A Survey on Recent Advancements in Cryptocurrency Mixer Deanonymization

Abstract— Cryptocurrency mixers have been utilized in enhancing privacy and anonymity in blockchain transactions. However, with the growing concerns regarding illicit activities and regulatory compliance, the need to deanonymize crypto mixers has become a critical area of research. This paper explores the challenges and implications associated with the deanonymization of cryptocurrency mixers, shedding light on the various techniques, vulnerabilities, and real-world examples of successful deanonymization efforts. We also delve into the potential consequences for users, the crypto ecosystem, and regulatory authorities. By analyzing the methods and their ethical considerations, this paper contributes to a better understanding of the evolving landscape of crypto mixer deanonymization and its broader impact on the cryptocurrency community.

Index Terms—bitcoin, tumblers, mixers, ethereum, privacy, anonymity.

I. INTRODUCTION

Ever since Satoshi Nakamoto published their seminal Bitcoin whitepaper which expressed their need for "an electronic payment system based on cryptographic proof instead of trust [1] ", the dominance of Bitcoin as the principal way in which these currencies are exchanged has endured well over a decade after becoming mainstream,as seen in fig. 1 [2]. In an attempt not to rely on traditional banking methods, in which some trusted third party, such as a financial institution, would facilitate the exchange of money between two people, Bitcoin, and blockchain-focused cryptocurrencies instead "announce all transactions publicly".

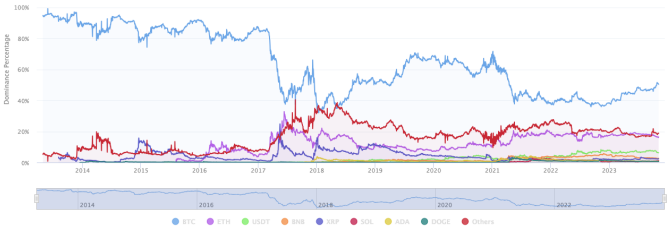


Fig. 1 Breakdown of the cryptocurrency market by cryptocurrency's percentage share of overall market

This is counterintuitive, in which a user's first reaction would be to think to keep all transactions hidden. However, "privacy can still be maintained by breaking the flow of information… by keeping the public keys anonymous" [1]. By publicly broadcasting transactions, keeping a shared ledger of all previous transactions and publicizing when an exchange is made, anonymity can still be assured, to a certain extent, by not associating the wallet addresses (derived from the public key), to the user it belongs to. This ensures a certain level of pseudo-anonymity; if the wallet address can be associated with a user, then all semblance of privacy is broken, even more so than in a traditional banking model, as a complete history of all transactions coming into and out of the wallet can now be seen. It is therefore of paramount importance for users who want to remain completely anonymous to employ additional techniques when transacting with cryptocurrencies, in addition to completely dissociating their wallet addresses with any information which links them to their real identities.

In short, "the aim of anonymization is to prevent attackers from discovering the relationship between Bitcoin addresses and real or virtual user identity information through the Bitcoin network and the blockchain used to record transactions. [3]" Therefore, given the constraints imposed by the Bitcoin protocol, users will begin to look for different ways of obfuscating their addresses, in an attempt to dissociate, as much as possible, their wallets to their identity. A widely talked about method to increase Bitcoin's 'anonymity' is by combining onion routing, through the use of the TOR browser. This can further be complemented with the use of a VPN, all of which aim to unlink the wallet address to an IP address which could be used to link transactions with users. However, "By exploiting Bitcoin's anti-DoS protection a low-resource attacker can force users which decide to connect to the Bitcoin network through Tor to connect exclusively through her Tor Exit nodes… totally isolating the client from the rest of the Bitcoin P2P network" [4].

Therefore, different methods must be employed by the user to decrease their risk of being de-anonymized. This is where the use of crypto tumblers, also known as mixers, come into use. Mixers "improve anonymity by breaking the connections between addresses… If there are multiple input-output transaction pairs, the mixer mixes them in such a way that associating input and output transactions from the outsider's point of view is impossible" [5]. However, as will be seen in this paper, ways of de-mixing these algorithms exist by exploiting vulnerabilities in the mixer services. Furthermore,

"a good number of mixers are scams" [6]. The extent to which a user is to trust a mixing service with their bitcoins extends only to the point where they believe the mixing service will legitimately perform the mixing with other user funds and give back the bitcoins, minus a service fee, once the mixing is complete, to a new address.

In addition to breaking mixers, side channel and traffic analysis attacks also exist, which "violate the privacy goals of these cryptocurrencies by exploiting side-channel information leaked by the implementation of different system components" [7]. By employing all of these techniques, a threat-actor can, under certain circumstances, completely deanonymize bitcoin and other cryptocurrency transactions, in some cases, in collaboration with crypto exchanges, even freeze wallets and recover funds, as seen in the real-world example of the ethereum-blockchain based game Axie Infinity.

II. BACKGROUND

A. *Bitcoin*

Bitcoin (BTC) is a digital currency that operates in a decentralized manner, utilizing a peer-to-peer (P2P) network to both store and verify transaction information. This information is recorded on a publicly accessible ledger, with users being represented by pseudonymous addresses [1].

Users generate pseudonymous addresses, each associated with a unique public-private key pair stored in their wallets. To safeguard against fraudulent transactions, Bitcoin users sign their transactions with their private keys which are stored privately. When transaction data is transmitted to nodes within the peer-to-peer network, these nodes use the sender's public key to confirm that the transaction has been signed by the appropriate corresponding private key. Every peer in the peer-to-peer network maintains its own copy of the blockchain, which serves as the basis for sharing and authenticating new transactions using this method. Ultimately, the blockchain prevents any single peer from exerting undue control [1].

B. *Ethereum*

Original proposed in 2014 and launched in 2015 by Vitalik Buterin who had dropped out of university under support of the Thiel fellowship, the intent behind the creation of Ethereum by Buterin was to "merge together and improve upon the concepts of scripting, altcoins and on-chain meta-protocols…by building what is essentially the ultimate abstract foundational layer: a blockchain with a built-in Turing-complete programming language [8]". Since its creation, Ethereum has evolved quite considerably, most notably in 2022 when it switched from proof-of-work to proof-of-stake so that it could be "more secure, less energy-intensive, and better for implementing new scaling solutions compared to the previous…architecture[9]".

Ethererum has since grown to become the second largest cryptocurrency, behind bitcoin, with a strong peak from October to December 2021 at the height of the NFT craze, with the value gradually decreasing and stabilizing to a more reasonable value, giving Ethererum a total market cap of above $200 billion, as seen in fig. 2 [10]. Ethereum has therefore become the blockchain of choice for games, defi (decentralized finance) and other applications which benefit from the underlying platform. This has in-turn caused Ethereum-based projects to be the target of many attacks, often exfiltrating large amounts of the cryptocurrency from compromised hot wallets, as seen in later sections.

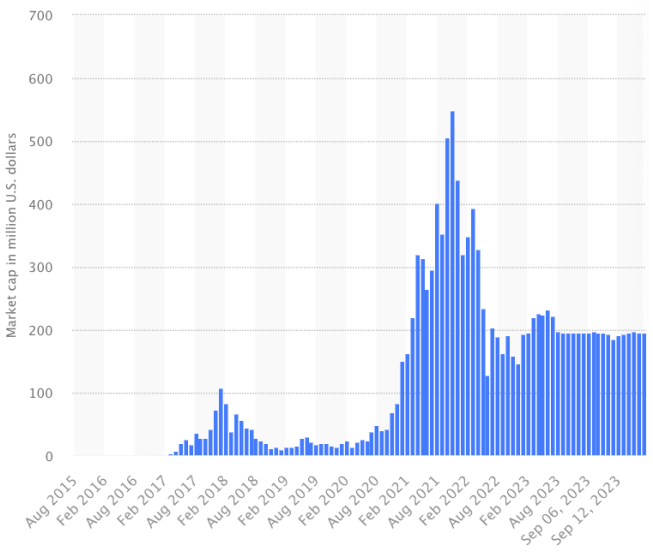


Fig. 2 Historical view of Ethereum total market cap [10]

1) *Proof-of-stake*

Having previously employed the same proof-of-work consensus mechanism as Bitcoin, in which miners would compete to create new blocks by solving computationally intensive mathematical problems, proof-of-stake is a "way to prove that validators have put something of value into the network that can be destroyed if they act dishonestly" [9]. ETH is essentially used as collateral, as users must contribute a total of 32 ETH to become validators on the blockchain, a value of $90,000 CAD at time of publishing.

After this stake has been made, validators then need to run three independent pieces of software, the execution, validator and consensus clients. These clients enable the validators to

participate in the consensus process, which is significantly more complex than proof-of-work, leading to increased complexity. Validators then enter the activation queue, in which new validators are joined to the network at a controlled rate. Upon entry, a validator can be chosen at each new slot, about 12 seconds on the blockchain, to propose a new block. A committee of validators will then attest to the validity of the new block which was proposed, checking it for correctness. Once validated, the new block is added onto the blockchain. When multiple possible blocks exist for a single slot, "the fork choice algorithm picks the block that forms the chain with the greatest weight of attestations…where weight is the number of validators attesting scaled by their ETH balance" [11].

C. *Cryptocurrency mixers*

Mixers, or tumblers, are services offering the ability to obfuscate user's funds. fig. 3 depicts the general functionality of a mixer with four users and the mixing operator. Each user sends their Bitcoin into the service and is returned another user's input to a different address. This output has a completely different transaction history associated with it. The mixer operator runs the service and is aware of all permutations between inputs and outputs. Although this high-level view may seem easily traceable, mixers use techniques that make it difficult to trace transactions and identify mixing service use on the blockchain.

