ChainArgos.com

Better blockchain intelligence.

How effective is blacklisting?

A CASE STUDY OF TETHER'S BLACKLISTING TRACK RECORD WITH DATA SUPPLIED TO THE WALL STREET JOURNAL

SEPTEMBER 17, 2024

Contents.

info@chainargos.com

Introduction

In the movie “Minority Report” Tom Cruise stars as Precrime Chief John Anderton who heads a specialized police department that apprehends criminals using foreknowledge provided by three psychics called “precogs”.

The idea of course is that psychics are able to predict when someone is going to commit a crime before they’ve actually done it, and therefore the *mens reus*, or intent alone, is sufficient to secure a conviction.

Fortunately, most legal systems do not operate this way.

Instead both the *mens reus* or intent to commit a crime needs to be combined with the *actus reus* or the actual criminal act, to constitute the crime alleged.

This is what makes the process of “blacklisting” blockchain addresses so challenging.

In this case study, we examine the stablecoin issuer Tether’s track record of “blacklisting” blockchain addresses, and provide data that was also supplied to the Wall Street Journal^, to provide a data-driven overview on the efficacy of “blacklisting”.

^ Please see “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” by Angus Berwick and Ben Foldy for the Wall Street Journal, September 10, 2024.

Available at the Wall Street Journal website:

https://www.wsj.com/finance/currencies/tether-crypto-us-dollar-sanctions-52f85459

info@chainargos.com

What is “blacklisting”?

There are two types of blockchain address “blacklisting”.

Freezing

“Freezing” is when crypto-assets or stablecoins in a blockchain address can no longer be transferred after the “blacklisting” has been implemented, usually by the centralized issuer of that crypto-asset or stablecoin.

One common misconception is that when a blockchain address has been “blacklisted” all of the crypto-assets and stablecoins in that blockchain address are “frozen” and can no longer be transferred out of the blockchain address.

However, only the centrally-issued crypto-assets or stablecoins with a “blacklisting” function can be “frozen” by their issuer, while the blockchain address can continue to transact in other crypto-assets and stablecoins not subject to such “freezing.”

For instance, the stablecoin USDT is centrally-issued by Tether, and when a blockchain address is “frozen” or “blacklisted” by Tether, only the stablecoin USDT can no longer be transferred out from that blockchain address.

If someone attempts to transfer USDT out of a blockchain address “blacklisted” by Tether, when their blockchain address makes a call to the smart contract operated by Tether, the administrative functions controlled by Tether prevent the USDT transfer.

However, other crypto-assets that are not USDT are not prevented from moving freely into and out of a blockchain address “blacklisted” by Tether.

For instance, ether, the native crypto-asset for the Ethereum blockchain, can continue to be transferred into and out of a blockchain address even after the address has been “blacklisted” by Tether.

Notification

Another type of “blacklisting” involves notification, usually by national or state authorities, that certain blockchain addresses are either subject to sanctions, or identified to be involved in illicit activity.

The Office of Foreign Assets Control for instance states clearly in its “blacklisting” of blockchain addresses that the provision of that information is intended as a convenience, and not intended to “be exhaustive”[#].

While a national or state authority may “blacklist” a blockchain address, crypto-assets and stablecoins in that “blacklisted” blockchain address can still be freely transferred unless the crypto-asset or stablecoin issuer has measures in place to “freeze” the asset or stablecoin, and does so.

[#] Office of Foreign Asset Control website: https://ofac.treasury.gov/faqs/562

info@chainargos.com

How much “freezing” does Tether do?

It is important to note that many crypto-asset issuers do not design their products to cater for “freezing”.

Blockchain networks are generally intended to facilitate permissionless transactions, with no central authority to block transfers. As such, the vast majority of crypto-assets are generally not susceptible to being “frozen”.

Nevertheless, centralized stablecoin issuers, such as Tether, do have in place systems to “freeze” their crypto-assets in specific blockchain addresses, but this usually only happens *after* those blockchain addresses have been identified as involved in illicit activity.

