Limitations of Privacy Guarantees in Cryptocurrency

By
Wai Wu
wuwc@seas.upenn.edu

Advisor:
Brett Falk
fbrett@cis.upenn.edu

EAS 499 Senior Capstone Thesis

School of Engineering and Applied Science
University of Pennsylvania

April 25, 2018

TABLE OF CONTENTS

Abstract

Cryptocurrencies record all transactions in a distributed public ledger called blockchain, therefore exposing their entire history of transactions to the public. Bitcoin transactions, in particular, have been thoroughly studied, and shown to be vulnerable to deanonymization through both passive network analysis as well as side channel attacks. In recent years, there have been many coins emerging, claiming to provide anonymity guarantees that earlier protocols, such as Bitcoin, could not provide. In this paper, we present a comprehensive overview of efforts to improve anonymity guarantees over the past decade. The first section of this paper will clarify what anonymity means in the context of cryptocurrency and provide a broad sample of key ideas in guaranteeing anonymity. The second part of the paper will focus on how deanonymization of cryptocurrency works, specifically referencing case studies done on Bitcoin. The third part will discuss the details of new protocols currently being employed to defend against common deanonymization techniques, zooming in on recent empirical studies done on Zcash(ZEC) and Monero(XMR). Finally, the paper will end with a framework to evaluate how any new cryptocurrency claiming to be privacy-centric should be measured against current privacy coins, by using the case study of a new privacy-centric coin called Verge(XVG). Verge is just one example of many other coins emerging in recent years that claim to provide anonymity even though they may not have strong unlinkability guarantees. This paper therefore seeks to equip investors and users of “privacy coins” with sufficient theoretical understanding of how the various privacy protocols works, as well as the ability to seek out and understand empirical studies that determine if the coins mined so far have lived up to their claims to anonymity. Additionally, this paper makes the point that to provide better privacy, systems need to make privacy with good and easily-applied settings a default, rather than relying on users to understand the system well enough to use it correctly, because users will inevitably make mistakes in configuring their privacy settings that will compromise other users.

Introduction

There have been many types of online payment systems created over the past decades that have enabled transactions to take place more efficiently, without the need for physical cash. Examples include payment card networks like Visa and Mastercard, as well as eWallets such as Paypal. However, all of these systems are centrally administered by a controlling authority with the technical and legal ability to link these transactions back to the payer and the payee [1].

Since 2009, a new class of independent online monetary system known as cryptocurrency has emerged, allowing payers and payees to make transactions that are not subject to the control of a central authority [1]. Instead, these transactions are cryptographically-signed transfers of funds from payer to payee validated by other peers in a global payment network. Since validation is provided by peers in the network rather than a central authority, each of these transactions has to be recorded on a public ledger that every participant in the network of payment has access to, consequently exposing the entire transaction history of the system to the public [2].

To provide some form privacy for users in the system, first-generation cryptocurrencies like Bitcoin have designed their protocols to be pseudo-anonymous, where users use public key addresses to conduct their transactions rather than their actual real world identities. Pseudonymity results in transactions being recorded as transfers of funds between one public key belonging to the payer to another public key belonging to the payee, thus preventing an observer from immediately identifying the real world identity of the payer and payee [3].

However, pseudonymity only guarantees that a payer and payee cannot be identified by a network participant casually observing a single transaction. Theoretically, since the entire network of transactions can be exposed on a public blockchain, an external adversary can de-anonymize users by taking advantage of other information provided by the network of transactions. In fact, there has been substantial empirical research showing that re-identification of user identity is feasible in the Bitcoin network [1][3], leading to concerns that the pseudonymity provided by cryptocurrency does not lead to any kind of meaningful anonymity guarantee against an informed adversary.

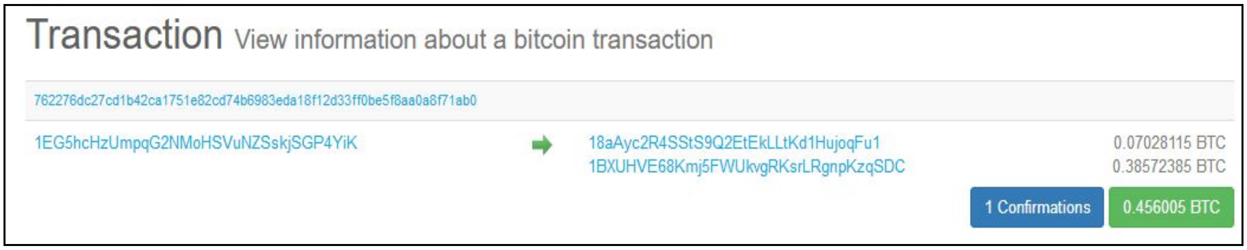
Computer scientists have realized that for anonymity guarantees to be meaningful, the cryptographic protocol would have to guarantee not just pseudonymity, but also unlinkability, where different interactions of the same user with the system should not be linkable to each other [4]. Unlinkability is difficult to achieve in practice, and even more difficult to guarantee formally. As a result, there have been many coins emerging in recent years that claim to provide anonymity even though they may not have strong unlinkability guarantees.

Investors and users of such “privacy coins” need to understand that there is never a guarantee of complete anonymity, and that the only meaningful measure of anonymity is to compare the amount of anonymity offered by each coin relative to one another. For such a comparison to be possible, they need to have a theoretical understanding of how the various privacy protocols work. Furthermore, investors should have the ability to seek out and understand empirical studies that determine if the coins mined so far have lived up to their claims to anonymity. Empirical studies conducted on both Zcash and Monero [31][34] have shown that while these privacy coins provide great tools to maintain anonymity, these tools might not be the defaults, resulting in improper usage by some people that compromised the coin. People who shield and immediately unshield in Zcash think they are getting some privacy, while people who participate in small mixins in Monero think they are getting sufficient privacy, but in both cases, they are actually vulnerable to anonymity attacks. The following sections will provide more background about the theory and practice of adding anonymity guarantees in cryptocurrency.

1. Overview of Anonymization

1.1 The Transaction Process

In order to understand what a meaningful anonymization of cryptocurrency transactions entails, we have to first understand how the transaction process is recorded on the blockchain. In the Bitcoin protocol, each transaction is recorded on the blockchain as a flow of a specified amount of Bitcoins between an input address and an output address. For example, in the diagram below, there is a transfer of 0.0703 BTC from sender address[1] to recipient address[2], as well as a transfer of 0.386 BTC from sender address to a second recipient address[3].



Transaction View information about a bitcoin transaction

762276dc27cd1b42ca1751e82cd74b6983eda18f12d33ff0be5f8aa0a8f71ab0

1EG5hcHzUmpqG2NMoHSVuNZSskjSGP4YiK → 18aAyc2R4SStS9Q2EtEkLLtKd1HujoqFu1 0.07028115 BTC
1BXUHVE68Kmj5FWUkvgRKsrLRgnpKzqSDC 0.38572385 BTC

Figure 1: Example transaction. Diagram taken from querying the Bitcoin Blockchain Explorer [5].

One key feature about a transaction is that it can have multiple inputs and multiple outputs. An input to a transaction is either the output of a previous transaction or a combination of newly-minted Bitcoins and a small transaction fee. As a result, a transaction can have multiple inputs from previous smaller transactions or the output of a previous large transaction can span across multiple inputs of smaller transactions. A transaction also often has two outputs, with one sending payment and the other returning change [3]. In Figure 1, the larger flow of 0.39 BTC to the second recipient address might be representing the payment, while the smaller flow of 0.070 BTC to the first recipient address might be representing the change returned to the payer.

1.2 Anonymity Definitions

Before we can say that a protocol guarantees anonymity, it is important to first understand what deanonymization means in the context of transactions. From a practical point of view, a successful deanonymization entails successful re-identification of the real world identities of the sender, the recipient and the amount being transacted. For example, since the transaction network is publicly accessible, a transaction can be de-anonymized if the identities of the owners of these public keys were voluntarily disclosed on online forums, because it would then be trivial for an adversary to link these public keys back to real world identities.

However, from a theoretical point of view, we take into account the amount of information the adversary already knows, and privacy is lost when the system has a weakness that can be exploited to give the adversary additional information that **increases** the probability that the adversary can correctly identify either the sender, the recipient or the amount of funds being transacted. For example, privacy is lost so long as the transaction can be linked back to a sender's address, or to a recipient's address, or to a specific amount, because each of these pieces of information can increase the probability that the real-world identities of the sender or recipient can be correctly identified.

[1] 1EG5cHzUmpqG2NMoHSVuNZSskjSGP4YiK
[2] 18aAyc2R4SStS9Q2EtEkLLtKd1HujoqFu1
[3] 1BXUHVE68Kmj5FWUkvgRKsrlRgnpKzqSDC

Since the theoretical view of privacy is so broad and ambiguous, researchers have come up with many definitions of privacy in the context of cryptocurrency, the most common being

anonymity = pseudonymity + unlinkability [4]

Pseudonymity is a basic feature already provided by the earliest iteration of Bitcoin. Pseudonymity is merely the feature of recording transactions as transfers of funds between one public key belonging to the payer to another public key belonging to the payee, rather than between the real world identities of the payer and the payee [4]. Pseudonymity therefore only breaks the link between a public key and a real world identity. From a practical point of view, if there is no absolutely no way of recreating this link between the public key and a real world identity, then pseudonymity is sufficient as a guarantee of anonymity. However, in practice, there are many ways to link public keys and real world identities. So, the second part of the definition, unlinkability, is also a crucial part of anonymity.

Unlinkability means that as a user interacts with the system repeatedly, these different interactions should not be able to be tied to each other from the point of view of some adversary. A transaction can be considered unlinkability if it is difficult to link different addresses or transactions of a receiver, difficult to link different addresses or transactions of a sender, and difficult to link the sender of a payment to its recipient. More formally, for any two outgoing transactions with receivers X and Y, it should be impossible or at least computationally infeasible, to prove they were sent to the same person (X = Y) [6]. Similarly, for any two incoming transactions with senders X and Y, it should be impossible or at least computationally infeasible, to prove they were sent by the same person (X = Y).

Unlinkability can also apply to a single transaction, which should not be traceable back to a specific sender or receiver. This type of unlinkability is also known as untraceability [10]. More formally, given a transaction input, the real output that is being redeemed should be anonymous amongst a set of other outputs. This is only possible if there are other decoy outputs mixed with the real output. Consider a hypothetical group of three people (Persons A, B, and C). If Person A wants to send money to Person B by transmitting a transaction message over the network, an observer should not be able to determine if Person A or Person B or Person C had sent it. In Bitcoin, the observer observes a message like “Person A wants to send 1 Bitcoin to Person B”, therefore ascertaining that Person A’s output is the real output being spent. On the other hand, if the observer sees a message like “One of the person in the three-people group of Person A, B, and C wants to send 1 Bitcoin to person B”, all senders would equiprobable and the unlinkability property is upheld from the sender’s perspective.

