УДК 004.9
DOI: 10.18523/2617-3808.2025.8.190-196

Яременко П. В., Гороховський К. С.

ОМНІЧЕЙН-ІНТЕГРАЦІЯ ТОКЕНА MOR НА ОСНОВІ СТАНДАРТІВ LAYERZERO OFT І WORMHOLE NTT

У статті представлено проєкт MORSOL — омнічейн-рішення для токена MOR, що поєднує стандарти LayerZero OFT і Wormhole NTT. Архітектура інтегрує Solana (Anchor-програма) та EVM-смартконтракти з мережевими компонентами LayerZero і Wormhole. Для контролю емісії використано мультипідпис: Squads Vault на Solana та Gnosis Safe на EVM. Описано реалізацію механізму burn/mint під час передання токенів між мережами, підтвердження VAA, а також безпекові функції, як-от пауза контрактів і контроль загальної емісії. Результати демонструють, що поєднання OFT і NTT дозволяє створити нативний мультиланцюговий токен MOR без обгортання, зі збереженням єдиної емісії та високою децентралізацією.

Ключові слова: омнічейн, крос-ланцюгова інтеграція, LayerZero OFT, Wormhole NTT, мультипідпис (multisig), Solana, Ethereum, інтероперабельність, децентралізація.

Вступ

У сучасних умовах розвитку блокчейн-екосистем дедалі більшої ваги набуває проблема інтероперабельності — можливості активів і додатків взаємодіяти між різними ланцюгами. Зокрема, існує потреба у тому, щоб криптовалютні токени могли вільно переміщуватися між кількома блокчейнами, залишаючись при цьому єдиним цілісним активом (без створення дублюючих «обгорнутих» версій).

Існують різні міжланцюгові протоколи для передання даних і активів. Одними з провідних рішень у сфері мостів є LayerZero та Wormhole — обидва надають інфраструктуру для обміну повідомленнями між блокчейнами, але реалізують різні моделі безпеки та довіри. LayerZero пропонує стандарт OFT (Omnichain Fungible Token) для випуску токенів одразу на декількох ланцюгах з використанням модульної моделі перевірки повідомлень незалежними верифікаторами (DVN). Wormhole, своєю чергою, запровадив фреймворк NTT (Native Token Transfers) для *нативного мультиланцюгового токена* з довіреною перевіркою повідомлень через децентралізовану мережу вартових (Guardians). Обидва підходи використовують модель burn-and-mint (спалення на вихідному ланцюгу та карбування на цільовому) замість обміну через ліквідні пули, що дозволяє переносити цінність без створення вторинних токенів.

Morpheus (MOR) — нативний токен екосистеми Morpheus (мережі персональних AI-агентів) — було задумано як омнічейн-актив, доступний на кількох платформах Web3.

У цій статті докладно описано реалізацію омнічейн інтеграції MOR, що отримала назву MORSOL. MORSOL забезпечує зв'язок між мережею Solana та EVM-ланцюгами з використанням гібридної архітектури: на Solana розгорнуто смарт-контракт (Anchor-програму), який інтегрується з LayerZero та Wormhole, тоді як на кожному EVM-ланцюгу працює стандартний контракт MOR (ERC-20 з розширенням OFT). Для управління критичними функціями (емісія, налаштування мереж тощо) залучено мультипідписні акаунти: Squads Vault на Solana та Gnosis Safe на Ethereum і сумісних ланцюгах. У розділі **Методологія** розглянуто алгоритми міжланцюгового переказу MOR, зокрема послідовність операцій burn/mint та механізми підтвердження (DVN у LayerZero та VAA у Wormhole). У розділі **Архітектура** описано основні компоненти системи та їхню взаємодію, зокрема роль LayerZero endpoint-контрактів і Wormhole-інфраструктури. Далі, у розділі **Результати**, аналізуються досягнуті показники та досвід використання запропонованої системи. **Висновки** підсумовують отримані результати та окреслюють внесок роботи в галузі мультиланцюгових технологій.

