IN THE SIXTEENTH JUDICIAL CIRCUIT OF MISSOURI
JACKSON COUNTY AT INDEPENDENCE

[redacted]	)	
[redacted]	)	
	)	
v.	)	Case No: [redacted]
	)	
[redacted], and	)	Division 10
	)	
DANA "[redacted]" [redacted]	)	Honorable [redacted]
	)	
Defendants	)	

AFFIDAVIT
OF CRYPTOCURRENCY FORENSIC INVESTIGATOR

BEFORE ME, the undersigned, personally appeared [redacted] and [redacted], who, being by me duly sworn, depose as follows:

I am [redacted]. I am [redacted]. I am of sound mind, capable of making this affidavit. I am personally acquainted with the facts herein stated:

QUALIFICATIONS

Our qualifications are as follows:

> Certified Specialist in Chainanalysis Technology (CEIC), a designation awarded by Chainanalysis Co-founder and CEO Michael Gronager, recognizing my proficiency in blockchain forensic investigations. I have successfully completed the requirements to obtain the Chainanalysis Ethereum Investigations Certification.
>
> Professional certification as a Chainanalysis Reactor (CRC), validated by Chainanalysis Co-founder and CEO Michael Gronager, signifying expertise in cryptocurrency tracing using Chainalysis tools.

With significant experience in cryptocurrency investigations, blockchain technology, and forensic tracing of stolen digital assets, each of us has worked extensively in identifying illicit financial activities on-chain.

Our qualifications in forensic cryptocurrency tracing and investigations are supplemented by our expertise in industry-leading analytics software, including Chainalysis Reactor, AMLBot Pro, Blockchain International Group's QLUE, and Crystal Intelligence. These tools allow each of us to meticulously track and analyze the movement of cryptocurrency transactions across multiple blockchains.

The identity of the information attached as Exhibit A is the blockchain technology tracing of cryptocurrency owned by [redacted] "[redacted]" [redacted] and transferred to [redacted]" [redacted] via www.[redacted].com. This includes accounts held by and moved within **Binance Holdings Limited** and/or **Binance Capital Management Company, Ltd.**

CRYPTOCURRENCY EXPLAINED

Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat (government issued) currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin (BTC), Tether (USDT), and Ether (ETH).

Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or on cloud-based servers. Although not usually stored in a physical form, public and

private keys (explained below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object.

Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction. Cryptocurrency is not illegal in the United States.

CRYPTOCURRENCY "WALLETS" EXPLAINED

Cryptocurrency is stored in a virtual account called a "wallet." Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A **public key** or address is akin to a bank account number, and a **private key** is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key.

To conduct transactions on a blockchain, an individual must use the public address (public key) and the private address (private key). A public address is represented as a case-sensitive string of letters and numbers, 26–36 characters long (See Exhibit A). Each public address is controlled and/or accessed using a unique

corresponding private key, the cryptographic equivalent of a password or PIN needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

Although cryptocurrencies have legitimate uses, like fiat currencies, cryptocurrency is also used by individuals and organizations to harm people, such as fraud. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes attempt to thwart any efforts to track their transactions.

MODE OF PREPARATION
BLOCKCHAIN ANALYSIS METHOD

Blockchain explorers as well as commercial services offered by blockchain analysis companies are used to analyze blockchain data. These companies, such as Chainanalysis, analyze virtual currency blockchains to identify the individuals and groups involved in transactions.

> For example, when an organization creates multiple [blockchain] addresses, it will often combine its [blockchain] addresses into a separate, central addresses (i.e., a "cluster"). An investigator can then identify a 'cluster' of [blockchain] addresses held by one organization by analyzing the blockchain's transaction history. Open-source tools and private software products can be used to analyze a transaction."

United States v. Gratkowski, 964 F.3d 307, 309 (5th Cir. 2020).

This flow of funds is indicative of tortious activity using cryptocurrency.

Defendants use known methods during the fraud to thwart efforts to trace, and ultimately recover, their illicit proceeds. These methods include:

The Use of Unattributable "0 Level" Deposit Addresses

Deposit addresses known as "0 Level" addresses are the initial addresses into which victims deposit funds on the blockchain. Defendants provide these addresses to victims. Fraudster Defendants usually provide 0 Level addresses corresponding to noncustodial, or "private," wallets that are difficult to attribute, rather than wallets hosted by exchanges or other third-party intermediaries to evade identification.

