交易系统安全性分析

> **文档定位**：本文是 Quantum Dream Fund I（QDFI）/ NovaMarket 交易与结算系统的**端到端安全性分析**，覆盖链上合约、链下执行/签名服务、平台与 API 三层。面向安全评审、第三方审计准备与主网上线决策。
>
> **状态**：Phase 1（Arbitrum Sepolia 测试网），待第三方审计。本文为内部安全分析，非投资要约，亦非审计结论。
>
> **关联文档**：`docs/08_SECURITY.md`（安全策略与检查表）· `qdf-contracts/audit-package/AUDIT.md` + `INVARIANTS.md` · `fund-platform/docs/FUND_CUSTODY_SEPARATION_AND_SECURITY.md` + `AUDIT_READINESS.md` + `SELF_AUDIT_REPORT.md`。
>
> **最后更新**：2026-06（基于当时代码侦察）。代码会演进，引用文件/函数请以仓库当前状态为准。

1. 摘要（Executive Summary）

QDFI / NovaMarket 交易系统采用 **「链上托管 + 链下执行」职责分离** 架构：投资者资金锁定在链上合约（FundVault / CapitalPool），交易在中心化场馆（Hyperliquid / Polymarket / Uniswap）由隔离的链下服务执行，链上仅通过受限接口划拨额度、记账盈亏，并用多签预言机回写净值。

总体评级：架构设计**中上**，纵深防御要素到位（多签 + 时间锁 + Guardian 暂停 + 提款限额 + 熔断 + 凭证密封 + 权限最小化）。核心残余风险集中在**离链信任**与**密钥单点**两处。

最高风险（按严重度）：

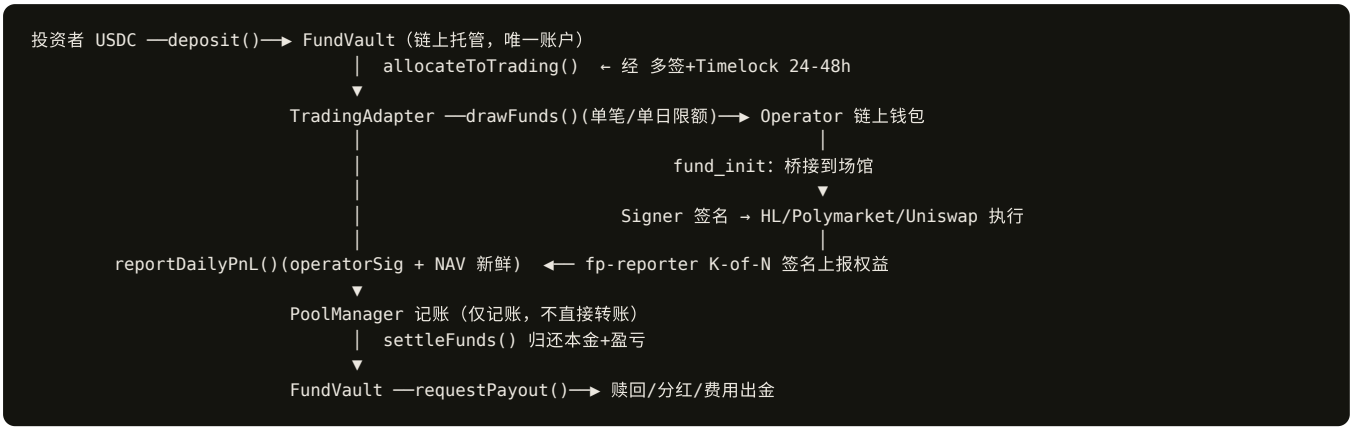
#	风险	层	严重度	现状
R-1	NAV/权益预言机签名人串谋伪报净值	链上+链下	🔴严重	K-of-N 多签 + 偏离熔断缓解；测试网为 Mock ZK PoR
R-2	Signer 进程被攻破 / `FP_CREDENTIAL_SECRET_KEY` 泄露 → 全部场馆私钥失守	链下	🔴严重	内网隔离 + 内存不落盘；待 KMS/HSM + 高可用
R-3	治理多签私钥失守（测试网为明文测试地址）	链上	🟠高（测试网）	主网前须切 Gnosis Safe / 机构托管
R-4	Keeper 单点故障致结算/赎回队列停滞	链下	🟠高	需冗余 + 监控告警
R-5	管理员认证仅单一 API Key（无 hash/2FA/RBAC）	平台	🟠中高	待升级账号体系

