ONYX AML

ЗВІТ РОЗСЛІДУВАННЯ

Злам Binance 29 жовтня 2026: як $6,3 млрд вийшли з гарячих гаманців, де вони зараз і чи їх зливають

Увечері 29 жовтня зловмисник за чотири години спустошив гарячі гаманці Binance у десяти блокчейнах. Більшість новин зупиняється на загальній сумі. Ми прочитали кожну адресу хакера напряму з блокчейнів, звірили заморозки з власним корпусом подій контракту Tether і перевірили, де кожна монета просто зараз. Коротко: близько $2,6 млрд у стейблкоїнах заморожено, біткоїн і ефір поки не рухались, активно виводиться лише TRX.

Дані станом на 30 жовтня 2026 року, 15:00 UTC
Onyx AML · onyxprotocol.trade · звіт ONYX-INC-2026-10-BNB

Дані станом на 30 жовтня 2026 року, 15:00 UTC. Баланси, час заморозок і перекази нижче Onyx AML прочитав напряму з вузлів Ethereum, TRON, Bitcoin, XRP Ledger, Solana і NEAR та з власного корпусу подій заморозки USDT. Загальні суми, атрибуція і обміни першої години взяті в Binance, Elliptic, TRM Labs і CoinDesk, і це позначено. Першопричину офіційно ще не підтверджено, тому ми розділяємо відоме і ймовірне.

Коротко в цифрах

Що	Цифра	Джерело
Викрадено загалом	близько $6,3 млрд (Binance), $6,36 млрд (TRM), $6,43 млрд (Elliptic), 10 мереж	Binance, TRM, Elliptic
Заморожено Tether на адресах хакера	1 759,2 млн USDT на 5 адресах (Ethereum 3, TRON 2)	блокчейн, Onyx
Заморожено Circle	823 млн USDC на головному гаманці і ще 1,56 млн на проміжній адресі	блокчейн, Onyx
Ефір у хакера	447 757 ETH на 4 гаманцях, з яких не було жодної вихідної транзакції	блокчейн, Onyx
Біткоїн у хакера	18 270,2 BTC на 19 адресах, нічого не витрачено	блокчейн, Onyx
Інші монети без руху	233,46 млн XRP, 970 554 SOL, 12,41 млн NEAR	блокчейн, Onyx
Рухається зараз	TRX: близько 73,7 млн із 684,6 млн розпорошено на свіжі адреси	блокчейн, Onyx
Атрибуція	північнокорейська група TraderTraitor: «висока впевненість» у TRM, «ймовірно» в Elliptic; офіційної заяви держав поки немає	TRM, Elliptic



Злам Binance 29.10.2026: де кошти зараз

ONYX AML

Стан адрес хакера на 30.10.2026, 15:00 UTC · прочитано напряму з блокчейнів, Onyx AML

ВИКРАДЕНИЙ АКТИВ	КУДИ ПІШОВ	СТАТУС ЗАРАЗ
1,18 млрд USDT + 823 млн USDC	Ethereum · головний гаманець хакера 0x5227…2f8c	ЗАМОРОЖЕНО Tether 21:01 · Circle 21:04 UTC
205 млн USDT	Ethereum · 2 проміжні гаманці 0xaa24…54a0, 0xb171…c8c3	ЗАМОРОЖЕНО Tether 21:15 і 21:19 UTC
447 757 ETH	Ethereum · 4 гаманці, з яких ще не було жодної транзакції	НЕ РУХАЛИСЬ 0x8532… · 0xc887… · 0x897c… · 0x79e7…
18 270,2 BTC	Bitcoin · розбито на 19 адрес, на 17 із них по 1 000 BTC	НЕ РУХАЛИСЬ жодна сатоші не вийшла з дерева
612,7 млн USDT у TRON	TG5i…GsGi і TCzB…7Y62	ЗАМОРОЖЕНО заморожено 378,7 млн · ~234 млн обміняно на TRX
684,6 млн TRX	5 гаманців: 518,2 млн TRX · 1 гаманець роздає далі	РУХАЮТЬСЯ ЗАРАЗ розпорошено вже ~73,7 млн TRX
233,46 млн XRP	XRP Ledger · rK21…zMx	НЕ РУХАЛИСЬ нативний XRP заморозити нікому
970 554 SOL · 12,41 млн NEAR	Solana · Affz…BEaU · акаунт NEAR	НЕ РУХАЛИСЬ нативні монети, функції заморозки немає

Перевірено в блокчейні: Tether заморозив 1,759 млрд USDT на 5 адресах хакера, Circle 823 млн USDC.
О 22:06 UTC Tether заморозив і сам гаманець Binance 14.

