

## 第 1 章

# 区块链审计基础

---

### 学习目标

- 了解区块链相关概念;
- 掌握区块链审计的定义;
- 掌握区块链审计的目标;
- 了解区块链审计的规范;
- 了解区块链审计的环境。

## 审计思政微案例：苏区首任“审计长”的“六不准”

1934年，阮啸仙当选为中华苏维埃共和国第一任中央审计委员会主任。阮啸仙对审计人员提出了很高的要求，他常说，自古正人先正己，凡事必须以身作则、以身示范，这样才能树立起一种正气、硬劲，没有正气难以审查出问题，没有硬劲难以除弊。为此他规定了“六不准”工作纪律：不准偏听偏信；不准弄虚作假；不准漏查和作不精确统计；不准徇私用情；不准吃馆子或吃公饭，外出审查一律自带干粮；不准收受被审人员任何物品。



### 1.1 区块链审计含义、特征及其分类

#### 1.1.1 区块链审计含义

区块链技术也称为分布式账本技术，是由多方共同维护，使用密码学保证传输和访问安全，实现数据一致存储、难篡改、防抵赖的一种记账技术（中国信息通信研究院和可信区块链推进计划，2018）。区块链技术中的区块链是由区块（block）组成，每一个区块均包含区块头和区块体，其中区块头记录当前区块的特征值——区块的生成时间（时间戳）、本区块的哈希值、上一个区块的哈希值等信息。区块体记录本区块的实际数据。哈希（hash）运算是一种不可逆的加密运算方法，实现了区块与哈希值的一一对应，通过各区块的时间序列以及上个区块的哈希值和本区块的哈希值，将记录不同内容的区块从逻辑上连接在一起，从而形成区块链这种特殊的分布式数据库系统。节点是运行区块链的用户或计算机。当两个节点之间发生业务，业务节点就会通过广播将业务通知所有节点，计算产生出新区块记录最新业务并链接在区块链上。区块链上的信息经过全网节点验证之后不可篡改。

在区块链技术下，所有节点通过共识机制参与区块链系统中数据的验证、上链存储和维护。从原理上看，区块链是交易各方信任机制建设的数字解决方案。从技术上

看，区块链是基于互联网的底层技术架构，将分布式技术、时间戳、密码学和共识机制等技术进行有机融合。区块链技术给各行各业带来了革命性的创新，同样也给审计行业带来了颠覆性的发展，区块链审计应运而生。学者们对区块链审计进行了大量的探讨，主要有技术赋能观、分布式数据库观、分布式账本观和混合观四类。区块链审计含义观点如表 1-1 所示。

表 1-1 区块链审计含义观点

| 分类      | 观点                                                                                                                                                                                              |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 技术赋能观   | 区块链技术能够为政府审计腐败治理功能的优化赋能 <sup>[1][2]</sup> 、扶贫审计 <sup>[3][4]</sup> 、国有企业招投标跟踪审计 <sup>[5]</sup> 、加密数字货币审计 <sup>[6]</sup> 、金融审计 <sup>[7]</sup>                                                     |
| 分布式数据库观 | 去中心化的分布式数据储存结构在审计中可以降低甚至消除信息不对称带来的审计风险提高审计质量 <sup>[8]</sup> 、应用区块链技术存储于分布式数据库，形成网络分析与可视化结合的智能分析平台 <sup>[9]</sup>                                                                                |
| 分布式账本观  | 区块链技术是一个去中心化共享总账，能够为审计数据提供安全保障 <sup>[10]</sup> 、能够对审计产生重大影响 <sup>[11]</sup> 、可以降低审计费用和提高报告真实度 <sup>[12]</sup> 、解决现有审计体系的数据分散化和易泄露问题 <sup>[13]</sup> 、在新区块形成的同时自动形成副本，保证审计数据的时效性 <sup>[14]</sup> |
| 混合观     | 区块链分布式账本就是分布式数据库存储区块链网络上发生的所有交易，节点之间是点对点的方式连接，应用于审计中能提升审计数据的真实性，且数据也不易被篡改 <sup>[15]</sup>                                                                                                       |

资料来源：根据中国知网相关文献整理

技术赋能观强调区块链技术对审计赋能，在反腐治理、扶贫审计、跟踪审计、金融审计等领域大有可为。分布式数据库观强调区块链技术去中心化的分布式数据库结构对审计的作用。分布式账本观强调区块链不同特点对审计数据、审计效率和效果的影响。而混合观则认为分布式数据库从功能上等同于分布式账本。综合表 1-1 中的观点，区块链审计是指审计人员在区块链环境下，运用区块链技术去中心化、防篡改、可追溯性等特点，执行审计业务，收集审计证据，完成审计报告或者是对区块链技术应用进行安全性等问题的审计。区块链环境是假定审计单位和被审计单位都运用区块链技术，在这一环境下，审计人员利用区块链技术对被审计单位的经济活动和经济事项予以认定，客观获取和评价审计证据，确认这些认定是否与既定标准相符，并出具审计报告的过程。在区块链环境下，审计人员也可以对被审计单位的区块链技术应用系统进行审计，主要是指对数据录入的准确性、及时性、可信性等进行审计；对智能化合约、区块链设置等合规性进行审计；对区块链可能收到

本地攻击和系统范围内的攻击的安全性进行审计，以便及时查出潜在风险和漏洞，从而防范审计风险，提高审计效率。因此，区块链审计包含区块链技术审计和审计区块链两种类型。这两种类型下的审计对审计人员的职业素养也有差别，其中，前者要求审计人员对审计业务精通，以及有更高的审计判断能力；后者要求审计人员掌握区块链技术原理、代码、程序和审计流程等相关知识。

### 1.1.2 区块链审计特征

区块链具有去中心化、不可篡改、可追溯、开放性、匿名性、自治性、共识机制等特性。区块链技术应用审计中，天然附带区块链特征，打破了现有的思维模式和运转方式，使其有别于目前任何其他技术。

#### 1. 去中心化

去中心化是区块链技术最显著的特征，区块链上的每一个节点实行自我管理，不再依赖于中央统一管理，实现数据分布式记录、存储和更新。区块链上所有节点权利和义务均等，区块链系统的数据维护和更新是由全网节点按照规定好的协议共同完成。由于每个区块链节点都遵循同一协议，同时每一次数据更新需要区块链上其他节点允许，所以不需要第三方中介机构进行“信任担保”。区块链技术的去中心化应用于审计方面，表现为通过区块链信任机制，审计人员直接获取财务数据，提高审计数据的传递效率，减少传统模式中因效率低下带来的交易成本。由此可见，去中心化是区块链技术的颠覆性特征之一。区块链去中心化使得网络中心服务器巨大的数据处理能力不再是信息传输的关键门槛，降低了相关硬件和软件的配置要求，节省了一定的设备和维护开支。同时，去中心化特征使系统中所有数据是公开、透明的，审计人员更容易获取充分、适当的审计证据，采用电子函证等程序，降低审计成本并且提高系统运营效率，让点对点直接交互的方式成为现实。

#### 2. 不可篡改和可追溯性

区块链使用密码学连接数据，后一个区块包含前一个区块的时间戳，按时间顺序排序，写入区块链的数据环环相扣，只要改变其中一个节点，其他节点也会受到影响。因此，区块链具备信息不可篡改、痕迹可以溯源的特性。不可篡改是指一旦数据通过验证写入区块链，任何人都无法在未经授权的情况下更改数据信息。一旦对数据有新的操作，系统会自动对当前所有账本进行比较，认为相同数量最多的账本是真账本，和他人数量不同的账本是假账本。在这种情况下，任何人篡改自己的账本是没有意义

的，除非同时掌握整个系统 51% 节点，才能对区块链信息进行篡改。可追溯性是指利用区块链时间戳功能查找过往的痕迹。区块链可追溯性应用于审计中，其时间戳功能，一方面可以协助系统记录信息登记时间，当审计人员需要某个时间点的数据时，可以及时、准确地查找到，从而提高审计工作的效率。另一方面，时间戳可以及时、准确地追踪被篡改的数据，大大降低审计人员的工作难度。例如，通过时间戳功能，公司发生的每一笔经济活动都会实时上传网络数据库进行保存，从而大大减少虚假交易的发生。区块链时间戳技术保障了审计的连续性，使随时随地查询审计事项成为可能，也为以后的交易查询提供便利。通过时间戳技术，每个审计结果形成的具体时间一直被储存，将保证审计结果的连续性，从而使审计情况得到完整、全面的反映，有利于强化审计结果的可靠性。

### 3. 开放性和透明性

区块链所有网络节点都可以参与区块链网络数据的记录维护，因此区块链网络是开放的。同时，区块链系统又是公开透明的，除了交易各方的私有信息被加密外，其他数据对全网节点是透明的，参与节点都可以通过公开的接口查询区块链数据记录，这是区块链系统值得信任的基础。区块链的公开透明性可以保证审计人员取得被审计单位上链的交易数据，防止被审计单位有意或无意不提供审计证据和数据信息。在审计工作中，区块链技术的公开透明性一方面有助于各单位之间的沟通，缩短层层查找和交换信息花费的时间，提高工作效率，保证审计数据的可靠性，降低审计风险；另一方面可以助力监管层提高审计监管的质量，遏制审计舞弊。例如，当区块链技术引入上市公司内部审计时，每一个区块都与上一个区块相扣，且所有数据都是经过全体节点认证的、相对真实的数据，想要单纯地篡改数据将变得十分不现实。储存于系统内每一项交易产生的数据都有迹可循，系统中所有数据记录都以完整的轨迹呈现在数据查询者面前，这种分布式记账技术使得内部的财务数据变得公开透明并且不可篡改。

