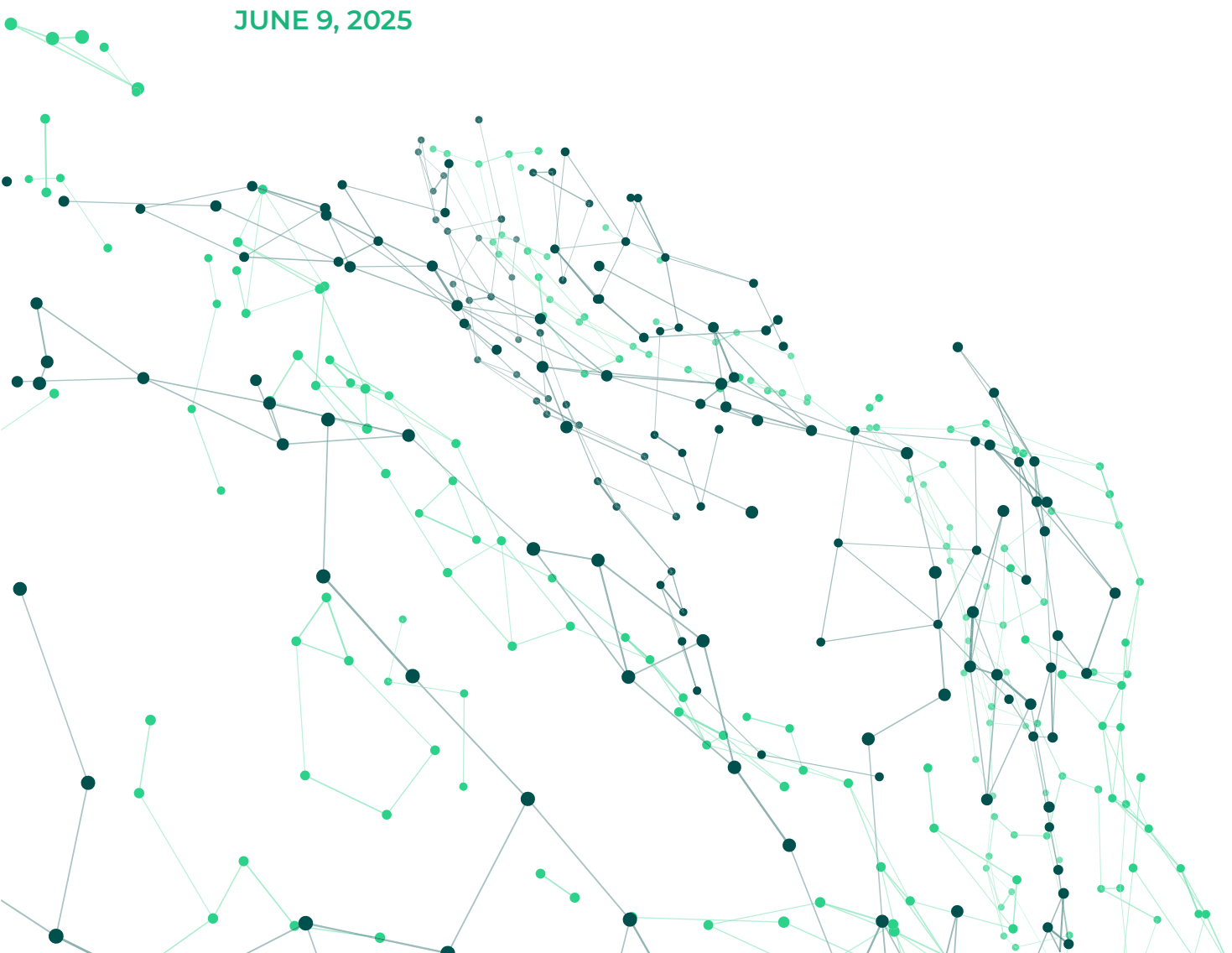


A Deeper Dive into the \$1.5 billion Bybit Hack

A JOINT CASE STUDY BETWEEN ALLIUM AND CHAINARGOS
PROVIDING ADDITIONAL DETAILS ON THE BYBIT HACK

JUNE 9, 2025



Contents.

Case Study	1. Introduction	3
	2. Cross-Chain Analysis and DeFi Link	4
	3. The Surge in THORChain Activity	7
	4. The Allium and ChainArgos Difference	13
About Us	Allium Overview	14
	What is ChainArgos?	15
	Featured Press	16
	Who is this for?	17
	How are we different?	18
	How do we do it?	19
	Better Attribution.	20



1. Introduction

On February 21, 2025, crypto-asset exchange Bybit was hacked and lost over US\$1.5 billion in ether tokens (ETH), with the hack widely attributed to North Korea's Lazarus Group.

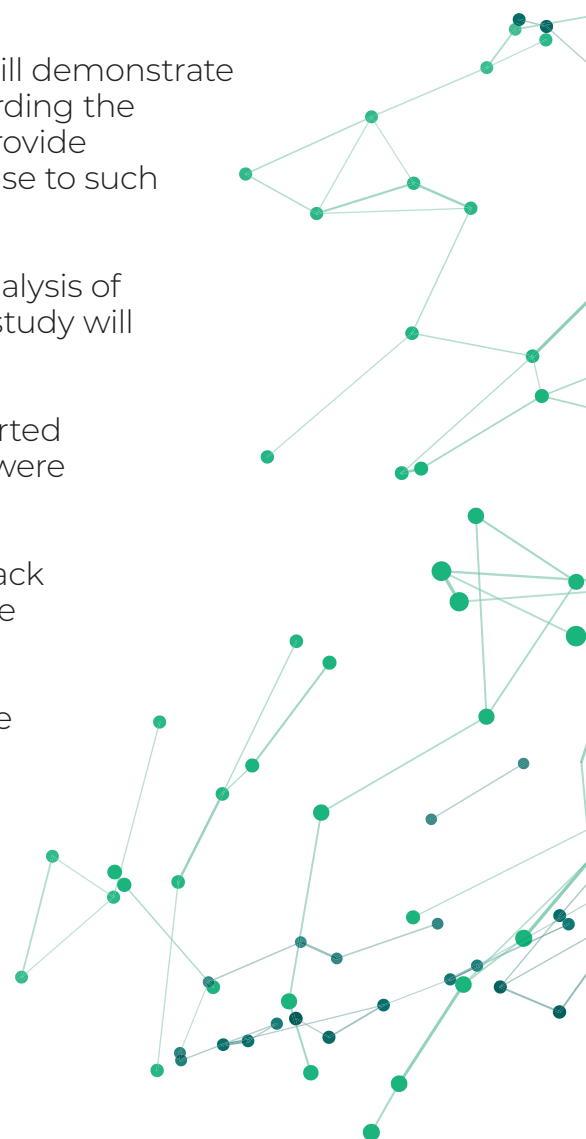
This joint case study, prepared by data teams from blockchain data provider Allium and blockchain intelligence firm ChainArgos, expands on the differing approaches to analyzing the aftermath of the Bybit hack.

