An Ego Network Analysis of Sextortionists

Frédérique Oggier[1], Anwitaman Datta[2], and Silivanxay Phetsouvanh[2]

[1] Division of Mathematical Sciences, Nanyang Technological University, Singapore
[2] School of Computer Science and Engineering, Nanyang Technological University, Singapore

Abstract. We consider a particular instance of user interactions in the Bitcoin network, that of interactions among wallet addresses belonging to scammers. Aggregation of multiple inputs and change addresses are common heuristics used to establish relationships among addresses and analyze transaction amounts in the Bitcoin network. We propose a flow centric approach that complements such heuristics, by studying the branching, merger and propagation of Bitcoin flows. We study a recent sextortion campaign by exploring the ego network of known offending wallet addresses. We compare and combine different existing and new heuristics, which allows us to identify (1) Bitcoin addresses of interest (including possible recurrent go-to addresses for the scammers) and (2) relevant Bitcoin flows, from scam Bitcoin addresses to a Binance exchange and to other other scam addresses, that suggest connections among prima facie disparate waves of similar scams.

Keywords: Bitcoin network · Ego graph analysis · Bitcoin scams

1 Introduction

Owing to their pseudo-anonymous nature, cryptocurrencies are often used by cybercriminals for collecting and laundering money from illegal activities. We consider Bitcoin, one of the most established cryptocurrencies, and the corresponding Blockchain network. Ransomware and scam extortions are two very lucrative criminal activities that have proliferated in the Bitcoin ecosystem - requiring ransoms to be paid to Bitcoin addresses, making it hard for law enforcement agencies to track the owner(s) of the address(es), while making it easy for criminals to run waves of attacks targeting millions of potential victims via malwares or personalized emails. Examples of previous Bitcoin forensics studies include [19, 27, 10, 15, 17, 3] for ransomwares, and [31, 28] for extortions, or more precisely sextortions. The term 'sextortion' has multiple interpretations - including blackmailing someone to obtain sexual favors, and reversely, blackmailing someone by using compromising information that is sexual in nature. In this work, we look at an emerging genre of sextortion that falls in the latter category, and furthermore, often (but not necessarily) is based on bluff rather than the blackmailer genuinely having access to compromising information about the victim. The overall modus operandi of the sextortion studied in this paper

works as follows: (1) A potential victim receives an email from a blackmailer, who pretends to know some sexually embarrassing information about the victim, see an example snippet of such an email in Figure 1. Sometimes, the attacker personalizes the message using as evidence information obtained from unrelated data breaches to convince the potential victim that the blackmailer has indeed hacked into the victim's computer to obtain claimed compromising information. (2) The scammer accordingly asks for a payment in exchange for not disclosing said information. Often this payment is requested in the form of cryptocurrency payment, e.g. to be paid to a specific Bitcoin address.

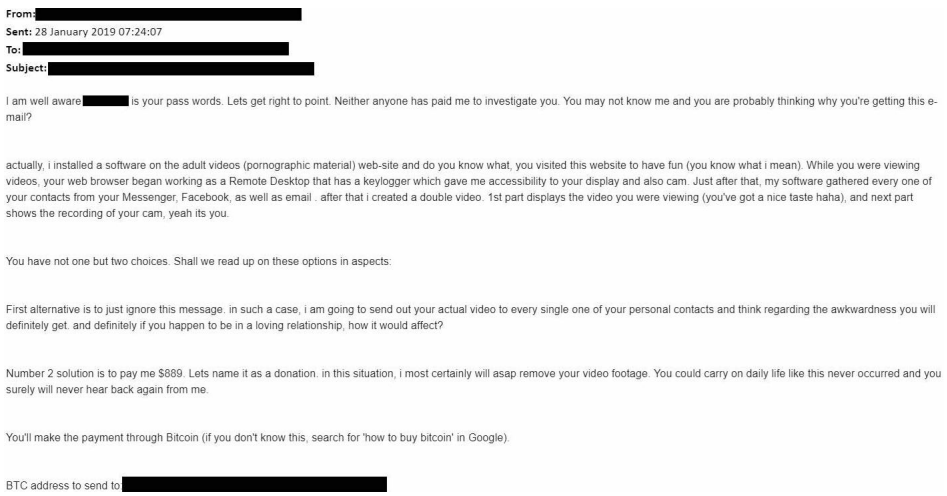


Fig. 1. An example of sextortion email [21].

We study the network created by Bitcoin transactions to understand scammers' interactions, how they launder money, and determine how distinct wallet addresses may or not be related to each other. The underlying enabler of our methodology is social network analysis, which has also been used in other contexts of digital forensics [16, 11] and user characterization [33].

We identify the relationship among wallet addresses using a flow based analysis to complement popular Bitcoin forensics and wallet address agglomeration heuristics which analyze transactions individually (e.g., the heuristics of clubbing together multiple inputs [30], and conditionally a change address [23]) and then coalesce address groups identified from such individual transactions. Such heuristics may be seen to be based on local information at individual nodes of the network, and have been created by leveraging on the observed typical behavioral patterns, which can thus also be thwarted by adversaries consciously choosing to behave differently, or by using mixing, which these local information based heuristics are inept in dealing with, while our approach leverages the ego network across a range of horizons, and money flow behavior to further deter-

mine relationships. Since we study the propagation of flows, and their mergers along the course of the flow, foremost it provides complementary information compared to the aforementioned heuristics [30, 23], and furthermore, they can be applied even in the presence of mixing of flows, since we continue to trace all the outgoing flows from a transaction which involves mixing, checking whether some of those flows merge again downstream.

We expose our methodology by studying events of sextortion that happened in March 2019 using Bitcoin blockchain data for the period of 26 Feb 2019 to 4 April 2019 (block height range: 564671-570195) where payments in Bitcoins were demanded from the victims of blackmails. We demonstrate how our flow based approach identifies relationships among wallet addresses by following branches of flows until some of them merge back downstream. Doing so allows us to identify special wallet addresses and Bitcoin flows. For example, we discover wallet addresses that are used to consolidate funds, re-disperse them post consolidation, or funnel them to a Bitcoin exchange using a particular 'go to' address that is used repeatedly to interact with said exchange. We also unveil Bitcoin flows among Bitcoin addresses appearing in a priori different waves (targeting victims from different countries and languages) of attacks during the same period.

Contributions: Technical contributions of this paper comprise a set of novel graph visualization and heuristics for mining subgraphs derived from the Blockchain network that we use for the purpose of Bitcoin forensics: (1) given a two-mode (directed graph) network model (Section 3) comprising transactions and wallet addresses as nodes, where multiple instances of a given wallet address are represented as separate nodes, we demonstrate how to gradually explore the ego networks of individual instances of a wallet address, leading to an algorithmically driven but visually tractable mechanism to follow the branching and merger of flows (explained in Section 4); (2) we study the proximity of any two address nodes in an undirected version of the two-mode network, characterizing the proximity by the number of (shortest) paths, and separately by the number of directionality flips in the directed version of said path, to capture the frequency of flow merger and dispersal events associated with a given connection among the nodes (Section 5). While there has been a lot of (social-)media discussions, blogs by cybersecurity professionals and organizations, blackmail scams have so far been relatively less studied in contrast to ransomwares in the academic context of Bitcoin forensics. In particular, this study is, to the best of our knowledge, the first study of the March 2019 sextortion campaign. Therefore the current study of a recent blackmail campaign further contributes in (3) curating a new dataset[3] which is in contrast to existing recent works on sextortion analysis, e.g. [28] and references therein, which use proprietary data that is not publicly available; and (4) actually singling out suspicious wallet addresses and Bitcoin flows, within a given scam, but also those that connect a priori distinct scams (Section 5). Since a blackmail campaign is easily replicated, it is of interest to figure out whether different groups happen to have sent similar blackmail emails during the March 2019 waves of scams, or if these were concerted.

