

OPINION

Analyzing Trump's Crypto Executive Order

AN OPINION PIECE ON US PRESIDENT DONALD TRUMP'S
"STRENGTHENING AMERICAN LEADERSHIP IN DIGITAL
FINANCIAL TECHNOLOGY" EXECUTIVE ORDER

JANUARY 27, 2025



Contents.

Opinion	Introduction	3
	Purposes and Policies	4
	Protecting and Promoting the Freedom to Transact	4
	Freedom to Secure and Validate Blockchain Network Transactions	4
	Right to Self-Custody Crypto-assets	5
	Protecting and Promoting Fair and Open Banking Access	6
	Regulatory Clarity	7
	Well-Defined Jurisdictional Regulatory Boundaries	8
	No Dollar CBDC	9
	The Importance of Definitions	10
	“Distributed” vs “Decentralized”	10
	“Publicly Available” Source Code	11
	“Publicly Available” vs “Open-Source”	11
	Conclusion	12
About Us	Who are we?	14
	Featured Press	15
	Who is this for?	16
	How are we different?	17
	How do we do it?	18
	Better Attribution.	19

Introduction

In this opinion piece, our General Counsel Patrick Tan reviews US President Donald Trump's Presidential Executive Order entitled "Strengthening American Leadership in Digital Financial Technology"¹ ("EO") and breaks down the provisions to gather insight into the Trump administration's general direction on crypto-assets.

Provisions in the EO related to the repeal of previous Executive Orders and the creation of Working Groups have been disregarded for brevity and as they do not provide any substantive insight into the Trump administration's policy approach for crypto-assets.

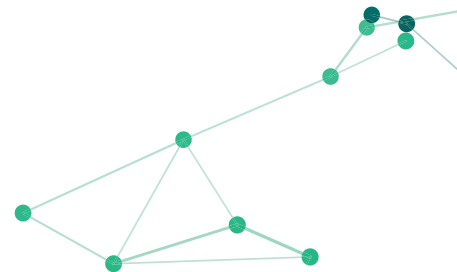
Analysis has been focused primarily on portions of the EO which are likely to guide the White House's policy initiatives in the immediate to medium term.

The absence of terms such as "decentralization" and "open-source" in the EO is telling, because it seems to envisage a future for blockchain technology where neither characteristics are required to fall under the Trump administration's definitions of this technology.

In summary, although the EO has limited practical implications, its provisions provide a glimpse into the Trump administration's perspective on crypto-assets and could serve to guide any proposed legislation for the sector put before Congress.



¹ <https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/>



Purposes and Policies

Section 1. Purposes and Policies

(i) protecting and promoting the ability of individual citizens and private-sector entities alike to access and use for lawful purposes open public blockchain networks without persecution, including the ability to develop and deploy software, to participate in mining and validating, to transact with other persons without unlawful censorship, and to maintain self-custody of digital assets;

Protecting and Promoting the Freedom to Transact

“Protecting and promoting the ability of citizens and private-sector entities alike to access and use for lawful purposes open public blockchain networks without persecution” simply means that blockchain networks and their access ought to be protected and promoted.

That right to access and use “public blockchain networks” is uncontroversial and from a practical standpoint, somewhat superfluous, because attempting to outlaw “lawful” use of a permissionless network would be akin to banning access to the Internet.

Freedom to Secure and Validate Blockchain Network Transactions

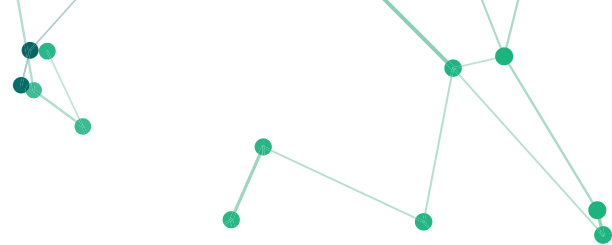
“To participate in mining and validating” is an interesting priority given that there are numerous blockchains for which one or both privileges do not exist, and it is unclear what the Trump administration’s stance on such blockchain networks is.

For instance, there are blockchains for which “validating” blockchain transactions is a carefully guarded privilege.

It is unclear what “unlawful censorship” could mean. For instance, if a wallet operator denied a user the ability to transact on a given blockchain network for undisclosed reasons, could this be interpreted as a “unlawful censorship”?

