

1 SUE FAHAMI  
Acting United States Attorney  
2 Nevada Bar Number 5634  
MISTY L. DANTE  
3 Assistant United States Attorney  
501 Las Vegas Boulevard South, Suite 1100  
4 Las Vegas, Nevada 89101  
(702) 388-6336  
5 Misty.Dante@usdoj.gov  
*Attorneys for the United States*

7  
8 **UNITED STATES DISTRICT COURT  
DISTRICT OF NEVADA**

9 United States of America,

10 Plaintiff,

11 v.

12 519803.53164 USDT and 1135.508 XMR  
that are associated with transaction hashes  
13 0x1ac48e72bb2fd83ad60a0f3f0cea5036e3bdc  
fe593a4a9be53c12c44a6197421,  
14 0xbc0e435002aba822c6355e4f7571fe9b0d82  
2e17e448c7262b2c9114ec325228, and  
15 0x3e989f0de45e39c89e86032acc59e33c5161  
d492dde3c7b09ea19408ba74c931 sent to  
16 Gate.io USDT address  
0x6BC5C2661D75f0Ced80754D3C7bD651f  
17 1d60f736 and held in the name of Avalanche  
Bridge,

18 Defendant.

2:25-CV-

**Complaint for Forfeiture in Rem**

19  
20 The United States of America in a civil cause for forfeiture, respectfully states as  
21 follows:

22 **SUBJECT MATTER JURISDICTION**

23 1. This Court has jurisdiction under 19 U.S.C. §§ 1603, 1608, and 1610;  
24 Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions (Fed.  
25 R. Civ. P. Supp. Rule) C, E, and G; 18 U.S.C. § 981(a)(1)(A); 18 U.S.C. § 981(a)(1)(C); 18  
26 U.S.C. § 983; 18 U.S.C. § 984; and 28 U.S.C. §§ 1345, 1355, and 1395 because (1) the  
27 United States of America commenced this civil in rem action; (2) any of the acts or  
28 omissions giving rise to this forfeiture occurred in this judicial district; (3) the forfeiture

1 proceeding accrues in this judicial district; and (4) the above-named property is currently in  
2 this judicial district.

3 **IN REM JURISDICTION**

4 2. This Court will have in rem jurisdiction over the defendant if this Court signs  
5 an Order for Summons and Warrant of Arrest in Rem for the Property and the Clerk of the  
6 Court issues a Summons and Warrant of Arrest in Rem for the Property, which will be  
7 executed upon the defendant and returned to the Court.

8 **VENUE**

9 3. This Court is the proper venue of this matter under 28 U.S.C. § 1395, Fed. R.  
10 Civ. P. Supp. Rule C(2)(c) and G(1) because (1) the forfeiture proceeding accrues in this  
11 judicial district and (2) the above-named property (a) is currently in this judicial district and  
12 (b) was brought into this judicial district.

13 **PARTICULAR DESCRIPTION**

14 4. The defendant is more particularly described as follows: 519803.53164  
15 USDT (519803 USDT)<sup>1</sup> and 1135.508 XMR (1135 XMR)<sup>2</sup> that are associated with  
16 transaction hashes  
17 0x1ac48e72bb2fd83ad60a0f3f0cea5036e3bdcfe593a4a9be53c12c44a6197421,  
18 0xbc0e435002aba822c6355e4f7571fe9b0d822e17e448c7262b2c9114ec325228, and  
19 0x3e989f0de45e39c89e86032acc59e33c5161d492dde3c7b09ea19408ba74c931 sent to  
20 Gate.io<sup>3</sup> USDT address 0x6BC5C2661D75f0Ced80754D3C7bD651f1d60f736 (property).

21 **PLACE OF SEIZURE**

22 5. On March 20, 2024, the Federal Bureau of Investigation seized the 519803  
23 USDT and 1135 XMR from gate.io through the transfer of the defendant property to an  
24 FBI cryptocurrency wallet.

25  
26 

---

<sup>1</sup> A type of digital coin named Tether. The value of this coin is backed by the value of the  
27 United States Dollar.

<sup>2</sup> XMR refers to cryptocurrency named Monero, a privacy-oriented cryptocurrency.

28 <sup>3</sup> Gate.io is a crypto exchange which provides a user of the platform the ability to buy, sell,  
or swap digital currencies.

**CUSTODY OF ASSET**

6. The defendant property is currently in the care, custody, and control of the FBI and is currently being stored in the FBI vault located in Las Vegas, Nevada.

**TIMELY FILING**

7. This Complaint is timely filed.

**VALUE**

8. At the time of the seizure, the value of the defendant property was \$519,803.53 for the USDT and \$158,000 for the XMR. The value of the defendant property will increase or decrease based on the current value of the cryptocurrency in the global marketplace.

