点对点安全交易：区块链在金融领域的应用与不足

刘轩铭，3180106071

（浙江大学，计算机科学与技术学院，软件工程专业）

摘　要：区块链通过自身的技术手段实现了“去中心化”的监管机制，同时有着点对点的安全交易手段。金融是人类生活的重要组成部分，自然也是区块链的重要应用场景。区块链可以被广泛用于金融领域的交易记录和新型支付清算等场景，同时也对未来的经济价值共识有着重要作用。但是，区块链在金融领域也有着实时性差等不足。由于目前区块链“泡沫化”现象严重，相关的监管机制必须进一步完善，新型的区块链产业标准也应该早日制定出来。

关键词：区块链，金融领域，共识，点对点交易

近年来，随着“挖矿”的热潮席卷全球，“区块链”逐渐进入了大众视野。前日，中国人民银行宣布基于区块链技术的“数字货币”正式落地，标志着我国进一步融入“数字时代”，区块链技术再一次吸引了大众的目光。

区块链技术的核心特点是“去中心化”，有着安全的点对点通信和交易机制。正是由于这一特点，该技术被广泛地应用在了数字经济，金融科技等众多领域。本文将结合区块链的技术特点，讨论其对于金融领域发展的作用与影响，并尝试勾勒其在未来金融生活中的应用图景。

一、区块链与其背后的“去中心化”概念

区块链技术是一种较为形式新颖，但底层原理并不复杂的计算机科学技术。笔者首先以通俗化的方式介绍其基本原理，以及“去中心化”和“点对点”的核心概念，方便读者理解后文。

在现实生活中我们常常遇到“记账”的需要。如设想一个村镇，村民们每天在午时来到村口进行交易。为了确保交易的可信和公平，一个自然的想法是寻找一个大家都能信赖的“记账员”，由他负责记录“某日某时，甲村民以若干价钱向乙村民购买了某物品”这样的信息。我们进一步规定，当日的交易记录要被记在账本的一页上，每一天记录新的一页。那么“记账员”将持有一个公共的账本，账本上保存着长久以来的交易记录，使得每一笔交易和资金的流向都有迹可循。

但是问题很快会被发现：如果“记账员”有不诚实的行为，比如和某个村民勾结，篡改了账本；或者以某种手段欺骗了村民，给自己的账上添加了许多金额，那么会极大地损害交易机制的公平性，也会降低村民的团结性。

于是我们提出新的监督机制：不再需要“记账员”的加入，而是让每位村民都保存有一个相似的账本。每一次交易发生时，需要交易的村民可以在村口大喊出相关的交易信息。所有的村民都能听到这些并默默地拿出小账本记录下这些信息。从而“人人拥有账本”，篡改账本的行为不可能再发生。这是因为一旦有人篡改账本，其他人可以立即发现这样的行为。

对于最具有权威的那个公共账本而言，如果把账本中的每一页理解成一个区块，那么页与页连结便形成了“区块链”，由于这个账本是人人都能获取和监督的，故难以被修改。这便是区块链防止信息被篡改的基本手段。

在上述故事中的第一种交易方式，便是我们日常生活中常见的“中心化”管理。在目前的金融行业中，银行、公司、证券所和国家机器等机构监督与管辖着金融活动者的行为。这种方式在有关机构拥有绝对公信力，并且信息被绝对安全地保存的情况下效果显著，但问题也同样明显：我们无法保证管理机构的管理是绝对公平的，同时，我们也难以确保重要数据和信息的安全和可靠。相较而言，区块链技术采取了“去中心化”的方式：“人人有着一个账本”，信息变得可追溯且透明。

在每一笔交易发生时，交易的双方只需要与彼此完成交易，然后将自己的交易记录广播出去，之后其他的村民会进行交易的有效性验证，（如果有效）并进行记录——这样，一笔交易会被大家所检验和接纳，并在一定时间后（生成新的区块时）被记录到“账本”里，这便是“点对点”的通信机制

