

Bitcoin Flows from Sanctioned Sources

Axel Flodmark*, Rasmus Samuelson*, David Hasselquist*, Martin Arlitt†, Niklas Carlsson*

*Linköping University, Sweden †Corelight, Canada

axefl087@student.liu.se, rassa328@student.liu.se, david.hasselquist@liu.se, martin.arlitt@gmail.com, niklas.carlsson@liu.se

Abstract—Cryptocurrencies’ pseudonymity property poses regulatory challenges and has attracted illicit actors that try to avoid oversight. To counter this, the U.S. Treasury’s Office of Foreign Assets Control (OFAC) sanctions individuals and entities using Bitcoin for cybercrime, terrorism financing, and other illicit activities. However, the effectiveness of these measures remains uncertain. This study analyzes over 13 million Bitcoin transactions linked to sanctioned entities, tracing fund flows and exchange interactions. We find that $\sim 175,000$ BTC was moved before sanctions took effect, with only 50 BTC remaining post-sanction, indicating preemptive fund displacement. Cybercrime-linked addresses accounted for the largest transfers—sometimes exceeding \$1 billion—while sanctioned entities favored large, direct transactions to exchanges. Despite activity dropping immediately after sanctions took effect, some entities continued transacting for up to 1,500 days, exposing enforcement gaps. Our findings highlight key challenges in sanction enforcement, including delayed restrictions, exchange compliance gaps, and strategic fund movements. These insights inform policymakers and regulators seeking to strengthen cryptocurrency financial controls.

Index Terms—Bitcoin, Flow Analysis, Sanctioned Sources

I. INTRODUCTION

The rise of Bitcoin and other cryptocurrencies has reshaped global finance, offering decentralized and borderless transactions [1], [2]. However, these features also make cryptocurrencies attractive to illicit actors seeking to evade financial oversight. Bitcoin’s pseudonymity has enabled its use in a wide range of illicit activities, including money laundering [3], [4], drug and human trafficking [5]–[7], ransomware payments [8], and cybercrime financing [9], [10].

Recognizing these risks, regulatory bodies such as the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) have imposed sanctions on some individuals and entities leveraging cryptocurrencies for cybercrime, terrorism financing, and other illicit activities. Yet, despite the transparency of blockchain transactions, effectively enforcing sanctions and disrupting financial flows associated with sanctioned actors remains a major challenge.

While prior research [2], [11]–[18] has explored illicit Bitcoin transactions in contexts such as darknet markets and scams, systematic analysis of cryptocurrency usage by sanctioned entities has been limited. In this study, we address this gap by investigating how sanctioned actors move funds, interact with exchanges, and attempt to circumvent restrictions.

Our key contributions are as follows:

- **Comprehensive Dataset:** Starting from the 386 sanctioned addresses on the Specially Designated Nationals (SDN) list [19], which together transferred $\sim 175,000$ BTC, we construct one of the largest datasets on Bitcoin

transactions involving sanctioned addresses, comprising over 13 million transactions and 18.6 million unique addresses. This dataset integrates transaction histories, balance data, and entity labels from multiple sources, enabling a detailed analysis of sanctioned entities’ financial activities and fund flows.

- **Transaction Flow and Fund Dispersion Analysis:** We analyze how sanctioned addresses move funds, categorizing transactions by input-output patterns and receiver type. Our findings show a preference for one-to-one and many-to-many transactions, with cybercrime-linked addresses accounting for the largest fund transfers—sometimes exceeding \$1 billion. Notably, 51.3% of funds sent to exchanges come from one-to-one transactions, despite these making up only 11.2% of transactions, indicating a preference for large, direct transfers. We also uncover varying compliance levels across exchanges.
- **Temporal Analysis of Sanctioned Entities’ Activity:** We analyze Bitcoin usage before and after sanctions, revealing that most entities were highly active for 2–3 years pre-sanction but saw sharp declines immediately after. Some, however, continued transacting for up to 1,500 days post-sanction, exposing enforcement gaps. Notably, sanctioned addresses moved $\sim 175,000$ BTC before restrictions took effect, retaining only 50 BTC post-sanction. While sanctions disrupt activity, they do not fully prevent illicit transactions, underscoring the need for strong and continuing enforcement.

By leveraging blockchain transparency, our work provides a novel perspective on the effectiveness of sanctions in disrupting illicit financial activity. Our findings highlight key enforcement challenges, including delayed sanction enforcement, exchange compliance gaps, and strategic fund movements by sanctioned entities. These insights offer practical recommendations for policymakers, regulators, and financial crime investigators seeking to strengthen cryptocurrency-related financial controls and enhance the sanction efficacy in digital finance.

Outline: After describing our methodology and dataset (Section 2), we present a high-level analysis (Section 3) and temporal analysis (Section 4) of the bitcoin flow associated with the sanctioned addresses. Finally, we present related work (Section 5) and conclusions (Section 6).

