

区块链技术调研报告之一： 具有颠覆所有行业的可能性

——区块链技术解析和应用场景畅想

穆启国 执业证书编号：S1100513040001
研究员 8621-68416988-208
muqigu@cczq.com

陆婕
联系人 8621-68416988
lujie@cczq.com

核心观点

- ❖ 区块链技术源自于比特币，通过对比特币运行体系的深入剖析，我们可以直观地了解区块链技术的原理。它的本质是运用计算机算法和密码学等技术创造一种去中心化的数字货币系统，实现货币的发行和交易功能。
- ❖ 区块链技术是一种互联网底层的分布式数据库技术，它的出现有望实现从信息互联网向价值互联网的转变。其特点包括去中心化、点对点传输、透明、可追踪、不可篡改、数据安全及信用的自我建立等。
- ❖ 区块链的应用不限于数字货币，众多特点决定了其广阔的应用空间，涉及到人类社会活动的方方面面，包括跨境支付、电子商务、投票、公证、知识产权保护、证券发行交易、众筹、契约、担保等，解决中心化带来的各种弊端。
- ❖ 海外市场广泛看好区块链技术的前景，金融机构、技术公司、政府部门纷纷加入区块链技术的研究的开发，积极应对即将到来的互联网技术变革。

川财证券研究所

成都
高新区交子大道177号中海国际
中心B座17楼，610041
总机：(028) 86583000
传真：(028) 86583002

目 录

通过比特币了解区块链技术的原理.....	4
比特币的历史	4
比特币的生成	4
比特币的交易和记录	5
双重支付的解决方案：时间戳.....	6
共识机制的解决方案：工作量证明.....	6
确保交易不可逆的解决方案：哈希算法	7
比特币的缺陷	7
区块链是一种互联网底层的分布式数据库技术	8
区块链是什么	8
区块链之关键词：比特币	9
区块链之关键词：底层.....	10
区块链之关键词：去中心化.....	10
区块链之关键词：信用的建立.....	11
区块链的发展的三个方向	11
区块链的应用场景丰富.....	13
区块链应用场景举例	13
海外区块链技术与投资广受追捧.....	15
全球性技术公司、咨询公司和金融公司积极寻求合作，探索区块链技术的应用场景	15
不同于比特币当年的境遇，区块链技术的开发得到各国政府部门的支持和鼓励 .	16
国外监管机构密切关注区块链技术的发展，为监管框架调整做好准备	17

图表目录

图表 1: 比特币交易示意图.....	5
图表 2: 时间戳示意图.....	6
图表 3: 工作量证明示意图.....	6
图表 4: 哈希算法示意图.....	7
图表 5: 区块链如何工作.....	8
图表 6: TCP/IP 协议族.....	10
图表 7: 定义技术时代.....	12
图表 8: 区块链的应用场景.....	13

通过比特币了解区块链技术的原理

比特币的历史

2008 年金融危机爆发之后不久的 11 月 1 日，中本聪在一个隐秘的密码学讨论组上发表了一篇论文《比特币：一种点对点的电子现金系统》(Bitcoin: A Peer-to-Peer Electronic Cash System)，阐述了基于 P2P 技术和加密技术等技术的电子现金系统的构架理念，即比特币系统的基本框架。2009 年 1 月 3 日第一个序号为 0 的比特币的区块——创世区块诞生。几天后的 1 月 9 日出现序号为 1 的区块，并与序号为 0 的创世区块相连接形成了链，标志着比特币区块链诞生。

简单来说，比特币是一种 P2P 形式的电子货币，它不需要特定的机构（中央银行）来发行，而是由计算机程序（算法）生成，并且这种电子货币可以在网络中进行点对点的支付，即从发行到流通，比特币都是去中心化的运作模式，这与法定货币有本质上的区别。

比特币已经运行了 6 年多的时间，虽然遭到多无数次的黑客攻击，但整个系统的运行从未停止过，市值已超过 100 亿美元。

比特币的生成

每一个网络中的节点都可以生成比特币，购买一台电脑，连接到互联网，安装一个软件，就可以加入到比特币的生成、交易和支付的活动中来。比特币的产生需要依据特定的算法，通过大量复杂的运算才能生成，俗称“挖矿”。所谓“挖矿”就是竞争网络中比特币交易的记账权，竞争的方式是用计算机解决一项复杂的数学问题，来保证比特币网络分布式记账系统的一致性。网络中算得最快最好的节点就能获得记账权，同时系统自动生成相应的比特币作为奖励。“挖矿”需下载专用的比特币运算工具，注册任意一个比特币合作网站，将注册的用户名和密码填入计算程序中，点击开始运算即可。

在设计比特币体系的时候，中本聪借用了金本位的思路，过去黄金可以成为流通货币的一个主要原因是稀缺性，即货币的总量是相对稳定或者说增长缓慢的，这就能从某种程度上避免通货膨胀的发生。比特币的生成在设计之初也考虑到了这个问