The problem with anonymity is that while pseudonymity is easily achieved, complete unlinkability is theoretically impossible to achieve, as the probability that a transaction can be linked back to its user is roughly $1 / |n|$, where n is the anonymity set, assuming that each of the spenders in the anonymity set is equally likely to have been the actual spender. As a result, anonymity is inevitably always “partial”, and there needs to be a way to quantify anonymity. One such way would be to use an anonymity set defined as a crowd that one attempts to “blend” into. To calculate such an anonymity set, one would have to first define the adversary model, and reason carefully about what the adversary knows, does not know and can never know [4]. What the adversary knows or does not know is highly context dependent and can only be meaningful tested through empirical studies, while what the adversary can never know can be reasoned by analyzing the theoretical underpinnings of each privacy protocol. Therefore, in each of the concepts introduced later, I will attempt to describe both the theory and empirical studies.

1.3 Overview of Anonymity Systems

Broadly speaking, unlinkability is achieved by mixing a transaction within an anonymity set (a group of other spenders acting as decoys), such that the probability that different transactions by the same user can be linked back to the actual user decreases as the group size increases. As a result, more recent versions of cryptocurrency have all incorporate some extent of mixing capabilities, either through mixing services, or protocol-level changes, thus claiming to provide stronger guarantees of privacy.

Mixing is the idea that anonymity of the sender and receivers can be ensured within an anonymity set of participants by permuting ownership of the coins so that an adversary can identify the pool that a transaction originated from but not the specific person by whom the transaction was created. Mixers can be anonymized service providers, or even done through a network of mixing services known as mixnets. There is a large amount of research regarding the security and accountability of mixers. Depending on who is doing the mixing and whether it is a trusted party, a user of a mixer could be susceptible to de-anonymization or even theft [7]. More recent implementations of mixing services have moved towards peer-to-peer systems, but in those cases, enforcing that mixing is done properly is not trivial and usually requires heavy-weight cryptography.

The concept of mixing can also be implemented at the protocol level, but that requires creating new types of cryptocurrency that are based on modified protocols. Two of such coins include Monero and Zcash. Monero [8] protects sender anonymity by creating groups of users and aggregating their transactions using ring signatures, so that each transaction can only be linked the group as a whole. Monero protects receiver anonymity by automatically generating one-time receiver addresses for each transaction (stealth addresses). Finally Monero shields transaction amount through Ring Confidential Transactions.

Zcash[9] essentially creates a shielded pool of money, where users can put money into the pool (minting transactions) and later spend the corresponding money out the pool (spending transactions). Adversaries can only see money going into the pool, and money coming out, but there is no way to link specific incoming transactions to outgoing ones. Zero Knowledge proofs are used to prevent users from spending more out of the pool than they put in.

Below is a summary table of different types of privacy-preserving services and protocols that will be considered in the paper, along with the type of anonymity guarantees they provide and the weaknesses they have. Note that these protocols are regularly updated to address known weaknesses, especially when rigorous empirical studies have been done to reveal new weaknesses [33].

TABLE I
SUMMARY TABLE OF VARIOUS PRIVACY PROTOCOLS, WITH THEIR PRIVACY GUARANTEES AND WEAKNESSES

Protocol	**Type of Anonymity**	**Main Weakness**
Bitcoin	Pseudonymous	Network Analysis
Single Mix Service	Pseudonymous Unlinkable	Side Channels
Mix Nets	Pseudonymous Unlinkable	Size of Anonymity Set
ZCoin/Zcash	Pseudonymous Unlinkable	Side Channels
Monero	Pseudonymous Unlinkable	Size of Anonymity Set

2. Deanonymization of Bitcoin Transactions

2.1 Network Analysis

The most direct way of deanonymizing Bitcoin transactions involves exploiting the weakness of the protocol itself through network analysis. Although the entire history of transactions is publicly available, an adversary still has to process the data in order to fully de-anonymize the transactions [1][3].

Firstly, public keys associated to a user has to be clustered together. As a user transacts within the system repeatedly, heuristics about common usage patterns can be used to cluster multiple public keys owned by a single entity into a single group. This allows the public key graph mapping public keys to transactions to be converted into a user graph mapping user entities to transactions. The flow of transactions from sender to recipient can then be easily traced. Finally, names can be mapped to user entities if the owners of the addresses have left proofs of their ownership on public domains, such as online marketplace and forums.

A) Clustering of Public Keys

One can analyze Bitcoin's overall transaction graph, with each address as a node and each transaction as a weighted, directed edge between nodes. Using the publicly available transaction history, a directed acyclic graph representing the transactions can be created, with the following specifications. Firstly, each node in the graph represents a transaction. Secondly, each directed edge contains a timestamp and value of bitcoins where an incoming edge represents the input to a transaction and the outgoing edge represents the output of a transaction. For example, Figure 2 shows the flow of 1.2 BTC from the output of transaction 1 to the input of transaction 3, on 01/05/2011.

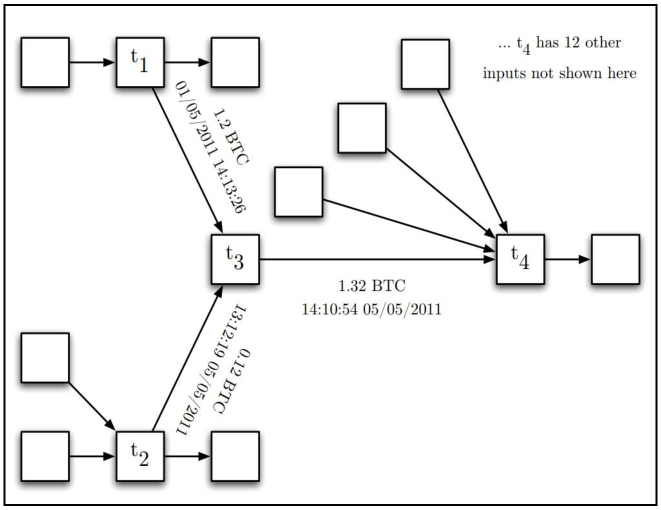


Figure 2: A transaction graph where each vertex represents a transaction and each directed edge represents the flow of Bitcoins from one transaction output to another transaction input. Diagram taken from [3].

Using the transaction DAG, an address graph could then be created on top of the transaction graph, representing the flow of Bitcoins between users, with the following specifications. Firstly, each node in the graph represents the public address of a user. Secondly, each directed edge represents an input-output pair of a transaction where the input's public-key (pk) belongs to sender and the output's public-key belongs to the receiver. For example, Figure 3 shows that the input of transaction 3 consists of 1 input to public-key 1 and 2 inputs to public-key 2.

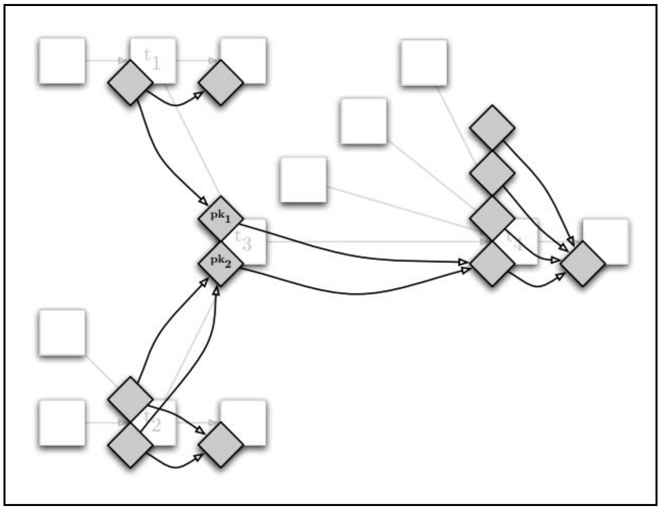


Figure 3: An address graph where each vertex represents the public address belonging to a user while each directed edge represents a pair of input public-key and output public-key. Diagram taken from [3].

With the address graph, it is then possible to use two types of heuristics [11] to cluster subsets of public keys belonging to the same user, such that a user graph representing the flow of bitcoins between users rather than public-key addresses could be created, as shown in Figure 4.

The first heuristic is termed “idioms of use” where it is assumed that all the inputs in a transaction are generated by the same user because different users rarely contribute to a single shared transaction in the real world [11]. This heuristic was already alluded to in the original Bitcoin whitepaper, where Nakamoto [2] stated that “Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner”. Using this heuristic, researchers [3] were then able to connect pairs of vertices where each pair corresponds to pairs of public keys used as inputs to the same transaction and are therefore associated to the same user, as a result creating connected components that each corresponded to a user, where each of the vertices in the connected component corresponded to a public key associated with the user.

The second heuristic utilizes the mechanism of “change address”, which is how the excess from the input address of a transaction is sent back to the sender [11]. In Bitcoin, the change address is created internally by the Bitcoin client and therefore never used again to receive payments from any other users. Therefore, for a transaction, if exactly one of its output had only one input, and if this output address was a completely new address that has never appeared elsewhere in the address graph, it could be deemed as a one-time change address that is linked to the input address. Both addresses can then be assumed to belong to the same user.

Using these heuristics, public keys can be successfully clustered to their respective users, as shown in Figure 4. Furthermore, because the entire blockchain transaction history is publicly available, one can then trace the flow of Bitcoins from user to user, such that each transaction can be unambiguously linked to a unique origin and a final recipient.

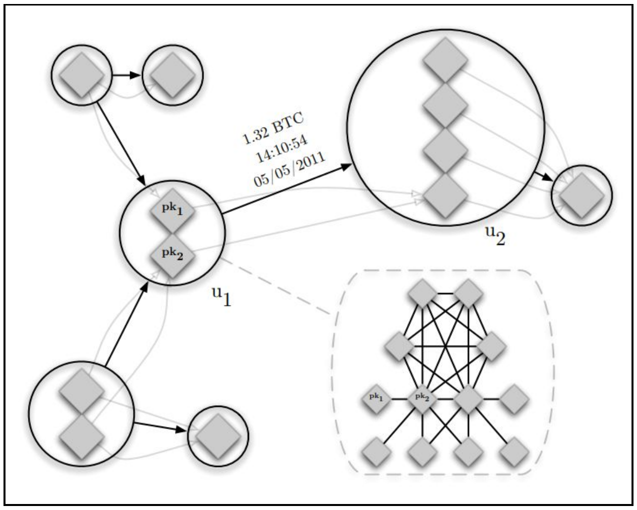


Figure 4: A user graph where each circular vertex represents a user while each directed edge represents the flow of Bitcoins from the sending user to the receiving user. Diagram taken from [3].

