ONYX AML

ОТЧЁТ РАССЛЕДОВАНИЯ

Взлом Binance 29 октября 2026: как $6,3 млрд ушли из горячих кошельков, где они сейчас и сливают ли их

Вечером 29 октября злоумышленник за четыре часа опустошил горячие кошельки Binance в десяти блокчейнах. Большинство новостей ограничивается общей суммой. Мы прочитали каждый адрес хакера напрямую из блокчейнов, сверили заморозки с собственным корпусом событий контракта Tether и проверили, где каждая монета прямо сейчас. Коротко: около $2,6 млрд в стейблкоинах заморожено, биткоин и эфир пока не двигались, активно выводится только TRX.

Данные на 30 октября 2026 года, 15:00 UTC
Onyx AML · onyxprotocol.trade · отчёт ONYX-INC-2026-10-BNB

Данные на 30 октября 2026 года, 15:00 UTC. Балансы, время заморозок и переводы ниже Onyx AML прочитал напрямую с узлов Ethereum, TRON, Bitcoin, XRP Ledger, Solana и NEAR и из собственного корпуса событий заморозки USDT. Общие суммы, атрибуция и обмены первого часа взяты у Binance, Elliptic, TRM Labs и CoinDesk, это отмечено. Первопричина официально ещё не подтверждена, поэтому мы разделяем известное и вероятное.

Коротко в цифрах

Что	Цифра	Источник
Украдено всего	около $6,3 млрд (Binance), $6,36 млрд (TRM), $6,43 млрд (Elliptic), 10 сетей	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 главном кошельке и ещё 1,56 млн на промежуточном адресе	блокчейн, Onyx
Эфир у хакера	447 757 ETH на 4 кошельках, из которых не было ни одной исходящей транзакции	блокчейн, Onyx
Биткоин у хакера	18 270,2 BTC на 19 адресах, ничего не потрачено	блокчейн, Onyx
Прочие монеты без движения	233,46 млн XRP, 970 554 SOL, 12,41 млн NEAR	блокчейн, Onyx
Движется сейчас	TRX: около 73,7 млн из 684,6 млн распылено по свежим адресам	блокчейн, Onyx
Атрибуция	северокорейская группа TraderTraitor: «высокая уверенность» у TRM, «вероятно» у Elliptic; официальных заявлений государств пока нет	TRM, Elliptic



Взлом Binance 29.10.2026: где деньги сейчас

ONYX AML

Состояние адресов хакера на 30.10.2026, 15:00 UTC · прочитано напрямую из блокчейнов, Onyx AML

УКРАДЕННЫЙ АКТИВ	КУДА УШЁЛ	СТАТУС СЕЙЧАС
1,18 млрд USDT + 823 млн USDC	Ethereum · главный кошелёк хакера 0x5227…2f8c	ЗАМОРОЖЕНО Tether 21:01 · Circle 21:04 UTC
205 млн USDT	Ethereum · 2 промежуточных 0xaa24…54a0, 0xb171…c8c3	ЗАМОРОЖЕНО Tether 21:15 и 21:19 UTC
447 757 ETH	Ethereum · 4 кошелька, из которых не было ни одной транзакции	НЕ ДВИГАЛИСЬ 0x8532… · 0xc887… · 0x897c… · 0x79e7…
18 270,2 BTC	Bitcoin · разбито на 19 адресов, на 17 из них по 1 000 BTC	НЕ ДВИГАЛИСЬ ни один сатоши не вышел из дерева
612,7 млн USDT в TRON	TG5i…GsGi и TCzB…7Y62	ЗАМОРОЖЕНО заморожено 378,7 млн · ~234 млн обменяно на TRX
684,6 млн TRX	5 кошельков: 518,2 млн TRX · 1 кошелёк раздаёт дальше	ДВИЖУТСЯ СЕЙЧАС распылено уже ~73,7 млн TRX
233,46 млн XRP	XRP Ledger · rK21…zMx	НЕ ДВИГАЛИСЬ нативный XRP заморозить некому
970 554 SOL · 12,41 млн NEAR	Solana · Affz…BEaU · аккаунт NEAR	НЕ ДВИГАЛИСЬ нативные монеты, функции заморозки нет

Проверено в блокчейне: Tether заморозил 1,759 млрд USDT на 5 адресах хакера, Circle 823 млн USDC.
В 22:06 UTC Tether заморозил и сам кошелёк Binance 14.

