امکان‌سنجی شرایط ادغام
ساختار داياچين در شبکه ققنوس

به سفارش «داياچين»
شرکت تدبيراندیشان نوین افروز

ویرایش نخست - ۱۶ اردی‌بهشت ۱۴۰۴
میرسهیل نیک‌زاد کلورزی

فهرست عناوین

مقدمه

شبکهٔ ققنوس (Kuknos) یک زیرساخت بلاکچینی کنسرسیومی است که ابتدا با فورک‌کردن کد استلار شکل گرفت ramzarz.academy. این شبکه تاکنون بر پایهٔ پروتکل استلار (Stellar SCP) اداره می‌شده و توکن بومی آن پیمان (PMN) نقش لومِن استلار (XLM) را برای کارمزدها ایفا می‌کند exir.io. شبکهٔ ققنوس برای توکنیزه‌کردن دارایی‌ها (مانند پشتوانه طلای توکن پیمان) و نقل‌وانتقال سریع ارزش میان میزبان‌های معتبر (بانک‌ها و نهادهای مالی) طراحی شده است exir.io. معماری کنونی اگرچه سرعت و هزینهٔ پایینی دارد، اما از نظر قابلیت برنامه‌پذیری محدود است؛ استلار ذاتاً برای انتقال پول طراحی شده و قرارداد هوشمند داخلی (ماشین تورینگ‌کامل) ندارد linkedin.com. به همین دلیل، بنیاد ققنوس تصمیم گرفته برای ارتقای قابلیت‌های شبکه (خصوصاً پشتیبانی از قراردادهای هوشمند و برنامه‌های غیرمتمرکز) به سراغ معماری اتریومی برود. در این تحقیق، طرح جامع ماشین مجازی اتریوم (EVM) برای یکی از میزبان‌های ققنوس (انکر «دایاچین») و نحوهٔ گذار تدریجی شبکه از زیرساخت استلاری به اتریومی تشریح شده است. این گذار به‌نحوی برنامه‌ریزی شده که تا پیش از مهاجرت کامل، سایر نودهای ققنوس تفاوتی احساس نکنند و تعاملات از طریق یک مبدّل پروتکلی بدون اختلال صورت گیرد.

در ادامه ابتدا معماری فنی راهکار پیشنهادی (ماشین اتریومی جایگزین) را به‌طور کامل معرفی می‌کنیم. سپس عملکرد و سناریوهای تعامل انکر دایاچین به‌عنوان نخستین میزبان مجهز به این ماشین بررسی می‌شود. بخش بعدی به طراحی و معرفی شبکهٔ تست‌نت «راخ» (Rakhs) می‌پردازد که بر پایهٔ EVM بوده و کاربران می‌توانند با همان هویت‌ها و کلیدهای شبکهٔ ققنوس در آن فعالیت کنند. در بخش چهارم، مراحل گام‌به‌گام مهاجرت کامل شبکه ققنوس به معماری اتریومی (ابعاد فنی، فرهنگی، حقوقی، اجماع و ارتقاء نودها) ارائه می‌گردد. سپس الزامات و ملاحظات قانونی انکرهای ایرانی در چارچوب رگولاتوری کشور و امکان‌پوشش آن‌ها توسط فناوری اتریوم (قراردادهای هوشمند، ابزارهای کنترلی EVM و ...) تحلیل می‌شود. نهایتاً با استناد به تجارب و تحلیل‌های پیشین مهاجرت از استلار به اتریوم در سایر پروژه‌ها، مزایا و چالش‌های این گذار جمع‌بندی خواهد شد.

معماری فنی پیشنهادی: ماشین اتریومی و مبدّل پروتکل

معماری پیشنهادی شامل طراحی یک گره ققنوس جدید مبتنی بر EVM است که بتواند در چارچوب شبکه فعلی (استلاری) فعالیت کند. این گره که در انکر دایاچین مستقر خواهد شد، از دو بخش اصلی تشکیل می‌شود: ماشین اتریومی داخلی و مبدّل پروتکلی Stellar–Ethereum. شکل زیر نمای ساده‌ای از این معماری را نشان می‌دهد:

شمای کلی معماری انکر دایاچین با ماشین مجازی اتریوم و مبدّل پروتکلی متصل به شبکه ققنوس (برگرفته از نقشه راه ققنوس).

الزامات فنی ماشین اتریومی

این ماشین باید از سازگاری کامل با EVM برخوردار باشد تا بتوان قراردادهای هوشمند سالیدیتی را اجرا کند. بدین ترتیب توسعه‌دهندگان قادر خواهند بود DAppهای دلخواه را روی شبکه ققنوس جدید پیاده‌سازی کنند. همچنین ماشین اتریومی باید کارایی متناسب با شبکه ققنوس داشته باشد؛ شبکه فعلی ققنوس توان پردازش ~۱۰۰۰ تراکنش در ثانیه با نهایی‌شدن در ~۵ ثانیه را دارد kuknos.org، لذا ماشین جدید نیز باید با تنظیمات اجماع مناسب (مثلاً کاهش زمان بلاک یا استفاده از الگوریتم اجماع پرسرعت) به تأخیر حداقلی و توان throughput بالا برسد. از منظر امنیت، EVM باید در این بستر ایزوله و کنترل‌شده اجرا شود تا اجرای قراردادهای کاربر هیچ خللی در عملکرد اصلی نود وارد نکند. انکر دایاچین به‌عنوان میزبان این ماشین، نیازمند سخت‌افزار قدرتمند (CPU/RAM بالا) و ماژول‌های امنیتی (مثلاً HSM برای نگهداری کلیدها) است تا اجرای همزمان پروتکل استلار و ماشین اتریوم را پشتیبانی نماید.

اجزای معماری

همان‌گونه که بیان شد، اجزای کلیدی شامل: ۱) هستهٔ EVM – معادل یک نود اتریوم که وظیفهٔ اجرای بایت‌کد قراردادهای هوشمند، مدیریت حالت حساب‌های اتریومی و ساخت بلاک‌های جدید را بر عهده دارد. این هسته می‌تواند بر پایهٔ یک کلاینت سبک اتریوم (مثلاً geth با تنظیمات PoA) پیاده‌سازی شود. ۲) ماژول تطبیق Stellar – بخشی که به ماشین EVM امکان می‌دهد با پروتکل

استلار صحبت کند. این ماژول نقش لایهٔ سازگاری (Compatibility Layer) را دارد؛ یعنی ورودی‌های شبکه ققنوس (تراکنش‌ها و پیام‌های اجماع SCP) را دریافت و برای ماشین اتریوم ترجمه می‌کند و بالعکس، خروجی‌های ماشین EVM (تغییرات وضعیت یا رویدادها) را به قالب قابل درک برای سایر نودهای استلاری تبدیل می‌نماید. ۳) مبدّل پروتکلی Stellar↔Ethereum – این مبدّل نوعی Gateway یا Bridge است که اطلاعات و دارایی‌ها را میان دو دنیای متفاوت جابه‌جا می‌کند. مبدّل شامل دو بخش نرم‌افزاری است: یکی داخل انکر دایاچین (جهت ترجمهٔ آنی پروتکل‌ها) و یکی به‌صورت ماژول سِروری جانبی که عملیات پیچیده‌تر bridging را انجام می‌دهد. برای مثال، اگر کاربری بخواهد دارایی خود را از شبکهٔ ققنوس به محیط EVM انتقال دهد، مبدّل تشخیص می‌دهد که یک تراکنش خاص در لجر استلار (مثلاً ارسال به آدرس انکر دایاچین با memo خاص) به معنای درخواست پل‌زدن دارایی است. مبدّل آنگاه روال زیر را طی می‌کند: تراکنش دریافتی استلار را پردازش کرده، مقدار توکن را در شبکهٔ اصلی قفل (freeze) می‌کند و معادل آن را در شبکهٔ اتریومی (ماشین دایاچین) مینت می‌نماید manual.threefold.iomanual.threefold.io. این توکن معادل می‌تواند یک توکن ERC-20 نمایندهٔ دارایی ققنوس (مثلاً پیمان) باشد. روند برعکس نیز توسط مبدّل پشتیبانی می‌شود: سوزاندن (burn) توکن معادل در زنجیرهٔ EVM همراه با ذکر آدرس مقصد استلاری، باعث آزادسازی آن مقدار دارایی در شبکهٔ ققنوس و ارسال به حساب کاربر می‌شود manual.threefold.io.

