30th ANNIVERSARY 1992 2022

大成 DENTONS

DENTONS CHINA

「大成 30 周年所庆文集」

区块链+制造业
全方位合规报告

大成律师事务所

课题
主持人

肖飒

高级合伙人

地点：大成北京
专业领域：刑事、银行与金融、
争议解决、知识产权

课题
参与人

袁承鹏

律师

地点：大成北京
专业领域：刑事、银行与金融、
争议解决、知识产权

王国全

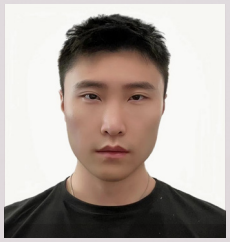
律师

地点：大成北京
专业领域：刑事、银行与金融、
争议解决、知识产权

课题
参与人

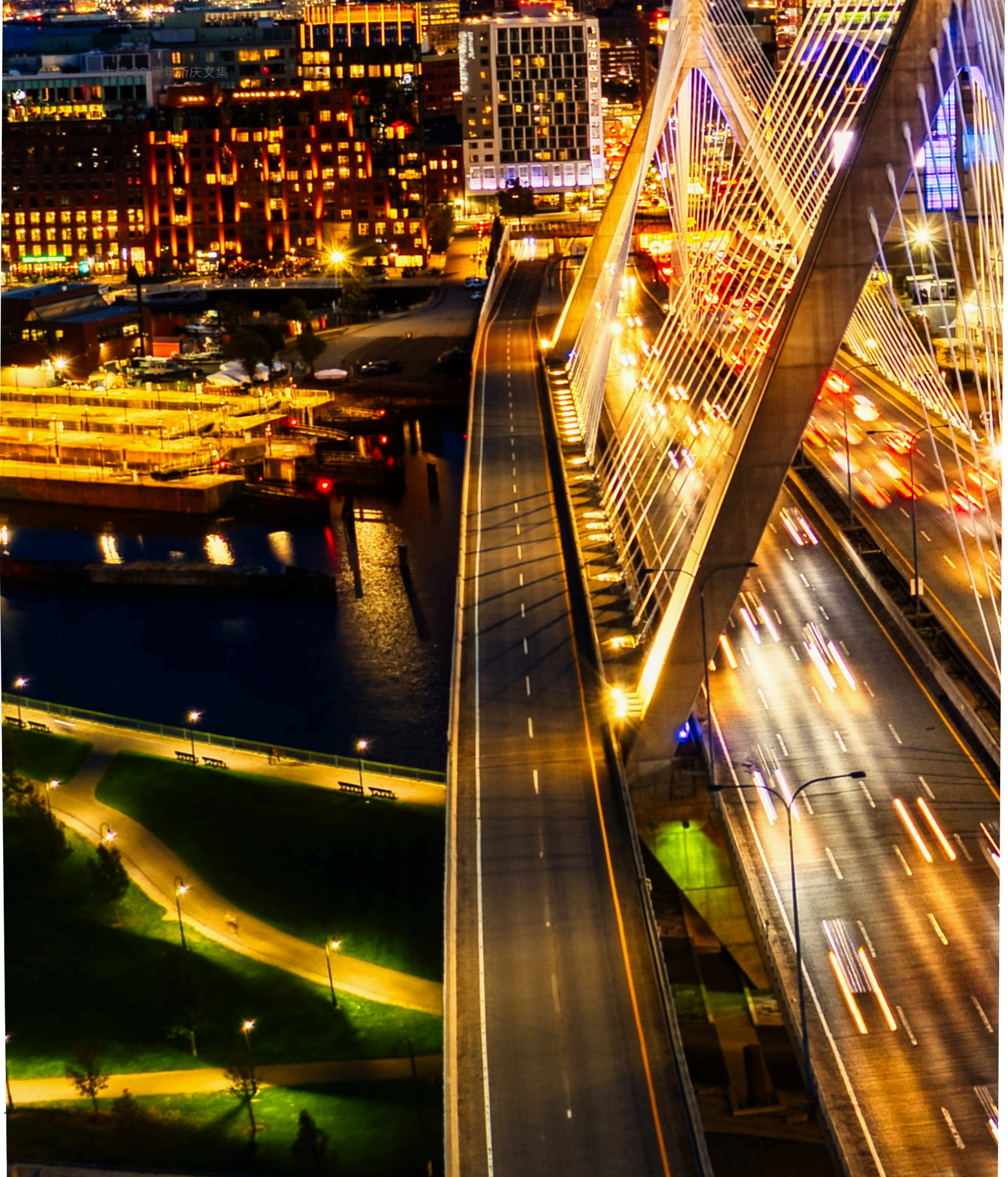
朱会会

实习生



杨子晗

实习生



大成 DENTONS
DENTONS CHINA

CONTENTS

前言

就在今年一月，中央网信办、中宣部、最高人民法院等十六部门联合印发通知，公布经地方和部门推荐、专家评审、网上公示等程序确定的 15 个综合性和 164 个特色领域国家区块链创新应用试点名单。该名单在“特色领域试点”一栏中共包括“区块链 + 制造”企业 15 家，船舶、汽车制造、钢铁、航空航天、港口物流等多个重点领域，表明了国家大力促进“区块链 + 制造业”融合的决心。

区块链技术早已不是理念性或描述性技术，其已经成为目前制造业转型升级过程中最具可操作性、最有前景的应用技术。所谓区块链，即网络上的节点给予共识算法将数据提交到按一定规则和密码学方法前后相继排列的区块，经验证后所形成的链式结构分布式账本。区块链技术允许分布式节点在一个不可信网络中进行点对点通讯，形成一致性意见，记录过程数据并防止篡改，这些特点可以为制造业企业提供工业原料可信溯源、关键过程性数据实时审计、数字仓储管理等多项应用，从而大幅度降低制造业质量体系监管成本和供应链物流成本，促进制造业转型升级。

但是区块链赋能制造业仍然面对着许多风险与合规问题。本报告将从区块链在制造业运用的多种场景出发，详细叙述区块链与制造业碰撞将会有何种“魔法效果”。并从各个应用场景出发，论述将会面对的法律风险，并最终为行业合规发展提出建议与畅想。

第一章

区块链应用概述

区块链应用项目概述

（一）区块链技术概述

区块链概念自2008年在比特币白皮书中被提出以来，引起全世界广泛关注，采用去中心化基础架构与分布式存储共识技术。从记账的角度出发，区块链是一种分布式账本技术或账本系统；从协议的角度出发，区块链是一种解决数据信任问题的互联网协议；从经济学的角度出发，区块链是一个提升合作效率的价值互联网。近年来，区块链逐渐从加密数字货币演变为一种提供可信区块链即服务(Blockchain as a Service,BaaS) 的平台，各行各业均对区块链青睐有加，积极探索“区块链+”的行业应用创新模式。区块链包含社会学、经济学和计算机科学的一般理论和规律，就计算机技术而言，包含分布式存储、点对点网络、密码学、智能合约、拜占庭容错(Byzantine Fault Tolerant,BFT)和共识算法等一系列复杂技术。

由于跨学科融合支撑，使得区块链构建了一个在数字世界中自治理、可信赖、可溯源的系统。

1.区块链平台建构

区块链平台整体上可划分为数据层、网络层、共识层、智能合约层和应用层5个层次。数据层采用合适的数据结构和数据库对交易、区块进行组织和存储管理；网络层采用P2P协议完成节点间交易、区块数据的传输；共识层采用算法和激励机制，支持拜占庭容错和解决分布式一致性问题；智能合约层通过构建合适的智能合约编译和运行服务框架，使得开发者能够发起交易及创建、存储和调用合约；应用层提供用户可编程接口，允许用户自定义、发起和执行合约。

2.分布式账本

尽管分布式账本技术(Distributed Ledger Technology,DLT)常被认为是区块链技术的同义词，但分布式账本是指可以在多个站点、不同地理位置或者多个机构组成的网络里实现共同治理及分享的资产数据库。从计算机技术的角度看，账本是一系列包含交易和信息的数据结构，账本可以记录多方资金的往来记录、物品交换记录等。在区块链系统中，交易被组织成块，然后块被组织成逻辑上的链，因此区块链是一本不断增长的账本。账本可以完全公开，例如比特币系统和以太坊系统，也可以在联盟内公开，例如Hyperledger Fabric。

3.共识算法

区块链系统的节点可自由加入组织，具备自治性，为更好适应区块链系统，大多系统采用 P2P 网络进行数据传播。P2P 网络中的每个节点均会承担网络路由、验证区块数据、传播区块数据、发现新节点等功能。为驱使区块链中的节点有效参与共识过程，区块链的共识算法包括设计合理的经济激励机制和公平选取特定的打包节点。

在传统分布式系统中，评价系统采用 CAP 标准，分别评价系统的数据一致性、数据可用性和分区容错性。对应到区块链系统中，有研究人员提出“不可能三角”的评价标准，包括去中心化可扩展性、安全性。然而对于任意的区块链系统，不能同时满足以上 3 个方面。去中心化主要描述参与共识的节点个数，参与共识的节点越多去中心化程度越高。可扩展性主要看吞吐量的大小考察其是否适用于多种应用场景。安全性考虑其规则被破坏的经济成本，破坏规则的成本越高安全性越高。安全性由多方面保证：包括共识算法的确定性，确定性包括绝对性确认和概率性确认。绝对性确认是指一旦交易被包含在区块中并添加到区块链上，该交易就会被立即视为最终确定；概率性确认是指包含交易的区块的后续区块越多，该交易被撤销的可能性越低。

4.智能合约

智能合约是一套以数字形式定义的承诺，包括合约参与方可以在其上执行这些承诺的协议。这些承诺指的是合约参与方同意的权利与义务，并且在智能合约中定义了实施办法。由此可见，智能合约不一定需要使用区块链技术，只是因为区块链技术能够较好地支持智能合约。

简言之，智能合约是传统合约的数字化版本，在区块链上是可执行程序。与传统程序一样，区块链智能合约拥有接口部分，接口可以接收和响应外部消息，并处理和储存外部消息。

5.密码学

为保证账本的完整性、公开性、隐私保护、不可篡改、可校验等一系列特性，区块链技术高度依赖密码学。正是密码学的一些理论研究和技术特性，使得公有链的所有节点能一定程度上达到公平、安全、可信赖。例如，在比特币系统中，哈希使得工作量证明算法成为全网的共识算法。基于椭圆曲线的公钥密码学的签名验签功能使得仅私钥拥有者可自由支配该账户，从而发起交易。

（二）区块链应用的法律依据

当前，我国区块链应用的法律依据主要集中在两方面，其一是全国人大制定的法律，其二是国务院及各部门、地方政府制定法规、规章。

法律层面，以全国人大及其常委会制定的基本法律《中华人民共和国民法典》以及三大网络数据法《中华人民共和国网络安全法》《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》为主。

行政法规层面，以中华人民共和国国务院公布的《中华人民共和国计算机信息系统安全保护条例》《互联网信息服务管理办法》等法规为主。其中，国家互联网信息办公室等部委制定的《区块链信息服务管理规定》是直接规范区块链应用的部门规章，也是现行有效且效力最高的，专门针对区块链应用的规范性文件。

本团队在长期为区块链企业提供法律服务的过程中，不仅熟悉涉及区块链应用领域的法律和法规，且在长期的研究实践中对我国行政机关的执法方式、办案流程较为熟悉，擅长风险预防与控制，在处理区块链企业相关的民事、刑事和行政案件中具备独特的优势。

