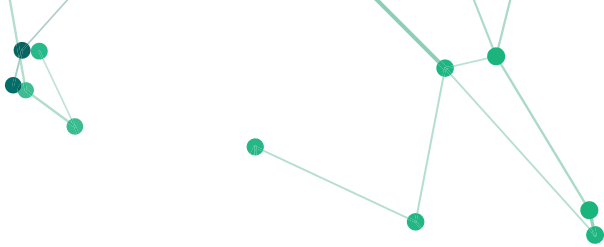




Can't Seize or Won't Seize? Circle's Criminal Charges vs Its Own USDC Code

HOW CIRCLE'S OWN CODE AND DOCUMENTATION
CONTRADICT ITS CLAIM THAT IT CANNOT SEIZE USDC

AUGUST 3, 2026



Contents.

Case Study	Executive Summary	3
	1. Why This Should Matter to You	4
	2. What Circle Claims	
	3. On-Chain Evidence That Circle Is Wrong	6
	4. Past Upgrades	7
	5. What Can an Upgrade Do?	10
	6. What Could Be Happening?	11
	7. What This Means for You	12

About Us	Who are we?	13
	Featured Press	14
	Who is this for?	15
	How are we different?	16
	How do we do it?	17
	Better Attribution.	18

Executive Summary

Circle Internet Group, Inc. (“Circle”) issues USD Coin (“USDC”), a dollar-denominated stablecoin that purports to maintain a 1:1 peg with the US dollar. Circle is listed on the New York Stock Exchange under the ticker CRCL. Circle is facing criminal charges in Wisconsin relating to its failure to seize certain USDC. Jonathan Reiter examined this matter in an opinion piece written for Blockhead¹ and the International Consortium of Investigative Journalists² (“ICIJ”) has covered the issue. In summary, in 2025 Wisconsin law enforcement requested that Circle freeze and seize certain USDC. Circle has not effected seizure, maintaining that it is unable to do so. Law enforcement has escalated the dispute by charging Circle criminally. That step suggests it does not credit Circle’s position.

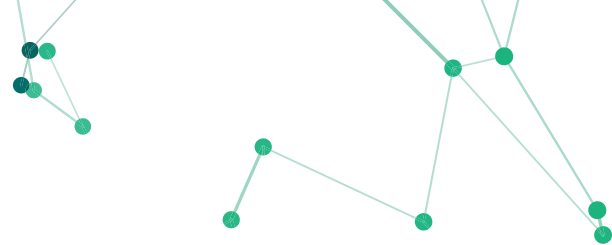
Further detail is available in the two articles linked above. There has been considerable exchange between the parties and Circle has committed to the position that it cannot effect seizure. The central argument of the Reiter opinion piece was that while Circle cannot effect seizure with USDC’s code as currently deployed, Circle can modify USDC’s code to make seizure possible. An issuer able to make arbitrary code changes is able to add a seizure function. Circle’s claim that it cannot seize is therefore misleading. A known remediation path exists and is available to Circle.

We analyze this in detail below. As a listed company, Circle has obligations to be truthful with the public. On the record as it stands, Circle appears to be making false or misleading statements either about how its own flagship product works or to the Wisconsin court. Either alternative might plausibly constitute securities fraud, not in the expansive sense where “everything is securities fraud”³, but in the narrow and serious sense that attaches to false written statements made to a court.

¹ <https://www.blockhead.co/2026/07/24/circles-claimed-impotence-usdc/>

² <https://www.icij.org/investigations/coin-laundry/crypto-giant-circle-rebuffed-efforts-to-help-scam-victims-police-say/>

³ <https://www.bloomberg.com/opinion/articles/2019-06-26/everything-everywhere-is-securities-fraud>



1. Why This Should Matter to You

If you hold, trade, accept, or supervise USDC, the token in your wallet is governed by code its issuer can change at will. Circle has told a Wisconsin court that it cannot seize USDC held in wallets it does not control. Circle's own code and documentation, quoted throughout this case study, say the opposite. One of those two positions is wrong, and whichever one it is, the consequences reach well beyond a single criminal case.