Данные: узлы Ethereum, TRON, Bitcoin, XRP, Solana, NEAR; корпус заморозок USDT Onyx. Контекст: Elliptic, TRM Labs, заявления Binance. onyxprotocol.trade

---

Как это произошло: слабые места

Первое заявление Binance указывало на взломанный ноутбук DevOps-инженера: через него злоумышленник получил доступ к сервисному контейнеру, из которого можно отправлять транзакции вывода. Биржа также заявила, что признаков утечки приватных ключей не нашла. Позже Binance сообщила, что расследование выявило «дополнительные точки проникновения». Полного технического отчёта пока нет, поэтому ниже то, что сегодня подтверждают данные блокчейна и публичные заявления.

1. Система подписи выполняла команды злоумышленника сразу в десяти сетях. Bitcoin, TRON, XRP, Solana, Avalanche, Polygon, Arbitrum, Optimism и Base опустели обычными подписанными переводами с кошельков Binance с разницей в несколько минут. Если системе можно приказать подписывать переводы в десяти сетях, а ключи при этом из неё не выходят, слабое место не в ключе, а в слое, который решает, что подписывать. К тому же выводу пришли Elliptic и TRM. Поэтому фраза «приватные ключи не утекли» ничего не гарантирует: ключам и не нужно было выходить.

2. Горячий кошелёк подписал делегирование EIP-7702. EIP-7702 (работает с обновления Pectra в мае 2025 года) позволяет обычному адресу одним подписанным разрешением «подключить» к себе код смарт-контракта. Злоумышленник отправил одну транзакцию с 50 такими разрешениями, каждое подписано ключом Binance 14 под другой порядковый номер (nonce). Сработало только одно. Эта деталь важна: тот, кто запрашивал подписи, мог их получить, но не знал текущего состояния кошелька. Это похоже на доступ к сервису подписи, а не на владение ключом. Мы проверили состояние блокчейна: начиная с блока 26 300 753 (20:20:59 UTC) на Binance 14 стоит маркер делегирования на контракт `0x63e842b054bd624a465454d533c33f573e9c6fae`. Его код верифицирован под именем «Target», развернул его адрес `0x7c8601d4645b93cea45f71e118a729332e6b5ca0` на стороне злоумышленника, который накануне пополнили через Tornado Cash. Горячему

кошельку, который делает только обычные переводы, незачем подписывать разрешение типа 4. Политика подписи, которая это пропустила, и есть самый очевидный сбой контроля, видимый в блокчейне.

3. Делегирование держалось почти четыре часа. Делегирование EIP-7702 действует, пока его не заменят. После установки любое новое поступление на Binance 14 можно было вымести без единой подписи. Злоумышленник выметал кошелёк ещё в 20:41, 20:59, 21:04, 21:44, 22:39 и 23:56 (TRM). В состоянии блокчейна маркер исчезает только в блоке 26 301 896, в 00:10:35 UTC 30 октября: 3 часа 49 минут 36 секунд открытого доступа. В итоге Tether в 22:06:23 UTC внёс в блеклист сам Binance 14, чтобы поступающие туда USDT нельзя было забрать. Насколько нам известно, это первый случай, когда эмитент замораживает собственный горячий кошелёк биржи, чтобы защитить его от чужого делегирования.

4. Слишком много денег в одном горячем кошельке. В Ethereum украли около $3,8 млрд, почти всё из Binance 14. Он также был исполнителем смарт-аккаунта Binance, и именно так забрали 823 млн USDC. Горячий кошелёк должен держать оборотный остаток, а не миллиарды. Эти же кошельки входят в доказательство резервов Binance, поэтому CoinDesk оценивает покрытие эфира примерно в 94%, пока не поступят средства на замену.

