Anonymity Technology in Virtual Assets:
Scope, Limitations, and Emerging Strategies

Nicholas F. Marko MD, FAANS, FACS

PUBB 763, Fall 2021

1. Introduction

One of the most significant challenges for those involved in any type of illicit trade is managing the financial flows. In recent history, managing large-scale illicit financial flows has been a costly, time-consuming, and laborious process that often involves creating numerous false businesses and false accounts across a variety of international jurisdictions, physical smuggling of distributed quanta of cash via "money mules," and complex structuring of transactions to avoid drawing attention to the illicit activities[1]. Management of financial flows is also one of the riskiest parts of illicit trade, as illicit funds are frequent targets for both internal diversion and external scrutiny. Illicit traders and law enforcement agencies alike recognize that the process of moving illicit funds renders the mover vulnerable to detection. Thus, the "money trail" remains a useful target for law enforcement agencies investigating criminal activities, and "following the money" has been the *modus operandi* for many, successful law enforcement operations. Illicit traders have recognized this for centuries, and, as their tactics have improved, law enforcement has labored to keep pace.

A new tool for elicit traders emerged in 2008 with the initial description of blockchain technology and its subsequent implementation as a distributed ledger system for virtual assets (VAs)[2]. VAs promised a form of currency free of the involvement of centralized banks that prioritized privacy, accessibility, and fungibility. As the technology became more mainstream, illicit traders seized the opportunity to begin to transact their business in cyberspace via a system where funds could be moved using virtual identities between multiple accounts in numerous physical jurisdictions, without government oversight or the need for intermediaries, and within seconds, for relatively little cost[3]. Law enforcement technologies and legislation predictably lagged, and by the beginning of this decade VAs had become a significant mechanism for financing illicit trade.

Ease of use, low cost, and widespread accessibility are necessary but not sufficient for an asset to become useful for financing illicit trade. The lynchpin in the system is anonymity.

Prior to the advent of VAs, no illicit transaction could be truly anonymous, and every transaction created an opportunity for detection and definitive identification for a member of a criminal network. The distinguishing feature of VAs that made them attractive to illicit actors was the apparent ease with which they were able to obfuscate the history of transactions and the identities of the transacting parties. However, as law enforcement tactics and technology began to catch up and as legislation targeted at VAs began to surface, the perception of the anonymity afforded by VAs began to wane. Private contractors for law enforcement surfaced with technologies capable of definitive attribution of VA transactions, and high-profile arrests were made[4]. Never fully deterred, both privacy advocates and illicit actors worked to develop more advanced systems capable of providing true anonymity, and, as authorities react, the long-enduring "cat-and-mouse" game continues.

The focus of this paper is anonymity in virtual assets. This subject is at the core of understanding the present and future of illicit financial flows, and thus it is essential knowledge for anyone studying or working to disrupt illicit trade. Specifically, this paper focuses on the evolution of the technologies that allow VAs to become pseudonymous or anonymous, the current limitations of these technologies, and the emerging trends that are moving the needle towards truly anonymous VA transactions. The discussion will be in four parts. The first section will present a brief background that includes definitions of relevant terminologies and necessary fundamental technical information on the core technologies associated with VAs. The second section will discuss the technical basis of limitations to anonymity associated with today's most popular and most prevalent VAs. The third section will illustrate strategies currently employed by both privacy advocates and illicit actors to improve anonymity and to thwart attempts at attribution of transactions with current VAs. The final section will focus on the next generation of anonymity-enhanced VAs, describing the technical approaches through which they attempt to address the inherent limitations of current VAs and the degree to which these may still be susceptible to attribution.

This paper focuses specifically on the technologies that provide pseudonymity and anonymity to the users of VAs. It is not intended as a comprehensive discussion of law enforcement tactics against illicit trade using VAs, nor does it discuss the current or future status of legislative efforts designed to regulate or constrain the scope of VA anonymity. Each of these topics could merit a similarly-comprehensive discussion on its own, and so we have

chosen to keep these outside the scope of this analysis. Ultimately, the goal of this discussion is to give readers a fundamental understanding of the technological drivers of anonymity in VAs and VA transactions, the limits and vulnerabilities of these technologies, and the strategies that have emerged to mitigate these limitations.

2. Definitions and Background

2.1. Virtual Assets. A virtual asset (VA) is defined by the Financial Asset Task Force (FATF) as, "any digital representation of value that can be digitally traded, transferred or used for payment. It does not include the digital representation of fiat currencies.[5]" Virtual assets include, but are not limited to, cryptocurrencies.

2.2. Virtual Asset Service Provider. FATF considers a virtual asset service provider (VASP) to be any person or business who conducts any of the following activities:

a) exchange between virtual assets and fiat currencies
b) exchange between one or more forms of virtual assets
c) transfer of virtual assets
d) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets
e) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset[5]

2.3. Distributed Ledgers. A ledger is a database of financial transactions. There is only one copy of a traditional ledger (as in a personal bank account), while there are multiple copies of a *distributed ledger.* A distributed ledger accessible only to its owners is said to be private, whereas a ledger that can be accessed by anyone is public. In practice, most distributed ledgers are public. All copies of a distributed ledger are maintained in an identical state through a process of consensus. If participation in this process is limited to a selected number of trusted agents, then the distributed ledger is considered to be *permissioned*. Conversely, the consensus process for an *unpermissioned* ledger is open to everyone, and therefore it has no single owner[6]. Most current virtual assets use some type of public, unpermissioned, distributed ledger.

2.4. Blockchain. In a continuous ledger, transaction entries are added sequentially as they occur. In a blockchain ledger, a group of entries are simultaneously added as a "block."

Block addition occurs periodically, with each new block "chained" to the one before. This is the most basic definition of "blockchain" – a decentralized ledger of transactions where transaction data is periodically added in blocks.