نحوهٔ تعامل با شبکهٔ فعلی

ایدهٔ کلیدی این است که انکر دایاچین علیرغم داشتن بطن اتریومی، برای سایر نودها یک نود استلاری عادی به‌نظر برسد. این امر با دو ابتکار میسر می‌شود: نخست آنکه انکر دایاچین همچنان یک Stellar Core (یا معادل آن) اجرا می‌کند که در اجماع SCP شرکت دارد و تراکنش‌های معمول ققنوس (مثل انتشار توکن، پرداخت‌ها و ...) را مشابه دیگر نودها پردازش می‌کند. دوم اینکه تمام تعاملات خاص اتریومی، پشت‌صحنه توسط مبدّل پردازش شده و نتیجهٔ آن در قالب تراکنش‌های معمول منعکس می‌شود. به بیان دیگر، اگر قراردادی روی EVM اجرا شود که نیاز به اثر گذاری در دفتر کل ققنوس دارد (مثلاً انتقال مالکیت یک توکن ققنوس از A به B به‌واسطهٔ قرارداد)، انکر دایاچین پس از اجرای قرارداد، یک تراکنش استاندارد استلار (مثلاً پرداخت دارایی از A به B) را ایجاد و امضا می‌کند و به شبکه می‌فرستد. سایر نودها آن تراکنش را مانند همیشه اعتبارسنجی کرده و در صورت معتبر بودن، در لجر نهایی ثبت می‌کنند – بی‌آنکه اصلاً متوجه شوند منشاء این عملیات، یک قرارداد هوشمند EVM بوده است. عکس این حالت نیز صادق است؛ مثلاً اگر در شبکه ققنوس رویدادی رخ دهد که برای قراردادی درون EVM حائز اهمیت است، مبدّل آن رویداد را به صورت فراخوان قرارداد یا ثبت لاگ در ماشین اتریوم اعمال می‌کند. این همگام‌سازی دوطرفهٔ وضعیت تضمین می‌کند که تا زمان مهاجرت کامل، هر دو سامانه (استلار و EVM) همخوان و یکپارچه باقی بمانند.

مکانیزم مبدّل و تطبیق پروتکل

مبدّل Stellar–Ethereum در قلب خود از الگوهای پل بلاکچین بهره می‌گیرد. یکی از این الگوها، ثبت آدرس متقابل در Memo تراکنش‌ها است manual.threefold.io. به عنوان نمونه، مبدّل ققنوس توافق می‌کند که اگر کاربری بخواهد پیمانِ خود را به معادل ERC-20 تبدیل کند، باید آن را به آدرس خاصی (متعلق به انکر دایاچین) بفرستد و آدرس اتریومی مقصد را در فیلد Memo درج کند manual.threefold.io. نرم‌افزار مبدّل مستقر در انکر دایاچین شبکهٔ استلار را رصد می‌کند؛ به‌محض مشاهدهٔ چنین تراکنشی، Memo را decode کرده و آدرس Ethereum مقصد و مقدار را استخراج می‌نمایدmanual.threefold.io. سپس به هستهٔ EVM فرمان می‌دهد که مثلاً تابع mint(address, amount) را در قرارداد توکن پیمان ERC-20 فراخوانی کند تا برای آدرس مذکور آن مقدار توکن صادر گردد. کل این فرایند در مقیاس چند ثانیه یا کمتر انجام می‌شود و در نهایت کاربر دریافت‌کننده می‌تواند دارایی خود را در زنجیرهٔ اتریومی راخ/دایاچین مشاهده و در قراردادهای هوشمند خرج کند. در مسیر عکس، کاربر در محیط اتریومی مثلاً تابع burn(amount, dest_memo) را روی قرارداد فراخوانی می‌کند و مبدّلِ مستقر در ماشین EVM، رویداد آن را دریافت و تفسیر کرده، یک تراکنش استلار از جانب انکر دایاچین می‌سازد که دارایی قفل‌شده را به آدرس مقصد آزاد نماید manual.threefold.io.

با این معماری، تمام اجزای شبکه فعلی ققنوس بدون نیاز به تغییر می‌توانند با انکر دایاچین تعامل کنند؛ تراکنش‌های مخصوص پل توسط مبدّل مدیریت می‌شوند و سایر نودها فقط تراکنش‌های استاندارد استلار را می‌بینند. انکرهای قدیمی صرفاً متوجه خواهند شد که انکر دایاچین گاهی مقادیر قابل توجهی توکن را به آدرسی منتقل یا از آن دریافت می‌کند، اما جزئیات اینکه چرا و چگونه، برایشان شفاف نیست (و البته نیازی هم نیست). به این ترتیب ریسک ایجاد اختلال یا ناسازگاری با نسخه‌های قبلی به حداقل می‌رسد.

عملکرد انکر دایاچین و سناریوهای تعامل با شبکه

انکر دایاچین به‌عنوان اولین میزبان مجهز به ماشین اتریومی، نقشی تعیین‌کننده در آزمون و ارزیابی این معماری ایفا می‌کند. در این بخش، هم توان عملیاتی و کارایی این انکر و هم سناریوهای کاربردی تعامل آن با شبکهٔ ققنوس را بررسی می‌کنیم.

توان پردازشی و کارایی

ماشین EVM طبیعتاً برای اجرای قراردادهای پیچیده طراحی شده و ممکن است از نظر سرعت خام، کندتر از اجرای بومی عملیات سادهٔ استلار باشد linkedin.comlinkedin.com. با این حال، طراحی ماژولار انکر دایاچین طوری است که وظایف پردازشی سنگین را از مسیر اجماع استلار جدا می‌کند. به این معنی که اجماع SCP ققنوس همچنان با همان سرعت قبلی پیش می‌رود (هر ۵ ثانیه یک Ledger بسته می‌شود) و تراکنش‌های معمول را پردازش می‌کند؛ ماشین EVM در پس‌زمینه ممکن است مشغول اجرای چند قرارداد طولانی باشد، اما تا هنگامی‌که خروجی آن آماده نشده، اثری بر شبکه نمی‌گذارد. در بدترین حالت، اگر انکر دایاچین تحت بار سنگین قراردادهای اتریومی قرار گیرد، ممکن است سرعت پاسخگویی پل کاهش یابد (برای نمونه، تبدیل پیمان به ERC-20 به جای ۵ ثانیه در ۱۰ ثانیه انجام شود)، ولی این موضوع سایر نودها را تحت تأثیر مستقیم قرار نخواهد داد. به منظور جلوگیری از هرگونه گلوگاه عملکردی، چند راهکار فنی مد نظر است: ۱) تخصیص منابع محاسباتی مجزا به فرآیند اجماع استلار و فرآیند EVM (مثلاً با استفاده از کانتینرها یا ماشین‌های مجازی جداگانه در یک سرور واحد). ۲) تعریف سقف گس (Gas) پایین‌تر برای قراردادهای راخ/دایاچین نسبت به اتریوم عمومی، تا از اجرای محاسبات بسیار پرهزینه جلوگیری شود. ۳) پایش بلادرنگ وضعیت انکر؛ چنانچه بار EVM بیش از حد مجاز شود، مبدّل ممکن است درخواست‌های پل جدید را موقتاً صف کند تا قراردادهای در حال اجرا تمام شوند. به کمک این تدابیر، انتظار می‌رود انکر دایاچین بتواند بدون کاهش محسوس کارایی شبکه، نقش یک دروازهٔ هوشمند را ایفا کند.

سناریوی صدور و انتقال دارایی از طریق قرارداد هوشمند

فرض کنید یک ناشر (مثلاً یک بانک) بخواهد اوراق قرضه یا دارایی مالی پیچیده‌ای را روی ققنوس منتشر کند که منطق تجمیع و توزیع سود پیچیده دارد. در معماری قدیم، چنین چیزی به سختی ممکن بود یا باید خارج از بلاکچین مدیریت می‌شد. اکنون با حضور انکر دایاچین، ناشر می‌تواند یک قرارداد هوشمند در بستر راخ بنویسد که منطق مدنظر (مثلاً پرداخت خودکار کوپن‌های اوراق به دارندگان توکن در بازه‌های زمانی مشخص) را اجرا کند. او ابتدا مقدار معینی از توکن پایه (مثلاً پیمان یا توکن ریالی) را به آدرس انکر دایاچین در شبکه ققنوس واریز می‌کند (قفل کردن سرمایه)، سپس معادل آن توکن "اوراق" در قرارداد ERC20 را در راخ مینت می‌کند و بین سرمایه‌گذاران توزیع می‌کند. سرمایه‌گذاران می‌توانند این توکن ERC20 را بین خود در راخ معامله کنند یا در بازارهای دیفای که احتمالاً روی راخ شکل می‌گیرد، مشارکت نمایند. در زمان پرداخت سود دوره‌ای، قرارداد هوشمند به طور خودکار از موجودی پیمان قفل‌شده، سود را محاسبه و برای صاحبان فعلی توکن‌ها آزاد می‌کند (این کار با یک تراکنش استلار از جانب انکر دایاچین به هر حساب ذینفع انجام می‌شود که مبدّل آن را ترتیب می‌دهد). تمام این فرایند برای سایر انکرها به صورت چند تراکنش عادی (پرداخت‌های دوره‌ای) جلوه می‌کند، اما در پس زمینه یک منطق پیشرفته در حال اجرا بوده است. این سناریو نشان می‌دهد چگونه قابلیت‌های دیفای و قراردادهای هوشمند می‌توانند بدون تغییر شبکه اصلی، توسط یک انکر هوشمند پیاده‌سازی شوند.