Conversely, lawful censorship of blockchain network transactions is contemplated by the Trump administration because surely there is no public interest served by facilitating illicit transactions on public blockchain networks.





Right to Self-Custody Crypto-assets

The right to hold crypto-assets in one's own capacity is uncontroversial, and to be sure, one that would be challenging to police in practice.

While the Trump administration appears to be promising Americans that their right to custody their own crypto-assets is sacrosanct, what is less clear is what happens when that chain of custody is broken.

For instance, there is no shortage of crypto-asset wallet providers claiming to facilitate the "self-custody" of a user's crypto-assets, but break that chain of "self-custody" when a user engages in a transaction such as swapping or staking crypto-assets.

In such cases, it is unclear and unlikely that the Trump administration intends to protect a crypto-asset wallet provider's right to custody crypto-assets on a user's behalf.

It is common for crypto-asset wallet providers to take custody of a user's crypto-assets when a user executes a swapping or staking transaction.

What typically happens is the user signs approvals handing over their crypto-assets to smart contracts or routers controlled by the crypto-asset wallet provider, which execute the transaction before returning a user their crypto-assets.

Even where transactions are "atomic," in other words they happen all at once, or not at all, the chain of custody is broken, even if momentarily. It does not appear the Trump administration's EO is intended nor ought to be interpreted as providing any form of protection for such activity and it is conceivable that existing licensing regimes would continue to apply.

Promoting and Protecting Dollar-backed Stablecoins

(ii) promoting and protecting the sovereignty of the United States dollar, including through actions to promote the development and growth of lawful and legitimate dollar-backed stablecoins worldwide;

This provision is consistent with current market conditions. The United States dollar is already the global reserve currency and promoting "dollar-backed stablecoins worldwide" can only help entrench the dollar's formidable hegemony.

What bears note however is the requirement that such "dollar-backed stablecoins" be "lawful and legitimate" which is open to a variety of interpretations.



Presumably, as envisaged by Coinbase CEO Brian Armstrong, a “lawful” and “legitimate” stablecoin could be backed by US Treasuries alone.²

It is less clear which stablecoins would not be considered “lawful” or “legitimate” and it is conceivable this could include stablecoins such as Tether, which has struggled to establish durable banking relationships and attracted no shortage of legal troubles.

Stablecoins without a “blacklisting” function, or the ability to stop illicit flows, are also unlikely to be the sort of stablecoin the Trump administration is looking to provide cover for and this would include the gamut of “permissionless” stablecoins with no freezing function.

Protecting and Promoting Fair and Open Banking Access

(iii) protecting and promoting fair and open access to banking services for all law-abiding individual citizens and private-sector entities alike;

Crypto-asset service providers have long struggled to establish and maintain durable banking relationships given the reticence of financial institutions to expose themselves to the risks inherent in the crypto-asset sector.

This provision of the EO provides for “law-abiding” individuals or entities to access banking services, but it is unclear whether the standard of a “law-abiding” alone is sufficient to compel a financial institution to provide such services.

Banks are for-profit businesses and access to banking services is not in and of itself an inalienable right.

It is entirely conceivable that banks may determine the compliance cost and reputational risk of providing banking services to a crypto-asset service provider are far in excess of the anticipated return and therefore refuse such service.

A bank has just as much right to determine it is not in their commercial interest to provide banking services to an individual or entity for any reason whatsoever and the mere denial of service in and of itself should not automatically be deemed arbitrary.

Just as a restaurant routinely refuses service to inappropriately dressed patrons, a bank should have the right to refuse the provision of financial services to an individual or entity they deem in their absolute discretion to be inappropriate for service.

² <https://www.wsj.com/livecoverage/stock-market-today-dow-sp500-nasdaq-live-01-21-2025/card/coinbase-would-delist-stablecoin-tether-if-required-by-law-ceo-says-YQjucrr0egRRssjPTCYh>

It is unclear how much this provision of Trump's EO can compel a financial institution to provide banking services.

Regulatory Clarity

(iv) providing regulatory clarity and certainty built on technology-neutral regulations, frameworks that account for emerging technologies, transparent decision making, and well-defined jurisdictional regulatory boundaries, all of which are essential to supporting a vibrant and inclusive digital economy and innovation in digital assets, permissionless blockchains, and distributed ledger technologies; and

It is unclear which crypto-asset regulations to date can be considered not “technology-neutral” but presumably the purpose of this provision is to establish regulatory frameworks that would not make value judgments with respect to “emerging technologies.”

