数字货币中的区块链及其隐私保护机制

王皓 宋祥福 柯俊明 徐秋亮

0 引言

2008年，一位化名“中本聪”的学者在网络上发表了一篇题为《比特币：一种点对点的电子现金系统》的文章，这篇看似普通的文章目前看来完全可以说具有划时代意义——无论是对金融或是对密码技术，真正的电子货币（或称数字货币、密码货币）从此诞生。历经近10年的发展，各种密码货币纷纷出现，但这篇文章中所创造的数字货币——比特币，一直保持着交易量全球第1的地位，比特币全球总市值已突破400亿美元。与此同时，支撑比特币运行的核心技术——区块链，由于具备去中心化、可验证、防篡改等特性，迅速成为各国政府、国际组织、大型财团、科研机构关注的热点，各种区块链项目如雨后春笋般爆发式增长。有观点认为，区块链技术对未来世界的改变，可能丝毫不亚于云计算、大数据等IT革新技术。

在我国，区块链技术受到政府等相关部门的高度重视。2016年12月，区块链技术首次被列入国务院印发的《“十三五”国家信息化规划》。与此同时，区块链行业规范也相继发布。2016年10月，在工业和信息化部信息化和软件服务业司的指导下，中国区块链技术和产业发展论坛发布了《中国区块链技术和应用发展白皮书（2016）》；2017年5月16日，中国区块链技术和产业发展论坛发布了国内首个区块链标准《区块链参考架构》。这些标准化工作有助于统一对区块链的认识，规范和指导区块链在各行业的应用，促进解决区块链的关键技术问题，对于区块链产业生态发展具有积极的推动作用。

1 区块链简介

为了准确理解区块链，首先对区块链技术最典型、最成功的应用——比特币——进行剖析。

1.1 比特币的工作原理

比特币作为无中心化的数字货币，其工作原理包含数据存储和共识机制两个方面。

1）比特币的数据存储在比特币系统中，采用了一种链式结构存储用户转账记录。与传统的链式数据结构略有不同，比特币系统中用哈希指针（Hash Pointer）实现数据块之间的逻辑链接，即当前数据块的头部记录着上一数据块的哈希值。

这种结构在很大程度上加大了篡改数据的难度，因为某一数据块中数据发生变化，将造成其直接后继数据块头部的哈希值变化，从而引起所有后续数据块的连锁反应。此外，由于后续数据块中隐含了前面数据块的信息，从而保证了数据块之间的时序关系。

2）比特币的共识机制无中心的货币系统必定需要共识机制。比特币系统采用了一种被称为“挖矿”的方法来保证共识。这里的“挖矿”与现实中的挖金矿具有本质类似性。黄金虽然有自身的自然价值，但作为货币时事实上却可以忽略它的自然价值。它是稀缺的，且通过一定的劳动量才能（概率地）获得。在比特币系统中，“矿工”付出工作量“挖出”的是符合某种条件的随机数，它与黄金一样是稀缺的、概率产生的。

比特币系统具体共识过程如下。

（1）矿工根据当前区块链末端的数据块计算新数据块的头部prev_hash。

（2）矿工生成随机数nonce，并将新数据块的头部prev_hash、收集到的若干转账记录Data、随机数nonce作为挑战哈希函数H（）的输入（在比特币系统中，H（）为连续两次SHA 256），计算H（prev_hash||Data||nonce）。若H（）的函数值小于某一个预设的阈值，则nonce合法；否则，重新生成nonce，继续计算。

（3）矿工找到合法的nonce后迅速进行P2P广播，其他矿工在收到该消息后停止挖矿并进行验证，验证通过后，认为新的区块已产生（达成共识）。

（4）新区块产生的同时，找到nonce的矿工从系统得到一定数量的比特币作为奖励。

（5）矿工基于新产生的区块继续挖矿。

比特币系统中使用的这种共识机制称为工作量证明（proof-of-work，PoW）。挖到矿的矿工获得一定奖金，可视为其挖到的“黄金”，代表了一定抽象的工作量。此外，在比特币系统中，工作量证明既是共识机制，也是发行机制。在对矿工奖励的同时，整个系统中的货币也在增加。

