Preprint version of Cryptocurrency and the Financing of Right-Wing Extremism: A Blockchain-Based Analysis. Available at: https://doi.org/10.4324/9781003473541-5

Cryptocurrency and the Financing of Right-Wing Extremism: A Blockchain-Based Analysis

Maria Jofre*

*Corresponding author

maria@openoswnership.org

Università Cattolica del Sacro Cuore and Transcrime

Via S. Vittore 43/45, 20123 Milan, Italy

https://orcid.org/0000-0001-6682-4668

Alberto Aziani

alberto.aziani@unimib.it

University of Milano – Bicocca

Piazza dell'Ateneo Nuovo, 1, 20126 Milan, Italy

https://orcid.org/0000-0002-4745-7337

Mirko Nazzari

mnazzari@uniss.it

University of Sassari

Viale Mancini, 5, 07100, Sassari, Italy

https://orcid.org/0000-0003-0019-3642

Preprint version of Cryptocurrency and the Financing of Right-Wing Extremism: A Blockchain-Based Analysis. Available at: https://doi.org/10.4324/9781003473541-5

Cryptocurrency and the Financing of Right-Wing Extremism: A Blockchain-Based Analysis

Right-wing extremists increasingly exploit cryptocurrencies to bypass traditional financial restrictions (e.g., PayPal bans) and leverage pseudo-anonymity, though empirical evidence remains sparse. This study analyzes 556 cryptocurrency addresses linked to U.S. far-right extremists (2012–2023) using blockchain forensics (Scorechain tool). Key findings reveal Bitcoin's dominance (87% of addresses), alongside growing adoption of Ethereum and Litecoin post-2017, with 40% of groups diversifying across blockchains. Non-custodial wallets (58% of addresses) facilitate regulatory evasion and high-volume transactions (averaging 183 per wallet). Extremist networks interact with 183,218 entities, including exchanges (41%), dark web services, and scams. Transactional activity peaked during Bitcoin's 2017 price increase but declined amid regulatory pressures (e.g., FATF's Travel Rule). USD balances revealed profit-driven strategies, with net outflows exceeding $6.6 million. These findings underscore extremists' adaptability to market and regulatory shifts, urging updated policies targeting non-custodial wallets, altcoin oversight, and cross-border collaboration. This study provides foundational empirical insights for disrupting extremist crypto-financing.

Keywords: right-wing extremism; cryptocurrency; Bitcoin; blockchain analysis; crowdfunding.

1. Introduction

Since the 2000s, the rapid expansion of financial technology (FinTech) innovations has significantly advanced the global economy by facilitating the swift and secure delivery of data-intensive financial services. However, alongside these advancements, concerns have arisen regarding the potential exploitation of said technologies for terrorist financing (Davis 2020; Jofre, Aziani, and Villa 2024; Reimer and Redhead 2022). These concerns have increasingly centered on virtual assets, notably cryptocurrencies, have captured the attention of policymakers in recent years as the latest frontier of terrorism financing (Salami 2018;

Kapsis 2023).

Compelling theoretical arguments support claims of potential cryptocurrency misuse for illicit activities (Akartuna, Johnson, and Thornton 2022; Goldman et al. 2017; Grant and Hogan 2015; Majumder, Routh, and Singha 2019). Scholars such as Carmona (2015) and Teichmann (2018) emphasize the potential for these technologies to provide anonymity in financial transactions. Furthermore, research by Choo (2015), Dion-Schwarz et al. (2019), and Wang & Zhu (2021) highlights how their accessibility and capacity for rapid international transfers introduces vulnerabilities that may be exploited for terrorist financing.

While terrorist groups dominate discussions of crypto-enabled financing, the involvement of other actors, such as political extremist groups, in leveraging these assets to fund their activities has been largely overlooked. The disproportionate scholarly and policy attention given to terrorist groups—rather than domestic political extremists—in cryptocurrency financing debates stems from structural, methodological, and perceptual biases. Post-9/11 counterterrorism frameworks prioritized combating transnational threats like ISIS or Al-Qaeda, cementing terrorism financing as a global policy imperative while sidelining extremist actors operating in legal gray zones. These groups, such as far-right movements, often exploit jurisdictional ambiguities: their activities may align with free speech protections in some democracies, complicating regulatory responses despite their role in spreading divisive ideologies (FATF 2021a; Knight, Woodward, and Lancaster 2017). This opacity is exacerbated by interdisciplinary silos: financial crime scholars focus on transactional risks, while extremism researchers rarely engage with blockchain forensics, leaving the nexus understudied. Meanwhile, institutional biases persist. Post-9/11, Western governments prioritized jihadist threats over politically driven domestic extremism, even as the latter's attacks surged (Campbell 2023; Dugan and Fisher 2023).However, this

perception fails to account for the potential dangers presented by these groups, even if their activities fall short of immediate criminality. Right-wing extremist groups, in particular, pose a significant social risk by exacerbating societal divisions and eroding trust in democratic institutions. Their ideologies, often centered around nationalism, ethnocentrism, and authoritarianism, can fuel social cleavages by promoting "us vs. them" narratives and demonizing out-groups (Carter 2018; Gerstenfeld, Grant, and Chiang 2003; Koehler 2016).

Research suggests exposure to extremist rhetoric can lead to increased prejudice, social anxiety, and a willingness to engage in violence against those perceived as threats (Canetti et al. 2013). Collective narcissism—defined as a defensive belief in a group's superiority and entitlement—can exacerbate hostility towards immigrants and justify extremist ideologies (Cichocka et al. 2022). Furthermore, the dissemination of misinformation and conspiracy theories by these groups can undermine public trust in established institutions, potentially leading to decreased social cohesion and political instability (Evangelatos et al. 2023; Goertzel 1994; Jolley, Meleady, and Douglas 2020). Investigating the social mechanisms by which right-wing extremism influences societal attitudes and behaviors is crucial for developing effective interventions to mitigate these risks.

Early detection of financial trends and resource allocation can be crucial in identifying and disrupting their efforts before they escalate. In line with this, several financial institutions have begun to reject payments associated with extreme right-wing groups due to violations of hate speech terms of services, prompting these groups to explore alternative financial channels (Keatinge, Keen, and Izenman 2019). Enhancing our comprehension of the financing mechanisms employed by these groups is imperative, particularly given the surge in extreme right-wing attacks witnessed in recent years (FATF 2021a). Understanding how these groups procure and utilize funds not only provides insights into their operational

Preprint version of Cryptocurrency and the Financing of Right-Wing Extremism: A Blockchain-Based Analysis. Available at: https://doi.org/10.4324/9781003473541-5

capabilities, but also informs strategic interventions aimed at disrupting their activities and safeguarding vulnerable communities from potential harm. However, there is still minimal empirical evidence on the stake that cryptocurrency funding has in right-wing circles

We aim to address this knowledge gap by offering, to the best of our knowledge, the first empirical analysis on the topic. Specifically, we focus on the financing activities of right-wing extremist groups in the United States using data collected by the Southern Poverty Law Center. The selection of the United States as our case study is driven by the fact that domestic violent extremism stands as one of the most pressing security threats facing this country today, and attacks perpetrated by right-wing extremist groups have significantly increased in recent years (Brookhouser 2021; Jones 2018).

