雄安新区区块链安全 区块链技术应用安全规范

目　录

一、范围

本标准规定了区块链系统上层应用所涉及到的“设备、软件、协议、数据和业务逻辑”的安全要求、方法、评测标准，用于保障区块链核心加密骨干网之外的应用组件安全，保障从终端用户接入、交互、业务推进等过程安全。

本标准适用于:

1.指导组织和机构建立、实施、保护和改进区块链系统应用安全体系。

2.为计划基于已有的区块链底层平台来搭建区块链应用的组织和机构提供安全参考。

3.为区块链技术企业的技术研发要求提供有效的参考和借鉴。

4.为区块链服务评估方的评估评测提供有效的参考和借鉴。

二、规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 5271.18—2008《信息技术 词汇 第 18 部分：分布式数据处理》

GB/T 9387.2—1995《信息处理系统 开放系统互连 基本参考模型 第 2 部分:安全体系结构》

GB/T 18794.7—2003《信息技术 开放系统互连 开放系统安全框架 第 7 部分：安全审计和报警框架》

GB/T 20271—2006《信息安全技术 信息系统通用安全技术要求》

GB/T 25069—2010《信息安全技术 术语》

GB/T 28452—2012《信息安全技术 应用软件系统通用安全技术要求》

GB/T 32399—2015《信息技术 云计算 参考架构》

CBD-Forum-001—2017《区块链 参考架构》

三、术语定义和缩略语

（一）术语定义

GB/T 5271.18—2008《信息技术 词汇 第 18 部分：分布式数据处理》、GB/T 9387.2—1995《信息处理系统 开放系统互连基本参考模型 第 2 部分:安全体系结构》、GB/T 18794.7—2003《信息技术 开放系统互连 开放系统安全框架 第 7 部分：安全审计和报警框架》、GB/T 25069—2010《信息安全技术 术语》、GB/T 32399—2015《信息技术 云计算 参考架构》以及CBD-Forum-001—2017《区块链 参考架构》中界定的以及下列术语和定义适用于本文件。

活动：一组特定任务的集合。

功能组件：参与活动所需的，可实现的一个功能性基本构件块。

网络：对各个实体及其互联所作的一种安排。

节点：在网络中，将其连接到一个或多个其他实体的实体。

服务：给定层及其以下各层为其高一层的实体提供的能力。

对等网络：一种仅包含对控制和操作能力等效的节点的计算机网络。

区块链：一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。

块链式数据结构：一段时间内发生的事务处理以区块为单位进行存储，并以密码学算法将区块按时间顺序连接成链条的一种数据结构。

智能合约：由事件驱动的、具有状态的、运行在可复制的共享区块链数据账本上的一段计算机代码，是现实世界中合约和规则的算法实现。

数据完整性：数据没有遭受以未授权方式所作的更改或破坏的特性。

散列/杂凑函数：将比特串映射为固定长度的比特串的函数，该函数满足下列两特性：

（1）对于给定输出，找出映射为该输出的输入，在计算上是不可行的。

（2）对于给定输入，找出映射为同一输出的第二个输入，在计算上是不可行的。

保密性：使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。

拒绝服务：一种使系统失去可用性的攻击。

安全审计：为了测试出系统的控制是否足够，为了保证与已

建立的策略和操作规程相符合，为了发现安全中的漏洞，以及为了建议在控制、策略和规程中作任何指定的改变，而对系统记录与活动进行的独立观察和考核。

审计机构：管理者，负责定义适用于实现安全审计的安全策略。

（二）缩略语

简写	英文全称	中文解释
ACK	Acknowledge Character	确认字符
API	Application Programming Interface	应用编程接口
CA	Certificate Authority	认证中心
CDN	Content Delivery Network	内容分发网络
DDoS	Distributed Denial of Service	分布式拒绝服务
DoS	Denial of Service	拒绝服务
DLT	Distributed Ledger Technology	分布式账本技术
KSI	Keyless Signature Infrastructure	无密钥签名基础设施
PKI	Public Key Infrastructure	公钥基础设施
P2P	Peer to Peer	对等网络
SQL	Structured Query Language	结构化查询语言
SYN	Synchronize Sequence Numbers	同步序列编号
TCP/IP	Transmission Control Protocol/Internet Protocol	传输控制协议/互联协议

