信息安全研究 第2卷 第12期 2016年12月
Journal of Information Security Research Vol.2 No.12 Dec. 2016

区块链关键技术中的安全性研究

朱 岩[1] 甘国华[1] 邓 迪[2] 姬菲菲[2] 陈爱平[2]
[1](北京科技大学计算机与通信工程学院 北京 100083)
[2](北京太一云科技有限公司 北京 100102)
(zhuyan@ustb.edu.cn)

Security Architecture and Key Technologies of Blockchain

Zhu Yan[1], Gan GuoHua[1], Deng Di[2], Ji Feifei[2], and Chen Aiping[2]
[1](*School of Computer & Communication Engineering, University of Science & Technology Beijing, Beijing* 100083)
[2](*Beijing Taiyiyun Technology Ltd, Beijing* 100102)

Abstract Blockchain, both the cryptocurrency and the underlying Bitcoin technology, have attracted significant attention around the world. The reason is that blockchain is a decentralization technology with Consensus-Trust Mechanism (CTM), which is obviously different from the traditional centralization system with Outer-Trust Mechanism (OTM). This has made a great influence on the trust mechanism of people and promoted the usage of security technology in the blockchain. In this paper, we present the security architecture and key technologies of the blockchain, and explain how the blockchain ensure the integrity, non-repudiation, privacy, consistency for the stored data through P2P network, distributed ledger, asymmetric encryption, consensus mechanism and smart contracts. Moreover, we analyze some new security threats and measures, for example, the preventing technology of Denial of Service (DoS) attack against the Transaction Storm (TS), the cryptographic access control (CAC) technology to enhance the data privacy, the key management technology against losing-and-stealing of digital asset, and so on. We also discuss the future security problems and technologies that might be discovered after the blockchain syncretizes new technologies, including, AI, Big Data, IOT, cloud computing, mobile Internet technologies.

Key words blockchain; distributed ledger; P2P network; asymmetric encryption; consensus mechanism; smart contracts

摘 要 区块链技术作为密码货币和比特币的底层技术，正在吸引着越来越多的人员投入进来.有别于传统信息系统的中心化他信机制，区块链是一种去中心化或者多中心化的共信机制，这对人们的信任机制产生了很大的影响，并促使人们开始重视区块链中的安全技术.对区块链中的关键技术及其安全架构展开了研究，阐述了区块链如何通过P2P网络技术、分布式账本技术、非对称加解密技术、共识机制技术、智能合约技术来实现对其数据完整性、不可否认性、隐私性、一致性等的安全保

收稿日期:2016-10-03
基金项目:国家自然科学基金面上项目(61472032,61170264)

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

护.此外,也对一些新的安全威胁和措施进行分析,例如,防止由于交易风暴引起的拒绝服务技术、保护区块链信息隐私的密文访问控制技术、以及防止因为密钥丢失或者泄露所引起的数字资产丢失或者被盗的密钥管理技术等等.也对区块链技术与人工智能、大数据、物联网、云计算、移动互联网技术相融合之后可能出现的新安全问题和安全技术进行了探讨.

关键词 区块链;分布式账本;P2P 网络;非对称加密;共识机制;智能合约

中图法分类号 TP393.08

当以云计算、大数据、物联网等技术为代表的新一代信息技术正在各个领域中得到广泛的应用时,区块链[1]技术作为又一项重量级信息技术越来越引起人们的关注,从早期的极客社区到创新企业、从科技巨头到跨境联盟,乃至各国央行和政府纷纷投入区块链技术的研究和应用实践中来.

目前,人们对于区块链技术的内涵理解基本能够保持一致,即区块链技术是一种基于密码学原理的分布式 P2P 网络共信智能账本技术,中国区块链技术和产业发展论坛编写的《中国区块链技术和应用发展白皮书》[2]将区块链定义为:分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式.一般认为区块链技术整合了以下几点关键技术[3-4]:1)P2P 网络技术;2)分布式账本技术;3)非对称加密技术;4)共识机制技术;5)智能合约技术.所有这些关键技术的引入或发明都是为了将区块链技术打造成一个开放公正、安全可靠、高效智能的新一代信息处理技术,其中,安全可靠又是这些技术所重点考虑的关键.本文就这 5 个方面关键技术中的安全性进行分析研究,阐明区块链技术是如何实现对整个区块链网络的健壮性、容错性以及对网络中传输和保存的信息数据的完整性、一致性、真实性、不可否认性和隐私性进行保障的[3,5-11].

