

区块链技术的实质、落地条件和应用前景

邓柯

(质数链网科技成都有限公司,四川 成都 610041)

摘要:区块链作为一种网络数据库、一种使用区块记录交易信息的账本,本质上是一种分布式公共账本,即以密码学为基础构建的一系列链式数据结构并保证其不可篡改和不可伪造。区块链不是一种单一技术或框架,而是对互联网时代技术和平台的分布式重构。区块链技术是一种将数据进行加密并打上时间戳,数据根据时间戳次序形成数据链,并以分布式的方式进行存储数据的一种技术。这种技术涵盖了点对点传输、共识机制、加密算法、分布存储等多种前沿计算机技术,并具有去中心化、不可篡改、可追溯和集体维护的特点。基于这些特点,区块链技术在征信管理、跨境支付结算、供应链金融、统一用户账户体系、数据共享平台、资产证券化、法定数字货币、金融市场服务、银行资产托管系统等多个领域突显效用。尽管区块链技术具有更新频率低、有效监督难等问题,但一旦突破诸多技术性和非技术性难题,区块链技术将孕育并革新各类底层技术平台,深度改变诸多领域的行业生态,进而推动整个人类经济社会生活的重大变革。

关键词:区块链;区块链技术;分布式重构;去中心化;不可篡改

中图分类号:TP 319;F 8

文献标识码:A

文章编号:1000-260X(2018)04-0053-09

近年来,“区块链”及其相关概念均受到大众广泛关注,并被定义为极有可能成为新一轮产业革命的基础。迄今为止,区块链技术已历经三个发展阶段,并且在不同领域取得了一定进展。

然而,虽然我们已经在区块链的实践上取得了一些成果,但我们现今对它的应用也还只是冰山一角。区块链还有很大的价值有待发掘。

一、区块链的本质、技术特点及分类

(一)区块链的本质

区块链技术的起源来自比特币。2008年11月,中本聪发表了《比特币:一种点对点的现金支付系统》一文,阐述了他对电子货币的新构想。2009年,中本聪在区块链的基础上,创建了比特币,它

不受任何央行和金融机构约束,同时,第一个区块诞生,该区块又名“创世区块”。2010年7月,比特币交易所 Mt.Gox 成立,比特币的价值被世界认可。2015年11月,NASDAQ 同 Chain 就私营企业股票发行及交易平台进行合作,该平台基于区块链技术完成了全球第一笔私募股权区块链交易。同年12月,美国纳斯达克首次在个股交易上使用区块链技术。与此同时,区块链联盟 R3CEV 成立,该联盟吸引了全球40家金融巨头。2016年可以说是“区块链元年”。

区块链就是通过标准算法,并且使用加密技术将数据压缩为一个64位字节的代码,称为“哈希”或者“散列”。这个数据可以代表一个记录、一笔资产、一项交易等等,将其同真实世界联系起来。由于哈希值难以解密,同时区块链的数据记录

收稿日期:2018-06-25

作者简介:邓柯,质数链网科技成都有限公司 CEO,主要从事区块链技术问题研究。

都会盖上一个时间戳,这样就确保了记录数据与真实世界交易的完全对应。

简而言之,区块链的本质就是一种基于密码学原理构建的分布式网络数据库,是一个使用区块记录交易信息的账本,这个账本具有严格的记账规则。每个用户节点都可以查看账本上的记录,但是其中的记录内容没有人可以修改。

(二)区块链的分类

区块链根据去中心化的程度分为公有链、私有链和联盟链。

公有链是完全去中心化的区块链,它的所有参与者都可以在链上读取和发送交易,而且都可以竞争记账权。公有链可以保护用户免受开发者特权的影响,其中的数据都是公开可读取的,但是由于参与者数量众多,交易速度会受到一定影响,其中的代表就是比特币、以太坊等。

私有链则需要预先设定满足条件的参与者和记账人区块链,区块是否生成需要所有记账人共同决定。其他的参与交易的节点不具有记账权。私有链去中心化程度低于公有链,存在成员联合欺诈的风险。由于它的运行和维护成本较低,交易速度较快,因此得到了广泛应用。