Figure 5 further illustrates how both the "idioms of use" heuristics and "change address" heuristics can be used. We see that transactions 2 and 3 both have the same input public-key address 5, so both transactions should have been initiated by the same user, and using the first heuristics, all the public key addresses that were inputs to transactions 2 and 3 (i.e. public-keys 3 through 7) have to belong to the same user. Furthermore, we see that public-key address 14 (an output of transaction 4) fits the second heuristics because the output address is completely new -- it has never appeared in the entire history of the Bitcoin blockchain and it will never be re-used on the blockchain to receive payments. We can deduce that this public key was created just once for the purpose of receiving change for transaction 4, and can therefore cluster it with the other public keys that were inputs of transaction 4 (public-keys 8 and 9).

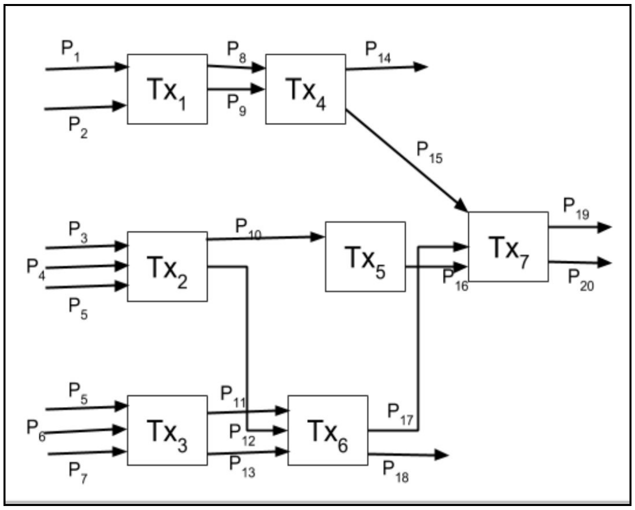


Figure 5: Example transaction graph where heuristics can be applied to cluster public keys belonging to the same user [12].

B) Re-Identification of User Identities

The next step of deanonymization is to match these public keys back to their real-world identities, by integrating off-network information. Although there is no user directory for the Bitcoin system, researchers have demonstrated that there are common ways of leaking information online that allow Bitcoin users to be associated to their known public-keys [1][3]:

1) Voluntary disclosure of information - Individuals sometimes publicly post a public key on a forum or website with corresponding Bitcoin address.

2) Trading bitcoins for fiat currency on an exchange - Since exchanges are subject to regulations, customers normally have to prove identity by uploading personal documents which can be subpoenaed by authorities eventually.

3) Purchasing items with Bitcoin - The merchant typically has to ship a product to a real world address, so a public key can be associated with a real home address.

Once the public keys are linked to real user identities, the deanonymization process is complete.

3. Improvements to the Bitcoin Protocol

There have been many efforts to improve the privacy guarantees of cryptocurrency ever since research showed that Bitcoin was vulnerable to passive blockchain analysis. Three broad categories of solutions have arisen, namely mixing protocols, mix nets, and alternative coins.

3.1 Mixing Protocols

A mixing protocol ensures anonymity of the sender and receivers within an anonymity set of participants by using a trusted mixing authority to permute ownership of the coins so that an adversary can identify the pool that a transaction originated from but not the specific person from whom the transaction was created. Mixers are anonymized service providers that divide transactions into smaller parts and mix them at random with other random parts of other transactions, so as to break the link between the user and coins transacted. These mixing protocols can also be peer-to-peer, so as to avoid the involvement of a third party, and prevent an adversary who has control over part of the network to deanonymize a transaction.

The most straightforward protocol for implementing peer-to-peer mixing is CoinJoin [13], where multiple transactions are merged by a centralized, trusted mixer, such that the inputs and outputs of the set of users are part of the same transaction, therefore ensuring that each specific output cannot be linked back to a specific input. CoinJoin therefore enables k users to atomically transfer funds from their k input addresses to their k output addresses in a random permutation. It is a general mixing solution for essentially any coin, and was instrumental in promoting the popularity of mixing services in cryptocurrency because it was the first known way of trustless mixing in Bitcoin transactions [52].

From Figure 6, we see that transactions by both Bob and Ted are joined into one transaction, with inputs and outputs unchanged. The set of users consisting of Bob and Ted has previously agreed, through their signatures, on their respective inputs and outputs. However because these inputs and outputs are merged into one transaction, no external adversary is able to figure out how to map the outputs to the correct inputs, and therefore, the transactions are unlinkable to their recipients and senders, from an external perspective.

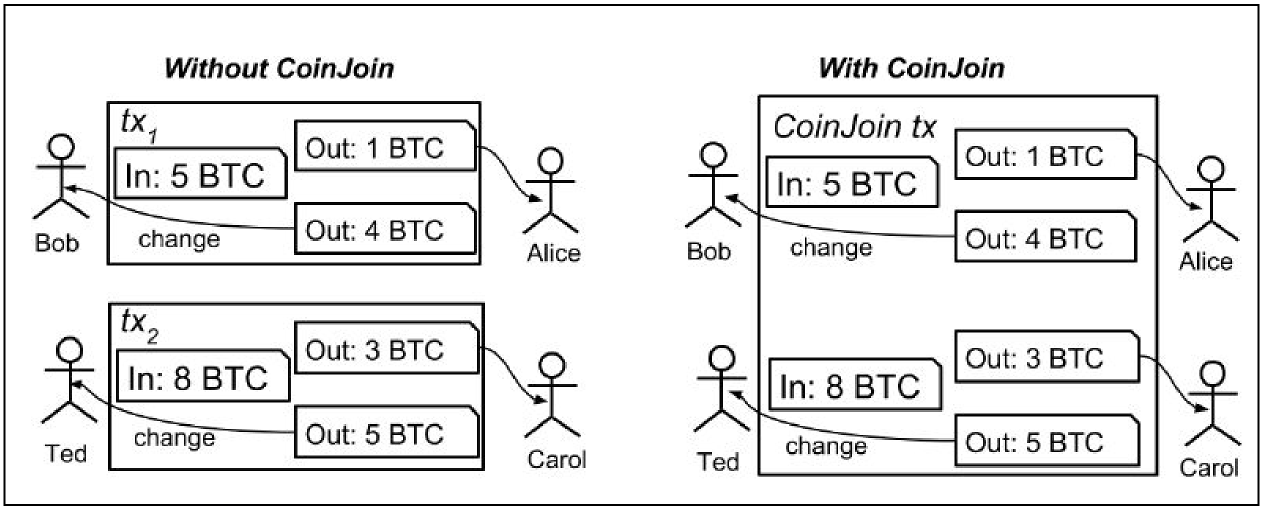


Figure 6: The schematic demonstrates the basic idea of CoinJoin by showing tx1 and tx2 joined into one transaction with CoinJoin, while leaving the inputs and outputs unchanged. Diagram taken from [12].

Although the transaction allows the participants to be mixed and therefore makes the transactions unlinkable, it is very complex to permute the output addresses without revealing the permutation to users within the mixing group. Alternately, a trusted facilitator can be used, but this leads to accountability issues, which will be discussed later. Regardless, CoinJoin is still an improvement over the Bitcoin protocol because it is resistant to network analysis. The "*idioms of use"* heuristic which relies on matching multi-input transactions to the same user, no longer works in this case, where multiple inputs of a single transaction originate from different users, and thus cannot be linked back to the same user.

Accountability Issues

One major issue is the necessity for each participant in the mixing set to sign the transaction and share their output addresses within the mixing set, allowing users within the mixing set to link the addresses back to the specific user. As a result, CoinJoin guarantees external unlinkability but not internal unlinkability, since the central mixing server learns the relation between input and output addresses and still needs to be trusted to ensure anonymity [12]. However, the issue of whether a mix can be trusted arises.

There are serious accountability issues when introducing mixes because once funds have been transferred to these mixing services, the mixes will send these funds to fresh addresses with no transaction history. It is possible that a malicious mix would send the funds to its own secret address instead of the requested address. Even if the intended recipient complains about the theft in order to undermine the mixes reputation, there is no definitive way that an outside auditor can determine who really owns the secret address. Since these theft allegations are difficult to prove, it is tough to determine which mixes are honest and therefore mixes may not have an incentive to be honest and refrain from theft [7].

Furthermore, since the mix learns that the same party owns both addresses, the anonymity of users depends on the mix keeping this pairing secret forever. A mix which is malicious, hacked, or subpoenaed might leak its records and undermine user anonymity. Furthermore, the mix could be badly designing its mixing service in a non-random manner, and thus inadvertently reveal the connection to observers [7].

To deal with accountability issues, two types of solutions have arisen. The first solution is to modify the protocols themselves through verifiable and reputable mixing.

Verifiable mixing [14] provides accountability by enforcing that all mixes issue a proof that their output is a permutation of their input. This is particularly important in cases where users cannot trace their own input through the mix.

In reputable mixing [15], each mix has to prove that each output corresponds to some input, as opposed to the mix itself originating the message. Mixcoin is a type of reputable mixing, where mixes issue signed warranties to users which roughly state: "if Bob sends me x coins by time t1, I will send x coins back to him by time t2." A user can then confidently send funds to the mix, knowing that if the mix misbehaves he or she can publish this warranty, damaging the mix's reputation and its business model. The Mixcoin protocol therefore adds accountability to the mixing process [7]. However, in all these solutions, even if mixes are honest, they remain a threat to user anonymity because they would know the internal mapping between users and outputs, therefore not guaranteeing internal unlinkability, as we have seen in the CoinJoin case.

The second solution is to therefore reduce relying on a trusted central mixing server altogether. One way of doing so is to cryptographically allow signing without having a central mixing server. Such improvements to the MixCoin protocol were implemented in BlindCoin, which extends the Mixcoin protocol by using blind signatures to conceal cryptographically the mapping between the user input and outputs, at the cost of requiring two extra transactions, where the sender has to publish the blinded token and the receiver has to redeem the blinded tokens [16].

Another way of not relying on a trusted central mixing server is to instead rely on a decentralized mix. Further improvements to the CoinJoin protocol were therefore implemented in CoinShuffle [17], which coordinates CoinJoin transactions using a cryptographic decentralized protocol that allows users to mix their coins with those of other interested users. The protocol is inspired from the anonymous group communication protocol Dissent to ensure anonymity and is similar to decryption mix networks (which will be described later). With this decentralized mixing technique, there is no reliance on a third party that can be compromised, therefore also guaranteeing internal unlinkability.