1 P2P 网络技术

比特币系统之所以能够从 2009 年一直稳定运行到现在,是与其采用了 P2P 网络技术密不可分的.相比较传统的客户机/服务器模式的信息系统而言,采用 P2P 网络结构的系统具有去中心、容错健壮、隐私保护、负载均衡等特点.按照设计思想、网络体系结构以及出现时间,可以将 P2P 网络分为 3 种类型[4].

1) 第 1 代混合式 P2P 网络.实际上是 C/S 模式与 P2P 思想结合的产物,由 1 台或多台服务器来记录节点索引表,网络中各节点从索引服务上查询目标节点的地址之后,直接与目标节点建立联系,典型代表有 Napster 和 BitTorren,这种 P2P 网络由于本质上还是 C/S 结构,存在可靠性、安全性、扩展性、性能瓶颈等问题.

2) 第 2 代无结构 P2P 网络.取消了索引服务器,各节点随机接入网络,地位相同,与邻居节点构成逻辑覆盖网络,通过邻居节点的接力来找到目标节点,并记录路径,防止环路.典型代表有 Gnutella 和 KaZaA.这种 P2P 网络由于采用洪泛的方式来广播消息,需要耗费大量网络资源,并且效率低下,准确性不高.

3) 第 3 代结构化 P2P 网络.为解决快速定位问题,采用 DHT(distributed Hash table)技术来构建 P2P 网络[12],每个节点只需要记录有限节点信息,取消了洪泛算法,有效减少消息发送量,从而提高了目标节点的查找效率和准确性.典型代表有 Chord,CAN,Tapestry,Pastry,Kademlia 以及常数度模型 Viceroy,Koorde 和 Cycloid.

已有研究表明,现实网络具有小世界模型[13]的特征:1)特征路径平均长度较小,即网络中任意 2 个节点之间的连接边数较小,研究统计表明该平均长度为 6;2)聚合系数较大,即近邻节点的聚合程度比较大.小世界模型的 P2P 网络结构如图 1 所示.

图 1 中,网络上的节点会组成一个个的簇,所有这些簇组成整个网络,每一个簇中有若干普通节点和一个簇首节点,其中普通节点主要记录了簇内节点信息,而簇首节点不仅记录了簇内节点的信息,还记录了其他簇首节点的信息.每一个节点在查找目标节点时[14]均优先在簇内查找,没有找到就会通过簇首节点来到其他簇中去查找.簇首节点并不是固定不变的,根据节点的能力贡献

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

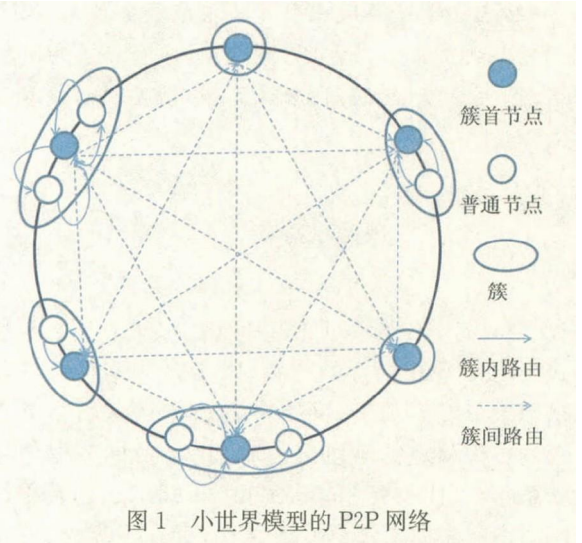

图1 小世界模型的P2P网络

以及其他一些随机因素，例如：节点加入、节点退出、节点变更等，簇内节点的角色和数量以及整个网络中的簇的组成与数量均发生着动态的变化.