First, this case study will look at how Allium's cutting edge blockchain data, enables cross-chain analysis to detect how Lazarus Group effectively laundered stolen funds through multiple DeFi protocols.

Then, building upon the initial analysis, this case study will demonstrate how asking a different set of questions, particularly regarding the role of THORChain in laundering the stolen funds, can provide investigators with better insight, and inform their response to such events.

ChainArgos uses tools designed primarily for financial analysis of blockchain transactions, and using such tools, this case study will demonstrate how:

- a significant spike in activity should have instantly alerted observers to the fact that funds from the Bybit hack were being laundered through THORChain;
- many of wallets that received funds from the Bybit hack were funded and anonymized by some kind of service provider; and
- many (if not all) the proceeds of the Bybit hack can be traced, but that transparency cannot be leveraged in the absence of the appropriate tools.



2. Cross-Chain Analysis and DeFi Link

While many reports detailed how THORChain, ParaSwap, and token transfers were used to launder funds, Allium analyzed cross-chain DeFi (decentralized finance) and DEX (decentralized exchange) activity to uncover an untold part of the story – how the Lazarus Group used DeFi aggregators to discreetly swap US\$386 million through DeFi protocols.

Though Lazarus laundered one-fifth of the stolen funds (US\$263 million) through PancakeSwap alone, this is the first report on the Bybit hack to highlight the protocol (at the time of writing) and the overarching role of aggregators.

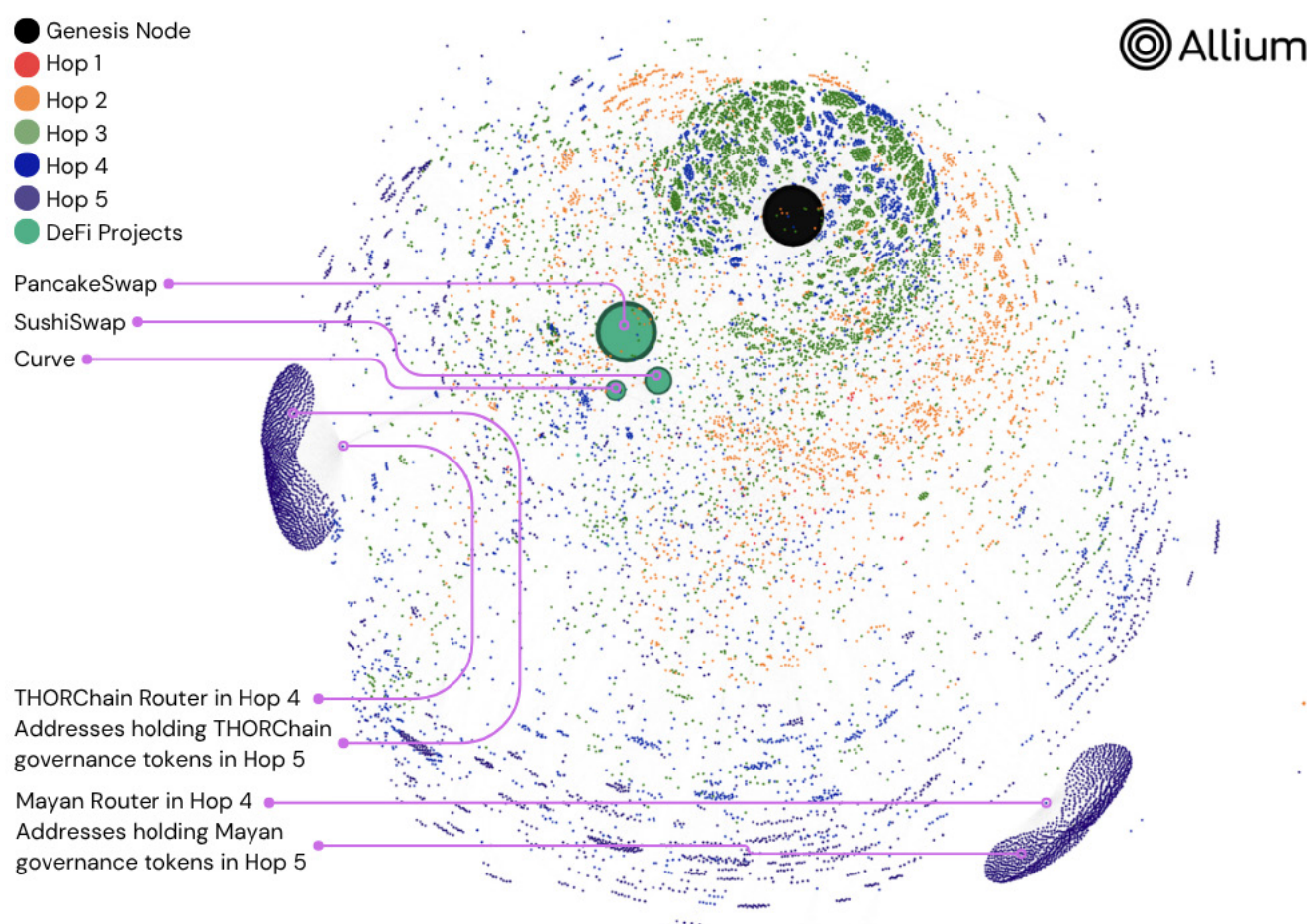


Figure 1. Graph visualization of Allium's cross-chain data, enabling data wizards to track and visualize every interaction within five layers of transactions on Ethereum. (Source: Allium)

Allium's cross-chain data enables data wizards to track and visualize every interaction within five layers of transactions on Ethereum and the analysis involved:

- 13,000 unique wallets,
- 127,000 transactions,

With a cumulative volume of \$12 billion,

- 5 hops away from the genesis node.

DEX Swaps¹ Make Recovery more Challenging and Liquidity more Available

DEX swaps make asset recovery more challenging by dispersing funds across multiple assets, requiring victims and authorities to contact each project separately for freezing.

Additionally, swapping a large amount of one asset for smaller amounts of multiple assets allows attackers to access more liquidity pools to cash out stolen funds.

