专题：区块链

区块链技术概览

杨白雪 卿苏德 张启 魏凯

摘要：区块链技术是多种技术融合再创新的结果。随着各界区块链的关注度居高不下，区块链技术也成为热点。由于涉及到的技术多而复杂，区块链技术的门槛一直比较高，不利于区块链技术的传播和普及，也造成了一定的行业乱象。本文结合主流开源区块链项目，对区块链涉及的账本结构、共识机制、证书机制、P2P协议等多种技术进行了总结归纳，并对区块链特征的产生从技术视角进行了剖析，旨在阐明区块链技术的本质，厘清区块链技术的逻辑，促进区块链技术的落地。本文研究结果对区块链从业者和区块链技术深入学习有参考价值。

关键字：区块链；点对点网络；共识算法；块链式结构；密码学

1 引言

2009年，中本聪发表《比特币：一种点对点的电子现金系统》，开创了区块链技术的先河。在10年中，以太坊、超级账本、R3corda等区块链技术纷纷兴起，引发了巨大的社会关注，聚集了大量的资本和先进技术。区块链被称为“创建信任的机器”、“新一代互联网基础设施”、“颠覆性技术”。区块链快速发展的过程中，社会对区块链技术的认识依然不到位。区块链技术是如何创造信任机制的？区块链可以看作可信的分布式数据库，用P2P网络通信机制、块链式账本存储机制、密码机制、共识机制4大核心机制，保证了系统的分布式特性、不可篡改特性、不可抵赖特性，使区块链系统“诚实”而“透明”，在应用中具有大范围、跨主体、高效率、低成本的特点。

由此可知，区块链技术是多种技术融合再创新的结果，本文就区块链系统涉及到的技术进行阐述，并说明这些技术在区块链中是如何应用的，以及达到的效果。

2 区块链技术概述

区块链是多种技术融合再创新的成果，其技术包括：P2P组网技术、块链式账本结构、共识机制、数字签名、加密机制、隐私保护机制等，这些技术各司其职，形成了区块链系统的分布式数据库、多方协作、公开透明、不可篡改、不可抵赖等特性。

●P2P组网是区块链系统启动的第一步，是区块链的通信基础。区块链运行在P2P网络上，是区块链“分布式”特性的来源。

●账本结构是区块链的核心，块链式的账本结构是区块链“不可篡改”特性的来源。

●共识机制是区块链的灵魂，通过算法协调系统各参与方，最终达成一致，是区块链系统“多方协作”特性的来源。

●签名机制是区块链的通行证，通过数字签名算法给系统各参与方分派数字证书，是区块链系统“不可抵赖”特性的来源。

●隐私机制是区块链实现私有信息保护和内容公开的途径，通过加密算法加密当事人身份，匿名参与系统，内容公开的同时隐藏当事人身份，保障参与方隐私，是区块链系统“公开透明”特性的来源。

3 组网方式—P2P协议

对等网络（Peer-to-Peer，P2P）被认为是代表无线宽带互联网未来的关键技术，其具有3大特征：自治性，

相比中央服务器而言；分布性，利用网络边缘的资源，如存储/计算能力和信息资源；动态性，网络边缘的资源处在动态的变化中，不断有新的资源加入和已有的资源退出。P2P因为节点信息存储与搜索方式的不同，分为结构化覆盖网络和非结构化覆盖网络两类。在分布式网络中，目前没有完美的解决方案，二者各有侧重。

（1）Bitcoin——非结构化的P2P覆盖网络（Non-Structured P2P Overlay Network）

在非结构化的覆盖网络中，每个节点存储自身的信息或索引。当某节点用户在P2P系统中进行查询时，该节点没有其他节点的信息和知识。例如最简单的泛洪式查找（类似于广播）和扩展环查找（从最近的n个节点开始，层层转发直到找到目标或超出了跳数的上限为止）。

