Article

Journal of Contemporary Criminal Justice
1–17

DOI: 10.1177/10439862231158004
journals.sagepub.com/home/ccj
SAGE

An Assessment of Cryptomixing Services in Online Illicit Markets

Thomas J. Holt[1], Jin R. Lee[2], and Elizabeth Griffith[1]

Abstract

The internet has become a popular marketplace for the sale of illicit products, including stolen personal information, drugs, and firearms. Many of these products are acquired using cryptocurrencies, which are generally defined as forms of digital currency that is traceable through blockchain ledger technology. These currencies are thought to be more secure than other forms of digital payment, though law enforcement and financial service providers have found ways to investigate account holders and their transactions. Consequently, several service providers have begun to offer cryptomixing services, which effectively launders payments to circumvent detection and investigation tools. Few have explored the practices of cryptomixing services, or the ways in which they are marketed on the Open and Dark Web. This inductive qualitative analysis will examine a sample of 18 cryptomixing services advertised on both the Open and Dark Web to better understand cryptomixing and its role in facilitating illicit transactions across the internet.

Keywords

cryptomixing, cryptocurrency, cybercrime, online illicit markets, Open and Dark Web

Research exploring the operations of online illicit markets has grown substantially over the last two decades (Hutchings & Holt, 2017; Tzanetakis et al., 2016). There has been particular emphasis among researchers on economically motivated offenses,

[1]Michigan State University, East Lansing, USA
[2]George Mason University, Fairfax, VA, USA

Corresponding Author:
Thomas J. Holt, School of Criminal Justice, Michigan State University, 655 Auditorium Road, 434 Baker Hall, East Lansing, MI 48825, USA.
Email: holtt@msu.edu

including the sale of stolen credit card data (Holt & Lampke, 2010; Hutchings & Holt, 2015) and cybercrime-as-service tools (Holt et al., 2022; Hutchings & Clayton, 2016; Leukfeldt et al., 2017). Over the last decade, research has grown considering the practices of illicit online markets selling various physical products, including drugs (Aldridge & Askew, 2017; Demant et al., 2018; Munksgaard & Tzanetakis, 2022), firearms (Copeland et al., 2020; Holt & Lee, 2022a; Lee et al., 2022), and passports (Holt & Lee, 2022b).

These studies illustrate the critical role and impact online payment platforms have in the completion of illicit economic exchanges through online markets. Research has documented the unique transitions observed in payment platforms used by cybercriminals over time (Holt et al., 2016; Kruisbergen et al., 2019; Trautman, 2014). Digital currency platforms such as e-gold were initially serviced in the mid-2000s by individuals who sought to open payment accounts and convert traditional currencies into separately valued currency (Holt et al., 2016). This system was eventually supplanted by other platforms such as Liberty Reserve and WebMoney, which were frequently serviced by hackers and other cybercriminals (Holt & Lampke, 2010; Hutchings & Holt, 2015; Trautman, 2014). Both the frequency and visibility with which these platforms were used in illicit online economies eventually led to their takedown by law enforcement agencies (Hutchings & Holt, 2017; Trautman, 2014).

Over the last decade, the rise and emergence of cryptocurrencies like Bitcoin have once again changed the way online economic transactions occur. Cryptocurrencies operate through blockchain technology, which logs transaction details between participants in a publicly accessible, verifiable, but de-identified manner (Fanusie & Robinson, 2018; Martin, 2014). While this system enables users to follow the path of payment between two parties, they are unable to connect the account holders with an offline identity. The anonymity afforded by these payment systems has led to their common use by actors in all manner of illicit markets to acquire goods and services (Aldridge & Askew, 2017; Copeland et al., 2020; Kruisbergen et al., 2019).

Given cryptocurrency's increased visibility among cybercriminals, both law enforcement and industry stakeholders have developed tools to better trace the accounts (also known as "wallets") associated with a given vendor or customer (Goldsmith et al., 2020; Zagaris, 2021). As these tools improve the capacity of agencies to investigate cryptocurrency-related crimes, new services have emerged to minimize these risks (Desmond et al., 2019; Goldsmith et al., 2020; Zagaris, 2021). Specifically, a new form of money laundering has emerged to obfuscate the paths of transactions, which is colloquially known as cryptomixing (Fanusie & Robinson, 2018; Pakki et al., 2021). Cryptomixing services enable individuals to obscure cryptocurrency transactions by sending different currencies to a designated account.

Despite its frequent use and employment within the online illicit marketplace, limited research has explored the practices of cryptomixing services, or the ways in which they are marketed by online illicit vendors (see Desmond et al., 2019; Fanusie & Robinson, 2018). While accurate estimates of its scale, cost, and consequences are limited, money laundering through cryptocurrency is a burgeoning problem that needs further research. Such insights are essential for law enforcement, anti-money

laundering professionals, and financial providers seeking to develop robust detection, prevention, and mitigation strategies. Given this gap in the literature, the current study examined a sample of 18 cryptomixing services hosted on both the Open and Dark Web to better understand its role in facilitating online illicit transactions. The findings of this inductive qualitative analysis provide direction for criminological theory and intervention by service providers, financial regulators, and law enforcement.