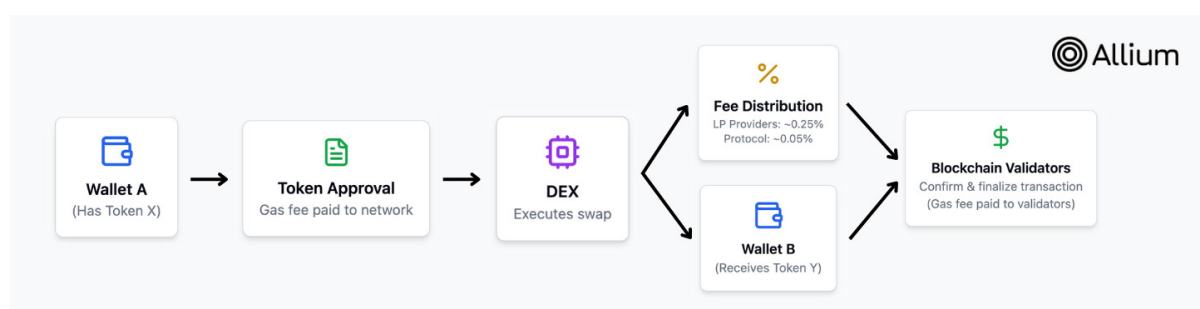


Figure 2. Basic anatomy of a DEX swap. (Source: Allium)

DeFi aggregators bring together trades across various decentralized finance platforms into one place. They aim to optimize trades by pulling competitive prices from across the DeFi landscape. DeFi aggregators permit users to analyze and combine other users' trading strategies, which could potentially make the process more efficient and user-friendly.²

¹ A crypto swap is a transaction that results in the direct exchange of one crypto for another, without the need for an intermediary to facilitate the trade. Trading on a centralized exchange is facilitated by an intermediary that exchanges your crypto on your behalf. Swapping on a decentralized exchange (like Uniswap Protocol) uses smart contracts to execute your swap, so there is never a third party in control of your funds. (Source: Uniswap).

² <https://www.coinbase.com/learn/advanced-trading/what-is-a-defi-aggregator#:~:text=DeFi%20aggregators%20bring%20together%20trades,from%20across%20the%20DeFi%20landscape.>

DeFi Project	USD Volume
PancakeSwap	\$263 million
SushiSwap	\$74 million
Curve	\$47 million
Uniswap	\$39 million
Fluid	\$10 million
DeBridge	\$3 million
Across	\$2 million
Polygon	\$836,000
Symbiosis	\$326,000
Arbitrum	\$9,000

Figure 3. Amounts from the Bybit hack processed through various DeFi projects. (Source: Allium)

DeFi Projects Enable Attackers to Launder Assets Pseudonymously

DeFi projects are used for laundering because they do not require KYC (Know Your Customer) verification to transact, creating a pseudonymous environment where attackers can directly interact with smart contracts.

While the IRS recently mandated³ that front-end DeFi platforms enforce KYC for tax reporting purposes, these regulations won't be enforced until 2027.

Instead, DeFi projects check an address's history to determine transaction eligibility.

However, these addresses must be flagged manually, and most data providers are too slow to support real-time transaction validation. To identify fraud-connected wallets in real-time, organizations need data that clearly shows all DEX and aggregator activity such as provided by Allium.

Conversely, centralized exchanges (Coinbase, Binance, and Bybit) implement AML (Anti-Money Laundering) controls similar to traditional banks. They require KYC verification, monitor transactions for suspicious patterns, and report unusual activities to regulators – creating clear audit trails linking blockchain addresses to verified identities.

Nonetheless, could an inexplicable surge in activity on a DeFi platform have alerted its operators of potential issues and anomalies?

³ <https://www.forbes.com/sites/shehanchandrasedera/2024/12/27/understanding-the-new-irs-defi-broker-tax-regulations/>

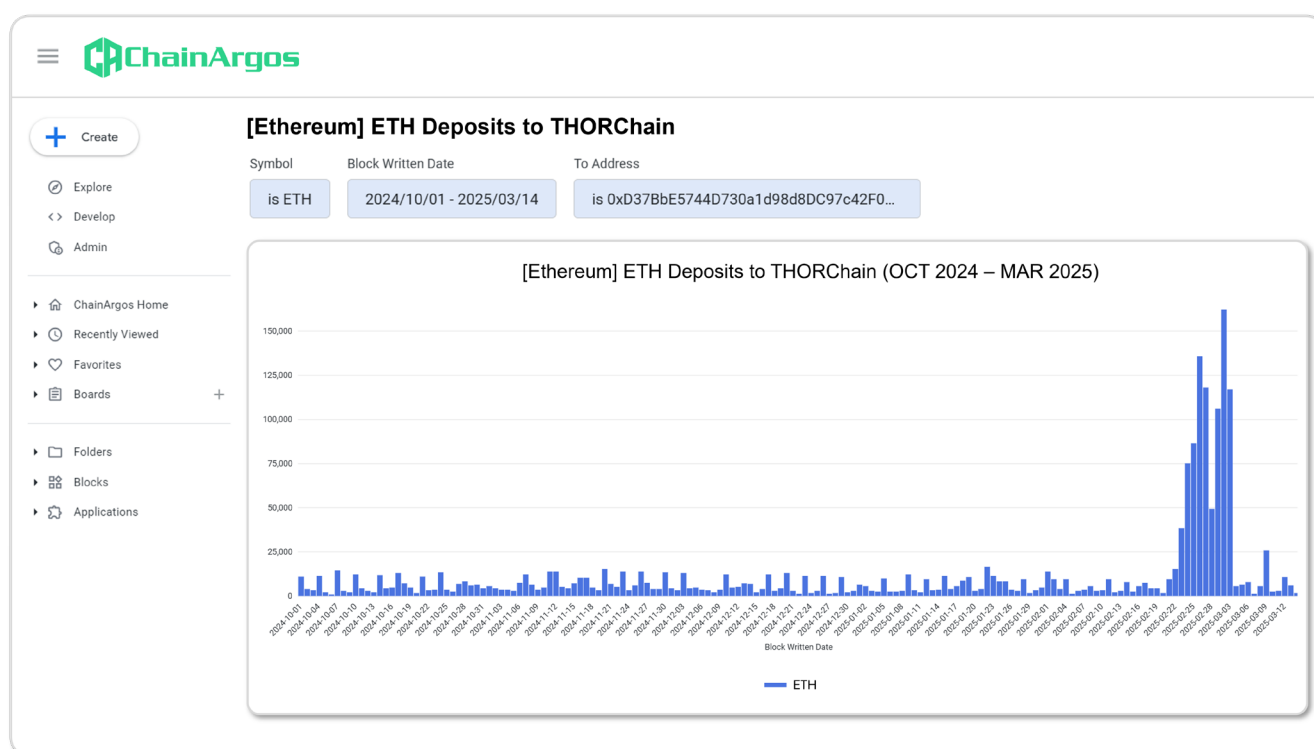
3. The Surge in THORChain Activity

While certain protocols might introduce complexity or require more diligent investigation, the underlying data on the blockchain remains accessible and analyzable if approached in the appropriate manner.

