

A complex network graph background with nodes and connecting lines in shades of green and black, representing blockchain transactions and relationships.

Is it wrong to make money laundering for North Korea?

A CASE STUDY ON HOW RAILGUN INVESTORS COLLECTED
FEES MADE FROM LAUNDERING FUNDS FOR NORTH KOREA

NOVEMBER 5, 2024

Contents.

Case Study	Introduction	3
	What is Railgun?	4
	Railgun's Use of EOAs & Manual Control	4
	A Railgun Timeline	5
	Fee Process Version 1	6
	Fee Process Upgrade Begins	7
	DPRK Use of Railgun	7
	Fee Process Version 2	8
	How are Railgun's fees claimed?	9
	Where do DCG's Railgun fees end up?	10
	Did DCG participate in "management"?	11
	Could this have been prevented?	11
	Appendix.	13
About Us	Who are we?	15
	Featured Press	16
	Who is this for?	17
	How are we different?	18
	How do we do it?	19
	Better Attribution.	20

Introduction

On October 31, 2024, Forbes¹, with support from ChainArgos, broke news that Digital Currency Group (“DCG”), a venture capital firm, earned fees generated from the laundering of funds for North Korea through DCG’s investment in crypto-asset mixer Railgun.

The 2-month long Forbes investigation revealed that DCG, which also owns the U.S.-regulated Grayscale Bitcoin Trust product, the first institutional bitcoin product, was the beneficiary of fees derived from the laundering of funds linked to North Korean hacking.

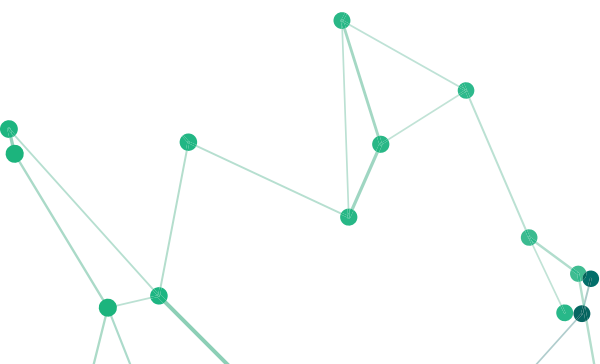
Railgun characterizes itself as a crypto-asset privacy protocol but has been used to obfuscate the proceeds of hacks, including the Harmony Bridge hack which was reported by the FBI to have been conducted by North Korea’s Lazarus Group.

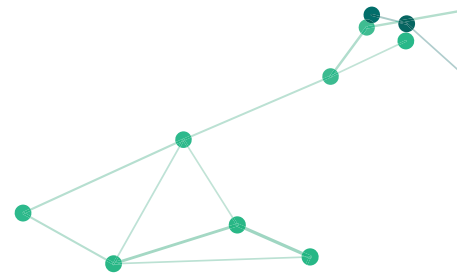
This case study will show you how ChainArgos traced the fees Railgun earned from the laundering of North Korean funds to DCG, where those fees ended up, and the significant degree of manual control involved in managing, processing and distributing these fees.

In this case study, you may come across terms such as “EOA”, “proxy contract” and “implementation contract” which you may be unfamiliar with. More information about these terms can be found in the Appendix attached to the end of the case study.



¹<https://www.forbes.com/sites/javierpaz/2024/10/31/did-digital-currency-group-profit-from-60-million-in-north-korean-crypto-money-laundering/>





What is Railgun?

Railgun claims to be a privacy protocol but operates in the same way a crypto-asset mixer does. It charges fees of 0.25% of the crypto-asset being mixed. So for instance, if the ETH token was being sent to Railgun the fees charged by Railgun would be 0.25% of the total amount of ETH running through Railgun's service.

Following the Harmony Bridge hack by North Korea ("DPRK") as reported by the FBI, as much as \$60 million worth of hacked crypto-assets were sent to Railgun for obfuscation².

Railgun's documentation describes the service as "100% non-custodial" and that it "has no owner."

However, this case study will show how fees earned from the DPRK's use of Railgun were transferred through externally owned accounts ("EOAs") during an upgrade process, before being transferred to DCG, an investor in the Railgun protocol.

EOAs are not automated, they are addresses controlled by off-chain private keys. By sending Railgun's fees through EOAs, Railgun "broke the decentralization" and showed that someone was running at least that part of the system manually.

Railgun's Use of EOAs & Manual Control

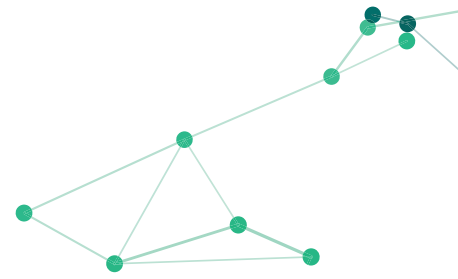
Over the course of Railgun's development the protocol has upgraded its fee process several times including periods when fees were generated from DPRK's use of Railgun's mixing service.

While upgrading Railgun's fees process, historical fees generated from Railgun's use which had accumulated up to that period would need to somehow be migrated from the old fee process to the new one.

Complicating matters, if there was a time lapse between legacy and upgraded versions of Railgun's fee process there would need to be some way to hold accumulated Railgun fees in the interim and that method was manually, through EOAs.

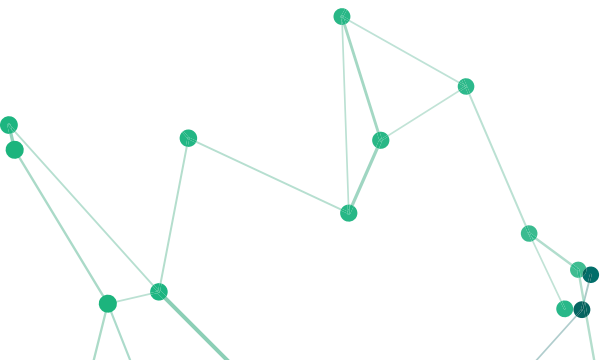
Around the time DPRK used Railgun, the Railgun Team effected an upgrade of the fee process that involved manual EOA-managed control of the fees that had been derived from DPRK use. This means fees derived from DPRK's use of Railgun were handled off-chain by the Railgun Team.

