An Analysis into the Practical Applications of Bitcoin Chaumian CoinJoin mixers

Rishab Kinnerkar, *Department of Electrical and Computer Engineering, Iowa State University*
riskin@iastate.edu

***Outline*— Criminal activity thrives in the dark net and is challenging to curb due to the high degree of anonymity and security provided by the network browser and transaction currency. Bitcoin is the most popular cryptocurrency used in the dark net and among criminals. It provides a high degree of anonymity for online transactions, primarily, because there is no personal information associated with Bitcoin accounts. However, each bitcoin transaction is stored on a publicly available blockchain ledger and the transaction history from a bitcoin account is available. In case of criminal activity, this could be used as potential evidence by law enforcement agencies for attributing bitcoin transactions to users. Thus, cryptocurrency tumblers (known as Bitcoin mixers in case of Bitcoin transactions) are used by bitcoin users who wish to make it further difficult for others to be able to track them. Most mainstream bitcoin mixers (centralized mixer) work by being a middleman between the bitcoin sender and the receiver during transaction and try to obscure the trail between them. One way they increase transaction anonymity is by adding multiple transactions between the sender and the receiver from different sources at different times. Thus, making it difficult to attribute the original transaction between the sender and receiver from the blockchain. Such services are sought after by criminal enterprises who want to launder money or in general by those who want to stay anonymous while transacting on the darknet. These mixers were usually short-lived mainly due to being taken down by law enforcement agencies. A theoretically superior cryptocurrency tumbling protocol which makes use of Chaumian Coin Join protocol had not yet been popular due to the difficulty involved in implementing it in practice. However, they are slowly starting to gain popularity with the advances being made towards their feasibility and they hold the potential to become the state-of-the-art Bitcoin mixers based on the higher security and integrity they provide in theory when compared with other mixing protocols. In this project, I have provided a background on the different types of bitcoin mixers. Have presented a case as to why Chaumian CoinJoin mixers such as Wasabi Wallet are gaining popularity and other centralized mixers are being phased out.**

***Index Terms*— Bitcoin mixers, Chaumian Coin Join, Decentralized mixers**

I. Introduction

In the Bitcoin system, like a secret banking system (e.g Swiss Banking) anonymity is achieved by hiding the names of the users carrying out transactions. However, Bitcoin transactions are publicly available on the Bitcoin blockchain, and this could be used for identifying a Bitcoin user. As an example, if one were to use Bitcoin to purchase their lunch at a specific time. The lunch seller could carry out a de-anonymization attack which would make use of patterns resembling these transactions on the blockchain and attribute it to the buyer. Once the bitcoin wallet is linked with its owner the attacker will be able to see all past transactions made through that wallet. This is one of the reasons why Bitcoin founders had recommended using different addresses for every new transaction. However, this method has a vulnerability which is that if payment is received to a bitcoin wallet with multiple transactions and then for the outgoing transaction from the wallet the money would be pulled from multiple addresses which would be a strong indication that all these addresses belong to the same wallet.

To strengthen anonymity cryptocurrency tumblers started being used. Bitcoin tumblers are mostly referred to as Bitcoin mixers and in the rest of this project I'll refer it in that manner. The main goal of these mixers is to hide transactions between the sender and receiver which are made available publicly in the Bitcoin blockchain. To do so there are broadly 2 different types of protocols-: Centralized mixing and Decentralized mixing.

Centralized mixers

Centralized mixers are the most popular bitcoin mixers. In this protocol a trusted entity serves as a middleman between the sender and the receiver. If there are many users directing their coins through the central mixer then attributing the outgoing coins to the incoming coins becomes very difficult and thus the user's identity is not compromised. An example of 3 people using a centralized mixer is shown in Fig.1.

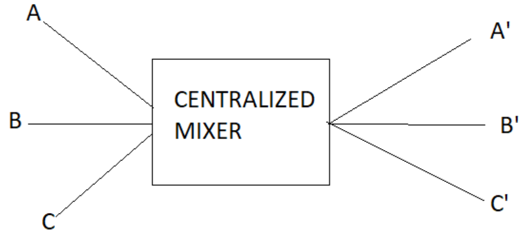


Fig.1 Shows a high-level overview of a centralized mixer. In the above protocol A, B, C are the senders and A', B', C' are the receivers corresponding to receiving from A,B,C respectively.