5. Часы видимой подготовки. 28 октября операционный кошелёк получил три вывода по 0,1 ETH из Tornado Cash, 29 октября в 15:59 UTC развёрнут контракт-«пылесос», и, по данным TRM, его отработали на тестовых кошельках примерно за четыре часа до атаки. Всё это было видно в блокчейне, просто никто не связал это с Binance, пока деньги не ушли.

Что из этого должны вынести биржи. Подписывать по политике, а не по запросу: для горячих кошельков разрешён только белый список типов транзакций, а разрешение EIP-7702 запрещено полностью. Следить за кодом на собственных адресах: если `eth_getCode` на горячем кошельке биржи возвращает что-то кроме пустого значения, это мгновенная тревога. Ограничивать баланс и скорость вывода горячих кошельков в каждой сети и считать одновременные крупные выводы в нескольких сетях одним инцидентом. Держать рабочие каналы заморозки с эмитентами: всё, что удалось спасти 29 октября, спасли Tether, Circle, Ripple и World Liberty Financial за время от 40 минут до двух часов, и только для токенов, которые вообще можно заморозить.

Хронология (UTC)

Время	Событие	Источник
28.10	Три вывода по 0,1 ETH из Tornado Cash пополняют операционный кошелёк	Elliptic, TRM
29.10 15:59	Развёрнут контракт-«пылесос»	Elliptic
~20:05	233,46 млн XRP уходят с пяти кошельков Binance в XRP Ledger	TRM
20:20	18 270,2 BTC уходят из Binance и делятся на пакеты по 1 000 BTC	TRM, блокчейн
20:20:59	На Binance 14 действует делегирование EIP-7702 (блок 26 300 753)	блокчейн, Onyx
20:22:45	612 729 468 USDT переходят с Binance-Hot 7 в TRON на TG5iBMQPrDzJJAUM8GMVBf1hRaJ1wvzsGi	блокчейн, Onyx
~20:24	С Binance 14 выметено 167 464 ETH и 63 токена	TRM, CoinDesk
20:45:51, 20:56:09	100 млн и 200 млн USDT в TRON пересланы на TPBkSjkCMn2ckrMuAP8n2J1jdjbw76bKN4, оттуда около 234 млн ушли в пулы SunSwap на обмен в TRX	блокчейн, Onyx

21:01:35	Первые заморозки Tether: главный кошелёк 0x5227…2f8c и ещё три кошелька хакера, блоки 26 300 954-26 300 960	корпус заморозок Onyx
21:04	Circle замораживает 823 млн USDC	TRM, Elliptic; подтверждено в блокчейне
21:09:12	Tether замораживает TG5i…GsGi, на котором оставалось 312,73 млн USDT	корпус заморозок Onyx
21:14:59, 21:18:59	Tether замораживает два промежуточных кошелька в Ethereum со 175,0 млн и 30,0 млн USDT	корпус заморозок Onyx
21:16:18-21:21:12	65,99 млн USDT пересланы на TCzBTkqn66yApqbYoPezaEQosM5DAd7Y62 и заморожены там через 4 мин 54 с	блокчейн, Onyx
22:06:23	Tether вносит в блеклист сам Binance 14	корпус заморозок Onyx
22:15	Binance останавливает выводы	Binance
23:56	Последнее выметание Binance 14	TRM, Elliptic
30.10 00:06	46,38 млн украденных TRX отправлены на новый адрес TRBdWqHnDVSZCVGfgHdKFLQPirQcA2PRki	блокчейн, Onyx
00:10:35	Делегирование с Binance 14 снято (блок 26 301 896)	блокчейн, Onyx
06:36	Слив токенов на DEX прекращается	Elliptic
10:20 и до сих пор	Ещё 120 млн TRX поступают на TRBd…PRki, и тот раздаёт их пакетами от 30 тыс. до 950 тыс. TRX на только что созданные адреса	блокчейн, Onyx

