区块链研究进展综述

中国人民银行数字货币研究所所长 姚前

区块链是信息互联网向价值互联网转变的重要基石，是现代数字货币体系的可选技术之一。它以密码学技术为基础，通过分布式多节点“共识”机制，可以“完整、不可篡改”地记录价值转移（交易）的全过程。区块链采用的具体技术包括密码学、共识协议、博弈论、数据存储、P2P 通信等，是多种已有技术的融合创新。本文从共识协议、安全与隐私保护机制、可扩展性与效率、系统 / 协议的安全分析与评估等四个方面，对区块链的研究进展进行了概要评述。

一、共识协议

共识协议用于在分布式系统中实现可用性与一致性，是区块链的关键技术，其核心指标包括共识协议的强壮性（容错、容恶意节点的能力）、高效性（收敛速度，也即系统达成一致性或“稳态”的速度）及安全性（协议抽象理论模型的安全界）。代表性协议包括 PBFT 为代表的 BFT 类共识、PoW/PoS 为代表的中本聪共识（Nakamoto Consensus）、新型混合共识等。

（一）BFT 类共识

BFT（Byzantine Fault-Tolerant）算法于 20 世纪 80 年代开始被研究，旨在解决所谓拜占庭将军问题。BFT 类算法中最著名的是 PBFT，该算法是基于消息传递的一致性算法，在弱同步网络下，算法经过三个阶段可以达成一致性，复杂度为 $O(n^2)$。在无法达成一致时，这些阶段会重复进行，直到超时。PBFT 的优点是收敛速度快、节省资源、具有理论上的安全界（理论上允许不超过 1/3 的恶意节点存在，即总节点数为 3k + 1，其中正常节点超过 2k + 1 个时，算法可以正常工作）。

Andrew Miller 在 2016 年提出的 HoneyBadgerBFT 对 PBFT 做了改进，其过程由原子广播（Atomic Broadcast）和异步公共子集协议（Asynchronous Common Subset）两部分组成，它使用 N 个二进制共识协议实例并根据其结果来决定一个公共子集。HoneyBadgerBFT 可以在异步网络下进行共识，不依赖于任何关于网络环境的时间假设 。

BFT 类共识随着参与共识节点的增加，通信开销会急剧上升，达成共识的速度则快速下降，难以支撑上万节点规模的分布式系统。此外，节点参与共识首先要获得投票权，因此要为节点的加入和退出过程设计额外的机制，增加了协议复杂度和实现难度。

（二）中本聪共识

比特币通过引入经济激励改造了共识投票的过程，将每次账本数据变化都安排一轮投票变为滚动的无限期投票：任何人都可以生成一个包含交易的区块（增加账本数据）并广播，其他人如果同意该区块纳入账本，则将该区块的哈希作为自己构造的区块数据的一部分，以对该区块进行“确认”；对某个区块的“确认”也包含了对该区块前序所有区块的“确认”；以工作量大小决定投票权重，投票附加的工作量大的区块胜出。这类共识机制的安全依赖于特别设计的经济激励，比如工作量证明（PoW）或者权益证明（PoS）等。

比特币的工作量证明是寻找满足特定难度值的区块头哈希，比特币之后的虚拟货币项目为了避免出现专用 ASIC 矿机，开始设计抗 ASIC 的 PoW 算法，其中一类的思路是通过串联不同的哈希函数来增加 ASIC 芯片设计的难度，但并不具备抗 ASIC 的能力。

另一类思路则是设计内存消耗型算法，比如 Ethereum 基于 Dagger-Hashimoto 的 Ethash，Zcash 基于广义生日悖论问题的 Equihash，æternity 基于二分图环路检测的 Cuckoo Cycle 等。这类算法在计算时需要占用大量内存，内存作为成熟产品优化空间小，设计专用 ASIC 芯片的成本优势不大。

为了克服 PoW 资源消耗大，运行成本高的问题，PeerCoin 最早提出并实现了权益证明（Proof of Stake，PoS）类的共识协议。PoS 协议下，节点获得区块创建权的概率取决于该节点在系统中所占有的权益比例的大小。

