专题:大数据

区块链技术原理、应用领域及挑战

李董,魏进武

(中国联合网络通信有限公司研究院,北京 100032)

摘　要:区块链技术是对所有交易或者电子行为进行记录的分布式数据记录方案,即公开账本技术。区块链技术以其分布式、去中心化、不可造假的特性逐渐走进公众的视线,引发了世界各行业的广泛关注和讨论。描述了区块链技术的工作原理和它在金融和非金融领域的一些应用,分析了区块链技术发展面临的挑战和商业机遇。

关键词:区块链原理;应用领域;挑战

中图分类号:TP393　　**文献标识码**:A

doi: 10.11959/j.issn.1000-0801.2016309

Theory, application fields and challenge of the blockchain technology

LI Dong, WEI Jinwu

China Unicom Research Institute, Beijing 100032, China

Abstract: Blockchain technology is a distributed data recording scheme to record all transactions or electronic behavior, namely public ledger technology. Blockchain technology has gradually caught attention of the public, causing widespread concern and discussion in the world with the features of distributed, decentralized and non fraud. The working theory of the blockchain and its application in the field of finance and non-finance were described. And the challenges and opportunities in the development of the blockchain technology were analyzed.

Key words: blockchain theory, application field, challenge

1　引言

区块链技术是一种对一段时间内所有交易或者电子行为进行记录的分布式数据记录技术,即一种按照时间顺序将数据区块以顺序相连的方式组合成的链式数据结构,并以密码学方式保证的不可篡改和不可伪造的分布式公开账本技术。在区块链上,每笔交易都可以被系统的参与者通过多数节点共识的机制进行审核。一旦被记载到区块链上,相关的交易信息就不能被修改、删除。区块链上的区块记录了一定时间内被审核通过的每笔交易记录。

比特币是区块链技术最本质的应用,它也因为在没有政府的干预下构造了上百万美元的匿名交易市场而成为最具争议性的区块链应用。然而,区块链技术本身可以被金融和非金融领域应用的事实并没有争议。

现阶段,电子金融领域建立在可靠的、可信任的第三方授权的基础上。用户网络交易必须依赖于第三方机构对交易双方进行身份和交易资格的确认。人们生活的电子世界在依靠第三方机构维系安全与个人电子资产隐私的背

收稿日期:2016-11-02;修回日期:2016-12-11

景中,并不是绝对的安全。因为第三方机构在这种背景下扮演了强有力的中心角色。而中心机构一旦被侵入,靠第三方机构维系的普通角色所面临的电子安全风险将无法保证。

在这种背景下,区块链的诞生通过对分布式共识的应用,对依靠第三方信任的电子世界规则提出了巨大改进。分布式共识和匿名性是其最重要的两个关键特征。通过这些特征的综合应用,在纷杂的网络环境中,区块链在没有第三方信任机构的参与下,对网络交易记录、电子资产记载提出了分布式账本的方式,有以下鲜明的特征。

(1)去中心化

去中心化是区块链技术最本质的特征。区块链技术的产生意味着在没有中央处理节点的情况下,实现了全网所有数据的分布式记录、存储并且能够保证数据记录的真实性。区块链技术通过 P2P(点对点)协议组成网络。不同于中心化网络模式,P2P 网络中各节点的计算机地位平等,每个节点有相同的网络权力,不存在中心化的服务器。

在这种去中心化的网络环境中,全网所有在网节点没有实质的区别,所有节点享有相同的权利和义务。区块链网络中的在网节点必须遵守同样的密码学规则,共同维护全网系统中的数据记录。对数据的记录、存储过程,必须得到区块链网络内其他节点的批准后才能执行。由于所有在网节点并没有第三方中介或者信任机构背书,所以在去中心化的区块链网络中,对单个节点的攻击无法控制或者对整个区块链网络产生影响。P2P 去中心化网络模式与中心化网络模式对比如图 1 所示。