سناریوی تعامل کاربر نهایی با DApp اتریومی

در حالت ایده‌آل، کاربران عادی ققنوس نباید نیازی به درک پیچیدگی پل و دو شبکهٔ زیرین داشته باشند. برای این منظور، کیف‌پول ققنوس (اپلیکیشن موبایل/دسکتاپ) ارتقا خواهد یافت تا از طریق یک رابط یکپارچه، امکان تعامل با DAppهای راخ را فراهم کند. به عنوان مثال، کاربر وارد کیف‌پول خود می‌شود و یک بخش جدید به نام «برنامه‌های غیرمتمرکز» را می‌بیند. او در آنجا لیستی از DAppهای موجود (مثلاً صرافی غیرمتمرکز، بازار NFT، قرارداد وام‌دهی توکن طلا و ...) را مشاهده می‌کند. هنگامی که کاربر یکی را انتخاب می‌کند (مثلاً DEX ققنوس)، کیف‌پول پشت‌صحنه توکن‌های لازم را از حساب کاربر به انکر دایاچین پل می‌زند و معادل آن را به قرارداد مربوطه در راخ واریز می‌کند، سپس نتیجهٔ معامله را دریافت و در صورت نیاز دارایی را برگردانده و به کاربر نشان می‌دهد. تمامی این تراکنش‌های میانی از دید کاربر پنهان می‌ماند؛ او فقط تجربهٔ کار با یک اپلیکیشن مالی را دارد که موجودی حسابش ممکن است کم و زیاد شود. این تجربهٔ کاربری یکپارچه به پذیرش فناوری جدید کمک شایانی خواهد کرد. در پشت صحنه، انکر دایاچین و

مبدّل باید قادر باشند در لحظه پل‌زدن دارایی را انجام دهند و همچنین هویت ققنوسی کاربر را به قرارداد هوشمند اعلام کنند (مثلاً از طریق امضای دیجیتال یا ارائهٔ یک توکن هویتی غیرقابل انتقال). ارائهٔ این سرویس‌های پیشرفته باعث می‌شود انکر دایاچین عملاً نقش واسط نوآوری در شبکه را بازی کند و اعتبارسنجی موفقیت این مدل باشد.

سناریوی استمرار خدمات قدیمی

یکی از نکات قوت طرح پیشنهادی این است که هیچ‌یک از خدمات فعلی ققنوس قطع یا مختل نمی‌شوند. انکر دایاچین همچنان وظایف مرسوم یک میزبان را دارد: نظارت و ثبت تراکنش‌های کاربران خودkuknos.orgkuknos.org، اجرای سرویس‌های پل KYC/AML داخلی برای بررسی مبادلاتkuknos.org، انتشار توکن‌های جدید به درخواست ناشران و ... . حتی اگر برخی میزبان‌ها نخواهند به این زودی از امکانات اتریومی بهره‌مند شوند، می‌توانند کماکان مثل قبل به کار با نسخهٔ استلاری ادامه دهند. به علاوه، چنانچه مشکلی در ماشین اتریومی یا پل به‌وجود آید، انکر دایاچین می‌تواند به حالت فقط-استلار سوییچ کند و شبکه دچار وقفه نشود. این سناریوی پشتیبان (Fail-safe) از طریق مکانیزم‌هایی مانند پرچم وضعیت در پروفایل انکر دایاچین پیاده می‌شود تا سایر میزبانان درصورت غیرفعال‌شدن امکانات پل، از ارسال درخواست‌های مرتبط خودداری کنند. در مجموع، انعطاف‌پذیری عملیات انکر دایاچین یکی از دلایل انتخاب آن به عنوان محیط پایلوت است.

شبکهٔ تست‌نت «راخ» (Rakhs): پل آزمایشی به‌سوی اتریوم

به موازات اجرای ماشین اتریومی در محیط محدود انکر دایاچین، بنیاد ققنوس قصد دارد یک **شبکهٔ آزمایشی مستقل** با معماری اتریومی راه‌اندازی کند تا **توسعه‌دهندگان و کاربران** بتوانند پیش از مهاجرت نهایی، در یک محیط ایزوله تجربه کسب کنند. این شبکهٔ تست که «راخ» (به معنای خاکستر، اشاره به ققنوس که از خاکستر برمی‌خیزد) نامیده شده، نقش **پل آزمایشی به‌سوی ققنوس جدید** را ایفا می‌کند.

طراحی فنی شبکهٔ راخ

راخ در واقع یک شبکه بلاکچین مستقل مبتنی بر اتریوم است که از همان ماشین مجازی اتریوم بهره می‌برد. این شبکه احتمالاً به صورت یک فورک از شبکه‌های آزمایشی اتریوم (مانند گورلی یا سپولیا) یا یک کانفیگ اختصاصی از گث/Parity در حالت PoA راه‌اندازی می‌شود. هدف آن است که راخ از نظر قوانین اجماع و تنظیمات، بسیار شبیه شبکهٔ ققنوس اتریومی نهایی باشد تا تمام رفتارها در شرایط واقعی شبیه‌سازی شوند. تعداد نودهای اعتبارسنج راخ ممکن است محدود (مثلاً چند سرور در اختیار تیم فنی ققنوس و شاید برخی میزبان‌های علاقه‌مند) باشد، اما برای کاربران نهایی این شفاف خواهد بود که این فقط یک testnet است و دارایی‌های آن ارزش واقعی ندارند. نکتهٔ مهم، سیاست هویت در راخ است؛ انتظار می‌رود تنها کسانی بتوانند در راخ فعالیت کنند که هویت ققنوسی تأییدشده داشته باشند (همان KYC فعلی). برای نیل به این هدف، مکانیزمی در نظر گرفته می‌شود تا همان کلیدها و حساب‌های ققنوس در شبکه راخ نیز قابل استفاده باشند. یکی از راه‌حل‌ها، استفاده از یک تابع درهم‌ساز برای تبدیل کلیدهای ED25519 به کلیدهای secp256k1 (استاندارد اتریوم) یا تعریف رابطهٔ چند امضایی بین این دو نوع کلید است. راهکار ساده‌تر، صدور توکن‌های هویتی غیرقابل انتقال (Soulbound Tokens) برای کاربران در راخ است که توسط میزبان مرجع آن‌ها در ققنوس امضا شده است؛ به این ترتیب هر کاربر در راخ یک توکن معرف هویت دارد و قراردادهای هوشمند می‌توانند وجود آن توکن را معادل عبور کاربر از احراز هویت تعبیر کنند.

قابلیت فعالیت با هویت‌ها و کلیدهای ققنوسی

اهمیت این ویژگی در این است که توسعه‌دهندگان و کاربران بتوانند سناریوهای دنیای واقعی را روی راخ تست کنند. برای مثال، اگر کاربری در شبکه اصلی یک حساب دارد که متعلق به بانک ملت است و KYC شده، بتواند با همان هویت (و ترجیحاً همان زوج‌کلید) وارد شبکه راخ شده و توکن‌های آزمایشی دریافت کند و به قراردادها ارسال نماید. این استمرار هویت باعث می‌شود حتی اگر در راخ دارایی حقیقی وجود ندارد، تراکنش‌ها از منظر انطباق و دسترسی، مشابه واقعیت باشند. البته پیاده‌سازی تکنیکی این امر چالش‌برانگیز است؛ زیرا الگوریتم رمزنگاری استلار (ED25519) با اتریوم (secp256k1) متفاوت است. یک پیشنهاد مطرح‌شده این

است که برای هر کاربر ققنوس، یک حساب متناظر اتریومی در راخ ایجاد گردد و در سامانهٔ هویت ققنوس لینک شود؛ به‌نحوی که وقتی کاربر در اپلیکیشن ققنوس به شبکه راخ سوئیچ می‌کند، کیف‌پول به طور خودکار از این حساب متناظر استفاده نماید. هر تراکنشی در راخ می‌تواند حاوی شناسهٔ کاربر در سامانه ققنوس در داده‌های خود باشد تا در صورت نیاز قابل ردیابی باشد.