In this black box diagram of a centralized mixer once it gets coins from A, B and C there are several ways in which the sending can be done to A', B' and C'. Mainly the coins are sent in smaller denominations with different addresses and at varying time intervals and these specifics vary across different mixer services. Examples of these different types of mixing protocols would be Mixcoin and Blindcoin.

There are 2 problems with a centralized mixing protocol. Firstly, the users need to trust the centralized mixer with their coins because if the mixing service were to not make any payments to the receiver and basically steal the sender's money there is nothing the sender can do about it. In the past there have been many bitcoin mixers which have turned to theft. At a given point when the centralized mixer had a significant amount of coins in its wallet it would shut down its service and keep the senders money. Centralized mixers using Mixcoin or Blindcoin protocol would be accountable in the fact that the sender would be allowed to know whether their coins have been received by the sender. But these protocols don't provide any protection from outright theft. However, they hold the mixers accountable and any theft could be detected, and it could damage the mixers reputation. Secondly, the mixing service could keep a log of the transactions each user makes, and they could use it or hand it over to the concerned authorities who could then use it for compromising the sender's identity. Although many centralized mixers claim to not keep any logs it is not easy to verify this because in a centralized mixer the coins are entirely trusted upon to the mixing service. This problem can only be mitigated by decentralized trustless environment operating mixers.

Decentralized Mixers

Theoretically, decentralized mixers are considered to provide the best user confidentiality and transaction integrity. Bitcoin founders recommended to use a new address for every transaction to be safe from ID de-anonymization. However, the problem with using different addresses for payments would be that to pull coins into the new address it would need to take it from the wallet. Now if multiple addresses are being transacted with a single wallet it is probable that all those addresses are linked to a single user. This makes the task of finding the users identity difficult but is still not considered a very strong safety measure. Along these lines a decentralized mixer requires a large group of people to cooperate with each other and send money to a mixing server which takes each user address as input and outputs fresh addresses. Essentially what happens is that the new address which the user receives money from has a highly difficult untraceable source. So, the user has coins which now cannot be linked back to their wallet. This protocol takes care of the two problems described for Centralized mixers. Users sending the money can verify whether the correct amount of money they are transacted for would be received at their new address and only then sign off on the transaction. A single user can thus abort the mix transaction. This prevents the mixing server from stealing coins from the users. Secondly, with proper implementations it is possible for users to keep their identity private from other users as well as the server. To do so a secure multi-party computation must be used. In this protocol, the participants use their private data, which in our case would be their bitcoin addresses, as inputs to a pre-image resistant function and send this output to the mixing service instead of their private addresses. Now the outputting addresses will depend on the input of every user but because the users don't reveal their private address to other user's and the mixer is not able to predict the input values from the output of the secure multi-party computation. What makes implementing MPC protocols inefficient is that it must handle the sorting of oblivious data for which no efficient algorithm is known. In addition, this method needs to have each, and every user sign off on the transaction and this leads the mixing service vulnerable to DOS attacks. CoinJoin, CoinParty, CoinShuffle are some examples of a decentralized mixer. As of November 2019, Wasabi Wallet, JoinMarket, Darkwallet, Shufflepuff are some decentralized bitcoin mixers. Chaumian Coin Join also called CoinJoin was detailed for the first time in 2013 by Gregory Maxwell but implementing this protocol in practice is difficult for the above-mentioned reasons and thus centralized mixers have been more popular. Wasabi Wallet is the most popular decentralized mixer using CoinJoin in its mixing and has seen a huge increase in popularity in 2019.