This study makes several contributions to the field of right-wing extremism research. Firstly, it pioneers the use of blockchain technology for tracing and analyzing extremist financial activities. This novel methodology offers a transparent and detailed examination of fund flows, potentially uncovering previously hidden aspects. Secondly, examining data spanning over a period of more than ten years, the study provides evidence of the shift towards anonymous and decentralized financing within extremist groups. By analyzing transactions across multiple cryptocurrencies, the research reveals the evolving nature of extremist financing, including portfolio diversification and strategic currency use. Thirdly, it broadens our understanding of these groups' operational tactics, encompassing not just ideology but also economic strategies and adaptation to financial pressures.

The rest of the paper is structured as follows. The next section, *Background*, reviews previous literature that investigated how extreme right-wing groups collect and move their funds. Section *Methodology* illustrates the data, blockchain analytic tools, and statistical

approaches employed in this study. Section *Results* presents empirical findings on cryptocurrency usage patterns, transactional dynamics, and temporal trends among US-based extremist groups; moreover, it synthesizes key limits of our study. The *Discussion* provides an analysis and interpretation of the research findings, while the *Conclusions* section offers a summary of the key findings succinctly.

2. Background

Research on the financing methods of right-wing extremists remains in its initial stages. While some speculation exists, robust empirical evidence and a cohesive theoretical framework are limited. Previous analyses have suggested that right-wing extremists commonly employ well-established methods for securing funding, including merchandise sales (clothing or symbolic items), event fees, and direct donations from supporters (Keatinge, Keen, and Izenman 2019; Golumbia 2016). These traditional approaches, grounded in historical practices, continue to serve as significant income sources for right-wing extremist organizations (FATF 2021a). Additionally, some right-wing extremist groups resort to illegal tactics akin to those used by other extremist groups, such as robberies, fraud, or trade in prohibited goods (FATF 2021a).

Beginning in the 2010s, the diffusion of social media platforms and cryptocurrencies has opened new avenues for right-wing extremist financing, echoing trends observed among terrorist groups. Analysts have noted how social media platforms offer anonymity, enabling extremist groups to broaden their reach and solicit donations from a larger audience (Caniglia, Winkler, and Métais 2020; Golumbia 2015; Keatinge, Keen, and Izenman 2019). Cryptocurrencies, characterized by their pseudo anonymity and ease of transfer, provide a convenient means for managing funds, catering to both legitimate initiatives and illicit

activities by right-wing extremists. The decentralized nature of cryptocurrencies complicates efforts to trace financial transactions. Indeed, despite tighter regulations on virtual asset service providers (VASPs), regarding industry's regulation including know-your-customer policies, significant gaps persist, particularly in non-cooperative countries, posing challenges for law enforcement and counterterrorism efforts.

The decentralized structure of cryptocurrencies not only provides practical benefits but also aligns with the anti-establishment ideology of some right-wing extremists, who view traditional financial institutions with suspicion (Keatinge et al., 2019). This ideological alignment manifests in multiple ways. Firstly, many right-wing extremists share a distrust of centralized authorities, perceiving traditional financial institutions as extensions of government power or tools of a global elite. Cryptocurrencies, devoid of central authority, symbolize a perceived liberation from such control. Secondly, some extremist groups are attracted to the technological innovation inherent in cryptocurrencies, seeing them as emblematic of a new, decentralized future (Caiani and Parenti 2009).

Overall, the extent and nature of cryptocurrency adoption among right-wing extremists remain elusive. Additional empirical investigations are necessary to understand how these groups leverage cryptocurrencies and other modern financial technologies for financing purposes (Keatinge et al., 2019; Golumbia, 2015). Future research endeavors should build upon existing literature to delve into the involvement of third-party entities such as cryptocurrency exchanges and dark web services, while also exploring potential intersection with emerging technologies like non-fungible tokens (NFTs) and the Metaverse (Keatinge et al., 2019). Examining the full spectrum of financing methods across different geographical contexts is essential for the development of robust counter-extremism strategies. This study aims to bridge this knowledge gap through blockchain analysis.

Preprint version of Cryptocurrency and the Financing of Right-Wing Extremism: A Blockchain-Based Analysis. Available at: https://doi.org/10.4324/9781003473541-5

3. Methodology

Data collection

The study leverages data from the Southern Poverty Law Center (SPLC) Hatewatch investigation, which examined the adoption of cryptocurrencies by right-wing and white supremacist groups for financial sustenance in the United States (Hayden and Squire 2021). This investigation resulted in the compilation and dissemination of a structured dataset comprising over six hundred cryptocurrency addresses associated with 97 of these groups. From this compilation, we conducted rigorous data cleaning and processing procedures. Leveraging Scorechain's blockchain technology, we successfully identified a total of 556 cryptocurrency addresses across three major blockchains: Bitcoin, Ethereum, and Litecoin. The resulting dataset includes essential information about each address and spans transactional activity from mid-January 2012 to late August 2023.

First, we have information on the blockchain to which the address belongs, namely Bitcoin, Ethereum, or Litecoin. Second, we identified whether the address is associated with a non-custodial wallet, meaning wallets where users retain control over their private keys. In contrast to custodial wallets, where a third party manages the private keys, non-custodial wallets grant users complete autonomy over their cryptocurrency holdings. Third, we utilized user-generated labels associated with blockchain addresses, which provide insights into the nature of the address (e.g., bank, mixing service, exchange) or potential issues related to it (e.g., scam, suspicious activity, hack). Analyzing these labels allows us to discern the opacity of addresses within right-wing extremist networks and the likelihood of their involvement in illegal or fraudulent activities. Fourth, we recorded the total number of transactions involving each address, the total amount of transacted assets, and the corresponding total counter value in USD. Additionally, we aggregated address data at the

extremist group level to calculate additional features, including the number of addresses, whether multiple blockchains were utilized, and the number of blockchains involved.

Transactional data extraction

Subsequently, transactional data for these addresses was retrieved using the same blockchain technology employed in the initial data collection phase. This transactional data comprised information on 75,439 transactions, with each transaction record including details such as the date and time of the transaction, sender(s) and receiver(s) addresses, blockchain used, and the amount of assets transacted along with their respective counter value in USD. Furthermore, information on the distinct types of entities involved in these transactions was collected, which encompassed data related to exchanges, payment services, donation websites, gambling platforms, and dark web services, among others.

Methodological approach

Given the descriptive and exploratory nature of the research, basic yet informative methodologies were employed. Initially, descriptive statistics such as mean, standard deviation, minimum, mode, maximum, and sum of all values were calculated to gain insights into the datasets. Hypothesis testing, specifically t-tests, was conducted to explore potential differences between groups or categories within the data. Finally, relevant and meaningful visualizations were generated to enhance the understanding of the exploratory findings and facilitate their interpretation.

Limitations

The methodology employed in this research has some limitations that merit consideration. Firstly, our reliance on data sourced from the Hatewatch investigation may introduce a potential bias into our analysis. While the dataset is comprehensive, the possibility of some

right-wing extremists being overlooked or omitted due to factors such as incomplete information or oversight cannot be entirely discounted. Furthermore, the Hatewatch database exclusively focuses on right-wing extremists operating within the United States, limiting the external validity of the findings, as right-wing extremists in other geographical regions may exhibit different patterns.

