GARY M. RESTAINO
United States Attorney
District of Arizona

JOSEPH F. BOZDECH
Assistant United States Attorney
California State Bar No. 303453
SETH T. GOERTZ
Assistant United States Attorney
Arizona State Bar No. 031645
Two Renaissance Square
40 North Central Avenue, Suite 1800
Phoenix, Arizona 85004-4408
Telephone: (602) 514-7500
Email: joseph.bozdech@usdoj.gov
Email: seth.goertz@usdoj.gov
Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

| | |
|---|---|
| United States of America,<br><br>Plaintiff,<br>v.<br><br>5,012,294.90 in TetherUS ("USDT"),<br>75,589,553.41 in Gala ("GALA"),<br>226.81 in BNB ("BNB"),<br>1,264.16 in Bitcoin ("BTC"),<br>1,495.72 in Litentry ("LIT"),<br>48,969 in Fantom ("FTM"),<br>47.17 in Ethereum ("ETH"),<br>501.41 in BUSD ("BUSD").<br><br>Defendants *In Rem*. | **VERIFIED COMPLAINT FOR FORFEITURE *IN REM*** |

Plaintiff United States of America brings this complaint and alleges as follows in accordance with Rule G(2) of the Federal Rules of Civil Procedure, Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions (Supplemental Rules):

## NATURE OF THE ACTION

1. This is a civil action *in rem*, brought to enforce the provision of 18 U.S.C. § 981(a)(1)(C) for the forfeiture of virtual currency, which constitutes or is derived from proceeds traceable to a violation of a specified unlawful activity as defined in 18 U.S.C. § 1956(c)(7), including but not limited to wire fraud, 18 U.S.C. § 1343, or a conspiracy to commit such offense.

2. This is a civil action *in rem*, brought to enforce the provision of 18 U.S.C. § 981(a)(1)(A) for the forfeiture of virtual currency, which is involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 and/or 1957.

3. Venue and jurisdiction in Arizona are based upon 21 U.S.C. § 881(j), and 28 U.S.C. §§ 1355(b) and 1395 as acts and omissions occurred in the District of Arizona that give rise to this forfeiture action. This Court has jurisdiction. 28 U.S.C. §§ 1345 and 1355, and 18 U.S.C. § 981(h).

## THE DEFENDANTS *IN REM*

4. The defendants consist of virtual currency seized from three separate Binance accounts (referred to collectively as the "**Binance Accounts**") via a federal seizure warrant (hereinafter, the "defendant property"). The defendant property is currently in the custody of the Federal Bureau of Investigation.

5. The first Binance account from which property was seized ("**Binance Account 1**") is held in the name of Kosit Sisawigon, and was registered on February 13, 2021, from Thailand. The following quantities of crytpocurrency were seized from **Binance Account 1**:

a. 79.15015536 in BNB

b. 0.09379305 in BTC

c. 935,793.055308 in USDT

6. The second Binance account from which property was seized ("**Binance Account 2**") is held in the name of Suradet Totsaponvised, and was registered on February 9, 2021, from Thailand. The following quantities of cryptocurrency were seized

from **Binance Account 2:**

a. 75,589,553.407047 in GALA

b. 3,873,201.805214 in USDT

c. 141.75987631 in BNB

d. 1,264.0644196 in BTC

7. The third Binance account from which property was seized ("**Binance Account 3**") is held in the name of Low Li Yu, and was registered on June 2, 2020, from Malaysia. The following quantities of cryptocurrency were seized from **Binance Account 3**:

a. 5.90402134 in BNB

b. 1,495.72000 in LIT

c. 48,969.00 in FTM

d. 47.16834 in ETH

e. 203,300.037192 in USDT

f. 501.413947 in BUSD

## BACKGROUND ON VIRTUAL CURRENCY

8. **Virtual Currency:** Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank, like traditional fiat currencies such as the U.S. dollar, but are generated and controlled through computer software. As discussed herein, cryptocurrency is a form of virtual currency. Bitcoin ("BTC") is a well-known type of cryptocurrency.

9. **Virtual Currency Addresses:** Virtual currency addresses are the particular virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of alphanumeric characters.

10. **Virtual Currency Wallet**: There are various types of virtual currency wallets, including software wallets, hardware wallets, paper wallets. The virtual currency

wallets at issue for the purposes of this affidavit are software wallets (*i.e.,* a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys). A virtual currency wallet allows users to store, send, and receive virtual currencies. A virtual currency wallet can hold many virtual currency addresses at the same time.

11. **Virtual Currency Exchanges (VCEs)**: VCEs are trading and/or storage platforms for virtual currencies. Many VCEs also store their customers' virtual currency in virtual currency wallets. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers (*i.e.*, "know your customer" or "KYC" checks) and to have anti-money laundering programs in place.

12. **Blockchain:** Many virtual currencies publicly record their transactions on what is referred to as the "blockchain." The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable and historical record of every transaction that has ever occurred utilizing that blockchain's specific technology. The blockchain can be updated multiple times per hour and record every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies. Investigators can follow or "trace" funds on public blockchains, a practice known as "blockchain analysis."

13. **Blockchain Analysis:** It is virtually impossible to look at a single transaction on a blockchain and immediately ascertain the identity of the individual behind the transaction. That is because blockchain data generally consist only of alphanumeric strings and timestamps. But law enforcement can obtain leads regarding the identity of the owner of an address by analyzing blockchain data to figure out whether that same individual is connected to other relevant addresses on the blockchain. To analyze blockchain data, law enforcement can use blockchain explorers as well as commercial services offered by blockchain-analysis companies. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups

involved in transactions. Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

14. **Stablecoins:** Stablecoins are a type of virtual currency pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar. USDT (also known as "Tether," the name of its issuer) is a stablecoin that resides on the Ethereum and Tron blockchains, among others. The value of USDT is tied to the value of the U.S. dollar; therefore, one unit of USDT is represented to be backed by one U.S. dollar in Tether's reserves, which is what makes it a "stablecoin."

15. **Ethereum:** Ethereum ("ETH") is a cryptocurrency that is open source, public, has its own blockchain, and is distributed on a platform that uses "smart contract" technology.

16. GALA is an Ethereum token that powers Gala Games, a platform for blockchain gaming. BNB is the cryptocurrency coin that powers the BNB Chain ecosystem and is issued by Binance. Litentry ("LIT") is the native token of the Litentry parachain network. Fantom ("FTM") is the native token of the Fantom network. BUSD is a stablecoin issued by Binance.

## INTRODUCTION

17. The purpose of this forfeiture action *in rem* is to establish the government's clear title to the defendant property. The defendant property was swindled from victims through the course of an investment fraud scam. The defendant property was subsequently laundered through a circuitous web of virtual currencies, wallet addresses, and blockchains. Following the government's seizure of the defendant property, the government now seeks to clear title so that, subject to the Attorney General's authority under 18 U.S.C. § 981(d) to dispose of petitions for remission of forfeited property, the defendant property may be returned to the victims of the fraud described herein.

18. The cryptocurrency seized in this matter is derived from an investment fraud scam, commonly referred to as "pig butchering," perpetrated on victims throughout

the United States, including in the District of Arizona.[1] The scheme often begins when a scammer sends a victim a seemingly innocuous and misdialed text or WhatsApp message. From there, the scammer will attempt to establish a more personal relationship with the victim by using manipulative tactics similar to those used in online romance scams.

19. The victims in pig butchering schemes are referred to as "pigs" by the scammers because the scammers will use elaborate storylines to "fatten up" victims into believing they are in a romantic or otherwise close personal relationship. Once the victim places enough trust in the scammer, the scammer brings the victim into a cryptocurrency investment scheme. The investment schemes are fake but have the appearance of a legitimate enterprise through the use of fabricated interfaces, derivative or "spoofed" websites that appear related to legitimate companies, and other techniques designed to bolster the scheme's legitimacy. This generally includes a fake investment platform operated through a website or mobile application that displays a fictitious investment portfolio with abnormally large investment returns.

20. Rarely, if ever, are the investment platforms anything more than a ruse, and the funds contributed are always routed directly to a cryptocurrency address the scammers control (this is when the scammers refer to "butchering" or "slaughtering" the victims). When the victims do attempt to withdraw their funds, they are unable to do so and are often met with various excuses or even required to pay "taxes" in order to release their funds. Eventually, most victims are completely locked out of their accounts and lose all of their funds.

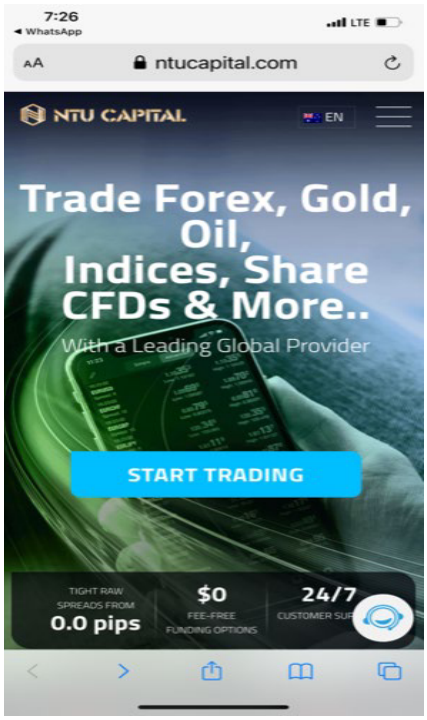
## BACKGROUND

21. Beginning in March of 2022, the Federal Bureau of Investigation ("FBI") identified numerous victims of a pig butchering scheme based on fraudulent investment platforms including NTU Capital Limited, which has utilized various domain name

[1] The term "pig butchering" is derived from the foreign-language phrase used to describe this scam, which originates from China and Southeast Asia. Based on Know Your Customer ("KYC") information provided to Binance, each of the Binance Accounts was registered from a country from which pig butchering schemes originate (Thailand and Malaysia).

iterations (*i.e.,* www.ntucapitallimited.com; www.ntucapital.com).[2] As set out herein, the FBI has identified several victims whose funds were sent to the **Binance Accounts**.