Методологія

Підхід до інтеграції: Проєкт MORSOL ставить за мету зробити токен MOR повноцінним омнічейн-активом, який циркулює одночасно на кількох блокчейнах без створення дублікативних wrapped-версій. Методологія побудована на принципі єдиного глобального балансу: незалежно від того, в якій мережі перебувають монети MOR, загальна кількість токенів в обігу залишається сталою. Для цього всі міжланцюгові трансфери виконуються через спалення та карбування: токени вилучаються (спалюються) з обігу на вихідному ланцюгу і створюються (карбуються) на цільовому ланцюгу у такій самій кількості. Ця модель підтримується як стандартом Wormhole NTT, так і LayerZero OFT, і дозволяє уникнути появи конкурентних копій токена та необхідності довіряти стороннім пулам ліквідності.

Підсумовуючи, методологія реалізації MORSOL базується на поєднанні найкращих практик двох різних протоколів: ми використовуємо стандартні, аудовані компоненти LayerZero та Wormhole без модифікацій ядра, додаючи при цьому свій управлінський шар (мультипідпис) для максимального контролю. Це дає змогу досягти мети — зробити MOR повністю мультиланцюговим токеном — із мінімальними змінами логіки токена.

Архітектура

Огляд архітектури: Система MORSOL складається з компонентів, розгорнутих у двох середовищах — мережі Solana та низці EVM-сумісних мереж, які тісно взаємодіють через повідомлення LayerZero і Wormhole. На рис. 1 (схема архітектури MOR на Solana) представлено загальну структуру рішення.

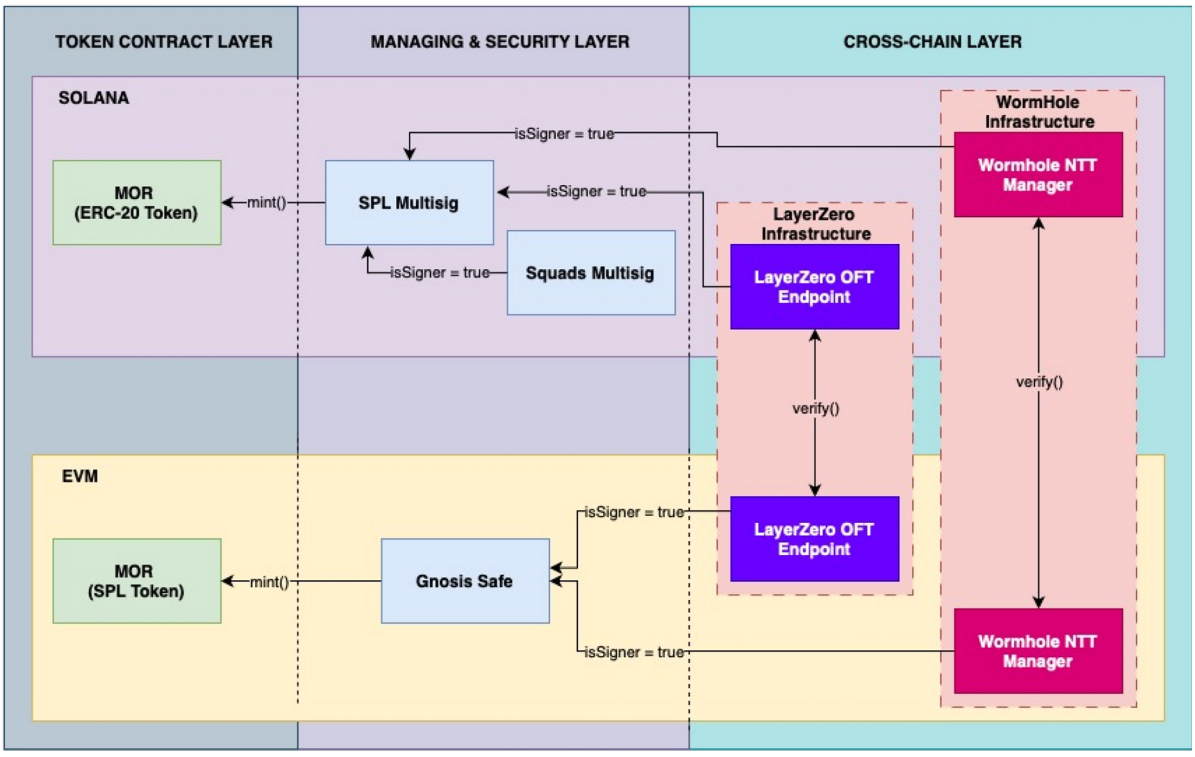

Рис. 1. Архітектура MORSOL

Основні складові можна розділити на кілька рівнів:

- **Рівень токен-контрактів.** Це контракти, що безпосередньо керують балансами MOR у певній мережі. На Solana роль токен-контракту виконує SPL-мінт MOR, а на EVM-ланцюгах — контракт ERC-20 MOR-OFT. Важливо, що всі ці контракти представляють *той самий* токен MOR, тобто загальна емісія розподілена між ними (сумарний оборот постійно 42 млн MOR відповідно до токеноміки). Контракт MOR на EVM успадковує функціонал LayerZero: він інтегрований з Endpoint-контрактом LayerZero і охоплює логіку відправки / отримання крос-ланцюгових

повідомлень. На Solana ж SPL-мінт MOR взаємодіє із Anchor-програмою MORSOL, яка виступає контролером випуску токенів. Той самий підхід реалізовано і для WormHole NTT.

- **Рівень керування і безпеки.** До нього належать *мультипідписні гаманці* та рольові налаштування, що контролюють критичні операції контрактів. У архітектурі MOR реалізовано дворівневу модель контролю: (1) багатопідписний контроль емісії токена на Solana через SPL Multisig та Squads Multisig для додаткової можливості контролю емісії, та (2) мультисиг-контроль адміністративних функцій контрактів на EVM через Gnosis Safe. На Solana SPL Multisig виступає власником (mint authority) токена MOR і має право дозволяти чи блокувати карбування нових монет. Крім того, цей самий мультипідпис може бути призначений повноважним підписантом для критичних інструкцій Anchor-програми (напряму або опосередковано). На EVM-ланцюгах мультипідписні гаманці Gnosis Safe (5 із 9 підписів) контролюють права адміністратора контрактів MOR, тобто можуть затверджувати оновлення логіки, зміну конфігурацій безпеки LayerZero (наприклад, список довірених DVN) або активацію екстрених механізмів на кшталт паузи. У сукупності, мультипідписна інфраструктура додає рівень децентралізованого управління поверх автоматизованих мостів: жоден окремий підписант, окрім контрактів, не здатен одноосібно випустити нові токени або змінити налаштування, не отримавши згоду кількох незалежних сторін.
- **Рівень міжланцюгової логіки.** Це компоненти, що забезпечують надсилання і прийом повідомлень між блокчейнами. У LayerZero це Endpoint-контракти (по одному на кожному ланцюгу); у Wormhole — Core (Core Bridge) контракти та пов'язані з ними NTT Manager контракти. LayerZero Endpoint являє собою універсальний комунікаційний модуль: всі звернення OMNI-додатків (таких як OFT) проходять через нього. Endpoint відповідає за формування стандартного пакета повідомлення, його доставку (разом з обраними DVN (Decentralized Verifier Networks) веріфаєрами) на інший ланцюг та виклик потрібної функції там. Wormhole Core — аналогічний за призначенням модуль, але працює інакше: він записує повідомлення на вихідному ланцюгу та ініціює збір підписів Guardians; на цільовому ланцюгу він перевіряє підписи в VAA (Verified Action Approvals) і передає дані в NTT Manager для виконання трансферу. NTT Manager — це окремий контракт, що розгортається на кожному ланцюгу для конкретного токена; він містить бізнес-логіку роботи з Wormhole (ініціювання burn, прийом VAA, карбування) і, як правило, належить інтегратору токена. У випадку MOR, Anchor-програма MORSOL на Solana підтримує NTT Manager (і одночасно OFT-адаптера) на стороні Solana, а для EVM-ланцюгів цю роль може відігравати або сам контракт MOR (через впровадження інтерфейсу Wormhole), або допоміжний контракт.

Компоненти Solana. В екосистемі Solana токен MOR представлений у вигляді SPL-токена. Його випуск і переміщення контролюються Anchor-програмою MORSOL. Основні інструкції програми охоплюють спалення MOR на Solana та надсилання повідомлення в іншу мережу; карбування MOR на Solana на основі отриманого підтвердження з іншого ланцюга та інші інфраструктурні задачі.