### 4. 匿名性

区块链在数据交易时双方可以公开身份交易，也可以进行匿名交易，前提是网络中各个节点必须要遵守相应的协议。在遵守协议的前提下，各个节点不需要知道对方的身份就可以直接进行数字交易，这种交易方式省去不必要的中间环节，既节约时间，又提高数据交易的效率。区块链技术结合 P2P 传输、分布式数据库、密码学、共识机制等技术，其核心技术之一——匿名性可以隐藏个人信息，将审计人员信息隐藏不仅

降低审计人员受贿的可能性，而且避免审计人员迫于外在压力影响审计效果，保证审计工作的独立性。例如，被审计公司在记录和确认项目公司的交易和资产时，传统审计可能存在舞弊行为，但在同一区块链下通常还得受到其他公司和机构的外部监督，客观上减少他们进行“合谋”调整报表的空间和机会，从而保证审计工作的独立性和客观性。

## 5. 自治性

区块链有使用规则和协议，系统中每一个节点都要遵守和按照协议上的要求进行数据交易，这种自定义规则和协议方式保证了区块链的高度自治性。规则可以由使用者根据自己的需求进行设定，满足使用需求，使区块链上节点只能按照协议要求去做正确的事。区块链采用基于协商一致的机制（比如一套公开透明的算法），使整个系统中所有节点能够在去信任的环境中自由安全地交换数据、记录数据、更新数据，任何人为干预都不起作用，这就是区块链自治性。区块链自治性应用于会计、审计领域，则是会计核算和审计工作大部分由网络中的使用者自发完成。区块链中的智能合约和共识机制，使只有达成共识的信息才能上链，将有效降低审计检查风险。区块链技术带来的高度标准化，使财务报表中绝大部分数据实现自动验证，这些特性在保证数据安全性的同时，显著降低了审计所需的时间与成本。

## 6. 共识机制

基于分布式架构特点，为解决节点之间的信任问题，区块链系统采用共识机制。当两个节点之间发生业务，业务节点就会通过广播将业务通知所有节点，计算产生出新区块记录最新业务，然后链接在区块链上。区块链上的信息经过全网节点的验证之后便不得更改。分布式节点之间的算力竞争保证了共识的安全性，保证了数据的真实和可靠，同时有效地解决了效率与安全之间的矛盾。区块链技术能使审计方和被审计方遵循同一共识机制。这不仅提高了鉴证业务信息的透明度，也加强了双方的信任关系，减少对审计工作的人力、物力投入，简化鉴证流程，降低风险隐患。

### 案例讨论

### 从獐子岛事件看区块链审计应用

獐子岛集团股份有限公司始于 1958 年，公司总部位于大连市，主要产业有海珍品育苗业、海水增养殖业、水产品加工业、国内外贸易等，主要产品有虾夷扇贝、刺参、鲍鱼、海参等，公司于 2006 年上市。獐



子岛扇贝 6 年间逃跑三次，在股票市场上引起了广泛的关注。2014 年 10 月獐子岛集团以北黄海异常冷水团为由宣称扇贝“逃跑了”；2018 年 2 月獐子岛集团以饲料短缺为由表示扇贝“饿死了”；2019 年 4 月獐子岛以受灾为由再次宣布扇贝“逃跑了”。对獐子岛集团进行审计的大华会计师事务所也于 2019 年解除了合约，其中不乏审计程序实施困难的理由。如何对獐子岛这类以生物资产为主的企业进行审计，解决审计程序难以实施的问题已成为当前关注的重点问题。

问题：请结合区块链审计特征思考，如何解决案例中消耗性生物资产审计中的难题？

### 1.1.3 区块链审计分类

为了正确理解和掌握不同的区块链审计形态，按照一定的标准，对区块链审计进行科学分类。区块链审计分类的标准很多，本节主要按照区块链技术在审计的功能、区块链技术类型等进行分类。

#### 1. 根据区块链技术在审计中的功能

区块链审计按照区块链技术在审计中的功能，分为基于区块链技术的审计和审计区块链系统两种类型。

##### 1) 基于区块链技术的审计

基于区块链技术的审计是指审计人员在区块链环境下，运用区块链技术去中心化、防篡改、可追溯性等特点，执行审计业务，收集审计证据，完成审计报告。即将区块链技术嵌入现有审计过程，利用技术赋能审计功能，提高审计效率。根据区块链技术具体应用的场景，有扶贫审计、金融审计等。

##### 2) 审计区块链系统

审计区块链系统是指在对区块链技术应用进行合规性、安全性等问题的审计。比如，智能合约安全审计是指仔细研究代码的过程，即把合约部署相关主网络中，并对其错误、漏洞和风险等方面的审查，然后讨论如何改进。因智能合约一旦部署不可修改、合约执行后不可逆、所有执行事务可追踪，因此，审计人员将对区块链系统的技术性、性能和安全性以及数据等内容进行审计和鉴证。这种审计需要审计人员掌握区块链底层技术结构中资源层、数据层、网络层、共识层等（见图 1-1），对智能合约等系统和算法熟悉，从而能够找到系统中的主要风险。

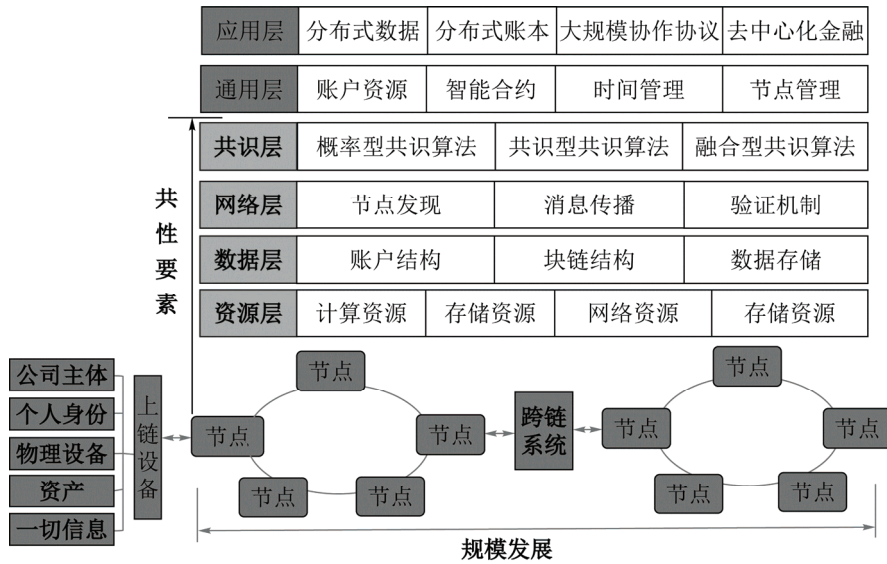


图 1-1 区块链底层技术

资料来源：《区块链基础设施研究报告（2021）》[http://science.china.com.cn/2021-07/19/content\\_41620771.htm](http://science.china.com.cn/2021-07/19/content_41620771.htm)

## 2. 根据区块链类型

根据区块链类型，分为对公有链审计、对私有链审计和对联盟链审计。

### 1) 对公有链审计

公有链是最早出现在人们视线范围的区块链，应用范围比较广、完全去中心化，任何人都能读取和发送交易，而且交易能够在区块链上得到有效的确认，任何人都可参与其中的共识过程。公有链的各个节点可以自由加入和退出网络，各节点之间的拓扑关系是扁平的。公有链具有三大特点：（1）公有链可以保护用户权益免受程序开发者的影响。在公有链中程序的开发者没有权利干涉用户，所以用户权益更容易得到保护。（2）公有链开放性强。在公有链上，任何用户都可建立自己的应用，从而产生一定程度的网络效应。任何满足一定技术条件的人都可以访问，也就是说，只要有一台能够联网的计算机就能够满足访问的条件。（3）数据公开透明。在公有链上的所有数据是默认公开的，每个参与者都可以看到系统中所有的账户余额和交易活动，即所谓的公开透明分布式“总账”系统。区块链的匿名性让参与者能够隐藏现实世界中的真实身份，从而找到公开信息与个人隐私保护之间的一个平衡。



## 2) 对私有链审计

私有链比较私密，其写入权限是在一个组织机构和单位手中，主要用于大型机构的内部，由机构进行中心化的控制，用于改善大型机构内部的运营流程，保证数据的安全，防篡改可追溯等。典型的有国际“四大”会计师事务所共同构建的区块链财务审计报告平台。私有链具有以下特点：（1）交易速度快，高信任度仅需点对点交易，无须所有节点认证。（2）交易成本更便宜。（3）隐私性好，无须处理访问权限问题，数据不会公开地被拥有网络连接的任何人获得。

## 3) 对联盟链审计

联盟链是介于公有链与私有链之间的一种系统形态，它由若干组织一起合作维护一条区块链，该区块链的使用是带有权限的限制访问，相关信息会得到保护，如供应链机构或银行联盟。联盟链的本质是分布式托管记账系统，系统由组织指定的多个“权威”节点控制，这些节点之间根据共识机制对整个系统进行管理。联盟链具有以下特点：（1）交易速度非常快。联盟链节点不多，并不需要每个节点来验证一个交易，达成共识容易，交易速度自然也就快很多。（2）部分去中心化。联盟链在某种程度上只属于联盟内部的成员所有，且很容易达成共识，所以只是部分去中心化。（3）可控性较强。联盟链的数据只限于联盟里的机构及其用户才有权限进行访问，联盟链只要所有机构中的大部分达成共识，即可将区块数据进行更改。