——它比传统的中心化交易更简单，同时在区块链的机制下也更加安全与透明。

二、以区块链作为交易和支付领域“变革”的“解决方案”

区块链技术的技术优势和性能优势非常明显。无独有偶，其解决的信息不透明，信息易被篡改等问题，正是金融领域长久以来的困扰。例如，在私募基金行业，长久以来存在着痛点：信息不对称性的问题。于是随着区块链 2.0，区块链 3.0 时代[1]的到来，区块链技术更多地作为解决方案被应用于金融领域。

1. 区块链技术可应用于金融交易的记录

金融和债券行业内有两个很显著的特点：一是应用具有交互性，交易非常频繁，用户对数据使用的频率很高；二是业务需要多方信任，平台上有任何一方修改了数据，其他的端口都需要同步显示变动，不能存在隐瞒事实的现象。

传统的金融服务系统采用的多是 C/S 架构，也就是客户端通过服务端进行中转，然后和另一客户端进行对接以及数据的流通，如图 2-1 所示。这样的数据流通方式较为简单，但是相应地存在两个问题：中转耗时较长且数据易被攻击篡改。

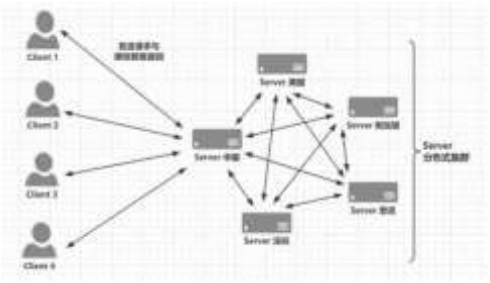

图 2-1 传统金融服务系统集群的大概模型[2]

而区块链技术本身就是点对点的传输，用户之间可以进行直接的沟通和交易，然后将交易记录以智能合约等形式写入自己的区块。进行一段时间的交易记录统计之后，用户进行争夺“记账权”，也就是系统内进行共识并生成新的区块，交易记录会被写入新的区块并被上链——这样一次交易就完成了。这里，虽然交易并不能保证即时生效，但是却更加方便——在“去中心化”的体系下，不再需要中介服务器地介入，交易可以简便地完成。此外，已经被上链的交易，是经过加密的，修改它需要极大的代价——要修改已经上链的交易，意味着修改对应的区块，这需要该用户长久获得区块链的“记账权”，是一件非常困难的事情。例如，使用 POW 证明（工作量证明）的区块链中的“51%算力攻击”，需要用户控制了一半以上的算力资源，才能完成对链的篡改行为，这在现实生活中的公链上是很难做到的。

区块链的这些特性使它能够被作为解决方案，用来进行金融交易的记录。

以私募基金行业为例。或是天然存在，或是刻意为之，私募基金行业的信息不对称性远高于大多数其他基金行业。项目方垄断式拥有公司的经营数据，投资方则需要花非常大的成本获取与评估其数据的真实有效性。早期投资方比后加入的投资方拥有更多信息，投资方比出资方又拥有更多信息[3]。当前私募基金行业上的交易，更像是一个“买菜”的过程：项目方进行宣传和吆喝，投资方按自己的分析进行考虑，双方你情我愿最后完成交易。

而引入区块链技术——建立一个被各方接受并参与的，基于区块链技术的私募行业信息平台，可以解决该问题。项目方自行选择是否将公司信息记入平台，并保持更新。投资方通过平台记录的项目信息为投资决策提供支持。是否参与该平台以及在平台上信息的完整程度，将成为项目方考虑投资与否的重要权重。这个平台会成为私募行业的标准之一。由于新技术的应用，该平台透明且难以被攻击，清晰的信息可以被各方直接获取。

