区块链技术应用研究与展望

Research and prospect of block chain technology

董慧,张成岩,严斌峰/DONG Hui, ZHANG Chengyan, YAN Binfeng
中国联通研究院 北京 100032
China Unicom Research Institute, Beijing 100032, China

摘 要:阐述了区块链技术的概念及原理,分析了区块链技术的优势;对区块链技术的应用进行了研究,并对区块链技术发展面临的主要问题进行了分析;最后提出了区块链技术最可能应用的领域及发展建议。

关键词:区块链;对等式网络;工作量证明

Abstract: The concept and principle of block chain technology was expounded. The advantages of block chain technology were analyzed. The application of block chain technology was studied, and the main problems in the development of block chain technology were analyzed. Finally, the most likely application areas and suggestions for the development of block chain technology were put forward.

Key words: block chain, peer-to-peer network, proof of work

1 区块链技术简介

区块链技术是近期比较火的一种技术,它伴随着比特币渐渐进入人们的视野,因此一提到区块链人们往往就会想到比特币,但实际上区块链并不等于比特币,它只是比特币的底层技术,是构建比特币区块链网络与交易信息加密传输的基础技术。区块链基于密码学原理而不是基于信用,使任何达成一致的双方可以直接支付,不需要第三方中介的参与,而比特币仅是区块链一个比较成功的应用,并不等价于区块链。

从本质上来说,区块链是一个安全、可信、去中心化的分布式数据库,或者说它就是一个分布式账本,记载所有的交易记录。前所未有的安全和可信,使区块链成为具有里程碑意义的应用技术,也就理所当然地成为目前数字货币的通用结构。

区块链技术并不是一种单一的技术,而是多种技术的整合和创新,包括密码学、数学、演算法与经济模型等技术,这些技术以新的结构组合在一起,形成了一种新的数据记录、存储和表达的方式。区块链技术中的核心技术主要包括以下几个方面。

(1)区块和链

区块链由一个个数据区块链接在一起形成,数据区块由区块头(Header)和区块体(Body)组成。区块头包括当前版本号(Version)、前一区块的散列值(hashPrevBlock)、当前区块的目标散列值(Bits)、当前区块共识过程的解随机数(Nonce)、Merkle 根节点散列值(hashMerkleRoot)和时间戳(Timestamp)。

hashMerkleRoot 是由区块主体中所有交易的散列值再逐级两两散列计算出的一个数值,主要用于检验一笔交易是否在这个区块中存在。

区块体包括当前区块的交易数量(Transaction Counter)以及经过验证的、区块创建过程中发生的所有交易记录(Transactions)。这些记录通过 Merkle

数的散列过程生成唯一的 Merkle 根并记入区块头。

每一数据区块都通过“前一区块的散列值”指向前一区块,形成一个巨大的链条,该链条一直追溯至源头即创世区块,创世区块的“前一区块的散列值”为零。

区块链通过时间戳来记账,形成了一个不可篡改、不可伪造的交易数据库。

(2)非对称加密

区块链所有权的信任基础是数学,用非对称加密算法保障交易数据的安全可信,每个节点都拥有一个私钥和公钥,私钥仅本节点拥有,公钥公开给 P2P 网络中所有的节点。交易发送时用私钥加密,接收方用发送方的公钥解密。

(3)分布式账本

即交易记账由分布在不同地方的多个节点共同完成,每一个节点都记录网络中所有的交易记录,因此它们都可以参与监督交易的合法性,也可以共同为某一交易作证。由于记账节点足够多,理论上除非所有节点都被破坏,否则账目就不会丢失,从而保证了账目数据的安全性。

区块链采用分布式记账、分布式传播、分布式存储,保证了系统内的数据存储、交易验证、信息传输全部都是去中心化的。

(4)共识机制

共识机制就是网络中的所有节点之间如何达成共识,认定一个交易的有效性,它既是认定的手段,也是防篡改的手段。区块链提出了 4 种不同的共识机制:工作量证明(PoW)、权益证明(PoS)、授权股份证明机制(DPoS)和验证池(Pool)。这 4 种共识机制适用于不同的应用场景,如比特币采用的是工作量证明机制。工作量证明的强大计算能力保证了区块链的安全性和不可篡改性,任何对区块数据的攻击或篡改都必须重新计算该区块以及其后所有区块的工作量,只有在控制了全网超过 51%的节点的情况下,才有可能伪造出一条不存在的记录,并且计算速度必须使伪造链长度超过主链,这种攻击难度导致的成本将远超其收益。