З погляду міжмережевої комунікації, Solana взаємодіє як із LayerZero, так і з Wormhole. MORSOL підключає Endpoint через CPI (Cross-Program Invocation): при відправці токенів у EVM вона викликає функцію Endpoint send() з необхідними параметрами, а при отриманні — Endpoint сам викликає зареєстрований хендлер програми після верифікації повідомлення (аналогічно до того, як це відбувається в EVM контрактах OFT). Взаємодія з Wormhole здійснюється через вбудовані програми Solana: Wormhole Core Bridge (Program Id відповідного моста) та, за необхідності, Wormhole Token Bridge. Для NTT-режиму Token Bridge може працювати в спеціальному режимі: MOR може бути зареєстрований як *нативний токен* замість стандартного обгорнутого. В будь-якому разі, мультипідпис на Solana є центральною ланкою: він зберігає mint-authority MOR та визначає, кому довірено право карбування. Так, при розгортанні MOR було створено обліковий запис-мультисиг (структура Solana, де задано M підписантів із N і поріг 1) і призначено Authority для MOR-мінта. Потім до списку підписантів цього мультисіг-акаунту були додані: (1) PDA скарбниці Squads (Vault PDA), (2) PDA самої Anchor-програми MORSOL як потенційний співпідписант, (3) зарезервоване місце для Wormhole NTT (буде додано після розгортання). Порог підписів встановлено таким чином, щоб для карбування MOR був потрібен підпис програми + підтвердження Vault (умовно 2 з 2) або, на перехідний період, 1 з 2 (де достатньо підпису програми за наявності VAA). Це означає, що навіть коли Anchor-програма виконує інструкцію карбування токенів (наприклад, при надходженні повідомлення з Ethereum), фінальна дія mint_to виконується токен-програмою Solana тільки за умови,

що підпис мультисиг-акаунту валідовано [1]. Практично, SquadsVault може *наперед схвалювати* певні дії в межах встановлених політик, наприклад дозволити програмі MORSOL карбувати до X токенів на добу, але в будь-якому разі програма не зможе перевищити ті ліміти без згоди кворуму ключів. Цей багатопідписний механізм істотно підвищує безпеку: навіть у разі теоретичного злому міжланцюгового мосту зловмисник не зможе самостійно «надрукувати» MOR на Solana — потрібна дія, схвалена колективно.

Компоненти EVM. На стороні EVM до архітектури входять один або кілька контрактів MOR (ERC-20/OFT) і потенційно допоміжні контракти-мости. Під час запуску MOR було вирішено максимально використовувати типовий контракт OFT від LayerZero без модифікацій протоколу. Контракт MOROFT.sol успадковує клас OFTCore (для нових токенів) і реалізує стандартні методи ERC-20 (transfer, balanceOf тощо) разом з новими (sendFrom, estimateSendFee тощо). Особливістю MOR є те, що його випуск здійснювався за схемою *Fair Launch* із розподілом на кількох мережах, тому контракт має фіксовану загальну кількість 42,000,000 MOR, але на початку не всі монети були випущені одразу на всіх ланцюгах. Контракт MOR на Ethereum був розгорнутий як основний мінт, із початковим випуском певної частини токенів, інші мережі почали з нульовим балансом і отримували токени в міру їх претендування або перенесення з Ethereum. Контракт MOROFT налаштований таким чином, що право карбування (mint) на ньому жорстко закріплене за окремим обліковим записом — L2MessageReceiver (або іншим контрактом-дистриб'ютором). Це зроблено для розмежування ролей: сам токен не може бути *довільно* накарбований навіть власником — випуск нових монет відбувається лише за наявності валідного крос-ланцюгового запиту (через контракт-посередник). Таким посередником в екосистемі MOR слугує контракт розподілу, що отримує підтвердження про зарезервовані для користувача токени з «головного» ланцюга і викликає mint на локальному MOR (це стосується фази емісії токена). У контексті міжланцюгових переказів функцію посередника виконує LayerZero механізм: коли MOR надходить з іншого ланцюга, повідомлення потрапляє прямо у функцію onOFTReceived контракту MOR, який і карбує монети для отримувача. Адміністраторські права контракту MOR (як-от призначення нового власника чи оновлення Proxy-логіки, якщо така використовується) закріплені за мультисиг-гаманцем Gnosis Safe. Для MOR був налаштований Gnosis Safe 5/9 на кожному основному EVM-ланцюгу, що включає ключі декількох членів спільноти Morpheus. Таким чином, усі незвичайні дії з контрактом MOR (наприклад, активація *pause* у LayerZero Endpoint або зміна налаштувань Trusted Remote) потребують колективного рішення декількох довірених осіб. Поточна реалізація контрактів MOR на EVM *без проксі*, тобто вони не можуть бути оновлені (immutable); однак безпечний власник (Safe) може у разі надзвичайної ситуації застосувати функції паузи (в LayerZero Endpoint є функція блокування виходу / входу повідомлень) або встановити ліміти переказів. Цими можливостями, втім, планується користуватися лише в разі критичної необхідності (наприклад, у випадку експлойту) — у звичайному режимі мультипідпис не втручається в роботу токена.