尽管上述的新型平台目前还没有被研制出来，但是国内已经有了类似的存储技术和基于区块链技术的交易平台：例如，北京众享比特科技

[1] 区块链 1.0 主要指不具备智能合约模块，只有区块链基本模块的链；区块链 2.0 模块以 POS 共识为主，技术方面多出智能合约部分；区块链 3.0 主要目标是实现高性能和大吞吐量。

[2] 林冠宏,《区块链：以太坊 Dapp 开发实战》, 清华大学出版社, 2019-08, 第 127 页

[3] 周凯,《论区块链技术在私募基金行业的应用性与可行性》, 国内刊号 CN61-1499/C, 2019 年 8 月（下）, 第 1 页

有限公司 ChainSQL 采用独特的内容寻址和 P2P 通信技术提供安全高效的去中心化网络服务，通过区块链技术实现公信透明的数据存储和智能合约应用；UChains 则记录和显示融资数据，支持超大账本和在线数据，满足复杂场景下大业务量和持续化运营需求[4]。西班牙桑坦德银行的一份报告出，如果全世界的银行系统都能将区块链技术完美结合，那么在 2020 年左右，在基础运营模式不变的情况下每年将为银行省下大概 200 亿美元[5]。

2. 区块链技术可应用于新型支付清算方式

在日常生活中，支付清算是极常见的现象。很多时候人们可能会忽略，例如在进行微信支付时，有一笔中介费用流入了中介公司的囊中。日常而言，这样的中介支付费用可能微不足道，但是当涉及大宗交易时，支付成本昂贵的问题就异常突出了。在某些交易中，甚至有高达转账金额的 7.68%需要付款人负担[6]。为了降低不必要的负担，如何从结构和形式上对支付清算方式改革成为了重要的问题。

由于区块链的点对点交易原理，通过区块链技术资金转移能够更加迅速——国际收付款人直接交易，排除中介机构的参与，缩短了交收流程，提高了交易效率，实现了资金快速结算，将成本降至最低。这样的革新，其效果在推动跨境支付的情景中尤为突出。

例如，美国的瑞波实验室率先使用了基于区块链的外汇支付系统。虽然现在该系统还不完善，且有许多问题亟待解决，但它是相对完整的一个区块链支付服务系统。在该系统内，中心化支付与清算功能被去除，资金通过中立货币进行周转——在区块链上，资金完成了从一个地址向另一个地址的转移过程。该系统以共享的开源数据库形式，低价、迅速、安全地将交易者的资金快速转移到确定的账户里。同时该系统安全性高，任何机构或个人都不能控制其网络。在这个系统里，各个国家的货币可以自由兑换——这里的货币可以是法定货币，也可以是虚拟货币。

瑞波实验室系统是分布式的账簿体系，是区块链技术核心思想的实践应用，给未来区块链的支付结算系统提供了广阔的发展空间。由于系统交易效率更高、时间更短，几乎没有交易费用，一笔交易在几秒钟就可完成且没有任何附加费用，所以受到了诸多的关注和研究。

此外，区块链技术对数字货币也有着深远的影响。区块链可以应用于数字货币的发行，改变支付清算的形式。

数字货币相对于传统纸币的发行成本低廉，方便快捷，具有较高的安全性。现有的数字货币在各国市场认可度很高。我国央行对数字货币的研发也早已提上日程，其技术栈中，应用了部分区块链相关的技术。该技术栈的大致架构图如下所示。