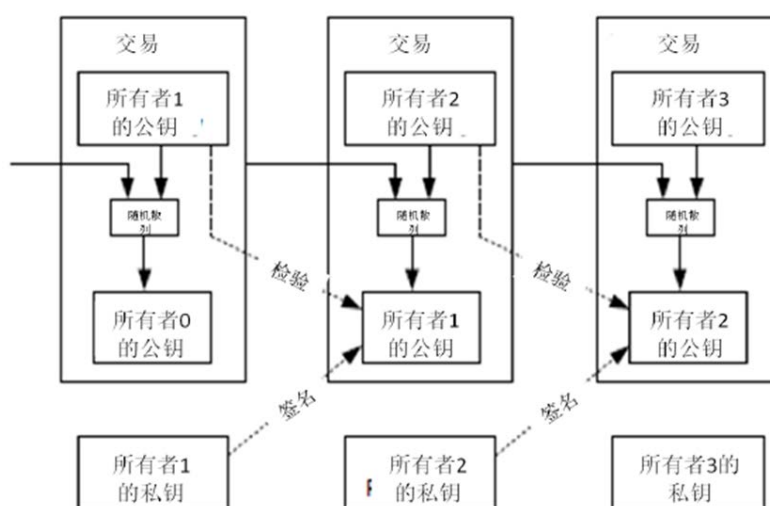
题，通过算法的设定，控制了比特币的生成速度，随着比特币总量的增加，新比特币生成的速度会减缓，并且设定了比特币的总量上限 2100 万个。在比特币诞生之初的 2009 年，每次挖矿的奖励是 50 个比特币，以每 10 分钟 50 个的速度增加，当总量达到 1050 万时，即上限 2100 万的一半时，奖励减半为 25 个，当总量达到 1575 万时，即新增量达到 1050 的一半时，奖励再减半为 12.5 个，以此类推，到 2140 年，比特币将达到 2100 万个的总量上限。

比特币的交易和记录

比特币使用整个 P2P 网络中众多节点构成的分布式数据库来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节安全性。在注册比特币合作网站时候将获得一个公钥，即比特币地址，只需将地址告诉别人，别人就可以通过比特币系统向你付款。同时，你会获得一个私钥，只有私钥才能打开电子钱包。如果将私钥丢失，你将无法找回你的比特币。

比特币在交易时的表现形式是一串字符，或者叫数字签名，这串字符包含了上一次交易的信息和下一个所有者的公钥信息，这个字符将被发送给收款方（下一个所有者），收款方会对这串字符进行验证，并向全网络广播。被全网络认可的交易信息将被确认形成区块，收款方可通过自己的私钥接受比特币汇款。

图表 1： 比特币交易示意图

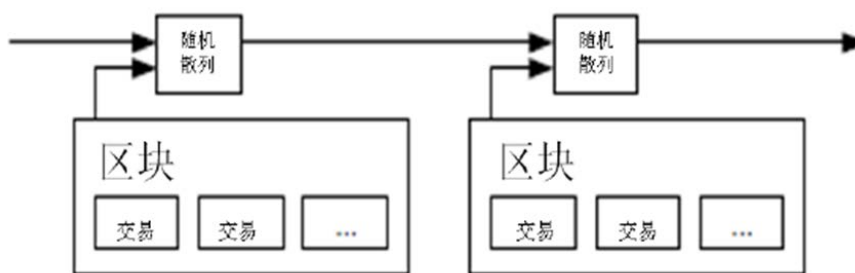


资料来源：中本聪《比特币白皮书》、川财证券研究所

双重支付的解决方案：时间戳

虽然数字签名可以解决付款方信息的真实性，但现有的支付系统还是需要一个第三方机构来确认交易的唯一性，避免同一笔资金支付给多个收款人。比特币区块链上的每一个区块都会被盖上时间戳，该时间戳能够证实特定数据必然于某特定时间是确实存在的，因为只有在该时刻存在了才能获取相应的随机散列值。每个时间戳应当将前一个时间戳纳入其随机散列值中，每一个随后的时间戳都对之前的一个时间戳进行增强，这样就形成了一个链条。

图表 2： 时间戳示意图

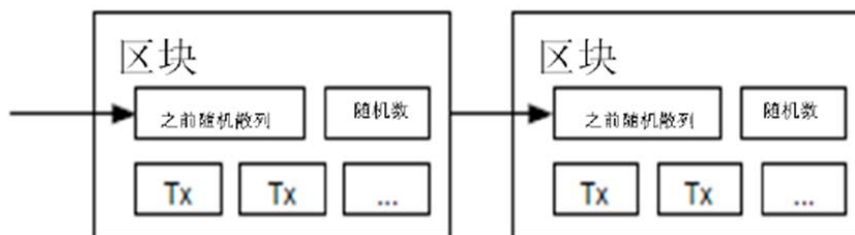


资料来源：中本聪《比特币白皮书》、川财证券研究所

共识机制的解决方案：工作量证明

交易的记账权或者说是区块的建设权需要竞争才能获得，即通过挖矿来计算一个复杂的数学问题，即找到下图中的随机数。通过提高寻找这个随机数的难度，可增加所需的计算量，这种计算量就构建了一个工作量的证明机制。之后的哈希算法部分将做具体的解释。如果想要修改某个区块内的交易信息，就必须完成该区块及其后续连接区块的所有工作量，这种机制大幅提高了篡改信息的难度。同时，工作量证明也解决了全网共识问题，全网认可最长的链，因为最长的链包含了最大的工作量。