同其他现实中的P2P网络一样，区块链网络也可以遵循小世界模型来设计和运行. 按照节点是否参选记账，可以将区块链节点分为非记账节点和候选记账节点. 其中，非记账节点可以从事交易活动和验证活动，候选记账节点则需要依据设定的共识算法来努力成为记账节点并执行记账活动，否则参与验证活动. 一旦记账节点得以产生，其他交易节点需要将交易信息发送给记账节点，以便记账节点打包生成区块并加入到区块链中. 在交易节点发送交易信息到记账节点的这个过程遵循的就是小世界模型的原理，每一条交易信息并不是通过洪泛的方式广播到区块链中的所有节点之上，而是就近发送给临近的簇首节点，然后由簇首节点广播给候选记账节点. 由于簇首节点是动态的、簇的组成和数量也是动态的，因此，并不能事先进行预测. 同时，由于小世界模型能够保证在节点变动（加入、退出、变化）的情况下，动态维持整个网络的稳定性，从而保证了区块链网络的健壮性，进而保证了区块链上的交易数据的完整性和一致性.

2 分布式账本技术

区块链与传统数据库的一个最大的区别就是传统的数据库提供对数据的增、删、改、查4种数据的基本操作，但是在区块链中却只有增加和查询2个操作，没有修改和删除操作. 传统数据库分为中心化数据库和分布式数据库，分布式数据库的基本思想是将原来集中式数据库中的数据分散存储到多个通过网络连接的数据存储节点上，以获取更大的存储容量和更高的并发访问量. 区块链被认为是一种分布式账本技术，与分布式数据库一样都是分布式的，但两者之间在存储方式和数据结构上存在不同.

1）存储方式

数据的存储方式可以分为集中式、分割式、复制式以及混合式. 集中式就是将所有数据都存储在同一个存储空间中. 分割式指的是将数据分割成固定大小或者不固定大小的块状，分别存在不同的存储空间，按照分割的维度，可以分为水平分割和垂直分割. 水平分割指的是按照某个条件对数据进行分割，每一个数据块都具有相同的数据属性信息，例如：在分布式数据库的每一个数据中心都具有相同的数据库表结构，但在存储数据时可能按照一定条件来选择存储空间，如按照地域. 垂直分割指的是按照数据属性对数据进行分割，每一块数据值包含有部分数据属性信息，例如在一个三中心的分布式数据库中，一个存放用户信息，一个存放业务信息，第3个存放日志信息.

复制式指的是同一份数据在分布式数据库中有1个或者多个备份，分别存在不同的数据存储空间中. 复制式还可以细分为全复制和部分复制，全复制指的是同一份数据在所有数据存储空间中都有备份，部分复制指的是同一份数据只在部分数据存储空间中有备份. 全复制拥有最高的数据存储可靠性，但太浪费空间，部分复制可以根据需要设定备份数量.

混合式是将分割式和复制式混合起来使用，首先是对数据进行分割，然后根据需要对所有分割的数据块进行复制，并将这些数据块分别存放到不同的数据存储空间中，同一数据存储空间不存在相同的数据块备份. 区块链的数据存储可以认为是一种混合模式，首先按照时间间隔打包封装成数据块，然后同步到所有区块链网络节点，每一个节点上拥有相同的数据，是水平分割的全复制存储方式，虽然有些区块链会允许某些节点为节省空间只存储部分数据块，但这并不影响区块

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

链的存储方式. 区块链的这种数据存储组织方式保证了数据的完整性和不可篡改性，并且还可以提高数据查询的效率.

2) 数据结构

传统数据库分为结构化数据库(如 my sql, MS SQL Server, Oracle, DB2 等)和非结构化数据库(也称 nosql 数据库，如 hadoop, mongoDB 等)，区块链的结构可以分 3 个层次来描述[1]，首先是链，然后是区块，最后是交易，同一个时间周期中的交易组成了区块，按时间顺序将区块链接起来就形成了区块链，以下图 2～4 分别对链、区块链、交易的数据结构进行了描述.