Дані: вузли Ethereum, TRON, Bitcoin, XRP, Solana, NEAR; корпус заморозок USDT Onyx. Контекст: Elliptic, TRM Labs, заяви Binance. onyxprotocol.trade

---

Як це сталося: слабкі місця

Перша заява Binance вказувала на зламаний ноутбук DevOps-інженера: через нього зловмисник дістався до сервісного контейнера, з якого можна подавати транзакції виведення. Біржа також заявила, що ознак витоку приватних ключів не знайшла. Пізніше Binance повідомила, що розслідування виявило «додаткові точки проникнення». Повного технічного звіту ще немає, тому нижче те, що сьогодні підтверджують дані блокчейну і публічні заяви.

1. Система підпису виконувала команди зловмисника одразу в десяти мережах. Bitcoin, TRON, XRP, Solana, Avalanche, Polygon, Arbitrum, Optimism і Base спорожніли звичайними підписаними переказами з гаманців Binance з різницею в кілька хвилин. Якщо системі можна наказати підписувати перекази в десяти мережах і ключі при цьому з неї не виходять, слабке місце не в ключі, а в шарі, який вирішує, що підписувати. До того ж висновку дійшли Elliptic і TRM. Тому фраза «приватні ключі не витекли» нічого не заспокоює: ключам і не треба було виходити.

2. Гарячий гаманець підписав делегування EIP-7702. EIP-7702 (працює з оновлення Pectra у травні 2025 року) дозволяє звичайній адресі одним підписаним дозволом «приєднати» до себе код смартконтракту. Зловмисник надіслав одну транзакцію з 50 такими дозволами, кожен підписаний ключем Binance 14 під інший порядковий номер (nonce). Спрацював лише один. Ця деталь важлива: той, хто запитував підписи, міг їх отримати, але не знав поточного стану гаманця. Це схоже на доступ до сервісу підпису, а не на володіння ключем. Ми перевірили стан блокчейну: починаючи з блоку 26 300 753 (20:20:59 UTC) на Binance 14 стоїть маркер делегування на контракт `0x63e842b054bd624a465454d533c33f573e9c6fae`. Його код верифікований під назвою «Target», а розгорнула його адреса `0x7c8601d4645b93cea45f71e118a729332e6b5ca0` на боці зловмисника, яку напередодні фінансували через Tornado Cash. Гарячому гаманцю, що робить лише звичайні перекази, нема чого підписувати дозвіл типу 4. Політика підпису, яка це пропустила, і є найочевиднішим збоєм контролю, видимим у блокчейні.

3. Делегування тривалось майже чотири години. Делегування EIP-7702 діє, доки його не замінять. Після встановлення кожне нове надходження на Binance 14 можна було вимести без жодного підпису. Зловмисник вимітав гаманець ще о 20:41, 20:59, 21:04, 21:44, 22:39 і 23:56 (TRM). У стані блокчейну маркер зникає лише в блоці 26 301 896, о 00:10:35 UTC 30 жовтня: 3 години 49 хвилин 36 секунд відкритого доступу. Зрештою Tether о 22:06:23 UTC вніс до блекліста сам Binance 14, щоб USDT, які туди надходять, не можна було забрати. Наскільки нам відомо, це перший випадок, коли емітент заморожує власний гарячий гаманець біржі, щоб захистити його від чужого делегування.

4. Забагато грошей в одному гарячому гаманці. На Ethereum викрали близько $3,8 млрд, майже все з Binance 14. Він також був виконавцем смарт-акаунта Binance, і саме так забрали 823 млн USDC. Гарячий гаманець має тримати оборотний залишок, а не мільярди. Ці ж гаманці фігурують у доказі резервів Binance, тому CoinDesk оцінює покриття ефіру приблизно в 94%, доки не надійдуть кошти на заміну.

5. Години видимої підготовки. 28 жовтня операційний гаманець отримав три виведення по 0,1 ETH з Tornado Cash, 29 жовтня о 15:59 UTC розгорнуто контракт-«пилосос», і за даними TRM його відпрацювали на тестових гаманцях приблизно за чотири години до атаки. Усе це було видно в блокчейні, просто ніхто не пов'язав це з Binance, поки гроші не пішли.

