ChainArgos.com

Better blockchain intelligence.

OPINION

Chainalysis Claims 95% Accuracy and Why That's Irrelevant

A RESPONSE TO BLOCKCHAIN TRACING FIRM CHAINALYSIS' RECENT BLOG POST CLAIMING ITS DATA IS 95% RELIABLE AND WHY THAT'S IRRELEVANT FOR THE BITCOIN FOG CASE

OCTOBER 9, 2025



Case Study	Background	3
	Introduction	3
	Chainalysis' Apparent Response To Our Amicus Brief	4
	It's Not The Size that Matters, It's Who Owns It That Counts	6
	When Guessing Games Become Deadly	7
	Positively Unsure	8
	An Aside On Disclosures Of Exculpatory Evidence	9
	The Peel Paper	10
	Why does this matter?	11
	Conclusion	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

Editor's note, September 26, 2026.

On September 25, 2026, the D.C. Circuit affirmed the convictions and sentence in *United States v. Sterlingov*, No. 24-3161. The court held that the trial court did not abuse its discretion in admitting the blockchain tracing evidence discussed below. It did not address the attribution issues raised in this piece or in our amicus brief.

Background

Roman Sterlingov, a citizen of Russia and Sweden, was convicted on March 12, 2024, in the U.S. District Court for the District of Columbia and sentenced on November 8, 2024, to 150 months (more than 12 years) in prison for allegedly operating Bitcoin Fog, a cryptocurrency mixing service.

Sterlingov was convicted of money laundering conspiracy, sting money laundering, operating an unlicensed money transmitting business, and violating the D.C. Money Transmitters Act, and his conviction was premised primarily on blockchain tracing provided by Chainalysis.

The prosecution argued that Sterlingov created and operated "Bitcoin Fog," a notorious darknet cryptocurrency mixer, a service designed to combine potentially illicit cryptocurrency with other funds to obscure the trail back to the original source, thereby providing anonymity and privacy.

Roman has always maintained he was only a user and not the operator of the service.

Introduction

On September 22, 2025, ChainArgos filed an Amicus Brief in support of Roman's appeal in *United States v. Sterlingov*[1] (the "Bitcoin Fog Case") arguing many of the blockchain forensics techniques used at trial were fundamentally unscientific and should never have been presented before a jury.

We also discovered a number of procedural issues specific to this case that emerge almost immediately once it is understood how the underlying blockchain tracing tools relied on by the prosecution operate.

In coming to these conclusions, ChainArgos relied on our extensive experience in both academic and professional settings. We also leaned on discussions with forensics experts, and standards as described in the landmark 2009 US National Academy of Sciences report entitled "Strengthening Forensic Science in the United States: A Path Forward" (the "USNAS Report").[2]

[1] https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208778227.0.pdf
[2] https://www.ojp.gov/pdffiles1/nij/grants/228091.pdf

info@chainargos.com

The USNAS Report was produced at the direction of the United States Congress as part of an effort to better understand and manage forensic techniques within the legal system. Insofar as blockchain tracing is submitted as evidence in court or used to inform investigations, the same basic issues applying to other forensic techniques ought to apply.

It is well understood that DNA evidence is exceptionally reliable if, and only if, the sample collection and lab forensics processes are performed correctly.

While blockchain tracing is nowhere near the levels of reliability of DNA evidence, the same basic requirement for proper application and treatment of blockchain tracing similarly applies.

None of the points we raise has anything to do with the legality of the Bitcoin Fog service because the primary issue at trial was whether the Defendant, Roman Sterlingov, actually created or operated Bitcoin Fog.

As the first criminal case pivoting on blockchain tracing to ever go through a US jury trial, this is the first opportunity for the US legal system to grapple with issues in blockchain tracing in a proper adversarial environment.

The US legal system is, at its core, an adversarial system where parties present evidence and argue their case before a judge and jury. Our contribution to the Bitcoin Fog Case is to argue that so-called "blockchain tracing evidence" which amounted to little more than "guessing" was presented as infallible at trial and ought never to have been admitted and certainly the jury should never have heard government agents present conjecture as scientific fact.