Number of Blockchain Addresses “Blacklisted” by Tether Since 2018

Figure 1. shows the number of blockchain addresses “blacklisted” by Tether between January 1, 2018 and August 31, 2024 on the Ethereum and TRON blockchain networks by date.

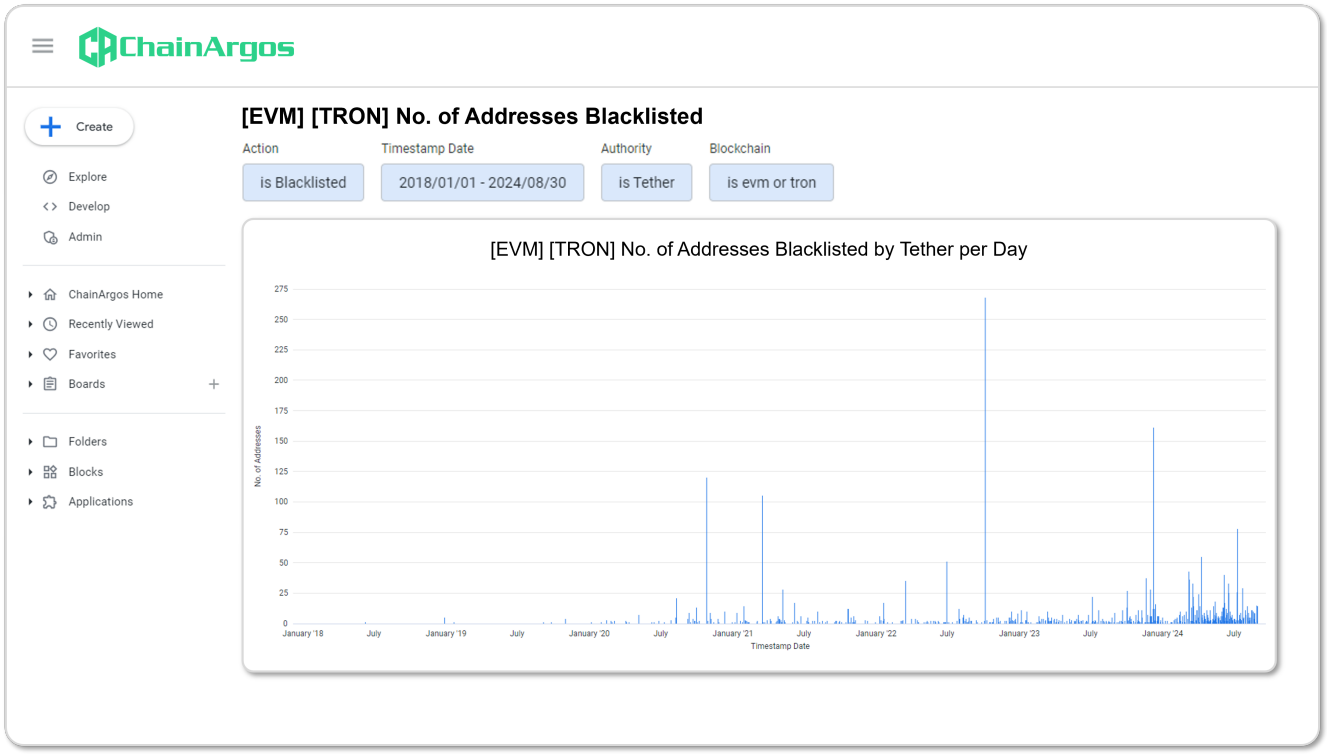


Figure 1. No. of Blockchain Addresses Blacklisted by Tether by Date on the Ethereum and TRON blockchain networks.

info@chainargos.com

The chart in Figure 1. provides some interesting observations.

For instance, the largest number of blockchain addresses “blacklisted” by Tether was October 6, 2022, when 268 blockchain addresses were “blacklisted.”

And while Tether has “blacklisted” blockchain addresses from time to time, the “blacklisting” activity really picked up in 2024.

The following chart in Figure 2. shows the number of blockchain addresses blacklisted by Tether monthly, from January 1, 2018, to August 31, 2024.