In order for a block to be added to the ledger and for all copies of the distributed ledger to update in an unpermissioned, distributed ledger system, consensus must be achieved regarding which block to add next. One example of how this process works in a digital blockchain is the "proof-of-work" method, which is used by many current virtual assets. The process begins when users of the ledger broadcast transactions to the distributed (peer-to-peer) network that is maintaining the ledger. First, public-key / private-key security is used by recipients of the broadcast to verify the validity of the transaction. Anyone on the network can receive these transactions and compile them into a block to be added next to the chain. This process is called "mining." In order to decide which miner's block is added next, the miner must perform computational work. Whichever is associated with the most computational work is accepted by consensus and is added to the chain. The "work" involves finding a number sequence (the "nonce") such that, when it is appended to the list of transactions and when this data is supplied as input

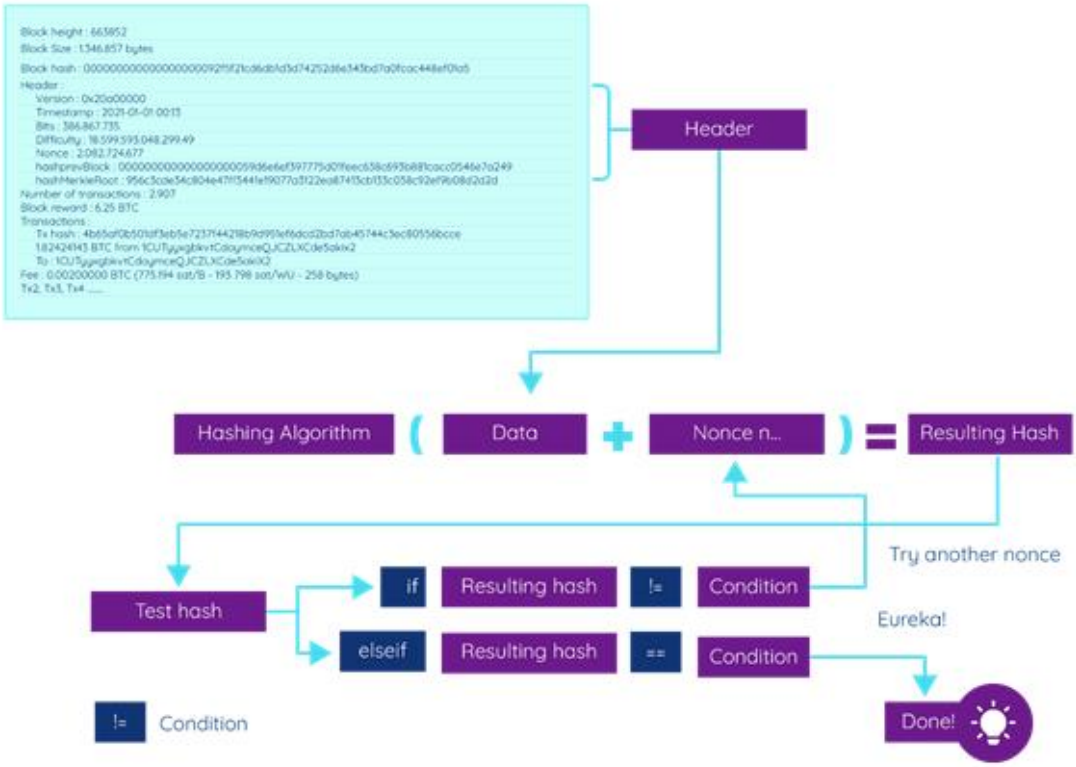

Figure 1: Blockchain Proof of Work Mining. From Centieiro [7]

to a cryptographic algorithm, a "hash" (a binary string of a set length) that begins with a specific number of zeroes is generated. Because the cryptographic function cannot be reverse-engineered, the only way to determine the correct nonce is trial and error. On average, it currently takes $8.4x10^{16}$ hashes to mine one block, and thus considerable computational "work" is done. The first miner (or pool of miners) to solve this computational problem "wins" and has their block added to the chain. Miners are incentivized to participate by receiving a reward when their block is chosen to be added. Forking in the blockchain is prevented by requiring that the hash from the previous block be included in the input to the cryptographic function[2, 7, 8].

2.5. Cryptocurrency. Cryptocurrency is a collection of binary data designed to function as a medium for exchange of value. It is "fiat" in the sense that it is not backed by any physical commodity, but it is not government issued like traditional fiat currencies. Whereas government fiat currencies derive their value from society's trust that is placed in the government, cryptocurrencies' values are based on trust in the security of their distributed ledgers. Almost all cryptocurrencies are based on blockchain distributed ledger technology, and approximately 90% of the total market capitalization of cryptocurrencies use proof-of-work consensus. The "crypto-" prefix refers to the fact that the currency's blockchain is secured via cryptographic algorithms, as described in §2.1.4. Cryptocurrencies are one type of virtual asset, but the two terms are not synonymous. Bitcoin was the first cryptocurrency and remains the best-known and the reference standard. However, as of November 2021 there were 7,557 different cryptocurrencies in existence worldwide[8, 9].

3. Limitations of the Anonymity of current Virtual Assets

3.1. Overview. There is a common misconception that any virtual asset built on blockchain technology is anonymous[10]. With the exception of some newer, anonymity-enhanced assets (see §5), this is almost universally untrue but the assumption stems from several features of blockchain-based VAs and their transactions[11]. First, there are mechanisms by which users can acquire these assets without presenting personally-identifiable information. An example is cryptocurrency mining, which generates cryptocurrency without the need for real-world identification. Many users believe that anonymous

acquisition of VAs prevents these instruments can be tied to them specifically[10]. Second, transactions for most VAs work mechanistically by completely consuming the source instrument and re-issuing two or more outputs, one to the sender and one (or more) to the recipient. This process is associated with a change in the identification number of the instrument[2, 12]. As a simplified example, if a holder of 10 bitcoin (BTC) makes a purchase for 1 BTC on a marketplace, the entire 10 BTC is consumed, the recipient gets a new instrument with a value of 1 BTC, and the sender receives "change" in the form of another new instrument with a value of 9 BTC. Many users assume that this means that the original asset[13] is now completely untraceable. Third, Darknet markets and services accessed via the TOR network are often used for illicit transactions, and many users believe that TOR makes these activities untraceable[14].

All of the aforementioned beliefs are actually misconceptions. The following sections will address each of these erroneous beliefs and illustrate how anonymity and freedom from legal consequence is not actually a feature of most, current VAs.

3.2. Attribution Strategies. Attribution refers to the ability to determine the true identity of the holder of a VA based on its transaction history. A truly anonymous VA would have no ability to be attributed; however, the pseudonymous nature of most VAs makes definitive attribution of VAs possible through both direct and indirect mechanisms. Direct attribution occurs when security failures on the part of the asset holder lead to an inadvertent connection between their true identity and the VA's pseudonym[13]. The most common source of this failure in operational security by a user occurs when they provide personal information to a cryptocurrency marketplace. Most mainstream crypto marketplaces now require users to verify their identity when creating accounts, and payments that can be traced to these accounts can therefore provide a link back to the true identity of the purchaser[15].

