基于区块链的保险业务模型及实现路径

胡鸿雁 朱建明
中央财经大学信息学院 北京 10001

摘要：区块链技术在比特币发行的成功应用而备受关注，其在金融、政法、征信等领域的应用研究也在不断探索中。本文从目前保险行业的现状和存在的问题出发，简要梳理了区块链技术的原理脉络,分析了保险行业应用区块链的路径,构建了保险行业区块链技术架构模型，并探讨了区块链技术的局限性以及改善措施。

关健字：保险 区块链 数字身份 智能合约 分布式记帐 互助保险

保险目的是有效对冲和管控风险，而制度和技术是风险管控的关键。区块链为“技术”监管提供了最大可能。基于区块链技术的无法篡改、可追溯特性，强化信息对称与交易安全，建立多方验证的交互式共识信任机制，搭建实时的“点对点”管理和监控系统，确保系统中的任何终端均无法作弊，实现保险资金流向合规、安全交易和跟踪监控，从而降低监管成本，提高监管效率，减少违规行为。区块链技术为保险业将身份管理、数据和流程的所有权和管理权授权给客户，构建一个具有刚性约束和透明可靠的信任体系，并通过利用新技术和新战略，推动保险行业改善业态结构，提高服务质量，创新商业模式，促进战略转型。

1. 目前保险行业的现状和面临的挑战

1.1 传统保险行业的现状

保险是一种契约经济关系，是投保人与保险人之间的合同关系，是广泛应用的风险管理工具，也是金融市场体系和社会保障体系的重要组成部分。保险业务是客户与保险公司之间在法律框架下，基于信任双方自愿达成的协议与支付承诺。一方面客户提供可保险利益的准确个人信息，另一方面又要求保险公司提供优质的保险产品及服务，并保证业务流程的完整性、透明度。

当前中国保险业正处于一个日益复杂、多变的市场环境。首先，从保险行业整体发展形势而言，中国是保险大国，却不是保险强国。衡量一国保险业发达程度的指标不只看保费收入，还要看保险深度（保费收入/GDP）与保险密度（保费收入/总人口）。而中国目前保费收入虽居世界第三位，但保险深度和保险密度尚未达到世界平均水平，保险的普及程度、险种的丰富程度、费率的优化程度、投保的受惠程度、市场的开放程度也有较大改善空间。其次，从保险行业商业模式和技术系统而言，存在着增值服务不够、保险消费误导、理赔效率低下、行业信息不对称，骗保骗赔信任缺失等问题。目前大多数保险公司现核心业务模式和业务信息系统仍停留在早期的采购开发系统，如何从技术层面推动保险核心业务系统转型，成为保险企业保持竞争力并取得先发优势的决定性因素。

1.2 互助保险的兴起及面临的挑战

互联网、大数据、区块链等技术与保险业务的深度融合为保险行业创造了更多的拓展空间，促进了互助保险的兴起和不断发展。互助保险改变了传统保险的商业和技术模式，可以有效的降低保费，并极大的惠及民众。

但互联网保险的线上交易带来了经济性和便捷性的同时，用户的个人信息、资金账户等

相关私密信息却面临着信息安全风险，而传统的技术工具和管理手段需要投入大量成本，且效果不佳，这成为制约互联网保险发展的严重技术问题。同时，由于目前主流互助保险平台在机制设计上存在缺陷，部分环节存在违规操作隐患，可能导致诸如平台篡改投保人数来让投保人多均摊保费；篡改投保时间、投保人身份违规输出利益；挪用保险资金池，给投保人的保险资金带来风险；投保人与鉴定机构、医院协同虚构病情、医疗档案形成不合理赔付等现象。

因此，保险行业需要积极寻求新技术和新模式完善管理机制，提升服务水平。区块链技术具有去中心化、信息不可篡改、透明公开、信息安全等特点，运用在保险行业，有助于加强对客户信息的保护、降低信息不对称风险、降低互联网保险成本，并可实现信息流、价值流的共享传输，为保险行业的技术发展创造了新的机遇。

2. 区块链技术在保险行业的应用机理

2.1 区块链技术的功能原理

区块链起源于中本聪的比特币，作为比特币的底层技术，本质上是一个通过去中介化的方式集体维护一个可靠分布式数据库的技术方案。区块链主要是让参与系统中的任意多个节点，形成一串使用密码学方法相关联产生的数据块（Block），每个数据块中包含了一定时间内的系统全部信息交流数据，并且生成数据指纹用于验证其他信息的有效性和链接下一个数据库块。区块链是一种类似于 NoSQL(非关系型数据库)技术解决方案的统称。能够通过很多的编程语言和架构来实现。目前常见的包括：PoW(Proof of Work 工作量证明法) 、PoS(Proof of Stake 权益证明法)和 DPoS(Delegate Proof of Stake 股份授权证明机制)等。区块链的应用领域从银行、保险、证券到产权登记、公证证明等等。