In this regard, it is unclear whether different types of “consensus mechanisms” represent distinct “technologies” in the same way it isn't clear the distinction between a parliamentary and presidential democracy are different “technologies.”

While it is clear that a parliamentary and presidential democracy are two functionally distinct forms of government, it is not clear these structures could be defined as “technologies” and begs the question whether “consensus mechanisms” should even be treated as “technologies.”

To that end, what about degrees of “decentralization”? Can varying degrees of “decentralization” in and of themselves be considered distinct “technologies” and therefore regulations bent to ignore their variation?

Presumably, the purpose of “technology-neutral regulations” is to enable the promoters of decentralized finance (“DeFi”) to disintermediate the financial services industry without requiring licenses by claiming the same sort of exemptions that Airbnb and Uber once carved out for themselves from the hotel and taxi industries.

It's easy to forget, but not so long ago, the provision of temporary accommodation and taxi services was once a heavily regulated industry and for good reason.

Today, we spend little if any time, considering the dangers of living in a stranger's home or boarding their vehicle. But the reason the hospitality and taxi industries were regulated and licensed to begin with was because of the myriad risks posed to customers from substandard accommodation and reckless drivers.

To the extent that DeFi is genuinely decentralized, where the promoters of such services do not deploy upgradeable proxy contracts, or possess administrative functions or control which provide *de facto* control over the system, then arguably such technology-agnostic carve outs ought apply.

However, in the vast majority of DeFi applications, significant and in some cases total control resides in the hands of a privileged few promoters, for whom it would be challenging to argue that they ought to be exempt from existing money transmission laws and compliance burdens.

Well-Defined Jurisdictional Regulatory Boundaries

As can be expected with any new technology, regulation, let alone legislation, severely lags the advancement and development of that new technology.

Because technological advancement almost always outpaces the ability of lawmakers to anticipate or manage the fallout of such innovation, that gap leaves a vacuum eagerly filled by regulators.

Emboldened by this legislative gap, regulatory agencies caught in a perpetual turf war sought to stake their claim for oversight of crypto-assets and by doing so elevate the status of their agencies and better their bargaining position for increased budgets.

Regulatory enforcement actions launched by both the Commodity Futures Trading Commission (CFTC) and the Securities and Exchange Commission (SEC), have led at times to conflicting outcomes, reducing the level of certainty for innovators in the crypto-asset space.

Although the Supreme Court in *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946) considered the definition of a “security” “embodies a flexible, rather than a static, principle, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits,” that flexibility was arguably over-stretched in some of the SEC’s enforcement actions.

Regulation by enforcement isn’t in and of itself good or bad, but the selective application of such enforcement can leave would-be entrepreneurs and financial institutions safely on the sidelines for fear of their crypto-asset initiatives attracting legal challenges.

Because crypto-assets don’t always fit into neat categories, with many possessing the qualities of both securities and commodities, determining which regulatory agency should hold sway over such matters is a step in the right direction.

That is not to say investor protections should be sacrificed at the altar of innovation, nor caution thrown to the wind.

Instead, making a determination as to which regulatory agency ought to have a pre-emptive right to pursue enforcement actions within a well-defined regulatory framework crypto-assets can at least inform an entrepreneur's decision-making process.

Many will interpret this provision of Trump's EO to mean the CFTC will be the pre-eminent regulatory agency to police all things crypto, but this would perhaps be too quick an assumption.

As it currently stands, the SEC has already announced it will be setting up a new task force, to develop a regulatory framework for crypto-assets.³ Assuming the SEC will no longer be involved in the crypto-asset conversation would be naïve,

"The Task Force's focus will be to help the Commission draw clear regulatory lines, provide realistic paths to registration, craft sensible disclosure frameworks, and deploy enforcement resources judiciously."

When the SEC eventually provides "realistic paths to registration" the penalties for those who choose not to avail themselves of such paths are likely to apply.

No Dollar CBDC

(v) taking measures to protect Americans from the risks of Central Bank Digital Currencies (CBDCs), which threaten the stability of the financial system, individual privacy, and the sovereignty of the United States, including by prohibiting the establishment, issuance, circulation, and use of a CBDC within the jurisdiction of the United States.

It was never clear how the United States would benefit from a CBDC but this provision of Trump's EO effectively brings the curtains down on any such initiative.

