Guidehouse
Outwit *Complexity*

Chainalysis

Financial Services

Cryptocriminals Can't Hide—Investigative Blockchain Technology Sniffs Out Illicit Activity

Introduction

Cryptocurrencies, like all currencies, present certain money laundering and terrorism risks and have been and continue to be used by bad actors to engage in illicit activities.[1] For example, on February 2, 2022, hackers exploited a vulnerability in the code of decentralized finance platform Wormhole Network and were able to steal cryptocurrency worth more than $320 million. While the hackers are in possession of these stolen digital assets, they have not been able to ride off into the sunset like the bank robbers of old.

Instead, blockchain analytics firms, such as Chainalysis, have traced the transactions related to the hack and are able to track the cybercriminals' every move.[2] Investigative tools, such as Chainalysis Reactor, allow investigators to identify any wallet or service that a cryptocurrency has ever passed through or will go through. This capability is not possible in the fiat currency space.

In the first of an ongoing series of partnered articles between Chainalysis and Guidehouse on conducting blockchain investigations, we will discuss how to mitigate and avoid transactions with bad actors through an understanding of indirect exposure.

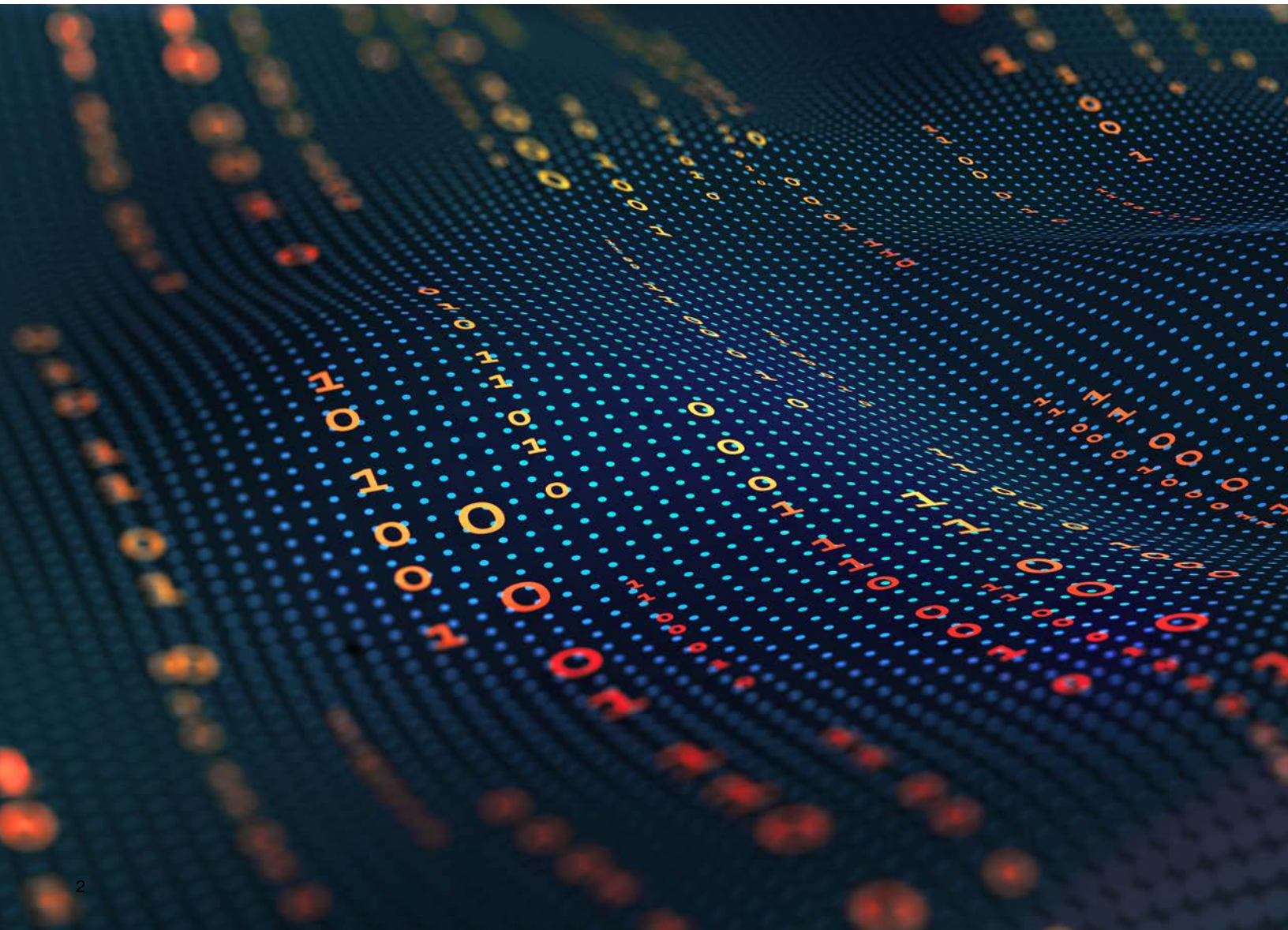
1. https://www.occ.treas.gov/news-issuances/news-releases/2021/nr-occ-2021-2a.pdf.
2. https://blog.chainalysis.com/reports/wormhole-hack-february-2022/.