应用区块链技术可以解决保险业务的信任和安全问题，其特点如下：

一是采用去中心化的分布式账本，保证数据安全性。区块链技术的交易记账分布在不同地方的多个节点共同完成，每一个节点都记录完整账目，且参与监督交易合法性，避免单一记账人被控制带来的安全性问题。且由于记账节点足够多，理论上讲除非所有的节点被破坏，否则账目就不会丢失，从而保证了账目数据的安全性。

二是实施加密和授权技术，确保数据隐私性。区块链衍生于比特币，是哈希密码、时间戳和 P2P 传输创造性组合的产物，其原理是使用全新的加密认证技术和去中心化的记录生成机制。区块链采用双向加密技术，用户存储在区块链上的交易信息是公开的，数据拥有者可对“私钥”进行授权，允许其他用户采用“公钥”访问。

三是优化共识机制，防止恶意篡改。区块链根据不同场景，为各节点认定记录有效性提出了四种共识机制。以比特币为例，采用的是工作量证明，只有全网超过 51%的节点均认可，才能产生或修改记录，保证了数据的不可篡改性。由于每一笔交易的发生，都需要区块链的认证，然后记入每一个比特币地址的帐本里，并有巨大的算力作为支撑，以保障帐本公开、透明，不被够篡。同时，价值传递过程可追溯，进而可追溯价值传递过程背后对应的实体关系。

四是构建智能合约，实现标准化输出。区块链技术可以自动执行一些预先定义好的规则和条款，实现智能合约的构建和标准化输出，如保险业标准化保险产品中的自动理赔等。能够在很大程度上简化投保和理赔服务的流程，通过机器的程序化运行，可以极大降低人为操作风险，从而将违规的可能性降到最低。

2.2 区块链技术对保险业务的影响

区块链技术对保险行业在身份识别、相互性、空间和时间上都产生了极大影响。

(1)技术融合，提升数据安全存储。在区块链上可以存储相关标的信息、承保信息及理赔信息等，记载的数据经过加密处理，能有效避免数据泄露、丢失等潜在风险，从而最大限度保证数据信息的安全存储和使用。区块链的不可篡改和可追溯特性，能够基于共识机制构建一个纯粹的信任链。区块链还可以在互联网基础上，使用接入互联网的端口接入区块链，将投保人身份信息、健康医疗记录、资产信息、权属信息、交易记录等迁移到区块链上，形成“数字身份证”。实现数据管理的真实和准确性，不再依靠第三方个人或机构来获得确认。区块链的不可篡改和可追溯特性，还可以在反保险欺诈、反洗钱等领域将具有广泛应用。如，可构建被保险人医疗信息区块链:利用区块链技术，保险公司可以与医院共同构建病人医疗信息档案，形成病人医疗信息区块链数据库。保险公司在核保时通过查询医疗信息区块链数据库中投保人的档案就可以确定投保人真实的健康情况，有效避免带病投保、虚假赔案等欺诈行为。

(2)优化流程，提升产品服务质量。全网的多方验证形成了数据信息的“自证明”模式。保险公司通过投保人区块链“数字身份证”构建客户信息区块链数据库，将审查验证的用户信息写入区块链，在整个保险业务流程中无须重复输入和查询投保人信息，既可以缩短投保时间也可以实现自动理赔。如可通过区块链技术储存一个手机碎屏险合约，再通过智能合约技术与互联网相连，获取用户上传的碎屏图片数据，再通过图像识别技术自动审核赔付。一旦上述智能合约被触发，便会自动支付赔款，优化了保险业务的流程，保障了消费者权益，增加了客户满意度。

（3）去中介化，降低机构运营成本。利用区块链开源、透明的特点，可构建以各保险机构为节点的联盟区块链，实现保险业信息的有效共享。也可以更大范围的建立业务相关方联盟区块链，如医院、银行、征信机构等。如在共保或再保情形下，保险事件发生后，合同相关的所有保险人、再保险人、承保代理人均希望跟进理赔流程并开展谈判。若通过搭建区块链，将理赔文件编写入块，所有成员机构均能监测到理赔进展并参与更新，不仅保证文件准确度，更能极大缩短理赔时间。可以建立封闭的自动化数据通道，按照“被保险人—保险人—再保险—转分保—资本市场”途径，将保单标准化设计，并赋予中间环节自动化流程，使消费者与资本市场通过区块链搭建的保险市场有机联系。实现了行业数据共享、保单自动化生成、公司间自动结算等功能。通过上述措施，可以有效提高投保和理赔效率，降低信息和交易成本。