关键结论：在测试网阶段安全设计合理；**主网上线前必须完成**第三方合约审计、密钥托管迁移（HSM/KMS + Gnosis Safe）、真实 ZK PoR 电路、Signer 高可用、管理员认证加固（见 §10 检查表）。

2. 系统范围与架构总览

2.1 三层架构

2.2 核心资金流与信任边界



信任边界要点:

- **资金托管 vs 交易执行分离**：链上合约托管资金，链下服务执行交易；二者通过 `TradingAdapter` 的限额接口连接，离链服务**无法绕过限额直接动用金库**。
- **drawFunds 之后资金在链外**：这是 custody/execution 的核心边界。`FundVault._deployed[asset]` 记账「已划拨未归还」，真实盈亏由 reporter 多签上报兑现——**这是最大的离链信任假设**（见 R-1）。

3. 信任模型与角色

角色	持有的密钥/凭证	权限	失守影响	缓解
投资者	自有钱包私钥	申购/赎回/领分红（链上自助）	自负	非托管；30 天锁定 + 赎回 T+3
Operator 操盘手	`FP_OPERATOR_PRIVATE_KEY`	`drawFunds` / `returnFunds`、发下单指令	受链上单笔/单日限额 + 熔断约束	限额、首损保证金、KMS
平台 Web	`NM_CREDENTIAL_PUBLIC_KEY`（**仅公钥**）、会话密钥	存/显示凭证状态、记账	**无法解密凭证**；Web 失守仅泄露密文（无用）	公私钥分离（关键设计）
Executor 执行器	`FP_CREDENTIAL_SECRET_KEY`（解密用）	解密凭证、调 Signer、读权益	可解开全部场馆凭证	内网隔离、KMS、内存不落盘
Signer 签名器	全部场馆私钥 + 解密密钥（内存）	签下单/转账/初始化	**单点失陷 → 资金全失**	localhost 绑定、KMS/HSM、高可用（待）

角色	持有的密钥/凭证	权限	失守影响	缓解
Reporter 报告器	`FP_REPORTER_PRIVATE_KEYS`（K-of-N）	多签上报权益/NAV	单签泄露不足以伪报	K-of-N（现 3-of-N）、偏离上限
Keeper 结算器	`FP_KEEPER_PRIVATE_KEY`	触发 `dailyTick` / `processQueue`（仅 gas）	权限最小，不动资金	链上条件 gate；permissionless 设计
治理多签	QDFMultiSig 5/9 owner	经 Timelock 改参数/角色	多签阈值保护	主网切 Gnosis Safe
Guardian	GUARDIAN_ROLE（5/9 多签）	**实时**暂停、冻结赎回	可恶意暂停（DoS），但不能盗资金	「暂停易、恢复难」（恢复经 Timelock）
KYC Admin	KYC_ADMIN_ROLE 多签	白名单/辖区屏蔽	可错误放行/阻断	链上无 PII；多签

信任最小化设计：Web「只加密不解密」、Reporter K-of-N、Keeper permissionless+限额、Guardian 只能暂停不能转账——这四点把单点权力切小。**剩余集中点**：Signer（明文私钥单进程）与 NAV 预言机（离链真实性）。