## 1.2 区块链审计目标

### 1.2.1 区块链审计目标含义

区块链审计目标是指审计人员通过区块链技术进行审计所期望达到的目的和要求。在区块链技术下，企业的商业模式从客户细分、价值主张、渠道、客户关系、收入来源、关键资源、关键活动、关键伙伴、成本结构九个维度发生颠覆性变化<sup>[16]</sup>。在区块链技术影响下，逐渐形成以消费者为核心、去中心化的特质创新商业模式。全新的商业模式进而带来商业生态系统的重塑，促使供应商、消费者、审计、金融、税务等不同利益相关者的加入。针对企业商业模式与商业生态系统的变化，审计人员需要通过区块链并协同金融、税务、监管等部门进行审计活动，进而达到所期望达到的目的和要求。由于区块链审计按照区块链技术在审计中的功能分为基于区块链技术的审

计和审计区块链系统两种类型。因此，区块链审计目标依次可以分为区块链审计的一般目标和区块链系统审计的目标两类。

### 1.2.2 区块链审计目标分类

#### 1. 区块链审计的一般目标

区块链审计的一般目标根据审计主题制定，比如扶贫审计、金融审计等。区块链审计的一般目标如表 1-2 所示。

表 1-2 区块链审计的一般目标

| 分类 | 再分类              | 审计目标    |
|----|------------------|---------|
| 财务 | 财务信息有无信息失真、业绩水平低 | 真实性、效益性 |
|    | 财务行为违规、不合理       | 合规性、合理性 |
|    | 财务制度设计或执行存在缺陷    | 健全性     |
| 业务 | 业务信息有无信息失真、业绩水平低 | 真实性、效益性 |
|    | 业务行为违规、不合理       | 合规性、合理性 |
|    | 业务制度设计或执行存在缺陷    | 健全性     |

资料来源：郑石桥，彭康晓雨，周敏李.企业审计目标：一个理论框架[J].会计之友 2019(06): 156-160.<sup>[17]</sup>

#### 1) 区块链扶贫审计目标

扶贫审计是指国家用于帮助贫困地区农民群众解决温饱、脱贫致富、发展经济的各种专用资金和项目进行审计。区块链扶贫审计是指以利用区块链技术完成扶贫财务与业务的一种审计类型。区块链扶贫审计的审计目标有以下几点：

(1) 保证扶贫财务信息与业务信息的真实性与效益性。在扶贫资金申领环节利用区块链技术将扶贫资金流所有环节上链，将审计应用服务层与数据存储对接，获得区块链上的动态信息，全程实时监控扶贫资金申领的全过程，防止虚假业务信息，获取财务信息与业务信息具有可信赖度，避免“假账真审”，确保扶贫财务信息与业务信息的真实性和效益性。利用区块链技术将不涉及机密的信息进行全网公开，提高公众参与度，共同监督扶贫资金的真实性与效益性。

(2) 保证扶贫财务行为与业务行为的合规性与合理性。利用区块链技术审核扶贫资金闲置时间，根据政策文件，在智能合约中设置相应的时间限制点，当扶贫资金的闲置期间达到时限点，发出审计疑点，审计人员需对审计疑点进行实时追踪，保证扶

贫财务行为与业务行为的合规性与合理性。区块链智能合约技术实现对控制贫困户条件、扶贫项目申请到验收的过程进行事前程序化控制，通过智能合约设置扶贫资金账户，防止财务行为与业务行为的不合规或不合理。

(3) 保证扶贫财务与业务制度执行的健全性。扶贫审计中将扶贫文件规定写入智能合约规则中，自动监控扶贫资金审批执行的健全性，对于违规财务与业务审批生成审计疑点。智能合约、时间戳等核心技术对扶贫财务与业务制度执行自动追踪与预警，做到事前预防、事中实时监控、事后控制的全过程审计。

## 2) 区块链金融审计目标

金融审计是指审计机构对金融机构会计记录、会计报表和其他反映业务活动的真实性、合规性和经济效益等财务资料进行监督和审查。区块链金融审计是指利用区块链技术完成金融财务与业务的一种审计类型。区块链金融审计的审计目标有以下几点：

(1) 保证金融机构财务信息与业务信息的真实性与效益性。面对庞杂繁复的交叉性业务、账户和数据，利用区块链分布式记账技术和弱中心化特性，评价所有节点共同记入公共账簿的金融交易业务与财务数据，确保高保真、可追溯和不可单一篡改、存在性和完整性，对各类金融数据实时采集、动态分析，保证金融机构财务信息与业务信息的真实性与效益性。

(2) 保证金融机构财务与业务行为的合规性与合理性。将区块链技术嵌入金融链条中，通过监管节点对金融机构实施全程跟踪审计核查，实时掌握审计对象整体财务和业务运作状况和金融市场的最新动态，保证金融机构财务与业务的合规性与合理性。评价被审计单位信息验证流程，验证各节点验证工作过程是否存在相应的缺陷。利用区块链将技术与风控模型结合，识别业务行为与财务行为潜在风险，在达到一定条件后自动出发风险预警。同时，利用区块链技术将资金流向和交易过程留存区块链中，对财务与业务行为的违规行为进行识别与监控并进行追溯，进而保证行为的合规性与合理性。

(3) 保证金融机构财务与业务制度设计及其执行的健全性。利用区块链技术合约将文件规定写入智能合约规则中，自动识别金融机构相关制度设计与执行的健全性，并对不健全部分进行预警。

## 2. 区块链系统审计的目标

区块链系统审计包括对区块链系统数据的审计和对区块链应用系统的审计。对应的审计目标分为两类：区块链系统数据审计目标和区块链应用系统审计目标。区块链系统数据审计要保证数据来源真实性、数据存储可靠性、数据内容完整性和数据之间

的相互印证性。区块链应用系统审计目标包含区块链应用系统基本要求、性能 and 安全性审计目标。

### 1) 区块链系统数据审计目标

区块链系统数据审计目标是：(1) 评价区块链数据来源的真实性，包括被审计单位采用的区块链技术存储平台的资质合规、产生数据的技术可靠、传递数据的路径可查。(2) 评价数据存储的可靠性，包括数据上链、各区块链存放内容相互印证、区块链节点生成时间符合逻辑。(3) 评价数据内容的完整性，即电子数据哈希值能验算一致未被修改。(4) 评价录入数据与其他数据相互印证的关联度。

### 2) 区块链应用系统审计目标

基于《区块链技术金融应用评估规则》(中国人民银行，2020)<sup>[18]</sup>中的评估确定对区块链应用系统的审计目标，区块链应用系统审计目标包括区块链应用系统基本要求审计目标、区块链应用系统性能的审计目标和区块链应用系统安全性审计目标。对区块链应用系统的基本要求、性能、安全性进行评估，公正、客观地评价系统是否能够保障区块链设施与应用的安全稳定运行。

(1) 区块链应用系统基本要求审计目标。区块链应用系统基本要求包括账本技术、共识协议、智能合约、节点通信、事件分发、密钥管理、状态管理、成员管理等审计目标。区块链应用系统基本要求审计目标如表 1-3 所示。

表 1-3 区块链应用系统基本要求审计目标

| 分类   | 审计目标                                              |
|------|---------------------------------------------------|
| 账本技术 | 评价数据存储技术、账本结构、历史数据可追溯、数据同步、数据归档、数据跨链功能、数据分片功能     |
| 共识协议 | 评价共识算法、共识算法一致性、共识节点数量、共识机制容错阈值、共识算法可靠性、共识算法可拓展性   |
| 智能合约 | 评价智能合约虚拟机、可编程能力、正确性、调用执行一致性、可靠性、业务隔离性、生命周期管理、版本控制 |
| 节点通信 | 评价组网方式、消息转发、节点加入、节点退出                             |
| 事件分发 | 评价完整性、一致性等                                        |
| 密钥管理 | 评价密钥生成、存储、更新、使用、撤销、销毁、归档                          |
| 状态管理 | 评价查询区块高度、查询区块详情、查询交易信息、查询交易结果、查询账本状态、账本状态更新       |

续表

| 分类   | 审计目标                                |
|------|-------------------------------------|
| 成员管理 | 评价用户注册、身份识别、权限变更、账户冻结和解冻、注销、信息查询、交易 |
| 交易系统 | 评价智能合约部署交易、智能合约方法调用交易、原生交易          |
| 接口管理 | 评价外部接口、用户接口、管理接口、系统间接口              |

资料来源：区块链技术金融应用评估规则（中国人民银行，2020）

（2）区块链应用系统性能的审计目标。区块链应用系统性能的审计目标包括评价区块链应用系统交易的吞吐率、查询吞吐率、交易同步性能、部署效率、账本数据增长率。区块链应用系统性能的审计目标如表 1-4 所示。

表 1-4 区块链应用系统性能的审计目标

| 分类      | 审计目标                                                                                                                                                                          |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 交易的吞吐率  | 评价原生交易吞吐率；在最大原生交易吞吐率需要的软硬件条件下，实际原生交易吞吐率；异常场景发生并恢复后维持的原生交易性能；智能合约调用吞吐率的数值；最大智能合约调用吞吐率所需要的软硬件条件下的数值；异常场景发生并回复后仍能维持智能合约调用的交易性能                                                   |
| 查询吞吐率   | 评价块信息查询吞吐率；节点在异常场景恢复后保证评价块信息查询吞吐率；交易信息查询吞吐率；节点在异常场景恢复后继续保证交易信息查询吞吐率；交易结果查询吞吐率；节点在异常场景恢复后继续保证交易结果查询吞吐率；智能合约数据查询吞吐率；节点在异常场景恢复后继续保证智能合约数据查询吞吐率；历史数据查询吞吐率；节点在异常场景恢复后继续保证历史数据查询吞吐率 |
| 交易同步性能  | 评价最大交易广播速度；交易的冗余率；交易广播时延；节点在异常场景恢复后继续保证申明的交易同步性能及时延；若支持无交易出空块，同步空块的速率；若支持无交易出空块，空块时延；若支持无交易出空块，节点在异常场景恢复后继续保证申明的空块同步性能及时延；同步满负载区块的速率；满负载区块广播时延；节点在异常场景恢复后继续保证申明的满负载块同步性能及时延   |
| 部署效率    | 评价系统搭建、节点扩容、节点升级、节点删除、节点增加的时间                                                                                                                                                 |
| 账本数据增长率 | 评价无交易状态下账本数据增长速率；满负载状态下账本数据增长速率                                                                                                                                               |