四、区块链技术应用安全体系

区块链技术应用安全体系包括对区块链协议、数据与应用程序的安全要求。区块链功能与应用角度的安全性要求，主要体现在链上基础功能的可靠稳定性、终端链设备应用程序安全以及区块链浏览器安全；对数据的安全性要求，体现为区块链应用端数据安全；较底层的安全要求，涉及到业务应用共识逻辑安全与审计以及区块链应用协议安全；其他安全方面包括区块链证书安全以及运维安全等。区块链技术应用安全体系框架见图 1。

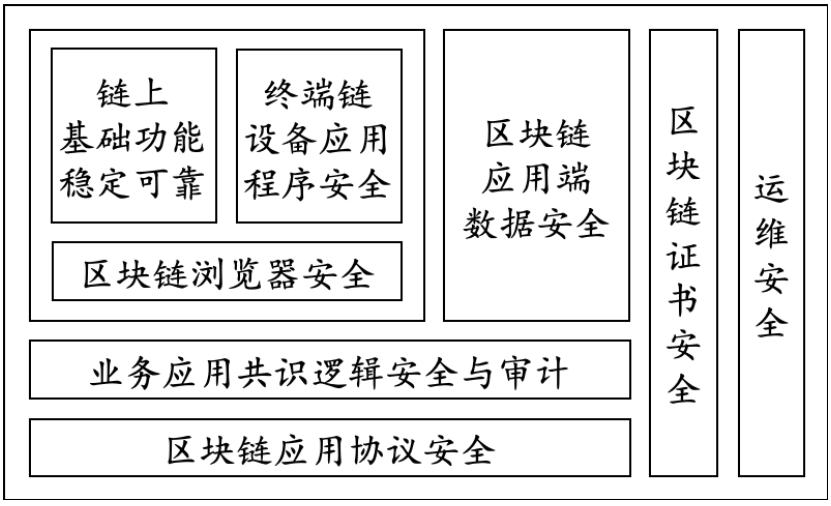

图 1 区块链技术应用安全体系框架

本标准依照图 1 分别提出以下安全要求：

（1）链上基础功能稳定可靠：区块链上基础功能的可靠稳定与安全性要求。

（2）终端链设备应用程序安全：区块链终端设备上应用程序的安全要求。

（3）区块链浏览器安全：区块链浏览器提供的功能组件、模块的安全要求。

（4）区块链应用端数据安全：区块链应用端上数据在存储、访问、传输等过程中的安全要求。

（5）业务应用共识逻辑安全与审计：业务场景中各节点之间的共识逻辑以及审计的安全要求。

（6）区块链应用协议安全：区块链应用防范各种漏洞攻击的安全要求。

（7）区块链证书安全：区块链系统对数字证书生成调用过程中的安全要求。

（8）运维安全：区块链应用在部署运行、版本升级、系统扩展以及维护过程中的安全性要求。

五、链上基础功能稳定可靠

链上基础功能是指区块链应用宜提供的数据查询、关联、交易、存证、接口等基础功能。

区块链应用可以通过自主开发区块链浏览器，或向区块链浏览器提供安全接口，来支持并保证链上基础功能稳定可靠地运行。

1.查询

区块链应用宜提供对于数据的实时查询功能，查询的数据包括但并不限于区块链总体信息、区块和交易信息、账户信息以及智能合约信息，需通过身份认证、访问控制等方式保护用户的隐私安全，同时借助区块链分布式存储的特性，提高查询功能的稳定可靠性。

2.关联

区块链应用应向用户明示数据公开收集的范围及用处，在征得用户同意的情况下，可提供对于数据进行关联的功能。将数据分析技术与智能合约进行结合，快速关联信息数据并形成数据画像，用户通过关联功能可以快速得到经过数学模型筛选后的数据。