Особливу увагу при проєктуванні EVM-частини приділено інтеграції Wormhole. На момент написання статті MOR ще не повністю задіяв Wormhole на Ethereum, але в архітектурі передбачено розгортання окремого контракту MOR-NTT Manager (можливо, як розширення наявного контракту або окремого модуля). Цей NTT Manager на Ethereum буде уповноважений спалювати MOR (з балансу користувача, який ініціює переказ) та карбувати MOR (на адресу отримувача після підтвердження VAA). Для цього мультисиг Safe, що володіє контрактом MOR, додасть NTT Manager як мінтер / бернер до токена MOR. Конфігурація Wormhole тоді віддзеркалить solana-сценарій: NTT Manager (Ethereum) + NTT Manager (Solana, тобто MORSOL програма) будуть зареєстровані одне в одного як довірені адреси, а Squads Vault слугуватиме кінцевим арбітром, який підтверджує випуск токенів на Solana.

Отже, архітектура EVM-складової є достатньо простою з точки зору користувача — це стандартний контракт токена MOR, сумісний з будь-якими гаманцями та біржами, тоді як «під капотом» він містить логіку LayerZero і прив'язку до мультисиг. Завдяки цьому MOR може безшовно переміщуватись між Ethereum та іншими мережами другого рівня, залишаючись під захистом налаштованої нами моделі безпеки.

[1] Squads — популярний мультисиг-сервіс у Solana, де Vault PDA — це програмно-генерована адреса, яка може тримати активи і підписувати транзакції після проходження голосування учасників мультипідпису. У нашому випадку Squads Vault не зберігає токени напряму, а використовується як довірений підписант операцій з мінтом MOR.

Результати

Функціональність мосту. Реальні тести переказів підтвердили коректність роботи як LayerZero-, так і Wormhole-компонентів. З Ethereum у Arbitrum та Base токен переміщується майже миттєво: завдяки тому, що LayerZero сплачує комісію на вихідному ланцюгу і оптимізує доставлення, користувач за декілька хвилин бачить токени на рахунку в цільовій мережі (з урахуванням часу фіналізації блоку). Перенесення між Ethereum та Solana (через Wormhole) займає більше часу, оскільки передбачає підтвердження від Guardian-мережі та очікування підтверджень в обох блокчейнах; проте і в цьому випадку транзакції проходять успішно, а затримка типово не перевищує 2-3 хвилини. Користувачі Morpheus отримали змогу безпечно переміщувати MOR, наприклад із Solana (де токен може використовуватися в Solana-програмах або DEXах) до Ethereum (для торгівлі на Uniswap та участі в Ethereum-діях) і назад. Це значно підвищує ліквідність та утилітарність токена, адже усуває розрив між ізольованими екосистемами — MOR функціонує як міст між спільнотами Solana та EVM.

Дотримання єдиної емісії. Одним із головних результатів є підтвердження того, що контроль за загальною кількістю MOR діє коректно. У процесі тестування спеціально моделювалися крайні ситуації — одночасні перекази великих сум через різні мости, спроби повторного відправлення того самого повідомлення тощо. У всіх випадках механізми безпеки (зокрема, Global Accountant Wormhole та перевірка nonce повідомлень у LayerZero) запобігли будь-яким дублюванням чи розбалансуванню постачання. Загальна кількість MOR на всіх ланцюгах після серії тестових транзакцій залишалася рівно 42,000,000, що підтверджує принцип збереження маси в нашій моделі.

