区块链、分布式账本在金融行业的应用的介绍

文 \ 黎江 何京汉

黎江为世纪互联创新研究院院长、中关村区块链产业联盟创始人，资深金融IT专家
何京汉为融云公司CEO，资深金融IT专家

区块链技术解读

“区块链”正像互联网一样改变世界。首先，什么是区块链技术？区块链技术本质上是基于分布式点对点网络（P2P）计算机的交易账本，在区块（账页）最终被“链接”入区块链时，得到了区块链全网或大多数交易节点的确认。该技术采用先进的加密技术，以确保交易安全，网络用户可以查看交易细节。因此，区块链在没有中心信任机构的监管下，通过全网或大多数账本共识机制，始终维持了一套正确的交易账本。减少了交易确认的冲突，提高交易速度和效率的交易。虽然区块链技术到目前最著名的应用还只是比特币的虚拟货币，但是区块链技术应用的潜在价值带来了很多启示。

由于区块链和分布式帐本技术与应用尚在孵化阶段，共识的机制尚未形成标准。为了更好地理解，需要对区块链的结构、区块链工作证明算法、区块链信任加密技术、区块链的共识机制、点对点网络协议等关键技术细节的深入研究。理解区块链技术本质，才能预测区块链金融的发展，特别是目前区块链技术还在发展的幼儿阶段，区块链、共享帐本有多个技术路线，技术、业务和管理的讨论在国内才刚刚开始。

区块链的结构解读

由于业务价值互联、工作确认算法、全网共识机制、多中心化都是通过区块链分布式账本实现，分析区块链分布式账本是理解区块链技术的核心工作

区块链的分布式账本贯穿了业务层（如资产）、应用层（如智能合约）、中间件层（如分布式交易共识）和底层技术层，从而达成业务价值互联、工作确认算法、全网共识机制、多中心化的业务目的。

区块数据结构：区块的头信息+区块账本信息（多个账本）。

这里有三项内容需要分析。

1.区块的头信息的作用。比特币公有链块的头信息（80字节）包含了链锁位、时间戳、工作量位、权属信息位。它代表的是描述这个块的基本信息。

链锁位：将区块“链”在一起。比特币网络的区块权属信息位：其值由私钥和

最后一笔交易哈希Hash计算所产生。它链接该区块（账页）的所有交易。比特币网络链接的是转账的交易。其他区块链公司链接的是块上账户（会计余额）交易、合约交易、资产交易。

时间戳：记录账页（区块）产生的时间。由于区块不可修改性，时间戳与权属信息可以共同用来确定区块（账页）的权属。

2.区块链分布式账本是一个还是多个?自从区块链分布式账本的概念提出来以后，分布式总账支持智能合约、智能资产的研究项目越来愈多。具有代表性的数字资产控股（DAH）的超级账本（HyperLeger）、R3CEV允许账本（Permissioned distributed ledgers）的方案中都支持多个账本，而比特币只支持一个账本。

3.多个账本的数据结构：目前的发展是将金融（多个子链）账户链、智能合约链、智能资产链与分布式账本（主链）分开。智能资产、智能合约穿越不同的参与者涉及不同的业务或法律实体，这需要一个复制的（每个节点上有交易的副本）、共享的（智能合约、账户、智能资产的交易结果是一致）分布式账本。

区块分布式操作

块上操作需要复制、共享的分布式账本，块下操作需要考虑每个参与者（节点）的私密性。根据我们的观察：块上操作以点对点网络协议为基础；块下操作基于分布式云计算和区块链技术加密技术混搭。

典型的块上操作：a.获得区块、下载和查询交易信息；b.区块生成。c.区块账户

区块链的工作确认算法全网共识机制

共识是分布式系统容错的基本问题。有各种分布式算法如PBFT、Raft、PAXOS被用于区块链技术核心中。它具有两重保护机制，产生正确的决定。第一，按照“提供优惠待遇者为首选”，第二，然后“首选”发布广播（用点对点协议）

相同交易数据给各服务器节点，让“其它节点”决定该交易是否记账—“少数服从多数”。典型的共识算法就是多个服务器对一个即将记入账本的数值进行投票，获得大多数的选举票者被记入账本。假设有5个区块链服务器对一个记入账本的交易进行投票，只要有3个服务器投“确认”即所有服务器都要服从这个决定。这种少数服从多数的机制，在其中少数服务器投了“否认”票（有意不承认、没回应等）的情况下的交易确认机制问题。确保了少数“坏服务器”不工作，全网照样记账的分布式记账难题。

典型的共识算法是构建在在“复制的”状态机的上下文中的容错系统组件中。每个服务器有一个状态机和日志。状态机是容错的哈西表，即使少数服务器不工作了，服务器的状态机也能够从服务器的日志中得到命令