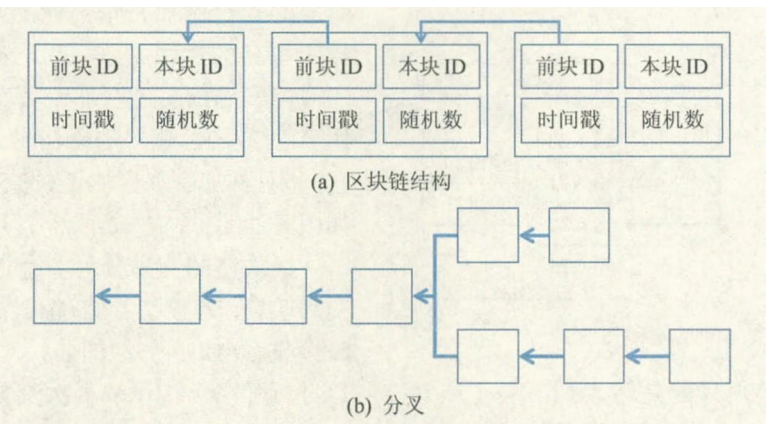

图 2　区块链结构

图 2(a)描述的是链的结构. 每一段时间内的数据组成了一个数据块，除了本身有一个 hash 值形式的 ID 之外，还记录了上一个区块的 ID，这样就能够将这些按照时间顺序生成的数据块链接起来形成一个链表. 在区块链的实际运行中可能存在分叉的现象，即同一时刻产生了 2 个区块，都指向了前一个区块，如图 2(b)所示. 区块链技术通过共识机制来解决分叉问题：哪条分支被接受的节点更多，那条分支即为主分支，其他分支被抛弃，不同区块链的共识机制需要不同的区块周期来确认主要分支，比特币是 6 个区块周期就可以确定主要分支. 区块链的这种链式结构保证了整个网络上的区块数据的一致性，从而维护了区块链上的数据安全.

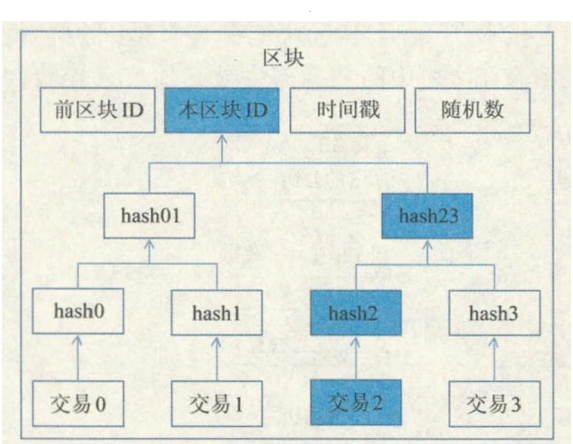

图 3　区块的内部结构

图 3 所示为区块的内部结构. 所有交易信息按照默克尔树的结构组织起来，在树的最底端，每一个交易经过哈希之后生成一个 hash 值，这些 hash 值再两两结合经过哈希得到新的 hash 值，以此向上最终生成一个 hash 值就是本区块的 ID. 假设区块中的某一个交易发生了改变(例如交易 2 发生改变)，则其 hash 值也会发生改变(hash2 发生改变)，当其重新与相邻的 hash 值进行哈希之后会得到不同于之前的 hash 值(hash23 发生改变)，由此而上，最终使得区块的 ID 发生改变，从而导致区块从区块链中断开. 一个从区块链中断开的区块是不能获得区块链网络承认的，因此，证明了这种数据存储结构能够起到防止数据篡改的作用. 虽然有些区块链可能不是采用默克尔树的结构来组织区块内的数据，但是效果是一样的，就是内部任何一个改动都会引起整个区块 ID 的变化. 区块内部的这种组成结构形式保证了数据的完整性，避免了因为敌手攻击等原因导致数据被篡改的情况发生.