What is Indirect Exposure?

Chainalysis,[3] a premier blockchain analytics tool, defines exposure as the relationship between entities that is created through transactions. As opposed to direct exposure (which is the direct transfer of funds from A to B), indirect exposure is the indirect connection between the source and the first service that is encountered.[4] In other words, tracing indirect exposure is the process of following funds from A to B through intermediaries C, D, and E. Investigating indirect activity reflects an understanding of how criminals and money launderers actually do business. In most situations, they look for ways to layer the movement of illicit funds to hide the source of their ill-gotten gains. Criminals in the cryptocurrency space typically try to do this by sending the proceeds of illicit activity through multiple intermediary wallets and through "mixers" and "tumblers" before the funds are sent to an exchange or a cash-out service.[5]

The very nature of the multiple movements underscores the necessity for financial institutions to look beyond their direct exposure, to their indirect exposure. To do this, Guidehouse strongly advises any institution that engages in cryptocurrency to develop and implement robust blockchain analytics protocols and technology.[6]

3. https://www.chainalysis.com/company/.
4. https://blog.chainalysis.com/reports/cryptocurrency-risk-blockchain-analysis-indirect-exposure.
5. https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws.
6. https://www.elliptic.co/blog/a-brief-guide-to-analytics-on-blockchain#:~:text=Blockchain%20analytics%20is%20the%20process,information%20about%20users%20and%20transactions.



How to Investigate Indirect Exposure

There is no one-size-fits-all approach to investigating indirect exposure in cryptocurrency transactions. However, the first step in conducting any cryptocurrency investigation is choosing the appropriate tool for the job. In most cases, this will be an enterprise blockchain analytics platform.[7] These platforms combine on-chain data with open-source intelligence (OSINT) and other methods to identify addresses and wallets that can be attributed with a high degree of certainty to a single controlling entity. This grouping is called "clustering." Using these clusters, investigators can determine if a counterparty is a commercial exchange, a mixing service, or a sanctioned entity.

Not all addresses can, however, be easily clustered, as it is not always possible to definitively cluster intermediary addresses, thus giving rise to the concept of indirect exposure. However, just because a blockchain analytics platform is not able to cluster a particular address, that does not mean an investigator cannot ascertain whether an intermediary address in a transaction is controlled by a bona fide third party or whether it is potentially being used to obfuscate a source or destination of funds.

Peel chains illustrate why it's important to account for every hop. According to Chainalysis, a peel chain is a transaction pattern commonly seen in blockchain analysis, in which there appear to be many intermediary addresses between a target cluster and another cluster of interest, such as a service or illicit entity. In reality, those intermediary addresses are part of the user's original wallet, and are systematically created to receive the **leftover change** resulting from certain transactions. Indirect exposure investigation is crucial here, enabling investigators to focus efforts on potentially suspicious wallet or address transactions more closely.