---

Куда ушли деньги: сеть за сетью

Стейблкоины в Ethereum: в основном перехвачены. Главный кошелёк хакера `0x5227f603c1ee34ce3c06efe6477003bdfccb2f8c` сейчас держит 1 175 464 713 USDT и 823 000 000 USDC, оба заморожены. Гонка была плотной: USDT пришли около 20:24, а заморозка сработала в 21:01, через 37 минут. За это время злоумышленник продал маркетмейкерам и через UniswapX и 1inch от 325 до 434 млн USDT за эфир со скидкой более 10% (TRM, Elliptic). Кто переплачивает за эфир 10%, тот очень торопится. По пути заморожены два промежуточных кошелька со 175,0 млн и 30,0 млн USDT. Эти два адреса, `0xaa246bf639586a6ba46762d378ce50ca4fc654a0` и `0xb171ca86f82070282138352ff7111b494060c8c3`, пока отсутствуют в публичном блоклисте Elliptic: мы нашли их через свой корпус заморозок, их заморозили в те же двадцать минут. Ещё один адрес, замороженный в этом окне, `0x7aa4d3029e4c6a8e916300014ad95b6d6c03bfd1`, делегирован на тот же код смарт-аккаунта, что и кошелёк хакера из блоклиста.

Эфир: припаркован. 413 477 ETH лежат на трёх кошельках: `0x8532fa14acaf483729c449b8458aeddb900543d4` (197 460 ETH), `0xc887af690e0301cd4edbbce8f8d31b4ec65b286a` (137 602 ETH) и `0x897c80d1a9729e94460e2bd93178bd5215158df3` (78 415 ETH). Ни один из них ещё не отправил ни одной транзакции (nonce 0). Четвёртый кошелёк-хранилище, `0x79e70d139fc05aa75f75611fdf2680e9952b544a`, держит ещё 34 280 ETH, собранных утром 30 октября с трёх кошельков хакера из списка; его тоже нет в публичном блоклисте Elliptic. Итого 447 757 ETH на четырёх кошельках. Активность, которую видно в эксплорерах, это входящая пыль и сообщения от посторонних, а не выводы. Кроме того, около 19 760 ETH заняты в Aave под залог 59,9 млн USDT, прежде чем Aave заморозил рынки (Elliptic).

Биткоин: разбит, но не продан. 18 270,2 BTC за несколько минут разбили на 19 адресов: на 17 ровно по 1 000 BTC, на двух 832,5 и 437,7. Мы прошли всё дерево: сумма непотраченных выходов равна

18 270,2 BTC, то есть ни одна монета его не покинула. Круглые пакеты по 1 000 BTC удобны для внебиржевых (OTC) продаж, и это самый вероятный следующий этап, но пока ничего не двигалось. У биткоина нет эмитента, и заморозить его некому.

TRON: гонка с Tether, в основном проигранная. 612,7 млн USDT ушли с Binance-Hot 7 в 20:22:45. До заморозки хакер успел переслать 300 млн: около 234 млн ушли в пулы SunSwap и вышли примерно 638 млн TRX, 65,99 млн переслали дальше и заморозили в течение пяти минут, а 312,73 млн заморозили на первом же кошельке-получателе. TRX затем собрали на одном адресе и разбили на пять: четыре кошелька со 158,2 млн, 120 млн, 120 млн и 120 млн TRX не двигались. Пятый отправил 120 млн TRX на `TRBdWqHnDVSZCVGfgHdKFLQPirQcA2PRki`, куда также напрямую пришли 46,38 млн TRX, украденных у Binance. Этот адрес создан в 00:06 UTC 30 октября и с тех пор раздал около 73,7 млн TRX пакетами от 30 тыс. до 950 тыс. на десятки новых адресов. Это единственная часть украденного, которую отмывают прямо сейчас. Elliptic также сообщает, что часть потока в TRON дошла до адреса, где лежат средства от сентябрьского взлома Bitget.

XRP, Solana, NEAR: без движения. 233 461 943 XRP лежат на `rK21t6nGLy4MNDqhvy3pGwcLFy25qgfzMx`, 970 554 SOL на `AffzFDKZbyMiU11zmVBoAqD25ugpr7xoWWyRyGigBEaU`, 12,41 млн NEAR на одном аккаунте. Это нативные монеты без функции заморозки, эмитенты здесь не помогут. Совет безопасности Arbitrum в 00:08 UTC вывел из-под контроля хакера 8 426 ETH и 74,6 млн ARB (TRM).

Сливает ли хакер средства?

