Knowing your Bitcoin Customer: Money Laundering in the Bitcoin Economy

Jesse Crawford
Electrical and Computer Engineering
Iowa State University
Ames, Iowa, USA
jbcrawf@iastate.edu

Yong Guan
Electrical and Computer Engineering
Iowa State University
Ames, Iowa, USA
guan@iastate.edu

***Abstract*—Cryptocurrencies like Bitcoin have the potential advantages to break traditional financial barriers, which have attracted great interests from civilian users, financial and online commercial industry, and researchers. However, a recent study [1] reported that approximately one-quarter of Bitcoin users and one-half of Bitcoin transactions are associated with illicit activity. Around US$72 billion of unlawful activity per year involves Bitcoin, which is close to the scale of the U.S. and European markets for illegal drugs. We have made an effort to understand and try our best to exhaustively discover Bitcoin mixing or tumbling services (essentially money laundering mechanisms) which exist or had existed. In our study, 69 services were identified, and evaluation of the public discussion around these services reveals certain trends in Bitcoin user understanding of privacy issues and enforcement of anti-money laundering regulation. So far, Law enforcement interference with Bitcoin laundering services is uncommon, while our study showed that most services failed due to lack of user trust. Trust is perhaps the greatest challenge amongst Bitcoin anonymization services, as many services that have existed appear to be outright scams, and even legitimate services sometimes disappear with user funds. We will report other observations and discussions at the end of the paper.**

I. Introduction

While Bitcoin is broadly thought by users to be an anonymous system, it is actually a pseudonymous system, in which users are identified by keypairs which can be created on-demand [2]. However, as a distributed ledger, the full history of Bitcoin transactions is accessible to any user. This makes Bitcoin transactions amenable to a variety of techniques which can be used to reidentify users and organizations in many cases [3], [4].

The possibility of reidentification if Bitcoin users has lead to substantial interest in services referred to as "mixers" or "tumblers" which accept Bitcoin from a user and then return an equal value (minus service fee) in Bitcoin transactions which cannot readily be linked to the original inputs. This amounts essentially to laundering Bitcoin by "breaking the chain" of possession of coins, and can be used for example to obscure the illegitimate origins of funds or preserve the privacy of a user paying for a service anonymously.

Most academic research into Bitcoin privacy systems have focused on improved methods of anonymization using cryptographic or other means. However, due to various practical limitations these methods do not appear to receive significant use. Some researchers have evaluated the operation of actual Bitcoin mixing services, but have only investigated a handful of services, likely due to the cost of test transactions [5], [6].

Bitcoin privacy is of significant practical interest to both users who wish to ensure their privacy and investigators of malfeasance involving Bitcoin. Cryptocurrency is commonly used as a payment channel for ransomware attacks [7] and is thought to be increasingly involved in other forms of crime, creating a significant incentive for law enforcement to better understand the privacy aspects of these systems as they are used.

II. Background

A. Bitcoin Mixing

Bitcoin is widely described as an anonymous currency, but this is largely incorrect. Bitcoin is a pseudonymous system, in that the identities (addresses) used are not directly tied to user identity. However, because the Bitcoin ledger is publicly available, many methods can be used to reidentify Bitcoin users [2].

In brief form, it is possible to follow the flow of Bitcoin currency through multiple transactions by inspecting the public ledger. By following the flow of currency and using various reidentification methods similar to those applicable to anonymized data sets, it is possible in many cases to determine who obtained Bitcoin and who they sent it to. This is, for example, extremely useful information to law enforcement in investigating crimes involving or paid off in Bitcoin.

As a result, Bitcoin mixing or tumbling services have emerged. These services effectively launder Bitcoin by accepting Bitcoin and "mixing" it through a complicated series of transactions involving multiple user's funds. After this mixing process, it is difficult or impossible to establish the correlation between Bitcoin entering the mixer and Bitcoin leaving. The result is that a Bitcoin user can submit their Bitcoin to a mixing service, and receive Bitcoin back that is not clearly linked to them.

Mixing services broadly fall into two categories. Centralized mixing services are those in which the mixer operator (or rather, software they developed) centrally controls the entire mixing process. This is simpler to implement and more

flexible, but has the downside that the mixer operator has knowledge of the relation of inputs to outputs.

Decentralized mixing services resolve this problem by using algorithmic means to allow multiple users to reach a consensus on a mixing transaction or series of transactions, without any user being aware of the activity of the other users. Decentralized mixing services are more secure in the sense that there is no one person with information on the full state of the mixer, but are more complex to implement and often come with significant limitations.