在非结构化P2P系统中，实现结构简单、无中心、节点之间完全平等、网络层次单一、节点之间无需维护拓扑信息，同时搜索算法带有一定的盲目性。

Bitcoin采用的通信协议Gossip协议就是非结构化的覆盖网络，完全基于TCP协议构建，主网端口为8333。

（2）Ethereum——结构化的P2P覆盖网络（Structured P2P Overlay Network）

在结构化P2P系统中，每个节点只存储特定的信息或特定信息的索引。当用户需要在P2P系统中获取信息时，他们必须知道这些信息（或索引）可能存在于哪些节点中。由于用户预先知道应该搜索哪些节点，避免了非结构化P2P系统中使用的泛洪式查找，因此提高了信息搜索的效率。

以太坊采用的通信协议是Kademlia协议，这是一种结构化P2P网络，提供UDP和TCP两种通信方式，节点发现是基于UDP的，节点的数据交换是基于TCP的。主网TCP端口为30303，推荐UDP端口30301。

4　账本结构

区块链系统的账本以区块链为单位，以特定算法获取上一区块链的特征嵌入下一个区块，连缀成链。区块链的名称即来源于此。区块链的账本结构是区块链系统最大的创新点，涉及到哈希算法、默克尔证明等技术。

（1）哈希函数（Hash Function）

哈希函数也叫散列函数、摘要函数，是一个把任意长度的数据映射成固定长度数据的函数。任何一种能将任意大小数据映射为固定大小数据的函数，都能被称为散列函数。哈希函数的返回值被称为哈希，也被称为散列值、摘要。

哈希函数有如下特性：一是消息的长度不受限制。二是确定性：对于相同的输入，使用同一哈希函数，它始终生成相同的哈希值，如果两个哈希值是不相同的，那么这两个哈希值的原始输入也是不相同的。虽然对于不同的输入可能会哈希成相同的输出（哈希碰撞），但是哈希碰撞的概率可以非常小，所以一般从哈希值来确定唯一的输入值。三是均匀性：良好的哈希函数应该输入尽可能均匀的映射到输出范围上。四是单向性：在加密应用程序中，哈希函数实际上是不可逆的，为加密和验证信息完整性而设计的哈希函数（又被称为单向散哈希函数或者消息摘要函数），对于给定的哈希值，没有有效方法可以反向计算出原始输入，因此很难伪造（见图1）。

（2）默克尔证明（Merkel Proof）

●Bitcoin的默克尔证明

Merkle Proof最早的应用是Bitcoin，它是由中本聪在2009年描述并创建的。Bitcoin的Blockchain利用Merkle proofs来存储每个区块的交易。而这样做的好处是中本聪描述到的“简化支付验证”（Simplified Payment Verification，SPV）的概念：一个“轻客户端”（Light Client）可以仅下载链的区块头即每个区块中的80字节的数据块，仅包含5个元素（上一区块头的哈希值，时间戳，挖矿难度值，工作量证明随机数nonce，包含该区块交易的Merkle Tree的根哈希），而不是下载每一笔交易以及每一个区块。

如果客户端想要确认一个交易的状态，它只需简单地发起一个Merkle Proof请求，这个请求显示出这个特定的交易在Merkle Trees之中，而且这个Merkle Tree的树根在主链的一个区块头中。

一个比特币轻客户端中至少会有一个节点会通知你关于你的地址中任何特定的交易支出。然而一笔交易的确切性质（Precise Nature）可以取决于此前的几笔交易，而这些交易本身又依赖于更为前面的交易，所以最终必须验证整个链上的每一笔交易。为了解决这个