图表 3： 工作量证明示意图

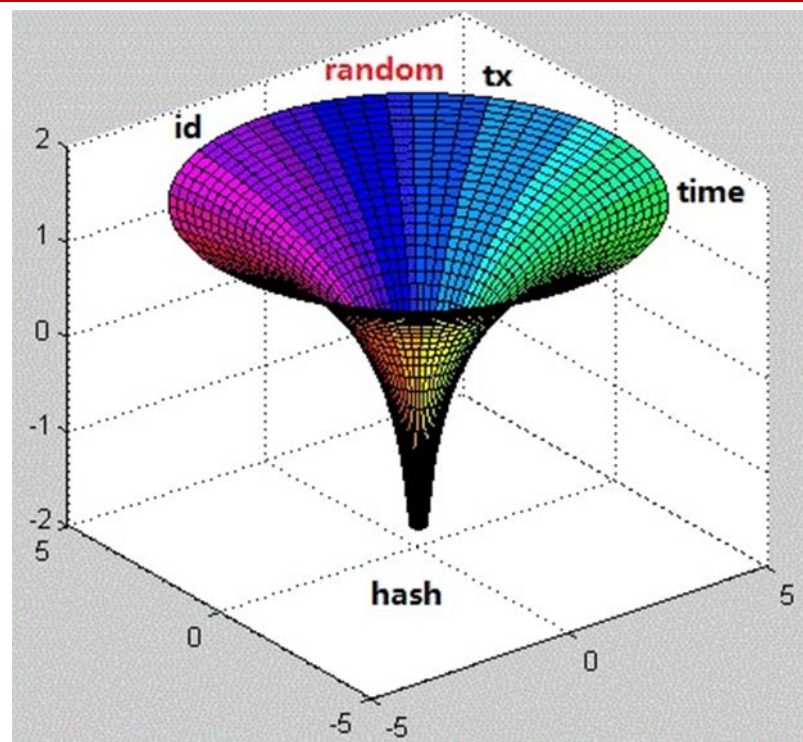


资料来源：中本聪《比特币白皮书》、川财证券研究所

确保交易不可逆的解决方案：哈希算法

上文中提到的随机散列值就是哈希值，它是区块链的重要构成部分。每一个区块中都包含了区块号（id）、交易信息（tx）、时间戳（time）和随机数（random）的信息，这些数据通过一个算法的压缩处理，就生成了一个哈希值，这种算法就是哈希算法，哈希算法的具体算法有多种，比特币采用的是 SH256 算法。只要区块中的信息发生细微的变化，哈希值就会完全变化，而从哈希值本身是无法还原出原有信息的，即整个压缩过程是不可逆的。挖矿从另一个角度来说就是数据的打包压缩，矿工通过改变随机数来生成不同的哈希值，挖矿的难度就是要通过调正随机数找到符合要求的哈希值。目前比特币对哈希值的要求是前 17 位都是零，概率之低可想而知。通过全网算力的协作，计算速度被控制在每 10 分钟找到一次。随着全网算力的不断提高，哈希值的难度也会跟着提高，即零的个数要求进一步增加，维持 10 分钟找到一次的频率。

图表 4： 哈希算法示意图



资料来源：鸣金网、川财证券研究所

比特币的缺陷

数量的限制或引发通货紧缩。根据比特币的设计原理，在比特币后期的总量增长会

非常缓慢。事实上，87.5%的比特币都将在最初的12年内被“挖”出来。长期看来，比特币的发行机制决定了它的货币总量增长速度将远低于社会财富的增长速度。这就将导致货币比特币升值，物价下跌，持续的物价下跌使人们倾向于延迟消费，需求萎缩，商品滞销，进一步降低商品价格，进入通货紧缩的恶性循环。

挖矿导致能源浪费。我们已经了解到挖矿其实就是运行计算机程序来解数学问题。矿工为了获得比特币奖励就必须竞争到合法的记账权，最终只有一个矿工能获得唯一的记账权，建立一个交易区块，而其他矿工的计算机算力其实都被浪费了，计算机运算的背后是对电力资源的消耗。事实上，现在中国大约拥有比特币全网60%的算力，而其中许多挖矿机都安置在云贵川地区的小水电站附近。