Що з цього мають винести біржі. Підписувати за політикою, а не за запитом: для гарячих гаманців дозволений лише білий список типів транзакцій, а дозвіл EIP-7702 заборонений повністю. Стежити за кодом на власних адресах: якщо `eth_getCode` на гарячому гаманці біржі повертає щось, крім порожнього значення, це миттєва тривога. Обмежувати баланс і швидкість виведення гарячих гаманців у кожній мережі та вважати одночасні великі виведення в кількох мережах одним інцидентом. Тримати робочі канали заморозки з емітентами: усе, що вдалося врятувати 29 жовтня, врятували Tether, Circle, Ripple і World Liberty Financial протягом від 40 хвилин до двох годин, і лише для токенів, які взагалі можна заморозити.

Хронологія (UTC)

Час	Подія	Джерело
28.10	Три виведення по 0,1 ETH з Tornado Cash фінансують операційний гаманець	Elliptic, TRM
29.10 15:59	Розгорнуто контракт-«пилосос»	Elliptic
~20:05	233,46 млн XRP виходять з п'яти гаманців Binance у XRP Ledger	TRM
20:20	18 270,2 BTC виходять з Binance і розбиваються на пакети по 1 000 BTC	TRM, блокчейн
20:20:59	На Binance 14 діє делегування EIP-7702 (блок 26 300 753)	блокчейн, Onyx
20:22:45	612 729 468 USDT переходять з Binance-Hot 7 у TRON на TG5iBMQPrDzJJAUM8GMVBf1hRaJ1wvzsGi	блокчейн, Onyx
~20:24	З Binance 14 виметено 167 464 ETH і 63 токени	TRM, CoinDesk
20:45:51, 20:56:09	100 млн і 200 млн USDT у TRON переслано на TPBkSjkCMn2ckrMuAP8n2J1jdjbw76bKN4, звідти близько 234 млн пішли в пули SunSwap на обмін у TRX	блокчейн, Onyx
21:01:35	Перші заморозки Tether: головний гаманець 0x5227…2f8c і ще три гаманці хакера, блоки 26 300 954-26 300 960	корпус заморозок Onyx
21:04	Circle заморожує 823 млн USDC	TRM, Elliptic; підтверджено в блокчейні

21:09:12	Tether заморожує TG5i…GsGi, на якому лишалось 312,73 млн USDT	корпус заморозок Onyx
21:14:59, 21:18:59	Tether заморожує два проміжні гаманці в Ethereum зі 175,0 млн і 30,0 млн USDT	корпус заморозок Onyx
21:16:18-21:21:12	65,99 млн USDT переслано на TCzBTkqn66yApqbYoPezaEQosM5DAd7Y62 і заморожено там через 4 хв 54 с	блокчейн, Onyx
22:06:23	Tether вносить до блекліста сам Binance 14	корпус заморозок Onyx
22:15	Binance зупиняє виведення	Binance
23:56	Останнє вимітання Binance 14	TRM, Elliptic
30.10 00:06	46,38 млн викрадених TRX надіслано на нову адресу TRBdWqHnDVSZCVGfgHdKFLQPirQcA2PRki	блокчейн, Onyx
00:10:35	Делегування з Binance 14 знято (блок 26 301 896)	блокчейн, Onyx
06:36	Злив токенів на DEX припиняється	Elliptic
10:20 і досі	Ще 120 млн TRX надходять на TRBd…PRki, і та роздає їх пакетами від 30 тис. до 950 тис. TRX на щойно створені адреси	блокчейн, Onyx

---

Куди пішли кошти: мережа за мережею

Стейблкоїни в Ethereum: здебільшого перехоплено. Головний гаманець хакера `0x5227f603c1ee34ce3c06efe6477003bdfccb2f8c` зараз тримає 1 175 464 713 USDT і 823 000 000 USDC, обидва заморожені. Перегони були щільні: USDT надійшли близько 20:24, а заморозка спрацювала о 21:01, через 37 хвилин. За цей час зловмисник продав маркетмейкерам і через UniswapX та 1inch від 325 до 434 млн USDT за ефір зі знижкою понад 10% (TRM, Elliptic). Хто переплачує за ефір 10%, той дуже поспішає. Дорогою заморожено два проміжні гаманці зі 175,0 млн і 30,0 млн USDT. Ці дві адреси, `0xaa246bf639586a6ba46762d378ce50ca4fc654a0` і `0xb171ca86f82070282138352ff7111b494060c8c3`, поки відсутні в публічному блоклісті Elliptic: ми знайшли їх через свій корпус заморозок, їх заморозили в ті самі двадцять хвилин. Ще одна адреса, заморожена в цьому вікні, `0x7aa4d3029e4c6a8e916300014ad95b6d6c03bfd1`, делегована на той самий код смарт-акаунта, що й гаманець хакера з блокліста.