The second limitation concerns the absence of data on the Monero blockchain. Although the original dataset included an additional 36 Monero addresses, we were unable to assess them further due to the impossibility to extract account and transactional data from this blockchain. This constrain is primarily attributed to the untraceability and unlinkability features inherent in the Monero Protocol, rendering the blockchain technology we employed incompatible with this specific blockchain. As a result, our analysis does not capture the use of Monero, which, in any case, represented only a small portion of the dataset.

4. Results

Blockchain preferences

Figure 4.1 illustrates the predominant utilization of Bitcoin as the preferred blockchain, accounting for 87% of all 556 addresses. Ethereum and Litecoin, while less dominant, still hold significant shares of 8% and 5%, respectively. This dominance of Bitcoin is further emphasized when examining transactional activities associated with these addresses, with a staggering 98% of all transactions occurring through Bitcoin (Figure 4.2).

Figure 4.1. Distribution of blockchains among addresses.

Preprint version of Cryptocurrency and the Financing of Right-Wing Extremism: A Blockchain-Based Analysis. Available at: https://doi.org/10.4324/9781003473541-5

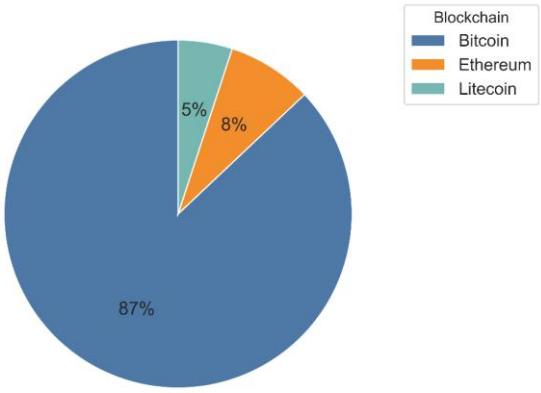
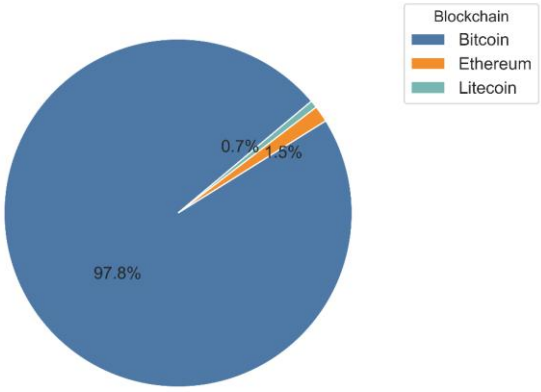


Figure 4.2. Distribution of blockchains among transactions.



Despite Bitcoin's prevalent usage, Figure 4.3 sheds light on a notable trend – a discernible increase in the adoption of altcoins. Transactions involving Ethereum and Litecoin began modestly in 2017 but have steadily increased in subsequent years, indicating a growing interest in these currencies and diversifying cryptocurrency usage. Specifically, while in 2017 Ethereum and Litecoin jointly accounted for the 2.4% of all transactions, their combined relative relevance grew to the 47% in 2021. This diversification strategy interest is round 40% of the total 97 extremist groups (Figure 4.4).

Figure 4.3. Distribution of the year of first transactions by blockchain.

Preprint version of Cryptocurrency and the Financing of Right-Wing Extremism: A Blockchain-Based Analysis. Available at: https://doi.org/10.4324/9781003473541-5

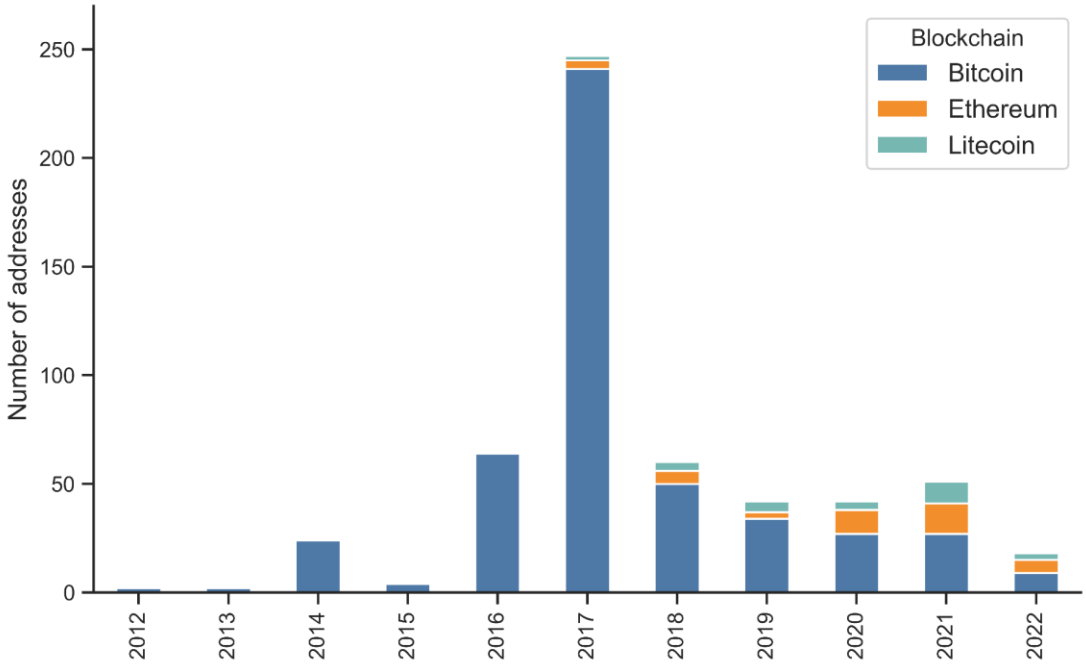
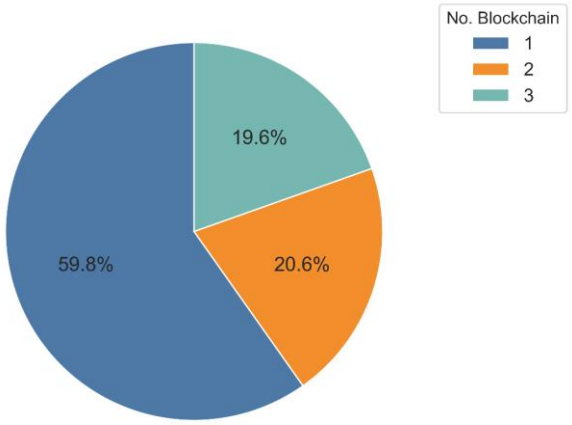


Figure 4.4. Distribution of the number of blockchains used by extremist groups.



When comparing extremist groups using a single blockchain and those exploiting multiple blockchains significant differences emerge regarding their blockchain patterns (Table 4.1). Aside the number of blockchain exploited which differs significantly, with the former group using only one and the latter utilizing an average of 2.5 blockchains. While the number of addresses utilized does not differ significantly, the multiple blockchain group employs significantly more Ethereum and Litecoin addresses compared to the single blockchain group, which predominantly utilizes Bitcoin. This further

provides evidence of the growing adoption of multiple blockchains among extremist groups, expanding beyond Bitcoin to include altcoins like Ethereum and Litecoin.