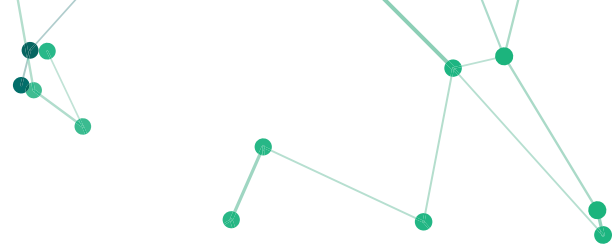
² <https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft>



A Railgun Timeline

SEP 2022	Railgun initial fee process deployed at Railgun Fee Proxy V1.
<hr style="border-top: 2px dashed red;"/>	
Railgun System Pause	
NOV 2022	<p>Railgun Team upgrades the fee process and Railgun Fees accrued to this point claimed by Railgun Team EOA on November 24, 2022.</p> <p>Railgun Team EOA sent these accrued fees back to the Railgun Treasury on the same day.</p>
DEC 2022	<p>Railgun Team upgrades the Railgun fee process, and deploys a new smart contract Railgun Sweeper 1.</p> <p>Railgun Sweeper 1 used to move accrued fees from Railgun Fee Proxy V1 back to the Railgun Treasury wallet, essentially “resetting” the fee system.</p> <p>Railgun Team deploys another smart contract to Railgun Sweeper 2 and on December 5, 2022, the Railgun Treasury sent some accrued fees to Railgun Sweeper 2.</p> <p>Railgun Sweeper 2 would continue to receive manually-triggered fee transfers from December 2022 to January 2023.</p>
JAN 2023	<p>Sometime between January 13 and 14, 2022, DPRK’s Lazarus Group sends around \$60 million worth of crypto-assets to Railgun for mixing.</p> <p>On January 20, 2023, after DPRK had used Railgun, Railgun deploys new fee process to Railgun Fee Proxy V2.</p> <p>Railgun Fee Proxy V2 was initialized with around \$500,000 worth of crypto-assets (at then prices) from an Unidentified EOA.</p> <p>The Unidentified EOA itself received accrued Railgun Fees from the Railgun Treasury wallet via Railgun Sweeper 2.</p>





Fee Process Version 1

On September 10, 2022, Railgun’s initial fee process was deployed by the Railgun Deployer³ to the Railgun Fee Proxy V1,⁴ an upgradeable proxy contract.⁵

At around the same time a system-wide “pause” feature built into Railgun was employed to effect a series of upgrades.⁶

Subsequently, in November 2022, Railgun deployed a series of upgrades and as part of this upgrade process, on November 24, 2022, Railgun Fees accrued to this point were claimed by the address Railgun Team EOA.⁷ The Railgun Team EOA then sent these fees back to the Railgun Treasury on the same day.

Already at this point the Railgun team is using EOAs rather than any automated processes to manage system fees during software upgrades.

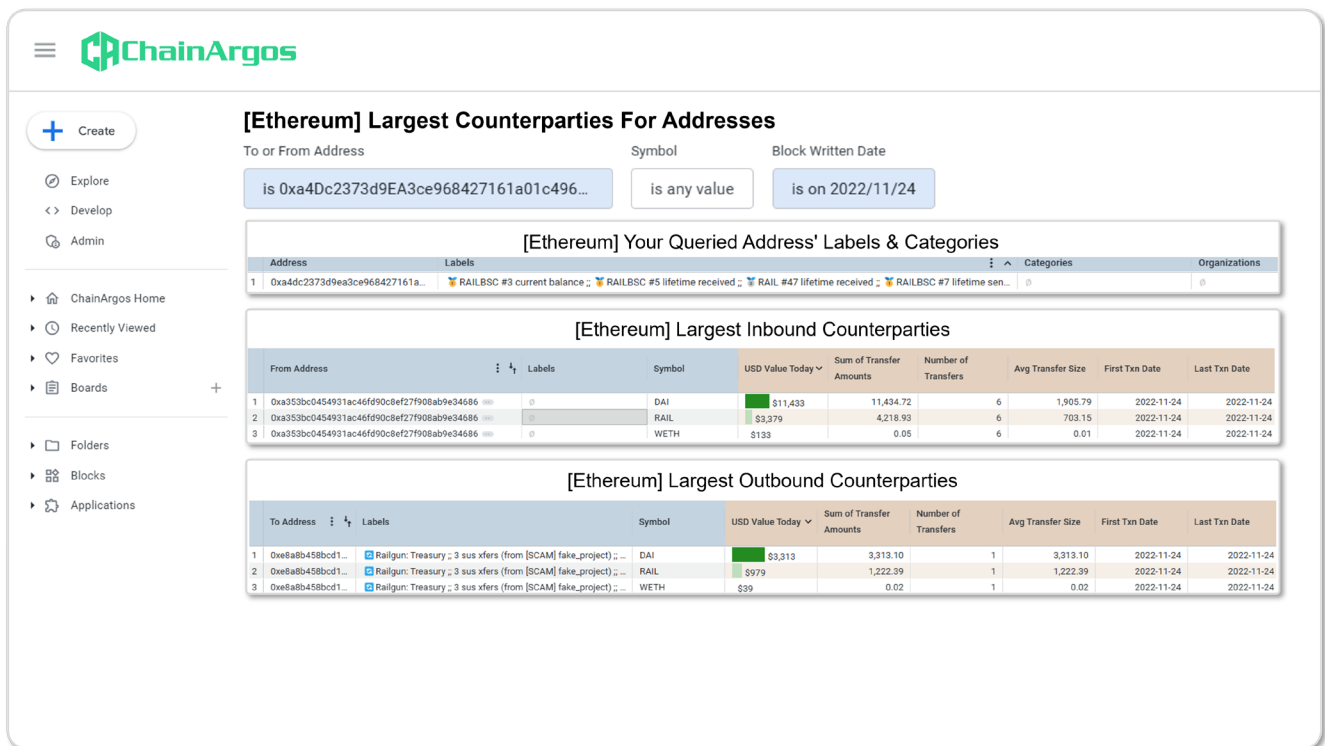


Figure 1. Largest Counterparties for Address analysis for Railgun Team EOA on November 24, 2022.