3.交易

区块链应用应支持交易信息公开透明、真实可信，交易过程由所有相关的分布式节点根据共识机制参与；交易内容由区块链的链式结构与加密算法确保不被篡改；在签署智能合约之后，应保证在合约条件达成时交易自动执行。

4.存证

区块链应用宜支持区块链全节点全链条存证，保证存证固化和永续性保存，以备必要时可以从节点中取证、核证。利用时间戳，清晰展示存证信息的先后，在通过多节点共识认可的电子数据存证或第三方权威机构参与等方式下，保证存证信息的真实性和有效性。

5.接口安全

区块链应用应设计带有身份令牌、签名、时间戳等的消息传播机制，来校验调用请求的合法性，检验数据是否被篡改，避免过期、非法、无效的请求对数据接口以及应用接口进行访问与调用。

六、终端链设备应用程序安全

终端链设备指位于区块链网络中的，作为区块链节点经由通

信设施进行发送或接收数据的设备。

终端链设备应用程序包含一系列的交互操作的界面、命令行工具或可后台运行的服务等应用程序，以供用户使用。

终端链设备应用程序应至少保证数据在身份识别、节点通信、数据存储、权限控制、安全审计等过程中的安全性。

1.身份识别

终端链设备应用程序宜通过密钥管理、证书管理等功能组件对连接终端链设备、登录终端链设备应用程序、进行数据传输的分布式节点身份进行识别，允许合法的接入、登录与传输，拒绝非法的接入、登录与传输。

2.节点通信

终端链设备应用程序需要与其他节点进行通信的建立，来进行数据的发送与接收。在建立节点通信之前，终端链设备应用程序应通过身份识别来验证通信节点的身份；在节点通信过程中，终端链设备应用程序需要根据区块链应用协议以及相关的数据传输策略来验证发送或接收数据的合法性。

3.数据存储

终端链设备需具备必要的 DLT 系统、非 DLT 系统以及应用程序。终端链设备操作系统应为终端链设备应用程序分配合理的存储空间，来存储必要的发送与接收的数据。同时通过使用安全可靠的区块链数据格式和链式结构、加密算法和摘要算法、强伪随机数以及可信时间戳等方式对数据进行保护，提升数据存储的安全性。

4.权限控制

终端链设备应用程序应具备权限控制功能。在用户通过终端链设备应用程序对数据进行增、查、改等操作时，对用户以及应用程序的权限进行查验，来确保数据操作的合法性，保障数据的安全。

5.安全审计

终端链设备应提供安全审计功能，定期对发生在终端链设备应用程序上的账本数据及其访问与变更、用户账户以及身份凭证的访问与更改等数据进行审计，确保数据的合法性与合规性。

七、区块链浏览器安全

区块链应用可以通过自主开发区块链浏览器，或向区块链浏览器提供安全接口，来向用户提供浏览、查询区块链上信息以及节点网络配置功能。

为防止区块链浏览器网页篡改、中断服务、窃取信息和控制网站等攻击情况的发生，区块链应用宜通过对外开放安全接口，以供区块链浏览器对相关功能模块的开发实现。

1.区块链应用宜通过对外开放安全接口，供区块链浏览器开发防篡改、监测、恢复等安全模块，降低网页服务中断的风险，提高系统的可用性。同时宜提供区块链总体运行情况的安全预览服务，基本地展现该区块链的核心安全指标。

2.区块链应用宜通过对外开放安全接口，供区块链浏览器实现包括交易区块、智能合约等信息展示和查询服务，为各类用户隐私信息提供安全保护服务，降低区块链浏览器敏感信息泄露的

安全风险。

3.区块链应用宜通过对外开放安全接口，供区块链浏览器支持安全方便的节点授权服务以及服务器配置服务，制定外部和内部用户访问控制策略、系统设备之间的访问策略，至少包括对共识节点和接入节点两种节点的安全配置服务。

八、区块链应用端数据安全

区块链应用端数据存储在区块链网络与链下数据库中。由于区块大小的限制以及出于对隐私信息的保护，区块链应用端数据通常采取链下存储数据，链上仅存储数据摘要。

（一）操作过程安全

区块链应用端数据应至少保证数据在以下过程中的安全性:

1.数据存储安全

在进行数据存储时，应将数据通过合理的加密技术进行存储，并根据数据量大小以及数据重要程度合理选择链上/链下存储，通过规章制度、访问控制以及权限分配等方式确保数据存储介质的物理安全和访问安全。

2.数据访问安全

数据的访问方式包括同链调用、跨链访问以及链外协同。区块链应用应提供权限设置的编程接口，供智能合约编写者在编写合约时设定访问控制权限和管理策略，并提供运维接口供区块链网络的运营方动态调整用户的访问控制权限。

3.数据传输安全

在进行数据传输时，应在通信节点之间建立安全传输通道，

保证数据传输的完整性和不可篡改性。应在风险评估的基础上采用合理的加密技术，并配备有相应的密钥管理方案。

（二）数据属性安全

区块链应用端数据安全性应至少包括数据完整性、数据保密性、不可否认性、数据的备份与数据的恢复等方面:

1.数据完整性

区块链应用应按照 GB/T 20271—2006《信息安全技术 信息系统通用安全技术要求》中 6.2.2.3 以及 GB/T 28452—2012《信息安全技术 应用软件系统通用安全技术要求》中 6.1.4 的要求，对应用软件系统控制范围内存储和传输的用户数据进行保护。

区块链应用宜通过检测网络设备操作系统、主机操作系统、数据库管理系统和应用系统的系统管理数据，来鉴别信息和重要业务数据的完整性是否受到破坏，并在检测到完整性错误时采取必要的恢复措施。具体措施包括并不限于:

（1）具备完整的用户访问、处理数据信息的操作记录能力，以备审计。

（2）经由不安全网络进行传输数据信息时，要在散列函数等密码学算法基础上对传输的数据信息提供完整性校验。

（3）应具备完善的权限管理策略，支持权限最小化原则，合理授权。

2.数据保密性

数据保密性用于保障业务平台重要业务数据信息的安全传输与处理，确保数据信息能够被安全、方便、透明的使用。

区块链应用应按照 GB/T 20271—2006《信息安全技术 信息系统通用安全技术要求》中 6.2.3.4 以及 GB/T 28452—2012《信息安全技术 应用软件系统通用安全技术要求》中 6.1.5 的要求，对应用软件系统控制范围内存储和传输的用户数据进行保护。

区块链应用宜采取合适的加密措施，使用对称或非对称国密算法并结合相应的密钥管理方案，实现业务数据的保密性。对于隐私保护等级要求较高的敏感数据，能够通过各种安全技术，支持在不获取数据的情况下对数据进行使用。

3.不可否认性

区块链应用宜使用数字签名等密码技术生成可靠的电子签名来实现实体对于数据操作的不可否认性，确保对于数据的增删改查等操作的实体身份的真实性与正确性。

4.数据的备份

区块链应用应按照 GB/T 20271—2006《信息安全技术 信息系统通用安全技术要求》中 6.2.2.5 以及 GB/T 28452—2012《信息安全技术 应用软件系统通用安全技术要求》中 6.1.6 的要求，对应用软件系统控制范围内存储和传输的用户数据进行备份。

区块链应用宜具有数据备份功能以便恢复数据，具体的备份方式应至少包括:

（1）备份数据

系统应确保对核心数据定期进行增量以及全备份；业务系统进行重大系统变更前，应对核心数据进行数据信息的全备份。

（2）备份介质

应采用性能可靠、不易损坏的介质。备份数据信息的物理介质应注明数据信息的来源、备份日期、恢复步骤等信息，并置于安全环境保管。

（3）备份周期

服务器和网络安全设备的配置数据信息应定期进行备份；当进行配置修改、系统版本升级、补丁安装等操作前也要进行备份。

（4）过程记录

备份执行过程应有详细的规划和记录，包括备份主体、备份时间、备份策略、备份路径、记录介质类型等。

5.数据的恢复

区块链应用应按照 GB/T 20271—2006《信息安全技术 信息系统通用安全技术要求》中 6.2.2.5 以及 GB/T 28452—2012《信息安全技术 应用软件系统通用安全技术要求》中 6.1.6 的要求，对应用软件系统控制范围内存储的用户数据进行故障恢复。