（三）区块链应用的法治环境

2021 年 10 月 24 日下午，中共中央政治局就区块链技术发展现状和趋势进行第十八次集体学习。习总书记在主持学习时强调，区块链技术的集成应用在新的技术革新和产业变革中起着重要作用。自此，发展和布局区块链技术已经成为我国基本战略布局。

1.国家层面

《“十四五”规划》中专门设置了“加快数字化发展建设数字中国”章节，并对加快建设数字经济、数字社会、数字政府，营造良好数字生态作出明确部署。

此外，2015 年国务院办公厅发布了《关于加快推进重要产品 追溯体系建设的意见》鼓励在食用农产品、食品、药品、农业生 产资料、特种设备、危险品、稀土产品等七个领域发展追溯服务产业。2020 年 10 月 1 日，由全国防伪标准化技术委员会 (SAT/TC218) 提出的《基于移动互联网的防伪溯源验证通用技术条件》颁布的防伪溯源标准，对区块链在防伪溯源领域的应用做了明确要求，这也是区块链首次进入防伪溯源类的国家标准。

2. 地方层面

《浙江省数字经济发展“十四五”规划》在涉及区块链应用方面指出：“要做优新兴产业。发展云计算、大数据、人工智能、物联网、区块链、虚拟现实等新兴产业。推进开源开放平台建设，加强云原生架构、关键算法资源、低代码工具等供给，培育具有国际竞争力的开源生态。推进“区块链 + 物联网”等融合创新产业生态。

（四）区块链应用概述

区块链作为一种利用加密算法、共识机制等计算机技术构建的，以去中心化、点对点传输为特点的，不可篡改、不可伪造的分布式记账系统，兼具数据存储功能。区块链作为一种底层协议或技术方案可以有效地实现价值的自由传递，在商业交易结算、数字政务、存证防伪数据等领域具有广阔前景。当前，区块链主要有以下几个应用场景：

1、数字货币与数字藏品

当前，数字货币已经成为数字经济时代的发展方向，数字人民币也已经进入紧锣密鼓的试点阶段。相比实体货币，数字货币具有易携带存储、低流通成本、使用便利、易于防伪和管理、打破地域限制，便于高效整合等特点。

2.金融资产交易结算

区块链技术天然具有金融属性，正对金融业产生颠覆式变革。支付结算方面，在区块链分布式账本体系下，市场多个参与者共同维护并实时同步一份“总账”，短短几分钟内就可以完成现在两三天才能完成的支付、清算、结算任务，降低了跨行跨境交易的复杂性和成本。

3.行政、税收等数字政务

区块链可以让数据跑起来，大大精简办事流程。区块链的分布式技术可以让政府部门集中到一个链上，所有办事流程交付智能合约，办事人只要在一个部门通过身份认证以及电子签章，智能合约就可以自动处理并流转，顺序完成后续所有审批和签章。区块链发票是国内区块链技术最早落地的应用。

4.存证溯源防伪

区块链可以通过哈希时间戳证明某个文件或者数字内容在特定时间的存在，加之其公开、不可篡改、可溯源等特性为司法鉴定、身份证明、产权保护、防伪溯源等提供了较好的解决方案。

5.元宇宙及其他商业化、工业化应用

由于区块链技术在数据流通和共享上的巨大作用，促进了下一代互联网新形态——元宇宙的诞生。作为聚合了人工智能、物联网、大数据、云计算、深度学习、可穿戴设备等软硬件技术的下一代互联网，元宇宙在城市建设、综合娱乐、商品贸易、工业模拟、慈善公益、金融、能源、物流等方方面面都有巨大的作用。

本团队深耕区块链及金融科技领域，长期为国内外数十家区块链应用企业提供专业法律服务，包括国内国外各大知名 NFT、数字藏品交易平台，虚拟货币交易所等。在区块链企业合规、知识产权保护和刑事诉讼方面具有丰富的经验。

区块链应用的价值

分布在全球的制造协作体，以市场化的组织方式共同完成制造过程，实现对需求的响应和价值创造，这是现代制造业的重要特征制造业的转型升级是为了更高效地融入这一全球制造协作体系。区块链具备分布共识 (Distributed Consenus) 、数据持久 (Data Persistence)、不可篡改 (Immutability)、数据可溯 (Data Provenance) 、数据透明 (Transparency) 等特性，与这种分布式协作的特征具有很高的契合性，因而在制造业的转型升级中拥有较大的应用潜力。如果将全球制造协作体视作一个复杂网络，每一家制造企业都是其中的一个单点，按照区块链应用所涉及的单点集合的拓扑结构特点，可以将区块链在制造业转型升级中的应用分为单点应用、链状应用和网状应用。

（一）单点应用：数据管理与工业控制

单点应用即适用于单个制造企业的应用。区块链技术能够应用于制造企业内部的数据管理，其分布共识特性能够规避中心化系统所面临的单点故障 (Single Point of Failure) 、恶意攻击和内部人篡改等问题，数据持久和不可篡改保证了数据共享的安全性和可靠性，数据可溯和数据透明则保证了制造企业的生产、财务、库存等数据都是可审计的，防止内部腐败和作假。进一步地搭配以智能合约，可对异常的生产数据、不合规的财务数据等自动示警。

区块链的引入还有助于提高工业控制系统 (Industial Control System) 的安全性。工控系统中，可编程逻辑控制器 (PLC) 按照接收到的指令控制设备运行，指令一旦遭到恶意篡改后果十分严重。引入区块链可以解决这一安全问题：发布时将指令文件摘要加上发布者私钥形成数字签名上传至区块链，收到指令文件的节点用公钥验证数字签名后证明指令文件无误才予执行，否则就向系统报警。

（二）链状应用：供应链管理

供应链是涉及产品制造、运输和销售的所有组织、个人、资源、活动和技术所构成的集合。供应链以共同的产品为链将上下游连接起来，部署于供应链的区块链应用可称为链状应用。制造业全球化的进程中，市场竞争力不仅取决于产品本身，也取决于通过供应链交付产品的效率，供应链管理因而变得重要。不过信息往往散落于供应链上的不同主体，每个主体只掌握自己的信息，供应链上的大公司才有可能对上下游的部分信息有所了解。因此，传统供应链上信息是不容易追踪的。

区块链可以帮助制造业供应链建立可信的溯源信息流。基于区块链的供应链管理系统 (SCM) 中，每一环节的主体都将产品特性与交易信息录入到区块链上，区块链的数据可溯保证了上链信息包含了产品从初级原料到终端消费者的整个生命周期完整、有序地呈现不可篡改保证了这一呈现的可靠性，数据透明保证了产品溯源信息对供应链利益相关者都是可查询的。不过区块链只能保证录入信息的可追溯和不可篡改，不能保证录入信息为真实信息。一个解决办法是以物联网设备录入代替人工录入：设置二维码、RFID 等身份标识，每个环节都由物联网中的传感器读取身份信息，并自动录入到区块链中。这一解决方案对供应链整体的转型升级要求较高，每一环节都要部署物联网，且无缝衔接；为保证安全性，物联网本身也要采用区块链架构；为确保身份标识的可靠性，还需引入量子云码化学签名等防伪技术。

（三）网状应用：社会化制造

全球化竞争态势下，制造的敏捷性日益重要。传统供应链管理的信息追踪是非现场因而滞后的，粗粒度因而不精确的，在此基础上实现的生产协同仍不是高效的，难以快速响应个性化需求。理想状态是打破企业壁垒，基于物联网、信息物理系统 (Cyber–Physical System)、数字孪生 (Digital Twin) 等工业 4.0 技术，将制造资源接入工业互联网，实现按需协同制造，即云制造 (Cloud Manufacturing) 或社会化制造 (Social Manufacturing)。协同制造不再局限于单一供应链，而是多供应链交错叠加形成复杂的协作网络，在更大空间范围内实现效率提升和柔性生产，部署于复杂制造网络的区块链应用即网状应用。

云制造的资源分布是非中心化的，但传统的云制造管理却是中心化的，因此具备了中心化系统的脆弱性。区块链为分布式的社会化制造体系的构建提供了技术基础。分布式社会化制造体系由于缺乏中心化实体来审核节点是否提供了合格的服务，因此需要引入信任机制。区块链分布共识的特性，提供了一种自组织、自维护、不需要系统外第三方背书的信任机制，使得分布式社会化制造体系具备可操作性。区块链的不可篡改、数据可溯和数据透明，能实时提供资源提供者的准确、完整的行为日志，在此基础上生成关于资源提供者能力和信用的可靠报告，大大降低了资源提供者的道德风险 也足以劝退不合格的制造资源所有者，进一步规避了逆向选择，从而吸引更多组织和个人成为社会化制造体系的资源使用者。社会化制造体系中的物联网设备和生产设备每时每刻都生成、收集、交互数据，数据一致性成为云制造系统的关键问题，而区块链的分布共识和不可篡改为之提供了保证。制造资源之间的协同，可以通过区块链上的智能合约进行，实现无人值守的智能制造。随着个性化定制在制造业中的份额扩大，3D 打印等增材制造 (Additive–Manufacturing) 技术将在社会化制造中得到广泛应用，区块链数据的不可篡改可以保证分布式 CAD 模型中存储和传输的数据与创建时一致，在此基础上交付的产品与设计原型相符，从而确保柔性制造的可靠性。

区块链的法律风险

（一）总体法律风险评估

区块链是新兴战略产业，具有技术创新和制度创新的双重属性。因此，区块链与航运物流业的融合是对现行物流法律制度与规则层面的创新尝试，且最终要落实到制度变革之上。然而，区块链融合物联网并应用于航运物流而复合出的新特征已引发一系列更为复杂的法律问题。

（二）具体风险分析

1.技术局限性转化为法律风险

技术局限性属于技术本身的风险，但因不可避免的技术局限性带来的后果可能转化为法律风险。区块链技术在航运领域广泛应用后，同样面临着作为底层技术被攻击的可能性，此时研究技术风险转化为法律风险就十分有必要。

区块链实则是一种技术，区块链系统的每个节点都在按照既定的代码规则运行。即便在区块链构建的数字化空间，技术仍需要一定规则加以运行，这一整套规则即构成区块链的法律规范制度。若想实现有限监管及规避法律风险，则需要事前对其技术规则进行界定，但是这方面在全球看尚无区块链技术规则的法律制度、技术指引或行业标准出台。区块链技术规则发生变化时，需尽可能得到那些相关参与者的认可。由于现在尚未有相关的法律对其进行行为规范，当这些相关参与者做出决策行为时，若实现各自利益的平衡则比较难，甚至会出现谈判的僵化或停止。技术属于内在规则范畴，法律则属于外在规则范畴，内外协同才能更好推动区块链良性发展区块链技术本身仍处于发展初级阶段，与之相关的法律体系尚不健全，使得区块链技术规则方面的法律问题更加凸显。

2.智能合约对具体规则的挑战

从法律角度看，智能合约并非法律意义上的合只是合约的一种履行方式。智能合约实则是一段代码或数字程序，并非合同内容，缺乏合同的一般要件，如合同形式、终结及适用法律等条款。

