

امنیت

در

ارزهای دیجیتال

تالیف:

ابوالفضل صدقی آزاد

آراده کتاب

سرشناسه	: صدقی آزاد، ابوالفضل، ۱۳۵۰ -
عنوان و پدیدآور	: امنیت در ارزشهای دیجیتال / تألیف: ابوالفضل صدقی آزاد.
مشخصات نشر	: تهران، آراد کتاب،
مشخصات ظاهری	: ۱۸۲ ص،
شابک	: ۹۷۸-۶۰۰-۱۸۶-۷۵۲-۱
وضعیت فهرست نویسی	: فیبا
موضوع	: ارزشهای دیجیتال
موضوع	: بلاکچین (پایگاههای اطلاعاتی) - تدابیر ایمنی
موضوع	: پایگاههای اطلاعاتی - امنیت
رده بندی کنگره	: HG۱۷۱۰
رده بندی دیویی	: ۳۳۲/۴
شماره کتابخانه ملی	: ۱۰۲۹۳۰۶۳

امنیت در ارزشهای دیجیتال

تألیف: ابوالفضل صدقی آزاد	ناشر: آراد کتاب
نوبت چاپ: اول ۱۴۰۴	تیراژ: ۲۰۰ جلد
چاپ و صحافی: صدف	قیمت: ۲۶۵۰۰۰ تومان
شابک: ۹۷۸-۶۰۰-۱۸۶-۷۵۲-۱	

حق چاپ برای ناشر محفوظ است. کلیه حقوق و حق چاپ متن، طرح روی جلد و عنوان کتاب با نگرش به قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان مصوب ۱۳۴۸ برای انتشارات آراد کتاب محفوظ است و متخلفین تحت پیگرد قانونی قرار می‌گیرند.

مرکز پخش و فروش:

انتشارات آراد کتاب تلفن: ۰۶۶۹۷۵۲۸۵ - ۰۶۶۴۸۲۲۲۶ - ۰۹۳۵۳۰۶۲۴۵۸

خرید آنلاین از سایت: www.aradbook.com

فهرست مطالب

عنوان	صفحه
پیشگفتار.....	8
درباره نویسنده	9
هشدار قانونی	10
♦ فصل 1: قراردادهای هوشمند.....	13
مفاهیم پایه‌ای قراردادهای هوشمند	13
تعریف قراردادهای هوشمند	13
تاریخچه قراردادهای هوشمند	14
ویژگی‌ها و عملکرد قراردادهای هوشمند	14
مزایای قراردادهای هوشمند	15
معایب و چالش‌ها.....	15
انواع حملات و آسیب‌های امنیتی در قراردادهای هوشمند	16
حملات تزریق کد (Code Injection)	16
حملات بازگشتی (Reentrancy Attacks).....	16
حملات عدم دسترسی (Access Control Attacks)	17
حملات سرریز حافظه (Buffer Overflow)	17
حملات سوءاستفاده از زمان (Time Manipulation Attacks)	18
حملات Overflow و Underflow	18
حملات Front-running	18
حملات DoS (Denial of Service)	19
حملات Sybil	19
حملات به داده‌های اوراق‌ها (Oracle Attacks)	20
حملات Flash Loan و شیوه‌های جلوگیری از آن	20
حملات 51% و نحوه محافظت از قراردادها.....	20
حملات استفاده از آسیب‌پذیری‌ها در کدهای قراردادهای هوشمند	21
نمونه‌هایی از آسیب‌پذیری‌ها:.....	21
حمله به پاریتی و مشکلات آن	21
حمله به شبکه‌های DeFi و نحوه وقوع آن	22
آسیب‌پذیری‌های ناشی از ورودی‌های نادرست	22
آسیب‌های رایج در کدهای هوشمند	23
اشتباهات در مدیریت وضعیت (State Management Errors)	23

23	استفاده نادرست از ذخیره‌سازی (Storage Issues)
24	عدم اعتبارسنجی ورودی‌ها (Lack of Input Validation)
24	استفاده از توابع غیر ایمن (Unsafe Function Usage)
25	نقص در کنترل دسترسی (Access Control Vulnerabilities)
25	چالش‌های مدیریت و نظارت بر قراردادهای هوشمند
25	نظارت بر عملکرد قراردادهای هوشمند
26	مدیریت تغییرات و ارتقاء قراردادهای هوشمند
26	چالش‌های مدیریت دسترسی و نقش‌ها
27	نظارت بر تطابق با مقررات و قوانین
27	شبیه‌سازی و آزمایش قراردادهای هوشمند
28	ملاحظات امنیتی در طراحی قراردادهای هوشمند
28	تحلیل و طراحی قراردادهای ایمن
28	استفاده از ابزارهای تست و شبیه‌سازی
29	ایجاد پروتکل‌های امنیتی برای مدیریت دسترسی
29	نظارت و ارتقاء امنیت قراردادهای هوشمند
29	به‌روزرسانی و patch کردن قراردادهای هوشمند
30	Audits و بررسی امنیت قراردادهای هوشمند
30	مفهوم Audits در قراردادهای هوشمند
30	اهمیت بررسی‌های امنیتی قبل از استقرار
31	روش‌ها و ابزارهای تحلیل امنیتی
31	فرآیند انجام امنیتی قراردادهای هوشمند
32	مراقبت‌های پس از استقرار قراردادهای هوشمند
32	بهترین شیوه‌های نوشتن قراردادهای هوشمند امن
32	الگوهای طراحی امن برای قراردادهای هوشمند
33	مفهوم استفاده از استانداردها در توسعه قراردادهای هوشمند
33	روش‌های جلوگیری از اشتباهات رایج در برنامه‌نویسی قراردادهای هوشمند
34	استفاده از کتابخانه‌ها و ابزارهای معتبر برای کاهش خطرات امنیتی
34	استراتژی‌های به‌روزرسانی و نگهداری قراردادهای هوشمند
34	تکنیک‌های شبیه‌سازی و آزمایش در امنیت قراردادهای هوشمند
35	مفهوم شبیه‌سازی در قراردادهای هوشمند
35	ابزارهای شبیه‌سازی قراردادهای هوشمند
36	تست‌های امنیتی متداول در قراردادهای هوشمند
36	استفاده از شبکه‌های تست (Testnets) برای آزمایش قراردادها
36	اهمیت انجام آزمایش‌های توزیع‌شده و شبیه‌سازی حملات