Without any further investigation, and without having ever tagged a single Bybit hacker address, the surge in ETH deposits into THORChain, in excess of the average deposit, should have immediately raised questions for anyone monitoring blockchains in general.

The Bybit hack occurred on February 21, 2025, and by the very next day, deposits of ETH to THORChain saw a 58% surge. By February 23, 2025, ETH deposits to THORChain increased by 155%.

This significant and unmistakable increase in ETH deposits to THORChain is obvious from Figure 4.



When the ETH deposits from the Bybit hacker addresses are superimposed on the same chart in Figure 5., it is even more apparent that almost all of the increase in ETH deposits to THORChain were as a result of the Bybit hackers pushing funds through the platform.

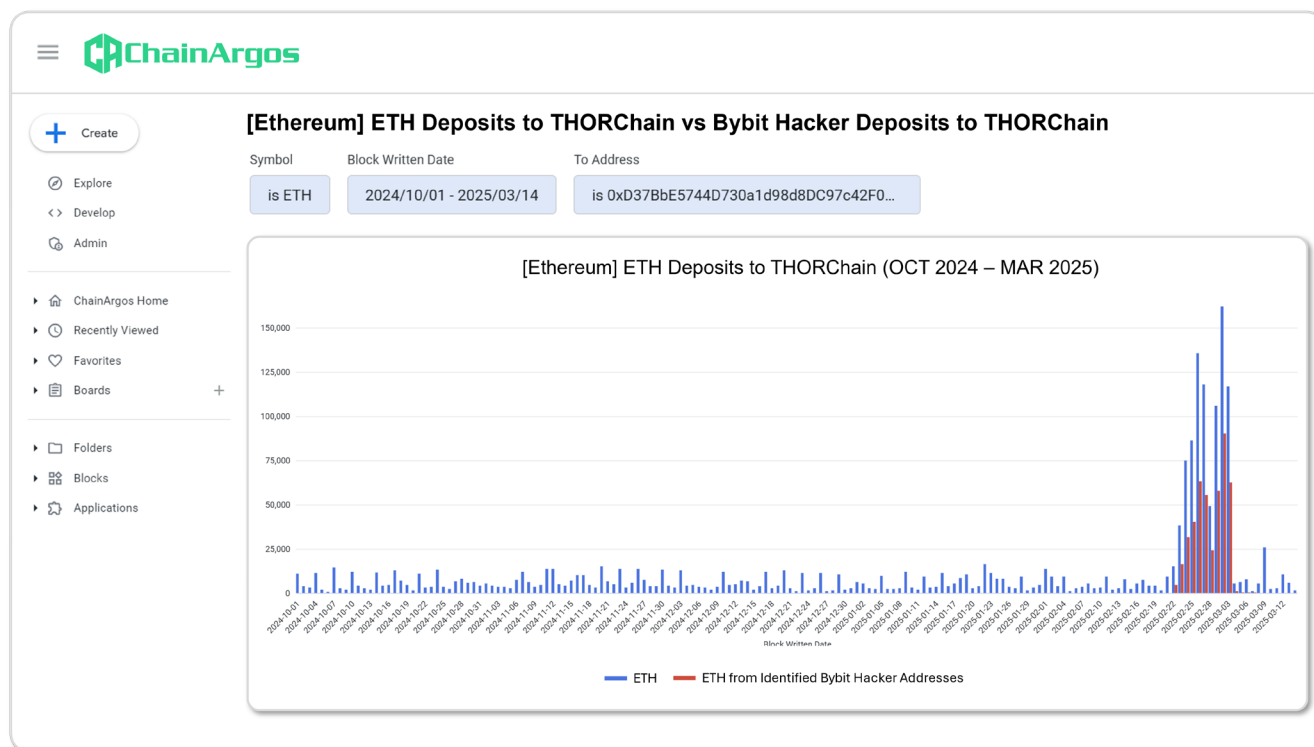


Figure 5. ETH deposits to THORChain (in blue) and ETH deposits to THORChain by identified Bybit hacker addresses (in red). Notice how the ETH deposits by the Bybit hacker addresses almost maps the increase in ETH deposits to THORChain identically. (Source: ChainArgos)

Notice that in Figure 5., the significant increase in ETH deposits to THORChain are almost entirely mapped to the Bybit hacker addresses.

As more Bybit hacker addresses are identified, the gap is expected to close even further, and it would not at all be surprising that the increase in ETH deposits to THORChain are almost entirely attributable to the Bybit hackers making such deposits.

Blockchain transaction activity can change for a variety of reasons, but a sudden increase, especially of the order of magnitude as seen by THORChain immediately after the Bybit hack could have been noted by both law enforcement and regulators.

Previously, ChainArgos noted how a purported 700% increase in the usage of the Ronin blockchain was in fact as a result of token airdrops, and not because of any genuine economic activity.

Because ChainArgos leverages Allium's blockchain data and applies traditional financial tools to analyze blockchain transactions, relevant authorities could have been automatically notified of the statistically significant increase in ETH deposits to THORChain, prompting timely investigation and remedial action.

Allium and ChainArgos enable macro analysis of blockchain transactions, allowing regulators and law enforcement agencies to very quickly identify areas of interest and potential investigations.

In the next section, we see how ChainArgos and Allium power micro analysis by investigating a Bybit hacker address and demonstrating how access to such data can ensure that constrained investigative resources are directed to the most effective areas.

Unidentified Service Providers

As identified by ZachXBT,⁴ and others,⁵ the Bybit Hacker 0x476 Address⁶ is one of the main addresses used to receive the proceeds of the Bybit hack.

