合规区块链指引

（2017）

赣州市人民政府

国家计算机网络应急技术处理协调中心

新华网股份有限公司

2017 年 7 月

目 录

1 区块链概述

1.1区块链定义

目前，对于区块链还没有一个统一的定义。一般认为区块链是一种去中心、防篡改、防抵赖的分布式账本技术。维基百科将区块链定义为带有时间戳、先后相连的数据块存储数据的分布式数据库技术。工信部《中国区块链技术和应用发展白皮书》将区块链定义为一种分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。

本指引从六个方面来描述区块链。

- 整合：区块链是一种基于 P2P 网络、整合了密码学、共识算法、智能合约等关键技术的分布式账本技术。
- 融合：区块链是架构在通信网络之上的、能够与物联网、大数据、云计算、人工智能等进行深度融合的新一代信息技术。
- 特点：区块链具有三个方面的关键特点：多方维护、不可篡改、开放透明。
- 本质：区块链是缺乏信任或者弱信任的多人/多物之间，按照既定的共识规则，进行协作的系统。
- 应用：区块链的应用可以归纳为 3 个基本应用点：存证溯源、交易支付、数据索引。
- 效用：区块链的根本效用是在物理世界与虚拟空间之间架起了桥梁，构建全新的数字社会。

1.2区块链关键技术

1）P2P 网络技术

P2P 网络分为三种类型：第一代混合式 P2P 网络、第二代无结构 P2P 网络、第三代结构化 P2P 网络。区块链网络属于第三代 P2P 网络，具有去中心、高性价、健壮、保护隐私、负载均衡等特点。比特币系统之所以能够从 2009 年一直稳定运行到现在，与其采用了 P2P 网络技术密不可分。

2）分布式账本技术

区块链与传统数据库在存储方式和数据结构上存在不同。区块链采用混合模式的数据存储方式，首先按照时间间隔打包封装成数据块，然后同步到所有区块链网络节点，这种水平分割的全复制存储方式保证了数据的完整性和不可篡改性。区块链的结构分 3 层，首先是链，然后是区块，最后是交易，同周期中的交易组成区块，按时间顺序将区块连接起来形成区块链。这种存储方式和数据结构使得区块链与传统数据库不一样，只有增加和查询操作，没有修改和删除操作。

3）非对称加密技术

保证区块链安全的基础技术。该技术含有两个密钥：公钥和私钥，首先，系统按照某种密钥生成算法，将输入经过计算得出私钥，然后，采用另一个算法根据私钥生成公钥，公钥的生成过程不可逆。由于在现有的计算能力条件下难以通过公钥来穷举出私钥，因此可以认为是密码学安全的，从而能够保证区块链的数据安全。非对称加密技术在区块链中有两种用途：数据加密和数字签名。

4) 共识机制技术

区块链中的另一个基础技术。共识机制用来决定记账节点、并对交易信息进行确认和一致性同步。经典的共识机制有：1）POW：工作量证明（Proof of Work），它将解决计算困难问题所需要的计算代价作为新加入块的凭证和获得激励收益；2）POS：权益证明（Proof of Stake），它以权益证明代替工作量证明，由具有最高权益的节点实现新块加入和获得激励收益；3）DPOS：股份授权证明（Delegated Proof of Stake），它是 POS 的一个演化版本，首先通过 POS 选出代表，进而从代表中选出块生成者并获得收益。随着人们的不断研究，适应新需求的共识机制会不断的被提出。

5) 智能合约技术

智能合约在区块链 2.0 中得到长足发展，以以太坊为代表的区块链将智能合约的应用推向了更高水平。早前，尼克萨博（Nick Szabo）将智能合约定义为：一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。对于区块链中的智能合约可以从以下几点进行理解：1）由一段脚本或者代码来实现其业务逻辑；2）能够被注入到区块链的执行环境中执行；3）具有图灵完备性；4）事件驱动；5）具有状态。

1.3区块链分类

按照区块链应用的用户范围与许可方式，可以将区块链分为三类：公有区块链、联盟区块链、私有区块链。

1) 公有区块链。

公有区块链上的数据所有人都可以访问，所有人都可以发出交易等待被写入区块链。共识过程的参与者通过密码学技术以及内建的经济激励维护数据库的安全。公有区块链是完全的分布式。

