Revealing and Concealing Bitcoin Identities: A Survey of Techniques

Karolina Bergman
Dept. of Cyber Intelligence & Security
Embry-Riddle Aeronautical University
Prescott, AZ, USA
bergmak1@my.erau.edu

Saeed Rajput
Dept. of Cyber Intelligence & Security
Embry-Riddle Aeronautical University
Prescott, AZ, USA
rajputs@my.erau.edu

ABSTRACT

Bitcoin remains the most widely used cryptocurrency. It has attracted users from tech enthusiasts to commercial investors to criminals, in no small part due to its reputation for anonymity. While not designed primarily for privacy, Bitcoin's architecture contains several provisions that can be exploited by criminals to conduct illegal activity including money laundering and collecting payments from ransomware and scams. Since Bitcoin's creation in 2008, various groups such as law enforcement, lawyers, criminals and privacy-focused Bitcoin users have been locked in a struggle between attempts to reveal hidden Bitcoin users' identities and attempts to keep those identities concealed. We present a survey of the techniques used within Bitcoin to reveal or conceal users' identities. We provide an easy to understand explanations of how these techniques work and provide a cross reference of which revealing techniques are effective for specific concealing techniques.

CCS CONCEPTS

• **Security and privacy~Human and societal aspects of security and privacy;** • Social and professional topics~Computing / technology policy~Government technology policy~Governmental regulations; • Security and privacy~Human and societal aspects of security and privacy~Privacy protections;

KEYWORDS

Bitcoin; security; privacy; cybercrime; deanonymization

ACM Reference format:

Karolina Bergman, Saeed Rajput. 2021. Revealing and Concealing Bitcoin Identities: A Survey of Techniques In *Proceedings of 2021 The 3rd ACM International Symposium on Blockchain and Secure Critical Infrastructure, (BSCI 2021), June 7, 2021, Virtual Event, Hong Kong.* ACM, New York, NY, USA. 12 pages. https://doi.org/10.1145/3457337.3457838

BSCI '21, June 7, 2021, Virtual Event, Hong Kong.

ACM ISBN 978-1-4503-8400-1/21/06...$15.00.
https://doi.org/10.1145/3457337.3457838

1 Introduction

Bitcoin, an online currency launched in 2008 by an unidentified individual or group using the pseudonym Satoshi Nakamoto, has surged in popularity over the years, gaining followers ranging from technology enthusiasts to speculative investors to criminals. It was originally designed to facilitate financial transactions which any entity could use safely and which did not rely on a trusted third party to provide the guarantee for that safety [1]. Nakamoto was inspired, in part, by a concern over the amount of control governments and banks had over the financial system and traditional currencies [2]. While privacy was not the main goal, several privacy-enhancing elements, such as pseudonymous address in place of names, were incorporated into the structure of Bitcoin, though these protections are not insurmountable [3]. These protections made the currency a popular choice for groups who did not trust either banks or governments or who had something to hide from these organizations.

Figure 1: An example of hacked Twitter accounts on July 15, 2020.

Bitcoin, and many other cryptocurrencies that followed, gained infamy as vehicles and abettors of illegal activity. Dark-web sites like the (now defunct) Silk Road advertised anything from drugs to assassinations in exchange for this new currency [4]. There are numerous ongoing attacks were hackers encrypt the victim's machines and demand ransoms in Bitcoin [5]. Most recently, the Twitter accounts of several prominent companies and individuals were hacked through social engineering [6] in an attempt to collect money in Bitcoin. Figure 1 shows an example of the hacked Twitter accounts on July 15, 2020.

Initial confusion over the legality of Bitcoin as a currency contributed to its infamy. Bitcoin wallets were used to transfer money overseas to avoid wealth transfer laws or to hide wealth from divorce courts by spouses [7]. Before Bitcoin and other cryptocurrencies became widely known, they functioned as an effective way to hide money, as few officials or courts would think to look for Bitcoin wallets when assessing an individual's wealth [8]. However, sources disagree on how much actual criminal activity has occurred using Bitcoin. In a 2018 interview, a DEA agent from the Cyber Investigative Task Force on dark-web and crypto investigations stated that criminal activity in 2018 comprised less than 10% of transactions, down from a high of 90% of transactions in 2013 [9]. Whereas a report from the company Chainanalysis, that conducts blockchain analyses for government agencies and financial institutions, stated that criminal activity made up less than 1% of transactions in 2019, down from a peak of 7% of transactions in 2012 [10]. A 2019 study by Foley et al. [11] concluded that 26% of Bitcoin users and 46% of Bitcoin transactions can be associated with illegal activity, and that in dollar values, this illegal activity makes up 23% of Bitcoin transaction value and 49% of Bitcoin holdings. However, all sources agree that while the percentage of criminal activity is decreasing, the total monetary value of illegal transactions using Bitcoin is increasing as it is more widely used. This increase in criminal activity amplifies the back-and-forth battle between law enforcement attempting to reveal the identities of the criminals trading over the Bitcoin network, and the criminals trying to conceal their identities to maintain anonymity. Parties in this conflict include governments, lawyers, privacy-concerned individuals, currency speculators, hackers, and many others. For simplicity, we have categorized these groups into two competing camps: 'revealers' versus 'concealers'.

We have also divided the revealing and concealing techniques used by these camps into 'primary' and 'secondary levels. Primary techniques seek to connect or obscure Bitcoin addresses from personally identifying characteristics. Secondary techniques seek to discover or obfuscate links between Bitcoin addresses which can tie an anonymous address to an identifiable one.

We present a survey of the techniques used by either side in this revealer against concealer competition. We provide an easy to understand explanations of how these techniques works and provide a cross reference of which revealing techniques are effective for specific concealing techniques. In section 2, we briefly introduce the structure of the Bitcoin system and how it impacts anonymity. In section 3, we describe techniques used by revealers to uncover Bitcoin identities. In section 4, we cover techniques used by concealers to hide their identities. In section 5, we cover techniques used by revealers seeking to counter the identity-concealing techniques. In section 6, we summarize our analysis by presenting cross reference tables.

2 Bitcoin Protocol Structure & Pseudonymity

While it also used by those who wish to remain anonymous, Bitcoin was primarily designed to be a transparent and publicly-verifiable transaction system so it could function without any centralized authority. It primarily relies on ECDSA [12] public key based digital signature algorithm and SHA-256 [13] secure hash algorithm. ECDSA is a variation of the Digital Signature Algorithm (DSA) algorithm used in NIST's DSS [14], while DSA itself is a variation of ElGamal signature scheme [15].

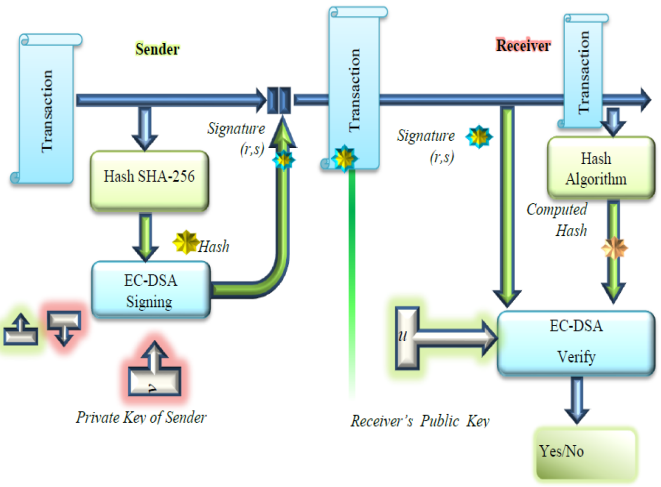

Figure 2: ECDSA Public-key Digital Signature Algorithm.