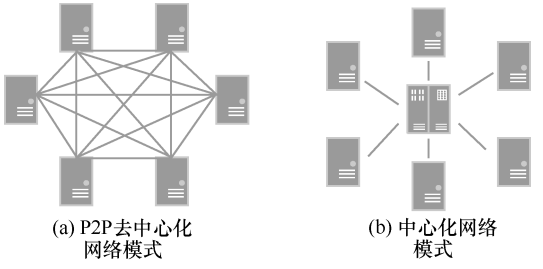

图 1　P2P 去中心化与中心化网络模式拓扑对比

(2)数据及操作的透明性

区块链技术作为分布式账本技术,系统内所有的数据记录及操作对于所有在网节点都是透明的。在典型的区块链网络中,每一个节点都能够存储全网发生的历史交易记录的完整、一致账本。区块链通过对非对称加密算法、散列加密等密码学技术的组合应用,保证区块链信息在全网的高度透明性。并且区块链网络运行的程序、规则、节点的接入方式都是公开的,这是区块链网络信任的基础。这些机制的运用,保证了区块链中记录的数据可以被全网所有节点审查、追溯。

(3)信息不可篡改性

区块链区块中的信息是不可篡改的,一旦数据信息被验证通过写入区块并加入区块链中,就无法被篡改。区块链的数据信息必须经过全网大部分节点的审核以后,才能允许被记录。除非能够控制系统中 51%以上在网节点,否则对单节点的区块记录篡改是没有意义的。即对个别节点的账本数据的篡改、攻击不会影响全网总账的安全性。这种信息的不可篡改性保证了区块链数据的稳定性与可靠性。

(4)匿名性

区块链技术在复杂的网络环境中解决了在网节点间的信任问题,因而区块链网络中的交易节点可以在无需了解对方身份的情况下进行交易。区块链网络中的交易是基于加密地址,而不会对交易双方身份进行认证。交易双方仅需要公布自己的地址就可以与对方进行交易通信。这种匿名性的技术基础就是非对称加密算法。

区块链网络的节点使用非对称加密技术构建节点间在匿名环境下的信任。所有节点维持自身的公私钥对,对区块链网络节点间的通信信息进行加密和解密。节点公开发布自己的公钥,保留自己的私钥。进行信息传递的发送方,使用信息接收方公布的公钥对将要传递的信息进行加密。信息接收方在接收到传递的加密信息后,使用自己的私钥对加密过的信息进行解密。通过这样的方式,节点间可以在不需要身份认证的情况下,完成匿名环境下的信任交易。常用的非对称加密算法有 RSA 和 ECC,非对称加密算法的过程如图 2 所示。

2　区块链工作原理

区块链技术不是单一的技术主体,而是多种技术整合

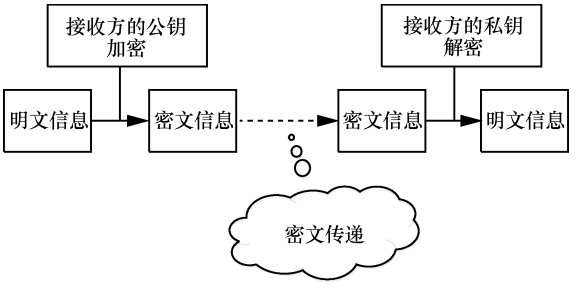

图 2　非对称加密算法的过程

的结果,包括密码学、数学、计算机网络等技术在内的有机整合完善了区块链的去中心化的数据记录方式。区块链技术主要解决了在没有第三方信任机构参与的情况下如何达成可靠的信任记录的问题。其完整的架构如图3所示。

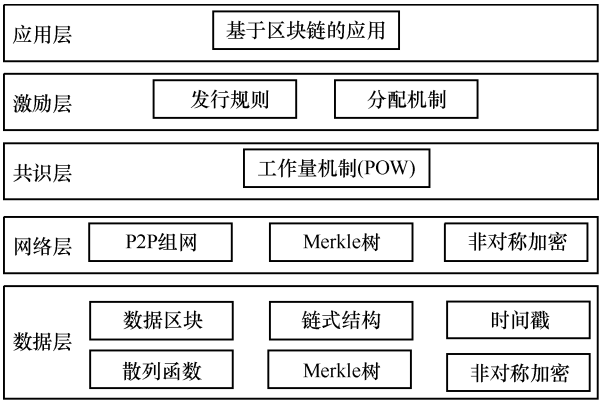

图3 区块链技术架构

互联网金融与第三方可信机构有很密切的关联。这些第三方金融机构在电子交易过程中扮演中介的角色,负责协调交易双方的信息。在整个交易过程中,第三方机构承担了审计、安全守卫、维持交易的责任。在线交易过程中存在的欺诈行为,突出了第三方金融机构的中介地位,同时也导致了较高的交易成本花费。比特币是区块链技术最本质的应用,但是区块链技术的应用并不局限于电子货币,它可以被应用到电子资产在线交换的各个领域。本文以比特币为例对区块链技术源的相关原理、概念进行阐述。