Ефір: припаркований. 413 477 ETH лежать на трьох гаманцях: `0x8532fa14acaf483729c449b8458aeddb900543d4` (197 460 ETH), `0xc887af690e0301cd4edbbce8f8d31b4ec65b286a` (137 602 ETH) і `0x897c80d1a9729e94460e2bd93178bd5215158df3` (78 415 ETH). Жоден з них ще не відправив жодної транзакції (nonce 0). Четвертий гаманець-сховище, `0x79e70d139fc05aa75f75611fdf2680e9952b544a`, тримає ще 34 280 ETH, зібрані вранці 30 жовтня з трьох гаманців хакера зі списку; його теж немає в публічному блоклісті Elliptic. Разом 447 757 ETH на чотирьох гаманцях. Рух, який видно в експлорерах, це вхідний пил і повідомлення від сторонніх, а не виведення. Крім того, близько 19 760 ETH позичено в Aave під заставу 59,9 млн USDT, перш ніж Aave заморозив ринки (Elliptic).

Біткоїн: розбитий, але не проданий. 18 270,2 BTC за кілька хвилин розбили на 19 адрес: на 17 рівно по 1 000 BTC, на двох 832,5 і 437,7. Ми пройшли все дерево: сума непотрачених виходів дорівнює 18 270,2 BTC, тобто жодна монета його не покинула. Круглі пакети по 1 000 BTC зручні для позабіржових (OTC) продажів, і це найімовірніший наступний етап, але поки нічого не рухалось. У біткоїна немає емітента, і заморозити його нікому.

TRON: перегони з Tether, здебільшого програні. 612,7 млн USDT вийшли з Binance-Hot 7 о 20:22:45. До заморозки хакер встиг переслати 300 млн: близько 234 млн пішли в пули SunSwap і вийшли приблизно 638 млн TRX, 65,99 млн переслали далі й заморозили протягом п'яти хвилин, а 312,73

млн заморозили на першому ж гаманці-приймачі. TRX потім зібрали на одній адресі й розбили на п'ять: чотири гаманці зі 158,2 млн, 120 млн, 120 млн і 120 млн TRX не рухались. П'ятий надіслав 120 млн TRX на `TRBdWqHnDVSZCVGfgHdKFLQPirQcA2PRki`, куди також прямо надійшли 46,38 млн TRX, викрадені в Binance. Цю адресу створено о 00:06 UTC 30 жовтня, і відтоді вона роздала близько 73,7 млн TRX пакетами від 30 тис. до 950 тис. на десятки нових адрес. Це єдина частина викраденого, яку відмивають просто зараз. Elliptic також повідомляє, що частина потоку в TRON дійшла до адреси, на якій лежать кошти з вересневого зламу Bitget.

XRP, Solana, NEAR: без руху. 233 461 943 XRP лежать на `rK21t6nGLy4MNDqhvy3pGwcLFy25qgfzMx`, 970 554 SOL на `AffzFDKZbyMiU11zmVBoAqD25ugpr7xoWWyRyGigBEaU`, 12,41 млн NEAR на одному акаунті. Це нативні монети без функції заморозки, тож емітенти тут не допоможуть. Рада безпеки Arbitrum о 00:08 UTC вивела з-під контролю хакера 8 426 ETH і 74,6 млн ARB (TRM).

Чи зливає хакер кошти?

Масово і зараз ні. Злив був у перші години і лише там, де вирішувала швидкість: стейблкоїни продавали чи обмінювали, поки емітенти не встигли заморозити, а дрібні токени зливали на DEX до 06:36 UTC (Elliptic). Відтоді біткоїн, припаркований ефір, XRP, SOL і NEAR не рухались. Єдиний активний потік це TRX через свіжі адреси, типова підготовка до сервісів обміну й OTC-брокерів. Якщо повториться сценарій попередніх великих крадіжок, далі будуть мости між мережами й позабіржові брокери, і це може тривати тижнями. Ринок поки реагує на страх, а не на продажі: 30 жовтня біткоїн упав приблизно на 4%, ліквідації сягнули близько $1,6 млрд.

