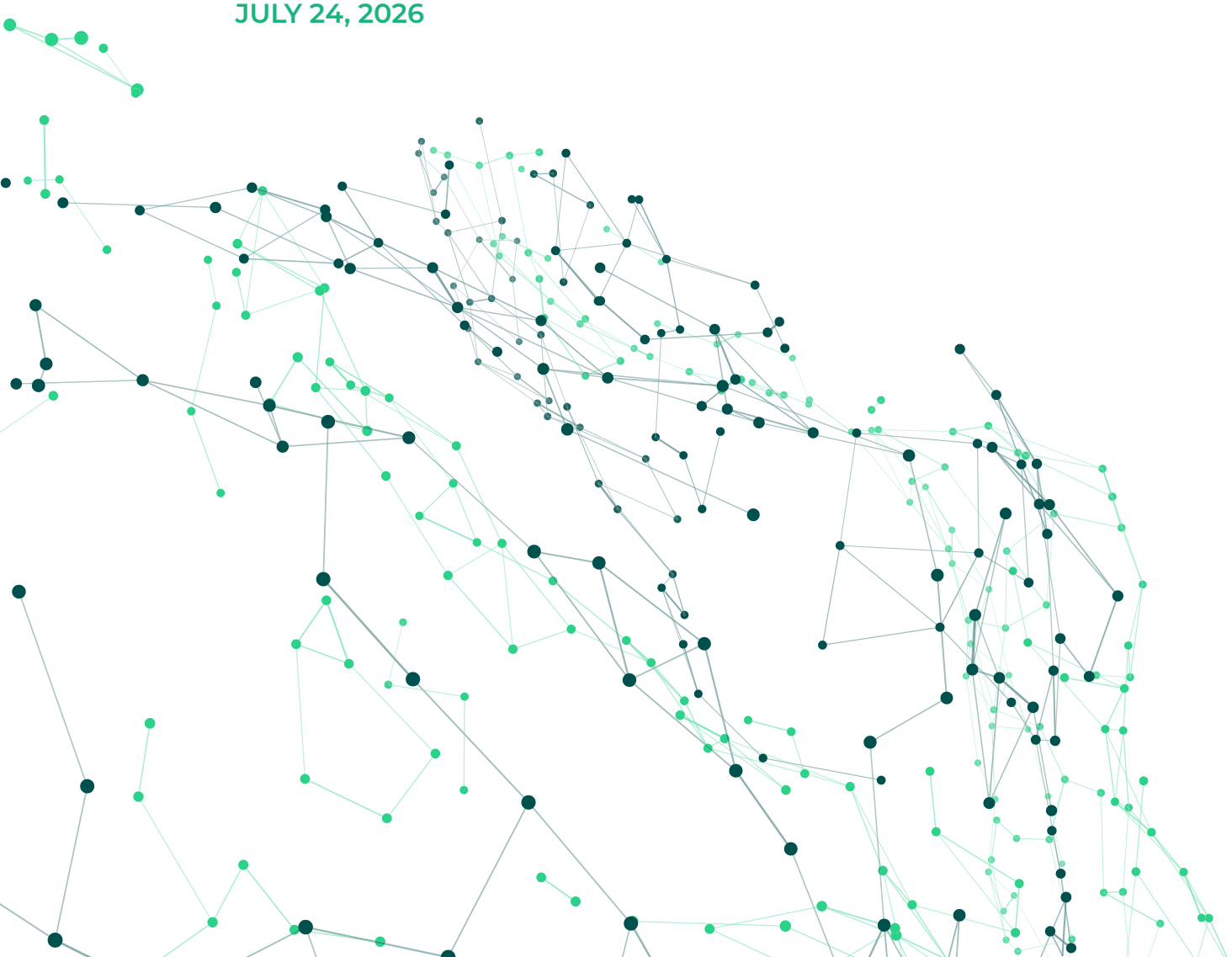
ChainArgos.com

Better blockchain intelligence.

Caught in a Cluster
Trapped by Blockchain Tracing

A CASE STUDY ON THE UNTESTED BLOCKCHAIN TRACING THAT SENT A MAN TO PRISON AND THE STANDARDS IT NEVER MET

JULY 24, 2026



Contents.

info@chainargos.com

Executive Summary

In March 2024, a jury convicted Roman Sterlingov of operating the Bitcoin Fog mixing service, substantially on the strength of a cluster of 925,743 bitcoin addresses that Chainalysis software attributed to Bitcoin Fog. The witnesses who carried that evidence into court could state no error rate for the software and could cite no peer-reviewed study of its accuracy. On June 29, 2026, with the appeal awaiting decision, Chainalysis published a formal ontology that adopts, point by point, the criticisms ChainArgos made of that evidence in its amicus brief.

Two weeks later, Chainalysis marketed the conviction as proof that its analytics are courtroom-ready. Measured by the standards Chainalysis now publishes, the evidence Chainalysis defended does not qualify as science. This case study documents that contradiction, entirely from public records, and explains what it means for anyone whose assets carry a blockchain label.

1. Why This Should Matter to You

If you hold, custody, trade, or supervise digital assets, opaque software somewhere may have already mischaracterized your transactions. Somewhere a secret labeling system determines which blockchain addresses belong together and makes claims about who they belong to. You have never seen these labels, you cannot examine the labeling system, and there is no published error rate or methodology for the creation of those labels.

Yet that black-box blockchain address labeling system decides real things that affect real people. Crypto-asset exchanges use that labeling to freeze accounts and file suspicious activity reports. Banks use that labeling to score customers and deny access to their services. Investigators use that labeling to obtain warrants and seize assets. Courts have accepted that labeling as a basis for suspicion, probable cause, and sometimes much more.[1] When the label is right, none of this troubles anyone. The problem is what happens when it is wrong, because today, almost no one can tell.

You do not need to trade crypto-assets for this to reach you. If you hold a stablecoin, the same software can label your address, using the same unpublished and untested tools, and your account can be frozen on the strength of the label alone.

One case shows just how far a label can go.