Again, October 2022 stands out, where a total of 282 blockchain addresses on the Ethereum and TRON blockchain networks were “blacklisted” by Tether.

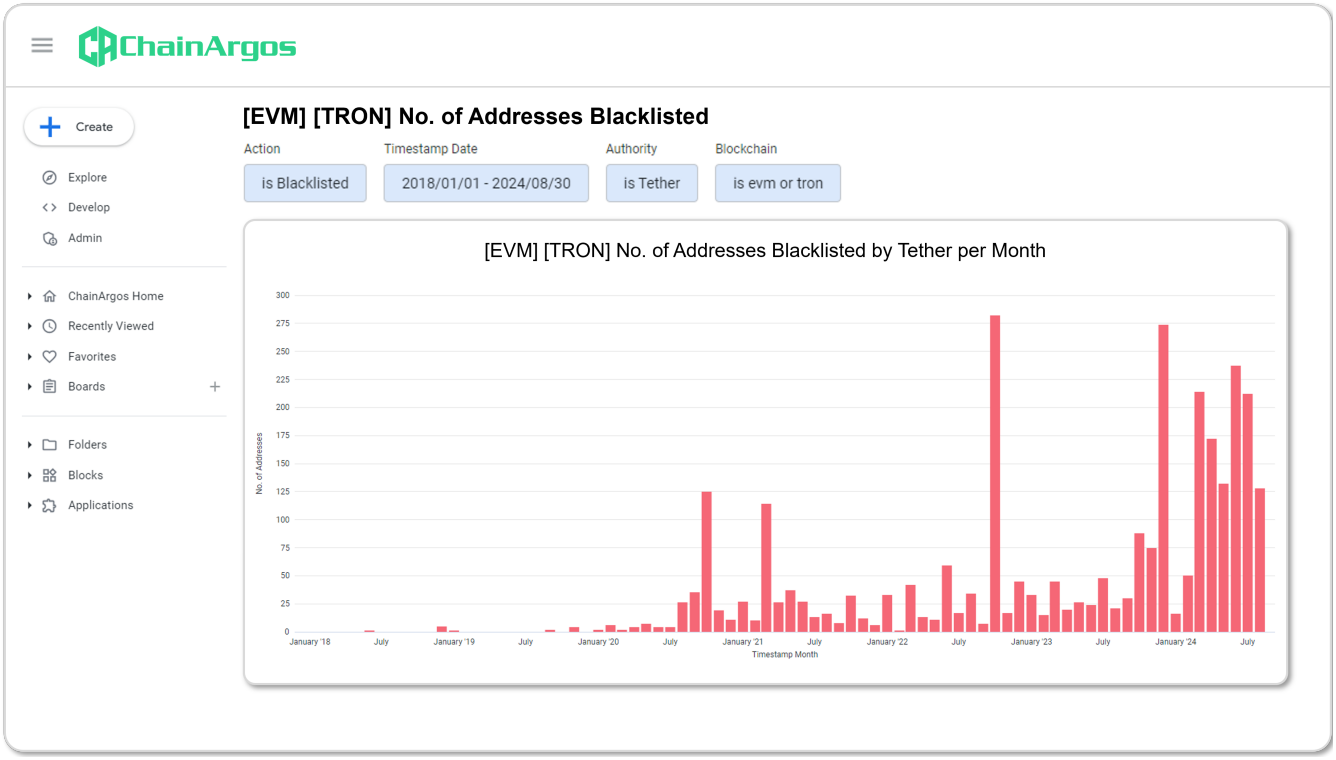


Figure 2. No. of Blockchain Addresses Blacklisted by Tether by Month on the Ethereum and TRON blockchain networks.

It is one thing to “blacklist” a blockchain address, but transaction data seems to suggest that it is far more difficult to trap supposedly illicit USDT flows through that blockchain address - the proverbial closing of the barn door after the horse has already bolted.

info@chainargos.com

How much Tether was “frozen”?

The amount of USDT that effectively gets caught when a blockchain address is “frozen” varies significantly from blockchain to blockchain.