这些找到了分布式环境下，陌生的交易对手（在没有过往业务往来的情况）之间，往来信息无法信任的算法。解决了传统的“拜占庭”信任危机的问题。

例如：超级账本项目使用PBFT（Practical Byzantine fault tolerance实用拜占庭容错算法，已经存在超过15年的算法）的共识算法。据称能处理每秒每池（每个节点）交易数以万计，而不需要资本密集的挖矿“工作证明”。这使得全网在识别、合规的原则下，每个参与者都知道彼此在交互处理分布式账本。

区块链加密技术

区块链的块信息、账本信息是通过加密算法MD5（文本加密）、SHA256（密钥加密）、ECDSA（非对称算法）以及HASH算法共同实现的。最终，发到线上的账本信息，某些节点有任何篡改，块上所有节点都会知道（通过全网“复制的历史交易数据，进行复核计

通过对区块链技术的解读，我们认为业务价值互联、工作确认算法及全网共识机制、加密技术、多中心化等 4 项技术属性是衡量该区块链产品和应用能否达到区块链技术的初衷的标准。这 4 项技术对现有金融 IT 技术具有替代作用，而且，这 4 项技术是通过数据紧耦合（天生长在一起）带来 IT 架构、应用架构的松耦合，改变目前金融机构紧耦合的 IT、应用架构。

算）。若发生这种情况，可能行动是否认这样的交易，需要“区块链工作确认算法”去解决（交易或不计入区块、或否认这些交易）这种不信任问题。

1.客户端利用MD5等算法对账本（资产、合约、账户、参与者等）进行加密，

2.发布上区块链的账本用SHA256进行加密，私钥（ECDSA、ED）进行签名

3.用Hash算法对账本信息进行计算，生成区块或获取区块信息

多中心化

我们进一步考虑这样的业务过程，想象这样一个平台存在：也许一个复制的、共享账本记录了所有的银行间交易余额或记录银行间的所有资产交易或衍生品头寸，这个共享的账本也是最权威的记录，具备足够的公信力。我们可以部署代码，描述我们的协议；构建企业间的业务逻辑；运行这样一个有效的交易处理系统，将降低成本和系统的复杂度。

通过对区块链技术的解读，我们认为业务价值互联、工作确认算法及全网共识机制、加密技术、多中心化等4项技术属性是衡量该区块链产品和应用能否达到区块链技术的初衷的标准。这4项技术对现有金融IT技术具有替代作用，而且，这4项技术是通过数据紧耦合（天生长在一起）带来IT架构、应用架构的松耦合，改变目前金融机构紧耦合的IT、应用架构。

区块链技术在金融行业的应用

区块链技术以显著的特性吸引金融行业：

• 几乎所有的无形资产业务文书可以在分布式账本中被编程或代码调用

• 交易的不可取消性。清算和结算可以以编程的方式在瞬间完成。分布式账本增强了交易数据的准确性和降低了结算风险。

• 点对点的交易处理方式，让交易近实时完成，降低了IT的成本

• 分布式账本的每笔交易都是公开验证、自动管理。这样的方式使历史记录难以逆转，可公开访问所有交易的历史记录。能有效地监管所有的参与者

• 全球商业、证券交易（如R3CEV联盟）所和全球技术公司（如IBM、三星等技术公司）的支持促进了区块链、分布式账本的应用。可以预期不远将来，区块链

和分布式帐本技术将成为可信的和可管理大型交易系统的核心技术。

区块链金融应用1.0

1.0的应用可能发生在账户间转账、借记卡、贷记卡支付、汇款、外币线上支付等支付交易领域，在这些领域区块链技术、分布式账本技术可以让买家和卖家不通过中介对交易的验证。

比特币利用共享数据库取代了成千上万个私人的银行账户，因此，凡是在互联网上的人都可以发出、接受支付款项。然而比特币只是半边账。购买比特币时，需要两条账户记录，一个是记录比特币的变化，另一个是记录资金的变化。比特币数据库知识持续跟踪了比特币端的交易。如果想用比特币换美元，需要经由其他交易系统完成美元的传递。比特币结算非常有效率“交易本身就是结算”，然而用比特币美元交易结算，需要二个账户完成交易。

区块链金融应用2.0

2.0的应用Ripple Lab等第二代系统将这种理念外延，将大交易量市场的交易纳入了进来，区块链技术还可在互联网上建立基于规则，数据、标准化智能合约，它用算法交易程序代替合同，当智能合约约定的日期、条件一旦达成，网络自动执行合约。智能合约主要应用在金融资产如债券、权益、衍生品和线上应收贷款。事实上，已经有许多项目将股票、债券、汽车、房产和商品用区块链技术储存和交易。这些区块附加资产的信息生成“智能资产”，或用“智能合约”记录和交易这些资产。智能合约和智能资产被嵌入了复杂的交易算法，这些记录和算法可不再被