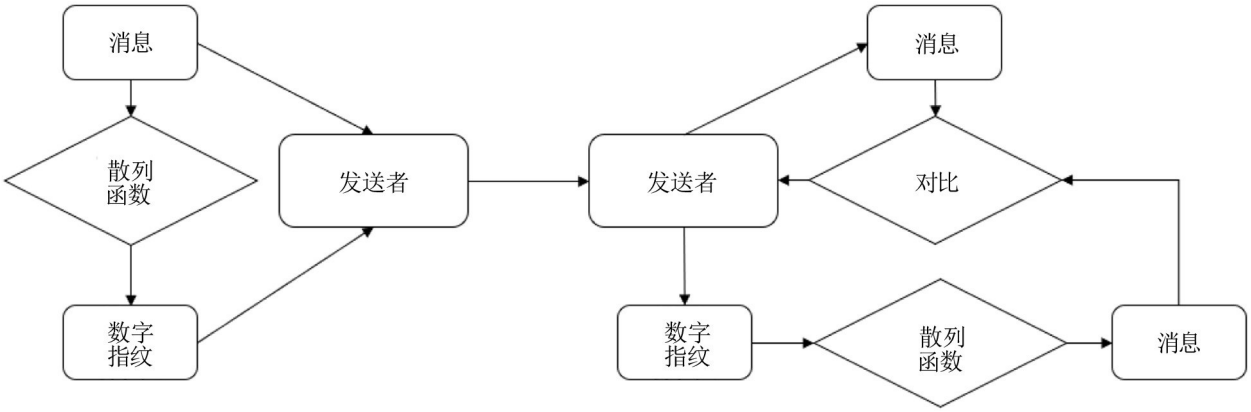

图1 哈希校验过程

问题，Ethereum的Merkle Tree概念会更进一步。

●Ethereum的默克尔证明

每个以太坊区块头不是包括一个Merkle Root，而是为3种对象设计的3棵树：交易（Transaction）、收据（Receipts）和状态（State）。

对于验证属于列表格式的信息而言，二叉Merkle Tree是非常好的数据结构。对于交易树来说二叉树也是可行的。但是，对于状态树情况会更复杂些。以太坊中的状态树基本上包含了一个键值映射，其中的键是地址，而值包括账户的声明、余额、随机数Nounce、代码以及每一个账户的存储。不同于交易历史记录，状态树需要经常地进行更新：账户余额和账户的随机数Nonce经常会更变，更重要的是，新的账户会频繁地插入，存储的键（Key）也会经常被插入以及删除。我们需要这样的数据结构，它能在一次插入、更新、删除操作后快速计算到树根，而不需要重新计算整个树的Hash。Ethereum所使用的Merkle Tree称之为“默克尔·帕特里夏树”（Merkle Patricia Tree），这种数据结构有两个非常好的特征：一是树的深度是有限制的，即使考虑攻击者会故意地制造一些交易，使得这颗树尽可能地深。不然，攻击者可以通过操纵树的深度，执行拒绝服务攻击（DDoS Attack），使得更新变得极其缓慢。二是树的根只取决于数据，和其中的更新顺序无关。换个顺序进行更新，甚至重新从头计算树，并不会改变根。

5 共识机制

共识机制本质上是控制参与方的数据一致性。

（1）权益类共识

拼算力共识PoW（Proof of Work）在区块中递增一个Nonce值，并针对每次的Nonce计算整个区块的哈希值，直到找到一个哈希值，该值满足所要求的零比特位数量，该节点获得打包权限，所有节点同步该节点打出的区块。在这种算法中，没有比遍历更快的方法找到符合要求的哈希值，因此，遍历速度是获得符合哈希值的重要参数，可以用简单运算硬件加速，如GPU或其他专用芯片。此算法有一定的偶然性，算力高的节点获得打包权的几率上升，但并不是一定获得打包权。这种共识机制去中心化程度较高，安全性较强，但资源消耗大，需要代笔作为激励机制维持系统健康运行。

拼权益共识PoS（Proof of Stake）、DPoS（Delegates Proof of Stake）以抵押资产的多少来分配获取打包权的概率，这在一定程度上缩短了共识达成的时间，不再需要大量消耗能源去竞争记账。这种共识去中心程度较弱，有可能出现寡头优势，安全性相比PoW较弱。同时DPoS节点代理是人为选出的，公平性相比PoS更低。

