正成为区块链行业发展的未来，而仅仅只能成为区块链发展道路上的一个过客。可能有人会说，互联网巨头们已经在区块链技术上占据了优势，并且他们开始将这些区块链技

术应用到他们生态体系当中的不同场景当中。从表面上看，互联网巨头在区块链发展当中占据了相当多的优势，并且从当下的发展状态下，互联网巨头是名符其实的排头兵，但是，如果互联网巨头们仅仅只是把区块链定位成为一个优化自身的方式和方法，而不去思考用区块链建构一个新世界，并且在这个新世界当中找到自己的位置，那么，他们现在的所谓的优势必然会被时间所吞噬。

经历了不断的洗牌之后，人们对区块链的未来发展方向有了一个相对明晰的认识，这个方向其实就是要把区块链看成是一个技术，而不是数字货币。虽然在当下的区块链行业当中依然有人会片面地认为区块链技术就是数字货币，甚至有人还在做披着区块链外衣的炒币的买卖，但是，从大的方向上来看，很多的玩家其实是把区块链看成是一种纯粹的技术来看待的，并且开始把区块链的真正意义看成是落地和应用，并且这种落地和应用是带有颠覆性的。

这才是区块链行业的未来和方向。需要明确的是，真正兼顾明晰且正确定义的区块链玩家并不太多，而是非常少的。正是因为这些玩家的稀少，所以，他们才是区块链行业真正未来的发展方向。这些玩家除了我们现在看到的一些专注技术研发的极客型的玩家之外，另外一个值得关注的玩家就是传统类型的玩家。对于传统类型的玩家，很多人一直持偏见，认为传统玩家只有被改造的命运，孰不知，很多传统玩家其实是期望借助区块链来打一个翻身仗的，在这些传统玩家当中，万向区块链其实是最值得我们关注的。

随着这种发展方向的逐渐明确，我们未来还将看到越来越多像万向区块链一样的传统玩家的出现。同互联网巨头们有一定的历史包袱不同，传统企业则是把区块链看成是一个打翻身仗的机会和手段。因此，他们在布局区块链的时候会真正完美诠释区块链的本质和意义，从而真正引领区块链的未来发展方向。

对于区块链技术的突破和创新，并不仅仅只是需要投资才可以实现的。它还涉及到底层技术的传输能力、加密技术的完备性等诸多方面的内涵和意义。此刻的区块链其实已经超脱了区块链技术本身，而涉及到了数据、数字等诸多的技术领域当中。等到比区块链技术还要底层的技术得到了颠覆和创新之后，区块链的创新才能真正被引爆，从而才能把区块链技术带入到一个有颠覆和创新的发展阶段。

当人们开始对区块链认识清楚的时候，我们就会发现互联网巨头绝不是区块链的未来和方向。真正意义上的区块链的未来和方向在于技术，在于改变传统的中心化体系，甚至在于改变现有的区块链运行体系。

（作者：孟永辉，资深撰稿人，专栏作家，特约评论员，行业研究专家。长期专注行业研究，累计发表财经科技文章超400万字。）

2.关于区块链的那些事，看完可以防忽悠

区块链到底有没有用？关于这个问题，大家心中都有各自观点。目前网络上主要有两种，一种是“区块链万能论”，另一种就是“区块链就是鸡肋”。

前者认为万物皆可区块链，他们认为，区块链是万能的，所有的行业都应该布局区块链，只有区块链才是未来的发展方向。即使目前的公链技术，像是比特币和以太坊，吞吐量低依然是发展公链的一刀致命伤，但那又如何？区块链的拥趸者们乐观地相信，公链市值惊人，代币可以成为资本，具有收购金融机构的潜力。况且，区块链尚处于起步阶段，未来的潜力不可限量，取代银行只是时间问题。

与之相反，后者对区块链不屑一顾，他们鼓吹“区块链无用论”。就目前而言，区块链的速度确实太慢了，应用在金融领域实在是多此一举，反而会增加不必要的麻烦。比特币与以太坊自是不必说，每秒的交易量也就几十笔，实在不足以支撑现在的金融环境。较为成熟的金融机构Visa网络，每秒要处理的交易量高达5.6万笔。如果用区块链来取代银行，未免太过天方夜谭了。

显然，这两种观点都太过绝对了。

区块链一定不是万能的，应该说是任何技术都不是万能的。目前的区块链依旧存在交易效率低、安全问题（假名制度）、信任机制转变困难以及去中心化存在矛盾等问题，但是它的去中心化、可追溯可以帮我们甄别信息，从根本上解决信息不对称的问题。是的，它的交易效率不高，却可以取消中间人，使跨境交易由繁入简等。再说的简单的一点，区块链本质上解决的是信任问题，是价值转移问题。