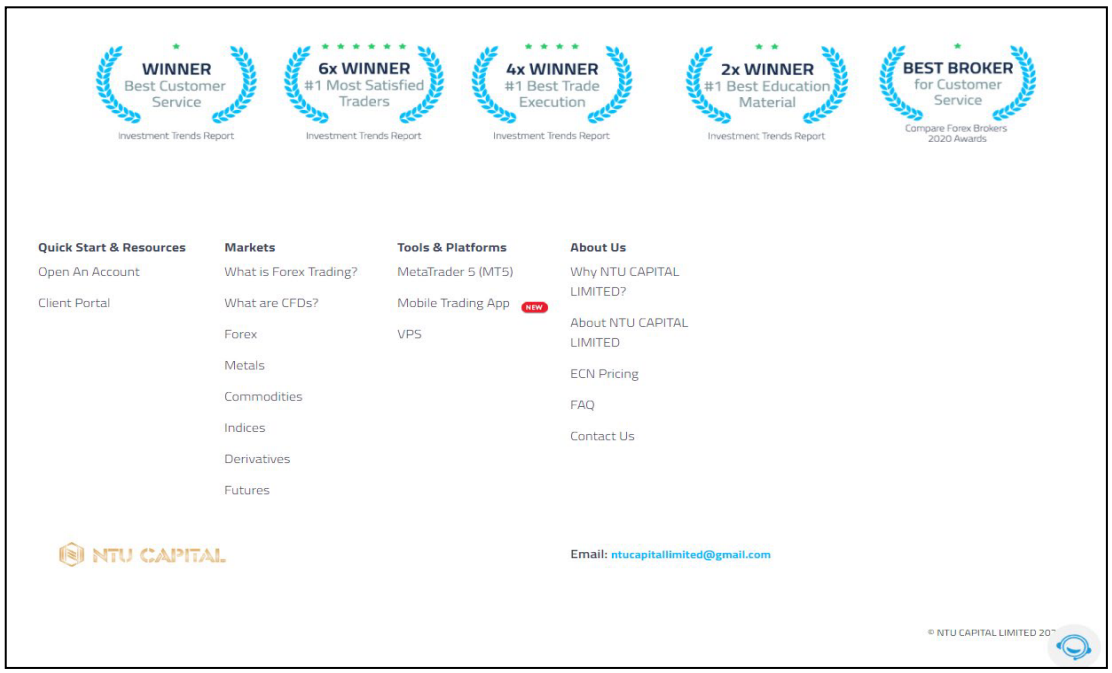
22. Throughout the course of the scheme, NTU Capital utilized several different domain names, but the overall presentation of the website (which is no longer available) generally remained the same, and appeared as follows:




23. The NTU website also had pages that claimed the platform was in compliance with FinCEN (the U.S. Treasury Financial Crimes Enforcement Network), that NTU Capital was regulated by the "United Stated (sic) Money Services Business," and that "client funds are held separately from the company's funds, in segregated client trust accounts, and reconciled each day," as depicted below:

[2] Investigators have linked other fraudulent platforms to the underlying scheme, but which are not explicitly referenced herein.


24. In addition, the NTU Capital website falsely claimed various awards that were meant to ease investor concerns and made the platform appear legitimate:




25. The FBI's investigation to date has revealed that each one of these statements were false.

## VICTIM MONEY FUNNELED TO FRAUDULENT ACCOUNTS

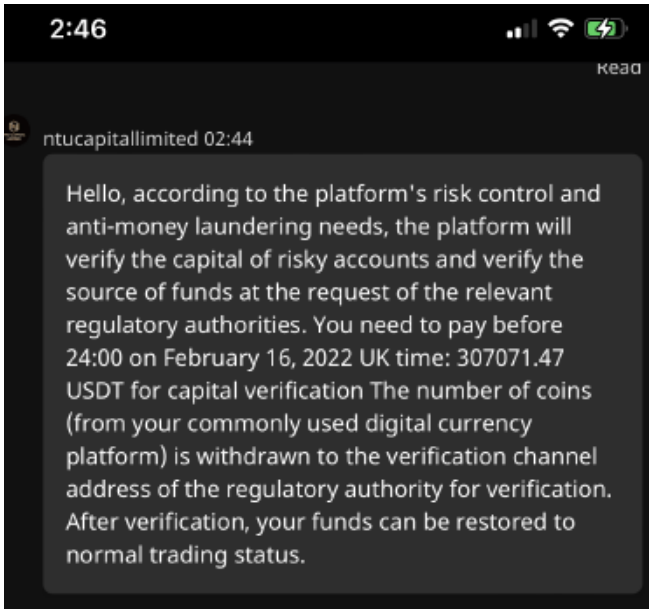
### Victim K.C.

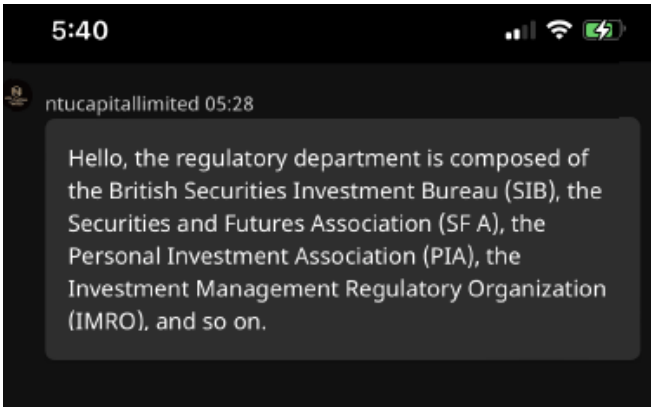
26. In December 2021, K.C., an Arizona resident, believed he was "mistakenly" contacted through WhatsApp by a female who identified herself as "Gracie." Gracie continued to communicate with him through WhatsApp, developing a relationship and eventually telling him about NTU Capital and opportunities for investment in cryptocurrency. Eventually, Gracie convinced K.C. to register on the NTU website (ntucapital.com) by telling him that an "expert trader" from NTU would help K.C. with transactions and that his funds would earn a high rate of return on short-term trading. Gracie also said that her uncle had a close relationship with NTU Capital management.

27. But rather than using the NTU Capital platform to conduct his "trading," Gracie instructed K.C. to open an account at Crypto.com where he would wire his money and convert it to cryptocurrency. After K.C. wired money to his Crypto.com account, Gracie instructed him to convert it into USDT and to transfer it to an address that she provided.

28. Right away, the platform showed a fraudulent account balance, which indicated that K.C. was receiving a return on his investment. K.C. then attempted to withdraw $5,000 of his purported "gains" and was able to do so. As a result, K.C. believed the NTU platform was legitimate, and he continued to convert more money into USDT through an exchange account and transfer it to addresses that Gracie provided. In total, K.C. converted approximately $1,000,000 into cryptocurrency and transferred the funds to addresses that Gracie provided. At all times, the fraudulent NTU platform falsely indicated that his investment was producing substantial returns.

29. In February 2022, K.C. attempted to withdraw $600,000 from his NTU account but the transaction was rejected. NTU subsequently froze K.C.'s account on the pretext that his withdrawal triggered the platform's "risk control system." Through a messaging function on the platform, NTU then told K.C. the only way that he could withdraw his funds was if he paid a $307,000 "capital verification fee." K.C. attempted to dispute this with NTU's customer service, but quickly realized he had been the victim of a scam:




**Victim W. C.**

30. Like K.C., W.C. was also a victim of the NTU Capital scam. In September 2021, someone claiming to be W.C.'s old friend—an individual who identified himself as

Bai Luai Lan—contacted W.C. on WhatsApp, and eventually convinced W.C. to invest in cryptocurrency through NTU Capital. Following Lan's instructions, W.C. created an account with NTU Capital and made an initial investment of $35,000 so that he could gain "comfort" with cryptocurrency trading. Like K.C., W.C. was instructed to open an account with Coinbase and to convert USD into USDT. From there, Lan provided the specific addresses where K.C. would send his funds.

31. Immediately, W.C.'s investment appeared to show large returns and Lan began to pressure W.C. to invest even more, which he did.[3] W.C. and W.C.'s spouse subsequently liquidated their retirement accounts, sold a rental home, and took a second mortgage on their personal residence in order to invest more money. From October 2021 to December 2021, W.C., under the direction of Lan, transferred approximately $950,000 into USDT and then transferred the cryptocurrency to addresses that Lan provided.