II. Existing Literature

The present research done has been mainly focused on centralized mixers. [3] Balthasar, Thibault et. Al. had chosen several different centralized Bitcoin mixers. They signed up for their services and carried transactions as the buyer and seller. They also kept a track of the existing centralized mixers and their lifespans. In addition to the trust aspect involved in centralized mixers this paper highlighted some of the common practices among these centralized mixers which make them not a fully safe tool to use. DarkLaunder, BitLaunder and CoinMixer were some of the most popular mixing services out there and had several common features which could possibly be because they had a common founder. It was found that these mixers store their user data regarding their user's previous transactions with the service, including their exact date, Bitcoin addresses and IPs. Many mixer services get arrested by law enforcement agencies and so for a mixer service to be storing information which could potentially lead to identifying the Bitcoin users using the mixing service is considered unsafe. In addition, it was possible to find the IP address of the server which was hosting the mixer. This research also brought into light the common paths these centralized mixers take while transacting and that the level of difficulty to trace back these transactions is not too hard. Helix was another popular mixing service and seemed to be safer than the above-mentioned 3 services for these vulnerabilities were not found in Helix. But Helix was found to have wallets and withdrawals of same customers on the same transaction which made it possible to identify them easily.

There have been different types of mixing protocols proposed which have a high degree of anonymity and can be implemented without happening to rely on the trust of the third party. One such protocol as described by Tran et al. is called Obscuro [2]. It makes use of trusted execution environments (TEEs) which lends credibility to the code of their mixing protocol and their data handling. In addition, their protocol prevents the manipulation of inputs which further increases the protocols security. As stated in [10], centralized mixers started to issue certificates to users to provide accountability. However, the problem with the certifier was that they had access to all the transactions in the mixer for that session. And so, certification was regarding to be an unsafe verifiability method implemented in the way mixers like BlindCoin and MixCoin had done. So, then later implementations in mixers allowed users to validate the remote attestation to see whether the mixing service is only running what it is supposed to.

Most of the proposed mixing protocols required extra transactions in addition to the sender-receiver coin exchange which resulted in a delay and higher fees. This problem is mitigated in CoinJoin mixers which perform mixing and transactions in a single step. This is possible since Bitcoin transactions can be fulfilled by multiple users. Many CoinJoin Mixers initially required their users to have the same amount of coins to be mixed [14]. This was done by mixers due to the perceived increase in anonymity. However, it has been proven by Maurer et Al. , that using the same amount of coins or different is providing the same security [14].

In the preceding section I have described the popular existing mixing services and have listed out their weaknesses and advantages.

1) Different Mixing services

Untrusted mixers

These are centralized mixers in name but do not actually make use of the centralized schemed safety protocols which are necessary for keeping the user address, transaction or receiver ID anonymous. They are like Bitcoin users placed in between a sender and a receiver all of which are under the command of 1 entity. Despite the low security and risk involved in the past some of the most popular mixers such as Alphabay, Bitmixer and Helix had been functioning as untrusted mixers and were the most used mixers in the world. A lot of these mixers were scams which would shut down when they had a significant amount of coins in the mixer and it would not be possible to trace them. Some of these mixers would get shutdown by law enforcement agencies. And their user data has fallen into the hands of law enforcement agencies. Since they did not use any significant security and would be a trusted middleman their anonymity was as good as doing Bitcoin transactions directly. This is because adding an extra node in the transaction path is considered to not increase security significantly [14].

Mixcoin

It is a centralized mixing system with an accountability mechanism implemented in it to prevent theft by the mixer. However, the accountability transcripts which make use of signed warrants would allow to show a theft taking place but not actually prevent any theft from happening. This would mean that mixers could still steal coins when there is a significant amount of coins in the mixer. In order to tackle the scam dealings of mixers, mixcoin was proposed. However, there isn’t any mainstream Bitcoin mixer using this protocol in practice.

Blindcoin

Blindcoin is a similar protocol to mixcoin but with improvements. It utilizes blind signatures which further increases security and the user has the option of committing coins to an address they own from the beginning of a session. So, in the mixing stage all party members give their target address and after receiving all the addresses the mixer proceeds with the transaction.