The Railgun Team EOA has been identified as associated with the Railgun Team because it received 2 million RAIL tokens during the initial distribution of RAIL tokens in July 2021, which could only have been received by contributors and developers to the Railgun protocol.

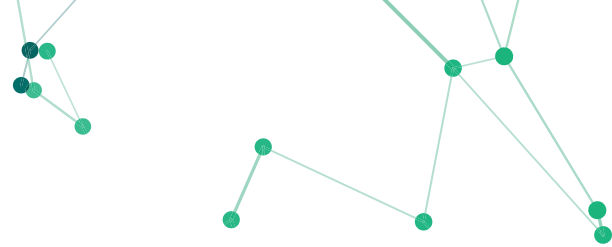
³ 0x76EB574EFF49FB64DE6f7F2854952B05B5E24624

⁴ 0xa353bc0454931ac46fd90c8ef27f908ab9e34686

⁵ 0x27d30e803a0ec079daa3a2e6c3590cca9f63c9d8 (Implementation Contract)

⁶ https://medium.com/@Railgun_Project/railgun-weekly-update-november-16-2022-railgun-2-0-d74ef08ffec

⁷ 0xa4Dc2373d9EA3ce968427161a01c4960A90B8431



Fee Process Upgrade Begins

For whatever reason Railgun chose to upgrade its Fee Process Version 1 and on December 2, 2022 the Railgun Team deployed a new smart contract using the Railgun Deployer to Railgun Sweeper 1.⁸

The Railgun Team then used Railgun Sweeper 1 to move accrued fees from Railgun Fee Proxy V1 back to the Railgun Treasury wallet. This, in some sense, “reset” the fee system so a new fee process could be deployed in its place.

Separately the Railgun Team deployed Railgun Sweeper 2⁹ and on December 5, 2022, the Railgun Treasury sent some accrued fees to Railgun Sweeper 2.

Railgun Sweeper 2 would continue to receive manually-triggered fee transfers from the Railgun Treasury throughout December 2022 and January 2023, a point we will return to later.

DPRK Use of Railgun

Between January 13th and 14th, 2023, the DPRK’s Lazarus Group sends some \$60 million worth of crypto-assets to Railgun for mixing, generating a substantially larger amount of fees for the Railgun Treasury then was typical for that period, and not repeated since.

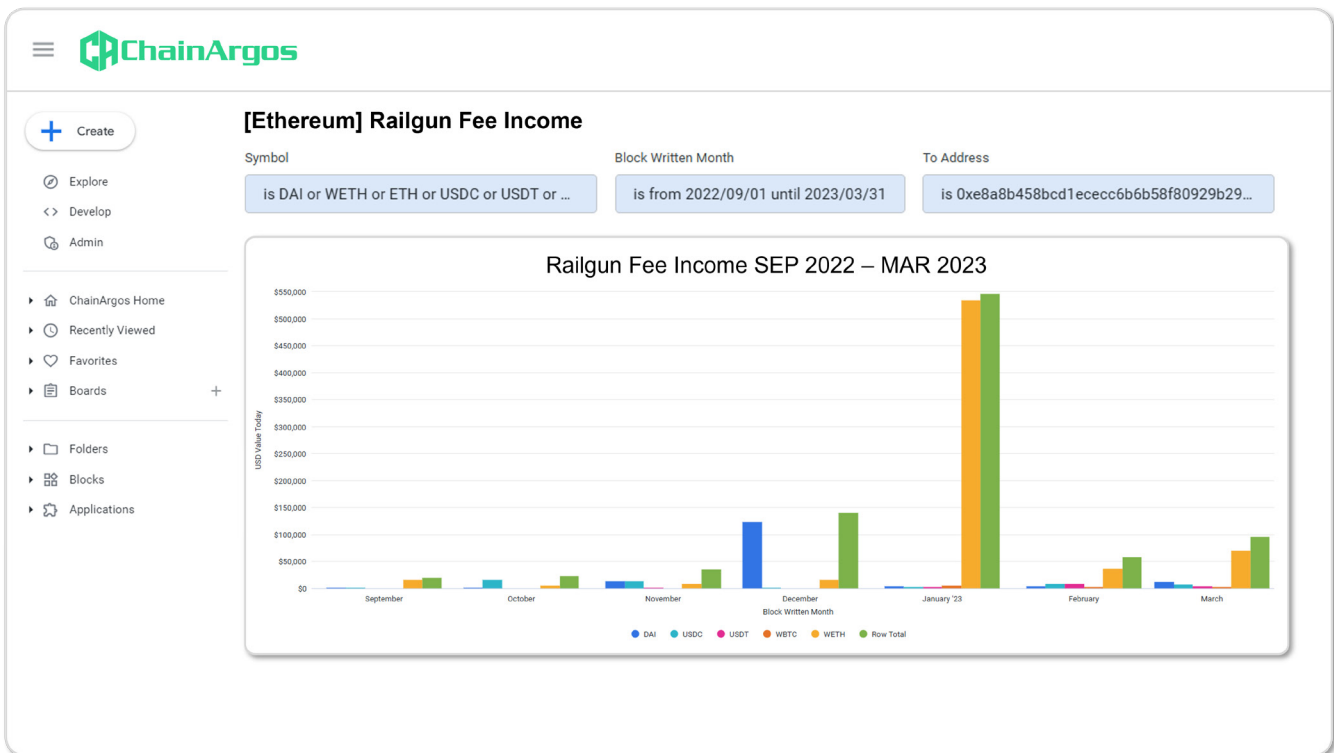


Figure 2. Railgun Fee Income between September 2022 and March 2023, with a distinct spike in fee income in January 2023, that has not been repeated since.

