

计算机

证券研究报告

2019年11月15日

数字货币支持效率提升，产业链细分梳理投资机会

投资评级

行业评级

强于大市(维持评级)

上次评级

强于大市

作者

沈海兵

分析师

SAC 执业证书编号: S1110517030001

shenhaibing@tfzq.com

行业走势图



资料来源: 贝格数据

相关报告

- 1 《计算机-行业研究周报:定量测算数字货币产业链机会,再融资宽松利好细分龙头(附表)》 2019-11-10
- 2 《计算机-行业研究周报:政治局集体学习,区块链迎来历史性机遇》 2019-10-27
- 3 《计算机-行业研究周报:DRGs 付费试点顶层设计完成,关注互联网大会新技术主题性机会》 2019-10-19

货币数字化的意义在于从体系上支持社会效率提升

短期来看,数字货币能够降低实体货币的高成本,并增强对交易过程中信息的把握;长期来看,数字货币有望丰富货币政策工具,促进跨境流转支持人民币国际化,最重要的是民生领域中有望增强资金流转效率并降低信用风险。当前国际上主要是发展中国家,出于增强法币地位、改善金融制度的原因发行数字货币,但也正是由于法币地位不足而难以取得成功。我国有望成为首个发行数字法币的主流经济体。

数字货币将在央行、商业银行、用户三个层面产生改变

数字货币在发行端(央行)主要将有数字货币系统和认证库的建设;在投放端(商业银行)主要要新建数字货币系统(包括钱包系统)、认证系统并改造传统账户系统;用户端依据 ToC 和 ToB,主要包括支付体系和行业应用的改变。预计市场空间将依央行->商业银行->用户端逐级递增。

产业链建设机会梳理

- 央行端:预计央行端系统将以自研自建为主,但央行端的关键技术选型将决定商业银行系统规格,预计认证/加密体系的选择将成为关键;
- 投放端:传统账户系统需要改造,银行机具或也有小幅改造可能;新建系统方面数字货币核心系统、认证系统、钱包系统预计空间在 180 亿左右;
- 流通端:支付机具有改造需求,整体替换需求在 200-300 亿左右;支付体系中服务商角色不会消亡,有望加速向服务化转型;ToB 应用发展预计在数字货币运行稳定之后,有望产生现象级应用空间广阔。

投资建议

央行层面建设规模较小,且预计以自研自建为主,企业参与机会不大,也可关注数据库、中间件、网络安全等基础设施行业的机会。

投放层面,传统系统改造与新系统建设,重点推荐长亮科技,建议关注润和软件、信雅达等;认证系统,重点推荐格尔软件、数字认证;银行机具改造,建议关注广电运通、聚龙股份等。

流通层面,支付机具重点推荐新大陆,建议关注新国都;支付体系建议关注新大陆、拉卡拉(传媒覆盖)、新国都;ToB 应用的成长期预计在数字货币稳定运行之后,当前时点建议关注有强运营能力的行业平台,如恒生电子、上海钢联、远光软件、航天信息、信息发展等。

风险提示:央行尚未正式发布数字货币系统;数字货币落地进展不及预期;数字货币系统建设规模不及预期。

重点标的推荐

股票代码	股票名称	收盘价	投资评级	EPS(元)				P/E			
				2018A/E	2019E	2020E	2021E	2018A/E	2019E	2020E	2021E
300348.SZ	长亮科技	19.35	买入	0.12	0.45	0.57	0.70	161.25	43.00	33.95	27.64
000997.SZ	新大陆	15.35	买入	0.56	0.83	1.09	1.42	27.41	18.49	14.08	10.81
603232.SH	格尔软件	30.33	增持	0.59	0.64	0.82	1.20	51.41	47.39	36.99	25.28
300579.SZ	数字认证	45.74	买入	1.29	1.73			35.46	26.44		

资料来源: 天风证券研究所,注: PE=收盘价/EPS



内容目录

前言	4
1. 货币数字化的意义在于从体系上支持社会效率提升	4
1.1. 数字货币短期意义在于改进支付，但长期可能带来体系改变	4
1.2. 国际社会开始关注，我国有望成为首个发行法定数字货币的主要经济体	4
2. 数字货币将在央行、商业银行、用户三个层面产生改变	6
3. 功能梳理：央行端承担主要归属结算职责	7
3.1. 数字货币的发行	7
3.2. 数字货币的支付流程	8
3.3. 数字货币的存款流程	9
4. 产业链建设情况梳理	10
4.1. 发行端系统中，认证系统将是建设的关键	10
4.1.1. 若央行采取偏中心化运营的方式，对央行数字货币系统性能要求较高	10
4.1.2. 认证体系是数字货币系统的关键基础建设，决定体系安全性	11
4.2. 预计商业银行系统将是民资主要参与的基础设施部分	12
4.2.1. 商业银行传统账户需对接数字货币系统，传统机具或有小幅改造空间	12
4.2.2. 预计银行端将新建数字货币核心系统、认证系统和数字货币钱包	12
4.3. 流通端短期变化在 ToC 端，长期来看 ToB 端可能出现现象级应用	13
4.3.1. 支付机具需支持数字货币交易，替换空间广阔	13
4.3.2. 三方支付商预计将加速转型，服务能力强的头部参与者优势更大	14
4.3.3. 数字货币连通资金流交易流，ToB 有望产生现象级平台应用	15
5. 投资建议	15
6. 风险提示	16

图表目录

图 1：数字货币体系系统简览	6
图 2：数字货币产业链关键建设/改造点一览	7
图 3：数字货币的发行流程	8
图 4：终端设备间的数字货币支付	8
图 5：由商业银行数字货币系统作为中介的数字货币支付	9
图 6：数字货币存款流程	9
图 7：此前央行构思的“一币两库三中心”原型架构	10
图 8：双离线支付的交易流程	11
图 9：ECC（SM2 的基础理论）与 RSA 密钥长度对比	11
图 10：ECC（SM2 的基础理论）和 RSA 的服务器响应时间对比	11
图 11：商业银行数字货币核心系统对应约 120 亿元市场空间	12
图 12：商业银行数字货币验证系统对应约 60 亿元市场空间	13
图 13：我国联网 POS 机具和联网商户数量情况	13
图 14：智能 POS 市场迅速增长	13

图 15: 三方支付体系的连接结构	14
图 16: 三方支付的服务流程.....	14
图 17: 通过智能合约实现条件支付的流程.....	15
图 18: 供应链金融预付款模式.....	15
图 19: 数字货币支付合约实现扶贫资金定向使用	15
表 1: 各国对数字货币的态度与进程.....	4

前言

此前一篇报告我们针对中国央行数字货币（DCEP）的基础特征和定位做了简单的介绍，本篇是我们数字货币与区块链系列的第二篇，我们尝试把数字货币放进近期以来逐渐明确的**依靠前沿科技提升治理能力与社会效率的主线**来看，从数字货币分发到流通的程序，梳理出产业链内的变化环节，并对市场关心的问题做一些解答。

1. 货币数字化的意义在于从体系上支持社会效率提升

1.1. 数字货币短期意义在于改进支付，但长期可能带来体系改变

短期来看，DCEP 聚焦于小额高频支付，主要意义在于改进当前支付体系中实体货币流通中的问题：

- **降低实体货币发行与流通过程中的高成本**：实体货币的流通过程中，存在着污损、伪造等问题，同时印刷铸造实体货币的过程本身也有成本，数字货币可以很好地避免这些成本；
- **增强对货币交易过程中信息的把握**：实体货币的交易是完全匿名的，监管无法追踪交易的情况；数字货币在保证一定程度的匿名性的基础上，可以通过大数据手段实现可控匿名，**满足 KYC 和 AMI 需求**。另外，数字货币的交易情况在线，央行可以宏观地获取社会交易的全局情况，**对经济情况的把握更为到位**。

