اسناد معماری فنی و امنیتی HSM

شناسه سند: MK-TECH-2026-02

مرجع صادرکننده: سازمان منطقه آزاد تجاری - صنعتی ماکو | بهبود بشیری، فرینا اکبری، بهزاد چهارباغی، مبین خیاطی و امیرحسین دارابی

موضوع: سند فنی مهندسی سیستم، مشخصات هسته معاملاتی و استاندارد رمزنگاری سازمانی

خلاصه و مرور کلان معماری فنی

این سند فنی تشریح‌کننده معماری لایه‌بندی‌شده، پروتکل‌های امنیتی، استانداردهای رمزنگاری سازمانی و سازوکار سخت‌افزاری پلتفرم مرجعیت ارزی ماکو است. سیستم با هدف تحقق **تسویه اتمیک**[1]، تطبیق سفارشات در تأخیرهای زیر میلی‌ثانیه و شفافیت غیرقابل انکار طراحی شده است. به‌کارگیری **ماژول‌های سخت‌افزاری امنیتی** (HSM) منطبق بر سطح استانداردهای FIPS، ساختار امانی چندامضایی بانکی، و اجماع بیزانسی در لایه DLT، تضمین‌کننده نفوذناپذیری کامل زیرساخت در برابر حملات سایبری، دستکاری داخلی داده‌ها و مخاطرات پولشویی است.

۱. ساختار لایه‌بندی‌شده سیستم[2]

معماری پلتفرم **"ماکو اف ایکس" بر اساس اصل تفکیک وظایف**[3] و کاهش وابستگی‌های سیستمی در سه لایه کاملاً مجزا اما به هم پیوسته طراحی گردیده است:

- **لایه اول – لایه داده، اجماع و دارایی‌های امانی:**[4] این لایه وظیفه ثبت نهایی، تسویه اتمیک تراکنش‌ها، نگهداری قراردادهای هوشمند و ایجاد هماهنگی با شبکه بانکی رسمی را بر عهده دارد.
- **لایه دوم – هسته تطبیق سفارشات و پایش بازار:**[5] موتور متمرکز پردازش بلادرنگ سفارش‌ها که بدون ایجاد اصطکاک در زنجیره بلوکی، وظیفه دفترداری سفارشات، صف‌بندی اولویت‌های قیمت-زمان، و پالایش رفتارهای مخرب را اجرا می‌کند.
- **لایه سوم – لایه شاخص‌سازی و توزیع داده:**[6] سامانه‌ای که داده‌های تراکنش‌های تأییدشده را دریافت کرده، نوسانات کاذب را فیلتر نموده و **شاخص رسمی قیمت میانگین وزنی حجم** (VWAP) را از طریق واسط‌های برنامه‌نویسی امن در اختیار گمرک، سامانه جامع تجارت و مرکز مبادله قرار می‌دهد.

۲. لایه زیرساخت دفتر کل توزیع‌شده سازمانی[7]

لایه تسویه پلتفرم بر پایه یک شبکه دفتر کل توزیع‌شده سازمانی مجاز مستقر می‌گردد. بر خلاف شبکه‌های بلاک‌چین عمومی که با ریسک‌های ناشی از **کارمزدهای نوسانی** (Gas Fees)، عدم قطعیت زمانی و ناشناس بودن هویت‌ها مواجه هستند، شبکه ماکو دارای ویژگی‌های استاندارد سازمانی است:

- **الگوریتم اجماع تحمل خطای بیزانس استانبول نسخه دو** (IBFT 2.0): در این الگوریتم، **نودهای اعتبارسنج**[8] منحصراً توسط نهادهای ذی‌صلاح قانونی اداره می‌شوند.