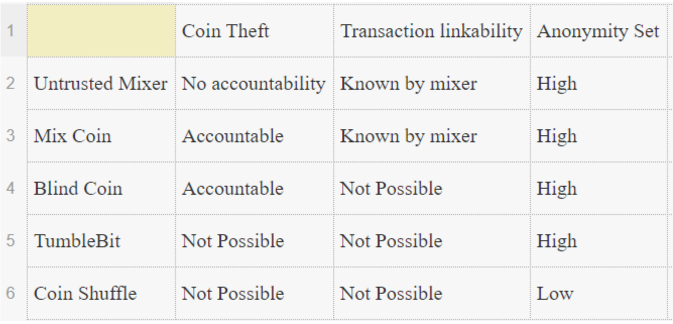
Tumblebit

Deriving its foundations from the RSA protocol, Tumblebit is a protocol which uses techniques from secure two-party computation and zero-knowledge proofs. Considered to be a secure and reliable protocol, its shortfall lies in the fact that it is expensive to maintain. At the beginning of this protocol Alice would request a bitcoin transaction with a certain number of bitcoins to the mixer. And parallelly Bob would contact the mixer for posting the same transaction to him. If the mixer decides to allot Alice’s request to Bob, then Bob would receive an RSA encrypted ciphertext. Now Bob cannot decrypt the RSA ciphertext since Alice’s private key is needed to decrypt it. Now in the payment phase, Bob will send a blinded part of the encrypted text to Alice. Alice in turn sends the blinded ciphertext to the mixer which can crack it since the corresponding private key to the blinded ciphertext is with the mixer. If the mixer accepts this as a valid pair, then the transaction proceeds. Stratis was a mixing service which makes use of this protocol. It would charge a mixing fee of about 2% of the transaction fee. The maintenance for such kind of a protocol is difficult as it is vulnerable to DOS and Sybil attacks.

Coin Shuffle

CoinJoin hides the shuffling of Bitcoins from outsiders but the ones having internal access can see which addresses the input addresses get linked to. Being a decentralized mixer, it requires participant coordination beforehand to identify peers and transactions. The communication cost in this protocol scales quadratically and it becomes to shuffle coins among large number of users. Thus, the anonymity set in Coin Shuffle protocol is limited. This is true for other decentralized protocols like Coin Party. Shufflepuff is a mixing service which uses Coin Shuffle protocol and has a maximum user limit of 50 for a mixing set.

Fig.2 below summarized the weaknesses and strengths of the 5 described protocols.



1		Coin Theft	Transaction linkability	Anonymity Set
2	Untrusted Mixer	No accountability	Known by mixer	High
3	Mix Coin	Accountable	Known by mixer	High
4	Blind Coin	Accountable	Not Possible	High
5	TumbleBit	Not Possible	Not Possible	High
6	Coin Shuffle	Not Possible	Not Possible	Low

Fig.2 Shows the protection from coin theft, transaction linkability and anonymity set provided by the 5 different mixing protocols

III. CoinJoin Mixers

According to [15], "CoinJoin mixing is a trustless method for combining multiple Bitcoin payments from multiple users into a single transaction to obscure the trail between the original sender and receiver". Below is the detailed functioning of the protocol.

In this example, Alice is a user who is one of several participants. Bob is also Alice but using a different TOR identity.

In the first step, Alice connects to the server. Alice would be able to see the coins which are being mixed currently and this would give her an idea of how long it would take for her coin mixing to be complete and what amounts of coins would she be allowed to mix in. And so, information Alice sends to the server during this session is in the form on inputs and blinded outputs as shown in Fig.3 Blinding is a technique by which an agent can provide a service to client in an encoded form without knowing either the real input or the real output. An implementation of blinding techniques in this protocol makes the user ID anonymous from the server and other users.

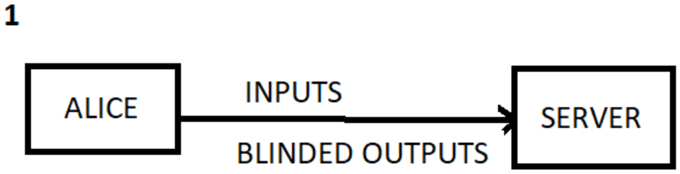


Fig.3 Alice initiates the process by verify the server information and sending her inputs and blinded outputs.