⁸ 0x9b1310bdcc19d172d0092240e33209a9156c8ee2

⁹ 0x2eca05b128bf5cbd5a73cc4bb625b51131ff119b

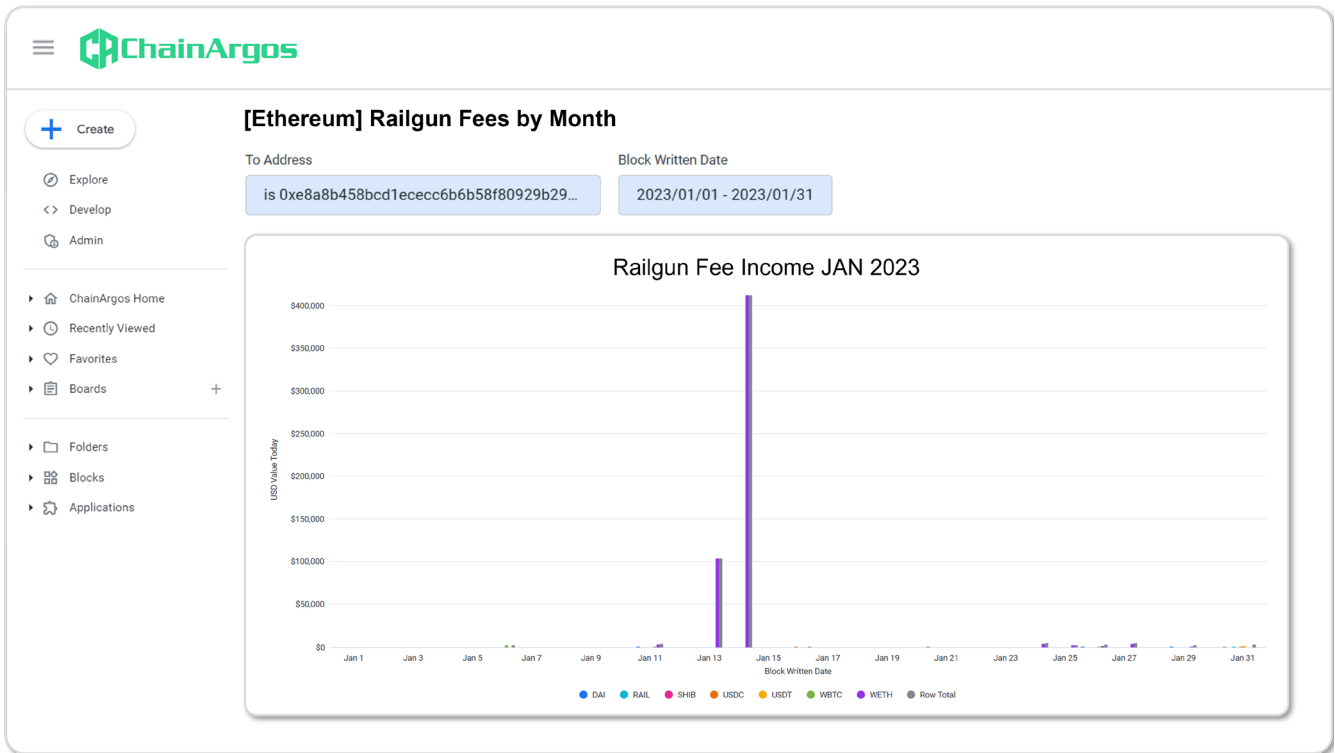
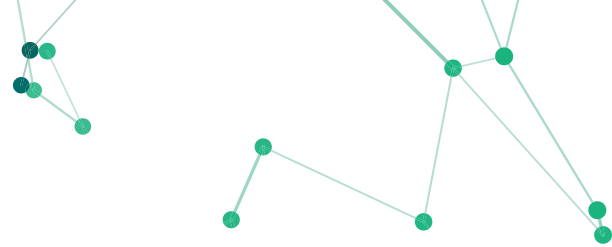


Figure 3. Railgun Fee income for the month of January, 2023 with noticeable spikes in token fees.

Between December 5, 2022 and January 18, 2023 fees from the Railgun Treasury, most of which had been generated by the DPRK’s use of Railgun, were ferried through Railgun Sweeper 2.

Fee Process Version 2

On January 20, 2023, and after the DPRK had already used Railgun, the Railgun Team deployed a new fee process to Railgun Fee Proxy V2¹⁰ an upgradeable proxy contract.¹¹

The Railgun Fee Proxy V2 was initialized with around \$500,000 worth of crypto-assets on January 20, 2023, from an Unidentified EOA¹² via three transactions.

The Unidentified EOA itself had received accrued Railgun Fees from the Railgun Treasury Wallet, via Railgun Sweeper 2, on January 20, 2023 - these were fees derived from the use of Railgun by the DPRK.

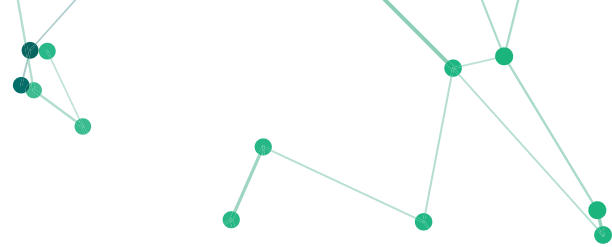
Railgun Sweeper 2 was deployed by the Railgun Team and used to relay fees since December 5, 2022.

Significantly, some \$382,660 worth of the stablecoin DAI was sent from the Unidentified EOA to the Railgun Fee Proxy V2.

¹⁰ 0xa02782ce1bf85f56f8cc7c0e66e61299ac75c86f

¹¹ 0xaF51CD5f71Ed88D6d1F65b575f1a8Ce3a78eC42b (Implementation Contract)

¹² 0xA140265ac0a55C49AD4373CDc92Bfa8baF41f459



In addition, the Unidentified EOA was itself initially funded by the crypto-asset exchange SideShift, which does not require users to provide any identify verification. This strongly suggests that whoever was operating the Unidentified EOA did not want to be associated with these series of transfers, given their connection with the DPRK.