نقش‌های آیندهٔ راخ فراتر از یک تست‌نت

اگرچه راخ در ابتدا یک شبکه آزمایشی است، اما می‌تواند کاربردهای بلندمدت‌تری نیز داشته باشد. یکی از نقش‌های محتمل، تبدیل‌شدن به شبکه پیش‌تولید (Staging) برای به‌روزرسانی‌های عمدهٔ ققنوس خواهد بود. به عبارت دیگر، هر ویژگی یا تغییر بزرگی ابتدا روی راخ پیاده و آزموده می‌شود و پس از تضمین پایداری، روی شبکه اصلی اعمال می‌گردد. چنین مکانیزمی ریسک اختلال در شبکه اصلی را به حداقل می‌رساند. نقش دیگر، محیط آموزش و نوآوری است؛ راخ می‌تواند محلی برای برگزاری Hackathonها، آموزش توسعه‌دهندگان قرارداد هوشمند و آزمایش ایده‌های نو توسط استارتاپ‌های فین‌تک ایرانی باشد – بدون نگرانی از تبعات مالی. بنیاد ققنوس می‌تواند راخ را به صورت بازتر اداره کند؛ حتی اجازه دهد نودهای بیشتری (مثلاً دانشگاه‌ها یا شرکت‌های نوآور) به عنوان اعتبارسنج در آن مشارکت کنند تا تجربهٔ نیمه‌عمومی‌بودن شبکه به‌دست آید. در آینده، راخ ممکن است به اکوسیستمی مجزا اما هم‌پیوند با ققنوس اصلی بدل شود؛ مثلاً به‌عنوان زنجیرهٔ موازی (Sibling Chain) جهت میزبانی از پروژه‌های خاص یا توکن‌های پرریسک که شبکه اصلی تمایلی به میزبانی مستقیم آن‌ها ندارد. به طور خلاصه، راخ فرصتی برای آزمون، آموزش و حتی انشعاب‌های کاربری جدید فراهم می‌کند و ارزش آن فراتر از یک تست‌نت ساده است.

نقشهٔ راه مهاجرت کامل به معماری اتریومی

مهاجرت کامل ققنوس از بستر استلار به معماری اتریومی یک پروژهٔ چندبعدی و حساس است که باید گام‌به‌گام و با هماهنگی همهٔ ذی‌نفعان انجام شود. در این بخش، مراحل پیشنهادی برای این گذار را در حوزه‌های فنی، فرهنگی و حقوقی مرور می‌کنیم:

۱. مرحلهٔ آزمایشی و آماده‌سازی (Pilot)

این همان فازی است که انکر دایاچین با ماشین EVM راه‌اندازی می‌شود. طی این مرحله، عملکرد فنی مبدّل و سازگاری آن با شبکه موجود زیر نظر گرفته می‌شود. همچنین آموزش‌های اولیه به تیم‌های فنی میزبان‌ها ارائه می‌گردد تا با مفاهیم EVM و قرارداد هوشمند آشنا شوند. در این فاز، ممکن است تنها دارایی‌های محدودی (مثلاً توکن پیمان) اجازهٔ پل‌زدن آزمایشی داشته باشند تا ریسک‌ها کنترل‌شده باشند. هدف این مرحله، اثبات عملیاتی بودن ایده و شناسایی اشکالات احتمالی است.

۲. راه‌اندازی شبکهٔ راخ (تست عمومی)

پس از اطمینان نسبی از فاز پایلوت، شبکهٔ راخ به صورت عمومی‌تر معرفی می‌شود. این مرحله شامل اطلاع‌رسانی به جامعهٔ کاربری ققنوس است که یک شبکه موازی برای اهداف آزمایشی وجود دارد و از آن‌ها دعوت می‌شود مشارکت کنند. به کاربران توضیح داده می‌شود که می‌توانند دارایی‌های خود را به توکن‌های آزمایشی تبدیل کرده و در راخ فعالیت نمایند. همچنین برنامه‌های تشویقی (Incentives) برای توسعهٔ قراردادهای هوشمند مفید روی راخ در نظر گرفته می‌شود (مثلاً مسابقهٔ ساخت بهترین DApp مالی با جوایزی در پیمان). در این مرحله، بنیاد ققنوس با جمع‌آوری بازخوردهای کاربران و توسعه‌دهندگان، نیازمندی‌های بهبود را استخراج می‌کند. از بعد فرهنگی، این فاز به جامعه فرصت می‌دهد تا بدون ترس از دست رفتن سرمایه، با فضای جدید خو بگیرند.

۳. تدوین چارچوب حقوقی و حاکمیتی جدید

به موازات مراحل فنی، کمیتهٔ رگولاتوری و حقوقی ققنوس باید تغییرات را بررسی و چارچوب‌های جدیدی تدوین کند. برای مثال، در معماری جدید ممکن است نقش میزبان‌ها تا حدی تغییر کند؛ شاید به جای مفهوم «ناشر معتمد» مدل قرارداد هوشمند تضمین‌شده مطرح شود. باید مشخص شود مسئولیت قانونی هر قرارداد هوشمند با کیست؟ آیا هر میزبان بر DAppهای ساخته‌شده توسط خود نظارت خواهد داشت یا نهادی مرکزی برای تایید قراردادها تشکیل می‌شود؟ همچنین لازم است اسناد بالادستی (سپیدنامه، توافق‌نامهٔ اعضا) به‌روزرسانی شوند تا مواردی چون نحوهٔ رأی‌گیری و اجماع در شبکهٔ جدید پوشش داده شود.

(شایان ذکر است که خود بنیاد ققنوس از سال ۱۴۰۱ بخشی از حاکمیتش را روی یک DAO در اتریوم عمومی مستقر کرده است[dayadiamond.ir](dayadiamond.ir) که نشان‌دهندهٔ حرکت در این مسیر بوده است). این اسناد پس از تدوین اولیه، برای نظرخواهی در اختیار اعضای بنیاد و حتی رگولاتور (مثلاً بانک مرکزی یا نهادهای ذیربط) قرار می‌گیرد تا تأییدیه‌های لازم اخذ شود.

۴. ارتقاء زیرساخت‌ها و توانمندسازی نیروی انسانی

تمامی میزبان‌های فعلی باید برای انتقال به پلتفرم جدید آماده شوند. از منظر زیرساختی، ممکن است نیاز به ارتقاء سخت‌افزاری سرورها یا نصب نرم‌افزارهای جدید (مثل کلاینت‌های اتریوم) باشد. تیم‌های فنی بانک‌ها احتمالاً در فناوری استلار مهارت یافته‌اند؛ اکنون باید دوره‌های آموزشی عمیق در زمینهٔ Solidity، امنیت قرارداد هوشمند، ابزارهای توسعهٔ اتریوم (مانند Hardhat، Truffle) و مدیریت گره اتریومی بگذرانند. این بخش، بُعد فرهنگی/آموزشی مهاجرت است که بسیار حیاتی محسوب می‌شود. برای کاهش مقاومت در برابر تغییر، می‌توان از تیم‌های پیشرو (مثلاً شرکت یکتا ققنوس پارس به عنوان بازوی فنی اصلی) استفاده کرد تا به سایرین کمک کنند. همچنین برگزاری کارگاه‌ها و ارائهٔ موفقیت‌های کسب‌شده در فاز آزمایشی (مثلاً DAppهایی که در راخ پیاده شده و مفید بوده‌اند) به جلب حمایت مدیران ارشد سازمان‌ها کمک می‌کند.

۵. انتخاب و پیاده‌سازی مکانیسم اجماع جدید

یکی از تصمیمات فنی کلیدی، الگوریتم اجماع در شبکه ققنوس اتریومی است. گزینه‌های مطرح احتمالاً Proof of Authority یا یک Proof of Stake کنسرسیومی خواهد بود؛ چرا که شبکه همچنان مجوزی (permissioned) باقی می‌ماند و اعضای اعتبارسنج همان میزبان‌های منتخب هستند. اگر PoA انتخاب شود، مثلاً الگوریتم IBFT یا Clique (مشابه شبکه‌های Quorum) قابل استفاده است. اگر PoS باشد، باید مدلی برای اختصاص سهام به میزبان‌ها تعریف شود (مثلاً هر میزبان مقداری پیمان به عنوان وثیقه در یک قرارداد قفل کند). تصمیم‌گیری در این خصوص نیازمند اجماع اعضای بنیاد و در نظر گرفتن ملاحظات حقوقی است (مثلاً آیا واژهٔ «ماینر» در اسناد حقوقی نباید به کار رود و فقط از «میزبان/اعتبارسنج» استفاده شود). پس از تعیین، پیاده‌سازی به صورت آزمایشی در راخ یا محیط موازی انجام و پارامترهای آن تنظیم می‌شود (تعداد تاییدیه لازم، زمان بلاک و ...).