PoS 一般需要用户时刻在线，这对应用带来了很大挑战。为了解决这个问题，衍生出了 DPoS（Delegated Proof of Stake）共识，其核心思想是从先从全网节点中选出部分节点，保证这些节点的有效性，然后在该子节点集合内进行 PoS 共识。

PoS 共识机制也引起了学术界的极大兴趣。康奈尔大学的 Elaine Shi 等在 2017 年提出了基于 Sleepy Model 的 PoS 共识，并对其进行了形式化描述和安全性分析，证明了该共识系统在分布式环境下有良好的健壮性。爱丁堡大学的 Aggelos Kiayias 等在 2017 年也设计了一种名为 Ouroboros 的 PoS 方案，该成果发表在密码学顶级国际会议 Crypto 2017 上。

（三）混合共识

Elaine Shi 等在 2017 年提出了将中本聪共识和 BFT 类共识进行有机结合的混合共识方案，该方案通过 PoW 机制来选取 Committee（负责交易的验证确认及区块创建），Committee 通过 PBFT 来进行交易及区块的共识确认。

而 Silvio Micali 等在 2017 年提出的基于可验证随机函数（VRF）的 Algorand 协议则从另一个角度出发，通过“加密抽签”的方法随机决定区块创建者后，用带权重的拜占庭协议达成全网共识，可视为一种多级动态验证组 BFT 共识和 PoS 的混合方案。Algorand 达成共识的情况会规约成 3 种，以大概率保证了只有唯一的输出，相比 Sleepy 和 Ouroboros 共识模型，确定性更好，不容易分叉。

二、安全与隐私保护机制

安全机制是区块链中最为核心与关键的组成部分，而密码原语与密码方案是安全机制的支撑技术。在公有链中，安全机制主要包括：隐私保护、共识协议安全性、智能合约安全性、数字账户安全（钱包私钥保护）、离链交易安全机制、密码算法的实现安全及升级机制等。

（一）隐私保护

在公有链中，需要对交易数据、地址、身份等敏感信息进行保护，同时又能让记账节点验证交易的合法性；对于联盟链，在构建隐私保护方案的同时，需考虑可监管性 / 授权追踪。可以通过采用高效的零知识证明、承诺、证据不可区分等密码学原语与方案来实现交易身份及内容隐私保护；基于环签名、群签名等密码学方案的隐私保护机制、基于分级证书机制的隐私保护机制也是可选方案；也可通过采用高效的同态加密方案或安全多方计算方案来实现交易内容的隐私保护；还可采用混币机制实现简单的隐私保护。

1. 混币技术

混币技术是指将多笔不相关的输入进行混合后输出，使得外界无法关联交易的输入与输出，从而分辨不出数字货币的流向。这是最朴素的匿名技术。

CoinJoin 是一种无关协议的匿名混币技术，使用者需要委托第三方，来构造一笔混合多笔输入的交易。CoinJoin 技术不是完全匿名的，即提供服务的第三方可以知道混币交易的流向。TumbleBit 协议是另一种混币技术。该协议是一种链下通道的混币协议，也需要第三方参与，但第三方无法知道交易细节，仅仅是提供服务。TumbleBit 分为 Puzzle-Promise Protocol 和 RSA-Puzzle-Solver Protocol 两个子协议，需要发送方、接收方和第三方进行多次交互。

2. 环签名

Monero（门罗币）在保证交易的隐私性方面应用了一次性环签名（One-time Ring Signature）技术，具有不可链接（Unlinkability）和不可追踪（Untraceability）两大特性。

门罗币里，用户有两对主公私钥对，用于生成一系列的一次性密钥对。这些一次性密钥在交易时使用，且无法关联到主公私钥对。进行交易时，发送者需要使用一次性公私钥来计算唯一的 key image，然后选择一个公钥集合来进行环签名。校验者可以验证

