2019 年 09 月 20 日

证券研究报告•宏观报告

专题报告

西南证券 SOUTHWEST SECURITIES

解密数字货币：概念、局限和前景

摘要

- **数字货币是一种基于节点网络和数字加密算法的虚拟货币。**不具有发行主体、基于有限的算法解数量实现总量固定以及交易过程需要网络中各个节点认可，这几个主要的数字货币特征决定数字货币的特定技术。其中满足这些要求的区块链技术是在数字货币中应用最为广泛的技术，因而数字货币与区块链成为孪生词，区块链技术也往往决定了数字货币的属性。

- **区块链本质上是一个去中心化的分布式数据库，具有去中心化、不可篡改性、去信任的技术特点。**每个区块包含前一个区块和自身的数字标签，自身数字标签是通过前一个区块的数字标签和自身存储的数据计算出来的。如果某一个区块的数据被篡改了，那么其数字标签也会改变，因而区块链具有不可篡改性。区块链语境下的去信任不意味着没有信用风险，而是指写入数据不需要依靠对某个中心机构的信任。

- **区块链与数字货币的核心约束是不可能三角，即：去中心化、安全和高效率低成本三者无法兼得。**区块链技术特性决定无法同时完成去中心化、安全性和高效率低成本三个目标，不可能三角是区块链技术落地必须面对的问题。而去中心化是区块链的核心思想，区块链系统不可能完全放弃去中心化，安全性是任何货币支付稳定存在的基数，但如果基于区块链技术的应用要大规模推广，就需要提升效率、降低成本。在数字货币实际应用过程中，不可能三角就转化为去中心化和交易规模扩大之间权衡的现实问题。

- **不可能三角决定了去中心化、成本效率和安全性无法同时实现，因此当前各类去中心化的“数字货币”难以成为主流货币，对传统货币体系冲击有限。**比特币高度去中心化，但也导致其运行速度过慢，无法应用于大规模交易；USDT 和 Libra 在一定程度上牺牲了去中心化，效率方面有所提升，但仍旧难以支持大规模交易。同时因为发行的中心化，此类“数字货币”还存在发行主体风险。

- **我国的央行数字货币（DCEP）是中心化的，属性和功能与纸币完全相同，主要是对 M0 的替代。**我国的央行数字货币依旧是中央银行的负债，这种债权债务关系并没有随着货币形态变化而改变，因此，DCEP 的发行是中心化的。同时 DCEP 可以像纸币一样流通，不需要绑定任何银行账户，具体场景中，只要手机上有 DCEP 的数字钱包，不需要网络，只要两个手机碰一碰，就能实现转账功能，也不需要实名认证或是绑定手机号等个人信息。

- **数字货币采用双层架构发行，不会导致商业银行被通道化或者边缘化，具体技术上，私有链适用于央行向商业银行发行管理数字货币。**DCEP 发行与纸钞类似，采用双层架构，央行先把数字货币兑换给商业银行，再由商业银行兑换给公众，数字货币属于 M0 范畴，是央行的负债，在商业银行的资产负债表之外。因此，数字货币交易不依赖商业银行账户与现金交易不依赖商业银行账户是类似的。

- 风险提示：央行政策超预期，技术进步超预期。

西南证券研究发展中心

分析师：杨业伟

执业证号：S1250517050001

电话：010-57631229

邮箱：yyw@swsc.com.cn

相关研究

1. 联储降息内部分歧加大，经济走势决定宽松持续 (2019-09-20)
2. 供需双缩经济放缓压力上升，稳增长政策需更有效 (2019-09-17)
3. 经济预期改善风险资产回升，调整还是反转？ (2019-09-15)
4. 信贷社融略超预期但不改融资收缩趋势 (2019-09-12)
5. 猪周期推升通胀，但无需过度担忧 (2019-09-10)
6. 贸易战影响渐显叠加全球经济走弱，外需继续走弱 (2019-09-08)
7. 降准后资金将继续在金融市场淤积 (2019-09-08)
8. 供需双缩，经济放缓压力上升 (2019-09-01)
9. 8 月 CPI 同比能否到“3”——基于商务部和农业部数据的不同预测结果 (2019-08-30)
10. 政策继续围于结构，信用收缩经济逐步放缓——月度经济预测 (2019-08-30)