۶. انتقال داده‌ها و دارایی‌ها

این گام از حساس‌ترین مراحل است. باید مشخص شود چگونه دفتر کل فعلی ققنوس (شامل موجودی حساب‌ها، سوابق تراکنش‌ها، دارایی‌های منتشرشده و ...) به پلتفرم جدید منتقل می‌شود. دو رویکرد اصلی وجود دارد: رویکرد Big-Bang (یکباره) و رویکرد Phased (مرحله‌ای). در روش یکباره، در یک تاریخ/ساعت مشخص شبکه قدیم متوقف و یک اسنپ‌شات از تمام موجودی‌ها گرفته می‌شود؛ سپس در شبکه جدید همان موجودی‌ها به حساب‌های معادل تخصیص می‌یابد و شبکهٔ جدید شروع به کار می‌کند. این روش سریع‌تر است ولی ریسک بالایی دارد (در صورت اشتباه، برگشت سخت خواهد بود). در روش مرحله‌ای، ممکن است دارایی‌ها طی چند مرحله یا دارایی به دارایی منتقل شوند. مثلاً ابتدا فقط توکن پیمان به شبکه جدید برده شود و مدتی هر دو شبکه فعال باشند ولی پیمان عملاً روی شبکه جدید گردش کند (شبکه قدیم صرفاً برای سایر توکن‌ها موقتاً فعال بماند). سپس به تدریج دارایی‌های دیگر هم مهاجرت کنند. حتی می‌توان پل موقت میان دو شبکه ایجاد کرد تا کاربران خود دارایی‌شان را تبدیل کنند (شبیه مکانیزمی که پروژهٔ SIX Network برای مهاجرت توکنش از استلار به اتریوم به‌کار گرفت[six.networksix.network](six.networksix.network)). تصمیم دربارهٔ روش انتقال باید با درنظرگیری تجربهٔ کاربری، ریسک گم‌شدن دارایی‌ها و هزینهٔ عملیاتی اتخاذ شود.

۷. راه‌اندازی شبکه ققنوس ۲.۰ (اتریومی) و خاموش‌کردن تدریجی شبکه قدیم

پس از طی مراحل قبل و اطمینان از آمادگی کامل، لحظهٔ سرنوشت‌ساز فرا می‌رسد: شبکهٔ جدید رسماً آغاز به کار می‌کند. این رویداد احتمالاً با نسخهٔ ۲.۱ یا ۳.۰ سپیدنامه همراه خواهد بود که همهٔ تغییرات را منعکس کرده است. تمامی میزبان‌ها نرم‌افزارهای گره جدید خود را اجرا می‌کنند و ارتباطات بین گره‌ها از پروتکل SCP به پروتکل جدید اجماع تغییر می‌یابد. انتظار می‌رود کاربران نهایی تغییر چندانی در ظاهر حس نکنند؛ کیف‌پول همان رابط کاربری را دارد و حساب‌ها و موجودی‌هاشان را نشان می‌دهد، هرچند در پشت صحنه دیگر استلار کور نبوده بلکه مثلاً Besu یا Geth در حال اجرای شبکه است. برای اطمینان از صحت انتقال، یک دورهٔ موازی در نظر گرفته می‌شود که در طی آن شبکه قدیم به حالت فقط-خواندنی (Read-Only) در می‌آید؛ یعنی دیگر تراکنشی

نمی‌پذیرد ولی اعضا برای اطمینان می‌توانند دفاتر قدیم را چک کنند و با جدید مقایسه کنند. پس از گذشت مثلاً چند هفته و عدم مشاهدهٔ مشکل، شبکه قدیم بطور کامل خاموش می‌شود. نکتهٔ مهم در این گام، اطلاع‌رسانی شفاف به جامعه است تا هیچ کاربری مثلاً به شبکه قدیم تراکنش نفرستد یا گمراه نشود. احتمالاً با همکاری رسانه‌های مرتبط و حتی اپ استورها (برای نمایش اخطار در نسخه‌های قدیمی کیف‌پول) این آگاهی‌رسانی انجام می‌شود.

۸. پساسازی (Post-Migration)

کار مهاجرت با شروع شبکهٔ جدید تمام نمی‌شود. باید پایش مداوم شبکه انجام شود تا هر خلل امنیتی یا عملکردی سریعا رفع شود. همچنین بازخورد کاربران جمع‌آوری گردد؛ ممکن است در عمل برخی فرآیندها نیاز به تنظیم یا اصلاح داشته باشد. بنیاد ققنوس در این دورهٔ پس از مهاجرت احتمالاً گزارشی جامع از این گذار منتشر می‌کند تا هم برای خودش درس‌آموخته باشد و هم سایر پروژه‌ها بتوانند استفاده کنند. از بُعد فرهنگی، حالا زمان آن است که ارزش‌های افزودهٔ شبکهٔ جدید پررنگ شود: مثلاً نشان داده شود که به لطف EVM، چه خدمات نوآورانه‌ای امکان‌پذیر شده که قبلاً نبود. این کار باعث دلگرمی اعضا و کاربران می‌شود که زحمات مهاجرت ثمربخش بوده است.

برای وضوح بیش‌تر، جدول زیر خلاصه‌ای از مهم‌ترین تغییرات فنی و عملیاتی در مهاجرت ققنوس به اتریوم را مقایسه می‌کند:

جنبه	وضعیت در معماری فعلی (استلاری)	وضعیت در معماری جدید (اتریومی)
اجماع و نودها	الگوریتم SCP استلار (FBA) بین ~۸ میزبان؛ نودها Stellar-Core اجرا می‌کنند.	الگوریتم PoA/PoS کنسرسیومی بین همان میزبان‌ها؛ نودها کلاینت Ethereum (مثلاً Besu/Geth) اجرا می‌کنند.
قراردادهای هوشمند	پشتیبانی محدود (از طریق تراکنش‌های چند امضایی و زمان‌بندی در استلار)linkedin.com؛ بدون ماشین تورینگ‌کامل.	پشتیبانی کامل از قراردادهای سالیدیتی/ وایپر با EVM؛ امکان اجرای DAppها و DeFi.
دارایی‌ها و توکن‌ها	توکن‌های IOU منتشر شده توسط میزبان‌ها؛ پیمان به عنوان کارمزد و واسط تبادل exir.io. امکان فریز توسط ناشر.	توکن‌های ERC-20/ERC-721 منتشرشده توسط قراردادهای هوشمند؛ پیمان احتمالاً همچنان توکن پایه (در قالب قرارداد) است. قابلیت‌های پیشرفته در قرارداد (مثلاً Freeze/Pause) قابل تعریف.
هویت و انطباق	هویت در لایهٔ بیرون-زنجیره مدیریت می‌شود (KYC توسط میزبان، سرورهای Compliance)kuknos.org؛ آدرس‌های بلاکچین به هویت‌های دنیای واقعی نگاشت می‌شوند.	امکان ثبت یا لینک‌دادن هویت‌ها روی زنجیره (از طریق توکن‌های هویتی، قراردادهای KYC)؛ همچنان میزبان‌ها نقش تأیید کننده هویت را دارند اما قراردادها فقط به آدرس‌های مجاز اجازهٔ تعامل می‌دهند.
مقیاس‌پذیری و TPS	~۱۰۰۰ TPS، نهایی شدن ~۵ ثانیه؛ مناسب پرداخت.	وابسته به پارامترهای شبکه جدید (احتمالاً TPS کمتر بدون بهینه‌سازی خاص). در صورت نیاز استفاده از راهکارهای لایه۲ آتی.

ابزار توسعه	ابزارهای محدود (سفارشی برای استلار فورک‌شده)؛ جامعهٔ برنامه‌نویسان کوچک و خاص.	ابزارها و کتابخانه‌های استاندارد اتریوم (Web3, Truffle, OpenZeppelin و ...)، بهره‌مندی از جامعه بزرگ توسعه‌دهندگان six.network.
اتصالات برون‌شبکه	نیاز به Gatewayهای مخصوص برای اتصال به اتریوم یا شبکه‌های دیگر؛ تاکنون Bridge محدودی وجود داشت (مثلاً Cross-Chain Service ققنوس).	امکان بهره‌گیری از Bridgeهای موجود اتریوم به سایر زنجیره‌ها (مثلاً استفاده از Allbridge برای ارتباط با استلار، سولانا و ...stellar.org)؛ تعامل ساده‌تر با صرافی‌های بین‌المللی برای لیست‌شدن توکن‌ها six.networksix.network.
حاکمیت شبکه	ساختار بنیاد ققنوس، رأی‌گیری آفلاین بین میزبان‌ها؛ DAO پایه‌ریزی‌شده روی اتریوم برای برخی امور dayadiamond.ir.	امکان استفاده کامل‌تر از DAOهای آن‌چین برای حاکمیت (مثلاً رأی‌گیری ارتقاء شبکه، اضافه‌کردن میزبان جدید از طریق قرارداد هوشمند)؛ شفافیت بالاتر و تغییرناپذیری قوانین حاکمیتی روی زنجیره.

