2019 年 10 月 22 日

中国宏观观察

区块链技术的运用

蔡涵
hanna.cai@bocomgroup.com
(852) 3766 1805

谭淳
karen.tan@bocomgroup.com
(852) 3766 1825

彭非
fei.peng@bocomgroup.com
(852) 3766 1804

- **有别于传统数据库，区块链本质上是一个以去中心化为核心的分布式账本数据系统。**其排除了被第三方中心控制的风险，从而更能保障信息的安全。在没有权威的中心化代理的背景下，区块链通过分布式存储，让所有节点的参与者共同维护一个数据库并彼此监督，以解决信息可信度和准确度的问题。

- **为了解决交易信息传递过程中发起交易人身份确认及信息被篡改的问题，区块链通过非对称加密来保护信息的准确性。**若过程中有任何环节被篡改，都将使得结果完全不同。因而解决了在这个公开、匿名、彼此无信任的分布式网络中的信任问题。而较长链认可规则则可以防止信息被篡改。若想要篡改区块链中的数据，重新计算的行为等同于将自己与其他所有的节点置于竞争的状况。除非拥有理论上超过 51%的算力，否则在区块链这个少数服从多数的规则下，篡改数据的构想不会成立。

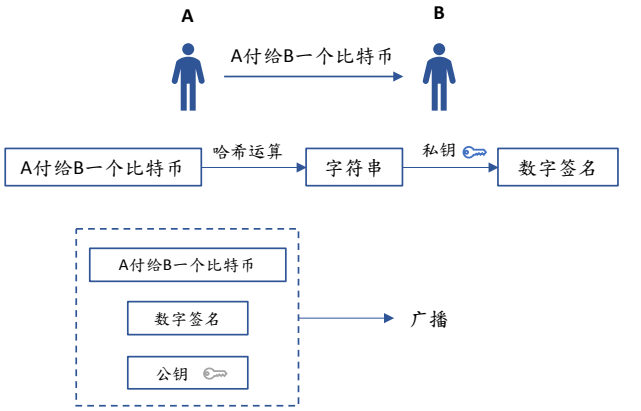
- **区块链的应用场景广泛多元。**本质上，区块链技术解决的核心问题是人与人之间的信任危机，目的在于建立一个互信共识的社会机制。其应用从对交易各方有建立相互信任的需求，却又难以在短时间内实现的领域开始，例如银行、证券以及保险等行业。区块链技术的公开、不可篡改特征解决了金融业去中心化后潜在的信任风险。在公共服务领域，受限于有限的数据维度、未建立的历史数据信息链时常导致政府、机构以及学校等无法获取真实完整的信息。此时区块链不可篡改的属性将有助于建立全新的数字化证明体系，在数字版权、知识产权及公益等领域实现其价值。

- **区块链自身的技术瓶颈及法律监管的不确定性等问题都是区块链应用未广泛落地的原因。**从技术层面来看，由于节点的延迟，区块链技术的交易速度缓慢，目前并不适合高频交易场景。从监管层面来看，其去中心化概念淡化了国家监管的概念，对现行的制度产生了一定冲击。对于一个分散式网络来说，监管资金动向也极为困难。比特币由于其匿名特性，正在成为犯罪资金的主要载体。

- **按照区块链的运行逻辑，加入区块链的节点越多，该链的信用度就越高。**然而，随着不断的上链，个人的一切信息在外界看来都将变得异常透明清晰。当人们在追求极致信任的道路上，个人与个人之间，机构与机构之间、甚至国家与国家之间将对彼此了如指掌，而这或许不是所有人希望见到的。当然，这种完全开放的公链多少带着些许乌托邦的气息，这也是后续诸如私有链、联盟链等不断涌现的原因。