The CBDC ban will insulate dollar-backed and dollar-based stablecoins from direct competition from the Federal Reserve and potentially foster the growth of more privately-issued stablecoins.

There are of course myriad benefits to a CBDC ban for the United States.

³ <https://www.sec.gov/newsroom/press-releases/2025-30>

With the dollar continuing to be the world's primary reserve currency, not having a Fed-issued CBDC strengthens the dollar's existing hegemony because it allows for private interests to further the dollar's distribution network in the form of dollar-backed stablecoins.

It's been estimated that as many as one out of every two dollars is in circulation outside of the United States⁴ and allowing more stablecoins to develop without fear of a Fed-issued CBDC challenging such endeavors will likely increase the number of stablecoins.

Unlike cash which has a high degree of friction, stablecoins glide effortlessly between its users and it is conceivable that such stablecoins will increase the demand for US Treasuries, to ensure that their backing is "lawful" and "legitimate."

Far from undermining America's considerable power to impose sanctions, where US Treasuries become the preferred backing for stablecoins, Washington can level sanctions even more effectively on her enemies by seizing such backing assets.

Here, the threat of sanction becomes even more effective in ways hitherto unfathomed because the failure by a stablecoin issuer to comply with US sanctions could risk the collapse of a stablecoin in its entirety.

The Importance of Definitions

The EO provides definitions for "digital asset," "blockchain" and "Central Bank Digital Currency" while noticeably omitting concepts such as "open-source" and "decentralization."

Omitting definitions is perhaps just as significant as providing them and provides a glimpse into the Trump administration's attitude on blockchain technology in general.

"Distributed" vs "Decentralized"

The term "distributed" is used throughout the EO, in favor of the term "decentralized" which regularly appears in other descriptions of blockchains found elsewhere and it is conceivable that the choice of "distributed" was not accidental.

"Distributed" just means that more than one person or entity is a participant, but makes no comment on whether that distribution is concentrated or otherwise, as opposed to "decentralized" which suggests a more equitable re-allocation of interest.

⁴ <https://www.uscurrency.gov/life-cycle/data/circulation#:~:text=As%20much%20as%20one%2Dhalf,54.6%20billion%20notes%20in%20volume.>

The absence of “decentralization” in the EO seems to suggest that blockchain networks need not be “decentralized” in their operation for them to qualify for “protection” and “promotion” under the EO.

“Publicly Available” Source Code

Sec. 2. Definitions.

(b) The term “blockchain” means any technology where data is:

(iv) composed of source code that is publicly available.

The express inclusion of “source code that is publicly available” is worth noting.

It is not uncommon for new blockchains, especially Layer 2 blockchains, to be dependent on a collection of source code that has both “publicly available” and repositories and private source code that sits on servers run by the blockchain’s promoters.

Dependence on both “publicly available” and privately held source code could potentially exclude such protocols from being considered a “blockchain” within the definitions of Trump’s EO.

This distinction, between a “blockchain” that has its source code “publicly available” and purported blockchain networks which do not, could inform regulatory agencies in their approach to enforcement.

“Publicly Available” vs “Open-Source”

However, it could also be argued that “publicly available” simply means anyone must be able to interact with the source code, without necessarily being able to inspect its content.

In that sense, the source code is certainly “publicly available” but not within the well-litigated concept of “open source.”

Presumably, the decision to exclude the term “open-source” should be telling.

A widely accepted definition of “open-source” software code is computer software that is released under a license in which the copyright holder grants users the rights to use, study, change and distribute the software and its source code to anyone and for any purpose.

That Trump’s EO contemplates “publicly available” but not “open source” software code is illuminating.

For instance, a corporation could establish its own blockchain network and while interaction with the source code is “publicly available” to the extent that there are published APIs, the content of that source code could be held privately, and it would satisfy the definition of a “blockchain” according to the EO.

In such cases, the corporation could argue that they would not require any money transmission licenses because the source code of the blockchain network they established was “publicly available” even though closed-source dependencies exist that provide the corporation with substantial administrative privileges.

Conclusion

Sec. 7. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department, agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

Executive orders require no approval from Congress and they have the force of law, much like regulations issued by federal agencies, but almost all executive orders come with the boilerplate language found in Sec.7.

Even though some will tout this EO as a victory for the crypto-asset industry, this EO has limited, if any, legal effect where such regulatory intent has been imprecisely articulated.

For instance, what constitutes “protecting and promoting” and what are the definitions of “fair and open access” are all concepts open to a wide variety of interpretations.