Money Laundering and Cryptocurrency

Money laundering is generally understood as the process of moving illegally acquired funds into the traditional financial system (Villanyi, 2021). Common examples of illegally acquired funds include proceeds from an illicit drug sale, payment for an illegal service, or even stolen cash itself (Villanyi, 2021). Several methods can be employed to redirect illegally acquired funds into the traditional financial system so that it can be used without raising suspicion. Smaller amounts may be spent directly with little concern of suspicious activity given its monetary value and size. However, for larger amounts, there is a somewhat consistent process of rerouting the funds to obfuscate the path of movement. The first step in the money laundering process is placement, which involves the illegally acquired funds being carefully brought into the traditional financial system. Common methods for placement involve depositing the money in several smaller transactions and from as many different people as possible. Identities may even be stolen to place the money into the financial system. The objective of this first step is to ensure the funds are brought into the traditional financial system without raising suspicion or concern.

The next step in the process involves layering the funds, which often involves wiring the funds through several foreign countries and shell companies owned by other organizations. In essence, a massive network of individuals are transferring money in a way that only the perpetrator can keep track and follow. The final step in the money laundering process is the integration stage, which is where the money is used to fund legal transactions. The source of where the funds originated from is often falsely reported to conceal the truth. For example, the money launderer may own a restaurant or bar and report the funds as being cash left by customers over time (Brenig et al., 2015). After integration, the proceeds can be spent on any usual transaction such as purchasing real estate or making other financial investments.

A new and recent development in money laundering has been the mixing of cryptocurrencies (Pakki et al., 2021; Rysin & Rysin, 2020). Cryptocurrencies are based on blockchain technology where every individual verifies that a transaction has occurred rather than that determination being made by a central authority such as a bank or financial institution (Campbell-Verduyn, 2018). Moving away from centralization means that financial transactions are published with only individuals' wallet numbers (e.g., account numbers) and not with the real names or offline identities of the individuals involved.

Given its added layer of anonymity, cryptocurrencies have become a popular choice to replace bank wire transactions, which are subject to money laundering investigation

in many countries, or physical transfer of cash or valuable goods, which is both expensive and time-consuming (Brenig et al., 2015; Rysin & Rysin, 2020). In fact, researchers have noted the rise of cryptocurrencies as a form of payment for various illicit goods and services sold online (e.g., Aldridge & Askew, 2017; Copeland et al., 2020; Holt & Lee, 2022b). The only prevention mechanism available is at the level of the exchange, where individuals convert traditional offline currency (e.g., dollars) into cryptocurrency or vice versa. Once the exchange is accomplished, financial transactions can be difficult to trace and can take significantly more effort to follow the money than it takes to launder it (Desmond et al., 2019).

The unique features of cryptocurrency can provide additional incentives for individuals interested in laundering money. For example, the global accessibility and speed of cryptocurrency transactions provide individuals with a faster and more efficient way to move funds compared with a traditional wire transfer or traveling in-person with cash (Brenig et al., 2015). The main hindrances for money launderers using cryptocurrency are its limited uses for purchases among the general public (i.e., few offline shops and vendors accept payment in cryptocurrency) and the volatility of its worth and value (Rysin & Rysin, 2020). These factors are important for launderers to consider as their objective is to have a spendable amount that is as close as possible to what they initially started with.

These factors have led cryptomixers to become a useful resource for criminals who employ cryptocurrencies. Cryptomixers typically begin when a customer sends a specific amount of cryptocurrency to a service provider's cryptowallet with directions to what third-party wallet it should be sent to (Fanusie & Robinson, 2018; Robinson, 2020). The cryptomixing service provider then inserts that currency into a larger pool of cryptocurrency they own. Finally, the service provider transfers the amount specified by the customer to the designated third party and retains a small percentage of the amount as fee for their involvement (Fanusie & Robinson, 2018). This process obfuscates the original source of the transfer, as the funds appear to come from a different originating wallet (Robinson, 2020).

Though preventing money laundering activities involving cryptocurrencies has been difficult for various stakeholders, particularly law enforcement and financial organizations, several methods have been developed to identify cryptocurrency transactions that may be connected to money laundering schemes. For one, the use of machine learning tools to analyze large volumes of cryptocurrency transactions has allowed for some forward movement in this space (Hu et al., 2019; Pakki et al., 2021). Global regulatory bodies have also identified strategies to detect money laundering and other problematic uses of cryptocurrencies which can be implemented by partner nations (FATF, 2020; Rysin & Rysin, 2020). Nation-state entities, such as The U.S. Department of Treasury, have also become more familiar with the technologies involved in laundering cryptocurrencies, as seen in their new rules requiring cryptocurrency exchanges to have the same level of identification available for customers as centralized banks in case of an investigation (Financial Crimes Enforcement Network, 2020). In addition, U.S. law requires individuals to report their cryptocurrency buying and selling activities to the Internal Revenue Service when filing their annual income

tax (Vega, 2022). Additional regulatory proposals in the United States involve updating the Bank Secrecy Act and other anti-money laundering provisions to require the reporting of large transactions and the identification of involved participants whenever possible.