中心化的登记机构拥有，而是全网的共享资源和全网共识的算法。

区块链金融应用3.0

将对交易、信息（messaging）和账本进行组合、配对，以清晰的区块链记录挑战现存IT应用系统。可以使用现实世界中的交易系统，产生配对成功交易或者“交易报告”，将交易或者交易报告传递给区块链总账。或者，可以将交易传递给现有帐本系统，如托管行账户。不仅是金融机构，一些互联网公司的系统也会受到区块链公司的挑战。在区块链的应用场景有很多想象，但金融行业最可能利用区块链技术产生落地应用。

区块链技术正处在快速发展阶段，全面的商业化还需几年才能实现。但是，金融行业为了不错过机遇，业务部门、技术部门与管理部门必须开始研究区块链技术的与应用。

区块链、分布式账本的金融业务深入解读

智能合约、智能资产的深入理解

智能合约就是将现在个别企业拥有的合约迁移、共享为区块链上多个企业之间的业务逻辑。可以把代码想象为两个企业之间共享的合约；该合约在区块链分布式账本上执行；该智能合约托管了资产，用来处理和回应各企业对资产的交易、发行等业务操作。由于智能合约是共享的，智能资产能为区块链上各企业提供共享的数据和业务逻辑，区块链上各个企业会发现没有必要保存对资产处理的所有业务逻辑和数据。

金融合约和金融资产的条款都是以合同文书、资产支持文书形式记载的。线上互联网金融技术实现了数字资产和数字合约，即利用平台实现了数据结构（包括合同文书、资产文书、贷款政策与文挡等）的电子存储和集中处理。而块上的区块链业务是希望使得数字资产和数字合约更加智能化，可利用合约的条款（合同文书的内容）编程，而且是每个参与者（节点）都可利用脚本语言对条款进行分布式处理。技术上以IBM hyperledge和以太坊为代表的公司，将智能合约放在"虚机"内，利用试图利用脚本语言传递合约和资产的部分业务逻辑（如期货衍生合约的到期执行条件）。

虽然只是这些块上“智能合约”、

智能合约就是将现在个别企业拥有的合约迁移、共享为区块链上多个企业之间的业务逻辑。可以把代码想象为两个企业之间共享的合约；该合约在区块链分布式账本上执行；该智能合约托管了资产，用来处理和回应各企业对资产的交易、发行等业务操作。

由于分布式账本在数据结构上包含了智能合约、智能资产、账户及对应的合约交易、账户交易、资产交易，区块链分布式账本能在全网穿透不同的参与者和涉及不同的合约或法律实体，全网在可识别的原则下，处理业务智能合约和智能资产的的结算交易，且每个参与者的交易在分布式账本上能交互地处理交易。

“智能资产”传递简单的起步，但为区块链“业务价值互联”的目标迈进了一大步。

第二代区块链如Ripple、Counterparty、Overstock等系统，在区块链中跟踪以“代币”形式存在的不同种类资产，解决了单边帐本问题。这些系统依托于银行、托管行等主题赎回“代币”并将公开显示资产过户给买方。使用了代币，用户可以买卖资产，并能在“一个账户”中体现完整交易。第二代系统也完善了交易，用户可以投标、开价，系统完成交易配对、转移资产而无需其他系统处理。由于“交易本身就是结算”，结算非常有效率。

分布式账本的业务功能

由于分布式账本在数据结构上包含了智能合约、智能资产、账户及对应的合约交易、账户交易、资产交易，区块链分布式账本能在全网穿透不同的参与者和涉及不同的合约或法律实体，全网在可识别的原则下，处理业务智能合约和智能资产的的结算交易，且每个参与者的交易在分布式账本上能交互地处理交易。

例如Clearmatics公司让智能合约的“分布式虚机”在行业标准的分布式总账下运行，穿越不同的参与者涉及不同的合约义务或法律实体，实现结算的自动化。

区块链金融用例研究

全球金融行业的研究和验证项目表明，以下金融领域的应用用例最有可能成为区块链实际应用的场景：

1. 私人股权和权益发行
2. 业务数据的认证和识别
3. 跨国支付汇款
4. 场外交易和外汇买卖结算和清算
5. 债券回购
6. 供应链金融
7. 贸易结算
8. 财团贷款

这些用例的共同特点是可以利用智能资产、智能合约，穿透不同的参与者涉及不同的合约或法律实体。而这些领域的参与者确实需要寻找一个共享信息的分布式账本，实现产业升级，提升数据的全网可信，提高结算和清算的效率。如果金融行业未能快速接受区块链，那么“技术脱媒”领域（例如互联网金融）将会加快它的发展，这就意味着，金融行业在未来的自动化交易市场中，只能分到很小的市场份额。