The use of the Unidentified EOA and Railgun Sweeper 2 were integral to Railgun's fee upgrade process because this allowed the Railgun Team to move historically accrued fees from the old version of the fee system to the new one.

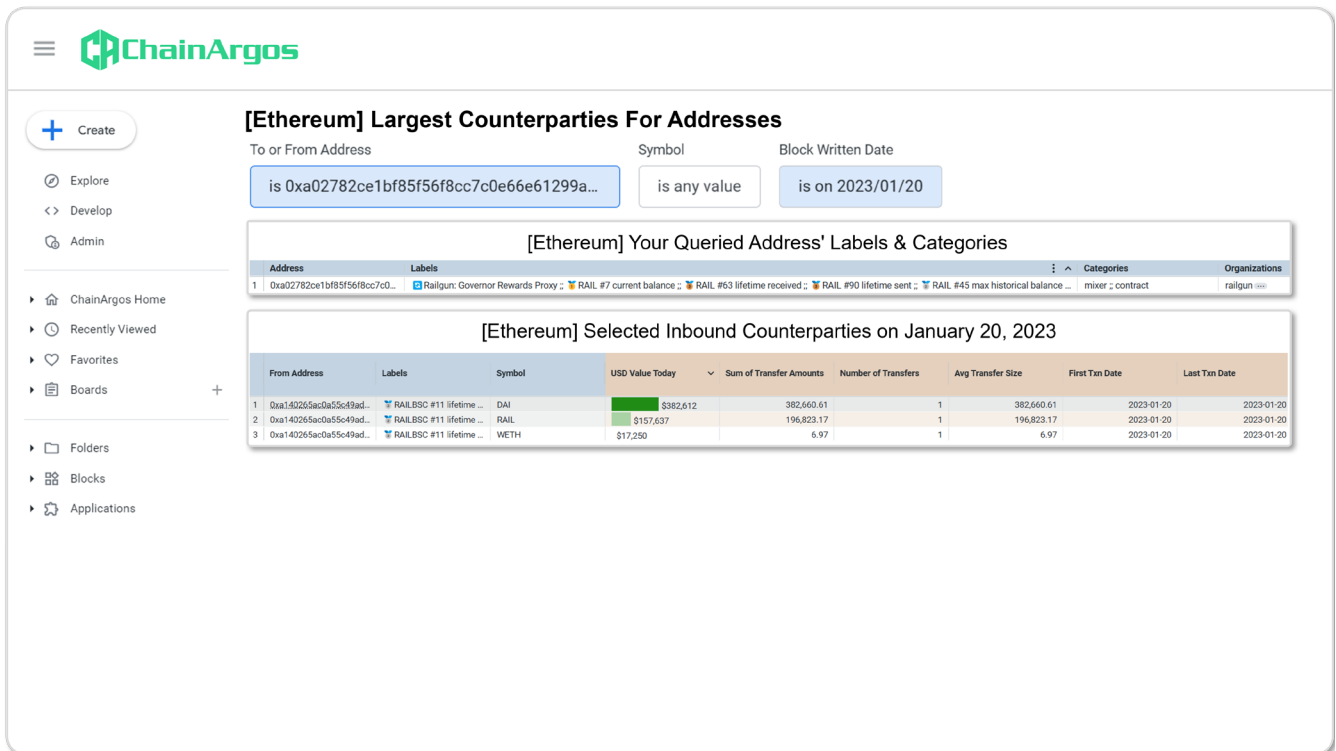


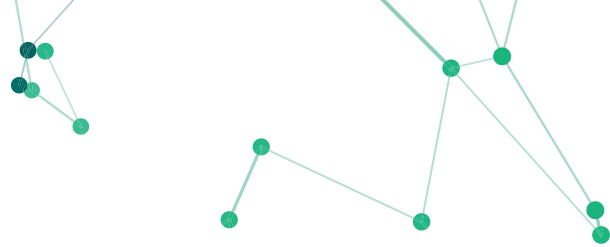
Figure 4. Railgun Fee Proxy V2 initialized by an Unidentified EOA via three transactions on January 20, 2023.

How are Railgun's fees claimed?

As with many blockchain-based protocols, fees in Railgun are “claimed” by the recipient rather than being proactively sent from the protocol. This is primarily the case because someone needs to pay transaction costs for all blockchain transactions and protocols, again generally, do not subsidize this for their users or investors.

Because sending out fees in and of itself attracts blockchain network transaction fees, Railgun apportions, segregates, and assigns fees due to investors in the protocol and beneficiaries can claim them at any time they choose.¹³

¹³ <https://github.com/Railgun-Privacy/contract/blob/612b9687eae8c94d34bf09291ec35f1d8eea1ed2/contracts/treasury/GovernorRewards.sol#L450>



Railgun fees are generated by the protocol's provision of mixing services, and investors who have "staked" Railgun tokens (locked them in the Railgun protocol to earn fees) receive a portion of such fees in proportion to the amount of Railgun tokens staked.

But instead of making these fees available for distribution constantly, Railgun transfers 2% of accumulated fees to its rewards process every 2 weeks, which means that every claim by an investor for fees necessarily includes fees from prior transactions.

Digital Currency Group ("DCG"), a U.S.-registered venture capital company that also owns the Grayscale Bitcoin Trust product, was one of the largest investors in Railgun.

DCG made its claim for its share of Railgun fees only in June 2023, almost five months after the DPRK's use of Railgun in January of that same year.

There are a variety of reasons why an investor may wait to claim fees they are due, including saving on transaction fees by allowing fees to accumulate, before claiming them in one large tranche.

It is also possible that investors who were aware of the DPRK's use of Railgun to launder funds wanted to distance themselves from fees generated through such activities.

Where do DCG's Railgun fees end up?