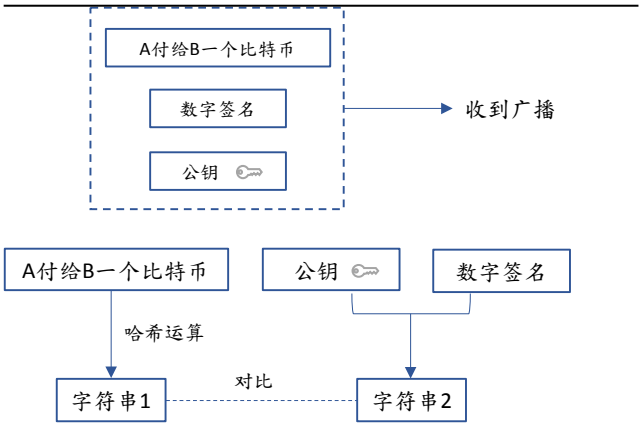
本周焦点图表

图表 1: 信息加密过程



资料来源：交银国际

图表 2: 信息解密验证过程



资料来源：交银国际

区块链技术的运行

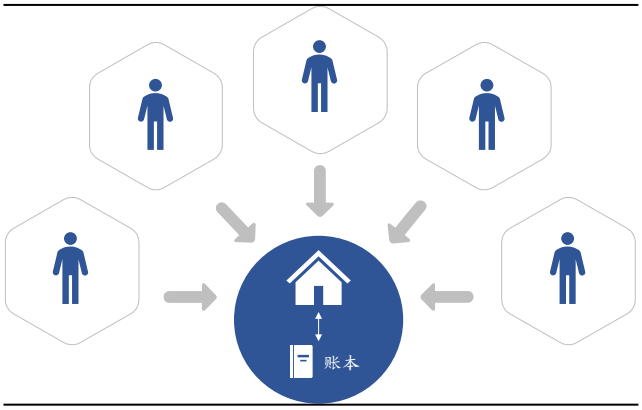
有别于传统数据库，区块链本质上是一个以去中心化为核心的分布式账本数据系统。在区块链的概念中，所有能够部署服务器节点的人均可参与。而所有参与者都有权利在系统中进行操作，最终各节点将在某种机制下完成同步，从而实现所有节点数据的一致性。

区块链的核心：去中心化

传统的数据库依赖于中心代理，交易流程除了买家与卖家外有第三方作为中心进行记账，因而所有的交易都围绕中心代理展开。好比在淘宝上购物，买家与卖家都需要通过支付宝这个第三方平台来完成交易。倘若交易出现问题则可以通过支付宝寻求帮助。这种以中心化思维为核心的交易方式通过权威方背书来获得各方信任，依赖其背后的资本与技术来保证数据的安全性与可靠性。

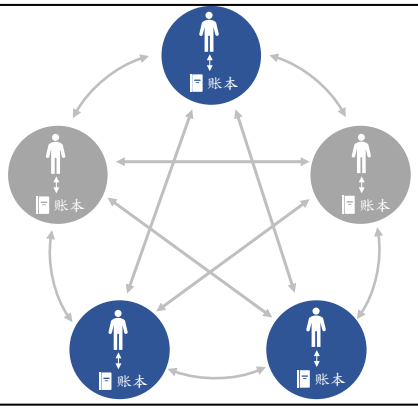
而去中心化的交易则是一个点对点的交易过程。也就是说，这笔交易只需要通过买家与卖家，双方认可即可完成。因此，去中心化的交易相较于传统的交易方式，由于排除了被第三方中心控制的风险，更能保障信息的安全。但在没有权威的中心化代理的背景下，信息的可信度和准确度将遭到质疑。区块链的设计通过分布式存储，让所有节点的参与者共同维护一个数据库并彼此监督，以解决上述问题。