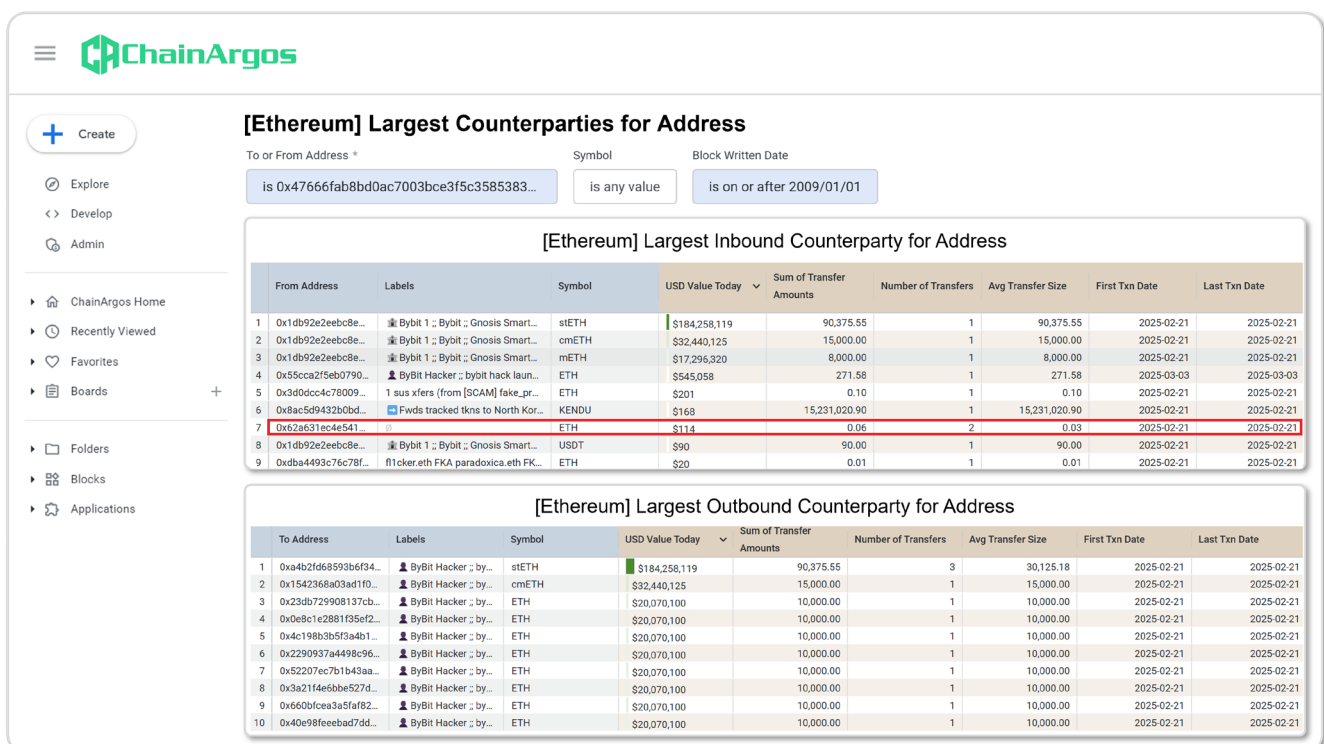


Figure 6. Largest Counterparties for the Bybit Hacker 0x476 Address. Several addresses send token amounts of ETH to the Bybit Hacker 0x476 address on February 21, 2025, and we will examine the 0x62a address which sends 0.06 ETH to the Bybit Hacker 0x476 address. (Source: ChainArgos)

⁴ <https://x.com/arkham/status/189303342422441885>

⁵ <https://slowmist.medium.com/slowmist-hacker-techniques-and-questions-behind-bybits-nearly-1-5-billion-theft-09f0b59da2e2>

⁶ 0x47666fab8bd0ac7003bce3f5c3585383f09486e2

We can see from Figure 6., that Bybit Hacker 0x476 Address is one the main addresses that receive stETH, cmETH and mETH from identified ByBit wallet addresses.

Notice however that the Bybit Hacker 0x476 Address itself receives a token amount of 0.06 ETH from the Service Provider 0x62a Address⁷ on the day of the Bybit hacking, February 21, 2025.

Outside of this token transfer of ETH (pun intended), the Service Provider 0x62a does not interact with the Bybit Hacker 0x476 on any other occasion.

The transaction of ETH from the Service Provider 0x62a Address to the Bybit Hacker 0x476 Address immediately stands out because the transfer of 0.06 ETH is small enough to create a reasonable inference this is for the provision of gas fees and informs the next step of our investigation.

Analyzing the transaction activity of the Service Provider 0x62a Address in Figure 7., it becomes immediately apparent that this address does not just provide gas fees to the Bybit Hacker 0x476 Address, but a slew of other addresses associated with the Bybit hack as well.

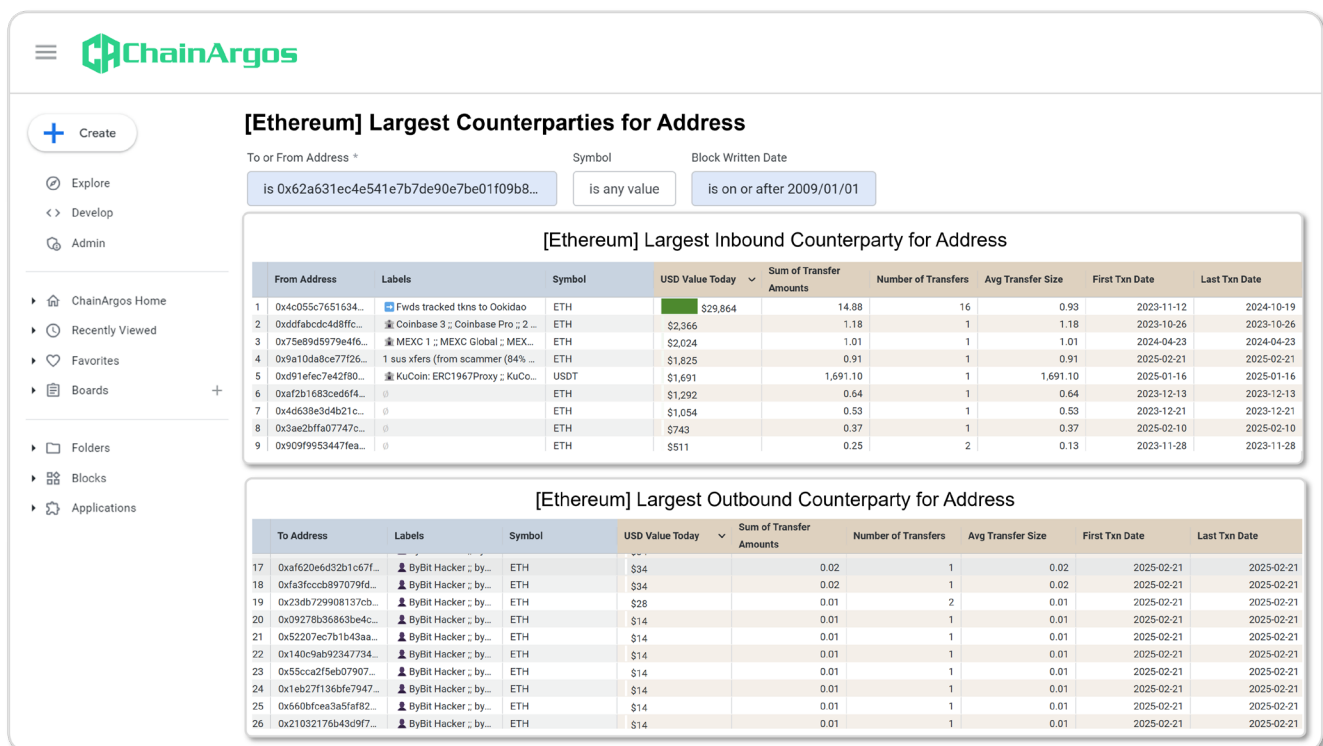


Figure 7. Largest Counterparties for the Service Provider 0x62a address. Notice how the Service Provider 0x62a address funds wallets associated with the Bybit hack on February 21, 2025. (Source: ChainArgos)