Figure 2 shows how a bitcoin transaction is signed and verified using ECDSA and SHA-256 algorithms. The signature is composed of two components *r* and *s*, both are used during the verification process. To receive payments, a user (receiver) can create Bitcoin identity by generating a cryptographic public-private key described above. The receive publishes the hash of their public key, known as an 'address', as shown in Figure 3.

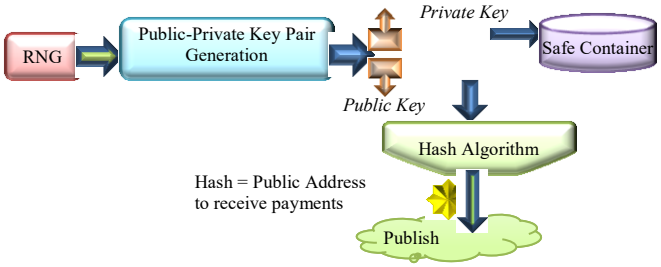

Figure 3: Generation of a public-private key pair.

This address can be advertised publicly, such as in the tweet shown in Figure 1, encouraging other Bitcoin owners (senders) to send money to that address. To cash that payment, the receiver uses their private key to unlock and access those funds. Transactions are sent to the peer-to-peer (P2P) Bitcoin network,

where Bitcoin miners compile them into blocks and attach them to the Bitcoin blockchain as shown in Figure 4, confirming and permanently recording them in an immutable ledger. This ledger remains available for anyone to download and examine at any time to ensure it is correct. It can also be used to detect transactions of interest [16]. Figure 4 shows that each block is composed of a header, a block reward transaction, and a variable number of normal transactions drawn from the individual mining node's pool of pending transactions. New blocks are generated roughly every 11 minutes.

The viability of Bitcoin depends on thousands of miners who are incentivized to act honestly and maintain full copies of this chain across the world. Thus, transactions are irreversible and publicly viewable on this blockchain. Each transaction contains both the sender's address, public key signature, and receiver's public address, so it is impossible to spend Bitcoin without the sender revealing their ownership of the public key. However, as it is the Bitcoin addresses rather than the users' names which are revealed, Bitcoin users do maintain a certain level of pseudonymity even in this public system.

Other than mining coins, the only other way users can get bitcoins is through transactions. Therefore, their "recipient" address will appear in the public ledger before they can spend them. However, no information about the user of the receiving address is recorded. The user can remain pseudonymous indefinitely in a newly-generated "recipient" address until the held coins are spent. This case is illustrated by more than a million Bitcoins thought to have been mined by Satoshi himself starting in 2009, which remain unspent and add more fuel to the mystery of who Satoshi actually is [17]. When a previously-dormant address which also mined coins in 2009 suddenly cashed out in 2020, the community panicked that it was Satoshi crashing the price of Bitcoin, even though the address was quickly revealed to have not belonged to any of the blocks which had been associated with Satoshi [18].

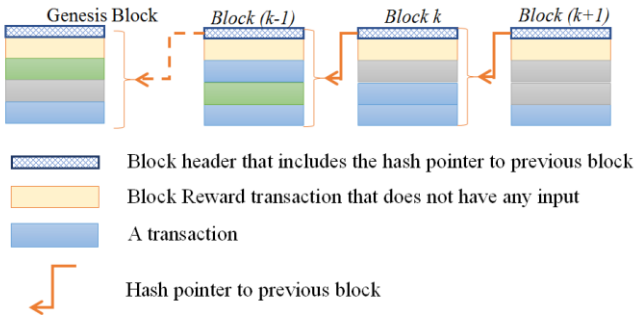

Figure 4: Depiction of a block-chain.

A Bitcoin transaction can include multiple input addresses (transactions received from multiple sources that are all being spent) and multiple output addresses (transactions going to multiple "recipient' addresses). **Error! Reference source not found.** depicts as Multi-Input, Multi-Output (MIMO) transaction with *m* inputs and *k* outputs.

Miners who create the next block in the blockchain get a "block reward" in freshly minted bitcoins. They also collect the "incentive" voluntarily left by the spender in a transaction to include it ahead of other transactions when compiling the next block. This is the difference between sum of all input amounts and sum of all outputs amounts.

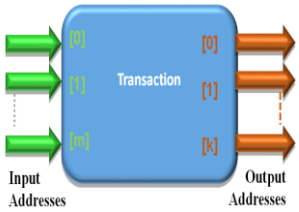

Figure 5 Schematic depiction of a multi-input, multi-output (MIMO) Bitcoin transaction (Tx) and a QR link to a real Tx on June 06, 2020. Source: https://live. blockcypher.com/

To spend bitcoin from an address, the user references one or more transactions sent to that address and must "prove ownership" of each by signing it by the corresponding private key. Each transaction automatically consumes all value of the referenced transactions (inputs) so the total amount must either perfectly match the sum of inputs to the value paid in the transactions (outputs), or include a secondary address – called a change address – to send excess bitcoin value back to themselves. If the total inputs amount is greater than outputs' the miner collects the difference as "incentive". Those output addresses then refer back to this transaction when they, in turn, spend their assigned bitcoins, forming a chain of transactions as illustrated in Figure 6. Its shows how Bitcoin transactions are linked to each other in a blockchain and how a transaction chain can be traced. In this example, the transaction t_3 consumes t_1, transaction t_5 consumes transactions t_2 and t_3, and transaction t_6 consumes t_5 as well as the block reward transaction t_4. Revealers can apply a wide variety of heuristic-based algorithms to this chain in order to conclude what manner of relationship the involved addresses may have, as discussed in section 5.

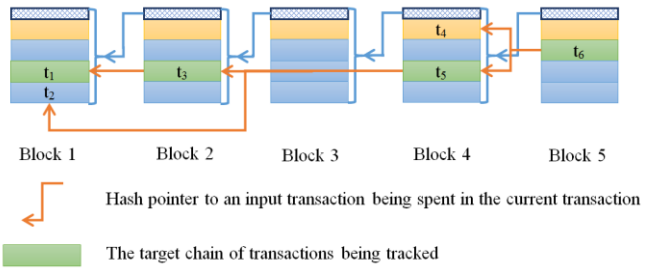

Figure 6: How transactions are linked in a Blockchain.

Figure 5 also provides a QR code link to a real transaction (tx: 8421c9acf34229e0a7628f21049a20ecab3b0b319592dd166889a0177e241260)

conducted on June 6, 2020 that has 3 inputs and two outputs. The reader can view it by scanning the QR code on their smart phone. Notice that the total input value is 1.0281161 BTC, while the accumulated value of the outputs is 1.02753842 BTC. There is a difference of 0.00057768 BTC, which is collected by the miner as an incentive.

While concealers develop their own identity-hiding strategies on top of the core Bitcoin protocol, Bitcoin developers have largely avoided incorporating additional obfuscation capabilities into the protocol itself. This is thought to be done for two main reasons: these capabilities, such as adding cryptography, would slow down the performance of the already slow Bitcoin transactions; and Bitcoin developers want to remain neutral in the tug-of-war between revealers and concealers [19].