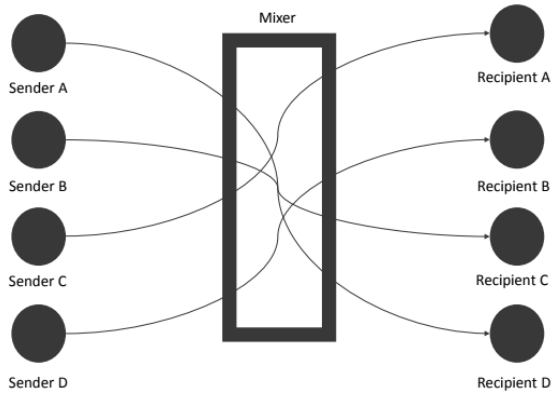


Fig.3 A High Level Mixer View

D. *Purpose of mixers*

In order to understand why a user might want to use mixers, we must first look at the previous historical approaches used by researchers to deanonymize users. Starting with large cryptocurrency institutions, such as crypto exchanges, to "reliably infer addresses is to actually transact with that service provider [12]". This includes sending or receiving bitcoins to one of the addresses the service provider has given. Knowing at least one address definitely belongs to the service provider, which will eventually be present on the blockchain, will then allow you to "tag that entire cluster with the service provider's identity [12]".

The reason why actually transacting with the provider is necessary is because, in most cases, fresh addresses will be generated every time you visit, with these addresses not yet appearing on the blockchain. A transaction therefore gives the user two important pieces of information:

- An address which can be directly linked to the service provider
- The fact that this address will end up on the blockchain.

This exact fact was used by Meiklejohn et al. as shown in fig. 4

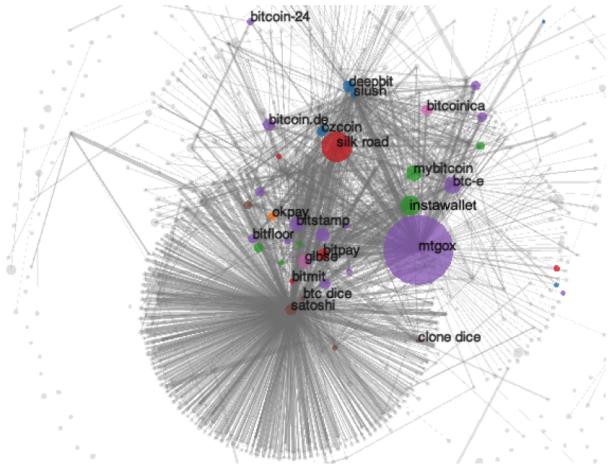


Fig. 4 Labeled visualization of bitcoin users in 2013 [13]

With this paper being published a decade ago, many of the users seen in fig. 4 have since stopped operating, such as the infamous implosion of the then-largest crypto exchange, Mt. Gox. Therefore, much more formal tools have since been created which do not require the user to individually transact with each provider. In instances when cryptocurrency was used in illegal transactions, users or members of the law enforcement community use Chainalysis, which provides users the chance to map addresses to named services.

For example, the Lazarus Group, which is believed to be a North-Korean backed hacking initiative, abused certain DeFi protocols to hop between different blockchains in their attempt to obfuscate their addresses. DeFi protocols "allow users to trade one type of cryptocurrency for another, which can make it more complicated to track the movement of funds — but unlike centralized services, many DeFi protocols

provide this ability without taking KYC information from users, making them more attractive to criminals [14]".

As seen in fig. 5, Lazarus group initially started with stealing ERC-20 tokens, which "address the need for a standard within smart contracts on the Ethereum blockchain" and are "interchangeable with another token [15]". DeFi protocols were then used to swap these tokens for Ethereum, send the Ethereum to a mixer, swap it again using more DeFi protocols for Bitcoin once the mixing was complete, and finally move then now cleaned Bitcoin to centralized exchanges to receive cash.

Having evolved a long way since Meiklejohn et al. paper in 2013, the fundamental concept of blockchain analysis remains the same, to try and link addresses with users in an attempt to de-anonymize transactions. With more sophisticated tools now being available to users, the need to use mixers has become even more crucial in trying to hide the true sources of transactions.

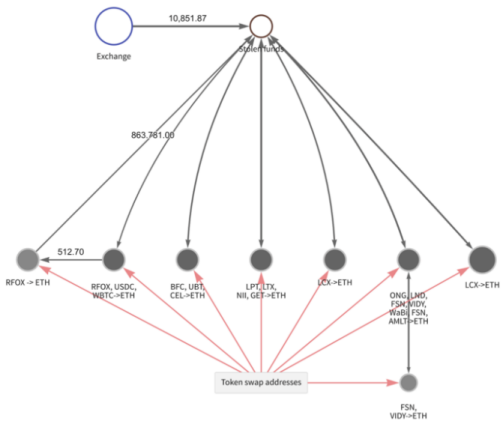


Fig. 5 Cross-blockchain analysis of hack using Chainalysis in 2022 [15]

E. *Types of cryptocurrency mixers*

1) *Centralized mixers*

Centralized crypto mixers operate by consolidating funds from multiple users into a single wallet, subsequently dividing and disbursing these combined funds through various crypto wallets. This process significantly complicates efforts by third parties to trace the origins of the funds [16].

To illustrate this idea, consider an example: Where Alice, Bob and Malice want to send funds to three other users while maintaining their privacy, They can opt for a crypto mixer and dispatch her crypto assets to it. The crypto mixer then blends these funds with other transactions, forwarding them from diverse wallets. This effectively conceals the identity of the sender and receiver, restricting this knowledge to only the middle man [20] .

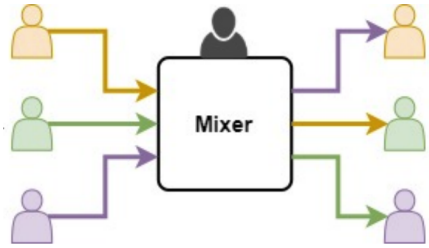


Fig. 6 Traditional Centralized Mixing with a middle-man [15]

1.1 Obscuro

Proposed by Tran Et al, To protect the mixing operations from a compromised OS and offer strong anonymity and security guarantees, They consider utilizing a hardware-based trusted execution environment (TEE).

A hardware-based TEE provides a secure environment for the mixer to run in, isolated from all other operations on the platform. This means that the mixer cannot be tampered with or interfered with by any other process. Additionally, a hardware-based TEE supports remote attestation, which allows a third party to verify that the mixer is running correctly and has not been tampered with. This is important for ensuring the integrity of the mixer and its results.[20].

1. The user makes sure that the mixer is who it says it is by requesting remote attestation and then creates a secure connection with the mixer in TEE.
2. The mixer gives the user its address (Addr Mixer) and public key (pubkey Mixer).
3. The user sends Bitcoin to the mixer's address (Addr Mixer).
4. Once the transaction is confirmed, the user tells the mixer where to send the Bitcoin back to (Addr recv).
5. The mixer mixes up the receiving addresses of all the users who sent Bitcoin.
6. The mixer sends a single transaction that sends everyone's Bitcoin to their new addresses.

The mixer destroys the address permutation after each mixing round to make it more difficult to track who sent Bitcoin to whom.

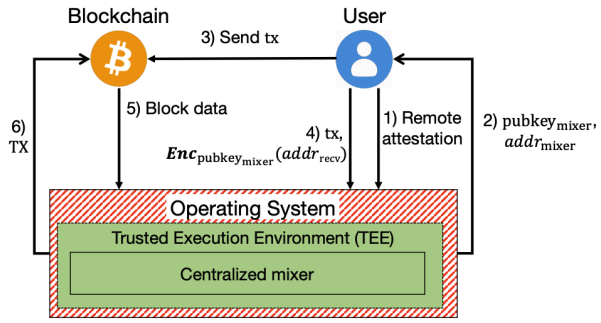


Fig. 7 Obscuro high level view. [20]

Since they are using Trusted Execution Environment, the strong memory isolation makes it hard for the malicious OS to tamper with the mixer's operations and learn the address permutation. Particularly, this baseline solution effectively addresses the following two attacks:

1. Coin theft: The attacker steals the coins that users submit to the mixer by either tricking users to send their coins to the attacker's address or by compromising the private key of the mixer's Bitcoin address.
2. Permutation leaks: The attacker learns the order in which the users' sending addresses are shuffled and their receiving addresses are assigned by reading the mixer's logs.

1.2 Mixcoin

Proposed by Bonneau et al [21], Mixcoin is a mixing protocol that provides accountability to expose malicious centralized mixers with the use of signed warranties, the warranties are implemented between the participants and the mixing service. if any malicious activity occurs on the mixers part (Stealing funds) users will have the proof of an agreement between both the parties. they can post this agreement online on public forums, raising the issues. These warranties can be verified with public information such as transactions or public keys. By doing this, Mixcoin provides an Incentive for mixers to operate in a reputable manner.

1.3 BlindCoin

Proposed by Valenta et al [22]. They propose a modification to the Mixcoin protocol that hides the input/output address mapping from the mixing server. They use a blind signature scheme and an append-only public log to achieve this. Their scheme is compatible with Bitcoin, forces mixes to be accountable, preserves user anonymity even against a malicious mix, is resilient to denial of service attacks, and scales easily to many users.

The Blindcoin protocol architecture, entities and communications are shown in Figure 8.

1. The coin sender starts the Blindcoin process by sending a Blindcoin offer to the middle mix's escrow address. The coin sender then pays the escrow address and reveals the coin receiver's address.
2. The middle mix accepts the Blindcoin offer and sends a Blindcoin partial warranty to the coin receiver. The middle mix then completes the Blindcoin warranty and sends Bitcoin to the coin receiver's address.
3. If the protocol is successful, the coin receiver receives Bitcoin anonymously.
4. The Blindcoin traffic is relayed by a peer-to-peer network. The Bitcoin transaction is then recorded on the Bitcoin blockchain. The Blindcoin partial warranty and warranty are published on a bulletin board.

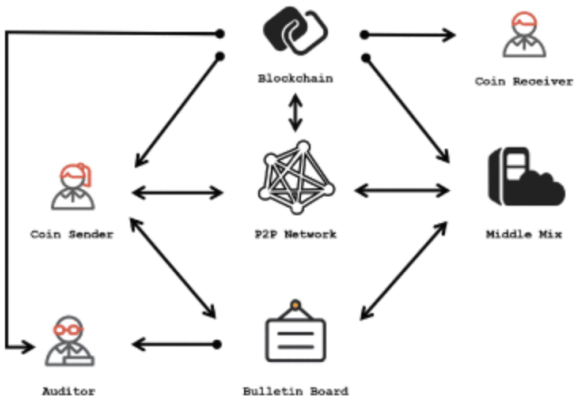


Fig. 8 Blindcoin protocol architecture [22].