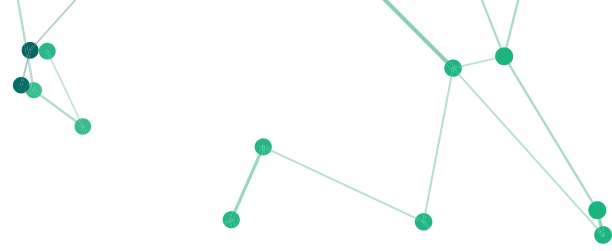
Forbes details how the address 0xFED429FB7d243380B25bC11B10561D5A27f42D8E receives DCG's share of Railgun fees.

What's interesting is that although the ETH and DAI tokens that DCG earned from Railgun's fee distribution were sent to Coinbase Prime Custody ("Coinbase"), RAIL tokens, were sent to a multi-sig wallet¹⁴ that appears linked to DCG.

It is unclear whether Coinbase performed any analysis of the source of DCG's ETH and DAI tokens, nor is it clear whether Coinbase would have rejected those tokens had it known they were fees derived from the DPRK's use of Railgun to launder funds.

Regardless, the ETH and DAI tokens that were generated from the DPRK's use of Railgun are, given the fee structure of Railgun, directly linked to the DPRK and eventually entered Coinbase's custody.

¹⁴ 0x6b3B9EC869F8fAb3C21b15b8E8663Dfa2941F2d0



Did DCG participate in “management”?

Unlike a corporation, Railgun, similar to many other so-called decentralized protocols, operates through a decentralized autonomous organization (“DAO”) which allows holders of Railgun’s RAIL token to vote on various proposals.

At the time this case study was prepared, DCG actively voted on two Railgun DAO proposals, both of which passed.

It is unclear if DCG’s voting in these proposals is sufficient to constitute “management” in the traditional sense, especially given Railgun has an identifiable team that also appears involved in parts of the protocol’s operation.

DAOs are a relatively new legal construct and there is limited precedent to go on at the present time.

Voting on proposals is not the same as management, but given that many DAOs hold themselves out as not having a centralized management team, an argument could be made that voters in the DAO are therefore acting as de facto managers in a common enterprise.

Could this have been prevented?

In May 2023, Railgun partnered with Chainway Labs to create Railgun’s Private Proofs of Innocence (“PPI”) to prevent the automated portions of Railgun’s system from accepting funds from OFAC-blacklisted addresses and other questionable sources.¹⁵

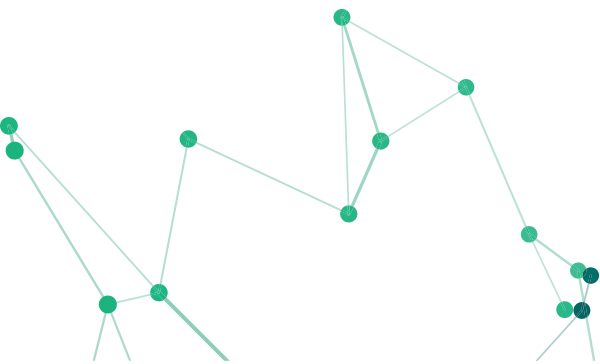
Software code for Railgun’s PPI appears in Railgun’s public code repository only from November 2023, well after the DPRK had used Railgun’s services.

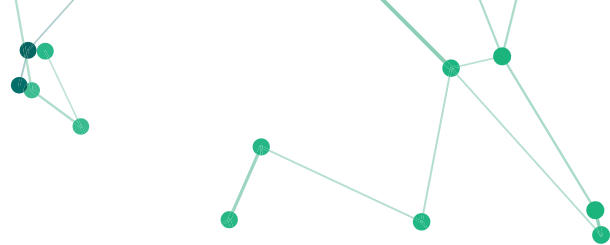
As all of the activities discussed here predate the introduction of PPI by months at the very least, Railgun’s PPI process could not possibly have stopped these DPRK flows.

Furthermore, PPI applies only to the automated portions of Railgun’s fee system, but as demonstrated by the various fee upgrades, fees accumulated prior to upgrades were routinely transferred manually to EOAs outside the supervision of Railgun’s PPI.

EOAs are not automated or constrained in any way. Whoever holds the keys can effect any transactions they wish.

¹⁵ <https://github.com/Railgun-Community/private-proof-of-innocence>





The PPI system requires Railgun users to provide cryptographic proof that their crypto-assets do not originate from sanctioned wallets. The thinking is that legitimate users of Railgun would provide such proofs whereas illicit users are unlikely to do so.

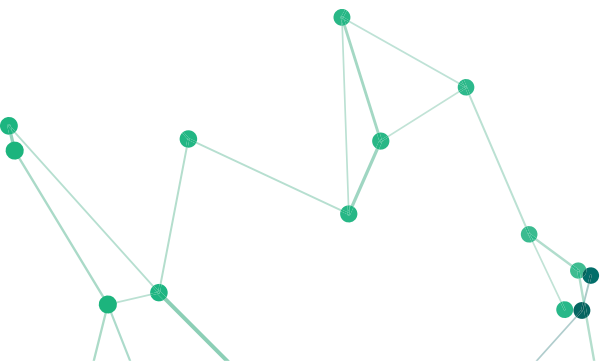
But given how bad actors can easily spin up fresh unsanctioned wallet address, and add layers of transactions between the illicit activity and the wallet address which eventually uses Railgun's services, it appears there may be trivial methods to overcome PPI.

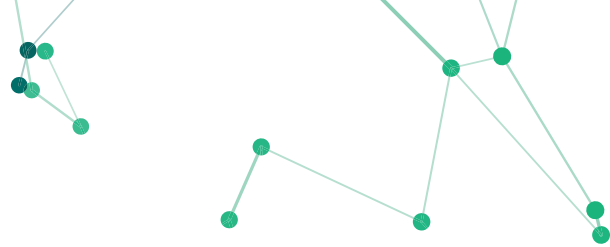
Prior to the DPRK's use of Railgun, the so-called privacy protocol was also not a very active obfuscation platform. This is reflected in the fees generated from the provision of its mixing services.