4. 链上合约层安全

> 仓库：`qdf-contracts/`（12 核心 + 治理，约 1,879 行 Solidity）；测试 97 passed，行覆盖 90.1%、分支 61.9%。NovaMarket 侧合约见 `fund-platform`（CapitalPool / PoolSettlement / NAVReporter，Foundry invariant 测试）。

4.1 资金托管 — FundVault（`contracts/core/FundVault.sol`）

- **唯一 USDC/USDT 托管账户**；所有子系统经 `requestPayout()`（`onlyAuthorized`）出金。
- 划拨交易：`allocateToTrading()`（GOVERNANCE_ROLE，经 Timelock）↑ `_deployed[asset]`；`returnFromTrading()`（仅 TRADING_ADAPTER_ROLE）↓。
- **防护**：ReentrancyGuard（3 函数）、SafeERC20 全覆盖、CEI。
- **缺口**：**无 first-loss 保证金层**（账户级隔离，交易亏损直接侵蚀本金）；GOVERNANCE_ROLE 单点出金权——靠 Timelock 24-48h 制约。
- 注：NovaMarket 侧 `FirstLossPolicy` 有首损瀑布（operator margin 先吸收亏损），与 QDFI FundVault 模型不同。

4.2 交易边界 — TradingAdapter（`contracts/core/TradingAdapter.sol`）「三铁律」

1. **资金权**：`drawFunds()`（onlyOperator）受 `maxDrawPerTx`（Sepolia 1M USDC）+ `dailyDrawLimit`（3M）约束，按 `block.timestamp/1 days` 重置日累计。
2. **回报权**：`reportDailyPnL()` 要求 operator 对 `(chainid, this, epoch, pnl)` 的 ECDSA 签名，且 NAV 须本 epoch + 26h 内新鲜；**仅记账不转账**（调 `poolManager.settleDailyPnL()`）。
3. **交叉校验/熔断**：`|pnl| > AUM * maxDailyPnLBps`（Sepolia 20%）→ `emergency.pause(ALL)`。
   - **防护**：digest 含 chainId 防跨链重放；ReentrancyGuard。
   - **风险**：单链内无 nonce，同 epoch 同 PnL 理论可重复上报（依赖 Keeper 幂等）；`tradingOperator` 单地址，私钥泄露可在限额内领/还资金。

4.3 净值预言机 — NAVOracle（`contracts/core/NAVOracle.sol`）/ NAVReporter（NovaMarket）

- **3-of-3 签名**（托管行 + 审计方 + Chainlink，须互异）对 `(chainid, this, epoch, navPerShare, totalAUM, porProofHash)`；**ZK 储备证明 PoR**；相邻 epoch 偏离 > 2% → 熔断（需 GOVERNANCE `resumeAfterDeviation`）。
- NovaMarket NAVReporter：**K-of-N 多签**（签名排序去重）+ epoch 严格递增（`NoFreshReport`）+ `maxDeviationBps` 偏离上限 + chainId 防重放。
- ⚠️ **测试网为 `MockZKVerifier`**；生产需真实 ZK 电路并审计。
- **风险（R-1，严重）**：验证人串谋可伪造任意净值 → 申购高估/赎回低估；NAV 停滞 > 26h 则申赎瘫痪（可用性）。

4.4 应急与风控 — EmergencyController（`contracts/core/EmergencyController.sol`）

- 模块化暂停：SUBSCRIPTION / REDEMPTION / DIVIDEND / TRADING / ALL。
- **双权力**：`pause()` 由 Guardian（5/9）**实时**触发；`unpause()` 须 GOVERNANCE 经 Timelock（24h）——「暂停易、恢复难」。
- 风控等级：NORMAL → HALT_NEW_TRADE（日 -3%）→ FULL_LIQUIDATION（日 -5%）→ DAO_VOTE（月 -10%）。Guardian 可冻结赎回 ≤7 天。