Массово и сейчас нет. Слив был в первые часы и только там, где решала скорость: стейблкоины продавали или меняли, пока эмитенты не успели заморозить, а мелкие токены сливали на DEX до 06:36 UTC (Elliptic). С тех пор биткоин, припаркованный эфир, XRP, SOL и NEAR не двигались. Единственный активный поток это TRX через свежие адреса, типичная подготовка к обменным сервисам и OTC-брокерам. Если повторится сценарий прошлых крупных краж, дальше будут мосты между сетями и внебиржевые брокеры, и это может растянуться на недели. Рынок пока реагирует на страх, а не на продажи: 30 октября биткоин упал примерно на 4%, ликвидации достигли около $1,6 млрд.

Слив FUN: что случилось с маленьким токеном

При выметании Binance 14 в 20:24 UTC хакер забрал и 714 911 344 FUN (FUNToken, бывший FunFair) на главный кошелёк. В 23:28:47 UTC всю сумму перебросили на свежий адрес `0x06ea1ab3ecf570029eb1f94dbb9eac06bc79685f`, и тот за 154 транзакции продавал их в тонкий пул FUN/WETH на Uniswap. Продано 134 145 256 FUN, а получено всего 111,48 ETH, около $250 тыс.; цена в пуле рухнула более чем на 90% (CoinDesk). В 06:30 UTC хакер прекратил продажу и вернул остаток, 580 766 088 FUN (около 5,4% всей эмиссии), на главный кошелёк, где они лежат и сейчас. Выручка 111,85 ETH ушла на кошелёк-хранилище 0x79e7...544a. FUNToken попросил биржи временно отключить депозиты FUN. Урок для держателей небольших токенов: горячий кошелёк биржи может держать заметную долю эмиссии вашего токена, и если его украдут, этот «навес» будет давить на цену, пока хакер его держит. А ещё кто-то начал слать хакеру нулевые переводы FUN с адреса-двойника: классическое отравление адресов, на этот раз против самого злоумышленника.

Что это значит для пользователей Binance

Binance заявляет, что балансы клиентов не пострадали, потому что украдены средства собственных горячих кошельков биржи, и что зарезервировала более $6,34 млрд на покрытие ущерба, из них около $5 млрд уже в тех же токенах. Выводы остановлены в 22:15 UTC 29 октября.

Биржа называет предварительный ориентир около 40 часов и обещает полное доказательство резервов к понедельнику. Депозиты работают.

- **Игнорируйте всех, кто предлагает «компенсацию» или «возврат» от Binance.** После каждого крупного взлома за несколько часов появляются фейковые аккаунты поддержки. Binance не просит сид-фраз, оплат и «проверочных переводов».
- **На этой неделе не спешите покупать USDT или TRX у незнакомцев на P2P.** Украденные TRX распыляют прямо сейчас. Монеты, прошедшие через эти адреса, могут заморозить ваш аккаунт на следующей бирже, даже если вы ничего не нарушали.
- **Проверяйте адрес контрагента перед сделкой.** Наш бесплатный чекер читает блеклисты USDT и USDC напрямую из контрактов, поэтому замороженные адреса хакера там видны сразу. Полный список адресов хакера есть в PDF.
- **Следите за доказательством резервов.** Вопрос не в общей сумме, а в каждом токене отдельно: действительно ли эфир и биткоин на замену лежат на указанных кошельках.

Метод и границы

Мы взяли за основу публичный блоклист Elliptic на 48 адресов и опубликованные CoinDesk кошелёк Binance 14 и хеши транзакций, прочитали текущие балансы, код контрактов и статус блеклистов USDT и USDC каждого адреса, прошли деревья биткоина и TRX до мест, где монеты остановились, и сверили каждую заморозку с собственным корпусом событий контрактов USDT в Ethereum и TRON. Окно делегирования найдено чтением кода Binance 14 на исторических блоках. Суммы в долларах, обмены первого часа, позиция в Aave и атрибуция взяты из источников, указанных в таблице. Первопричина не подтверждена, пока Binance не опубликует свой отчёт; как только это случится, мы обновим страницу.

