1. 区块链技术，又称分布式共享记账技术，具有去中心化与分布式存储的特点。区块链是由多个区块组成的链状结构，每个区块包含区块头和区块体两部分。区块头存储上一个区块的哈希值（preHash）、本区块体的哈希值（Hash）和时间戳等信息，区块体存储本区块的行为记录、交易信息或其他数据信息等内容。区块与Hash一一对应，本区块的Hash与下一区块的preHash相等。区块链技术通过点对点通信、共识机制、加密算法、等技术构建数据链，其不可篡改、可溯源、自治理的特性使之成为“构建信任的机器”[1]。
2. 智能合约是一种数字定义的协议，以计算机交易协议和数字形式控制的物理实体作为信任载体，可以高效自动履行合约并创建智能资产。智能合约无需中介，可自我验证并自动执行合约[2]。运行在区块链上的智能合约具有去中心化、不可篡改、匿名可溯源等特性，其实际应用价值在实践中得到验证。
3. 由于区块链技术的去中心化、匿名性、结构复杂、安全等级参差不齐、不可篡改等特性，使得针对区块链智能合约安全漏洞的攻击实施成本低、难追踪、难监管，传统的入侵检测、防火墙等网络安全技术不能很好地适用于智能合约交易环境，一旦攻击成功将造成无法挽回的损失[5]。
4. 智能合约安全可以分为链上安全和链外安全，其中链上安全包括智能合约与区块链内部要素交互过程中的安全问题，如架构安全、代码安全、运行安全等，链外安全包括智能合约与链外数据交互过程中的安全问题，如数据安全等[6]。基于智能合约程序和传统程序的区别，可以将智能合约链上安全分为三个层面：高级语言层面、虚拟机层面、区块链层面。其中高级语言层面与语言设计模式和代码质量有关，如变量覆盖、整数溢出、未校验返回值、任意地址写入、拒绝服务、未初始化变量、资产冻结、影子变量等。虚拟机层面与字节码规范和运行机制有关，如重入、代码注入、短地址攻击、不一致性攻击等。区块链层面与区块链运行平台有关，如时间戳依赖、条件竞争、随机性不足等[7]。目前爆出的安全漏洞多产生于高级语言层面和虚拟机层面，针对智能合约代码安全的研究是提高合约安全性的重要手段之一。