（4）风险管控，预防系统性风险。在传统保险业务运营中，由于各种原因导致的风险时有发生，监管机构只能采取事前审核或者事后约束的措施。而区块链技术是进行风险监管的有效技术手段。监管机构开发一个记账节点，就可以实时的观察到保险公司的全部业务动向。如资金流向和投资构成、产品的承保和赔付数据、主要的人事和管理操作等，无需等到保险公司事后申报，从而及时发现可能存在的业务风险和违规操作。

3. 基于区块链的保险业务模型

从区块链技术和保险业务的特征出发，以技术与业务的融合作为切入点，应用密码学，哈希算法、点对点传输、时间戳验证、分布式记帐、智能合约等区块链的核心技术来构建更智能化、安全可靠，更低成本，更便于交易的保险业务新体系。

3.1 基于区块链的保险业务模型

保险区块链应用要关注顶层设计，初期应用需要树立相对独立的局部思维，寻找最为可能技术实现的突破口。目前初期阶段基于区块链技术可以有以下几方面的应用路径。

（1） 基于哈希函数、时间戳，构建区块链数字身份识别和管理系统

区块链本身是一串链接的数据区块。区块数据结构是由“区块的头信息 + 区块账本信息”构成。区块的头信息包含了链锁位、时间戳、工作量位、权属信息位。其链接指针是采用密码学哈希算法对区块头进行处理所产生的区块头哈希值。每一个数据块中记录了一组采用哈希算法组成的树状交易状态，这样保证了每个区块内的交易数据不可篡改，各链接的区块不可篡改。因而形成一个公开透明且对等网络的分布式帐本数据库。一个完整的区块链身份识别系统包含了很多的技术，其中有基于哈希算法的数据区块及其上的数字签名、时间戳、Merkle 树、P2P 网络和共识算法等，为区块链交易、验证、链接等功能提供了有效的技术支持。区块链通常并不直接保存原始数据或交易记录，而是保存其哈希函数值。为快速归纳和校验区块数据的存在性和完整性，Merkle 树成为区块链的重要数据结构。公私钥密码系统被用来实现区块链中的数据签名。而且数据分布式记录和存储，可以使系统参与者集体维护且所有节点可以保存数据；可以生成一套按照时间先后顺序记录的、不可篡改的、可信任的数据库，并通过去中心化、去信任和加密算法去维护这套分布式数据库运转，相当于每个参与的节点都是“自中心”，即使部分节点受到攻击或者损坏，也不会影响整个数据库的完整性和信息更新。

基于区块链技术可以建立保险区块链数字身份识别与管理系统：投保人 A 通过系统入口输入真实的个人资料，公安、教育、银行、医疗及保险等机构验证投保人信息的真实性，并加盖时间戳，形成“数字身份识别区块 A”。投保人 A 进入保险业务管理区块进行财险 II 的投保业务办理程序，经过受理、验证和审核后，形成投保人 A 新的”财险业务区块 A+”，随后记入到投保人区块链数字身份识别和管理系统中。同理，投保人 B 通过系统入口输入真实的个人资料，进入系统进行寿险 I 的投保业务办理流程，之后形成投保人 B 新的“寿险业务区块 B+”，并记入区块链数字身份识别和管理系统中。以此类推，形成一个集个人身份信息和保险业务信息为一体的区块链数字身份识别与管理系统。

身份证明本质是基于第三方信任体系对身份的识别与确认。传统的身份识别系统不仅相对效率低，也容易受到篡改和攻击，且需要庞大的维护成本。基于区块链技术的数字身份识别系统能够安全自主地管理和使用自己的身份信息。区块链数字身份识别系统中数据的存储、传输、验证等均可以基于区块链的分布式结构。而这个系统可以改变人们以往管理自己个人信息的方式，既可以拥有自己的个人数据存储和管理平台，又可以形成一个第三方访问个人信息的权限框架。这样将大大降低身份欺诈和索赔欺诈的概率，减少保险机构的经营损失，并增加人们对保险产品的信任度。如利用区块链，可以实现车辆信息、资产权属信处等投保标的信息的核查记录，建立投保人身份信息、医疗健康信息、财产信息、信用信息的上链记录，整合保险机构的保单投保信息、出险事赔记录、保险欺诈信息、保单保全信息等关联记录，保证上上链信息的真实、完整、中立、安全、可溯和高效地实现保险客户的身份在线校验、信用验证与风险识别，充分发挥行业信息共享平台的服务和管理效能，服务保险业发展，支持保险监管，保护保险消费，辅助社会治理。