[1] *In re Search of Multiple Email Accounts*, 585 F. Supp. 3d 1, 20 (D.D.C. 2022), cited by Chainalysis in its amicus brief (note 5) at 14.

info@chainargos.com

In March 2024, a jury in Washington, D.C. convicted Roman Sterlingov of operating Bitcoin Fog, a crypto-asset mixing service. Roman is serving 12.5 years in prison[2] and the central evidence was a cluster of 925,743 Bitcoin addresses that software created by blockchain tracing firm Chainalysis attributed to Bitcoin Fog, presented to the jury as a single fact. At the hearing that decided whether that blockchain tracing evidence could be used, an expert witness from Chainalysis could not state the software's error rate, could not name a peer-reviewed study that tested its accuracy, and testified that she was not aware of a single false positive across hundreds of investigations.[3] During the trial an FBI analyst testified that in his experience he had not encountered false positives, while conceding he could not quantify the false positive rate at all. In the real world, observing no failures is not a sign that something works flawlessly. It is a sign that something was tested insufficiently.

The court admitted the expert testimony as evidence anyway.[4]

We were not involved in Roman's trial.

But when we became aware of the circumstances leading to Roman's conviction, we felt, given the egregious level of errors in the testimony that led to Roman's 12.5-year prison sentence, compelled to file an amicus brief at Roman's appeal. In February 2026, months after the filing of our amicus brief in Roman's appeal, Chainalysis responded with an amicus brief of their own, arguing our amicus brief was "meritless."[5]

Then, this summer, Chainalysis published two documents in the space of two weeks. The first, a formal ontology by Chainalysis Chief Scientist Jacob Illum, that adopted the substance of the criticisms in our amicus brief in Roman's appeal, point by point. The second, a Chainalysis marketing post, holds up the very ruling under appeal in Sterlingov as a credential. Read together, these statements put out by Chainalysis raise questions everyone should be asking. What exactly is the accuracy of the blockchain tracing tools being sold here, when was it ever demonstrated, and could your person and property be at risk due to unjustified faith in untested commercial software?

[2] *United States v. Sterlingov*, No. 1:21-cr-00399 (D.D.C.), verdict returned March 12, 2024, sentence imposed November 8, 2024. The appeal is pending as No. 24-3161 (D.C. Cir.), argued May 12, 2026.

[3] Transcript of Motions Hearing, *United States v. Sterlingov*, No. 1:21-cr-00399 (D.D.C. June 23, 2023), ECF No. 224, at 74, 117, 119-20, 122-23, 127-28, 139-40, https://storage.courtlistener.com/recap/gov.uscourts.dcd.232431/gov.uscourts.dcd.232431.224.0.pdf

[4] Memorandum Opinion and Order, *United States v. Sterlingov*, No. 1:21-cr-00399, ECF No. 259 (D.D.C. Feb. 29, 2024), https://storage.courtlistener.com/recap/gov.uscourts.dcd.232431/gov.uscourts.dcd.232431.259.0.pdf

[5] Brief for Amicus Curiae Chainalysis Inc., *United States v. Sterlingov*, No. 24-3161 (D.C. Cir. Feb. 25, 2026), at 23, https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208825487.0.pdf

info@chainargos.com

2. The Case That Tested the Evidence

Bitcoin Fog was a crypto-asset mixer, a service that pools bitcoin deposits from many users and pays them out in a way intended to break the link between deposits and withdrawals. The government charged Roman with creating and operating the mixing service.

Roman has always maintained he was just a user and not the operator of Bitcoin Fog. The government never seized servers, never captured ledgers or operator credentials, and had no direct evidence that Roman operated Bitcoin Fog. Nothing directly connected to Bitcoin Fog's operator was presented as evidence against Roman. The case for who operated Bitcoin Fog relied substantially, if not almost entirely, on blockchain tracing. ChainArgos filed an amicus brief in the appeal, *United States v. Sterlingov* (D.C. Cir. No. 24-3161), on September 22, 2025.[6] Our argument was narrow and intended to assist the appellate court in understanding the severe limitations of blockchain tracing.

We did not claim the government's blockchain tracing tools were useless or fraudulent. We said the expert testimony that carried the attribution cluster into evidence in Roman's case made claims of accuracy and reliability that were dramatically overstated and fundamentally unscientific as presented.

In the US legal system there are many important precedents which establish standards for what qualifies as "forensic" or "expert" evidence. Blockchain tracing is new as a branch of forensic science, but the use of new tools in court is still subject to the existing rules applicable to all other evidence.

[6] Brief of Amicus Curiae ChainArgos, *United States v. Sterlingov*, No. 24-3161 (D.C. Cir. Sept. 22, 2025), https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208778227.0.pdf

If it disagrees with experiment it is wrong.
In that simple statement is the key to science.

Richard Feynman

info@chainargos.com

In our amicus brief at Roman's appeal, we presented four specific criticisms of the use of blockchain tracing as evidence in *United States v. Sterlingov.*

- **The heuristics were never validated.** A heuristic is an educated guessing scheme which asserts certain characteristics are sufficient to associate two seemingly separate samples. Good guessing schemes become forensic methods through testing, with published error rates, and after being subject to independent scrutiny and certainly not through witnesses testifying that they have not personally observed any failures. Just because all the swans you've ever seen are white doesn't mean there's no such thing as a black swan and you certainly cannot treat testimony consisting of anecdotes as an observation of fact.

- **"No false positives observed" is not an error rate.** The prosecution's case against Roman contained exactly one test against "ground truth," the term used for answers already known to be correct, against which a tool's output can be checked. Government agents had used Bitcoin Fog undercover, so five blockchain addresses were known with certainty to belong to the Bitcoin Fog mixing service. Chainalysis attributed four of the five blockchain addresses. Missing one known address out of five is a 20% false negative rate, a measure of what Chainalysis's software failed to catch, and that rate was never characterized statistically at Roman's trial, it simply went unaddressed.[7]

- **Behavioral "fingerprints" are not proof of common ownership.** The prosecution in Roman's trial also relied on Chainalysis's "behavioral heuristic," which attempts to group otherwise anonymous blockchain addresses according to the "digital fingerprints" wallet software leaves in transactions. Yet Chainalysis's own expert could not say precisely how it works. What is certain is that a fingerprint belongs to the software, not the person. Strangers using the same wallet software leave the same fingerprint, and anyone who builds their own blockchain transactions can fake one. Use the same software as a criminal and pattern-matching can put your blockchain addresses in their cluster. That is inference presented as fact.

- **The conclusions had no vocabulary.** Structural grouping, entity attribution, and operator determination were fused into a single assertion, "this blockchain address belongs to Bitcoin Fog," with no mechanism for the court, the jury, or the defense to interrogate the evidentiary basis of each component.