However, even users who take effective steps to protect true anonymity during VA acquisition can still be subject to attribution by indirect strategies. These approaches are largely based upon probabilistic analyses and pattern recognition, often involving purpose-built AI systems. The precise details of many of these methods remain trade secrets, developed and used by contractors for law enforcement and financial institutions (e.g., CipherTrace, Elliptic, Chainalysis)[8, 16]. Notwithstanding, academic literature provides

some insight into the basic operational methods of such technologies[8, 17, 18]. Pattern recognition and network analysis approaches often begin by specific public keys associated with suspicious transactions. From here, behavioral patterns can be inferred for these users, network connectivity can be determined, and open-source intelligence can also be integrated. This, in turn, may lead to identifying other transactions by the suspicious users. This information is often supplied by contractors to their law enforcement partners, who use subpoena power to deanonymize key aspects of the related transactions. This strategy was used by Chainalysis working in conjunction with law enforcement to identify the operator of the infamous "Welcome 2 video" child pornography hosting site as 23-year-old South Korean citizen Son Jung-woo. The investigation led to 337 arrests and disruption of a site that hosted in excess of 220,000 downloads of illegal videos[8, 19].

Methods for attribution are constantly evolving, and a complete discussion of every available technology is beyond the scope of this paper. More direct methods, including inserting micro-transactions to improve traceability[8], using software-defined networks[20], and manipulating data contained within blockchain-associated scripts[17] are all examples of novel approaches, and additional technologies are being developed aggressively by government and the private sector. The ultimate message is that the pseudonymity of many blockchain-based VAs opens the door to a variety of computational strategies for attribution, and more are on the horizon.

3.3. Blockchain traceability. Illicit users of VAs sometimes believe that the mechanics of the associated digital transactions render the providence of a given asset untraceable. However, because the blockchain stores data regarding all prior transactions, this belief is inaccurate. In fact, because VAs use public ledger systems, the complete transaction history is publicly available and can be explored by anyone. This, in turn, allows the data to be utilized by a growing variety of public or commercial transaction analysis tools that use pattern detection algorithms and artificial intelligence to track illicit transactions. This actually makes these instruments more traceable than many traditional financial instruments, where ledgers are often private and inaccessible even to law enforcement.

An example of this type of analysis can be generated using the publicly-available blockchain browser hosted at www.oxt.me. This software creates graphs of inflows and outflows of BTC based on a seed BTC transaction number. Supplying the identification number of an unusually-large transaction from 7 May 2019 (7074.18 BTC, $43,066,900 USD) produces the graph in Figure 2 after just a few clicks. This graph shows numer

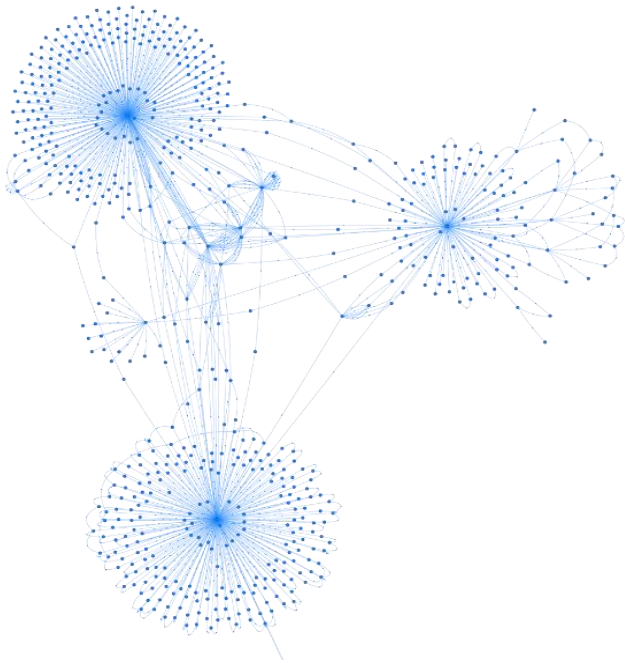

Figure 2: Binance Hack Transactions (generated using www.oxt.me)

followed by a complex web of outgoing BTC flows wherein multiple transactions, various combination and splitting steps, and ultimately dissemination into a large number of smaller outflows was used in an attempt to obfuscate both the origin and the destination of the funds. Moreover, a blockchain explorer can be used to show that the originating account had a history of over 7 million bitcoin transactions, which is clearly uncommon. This transaction is now known to be associated with the hack of the primary wallet for the cryptocurrency marketplace (VASP) , Binance[21].

In addition to being used by law enforcement in conjunction with specific criminal investigations, VA transaction tracing software is now routinely employed by many cryptocurrency marketplaces and VASPs to analyze the providence of virtual currencies attempting to be traded on their platforms. This allows them to reject individual transactions whose instruments have a high probability of being associated with prior, illicit activity. This, in turn, has led to differential valuation of "clean" versus "dirty" VAs. Holders of specific pieces of cryptocurrency that may have previously been part of an illicit transaction can have their ability to utilize the asset compromised, leading to differential valuation of individual VAs[22, 23]. This is akin to a store being able to reject a specific dollar bill because of evidence that it may have been used in prior criminal activity.

Moreover, it may cast the holder in a suspicious light. This capability fundamentally restricts the fungibility of the VA[24], which threatens the perceived value held in the entire ecosystem. This is one major reason for the emergence of technologies designed to "clean" these dirty assets and also new, anonymity-enhanced VAs that are not susceptible to the same traceability.

3.4. TOR anonymity compromise. The TOR network refers to a network of connected nodes used to route internet traffic in an anonymous fashion. The system was originally developed by the U.S. Naval Research Laboratory in the 1990s as a method for anonymous communications, but it has since been taken over and open-sourced by the TOR project[25, 26]. The TOR network is accessed via a software application called "The Onion Router," which directs internet traffic from a computer to a "guard node" (entry node). From here, traffic is routed at random across a series of relays ("middle nodes"), each of which is capable of reading only the information on the next routing but not the encrypted information being passed. Traffic may end internally on the TOR network at a "TOR hidden service" (which has no connection to the standard internet, or "Clearnet"), or it may leave the TOR network via an "exit node" to reach a Clearnet destination[27]. This architecture, as well as the privacy reputation of the TOR project, lead many users to believe that using TOR provides anonymous access to both the Darknet and the Clearnet.