MIxing services can therefore reliably provide mix indistinguishably, where the anonymity set is the set of all users interacting with any mix at the same time, so passive adversaries cannot determine which mix a user is interacting with, and therefore cannot do network analysis.

Privacy Threats through Side Channels

Since mixes are able break the links between transactions inputs/outputs and public keys, de-anonymization is no longer possible through network analysis. Even if the protocol itself is not vulnerable to privacy attacks, there may be other privacy attacks that are possible through information leaked by side channels, such as timing, precise values and IP address information [18].

Timing information can be exploited through an Intersection Attack. Each mixed chunk have an implicit timestamp of the last mixed they were mixed. So if Alice immediately mixes *n* equal quantities of income on *n* specific dates and later uses a random subset to make a payment, the adversary can still trace the payment back to Alice if it contains a mix of chunks from these *n* times and only Alice was mixing at each of these times [19].

Precise payment sizes are exploited through Packet Counting Attacks. If Alice is observed receiving and mixing a very specific amount of Bitcoins at her known address, and a day later, the observer sees that an equal quantity of mixed chunks are combined for a payment, the observer can infer that Alice made the payment [3].

IP Address information can be exploited in a Network Layer attack. An adversary can use the Bitcoin P2P network to link a Bitcoin pseudonym to an IP address, because a node in the network can leak its IP address while broadcasting a transaction. Studies have shown that an adversary could connect in the network and by observing the transaction traffic, link users' public keys to their IP addresses with up to 30% accuracy [20].

Mixes have developed ways of defending against side channel attacks, especially intersection attacks that exploit timing information. In order to destroy timing information, Alice should make payments only by using chunks that were mixed contemporaneously. This works if payments are small enough. Secondly, Alice should mix all of her chunks of funds again every time she receives income. By doing so, she would destroy the timing information, but that is very expensive [7].

Both precise payment sizes and timing information can also be destroyed if Alice has advance notice before needing to make a payment. She can employ input/output mixing, where she mixes her funds as soon as she receives income [7]. Then, when Alice needs to make an actual payment, she can mix a set of already mixed chunks that add up to the final amount she owes. She can then pay out this amount of mixed chunks at different times, at the cost of introducing a delay in payment equivalent to the total mixing time (this is also why Alice must pay in advance of the deadline).

3.2 Mix Nets

While mixing protocols require a trusted mixer and therefore run into accountability issues as explained in the earlier sections, mix networks do not rely on any particular mixer, and therefore avoid liability issues caused by malicious mixers. Mix networks were in fact first introduced by Chaum [21] in 1981 for anonymous communication, but have since been adapted to a variety of use cases, including Bitcoin.

These mix networks work by chaining multiple mixes together, that take in and shuffles messages from a group of senders, and sends these messages out in a random sequence to the next mix node, until the messages eventually reach their final destinations [22][23]. The messages have a layer of public key cryptography that is specific and unique to each mix node, so every time it gets to the next mid node, a layer of encryption will be removed by that mix node to determine where to send the message to next, as can be seen in Figure 7. Because each mix only knows either the node that immediately preceded it or the node that it passed the message on to, this makes the network resistant to malicious individual nodes [21]. In the worst case scenario where all but one of the mix nodes are hacked into by a determined adversary, unlinkability can still be maintained.

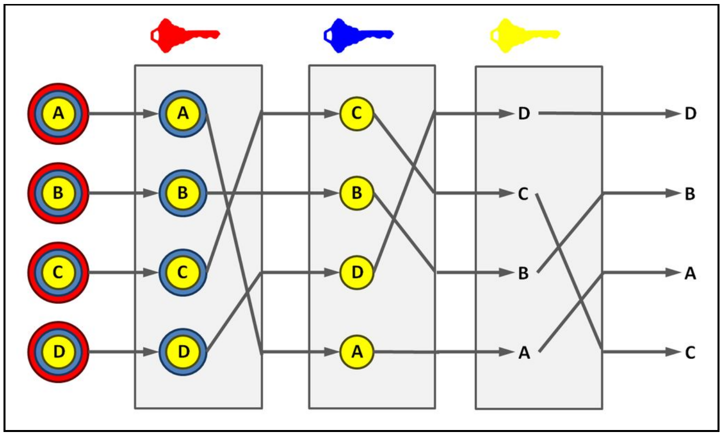


Figure 7: Mechanism for Mixnets. Diagram taken from [24]

The main weakness of mix nets lies in the size of its anonymity set [51], where the level of anonymity is dependent on the how well the anonymity set is sampled and how large it is. If the anonymity set consists of just one mix, the mix net would be equivalent to a normal mixing service, and subject to the same weaknesses. More ideas about anonymity set will be explored when Monero is discussed later.

3.3 Altcoins

The techniques we have seen so far are simply modifications to the Bitcoin protocol that seek to improve privacy guarantees. However, there are also alternative cryptocurrencies, called altcoins, that are either extensions to the Bitcoin protocol or new cryptocurrencies based on entirely different protocols. Several of these currencies were created for the explicit purpose of creating stronger privacy guarantees. In particular, they utilize specific cryptographic methods to remove information leakage to a trusted third party or an inner circle of people, so as to guarantee that internal unlinkability is also preserved, instead of merely external unlinkability. In this paper, we will analyze Zcash(ZEC) and Monero(XMR) in particular, as they have emerged as the popular privacy altcoins with highest market capitalization[4].

[4] Monero is 11th coin with $3,880,467,461 market cap, while Zcash is 26th with $986,859,667 market cap (as of 04/19/2018)

A) Zcash: Zero-knowledge Proof

Theoretical Background

Zero-knowledge proofs permit users to convert bitcoins to other types of cryptocurrencies and spend these new coins using anonymous proof of ownership instead of explicit public-key based digital signatures, thus effectively shielding the transaction history of a coin [30].

One of the earliest cryptocurrencies that utilized zero-knowledge proofs was Zerocoin, where making a transaction takes place in two stages -- a *mint* stage and a *spend* stage. In the minting stage, the user first puts an amount of Bitcoin into an escrow pool. Essentially, the user is destroying a Bitcoin in exchange for a random serial number that he or she is cryptographically committing to. In the spend stage, the user can then redeem that same amount of money out of the escrow account as an equivalent value of Zerocoin. At this stage, the user has to broadcast a Zero-Knowledge proof that he or she had escrowed more money than he or she is now withdrawing, so as to to ensure that money is not illegitimately minted, and will also broadcast the serial number of the coin so that it can be marked as used and not double-spent later on [26]. Since the proof is zero-knowledge, people seeing the proof can verify that the user has spent a legitimately minted coin, without knowing which of the minted coins the spent coin corresponds to. This means that all that someone can deduce from the mint and spent transactions of the Zerocoin is that the person who spent it must be one of the many people who did a Zerocoin mint, without really being able to pinpoint the exact person out of that large group of people [27]. Figure 8 compares a Zerocoin transaction to a normal Bitcoin transaction and shows how the spend trade and mint trade cannot be connected.

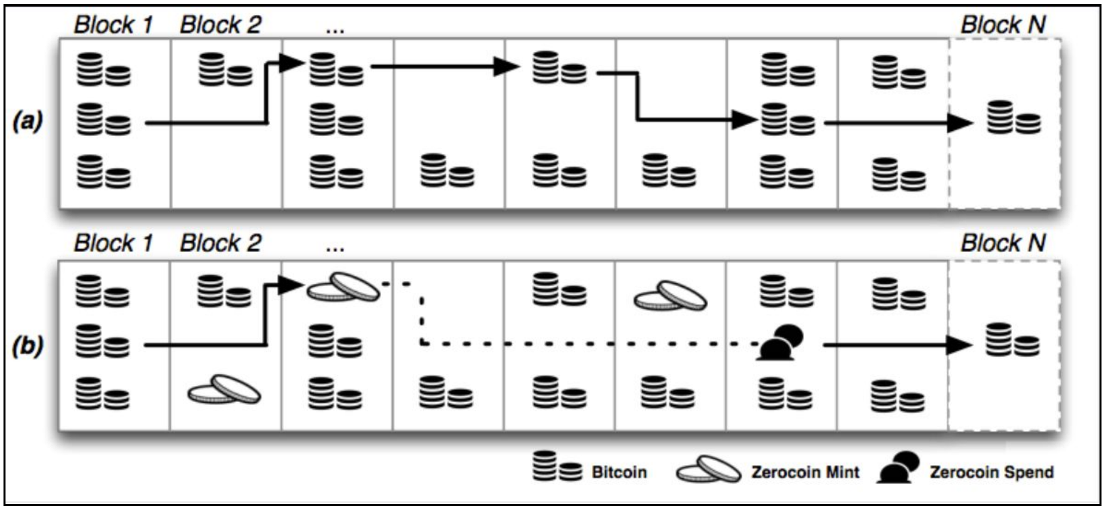


Figure 8: Comparison of Bitcoin transaction with Zerocoin transaction. In (a), Bitcoin can be traced through a series of transactions. However, in (b), a Bitcoin is traded for an untraceable Zerocoin (mint stage). Later, the Zerocoin is redeemed for another new Bitcoin (spend stage). The dotted line shows that the spend trade and the mint trade cannot be connected. Diagram is taken from [27].

More formally, as described in the Zerocoin paper [26], a mint transaction involves creating a coin commitment, $cm = COMM_r(SN)$, where SN = serial number of the coin and r = random trapdoor. Then the mint transaction containing the coin commitment, *cm*, is appended to the public ledger. In the second stage, the spend transaction, the spender has to provide the serial number of the coin (SN), as well as a proof π, of the statement "I know the random trapdoor *r,* such that $COMM_r(SN)$ appears in the list of all coin commitments that have already been appended to the ledger". In this way, the protocol reveals the serial number of the coin but not the random trapdoor *r*, so anyone can verify that the spend transaction is valid, but no external adversary can determine which commitments in the coin commitment ledger corresponds to the spend transaction, because that requires inverting $f(x) = COMM_r(SN)$, which is mathematically very difficult. Therefore, the external adversary cannot link the spent coin back to the minted coin.

Since there is no way to link incoming mint transactions to outgoing spend transactions (other than by heuristics), Zerocoin is able to uphold the external unlinkability guarantee. Furthermore, instead of exposing information to a fallible third party (as was the case in the mixing protocols discussed earlier), the user merely produces a zero-knowledge proof that he or she has escrowed a bitcoin and therefore is legal in spending an equivalent value of Zerocoin. In this way, users on the network can verify transactions without ever knowing the real spender's identity, and therefore preserve the internal unlinkability that could not be attained in mixing services. An extension of Zerocoin, called Zcash (ZEC), uses an improved version of zero-knowledge proof, called zk-SNARKs, that additionally hides the value of transactions and the receiver's address [28][29], providing additional anonymity guarantees.