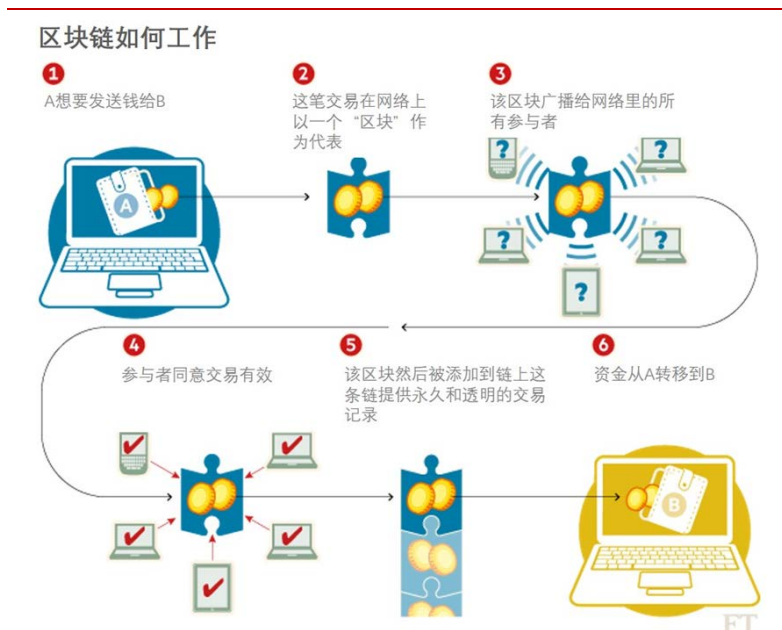
区块链是一种互联网底层的分布式数据库技术

区块链是什么

“区块链（Blockchain）是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。该技术方案让参与系统中的任意多个节点，把一段时间系统内全部信息交流的数据，通过密码学算法计算和记录到一个数据块（block），并且生成该数据块的指纹用于链接（chain）下个数据块和校验，系统所有参与节点来共同认定记录是否为真。”——区块链新经济

区块链技术的开发和应用有望实现从信息互联网向价值互联网的转变。区块链通过构建P2P自组织网络、时间有序、不可篡改的加密账本、分布式共识机制，从而实现去中心化信任。全网记账，共同公证，创造基于计算机算法而不依赖第三方的信任机制，实现价值的点对点传输。由于区块链系统建立在了大量计算机运算之上，具有非常强的冗余性，因而有很强的容错的功能，并且它能够在没有中心化服务器和管理的情况下，安全稳定地传输数据。

图表 5: 区块链如何工作



资料来源：金融时报、川财证券研究所

区块链之关键词：比特币

区块链与比特币同时诞生于 2008 年，比特币是截止到目前，区块链技术最成功的一个应用案例。截至目前 6 年多的存续时间也佐证了区块链技术的可靠性。

区块链是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了过去十分钟内所有比特币网络交易的信息，用于验证其信息的真实性并生成下一个区块。该概念在中本聪的白皮书中提出，中本聪持有第一个区块，即“创世区块”。

整个区块链就是比特币的公共账本，网络中的每一个节点都有比特币交易信息的备份。当发起一个比特币交易时，信息被广播到网络中，通过算力的比拼而获得合法记账权的矿工将交易信息记录成一个新的区块连接到区块链中，每一个区块都包含了上一个区块的部分信息。

一旦被记录，信息就不能被随意篡改，只有当算力达到全网络总和的 51% 时才能修改已经被记录的信息，这样做的成本是巨大的，实现的可能性极低。

区块链曾经在大众眼里和比特币是直接划等号的，但近些年来，人们开始意识到区

区块链的技术不仅可以用来支持比特币系统的运转，还有其他更广阔的应用空间。

区块链之关键词：底层

可以将区块链技术理解为一种互联网协议，即在网络中传递和管理信息的一些格式和规则。正如人与人之间的语言交流，因为我们学习了相同的词汇和语法，这才使交流沟通成为可能。在互联网的世界里同样需要这样的规范，在这种规范之下的信息才能在互联网中自由传递，信息接收方才能确保收到正确的信息内容。

目前的互联网协议中最基础的协议就是 TCP/IP 协议，又名网络通讯协议，是国际互联网络的基础，由网络层的 IP 协议和传输层的 TCP 协议组成。TCP/IP 定义了电子设备如何连入因特网，以及数据如何在它们之间传输的标准。互联网上的每个节点都执行这个协议，赋予信息相同的格式，使信息能自由地在互联网上点对点的传输。基础协议好比是互联网的地基，而应用程序是盖在上面的房子。区块链同样也是一种互联网的“地基”，比特币是盖在这种地基上最早最大的房子，但是还有其他类型的房子可以建造。

看似简单的理念，构筑了互联网的世界的基石，使信息全球化变成了现实。

图表 6: TCP/IP 协议族

层级	协议
应用层	FTP、TELNET、DNS、SMTP、NFS、HTTP
传输层	TCP、UDP
网络层	IP、ICMP、ARP、RARP
网络接口层	Ethernet 802.3、Token Ring 802.5、X.25、Frame relay、HDLC、PPP ATM