این جدول نشان می‌دهد که حرکت به سوی معماری اتریومی تغییرات متنوعی به همراه دارد؛ از زیرساخت فنی گرفته تا تجربیات کاربری و حاکمیت. در ادامه به‌طور ویژه ملاحظات قانونی این گذار را بررسی می‌کنیم.

الزامات قانونی و انطباقی میزبان‌های ایرانی و پوشش آن توسط اتریوم

فعالیت شبکه ققنوس در چارچوب قوانین و مقررات جمهوری اسلامی ایران انجام می‌شود. میزبان‌های ققنوس عمدتاً بانک‌ها و مؤسسات مالی دارای مجوز هستند، بنابراین رعایت الزامات قانونی مانند KYC/AML، قوانین بانک مرکزی، مقررات مبارزه با تأمین مالی تروریسم و تطبیق با ضوابط بورس (در مورد توکن‌های اوراق بهادار) برایشان اجباری است kuknos.org. در معماری فعلی، همان‌طور که اشاره شد، این الزامات از طریق راهکارهای خارج از زنجیره تأمین می‌شود؛ مثلاً هر میزبان یک سامانهٔ انطباق دارد که پیش از صدور تراکنش، اطلاعات هویتی فرستنده و گیرنده را تطبیق می‌دهد kuknos.org و در صورت تأیید، تراکنش را به شبکه می‌فرستد. همچنین ناشران می‌توانند توکن‌های خود را مسدود یا توقیف کنند (feature Freeze در استلار) تا در صورت دستور مقام قضایی، دارایی متخلف بلوکه شود. حال سوال این است که با مهاجرت به پلتفرم اتریوم و افزایش ویژگی‌های غیرمتمرکز، چگونه می‌توان این نیازهای قانونی را برآورده ساخت؟

کنترل دسترسی و لیست‌های مجاز/ممنوع

خوشبختانه، اتریوم به دلیل قابل‌برنامه‌ریزبودن، امکان تعریف قواعد سفارشی در قراردادهای هوشمند را فراهم می‌کند. به عنوان نمونه، می‌توان توکن پیمان و سایر توکن‌های مهم را نه به شکل ERC-20 ساده، بلکه به صورت توکن دارای کنترل دسترسی پیاده کرد. از استانداردهای موجود می‌توان به ERC-1404 (توکن با محدودیت انتقال) یا حتی ERC-20 همراه با مکانیزم transferAllowed اشاره کرد. در این روش، هر بار که توکن قرار است منتقل شود، قرارداد هوشمند یک لیست یا قانون را چک می‌کند تا ببیند آیا هر دو آدرس فرستنده و گیرنده در لیست مجاز (Whitelist) قرار دارند یا خیر. این لیست مجاز می‌تواند توسط هر میزبان برای مشتریان خودش مدیریت شود. به عنوان مثال، بانک ملی یک قرارداد «لیست سفید» دارد که آدرس‌های اتریومی تمامی مشتریان تأییدشده‌اش را ثبت کرده است. قرارداد توکن پیمان طوری برنامه‌ریزی می‌شود که فقط اجازه انتقال به/از آدرس‌هایی را بدهد که حداقل در یکی از لیست‌های سفید میزبان‌ها وجود داشته باشند. بدین ترتیب نقل و انتقال توکن بدون احراز هویت عملاً ممکن نخواهد بود حتی اگر شبکه باز به نظر برسد. از سوی دیگر، برای پاسخ به دستور قضایی مبنی بر توقیف دارایی یک شخص، می‌توان از امکانات pause یا freeze در قرارداد بهره گرفت؛ مثلاً نقش «قاضی» تعریف شود که اجازه دارد یک آدرس خاص را در توکن Mark as frozen کند و قرارداد از آن پس انتقال از/به آن آدرس را مسدود خواهد کرد. تمامی این منطق‌ها باید در زمان طراحی

قراردادهای اصلی شبکه (توکن‌های بنیادین و perhaps یک لایهٔ کنترل تراکنش) لحاظ شود تا انطباق‌پذیری قانونی در بطن پروتکل تضمین گردد.

حفظ حریم خصوصی و دسترسی نظارتی

در مقررات ایران، حفاظت از داده‌های کاربران مهم است ولی در عین حال نهادهای نظارتی باید امکان پیگیری تراکنش‌های مشکوک را داشته باشند. بلاکچین عمومی اتریوم کاملاً شفاف است و هرکس می‌تواند کل تاریخچه را ببیند. اگرچه ققنوس یک شبکه خصوصی/کنسرسیومی است، اما مشابه اتریوم عمل می‌کند و همهٔ میزبان‌ها به تمام تراکنش‌ها دسترسی خواهند داشت. این سطح شفافیت برای بسیاری از الزامات نظارتی مفید است (زیرا جعل و تغییر در داده امکان‌پذیر نیست). با این حال، برای حفظ حریم شخصی کاربران عادی، شاید نیاز باشد برخی اطلاعات حساس (مثل نام صاحب حساب) مستقیماً روی زنجیره ذخیره نشود. اتریوم می‌تواند این را با استفاده از شناساگرهای مستعار و اثبات دانش صفر حل کند. برای مثال، به جای اینکه کد ملی فرد روی زنجیره بیاید، یک هش از آن یا یک شناسهٔ داخلی ققنوس استفاده می‌شود که تنها میزبان مربوطه می‌تواند آن را به هویت واقعی نگاشت کند. از طرف دیگر، می‌توان از قراردادهای ثبت لاگ‌های انطباقی استفاده کرد؛ مثلاً هر تراکنش علاوه بر انتقال توکن، یک رویداد لاگ حاوی کد میزبان‌های مبدا و مقصد ثبت نماید. این لاگ‌ها به نهاد ناظری مانند دبیرخانهٔ ققنوس یا حتی بانک مرکزی اجازه می‌دهد ترافیک بین میزبان‌ها را پایش کند بدون اینکه جزئیات ریز هویت افراد را ببینند. چنین طراحی‌هایی نیازمند مشورت با حقوقدانان و متخصصان حریم خصوصی است تا ضمن تأمین الزامات قانون مبارزه با پولشویی (که نیازمند امکان ردیابی است)، حقوق شهروندی افراد نیز رعایت شود.

قراردادهای هوشمند قابل اعتماد و ممیزی

یک دغدغهٔ رگولاتوری دیگر این است که کدهای خودکار (قراردادها) مبادا حاوی باگ یا رفتار مخربی باشند که به زیان عموم تمام شود. در سیستم قدیم، چون منطق‌ها بیشتر خارج از زنجیره بود، تنظیم‌گر می‌توانست با اطمینان از عملکرد مؤسسات مالی نظارت کند. در شبکهٔ جدید، باید ترتیبی اتخاذ شود که قراردادهای مهم قبل از اجرا، ممیزی و تأییدیهٔ رسمی دریافت کنند. برای این منظور می‌توان یک چارچوب صدور گواهی قرارداد تعریف کرد. مثلاً هر قرارداد هوشمند مرتبط با توکن‌های مالی باید توسط حداقل X میزبان معتبر (یا یک کمیته تخصصی) امضا و تأیید شود تا اجازه Deployment روی شبکه اصلی بیابد. این امضاها می‌تواند در متادیتای قرارداد ثبت شود و کاربران نیز هنگام تعامل، از طریق واسط کاربری ببینند که قرارداد مذکور تأیید شده و هویت نویسنده و تأیید کنندگان مشخص است. چنین راهکاری هم از نظر فنی ممکن است (با استفاده از استاندارد ERC-1820 یا یک registry از قراردادهای مجاز) و هم اعتماد قانون‌گذاران را جلب می‌کند که شبکه رها نشده تا هر کس کد دلخواهش را روی آن اجرا کند.

