

فهرست مطالب

صفحه	عنوان
۸	پیشگفتار
۹	درباره نویسنده
۱۰	هشدار قانونی
۱۳	❖ فصل ۱: قراردادهای هوشمند
۱۳	مفاهیم پایه‌ای قراردادهای هوشمند
۱۳	تعریف قراردادهای هوشمند
۱۴	تاریخچه قراردادهای هوشمند
۱۴	ویژگی‌ها و عملکرد قراردادهای هوشمند
۱۵	مزایای قراردادهای هوشمند
۱۵	معایب و چالش‌ها
۱۶	انواع حملات و آسیب‌های امنیتی در قراردادهای هوشمند
۱۶	حملات تزریق کد (Code Injection)
۱۶	حملات بازگشتی (Reentrancy Attacks)
۱۷	حملات عدم دسترسی (Access Control Attacks)
۱۷	حملات سرریز حافظه (Buffer Overflow)
۱۸	حملات سوءاستفاده از زمان (Time Manipulation Attacks)
۱۸	حملات Underflow و Overflow
۱۸	حملات Front-running
۱۹	حملات DoS (Denial of Service)
۱۹	حملات Sybil
۲۰	حملات به داده‌های اوراکل‌ها (Oracle Attacks)
۲۰	حملات Flash Loan و شیوه‌های جلوگیری از آن
۲۰	حملات ۵۱٪ و نحوه محافظت از قراردادها
۲۱	حملات استفاده از آسیب‌پذیری‌ها در کدهای قراردادهای هوشمند
۲۱	نمونه‌هایی از آسیب‌پذیری‌ها:
۲۱	حمله به پارتیتی و مشکلات آن
۲۲	حمله به شبکه‌های DeFi و نحوه وقوع آن
۲۲	آسیب‌پذیری‌های ناشی از ورودی‌های نادرست
۲۳	آسیب‌های رایج در کدهای هوشمند
۲۳	اشتباهات در مدیریت وضعیت (State Management Errors)

۲۳	استفاده نادرست از ذخیره‌سازی (Storage Issues)
۲۴	عدم اعتبارسنجی ورودی‌ها (Lack of Input Validation)
۲۴	استفاده از توابع غیر ایمن (Unsafe Function Usage)
۲۵	نقص در کنترل دسترسی (Access Control Vulnerabilities)
۲۵	چالش‌های مدیریت و نظارت بر قراردادهای هوشمند
۲۵	نظارت بر عملکرد قراردادهای هوشمند
۲۶	مدیریت تغییرات و ارتقاء قراردادهای هوشمند
۲۶	چالش‌های مدیریت دسترسی و نقش‌ها
۲۷	نظارت بر تطابق با مقررات و قوانین
۲۷	شبیه‌سازی و آزمایش قراردادهای هوشمند
۲۸	ملاحظات امنیتی در طراحی قراردادهای هوشمند
۲۸	تحلیل و طراحی قراردادهای ایمن
۲۸	استفاده از ابزارهای تست و شبیه‌سازی
۲۹	ایجاد پروتکل‌های امنیتی برای مدیریت دسترسی
۲۹	نظارت و ارتقاء امنیت قراردادهای هوشمند
۲۹	به‌روزرسانی و patch کردن قراردادهای هوشمند
۳۰	Audits و بررسی امنیت قراردادهای هوشمند
۳۰	مفهوم Audits در قراردادهای هوشمند
۳۰	اهمیت بررسی‌های امنیتی قبل از استقرار
۳۱	روش‌ها و ابزارهای تحلیل امنیتی
۳۱	فرآیند انجام امنیتی قراردادهای هوشمند
۳۲	مراقبت‌های پس از استقرار قراردادهای هوشمند
۳۲	بهترین شیوه‌های نوشتن قراردادهای هوشمند امن
۳۲	الگوهای طراحی امن برای قراردادهای هوشمند
۳۳	مفهوم استفاده از استانداردها در توسعه قراردادهای هوشمند
۳۳	روش‌های جلوگیری از اشتباهات رایج در برنامه‌نویسی قراردادهای هوشمند
۳۴	استفاده از کتابخانه‌ها و ابزارهای معتبر برای کاهش خطرات امنیتی
۳۴	استراتژی‌های به‌روزرسانی و نگهداری قراردادهای هوشمند
۳۴	تکنیک‌های شبیه‌سازی و آزمایش در امنیت قراردادهای هوشمند
۳۵	مفهوم شبیه‌سازی در قراردادهای هوشمند
۳۵	ابزارهای شبیه‌سازی قراردادهای هوشمند
۳۶	تست‌های امنیتی متداول در قراردادهای هوشمند
۳۶	استفاده از شبکه‌های تست (Testnets) برای آزمایش قراردادها
۳۶	اهمیت انجام آزمایش‌های توزیع‌شده و شبیه‌سازی حملات