High Velocity Flow of Funds to Consolidation Wallet

After duping victims into depositing their investment funds into the 0 Level Address, Defendants typically rapidly transfer the fraudulently obtained funds through multiple wallets to a consolidation wallet, where the fraudsters then commingle the proceeds with their other funds. Plaintiff's funds followed such a path: after being deposited, the fraud proceeds were transferred to a different wallet, and after that, the fraud proceeds were transferred yet again, this time to a "consolidation" wallet, where the fraud proceeds briefly remained.

Use of a Consolidation Wallet to Commingle Funds

As a part of a "layering" stage of the hiding process, criminals commingle fraud proceeds in consolidation wallets with their other funds to conceal the nature, source, ownership, location, and control of the fraud proceeds, and in that process, make it harder

for investigators to trace the disposition of the fraud proceeds.

Fraudsters commingle fraud proceeds they obtain at almost every step in the flow of those fraud proceeds and, ultimately, they commingle fraud proceeds in large transactions.

Absence of Commercial or Private Purpose

There is no known reason, economic or otherwise, for legitimate businesses or individuals to conduct cryptocurrency transfers in the above fashion. Every individual cryptocurrency transfer costs money. For stable coins, like in this case, that cost is paid via "gas" fees levied by operation of the Ethereum blockchain.

It is reasonable to assume that businesses and individuals who seek to transfer legitimate funds from one address to another will strive to minimize the fees by conducting transfers with as few transactions, or "hops," as possible.

Unnecessary intermediate cryptocurrency transactions also delay the process of disposing of cryptocurrency funds, and thus defeat much of the advantage that cryptocurrency offers as a quick means of exchange.

Businesses and individuals engaging in legitimate cryptocurrency transactions, who are unconcerned with obfuscating the source and destination of their funds seek to minimize their crypto transaction costs by using "retail" exchanges. Retail exchanges, like Coinbase or Binance, can consolidate crypto transactions, and thereby lower customer transaction fees. Criminals laundering through cryptocurrency, however, often avoid retail

exchanges as much as possible because transactions conducted through retail exchanges are more readily attributed using blockchain analysis tools, and because retail exchanges are often responsive to legal process.

ANALYSIS EVIDENCE IN THIS CASE

In this investigation, we identified and analyzed the specific wallet addresses linked to Defendants. By leveraging blockchain explorer tools and forensic tracing methodologies, I examined transactional details, including amounts transferred, timestamps, and receiving addresses. Further analysis revealed a pattern of movement across multiple wallets, employing tactics consistent with efforts to obfuscate the origin and ultimate destination of funds. These end wallets are linked to fraud activity and efforts to hide that fraud.

Furthermore, based on the transactional patterns observed on-chain, I have been able to identify additional wallets linked to the same scammers. These findings support the broader tracing effort and strengthen the case for targeted enforcement actions.

The information regarding the cryptocurrency wallet addresses included in Exhibit A is based upon my own observation, investigations, and information. The following evidence shows the transaction evidence linking legitimate victim funds to the cryptocurrency wallet addresses identified in Exhibit A:

FURTHER THIS AFFIANT SAYETH NOT.

Signed **X**_____

[redacted]

FURTHER THIS AFFIANT SAYETH NOT.

Signed **X**_____

[redacted]

NOTARY SEAL

STATE OF MISSOURI)
) ss.
COUNTY OF CASS)

I, the undersigned, an officer authorized to administer oaths, certify that [redacted] [redacted], having been first duly sworn, executed this Affidavit, that he willingly signed as his voluntary act, that he was over eighteen years of age, had capacity, and was under no constraint or undue influence