Ваши средства заморожены и вы считаете это ошибкой? Опишите ситуацию в бесплатной оценке кейса: честно скажем, какие шансы и с чего начать.

Приложение A. Реестр адресов

Каждый адрес ниже прочитан напрямую из своего блокчейна в 15:00 UTC 30 октября 2026 года. Время заморозки взято из корпуса событий контракта USDT (Tether) Onyx. «Нет в списке Elliptic» отмечает адреса, которые мы выявили и которых на момент написания нет в публичном блоклисте Elliptic.

Адрес	Сеть	Роль	Баланс сейчас	Статус
`0x28c6c06298d514db089934071355e5743bf21d60`	Ethereum	Горячий кошелёк Binance 14, делегирование EIP-7702 с 20:20:59 до 00:10:35	1 352 018 USDT	Binance (пострадавший); заморожено Tether 22:06:23
`0x5227f603c1ee34ce3c06efe6477003bdfccb2f8c`	Ethereum	Главный кошелёк хакера, принимал выметания	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	Кошелёк хакера	~0	заморожено Tether 21:01:35
`0x0ddf0480016e6bcb2c1f5d190d221fba1320697e`	Ethereum	Кошелёк хакера	0,06 ETH	заморожено Tether 21:01:47
`0x8d53903625b8e839b9df4bd28b0efb1cd6b8639a`	Ethereum	Кошелёк хакера	0,10 ETH	заморожено Tether 21:02:47
`0xaa246bf639586a6ba46762d378ce50ca4fc654a0`	Ethereum	Промежуточный кошелёк *(нет в списке Elliptic)*	174 999 872 USDT	заморожено Tether 21:14:59
`0xb171ca86f820702821383 52ff7111b494060c8c3`	Ethereum	Промежуточный кошелёк *(нет в списке Elliptic)*	30 000 000 USDT	заморожено Tether 21:18:59
`0xccbef95633adb5cd2b5038db5a38d77e726ca263`	Ethereum	Промежуточный кошелёк *(нет в списке Elliptic)*	0,03 ETH	заморожено Tether 21:16:47
`0x7aa4d3029e4c6a8e916300014ad95b6d6c03bfd1`	Ethereum	Кошелёк хакера, делегирован на код смарт-аккаунта *(нет в списке Elliptic)*	0,04 ETH	заморожено Tether 21:12:35
`0x77edef23fbd05921c26fe29fcc3a65e14d2ac3eb`	Ethereum	Кошелёк хакера, делегирован на код смарт-аккаунта	0,01 ETH	
`0x8532fa14acaf483729c449b8458aeddb900543d4`	Ethereum	Кошелёк-хранилище, ни одной исходящей транзакции	197 460 ETH	без движения
`0xc887af690e0301cd4edbbce8f8d31b4ec65b286a`	Ethereum	Кошелёк-хранилище, ни одной исходящей транзакции	137 602 ETH	без движения
`0x897c80d1a9729e94460e2bd93178bd5215158df3`	Ethereum	Кошелёк-хранилище, ни одной исходящей транзакции	78 415 ETH	без движения
`0x7c8601d4645b93cea45f71e118a729332e6b5ca0`	Ethereum	Оператор, развернул контракт-«пылесос»	1,18 ETH	
`0x63e842b054bd624a465454d533c33f573e9c6fae`	Ethereum	Контракт-«пылесос» «Target», цель делегирования Binance 14 *(нет в списке Elliptic)*	~0	