图表 3: 中心化交易模式



资料来源：交银国际

图表 4: 去中心化交易模式

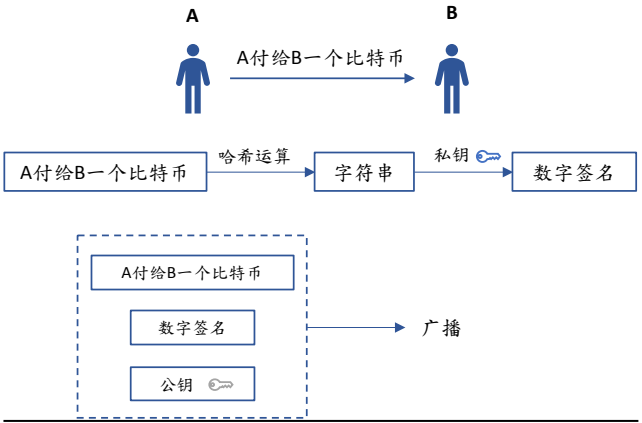


资料来源：交银国际

精巧的密码学设计以保证数据的可信度

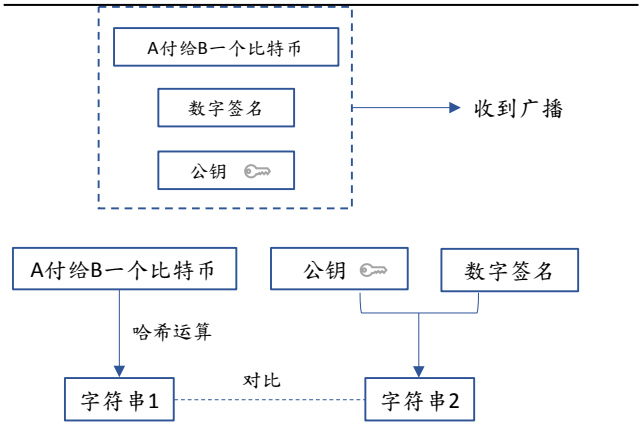
为了解决交易信息传递过程中被人篡改及发起交易人身份确认的问题，区块链通过精巧的密码学设计以保障数据的可信度及准确度。传统的身份认证方式例如人脸识别、签名、指纹等在计算机系统中均可被拷贝，因而产生了电子签名的方式——通过非对称加密，对交易信息进行加密及解密验证来保护信息的准确性。具体而言，以比特币交易“A 付给 B 一个比特币”为例，A 将这条交易信息通过哈希运算进行处理得到一条固定长度的字符串，通过私钥进行再次加密获得被称之为数字签名的字符串，然后将这条信息、公钥和数字签名广播给其他人。验证信息的人也将通过哈希运算对信息进行处理得到字符串 1，同时使用公钥对数字签名进行解密得到字符串 2，若两者相同，即可认为消息不是伪造的。这种环环相扣的加解密方式，若之中有任何环节被篡改，都将使得结果完全不同，因此，能在这个公开、匿名、彼此无信任的分布式网络中解决信任问题。

图表 5: 信息加密过程



资料来源：交银国际

图表 6: 信息解密验证过程

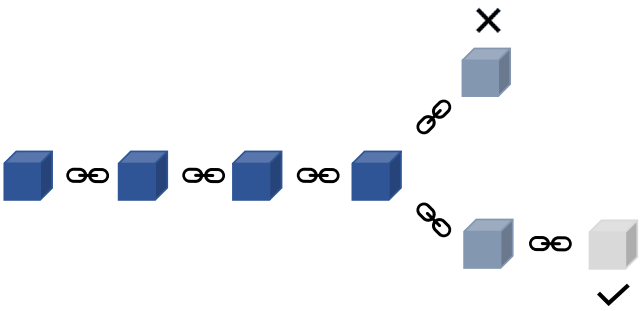


资料来源：交银国际

较长链认可规则防止信息篡改

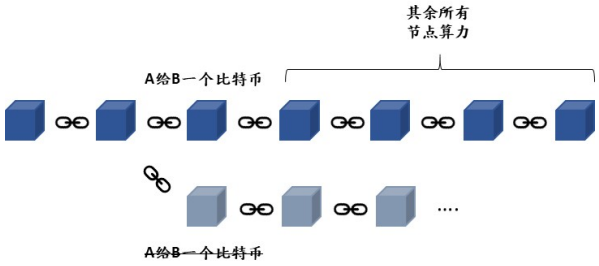
若不只一个节点同时参与了对区块的校验，并通过了验证将区块上链，那区块就被分叉，即违背了所有节点维护同一份数据的原则。因而，在区块分叉的情况下，拥有最长链的区块将被认可。因此，在理论上，分叉这种僵局很快会在下一个区块被挖出来时被打破。若想要篡改区块链中的数据，重新计算的行为等同于将自己与其他所有的节点置于竞争的状况。除非拥有理论上超过 51%的算力，否则在区块链这个少数服从多数的规则下，篡改数据的构想不会成立。

图表 7: 拥有较长支链的区块将存活



资料来源：交银国际

图表 8: 篡改区块链中的数据等同于将自己与其他所有的节点置于竞争中



资料来源：交银国际

以去中心化为核心的区块链技术的运用

当我们提及区块链，很多时候只会联想到比特币。事实上，比特币仅仅是区块链概念集合内极小的子集。区块链的意义在于可以构建一个可靠的互联网网络，以较低的成本及简化的流程解决价值交换与转移中可能存在的不诚信现象。随着区块链的逐步落地应用，社会将会建立起一个相互无信任的完全信任体系。