Some, but not all, mixing services are available via Tor hidden services. These websites are accessed directly through the Tor network which anonymizes both the user and the service operator, allowing users to access the mixing service without the IP address of either the user or the server providing the service being know to the other party.

B. Anti-Money Laundering

In the United States, a system of regulations centered on the Bank Secrecy Act of 1970 requires financial institutions to be actively involved in deterring and detecting money laundering. This system of regulation is known as anti-money laundering (AML), and for the purposes of AML regulation financial institutions are interpreted broadly as any organization which is involved in converting or transacting large amounts of cash. For example, casinos and pawn shops are subject to AML requirements to the extent that they handle cash transactions.

Financial institutions are required to report certain types of transactions to the Financial Crimes Enforcement Network (FinCEN) and to operate a proactive anti-money laundering program. Such AML programs generally focus on know your customer (KYC), a program through which financial institutions collect information on the identity and activity of their customers.

FinCEN has issued regulatory guidance that the majority of Bitcoin service providers qualify as money transfer services for the purposes of AML regulation [8]. This requires organizations which exchange and transfer Bitcoin customers to operate an AML program including KYC and customer due diligence.

Bitcoin mixing services, essentially by definition, are not compliant with these requirements. Because it is explicitly the purpose of a mixing service to obscure the ownership of Bitcoin, mixing services do not identify their customers and do not operate AML programs.

C. Analyzing Bitcoin Mixing

Bitcoin mixers are imperfect and various methods exist to attempt to reverse the mixing process and determine the owner of mixed coins [5], [9]. There are two broad methods.

The first method, taint analysis, is a method of tracing Bitcoin as it moves through the transaction graph. A Bitcoin known to belong to an individual is "tainted." Any later transaction involving the tainted Bitcoin inherits the taint. As the taint is propagated forward through the transaction graph, all tainted Bitcoin potentially belongs to the original user. It may be possible to confirm this ownership based on user behavior.

The second method is focused on examining the inputs and outputs of a mixing service. It may be possible to identify all of the Bitcoin addresses used by a mixing service using various graph analysis techniques. Transactions entering and exiting this cluster of addresses can be assumed to be inputs and outputs from and to users of the mixing service. Analysts can rely on a basic property of mixing services: the amount of Bitcoin returned to a mixing service user will be the same as the amount they submitted to the service, minus a transaction fee. Thus outputs which are slightly less than an input are a candidate for being the same user's Bitcoin returned to them.

III. A List of Bitcoin Laundering/Mixing Services for Our Investigative Study

A. Methodology

To better understand the ecosystem of Bitcoin mixing services, an attempt was made to enumerate mixing services in use. The Bitcoin Forums are an extremely popular central resource on the Bitcoin Community, and a large portion of all Bitcoin services, particularly those oriented towards every-day users and those concerned about privacy, are announced and promoted there.

The "Services and Announcements" section was reviewed based on keyword search and manual discovery to find all announcements of Bitcoin mixing services. Further, discussions on privacy and mixing were reviewed for any mixing services that they mentioned. The result is an enumeration of 69 Bitcoin mixing services that were either in use or announced at some point in time.

This method does not produce an exhaustive listing, but because these forums are a major source of information on mixing services it should reveal a significant sample of existing mixing services. Because the Bitcoin forums are on the public internet, they may underrepresent darknet-based mixing services which are advertised on various more ephemeral darknet forums.

B. Listing

We have collected data and analyzed the mixing services in Table 1. For Disposition, "current" indicates a currently active service. "SDBO" indicates a service which was shut down by its owner. "NI" indicates a service which failed to garner sufficient interest to be discussed or reviewed, and which is no longer operating. Finally, "scam?" indicates a service which appears to have been a scam, based on user reports.

IV. Major Findings about Bitcoin Mixing Services

To better understand the ecosystem of Bitcoin mixing services, we have used the collected data and made an attempt to enumerate all mixing services that exist or have existed. The Bitcoin Forums are an extremely popular central resource on the Bitcoin Community, and a large portion of all Bitcoin services, particularly those oriented towards every-day users and

