区块链技术原理与应用价值

骆慧勇

摘要:本文从技术层面解析区块链的核心,介绍了区块链相关计算机技术、数学知识以及区块链的信息交互原理,总结了区块链技术的三大价值和优缺点,并对未来应用前景进行预测。

关键词:区块链 技术原理 应用价值

中图分类号:F831.2 文献标识码:A 文章编号:1009-1246(2016)07-033-05

一、区块链概念

严格来说,区块链与区块链技术是两种概念,区块链是指利用数学和技术手段记录数据信息,对达到指定大小的数据进行打包形成区块并链接进入往期区块形成统一数据链的数据记录方式。区块链技术则是指不依赖第三方、通过自身分布式节点进行数据交互、验证、存储的一种技术方案。一般情况下提到的区块链均指区块链技术。

区块链技术起源于比特币,却并不局限于比特币。区块链因自身特点,可以应用到信用证明、权益交易等领域,因此区块链技术受到多方关注。如2016年1月中国人民银行行长周小川在北京数字货币研讨会上提出需要关注区块链等技术对金融发展带来的影响。

区块链技术的重大意义在于实现了不可信环境中可信信息交互问题。区块链技术去中心化、安全性等特点也具有较高的创新意义。在实际应用中,区块链可以根据去中心化的程度分为公共链、联盟链、私有链,公共链类似比特币完全去中心化,联盟链则具有一定中心权威机构,私有链则是具有完全中心机构的区块链技术应用。

二、区块链技术原理

由于区块链技术被大量改造,与比特币原有技术已有一定的区别,但核心技术构架并未改变,本文仍以比特币底层区块链技术作为标准对区块链技术进行介绍,主要内容如下:

(一)相关知识介绍

1. P2P网络

一般网络系统都是由服务器与客户端组成,而P2P网络则只通过客户端直接通信,客户端可能既是数据读取者也是数据发送者,信息可能需要经过多次转发才能到达最终使用者。由于P2P网络的这种广播特性,重要数据保密性及信息发送者的验证成为重要问题。

2. 非对称加密算法

通过设置一对秘钥,分别用于信息加密与解密。可以公开一个秘钥,成为公钥(Public

key),另一个保密并成为私钥(Private key)。加密信息使用公钥,私钥则用作解密,在得知一个秘钥的情况下无法推算出另一个秘钥。如果一对秘钥满足这样的条件,这一类加密算法被统称为非对称加密算法。

3. 哈希(Hash)算法——散列函数

哈希算法可以将任意长度的输入经过转换得到固定长度的输出,具有单向及固定长度输出的特点,一般用作验证数据的完整性。

(二)信息交互原理

通过研究比特币交易流程,可以理解区块链应用中如何实现交互信息的记录。以在比特币交易中所有者1尝试向所有者2支付为例,所有者1则提供:资金来源(即上次交易单的哈希值,交易单1此时已通过P2P全网认证)、支付金额、收款地址(所有者2的公钥)、交易单1的内容与所有者2的公钥连接后通过哈希算法得到的哈希值,再用所有者1的私钥进行加密,得到的密文作为数字签名放在新的交易内容中。新的交易内容制作完成后,所有者1计算哈希值并作为新交易单的ID,将ID和新交易单内容向P2P全网广播。交易数据交互情况如图1所示。

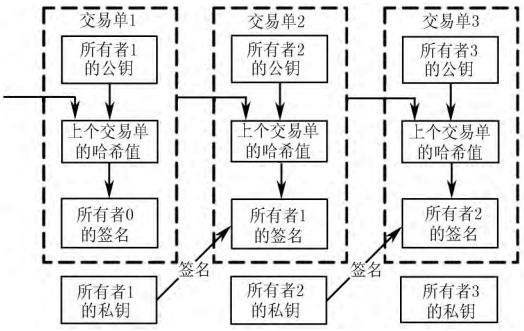

图1 比特币交易数据交互

当进行全网广播后,P2P网络其他节点,通过新交易单中上次交易单的ID获取交易单1,根据所有者1的公钥对交易单2中的数字签名进行解密得到哈希值,同时将交易单1的内容与所有者2的公钥连接并计算哈希值,如果两次计算得到的哈希值相同,则可以认为交易有效。