资料来源：川财证券研究所

区块链之关键词：去中心化

区块链的核心思想是去中心化。数据的传输不再依赖某个中心节点，而是 P2P 的直接传输。全网络的每个节点都依据共识开源协议，自由安全地传输数据。所有交易记录是对全网络公开的，每个节点都可备份。

网络去中心化的一个著名案例就是 BT 下载，其基础就是 P2P 多点共享协议。以往数据存储中央服务器上，需要下载资源的人越多，服务器承载的压力就越大，下载速度缓慢。而 BT 下载使一个文件在下载的同时，也不断将数据传输给别人，每个节点不仅是下载者，同时也是服务器，使资源的分享不再依赖于中央服务器，在这种去中心化的网络中，下载的节点越多，下载的数据越快。

区块链之关键词：信用的建立

区块链最大的颠覆性在于信用的建立。在我们日常的社会活动中，信任的产品往往需要依靠第三方机构的证明，这种方式通常会增加交易的成本，降低效率，滋生腐败，造就官僚机构。区块链系统本身能产生信用，这种信用的产品不是来自第三方，而是来自程序（算法），因为区块链记录信息的产生是需要全网络节点确认的，一旦生成将永久记录，无法篡改。除非能拥有全网络总算力的 51% 才有可能修改最新的生成的一个区块记录。

区块链技术本质是去中心化、分布式结构的数据存储、传输和证明的方法，用数据区块取代了目前互联网对中心服务器的依赖，使所有数据信息都被记录在一个云系统之上，理论上实现了数据传输中的数据自我证明，深远来说，这超越了传统和常规意义上需要依赖第三方的信息验证模式，降低了全球信用的建立成本。

TCP/IP 协议使信息可以在互联网上自由传递，而区块链技术将实现信息的自由公证。

区块链发展的三个方向

2015 年是区块链技术被讨论得特别热烈的一年，形成了区块链 1.0、区块链 2.0 和区块链 3.0 的概念。区块链 1.0 就是以比特币为代表的虚拟货币，虽然问题重重，包括价格的剧烈波动、数量上限可能导致的通货紧缩、挖矿对能源的浪费、各国政府监管的限制等等，但其仍然是区块链技术最成功的应用，并为人们勾勒了一幅理想的远景——全球货币的统一。货币的发行不再依赖于各国的央行。这个 1.0 起点很高，但路途可能是最遥远的，因为要连起这样一个全球的区块链网络，需要所有个人和机构的共同参与才能达成。

区块链 2.0 可以被理解为区块链技术在其他金融领域的运用。包括目前华尔街银行

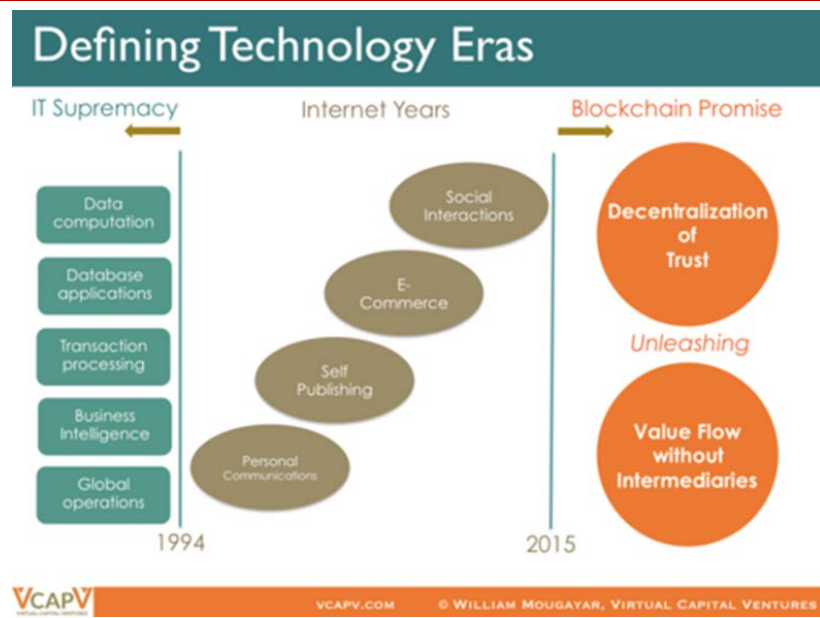
联合想要打造的区块链行业标准，提高银行结算支付的效率，降低跨境支付的成本；交易所积极尝试用区块链技术实现股权登记、转让等功能。

区块链 3.0 将区块链应用的领域扩展到的金融行业之外，覆盖人类社会生活的方方面面，在各类社会活动中实现信息的自证明，不再依靠某个第三人或机构获得信任或建立信用，实现信息的共享，包括在司法、医疗、物流等各个领域，区块链技术可以解决信任问题，提高整个系统的运转效率。