Blockchain network transaction data from the Ethereum and TRON blockchain networks between January 1, 2018 and August 31, 2024, is presented in Figure 3.

Blockchain	No. of Addresses Blacklisted	Total Received	Total Sent	Amount Frozen	Frozen as % of Total Received
TRON	1,699	$149.8 billion	$149.1 billion	$730.9 million	0.49%
Ethereum	1,760	$5.26 billion	$4.26 billion	$1.01 billion	19.2%

Figure 3. Tether Blacklisting figures between January 1, 2018 and August 31, 2024.*

In Figure. 3, the sheer volume of USDT flowing through blockchain addresses “blacklisted” by Tether on the TRON blockchain network completely dwarfs the USDT volumes through the Ethereum blockchain network.

That there is more USDT flowing through blockchain addresses that are “blacklisted” by Tether on the TRON blockchain network should come as no surprise, as in general, there are far more transactions for USDT on TRON than on Ethereum.

Transaction fees are significantly lower for USDT on TRON than on Ethereum, which is why many choose to transact USDT on the TRON blockchain network, instead of Ethereum.

Regardless, the amount of USDT Tether has been able to “freeze” on different blockchain networks also differs dramatically.

On the TRON blockchain network, Tether only managed to “freeze” around 0.49% of all inbound USDT to “blacklisted” blockchain addresses, meaning a whopping 99.51% of possibly illicit USDT made it through.

Whereas Tether has had far more success “freezing” USDT on the Ethereum blockchain network, with almost 1 in 5 USDT flowing into “blacklisted” blockchain addresses successfully “frozen”.

The observations are not intended to be a criticism of Tether, but rather to highlight the difficulty involved with trying to “freeze” illicit fund flows in a permissionless environment.

* Please note that the Wall Street Journal data covers the period from January 1, 2018 to June 30, 2024. In this case study, we have expanded the time frame from January 1, 2018 to August 31, 2024. USDT values have not been rounded up or down and totals are inexact. The “Total Received” and “Total Sent” refer to USDT totals received by and sent from blockchain addresses ultimately “blacklisted” by Tether.

info@chainargos.com

Does transaction behavior change before “blacklisting” by Tether?

Figure 4. takes a look at USDT flows out of blockchain addresses up to 90 days before they are “blacklisted” by Tether on the Ethereum blockchain network.

It is clear that in the week or so before a blockchain address is “blacklisted” by Tether, there is both an increase in the number of unique transactions, as well as the volume of USDT being transferred out.