(三)区块链原理

由于P2P网络没有可信中心服务器,无法实现准确的时间同步,因此各个节点时间可能存在延迟。在交易过程中可能存在不同节点收到信息不一致的情况。为了规避该问题,通过人为设定一段时间将交互数据打包,形成一个区块。区块的生成通过最先完成特定数学运算的客户端产生,当多个节点得到正确答案时产生的区块,这时候会以交易链长的区块作为主链,其它的丢弃。

区块链通过时间戳的方式解决了区块的排序问题。在客户端生成区块时记录上一个区块通过哈希算法得到的哈希值,实现了区块生成次序与系统时间脱钩。另外,一旦区块的次序固化,当攻击者试图改变某区块内交易时,需要对该区块及以后的区块进行重新计算及修改,在P2P网络中几乎不可能实现,更好地达到了安全性要求。区块链结构示意图如图2所示。

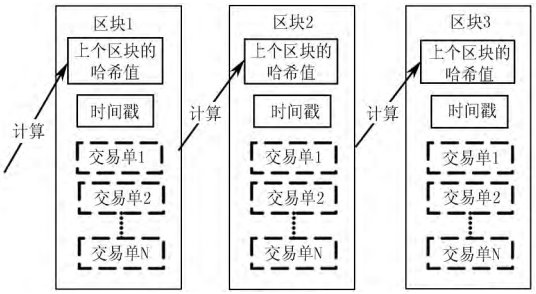

图2 区块链结构示意

三、区块链价值

区块链技术起源于比特币,随着公共链、

联盟链、私有链应用后,其价值在更多的应用中逐步体现出来,根据这些分层应用情况,可以总结出区块链技术的价值共性:

(一)解决了"信"的问题。区块链技术提供了一种无需信任单个节点,还能按照共识基础进行安全信息交互而不用担心数据篡改的方法,应用技术手段实现了不可信渠道的信息传递,也解决了不可信用户之间可信交互的验证问题。

(二)解决了"账"的问题。区块链技术在记录信息交互过程中使用P2P网络实现客户端节点全数据记录,具有足够的数据冗余,保障了账的保存安全。另外根据区块链技术构架,如果要对区块内部数据进行非法篡改,需要控制P2P全网51%的客户端节点,这也意味着篡改难度极大。

(三)解决了"实"的问题。区块链技术限制参与信息交互者,如不能被全网证明拥有某权益等,则不能进行交互,不能实现类似信用透支之类的操作。这进一步夯实了区块链带来的价值体系——不可预支。通过"实"可以实现权益的证明,如资金、房产,也可以实现对信息的验证,如证书、执照的证明。

四、区块链优缺点

(一)区块链的优点

1. 安全性:区块链技术的安全性主要体现在信息交互能够有效避免人工干预。去中心化特性及信息交互时严格遵守指定的数学规则,可以有效保障信息交互防篡改;参与区块链交互者在安全保存私钥的前提下,信息交互的安全能够得到有效保障。

2. 便捷性:区块链技术对信用问题的解决相对完善,在信息交互中不需要复杂的中心权威机构身份验证,信息交互时更为便捷。同时由于无需构建专用存储环境、信用体系,在构建应用环境、建设相关应用时更为便捷。

3. 透明性:区块链的交互信息由于具备分布式记账、全副本、可追溯等特点,对于任何信息交互均可以追踪和查询,可以提升信息交互的透明度。

(二)区块链的缺点

1. 安全性问题:区块链应用中的账户即为用户的公钥,进行信息交互的手段则是私钥。一旦私钥丢失,用户原有参与信息交互的权利随即丢失,没有中心机构可以实现信息重置,这种对安全性的担忧,是技术无法解决的。另外在防篡改方面,虽然必须在掌控全网51%以上客户端节点的基础上才能够对区块链的信息交互记录进行篡改,但通过整合算力等技术手段,仍然有可能对区块链应用的安全造成威胁。

2. 调解难题:区块链应用由于去中心化很难实现纠纷调解。即便是私有链,也可能存在着由于权益导致的纠纷,发生纠纷后就算有类似纠纷调解机构或者机制,也存在着调解难的问题。承担调解职责的第三者因为没有相关的私钥,无法实现强制操作,必须调解双方达到共识并进行操作,才能完成权益的重新分配。