区块链本着公平公正的精神诞生，尽管它在实际落地上还存在着一些问题，但毫无疑问，区块链是有价值的。前央视主持人张泉灵直言：“有些人在区块链里一天挣的钱，超过在互联网时代里十年挣的钱。一帮草莽一开始把这个事情做得各种漏洞，各种泡沫，甚至违反国家法令，但区块链技术本身有颠覆性。”

马云也说，“区块链不是泡沫，但是，今天的比特币是泡沫。比特币只是区块链一个很小的应用。我们并不对区块链技术有着深刻的理解和了解，今天的区块链不是五年以后的区块链，更不是十年以后的区块链，区块链不是一个巨大的金矿。在我认为，至少在阿里巴巴内部，区块链必须是一个解决方案，是解决在进入数据时代的隐私和安全的解决方案。”

区块链就好比早期的移动互联网。曾经，巴菲特说他不会投资任何的互联网公司，现在，巴菲特说我不看好任何数字货币。历史总是惊人的相似，我们曾经认为互联网不过是黄粱一梦，但时间给了我们最好的证明。现在的区块链还在孵化过程中，它有潜力也有能力解决好现在的应用难题。

区块链本质是分布式的公开协议+价值网络，它既避免中心化的单点故障，又降低信息的不确定性以达成大规模协议；既保证了每个个体的自私人性，又维持生态的良性发展。

区块链的四要素可以判断区块链项目的真伪：

一是确认信息真实性的成本高。

区块链是一个公开的账本，用以达成全网共识，因此区块链技术特别适合信息真实性难以确认的领域。而那些本来信息确认就轻而易举的行业，根本用不着区块链技术。很多行业的信息确认非常简单，如果真的非要使用区块链，就像是用屠龙刀割韭菜，未免大材小用的。

什么行业的信息确认成本高？

典型的就是金融。金融市场有大量信息不对称，导致市场充满不确定性。举个最简单的例子，转账，在过去转账你是不知道有没有到账的，所以才有了银行，银行作为第三方跟你说到账了，你才知道到账了。而现在区块链可以更好地解决这个问题。类似的信息确认问题在金融领域还有市场数据、授信、合同等等。

区块链的四要素可以判断区块链项目的真伪：

一是确认信息真实性的成本高。

区块链是一个公开的账本，用以达成全网共识，因此区块链技术特别适合信息真实性难以确认的领域。而那些本来信息确认就轻而易举的行业，根本用不着区块链技术。很多行业的信息确认非常简单，如果真的非要使用区块链，就像是用屠龙刀割韭菜，未免大材小用的。

什么行业的信息确认成本高？

典型的就是金融。金融市场有大量信息不对称，导致市场充满不确定性。举个最简单的例子，转账，在过去转账你是不知道有没有到账的，所以才有了银行，银行作为第三方跟你说到账了，你才知道到账了。而现在区块链可以更好地解决这个问题。类似的信息确认问题在金融领域还有市场数据、授信、合同等等。

八、技术交流

规模化区块链应用实践的必然选择之一：扩容

区块链凭借安全可信、分布式、难篡改等特点被广泛关注，随着区块链技术的快速发展和实践应用，其数据存储代价大、性能低、网络延迟高等问题逐步凸显。因此区块链作为一种可信数据管理机制，亟需解决可扩展和性能问题，包括比特币、以太坊等主要区块链社区、开发团队等纷纷开始区块链扩容方案的研究。

（1）为什么扩容——区块链扩容的需求分析

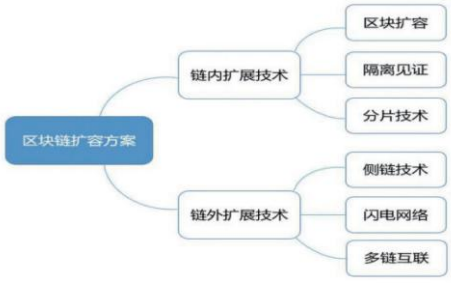
区块链容量问题天然存在，随着节点和交易量增多日益加剧。自中本聪发明比特币以来，比特币节点数量暴涨，链上的交易量剧增。比特币网络中的交易需经矿工打包成区块后广播给其他节点，由于比特币区块大小1M的限制，单个区块只能容纳有限的交易事务，据统计，单个区块实际容纳的交易数约为1700多，区块每隔10分钟打包确认，因此比特币交易速度约为每秒3笔。而市场上常用的支付手段如VISA平均每秒处理5000到8000次交易，支付宝处理交易的峰值可达每秒近10万笔交易。比特币缓慢的交易导致网络中待确认的交易越来越多，造成网络堵塞。