4.5 申购 / 赎回

- **Subscription**（`SubscriptionManager.sol`）：KYC + 稳定币白名单 + 最低 10,000 USDC + NAV 新鲜，按当日 NAV 即时铸份额并锁定 30 天。
- **Redemption**（`RedemptionManager.sol`）：两阶段（入队 → Keeper `processQueue`）；**T+3 结算延迟、单日 ≤ AUM 10%**（首笔始终放行防死锁）、**阶梯赎回费**（<90d 2% / 90-180d 1% / ≥180d 0%，费入梦想储备 Pool C）。
- **设计意图**：30 天锁定 + T+3 + 单日上限 = 给净值操纵留检测窗口、防挤兑。**风险**：极端行情下赎回队列可能阻塞（部分用户延迟超一周）。

4.6 份额代币 — QDFToken（`contracts/core/QDFToken.sol`）

- ERC20（6 位精度）+ **FIFO Lot 机制**（每笔申购一个带锁定期 Lot）；转账须目标 KYC 通过 + 足额未锁定份额。
- **风险（K-2）**：Lot 队列 O(n) 迭代，单地址申购数千次可能 gas OOM（AUDIT.md 待整改：Lot 上限/合并）。

4.7 治理 — QDFMultiSig (5/9) → QDFTimelock (24-48h)

- 所有 GOVERNANCE 改参/改角色经 5/9 多签提案 → Timelock 延迟 → 执行；紧急 `pause` **不经** Timelock。
- **风险（R-3）**：测试网 9 个签名人私钥在 `keys/multisig-signers.json`（明文测试地址）——**主网前必须切 Gnosis Safe / 机构托管**（AUDIT.md K-4）。

4.8 重入与安全模式矩阵

合约	ReentrancyGuard	SafeERC20	CEI
FundVault / TradingAdapter / Subscription / Redemption / Dividend	✓	✓	✓
NAVOracle / PoolManager / EmergencyController	（仅状态写，无外部转账）	N/A	✓
QDFToken	（ERC20 无重入点）	✓	✓
FeeManager	依赖 FundVault 的 Guard	⚠️ 外部调用 FundVault	⚠️

链上不变量（Foundry/INVARIANTS.md）：资金守恒 `cashInvestor + marginStaked + marginForfeited + surplus == poolBalance`、份额-NAV 一致、净值单调、治理约束、分红单次、暂停回滚。

5. 链下执行与密钥安全

> 服务：`fund-platform/services/`（Python）：executor / signer / keeper / reporter / risk_engine / connectors / fund_init。

5.1 执行流程与原子性

- **fp-executor**（`services/executor/server.py`）每 ~30s 轮询每池 PENDING 订单，`UPDATE ... FOR UPDATE SKIP LOCKED` **原子声明**（防重复处理），逐单执行（place/flatten/cancel）→ `mark_result` 写回 venueOrderId/raw。
- **fp-keeper** ~600s 扫结算条件触发链上 `dailyTick`；**fp-reporter** 读场馆权益、K-of-N 签名上报；**fp-risk** 实时监控超阈值 → `flatten` + `pause`。

5.2 场馆集成（Hyperliquid / Polymarket / Uniswap）

- **隔离签名模式**（生产）：executor **无私钥**，经 HTTP 调 Signer（`/hl-order`、`/sign-and-post` 等）；私钥永不离开 Signer 进程。本地签名模式仅 dev fallback。
- **Hyperliquid**：main wallet（持资金/可提）+ agent wallet（`approve_agent` 授交易权、**无提取权**）。
- **Polymarket**：CCTP 跨链（Arbitrum→Polygon 原生 USDC）→ funder 钱包；EIP-712 下单。
- **桥接限额护栏**：`FP_BRIDGE_MAX_USDC6_PER_TX/PER_DAY`、`FP_VENUE_MAINNET_ENABLED=false`、`FP_POLYMARKET_MAINNET_ENABLED=false`（真实资金开关默认关）。