2) Decentralized mixers

Decentralized crypto mixers function in a manner similar to their centralized counterparts, with a critical distinction: they operate without the oversight of a central authority. Instead, decentralized crypto mixers employ peer-to-peer (P2P) methods to enable individuals to transfer cryptocurrency without the need for third-party intermediaries [18] .

To illustrate this point, consider Bob and Alice. Rather than relying on a centralized system, Through the use of P2P technology, the crypto mixer facilitates the exchange of cryptocurrency between Alice and Bob, ensuring the security and anonymity of their transactions, all without the involvement of third-party entities .

2.1 CoinJoin

Coinjoin combines multiple Bitcoins (UTXOs) from multiple users into a single transaction. The output of this transaction yields the same value of bitcoin, but the addresses have now been changed. This makes it extremely difficult for external parties to deduce the relationship between the coinjoin transaction's inputs and outputs, because the sources of the UTXOs are obfuscated.

1. Input registration: Multiple users register their inputs (UTXOs) with the CoinJoin service.
2. Output registration: The service creates outputs (fresh addresses) for each user.
3. Coinjoin transaction creation: The service combines all of the inputs and outputs into a single transaction.
4. Transaction signing: Each user signs the transaction with their private key.
5. Transaction broadcast: The service broadcasts the transaction to the Bitcoin network.

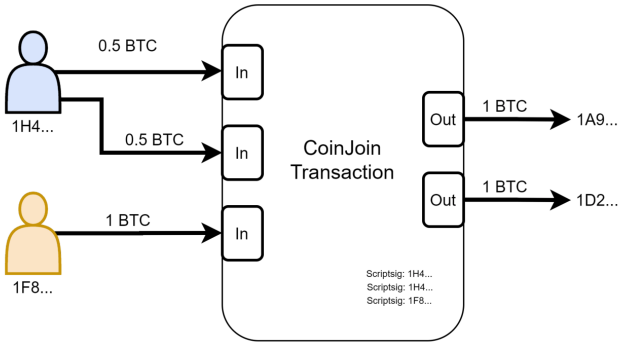


Fig. 9 CoinJoin, high level architecture [15]

2.2 CoinShuffle

Ruffing et al [23]. proposed a mixing protocol based on CoinJoin, which requires no 3rd party and is compatible with the existing bitcoin network.

CoinShuffle is implemented in three phases: Announcement phase, Shuffling phase, and Transaction Verification phase.

1. Announcement Phase : Each user creates a new, ephemeral encryption and decryption key pair, and shares the public encryption key with everyone else.

2. Shuffling Phase: Each participant in the mixing process creates a new Bitcoin address, which will be used to receive their mixed coins. The participants then shuffle these new addresses in a way that no one knows who owns which address [24]. This helps to obscure the link between the original inputs and outputs of the mixing transaction, making it more difficult to track the coins.

3. Transaction Verification Phase : Each participant in the mixing process can individually verify that their output address is in the list of output addresses. Once all participants have verified that their output addresses are in the list, they each deterministically create a (not yet signed) mixing transaction. This transaction spends coins from all of the input addresses and sends them to the shuffled list of output addresses.

Each participant then signs the transaction with their Bitcoin signing key and broadcasts the signature to the other participants. Once all participants have received signatures from each other, they can each create a fully-signed version of the mixing transaction. This transaction is now valid and can be submitted to the Bitcoin network.

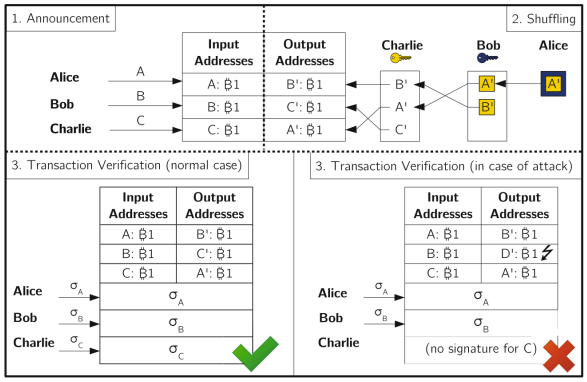


Fig. 10 Coinshuffle Phases Architecture [23]

2.3 Xim

Proposed by Bissias et al [25], We discussed the dangers of Sybil-based denial-of-service attacks on Bitcoin mixing services. To address this, the authors propose Xim, a new way to mix Bitcoin. Xim is different from previous methods because it allows participants to find each other in a decentralized way. It also does not require any changes to the existing Bitcoin software. Xim is designed to allow parties to find each other, partner, and exchange funds while protecting their privacy and ensuring fairness.

The Xim protocol works in two phases: Discovery and Fair Exchange.
Discovery Phase : In the Discovery phase, two participants, A and R, randomly take on the role of advertiser or respondent. Advertiser A posts an ad to a public messaging platform, stating their anonymous messaging platform, a unique nonce,

and the amount they desire to mix. The ad is encrypted with A's public key. Respondent R can then respond to the ad, including the ad, a nonce, and their anonymous messaging platform. R's response is also encrypted with A's public key.

Once A has selected a respondent, A posts a signed message containing their nonce and the hash of R's nonce. This notifies R that they have been selected. R then posts an ad via a transaction, which contains the message posted by A encrypted with A's public key. Finally, A publishes a response ad, which contains the hash of R's nonce. At the end of this phase, both parties have confirmed their interest in participating in a fair exchange using the protocols outlined in the rest of the document.

Fair Exchange:

The second phase of the protocol is the actual fair exchange, and it can be done using either Barber's Fair Exchange Protocol or SMC in Bitcoin.

Barber's Fair Exchange Protocol is a two-party protocol that allows two parties to exchange secrets without revealing them to each other until both parties have revealed their secrets. The protocol works by having each party generate a random secret and then commit to it using a cryptographic commitment scheme. The parties then exchange their commitments, and then they each reveal their secrets [26].

SMC in Bitcoin is a technique that allows two parties to perform secure multi-party computation on Bitcoin transactions. This means that two parties can jointly compute a function on their inputs without revealing their inputs to each other [27].

III. BITCOIN

A. Recent advancements in Bitcoin.

With Bitcoin making its comeback it's not only due to economic causes; the emergence of the Layer 2 ecosystem has been critical. Stacks and the Lightning Network are two projects that have considerably expanded Bitcoin's functionality and utility. Stacks, a Layer 2 companion chain for Bitcoin-focused smart contracts, has brought decentralized financial services to Bitcoin.

Additionally, the Lightning Network's infrastructure has improved Bitcoin's adaptability, resulting in a more effective competitor to established payment methods. The transaction cost for moving Bitcoin across the Lightning Network is $0.84 for a single transaction, highlighting its extraordinary affordability when weighed against traditional payment systems such as Visa and Mastercard. Beyond the economic and advancements in technology,

Bitcoin holds a further trick up its sleeve with the upcoming doubling in 2024. Originally, such events, which cut the incentives for processing new BTC by 50%, have been favorable for Bitcoin, adding to its attractiveness. With the changing socio-economic scenario and technological improvements surrounding the Bitcoin network, Bitcoin in 2023 has demonstrated that its finest days are likely yet ahead of it. It is not only rejuvenated; it is more powerful, more knowledgeable, and fully prepared to take back its place in the shifting global financial scene.

B. Recent Advancements in Mixing services.

Recent Advancements in mixing services have led to the development of wallet-level mixing solutions. These solutions offer several advantages over traditional mixing services, which require users to use a third-party service.

Wallet-level mixing typically works by using CoinJoin. This makes it difficult to trace the origin of any particular transaction, and it can significantly improve the privacy of cryptocurrency transactions.

We will look at a couple of these services :

Wasabi wallet :

Wasabi Wallet is an open-source, non-custodial, privacy focused wallet supporting all operating systems. It is designed to help users protect their privacy when using Bitcoin by employing privacy enhancing techniques at the wallet level itself [54].

It uses couple of methods that we saw earlier,

- Wasabi Wallet has built-in CoinJoin functionality that makes it easy for users to participate in CoinJoins.
- Tor : helps protect users' privacy by routing their internet traffic through a series of relays. Wasabi Wallet can be configured to use Tor to further enhance user privacy.
- Bech32: Bech32 is a newer address format that is more secure and efficient than the older P2SH address format. Wasabi Wallet supports Bech32 addresses by default
- Full node support: This gives users the ability to verify transactions for themselves and avoid relying on third-party nodes.

Samourai Wallet :

Samourai Wallet is a bitcoin-only wallet that is available only on Android mobile. It is a non-custodial, open-source wallet that prioritizes privacy and security [53].

It uses a couple of methods that we saw earlier, and is similar to wasabi with few extra features.

- Whirlpool: Whirlpool is an implementation of Chaumian CoinJoin designed to be extremely fast for a mobile first experience, but available on any platform.
- PayNym : is a feature that allows users to generate a payment code to receive funds. This code is more privacy-friendly as it does not link directly to the user's Bitcoin address.
- Enhanced Coin Control : allows users to have more control over the selection of inputs when sending transactions. This can be useful for managing privacy and avoiding unintentional linkage of inputs.
- Full node support: This gives users the ability to verify transactions for themselves and avoid relying on third-party nodes.
- Flat Fee: Charges a fixed Fee for transactions regardless of amount being sent (Helps with Privacy in chainanalysis)
- Verifiable Anonymity Set : The group of users whose transactions are mixed together is verifiable.

C. Deanonymization Attacks.

We will begin by examining some of the most prevalent attack techniques. Subsequently, we will examine how these attacks can be applied to each of the mixers discussed in Section II.

- **Permutation Leak:**

If an adversary can observe the permutation of input and output addresses, they can effectively reverse the mixing process and identify the true sources of the bitcoins.

For example, an adversary is able to see the logs or database that shows how the input and output addresses are linked together. This is a major issue with Centralized mixers, as usually centralized ones have access to the mappings of input to output transactions [15].

- **Sybil Attacks:**

Sybil attacks occur when a single attacker creates multiple identities and uses them to manipulate the network. In the methods like CoinJoin, a Sybil attacker could create fake participants to inflate the anonymity set and once users try to mix their funds, since the attacker controls most of the participating user address, he could potentially trace the origin of transactions. as the anonymity of the whole method relies on the anonymity set [51].