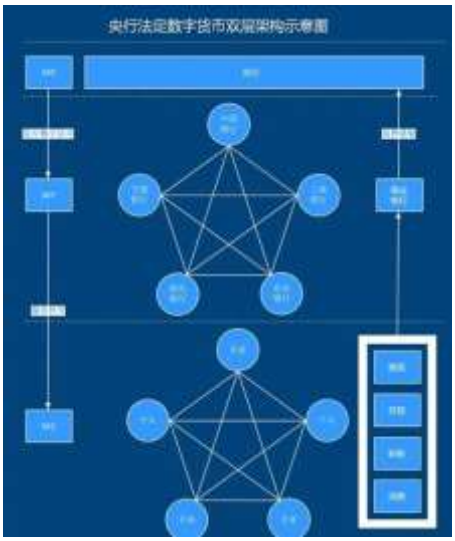

图 2-2 央行数字货币架构图

数字货币的应用是建立在全网信息记录、全名网上诚信、信用实时计算、货币法定授权、底层技术安全、算法不可破解等技术基础上的。[7]以比特币为例，它是区块链技术的完美体现，不仅可以用来直接支付交易，而且还发展出其他衍生产品，如比特币借记卡和 ATM 机等；国际上主流交易平台也支持比特币和其他国家货币的兑换，如在美国最大的比特币兑换网站上美元、欧元和英镑可以和比特币完成兑换。如图是 Gate 数字货币交易平台的浏览器门户。

[4] 工信部信息中心,《2018 年中国区块链产业白皮书》, 第 24 页
[5] 渤海大学经法学院,《区块链技术对传统金融业的影响》,《合作经济与科技》, 第 590 期
[6] 渤海大学经法学院,《区块链技术对传统金融业的影响》,《合作经济与科技》, 第 590 期
[7] “数字货币”词条, 百度百科

图 2-3 Gate 货币交易平台门户图

利用上述新型支付方式和货币形式进行支付，有着鲜明的技术特点和时代特点，也是未来发展的一种趋势。区块链在其中发挥着不可或缺的作用。

三、在未来，区块链技术会在经济价值共识上发挥重要作用

以上两方面着重于区块链目前正在或者已经落地的一些应用场景。它们都是基于区块链本身的功能和特点进行的。除此之外，共识机制也是区块链以及其他分布式系统的重要特点。所谓“共识”，就是让大家都达成某个一致的观点，在区块链系统中体现为大家都认为某一个区块是有效的，并将它上链。在区块链的不断发展历程中，诞生了许多的共识算法，如 POW，POS，DPOS 等，笔者认为，共识算法也会在未来的经济价值共识等方面发挥重要的作用。

互联网诞生最初，最早核心解决的问题是信息制造和传输，我们可以通过互联网将信息快速生成并且复制到全世界每一个有着网络的角落，但是它始终不能解决价值转移[8]问题。

在目前的互联网中有各种各样的金融体系，也有许多政府银行提供或者第三方提供的支付系统，但是它们还是依靠中心化的方案来解决。例如，以某个公司或者政府的信用作为担保，将所有的价值转移计算放在一个中心服务器（集群）中。尽管这样的中心化操作中，所有的计算也是由程序自动完成，但是利益相关者却必须信任这个中心化的人或者机构。很明显，此时“信用”的概念会局限在一定的机构、地区或者国家的范围之内。在此之外，价值和信用的概念会变得模糊和不可信。

由此可以看出，价值转移的核心问题是价值和信用的共识。在纷繁复杂的全球体系中，要凭空建立一个全球性的信用共识体系是很难的。由于每个国家的政治、经济和文化情况不同，对于两个国家的企业和政府完全互信是几乎做不到的。所以跨国之间的价值交换即使可以完成，也有着巨大的时间和经济成本。

共识机制则是这一问题的解决方案。例如，当某一节点宣称其拥有的资金（在比特币中被称为 UTXO[9]）时，其他的节点会进行验证，如果他们验证的结果为真，则会把这样的记录纳入自己的区块中；否则，会宣布该记录无效。而之后真正被上链的区块，则是通过共识机制选举出的。一般而言，它代表了大多数人的意志，从而被认为是有效的。这样一来，人们其实不需要花费太多的代价或口舌，自然地便可以完成价值的证明和转移。

事实上，基于区块链机制已经诞生了众多的数字货币。数字货币之间的流通本身就是价值的转移。例如，“币圈”普遍采用一种名为“UTSD”（泰达币）的数字货币作为中介，进行货币的交易，此时，共信共识便已经达到。而长远来看，世界上的国与国之间应该能够基于区块链建立更加完善的价值流通体系，从而使得经济价值的共识成为可能。