Chainalysis' Apparent Response To Our Amicus Brief

Shortly after ChainArgos' Amicus Brief was filed, Chainalysis, the blockchain tracing firm employed by the government in the Bitcoin Fog Case, published a blog post entitled "Chainalysis Data Stands Alone: Independently Proven Accurate and Reliable."[3]

This blog post focused on an academic paper to assess the reliability of Chainalysis' "clustering" techniques and concluded that Chainalysis' tools were reliable up to 95% for "clustering" "illicit services" addresses, an impressive feat, but largely irrelevant with respect to the Bitcoin Fog Case.

Clustering in the context of Chainalysis' blockchain tracing is the process of identifying and grouping multiple blockchain addresses that are highly likely to be controlled by the same individual or entity (such as an exchange, a darknet market, or a specific criminal group).[4]

[3] https://www.chainalysis.com/blog/chainalysis-data-independently-proven-accurate-and-reliable/

[4] https://www.chainalysis.com/blog/chainalysis-data-accuracy/#:~:text=At%20its%20core%2C%20that%20knowledge,a%20process%20we%20call%20clustering.

Unfortunately, Chainalysis' touted reliability in clustering has nothing to do with the issue at hand in the Bitcoin Fog Case, yet Chainalysis specifically refers to the Bitcoin Fog Case in their blog post, even though there are important distinctions between "clustering" and "attribution":

1. A reliable "clustering" technique for services like Bitcoin Fog implies an ability to estimate the size of the service in question. However, the Bitcoin Fog Case was not about measuring the size of that service, the case turned on who ran Bitcoin Fog. Therefore, even if the research cited by Chainalysis is accurate, it is irrelevant in the context of the Bitcoin Fog Case.

2. The specific blockchain traces claimed by Chainalysis at trial to show that Roman Sterlingov ran Bitcoin Fog involve addresses outside of their own Bitcoin Fog clusters. We know this with certainty because the prosecution in the Bitcoin Fog Case presented CSV files of the clusters as evidence at trial and these are in the public record. Anyone can observe that the blockchain traces detailed in Appendix A of our Amicus Brief claim attribution to Roman for blockchain addresses not included in Chainalysis' identified clusters. So, again, Chainalysis' defense of its "accuracy" through its cited academic research is irrelevant. If anything, this sort of out-of-cluster attribution needs greater scrutiny the more reliable the underlying clustering techniques are.

3. To make matters worse, expert witness testimony was presented to the jury at Roman's trial in early 2024, but Chainalysis' independent verification of its data only took place in early 2025, about a year after the trial concluded. The legal system does not afford "experts" the luxury of guessing an outcome and then determining if their guesses were reliable a year later. This would be the equivalent of allowing punters to guess as many lottery numbers as they like, but only pay for the winning ticket in the event they guessed correctly. Regardless, Chainalysis' referenced research is irrelevant to the Bitcoin Fog Case in that it was done a year after the expert testimony it claims to justify and it also does not address that testimony but instead only vaguely related issues, without dealing with the crux of the matter.

Each of these points relates to a different issue with blockchain tracing.

The first point boils down to this recent Chainalysis-cited study being irrelevant as far as the Bitcoin Fog Case is concerned. Imagine for a moment the only question here was the size of Bitcoin Fog's service to determine a sentence or fine. Chainalysis is presenting evidence their blockchain tracing tools are reliable for identifying the full set of blockchain addresses associated with services like Bitcoin Fog. That would indicate reliability for measures like total volume and transaction count. Even if this was accurate, it is irrelevant because the issue at hand in the Bitcoin Fog Case is about who ran the mixing service, not how large it was.

info@chainargos.com

Now if Chainalysis' blockchain tracing tools were demonstrably bad at clustering that measures size, that would necessarily raise questions about their reliability in other areas. But it does not follow that being good at detecting X necessarily makes one good at detecting Y. Police radar systems may be good at detecting speeding violations but are useless at finding concealed drugs. That's why the police have dogs. It is critical to use the right tool for the job at hand, the same way it is imperative to tout the appropriate ability for the task that matters.

It's Not The Size that Matters, It's Who Owns It That Counts

Irrelevance of Chainalysis' cited academic research aside, where it becomes more problematic is that we know exactly what blockchain addresses were claimed as part of Bitcoin Fog because CSV files with those lists were entered into evidence in the Bitcoin Fog Case and are in the public record.

Chainalysis is almost certainly aware of this and they must know the blockchain tracing detailed in our Amicus Brief concerns blockchain addresses not in those lists.