**FORFEITURE STATUTES**

9. Because of the information below, the defendant property is subject to forfeiture to the United States of America under 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C).

**FACTS**

10. On August 18, 2023, a company (Victim A) located in Las Vegas, Nevada, was the victim of a cyber-attack.

11. The unknown subjects gained unauthorized access into Victim A's network and stole sensitive company data.

12. The unknown subjects demanded Victim A to pay the unknown subjects in bitcoin (BTC)<sup>4</sup> and threatened that the data would be publicly released if Victim A did not comply.

13. The unknown subjects initially demanded \$30 million USD worth of BTC be paid by Victim A or the sensitive data would be publicly released.

14. Victim A negotiated the extortion payment down to approximately \$15 million USD. The unknown subjects promised to delete the stolen data after they received the payment.

---

<sup>4</sup> A glossary of cryptocurrency-related terms is provided in Exhibit 1 to the Complaint.

1 15. Victim A paid the extortion payment in two separate purchases of BTC.  
2 Through subsequent analysis (using a commercially available crypto-tracing tool), law  
3 enforcement traced the BTC transactions sent from Victim A to a point known in crypto  
4 currency transactions as a bridge, in this case extortion payment wallets Avalanche Bridge.  
5 The property was traced based on the “Illegal Proceeds In, First Out” (or last-in, first-out)  
6 accounting principle, which assumes that the last or most recent incoming assets are the  
7 first expended or sent out. *See United States v. Banco Cafetero Panama*, 797 F.2d 1154, 1160  
8 (2d Cir. 1986) (government can establish prima facie case for forfeiture by relying on the  
9 “last-in, last-out” approach or the “last-in, first-out” approach.)<sup>5</sup>

10 16. A detailed summary flowchart attached as Exhibit 2 describes the transfer of  
11 the illegal proceeds from the extorted payments made by Victim A to the unknown  
12 subjects.

13 17. When the illegal proceeds were transferred from the extorted payments made  
14 by Victim A to the unknown subjects, BTC fees, in the form of a minute portion of the  
15 BTC, may have been paid in small amounts as each transaction progressed.<sup>6</sup>

16 18. Victim A paid the unknown subjects through two separate transactions. On  
17 September 11, 2023, Victim A sent the first payment in the amount of approximately 297  
18 BTC to BTC address bc1qmrcc0dtdn3c785phmcf5wtz98q9qy8ndpd5ev (Extortion Wallet  
19 1).

20 / / /

21 \_\_\_\_\_  
22 <sup>5</sup> Also known as the “‘drugs-in, first-out’ rule. As the name suggests, this rule posits that  
23 when withdrawals are made, tainted money leaves the account first.” *United States v. Dillion*,  
24 No. 1:16-cr-00037-BLW, 2022 WL 2105974, \*4 (D. Ida. Jun. 10, 2022) (citing *Banco*, 797  
25 F.2d at 1158

26 <sup>6</sup> Bitcoin (BTC) fees are the costs that users pay to have their transactions processed by  
27 miners on the Bitcoin network. These fees incentivize miners to include transactions in the  
28 blocks they create. The amount of the fee can vary based on several factors, including  
network congestion and the transaction size. Network congestion occurs when the Bitcoin  
network is congested (i.e., there are more transactions waiting to be processed than available  
space in the blocks), fees increase because users compete to have their transactions  
confirmed quickly. Transaction size fees are calculated based on the size of the transaction  
in bytes, rather than the amount of Bitcoin being transferred. Larger transactions (in terms  
of data size) will require higher fees. *See also*  
<https://youtu.be/waP7n8crMhg?si=SAPuglPJD5AqE3HU>.

1 19. On October 11, 2023, Victim A paid the second payment in the amount of  
2 approximately 277 BTC. As instructed to do so by the unknown subjects, Victim A sent the  
3 second payment to BTC address bc1q5ft3et8h0qp4ppk6hjjhfxmmy32egzgvrgtwsn  
4 (Extortion Wallet 2).

5 20. Prior to these transfers, Extortion Wallet 1 and Extortion Wallet 2 did not  
6 have a balance, nor did either wallet receive any additional payments. Therefore, there was  
7 no co-mingling of any previous cryptocurrencies. Upon information and belief, Extortion  
8 Wallet 1 and Extortion Wallet 2 appeared to have been opened only for the purpose of  
9 receiving these two payments.

10 21. On September 12, 2023, the unknown subjects who had access/ownership of  
11 Extortion Wallet 1 sent approximately 125 BTC (of the initially deposited 297 BTC) from  
12 Extortion Wallet 1 to bc1qy43glppnqfrey5yt97xv7fyrn0a04npfwtef5 (Transfer Wallet 1).  
13 Prior to this transfer, Transfer Wallet 1 did not have a balance, nor did it receive any  
14 additional payments. Therefore, there was no co-mingling of any previous  
15 cryptocurrencies. Upon information and belief, Transfer Wallet 1 appeared to have been  
16 opened only for the purpose of receiving the transfer of Victim A's first payment.