2）联盟区块链。

联盟区块链的节点是联盟成员商定选择的，节点间可以有很好的网络连接。这样的区块链上可以采用非工作量证明的其他共识算法，比如有 100 家金融机构之间建立了某个区块链，规定必须 67 个以上的机构同意才算达成共识。

3）私有区块链。

私有区块链一般在一个企业内部或者机构内部使用，参与的节点只有内部用户自己，数据的访问和使用有严格的权限管理。

1.4区块链应用场景

区块链的应用前景非常广阔，除了数字货币，区块链在金融领域还可以有很多其他应用方式，在非金融领域则有更大的潜在应用空间。

1）金融

区块链技术的可靠性、实时性、容错性、不易出错性、追溯性可以在金融领域得到很好的利用，甚至可以重构金融业务秩序。具体的金融业务应用有：交易支付（特别是跨境支付）、资产数字化、智能证券、清结算、客户识别等。

2）供应链

传统的供应链上原料采购、生产加工、仓储物流、分销零售等各

个节点相互独立，不能够有效的链接在一起，区块链能够将这些相互独立的节点链接起来，形成完整的链条，促进供应链的健康发展。

3）文化娱乐

文娱产品存在多方面的问题，如：版权登记、交易流通、侵权公证等。采用区块链技术搭建一个平台，将文娱产业各种角色纳入服务范围，可以有效提升产业发展速率，塑造领域公正发展环境，并最终让老百姓受益。

4）智能制造

将区块链技术应用到工业互联网领域，既是领域的需求，也是区块链的特性决定。智能制造是工业互联网的方向，通过区块链技术将智能制造中的各个环节链接起来，从订单、设计到生产、发货等一连串的业务可以很好的衔接和优化的安排，从而达到节省成本，提高效益的作用。

5）社会公益

由于种种原因，公益事业推进非常困难，甚至形象大减，主要是由于公益事业中，缺少透明、难以跟踪。采用区块链技术可以将公益的资金来源、项目选择、项目实施、效果反馈等情况，清楚明白记录到链上，供社会查询监督。

6）其他

区块链还可以在教育、就业、食品、旅游、票据、游戏、存证、保险、资产、登记等多个领域获得应用。

2 合规区块链的必要性

2.1从金融科技到监管科技

根据金融稳定理事会的定义，金融科技（FinTech）是指技术带动的金融创新，它能创造新的业务模式、应用、流程或产品，从而对金融市场、金融机构或金融服务的提供方式造成重大影响。互联网金融是金融科技 1.0 阶段，现在金融科技逐步进入 2.0 阶段，并逐步呈现出四个重要特征，即跨界化、去中介化、去中心化和自伺服功能，这些特征将对金融体系产生深远的影响。从业务领域看，目前对金融市场影响较大的金融科技已经形成四大领域：1）支付清算。包含手机和网络支付、电子货币以及区块链;2）囊括直接融资、间接融资在内的融资模式。包括众筹、P2P 网贷、电子货币、区块链等;3）基础设施。包含电子聚合器、智慧合同、大数据、云计算、电子身份认证;4）投资管理。包含机器人投资顾问、电子自动交易、智慧合同。

伴随着金融科技的发展，监管科技（RegTech）也得到了长足的发展，这是与金融科技发展的规律有着很大的关系。由于金融科技更加隐蔽快捷、更加直接、更加依赖技术和数据、使得金融科技领域存在着比较大的风险。同时，金融科技在服务于实体经济的过程中，对监管科技也存在一些内在需求，FinTech 需要在监管的引导下，通过真正意义上的金融创新，来弥补传统金融的不足，以提高落后地区金融的可达性来促进金融的普惠性，以提高资金的配置效率来促进实体经济的发展。只有在监管的引导下，才能使区块链、大数据、云计算和人工智能等技术真正用于服务实体经济，而不是进行监管套利。再次，

FinTech 还可能涉及到的消费者隐私保护的问题，FinTech 的创新，必须是负责任的创新，这需要监管当局牢固树立金融消费者保护的监管原则，探索多种监管方式与手段保护金融消费者。

2.2区块链技术与应用的发展现状

目前，主流观点认为区块链技术的发展可以分为三个阶段：区块链 1.0、2.0、以及 3.0。区块链 1.0 对应的应用主要是比特币等虚拟货币，这方面的应用和货币有关，例如货币转移、汇兑和支付系统等。区块链 2.0 对应的是智能合约，这方面的应用主要在金融领域，但其可延伸范围比简单的货币转移要宽广，可以涵盖例如股权、债券、信贷等。区块链 3.0 则对应的是货币、金融市场以外的应用，如医疗健康、知识产权、物联网、社会管理、慈善公益等。纵观区块链的发展情况，有如下几点现状或者趋势。