Empirical analysis of the traceability of Zcash

A study [31] was conducted exploiting the weakness of non-shielded transaction amounts, where a certain amount of Zcash was moved from a transparent address (public visible) into a shielded address (not publicly visible on the blockchain), after which the same amount was moved out into another transparent address. An observer can deduce that the amount of money sent from the first transparent address must have been sent to the second transparent address, therefore allowing the final recipient to be traced back to the original sender.

The study found that 31.9% of coins being shielded conformed to this pattern and out of these traceable coins, 84.64% of them were from newly-mined coins, implying that mining pools were shielding these coins only because they were forced to do so by the Zcash protocol, with the intention of eventually sending these coins to miners through transparent addresses. The remainder were possibly from users who did not understand that shielding and then deshielding Zcash does not provide strong privacy [31].

In response to this empirical study, Zcash development team acknowledged the need to educate users that storing money in shielded addresses and then sending portions of them out as needed gives much stronger privacy than immediately moving out the same amount of money [53].

B) Monero: CryptoNote Protocol

Theoretical Background

Monero (XMR) is a privacy coin based on the CryptoNote protocol [6]. The CryptoNote protocol was designed to allow users to obscure their transactions by including "mixins" along with the actual coins they spend. It seems similar to the mixing protocols discussed earlier, however one important distinction is the autonomy where the sender is not required to cooperate with other users or a trusted third party to make his or her transactions, instead relying on a cryptographic primitive called a *group signature*, that allows a user to sign his or her message on behalf of the group without interacting with the other members of the group. Therefore, Monero avoids the problem of bad mixes or peers that commonly plague other types of cryptocurrency [6][32].

Monero is also resistant to blockchain analysis because it provides privacy guarantees over various parts of the transaction process. Here is a table summarizing how the features provided by Monero provides protection over each part of the transaction process.

TABLE II

FEATURES OF MONERO

Ring Confidential Transactions	Shields transaction amount
Ring Signature	Prevents transaction from being linked to the sender.
Stealth Addresses	Prevents transaction from being linked to the receiver.

Ring Confidential Transactions anonymize the transaction amount, by applying a mathematical function to all funds so that a public observer can see that the transactions are legitimate but not know how much the actual amount was, thus preventing attacks reliant on transaction amounts [6][32]. For example, Ring Confidential Transactions can protect against blockchain analysis using the "change address" heuristic and side channel techniques based on Packet Counting Attack discussed earlier.

Ring Signatures include both the real sender's public key as well as several other users public keys as a possible source of the funds being sent. More concretely, a ring signature is done over N public keys, and one private key matching one of the N public keys. The public keys are selected from all the outputs on the blockchain that have the same amount as the output being spent. Ring signatures can therefore prove that one out of n people signed a transaction without revealing which one of the n. A verifier will therefore be able to be convinced that the real signer is a member of the group but cannot exclusively identify the signer. As a result, ring signatures anonymize the sender's address and guarantees that a transaction cannot be traced back to an individual sender with certainty [6][32].

Note that over the course of k steps the possible transaction history might be in any of O(n^k) states. Typically $n=5$, thus providing a large anonymity set [33]. Some limitations exists, for example, anything lower than typical ring size of 5 is weak since not all ring members are equal given that transaction fees, ring sizes, payment IDs, in/out counts are all metadata that can be leaked and used to distinguish members within the ring.

Stealth Addresses compose of two public keys owned by the recipient, which the sender will use to produce new one-time bitcoin addresses to send the coins to. Even though these new addresses are generated by the sender and unknown to the recipient until the transaction is made, it will be controlled by the recipient because only the recipient has the private keys needed to reconstruct the public key.

In a hypothetical transaction where Alice sends some coins to Bob, Bob will be able to recover the funds sent to a one-time public key P from the two pieces of information: r and his secret key. Without Bob's secret key, both r and the one-time public-key P look random and unconnected to Bob. As a result, each transaction cannot be linked to a receiver.

A step by step breakdown of the transaction process will highlight more technical points about stealth addresses, which is important to understand for a subsequent discussion on stealth address in Verge [6]:

1. Bob creates two pairs of private and public keys, **(*a,A*) and (*b,B*)**, where $A = aG$ and $B = bG$. Bob makes the pair of public keys (A,B) available on the network as his stealth address, while keeping the pair of private keys (a, b) private.

2. Alice wishes to send 1 coin to Bob. To do so, she has to assign 1 bitcoin to a public key P such that Bob knows x and $P = xG$[5]. She will construct $P = H(rA)G + B$ where: (A,B) is Bob's stealth address, H is a hashing function, and r is a random big number.

[5] G is a base point in the elliptic curve cryptographic scheme used by CryptoNote protocol

3. Alice sends the bitcoin to *P (*the destination key) and also packs *R = rG* into the transaction.

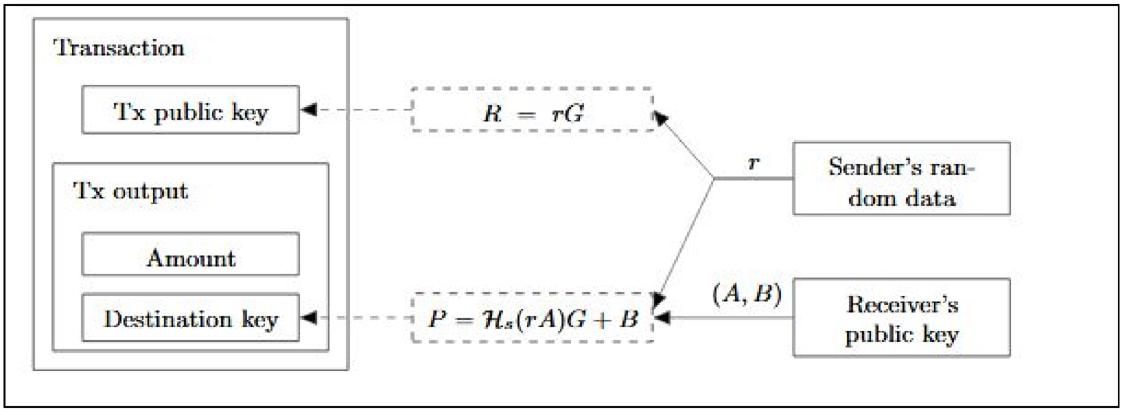


Figure 9: High-level schematic of the sender constructing the destination key *P. Diagram taken from [6].*

4. In order to ***recognize*** that the transaction is meant for him, Bob continuously listens on the network for all new transactions to scan for the one that belongs to him. For each transaction, he uses half of his pair of private keys *(a, b)* to compute a ***one-time public key*** *P' = H(aR)G + B* . If Alice transaction was meant for Bob, then *aR = arG = raG = rA,* therefore ***P' = H(rA)G + B = P****.*

5. In order to actually recover and ***spend*** the output, Bob has to **prove ownership** and will have to use his pair of private keys (*a, b)* to calculate a ***one-time private key*** *x := H(aR)+b*, such that *xG = (H(aR)+b)G = H(aR)G+bG = H(arG)G+bG = H(raG)G+bG = H(rA)G+B = P*. He can then use *x* to sign a transaction and spend the output.

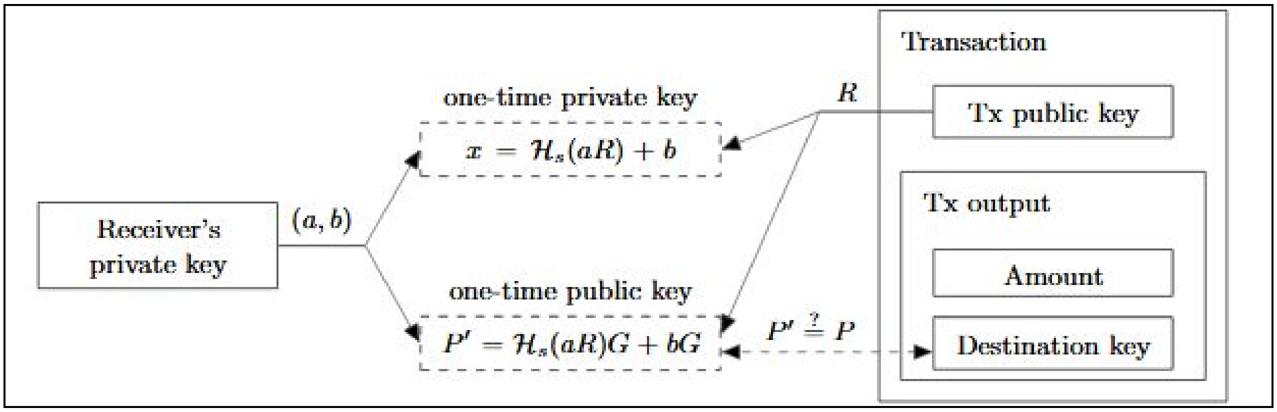


Figure 10: High-level schematic of the receiver constructing the one-time private key to spend the output. *Diagram taken from [6].*

Bob has proved ownership of the fund sent by reconstructing an *x* using his private keys (a, b), such that the public key *P* constructed by the sender is equivalent to *xG.* Because x is derived from a pair of unique private keys, neither Alice the sender, nor any other observer on the network has the ability to derive *x*, therefore only Bob uniquely owns the funds.

Stealth addresses thus allow a recipient to effectively prove ownership of a transaction's output without revealing that he or she is linked to the transaction. However, even though Bob (the recipient) cannot be linked to the transaction, it is still visible to any observer on the network that Alice (the sender) had made a transaction. So Monero implements the use of Ring Signatures, which will allow senders to include signatures from other members in a group, such that the sender can produce a proof that one of the members in the group did send a coin to Bob, but not let an adversary know who was the sender.

Empirical analysis of Monero

Recently, researchers empirically evaluated two weaknesses in Monero's mixin sampling strategy [34]. Firstly, they showed that 62% of transaction inputs with one or more mixins are vulnerable to "chain-reaction" analysis, because the real input could be deduced by elimination of inputs that are already spent by 0-mixin transactions [34]. Researchers used an iterative algorithm, where in each iteration, they mark all the mixin references that cannot be the real spend since they have already been deduced that the corresponding output has been spent in a different transaction. For example, from 0-mixin transactions, one could rule out the reference to transaction A. So in a 1-mixin transaction which references both transaction A and transaction B, one could also rule out transaction A as a real spend since the output of A was already spent in the 0-mixin transaction. Therefore, the output of transaction B is concluded to be actually spent as the input to the 1-mixin transaction. This process of elimination could then be continued with transactions with incrementally more mixins.