II. METHODOLOGY AND DATASET

We first describe our data collection and analysis of Bitcoin transactions linked to sanctioned addresses, including data sources and tracking methodology.

TABLE I: Relevant sanctions programs and their respective descriptions.

Program code	Short name	Description
CYBER2	Cybercrime	Designations related to significant cyber activities
DPRK3	North Korea (1)	Designations of North Korean entities per specified regulations
DPRK4	North Korea (2)	Additional sanctions with respect to North Korea
ELECTION-EO13848	U.S election	Interference in U.S. elections
IFSR	Iran financial	Iranian Financial Sanctions Regulations
IRGC	IRGC (Iran)	Designations targeting the Islamic Revolutionary Guard Corps
ILLICIT-DRUGS-EO14059	Illicit drugs	Illicit drug activities
NPWMD	Weapons proliferation	Designations on proliferation of weapons of mass destruction
RUSSIA-EO14024	Russia	Russian harmful foreign activities
SDGT	Terrorism	Specially Designated Global Terrorists under executive orders
SDNTK	Narcotics kingpins	Specially Designated Narcotics Trafficking Kingpins

A. Data Sources

SDN List: The U.S. Office of Foreign Assets Control (OFAC) maintains the Specially Designated Nationals (SDN) and Blocked Persons list, which identifies individuals and entities involved in activities threatening U.S. foreign policy or national security [19]. The list includes various sanctions programs, each based on specific legal frameworks. For our analysis, we focused on sanctions tied to bitcoin addresses, as detailed in Table I.

Blockchain.com: We used the Blockchain Data API from a platform that serves as both a blockchain explorer and exchange for various cryptocurrencies [20] to retrieve the transaction history of the studied bitcoin addresses and to follow the money flows associated with the sanctioned addresses (Section II-B).

OXT.me: We used OXT.me, a now defunct blockchain analysis platform previously developed and run by Samurai Wallet, to provide entity labels and types for both the studied and discovered addresses. Employing a variety of heuristics and human-provided sources, they mapped bitcoin addresses to the entities presumably controlling them, capturing relationships between an address and an entity [21], as well as the entity name and type. While OXT.me was shut down on April 24th, 2024, following the arrests of the site owners [22], we were able to collect mappings for the sanctioned addresses as well as the addresses responsible for most of the funds that we observed transferred (as we started with the addresses with most funds transferred and were able to collect data for 2.8 million out of 18.6 million addresses before the platform was taken offline).

Price Data: We used the daily opening price of Bitcoins (Yahoo Finance) from 2014/9/14 to 2024/3/6, to quantify the size of each transaction. Any transactions that took place outside this time window were dropped from our analysis.

B. High-Level Dataset Construction

The dataset was created in iterations, starting with sanctioned addresses from the SDN list. First, the transaction history of these addresses was retrieved, and outgoing transactions exceeding \$5,000 were followed. This threshold was selected to prioritize larger transactions and limit the total number of addresses to collect. With this choice, the kept addresses are responsible for roughly 90% of the money

flow in the first step. To limit the growth even further, we added a spending limit on the addresses in each step, not allowing them to spend more bitcoins than initially received from our SDN addresses. Entity labels were then collected from OXT.me. Furthermore, using this information, endpoints such as exchanges, dark markets, and known mixing services were removed (before each next step) to focus on illicit flows. We repeated this process for five steps.

Starting from the first iteration, we analyzed 385 sanctioned addresses, growing to 214,048 addresses by the fifth iteration. More specifically, each step contained (1) 385, (2) 13,420, (3) 33,018, (4) 93,107, and (5) 214,048 addresses. In addition to collecting the full transaction and label data for these addresses, we collected OXT.me labels for 2.8 million addresses (1.8 million of these had labels) and the balance information, transaction count, and total sent/received amounts for a total of 18.6 million addresses (including the addresses of interest performed transactions with). In summary, the data extracted included:

- Full transaction history for the 385 SDN-listed addresses.
- Full transaction data for the 353,978 non-endpoint addresses (excluding exchanges and dark markets) receiving more than \$5,000, each tracked further.
- Balance information, transaction count, and total sent/received amounts for 18.6 million unique addresses that the above addresses transferred funds to.
- Entity labels for 1.8 million out of 2.8 million queried high-transaction addresses, including the addresses that we tracked.

C. Tracking and Labeling Flows

To track flows of funds, transactions were categorized based on input-output relationships. While it is trivial to track funds in the cases of one-to-one, one-to-many, and many-to-one transactions, this task is less trivial for the many-to-many case, which may also indicate a mixing service being used. For many-to-many transactions, we made a proportional distribution assumption regarding the inputs across outputs based on value contributions. Consider a 3-to-2 transaction with three inputs and two outputs, totaling 6 bitcoin. To analyze the flow of funds, we allocate each input's contribution to the outputs based on their share of the total output value. For example, if input 2 contributes 2 bitcoins, then the distribution to output 1

TABLE II: Transaction summary of the sanctioned programs and number of addresses.