Злив FUN: що сталося з маленьким токеном

Під час вимітання Binance 14 о 20:24 UTC хакер забрав і 714 911 344 FUN (FUNToken, колишній FunFair) на головний гаманець. О 23:28:47 UTC усю суму перекинули на свіжу адресу `0x06ea1ab3ecf570029eb1f94dbb9eac06bc79685f`, і та за 154 транзакції продавала їх у тонкий пул FUN/WETH на Uniswap. Продано 134 145 256 FUN, а отримано лише 111,48 ETH, близько $250 тис.; ціна в пулі впала більш ніж на 90% (CoinDesk). О 06:30 UTC хакер припинив продаж і повернув решту, 580 766 088 FUN (близько 5,4% усієї емісії), на головний гаманець, де вони лежать і зараз. Виручка 111,85 ETH пішла на гаманець-сховище 0x79e7…544a. FUNToken попросив біржі тимчасово вимкнути депозити FUN. Урок для власників невеликих токенів: гарячий гаманець біржі може тримати помітну частку емісії вашого токена, і якщо його вкрадуть, цей «навіс» тиснутиме на ціну, доки хакер його тримає. А ще хтось почав слати хакеру нульові перекази FUN з адреси-двійника: класичне отруєння адрес, цього разу проти самого зловмисника.

Що це означає для користувачів Binance

Binance заявляє, що баланси клієнтів не постраждали, бо викрадено кошти власних гарячих гаманців біржі, і що зарезервувала понад $6,34 млрд на покриття збитку, з них близько $5 млрд уже в тих самих токенах. Виведення зупинено о 22:15 UTC 29 жовтня. Біржа називає попередній орієнтир близько 40 годин і обіцяє повний доказ резервів до понеділка. Депозити працюють.

- **Ігноруйте всіх, хто пропонує «компенсацію» чи «повернення» від Binance.** Після кожного великого зламу за кілька годин з'являються фейкові акаунти підтримки. Binance не просить сід-фраз, оплат чи «перевірочних переказів».
- **Цього тижня не поспішайте купувати USDT чи TRX у незнайомців на P2P.** Викрадені TRX розпорошують просто зараз. Монети, що пройшли через ці адреси, можуть заморозити ваш акаунт на наступній біржі, навіть якщо ви нічого не порушували.

- **Перевіряйте адресу контрагента перед угодою.** Наш безкоштовний чекер читає блеклісти USDT і USDC напряму з контрактів, тому заморожені адреси хакера там видно одразу. Повний перелік адрес хакера є в PDF.
- **Стежте за доказом резервів.** Питання не в загальній сумі, а в кожному токені окремо: чи справді ефір і біткоїн на заміну лежать на зазначених гаманцях.

Метод і межі

Ми взяли за основу публічний блокліст Elliptic на 48 адрес і опубліковані CoinDesk гаманець Binance 14 та хеші транзакцій, прочитали поточні баланси, код контрактів і статус блеклістів USDT і USDC кожної адреси, пройшли дерева біткоїна і TRX до місць, де монети зупинились, і звірили кожну заморозку з власним корпусом подій контрактів USDT в Ethereum і TRON. Вікно делегування знайдено читанням коду Binance 14 на історичних блоках. Суми в доларах, обміни першої години, позиція в Aave і атрибуція взяті з джерел, зазначених у таблиці. Першопричина не підтверджена, доки Binance не опублікує свій звіт; щойно це станеться, ми оновимо сторінку.

Ваші кошти заморожені і ви вважаєте це помилкою? Опишіть ситуацію на безкоштовній оцінці кейса: чесно скажемо, які шанси і з чого почати.

Додаток А. Реєстр адрес

Кожну адресу нижче прочитано напряму з її блокчейну о 15:00 UTC 30 жовтня 2026 року. Час заморозки взято з корпусу подій контракту USDT (Tether) Onyx. «Немає в списку Elliptic» позначає адреси, які ми виявили і яких на момент написання немає в публічному блокліст Elliptic.