[3] The curated ego network dataset used in this paper can be found at [26].

Notation and terminology: We recall that Bitcoin users can acquire one or several Bitcoin (or wallet) addresses. These addresses are used in Bitcoin transactions. A transaction comprises inputs and outputs. An output of a transaction is assigned to a wallet address. An input of a transaction is a prior (and yet unused) transaction output. In the paper, we will use their first 5 symbols to represent both wallet addresses and transaction hashes, and the latter are underlined. Some addresses are further highlighted in bold font, because they play a key role in our discussion of the analysis. Refer to Tables 4 and 5 in the Appendix for the corresponding complete address and transaction hashes.

2 Case study: A March 2019 Sextortion Campaign

There is a plethora of online scams and extortion schemes. Some involve malicious softwares, others are purely confidence tricks, or a combination of both. Ransomwares typically make users' access to data or services unavailable, spywares steal user's data, while leakwares steal data and threaten to expose confidential data. For example, in response to US city mayors' resolution not to pay ransoms [1], cyber-criminals threatened to leak stolen data [2]. There are scarewares, which create a perception of threat to manipulate user behavior, for instance, 'buy fake protection', while in other occasions, the criminals simply deceive the victim without ever compromising the security of their computing infrastructure at all, e.g., just make believe the user that some compromising information is known to the attacker, and extort based on this perception.

Cryptocurrencies such as Bitcoin are used to collect ransoms in many variations of such scams - including in the cases involving malwares such as ransomwares and leakwares, as well as other scenarios where even though no information might be stolen, a perception of threat is somehow created. Sextortions is a subclass of such extortions, where the attacker convinces the victim that some sexually compromising information is available to the attacker. This is often a bluff (as was the case for the specific case study investigated in this paper), but it may also be true in some occasions, and the cyber-criminals may leverage on data breaches and leakwares, including breaches at third party sites, to create such perceptions of threat.

2.1 Bitcoin Extortions: Ransomwares and Blackmail Scams

Extortion campaigns enabled by the Bitcoin ecosystem can be broadly categorized into ransomwares and blackmail scams. In both cases victims are coerced to deposit a ransom into a Bitcoin address. However, they differ on the fact that a ransomware actually disables access to the victim's data (there is no doubt that the attack happened), while blackmail scams mostly rely on making a victim believe that the attacker knows something critical about him/her (which is not necessarily true). A consequence is that targeted victims of ransomwares have already been compromised, and there is a tendency to thus hide that they got breached (e.g., it could be a reputation damage for a company, or victim shame).

In contrast, targeted individuals who do not fall prey to a blackmail scam often 'retaliate' by publicizing the Bitcoin address and/or blackmail email content (though nothing prevents a scammer to create noise by reporting legitimate addresses as being fraudulent ones). There is thus a difference in methodology in getting Bitcoin 'seed' addresses, the first addresses needed to start the forensics analysis. Because of the financial impact of ransomwares on companies, the cybersecurity industry has greater (financial) interests in investigating and understanding ransomwares, which is echoed in the curation of datasets by different interest groups (e.g. Locky ransomware data is provided by the Anti-Phishing Working Group [27]), which would otherwise have been difficult to obtain. [15] uses ransomware binaries to deliberately infect controlled (virtual) machines, to generate fake victims, and thus try to identify Bitcoin addresses used by extortionists to collect ransoms. Data on scams is scattered across different forums. While certain third party entities, e.g., ISPs, companies providing email spam filtering products, etc. may have access to further relevant information, this is often not readily available in the public domain. The first step in carrying out a Bitcoin scam forensics analysis without access to any specific proprietary data is thus to gather, from different blogs and forums, Bitcoin addresses that can be used as seed addresses.

There have been several waves of extortion scams (see e.g. [13, 35]), and they continue to proliferate for several reasons: (1) horde of personal data is easily available (e.g. from data breaches) to nefarious actors, which makes it easy to carry out personalized and targeted scams, (2) this form of attack requires very little technical skills or resources on the part of the attackers who can use readily and cheaply available tools and services, and finally, (3) they are very lucrative, several thousands of dollars could be obtained even from just one or two victims. We chose to focus and gather information on one particular such sextortion campaign from March 2019 [22, 34] (the term 'sextortion' in this context is used to refer to blackmail campaigns based on supposedly compromising information about the victim, typically involving watching pornography, though other interpretations of the term exist, as discussed earlier in the paper).

The rationale for considering this particular campaign is that: (1) It has attracted attention for being lucrative and recurrent. This is likely because cybercriminals share with the intended target his/her email login and password, to claim that the target's personal devices and network were breached (even though, the login/password information was obtained by breaching a 3rd party website, often by more sophisticated criminal groups, who then sell the stolen data to the lower rung cybercriminals). The fact that several victims pay means abundant traces of the attacks are available on the blockchain. (2) Some preliminary studies are available for points of comparison, which also helps in gathering seed addresses. (3) It is recent, therefore attackers could possibly have tried to hide their traces using decentralized protocols (such as Coinjoin [14], a protocol for combining several Bitcoin payments from diverse spenders into a single transaction), mixing services (also called tumblers, which are services that mix possibly identifiable cryptocurrency funds with others, leading to a similar effect

as of mixing), or shape shifting [9, 36], a technique that consists of moving the funds across different cryptocurrencies. Study of data sets from earlier periods [32, 31] were unencumbered with the possibility of such additional obfuscation mechanisms. In contrast, the data set studied in this work is from a time where all these techniques are being deployed by savvy cybercriminals (but that is still not necessarily the case for our dataset). Our flow based graph traversal approach is expected to be robust in the presence of mixing, however, shape shifting is outside the scope of the proposed approach.

2.2 Prior Findings

We first summarize the findings [22, 34] that have already been reported for the particular March 2019 sextortion campaign we study. This allows us to present commonly used heuristics such as aggregation of multiple inputs to a transaction [25, 32]. Addressing some of the shortcomings and limitations acknowledged in [22, 34] partly motivates our approach.

The investigation [22] starts with the Bitcoin address 163qc mentioned in a reported extortion email. As of end of March 2019, it received money from only two addresses, amounting 0.25924622 BTC (worth ≈USD 1000 on 13th March 2019 when the wallet was emptied out), which it forwarded to **3HXdb** in the transaction 94c86. Each of the two transactions in which 163qc actually received money involved a single address making payments to many addresses. It is thus unclear whether the Bitcoins received by 163qc were directly from extortion victims, or other funds being channeled by the extortionists themselves. However 163qc has been reported on the online Bitcoin Abuse Database [7] on many occasions spanning a long period of times for similar extortion attempts. This gives credence to the initial assumption made in [22].

The transaction 94c86 where 163qc forwards its money to **3HXdb** comprises 14 unique addresses including 163qc as inputs, and no other output address. Thus, following the multiple-input heuristic, one can aggregate the 14 input wallet addresses and **3HXdb**. There are in fact 11 additional similar transactions in which **3HXdb** received Bitcoins. This indicates a generic pattern which was observed in a recent study of the ransomware ecosystem [27], where it was noted that often the extorted money is first funneled into a 'collector' wallet. Note that each transaction involving the identified collector **3HXdb** thus yields a set of addresses that can be grouped together, and the union of these sets all are determined to belong to the same entity by a logic of transitivity. This yielded 80 unique input addresses, and one can also determine that the collector **3HXdb** gathered 21.6847451 BTC, which was roughly 80,000 USD as per the BTC exchange rate in mid-March 2019. Then **3HXdb** funneled Bitcoins through 12 transactions, each with two output addresses. The analysts [22] conclude by stating (we quote verbatim) 'Further analysis past the consolidation address becomes difficult as the thieves begin a laundering process to hide their illicit gains by splitting and mixing the stolen funds.'