Program	Address	Transactions		BTC		
		Tx in	Tx out	Vol. in	Vol. out	Balance
Cybercrime	280	$0.99 \cdot 10^5$	$5.37 \cdot 10^4$	$1.79 \cdot 10^5$	$1.79 \cdot 10^5$	$1.44 \cdot 10^0$
Illicit drugs	60	$4.66 \cdot 10^3$	$2.17 \cdot 10^3$	$2.01 \cdot 10^3$	$2.01 \cdot 10^3$	$6.25 \cdot 10^{-1}$
North Korea (1)	39	$1.28 \cdot 10^3$	$0.98 \cdot 10^3$	$1.76 \cdot 10^4$	$1.76 \cdot 10^4$	$1.80 \cdot 10^{-3}$
U.S election	30	$3.17 \cdot 10^4$	$1.45 \cdot 10^4$	$1.02 \cdot 10^3$	$1.02 \cdot 10^3$	$1.16 \cdot 10^{-1}$
Narcotics kingpins	11	$2.77 \cdot 10^2$	$1.19 \cdot 10^2$	$1.76 \cdot 10^3$	$1.71 \cdot 10^3$	$4.89 \cdot 10^1$
Russia	7	$3.11 \cdot 10^2$	$2.44 \cdot 10^2$	$0.96 \cdot 10^3$	$0.96 \cdot 10^3$	0
Iran financial	6	$1.42 \cdot 10^2$	$4.10 \cdot 10^1$	$5.15 \cdot 10^0$	$5.15 \cdot 10^0$	$6.66 \cdot 10^{-6}$
IRGC (Iran)	6	$1.42 \cdot 10^2$	$4.10 \cdot 10^1$	$5.15 \cdot 10^0$	$5.15 \cdot 10^0$	$6.66 \cdot 10^{-6}$
Weapons prolif.	3	$6.60 \cdot 10^1$	$3.90 \cdot 10^1$	$1.81 \cdot 10^0$	$1.81 \cdot 10^0$	0
North Korea (2)	2	$3.20 \cdot 10^1$	$3.00 \cdot 10^1$	$1.10 \cdot 10^2$	$1.10 \cdot 10^2$	0
Terrorism	2	$1.13 \cdot 10^4$	$7.14 \cdot 10^3$	$1.02 \cdot 10^4$	$1.02 \cdot 10^4$	$2.74 \cdot 10^{-3}$

(with 2 bitcoins) is $\frac{2}{6} \times 2 = \frac{2}{3}$ bitcoins, and to output 2 (with 4 bitcoins), it is $\frac{4}{6} \times 2 = \frac{4}{3}$ bitcoins.

For each address receiving funds from an SDN-listed source, sanction program information was propagated to subsequent addresses across five steps. If an address received funds from multiple sanctioned programs, it was assigned all relevant labels. Again, as noted above, addresses identified as exchanges and dark market endpoints were filtered out to prevent artificial linkages.

The above methodology allows us to go from raw transaction data from Blockchain.com to filtered and labeled transaction data with dollar value calculations and individual labeled contribution breakdowns. This allows identification and analysis of Bitcoin transactions linked to sanctioned entities and ensures a structured approach to tracking illicit financial flows.

D. Limitations

While our methodology provides a structured approach to tracking Bitcoin transactions linked to sanctioned addresses, it has several limitations. First, the accuracy and completeness of entity labels from OXT.me are constrained. This platform mapped Bitcoin addresses to entities using heuristics and external sources. Its abrupt shutdown in April 2024 limited our data collection to 2.8 million labeled addresses, only a subset of the 18.6 million in our dataset. However, our prioritized query strategy ensured coverage of the most relevant addresses.

Second, tracking exact fund flows remains challenging due to Bitcoin’s UTXO model. While one-to-one, one-to-many, and many-to-one transactions are straightforward to trace, many-to-many transactions require proportional allocation assumptions, which may not fully reflect real-world intent, especially when CoinJoin or other mixing techniques are involved. To mitigate this, we focused on high-value transactions and filtered known mixing services.

To improve reliability, we focus on first-hop transactions and use relative measures to minimize noise and speculative tracing. By analyzing transactions closest to sanctioned addresses, we capture key fund distribution patterns while avoiding deeper, uncertain laundering paths. Although absolute figures may be affected by data constraints, our approach ensures robust relative comparisons, offering meaningful insights into sanctioned actors’ cryptocurrency activity.

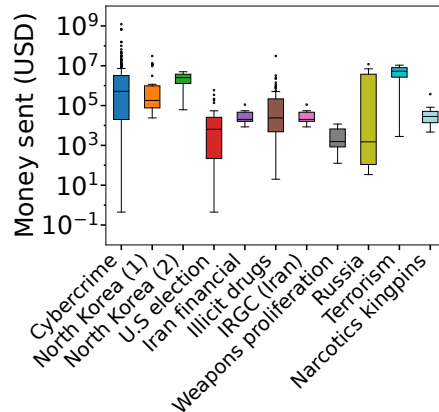


Fig. 1: Sent USD from SDN addresses per sanction program.