32. Shortly thereafter, W.C.'s account appeared like it had rapidly increased to approximately $12 million—as displayed on the NTU Capital platform. After W.C.'s investment increased, W.C. and W.C.'s spouse retired from their jobs. W.C. also recruited five of his close friends to invest for themselves.

33. W.C. ultimately invested approximately $4.3 million of his and his friends' funds through "NTU" as well as another fraudulent platform named Create Wealth Global ("CWG"), with the domain cwg-itd.com. Like with his own funds, W.C. converted his friends' money into USDT and then transferred it to addresses that Lan provided. In this time, W.C.'s account purportedly grew to approximately $30 million.

34. Eventually, W.C. attempted to withdraw funds from his account but was told that he could not do so by the CWG platform. Instead, CWG told W.C. that he had to deposit additional money (approximately $524,000) to "verify" W.C.'s capital source. W.C. deposited the additional money requested (approximately $524,000) but was still unable to withdraw any of his funds from the platform.

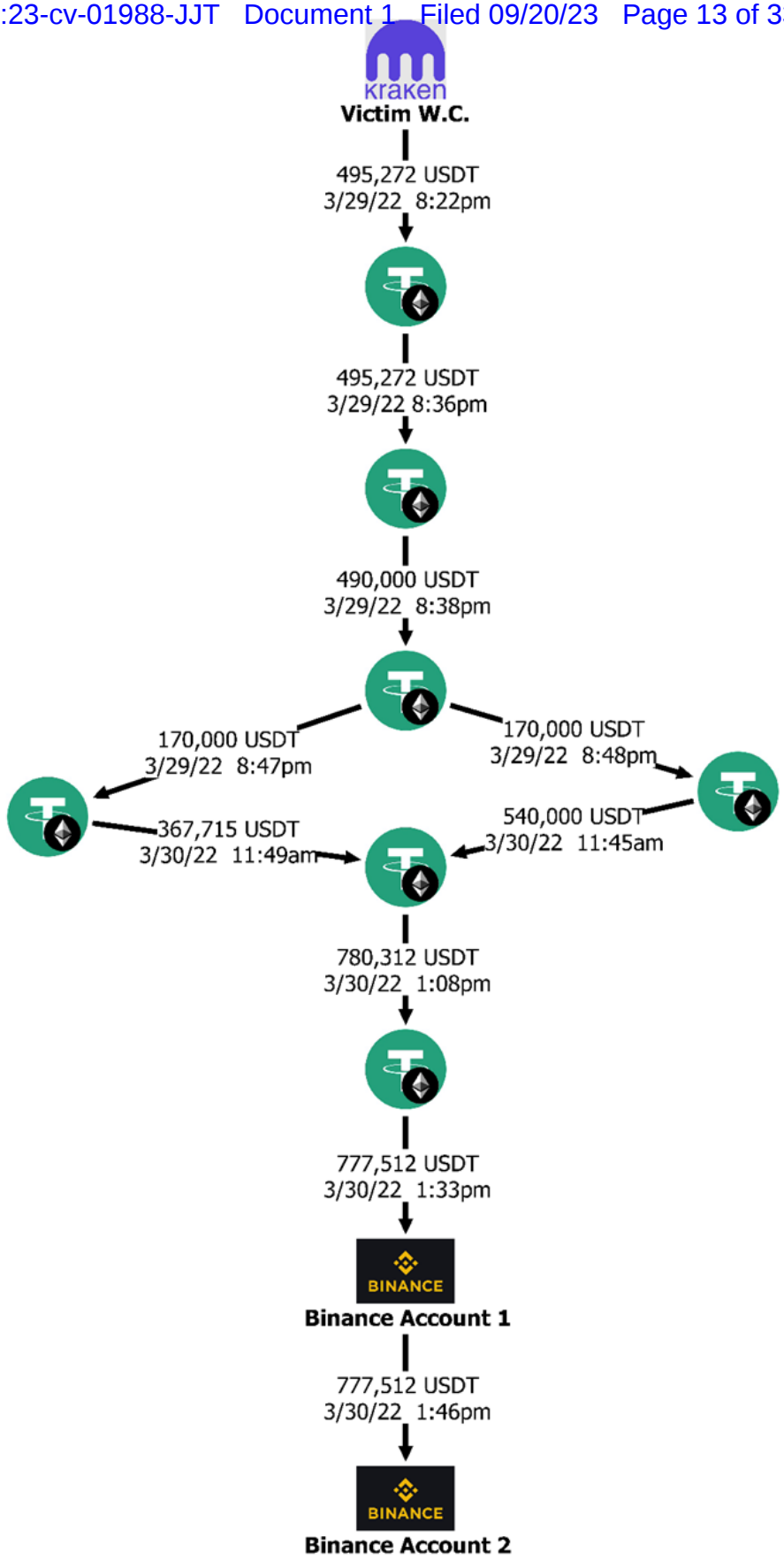
[3] Investment returns displayed on the platform were completely fraudulent and manipulated by the scam organization. In reality, funds are stolen at the moment victims send them to the cryptocurrency addresses provided by the scammers.

35. After W.C. realized he and his friends could not withdraw any funds, he reported the scam to law enforcement, and the FBI traced the W.C. funds, to all three Binance Accounts.

**Direct Tracing of W.C.'s Funds to the Binance Accounts**[4]

36. On March 29, 2022, at Lan's direction, W.C., converted $500,000 USD into USDT, and transferred the cryptocurrency to an address that Lan provided. From there, the funds were rapidly passed through several intermediary addresses between 8:22 p.m. and 8:38 p.m., at which point the funds were split into two 170,000 USDT increments and sent through two more intermediary addresses, where they were comingled with other funds, before arriving at **Binance Account 1.** The funds were then immediately passed through to **Binance Account 2**. These transactions are illustrated below:

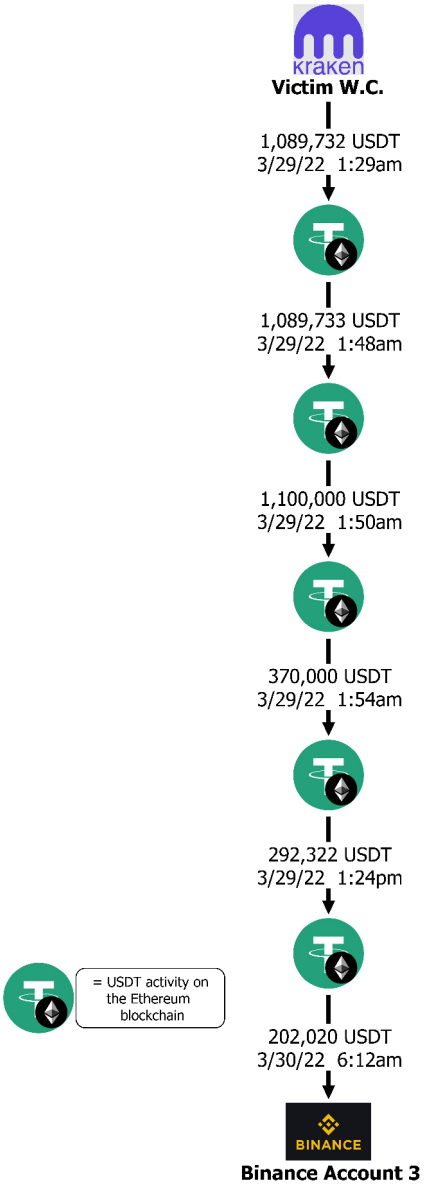
[4] Multiple charts are used in this affidavit to illustrate the flow of cryptocurrency and the connection to the Binance Accounts.


kraken
Victim W.C.
495,272 USDT
3/29/22 8:22pm
495,272 USDT
3/29/22 8:36pm
490,000 USDT
3/29/22 8:38pm
170,000 USDT
3/29/22 8:47pm
170,000 USDT
3/29/22 8:48pm
367,715 USDT
3/30/22 11:49am
540,000 USDT
3/30/22 11:45am
780,312 USDT
3/30/22 1:08pm
777,512 USDT
3/30/22 1:33pm
BINANCE
Binance Account 1
777,512 USDT
3/30/22 1:46pm
BINANCE
Binance Account 2

37. In addition to **Binance Accounts 1 and 2**, money W.C. transferred at Lan's direction was also transferred into **Binance Account 3**—after following a similarly circuitous route through multiple transfers and comingling with other funds.

38. On March 28, 2022, W.C. converted $1,100,000 into USDT (1,089,732) through the cryptocurrency exchange Kraken, and from there, he transferred it to a cryptocurrency address at Lan's direction.