TABLE I
MIXING SERVICES EVALUATED

Name	Date Announced	Type	Disposition	Darknet
bitcoinfog.com	2011-10-27	central	Scam?	No
easywallet.org	2012-04-06	central	SDBO	No
MixMyCoin	2013-11-21	central	Scam?	No
BitLaunder	2014-01-04	central	Scam?	No
bitmixer.io	2014-01-14	central	SDBO	No
bitcoin blender	2014-01-28	central	Scam?	
coinclean.cc	2014-03-05	central	SDBO	Yes
BitiMix	2014-06-05	central	NI	Yes
bitmix	2014-06-13	central	NI	No
BctMixPot.com	2014-07-28	central	NI	No
btctumbler	2014-08-20	central	NI	Yes
btcmix.me	2014-08-29	central	NI	No
btcmixing.com	2014-09-16	central	NI	Yes
JoinMarket	2015-01-09	coinjoin	NI	Yes
mixing.space	2015-03-04	central	NI	Yes
coinmixer.se	2015-06-13	central	sdbo	Yes
anonymizer5lg2fz.onion	2015-07-23	central	SDBO	Yes
coinmixer.net	2015-08-19	central	Scam?	Yes
darklaunder.com	2015-08-19	central	Scam?	No
spacechain.io	2015-08-31	central	Scam?	No
DeepMix	2015-09-09	mixcoin	NI	Exclusively
bitmix.in	2015-09-20	central	Scam?	Yes
Bitcloak	2016-02-21	central	current	Exclusively
bitcloak	2016-02-21	central	current	Yes
cryptomixer.io	2016-03-30	central	current	Yes
mixcoin.tk	2016-11-27	central	Scam?	Yes
mixem.io	2016-12-19	central	NI	No
mixer.money	2016-12-22	central	current	Exclusively
Burger	2017-02-17	central	NI	No
chipmixer	2017-05-26	chip	current	Yes
gocrypto.io	2017-05-29	central	NI	Yes
FRECOINLAUNDRY	2017-07-03	central	NI	Exclusively
5ifblitg2ywjjo2t.onion	2017-07-31	central	NI	Yes
bitmixer.co	2017-08-05	central	SDBO	No
bitmix.biz	2017-08-18	central	current	Yes
bitmix.biz	2017-08-18	central	current	Yes
btcmixer.biz	2017-08-24	central	NI	Yes
privcoin.io	2017-09-09	central	current	No
bitmixcoin.io	2017-09-10	central	Scam?	Yes
mixer.to	2017-09-16	central	Scam?	Yes
foxmixer	2017-10-01	central	current	Yes
http://2ovmq6sfab6u4ucr.onion/	2017-10-26	central	Scam?	No
smartmix.io	2018-01-24	central	current	Yes
bestmixer.io	2018-03-16	central	takedown	Yes
bitwhisk.io	2018-03-27	central	SDBO	
bitsafe.pro	2018-05-03	central	Scam?	No
bitmaximum.io	2018-06-30	central	SDBO	Yes
jambler.io	2018-07-13	central	current	Yes
doublemixer.com	2018-08-16	central	Scam?	No
mixtum.io	2018-08-27	central	current	Yes
wasabi wallet	2018-09-24	coinjoin	current	Yes
ecomix.io	2018-09-25	central	SDBO	Yes
blender.io	2018-10-18	central	current	Yes
coinmixer.be	2018-11-20	central	Scam?	Yes
bitcoin laundry	2018-12-03	central	Scam?	Yes
zatoshi	2018-12-05	coinjoin	NI	Yes
domixer	2019-03-15	central	NI	Yes
bitcoin.dj	2019-03-27	central	NI	No
bitmixer.xyz	2019-04-17	central	Scam?	Yes
btcanonmixer.com	2019-04-18	central	Scam?	Yes
mybitmix.com	2019-05-16	central	current	Exclusively
mixertumbler.com	2019-05-21	central	current	Yes
bmc	2019-07-17	central	NI	Exclusively
smartmixer.io	2019-07-24	central	current	Yes
sharedcoin.com		coinjoin	SDBO	Yes
Fogify		central	shut down	Exclusively
pay shield		central	current	
Helix Light		central	Scam?	No
Helix Grams		central	SDBO	Yes

those concerned about privacy, are announced and promoted there.

The "Services and Announcements" section was reviewed based on keyword search and manual discovery to find all announcements of Bitcoin mixing services. Further, discussions on privacy and mixing were reviewed for any mixing services that they mentioned/stated. The result is an enumeration of 69 Bitcoin mixing services that were either in use or announced at some point in time. The full list is included in Table 1.

Examination of a large number of Bitcoin mixing services shows the difficulty of establishing commercial trust in a rapidly-changing marketplace with significant use of privacy technology. Many mixers have very similar names, which may be an intentional misrepresentation or simply a result of the desire for obvious names (e.g. "bitmixer"). Many mixers operate Tor hidden services, which have randomized addresses and so are often duplicated by fraudulent operators—and may also legitimately change their addresses.