长期来看，数字货币造成的体系性改变更加值得关注：

- **丰富货币政策工具**：传统货币体系中，实体货币不付息，利率为零，导致央行实际上无法实行负利率政策；**而数字货币可通过收取保管费的方式实现实质上的负利率**，虽然在可预见的未来内我们不认为央行会使用这样的手段，但对货币政策工具箱有所补充。
- **有望为增强人民币国际化打下基础**：当前国际贸易中通行的跨境清算系统以 SWIFT 和 CHIPS 为主，在我国 CIPS 上线前，人民币的跨境清算也高度依赖这两个系统。数字货币能够大大降低跨境汇款与清算的成本与时间，同时有望改进兑换自由性，为人民币国际化提供必要基础。
- **增强民生领域资金流转效率和并降低信用风险**：在民生领域，数字货币将大有可为。以保理行业为例，保理商需要对接买卖双方多个账户，同时存在票据转让后归属不明确导致付款对象错误等问题，数字货币可以简化管理，同时可以通过智能合约等手段将资金流与信息流结合起来，增强资金流转效率。另外以精准扶贫领域为例，数字货币可以通过发行端设置的方式实现提前指定资金用途，可以减少扶贫款项流通过程中的挪用问题。

1.2. 国际社会开始关注，我国有望成为首个发行法定数字货币的主要经济体

随着区块链和数字货币技术的发展，各国官方对本国的法定数字货币也纷纷进行了研究或表态。目前已有包括厄瓜多尔、委内瑞拉等国在内的数个国家正式发行了本国的法定数字货币；同时有一些国家正在进行相关的技术储备和研究，如新加坡、瑞典等；但也有部分国家明确表示了反对意见，如韩国、澳大利亚等。

表 1：各国对数字货币的态度与进程

国家	年份	状态	要点
厄瓜多尔	2015	已发行	2015 年 2 月开始使用，是世界上第一个国有电子货币系统。 目的：去美元化
突尼斯	2015	已发行	由政府及央行背书的基于区块链技术的数字货币。 目的：推动国内金融制度改革

塞内加尔	2016	已发行	基于区块链技术，享有与塞内加尔官方货币非洲法郎同等的法律地位。 目的：金融普惠
乌拉圭	2017	已发行	乌拉圭中央银行(BCU)于 2017 年 11 月 3 日正式推出了其开创性的乌拉圭比索数字化。银行的负责人指出它“不是比特币之类的加密货币”，而是“一种仍由 BCU 负责的货币”。 目的：钞票的印刷、分销、运输和交易的不透明带来了高昂费用
马绍尔群岛	2018	已发行	2018 年 2 月，马绍尔群岛议会通过立法正式宣布马绍尔群岛通过 ICO 的方式，发行新的国家数字货币 SOV。 目的：取代美元的货币流通体系，实现国家经济独立地位
委内瑞拉	2018	已发行	2018 年 2 月 20 日，委内瑞拉正式开始“石油币”的预售。委内瑞拉政府透露，他们发行的石油币将受到巨额石油、天然气、黄金和钻石的支撑。 原因：国家陷入恶性通货膨胀，原有的法定货币体系崩溃
新加坡	2016	计划推出	新加坡金融管理局主导启动了名叫 project ubin 的国家级项目，在项目的最后阶段是发行央行的数字货币。
瑞典	2017	计划推出	瑞典央行就央行数字货币开始了“e-Krona（电子克朗）”项目，计划将其作为现金的补充，将其用于消费者，公司和政府机构之间的小额交易。 目的：作为现金的补充，减少国民对于私人支付系统的依赖，防止危机时期私人支付系统产生故障。
俄罗斯	2017	计划推出	2017 年 10 月 16 日，俄罗斯总统普京（Vladimir Putin）正式宣布，俄罗斯将在莫斯科举行的闭门会议上发布官方数字货币“加密卢布” CryptoRuble。CryptoRuble 不能由挖矿而得，只能由管理当局发放、管理和维护。 目的：在金砖国家内部，加密货币可以取代成员国之间使用的美元和其他货币
泰国	2018	计划推出	2018 年 8 月 21 日，泰国中央银行(BOT)对外宣布了名为 Inthanon 的中央银行数字货币(CBDC)项目 目的：让银行间的交易能因为中介过程更少，加速交易速度并降低成本
荷属库拉索岛和圣马丁岛中央银行	2018	计划推出	2018 年 8 月 14 日位于巴巴多斯的金融科技初创公司 Bitt 公司与库拉索和荷属圣马丁中央银行签署谅解备忘录，双方将会开发中央银行数字货币来促进金融支付
乌克兰	2019	计划推出	2019 年 2 月 25 日，乌克兰央行已经完成了本国数字货币“e-hryvnia”的试点计划。
立陶宛	2019	计划推出	立陶宛央行 2019 年将发行数字货币。“LBCOIN”，基于区块链技术。它不是一种加密货币，而是一种数字货币。这是一枚纪念币，发行数量有限。 目的：旨在测试加密货币和分布式账本技术
巴哈马	2019	计划推出	巴哈马央行于 2019 年 5 月 30 日就开发法定数字系统达成正式协议，计划将于 2020 年全面采用数字货币
东加勒比中央银行	2019	计划推出	东加勒比中央银行（ECCB）即将对基于区块链的央行数字货币（CBDC）进行试点，并计划在 2020 年全面推出该货币。 目的：将国内流通现金减少 50%，并为金融部门带来更多稳定性，促进 ECCU 成员国的发展
加拿大		研究中	加拿大和新加坡已首次完成数字货币跨境支付试验，但未表示要推出加拿大数字货币
巴西		研究中	巴西央行认为数字货币不是货币，而是一种“加密资产”和一种风险
英国		研究中	英格兰银行正在投资区块链技术，并正在调查其他央行在这一领域进一步的用途
丹麦		研究中	尚不清楚哪种央行数字货币能够提供目前支付解决方案尚未涵盖的资金
以色列		研究中	以色列无意成为首个发行国家数字货币的发达国家
德国		暂不考虑	原因：德国央行行长表示，数字中央银行资金的广泛使用可能会产生严重后果。在没有经过深思熟虑的情况下，不应引入数字中央银行
日本		暂不考虑	原因：还在研究数字货币对货币体系的作用

韩国	明确反对	原因：担心央行数字货币可能会破坏经济稳定
澳大利亚	明确反对	原因：认为加密货币仍存在“结构性缺陷”，从而限制了其发展潜力，在可扩展性和治理方面远远落后于 Visa 等传统支付方式
新西兰	明确反对	原因：其现有的可扩展性限制和长时间的交易确认流程，中央银行发行加密货币在金融业务上并不稳定

资料来源：IMF，《中国央行数字货币解析》零壹财经，《数字货币初探》，天风证券研究所

发展中国家出于弯道超车的想法对数字货币应用的态度较为积极，发达国家态度普遍较为谨慎。发展中国家法币地位普遍较低，甚至导致国内经济出现问题，更希望通过法定数字货币的发行改革金融制度，改善国内经济；而发达国家出于技术不成熟和维持经济稳定的考量，对法定数字货币的发行普遍持谨慎态度。