Nevertheless, if one tries to follow the money trail manually, for instance by taking one of the outputs, namely 39rvS, from the latest outflows from **3HXdb**,

one would observe that this goes to **bc1qq**, a SegWit address. Such addresses are not supported (yet) by all wallets. It is also difficult (as of 2nd May 2020) to navigate this information on many popular blockchain explorers such as `https://www.blockchain.com/`.

In fact, [34] traces some of the flows to **1NDyJ** and identifies it as a consolidation address. As per the original writing of [34], an estimate of 6,229,301.73 BTC (≈68,787,064,396.14 USD) of transactions were attributed to **1NDyJ** in [34]. Incidentally, as of 21st September 2019, Bitcoin Abuse Database [7] and Bitcoin Whos Who [8] also consider **1NDyJ** to be fraudulent because it has been reported for scams. Several other 'consolidation' addresses were also identified in that original post [34]. However, in an update dated 2019-08-05, the analyst states (we quote verbatim) 'I am being told that my methodology was faulty and that some of these are BTC wallets are known valid. This clearly needs more investigation. Sorry!' This illustrates how complicated Bitcoin forensics is with currently available tools to process the information, and the consequent risk of jumping to misleading conclusions: **1NDyJ** actually belongs to Binance (as claimed by Binance through their official Twitter handle [5]), which is one of the largest cryptocurrency exchanges. Unsurprisingly, it transacts humongous volumes of Bitcoins, arguably coming from both good and bad sources.

2.3 A Motivating Example: The Junction Conjecture

The idea of finding out which consolidation addresses are being used by the scammers to transfer the money to an exchange (or tumbler) has merit.

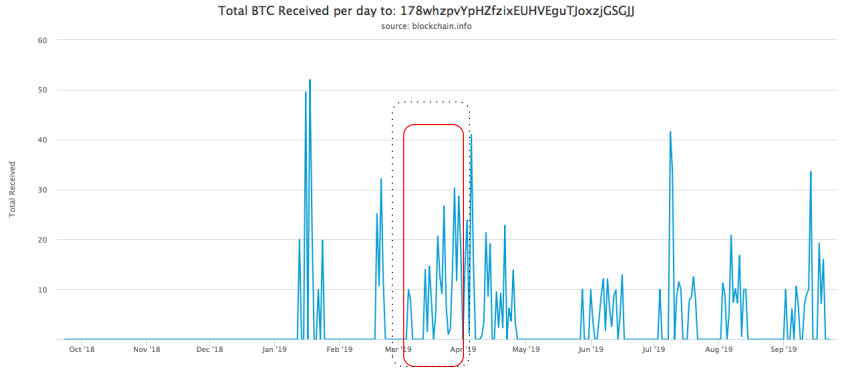


Fig. 2. Bitcoin reception pattern of **178wh** (source: blockchain.info). The inner box highlights the period over which we have confirmed reports of sextortion events, while the outer box represents the period of data we used in this study.

In the current example, one of the flows out of **3HXdb** involves **178wh** as the address immediately before the exchange address **1NDyJ**. Looking at the temporal Bitcoin reception pattern of **178wh** (as shown in Figure 2), we observe

that **178wh** has been intermittently active in bursts, including during the period of the specific extortion campaign being studied. This suggests to systematically check whether we can trace other flows to **178wh** to determine if it acts as a junction between the scammers, and the cryptocurrency exchange. As stated in [22], (manually) following all the branches of Bitcoin flows is difficult. However only studying the individual transactions or addresses separately seclude analysts from the bigger picture, and in some cases lead to wrong conclusions [34]. This motivates the design of heuristics to aide algorithmic explorations of the graph induced by wallet addresses and transactions.

3 Data Representation: A Two-mode Network Model

Information from Bitcoin transactions can be encapsulated using different network models. The choice of representation is determined by and in turn constrains or facilitates certain sorts of analyses. In [31] these representations are broadly classified as (i) a directed network of wallet addresses (e.g.,[18, 32, 31]), (ii) a directed network of transactions (e.g., [31]) and (iii) a two-mode (heterogeneous) directed network comprising nodes of two kinds, wallet addresses and transactions (e.g., used in [6] for the purpose of visualization with some basic filtering options, such as showing only transactions involving a certain amount).

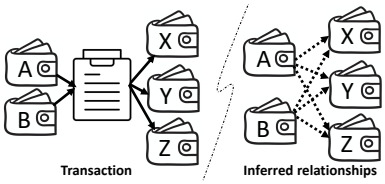


Fig. 3. From a transaction with inputs from wallet addresses A and B, and with outputs to wallets X, Y and Z, because of the obfuscation technique of the Bitcoin protocol, one can infer only a 'noisy' relation information, that Bitcoin(s) from A might have been paid to one or several of X, Y and Z, and likewise for B.

The wallet address network, which is arguably the most frequently analyzed Bitcoin network, is constructed as follows [18]: Each wallet address which contributes as an input to a given transaction is connected to every wallet address which receives any output from said transaction. This process provides a wallet-centric viewpoint which has the advantage of consolidating Bitcoin flows by addresses, yet it has several downsides. Foremost, this process is noisy: not all the inputs of a transaction may actually have any relation with all the outputs of the transaction (in particular, in the case of mixing or a currency exchange), and yet numerous relationships (product of the in/out-degrees of the transactions) are perceived. An elaborative example is depicted in Figure 3. In this example, the transaction inputs are derived from wallet addresses A and B. Because of

the nature of obfuscation created by design in the Bitcoin protocol [24], one cannot in general unambiguously determine which outputs are derived from which inputs. As such, each of A and B might have paid any or several of the wallet addresses X, Y and Z. Then by design, all occurrences of a given address are collapsed with a single representation of the wallet address. This process loses information, for instance, which subset of neighboring addresses does it interact in separate instances. The wallet address network is useful for certain analysis scenarios, but it is inadequate for others, e.g., if we want to identify the specific nodes involved in particular subset of transactions.

We chose as model a two-mode network where multiple involvements of an individual wallet address are retained as separate node instances. By the nature of Bitcoin transactions, a transaction node remains unique in this representation.

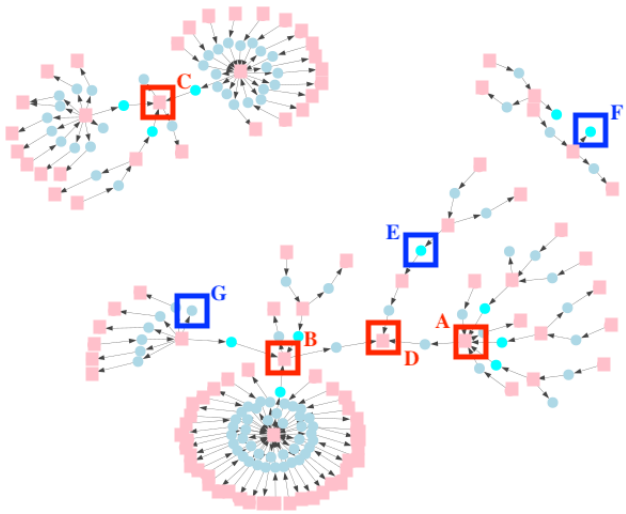


Fig. 4. A two-mode network example: Ego-centric view for **1AELp**.