A. Marketing

It is difficult to overstate the significance of the Bitcoin Forums to the Bitcoin community and economy. These forums serve as an almost universally known central point for discussion and advertising of Bitcoin services. As a result, mixing services are often announced first on the Bitcoin Forums and later advertised there.

Following the announcement of a service (where the features are usually listed, as well as clearnet and Tor addresses), mixing services may take a number of further steps to promote themselves and gain trust. First, some new services will agree to place a small number of coins in "escrow" with a well-established member of the Bitcoin Forums community. This ad-hoc arrangement gives users some confidence that they will not lose their Bitcoin, as if the mixing service fails to return their coins they can use the signed "proof of mixing" letter that these services generally issue to request that the trusted user make them whole.

Second, services may use paid advertising. Because of the legal issues surrounding these services it is not common for them to advertise by conventional means. Instead, they may launch a "signature campaign" wherein they pay prominent Bitcoin Forums members to paste advertisements for the service into their forum post signatures. Payment is typically made in the form of Bitcoin.

B. Features

Newly launched laundering services are entering a crowded market. Users are very hesitant to trust new services, and with several well-established services operating at almost every point in Bitcoin's history it is difficult for new services to find users.

New mixers use several methods to attract new users. The first, and perhaps most important, is the sets of claims made by new services when they are announced. By far the most common marketing claim made by new mixers is "zero taint." This indicates that users, or at least mixer operators, are well aware of taint analysis as an analysis technique. However, mixing services virtually never advertise that they prevent *other* mixing methods, suggesting that the community is focused primarily on evading taint analysis at the cost of preventing other methods of analysis.

Users of mixing services appear to be aware of the fact that centralized mixing services are capable of reidentifying their users. As a result, many mixing services explicitly advertise that they do not retain any logs or other identifying information on users. It is also common for services to advertise that they do not require users to "sign up" for an account or provide any identifying information (such as an email address), although many mixing services do require that users set up an account and provide additional identifying information.

Another common advertising claim is that user of the mixer does not require Javascript. This is in response to the large number of users who access mixing services via the Tor Browser Bundle, which in many versions blocks Javascript execution by default.

Common features advertised by mixing services include:

- Random delay times from input to output, which prevent simple correlation analysis based on timing.
- Randomized fees, which make correlation analysis based on amount more difficult.
- Cryptographically signed documents stating the mixing service's obligation to pay out, which could be used to prove that the mixer fraudulently failed to return a user's coins.

These features show user awareness of the risks of using centralized mixing services, including both fraud and capture of their information from the service operator.

It is important to note that the two common features intended to frustrate correlation analysis, random delay times and randomized fees, are of only limited value if an analyst is able to determine the full set of wallets in use by a mixing service. However, mixing services almost never make any claims about the quality or complexity of their internal mixing process. This likely reflects primarily the difficulty of describing these internal mixing processes succinctly, even though they appear to generally be fairly simple.

C. Failure to Launch

69 mixing services over the relatively short lifetime of Bitcoin seems like a high rate of new service introductions. Were they evenly distributed, this would be about eight new services a year, but in practice the rate of launch of new mixing services has increased, with more than once introduced per month starting in 2017.

This large set of new mixing services are seldom successful. Of the mixing services identified, 26 or 38% simply failed to generate any interest. Few of these are still available, suggesting that they did little business and so their operators closed them down.

Many announcements generate one or two replies suggesting that there is no reason to trust a new service based on a brief announcement. This suggests that the problem of

fraudulent services (which simply keep deposits) presents a real challenge to adoption of new mixing services, and so the community will prefer to continue to use a small number of trusted services.

The tendency of users to distrust new services poses an additional challenge to the adoption of improved mixing technology, since even for services which employ technical means to prevent fraud such as CoinJoin, user may be hesitant to leave services which they know to be reliable.

D. Scams

One of the most obvious conclusions from an enumeration of announced Bitcoin mixing services is how few have survived to the present day. In fact, the majority of mixing services announced appear to have been scams.

The problem of Bitcoin services, particularly those which advertise anonymity, being fraudulent is well known. The Bitcoin Forums feature a thread reputation system in an attempt to mitigate fraud, with users either "vouching" for or "warning" of services based on their knowledge and experiences.