比特币可以看作是一种基于区块链技术的特殊货币。在比特币系统中，每个节点拥有区块链的一个副本，当有交易发生时，节点通过执行共识协议，对区块链进行更新，并在所有节点间进行同步，从而杜绝了“双花”行为的发生。

1.2　区块链的定义

区块链作为支撑比特币运行的核心技术，是一种利用链式数据结构来验证和存储数据、利用分布式节点共识机制来生成和更新数据的去中心化基础架构。去中心化、可验证、防篡改是其基本性质。

链式数据结构仅仅是区块链的存储结构。如何形成这样的存储结构、如何保证其可信、如何保证其安全性、如何保证分布式存储的一致性，都依赖于共识机制。因此，共识机制是区块链的灵魂，区块链的工作原理和应用场景都取决于其共识机制。

1.3　区块链的分类

区块链系统根据应用场景和设计体系的不同，一般分为公有链、联盟链和专有链。

1）公有链的各个节点可以自由加入和退出网络，并参加链上数据的读写；运行时以扁平的拓扑结构互联互通，网络中不存在任何中心化的服务端节点。目前，基于区块链的数字货币或智能合约平台均属于公有链的范畴，如比特币、以太坊等。

2）联盟链的各个节点通常有与之对应的实体机构组织，通过授权后节点才能加入与退出网络。各机构组织组成利益相关的联盟，共同维护区块链的健康运转。目前，企业界更多关注联盟链的搭建和使用。

3）专有链的各个节点的写入权限归内部控制，读取权限可视需求有选择性地对外开放。专有链仍然具备区块链多节点运行的通用结构，适用于特定机构的内部数据管理与审计。

2　共识机制

当前区块链技术所使用的共识机制主要分为以下 4 类：拜占庭容错算法（practical byzantine fault tolerance，PBFT），工作量证明（proof-of-work，PoW），权益证明（proof-of-stake，PoS）和授权权益证明（delegated proof-of-stake，DPoS）。

1）PBFT

PBFT 机制源于拜占庭将军问题，即拜占庭帝国军队的将军们需要一致决定是否攻击某一支敌军。由于拜占庭协议是基于实体之间的消息传递达成共识的，因而容易导致名为“女巫攻击”的攻击方法，即一个敌手控制或建立了许多恶意节点，如果敌手拥有足够多的恶意节点，就可以控制最终结果。一般认为，当网络中存在 f 个恶意节点时，整个网络有不少于 $2f+1$ 个诚实节点，才可以正常达成共识。在比特币系统中，参与方可以类比为将军，交易就是达成共识的过程。只有大部分参与方都承认交易的合法性，该交易才是有效的。

利用这类共识机制可以快速生成新的区块，达成不分叉的快速共识。但这类机制要求在一个封闭的节点集合中两两节点进行通信，因此比较适合于节点数量不多的联盟链和私有链。联盟链多采用技术成熟的 PBFT 机制及其相应的变种 RAFT 和 HBFT 等来达成共识，如 2016 年 Linux 基金会发起的开源超级账本（HyperLedger）、IBM 推出的 Fabric 基础设施项目等。

2）PoW

PoW 机制的核心思想是通过计算能力竞争的方式来保证数据一致性从而达成共识。在比特币系统中，各节点（即矿工）基于各自的计算机算力的相互竞争来解决一个求解困难但验证容易的 SHA 256 挑战，最快解决该难题的节点获得区块记账权，即该参与方创建了一个区块，所有其他参与方更新本地区块链。就女巫攻击而言，敌手需要控制大部分的计算能力，这比控制大部分节点更难，因此该机制从某种程度上保证了系统的安全性。PoW 机制的缺陷是存在资源浪费和女巫攻击等安全性问题。