III. HIGH-LEVEL BITCOIN USAGE OF SANCTIONED ADDRESSES

Table II presents an overview of the aggregate transactions and money flows in/out of the Bitcoin addresses of the sanctioned programs, sorted from the program with the most to the least sanctioned Bitcoin addresses. We note that all programs see more transactions sent to them (Tx in) than out (Tx out), with Cybercrime being the program with most sanctioned addresses, followed by Illicit drugs, North Korea (1), and U.S. election interference. Looking at the number of transactions, the top-3 are Cybercrime, U.S. election interference, and Terrorism. Finally, looking at the amount of transferred Bitcoin funds, the top-3 are Cybercrime, North Korea (1), and Terrorism. Being at the top of all three of these lists, regardless of dimension, the Cybercrime program clearly stands out.

The Cybercrime program also stands out when looking at the total funds sent from each address associated with the different programs, where this category is responsible for (by far) the largest number of outliers, responsible for (very) large amounts of money being sent, including some reaching upwards of 1 billion USD. This is illustrated in Fig. 1, which shows a whisker plot of the total amount (in USD) sent from the SDN addresses of each sanctions program.

A. Where Does the Money Go?

To glean some initial insights into where the funds are transferred, we tracked the flows over several steps. Fig. 2 illustrates

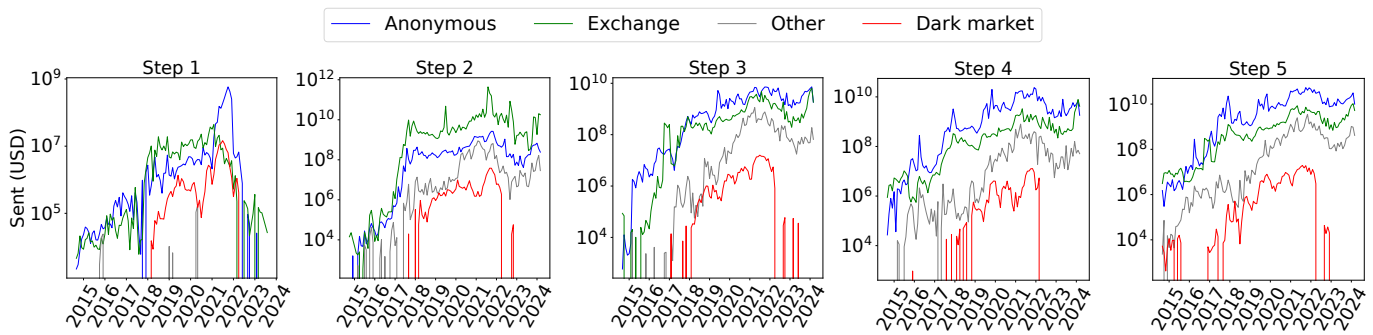


Fig. 2: Amount of USD sent to each entity from each step.

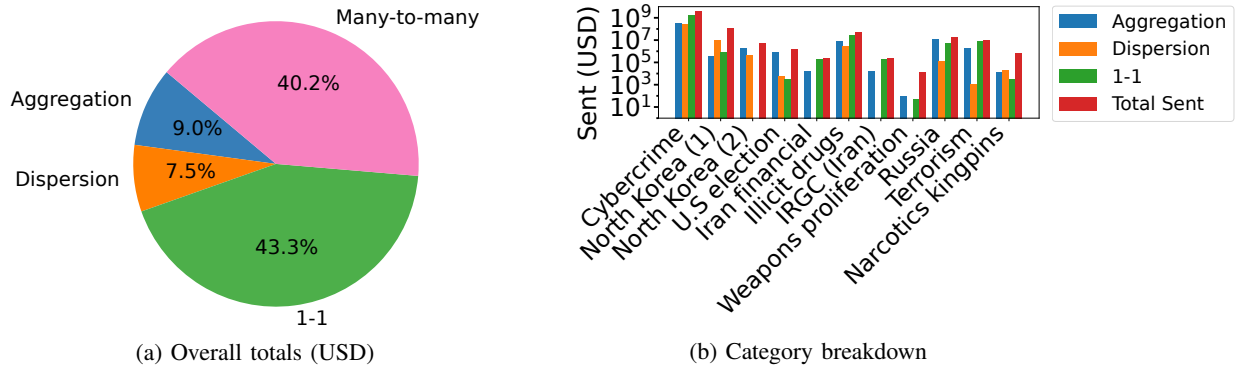


Fig. 3: Transaction type shares of the total sent amount in USD.

the total funds (in USD) sent from the SDN programs to different relays or endpoint categories, as observed from step one (directly from SDN addresses) to step five. To account for significant differences in the amount of funds tracked in each step, different scales were used in each step. Here, we also exclude unlabeled flows and group labels other than “Anonymous”, “Dark Market”, and “Exchange” as “Other”.