17 22. On January 19, 2024, the unknown subjects who had access/ownership of  
18 Extortion Wallet 2 and Transfer Wallet 1 combined the BTC in Extortion Wallet 2 and  
19 Transfer Wallet 1 into the BTC address bc1qpy24cr5lukg33cpt3mx9xx3368mu4x2znswt4  
20 (Combined Wallet 1): approximately 125 BTC was sent from Transfer Wallet 1 and  
21 approximately 277 BTC was sent from Extortion Wallet 2. Prior to this transfer, Combined  
22 Wallet 1 did not have a balance, nor did it receive any additional payments. Therefore,  
23 there was no co-mingling of any previous cryptocurrencies. Upon information and belief,  
24 Combined Wallet 1 appeared to have been opened only for the purpose of receiving the  
25 transfer of Victim A's first and second payments.

26 23. The unknown subjects who had access/ownership of Combined Wallet 1  
27 then transferred all the cryptocurrencies in Combined Wallet 1 to the Avalanche Bridge

28 / / /

1 BTC address bc1q2f0tczgrukdxjrhdpft2fehzcprwrz549u90 (Avalanche Wallet 1) via two  
2 separate transactions by the unknown subjects.

3 24. On January 19, 2024, at 07:57 (UTC), Avalanche Wallet 1 received  
4 approximately 125 BTC from Combined Wallet 1.

5 25. On the same day, at 22:36 (UTC), Avalanche Wallet 1 received  
6 approximately 277 BTC from Combined Wallet 1.

7 26. As a result of these transactions, Avalanche Wallet 1 received a total amount  
8 of approximately 402 BTC.

9 27. On January 19, 2024, the FBI contacted Ava Labs, Inc., and requested it to  
10 voluntarily freeze the 402.41203181 BTC sent to Avalanche Wallet 1.

11 28. Ava Labs, Inc., agreed to voluntarily freeze the 277.56327614 BTC  
12 transferred from Extortion Wallet 2 to Avalanche Wallet 1 (which went to Combined  
13 Wallet 1 before Avalanche Wallet 1), until service of a civil forfeiture seizure warrant.  
14 However, Ava Labs, Inc., was not able to voluntarily freeze the 125 BTC transferred from  
15 Extortion Wallet 1 to Avalanche Wallet 1 (which went to Combined Wallet 1 before  
16 Avalanche Wallet 1) because the 125 BTC had already been transferred from Avalanche  
17 Wallet 1.

18 29. On January 19, 2024, an unknown actor transferred the 125 BTC from  
19 Extortion Wallet 1 that was now in Avalanche Wallet 1 through the Avalanche Bridge to  
20 the wallet 0x97937B9CF687379322E54A8DA35d5D2b243857E6 (BTCB Wallet). The  
21 approximate 125 BTC was valued at \$5,152,669.48 USD. Prior to this transfer, the BTCB  
22 Wallet did not have a balance.<sup>7</sup> A more detailed overview is found in Exhibit 3.

23 30. Between January 20, 2024, and January 21, 2024, cryptocurrency totaling in  
24 the amount of \$3,185,995.35 USD was sent to wallet  
25 0x1934d0D0CbF872Ff11cDb859deD6Dd6c5C7cbC1e (AVAX Wallet 1) from the BTCB  
26 Wallet. Prior to this transfer, AVAX Wallet 1 did not have a balance.

27 / / /

28 <sup>7</sup> Exhibit 3 is attached hereto and incorporated herein by reference as if fully set forth herein.

1 31. On January 21, 2024, cryptocurrency totaling in the amount of  
2 \$2,198,220.27 USD was sent to wallet  
3 0xA3631164d97ec60407DFe79b91b19C8eF83ADABe (AVAX Wallet 2) from AVAX  
4 Wallet 1. Prior to this transfer, AVAX Wallet 2 did not have a balance.

5 32. On January 22, 2024, at 23:06 UTC, cryptocurrency totaling in the amount  
6 of \$699,045.50 USD was sent to wallet 0x4C526de3f37Da24d2F21155222374633036fc619  
7 (AVAX Wallet 3) from AVAX Wallet 2. AVAX Wallet 3 had a previous balance of  
8 \$131.67 USD prior to this transaction.

9 33. On January 22, 2024, at 23:47 UTC, cryptocurrency totaling in the amount  
10 of \$699,059.36 USD was sent to wallet  
11 0xe7eCA93471d1105947038f6A927C1E03c43D67E9 (AVAX Wallet 4) from AVAX  
12 Wallet 3. AVAX Wallet 4 had a previous balance of \$10.10 USD prior to the transaction.