区块链扩容需求广泛存在，各界都在研究区块链扩容方案。比特币区块链网络中用户为加快交易速度，必须增加交易的手续费使矿工优先处理交易。大量的交易手续费和严重的交易延迟限制比特币的发展，这也是整个区块链技术发展面临的问题。以太坊创始人维塔利克·布特林在以太坊说明文件中提到区块链系统在“去中心化”、“可扩展性”和“安全”三方面中只能完美解决两点，即“去中心化”和“安全”。但随着网络规模的扩展，区块链系统必须考虑“可扩展性”问题的解决方案。比特币核心开发团队提出如BIP101、隔离见证等多种扩容方案；比特币新矿池ViaBTC部署Bitcoin Unlimited扩容方案，并得到澳大利亚计算机科学家莱特支持；中科院袁勇团队研究并提出平行扩容方案；康奈尔大学提出比特币扩容方案Bitcoin-NG；金融密码与数据安全国际学术会议上讨论比特币扩容方案；以太坊也提出分片、状态通道、Plasma等扩容方案。

区块链扩容方案实现复杂，是一个复杂的关联性问题。在互联网时代，应用软件都是通过更新迭代的方式升级，来满足用户量日益增多和服务升级的需求。对应用软件来说，软件升级相对容易，系统升级通过更新升级服务器就能达到目的，性能低下通过增加服务器来支撑庞大的交易，但在区块链场景中扩展升级十分复杂。区块链基于分布式的架构，具有众多节点，每个节点都部署服务和存储数据，区块链升级需要每个节点都升级本地系统才能完成整个区块链的升级。区块链升级需修改底层源代码，新旧版本的存在会使得区块链中打包出来的区块存在两个不同版本，各节点和矿池也会选择所支持的版本，进而导致硬分叉为两条链甚至多条链，违背原本去中心化共识的思想。

（2）如何扩容——区块链扩容的技术方案

目前区块链扩容方案主要有包括链内扩展技术和链外扩展技术，也称作第一层扩容技术和第二层扩容技术。



区块链扩容技术方案

A.链内扩展技术

链内扩展技术主要是基于对区块链自身进行改进，主要包括区块扩容和隔离见证。

（a）区块扩容：是一种最直接的扩容方式，即增加区块大小，如将比特币当前区块大小从1MB扩展到2MB，区块大小的扩展可以使每秒交易处理增加。理论上，区块容量越大，交易处理速度就越快，但在实践中，若块容量太大，矿工打包块的速度会变慢，区块在网络传输过程中因网络无法对大文件进行快速传输，又会出现新的问题，因此直接对区块大小进行扩容的方案是有限度的。2017年8月，比特币硬分叉为比特币（BTC）和比特币现金（BCC），BCC实现区块大小从1MB到8MB的扩容。

（b）隔离见证：字面意思就是将见证的内容隔离开来。区块中存储的是交易数据，隔离见证通过缩小交易数据的尺寸，使每个区块可容纳更多的交易来达到扩容的目的。比特币交易是发起者通过签署UTXO（未花费交易输出，类似于支票）并填写接受者地址而建立的，这个过程就是“见证”。为保证交易事务唯一性，比特币对每条交易事务数据进行哈希计算得到交易事务ID。交易事务中的关键数据包括签名、接收方和交易金额，其中签名占据了大量存储空间，而该签名信息的作用是由矿工见证交易数据来源的合法性，普通节点并不验证签名信息，因此签名数据部分就可被隔离存储到其他区域，节省了区块的存储空间，也就实现了隔离见证。2017年5月莱特币通过用户激活软分叉方案，绕过矿工和矿池的支持，完成了隔离见证。

（c）分片技术：是将网络中的节点分成不同碎片，各分片处理不同交易数据，每个片区内部共同处理同一交易事件，网络中可并行处理交易大大提高网络并发量。为了实现节点随机分配和片区验证者分配，需再建立一条单独的区块链（以太坊2.0中称为信标链），负责执行维护整个网络所需的操作。这种方式即为二次方分片，是通过网络双层设计增加交易量。具体地，将以太坊网络上的节点分成100片，分片系统由主链上发布的校验器管理合约（VMC）进行维护，每个片区都是独立存在的，当以太坊中有交易时，只选择其中一个分片处理，如果网络内有M件事务待处理，现在每个节点只需要处理M/100件即可，之后这些打包的子区块的数据组成一个主链上的区块，相当于主链区块容量扩大了100倍。目前以太坊2.0信标链还未正式上线发布。另外EOS采用的DPOS共识机制中只有部分节点参与造块，而且没有挖矿竞争，更注重扩展性，和以太坊的分片技术异曲同工。