Our analysis reveals Darknet market activity primarily in the early steps between 2018 and 2022, with additional activity in 2015–2016 in steps four and five. Transactions to exchanges and anonymous addresses dominate in volume, with funds moving rapidly toward exchanges, particularly in steps one and two. Bitcoin price spikes in 2017 and 2020–2021, where values surged tenfold, are reflected in transaction trends (Fig. 2). Step one shows low volume during the 2017 peak but increased activity as prices declined in 2018, a trend that persisted until 2022 before dropping sharply. In contrast, step five exhibits steady transaction activity over time, except for fluctuations in the Darknet market.

B. How Does the Money Disperse?

We next look at whether there are major differences in how the money is transferred away from the sanctioned accounts; specifically, whether the funds are aggregated (many-to-one transactions), dispersed (one-to-many transactions), sent one-to-one, or if the funds are moved using many-to-many transactions. Fig. 3 summarizes these results. Here, Fig. 3(a) shows

the overall values and Fig. 3(b) provides the per-category breakdowns.

Looking at the total, it is apparent that one-to-one and many-to-many are the two most commonly used transaction types, responsible for sending the most money. Looking closer at the transaction numbers, we have found that many-to-many is used in more transactions (44.1% many-to-many vs. 30.2% one-to-one), but one-to-one has sent more money (40.2% many-to-many vs. 43.2% one-to-one), although it is very close.

Finally, and perhaps most interestingly, looking closer at the money sent to exchanges, we have found that one-to-one transactions are responsible for 51.3% of the total money sent to exchanges, despite being responsible for only 11.2% of the transactions to exchanges. This is in stark contrast to many-to-many transactions, which are responsible for 71.6% of the transactions but almost none of the funds sent to exchanges (<0.1%). We believe that most of this is due to these accounts typically performing larger transactions using a single account at a time. For example, we observe that the small fraction of dispersion transactions (2.3%) transferring funds to exchanges are responsible for transferring more funds to exchanges (27.0% vs. 21.7%) than the much larger fraction of aggregation transactions involving exchanges (14.9%).

Per-Category Analysis: Fig. 3 shows the sent amounts in USD for different SDN categories. The bars represent the transaction type, distinguishing between aggregation, dispersion, one-to-one, and all transactions. We note that SDN

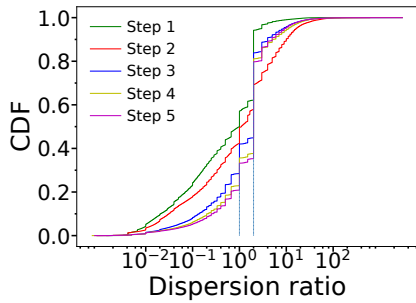


Fig. 4: CDF of dispersion ratio of all sent transactions across the five steps.

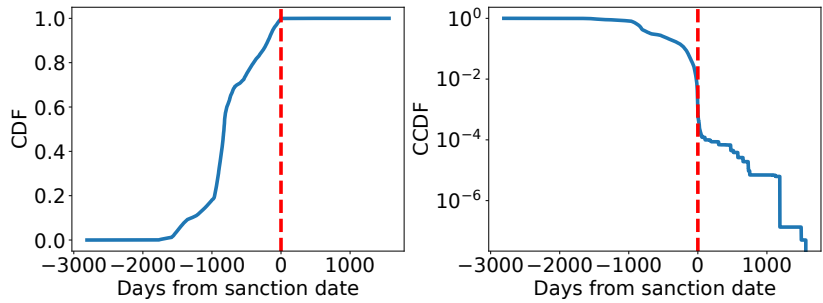


Fig. 5: CDF and CCDF over the transaction count for the SDN addresses relative to their sanction date.

addresses sanctioned for Cybercrime have sent the most money overall and across all transaction types. Most programs use all transaction types, and nine of eleven have sent more via aggregation than dispersion.

Step-Based Dispersion Analysis: We have also found that the dispersion is lowest in the first step of our multi-step analysis, suggesting that the original SDN accounts may tend to direct their funds more purposefully (either from more inputs or to a smaller set of outputs) than the accounts that later are in contact with the transferred funds. To see this, we refer to Fig. 4, which shows the CDFs of dispersion ratios for all sent transactions from step one through five. Here, the dispersion ratio is calculated by dividing the total amount of output addresses in a transaction by the total amount of input addresses. On the left side of 1, the transactions have more inputs than outputs, and on the right side they have more outputs than inputs. We can see that most of the data, for all of the steps, lies in the ratio range of 0.1-10. The dotted lines are placed for the ratios 1 and 2, and are included to highlight the most prominent straight vertical spikes. These spikes indicate the most common ratios, out of which 2 is the most common, since the spikes are the longest for that value for all steps. It is apparent that, initially, when the CDFs get closer towards 2 on the x-axis, they do so in reverse step order. Essentially, this means that the step 5-CDF reaches the vertical spike of ratio 2 first, the step 4-CDF second, and so on.