这三个版本不会是依次实现的过程，而是共同发展，相互促进的过程。正如之前提到的，区块链 1.0 的目标很宏伟，但是实现的前路很难长，后来人们意识到，不如在其他领域小范围尝试该技术的运用来解决实际的问题。

在 1994 年之前，信息技术的运用体现在数据计算、数据库应用、商业智能和全球运营。之后我们进入了互联网时代，互联网技术拓宽了人际交流的渠道、提供了自我展示的平台，发展了电子商务，增进了社群互动。2015 年之后，区块链技术为我们展开了新的愿景：去中心化的信任和去中介的价值传递。

图表 7： 定义技术时代

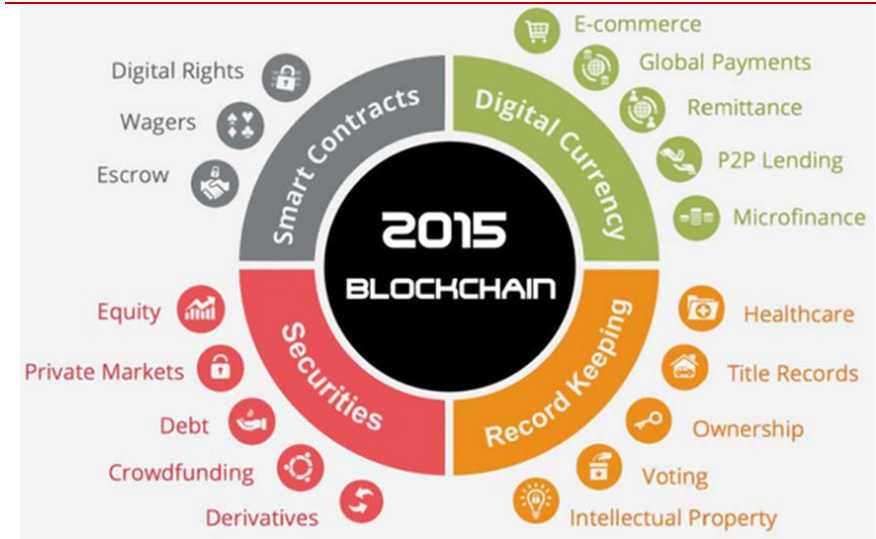


资料来源：VCAPV、川财证券研究所

区块链的应用场景丰富

区块链的应用场景大致可分为数字货币、记录保存、智能合约和证券。具体包括跨境支付、电子商务、投票、公证、知识产权保护、证券发行交易、众筹、契约、担保等各类社会事务。

图表 8： 区块链的应用场景



资料来源：coindesk、川财证券研究所

区块链的应用必须建立在大量群体参与并共享的基础上才能体现价值，封闭的系统并不能发挥区块链技术的优势，只有开放互通才能体现区块链的价值。

区块链应用场景举例

Bitmessage

区块链在通讯领域的早期应用。传统通讯工具的设计思路是如何最快地把信息传递给对方，所以程序会在所有网络节点中选择最短最快的路径进行传输，把信息复制过去。通过 Bitmessage 发送邮件的时候，不再像以往这样将信息传输给特定的节点，而是将信息发送给网络中所有节点。虽然每个节点都收到了信息，但是只有唯一一个有私钥的节点才能打开信息。这样做的好处是不但可以确保对方可以收到信息，还能提高信息传输的安全性，使信息的传输路径无法被跟踪。

Namecoin

基于区块链技术的域名管理系统。域名是互联网的基础资源，目前由一个美国的名为 ICANN 的机构进行管理协调，非常中心化的结构。Namecoin 通过区块链技术，将域名管理系统变成一个分布式的结构，系统中每个节点都可以对域名进行解析，而不再需要通过的中心化管理，在这种情况下，任何一个节点部分的损失，不会对整个域名系统造成有任何问题。

Ascribe

艺术家用于发布作品的网站，将艺术品数字化，通过区块链技术来声明所有权，发行作品。同时可在该网站进行交易，无需通过第三方，卖家和买家直接在基于区块链技术的网站上进行交易，确保交易作品和交易过程的真实性。

Edgelogic

将贵重的钻石登记在基于区块链技术的公共账目记录本上，一旦被全网络验证并记录之后就无法修改，可追溯钻石交易的历史，确保钻石的真实性及合法性。增加钻石盗贼出售赃物和进行保险欺诈的难度。

Ripple

降低跨境支付的成本，提高跨境支付的效率。在区块链上转移电子货币，进行跨境支付，大大缩减到账时间。目前的结算系统十分复杂，资金需要通过银行、中央银行和国际组织多个清算系统的转移才能到账，而区块链做到了点对点即时支付。

Factom

将区块链用于数据保管，确保数据的完整性和一致性，提供公证服务。可应用的数据包括审计账簿和医疗记录等，促进整个社会公共事务的数据透明化。已经开始实施的项目包括洪都拉斯的房产登记等。