Chainalysis claiming their "clustering was reliable for Bitcoin Fog" and "helped with the Bitcoin Fog prosecution" without mentioning that their clustering did not find the key evidence is a peculiar marketing choice.

On this point, also note that Chainalysis' recent blog post claims their clustering techniques are "complete" in that they find nearly all blockchain addresses associated with a service. If you believe that claim then a blockchain address failing to appear in a cluster list is, according to Chainalysis itself, fairly good proof that that blockchain address is not part of the service in question.

Our core issue in the Bitcoin Fog Case is that the prosecution's evidence relied on attributions that have not been explained, did not come from Chainalysis' own clustering techniques, and consist of clearly different transaction behaviors across blockchain addresses attributed to the same person and for which no additional evidence is presented as to why they should belong to the same person.

Instead, the prosecution's expert evidence does not go beyond a vague appeal to untested but allegedly infallible "heuristics". If the heuristics relevant to the important attributions have been studied, nothing has yet emerged even though, again, this defendant was arrested in April 2021. More than 4 years ago.

info@chainargos.com

When Guessing Games Become Deadly

In the context of Chainalysis, “heuristics” are the rules, patterns, or assumptions that blockchain tracing tools use to group otherwise anonymous blockchain addresses together, concluding that they are all controlled by the same real-world entity or individual. In other words, “heuristics” are no more than “guesses,” educated or otherwise.

While it would be tempting to argue that a reliable (and allegedly flawless) clustering technique not identifying certain blockchain addresses to be part of Bitcoin Fog (exactly what Chainalysis’ clustering found in the Bitcoin Fog Case) supports Roman’s defense quite strongly, we would not go that far because, again, nobody has presented sufficient evidence these techniques work well enough that they should even be allowed into the conversation.

Unless Chainalysis intends to retract their expert witness testimony in the Bitcoin Fog Case or issue a clarification that they disagree with testimony given in the case, we appear to have a bit of a problem.

Several heuristics and techniques were presented by Chainalysis as reliable at trial in early 2024, and the work since has produced no more than a single study that a single heuristic is “reliable.” This is also, unfortunately, not the heuristic that matters in the Bitcoin Fog Case.

While it could be said that the absence of evidence is not evidence of absence in science (it simply means that your experiment was unable to detect what you were searching for), in criminal justice, the absence of evidence necessitates the absence of responsibility.

In simpler terms, the criminal justice system generally does not convict people without any evidence of such crime being committed.

Being presumed innocent requires that the absence of evidence that the government’s forensic techniques are reliable means those techniques cannot and should not be used to determine culpability.

The government is not entitled to present DNA evidence at trial unless it can demonstrate the evidence collection and lab processes followed the required and accepted standards that have been firmly established (TV and movies often portray this incorrectly for dramatic reasons).

info@chainargos.com

Forensic evidence within the context of the legal system is not a crapshoot where the goal is to present as much forensic evidence as possible to the jury so the jury can work out which version of the DNA sequencing machine's calibration processes should be used.

Because blockchain tracing is being presented as forensic evidence, it differs significantly from eyewitness testimony and it is wholly unreasonable to expect judges and juries to review the scientific literature on novel forensic techniques.

Finally, this last point should be obvious to everyone: You cannot present your tools as "reliable" in court testimony and then present evidence of that reliability a year later and expect to be taken seriously.

Claiming your product is "the best" or "incredibly reliable" or something like that in marketing is perhaps less unctuous. But when you are testifying "the tracing is accurate" there needs to be something behind that claim. When that "something" turns out to be a future study that was never presented to the court such as in the Bitcoin Fog Case, this raises even more questions.

Positively Unsure

In the Bitcoin Fog Case, a prosecution witness testified "we analyzed all of the subpoena returns that I used in my analysis for this case and found no false positives".

That's right, a government expert for the prosecution testified they found "no false positives" at the trial of Roman Sterlingov. Anyone with any real-world experience knows a 0% error rate is suspicious outside of purely mathematical (and often academic) pursuits.

Discussion of this asserted 0% false positive error rate with a range of medical professionals produced laughter without exception.

Even the recent study cited by Chainalysis itself claims a non-zero error rate.