Figure 4 shows an example of a two-mode subnetwork derived from our dataset (refer also to Figure 6 for another synthetic but simpler example), comprising nodes within a distance of three (over an undirected representation) of the wallet address **1AELp**. The transaction nodes are represented in pink (highlighted in this figure also using a square shape), while the wallet address nodes are in blue, in a round shape, with a distinctive cyan coloring for highlighting the ego **1AELp** of the network. This representation is well suited to understand individual flows. For example, in the transaction box-A (in the figure), **1AELp** is consolidating some of its fund (but also again branching it out). Similar consolidations are happening in transactions highlighted in box-B and box-C. Also, one of the branches from box-B and the branch from box-A meet a third flow

also originating from **1AELp** (shown as box-E) in transaction box-D. Increasing the radius of the network allows one to follow these flows once they leave box-D.

Some of the Bitcoins that **1AELp** received remain unspent (e.g., box-F: there is no outgoing edge) within the period of our study. In fact **1AELp** was indeed in receipt of Bitcoins on 4th April 2019 (the last day of our studied period), which remained unspent within that period. Eventually, all funds at **1AELp** were emptied out on 13 April 2019, which was the last transaction of **1AELp** as of 21 September 2019. Box-G shows another wallet address, which similarly had unspent funds in that period.

To study the March 2019 sextortion campaign, we build a two-mode graph with the node **3HXdb** which was identified as a collector [22] as ego. To do so, we extracted from the Blockchain the raw information for the time period of interest. This was done by installing a Bitcoin client. We then processed the data so it can be uploaded and stored in the Neo4j graph database. We did so by mapping the obtained raw information in the aforementioned two-mode network model, representing transaction nodes linked to wallet address nodes involved in said transactions. This representation allowed us to discern each occurrence of a wallet address node, which we used to extract ego-networks with a given radius (e.g., as shown in Figure 4). This radius was chosen such that all instances of ego-networks of an individual wallet address of interest connect to each other, resulting in a single network. In the Appendix we report several nodes that stand out in this network, namely addresses which appear particularly often, and transactions with (very) high out-degree, more than 100, ranging up to more than 3500. The heuristics presented next were tested on this graph.

4 Sextortion Case study Revisited

We will like to preface the upcoming analysis with a disclaimer. Forensic analysis of Bitcoin transactions is difficult, and inferring things wrongly because of a misinterpretation or due to lack of adequate information is very easy (case in point: [34]). We may also be wrong in some of our conclusions, and there is no full-proof mechanism to validate the hypothesis. Thus while the approach is meaningful intuitively, and takes into account typical real world behavior, and likewise the data analyzed is real, our inferences are best treated as speculative.

4.1 A Motivating Example Continued

In Subsection 2.3, we identified a flow of money from **3HXdb** which reached **1NDyJ** (known to belong to the Binance cryptocurrency exchange) via **178wh** being the wallet address immediately preceding the exchange **1NDyJ**. Given its special position in the transaction flow, as well as **178wh**'s temporal activity pattern and preponderance of transactions with **1NDyJ**, we wanted to determine whether there are other flows that branch out from **3HXdb** which are subsequently consolidated at **178wh**. The two-mode network model helps discern such individual flows, in contrast to the wallet address network model [18],

which would have collapsed multiple instances of common path segments in distinct flows (it might also have created spurious paths because of the introduction of noise in the address-address relationships).

Specifically, we found five distinct flow branches from **3HXdb** that merge and arrive at **178wh**: one path each of lengths 3,4 and 6, and two paths of length 5. Three of these paths merge already at **bc1qq**. An overview of these flows among different wallet addresses is depicted in Figure 5 (each unique wallet address is represented with a single node in this figure). The complete paths are provided in Table 1.

Table 1. Sequence of wallet addresses in distinct paths between **3HXdb** to **178wh**.

3GHTBKpBoAsSr5cWw975nCbNbu5ku4swEh
3C8pHQZ1yigTdXDRbMLarJhCX5o5Am7MFt
3KEvWguGq9Bc6CgTUk3vLTAXwn2x5waYz8
bc1q0ypwlg24nn5wj8phnrcgvnv2ss43pz6auw85rm
3MNXVhRDyCBeqBDe8eXHx1dHUPPxDA5aso
3KmVfeXZf3cUY8Q4eZ6QzeQhGDZM8sQqUG
bc1qqvh3lhkhcxhpnhmh0uv6plvlqtymejsuj2t8vd
3ErKQRHjZxjH3tuFCh39RCnA7FLUCSNVmE
32ae9v8v69MDdim6ZadNfS25qC3Uf3rXCG
39N5MaJo7MJBYq33FZdVCfEXQsvT5SWuTe
3FFP8mTpoW5B6Y8W3edKrV5QWdJdKMGvhH
bc1qqvh3lhkhcxhpnhmh0uv6plvlqtymejsuj2t8vd
3ExisQ59Bf146v3itwaAYFXZHMJH1zAjTR
3JxYm5GDAUpZZdkGCMPFp3ZKFidwMN3KGj
3MRJ25rcUkoTv9ufviwFec9z4Dx2aqUeTU
bc1q7z8r7g893s8g7054dn8lcadrjmsz4ytv8flnj4
39rVSdvsf5oHYVkvkwUHKrQ9V9R7mY4Boy
bc1qqvh3lhkhcxhpnhmh0uv6plvlqtymejsuj2t8vd

The existence of multiple such flows to **178wh** from the collector address **3HXdb** provides evidence in favor of the hypothesis that **178wh** is a wallet address under the control of the scammers, and **178wh** acts as a junction where the Bitcoins move from addresses controlled by the scammers to the exchange (Binance). Identification of **178wh** being potentially a go-to address that the scammers use to exchange their funds is useful in several manners: (i) If Binance has proper 'know your customer' (KYC) mechanisms and co-operate (or, depending on jurisdictions, is compelled to co-operate), law enforcement agencies would be able to obtain further leads about the particular cybercriminals-criminals who carried out the sextortion campaign. (ii) The temporal activity pattern (shown in Figure 2) indicates an almost monthly wave of activities, which suggests regular waves of extortion campaigns. Accordingly, tracing back the money flows in those other periods to known (reported) wallet addresses extorting money in

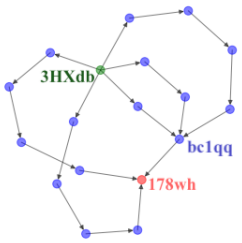


Fig. 5. A wallet address graph view tracing five distinct flows from **3HXdb** to **178wh**. Three merge at **bc1qq**.

the corresponding periods would be an interesting future work, and would help further reinforce the current inference.

4.2 Flow Branchifications and Mergers

We now elaborate the details of our flow based graph traversal mechanism with which we found the distinct paths between **3HXdb** and **178wh** exhibited above.

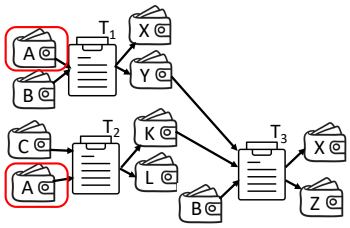
The two-mode network represents each instance of a given wallet address as a distinct node. Therefore whenever multiple instances of a wallet address appears in the network, we are looking at merging of flows initiated at these address instances. An example is shown in Figure 6 with wallet 'A' being the wallet of interest, from which the flows are being traced.

This is done algorithmically by proposing a flow based graph transversal, which consists of setting these address instances as roots of trees, and by letting the trees grow one step at a time, letting the branches go alternately at each step through transaction and address nodes, until any two branches merge. At step 0 of the algorithm we thus have isolated points, recorded in a set S_0. At step 1, each address instance is connected as an input to a given transaction, forming a set S_1. A merging could already happen if two instances are both inputs to the same transaction. This iteratively builds a set S_i given by

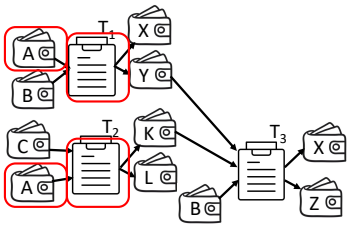
$$S_i = \{v \text{ such that } (u, v) \in E,\ u \in S_{i-1}\},$$

where E denotes the set of edges of the two-mode network, inducing a forest whose number of connected components (understood as undirected graphs) starts as the number of roots. At every iteration of the algorithm, we count how many connected components are present. Whenever the number is less than the number of connected components in the previous iteration, it indicates that merger(s) has/have happened, giving some node of interest to be looked at. The algorithm is described in Algorithm 1. The condition of the while loop can be adjusted to include more mergings than the first one.