智能合约作为区块链的核心技术，对于区块链应用至关重要。《民法典》规定了合同无效、变更、撤销的种类及法律后果，现实中的一般合同关系较清晰，且合同签订主体达成共识后可以修改、废止、补充等。在智能合约中，合同条款以数据代码形式写入区块链的分布式账本，便直接生效、无法干预，甚至违反了法律条款也会得以执行。智能合约因其自身特性及依托技术特性等因素，则不可篡改、不可撤销、自动执行，合同当事人也无法违约。可见，智能合约的出现对《民法典》等民事法律体系带来新的挑战。不仅如此，由于区块链技术带来的智能合约可匿名性，若匿名的智能合约发生法律纠纷时，纠纷的另一方是谁都将无法确定，采取传统的诉讼方式进行解决则将难度变大。

3.数据隐私的法律隐患

分布式账户技术面临最大的风险在于数据隐私，因其数据可能存放在多个不同的地点且数据不能被更改。一旦在区块链上存续了数据，用户在任何情况下都无法删除。更为致命在于，区块链中所有成员都共同参与，任何成员只要持有私钥都能读取区块链中的数据或信息。私钥若发生丢失或遗忘，则存续在区块链中的数据或信息将无法使用，导致信息泄露或被公开的风险。

4.行业标准和技术协议缺乏统一标准

制造业涉及买卖、运输、保险、结算、海关、检验检疫等环节且具有较强的涉外性。因此创新区块链 + 制造业模式面临不同国家、不同行业、不同系统之间行业标准和技术协议不统一的问题。

（三）风险形成的原因

1.技术局限性

当前，区块链技术刚刚起步，尚未取得突破性进展，欠缺较为成熟的产品，目前在港口航运业更多地用于提高行政效率、降低财务成本等方面，深度融合运用仍有待进一步开发和探索。并且，区块链技术并非一项独立的技术，需要与云计算、大数据、物联网、移动互联网以及人工智能技术融合运用，实现由“万物互联”向“万链互联”的演进。

2.法律滞后性

不同的区块链缺乏统一的应用标准，在区块链应用时存在跨链的可用性风险。一方面，在同一领域的应用中，不同的企业选择不同的区块链技术提供商，用户使用区块链时受到的约束不同，会给用户造成诸多不便，造成业务的低效率；另一方面，各公司之间数据无法互通，可能会形成众多的新的数据孤岛，无法真正达到区块链所设想的数据互联互通、透明共享的目的。

（四）风险发生的特点

1.风险范围广

区块链技术与大数据、云计算、人工智能等其他新兴技术的交叉与融合，其应用场景以“三环扩散”的水中涟漪形态扩散到各个业务领域。

2.监管难度大

相较于传统的风险监管，区块链技术风险监管的对象、技术要求和风险特点都有变化。从监管对象、监管技术、监管体制等方面都存在很多问题亟待解决。

3.责任认定难

由于区块链中每个节点的用户都是匿名的，参与交易的各方都是通过地址传递信息，即使获取了全部的区块信息也无法识别参与者真实身份。

4.数据跨境引发法律问题

从法律层面来讲，法律和行政规章等适用于管辖国境内的违法行为，对于在国外实施的违法行为不能直接管辖；即使损害后果发生在中国，中国具有管辖权，也有较大的执法障碍。

第二章

“区块链+制造业”的具体应用

正如上文所言，区块链技术允许分布式节点在不可信的网络中形成一致性意见，记录过程数据并防止篡改，该描述学界一般称之为分布式协同性，分布式协同性包括分布共识（Distributed Consenus）、数据持久（Data Persistence ）不可篡改（Immutability）、数据可追溯（Data Provenance）、数据透明（Transparency）五大特征。现代制造业同样存在分布式协同性，分布在全球的制造协作体，以市场化的组织方式共同完成制造过程，这正是现代制造业的精髓所在。因此分布式协同性成为现代制造业与区块链技术的契合点，“区块链 + 制造业”融合的应用场景也均离不开分布式协同性。

制造业 + 供应链物流

国内某钢铁企业利用区块链技术改造传统仓库，将区块链技术与仓储管理相结合，打造高效、协同、可信的第三方数字监管仓平台，填补了全球范围内大宗工业品中厚板领域数字化监管能力的空白。数字监管仓平台通过三维立体定位、智能影像识别、UWB等物联网设备收集的库存资产信息，进行区块链存证，并和业务流数据进行比对，从而将物理仓库与存货资产、数字仓库与存货资产进行同步映射，实现实物资产、员工、系统、设备、环境等要素实现“数字孪生”,实现了货物入库、移动和出库的实时监控，异常出库预警、人员车辆监测等功能，大幅提高仓储管理效率和管理水平。

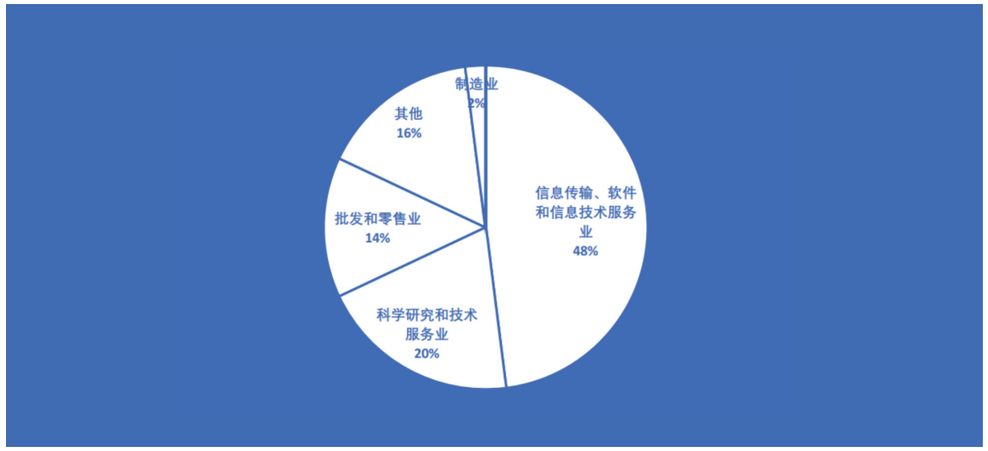
（一）行业宏观图景

一般认为物流业是生产性服务业，严格意义而言其不属于制造业。但生产性服务业并不能脱离制造业独立存在，制造业的发展离不开供应链物流活动，物流业与制造业之间存在着大量的资金、信息交换，两者的发展早已融会贯通。早在2009年国务院发《物流业调整和振兴规划》中就已经将制造业与物流业联动进展列为“九大工程”之一，因此本报告虽面向区块链+制造业，但在论及区块链+制造业的具体应用时，依然将区块链在供应链物流领域中的应用作为研究对象。

1.国内提供“区块链+供应链物流”解决方案企业数量极少

目前我国区块链企业图景可以用“蓬勃发展但偏科明显”来概括。从全球范围来看，拥有区块链企业数量和规模排名前两位的国家分别是美国(约32%)和中国(约30%),两国区块链企业数量占全球的60%以上。单就企业数量上而言，我国是很典型的区块链行业强国。但我国区块链企业目前“偏科”现象明显。利用某企业信息统计查询工具查询显示，目前我国区块链企业注册行业主要集中在信息传输、软件和信息技术服务业及科学研究和技术服务业两者企业数占区块链企业注册总数的近70%,而制造业行业的区块链企业仅占区块链企业总数的2%左右(如下所示)。

在数量占比仅2%的“区块链+制造业”企业中，专门提供供应链物流解决方案的企业屈指可数。本报告将在“区块链+供应链物流”具体应用部分进行举例。



2.“区块链+供应链物流”具有较为广阔的应用前景

在政策扶持方面，《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》明确提出以联盟链为重点发展区块链服务平台和供应链管理等领域应用方案，完善监管机制。工信部和网信办联合发布的《关于加快推动区块链技术应用和产业发展的指导意见》明确指出聚焦供应链管理等实体经济领域，推动区块链融合应用，支撑行业数字化转型和产业高质量发展。此外，随着今年四月，《中共中央国务院关于加快建设全国统一大市场的意见（以下简称“《意见》”)发布，在国家层面大力扶持“区块链+供应链物流”应用几乎成为必然。《意见》全文共10次提及“流通”,8次提及“物流”,4次提及“供应链”,可见国家对于强化我国现代物流体系的重视程度。

在发展空间方面，目前我国供应链物流存在明显短板，提升潜力巨大。基于物联网、区块链等技术构建全供应链范围内的流转网络，实现全供应链数字化运营，是我国目前供应链物流行业发展的目标。而要实现“全供应链数字化管理”,基于区块链技术的综合供应链物流解决方案就必不可少，提供相关解决方案的企业市场潜力巨大。

（二）行业具体应用

1.区块链+链上监管仓

“区块链+链上监管仓”模式目前在我国已有较为成功的案例。国内某工业区块链解决方案提供商为国内某钢铁企业提供的工业区块链综合解决方案中就已经包含“区块链+链上监管仓”应用。在这个案例中，该钢铁企业利用区块链技术改造传统仓库，将区块链技术与仓储管理相结合，打造高效、协同、可信的第三方数字监管仓平台，填补了全球范围内大宗工业品中厚板领域数字化监管能力的空白。数字监管仓平台通过三维立体定位、智能影像识别、UWB等物联网设备收集的库存资产信息，进行区块链存证，并和业务流数据进行比对，从而将物理仓库与存货资产、数字仓库与存货资产进行同步映射，实现实物资产、员工、系统、设备、环境等要素实现“数字孪生”，实现了货物入库、移动和出库的实时监控，异常出库预警、人员车辆监测等功能，大幅提高仓储管理效率和管理水平。

2.区块链+海关保税物流监管和追溯

早在2019年部分行业从业者就已经将类似的应用系统申请专利,这类工业区块链应用通常包含区块链存储包、定位模块、通讯模块和监控等模块，利用区块链技术可以及时提供相应的物流车辆跟踪信息和报关人员信息并进行监控和管理，实时掌握报关企业业务信息、车辆货物信息、人员信息及地理信息。该系统可以加快国际物流信息的传递速度和信息的透明度，使得通关速度快速提高从而显著降低企业供应链物流的运营成本。目前类似的系统已经被北京海关、青岛海关、南昌海关等单位引进，进而实现国际货物运输全程信息流、物流、资金流、关务流的互通互认和贸易全链条闭环数字化运行。

（三）法律风险点

如前所述，无论是区块链+链上监管仓还是将区块链+海关保税物流监管都会涉及大量的数据要素，这些数据要素要么涉及地理位置信息、人员信息，要么涉及到企业运营信息及供应链信息，因此这些数据要素的安全性就成为区块链+供应链物流应用中最大、也是最为重要的法律风险点。

1.区块链+供应链物流中的数据安全关乎国家安全

习近平总书记在中共中央政治局就实施国家大数据战略进行第二次集体学习时明确强调，要切实保障国家数据安全，加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。数据安全已经成为未来大国博弈的焦点。习近平总书记指出要完善国家安全制度体系，重点加强数字经济安全风险预警、防控机制和能力建设。实现核心技术、重要产业、关键设施、战略资源、重大科技、头部企业等安全可控。

“区块链+供应链物流”应用所服务的单位多涉及海关、港口物流、船舶、钢铁、航空航天等多个重点领域，可以说是“大国重器”,因此上述单位的上链数据安全关乎到国家安全，单位如何在自身运营过程中保障链上数据安全，配合公权力机关完成数据国家安全评估，便成为亟待解决的问题。