Therefore, the ultimate strategy of Bitcoin identity revealing techniques is to match a target Bitcoin address with a user-identifying piece of data, while the goal of Bitcoin identity concealing techniques is to retain the veil of pseudonymity by keeping identities disassociated from their Bitcoin activity.

3 Identity Revealing Techniques

For a revealer to peel back the pseudonymity, they need to link the address to a piece of identifying information such as a name, IP address, physical address, email, phone number, or other information directly tied with the identity of the concealer. These are defined as primary revealing techniques. These techniques are ways that a concealer may reveal themselves, be revealed by conducting business with third parties, or be revealed by behavioral or network data.

3.1 Voluntary Reveal

In some cases, a revealer may find that their target has already identified themselves by publicly disclosing their Bitcoin address. Many Bitcoin users post their Bitcoin address on their website or social media because they are publicly conducting business in Bitcoin, seeking donations, or simply showing off their involvement with cryptocurrency technology [20]. Due to the near-impossibility of completely removing information from the internet, and the permanent, immutable nature of the blockchain, a single instance where the entity revealed its Bitcoin address can be uncovered and checked at any point in the future. Some websites, particularly those on the dark-web or belonging to organizations that may cause legal or political consequences for their donors if their relationship is identified, will ask for donations in Bitcoin due to its perceived anonymity and independence from governments or companies [21]. While these sites typically change the receiving Bitcoin address regularly, often generating a new address for each donation, the practice of posting an address publicly can still lead to deanonymization of each address through use of linking techniques described in section 5.

3.2 Third-Party Connections

Unless a user purchases Bitcoin mining equipment and manages to collect a Bitcoin reward for mining a new block, they have to get their Bitcoin from someone else. In the process, this 'someone else' is likely – or legally required – to gather information that can be used to deanonymize the user. For a prospective Bitcoin owner, a Bitcoin exchange is likely the first place they would visit to acquire Bitcoin. While exchanges used to operate under little to no oversight, they came under increasing scrutiny as cryptocurrency usage grew. Currently, they are required to operate under Anti-Money Laundering (AML) regulations and follow the Know Your Customer (KYC) laws in many countries [22]. Among other things, these laws require exchanges operating in compliant countries to gather enough information from its users to confirm their real identities. These exchanges are required to report information to their governments when subpoenaed. This means that law enforcement or lawyers can use the information on a user gathered by the exchange to identify the user. In addition, stored user information can be susceptible to hacking or sale to other third parties.

Those wishing to use Bitcoins, not just holding them as investment, have to find an avenue to spend it. The acceptance of Bitcoin payments has been spreading among vendors that often have their own user accounts to process customer payments as well as track customers' information and spending history. When a user spends Bitcoin using that vendor account, their Bitcoin address is linked to that account's identity. It often contains personal information or payment information that can uniquely identify the user. Any legally operating company could be subpoenaed to give law enforcement all the information they have collected on a user.

Not only do online purchases allow a company to record user information, they also have a tendency to expose data to other third parties. In a 2017 study, Goldfeder et al. [23] examined the traceability of Bitcoin payments through vendor websites. They found that many online purchases exposed enough information to possibly connect the purchase to its corresponding Bitcoin transactions on the blockchain's public ledger. They found that while most data was collected purposefully for vendors' own advertising or analytics, many websites sent or sold this user data to dozens of other trackers as well. This data included information such as the payment timestamp, the payment Bitcoin address, the price of the purchase, and the purchaser's personal account information. The account data gives a revealer more options to connect an online purchase to its transaction on the blockchain, thus linking the transaction's input address to the account on the website and deanonymizing their Bitcoin identity.

Lastly, for any legal case, disclosure rules can require any third party with knowledge of a user's Bitcoin holdings to reveal this information. These laws apply to companies and Bitcoin exchanges, as well as to any individuals such as a spouse, family member, or business partner [8]. This means that the disclosure of

Bitcoin ownership to any entity could allow law enforcement to subpoena that entity and have them identify the Bitcoin owner.

3.3 Side Channel Attacks

Sides channels are indirect leakages of information such as location data or timing of activity. This technique can include strategies such as tracking what patterns of time a Bitcoin address is active and correlating these patterns with the activity times of another account, such as a Twitter account. Afterwards, the revealer can conclude that the Bitcoin user is the same person as the owner of that Twitter or other account [16]. A number of studies [24] [25] found that Bitcoin users could be identified and tracked by analyzing their patterns of the transactions' features.

3.4 Network-Layer Deanonymization

A revealer that has access to enough scattered nodes in Bitcoin's P2P network can use network-layer deanonymiz-ation. The revealer can observe and obtain the time of arrival of a specific transaction. The calculated differences in the time each controlled node receives the transaction can be used to determine which individual node first broadcasted the transaction [16]. This can reveal the sender's IP address, enabling the revealer to use a variety of tools to find the identity of the owner of that IP address, such as subpoenaing the user's Internet Service Provider (ISP). If the user has not used VPN or encryption, their ISP will also have records of most of the user's online actions.

4 Identity Concealing Techniques

The techniques presented in section 3 pose a challenge to concealers wishing to retain their pseudonymity. Because the blockchain ledger is public, concealers cannot hide their Bitcoin addresses, and therefore must resort to techniques which either conceal their real-world identity while handling Bitcoin, or transfer Bitcoin from an identifiable address to an unidentifiable address. These techniques include obtaining Bitcoin without compromising personal information, switching to a new pseudonymous Bitcoin address, changing normal behavioral patterns, mixing coins to confuse revealers, and using specialized wallets or browsers to keep identifiable information concealed.

4.1 Buying Bitcoin Anonymously

While AML laws and KYC laws have attempted to curb the ability to move wealth by purchasing Bitcoin anonymously, concealers seeking to reclaim anonymity have scrambled to find and advertise methods to get around them. One such method is to deal with a Bitcoin exchange based in a nation that does not adhere to laws requiring customer identification. Alternatively, a concealer can find a Bitcoin ATM in certain locations [26]. Purchasing Bitcoin using cash or a pre-paid credit card, and instructing the ATM to print a physical wallet – a piece of paper with a public address and its corresponding private key printed on it – allows the user to later connect from a secure computer or anonymized browser and access their funds [27]. A concealer could also find another individual who already owns Bitcoin and is willing to sell some in return for payment in cash or another untraceable medium. However, the method of contacting and paying this individual may cause the user to be identified later, by having communication intercepted or the seller identifying them. Lastly, a concealer can purchase their own Bitcoin mining equipment, create a mining node, connect to the Bitcoin network, mine a block ahead of all other miners and then collect the Bitcoin reward. While mining one's own coin seems to be the most secure method of obtaining completely anonymous Bitcoin, it is not foolproof. It is unlikely for an individual to mine a block before any of the specialized, industrial-scale mining operations, making it infeasible for a user to use it as a short-term or regular way to earn bitcoin. A miner is still susceptible to network-layer analysis that could identify their mining node, which then could be used to discover their physical or IP address and lead to deanonymization.

4.2 Generating New Addresses

The simplest built-in privacy function in Bitcoin is to generate a new address whenever they want a new pseudonym. Bitcoin users can do so easily. New addresses are not automatically traceable back to a user's previous addresses. Satoshi himself advised that privacy-conscious users should generate a new address for every single transaction [1]. However, this strategy is not a guarantee of anonymity. While a new address is unlinked to any previous addresses that means it has no access to the funds owned by any other address, either. Transferring money from those older known accounts to the new address may taint it, allowing revealers to follow the individual to their new address and deanonymize it.