资料来源：区块链技术金融应用评估规则（中国人民银行，2020）

（3）区块链应用系统安全性审计目标。区块链应用系统安全性审计目标包括基础硬件、基础软件、密码算法、节点通信、账本数据、共识协议、智能合约、身份管理、隐私保护、监管支撑、安全运维和安全治理等。区块链应用系统安全性审计目标如表 1-5 所示。

表 1-5 区块链应用系统安全性审计目标

| 分类   | 审计目标                                                 |
|------|------------------------------------------------------|
| 基础硬件 | 评价硬件基本条件、物理安全、网络安全                                   |
| 基础软件 | 评价基本条件、账本结构、数据存储、共识模块、分布式组网、智能合约、接口设计、数据传输、时间同步、操作系统 |
| 密码算法 | 评价算法基本条件、保密性、完整性、真实性                                 |
| 节点通信 | 评价节点身份验证、通信完整性、通信保密性                                 |
| 账本数据 | 评价账本数据的完整性、一致性、保密性、数据冗余                              |
| 共识协议 | 评价共识协议合法性、正确性、终局性、不可伪造性、健壮性、低延时、激励相容、可监管性            |
| 智能合约 | 评价访问控制、智能合约原子性、智能合约安全审计、攻击防范、安全验证                    |
| 身份管理 | 评价身份注册、身份核实、账户管理、凭证生命周期管理、节点标识管理、身份更新和撤销、身份监管审计      |
| 隐私保护 | 评价隐私保护策略、隐私保护技术、隐私保护监控与审计                            |
| 监管支撑 | 评价交易信息监管、监管系统、应急事件报警、智能合约监管                          |
| 安全运维 | 评价权限管理、审计记录、系统更新                                     |
| 安全治理 | 评价系统安全管理机制、节点管理、干预机制                                 |

资料来源：区块链技术金融应用评估规则（中国人民银行，2020）

## 1.3 区块链审计规范

### 1.3.1 区块链技术标准

#### 1. 区块链技术标准的定义及范围

区块链技术标准是指区块链技术运行的规则，即区块链技术在不同领域对于区块数据信息的输入、储存及查询等方面普遍化、标准化的应用规范。目前区块链技术标准范围主要应用于金融行业、能源企业、会计审计领域等方面各个重要的业务经营环节，即从原始节点的数据输入开始，一直到当前用户的使用、存储数据，都需要遵守区块链技术的标准，使用规定的方法和规范的格式存储数据信息。区块链中涉及多个数据获取、分析及存储的相关应用和技术，应加强对这些数据的安全应用、安全技术、安全能力测评。安全测评是评判区块链数据平台是否能为区块链用户提供安全可靠的区块链数据。通过安全测评可以进一步发现区块链数据标准的漏洞与安全隐患，并及时修改，有效防止数据风险，为区块链安全机制和数据标准提供较为安全的服务奠定基础。2021 年 5 月，全国区块链



和分布式记账技术标准化技术委员会（SAC/TC590）成立，工作与国际标准化组织区块链技术委员会（ISO/TC307）对应，旨在规范区块链和分布式记账技术发展，促进我国深入参加本技术领域的国际标准化工作。国家级区块链技术标准如表 1-6 所示。

表 1-6 国家级区块链技术标准

| 序号 | 发布时间           | 标准号/计划号        | 名称                      |
|----|----------------|----------------|-------------------------|
| 1  | 2020 年 4 月 1 日 | 20201612-T-469 | 信息技术区块链和分布式记账技术存证应用指南   |
| 2  | 2018 年 1 月 9 日 | 20173824-T-469 | 信息技术区块链和分布式账本技术参考架构     |
| 3  | 2020 年 4 月 1 日 | 20201615-T-469 | 信息技术区块链和分布式账本技术智能合约实施规范 |

资料来源：端震，朱嘉慧.我国区块链技术标准发展现状综述[J].软件，2020，41(10):242-245+259.[9]

## 2. 区块链技术标准的基本原则

（1）连续性原则。区块链技术标准连续性原则体现在业务连续性，即无论用户处在区块链内业务的哪一个节点上，其获取和存储数据信息的标准都是统一的、连续的且不间断的。节点上的信息会实时更新数据资料。即使前面某一业务节点信息是错误的，也不会影响下一业务节点的使用，因为会通过新增业务数据链来调整错误的数  
据，新增条链的运行标准与原条链一致。

（2）可用性原则。区块链技术标准的可用性原则主要体现在两方面：一方面，通过区块链技术标准分析和存储数据信息的真实、可靠，且能为区块链用户使用，标准的数据信息容错性较好，不易受拜占庭节点以及非拜占庭容错的影响；另一方面，通用的区块链技术标准可以满足于大多数行业需求和业务要求，数据算法、数据输入格式规范以及数据存储方式的相关准则可使用性较强。

（3）安全性原则。区块链技术标准的安全性原则重点在于保证用户及其区块链节点数据的信息安全。信息安全是指用户执行与存储在节点的数据安全、不可篡改。区块链技术标准安全性原则的总体要求包括数据安全、共识安全、个人信息保护、智能合约安全和内容安全五个方面。安全性原则的层面要求包括基础设施层安全、协议层安全和拓展层安全。

## 3. 区块链技术标准的框架及主要要素

（1）区块链技术标准框架包含扩展层、协议层与基础设施层（如图 1-2 所示）。

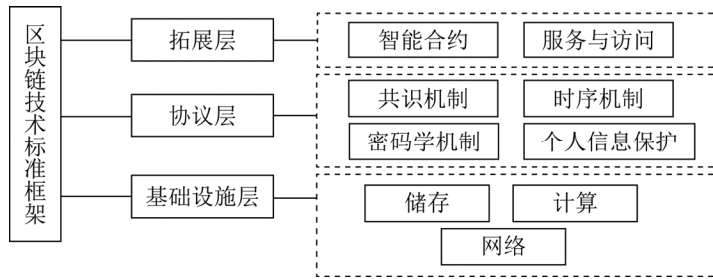


图 1-2 区块链技术标准框架图

基础设施层将传统网络安全与区块链安全联系起来。协议层基于基础设施层提供的硬件或网络基础体系实现相应功能，并为扩展层提供相应功能支持服务；协议层包含区块链技术的几大关键机制：共识机制、密码学机制、时序机制以及个人信息保护，协议层向下连接基础设施层，向上衔接扩展层。扩展层通过调用协议层功能组件，可以提供多元化的服务和访问。需要指出的是，区块链应用安全也是区块链安全不可忽视的关键环节。

(2) 区块链技术标准的要素有智能合约、共识机制、密码学机制、时序机制、服务与访问等，其中最主要的、应用最多的是智能合约、共识机制和密码学机制等要素。

①智能合约。1996 年，美国密码学家兼程序员 Nick Szabo 首次提出智能合约的概念。智能合约是一套信息传输的数字协议，包括合约参与方可以执行这些约定的协议。通过算法在满足既定条件后自动执行交易，并完全控制整个过程。区块链技术标准中智能合约的执行要注重保持独立性、保障可靠性、保证高效率、注重安全性。智能合约规范标准包括合约构建要求、合约触发要求、合约事件约束、合约运行过程和合约评价方法五个方面。

②共识机制。共识机制是通过特殊节点投票完成对交易的验证和确认。共识机制是区块链技术的核心基石，是区块链系统安全性的重要保障。区块链技术标准中要加强共识协议在容错性上的设计，使其可以容忍一定范围的节点物理或网络故障导致的非恶意节点断线和网络分区，并且能够抵御合谋攻击、女巫攻击等恶意攻击行为；确保多个节点参与共识和确认，防止任何独立节点的恶意操作；通过引入链外可信第三方的方式来增强联盟链的数据不可篡改性；根据网络规模、参与方数量、交易吞吐率等需求调整算法规模。区块链技术标准应确保任何已经被记录在区块链上并达成共识的交易都无法更改；应确保诚实节点提交的合法数据终将由全网节点达成共识并被记录在区块链上。

③密码学机制。密码学机制有两个基本原则：消息包含一定冗余度和采取措施对



抗重放攻击。另外，关于密码学系统的设计遵循 Kerckhoff 原则，即“密码算法必须公开，只有密钥需要保密”。对于密码学机制，区块链技术标准为保证用户密码使用的安全、可靠，使用较为安全的哈希算法，如国密算法 SM3、SHA256 等。非对称加密算法用于信息加密、数字签名和登录认证等场景。在重要业务场景，使用权威公正的第三方证书认证中心机构签发的数字证书来进行数字签名和签名验证等相关工作，确保信息的机密性、完整性和不可抵赖性。在使用随机数时，按照国家密码管理部门的要求生成随机序列。