（2）拜占庭类共识

●拜占庭问题（Byzantine Question）

拜占庭问题是当一群参与方中，有不超过一定数目的恶意方发送欺骗消息时，参与方总体能通过三轮投票，做出正确的决定。拜占庭问题能容忍不高于参与方总数1/3的恶意方。

●拜占庭共识（Practical Byzantine Fault Tolerance，PBFT）

PBFT是一种基于消息传递的一致性算法。该算法经过3个阶段：预准备（Pre-prepare）、准备（Prepare）和确认（Commit）达成一致性，以计算为基础，也无需代币奖励。由链上所有人参与投票，少于（N-1）/3个节点反对时就获得公示信息的权利。拜占庭共识算法的可靠性有严格的数学证明，具备（N-1）/3容错性。当有1/3或以上记账人停止工作后，系统将无法提供服务，此外拜占庭共识经过三个阶段的投票，对通信资源消耗较大，随着节点规模扩增，通信量指数级增加。

●分布式数据一致性共识

这类共识机制在联盟链应用广泛，采用分布式数据库的一致性算法，在信任环境中使用RAFT或Kafka来控制区块链参与方的数据一致性。

这类共识机制无分叉可能、无交叉验证、通讯量小，但是仅能运行在可信环境中，对关联交易支持有限，区块链特性较弱。

6　证书机制

（1）数字签名

区块链系统使用数字签名机制来实现不可篡改、不可抵赖的重要特征。在区块链系统种，除了保证数据内容的完整性之外，还需要确保数据来源的可认证性（身份识别）和数据发送行为的不可否认性（防止抵赖行为）。

任何一个公钥密码体系都可以单独作为一种数字签名方案使用，流程如下：发送方使用私钥对消息原文做签名（加密）处理，生成出消息原文的“数字签名”，然后将消息原文连同它的数字签名（即加密后的消息密文）一起发送给接收方。然后接收方使用公钥对接收到的消息密文做解密处理，并将公钥解密后的消息与原来的消息进行比较。

如果需要对所有信息原文进行加密操作，效率是非常低的。常用的数字签名算法可以看做是一种带有密钥的消息摘要算法，并且这种密钥包含了公钥和私钥，也就是说，数字签名算法是非对称加密算法和消息摘要算法的结合体。几乎所有的数字签名方法都要和快速高效的哈希算法搭配，才能成为有效的数字签名方案。

（2）数字身份和认证

系统参与方的数字身份通过数字证书来管理，数字证书（Digital Certificate）是经认证中心授权颁发并经认证中心数字签名的包含公开秘钥拥有者及公开秘钥相关信息的电子文件，可以用来判别数字证书拥有者身份。

数字证书包含：公钥、证书名称信息、签发机构对证书的数字签名以及匹配的私钥。证书可以存储在网络中的数据库中，用户可以利用网络彼此交换证书，当证书失效后，签发此证书的认证中心仍存档此证书的副本。认证中心（Certificate Authority）一般是一个公认可信的第三方机构，其作用主要是为每个用户颁发一个独一无二的包含名称和公钥的数字证书。

7　加密机制

加密简单而言就是通过一种算法手段将对原始信息进行转换，信息的接收者能够通过秘钥对密文进行解密从而得到原文的过程。按照加密方和解密方秘钥相同与否可以将加密算法大致分为3种类型。

（1）对称加密

对称加密的加密解密方使用相同的秘钥，这种方式的好处在于加解密的速度快但是秘钥的安全分发比较困难。

（2）非对称加密

非对称加密体系也称为公钥体系，加解密时加密方拥有公钥和私钥，加密方可以将公钥发送给其他相关方，私钥严格自己保留。例如银行的颁发给个人用户的私钥就存储在个人的U盾里；非对称加密可以通过私钥加密，他人能够使用公钥进行解密，反之亦然；非对称加密算法一般比较复杂执行时间相对对称加密较长；好处在于无秘钥分发问题。常见的非对称加密算法有RSA、ECC，区块链中主要使用ECC椭圆曲线算法。