If you are an investor in Circle, a company listed on the New York Stock Exchange, the stakes are direct. A listed company that makes false statements to a court, or that maintains inaccurate public documentation about its flagship product for years, faces plausible securities fraud exposure. Investors who suffered losses during the relevant period may hold claims for damages.

If you are a victim of fraud, or an investigator working to recover stolen USDC, this dispute defines what a court order is worth. Wisconsin law enforcement obtained an order directing seizure of USDC and the USDC has not moved. If an issuer's claimed technical limits can defeat a lawful seizure order, every future recovery effort inherits that problem.

If you are a compliance officer, a bank, or an institution that relies on stablecoin issuers' representations, this case is a test of whether those representations survive contact with the issuer's own code. The evidence needed to check them is public. This case study shows how to read it.

2. What Circle Claims

The linked articles provide further detail. The following excerpts make Circle's position sufficiently clear. The first is a statement from Circle:

Beyond the ability to blocklist wallets, however, Circle has no control of USDC held in third-party wallets and has no ability to invalidate and reissue such USDC or to transfer them.



The second is drawn from law enforcement's account:

Circle also communicated to Detective Kuchta that (1) the address was not held at Circle; (2) Circle did not have the private keys for the address; (3) Circle could not, therefore, transfer USDC from the wallet; and (4) to recover the USDC for the victim law enforcement would need to locate the private keys for the address.

The filings contain further commentary, but the excerpts above are sufficient to understand the impasse. We nonetheless encourage readers to review the filings in full. Circle presents itself there as an aggrieved party while advancing claims that, as set out below, are difficult to reconcile with the public record.

The substance of Circle's claim is that it can freeze USDC but cannot move USDC held in wallets it does not directly control. There is a court order directing Circle to seize the USDC. Circle has no objection to freezing USDC but seizure requires moving USDC from a blockchain address identified by law enforcement to one controlled by law enforcement. Circle asserts that it lacks the technical capability to do so.

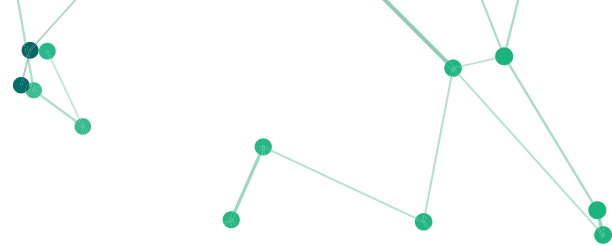
Notably, Circle's S-1⁴ includes the following text:

Payment stablecoins issued by a foreign issuer cannot be traded on U.S. custodial trading platforms unless the foreign payment stablecoin issuer satisfies a safe harbor to be established by the Treasury Secretary or the issuer: (i) complies with lawful orders to seize, freeze, burn or prevent the transfer of outstanding stablecoins;

This text concerns foreign issuers and the then-proposed GENIUS Act. A later version of that proposed act was subsequently passed. It is difficult to believe anyone at Circle or elsewhere believed, or believes, that only non-US issuers were expected to "compl[y] with lawful orders to seize...stablecoins."

⁴ <https://www.sec.gov/Archives/edgar/data/1876042/000119312525178989/d839239ds1.htm>





3. On-Chain Evidence That Circle Is Wrong

The Reiter opinion piece included the following:

If we read the claims in the dispute broadly: Circle is not being candid. If we read the claims narrowly: Circle is not being honest. Unless Circle has somehow lost the ability to upgrade USDC – which would be a far larger problem if kept hidden for so long – we just cannot see a way they are telling the truth here. Maybe there is one but there is certainly no hint of such an explanation in the court filings to date.

The ICIJ reporting includes references to, and quotes from, a number of experts who question Circle's claimed inability to comply. Below we set out the technical evidence that Circle is wrong.