四、区块链在金融场景中仍有发展空间，也有着成为泡沫的风险

区块链技术在金融领域确实有许多的应用场景，也可以成为众多难题的解决方案。

然而，也有一些技术上的瓶颈瓶颈亟待解决。例如，不同区块链所采用的共识机制是不一样的。其中一些共识机制有着容易受到攻击，而且验证方式较为复杂的问题。以比特币采用的“工作量证明”为例，如果全网有一半以上的恶

[8] 所谓价值转移是指，在网络中每个人都能够认可和确认的方式，将某一部分价值精确的从某一个地址转移到另一个地址，而且必须确保当价值转移后，原来的地址减少了被转移的部分，而新的地址增加了所转移的价值。这里说的价值可以是货币资产，也可以是某种实体资产或者虚拟资产（包括有价证券、金融衍生品等）。而这操作的结果必须获得所有参与方的认可，且其结果不能受到任何某一方的操纵。

[9] UTXO，即未使用交易输出

意节点参与到了共识中时，区块链难以保证接下来产生区块的正确性；同时，工作量证明所需要的算力非常大，容易造成资源的浪费：一般而言，为了完成一次共识，全网的节点需要不断地计算一个给定哈希值的原值，而这一过程是非常漫长的。此外，用户对于数据的校验需要遍历之前的每个区块，这使得随着区块数量增加，网络承担的负担和延迟也会增加。

当涉及到金融场景时，区块链可能体现出交易的实时性较差等问题。而关于这一方面的问题解决，还需要长时间研究进行突破。

此外，由于“币圈”的火爆，目前区块链衍生出的各种代币层出不穷，各种玩家趋之若鹜。然而，其中涉及到许多的商业骗局，有待进一步的监管。以最新发行的 Filecoin（FIL）币为例，由于它是被誉为“新一代互联网传输机制”——IPFS[10]的子产品和衍生物，许多人对其抱有较高的期待，甚至将其誉为“比特币 2.0”，许多骗局也油然而生。然而，自 10 月 15 日主网上线以来，表现却不尽如人意。

图 4-1 上线以来 FIL 币值走势图

在金融领域，区块链体现出的类似问题还有很多。历史上有三大泡沫：荷兰郁金香泡沫、法国密西西比泡沫、英国南海泡沫，聪明如牛顿也曾为之折戟。许多人曾将区块链称之为“第四个泡沫”。为了避免类似的情况发生，相关的监管也势在必行。

随着区块链技术的成熟程度进一步增加，和产业结合更紧密，行业监管制度体系应进一步建设完善，以打造良好的发展环境，为产业区块链项目深入服务实体经济提供有力保障，一些违法违规的项目则应受到严格监管。

五、总结

金融本身是人类生活的重要组成部分。区块链作为新兴的技术，金融是其重要应用场景。

如前所述，区块链确实能在交易记录，支付清算等场景中发挥重要作用，同时也能为长远而言的价值共识等做出贡献。然而，区块链本身也有着应用场景中的不足，许多黑色迷雾也渐渐开始笼罩。

随着区块链技术的深入发展，行业应该尽快推进对于相关技术的落地和应用；同时区块链标准也应该逐步完善，这对构建和完善区块链产业生态，促进区块链技术场景落地具有积极的推动作用[11]。另外，监管部门也应该发挥积极作用避免不良金融现象的发生。在进一步的研究以及多方面的改良和配合下，区块链应该能在金融领域发挥更加积极的作用。

[10] 全称是星际文件系统。星际文件系统是一个旨在创建持久且分布式存储和共享文件的网络传输协议。它是一种内容可寻址的对等超媒体分发协议。在 IPFS 网络中的节点将构成一个分布式文件系统。

[11] 工信部信息中心，《2018 年中国区块链产业白皮书》，第 96 页