5.3 凭证密封（Sealed-Box）— 关键设计

- **X25519 sealed-box**（Web `tweetnacl-sealedbox-js` ↔ Python `PyNaCl SealedBox`，libsodium 标准 X25519 + XSalsa20-Poly1305）。
- 流程：操盘手在 Web 输入场馆 API key/私钥 → `sealSecret()` 用**公钥**密封 → 存 `VenueCredential.sealed`（Web 永不 SELECT 回明文）→ Executor/Signer 用**私钥** `unseal()` 解密，**仅存内存**，tick 结束丢弃。

- **信任模型**：Web 持公钥**无法解密**；Web 漏洞只能泄露无用密文。
- **已知坑**：`libsodium-wrappers` 在 Turbopack 打包损坏 → 必须用纯 JS 的 `tweetnacl-sealedbox-js`（已规避，记于 `08_SECURITY.md §3.2`）。

5.4 密钥来源与落盘

- `resolve_secret()`（`services/common/config.py`）支持 `plain`（仅 dev）/ `env:` / `file:`（chmod 600）/ `awskms:` / `vault:`。
- Signer（`signer/store.py`）：首次 `/keygen` 生成 EOA → 立即密封存库 → 仅内存缓存；唯一持明文私钥的进程。
- **主网约束**（`08_SECURITY.md §2.1`）：所有 `*_PRIVATE_KEY` 禁明文 .env，改 KMS/Vault/HSM；K-of-N reporter key 分散不同主机；NAV verifier → HSM/冷钱包。

5.5 网络暴露

服务	监听	暴露	风险	缓解
Signer	127.0.0.1:8088	仅内网	HTTP 无认证	localhost 绑定 + 私网/VPN/mTLS（待）
Executor/Keeper/Reporter/Risk	无入站	出站 DB+RPC+场馆	—	防火墙 + VPC 隔离 + RPC TLS

5.6 注入与重放防护

- **SQL**：asyncpg/Prisma 全参数化，**无注入面**。
- **命令注入**：无 shell/subprocess 拼接。
- **订单重放**：`Order.clientOrderId @unique`（Web 幂等，重复 409）；场馆 SDK 内置 nonce/timestamp。
- **权益上报重放**：digest 含 chainId（防跨链）+ epoch 严格递增 + 偏离上限。

5.7 链下风险

风险	影响	严重度	缓解
`FP_CREDENTIAL_SECRET_KEY` 泄露	解密全部场馆凭证	🔴严重	KMS/HSM、访问控制、审计日志
Signer 被攻破（R-2）	资金全失	🔴严重	内网隔离、HSM、高可用、审计日志
`sealed` 列泄露（DB）	该场馆下单/提取	🔴严重	PG TLS+密码+IP 白名单、备份加密
Reporter 单签泄露	不足以伪报（K-of-N）	🟠高	K-of-N、HSM、异常侦测
Operator key 泄露	限额内 draw	🟠高	链上限额+熔断、KMS、轮换
`.env` 误入 git	全私钥暴露	🔴严重	.gitignore、secret scanner、CI 门禁

6. 平台与 API 层安全

> `qdf-platform`（api.fstar.io / app.quantumdream.fund）与 `fund-platform/web`（NovaMarket）。

6.1 认证

- **SIWE（钱包登录）**：nonce（qdf 10min TTL；NovaMarket 持久化 DB `authNonce` 单次消费 + `updateMany` 防竞态）→ `SiweMessage.verify()` → HS256 JWT（qdf 24h cookie `qdf_session`；NovaMarket 7d，cookie `nm_session` + Bearer 移动端）。cookie 均 httpOnly + secure + SameSite=lax。
- **管理员（qdf）**：单一 `ADMIN_API_KEY` **明文字符串比较** → HS256 JWT 8h（cookie `qdf_admin`）。**风险（R-5）**：无 hash/salt、无 2FA、无 RBAC（所有 admin 等权）。