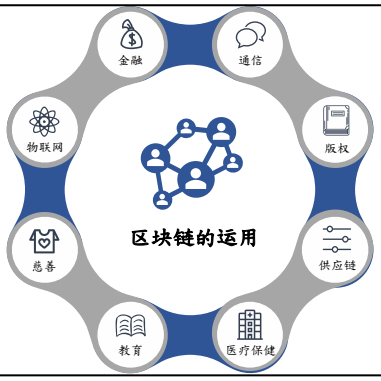
区块链的应用将从对交易各方有建立相互信任的需求，却又难以在短时间内实现的领域开始，例如银行、证券以及保险等行业。区块链技术的公开、不可篡改特征解决了金融业去中心化后潜在的信任风险。各类金融产品，如股权、债券、票据等均可以通过整合进区块链账本，成为区块链上的资产而实现快速又低成本的链上存储、转移及交易。举例来说，随着全球一体化的推进，跨境支付需求日益旺盛。传统的跨境支付不可避免的存在大量中心化的信用中介和信息中介，在降低资金流动效率的同时增加了资金往来成本，使得一笔跨境支付需要至少 24 小时完成。而应用区块链的跨境支付，不仅可以提供 7x24 小时不间断的服务，更能减少支付流程中大量人工对账操作，大大缩短清算结算时间。此外，金融机构在运营中需要时刻履行了解你的客户的义务（know your customer），而核实客户信息的过程耗时冗长又难以保证信息的真实性。此时，利用区块链技术建立信任，存储客户身份的电子档案，在满足监管要求的前提下也保护了客户的信息安全，可谓一举多得。

随着应用的逐步普及，区块链技术将向其他领域逐步渗透。在公共服务领域，受限于有限的数据维度、未建立的历史数据信息链时常导致政府、机构以及学校等无法获取真实完整的信息。此时区块链不可篡改的属性将有助于建立全新的数字化证明体系，在数字版权、知识产权及公益等领域实现其价值。

以贴近生活的音乐产业为例，当前互联网行业内版权费用的支付链条复杂繁琐，一般情况下需要经过版权代理方、唱片公司、艺人经纪人、音乐平台等多方才能最终到达音乐人的口袋，该过程不仅耗时、且在多方不断抽成的情况下压榨了音乐人的收入。区块链技术的介入将使得每一首在区块链平台上注册的歌曲的数字内容，包括词曲、唱片内容、版权授权以及用户信息等完整的独立保存且无法篡改，作品在区块链上被确权后，后续交易都会进行实时记录，实现数字版权全生命周期管理，因此音乐人可以不经过唱片公司来注册自己的产品版权，意味着其可以直面客户，及时便捷的获取版权费用。同样的，区块链技术可以应用到诸如教育、产权登记及医疗健康等领域，显著改善公共服务领域的管理质素。

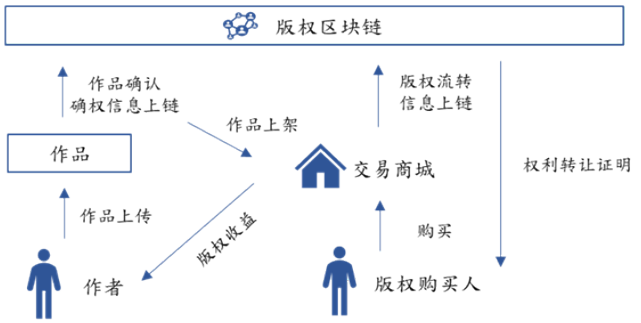
区块链的应用场景广泛多元，物联网、供应链管理、公益慈善领域等均可见到其身影。本质上，区块链技术解决的核心问题是人与人之间的信任危机，目的在于建立一个互信共识的社会机制。

图表 9: 区块链运用广泛



资料来源：交银国际

图表 10:区块链运用：版权



资料来源：交银国际

区块链技术的局限性

截至目前，除了比特币之外，在市场中成熟运行并被广泛接受或认知的区块链应用并不多见。自身的技术瓶颈及法律监管的不确定性等问题都是区块链未广泛运用的原因之一。

从技术层面来看，由于节点的延迟，区块链技术的交易性能目前并不适合高频交易场景。典型的区块链如比特币需要约 10 分钟来确认交易，安全的交易确认时间甚至需要一个小时左右，平均交易速率约为每秒 4 个交易。以太坊的交易吞吐量略高，能够达到 10-20 个。然而与传统VISA交易网络平均每秒处理 2,000 笔交易、几秒钟内确认交易相比也只能是小巫见大巫了。

从监管层面来看，区块链的去中心化概念淡化了国家监管的概念，对现行的制度产生了一定冲击。各国监管机构目前对于该项技术的落地缺乏理论准备及制度讨论，不同国家亦持有不同态度。以区块链为技术背景的数字货币对国家货币发行造成挑战，影响货币政策同时弱化央行经济调控能力。除此以外，对于一个分散式网络来说，监管资金动向也极为困难。比特币由于其匿名特性，正在成为犯罪资金的主要载体。