图 4 所示为交易的结构和关系. 在每一笔交易中记录了数字货币的输入和输出信息，输入的数字货币必须是从上一个或者几个交易中转入，

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

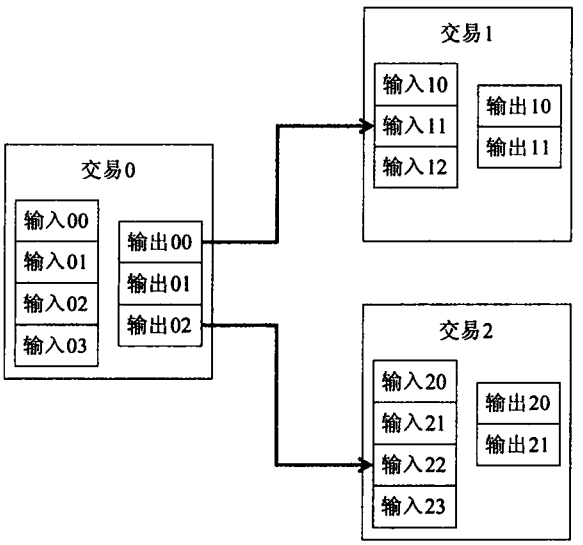

图 4　交易的结构和关系

输出的数字货币也必须只能是转入到下一个或几个交易中. 通过这种输入输出关系的建立，每一笔数字货币的转移都可以进行追溯，直到该数字货币产生的那个区块. 通过这种方式，区块链技术实现了对交易信息的溯源，从而保证了数据的真实性.

3　非对称加密技术

非对称加密技术[15]是保证区块链安全的基础技术. 非对称加密技术含有 2 个密钥：公钥和私钥，首先，系统按照某种密钥生成算法（例如 SHA256 hash 算法、base58 转换），将输入（例如随机数）经过计算得出私钥（一串固定长度的字符串），然后，采用另一个算法（例如 secp256k1 椭圆曲线）根据私钥生成公钥，公钥的生成过程不可逆. 由于采用 SHA256 算法的私钥可达到 2^{256} 个，在现有的计算能力条件下难以通过公钥来穷举出私钥，因此可以认为是密码学安全的，从而能够保证区块链的数据安全.

非对称加密技术在区块链中有 2 种用途：1）数据加密；2）数字签名. 数据加密的过程为：信息发送者（记为 A）采用信息接收者（记为 B）的公钥对待发送的信息进行加密后发送给 B，B 采用自己对应的私钥对加密信息进行解密获得原始信息. 数字签名的过程为：信息发送者 A 采用自己的私钥对待发送信息进行加密后发送给接收者 B，B 采用 A 对应的公钥对加密信息进行解密获得原始信息. 非对称加密在区块链的交易信息中得以应用，如图 5 所示[1].

区块链的交易分为 2 个过程：1）交易签名；2）交易验证. 交易签名的过程：1）本次交易（如交易 2）接收者（如用户 2）的公钥对上一次交易（如交易 1）进行加密 hash；2）本次交易发送者（如用户 1）采用自己的私钥对第 1 步的 hash 进行签名. 交易验证的过程：1）本次交易的发送者（如用户 1）的公钥对其签名进行解密，获得信息 X；2）上一次交易数据与本交易交易的接收者（如用户 2）一起拼接起来采用同样的算法进行 hash 运算，得到信息 Y；3）如果 $X==Y$，则证明了本次交易的发送者确实是用户 1，接收者确实是用户 2，用户 1 确实要与用户 2 进行本次交易. 非对称加密技术的应用使得区块链具备了秘密性和真实性.

随着对区块链技术的深入研究以及区块链应用的需求，非对称加密技术已经不仅仅用在交易签名验证之上，例如：为了达到有限匿名，还需要考虑将记录在区块链的数据进行加密，只有拥有解密钥匙的人员才能打开查看，这就用到了多重签名技术[16-17]. 但是，区块链有一个重要的机制就是记录在区块中的数据需要被其他节点校验，而