⁷ 0x62a631ec4e541e7b7de90e7be01f09b88f67126

In total, the Service Provider 0x62a Address appears to have funded the gas fees for a total of 41 addresses identified as being controlled by the Bybit hacker.

But perhaps more significantly, whoever controls the Service Provider 0x62a Address also has accounts with the crypto-asset exchanges Coinbase, MEXC, and KuCoin.

We know this because addresses identified as belonging to these exchanges had approved transfers of ETH to the Service Provider 0x62a Address as highlighted in Figure 8.

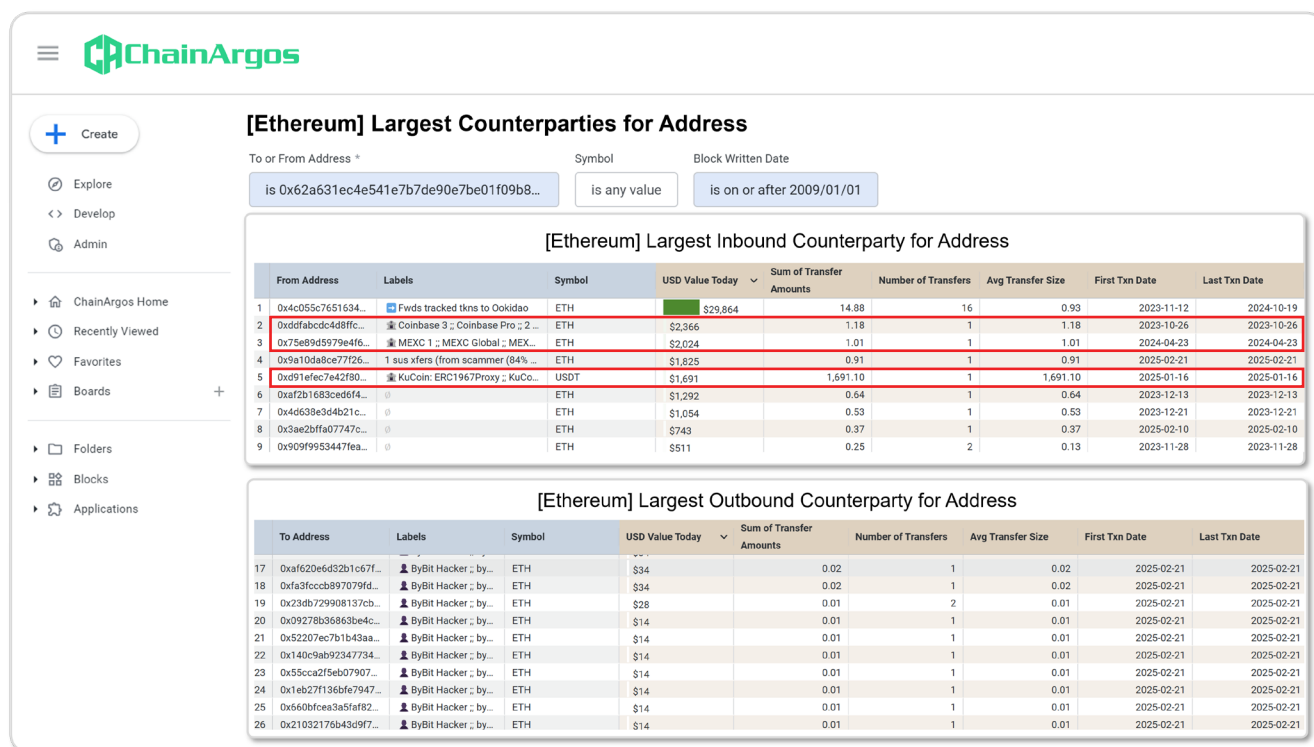


Figure 8. Largest Counterparties for the Service Provider 0x62a Address. The various crypto-asset exchanges from which the Service Provider 0x62a Address has received crypto-assets from has been highlighted. (Source: ChainArgos)

Typically, exchanges facilitate the transfer of crypto-assets from the exchange's wallet addresses to external addresses only after they have been "whitelisted" or proved to belong to the owner of the account with that exchange.

It would stand to reason that Coinbase, MEXC, and KuCoin would be in possession of the requisite know-your-customer documentation of whoever controls the Service Provider 0x62a Address.

With this information, investigators could query the owner of the Service Provider 0x62a address as to why they provided gas fees to the various Bybit hacker wallet addresses, or if they were providing such pre-funded wallets as a service.

In the past, one of the easiest ways to anonymously fund an Ethereum wallet was to mine ETH, essentially making the source of funds of such a wallet “untraceable.”

As Ethereum moved to Proof-of-Stake, such anonymization methods became less practicable and in the wake of this shift, a cottage industry of service providers emerged to provide such anonymization services, often using ETH that had been mined a long time ago.

It is entirely possible that whoever was operating the Service Provider 0x62a Address did not know the wallets they were funding on February 21, 2025 would be used to receive the proceeds of the Bybit hack.

Nevertheless, identifying such service providers enables authorities to push investigations forward.

4. The Allium and ChainArgos Difference

As more economic activity moves onto the blockchain and as more assets are tokenized, the need for tools that enable effective financial analysis of blockchain transactions grows.

Leveraging Allium's blockchain data solutions, ChainArgos is able to focus on building effective applications that allow both macro and micro financial analysis of blockchain transactions, enabling unprecedented insight.

