doi :10.3969/j.issn.1671-1122.2016.09.038

区块链技术及其应用研究

谢辉，王健
（达闼科技成都有限公司，四川成都 610041）

摘　要：区块链最早作为比特币的底层“账本”记录技术，起源于2009年。经过几年的发展和改进，逐渐成为了一种新型的分布式、去中心化、去信任化的技术方案。特别是近两年以来，区块链已逐步脱离比特币，独立地成为技术创新的热点，开创了一种新的数据分布式存储技术，引导了系统与程序设计理念的变化，并可能颠覆现在商业社会的组织模式，其应用受到了越来越多的关注。文章从技术角度研究了区块链的设计与实现，从区块链自身和应用两方面分析了区块链的安全性，从安全架构的角度对区块链安全体系与传统中心化模式的安全体系进行了比较，并对区块链的优势与不足，以及可能应用的场景进行了总结。

关键词：区块链；去中心化；安全架构；应用场景
中图分类号：TP309　　**文献标识码：**A　　**文章编号：**1671-1122（2016）09-0192-04

中文引用格式：谢辉，王健 . 区块链技术及其应用研究 [J]. 信息网络安全，2016（9）：192-195.
英文引用格式：XIE Hui，WANG Jian. Study on Block Chain Technology and Its Applications[J]. Netinfo Security, 2016(9):192-195.

Study on Block Chain Technology and Its Applications

XIE Hui, WANG Jian
(*CloudMinds Technologies Chengdu Co., Ltd. Chengdu Sichuan* 610041, *China*)

Abstract: Since 2009, blockchain was used for base record technology of account book in BitCoin. It has graduated as a new distributed, non-centralized and non-trust solution after several years. Especially in last two years, blockchain has gradually gotten out of BitCoin as an independent innovation hot point. It creating a new distributed data storage technology with an innovation change on system/program design. Maybe, it will subvert the organizational model of current business community in future. So it received more and more attention from Business and Technology communities. This article do more research and investigation on the design and implementation of blockchain. Include security investigation for blockchain and blockchain related application, and the security architecture compare for blockchain security system and traditional centralized mode system. Did the summaries for the advantages and disadvantages of the blockchain, and more actual application scenarios are derived.

Key words: block chain; decentralization; security architecture; application scenario

收稿日期：2016-07-25
作者简介：谢辉（1981—），男，四川，硕士，主要研究方向为信息安全；王健（1981—），男，四川，本科，主要研究方向为信息安全。
通信作者：谢辉 victor.xie@cloudminds.com

0 引言

自 2008 年一位化名为“中本聪”研究者（或研究团体）在 Cryptography 邮件列表中发表了比特币规范及其概念证明以来，区块链作为比特币交易系统中最核心的技术受到了越来越广泛地重视。

比特币狭义上可以理解为一种全新的数字货币，广义上则被认为是一种去中心化的数字货币支付系统。“中本聪”发明并采用了一种名为区块链的技术方案来记录和维护比特币的交易账本。区块链技术方案中没有中心服务器，每个运行区块链软件的计算设备都是区块链网络中的一个对等节点，节点之间无需建立信任关系，系统中的任意多个节点，把一段时间系统内全部信息交流的数据，通过密码学算法计算和记录到一个数据块（区块），并且生成该数据块的指纹（哈希）用于链接下个数据块和校验，通过集体验证和维护的方式来建立一个可靠数据库 [1-3]。

比特币的区块链技术革命性地解决了“拜占庭将军问题”，具有不可更改、不可伪造、完全可追溯的安全特性，实现了一种无信任的共识网络系统。这种无需信任某个中心节点的共识网络系统，从根本上与当今人类社会和互联网络系统的组织结构不同，是一种更贴近自然界与人性的组织结构。越来越多的科技巨头、研究机构和技术团体已认识到区块链技术的颠覆性，并参与到区块链的研究中 [4-6]。

本文将从技术角度剖析区块链技术的协议和机制，从底层和应用两方面分析其安全性，与传统中心化安全机制进行对比，并总结现有发展和改进情况、优势与不足，以及可能的应用场景。

1 区块链技术分析

区块链是由区块链网络中所有节点共同参与维护的去中心化分布式数据库系统，它是由一系列基于密码学方法产生的数据块组成，每个数据块即为区块链中的一个区块。根据产生时间的先后顺序，区块被有序地链接在一起，形成一个数据链条。