Against this backdrop, it should be obvious that a government expert testifying a given technique has "no false positives" will materially influence the jury to the prejudice of the defense, precisely because a jury is not equipped to make such determinations.

A jury member with no scientific background would more likely than not accept a 0% false positive error rate at face value and not recognize the absurdity of such a claim.

info@chainargos.com

If the company providing the tools in the Bitcoin Fog Case (Chainalysis) is now touting a small (0.15%) but non-zero false positive rate as a victory, that raises even more uncomfortable questions.

Presumably, the government expert in the Bitcoin Fog Case was describing an informal survey of a small set of cases and we are not suggesting no work was performed in delivering this testimony. But when law enforcement officials start discussing sample sizes and survey techniques before a jury, this is precisely the area of forensic evidence the USNAS Report warned that judges and juries are ill-equipped to assess.

An Aside On Disclosures Of Exculpatory Evidence

Roman Sterlingov was arrested April 27, 2021 at Los Angeles International Airport. Roman's arrest warrant dated April 26, 2021 is based on a long statement of facts signed by a federal agent and approved by a magistrate. This statement of facts contains an error where a blockchain address is incorrectly identified as starting with "1 WMex" when the correct prefix was "1 WMcx" – the "e" in the sworn statement should have been a "c".

This error may seem immaterial, but blockchain addresses are like DNA sequencing (not to be confused with DNA evidence), a difference of a single letter or number leads to an entirely different blockchain address, the same way a different DNA sequence indicates an entirely different individual.

The incorrect blockchain address relied on to arrest Roman has never been used and can never have been correct or produced by any reasonable blockchain tracing tool.

We accept that typographical errors can and do happen and we do not claim that this error alone is sufficient to invalidate the prosecution's case because that would be an absurd and unreasonable standard.

But there are real issues as a consequence of this typographical error in the Bitcoin Fog Case because a government agent (different from the arresting agent who prepared the warrant) claimed, again in front of the jury, that procedures related to this were flawless.

There are strong indications that members of the government's prosecution or investigation teams knew about this error and that information was never disclosed to the defense.

info@chainargos.com

If so, these are no longer merely administrative or clerical lapses, but hint strongly at a violation of the defendant's due process rights as established by the Supreme Court's 1963 decision in *Brady v. Maryland*. Not because typographical errors are bad – but rather because the circumstances around this case strongly suggest the government had evidence in its possession that the procedures used here were not 100% reliable before the testimony discussed above was offered. Under the *Brady* standard the government is compelled to disclose information in its possession that would help the defense impeach government witnesses.

The Peel Paper

A paper entitled "How to Peel a Million: Validating and Expanding Bitcoin Clusters" (the "Peel Paper") was presented at a conference in Boston in August 2022.[5] The Peel Paper was written by a collection of well-respected academics and explored blockchain address clustering techniques. Included in the Peel Paper was analysis of Bitcoin Fog with a citation to a publicly available copy of the statement of facts used to support Roman's arrest warrant.[6]

One of the authors of the Peel Paper is a part-time contractor at Chainalysis[7] while another author has delivered talks at Chainalysis.[8]

Another author of the Peel Paper was an author on one of the earliest papers about blockchain tracing that birthed Chainalysis and routinely collaborates with Chainalysis and other similar companies.[9]

But the Peel Paper was presented a whole 16 months after Roman's arrest so the underlying work for the Peel Paper was clearly performed at least a year after the arrest.

Certainly the work referenced in the Peel Paper could not have been performed before Roman's arrest because no blockchain addresses in the Bitcoin Fog Case were yet public at the time, and the documents to cite in the Peel Paper did not exist yet.

[5] https://www.usenix.org/system/files/sec22-kappos.pdf
[6] https://storage.courtlistener.com/recap/gov.uscourts.dcd.230456/gov.uscourts.dcd.230456.1.1_1.pdf
[7] https://georgekap.github.io/
[8] https://www.haaroonyousaf.com/
[9] https://smeiklej.com/

info@chainargos.com

Why does this matter?

Because the authors of the Peel Paper referenced Roman's arrest warrant (remember the one containing the incorrect blockchain address?) and somehow managed to find the correct blockchain address.

From the Peel Paper, it is reasonable to infer that the authors of the Peel Paper had close connections to the agents who prepared Roman's arrest warrant or outside contributors or consultants associated with the preparation of that document.