It is also not at all clear the extent to which regulatory agencies within the sphere of the Trump administration's influence will hew to this EO's aspirations because "regulatory clarity" and "certainty" are concepts, not measurements.

Nothing in Trump's EO impairs the power of existing regulatory authorities nor does it hamstring agencies such as the SEC from pursuing enforcement action where it deems appropriate.

While it is clear the provisions of the EO with respect to the creation of a Working Group and the ban on CBDC development have practical implications, it is less clear what effect the more aspirational provisions will have.

Some will view the absence of references to "open-source" and "decentralization" as a cynical approach to crypto-assets, while others will argue that these concepts ought not be features which define blockchain technology.

Suffice to say that if this were the case, then the development of blockchain technology has advanced well beyond its bitcoin roots.

Given the degree of crypto-asset concentration in many blockchain networks, it may be impractical to require "decentralization" as a key characteristic of a blockchain, but if so, begs the question whether such services need to be regulated consistent with existing standards applied to money transmitters.

The foregoing represents the personal opinions of our General Counsel and is the product of their professional research. It is not meant to represent the position or opinions of ChainArgos, nor the official position of any of its staff members. Any errors remain strictly the fault of the author of this opinion piece. Please refer to the legal disclaimer at the end of this document for more information.

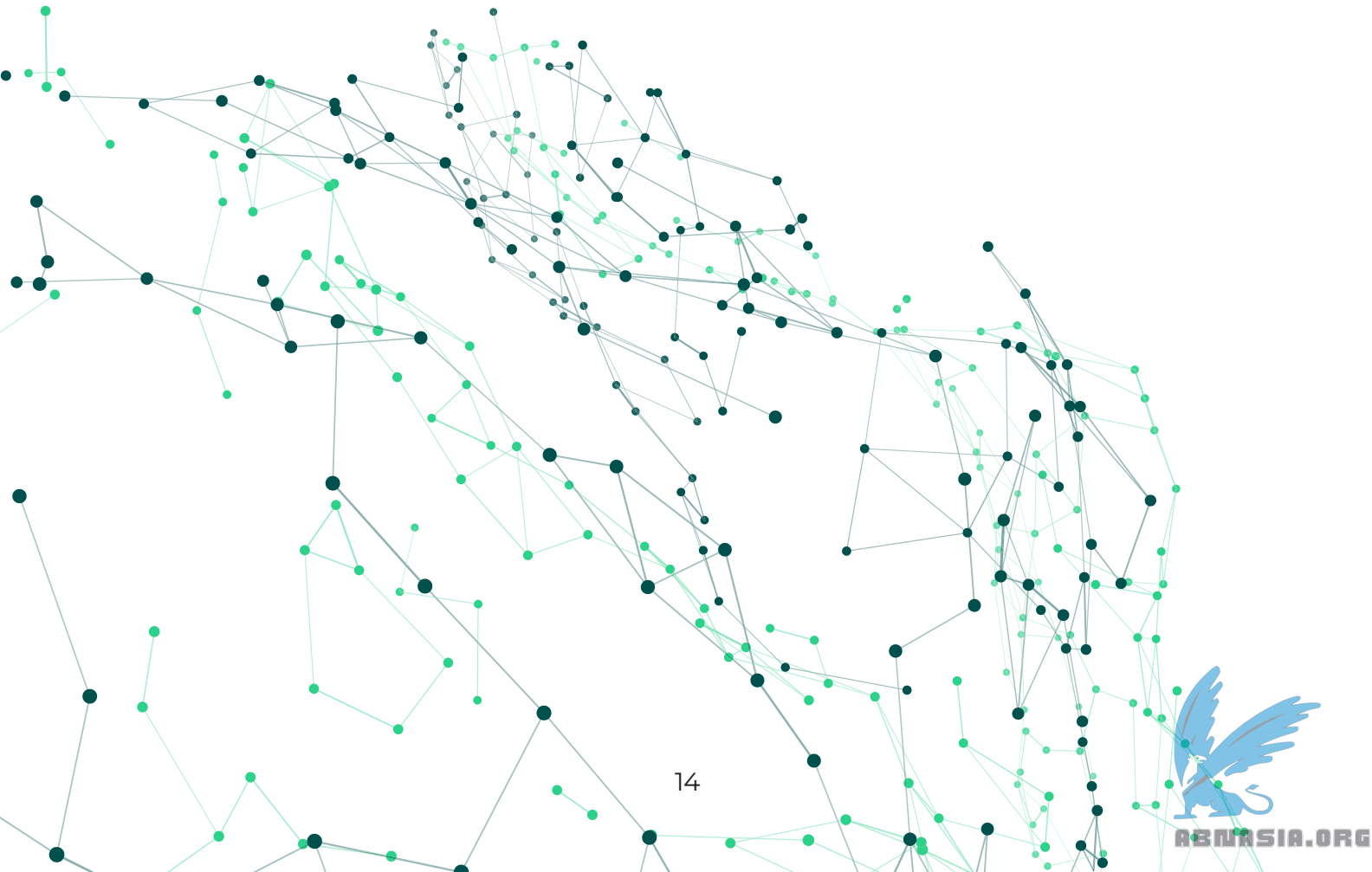
Who are we?