[7] ChainArgos Amicus Br. (note 6) at 24-25, https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208778227.0.pdf

info@chainargos.com

Every one of the criticisms in our amicus brief was aimed at testimony that is now public record.

The hearing that admitted the blockchain tracing evidence relying on Chainalysis's Reactor software in Roman's trial was a *Daubert* hearing, named for the Supreme Court case that sets up trial judges as gatekeepers of expert evidence and provides the framework within which they are to evaluate admissibility.

The transcript of that *Daubert* hearing, dated June 23, 2023, shows the Chainalysis witness, an investigator employed by Chainalysis Government Solutions, a subsidiary of Chainalysis, answering, under oath, that she could not state a statistical error rate for Reactor, Chainalysis's flagship blockchain tracing software, that Chainalysis did not to her knowledge collect error rates or information on false positives, and that she could not cite a single peer-reviewed paper attesting to the accuracy of the Reactor software.

Asked on a later occasion whether Chainalysis had ever done an internal analysis of Reactor's error rates, the same witness answered that it had not. This is the evidentiary foundation on which a cluster associating 925,743 blockchain addresses was placed before a jury.[8]

> **The first principle is that you must not fool yourself - and you are the easiest person to fool.**
>
> **Richard Feynman**

[8] *Daubert* Hearing Transcript (note 3) at 117, 119-20, 127-28, 139-40, https://storage.courtlistener.com/recap/gov.uscourts.dcd.232431/gov.uscourts.dcd.232431.224.0.pdf

info@chainargos.com

3. What Chainalysis Told the Court

Chainalysis filed its own amicus brief on February 25, 2026, in Roman's appeal telling the D.C. Circuit that its Reactor software was highly accurate and that testing had proved it. It said blockchain analysis tools "like Chainalysis Reactor" were widely accepted and peer reviewed. It described the 20% false negative rate we identified as a feature of conservative design rather than an error rate requiring characterization. Chainalysis argued further that the defense at Roman's trial had no business reviewing Reactor's source code at all, comparing the situation to an economist who uses Excel without knowing how Excel computes its formulas.[9]

Our arguments were addressed in a dedicated section titled "ChainArgos's Criticisms Are Equally Meritless."[10]

> **C. ChainArgos's Criticisms Are Equally Meritless**
>
> In its amicus brief supporting Sterlingov, ChainArgos advances a litany of arguments attacking Reactor's accuracy and otherwise echoing many of Sterlingov's assertions. Those arguments fail as well.

(Source: The dedicated section heading in the Chainalysis amicus brief, February 25, 2026, at page 23 (note 5).)

[9] Chainalysis Amicus Br. (note 5) at 13, 17, 21-22 (the Excel comparison, citing *United States v. Morgan*), and 24-25, https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208825487.0.pdf

[10] Chainalysis Amicus Br. (note 5) at 23, https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208825487.0.pdf

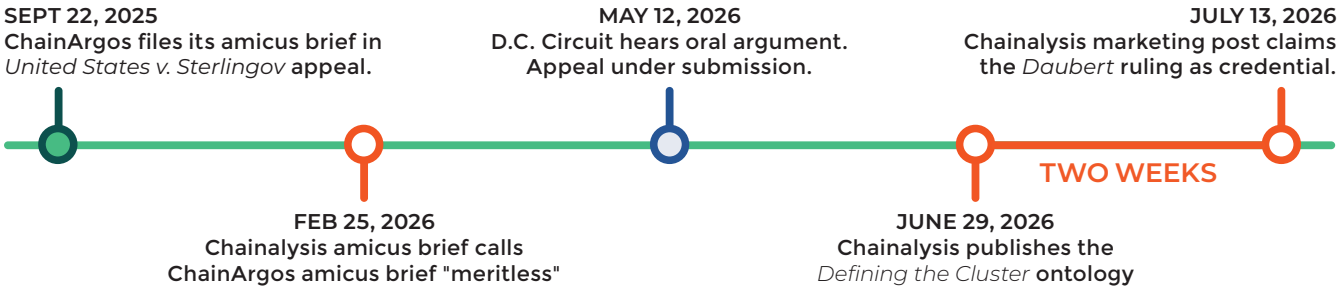
Science is the belief in the ignorance of experts.

Richard Feynman

4. What Chainalysis Now Publishes

On June 29, 2026, four months after Chainalysis's amicus brief and seven weeks after the D.C. Circuit heard oral arguments, Chainalysis published *Defining the Cluster: A Formal Ontology for Blockchain Address Analysis and Intelligence Claims*, authored by its Chief Scientist, Jacob Illum.[11] The paper proposes standards for the entire blockchain tracing industry. Position by position, Illum's paper now agrees with the very criticisms ChainArgos made of the Chainalysis testimony in Roman's trial.

Section references below are to *Defining the Cluster* (June 29, 2026), and everything quoted comes from public court filings, public transcripts, or Chainalysis's own publications, with the reference given each time so nothing has to be taken on trust.



4.1 A *Daubert* ruling validates a methodology, not a field

In Section 2.1 of the ontology, Chainalysis says that the *Sterlingov* ruling validated only the specific methodology examined in that specific proceeding, not the field and not other providers' implementations.[12] The same section criticizes blockchain tracing industry providers who have wrongfully held the ruling up as a general endorsement of the entire field.

We agree, and the logic cuts in both directions.

If *Sterlingov* does not validate the blockchain tracing field, it also does not validate versions of a methodology that were never examined. The ontology's own introduction acknowledges that Chainalysis's implementation "continues to evolve."[13]

[11] Jacob Illum, *Defining the Cluster: A Formal Ontology for Blockchain Address Analysis and Intelligence Claims* (Chainalysis, June 29, 2026), https://www.chainalysis.com/reports/defining-the-cluster/

[12] *Defining the Cluster* (note 11), Section 2.1, https://www.chainalysis.com/reports/defining-the-cluster/

[13] *Defining the Cluster* (note 11), at 5, https://www.chainalysis.com/reports/defining-the-cluster/

The *Daubert* hearing in Roman's case took place on June 23, 2023. By Chainalysis's own account, the methodology the district court examined in Roman's case was not a fixed object. The ontology itself warns about exactly this danger. When the algorithms behind a blockchain address cluster are updated without versioned documentation, it becomes impossible to reconstruct how the blockchain address clustering scheme was built in the first place.[14] The question for the D.C. Circuit is whether the 2023 record supports admissibility of blockchain tracing at all.