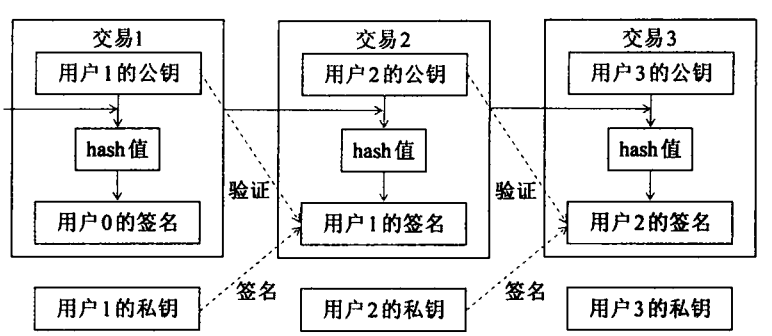

图 5　非对称加密在区块链交易中的应用

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

有不愿意让校验者看到真实的信息，此时需要使用盲签名技术[17]. 通过多重盲签名技术来实现对区块链数据的签名和保护将是区块链研究与应用的重要课题，就在本文完稿前几天创世的 ZCash 零币就是采用了多重签名技术，只能由交易双方来打开，从而实现了对交易双方的隐私保护.

4 共识机制技术

共识机制技术是区块链中的另一个基础技术. 共识机制用来决定区块链网络中的记账节点、并对交易信息进行确认和一致性同步. 目前，人们研究和采用的共识机制有：

1) 工作量证明(proof of work, POW). 它将解决计算困难问题所需要的计算代价作为新加入块的凭证和获得激励收益.

2) 权益证明(proof of stake, POS). 它以权益证明代替工作量证明，由具有最高权益的节点实现新块加入和获得激励收益.

3) 股份授权证明(delegated proof of stake, DPOS). 它是 POS 的一个演化版本，首先通过 POS 选出代表，进而从代表中选出块生成者并获得收益.

POW 的基本思想是设定一种激励机制[3](奖励一定数量的数字货币)吸引区块链网络中的节点来做一个求解困难但验证容易的 SHA256 数学难题，该数学难题要求计算得出的随机数小于或者等于目标 hash 值. 符合要求的随机数通常由多个前导零组成，如果目标 hash 值越小，则找到这个随机数的难度越大. 为了找到这个随机数需要耗费大量的计算能力，如果有节点试图改变既有区块链，则需要投入更大的计算能力来重新计算，这种情况还只是停留在理论上，而且随着高度增加，所需计算能力呈几何级别增加. 正是由于这种机制保证了区块链的数据一致性和不可篡改性，但是同时也带来了资源浪费，甚至由于超大矿池的出现而失去了去中心的优势.

POS 的基本思想是以权益证明替代工作量证明[2]，由区块链网络中具有最高权益的节点而不是拥有最高计算能力的节点来记账并获得激励收益. 权益表示的是节点对特定数量数字货币的所有权，采用币龄或者币天数(coin days)表示，是币数与最后一次交易的时间长度的乘积. 不同于 POW 中各节点在挖矿上具有相同的难度，POS 的共识机制中难度与交易中所消耗掉的币龄成反比，消耗掉的币龄越多则难度越低，越有可能成为记账节点，累计消耗币龄最多的区块将加入到主链. POS 算法使得网络的所有节点都可以参与防卫，抵御攻击，保障网络的安全性，任何敌手试图私藏一个含有比主链更多销毁币龄的区块链都需要付出更多的成本.

DPOS 的基本思想是每个节点[3](类似股份公司中的股东)按照其所拥有的股份享有对应的投票权利，节点可以将其选票投给某一个代表节点，最后获得票数最多的前 100 个节点按照既定的时间表轮流负责封装交易产生区块，每个区块中所包含的交易费的 10%作为激励平均分发给这 100 个代表节点. 作为代表节点必须保证实时在线，为大家提供良好的区块生成广播服务，否则，很有可能失去大家的投票进而失去代表节点资格. DPOS 共识机制中每个节点都能够自主决定其信任的授权节点且由这些节点轮流记账生成新区块，大幅减少了参与验证和记账的节点数量，可以实现快速共识验证，这与 POW 共识机制必须信任最高算力节点和 POS 共识机制必须信任最高权益节点不同，但这并不影响其保证区块链网络数据的安全性.