签名的合法性，但无法知道签名者的公钥。在网络里，节点需要维护一张表，来记录每次使用过的 key image，否则会出现双花问题。环签名可以有效提高匿名性的同时，无需任何第三方协作参与。但相比椭圆曲线签名，环签名的签名长度明显增大，生成签名和验证签名的复杂度也大大增加，这会给网络带来多余的负担。

3. 零知识证明

ZCash 采用了名为 zk-SNARK 的零知识证明技术，来保证交易的发送者、接受者和交易金额的机密性。在 ZCash 里，发送者通过向全网广播承诺（commitment）和废弃值（nullifier）来进行转账交易。zk-SNARK 用于向网络证明承诺和废弃值的合法性，同时又不揭露发送者的身份。

zk-SNARK 具有两个特点：简洁性（Succinct），即验证者只需要少量计算就可以完成验证；非交互性（Noninteractive），即证明者和验证者只需要交换少量的信息即可。zk-SNARK 可以证明所有的多项式验证问题。它提供了一个系统化的方法，可以把任何验证程序转化成一个名为 Quadratic Span Program (QSP) 的多项式验证问题。因此，任意复杂的验证问题都可以由 zk-SNARK 来证明。zk-SNARK 的缺点在于计算验证数据时，需要一定的计算量。此外，zk-SNARK 还有一个初始参数设置阶段，来生成一个“绝对机密”的随机信息。使用这些初始化的随机信息可以欺骗验证者，因此需要保证该过程的绝对机密与安全。

（二）数字账户安全

钱包私钥直接关系到账户安全，需要对钱包私钥进行妥善保护。可采用无密钥的密码算法（标准算法的白盒化方案或设计新型的白盒密码算法）和代码混淆技术，实现敌手无法提取核心密码算法和密钥信息；或采用基于口令、身份、生物特征等认证因子的加密算法对密钥进行加密存储；基于 TEE（可信执行环境）、辅助硬件的技术方案也是保障数字账户安全的可选方案之一。

（三）密码算法的实现安全及升级机制

需确保区块链中密码算法的实现安全，并构建密码算法更新 / 升级时的安全机制。密码算法的实现安全包括软件实现的安全性及硬件实现的安全性，避免密码误用，有效抵抗旁路攻击。

三、可扩展性与效率

可扩展性旨在分布式账本协议的基础上，对整体进行性能效率的提升、扩容或功能性上的扩充，可选方法包括：缩短区块的产生间隔、增加区块大小、采用双层链结构、引入闪电网络、在不影响安全性的前提下修剪区块中的数据等。

（一）闪电网络

闪电网络是比特币的链下扩容方案，旨在扩大比特币的交易规模和交易速度。闪电网络的基础是交易双方建立双向微支付通道。HTLC（Hashed Timelock Contract）定义了该双向微支付通道的基本工作方式。双方在转账时，转账人将一笔钱冻结，并提供一个哈希值。在一定的时间内，若有人可以给出哈希原像，就可以使用这笔钱。在这个基础上，两两各自建立链下微支付通道，最终可以扩大成一个链下支付网络。一旦链下网络达到一定的规模，用户找到一个通道数较多的节点后，便可连接到其他用户，从而完成链下交易。由于不需要上链，闪电网络中的交易是即时完成的，只有最终的清算才需要上链。

目前比特币和莱特币均已支持闪电网络。然而，在闪电网络方案中，链下网络的建立及路由协议还存在较大的不足之处，伊利诺伊大学香槟分校 Andrew Miller 等在 2017 年提出了一种新型的闪电网络协议，进一步优化提升了闪电网络在链下网络建立及路由方面的性能效率。

（二）采用双层链结构

Bitcoin-NG 采用了双层链结构，其主要思想是：矿工解决哈希难题并由此创建的区块称为 keyBlock，创建 keyBlock 的矿工在下一个 keyBlock 出现之前每隔一小段时间可以发布一个 microBlock。系统的安全性和健壮性建立在 keyBlock 的 PoW 机制上，而系统的交易吞吐量则通过 microBlock 的频繁发布得以显著提高。