ChromaWay

用区块链上的虚拟货币标记资产，包括证券、黄金和房产。这也意味着可以在区块链上发行和交易证券。目前，这些资产的交易需要大量的公正、登记工作，而区块链技术的运用可减轻这部分的工作量。

Blockstream

实现不同虚拟货币之间的兑换。由于都是建立在区块链技术之上的电子货币，比特币和其他币可以实现相互兑换，使用户能自由选择需要使用的虚拟货币。

TIERION

将区块链技术应用到医疗领域，主要是病例资料和基因图谱的保存。已有项目计划包括与飞利浦医疗合作，内容包括病例资料的认证和隐私保护。

Deloitte's Perma Rec

德勤利用区块链技术开发的全球性分布式账本，通过与各种财务报告系统的对接，提高购销过程的透明度。该项目的最终目标是实现审计数据的全覆盖与自动化的税务合规申报，使用户和监管部门同时收益。

海外区块链技术与投资广受追捧

全球性技术公司、咨询公司和金融公司积极寻求合作，探索区块链技术的应用场景

IBM 的 Linux 基金会推出了“开放账本项目”(Open Ledger Project)，通过开源，实现区块链的巨大潜力。埃森哲，澳新银行，思科，第一信贷，德意志交易所，DAH 数字资产控股，DTCC，富士通，IC3，英特尔，摩根大通，伦敦证券交易所集团，三菱 UFJ 金融集团，R3，State Street，SWIFT，VMware 和富国银行加入了该计划。

微软公司的 Azure 区块链服务项目(MSFT)，与多家区块链初创公司合作，为用户、合伙人和开发者提供技术和服 务支持，推进区块链技术的应用场景落地，其成员包括 ConsenSys、Ripple、Eris，CoinPrism 和 Factom 等。

管理咨询公司埃森哲的金融创新实验室也加入了区块链初创公司，包括在香港的汇款初创企业 Bitspark 和能够使用区块链机制，通过众筹的方式来发行证券的 Crowdaura。

德勤在 2 年前就投入了关于区块链技术的研究，集合力来自 12 个国家 100 多名研究人员组建了区块链研发 Rubix 平台，与多家银行合作开发了多个应用案例，同时帮助非金融行业企业策划了近 30 个应用模型。四大中的安永和 PWC 也各自展开了相关研究。

Visa 联合 Coinbase 推出了首张在美国可以使用的比特币借记卡。在 2015 年 11 月 30 日的伦敦 UnBound 大会上，Visa 欧洲创新实验室展示了一款“概念证明”（proof-of-concept）汇款应用，通过这款应用，人们可以在比特币区块链上汇款。

不同于比特币当年的境遇，区块链技术的开发得到各国政府部门的支持和鼓励

英国是全球最热衷于金融科技的国家，希望能占区块链技术发展的先机重夺回国际金融中心的地位。英国央行已组建了区块链技术团队，并考虑发行电子货币的可能性。英国政府对科技金融企业大力扶持，尤其是区块链初创企业，给予前所未有的优惠政策，并向全球招募区块链技术人才。区块链投资公司 Coinsilium 在伦敦 ISDX 交易所 IPO，成为世界上第一家成功上市的区块链技术公司。Coinsilium 是一家专注于投资区块链初创企业的投资公司，成立于 2014 年初，已经投资了 11 家区块链互联网金融相关公司，市值达到了 698 万英镑。

美国的硅谷和华尔街，技术和金融大佬们也大幅增加对于金融科技的的投资力度，积极投身区块链技术研究。创投公司 R3 联合包括高盛、摩根大通、汇丰银行在内的 42 家银行机构进行区块链研究，致力于建立金融服务领域的区块链行业标准。IBM 正在将区块链技术应用于物联网。2015 年 12 月 30 日，NASDAQ 的私人股权投资系统的 Linq 平台上完成里第一笔股票发行记录。区块链初创公司 Gem 宣布完成 710 万美元的 A 轮融资，Gem 和以太坊都是为开发者提供开放环境和服务的公司，目前 Gem 已为比特币开发者提供了多签名的 API 服务，今后还将继续扩展成一个可以跨行业的模块化平台。

日本最大的互联网和电信公司软银（Softbank）联合 Topcoder，针对创业者和初创公司，共同举办了一次关于去中心化区块链的开发竞赛，本次竞赛将会持续三个月，从 2016 年的 1 月 6 日开始到 3 月 31 日结束，软银希望通过这次竞赛，找到一个基于区块链技术、去中心化、透明的互联网筹款平台基本原型。

新加坡资讯通讯发展局（Infocomm Development Authority of Singapore）联合新加坡星展银行和渣打银行共同开发首个发票金融的区块链应用，目前还在概念证明阶段，该概念设备将会被用于让发票金融贸易变得更加安全和简单，包括对企业和放贷银行。新加坡政府正在努力将自己打造成“智能国家”。