（3）对称加密与非对称加密的结合

这种方式将加密过程分为两个阶段，阶段一使用非对称加密进行秘钥的分发使得对方安全地得到对称加密的秘钥，阶段二使用对称加密对原文进行加解密（见表1）。

8　隐私保护机制

区块链系统尤其是非许可类区块链，其交易内容是公开透明的，需要附加隐私保护机制来保证参与方

表1 加密算法类型

加密类型	名称	计算方式	复杂度	速度	强度
非对称	RSA	基于可逆模幂运算	亚指数级	中	取决于因式分解难度
	ECC/SM2	基于椭圆曲线算法	指数级	快	ECDLP 数学问题
对称	AES	RIJNDAEL 算法		快	较高
	SM4	迭代和线性变换	32	快	较高
	DES	逻辑算法	48	慢（可硬件加速）	较高

的隐私权。通常采用的策略有3种：一是基于事务隔离的策略，主要面向分片、多链、多通道等模式；二是基于隐私保护算法的策略，多种开源非许可链采用的模式；三是基于应用层权限控制的策略，许可类区块链采用的模式。

（1）事务隔离

事务隔离是一个事务使用的资源或数据与其他事务相隔离。在区块链中，基于隔离的隐私保护策略将不同参与方或不同类型的业务隔离开，使不同参与方或不同类型事务中的数据部分共享，以此达到简单的隐私保护的目的。以太坊采用的分片机制、超级账本采用的多通道机制以及Corda的见证人机制，都属于这个范畴。

基于隔离的隐私保护策略具有一些优点：思路简单，实现较容易；数据隐私性好，硬隔离的机制使数据保护安全等级较高。这种简单的隔离机制也有一些不足：数据共享性差，硬隔离的机制使数据共享变得困难；互操作性差，同样的参与方对于不同的业务，或者不同参与方对于同一业务，因为隔离的原因，互操作性受到影响。

（2）隐私保护算法

基于隐私保护算法的策略主要是保护参与方的私密信息不被明文获取。实现方式有挖矿、同态加密、零知识证明、环签名等多种方式。这种策略的内容保护指向性更好，更便于互操作性和日后可能的互联互通，但是实现难度较大，容易出现安全漏洞，也存在一定的监管风险。

●挖矿

将来自多个用户的货币混在一起，再将它们分成较小的量，然后将钱重新分配给预期的接收者，将交易历史随机化。比特币采用了这种策略。

●环签名

用来隐藏交易的发送地址。使用环形签名可以使交易拥有多个发送者，而其中只有一个是真的。仅仅通过查看环签名不可能辨别是哪个地址发起并最终签署了交易。门罗币采用了这种策略。

●同态加密

允许在加密数据上进行计算，而无需将密文数据先解密。这意味着可以在对其执行计算时保护数据的隐私性和安全性，不必揭示数据的内容就可以使用它来证明关于一组数据的陈述。只有具有相应解密密钥的用户才能访问数据或交易的详细信息。

例如零知识证明用于对加密的交易数据执行加密验证，在保证数据私密性情况下，使发送者和交易额被证明是合法的。Zcash采用了这种策略。

（3）应用层权限控制

在许可类区块链中，通过隐藏底层链入口，来实现数据分类分级管理，进而通过控制数据访问权来达到隐私信息保护的目的。这种策略简单、容易实现，主要依赖于应用层控制，根据业务场景的适应性好。但是这种策略仅适用于许可类区块链，而且性能受密码学算法的影响。

9 总结与展望

从发展历程来看，区块链技术依旧处于较初期的发展阶段，技术还在进行快速的迭代和演进。区块链在社会应用中有广泛的前景，但是区块链人才依旧比较缺乏，区块链与实体经济的融合还比较初步。本文系统梳理了研习区块链技术所需要的技术储备，介绍了多种技术在区块链系统中的角色，以期为希望深入研究区块链技术或区块链从业者提供启发和借鉴。