Висновки

У цій роботі представлено комплексне рішення для омнічейн-інтеграції токена MOR, яке поєднує дві провідні міжланцюгові технології — LayerZero OFT та Wormhole NTT. Проєкт MORSOL показав, що мультиланцюговий токен може бути реалізований безпечним і прозорим чином, якщо грамотно скомбінувати сильні сторони різних протоколів і додати рівень децентралізованого контролю. Архітектура MOR охоплює Anchor-програму на Solana, мережу смарт-контрактів на EVM-ланцюгах, а також інфраструктурні компоненти LayerZero (endpoint-и, DVN) та Wormhole (Core, Guardians, VAA). Ключовою особливістю є використання мультипідписної моделі управління: всі операції карбування токена MOR на Solana здійснюються за участі Squads-мультисиг, а критичні налаштування контрактів на Ethereum перебувають під контролем Gnosis Safe. Це гарантує, що жодна транзакція переміщення або випуску MOR не відбувається без колективної згоди, — потужний запобіжник проти зловживань або експлойтів.

Запропоноване рішення забезпечує уніфікований обіг токена MOR на різних платформах: замість ізольованих wrapped-версій, MOR існує всюди як той самий актив, дотримуючись єдиної економіки і загального максимального обсягу. Завдяки механізму burn-and-mint та перевіркам LayerZero / Wormhole, вдалося досягти цього без втрати швидкості або зручності для користувачів. Аналіз безпеки показав, що комбінована модель має високу стійкість: навіть у разі гіпотетичного прориву одного рівня захисту інший рівень (наприклад, мультисиг) візьме на себе запобігання негативним наслідкам.

Практичні результати впровадження MORSOL підтвердили ефективність підходу. MOR успішно функціонує на мережах Solana, Ethereum, Arbitrum, Base, забезпечуючи користувачам свободу переміщувати свої токени між ними і використовуючи там, де це найбільш вигідно. Це підвищує ліквідність токена і сприяє інтеграції спільнот різних блокчейнів у єдину економічну систему проєкту Morpheus. Водночас було досягнуто високого рівня довіри з боку спільноти: прозора мультипідписна інфраструктура та публічні аудити дали впевненість, що з токеном не станеться непередбачуваних емісій чи блокувань.

Отже, проєкт MORSOL робить вагомий внесок у розвиток концепції омнічейн-токенів. На практичному прикладі продемонстровано, що децентралізований крос-ланцюговий контроль є можливим без істотних втрат у продуктивності чи юзабіліті. Отримані знання можуть бути використані іншими розробниками токенів, які прагнуть максимальної міжланцюгової сумісності своїх проєктів. Поєднання LayerZero OFT та Wormhole NTT, доповнене механізмами DAO-управління, може стати новим стандартом для випуску активів у багатоланцюговому світі Web3.

У підсумку, інтеграція MOR засвідчує, що бачення One Token, Many Chains уже реалізується на практиці. Очікується, що з часом все більше проєктів ітимуть цим шляхом, розмиваючи межі між блокчейнами і створюючи по-справжньому універсальні криптоактиви. Досвід MOR підтверджує: правильна архітектура та орієнтація на безпеку здатні подолати бар'єри сумісності, відкривши шлях до більш зв'язаного і децентралізованого криптосередовища.

Список літератури

1. Blockchain Technology for Tracing Drug with a Multichain Platform: Simulation Method [Electronic resource] / E. Fernando et al. // Advances in Science, Technology and Engineering Systems Journal. — 2021. — Vol. 6, no. 1. — Pp. 765–769. — Mode of access: https://doi.org/10.25046/aj060184 (date of access: 25.06.2025).
2. Documentation | Morpheus [Electronic resource]. — Mode of access: https://gitbook.mor.org/smart-contracts/documentation (date of access: 25.06.2025).
3. Hwang W.-Y. A Study on the Interoperable Method of Security Tokens Between Permissioned and Public Blockchains [Electronic resource] / W.-Y. Hwang, H.-K. Kim // Korea Industrial Technology Convergence Society. — 2025. — Vol. 30, no. 1. — Pp. 23–29. — Mode of access: https://doi.org/10.29279/jitr.k.2025.30.1.23 (date of access: 25.06.2025).
4. Isaac D. Technical Deep Dive: Multichain Tokens [Electronic resource] / D. Isaac // Medium. — Mode of access: https://defi-isaac.medium.com/technical-deep-dive-multichain-tokens-452cbb8c82cc (date of access: 25.06.2025).
5. Nelson D. Crypto Bridge LayerZero Connects to Solana Blockchain [Electronic resource] / D. Nelson // CoinDesk. — Mode of access: https://www.coindesk.com/tech/2024/05/29/crypto-bridge-layerzero-connects-to-solana-blockchain (date of access: 25.06.2025).
6. Omnichain Tokens | LayerZero [Electronic resource]. — Mode of access: https://docs.layerzero.network/v2/concepts/applications/oft-standard (date of access: 25.06.2025).
7. Wormhole: Native Token Transfers (NTT) [Electronic resource] — Mode of access: https://app.blockworksresearch.com/unlocked/wormhole-native-token-transfers-ntt (date of access: 25.06.2025).