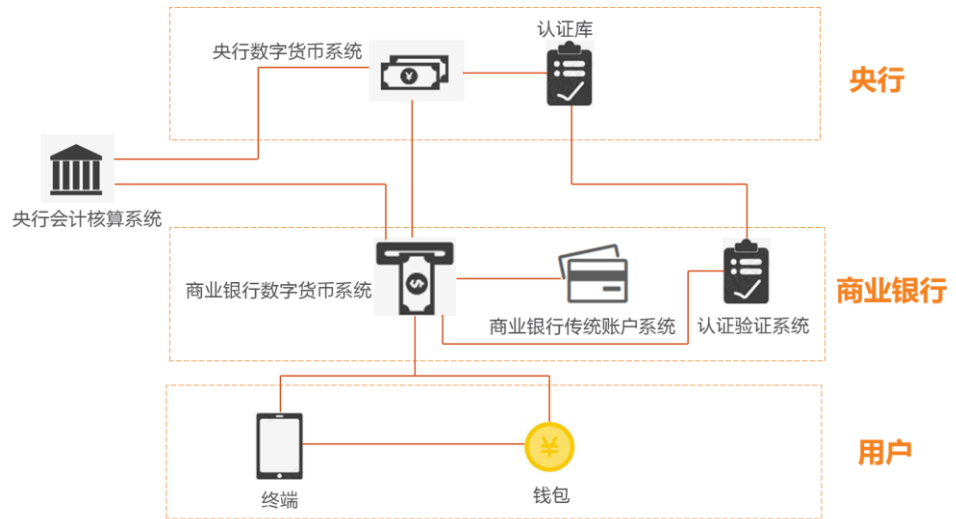
货币数字化是未来强势货币的基础设施但不是万能妙药，主要经济体研究任重道远，我国有望成为首个发行数字法币的主流经济体。部分发展中国家发行的数字货币缺少足够的政府信用为其背书，加之数字化移动终端设备的不普及，导致民众对其的使用率很低，因此目前已发行的数字货币并没有收到很好的效果。如厄瓜多尔政府于 2015 年发行的厄瓜多尔币，由于在运行后的一年时间，其流通量只占整个经济体的万分之零点三不到，其已于 2018 年 4 月份宣告停止运行。主要经济体也逐步开始研究，如路透社报道欧洲央行也开始进行数字货币的可行性研究，但该项目也面临长期挑战。我国凭借着良好的货币信用和支付体系，有望成为首个发行数字法币的主流经济体。

2. 数字货币将在央行、商业银行、用户三个层面产生改变

基于双层投放结构，数字货币参与方主要可分为央行、商业银行、用户三类。在双层投放结构下，商业银行向央行存放 100% 备付金，获得央行发行的数字货币。用户端可通过实体现金或银行账户中的现金资产兑换等额的数字货币，并通过数字货币进行交易。根据壹零财经依据专利信息进行的分析，数字货币体系将主要由央行数字货币系统、认证系统、商业数字货币系统和客户端组成。结合此前“一币两库三中心”的构想，我们在引用基础上有小幅增补。我们认为该系统在当前可知公开信息上是较为合理的推断，不排除此后系统正式发布时有变动，主要系统组成部分如下：

- **央行端：央行数字货币系统和认证库。**央行数字货币系统主要处理数字货币的发行、回笼、属权变更等操作，以及对数字货币整体运行的分析，可视作系统的中心节点。认证系统主要承担数字货币本体以及交易请求的加密和解密工作；
- **投放端：**投放端预计主要是大型商业银行和大型第三方机构，我们以商业银行举例。投放端主要承担用户请求受理和数字货币/现有账户体系互换的职责，主要系统包括新建的**商业银行数字货币系统、认证系统和改造的传统账户系统。**
- **用户端：**用户端身份多样，但整体可归为**终端（硬件）和钱包（软件地址）**，分别主要用于交易过程中的交互和数字货币的“储存”。

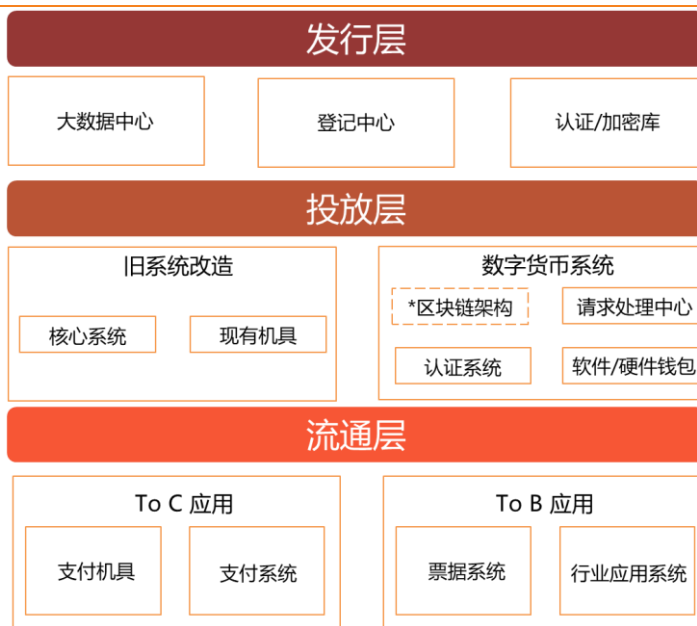
图 1：数字货币体系系统简览



资料来源：《中国央行数字货币解析》零壹财经，《中央银行数字货币原型系统实验研究》，天风证券研究所（有改动）

市场空间预计依发行层->投放层->流通层递进。依据梳理系统建设，我们对系统中关键的建设/改造点进行了梳理。整体来看，发行层系统预计将以央行自建/合作开发为主，社会企业参与度预计不高，但认证系统有望成为企业参与的重点；投放层系统预计属于有条件招标，现有金融科技供应商和拥有成熟方案的技术商有望参与；流通层系统建设空间较大，其中 ToC 板块的支付机具、支付系统市场化程度相对较高，ToB 层面预计短期以项目型开发为主，中长期有望产生平台型公司。

图 2：数字货币产业链关键建设/改造点一览



资料来源：《中央银行数字货币原型系统实验研究》，《中国央行数字货币解析》零壹财经，天风证券研究所绘制

*代表非必要建设

3. 功能梳理：央行端承担主要归属结算职责

本段主要介绍几种数字货币常用功能，帮助理解数字货币的技术环节。通过对几项常用功能的梳理，可以看出央行端承担着主要结算职责。

3.1. 数字货币的发行

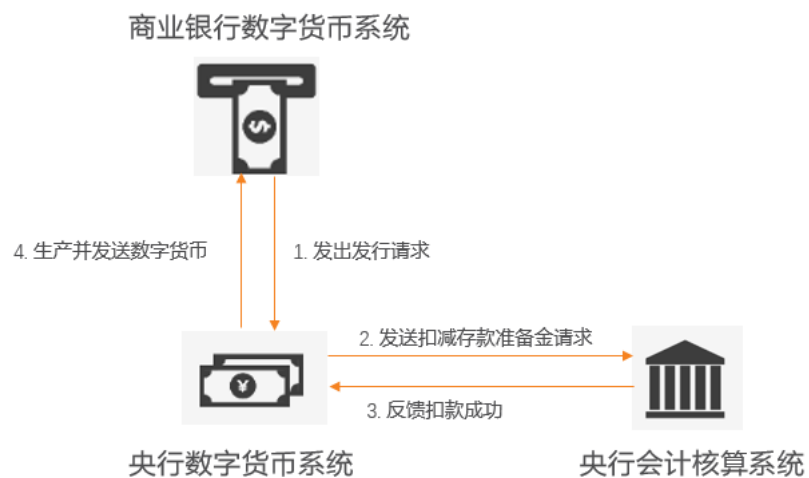
根据央行数字货币研究所的专利信息和中国银行支付结算司副司长穆长春的解读，法定数

数字货币的发行采用的是双层运营体系，由人民银行先把数字货币兑换给银行或其他运营机构，再由这些机构兑换给公众。为保证数字货币不超发，商业银行需要向央行全额缴纳 100% 的准备金，保证央行数字货币是中央银行负债，由中央银行信用担保，具有无限法偿性。