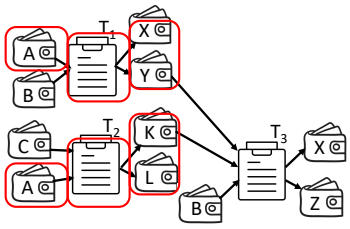
Other special nodes include (very) high degree nodes, which are indicators of reaching an exchange or a tumbler. The process of flow based graph traversal



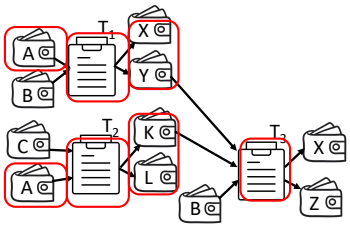
(a) The address A is used twice. The set S_0 contains these two nodes.



(b) Each instance of A is the input of a transaction. The set S_1 contains T_1, T_2.



(c) Each transaction which is an output of A leads to two wallet addresses.



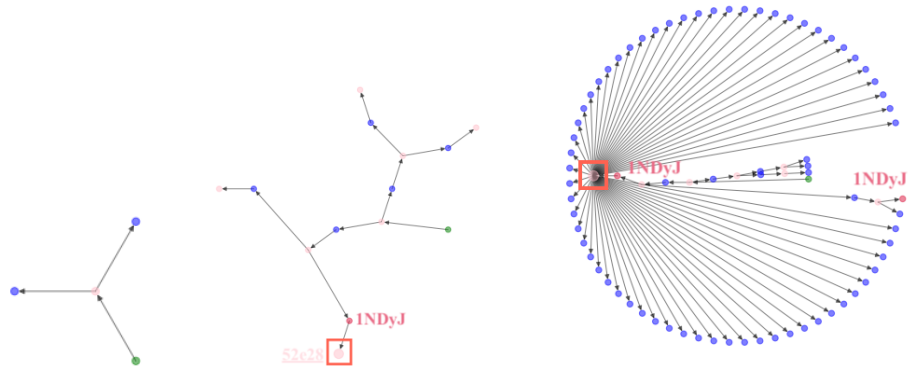
(d) Flows initiated at A merge at transaction T_3.

Fig. 6. An illustration of the proposed flow based graph transversal.

Algorithm 1

Let $S_{-1} = S_0$ be the set of nodes containing instances of the Bitcoin address of interest.
Let $ncc(S_0)$ be the number of undirected connected components generated by the vertices in S_0.
$i := 0$.
while $ncc(S_i) = ncc(S_{i-1})$ **do**
  $i := i + 1$
  $S_i = \{v$ such that $(u, v) \in E,\ u \in S_{i-1}\}$, for E the set of edges of the two-mode network.
end while

used here has similarities to the one used in BitConeView [12]. In that work, the graph studied comprised only the transaction nodes, in contrast to our use of the two-mode network; that study was thus useful for tracing the flow of the Bitcoins themselves, while our emphasis is to study the wallet addresses individually. The flow of the Bitcoins is naturally subsumed in our analysis. The intuition of flow mergers being used as an evidence of relationship may be interpreted as a dual to the social network mining task of link prediction [20, 4].



(a) Two steps (b) Five steps (c) Six steps

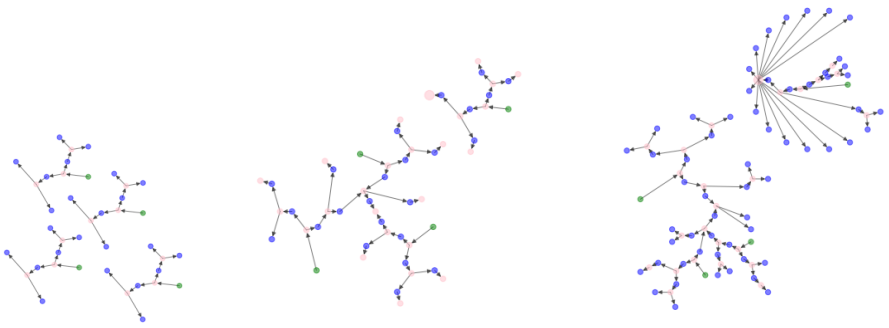
Fig. 7. Illustration of the process of growing trees.

We illustrate the above algorithm by studying the flows branching out of **3HXdb**. There were 12 transactions in which **3HXdb** participated as input, and the outputs from these transactions created branching of the flows. These twelve occurrences of the wallet address **3HXdb** form 12 roots, growing into trees whose branches trace how the flows propagate across the network, and whether and where they merge. For the ease of exposition and knowing prospectively how the flows actually merge, we have separated these twelve **3HXdb** instances in smaller groups, and show some of these smaller groups in Figures 7-8.

In Figure 7, we show a single instantiation of **3HXdb** (out of the 12) as an *ego* node (shown in green), to illustrate the transversal algorithm, where we gradually expand and explore the vicinity of the network of an *ego* node. In Figure 7a we show the first two steps. Since we use a two-mode network representation, the first step is simply to the transaction node (shown in pink), to which this instance of **3HXdb** is (an) input. At the second step, we thus essentially see how the flow is being branched into two other wallet addresses (shown in blue). The path from **3HXdb** to the transaction 52e28 is given by: **3HXdb** → 466ef → 16p7u → 61dca → **1NDyJ** → 52e28. This path is also branching at 61dca, following this branch leads to the following path: 61dca→358E8 → 89420→ **1NDyJ**. The wallet address **1NDyJ** (belonging to the cryptocurrency exchange Binance) and

the transaction 52e28 (boxed) are highlighted in Figures 7b & 7c. The branch reaching the exchange stops, but other branches could be further expanded.

We next illustrate the merger of flows by looking at other instantiations of **3HXdb** (out of the 12).



(a) Four steps (b) Five steps (c) Six steps

Fig. 8. Illustration of the process of flow mergers.

We start with four instances of **3HXdb**, shown in green in Figure 8. We choose these four instances as the egos, because, up to a horizon of four steps (Figure 8a), one can observe an identical network pattern - which suggests that the launderers (sometimes) use certain templates for the branching process (be it manually or with some automation tools). By the fifth step, three of these flows merge at two different transactions (boxed): one of these transaction happen to be three steps from one of these ego instances, as can be seen in Figure 8b. Figure 8c shows the snapshot after six steps. We observe that the consolidated funds are again undergoing branching (encircled). We have used identical colors for the boxes and circles across Figures 8b & 8c to cross-refer the individual nodes highlighted in the two snapshots. The eventual merging point of the three flows is 020be. The path from **3HXdb** at 020be is given by: **3HXdb**→ e5492→1AXKg→ 2918a→ 17XVP → d2ae0 → 19hAV → 020be. The path from **3HXdb** at 020be is given by: **3HXdb**→ da4df→19j7C→ d2ae0→ 19hAV → 020be. These two both branches merge already at the transaction d2ae0. The third branch however indeed merges only at 020be: **3HXdb**→ 9a3b5→38Yb9→ 7e681→ 1BjiY → 020be.