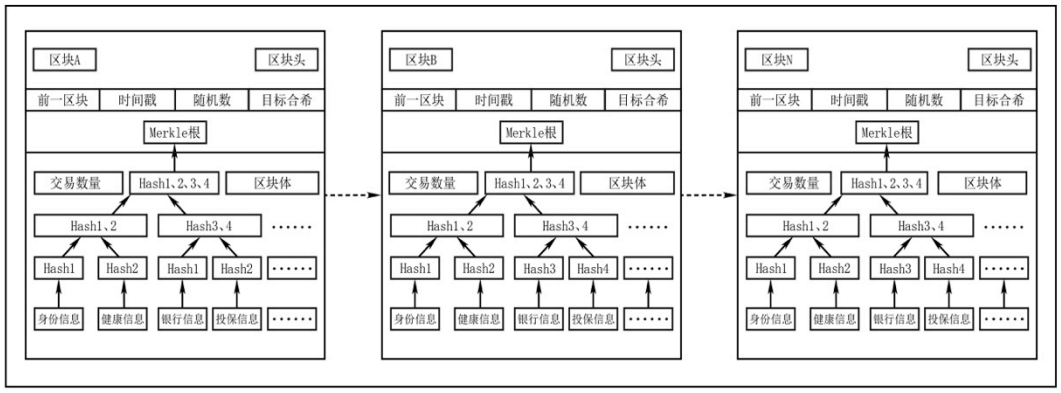

图 1：数字身份识别区块链模型

（2）基于智能合约构建保险的核心业务处理系统

智能合约是一种计算机协议，协议一旦制定和部署就能实现自我执行（self-executing）和自我验证（self-verifying），而且不再需要人为的干预。其原理是将合约条款嵌入到计算机中，由代码进行定义合约条款，而且由代码强制执行，完全自动且无法干预，订立合同的双方无法在合同完成前单方面违约，一切都是按合同的约定自动执行。由于智能合约部署基于事先设定的合同条款等，可以不依赖于第三方媒介，进行高效的实时更新和准确无误的执行，最大限度地减少恶意欺诈行为，节约交易成本。

智能合约基于区块链数字身份识别和管理系统的基础上，部署能够确保保险标的、保险条约、保险业务自动执行程序，就可能实现自动化的验证、办理、审核和后来的理赔等业务流程。当在保险业务管理系统中通过智能合约预设自动触发的业务条款和索赔条款及执行条件后，在投保人正常办理保险业务中，系统会让参与各方立即接触到执行指令信息，并对过程进行监控和审查，自动完成受理、验证、审核各环节流程，自动完成保险业务办理，最终达成保险合同和保险费用支付。智能合约系统自动执行过程中避免了人为的出错也减少了人力成本；而且节约了时间成本，在地域受理上也更方便易行；法律确定性更强，并且改善客户服务。在智能合约运营模式下，还可以执行保险的自动理赔业务。当保险标的出现时，只要满足理赔条件，保单条款将自动触发进行理赔，并自动完成理赔款面的支付，参照图（2）。整个过程无须投保人主动申请理赔，也不需要保险公司对理陪进行比准，实现效率提升，并使某些保险产品随着时间的推移实现自我管理。智能合约可以降低执行成本和监督成本，实现去中心化的、完全无人工干预的、复杂的价值交换。

智能合约本质上是一段程序，存在出错的可能性，甚至会引发严重问题或连锁反应，因此需要做好充分的容错机制，通过系统化手段，结合运行环境隔离，确保合约在有限时间内按预期执行。完全去中心化的智能合约是否已经成熟以及面临攻击该如何应对都将成为未来主要探讨的问题，区块链技术和智能合约都将成为未来互联网发展的重要方向，现在面临的挫折是新技术成熟的必然过程。