6.2 授权 — 链上为最终权限源

- NovaMarket `requireOperator()`（`web/src/lib/auth/requireOperator.ts`）：解析 caller（Bearer/JWT/cookie）→ API key pool scope 校验 → **读链上** `CapitalPool.operator()` 比对 → 不符 403。凭证/账户/策略类写操作**仅允许 session（不允许 API key）**。
- **薄弱点**：qdf 管理员无 RBAC；NovaMarket API key `scopes.pools` 可选，空 scope 默认全部池。

6.3 托管模型

- **QDFI（qdf-platform）**：**非托管**——资金在链上 FundVault/ERC-4626，平台仅记录链上事件 + KYC；无用户私钥。
- **NovaMarket**：投资者资金锁 CapitalPool（合约控制）；交易凭证 sealed-box（Web 无解密权）→ **凭证非托管 + 资金合约托管**，操盘手无权直接触碰投资者资金。

6.4 输入校验 / 限流 / CORS / 错误

- **Zod 全覆盖**（body/query/param），钱包地址 `/^0x[0-9a-fA-F]{40}$/`、BigInt `^\d+$` 防溢出；**Prisma ORM 无原生 SQL**。
- **限流不全面**：仅 `/api/reservations` 按 email 限流（1h 5 次）；**登录/下单/赎回等无限流**（待补，R-级中）。
- **CORS**：白名单明确（fstar.io / app.quantumdream.fund；novamarket.io），但存在 `*` fallback——NovaMarket 对 POST/DELETE 建议移除 fallback。
- **CSRF**：靠 SameSite=lax + Bearer（无 cookie 自动发送）；交易端点无显式 CSRF token。
- **错误**：多为通用信息；部分端点回 `zod.issues`（泄露字段名，不含敏感数据）。

6.5 关键交易类端点（节选）

平台	端点	方法	鉴权	风险
qdf	`/api/admin/nav/publish`	POST	admin session	中（关键财务）
qdf	`/api/admin/login`	POST	`ADMIN_API_KEY`	中高（无 hash/2FA）
qdf	`/api/me/redemptions/quote`	GET	session	低
NM	`/api/pools/[addr]/credentials`	POST	operator + **session only**	中高（敏感凭证）
NM	`/api/pools/[addr]/orders`	POST/DELETE	operator	中（交易执行）
NM	`/api/pools/[addr]/accounts/provision`	POST	operator + session only	高（生成密钥）

6.6 部署 / 运维

- pm2（`manzi-web` / `novamarket-web` 127.0.0.1:3105、qdf-platform `/opt/apps/qdf-platform`）+ nginx SSL 反代；Docker `node:22-alpine` 非 root（`adduser -S nextjs`）多阶段构建。
- Postgres 16 本地 127.0.0.1:5432；`NEXT_PUBLIC_*` 构建时内联（注意敏感值勿用该前缀）。
- **建议**：env 改密钥管理服务；DB 启 SSL + IP 白名单；SSH key-only。

7. 威胁模型与攻击面

威胁场景	攻击路径	现有控制	残余风险
预言机操纵	串谋伪报 NAV/权益 → 套利申赎	3-of-3 / K-of-N、偏离熔断、PoR、T+3	🔴串谋仍可（信任假设）；测试网 Mock PoR
密钥失窃	盗 Signer/解密密钥 → 签恶意订单/提款	内网隔离、内存不落盘、限额、首损	🔴Signer 单点；待 HSM+高可用
治理劫持	控制 ⩾5/9 多签 → 改角色/抽资金	多签 + Timelock 24-48h（留反应窗口）	🟠测试网明文 key（主网切 Safe）
可用性/DoS	Keeper 宕机、NAV 停滞、Guardian 恶意暂停	permissionless dailyTick、监控	🟠Keeper 单点、暂停 DoS
挤兑	大批赎回耗尽流动性	30d 锁定、T+3、单日 10% 上限	🟠队列阻塞致延迟
跨链桥	CCTP burn/mint 被篡改/卡单	Circle 标准、桥接限额护栏、mainnet 开关	🟠依赖 Circle Iris 可用性
重放	重放订单/上报	clientOrderId 唯一、chainId+epoch、SDK nonce	🟢低
Web 入侵	攻破 Web 层	公私钥分离（Web 无解密权）、链上鉴权	🟢仅泄密文/记账，盗不到资金
应用层	注入/越权/admin 弱认证	Zod、Prisma、链上权限源	🟠admin 无 2FA/RBAC、限流不全