Although progress in research and regulation is being made in this burgeoning area (e.g., Pakki et al., 2021), some argue that cryptocurrency users will continue to develop innovative ways to circumvent existing regulation (Rysin & Rysin, 2020). In turn, this will escalate the number of regulatory procedures that will be symbolically followed until the regulation is more complicated and costly than the crimes being prevented (Dupuis & Gleason, 2020). Although some have claimed great success in identifying money laundering transactions, the continually growing transaction volume has prevented any reliable identification of how many cryptocurrency transactions may be considered money laundering.

There is also an absence of widely agreed-upon estimates of the scope and scale of the problem. Cryptocurrency supporters are eager to note that only a fraction of total money laundering incidents involves cryptocurrency. In fact, of the US$2 trillion laundered each year, only around US$8 to US$10 billion are reported as having involved cryptocurrency (Chainalysis, 2022). While this amount is still concerning, more research exploring money laundering behaviors involving cryptocurrency is needed to develop comprehensive prevention and intervention strategies (Pakki et al., 2021).

Present Study

The limited body of research on the practices of cryptomixing services requires deeper investigation to better understand how illegal activities may be disrupted. The current study attempted to address these issues through an exploration of 18 cryptomixing service providers operating on both the Open and Dark Web. This qualitative study considered the ways in which cryptomixing services are advertised to customers to understand the ways in which vendors operate their services. The findings generated from this analysis will be used to identify potential disruption strategies to affect the illicit operations of both money launderers and cybercriminals.

Data and Methods

The current study utilized a sample of 18 shops offering cryptomixing services on the Open ($n = 3$) and Dark Web ($n = 15$) between 2018 and 2020 (see Table 1 for detail). Data collection ensued for 18 months (August 2018–February 2020) to capture an overall range of cryptomixing services (see also Holt & Lee, 2022b; Hutchings & Holt, 2015). Sites were identified using keywords on both Open and Dark Web search engines, including phrases such as "cryptocurrency mixer service." The research team also examined various Dark Web indexes, such as the Hidden Wiki, to identify online vendors that had been observed in the past (Copeland et al., 2020; Flamand & Décary-Hétu, 2019). As such, the current study provides a purposive sample of various online environments where individuals can purchase and acquire cryptomixing services.

Table 1. Descriptive Information.

Vendor identification	Hosting location
1	Dark Web
2	Dark Web
3	Dark Web
4	Open Web
5	Dark Web
6	Open Web
7	Dark Web
8	Dark Web
9	Dark Web
10	Dark Web
11	Dark Web
12	Open Web
13	Dark Web
14	Dark Web
15	Dark Web
16	Dark Web
17	Dark Web
18	Dark Web

To generate the data for this analysis, the contents from each site were saved as HyperText Markup Language (HTML) files for subsequent examination. All text and images from these HTML files were then read and coded by hand to assess the practices of both vendors and their customers (see also Aldridge & Askew, 2017; Copeland et al., 2020; Hutchings & Holt, 2015). The three-step coding process of open, axial, and selective coding used in grounded theory analysis was applied in the current analysis (see Corbin & Strauss, 1990), which mirrors prior cybercrime-focused qualitative studies (e.g., Blevins & Holt, 2009; Holt & Lampke, 2010). This analysis focused on information provided directly by vendors on both their websites and customer interfaces to better understand cryptomixing and its role in facilitating online illicit transactions. Specifically, the researchers examined all details provided by vendors as to their process for "mixing" or concealing cryptocurrency transactions, as well as any fees noted for their services. Comments regarding customer privacy or vendors' awareness of regulation (e.g., compliance with existing financial regulations and criminal laws) were also explored.

Findings

Four concepts related to cryptomixing as a facilitator for online illicit transactions emerged from the data: (a) the benefits of cryptomixing, (b) the mixing process, (c) vendor legitimacy, and (d) the costs and procedures of mixing. Direct quotes were presented with all spelling and grammar intact where appropriate. Similar to previous studies exploring online illicit market operations, all vendors in the current study were

assigned pseudonyms to ensure anonymity (see Aldridge & Décary-Hétu, 2016; Holt & Lampke, 2010; Hutchings & Holt, 2015).

The Benefits of Cryptomixing

Several cryptomixing services couched the benefits of using their platform in the notion of protecting individuals' anonymity. For instance, Vendor 4 stated that their service "helps you to obfuscate your Bitcoin (BTC) transactions using unique algorithms and to secure your identity. Trusted crypto mixer dissociates your identity from your transactions by adding an extra layer of privacy." Similarly, Vendor 3 stated:

> A very impressive service if you want to maintain your anonymity when you make purchases online. It can also be useful if you want to do p2p [Peer-To-Peer] payments and donations. The service is used to mix a person's funds and give this person some fresh bitcoins. The focus here is on making sure that the blender has the ability to confuse the trail as somebody could try to figure out the source. The best mixer is that one that keeps your anonymity at a max. You want each bitcoin transaction to be very hard to trace. This is where using our bitcoin mixing service makes a lot of sense. Protect your income and personal information becomes much easier. The reason why you want to use our service is because you want to hide your coins from hackers and third-parties. They can do a blockchain analysis, they may be able to track your personal data to steal your bitcoins. With our bitcoin tumbler, you don't have to worry about that anymore.