Адреса	Мережа	Роль	Баланс зараз	Статус
`0x28c6c06298d514db089934071355e5743bf21d60`	Ethereum	Гарячий гаманець Binance 14, делегування EIP-7702 з 20:20:59 до 00:10:35	1 352 018 USDT	Binance (потерпілий); заморожено Tether 22:06:23
`0x5227f603c1ee34ce3c06efe6477003bdfccb2f8c`	Ethereum	Головний гаманець хакера, приймав вимітання	4,50 ETH, 1 175 464 713 USDT, 823 000 000 USDC, 580 766 088 FUN	заморожено Tether 21:01:35; USDC заморожено Circle
`0x9749292d74fd460982d0912ea9515ea24736c762`	Ethereum	Гаманець хакера	~0	заморожено Tether 21:01:35
`0x0ddf0480016e6bcb2c1f5d190d221fba1320697e`	Ethereum	Гаманець хакера	0,06 ETH	заморожено Tether 21:01:47
`0x8d53903625b8e839b9df4bd28b0efb1cd6b8639a`	Ethereum	Гаманець хакера	0,10 ETH	заморожено Tether 21:02:47
`0xaa246bf639586a6ba46762d378ce50ca4fc654a0`	Ethereum	Проміжний гаманець *(немає в списку Elliptic)*	174 999 872 USDT	заморожено Tether 21:14:59
`0xb171ca86f82070282138352ff7111b494060c8c3`	Ethereum	Проміжний гаманець *(немає в списку Elliptic)*	30 000 000 USDT	заморожено Tether 21:18:59
`0xccbef95633adb5cd2b5038db5a38d77e726ca263`	Ethereum	Проміжний гаманець *(немає в списку Elliptic)*	0,03 ETH	заморожено Tether 21:16:47
`0x7aa4d3029e4c6a8e916300014ad95b6d6c03bfd1`	Ethereum	Гаманець хакера, делегований на код смарт-акаунта *(немає в списку Elliptic)*	0,04 ETH	заморожено Tether 21:12:35
`0x77edef23fbd05921c26fe29fcc3a65e14d2ac3eb`	Ethereum	Гаманець хакера, делегований на код смарт-акаунта	0,01 ETH	
`0x8532fa14acaf483729c449b8458aeddb900543d4`	Ethereum	Гаманець-сховище, жодної вихідної транзакції	197 460 ETH	без руху
`0xc887af690e0301cd4edbbce8f8d31b4ec65b286a`	Ethereum	Гаманець-сховище, жодної вихідної транзакції	137 602 ETH	без руху
`0x897c80d1a9729e94460e2bd93178bd5215158df3`	Ethereum	Гаманець-сховище, жодної вихідної транзакції	78 415 ETH	без руху
`0x7c8601d4645b93cea45f71e118a729332e6b5ca0`	Ethereum	Оператор, розгорнув контракт-«пилосос»	1,18 ETH	
`0x63e842b054bd624a465454d533c33f573e9c6fae`	Ethereum	Контракт-«пилосос» «Target», ціль делегування Binance 14 *(немає в списку Elliptic)*	~0	
`0x19bee294a6daab49c9e5ab69a5da6c035c70f2bf`	Ethereum	Контракт, розгорнутий оператором	~0	
`0xa97bf7836f8a08f9ed91d41453d371493fae8d10`	Ethereum	Гаманець для обмінів	0,37 ETH, 123 176 USDC	USDC заморожено Circle