This technique is widely used for sites such as Wikileaks and other entities whose associations might cause problems for donors. By providing a fresh address for each donor, the website grants them a certain level of privacy, as the newly-generated receiving address is not overtly linked to the entity it belongs to [16]. However, despite the simplicity of generating new addresses, studies show that the majority of Bitcoin users repeatedly reuse the same address, which suggests that the majority of Bitcoin users do not place a high value on anonymity [4].

New addresses are the basis for multiple other concealing tactics. Unlike the previous primary techniques, which link or unlink a Bitcoin address from a real-world identity, the secondary techniques based on new address generation focus on unlinking and concealing Bitcoin addresses from other addresses.

4.3 Merge Avoidance

Merge avoidance is the practice of splitting or combining transactions to try to fool address-linking heuristics that detect common merging transaction patterns. A merge occurs when an individual makes a purchase with a higher value than the value of any single one of their addresses, and therefore creates a transaction that pools multiple of their addresses together to make the purchase. If there is excess value beyond the purchase, they send the 'change' back to one of their own addresses. The QR code link for an example of a real merge transaction (tx: `c01b0be2a4fd6cf41b076c3033fb9bfdc1fca06b059f2cd47f1de751a147db84`),

without a change address, is in Figure 7. It merged 104 input transactions into a single output. This structure reveals that all input addresses belong to the same individual. Merge avoidance therefore either splits this transaction into multiple transactions, preventing their input addresses from appearing alongside one another, or combines this transaction with one or more other transactions, so that the relationships between the input and output addresses are less clear to a revealer observing the transaction [16].

The splitting method of merge avoidance spreads a single payment over multiple transactions, each using a unique address from the sender's for input and a unique receiver's address for the output. This way, the concealer avoids using all their input addresses visibly in the same transaction. A revealer viewing the transactions on the public ledger would not be able to cluster the addresses together to conclude shared ownership. Furthermore, each component transaction can be published at a different time to further obscure that it is a component of a larger payment.

Figure 7: The QR link to a real merge transaction that took place on June 06, 2020. Source: https://live.blockcypher.com

The combining method of merge avoidance combines multiple different planned payments into a single transaction, with enough input and output addresses involved that a revealer examining the transaction would find it difficult to ascertain the relationships. This method utilizes Bitcoin's ability to create transactions with a large number of both input and output addresses in the same transaction, as illustrated earlier in **Error! Reference source not found.**.

Merge avoidance can impede or misdirect typical address clustering techniques by obfuscating whether the addresses in the split or combined transactions have any meaningful relationship to each other. The technique can further benefit the user by providing them with multiple smaller value addresses, providing them with greater flexibility to spend from any of those addresses later without revealing the total value of the first transaction.

However, merge avoidance has some drawbacks that keep many non-privacy-focused users from regularly utilizing the technique. Splitting a transaction requires coordinating with the receiver using a channel external to Bitcoin protocol. It also requires a receiver willing to go through the hassle of providing multiple Bitcoin addresses and then tallying up multiple small transactions to confirm a single purchase. Combining transactions can also require a user to postpone a planned transaction until they have other transactions to combine it with, which could cause either senders or receivers to become impatient.

4.4 Mixing

If a person wants to anonymously use a balance belonging to an address they know has been identified or is being watched, they must transfer it out from the compromised address without letting revealers follow the trail right to their new address. This is what mixing was created to do.

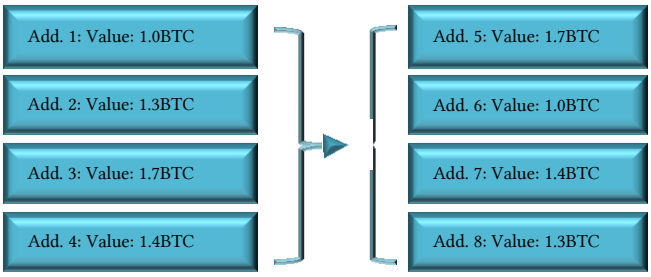

Figure 8: An example of a mixing transaction with 4 input addresses and 4 output addresses.

Mixing services work by having users transfer their desired amount of Bitcoin to an address belonging to the mixer, and communicate an output address for the mixer to deposit the mixed coins into over a different channel. The mixer then creates a MIMO transaction, combining several users' transfers together into a single transaction with an apparently random selection of input and output addresses, as seen in Figure 8. Commercial mixing services typically utilize multiple rounds of mixing transactions to further confuse the trail.

Mixing aims to include enough different addresses in a transaction to scramble the relationships of the input addresses and the output addresses. Once scrambled, a revealer would have to spend a significant amount of time and effort in sorting through all possibilities. A revealer would need to keep track of every address involved and the bitcoin value for each input and output address, and continue doing so for every round of mixing until their target has left the mixing pool. Since there are no obvious indicators to show when a target leaves the mixing pool, the task becomes even more difficult for the revealer. This creates a lopsided situation where revealers must spend far more effort tracking a concealer using a mixer than the concealer spends to mix their coins.

The addresses involved in a mixing transaction make up the *anonymity set*: the total set that an individual user is trying to blend in with. The larger the anonymity set, the more difficult it is to track a single user through the system. Many mixers will set a minimum number of users for a mixing transaction to take place, because these transactions with a small anonymity set do not obscure the relationships between the input and output addresses well. However, the larger the required anonymity set, the longer it takes to form a mixing transaction and therefore the longer it

takes a user to get their mixed coins out of the mixer for personal use.

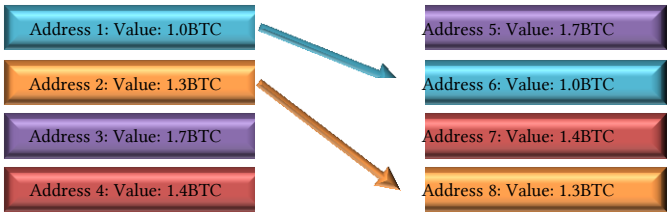

Figure 9: A mixing transaction with varying input values.

If each concealer inputs unique Bitcoin amount, it would be easy for a revealer to match an input address with an output address by following the specific amounts of Bitcoin being shuffled, as seen in Figure 9. To make each user indistinguishable most mixers set a standard value to be mixed in each transaction.

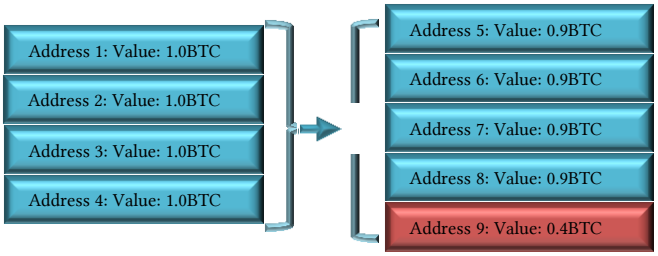

Figure 10: Percentage fee can reveal mixer's address.

However, this creates its own issues as well: setting a small standard value means that users wishing to send large values will have to pay more in transaction fees. Setting a large standard value would limit the size of anonymity set. Creating separate value tiers can offset this risk, but that also means that each tier will have a smaller anonymity set. However, after making all of these as standard and indistinguishable as possible, the mixer has to figure out a mechanism to collect a fee. If the mixer takes a percentage or set fee from each standard value input, then the fee output address will be identifiable due to having a different value than the standard mixer output as shown in Figure 10, lowering the anonymity set of the mixer.