In the second step, the server receives Alice's input and checks for the validity of her inputs and determine which all transaction can they be used for. If Alice is verified and her transaction can proceed then the server replies with a blinded signature to Alice as shown in figure Fig. 4

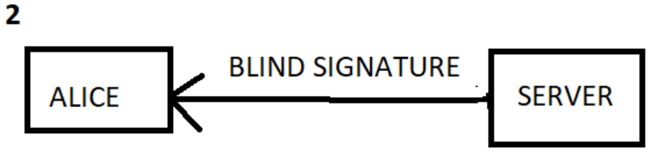


Fig.4 Once Alice's inputs are verified the server will send Alice a blind signature.

The second step is over when all participants have been verified. Next is the output registration phase. Alice would now reconnect under a new TOR identity, in this case Bob. And would submit the unblinded output and unblinded signature to the server as shown in Fig.5.

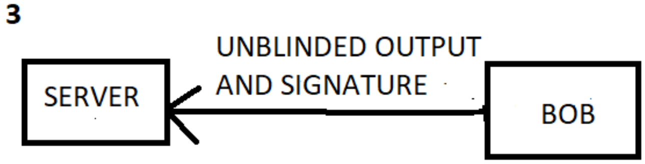


Fig.5 Alice takes on a new TOR identity Bob and sends the unblinded output and signature to the server for that session.

This verifies that Bob is a participant for the session. The blind signature is only verifiable by Alice, but the server doesn't know that Bob is Alice. And this anonymity is higher the more participants are in the coin join session.

Once the server has received the unblinded output and signature from all the participants the server validates all of them. And after the validation if all user's checkup then the server issues a challenge to the users. The users can validate the transactions or even choose to decline it if they find any mistakes. This is how the users are ensured that their coins would be mixed and send to them with a guarantee.

The overview of the entire process is shown in Fig 6. There are several users who take the Alice-Bob identity pair.

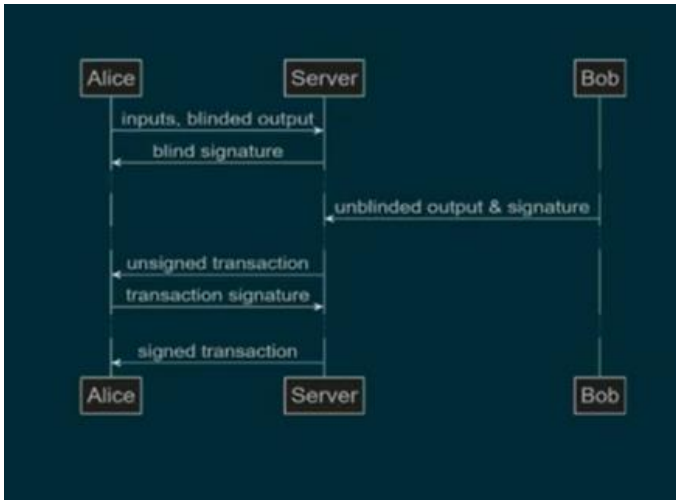


Fig.6 Denotes the overview of the protocol. There are multiple users who act as Alice and Bob.

The above process can be aborted if 1 user chooses to decline their transaction. This leaves the CoinJoin protocol vulnerable to DOS attacks. DOS attacks can occur either by a user denying signing on a valid joint transaction or they spend their input out from under the joint transaction before it completes. In Fig.6 we see that the process is repeated for every user and thus some users would have coins available to them before another user. So, they can create a conflicting transaction which would abort the session. Another DOS attack could be if a participating user is kept idle and doesn't sign off. The solution would be to leave the bad parties and try again.