---

[1] Atomic Settlement
[2] Three-Tier Platform Architecture
[3] Separation of Concerns
[4] Data, Settlement & Escrow Layer
[5] CLOB & Market Surveillance Engine
[6] Index & API Distribution Layer
[7] Enterprise Permissioned DLT
[8] Validator Nodes

- **ترکیب نودهای حاکمیتی**: شـــامل نود حاکمیتی بلنک مرکزی جمهوری اســـلامی ایران، نود ســـازمان منطقه آزاد ماکو، نودهای بانک‌های تجاری همکار (پایلوت امانی)، نود گمرک جمهوری اســـلامی ایران و در فاز تکمیلی نود ارتباطی **مرکز مالی بین‌المللی استانبول** (IFC) خواهد بود.
- **شاخص‌های عملکردی**: این ساختار دستیابی به قطعیت **تراکنش زیر ۲ ثانیه**[9] را بدون نیاز به ماینینگ یا الگوریتم‌های پرمصرف اثبات کار تضمین نموده و از **پدیده انشعاب زنجیره**[10] کاملاً مصون است.

۳. الزامات امنیتی ماژول‌های سخت‌افزاری (Hardware Security Modules - HSM)

کلیدهای خصوصی امضاکننده تراکنش‌های سازمانی، قراردادهای ضرب و ابطال توکن‌ها و دسترسی‌های مدیریتی به هیچ‌وجه در سرورهای متصل به اینترنت یا حافظه‌های نرم‌افزاری ذخیره نمی‌شوند. امنیت پایانه منحصراً بر پایه **ماژول‌های سخت‌افزاری امنیتی**[11] پایه‌ریزی شده است:

۱) **استاندارد تأییدیه امنیتی FIPS 140-2/3 Level 3**: کلیه دستگاه‌های HSM مستقر در سایت‌های عملیاتی دارای گواهینامه **امنیتی ضد دستکاری فیزیکی**[12] هستند. هرگونه تلاش فیزیکی برای نفوذ به محفظه چیپ‌های رمزنگاری منجر به پاکسازی خودکار **کلیدهای فوق محرمانه**[13] می‌گردد.

۲) **جداسازی کلیدهای عملیاتی و ریشه‌ای Root & Operational Key Hierarchy**: کلیدهای ریشه‌ای شبکه در گاوصندوق‌های آفلاین سرد نگهداری شده و کلیدهای عملیاتی امضای بلاک‌ها صرفاً تحت توابع رمزنگاری بیضی‌گون (ECDSA secp256k1) و (Ed25519) درون HSM پردازش می‌شوند.

۳) **احراز هویت چندعاملی مبتنی بر کارت‌های هوشمند M-of-N**: هرگونه بازگشایی نشست کاربری، به‌روزرسانی پارامترهای موتور تسویه یا تغییر قراردادهای هوشمند نیازمند حضور هم‌زمان حداقل ۳ نفر از دارندگان کارت‌های مجاز فیزیکی (Quorum Authentication) خواهد بود.

۴. معماری استخرهای امانی چندامضایی[14] و اوراکل‌ها

حساب‌های امانی ارزی، قلب تپنده پشتوانه‌سازی توکن‌های mUSD و mTRY هستند. ساختار امضایی این استخرها بر منطق **قراردادهای هوشمند چندامضایی** (m-of-n Multi-Sig) استوار است:

- **تأیید سه‌جانبه برای ضرب یا آزادسازی وجوه**: امضای دیجیتال کاربر/بازرگان، امضای دیجیتال بانک تجاری امانت‌دار فیات، و امضای رگولاتور پلتفرم ماکو.
- **اوراکل‌های رمزنگاری‌شده سازمانی**:[15] پروتکل همگام‌سازی مانده‌های بانکی با دفاتر تسویه دیجیتال از طریق این اوراکل‌ها صورت می‌گیرد. این ابزارها با استعلام مستقیم از سوئیچ بانکی رسمی و **سامانه‌های تسویه ناخالص آنی** (RTGS)، تغییرات حساب را با **پروتکل اثبات ذخایر**[16] در هر ۵ دقیقه تطبیق می‌دهند تا امکان کسری پشتوانه یا صدور بدون وثیقه به صفر برسد.