比特币基于密码技术的基础,在有交易倾向的双方之间充当第三方中介的角色。在具体交易过程中,每一笔交易都通过电子签名进行保护确认。在比特币网络中,交易的发起者通过自有私钥对交易进行签名,并发送到接收者的账户地址(即公钥)。在花费比特币时,比特币的持有者需要证明自己拥有对交易签名的私钥。比特币交易审核时,通过发送者的公钥对其交易签名进行验证,进而确定交易方是否可以使用对应的比特币。

每一笔交易都将被广播发送到比特币网络的每一个节点上,在节点通过审核后被记录到生成的区块链区块中。所有比特币网络中的在网节点,共同维护生成的区块链交易记录。通过所有节点保存账本记录的方式,防止交易记录造假、被篡改、被删除等欺诈行为。交易的审核节点需要在记录之前确保以下两个事情。

· 比特币的花费者确实拥有对应的电子货币:在交易中的电子签名验证。

· 比特币花费者在其账户中拥有足够的电子货币:通过检查花费一方的账户(公钥地址)在区块链账本上的交易记录。

但是,在比特币P2P网络中,需要保持广播的交易并不是按照它们产生的顺序进行广播的,每笔交易在比特币网络中通过节点一个接一个地形成广播。因此在比特币网络中需要一定的机制处理这些并不是严格按照顺序广播的交易,进而防止双重花费情况的发生。

区块链技术的应用,正是比特币解决“双花”问题的关键。在比特币系统中,对一段时间内交易进行收集、审核,并最终记录在区块上。通过把每一个区块连接成区块链,对每一笔交易进行追踪。在同一个区块上记录的交易记录可以看作同一段时间内发生的交易。这些区块通过把前一个区块的散列值写入自身区块头字段的方式,按照区块生成时间的先后顺序连接成遵循时间顺序排列的区块链。

这种通过时间顺序连接记录交易的方式,带来了另一个问题,即在比特币网络中的每一个节点都可以收集未确认的交易、生成区块并把新生成的区块广播到全网其他节点。那么比特币网络怎么决定哪一个生成的区块应该被链接到之前区块链的末端?

比特币系统通过引入一个计算数学难题来竞争区块链的生成权,也就是大家熟知的工作量机制(POW)。每个节点生成区块需要证明它付出了一定的计算资源来竞争解决对应的数学难题。具体来说,每个节点被要求寻找一个随机数(nonce),当这个随机数、交易记录与前一个区块的散列值共同进行散列化后的数值的开头包含一定数量的0,并且小于目标值,即散列(前一区块的散列值+Merkle树根+随机数)<T(目标散列)。

但是这个数学难题并不是一成不变的,比特币系统通过调整它的难度来平衡区块的生成时间,使系统内平均10 min产生一个新的、被接受的区块。在网节点通过贡献其自身的计算资源来解决数学难题,竞争产生区块。最早成功计算出数学难题解的节点,将有权利把本节点生成的区块连接到区块链末端,被其他节点接受,并被授予一定数量的比特币作为对它贡献计算资源的奖励。