The sudden spike in inflows to Railgun in January 2023 should have drawn attention from the Railgun Team, especially given it was a significant change in flows.

Instead, the Railgun Team elected to deny the DPRK had used their services,¹⁶ and opted to handle the fees generated from the DPRK's use of Railgun in manually-controlled EOAs over the course of their various upgrades to the Railgun fee system.

¹⁶ <https://cointelegraph.com/news/railgun-denies-north-korea-links-nears-1b-volume>





Appendix.

Externally Ownend Account (EOA)

An Externally Owned Account is a blockchain address where control of the address sits entirely with a private key stored off-chain. Think of the private key as a password and whoever has the password controls the account.

The canonical example of such an address is an Ethereum address that is not a smart contract, it is just an address secured by the private keys which sit entirely outside the blockchain system.

Proxy Contract

A proxy contract is a type of smart contract that acts as an intermediary smart contract that delegates calls to another smart contract known as the “implementation contract”.

In cases where a proxy contract is used, interaction with the underlying implementation contract should be done through the proxy contract. The most common flow is:

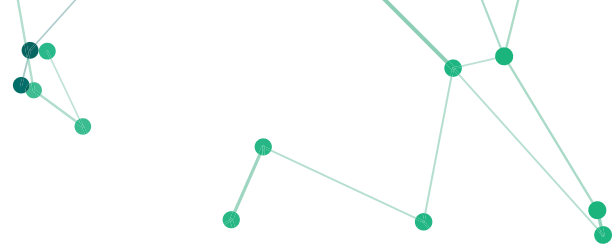
1. The user initiates a function call to the Proxy Smart Contract.
2. The Proxy Smart Contract redirects the function call to the Implementation Contract.
3. The Implementation Contract executes the intended smart contract code for the function the user originally requested.
4. The return is then fed back from the Implementation Contract through the Proxy Contract and back to the User.

A proxy contract is considered “not upgradeable” when there is no facility to change the underlying implementation control’s address. For upgradeable contracts, ownership is considered to be renounced when it is changed to the null address.

Implementation Contract

The smart contract that executes the function or program desired behind a proxy. The implementation contract is the “executor” which powers the smart contract operation and performs whatever actions the smart contract was designed to perform.

For upgradeable proxy contracts the implementation contract address can be changed. For these contracts the overall functionality may change in unexpected ways if proxy contract redirects to a different or unexpected implementation contract.



Upgradeable Proxy Contract

Indirection is an established and fundamental tool used in building software.

In computer programming, indirection (also known as “dereferencing”) is the ability to reference something using a name, reference, or container, instead of the value itself. The most common form of indirection is the act of manipulating a value through its memory address. One example of indirection is the domain name system, which enables names such as “en.wikipedia.org” to be used in place of network address such as “208.80.154.224.”

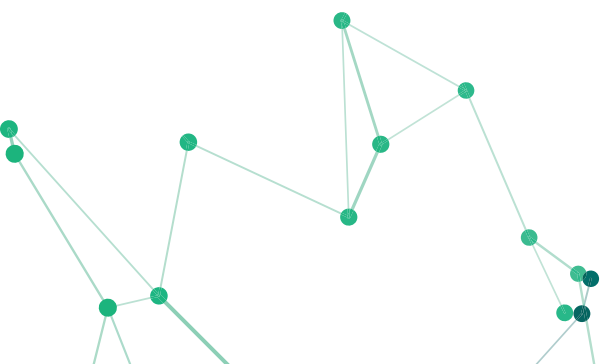
The Ethereum blockchain network and proxy contracts both use indirection, to facilitate building software on the Ethereum blockchain network.

A proxy contract is a type of smart contract that acts as an intermediary smart contract that delegates calls to another smart contract known as the “implementation contract”. In cases where a proxy contract is used, interaction with the underlying implementation contract must be done through the proxy contract.

The proxy contract stores the address of the implementation contract so when a user interacts with the proxy contract, the proxy contract delegates the call to the implementation contract, which then executes the requested function and returns the result to the proxy contract, which in turn, returns the result to the user.

Some of the benefits of using proxy contracts include the ability:

1. to upgrade the implementation contract without changing the proxy contract blockchain address, which allows rollback to previous versions of implementation contracts, and implementation contract upgrades could be executed without users having to change the smart contract blockchain address they intend to interact with, because the proxy contract would still have the same blockchain address; and
2. to deploy a new implementation contract which uses less gas instead of deploying an entirely new implementation contract, minimizing the need to update references to the implementation contract’s blockchain address in decentralized applications.



Who are we?

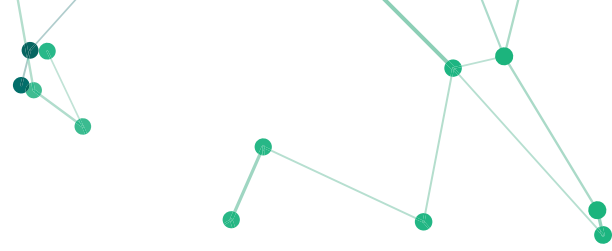
ChainArgos is the blockchain intelligence firm best known for uncovering crypto-asset exchange Binance's \$1.4bn BUSD stablecoin undercollateralization, forcing the New York Department of Financial Services to take action.

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:

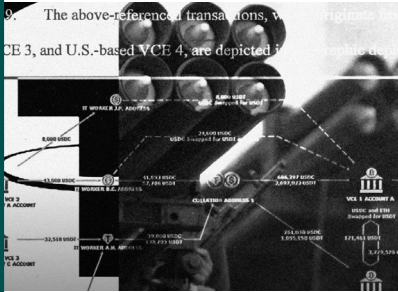
Bloomberg



Stablecoin Operator Moves \$1 Billion in Reserves to Bahamas

- Move reflects worsening US banking conditions for crypto firms
- TrueUSD's circulation has more than doubled in the last month

THE WALL STREET JOURNAL.