USDC's smart contract token code on the Ethereum blockchain resides at 0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48. This is confirmed by Circle's own documentation⁵ and the contract is tagged on Etherscan⁶ among many other places. Circle uses this blockchain address in its own examples.⁷ This is the relevant contract. USDC is whatever the code at this blockchain address says it is.

This is a proxy contract. That can be confirmed by inspecting the code on Etherscan⁸ or by reading Circle's own MiCA-mandated Whitepaper,⁹ which states in part:

USDC is deployed using upgradeable smart contract architectures via the proxy patterns of the Universal Upgradeable Proxy Standard (UUPS) – introduced via ERC-1822 – on Arbitrum, Avalanche, Base, Celo, Ethereum, HyperEVM, Ink, Optimism, Plume, Polygon, Sei, Sonic, XDC and ZKsync, and more generally, on all EVM chains. These implementations allow the contract logic to be modified without changing the token address.

Circle's technical documentation and code, available on GitHub, are consistent and provide more detail.¹⁰ There is no serious question as to which blockchain addresses, contracts, and lines of code are relevant here.

Circle's own documentation states that the token is "upgradeable", which settles the question. The code supports, among other things, upgrades that are executed by an administrator. The code also provides a mechanism for changing the administrator. And every one of these actions is observable on-chain. Whoever holds the administrator role can "allow the contract logic to be modified" without restriction.

⁵ <https://developers.circle.com/contracts/erc-20-token>

⁶ <https://etherscan.io/address/0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48>

⁷ <https://developers.circle.com/api-reference/wallets/user-controlled-wallets/create-transaction-estimate-fee>

⁸ <https://etherscan.io/address/0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48#code>

⁹ <https://www.circle.com/legal/mica-usdc-whitepaper>

¹⁰ <https://github.com/circlefin/stablecoin-evm/blob/master/doc/tokendesign.md>

We explore the extent of this power, and Circle's acknowledgement that new functionality can be added, below. The current administrator can also pass administrative control to a different blockchain address. We turn now to the on-chain data.

4. Past Upgrades

USDC on Ethereum has been upgraded three times:

Block	Tx Hash	Implementation
10743414	0xe6f0f754398d89583da8e4229c5d7aaa00739a3ae334ecfc2839ac396b4836e3	0xb7277a6e95992041568d9391d09d0122023778a2
12317814	0xe2e40640ffd5f76538cd23660cf56f00bfebd5fe925ebad6b8067c4cee18a2c3	0xa2327a938febf5fec13bacfb16ae10ecbc4cbdcf
18963716	0xae3ad89e569f27d47a8a02999a6d937c12aaa6bc50e66650e7cbd3244bde9951	0x43506849d7c04f9138d1a2050bbf3a0c054402dd

Each of these transactions can be verified using any public block explorer. The most recent upgrade was in early 2024. USDC is not only upgradeable. It has been repeatedly upgraded. The power is not theoretical.¹¹

The administrator of USDC has changed eight times:

Block	Tx Hash	Admin
6082473	0xf73f2dd1e79552c5e13e92b16ed0a3a59b9e28fd134d6759a4e8cfbf3385a3c6	0x69005ff70072c57547dc44ea975d85ea60e5b196
6278324	0xda436c8e42f88e4c9478b03ff525dfba7035be7d894bf91ca5321bf3c360f7d9	0x807a96288a1a408dbc13de2b1d087d10356395d2
10743406	0x621f3c01567c619197df60b25e083f393d22b9a6c7718b45a279d8ab77d8620d	0xed24bd79a3f2ba4325e9c553164e299c65e272fc
10743414	0xe6f0f754398d89583da8e4229c5d7aaa00739a3ae334ecfc2839ac396b4836e3	0x807a96288a1a408dbc13de2b1d087d10356395d2
12317806	0x5c5ffdeab45e37fdb2112c5e09a2e361d59faa3eed9e0584fe3ad50de5bfeaca	0xd13689e8da0ed95b55100e27b7dbc95c03b5259b
12317814	0xe2e40640ffd5f76538cd23660cf56f00bfebd5fe925ebad6b8067c4cee18a2c3	0x807a96288a1a408dbc13de2b1d087d10356395d2
18963710	0x4441f5f0d30b59f9db3083034605e5cfb35e3606a30e12f075feef3b1df81a15	0x9999fa87f5a1d1c64e7c709838b92006ab0cc1ad
18963716	0xae3ad89e569f27d47a8a02999a6d937c12aaa6bc50e66650e7cbd3244bde9951	0x807a96288a1a408dbc13de2b1d087d10356395d2