From looking at the places where the CDF's first intersect with the line representing ratio 1, we can deduce that around 50% of transactions in the first step have more inputs than outputs, around 40% for step 2, around 30% for step 3, around 25% for step 4, and lastly around 22% for step 5. Furthermore, for transactions with ratios between and including 1 and 2, we observe that they account for around 45% for step 1, around 30% of step 2 transactions, around 55% of step 3 transactions, around 55% of step 4 transactions, and around 60% of step 5 transactions. In addition, we observe that only around 10% of transactions, for all steps respectively, have ratios over 10.

IV. TIMING-BASED ANALYSIS

Next, we look at the relative timing of the activity associated with the sanctioned addresses and the date each sanction took place. Here, we use the official dates listed in the SDN list.

A. When Were They Sanctioned and Most Active?

Fig. 5 shows the CDF and CCDF of the transactions that took place at different days relative to the sanction date. Several observations are possible. For example, as perhaps expected, almost all activity took place before the sanction dates (e.g., CCDF drops to around 10^{-4} near the sanctioned date). This shows that the sanctions do have significant effects on the listed addresses, suggesting that imposing sanctions may be an effective means of disrupting the financial operations of sanctioned entities (or force them to move to other addresses).

Second, we observe that some post-sanction activity persists for up to 1,500 days, with a slight shift in transaction patterns. Before sanctions, 21% of transactions were incoming and 79% outgoing, whereas post-sanction, incoming transactions dropped to 15% while outgoing transactions rose to 85%.

Third, sanctioned addresses exhibited high activity for years before restrictions, with transactions occurring up to 3,000 days prior and peaking 2-3 years before sanctions, as seen by the greatest slope in the CDF in Fig. 5. This indicates that these entities were operational for a significant duration before restrictions were applied. Activity remained high until the sanction date, suggesting earlier enforcement could have been beneficial.

B. When Were the Most Funds Transferred?

We also studied the relative funds sent, received, and the balance of the different addresses. Fig. 6 shows the CDF of the first two metrics and Fig. 7 shows the combined balance of the accounts as a function of the time until being sanctioned. We note that the funds moved in are typically transferred elsewhere quickly (e.g., closely matching lines in Fig. 6 and the—in relative terms—lower balance amounts). We also note that the peak balance for the addresses occurred roughly 1,000 days before the sanction date, with the most extreme spike being attributed to a single address. In total, we note that roughly 175,000 bitcoins were received by and then sent from these addresses before their respective sanction date. Of these, only approximately 50 bitcoins remained at these sanctioned addresses (well after the sanctioned dates), suggesting that most funds were retrieved by somebody (e.g., the illicit actors or seized).

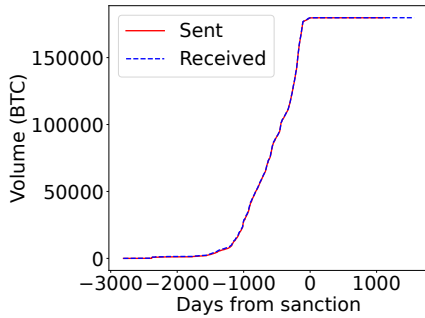


Fig. 6: Sent/received BTC for the SDN addresses.

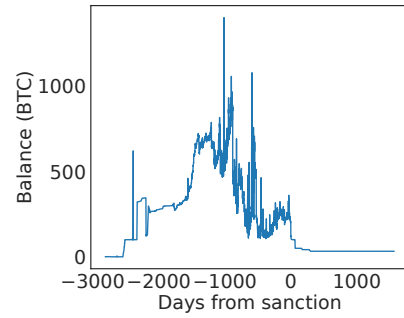


Fig. 7: The cumulative balance for all SDN addresses with regards to their sanction date.

C. Are There Category-Based Differences?

Finally, we have investigated whether there are differences in how long it took before addresses associated with different sanction programs were sanctioned. Fig. 8 shows the average duration for which an address remains active before being sanctioned across various programs. Here, an address is considered active from the time of its first transaction. We note that programs related to U.S. elections, illicit drugs, terrorism, and narcotic kingpins all have average active periods exceeding 1,100 days prior to sanctioning. Most other programs show an average active period of around 600 days, except for weapon proliferation, which is slightly under 500 days. This data indicates that, generally, addresses operate for one to three years before sanctions are enforced.