Table 4.1. T-test results comparing groups using single blockchain vs. multiple blockchains.

Variable	Single blockchain (Mean)	Multiple blockchain (Mean)	T-Statistic	P-Value	Sign.
No. blockchain	1.00	2.49	-22.425	0.000	***
No. addresses	6.07	5.23	0.209	0.835	
No. Bitcoin addresses	6.05	3.41	0.662	0.510	
No. Ethereum addresses	0.00	1.13	-10.343	0.000	***
No. Litecoin addresses	0.02	0.69	-7.234	0.000	***

Non-custodial wallets

The analysis reveals the widespread adoption of non-custodial wallets, constituting 58% of all 556 addresses (Table 4.2). Although their usage is prevalent across all three blockchains, Ethereum and Litecoin addresses favor non-custodial wallets, while Bitcoin addresses are distributed more evenly.

Table 4.2. Distribution of individual addresses and wallet addresses across different blockchains.

Type of address	Bitcoin	Ethereum	Litecoin	Total
Individual addresses	223 (46%)	2 (5%)	7 (25%)	232 (42%)
Non-custodial wallet addresses	261 (54%)	42 (95%)	21 (75%)	324 (58%)
Total	484	44	28	556

A t-test comparing individual addresses with those associated with non-custodial wallets underscores significant differences in their blockchain and transactional characteristics

(Table 4.3). While individual addresses are primarily linked to Bitcoin, wallet addresses extend into the Ethereum domain. Moreover, addresses linked to non-custodial wallets engage in statistically significant more transactions than individual addresses, particularly in the case of Bitcoin. This suggests that while wallet addresses are associated with wallets that include altcoins, their predominant reliance is on Bitcoin for most transactions conducted.

Table 4.3. T-test results comparing individual addresses vs. non-custodial wallet addresses.

Variable	Individual addresses (Mean)	Non-custodial wallet addresses (Mean)	T-Statistic	P-Value	Sign.
Bitcoin (dummy)	0.96	0.81	5.527	0.000	***
Ethereum (dummy)	0.01	0.13	-5.335	0.000	***
Litecoin (dummy)	0.03	0.07	-1.844	0.066	
No. transactions	70.25	183.09	-4.287	0.000	***
No. Bitcoin transactions	67.66	179.20	-4.221	0.000	***
No. Ethereum transactions	1.61	2.97	-1.080	0.281	
No. Litecoin transactions	0.98	0.92	0.131	0.896	

Transactional patterns

A closer examination of the descriptive statistics related to transactional patterns is presented in Table 4.4. The analysis reveals that out of the 556 addresses under consideration, a total of 75,439 transactions were conducted. On average, each address is associated with 136 transactions, with the distribution being right-skewed, indicating that a small number of addresses are responsible for a considerable proportion of transactions. Approximately 79% of these transactions involved the extremists' addresses as recipients,

while the remaining 21% were initiated by them as senders. Moreover, it is noteworthy that while the disparity between the average amounts of cryptocurrencies received and sent by each address is minimal, with only a difference of 0.4 units, the disparity between the corresponding countervalue in USD is quite large, reaching almost $12,000.

The analysis underscores two key features. First, it reveals the pivotal role of addresses associated with right-wing extremists in facilitating the flow of funds within the networks. These addresses serve as central channels for the movement of funds, with transactions directed towards them. Moreover, they exhibit a transient nature, with minimal cryptocurrency units remaining in their balances after transactions. The transactional behavior observed suggests a pattern of balancing multiple low-value incoming transactions with fewer, but higher-value outgoing transactions.

Second, while the balance in terms of cryptocurrency assets is, on average, close to zero, the balance in terms of USD is negative, indicating that the sent value is higher than the received value. This suggests a profit-making feature of these funding schemes, wherein the fluctuation in the value of cryptocurrencies over time generates profit for the ultimate recipients of transacted funds.

Table 4.4. Descriptive statistics of transactional information for addresses.

Variable	Mean	Std. Dev.	Min.	50%	Max.	Sum
No. transactions	135.7	310.9	1	13	5,122	75,439
No. Bitcoin transactions	132.7	311.09	0	4	5,122	73,760
No. Ethereum transactions	2.1	12.8	0	0	188	1,153
No. Litecoin transactions	0.9	5.6	0	0	62	526
No. received transactions	107.7	277.4	1	9	5,088	59,892
No. sent transactions	28.0	58.6	0	2	572	15,547

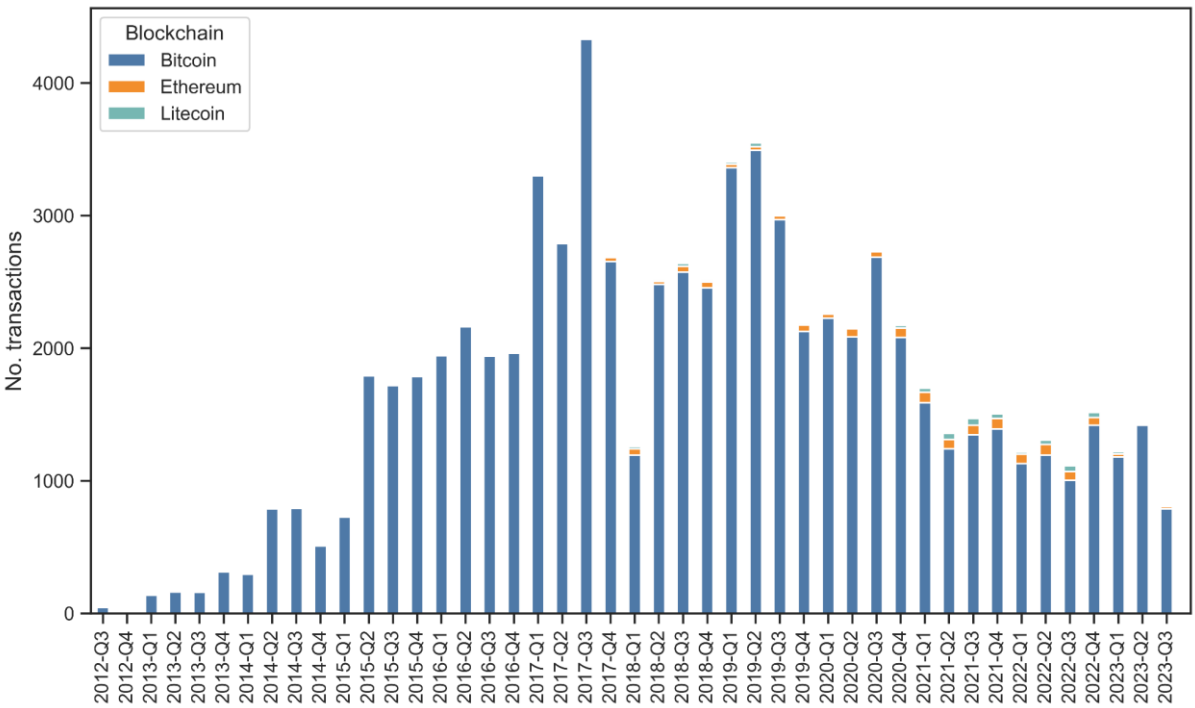
Preprint version of Cryptocurrency and the Financing of Right-Wing Extremism: A Blockchain-Based Analysis. Available at: https://doi.org/10.4324/9781003473541-5

Cryptocurrencies received	17.6	67.6	0	1	703.1	9,768
Cryptocurrencies sent	17.2	67.6	0	0.5	702.8	9,555
Cryptocurrencies balance	0.4	3.1	0	0	55.3	213
USD received	87,458.5	709,284.9	0.1	3,123.7	8,370,922.1	48,626,908
USD sent	993,31.7	694,785.2	0.0	3,886.8	8,103,157.1	55,228,421
USD balance	-11,873.2	90,950.1	-1,671,596.0	-10.7	267,765.0	-6,601,512

Temporal patterns

An analysis of the temporal evolution of transactional data associated with the 556 addresses reveals an inverted u-shaped dynamic pattern (Figure 4.5). Transaction activity surged from 2012, peaking in mid-2017, before gradually declining until the end of the observation period.