- **Address Clustering**:

Grouping addresses based on certain characteristics, such as common ownership or spending patterns, could reveal information about the users behind those addresses [50].
Some examples of Address clustering

- Deposit address reuse :

The fact that the exchange deposit addresses can be reused provides a way to link every other address that interacts with that address, and since Exchanges have KYC requirements. Any analytics firm that has a partnership with that particular exchange can access personal information about the individual's Ethereum blockchain. These distributions are carried out using smart contracts, where the owners determine the recipients based on their past activity or online form submissions.

A single user could create multiple addresses and perform actions with numerous social media accounts to game the system

- Airdrop multi-participation

Airdrops are a common method of distributing tokens on them. but usually the multiple addresses that the user uses would be linked to one. using on-chain address clustering we can map these and reward the legit users. and filter out the malicious users who are trying to take advantage of the airdrops.

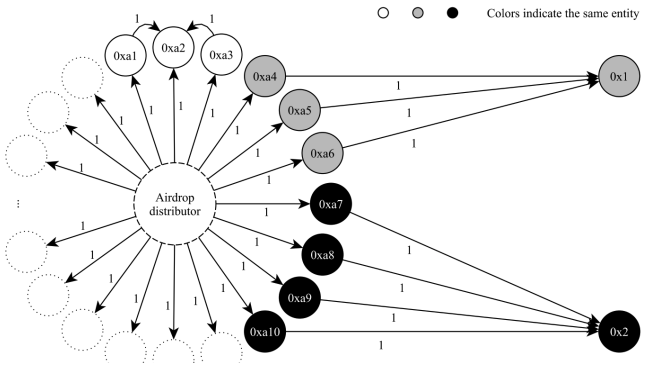


Fig. 11 address clustering using Transaction Graph analysis to figure out sybil attacks in airdrop participations [50].

- **Timing Analysis :**

Timing analysis is a technique used to investigate the temporal patterns of transactions in blockchain networks [52]. By scrutinizing the timestamps associated with transactions, analysts can uncover potential links between seemingly unrelated transactions. This approach is particularly valuable for tracing the movement of funds through obfuscated transactions, involving mixing services.

If a user initiates a transaction shortly before or after using a mixing service, it raises suspicion that the two transactions may be linked. This is because the user's funds are likely to be mixed together with those of other users, and the timing of their transactions could provide a clue about the movement of those funds.

For instance, if a user sends a large sum of cryptocurrency to a mixing service and then shortly thereafter initiates a transaction sending a similar amount of cryptocurrency to a different address, it is reasonable to suspect that these transactions are related. The timing of the transactions suggests that the funds from the mixing service were likely used to fund the second transaction. We will look at the deanonymization of the FTX Hacker using this method later on in this report.

- **Off chain - Network Traffic Analysis :**

By monitoring the network traffic between users and the mixer, analysts can observe various patterns and correlations that can aid in identifying the origin or destination of transactions [15].

Usually, the frontend of the mixing service is hosted on a Centralized server. if an adversary can log the connections to and from the centralized server, this can lead to deanonymization attacks.

For instance, if a user connects to the mixer from a specific IP address or geographic location, it could indicate that the user is based in that region. Additionally, if a user's network traffic patterns closely resemble those of another user, it could suggest that the two users are related or have similar activity patterns.

Hence, most of the users who participate in mixing services usually access these services over TOR and VPNs. which provide an additional layer of anonymity.

- **Compromised Mixer :**

Mixer services could be compromised or coerced to get the transaction details. The possible way for this method to work is if the law enforcement has access to both the input and output of the mixer service, they may correlate the data to deanonymize users. This is a rare chance but possible and usually occurs with centralized mixing services.

- **Use of Unmixable Coins:**

If users send or receive cryptocurrency that is unique or distinguishable in some way, these coins may become identifiers that link transactions together, for example if a User sends a transaction with certain decimal value, the output of the transaction is set to have a similar decimal value after the fess. an adversary uses this value to perform taint analysis and map the transactions.

We will look at the deanonymization of the FTX Hacker using this method later on in this report.

- **Small Mixing Set Size:**

The number of people who are mixing at the same time is a good indicator of how well the mixing is working. A large mixing set will protect people's identities and make it harder to track down transactions on the blockchain.

This is especially true with Coinjoin based Mixing services, as in those the mixing set size is proportional to the anonymity provided by the mix.

- **Compromised Randomization**

Since the mixing service is randomized, it could lead to patterns or predictability in the mixing, reducing the effectiveness of the anonymization process.

Most of the on-chain de-mixing algorithms aim to predict the randomization of the mixing service.

- **Join-then-abort**:

The adversary joins the mixing process but then stops before it is finished, which messes up the mix. This will lead to more availability attacks as participants must restart the whole mixing process [15].

- **Dropping of Participants:**

The mixer operator or an adversary can stop certain users from taking part in the mixing process to make the group of people who are mixing smaller.

- **Fee analysis :**

Analyzing transaction fees associated with mixing transactions might provide insights into the origin of funds [21].

There are a number of tools and techniques available for tracing transactions through fee analysis. Some of the most common methods include:

- Clustering: This method involves grouping transactions together based on their fee rates. Transactions with similar fee rates are likely to have been sent from the same source or destination.

- Heuristics: This method involves using various anomalies to identify transactions that are likely to be suspicious. For example, transactions with very high fees may be flagged for further investigation.
- In the earlier days of bitcoin, mixing services had a fixed mixing fee, this led to blockchain analysts figure out if a transaction is related to a mixing service or not based on the transaction fee paid to the mixing operator.

- **Cookies :**

When performing online blockchain-based transactions, websites or payment gateways generate cookies. These cookies gather various user data, including personal information like name, email, and address, as well as transaction details like items purchased and time of purchase. Websites also utilize cookies to collect additional information, such as transaction-specific wallet addresses.

The collecting user data through cookies can serve legitimate purposes, such as retargeting advertisements, but it also carries the potential for malicious exploitation. Cookies can be employed to establish a link between a user's identity and their blockchain account, including cryptocurrency wallets and portal accounts. This linkage can then be used to uncover a user's true identity. Additionally, unintentional data leaks from cookies can be combined with JavaScript code to track a user's system configurations and gather detailed information about their device [49].

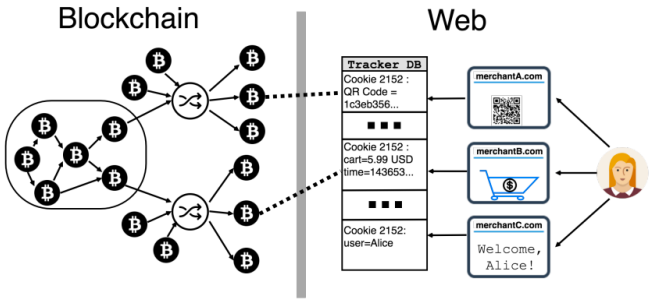


Fig. 12 High level diagram of how cookies can be used to trace users even if they use different wallet addresses [49].

- **Wallets and Clients :** These can be used to track users.

A revised privacy agreement published recently says that the wallet provider MetaMask will collect users' IP and Ethereum wallet addresses in on-chain transactions. This is significant news as Metamask is one of the most popular wallet providers for EVM based chains with more than 30 Million active monthly users.

The privacy implications of this is tremendous as now that wallet provider has access to what Dapps you use, the websites that you visit, and the transactions and other on-chain activities that you perform [48].

For example, if you used a Mixer with this wallet to mix your funds, it's essentially useless as the wallet provider knows your wallet addresses and your on-chain activities and can export this data to anyone who requests it.

Now We will look into some of the deanonymization and availability attacks on the Mixing methods that we saw earlier.

1) Obscuro

Availability Attacks :

Since the Mixing operations are inside an Trusted Execution Environment, we can ensure that after each round of mixing, the recipient will get the coins. If the mixer transaction is not submitted to the bitcoin network, the senders can get the coins back after a set time period using the refund script that was provided in the deposit transaction.

Anonymity attacks :

Obscuro addresses some of the drawbacks associated with centralized mixers, such as the risk of compromised mixer operators as it operates inside a Trusted Execution Environment.

- Permutation performed within a Trusted Execution Environment is not accessible to the adversary.
- Obscuro's design ensures that it is hard for an adversary to prevent users from learning the identity of the mixer, unless the adversary controls all the public bulletin boards that users can access.
- An adversary cannot tamper with the blockchain data that Obscuro is processing because Obscuro does not store it outside of a Trusted Execution Environment. Data within a TEE is protected with an integrity guarantee, making it impossible to tamper with.
- If an adversary restarts Obscuro and feeds a malicious blockchain fork, Obscuro will not be able to collect the deposits from that blockchain because its secret keys are destroyed when the previous execution is terminated

during the restart. Similarly, because the Obscuro uses a new address to receive coins when it detects malicious blockchain forks, any deposit transaction will be used to mix at most once.

- Even if an adversary manages to link some senders and recipients in the malicious blockchain fork, the recipient addresses will never appear on the main blockchain. Instead, affected users will receive their deposits back through our refund mechanism script.

While Obscuro addresses some of the concerns with centralized mixers, On-chain analysis can still leak a lot of information.

- Obscuro's mixing set size is limited by the capacity of the mixer. This means that it may not always be possible to mix a large number of transactions together, which can reduce the anonymity of the mixing process.

- Potential for collusion: The centralized nature of Obscuro also makes it vulnerable to collision attacks. In a collusion attack, the mixer operator could collude with other parties to deanonymize users' transactions.
- Vulnerability to blockchain and timing analysis, as Obscuro doesn't provide any time delays, Timing analysis is possible by an adversary.

2) Mixcoin

Anonymity attacks :

- Mixcoin does not fully guarantee relationship anonymity, even though users cannot directly identify the recipient addresses of others. This is because the mixer operator maintains a record of all connections between senders and their recipients.
- It also does not provide a Large mixing set guarantee, this would lead to a smaller anonymity set, leading to on chain taint analysis.
- It uses randomized mixing fees, this can prevent forms of on-chain analysis as a fixed mixing fee can serve as taint on the transaction.
- Finally, Mixcoin is not effective against strong active attackers. An active attacker could link every escrow address to its originating mix, and then deanonymize users.

Availability Attacks :

- Mixcoin is resistant to join-then-abort attacks because users participate in the mixing process independently. This means that an attacker cannot disrupt the mixing process by joining and then aborting the transaction.