رعایت قوانین پولی و مالی

برخی قوانین مشخص در ایران وجود دارد که باید در طراحی جدید ملحوظ شوند. برای مثال، سقف تراکنش‌های ریالی روزانه برای افراد یا محدودیت حجم انتقال ارز. در سیستم بانکی سنتی این با سخت‌گیری بانک‌ها انجام می‌شود. در شبکه ققنوس، احتمالاً انتقال ریال توکنیزه‌شده هم باید سقف داشته باشد. این را می‌توان در قرارداد توکن ریال برنامه‌ریزی کرد که مثلاً هر آدرس شخصی حداکثر N ریال در روز می‌تواند منتقل کند (با استفاده از timestampها و محدودیت در کد). یا مثلاً کارمزدهای شبکه: در استلار کارمزد اندک بود (مثلاً ۰٫۰۰۰۰۱ پیمان) صرفاً برای جلوگیری از اسپم. در شبکه جدید شاید نیاز باشد کارمزدها را بیشتر تنظیم کرد تا هزینه اجرای قراردادها تأمین شود. این البته اقتصادی است ولی بُعد قانونی آن هم مطرح است چون نباید آنقدر بالا باشد که خدمات مالی دچار اختلال شوند. تصمیماتی از این قبیل (نرخ کارمزد، نحوه توزیع کارمزد بین میزبان‌ها و صندوق‌های ضمانت و غیره) نیازمند تصویب بنیاد با درنظرگیری قوانین تجارت الکترونیک و بانکداری است.

استفاده از ابزارهای اتریوم برای تطبیق

سخن پایانی در این بخش: اتریوم اکوسیستم پرباری از ابزارهای انطباق و رگ‌تک (RegTech) دارد که ققنوس می‌تواند آنها را به خدمت بگیرد. برای نمونه، تحلیلگرهای تراکنش که در Ethereum برای کشف فعالیت‌های مشکوک (مثل پولشویی) استفاده می‌شوندsix.networksix.network، می‌توانند با داده‌های بلاکچین ققنوس آموزش داده شوند و به واحدهای تطبیق میزبان‌ها

بینش بهتری دربارهٔ الگوهای تراکنش بدهند. یا کیف‌پول‌های قرارداد هوشمند که امکان تعریف امضای دوتایی یا محدودیت برداشت روزانه دارند، می‌توانند برای حساب‌های کاربران پیاده شود تا اگر قانون‌گذار خواست سقف برداشت را enforce کند، از طریق خود قرارداد کیف‌پول اجرایی شود نه صرفاً توافق‌نامهٔ کاربری. این‌ها همه نشان می‌دهد فناوری اتریوم نه تنها مانعی برای رعایت قانون نیست، بلکه می‌تواند با ابزارسازی مناسب، ضامن بهتری هم باشد. مهم این است که طراحان شبکه ققنوس جدید از ابتدا این ملاحظات را در architecture مدنظر قرار دهند.

مطالعهٔ موارد مشابه: مهاجرت از استلار به اتریوم در عمل

حرکت ققنوس به سمت اتریوم پدیده‌ای منحصربه‌فرد نیست و در اکوسیستم بلاکچین، نمونه‌هایی از تصمیم به مهاجرت یا پل‌زدن میان پلتفرم استلار و اتریوم وجود داشته که می‌توان از تجربهٔ آن‌ها بهره برد. در این بخش به چند نمونه و تحلیل کلان اشاره می‌کنیم:

۱. مهاجرت توکن SIX از استلار به اتریوم (۲۰۲۳)

شبکه SIX که یک پروژهٔ بلاکچینی در جنوب شرق آسیا است، در اواخر ۲۰۲۳ اعلام کرد توکن اصلی خود را از استلار به استاندارد ERC-20 اتریوم منتقل می‌کند six.network. دلایل آنها جالب توجه است: بهره‌گیری از قدرت ماشین مجازی اتریوم و امکان تعامل توکن SIX با قراردادهای هوشمند six.network، دسترسی به اکوسیستم پرجنب‌وجوش اتریوم شامل DAO، DeFiها، NFTها و ... six.network، افزایش نقدشوندگی و دسترسی به صرافی‌های بزرگ که عمدتاً از توکن‌های اتریومی پشتیبانی می‌کنند six.network و جذب اعتماد بیشتر از سوی موسسات بین‌المللی به‌دلیل شناخته‌شده‌بودن اتریوم six.network. این مهاجرت گرچه صرفاً انتقال یک دارایی بوده (و نه کل شبکه)، اما نشان داد که حتی پروژه‌هایی که روزی به خاطر کارمزد پایین و سرعت به استلار روی آورده بودند، برای بهره‌مندی از قابلیت‌های پیشرفته اتریوم حاضرند هزینه و پیچیدگی مهاجرت را بپذیرند. ققنوس نیز می‌تواند از استدلال مشابهی بهره ببرد؛ چرا که اتریوم زیرساخت مناسب‌تری برای نوآوری مالی و قراردادهای هوشمند پیچیده فراهم می‌کند linkedin.com.

۲. پروژه StarBridge و پل‌های استلار-اتریوم

Stellar Development Foundation در سال‌های اخیر روی پروژه‌ای به نام StarBridge کار کرده که هدف آن ایجاد پل غیرمتمرکز بین شبکه استلار و زنجیره‌هایی مانند اتریوم است leighmcculloch.com. این پل به کاربران اجازه می‌دهد دارایی‌هایی چون USDC را بین استلار و اتریوم جابجا کنند stellar.org. هرچند Soroban (پلتفرم قراردادهای هوشمند بومی استلار) بعدها معرفی شد، اما وجود چنین پل‌هایی نشان‌دهندهٔ رغبت جامعهٔ استلار به تعامل با اتریوم است. ققنوس در مقایسه راه جسورتری انتخاب کرده و به جای پل‌زدن بین دو شبکه مجزا، می‌خواهد ماهیت شبکه را اتریومی کند. اما در هر حال تجربهٔ StarBridge و حتی پل‌های شخص ثالث (مثل AllBridge یا Transfuse) می‌تواند از نظر مکانیزم‌های فنی bridging و امنیت حفره‌های دو زنجیره برای ما آموزنده باشد stellar.org.

۳. تجربه Kin: تغییر مسیر از استلار به سولانا (و بالعکس)

ارز دیجیتال Kin ابتدا یک توکن ERC-20 بود، سپس در ۲۰۱۸ تصمیم گرفت بلاکچین اختصاصی خود مبتنی بر فورک استلار بسازد تا کارمزدها را حذف و سرعت را بالا ببرد. جالب این که بعدها در ۲۰۲۰ این پروژه باز هم مهاجرت کرد و این بار به سولانا نقل مکان کرد، چون احساس شد مقیاس‌پذیری و پشتیبانی توسعه‌دهندگان در سولانا بهتر است. از این داستان می‌توان نتیجه گرفت که انتخاب پلتفرم بلاکچین امری ایستا نیست و بسته به شرایط و پیشرفت‌ها، پروژه‌ها ممکن است چندین بار مهاجرت کنند. بنابراین ققنوس باید نگاه بلندمدت داشته باشد: مهاجرت به اتریوم نباید پایان راه نوآوری باشد. بلکه باید زیرساخت را طوری بنا کند که اگر در آینده نیاز به بهره‌گیری از راهکارهای لایه ۲ اتریوم (مانند رول‌آپ‌ها برای افزایش TPS) یا حتی سوئیچ به پلتفرم‌های تازه (مثلاً در آینده دور یک تکنولوژی جدید) بود، انعطاف و امکان انجام آن وجود داشته باشد. خوشبختانه طراحی ماژولار با استفاده از پل‌ها و لایهٔ تطبیق

که در این گزارش ارائه شد، این قابلیت را ذاتاً دارد؛ زیرا هم‌اکنون هم یک لایهٔ ترجمه بین استلار و اتریوم تعریف کرده‌ایم که می‌تواند در آینده بین اتریوم و هر زنجیرهٔ دیگری تطبیق یابد.

۴. تحلیل مقایسه‌ای پلتفرم‌ها

برخی کارشناسان صنعت بلاکچین، اتریوم و استلار را مکمل اهداف متفاوت دانسته‌اند. برای مثال Marcin Rzetecki در لینکدین اشاره می‌کند که «اتریوم یک پلتفرم جهانی منبع‌باز برای اپ‌های غیرمتمرکز است که می‌توان روی آن کدی (قرارداد هوشمند) نوشت که ارزش دیجیتال را کنترل کند و همان‌طور که برنامه‌ریزی شده اجرا شود، در حالی که استلار یک شبکهٔ باز برای ذخیره و جابجایی پول است. به‌بیان دیگر اتریوم در پیاده‌سازی قراردادهای هوشمند در یکپارچه‌سازی‌های کسب‌وکار عملکرد بهتری دارد، درحالی‌که استلار تسهیل انتقال وجوه را بر عهده دارد linkedin.com.» همچنین تاکید می‌کند که استلار اساساً ماشین مجازی داخلی برای کدنویسی دلخواه ندارد و قراردادهای هوشمندش صرفاً از کنار هم چیدن تراکنش‌ها و شرایط حاصل می‌شودlinkedin.com. این تحلیل، تصمیم ققنوس برای تغییر زیرساخت را تائید می‌کند: ققنوس در مرحله‌ای است که از صرفاً نقل‌وانتقال توکن فراتر رفته و نیازمند منطق‌های قراردادی پیچیده (مثلاً برای بازار سرمایه، بیمه، تأمین مالی جمعی و ...) است. بنابراین انتخاب اتریوم به عنوان بستر جدید منطقی و مطابق روند صنعت است. به علاوه، جامعه توسعه‌دهندگان اتریوم بسیار گسترده‌تر بوده و منابع آموزشی، کتابخانه‌ها و ابزارهای متعددی داردsix.network که می‌تواند نوآوری در ققنوس را شتاب دهد.