While that is a minor loss of anonymity, these fee mechanisms would also show differences in value between addresses that had gone through multiple rounds and those that had just joined the mixing pool. This is shown in Figure 11, where an example mixer runs multiple cycles while charging 0.1 BTC each mixing round. It shows an example of how a regular fee per transaction could allow a revealer to trace new entrants into a mixing pool by observing multiple rounds of mixing. Each round subtracts a 0.1 BTC fee from each address, which causes new entrants to the mixer to have visibly different values than the addresses which have already gone through previous rounds.

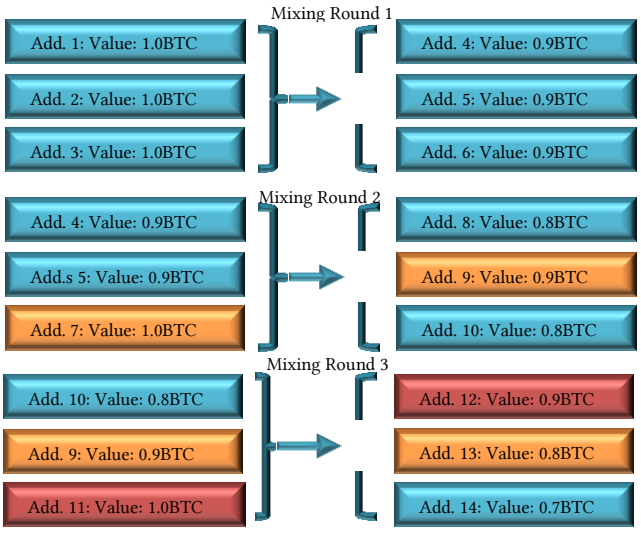

Figure 11: Enhanced traceability with percentage fee model when multiple rounds of mixing are used.

To solve this problem, many mixers are designed to simply absorb the occasional standard value chunks in whole, redirecting it to the mixer's coffers rather than to its intended recipient. While this retains the anonymity benefits of standard value transactions, an unlucky user may find their entire set of Bitcoin vanished into the mixer with no recompense. This method has led to multiple cases of mixing services being denounced as thieves [28]. The resulting dissatisfaction, and the inability to monitor third-party mixers, causes many mixing services to be short-lived, and the Bitcoin mixing field experiences high turnover rates.

While a determined revealer can usually track a target through the mixing process, a typical resource-limited revealer can be set back by using a mixing service [23][28]. While mixing coins is legal, mixing services can be taken down under AML laws if the mixing service advertises itself as a way to get around the law. Many services over the years with suggestive names such as "BitLaundry" imply that these services are fully aware of their users' likely goals [28].

4.4.1 CoinJoin (CJ): Many concealers see mixing services as risky and seek to replicate their function by mixing coins on their own. CoinJoin (CJ) [16] is a method where users get together and create their own MIMO transaction to obfuscate the mapping between each input address and each output address, just as a mixer would do. CJ has a similar focus to mixing, but it does not require a central entity to organize transactions, although it can function with a central coordinator as well. When used with a centralized coordinator, CJ participants send their signed input addresses and intended output addresses to the coordinator, who assembles them into a transaction. This exposes the address relationships to the coordinator, which creates an additional avenue that could lead to the user being identified. When used without a coordinator, a CJ participant sends out an unsigned and thus unpublishable transaction with their own input and output

addresses included to another participant. That participant adds their own unsigned input and output addresses, and sends it on to yet another participant, continuing until all participants have added their inputs and outputs. Once all the participants agree to finalize the transaction, each participant reexamines the unsigned transaction to ensure their input and output addresses are still included and their values are correct, and then add their signature to the transaction. Once all signatures are collected, the transaction is published to be verified and then added to the blockchain. While the use of CJ allows users to mix coins without trusting a mixing service, it does have four main drawbacks: 1) the lack of standard rules, 2) the additional time needed to make a transaction, 3) a low anonymity pool, and 4) the risk of a single participant quitting and therefore scrapping the entire transaction.

First, CJ transactions face a similar problem as centralized mixers: differences in input and output values can be used to determine which inputs correspond to which outputs. Without a central mixer to set standards, CJ participants have to either impose these standards on each other, or accept a weaker anonymity gain.

Secondly, CJ transactions typically take a longer time to assemble than normal as well as mixing service transactions. It takes time to a) locate other users who may wish to join the CJ transaction, b) let each user add to the transaction, c) send the complete transaction out again so that each user verifies their addresses are present and amounts are correct, d) collect their signatures, then e) publish the complete transaction. Furthermore, this lengthy process produces only a single transaction. A user who wants additional mixing rounds would have to begin the entire process over again. This makes CJ far slower than a dedicated mixing service, which has full control over all addresses used in mixing rounds and thus can construct transactions faster.

Thirdly, CJ transactions typically have a lower number of participants and thus a smaller anonymity set, as CJ requires users or a coordinator to persuade other users to join their transaction while the individual transaction is under construction, as compared to an advertised mixing service conducting a steady stream of mixing transactions.

Lastly, due to the time it typically takes to assemble and publish a CJ transaction, participants run the risk of having impatient or malicious users abandon the transaction. They might spend their committed coins elsewhere before the CJ transaction is finalized and published. This causes the CJ transaction to be rejected when the other users attempt to publish it, as the inputs cannot be validated if a single user has already spent their referenced coins in another transaction. The longer it takes for a CJ transaction to complete, the more likely it is for one of these impatient or malicious users to invalidate it. Such a result forces the other participants in the CJ transaction to start the process over again.

4.5 Privacy-Focused Wallets

Multiple wallet programs and devices have evolved to provide concealers with additional layers of privacy. Bitcoin wallets are applications or devices that provide the interface with which users can access and handle their Bitcoins. Privacy-focused wallets automatically incorporate several of the aforementioned identity-hiding techniques for their users' convenience. However, these wallets are ultimately constrained by Bitcoin's hardcoded limitations such as the requirement for publicly viewable transactions. They vary in techniques used and concealment offered, as shown in the following examples, including variations on new address generation, a variation of CJ, and using mixing automatically.

Darkwallet: As we have seen, chain analysis is the primary revealing technique to link public keys with real world identities. The wallet program Darkwallet was one of the first privacy wallet to counter these techniques. It adds a layer of privacy by utilizing a system called stealth addresses [29] rather than the usual hashed address method. A stealth address decreases linkability of a user's addresses by breaking the direct link between a sender and a receiver. This technique takes advantage of the way that ECDSA algorithm, described in Section 2, works. Rather than asking all users to send their payments to a single fixed address, this technique allows senders to generate a new public key for every transaction, based on a fixed known public key. To use the method, anyone who wants to receive Bitcoin has to publish the known fixed public key, u, which is calculated from the receiver's fixed private key v like so: $u = g^v$. A person sending bitcoin to the receiver generates a random nonce r. The sender calculates a new public key using the nonce and the published public key: $u' = u^r \ mod \ p$. The payment is made to the new public key u', and the sender has to separately provide the nonce r to the receiver by either hiding it within the Bitcoin transaction using sophisticated protocols or by sending it through a side channel. The receiver can compute the new private key from its fixed private key $v' = (vr) \ mod \ p$. This means that a revealer searching the public ledger would only see the stealth address rather than the receiver's original Bitcoin address. However, this approach has some drawbacks. First, the sender must find a way to communicate the nonce to the receiver, and second, the receiver only realizes they have received bitcoin when the sender tells them where to look for it. In addition, since this strategy requires publishing the entire public address rather than the hash of the address, it is more memory- and computationally-intensive than normal Bitcoin transactions.