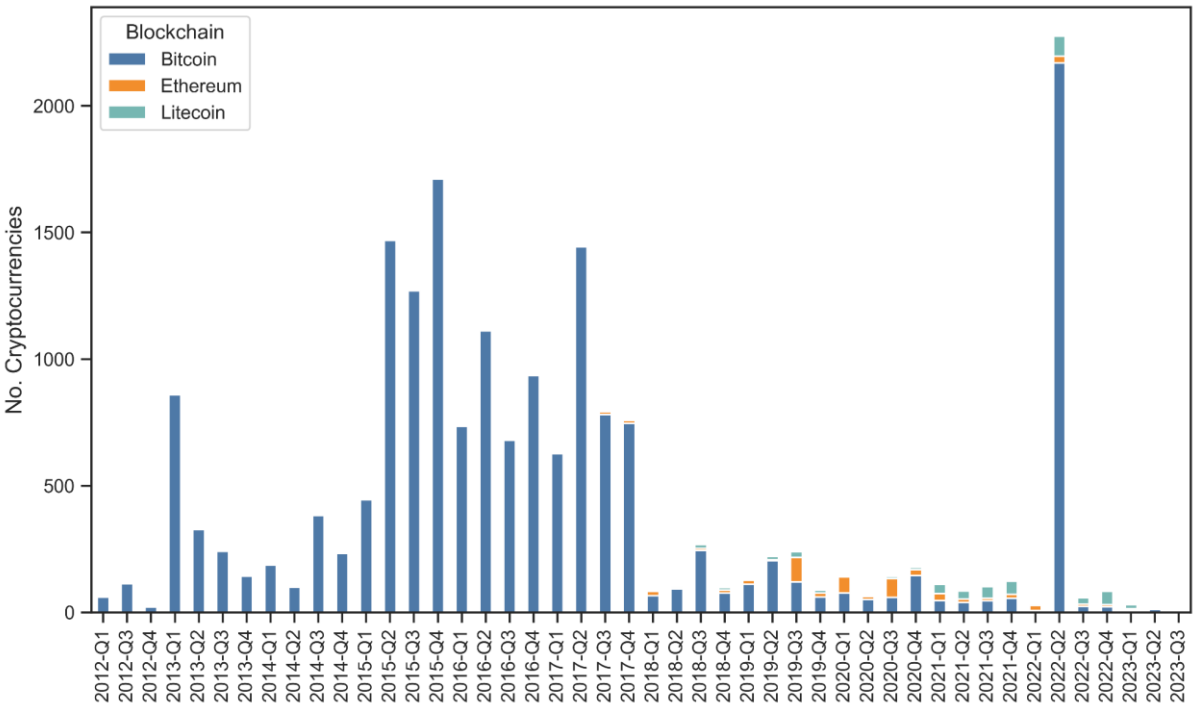
Figure 4.5. Temporal evolution of transactions by blockchain.



When observing the actual assets involved in such transactions, a distinct trend emerges (Figure 4.6). After initial fluctuations, the number of assets significantly decreases, with

a sudden surge in activity towards the end of the observation period, followed by a decline to near-zero levels. Interestingly, the transactional activity involving altcoins, such as Ethereum and Litecoin, intensified during periods of reduced overall transaction volume spanning from 2018 to the first quarter of 2022.

Figure 4.6. Temporal evolution of cryptocurrency amount transacted by blockchain.

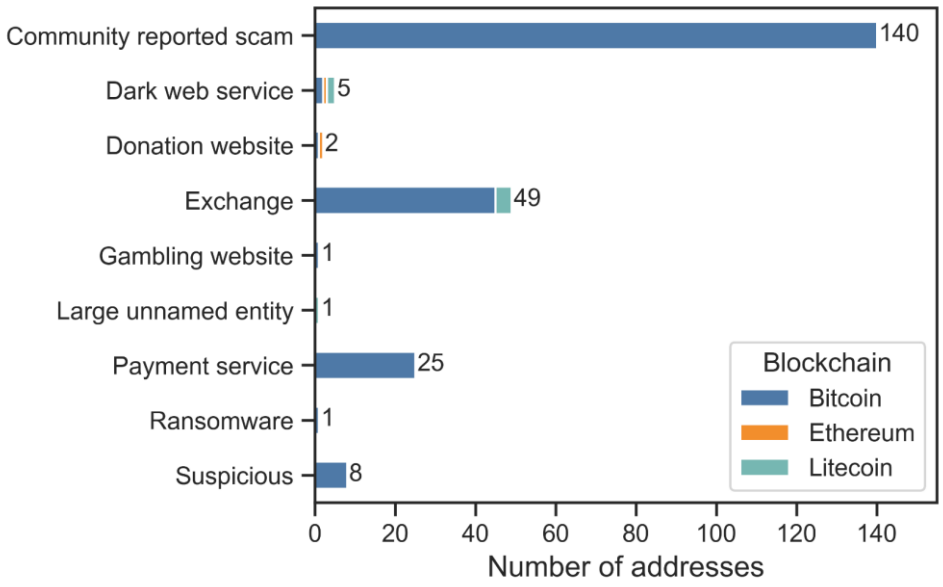


Types of entities involved in transactions

In the final step of our analysis, we examined the labels associated with extremists addresses and the accounts interacting with them. Among the 556 addresses linked to extremist groups, a notable portion has been flagged with specific labels by the cryptocurrency community (Figure 4.7). Specifically, 140 addresses have been identified as scams, while 49 are associated with exchanges and 25 with payment systems. Additionally, eight addresses are linked to suspicious accounts, five to dark web services, and two to donation websites. Differently from the other categories the latter two, namely

dark web services and donation websites, are associated with all the three blockchains. Furthermore, individual addresses are directly connected to gambling websites, large unnamed entities, and ransomware activities.