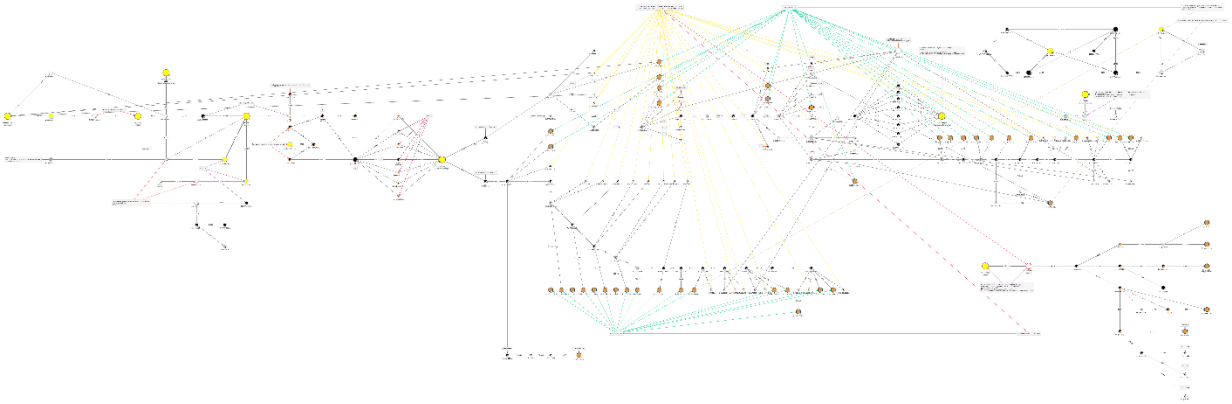
IN WITNESS WHEREOF, I have hereunto subscribed my name and affixed my official seal this _____ day of _____, 2025.