### 1.3.2 区块链审计标准

#### 1. 区块链审计标准定义和范围

区块链审计标准是指审计人员在执行审计时应当遵守的职业规范。具体来说，是基于区块链技术各项运行规则，审计人员在审计过程中，用来判断和评价区块链内各个节点获取的被审计事项、作出审计结论和得出合理审计意见的重要依据。包括区块链审计基本准则、技术准则以及区块链技术下审计人员的职业道德等内容。审计人员在利用区块链技术执行审计时，在遵守区块链技术标准及使用规范的基础上，按照审计需要和区块链审计规范，对各个节点获取相应的审计数据，根据具体的会计、审计准则要求，对区块链内各个节点的审计数据进行识别，并判断其是否存在重大错报风险，得出相关审计结论，出具合理的审计意见。与传统审计标准类似，区块链审计标准也具有层次性、时效性的特点。区块链审计标准的层次性是指因管辖范围和权威性的大小而有不同的适用层次，如国家法律、国务院颁布的行政法规、地方性法律及法规、主管部门制定的规章制度、被审计单位制定的规章制度。时效性是指区块链审计标准受政策法规的变化、区块节点的数据规则变化等影响，其效力时间是有限制的，而非永远不变的。

目前，我国审计领域区块链技术处在研发阶段，还未出台较为完善的相关执行标准、行业规范和法律条例。区块链技术不确定性和潜在风险是区块链审计发展的重要因素。因此，现阶段重点关注区块链技术的安全审计。2018 年，我国《区块链智能合约实施规范》中提到安全审计，即智能合约的安全审计和评估对象包括智能合约设计及业务逻辑安全、源代码安全审计、编译环境审计及相关应急响应等。其中，设计及业务逻辑安全审计是对业务逻辑的安全评估，可通过人工阅读和源代码的方式，对智能合约的业务流程进行安全性的测试和评估；当发现智能合约漏洞后，应及时检查和修

复智能合约代码。2020年，上海市质量技术监督局发布的《区块链技术安全通过规范（征求意见稿）》中提到：区块链技术应提供安全审计功能，对重要操作进行审计；安全管理机构的所有干预操作行为应被记录实现不可更改并可被查询，做到可审计、可追溯；应提供内容监管服务，强化区块链的安全监管；应支持安全管理机构接入，在发生特殊突发事件时，可对区块链系统进行干预。

## 2. 区块链审计标准的重要意义

（1）提高审计效率。标准化的区块链审计标准在区块内按照统一的规则运行，各节点有条不紊地执行指令和存储审计证据信息，节约审计人员收集审计证据的时间，直接在被审计单位授权之后便可获取相关数据，极大地提高审计工作效率。另外，在区块链技术中建立多方交流平台和不同区块，各节点在区块内就能及时沟通。比如，电子函证可代替传统函证工作，通过区块链将被审计单位的节点与银行节点进行对账，不论佐证或矛盾，最终结果都会记录在区块链上，审计人员在获得授权后可以查看被审计单位的相关资料，确定是否进行进一步审计程序，区块内的电子函证方便快捷，不但节约了审计工作函证邮寄成本，同时也提高了审计效率和效果。

（2）降低审计风险。区块链“去中心化”的特征是权力分散，每个节点地位平等，且数据不能篡改。区块链审计标准表明，如果想要修改或记录信息需要其他节点的一致通过。这为串通舞弊增加难度，由此降低部分审计风险。区块链的另一特性—智能合约，旨在基于信息的方式传播、验证或执行合同的计算机协议。在使用区块链时，这些可靠的、不可修改的数据自动执行一些完善的、统一的、标准的规则和程序。即运用去中心化，在没有第三方管理员监督下自动进行的可靠交易，保证整个过程透明化、可追踪化。基于区块链智能合约不仅便于交易双方及时发现问题并沟通解决，根据交易信用、交易规模等方面判断风险程度，一旦发现某节点的风险过大及时退出，且安全地存储已获取的审计数据，在将智能合约写入区块链的同时奠定其信息永久储存的基础<sup>[20]</sup>。

（3）保障审计独立性。审计作为平衡被审计单位管理层和报表预期使用者的独立体，最主要任务是识别被审计单位有无重大错报、财务报表是否按照会计准则编制。被审计单位管理层在此过程中可能会出现财务造假，审计人员不可能发现所有的错报漏报。因此，区块链审计应用极大地解决了这个问题，财务数据的不可篡改、信息的可追溯性以及加密性等功能都有助于审计人员识别管理层的舞弊行为，在审计过程中能始终保持应有的独立性。例如，在区块链审计过程中获取被审计单位相关数据时，非对称加密

技术有公钥和私钥，用公开钥匙加密，则需要对应的私有钥匙才能解开。非对称加密技术能够更好地保证审计人员的独立性，在一定程度上减少了被审计单位管理层舞弊的行为。

### 1.3.3 区块链技术数据标准

#### 1. 区块链技术数据标准定义及分类

区块链技术数据标准是对区块链技术下数据信息获取、判断、评估的准则，旨在保证存储在区块链内各个节点上数据信息的真实、可靠，确保用户安全的使用节点数据并能实施追溯。区块链技术相关的数据对象结构包括区块、事务、实体、合约、账户、配置六个主要数据对象。其中，区块链核心数据对象包括区块、事务、实体和合约。每一区块数据对象中包含一个或多个事务数据对象，每个事务对象包括属性类的实体数据对象，还包括事务的业务逻辑，即合约数据对象。在区块链核心数据对象之外，包括配置数据对象，提供区块链系统正常运行过程中所需的配置信息。配置数据对象和区块链核心数据对象共同构建了区块链运行所需的基础数据基础。而账户数据对象表示区块链业务的实际发起者和相关方对应的数据结构<sup>[21]</sup>。

以数据对象的类别为依据，将区块链数据分为以下六类：

(1) 账户数据。账户数据是指描述区块链事务实际发起者和相关方的数据。区块链中记录的事务信息均被关联相关账户之上，每个区块链服务客户拥有一个或多个账户来使用区块链服务。

(2) 区块链数据。区块链数据是指区块链网络的底层链式数据，把一定时间内发生的事务处理结果转化为不同的区块链式数据结构。通常情况下，区块由区块头和区块体组成。区块头包含区块相关的控制信息，区块体包含具体的事务数据。

(3) 事务数据。事务数据是指描述区块链系统上承载具体业务动作的数据。其中，事务既包括交易类型事务，也包括非交易类型事务。

(4) 实体数据。实体数据是指描述事务静态属性的数据。通常包括发起方地址、接收方地址、交易发生额、交易费用、存储数据和实体数据备注。

(5) 合约数据。合约数据是指描述事务动态处理逻辑的数据。合约又称智能合约，是一套以计算机代码形式定义的承诺，以及合约参与方可执行承诺的协议。这里合约数据既包括处理逻辑的可执行代码，也包括处理逻辑的执行结果。

(6) 配置数据。配置数据是指区块链系统正常运行过程中所需的配置信息。通常包括共识协议版本号、软件版本号和网络通信底层对等节点配置信息等。

## 2. 国际区块链技术标准

2016 年 9 月，国际标准化组织成立了区块链和分布式记账技术（ISO/TC307），负责区块链和分布式账本技术的标准研制，主要工作范围是制定区块链和分布式记账技术领域的国际标准，以及与其他国际性组织合作研究区块链和分布式记账技术领域的标准化相关问题。国际标准化组织正在制定八项关键区块链标准。2017 年，ISO/TC307 加快推动基础类、智能合约、安全隐私、身份认证、互操作等方向的重点标准研制工作。目前，术语、参考架构、分类和本体等国际标准已完成立项，进入研制阶段。ISO/TC307 现阶段标准研制情况如表 1-7 所示。

表 1-7 ISO/TC307 现阶段标准研制情况

| 序号 | 英文名称                                                                                                                                  | 中文名称                          |
|----|---------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| 1  | ISO/DIS 22739 BLOCHIAN AND DISTRIBUTED LEDGER TECHNOLOGIES-TERMINOLOGY                                                                | 区块链和分布式账本技术——术语               |
| 2  | ISO/CD TR 3242 BLOCHIAN AND DISTRIBUTED LEDGER TECHNOLOGIES-USE CAES                                                                  | 区块链和分布式账本技术——用例               |
| 3  | ISO/CD TR 23576 BLOCHIAN AND DISTRIBUTED LEDGER TECHNOLOGIES-SECURITY MANAGEMENT OF DIGITAL ASSET CUSYODIANS                          | 区块链和分布式账本技术——数字资产托管人的安全管理     |
| 4  | ISO/WD23257.2 BLOCHIAN AND DISTRIBUTED LEDGER TECHNOLOGIES-REFERENCE ARCHITECTURE                                                     | 区块链的分布式账本技术——参考架构             |
| 5  | ISO/CD TR 23245 BLOCHIAN AND DISTRIBUTED LEDGER TECHNOLOGIES-SECURITY RISKS, THREATS AND VULNERABILITIES                              | 区块链和分布式账本技术——安全风险和漏洞          |
| 6  | ISO/WD TS 23258 BLOCHIAN AND DISTRIBUTED LEDGER TECHNOLOGIES-TAXONOMY AND ONTOLOGY                                                    | 区块链和分布式账本技术——分类和本体            |
| 7  | ISO/CD 23257.2 BLOCHIAN AND DISTRIBUTED LEDGER TECHNOLOGIES-PRIVACY AND PERSONALLY IDENTIFIABLE INFORMATION PROTECTION CONSIDERATIONS | 区块链和分布式账本技术——隐私和个人可识别信息保护注意事项 |
| 8  | ISO/NP TS 23635 BLOCHIAN AND DISTRIBUTED LEDGER TECHNOLOGIES-GUIDELINES FOR GOVERNANCE                                                | 区块链和分布书账本技术——管理准则             |
| 9  | ISO/AWI TS 23259 BLOCHIAN AND DISTRIBUTED LEDGER TECHNOLOGIES-LEGALLY BINDING SMART CONTRACTS                                         | 区块链和分布式账本技术——法律约束的智能合约        |