At this stage, the fourth instance of the ego network remains isolated but one of its branches goes to the wallet address **3BK5N** (which is the input of a high out-degree transaction 99e4b) following the path: **3HXdb** → 929e2 → 35n3Q → 92d56 → **3BK5N**. As shown in Figure 9, one of the branches from this instance of the **3HXdb** ego network too merges with other flows emanating out of **3HXdb** subsequently. The snapshot from Figure 8c further led us to another interesting finding. The transaction 99e4b had only a single input **3BK5N**, but

it was worth 44.66240606 BTC which was approximately USD 440,000 on 13 March 2019. This is so because, aside from the flow originating from **3HXdb**, the wallet address **3BK5N** consolidated funds through 116 other unique wallet addresses (these other flows to **3BK5N** are not shown in the Figure 8).

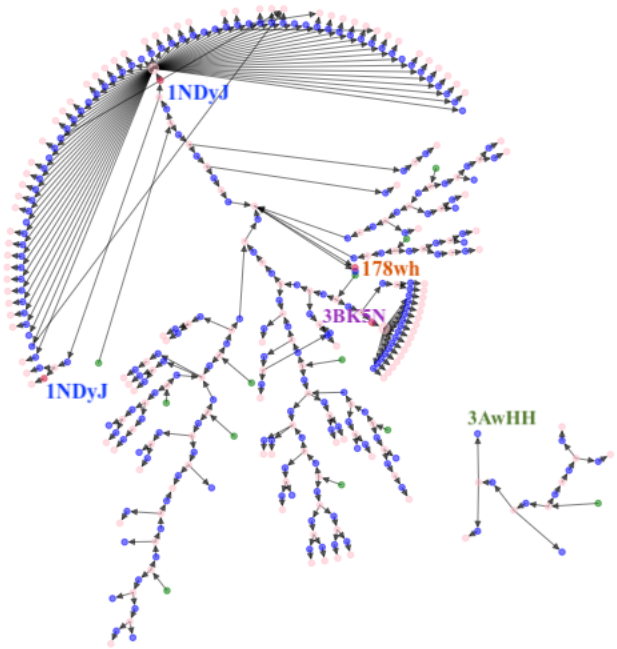


Fig. 9. Flows from eleven of the twelve instances of **3HXdb** merge in seven steps.

We see from Figure 9 that flows from eleven of the twelve instances (shown in green) of **3HXdb** merge within seven steps in the two-mode network. We highlight some of the interesting nodes we have previously discussed (along with their addresses). The Binance wallet address **1NDyJ** appears twice within this horizon of the ego network, which corresponds to the two occurrences we had observed in Figure 7. The wallet address **178wh** appears only once and is a leaf node in the presented view. This instance essentially corresponds to the wallet address network path of length three between **3HXdb** and **178wh** from Figure 5. Outgoing edge from this instance of **178wh** to a new instance of **1NDyJ**, and other instances of **178wh** would be visible only when a network with a larger horizon is created. Incidentally, since **1NDyJ** corresponds to the Binance

exchange, and there is also the large volume of branching through **3BK5N**, the view with any larger horizon gets cluttered by an explosion of the number of nodes (which is why Figure 9 is restricted to the current horizon of seven steps).

We notice that one of the twelve instances remains detached. Furthermore, in that instance, two flows appear to not even go the whole seven steps. This is because these wallet addresses just happen not to have spent the received funds within the time frame of our study. We highlight as example the address 3AeHH. This address received the funds on 15th March 2019, however 3AeHH spent it only on 24th May 2019.

5 One Scam, Multiple Manifests?

Sextortion campaigns have been coming in different waves over time, and in different flavors: extortionists change the language, the phrasing, the wording of the threat. See e.g. [29] for a collection of such examples of emails. In fact, the address **1AELp** we used previously in Section 3 to introduce our two-mode network model is an address we identified from [7] to have predominantly targeted francophones during the same time period as our current study.

Thus one may wonder whether the same group is randomizing email phrasings, or whether different groups are operating using the same techniques, and even reusing the same phrasings. A first indicator could be the timeline, though arguably a group of attackers could phase their campaigns, while on the other hand, a group could be "inspired" to start its own attack after witnessing the attack of another group, leading to multiple distinct groups carrying out similar blackmail campaigns simultaneously.

To gather data regarding different blackmail campaigns, we wrote a small Python tool[4] which first crawls relevant webpages based on keyword searches using (combinations of) words such as "Bitcoin", "scam", "blackmail", "secret", "webcam" and distinctive phrases (e.g. 'is fair price for our little secret') that we noted from the samples of sextortion emails, and then scrape the content of each such a page and extract the found Bitcoin addresses. We found reports for **1AELp** containing the phrase 'est un juste prix pour notre petit secret', which is what we obtain by translating the English phrase on Google translate as on 21st September 2019. Different online forums gave a set of Bitcoin addresses reported as being involved in sextortions. We then look for them in the data/period considered (block height range 564671-570195) and found four addresses **1AELp**, **1L47w**, **1PAco** and **12s4c** which had no immediate relations with the addresses we discovered from the study above.

Considering the two-mode graph as undirected, we look for paths among these four addresses and **3HXdb**. Finding directed paths is a valuable indicator, but the nature of the two-mode graph is such that having a 'flip' in the directionality may still be an indicator of a relationship among flows, and thus, among addresses associated with the flows: given two address nodes a, a' and a

[4] Our tool uses the Python library Beautifulsoup4.

transaction node t, a flow through the directed edges $(a,t),(t,a')$ indeed means a flow from a to a' through t, but having edges $(a,t),(a',t)$ means that the flows coming from a and a' are merging at the transaction t, which is also a valuable indicator. Similarly, edges $(t,a),(t,a')$ mean that both a,a' are out-going addresses of the transaction t, which could be result of a split of some flow at t.

We thus provide a two-step analysis of the paths among scam addresses.

Step 1. We look at short (undirected) paths among them in the two-mode network.

Steo 2, We single out paths with few 'flips'.

Table 2 summarizes connections among scam addresses in terms of shortest undirected paths. We only use a snapshot of the Bitcoin blockchain, thus these numbers are bounds and more (or shorter) paths might exist. Since the paths are undirected, the table is symmetric (we only indicate the upper diagonal elements). The number of shortest paths between each pair is reported, along with the corresponding path length, which varies between 6 and 16. Since the number of hops count both transaction and address nodes, a length of 6 means three transactions and three wallet addresses. Thus the pair **1PAco**, **12s4c** looks close, with fifteen paths of length 6. For the pair **1PAco**, **1AELp**, we argue that by transitivity, since we can reach **1PAco** from **1AELp** via e.g. **12s4c**, we get $15 \cdot 3$ paths of length $6+8=14$. Also **1L47w** is arguably the closest to **3HXdb**, since we found 28 paths of length 14.

Table 2. Undirected short paths between scam addresses identified from diverse sources, and with no a priori immediately identifiable relationships.

	1AELp	**1L47w**	**1PAco**	**12s4c**	**3HXdb**
1AELp	-	2 paths, length 14	45 paths length 14	3 paths, length 8	9 paths, length 12
1L47w		-	39 paths, length 16	10 paths, length 14	28 paths, length 14
1PAco			-	15 paths, length 6	12 paths, length 12
12s4c				-	3 paths, length 10
3HXdb					-

When considering 'flips' in the paths, we do not focus on finding the shortest paths, but rather the paths with the least number of 'flips'. Our finding is that per this measure, **1L47w** is also the closest to **3HXdb**, since there are paths of length 16 (we found 4), with only 2 flips. We also found one path between **12s4c** and **1L47w** of length 14 with 2 flips. Note that all flips we identified happened at transaction nodes.

Table 3 shows the number of paths among these nodes but with three flips.

Table 3. Number of undirected paths with 3 flips between scam addresses identified from diverse sources, and with no a priori immediately identifiable relationships.