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:

<p>Bloomberg</p>  <p>Binance Acknowledges Past Flaws in Maintaining Stablecoin Backing</p> <ul style="list-style-type: none"> Blockchain analyst Reiter had flagged gaps in Binance-peg BUSD Binance says earlier 'operational delays' have now been fixed 	<p>Forbes</p>  <p>Did Digital Currency Group Profit From \$60 million In North Korea Crypto Money Laundering?</p>	<p>THE WALL STREET JOURNAL.</p>  <p>From Hamas to North Korean Nukes, Cryptocurrency Tether Keeps Showing Up</p> <p>Tether has allegedly been used by Hamas, drug dealers, North Korea and sanctioned Russians</p>
<p>THE WALL STREET JOURNAL.</p>  <p>The Shadow Dollar That's Fueling the Financial Underworld</p> <p>Cryptocurrency Tether enables a parallel economy that operates beyond the reach of U.S. law enforcement</p>	<p>Bloomberg</p>  <p>Stablecoin Operator Moves \$1 Billion in Reserves to Bahamas</p> <ul style="list-style-type: none"> Move reflects worsening US banking conditions for crypto firms TrueUSD's circulation has more than doubled in the last month 	<p>South China Morning Post</p>  <p>How crypto investigators uncover scammers' blockchain billions, scale of money laundering in Asia</p>

Who uses blockchain intelligence?



Finance and
Banking



Compliance



Law Enforcement



Regulators and
Policymakers

Finance and Banking

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

Compliance

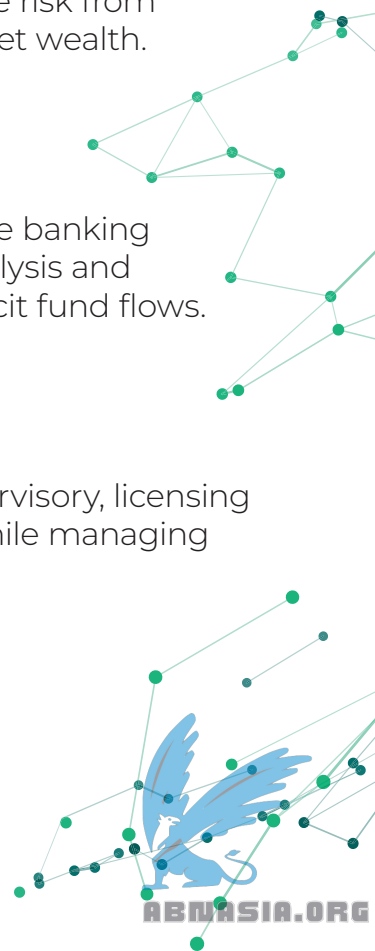
Fight money laundering, expand know-your-customer tools, and combat the financing of terrorism while expanding your customer base. Manage risk from customer crypto-assets and confidently verify sources of crypto-asset wealth.

Law Enforcement

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

Regulators and Policymakers

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



How are we different?

We deliver actionable blockchain intelligence.

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

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

Whether you're looking to on-board a customer, determine source of wealth, or ensure your evidence isn't rejected on appeal, our blockchain intelligence is based on established principles of statistics, math, and forensic science.

Extreme Versatility

Create compliance and commercially-driven analysis in a single place and arrive at better business decisions faster.

No-Code Customization

Build any query or analysis without programming skills or coding.

Financially-Relevant

Standard financial measures combined with blockchain intelligence for actionable insight.