The use of cryptomixing services to evade tracking tools and financial regulation was emphasized by several vendors. For instance, Vendor 17 used similar phrasing, stating:

> The main purpose of our Service is protect your transactions of cryptocurrencies from bad guys . . . We offer our clients best privacy they can get from mixer and they can stop bothering about possible ways to identify source of funds after using of our service . . . our main goal is make you as much anonymous as possible while using cryptocurrencies . . . We proudly can say that ChainAnalysis can't analyse our transactions and find real source of funds.

Vendor 11 similarly stated: "Mixer helps you make your Cryptos unidentifiable and, thus, allows you to rest easy knowing that neither crypto-hackers nor security agencies can keep track of your financial activities." Vendor 18 specifically noted the ability of their services to bypass legal regulations related to cryptocurrencies:

> Launder your Bitcoins without any fees, all we charge is the network fee we pay to bitcoins miners. For mixing your Bitcoins, or washing them, it is best to use a Tor hidden service like [Vendor 18] because all mixers operating a clearnet website, including [name removed], are subject to government control. And with more and more exchanges and other services following AML [Anti-Money Laundering] and KYC [Know Your Customer] policies, its getting really hard to stay anonymous to government agencys [SIC] when dealing with bitcoins . . . no one knows who we are, we do not have to follow any AML and KYC policies, so we cannot be forced to give out any of our users information.

Though multiple vendors noted the benefits of using their services to circumvent tracing and legal risks, they also indicated that their operations were legal. For example, Vendor 1 stated: "there are no laws against mixing bitcoins and it is actually encouraged to always mix your bitcoins from many privacy advocates. For extra privacy use TOR and use our onion [Dark Web] btc mixer."

The Mixing Process

The ways in which cryptomixing vendors operated their services were explained somewhat consistently across vendors' advertisements. For instance, two vendors noted that they provided customers with newly mined cryptocurrencies rather than moving coins across existing accounts. For instance, Vendor 1 stated:

> If you want to hide your spending habits and how much Bitcoin you control, it is recommended to always mix or blend your bitcoins with [Vendor 1]. We have a rotating supply of fresh bitcoins daily and can usually swap up to around 50 bitcoins per transaction.

Similarly, Vendor 13 wrote:

> With us you can buy freshly mined new virgin bitcoins. Simply buy them in our shop and 12-24 hours later we will transfer them to the addresses you give us at checkout. You can give us as many bitcoin addresses as you want, and tell us how much bitcoins you want on each of them. We will mine the coins directly to your addresses, which means the input will be a coinbase [a primary cryptocurrency exchange] transaction from a [cryptocurrency] miner!.

Freshly mined Bitcoins, also known as "Virgin Bitcoins," are untainted cryptocurrencies that have not been used in any transaction. This means they have no previous transaction history linked to it on the blockchain ledger. Since newly mined coins are void of any prior transaction history, there is less risk for users who are concerned that their cryptocurrency may be associated with both unknown and/or unwanted transactions (Stevens, 2022). In other words, not having a prior record means there is enhanced privacy and confidence with its employment and ownership. Given these affordances, freshly mined cryptocurrencies are highly favored within the cryptocurrency marketplace. In fact, fresh coins are often traded at higher costs with mark ups between 10% and 30% across different cryptocurrency markets (see Vertex Marketplace, 2019).

Vendors who used preexisting pools of cryptocurrency to mix customers' funds had different processes. This was explained clearly in an advertisement from Vendor 11 that stated:

> Your Cryptos will go through a process with three steps
>
> Step 1: Assigning coins to a Pool.
>
> We use three different pools (STANDARD POOL, SMART POOL, and STEALTH POOL) with cryptocurrencies of different combinations of sources. You can assign

> your cryptocurrencies to one of the three pools with setting the mixing strength to the respective range. The higher the strength the cleaner the cryptocurrencies inside the pool.
>
> Step 2: Mixing in the Pool.
>
> After your cryptocurrencies have been assigned to a pool, they will be mixed with other cryptocurrencies from the sources mentioned above. In doing so, [Vendor 11] breaks all connections between the real sender and the receiver. In the end, you get coins that are not traceable to you.
>
> Step 3: Sending out the Coins to the Provided Receiver Address.
> After making your cryptocurrencies anonymous using our mixing process, we send it to the receiver addresses you provide. You are at liberty to provide a receiver address of any person or company you want to pay, or you can provide your personal addresses if your concern is to clear the history of your cryptocurrency transactions.
>
> Customers were, however, required to carefully manage their account details and information to minimize the risk of error or financial loss.

Vendor Legitimacy

A portion of vendors also made claims regarding their ability to be trusted with large sums of money. For instance, Vendor 11 stated:

> We do not profit by running away with your coins but by rather running longer in the business. If you feel insecure sending large amount of coins, you have the choice of sending money over a longer period of time in a number of transactions instead. The code within the mixer ensure your coins are never mixed with your own coin and sent back. This ensures security, transparency and anonymity.

Similarly, Vendor 6 stated: "you can mix small coins portions if you have any doubts, to ensure step by step that everything is crystal clear. Our mixed code guarantees that your past coins will not be mixed with the new ones." Several vendors also noted that they had large reserves of cryptocurrencies that could be validated on the blockchain to reinforce their legitimacy. For instance, Vendor 2 wrote: "The fact that we hold over 5000 BTC should stand testimony to the amount of skin we have in the game. Our reserves are publicly proven on [website name removed]."