- 投融资活动明显加速，ICO 疯狂上市，热点不断，冷静不足，急需监管。
- “链圈”区块链应用开始铺开，涉及政务、商务、民用各个领域，但尤以企业应用发展最快。
- 国内以北京、上杭、广深为中心，逐渐向全国各地发展起来，区域区块链产业发展正强劲展开。
- 协会联盟纷纷成立，赛事活动接踵而来，有关区块链的活动接二连三的举办。
- BaaS、云节点将成为区块链网络的基本形态。
- 物联网将大大扩大区块链的应用范围，未来的交易不仅仅是发

生在人与人之间，还会发生在物与物之间以及人与物之间。

- 身份链、大数据链将成为基础区块链。
- 区块链与人工智能结合，将使得区块链的应用走向更高层次。
- 跨链交易、多链交互将成为区块链互通的必然要求，区块链互联网悄然形成。
- 专利布局已成为区块链创新机构的重要竞争力形成举措。
- 区块链领域的创新层出不穷，监管的需求已经提上日程，合规区块链指引将为区块链产业健康发展起到重要作用。

2.3区块链技术与应用的重要问题

目前区块链相关行业缺乏自律，违规操作多，相关业务存在诸多问题，威胁用户资金安全、国家金融秩序和社会稳定。企业不公开不透明情况广泛存在，部分企业违规开展融资融币、理财等业务，利用信息不对称大量炒作诱导投资者。同时，大量山寨虚拟币浑水摸鱼，部分企业打着区块链技术和虚拟数字货币的幌子开展传销、诈骗、非法集资等违法犯罪活动。部分数字货币交易平台对上线交易的币种审核不严，信息披露不充分甚至不披露。不严格执行身份认证和反洗钱规定，为违法犯罪活动提供便利。归纳起来，区块链的技术与应用存在如下几个方面的重要问题。

1）身份问题

区块链的一个特性就是匿名性，该特性为区块链的应用，特别是公有链的应用起到了很大的作用，然而，因为匿名性，一些不法行为也借此在区块链上得以实施发展。有必要对区块链上的身份进行有限

的识别，一旦发现违法行为，能够快速的进行查证。目前，有些区块链平台采用了实名制的方式来解决这个问题，将实名账号与区块链地址进行映射绑定，区块链上的业务依然采用匿名，但可以通过映射关系来查证实际的用户。例如，在对数字货币进行监管的时候，就采用黑白灰名单的方式，来记录账号对应关系，从而为监管提供必要支撑。

2）性能问题

比特币的交易速率为平均 7 笔/秒，这个速度远远不能满足现实生活的需要。为了扩大区块链的应用，需要从理论和实践上加大对区块链性能的研究。在金融支付领域、防伪溯源领域、数据存证领域等等，均存在高并发访问计算的需求，有的甚至要求达到几万笔/秒的速率。当前，已经有一些区块链研究团队提出了一些提升性能的解决方案。

3）安全问题

相对于传统中心化系统，区块链在安全方面有一些优势特点，但并不是绝对安全，甚至存在一些相比较中心化系统的不足。首先，密钥安全就是区块链中的一个重要安全因素，不同的密钥管理办法只能适应一定的应用场景。例如，对于一些公有链，密钥由用户自行保管，但是，一旦发生丢失或者遗忘，则会为用户带来资产损失。其次，数据安全也是一种重要方面。区块链采用密码学技术进行数据的传输和存储，如果采用的是级别比较低的密码技术，则容易被破解造成数据泄露。再次，由于区块链的公开透明，区块上记录的数据对所有用户开放，如果数据不经加密直接记录，则对用户隐私造成威胁。

4）监管问题

随着区块链技术越来越多的应用于各个领域，特别是金融领域，其作用得到了更大的发挥。然而，同许多其他技术一样，区块链技术本身是中性的，它是否真正为社会带来积极的作用，取决于使用该技术的人以及使用方式。金融科技方面的创新已经对我们的社会产生了很大的影响，其中不乏消极方面的影响，例如 P2P 领域的“e 租宝”等事件。作为金融科技中的重要技术，区块链技术同样也可以在监管科技中得到重点使用。对于区块链的监管主要包括三个方面：1）主体监管，也就是对区块链的运营主体的监管；2）平台监管，就是对区块链平台系统的监管；3）业务监管，即对区块链平台上的业务参与者、业务本身、业务涉及对象的监管。