۳۷	قراردادهای هوشمند و حریم خصوصی
۳۷	چالش‌های حریم خصوصی در قراردادهای هوشمند
۳۸	مکانیزم‌های حفظ حریم خصوصی در بلاک‌چین
۳۸	استفاده از Zero-Knowledge Proofs (ZKPs) در قراردادهای هوشمند
۳۸	مزایای ZKPs در قراردادهای هوشمند
۳۹	حریم خصوصی در DeFi و شبکه‌های مالی
۳۹	راهکارهای آینده در حفظ حریم خصوصی در قراردادهای هوشمند
۴۰	آینده قراردادهای هوشمند و چالش‌های آن
۴۰	پیشرفت‌های فناوری و تأثیر آن بر قراردادهای هوشمند
۴۰	چالش‌های مقیاس‌پذیری در قراردادهای هوشمند
۴۱	توسعه‌های آینده در امنیت قراردادهای هوشمند
۴۲	روندهای آینده در حریم خصوصی و مقررات
۴۲	چشم‌انداز قراردادهای هوشمند در صنعت‌های مختلف
۴۳	رابطه قراردادهای هوشمند و اینترنت اشیا (IoT)
۴۳	روندهای قانونی و مقرراتی در زمینه قراردادهای هوشمند
۴۳	آینده بلاک‌چین و قراردادهای هوشمند در دنیای غیرمتمرکز
۴۴	قراردادهای هوشمند و تأثیر آن‌ها بر دنیای مالی
۴۴	نقش قراردادهای هوشمند در سیستم‌های مالی غیرمتمرکز (DeFi)
۴۵	استفاده از قراردادهای هوشمند در پرداخت‌های بین‌المللی
۴۶	تأثیر قراردادهای هوشمند بر امنیت و شفافیت تراکنش‌های مالی
۴۶	چالش‌های حقوقی و مالی در پذیرش قراردادهای هوشمند
۴۷	چند راهکار برای حفاظت از قراردادهای هوشمند
۴۷	استفاده از Audits برای امنیت قراردادها
۴۷	استفاده از روش‌های رمزنگاری در قراردادهای هوشمند
۴۸	استفاده از کدهای امن و استاندارد در توسعه قراردادها
۴۸	آموزش و آگاهی از آسیب‌پذیری‌های امنیتی برای توسعه‌دهندگان
۴۹	سیستم‌های شناسایی و پیشگیری از حملات
۴۹	تأثیرات حملات بر بازار ارزهای دیجیتال و قراردادهای هوشمند
۴۹	تأثیر حملات امنیتی بر قیمت ارزهای دیجیتال
۵۰	نقش حملات در تغییرات در اعتماد کاربران به قراردادهای هوشمند
۵۰	واکنش‌های جامعه و پروژه‌ها به حملات
۵۱	بررسی حملات بزرگ و اثرات بلندمدت آن‌ها بر اکوسیستم
۵۱	آینده و چالش‌های امنیتی بازار ارزهای دیجیتال

◆ فصل ۲: انواع متدهای هک ۵۳
 صد و یک متد رایج هک دارایی های دیجیتال ۵۳

◆ فصل ۳: بررسی مهمترین توابع کد کانترکت ۷۳
 بررسی ۵۰ تابع مهم در کد کانترکت قراردادهای ERC-20 ۷۳
 ۱. totalSupply ۷۴
 ۲. balanceOf(address account) ۷۵
 ۳. transfer(address recipient, uint256 amount) ۷۷
 ۴. transferFrom(address sender, address recipient, uint256 amount) ۷۹
 ۵. approve(address spender, uint256 amount) ۸۱
 ۶. allowance ۸۳
 ۷. name ۸۴
 ۸. symbol ۸۶
 ۹. decimals ۸۷
 ۱۰. mint ۸۸
 ۱۱. burn ۸۹
 ۱۲. increaseAllowance ۹۰
 ۱۳. decreaseAllowance ۹۱
 ۱۴. owner ۹۳
 ۱۵. renounceOwnership ۹۵
 ۱۶. transferOwnership ۹۶
 ۱۷. pause ۹۸
 ۱۸. unpause ۱۰۱
 ۱۹. paused ۱۰۳
 ۲۰. blacklist ۱۰۵
 ۲۱. unblacklist ۱۰۸
 ۲۲. isBlacklisted ۱۱۰
 ۲۳. freeze ۱۱۱
 ۲۴. unfreeze ۱۱۴
 ۲۵. frozen ۱۱۵
 ۲۶. permit (EIP-2612) ۱۱۶
 ۲۷. nonces ۱۱۸
 ۲۸. DOMAIN_SEPARATOR ۱۲۰

۱۳۱.....	snapshot - ۳۹
۱۳۴.....	getCurrentSnapshotId - ۳۰
۱۳۷.....	getBalanceAtSnapshot ۳۱
۱۳۸.....	multicall ۳۲
۱۳۱.....	flashLoan تابع ۳۳
۱۳۵.....	withdraw ۳۴
۱۳۷.....	deposit ۳۵
۱۳۹.....	claim ۳۶
۱۴۱.....	delegate ۳۷
۱۴۴.....	delegates ۳۸
۱۴۶.....	getVotes ۳۹
۱۴۸.....	getPastVotes ۴۰
۱۴۹.....	metaTransaction ۴۱
۱۵۳.....	executeMetaTransaction ۴۲
۱۵۸.....	bridge ۴۴
۱۶۱.....	crossChainTransfer ۴۵
۱۶۳.....	upgradeTo ۴۶
۱۶۵.....	upgradeToAndCall ۴۷
۱۶۷.....	implementation ۴۸
۱۶۸.....	emergencyWithdraw ۴۹
۱۷۱.....	recoverERC20 ۵۰

◆ فصل ۴: توصیه‌های عملی برای امنیت دارایی‌های دیجیتال ۱۷۲

۱۷۲.....	بخش اول: امنیت پیش از خرید و سرمایه‌گذاری
۱۷۶.....	بخش دوم: امنیت در زمان نگهداری دارایی‌ها
۱۷۷.....	بخش سوم: امنیت در هنگام فروش و برداشت دارایی‌ها
۱۷۹.....	فهرست منابع