在比特币之前，B-Money、Karma、RPOW、BitGold 或多或少地应用了 PoW 机制。当前，除比特币外，Litecoin、Dogecoin、MAVE-

PAY、FawkesCoin 等货币系统使用了改进的 PoW 机制。

3）PoS

PoS 机制要求货币持有者对某些数量的货币展示所有权。这种机制是基于“币龄”实现的，币龄被定义为交易输入大小和它存在时间的乘积。显然，长期持有货币的人拥有更多的币龄，从而也就拥有更大的权益，因此也更容易挖矿成功。由此可见，PoS 机制在一定程度上解决了 PoW 机制资源浪费的弊端，缩短了达成共识的时间。PoS 机制一方面解决了垄断问题，让“富者更富”转化成“穷者更容易富”；另一方面一定程度上缓解了51%攻击的威胁，如果敌手想要实行 51%攻击，则需要摧毁大量的币龄，这显然是不划算的。PoS 机制的缺陷在于最高权益节点拥有最终决定权。

当前，PPCoin、Nextcoin 等货币系统使用 PoS 机制。此外，也有不少货币系统对 PoS 机制进行了改进，其中最重要的一种改进就是 DPoS 机制。

4）DPoS

DPoS 机制主要基于“董事会决策”的思想，即每一个“股东”节点将其持有的股份权益授予某个“代表”节点，拥有股份最多的前 101 个“代表”节点组成“董事会”，轮流执行产生新区块的任务。这些“代表”节点可以获得相应的奖励，但是也必须缴纳保证金以保证其尽职尽责。一旦出现不称职的行为，股东们可以行使权力将其废除，并选取其他节点代行职责。通过此选举方式，系统中的每个节点均有选择其信任的授权节点的自主权，且轮流工作模式使得参与验证和记账的节点数量大大减少，从而达到快速共识的目的。

当前主要有 Bitshares 基于 DPoS 机制。

除以上 4 种经典的共识机制外，还存在一些变种机制。

1）股权速率证明（PoSV）。该机制解决了 PoS 机制中通过收藏货币来累加币龄的行为。PoSV 机制的原理为：如果货币进行了交易导致货币的币龄清零，则交易的货币的币龄上升速率将会高于不交易的货币的币龄上升速率，这在一定程度上鼓励了线上交易，减少了线下囤积的不利现象。

当前主要有 Reddcoin 运用 PoSV 机制对货币升值速率进行调整。

2）活跃度证明（PoA）。该机制对线上的活跃节点进行奖励。目前大部分的电子货币在“发行”之后就转为线下，从而减少了线上交易。PoA 机制中的矿工挖矿过程类似于 PoW 机制，当矿工找到新的区块时，会随机选择线上的 N 个活跃节点发送新发现的区块。前 $N-1$ 个活跃节点验证新发现的区块并签名，第 N 个活跃节点除了验证区块和签名外，还要对区块进行包装，并广播该区块。矿工和 N 个活跃节点都将因此收到奖励费用。如果 N 个活跃节点中有一个不活跃节点，那么它将不能对区块进行签名，从而不能收到相应的奖励费用。因此，PoA 机制可以有效地解决囤积货币的行为，在点对点的网络中有着很重要的应用。

PoA 机制的应用场景有 BitTorrent。

3）摧毁证明（PoB）。该机制解决了如何创建新货币的问题。与比特币由创世块（Genesis Block）声明该货币的产生不同，PoB 机制是通过一种可验证的方式来摧毁一种货币，建立和分配另一种货币。这种方式虽然很残酷，但却利用了 PoW 的思想，采用昂贵的资源防止了女巫攻击。随着货币的发展，旧的货币系统必然要升级到新的货币系统。升级的方式有两种：软分叉和硬分叉。软分叉是指新的货币系统在旧的货币系统中依然适用。硬分叉是指新的货币系统在旧的货币系统中不再适用，所有的客户端都需要升级；否则，两条不同的区块链将会出现。对于 PoB 机制而言，升级问题将轻而易举地得到解决，它可以通过摧毁货币对货币进行升级。