联盟链是由公司或者私人控制的,其记账权不公开且只记录内部数据,读取权限的限制与开放由拥有者决定。联盟链拥有极快的交易速度,强大的隐私保障,交易成本很低,且有利于内部审计,一般应用于企业中心化系统上链。

(三)区块链技术特点

区块链技术具有弱中心化、不可篡改、可追溯和集体维护的技术特点。

弱中心化的特点又称分布式特点,它使得区块链网络中的众多节点可以自由链接,发生包括资产和信息的交换。每个区块链中的节点都保存着完整的总账,交易发生后,链上的全部计算机都会同步更新相关数据。在这个过程中省略了第三方机构,例如在转账中的银行。而不可篡改的特点是利用了密码学原理、时间戳等技术,用随机散列算法(哈希算法)对区块内的数据进行加密。同时,

通过公钥、私钥不同的非对称加密法来保证节点用户的信息安全,如图 1。并且根据区块链信息全网广播的机制,若攻击者意欲更改交易数据,其付出的努力可能远大于成为一名诚实参与者。



图 1 区块链工作原理示意图

至于可追溯的特点,我们一样可以由图 1 得出。在每一个区块的区块头,都记录了前一个区块的 HASH 值,这就保留了从第一个区块开始的所有数据,区块链上的任意一条记录都可以通过其链式结构追溯本源。而区块链的集体维护特点则源自其独特的记账方式。区块链的记账参与方应当由多个利益不完全一致的实体组成,并且在不同的记账周期内,由不同的参与方主导发起记账(轮换方式取决于不同的共识机制),而其他的参与方将对主导方发起的记账信息进行共同验证。

二、区块链技术的演进

自 2009 年诞生以来,新兴的区块链技术已经经历了三个不同的发展阶段。

第一阶段:2009~2014 年“区块链 1.0”阶段,是区块链出现的初期。该阶段区块链主要应用在数字货币上,从比特币诞生、第一个公允汇率出现、交易平台成立,到世界各国开始认识到比特币的价值,比特币作为一种支付手段成为唯一的统治代币。同时,像莱特币、以太币等不同的虚拟货币也开始崭露头角。此时的区块链构建了一种去中心化的数字支付系统,与当时的依赖中心的支付体系相比,更加安全、高效、便宜。为解决对中心体系的不信任而产生并发展的区块链技术,此阶段呈现出对抗性,即对抗既有体系及思想。

第二阶段:2014~2017 年“区块链 2.0”阶段,区块链技术产生了一些支付之外的应用,并开始向金融领域扩张,因此呈现出金融性,比如点对点交易、智能合约、众筹、产权记录和保存等。与此同

时,人们开始对智能合约以及通用的区块链产生兴趣,例如以太坊。任何人都可以基于以太坊构建和使用运行于区块链技术之上的去中心化应用。

第三阶段:在 2017 年以后的“区块链 3.0”阶段,区块链技术成为了“万物互联”的一种最底层的协议。区块链技术开始从金融领域向外扩张,大规模产生区块链的主流应用,例如身份认证、医疗、仲裁、投票等,这也正是“区块链技术”对传统行业的革新性。



图 2 区块链技术发展阶段

三、区块链技术落地的条件及应用空间

区块链经过了数年的发展,毫无疑问,技术的改进使得现有的区块链拥有了更多的落地场景,区块链技术本身并不是一个全新的技术,而是由多个现有技术组合而来,它所带来的不可篡改性、分布式等特性使得其在一些实际应用领域有很好的落地场景,但由于发展时间比较短,一些方面(诸如信息隐匿性)仍未成熟,这些也限制了区块链技术在一些应用场景的落地。在现有的技术条件下,它的落地是有一定的场景选择的。