V. RELATED WORK

Bitcoin research has extensively examined deanonymization, clustering heuristics, and privacy vulnerabilities, revealing how its public ledger and user behaviors compromise privacy, particularly in illicit activities [1], [23], [24]. Beyond anonymity concerns, studies have analyzed Bitcoin’s role in crime [2], [11]–[18]. Rosenquist et al. [17] found that ransomware, darknet markets, and tumblers handle the largest illicit funds, while sextortion and blackmail scams receive smaller amounts despite frequent reports. Their findings highlight the need for improved real-time monitoring and regulation, as most illicit transactions occur before reports are filed.

To further obscure illicit transactions, Bitcoin users often rely on money laundering techniques such as transaction mixing (tumbling) to break the link between senders and recipients [4]. Some works explore the limitations of existing tumbling services and the development of new cryptographic protocols to improve transaction anonymity, ranging from centralized mixing solutions [25], [26] to decentralized coin-mixing protocols [27].

Ransomware is another major threat, where victims must pay Bitcoin ransoms to regain access to encrypted files. Some have analyzed long-term trends, ransom payment flows, and fund laundering [28]–[32]. Others have studied Bitcoin sextortion scams, where criminals extort victims by threatening to expose sensitive information [9], [10], and its role in darknet markets [5], [7].

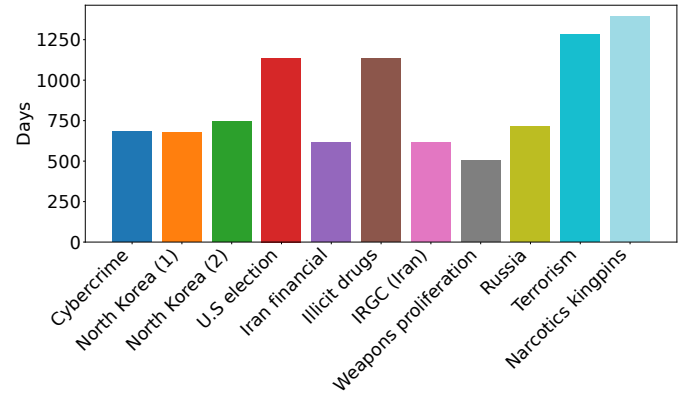


Fig. 8: Average active time for each program before getting sanctioned.

VI. CONCLUSION

This study provides a large-scale analysis of Bitcoin transactions involving sanctioned entities, uncovering key challenges in enforcing financial restrictions. Our findings reveal that sanctioned actors strategically move funds before restrictions take effect, with cybercrime-linked addresses facilitating the largest transfers—sometimes exceeding \$1 billion. Despite an immediate drop in activity post-sanction, some entities continued transacting for up to 1,500 days, highlighting enforcement gaps and the need for stronger regulatory measures.

While sanctions disrupt illicit financial activity, they do not fully prevent sanctioned entities from accessing cryptocurrency services, particularly through exchanges with inconsistent compliance. Strengthening enforcement mechanisms, improving exchange oversight, and leveraging blockchain analytics are critical to enhancing the effectiveness of sanctions in the digital asset space. Our work informs policymakers, regulators, and financial crime investigators seeking to mitigate cryptocurrency-based illicit finance. The dataset can be found here: <https://www.ida.liu.se/~nikca89/papers/lcn25.html>

ACKNOWLEDGMENT

This work was partially supported by the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by the Knut and Alice Wallenberg Foundation.