(5)智能合约

智能合约就是一种协议,它采用编程语言(脚本)而不是法律条文,基于可信的、不可篡改的数据,使系统有机会处理一些无法预见的交易模式,当约定的条件满足时,自动化地执行一些预先定义的规则和条款。

区块链分为三大类。

(1)公有区块链

无官方组织、无管理机构、无中心服务器,世界上任何个体或者团体都可以作为节点按照系统规则自由接入网络、不受控制,任何节点都可以发送交易,且交易能够获得该区块链的有效确认,任何人都可以参与其共识过程。公有区块链是最早的区块链,也是目前应用最广泛的区块链,各大比特币系列的虚拟数字货币均基于公有区块链。

(2)私有区块链

属于公司或个人所有,系统运行规则根据公司或个人需求进行设定。读写权限仅限于少数节点,只是使用区块链的总账技术进行记账,与其他分布式存储方案没有太大区别。

(3)联盟区块链

介于公有区块链和私有区块链之间,在某个群体内部指定多个预选的节点为记账人。每个块的生成由所有的预选节点共同决定,预选节点参与共识过程,其他接入节点可以参与交易,但不过问记账过程。其他任何人都可以通过该区块链开放的 API进行限定查询。

2 区块链技术的优势

(1)去中心化

区块链由众多节点共同组成一个端到端的网络,不存在中心化的设备或管理机构。任意节点的权利和义务都是均等的,节点之间数据交换通过数字签名技术进行验证,无需互相信任,只要按照系统既定的规则进行,节点之间不能也无法欺骗其他节点,且任一节点的损坏或者失去都不会影响整个系统的运作。区块链系统的去中心化结构具有极好的顽健性,同时,这种去中心化的结构大大提高了系统的运行效率,并大大降低了运营成本。

(2)公开透明

区块链系统是开放的,除了交易各方的私有信息被加密外,区块链中的所有数据对所有人公开,任何人都可以参与到区块链网络中,可以通过公开的接口查询区块链数据和开发相关应用,每一台设备都能作为一个节点,每个节点有一份完整的分布

式账本的数据库拷贝，因此整个系统信息高度透明。以比特币为代表的数字货币在交易验证环节的去中心化和集体参与的特点，是分布式账本公开透明的决定因素。价值在比特币网络中的传递并不依赖专门的第三方机构作为中介，每一笔交易都由所有矿工共同参与验证，由几乎随机的一个矿工记账。

(3)安全性

区块链用纯数学的方法建立信任关系，通过非对称密钥算法进行交易数据的加/解密，在每笔交易加入到主链中时，都将运行基于交易数据、交易方身份及历史交易结果的复杂的散列算法，以确保交易的正确性和安全性。每个节点存储全部交易数据，攻击者无法更改历史交易，从而使所有节点能够在去信任的环境中自由安全地交换数据，使得对人的信任变成了对机器的信任，任何人为的干预都不起作用。在以比特币为代表的数字货币网络中，所有参与者都拥有自己的账本备份，并且账本实时保持同步，已经被验证和记录的数据不可篡改。

(4)不可篡改

数据一旦经过验证并添加至区块链，就会被永久存储，除非能够同时控制住系统中超过 51%的节点，否则单个节点上对数据库的修改是毫无意义的，因此区块链的数据稳定性和可靠性极高。区块链中的每一笔交易都通过密码学的方法与相邻两个区块串联，因此可以追溯到任何一笔交易费的交易记录。

(5)匿名性

区块链的运行规则和数据信息是公开透明的，节点之间的数据交换遵循固定的算法，数据交互无需信任，因此，节点之间无需公开身份让对方对自己产生信任，每个参与的节点都是匿名的，极大保护了用户的隐私。

3 区块链技术的应用

区块链随比特币而生，却超越比特币，成为“互联网+”时代在互联网底层协议层面的重大技术突破。区块链技术发展到今天，其应用需求已经从最初的数字货币扩展到社会领域的方方面面。区块链凭借其去中心化、去信任、不可篡改、信息安全等特性，对于解决中心平台垄断、信息不对称等行业难题具有重要意义，在物联网、金融、大数据、云计算、通信、医疗、物流等领域拥有广泛的应用前景。

3.1 在金融领域的应用

区块链去中心化的分布式结构使人与人之间可以在去信任的情况下自行交易，无需中介机构的参与，因此，未来最可能应用区块链的领域就是金融行业的基础体系，如数字货币、征信系统、跨国支付与清算、证券登记转让与清算/结算系统等。这些系统现在都是中心化的，收费高且效率低，如果区块链技术能成功应用于这些领域，即使只节省 1%的中间费用，其应用前景也是相当吸引人的。