比特币通过竞争计算散列值的方式,依据POW,保证平均每10 min会有新的区块产生,通过新区块的生成来发行新的比特币。最终生成的区块链区块格式如图4所示。

具体的区块链的工作流程如下。

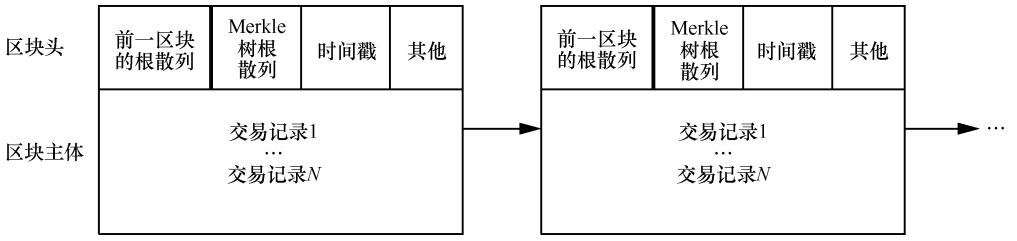

图 4　区块链结构示意

- 在网节点收集一段时间内所有的交易信息。
- 接收节点对收到的交易信息进行检验，审核交易是否合法。通过检验的交易记录将被记录到新区块的主体中。
- 在网节点通过对区块主体中交易信息进行计算，结合区块链当前末端区块的散列值，计算寻找满足条件的新区块的散列值。
- 最先计算得出满足条件的散列值的节点，将把新生成的区块信息广播到全网其他节点。
- 节点对该新生成区块进行验证，当审查无误以后，所有节点接受该区块。而接受的方式，就是把该新生成区块确定为区块链当前末端区块。

通过以上的步骤，区块链网络中所有在网节点共同参与、维护、审查区块链区块的生成过程，并且区块链网络在网节点都维护相同的区块链账本记录，保证了区块链上区块记录的真实、可靠与不可篡改。

在区块链中，区块中的信息由区块头和区块主体中的信息构成。其中，区块主体中将记录具体的交易信息，包括交易双方的公钥地址、交易数量、签名验证等信息。而区块头的大小为固定字节，以比特币为例（见表 1），比特币区块头大小始终为 80 byte。

表 1　区块信息

字段	字段描述	大小/byte
版本号	软件协议的版本号	4
前一区块的散列值	通过计算得出的前一区块的散列值	32
Merkle 树根	本区块中所有交易信息计算生成的散列值	32
时间戳	区块生成的时间	4
难度	POW 的难度目标（动态变化）	4
随机数	用于 POW 计算中寻找满足难度的数字	4

通过区块的散列值，可以唯一地标识出区块链中的区块。每一个区块通过对前一区块散列值字段的引用，指向前一区块。通过时间戳+散列引用的方式，构建了区块链为一条可以按照交易时间先后顺序追踪交易记录的链条，确保了区块链所记录的交易次序是按照时间依次发生的。而引入随机数+Merkle 树根+前一区块的散列值的当前区块散列值的计算方式，保证了交易信息的真实、可靠。

3　区块链在金融与非金融领域的应用

区块链是完全开源的系统，原理及代码都公开，并在运行过程中接受系统内所有节点的监督。围绕区块链这套开源体系能够创造非常丰富的服务和产品。区块链将可以让人类以去中心化、去信任的方式来进行大规模协作。它能应用的领域将不仅仅限定在金融支付领域，可以被扩展到许多延伸行业，诸如去中心化的物联网、租房、打车等应用。但是区块链技术尚处于起步阶段，虽然不少公司已经开始开发基于区块链的应用，但还缺少成熟的产品。接下来，本文将对区块链在出了电子货币意外的金融和非金融领域的应用进行介绍。

3.1　金融领域应用

（1）私有证券

银行、财团等组织必须在处理好交易安全的同时吸引投资者的资金。股票交易为二级市场列出公司的股份，需要使交易和结算活动在安全的环境下、按照时间顺序进行。理论上，一些公司可以通过区块链技术直接分配股份。这些被记录在区块链上的股份可以在二级市场上被出售和购买。

纳斯达克计划用区块链技术开展自身私募股权业务。纳斯达克在 2014 年开始它的私募股权交易业务。这项业务与将要 IPO 或者民营公司的财务报表和投资关系等事物有深切的关系。当前交易股权的程序因为第三方机构的参与而效率低下与缓慢。纳斯达克加入了基于智能合约的区块链项目以实施他们的私募股权业务。这项业务因此也变得更快、更有效率，且可追踪。该项目的范围可以从股票、红利、有价证券等相关衍生物，延伸到银行账户安全、

抵押借款等领域。

(2)资产数字化记录

各类能够被一个或者多个标识符唯一确定标识的资产可以被记录在区块链上,如股权、债券、票据、收益凭证等,均可成为链上数字资产。这种方式可以验证资产的归属权,同时也可以对交易记录进行追踪,在资产转移时无需通过第三方中介机构就能发起交易。无论是物理财产,还是电子资产都可以通过区块链公开账本记录对归属权、交易记录进行公开的审计。