1.1 比特币中的区块链

比特币作为一种数字货币交易系统，交易记录是比特币系统中最基本的组成部分。通过使用巧妙设计的数据结构和基于密码学的保护验证机制，比特币的区块链将所有交易完整无误地记录到各个区块中。因此，可以把比特币中的区块链看作一种分布式账单系统。

1）交易

比特币中的交易记录本质上是比特币的转账信息，一条交易记录存储一次转账的信息。交易记录主要由资金来源和资金去向两部分组成，如表 1 所示。

表1 交易数据结构

字段	子字段	大小	描述
版本号		4 字节	标识交易数据结构版本
资金来源数量		1~9 字节	资金来源的个数
资金来源	交易哈希值	32 字节	指向代表资金来源的交易哈希值
	资金去向序号		资金来源交易中的资金去向序号
	解锁指令长度	1~9 字节	解锁指令的字节大小
	解锁指令	由上一字段决定	资金来源所有权证明
资金去向数量		1~9 字节	资金去向的个数
资金去向	转出资金数量	8 字节	转出比特币数量，单位为 10^{-8} 比特币
	锁定指令长度	1~9 字节	锁定指令的字节大小
	锁定指令	由上一字段决定	指定资金转出后的所有人
锁定时间		4 字节	设定本交易生效（被记入区块链）的时间

注：“资金来源”和“资金去向”字段可多次重复，其重复次数由各自对应的数量字段决定。

在一条交易中，可有多项资金来源，每项资金来源均指向之前已发生且合法（已记录入区块链）的某条交易记录中的某项资金去向。每项资金去向均在锁定指令中记录了可使用该项资金的所有人信息，使用该资金去向的交易必须在交易数据结构的资金来源解锁指令中提供资金所有人证明，才能使交易成为一条合法有效的交易。在比特币交易系统中，资金所有人采用其掌握公钥哈希值的 Base58 编码 [3] 表示，资金所有人的证明一般包括两部分，一部分是上述公钥本身，另一部分是采用上述公钥所对应私钥计算得到的数字签名。当交易被发布到区块链网络后，网络中的每个节点都将使用交易数据结构中所提供的资金所有人证明来验证交易的合法性，如果交易不是合法有效的，区块链网络节点将直接丢弃该交易 [7-9]。

2）区块与区块链

区块是记录比特币交易信息的数据单元，它由区块头和区块内容两部分组成。如表 2 所示。

表2 区块数据结构

字段	子字段	大小	描述
区块头	区块大小	4 字节	本区块字节大小（不含本字段在内）
	版本号	4 字节	标示区块协议版本
	父区块哈希值	32 字节	上一区块（父区块）的区块头部哈希值
	默克尔树[11]根	32 字节	本区块中所记录交易的默克尔树根哈希值
	时间戳	4 字节	本区块的产生时间
	难度目标	4 字节	产生本区块所进行的工作量证明计算的难度目标
	随机数	4 字节	用于工作量证明算法的随机数
区块内容	交易数量	1~9 字节	本区块记录的交易数量
	交易	由交易数量决定	本区块的所有交易，采用表 1 数据结构记录

区块的链接是通过区块头数据的哈希值来完成的，区块链使用这个哈希值作为所有区块的唯一标识，通过区块头中所记录的父区块哈希值便可在区块链中找到所链接的唯一区块。这样就通过每个区块链接到各自父区块的哈希值序列创建了一条从最新区块追溯到第一个区块的链条，从而形成所有区块的一种链状数据结构，如图 1 所示。

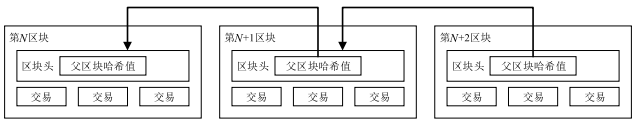

图1 区块之间的链接

区块链网络采用一种被称之为“工作量证明”的竞争机制来产生新区块，区块链网络中的每个节点都可参与该竞争。其根本是一种需要利用密码学方法来解决的需消耗大量计算能力和时间的数学问题。具体来说，区块链中的“难度目标”对标识区块唯一性的区块哈希值进行了严格规定，即一定的“难度目标”代表了区块哈希值从第 1 位开始值为 0 的位数，这就需要产生新区块的节点使用不同“随机数”来计算新区块的哈希值，直到找到一个“随机数”所计算得到的区块哈希值满足对应的“难度目标”。