39. FBI forensic accountants have traced those funds through several intermediary wallets—where they were commingled with other funds—before a portion of the funds arrived at **Binance Account 3**, as described in the diagram below:



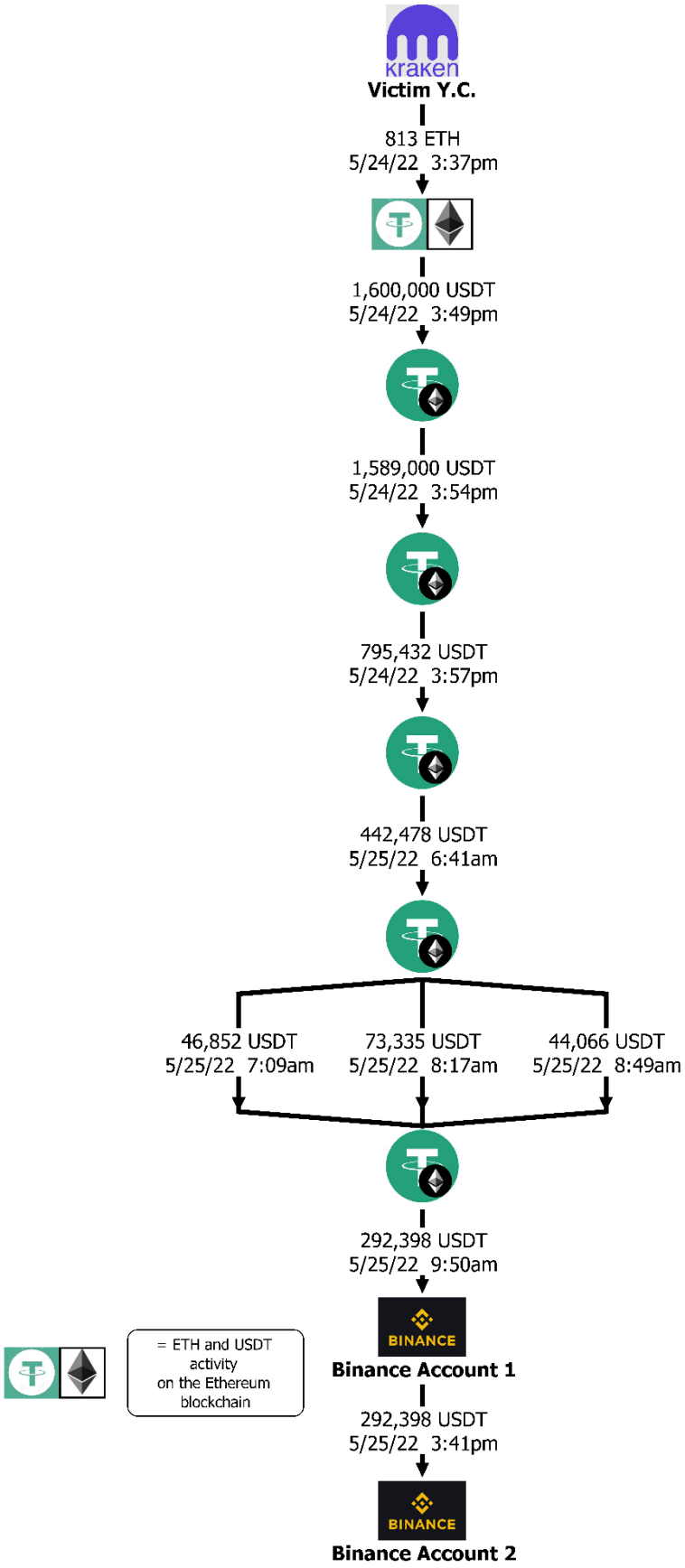
**Victim Y.C.**

40. Y.C. is another victim whose funds were routed through intermediary addresses before arriving in Binance Accounts 1 and 2. In April of 2022, Y.C. was contacted on LinkedIn by an individual who identified herself as "Soda Wang." Wang eventually introduced Y.C. to a cryptocurrency trading platform called "Deribit," a derivative/spoof of a legitimate cryptocurrency trading platform.

41. Wang convinced Y.C. to invest with her and Y.C. then began to invest large sums of money with Wang through a derivative Deribit link that Wang provided. From April to June of 2022, Y.C. sent nearly $5 million in cryptocurrency to addresses at Wang's direction. Eventually, Y.C. attempted to withdraw some of his money but was unable to do so. At this point, he lost contact with Wang and was unable to recover any of the money he invested.

42. Like the other victims, funds that Y.C. transferred at Wang's direction were routed and commingled through several intermediary addresses before arriving at **Binance Accounts 1 and 2**. For example, on May 24, 2022, Y.C. transferred 813 ETH to an address that Wang provided. From there, the funds were immediately converted to USDT, at which point the funds were transferred through five intermediary addresses before arriving in **Binance Accounts 1 and 2**.

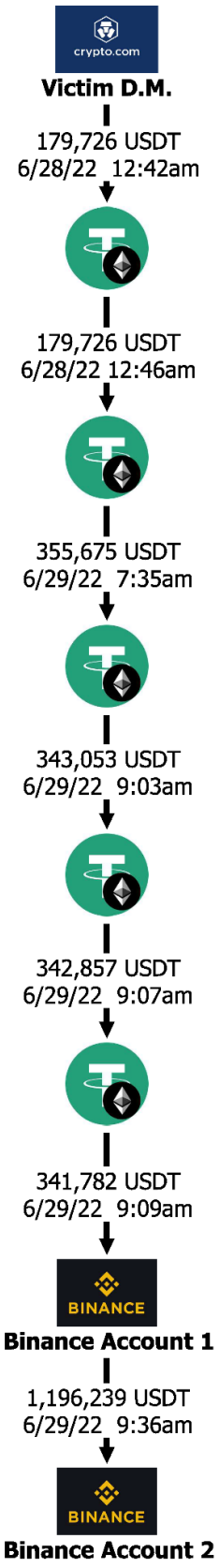
43. Like the other victims, funds that Y.C. transferred at Wang's direction were routed and commingled through several intermediary addresses before arriving at **Binance Account 1**. Later that same day, the funds were withdrawn from **Binance Account 1** and transferred to **Binance Account 2**, as depicted in the following diagram:


kraken
Victim Y.C.
813 ETH
5/24/22 3:37pm
1,600,000 USDT
5/24/22 3:49pm
1,589,000 USDT
5/24/22 3:54pm
795,432 USDT
5/24/22 3:57pm
442,478 USDT
5/25/22 6:41am
46,852 USDT
5/25/22 7:09am
73,335 USDT
5/25/22 8:17am
44,066 USDT
5/25/22 8:49am
292,398 USDT
5/25/22 9:50am
BINANCE
Binance Account 1
292,398 USDT
5/25/22 3:41pm
BINANCE
Binance Account 2
= ETH and USDT activity on the Ethereum blockchain

**Victim D.M.**

44. D.M. is another victim of a pig butchering scheme whose funds were directed **to Binance Account 1** and then passed through to **Binance Account 2**. The scheme began when a woman who identified herself as "Irene" "mistakenly" contacted D.M. on WhatsApp. Irene eventually convinced D.M. to invest approximately $90,000 through a fraudulent investment platform called "Aly Financial" apparently meant to spoof legitimate company Ally Financial. Very shortly after D.M.'s initial investment, D.M.'s account showed that it had risen to $1.3 million. As a result, D.M. invested more than $800,000 in total funds. When he attempted to withdraw funds from his account, he was unable to do so and realized he was the victim of a scam.

45. Like others, funds that D.M. converted to cryptocurrency and then transferred to an address that "Irene" provided were eventually commingled with other funds and passed through several intermediary addresses in route to **Binance Account 1**, and from there were passed through to **Binance Account 2**. On June 28, 2022, D.M. converted approximately $190,000 into USDT (which was reduced to 179,726 in USDT due to conversion fees) and transferred it to an address that Irene gave him. From there, the funds were transferred through four intermediary addresses, where they were comingled with other funds, before they arrived at **Binance Account 1** at 9:00 a.m. the next day. The funds were then commingled with four other transfers totaling 1,196,239 USDT. Less than thirty minutes later, 1,196,239 USDT was withdrawn from **Binance Account 1** and transferred to **Binance Account 2**:


crypto.com
Victim D.M.
179,726 USDT
6/28/22 12:42am
179,726 USDT
6/28/22 12:46am
355,675 USDT
6/29/22 7:35am
343,053 USDT
6/29/22 9:03am
342,857 USDT
6/29/22 9:07am
341,782 USDT
6/29/22 9:09am
BINANCE
Binance Account 1
1,196,239 USDT
6/29/22 9:36am
BINANCE
Binance Account 2