具体的发行流程为：

1. 首先由中央银行数字货币系统接收商业银行数字货币系统的数字货币发行请求；
2. 之后由认证系统对数字货币发行请求进行业务核查，核查通过后向会计核算系统发送扣减存款准备金的操作；
3. 会计核算系统进行扣减存款准备金操作，并向央行数字货币系统进行反馈；
4. 接收到会计核算系统发送的扣款成功的应答后，中央银行数字货币系统通过公钥加密产生数字货币，并将数字货币字符串发送到发出申请的商业银行数字货币系统。

图 3：数字货币的发行流程



资料来源：《中国央行数字货币解析》零壹财经，天风证券研究所

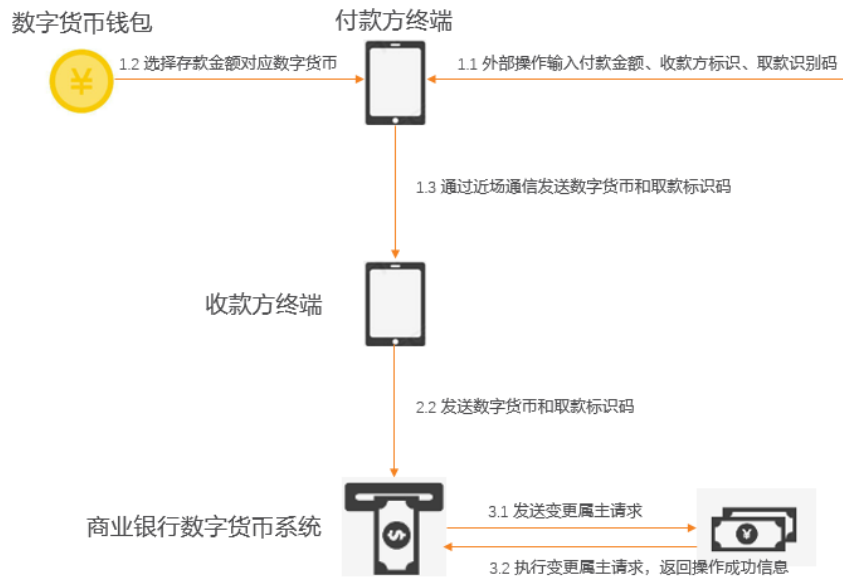
3.2. 数字货币的支付流程

央行数字货币的支付流程需要通过用户、商业银行和中央银行三个层面完成。其基本流程为：

1. 首先付款用户的终端设备接收付款指令，从付款方的数字钱包中提取金额等于付款金额的数字货币；
2. 之后付款方或收款方终端将数字货币和收款方地址/标识发送给商业银行数字货币系统；
3. 最后商业银行数字货币系统将接收到的相关信息发送给中央银行数字货币系统，由中央银行完成对数字货币属主变更的操作，并根据场景决定是否将数字货币发送给收款方。

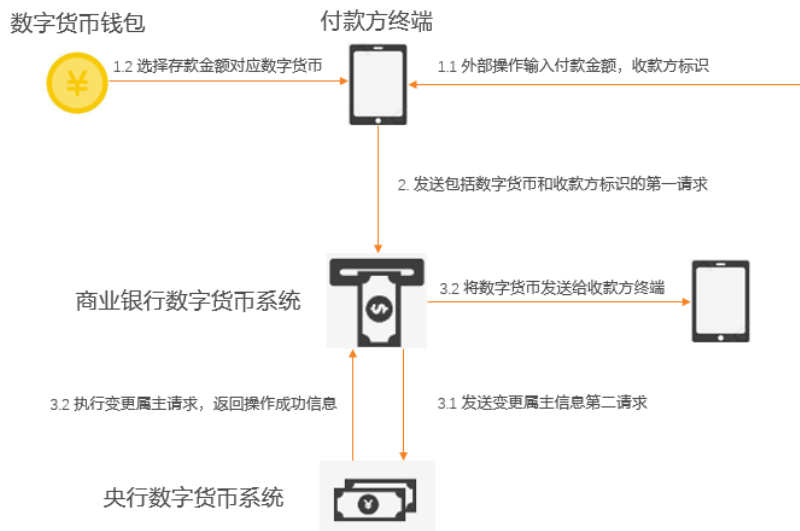
根据操作方式的不同，可分为终端设备间的支付和由商业银行数字货币系统作为中介的支付。这两种方式的主要区别是数字货币是否在收付款方之间进行直接转移。对终端设备间的支付，数字货币可通过近场通信的方式直接发送给付款方，中央银行数字货币系统仅完成属主信息的更改；而由商业银行数字货币系统作为中介的支付中，收付款方的终端设备无法直接产生交互，数字货币先由付款方终端生成第一请求，将数字货币与收款方标识一起发送给商业银行，再经商业银行生成变更属主信息的第二请求发送给中央银行，由中央银行完成属主信息的变更后发送给收款方。

图 4：终端设备间的数字货币支付



资料来源：《中国央行数字货币解析》零壹财经，天风证券研究所

图 5：由商业银行数字货币系统作为中介的数字货币支付



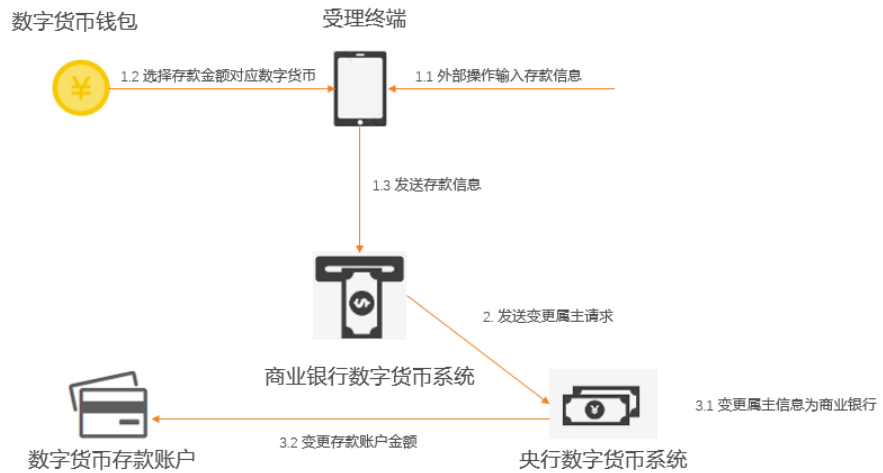
资料来源：《中国央行数字货币解析》零壹财经，天风证券研究所

3.3. 数字货币的存款流程

央行数字货币的存款流程与其支付过程类似，只是最终数字货币的去向变为与数字货币存款账户对应的商业银行。其基本流程为：

1. 受理终端设备接收外部操作输入的存款信息，并将存款信息发送至商业银行数字货币系统，存款信息包括存款账户信息、数字钱包（数字货币芯片卡）信息以及与存款金额等值的数字货币；
2. 商业银行数字货币系统在接收到存款信息后，向中央银行数字货币系统发送变更属主的请求；
3. 最后中央银行数字货币系统在接收到请求后，将数字货币的属主变更为商业银行，并对存款账户的金额进行变更。