3. 延时问题:由于P2P网络的天然缺陷,必然造成时间的同步问题,所以高度的实时同步很难做到。另外交易的确认需要全网客户端参与,具有较高的延时特性,所以区块链会有一定的实时交互问题。这一问题在比特币

的流通中也存在,是相对传统货币的弱势。

4. 资源浪费问题:区块链技术需要在 P2P 网络参与客户端中存储整个信息交互账簿,对数据存储具有较高的要求,如比特币运行至今,若完全保存所有区块需要 60G 以上的存储空间,重复的数据存储造成较为严重的存储资源浪费;区块链在信息交互中进行数据加密、哈希运算、形成新区块时需要大量的算力,相对中心结构的应用具有明显的算力资源浪费。

五、区块链技术应用前景

目前,纳斯达克、纽交所、花旗银行等数十家金融机构已对区块链技术进行了多种尝试,如 2015 年纽交所宣布投资比特币交易平台 Coinbase;2015 年 12 月美国纳斯达克推出基于区块链技术的证券交易平台 Linq,成为区块链技术应用的重要里程碑;2016 年 1 月英国政府发布了一份名为《分布式账本技术:超越区块链》的报告,主要介绍了区块链如何减少金融诈骗、错误、改造流程等,最重要的是试图由政府参与数字货币与区块链的立法。根据目前的发展情况,预判区块链未来主要发展前景如下:

(一)从发展现状来看,公共链主要应用集中于数字货币

数字货币主要有比特币、莱特币(Litecoin)、域名币(Namecoin)、点点币(Peercoin)等,这些数字货币应用改造过的区块链技术能够在一定程度上提高交易效率、实现更多的隐私保护、降低交易成本、交易可以强制回滚等,这可以改善部分区块链技术的缺点。

(二)从发展可行性来看,联盟链在金融领域将大有作为

联盟链一般是由多个中心化机构联合组成,是介于私有链和公有链之间的区块链应用,特别适合在产业、行业内部进行应用。联盟链本质上不是简单的去中心、反中心,而是多中心或弱中心。

建立银行业联盟链,可以实现更低成本、更准确、更安全的金融服务。银行业作为金融机构体系的主体,在经营领域具有业务综合、功能全面、覆盖面广等特点。通过银行业联盟链应用,可以逐步实现更多的金融领域的联盟链应用,进而对支付体系产生一定的改变。基于现有金融体系的构架,联盟链应用需要关注以下几点:

1. 建立银行业联盟链组织构架

建立银行业联盟链,首先应考虑组织构架,才能够明确、统一具体的技术标准、应用规范,因此需要权威机构对区块链技术在银行业的使用制定行业标准、技术协议等。权威机构在面对未来可能的国际标准协议制定时,也具有较强的话语权。

2. 以自金融为出发,逐步拓展跨行业应用

“自金融”是互联网时代提出的新概念,可以理解为居民之间的直接投融资行为,也可以理解为去中介机构、去交易媒介的交易行为。银行业联盟链的建设应以银行、客户为中心,实现快速的自金融服务,并逐步拓展银行之间、银行客户之间的自金融服务。

3. 银行业联盟链仍需要解决的一些问题

区块链由于其技术构架带来的天然缺陷,致使实时交易无法实现。联盟链虽然可以一定程度上规避该问题,但由于银行业对实时交易的高要求,仍然需要关注交易实时

性问题,该问题可以从网络提速、节点数量控制、时间校准、统一应用、基础协议等方面进行考虑。

如何实现安全、可信的初始交易货币输入是银行业联盟链的另一难题。比特币根据算法实现单位时间内产生定量货币,并根据节点计算量进行分配。而联盟链由于多中心特点,如何实现可靠货币源是一大难题。依托唯一的权威中心作为货币源机构进行资金的证明是一个比较可行的方案,同时应更多地考虑实现资金来源的全网信任,更好地体现区块链技术的"数字化信用"优势。另外需要注意的是由于区块链技术对交易的严格校验,一旦初始货币输入错误、异常则难以调整,因此对输入准确性、货币源的机构信息安全性要求较高。