区块链运维系统应根据不同业务系统实际拟定需要测试的备份数据信息以及测试的周期。当链下数据遭到破坏时，通过记录的日志、备份的数据等进行数据恢复。

九、业务应用共识逻辑安全与审计

业务应用共识逻辑是指特定应用场景中，各分布式节点间达成共识的规则和逻辑。

区块链应用应对区块链网络中的数据、账本记录以及共识过程进行审计，对区块链共识算法以及智能合约的业务设计、代码安全、应急响应机制等相关信息进行审计记录，以实现区块链网

络的审计内控、责任鉴定和事件追溯等方面的要求。区块链应用应保证:

1.多方参与共识

支持多个节点参与业务的共识和确认，任何独立节点未经业务应用共识机制确认，而在区块链系统中进行信息记录或修改，其它独立节点可以对区块链网络提交的相关信息进行有效性验证，且有权拒绝同步。

2.业务应用共识容错性

业务应用共识应具备一定的容错性，包括节点发生物理或网络故障的非恶意错误和节点遭受非法控制的恶意错误，以及节点产生不确定行为的不可控错误。

3.共识审计机构的设立

区块链服务审计机构可加入区块链网络作为其中一个节点进行审计工作，或允许区块链服务审计机构作为区块链网络之外的第三方机构，按需或定时获得区块链网络中的数据与证据。数据和证据包括但不限于区块链所有相关方的业务应用活动和运营环境条件的记录和日志、审计员的审计查看动作记录、审计过程和结果信息等，应避免审计信息的泄漏。

4.联盟链机构安全

实现基于证书的权限控制与准入机制。区块链平台的身份认证体系针对联盟链环境的参与节点，为了达成机构级别的安全控制和审计监管，首先需要对联盟链参与节点进行身份认证和准入控制,可通过第三方的可信 CA，在网络上验证参与节点的身份。

十、区块链应用协议安全

区块链应用协议主要是指基于底层链平台来实现特定功能应用的一组规则。

区块链应用协议基于区块链底层平台来实现特定功能应用，基于区块链的业务应用系统宜具备基本的网络边界防护、设定节点准入机制、网络入侵检测与病毒防御机制，避免出现 DDoS 攻击、Web 注入攻击、账户信息泄露、共识机制破坏以及智能合约漏洞等安全方面的漏洞，附录部分将对区块链应用协议安全的关键技术问题提供进一步描述。

1.DDoS 攻击

区块链应用协议宜通过安装专业抗 DDoS 防火墙、部署 CDN 内容分发网络等方式，抵御攻击者利用应用平台信息传输协议发起针对性的 DDoS 攻击，以保证机器的正常响应以及各类应用业务的正常进行。

2.SQL 注入攻击

区块链应用协议宜通过对输入数据合法性的判断,来避免攻击者通过应用端向 web 连接的数据库发送恶意的 SQL 语句，以保证区块链应用中的验证请求信息成功响应，防止隐私信息泄露。

3.账户信息泄露攻击

区块链应用协议宜通过对登陆请求进行会话判断、要求登录密码复杂度等方式，强化网站登陆接口请求限制以及风险控制，避免攻击者利用应用端上的相关用户信息向网站持续性发送请

求，以暴力破解来获得关键信息。

4.针对共识机制的攻击

区块链应用协议宜结合业务需求与应用场景，采取适当的共识机制来避免攻击者利用共识机制的漏洞，破坏区块链网络。区块链应增加相应的应用协议以避免如双花攻击、自私挖矿及女巫攻击等漏洞，以保证区块链应用的有序运行。

5.智能合约漏洞

智能合约的执行应在可信的软硬件支持的环境中执行，并且智能合约代码宜加密存储，不能被第三方明文读取。除此之外，区块链智能合约宜支持函数级别访问控制，在合约中对一些高权限函数调用进行地址校验，从而实现访问权限控制。区块链应用协议应对智能合约采取规范设计、合理加密、安全审计以及定时维护等方式，避免攻击者使用代码重入，反复执行恶意合约代码的行为，同时应该及时有效的排查智能合约中的整数溢出、变量混淆、拒绝服务等漏洞，以保证智能合约的安全可靠。