A 2026 paper by Chainalysis, the producer of the blockchain tracing examined at that 2023 hearing, cannot retroactively supply the documentation, enumerated failure modes, or error characterization that were absent from that record at the time of that trial. That very 2026 paper would seem to argue for the inadmissibility of the tools at issue given the lack of specificity provided pre-trial and during the trial.

4.2 The cluster conflates three claims

In Section 3.2 of the ontology, Chainalysis explained that a single sentence (this address belongs to Cluster X, which is Exchange Y) actually encodes three separate claims.

- a structural claim (these blockchain addresses move together)
- an attribution claim (these blockchain addresses belong to this named entity)
- an operator claim (a specific person or organization operates the entity behind them)

Each claim carries different evidence types and error profiles. In Section 3.3, the ontology describes two dangers with this approach.

The first is propagation amplification, where one incorrectly attributed blockchain address silently contaminates thousands of downstream labels of other blockchain addresses.

The second is evidentiary opacity, where an investigator cannot tell whether a grouping of blockchain addresses relies on "co-spend" analysis (a heuristic that purports to link bitcoin blockchain addresses simply because their bitcoin were spent together in a single transaction) or on a machine-learning prediction (a pattern guess produced by trained software). The blockchain address cluster presents a conclusion without exposing the reasoning behind it.[15]

This is the vocabulary gap our amicus brief identified in Roman's appeal.

[14] *Defining the Cluster* (note 11), Section 3.2, https://www.chainalysis.com/reports/defining-the-cluster/
[15] *Defining the Cluster* (note 11), Sections 3.2 and 3.3, https://www.chainalysis.com/reports/defining-the-cluster/

info@chainargos.com

At trial, the jury heard that 925,743 addresses belonged to a "Bitcoin Fog cluster." Under the framework Chainalysis now proposes, that assertion would need to have been broken apart during Roman's trial. Which addresses were grouped by fixed rules applied to the public transaction record? Which by proprietary behavioral heuristics, and which by intelligence gathered outside the blockchain? At what confidence level, and with what documented failure modes for each? No such decomposition was available to the defense, the district court, or the jury in Roman's case.

If your compliance system flags a counterparty based on a blockchain address label supplied to you by a vendor today, no such decomposition is available to you either.

4.3 Pattern-matching cannot produce forensic claims

In Sections 4.3.1 and 5.4 of the ontology, Chainalysis excludes trained predictive models, software that learns patterns from past data rather than following stated rules, from structural claims entirely, because their failure modes cannot be exhaustively enumerated and their reasoning cannot be independently examined. The ontology's introduction opens with a cautionary tale in which pattern-matching led one analytics tool (presumably not Chainalysis) to label a gambling service's deposit address as child sexual abuse material, on the basis of small, regular payments of similar size and frequency looking alike through a narrow statistical lens.[16]

Now set that against the testimony in Roman's case.

At the June 23, 2023 hearing in *Sterlingov*, the Chainalysis witness described the behavioral heuristic, the pattern-based method behind a large share of the Bitcoin Fog blockchain address cluster, as "provable because it's done and replicated time and time again and very reliable," while conceding in the same exchange that she could not cite a single peer-reviewed paper validating its accuracy.[17] Chainalysis's own ontology now says appearance-based conclusions are dangerous and belong in a lower evidentiary tier than forensic fact. Yet at Roman's trial, behavioral heuristics were presented alongside "co-spend" results as components of a single, undifferentiated blockchain address cluster, exactly the standard collapse Chainalysis warns against in Section 3.3 of its ontology.[18]

[16] *Defining the Cluster* (note 11), Sections 4.3.1 and 5.4, and Introduction, https://www.chainalysis.com/reports/defining-the-cluster/

[17] *Daubert* Hearing Transcript (note 3) at 127-28, https://storage.courtlistener.com/recap/gov.uscourts.dcd.232431/gov.uscourts.dcd.232431.224.0.pdf

[18] *Defining the Cluster* (note 11), Sections 3.3 and 5.4, https://www.chainalysis.com/reports/defining-the-cluster/

info@chainargos.com

4.4 Digital Fingerprints alone do not establish co-ownership

In Section 4.3.1 of the ontology, on reverse-engineered wallet infrastructure, Chainalysis adds a caveat that closely tracks our amicus brief. Digital "fingerprints" without a transactional link between blockchain addresses do not establish co-ownership, because multiple independent wallets may exhibit identical characteristics by using the same or similar software.[19] Our amicus brief made the same point at Section I.C, and we showed an internal inconsistency in the government expert's own application of the behavioral heuristic to Groups A and B of the pre-launch blockchain transactions for Bitcoin Fog.[20]

If you use the same wallet software as someone under investigation, you could be implicated simply on the basis of this type of wallet label clustering as well, even if you had nothing to do with the alleged illicit activity.

4.5 The plural of anecdote is not data

In Section 5.2 of the ontology, Chainalysis requires four procedural commitments for any structural claim. It demands documented methodology, enumerated failure modes, documented safeguards for each failure mode, and reproducible results. In Section 6.3, the ontology calls for error rates to be reported separately against ground truth, with a number for how often the grouping is right, a number for how much of the real entity it captures, and a number for how often the attached name is correct (structural precision, structural coverage, and attribution accuracy).[21]

Roman's trial record contained none of this.