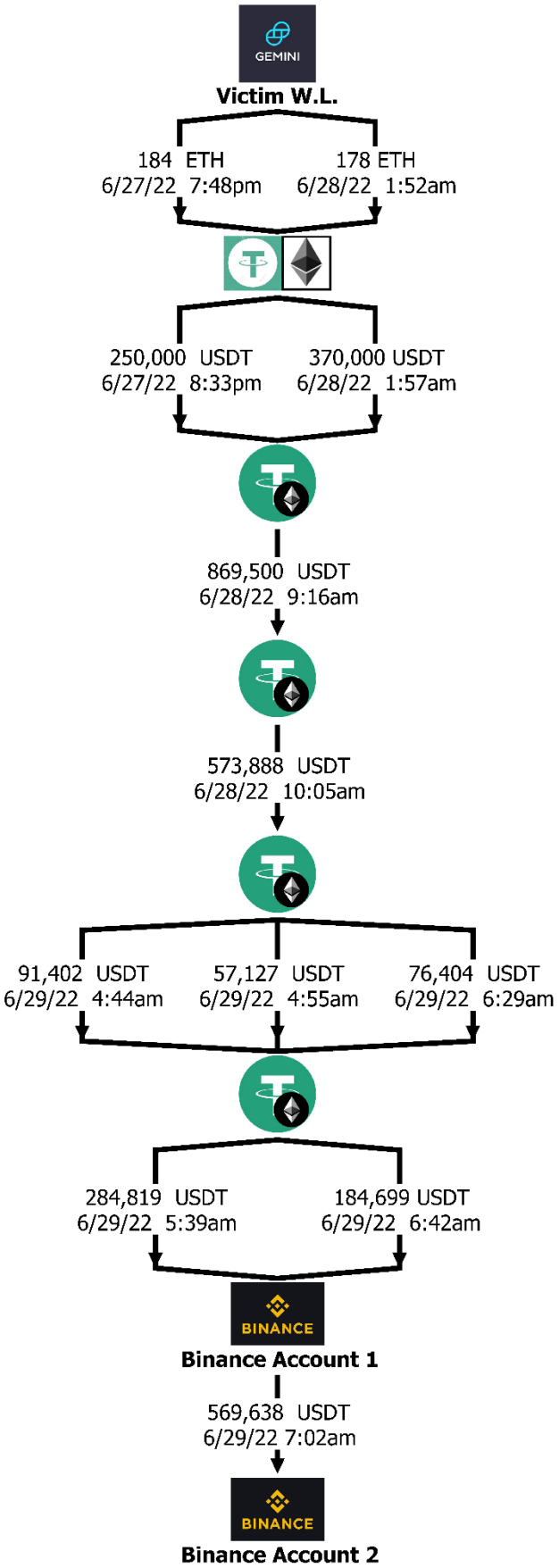
**Victim W.L.**

46. In addition to the victims mentioned above, the FBI also received an online complaint submitted through the website, IC3.gov, from a victim, W.L., whose funds were also routed to **Binance Accounts 1 and 2**. According to the complaint submitted on August 7, 2022, W.L. lost $1,690,000 in an online investment scam. W.L. reported that he was approached by an unknown female, whom he identified as "Ailin Chen," through LinkedIn in early June 2022. Chen told W.L. that there was an excellent opportunity to invest in cryptocurrency (specifically in a coin called "MANA") by following a large investor who was trading on its future contract.

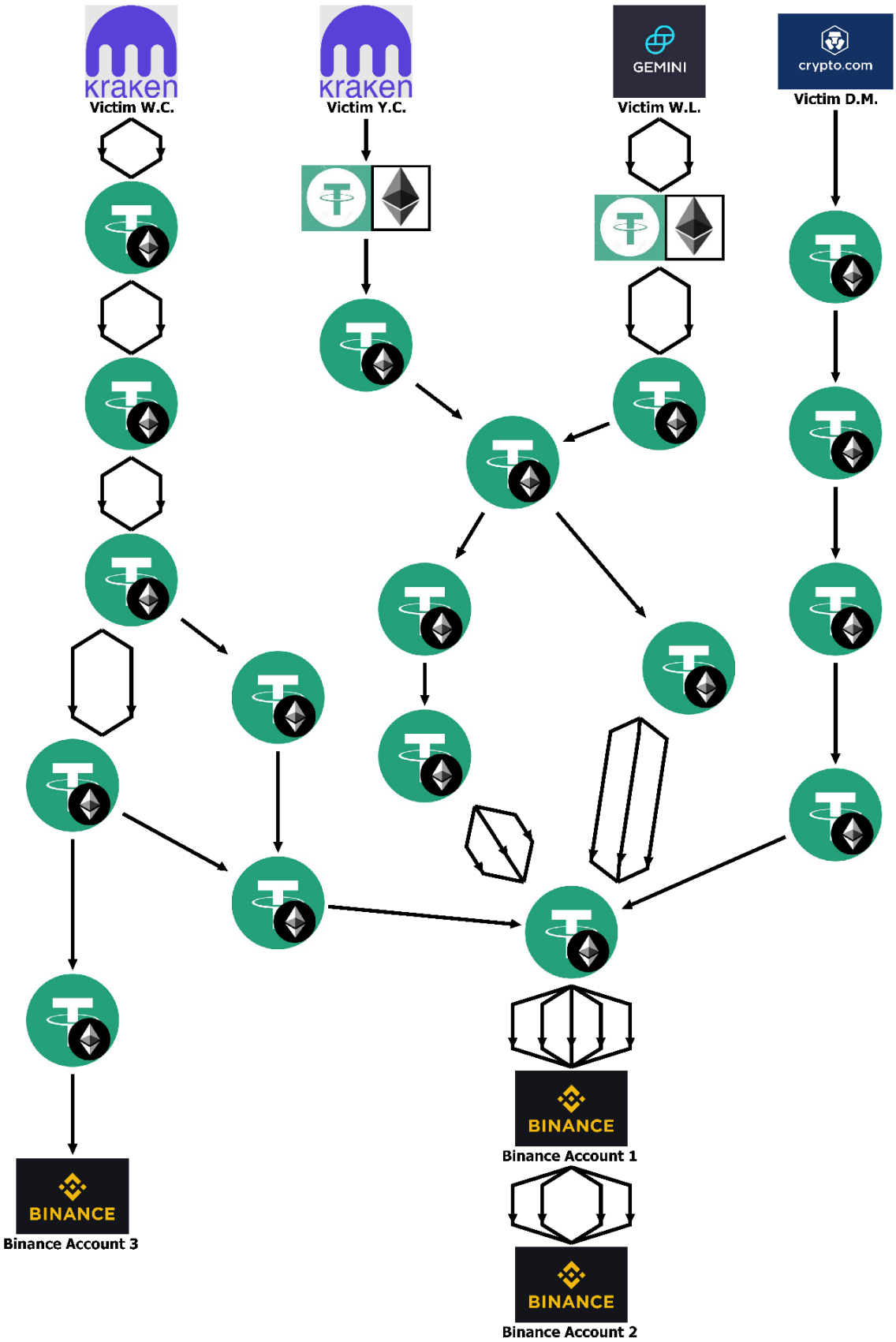
47. Chen convinced W.L. to "invest" in another fraudulent derivative of the Deribit site (deribit-w.net). Chen then showed W.L. how to open an account on the derivative site. After that, Chen told W.L. to open an account at the cryptocurrency exchange Gemini to convert funds from his bank to cryptocurrency.

48. W.L. agreed to do so, and started with $10,000, which he converted to the cryptocurrency MANA and transferred to an address that Chen provided. W.L. eventually converted more than $1,500,000 into cryptocurrency and transferred it to addresses that Chen provided. At one point, W.L.'s "account" purportedly showed that his investment had gone up to $4.9 million in equivalent USD. When W.L. attempted to withdraw his funds, he was unable to do so.

49. Like other victims, funds that W.L. sent to addresses Chen provided were ultimately directed to **Binance Accounts 1 and 2**. For example, on June 27, 2022, W.L. transferred 184 ETH to an address that Chen provided. The next day, on June 28, W.L. transferred another 178 ETH to the same address. As provided in the chart below, both amounts of ETH were immediately converted to USDT and were subsequently transferred through several intermediary addresses before a portion of the funds were transferred into **Binance Account 1** on June 29, 2022. Later that same morning, the funds were then transferred to **Binance Account 2**:


GEMINI
Victim W.L.
184 ETH
6/27/22 7:48pm
178 ETH
6/28/22 1:52am
250,000 USDT
6/27/22 8:33pm
370,000 USDT
6/28/22 1:57am
869,500 USDT
6/28/22 9:16am
573,888 USDT
6/28/22 10:05am
91,402 USDT
6/29/22 4:44am
57,127 USDT
6/29/22 4:55am
76,404 USDT
6/29/22 6:29am
284,819 USDT
6/29/22 5:39am
184,699 USDT
6/29/22 6:42am
BINANCE
Binance Account 1
569,638 USDT
6/29/22 7:02am
BINANCE
Binance Account 2

50. In sum, each of the four victims referenced above were victims of similar pig butchering schemes. The following chart depicts the sophisticated and convoluted movement of victim funds described above, with the common denominator being that some portion of the victims' funds were in various ways directed to the **Binance Accounts**. Moreover, the same individual(s) or entity(ies) appear to control the **Binance Accounts**. Indeed, the use of purportedly separate accounts, which are actually linked to the same scheme, is a tactic that criminals use when attempting to disguise the ultimate source and destination of funds, as displayed below:

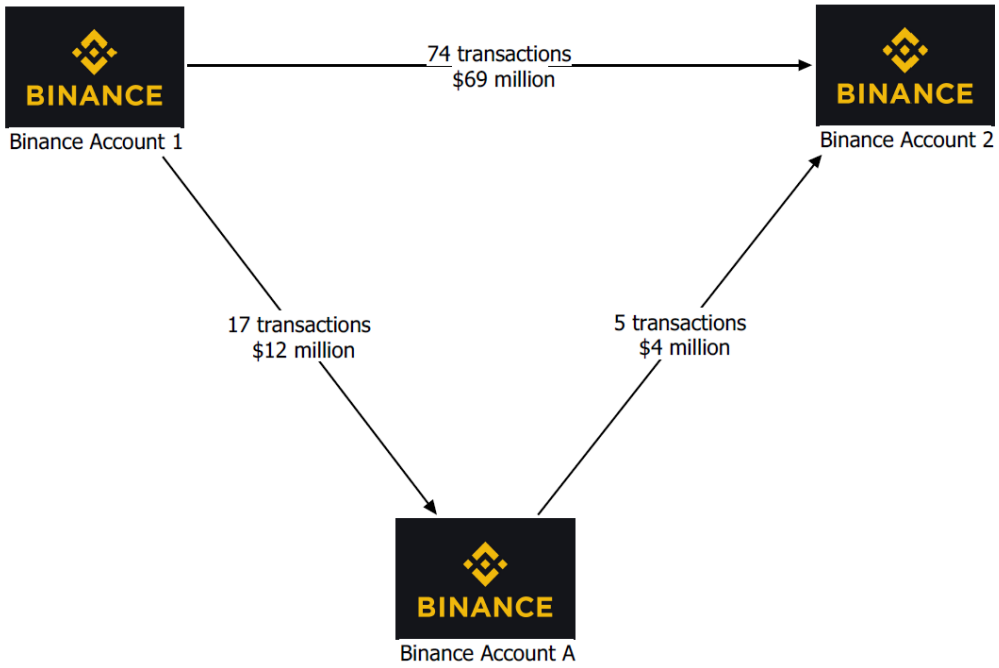

kraken
Victim W.C.
kraken
Victim Y.C.
GEMINI
Victim W.L.
crypto.com
Victim D.M.
BINANCE
Binance Account 3
BINANCE
Binance Account 1
BINANCE
Binance Account 2