`0xc39e690bea48448cc47e7acddfe30e6453e09824`	Ethereum	Проміжна адреса мосту з Avalanche	1 563 813 USDC	USDC заморожено Circle
`0xb3ddec0ccc5c3ba733fcdf5a15f98c95ec5a5fdb`	Ethereum	Гаманець для обмінів	33 005 USDC	USDC заморожено Circle
`0xcf4ca2bdf21bc3a467a00b6afe72b833982723e0`	Ethereum	Гаманець хакера	~0	порожній
`0x42cdf00c85005630cc8605731b9364f712077810`	Ethereum	Гаманець хакера	~0	порожній
`0xe7024ab80143b1ef843efe6a58368696cb87958d`	Ethereum	Гаманець хакера	0,02 ETH	
`0x7f9dc988b46336ad536828fad50fa8fa1e5415e3`	Ethereum	Гаманець хакера	~0	порожній
`0x8c7111e9a3270457b76f0bd137209089047a6aa4`	Ethereum	Гаманець хакера	~0	порожній
`0x0084847bb9384d2fc5e8836e663689467e3e4c81`	Ethereum	Гаманець хакера	0,05 ETH	
`0xa3b3dee870f01560fdbe5af659c9c9135748886f`	Ethereum	Гаманець хакера	~0	порожній
`0x600d6f00eadabdb514561ceeb43730a7103e8298`	Ethereum	Гаманець хакера	~0	порожній
`0x811f15855476156ebf86ba3b84fafb8ceaa4e84c`	Ethereum	Гаманець хакера	~0	порожній
`0x79e70d139fc05aa75f75611fdf2680e9952b544a`	Ethereum	Гаманець-сховище, зібрав 34 280 ETH з трьох гаманців хакера *(немає в списку Elliptic)*	34 280 ETH	без руху
`0x06ea1ab3ecf570029eb1f94dbb9eac06bc79685f`	Ethereum	Продавець FUN: продав 134,1 млн FUN на Uniswap за 111,48 ETH *(немає в списку Elliptic)*	~0	порожній
`TDqSquXBgUCLYvYC4XZgrprLK589dkhSCf`	TRON	Binance-Hot 7 (TRON), джерело 612,7 млн USDT		Binance (потерпілий)
`TG5iBMQPrDzJJAUM8GMVBf1hRaJ1wvzsGi`	TRON	Перший приймач у TRON	312 729 468 USDT	заморожено Tether 21:09:12
`TPBkSjkCMn2ckrMuAP8n2J1jdjbw76bKN4`	TRON	Пересилач у TRON до SunSwap	~0	заморожено Tether 21:17:39
`TCzBTkqn66yApqbYoPezaEQosM5DAd7Y62`	TRON	Проміжна адреса TRON *(немає в списку Elliptic)*	65 990 000 USDT	заморожено Tether 21:21:12
`TSpe5HC3PRD2svJcr1YoGszhHk2mtkyZ8A`	TRON	Збір TRX *(немає в списку Elliptic)*	~0	порожній
`TKkH2vH6kyi2QKcMbqym53WMuvdd1xvw6K`	TRON	Гаманець-сховище TRX *(немає в списку Elliptic)*	158 200 902 TRX	без руху
`TJajtPqDqUGh1Sr1j8ugHoSXBVpaFLLHKT`	TRON	Гаманець-сховище TRX *(немає в списку Elliptic)*	120 000 000 TRX	без руху
`TCBAz7itvtX5CjBzVMPQdrbwQLN63ao1fk`	TRON	Гаманець-сховище TRX *(немає в списку Elliptic)*	120 000 000 TRX	без руху
`TL2F4GhnaFVZBZPncHYjwfYZFW44NcfVwj`	TRON	Гаманець-сховище TRX *(немає в списку Elliptic)*	120 000 000 TRX	без руху
`TAk1xJNWuBYvJHLsUiBFLeuK6xvpQUFYP5`	TRON	Гаманець TRX, переслав 120 млн TRX *(немає в списку Elliptic)*	~0	порожній