B.链外扩展技术

改进区块链本身的链上扩展技术有很多局限性，因此在链外使用技术手段进行扩容的方案逐步出台，链外扩展技术主要包括侧链技术、闪电网络和多链扩展。

（a）侧链技术：是在区块链的主链之外引入侧链，在侧链上完成数据（价值）分流。侧链协议可以实现多个区块链之间的交易和价值转移，侧链是相对于主链而言的，多个可以实现价值转移的区块链之间可以互为侧链。侧链技术实现区块链扩展是采用双向锚定的思想，在主链上冻结一定价值的资

产，由矿工确认冻结的资产在侧链上的对等价值，兑换后用户在侧链上使用对等价值的资产。侧链有两种实现方式，一种是单一托管，即将主链上的资产发送到一个单一托管的机构控制并冻结资产，然后在侧链上激活，这种实现方式是中心化的，存在安全风险；另一种是多重签名，主链上冻结的资产通过多重签名的地址控制，资产交易消息需要经过多方的签名才有效合法，大大提高了安全性。侧链技术可以实现完全不同架构、技术和共识的区块链间交易，是一种解决区块链扩容的较理想方案。

（b）闪电网络：是一个点对点的对等网络，完全去中心化的数字货币微支付系统。闪电网络在区块链外开辟一个基于买卖双方的独立双向支付通道，通道创建初期记录一个原始资金分配方案保存双方的初始资金，交易记录经双方签名更新在资产分配方案中。在链下的支付通道中可以发生一次或多次交易，这些交易在支付通道关闭之前都只在闪电网络的资产分配方案中更新，不会在链上共识，直到交易结束后将最终余额分配结果更新到链上共识。频繁交易记录在链下进行大大减少了主链上交易次数，可以显著提高容量、可扩张性、交易吞吐量，且通过闪电网络通道进行的所有微支付几乎都无法被追踪，保障交易更加匿名安全。但闪电网络是基于智能合约建立的双向支付通道，需要智能合约的支持，对于比特币区块链的实现较为复杂，且在实现闪电网络过程中需要打开和关闭支付通道，频繁操作通道可能会加剧网络拥堵。以太坊使用类似思想并升级惩罚机制的雷电网络作为一种链外扩展技术。

（c）交互的多链架构理念。跨链连接器类似于“中间件”，负责定义各链之间进行交互的数据交换标准规范，多链结构中每条链都是一个单独的体系，链内可以自主共识、记账、查询、校验，链间通过跨链连接器进行跨链交易、价值转换。整个多链架构根据业务功能需求搭建并实现，整个体系可以实现多链业务协同，链间数据隔离，极大提高价值网络并行计算能力，保证良好的可扩展性和可利用性。

（3）小结

发挥区块链在技术创新和产业发展方面的作用，扩容问题就成为区块链新型基础设施、助力产业实践必须重视的关键问题。在此背景下，产业各方推动区块链技术发展，商业规模化应用落地，区块链扩容问题解决方案呈现遍地开花的局面。

各方案优劣势分析。对比分析各扩容方案，区块扩容和隔离见证方案局限性较大，会造成硬分叉和中心化问题，影响到整个区块链网络的平衡。侧链技术可以很好地帮主链做分流，但侧链作为一条独立运行的链，没有足够算力保证交易和区块链的安全，攻击者可以使用较小的代价对侧链展开51%攻击。闪电网络主要采用通道技术，因建立支付通道需要先投入一部分资金，适合于可支配的资金较富余且交易频繁的节点，因此支付通道交易也一般是矿池，矿池持续性链下交易会导致“中心化”问题，且支付通道交易的匿名性违背区块链“交易可追踪”的理念。

扩容方案发展趋势。目前分片技术和多链互联是研究的热点方向，但在实际应用中，单纯地使用某一种技术方案是不够的。目前，国内各大区块链平台系统主要采用链下扩容技术，并将多种方案融合在系统中使用，如采用侧链等跨链技术、升级优化国内共识算法、提高硬件性能等多种手段共同提升区块链底层平台性能。分片技术也是多数区块链平台未来的重点发展方向，该技术在逻辑上简单但技术实现难度大，如何合理的计算分片规模、分片数量得到区块链网络分片最优解还需各方研究。