2.区块链+供应链物流应用过程中极易发生数据滥用问题

以上文区块链+海关保税物流监管和追溯系统的专利为例，该系统可允许对报关人信息、地理位置等敏感数据进行采集，这就极易造成数据剥削与滥用。但目前大多数相关企业、单位尚未绷紧数据剥削与滥用的弦，从这个角度而言，上述企业单位必须明确对应用区块链技术产生的数据合理使用的界限在何处，否则极易造成市场不正当竞争风险和数据滥用风险。

制造业+链上电子仓单质押融资

国内某大型港口利用区块链技术改造传统仓单系统。区块链电子仓单是结合区块链技术打造的一种数字化凭证，可将传统的港存货物转化为优质安全、具有良好流动性的可信资产。链上电子仓单依靠区块链不可篡改、数据持久、数据可追溯特征，在生成、流转注销等流程中通过区块链存证和溯源，可大幅度提高仓单的真实性和有效性。金融机构通过链上仓单可以更好地进行贷款风控评估。

（一）行业具体运用

区块链技术支撑起的电子仓单系统不同于一般的电子仓单系统其将仓单质押过程中的每一个信息打包成一个个区块，并利用这些区块不可篡改、永久储存、可追溯、可随时更新等特点，将这些区块传播到全网，仓单链条上的每一个主体都可以随时且反复确认每一区块信息的真实性，从而保证整个仓单系统的顺利运行。因此，如果能够引入区块链技术，那么就可以大大减少纸质仓单的弊端，这种“去中心化”的技术同时也给仓单系统的维护和运作减轻了压力，可以防止数据的丢失与损毁，更好地保存信息。

1.识别仓单造假

目前对于仓单的开具和流转过程无法做到公开化和透明化，而银行处于信息不对称的一方，因此融资方和仓储部门可以借助这片监管空白进行合谋，开具虚假仓单，比如质押物数量不足或者品质难以保证等。也很容易进行质押物的重复质押，甚至通过虚构交易来实现套利、套汇及套税的“三套”行为，这严重违背了大宗商品交易市场规则和道德底线。区块链的追溯功能使得每笔交易都可查询，区块链的加密技术使得每笔交易都真实可靠。

2.解决仓单流转困难问题

港口仓储企业开具的仓单缺乏业界的权威性，流通性相对而言比较差，仓单最终持有者若向其他银行申请质押融资，可能不被其认可，或者转让给其他交割方时不被接受。此外，仓单的拆分和转 让的手续也十分复杂，需要重新开具新的仓单、重新背书、更改现有仓单所有人等，这些操作需要多方共同参与，流程繁杂，导致效率低下、安全性弱，因此容易造成仓单的流失以及被篡改等风险。区块链智能合约的应用能够自动执行仓单的交易，效率高。

3.解决信息不透明导致企业间信息孤岛问题

港口仓储企业、银行、中小企业等参与方的信息不畅通，没有一个可信的第三方交易平台，大宗商品交易过程中的“四流”很难合一。银行难以获取中小企业的信用信息，风控难度加大，也提高了中小企业的融资难度。仓单信息上链后无法篡改，可信度高；分布式账本管理，信息传递更加方便；实行点对点交易，信息公开透明。

4.降低中小企业履约风险

大宗商品进出口贸易商和供应商数量庞大，信用状况难以把控银行根据签订的三方协议以及缴纳的保证金来约束融资企业的还款行为，而对于融资企业的资金使用情况不可控。因为中小企业除了进行正常的贸易行为外，还可以将资金用于其他生产交易活动。此外中小企业也可能违背契约精神，故意拖欠贷款，恶意违约。区块链约定多方协议，由智能合约执行，数字签名和背书策略容易确定责任人，每笔交易需要全网节点共同背书；银行可以通过对区块链存储的交易记录确定用户画像，减少征信成本。

（二）行业风险点

1.去中心化及不具名性的特征难以审查

与传统的由特定金融中介机构控制交易流程及信息相区别，去中心化必然导致责任认定的审查难度。依据我国现行《侵权责任法》的规定，网络用户、网络服务提供者利用网络侵害他人民事权益的应当承担侵权责任；网络服务提供者知道网络用户利用其网络服务侵害他人民事权益，未采取必要措施的，与该网络用户承担连带责任。而在区块链技术背景下，如何认定“网络服务提供者”的范围及身份，是摆在监管机构面前亟待解决的难题。

2.智能合约存在漏洞

区块链体系亦是一个智能合约系统，节点参与者在其上以代码的形式将交易各方的信息以及交易内容写入区块，通过智能合约体系在不须人为干预的情况下进行自动执行交易。区块链的基于哈希算法和时间戳的架构使之具有较高的安全性，但事实证明智能合约体系仍然可能被黑客攻击。

3.去中心化与中心化体系的协调存在障碍

目前以区块链为基础架构的去中心化系统基本仅应用于边缘化创新性领域，尚未独立于通行的中心化金融体系。但随着区块链技术的发展及去中心化理念的传播，传统的银行、金融机构等实体与区块链平台之间的界限必将进一步模糊化，且金融产品的流通性也必然要求二者的联结。因此如何实现传统实体与区块链平台的互联互通，同时减小技术创新对传统实体带来的巨大冲击和风险必将成为监管机构的研究重点。

区块链 + 零配件链上溯源

（一）零配件产业的困境

零配件，指的是已经完工、已构成用户产品的组成部分的产品如集成电路块、仪表、仪器等。它们虽然不能独立发挥作用，但却能直接影响用户产品的正常运行。无论是精小的电子产品或是相对 大型的汽车，其安全性以及高性能都需要零配件的配合，只有质量合格的零配件才能支撑产品的良性运行。

尽管随着技术的不断进步，制作合格的零配件并不是一件难事但事实上，因为零配件而引发的质量问题却难以避免。2021 年 12 月 3 日，因悬架转向节存在问题，有断裂风险，特斯拉（上海）有限公司便宣布召回 2021 年 2 月 4 日至 2021 年 10 月 30 日期间生产的 21599 辆国产 ModelY 型电动汽车。而此前，仅仅在汽车行业，玛莎拉蒂、大众、本田、现代等知名汽车品牌也曾出现过不同的因零配件质量而引发的车辆质量问题。

而实际上，除了上述质量问题，在零配件市场还有诸多问题存在：

其一，有一些维修商或零配件销售者在对产品进行维修或进行零配件销售时，利用与消费者之间的信息不对称，以次充好，实际上侵犯了消费者的权益。

其二，消费者出于对前述情况的担忧，往往在进行维修或购买时，担忧零配件的质量，缺乏对行业的信任。

其三，事后追责效率低。即便事后能够定位到是某一零配件出现了质量问题，但是该零配件产生问题的原因以及如何定位厂家，甚至于厂家如何进行问题产品召回处理仍然是很大的难题，需要消耗大量的人力物力以及时间，效率很低。

（二）解决路径：零配件链上溯源

而事实上，运用区块链技术进行零配件链上溯源打造零配件链上溯源系统能够更好地解决上述问题。具体而言，这需要产品零配件制造商在制作零配件时，将该零配件的生产时间、生产批次、物流运输等数据运用区块链技术进行上链 并且在该零部件从制造商转移到物流商、渠道商等企业以及终端消费者时也会将有关信息持续更新到链上。那么，利用区块链技术的去中心化、共识机制、信息可追溯等特点，前述问题便能够得到解决。尽管并不能保证所生产应用的每一个零部件都不会出现问题，事实上这也不能保证，但由于每个零配件的相关信息已经被上传于链，那么通过查询链上记载的信息就能辅助判断该零配件的品质，并且能够获悉该零配件的供应路径，这就能够起到防伪溯源的功效这种防伪溯源体系的建立会实质地对消费者、企业产生深刻影响。对消费者而言，该体系的建立不仅能让他们免去后顾之忧，不必过分担心所用零配件并不存在太大的质量问题，而且在实际发生了问题之后，他们也能通过上链的信息，准确地进行追责，维护自身合法权益。对企业而言，该体系的建立意味着，当某产品的零配件出现问题时，企业可以通过区块链进行信息回溯，准确找到问题零配件的制造商，从而降低企业召回问题产品的成本，提高召回速度和效率同时这也有利于让产品售后的服务商实时掌握产品健康状况，并且通过对累积的产品历史数据进行分析，以提前预防产品可能出现的故障，增强产品使用的安全性，以提供更为完善的产品售后服务。此外，这对于提升整个零配件供应链上所涉及企业的服务质量和产品质量都有促进效果。换言之，正是因为相关信息存储于链上，因此通过比较很容易便能够判断出哪些企业提供的服务或零配件更好，这便促使企业不得不提升自己的零配件质量和服务质量，以此获得更大的竞争力，从而间接地达到了杜绝企业以次充好、提供质量不佳零配件行为的效果。

（三）零配件链上溯源体系下的法律风险

尽管运用区块链技术进行防伪溯源，搭建零配件链上溯源体系能够有效解决零配件产业中的相关问题，但区块链技术的应用并非毫无法律风险，零配件链上溯源体系亦是如此。其法律风险大致有如下几类。

1.数据、信息安全的法律风险

其一，由于在零配件链上溯源体系下需要将有关信息上传，而传输的信息本身属于数据的范畴，其中的部分内容甚至可能涉及个人信息或个人隐私，因此其是否能够合法使用以及如何合法使用该数据便是一个风险点。换言之，如果企业上链所用数据是采用非法 手段进行收集和使用，那么就违反了《数据安全法》《个人信息保护法》等法律的规定，甚至可能构成诸如侵犯公民个人信息罪等犯罪。

其二，即便企业在上链以及后续使用数据时所采取的方法完全合法，在后续存储数据的过程中仍然存在法律风险。区块链技术的性质决定了一旦在链上存储了数据，上链者在任何情况下都无法删除该数据，且该数据能够被参与该区块链的所有成员看见，任何成员只要持有私钥都能读取区块链中的数据或信息。这也就意味着，如果私钥发生丢失或遗忘，或是私钥持有人故意实施某些违法行为则存续在区块链中的数据或信息将无法使用，有信息泄露或被公开的风险。

2.技术固有的法律风险

尽管目前看来，区块链技术在存证溯源的有关应用下已被认可为一项可以应用的高新技术，但是这并不意味着其本身不会出现任何法律风险。事实上，任何一种技术只要是作为技术存在，都有着被攻击的潜在可能性。这种攻击一旦发生通常难以避免，且其后果一般也在事前难以想象，会给企业带来较大的损失。

此外，由于区块链的技术特性，一旦记述的初始信息发生错误那么该错误将不可撤销地共享给其他网络节点，从而产生几乎不可能更改的错误记录。因此，如果在零配件信息上链过程中上链人员出现过错或设计的程序出现较为致命的漏洞，那么就可能导致错误的信息被登记上链，这一方面会给零配件链上溯源带来困难，难以发挥其防伪溯源的效果，影响整个体系的正常运作。而另一方面若错误的信息导致了后续参与者的错误信赖，并基于此错误信赖而行动导致了他方的损失产生，那么导致该错误登记者，可能需要承担相应责任，除非他能证明该错误无法避免。应当注意的是，如果该错误是由企业员工自身所致，但由于该员工所作行为本身仍属于因执行工作任务，因此所导致的损害仍然应当由企业承担赔偿责任，企业仅能在员工自身属于故意或重大过失的情况下，在赔偿后向其追偿。