Wasabi Wallet: Wasabi Wallet attempts to break the sender/receiver link using Chaumian CJ transactions [30]. This type of transaction works by using blind signatures [31] to allow a central coordinator to assemble CJ transactions, but allowing participants to separately submit their input and output addresses so that even the coordinator does not know which input corresponds to which output. In the Chaumian blind signature method, a sender creates a normal transaction header but blocks out the data about who the receiver will be, and sends it to a central organizer called a tumbler. The tumbler first verifies the sender's information and that they control the funds needed to

initiate the transaction, then signs the blinded output, and finally returns the signed output to the sender. The tumbler then adds the submitted input address used to verify funds to a draft CJ transaction. Once that stage is complete, the sender can take their signed output, unblind the destination address, connect to the tumbler again from a different pseudonymous address and present the signed output as proof that their output address can be added to the transaction. The tumbler does not recognize the user but does recognize its own signature, and therefore accepts the output address request as valid and adds that address to the draft CJ transaction without the concealer needing to reveal which input address was used to obtain the signature. The tumbler can then assemble a CJ transaction with multiple of these separately submitted sending and receiving addresses, without itself knowing which sender correlates to which receiver. Since the wallet controls each address involved in these CJ transactions, it can construct and publish these transactions much faster than user-initiated CJ transactions, although this process can still cause delays in users' normal Bitcoin activity.

Samourai Wallet: To minimize linkability, Samourai Wallet automatically generates new addresses when receiving outside payments and when sending coins to a change address. It also optionally sends a user's transaction through multiple dummy addresses before sending it to the intended recipient to further obscure the payment trail. It can also stagger the time between these in-between payments so they show up in different blocks with different timestamps, making it more difficult for a revealer to identify the user by using time-based side channel attacks [32].

4.6 TOR and Proxy Servers

The Onion Router (TOR) is an anonymizing peer-to-peer (P2P) network used widely to avoid being tracked online. Concealers also use TOR to shield their Bitcoin activity. Several privacy-focused Bitcoin applications, such as the mixing service Bitcoin Fog, requires the user to connect through TOR. Conversely, Bitcoin is the most common currency for TOR-based sites to conduct business with or request donations in, because of their similar reputations for anonymity [20]. A web proxy server commonly but incorrectly referred to as VPN, grants users another layer of privacy by hiding their IP addresses. The proxy service indeed funnels users' traffic through true VPN (encrypted) tunnels to its own servers. From there the traffic is placed on the internet. Because it is mixed with other users' traffic, a revealer tracing a connection would only be able to track it back to the service's proxy server and not to the user's IP address. However, in many jurisdictions such a service is required to keep logs of users' activity. These logs can be subpoenaed or hacked.

TOR has no underlying company compiling records, so it avoids these risks. Using TOR, concealers can send encrypted data over a P2P network. Their activity is traceable back only to a TOR exit node rather than their own IP address. While it does not overcome Bitcoin's inherent privacy limitations, TOR does protect the concealers from several primary revealing techniques, like side channel attacks which trace Bitcoin activity to an IP address or to the concealer's Internet Service Provider which a revealer could then subpoena to obtain the concealer's information. Many concealers consider anonymity network crucial for privacy or maintaining anonymity when using Bitcoin [33]. Mere use of TOR is not enough to have Bitcoin anonymity. In fact, Bitcoin's comparatively lower privacy protections may actually be used to deanonymize TOR users. Jawaheri et al. [20] used Meiklejohn's clustering heuristics [34], discussed in section 5, to link multiple pseudonymous TOR identities to real identities by finding links between their pseudonym's Bitcoin addresses and their personally identifiable Bitcoin addresses.

4.7 Trading through altcoins

A concealer can avoid Bitcoin's privacy limitations altogether by swapping to an altcoin – a cryptocurrency other than Bitcoin – with stronger privacy architecture, such as Monero [35], and conducting transactions there instead. In this technique, a concealer uses Bitcoin to buy a certain amount of an altcoin, conducts the transaction in that altcoin, and then trades any change back into Bitcoin.

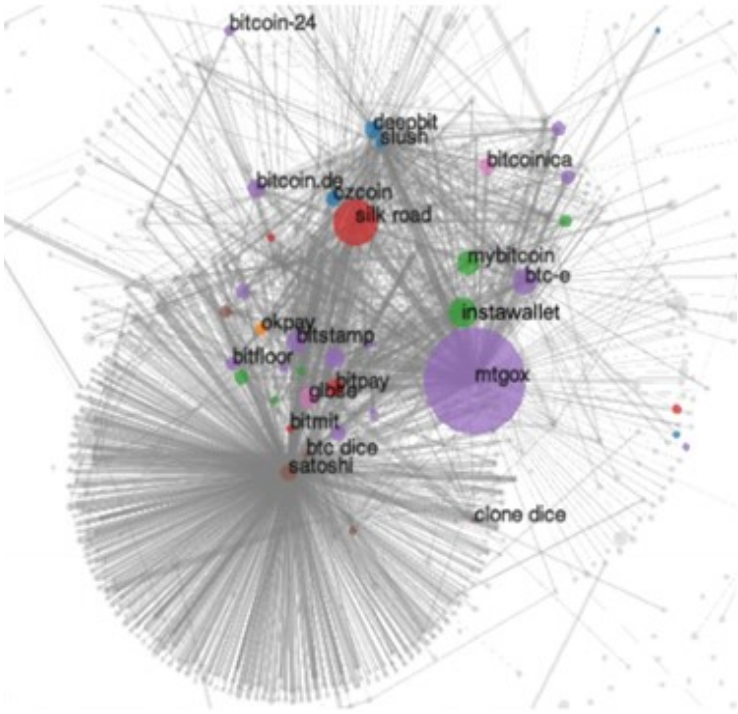

Figure 12: A visualization of Bitcoin address clusters. Source: Meiklejohn [34]

This technique is limited by the security of the specific altcoin being used, the speed at which one can transact using that altcoin, and the size of the anonymity pool that altcoin has. While many existing altcoins have better privacy architecture than Bitcoin, these altcoins are accepted at far fewer places. Additionally, altcoins with better privacy architecture usually require more time to complete transactions, whether due to encrypting and decrypting data, waiting to form a suitably large anonymity pool,

or other functions. Lastly, since most altcoins have a smaller pool of users, even an altcoin designed for anonymity will typically offer a smaller anonymity.

While it is easier to anonymously or pseudonymously trade one cryptocurrency for another than to trade fiat currency for a cryptocurrency, there is still the risk of a concealer accidently leaking information in the process, such as going through a cryptocurrency exchange that is subject to reporting requirements. The concealer could potentially also be tracked if the timing of their purchase of an altcoin could be linked with the timing of that altcoin pseudonym receiving the funds, though this depends on how much information the altcoin leaves visible.

Despite the enhanced privacy benefits of many anonymity-enabling altcoins, such as Monero [35] which allows concealers to transact without publicly broadcasting their addresses, the majority of criminal cryptocurrency activity continues to use Bitcoin. This is likely due to Bitcoin's larger population to serve as an anonymity set, the wider acceptance of Bitcoin compared to other cryptocurrencies, and the greater liquidity of Bitcoin compared to other privacy-centric altcoins [9].