13 34. AVAX Wallet 3 had a remaining balance of \$138.78 USD. There were no  
14 other transactions after the transfer from AVAX Wallet 2 to AVAX Wallet 3 or before the  
15 transfer from AVAX Wallet 3 to AVAX Wallet 4.

16 35. Between January 22, 2024, and January 23, 2024, cryptocurrency totaling in  
17 the amount of \$690,755.00 USD was sent to wallet  
18 0x198a65D7AC0e785Ab99A2c671b41a534dBa72f44 (Stargate Wallet 1) from AVAX  
19 Wallet 4. Prior to this transfer, Stargate Wallet 1 did not have a balance.

20 36. AVAX Wallet 4 had a remaining balance of \$5,862.897 USD. There were no  
21 other transactions after the transfer from AVAX Wallet 3 to AVAX Wallet 4 or before the  
22 transfer from AVAX Wallet 4 to Stargate Wallet 1.

23 37. On January 23, 2024, cryptocurrency totaling in the amount of \$690,901.68  
24 (519845.30160479 USDT and 1135.51517101 XMR) was sent to Gate.io wallet  
25 0x6BC5C2661D75f0Ced80754D3C7bD651f1d60f736 (Gate.io Wallet) from Stargate  
26 Wallet 1. These cryptocurrencies were sent in three separate transactions:

27 0x1ac48e72bb2fd83ad60a0f3f0cea5036e3bdcf593a4a9be53c12c44a6197421,

28 / / /

1 0xbc0e435002aba822c6355e4f7571fe9b0d822e17e448c7262b2c9114ec325228, and  
2 0x3e989f0de45e39c89e86032acc59e33c5161d492dde3c7b09ea19408ba74c931.

3 38. Stargate Wallet 1 had a remaining balance of .021445 USDT and 10.0415  
4 MATIC.

5 39. On January 24, 2024, the FBI contacted Gate.io and requested it to  
6 voluntarily freeze the 519845.30160479 USDT and 1135.51517101 XMR sent to the  
7 Gate.io Wallet. On February 4, 2024, Gate.io confirmed the cryptocurrency were  
8 voluntarily frozen in the Gate.io Wallet 1. The Gate.io Wallet 1 contains 519803.53164  
9 USDT and 1135.508 XMR. Based on the amount of funds in the wallet, and the fact that  
10 Gate.io froze these funds, it is unlikely that there was a balance in Gate.io Wallet 1 prior to  
11 this transaction.

12 **FIRST CAUSE OF ACTION**

13 40. The United States realleges, readopts, and reincorporates all the allegations  
14 contained in paragraphs 1 through 39 as though fully set forth herein.

15 41. The defendant is any property, real or personal, which constitutes or is  
16 derived from proceeds traceable to violations of 18 U.S.C. § 1030(a)(2)(C), or a conspiracy  
17 to commit such offense, and is subject to forfeiture under 18 U.S.C. § 981(a)(1)(C).

18 **SECOND CAUSE OF ACTION**

19 42. The United States realleges, readopts, and reincorporates all the allegations  
20 contained in paragraphs 1 through 39 as though fully set forth herein.

21 43. The defendant is any property, real or personal, which constitutes or is  
22 derived from proceeds traceable to violations of 18 U.S.C. § 1030(a)(2)(C), a specified  
23 unlawful activity as defined in 18 U.S.C. § 1956(c)(7)(D), or a conspiracy to commit such  
24 offense, and is subject to forfeiture under 18 U.S.C. § 981(a)(1)(C).

25 **THIRD CAUSE OF ACTION**

26 44. The United States realleges, readopts, and reincorporates all the allegations  
27 contained in paragraphs 1 through 39 as though fully set forth herein.

28 / / /



1 45. The defendant is any property, real or personal, which constitutes or is  
2 derived from proceeds traceable to violations of 18 U.S.C. § 1030(a)(5)(A), or a conspiracy  
3 to commit such offense, and is subject to forfeiture under 18 U.S.C. § 981(a)(1)(C).

4 **FOURTH CAUSE OF ACTION**

5 46. The United States realleges, readopts, and reincorporates all the allegations  
6 contained in paragraphs 1 through 39 as though fully set forth herein.

7 47. The defendant is any property, real or personal, which constitutes or is  
8 derived from proceeds traceable to violations of 18 U.S.C. § 1030(a)(5)(A), a specified  
9 unlawful activity as defined in 18 U.S.C. § 1956(c)(7)(D), or a conspiracy to commit such  
10 offense, and is subject to forfeiture under 18 U.S.C. § 981(a)(1)(C).

11 **FIFTH CAUSE OF ACTION**

12 48. The United States realleges, readopts, and reincorporates all the allegations  
13 contained in paragraphs 1 through 39 as though fully set forth herein.