参考文献

[1] Satoshi Nakamoto, Bitcoin：a peer-to-peer electronic cash

system[EB/OL].(2008)[2018-03-15].https: //bitcoin.org/bitcoin.pdf.
[2] Vitalik Buterin. Ethereum white- paper[EB/OL]. (2014)[2018- 05- 20].https: //github.com /ethereum /wiki /wiki /White-Paper#applications.
[3] Hyperledger. Hyperledger fabric transaction flow[EB/OL]. (2006) [2018- 06- 30].http: // hyperledger- fabric.readthedocs.io/en/latest/txflow.html.
[4] Vitalik Buterin. Merkling in bitcoin[EB/OL]. (2014)[2018-06-05].https://blog.ethereum.org/2015/11/15/ merkling-in-ethereum/.
[5] 中国信息通信研究院. 区块链(2018)[EB/OL]. (2018-09)[2018-09-09].http://www.caict.ac.cn / kxyj / qwfb/bps /201809/P020180905517892312190.pdf.
[6] 洒脱喜. 谈谈以太坊的Merkle树[EB/OL]. (2015-11-23)[2018-06-01-10].http://www.8btc.com/merkling-in-ethereum.
[7] 数字证书认证系统密码协议规范. GM/T 0014-2012 [S].北京:中国标准出版社.
[8] 维基百科. 默克尔树[EB/OL]. (2016)[2018-05-05].https://en.wikipedia.org/wiki/Merkle_tree.
[9] 维基百科. 哈希函数[EB/OL]. (2016)[2018-05-05].https://en.wikipedia.org / wiki / Hash_function # Hash_function_algorithms.
[10] 梁成仁, 李健勇, 黄道颖, 等. 基于 Merkle 树的 BT 系统 torrent 文件优化策略[J]. 计算机工程, 2008, 34(3): 85-87.
[11] A. Rowstron and P. Druschel. Storage management and caching in PAST, a large-scale, persistent peer-to-peer storage utility [J].In Proc. ACM SOSP,01, Banff, Canada, Oct. 2001.

作者简介：

杨白雪 中国信息通信研究院云计算与大数据研究所工程师
卿苏德 中国信息通信研究院云计算与大数据研究所高级工程师
张启 中国信息通信研究院云计算与大数据研究所工程师
魏凯 中国信息通信研究院云计算与大数据研究所大数据部主任

Overview of blockchain technology

YANG Baixue, QING Sude, ZHANG Qi, WEI Kai

Abstract: Blockchain technology is the integration and innovation of multiple technologies and it has also become a hot spot with the attention from various aspects. Due to the complexity of the technologies involved, the threshold of blockchain technology has been relatively high, which is not conducive to the spread and popularity of blockchain technology. This paper summarizes of the structure, consensus mechanism, certificate mechanism, P2P protocol and other technologies involved in the blockchain according to the mainstream open source blockchain projects, and analyzes the features of blockchain from a technical perspective. Besides,it aims to clarify the characteristics of blockchain technology, the logic of blockchain techno logy, and promote the practical of blockchain technology. The conclusion of this paper have reference value for the in-depth study of blockchain practitioners and blockchain technology.

Key words: blockchain; P2P; consensus; blockchain structure; cryptography

（收稿日期：2018-12-22）

中国电信与中国邮政签署战略合作协议 深化战略合作

12月21日，中国电信集团有限公司（以下简称中国电信）与中国邮政集团公司（以下简称中国邮政）签署战略合作协议。中国电信董事长杨杰、总经理柯瑞文、副总经理陈忠岳，中国邮政董事长刘爱力、总经理张金良、副总经理张荣林出席签约仪式。中国电信总经理柯瑞文、中国邮政总经理张金良代表双方签署协议。

中国电信和中国邮政作为大型国有企业，在各自领域拥有资源、业务和服务优势，本着“资源共享、优势互补、合作共赢、共促发展”的原则，双方深化战略合作伙伴关系，在基础设施与通信服务、金融业务、渠道网点、大数据及物联网、新技术开发、资本运作、寄递物流等领域推动深层次合作，不断推进双方技术创新、服务创新与商业模式创新，将全面、长期和稳定的战略合作伙伴关系落到实处。