5）互通问题

越来越多的区块链得以上线运行，每一条区块链存在很多方面的不同，例如：数据格式、共识机制、密码算法、业务形态、合约机制、区块链大小与周期等等。这么多的区块链独立运行，互不影响，然后，实际需求是希望不同区块链之间能够进行必要的交互，从而实现更多的业务需求，更好的提供服务功能。当前，学术界产业界，均开始考虑这个问题，一个可行的办法就是在不同的区块链之间提供接口，还有一种办法就是尽快起草标准并统一遵守，为多链交互提供基础。

3 合规区块链指引

作为一种新兴的技术，区块链技术本身是中性的，如果区块链技术的某些不足被利用起来从事非法活动，则对社会将产生很大的伤害，因此有必要对区块链的合规性进行研究和规范，以便于发挥区块

链的积极作用，规避区块链的消极作用。

本指引从三个方面对区块链的合规性进行研究和规范。一是在技术层面规范区块链规范区块链关键底层技术，作为区块链系统安全、稳定和可靠运行的基石；二是在业务应用层面规范区块链相关业务开展，防范潜在风险；三实在监管层面，探索基于区块链的监管科技，提升监管能力。

3.1合规区块链技术指引

3.1.1密码机制

区块链是建立在密码学基础之上的技术，密码机制的合规直接决定了区块链的技术合规。

- 密码标准：能够按照不同业务需求和当地法规要求采用不同的合规的密码标准。例如：在中国，大部分要求必须采用国密标准，而对于一些国际化区块链，还需要支持更多的密码标准。
- 密码模块：由于可能采用不同的密码标准，需要支持密码算法的灵活切换。

3.1.2访问控制

访问控制对于区块链的大范围应用起到非常重要的作用，是人们放心使用区块链的重要考虑点。

- 机制：能够根据不同的业务需求及技术条件选择合适的访问控制机制。
- 一致：不管采用何种访问控制机制，都需要做到一致性，即授权与鉴权的一致性，不能留有授权漏洞和鉴权偏差。

- 效率：不管采用何种访问控制机制，都需要考虑到效率，包括授权效率和鉴权效率，不因访问控制而对业务的效率产生较大的影响。

3.1.3密钥管理

从用户使用角度来看，密钥管理直接决定了用户数据的安全，现实中，需要综合考虑安全与效率因素，为用户提供合适的密钥管理方法。

- 密钥机制：能够根据不同的业务需求及技术条件选择合适的密钥管理机制。例如：KPI 机制、代理机制。
- 密钥保管：能够根据不同的业务需求及技术条件选择合适的密钥保管方式。例如：自我保管方式、托管方式。根据需要，提供密钥恢复、重置机制。
- 密钥效用：能够灵活准确的生成密钥，并能保证密钥的时间、空间等各中条件下的效用属性。

3.1.4共识机制

共识机制是区块链的基础技术，共识机制的表现直接决定了该区块链是否合理。

- 公平公正：共识机制首先要保证公平公正，不存在任何后门以便特殊人员为了特殊目的干扰共识机制的达成逻辑，从而形成有利于特定人员的共识结论。
- 不可预测：共识机制必须要做到不可预测，避免出现因为可以预测而被恶意利用或者攻击，从而形成有损区块链用户的不公正

结果。

- 高效稳定：共识机制必须稳定可靠，必须能够终止，同时还需要能够尽量快速的达成共识，以适应各种不同的业务需求，提高业务的处理效率。

3.1.5数据处理

数据处理是区块链得以支持业务的重要功能，数据处理的表现直接决定了业务的表现。

- 正确完整：区块链及对接平台上的数据处理、传输、存储要做到正确完整，不能有任何错误，也不能丢失任何数据，通过数据获取接口能够获取正确完整的数据。
- 快速高效：区块链的链上链下数据均需要能够进行快速高效的处理。例如：在数据传输的时候，选择最优路径，以便以最快的速度传送到目标节点。
- 安全可靠：数据在处理、传输、存储中，都需要保证数据的安全可靠，不能丢失破坏数据，也不能泄露数据，保证数据在正确的条件下，被正确的主体以正确的方式进行处理。