PoB 机制的应用场景有 Counterparty、Mastercoin 和 Permacoin 等。

4）中心化指定权限。在商业领域中，比特币的去中心化一直被作为“卖点”来宣传，但是如果我们可以相信一小部分拥有指定权限的人群，那么所有的共识问题都将变得简单，并且可以不用再考虑稳定性和计算能力浪费的问题。需要注意的是，拥有指定权限的人群需要执行诚实的行为，不诚实的行为不会为他们带来任何收益。拥有指定权限的人群需要利用网络进行选举或者由矿工指定，具体的安全

性有待讨论。MICALI 在 2016 年提出了名为 ALGORAND 的公共账本，其共识机制使用密码抽签（cryptographic sortition）的方式来决定出一部分人参与创建和验证区块。其中创建者称为 leader，由系统随机选择。leader 创建一个新区块，随机选择一个 verifier 集合，用以验证区块。

3 匿名与隐私保护

作为区块链技术最典型和最成功的应用，比特币在设计之初，创始人“中本聪”期望通过使用无限量的可以自由生成的交易地址来实现用户的匿名和交易的不可追踪，从而实现较强的隐私保护。然而，近几年的研究发现，由于区块链数据的公开性，因此通过分析大量的交易和网络数据，可以设计各类去匿名方案。区块链上的匿名与隐私保护面临巨大挑战。

我们以比特币为例，首先阐述目前基于区块链的数字货币中匿名和隐私保护面临的挑战；然后针对这些挑战，介绍目前的解决方案和研究进展情况；最后阐述新形势下的匿名和隐私保护问题。

3.1 匿名和隐私保护面临的挑战

1）推断交易地址归属在比特币交易中，如果两笔交易的接收方地址一致，那么可以肯定这两笔交易的接收方是同一人。为了防止这样的信息泄露，接收方可以每次使用一个全新的地址来接收比特币。然而，发送方的比特币金额很大程度上是分散在不同的交易输出中。因此，当单个交易输出金额不足以支付时，发送方不得不把多个交易输出金额合并作为输入金额。对于这种多输入交易，人们可以以高概率推断出多个输入属于同一人所有。

可以将整个交易历史看作一个巨大的有向图，图中节点代表不同的交易地址，有向边的始点为交易的发送方，终点为交易的接收方。由于比特币中交易数据的公开性，任何人都可以查看历史上的所有交易，针对交易图进行分析，获得交易地址间的关联信息，从而严重威胁用户隐私。

2）交易金额可见

在比特币交易中，交易金额是公开的，这是因为在矿工验证交易是否合法的过程中，需要根据交易金额进行交易合法性判定。然而，交易双方并不希望让其他人知道交易的具体金额。因此，如何在隐藏交易金额的同时，保证矿工能够对交易合法性进行判定，成为了客观需求。

3.2 现存的匿名和隐私保护方案

在保证交易金额的隐私性方面，比特币核心开发者 Greg Maxwell 首先正式提出了“机密交易”（confidential transactions）的概念，能够完全隐藏交易金额。该方案基于彼德森承诺和范围证明。在交易中发送方将盲化的交易数据（机密资金）发送给接收方，接收方可以验证交易金额。同样，接收方可以将接收到的机密资金用于一笔新的机密交易中。彼得森承诺可以隐藏交易中资金的具体数额，同时发送方需要向矿工提供零知识证明，证明交易输出的合法性。零知识证明可以保证矿工在不知道交易具体金额的前提下，对交易的合法性进行验证。