图 6：数字货币存款流程



资料来源：《中国央行数字货币解析》零壹财经，天风证券研究所

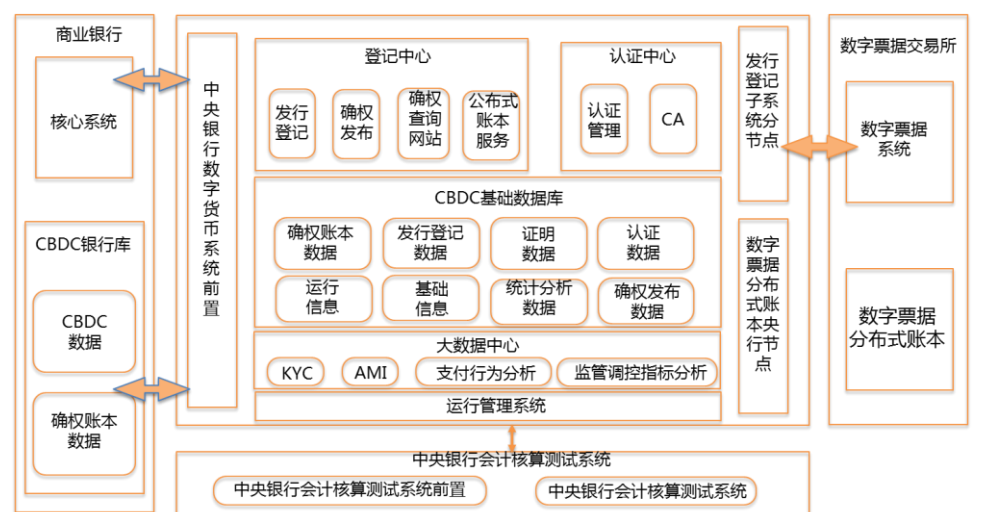
4. 产业链建设情况梳理

4.1. 发行端系统中，认证系统将是建设的关键

4.1.1. 若央行采取偏中心化运营的方式，对央行数字货币系统性能要求较高

央行数字货币系统主要包括登记中心、大数据中心和认证中心。登记中心主要记录已发行数字货币的归属情况；大数据中心负责在分析支付行为，在特定条件下做到 KYC 和 AMI；认证中心负责储存系统中的密钥对，做到对数字货币和参与方的认证。

图 7：此前央行构思的“一币两库三中心”原型架构



资料来源：《中央银行数字货币原型系统实验研究》，天风证券研究所

根据目前的专利信息，数字货币发行和确权登记均在央行系统完成，系统要求高并发、大容量、强灾备、快速处理，预计以自研自建或合作开发为主。前文所述，发行端系统主要是央行数字货币系统和认证系统。其央行数字货币系统主要是登记中心和大数据中心，主要对数字货币进行签发、回笼和确权变更的操作和使用数据的分析。由于实质上要处理全网的数字货币交易，对于系统的高带宽、高并发、大容量、强灾备、快速处理等能力均提出了较高的挑战，但预计整体系统将以自研自建或合作开发为主，针对社会层面将仅有有限开放招标。

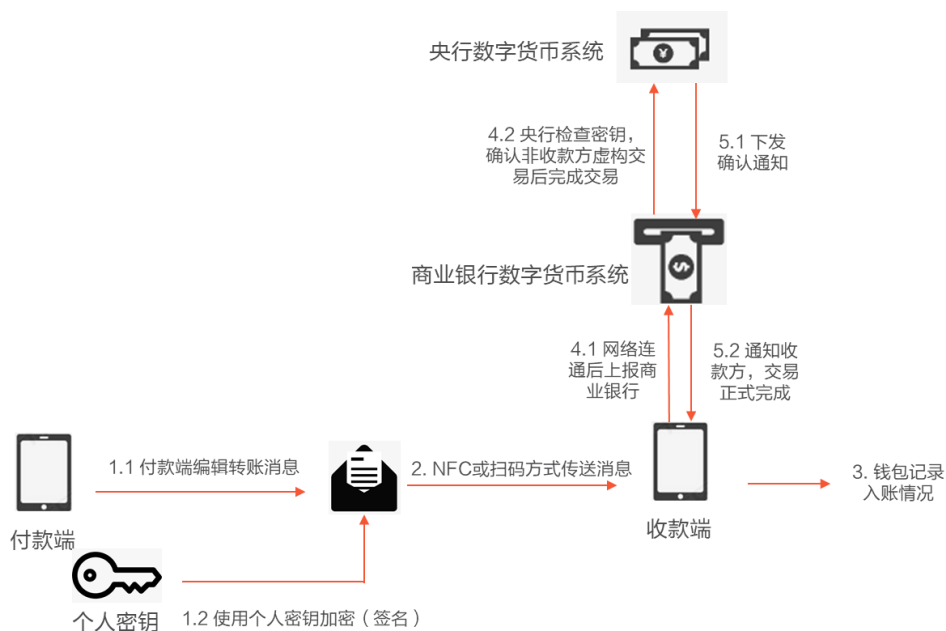
4.1.2. 认证体系是数字货币系统的关键基础设施建设，决定体系安全性

数字货币的本质是加密字符串，认证和密码体系是关键基础设施。数字货币的本质是央行以一定规则加密的字符串，在使用货币的过程中各方也需要不断地对指令进行加密与解密，所以认证和密码体系会覆盖数字货币的全流程，是数字货币系统最关键的基础设施之一。为了管理密钥对，预计央行系统内将会建设认证中心。

加密认证体系也是实现双离线支付的关键技术。在传统银行账户支付体系中，POS 机将借记卡/信用卡信息、交易金额、密码等数据加密后传送至网联/银联，银联重新组织报文并发送给相应的银行，由银行处理后将信息传回网联再传回 POS 机，交易需全程在线。数字货币需支持双离线支付，在没有网络的情况下，付款方无法将请求上传，而如果由收款方上报，则需要避免收款方虚构交易的情况。加密体系使得双离线支付成为了可能，在数字货币体系中：

1. 付款方编辑金额+收款方地址的信息，利用自己的私钥进行签名；
2. 付款方将加密过的交易信息通过 NFC 传送或生成二维码供收款方接收；
3. 收款方获取交易信息，解密并验证金额是否正确，此时交易已经完成；
4. 收款方连线后，将交易信息按正常流程上报给商业银行和央行，由于交易中付款方已经使用私钥进行过签名，杜绝了收款方虚构交易的可能性。央行解密验证后将执行转账交易；
5. 收款方与付款方收取商业银行转来的央行交易成功的确认，交易正式成功。

图 8：双离线支付的交易流程



资料来源：天眼查，天风证券研究所绘制

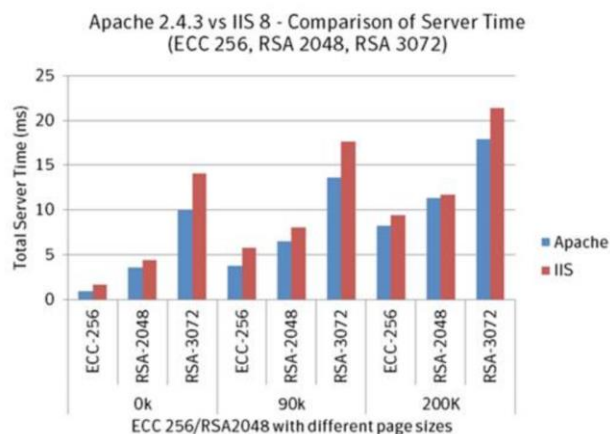
密码性能决定系统效率和安全性，国产密码性能水平已不输国外对手。密码的性能主要表现在抗攻击性、内容使用、CPU 占用、网络消耗、加密速度等。以我国自主设计的 SM2 算法和被广泛使用的 RSA 为例。SM2 是我国自主研发的基于 ECC 椭圆曲线密码理论的公钥密码算法。在安全性能上，基于 ECC 的 SM2 证书普遍采用 256 位密钥长度，加密强度等同于 3072 位 RSA 证书，远高于业界普遍采用的 2048 位 RSA 证书，同时增长速度较慢；在算法速度上，ECC 算法 Web 服务器响应时间比 RSA 算法快十几倍。