目 录

图 目 录

表 目 录

自 2009 年比特币问世以来，数字货币不断成为讨论的热点，大量数字货币的创立与炒币热潮更是将数字货币的关注度推向顶峰。各国央行也相继对数字货币表示关注，甚至计划推出自己的数字货币，更是凸显了数字货币的和重要性。而在提到数字货币的同时，区块链往往是一个伴生的词语，似乎二者是一对孪生兄弟。那么，到底什么是数字货币？数字货币与区块链有什么关系？数字货币能够替代传统货币吗？数字货币对传统货币体系冲击如何？本文通过对数字货币、区块链的介绍分析，阐述分析区块链能做什么、不能做什么，以及数字货币与区块链的关系。进而分析数字货币对传统货币体系的可能冲击，以及我国央行将推行的数字货币可能的模式和对货币体系的影响。

1 数字货币与区块链优势与约束

1.1 什么是数字货币，什么是区块链

数字货币英文是 Digital Currency，简称为 DIGICCY。**对数字货币缺乏统一的定义，一般认为数字货币是一种基于节点网络和数字加密算法的虚拟货币**。狭义的定义中要求数字货币没有发行主体，确定的算法解数量决定总量固定，同时交易过程需要网络中各个节点认可。而这些技术特点都诞生于比特币，因而狭义数字货币基本上指以比特币为样本的货币。而相对广义的数字货币则在这些技术特点方面有所放松，部分拥有发行主体，部分总量基于某些可增加的资产而不固定等。扩展后的数字货币甚至纳入了部分网络主体发行的，加密性并不是很高的虚拟货币。

总的来说，不具有发行主体、基于有限的算法解数量实现总量固定以及交易过程需要网络中各个节点认可，这几个主要的数字货币特征决定数字货币的特定技术。其中满足这些要求的区块链技术是在数字货币中应用最为广泛的技术，因而数字货币与区块链成为孪生词，区块链技术也往往决定了数字货币的属性。由于数字货币大多基于区块链技术，我们通过对区块链的分析介绍，来了解数字货币的特点和优势。

区块链本质上是一个去中心化的分布式数据库。具有去中心化、不可篡改性、去信任的技术特点。

首先，区块链是一个数据库，它是一系列区块的链接，每个区块包含了需要加密的数据和数字签名，其中数字签名的逻辑关系是连接区块的纽带。每个区块包含三个部分：需要存储的数据、上一个区块的数字签名和自己的数字签名，其中自己的数字签名是通过上一个区块的数字签名和自身存储的数据按照预先设定的规则计算出来的。以比特币为例，每一个区块中保存的是比特币的交易信息，随着交易不断发生，需要越来越多的区块存储信息，新的区块按照时间顺序线性补充到区块链上。

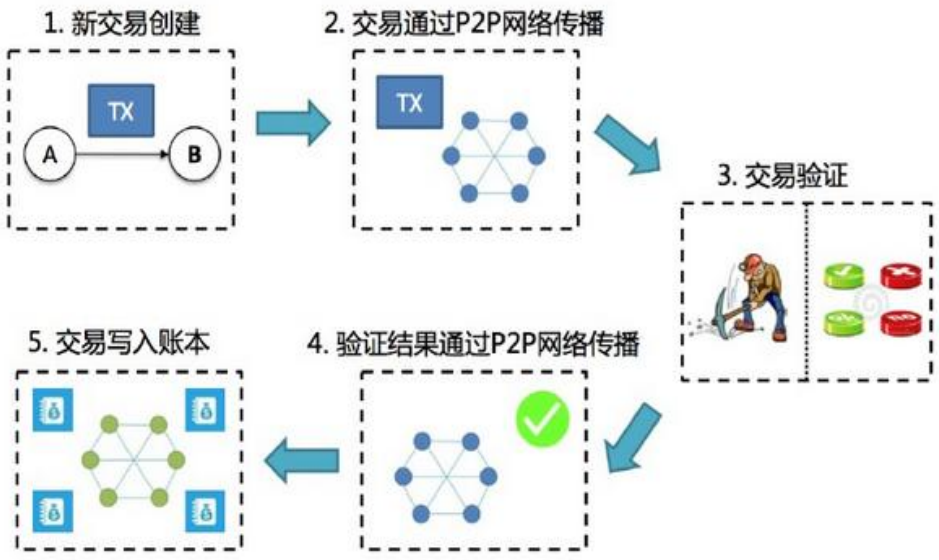
图 1：区块链的技术逻辑（图中 hash 值即为数字签名）

数据来源：Cnblogs，西南证券整理

其次，在区块+链结构的基础之上，区块链上数据的记录和存储是分布式、去中心化的。传统的数据库是中心化的，如市面上的各类网盘，所有用户的数据存储于运营商的服务器中，每位用户上传下载数据都要和运营商服务器进行交互，用户权限是有限的，仅能访问和修改数据库的部分数据，而运营商权限理论上是无限的，可以访问和修改所有数据。