If not, the Peel Paper's authors could not have found the correct transactions without either:

1. asking the agents who prepared the statement of facts for the correct blockchain address(es); or

2. running some sort of wildcard search themselves and finding the correct blockchain addresses with those tools. If it is Option 1, then communications surely exist between the government and some of the academics clarifying the blockchain addresses. If it is Option 2, then it is also likely such communication exists confirming the typographical error and that they had found the right blockchain address.

It is of course possible the authors of the Peel Paper spotted the typographical error in Roman's arrest warrant, somehow found the correct blockchain address, never asked anyone about it and chose to cite the source document without any footnote or other indication of the correction.

At this juncture we need to ask whether that feels likely for a group of academic computer scientists with close connections to the blockchain tracing company behind the source document?

As we will see, even in this case, the government's decision to redo the research and present that blockchain tracing afresh at Roman's trial suggests there are internal records about this error, records not made known to Roman's defense team.

Any such communications or records would undercut the claims of a "perfect record" made on the stand by the government's expert witness and should have been disclosed to the defense.

Further, the federal agent that testified at trial is not the one who signed the statement of facts.

Was that some sort of staffing issue? Was it a coincidence? Was it a tactical choice to cut off the defense's ability to ask "if you say the error rate is zero can you explain why a blockchain address in your sworn statement does not appear to exist?"

We do not know.

What we do know is that the federal agent who testified at trial clearly redid the blockchain tracing in the Bitcoin Fog Case using the correct blockchain address.

While we are speculating as to whether the authors of the Peel Paper communicated with government investigators in the Bitcoin Fog Case, it beggars belief that there is no note in a file somewhere indicating the initial statement of facts differs from the report used at trial because of the error.

Such a note must exist because the first investigator picking up the case would start from the original sworn statement of facts and spot the error quickly.

Consider the alternative in this case.

Think about how Roman's defense could have questioned the federal agents involved. For instance, Roman's defense attorney could have asked the federal agents involved,

"So you rechecked the blockchain tracing and found a typographical error in the initial address?"

If the answer to that question is "yes" then surely the federal agents would have noted down the error, and if so, why was this information not provided to the defense?

If the federal agents had noted the error but did not document it, then a federal agent would be testifying it is not their practice to record errors in analysis when found.

That would be an appeal opportunity for every person convicted on the basis of forensic evidence in the entire country.

More likely than not, the error was written down, in which case it should have been disclosed to the defense, but the fact remains that it was not.

We believe these federal agents are competent, well-intentioned, and reasonable people. It is reasonable to assume that these federal agents would check their own work and that of their colleagues, and note when errors are found and corrected.

Yet for some inexplicable reason, no one thought to disclose those notes to the defense.

It's probable no one even thought to ask about the existence of such a note because nobody foresaw that the prosecution's case would hinge on representations to the jury as to the level of infallibility of the prosecution's presented blockchain tracing process.

If the government had disclosed there was a typographical error to the defense, and their analysis was repeated several times all with the same result, and they intended to and did assert a small, but non-zero error rate at trial, this would perhaps be less of an issue.

But this did not happen, and as such, we can no longer deal in hypothetical situations that have no option of existing.

It seems unlikely that there was any malice intended on the part of the prosecution in their omission to inform the defense with respect to the typographical error in the blockchain address.

In all likelihood, the prosecution probably did not anticipate that their expert witness was going to testify before the jury that their blockchain tracing methodology had a zero error rate.

Minor errors are predictable, but testifying on the stand before a jury that your methodology has zero error rates is wholly outside the realm of predictability, even with no background in statistics or the scientific method.

Even the most conscientious document review before the trial may well have missed this typographical error, but that nonetheless does not absolve the prosecution of its obligation to disclose such an error to the defense.

Conclusion

Blockchain tracing can be useful for a wide variety of purposes, including for the investigation of crimes. But like any forensic technique, indeed, like any technique or tool used in the real world, blockchain tracing has both advantages and disadvantages, blind spots and error rates, and all the limitations of using a tool under real-world circumstances.

Does that mean blockchain tracing should never be admissible in court?

Of course not.