IV. Wasabi Wallet

The most popular CoinJoin mixing service is the Wasabi Wallet. It is a non-custodial wallet and a decentralized mixing service in which the users private key is only stored on their side and so no third party can freeze or lose their funds. Wasabi Wallet is compatible only with the TOR network for transmitting data. It was introduced in November 2018 and as of November 2019 it doesn't seem to have any of the typical vulnerabilities which Coin Join protocols face. As far as speed compared to centralized mixers it is not very fast, but users can keep their coins for mixing and not have to wait for a transaction. Wasabi wallet has a low fee of 0.003% per participant in the anonymity set. Typically, users have around 50 participants and in that case the fees would add up to 50*0.003 = 0.15% of the transaction which in comparison to centralized mixers who charge 2-3% per transaction is much less. This year, Wasabi wallet has exponentially been growing as seen from Fig.7

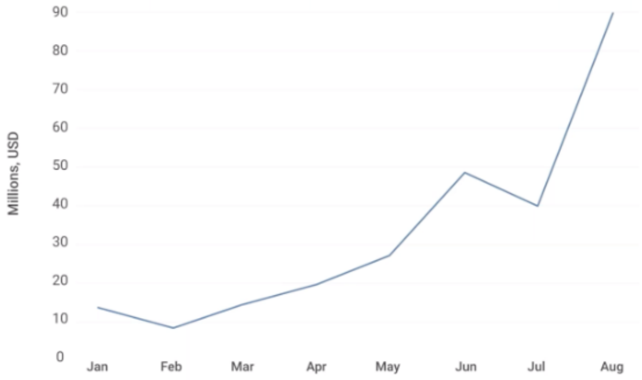


Fig 7. Shows the amount of money users have been depositing into Wasabi Wallet.

From January to August 2019 Wasabi Wallet had mixed coins worth $250 million. Wasabi Wallet makes use of SMPTC for which users must mix their coin locally and then it goes to the mixing server. Since a significant part of the mixing process takes place on the user's local machine Wasabi Wallet is called as a decentralized mixer. But technically it has a trustless centralized server.

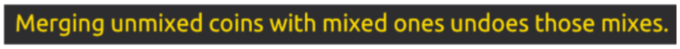
As a CoinJoin mixer Wasabi wallet should be mainly vulnerable to DOS attacks. The users could purposely choose to not sign off on a joint transaction, choose to remain idle, or create a conflicting transaction during the session. Wasabi Wallet handles these issues by implementing an automated process which puts users in new groups while retrying to pair users in session. The automated process likely aims to quarantine bad behaving users and has been ensuring the smooth mixing of real users. In this way the end user is not aware of any malicious users who may have been in the mix with them and it preserves the integrity of the mixer.

Now Wasabi wallet can mix 1.5Bitcoins on average per day for a user. This number varies a lot and is mainly dependent on the user behavior. In the best case, wherein, the users cooperate, and the transaction gets signed off without any of the above-mentioned interruptions Wasabi Wallet performs as fast as any other decentralized mixing service. Wasabi Wallet has options to set the anonymity set for each user. If the user is in a mixing session with 50 users and some users sign off but other don't then the CoinJoin will happen with the participating users and wait for other participating users. This way the users waiting on other peers get paired up quickly. The pairing up and signing is time bound for each user and the joint transaction would terminate for that session and a new session would begin with the members who signed off, searching for other users to join their group.

In my further investigation into the rise of popularity behind Wasabi Wallet I focused on the security measures recommended by Wasabi Wallet developers and tried to detect the potential vulnerabilities Wasabi Wallet might have.

Should not merge mixed and unmixed coins

Wasabi Wallet has told users that they should not merge mixed and unmixed coins because the unmixed coins leave a trail which could link the user with all the coins. This is a common advice decentralized mixing services give to their users. When users try to do this kind of mixing Wasabi gives an error message as shown in Fig.8



Merging unmixed coins with mixed ones undoes those mixes.

Fig.8 Shows an error message which users encounter when they try to merge unmixed coins with mixed ones.

Good labeling and not re-using addresses

Wasabi wallet has a feature of labeling for each set of coins a user receives. And so, in the wallet history users would make a note of the name and person who sends them coins. Now during the CoinJoin protocol it would not be possible for any other user or the decentralized mixing server to know which coins are getting mapped from specific users. However, after the coins have been mixed and the user labels the source of the coins and the user sending them the coin, it creates a record which if compromised would de-anonymize the user and their transactions from the wallet. Furthermore, these labels seem to be not encrypted by Wasabi Wallet and it is not clear how Wasabi Wallet would not have access to a user coin labelled history. So, a good practice for users would be to label their Wasabi Wallet transactions in code names which even if they were compromised would not reveal personal transaction information of the user.