In experimenting with Bitcoin mixers, one group of investigators lost their Bitcoin to a scam in three out of five attempts [6]. Another had to eliminate a possible scam from their planned set of mixing services [9]. And with Bitcoin services with profiles as large as Mt. Gox disappearing and taking their users funds with them, fraud is obviously a possibility with mixing services.

In this enumeration, mixers were considered a likely scam if there were indications in the Bitcoin Forums discussion around them that they were a scam, of if they were reported later elsewhere on the internet to have disappeared with user funds. It is likely that this undercounts actual scams since many mixers failed to generate any attention at all. It also undercounts scams occurring via Tor hidden services, where the same service will often frequently generate new addresses, making counting difficult.

With this likely undercount in mind, 19, or 28%, of discovered Bitcoin mixers were likely scams. This set of fraudulent mixing services reveals an interesting challenge in the loosely organized and often informal Bitcoin industry: many simply duplicated the name of an existing, reputable mixer in order to gather coins from confused customers arriving at the wrong website.

A notable example surrounds Helix Light by Grams, a well-known mixing service from the popular darknet search engine Grams. Helix Light was discontinued by its operator, but a visually identical service also calling itself Helix Light appeared at a different address and solicited payments. This seems to have been a simple scam on users who had not heard that Helix Light had shut down.

The problem of evil twins is further compounded by the heavy use of Tor hidden services, which have long, randomized addresses which are often not very memorable or recognizable. This makes it easy to post an address on the internet which claims to be for a well-known service but actually leads to a fraudulent duplicate.

The dual internet/Tor nature of many mixers opens up an interesting novel class of evil twin. Bitcoin Fog is a popular and trusted mixing service which operates only as a Tor hidden service. The visually identical Bitcoin Fog website on the public internet was fraudulently created by a different operator, and capitalizes on Bitcoin Fog's well-known name and lack of internet presence.

E. Types of Mixers

Of the Bitcoin mixers considered, the vast majority are centralized mixers which make no particular claims about their architecture. 62, or 90% of announced mixers are centralized mixers. Eliminating apparently fraudulent services and services which failed to gain interest, 77% are still centralized.

This result is surprising considering the disadvantages of centralized mixers, which include a greater potential for fraud, vulnerability to seizure or exfiltration of records by law enforcement, and opaque operations which may obscure poor design. However, it is understandable in consideration of usability factors.

Centralized mixers are generally highly user-friendly. A user need only access a website (possibly through the Tor network), enter some information, provide output addresses and deposit coins to an input address from the wallet of their choice, potentially including a custodial wallet service (which operates a Bitcoin client and manages a user's keys on behalf of that user for ease of use).

This type of service is easy to understand and use for novice users, and are highly compatible with whatever wallet solution a user is already familiar with. They are also easy to discover via search engines, darknet search engines, and websites where Bitcoin is discussed.

On the other hand, decentralized mixing systems require that the user download and use a client software program. Depending on the system, the user may also need to use the client software program as their wallet, importing or generating new keypairs. This complexity, and the risk of using an unknown application, is likely a discouragement to new users.

F. Anonymity Protections

To prevent mixing services (or others) identifying users based on their IP addresses, users are commonly advised to access mixers using an anonymizing network such as Tor. To facilitate this, many mixers provide a Tor hidden service, and some operate exclusively in this fashion.

The function of Tor hidden services is to provide anonymity of the *provider* of the service, and so offering a hidden service alongside a "clearnet" or public internet website negates this security [10]. However, this is a common practice. The willingness of mixer operators to shed some amount of anonymity by providing a clearnet website (with associated domain registration, IP address, and other information which could be used to identify them) suggests that many users are not sophisticated enough or not willing to access such services through Tor.

On the other hand, the decision of these mixers to provide a hidden service despite also offering a clearnet service, when this has a reduced advantage to their users, suggests pressure to appear to use various conventionally expected security measures.

Of 69 hidden services, 39, more than, provide both a clearnet website and a hidden service. 8 are accessible exclusively via a Tor hidden service. 19 are accessible exclusively via clearnet. The remainder are client-based mixers which do not use their website as part of mixer operation.

G. Operator and Law Enforcement Actions

Of the 69 services examined, only one was publicly shut down by law enforcement. This service, bestmixer.io, was seized by the Dutch Financial Criminal Investigative Service after a multinational investigation. The primary fault in bestmixer's efforts to evade law enforcement seems to have simply been their location in the European Union—a vulnerability they were apparently aware of as they falsely advertised their location as Curacao [11].