续表

| 序号 | 英文名称                                                                                                                                                                        | 中文名称                                 |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| 10 | ISO/NP TR 23246 BLOCHIAN AND DISTRIBUTED LEDGER TECHNOLOGIES-OVERVIEW OF IDENTITY MANAGEMENT USING BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLIGIES                           | 区块链和分布式账本技术——基于区块链和分布式账本的身份识别技术综述    |
| 11 | ISO/TR 23455:2019 BLOCHIAN AND DISTRIBUTED LEDGER TECHNOLOGIES-OVERVIEW OF AND INTERACTIONS BETWEEN SMART CONTRACTS IN BLOCKCHAIN AND DISRIBUTED LEDGER TECHNOLOGUY SYSTEMS | 区块链的分布式账本技术——区块链和分布式记账技术系统中智能合约的交互概述 |

资料来源：公开资料搜索

其中，术语和参考架构等基础类标准主要回答区块链是什么和怎么用的问题，同时建立标准语言并指导其他标准的研发；安全风险和漏洞、隐私和个人可识别信息保护注意事项、身份识别、智能合约等相关标准则主要回答如何在保证安全性、隐私保护和合规性的前提下设计、开发、维护和使用区块链系统。

3. 我国区块链技术标准

2017 年 12 月 22 日，中国区块链技术和产业发展论坛标准发布《区块链数据格式规范》，该规范给出了数据格式规范，尤其是明确了数据项标识符和共识机制的相关数据格式，在一定程度上规范了区块链技术的数据标准。尽管出台了一些区块链的相关法规和指南，但我国区块链技术数据标准仍然处于研发阶段，有许多问题需要解决。首先，缺少专门针对区块链技术数据标准的准则和应用指南，通常都是一个整体指南指导所有区块链技术的运行，缺乏问题的针对性和归纳性；其次，各行各业对于区块链技术数据标准的需求各有不同，金融、会计、审计等领域对数据标准的获取方式、分析模式和存储条件都有所差别，但目前还未有很明确的行业区块链数据标准；最后，现行的数据标准以区块链技术标准为主执行，不但用户的执行力不强，各行各业有自己的一套解释，而且市场监管力度弱，不能很好地监督区块链内各个节点的数据运行是否符合规则要求、数据运行是否安全、是否存在违规操作以获取不法利益等。

区块链中涉及多个数据获取、分析及存储的相关应用和技术，应加强对这些数据安全应用、安全技术、安全能力的测评。安全测评是评判区块链数据平台是否能为区块链用户提供安全可靠的区块链数据。通过安全测评可以进一步发现区块链数据标准的漏洞与安全隐患，并及时修改，有效防止数据风险，为区块链安全机制和数据标准

提供较为安全的服务奠定基础。

## 1.4 区块链审计环境

### 1.4.1 区块链审计环境的含义

区块链审计环境是指区块链技术应用于审计活动中的客观环境。审计环境的分类可以分为宏观环境、中观环境与微观环境。其中，宏观环境主要是指国家关于区块链技术及其监管的法律、法规、规章和制度。中观环境主要是地区或者行业组织对区块链技术标准的制定等。微观环境是指应用区块链技术主体对区块链技术引入程度、人力资本投入以及各种技术运行保障等。



国外法规颁布的数量远远超过我国关于区块链技术的法规。国外区块链法规与政策的颁布多集中与对区块链技术的监管，规范区块链技术的使用。我国区块链法规、政策的颁布大部分是鼓励与支持区块链技术的发展与应用，为区块链技术创新提供较大的扶持力度。近几年，随着区块链技术的不断发展，我国也在逐步加强对区块链监管力度，为区块链技术发展提供良好的监管环境。

### 1.4.2 国内外区块链法规和政策

#### 1. 国外区块链法规和政策

中本聪 2008 年在“比特币：一种点对点的电子现金系统”（Bitcoin: A Peer-to-Peer Electronic Cash System）<sup>[22]</sup>文章中提到区块链概念后，其优势逐渐被各国认可，并在多领域积极探索技术的推广应用，各国政府积极对区块链技术进行战略布局。国外区块链法规和政策如表 1-8 所示。

表 1-8 国外关于区块链的相关法规和政策

| 年份   | 内容                                                                                    |
|------|---------------------------------------------------------------------------------------|
| 2016 | 英国政府发布《分布式账本技术：超越区块链》白皮书，肯定了区块链的价值                                                    |
| 2017 | 日本实施了《支付服务法案》，正式承认比特币是一种合法的支付方式，对于数字资产交易提出了明确的监管要求；同年，日本新版消费税正式生效，比特币交易不再需要缴纳 8% 的消费税 |

续表

| 年份   | 内容                                                                                               |
|------|--------------------------------------------------------------------------------------------------|
| 2019 | 德国经济能源部和财政部联合发布了《国家区块链发展战略》，率先将区块链上升为国家战略，并首先开展区块链技术的数字身份试点项目                                    |
| 2019 | 美国国会发布《区块链促进法案》，要求联邦政府商务部门区块链工作组，推动区块链技术定义及标准的统一，以及区块链在非金融领域更大范围的应用，从而促进区块链技术创新和保持美国高新技术在全球的领先地位 |
| 2020 | 澳大利亚政府发布《国家区块链路线图：朝着区块链赋能的未来迈进》，重点关注三大领域：法规和标准；技能、能力和创新；国际投资与合作                                  |

资料来源：根据《区块链白皮书（2020年）》资料整理

英国、美国、德国、澳大利亚和日本等国政府均在大力支持区块链技术的发展，助力区块链技术的创新。区块链技术除了应用于比特币等加密货币以外，还有其他方面的应用潜力。2018年，美国联邦政府和各州政府出台区块链相关立法，比如《2018年联合经济报告》《区块链：背景和政策问题》《区块链在政府应用中的适用性》《区块链技术概论》等报告，阐明美国政府对监管和发展的思路。由于区块链技术还处于早期发展阶段，美国政府也重视区块链安全风险问题，通过出台《2018年国防授权法案》对区块链技术进行安全风险预评估。

## 2. 国内区块链法规和政策

### 1) 国家层面

2016年12月，国务院印发了《“十三五”国家信息化规划》，鼓励针对区块链等战略性前沿技术进行提前布局，发挥先发主导优势，标志着我国开始推动区块链技术和应用发展。2017年6月，中国人民银行下发了《中国金融业务信息技术“十三五”发展规划》的通知，明确提出积极推进区块链、人工智能等新技术应用研究，并组织进行国家数字货币的试点。2018年以来，监管层对区块链发展的态度逐步引导至服务实体经济。2019年2月，国家互联网信息办公室发布的《区块链信息服务管理规定》正式实施，明确区块链信息服务提供者的信息安全管理责任，规范和促进区块链技术及相关服务健康发展，规避区块链服务安全风险，为区块链信息服务的提供、使用、管理等提供有效的法律依据。2019年10月，中共中央政治局就区块链发展现状和趋势进行了第十八次集体学习，中央领导明确强调把区块链作为核心技术自主创新的重要突破口，加快推动区块链技术和产业创新发展，区块链技术已经上升至国家高度。目前，我国在技术、应用、监管和其他等方面出具一系列的国家层面区块链法规和政策。国家层面区块链法规与政策如表1-9所示。

表 1-9 国家层面区块链法规和政策

| 分类 | 年份             | 政策名称                              | 政策主要内容                                          |
|----|----------------|-----------------------------------|-------------------------------------------------|
| 技术 | 2016 年<br>12 月 | 国务院：《“十三五”国家信息化规划》                | 首次将区块链纳入新兴技术范畴并作前沿布局，标志着我国开始推动区块链技术和应用发展        |
|    | 2017 年<br>7 月  | 国务院：《关于新一代人工智能发展规划的通知》            | 促进区块链技术与人工智能的融合，建立新型社会信任体系                      |
|    | 2018 年<br>6 月  | 工信部：《工业互联网发展行动计划（2018—2020 年）》    | 鼓励推进边缘计算、深度学习、区块链等新兴前沿技术在工业互联网的应用研究             |
|    | 2018 年<br>1 月  | 工信部：《“十三五”国家国家信息化规划的通知》           | 积极构建完善区块链标准体系，加快推动重点标准研制和应用推广，逐步构建完善标准体系        |
| 应用 | 2017 年<br>1 月  | 国务院：《关于积极推进供应链创新与应用的指导意见》         | 提出要研究利用区块链、人工智能等新兴技术，建立基于供应链的信用评价机制             |
|    | 2017 年<br>11 月 | 国务院：《关于深化“互联网+先进制造业”发展工业互联网的指导意见》 | 促进边缘计算、人工智能、增强现实、虚拟现实、区块链等新兴前沿技术在工业互联网中的研究与探索   |
|    | 2018 年<br>2 月  | 工信部：《关于组织开展信息消费试点示范项目申报工作的通知》     | 积极探索利用区块链技术开展信息物流全程监测，推进物流业信息消费降本增效             |
| 监管 | 2019 年<br>1 月  | 国家互联网信息办公室：《区块链信息服务管理规定》          | 规范我国区块链行业发展所发布的备案依据。出台意味着我国对于区块链信息服务的“监管时代”正式到来 |
| 其他 | 2017 年<br>1 月  | 工信部：《软件和信息技术服务业发展规划（2015—2020）》   | 提出区块链等领域创新达到国际先进水平等要求                           |
|    | 2018 年<br>3 月  | 工信部：《2018 年信息化和软件服务业标准化工作要点》      | 推动组建全国信息化和工业化融合管理标准化技术委员会、全国区块链和分布式记账技术委员会      |