韩国的新韩银行参与了区块链初创企业 Streami 的 200 万美元投资，该银行在这次投资中一共投资了 5 亿韩元（大约 42.7 万美元）。Streami 的支持者还包括新韩数据系统（Shinhan Data Systems），是新韩银行旗下的 IT 公司；ICB，一家和亚洲电子商务巨头阿里巴巴合作的韩国支付公司；以及由一群天使投资者组成的风投公司 Bluepoint Partners。该公司的主要业务是亚洲地区的汇款业务，包括韩国、中国、菲律宾，香港，印尼，新加坡，泰国等市场。

国外监管机构密切关注区块链技术的发展，为监管框架调整做好准备

在 2015 年 12 月 16 日，欧洲证券及市场管理局（ESMA, European Securities and Markets Authority）在巴黎举办的一个金融创新研讨会上，区块链和分布式账本被作为议题进行了讨论。作为欧盟在金融危机成立的三大监管机构之一，ESMA 对新技术具有较高的敏感性，在考虑金融监管框架结构的变化时必须对区块链技术有充分的了解。

美国商品期货交易委员会（CFTC, Commodity Futures Trading Commission）宣布，将会在 2016 年 1 月 26 日，在其技术咨询委员会（TAC, Technology Advisory Committee）的会议期间讨论区块链技术在衍生品市场的应用。CFTC 是美国政府的一个独立机构，负责监管商品期货、期权和金融期货、期权市场。CFTC 几个月前曾经表示计划将会把比特币和其他数字货币作为商品进行监管。

无论是金融机构、企业还是监管部门，积极应对才是上策。

风险提示

风险一 区块链技术升级速度不及预期

风险二 金融监管的风险

分析师承诺

本人具有中国证券业协会授予的证券投资咨询执业资格并注册为证券分析师，以勤勉尽责的职业态度、专业审慎的研究方法，使用合法合规的信息，独立、客观地出具本报告，并对本报告的内容和观点负责。本人薪酬的任何部分过去不曾与、现在不与、未来也不会与本报告中的具体推荐意见或观点直接或间接相关。

投资评级说明

证券投资评级：

以研究员预测的报告发布之日起 6 个月内证券的绝对收益为分类标准。

买入：20%以上；

增持：5%-20%；

中性：-5%-5%；

减持：-5%以下。

行业投资评级：

以研究员预测的报告发布之日起 6 个月内行业相对市场基准指数的收益为分类标准。

超配：高于 5%；

标配：介于-5%到 5%；

低配：低于-5%。

免责声明

本报告由川财证券有限责任公司（已具备中国证监会批复的证券投资咨询业务资格）制作。本报告仅供川财证券有限责任公司（以下简称“本公司”）客户使用。本公司不因接收人收到本报告而视其为客户。

本报告基于本公司认为可靠的、已公开的信息编制，但本公司对该等信息的准确性及完整性不作任何保证。本报告所载的意见、评估及预测仅为本报告出具日的观点和判断，该等意见、评估及预测无需通知即可随时更改。在不同时期，本公司可能会发出与本报告所载意见、评估及预测不一致的研究报告。同时，本报告所指的证券或投资标的的价格、价值及投资收入可能会波动。本公司不保证本报告所含信息保持在最新状态。本公司对本报告所含信息可在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。

本公司力求报告内容客观、公正，但本报告所载的观点、结论和建议仅供投资者参考之用，不构成所述证券的买卖出价或征价。该等观点、建议并未考虑到获取本报告人员的具体投资目的、财务状况以及特定需求，在任何时候均不构成对客户私人投资建议。投资者应当充分考虑自身特定状况，并完整理解和使用本报告内容，不应视本报告为做出投资决策的唯一因素，必要时就法律、商业、财务、税收等方面咨询专业财务顾问的意见。对依据或者使用本报告所造成的一切后果，本公司及作者均不承担任何法律责任。

本公司及作者在自身所知情的范围内，与本报告所指的证券或投资标的不存在法律禁止的利害关系。在法律许可的情况下，本公司及其所属关联机构可能会持有报告中提到的公司所发行的证券头寸并进行交易，也可能为之提供或者争取提供投资银行、财务顾问或者金融产品等相关服务。本公司的投资业务部门可能独立做出与本报告中的意见或建议不一致的投资决策。

本报告版权仅为本公司所有。未经本公司书面许可，任何机构或个人不得以翻版、复制、发表、引用或再次分发他人等任何形式侵犯本公司版权。如征得本公司同意进行引用、刊发的，需在允许的范围内使用，并注明出处为“川财证券研究所”，且不得对本报告进行任何有悖原意的引用、删节和修改。本公司保留追究相关责任的权力。所有本报告中使用的商标、服务标记及标记均为本公司的商标、服务标记及标记。

本公司具有中国证监会核准的“证券投资咨询”业务资格，经营许可证编号为：J19651000。