同样在上述情况下，如果所错误登记的信息涉及第三方隐私或个人信息，那么该信息将不可避免地共享给所有相关方，显然由于该行为并未事前获得第三方个人的授权同意，应当属于违反《个人信息保护法》的行为。尽管该种情况仍然与数据以及个人信息有关可以归纳为数据安全方面的法律风险，但是由于其本质上是因为区块链技术自身的局限性引起的，因此将其归纳为技术所引发的法律风险之中。

3.实物与链上信息不匹配的法律风险

如前所述，零配件领域的一个重要难题便在于存在许多以次充好的现象，而通过区块链技术，建设零配件链上溯源体系是一个很好的解决方式，消费者一旦发现零配件出现问题，便能够通过链上信息准确找到该零配件的生产商，从而依法维护自身的权益。

但是应当注意的是，尽管链上信息能在一定程度上印证所购买的零配件实物的生产情况以及流转情况，但是这种对应关系并非是绝对的。

换言之，一方面，线上信息在上链时可能因为上链人员的故意或过失或者程序上的错误导致其与实物之间存在误差，从而使得出现实物与链上信息不匹配的法律风险。由于这部分风险产生的根本原因是区块链技术的固有局限性，因而这部分法律风险已经在前面第二点中予以提示。而另一方面，在登记上链前或者登记上链后的实体物流转过程中，也可能产生实物与链上信息不匹配的情况。具体而言，可能会有员工因为失误将 A 号零配件误认为 B 号零配件进行登记，导致出现链上记载的是 B 号零配件，实际需要的是 B 号零配件，但产品中的零配件是确实 A 号的情况。此种情况下，若 A 与 B 号零配件的性能呈现较大差异，消费者极有可能认为是该批产品的质量存在问题，从而要求相关主体进行赔偿。但对于企业而言，更为致命的是，如果该零配件在整个产品安全性中处于重要地位，不可或缺，而现在却发生了性能上的较大差异，由此便会给产品带来安全隐患，并带来巨大的法律风险。

除此以外，在实体物的流转过程中，还有一种可能产生实物与链上信息不匹配的情况是，企业或员工故意用伪劣零配件冒充正品原配件进行上链。那么，该种情况下，与不采用零配件链上溯源体系而以次充好的行为没有实质上的差异。而且由于链上信息不断流转带来的增信效果，消费者会更加信赖和信任产品零配件的真实性这也就意味着，一旦真的出现问题，消费者对该企业的不信任也会更容易达到峰值，从而给企业带来负面影响。

这实际上也说明了运用区块链技术进行零配件链上溯源并不能保证链上信息与实物的一一对应，上链信息实际上也不能独立证明产品的来源，而仅仅只能是一种增信和辅助的工具。但毫无疑问的是，区块链技术的存在，零配件链上溯源体系的建立使得现阶段即便是造假也需要更高昂的成本，从而能够达到保证链上信息与实物基本相对应的目的，发挥防伪溯源的功效。

区块链 + 生物技术

（一）行业应用图景

在区块链工业化应用的完整生态中，生物信息识别是其中一个前景广阔、经济价值巨大的细分方向。目前来看，以区块链十生物识别的技术是否应用于人作为区分标准，可以将该技术的主要应用场景大致分成两类：一类是用于传统畜牧业、宠物行业的产品追踪 溯源，这类应用事实上也属于广义上的区块链十供应链应用的一部分；另一类则是应用于医学诊疗、基因生物技术研发、个人信息的采集、存储和验证等领域。

实际上，此两类应用场景存在较大的差别，第一类应用场景涉及的法律合规问题主要集中在区块链技术合规、数据合规等方面。第二类应用场景由于涉及生物数据安全、个人信息（特别是敏感信息）保护和科技伦理等多方面，需要视具体应用方式的不同，探寻在现行法律框架下的具体合规道路。另外，对于涉及人类基因研究的应用领域，尤其不能忽视伦理问题。

1.畜牧业

在当今时代，全行业信息化已经成为大势所趋，数据日益成为影响 生产力的关键生产要素，因此，实现农业信息化在某种意义上也是当前我国农业现代化的必经之路，是促进产业升级的关键。在互联网蓬勃发展的二十年里，畜牧业信息化已经初见成效，网络化管理已经成为当前畜牧业发展的常态，并在产品生产、物流运送、成本控制、互联网营销等当面发挥了巨大的效用。但是，对于畜牧养殖企业中心化的管理结构，保险、银行等金融机构难以对其完全信任尤其涉及投保业务时，养殖数据的真实性、有效性无法保障，成为当前制约畜牧业进一步发展的关键原因。如何让畜牧业进一步实现信息化、智能化、智慧化发展，也成为了我国畜牧业面临的现实问题。区块链技术由于具有去中心化、信任强化、分布式共识、不可篡改等特性，在结合生物识别技术的前提下，可以实现对畜牧资产的有效监管，以保障系统追溯数据的真实性及可用性。因此，利用区块链技术为畜牧业赋能，开拓出区块链十畜牧业的新型应用，打通畜牧业关键节点，保证从生产到流通再到消费的全流程信息透明可追溯，是畜牧业未来发展的必由之路。

在具体实现区块链 + 畜牧业的措施中主要需利用高速移动互联网、云计算和物联网等技术，依托部署在畜牧业生产现场的各种传感节点（养殖环境温湿度、氨气、二氧化碳浓度、通风量等）和无线通信网络，实现畜牧业生产环境的智能感知、智能预警、智能决策、智能分析，为畜牧业生产提供精准化养殖、可视化管理、智能化决策。以牛奶的智能化生产为例，区块链技术已经在部分地区被实际投入运用。当然，如前所述，区块链技术在实际运用中并不是孤立存在的，而是通过区块链和物联网、大数据在奶牛生产中的实践应用相互配合，才能保证牛奶的质量安全。

首先，在牛奶的智能化生产全流程中，需要对奶牛进行个体识别、体重测定、产奶性能、发情监测、精准饲喂、环境控制等各个环节的数据进行采集和分析。事实证明，在奶牛生产规模化、集约化达到了一定的水平后，物联网（IoT）和自动化技术在奶牛生产中可以起到更好的作用，大数据和人工智能可以很大程度上提升牧场的管理水平和经济效益。但是，仅仅依靠大数据和人工智能是不够的，一直以来，畜牧养殖资产监管系统数据采集源头设备的不可信，牲畜个体身份标识识别复杂，养殖敏感数据机密性差等问题都制约着生产力的进一步发展。

此时，区块链技术 + 生物识别就派上了用场，目前来看正是“破局”利器。上海海洋大学信息学院和国家农业信息化工程技术研究中心等研究机构的学者们提出了一种基于区块链技术和聚合签名算法的畜牧资产身份认证方案，以实现资产监管系统中，数据采集源头、数据存证展示的全流程真实可信，以及监管系统各节点、各物联网设备间身份验证的可信可溯，有效保障了畜牧资产监管系统从区块链网络到节点及物联网设备间细粒度的身份验证。同时，该系统由于具有高效的批量身份验证性能，可以满足畜牧资产监管过程中设备身份认证需求。最终实现监管系统数据全流程真实可信，区块链网络到节点及接入设备间的细粒度身份可信可溯，签名验证方便高效，构建了监管系统一体化的数据身份真实可溯，为畜牧行业金融发展提供有力支持。

2.宠物行业

区块链技术在宠物行业中的应用与畜牧业相似，但稍有不同。对于畜牧业来说，畜牧资产管理和农产品溯源是区块链的主要用武之地，而对于宠物行业来说，最重要的则是对宠物“血统纯正”的真实性进行验证，这就意味着区块链在宠物行业中主要发挥着与司法领域类似的“存证”功能。立足我国当前的宠物行业来看，相比欧美等国家已经发展出较为成熟的全产业链，中国宠物行业尚处于初级阶段，但同时由于近年来“萌经济”、“猫咪经济”的发展，我国已经形成了一个足够巨大的宠物市场，据国家统计局数据显示 2010 年到 2016 年，中国宠物行业年复合增长率达到 49.1%。2016 年，仅宠物犬、猫市场的行业规模就达到 1720 亿元。

庞大的市场与发展不成熟的产业链产生了矛盾，逐渐滋生出“好品牌难做”、“出了问题不仅难查原因且无人负责”、“星期猫星期狗”（即不良商贩卖出的存活时间短、有问题的不健康宠物）、“养宠学习成本高”、“医疗贵”等问题。另外，在宠物行业中，宠物个体血统的纯正性往往直接决定了其价值高低。但是，一直以来，国内外的宠物市场上都存在着大量以假充真、以次充好的现象，各类真真假假的证书大量充斥市场，这就使得宠物商家和消费者们往往只能通过宠物的外表特征，结合自身经验对其血统的纯正性做出主观判断，不少经验不足的消费者为此交了一大笔“学费”，甚至经验老到的宠物商人也不能保证自己的判断能准确无误。

2017 年 7 月，北京一女孩因喜爱猫咪，在激情消费等原因的促使下，前前后后共购买了 81 只纯血猫咪（甚至有不少赛级猫咪），导致自己欠款达到约 70 万元，在还贷的巨大压力下，她本想先出售几只“赛级猫”缓解经济压力，未料几万元买来的“名猫”在售卖时却只值几千元。原来，女孩遭到了不良宠物商贩的诈骗，其购买的所谓“纯血赛级猫”是以假充真、以次充好的猫咪，虽然很可爱但却难以挽回巨额经济损失。千亿规模的宠物行业遭受“信息”孤岛之困，是行业之殇。那么，区块链技术可以为宠物行业做什么？目前来看，主要可以实现以下两个功能：

(1) 实现宠物交易的可信

区块链存证可以有效保证宠物繁殖链的信息连续性，打造宠物专属生物档案，为每一只宠物打造独一无二的 ID，将宠物品种信息、遗传病史、健康状况、疫苗情况、体检情况、治疗情况、繁育数据等一一记录。

(2) 保证宠物终生信息透明

区块链对整个宠物行业上下游都具有重要意义。宠物从出生到殡葬的整个行业链条，都可以利用区块链数据不可篡改的优势，做到宠物全流程信息可溯源的透明状态下，任何一环节出问题都能落实到具体责任方，从而建立信任机制。

3.医疗诊断

医疗诊断是区块链十生物信息识别在第二类应用场景中的重要实践领域。同样是利用区块链技术的分布式存储、数据防篡改等特性，对患者病情、用药数据和医疗器械使用情况进行统一管理。

2020 年 9 月 27 日，国家卫生健康委员会办公厅发布了《关于加强全民健康信息标准化体系建设的意见》（国卫办规划发〔2020〕14 号）。意见指出，要推进互联网、大数据和区块链等新兴信息技术与卫生健康行业的创新融合发展，探索研究区块链在医疗健康领域应用场景。目前，医疗健康领域已经开始尝试将区块链技术实际应用到各个领域，取得了一定的成果。

但值得注意的是，此类应用与第一类应用具有显著的区别，医疗诊断由于涉及到患者病情信息及各类敏感隐私数据，区块链技术的应用在此方面既面临合规挑战，同时也需注意伦理道德风险，相较第一类应用来说复杂得多。具体而言，区块链技术在医疗诊断中得应用可以细分为以下几个方面：

(1) 患者敏感隐私数据保护

在医疗行业中，患者隐私保护一直是一个难以解决的痛点。我 们每个人在医疗机构接受诊断治疗的过程中会产生大量的隐私数据 这些数据长期以来在患者本人不知情的情况下会被用于科研、市场 营销等用途，隐私数据被滥用的现象严重，因此，对健康大数据的隐私保护及数据共享如何得到更好的平衡是亟待解决的关键问题。