4. 金融监管、调解将出现新的改变

金融领域、货币领域联盟链一旦形成后,货币流转被确认的过程就是清算、结算和审计过程,监管需要的交易数据不再依赖于现场查账、数据对比、统计报送等传统手段,规避了数据收集、反馈、交流中容易出现的迟滞、失真、片面等问题。任意中心的全账本数据能提供非常准确的交易数据,但数据类型单一、与监管需求数据存在差距,同时也面临着交易复杂、数据量大、监管规则配置繁琐等问题。如何实现自动化的监管对象确认、规则配置、数据分析、数据筛选将是新的问题。

此外,联盟链无法较好地规避调解难题。金融纠纷发生后,中心机构是否能够强制实现交易回滚是实现调解的关键,技术上可以实现但引入类似机制则会破坏信用体系,这是一个很难规避的问题。联盟链解决调解难题不光需要制定可靠的技术方案,更应建立合理的约束管理机制。

(三)从区块链技术应用方向进行考虑,当前主流方向主要有三大类别

信息安全服务:区块链 P2P 网络中客户端均有同样的数据副本,实现了数据的存储不再依赖极少的中央服务系统;信息交互使用时间戳、数字签名等手段,避免了受到黑客攻击时数据受到非法篡改的情况;区块链技术的多重签名扩展技术可以保证重要数据的访问权限不易被非法获得。这些应用特点可以实现用户个人隐私数据的安全存储服务,例如个人的财产、医疗等隐私信息。

公共信用服务:区块中哈希值效验、时间戳等严格界定了区块的次序,保障了区块信息的不可篡改和伪造。因此区块链技术可以用作政府机构颁发的证书、执照、许可证,甚至可以作为个人身份信息的证明,实现诸如选举投票、民主评议等。同时在对相关信用信息进行验证时,任意时间都可以通过区块链数据访问快速证明信用信息的真实性,减少原有通过纸质、人工进行复杂验证的损耗。

金融交易服务:区块链的不可预支价值体系保障了区块承载权益的"真实性",保障了不可信双方间进行金融权益交易的安全性。因此可以用于资金交易、债券交易、网络借贷等商业模式,能够避免繁琐的身份验证、交易清算过程,降低金融交易成本。金融交易服务是区块链技术应用中最早也是最为适合的应用环境。 (下转第 76 页)

村金融研究,2010,(5).

[5] 杜晓山. 小额信贷的发展与普惠性金融体系框架[J]. 中国农村经济,2006,(8).

[6] 杜晓山. 建立可持续性发展的农村普惠性金融体系——在2006年中国金融论坛上的讲话[J]. 金融与经济,2007,(2).

[7] 梁岩. 信用信息识别型信贷配给及二元信用约束下农村普惠金融发展的困境与纾解[J]. 华北金融,2016,(1).

[8] 嵇少峰. 中国普惠信贷困局再思考[J]. 中国银行业,2015,(9).

课题组组长:戚军

课题组成员:陈明政、蔡士明、梁岩(执笔人)

作者简介:

戚军,男,供职于中国人民银行宿州市中心支行。

(责任编辑:彭恒文 校对:JZY)

(上接第37页)

参考文献:

[1] 蒋润祥,魏长江. 区块链的应用进展与价值探讨[J]. 甘肃金融,2016,(2).

[2] 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).

[3] 庞博. 比特币能否取代传统货币[J]. 电子制作,2013,(16).

[4] 陈怡璇. 区块链技术 "分布式账簿"[J]. 上海国资,2016,(3).

[5] 龚鸣. 英国对区块链技术的态度[J]. 金融博览,2016,(3).

[6] 肖风. 从公有链到私有链:区块链回归现实[J]. 当代金融家,2016,(2-3).

[7] 王永利. 区块链,下一代互联网金融革新技术[J]. 博鳌观察,2016,(2).

[8] 张波. 国外区块链技术的运用情况及相关启示[J]. 金融科技时代,2016,(5).

作者简介:

骆慧勇,男,供职于中国人民银行泰州市中心支行。

(责任编辑:冯娟娟 校对:CL)