区块链则允许每一个用户都记录并存储所有的数据，并且实时更新，如果某个节点想要将新的数据写入区块链，它需要在整个区块链网络内广播，只有全网大部分节点认可该记录时，数据才被允许写入区块链中，并在整个网络内更新。

图 2：区块链写入新交易数据的流程图



数据来源：CSDN，西南证券整理

以比特币为例，如果 A 想要向 B 转账，交易数据会被打包成区块发送到整个网络中，矿工们对数据进行验证并计算新区块的数字签名，当该交易被大部分节点验证通过后，验证结果通过网络传播并写入账本，在比特币系统中，为了鼓励矿工验证交易、参与数据的存储和记录，成功计算出数字签名的矿工会获得一定数量的比特币作为奖励。

数字签名和去中心化设计使区块链具有不可篡改性和去信任的特点。每个区块包含前一个区块和自身的数字标签，自身数字标签是通过前一个区块的数字标签和自身存储的数据计算出来的。如果某一个区块的数据被篡改了，那么其数字标签也会发生变化，这会导致后续所有区块的数字标签发生变化，而在去中心化的系统中，这样的篡改是不会被其他节点验证通过的，因而区块链具有不可篡改性。

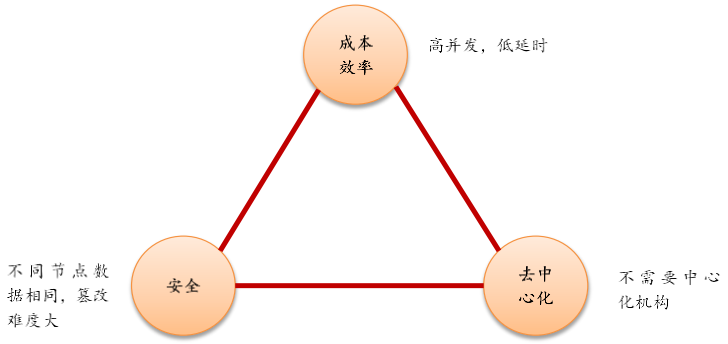
区块链语境下的去信任不意味着没有信用风险，而是指写入数据（加密货币交易实际上也是写入数据）不需要依靠对某个中心机构的信任。第一，传统的网络系统中，参与者必须对中心机构有足够的信任，随着参与者越来越多，中心机构运营难度会越来越大，参与者对中心机构的信任度也会受到影响，但区块链系统恰恰相反，随着参与者的增加，整个系统的安全性反而增加了。第二，当使用区块链内加密货币进行交易时，去信任指的是加密货币的状态变更和交易确认同步发生这一安排。假设 A 以比特币向 B 买入某一商品，A 向 B 支付比特币这一过程无需两人之间有任何了解，也无需受信任的第三方机构，就可以在区块链内有保障地进行，但在交易的另一端，A 如何确保 B 会按时向她交付合格的货物？只要做不到一手交比特币、一手交货，就存在不容忽视的交易对手信用风险。

1.2 数字货币与区块链的局限——不可能三角

区块链技术具有去中心化、去信任、不可篡改等诸多优秀特性，基于区块链技术的加密货币（如比特币）似乎很适合用做支付工具，但实际上，比特币作为支付工具的使用不频繁，并没有成为一种主流的货币，大部分比特币由投资者和非频繁使用者持有。

比特币至今没有成为主流货币的原因有很多，其中最根本的原因是 Abadi 和 Brunnermeier （2018）[1]经分析提出的区块链的不可能三角，即：去中心化、安全性和成本效率三者无法兼顾。比特币高度去中心化，同时安全性也很高，但比特币网络每秒只能处理 7 笔交易，在当前比特币没有大规模应用于支付的情况下从交易提交到最终成交往往需要数十分钟，因此比特币难以成为广泛使用的支付方式。而 “黑市”交易则是比特币的天然土壤，对于将比特币用于非法交易的用户来说，它们看中的是比特币的高度隐蔽性和不可追踪性。 Foley et al. (2018)研究了比特币在非法经济活动中的应用，发现 25%的比特币用户和 44%的比特币交易与非法经济活动有关。

图 3：区块链的不可能三角



数据来源：西南证券整理

[1] Abadi, Joseph, and Markus Brunnermeier, 2018, “Blockchain Economics”.