In addition, virtually all vendors noted that they did not retain customer logs of transactions. For example, Vendor 9 wrote: "we do not store any logs so we cannot help any organization or individual with their questions about users activity. We do this for system storage optimisation and for users anonymity." Despite these claims, there was some inherent risk of detection depending on where the cryptomixing service was advertised. Specifically, sites operating on the Open Web could be subject to requests for server logs from law enforcement. Dark Web vendors, however, cannot be

forced to provide this information as they operate on a different portion of the internet. This was explained in detail by Vendor 2:

> The Clearnet bitcoin tumblers and mixer KEEP LOGS. They are forced to keep laws by law enforcement. Because the websites on the clear net have domain names ending in .com, .net, .org, .eu, they have a public whois record and hosting IPs . . . Law enforcement gets a subpoena and pay the company a visit, as well as to the hosting company, asking for access to the server and logs to track the criminal who cleaned bitcoin through their service. If the company refuses to give logs, or if the company doesn't keep logs, law enforcement can accuse them of accessory to the crime that the criminal is doing, and can charge them with obstruction of justice and other legal accusations. Law enforcement can even close the company that runs the bitcoin mixer if they don't keep logs and don't help with tracking criminals . . . All clean net bitcoin mixers ARE NOT SAFE and can be tracked down to their owners, and the owners will give information about the users to save their asses . . . Always use bitcoins mixers on the dark web. Try our mixer. If you don't like it use another mixer on the dark web. But always on dark web. And it not ok if a bitcoin on the dark web has also an address on clear net. Police can find them with the clear net address and ask about their dark web site and ask for logs.

This language explicitly conveys the risk customers may face when using Open Web cryptomixing services, which may not be evident to all users. As such, there may be greater value in the use of Dark Web cryptomixing services for those who are particularly concerned about their safety and preserving anonymity.

Costs and Procedures of Mixing

The fee structure for employing cryptomixing services was variable with multiple vendors conditioning the price based on the total amount mixed. For instance, Vendor 9 charged .05% of the total for mixing smaller amounts. Another vendor had a fee structure dependent on the total transaction. For instance, Vendor 14 explained:

> We don't charge any fees for the online wallet except for the transaction fees on the bitcoin network which is currently set to 0.001 ฿ . For our mixing service we charge between 0.5% and 1.2%. Payouts from the mixer will allways [SIC] be splitted [SIC] to 2 random amounts if only one address is given. So fees are 0.5-1.2% + 2 x 0.001 BTC transaction fees.

Similarly, Vendor 13, which would mine new coins to users' accounts, noted a proportional cost, stating: "We mine bitcoins worth $250 to your addresses 262.5 USD=0.00544BTC . . . We mine bitcoins worth $2500 to your addresses 2540 USD=0.05267BTC." Vendor 12 was one of the few to offer a flat fee, stating: "Unlike other services that charge a volume based fee—meaning the more you mix the more you pay—[Vendor 12] charges a flat fee—meaning you end up paying less the more you mix!"

Vendors 1 and 7 noted that they would allow customers to set their own fee, which they argued was a security feature. Vendor 1 explained:

> Unlike . . . other BTC mixers who charge a flat static fee, [Vendor 1] allows you to set a custom one with every bitcoin mix. If attacker knows service fee, he can analyse blockchain to find exact sum transferred and discover your destination account. For example if you send 1 BTC with a fixed fee 0.5%, you should receive 0.9995 BTC. It is not so difficult to check blockchain after 24 hours and find all exact transactions. Even if you use several forward addresses it is quite easy. That is why our system allows you to set custom fee, combined with several forward addresses and time delay.

Vendors 2 and 4 noted they had a variable fee structure, as with Vendor 4 who simply stated: "We charge random commission 2-5% for every transaction." Vendor 2 noted that their fees were less than 1%, but randomized the final amount. They were very specific in their rationale, stating it was for the protection of their customer and their anonymity, stating:

> Because transactions with fixed fees can be easily detected by law enforcement and fornesic [SIC] software. Example, say you want to mix 1 Bitcoin. You will send 1 Bitcoin to an external mixer, and you receive exactly 0.99 btc back. It doesn't matter what the mixer does to mix your bitcoin, an law enforcement agent can see the amount you send and the look for exactly that amount minus the mixer fixed fee on the block chain. When he sees the transaction that match the mixer fee coming back to an other [SIC] address, they will know is yours. With random fee this cannot be traced. You send 1 Bitcoin from your address to our mixing address. Then we send back to you clean bitcoin of mining farms 0.9982938 or some similar amount. Because there are many similar transactions on the blockchain, they can't know which transaction went to you or what is your address.

Cryptomixing services also communicated clear operational boundaries to their users, including the amount of cryptocurrency they could process for customers. For instance, Vendor 2 stated: "Minimum amount to be mixed: 0.001 BTC (~US$8) Maximum amount to be mixed: 100 BTC (~ 800 000 USD)." Several vendors noted their minimum mixing amount was .001 Bitcoin, though maximum values were variable to the vendor. For instance, Vendor 6 noted:

> What is the largest deal amount [to mix]? It depends on the current amount of coins we have in our reserve and the amount you previously sent to the service. We will not send back your previous coins to you (in case you've used the mixing code). You will be informed about the maximum amount of coins available for mixing.