14 49. The defendant is any property, real or personal, which constitutes or is  
15 derived from proceeds traceable to violations of 18 U.S.C. § 1030(a)(7), or a conspiracy to  
16 commit such offense, and is subject to forfeiture under 18 U.S.C. § 981(a)(1)(C).

17 **SIXTH CAUSE OF ACTION**

18 50. The United States realleges, readopts, and reincorporates all the allegations  
19 contained in paragraphs 1 through 39 as though fully set forth herein.

20 51. The defendant is any property, real or personal, which constitutes or is  
21 derived from proceeds traceable to violations of 18 U.S.C. § 1030(a)(7), a specified  
22 unlawful activity as defined in 18 U.S.C. § 1956(c)(7)(D), or a conspiracy to commit such  
23 offense, and is subject to forfeiture under 18 U.S.C. § 981(a)(1)(C).

24 **SEVENTH CAUSE OF ACTION**

25 52. The United States realleges, readopts, and reincorporates all the allegations  
26 contained in paragraphs 1 through 39 as though fully set forth herein.

27 / / /

28 / / /

1 53. The defendant is any property, real or personal, involved in transactions or  
2 attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(B)(i), or any property  
3 traceable to such property, and is subject to forfeiture under 18 U.S.C. § 981(a)(1)(A).

4 **EIGHTH CAUSE OF ACTION**

5 54. The United States realleges, readopts, and reincorporates all the allegations  
6 contained in paragraphs 1 through 39 as though fully set forth herein.

7 55. The defendant is any property, real or personal, which constitutes or is  
8 derived from proceeds traceable to violations of 18 U.S.C. § 1956(a)(1)(B)(i), a specified  
9 unlawful activity as defined in 18 U.S.C. §§ 1956(c)(7)(A) and 1961(1)(B), or a conspiracy  
10 to commit such offense, and is subject to forfeiture under 18 U.S.C. § 981(a)(1)(C).

11 **NINTH CAUSE OF ACTION**

12 56. The United States realleges, readopts, and reincorporates all the allegations  
13 contained in paragraphs 1 through 39 as though fully set forth herein.

14 57. The defendant is any property, real or personal, involved in transactions or  
15 attempted transactions in violation of 18 U.S.C. § 1957, or any property traceable to such  
16 property, and is subject to forfeiture under 18 U.S.C. § 981(a)(1)(A).

17 **TENTH CAUSE OF ACTION**

18 58. The United States realleges, readopts, and reincorporates all the allegations  
19 contained in paragraphs 1 through 39 as though fully set forth herein.

20 59. The defendant is any property, real or personal, which constitutes or is  
21 derived from proceeds traceable to violations of 18 U.S.C. § 1957, a specified unlawful  
22 activity as defined in 18 U.S.C. §§ 1956(c)(7)(A) and 1961(1)(B), or a conspiracy to commit  
23 such offense, and is subject to forfeiture under 18 U.S.C. § 981(a)(1)(C).

24 **CONCLUSION**

25 60. Because of the foregoing, the defendant is subject to forfeiture and has  
26 become and is forfeited to the United States of America, plaintiff, under 18 U.S.C. §  
27 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C).

28 / / /

**PRAAYER FOR RELIEF**

WHEREFORE, the United States of America, Plaintiff, prays as follows:

1. Due process issue to enforce the forfeiture of the defendant;
2. Due notice be given to any interested party to appear and to show cause why the forfeiture should not be decreed;
3. The defendant be condemned and be forfeited to the United States; and
4. This Court enter other and further relief as it deems just and proper.

Dated: March 21, 2025.

Respectfully submitted,

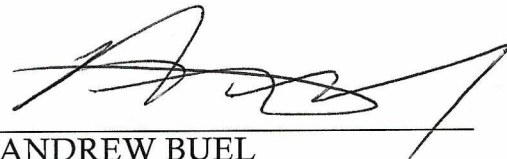
SUE FAHAMI  
Acting United States Attorney

/s/ Misty L. Dante  
MISTY L. DANTE  
Assistant United States Attorney

VERIFICATION

I, Andrew Buel, am a Special Agent with the Federal Bureau of Investigation. I have read the contents of the foregoing Complaint, and under 28 U.S.C. § 1746(2), I declare and verify under penalty of perjury that the foregoing is true and correct.

Executed this March 21, 2025.