References

Blockworks Research. (n. d.). Wormhole : Native Token Transfers (NTT). https://app.blockworksresearch.com/unlocked/wormhole-native-token-transfers-ntt.

Fernando, E., Rizal, M., Ramadhan, I., Setiawan, A., & Sulistyono, A. (2021). Blockchain technology for tracing drug with a multichain platform: Simulation method. *Advances in Science, Technology and Engineering Systems Journal*, *6* (1), 765–769. https://doi.org/10.25046/aj060184.

Hwang, W.-Y., & Kim, H.-K. (2025). A study on the interoperable method of security tokens between permissioned and public blockchains. *Korea Industrial Technology Convergence Society*, *30* (1), 23–29. https://doi.org/10.29279/jitr.k.2025.30.1.23.

Isaac, D. (n .d.). Technical deep dive: Multichain tokens. Medium. https://defi-isaac.medium.com/technical-deep-dive-multichain-tokens-452cbb8c82cc.

LayerZero. (n. d.). Omnichain tokens. https://docs.layerzero.network/v2/concepts/applications/oft-standard.

Morpheus. (n. d.). Documentation | Morpheus. https://gitbook.mor.org/smart-contracts/documentation.

Nelson, D. (2024, May 29). Crypto bridge LayerZero connects to Solana blockchain. CoinDesk. https://www.coindesk.com/tech/2024/05/29/crypto-bridge-layerzero-connects-to-solana-blockchain.

P. Yaremenko, K. Gorokhovskyi

OMNICHAIN INTEGRATION OF THE MOR TOKEN BASED ON LAYERZERO OFT AND WORMHOLE NTT STANDARDS

This article presents the architecture, implementation, and interoperability strategy of the MORSOL system — a cross-chain solution for deploying the MOR token across multiple blockchain ecosystems. The system is based on two widely adopted omnichain token standards: LayerZero's OFT (Omnichain Fungible Token) and Wormhole's NTT (Native Token Transfers), enabling seamless transfers of MOR tokens between Solana and EVM-compatible blockchains.

A distinguishing feature of the architecture is that the MOR token exists in native form across chains, without relying on traditional wrapped token models. The system ensures that MOR has a single, globally tracked total supply, maintained through a burn-and-mint mechanism. This method guarantees that when MOR is transferred from one chain to another, it is burned on the source chain and freshly minted on the destination, eliminating the risk of inflation or double-spending.

The cross-chain functionality is facilitated by a combination of smart contracts and protocol-specific infrastructure. On Solana, the project uses an Anchor-based program, and on EVM networks, Solidity contracts are deployed. LayerZero endpoints handle message relaying and verification through Decentralized Verifier Networks (DVNs), while Wormhole utilizes its Guardians to provide VAA (Verified Action Approval) proofs that validate token transfers.

Governance and token emission are controlled by decentralized multisignature infrastructure: Squads Vault (via PDA accounts) on Solana and Gnosis Safe on EVM chains. These multisigs are used to authorize minting and burning operations and are critical for maintaining control over token supply across chains.

Security features include the ability to pause token transfers, upgrade contracts when needed, and enforce strict validation through the LayerZero and Wormhole relayer networks. A comparative analysis of OFT and NTT protocols is included, showing how their integration leverages the advantages of both approaches—such as LayerZero's modularity and Wormhole's proven track record in VAA validation.

The result is a robust, scalable, and secure omnichain token infrastructure for MOR, capable of supporting decentralized applications (dApps) across multiple ecosystems. This implementation serves as a reference model for other projects seeking to maintain synchronized assets in a multichain environment while preserving decentralization and security.

Keywords: omnichain, MOR token, LayerZero OFT, Wormhole NTT, cross-chain transfer, burn-mint, multisig governance, Squads Vault, Gnosis Safe, decentralized interoperability.

Матеріал надійшов 27.06.2025