最初，Grey Maxwell 提出了混币方案 CoinJoin。该方案的具体思想如下：每个混币交易对应一个标准的多输入多输出比特币交易，其中每个输入金额相等。交易的输出对应参与者的接收地址，每个接收地址都可能接收任意一个交易输入。如果参与者发现自己的接收地址被包含进了该交易中，就选择对该交易进行签名。一旦所有参与者完成签名并写入比特币区块链中，混币完成。在外人看来，该方案不能通过交易的输入输出来断定输入输出的关联性，因而提供了外部不可关联性。但是对于参与者来说，该方案并没有提供不可关联性。

随后，为了避免单个 mix 节点偷窃和记录输入输出对应关系，BONNEAU 等人设计了混币（Mixcoin）协议，提出了“混币链”的概念。具体说来就是将多个 mix 节点串联起来，使得前一个 mix 节点的输出作为后一个 mix 节点的输入。只要有一个 mix 节点诚实，混币隐私就能得到保障。同时，该方案通过交易费激励机制，保障理性的 mix 节点诚实执行混币协议。

目前，数字货币达世币（DashCoin）就是基于 CoinJoin 和 Mixcoin 的思想。达世币中混币过程需要由主节点来完成。为了防止主节点作弊或被攻击，达世币引入链式混合和盲化的思想。链式混合指用户交易时随机选择多个主节点进行混

合，最后输出结果。盲化技术是指用户不需要将输入和输出发送到交易池，而是指定主节点将输入和输出传递到另一个主节点。这样，每一个主节点只看到所有执行过程中属于自己的部分，从而很难发现用户身份。

Ruffing 等人通过改进可追踪匿名群组通信协议 Dissent，设计出和比特币完全兼容的去中心化混币方案 CoinShuffle。该方案不依赖中心化节点，计算、通信开销小且无需手续费。

为了避免交易可链接，早期的解决方案多基于比特币原有结构，随后的一些增强方案提供了更为丰富的功能和特性，但这些方案要求对比特币系统进行升级，至少需要比特币系统进行软分叉。此后，很多人将目光投向设计匿名性和隐私程度更高的数字货币，通过将密码学工具，如承诺、环签名和零知识证明等引入数字货币，构造能够直接实现匿名和隐私保护的数字货币方案。目前来看，该类方案逐渐成为研究热点，比较典型的有 CryptoNote、Zerocoin 和 Zerocash。

CryptoNote 引入 Stealth Addresses 来实现接收方的外部不可见性。具体说来就是发送方通过接收方的公开信息生成一个随机地址，该地址允许接收方通过自己的秘密信息恢复相应的私钥。然而，发送方仍然可以获知接收方对货币的使用情况。为了解决这个问题，CryptoNote 引入环签名所提供的匿名集合来实现隐私保护。CryptoNote 协议通过一次环签名的方式，允许交易发送方将交易隐藏进一个容量为 k 的匿名集合中。同时，一次环签名能够提供一种链接机制，使得任何双花都能被检测。目前市值位列第 5 的门罗币采用的就是 CryptoNote 协议。除此之外，门罗币还提供了环状机密交易 RingCT 来隐藏交易金额和交易地址。

所有基于匿名集合的混币方案，无论是兼容比特币的方案，还是基于环签名的方案，本质上都是将真实的交易行为隐藏在匿名集合中。实际操作中，用户对匿名集合选取不当也会带来匿名和隐私保护问题。MILER 等人针对 Monero 交易的分析表明，80%的 Monore 交易是可链接的。

为了提供更高的匿名性，MIERS 等人提出了 Zerocoin 方案，该方案能够提供内置的不可链接性。该方案的匿名集合是系统中现存的所有 Zerocoin，允许用户将一个比特币通过“铸币”手段转化成一个 Zerocoin。当需要花费 Zerocoin 时，用户使用零知识证明的方法向矿工证明自己的 Zerocoin 存在于系统中且未花费过。

然而，Zerocoin 不能在原有的比特币系统中实现，需要比特币系统进行软分叉；Zerocoin 的币值金额是固定的，不能实现金额的任意切分；Zerocoin 不支持非交互交易且零知识证明过程过长。为了改善这种状况，SASSON 等人提出了 Zerocash 方案。