It has been repeatedly demonstrated that the anonymity of TOR users can be compromised. These compromises generally fall into one of three categories. The first category includes user errors or technical deficiencies in browsers or operating systems that lead to "data leaks" that allow users to be identified. Operational examples include users voluntarily providing potentially-identifying information to websites when using TOR (account information, passwords, identifiable transactions), creating credentials that are similar to identifiable counterparts on the Clearnet, simultaneously using online services not being routed through TOR, or accessing TOR from identifiable locations to which the user can be traced[26]. Technical issues often derive from vulnerabilities in browsers or the use of various browser plugins (Captcha, PDFs, Java, cookies, or FLASH) that share data outside of the TOR network[8]. While good operational security can prevent most of these issues, this category remains the largest contributor to deanonymization of TOR users.

The second category of TOR anonymity compromise methods is compromised TOR relays. Users who seek to hijack the personal information of TOR users can create guard, relay, or exit nodes that allow them to create man-in-the-middle (MIM) attacks. This is a form of eavesdropping where the user managing the relay can view all unencrypted traffic passing over the relay. This allows private or identifiable information (account credentials, private cryptographic keys, etc.) to be intercepted and then exploited by the attacker. TOR contributor nusenu has studied this extensively[28, 29], and, as recently as 2019, found that up to 23% of TOR exit nodes were controlled by a single, malicious attacker conducting MIM attacks[28].

The third category is overt hacking of the TOR network. Much of this work has been done by US government and law enforcement agencies, and many of the details regarding the exact vulnerabilities exploited in these hacks remain classified. They are, nonetheless, well documented. In 2013 the Washington Post reported on US Government hacking of TOR that had been occurring since at least 2006[25, 30]. In 2014 the US Department of Defense collaborated with researchers at Carnegie Mellon University used a zero-day vulnerability to insert relays that modified TOR protocol headers[31] in such a way that they could simultaneously conduct both a "traffic confirmation attack" and a "Sybil attack." (complete technical details are available through TOR[32]). It is believed that this is the technology that supported the FBI/Europol Operation Onymous[33] (including the takedown of the Silk Road 2.0 Darknet market[34]) and Operation Shrouded Horizon[35]. In 2017 the FBI chose to dismiss charges against Jay Michaud, who was accused of accessing the Darknet child pornography site "Playpen," rather than to disclose the technical details of the methods that they used to compromise TOR[36]. Given all of these instances, it is believed that the U.S. government at least had (and may still have) the technical capabilities to deanonymize TOR users.

4. Mitigation Strategies

4.1. Obtaining VAs Anonymously. Most large, centralized VA exchanges require proof of identification to purchase assets, and this creates an automatic link between an individual and a specific VA. Avoiding creating this link is a critical piece of operational security

for those intending to use VAs illicitly, and so, while these are the primary means that licit users acquire VAs, they are not an option for those intent on illicit use.

There are two major scenarios for obtaining VAs anonymously in conjunction with illicit activities. *Scenario 1* involves converting cash into VAs in order to either launder the proceeds of previous illicit activity or to use the VAs to fund downstream illicit activities. Currently there are four strategies available, each with its own pros and cons[37]:

1. **Mining VAs.** This creates new VAs out of "thin air" in an anonymous fashion. This is likely the most secure method, but it takes considerable time, computational resources, and technical knowledge. For example, one of the largest and most efficient BTC mining operations in the world (Moscow, Russia) mines 600 BTC monthly (~$36M USD) with an energy cost of $120,000 per month and a large fixed hardware overhead[38]. The massive fixed energy overhead and the physical space required makes this type of operation very conspicuous, and therefore VA mining at the scale required for significant ML activities is impractical.
2. **Crypto ATMs or Kiosks.** These devices function like traditional ATMs, and deposits of cash can be made and then funds can be transferred to an anonymous VA account. Their downsides include very high transaction fees (up to 27%)[39], use of cameras by the ATMs and on-premises security, general risks of personal public exposure, and transaction limits.
3. **Local VA exchanges.** Websites, such as localbitcoins.com[40], facilitate online or in-person meetings between interested buyers and sellers of VAs. In theory this can be made anonymous by avoiding personal disclosures and maintaining anonymity through good operational security for in-person transactions. The advantage is that there is no theoretical limit to the transaction size. The downsides are the safety risks associated with illegal, in-person transactions of large sums of money.
4. **Conversion to an intermediary.** Someone holding physical cash can convert it anonymously to an intermediary instrument by using the cash to purchase prepaid credit cards, money orders, or other, similar instruments that do not require identification to purchase. These can then be used to fund online transactions through local or anonymous exchanges (as described below for scenario 2). Downsides here

include limits to the number of prepaid cards or money orders that one can purchase without raising suspicion and also the physical security (cameras, etc.) located at the point of sale.

Scenario 2 involves using an existing digital asset to purchase VAs anonymously. These types of transactions are used, for instance, when the user has already obtained a large amount of a VA (e.g., BTC paid as a ransom for a malware attack) and wishes to use it to convert it to a different VA anonymously. Here there are three options:

1. **Local VA exchanges.** These are described above and can be used for online transactions between individuals as well. The lack of most security guarantees here is a downside.
2. **Anonymous online VA brokers.** These VASPs accept digital assets (VA or other types) as payment and use this to purchase VAs anonymously, for a fee. They do not require personal identification for transactions[41]. However, conversions between certain types of VAs may still be traceable through the blockchain.
3. **Unregistered Peer-to-peer (P2P) exchangers.** These are a form of unregulated VASP and are discussed in detail in the next section.

4.2. Unregistered and Foreign Peer-to-peer (P2P) Exchangers. P2P exchangers are individuals or entities (VASPs) offering to exchange fiat currencies for VA or one VA for another. Whereas VA exchanges only facilitate meetings between individuals for subsequent person-to-person transactions, P2P exchangers actually transact the currency exchange FinCEN noted in 2019 that, "in undertaking these activities, P2P exchangers function as [Money Service Businesses] MSBs and, therefore, must comply with all requirements for MSBs under the Bank Secrecy Act.[42]" Many unregistered P2P exchanges exist on both the Clearnet and Darknet, and they do not comply with current MSB regulations in the US. More exist outside of US jurisdiction in countries with weak anti-money laundering (AML) practices, although they are technically covered under US AML laws if they transact business, "wholly or substantial part within the United States.[43]" These entities do not typically comply with KYC practices and frequently serve as intermediaries in VA laundering activities. Additionally, some employ mixing and tumbling services (described below), and others have been found to use currency mules to further obfuscate trading activities[42].