**Binance Accounts 1 and 2 Facilitated Money Laundering**

51. Forensic analysis of **Binance Accounts 1 and 2** revealed the use of hundreds of intermediary wallet addresses, entirely separate blockchains, and multiple layers of exchange accounts, used to obfuscate the flow of funds into **Binance Accounts 1 and 2**.[5]

52. To start, because **Binance Accounts 1 and 2** are located at the cryptocurrency exchange Binance, transfers between them are not recorded on a public blockchain. This means that transfers between them cannot be viewed by the public or anyone doing an analysis of the blockchain without legal process or cooperation from Binance.

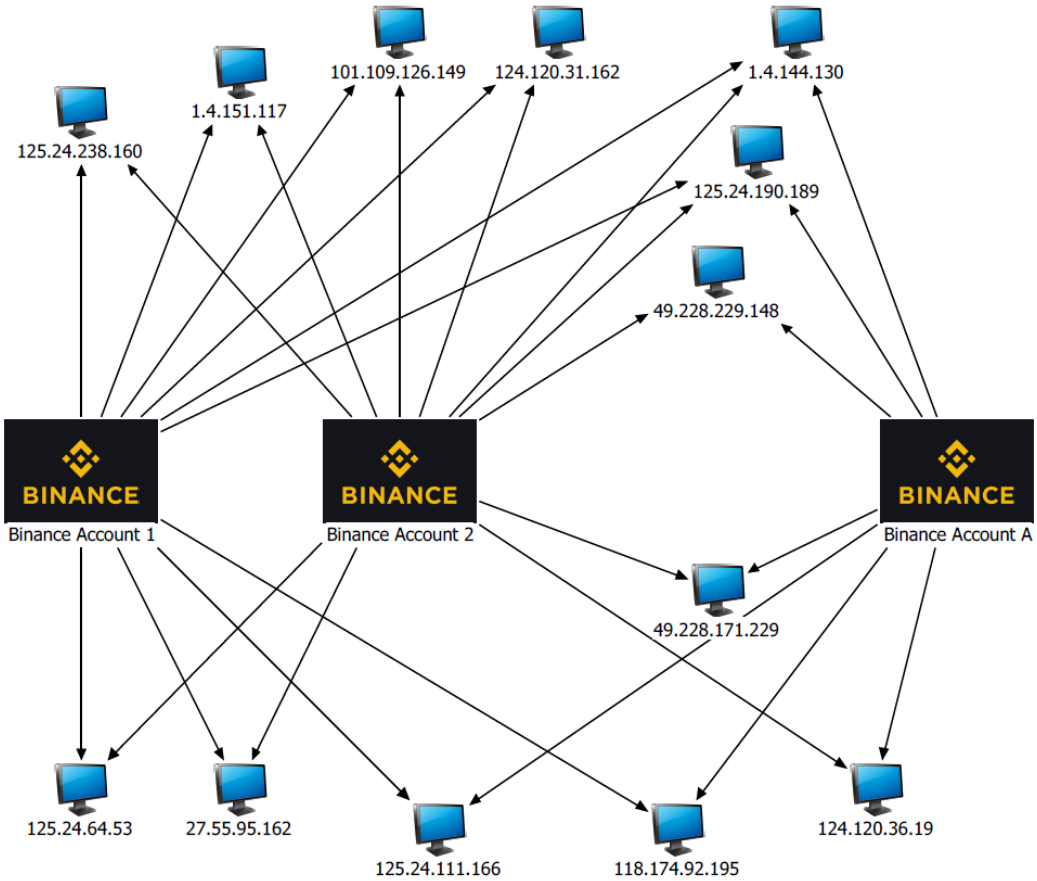
53. Over its entire history, **Binance Account 2** has only ever received transfers from two other Binance accounts: **Binance Account 1** and a Binance account identified as "Binance Account A":




[5] The section does not focus on **Binance Account 3** because the amount of fraudulent funds traced into **Binance Account 3** closely mirrored the account balance when seized. Nevertheless, **Binance Account 3** was also used to launder fraudulently obtained funds as alleged in ¶¶ 41-43.

54. As depicted above, from February 2021 to August 2022 **Binance Account 1** transferred approximately $69 million to **Binance Account 2** over the course of 74 transactions. The only other account that sent money to **Binance Account 2** throughout its entire history was Binance Account A (depicted above). Binance Account A sent approximately $4 million to **Binance Account 2** over the course of five transactions.

55. Even though these accounts are registered in the names of separate individuals, they appear to be under common control. Forensic analysis of **Binance Accounts 1 and 2,** and Binance Account A, demonstrate that all three accounts have been accessed from the same IP addresses. For example, there were 266 instances in which the same IP address was used to access more than one of these accounts.[6] The following figure shows the IP addresses that were used to access more than one of the accounts:



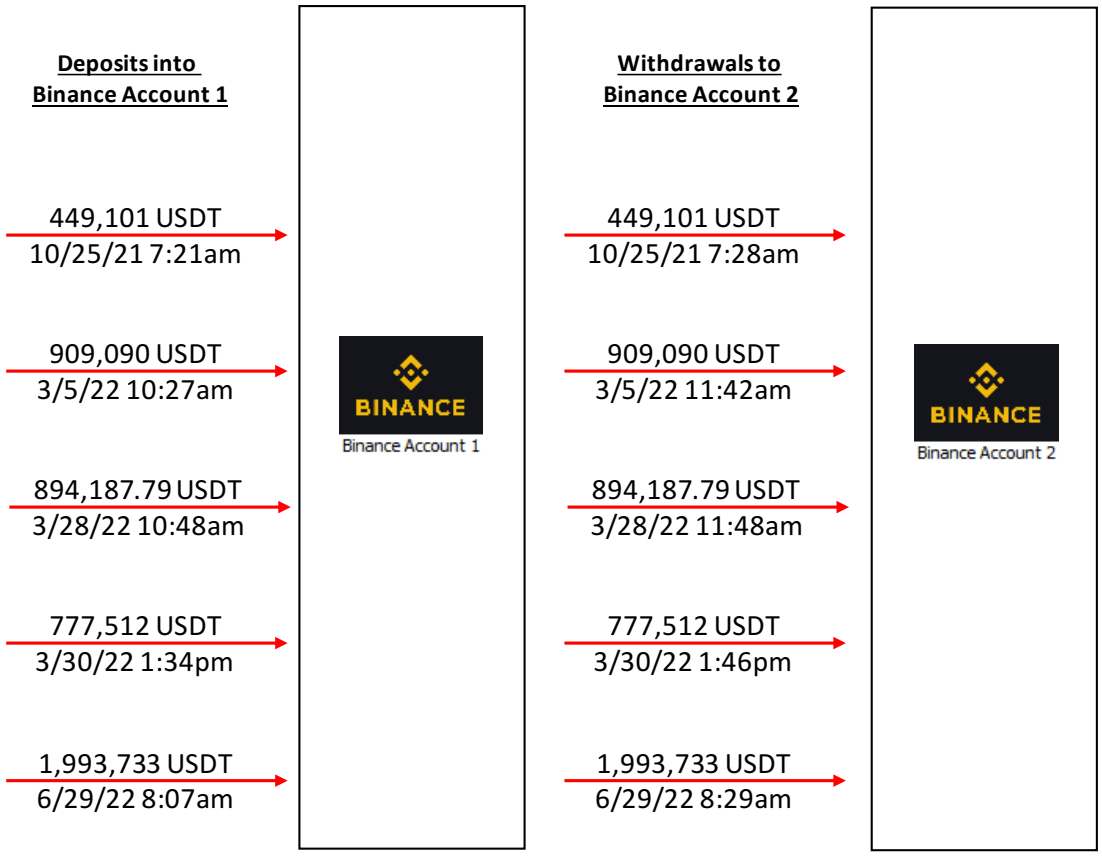

[6] An IP address is a numerical label connected to a computer network, which serves to identify a specific network and its location.

56. For many of these contacts, the same IP address accessed more than one of the accounts within minutes of each other.

57. Forensic analysis of **Binance Accounts 1 and 2** also demonstrates that **Binance Account 1** is most likely a pass-through account that is *not* intended to store funds because nearly all the funds sent to **Binance Account 1** were almost immediately passed through to **Binance Account 2**.