Instead, at the *Daubert* hearing, the Chainalysis witness testified that she was not aware of a single false positive across hundreds of investigations. When the court itself asked whether Chainalysis collects any information about error rates or false positives, the Chainalysis witness answered, "Not to my knowledge."[22]

Yet under the framework Chainalysis now proposes, that is not an error rate. It is an anecdote, precisely what our amicus brief said it was, citing the National Academy of Sciences' warning that conformance with a checklist does not establish reliability.[23]

[19] *Defining the Cluster* (note 11), Section 4.3.1, https://www.chainalysis.com/reports/defining-the-cluster/

[20] ChainArgos Amicus Br. (note 6) at 23-24, Section I.C, and Appendix A, Figure 1, https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208778227.0.pdf

[21] *Defining the Cluster* (note 11), Sections 5.2 and 6.3, https://www.chainalysis.com/reports/defining-the-cluster/

[22] *Daubert* Hearing Transcript (note 3) at 117, https://storage.courtlistener.com/recap/gov.uscourts.dcd.232431/gov.uscourts.dcd.232431.224.0.pdf

[23] ChainArgos Amicus Br. (note 6) at 12, discussing National Research Council, *Strengthening Forensic Science in the United States: A Path Forward* (2009), https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208778227.0.pdf

> **Whenever a theory appears to you as the only possible one, take this as a sign that you have neither understood the theory nor the problem which it was intended to solve.**
>
> **Karl Popper**

5. Courtroom-Ready, Two Weeks Later

On July 13, 2026, two weeks after the ontology, Chainalysis published a marketing post titled *Courtroom-Ready Analytics: How Chainalysis Met the Daubert Standard*.[24] The post states that Chainalysis is "the first and only blockchain analytics provider to successfully meet the Daubert standard" and that "the judge held that Chainalysis' blockchain analytics was reliable and admissible as substantive evidence in the Sterlingov case." In fairness, it carries a version of the caveat from Section 2.1 of the ontology, acknowledging that the ruling "does not validate every blockchain analytics provider." It does not mention however that the ruling in *Sterlingov* is on appeal, nor that the D.C. Circuit heard argument on that appeal in May.

> **"Chainalysis is the first and only blockchain analytics provider to successfully meet the Daubert standard."**
>
> **Chainalysis, *Courtroom-Ready Analytics: How Chainalysis Met the Daubert Standard*, July 13, 2026**

Published by Chainalysis two weeks after the ontology, while the Sterlingov appeal was still awaiting a decision. The same Chainalysis post also conceded that Reactor "had not been peer reviewed at the time of the [Sterlingov] hearing."

[24] Chainalysis, *Courtroom-Ready Analytics: How Chainalysis Met the Daubert Standard* (July 13, 2026), https://www.chainalysis.com/blog/chainalysis-daubert-standard-sterlingov/

info@chainargos.com

The Chainalysis post walks through the four factors judges weigh under *Daubert*. Let's hold each one against the record of the trial Chainalysis celebrates.

- **Testability.** Chainalysis says the methodology is transparent enough that its conclusions can be independently verified.[25] At Roman's trial, the heuristics relied on to convict Roman were produced to the defense only under court protective orders that sharply limited who could examine them, the defense expert's review was never completed, and Chainalysis's position on appeal remains that source-level review would have been inappropriate.

- **Peer review.** Chainalysis concedes that its Reactor software "had not been peer reviewed at the time of the hearing" and points to a study that "attested to its precision in 2025."[26] The *Daubert* hearing was in 2023. Roman was convicted in early 2024. A study published after the verdict cannot have supported the testimony the jury heard.

- **Error rate.** Chainalysis's post answers with an FBI analyst who "had not encountered false positives in his experience," plus conservative design framed as a feature rather than a bug. The ontology's own Section 6.3 requires separately reported error rates against ground truth. At the *Daubert* hearing, the court asked directly whether Chainalysis collects error-rate or false-positive information. The answer was no.[27]

- **General acceptance.** Chainalysis points to widespread adoption by law enforcement and financial institutions. However, adoption measures popularity, not accuracy. The ontology itself, in Section 2.1, says the ruling of the district court in *Sterlingov* validates only the methodology examined and the methodology, by Chainalysis's own account, "continues to evolve."[28]

Chainalysis is marketing its courtroom credentials on a record that, by its own newly published standards, was missing every element that makes an analytical claim trustworthy, namely documented methodology, enumerated failure modes, separately reported error rates, and independent examination.

We do not argue that blockchain tracing is useless. We argue that its outputs are worth exactly what the record behind them shows, and in the one case where the record was tested, the showing was manifestly inadequate.

[25] *Courtroom-Ready Analytics* (note 24), https://www.chainalysis.com/blog/chainalysis-daubert-standard-sterlingov/
[26] *Courtroom-Ready Analytics* (note 24), https://www.chainalysis.com/blog/chainalysis-daubert-standard-sterlingov/
[27] *Courtroom-Ready Analytics* (note 24), https://www.chainalysis.com/blog/chainalysis-daubert-standard-sterlingov/ *Daubert* Hearing Transcript (note 3) at 117, https://storage.courtlistener.com/recap/gov.uscourts.dcd.232431/gov.uscourts.dcd.232431.224.0.pdf
[28] *Courtroom-Ready Analytics* (note 24), https://www.chainalysis.com/blog/chainalysis-daubert-standard-sterlingov/ *Defining the Cluster* (note 11), at 5, https://www.chainalysis.com/reports/defining-the-cluster/

info@chainargos.com

6. Their Standards, Applied to Their Evidence

Take each standard Chainalysis published on June 29, 2026, and hold it against the record in *Sterlingov*. Every entry below comes from Chainalysis's own filings, testimony, and publications, and nothing has been added.

"These requirements closely mirror accepted factors for admissibility of expert testimony: testability, peer review, known error rates, and general acceptance."[29]	
WHAT THE RECORD IN *STERLINGOV* SAID No error rate was ever stated. Asked whether Chainalysis collects error-rate or false-positive information at all, its witness answered "**Not to my knowledge.**"[30]	WHAT CHAINALYSIS SAID LATER Reactor is "**highly accurate and testing has proved it.**"[31]
"A technique can be trusted only when no unaddressed failure mode remains."[32]	
WHAT THE RECORD IN *STERLINGOV* SAID The only ground-truth test in *Sterlingov* saw Chainalysis's software attribute four of five known Bitcoin Fog blockchain addresses to the cluster. The **20% miss** was never statistically characterized.[33]	WHAT CHAINALYSIS SAID LATER The miss was characterized as "**conservative design**," not an error rate requiring characterization.[34]

[29] *Defining the Cluster* (note 11), Section 5.2, https://www.chainalysis.com/reports/defining-the-cluster/
[30] Transcript of Motions Hearing, *United States v. Sterlingov*, No. 1:21-cr-00399 (D.D.C. June 23, 2023), ECF No. 224, at 117, 119-20, https://storage.courtlistener.com/recap/gov.uscourts.dcd.232431/gov.uscourts.dcd.232431.224.0.pdf
[31] Chainalysis Amicus Br. (note 5) at 13, https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208825487.0.pdf
[32] *Defining the Cluster* (note 11), Section 4.3.1, https://www.chainalysis.com/reports/defining-the-cluster/
[33] ChainArgos Amicus Br. (note 6) at 24-25, https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208778227.0.pdf
[34] Chainalysis Amicus Br. (note 5) at 24-25, https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208825487.0.pdf

info@chainargos.com

"[P]roviders who resist invite the inference that their claims cannot survive the decomposition."[35]