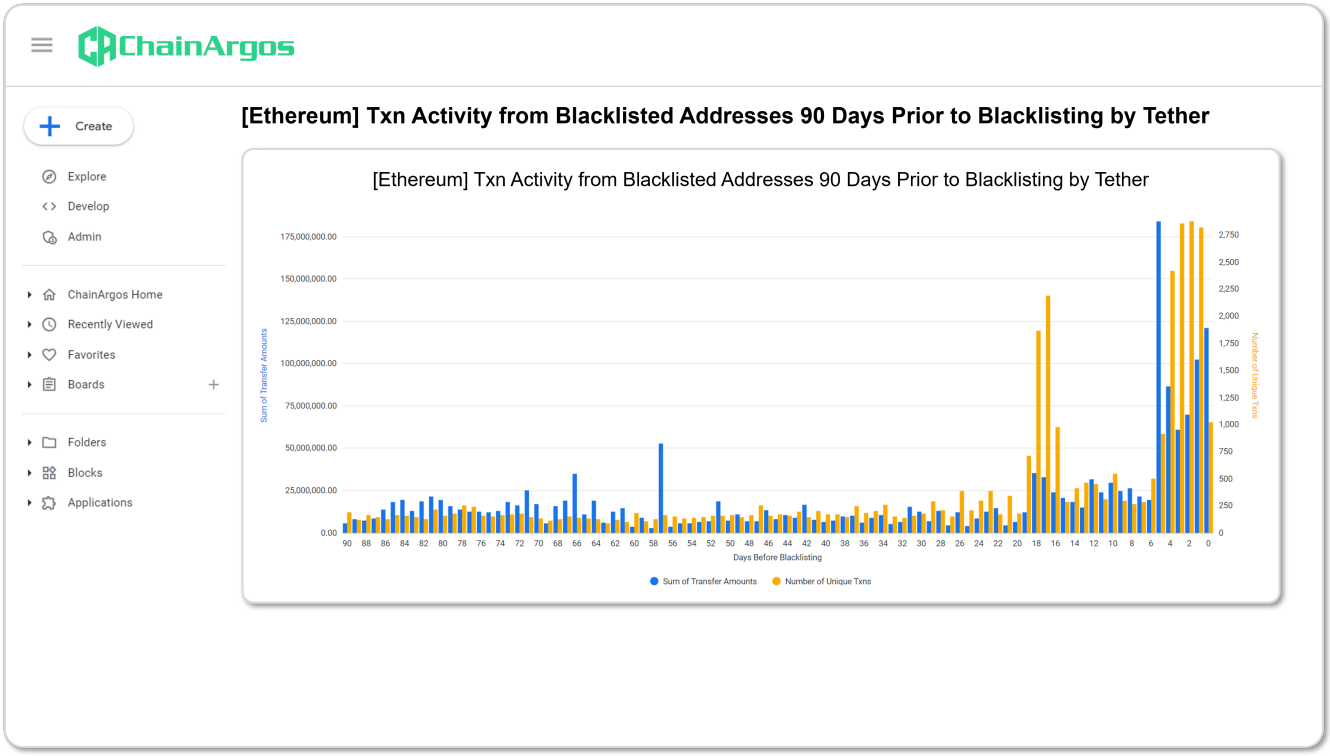


Figure 4. Sum of USDT Transfers and No. of Unique Transactions to 90 days before “blacklisting” by Tether on the Ethereum blockchain network.

In Figure 4., the yellow bars represent the number of unique transactions from a blockchain address on the Ethereum blockchain network that will eventually be “blacklisted” by Tether. The blue bars represent the sum of transfer amounts of USDT.

“Unique transactions” means the transaction count. There is a significant increase in transactions in the week just before the blockchain address is “blacklisted” by Tether.

It is obvious that on the Ethereum blockchain network, blockchain addresses that face imminent “blacklisting” see a significant increase in both amounts and unique transactions just before their USDT is “frozen” by Tether.

info@chainargos.com

This in no way implies any impropriety or information leakage on the part of Tether to these blockchain addresses before their USDT is “frozen.”

For instance, citizens of a city fleeing ahead of an air strike, doesn’t necessarily imply that news of an imminent attack has been leaked, but rather a general awareness that dangers lay on the horizon in a time of conflict.

It’s entirely possible that owners of these blockchain addresses ultimately “frozen” by Tether were aware of impending law enforcement action and were moving funds as quickly as possible to prevent them from being lost to “freezing”.

Figure 5. examines USDT transaction activity 90 days before Tether “freezes” these blockchain addresses on the TRON blockchain network.

Again we see the same sort of uptick in transaction volumes and unique transactions, just prior to “blacklisting” by Tether on the TRON blockchain network as was observed on the Ethereum blockchain network.