This chain reaction analysis exposed a weakness in the anonymity guarantees provided by the ring signature, which varies according to the size of the anonymity set. Remember that the ring signature merely guaranteed that Bob can hide every input among the other people in the anonymity set, and all possible spenders will be equiprobable. Therefore, if the sender specifies n other outputs and mixes them together with his or her own, the ambiguity degree would be n, resulting in a $1/(n + 1)$ probability that the spender has spent the output. For example, if the spender chooses an ambiguity degree of 1, his or her transaction output will be mixed with one other person's output, therefore there is a 50% chance that he or she has spent the output.

Since the size of the resulting signature increases linearly as $O(n + 1)$, the improved anonymity does add to the spender's transaction fees, resulting in users opting to choose smaller mixins even if that provides less anonymity guarantees. A user could even use 0-mixin transactions, where $n = 0$. Recent research showed that 64.04% of all Monero transaction outputs prior to February 2017 were indeed such 0-mixin transactions. Unfortunately, the Monero development team did not enforce non-zero mixins during its introduction in April 18, 2014, even though the author of the original CryptoNote white paper [6] did warn that that would result in the ring signature consisting of only one element, and therefore identify the spender as the real spender and defeat the purpose of Monero's privacy guarantees. The Monero development team only started enforcing a "2+ mixin" requirement from March 23, 2016. At that point, there was already a large amount of zero-mixin transactions, which were dangerous because they compromised the anonymity transactions that interacted with zero-mixin transactions, even if these other transactions had multiple mixins [34].

Apart from the weaknesses of anonymity sets containing 0-mixins, researchers also identified weaknesses in Monero's sampling strategy through temporal analysis. They showed that the actual spend-time distribution of Monero is highly right skewed, where users tend to spend coins soon after receiving them. However, the Monero client's sampling mechanism samples from a distribution that does not represent the real spending behavior, because it samples mixins to include by choosing randomly from a set of transaction outputs with the same denomination as the coin being spent. These researchers then showed that the real input is the "newest" input 92.33% of the time using a simulation, thus an external adversary could simply identify the real spend of the transaction by choosing the most recent transaction in the anonymity set, and be correct 92.33% of the time.

Both these weaknesses identified through empirical research have shown that an effective sampling strategy for the anonymity set is crucial to ensuring that the theoretical privacy guarantees that Monero claims to have will perform as expected in reality [34]. Since then, there have been other research studies conducting traceability analysis that showed similar weaknesses of Monero to ineffective sampling strategies [35]. While such weaknesses had been identified as potential privacy problems in earlier Monero Research Lab reports [36], the empirical studies were crucial in really showing how severely compromised Monero coins were. Monero Research Lab claims that the Ring Confidential Transactions enforced in 2017 now prevents the Monero coins from being compromised by the previously ineffective sampling strategy [37], but more empirical studies are needed to test that claim.

4. Comparison with Newer Privacy Coins

4.1 Overview of Privacy Coins Discussed

This paper ultimately seeks to provide a framework to examine how any new cryptocurrency claiming to be privacy-centric should be measured against current privacy coins. Most privacy coins are not inventing new ideas but rather combining and optimizing concepts already pioneered by the coins that were previously discussed. Therefore, Table III on the next page provides a summary of the discussion so far about various mixing protocols, mixnets and altcoins, so that any theoretical discussion of privacy coins can be grounded in a comparison with existing privacy coins.

TABLE III

SUMMARY OF MIXING PROTOCOLS AND PRIVACY ALTCOINS DISCUSSED SO FAR

General Category	**Privacy Strategy**	**Coin / Protocol**	**Level of Privacy Guaranteed**	**Problems / Limitations**
1) Mixing Protocols	Multiple inputs and outputs combined into single transaction through a trusted third party	CoinJoin	Unlinkability (External)	Internal Unlinkability not guaranteed Lack of accountability of mixes
	Rout funds through multiple addresses using a trusted third party, to add **accountability**.	MixCoin	Unlinkability(External)	Internal Unlinkability not guaranteed
	Same as Mixcoin, but using blind signature to address third party weakness	BlindCoin	Unlinkability (External and Internal)	Higher cost than MixCoin since there are two additional transactions
	Same as CoinJoin, but using decentralized protocol for mixing transactions	CoinShuffle	Unlinkability (External and Internal)	Unlinkability depends on size of anonymity set
2) Mix Nets	Mixing networks where funds are routed through multiple addresses to provide resistance to malicious individual nodes	Mix Nets	Unlinkability(External and Internal)	Unlinkability depends on size of anonymity set
3) AltCoin (Zero knowledge proofs)	Mint a new coin from a bitcoin in escrow, and use zero knowledge proofs to verify that a spend transaction with new coin is valid	Zerocoin / Zcash	Unlinkability (External and Internal) Untraceability	Empirical studies show that the anonymity set is small because of z-t-z transactions. Not all transactions are shielded Information leakage through timing and transaction amount
4) AltCoin (CryptoNote)	Combines ring signatures and stealth addressing	Monero v0	Unlinkability (External and Internal) Untraceability	Empirical studies show that prevalence of 0-mixins tx's compromise privacy of other tx that use these tx outputs in their mixins.
	Enforced 2-mixin min	Monero v0.9.0	Provides resistance against 0-mixins compromising unlinkability	Empirical studies show that mixins sampling are vulnerable to temporal analyses.
	Enforced Recent Zone sampling strategy	Monero v0.10.1	Provides resistance against temporal analysis of sampling	Theoretically, it still possible to link transactions back to real-world events by analyzing the amount of funds being transacted (Addressed with Ring Confidential Transactions)

4.2 Theoretical Comparison of Privacy Coins

This paper will use the case study of Verge to demonstrate how such a comparative analysis of privacy coins can be conducted. Based on the summary table above, it seems that Verge should be compared to other altcoins, since it claims to use an entirely new protocol called the “Wraith protocol” [38]. In particular, Verge seems the most similar to Monero, due to its use of *stealth addressing*. We therefore base our theoretical analysis of Verge using Monero as a benchmark against which we compare features.

To ensure anonymity, the Wraith protocol uses *stealth addressing*. This is similar to the stealth addressing in CryptoNote protocol used by Monero. Stealth addresses in Wraith protocol also use the Diffle-Hellman Exchange to allow two individuals who know each others’ public keys to calculate a shared secret that can only be decrypted by the recipient [38]. However, unlike the CryptoNote protocols that Monero is based on, the Wraith protocol lacks the use of Ring Signatures to obfuscate the sender. This means that while recipient unlinkability is guaranteed by stealth addressing (such that for any two outgoing transactions, it is not possible to prove that they were meant for the same person), sender unlinkability is not guaranteed and it is possible to prove that multiple transactions were sent by the same person. Stealth addresses, when used alone, is sufficient only for recipient unlinkability but not for sender unlinkability.

Furthermore, compared to Monero, Verge lacks Ring Confidential Transactions to obfuscate the amount of funds in the transaction. Since the amount being transacted is also visible, Verge is still vulnerable to side channel attacks like packet counting attacks. Although Verge claims to be resistant to other side channel attacks like network layer attacks because it hides IP addresses through the TOR network, one should note that TOR can be used by any other cryptocurrency [54] because it is merely a way to route a transaction through a network rather than a protocol level feature, and should not be treated as a feature inherent to Verge.

Thus, from a theoretical point of view, Verge seems to fare worse than Monero in its anonymity guarantees.

4.3 Empirical Comparison of Privacy Coins

However, privacy is not just about the property of the systems, but also how people are using the systems. The previous sections have revealed that even privacy coins with solid theoretical underpinnings are compromised by improper usage or configuration of privacy settings. 62% of Monero’s coins are actually traceable to their real spender or receiver while compared to 32% of Zcash coins [31][34]. None of these coins were 100% untraceable, contrary to their claims to be anonymous.

While we would not have been able to distinguish how effective Zcash is against Monero through a purely theoretical standpoint, we are now able to distinguish the effectiveness of these two coins so far since their conception through these empirical studies.

Default privacy in Zcash vs. Monero

The following is an example comparison of empirical studies done on Zcash and Monero, with arguments synthesized from online forums [39][40][41]. In both cases, the anonymity set has been compromised by privacy settings not being used the way they were originally intended.

In the case of Zcash, a large percentage of the coins are also traceable because users improperly moved a certain amount of money into a shielded address, and then moved that same amount out again almost immediately, thus allowing an external observer to figure out that those two transactions were essentially the same transaction. The proper way of shielding coins would be to move coins into a z-address and leave it there for quite a while as shielded, but many people skip the implicit step of waiting. Out of these pool of people, around 85% were shielding newly-mined coins, which the Zcash protocol requires to be shielded before they can be sent to transparent addresses. The fact that these coins were subsequently deshielded showed that the recipients opted to receive their mining payouts at a transparent address, implying that users did not want privacy in the first place but were only forced to shield and deshield because of the rules of the protocol. The problem is if people do not shield their coins properly, then the anonymity set of Zcash will be very small and ineffective. However, one has to bear in mind that people are choosing not to shield their coins properly because there is a large amount of time and resource required in computing their zero-knowledge proofs to allow shielding. Given that Zcash's next major upgrade, codenamed Sapling [42], will feature a set of groundbreaking performance improvements for their shielded transactions[6], a user of Zcash can look forward to the default changing from opt-in privacy to opt-out privacy in future, thus dealing away with unshielded transactions altogether in the future, and preventing such transactions from compromising the anonymity set in Zcash. One should therefore wait until Sapling goes live before being too critical of the Zcash ability to provide real privacy guarantees.

In the case of Monero, the anonymity set was compromised because many people actively chose to use a decoy set of 0, essentially making their transactions public and counter-effective as decoys, thus further compromising the privacy of other coins. Just as we have seen in Zcash, privacy was optional, and that was a deliberate design choice made because of the amount of time and resources that go into the extra steps to provide stronger privacy guarantees (computing zero-knowledge proofs for Zcash and creating larger mixins for Monero). Developers on both Zcash and Monero have stated that they would be actively looking for way to reduce the computation time required to build the anonymity sets, and therefore one can look forward to stronger privacy guarantees in the near future. This is good because it is reassuring when a privacy coin has a core research team that responds to weaknesses identified by studies conducted by researchers.