Everledger 公司利用区块链技术永久地记录钻石证书机器交易历史。诸如重量、大小、颜色等可以标识钻石的信息都被散列化以后注册到区块链的区块上。因此保险公司、执法机构、拥有者等多方机构可以对钻石进行审计。

3.2 非金融领域应用

(1)真实性验证

对文件的真实性验证可以通过区块链完成,这一过程减少了对中心授权机构的依赖程度。文件真实性鉴定服务可以为权利的归属、权利的存在及权利真实性提供证明。这样的鉴定服务可以为第三方机构提供鉴伪的支撑。使用区块链技术进行公正服务,保护了文件和追踪鉴定机构的隐私。对文件使用加密散列的方法,将文件记录到区块链区块中并加载上对应的时间戳,这种文件公示的方式可以减少高额的公证费,同时提高证明文件转移交换的效率。

Stampery 公司使用区块链对包括邮件在内的文件进行标识。该公司提供的服务简化了邮件的审核过程。其客户可以通过该公司的技术在付出较小花费的情况下审核文件。

(2)去中心化存储

现有的云存储解决方案往往面临安全、隐私、数据控制方面的挑战。用户只有在相信云存储公司服务方案的前提下,才会对自身机密文件进行云存储。

Storj 公司提供了基于区块链的点对点分布式云存储平台,为用户提供不依赖第三方机构的数据转移和共享服务。用户可以通过这项服务共享闲置的互联网带宽和将用户计算设备上空闲的硬盘空间共享给其他有文件存储需求的客户。中心化控制的减少相应地减弱了传统数据方面的缺陷,同时显著地提高了数据安全、隐私和对数据的把控能力。Storj 平台依靠算法给网络中参与的用户提供适当奖励。通过这样的方式,Storj 平台可以定期通过密码的形式检查文件的真实性和可用性,借此给提供文件存储服务的用户以奖励。

(3)去中心化物联网

物联网技术在企业和用户的角度上都逐渐变成受追捧的技术。许多基于中心化的物联网模型、物联网设备间的交互都是通过代理或者中心控制的方式进行。但是,这种方式在某些需要匿名通信的应用场景中并不太适合,这种特定的需求导致了去中心化物联网平台的产生。

区块链技术恰好为这种去中心化物联网平台的搭建提供了可能。由于点对点传输和安全度高的特性,区块链技术可以成为物联网底层的基础设施。在这种平台架构中,区块链扮演公开账本的角色,对智能设备之间所有的信息交换进行可靠、信任的记录。

IBM 和三星一直在致力于打造发展 ADEPT(去中心化的 P2P 自动遥测)系统,将采用区块链技术形成物流网设备分散式网络的骨干。ADEPT 技术的成熟代表独立分散的点对点遥测技术的发展,区块链在这个系统中将作为一个公共分类账设备,这将不再需要一个中央集线器来调解它们之间巨大的信息沟通量。没有一个中央控制系统确定彼此,这些设备将能够相互自主地沟通、管理软件更新、更正错误或实现能源管理。

4 区块链技术应用面临的挑战

区块链技术是很有应用前景的进步,正如前文所述,可以被应用到多种应用开发和问题解决上。从金融领域(从价值转移到投资等业务)到诸如文件鉴伪、物联网等非金融应用,区块链都可以发挥它去中心化、信息真实可靠的特点。然而,这些重要的区块链技术的创新使用同样面临一定的风险。

(1)行为改变

创新始终存在,但是对创新的接受程度,需要经过时间的沉积。在没有切实可信的第三方机构存在的环境中,区块链可以发挥自身最大的作用,区块链用户也将会适应区块链技术提供的安全、完整的交易环境。现阶段的第三方机构,比如 Visa、银联等机构,也需要接受这种地位上根本的改变,并对应用区块链技术采取积极的回应。但是在区块链技术大范围应用、改变用户的行为习惯之前,这些第三方机构还是会长久存在并为用户提供相应的服务。