资料来源：《中国区块链政策现状及趋势分析报告》

## 2) 地方层面

在国家层面区块链技术法规、政策的示范下，地方层面也出具了相关的法规与政策。主要可以分为技术层面、产业层面与应用层面。

(1) 技术层面。各地区在技术方面，鼓励区块链技术的创新研究和应用，并强调区块链技术标准体系的制定，鼓励区块链技术与大数据、人工智能等技术的融合研究和应用，以解决社会信用、成本、效率等方面的问题。地方层面区块链技术层面政策法规如表 1-10 所示。



表 1-10 地方层面区块链技术层面政策法规

| 年份   | 政策名称                                        | 相关内容                                                                                                                                            |
|------|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 2016 | 《贵阳区块链发展和应用白皮书》                             | 涉及重大理论创新提出包括主权区块链、“绳网结构理论”以及“块数据”与“绳网结构”理论的融合                                                                                                   |
| 2017 | 《贵州省数字经济发展规划（2017—2020）》                    | 推进区块链技术发展应用，建设区块链数字资产交易的平台，构建区块链应用标准体系，为资产的数字化流通提供系统支持                                                                                          |
| 2017 | 《浙江省人民政府办公厅关于进一步加快软件和信息服务业发展的实施意见》（代拟稿）     | 加快云计算、大数据、量子通信、无人驾驶、虚拟现实、区块链、人机物融合计算等前沿领域技术研究和产品创新                                                                                              |
| 2018 | 《2018 年度上海市软件和集成电路产业发展专项资金（软件和信息服务业领域）项目指南》 | 区块链作为产业发展的方向之一，支持研发基于区块链技术的自主开源平台，开发新型加密算法和共识机制，构建区块链技术底层基础架构及各方面应用                                                                             |
| 2018 | 《广东省数字经济发展规划（2018—2025）》                    | 加快研究共识算法、非对称加密、容错机制、分布式存储等区块链关键技术，支持发展高并发、高吞吐、低延迟、高可靠性区块链解决方案，大力发展区块链即服务，推动区块链与云计算、人工智能的融合创新。积极拓展区块链应用场景，加强区块链技术在金融、商贸、政务、民生、智能制造、物流、能源等重点行业的应用 |
| 2018 | 《河北雄安新区规划纲要》                                | 推动信息安全技术研发应用，发展规模化自主可控的网络空间安全产业，超前布局区块链、太赫兹、认知计算等技术研发及实验                                                                                        |
| 2019 | 浙江：《关于加强区块链信息服务管理工作的实施意见》                   | 区块链信息服务的主体需尽快登录国家网信办区块链信息服务备案管理系统进行申报备案，并且所有操作合法合规                                                                                              |
| 2019 | 《云南省区块链产业发展规划》                              | 区块链产业发展要从数据、算力、算法与应用四个方面，构筑区块链创新应用生态                                                                                                            |

数据来源：公开资料搜集

（2）产业层面。北京市、河北省、江苏省、湖南省、广东省、广西壮族自治区、海南省先后发布了针对区块链产业发展的专项政策，设定各地区区块链产业发展目标。截至 2019 年底，全国共有 23 个城市或地区成立 30 余家区块链产业园区。据统计，国家互联网信息办公布的 801 个区块链信息服务备案清单中，北京、广州、上海、浙江、江苏、山东为备案企业最多的省份。截至 2019 年年底已有超过 80 家上市公司涉足区块链领域，积极部署供应链金融、资产管理、跨境支付、跨境贸易的应用，多数企业呈现多领域协同发展态势。从地理位置来看，北京、上海、杭州、广州、重庆、青岛等城市区块链产业园区数量较多，

形成以北京、山东为主的环渤海聚集效应，以浙江、上海、江苏为主的长三角聚集效应，以广东为主的珠三角聚集效应和以重庆、湖南为主的湘黔渝聚集效应。产业园的建设规划，为企业的聚集效应提供了基础。地方层面区块链产业计划如表 1-11 所示。

表 1-11 地区区块链产业计划

| 年份   | 政策名称                             | 相关内容                                                                                                                             |
|------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 2017 | 重庆:《关于加快区块链产业培育及创新应用的意见》         | 到 2020 年,力争在重庆全市打造 2~5 个区块链产业基地,引进和培育区块链国内细分领域龙头企业 10 家以上、有核心技术或成长型的区块链企业 50 家以上,引进和培育区块链中高级人才 500 名以上,将重庆市建成国内重要的区块链产业高地和创新应用基地 |
| 2020 | 《湖南省区块链产业发展三年行动计划(2020—2022)》    | 力争 2022 年建成 10 个以上区块链公共服务平台,推动 3 万家企业上链,建成 5 个左右区块链产业园,相关产业营业收入达到 30 亿元,建设成为全国有影响力的区块链技术创新高地、产业聚集洼地和应用示范基地                       |
| 2020 | 《广州市推动区块链产业创新发展的实施意见(2021—2022)》 | 截至 2022 年,突破一批区块链底层核心关键技术,引进培育 2~3 家国内领先且具有核心技术的区块链龙头企业;推进以区块链为特色的中国软件名城示范区建设,打造 2~3 个区块链产业基地,培育一批具有安全稳定区块链产品的行业重点企业等            |
| 2020 | 贵州:《关于加快区块链技术应用和产业意见》            | 截至 2022 年,将建设 3~5 个区块链开放创新平台及公共服务平台,打造 2~3 个区块链产业基地,引进培育 100 户以上成长型区块链企业,形成 30 个以上行业区块链应用解决方案,推广 50 个以上区块链典型应用示范                 |
| 2020 | 《北京市区块链创新发展行动计划(2020—2022)》      | 截至 2022 年,把北京初步建设成为具有影响力的区块链科技创新高地、应用示范高地、产业发展高地、创新人才高地,率先形成区块链赋能经济社会发展的“背景方案”,建立区块链科技创新与产业发展融合互动的新体系,为北京经济高质量发展持续注入新动能新活力       |
| 2020 | 云南:《普洱市区块链产业发展规划(2020—2025)》     | 目标是截至 2025 年,力争将普洱建设成为国家区块链应用示范先导区、西南区块链创新发展引领城市、云南区块链产业核心聚集地                                                                    |
| 2020 | 《广西壮族自治区区块链产业与应用发展规划(2020—2025)》 | 截至 2025 年,形成 100 个特色鲜明、可复制可推广的区块链典型应用示范;引进和培育 10 家以上区块链领军企业,打造形成 5~10 个区块链产业基地;形成 15 个以上区块链技术创新平台及公共服务平台;培育引进中高级人才 1 000 名以上等    |

续表

| 年份   | 政策名称                          | 相关内容                                                                                                                                                                 |
|------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2020 | 《河北省区块链专项行动计划（2020—2022）》     | 将加强区块链理论研究和技术研发，加速区块链产业生态建设，提高区块链应用和管理能力，截至 2022 年年底，区块链相关领域企业和龙头企业达到 20 家，培育一批区块链应用产品，力争打造出 1~3 个全国知名区块链品牌，形成 3 个具有区域影响力的区块链产业集聚园区，区块链产业竞争力位居国内前列                   |
| 2020 | 《成都市区块链应用场景供给行动计划（2020—2022）》 | 力争截至 2022 年，在政务服务、城市治理、新消费、跨境贸易、智能制造、智慧农业、智慧教育、智慧医疗、金融服务、知识产权等区块链应用领域形成开放共享生态，打造 30 个典型区块链应用示范场景，形成 2~3 个区块链产业集聚发展区，将成都建设成为区块链技术创新先发地、区块链产业创新发展示范区                   |
| 2020 | 《济南市区块链产业创新发展行动计划》            | 计划截至 2022 年，区块链核心业务收入超过 10 亿元，带动行业相关收入 100 亿元以上，区块链相关企业超过 50 家，培养行业国内知名企业 2 家以上；区块链相关研究机构超过 20 个，培育国产区块链平台和底层公共服务平台 2 个以上；培育国内重点区块链应用产品或解决方案 50 个以上；培育区块链产业集聚区 2 个以上 |

数据来源：公开资料搜集

（3）应用层面。各省市政策多是鼓励区块链技术应用的落实，主要集中在正在创新发展、金融、政务及公共服务等领域，也涉及农业、贸易商贸、公共卫生、交通运输、知识产权等。但是从政策数量上来看，鼓励区块链技术在金融领域应用的政策最多。部分地区加强了区块链技术在金融领域的监管政策。例如，2017 年上海颁布的《互联网金融从业机构区块链技术应用自律规则》，要求区块链技术服务实体经济，注重创新与规范、安全的平衡，明确金融稳定与信息安全的底线，互联网金融从业机构应用区块链技术应当向当地监管部门及行业自律组织进行报备，主动接受行业监管与自律管理，报备信息至少应包括项目名称、责任人、业务模式、业务风险、风控措施等。

随着国家层面在应用方面出具的支持法规与政策，许多企业开展了区块链的应用，如能源行业。在能源行业中，企业的区块链能源行业主要分布在能源贸易（如化工能源贸易、石油贸易）、能源数据共享、分布式能源交易及节能减排四方面。

能源贸易中的代表企业为中国石油化工集团有限公司与中国中化集团有限公司。中石化下属科技有限公司—中化能源科技旗下的“壹能链”助力化工品交易的区块链

应用；中国中化集团完成我国第一单区块链原油进口交易试点，区块链大幅提升原油交易执行效率，并优化 20%~30% 交易融资成本。

数据共享中的代表企业为国家电网有限公司与中国南方电网有限责任公司。国家电网有限公司基于自主研发的区块链底层平台，通过区块链和物联网有机结合实现了能源计量数据的安全共享问题；中国南方电网有限责任公司开展了电网企业区块链技术研究及应用验证等项目。