Coin theft attacks :

- The mixer operator may steal users' coins. To provide accountability, they give users signed certificates. However, this can damage the reputation of a malicious mixer operator.

3) Blindcoin

Anonymity attacks :

- Blindcoin improves Mixcoin's anonymity by employing a blind signature technique, ensuring that the mixer operator remains unaware of the relationship mappings between transactions.
- It also does not provide a Large mixing set guarantee, this would lead to a smaller anonymity set, leading to on chain taint analysis.
- Blindcoin does not achieve perfect mix indistinguishability. This is because Blindcoin uses a predictable mixing process, which can be used to link input coins to output coins.

Availability Attacks :

- Blindcoin is the same as mixcoin in terms of availability and is resistant to join-then-abort attacks because users participate in the mixing process independently. This means that an attacker cannot disrupt the mixing process by joining and then aborting the transaction

Coin theft attacks :

- The mixer operator may steal users' coins. To provide accountability, they give users signed certificates. However, this can damage the reputation of a malicious mixer operator.

4) CoinJoin

Availability Attacks :

A large anonymity set can make CoinJoin transactions more susceptible to Denial-of-Service (DoS) attacks. it only needs one malicious participant to start the mixing process and then halt it halfway through to disrupt.

Coordinating a large number of users to participate in a CoinJoin transaction can be difficult and time-consuming. This is because users need to find each other, agree on the terms of the transaction, and synchronize their actions.

Anonymity Attacks :

One of the drawbacks of CoinJoin is that at least one party involved in the mixing transaction usually has access to the mapping between inputs and outputs. For example, the initiator of a CoinJoin transaction made via JoinMarket has access to this information, and he pays for the privilege of knowing his counterparties don't also have access to that information [28].

Since Coinjoin requires n-of-n multisignature transactions where N is usually large, it can be very easy to spot on the blockchain through chainanalysis since the size of the n-of-n multisig transaction is usually very large, this leaks some anonymity.

Some forms of coinjoin use a centralized coordination service to facilitate the whole process. This gives the opportunity for the centralized mixing service to be a passive adversary.

The anonymity set of a coinjoin transaction is the number of participants in the transaction. so implementations of this mixing solution should enforce a large anonymity set for mixing to take place. otherwise, it would be easy for an adversary to link the transactions, since there are only a limited number of people who were using the service at that particular mix. There have been cases where a smaller anonymity set has led to funds being traced.

Factors Affecting Anonymity Set:

- Number of participants: The more participants in a coinjoin transaction, the larger the anonymity set.
- Transaction size: The larger the transaction size, the more difficult it is to anonymize. This is because the number of participants for larger transactions drops significantly.
- Coinjoin software: Different coinjoin software may have different anonymity set guarantees.

a Sybil attacker could create fake participants to inflate the anonymity set and once users try to mix their funds, since the attacker controls most of the participating user address, he could potentially trace the origin of transactions. as the anonymity of the whole method relies on the anonymity set.

5) CoinShuffle

Availability Attacks :

CoinShuffle is based on coinjoin, so it's vulnerable to the same set of availability attacks, as Denial-of-Service attacks. using which an adversary could flood the network with fake Coinshuffle transactions, preventing legitimate transactions from being processed.

CoinShuffle can detect and remove aborted users in join-then-abort attacks, the remaining participants must restart the whole mixing process. Consequently, They only mix among a relatively small set of users (e.g., 50 participants).

Coordinating a large number of users to participate in a CoinShuffle transaction can be difficult and time-consuming. This is because users need to find each other, agree on the terms of the transaction, and synchronize their actions.

The last peer in the decryption mixnet is in a unique position to determine the outcome of the shuffling.

Anonymity Attacks :

- in Coinshuffle, none of the parties have access to the mappings between inputs and the output, unlike coinjoin where one does [29].
- Coinshuffle uses an "Accountable Anonymous Group Messaging" protocol called dissent to resolve traffic analysis attacks.
- In terms of Anonymity set and its relativity to privacy, it is the same as Coinjoin and the same issues mentioned in Coinjoin section III apply here.

6) Xim

Availability Attacks :

Since XIM is a two-party mixing protocol that mandates participants to pay a participation fee and advertise their availability on the network, it prevents Join-then-abort attacks.

Anonymity Attacks :

It has the same level of anonymity as a coinjoin transaction, that is at least one party involved in the mixing transaction usually has access to the mapping between inputs and outputs.

D. Known successful Deanonymization attacks

1) Wasabi Wallet (Coin Join)

One of the most prominent claims of Wasabi's deanonymization came from Chainalysis, a blockchain analytics firm. In 2019, Chainalysis published a report claiming to have successfully demixed Wasabi transactions,

linking them to their original sources. Chainalysis's methods involved analyzing the patterns of Bitcoin transactions and identifying connections between mixed coins.

The analyst from Chainalysis started with the transaction ID, which he knew belonged to the entity that he was going to be tracking.he was tracking a input of 25 BTC, He looked at the inputs and one output, and opened up the one output through transaction graph analysis. He knew this was the target, so he marked . This one output was a wasabi mix, as he could see. He knew 50 bitcoin went in, and it was the largest input in the entire mix. He could see that there was a change output here of 43.99. This was his entity that he was tracking. He went ahead and marked this past them.

So on his second mix here, he again went down and he expanded the unmixed change. He followed long, again, and he marked this as his entity in the third mix. He went ahead and expanded the exchange again, and followed them along. This was the fourth mix.

On the fourth mix, he could see that this 25 bitcoin output had been clustered, meaning that an address was reused somewhere. The 25 BTC unmixed change went to the same address as a 0.401 BTC mixed output. User didn't do this address reuse, the client did. What he would do is he would expand this as it enters into the fifth mix one, two, three, four, and five.

So all the analyst from chainanalysis had to do was follow the unmixed change until they reached this point where they noticed address reuse, combining the 25 bitcoin change from this mix and a post mix output. That postmates output was right here, because of this one postmates output that is connected to this mic uh unmixed change, we are able to associate all of these post mix outputs to this entity.

And because they spent it to poloniex, anyone who has a relationship with poloniex like chainanalysis could ask them for more information. Poloniex has kyc information, so all they have to do is look in their records and can provide identity information to law enforcement or anyone who's asking.

So in short, even though the user didn't make any mistakes in the mixing process, the mixer client did, wasabi mixer had a poor implementation of the CoinJoin Method, where one of the addresses used in mixing, mixed with the inputs and outputs. This led to the user being de-anonymized.

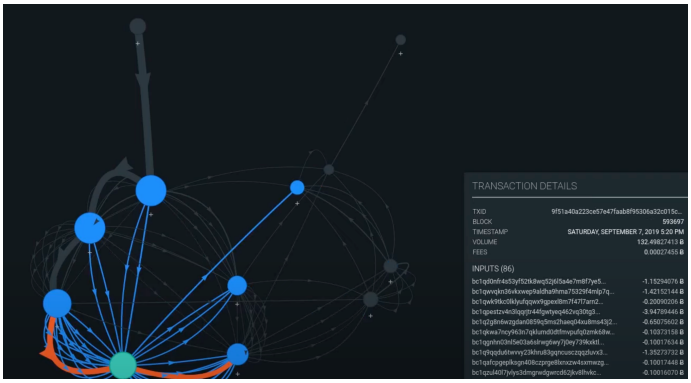


Fig. 13 Transaction Graph analysis done by this analyst. Green Node is the reused address.

2) FTX exploiter

In the FTX's collapse in November 2022, an unknown actor executed a sophisticated hack, stealing a staggering $480 million in customer funds in the Ethereum network.An analytics firm, reported that the exploiter swapped nearly 72,500 ETH to bitcoin via ThorChain. Soon after, ThorChain paused its operations, due to concerns over potential law enforcement scrutiny due to the value of funds being transferred from the hack.

Then he swapped the funds to the Bitcoin network. But why is the exploiter swapped from Ethereum to Thor to Bitcoin to begin with? One of the main reasons is liquidity. On Bitcoin there's more mixers, and they're different. On Ethereum, after Tornado was sanctioned, a lot of people stopped using it and liquidity decreased, and as a result the anonymity set also decreased.

The hacker tried to mix about 4,000 BTC through Sinbad (Centralized mixer, a clone of the Blender.io mixing service) but due to the huge volume of funds (4,000 BTC) at once the anonymity set of the mixer was essentially ruined. The mixer was basically overused. so even after the mix, the funds were linked back to the hacker and were traced.

This is an example of a Volume and timing analysis attack on a mixer, by tracing the net volume flow. you can essentially deanonymize the user if they are distinct enough.

IV. ETHEREUM

A. Recent advancements

1) *Current state of crypto regulations in Canada*

To precede discussions on Ethereum-specific uses of mixers, gaining a holistic view of how the government of Canada currently approaches dealing with cases of cryptocurrency mixers in the context of money laundering

(ML) will provide insight on how their use is controlled and investigated on the federal level.

A noticeable change in rhetoric with how the Canadian government was addressing crypto exchanges in particular happened in February of 2023, in the aptly named "Crypto Asset Trading Platforms: Pre-Registration Undertakings Changes to Enhance Canadian Investor Protection [31]". The notice was published to "describe a change in the CSA (Canadian Securities Administrators) staff practice in connection with our expectation that crypto asset trading platforms (CTPs)... while they seek registration and related exemptive relief file a pre-registration undertaking". The notice specifically cites recent large-scale crypto lender insolvencies such as Voyager, Celsius and FTX as the catalyst for this notice needing to be made. The notice imposed a series of restrictions on how, moving forward, CTPs could continue to operate in Canada.

These new rules and restrictions included:

- Restricting using crypto assets for pledging or re-hypothecation
- Restricting offering margin credit or leverage in crypto trading
- Restrictions on proprietary tokens issued by the CTPs themselves in calculating working capital
- Any global affiliates of the CTPs will also need to sign the notice
- CTPs now need to have a chief compliance officer
- Restricting the specific crypto assets available for sale, including stablecoins.