5 Counter-Concealing Techniques: Address Clustering

Many of the previously mentioned concealing strategies are secondary: moving from a starting address to a concealed destination address while obfuscating the trail between the two. A revealer's job then is to link an address not only to some identifying information, but also to any new pseudonymous address behind which the concealer may be hiding. To achieve these objectives revealers have developed secondary revealing techniques that investigate the public blockchain to determine which pseudonymous addresses are controlled by the same entities through discovering clusters.

Address clustering is the general name given to this technique. Figure 6 illustrated how Bitcoin transactions are linked by pointers to previous transactions to form a chain of transactions. Revealers can apply a wide variety of heuristics to this chain in order to discover the nature of relationships. Once links between addresses are discovered, compromising the identity of any one address using the techniques in section 3 can identify the entire web of associated pseudonymous addresses. Therefore, address clustering is a powerful tool for identifying concealers who attempt to re-anonymize themselves by mixing or transferring coins between addresses. In 2013, Meiklejohn et al [34] tested address-clustering heuristics by analyzing the entire Bitcoin blockchain. They linked together addresses into clusters representing single entities controlling large numbers of addresses.

To ascertain the identities of the owners of some of the notable clusters, the researchers created their own accounts with major Bitcoin businesses they suspected might be an owner of one of these address clusters. They conducted small transactions with these businesses, and then followed subsequent transactions on the blockchain until they connected to one of the addresses from a cluster in a way that implied shared ownership. Once this occurred, the researchers were able to identify the entire cluster. Figure 12 shows a resulting labelled chart of this experiment. It provides a visualization of Bitcoin address clusters. Larger dots represent larger controlled Bitcoin value, and thicker lines represent more transactions between the end addresses.

This experiment showed how the use of secondary revealing tactics could allow revealers to bring primary revealing techniques to bear on otherwise unidentifiable Bitcoin addresses. While this experiment only used Voluntary Reveal by associating with businesses that provided their own addresses, other primary revealing techniques could be used to give a revealer more avenues to identify a concealer.

Other researchers have developed a variety of different address clustering methods, each varying in the logic or heuristics used to analyze blockchain data to determine which associations of addresses indicate a shared identity behind them. These methods often work by searching for common idioms or patterns of use, such as a user combining two of their addresses to make a payment, or sending Bitcoins back to themselves. However, many address clustering methods can indicate false associations where none actually exist, confusing the revealer, and tend to become less effective over time as concealers adapt to counter them [33]. While each address clustering method varies in how it is constructed, most strategies use the same basic components: measuring how often addresses interact, searching for common transaction templates and taking note of repeated patterns.

Taint Analysis: Taint is the measurement of how often the two addresses interact, whether by regularly transacting with each other, often appearing alongside each other as inputs in transactions, having a payment to one address regularly end up in a second address, or otherwise appearing together in similar situations. Such behavioral patterns between two addresses will provide a high taint score [16]. This score is then used to decide if further investigation is warranted. Taint analysis is difficult for concealers to obfuscate because of the permanent nature of the blockchain, as addresses used in every historical transaction are available for analysis at any time.

Shared Spending Detection: Shared spending is the common name for a merging transaction that pools multiple of a user's addresses together for a single purchase, as detailed in section 4.3. Detecting these transactions allows a revealer to deduce that all the input addresses belong to the same identity [16].

Change Address Detection: A concealer will usually specify one or more different change addresses in transaction. If a revealer finds such a transaction, they can note the different change address and link it to the same identity that owns the input addresses [16].

High-Level Flow Detection: This component involves checking for a regular pattern of payments on the blockchain, such as a monthly

salary or repeated periodic payment [16]. The repeating pattern of time and amount makes it difficult for a user to conceal this kind of transaction, and establishes a high taint score between the sender and receiver.

Table 1: Revealing versus Concealing

Concealing Techniques	Buying Bitcoins Anonymously	Generating New Addresses	Merge Avoidance	Mixing	Privacy-Focused Wallets	TOR and	Trading through altcoins
Revealing Methods							
Voluntary Reveal	P					P	
Third-Party Connections	P						P
Side Channel Attacks	P					P	
Network-Layer Deanonymization	P						
Address Clustering		S	S	S	S		

6 Revealing vs Concealing: Cross-Reference

We summarize our analysis by presenting cross-referencing tables. The rows of Table 1 list revealing techniques, while the columns represent concealing techniques. An entry of "P" in a cell indicates that the technique causes a primary reveal, while "S" indicates a secondary reveal.

Conversely, rows of Table 2 list concealing techniques and columns represent revealing techniques that each concealing technique does or does not counter. P indicates that the technique protects the user from a primary reveal, while S indicates protection from a secondary reveal.

Table 2: Concealing versus Revealing

Revealing Techniques	Voluntary Reveal	Third-Party Connections	Side Channel Attacks	Network-Layer Deanonymization	Address Clustering
Concealing Methods					
Buying Bitcoins Anonymously		P			
Generating New Addresses	P	P			
Merge Avoidance					S
Mixing					S
Privacy-Focused Wallets		P	P		S
TOR and *and Proxy Server*		P		P	
*Trading Through Alt coins*Trading through altcoins					S

7 Conclusion

While developers have created other cryptocurrencies with better built-in privacy, the majority of concealers have remained with Bitcoin. Although the percentage of criminal use in Bitcoin compared to total Bitcoin use is decreasing, the total value embedded in criminal transactions is increasing due to the cryptocurrency's overall rise in use. This makes it more important for law enforcement to know how to uncover hidden criminal Bitcoin identities and for lawyers and government officials to know how to find and analyze Bitcoin ownership or investments.

Bitcoin appears to be succeeding as a currency that functions without the need for government support or permission. Even more than a decade after its creation, Bitcoin occupies a legal gray area. Anti-Money Laundering laws and Know Your Customer laws have been applied to the currency, but concealers quickly created avenues to avoid or mitigate them, and Bitcoin and cryptocurrencies are still not well-understood by legislators.

As each side develops new tools or techniques, the other works immediately works to counter them. On the one side, revealers use concealers' own statements, company connections, side channel data, address clustering, and network-level data to discover their real identity, while on the other, concealers use anonymous purchases, new pseudonymous addresses, merge avoidance, Bitcoin mixers, privacy-enhancing wallets, and anonymizing browsers and networks such as TOR to remain concealed. As the slow pace of legislation attempts to catch up to the unique cryptocurrency environment Bitcoin has pioneered, the never-ending battle between revealers and concealers will continue to evolve and escalate.

REFERENCES

[1] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[2] Alice Huang. 2015. Reaching Within Silk Road: The Need For A New Subpoena Power That Targets Illegal Bitcoin Transactions. *Boston College Law Review*, vol. 56, no. 85, pp. 2093-2125,https://lawdigitalcommons .bc.edu/bclr/vol56/iss5/10

[3] Mauro Conti, E. Sandeep Kumar, Chhagan Lal and Sushmita Ruj. 2018. A Survey on Security and Privacy Issues of Bitcoin. IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416-3452, Fourthquarter. https://doi.org/10.1109/COMST.2018.2842460 .