Discussion and Conclusion

Although research examining the operations of online illicit markets has increased over the last two decades (see Hutchings & Holt, 2017; Tzanetakis et al., 2016), few have explored the practices of cryptomixing services, or the ways in which they are

marketed online (Pakki et al., 2021). Given this gap in the extant literature, the current study conducted an inductive exploratory analysis of cryptomixing services hosted on both the Open and Dark Web to better understand cryptomixing and its role in facilitating online illicit transactions. Four concepts related to cryptomixing and its involvement in facilitating online illicit transactions emerged from the data, including the benefits of cryptomixing, the mixing process, vendor legitimacy, and the costs and procedures of mixing.

The current analysis demonstrated that cryptomixing vendors were aware of the benefits associated with using their services—namely, to enhance the security of financial transactions involving cryptocurrencies (see also Desmond et al., 2019; Pakki et al., 2021). Vendors were cognizant of the various tracking tools and legal regulations imposed on their services by different organizations and emphasized their ability to bypass existing financial regulations. Despite acknowledging the presence of formal sanctions, several vendors explicitly noted that their services were legal and not in violation of any specific financial rules.

To that end, cryptomixing services may not always be used for illegal or nefarious purposes, as there may be individuals who employ cryptomixing services to anonymize their legal financial transactions (Desmond et al., 2019; Pakki et al., 2021). The reasons behind wanting to anonymize legal transactions may range from a desire to shield a particular purchase or simply for economic privacy. Though not all cryptomixing users are criminally motivated, vendors acknowledged the general demand for mixing funds and were aware of what their services provided.

Similar to other online illicit markets, cryptomixing vendors took considerable effort to explain how their services worked and operated (Aldridge & Askew, 2017; Copeland et al., 2020; Holt & Lee, 2022b). The analysis revealed several different methods used by vendors to mix cryptocurrency (Pakki et al., 2021). Some vendors specified that they provided customers with newly mined cryptocurrencies, whereas other services explained they moved preexisting coins across existing accounts. There was even variation among those who used preexisting pools of cryptocurrency to mix customers' funds. Regardless of the mixing method employed, vendors were keen to note the precise methods taken to obfuscate the path of transactions (Pakki et al., 2021). The variations in method may suggest different levels of trust, reliability, and security based on the techniques employed, as customers may prefer one mode over another based on how comprehensive and secure the mixing process is described (see also Copeland et al., 2020; Holt & Lee, 2022b). In fact, detailed descriptions of the mixing process could be a strategy used by vendors to generate comfort and confidence in prospective customers (see also Copeland et al., 2020; Hutchings & Holt, 2015).

Cryptomixing vendors also reinforced their reliability and trustworthiness in various ways. First, vendors noted they had large reserves of cryptocurrencies that could be validated on the blockchain. Vendors were intentional in conveying their ability to safely move large sums of money, demonstrating their care and preoccupation with security, reliability, and efficiency in service. Similar to other cybercrime-as-service vendors (e.g., booter and stresser operators), most cryptomixing services also stated

that they did not retain customer logs of transactions, which is done to protect customers in the event law enforcement investigations and takedowns occur (see also Holt et al., 2022; Hutchings & Clayton, 2016). In addition, vendors operating on the Dark Web mentioned the security features inherent with functioning on the Dark Web which were not possible for Open Web operators. In effect, vendors may be practicing some level of restrictive deterrence as they recognize the inherent risks of operating their services on the Open Web, similar to other illicit market operations (Aldridge & Askew, 2017; Holt & Dupont, 2019).

The emphasis on operating a secure and reliable service was also evident in vendors' cost structures. Some vendors priced their services based on the total amount being mixed, while others allowed customers to set their own fee, which was purposely implemented as an added security feature. Allowing customers to set their own price meant vendors could avoid establishing patterns and routines that would make detection easier for law enforcement. In fact, several vendors directly stated that they randomized the cost of their services to avoid law enforcement detection and circumvent tracking tools (see also Pakki et al., 2021). The reasons were specifically stated as protecting their customers and the anonymity of the vendor.

Overall, the findings of this study provide multiple insights for our understanding of cybercrime specifically and criminality generally. For one, cryptomixing services appear to operate as legitimate services that are effectively legal, making them useful facilitatory services that simplify aspects of criminal operations (Clarke, 1997; Ekblom & Tilley, 2000). Their existence also creates opportunities for investigation and prosecution under money laundering charges or violations of financial transaction laws (FBI, 2020). Similarly, investigating cryptomixing providers may generate information about their customers, who could be pursued for criminal charges related to illicit narcotics or other illicit services as have been observed in other arrests of cybercrime service providers (see Holt et al., 2022; Hutchings & Holt, 2015). Such efforts may deter some mixer operators, or cause their customers to displace to other payment platforms which could have a general destabilizing effect on the illicit use of cryptocurrencies generally (see also Holt et al., 2022; Hutchings & Holt, 2017). Analyses of any law enforcement strategies would be vital to improve our understanding of the ways in which economic cybercrime can be affected by formal and informal mechanisms of social control and the degree of displacement that may occur (e.g., Newman & Clarke, 2003).