WHAT THE RECORD IN *STERLINGOV* SAID	WHAT CHAINALYSIS SAID LATER
Heuristics were produced to the defense **only under protective orders**. The defense expert's review of them was never completed. The source code was never examined.[36]	Source-level review would be inappropriate. An expert using software need not know its workings, **like an economist using Excel without reading its formulas**.[37]

"Fingerprints without a transactional link between addresses does not establish co-ownership, as multiple independent wallets may exhibit identical characteristics by using the same or similar software."[38]

WHAT THE RECORD IN *STERLINGOV* SAID	WHAT CHAINALYSIS SAID LATER
The behavioral heuristic stood behind the bulk of the 925,743-address cluster, presented as a single undifferentiated fact. Its stated support was that it is "**provable because it's done and replicated time and time again and very reliable**," with no study of its accuracy cited.[39]	Peel chaining, a method that links addresses by following the leftover change from each payment, which "**undergirds**" the behavioral heuristic, has been "**reviewed and accepted**" in the community.[40]

"[A] Daubert ruling only validates the specific methodology examined, not the field, and not other providers' implementations."[41]

WHAT THE RECORD IN *STERLINGOV* SAID	WHAT CHAINALYSIS SAID LATER
The 2023 hearing examined one version of a methodology that, per the ontology itself, "**continues to evolve**." The study said to attest Reactor's precision arrived in 2025, **after the trial verdict**.[42]	Chainalysis is "**the first and only blockchain analytics provider to successfully meet the Daubert standard**."[43]

[35] *Defining the Cluster* (note 11), Section 7.2, https://www.chainalysis.com/reports/defining-the-cluster/
[36] See Sections 5 and 7 of this case study.
[37] Chainalysis Amicus Br. (note 5) at 21-22, https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208825487.0.pdf
[38] *Defining the Cluster* (note 11), Section 4.3.1, https://www.chainalysis.com/reports/defining-the-cluster/
[39] Transcript of Motions Hearing, *United States v. Sterlingov*, No. 1:21-cr-00399 (D.D.C. June 23, 2023), ECF No. 224, at 126-28, https://storage.courtlistener.com/recap/gov.uscourts.dcd.232431/gov.uscourts.dcd.232431.224.0.pdf
[40] Chainalysis Amicus Br. (note 5) at 18, https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208825487.0.pdf
[41] *Defining the Cluster* (note 11), Section 2.1, https://www.chainalysis.com/reports/defining-the-cluster/
[42] *Defining the Cluster* (note 11), at 5, https://www.chainalysis.com/reports/defining-the-cluster/ *Courtroom-Ready Analytics* (note 24), https://www.chainalysis.com/blog/chainalysis-daubert-standard-sterlingov/
[43] *Courtroom-Ready Analytics* (note 24), https://www.chainalysis.com/blog/chainalysis-daubert-standard-sterlingov/

- **In February 2026, Chainalysis told the court its software is highly accurate and that testing has proved it.** On June 29, 2026, its ontology says error rates must be reported separately, against ground truth, for every kind of claim. At the hearing that mattered, the Chainalysis witness could not state an error rate and, asked whether Chainalysis collects error-rate or false-positive information, answered "Not to my knowledge."[44]

- **In February 2026, Chainalysis described the 20% miss on the government's only ground-truth test as conservative design.** On June 29, 2026, its ontology requires enumerated failure modes with documented safeguards for each. The 20% miss was never characterized at all.[45]

- **In February 2026, Chainalysis argued that reviewing its methodology at the source level was unnecessary, like an economist using Excel.** On June 29, 2026, its ontology says credible methodology must be documented, auditable, reproducible, and open to adversarial scrutiny, and that providers who resist "invite the inference that their claims cannot survive the decomposition."[46] We agree.

- **In June 2023, the Chainalysis witness called the behavioral heuristic "provable because it's done and replicated time and time again and very reliable."** On June 29, 2026, its ontology excludes appearance-based methods from forensic claims entirely.[47]

- **In July 2026, a Chainalysis marketing post calls the company "the first and only blockchain analytics provider to successfully meet the Daubert standard."** The same post concedes that Reactor "had not been peer reviewed at the time of the hearing." The Chainalysis ontology says the ruling validates only the methodology examined.[48]

These positions cannot all be true at once.

[44] Chainalysis Amicus Br. (note 5) at 13, https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208825487.0.pdf
Defining the Cluster (note 11), Section 6.3, https://www.chainalysis.com/reports/defining-the-cluster/
Daubert Hearing Transcript (note 3) at 117, 119-20, https://storage.courtlistener.com/recap/gov.uscourts.dcd.232431/gov.uscourts.dcd.232431.224.0.pdf

[45] Chainalysis Amicus Br. (note 5) at 24-25, https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208825487.0.pdf
Defining the Cluster (note 11), Section 5.2, https://www.chainalysis.com/reports/defining-the-cluster/

[46] Chainalysis Amicus Br. (note 5) at 21-22, https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208825487.0.pdf
Defining the Cluster (note 11), Sections 5.2, 7.1, and 7.2, https://www.chainalysis.com/reports/defining-the-cluster/

[47] *Daubert* Hearing Transcript (note 3) at 127-28, https://storage.courtlistener.com/recap/gov.uscourts.dcd.232431/gov.uscourts.dcd.232431.224.0.pdf
Defining the Cluster (note 11), Sections 4.3.1 and 5.4, https://www.chainalysis.com/reports/defining-the-cluster/

[48] *Courtroom-Ready Analytics* (note 24), https://www.chainalysis.com/blog/chainalysis-daubert-standard-sterlingov/
Defining the Cluster (note 11), Section 2.1, https://www.chainalysis.com/reports/defining-the-cluster/

info@chainargos.com

Either the ontology's requirements are what trustworthy blockchain tracing demands, in which case the evidence presented in Roman's trial did not meet them, or the record in Roman's trial was sufficient, in which case the ontology's requirements are aspirational but unnecessary.