十一、区块链证书安全

区块链运维管理系统可通过基于非对称加密技术的 PKI、基于哈希加密技术的 KSI 等技术方式，来管理本组织内部的用户和节点密钥证书，进行多组织协同参与、联盟组织自治的分布式密钥证书管理。区块链证书安全应至少包括：组织根证书安全、节点证书安全、用户证书安全、通信证书安全及应用开发者证书安全。

1.组织证书安全

组织证书用于组织身份认证及组织内节点和用户的证书派生。区块链系统应提供安全的证书生成工具，调用生成组织根证书。

2.节点证书安全

节点证书用于节点身份认证，通过组织根证书派生。区块链系统应提供安全的证书生成工具，调用生成节点证书。

3.用户证书安全

用户证书用于用户身份认证，通过组织根证书派生。区块链系统应提供安全的证书生成工具，调用生成节点证书。

4.通信证书安全

通信证书用于组织和区块链运维管理系统通信认证。区块链系统应提供在安全的通信证书生成工具，调用生成组织通信证书。

5.应用开发者证书安全

应用开发者证书用于应用开发者身份认证。区块链运维管理系统应提供证书生成接口，调用生成密钥证书。

十二、运维安全

区块链应用应保证在部署运行、版本升级、系统扩展以及维护过程中的安全性。

1.安全部署环境

区块链应用应在安全的环境下进行部署。宜整合安全加密算法、对接安全 P2P 网络对数据传输进行加密保护，防止密钥派生分发过程中用户密钥泄露、节点配置过程中隐私配置信息泄露等

情况的发生。

2.安全升级控制

区块链版本升级策略，应保证升级过程中业务的平稳运行。

区块链应用的应用软件宜支持版本的向下兼容，升级操作做好日志记录，方便审计和追溯，以支持必要的升级需求。升级过程中如果发生异常情况，保证可以正常回滚，恢复到之前的版本。

3.系统安全扩展

区块链网络节点的动态扩展以及区块链节点资源的扩展，都要保证账本、区块数据的同步，同时加入网络的节点要符合区块链标准体系。动态扩展过程中，保证对原有业务的平稳运行不产生影响。

4.安全维护环境

区块链应用宜提供网络监控功能，对整个区块链网络的交易、流量等数据进行实时监控，保证区块链网络的正常运作，并在必要时提供应急措施。可将监控信息通过区块链浏览器等进行可视化展现，方便区块链应用系统进行运维工作。

附录（资料性附录）网络协议攻击示例

本附录对区块链关键技术的安全问题提供进一步描述。

（一）DoS 攻击

DoS 攻击是指故意攻击网络协议中存在的缺陷或直接通过野蛮手段耗尽目标对象的资源，目的是让目标计算机或网络无法提供正常服务，使目标系统停止响应甚至崩溃。DoS 攻击可以分为利用软件存在的缺陷、利用协议的漏洞及进行资源比拼等类型。

1.利用软件存在的缺陷

软件开发过程中对某种特定类型的报文或请求未进行处理，若软件遇到此类型的报文，运行会出现异常，导致软件崩溃甚至系统崩溃。

2.利用协议的漏洞

以 SYN Flood 攻击为例，SYN Flood 攻击利用 TCP/IP 协议的漏洞进行攻击。通常一次 TCP 连接的建立为：客户端发送 SYN 包给服务器端，服务器分配一定的资源进行连接并返回 SYN/ACK 包，客户端向服务器发送 ACK 报文，客户端与服务器之间建立连接继而传送数据。SYN Flood 攻击指客户端向服务器持续发送 SYN 报文，而不返回 ACK 报文，服务器占用过多资源，从而导致系统资源占用过多，不能响应正常的网络请求。