Despite the study's contributions, there are several limitations that may affect the generalizability of the study. For one, the behaviors and market practices noted in this study may not be representative of vendors' current operations as the sampling strategy used in the current study was limited to data collected between 2018 and 2020. In fact, various aspects of the mixing process, the costs of mixing, and how vendors demonstrate legitimacy may have changed with the evolution of the cryptomixing marketplace (see also Demant et al., 2018; Munksgaard et al., 2016).

In addition, this study focused on the direct language used by vendors within their sites and advertisements, which may not reflect their actual practices and operations (Copeland et al., 2020; Hutchings & Holt, 2015). Since the researchers did not interact

with vendors, it is plausible that vendors' true practices may differ from their sites and service advertisements (Holt et al., 2016; Hutchings & Holt, 2015; Smirnova & Holt, 2017). Finally, this study was unable to determine whether service advertisements were generated by actual sellers or other interested stakeholders, such as law enforcement or cybercrime researchers (see Holt et al., 2016). Future research would benefit from extending this line of inquiry using more comprehensive samples and methodological techniques to better understand the behaviors influencing illicit online market operations (see also Pakki et al., 2021). Given the scarcity of research on cryptomixing services, there is an intrinsic need for more robust datasets and multidisciplinary approaches to improve our understanding of cryptomixing services and their involvement in online money laundering behaviors (see also Wu et al., 2021).

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Department of Homeland Security under grant 17STCIN00001-02-00. The opinions and findings expressed are those of the researchers and not of the funding agency, its employees, or staff.

References

Aldridge, J., & Askew, R. (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy*, *41*, 101–109.

Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy*, *35*, 7–15.

Blevins, K. R., & Holt, T. J. (2009). Examining the virtual subculture of johns. *Journal of Contemporary Ethnography*, *38*(5), 619–648.

Brenig, C., Accorsi, R., & Muller, G. (2015). Economic analysis of cryptocurrency backed money laundering. *ECIS 2015 Completed Research Papers*, *1*(2015), 20.

Campbell-Verduyn, M. (2018, January 19). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime Law Social Change*, *69*, 283–305.

Chainalysis. (2022, January 26). DeFi takes on bigger role in money laundering but small group of centralized services still dominate. *Chainalysis Blog*. https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/

Clarke, R.V. (1997). Situational Crime Prevention. *Crime and Justice*, *19*, 91–150.

Copeland, C., Wallin, M., & Holt, T. J. (2020). Assessing the practices and products of Darkweb Firearm vendors. *Deviant Behavior*, *41*(8), 949–968.

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*, *13*(1), 3–21.

Demant, J., Munksgaard, R., Décary-Hétu, D., & Aldridge, J. (2018). Going local on a global platform: A critical analysis of the transformative potential of cryptomarkets for organized illicit drug crime. *International Criminal Justice Review*, *28*(3), 255–274.

Desmond, D. B., Lacey, D., & Salmon, P. (2019). Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review. *Journal of Money Laundering Control*, *22*, 480–497.

Dupuis, D., & Gleason, K. (2020). Money laundering with cryptocurrency: Open doors and the regulatory dialectic. *Journal of Financial Crime*, *28*(1), 60–74.

Ekblom, P., and Tilley, N. (2000). Going equipped. *The British Journal of Criminology*, *40*(3), 376–398.

Fanusie, Y., & Robinson, T. (2018). Bitcoin laundering: An analysis of illicit flows into digital currency services. *Center on Sanctions and Illicit Finance Memorandum, January*.

FBI. (2020, April 13). *FBI expects a rise in scams involving cryptocurrency related to the COVID-19 pandemic*. https://www.fbi.gov/news/press-releases/fbi-expects-a-rise-in-scams-involving-cryptocurrency-related-to-the-covid-19-pandemic

Financial Action Task Force. (2020). *FATF report to the G20 finance ministers and central bank governors on so-called stablecoins*. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf

Financial Crimes Enforcement Network. (2020, December 23). Requirements for certain transactions involving convertible virtual currency or digital assets. *Federal Register*. https://public-inspection.federalregister.gov/2020-28437.pdf

Flamand, C., & Décary-Hétu, D. (2019). The open and dark web: Facilitating cybercrime and technology-enabled offences. In E. R. Leukfeldt & T. J. Holt (Eds.) *The human factor of cybercrime* (pp. 60–80). Routledge.

Goldsmith, D., Grauer, K., & Shmalo, Y. (2020). Analyzing hack subnetworks in the bitcoin transaction graph. *Applied Network Science*, *5*(1), 1–20.

Holt, T. J., & Dupont, B. (2019). Exploring the factors associated with rejection from a closed cybercrime community. *International Journal of Offender Therapy and Comparative Criminology*, *63*(8), 1127–1147.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies*, *23*(1), 33–50.

Holt, T. J., & Lee, J. R. (2022a). A crime script model of dark web firearms purchasing. *American Journal of Criminal Justice*, 1–21. https://doi.org/10.1007/s12103-022-09675-8

Holt, T. J., & Lee, J. R. (2022b). A crime script analysis of counterfeit identity document procurement online. *Deviant Behavior*, *43*(3), 285–302.