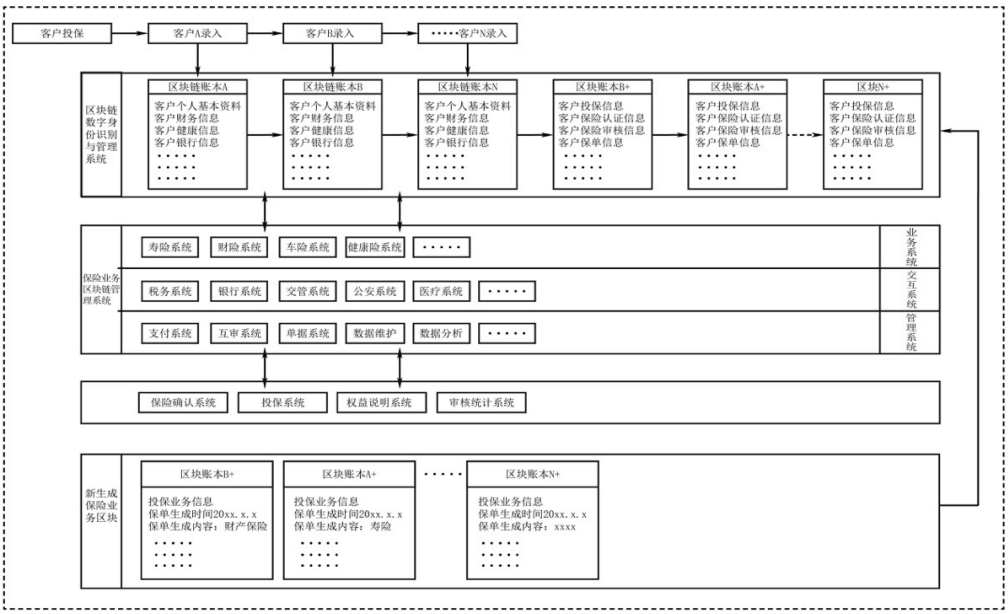

图 2：保险业务核心管理系统模型

(3)基于分布式帐本建立保险核心业务的技术构架

区块链分布式账本是区块链技术的核心，区块链系统构建中的业务价值互联、工作确认算法、全网共识机制、多中心化都是通过分布式账本实现的。保险业务的分布式账本构建可以设计为数据层、互联层、技术层、业务层和应用层（如图 3）。

分布式账本是允许用户在多个节点接入，网络中进行点对点交易运行的数据库。网络参与者均可以获得一个唯一的由共识协议生成的真实账本的副本。账本中的任何修改都需要全体用户进行多数确认后被生成新的记录，而新记录变化也会体现在任何一个对应的副本中。分布式帐本用密码学为账本加上了保障，使用公私钥和签名来控制对账本资产信息的访问，确保了账本记录的安全性和准确性。通过智能合约的修改和共识机制，可指定人或团体对资产进行权限修改。实体资产、虚拟资产和其他在金融和法律上加以定义的资产都可以使用分布式账本进行存储。即在区块链分布式记账技术模式下，可以建立一套完备的保险业务核心体系，实现各子系统的数据互联和信息分布，让数据在所有的参与节点实时更新，让信息流、资金流在系统中点对点进行交互，真正实现了信息链到价值链的应用。此外，区块链技术本质上仍是一种 P2P 技术，有助于信息的传递和分享，极大提升资产交易的结算速度。

在系统论中，中心化程度越高的系统，其容错率就越低，可能出现问题的概率就越高。传统保险机构系统大多是使用中心服务器实现所有的信息交换和数据存储，负载过大，容易产生服务器响应延迟、数据丢失或损坏，造成经济损失，同时被黑客攻击的风险相对较大。分布式账本具有去中心化的底层设计，其在技术层面上极难被攻破。黑客想对资产条目进行修改攻击时，由于存储在整个区块链网络中每个节点都拥有一个副本，需要其同时对整个区块链网络帐本进行修改攻击，这个难度极其大。而由于共识机制，出错的节点将会被整个网络舍弃。另外，去中心化的数据传递，降低了传统模式下系统的维护和优化成本，包括设备投入、数据备份、应急管理，同时也减少系统中心化带来的风险。