۵. سایر ملاحظات

مهاجرت‌های موفق معمولاً آن‌هایی بوده‌اند که کاربران را در تصمیم مشارکت داده و مزایا را شفاف کرده‌اند. برای نمونه، پروژه SIX قبل از مهاجرت با ارائه اینفوگرافیک و جزئیات به کاربران خود اطمینان خاطر داد که دارایی‌شان از بین نمی‌رود و برای تبدیل فرصت کافی خواهند داشتsix.network. همچنین مزایای ملموس (مثل امکان استفاده از کیف‌پول‌های اتریوم و شرکت در ییلد فارمینگ) را برجسته کرد six.networksix.network. ققنوس نیز باید از لحاظ ارتباطات عمومی (PR) دقیق عمل کند. کاربران نهایی شاید درکی از تفاوت استلار و اتریوم نداشته باشند؛ لذا باید به زبان ساده برایشان توضیح داد که شبکهٔ جدید چه کارهایی می‌تواند بکند که قبلاً ممکن نبود (مثلاً «وام‌دهی خودکار روی وثیقه طلا» یا «خرید و فروش توکن‌ها بدون نیاز به صرافی‌های متمرکز» و ...). همچنین احتمال دارد نگرانی‌هایی مطرح شود، مثل امنیت قراردادهای هوشمند (با توجه به اخبار هک در دیفای). بنیاد باید برنامهٔ خود برای ممیزی امنیتی و استفاده از بهترین رویه‌ها (مانند چارچوب OpenZeppelin) را بیان کند تا اعتمادسازی صورت گیرد.

در مجموع، با بررسی تجارب مشابه می‌توان نتیجه گرفت که مهاجرت ققنوس به معماری اتریومی یک حرکت استراتژیک مثبت برای بقای بلندمدت و رشد اکوسیستم آن است، به شرط آنکه به‌درستی مدیریت شود. مزایایی چون دسترسی به اکوسیستم جهانی اتریوم، امکان برنامه‌ریزی و انعطاف در محصولات مالیsix.network، جذب توسعه‌دهندگان بیشتر و ارتقای جایگاه تکنولوژیک شبکه، کفهٔ ترازو را سنگین‌تر از چالش‌ها می‌کند. از سوی دیگر، موفقیت این طرح نیازمند دقت فنی، شفافیت حقوقی، آموزش و همراه‌سازی کاربران است؛ همان عواملی که در مطالعهٔ موارد بالا نیز بارها به چشم خورد.

جمع‌بندی

طراحی و پیاده‌سازی ماشین اتریومی برای انکر دایاچین و مهاجرت تدریجی شبکه ققنوس به معماری جدید، گامی بزرگ در تحول پلتفرم توکنایز ایران به‌شمار می‌رود. در این گزارش، معماری پیشنهادی را با جزئیات تشریح کردیم: ماشینی مبتنی بر EVM که از طریق یک مبدّل هوشمند، با شبکهٔ استلاری فعلی هماهنگ می‌شود و امکان اجرای قراردادهای هوشمند را فراهم می‌سازد بدون آن‌که سایر نودها متوجه تفاوتی شوند. سپس دیدیم که انکر دایاچین چگونه می‌تواند نقش پل دنیای قدیم و جدید را ایفا کند و سناریوهایی از کاربردهای عملی آن (از DeFi گرفته تا بهبود تجربهٔ کاربری) مطرح شد. شبکهٔ آزمایشی راخ را به‌عنوان آزمایشگاه نوآوری معرفی کردیم که محیطی کم‌ریسک برای آزمون فناوری جدید توسط کاربران با هویت‌های فعلی‌شان است و می‌تواند به عنوان بستری دائمی برای آزمایش و آموزش باقی بماند. نقشهٔ راه مهاجرت کامل را در هشت گام از فاز آزمایشی تا راه‌اندازی شبکهٔ نهایی و بعد آن تدوین کردیم و بر اهمیت هر مرحله – چه از نظر فنی (اجماع، انتقال داده) و چه غیر فنی (حقوقی، آموزشی، فرهنگی) – تاکید شد. در بخش الزامات قانونی نشان دادیم که فناوری اتریوم توان انعطاف‌پذیری بالایی برای پوشش نیازهای رگولاتوری ایران دارد؛ به شرط مهندسی صحیح می‌توان تمامی ملزومات KYC/AML، کنترل نقل‌وانتقالات و دستورات قضایی را در قالب قراردادهای هوشمند و

سازوکارهای زنجیره‌ای گنجاند و حتی نظارت را شفاف‌تر و لحظه‌ای‌تر کرد linkedin.comkuknos.org. در پایان، مروری بر موارد مشابه در دنیا داشتیم که مؤید تصمیم ققنوس در حرکت به سوی اتریوم است – چرا که مسیر آیندهٔ بلاکچین برای ارائه خدمات مالی نوین، ناگزیر از قراردادهای هوشمند و تعامل‌پذیری بیشتر است coindesk.com.

ققنوس با این مهاجرت، از پوستهٔ یک شبکه بستهٔ اختصاصی به درخواهد آمد و به بخش فعالی از اکوسیستم جهانی بلاکچین بدل خواهد شد. البته شبکه همچنان کنترل‌شده و منطبق با قوانین کشور عمل می‌کند، اما از نظر تکنیکی روی ریل استانداردی می‌افتد که توسعه بین‌المللی را تسهیل می‌کند. این بدان معناست که در آینده می‌توان همکاری‌ها و ابتکارات مشترک میان ققنوس و سایر شبکه‌های مبتنی بر اتریوم (داخل یا حتی خارج از ایران) را متصور شد – از لیست‌شدن پیمان در صرافی‌های غیرمتمرکز جهانی گرفته تا امکان اتصال نقدینگی شبکه ققنوس با بازارهای دیفایsix.networksix.network. تمامی این فرصت‌ها در گرو اجرای موفقیت‌آمیز برنامهٔ مهاجرت است. خوشبختانه، برنامه‌ریزی و تحلیل انجام‌شده نشان می‌دهد چالش‌های مسیر شناسایی و برایشان راهکار اندیشیده شده است. با پیشروی گام‌به‌گام و مشارکت همه اعضای اکوسیستم ققنوس – از بانک‌ها و شرکت‌های فناوری گرفته تا کاربران نهایی – ققنوسِ نوین همچون ققنوس افسانه‌ای از خاکستر پلتفرم پیشین بر خواهد خاست و فصل تازه‌ای را در اقتصاد دیجیتال ایران رقم خواهد زد.

منابع و مراجع

- سپیدنامه شبکه ققنوس و توکن پیمان (نسخه‌های ۲.۰ و ۲.۱)، بنیاد ققنوس – ۱۴۰۱ و ۱۴۰۲.
- وب‌سایت رسمی ققنوس (kuknos.org) – بخش‌های معرفی شبکه، سوالات متداول و مقالات وبلاگ.
- Rzetecki, M. *"Ethereum smart contracts vs. Stellar smart contracts."* LinkedIn Article, Feb 2020 – مقایسه اتریوم و استلار linkedin.comlinkedin.com.
- SIX Network Blog – *"SIX Token Migrates to Ethereum (ERC-20) — Empowering a New Chapter of Growth!"* Dec 2023 – اعلان رسمی مهاجرت توکن SIX six.networksix.network.
- ThreeFold Manual – *"Ethereum-Stellar Bridge"*. (دستورعمل پل استلار-اتریوم پروژه ThreeFold) – شرح مکانیزم‌های پل زدن دارایی بین استلار و اتریوم manual.threefold.iomanual.threefold.io.
- CoinDesk – *"Stellar … Adds Smart Contracts to Take on Ethereum."* Oct 2023 – گزارش اضافه‌شدن Soroban و تحول استلار coindesk.com.