ANDREW BUEL  
Special Agent  
Federal Bureau of Investigation

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**EXHIBIT 1****Glossary of Cryptocurrency-Related Terms**

1  
2  
3 1. Bitcoin<sup>8</sup> (or BTC) is a type of cryptocurrency. Payments or transfers of value  
4 made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by  
5 any single administrator or entity. As mentioned above, individuals can acquire bitcoin  
6 through exchanges (i.e., online companies which allow individuals to purchase or sell  
7 cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or  
8 directly from other people. Individuals can also acquire cryptocurrencies by mining. An  
9 individual can mine bitcoins by using his or her computing power to solve a complicated  
10 algorithm and verify and record payments on the blockchain. Individuals are rewarded for  
11 this task by receiving newly created units of a cryptocurrency. Individuals can send and  
12 receive cryptocurrencies online using many types of electronic devices, including laptop  
13 computers and smart phones. Even though the public addresses of those engaging in  
14 cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or  
15 entities behind the public addresses are not recorded on these public ledgers. If, however, an  
16 individual or entity is linked to a public address, it may be possible to determine what  
17 transactions were conducted by that individual or entity. Bitcoin transactions are therefore  
18 sometimes described as pseudonymous, meaning that they are partially anonymous. And  
19 while it's not completely anonymous, Bitcoin allows users to transfer bitcoin more  
20 anonymously than would be possible through traditional banking and financial systems.  
21  
22  
23

24 / / /

---

25  
26  
27 <sup>8</sup> Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted  
28 practice is to use Bitcoin (singular with an uppercase letter B) to label the protocol, software,  
and community, and bitcoin (with a lowercase letter b) to label units of the cryptocurrency.  
That practice is adopted here.

1           2.       Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer,  
2 network-based medium of value or exchange that may be used as a substitute for fiat  
3 currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies.  
4 Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist  
5 digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although  
6 not usually stored in any physical form, public and private keys (described below) used to  
7 transfer cryptocurrency from one person or place to another can be printed or written on a  
8 piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to  
9 person, through a cryptocurrency exchange, or through other intermediaries. Generally,  
10 cryptocurrency is not issued by any government, bank, or company; it is instead generated  
11 and controlled through computer software operating on a decentralized peer-to-peer  
12 network. Most cryptocurrencies have a blockchain, which is a distributed public ledger, run  
13 by the decentralized network, containing an immutable and historical record of every  
14 transaction.<sup>9</sup> Cryptocurrency is not illegal in the United States.

15           3.       Cryptocurrency is stored in a virtual account called a wallet. Wallets are  
16 software programs that interface with blockchains and generate and/or store public and  
17 private keys used to send and receive cryptocurrency. A public key or address is a unique  
18 number associated with cryptocurrency that is used to display it, and a private key is akin to  
19 a password that allows a user the ability to access and transfer value associated with the  
20 public address or key. To conduct transactions on a blockchain, an individual must use the  
21 public key (or public address) and the private key (or private address). A public key is  
22 represented as a case-sensitive string of letters and numbers, 25–26 characters long. Each  
23 public key is controlled and/or accessed using a unique corresponding private key—the  
24 cryptographic equivalent of a password or PIN—needed to access the address. Only the  
25 holder of a public key’s private key can authorize any transfers of cryptocurrency from that  
26 public key to another cryptocurrency key.

---

27  
28 <sup>9</sup> Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

1 4. Although cryptocurrencies such as bitcoin have legitimate uses, individuals  
2 and organizations use cryptocurrency for criminal purposes such as money laundering and  
3 is an often used means of payment for illegal goods and services on hidden service websites  
4 operating on the Tor network. By maintaining multiple wallets, those who use  
5 cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track  
6 purchases within the dark web marketplaces. As of January 31, 2024, one bitcoin is worth  
7 approximately \$42,664.21 USD. The value of bitcoin is generally much more volatile than  
8 that of fiat currencies.

9 5. Exchangers and users of cryptocurrencies store and transact their  
10 cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms,  
11 including on a tangible, external device (hardware wallet), downloaded on a PC or laptop  
12 (desktop wallet), with an Internet-based cloud storage provider (online wallet), as a mobile  
13 application on a smartphone or tablet (mobile wallet), printed public and private keys (paper  
14 wallet), and as an online account associated with a cryptocurrency exchange. Because these  
15 desktop, mobile, and online wallets are electronic in nature, they are located on mobile  
16 devices (e.g., smart phones or tablets) or at websites that users can access via a computer,  
17 smart phone, or any device that can search the Internet. Moreover, hardware wallets are  
18 located on some type of external or removable media device, such as a USB thumb drive or  
19 other commercially available device designed to store cryptocurrency (e.g., Trezor,  
20 Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code<sup>10</sup>  
21 with the public and private key embedded in the code. Paper wallet keys are not stored  
22 digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or  
23 CDs, and accessed through a recovery seed (random words strung together in a phrase) or a  
24 complex password. Additional security safeguards for cryptocurrency wallets can include  
25 two-factor authorization (such as a password and a phrase). Individuals possessing  
26 cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become  
27

---

28 <sup>10</sup> A QR code is a matrix barcode that is a machine-readable optical label.

1 further secured in the event their assets become potentially vulnerable to seizure and/or  
2 unauthorized transfer.