۵. هسته تطبیق سفارشات الکترونیک (CLOB Engine) و ارتباطات FIX

موتور تطبیق متمرکز (Central Limit Order Book) بر مبنای **معماری حافظه‌محور**[17] و با زبان‌های ســـطح پایین C++ و Rust بازطراحی شده است تا حداکثر کارایی را در مقایسه با روش‌های کند بلاک‌چینی ایجاد کند:

---

[9] Transaction Finality
[10] Forking
[11] Dedicated HSM
[12] Tamper-Resistant & Tamper-Evident
[13] Zeroization
[14] Multi-Signature Escrow
[15] Enterprise Cryptographic Oracles
[16] Proof of Reserves - PoR
[17] In-Memory Processing

- **ظرفیت پردازشی:** پردازش بیش از ۱۰۰ هزار سفارش بر ثانیه با **زمان تأخیر تطبیق**[18] زیر ۱ میلی‌ثانیه.
- **پروتکل پیام‌رسانی استاندارد FIX 5.0 SP2**: پلتفرم از پروتکل تبادل اطلاعات مالی بین‌المللی استفاده می‌کند که اتصال مستقیم سامانه‌های بانک‌های تجاری، صرافی‌های رتبه برتر و پایانه IFC استانبول را با کمترین تأخیر شبکه (زیر ۱۵ میلی‌ثانیه) میسر می‌سازد.
- **الگوریتم‌های ضد تبانی و لغو مشکوک** (OCR & VPIN): موتور معاملاتی به صورت خودکار **نسبت سفارش به معامله و نسبت لغو**[19] را محاسبه می‌کند. سفارشاتی که با هدف اشباع پهنای باند و فریب الگوریتمی ثبت شوند، پیش از ورود به عمق بازار بلاک شده و کاربر متخلف مشمول جریمه کارمزدی می‌گردد.

۶. جدول مشخصات فنی، زیرساخت و پروتکل‌های امنیتی

لایه سامانه‌ای	مؤلفه فنی و تکنولوژیک	استاندارد امنیتی / عملکردی	کارکرد عملیاتی در طرح "ماکو اف ایکس"
لایه اجماع	DLT زنجیره مجاز با الگوریتم IBFT 2.0	قطعیت زیر ۲ ثانیه، بدون فورک	ثبت تغییرناپذیر اسناد مالکیت و تسویه اتمیک حوالجات
ماژول رمزنگاری	سخت‌افزار اختصاصی HSM سازمانی	FIPS 140-2 Level 3 و CC EAL4+	حفاظت فیزیکی و رمزنگاری کلیدهای اختصاصی شبکه
موتور معاملات (Core)	دفتر سفارش متمرکز (CLOB) با C++	تأخیر زیر ۱ میلی‌ثانیه، 100K TPS	تطبیق سفارشات خرید و فروش صادرکننده و واردکننده
پروتکل فرامرزی	درگاه FIX Protocol 5.0 SP2	رمزنگاری تونل اختصاصی TLS 1.3 / IPsec	اتصال به بازارسازان و تأمین‌کنندگان نقدینگی ترکیه و استانبول
حساب امانی و توکن	پروتکل Multi-Sig با Escrow PoR	نسبت وثیقه‌گذاری دقیق ۱:۱	انتشار و ابطال توکن‌های mUSD/mTRY با پشتوانه بانکی

۷. پایش بلادرنگ، قابلیت اطمینان و طرح بازیابی[20]

زیرساخت پلتفرم **"ماکو اف ایکس"** با شاخص پایداری و در دسترس‌پذیری ۹۹.۹۹ درصد (High Availability Tier-3+) طراحی شده است. سایت اصلی عملیاتی در منطقه آزاد ماکو مستقر بوده و **سایت پشتیبان گرم**[21] در یک مرکز داده امن در تهران به موازات فعالیت می‌کند.

همگام‌سازی بلادرنگ داده‌ها میان سایت اصلی و پشتیبان با سازوکار همگام دوقلو انجام می‌شود، به‌گونه‌ای که **شاخص زمان بازیابی از خرابی** (RTO) زیر ۳۰ ثانیه و **شاخص نقطه بازیابی داده‌ها** (RPO) صفر مطلق خواهد بود. کلیه بسته‌های داده‌ای با الگوریتم‌های رمزنگاری پساکوانتومی و **کلیدهای تولیدشده توسط مولد تصادفی واقعی** (TRNG) مستقر در سخت‌افزار HSM محافظت می‌شوند.

---

[18] Matching Latency
[19] Order-to-Cancellation Ratio
[20] Disaster Recovery
[21] Hot Standby Site