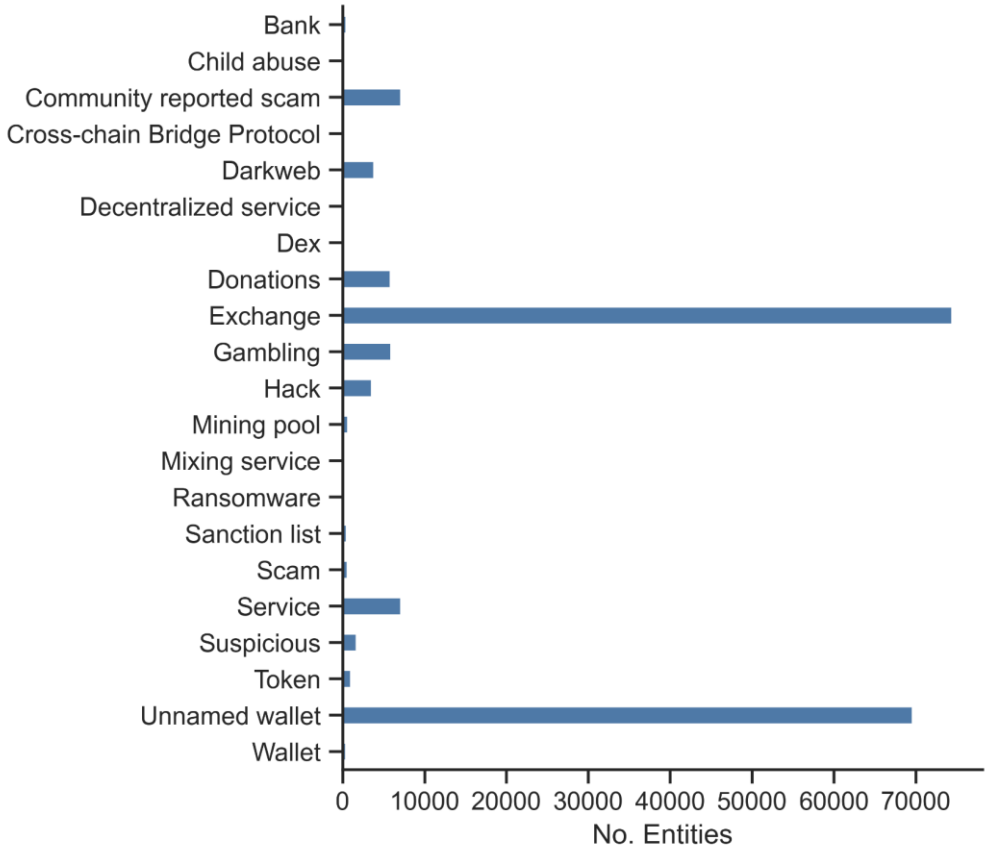
Figure 4.7. Frequency of entity types of addresses.



Further analysis of the external entities involved in transactions reveals interactions with a total of 183,218 identifiable entities across various categories. As depicted in Figure 4.8, most of these entities, nearly 41%, are categorized as exchanges, while 38% are classified as unnamed wallets. A smaller proportion of transactions are associated with addresses reported as scams, payment services, gambling and donation websites, dark web services, as well as hack and suspicious accounts.

Figure 4.8. Frequency of entity types involved in transactions by blockchain.

Preprint version of Cryptocurrency and the Financing of Right-Wing Extremism: A Blockchain-Based Analysis. Available at: https://doi.org/10.4324/9781003473541-5



5. Discussion

This study offers insights into the funding strategies and operational dynamics of right-wing extremists, with a particular focus on their use of cryptocurrencies. Our analysis of 556 addresses compiled by the Southern Poverty Law Center (SPLC) using blockchain technology (Scorechain tool), provides valuable insights into the modus operandi of right-wing extremists in the United States between 2012 and 2023.

Our findings underscore the multifaceted landscape within which US right-wing extremists operate, encompassing various systems and technologies such as social media and the deep web. While this study does not directly compare the importance of crypto assets to traditional value-transfer methods, the scale of transactions and deposits observed suggests a significant reliance on cryptocurrencies among far-right extremists, potentially surpassing that within most terrorist networks (see Jofre, Aziani, and Villa

2024).

Often advocating for self-sufficiency and limited government intervention, right-wing extremists find cryptocurrencies appealing due to their enhanced anonymity and capacity to operate beyond traditional regulatory frameworks (Keatinge, Keen, and Izenman 2019; Golumbia 2016). In this respect, evidence from our study confirms the widespread preference for Bitcoin among these extremist groups. However, unlike other cryptocurrencies such as Monero and Zcash, Bitcoin offers only pseudo anonymity, thoughthe identities of users behind the addresses involved in a transaction are not readily apparent, the flow of money can, nonetheless, be traced on the public blockchain and, eventually, identities can be uncovered by correlating blockchain data with attribution data from other sources. One potential explanation for this finding is that right-wing extremists prioritize higher tradability, real-time trading, and withdrawal capabilities over enhanced security features. This preference may be influenced by a lower level of law enforcement pressure or by the legal nature of both the funding and the activities funded by groups exclusively using Bitcoins.

However, starting in 2017, we observed a gradual increase in the use of altcoins like Ethereum and Litecoin. This trend underscores the adaptability and strategic diversification of these groups. Notably, the simultaneous use of multiple blockchains is more prevalent among addresses associated with non-custodial wallets. This observation suggests the presence of two distinct categories of extremist groups: those employing more sophisticated strategies involving both multiple cryptocurrencies and secure wallets, and those relying on simpler cryptocurrency usage. Further research could investigate whether these differing behaviors are driven by involvement in illegal activities, variations in technical proficiency between the groups, or other yet-to-be-unidentified factors.

It might be speculated that the observed inverted U-shaped pattern in transaction volume, peaking in mid-2017 and declining thereafter, could potentially align with Bitcoin's historical price dynamics. One could hypothesize that the 2017 bull run, during which Bitcoin's price surged from approximately $1,000 to nearly $20,000, may have incentivized right-wing extremists to explore rising asset values for fundraising and profit generation. It is conceivable that the subsequent decline in transaction volume after 2017 correlates with Bitcoin's sharp price correction in early 2018 (dropping to $3,000 by December 2018), which might have diminished the perceived utility of holding or transacting in Bitcoin for short-term gains (see, CoinMarketCap 2025). Perhaps this volatility could explain the gradual shift toward altcoins like Ethereum and Litecoin starting in 2017, as extremist groups may have sought to diversify their portfolios to mitigate risks associated with Bitcoin's price instability (Corbet, Lucey, and Yarovaya 2018).

It is possible that the FATF's 2019 "Travel Rule," which mandated that virtual asset service providers (VASPs) collect and share sender/receiver information, potentially influenced transactional behavior. It could be argued that the post-2019 increased use of Ethereum and Litecoin reflects potential efforts to evade scrutiny, as these blockchains were possibly initially less regulated than Bitcoin. Furthermore, the increase in non-custodial wallet usage might align with regulatory avoidance strategies, as these wallets bypass VASP oversight (FATF 2021b). It is also possible that the decline in overall transaction volume after 2017 reflects potential heightened compliance pressures, pushing extremist groups toward smaller, fragmented transactions to avoid detection thresholds.

These trends could suggest an interplay between market forces and regulatory environments in shaping extremist financial behavior. It's theorized that the

diversification into altcoins and non-custodial wallets is not merely a technical preference, but a potential strategic response to Bitcoin's diminishing anonymity under regulatory scrutiny and its volatility as a store of value. Future research might explore how macroeconomic trends and evolving regulations continue to potentially influence extremist crypto adoption.