(2)区块链体积

区块链系统的所有在网节点都持有区块链的所有区块记录。随着区块链的发展,节点存储的区块链数据体积会越来越大,存储和计算负担越来越重。这对区块链应用的新入

用户有一定的门槛。第一次加入系统的用户,必须花费时间和存储空间,同步所有的区块链区块记录,然后才能参与对区块链网络中具体交易的审核与追踪。以比特币区块链为例,其完整的数据大小当前已超过 70 GB。新用户加入比特币网络后,使用比特币核心客户端进行数据同步的时间超过 3 天。

(3)犯罪行为

基于区块链技术的交易有高度可匿名的特点,且区块链技术天然具有对价值转移行为的支持能力,因此区块链技术的应用,淡化了国家、监管的概念,弱化了现阶段执法部门的监督执法力度,增加了法务部门对洗钱等金融犯罪行为的查处难度。在区块链技术大范围应用以后,各国央行对经济能力的把控,尤其是货币政策的制定,需要更加的谨慎。

(4)性能瓶颈和高使用门槛

区块链通过提高算力的方式,解决分布式系统中的信任问题,因而在性能方面并不突出。比特币作为区块链技术的典型应用,它每秒只能处理 7 笔交易,而全网同步时间会达到 60 min(比特币每 10 min 产生一个区块,经过 6次确认以后的区块才能被接受),这在实际生产环境中效率过于低下,离应用级别效率差距太远。

5　结束语

总的来说,区块链分布式账本的功能性特点同时保证了它的安全性,因此区块链技术在金融和非金融领域都有广泛的应用。一些金融机构希望能够通过应用区块链技术发掘新的商业模式,获得新的盈利模式。

虽然区块链解决了信任问题,但带来了成本的上升和效率的下降。区块链技术与现有制度的整合成本过大,对于一些对时效性要求高、数据容量比较大的行业,在现阶段并没有很好的支撑方法。政策和资金是产业发展基础和催化剂,二者合力拉动区块链技术的快速发展与应用。区块链产业链完善,助力产业可持续发展。围绕区块链技术的生态圈丰富且完善,其不仅涉猎封闭保守的货币、金融等市场,更触及了去中心化、去中间信任等新兴领域,完善的产业链足以支撑区块链技术的快速、可持续发展。

未来产业结合点众多,市场投资机遇巨大。可以预见的是,区块链技术拥有广阔的应用场景,一切数字化及可以被数字化的场景都会有区块链技术的身影。可以说区块链技术的应用范围非常之广,包括货币、金融、智能资产、公证、物联网、医疗、通信、数据存储、供应链等诸多领域。但区块链技术底层技术不成熟,还处在早期阶段。未来 2~3 年区块链技术会在金融领域落地,重点关注金融科技类公司在区块链领域的应用以及布局。除此之外,还可以关注采用区块链技术服务的上市公司,主要看点在于公司业务是否适合采用区块链技术,采用区块链技术后,公司的产品和服务是否能够产生全新的商业模式或者远低于竞争对手的成本优势。

参考文献:

[1] 长铗, 韩锋. 区块链: 从数字货币到信用社会[M]. 北京: 中信出版社, 2016.
CHANG J, HAN F. Blockchain: from digital currency to credit society[M]. Beijing: China Citic Press, 2016.

[2] 杨晓晨, 张明. 比特币: 运行原理、典型特征与前景展望[J]. 金融评论, 2014(1): 38-53.
YANG X C, ZHANG M. Bitcoin: operating principle, typical characteristics and prospect [J]. Financial Review, 2014 (1): 38-53.

[3] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Consulted, 2009.

[4] HALABVRDA H, SARVARY M. Beyond bitcoin [M]. Berlin: Springer, 2016.

[5] AMMOUS S H. Blockchain technology: what is it good for[J]. Social Science Electronic Publishing, 2016.

[作者简介]

李董(1990–),男,现就职于中国联合网络通信有限公司研究院软件与系统实验室,主要从事大数据架构新技术研究、规划验证等工作。

魏进武(1978–),男,博士,中国联合网络通信有限公司研究院软件与系统实验室主任、副教授,负责和参与了国家“863”计划重大项目 5 项、国家科技重大专项课题 2 项,负责中国联通研发项目 50 余项,主要从事大数据、云计算以及电信 IT 系统等的设计及研发工作。