3.1.6智能合约

智能合约是区块链得以更加广泛应用的技术，其创建、检测、上链、运行都关系到区块链的表现。

- 完备性：智能合约首先要符合图灵完备。
- 一致性：智能合约在相同的条件下，执行的结果应该是一致的，不允许智能合约产生二义性。

- 强制性：智能合约具有法律效应，针对合约约定的条件和事项，智能合约能够强制执行，不受人为干扰。
- 保密性：智能合约记录了合约方的一些秘密信息，不能对外泄露，因此必须保证智能合约的保密性。

3.1.7互联互通

一条封闭的区块链，其作用比较有限，技术发展和现实要求，必须考虑多链关联的情况，保证多链融合下技术的合规。

- 多链架构：区块链平台支持多链架构，包括多链交互和跨链交易，对于将来同其他厂商的区块链的对接，也要留出预备接口或者扩展点。
- 业务整合：区块链还需要能够与传统 IT 系统进行整合，通过充分发挥区块链和传统 IT 系统各自的优势，达到业务快速安全整合的目标。

3.1.8系统运维

系统运维是区块链得以健康运行的保障，系统运维必须保证在合规的限制下进行。

- 程序升级：针对已经运行的区块链平台，提供平滑兼容的程序升级功能，并能够在升级不成功的时候，统一回退正常运行。
- 系统配置：提供全局和本地的系统配置功能，以便各个区块链网络节点能够按照一致的配置进行运行。
- 节点管理：能够对全网区块链节点进行管理，能够按照既定的规则进行节点的加入、退出、限制的操作。

- 运营监控：对区块链网络进行系统和业务上的监控，发现问题并在权限许可范围内对区块链平台进行必要的控制，例如：当发现有人在利用区块链从事非法活动，就可以启动冻结节点和账号，跟踪业务流的程序。

3.2合规区块链应用指引

3.2.1信息公开

目前围绕区块链的业务开展缺乏规范信息披露的法规文件，且区块链技术概念较新，普通用户无法轻易理解，导致信息披露不足、不实以及诱导甚至欺骗投资者等事件频发，严重影响行业的健康有序发展。

- 信息披露真实性，信息披露义务人所公开的信息必须与真实情况相符，不得弄虚作假，不得诱导和欺骗用户。在实践中，部分企业伪造企业背景、资质以及产品的应用场景以吸引投资者，部分企业伪造交易量等信息欺骗投资者。
- 信息披露准确性，披露的信息应尽可能具体、准确，采用便于理解的方式披露，尽量达到普通用户可理解的程度，使用户准确了解所选择的业务对象，不得有意使用过度专业化的表达。
- 信息披露完整性，应保证信息披露的充分性，使用户尽可能全面地了解所选择的业务对象。不得有意隐瞒或遗漏，不得刻意回避对自身不利的信息。实践中存在大量信息披露不完整的情况，例如部分数字资产交易平台对上线交易的币种信息、主体信息完全不披露。

- 信息披露及时性，当源信息发生变化时，应及时更改和补充
- 信息披露的内容应至少包括运营主体工商信息、高管等主要人员信息、币种信息、相关源码、技术路线、业务模式等。

3.2.2身份管理

互联网具有虚拟属性，网络身份的确认、信用风险、交易欺诈、洗钱等一系列问题，都是源于网络的虚拟化而带来的信任问题。尤其是区块链技术特有的匿名性，进一步加强了这种虚拟性。一方面，一旦出现遗忘账号、系统故障等情况，没有实名认证的账号就很难挽回损失。同时，匿名账号为洗钱、套现、欺诈或违法交易提供了便利。包括：

- 用户认证：能够按照不同业务需求采用不同等级的实名认证，建立完善的网络身份认证体系和客户身份识别制度，不得为身份不明的用户开设账户或提供相关金融服务，如发现用户身份证件或资料造假，应拒绝办理。例如，一般的业务系统可以只需要关联手机号码的用户认证，安全性要求比较高的就需要身份证加活体认证。
- 用户管理：能够按照不同业务需求采取不同的用户管理方式。例如：用户自由加入退出、用户受控加入退出、强行注销冻结用户等。
- 用户隐私：能够按照不同业务需求采取不同的用户隐私保护方式。例如：有些业务需要某些用户必须对外公示，满足社会的知情权，而有些业务则需要考虑用户的隐私，避免暴露用户信息。