Analysis of transactional data revealed also that cryptocurrency addresses associated with far-right groups function as conduits, facilitating transactions among various parties. Our analysis identified economic interactions between the 97 extremist groups and 183,218 other entities. These entities spanned various categories, including dark web addresses, suspected scam operations, and gambling services. These findings align with previous research indicating collaborative engagement of third parties for funding purposes. While addresses linked to clear (e.g., frauds) or suspected illegal activities (e.g., money laundering) were a minority, the extreme rights' crypto accounts connected to illegitimate addresses should warrant scrutiny by law enforcement. Indeed, the volume of transactions and the types of entities involved raise concerns about potential illicit activities within these extremist networks.

Finally, our analysis revealed a discrepancy between cryptocurrency balances, which often remained at zero (indicating incoming and outgoing transactions balanced each other), and USD balances, which showed a pattern of outflows exceeding inflows. This suggests that right-wing extremists may not only use their cryptocurrency addresses to manage fundraising but also potentially for profit generation, as already stressed by previous literature (Argentino, Davis, and Hamming 2023). However, the extent to which these profits are used to fund extremist activities or are appropriated by individual leaders managing fundraising campaigns remains unclear. Further investigation is needed to understand the flow of these funds and their ultimate purpose.

In terms of policies, the prevalence of non-custodial wallets (58% of addresses) highlights a critical regulatory gap. Unlike custodial platforms, non-custodial wallets operate outside conventional anti-money laundering frameworks, enabling extremists to bypass know your customer checks. To address this, regulators should expand the FATF's Travel Rule to mandate transaction reporting for non-custodial wallets above threshold values, similar to requirements for exchanges. Additionally, wallet providers could be compelled to integrate forensic tools to flag suspicious activity linked to extremist-associated addresses.

The shift of extremist financial activities towards a broader range of cryptocurrencies, including Ethereum, Litecoin, and notably, privacy coins like Monero, reveals a critical vulnerability in current regulatory frameworks. Existing AML measures often focus disproportionately on Bitcoin, leaving altcoins and privacy-focused currencies under-scrutinized. This disparity creates a significant regulatory gap, as illicit actors exploit the varying levels of oversight. To effectively counter this, policymakers must prioritize the development of adaptable, harmonized anti-money laundry regulations that encompass all virtual assets. This requires a multi-faceted approach, including: enhanced and evolving blockchain analytics partnerships capable of tracking transactions across diverse blockchains; stricter and more comprehensive virtual asset service provider licensing requirements that account for the unique challenges posed by privacy coins; and ongoing international collaboration to address the rapidly evolving nature of cryptocurrency technology.

Finally, the cross-border nature of blockchain transactions necessitates global coordination. Initiatives like the EU's Markets in Crypto-Assets (MiCA) regulation should be monitored and eventually replicated internationally, with shared databases for extremist-linked addresses and standardized reporting mechanisms for suspicious

transactions.

6. Conclusion

This research contributes to bridging a knowledge gap in our understanding of how right-wing extremist movements exploit cryptocurrencies for funding and resource management. Prior to this study, the area remained largely speculative. Our investigation sheds light on this previously opaque domain by conducting an in-depth analysis of 556 cryptocurrency addresses associated with 97 right-wing extremists, encompassing 75,439 distinct crypto transactions.

Our findings underscore a prevalent use of Bitcoin among right-wing extremists, with a notable trend towards diversification into Ethereum, Litecoin, and Monero starting in 2017. This strategic shift suggests a deliberate effort to avoid detection by leveraging the capabilities offered by different digital currencies. Additionally, engagement with non-custodial wallets and various services such as exchanges, mixers, and dark web platforms indicates a sophisticated and layered financial infrastructure supporting extremist crypto financing.

While our research provides valuable insights into the funding of right-wing extremists, it is not without limitations. These include dependence on specific datasets and the challenge posed by privacy coins like Monero. These limitations highlight the need for ongoing research in this rapidly evolving threat landscape. Furthermore, future studies, incorporating methodologies such as social network analysis and time series analysis, can shed light on the relationships between addresses and entities, as well as the dynamics of transactional data. This deeper understanding could unveil the roles of different addresses within extremist networks and their transactional strategies.

Preprint version of Cryptocurrency and the Financing of Right-Wing Extremism: A Blockchain-Based Analysis. Available at: https://doi.org/10.4324/9781003473541-5

References

Akartuna, Eray Arda, Shane D. Johnson, and Amy E. Thornton. 2022. "The Money Laundering and Terrorist Financing Risks of New and Disruptive Technologies: A Futures-Oriented Scoping Review." *Security Journal*, September, 1–36. https://doi.org/10.1057/s41284-022-00356-z.

Argentino, Marc-Andre, Jessica Davis, and Tore Refslund Hamming. 2023. "Financing Violent Extremism: An Examination of Maligned Creativity in the Use of Financial Technologies." 22. Reports, Projects, and Research. National Counterterrorism Innovation, Technology, and Education Center; and International Centre for the Study of Radicalisation. https://digitalcommons.unomaha.edu/ncitereportsresearch/22.

Brookhouser, J. J. 2021. "Through the Extremist Lens: Uncovering the Correlation Between Domestic Right-Wing Extremist Ideology and Violence in the United States from 2000 to 2020." *Global Security and Intelligence Studies* 6 (1). https://doi.org/10.18278/gsis.6.1.2.

Caiani, Manuela, and Linda Parenti. 2009. "The Dark Side of the Web: Italian Right-Wing Extremist Groups and the Internet." *South European Society and Politics* 14 (3): 273–94. https://doi.org/10.1080/13608740903342491.

Campbell, Kristy. 2023. "Examining Structural Disparities in Domestic and International Counterterrorism Policy in the US and Their Consequences." Ph.D., United States -- Virginia: George Mason University. https://www.proquest.com/docview/2849749669/abstract/CA6ADC286C24416EPQ/1.

Canetti, Daphna, Brian J. Hall, Carmit Rapaport, and Carly Wayne. 2013. "Exposure to Political Violence and Political Extremism: A Stress-Based Process." *European Psychologist* 18 (4): 263–72. https://doi.org/10.1027/1016-9040/a000158.

Caniglia, Mattia, Linda Winkler, and Solène Métais. 2020. "The Rise of the Right-Wing Violent Extremism Threat in Germany and Its Transnational Character." European Strategic Intelligence and Security Center.

Carmona, Anais. 2015. "The Bitcoin: The Currency of the Future, Fuel of Terror." In *Evolution of Cyber Technologies and Operations to 2035*, edited by Misty Blowers, 127–35. Advances in Information Security. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-23585-1_9.

Carter, Elisabeth. 2018. "Right-Wing Extremism/Radicalism: Reconstructing the Concept." *Journal of Political Ideologies* 23 (2): 157–82. https://doi.org/10.1080/13569317.2018.1451227.

Choo, Kim-Kwang Raymond. 2015. "Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks?" In *Handbook of Digital Currency*, edited by David Lee Kuo Chuen, 283–307. San Diego: Academic Press. https://doi.org/10.1016/B978-0-12-802117-0.00015-1.

Cichocka, Aleksandra, Konrad Bocian, Mikolaj Winiewski, and Flavio Azevedo. 2022. "'Not Racist, But…': Beliefs About Immigration Restrictions, Collective Narcissism, and Justification of Ethnic Extremism." *Political Psychology* 43 (6): 1217–34. https://doi.org/10.1111/pops.12813.