Holt, T. J., Lee, J. R., & Smirnova, O. (2022). Exploring risk avoidance practices among on-demand cybercrime-as-service operations. *Crime & Delinquency*, *69*(2) 415–438.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). *Data thieves in action: Examining the international market for stolen personal information*. Springer.

Holt, T. J., Smirnova, O., & Hutchings, A. (2016). Examining signals of trust in criminal markets online. *Journal of Cybersecurity*, *2*(2), 137–145.

Hu, Y., Seneviratne, S., Thilakaranthna, K., Fukuda, K., & Seneviratne, A. (2019, December 27). Characterizing and detecting money laundering activities on the Bitcoin network. *Social and Information Networks*. Advance online publication. https://doi.org/10.48550/arXiv.1912.12060

Hutchings, A., & Clayton, R. (2016). Exploring the provision of online booter services. *Deviant Behavior*, *37*(10), 1163–1178.

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*(3), 596–614.

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: Disruption and intervention approaches. *Global Crime*, *18*(1), 11–30.

Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2019). Money talks money laundering choices of organized crime offenders in a digital age. *Journal of Crime and Justice*, *42*(5), 569–581.

Lee, J. R., Holt, T. J., & Smirnova, O. (2022). An assessment of the state of firearm sales on the dark web. *Journal of Crime and Justice*, 1–15. https://www.tandfonline.com/doi/abs/10.1080/0735648X.2022.2058062

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology*, *57*(3), 704–722.

Martin, J. (2014). *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Springer.

Munksgaard, R., Demant, J., & Branwen, G. (2016). A replication and methodological critique of the study "evaluating drug trafficking on the tor network." *International Journal of Drug Policy*, *35*, 92–96.

Munksgaard, R., & Tzanetakis, M. (2022). Uncertainty and risk: A framework for understanding pricing in online drug markets. *International Journal of Drug Policy*, *101*, 103535.

Newman, G. R., & Clarke, R. V. (2003). *Superhighway robbery*. Willan.

Pakki, J., Shoshitaishvili, Y., Wang, R., Bao, T., & Doupé, A. (2021, March). Everything you ever wanted to know about bitcoin mixers (but were afraid to ask). In I. Eyal & J. Garay (Eds.) *International Conference on Financial Cryptography and Data Security* (pp. 117–146). Springer.

Robinson, T. (2020, December 9). Over 13% of all proceeds of crime in Bitcoin are now laundered through privacy wallets. *Elliptic*. https://www.elliptic.co/blog/13-bitcoin-crime-laundered-through-privacy-wallet

Rysin, V., & Rysin, M. (2020). The money laundering risk and regulatory challenges for cryptocurrency markets. In M. Dziura, A. Jaki, & T. Rojek (Eds.), *Restructuring management models-changes-development* (pp. 187–201). Dom Organizatora.

Smirnova, O., & Holt, T. J. (2017). Examining the geographic distribution of victim nations in stolen data markets. *American Behavioral Scientist*, *61*(11), 1403–1426.

Stevens, R. (2022, March 8). Bitcoin mixers: How do they work and why are they used? *CoinDesk Latest Headlines RSS*. https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used/

Trautman, L. J. (2014). Virtual currencies; Bitcoin & what now after liberty Reserve, Silk Road, and Mt. Gox? *Richmond Journal of Law and Technology*, *20*(13), 108.

Tzanetakis, M., Kamphausen, G., Werse, B., & von Laufenberg, R. (2016). The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *International Journal of Drug Policy*, *35*, 58–68.

Vega, N. (2022). If you traded crypto last year, you need to report it on your tax return: "One of the misconceptions of crypto is that it's anonymous." *CNBC*. https://www.cnbc.com/2022/03/31/if-you-bought-and-sold-cryptocurrencies-in-2021-you-might-owe-taxes.html

Vertex Marketplace. (2019, August 13). *What are Virgin Bitcoins and where can I buy them?*. https://vertexmarket.medium.com/what-are-virgin-bitcoins-and-where-can-i-buy-them-d6eab0f669e0

Villanyi, B. (2021). Money laundering: History, regulations, and techniques. In *Oxford research encyclopedias (Vol. Criminology and Criminal Justice)*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190264079.013.708

Wu, J., Liu, J., Chen, W., Huang, H., Zheng, Z., & Zhang, Y. (2021). Detecting mixing services via mining bitcoin transaction network with hybrid motifs. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *52*(4), 2237–2249.

Zagaris, B. (2021). Money laundering and bank secrecy and counter-terrorism financing. *International Enforcement Law Reporter*, *37*, 4.

Author Biographies

Thomas J. Holt is a Professor in the School of Criminal Justice at Michigan State University and its Director. His research focuses on computer hacking, malware, and the role of the internet in facilitating all manner of crime and deviance. He received his PhD from the University of Missouri-St. Louis in 2005.

Jin R. Lee is an Assistant Professor in the Department of Criminology, Law and Society at George Mason University. His research interests are in cybercrime, online interpersonal violence, cybersecurity, cyberpsychology, computer-mediated communications, and big data.

Elizabeth Griffith is a master's student in the School of Criminal Justice at Michigan State University. Her interests center on cybercrime and issues of counterfeiting and intellectual property violations.