3         6. Bitcoin exchangers and exchanges are individuals or companies that  
4 exchange bitcoin for other currencies, including United States currency. According to  
5 Department of Treasury, Financial Crimes Enforcement Network (FinCEN) Guidance  
6 issued on March 18, 2013, virtual currency administrators and exchangers, including an  
7 individual exchanger operating as a business, are considered money services businesses.<sup>11</sup>  
8 Such exchanges and exchangers are required to register with FinCEN and have proper state  
9 licenses (if required under applicable state law). Registered money transmitters are required  
10 by law to follow Bank Secrecy Act anti-money laundering (AML) regulations, Know Your  
11 Customer (KYC) protocols, and other verification procedures like those employed by  
12 traditional financial institutions. For example, to open and maintain accounts on their  
13 exchange, FinCEN-registered cryptocurrency exchangers often require customers to provide  
14 their name, address, phone number, and the full bank account and routing numbers that the  
15 customer links to an exchange account. As a result, there is significant market demand for  
16 illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and  
17 often also advertise their ability to offer customers stealth and anonymity. These illicit  
18 exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in  
19 person or by shipping cash through the mail. Due to the illicit nature of these transactions  
20 and their customers' desire for anonymity, such exchangers are frequently able to charge a  
21 higher exchange fee, often as high as 9–10%; in contrast to registered and Bank Secrecy Act  
22 compliant exchangers, who charge fees as low as 1–2%.

23         7. Some companies offer cryptocurrency wallet services which allow users to  
24 download a digital wallet application onto their smart phone or other digital device. A user  
25 typically accesses the wallet application by inputting a user-generated PIN or password.  
26

---

27 <sup>11</sup> See “Application of FinCEN’s Regulations to Person Administering, Exchanging, or  
28 Using Virtual Currencies,” *available at* <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>.



1 Users can store, receive, and transfer cryptocurrencies via the application; however, many of  
2 these companies do not store or otherwise have access to their users' cryptocurrencies or the  
3 private keys that are necessary to access users' wallet applications. Rather, the private keys  
4 are stored on the device on which the wallet application is installed (or any digital or  
5 physical backup private key that the user creates). As a result, these companies generally  
6 cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless,  
7 law enforcement could seize cryptocurrency from the user's wallet directly, such as by  
8 accessing the user's smart phone or other digital device, accessing the wallet application,  
9 and transferring the cryptocurrency therein to a law enforcement-controlled wallet.

10 Alternatively, where law enforcement has obtained the recovery seed for a wallet (see  
11 above), law enforcement may be able to use the recovery seed phrase to recover or  
12 reconstitute the wallet on a different digital device and subsequently transfer  
13 cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

14 8. The terms communications, records, documents, programs, or materials  
15 include all information recorded in any form, visual or aural, and by any means, whether in  
16 handmade form (including, but not limited to, writings, drawings, paintings), photographic  
17 form (including, but not limited to, pictures or videos), or electrical, electronic, or magnetic  
18 form, as well as digital data files. These terms also include any applications, i.e., software  
19 programs. These terms expressly include, among other things, emails, instant messages, chat  
20 logs, correspondence attached to emails (or drafts), calendar entries, buddy lists. etc.

21 9. Internet Protocol address, or IP address, refers to a numeric address used by a  
22 computer to access the Internet. IP addresses can be dynamic, meaning that the Internet  
23 Service Provider (ISP) assigns a unique number to a user's device at set intervals (called  
24 lease periods) when the device accesses the Internet. IP addresses might also be static, that  
25 is, an ISP assigns a user's device a particular IP address, which is used each time the  
26 computer accesses the Internet.

27 10. In general terms, a server is a physical computer that processes data for one or  
28 more users over a local network or the Internet. An example is a physical computer

1 operated by a popular email service like Google or Yahoo, which stores and receives emails  
2 for many users who access the server through the Internet. In some cases, a host/operator of  
3 a physical server allows others to remotely (e.g., via the Internet) rent or lease part of the  
4 server to use as their own, smaller server. These smaller, leasable servers are often called  
5 virtual private servers (VPS) because virtual-machine technology is what allows the server  
6 operator to run multiple private servers on the same physical server.