The ontology and the February 2026 brief both carry the name "Chainalysis."

So which is it?

Measured by the standards Chainalysis itself published on June 29, 2026, the evidence Chainalysis defended in February 2026 does not qualify as science. That is not our characterization. It follows necessarily from Chainalysis's own documents and public statements.

7. The Questions Chainalysis Says Every Provider Must Answer

In Section 7.1 of the ontology, Chainalysis proposes that any blockchain tracing provider should be able to answer three questions about any cluster it produces.

1. By what method were these addresses grouped, and does that method meet the structural soundness standard?

2. What evidence supports the attribution, and is it separable from the structural claim?

3. Has the operator-beneficiary relationship been assessed?[49]

In Section 7.2 of the ontology, Chainalysis goes further and writes that "providers who resist invite the inference that their claims cannot survive the decomposition."[50]

"None of these questions require disclosing proprietary methods. They require describing the nature of claims using shared vocabulary. We welcome these questions about our own work. Providers doing rigorous work should welcome them too; providers who resist invite the inference that their claims cannot survive the decomposition."[51]

Defining the Cluster: A Formal Ontology for Blockchain Address Analysis and Intelligence Claims
(Chainalysis, June 29, 2026)

[49] *Defining the Cluster* (note 11), Section 7.1, https://www.chainalysis.com/reports/defining-the-cluster/
[50] *Defining the Cluster* (note 11), Section 7.2, https://www.chainalysis.com/reports/defining-the-cluster/
[51] *Defining the Cluster* (note 11), Section 7.2, https://www.chainalysis.com/reports/defining-the-cluster/

info@chainargos.com

That paragraph describes the procedural history of *Sterlingov*.

Access to the heuristics underlying the Bitcoin Fog blockchain address cluster was available to the defense only under protective orders that excluded the practitioners most capable of evaluating them. The defense expert's review of the heuristic information was never completed, and Chainalysis's amicus brief maintains, in 2026, that reviewing the operative methodology at the source level would not have been appropriate at all, because an expert using software need not understand how that software works.[52]

One cannot simultaneously hold that the line-by-line operation of a software tool is irrelevant and that the industry's credibility depends on methodology that is documented, auditable, reproducible, and open to adversarial scrutiny.[53]

Excel's formulas are published, standardized, and independently verifiable by anyone. That is why the economist need not inspect them. It is not an argument for shielding proprietary heuristics from the defense in a criminal trial. It is an argument for publishing them.

[52] Chainalysis Amicus Br. (note 5) at 21-22, https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208825487.0.pdf

[53] Chainalysis Amicus Br. (note 5) at 22, https://storage.courtlistener.com/recap/gov.uscourts.cadc.41492/gov.uscourts.cadc.41492.01208825487.0.pdf *Defining the Cluster* (note 11), Sections 5.2 and 7.1, https://www.chainalysis.com/reports/defining-the-cluster/

The game of science is, in principle, without end. He who decides one day that scientific statements do not call for any further test, and that they can be regarded as finally verified, retires from the game.

Karl Popper

8. What This Means for You

If you simply hold or receive stablecoins. You do not need to trade crypto-assets for a label to affect you. If blockchain tracing software has incorrectly grouped one of your counterparties with illicit activity, the payment they send you can be enough to freeze your account, and the freeze arrives with no explanation you can check. The standard Chainalysis itself has now published, that a provider must be able to show how any blockchain address label was produced, is your protection too.

If you rely on blockchain tracing for compliance or risk. The three questions in Section 7.1 of the ontology are now your vendor-diligence checklist, written by the largest vendor in the industry. When your provider labels a blockchain address, can it surface the underlying method and reasoning, or only the conclusion? Is the attribution separable from the structural grouping, so a revised attribution does not silently invalidate your exposure calculations? Are outputs version-stamped, so a screening decision made today can be reconstructed when a regulator questions it next year? A blockchain address label you cannot examine is one you cannot defend.

If you or your clients face cluster evidence. Chainalysis's own ontology now says that a blockchain address cluster fuses three distinct claims, that trained models cannot produce forensic structural claims, and that an unexamined blockchain address label is a conclusion rather than evidence. When a witness testifies that a blockchain address "belongs to" a cluster, Chainalysis's own published framework supports asking which claim is being made, on what method, with what documented failure modes, and to what error rate.

If you supervise, regulate, or study this field. Standards are arriving, which is welcome, but they are arriving by vendor self-publication, after the fact, while a federal appeal turning on exactly these questions has been argued and awaits decision. A methodology standard authored and graded by the largest incumbent is a starting point for a conversation, not the end of one. Documents like the ontology deserve to be treated as proposals to be tested, not standards to be adopted.

info@chainargos.com

Let us be clear about what this case study does not argue. We do not suggest Chainalysis's ontology is wrong. Much of it is right, and parts of it are genuinely well done. The separation of hard on-chain facts from confidence-graded intelligence claims is the correct architecture. The exclusion of trained models from forensic claims is the correct line. The demand for enumerated failure modes and separately reported error rates is exactly what forensic science requires, and it is exactly what ChainArgos has built its methodology around since inception, using established mathematics, independently reproducible results, and no heuristic edges.

Our point is about the record, and about what the record means for everyone who relies on blockchain tracing.

Roman Sterlingov is serving a 12.5-year sentence built almost entirely on blockchain tracing that was presented to the jury as a single, undifferentiated fact. That evidence used vocabulary Chainalysis now says the industry must abandon. It was produced by methods whose failure modes were never enumerated in the record. It was tested against ground truth exactly once, and it missed one address in five, a rate no one ever characterized. And it was shielded from the adversarial scrutiny that the Chainalysis ontology now describes as the test of whether claims based on blockchain tracing deserve trust. Two weeks after publishing that ontology, Chainalysis marketed Roman's conviction as proof that its blockchain analytics are courtroom-ready.

If the ontology's requirements are the right ones, and we believe they are, then they were also the right ones in June 2023, when Roman's *Daubert* hearing was held, and in February 2024, when the jury deliberated. Chainalysis cannot argue that the ontology's framework is urgent enough to publish now and at the same time irrelevant to the appeal in which Chainalysis itself is an amicus.