图 9：ECC (SM2 的基础理论) 与 RSA 密钥长度对比

图 10：ECC (SM2 的基础理论) 和 RSA 的服务器响应时间对比

对称密钥长度 (bit)	RSA密钥长度 (bit)	ECC密钥长度 (bit)	保密年限
80	1024	160	2010
112	2048	224	2030
128	3072	256	2040
192	7680	384	2080
256	15360	512	2120

资料来源：沃通官网，天风证券研究所



资料来源：沃通官网，天风证券研究所

密码法落地在即，预计央行将选用国产密码支撑数字货币体系。2019年10月26日，《中华人民共和国密码法》获人大常委会表决通过，将在2020年1月1日起实施。《密码法》中明确规定，要加强密码工作机构建设，保障其履行工作职责，同时要建立和完善商用密码体系。同时，也基于数字货币体系的自主可控考虑，预计央行将会选用国产密码算法作为数字货币的底层架构。

4.2. 预计商业银行系统将是民资主要参与的基础设施部分

4.2.1. 商业银行传统账户需对接数字货币系统，传统机具或有小幅改造空间

商业银行承担数字货币投放职责，同样属于基础设施。商业银行承担着央行与用户的连接任务，用户绝大多数的指令需要经过商业银行的转达提交给央行。我们认为，商业银行需要对用户的请求进行预处理，只选取有效请求传达给央行，以降低央行端的系统负载。所以，商业银行的系统将迎来大量新建与改造需求，以满足数字货币体系的运行。

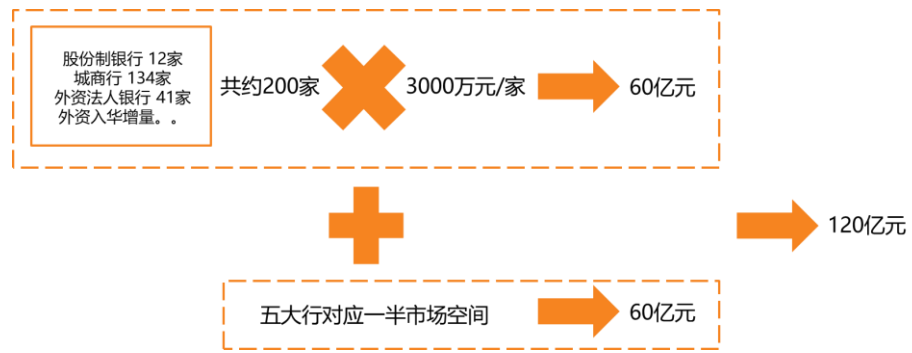
银行传统系统中，网点和账户系统须与数字货币系统对接，传统机具或也有小幅改造升级需求。银行网点和用户账户的远程访问是当前用户管理现金资产的两大入口，未来用户要使用数字货币，需先从现金资产兑换成数字货币，银行需要对当前的网点系统和账户系统做改造，对接数字货币系统。传统机具方面，由于数字货币研究所还曾注册过基于芯片卡的数字货币系统专利，ATM机等传统机具可能有少部分要进行改造，以适应芯片卡操作的需求。

4.2.2. 预计银行端将新建数字货币核心系统、认证系统和数字货币钱包

预计数字货币核心系统和认证系统建设规模较大，市场空间预计在180亿左右，具有较强技术能力的厂家有望在验证后参与建设。投放层中，我们预计用户的数字货币钱包会绑定在申请开户的商业银行上，对应的商业银行也就承担着链接全网用户交易请求与央行处理情况的职责，对系统压力较大。同时商业银行也要承担对用户指令初步验证的职责，确认指令合法后才上报央行，以降低央行系统负载，带来认证解密系统的建设需求。商业银行层面，预计民营厂商将存在市场机会，在通过选型验证后，有望进入两大重点系统建设工程。

核心系统层面，假设数字货币稳定使用后，全国规模性银行均需支持数字货币。目前全国股份制银行+城商行接近150家，加上现有外资法人银行以及此后外资入华过程中可能扩充的部分，假设共200家左右。假设每家建设规模在3000万元，对应市场空间60亿元。参考目前银行核心系统的建设规模，五大行基本占到行业的一半，对应五大行空间60亿元，共计约120亿元。

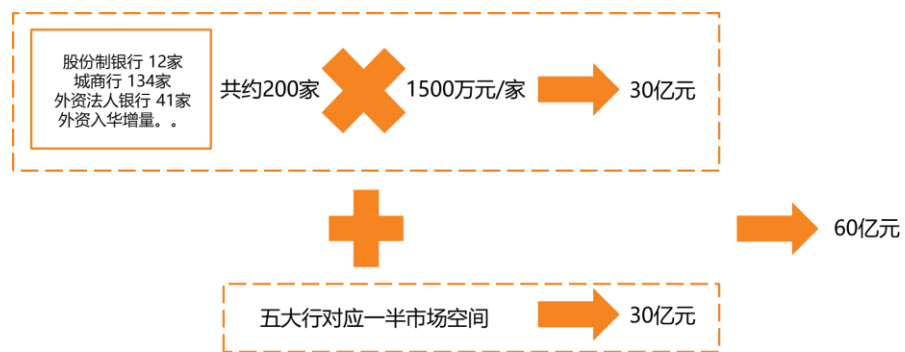
图 11：商业银行数字货币核心系统对应约 120 亿元市场空间



资料来源：银保监会，采招网，天风证券研究所绘制

认证系统层面，假设单家建设金额在 1500 万元，同样假设五大行对应一半市场空间，市场空间对应 60 亿元左右。

图 12：商业银行数字货币验证系统对应约 60 亿元市场空间



资料来源：银保监会，采招网，天风证券研究所绘制

预计数字货币钱包将采取绑定管理，商业银行系统建设规模约 4 亿元。我们预计，数字货币钱包虽属于个人，但开通数字货币钱包的操作仍需通过投放层机构完成，同时钱包开通后的进行的操作也更可能挂靠在开通钱包的商业银行的通道上上报。商业银行需建设数字货币钱包系统，假设每家建设规模约 200 万元，建设银行家数在约 200 家，对应约 4 亿元市场空间。

4.3. 流通端短期变化在 ToC 端，长期来看 ToB 端可能出现现象级应用

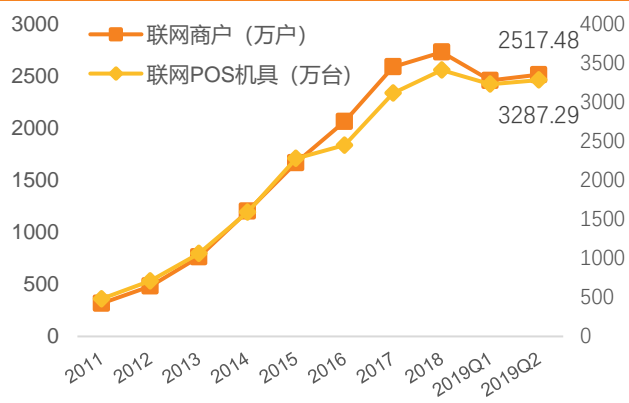
4.3.1. 支付机具需支持数字货币交易，替换空间广阔

数字货币时代，支付机具整体需求预计变动不大。数字货币使用过程中，用户间点对点支付将会变得更加便捷，但我们认为支付机具需求不会受到太大冲击。类比当前电子支付情景，微信/支付宝钱包同样以小额高频支付为主，支持用户间点对点扫码转账，便捷程度较高同时不产生手续费；但由于餐饮、商场等场景中，有一对多收款需求和银行卡/电子钱包聚合收款的需求，支付机具仍然是大多数商家的标配，预计数字货币时代变动不大。