结合区块链的特性,区块链技术主要用于采用低成本方式解决信任问题,基于此,区块链技术的落地需要满足以下一些条件,才能发挥出区块链本身优势。

1.场景需要多方参与。有多方参与才会有信任问题,如果参与方仅仅只有一方,本质上就没有信任问题的产生。

2.多方需要协调完成同一项业务。一项业务(或者交易)本身,如果仅仅需要一方决策或者同意就

可以完成,这样的业务要求仅需一个中心化决策就可以达成。

3.复杂交易。通常来说,一个交易总是需要至少两方参与,一些更复杂的交易可能还需要更多的参与方或者更多的流程,这些流程在执行过程中,在不同的步骤需要不同的参与方(每个步骤可能并非全部参与方),需要利用区块链的特性确定需要的参与方一定参与了,同时不需要的参与方一定没有参与。

4.多方确认。账本本身由单一账本向分布式账本迁移,目的是将之前由一个账本做出的决策,向多个账本达成共识来转化,这从根本上说,是一种确权方式的转化。

5.可追溯性。这个特性涉及到账本的设计目标,现有中心化系统的账本一般采用单边账(即流水账)或复式记账,而区块链系统更多地采用 UTXO,当然也有采用余额+state 的方式(Ethereum),但无论如何,由于区块链需要多方确认账务的正确性,对它的账本要求,总是需要进行快速溯源的,这点,在现有账本技术中(复式记账)也可以完成,但效率不高,因此,实时的账务数据的追溯本身通过现有技术很难达成。

6.一些单纯目标的应用场景。如存证,只是利用区块链进行数据存储,保证其不被篡改,这样的应用其实也可以有其他的技术方案进行替代,本质上并非一定要使用区块链来解决。

从这几个方面的判断而言,我们选择了以下一些典型应用场景来探究区块链的落地境况。

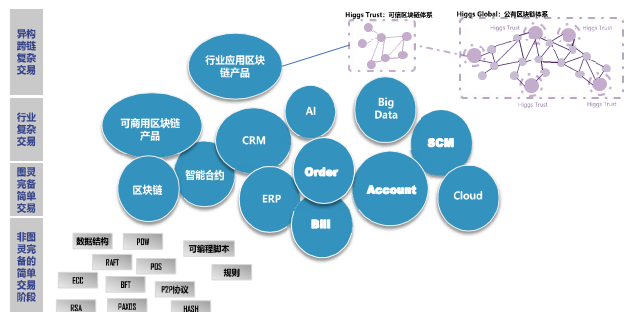


图 3 区块链技术在实体行业落地思考

(一) 征信管理

长期以来,征信数据交易无法从纸质协议向

电子化协议作出突破,其主要原因在于数据无法综合流通、加工以及使用,并且难以在二次交易时稽核和管控。由于区块链技术使其交易公开、安全、可信、难以篡改,征信数据交易有了数字化发展的可能。私有链或联盟链可以让数据供方对征信数据需方授权然后读取,数据可以在采集与加工的同时,对授权文件进行同步流通与校验,从而实现校验授权的真实性,并达到二次交易稽核及管控的目的。将区块链技术引进征信管理,使用方可以不用改变现存的业务流程,而且可以随时获取实时更新的数据。

使用区块链技术进行征信管理,可以在保障数据安全私密的基础上进行有限可控的数据共享以及信用验证。联盟链对各个征信相关行业共享交易数据,构建征信数据共享交易平台,使参与者大大减小了成本、控制了风险,并且加速了信用数据的存储、流通和交易。随着区块链技术的成熟以及对其应用的不断探索,未来在征信数据交易领域区块链将发挥更大的作用。

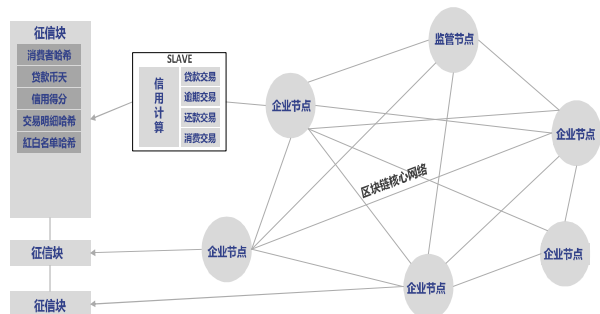


图 4 征信链解决思路

(二) 跨境支付结算

区块链技术的分布式账本特点,有效地解决了上文提到的跨境交易的高成本、低效率问题。成立于 2012 年的 Ripple 就是基于区块链技术提供跨境支付服务,它使用云联网时代的基础架构协议,让不同的支付体系进行交流,这就使银行无需通过代理银行可实现直接、即时的交易,降低总结算费用。Ripple 表示,自己的技术能让银行在支付中减少 33% 的成本,数秒内即可完成交易。国内目前已经有民生银行、招商银行和平安集团等先后加入 R3 等国际区块链组织,参与标准的统一制定