`0x19bee294a6daab49c9e5ab69a5da6c035c70f2bf`	Ethereum	Контракт, развёрнутый оператором	~0	
`0xa97bf7836f8a08f9ed91d41453d371493fae8d10`	Ethereum	Кошелёк для обменов	0,37 ETH, 123 176 USDC	USDC заморожено Circle
`0xc39e690bea48448cc47e7acddfe30e6453e09824`	Ethereum	Промежуточный адрес моста из Avalanche	1 563 813 USDC	USDC заморожено Circle
`0xb3ddec0ccc5c3ba733fcdf5a15f98c95ec5a5fdb`	Ethereum	Кошелёк для обменов	33 005 USDC	USDC заморожено Circle
`0xcf4ca2bdf21bc3a467a00b6afe72b833982723e0`	Ethereum	Кошелёк хакера	~0	пустой
`0x42cdf00c85005630cc8605731b9364f712077810`	Ethereum	Кошелёк хакера	~0	пустой
`0xe7024ab80143b1ef843efe6a58368696cb87958d`	Ethereum	Кошелёк хакера	0,02 ETH	
`0x7f9dc988b46336ad536828fad50fa8fa1e5415e3`	Ethereum	Кошелёк хакера	~0	пустой
`0x8c7111e9a3270457b76f0bd137209089047a6aa4`	Ethereum	Кошелёк хакера	~0	пустой
`0x0084847bb9384d2fc5e8836e663689467e3e4c81`	Ethereum	Кошелёк хакера	0,05 ETH	
`0xa3b3dee870f01560fdbe5af659c9c9135748886f`	Ethereum	Кошелёк хакера	~0	пустой
`0x600d6f00eadabdb514561ceeb43730a7103e8298`	Ethereum	Кошелёк хакера	~0	пустой
`0x811f15855476156ebf86ba3b84fafb8ceaa4e84c`	Ethereum	Кошелёк хакера	~0	пустой
`0x79e70d139fc05aa75f75611fdf2680e9952b544a`	Ethereum	Кошелёк-хранилище, собрал 34 280 ETH с трёх кошельков хакера *(нет в списке Elliptic)*	34 280 ETH	без движения
`0x06ea1ab3ecf570029eb1f94dbb9eac06bc79685f`	Ethereum	Продавец FUN: продал 134,1 млн FUN на Uniswap за 111,48 ETH *(нет в списке Elliptic)*	~0	пустой
`TDqSquXBgUCLYvYC4XZgrprLK589dkhSCf`	TRON	Binance-Hot 7 (TRON), источник 612,7 млн USDT		Binance (пострадавший)
`TG5iBMQPrDzJJAUM8GMVBf1hRaJ1wvzsGi`	TRON	Первый получатель в TRON	312 729 468 USDT	заморожено Tether 21:09:12
`TPBkSjkCMn2ckrMuAP8n2J1jdjbw76bKN4`	TRON	Пересыльщик в TRON к SunSwap	~0	заморожено Tether 21:17:39
`TCzBTkqn66yApqbYoPezaEQosM5DAd7Y62`	TRON	Промежуточный адрес TRON *(нет в списке Elliptic)*	65 990 000 USDT	заморожено Tether 21:21:12
`TSpe5HC3PRD2svJcr1YoGszhHk2mtkyZ8A`	TRON	Сбор TRX *(нет в списке Elliptic)*	~0	пустой
`TKkH2vH6kyi2QKcMbqym53WMuvdd1xvw6K`	TRON	Кошелёк-хранилище TRX *(нет в списке Elliptic)*	158 200 902 TRX	без движения
`TJajtPqDqUGh1Sr1j8ugHoSXBVpaFLLHKT`	TRON	Кошелёк-хранилище TRX *(нет в списке Elliptic)*	120 000 000 TRX	без движения
`TCBAz7itvtX5CjBzVMPQdrbwQLN63ao1fk`	TRON	Кошелёк-хранилище TRX *(нет в списке Elliptic)*	120 000 000 TRX	без движения