The cluster label at issue in *Sterlingov* is the same kind of label that decides, every day, whose transaction clears, whose account freezes, and whose funds are seized. That includes the stablecoin balances that more and more people treat as ordinary money. As more assets move on-chain, more people stand on the receiving end of conclusions they cannot examine, let alone challenge. Chainalysis has now written down what those conclusions must look like to deserve trust. Whether its own outputs have ever met that standard is a question the record does not answer in its favor.

info@chainargos.com

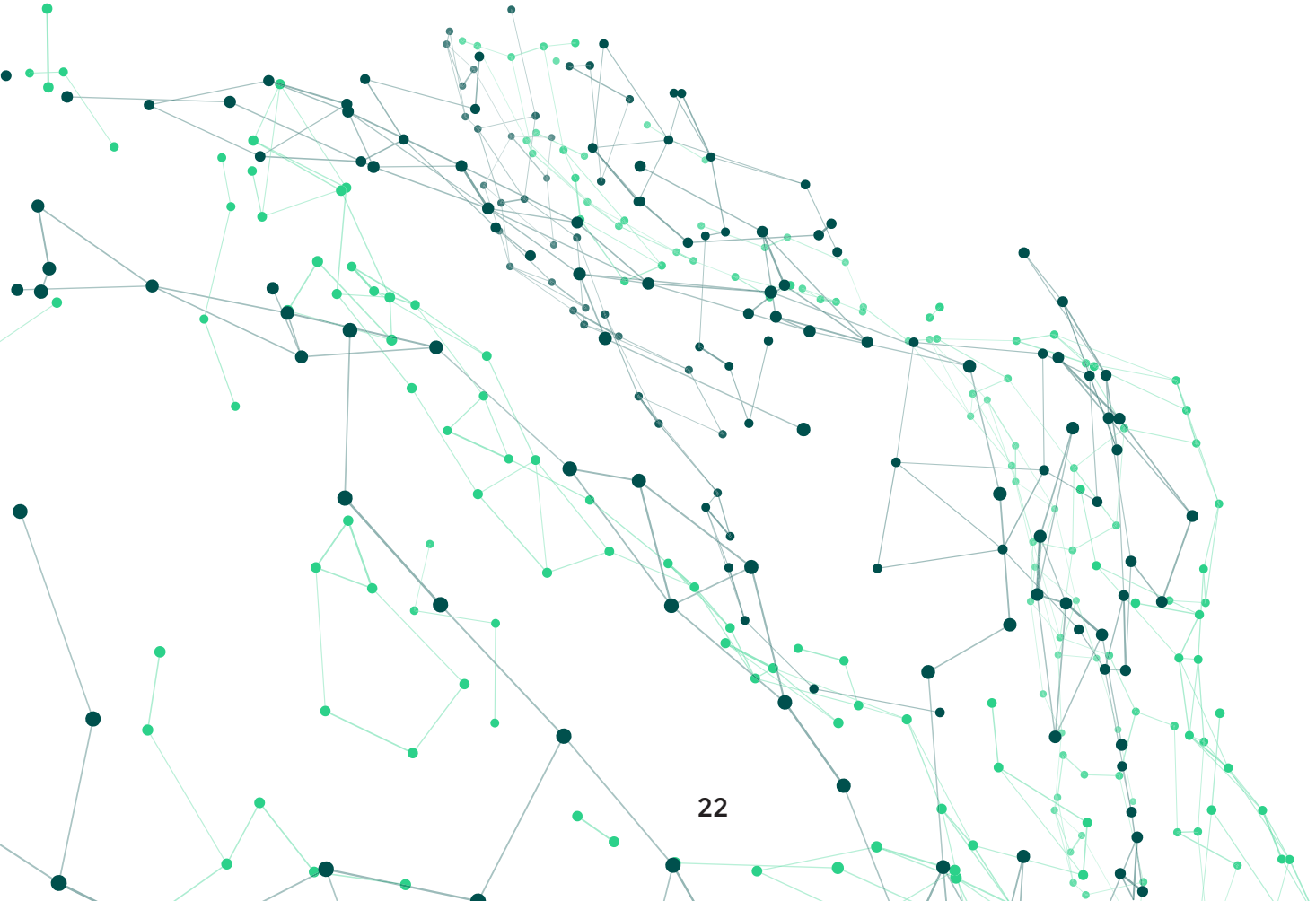
Who are we?

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

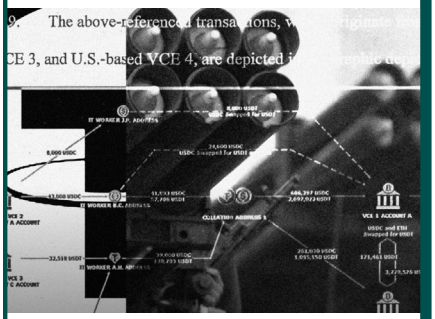
Binance Acknowledges Past Flaws in Maintaining Stablecoin Backing

- 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 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.

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.

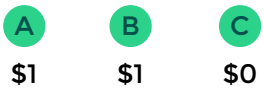


Fig. 1

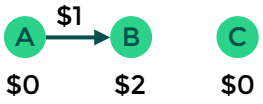


Fig. 2

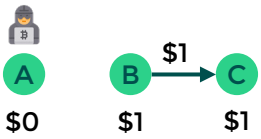


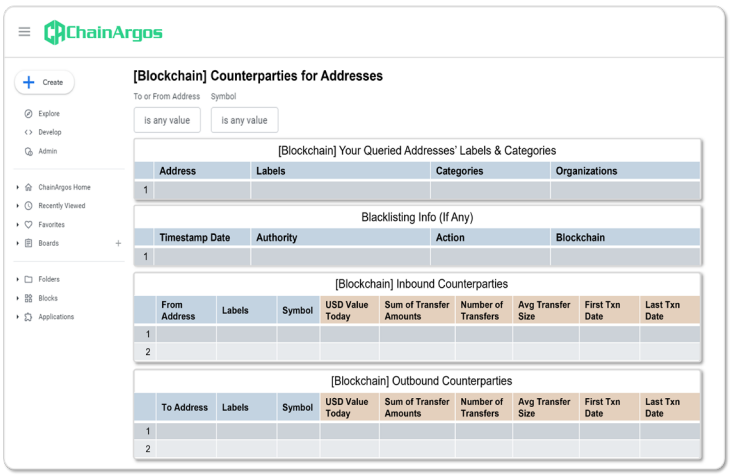
Fig. 3

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 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.

info@chainargos.com