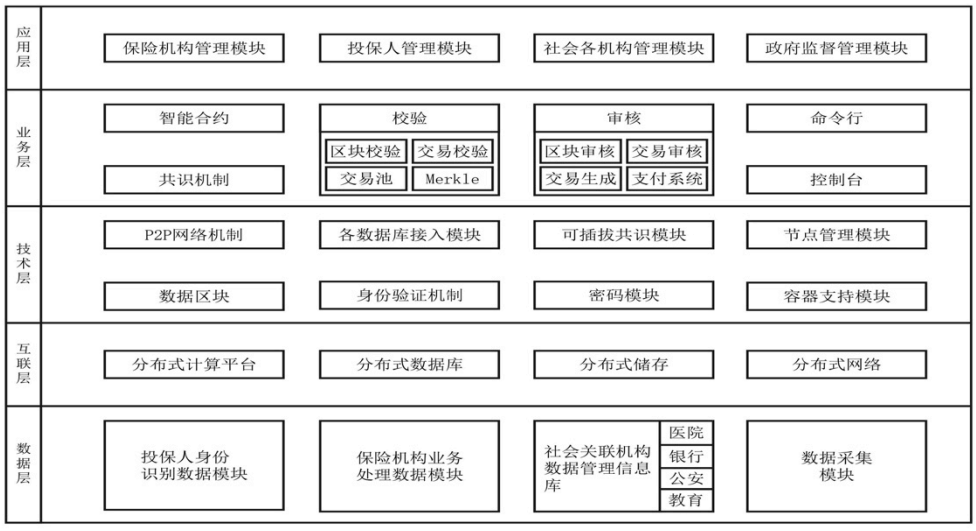

图 3：保险核心业务技术架构模型

4.基于区块链的保险业务实现路径

将区块链与保险业务结合，需要完成区块链与现有保险业务系统的融合。在技术层，通过密码学、数字签名、哈希、时间戳等技术手段实现用户身份验证、数据保存等问题；在业务层，通过智能合约实现更丰富灵活的跨系统业务逻辑，使多方合作业务更容易实现；而区块链的 P2P 通信、分布式数据存储架构技术能够实现系统多中心化计算和存储，从而在互联层和数据层上保障了系统数据安全和可靠。

一个基于区块链的保险项目就是要通过区块链的技术特点，在数据层、互联层、业务层、技术层上提供有力的支持，保障保险相关的业务层各个系统正常运行。与中心化信息系统不同，区块链是一个多方参与的分布式系统，相对于传统的集中式信息系统，在同一条区块链上一般会有多个业务系统进行连接，并进行业务交互。在基于区块链技术的保险业务中，一般可以通过如下几个步骤来实现。

（1） 确定各个参与方。

一个基于区块链的保险系统，首先要确定参与的各个机构。如在寿险中，一般需要保险公司、医疗机构、银行等参与方加入到区块链系统来，共同参与区块链系统的建设。而在财险中，以车险为例，可能就需要保险公司、交管机构、银行等参与到区块链系统的建设中。甚至，可以将保险监管机构加入到区块链中，成为其中的一个重要角色或者机构。区块链天然的共享账本特性，可以有效地提高监管的效率，从而提高区块链参与各方的公信力。

参与的各方往往是由业务决定。可能同一条区块链上，有多家医疗机构、多家银行、多家保险公司参与。有的同行业的参与方还存在着竞争关系，因此，如何协调上链的各个参与方关系往往成为系统建设的关键。一般在项目开始阶段，每个角色都只允许一个参与方加入到区块链上来，比如一家银行，一家医疗机构，一家保险公司，使业务逐步开展起来，后续如果有某个机构想参与进来，需要与已进入的机构进行沟通、协商，得到允许后就可以加入进来。参与保险业务区块链的各方，一般要遵照一定的行业规范，可设定一定的条款约束参与区块链的各方机构。参与方越多，区块链上的验证节点就会越多，就更容易形成多中心验证，从而实现去中介化，降低机构运营成本。从系统建设考虑，也要确定各个参与方的接入顺序。在保险行业应用场景中，保险机构管理模块和投保人管理模块处于核心地位，需要优先接入。而医疗机构和银行机构可在保险业务系统接入后进行接入联调。政府监管管理模块可根据需要再酌情考虑接入，这样能保证系统建设的有序稳妥。

（2） 确定上链数据内容及格式。

由于区块链连接了各个业务系统，而各业务系统往往都是已有的，并且由参与方自己建设完成。因此，就需要各参与方约定上链数据的内容及格式，从而实现通过链上数据的互联互通，达到信息共享的目的。因此，需要在数据层中，在投保人身份识别数据模块、保险机构业务处理数据模块、其他社会关联机构之间达成数据层面的共识，提炼共同认可的数据内容和格式。

数据内容的确定。确定上链数据的内容是整个区块链项目建设的重点，往往决定项目建设的难易程度以及项目建设的周期。而数据内容的确定一般又是由区块链上参与的多方角色一起制定商讨出来的，这个讨论过程又往往是艰难的。比如在保险公司、医疗机构、银行的三个参与角色中，参与的各方从自身利益角度出发，一定不会将自己全部数据都写入到区块链上。银行从信息安全的角度出发，不会发布用户的资产情况，一般只提供转账服务和一定的账户信息。医疗机构从保护病患信息角度出发，不会将患者的病史信息发布到区块链上，一般只会提供病人的自然信息以及医疗过程中的费用清单等相关信息。保险公司一般只会将保单中的部分信息写入到区块链上，而其后台的一些分析计算数据一般没有必要写入到区块链上。因此，对于上链数据的确认不是一蹴而就，而是需要参与各方多次讨论才能最终确定数据的内容。

