基于区块链技术的应用研究

尹子君　何小虎

摘要：区块链作为比特币的底层技术，重构了信用机制。其通过分布式节点对网络数据进行存储、验证、传递和交流，自被开发以来就受到全世界各个行业的追捧，成为当今最热门的信息技术之一。本文主要介绍了区块链系统的基本流程和基本框架，在对区块链相关基础技术进行说明后，从区块链发展的三个阶段来分别对区块链技术的应用进行分析。

关键词：区块链；比特币；区块链技术原理；非对称加密；区块链技术应用

中图分类号：TP311.13；F125；F832.2　　**文献标识码**：B

基金项目：陕西省教育厅基金项目（18JK0279）、陕西省军民融合研究基金项目（17JMR28）、渭南师范学院项目（17YKS13）、渭南师范学院大学生创新创业训练项目（18XK052）。

作者单位：渭南师范学院网络安全与信息化学院

一、引言

比特币在过去几年的时间里成为全世界追逐的浪潮，虽说最近这股浪潮已经逐渐趋于平淡，但是其背后的底层技术——区块链技术却逐渐引起了人们的重视。在信息技术高速发展的今天，各行各业的人都在寻求一种新的技术来注入自身的行业中，使自身能够在社会经济不断发展的大环境下不被淘汰，而区块链技术便是信息技术行业所能注入的“新鲜血液”。区块链已经被认为是网络交易双方信任的机器，这种形式在不久的将来将改变我们网上交易传递的方式。

二、区块链系统运行的基本流程

区块链主要使用地址来识别交易双方。交易双方的全部交易信息是要被记载到一个统一的账目本上，但是这个账目本的信息是要通过区块来完成的。在网络交易中，会产生新的区块，每个新区块产生都会记录产生的时间，然后对产生的每个区块会按照记录的时间进行排序，并在区块中记录交易的证明。每个交易中的节点都点对点建立联系，通过这种形式的交易模式，改变原来的中心化方式，采用由所有节点组成的分布式交易形式。

网络中区块链交易的基本过程主要包含5个步骤。

第1步，建立交易。每个交易中会使用自己的私钥对上一个交易者和下一个交易者专门签署一个安全的数字签名，在每次交易时都会把签署的数字签名和货币集中到一起，从而生成这次的交易记录单。

第2步，在网络的交易中采用的是点对点的网络模式。当交易一方交易时首先会把交易的记录单发布到网络中，然后把交易币发给另一个交易方。网络中的每一个节点都会收到网络中发布的交易单，从而把交易信息加入到区块中。但是，接受交易币的一方需要网络中6个以上的区块进行确认后才能获得这次交易的费用，否则是不能得到交易的比特币的。

第3步，在交易中进行安全验证。网络中的每个节点需要解决网络中提供的1道题，答对这道题才能获得建立区块的权利，建立好区块后也可以获得比特币的奖励。

第4步，验证结果。如果某一个节点求出数学题的解时，就会向网络中发布自己进行交易的全部时间记录，然后由网络中其他节点对时间记录进行核实。在核实过程中需要从5个以上节点获取时间进行核实，然后取所有时间的中间值作为最后的交易时间戳。

第5步，交易信息计入账目本。在整个网络中，其他所有节点都会核实该区块交易记账记录的正确性，如果没有任何问题后大家就会把刚才交易的区块合法，然后再申请下一个区块，通过这种形式慢慢形成一条合法的区块链。

比特币网络中每个节点都基于已存在的最新区块生成下一个区块，同时将网络中未确认的合法交易包含进去。在完成工作量证明之后，将新的区块广播到全网，同时获得取款的奖励，这个过程就是将所有的交易打上时间戳标记的过程。

三、区块链技术的应用实例分析

虽说区块链技术起源于比特币，但如今区块链技术的应用早已不局限于比特币。区块链技术如今已经在多个领域各行各业中得到应用，因为其不需要第三方参与（即无需中介），数据安全度较高，过程高度透明且成本低廉，所以，任何行业只要有需求，就都会有机会使用到区块链技术。

（一）区块链1.0：货币和支付系统（以Ripple为例）

Ripple系统所属运营公司为美国的Ripple Labs，Ripple实验室正式成立于2012年，其研发的Ripple平台旨在为全球银行类金融机构提供跨境支付服务。通过Ripple支付网络

可以转账任意一种货币,简便快捷,交易确认通常在几秒内就可完成,交易费用几乎是零,不存在所谓的跨行异地和跨国支付费用。作为分布式点到点的支付网络,Ripple 让世界各地的银行可以无需通过中央银行或代理银行直接交易,其在跨境支付领域的应用能够帮助银行节省运营时间和成本。全球中第一笔采用区块链的跨境银行交易大概需要 2 到 6 个工作日,但是采用了 Ripple 新技术后,仅仅需要 8 秒之内即完成了交易。加拿大的 ATB Financial 银行, 在 2016 年 7 月 14 日宣布成功借助 Ripple 的区块链网络,仅仅用了 20 秒就将 1000 加元成功发送给德国。