Send coins in parallel to the cold storage

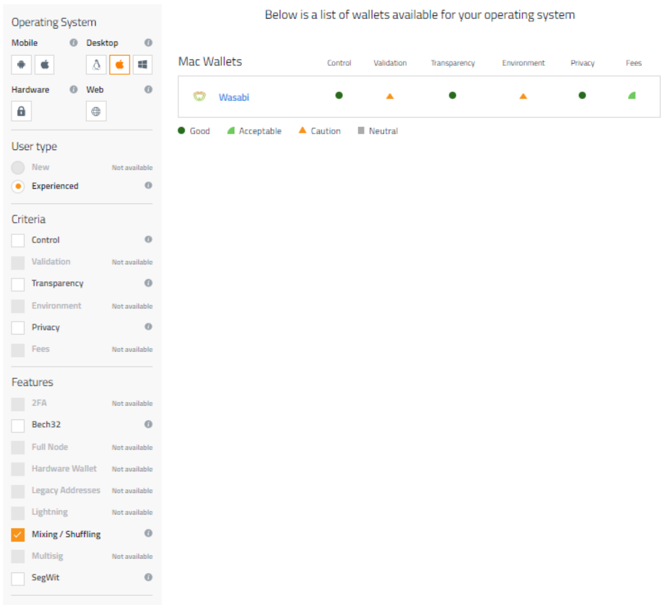
Cold storage refers to the storage of coins offline as opposed to a cloud-based wallet. They offer a better level of security since keys are stored offline and can also use offline hardware for authentication as opposed to exposing the keys on a network. It is advised that when sending mixed coins to the cold storage they must be sent in parallel and not to mix all of them in a single transaction. This is because when we assume that coins are going to be sent to a cold storage it is assumed that the wallet would store them for a long time and if all coins are mixed in a single transaction pointing towards the cold it becomes easier to link the coin trail.

Drawbacks

It is possible that the user who is mixing coins using Wasabi Wallet may have small amounts of un-mixed change from previous CoinJoins and is unable to meet the requirements to engage in a CoinJoin. Now in such a case if the user were to mix the un-mixed coins with the mixed coins then they would end up unmixing the mixed set of coins so they would have to keep it in their active wallet.

V. Future Trends For Decentralized Mixers

In the past centralized mixers dominated because it was easier and quicker to implement them. However, there seems to be a shift to decentralized mixers because they provided better anonymity, reliability and are cheaper. In the past, they have been slower than centralized mixers and this is because to achieve a high degree of anonymity there need to be a certain number of users willing to pitch in their coins to mix. Users were wary of this because of the risk of being exposed to other peers. In addition, decentralized mixers were not popular and so to get a set of participating users for a CoinJoin would take a long time. Wasabi Wallet has a strong user base who entrust them. On the official website of bitcoin(www.bitcoin.org), when one searches for wallets with a mixing/shuffling criteria selected, Wasabi Wallet is the only wallet giving results as shown in Fig.9



● Experienced

☑ Mixing / Shuffling

Below is a list of wallets available for your operating system

Mac Wallets	Control	Validation	Transparency	Environment	Privacy	Fees
Wasabi	●	▲	●	▲	●	◢

● Good ◢ Acceptable ▲ Caution ■ Neutral

Fig.9 Shows wallet search results on the official Bitcoin website for mixing/shuffling supported mixers.

In addition to having a mixing feature the official Bitcoin website also vouches for Wasabi wallets transparency (Source code is open source) and privacy (from server and peers by rotating addresses).

Before 2018, there was no such decentralized wallet officially endorsed by Bitcoin. This endorsement is a major factor in Wasabi Wallets rise in users and thus it can carry out CoinJoins quickly.