37	قراردادهای هوشمند و حریم خصوصی
37	چالش‌های حریم خصوصی در قراردادهای هوشمند
38	مکانیزم‌های حفظ حریم خصوصی در بلاک‌چین
38	استفاده از Zero-Knowledge Proofs (ZKPs) در قراردادهای هوشمند
38	مزایای ZKPs در قراردادهای هوشمند
39	حریم خصوصی در DeFi و شبکه‌های مالی
39	راهکارهای آینده در حفظ حریم خصوصی در قراردادهای هوشمند
40	آینده قراردادهای هوشمند و چالش‌های آن
40	پیشرفت‌های فناوری و تأثیر آن بر قراردادهای هوشمند
40	چالش‌های مقیاس‌پذیری در قراردادهای هوشمند
41	توسعه‌های آینده در امنیت قراردادهای هوشمند
42	روندهای آینده در حریم خصوصی و مقررات
42	چشم‌انداز قراردادهای هوشمند در صنعت‌های مختلف
43	رابطه قراردادهای هوشمند و اینترنت اشیا (IoT)
43	روندهای قانونی و مقرراتی در زمینه قراردادهای هوشمند
43	آینده بلاک‌چین و قراردادهای هوشمند در دنیای غیرمتمرکز
44	قراردادهای هوشمند و تأثیر آن‌ها بر دنیای مالی
44	نقش قراردادهای هوشمند در سیستم‌های مالی غیرمتمرکز (DeFi)
45	استفاده از قراردادهای هوشمند در پرداخت‌های بین‌المللی
46	تأثیر قراردادهای هوشمند بر امنیت و شفافیت تراکنش‌های مالی
46	چالش‌های حقوقی و مالی در پذیرش قراردادهای هوشمند
47	چند راهکار برای حفاظت از قراردادهای هوشمند
47	استفاده از Audits برای امنیت قراردادها
47	استفاده از روش‌های رمزنگاری در قراردادهای هوشمند
48	استفاده از کدهای امن و استاندارد در توسعه قراردادها
48	آموزش و آگاهی از آسیب‌پذیری‌های امنیتی برای توسعه‌دهندگان
49	سیستم‌های شناسایی و پیشگیری از حملات
49	تأثیرات حملات بر بازار ارزهای دیجیتال و قراردادهای هوشمند
49	تأثیر حملات امنیتی بر قیمت ارزهای دیجیتال
50	نقش حملات در تغییرات در اعتماد کاربران به قراردادهای هوشمند
50	واکنش‌های جامعه و پروژه‌ها به حملات
51	بررسی حملات بزرگ و اثرات بلندمدت آن‌ها بر اکوسیستم
51	آینده و چالش‌های امنیتی بازار ارزهای دیجیتال

◆ فصل 2: انواع متدهای هک 53

53 صد و یک متد رایج هک دارایی های دیجیتال

◆ فصل 3: بررسی مهمترین توابع کد کانترکت 73

73 بررسی 50 تابع مهم در کد کانترکت قراردادهای ERC-20

74 1. totalSupply

75 2. balanceOf(address account)

77 3. transfer(address recipient, uint256 amount)

79 4. transferFrom(address sender, address recipient, uint256 amount)

81 5. approve(address spender, uint256 amount)

83 6. allowance

84 7. name

86 8. symbol

87 9. decimals

88 10. mint

89 11. burn

90 12. increaseAllowance

91 13. decreaseAllowance

93 14. owner

95 15. renounceOwnership

96 16. transferOwnership

98 17. pause

101 18. unpause

103 19. paused

105 20. blacklist

108 21. unblacklist

110 22. isBlacklisted

111 23. freeze

114 24. unfreeze

115 25. frozen

116 26. permit (EIP-2612)

118 27. nonces

120 28. DOMAIN_SEPARATOR

121.....	snapshot – 29
124.....	getCurrentSnapshotId – 30
127.....	getBalanceAtSnapshot .31
128.....	multicall .32
131.....	flashLoan تابع .33
135.....	withdraw .34
137.....	deposit .35
139.....	claim .36
141.....	delegate .37
144.....	delegates .38
146.....	getVotes .39
148.....	getPastVotes .40
149.....	metaTransaction .41
153.....	executeMetaTransaction .42
158.....	bridge .44
161.....	crossChainTransfer .45
163.....	upgradeTo .46
165.....	upgradeToAndCall .47
167.....	implementation .48
168.....	emergencyWithdraw .49
171.....	recoverERC20 .50

◆ فصل 4: توصیه‌های عملی برای امنیت دارایی‌های دیجیتال 173

173.....	بخش اول: امنیت پیش از خرید و سرمایه‌گذاری
176.....	بخش دوم: امنیت در زمان نگهداری دارایی‌ها
177.....	بخش سوم: امنیت در هنگام فروش و برداشت دارایی‌ها
179.....	فهرست منابع