CoinMarketCap. 2025. "Bitcoin Price History and Historical Data." CoinMarketCap. 2025. https://coinmarketcap.com/currencies/bitcoin/historical-data/.

Corbet, Shaen, Brian Lucey, and Larisa Yarovaya. 2018. "Datestamping the Bitcoin and Ethereum Bubbles." *Finance Research Letters* 26 (September):81–88. https://doi.org/10.1016/j.frl.2017.12.006.

Preprint version of Cryptocurrency and the Financing of Right-Wing Extremism: A Blockchain-Based Analysis. Available at: https://doi.org/10.4324/9781003473541-5

Davis, Jessica. 2020. "New Technologies but Old Methods in Terrorism Financing." 2. Research Briefing. RUSI. https://static1.squarespace.com/static/5e399e8c6e9872149fc4a041/t/5f18579880818c6feb0e6a49/1595430886467/CRAAFT+Jessica+Davis.pdf.

Dion-Schwarz, Cynthia, David Manheim, and Patrick B. Johnston. 2019. "Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats." RAND Corporation. https://www.rand.org/pubs/research_reports/RR3026.html.

Dugan, Laura, and Daren Fisher. 2023. "Far-Right and Jihadi Terrorism Within the United States: From September 11th to January 6th." *Annual Review of Criminology* 6 (Volume 6, 2023): 131–53. https://doi.org/10.1146/annurev-criminol-030521-102553.

Evangelatos, Spyridon, Thanasis Papadakis, Nikolaos Gousetis, Christos Nikolopoulos, Petrina Troulitaki, Nikos Dimakopoulos, George Bravos, Michael V. Lo Giudice, Ali Shadma Yazdi, and Alberto Aziani. 2023. "The Nexus Between Big Data Analytics and the Proliferation of Fake News as a Precursor to Online and Offline Criminal Activities." In , 4056–64. IEEE Computer Society. https://doi.org/10.1109/BigData59044.2023.10386618.

FATF. 2021a. "Ethnically or Racially Motivated Terrorism Financing." Paris: FATF. https://www.fatf-gafi.org/publications/methodsandtrends/documents/ethnically-racially-motivatedterrorism-financing.html.

———. 2021b. "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." Paris: Financial Action Task Force. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf.

Gerstenfeld, Phyllis B., Diana R. Grant, and Chau-Pu Chiang. 2003. "Hate Online: A Content Analysis of Extremist Internet Sites." *Analyses of Social Issues and Public Policy (ASAP)* 3 (1): 29–44. https://doi.org/10.1111/j.1530-2415.2003.00013.x.

Goertzel, Ted. 1994. "Belief in Conspiracy Theories." *Political Psychology* 15 (4): 731–42. https://doi.org/10.2307/3791630.

Goldman, Zachary K., Elly Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss. 2017. "Terrorist Use of Virtual Currencies. Containing the Potential Threat." Center for a New American Security. https://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf.

Golumbia, David. 2015. "Bitcoin as Politics: Distributed Right-Wing Extremism." SSRN Scholarly Paper. Rochester, NY. https://doi.org/10.2139/ssrn.2589890.

———. 2016. *The Politics of Bitcoin: Software as Right-Wing Extremism*. 1st edition. Minneapolis: Univ Of Minnesota Press.

Grant, Gerry, and Robert Hogan. 2015. "Bitcoin: Risks and Controls." *Journal of Corporate Accounting & Finance* 26 (5): 29–35.

Hayden, Michael Edison, and Megan Squire. 2021. "How Cryptocurrency Revolutionized the White Supremacist Movement." Southern Poverty Law Center. https://www.splcenter.org/hatewatch/2021/12/09/how-cryptocurrency-revolutionized-white-supremacist-movement.

Jofre, Maria, Alberto Aziani, and Edoardo Villa. 2022. "Terrorist Financing and the Use of Traditional and Emerging Financial Technologies." *SSRN Electronic Journal*. https://www.academia.edu/89777420/Terrorist_Financing_and_the_Use_of_Traditional_and_Emerging_Financial_Technologies.

———. 2024. "Terrorist Financing: Traditional vs. Emerging Financial Technologies." *Terrorism and Political Violence* 0 (0): 1–14. https://doi.org/10.1080/09546553.2024.2433635.

Jolley, Daniel, Rose Meleady, and Karen M. Douglas. 2020. "Exposure to Intergroup Conspiracy Theories Promotes Prejudice Which Spreads across Groups." *British Journal of Psychology* 111 (1): 17–35. https://doi.org/10.1111/bjop.12385.

Jones, Seth G. 2018. "The Rise of Far-Right Extremism in the United States." Center for Strategic and International Studies (CSIS). JSTOR. http://www.jstor.org/stable/resrep22336.

Kapsis, Ilias. 2023. "Crypto-Assets and Criminality. A Critical Review Focusing on Money Laundering and Terrorism Financing." In *Organised Crime, Financial Crime and Criminal Justice: Theoretical Concepts and Challenges*, edited by Ed Johnston, Dan Jasinski, and Amber Phillips. The Law of Financial Crime. London ; New York: Routledge, Taylor & Francis Group.

Keatinge, Tom, Florence Keen, and Kayla Izenman. 2019. "Fundraising for Right-Wing Extremist Movements: How They Raise Funds and How to Counter It." *The RUSI Journal* 164 (2): 10–23. https://doi.org/10.1080/03071847.2019.1621479.

Knight, Sarah, Katie Woodward, and Gary L. J. Lancaster. 2017. "Violent versus Nonviolent Actors: An Empirical Study of Different Types of Extremism." *Journal of Threat Assessment and Management* 4 (4): 230–48. https://doi.org/10.1037/tam0000086.

Koehler, Daniel. 2016. "Right-Wing Extremism and Terrorism in Europe: Current Developments and Issues for the Future." *PRISM* 6 (2): 84–105.

Majumder, Amit, Megnath Routh, and Dipayan Singha. 2019. "A Conceptual Study on the Emergence of Cryptocurrency Economy and Its Nexus with Terrorism Financing." In *The Impact of Global Terrorism on Economic and Political Development*, edited by Ramesh Chandra Das, 125–38. Emerald Publishing Limited. https://doi.org/10.1108/978-1-78769-919-920191012.

Reimer, Stephen, and Matthew Redhead. 2022. "Bit by Bit: Impacts of New Technologies on Terrorism Financing Risks." *RUSI Europe Occasional Paper*. https://static.rusi.org/266-OP-EU-Terrorism-Financing-New-Tech.pdf.

Salami, Iwa. 2018. "Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?" *Studies in Conflict & Terrorism* 41 (12): 968–89. https://doi.org/10.1080/1057610X.2017.1365464.

Teichmann, Fabian Maximilian Johannes. 2018. "Financing Terrorism through Cryptocurrencies – a Danger for Europe?" *Journal of Money Laundering Control* 21 (4): 513–19. https://doi.org/10.1108/JMLC-06-2017-0024.

Wang, Shacheng, and Xixi Zhu. 2021. "Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing." *Policing: A Journal of Policy and Practice* 15 (4): 2329–40. https://doi.org/10.1093/police/paab059.