5 智能合约技术

智能合约在区块链 2.0 中得到长足发展，以以太坊为代表的区块链将智能合约的应用推向了更高水平. 早前，尼克萨博(Nick Szabo)将智能合约定义为：一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议. 对于区块链中的智能合约可以从以下 5 点进行理解：1)由一段脚本或者代码来实现其业务逻辑；2)能够被注入到区块链的执行环境中执行；3)具有图灵完备性；4)事件驱动；5)具有状态. 所谓图灵完备指的是在可计算理论中，当一组数据操作的规则(一组指令集、编程语言或者元胞自动机)满足任意数据按照一定的顺序可以计算出结果，被称为图灵完备(Turing complete).

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

从安全的角度来看，智能合约首先是同一般的区块链数据一样，具有分布式、存证、一致完整、不可篡改删除等特性；其次，智能合约也是作为保证区块链安全的一种技术手段. 在智能合约里规定了参与方的权利义务，合约执行的触发条件以及对应结果，一旦该智能合约被加入到区块链中就可以不受任何一方影响，客观、准确地执行.

在提供了安全的区块链环境之后，智能合约的安全很大程度上取决于合约代码. 如果合约代码里的实现逻辑存在问题就严重影响到区块链的安全，因此，有必要对上链的智能合约进行慎重检查. 一种效率较高的解决办法就是提供智能合约模板，智能合约模板经过了专业审核、试用验证，用户在使用智能合约模板时只需要填写相关输入数据即可.

为了提高智能合约安全性检查的效率，可以引入形式化方法，将模式化驱动工程(MDE)和模式化驱动框架(MDA)的理论和实践应用到智能合约的建模、生成、测试中.

6 其他安全技术

基于区块链的系统在运维过程中还面临着许多其他的安全问题挑战，需要采取相应的技术应对. 例如：密钥管理技术、密文访问控制技术、防DDoS攻击技术等等.

在区块链中，如何安全合理地管理密钥、防止因密钥丢失导致财产丢失，或者因密钥泄露导致财产被盗，这是区块链应用需要解决的问题. 根据实际需要，密钥管理会有所不同，可以是一人多个密钥的管理，也可以是群组密钥的管理.

隐私保护已经成为区块链技术应用的重要关注点，需要采用访问控制技术，特别是密文访问控制技术[18]. 所谓密文访问控制就是将一般访问控制技术同密码学工具相结合，实现对访问对象的安全访问. 随着区块链技术研究的深入，区块链上记录的信息会随着应用的需要进行扩展，更多的属性数据被记录到区块中，这些属性信息往往包含了数据所有人的关键隐私数据. 因此，为了实现对这些数据的隐私保护，可以考虑采用基于属性的密码访问控制技术[19-22].

在区块链中，如果有用户快速大量地执行一些假的交易操作，形成交易风暴，发起拒绝服务攻击，就会给区块链造成堵塞，让真的交易操作无法顺利执行. 为了防止这种问题的出现，可以采用交易费的措施来对交易进行控制，使得敌手在发起拒绝攻击时需要耗费大量的费用，得不偿失.

未来，区块链将与人工智能、大数据、云计算、物联网、移动互联网等技术越来越深入融合，其安全问题也会不断涌现，相应的安全技术手段也会越来越丰富. 除了传统安全手段之外，还需要将这些领域中的安全技术手段与区块链的安全技术手段相结合，使得相互融合的信息技术获得更加可靠的安全性. 同时，将区块链技术与这些新一代信息技术相结合，本身也可以提供更加安全的信息服务. 例如，将区块链和大数据相结合，可以提供微观和宏观的精准的数据鉴别与存证服务，从而为人们提供更加真实、安全的信息服务. 还有，将区块链与物联网技术相结合，可以提供防伪追溯服务，通过物联网技术将食品、药品、名贵烟酒等，从生产到消费整过过程中的信息都采集起来，并通过相关技术记录到区块链上，从而实现了在更大范围的防伪溯源.

7 结束语

区块链从第1天应用到比特币中就非常重视安全，从区块链1.0，2.0到现在的3.0，区块链的安全技术不断得到改进，为了满足更多的工程化应用的需要，新的安全需求和安全技术不断的被提出和研究，人们对区块链安全的认识也发生了一些改变，例如，为了适应社会管理的需要，也是为了保护用户利益的需要，在实际的应用中还需要提供身份认证、日志审计、监管等功能.