与合作。同时各大银行都在加强自身技术的研发与应用,在不同的领域进行积极尝试。目前,通过应用首创区块链直联跨境支付技术,招商银行实现了首单应用跨行支付,即国内的南海控股有限公司通过永隆银行向其香港同名账户实现跨境支付,这在国内区块链金融应用领域具有里程碑意义。另外,2017 年 11 月 3 日,招商银行西安高新科技支行通过招商银行总行自主研发的区块链直联跨境支付应用技术,成功完成一笔美元跨境支付业务。

(三) 供应链金融

传统的供应链金融以供应链上的核心企业为中心,集中管理与其相关的上、下游企业的商流、资金流、物流和信息流,以自偿性贸易融资的方式,对供应链上下游企业提供综合性金融产品和服务。这既有利于企业融资,又有利于银行管理风险。然而,在实际操作过程中,多级供应商在传统供应链金融模式下依然面临融资难的问题,其原因主要源于:

- 一是一级以上的供应商或者经销商,无法满足资金端的贷款要求,无法提供资金端需要的抵押物。
- 二是核心企业应收账款本身是可以充当抵押物的,但又存在对应收账款确权的问题,这里就是一个多方参与的问题。
- 三是传统的票据包含商业承兑票据和银行承兑票据,两种票据本质上都是需要经过银行才能发行的,并且本质上是无法拆分的,电子票据的发展就是为满足这样的需求而出现的。

从以上的描述来看,它满足我们前面描述的区块链落地的几个重要的参考指标,即多方参与、复杂交易、共同见证。

而将区块链技术引入供应链金融,则有利于解决现存的问题,推动供应链金融更加成熟。对于多方参与的供应链金融,区块链依托分布式账本、加密账本结构、智能合约等核心技术,为解决以上问题提供了很好的方案^[1]。

在整个应收账款供应链金融方案中,有几个重要的步骤可以借用区块链技术得以在流程中进

行优化:

1.应收账款的开立。应收账款的开立过程需要多个机构的参与,以便对应收账款进行共同见证。应收账款本身其实是一个合同条款,多方(通过多岗位)要在应收账款的各个属性中确立自身的权利和义务,而这些步骤在放入区块链中以后,就会以 UTXO 的形式被记录下来,并且无论是核心企业、资金端还是多级供应商、经销商都可以使用一致性账本来保障这些申明的权利和义务。

2.应收账款的转让。由于在整个流程中存在复杂的交易,应收账款的转让就意味着权利和义务的转移,这种情况下,各参与方需要首先确认应收账款的真实性和正确性,这里需要对应收账款进行溯源确权,这就意味着多方进行参与并将确权的流程在区块链中记录并达成共识。由于多方参与的不确定性,这里需要完成对转让的智能合约的编写,并且在区块链共识层通过智能合约完成多方的共识。

3.应收账款的拆分。由于多级供应商和经销商的存在,核心企业开立的应收转款本身需要在各级供应商和经销商之间进行拆分,各级供应商和经销商正是用这些拆分的应收账款向资金端申请融资。这里需要对应收账款本身进行溯源确权,同时,还需要通过 UTXO 的账本技术确保不能“一单多融”,在区块链技术中,这就是保证不能“双花”。

4.应收账款的融资。应收转款的供应链金融的最核心的目标,就是让各级供应商和经销商可以通过核心企业开立的应收账款本身向资金端申请融资,这些已经被拆分的应收账款首先需要进行确权,同时,在融资流程中还需要多方对融资的具体属性进行确认。比如,核心企业对于每个层级不同的供应商和经销商其对应的融资成本可能是不同的,这就需要在融资过程中让资金端和核心企业共同对融资成本达成一致,并且在达成一致以后,将这些数据写入区块链,同时,在区块链上还会对这些应收账款的余额进行多方的一致性判断,以此来保证各方对这笔融资的所有属性都达成了一致。同时,还需要将融资过程中的所有各方进行的确认和协商的行为也进行记录。任何一方都不会拥有分类账的所有权,也不可能为牟取私