去中心化是区块链的核心思想，区块链系统不可能完全放弃去中心化，但不可能三角是区块链技术落地必须面对的问题，任何基于区块链技术的应用都必须在成本效率、安全性和去中心化三者间做出平衡。

2 各类区块链形式与数字货币的发展方向

2.1 区块链的三种部署形式

早期以比特币为代表的区块链系统高度重视去中心化，但此类系统在成本效率上的固有缺陷极大的限制了其应用落地，因此**人们在其基础上做出改进，提出了公共链、联盟链和私有链三种区块链的部署形式。这些新的部署方式实际上是在不同程度上放松了去中心化，以满足不同应用场景的需求。**

表 1：区块链的三种部署形式

	公有链	联盟链	私有链
去中心化程度	去中心化程度最高，每个节点权重相同	去中心化程度一般，写入数据需要共识机制确认，但只有事先设定好的节点能够参与	去中心化程度差，中心控制者可以指定参与和验证交易的成员范围
参与者	公开的，任何节点无需授权均可接入	仅对特定节点开放，接入需授权	
共识机制	往往需要“数字货币”作为参与验证节点的奖励；能耗高；所有节点均可参与验证，理论上控制50%以上 节点即可以控制整个区块链	一般不需要提供“数字货币”作为参与验证节点的奖励；相比公有链，更加轻量级，能耗低；仅特定节点可参与验证	
运行速度	缓慢的，新数据写入（如提交一笔交易）需要数十分钟	快速的，写入新数据速在数秒，甚至一秒内完成	

数据来源：西南证券整理

公有链是真正意义上去中心化的区块链。公有链节点面向公众开放，所有参与者均可以存储、记录和验证交易，往往需要“数字货币”作为参与验证节点的奖励，因为参与节点数量多，公有链能耗高，运行效率低。

相比公有链，私有链几乎放弃去中心化，严格意义上已经不具有区块链分布式、去中心化的特征。该网络的写入权限由某个中心化组织全权控制，它可以指定参与和验证交易的成员范围，数据读取权限受组织规定，与公有链相比，私有链达成共识的时间相对较短、交易速度更快、效率更高、成本更低。

联盟链是一种介于公有链和私有链之间的区块链部署形式。联盟链是指有若干个机构共同参与管理的区块链，每个机构都运行着一个或多个节点，数据只允许系统内机构进行读写和发送交易，并且共同记录交易数据，联盟链是多中心的，参与成员需要符合某些特征（如上交所会员单位等），同样具有成本较低、效率较高的特点。

2.2 区块链的三种应用

近年来人们总是将区块链和数字货币联系在一起，但数字货币只是区块链技术的应用之一，而数字货币也不一定依赖于区块链技术。参考徐忠（2018）[2]分类方式，我们从区块是

[2] 徐忠、邹传伟，2018，《区块链能做什么，不能做什么》，中国人民银行工作论文，2018 年第 4 号。

否涉及数字货币角度，将区块链的应用分为三类：无币区块链、非公开发行数字货币的区块链以及公开发行数字货币的区块链。

无币区块链可以理解成一个分布式、不可更改的记账本。区块链的公共共享账本功能有助于缓解经济活动参与者之间的信息不对称，提高分工协作的效率，目前典型应用有中国人民银行数字货币研究所的湾区贸易金融区块链平台和基于区块链技术的资产证券化信息披露平台。**非公开发行数字货币的区块链中，“数字货币”代表了区块链外的资产或权利，作为内部结算工具，可以提高结算效率，减少资金占用**，实务中还依赖外部世界的法律，目前典型应用有上交所推出的数字票据交易平台。

相比公有链，联盟链和私有链是无币区块链和非公开发行数字货币区块链更适合的部署形式。第一，这两个应用方向均无需面向全部公众；第二，这两类应用的参与者身份透明度高，区块链外的法律、道德等对成员约束力强，去中心化诉求不高；第三，这两类应用的优势在于效率高，安全性好，在效率、安全性和去中心化不可兼得的情况下，去中心化是最先被放弃的。

表 2：区块链的主要应用方向

应用方向	应用逻辑	代表性应用场景	适合的部署方式
无币区块链	区块链本质是一个数据库，发挥其共享账本功能，但不涉及直接的财产和风险转移	供应链管理、数据共享、社会诚信、贸易管理和金融信息披露等	私有链、联盟链
非公开发行“数字货币”的区块链	“数据货币”代表区块链外的资产或权利	资产上链以及供应链金融和数字票据等	联盟链
公开发行数字货币的区块链	以“数字货币”为计价单位或标的资产的经济活动，依赖区块链外的法律框架	比特币期货、比特币ETF	公有链
	以“数字货币”为支付工具和激励手段重构经济活动	比特币、Libre等	公有链

数据来源：中国人民银行工作论文，西南证券整理

2.3“数字货币”如果要有大发展，需要部分放弃去中心化

公开发行“数字货币”的区块链是是近年来市场的焦点，但我们认为目前现有的去中心化“数字货币”难以成为主流货币，主要是去中心化会大幅降低效率，因而“数字货币”如果要有大发展，必须部分放弃去中心化。