区块链能为患者隐私保护做什么？在医疗领域，既要保证患者 数据对诊疗团队的透明、真实、可访问，又要保证对除诊疗团以外的人员的严格保密。利用区块链技术存储数据的不可篡改性和不可逆性，对信息、序列、时间等进行同时叠加记录，将数据在同一时间存储于不同的分中心，就可以实现数据的有效存储和不会被轻易篡改，保障了对患者敏感医疗数据的保密要求。同时，利用区块链技术将这些数据信息加密，只有区块链内部掌握密钥，并使只在特定区域内的人们才能接触到这些数据，就可以实现数据对诊疗团队的透明、真实、可访问。另外，由于患者的医疗数据信息可以被换算为哈希值进行上链存储，这就使得患者医疗数据的真实可信防篡改。

(2) 医疗健康数据流转与安全共享

在对患者的医疗数据进行验真后，另一个关键就是确保患者的医疗数据流转、可安全共享。在实践中，患者往往可能辗转不同的医院医疗机构寻求医疗救助，每每去到不同的医院或与医疗机构，医生都需要对其既往病史从头研究，并要求患者再次在本医院或医疗机构进行各项基础诊疗测试，以帮助作出足够准确的诊断结果。这种做法有一定的现实意义，毕竟患者的身体情况在不断的变化中，有必要对其当前的身体状况进行详细检查。但是从另外一个角度看，部分检测项目并非必须，重复检测为患者带来的身心压力、经济压力以及医疗资源的浪费是不必要的。据此，医疗健康数据流转与安全分享此时就具有重大意义。

当前，我国已经有部分学者，提出了具体的，基于区块链的医联体医疗健康数据流转与安全共享方案。具言之，首先。在达成共识的多个医

疗组织或机构之间构建多中心化的联盟链区块链（ 不可为公链 ），已被授权的组织或机构用户均可使用，在经过患者授权后，将患者医疗健康数据上传到区块链上。其次，将各级医院的医院信息系统 (HIS)、实验室信息管理系统 (LIS)、影像归档和通信系统 (PACS)、电子病历管理系统 (EMR) 以及一些其他临床系统分别部署在安全性高、可靠性高的不同的云服务器上，以保证医疗健康数据原始记录存储的安全性。经过患者授权后，存储在云平台中的各级医院患者的医疗健康数据的哈希值和存放地址上链，即存储到医联体医疗健康数据共享联盟链中。实现各级医院之间患者医疗健康数据传递的真实性。以此，尽量避免患者的重复检查，提高医生诊断的准确率，降低了患者的医疗成本。

(3) 医疗器械溯源监管

医疗器械溯源是指使用自动识别和计算机技术，对医疗器械的生产 物流、进销、使用等环节信息进行记追踪，该工作需要多方参与，同时服务于各个环节用户以及监管者。长久以来，由于医疗器械使 用不当、消毒措施不到位、重复使用或留置于患者体内等原因而产生的各种医疗事故比比皆是。作为直接或间接地用于人体的设备、器具、仪器，此类医疗事故的发生往往会对患者的健康产生严重的不良影响，甚至危及生命。根据国家药品监督管理局 2020 年发布的《国家医疗器械不良事件监测年度报告》2020 年，我国医疗器械不良事件监测信息系统共接收到医疗不良事件报告 53 万余份，与 2019 年相比显著增加 35．25%，每百万人口平均报告数已经达到了 402 例。可以说，医疗器械导致的医疗事故逐渐增加，医疗器械溯源工作对防范医疗事故发生、确定医疗事故责任等方面有着越来越重要的作用。

在医疗器械溯源监管方面同样也已经有了一些实践案例。上海理工大学健康科学与工程学院和上海健康医学院的谢亚平和王云光将区块链技术与医疗器械溯源相结合，提出基于 Fabric 区块链的医疗器械溯源监管系统，以解决传统医疗器械溯源系统中存在的信息记录不完整、数据中心化以及数据易篡改等问题。Fabric 系统具有 (1) 为记录的数据提供更细粒度的访问控制，从而增强隐私保护；(2) 溯源信息上链，多节点共同管理的分布式记账的管理模式；(3) 多方存储和异步查询保障信息安全；(4) 智能合约对恶意攻击者进行安全审计和监测管理。

(4) 传染病防治

疫情当下，流行病学调查 (以下简称“流调”) 逐渐成为一个为大众所熟知的词语。所谓流调是指用流行病学的方法对传染性疾病的传染路径、病毒传播链条进行的调查研究，主要用于研究疾病健康和卫生事件的分布及其决定因素。通过这些研究提出合理的预防保健对策和健康服务措施，并评价这些对策和措施的效果。当前《中华人民共和国传染病防治法》和《突发公共卫生事件应急条例均对流调作出了相应的规定。这体现出医疗大数据在重大传染病和新发突发传染病公共卫生能力建设方面的应用正逐渐走向成熟。

然而，传统的医疗大数据平台建设仍面临很多难题，信息孤岛依然在严重制约着医疗大数据在流调中的实际应用。集中表现为：(1) 医疗服务中的大量数据还未被充分利用；(2) 传染病领域的医疗大数据信息的安全性、准确性、及时性和覆盖面等有待提高。利用区块链的防篡改、分布式记账技术等解决医疗大数据领域的信息孤岛难题，助力传染病防治是一条可行的道路。

4.生物医学研究

很多人相信，21 世纪是生物医学的时代，与其他科研项目相比针对基因的研究是一项自微末观宏大的壮举，对人类理解自然规律探寻自身起源有着无与伦比的作用。

2022 年 3 月，据《科学》杂志网站报道，一个名为“端粒到端粒联盟”的科研团队首次完成人类全基因组测序壮举。为什么称其为“壮举”？原因在于人类全基因组测序是无数生物医学研究者多年未尝的夙愿，这项开始于 30 多年前，为人体 23 对染色体上脱氧核糖核酸 (DNA) 的基因全测序的研究，事实上在 2003 年已取得阶段性重大突破 — — 发布人类基因组图谱。但这份图谱只完成人类 92% 的基因组测序，剩下 8% 因为含有重复 DNA 片段，工作量巨大，以当时科研手段难以完成测序。10 年来，随着基因测序技术提高，研究人员得以补全最后 8% 的测序拼图，绘制出人类基因组完整图谱。据悉最后的完整图谱包括逾 30 亿碱基对序列和近 2 万个蛋白质编码基因。这些基因中，有约 2000 个基因为这次研究新发现。为人类进一步理解生命起源作出了划时代意义的贡献。同时，随着基因测序技术的进步，测序成本也从三十年前的数十亿美元下降到数千美元，甚至我国某著名基因大厂已经公开宣布当前基因测序仅需数百元即可实现。这样低的门槛使得普通人也有能力对自身基因进行测序，以了解自身身体情况、潜在的疾病风险并据此采取预防措施。

(1) 基因测序赋能

传统的基因数据共享模式是以基因组学公司为中心，用户需要向基因组学公司支付一定的费用并提供 DNA 样本，基因组学公司对 DNA 样本进行检测之后会得到基因数据以及一份基因分析报告，用户仅获得基因分析报告，而基因组学公司获取了被测序者的基因数据，并经常在未经被测序者许可，甚至在其不之情的情况下将基因 数据出售给其他研究机构、商业实体。这种行为：(1) 会导致基因数据垄断导致价格不合理；(2) 严重的个人隐私泄露。导致许多人抵触基因测序，严重阻碍了人类基因研究的发展。

区块链技术在解决基因数据所有权以及价值分配方面显出了卓越的成效。区块链本身具备的去中心化、数据不可篡改等特性可以与大数据、云计算、云存储等相结合的方法存储和应用基因数据，哈希算法可以实现高效的基因数据传输；另外，区块链技术对于帮助用户掌握自身基因数据、保护自身隐私、保障利益分配也具有显著作用。

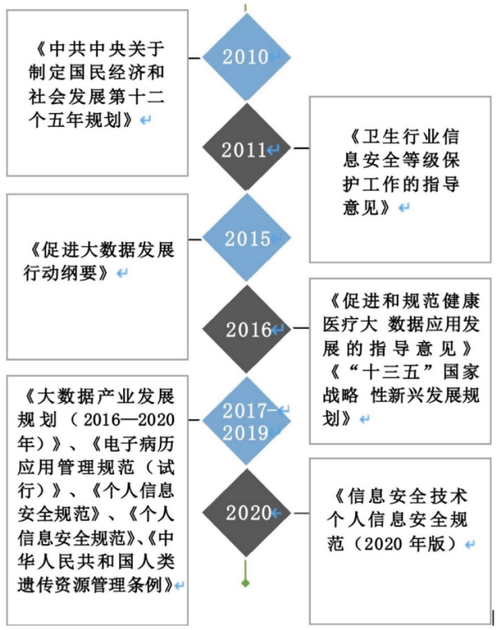
(2) 全球基因库建设

建立全球基因数据库事实上是一个有助于生物医学和基因技术 实现快速发展的极佳途径，对于科研人员来说，基因样本约大实验 结果更具有可信度，一些重大科研项目也有了进一步展开的可能。但是，全球基因库的建设存在重重阻碍，关键就在于基因数据不仅 具有巨大的经济价值，关乎个人的切身利益，也直接影响着各国生物医学科研水平的提升。在当前充满竞争的国际环境下，尚未有任何一个国家完全对外开放本国公民的基因数据库，更遑论建设一个全球基因数据库。

（二）行业法律风险

2010 年十七届五中全会通过的《中共中央关于制定国民经济和社会发展第十二个五年规划的建议》（以下简称《建议》）首次 提出健全卫生行业覆盖全行业的卫生信息网络，推动居民健康卡建设，加强信息化标准和信息安全体系建设。该方案是国家层面第一次在医疗卫生行业提出信息安全这个概念，填补了我国针对医院信息化建设中数据安全的研究空白。

“十二五”期间，随着我国信息产业的飞速发展，医疗卫生行业逐渐向信息化转型，医疗卫生领域的信息技术不断革新，积累了 丰富的医学数据资源，为“十三五”时期我国医学大数据产业的发展奠定了坚实基础。也是在这个背景下，我国根据各个时期的国情制定了不同的数据安全保护政策。（具体如下页图所示）



在区块链十生物技术的实践领域中，根据不同的应用场景会滋生不同的法律风险，具体而言比较集中于数据合规和生物安全两个部分 。

1.个人信息安全

对于前文探讨的第一类区块链十生物技术应用来说，由于不涉及或鲜少涉及生产者、运输者、消费者的个人数据，因此在个人信息保护方面，我们主要探讨的是在第二类应用中有可能出现的侵犯个人信息安全的现象。

谈及个人信息安全的法律风险，我们首先就要明白什么是个人信息？个人信息的分类有哪些？根据《个人信息保护法》第四条：个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。因此，在区块链十生物技术应用领域，特别是基因研究领域所涉及到的个人数据应如何收集、存储、使用、加工、传输、提供、公开、删除等是一个需着重考虑的问题。