参 考 文 献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. [2016-10-07]. https://bitcoin.org/bitcoin.pdf

[2] 周平. 中国区块链技术和应用发展白皮书[M]. 北京：工业和信息化部，2016

[3] 袁勇，王飞跃. 区块链技术发展现状与展望[J]. 自动化学报，2016，42(4)：481-494

[4] Crosby M, Pattanayak P, Verma S, et al. BlockChain Technology: Beyond Bitcoin [M]. Berkeley: Applied Innovation Review, 2016

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

[5] Buterin V. Ethereum Homestead Documentation [EB/OL]. 2013 [2016-10-07]. http://ethdocs.org/en/latest/introduction/index.html

[6] Archana M. Naware. Bitcoins, its advantages and security threats [J]. International Journal of Advanced Research in Computer Engineering & Technology, 2016, 5(6): 1732-1735

[7] BitFury Group. Proof of stake versus proof of work white paper [EB/OL]. Bifury Group Limited, 2015 [2016-10-07]. http://www.cryptocoinsnews.com/bitcoins-future-proof-of-stake-vs-proof-of-work/

[8] Huan Meng. Security architecture and service for the bitcoin system [D]. Stolkholm, Sweden: Royal Institute of Technology, 2014

[9] Sompolinsky Y, Aviv Zolar. Bitcoin's security model revisisted [EB/OL]. [2016-10-07]. https://arxiv.org/abs/1605.09193v2

[10] Wust K. Security of Blockchain Technologies [D]. Zurich: Department of Computer Science, 2016

[11] Decher C. On the Scalability and Security of Bitcoin [D]. Germany and Switzerland: Sciences of ETH Zurich, 2016

[12] 陶林君. 基于DHT的P2P关键技术研究[D]. 南京: 南京邮电大学, 2008

[13] Ken Y K Hui, John C S Lui, David K Y Yau. Small-word overlay P2P networks: Construction, management and handling of dynamic flash crowds [J]. Computer Networks, 2006, 50: 2727-2746

[14] 卢苇, 周韬, 邢薇薇. 一种改进的非结构化P2P网络洪泛搜索机制[J]. 西北工业大学学报, 2015, 33(2): 342-350

[15] 冯登国. 密码学原理与实践[M]. 3版. 北京: 电子工业出版社, 2009

[16] 祁明, 史国庆. 多重盲签名方案及其应用[J]. 计算机工程与应用, 2001, 37(3): 91-92

[17] 严安, 杨明福. 基于椭圆曲线的有序多重数字签名方案[J]. 计算机应用与软件, 2007, 24(2): 164-165,183

[18] 李勇, 雷丽楠, 朱岩. 密文访问控制及其应用研究[J]. 信息安全研究, 2016, 2(8): 721-728

[19] 苏金树, 曹丹, 王小峰, 等. 属性基加密机制[J]. 软件学报, 2011, 22(6): 1299-1315

[20] 冯登国, 陈成. 属性密码学研究[J]. 密码学报, 2014, 1(1): 1-12

[21] 林莉, 怀进鹏, 李先贤. 基于属性的访问控制策略合成代数[J]. 软件学报, 2009, 20(2): 403-414

[22] 沈志荣, 薛巍, 舒继武. 可搜索加密机制研究与进展[J]. 软件学报, 2014, 25(4): 880-895

朱 岩

博士,教授,主要研究方向为网络与信息安全、密码学与安全计算、计算复杂性理论.

zhuyan@ustb.edu.cn

甘国华

博士研究生,主要研究方向为区块链、软件工程.

ganguohua01@163.com

邓 迪

本科,高级工程师,主要研究方向为区块链、云计算.

dengdi@taiyiyun.com

姬菲菲

硕士,高级工程师,主要研究方向为区块链、金融.

jifeifei@taiyiyun.com

陈爱平

本科,高级工程师,主要研究方向为区块链、应用数学.

chenaiping@taiyiyun.com

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net