3.进行资源比拼

攻击者凭借丰富的资源，向目标系统发送大量的垃圾数据，导致目标系统拒绝服务。

（二）DDoS 攻击

分布式拒绝服务攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高 DoS 攻击的威力。通常，攻击者使用一个偷窃帐号将 DDoS 主控程序安装在一个计算机上，主控程序将在一个设定的时间与大量代理程序通讯，代理程序已经被安装在网络上的许多计算机上。代理程序收到指令时就发动攻击。利用客户/服务器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行。

DDoS 攻击通过大量合法的请求占用大量网络资源，以达到瘫痪网络的目的，这种攻击方式可分为以下几种:

1.通过使网络过载来干扰甚至阻断正常的网络通讯。

2.通过向服务器提交大量请求，使服务器超负荷。

3.阻断某一用户访问服务器。

4.阻断某服务与特定系统或个人的通讯。

（三）SQL 注入攻击

SQL 注入攻击是指通过构建特殊的 SQL 输入语句作为参数传入 Web 应用程序，攻击者通过编写的 SQL 语句进行攻击，若应用程序没有过滤用户的输入数据，会使非法数据侵入系统。

SQL 注入可以分为平台层注入和代码层注入。前者由不安全的数据库配置或数据库平台的漏洞所致; 后者主要是由于程序员对输入未进行细致地过滤，从而执行了非法的数据查询。基于此，SQL 注入的产生原因通常表现在以下几方面:

1.不当的类型处理。

2.不安全的数据库配置。

3.不合理的查询集处理。

4.不当的错误处理。

5.转义字符处理不合适。

6.多个提交处理不当。

（四）针对共识机制的攻击

共识协议是区块链的重要组成部分，在生成区块时需要依赖于区块链的共识机制来选择矿工打包区块，目前主要的共识协议攻击手段有双花攻击、自私挖矿及女巫攻击等。

1.双花攻击

双花攻击针对工作量证明机制，指的是攻击者通过某种方式拥有区块链全网络一半以上的算力，并通过其算力让区块链产生分叉，从而引导主链走向改变的攻击方法。

2.自私挖矿

自私挖矿指攻击者在计算出新区块时，不将其发现的新区块广播给区块链中的其他节点，继续挖新区块的下一个区块，直到其他挖矿者挖到有效区块时，攻击者将先前挖到但未广播给其他节点的所有区块公开。因为攻击者已经成功发送多个连续区块，所以攻击者所在的链分支比其他分支更长，从而使得区块链主链走向由攻击者控制。

3.女巫攻击

区块链网络中，一个恶意节点可以具有多重身份。女巫攻击

是指恶意节点通过利用少数节点控制多个虚假身份，从而利用这些身份控制或影响网络的大量正常节点的攻击方式。

（五）智能合约安全漏洞

智能合约是区块链的重要组成部分，由于智能合约的编写依赖于开发人员的主观性，使得智能合约代码存在很多漏洞。常见的智能合约漏洞主要为重入漏洞、整数溢出漏洞、变量混淆漏洞、拒绝服务漏洞及随机数生成漏洞等。

1.重入漏洞

在区块链交互功能操作非常复杂的情况下，通常需要进行合约调用合约的操作，一旦多个合约相互调用的关系变得复杂，则可能会出现代码重入问题，即在某个时刻调用方法中断以至于执行其他的合约代码时，合约代码又再次调用了该发生中断方法。攻击者利用代码重入问题，使程序反复执行攻击者的恶意代码，以从中获利。

2.整数溢出漏洞

整数溢出是由于计算机中整数具有上限和下限，如果一个整数超过其上限或者小于其下限，该整数就会发生溢出，攻击者在合约进行转账过程中利用该漏洞实现无偿获取货币的目的。

3.变量混淆漏洞

变量混淆漏洞是由于合约开发人员在开发过程中，混淆合约语言变量发生的错误。

4.拒绝服务漏洞

拒绝服务漏洞就是攻击者通过某种手段让某些代码逻辑执

行失败，以这种方式持续消耗调用合约需要的资源。

5.随机数生成漏洞

安全的随机数的生成具有不可预测性，若合约中采用的随机数生成算法结果可预测，攻击者可以利用该漏洞在使用随机数设计的代码逻辑部分预先计算出执行结果，为后续业务的执行埋下安全隐患。