VI. Conclusion

Trust, privacy and transparency are the most sought-after services by users from Bitcoin mixers. Centralized mixers had a lot of problems and issues which is leading to their fall and rise in decentralized mixers. Wasabi wallet is the first decentralized mixer to be officially endorsed by Bitcoin. There are no major vulnerabilities found in Wasabi wallet and seeing the trends along with other factors it seems that Wasabi Wallet would continue to rise. The mixing is anonymous from other peers and the server, virtually leaving no trace. This has made the task for law enforcement agencies difficult to attribute users to transactions through the network. In addition, being a decentralized mixer law enforcement agency cannot easily take down the Wallet like a centralized mixer whose main operations are on a centralized server which makes it easier to attack and put a stop to all activities. Typically, Bitcoin mixers have been short-lived, but Wasabi Wallet is the first coin mixing service to be endorsed by Bitcoin with a high level of user trust and well implemented security features along with transparency regarding its functioning. Thus, it is likely that Wasabi Wallet will, and other decentralized mixers will continue to rise in popularity.

ACKNOWLEDGEMENT

I would like to express my gratitude towards Dr.Guan for guiding me and introducing me to Bitcoin mixers. This was a new topic for me, and it was something I really enjoyed learning and working upon. Initially, I had planned to carry out a simulation of the features implemented in Wasabi Wallet, specifically the Chaumian CoinJoin mixing over the Bitcoin protocol but I underestimated the complexity of such a simulation in terms of the time required and chose to continue working on my project by experimenting with the downloadable software.

REFERENCES

[1] van Wegberg, Rolf, Jan-Jaap Oerlemans, and Oskar van Deventer. "Bitcoin money laundering: mixed results?." *Journal of Financial Crime* (2018).

[2] Tran, Muoi, et al. "Obscuro: A bitcoin mixer using trusted execution environments." *Proceedings of the 34th Annual Computer Security Applications Conference*. ACM, 2018.

[3] de Balthasar, Thibault, and Julio Hernandez-Castro. "An analysis of bitcoin laundry services." *Nordic Conference on Secure IT Systems*. Springer, Cham, 2017.

[4] Ruffing, Tim, Pedro Moreno-Sanchez, and Aniket Kate. "P2P Mixing and Unlinkable Bitcoin Transactions." *NDSS*. 2017.

[5] https://cryptalker.com/best-bitcoin-tumbler/

[6] https://news.bitcoin.com/one-of-the-largest-bitcoin-mixing-services-closes-its-doors/

[7] https://www.buybitcoinworldwide.com/anonymity/

[8] https://link.springer.com/chapter/10.1007/978-3-319-11212-1_20

[9] Hamada, K., Kikuchi, R., Ikarashi, D., Chida, K., Takahashi, K.: Practically efficient multi-party sorting protocols from comparison sort algorithms. In: Kwon, T., Lee, M.-K., Kwon, D. (eds.) ICISC 2012. LNCS, vol. 7839, pp. 202–216. Springer, Heidelberg (2013)

[10] https://bitcoinmagazine.com/articles/chainalysis-most-mixed-bitcoin-not-used-for-illicit-purposes

[11] https://medium.com/datadriveninvestor/de-anonymizing-anonymous-crypto-services-a80258132e5b

[12] https://www.youtube.com/watch?v=yJFCRNCa6s0

[13] Joseph Bonneau, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A Kroll, and Edward W Felten. Mixcoin: Anonymity for bitcoin with accountable mixes. In International Conference on Financial Cryptography and Data Security, pages 486–504. Springer, 2014.

[14] Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate. Coinshuffle: Practical decentralized coin mixing for bitcoin. In European Symposium on Research in Computer Security, pages 345–364. Springer, 2014.

[15] http://web.eecs.umich.edu/~genkin/papers/privacy-cryptocurrencies.pdf

[14] Maurer, Felix Konstantin, Till Neudecker, and Martin Florian. "Anonymous CoinJoin transactions with arbitrary values." *2017 IEEE Trustcom/BigDataSE/ICESS*. IEEE, 2017.

[15] https://en.bitcoin.it/wiki/CoinJoin

[16]https://www.reddit.com/r/WasabiWallet/comments/avxbjy/combining_mixed_coins_privacy_megathread/

[17] https://bitcoin.org/en/choose-your-wallet?step=5&platform=windows