¹¹ Were the power purely theoretical, our conclusion that Circle is making false statements to someone would be unchanged. We have observed, however, that many legal practitioners in the digital asset industry decline to engage with theoretical issues until those issues materialize, typically in the form of a hack or a theft.

Again, all of this can be verified using any block explorer. The administrator before the first change was 0x95ba4cf87d6723ad9c0db21737d862be80e93911. That blockchain address originally deployed USDC and is therefore Circle-controlled. This can be established from, among other sources, the deployment transaction or the first upgrade event's previousAdmin field. None of this information is hidden, abstract, or open to interpretation.

In total there are six distinct administrator blockchain addresses over the life of USDC so far:

Admin	Type
0x95ba4cf87d6723ad9c0db21737d862be80e93911	EOA, deployer
0x69005ff70072c57547dc44ea975d85ea60e5b196	EOA
0x807a96288a1a408dbc13de2b1d087d10356395d2	EOA, current admin
0xed24bd79a3f2ba4325e9c553164e299c65e272fc	Upgrader contract
0xd13689e8da0ed95b55100e27b7dbc95c03b5259b	Upgrader contract
0x9999fa87f5a1d1c64e7c709838b92006ab0cc1ad	Upgrader contract

Some of these are simple EOAs¹² while others are smart contracts. Circle clearly controlled all of them, at least at some point. For the smart contracts one might examine whether control has since been relinquished, or analyze the code directly. However, the pattern of upgrades and administrator changes above makes the arrangement clear. Control is passed to a contract to effect upgrades, and the upgrade process quickly passes control back to the same EOA.

A review of the block numbers of the upgrades and administrator changes shows a pair of administrator changes only a few blocks apart, in which the administrator changes from EOA to smart contract and then back. And the “back” step occurs alongside an implementation upgrade. The blockchain addresses we describe as “upgrader contracts” are part of Circle’s software maintenance process.

This has been the pattern for years. Each upgrader contract is new, but control reverts to the same place, the current administrator, every time. This is confirmed by analysis of the upgrader contracts and of the upgrade process documentation below.

¹² Externally Owned Account (EOA) is the term used to describe blockchain addresses controlled off-chain by private keys. In colloquial terms this means nothing is automated and a person controls the address manually via an internet-connected computer.

Circle plainly held the private keys for the current administrator blockchain address for years. It is conceivable that Circle has since lost those private keys. The undisclosed loss of the administrator private keys to a listed company's flagship product would itself be a serious matter. We set that possibility aside here and return to it in the final section. As discussed there, that scenario is likely the worse one for Circle.

Inspecting the upgrader contracts confirms the “control reverts to the same EOA” pattern described above. The public code for the most recent upgrade, published under a Circle copyright notice, includes the following explanation of what the code does:

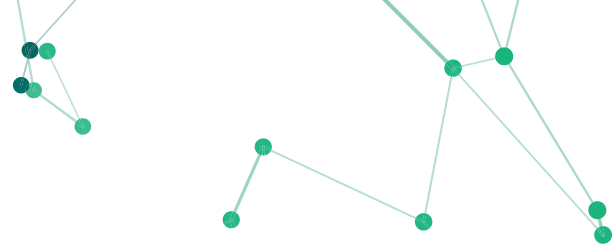
```
/**
 * @title V2.2 Upgrader
 * @notice Performs FiatToken v2.2 upgrade, and runs a basic sanity test in a single
 * atomic transaction, rolling back if any issues are found. By performing the
 * upgrade atomically, it ensures that there is no disruption of service if the
 * upgrade is not successful for some unforeseen circumstances.
 * @dev Read doc/v2.2_upgrade.md
 */
```

This is consistent with the entire upgrade process as documented in publicly-visible files in Circle's GitHub.¹³ Generic upgrade documentation is also provided by Circle¹⁴ which states that, assuming all the tests pass and the upgrade goes as expected, a human administrator should “Verify that the proxy admin role is transferred back to the Admin Key.”