TL2F4GhnaFVZBZPncHYjwfYZFW44NcfVwj	TRON	Кошелёк-хранилище TRX *(нет в списке Elliptic)*	120 000 000 TRX	без движения
TAk1xJNWuBYvJHLsUiBFLeuK6xvpQUFYP5	TRON	Кошелёк TRX, переслал 120 млн TRX *(нет в списке Elliptic)*	~0	пустой
TRBdWqHnDVSZCVGfgHdKFLQPirQcA2PRki	TRON	Распылитель TRX, создан 30.10 в 00:06 *(нет в списке Elliptic)*	92 717 498 TRX	движется
bc1q0mtc2f5agpkvlq6hhahmfr3hlr55kyfjhl2mnm	Bitcoin	Корень BTC, разбил 18 270,2 BTC	~0	пустой
bc1qxrxujwxfnvz040jw76d26zhjdg5jura7hs968s	Bitcoin	Адрес-хранилище BTC	1 000,0 BTC	без движения
bc1qepc70u3u476vgvg3hfcwjgu4mecxe2uchs4lag	Bitcoin	Адрес-хранилище BTC	1 000,0 BTC	без движения
bc1qnq6jj9jmlf3945m3l8s0kxnqehrsga300k8t3s	Bitcoin	Адрес-хранилище BTC	1 000,0 BTC	без движения
bc1qdfhmlrdvg4tm87zjl0vyf0xflp5ql50q3g88gw	Bitcoin	Адрес-хранилище BTC	1 000,0 BTC	без движения
bc1qz8hdwv8gmml0u96dsvnzsagz6krjyzxmgxupdp	Bitcoin	Адрес-хранилище BTC	1 000,0 BTC	без движения
bc1q42flhayrzy3zh8lkyevw8qcjduurt9a35wlsyx	Bitcoin	Адрес-хранилище BTC *(нет в списке Elliptic)*	1 000,0 BTC	без движения
bc1qjwdw6vrzq4vf6hckutvx4ucj86awwv99mxnz7w	Bitcoin	Адрес-хранилище BTC	1 000,0 BTC	без движения
bc1q0ts8gaf9ht0rr4u02hr56f8thndqsc4kmkmfv3	Bitcoin	Адрес-хранилище BTC	1 000,0 BTC	без движения
bc1qalwnl7dtaa73fsq5tyn0ghfy3fgfpqkt69tca8	Bitcoin	Адрес-хранилище BTC *(нет в списке Elliptic)*	1 000,0 BTC	без движения
bc1q2wvz0kcsn4hqmajwtey30ud27fl25w8pveznn6	Bitcoin	Адрес-хранилище BTC *(нет в списке Elliptic)*	1 000,0 BTC	без движения
bc1qs3aej5tmcdz0vctz8y9rjcxtxg8v5385577s56	Bitcoin	Адрес-хранилище BTC	1 000,0 BTC	без движения
bc1qs6xnmhar38z44g2za93pv8ygdcwurrh8l87w3v	Bitcoin	Адрес-хранилище BTC *(нет в списке Elliptic)*	1 000,0 BTC	без движения
bc1qm2j6v3247khlwzxl7p9vqnfkghcllyhv9wjaat	Bitcoin	Адрес-хранилище BTC	1 000,0 BTC	без движения
bc1q63qrfrpsg5hh0zzn3kp2xx9vljl7dq7tatsjxp	Bitcoin	Адрес-хранилище BTC *(нет в списке Elliptic)*	1 000,0 BTC	без движения
bc1qg3nrzpuvq2pxqx74tcrywr09dc208ze96n3t53	Bitcoin	Адрес-хранилище BTC *(нет в списке Elliptic)*	1 000,0 BTC	без движения
bc1qm8v88m5fy6kuq9myva2eemwycxqd3e0zcrs2l8	Bitcoin	Адрес-хранилище BTC *(нет в списке Elliptic)*	1 000,0 BTC	без движения
bc1qf5cyvv9w50tx9xx9s3xwsne0z87wvjj9l8a35u	Bitcoin	Адрес-хранилище BTC *(нет в списке Elliptic)*	1 000,0 BTC	без движения
bc1qrg025e2pgx0rwya2kpgtj30972p64jt0hn6zyt	Bitcoin	Адрес-хранилище BTC	832,5 BTC	без движения
bc1qxg0l4p6xc50zuv9cl5f0l0wmaxjpg8wcy7s9ra	Bitcoin	Адрес-хранилище BTC	437,7 BTC	без движения
rK21t6nGLy4MNDqhvy3pGwcLFy25qgfzMx	XRP Ledger	Хранилище XRP	233 461 943 XRP	без движения

AffzFDKZbyMiU11zmVBoAqD25ugpr7xoWWyRyGigBEaU	Solana	Хранилище SOL	970 554 SOL	без движения
efd224256518a7cacd209867963276efed302a8e222c013c43f4b1bd369ae5af	NEAR	Хранилище NEAR	12 410 068 NEAR	без движения

Приложение Б. Источники

- 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