根据应用平衡选择扩容。区块链作为分布式系统，占有硬件和服务资源量较大，盲目扩展会付出巨大的资源代价。从应用场景的角度来看，实际应用场景中应根据业务需求对区块链性能进行必要的扩展，做好服务器资源和链上的效益平衡。且从区块链系统 “去中心化、安全性、可扩展”三大特性来看，也需根据实际应用平衡三者关系。如在规模化数字支付场景对性能要求较高，但在一些企业联盟链低频次大额交易中，性能并非首要问题，应更加注重安全性。

（来源：中国信息通信研究院，作者：李雨蓉）

九、术语解析

确定性

“确定性”是区块链交易的一种特性，可定义为交易被打包进区块之后的一种状态，即，如果我们看到某个区块之后挖出了足够多的区块，就可以确信这个区块内的交易不会被网络拒绝。也就是说，这个交易及其结果（对代币余额的更改）会永远留存下来。工作量证明区块链的确定性不是非此即彼的：交易不会在某个时刻得到最终确定，交易被拒绝的概率会随着时间流逝呈指数级下降，因为网络会就最长链达成共识。区块链在任何时刻都有可能出现分叉，导致某个交易失败，但是只要看到有新的区块出现并指向包括这个交易在内的区块，这种可能性就越来越低。不包含我们的交易的分叉链越长，我们的交易被拒绝的可能性就会越高。也有可能出现这样的情况：我们的交易可能都无法实现确定性，而是变成了 “反确定性” 的，也就是说我们可以确信这个交易已经被拒绝了。当网络遭到所谓的 51% 攻击时，就会出现这种情况。我们永远无法确定最后会是哪种结果：但是随着时间的流逝，我们对交易被拒绝的可能性的预测会无限趋近 0 或 1 。只要等待足够长的时间，我们就能从实际意义上得出确定的结论。

DeFi

DeFi是去中心化金融（Decentralize Finance）一词的缩写， 是“去中心化”和“金融”的巧妙组合，描述了建立在区块链上的金融服务。去中心化系统是一个需要多方独立决策的系统，在这样一个去中心化系统中，没有中央集权机构作为代表进行决策。

金融的本质可以浓缩成为：效用跟风险在时空中的交换。理论上，去中心化金融提供的所有服务和产品都与传统金融世界相同。在传统的金融系统中，金融服务包括融资投资、储蓄、信贷、结算、证券买卖、商业保险和金融信息咨询等业务，都是由中心化的金融机构为用户提供的。然而，DeFi使用分布式账本技术，包括区块链、加密货币、智能合约，来提供贷款、融资、稳定币和信贷安排等服务。

侧链

侧链协议本质上是一种跨区块链解决方案，一种合并机制，允许将诸如令牌之类的数字资产安全地从一个区块链转移到另一个区块链，然后再转移回去。通过该解决方案，可以实现双向锚定，并且可以在主链和侧链之间安全地转移数字资产。侧链的概念是相对于主链而言的。只要区块链符合“侧链协议”，例如以太坊和莱特币就可以成为侧链。对于区块链，主链和侧链就像道路上的主干道和支路，主链就是主干道 ，侧链是分支路。因为主链上的吞吐量链非常大，所以内存运行速度较慢，甚至服务器都崩溃了。为了减轻这种现象的发生，已经开发了侧链，它不会影响主链的运行并减轻服务器压力。

侧链作为跨链技术实施有三个作用。首先，从应用程序扩展方面，通过侧链技术，可以在主链的基础上提供一些新功能，例如智能合约和隐私保护。它会影响主链的性能/延迟/ TPS。例如，比特币可以通过侧链转移主链上的某些交易。在小范围内达成共识的同时，它可以加快交易速度，降低成本并提高交易效率。其次，从安全性角度看，侧链和主链是相互独立和相互依存的。如果侧链上有大量资金被盗或出现代码漏洞，则主链的安全性和稳定性将不受此影响。即使同时运行多个侧链，也不会引起主链运行效果和安全性。就像分支道路上的车祸一样，主干道不会受到影响。最后，就实现智能合约，隐私等功能而言，在大多数情况下，用户可以通过将令牌持有在主链上来进一步扩展区块，从而体验到由侧链提供的不同服务。技术的基础是基础。如果要将比特币主链移动到侧链，则可以使用侧链上的各种功能来达到原始目的。

江苏省互联网协会

江苏可信区块链

搭建政府、企业、网民沟通的桥梁

提供政府决策

促进行业发展

服务企业需要

普及网民知识