利而操控数据^[2],加上交易进行过加密,并具有不可改变的性质,所以分类账不会受到损害。此外,基于区块链技术的供应链金融业务将能大幅减少人工的介入,目前将通过纸质作业的程序数字化^[3]。所有参与方都能使用一个去中心化的账本分享文件,并在达到预定的时间和结果时自动进行支付,这可以极大地提高效率及减少人工交易可能造成的失误。

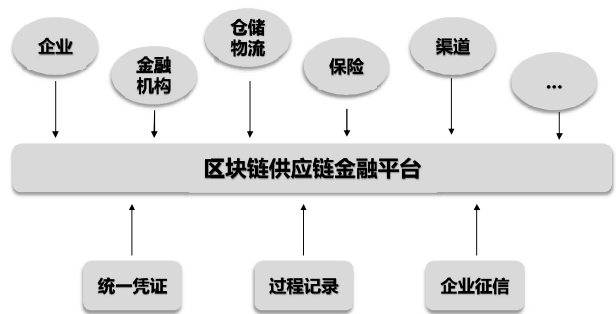


图 5 区块链技术供应链金融应用场景



图 6 区块链与供应链金融架构思考

(四)统一用户账户体系

大型金融集团中,不同的机构通常都是根据自身业务来进行发展的,业务发展前期,这个模式可以迅速有效地完成业务生存与发展。然而,当企业发展到了一定阶段,由于各项业务均拥有自身的用户和账户体系,将反制于企业发挥金融流动性。例如,同属于一个集团的 A 和 B 可能都拥有自身的用户账户系统,同一个客户在 A 和 B 中都需要进行业务流通,并且时常需要在 A、B 业务中进行资金的调拨和划转,由于分处于不同的账户体系,这样的调拨和划转的代价很高,并且在时间上很难保证及时性,最终的结果会导致资金的流动性减少,客户体验不佳。此时,可以通过区块链系统解决流通成本高企及运营管理不作为的困境,

即在业务层面使用智能合约,建立用户体系并完成多方对接。

第一步:在用户系统层面,通过业务投票方式完成用户信息的确认,各个业务系统均可使用统一的用户识别和登陆;

第二步:跨平台的用户确认以后,会将这些数据放入到区块链中,并且在下次登陆验证用户时在区块链数据中做检查,这些数据就被放入到区块链的一致性账本中完成存储;

第三步:完成各个业务节点统一用户系统后,根据同样原理对接流通资金系统。数据上传到区块链以后,所有的资金变动都会在区块链系统上体现,用户的余额生成等都能通过区块链系统完成共识。

(五)数据共享平台

随着大数据关键技术不断突破,应用领域不断拓展和产业体系的初步建立,标志着我国大数据产业进入高速发展期^[4]。然而,基础数据资源开放进程缓慢,个人信息泄露问题频发,交易的市场机制和法律体系尚不完善等众多问题,阻碍了数据的流通。虽然近年来多个大数据交易所成立,但整体来说,大数据企业众多而弱小,数据孤岛多,很难实现行业优势。

由于所有的数据是通过不同的渠道收集来的,很多数据使用的场景并非是一项业务,例如,通过一些 IOT 设备可以收集到一些汽车行驶的信息,这些信息的收集本身可能并不能为生成 IOT 设备的企业所使用,而是通过某种方式,数据可能被车后管理,如 4S 店、保险等业务所使用,数据收集以后进行归类划分,并定制相应的权限,这些数据写入到区块链中以后,未来通过智能合约对权限方面进行限制,则可以方便进行数据的分类共享。

区块链技术拥有不可篡改、集体维护等特点,可以通过数据所有者的私钥签名,保护所有权不可侵犯;可以通过智能合约保障数据必须授权并付费后才可访问;通过底层区块链保障数据不可篡改。由此丰富大数据维度,形成行业平台;并且可以通过授权收取相应的费用,打造新的商业模式。