Circle has, in effect, held continuous control via the current administrator EOA for years. The administrator changes to upgrader contracts were operational details of the upgrades. Each step was designed either to complete the upgrade and transfer administrative control back to Circle or, in case of failure, to revert everything and transfer administrative control back to Circle. Circle never relinquished control.

¹³ https://github.com/circlefin/stablecoin-evm/blob/master/doc/v2.2_upgrade.md

¹⁴ <https://github.com/circlefin/stablecoin-evm/blob/master/doc/upgrade.md>



5. What Can an Upgrade Do?

The technical documentation is clear as to what can be upgraded. It is unnecessary to work through the code to demonstrate that Circle can add arbitrary functionality. The documentation states the following:

An upgraded token can have:

1. New logic (functions)
2. New state variables (data)
3. New logic and new state variables
4. Renamed state variables
5. Updated logic for existing functions
6. Each situation is addressed in a section below.

Further, the documentation explicitly addresses the addition of new functions:

All that remains is to add the new logic (functions) as part of the body (denoted by ... in the code above) of the contract. Note that private functions will not be inherited in subsequent contract versions and should be added with care.

These are all public statements by Circle that have been publicly available for many quarters.

Readers familiar with Solidity can verify the precise mechanics. All the relevant code is linked in the footnotes to this document. In practice, the upgrade documentation makes the point more efficiently than the code itself, but we encourage readers to verify both.

We note also that allowing code upgrades while restricting what functionality those upgrades can affect is far harder to engineer than allowing arbitrary changes. Had Circle wished to limit what could be changed, a large amount of additional machinery would have been required. Such limits could also introduce future compliance problems,¹⁵ including the possibility that the upgrade powers prove inadequate to satisfy a court order. Circle imposed no such restrictions, yet now represents to the court that it is unable to comply.

¹⁵ <https://www.nature.com/articles/s41598-024-84612-9>





6. What Could Be Happening?

Unless Circle lost the private keys to the current administrator EOA, we cannot see how Circle is telling the Wisconsin court the truth. If Circle has lost the keys or has otherwise lost the power to upgrade these contracts, then all of the public documentation linked and quoted above is wrong. Either situation is serious for a public company. Circle appears caught between the two.

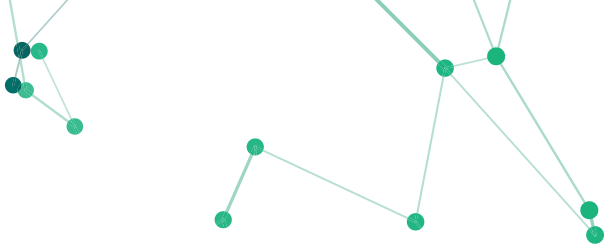
The Wisconsin charges may well be the lesser exposure compared with a large, heavily traded public company maintaining inaccurate documentation for its flagship product in public view for many quarters. Not only might this plausibly constitute securities fraud, but investors who purchased Circle stock and suffered losses during the period the documentation was inaccurate might have claims for damages. Given that Circle's stock has declined more or less continuously since its listing approximately a year ago, that group is likely large.

For context, this is not the only matter of which we are aware in which Circle's own code and documentation, paired with on-chain evidence, contradict Circle's public statements. We expect the problems discussed in this document stem from an inadequate understanding of how Circle's own products work, and of how Circle's own employees have communicated how those products work, within or adjacent to the legal team. We find it unsurprising that inaccurate statements made their way into court documents. We hold documented evidence of discrepancies in other areas consistent with the same inadequate understanding in Circle's legal and compliance functions.