ChainArgos is not arguing that only immaculate evidence can ever be presented before a jury and we are certainly not arguing that a small number of errors renders a technique entirely useless.

info@chainargos.com

Instead, our position is synchronous with that of the USNAS Report that states:

> *Law enforcement officials and the members of society they serve need to be assured that forensic techniques are reliable. Therefore, we must limit the risk of having the reliability of certain forensic science methodologies judicially certified before the techniques have been properly studied and their accuracy verified by the forensic science community.*

and further,

> *The judicial system is encumbered by, among other things, judges and lawyers who generally lack the scientific expertise necessary to comprehend and evaluate forensic evidence in an informed manner, trial judges (sitting alone) who must decide evidentiary issues without the benefit of judicial colleagues and often with little time for extensive research and reflection, and the highly deferential nature of the appellate review afforded trial courts' Daubert rulings. Given these realities, there is a tremendous need for the forensic science community to improve. Judicial review, by itself, will not cure the infirmities of the forensic science community.*

Lest we be accused of casting aspersions on the legal and forensic science communities, the authors of the USNAS Report include revered judges, lawyers, law professors, chief medical examiners, and professors of forensic sciences.

The director of the federal judicial center and the director of that center's program on scientific and technical evidence both signed the USNAS Report.

Those comments are clearly meant, both in the USNAS Report and as quoted here, as constructive criticism intended to improve things.

As so many lobbyists and lawyers working on blockchain-related issues are wont to say, evidentiary regulations should be technology-neutral. Standards for blockchain tracing and fingerprint matching are clearly not identical, not least because their mechanical processes are so different, but the principles and frameworks nonetheless ought to be consistent.

Blockchain tracing is a technical discipline like any other and it is therefore essential we are clear about how various tools work, what they can and cannot do, and how reliable various methods are absent independent corroboration or validation. This is not an extreme position. It is, however, not consistent with government experts testifying to juries that untested methods have a zero error rate. To be fair, we do not blame those experts because they are almost certainly parroting what they were taught by the providers of these blockchain tracing tools.

And so we find ourselves in a strange situation where an industry that should be able to lead in terms of rigor and transparency – blockchain is after all about transparency and these analytics firms are essentially tech businesses built atop software that is easier to test than, say, a blood splatter analysis technique – is somehow well behind. It's time to fix that.

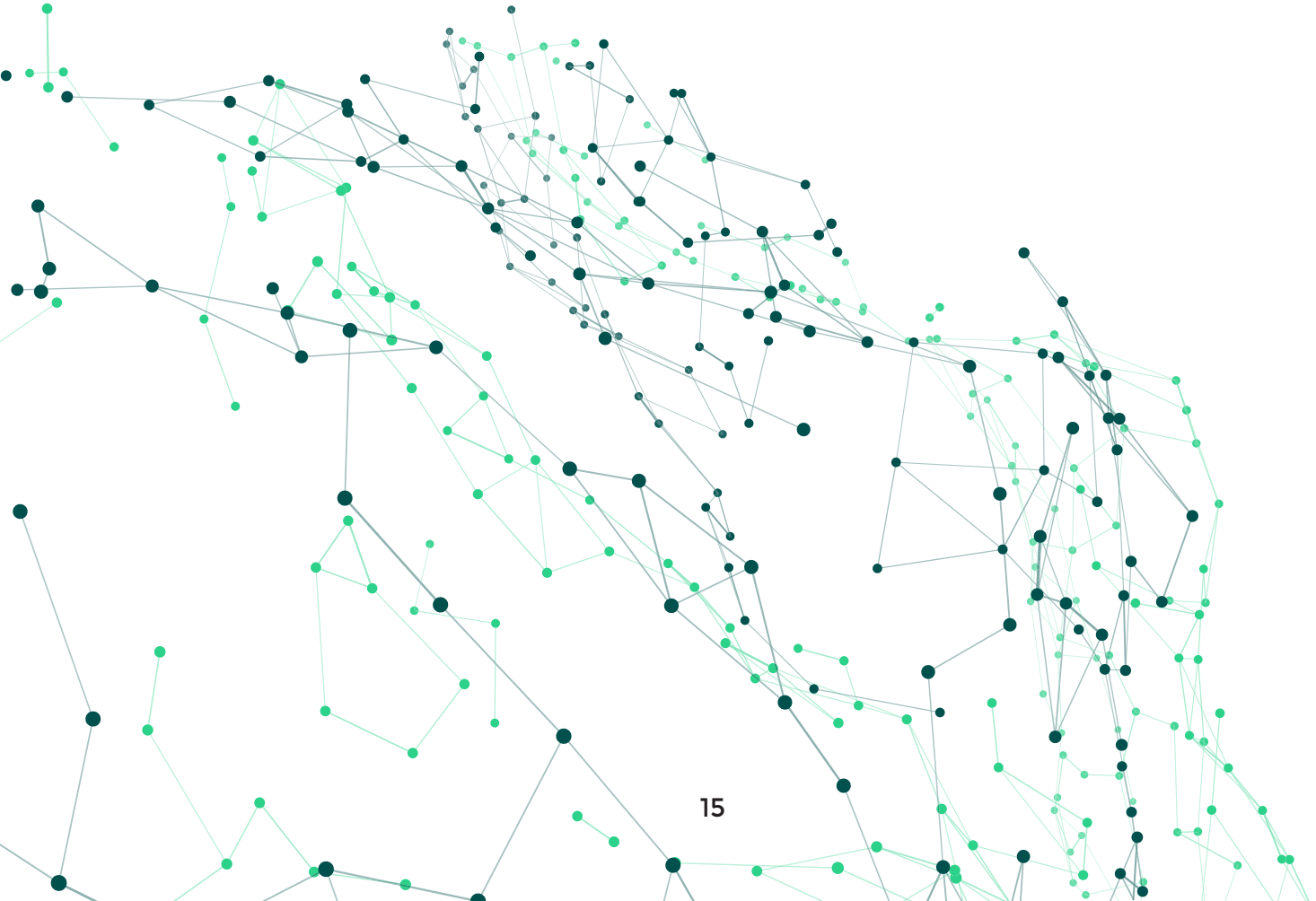
Who are we?