(六)资产证券化

资产证券化是一个非常适合区块链落地的场景,总的来看,它的全过程非常长,并且参与方非常多,不仅在各个阶段需要不同的参与方确权,还需要在后续过程中进行信息披露,全流程会明显地分为几个过程,以下我们作一些简要的分析。

1.资产池形成阶段:在形成资产池的过程中,首先需要多方对入池候选资产进行评估,原始权益人需要将资产的详细内容如主承销方、第三方监督方、发行方、律师事务所、托管机构(通常为信托)等等进行公示,接着各方需要对资产的来源、未来可能产生的现金流等等详细资料进行评估并确认,形成统一资产池,这些过程需要多方对资产评估进行确认,这会形成一个多方的确认为数据,这些数据写入到区块链中,并以智能合约的形式要求各方的参与,并在共识系统中保证各方的确认都真实有效,才能为下一步的发行做好准备。

2.SPV 的设立:原始权益人需要对入池资产进行剥离,放入到 SPV 中,SPV 的设立需要多方确认,主要包含原始权益人和托管机构,双方要真实地确认这些资产真的与原始权益人进行了剥离,这些步骤也需要通过智能合约和共识系统进行确认。

3.发行阶段:当主承销方要对资产进行分层和发行时,仍然需要经历一些合规性的检查,此时,对发行资产的检查需要对资产池进行穿透,通过 UTXO 的使用可以完成溯源的穿透式检查,这对于未来的信息披露有很重要的意义。

4.存续阶段:在债权存续阶段,第三方监督、律师事务所需要定期进行信息披露,由于资产本身随着时间的推移可能发生变化,甚至发生非常大的变化,特别是发生资产价值的很大变化导致可能出现资不抵债的情况,此时,信息披露非常重要,通过区块链的统一账本机制,可以穿透性地进行信息披露,甚至有望做到实时披露,降低投资人风险。

5.现金流的结算:在资产证券化存续期间,资产产生的现金流收益将会通过信托、SPV 向投资人进行分配,并且最终通过托管机构进行分配,这

个过程主要参与方是 SPV、结算银行和托管机构、投资者等,现金流分配是一个比较复杂的过程,无论哪个机构在分配时都需要多次的确认和实现自身的职责,这些职责在借助前面已经进入到区块链中的交易数据和交易行为数据,并通过智能合约进行检查和确认,确保债权收益能够进入到真正的投资人手中。

(七)法定数字货币

数字货币是基于互联网发行的、以数字信息实现流通和支付的货币,例如比特币。法定数字货币则是由国家的货币当局发行的数字货币。与一般的数字货币相比,法定数字货币是有国家信用担保的,因此,法定数字货币微观上更加安全,宏观上又可以作为一国法定货币的重要补充。第一,它可以有效地替代现金流通,减少纸币印刷、发行、清分和销毁的高额成本;第二,法定数字货币可以个人对个人即时支付结算,减少了银行、央行的清算以及系统对账,提高了资金的流转效率;第三,由于法定数字货币基于区块链的可追溯的特点,它对反洗钱、反恐怖活动也有很强的监控作用,并且有利于完善对农村偏远地区和弱势群体的金融服务;第四,在央行和政府对国家宏观经济的调控上,使用法定数字货币便于把握货币市场的运转,支持制定有效的货币政策和财政政策。

然而与法定数字货币相关的规章制度仍不完善,所以现阶段各国都处在尝试和探寻阶段。日本各大银行与日本的金融监管机构计划合作推出 J-Coin 为法定数字化货币,该货币与日元的兑换比为 1:1,计划于 2020 年东京奥运会前后开始流通。美国、英国、俄罗斯、澳大利亚、丹麦以及乌拉圭等国也在积极筹备法定数字货币的研究与实践。我国也在积极研究法定数字货币,自 2014 年就由央行成立了专项研究小组。2017 年,央行成功测试了基于区块链的数字票据交易平台,并且试运行了采用分布式记账等区块链技术的数字货币,用户之间通过使用安全芯片的数字货币移动终端进行交易。数字货币系统通过基于云计算的可信服务管理模块收集信息并进行服务,其上游包括登记中心、认证中心、数字货币发行库以及数字货币银