4.3. Currency Mixers and Tumblers. Mixing or Tumbling services (the terms are synonymous) are designed enhance anonymity in VA transactions by using asset mixing to breaking the connection between senders and receivers of VAs[44]. FATF defines a tumbler as, "a type of anonymizer that obscures the chain of transactions on the blockchain by linking all the transactions in the same … address and sending them together in a way that makes them look as if they were sent from another address.[45]"

In practice, this works by combining the VAs from multiple users into a single location, usually via multiple, small transactions. Once all of the currencies are mixed, this process is repeated ("tumbled") multiple times in a random fashion. Ultimately the same amount of the initial VA submitted for tumbling by the user (less a fee) is sent back to the user vial multiple transactions of random sizes at random time intervals. Because new identification numbers are created with each transaction (see §3.1), this random and iterative process makes it difficult to trace the origin of a specific VA once tumbling has occurred[44].

Most tumblers are centralized, meaning that a private entity (a VASP) collects the VAs of multiple users, conducts the tumbling, and returns the VAs back to the users. An alternate version is a decentralized tumbler, which is available specifically on blockchain platforms that support smart contracts[46]. These services function in the same fashion but without a centralized authority, requiring the users to process the tumbling themselves. The process is highly technical and is only suitable for advanced users, but it has the advantage of removing a central authority where logs may be kept[44]. CoinJoin[47] is an example of this approach, and the technology is built into advanced VA wallets, such as Samourai Wallet[48].

4.4. Avoiding Red Flags and Patterns. Traditional forensic accounting and AML work relies heavily on recognition of suspicious patterns of behavior in trades and transactions, and detecting illicit activity using VAs is fundamentally similar. Because much of the pattern recognition logic associated with commercial AML software for VA markets remains proprietary, it is impossible for illicit actors to know every possible potential indicator that may draw attention to their activities, nor is it possible to know the combinations of activities that are likely to elicit the strongest signals. Notwithstanding, FATF has published and made publicly available a list of red flags and patterns that are often

associated with illicit VA transactions based on 100 previous case studies[4], and it is safe to assume that modern AML strategies in this space detect *at least* these indicators. This publication, therefore, also provides a convenient reference for illicit actors regarding what practices to avoid or to attempt to obfuscate in the interest of evading detection.

The complete list of 58 indicators is not reproduced here for the sake of brevity, but it is readily available online[4]. In summary, the indicators involve one or more of several practices. The first category is traditional AML indicators, including multiple, frequent transactions just below reporting thresholds ("smurfing"), complex networks of transactions designed to obfuscate the flow of funds, heavy use of new accounts with large initial deposits, unclear sources of wealth, transactions that completely drain associated accounts, and transactions in geographies known to be associated with lax regulations or policing capabilities. The second category includes conspicuous use of strategies designed to enhance anonymity associated with VA transactions, including conversion of VAs with public ledgers to anonymity-enhanced VAs (see §5.1), frequent conversions between multiple different types of VAs, and transactions that occur using DNS proxies, the TOR network, and unregistered or unlicensed VASPs. The third category involves heavy or frequent use of obfuscation technologies specific to VAs, including P2P exchanges, mixing and tumbling services, and crypto-ATMs or kiosks[4].

When red flags appear, and particularly when they occur in patterns that have been learned by AI networks or previously observed in VA ML cases, they place the user at risk of detection. Knowing this, VA launderers can adopt one or both of two, general strategies. The first is pattern avoidance – minimizing the use of red flag practices or attempting to structure them in a way that will not be readily recognized by law enforcement or AI. This is a constant cat-and-mouse game between criminals and enforcement agencies. The second is to build better technologies for enhancing anonymity such that, even when patterns are detected, authorities are physically unable to extract any identifying information about the participants through hacks or exploits[49]. Once again this is a give-and-take game. Together these practices comprise the operational security of the illicit VA user.

5. Anonymity-Enhanced Cryptocurrencies

5.1. Overview. The limitations in anonymity and traceability inherent in early-generation VAs (see §3) can be mitigated (see §4) but not eliminated. The ongoing demand for VAs associated with better anonymity strategies from both licit and illicit customers has given rise to a new generation of VAs that seek to allow truly anonymous usage. These instruments have been called "anonymity-enhanced cryptocurrencies (AECs)," "privacy coins," "private coins," or "anonymous coins." Currently these VAs are limited to the cryptocurrency space and comprise products including Monero, Zcash, Verge, Beam, Grin, Dash (originally called Xcoin, then Darkcoin, then rebranded as Dash), and Pirate Chain[50]. While privacy advocates tout the benefits of a non-bank-controlled currency system that offers comprehensive privacy features, law enforcement and regulatory agencies note the increased difficulty in conducting AML and other criminal investigations when these instruments are employed. Indeed, AECs are among the fastest growing VAs traded on illicit Darknet markets[3, 51], and concerns regarding illicit use has led to the delisting of these instruments from several, large, commercial VA exchanges[52]. FinCEN summarizes the potential risks of illicit AEC use, stating, "several types of AEC are increasing in popularity and employ various technologies that inhibit investigators' ability both to identify transaction activity using blockchain data and to attribute this activity to illicit activity conducted by natural persons.[53]" This section will examine the technology that drives AECs as well as assess their claims of anonymity.

5.2. AEC Technology. AECs leverage additional cryptographic and computational technology to obfuscate transactions in order to achieve anonymity and preserve fungibility. While each AEC takes a different approach to this process, the most popular AEC, Monero, serves as a prototypic example of the category and will be discussed in detail here for illustrative purposes.

Many of the aforementioned limitations of VAs (§3) were recognized, at least in theory, within a few years of the original blockchain paper[2]. In 2013, Nicholas van Saberhagen released a whitepaper describing CryptoNote 2.0, an application-layer protocol designed to be used with cryptocurrencies in order to address the limitations[54]. The cryptography community adopted the work described by van Saberhagen into the design of a new, decentralized and open-source VA, Monero, which was deployed in

2014[55]. Monero deploys additional cryptography in three steps designed to ensure the anonymity of the sender, the recipient, and the transaction. These three domains will be discussed below. Additionally, Monero also employs additional security measures, including incorporating the Dandelion++ security protocol[56] and compatibility with TOR and I2P anonymous networks[55].