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

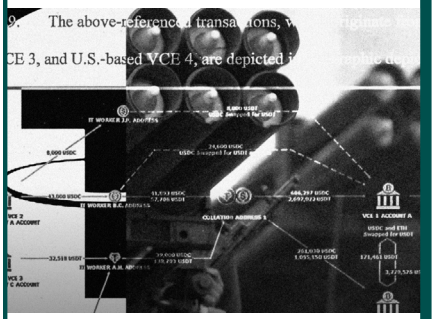
- Blockchain analyst Reiter had flagged gaps in Binance-peg BUSD
- Binance says earlier 'operational delays' have now been fixed

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

info@chainargos.com

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 fight crime, prosecute criminals, and track 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 knowledge.

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.

info@chainargos.com

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.

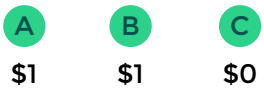


Fig. 1

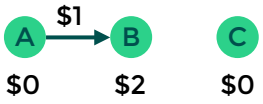


Fig. 2

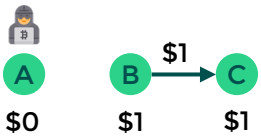


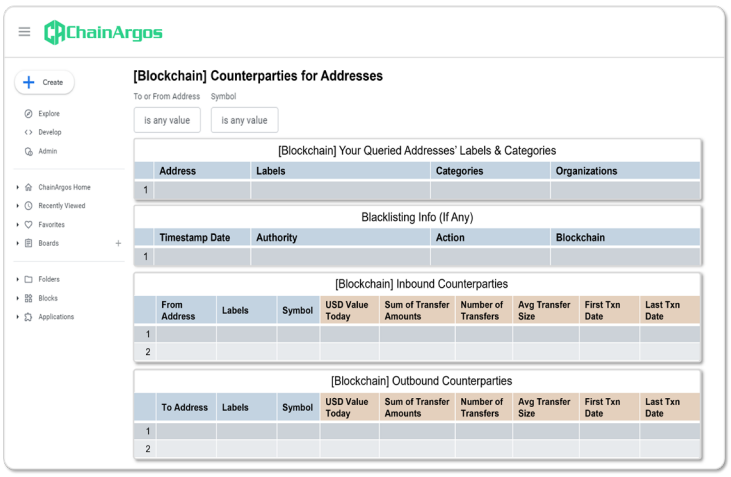
Fig. 3

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.

info@chainargos.com

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.

info@chainargos.com

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 nor 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.

info@chainargos.com



© 2024 ChainArgos Pte. Ltd. All rights reserved.