	1AELp	**1L47w**	**1PAco**	**12s4c**	**3HXdb**
1AELp	-	1	0	6	1
1L47w		-	0	4	41
1PAco			-	40	3
12s4c				-	21
3HXdb					-

The evidence of connections we were able to find among these five addresses are not wholly conclusive on their own. Nevertheless, this is an additional aspect of circumstantial evidence, that can be added along with the other circumstantial evidences of temporal coincidence and linguistic similarities of the blackmail campaigns. The presence of so many (not so long) paths among these addresses together with multiple paths with few flips overall prompt us to conclude that these wallet addresses with no a priori immediately identifiable relationships indeed belong to either a single group or co-ordinated groups. Carrying out a more rigorous study of relationship among similar scams using a more systematically gathered dataset is how we expect to extend the current work in future.

6 Concluding remarks

Popular Bitcoin forensics heuristics [30, 23, 32] tend to be based on local information at individual nodes (such as input/output of a given transaction). We argue that nearby graph structures and paths can complement the known heuristics by helping to trace the money flow behavior and in turn determine further relations among Bitcoin addresses. We provided two algorithms: one based on trees growing and eventually merging, and one based on computing distances between addresses, taking into account "flips" of direction (characteristics of two flows merging or branching at a transaction) rather than directed paths. Both algorithms were demonstrated on a sextortion case that happened in March 2019. Considering as tree roots instances of a collector address, we followed its outgoing flows to wallet addresses of interest, including the exchange Binance, and possible go-to addresses for the scammers. With the case study, we demonstrate that the methodology designed in this paper facilitates the identification of Bitcoin wallet addresses that might be under the control of a single entity based on the orchestration of the flow of the Bitcoins, in a novel manner distinct from and complementary to existing popular wallet address agglomeration heuristics. Furthermore, starting from Bitcoin addresses possibly belonging to different sextortion scams, we found a number of both short paths and short paths with few flips, suggest ting proximity among the disparate addresses, thereby indicating a greater likelihood of them belonging to a single group of cybercriminals.

The presented work suggests multiple avenues for future work. We want to carry out a more extensive study of whether scams that are identical or are very

minor variants, but have been carried out in sextortion campaigns spanning different time periods over multiple years are linked to same criminal organization. We will also like to investigate whether other kinds of scams can be linked to the identified suspect Bitcoin wallet addresses. Furthermore, we want to apply our methodology to existing data sets from other third party studies of tracing tainted Bitcoins, both to compare with and enhance the findings of those studies. This will also lay out a pathway for integrating such complementary approaches for designing a more robust Bitcoin forensics toolkit. Finally, a probabilistic study of the path lengths among tainted addresses could provide a theoretical way to identify anomalies.

References

1. C. Cimpanu: US mayors group adopts resolution not to pay any more ransoms to hackers (2019), https://www.zdnet.com/article/us-mayors-group-adopts-resolution-not-to-pay-any-more-ransoms-to-hackers/ (accessed on May 2, 2020).
2. L. Tung: Ransomware: Cybercriminals are adding a new twist to their demands (2019), https://www.zdnet.com/article/ransomware-cybercriminals-are-adding-a-new-twist-to-their-demands/ (accessed on May 2, 2020).
3. C.G. Akcora, Y. Li, Y.R. Gel, M. Kantarcioglu: Bitcoinheist: Topological data analysis for ransomware detection on the bitcoin blockchain. In: arXiv. No. 1906.07852 (2019).
4. J. Ayoub, D. Lotfi, M. El Marraki, A. Hammouch: Accurate link prediction method based on path length between a pair of unlinked nodes and their degree. Social Network Analysis and Mining **10**(1), 9 (2020).
5. Binance: https://twitter.com/binance/status/961666467325358081 (accessed on May 2, 2020).
6. S. Bistarelli, F. Santini: Go with the -bitcoin- flow, with visual analytics. International Conference on Availability, Reliability & Security (ARES) (2017).
7. BitcoinAbuse.com: Bitcoin abuse database, https://www.bitcoinabuse.com/ (accessed on March 3, 2020).
8. BitcoinWhosWho.com: Bitcoin whos who, https://bitcoinwhoswho.com (accessed on March 3, 2020).
9. N. Borggren, G. Koplik, P. Bendich, J. Harer: Deanonymizing shapeshift: Linking transactions across multiple blockchains (2017).
10. E. Bursztein, K. McRoberts, L. Invernizzi: Tracking desktop ransomware payments. Black Hat USA presentation, Las Vegas, United States (2017).
11. S. Catanese, E. Ferrara, G. Fiumara: Forensic analysis of phone call networks. Social Network Analysis and Mining **3**(1), 15–33 (2013).
12. G. Di Battista, V. Di Donato, M. Patrignani, M. Pizzonia, V. Roselli, R. Tamassia: Bitconeview: visualization of flows in the bitcoin transaction graph. IEEE Symposium on Visualization for Cyber Security (VizSec) (2015).
13. Digital Shadows: A tale of epic extortions: How cybercriminals monetize our online exposure. Digital Shadows Report. https://resources.digitalshadows.com/whitepapers-and-reports/a-tale-of-epic-extortions-how-cybercriminals-monetize-our-online-exposure (accessed on March 3, 2020).

14. Gmaxwell: Coinjoin: Bitcoin privacy for the real world. https://bitcointalk.org/?topic=279249 (2013) (accessed on March 3, 2020).
15. D.Y. Huang, M.M. Aliapoulios, V.G. Li, L. Invernizzi, K. McRoberts, E. Bursztein, J. Levin, K. Levchenko, A.C. Snoeren, D. McCoy: Tracking ransomware end-to-end. IEEE Symposium on Security and Privacy (2018).
16. M. Huber, M. Mulazzani, M. Leithner, S. Schrittwieser, G. Wondracek, E. Weippl: Social snapshots: Digital forensics for online social networks. 27th annual computer security applications conference (2011).
17. A. Kharraz, W.K. Robertson, D. Balzarotti, L. Bilge, E. Kirda: Cutting the gordian knot: A look under the hood of ransomware attacks. International Conference on Detection of Intrusions and Malware, andVulnerability Assessment (2015).
18. D. Kondor, M. Pósfai, I. Csabai, G. Vattay: Do the rich get richer? an empirical analysis of the bitcoin transaction network. PLoS ONE **9**(2) (2014).
19. K. Liao, Z. Zhao, A, Doupé, G.J. Ahn: Behind closeddoors: Measurement and analysis of cryptolocker ransoms in bitcoin. IEEE APWG Symposium on Electronic Crime Research (eCrime) (2016).
20. D. Liben-Nowell, J. Kleinberg: The link-prediction problem for social networks. Journal of the American society for information science and technology **58**(7), 1019–1031 (2007).
21. Malwarebytes: Malwarebytes Labs blog, `https://blog.malwarebytes.com/cybercrime/2019/02/sextortion-bitcoin-scam-makes-unwelcome-return` (accessed on March 3, 2020).
22. Malwarebytes: The lucrative business of bitcoin sextortion scams. Malwarebytes Labs blog (2019), `https://blog.malwarebytes.com/scams/2019/08/the-lucrative-business-of-bitcoin-sextortion-scams/` (accessed on March 3, 2020).
23. S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G.M. Voelker, S. Savage: A fistful of bitcoins: Characterizing payments among men with no names. ACM Conference on Internet measurement (2013).
24. S. Nakamoto: Bitcoin: A peer-to-peer electronic cash system (2008).
25. J. Nick: Data-driven de-anonymization in bitcoin. ETH Master Thesis (2015).
26. F. Oggier, A. Datta, P. Silivanxay: An ego network of suspected sextortionist(s). DR-NTU (Data) (2019), `https://doi.org/10.21979/N9/VSK3KB` (accessed on March 3, 2020).
27. M. Paquet-Clouston, B. Haslhofer, B. Dupont: Ransomware payments in the bitcoin ecosystem. CoRR **abs/1804.04080** (2018), `http://arxiv.org/abs/1804.04080`.
28. M. Paquet-Clouston, B. Haslhofer, M. Romiti, T. Charvat: Spams meet cryptocurrencies: Sextortion in the bitcoin ecosystem. Proceedings of Advances in Financial Technologies (2019).
29. C. Quintin: Sextortion scam: What to do if you get the latest phishing spam demanding bitcoin. EFF Blog (2018), `www.eff.org/deeplinks/2018/07/sextortion-scam-what-do-if-you-get-latest-phishing-spam-demanding-bitcoin` (accessed on March 3, 2020).
30. F. Reid, M. Harrigan: An analysis of anonymity in the bitcoin system. Springer (ed.) Security and privacy in social networks. pp. 197–223 (2013).
31. S. Phetsouvanh, F. Oggier, A. Datta: Egret: Extortion graph exploration techniques in the bitcoin network. IEEE International Conference on Data Mining Workshops (ICDMW) (2018).
32. M. Spagnuolo, M. Federico, Z. Stefano: Bitiodine: Extracting intelligence from the bitcoin network. Intl. Conf. on Financial Cryptography & Data Security (2014).