(二)区块链 2.0:智能合约(以以太坊为例)

以太坊是基于区块链技术的智能合约和去中心化应用平台,是区块链 2.0 的代表应用。比特币开创了去中心化加密货币的先河,从上线至今多年的时间充分检验了区块链技术的可行性和安全性。但比特币并不完美,其中的不足之处在于协议缺乏扩展性,使比特币区块链难以拓展更高级的应用, 而以太坊从设计上就是为解决比特币扩展性不足的问题。

2013 年年末, 以太坊创始人 Vitalik Buterin 发布了以太坊初版白皮书,在全球的密码学货币社区陆续召集到一批认可以太坊理念的开发者,启动了项目。类似安卓或 IOS 操作系统,以太坊作为开源的区块链底层系统,提供了非常丰富的接口,让许多开发者能够在上面快速开发出各种区块链应用。目前, 已有超过 200 多个应用在以太坊上开发。比如 Branche 就是基于以太坊区块链网络构建的去中心化金融服务项目,旨在为没有银行卡或无法获得银行金融服务的人群提供小额贷款、借贷、支票兑现以及其他基础金融服务。当客户进入 Branche 网络并需要像小额借贷这样的金融服务时,系统就会自动匹配一个供应商,同时启动一个智能借贷合约并强制保证合约的执行。

(三)区块链在 P2P 网络借贷中的应用优势

P2P 网络借贷的发展能够在一定程度上缓解金融资源错配、小微企业融资难问题,但目前行业仍然乱象丛生、问题频发,一些劣质平台违规经营、非法获利,利用 P2P 网贷平台非法集资进行放贷,在资金链断裂时跑路,给投资者造成损失,也扰乱了正常的市场秩序。在当前 P2P 网络借贷行业加强监管、规范整治的背景下,利用区块链技术有利于 P2P 网络借贷行业的规范发展,从而更好地保护投资者的利益。

在区块链模式下,平台只是作为交易的场所,而非交易的中介机构。具有资金需求的借贷人以及拥有理财需求和闲置资金的出借人可以在平台上直接进行交易而无需第三方撮合。具体而言,借贷人在平台上发布资金需求,由于区块链的公开透明特性,出借人可以查询借贷人的历史还款记录来判断借贷人的信用状况。平台上的每个借贷人和出借人都是系统中的节点,存储着所有区块交易数据的副本,能够随时随地下载更新账本,参与共识验证交易的合法性。

四、结束语

从比特币掀起的数字货币浪潮开始到现在,区块链技术已经逐渐成为学术界和商业界以及金融界的热门话题,由于区块链技术的去中心化、不可篡改等特点,使其在商业界和金融界已经有了广泛的应用。笔者从区块链技术的特征入手,逐步浅析区块链技术的原理,再从其原理转到当今已经应用到区块链技术的一些应用中去,从应用中浅析区块链技术的特点,从而得出区块链技术的发展前景及发展限制。

参考文献:

[1]马昂,潘晓,吴雷,郭景峰,黄倩文.区块链技术基础及应用研究综述[J].信息安全研究,2017,3(11):968-980.

[2]张健.区块链[M].北京:机械工业出版社,2017.

[3]阿迪瓦特·德什潘德,凯瑟琳·斯图尔特,路易斯·列皮特,莎莉·古娜什卡尔,韩晓涵.理解分布式账本技术/区块链——挑战、机遇和未来标准[J].信息安全与通信保密,2017(12):20-29.

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

[5]何蒲,于戈,张岩峰,鲍玉斌.区块链技术与应用前瞻综述[J].计算机科学,2017,44(04):1-7+15.

[6]姚忠将,葛敬国.关于区块链原理及应用的综述[J].科研信息化技术与应用,2017,8(02):3-17.

[7]李董,魏进武.区块链技术原理、应用领域及挑战[J].电信科学,2016,32(12):20-25.

[8]张偲.区块链技术原理、应用及建议[J].软件,2016,37(11):51-54.

[9]谢辉,王健.区块链技术及其应用研究[J].信息网络安全,2016(09):192-195.

[10]骆慧勇.区块链技术原理与应用价值[J].金融纵横,2016(07):33-37+76.

[11]李政道,任晓聪.区块链对互联网金融的影响探析及未来展望[J].技术经济与管理研究,2016(10):75-78.

[12]叶小榕,邵晴,肖蓉.基于区块链、智能合约和物联网的供应链原型系统[J].科技导报,2017,35(23):62-69.