然而，在 Bitcoin-NG 中存在两个安全隐患：

一是不能有效阻止自私挖矿，二是当某个矿工创建 keyBlock 之后，他可在短时间内发布大量的 microBlock，从而引发系统大量分叉并最终对共识机制的收敛性造成很大影响，同时也大大加重了系统的通信负荷。

（三）MimbleWimble

MimbleWimble 技术删除交易中所有已花费的输出，可以有效压缩区块数据的大小。MimbleWimble 使用单向聚合签名（OWAS）对金额进行隐藏，其隐藏公式为，其中 C 是 Pedersen commitment，G 和 H 是与椭圆曲线加密函数（ECDSA）生成的无关的固定值，v 是金额，而 r 是一个秘密的 random blinding key（随机盲密匙）。此后，需要通过 range proof 证明输出在正常的取值范围内。用户不需要遍历整个区块链，只需要验证整个区块链的输入之和和未花费的输出之和是否相等，依次证明整条区块链是正确的。因此，用户可以删除所有已花费的输出，来有效压缩区块数据的大小。除此之外，MimbleWimble 还提供一定的隐私和扩展性，但该方案无法支持复杂的比特币脚本。

四、区块链 / 协议的安全分析与评估

在区块链（协议）的安全性分析与评估中，一方面，需要对已有的共识协议建立抽象理论模型，并基于该模型研究共识协议的安全性；另一方面，需要研究在不同攻击方法（或场景下）区块链的安全性，例如：分别在高同步性、高异步性网络条件下，基于合理的困难问题假设、攻击者的计算能力、攻击类型及方法等建立相应的统计分析模型，给出共识协议能有效抵抗相应攻击的安全界；需分析在激励机制失效下系统的安全性；需对系统中密码方案软硬件实现进行安全性分析等。

（一）自私挖矿

传统观点认为比特币是有激励相容机制的，即没有人可通过损害集体利益去实现自己利益的最大化。但自私挖矿（selfish mining）的提出证明了这种观点是不完全正确的。在矿工是追求最大化利益的理性者的条件下，只要矿池能控制全网超过 1/3 的算力，就可以发起自私挖矿攻击，获取更大的收益，并对网络安全造成威胁。

自私挖矿的分析是基于理性者条件的假设下，但现实中人往往不是完全理性的，且存在多方博弈，因此实现自私挖矿攻击还是存在一定的难度。

（二）分区攻击

在 P2P 网络里，只要控制一定数量的节点，就可以进行 Eclipse Attack，从而发起 51% 攻击，控制整个网络。这是一种分区攻击。假设网络中只有 3 个节点在挖矿，其中两个分别拥有 30% 的全网算力，剩余一个有 40% 全网算力。如果攻击者可以控制拥有 40% 算力的节点，则他可以隔离其他两个节点，使得他们无法达成共识。最终的结果是，攻击者所生成的链会经共识成为最终的区块链。因此在分区攻击下，攻击者不需要拥有超过一半的算力，就可以发起 51% 攻击。发起这种攻击的前提条件是，被隔离节点链接到的所有节点都受攻击者控制。在网络规模不大的时候，这比较容易实现。

（三）大数据分析

区块数据在全网都是公开的，因此可以很容易地对它们进行分析。Kumar Amrit 等在 2017 年通过对 Monero 历史区块数据的分析，得到了如下结果：65% 以上的 input 会产生级联影响，影响到 22% 的交易被追踪到；来自同一交易的 output 在下次交易时通常会聚合在一起；匿名集中最近发生的 output 很可能就是真实被花费的 output。

因此，尽管 Monero 具有良好的匿名特性，但通过数据分析，还是有超过半数的交易被追踪并分析出来。这说明了系统的参数选择和用户的使用习惯也会导致隐私暴露。

（四）共识协议的抽象理论模型的安全性分析

Aggelos Kiayias 等在 2017 年构建了比特币的 PoW 协议的抽象理论模型，并借鉴密码学中可证明安全的思想证明了该抽象理论模型的安全性；Elaine Shi 等在 2017 年提出了基于 Sleep Model 的 PoS 共识模型，并对其进行了形式化描述和安全性分析，证明了该共识系统在分布式环境下有良好的健壮性。