当新区块产生并发布到网络后，区块链网络中的每个节点都会参与新区块的合法性验证工作，只有被验证为合法的区块才会被区块链网络节点记录下来。新区块合法性验证主要包括三方面：1）新区块数据结构正确性；2）对“随机数”是否满足“难度目标”进行验证；3）对新区块记录的所有交易进行合法性验证。

1.2 区块链安全分析

1）区块链自身安全分析

区块链网络中没有中心服务器，参与系统的每个节点都有义务验证交易和区块的合法性、参与交易和区块的存储转发，也同时具有丢弃其认为不合法的交易和区块。因此，区块链系统中的所有节点均是平等的，每个节点都具有完整的数据记录。即使系统中的某个或某些节点受到攻击或破坏，不会对系统的完整性和可用性造成威胁 [10]。

区块链采用数字签名等密码学机制对其记录的每项信息进行保护，保证了信息是可验证的，实现了信息本身无法被伪造和篡改。采用“工作量证明”的竞争机制来记录信息，使得记录到区块中的信息很难被撤销或销毁，参与系统的节点数量越多，系统的安全性越高。

“工作量证明”机制以计算能力为基础，是一把双刃剑，它一方面保证了区块链本身的安全性，另一方面也带来了“51% 攻击”的问题。“51% 攻击”即掌握了全网 50% 以上的计算能力后，就可以通过重新计算已确认的区块或控制新区块的产生，实现双重支付、阻止交易的确认和阻止其他节点产生新区块。但“51% 攻击”不能伪造或修改他人的交易或直接窃取他人的比特币。

2）区块链应用安全分析

区块链的安全问题除了其自身底层协议和机制的安全性外，还包括其上层应用的安全性。区块链自身的底层协议具有较完备的安全机制，安全性较高，但与智能手机中的应用程序漏洞或恶意应用程序造成的系统安全问题类似，把区块链作为某种应用的底层技术时，区块链自身的安全性并不能保证区块链之上的应用本身的安全性。

比特币的区块链所使用协议和密码学规则在运行多年后仍安全可靠，说明了区块链技术本身的安全设计具有非常高的可靠性。但如同其他所有软件一样，比特币软件在实现和执行过程中，也被发现了安全漏洞并予以了修正，以及运行于以太坊区块链基础上的 TheDao 应用被攻击造成大量资金被盗事件，均证明了区块链本身的安全并不能保证以区块链为基础的应用的安全。因此，在使用区块链进行应用开发时，应用本身的安全性必须得到足够的重视。

3）与传统中心化安全体系的对比分析

在传统的中心化体系结构中，其系统安全通常由一系列访问控制机制和审查制度组合而成的安全架构来保证。此类安全架构一般基于一个可信中心（可信根），可信中心自身的安全成为系统安全中最核心的问题，也成为最大的安全风险所在。同时，为了避免系统的通信被中间人攻击或窃听、系统数据库被窃取，还需采用端到端加密、存储加密等措施以保证系统数据的安全性。随着系统复杂性的日益增加，中心化的安全架构也会越来越庞大与复杂，使其更容易出现安全问题。

区块链的核心准则是去中心化，这对其安全策略与机制提出了非常高的要求。与中心化的安全框架不同，区块链基于“工作量证明”的无信任共识机制，创建了一个可公开的数据系统，从而将安全责任和控制权转移到了用户侧，

用户侧通过验证和使用从初始区块到当前区块的可信数据链，来确保用户身份和数据的正确性，使得分布存储在每个区块链网络节点的区块链本身成为去中心化系统中的可信根。

区块链为了实现去中心化而将安全责任下移到用户侧的做法，对用户提出了更高的要求，用户必须具备安全使用和存储自身密钥的意识和能力。由于区块链中并没有将密钥与用户身份建立关联关系的机制，这在保护了用户身份私密性的同时，也造成了用户私钥一旦丢失或泄露，用户资金将无法追回的后果。