_____
Notary Public

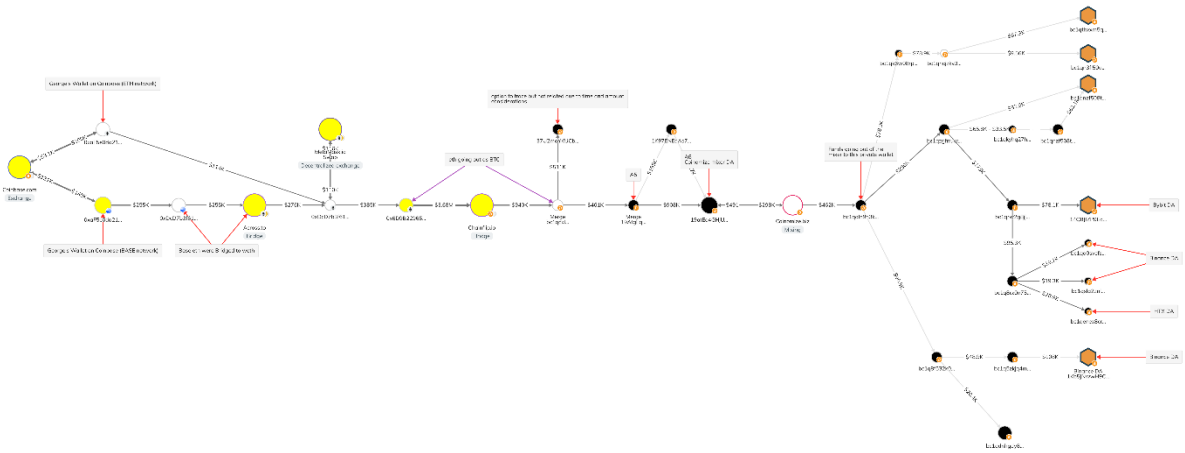
Notary's Term Expires: _____

Binance Wallet Address
1Kb[redacted]u

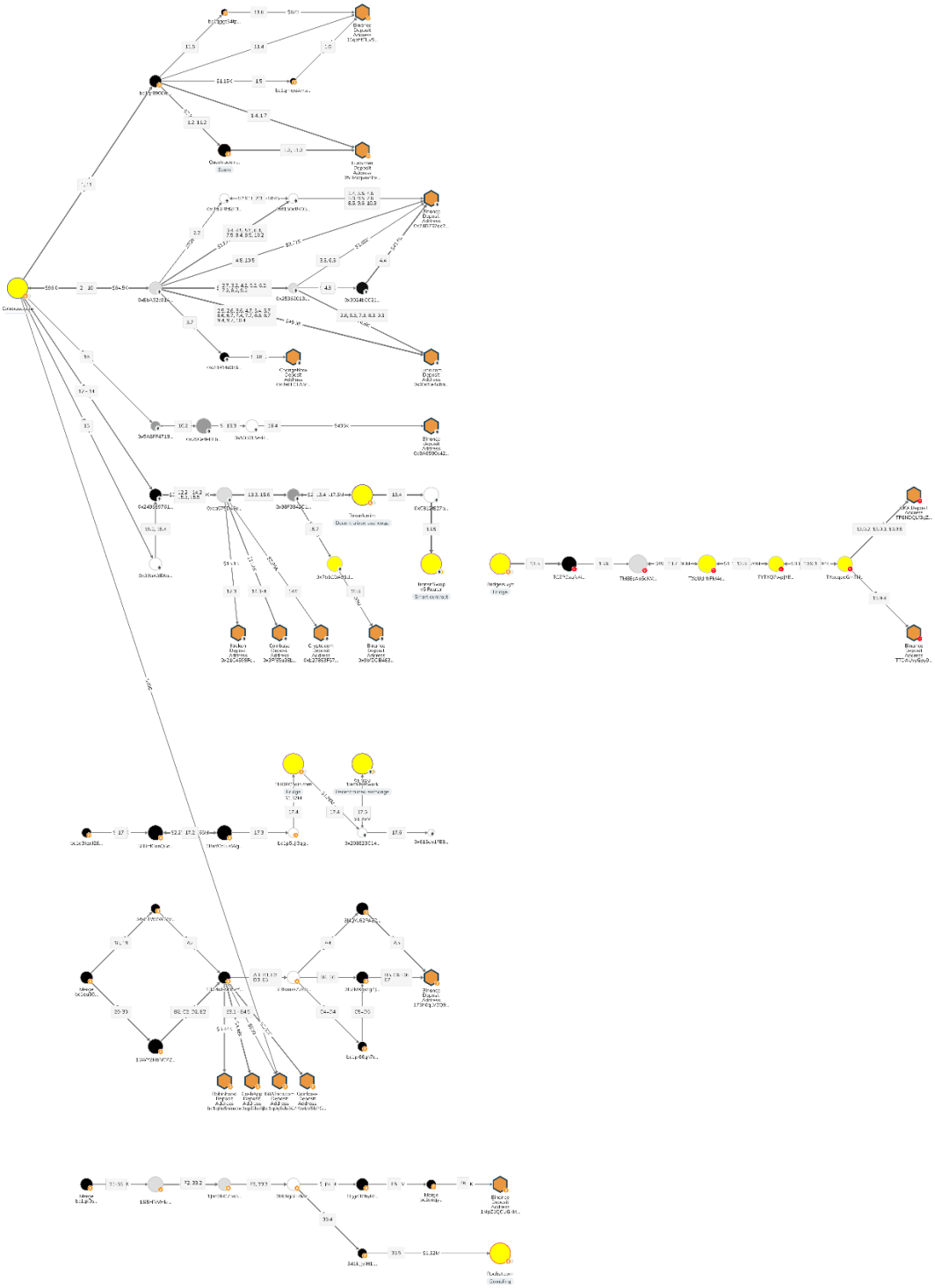
In Detail:



Simplified:



Binance Wallet Addresses
0x9A[redacted]b, and
173[redacted]b



Binance Wallet Addresses
0xf93[redacted]B, and
0x158[redacted]6

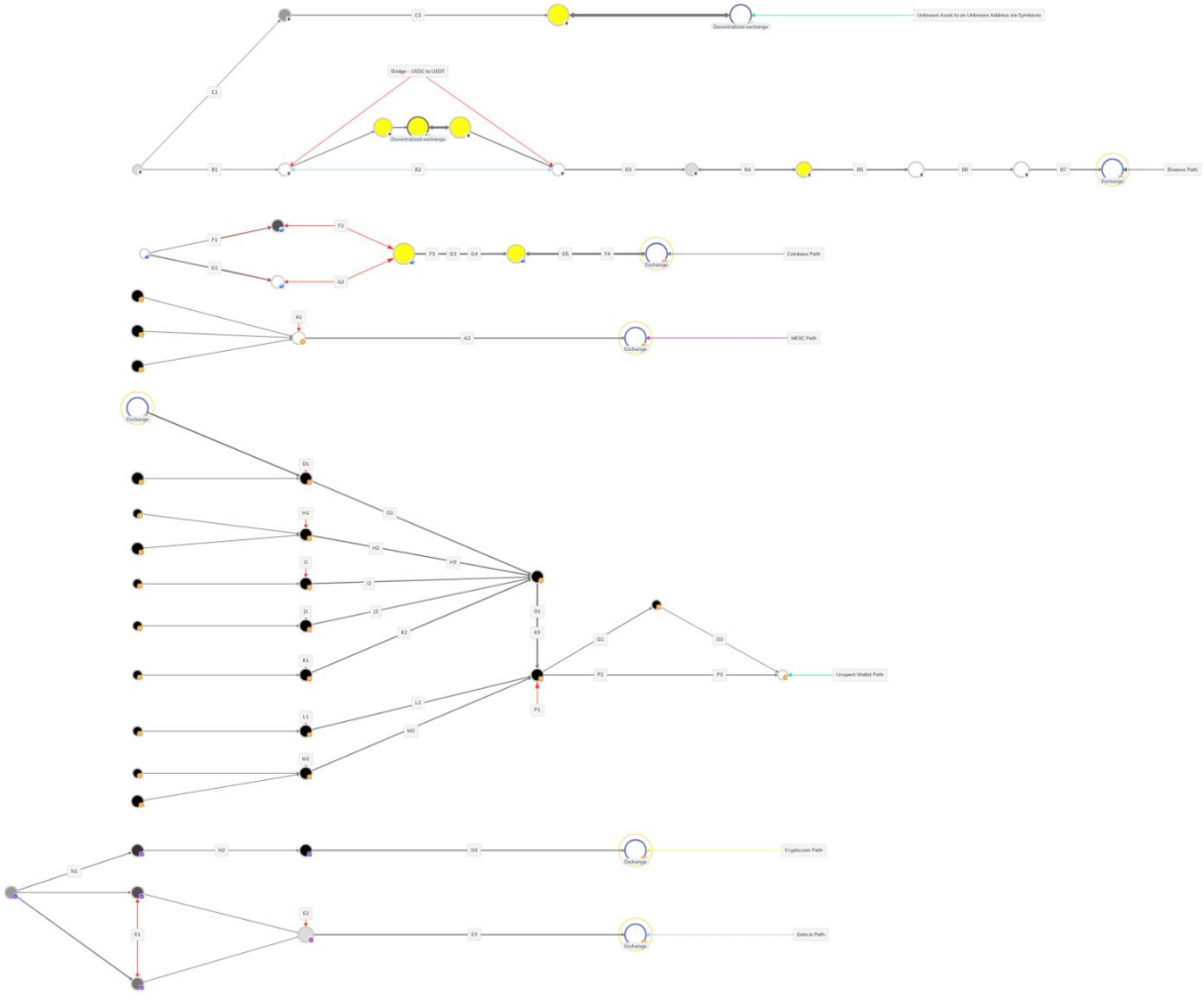
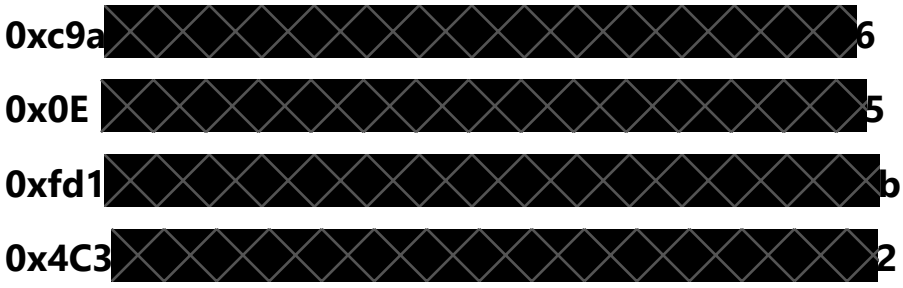
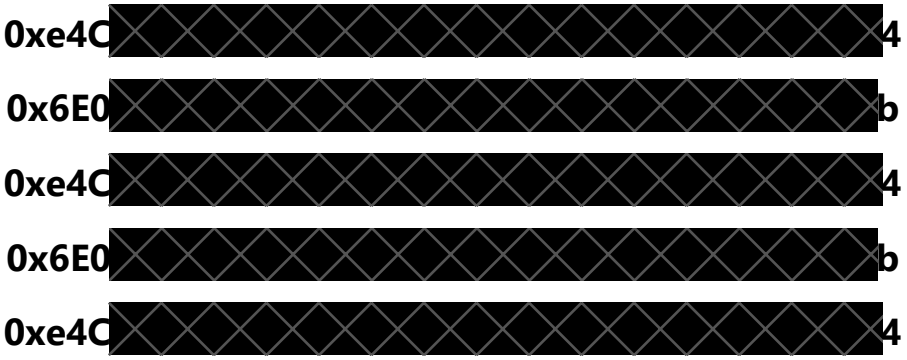


EXHIBIT A

DEFENDANTS' BLOCKCHAIN WALLETS SUBJECT TO JUDGMENT



Binance



Defendants Further Binance Wallets