- **Identify Key Transaction Clusters:** Start by identifying the initial outflows of ETH from the known Bybit exploit addresses, then track transactions where significant amounts of ETH were moved, to understand the areas to focus investigations.
- **Focus on Counterparties:** Look for patterns in the destination addresses of the swapped cryptocurrencies. Are funds being consolidated in a few addresses? Are these addresses known to interact with specific service providers? Small transfers shouldn't be ignored and can often provide insight into previously unidentified service providers, or unexpected relationships.
- **Financial Analysis:** As demonstrated from the Bybit hack, tracking and tracing the flow of hacked proceeds alone does little to advance safety or security on the blockchain. Instead, a combination of macro and micro financial analysis helps identify service providers such as Service Provider 0x62a, creating a potential weak point that authorities can leverage to break apart such networks that facilitate illicit activities.

Blockchain intelligence doesn't need to be complicated. Because one of the fundamental goals of any blockchain transaction is the transfer of value, blockchain transactions need to be viewed through a financial lens, to deliver actionable insight.

What is the economic purpose of a transaction? Who is providing the wherewithal to facilitate that transaction and what means are they using?

Working with Allium, ChainArgos is powering an entirely different approach to blockchain intelligence, putting in the hands of analysts and investigators powerful tools for financial analysis, to enable the uncovering of key players, service providers, and relationships that would otherwise have gone unnoticed.

Allium Overview

Allium delivers **accurate**, **fast**, and **simple** blockchain data and insights in a unified platform. Leading institutions and companies like Visa, Stripe, Fidelity, Grayscale, Uniswap, and Phantom leverage Allium to easily answer strategic questions, identify investment & growth opportunities, manage business reporting & compliance, and power their applications.

Our Core Segments



Segment	Backend Data Infrastructure	Derived Data Products	Research Institutions	Ecosystem & Growth	Finance & Accounting	Compliance & Investigations
Use Case	Power application backends	White-label analytics and reports	Deep-dive onchain activity - assets, flows, staking, yields	Monitor competitor market share and user behavior	Transaction ledger reconciliation	Flagging suspicious users and activity
Use Case	Brokerages, Wallets, Payments	Analytics Providers	Funds, Banks, Researchers, Strategy Teams	Strategy Teams, Growth Teams	Payments, Custodians, Funds, Banks	Payments, Regulators, Investigators
Featured	Phantom trusts Allium's data platform to fetch real-time transactions and serve millions of user requests.	Visa , Messari , RWA.xyz , and DeFiLlama use Allium's data to build their data dashboards and provide insights to others	Visa , Fidelity , Grayscale , Brevan Howard , and Electric Capital leverage Allium's data platform to guide strategy and build investment theses	Uniswap , Magic Eden , and Wormhole utilize Allium to understand market share , protocol revenue, and onchain user behavior	MoonPay and Anchorage Digital trust Allium's securely-shared data across 80+ chains to power financial reconciliation	Stripe leverages Allium's data for payments fraud detection . Wormhole , Jupiter , Jito , and Drift rely on Allium to detect fake accounts and bot farms
Public Examples	Phantom x Allium	DeFiLlama x Allium Visa Stablecoin Dashboard	Grayscale ETH Report BHD Stablecoin Report Electric Capital NFT Analytics	Uniswap x Allium for DEX Analytics	Double Entry Bookkeeping Schema	Wormhole x Allium Sybil Detection Jupiter Botnet Report

What is ChainArgos?

ChainArgos is the blockchain intelligence firm best known for uncovering crypto-asset exchange Binance's \$1.4bn BUSD stablecoin undercollateralization, forcing the New York Department of Financial Services to take action.

We provide unparalleled blockchain intelligence by focusing on the financial drivers of transactions, facilitate investigations and analysis centered on the economic value of transfers, and provide insight into the motivation behind specific flows.

ChainArgos is recognized globally as a leader in blockchain intelligence.



We've tracked illicit flows funding terrorism and sanctions evasion, analyzed transaction patterns connecting global scams, and uncovered crypto-asset trading opportunities before the market.

Where else have you seen us?

ChainArgos works with the United Nations, governments, central banks, financial institutions, hedge funds, proprietary trading firms, regulators, law enforcement and intelligence agencies, research institutes, universities, and crypto-asset service providers globally.

We're trusted by top news outlets including the Wall Street Journal, Bloomberg, Forbes, Fortune, Thomson Reuters, and the South China Morning Post, for unimpeachable blockchain intelligence.

Here's just a selection of our blockchain intelligence that created news:

<p>Bloomberg</p>  <p>Binance Acknowledges Past Flaws in Maintaining Stablecoin Backing</p> <ul style="list-style-type: none"> Blockchain analyst Reiter had flagged gaps in Binance-peg BUSD Binance says earlier 'operational delays' have now been fixed 	<p>Forbes</p>  <p>Did Digital Currency Group Profit From \$60 million In North Korea Crypto Money Laundering?</p>	<p>THE WALL STREET JOURNAL.</p>  <p>From Hamas to North Korean Nukes, Cryptocurrency Tether Keeps Showing Up</p> <p>Tether has allegedly been used by Hamas, drug dealers, North Korea and sanctioned Russians</p>
<p>THE WALL STREET JOURNAL.</p>  <p>The Shadow Dollar That's Fueling the Financial Underworld</p> <p>Cryptocurrency Tether enables a parallel economy that operates beyond the reach of U.S. law enforcement</p>	<p>Bloomberg</p>  <p>Stablecoin Operator Moves \$1 Billion in Reserves to Bahamas</p> <ul style="list-style-type: none"> Move reflects worsening US banking conditions for crypto firms TrueUSD's circulation has more than doubled in the last month 	<p>South China Morning Post</p>  <p>How crypto investigators uncover scammers' blockchain billions, scale of money laundering in Asia</p>

Who uses blockchain intelligence?



Finance and
Banking



Compliance



Law Enforcement



Regulators and
Policymakers

Finance and Banking

Assess the risks and opportunities in crypto-assets, stablecoins, and decentralized finance. Develop innovative products, explore tokenization opportunities, and generate new revenue streams.

Compliance

Fight money laundering, expand know-your-customer tools, and combat the financing of terrorism while expanding your customer base. Manage risk from customer crypto-assets and confidently verify sources of crypto-asset wealth.

Law Enforcement

Terrorists and criminals are using blockchain technology to avoid the banking system, launder money, and fund operations. Blockchain wallet analysis and transaction tracing fights crime, prosecutes criminals, and tracks illicit fund flows.

Regulators and Policymakers

Develop and implement effective crypto-asset and stablecoin supervisory, licensing tax, compliance, and regulatory frameworks to foster innovation, while managing threats to national security and the financial system.

How are we different?

We deliver actionable blockchain intelligence.

Say “no” to pseudo-science and “yes” to blockchain intelligence you can count on for commerce, compliance, and crime-fighting.