2 区块链技术应用

2.1 区块链的发展与改进

比特币中的区块链是专门为数字货币交易而设计的，采用以计算能力为基础的共识机制，在一定程度上限制了它的应用范围。随着区块链技术受重视程度的不断提高，在最初的区块链基础上，出现了一些新的区块链技术和概念。

1）私有链

比特币的区块链是完全公开的，所有人都可以参与其中，可以将其看作一种“公开链”，相对于此，将区块链网络限制在一定范围内即成为“私有链”。根据将区块链私有化所采用技术方式不同，私有链又可以细分为联盟链、许可链等。

2）以太坊[5]

以太坊作为与比特币类似的数字货币交易系统的同时，也是一套完整的去中心化应用平台。在使用以太坊进行数字货币交易的同时，任何人都可以在以太坊上发布和使用去中心化应用（Decentralization Application）。以太坊的优秀之处在于其提供了去中心化应用开发、部署和使用的完整工具链，使得基于区块链的应用开发变得极其便利。

2.2 区块链的应用

区块链虽因数字货币而生，但因其实现了去中心化的共识，同时具有优异的安全特性，有着非常广泛的应用前景，如表3所示。可以说，涉及记“账”、分“账”、转“账”的各个方面都可以使用区块链实现。这里所说的“账”并不只是单一的“账单”，而可以理解为用于某种事实证明的数据。

表3 区块链应用场景

分类	实例
金融保险	股票交易、股权管理、债券、集资、跨机构清算/结算、基金管理、保险证明等
产权证明	实物产权（例如房产证明、车辆登记、租赁等）、无形资产（例如专利、商标等）
身份验证	身份证明、护照、电子签名等
社会生活	公正证明、遗嘱、彩票、投票等
其他	分布式数据库、物联网、自治组织、物品溯源等

2.3 区块链的优势与不足

区块链具有去中心化、去信任化、数据防篡改的优势，在匿名的同时又具有数据透明的特点，但并不意味着区块链技术不存在局限性。例如，区块容量限制、确认时间长、基于工作量证明的共识机制能耗大等问题，限制了其在商业上的大规模应用。同时，其数据透明性造成的隐私泄露、如何与现有系统平滑接轨、法律及监管等问题，还需要不断的研究和解决，如同任何新技术一样，区块链技术的突破，还需要较长时间的积累。

3 结束语

区块链自诞生以来，因其具有的去中心化、去信任、共同维护、数据可靠、隐私保护等特性，以及应用的广泛性，得到了前所未有的重视，发展非常迅速。但同时，也应该清醒地认识到任何新技术都具有其局限性，区块链也不例外，如51%攻击、计算效率问题，以及最近发生的针对区块链历史上最大众筹项目（TheDAO）的攻击事件反映出的安全问题。但这些并不影响区块链被认为是一种可重构各行业生态逻辑和架构的颠覆性技术，值得持续的研究和探讨。（责编 吴晶）

参考文献：

[1] 卿斯汉 . 关键基础设施安全防护 [J]. 信息网络安全，2015（2）：1-6.
[2] 龚鸣 . 什么是区块链 [EB/OL]. http://chainb.com/?P=Cont&id=6, 2016-9-2.
[3] Wikipedia. Base58 编 码 [EB/OL]. https://zh.wikipedia.org/zh-cn/Base58, 2016-9-2.
[4] 王红凯，王志强，龚小刚 . 移动互联网安全问题及防护措施探讨 [J]. 信息网络安全，2014（9）：207-210.
[5] Ethereum community. Ethereum Homestead Documentation[EB/OL]. http://ethdocs.org/, 2016-1-15.
[6] Andreas M. Antonopoulos. Mastering Bitcoin[EB/OL]. http://chimera.labs.oreilly.com/books/1234000001802/index.html, 2015-1-15.
[7] 龚鸣 . 区块链社会 [M]. 北京：中信出版集团，2016.
[8] 王学强，雷灵光，王跃武 . 移动互联网安全威胁研究 [J]. 信息网络安全，2014（9）：30-33.
[9] Ethereum WiKi. White Paper[EB/OL]. https://github.com/ethereum/wiki/wiki/White-Paper, 2016-1-15.
[10] Gavin Wood. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER[EB/OL]. http://gavwood.com/Paper.pdf, 2015-1-15.