58. For instance, at the time the accounts were frozen, in the fall of 2022, **Binance Account 1** only had a balance of $935,000 in USD equivalent cryptocurrency, despite passing more than $69 million through to **Binance Account 2** over its lifetime. Likewise, as discussed above, aside from five transactions, the entirety of funds flowing into **Binance Account 2** all come from **Binance Account 1**.

59. Forensic analysis also uncovered a pattern of rapid transfers from **Binance Account 1** to **Binance Account 2**. The following figure provides an example of several large transactions that were delivered to **Binance Account 1** and then almost immediately (within approximately one hour) transferred to **Binance Account 2**:

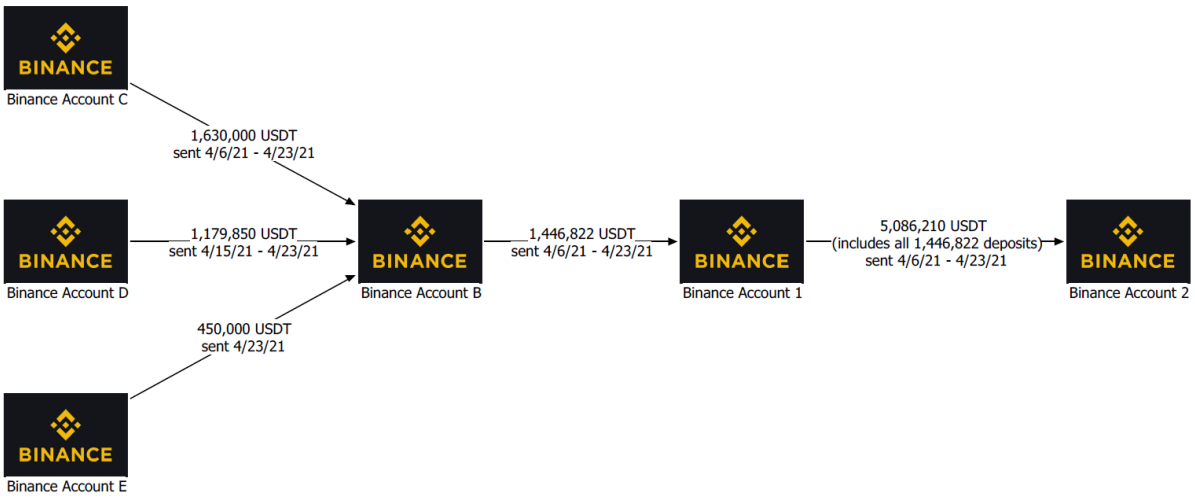



**Binance Account 1 is a Pass-Through Account**

60. In addition to what has already been identified above, forensic analysis revealed a sophisticated and concerted effort to obfuscate the flow of funds into **Binance Account 1** (nearly all of which were then passed through to **Binance Account 2**).

61. To start, investigators identified a rapid movement of funds between other Binance accounts into **Binance Account 1**. For instance, investigators discovered that several layers of Binance accounts were used to move funds into **Binance Account 1**, which is a common method that can be used to hide the flow of funds from the public blockchain, thereby making the funds harder to identify and trace.

62. The following figure is one example that investigators identified to demonstrate the movement of funds through several different Binance accounts on their way to **Binance Accounts 1 and 2**, all within a narrow date range:




63. As shown above, from April 6 to April 23, 2021, investigators identified that the Binance account identified as "Binance Account B" above deposited 1,446,822 USDT into **Binance Account 1** (all of which was subsequently passed through to **Binance Account 2**). When investigators then attempted to analyze the flow of funds into Binance Account B, they discovered that 89% of the deposits came from other Binance accounts—including those identified as Binance Accounts C-E above.[7] As previously explained, moving cryptocurrency from one Binance account to another is a potential method to hide the flow of funds from publicly available blockchains, thereby making it harder for law enforcement to trace.

64. In addition, upon reviewing the individual transactions from the April 6 to April 23, 2021, time period depicted above, FBI forensic accountants discovered that funds were often moved from one account to another in a coordinated manner. For instance, on April 23, 2021, a single Binance account transferred the exact same amount (151,837 USDT) to **Binance Account 1** in three separate transactions over the course of one hour (similar events occurred on April 21, 2021, and from April 7 to 19, 2021). This

[7] The deposit history in Binance Accounts C-E similarly showed that the source of funds was largely other Binance accounts. For example, Binance Account E had total deposits of over 30 million USDT, and all but a single deposit came from other Binance accounts. These accounts also appear to be linked because there are two IP addresses that accessed both Binance Accounts C and D, indicating that the same individual(s) may be controlling both accounts.

conduct is indicative of layering in order to disguise the flow funds as it hard to conceive of an otherwise legitimate basis for coordinating the transfer of funds in this manner, not least because each transfer generates its own transfer fee that could be avoided simply by transferring the entire amount in one transaction.

65. In short, before funds even get to **Binance Account 1** (and are then passed into **Binance Account 2**) there are several layers of preceding transactions that are methodically coordinated to obscure the flow of funds, which are all hidden from public view.

**Chain Hopping**

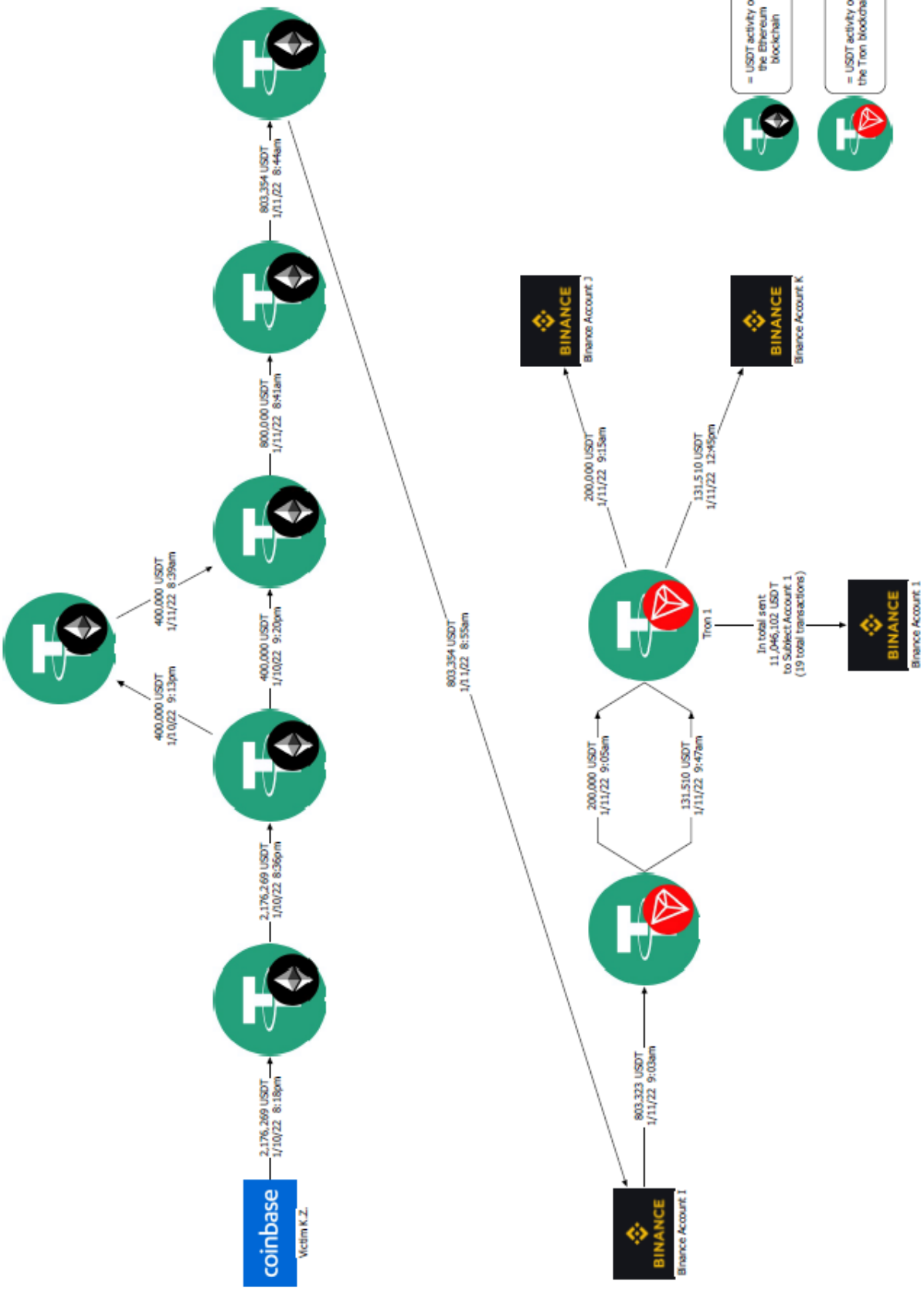
66. "Chain hopping" occurs when the holder of cryptocurrency converts it from one from of cryptocurrency to another—for instance, converting Bitcoin to Ethereum. When cryptocurrency is converted, it can make it harder to trace because it will often result in the currency being moved onto a separate blockchain ledger.