行库,由此进行法定数字货币的发行和管理。现在央行数字货币系统仍处于探索和试验阶段,推向大范围的实践仍需一定的时间。

(八)金融市场服务

基于区块链技术的应用在金融市场中也有很大的发展前景,其不可篡改的特点保障了金融交易数据的安全,具有核心优势。2015 年 10 月,美国 NASDAQ 交易所推出了 Ling——基于区块链技术打造的私营公司股票发行及交易市场,私营企业可以凭借这一平台完成股票的发行、销售、交易、登记等功能。而正是有赖于区块链的不可篡改技术特点,私营公司股票的发行业务得以永久保存,股权交易得以高效进行,大大方便了私营公司在市场上进行融资。

国内的初创公司质数链网也推出了小微贷款的监管链。质数链网通过区块链进行小微贷款交易,由某些特定节点进行监管,使用智能合约检查交易是否符合规定,并且留存交易记录。这不仅保障了交易的真实记录和储存安全,与此同时,也促进了小微贷款的发展。

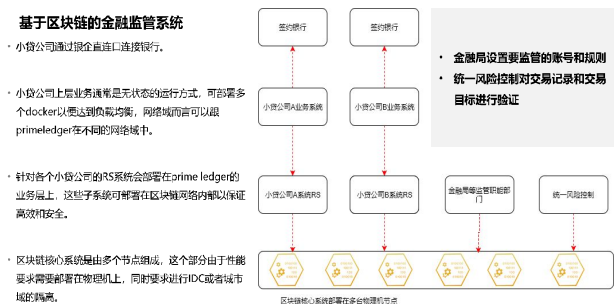


图7 区块链与监管架构思考

(九)银行资产托管系统

区块链技术的分布式账本和智能合约等机制,不可篡改和全网维护的特性,使其在银行的资产托管领域有很大的应用价值。基于区块链技术的银行资产托管系统,完成了个人数据和交易数据在确保安全的情况下的共享,保证了所有交易都规范地完成,所有的交易数据都整合在区块链中,不可篡改而又可以追溯。而审计部门和监管部门又可以方便快速地获取信息,即时管控,降低风

险。在此过程中又节省了很多例如信用校验的时间和精力,减少了成本,提高了运行效率。

除去金融领域的应用,区块链在非金融领域的具体应用也有很多。例如投票公司 Follow My Vote 的投票应用,物联网公司 Adept 的物联区块,还有基于 Higgs Chain 的交易监管链——自贸区监管沙盒。区块链技术在各个领域都获得了一定的应用,将来的应用领域和应用方式也会越来越多。

四、区块链技术存在的问题和未来展望

(一)区块链技术存在的问题

区块链技术虽然具有众多的优点,然而这一技术并非完美无暇。在支付交易方面,现有的交易制度需要控制交易过程中的每一个环节,包括交易合规性、交易对象身份验证、反洗钱检查等等,而区块链技术却是完全开放,少有准入门槛,虽然记录不可篡改,但并不能保证每个记录都真实正确。区块链的主要贡献是在保证快速、便捷的基础上,较好地解决支付双方的信任问题,但目前只是解决了支付双方的信任问题,而整个支付流程,不只是完成付款一个动作那么简单,而是涉及到记账、追缴等一系列系统和机制,区块链技术的大规模应用有待监管的统一、市场的认可。我们认为,目前区块链技术进行大规模应用还存在以下主要问题:

1. 技术本身能否支撑业务的发展。

当前阶段区块链技术由于其区块大小及更新速度的限制,仅仅适用于低频率的信息登记场景,在高实时性交易场景下区块链技术需要更新和改进。此外,作为新兴技术,区块链技术能否在可靠性、稳定性方面达到金融系统和监管系统的要求还不可知。虽然区块链技术在金融领域有着巨大的应用潜力和空间,但大规模使用后,其使用及维护的成本也必将是商业上应重点考虑问题之一。