Evaluation of Verge (XVG)

Similar to Monero and Zcash, Verge is also making its privacy optional. However, unlike the two, Verge developers highlight optional privacy as a key selling point rather than a weakness, claiming that the "Wraith Protocol" would make it possible for a user to choose between a public ledger if they require transparency or a private ledger if they prefer complete anonymity [38]. The problem with optional privacy, as we have seen in Monero and Zcash, is that users tend to stick with the transparent default (0-mixin for Monero and t-z-t transactions for Zerocoin) and choose to toggle to private features only when they need the private features, thus creating a much smaller anonymity set. Furthermore, if majority of transactions are public, then the private ones stand out, and become even more obvious. Default privacy is therefore considered to be necessity in ensuring that the anonymity set is robust and provides meaningful anonymity guarantees. In the case of Verge, by not making privacy default, the optional privacy that underpins the Wraith protocol could end up compromising the size of the anonymity set and lead to more privacy issues in future. It is quite clear that privacy guarantees that Verge offers are not likely to be strong in practice, even if the theory behind the privacy guarantees had been sound, which we evaluated to be not the case in the previous section. Therefore, from both a theoretical and empirical perspective, Verge would not be considered a privacy-safe coin with good anonymity guarantees.

[6] Zcash blog states "Rough estimate indicates an 80% reduction of proving time, and a 98% reduction in memory usage which is a key requirement for opening up mobile support for Zcash shielded addresses."

5. Implications of Better Anonymity Guarantees

This section seeks to address why is privacy is so important in the first place and the stakeholders involved in anonymous cryptocurrency transactions.

5.1 Importance of Anonymity

From the consumer perspective, there are clear detrimental economic effects on the individual consumer when companies are able to obtain information about each consumer's transactions. The issue of privacy actually extends to everyone around the world, as long as they are using cryptocurrency for making payments. If all the transaction history of a user can be made available to the public, any observer would be able to deduce the income level of anybody, as well as the kind of payments anybody is receiving or sending. This allows more targeted advertising that could influence a consumer to buy a product that is more expensive and unnecessary than he or she might have originally bought without the influence of advertising. More information about an individual's income level can also enable companies to practice dynamic pricing, where a user might be charged more for the same product simply because the user is able to pay more than average. Consumer prices and choice will be implicated if transaction data is harvested from the blockchain by companies.

From an user perspective, it is catastrophic if millions of people mistakenly believe that cryptocurrency provides users complete anonymity and lose all the money they invest when these privacy claims turn out to be false. Furthermore, some users might compromise their safety by making sensitive transactions on the blockchain rather than more secure traditional payment networks (like Visa and Paypal), exposing them to risks of getting caught in engaging in activities that are better kept under the radar.

From a more philosophical point of view, the whole point of blockchain was to prevent too much power from falling into the hands of a central, controlling authority which might abuse that power or make mistakes that would compromise the safety of the data of many people. However, if blockchain itself is susceptible to privacy attacks and does not prove a safer alternative, then perhaps the world is better off sticking with the default practice of governments regulating large monopolies to make sure that they get better and more responsible with handling users' data. The issue of lack of responsibility and accountability of large technological monopolies over consumer data is especially important in this year, where there has been intense public scrutiny over big technology firms that have made fiascos in the way they have been handling their usage, storage and selling of data, for example, in the Facebook debacle with the improper use by Cambridge Analytica of Facebook data [55].

Last but probably most importantly, from a constitutional point of view, privacy is seen as our individual right to be free from unwarranted intrusion by the government. There has been recent constitutional debates about the changing expectation of privacy with the rise of new technologies that threaten to encroach on our right to privacy. For example, in *Carpenter v. United States (2017)*, the supreme court debated whether the government's acquisition of historical cell-site records violated the Fourth Amendment rights of the individual customer to whom the records pertain [47]. Similarly, we need to question if new technologies like the blockchain will facilitate increased surveillance of personal activity and violate our rights to privacy. Cryptographic technologies are the center of this debate, because they allow us to secure data on notoriously vulnerable networks that we routinely use in our daily lives. However, law enforcement agents are concerned that cryptographic technologies work too well and prevent investigators from extracting essential evidence, thus calling for encryption systems to incorporate special backdoor access features allowing government agents to decrypt data when needed to aid an investigation [46]. This happened because privacy coins have been found to be used by people engaging in illegal transactions who wish to be anonymous. For example, Bitcoin was used by many to purchase illegal drugs on an online black market known as Silk Road [48]. The next section will explore some of implications that privacy-centric cryptocurrencies have on law enforcement, as well as the counter-measures that law enforcement agencies have come up with in response.

5.2 Implications on Law Enforcement

In the previous sections, we explored how main and side channel attacks can potentially be resisted by some privacy coins, this leads to concerns that illegal activity can be effectively untraceable. Due to the rapid growth of cryptocurrencies and their ability to facilitate illegal transactions anonymously, governments are starting to take great interest in ways to break anonymity in cryptocurrency so that they can track down the illicit transactions.

Tracking down transactions that are presumably anonymous is possible, because as we have seen in previous sections, even the best privacy coins have not worked out perfectly in practice. There are still ways for law enforcement agencies to work with other agencies in extracting information about transactions that can help law enforcement agencies trace criminal activity.

Many companies have surfaced in recent years, offering to trace stolen or "tainted" coins, such as Chainanalyis, Coinfirm, and Ciphertrace. One technique they use is taint analysis, where they can either put a taint percentage to any coin that comes out of a mix that includes tainted coins, where the taint between the input addresses and output address is defined as the percentage of the balance of the output address that came from the input address. Commercial software conducting automated blockchain analysis such as BitIodine [43], and graphical tools for visual analysis of bitcoins flowing in a blockchain such as BitConeView [44] are now available through these companies. In general, these tracking companies provide a set of tools to analyze the blockchain to identify illicit activities and even help to identify the Bitcoin users in the process, although many do not reveal exactly what methods they use.

Law enforcement agencies also sometimes look for entities that process a large amount of transaction volume of a cryptocurrency, the best example being cryptocurrency exchanges, such as ShapeShift. ShapeShift [49] has been widely recognized by the cryptocurrency industry, market and community as the most efficient and private exchange to trade alternative cryptocurrencies or altcoins, because it does not require users to provide any personal information or financial data when trading digital currencies on its trading platform. As a result, it is estimated that 7-15% of transactions with Monero pass through Shapeshift [10]. However, ShapeShift has recently cooperated with law enforcement to trace the transactions of a ransomware team, giving law enforcement agencies exceptional access to all addresses associated with the WannaCry attackers [50]. Similarly, law enforcement agencies are looking for more ways to add backdoors to cryptocurrency exchanges for other privacy coins.

5.3 Law Enforcement vs. Privacy

Law enforcement agencies push for backdoors allowing exceptional access so that they can track down criminals, however privacy advocates complain that these backdoors violate the individual's right to be free from unwarranted intrusion by the government. While the privacy vs backdoor debate could be framed as a philosophical one, the reality is that cryptography and security are not just political issues, but also very difficult technical ones,

Security pundits argue that backdoors compromise the effectiveness of the privacy coins even for those not involved in illegal trade. In the case of ShapeShift, well-informed Monero users argue that there are huge implications of backdoors on the anonymity set of Monero. If a single entity like ShapeShift, runs a significant portion of the network by transaction volume, then with one hack, an attacker will be able to eliminate many fake decoys from other transaction rings, thus making the anonymity set of Monero much smaller.

Experts in the cryptocurrency space are also against the idea of backdoors. Professor Matt Blaze at the University of Pennsylvania has argued against backdoors are inherently bad ideas as they compromise security of systems. He wrote in an article that "there is overwhelming consensus in the technical community that even ostensibly "secure" backdoors put the systems into which they are incorporated at increased risk of outside attack and compromise" [45]. Studies have shown that there are three main weaknesses of backdoors [46]. Firstly, on a conceptual level, providing exceptional access to communication would contradict current best practices used such as forward secrecy, where decryption keys have to be deleted immediately after they are used. Secondly, having to design a backdoor in the system would significantly increase the complexity of the system, and complexity is widely agreed on to be the biggest enemy of security, since each additional feature can potentially interact with existing ones to create more vulnerabilities. Furthermore, these exceptional access features are typically used infrequently, so security testing would be more difficult. Finally, the best case scenario would be that a backdoor increases the “attack surface” of the system and creates a abundance of new opportunities for hackers to exploit hidden software bugs, or even non-technical ways to exploit the exceptional access to the backdoor, for example, by stealing credentials from key government personnel.

On top of the security risks, there are also jurisdiction issues to having backdoors. Building in exceptional access would be risky enough even if it was given to only one law enforcement agency in the entire world. However, if other governments around the world require exceptional access to the backdoors, that leads to questions of how an international exception access framework could be built, funded, and maintained. Furthermore, even if an international exception access framework were to be successfully built, many questions remain about whether other countries can be trusted to respect the rule of law when requesting for exceptional access.

Conclusion

Privacy is a very personal matter for many people, especially when it comes to privacy over transactions made. Most of us have been expectations of privacy that we trust established payment networks like Visa and Mastercard to uphold. As more and more people start to use cryptocurrency to make transactions, it also becomes increasingly important that people's expectation of the level of privacy they think cryptocurrency offers should match the actual level of privacy offered.

There has been a vast amount of research in improving privacy guarantees conducted over the past decade, resulting in the creation of numerous privacy protocols and privacy-centric altcoins, all of which are marketed to the average person as completely anonymous. As a result, many users of such “privacy coins” are not aware that they still have to take precautions to use these coins as they were intended to be use. This is problematic as empirical studies have shown that some of the most popular privacy coins have been compromised by improper usage. People who shield and immediately unshield in Zcash think they are getting some privacy, while people who participate in small mixins in Monero think they are getting sufficient privacy, but in both cases, they are vulnerable to anonymity attacks where their coins can be linked back to them. Furthermore, when these coins are compromised, they also compromise the anonymity set that they are mixed in, thus affecting the entire pool of coins.

As a result, privacy coins do not offer the level of privacy that people expect them to be offering. It is crucial that cryptocurrency developers address the failure of privacy measures in practice, by first understanding that the two biggest obstacles to users adopting best privacy practices are their high cost and complexity. In order for users to adopt best practices when using privacy coins, these best practices should be made affordable and easy to adopt.

On the cost side, bigger anonymity sets give more privacy guarantees but inevitably adds on to transaction costs. Fortunately, researchers are making great progress in improving the performance and costs of transactions, for example, in developing Sapling for Zcash. On the complexity side, some coins are designed such that the default setting is the no-privacy setting (0-mixins for the earlier pool of Monero coins) or require complicated transfers of money between accounts (Zcash). If users have to understand how privacy works in order to effectively use these privacy coins, they will inevitably use the coins wrongly. Instead, developers working on privacy protocols or privacy coins should make privacy make the default option, or at least make it easy for users to "toggle" their privacy settings.