在个人信息的分类方面，《个人信息保护法》以信息处理主体 所处理信息与个人联系的紧密程度、重要程度为区分标准，将个人信息划分为两类：(1) 一般个人信息和 (2) 敏感个人信息。根据《个人信息保护法》第二十八条：敏感个人信息是指一旦泄露或者 非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安 全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医 疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人 的个人信息。只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。目前针对一般个人信息，《个人信息保护法》围绕“告知 – 同意”原则构建，也就是说信息处理者处理个人信息的前提是取得个人的同意但在以下情形中除外：(1) 为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；(2) 为履行法定职责或者法定义务所必需；(3) 为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；(4) 为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；(5) 依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；(6) 法律、行政法规规定的其他情形。在处理个人信息的过程中还应当遵循信息采集最小化原则，避免过度收集个人信息，保障所收集的个人信息的质量和准确性，合法处理个人信息。

针对敏感个人信息，《个人信息保护法》建立了以“单独同意为原则的处理规则。由于敏感个人信息一旦泄露或者被非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害因此，法律对企业处理敏感个人信息时提出了更高的要求。具体而言，企业只有在：(1) 在具有特定的目的和充分的必要性；(2) 采取严格保护措施；(3) 向个人告知处理敏感个人信息的必要性以及对个人权益的影响的前提下，经单独同意才能利用区块链技术处理敏感个人信息。

2.医疗诊断领域

在区块链技术与医疗诊断相结合的应用场景中，由于涉及患者的个人信息较多、较敏感，因此对个人信息保护的要求很高。《个人信息保护法》第二十八条已经明确，医疗健康信息属于个人敏感信息，这就意味着在利用区块链技术对患者进行诊疗、病历记录、信息流转共享的过程中，需要额外对患者敏感个人信息进行保护。

事实上，在医疗健康领域患者被采集的个人信息不仅数量大，也是与其个人联系最紧密的，由于医师需要对患者病情的诊疗需要在进行大量医学检验的基础上才能作出，这就导致信息采集最小化原则由于难以把控，在医疗诊断的实践中难以切实实现，常常发生过度采集的问题。

另外就是患者医疗数据泄露问题，医疗保健行业在2020年已确认的数据泄露事件同比增加了58%。据360报告，该公司在疫情期间曾多次捕获到境外ATP组织对我国医疗机构的定向网络攻击。在医疗行业不断践行数字化转型之时，网络安全问题却为其带来了严重挑战。根据Verizon公司的统计，过去三年中，有超过93%的医疗保健组织曾经历数据泄露；而在疫情下的2020年，医疗保健行业已确认的数据泄露事件同比增加了58%。另外，根据CAICT中国信通院和腾讯安全联合发布的《2019健康医疗行业观测报告》数据，医疗行业总体处于“较大风险”级别，存在多种网络安全风险及大量可被利用的安全隐患，健康医疗行业存在大量应用服务(如数据库服务、FTP服务、打印机服务等)如果这些暴露的应用服务管理存在缺陷，那么攻击者从公共互联网会轻易地窃取到医疗相关数据区块链应用离不开大数据，在互相配合的过程中，数据合规建设具有重要意义，特别在个人信息保护领域，务必提起重视。

3.人类遗传资源保护

根据《人类遗传资源管理条例》和科技部发布的相关人类遗传审许可指南的规定，人类遗传资源包括人类遗传资源材料和人类遗传资源信息，其中人类遗传资源材料是指含有人体基因组、基因等遗 传物质的器官、组织、细胞等遗传材料，如全血、血清、血浆、尿液、粪便、血细胞、脑脊液、骨髓、骨髓涂片、血涂片、组织切片其他样本等；人类遗传资源信息是指利用人类遗传资源材料产生的数据等信息资料，主要包括：(1)临床数据，如人口学信息、一般实验室检查信息等；(2)影像数据，如B超、CT、PET-CT、核磁共振、X射线等；(3)生物标志物数据，如诊断性生物标志物监测性生物标志物、药效学/反应生物标志物、预测性生物标志物、预后生物标志物、安全性生物标志物、易感性/风险生物标志物；

(4)基因数据，如全基因组测序、外显子组测序、目标区域测序、人线粒体测序、全基因组甲基化测序、lncRNA测序、转录组测序单细胞转录组测序、smal1RNA测序等；(5)蛋白质数据；(6)代谢数据等。因此，此处涉及生物安全和涉及人的伦理安全审查问题，较为复杂，各类法律关系呈现相互交叉、交融的态势。人类样本库伦理要求明确“人类生物样本保藏的相关活动，主要包括了采集、收集、保存、分发、传输、使用和处理、共享、转让、结果发布、药物研发、国际合作等”。这些活动主要涉及数规相关问题外，还涉及生物安全和涉及人的伦理安全审查问题，较为复杂，各类法律关系呈现相互交叉、交融的态势。人类样本库伦理要求明确“人类生物样本保藏的相关活动，主要包括了采集、收集、保存、分发、传输、使用和处理、共享、转让、结果发布、药物研发、国际合作等”。这些活动主要涉及数据的交易和流动，主要收到我国《数据安全法》、《生物安全法》、《人类遗传资源管理条例》、《网络数据安全管理条例》(征求意见稿)和《关键信息基础设施安全保护条例》等法律法规的规制。特别是在《人类遗传资源管理条例》出台后，我国对人类遗传资源的出境与输入都采取了严格的监管措施，根据该条例第三十条规定：将在中国境内采集的中国人类遗传资源输出境应当报国务院科学技术行政主管部门批准。未经批准，任何组织和个人不得以任何形式将在中国境内采集的中国人类遗传资源输出境。

为了科学研究目的将在境外收集的人类遗传资源输入境的，应报国务院科学技术行政主管部门备案。违反该条例规定可能面临严重的行政处罚，构成犯罪的，还有可能被依法追究刑事责任。

4.伦理安全审查

基因技术的研究、应用和数据存储、流转都须有伦理审查作为“守门员”。特别是在涉及人类基因的各项研究和技术应用中，伦理审查也是非常重要的一方面，以防止基因技术研究者出现违背伦理道德，乃至违法犯罪的操作。数年前轰动一时的深圳某研究院非法基因编辑婴儿事件就是一个典型案例，已逾越了伦理的底线，涉嫌犯罪。

目前按照《中华人民共和国人类遗传资源管理条例》第九条规定：采集、保藏、利用、对外提供我国人类遗传资源，应当符合伦理原则，并按照国家有关规定进行伦理审查。由于我国基因技术起步较晚，伦理审查一直没有引起足够的重视，相应的在法律规范的制定层面和执行层面都出现了不少空白领域。

一直以来我国在基因领域的法律规范主要是由原卫生部和科技部制定的几个规范性文件和部门规章。其中部分内容涉及基因编辑的伦理审查，如《人类辅助生殖管理办法》中规定，人类辅助生殖技术的应用，应符合伦理原则；申请开展人类辅助生殖技术的医疗机构应设有医学伦理委员会；实施人类辅助生殖技术涉及伦理问题的，应提交医学伦理委员会讨论。关于人类基因编辑伦理审查的直接规范主要有《人胚胎干细胞研究伦理指导原则》《人类辅助生殖技术和人类精子库伦理原则》《涉及人的生物医学研究伦理审查办法》等。

第三章

区块链应用的合规对策

针对数据、信息安全的法律风险的合规对策

区块链应用不仅广泛，而且细分领域众多，但无论哪个领域都会涉及数据合规的问题。当前数据合规建设已经越来越成为决定企业发展的重要条件之一。现就数据合规要点和对策提示如下：

（一）数据采集

《个人信息保护法》规定，个人数据的采集以“知情–同意”为基本原则。所谓“告知”指的是个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：个人信息处理者的名称或者姓名和联系方；个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；个人行使本法规定权利的方式和程序；法律、行政法规规定应当告知的其他事项。个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。

“同意”指的是在个人充分知情的前提下自愿、明确表示同意。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。当然，基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

（二）数据存储

《网络安全法》《数据安全法》和《个人信息保护法》作为数据合规领域效力级别最高的三部法律，建立起了我国数据安全法律的基本框架，配合国务院出台的行政法规和部门规章、地方性法规为我国数字经济的发展奠定了基石。而数据存储一定程度上还有可能影响不同国家之间的科技发展水平，因此就显得尤为敏感和重要。

《网络安全法》和《数据安全法》主要聚焦于“关键信息基础设施服务提供者”的数据存储问题。根据《关键信息基础设施安全保护条例》第二条之规定，关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

《个人信息保护法》则专门将个人信息跨境提供的规则作为一个章节进行规定。根据《个人信息保护法》第四十条：关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的从其规定。那么，具体多少条应当本地储存，跨境流动需通过所在地省级网信部门向国家网信部门申报数据出境安全评估。根据《数据出境安全评估办法(征求意见稿)》第四条之规定，处理个人信息达到一百万人的个人信息处理者向境外提供个人信息；累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息。

如果区块链企业擅自将数据跨境传输或违反存储规定，就会存在非常大的行政违法风险，甚至有可能构成《中华人民共和国刑法第二百八十六条之一规定的【拒不履行信息网络安全管理义务罪】

（三）数据传输

目前除关键信息基础设施的数据传输受到重点关注外，个人信息处理者向其他个人信息处理者提供其处理的个人信息的也应当合法合规。根据《个人信息保护法》之规定，信息处理者在向其他个人信息处理者提供其处理的个人信息应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的处理方式的，应当依照本法规定重新取得个人同意。

另外，当涉及个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当向个人告知接收方的名称或者姓名和联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

（四）敏感个人信息处理

如前所述，敏感个人信息指的是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。由于敏感个人信息与个人关联的紧密性，只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。最关键的一点就在于：处理敏感个人信息应当取得个人的单独同意；处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

此外，在告知方面，除履行一般告知义务外，企业还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响；依照本法规定可以不向个人告知的除外。

（五）警惕生物研究领域禁止性规定

1.个人不得收集人类遗传资料

在我国，实行人类遗传资源材料收集与保藏单位资质审批制度未经批准，任何单位和个人不得收集与保藏中国人类遗传资源材料。

另外，任何组织和个人不得买卖或者变相买卖人类遗传资源材料从事人类遗传资源材料收集与保藏的单位应当具备下列条件：在中国境内依法成立的法人；收集与保藏人类遗传资源材料的目的明确、合法；具备收集与保藏人类遗传资源材料所需的场所、设施设备和稳定的经费支持；具备收集与保藏人类遗传资源材料所需的技术力量；设有符合规定的伦理委员会。经批准收集与保藏人类遗传资源材料的单位，应当每年还应当向省级人民政府科学技术行政主管部门提交收集与保藏工作情况报告。人类遗传资源材料的收集与保藏应当遵循自愿和知情同意原则。此外，征求意见稿还规定，经批准收集与保藏人类遗传资源的单位，应当按照资源提供者同意的目的利用其收集与保藏的人类遗传资源。在资源提供者同意的目的之外利用其遗传资源时，应再次取得资源提供者的同意。

2.单位需向提供者发放书面知情同意书

征求意见稿规定，从事人类遗传资源材料收集与保藏的单位在收集人类遗传资源材料前，应当向每位人类遗传资源材料提供者发放书面的知情同意书，内容包括收集目的、用途、对健康可能产生的危害、利益分享办法、保护个人隐私、自愿参与的选择权、可随时无条件退出的权利等。

征求意见稿指出，负责保藏人类遗传资源材料的单位应当制定人类遗传资源材料管理规范，建立保管制度、使用制度、监测登记制度、事故报告制度和应急预案，确保人类遗传资源材料的合法使 用。在收集、保藏和研究开发过程中，应完整记录并妥善保存遗传资源材料的来源信息。征求意见稿规定，未经批准，任何组织和个人不得以任何形式将在中国境内采集的中国人类遗传资源输出境。