TRBdWqHnDVSZCVGfgHdKFLQPirQcA2PRki	TRON	Розпилювач TRX, створений 30.10 о 00:06 *(немає в списку Elliptic)*	92 717 498 TRX	рухається
bc1q0mtc2f5agpkvlq6hhahmfr3hlr55kyfjhl2mnm	Bitcoin	Корінь BTC, розбив 18 270,2 BTC	~0	порожній
bc1qxrxujwxfnvz040jw76d26zhjdg5jura7hs968s	Bitcoin	Адреса-сховище BTC	1 000,0 BTC	без руху
bc1qepc70u3u476vgvg3hfcwjgu4mecxe2uchs4lag	Bitcoin	Адреса-сховище BTC	1 000,0 BTC	без руху
bc1qnq6jj9jmlf3945m3l8s0kxnqehrsga300k8t3s	Bitcoin	Адреса-сховище BTC	1 000,0 BTC	без руху
bc1qdfhmlrdvg4tm87zjl0vyf0xflp5ql50q3g88gw	Bitcoin	Адреса-сховище BTC	1 000,0 BTC	без руху
bc1qz8hdwv8gmml0u96dsvnzsagz6krjyzxmgxupdp	Bitcoin	Адреса-сховище BTC	1 000,0 BTC	без руху
bc1q42flhayrzy3zh8lkyevw8qcjduurt9a35wlsyx	Bitcoin	Адреса-сховище BTC *(немає в списку Elliptic)*	1 000,0 BTC	без руху
bc1qjwdw6vrzq4vf6hckutvx4ucj86awwv99mxnz7w	Bitcoin	Адреса-сховище BTC	1 000,0 BTC	без руху
bc1q0ts8gaf9ht0rr4u02hr56f8thndqsc4kmkmfv3	Bitcoin	Адреса-сховище BTC	1 000,0 BTC	без руху
bc1qalwnl7dtaa73fsq5tyn0ghfy3fgfpqkt69tca8	Bitcoin	Адреса-сховище BTC *(немає в списку Elliptic)*	1 000,0 BTC	без руху
bc1q2wvz0kcsn4hqmajwtey30ud27fl25w8pveznn6	Bitcoin	Адреса-сховище BTC *(немає в списку Elliptic)*	1 000,0 BTC	без руху
bc1qs3aej5tmcdz0vctz8y9rjcxtxg8v5385577s56	Bitcoin	Адреса-сховище BTC	1 000,0 BTC	без руху
bc1qs6xnmhar38z44g2za93pv8ygdcwurrh8l87w3v	Bitcoin	Адреса-сховище BTC *(немає в списку Elliptic)*	1 000,0 BTC	без руху
bc1qm2j6v3247khlwzxl7p9vqnfkghcllyhv9wjaat	Bitcoin	Адреса-сховище BTC	1 000,0 BTC	без руху
bc1q63qrfrpsg5hh0zzn3kp2xx9vljl7dq7tatsjxp	Bitcoin	Адреса-сховище BTC *(немає в списку Elliptic)*	1 000,0 BTC	без руху
bc1qg3nrzpuvq2pxqx74tcrywr09dc208ze96n3t53	Bitcoin	Адреса-сховище BTC *(немає в списку Elliptic)*	1 000,0 BTC	без руху
bc1qm8v88m5fy6kuq9myva2eemwycxqd3e0zcrs2l8	Bitcoin	Адреса-сховище BTC *(немає в списку Elliptic)*	1 000,0 BTC	без руху
bc1qf5cyvv9w50tx9xx9s3xwsne0z87wvjj9l8a35u	Bitcoin	Адреса-сховище BTC *(немає в списку Elliptic)*	1 000,0 BTC	без руху
bc1qrg025e2pgx0rwya2kpgtj30972p64jt0hn6zyt	Bitcoin	Адреса-сховище BTC	832,5 BTC	без руху
bc1qxg0l4p6xc50zuv9cl5f0l0wmaxjpg8wcy7s9ra	Bitcoin	Адреса-сховище BTC	437,7 BTC	без руху
rK21t6nGLy4MNDqhvy3pGwcLFy25qgfzMx	XRP Ledger	Сховище XRP	233 461 943 XRP	без руху
AffzFDKZbyMiU11zmVBoAqD25ugpr7xoWWyRyGigBEaU	Solana	Сховище SOL	970 554 SOL	без руху
efd224256518a7cacd209867963276efed302a8e222c013c43f4b1bd369ae5af	NEAR	Сховище NEAR	12 410 068 NEAR	без руху

Додаток Б. Джерела

- Binance, official statements, 29-30 Oct 2026 (via CoinDesk, crypto.news)
- Elliptic, "The largest theft in history: North Korea likely behind the $6.4 billion Binance hack", elliptic.co/insights/binance-largest-hack-in-history, and public blocklist data-cdn.elliptic.co/blocklists/binance-hack-blocklist.csv
- TRM Labs, "North Korea steals USD 6.36 billion from Binance in the largest hack in history", trmlabs.com
- CoinDesk, "Binance says customer money is safe after huge hack drains key reserve wallets", 30 Oct 2026; "Binance arranges $6.34 billion to cover losses", 30 Oct 2026
- CNBC, 29-30 Oct 2026; Yahoo Finance, 30 Oct 2026 (market impact)
- Ethereum node (eth.drpc.org, archive state), Blockscout; TronGrid, Tronscan; mempool.space; XRP Ledger s1.ripple.com; Solana mainnet-beta RPC; NEAR RPC
- Onyx AML corpus of USDT contract events (AddedBlackList) on Ethereum and TRON