Recall the excerpt above from Circle's S-1. We concede it is theoretically possible that Circle's legal team holds the incorrect belief that Circle is unable to seize USDC and that Circle's legal team believes in good faith that regulated US stablecoin issuers are permitted to issue products where they knowingly cannot effect seizure. It is also possible, again referencing Circle's S-1 as quoted above, that Circle's legal team believes it "satisfies a safe harbor [] established by the Treasury Secretary" following the passage of the GENIUS Act. We can find no public references to any Treasury statements that US stablecoin issuers can issue products which are knowingly and intentionally designed in such a way as to frustrate US court orders. We nonetheless concede such a document may exist. Whether such a document would hold any value in court is a question we will leave to others.¹⁶

¹⁶ Presumably the executive branch cannot empower anyone to defy the judicial branch any more than it can pardon future crimes. This is not a legal study but "It is emphatically the duty of the Judicial Department to say what the law is" (*Marbury v Madison*, 5 US 137, 1803) is perhaps the most settled principle of constitutional law in the US.





In any event, Circle *can* seize USDC. At best, the legal team holds mistaken “good faith” beliefs in this area because it was misinformed by the engineering team. In such a scenario, liability for fraud might not rest with Circle the company but rather with individual employees of Circle. We expect civil liability for the inaccurate statements would still fall on the company. In either case the company is the more likely target of litigation because it has greater resources than the engineers.

Circle therefore faces two alternatives, either of which might plausibly constitute securities fraud, and either of which concerns a substantial population of investors with losses. Either Circle’s statements in the Wisconsin court papers are false, or Circle has maintained inaccurate documentation about its core product for years. No third alternative is apparent.

7. What This Means for You

If you hold or accept USDC. Treat an issuer's statements about what it can and cannot do as claims to verify rather than facts to accept. The controlling fact is the deployed code, and the deployed code is public. When an issuer's representations and its own code disagree, the code is the better guide to what can actually happen to the USDC you hold.

If you rely on stablecoin issuers for compliance or risk. An issuer's representations about its technical capabilities can be tested against its deployed contracts and published documentation before you rely on them. This case shows the test requires only public tools, a block explorer and the issuer's own GitHub repositories. A representation that fails that test should not enter your risk model.

If you are pursuing recovery of stolen USDC. The on-chain record of the administrator role, the upgrade history, and the pattern of control is public and verifiable. Nothing in the deployed code prevents the issuer from complying with a seizure order. Parties seeking recovery can put that record before a court, as Wisconsin law enforcement has now done.

If you supervise, regulate, or study this field. The gap in this case is not technical opacity. Every fact needed to evaluate Circle's claim is public. The open question is whether representations made by issuers to courts and to investors are routinely tested against the on-chain record. This case study shows what that test looks like.

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.

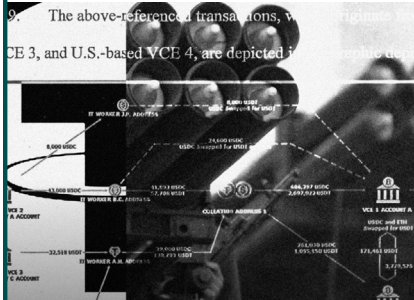


Where else have you seen us?

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  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	Forbes  Did Digital Currency Group Profit From \$60 million In North Korea Crypto Money Laundering?	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
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	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	South China Morning Post  How crypto investigators uncover scammers' blockchain billions, scale of money laundering in Asia