ChainArgos is built by finance, legal, and technology professionals to deliver actionable blockchain intelligence focused on financially-relevant analysis.

Whether you're looking to on-board a customer, determine source of wealth, or ensure your evidence isn't rejected on appeal, our blockchain intelligence is based on established principles of statistics, math, and forensic science.

Extreme Versatility

Create compliance and commercially-driven analysis in a single place and arrive at better business decisions faster.

No-Code Customization

Build any query or analysis without programming skills or coding.

Financially-Relevant

Standard financial measures combined with blockchain intelligence for actionable insight.

Data Integrity

ChainArgos runs its own blockchain nodes, and we never enrich our data with yours, so you can be sure of data integrity.

API Ready

Robust and resilient APIs with 99.99% uptime. Minimal code required for easy integration.

Automated Alerts

Schedule automated alerts and reports via Email, Webhook, Amazon S3 and SFTP so you're always in the know when something happens.

How do we do it?

Blockchain intelligence is a relatively new industry, and it's not uncommon to hear of methods which have little basis in finance, let alone forensic science.

Let's look at one example to understand the limitations of blockchain tracing.

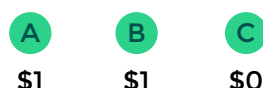


Fig. 1

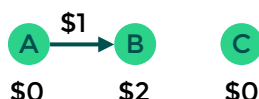


Fig. 2

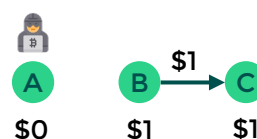


Fig. 3

In Fig. 1, A and B start with \$1, while C starts with \$0. In Fig. 2, A transfers their \$1 to B who now has \$2. Finally, in Fig. 3, B transfers \$1 to C, who now has \$1.

If it turns out A is an illicit actor, with what degree of confidence can we say that C has received \$1 from illicit sources? 50-50?

Would you accept a “risk score” of 50%?

Follow the money.

Instead of passing off “risk scores” as “risk management” ChainArgos helps you follow the money.

Most blockchain transactions don't derive from a single source, and believing they do is what leads to poor outcomes.

Make better decisions by focusing on what matters - where the money went, where it came from, and where does it look like it's headed to?

How much does one address deal with another? What's the average transaction size? What's the frequency? What's the crypto-asset or stablecoin of choice? What's the transaction behavior? When did the transaction size change?

And so much more.

The screenshot shows the ChainArgos web application. The main content area displays data for a specific address, organized into several sections:

- [Blockchain] Counterparties for Addresses**: Includes input fields for 'To or From Address' and 'Symbol'.
- [Blockchain] Your Queried Addresses' Labels & Categories**: A table with columns: Address, Labels, Categories, Organizations. It shows one row with address '1'.
- Blacklisting Info (If Any)**: A table with columns: Timestamp Date, Authority, Action, Blockchain. It shows one row with timestamp '1'.
- [Blockchain] Inbound Counterparties**: A table with columns: From Address, Labels, Symbol, USD Value Today, Sum of Transfer Amounts, Number of Transfers, Avg Transfer Size, First Txn Date, Last Txn Date. It shows two rows, '1' and '2'.
- [Blockchain] Outbound Counterparties**: A table with columns: To Address, Labels, Symbol, USD Value Today, Sum of Transfer Amounts, Number of Transfers, Avg Transfer Size, First Txn Date, Last Txn Date. It shows two rows, '1' and '2'.

Better attribution.

Don't risk critical legal, trading, and compliance decisions to questionable or subjective attribution methods. Trust math and science.

ChainArgos is the only blockchain intelligence firm that delivers programmatic address labels and wallet tags that are unassailable whether you're making business decisions or preparing to sue someone.

Blockchain addresses are automatically ranked and labeled based on a variety of factors including:

- **Transaction Count:** the number of transactions by an address. Sending \$100,000 in one transaction may have very different implications from sending 10 transactions of \$10,000 each. Either way, you'll know the difference.
- **Lifetime Sent/Received:** lists the biggest sender and/or receiver of any given crypto-asset or stablecoin currently. Markets are extremely dynamic. The biggest movers today may not be the same tomorrow.
- **Max. Historical / Current Balances:** helps you decide whether an address is participating in affiliated crypto-assets and/or stablecoins based on their maximum historical balance and who's stocking the highest current balances.
- **Recipient Number:** gives you a sense of whether they were an early adopter, or even possibly an insider of a crypto-asset or stablecoin. Recipients are ranked according to the date and time they received a crypto-asset or stablecoin.

Say "no" to dodgy wallet tagging and "yes" to attribution you can trust.

Legal Disclaimers.

THE INFORMATION CONTAINED IN THESE MATERIALS IS FOR INFORMATION PURPOSES ONLY AND NOT INTENDED TO BE RELIED UPON.

The information contained herein is information regarding research and analysis performed by ChainArgos Pte. Ltd., a company incorporated with limited liability under the laws of the Republic of Singapore with registration number 202303560W ("the Company"). The information herein has not been independently verified or audited and is subject to change, and neither the Company or any other person, is under any duty to update or inform you of any changes to such information. No reliance may be placed for any purposes whatsoever on the information contained in this communication or its completeness. No representation or warranty, express or implied, is given by, or on behalf of the Company or any of their members, directors, officers, advisers, agents or employees or any other person as to the accuracy or completeness of the information or opinions contained in this communication and, to the fullest extent permitted by law, no liability whatsoever is accepted by the Company or any of their members, directors, officers, advisers, agents or employees nor any other person for any loss howsoever arising, directly or indirectly, from any use of such information or opinions or otherwise arising in connection therewith. In particular, no representation or warranty is given as to the reasonableness of, and no reliance should be placed on, any forecasts or proposals contained in this communication and nothing in this communication is or should be relied on as a promise or representation as to the future or any outcome in the future.

This document may contain opinions, which reflect current views with respect to, among other things, the information available when the document was prepared. Readers can identify these statements by the use of words such as "believes", "expects", "potential", "continues", "may", "will", "should", "could", "approximately", "assumed", "anticipates", or the negative version of those words or other comparable words. Any statements contained in this document are based, in part, upon historical data, estimates and expectations. The inclusion of any opinion should not be regarded as a representation by the Company or any other person. Such opinion statements are subject to various risks, uncertainties and assumptions and if one or more of these or other risks or uncertainties materialize, or if the underlying assumptions of the Company prove to be incorrect, projections, analysis, and forecasts may vary materially from those indicated in these statements. Accordingly, you should not place undue reliance on any opinion statements included in this document.

By accepting this communication you represent, warrant and undertake that you have read and agree to comply with the contents of this notice.