数据格式的确定。在数据内容确定的基础上，需要对上链数据的格式进行确定。由于区块链采用了创造性的块链式的数据结构，从而实现了不可篡改、可追溯等特性。但正因为采用块链式的数据结构，一般情况下，区块链上的数据不易过大，如视频、音频、图片这样的数据不适合写入到区块链上。如果业务系统需要处理音视频这样的大文件，一般采用将大文件进行哈希运算，将最终的哈希值保存到区块链上。其他的文本类信息可根据各业务系统的情况，以 xml、json 等各种流行的数据传输格式记录到区块链上。

（3） 各业务系统的改造及与区块链对接。

在参与方、上链数据的内容、上链数据的格式都确定后，就需要将区块链与参与各方的业务系统进行对接。一般业务系统是由参与方各自建设并维护的，要想与区块链进行对接，或多或少要对原有系统进行一些改造或升级。在这个过程中，需要区块链技术人员与各业务系统开发运维人员进行沟通。沟通的内容主要有两方面。

原有业务开发人员对区块链技术和开发方法的学习和理解。因为区块链是一种新的技术解决方案，相对于传统的中心化信息系统存在着很大的不同。业务开发人员需要学习理解区块链的去中心化的理念，了解数据加密解密以及签名验证的概念，初步认识共识机制的原理和特点。除此之外，业务开发人员还要学习区块链的开发接口，只有充分了解了接口功能，才能有效发挥区块链技术的特点，完成业务逻辑的编码和测试。

区块链技术人员对保险行业业务和流程关系也需要学习和理解。保险行业是一个传统的金融行业，但也在不断的创新发展，采用区块链技术就是其重要的突破。这也要求区块链技术从业人员，要快速学习包括保险在内各种金融业务。区块链技术人员应该做到快速理解保险业务系统的逻辑关系，数据的存储方式，这样，才能有效地跟保险从业人员探讨业务设计，帮助保险业务开发人员完成产品需求及设计，并能够提出合理的基于区块链解决方案及建议，实现系统的快速构建。

（4） 测试与验证。

在以上步骤都已完成后，还需要对基于区块链的保险应用的各系统进行测试和验证。由于区块链系统需要连接多个上链业务系统和机构，因此需要完善的测试和验证后才能够正式上线。测试和验证的重点主要围绕以下几个方向。

上链数据的完整性。也就是说，各业务系统写入的数据是否按照原有设计的内容和格式写入到区块链上需要充分验证。

保险业务的完整性。基于区块链技术的保险业务应该在不影响原有保险业务的情况下，提供更丰富的业务模式。因此，应该从保险业务模型角度，多做功能验证，保证原有保险业务逻辑不受影响。

上链数据的保密性。在区块链上有多个同业机构的情况下，为了防止数据被公开，数据一般都采用加密并且只有授权才能可见的方式。因此，数据保密性就特别关键。

上链数据的不可抵赖性。链上数据的每次操作都需要进行签名和验签，以保证写入的数据和操作是不可抵赖。因此，需要保证任何区块链的操作都要有用户的签名，任何数据的修改都需要验证用户的签名和权限，这样才能防止用户恶意篡改数据。

（5） 其他。

做完以上步骤后，往往一个区块链的项目就可以上线投产了。但在系统和业务的运行发展过程中，可能会有新的问题及新的需求。如：有新的机构要加入进来，有新的数据需要写入到区块链上等等这样的问题。因此，就要求整个系统的设计者，在设计数据的内容和格式时，要有一定的前瞻性，要熟悉保险的业务场景，能够保证满足一定的业务扩展需要。这里也需要保险业务开发人员与区块链技术人员在系统设计初期多多沟通，互相学习，设计具有扩展性的方案，使新的需能够更容易就可以实现，快速满足业务需求。

4.1 区块链技术存在的问题

目前区块链技术依然存在几大问题：首先，高能耗问题。正如比特币的实际应用中，其发展带来的结果是实现了计算机硬件的快速提升和膨胀，在“挖矿”过程中的主要成本也转移到硬件成本和由之带来的电力成本等。因此，区块链技术实现权益成本收益后，使其技术功效发挥至最大化将成为未来急需解决的重点之一。其次，数据存储空间问题。区块链系统中每一节点的信息记录以及存储更新，都对每个参与节点的存储空间容量提出了极高的要求。第