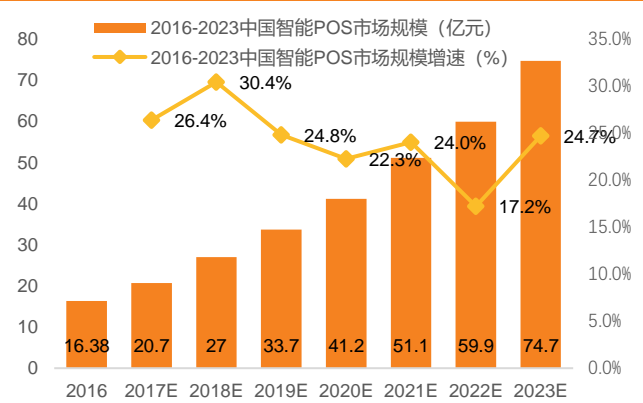
支付机具总规模整体稳定增长，叠加智能化替换浪潮，整体换机市场规模最高可达 200-300 亿元。我国 POS 机和联网商户自 2011 年至 2017 年处于快速增长期，2018 至 2019 年一季度，在监管压力下增速有所放缓乃至出现下滑，2019 二季度已重回小幅增长区间，POS 机总量和联网商户数分别达 3287 万台和 2517 万户。同时，POS 机智能化趋势较为明显，预计若 POS 机因数字货币导致换代，智能 POS 机将逐步占据主流。智能 POS 机价格约在 800-1000 元/台，按 POS 机总量全体换代，规模最高可达 329 亿元；按 800 元/台算，假设联网商户每户一台新机，对应规模也有 201 亿元。

图 13：我国联网 POS 机具和联网商户数量情况

图 14：智能 POS 市场迅速增长



资料来源：支付清算协会，天风证券研究所

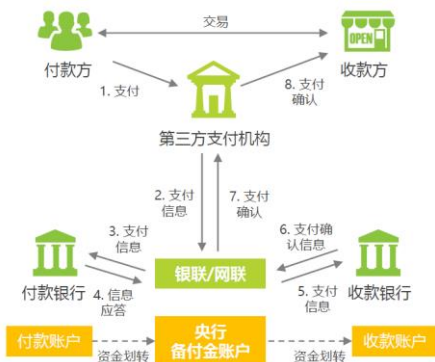


资料来源：中国产业信息网，天风证券研究所

4.3.2. 三方支付商预计将加速转型，服务能力强的头部参与者优势更大

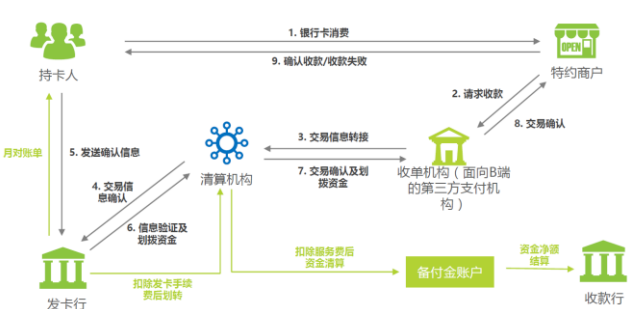
三方支付本质上是商业银行的渠道延伸，数字货币或对三方支付体系中小额高频交易的部分产生竞争，但预计对大额支付影响较小。我们认为，在央行出台“备付金全额上缴”政策后，三方支付行业已明确其为支付体系中商业银行的渠道延伸，从其盈利模式中也可可见一斑。“96 费改”后，行业收费分成模式规定为“721”，即发卡行、银联、三方支付按 7:2:1 的比例进行手续费分成。本质上，商业银行难以将其收单渠道下放是三方支付行业产生的客观原因。数字货币主要应用在小额高频支付场景内，我们认为对于三方支付中同属小额高频的部分将会产生挤压效应，但对支付体系中大额支付的部分影响较小。

图 15：三方支付体系的连接结构



资料来源：艾瑞咨询，天风证券研究所

图 16：三方支付的服务流程



资料来源：艾瑞咨询，天风证券研究所

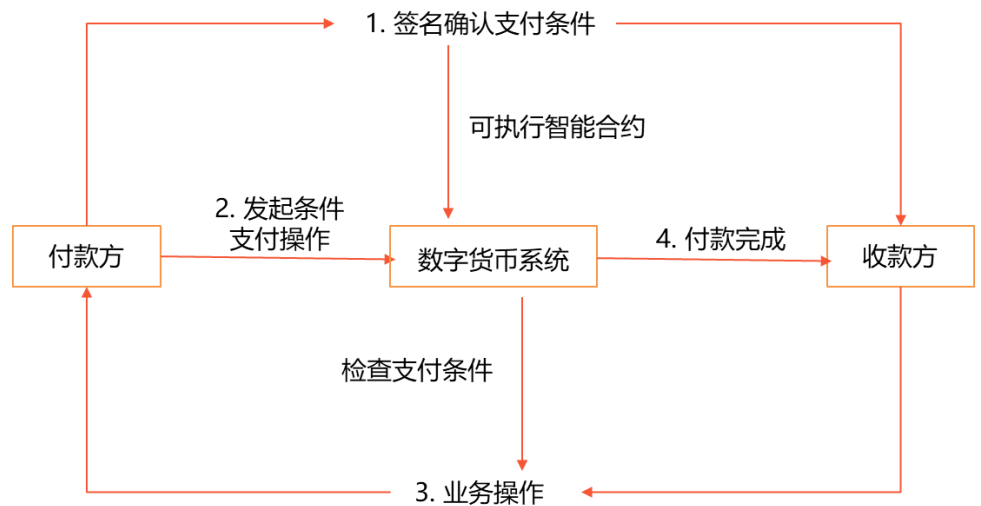
数字货币支付体系中第三方支付运营商角色仍十分必要。我们认为，商业银行在数字货币支付中由于没有类似账户支付体系中天然具备的手续费率，将不会大举投入数字货币支付的细分服务领域。但是在第三方支付运营商的培养下，支付体系中的服务对于商户和用户正变得越来越重要，ToB 端服务种类从最初的记账管理逐步扩展到包括客户运营、卡券核销、库存管理、金融服务等在内的服务体系；C 端的钱包也有包括生活助手、卡券管理等需求。同时，商户正常运营中一对多收款的基本需求也要得到满足，我们认为数字货币支付体系中第三方支付运营商的角色不会消失。

支付服务运营商需加速转型，行业有望向头部集中，中长期分成比例或有实质提升，商业模式静待行业演绎。在没有天然手续费收入的情况下，第三方支付服务运营商需加速向服务商角色转变。当前行业内长尾收单机构服务能力较弱，我们预计行业有望更进一步向服务能力更强的头部机构集中。另外，虽然商户端收取的整体费率可能降低，但由于三方支付服务商不需再跟银联、商业银行分成，服务商部分的费率或有上升。正如三方支付体系经历了多年发展才沉淀成当今的成熟体系，我们认为数字货币三方支付体系建立的初期也会经历行业模式的持续进化，静待产业发展达成均衡状态。