Sender privacy: Ring Signatures. A ring signature is a private key-based, digital cryptographic authentication that can be used by any member of a group to authorize a transaction (much like a joint bank account), but it is computationally infeasible to determine which of the group members' keys was used to produce the signature. When a holder of Monero digitally signs a "send" transaction, the signatures of a number of additional non-signers are also added to the group as decoys (called "mixins"). These decoys are real Monero users who previously made transactions on the system. The digital signatures of the transactor and the mixins are combined cryptographically into a unique, one-time use signature for the group as a whole, and this signature is capable of authorizing the transaction on the blockchain network. In this way, even the miners cannot determine who the true initiator of the transaction is, but they can see that the transaction is valid based on the valid group "ring" signature. This creates a form of plausible deniability for the true sender, as they are just as likely to have been pulled into the ring as a mixin as they are to have been the true initiator of the transaction. This is also why, to an outside observer, all Monero users appear to be engaging in frequent transactions, even though most of them are mixins and thus are not real. The problem of preventing double-spending is solved using a cryptographically-generated "key image" that is unique for every transaction yet not associated with the sender[55, 57, 58].

Recipient privacy: Stealth Addresses. A stealth address is a randomly-generated, one-time address that is created by the sender on behalf of the recipient when the transaction is initiated. To accomplish this cryptographically, Monero users actually have four cryptographic keys rather than two: a public spend key, a public view key, a private spend key, and a private view key. When a sender initiates a transaction, they use the recipient's public view and spend keys to generate the stealth address. Only the recipient can recognize the transaction as being destined for them by using their private view key to decrypt the one-time address. Additionally, only the recipient can, in turn, spend that

currency by using their private spend key to authorize a transfer. In this way, the transactions on the Monero blockchain all have a unique identification, but this is actually an encrypted address that can only be recognized (and later spent) via decryption by the recipient[55, 57, 58].

Transaction privacy: RingCT. RingCT is a technology implemented by Monero in 2017 that allows the actual transaction amounts to be encrypted, and thus visible to the sender and the recipient, but invisible to outside observers of the blockchain. However, miners must be able to verify that the transaction is valid by verifying that [(input) = (amount to recipient) + (change to sender) + (transaction fee)]. In order to allow the validity of this condition to be verified without knowing the actual amounts, a cryptographic function called a Pedersen commitment is used. However, it is impossible to work backwards from the output of the Pedersen commitment algorithm to the original amounts. Moreover, because of the topology of the ring signature system of sending, the miner can only (and need only) verify that some combination of the Pedersen commitment values in the ring produce a balanced equation[55, 57, 58]. The mathematical details of this are beyond the scope of this discussion, but are described elsewhere[59].

5.3. Cracking AECs. Monero claims that the combination of cryptographic methods described above make senders and recipients truly anonymous. This obviously presents a challenge to authorities, vendors, and hackers, and putative results by each of these groups have recently been reported. In August 2020, the commercial vendor, CipherTrace, announced proprietary technology capable of tracing Monero transactions[60, 61]. Weeks later, in September 2020, the IRS issued a request for proposals to break Monero's privacy, stating, "the IRS-CI is seeking a solution with one or more contractors to provide innovative solutions for tracing and attribution of privacy coins, such as expert tools, data, source code, algorithms, and software development services.[62]" Shortly thereafter the IRS awarded contracts to Chainalysis and Integra FEC[63], presumably based at least on proof-of-concept work that illustrates their ability to compromise Monero. Additionally, allegedly-verified internet leaks of internal Chainalysis slides show the company stating that, "of the cases that Chainalysis worked on in collaboration with law enforcement, we were able to provide usable leads in approximately 65% of cases involving Monero.[64]" Finally, on 5 November 2021 a Twitter user claimed to have "broken" the privacy of

Monero and released transaction IDs associated with unique IP addresses and geographic locations[65].

Law enforcement and critics of AECs take these various developments as signs that even AECs are not truly anonymous, and this seems to bode well for AML and other investigative efforts. However, all of the aforementioned announcements have been criticized by Monero supporters. First, they note that CipherTrace made bold claims, but presented no evidence[60], and they point to the fact that the IRS did not select CipherTrace as a winner of its request for proposals[66] as evidence that the CipherTrace product is ineffective. They also criticize the Chainalysis claims, noting that there is a significant difference between, "usable leads," and definitive de-anonymization[64]. Finally, the lead developer of Monero has criticized the results of the alleged Twitter hacker, claiming that their efforts were little more than a cyberattack that was too small to compromise the Monero system and was not capable of producing reliable deanonymization against anyone using standard privacy practices (TOR, VPN, etc.)[65].

In summary, the efficacy of these early attempts to compromise the most popular AEC remains unknown. Many agree that true de-anonymization of Monero will be difficult and that the most likely results will be "educated guesses" based on probability heuristics rather than a definitive breach of anonymity. From a law enforcement perspective, however, such results may prove sufficient as part of a larger and more traditional investigation targeting users attempting to employ AECs for illicit purposes. All of these caveats notwithstanding, the case of emerging AEC use shows how privacy, anonymity, illicit trade, and enforcement are currently engaged in a cyclical pursuit of the next, more advanced, and more anonymous VA.

6. Conclusions

Virtual assets have become popular financial instruments for transacting illicit trade, and the perception of anonymity associated with VAs is a major factor contributing to this popularity. This discussion illustrates that first-generation VAs (including cryptocurrencies, such as Bitcoin) are based on technology that affords pseudonymity, but not true anonymity. Law enforcement agencies have leveraged this limitation, using a combination of novel digital tools and traditional criminal investigation strategies to develop strategies for successful

attribution of VA transactions in many circumstances. Privacy advocates and illicit actors have studied these techniques and have responded with novel operational security practices (e.g., "red flag" pattern avoidance) and novel technologies (VA mixing services, unregulated P2P exchanges, etc.) that confound but do not eliminate the possibility of attribution. Recently, a second generation of VAs focused on privacy and anonymity have surfaced (AECs), and they continue to evolve towards a goal of providing truly anonymous transactions. There is some suggestion that even these AECs may be vulnerable to attribution attempts, although for now it is more likely that these tools use probability heuristics to suggest attribution rather than provide definitive identification. Regardless of the extent of vulnerability of current AECs, the quest for improved anonymity in VA transactions is likely to continue, and law enforcement agencies are now acutely aware of the challenge and are working with private partners to keep pace. As has been the rule since antiquity, the back-and-forth will likely continue as illicit trade moves onward in the 21st century.