There are no other reported incidents of law enforcement seizure of bitcoin mixing services, suggesting that global enforcement of AML regulations and criminal laws is limited. While it is difficult to determine the country of origin of mixing services, a likely explanation for limited law enforcement is that the most successful mixing services are located in countries with little or no AML policy.

Far more common than interference by law enforcement is the decision of an operator to shut down their own mixing service. At least 11 services were closed by their operator, some after they had failed to gain any significant attention, but others were shut down despite widespread popularity.

The major Bitcoin mixer bitmixer.io closed doors after the operator posted online that they had realized that "Bitcoin is transparent non-anonymous system by design"[1]. Although it is difficult to verify this claim, bitmixer.io has stated that they processed 65,000 BTC per month, making it a very significant player in the market and a surprising service to so abruptly close [12].

V. Observations and Discussions

A. Difficult to Establish

While the number of Bitcoin mixing services which have existed is fairly large (with 69 almost certainly being an undercount), the number of services which are trusted by the broader Bitcoin community is fairly small—perhaps a half dozen. One often-linked-to list on the Bitcoin Forums includes 14 mixing services not thought to be scams, several of which are still fairly new.

For potential users of Bitcoin mixers, the greatest hazard appears to be common scams, including simple duplicates of popular mixing services. Users seem to also face the challenge of technical complexity, with the most easily used mixers (centralized services available on the clearnet) also being the highest risk for both fraud and reidentification.

The greatest hazard faced by mixing services themselves seems to be a crowded marketplace in which trust is difficult to earn. Mixing services far more often fail due to the inability to earn customers than due to law enforcement action. While the possibility of criminal charges is no doubt a factor in the decision of some operators to shut down their mixing services, the challenges of remaining profitable while keeping up with changing technology and the instability of the Bitcoin market are likely also significant factors.

B. Community Response to Scams

Because of the ease of launching a Bitcoin service and the anonymity with which these services often operate, scams are a significant challenge in the Bitcoin grey market.

The community has developed several ad-hoc measures to detect mixing services which are merely scams that intend to shut down and retain the funds which had been sent to them. The first is the practice of some services of placing funds in escrow with respected members of the Bitcoin Forums. This provides the community with assurance that they will not lose their funds, to the extent that they trust the individual who holds the escrowed Bitcoin.

Further, because the Bitcoin Forums are a common central point for information on Bitcoin services, its users have developed an informal reputation system. Users often report any apparently fraudulent behavior on the announcement page for a service, and discuss scams in other sections of the forum. This evolved into a system where users can "vouch" for a service or report a scam. If multiple users accuse an announced service of operating as a scam, a clear warning displays above the thread.

VI. Blockchain Analysis Services

While Bitcoin mixing services intentionally do not comply with AML regulations, legitimate Bitcoin services based in the US (and to a lesser extent globally) are motivated to comply with AML regulations to avoid legal sanctions. The application of AML and KYC requirements to Bitcoin remains somewhat unclear, but various services have emerged which promise to assist Bitcoin services in compliance.

These can broadly be placed in two categories: AML/KYC products which are intended for use *prior* to any incident as a risk management process, and investigatory products intended for use *after* an incident. These two classes of tools approach the problem from somewhat different directions. KYC products generally attempt to determine whether or not a transaction has been intentionally anonymized, and if so do little further than indicate a high risk. Investigatory products, on the other hand, are often used explicitly because the transaction has been anonymized, and must attempt to reverse the anonymization process.

Many services which advertise themselves as blockchain KYC/AML solutions (or as more general solutions which are applicable to cryptocurrency as well) only address the

[1] https://bitcointalk.org/index.php?topic=2042470.0

customer identification program (CIP) component by collecting and verifying customer identification documents. While important, this component of AML compliance does not involve the actual analysis of the blockchain and so is excluded from this discussion.

A. AML/KYC Services

Five providers offer a cryptocurrency AML solution based on analysis of the blockchain. It is difficult to provide substantial analysis of these services because they publish very little about their internal methodology, perhaps out of concern that it could be contravened by actors with knowledge of the algorithms in use. Some inferences about the state of the art in Bitcoin transaction risk analysis can be drawn from the open literature on the subject.

[13] discuss two important heuristics in analysis of the blockchain: first, all of the inputs to a transaction generally belong to the same person. Second, there is usually a change output on the transaction which also belongs to the same person as these inputs, subject to certain constraints on the identification of the change address. It is shown that these two heuristics allow substantial clustering of Bitcoin addresses by ownership, and that these clusters allow for reidentification of addresses belonging to users one has interacted with (and out to additional degrees).