3.2.3投资者保护

围绕数字货币的产生、存储、交易、应用等形成了产业生态，并发展形成了大量的衍生业务。由于监管、规范等不到位，且行业缺乏自律，违规操作多，相关业务存在诸多问题，威胁用户资金安全、国家金融秩序和社会稳定。

- 不得利用区块链技术、数字货币等开展传销、诈骗、非法集资等活动。
- 数字货币交易平台应对上线交易的币种严格审查，不得上线涉嫌传销、诈骗、非法集资等非法犯罪行为的币种。
- 不得利用信息不对称恶意炒作，不得煽动市场情绪。
- 不得采用诱导性宣传，应进行充分的风险提示，完善投资者保护。

3.2.4反洗钱

区块链系统与传统金融交易系统在交易模式、身份验证、存储结构方面都有着本质区别。由于去中心化和匿名化的特点，虚拟货币网络没有中央控制点的概念，交易者的身份信息被隐藏，且可全网流通，不受国界限制，为犯罪资金转移、洗钱等行为提供了便利。

- 相关企业应严格执行国家有关反洗钱的法律法规以及中国人民银行等部门的有关规定，制定和完善反洗钱制度和操作流程，将反洗钱工作落实到日常业务运作中。
- 建立健全反洗钱制度体系，包括但不限于客户身份识别、大额交易和可疑交易上报、客户身份资料和交易记录留存等。

- 根据行业特征和业务类型等，建立洗钱风险评估指标体系和大数据分析系统，识别和发现可疑交易。
- 行业内不同企业之间应建立适当数据共享机制，通过大数据分析识别、发现并上报可疑行为。
- 应配合国家有关部门对涉嫌洗钱活动所进行的调查工作。

3.2.5监管对接

为了保障区块链平台的正常合法运行，区块链平台需要自觉支持监管需求，遵照相关要求对接监管机构的系统。

- 监管功能：能够按照监管要求，提供监管功能，方便区块链运营者和管理者实时把握区块链网络状态，实施权限允许范围内的监控操作。
- 监管接入：能够对外提供监管接入接口，向上提供监管信息，以便从更高层次审视区块链的健康程度。
- 监管记录：对于监管，除了要求必须有具备监管权限的主体来实施，同时，对于日常的监管，能够自动记录，方便后续分析挖掘。

3.2.6网络信息安全

网络与信息安全是业务持续稳定发展的重要基础，应按照“谁运营，谁负责”的原则建立网络与信息安全责任制，通过技术手段和管理制定，维护系统的可靠稳定运行，确保业务的连续性和可靠性，保证客户信息的安全。

- 遵从相关管理规定和技术标准，实现相应的网络信息安全防护

能力。

- 建立健全信息安全管理体系，包括机构设置、人员分工、规章制度等。
- 完善安全保障措施，包括网络运维、数据安全、信息安全等相关措施。
- 定期开展网络信息安全风险评估，预警和防范内外部风险。
- 完善应急预案和应急响应措施，保障业务连续性。

3.2.7数据存证

所有应用，不管是区块链平台应用，还是传统平台的应用，其底层均是对数据进行操作，在这些操作中所产生的数据存在需要第三方进行公证的需求，以此来保护平台、用户的数据权益。以区块链技术来构建数据存证平台，有利于这一需求的实现。

- 主体数据存证：这里的主体指的是与平台系统相关的各种主体，包括平台的创建运营主体、平台的使用单位和用户、平台的监管单位等等，将这些主体必要信息进行存证。
- 业务数据存证：针对平台上运行的业务进行存证，可以不用涉及具体业务信息，采用密码学技术来实施业务数据的存证，起到既有存证数据，又不会干涉暴露业务隐私。
- 数据保全公证：对数据进行存证，其目的就是为了对外提供保全公证的服务，采用区块链技术来保全各类数据，借助区块链的特点来提供权威的公证服务。

3.3 合规区块链管理指引

3.3.1互联网金融监管

互联网金融的表现形式多种多样，由于其技术先进性和监管滞后的特点，近年来，互联网金融领域出现了一些不和谐的现象，个别事件严重影响到社会稳定。采用区块链技术可以从包括但不限于如下几个方面对互联网金融进行合适、必要的监管。