[4] Tin Tironsakkul, Manuel Maarek, Andrea Eross and Mike Just. 2019. Probing the Mystery of Cryptocurrency Theft: An Investigation into Methods for Cryptocurrency Tainting Analysis. *Heriot-Watt University, Edinburgh, UK.* https://arxiv.org/abs/1906.05754

[5] Bernhard Haslhofer, Benoit Dupont and Masarah Paquet-Clouston. 2019. Ransomware payments in the Bitcoin ecosystem. *J.of Cybersecurity*, vol. 5, no. 1, p. tyz003.

[6] Nick Statt. 2020. Barack Obama, Joe Biden, Elon Musk, Apple, and others hacked in unprecedented Twitter attack. *The Verge.* https://www.theverge.com/2020/7/15/21326200/elon-musk-bill-gates-twitter-hack-bitcoin-scam-compromised, [Accessed July 16, 2020].

[7] Howard Wiener, et al. 2013. Chomping at the bit: U.S. federal income taxation of bitcoin transactions. *J. of Taxation of Financial Products*, vol. 11, no. 3, pp. 35-47. http://heinonline.org/HOL/LandingPage?handle=hein.journals/jrlfin11&div=28

[8] Fulya T. Yalabik & Ismet Yalabik. 2019. Anonymous Bitcoin v enforcement law. *Int. Review of Law, Computers, & Tech.*, vol. 33, no. 1, pp 34-55. https://doi.org/10.1080/13600869.2019.1565105.

[9] Kevin Helms. 2018. Illegal Activity No Longer Dominant Use of Bitcoin: DEA Agent. *Bitcoin.com.* https://news.bitcoin.com/illegal-activity-use-bitcoin-dea-agent/

[10] Max Boddy. 2019. $515 Million in Bitcoin Spent on Illicit Activity This Year. *CoinTelegraph.com.* https://cointelegraph.com/news/515-million-in-bitcoi n-spent-on-illicit-activity-this-year-representing-1-of-total-btc-activity

[11] Sean Foley, Jonathan R. Karlsen & Tālis J. Putniņš. 2019. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? *The Review of Financial Studies*, vol. 32, no. 5, pp. 1798-1853. https://academic.oup.com/rfs/article/32/5/1798/5427781

[12] Don Johnson, Alfred Menezes & Scott Vanstone. 2014. The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Sec.. 1*, Jan. 31, 2014, pp 36-63. https://doi.org/10.1007/s102070100002 .

[13] FIPS Pub 180-4. Secure Hash Standards (SHS). 2015. *Fed. Information Processing Standards, ITL, NIST* , http://dx.doi.org/10.6028/NIST.

[14] FIPS Pub 186-4. Digital Signature Standard (DSS). July 2013. *Fed. Information Processing Standards, ITL, NIST.* , http://dx.doi.org/10.6028/

[15] Taher ElGamal. 1985. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Trans. on Info. Theory.* 31 (4), pp 469–472. . (conf. version appeared in CRYPTO'84, pp. 10–18). http://doi.org/10.1109/TIT.1985.1057074

[16] Arvind Narayanan, et al. 2016. Bitcoin and Cryptocurrency Technologies. *Comp. Sc. & Elect. Engr., Princeton Univ. Press*, ISBN: 9780691171692

[17] Sergio Lerner. 2013. The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin Creator, Visionary and Genius. https://bitslog.com/2013/04/17/ the-well-deserved-fortune-of-satoshi-nakamoto/ [Accessed Dec 21, 2020].

[18] Will Heasman. 2020. Here's what happened to those Satoshi-era Bitcoins – so far. *News-Coin Decrypt,* https://decrypt.co/29772/what-happened-sato shi-era-bitcoin-so-far [Accessed Dec 21, 2020].

[19] Malte Möser and Arvind Narayanan. 2017. Obfuscation in Bitcoin: Techniques and Politics. *CoRR Cornell University.* vol. https://arxiv.org/abs /1706.05432

[20] Husam Al Jawaheri, et al. 2020. Deanonymizing Tor hidden service users through Bitcoin transactions analysis. *Computers & Security* vol. 89, 101684, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2019.101684.

[21] Jamie Redman. 2020. Wikileaks Gathers $37M in BTC Since 2010 – over $400K Sent After Julian Assange's Arrest, *News Bitcoin.com*, https://news.bitcoin.com/wikileaks-gathers-37m-in-btc-since-2010-over-400k-sent-after-julian-assanges-arrest/ [Accessed Dec 21, 2020].

[22] Malcolm Campbell-Verduyn. 2018. Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law & Social Change*, vol. 69,no. 2, pp. 283-305. https://doi.org/10.1007/s10611-017-9756-5

[23] Steven Goldfeder, et al. 2018. When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. *Proc.s on Privacy Enhancing Technologies* , *Sciendo*, vol.2018, no. 4. https://content.sciendo.com/view/journals/popets/2018/4/article-p179.xml

[24] John V. Monaco. 2015. Identifying bitcoin users by transaction behavior. In *Biometric & Surveillance Technology for Human and Activity Identification SPIE Proc.s.* XII 945710 (2015). https://doi.org/10.1117/12.2177039

[25] Fergal Reid and Martin Harrigan. 2013. An analysis of anonymity in the bitcoin system, *In: Altshuler Y, Elovici Y, Cremers A, Aharony N, Pentland A (eds), Security & Privacy in Social Networks.* Springer, NY, pp 197–223. https://doi.org/10.1007/978-1-4614-4139-7_10

[26] Coin ATM Radar, https://coinatmradar.com/ [Accessed Dec 21, 2020].

[27] Ofir Beigel. 2019. Buying and Using Bitcoin Anonymously / Without ID. *99bitcoins.org.* https://99bitcoins.com/buy-bitcoin/anonymously-without-id/

[28] Malte Möser, Rainer Böhme & Dominic Breuker. 2013. An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. In *eCrime Researchers Summit*, Washington, D.C. https://ieeexplore.ieee.org/abstract/document/ 6805780

[29] Nicolas T. Courtois & Rebekah Mercer. 2017. Stealth Address and Key Management Techniques in Blockchain Systems. *Proc.s of the 3rd Int. Conf. on Info. Systems Security & Privacy (ICISSP 2017),* vol. 1. SCITEPRESS – Sc. & Tech Pub.s, pp 559-566. http://doi.org/10.5220/0006270005590566

[30] nopara73 and TDevD. ZeroLink: The Bitcoin Fungibility Framework, https://github.com/nopara73/ZeroLink . [Accessed 21 Dec. 2020].

[31] David Chaum. 1983. Blind Signatures for Untraceable Payments. *In: Chaum D., Rivest R.L., Sherman A.T. (eds) Advances in Cryptology.* Springer, MA, pp.199-203, https://doi.org/10.1007/978-1-4757-0602-4_18 .

[32] Steve Walters. 2019. Samourai Wallet Review: The Privacy Focused Bitcoin Wallet. *Coinbureau.com.* https://www.coinbureau.com/review/samourai-wallet/

[33] Joseph Bonneau, et al. 2015. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, *In IEEE Symp. on Security & Privacy, San Jose, CA,* , pp. 104-121, http://doi.org/10.1109/SP.2015.14

[34] Sarah Meiklejohn et al. 2016. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. *Communications of the ACM*, April 2016, vol. 59 no. 4, pp 86-9310. http://doi.org/10.1145/2896384

[35] What is Monero (XMR), https://web.getmonero.org/get-started/what-is-monero/ [Accessed Dec 21, 2020].