In a different vein, a set of methods have been discussed for graph analysis of money laundering in general (that is, not specifically for cryptocurrency) [14]. It is shown that link analysis can be used to identify likely participants in money laundering based on characteristic patterns, such as dividing money across multiple activities and then recombining at a later time.

These approaches can be combined to detect finances involved in money laundering. In fact, this is the easiest formulation of the problem of analyzing Bitcoin mixing services, since the only requirement is to identify the outputs of a mixing service, with no need to identify inputs or their relations.

First, addresses belonging to mixing services are identified. This can be done by a number of methods, but the most obvious is to initiate transactions with mixing services so that they reveal an address to be used as an input.

Clustering methods are then used to identify further addresses related to a mixing service. Addresses in use by mixing services tend to be tightly clustered according to well-known heuristics, and so a large portion of the addresses used by a mixing service can be identified in this fashion [5], [9], [13].

The result is a database of addresses known to belong to mixing services. Any transaction can then be traced back in terms of its inputs. Any path back which leads to a mixing service indicates a higher risk of money laundering or fraudulent activity, with that risk decaying according to the number of steps in between and the portion of the transaction funded by apparently laundered coins.

This method is essentially taint analysis performed in reverse: from a given transaction, coins are traced backwards in order to establish whether or not they are tainted.

B. Existing Blockchain Investigative Tools

A number of tools also exist which are intended for post-hoc investigation of blockchain activity. These are intended primarily for law enforcement and investigators for litigation, and are oriented around understanding the flow of money that is known to have been involved in a criminal or otherwise suspect act.

These tools usually combine visualization tools along with annotation tools, and may include clustering features. Visualization tools allow an investigator to easily follow the flow of bitcoin between transactions by visually moving between inputs and outputs. Transactions are usually presented in a graph format but the view is often simplified or reduced in scope to maintain ease of use.

Annotation in forensic tools usually consists of a vendor-provided database of addresses annotated by known owners, and the ability for the user to add their own annotations to addresses as their owners are determined. Clustering tools may assist in annotating other addresses which apparently belong to the same owner.

Because investigative tools are intended for manual post-hoc use, they are impractical for use as part of an AML program because of the time and effort which would be required to manually investigate a large number of transactions.

C. Implications for the Bitcoin Market

Risk scoring tools for Bitcoin transactions are becoming increasingly common as exchanges and other service providers develop AML compliance programs. The result is that an individual possessing Bitcoin which is tainted may have a difficult time using it—a situation similar to counterfeit money, and with the similar disadvantage that the holder of such Bitcoin may have obtained it legitimately and not be aware of its suspect past.

This has interesting implications on the broader Bitcoin market. Bitcoin may have an additional axis of value beyond its denomination: that of trust. Bitcoin which has a suspect or high-risk past may be less valuable to many users than Bitcoin without such a taint [15]. Further, any person receiving Bitcoin may run a risk that it is tainted and is not only less valuable in its own right but may even reduce the value of any Bitcoin with which it is mixed.

There are implications of this heterogeneous aspect of Bitcoin, which could significantly complicate the Bitcoin market by making Bitcoin payments a higher-risk activity which will be less reliable due to the need of parties involved to protect themselves by rejecting high-risk transactions [16]. Considering the likelihood that, over a long span of time, all circulating Bitcoin will pass through a mixing service, this presents a significant practical problem.

D. Dusting

This problem also presents the possibility of intentional manipulation of Bitcoin risk. Indeed, such an event has occurred at least once. On October 23rd of 2018, major Bitcoin mixing service BestMixer.io sent small amounts of Bitcoin referred to

as "dust" to a large number of recipients. While BestMixer.io publicly identified this as a new form of advertising, it is broadly thought to have been an effort to foil automated AML analysis by artificially tainting a large number of legitimate wallets [17].

This activity can be located on the blockchain using relatively simple heuristic analysis, by identifying transactions with large numbers of small outputs. Other such transactions also appear on the blockchain, suggesting that dusting attacks have occurred in multiple cases and perhaps by multiple actors. It is not entirely clear whether these were intended to complicate taint analysis or enable it by generating artificial inputs to known addresses in the hope that they would be spent. However, at the minimum, dusting activity does somewhat complicate taint analysis.

This type of activity has also occurred in the case of LiteCoin, although there is some debate around the motivations underlying the dusting [18]. Further, it is not clear if such activity has continued in the Bitcoin blockchain since the shutdown of BestMixer.io by law enforcement.