These restrictions have proved too much for certain crypto exchanges to adhere to, including exchanges created in Canada, most notably, Binance. In May of 2023, only 3 months after this notice was made, Binance decided to completely withdraw from Canada, citing that "(the) new guidance related to stablecoins and investor limits provided to crypto exchanges makes the Canada market no longer tenable for Binance at this time [32]". This would mean that the potential losses of completely pulling out of the Canadian market were less than the potential revenue to be gained from entering new markets or increasing market share in markets with fewer restrictions. Perhaps key in Binance's decision to pull out was the value of their very own proprietary token, Binance Coin, or BNB, as seen in fig.12 [33].

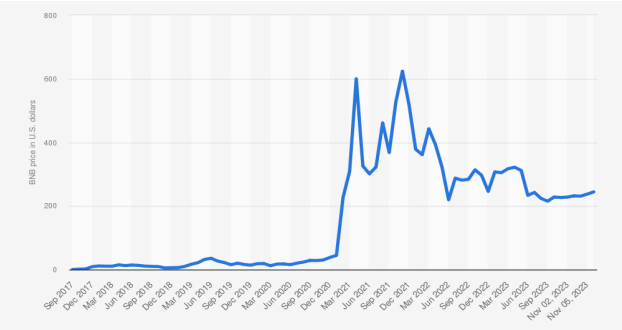


Fig. 14 Binance Coin historical price graph, with total market cap of over $37 billion USD.

Furthermore, the Canadian government has tried to curb the rise of mixer based crypto fraud and ML through a few new initiatives such as [34]:

- The Financial Innovation Act in Alberta, in which fintech companies can test new crypto coins in sandboxes.
- The Bank of Canada exploring state-backed cryptocurrencies
- The Ontario Securities commission providing certain tokens exemptive relief from dealer registration

However, "while Canada's cryptocurrency regime may be evolved and quite regulated, this is not necessarily true for its crypto laundering mitigation regime [34]". Governmental agencies, such as the Anti-Fraud Center go on to say that "most of these schemes offered higher-than-standard monetary returns which consistently resulted in large scale losses or total losses to investors [34]". This goes hand-in-hand with the RCMPs documents "400 percent increase in cryptocurrency fraud" between 2017 and 2021. With the rise of fraud clearly being known to the Canadian government, in which citizens may be losing considerable sums of money with no reprise in making their money back, the ways in which the government institutes oversight on cryptocurrencies is still "limited (in) jurisdictional oversight and clarity on deconflicting responsibilities…Canada has redundant resources and roles among various organizations [34]"

With the apparent lack of technical expertise, resources and cross-institutional support between different agencies in solving crypto related crimes, in can be concluded that "the RCMP would benefit from looking at tumblers and mixers as integral to money laundering schemes, analyzing and investigating them as they do banks in traditional financial crime schemes [34]".

2) Tornado Cash

One of the most infamous instances of an Ethereum-based mixer is that of Tornado Cash, which is a "is a smart contract-based crypto asset mixer that uses zkSNARKs to create a decentralized privacy-enhancing protocol [35]". The reason for its infamy is due to its highly publicized addition to the Foreign Assets Control (OFAC) sanctions in 2022, making the use of the Tornado Cash protocol itself illegal to any U.S Citizen. Understanding why a mixing service caught the attention of a major world power is understanding what made Tornado Cash so effective and mixing funds.

Tornado Cash utilizes zkSnark, or Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, which is an implementation of zero-knowledge proof, in which the prover shows the verifier their attainment of a piece of information without revealing the information itself. Looking at zkSnark specifically from a Tornado Cash perspective, zkSNARKs are used to prove that users have the right to withdraw funds from a pool without revealing which funds belong to them. This is accomplished by generating a proof that the user has knowledge of a secret key that allows them to withdraw funds from the pool, without revealing the key itself. This means that zkSnark allows Tornado Cash to break the link between a deposit and a withdrawal address, meaning that it is difficult to trace the flow of funds on the blockchain. Furthermore, it is important to note that since Tornado Cash runs on the Ethereum blockchain, it utilizes smart contracts to manage the deposit, pooling, and withdrawal of funds [35]. Finally, Tornado Cash utilizes Merkle trees for storing the commitments of the deposited funds. This approach ensures that the funds are securely held in the smart contract and facilitates effective verification of zero-knowledge proofs produced by the smart contract. It enables efficient and secure storage of fund commitments, contributing to maintaining protocol privacy and security.
The combination of smart contracts, Merkle trees and zkSnark allows the underlying algorithms of Tornado cash to be cryptographically secure, however, to effectively mix funds, Tornado Cash's operation can be broken down into three main stages:

1. Deposit: A user transfers their cryptocurrency to a Tornado Cash smart contract on the blockchain. The smart contract then provides the user with a unique deposit address and allows them to select the amount of cryptocurrency they wish to deposit and the anonymity set they want to be included in. This anonymity set represents the number of other users' deposits that will be mixed along with theirs.
2. Pooling: once a specific number of users have completed their deposits, their funds are combined in a pool. This process ensures that it becomes challenging to trace back the original source of these funds. Furthermore, mixing is conducted in such a way as to prevent anyone from connecting any given deposit with subsequent withdrawals.
3. Withdrawal: Users can proceed with withdrawing their funds from the pooled resources into another address without revealing which specific funds belong to them. New addresses will typically be generated for this, so as to leave no trace of the original address or to potentially link the address with the user.

The efficient implementation of Tornado Cash, along with the ease-of-use of DeFi protocols in exchanging one cryptocurrency for another has meant that "individuals and groups had allegedly used the mixer to launder billions worth of crypto since 2019, including the $455 million stolen… by the Lazarus Group. [36]". Culminating into the aforementioned inclusion on the OFAC sanctions list. It is important to note however that "no person or organization can 'pull the plug' as easily on Tornado Cash as they could with a centralized service. [VI]" The decentralized nature of Tornado Cash has meant that even after its sanctioning, a significant amount of currency still flows through it, even today, as seen in fig 15 [37]. Two of the three founders of Tornado Cash have also been indicted on money laundering among other charges, with the third founder currently still at large [38].

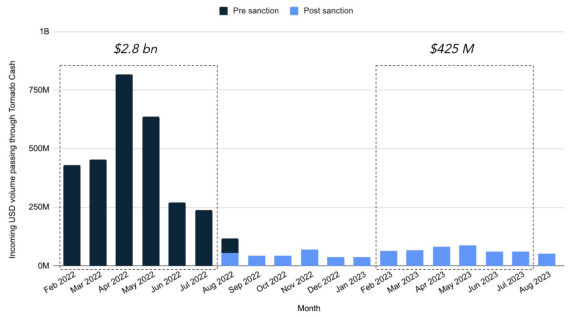


Fig. 15 Pre and post sanction incoming USD trading volume passing through Tornado Cash.

3) Related Works

Wang et al. [39] have conducted an empirical study on how zero-knowledge proof blockchains may improve or worsen privacy. It explains that non-privacy-focused blockchains offer pseudonymity rather than anonymity, and retrofitting a

blockchain with privacy is challenging. The authors also found that the accuracy of anonymity set claims made by ZKP mixers is often overstated, which can have significant implications for user privacy. Seres et al [40] have provided a practical and efficient solution for coin mixing on Ethereum, achieving strong anonymity and resistance to denial-of-service attacks. The protocol uses a combination of encryption, shuffling, and zero-knowledge proofs to ensure privacy without relying on a trusted setup.

B. Axie Infinity

1) *Background*

Axie Infinity is a blockchain-based game that was developed by Sky Mavis, a Vietnamese game studio, and launched in 2018. The game is built on the Ethereum blockchain and uses non-fungible tokens (NFTs) to represent the 'Axies', which are the virtual creatures that players collect, breed, and battle with. In traditional gaming, players spend money to purchase in-game items, but they do not receive any monetary compensation for their time and effort spent playing the game. In contrast, "play-to-earn" games like Axie Infinity allow players to earn in-game tokens like "Smooth Love Potions" (SLP) and "Axie Infinity Shards" (AXS), which can be exchanged for real money. Players can acquire these tokens by participating in various activities within the game. Axie Infinity has also attracted significant investment, with the game's native token, AXS, reaching a market capitalization of over $10 billion in August 2021[41]. The game is typically played by battling your team of 'Axies' versus another player, with an example of a match being shown in fig. 16 [42].

Fig. 16 A typical Axie Infinity battle environment

With the potential to make money whilst playing the game exists for players, it is evident that certain players will try to use advanced tools or algorithms to maximize their revenue. Papers such as 'Artificial Intelligence to Learn Battle Strategies in Axie Infinity' by Chen [42] describes the use of Monte Carlo Tree Search (MCTS) to train an AI for Axie Infinity battles. Although the ultimate goal of creating an AI that can beat human opponents more than it loses was not reached, it does show that there is significant interest in exploiting the game's mechanics and underlying systems for the benefit of the player.

2) *Deanonymization and side channel attacks*

In March of 2022, hackers now known to have been associated with the Lazarus Group targeted and managed to steal $600 - 650 million worth of ETH from the Ronin Network, an Ethereum sidechain specifically created for Axie Infinity. This marks it as the world's single largest cryptocurrency hack [43]. The hack was made possible due to compromised private keys obtained from a social engineering attack. At the time, "the Ronin Network used a set of nine validator nodes to approve transactions on the bridge, and a deposit or withdrawal requires approval by a majority of five of these nodes [43]". By exploiting vulnerabilities in the cross-chain bridge, the centralized proof of authority scheme used by Sky Mavis meant that 4 of these validators were now compromised, with one more being needed until full access of the entire network was reached. The fifth validator was controlled by the Axie Decentralized Autonomous Organization (DAO), and was able to be accessed by a program which allowed the platform to perform better under heavy loads.

After the hack was made public, it was seen that some of the stolen Ether was making its way to centralized exchanges, such as Binance, which was able to track 86 compromised accounts and recover $5.8M of stolen funds [44]. However, there was still a considerable amount of funds yet to be recovered, which prompted the use of different side channel approaches.