- 信息披露：包括互金平台、互金平台运营者、互金平台用户等方面的信息披露并记录到区块链上。
- 存证溯源：针对互金平台的各种业务，采用区块链技术进行存证，确保业务安全可监管的运转。
- 主体监管：对平台的各参与主体进行监管，包括平台、创建者、运营者、用户、产品等，并将这些信息记录到区块链上以备查证。
- 资金动向：对平台上的资金动向进行监管，特别是出入境的资金动向，减少用户通过平台来从事洗钱等非法业务，所有监管记录上链，以作公证证据。

3.3.2数字货币、ICO监管

随着比特币、以太币在全球范围内的流转，各路资金纷纷加入追逐行列，这也给各种 ICO 以极大的鼓励，纷纷包装上线，发行自己的代币。相比较其他融资方式，目前的 ICO 具有简单快捷、成本低廉等特点，成为资本市场上一种不可低估的金融模式。虽然有不少领域行家，能够分辨优劣，但更多的是跟风炒作，其中的风险难以估量，一旦出现问题，其损失难以评估、责任不好界定，P2P 中曾经发生的故

事有可能重演。采用区块链技术可以从包括但不限于以下几个方面对数字货币、ICO 进行合适、必要的监管。

- 监管对接：将各数字货币、ICO 代币的交易平台接入监管中心的监管平台，并用区块链进行记录。
- 黑白名单：面向境内所有数字货币、ICO 代币的交易平台，设立黑白名单机制，汇总多方数据进行比对验证，并记录到区块链上供各平台和社会查询验证使用。
- 主体监管：对数字货币和 ICO 代币交易平台、发行方、主要负责人等进行严密监管，特别是对其境外活动动向进行跟踪监管，严防“跑路”情况出现。
- 资金监管：加大对资金动向的跟踪与监管，特别是针对大额资金动向、汇出境外的资金动向进行监管，防止利用数字货币、ICO 代币的特点进行非法资产转移的情况出现。
- 信息公开：所有监管结果，只要不涉及法律问题，均需要上链公示，既是对相关方的一种约束，也是对公众的一种告知，在公开的环境下达到公平公正的目标。

3.3.3供应链金融监管

供应链金融是金融领域和供应链领域非常重要的业务形态，基于区块链构建的供应链金融平台，能够将原本分散断链的各个供应链环节串联起来，形成连续的业务和监管模式。采用区块链技术可以从包括但不限于以下几个方面对供应链金融进行监管。

- 监管环节：对供应链各个环节，包括原材料、生产加工、仓储

物流、分销零售、应用消费等，均需要进行监管，如此才能做到全面不遗漏。

- 监管对象：重要是对供应链中的商品流、资金流、信息流进行监管，这里的资金流包括实际的法币，也可以是各种代币，除此外，还要对用户、凭据等进行监管。
- 监管方式：如果供应链金融平台直接就是基于区块链技术构建，则其监管可以采用设立监管节点的方式来实施，如果采用的是传统的技术构建，则需要进行监管对接，用区块链来记录监管信息。

3.3.4食品安全监管

食品安全一直以来都是政府和民众关心的问题，各种措施、系统纷纷得以采用，但效果依然不能达到人民的期望，主要表现在食品的生产、运输、销售等环节的追踪溯源与防伪方面做得还不够好。采用区块链技术可以从包括但不限于以下几个方面对食品安全进行监管。

- 责任人监管：保障食品安全的一个抓手就是明确到责任人，在食品相关的各个环节，均关联明确的责任人，通过对责任人的监管来保证食品的安全，这些信息都要上链，便于查询。
- 原产地监管：原产地是食品安全的源头，源头的安全状况对后续所有环节都产生影响，通过将原产地及生产状况信息上链记录，可以找到食品的根源，
- 流转监管：食品流转中的各个环节，均存在作假串货的可能，以区块链记录流转过程，则为食品提供了一个连贯的溯源链，食

品流转情况再链上一目了然，且不可更改，即使作假也是留下了证据。

- 认证监管：人们对食品以及食品的生产加工企业难以辨别优劣，需要引入一些检测认证机构，通过对食品本身以及食品企业的认证检测，并记录入链来起到公示作用，作为民众选择食品的参考，同时也是食品行业自律的保证。
- 防伪监管：通过采用传统防伪技术与区块链的融合，提升食品防伪的技术能力和应用效率，采用区块链首先是对防伪技术的记录，然后是对防伪技术应用运营情况记录，消除因传统防伪验证系统的原因导致防伪失效的问题。