按照区块链的运行逻辑，加入区块链的节点越多，该链的信用度就越高。然而，随着不断的上链，个人的一切信息在外界看来都将变得异常透明清晰。当人们在追求极致信任的道路上，个人与个人之间，机构与机构之间、甚至国家与国家之间将对彼此了如指掌，而这或许不是所有人希望见到的。当然，这种完全开放的公链多少带着些许乌托邦的气息，这也是后续诸如私有链、联盟链等不断涌现的原因。

图表 11: 公有链、联盟链及私有链对比

	公有链	联盟链	私有链
去中心化程度	去中心化	多中心化	（多）中心化
参与者	任何节点	联盟成员	企业、机构或个体内部
记账人	所有节点	联盟规则决定	自定义
奖励机智	需要	可选	不需要
承载能力	3-20 (TPS)	1000-10000 (TPS)	1000-100000 (TPS)
运用	数字货币	机构间的交易、结算	审计、内部数据管理

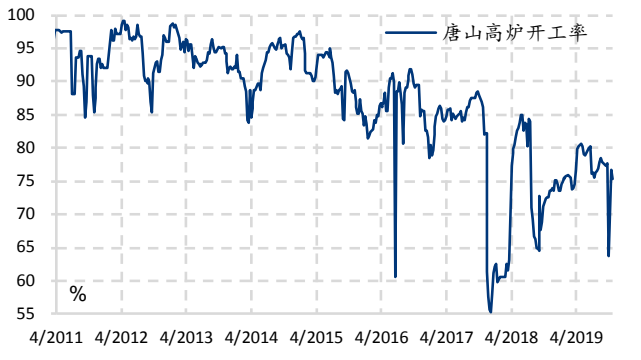
资料来源: 公开资料整理，交银国际

经济领先指标

图表 12: 螺纹钢价格（周度）

资料来源：Macrobond，交银国际

图表 13: 唐山高炉开工率（周度）



资料来源：彭博，交银国际

图表 14: 铁矿石价格指数及进口量

资料来源：Macrobond，交银国际

图表 15: 铁矿石库存同比增速（周度）

资料来源：彭博，交银国际

图表 16: 水泥市场价格（周度）

资料来源：CEIC，交银国际

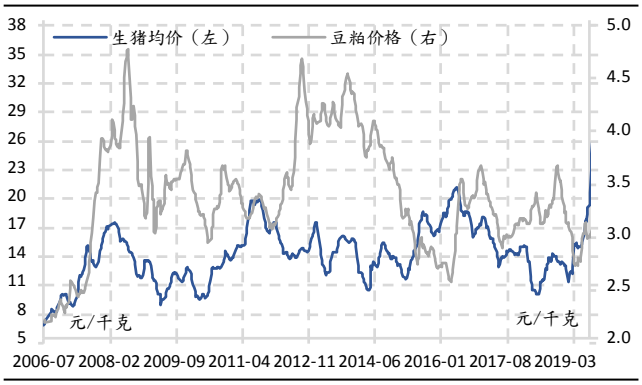
图表 17: 西部地区水泥市场价格（周度）

资料来源：CEIC，交银国际
注：西部地区城市包括昆明、成都、重庆、贵阳、西安、兰州、西宁和银川。

图表 18: 长江有色市场无氧铜丝价格（日度）

资料来源：彭博，交银国际

图表 19: 生猪、豆粕价格（周度）

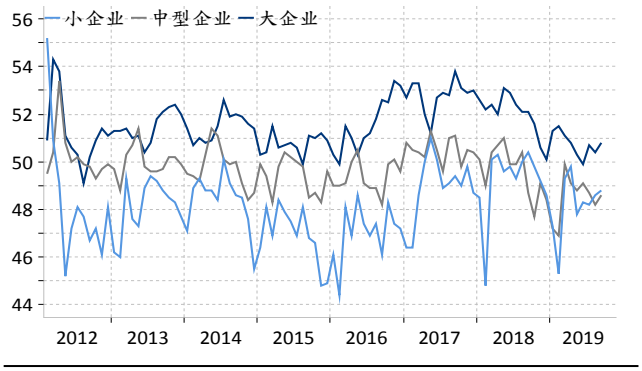


资料来源：万得，交银国际

图表 20: PMI 中国制造业与非制造业（月度）

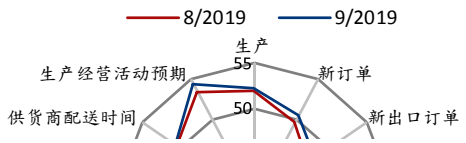
资料来源：Macrobond，交银国际

图表 21: PMI 中国大中小企业 - 带季调（月度）



资料来源：Macrobond，交银国际

图表 22: PMI 制造



图表 23: PMI 非制造