Zerocash 方案将密码学中非交互零知识证明技术 zk-SNARK 引入到数字货币中。Zerocash 方案保障了交易的不可链接和金额保密，且支持金额的任意切分。Zerocash 方案和比特币系统完全独立，支持 Zerocash 货币的直接交易，实现了当前最高程度的隐私保护和匿名性。然而，Zerocash 方案基于的零知识密码方案需要初始化秘密数据，任何知道该秘密数据的一方都可以凭空产生货币。基于 Zerocash 方案的新兴数字密码货币 Zcash 的秘密参数虽然是不同地点的 6 个人共同协作生成，但是到目前为止，这种生成方式仍然备受怀疑。

3.3 新形势下的匿名和隐私保护问题

3.3.1 离链支付协议中的隐私保护问题 为了解决公有链的可拓展性问题，很多研究着重于构造离链支付协议，如双向微支付通道、闪电网络和 Spirtes。这些方案中，双方交易达成需要借助中继节点的参与。然而，目前离链支付方案中，交易双方实体和交易金额是对中继公开的，中继知道了很多交易双方不想公开的内容。

针对离链支付协议的隐私保护问题，目前已经有一些研究在进行，如 HEILMAN 等人提出的 TumbleBit 方案。该方案能够将支付通道信息对中继隐藏。此外，TumbleBit 方案和比特币系统完全兼容。

GREEN 等人提出 Bolt 方案。Bolt 方案保障同一通道下的多重支付不能被链接在一起，即使密谋的个体之间也不能做到。且支付发生在毫秒级，不需要区块确认，接收方仅需要知道有人在他所提供的支付通道中进行了付款操作。支付

也可以被安排由第三方实现，避免了交易双方开关支付渠道的复杂性。Bolt 方案使得第三方不能从中作恶（即使第三方串通在一起也不能实现），同时交易的资金也是保密的。

对于支付协议的安全性，目前还存在许多亟待解决的问题。例如，在争端出现时，如何在不泄露争议双方最终金额信息的情况下进行调停；如何设计高效的隐私保护支付路由。目前关于保密支付协议的研究还在火热进展中。

3.3.2 现存区块链实现方案匿名和隐私保护的评估 很多密码协议在实现后，由于具体的实现细节，往往存在理论和实际不匹配的情况。例如，CryptoNote 协议通常假设将真实的交易隐藏到一个很大的匿名集合中，在基于该协议实现的 Monore 数字货币中，用户在选取匿名集合时，匿名集合往往很小，或者 Monore 交易通过非匿名方式执行。这些用户行为给去隐私和匿名分析带来可能。另外，以太坊 The DAO 被攻击事件之后，如何对智能合约代码进行自动审查和形式化验证也提上日程。因此，对现存区块链方案的安全性、隐私保护和匿名性的测量、分析和评估也是目前研究的热点。

3.3.3 其他公开问题 如何用安全多方计算生成 Zcash 的初始秘密参数，如何设计基于区块链的匿名方案，如匿名证书、匿名消息系统，都是下一步区块链匿名、隐私保护的研究热点。此外，目前公有链上隐私保护的研究已经全面展开，联盟链上的隐私保护仍有大量问题值得研究。例如，在联盟链中，业务信息是否可以加密，加密后如何保证运算、如何保证检索、如何进行权限控制等。

4 结束语

区块链作为支撑比特币运行的核心技术，由于其去中心化、可验证、防篡改等特性，已迅速成为各界关注的热点，相关研究呈现蓬勃发展之势。然而，基于区块链的数字货币在共识效率及隐私保护等方面仍然存在较多问题。本文探讨了数字货币中区块链的工作原理，介绍了区块链技术所使用的各类主流共识机制及其变形，并对基于区块链的数字货币中匿名和隐私保护问题进行了深入分析。■

【作者单位：山东大学软件学院；山东师范大学信息科学与工程学院】

（摘自《信息网络安全》2017 年第 7 期）