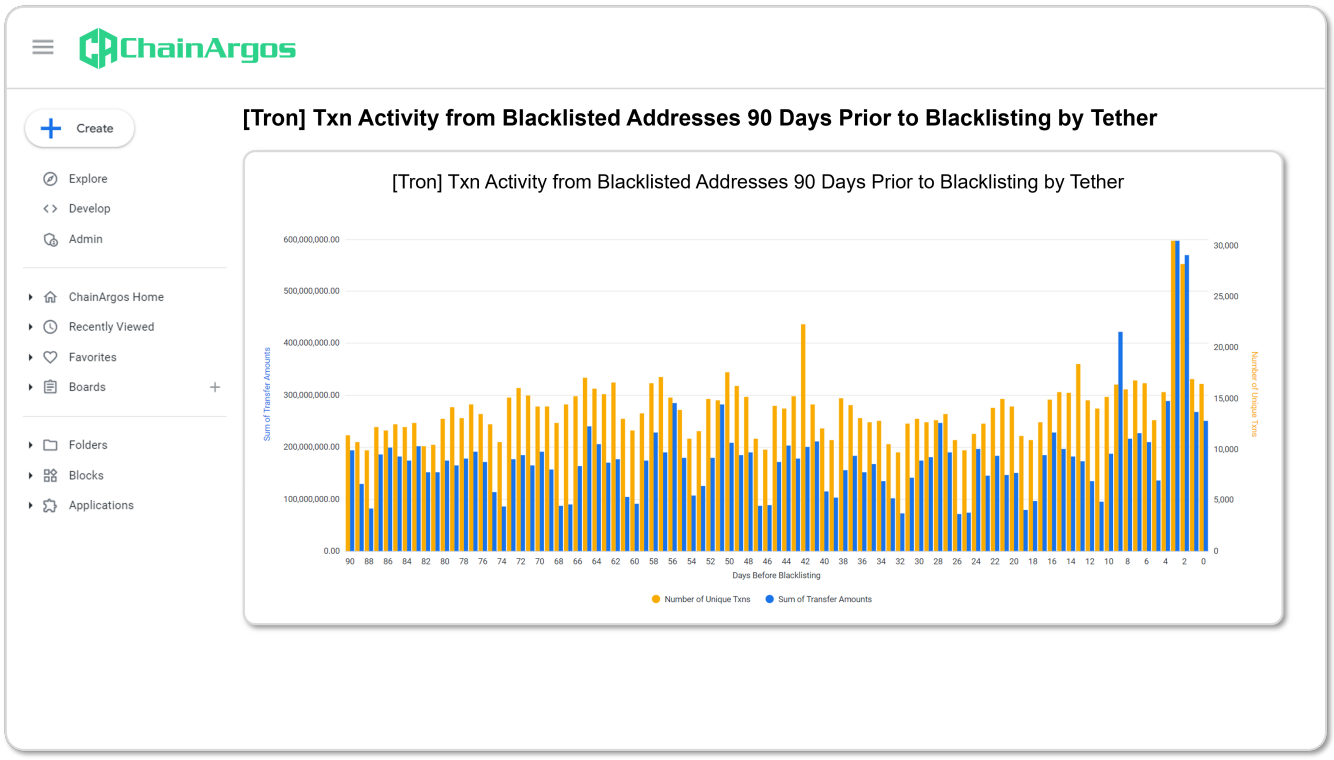


Figure 5. Sum of USDT Transfers and No. of Unique Transactions to 90 days before “blacklisting” by Tether on the TRON blockchain network.

info@chainargos.com

Can we do better?

The data reviewed suggests that if the goal of "blacklisting" is to stop the flow of illicit funds, then "blacklisting" may not be the best way to do it.

While it may be possible for Tether to pre-emptively and pro-actively "freeze" blockchain addresses it suspects are involved in illicit activity, or will *potentially* be involved in illicit activity, doing so reliably assumes Tether has access to "precogs".

The problem is exacerbated by the fact that it's trivial for nefarious actors to create new blockchain addresses, staying one step ahead of "blacklisting" in a neverending cat-and-mouse game that issuers like Tether are ill-equipped to win.

This issue isn't as pronounced in the traditional financial system as banks are heavily regulated, licensed entities, which generally have in place frameworks that are designed to prevent and stop illicit fund flows.

For instance, it's not trivial to open a single bank account on one day, let alone multiple bank accounts by the same individual on a single day.

While some may argue the ability to open bank accounts quickly is disadvantageous from the perspective of efficiency, there are clearly advantages in the context of compliance with existing regulations.

More importantly, banks and financial institutions operate in a highly "permissioned" environment, where transfers require interemediaries that act as chokepoints, to prevent uncontrolled illicit flows.

However, crypto-assets and stablecoins operate on "permissionless" blockchain networks, with no central intermediaries.

No system is perfect of course.