8. 风险登记册（Risk Register）

ID	风险	层	严重度	可能性	缓解 / 状态
R-1	预言机签名人串谋伪报净值	链上+链下	🔴 严重	低	K-of-N+偏离熔断+PoR；主网需真实 ZK + 独立审计签名人
R-2	Signer 失陷 / 解密密钥泄露 → 资金全失	链下	🔴 严重	低-中	内网+内存不落盘；**待 HSM/KMS + 高可用 + 审计日志**
R-3	治理多签私钥（测试网明文）	链上	🟠 高(测试网)	中	**主网前切 Gnosis Safe/机构托管**
R-4	Keeper 单点 → 结算/赎回停滞	链下	🟠 高	中	**冗余 Keeper + 监控告警**
R-5	管理员单 API Key（无 hash/2FA/RBAC）	平台	🟠 中高	中	**升级账号+2FA+RBAC**
R-6	无 first-loss 缓冲（QDFI FundVault）	链上	🟠 中	低	NovaMarket 有首损瀑布；QDFI 靠限额+熔断
R-7	QDFToken Lot O(n) gas OOM	链上	🟠 中	低	AUDIT.md K-2：Lot 上限/合并
R-8	NAV 停滞 >26h → 申赎瘫痪（可用性）	链上	🟠 中	中	Keeper 可靠性 + 告警
R-9	赎回队列极端行情阻塞	链上	🟡 中低	中	单日 10%+T+3（设计折中）
R-10	登录/下单/赎回端点无限流	平台	🟡 中低	中	**补全速率限制**
R-11	CORS `*` fallback（POST/DELETE）	平台	🟡 低	低	移除 fallback，严格白名单
R-12	桥接依赖 Circle CCTP 可用性	链下	🟡 低	低	限额护栏 + mainnet 开关

9. 已实现的防御控制

链上：5/9 多签 + Timelock 24-48h、Guardian 实时模块化暂停、TradingAdapter 单笔/单日提款限额、PnL 异常熔断、NAV 偏离熔断、K-of-N/3-of-3 签名预言机、ReentrancyGuard + SafeERC20 + CEI、资金守恒等不变量（Foundry/Slither 0 critical）、首损瀑布（NovaMarket）、permissionless dailyTick。

链下：凭证 sealed-box（Web 无解密权）、Signer 隔离 localhost、私钥内存不落盘、`resolve_secret` 支持 KMS/Vault、订单 `FOR UPDATE SKIP LOCKED` 原子、桥接限额护栏 + mainnet 开关、权限最小化（executor 无签权、keeper 仅触发）。

平台：SIWE + 单次 nonce、JWT httpOnly/secure/SameSite、链上 `operator()` 鉴权、Zod 全校验、Prisma 参数化、CORS 白名单、公私钥分离托管模型。

10. 主网上线前安全检查表

> 综合 `docs/08_SECURITY.md`、`qdf-contracts/audit-package/AUDIT.md`、`fund-platform/docs/AUDIT_READINESS.md`。

审计与合约
- [ ] 第三方合约审计通过（Trail of Bits / OpenZeppelin / 等价）+ 修复闭环
- [ ] 真实 ZK PoR 电路替换 `MockZKVerifier` 并审计
- [ ] QDFToken Lot 上限 / 强制合并（K-2）
- [ ] Bug bounty 计划上线