Thanks to the accounts provided by Erin Plante, current VP of Investigations at Chainalysis in September of 2023 on the 'Planet Money' podcast, a look into the real-world deanonymization process could take place [45]. According to details revealed on the podcast, Chainalysis was able to 'reverse the mixing process', or de-mix transactions. it was revealed that they were 'taking advantage of certain vulnerabilities' which, on the podcast, was inferred to mean storing all addresses linked to a mixer, tracking addresses coming and out of the mixer, and analyzing patterns in how the money flows. Chainalysis claims that it knows where "90% of the stolen crypto is", and is waiting for the Lazarus group to cash-out the crypto from centralized exchanges so that it can freeze the transaction from taking place, thereby recovering the funds. Plante describes that there was only a 20

minute to 1 hour window between the crypto moving addresses before it would be impossible to keep tracking. By cooperating with the exchanges, Chainalysis was able to recover $30M [46]. However, since much of the details were left out of the podcast, this prompted more research into the previously discussed transaction graph analysis of section II and into network-level deanonymization.

3) *Network-Layer Deanonymization*

By attributing the blockchain to the application layer and the P2P network it uses as the network layer, it was noticed that "when a node creates a transaction, it connects to many nodes at once and broadcasts the transaction. If sufficiently many nodes on the network collude with one another (or are run by the same adversary), they could figure out the first node to broadcast any transaction [12]." This would mean that the original person who requested the transaction could be revealed. The adversary could "link the transaction to the node's IP address [12]".

In their paper "Deanonymization and linkability of cryptocurrency transactions based on network analysis [47]", Biryukov and Tikhmirov argues that network level attacks can be used to link transactions to specific users and together with timing attacks, can reveal the origin of a transaction.

Mixers are also mentioned in the paper [47]:

- Mixers and tumblers can help to obfuscate the flow of coins in cryptocurrency transactions.
- However, users must agree to co-sign the transaction using additional means of communication, which is unscalable without coordination by a trusted third party.
- Mixers and tumblers can be vulnerable to attacks by malicious operators who may steal users' funds or spy on transactions.
- Alternative implementations of mixing protocols include CoinJoin and CoinShuffle, but these protocols also have limitations, such as coordinating the transactions and needing many participants.
- While mixers and tumblers can provide some privacy benefits, they are not a complete solution to the deanonymization and linkability issues surrounding cryptocurrency transactions.

The paper focuses on discussing and analyzing the behavior of nodes in the network, and more closely, how messages going through these nodes propagate through the network. By looking at the content of the message along with their timing, a well-connected adversarial node can use this information to deanonymize users and link their transactions to their IP addresses. The propagation of messages across different Bitcoin testnet can be seen in fig.17, the difference of propagation time between regions can be used to deduce what region the message originated from.

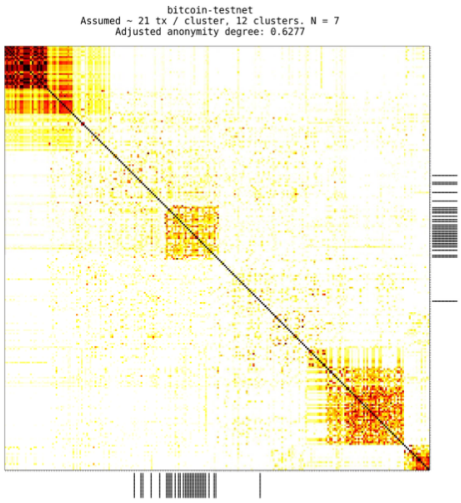


Fig. 17 Propagation of messages in combined Bitcoin testnet of California, Tokyo and Frankfurt

The paper also mentions address advertisement messages (ADDR). These messages are used by nodes in the network to advertise their IP addresses to other nodes. When a new node joins the network, it sends an ADDR message to its peers to let them know its IP address. Other nodes can then use this information to connect to the new node and propagate transactions.

The paper examines the behavior of ADDR messages in the network and proposes a technique for leveraging this information to link transaction clusters to IP addresses. By analyzing the number of nodes that relay an ADDR message, we can distinguish between recently joined nodes and older nodes that are re-broadcasting old ADDR messages. This information can then be used to identify the IP addresses of nodes in a transaction cluster, which may be entry nodes for the transaction originator.

C. Kucoin Hacker

1) Background

Kucoin, a prominent cryptocurrency exchange, suffered a recent hack (2020), losing over $150 million in assets. The attacker employed Tornado Cash, a non-custodial mixer, to conceal a portion of the stolen funds. However, an examination of on-chain activity has uncovered clues that

could aid in the identification of the perpetrator. We will delve into the hacker's technique of depositing a substantial amount of ETH into Tornado Cash. Subsequently, an analysis of Tornado Cash withdrawals is presented, revealing a collection of addresses likely owned by the hacker.

2) Deanonymization

Soon after the hack, the hacker moved large amounts of ETH and ERC20 Tokens and other cryptocurrencies from Kucoin's hot wallets.

He then swapped the tokens for ETH using the Uniswap router, and then deposited the ETH into Tornado cash's 10 ETH and 100 ETH Contracts [55].

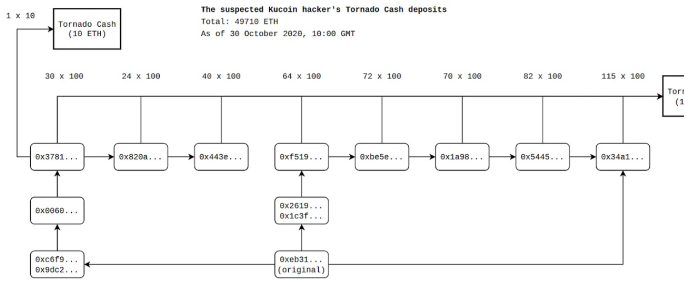


Fig. 18 Connections between accounts believed to be controlled by the hacker. Each edge represents a Transfer of ETH [55].

He deposited 497 deposits of 100 ETH each into the Mixers contract and then two addresses did 437 withdrawals of 100 ETH each after a short-while.Given the Volume of ETH and the timeline, it gives an obvious mapping of input and outputs for these mixing transactions.

This is an example of Timing and Volumetric analysis to deanonymize the transactions.

After this, the attacker transferred funds to Binance and was found to be conducted by the same set of hackers as the Axie infinity hack, Lazarus - A north korean based hacking group which is believed to be state affiliated.

V. CONCLUSION

The cryptocurrency landscape has witnessed significant advancements in recent years, particularly in the realm of privacy-enhancing technologies. Bitcoin and Ethereum, two of the most prominent cryptocurrencies, have seen the development of various mixing services aimed at obfuscating transaction history and enhancing user anonymity. While these mixers offer a degree of anonymity, they are not without their vulnerabilities. Deanonymization attacks have emerged as a growing threat, posing challenges to the privacy and security of cryptocurrency users.

The effectiveness of mixing services depends on their ability to resist deanonymization attacks. Centralized mixers, such as Obscuro, Mixcoin, and BlindCoin, have been shown to be susceptible to various attack vectors, including availability attacks, anonymity attacks, and coin theft attacks. Decentralized mixers, such as CoinJoin, CoinShuffle, and Xim, offer improved resilience against these attacks, but they are not entirely immune.

The Ethereum blockchain has also seen advancements in privacy-enhancing technologies, with the development of Tornado Cash and other mixer protocols. These protocols leverage the unique features of Ethereum to provide enhanced anonymity compared to Bitcoin mixers. However, their long-term resilience to deanonymization attacks remains to be seen.

In conclusion, the pursuit of anonymity in the cryptocurrency space is a complex and evolving endeavor. While mixing services offer a degree of privacy, they are not without their vulnerabilities. Ongoing research and development in privacy-enhancing technologies are crucial for addressing these challenges and ensuring the security and anonymity of cryptocurrency users.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009, http://www.bitcoin.org/bitcoin.pdf.

[2]"Live cryptocurrency charts & market data," CoinMarketCap, https://coinmarketcap.com/charts/

[3]Q. ShenTu and J. Yu, "Research on Anonymization and De-anonymization in the Bitcoin System", https://doi.org/10.48550/arXiv.1510.07782

[4] A. Biryukov and I. Pustogarov. "Bitcoin over Tor isn't a good idea", https://doi.org/10.48550/arXiv.1410.6079

[5] Y. Hong, J. Lee, H. Kwon, J. Hur, "A Practical De-mixing Algorithm for Bitcoin Mixing Services", https://dl.acm.org/doi/10.1145/3205230.3205234

[6] J. Crawford and Y. Guan. "Knowing your Bitcoin Customer:Money Laundering in the Bitcoin Economy" *13th*

International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE), 202
[7] F. Tramer, D. Boneh K.G.Paterson, ”Remote Side-Channel Attacks on Anonymous Transactions”, https://eprint.iacr.org/2020/220.pdf
[8] V. Buterin “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform”. https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf
[9]“Proof-of-stake(POS),”ethereum.org, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
[10] R. de Best, “Ethereum Market Cap 2013-2023,” *Statista*, https://www.statista.com/statistics/807195/ethereum-market-capitalization-quarterly/
[11] “Consensus mechanisms,” ethereum.org, https://ethereum.org/en/developers/docs/consensus-mechanisms/
[12] A. Narayanan, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton: Princeton University Press, 2016.
[13] S. Meiklejohn et al., “A fistful of bitcoins: Characterizing payments among men with no names: Communications of the ACM: Vol 59, no 4,” Communications of the ACM, https://dl.acm.org/doi/10.1145/2896384
[14]“Theft, money laundering, and NFT market manipulation underline importance of safety and compliance in WEB3,” Chainalysis, https://www.chainalysis.com/blog/chainalysis-web3-report-preview-safety-compliance-defi/
[15] J. Pakki, Y. Shoshitaishvili, R. Wang, T. Bao, and A. Doupé, “Everything you ever wanted to know about bitcoin mixers (but were afraid to ask): Financial Cryptography and data security,” Guide Proceedings, https://dl.acm.org/doi/abs/10.1007/978-3-662-64322-8_6
[16]R. Stevens, “Bitcoin mixers: How do they work and why are they used?,” CoinDesk Latest Headlines RSS, https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used/
[17] Gregory Maxwell, “CoinJoin: Bitcoin privacy for the real world,” 2013. [Online]. Available: https://bitcointalk.org/index.php?topic=279249
[18]T. Ruffing, P. Moreno-Sanchez, and A. Kate, “CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin,” Tech. Rep.
[19] J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, “CoinParty: Secure multi-party mixing of bitcoins,” in CODASPY 2015 - Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. ACM, mar 2015, pp. 75–86. [Online]. Available: http://dl.acm.org/citation.cfm?id=2699026.2699100
[20] M. Tran, L. Luu, M. Suk Kang, I. Bentov, and P. Saxena, “Obscuro: A Bitcoin Mixer using Trusted Execution Environments,” in ACSAC ’18 (Annual Computer Security Applications Conference), ser. ACSAC ’18, vol. 18. New York, NY, USA: ACM, 2018, pp. 692–701. [Online]. Available: https://dl.acm.org/citation.cfm?id=3274750
[21] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, “Mixcoin: Anonymity for bitcoin with accountable mixes,” in Financial Cryptography and Data Security, N. Christin and R. Safavi-Naini, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 486–504.
[22] L. Valenta and B. Rowan, “Blindcoin: Blinded, accountable mixes for bitcoin,” in Financial Cryptography and Data Security, M. Brenner, N. Christin, B. Johnson, and K. Rohloff, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 112–126.
[23] T. Ruffing, P. Moreno-Sanchez, and A. Kate, “CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin,” Tech. Rep.
[24] Chaum, D.L.: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM 24(2), 84–90 (1981)
[25] G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, “Sybil-resistant mixing for Bitcoin,” in Proceedings of the ACM Conference on Computer and Communications Security, ser. WPES ’14. ACM, 2014, pp. 149–158. [Online]. Available: http://doi.acm.org/10.1145/2665943.2665955
[26] S. Barber, X. Boyen, E. Shi, and E. Uzun, “Bitter to better — how to make bitcoin a better currency,” in Financial Cryptography and Data Security, A. D. Keromytis, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 399– 414.
[27] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, “Secure multiparty computations on bitcoin,” in 2014 IEEE Symposium on Security and Privacy, 2014, pp. 443–458.
[28]https://coinjournal.net/news/bitcoin-privacy-improvement-compare-coinjoin-coinshuffle/
[29]Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate”CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin?”
[30] https://poloniex.com/ Crypto Excahnge.
[31] Canadian Securities Administrators Staff notice 21-332 - OSC, https://www.osc.ca/sites/default/files/2023-02/csa_20230222_21-332_crypto-trading-platforms-pre-reg-undertakings.pdf
[32] “Binance pulls out of Canada amid new crypto regulations,” Reuters,