But the empirical evidence is compelling that a system of "permissionless-access with backward-looking blacklisting" is meaningfully ineffective in stopping, or trapping, illicit funds. Further, it is clear this is not a minor shortcoming that can be fixed with incremental technical upgrades but rather an in-built feature of richly programmable permissionless systems that necessitate compromise[+].

In this context regulators, policymakers, and law enforcement should consider whether the current permissionless system's performance merits official approval or if a different approach is required.

[+] For a more detailed discussion on compliance frameworks in permissionless systems, please see Charoenwong, Ben and Kirby, Robert M. and Reiter, Jonathan, Decentralized Finance and Financial Regulation: Limits On Mutable Turing Machines (March 6, 2024).

Available at SSRN: https://ssrn.com/abstract=4597651 or http://dx.doi.org/10.2139/ssrn.4597651

info@chainargos.com

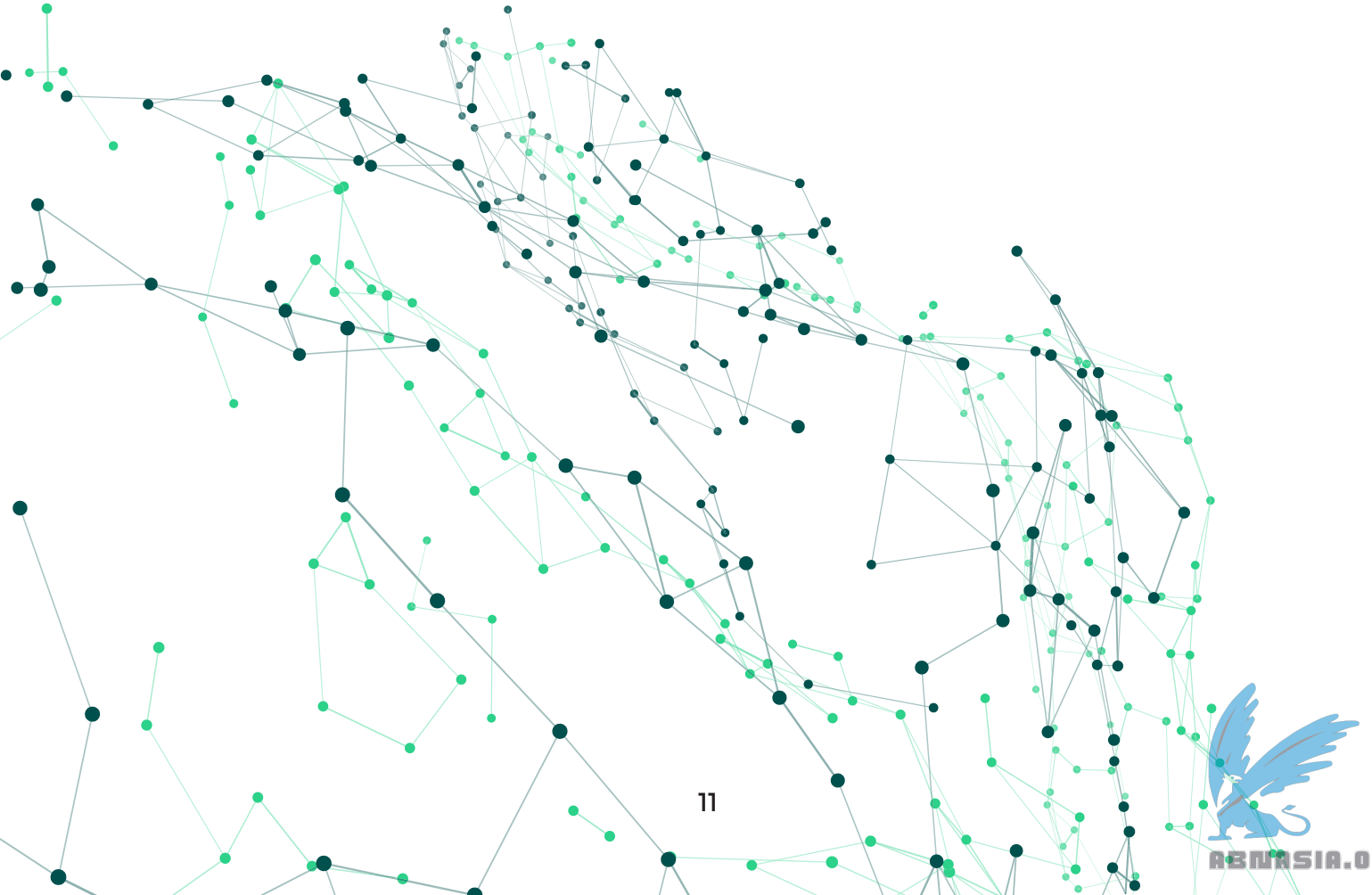
Who are we?