REFERENCES

1. Shelley, L.I., *Dark commerce : how a new illicit economy is threatening our future*. 2018, Princeton, New Jersey: Princeton University Press. xiii, 357 pages.
2. Nakamoto, S. *Bitcoin: A peer-to-peer electronic cash system*. 2008; Available from: https://bitcoin.org/bitcoin.pdf.
3. McSweeney, M. *Bitcoin is still the crypto of choice for darknet marketplaces*. The Block Research 2020; Available from: https://www.theblockcrypto.com/linked/74384/bitcoin-darknet-markets-choice.
4. FATF. *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*. 2020; Available from: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf.
5. FATF. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations*. 2012; Available from: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.
6. *Distributed Ledger Technology: beyond block chain*. UK Government office for Science 2016; Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.
7. Centieiro, H. *Bitcoin Proof of Work — The Only Article You Will Ever Have to Read*. LevelUp Coding 2021; Available from: https://levelup.gitconnected.com/bitcoin-proof-of-work-the-only-article-you-will-ever-have-to-read-4a1fcd76a294.
8. Irwin, A. and A. Turner. *Illicit Bitcoin transactions: challenges in getting to the who, what, when and where*. Emerald Insights 2018; Available from: https://www-emerald-com.mutex.gmu.edu/insight/content/doi/10.1108/JMLC-07-2017-0031/full/pdf.
9. *Number of Cryptocurrencies Worldwide*. Statista 2021; Available from: https://www.statista.com/statistics/863917/number-crypto-coins-tokens/.
10. Orcutt, M. *Criminals thought bitcoin was the perfect hiding place, but they thought wrong*. Technology Review 2017; Available from: https://www.technologyreview.com/2017/09/11/149211/criminals-thought-bitcoin-was-the-perfect-hiding-place-they-thought-wrong/.
11. *Privacy*. Bitcoin Wiki 2021; Available from: https://en.bitcoin.it/wiki/Privacy.
12. *How do BItcoin transactions work?* 2021; Available from: https://www.bitcoin.com/get-started/how-bitcoin-transactions-work/.
13. *Protect your privacy*. Bitcoin.org 2021; Available from: https://bitcoin.org/en/protect-your-privacy.
14. Redman, J. *'You Are Not Anonymous on Tor' - Study Shows Privacy Network Offers Superficial Anonymity*. Bitcoin.com 2021; Available from: https://news.bitcoin.com/you-are-not-anonymous-on-tor-study-shows-privacy-network-offers-superficial-anonymity/.
15. McGraw, J. *Dirty Crypto Takedown: How Gov'ts Deanonymize Crypto Transactions to Fight Crime*. 2020; Available from: https://beincrypto.com/dirty-crypto-takedown-how-govts-deanonymize-crypto-transactions-to-fight-crime/.

16. Brown, D. *Tracking stolen crypto is a booming business: How blockchain sleuths recover digital loot*. Washington Post 2021; Available from: https://www.washingtonpost.com/technology/2021/09/22/stolen-crypto/.
17. Christodoulou, K. and E. Iosif. *Identity Discovery in Bitcoin Blockchain: Leveraging Transactions Metadata via* International Conference on Vision, Image and Signal Processing 2019; Available from: https://dl-acm-org.mutex.gmu.edu/doi/pdf/10.1145/3387168.3387212.
18. Biryukov, A. and S. Tikhomirov. *Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis*. in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. 2019.
19. *Dark web child abuse: Hundrreds arested across 38 countries*. BBC News 2019; Available from: https://www.bbc.com/news/world-50073092.
20. Wallace, V. and S. Scott-Hayward. *Can SDN deanonymize Bitcoin users?* in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*. 2020.
21. Valinsky, J. *Hackers steal $40 million worth of bitcoin in massive security breach*. CNN 2019; Available from: https://www.cnn.com/2019/05/08/tech/bitcoin-binance-hack/index.html.
22. Demchuk, S. *Dirty Bitcoins: How to Conduct an Anti-Money Laundering Check on Your Crypto*. 2021; Available from: https://beincrypto.com/dirty-bitcoins-how-to-conduct-an-anti-money-laundering-check-on-your-crypto/.
23. Korin, N. *Are your bitcoins clean or dirty?* 2021; Available from: https://www.orbs.com/are-your-bitcoins-clean-or-dirty/.
24. Birch, D. *You cant launder bitcoins!* Forbes 2021; Available from: https://www.forbes.com/sites/davidbirch/2021/02/28/you-cant-launder-bitcoins/.
25. Gellman, B., C. Timberg, and S. Rich. *Secret NSA documents show campaign against Tor encrypted network*. The Washington Post 2013; Available from: https://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story.html.
26. *The Tor Project*. 2021; Available from: https://www.torproject.org/.
27. *Defending Against the Malicious Use of the Tor Network*. 2021; Available from: https://www.cyber.gov.au/acsc/view-all-content/publications/defending-against-malicious-use-tor-network.
28. nusenu. *How Malicious Tor Relays are Exploiting Users in 2020 (Part I)*. 2020; Available from: https://nusenu.medium.com/how-malicious-tor-relays-are-exploiting-users-in-2020-part-i-1097575c0cac.
29. nusenu. *The Growing Problem of Malicious Relays on the Tor Network*. 2019; Available from: https://nusenu.medium.com/the-growing-problem-of-malicious-relays-on-the-tor-network-2f14198af548.
30. *Is TOR trustworthy and safe?* Restore Privacy 2019; Available from: https://restoreprivacy.com/tor/.
31. Hill, K. *The attack that broke the Dark Web—and how Tor plans to fix it*. Forbes 2015; Available from: https://www.forbes.com/sites/kashmirhill/2014/11/07/how-did-law-enforcement-break-tor/?sh=4a7fa4b54bf7.