密钥与治理
- [ ] 部署后 deployer `renounce DEFAULT_ADMIN_ROLE`，角色迁移至 Timelock
- [ ] 9 个治理多签 owner → Gnosis Safe / 机构托管（弃测试地址 K-4）
- [ ] 3 个 NAV verifier → HSM/冷钱包，签名人独立可审计
- [ ] 全部 `*_PRIVATE_KEY` 改 `awskms:` / `vault:` / `file:`(chmod600)，禁明文 .env
- [ ] K-of-N reporter key 分散不同主机/HSM
- [ ] 私钥丢失演练（5-of-9 中 4 不可用仍可治理）+ 轮换流程

链下服务
- [ ] Signer 部署隔离物理机，绑 127.0.0.1 + VPN/mTLS，**高可用主从**
- [ ] Signer 审计日志持久化（谁/何时/签了什么）
- [ ] 冗余 Keeper + 结算/NAV 停滞告警（R-4/R-8）
- [ ] 所有出站 RPC TLS + 证书校验；`FP_*_MAINNET_ENABLED` 审慎开启

平台与运维

- [ ] 管理员认证升级：账号+密码(hash)+2FA+RBAC（R-5）
- [ ] 登录/下单/赎回/凭证端点加速率限制（R-10）
- [ ] 移除 CORS `*` fallback（R-11）
- [ ] Postgres SSL + 密码 + IP 白名单 + 备份加密；SSH key-only
- [ ] Sentry + Slack/Telegram 告警上线；备机还原演练（RPO ≤ 24h）

11. 改进建议（按优先级）

P0（主网阻断项）：① 第三方合约审计 + 真实 ZK PoR；② 密钥托管迁移（Signer→HSM/KMS、多签→Gnosis Safe、verifier→冷钱包）；③ Signer 高可用 + 审计日志；④ 管理员认证加固（2FA/RBAC）。

P1（强烈建议）：⑤ 冗余 Keeper + 全链路监控告警（NAV/结算/赎回/权益偏离）；⑥ 关键端点速率限制 + 移除 CORS fallback；⑦ 评估为 QDFI 引入 first-loss 缓冲或明确披露无缓冲。

P2（增强）：⑧ QDFToken Lot 上限；⑨ TradingAdapter 上报加 nonce 防同 epoch 重复；⑩ DB 行级安全（RLS）评估；⑪ 赎回队列拥塞的用户侧可视化与优先级策略。

12. 附录：关键文件速查

域	路径
链上核心合约	`qdf-contracts/contracts/core/*.sol`（FundVault/TradingAdapter/NAVOracle/EmergencyController/Subscription/Redemption/PoolManager/QDFToken/Fee/KYC）
链上治理	`qdf-contracts/contracts/governance/QDFMultiSig.sol`、`core/QDFTimelock.sol`
链上审计包	`qdf-contracts/audit-package/AUDIT.md` · `INVARIANTS.md` · `DEPLOYMENT.md`
NovaMarket 合约/不变量	`fund-platform/`（CapitalPool/PoolSettlement/NAVReporter/FirstLossPolicy）、`fund-platform/docs/AUDIT_READINESS.md` · `SELF_AUDIT_REPORT.md` · `FUND_CUSTODY_SEPARATION_AND_SECURITY.md`
链下执行	`fund-platform/services/{executor,signer,keeper,reporter,risk_engine,connectors,fund_init,common}`
凭证密封	web `src/lib/{credentials,crypto}.ts` · services `common/crypto.py` · `signer/store.py`
平台认证	qdf `src/lib/{siwe,session,admin-auth}.ts` · NovaMarket `src/lib/auth/*`
安全策略	`docs/08_SECURITY.md`（本文为其交易系统专项分析补充）

本文基于代码侦察撰写，旨在支撑安全评审与审计准备；不构成审计结论或安全保证。所有金额/参数以 Arbitrum Sepolia 测试网部署为准，主网参数以最终治理为准。