While each blockchain has particularities in how to investigate, understand, and attribute indirect exposure, there are several overarching methods that an investigator can use to clarify indirect exposure:

Use a risk-based investigative approach.	It may not be feasible to investigate every instance of indirect exposure. While there are some risks that institutions have a zero-tolerance threshold for (such as sanctioned entities, terrorist financing, and child abuse materials), other risks may only be worth investigating based on an institution's risk and threshold tolerance.
Evaluate a cluster's transaction risk characteristics.	Clusters with numerous, recent, or high value indirect exposure to high risk counterparties likely require more scrutiny than those that have limited, historic, and low value transactions.
Evaluate a wallet's transaction risk characteristics.	If an intermediary address conducts hundreds of transactions worth thousands of dollars per week it is likely a service (such as an exchange) and likely represents a change in control of the cryptocurrency.
Transfers through numerous addresses do not necessarily represent a change in control.	Given the ease of conducting transactions on blockchains, an investigator cannot rely on a large number of intermediary addresses to indicate that a cryptocurrency has changed hands. It is relatively easy to route a transaction through dozens or even hundreds of addresses controlled by a single entity in an attempt at obfuscation.
Transfers in round cryptocurrency or fiat values can be payments for legal goods and services.	While cryptocurrency is not as widely adopted as fiat currency, it is often used to pay for legal goods and services. Transfers in round cryptocurrency or fiat values are indications that the transfer may be a payment and therefore could be a change in control of the cryptocurrency.
Pay attention to a transfer's value and timing.	When viewing a chain of transfers, those of the same or similar value sent soon after one another could indicate a continuity of control. Similarly, if an address holds funds for a long period of time before transferring them, this could indicate a change of ownership.
OSINT can identify addresses.	While enterprise blockchain analytics tools conduct their own OSINT, it is not possible for them to capture everything. Investigators can and should supplement this by conducting their own desktop research to attempt to identify addresses.

It is important to remember that while the above methods apply generally across blockchains, each specific protocol has specific methods for understanding indirect exposure that are unique to that blockchain. Engaging highly trained investigators is vital to understanding and applying these nuances.

7. Notable blockchain analytics platforms include Chainalysis, CipherTrace, TRM Labs, and Elliptic.

How Guidehouse Can Help

Guidehouse's team has in-depth knowledge of blockchain analysis and investigation in the United States, Europe, and globally, and understands best practices operated by cryptocurrency providers. Our team includes compliance officers, attorneys, bankers, former regulators, prosecutors, law enforcement officers, accountants, and IT professionals. Our professionals bring to bear critical expertise and resources to help clients rapidly conduct blockchain investigations and assess your financial crime framework to determine whether it is operationally effective and meets regulatory expectations.

Our relevant expertise includes the following:		
Compliance Program and Policy and Procedure Reviews	**Customer Reviews**	**Vendor Sourcing and Governance**
Transaction Reviews	**Global Investigative and Operational Services**	**Training and Quality Assurance**
AML and Sanctions Consulting	**Technological Services**	**Outsourced Money Laundering Officer Services**

Guidehouse can quickly review and assess your anti-money laundering (AML) and sanctions compliance program to determine whether it is sound, to identify gaps or weaknesses, and/or to conduct training on AML and Sanctions investigations and compliance.

Guidehouse is well-equipped to make an individualized assessment of your unique circumstances and offer innovative advice and solutions for responding to heightened regulatory requirements.

Contacts

Alma Angotti
Partner and Global Legislative & Regulatory Risk Leader
alma.angotti@guidehouse.com

Gregory Schwarz
Associate Director
Financial Crime Solutions
gschwarz@guidehouse.com

Contributor: **Nick Bohmann**

guidehouse.com/financialservices linkedin.com/showcase/guidehouse-financial-services twitter.com/GuidehouseFSAC

guidehouse.com

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 12,000 professionals in over 50 locations globally. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit: www.guidehouse.com.

Guidehouse
Outwit *Complexity*