三,抗压能力问题。基于区块链构建的系统同样遵循木桶理论,网络系统处理速度和网络环境最差的节点将对整体系统的设计容纳能力造成影响。一旦将区块链技术推广至大规模交易环境下,每秒产生的交易量超过最弱节点的容纳能力,那么交易就自动进入队列进行排队,延长交易时间。

4.2 区块链在保险行业应用亟待解决的问题

在区块链的应用过程中，还需解决以下几个问题：首先，区块链的算力难以保证系统的稳定性。区块链目前还是一项全新的技术，尚未达到大规模应用的要求，其运算能力还有待于进一步提升；区块链技术风险难以完全避免，在完全去中心化条件下，区块链的交易规则以及智能合约实际上都是由计算机程序和语言控制的，当失误未被及时发现时，系统将按照错误程序继续执行。其次，区块链的制度建设和法律监管相对滞后。 一旦发生区块链被攻击、客户个人信息泄漏等事件时，缺乏标准应急处理程序。一旦造成不良后果，整个区块链技术生态环境将会受到负面影响。第三,区块链与保险行业的复合型人才队伍建设亟待加强。区块链技术还处于发展的早期阶段，存在多种可能性和无数的未知数。无数初创企业也在努力突破区块链的技术应用，这都需要大量的复合型人才。第四，信息共享的制度壁垒依然存在。在目前的基础条件下突破现有的传统保险平台,构建统一和共享的区块链保险信息平台，为保险机构之间以及保险与其他行业之间信息共享提供数据服务和技术支持,实现保险行业内外的信息交互共享，需要实施较大的改革。

4.3 区块链在保险行业应用的几点建议

作为促进保险行业发展的重要创新技术,保险业应高度重视区块链技术与保险业务的融合，以顶层设计统领并统筹保险产品的具体应用，创新区块链保险的商业模式。首先，在保险行业应用场景、技术方案和商业模式上需要不断探究和创新，不断深入研究区块链技术的适用标准。其次，不断改进和完善区块链技术，着力改善或解决高耗能、数据存储空间制约、处理大规模交易的有效性和抗压性等问题；第三，完善制度安排，形成协同氛围，实现保险领域的高度“自治”，有效降低市场对监管的需求，推动保险监管向制度性、平台式、社会化监督转变。尤其是要切实解决去中心化的区块链与中心化的政府监管之间如何有效融合、线上线下关联公证、法律效益保障、价值认可等关键难题。

随着保险行业改革创新进程不断加快，区块链在保险行业未来应用具有广阔前景。

参考文献：

[1] 谭磊，陈刚.区块链 2.0[M].电子工业出版社，2016 年.

[2] 徐明星，刘勇，段新星，郭大治.区块链—重塑经 济与世界[M].中信出版社，2016 年.

[3] 陆磊，姚余栋主编.新金融时代[M].中信出版社， 2015 年.

[4] 温信祥，张蓓.区块链的能与不能[J].财经，2016，（6）.

[5] 赵大伟.区块链能拯救 P2P 网络借贷吗？[J].金融 理论与实践，2016，（9）.

[6] 伍旭川，刘学.The DAO 被攻击事件分析与思考 [J].金融纵横，2016，（9）.

[7] 王 和 周运涛，区块链技术与互联网保险 《中国金融》,2016(10):74-76

[8] 黄颖 关于区块链技术在保险业中应用的思考 中国保险报

[9] 邹均 张海宁 唐屹 李磊 《区块链技术指南》 机械工业出版社 2017.

[10]《区块链金融》 深圳前海瀚德互联网金融研究院 2016.

[11]《保险区块链研究》保险区块链项目组 2017.

[12] 黎江 何京汉 区块链、分布式账本技术解读 《金融电子化》2016.（3）.

[13] 陈怡璇 区块链技术:“分布式账簿”《上海国资》 2016(3):78-79.

[14] 王晓峰 基于区块链的分布式账本技术在金融领域的应用及监管建议
《商业经济》 ,2017(4).

[15] 阿尔文德.纳拉亚南 纳什.贝努 爱德华.费尔顿 安德鲁.米勒《区块链技术驱动金融》.

[16] 原文：http://www.longfinance.net/publications.html?id=903.
作者：Michael Mainelli & Chiara von Gunten.

[17] 李凡 区块链技术与保险风控.