针对技术固有的法律风险的合规对策

事实上，区块链技术固有的法律风险往往具有不可预测性和专业性，因此，要预防其技术固有的法律风险，必须得到专业人员的支持。因此，参与该链的各主体企业应当联合区块链技术的提供方由该区块链技术提供方派遣专业人员与各主体企业有关部门组建专业的技术风控小组，专门针对区块链技术种可能存在的法律风险和法律问题建立相应的制度和规范予以防范和解决。同时小组应当对其他从事相关业务的人员开展专业化培训，使其基本能够解决日常工作运营中所会遇见的常规问题，提高工作效率同时，为了保证培训的效果和制度的良好运作，小组还应成立监察组对相关情况进行不定期或定期监察，以确保制度发挥效果，防止可能发生的风险。

此外，为了确保链上的信息与实物一致，排除链上信息记录错误导致的一系列问题，各企业主体应当在关键节点对链上信息进行确认，以保证其记录事项与计划事项一致，排除记录错误的可能性，如发现确有错误，应当及时修正。在此过程中，如发现因错误而记录的信息属于个人信息的，应当及时联系有关主体，由双方协商解决问题，从而防止对企业带来负面影响，规避可能的风险。同时，针对前述可能发生的错误，建立适当的事后审查机制和惩处机制，对有关人员进行调查和惩处，尽力杜绝类似事件的发生。

针对实物与链上信息不匹配的法律风险的合规对策

为了解决此处的法律风险，确保链上的信息与实物一致，同样需要链上相关主体在关键节点对链上信息进行确认，但不同于第二点中的确认。第二点中的确认更多的是保证链上信息与产品所需要的信息相一致，换言之，是确保链上记录的零配件信息与产品上所写的信息相一致，即产品上写此处所用零配件应当是A型零配件，那么链上信息记录的应当也是A型零配件的信息。而此处的信息确认，是为了确保实物与链上信息一致，即链上信息是A型零配件，实物也应当是A型零配件。在此基础上，就能够达到实物信息与链上信息以及产品所需信息相匹配，解决信息不匹配的问题，保障防伪溯源功能能够正确运行。同样，这也需要建立的事后审查机制和惩处机制，对有关人员进行调查和惩处，尽力杜绝类似事件的发生。

而针对可能出现的以次充好的行为，各相关企业发现后可以根据链上信息逐步往前追溯，首先锁定可能做出该行为的企业，进而确认做出该行为的具体人员。各主体可以建立调查小组，共同调查该行为，通过获得的有关证据，逐步确认以下事实：其一，该行为实施的时间、地点；其二，行为人实施的动因；其三，行为人是否因此获益。以此来最终确认实施该行为的主体究竟是员工个人还是企业，从而确定不同的惩治措施，对前者由企业内部自行处理并将相关情报告知给有关企业，以警戒后续人员认真工作，对后者应当根据企业的具体情况采取对策，严重者可以考虑重新选择合作伙伴保证零配件链上溯源体系的健康良心运作。

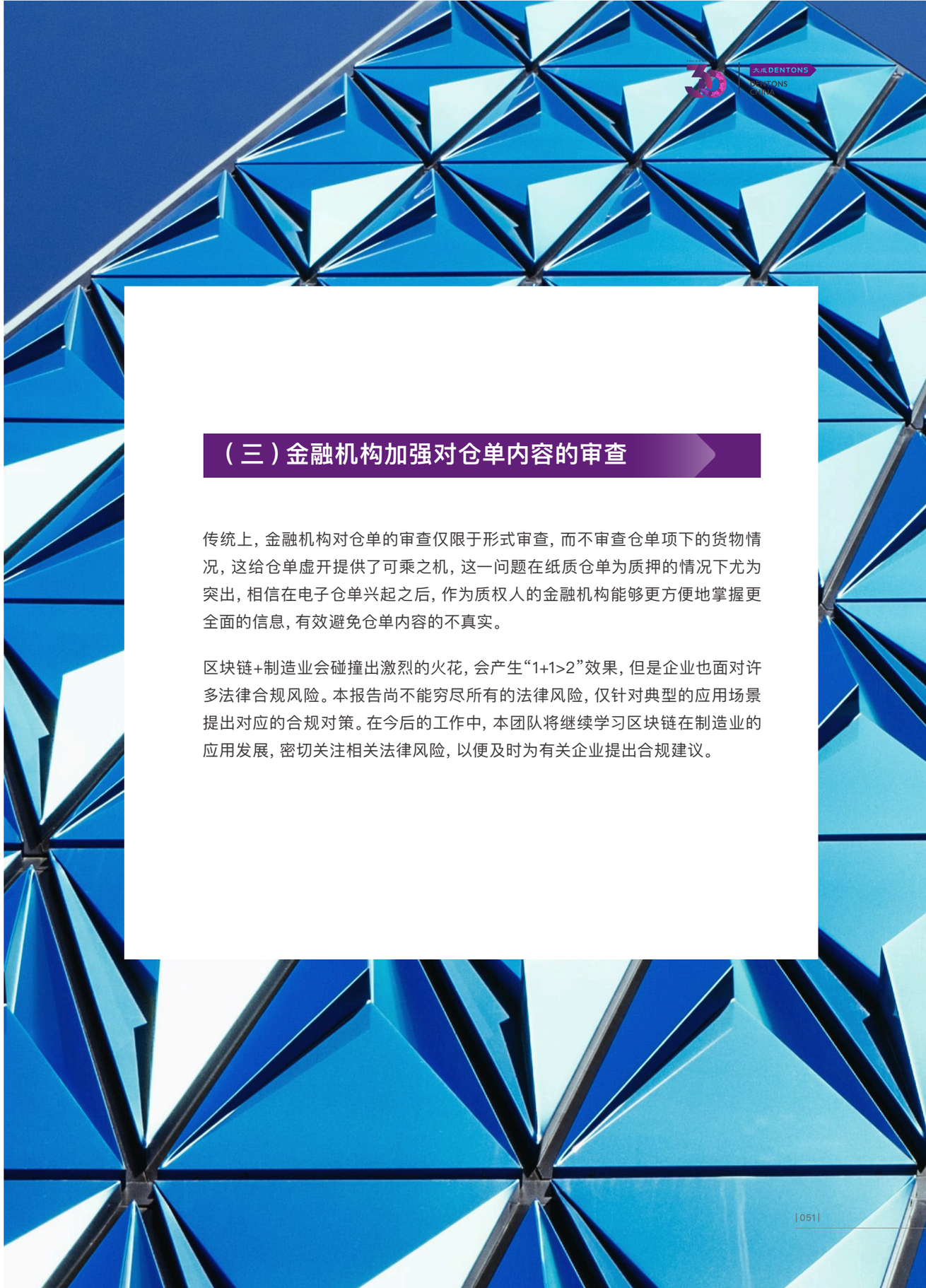
针对区块链电子仓单的法律风险的合规对策

（一）通过立法明确仓单质押登记机构及登记效力

为了解决仓单质押登记机构没有法律法规的授权、机构之间信息不互通、信息不公开的问题，应当首先在立法上赋予三大交易所做仓单质押登记的合法性，或在全国范围内设立专门机构，或指定某一机构作为仓单质押的合法登记部门，以解决登记机构的资质问题。

（二）建立全国统一 的电子仓单管理系统，制定行业标准

建立全国统一的电子仓单管理系统，制定统一的仓单质押规范。改变只有期货交易所会员可以查询登记信息的现状，让仓单质押设立登记信息公开化、透明化。同时，加强征信中心对三大交易所的监管，保证征信中心与三大交易所登记信息交流通畅。此外，还应当考虑引入非标准仓单公司的区块链技术和物联网数据，以提高电子仓单融资效率。



（三）金融机构加强对仓单内容的审查

传统上，金融机构对仓单的审查仅限于形式审查，而不审查仓单项下的货物情况，这给仓单虚开提供了可乘之机，这一问题在纸质仓单为质押的情况下尤为突出，相信在电子仓单兴起之后，作为质权人的金融机构能够更方便地掌握更全面的信息，有效避免仓单内容的不真实。

区块链+制造业会碰撞出激烈的火花，会产生“1+1>2”效果，但是企业也面对许多法律合规风险。本报告尚不能穷尽所有的法律风险，仅针对典型的应用场景提出对应的合规对策。在今后的工作中，本团队将继续学习区块链在制造业的应用发展，密切关注相关法律风险，以便及时为有关企业提出合规建议。

第四章

区块链监管展望及风控规划

监管展望

近年来，随着诸多规范性文件的出台，国内对于区块链的监管呈现出愈发严厉的趋势。2021 年十部委《关于进一步防范和处置虚拟货币交易炒作风险的通知》均明确指出区块链应用之一虚拟货币属于非法定货币，且将涉虚拟货币金融活动定性为非法金融活动。

但是，不同于被严厉禁止的代币发行融资行为，事实上，国家对区块链监管的态度从来不是严厉禁止，而是正向引导。从 2016 年 6 月 15 日中国互联网协会决定正式成立区块链研究工作组，从 2019 年国家互联网信息办公室发布的《区块链信息服务管理规定》到 2021 年《人民法院在线诉讼规则》所赋予的区块链证据的强证明力，以及现在各类关于区块链技术的应用研究中都能看出，在区块链技术上，国家希望能够正确运用区块链技术为社会作出贡献，而非采取完全禁止的形式排斥区块链的存在。

因此，在未来可预期的时间内，国家对区块链监管的总体态度仍然不会改变，依旧是正向引导为主。

风控规划

为了建立规范、有效的风控体系，服务团队现对后续风控体系初步规划如下：

（一）细化风控管理体系，推进风险最小化

各风控部门对各主体内部风控管理制度进行制定和定期修正，以适应发展过程中不断出现的新问题，同时建立诸如重大风险预警制度等有效制度对风控管理体系和风控流程进行进一步完善。

（二）加强司法政策学习，推动合规现代化

组织各主体有关人员进行有关法律、政策学习，及时更新有关区块链技术知识，了解最新的风险点，并积累风控管理经验，以提高有关人员的工作能力和综合素质。必要时可以安排各部门或各主体风控部门进行交流，以共同进步。

（三）落实部门岗位责任，促进风险范围明确化

定期收集有关风控的信息以及可能出现风险点的事项，对其进行风险评估，制作应对方案。

（四）建立部门沟通制度，防范部门风险隐蔽化

尽量降低区块链应用过程中可能给上述各体系带来的风险，并做好衔接工作，妥善划分各主体风控范围。完善有关风控事项的信 息披露制度。通过合理收集和处理以及披露有关风控事项，保障各主体和部门间合作顺畅，有利于发现风险点。

（五）完善企业监察制度，促使企业管理规范化

组建专门的监察部门对内部风控体系进行监察，通过定期监督与不定期抽查相结合的方式，对内部风控体系运行情况进行有效评估，以确保风控体系正确有效运行。

30th ANNIVERSARY 1992 2022

大成 DENTONS

DENTONS CHINA

大成律师事务所

微信扫描二维码
关注公众号

地址：北京市朝阳区朝阳门南大街10号
兆泰国际中心B座 16–21 层
邮编：100020
总机：+86 10 5813 7799
传真：+86 10 5813 7788
网站：www.dentons.com
邮箱：beijing@dentons.cn