33. T. Tuna, E. Akbas, A. Aksoy, M.A. Canbaz, U. Karabiyik, B. Gonen, R. Aygun: User characterization for online social networks. Social Network Analysis and Mining **6**(1), 104 (2016).
34. R. Wanner: Sextortion: Follow the money - the final chapter. SANS ISC InfoSec Forums (2019), `https://isc.sans.edu/forums/diary/Sextortion+Follow+the+Money+The+Final+Chapter/25204/` (accessed on March 3, 2020).
35. J. Whalley: What happened when sextortion scammers targeted a bbc trending reporter? BBC.com video (2018), `www.bbc.com/news/av/stories-46323625/what-happened-when-sextortion-scammers-targeted-a-bbc-trending-reporter` (accessed on March 3, 2020).
36. H. Yousaf, G. Kappos, S. Meiklejohn: Tracing transactions across cryptocurrency ledgers. 28th USENIX Security Symposium (2019).

Appendix

Table 4. List of Bitcoin addresses referred in this paper using the first five symbols.

163qcNngcPxk7njkBGU3GGtxdhi74ycqzk
16p7uibFCyXDgdmRqTx2z4GPhyRCpiDuNt
178whzpvYpHZfzixEUHVEguTJoxzjGSGJJ
17XVPHG6oabUykxJyn8fiPX3YVxV1JQKir
19hAVdLhVJzMVeg4yADyfrRVtFsnc9LmwF
19j7C4jx2sKMJv2pyqJy4aJeknwGGGXzHH
1AXKgxjzNrhkAuGR7fVVuoZXy1kbJfAzfV
1BjiYVqtZxrmrrmrKgVxg8YkBVeiESDRWU
358E8DEnvYfRgVJb49DUatpBdVEL3vFABE
35n3QKnYFAPoxxR4pfwBq1XRBHbzDDUrNk
38Yb9GZZSKVkUCkyS5t6cV1CV5667HM6z2
39rVSdvsf5oHYVkvkwUHKrQ9V9R7mY4Boy
3AwHHGrYwXUMgrwNxZRVE6FB4V25poCiB2
3BK5Ndr7aMwQgkc9GSYyjeEtp7TQJCgELV
3HXdb3HAw1wVzU9b7ZSigvGaStd8KoZ3zJ
bc1qqvh3lhkhcxhpnhmh0uv6plvlqtymejsuj2t8vd
Addresses from (possibly) other scams
1AELppzruEPxcVC9oLmLgzZ68iG1LsepwA
1L47wHe7FXWQ6pfPTbnykdX44FxQGstFeS
1PAcoXVyzBDRryyg3MAmBQhDuofNYu55Uo
12s4cfoNTzT68gSdxLjmSRT3qdvaqwDWNz
Addresses with high occurence
35FF8b8jYnr24HizqgwVHxHHHDucjLEpYB
1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s
1BtSE7AXX5RuRRcnbhiM3qBwMhEYwxqBsm
1LMzzbZPpMDn7XoNMLiQCwZvq27b9nseKE
37Tm3Qz8Zw2VJrheUUhArDAoq58S6YrS3g
3CQCs6Vx5rfmZsK7X2wvwAeHYuHT8Ugfvb
1N52wHoVR79PMDishab2XmRHsbekCdGquK
1LcUj5TtKREfnD1xH6vWvs3Vp6JaeSJf61
38f8RHFQ8v6avZqCmaYTga5bTYiuhoM6fh
3DFqkpiQ4N467oHFZ1TpBiGjUzNFBqH4kJ

Table 5. List of transaction hashes referred in this paper using the first five symbols.

020be428fe1117116240ec7538e686074aa6ebf2f2c4583ed91e0575879c466b
2918a0635178e23b51f440347a66a536cb49d87e1a41f6a4ff34f1f8856b4fb5
466efc61cce0eda70554f1b2491735d46e42e6ac85e9e11aff5360f92e3166dc
52e289b4b88f842a436f50e6f22b9c02283bbf117c1f5e0060f3cc72ed417d56
61dca79625ea51a5debde8496db33939fe8a3377ee5bfe18f1e6bd14ce1e9bcb
7e6816a207e00823d853fcb57351170e3b2e9a24f6503feab466eb66ca9421ae
89420d2ee8095ccab017e6f7637b7a3ded2cd45e97ce641de3bbe37557ace5e0
929e21f73ff550c12198d53034f99dba7de6a9261bd1d69772b876cf21051651
92d562d7f0b3e057d845e4badba08dc0e005e6a43eda0856b2d6f62b212ce354
94c86a55bb3081312d6020e67202e8c93a43d897f4a289cc655c0e9e6d9e31b4
99e4b54a2eb2da5f68bd7bf3cc883234eaa3cf9ea4d2a305cd9fdf1516392ff7
9a3b50413f24a9caa8dfd3f6557920babe0ec19d980c0b67814813a12fc235c5
d2ae05cf6b2d8b0d54d68b24f2fd4f9d87d365aac60a01774a8109c7259cb08c
da4dfbeb45f1c9bec96c0889012a9ea271973bab9fd6e5a4170011441f2dfea4
e549262ad8fe437568b59939aae027e95cb04e775bcb68f67654031e1f61f77a
Transactions with out-degree more than 100
a9f07bd786847fbec8c23e132d66c8d8c5d86a0be3389f2785e43567242a564f
f5985d07f650c4932f375fd66c8d845feb6b6ac425b4b52c3420ae1ccf9e43d6
7adef60bcb915e30e2d6c192546bb156bbf2b1ee0d39e1a534524f35dfe1d316
8a8b9f4eab28d378e1274f673e5a4f0dee9316dd307f379541d3e85ebd5cdc54
eac6f41dfd31d1a231d9daf53be62e2b37a1834ae92bb70762896c71d2e7fccf
0571cdcf094e3fdc6595fd2b86e65c0bfff2ed4aa6cfff2a22d7fa05d3471e4e
830c09d02cb05f0ecc5d90684c5b35d0f87c3a44c6432b17e30c0c3f3fc74408
0d6509e8abf3b21c326d21597e56ee5950c485e3a4d456fd29030748dccfbcd4
80bb2af4409405982a8246f695c9d411a7ba131cd17a06b81bf7ab8fb7a07b41
10beb6e3d6dcd3effad133eeaf466e587377fc7c9dab08f56b77bfa8539f165a