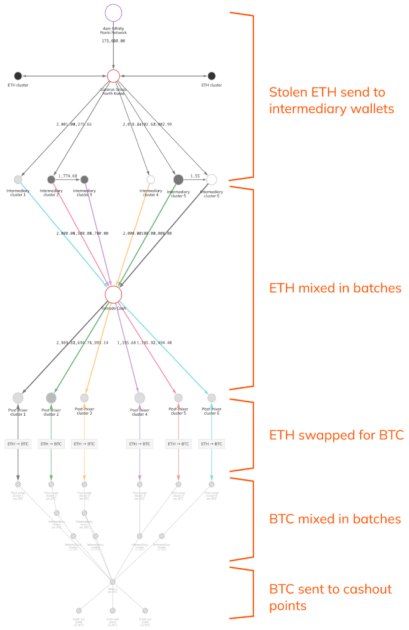
https://www.reuters.com/technology/binance-will-proactively-withdraw-canada-2023-05-12/
[33] R. de Best, “Binance Coin Price History Sep 2017 - Nov 16, 2023,” Statista, https://www.statista.com/statistics/1274339/binance-coin-price-index/
[34] C. Leuprecht and J. Ferrill, *Dirty Money: Financial Crime in Canada*. Montreal: Published for the Institute of Intergovernmental Relations School of Policy Studies, Queen’s University by McGill-Queen’s University Press, 2023
[35] M. Nadler and F. Schär, “Tornado cash and Blockchain Privacy: A primer for economists and policymakers,” Economic Research - Federal Reserve Bank of St. Louis, https://research.stlouisfed.org/publications/review/2023/02/03/tornado-cash-and-blockchain-privacy-a-primer-for-economists-and-policymakers
[36] B. Quarmby, “Sanctions couldn’t ‘pull the plug’ on tornado cash: Chainalysis,” Cointelegraph, https://cointelegraph.com/news/decentralization-meant-sanctions-couldn-t-pull-the-plug-on-tornado-cash-chainalysis
[37]“Tornado cash volume dramatically reduced post sanctions, but illicit actors are still using the mixer: Trm insights,” RSS, https://www.trmlabs.com/post/tornado-cash-volume-dramatically-reduced-post-sanctions-but-illicit-actors-are-still-using-the-mixer
[38]M. Sigalos, “Tornado cash founders charged with laundering more than $1 billion, including millions for North Korea,” CNBC, https://www.cnbc.com/2023/08/23/tornado-cash-founders-charged-with-laundering-more-than-1-billion-including-millions-for-north-korea.html
[39]Z. Wang et al., “On how zero-knowledge proof blockchain mixers improve, and worsen user privacy,” arXiv.org, https://arxiv.org/abs/2201.09035
[40]I. A. Seres, D. A. Nagy, C. Buckland, and P. Burcsi, “Mixeth: Efficient, trustless coin mixing service for Ethereum,” Cryptology ePrint Archive, https://eprint.iacr.org/2019/341
[41] E. A. Cavalheiro, L. R. Falck, A. M. Rodriguez, and A. S. Pereira, Cryptocurrency Dynamics Revealed: Unveiling the Intricate Interaction Between Price, Rewards, and Token Allocation in the Axie Infinity Ecosystem, https://www.arcjournals.org/pdfs/ijmsr/v11-i9/1.pdf
[42] Alex Chen, Artificial Intelligence to Learn Battle Strategies in Axie Infinity, https://www.publish0x.com/axie-infinity-research-and-journey/axie-infinity-strategy-guide-choosing-the-right-axies-for-ba-xoomnlm
[43] 10 biggest crypto heists of all time (to date) , https://www.techopedia.com/biggest-crypto-heists-of-all-time
[44] S. Bertillo, “Binance recovers $5.8m worth of stolen funds linked to Axie Infinity Hack,” BitPinas, https://bitpinas.com/news/binance-recovers-5-8m-worth-of-stolen-funds-linked-to-axie-infinity-hack/
[45] J. Guo, “How investigators cracked the Axie Infinity crypto hack,” NPR, https://www.npr.org/2023/09/21/1200738378/planet-money-how-investigators-cracked-the-axie-infinity-crypto-hack
[46] N. D. and D. Nelson, “US government recovers $30m from crypto game Axie Infinity Hack,” CoinDesk Latest Headlines RSS, https://www.coindesk.com/policy/2022/09/08/us-government-recovers-30m-from-crypto-game-axie-infinity-hack/
[47] A. Biryukov and S. Tikhomirov, Deanonymization and linkability of cryptocurrency transactions based on network analysis, https://ieeexplore.ieee.org/document/8806723/
[48] ”MetaMask Stores User IPs And Wallet Addresses” https://medium.com/coinmonks/metamask-stores-user-ips-and-wallet-addresses-do-this-to-avoid-getting-tracked-231d5265a0a5
[49] ”The Role of Cookies in Blockchain Security” https://www.cookielawinfo.com/cookies-and-blockchain-security/currency).
[50] Victor, F. (2020). Address clustering heuristics for Ethereum. In Financial Cryptography and Data Security (pp. 32-47).
[51] Bissias, G., Ozisik, A. P., Levine, B. N., & Liberatore, M. (2016, October). Sybil-resistant mixing for Bitcoin. In Proceedings of the 13th Workshop on Privacy in the Electronic Society (pp. 371-378). ACM.
[52] Neudecker, T., Andelfinger, P., & Hartenstein, H. (2016, July). Timing Analysis for Inferring the Topology of the Bitcoin Peer-to-Peer Network. In 2016 IEEE 13th International Conference on Advanced and Trusted Computing (ATC) (pp. 113-119). IEEE.
[53] https://samouraiwallet.com/ A privacy focused bitcoin wallet for Mobile devices.
[54] https://wasabiwallet.io/ a privacy focused Bitcoin Wallet with builtin CoinJoin Functionality.
[55] https://github.com/weijiekoh/tracing_the_kucoin_hacker The repository contains the data and code used for identifying the September 2020 Kucoin hacker's withdrawal addresses from Tornado Cash.
[56]Joinmarket,“Joinmarket,”URL:https://github.com/JoinMarket-Org/ joinmarket-clientserver,2015.
[57]Möser, M., & Böhme, R. (n.d.). Join Me on a Market for Anonymity. Retrieved November 17, 2023,

fromhttps://www.infosecon.net/workshop/downloads/2016/pdf/Join_Me_on_a_Market_for_Anonymity.pdf
[58]Ghesmati, S., Fdhila, W., & Weippl, E. (n.d.). Usability of Cryptocurrency Wallets Providing CoinJoin Transactions. Retrieved November 17, 2023, from https://eprints.cs.univie.ac.at/7392/1/2022-285.pdf
[59][ANN] Joinmarket - Coinjoin that people will actually use. (n.d.). Bitcointalk.org. Retrieved November 17, 2023, from https://bitcointalk.org/index.php?topic=919116.0
[60] Design for improving JoinMarket's resistance to sybil attacks using fidelity bonds. Gist. Retrieved November 17, 2023,https://gist.github.com/chris-belcher/18ea0e6acdb885a2bfbdee43dcd6b5af/
[61]Cynthia Turcotte , ChipMixer : Building a Better Bitcoin Mixer,https://bitcoinist.com/chipmixer-building-a-better-bitcoin-mixer/
[62] LiveDarknet, "ChipMixer: Complete Guide On How To Use A ChipMixer" https://livedarknet.com/p/chipmixer-a-complete-guide-on-how-to-use/
[63]One of the darkweb's largest cryptocurrency laundromats washed out, https://www.europol.europa.eu/media-press/newsroom/news/one-of-darkwebs-largest-cryptocurrency-laundromats-washed-o
[64]"Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over $3 Billion of Unlawful Transactions" https://www.justice.gov/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3
[65]"ChipMixerReview2023",https://thebestbitcoinmixers.com/chipmixer-review/

APPENDIX

Research papers used and other Miscellaneous documents**:**

INSE 6120 Research



A full breakdown of the Axie Infinity deanonymization process by Chainalysis.

E. Plante, "Crypto community makes profiting hard for North Korean hackers," Chainalysis, https://www.chainalysis.com/blog/axie-infinity-ronin-bridge-dprk-hack-seizure/