Data Integrity

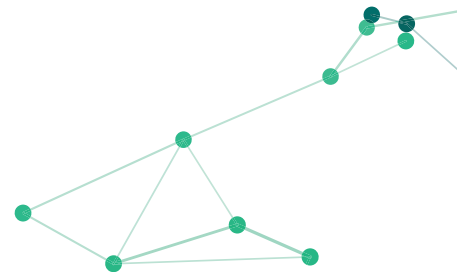
ChainArgos runs its own blockchain nodes, and we never enrich our data with yours, so you can be sure of data integrity.

API Ready

Robust and resilient APIs with 99.99% uptime. Minimal code required for easy integration.

Automated Alerts

Schedule automated alerts and reports via Email, Webhook, Amazon S3 and SFTP so you're always in the know when something happens.



How do we do it?

Blockchain intelligence is a relatively new industry, and it's not uncommon to hear of methods which have little basis in finance, let alone forensic science.

Let's look at one example to understand the limitations of blockchain tracing.

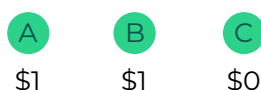


Fig. 1

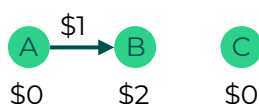


Fig. 2

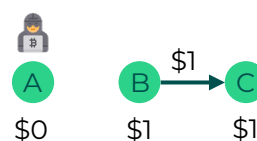


Fig. 3

In Fig. 1, A and B start with \$1, while C starts with \$0. In Fig. 2, A transfers their \$1 to B who now has \$2. Finally, in Fig. 3, B transfers \$1 to C, who now has \$1.

If it turns out A is an illicit actor, with what degree of confidence can we say that C has received \$1 from illicit sources? 50-50?

Would you accept a "risk score" of 50%?

Follow the money.

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

Most blockchain transactions don't derive from a single source, and believing they do is what leads to poor outcomes.

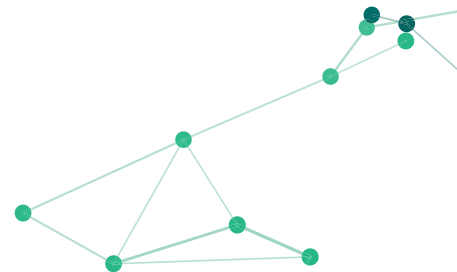
Make better decisions by focusing on what matters - where the money went, where it came from, and where does it look like it's headed to?

How much does one address deal with another? What's the average transaction size? What's the frequency? What's the crypto-asset or stablecoin of choice? What's the transaction behavior? When did the transaction size change?

And so much more.

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

- [Blockchain] Your Queried Addresses' Labels & Categories**: A table with columns 'Address', 'Labels', 'Categories', and 'Organizations'. It shows one row with address '1'.
- Blacklisting Info (If Any)**: A table with columns 'Timestamp Date', 'Authority', 'Action', and 'Blockchain'. It shows one row with timestamp '1'.
- [Blockchain] Inbound Counterparties**: A table with columns 'From Address', 'Labels', 'Symbol', 'USD Value Today', 'Sum of Transfer Amounts', 'Number of Transfers', 'Avg Transfer Size', 'First Txn Date', and 'Last Txn Date'. It shows two rows with 'From Address' values '1' and '2'.
- [Blockchain] Outbound Counterparties**: A table with columns 'To Address', 'Labels', 'Symbol', 'USD Value Today', 'Sum of Transfer Amounts', 'Number of Transfers', 'Avg Transfer Size', 'First Txn Date', and 'Last Txn Date'. It shows two rows with 'To Address' values '1' and '2'.



Better attribution.

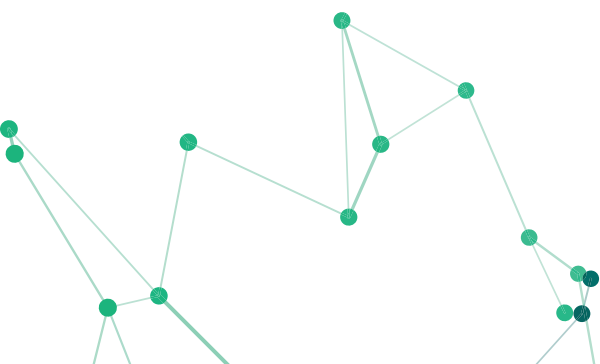
Don't risk critical legal, trading, and compliance decisions to questionable or subjective attribution methods. Trust math and science.