(1)数字货币

区块链在金融领域最成功的应用就是比特币。自从 2009 年比特币诞生以来，虽价格波动较大，仍以其稳定性和广泛的认可度征服了大量参与者。比特币实现了 7 年平稳地运行，承受了无数次网络攻击，且无专人维护，目前比特币产业链发展已相对完善。现实生活中比特币已逐渐被商家接受。北京一家餐馆从 2013 年 11 月底开始接受比特币支付，消费者在用餐结束时，把一定数量的比特币转账到该店账户，即可完成支付。2014 年 1 月，Overstock 开始接受比特币，成为首家接受比特币的大型网络零售商。世界首台比特币自动提款机于 2013 年 10月 29 日在加拿大温哥华启用，办理加拿大元与比特币的兑换业务。

(2)征信系统

目前金融行业的信用系统都是一个个独立的“孤岛”，各大银行之间并不互通。这种系统有着明显的缺陷，比如一个人上了一家银行的黑名单，那么他依然可以从另一家银行借到钱，因为信息不共享。但是数据的共享是市场的需求，是征信发展的大趋势。区块链技术可以将征信系统变为分布式存储，每个节点之间的数据是完全同步的，且不可被篡改，只有拥有正确的密钥才能访问数据，这样就可以实现征信数据的安全共享。

(3)跨国支付与清算系统

支付与清算领域存在很多痛点，最主要的就是安全问题频出、成本高昂、运行速度慢、效率低，在跨境支付、机构间清算尤其是跨境清算领域更为常见。区块链的安全性和分布式存储可有效弥补现在支付清算领域的不足，使跨境支付与清算更安全、

成本更低、效率更高。鉴于区块链技术在支付结算上的重要价值,国际上许多跨国大银行都积极参与到相关的研发测试中。2015 年 9 月,摩根大通、巴克莱银行、高盛等 9 家金融巨头共同投资创立了 R3 CEV 区块链初创公司,之后许多跨国银行纷纷加入其中,使之成为国际区块链联盟;2016 年 5月,中国平安也加入其中,成为首个来自中国的成员。

截至目前,金融领域是区块链技术介入最多、需求最大的一个领域。区块链技术的出现,让金融的去中心化成为了可能。首先,金融领域对区块链的第一个需求是数字货币,比特币由此诞生。其次,数字货币的成功发行大大刺激了传统银行业,银行、股权/有价证券交易所领域、保险领域也纷纷表现出了对区块链技术的强烈需求。由于金融领域与社会经济直接挂钩,因此其对区块链技术的探索也是走在时代最前沿的,技术需求会更快地转化为动力,加速区块链技术应用的落地。

3.2 在物联网领域的应用

近年来,物联网技术已经得到加速发展,根据 IDC 最新发表的一份统计报告,到 2020 年,全球物联网市场规模将增长至 30 000 亿美元,而全球物联网设备将达到 300 亿台。但是目前物联网技术发展面临一些问题,最突出的一个问题就是设备之间的互联互通性差,连接成本较高。由于物联网缺乏统一的标准,设备厂商各自为政,采用私有协议,导致不同厂商之间的设备无法互联互通,形成一个个“孤岛”。其次,物联网中心化的网络结构导致系统运行效率低,运营成本高,数据存储不安全,无法满足大规模的物联网设备的需求,海量物联网设备的海量信息给物联网信息处理中心带来了极大的负荷,一旦出现通信故障,将会造成灾难性的后果。物联网面临的另一个问题就是网络中的用户与用户、用户与设备、用户与网络之间的相互信任与安全问题。

区块链技术的去中心化、匿名性可以很好地解决物联网的上述问题。区块链技术无疑是针对物联网中存在问题的完美解决模式。智能设备以开放的方式接入物联网中,设备与设备之间以分布式的网络相连接,不再需要一个集中的服务器充当消息中介的角色,设备之间建立一个低成本的、点对点的直接沟通网络,在网络中每个设备都互不认识,充分保护了用户的隐私性。

在物联网领域已有一些应用案例:如 IBM 正在开发的 Adept 项目中使用区块链技术创建一个可行的分布式网络,该系统使用 BitTorrent(文件分享)、Ethereum(以太坊平台)和 TeleHash(点对点信息发送系统)来支撑 Adept 系统,是一个在物联网领域使用区块链技术的概念验证;Slock.it 公司致力于通过区块链实现闲散资金的共享;VISA 与 DocuSign 联合推出区块链汽车租赁项目等。这些应用或应用常识充分证明了业界对区块链在物联网领域的应用抱有积极的态度,并尝试应用的落地。