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

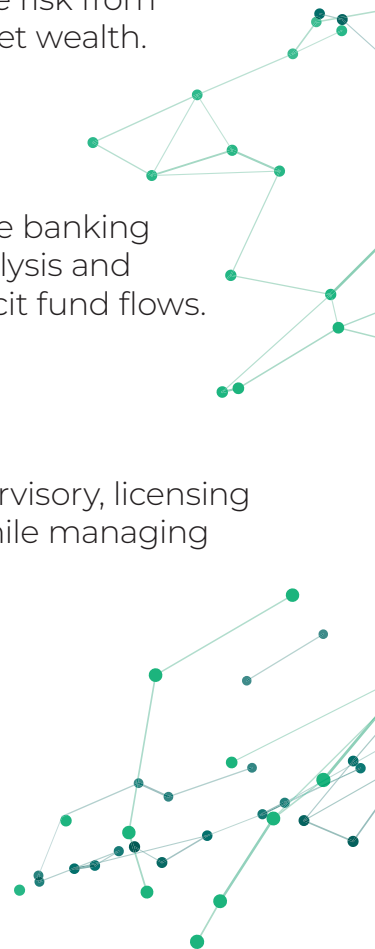
Fight money laundering, expand know-your-customer tools, and combat the financing of terrorism while expanding your customer base. Manage risk from customer crypto-assets and confidently verify sources of crypto-asset wealth.

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

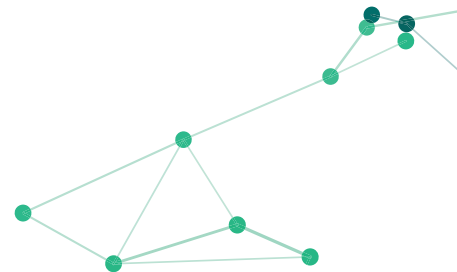
ChainArgos runs its own blockchain nodes, and we never enrich our data with yours, so you can be sure of data integrity.

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.

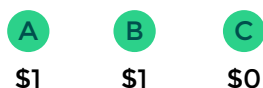


Fig. 1

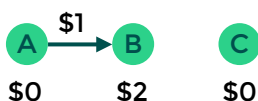


Fig. 2

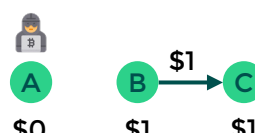


Fig. 3

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.

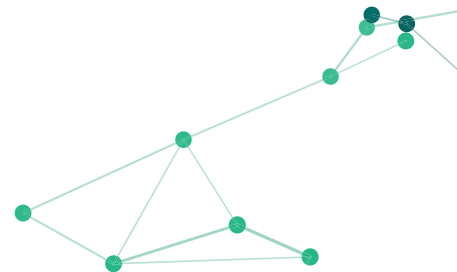
The screenshot shows the ChainArgos interface with a sidebar on the left containing navigation links: ChainArgos Home, Recently Viewed, Favorites, Boards, Folders, Blocks, and Applications. The main content area is titled "[Blockchain] Counterparties for Addresses" and includes search filters for "To or From Address" and "Symbol". Below the filters are four data tables:

[Blockchain] Your Queried Addresses' Labels & Categories			
Address	Labels	Categories	Organizations
1			

Blacklisting Info (If Any)			
Timestamp Date	Authority	Action	Blockchain
1			

[Blockchain] Inbound Counterparties								
From Address	Labels	Symbol	USD Value Today	Sum of Transfer Amounts	Number of Transfers	Avg Transfer Size	First Txn Date	Last Txn Date
1								
2								

[Blockchain] Outbound Counterparties								
To Address	Labels	Symbol	USD Value Today	Sum of Transfer Amounts	Number of Transfers	Avg Transfer Size	First Txn Date	Last Txn Date
1								
2								



Better attribution.

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

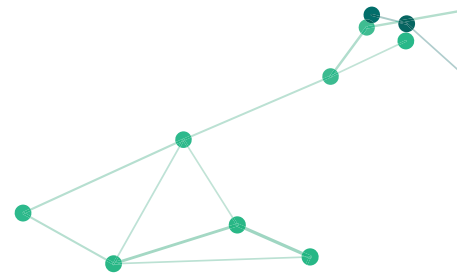
ChainArgos is the only blockchain intelligence firm that delivers programmatic address labels and wallet tags that are unassailable whether you're making business decisions or preparing to sue someone.

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.





© 2026 ChainArgos Pte. Ltd. All rights reserved.