REFERENCES

- [1] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of Bitcoins: Characterizing payments among men with no names," in *Proc. ACM Internet Measurement Conference (IMC)*, 2013.
- [2] G. Gomez, P. Moreno-Sanchez, and J. Caballero, "Watch your back: Identifying cybercrime financial relationships in Bitcoin through back-and-forth exploration," in *Proc. ACM Computer and Communications Security (CCS)*, 2022.
- [3] C. Albrecht, K. M. Duffin, S. Hawkins, and V. M. Morales Rocha, "The use of cryptocurrencies in the money laundering process," *Journal of Money Laundering Control*, 2019.
- [4] M. Möser, R. Böhme, and D. Breuker, "An inquiry into money laundering tools in the Bitcoin ecosystem," in *Proc. APWG eCrime Researchers Summit*, 2013.
- [5] S. Lee, C. Yoon, H. Kang, Y. Kim, Y. Kim, D. Han, S. Son, and S. Shin, "Cybercriminal minds: An investigative study of cryptocurrency abuses in the dark web," in *Proc. Network and Distributed System Security Symposium (NDSS)*, 2019.
- [6] R. S. Portnoff, D. Y. Huang, P. Doerfler, S. Afroz, and D. McCoy, "Backpage and Bitcoin: Uncovering human traffickers," in *Proc. Knowledge Discovery and Data Mining (KDD)*, 2017.
- [7] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace," in *Proc. World Wide Web (WWW)*, 2013.
- [8] D. Y. Huang, M. M. Aliapoulos, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, A. C. Snoeren, and D. McCoy, "Tracking ransomware end-to-end," in *Proc. IEEE Symposium on Security and Privacy (S&P)*, 2018.
- [9] M. Paquet-Clouston, M. Romiti, B. Haslhofer, and T. Charvat, "Spams meet cryptocurrencies: Sextortion in the Bitcoin ecosystem," in *Proc. ACM Advances in Financial Technologies (AFT)*, 2019.
- [10] F. Oggier, A. Datta, and S. Phetsouvanh, "An ego network analysis of sextortionists," *Social Network Analysis and Mining*, 2020.
- [11] S. Pastrana and G. Suarez-Tangil, "A first look at the crypto-mining malware ecosystem: A decade of unrestricted wealth," in *Proc. ACM Internet Measurement Conference (IMC)*, 2019.
- [12] S. Pastrana, A. Hutchings, D. Thomas, and J. Tapiador, "Measuring ewhoring," in *Proc. ACM Internet Measurement Conference (IMC)*, 2019.
- [13] A. V. Vu, J. Hughes, I. Pete, B. Collier, Y. T. Chua, I. Shumailov, and A. Hutchings, "Turning up the dial: The evolution of a cybercrime market through set-up, stable, and Covid-19 eras," in *Proc. ACM Internet Measurement Conference (IMC)*, 2020.
- [14] D. Ron and A. Shamir, "How did dread pirate roberts acquire and protect his Bitcoin wealth?" in *Proc. Financial Cryptography and Data Security (FC)*, 2014.
- [15] D. Y. Huang, H. Dharmdasani, S. Meiklejohn, V. Dave, C. Grier, D. McCoy, S. Savage, N. Weaver, A. C. Snoeren, and K. Levchenko, "Botcoin: Monetizing stolen cycles," in *Proc. Network and Distributed System Security (NDSS)*, 2014.
- [16] X. Li, A. Yepuri, and N. Nikiforakis, "Double and nothing: Understanding and detecting cryptocurrency giveaway scams," in *Proc. Network and Distributed System Security (NDSS)*, 2023.
- [17] H. Rosenquist, D. Hasselquist, M. Arlitt, and N. Carlsson, "On the dark side of the coin: Characterizing Bitcoin use for illicit activities," in *Proc. Passive and Active Measurement (PAM)*, 2024.
- [18] L. Ingemarsson, K. Duckert Karlsson, and N. Carlsson, "Using venom to flip the coin and peel the onion: Measurement tool and dataset for studying the Bitcoin-dark web synergy," in *Proc. ACM Conference on Data and Application Security and Privacy (CODASPY)*, 2025.
- [19] Office of Foreign Assets Control, "OFAC Sanctions List Service," <https://sanctionslist.ofac.treas.gov/Home/SdnList>, 2024.
- [20] Blockchain.com, "Blockchain developer APIs," https://www.blockchain.com/explorer/api/blockchain_api, 2024.
- [21] Samourai Wallet, <https://oxt.me>, 2024.
- [22] U.S. Attorney's Office, "Founders and ceo of cryptocurrency mixing service arrested and charged with money laundering and unlicensed money transmitting offenses," 2024.
- [23] A. Biryukov and I. Pustogarov, "Bitcoin over Tor isn't a good idea," in *Proc. IEEE Symposium on Security and Privacy (S&P)*, 2015.
- [24] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in Bitcoin," in *Proc. Financial Cryptography and Data Security (FC)*, 2013.
- [25] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for Bitcoin with accountable mixes," in *Proc. Financial Cryptography and Data Security (FC)*, 2014.
- [26] L. Valenta and B. Rowan, "Blindcoin: Blinded, accountable mixes for Bitcoin," in *Proc. Financial Cryptography and Data Security (FC)*, 2015.
- [27] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "Coinshuffle: Practical decentralized coin mixing for Bitcoin," in *Proc. European Symposium on Research in Computer Security (ESORICS)*, 2014.
- [28] M. Spagnuolo, F. Maggi, and S. Zanero, "Bitiodine: Extracting intelligence from the Bitcoin network," in *Proc. Financial Cryptography and Data Security (FC)*, 2014.
- [29] S. Pletinckx, C. Trap, and C. Doerr, "Malware coordination using the blockchain: An analysis of the Cerber ransomware," in *Proc. IEEE Communications and Network Security (CNS)*, 2018.
- [30] T. Taniguchi, H. Griffioen, and C. Doerr, "Analysis and takeover of the Bitcoin-coordinated pony malware," in *Proc. ACM Asia Computer and Communications Security (ASIA CCS)*, 2021.
- [31] K. Wang, J. Pang, D. Chen, Y. Zhao, D. Huang, C. Chen, and W. Han, "A large-scale empirical analysis of ransomware activities in Bitcoin," *ACM Trans. on the Web*, 2021.
- [32] M. Conti, A. Gangwal, and S. Ruj, "On the economic significance of ransomware campaigns: A Bitcoin transactions perspective," *Computers & Security*, 2018.