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.

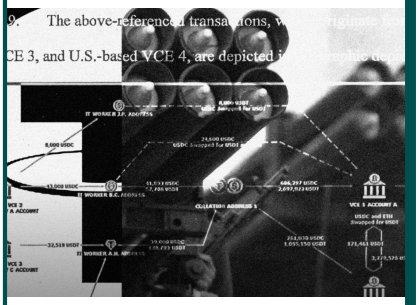
Here's just a selection of our blockchain intelligence that created news:

Bloomberg

Stablecoin Operator Moves $1 Billion in Reserves to Bahamas

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

THE WALL STREET JOURNAL.



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

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

South China Morning Post

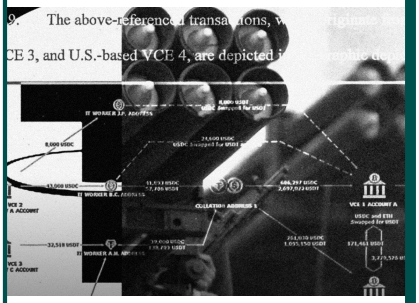
How crypto investigators uncover scammers' blockchain billions, scale of money laundering in Asia

THE WALL STREET JOURNAL.

The Shadow Dollar That's Fueling the Financial Underworld

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

THOMSON REUTERS®



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

Bloomberg

Binance Acknowledges Past Flaws in Maintaining Stablecoin Backing

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

info@chainargos.com

Who is this for?

Finance and Banking

Compliance

Law Enforcement

Regulators and Policymakers

Finance and Banking

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

Compliance

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

Law Enforcement

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

Regulators and Policymakers

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

How are we different?

We deliver actionable blockchain intelligence.

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

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

Whether you’re looking to on-board a customer, determine source of wealth, or ensure your evidence isn’t rejected on appeal, our blockchain intellignce 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.

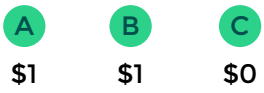


Fig. 1

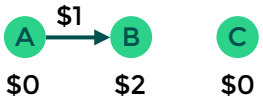


Fig. 2

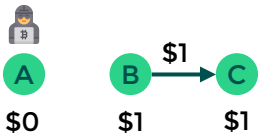


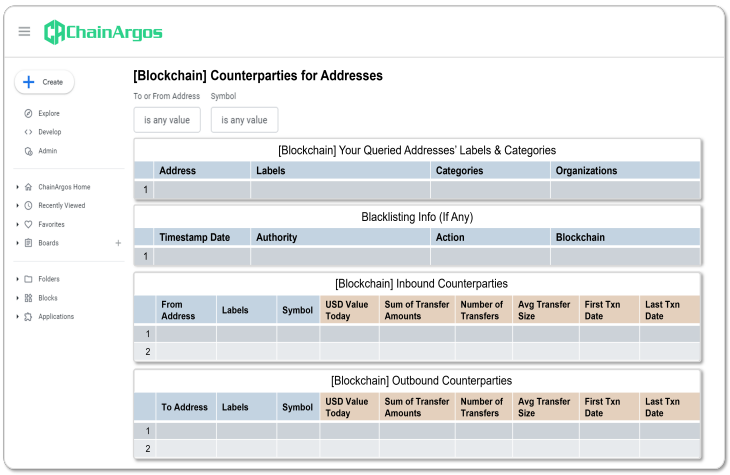
Fig. 3

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

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