It is not clear if AML analysis services have taken countermeasures against incorrectly assigning high risk to wallets due to previous dusting attacks. Correcting for this artificial activity is fairly straightforward: since the BestMixer transactions sent amounts between 666 and 888 Satoshi, very small amounts, an AML service would be well advised to simply ignore inputs of such small size unless they cumulatively add to a larger value in a single wallet.

VII. Summary and Future Directions

The number of Bitcoin mixing services which have existed is significant, with new announcements on a regular basis. However, these services depend heavily on user trust which is very difficult to acquire. Ultimately, the number of services which are considered popular and trustworthy is quite small. All of these services are centralized, leaving users potentially vulnerable to compromise of the service operator.

From the perspective of an investigator, this greatly simplifies the situation, as it is only necessary to analyze the operation of a relatively small number of systems. However, for privacy-seeking users the current situation poses a significant challenge. It is extremely difficult for users to evaluate the trustworthiness or efficacy of any given service, and so users expose themselves to appreciable risk by using and relying on a mixing service.

VIII. Acknowledgements

We would like to thank the anonymous reviewers for their insightful feedback. This work was partially funded by NIST under Cooperative Agreement No. 70NANB15H176 and NSF under grants No. CNS-1527579, CNS-1619201, and CNS-1730275, and the Boeing Company.

References

[1] S. Foley, J. R. Karlsen, and T. J. Putnins, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?" in *Review of Financial Studies*, 2018. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3102645

[2] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in *Security and privacy in social networks*. Springer, 2013, pp. 197–223.

[3] M. Fleder, M. S. Kester, and S. Pillai, "Bitcoin transaction graph analysis," *arXiv preprint arXiv:1502.01657*, 2015.

[4] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in *International Conference on Financial Cryptography and Data Security*. Springer, 2013, pp. 34–51.

[5] T. de Balthasar and J. Hernandez-Castro, "An Analysis of Bitcoin Laundry Services," in *Secure IT Systems*, ser. Lecture Notes in Computer Science, H. Lipmaa, A. Mitrokotsa, and R. Matulevičius, Eds. Springer International Publishing, 2017, pp. 297–312.

[6] R. van Wegberg, J.-J. Oerlemans, and O. van Deventer, "Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin," *Journal of Financial Crime*, vol. 25, no. 2, pp. 419–435, 2018.

[7] N. Hampton and Z. A. Baig, "Ransomware: Emergence of the cyber-extortion menace," 2015.

[8] FinCEN, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," Tech. Rep. FIN-2013-G001, Mar. 2013.

[9] M. Möser, R. Böhme, and D. Breuker, "An inquiry into money laundering tools in the Bitcoin ecosystem," in *2013 APWG eCrime Researchers Summit*, Sep. 2013, pp. 1–14.

[10] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," Naval Research Lab Washington DC, Tech. Rep., 2004.

[11] S. Higgins, "EU Authorities Shut Down Bitcoin Transaction Mixer," May 2019. [Online]. Available: https://www.coindesk.com/eu-authorities-crack-down-on-bitcoin-transaction-mixer

[12] J. Buntinx, "Popular Bitcoin Mixing Service Bitmixer.io Shuts Down Immediately," Jul. 2017. [Online]. Available: https://themerkle.com/bitmixer-shuts-down/

[13] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: characterizing payments among men with no names," in *Proceedings of the 2013 conference on Internet measurement conference*. ACM, 2013, pp. 127–140.

[14] T.-M. Cheong and Y.-W. Si, "Event-based approach to money laundering data analysis and visualization," in *Proceedings of the 3rd International Symposium on Visual Information Communication*. ACM, 2010, p. 21.

[15] M. Möser and R. Böhme, "Join me on a market for anonymity," in *Workshop on Privacy in the Electronic Society*, 2016.

[16] M. Möser, R. Böhme, and D. Breuker, "Towards risk scoring of Bitcoin transactions," in *International Conference on Financial Cryptography and Data Security*. Springer, 2014, pp. 16–32.

[17] Jake, "ALERT: Crypto Dusting is a New Type of Blockchain Spam that..." Dec. 2018. [Online]. Available: https://ciphertrace.com/crypto-dusting/

[18] J. Mapperson, "Understanding Litecoin's Dusting Attack: What Happened and Why," Aug. 2019. [Online]. Available: https://cointelegraph.com/news/understanding-litecoins-dusting-attack-what-happened-and-why