From Hamas to North Korean Nukes, Cryptocurrency Tether Keeps Showing Up

Tether has allegedly been used by Hamas, drug dealers, North Korea and sanctioned Russians

South China Morning Post



How crypto investigators uncover scammers' blockchain billions, scale of money laundering in Asia

THE WALL STREET JOURNAL.



The Shadow Dollar That's Fueling the Financial Underworld


Cryptocurrency Tether enables a parallel economy that operates beyond the reach of U.S. law enforcement

THOMSON REUTERS®



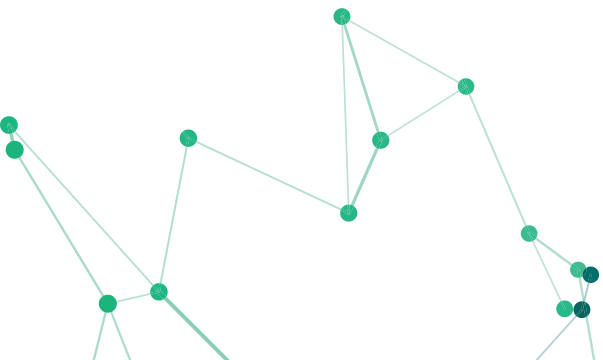
SPECIAL REPORT: Russian-owned, UK FCA-authorized payment firms show financial crime red flags; mule accounts for sale on dark web

Bloomberg



Binance Acknowledges Past Flaws in Maintaining Stablecoin Backing

- Blockchain analyst Reiter had flagged gaps in Binance-peg BUSD
- Binance says earlier 'operational delays' have now been fixed



Who uses blockchain intelligence?



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

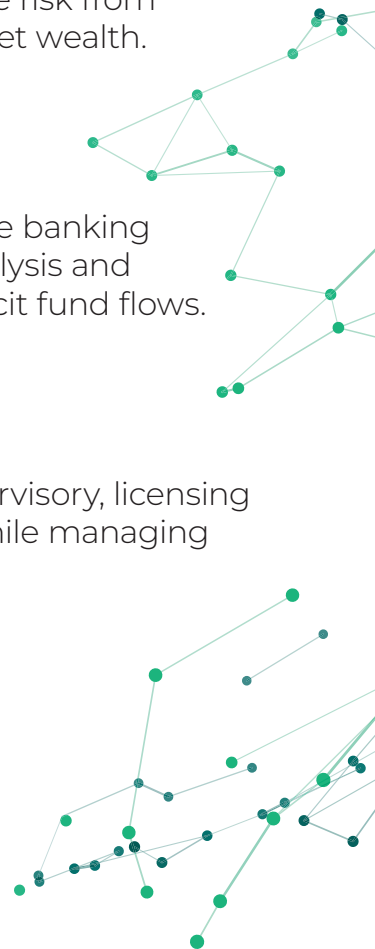
Fight money laundering, expand know-your-customer tools, and combat the financing of terrorism while expanding your customer base. Manage risk from customer crypto-assets and confidently verify sources of crypto-asset wealth.

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

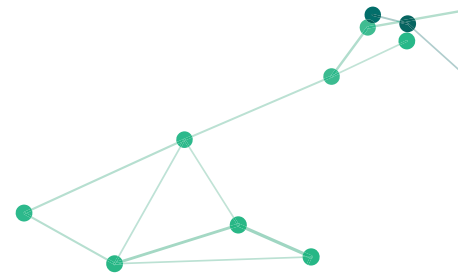
ChainArgos runs its own blockchain nodes, and we never enrich our data with yours, so you can be sure of data integrity.

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.

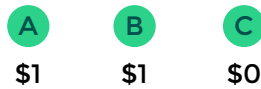


Fig. 1

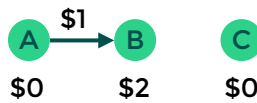


Fig. 2

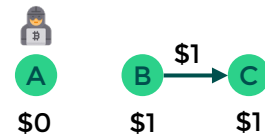


Fig. 3

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.

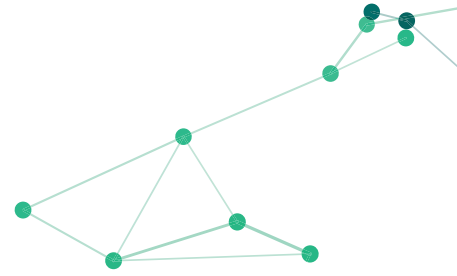
Instead of passing off "risk scores" as "risk management" ChainArgos helps you follow the money.

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.



Better attribution.

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

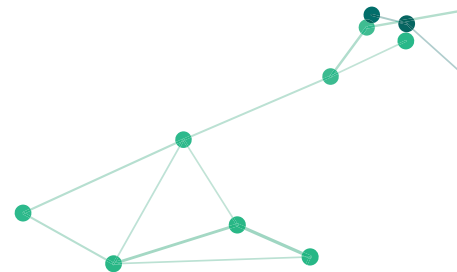
ChainArgos is the only blockchain intelligence firm that delivers programmatic address labels and wallet tags that are unassailable whether you're making business decisions or preparing to sue someone.

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.





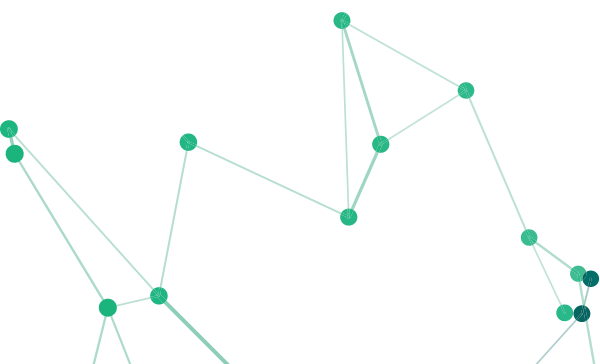
Legal Disclaimers.

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.





© 2024 ChainArgos Pte. Ltd. All rights reserved.