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

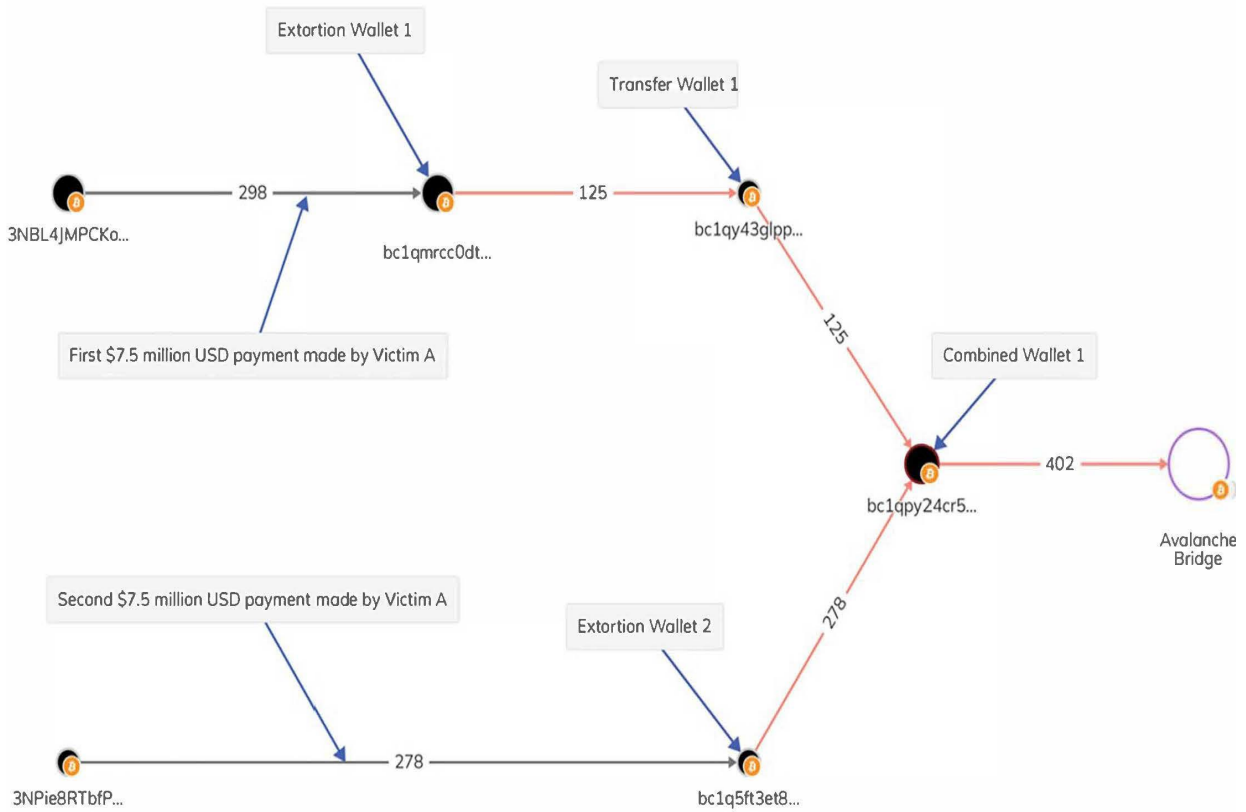
27

28

**EXHIBIT 2**

Overview of Payment and Transfer of 402.41203181 BTC

Date	Source	Destination	Amount
9/11/2023	Victim A	bc1qmrc0dtdn3c785phrncf5wtz98q9qy8ndpd5ev	297.6792
9/12/2023	bc1qmrc0dtdn3c785phrncf5wtz98q9qy8ndpd5ev	bc1qy43glppnqfrey5yt97xv7fyrn0a04npfwtef5	124.849
10/12/2023	Victim A	bc1q5ft3et8h0qp4ppk6hjjhfxmmy32egzgvrgtwsn	277.5636
1/19/2024	bc1qy43glppnqfrey5yt97xv7fyrn0a04npfwtef5	bc1qpy24cr5lulg33cpt3mx9xx3368mu4x2znnswt4	124.849
1/19/2024	bc1q5ft3et8h0qp4ppk6hjjhfxmmy32egzgvrgtwsn	bc1qpy24cr5lulg33cpt3mx9xx3368mu4x2znnswt4	277.5634
1/19/2024	bc1qpy24cr5lulg33cpt3mx9xx3368mu4x2znnswt4	bc1q2f0tczgrukdxjrhadpft2fehzipcrwrz549u90	124.8488
1/19/2024	bc1qpy24cr5lulg33cpt3mx9xx3368mu4x2znnswt4	bc1q2f0tczgrukdxjrhadpft2fehzipcrwrz549u90	277.5633



**EXHIBIT 3**

Date	Source	Destination	Amount
1/19/2024	Avalanche Bridge	BTBC Wallet 1	\$5,152,669.48
1/20-21/2024	BTBC Wallet 1	AVAX Wallet 1	\$3,185,995.35
1/22/2024	AVAX Wallet 1	AVAX Wallet 2	\$2,198,220.27
1/22/2024	AVAX Wallet 2	AVAX Wallet 3	\$699,045.50
1/22/2024	AVAX Wallet 3	AVAX Wallet 4	\$699,059.36
1/22/2024	AVAX Wallet 4	Stargate Wallet 1	\$690,755.00
1/23/2024	Stargate Wallet 1	Gate.io Wallet	\$690,901.68 (519845.30160479 USDT and 1135.51517101 XMR)