67. In this case, the FBI discovered that approximately half of all the funds transferred into **Binance Account 1** were from the "Tron" blockchain, which is a separate blockchain from those discussed thus far. Of those deposits into **Binance Account 1**, approximately 75% were from the same two addresses, which are referred to below as Tron 1 and Tron 2

68. To start, **Binance Account 1** received more than 11 million USDT from Tron 1 over 19 transactions. When analyzing the transactions in Tron 1, the FBI identified cryptocurrency that was traced backwards from Tron 1 to another victim (K.Z.) of a similar pig butchering scheme. K.Z. ultimately sent over $5 million to addresses provided by scammers before realizing it was a scam.

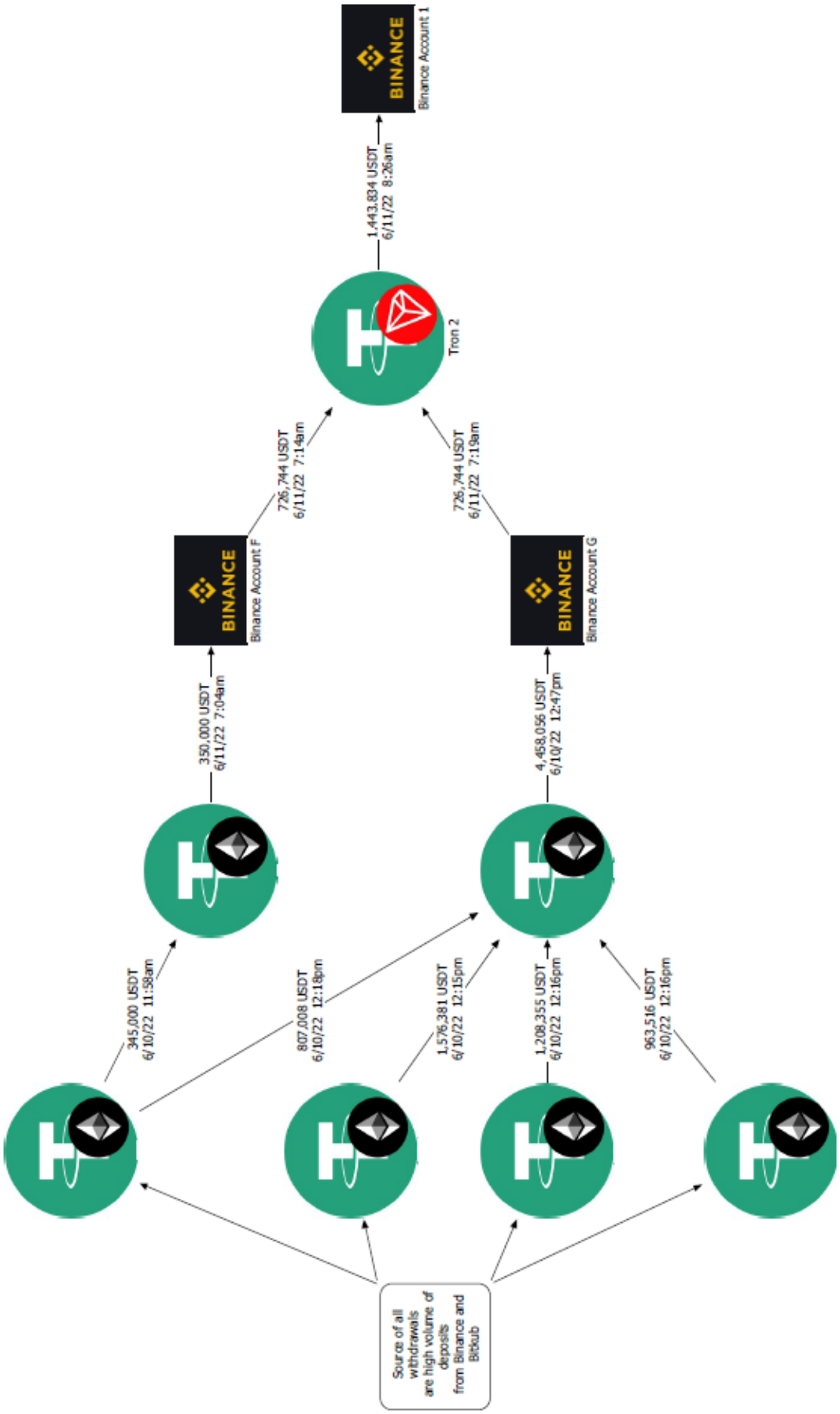
69. One of K.Z.'s transactions, for 2,176,269 USDT, was eventually traced to Tron 1. The diagram below shows the flow of K.Z.'s funds, which started as USDT on the Ethereum blockchain, but were then converted to USDT on the Tron blockchain, before they were ultimately directed to Tron 1 and then to two other Binance accounts:[8]

[8] The diagram also demonstrates the 11 million USDT that Tron 1 transferred to **Binance Account 1.**


= USDT activity on the Ethereum blockchain
= USDT activity on the Tron blockchain
coinbase
Victim K.Z.
2,176,269 USDT 1/10/22 8:18pm
2,176,269 USDT 1/10/22 8:36pm
400,000 USDT 1/10/22 9:13pm
400,000 USDT 1/11/22 8:39am
400,000 USDT 1/10/22 9:20pm
800,000 USDT 1/11/22 8:41am
803,354 USDT 1/11/22 8:44am
803,354 USDT 1/11/22 8:55am
803,323 USDT 1/11/22 9:03am
200,000 USDT 1/11/22 9:05am
131,510 USDT 1/11/22 9:47am
200,000 USDT 1/11/22 9:15am
131,510 USDT 1/11/22 12:45pm
In total sent 11,046,102 USDT to Subject Account 1 (19 total transactions)
Tron 1
BINANCE
Binance Account 1
Binance Account 2
Binance Account K

70. Efforts to trace the remaining deposits into Tron 1 were difficult, however, because the funds were moved through a vast network of addresses and Binance accounts. For instance, on May 24, 2022, Tron 1 sent two transactions to **Binance Account 1** just minutes apart for a total of 1,033,034 USDT. Utilizing the publicly available Tron blockchain, the USDT was traced backwards through five addresses, which showed that the funds were transferred in rapid succession just minutes and hours apart. But after following these first five addresses, the ability to forensically reconstruct the flow of funds broke down because the address that initiated the flow of funds received 47 deposits from 15 different Tron addresses.

71. The FBI discovered similar patterns of rapid transfers through various intermediary wallet addresses all designed to obfuscate the flow of funds when analyzing the flow of funds into Tron 2 and then to **Binance Account 1**. For instance, on June 11, 2022, **Binance Account 1** received 1.4 million USDT in a single deposit from Tron 2. Those funds, however, were initially routed to Tron 2 from a separate blockchain, and through multiple Binance accounts, in a coordinated manner as displayed in the figure below:


BINANCE
Binance Account 1
1,443,834 USDT
6/11/22 8:26am
Tron 2
726,744 USDT
6/11/22 7:14am
726,744 USDT
6/11/22 7:19am
BINANCE
Binance Account F
BINANCE
Binance Account G
350,000 USDT
6/11/22 7:04am
4,458,056 USDT
6/10/22 12:47pm
345,000 USDT
6/10/22 11:58am
807,008 USDT
6/10/22 12:18pm
1,576,381 USDT
6/10/22 12:15pm
1,208,355 USDT
6/10/22 12:16pm
963,516 USDT
6/10/22 12:16pm
Source of all withdrawals are high volume of deposits from Binance and Bitkub

72. In short, the rapid transfer of funds described above—which come from several different wallet addresses and are then reconsolidated before being passed through Tron 2 on their way to **Binance Account 1**—indicate a concerted effort to obfuscate the flow of funds and to hide entirely the location and source of the funds.

73. Furthermore, the evidence presented herein, and further developed throughout the FBI's investigation reveals that the **Binance Accounts** were deliberately set up to hide the flow of funds from victims—such as W.C., Y.C., D.M. and W.L.—whose funds were distributed through various intermediate wallet addresses and accounts in a sophisticated and circuitous manner meant to obfuscate their origin and make them difficult to trace.

## FIRST CLAIM FOR RELIEF

74. The United States realleges, adopts, and incorporates all allegations stated in paragraphs 1 to 73 as though fully set forth herein.

75. The defendant property constitutes or is derived from proceeds traceable to a violation of a specified unlawful activity as defined in 18 U.S.C. § 1956 (c)(7), including wire fraud, 18 U.S.C. § 1343, or a conspiracy to commit such offense, and therefore is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

## SECOND CLAIM FOR RELIEF

76. United States realleges, adopts, and incorporates all allegations stated in paragraphs 1 to 73 as though fully set forth herein.

77. The defendant property was involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 and/or 1957, and therefore is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

## PRAYER FOR RELIEF

WHEREFORE, the United States of America prays that process issue for an arrest warrant *in rem* issue for the arrest of the defendant property; that due notice be given to all parties to appear and show cause why the forfeiture should not be decreed; that judgment be entered declaring the defendant property be forfeited to the United States of America

for disposition according to law; and that the United States of America be granted such other and further relief as this Court deems just and proper, together with the costs and disbursements of this action.

Respectfully submitted this 20th day of September, 2023.

GARY M. RESTAINO
United States Attorney
District of Arizona

*s/Joseph F. Bozdech*
JOSEPH F. BOZDECH
SETH T. GOERTZ
Assistant United States Attorneys