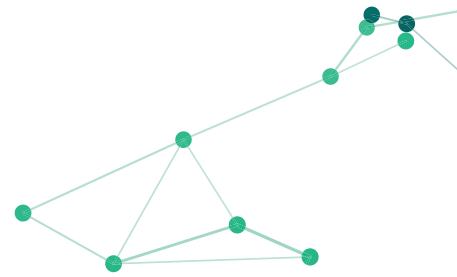
ChainArgos is the only blockchain intelligence firm that delivers programmatic address labels and wallet tags that are unassailable whether you're making business decisions or preparing to sue someone.

Blockchain addresses are automatically ranked and labeled based on a variety of factors including:

- **Transaction Count:** the number of transactions by an address. Sending \$100,000 in one transaction may have very different implications from sending 10 transactions of \$10,000 each. Either way, you'll know the difference.
- **Lifetime Sent/Received:** lists the biggest sender and/or receiver of any given crypto-asset or stablecoin currently. Markets are extremely dynamic. The biggest movers today may not be the same tomorrow.
- **Max. Historical / Current Balances:** helps you decide whether an address is participating in affiliated crypto-assets and/or stablecoins based on their maximum historical balance and who's stocking the highest current balances.
- **Recipient Number:** gives you a sense of whether they were an early adopter, or even possibly an insider of a crypto-asset or stablecoin. Recipients are ranked according to the date and time they received a crypto-asset or stablecoin.

Say "no" to dodgy wallet tagging and "yes" to attribution you can trust.





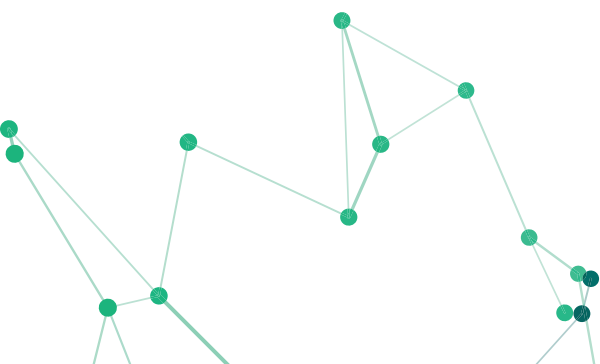
Legal Disclaimers.

THE INFORMATION CONTAINED IN THESE MATERIALS IS FOR INFORMATION PURPOSES ONLY AND NOT INTENDED TO BE RELIED UPON.

The information contained herein is information regarding research and analysis performed by ChainArgos Pte. Ltd., a company incorporated with limited liability under the laws of the Republic of Singapore with registration number 202303560W ("the Company"). The information herein has not been independently verified or audited and is subject to change, and neither the Company or any other person, is under any duty to update or inform you of any changes to such information. No reliance may be placed for any purposes whatsoever on the information contained in this communication or its completeness. No representation or warranty, express or implied, is given by, or on behalf of the Company or any of their members, directors, officers, advisers, agents or employees or any other person as to the accuracy or completeness of the information or opinions contained in this communication and, to the fullest extent permitted by law, no liability whatsoever is accepted by the Company or any of their members, directors, officers, advisers, agents or employees nor any other person for any loss howsoever arising, directly or indirectly, from any use of such information or opinions or otherwise arising in connection therewith. In particular, no representation or warranty is given as to the reasonableness of, and no reliance should be placed on, any forecasts or proposals contained in this communication and nothing in this communication is or should be relied on as a promise or representation as to the future or any outcome in the future.

This document may contain opinions, which reflect current views with respect to, among other things, the information available when the document was prepared. Readers can identify these statements by the use of words such as "believes", "expects", "potential", "continues", "may", "will", "should", "could", "approximately", "assumed", "anticipates", or the negative version of those words or other comparable words. Any statements contained in this document are based, in part, upon historical data, estimates and expectations. The inclusion of any opinion should not be regarded as a representation by the Company or any other person. Such opinion statements are subject to various risks, uncertainties and assumptions and if one or more of these or other risks or uncertainties materialize, or if the underlying assumptions of the Company prove to be incorrect, projections, analysis, and forecasts may vary materially from those indicated in these statements. Accordingly, you should not place undue reliance on any opinion statements included in this document.

By accepting this communication you represent, warrant and undertake that you have read and agree to comply with the contents of this notice.





© 2024 ChainArgos Pte. Ltd. All rights reserved.