3.3.5版权保护监管

版权保护一直是 IP 及相似领域的重要课题，传统版权保护依赖于中心化权威机构，在普适性和效率方面均存在不足，相比较社会对版权保护的需求还有很大的差距。采用区块链技术可以从包括但不限于以下几个方面对版权进行监管。

- 版权登记监管：版权登记是监管的源头，将版权登记到区块链上可以保证登记的效率和公证，采用区块链技术，在版权登记的时候进行监管，有利于维护版权登记源头的合规性。
- 版权托管监管：一些类型的版权的原始对象，除了自己保管之外，还存在托管的需求，这就要求将托管也纳入监管，通过区块链记录托管相关信息，保障版权所有人的相关权益和数据安全。
- 版权交易监管：版权交易是版权需求人取得版权使用权的渠

道，版权交易需要得到公证，通过区块链可以记录交易信息，从而为版权的传递提供公证。

- 版权使用监管：版权的使用是版权保护的重要阶段，盗版、未授权使用时有发生，版权使用的监管主要是记录证据、提供证据，通过对版权使用信息的抓取记录和分析，给出公证支持，所有这些信息均记录在区块链上。

3.3.6公益慈善监管

人们从事公益慈善的意愿越来越强烈，行动越来越多，一些有损公益慈善形象的事件也时有发生，为了修复公益慈善的形象，让更多需要帮助的人们和事业获得更多的支持，需要加入监管机制。采用区块链技术可以从包括但不限于以下几个方面对公益慈善进行监管。

- 机构监管：对于从事公益慈善事业的个人、机构进行必要的监管，目的是为了维护真实公益慈善机构的形象，打击虚假公益慈善的行为。通过区块链来记录慈善机构和个人的信息，供人们公开查阅监督。
- 项目监管：对公益慈善项目的监管是为了保障人们的善意行为投入到真正需要帮助的项目中，从项目识别、项目选择、项目启动、项目实施、项目效果进行全程监管，所有监管信息记录上链，对外公开。
- 善款善物监管：善款善物的监管是公益慈善的重点，很多有损公益慈善形象的事件均出在善款善物的收集、流转、分发、使用之上，通过区块链将这些信息全部记录上链，善款善物的全生命

周期公开透明，一目了然。

- 名誉监管：名誉是给予从事公益慈善事业的个人或者机构的荣誉，加强名誉监管是为了打击那些借助公益慈善之名，从事不道德甚至违法活动，谋取自身利益的行为和个人或机构，通过区块链记录各类公益慈善事件，对名誉进行公证。

3.3.7数据服务监管

数据即财富，大数据时代，自己的数据却不是自己能把握的，其价值正在为他人带来利益，数据权利得不到有效保护，数据需求者正当安全获取数据的渠道有待拓展。采用区块链技术可以从包括但不限于以下几个方面对数据服务进行监管。

- 数据采集监管：各业务平台在为用户提供服务的时候，需要采集一些用户数据，有必要对这些数据的采集进行监管，哪些可以采集，哪些不能采集，都记录到区块链上进行监管。
- 数据确权监管：各种数据的权利应该正确的归属于相关主体，通过区块链来登记数据，可以为数据确权提供公证保障。
- 数据托管监管：数据所有者在区块链上登记数据之后，还可以选择数据中心对其数据进行托管，这些托管信息也要记录在区块链上，以证明托管者的托管权和方便后续服务。
- 数据交易监管：数据交易实现数据价值，将数据交易过程记录到区块链上进行存证，是保护数据所有者和数据购买者权益的有效保障手段。
- 数据服务监管：数据最终的价值体现在于为数据需求者提供了

服务，通过区块链监管数据服务，以判定数据服务是否符合数据授权的权利。

- 数据保密监管：一些数据既需要对外提供服务，有需要有限保护自身的秘密，这就要求在提供数据服务的时候进行脱密，采用区块链记录数据保密要求，并通过数据服务的实际情况进行比较验证，以实现对数据保密的监管。

4 总结与展望

本指引在分析了区块链技术与应用的现状和存在的问题之后，分别从技术和应用两个方面给出了一些合规方面的意见，作为区块链得以健康发展的参考。随着区块链技术与应用的不断发展，该指引也会不断更新，力图更加客观的反应现状需求，成为区块链行业发展的推动力。