3.3 在大数据领域的应用

大数据共享的主要难点和挑战是如何在保护个人隐私的情况下开放数据。基于区块链的散列处理等加密算法可将一些数据进行脱敏处理,为隐私保护下的数据开放提供了解决方案。例如,基于区块链技术的英格码(Enigma)系统,在不访问原始数据的情况下运算数据,可以对数据的私密性进行保护,杜绝数据共享中的信息安全问题。

对于个人或机构有价值的数据资产,可以利用区块链对其进行注册,交易记录是全网认可的、透明的、可追溯的,明确了大数据资产来源、所有权、使用权和流通路径,对数据资产交易具有很大价值。

区块链的可信任性、安全性和不可篡改性,保障了大数据的安全性、隐私性及不可篡改性,非常符合大数据的核心需求,将来必会在大数据领域广泛应用。

3.4 在通信领域的应用

通信领域最重要的问题是信息安全问题。区块链技术通过去中心化方式,完全改变了信息传输的渠道,由于网络中的每个人都能收到这份信息,但只有拥有私钥的人才能打开,这就保证了即使信息被拦截也无法被获取,而信息的跟踪也就无法实现。

3.5 在医疗领域的应用

医疗行业中的许多资料都是非常私密的,对其阅读与管理权限的保护要求也十分苛刻。然而,目前中心化结构下的资料存储方式无法很好地保证资料的安全性,经常会造成病人的健康数据被泄露。而且一旦系统出现问题就会造成大规模的数据外泄,带来严重后果。区块链技术可以通过非对称

加密技术和签名技术来防止这类情况的出现。当数据被散列处理后放置在区块链上,使用数字签名技术就能控制数据的访问权限,使只有获得授权的人才可以访问数据。健康数据统一存储在去中心化的区块链上,在不访问原始数据的情况下进行数据分析,既可以对个人健康数据的私密性进行保护,又可以安全地提供给全球科研机构或医生共享,作为全人类的基础健康数据库,对未来解决突发疾病、疑难疾病带来了极大的便利,其应用前景非常广阔。

3.6 在物流供应链领域的应用

目前市场中的供应链系统并没有为货物提供一套完全可追踪的物流数据,许多物品的物流信息中途流失,为假冒伪劣产品的横行提供了机会。如果区块链技术能为供应链中的物流信息提供认证服务,那么通过区块链数据库的源头追踪功能就可以很快地找到问题所在,实时追踪商品流转信息,实现全透明消费。

3.7 在投票领域的应用

目前社会中的投票方式还很不完善。基于区块链技术的投票可以在很好地保护投票人身份的同时,快速统计出结果,让整个投票系统能高效率、低成本地运行。目前纳斯达克已经正式试行区块链技术,未来,来自投票领域的需求还会进一步扩大。

3.8 来自其他领域的需求

以上几个领域都是较早接触区块链技术并已开始取得初步探索成果的领域。现如今,随着区块链技术越来越广为人知,更多的领域开始意识到区块链技术的重要性,也逐渐展现了对这种全新技术的需求。P2P 借贷领域需要区块链的去中心化信任功能来建立一个公开透明的借贷市场;审计领域需要区块链的数据库功能来保证审计数据的真实性与可追踪性;拍卖领域需要区块链数据的公开透明功能来保证拍卖的正常进行;教育领域需要区块链的时间戳及数据库功能来帮助提供学历证书的认证;智能资产领域需要区块链的数据自动处理功能帮助资产实现智能化和自动化;甚至游戏、彩票领域也需要区块链的数学功能来保证摇奖时的公正性。除此之外,还有许多其他领域也有应用区块链技术的需求。

4 区块链技术应用面临的问题

尽管区块链有明显的优点,但是它也存在一些明显的问题。

① 由于私钥只有节点自己拥有,现有的机制对私钥没有构建私钥恢复机制,如果丢失私钥,该节点就无法查阅所有的历史数据。如果是比特币,就相当于丢失了自己所拥有的比特币资产,没有任何人可以得到和私钥对应的那些比特币。

② 区块链的匿名性增加了犯罪组织洗钱的可能性。由于交易双方都不了解对方,一些犯罪组织可以在网络中隐姓埋名,从而实现洗钱的目的。

③ 海量的数据存储。由于每个节点都需要保留所有的交易数据,导致了海量数据需要存储,安全可靠地保存这些数据需要大量的数据存储设备。

④ 极高能耗。由于每个节点都想争当矿工,而计算一个随机数并不是很简单的事情,因此需要计算机 24 h 不间断地计算并解决难题,现有的挖矿机制需要优化。

⑤ 安全性。从理论上来讲,获取区块链上 51% 的节点的数据并进行伪造是有可能的。随着计算机技术的飞速发展,未来可能会生产出高效计算机,这些超高速计算机可以极大地缩短节点计算机的计算时间,占领区块链上 51%的节点。