32. *Tor security advisory: "relay early" traffic confirmation attack*. TOR Blog 2014; Available from: https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack/.
33. EUROPOL. *Operation Onymous*. 2014; Available from: https://www.europol.europa.eu/activities-services/europol-in-action/operations/operation-onymous.
34. Goodin, D. *Did feds mount a sustained attack on Tor to decloak crime suspects?* Ars Technica 2015; Available from: https://arstechnica.com/tech-policy/2015/01/did-feds-mount-a-sustained-attack-on-tor-to-decloak-crime-suspects/.
35. FBI. *Cyber Criminal Forum Takedown: Operation Shrouded Horizon*. 2015; Available from: https://www.fbi.gov/news/stories/cyber-criminal-forum-taken-down.
36. Newman, L. *The Feds Would Rather Drop a Child Porn Case Than Give Up a Tor Exploit*. Wired.com 2017; Available from: https://www.wired.com/2017/03/feds-rather-drop-child-porn-case-give-exploit/.
37. *How to Anonymously Buy Bitcoin Online and in Person*. Bitcoin.com 2021; Available from: https://news.bitcoin.com/how-to-anonymously-buy-bitcoin/.
38. *Largest Bitcoin Mining Farms in the World*. Sunbird 2021; Available from: https://www.sunbirddcim.com/blog/largest-bitcoin-mining-farms-world.
39. *Buy Fee Size at Bitcoin ATMs*. Coin ATM Radar 2021; Available from: https://coinatmradar.com/charts/buy-fees/.
40. *LocalBitcoins*. 2021; Available from: https://www.localbitcoins.com.
41. *Bisq.com*. 2021; Available from: https://www.bisq.com.
42. Network, F.C.E., *Advisory on Illicit Activity Involving Convertible Virtual Currency*. 2019, United States Department of the Treasury.
43. FinCEN. *FinCEN Guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*. 2013; Available from: https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.
44. Hanif, H. *Cryptocurrency Tumblers: A headache for regulators?* Altcoin magazine 2019; Available from: https://medium.com/the-capital/cryptocurrency-tumblers-a-headache-for-regulators-d6a7e0ab5e3b.
45. FATF. *Virtual Currencies Key Definitions and Potential AML/CFT Risks*. 2014; Available from: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.
46. *What are smart contracts on blockchain*. IBM 2021; Available from: https://www.ibm.com/topics/smart-contracts.
47. *CoinJoin*. 2021; Available from: https://en.bitcoin.it/wiki/CoinJoin#:~:text=From%20Bitcoin%20Wiki,paid%20which%20recipient%20or%20recipients.
48. *Whirlpool*. Samourai Wallet 2021; Available from: https://samouraiwallet.com/whirlpool.
49. Narayanan, A. and M. Moser. *Obfuscation in Bitcoin: Techniques and Politics*. International Workshop on Obfuscation: Science, Technology, and Theory 2017 2017; Available from: https://arxiv.org/abs/1706.05432.
50. Farooque, F. *The 7 Best Cryptos to Buy for Privacy*. NASDAQ 2012; Available from: https://www.nasdaq.com/articles/the-7-best-cryptos-to-buy-for-privacy-2021-06-07.
51. Murphy, H. *Monero emerges as crypto of choice for cybercriminals*. Financial Times 2021; Available from: https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6.

52. Graffeo, E. *XRP delisted on more platforms following SEC's Ripple complaint*. 2020; Available from: https://markets.businessinsider.com/news/currencies/xrp-delisted-ripple-sec-complaint-coinbase-crypto-okcoin-trading-platform-2020-12.
53. *Federal Register Vol 85, No 247*. 2020; Available from: https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28437.pdf.
54. vanSaberhagen, N. *CryptoNote v 2.0*. 2013; Available from: https://bytecoin.org/old/whitepaper.pdf.
55. *getmonero.org*. Monero 2021; Available from: https://www.getmonero.org/.
56. Fanti, G., et al. *Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees*. Sigmetrics 2018 Emerging Areas Section 2018; Available from: https://dl.acm.org/doi/pdf/10.1145/3292040.3219620.
57. Rosic, A. *What is Monero? [The Most Comprehensive Step-by-Step Guide]*. Blockgeeks 2020; Available from: https://blockgeeks.com/guides/monero/.
58. Nuzzi, L. *Monero Becomes Bulletproof*. Digital Asset Research 2018; Available from: https://medium.com/digitalassetresearch/monero-becomes-bulletproof-f98c6408babf.
59. *Monero*. Delfr 2018; Available from: https://delfr.com/category/monero/.
60. *Ciphertrace Allegedly Builds Monero-Tracing Tools, XMR Proponents Disagree*. Bitcoin.com 2020; Available from: https://news.bitcoin.com/ciphertace-allegedly-builds-monero-tracing-tools-xmr-proponents-disagree/.
61. *CipherTrace Announces World's First Monero Tracing Capabilities for Law Enforcement, Government, and Virtual Asset Service Providers*. 2020; Available from: https://ciphertrace.com/ciphertrace-announces-worlds-first-monero-tracing-capabilities/?utm_content=138708196&utm_medium=social&utm_source=twitter&hss_channel=tw-3972254294.
62. *Request for Proposal 2032H8-20-R-00500*. IRS 2020; Available from: https://sam.gov/api/prod/opps/v3/opportunities/resources/files/bb0247a3accc46beb2901af74b78438d/download?&status=archived&token=.
63. *Pilot IRS Request for Proposal Cryptocurrency Tracing: FBO Award Notice*. 2020; Available from: https://sam.gov/api/prod/opps/v3/opportunities/resources/files/16d2a490eeb2481b971a5fe521c94c32/download?&status=archived&token=.
64. Nelson, D. and M. Hochstein. *Leaked Slides Show How Chainalysis Flags Crypto Suspects for Cops*. CoinDesk 2021; Available from: https://www.coindesk.com/business/2021/09/21/leaked-slides-show-how-chainalysis-flags-crypto-suspects-for-cops/.
65. Mollen, F. *Yes, Monero Was Attacked: But It Was Not "Broken"*. CryptoPotato 2021; Available from: https://cryptopotato.com/monero-xmr-sybil-attack-not-broken/.
66. Prius, B. *Open sesame: Will 'cracking' Monero reveal treasure or fool's gold?* 2020; Available from: https://cointelegraph.com/news/open-sesame-will-cracking-monero-reveal-treasure-or-fool-s-gold.