2. 去中心化所带来的信任和监管问题。

完全的去中心化容易带来两个问题,一是并不能保证交易双方的信用,一旦交易的某一方出

现信用问题,这笔交易是无法撤销的;二是在面对欺诈、转移非法所得等非法行为时,追缴资金会存在一定的难度。这就导致了严重的信用和监管问题。因此有必要在此基础上建立严格的追责机制和监管体系^[9],确保交易的安全性与合法性。

3. 难以形成有效的线上流量和场景。

目前银行使用区块链技术更多的是现有技术的优化,而非变革,这些优化会体现在“提高效率、减少成本方面”。目前比特币作为区块链最成功的应用领域,我们看到了比特币的便利和快捷。但是对于商业银行等金融机构而言,对于客户的了解才是核心,如若无法形成有效的存量数据的跟踪和解析,区块链技术对于商业银行而言,进一步的应用价值可能受限。

(二)区块链技术前景展望

区块链技术弱中心化、不可篡改、可追溯和集体维护的特点使它具有无比广阔的应用前景,尤其在金融、公共服务、物联网、供应链和公益慈善等领域已经有了一定程度的应用。

在金融领域,随着区块链技术的完善,更多领域“区块链+”的应用都将得到完善和发展,金融创新的步伐不断地加快。就像早期的算盘和16世纪的复式记账法一样,21世纪的区块链作为技术手段,在保留金融本质的情况下,将金融的层次大大提高。现如今数字资产证券化刚刚起步,金融科技的发展还在早期阶段,还有很大的发展空间。将区块链技术与金融深度结合,金融业的效率也将快速提高,成本也会大幅降低,而且还能进一步增加透明度以及普惠性。金融的发展也会反哺区块链技术的研究和“区块链+”企业的兴起。区块链技术等金融科技对金融的深度赋能将发挥后者对百业和实体经济发展更强有力的支撑,使区块链技术在其他领域也得到广阔的应用。

结合以上的分析,区块链技术在基础应用方面的革新将孕育各类底层技术平台以及提供区块链技术服务和解决方案的企业,进而将区块链技术延展深入到各个业务领域,进一步建立健全以区块链为基础和解决思路的行业生态。区块链技术无疑将加速推进新一轮产业革命,进而推动整个人

类经济生活的重大变革。

参考文献:

- [1] 张明裕.区块链驱动供应链金融创新[N].新理财,2017-11-01.
[2] 何阳.金融科技加速变革,四大技术趋势凸显[J].人民邮电,2018.

[3] 张锐.全球金融业布局区块链[N].中国财经报,2016-07-19.

[4] 王宇霞.我国大数据产业发展的五大痛点[N].通信产业报,2017-02-27.

[5] Allen&Overy.Fintech, Research Report[R].2016.

【责任编辑:来小乔】

Essence, Application Conditions and Prospects of Block Chain Technology

DENG Ke

(Prime Chain Network Technology Chengdu Co., Ltd., Chengdu, Sichuan, 610041)

Abstract: Block chain, as a network database, a book that uses block records to record transaction information, is essentially a distributed public ledger, namely, a series of chained data structures constructed on the basis of cryptography and ensured not tamperable or forgeable. Block chain is not a single technology or framework, but a distributed reconfiguration of technologies and platforms in the Internet age. Block chain technology is a technique for encrypting and time-stamping data, forming data chains according to time stamp order, and storing data in a distributed manner. This technology covers a variety of cutting-edge computer technologies including point-to-point transmission, consensus mechanism, encryption algorithm, distributed storage, and has the characteristics of decentralization, non-tampering, traceability and collective maintenance. With these characteristics, block chain technology is especially effective in credit management, cross-border payment and settlement, supply chain finance, unified user account system, data sharing platform, asset securitization, legal digital currency, financial market services, bank asset trustship systems, etc. Although block chain technology has problems such as low update frequencies and difficult supervision, once it breaks through in many technical and non-technical areas, block chain technology will nurture and innovate various underlying technology platforms, and profoundly change the ecosystem in many industries, and then trigger major changes in the entire economic and social life.

Key words: block chain; block chain technology; distributed reconfiguration; decentralization;