⑥ 无索引大规模数据检索困难。

⑦ 无政府主义,无法监管。区块链发明的初衷就是不想让人来监管,而缺少监管会带来另外一些问题,如现在美国有很多人利用比特币网络卖毒品、卖军火,却无法查询到具体交易信息;也有人利用区块链技术洗钱,却无法查询到具体操作者。这些问题都会给社会安全带来隐患。如何在保留区块链技术特点和优势的前提下解决安全问题,是第一个要面临的挑战。

⑧ 合规性问题。在做区块链应用落地(如跨境交易)时要考虑怎样才能合规、合法。

⑨ 区块链技术本身的问题。由于区块链技术设计的初衷是保证安全,为了保证安全,需要全部节点见证交易过程,这将会导致交易速度比较慢,因此不能达到银行的要求。

区块链技术不会因为上述问题而停滞不前。随着人们对区块链技术优势的认识越来越深刻,越来

越多的资本、人才、资源正在源源不断地投入到相关技术的研究中,区块链技术的上述缺陷得到解决只是时间问题,应用也会越来越普及。

5 结束语

区块链技术的发展及应用在世界各地产生了重要的影响,相关的成果也越来越多。在中国,关于区块链技术的发展及应用如火如荼,一些崭新的理念与突破性的成果引起了人们对于区块链技术的关注。不过,作为一门新兴的技术,区块链技术尚处于发展阶段,目前对区块链的应用更多地还停留在理论研究与验证阶段,真正基于区块链技术的商用应用或产品还不多。要想广泛应用区块链技术,应该聚焦于如何解决一些公司的痛点,找到合适的落脚点并在现实中发挥作用,这是区块链技术应用亟待解决的问题。

根据笔者的研究,区块链技术的应用应该划分为以下几大类。

① 区块链技术基础平台,也可以叫区块链即服务 BaaS(Blockchain as a Service),对外提供区块链技术的基本功能,如以太坊;

② 基于区块链技术平台开发的区块链应用或产品;

③ 区块链的安全性研究;

④ 基于区块链的大数据挖掘与分析。

区块链技术经历了 1.0 数字货币、2.0 智能合约和 3.0 治理 3 个阶段,随着研究的深入将会带来一系列新的变革。

参考文献:

[1] 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.

[2] 中本聪. 比特币:一种点对点电子现金系统[EB/OL]. https://bitcoin.org/bitcoin. 2009.

[3] 谭磊,陈刚. 区块链 2.0[M]. 北京: 电子工业出版社, 2016.

[4] 唐文剑. 区块链将如何重新定义世界[M]. 北京: 机械工业出版社, 2016.

[5] 梅兰妮·斯万. 区块链: 新经济蓝图及导读 [M]. 北京: 新星出版社, 2016.

作者简介

董慧(1971–),女,现就职于中国联通研究院研究院终端与测试实验室, 主要从事移动终端、智能卡、移动应用等相关领域的关键技术、业务和安全的研究工作。

张成岩(1977–),男,现任中国联通研究院终端与测试实验室终端数据与应用研发组组长,主要从事移动终端、智能卡、移动业务、移动应用等方面的研究、开发与测试工作。

严斌峰(1977–),男,中国联通研究院终端与测试实验室主任、高级工程师,主要从事终端与智能卡相关研发工作, 主要研究方向为移动增值业务、终端与智能卡相关技术、终端基础软件技术等。

· 30 日扫描 ·

工业和信息化部要求运营商全面落实电话实名制

11 月 7 日,为了有效打击电信诈骗犯罪,工业和信息化部发文要求各家运营商必须从严、从快全面落实电话用户实名制, 必须在年底前实现 100% 的实名率。

“各基础电信企业要加快推进未实名老用户补登记,在 2016 年底前实名率达到 100%。”在规定时间内未完成补登记的用户,一律予以停机。对于新入网的电话,工业和信息化部要求运营商严格落实用户身份证件核查责任,采取二代身份证识别设备、联网核验等措施验证用户身份信息, 并现场拍摄和留存办理用户照片。通过网络渠道发展新用户时,要采取在线视频实人认证等技术方式核验用户的身份信息。