Users should simultaneously educate themselves about what privacy really means and how to use privacy coins. There are three parts to the puzzle. Firstly, before even deciding to use cryptocurrency to make transactions, users should understand what anonymity means in the context of cryptocurrency transactions, and how deanonymization happens. These concepts are covered in Section 1 (Overview of Anonymization) and Section 2 (Deanonymization of Bitcoin Transactions). Secondly, when choosing which type of privacy coin to go for, users should think about what options are currently available, and can reference Section 3 (Improvements to the Bitcoin Protocol) and the comparison of coins in Table III. Users can also adopt the comparison framework described in Section 4 (Comparison with Newer Privacy Coins) to weigh their options.

Privacy is a fundamental individual right and we should actively protect our right to privacy. However, we should also be aware that increased privacy in cryptocurrency implies more difficulty for law enforcement agencies when tracking criminals. While we work work to improve privacy, we should be cognizant of its effects on security, and strive to find an an appropriate balance of privacy and security.

Works Cited

[1] S. Meiklejohn et al., “A Fistful of Bitcoins: Characterizing Payments Among Men with No Names,” in Proceedings of the 2013 Conference on Internet Measurement Conference, Barcelona, Spain, 2013, pp. 127–140.

[2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[3] F. Reid and M. Harrigan, “An Analysis of Anonymity in the Bitcoin System,” arXiv [physics.soc-ph], 22-Jul-2011.

[4] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, “Bitcoin and cryptocurrency technologies.” s Princeton University Press, 2016.

[5] “Bitcoin Block Explorer - Blockchain.” [Online]. Available: https://blockchain.info/. [Accessed: 24-Apr-2018].

[6] N. Van Saberhagen, “Cryptonote v 2. 0.” 2013.

[7] 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, 2014, pp. 486–504.

[8] “How does Monero’s privacy work?” [Online]. Available: https://www.monero.how/how-does-monero-privacy-work. [Accessed: 24-Apr-2018].

[9] “Zcash - Technology.” [Online]. Available: https://z.cash/technology/index.html. [Accessed: 24-Apr-2018].

[10] N. Asokan, P. A. Janson, M. Steiner, and M. Waidner, “The state of the art in electronic payment systems,” *Computer* , vol. 30, no. 9, pp. 28–35, 1997.

[11] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, “Evaluating User Privacy in Bitcoin,” in Financial Cryptography and Data Security, 2013, pp. 34–51.

[12] M. Conti, S. K. E, C. Lal, and S. Ruj, “A Survey on Security and Privacy Issues of Bitcoin,” arXiv [cs.CR], 03-Jun-2017.

[13] G. Maxwell, “CoinJoin: Bitcoin privacy for the real world,” in Post on Bitcoin forum, 2013.

[14] K. Sako and J. Kilian, “Receipt-Free Mix-Type Voting Scheme,” in Advances in Cryptology — EUROCRYPT ’95, 1995, pp. 393–403.

[15] P. Golle, “Reputable Mix Networks,” in Privacy Enhancing Technologies, 2005, pp. 51–62.

[16] L. Valenta and B. Rowan, “Blindcoin: Blinded, Accountable Mixes for Bitcoin,” in Financial Cryptography and Data Security, 2015, pp. 112–126.

[17] T. Ruffing, P. Moreno-Sanchez, and A. Kate, “CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin,” in Computer Security - ESORICS 2014, 2014, pp. 345–364.

[18] J.-F. Raymond, “Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems,” in Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability Berkeley, CA, USA, July 25–26, 2000 Proceedings, H. Federrath, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 10–29.

[19] R. L. Rivest, “Electronic lottery tickets as micropayments,” in Financial Cryptography, 1997, pp. 307–314.

[20] A. Biryukov, D. Khovratovich, and I. Pustogarov, “Deanonymisation of Clients in Bitcoin P2P Network,” in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, Arizona, USA, 2014, pp. 15–29.

[21] D. L. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,” Commun. ACM, vol. 24, no. 2, pp. 84–90, Feb. 1981.

[22] G. Danezis, “Mix-Networks with Restricted Routes,” in Privacy Enhancing Technologies, 2003, pp. 1–17.

[23] C. A. Ardagna, S. Jajodia, P. Samarati, and A. Stavrou, “Privacy Preservation over Untrusted Mobile Networks,” in Privacy in Location-Based Applications: Research Issues and Emerging Trends, C. Bettini, S. Jajodia, P. Samarati, and X. S. Wang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 84–105.

[24] N. Schottelius, ceof. Github.

[25] “Cryptocurrency Market Capitalizations | CoinMarketCap.” [Online]. Available: https://coinmarketcap.com/. [Accessed: 24-Apr-2018].

[26] I. Miers, C. Garman, M. Green, and A. D. Rubin, “Zerocoin: Anonymous distributed e-cash from bitcoin,” in Security and Privacy (SP), 2013 IEEE Symposium on, 2013, pp. 397–411.

[27] Eli Ben-Sasson, “Zerocoin Project.” [Online]. Available: http://zerocoin.org/. [Accessed: 24-Apr-2018].

[28] Eli Ben-Sasson, “Zcash - Technology.” [Online]. Available: https://z.cash/technology/index.html. [Accessed: 24-Apr-2018].

[29] E. B. Sasson et al., “Zerocash: Decentralized anonymous payments from bitcoin,” in Security and Privacy (SP), 2014 IEEE Symposium on, 2014, pp. 459–474.

[30] O. Goldreich and Y. Oren, “Definitions and properties of zero-knowledge proof systems,” J. Cryptology, vol. 7, no. 1, pp. 1–32, Dec. 1994.

[31] J. Quesnelle, “On the linkability of Zcash transactions,” arXiv [cs.CR], 04-Dec-2017.

[32] “How does Monero’s privacy work?” [Online]. Available: https://www.monero.how/how-does-monero-privacy-work. [Accessed: 24-Apr-2018].

[33] “Monero Is Less Untraceable Than It Seems | Hacker News.” [Online]. Available: https://news.ycombinator.com/item?id=16687008. [Accessed: 24-Apr-2018].

[34] M. Möser et al., “An Empirical Analysis of Traceability in the Monero Blockchain,” Proceedings on Privacy Enhancing Technologies, vol. 1, p. 21.

[35] A. Kumar, C. Fischer, S. Tople, and P. Saxena, “A traceability analysis of monero’s blockchain,” in European Symposium on Research in Computer Security, 2017, pp. 153–173.

[36] S. Noether and A. Mackenzie, “A note on chain reactions in traceability in cryptonote 2.0,” Research Bulletin MRL-0001. Monero Research Lab, 2014.

[37] S. Noether, A. Mackenzie, and T. M. R. Lab, “Ring Confidential Transactions,” Ledger, vol. 1, no. 0, pp. 1–18, Dec. 2016.

[38] CryptoRekt, Verge-Blackpaper. Github. Available: https://vergecurrency.com/static/blackpaper/Verge-Anonymity-Centric-CryptoCurrency.pdf. [Accessed: 24-Apr-2018]

[39] “What is the most private Monero or Zcash? - Quora.” [Online]. Available: https://www.quora.com/What-is-the-most-private-Monero-or-Zcash. [Accessed: 24-Apr-2018].

[40] “Zcash vs. Monero? • r/Monero,” reddit. [Online]. Available: https://www.reddit.com/r/Monero/comments/7u6s94/zcash_vs_monero/. [Accessed: 24-Apr-2018].

[41] “Why is Monero better than Zcash or any other privacy minded coin? • r/Monero,” reddit. [Online]. Available: https://www.reddit.com/r/Monero/comments/6gbsl1/why_is_monero_better_than_zcash_or_any_other/dip5its/. [Accessed: 24-Apr-2018].

[42] S. Bowe, “Cultivating Sapling: Faster zk-SNARKs – Zcash Blog,” Zcash Blog, 13-Sep-2017. [Online]. Available: https://blog.z.cash/cultivating-sapling-faster-zksnarks/. [Accessed: 24-Apr-2018].

[43] M. Spagnuolo, F. Maggi, and S. Zanero, “BitIodine: Extracting Intelligence from the Bitcoin Network,” in Financial Cryptography and Data Security, 2014, pp. 457–468.

[44] G. Di Battista, V. Di Donato, M. Patrignani, M. Pizzonia, V. Roselli, and R. Tamassia, “Bitconeview: visualization of flows in the bitcoin transaction graph,” in Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on, 2015, pp. 1–8.

[45] H. Abelson *et al.*, “Keys under doormats: mandating insecurity by requiring government access to all data and communications,” *J Cyber Secur*, vol. 1, no. 1, pp. 69–79, Sep. 2015.

[46] “Opinion,” *The Washington Post*, The Washington Post, 15-Dec-2015.

[47] O. Kerr and O. Kerr, “Opinion,” *The Washington Post*, The Washington Post, 05-Jun-2017.

[48] N. Christin, “Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace,” in *Proceedings of the 22Nd International Conference on World Wide Web*, Rio de Janeiro, Brazil, 2013, pp. 213–224.

[49] “ShapeShift | Cryptocurrency Exchange | Simple Coin Conversion.” [Online]. Available: https://shapeshift.io/#/coins. [Accessed: 24-Apr-2018].

[50] “ShapeShift is Assisting Police to Trace Cashed Out Bitcoin From WannaCry Ransomware,” *CCN*, 10-Aug-2017. [Online]. Available: https://www.ccn.com/shapeshift-is-assisting-police-to-trace-cashed-out-bitcoin-from-wannacry-ransomware/. [Accessed: 24-Apr-2018].

[51] K. Sampigethaya and R. Poovendran, “A survey on mix networks and their secure applications,” *Proc. IEEE*, vol. 94, no. 12, pp. 2142–2181, 2006.

[52] S. Meiklejohn and C. Orlandi, “Privacy-Enhancing Overlays in Bitcoin,” in *Financial Cryptography and Data Security*, 2015, pp. 127–141.

[53] Z. Wilcox and J. Gavigan, “New Empirical Research into Zcash Privacy – Zcash Blog,” *Zcash Blog*, 04-Dec-2017. [Online]. Available: https://blog.z.cash/new-research-on-shielded-ecosystem/. [Accessed: 25-Apr-2018].

[54] P. Koshy, D. Koshy, and P. McDaniel, “An Analysis of Anonymity in Bitcoin Using P2P Network Traffic,” in *Financial Cryptography and Data Security*, 2014, pp. 469–485.

[55] “Cambridge Analytica and Facebook: The Scandal and the Fallout So Far,” *The New York Times*, 04-Apr-2018.