4.3.3. 数字货币连通资金流交易流，ToB 有望产生现象级平台应用

数字货币应用上最重要的能力之一是打通资金流和交易流。在当今的交易平台中，往往能够在交易流、信息流层面对买卖双方进行打通，但涉及到资金的部分往往要涉及到由可信第三方进行处理，对第三方产生信用依赖，同时资金流和交易流处于脱节状态。数字货币结合智能合约能够做到有条件支付，由交易节点触发资金流动，真正将资金流与交易流打通。

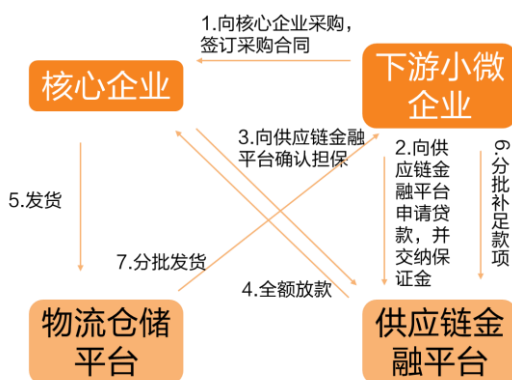
图 17：通过智能合约实现条件支付的流程



资料来源：《数字货币初探》，天风证券研究所

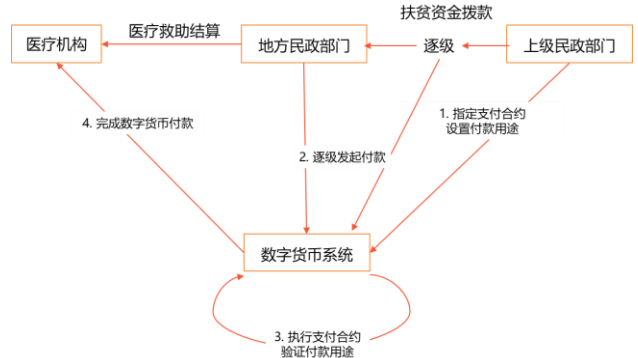
ToB 端有望产生现象级平台应用，提升当前行业运行效率。基于资金流与信息流结合，许多现有行业平台将迎来效率与服务质量改善机会。如供应链金融平台，结合物联网可实现物权融资自动化操作，买家提货的同时资金自动到账。如扶贫基金拨款过程中，专项资金是否专用难以验证，结合智能合约可实现专款专用。ToB 应用发掘或仍需时间，但受益于数字货币带来的效率大幅提升，特定领域有望产生现象级平台应用。

图 18：供应链金融预付款模式



资料来源：帝隆科技官网，天风证券研究所绘制

图 19：数字货币支付合约实现扶贫资金定向使用



资料来源：《数字货币初探》，天风证券研究所

5. 投资建议

我们认为，央行层面建设规模较小，且预计以自研自建为主，企业参与机会不大，也可关注数据库、中间件、网络安全等基础设施行业的机会。

投放层面，传统系统改造与新系统建设，重点推荐长亮科技，建议关注润和软件、信雅达等；认证系统，重点推荐格尔软件、数字认证；银行机具改造，建议关注广电运通、聚龙股份等。

流通层面，支付机具重点推荐新大陆，建议关注新国都；支付体系建议关注新大陆、拉卡拉（传媒覆盖）、新国都；ToB 应用的成长期预计在数字货币稳定运行之后，当前时点建议关注有强运营能力的行业平台，如恒生电子、上海钢联、远光软件、航天信息、信息发展等。

6. 风险提示

1. 央行尚未正式发布数字货币系统：央行尚未正式发布，本报告基于现有公开数据进行合理推测，与未来正式发布情况或有出入；
2. 数字货币落地进展不及预期：数字货币推出时间或晚于预期，系统建设进度均需要顺延；
3. 数字货币系统建设规模不及预期：数字货币系统建设规模或低于现有的预期，同时某些系统改造规模可能不及预期。

分析师声明

本报告署名分析师在此声明：我们具有中国证券业协会授予的证券投资咨询执业资格或相当的专业胜任能力，本报告所表述的所有观点均准确地反映了我们对标的证券和发行人的个人看法。我们所得报酬的任何部分不曾与，不与，也将不会与本报告中的具体投资建议或观点有直接或间接联系。

一般声明

除非另有规定，本报告中的所有材料版权均属天风证券股份有限公司（已获中国证监会许可的证券投资咨询业务资格）及其附属机构（以下统称“天风证券”）。未经天风证券事先书面授权，不得以任何方式修改、发送或者复制本报告及其所包含的材料、内容。所有本报告中使用的商标、服务标识及标记均为天风证券的商标、服务标识及标记。

本报告是机密的，仅供我们的客户使用，天风证券不因收件人收到本报告而视其为天风证券的客户。本报告中的信息均来源于我们认为可靠的已公开资料，但天风证券对这些信息的准确性及完整性不作任何保证。本报告中的信息、意见等均仅供客户参考，不构成所述证券买卖的出价或征价邀请或要约。该等信息、意见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任何人的个人推荐。客户应当对本报告中的信息和意见进行独立评估，并应同时考量各自的投资目的、财务状况和特定需求，必要时就法律、商业、财务、税收等方面咨询专家的意见。对依据或者使用本报告所造成的一切后果，天风证券及/或其关联人员均不承担任何法律责任。

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。过往的表现亦不应作为日后表现的预示和担保。在不同时期，天风证券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。

天风证券的销售人员、交易人员以及其他专业人士可能会依据不同假设和标准、采用不同的分析方法而口头或书面发表与本报告意见及建议不一致的市场评论和/或交易观点。天风证券没有将此意见及建议向报告所有接收者进行更新的义务。天风证券的资产管理部门、自营部门以及其他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。

特别声明

在法律许可的情况下，天风证券可能会持有本报告中提及公司所发行的证券并进行交易，也可能为这些公司提供或争取提供投资银行、财务顾问和金融产品等各种金融服务。因此，投资者应当考虑到天风证券及/或其相关人员可能存在影响本报告观点客观性的潜在利益冲突，投资者请勿将本报告视为投资或其他决定的唯一参考依据。

投资评级声明

类别	说明	评级	体系
股票投资评级	自报告日后的 6 个月内，相对同期沪深 300 指数的涨跌幅	买入	预期股价相对收益 20%以上
		增持	预期股价相对收益 10%-20%
		持有	预期股价相对收益 -10%-10%
		卖出	预期股价相对收益 -10%以下
行业投资评级	自报告日后的 6 个月内，相对同期沪深 300 指数的涨跌幅	强于大市	预期行业指数涨幅 5%以上
		中性	预期行业指数涨幅 -5%-5%
		弱于大市	预期行业指数涨幅 -5%以下

天风证券研究

北京	武汉	上海	深圳
北京市西城区佟麟阁路 36 号	湖北武汉市武昌区中南路 99	上海市浦东新区兰花路 333	深圳市福田区益田路 5033 号
邮编：100031	号保利广场 A 座 37 楼	号 333 世纪大厦 20 楼	平安金融中心 71 楼
邮箱：research@tfzq.com	邮编：430071	邮编：201204	邮编：518000
	电话：(8627)-87618889	电话：(8621)-68815388	电话：(86755)-23915663
	传真：(8627)-87618863	传真：(8621)-68812910	传真：(86755)-82571995
	邮箱：research@tfzq.com	邮箱：research@tfzq.com	邮箱：research@tfzq.com