分布式能源交易的代表企业为国家能源投资集团有限责任公司，建立了国家第一个分布式能源区块链交易项目，支持分布式能源发电业主与用电客户间的实时电力交易及账务处理。

节能减排的企业为鞍钢集团有限公司，与金山云共建“精钢云”平台，结合云计算、物联网、人工智能与区块链技术建设工业领域质量跟踪、节能减排、智慧物流等应用场景。

近几年，随着区块链技术的不断发展，我国也在逐步加大对区块链的监管力度，为区块链技术的发展提供良好的监管环境。在区块链审计上，由于政策支持，国内国外区块链审计都有一定的发展。例如，在国际上“四大”会计师事务所对区块链审计的探讨与应用，国内皓风审计链的出现。区块链审计具有区块链技术的特性，降低了传统审计中的风险，提高审计报告内容质量，审计的透明度也有所增加。

### 1.4.3 区块链环境对审计的影响

区块链审计环境对审计目标、审计规范、审计假设、审计流程、审计方法、审计证据、审计风险、审计报告等方面都产生影响。

#### 1. 审计目标的变化

审计目标是为了满足客户应对市场环境变化防范风险需求而制定的。在区块链技术的影响下，审计环境发生巨大变化，审计目标也随之变化。审计目标总体上从传统的静态思路即“鉴定财务报表的公允和真实”向动态思路即“降低信息风险”转变，从传统重视从结果进行审查，到重视审计全过程的控制。

在区块链技术的影响下，审计目标包括区块链审计与审计区块链系统两种类型的审计目标。其中，区块链审计目标受到具体审计内容的影响，需要根据不同审计内容进行探讨具体的审计目标（如扶贫审计、金融审计等）；审计区块链系统的审计目标主要有审计区块链数据真实性与审计区块链应用系统两个审计目标。

## 2. 审计规范的变化

审计规范是在组织实施审计工作和审计管理中应遵循的行为准则。它是衡量和判断审计机构和审计人员的各种活动是否合法、合规、高质、有效的标准和依据。在区块链技术下，审计规范需要考虑区块链技术标准、区块链审计标准与区块链技术数据标准来规范审计机构与审计人员的审计行为。

(1) 区块链技术标准。区块链技术标准是指区块链技术运行的规则，即区块链技术在不同领域对于区块数据信息的输入、储存及查询等方面普遍化、标准化的应用规范。区块链技术标准包括连续性原则、可用性原则、安全性原则，保证被审计单位使用规定的方法和规范的格式存储数据信息。

(2) 区块链审计标准。目前，我国审计领域区块链技术应用缓慢，还没有区块链审计标准。随着区块链技术的发展，未来区块链审计还需要建立并不断完善相应的行业准则、进一步开发区块链审计技术，明确在区块链技术下审计人员的职责与道德规范，促进区块链审计的进一步发展。

(3) 区块链技术数据标准。目前我国缺少区块链技术数据标准专门的准则和应用指南，需要规范区块链技术数据确保数据对象结构、数据分类与数据规范的标准，来保证存储在区块各个节点上的数据信息的真实、可靠，保证审计数据的真实与可靠。同时，还要加强对区块链技术数据标准的安全测评。

## 3. 审计假设的变化

审计假设是基于区块链生态环境下进行审计而作出的假设，区块链审计假设包括区块链审计生态系统多方参与与区块链审计生态系统运行假设。

(1) 区块链审计生态系统中多方参与。区块链生态系统由审计单位、被审计单位、被审计单位上下游企业、金融机构、税务机构、物流企业、监管机构以及区块链技术供应商等多方共同组成和维护。

(2) 区块链审计生态系统运行假设主要有：审计单位与被审计单位均使用区块链技术；区块链审计生态系统运行的效率可控，保障区块链审计生态系统的效率；区块链审计生态系统匿名性引发的法律风险可控，保障整个区块链系统运行的安全性。

在区块链审计生态系统多方参与与区块链审计生态系统运行假设的背景下，区块链审计模式重构，在实践层面出现双链架构的混合审计模式以及其他区块链审计模式的实践应用。

#### 4. 审计流程的变化

区块链审计过程包括区块链审计全过程、区块链审计流程和智能审计程序。

(1) 区块链审计全过程。区块链审计全过程是指审计项目在区块链系统下从开始到结束的过程中的各个步骤，包括区块链技术审计准备阶段、区块链技术实施阶段和区块链技术审计报告阶段。

(2) 区块链审计流程。区块链审计流程本质上是一种数据流程导向的审计流程，是以区块链审计应用系统已有数据、被审计单位数据、外围数据为基础，开展数据分析比对和计算，锁定问题疑点，精准现场核查，综合分析评价，出具审计结论，开展实时监督的过程。

(3) 智能审计程序。智能审计程序是指借助人工智能与区块链技术的支持，通过物联网中的各类传感器进行数据采集，并在物联网中的各节点上加载人工智能算法的处理器进行审计数据分析，再由物联网中的输出终端生成审计报告的审计全过程自动化运行环境。智能审计程序包括智能风险评估程序、智能控制测试以及智能实质性程序。

#### 5. 审计方法的变化

区块链技术的广泛应用，改变了审计对象，对于审计方法、审计测试流程等形成了巨大的冲击。审计方法变化包含区块链电子函证、区块链审计数据分析和区块链全面审计。

(1) 区块链电子函证。数字函证平台可实现会计师事务所发函、银行收函、被审计企业确认、银行回函、会计师事务所接收回函全流程线上处理，进而有效提升效率、降低成本。

(2) 区块链审计数据分析。审计数据分析是指审计人员通过对被审计单位电子数据的采集、整理，形成自身所需要的审计中间表，在此基础上运用查询、验证、挖掘等方式进行数据的观察和分析，从而达到把握总体、突出重点、精确延伸的审计目标。

(3) 区块链全面审计。区块链技术的介入，减少审计抽样的运用。区块链技术的各种核心技术与优势能够保证交易数据的真实性与可靠性。区块链的某些应用项目，如电子函证，能够促进纸质媒介上的信息（如纸质发票、合同等）向结构化电子数据的转换，进一步扩大对总体而不是样本进行审计的范围。利用区块链技术推动审计测试的范围由代表性样本扩展至整个总体，已经进入实际操作的阶段。

#### 6. 审计证据的变化

区块链技术对审计证据的特征、获取方式与数据类型产生一定的影响，具体如下：

(1) 区块链审计证据取证环境。区块链数据的安全性、可靠性、可追溯性与永久存储保证区块链在审计取证领域应用的可行性。同时，区块链技术对审计证据产生一定的影响，包括取证程序、取证时间的由繁到简，取证范围的由局部到全面。

(2) 区块链审计证据的特征。区块链审计证据较传统审计更加具有充分性、相关性与可靠性。充分性主要是区块链技术带来内部信息与外部信息的范围、质量、数量大幅提高。相关性是指区块链技术能够保证审计单位获取审计证据的时效、保证审计证据多渠道、多类型的获取，保证审计证据的及时、客观、准确。可靠性是指在区块链技术下，审计证据是可以被验证的、完整的，保证审计证据的真实、可信并确保审计证据能够包含证明审计对象所有必要信息。

(3) 区块链审计证据的获取方式。在区块链技术下，审计证据获取方式的变化体现为：能够进行数据自动化筛选，把与审计业务相关的信息自动进行清洗筛选，形成有规则、有效的审计信息；能够进行基础分析；实现财务数据真实性和准确性；实现证据获取加密；自动且进行分布式的审计证据留存。

(4) 区块链审计证据获取的类型。在区块链技术下，获取的审计证据根据是否上链分为链上数据与链下数据；根据结构类型分类可以分为结构化数据、非结构化数据与半结构化数据。

## 7. 审计风险的变化

区块链技术为审计带来便捷的同时，也引入了新的审计风险，如安全风险、技术风险、信用机制重构风险、跨界风险、监管风险等。对于安全风险的控制，主要是采取加密技术保证算法安全、采用严格完整测试协议安全与保护秘钥进行控制；技术风险的控制主要从审计信息全面覆盖、甄别链上数据真伪、建立激励机制进行控制；审计人员增强区块链等高新技术的知识储备量进行控制跨界风险；加强区块链的立法，建立规范体系来进行控制监管风险。

## 8. 审计报告的变化

区块链技术保证审计报告的不可篡改性避免主观错误的发生。在区块链技术下，审计报告的主要变化有形式、时效与可视化。

(1) 审计报告的形式。首先，区块链技术下的审计报告可以按照使用者主体的不同按需提供不同的审计报告；其次，审计报告形式包括事项审计报告，提高审计报告的可用性。

(2) 审计报告的时效。在传统的信息系统之中，企业的财务报告及其审计工作受

制于成本因素，具有明显的滞后性，降低了财务会计信息和审计报告的决策有用性。区块链技术的各种核心技术促进实时审计的实现，审计报告的时效性较传统审计下的审计报告大幅增强。

(3) 审计报告的可视化。区块链技术下的审计报告可以可视化的形式来表达。例如，用图标的形式展示审计结果，也可以用动态图、立体图等形式展示细节。

## 本章小结

本章讲述了区块链审计概念及分类，区块链审计目标、区块链审计规范和区块链审计环境。将区块链审计分为区块链技术审计与区块链系统审计两类，将区块链审计目标分为区块链技术审计的审计目标与区块链系统的审计目标两类，并进行深入探讨。从区块链技术标准、区块链审计标准以及区块链技术数据标准三个方面详细阐述区块链审计规范。区块链审计环境首先探讨了区块链审计环境定义并对国内外区块链法规与政策进行细分，进一步阐述区块链审计环境的变化，进而引出区块链审计环境对审计的影响。

