A Survey of Anonymity of Cryptocurrencies

Niluka Amarasinghe
Queensland University of Technology
Brisbane, Australia
niluka.amarasinghe@qut.edu.au

Xavier Boyen
Queensland University of Technology
Brisbane, Australia
xb@boyen.org

Matthew McKague
Queensland University of Technology
Australia, Queensland
matthew.mckague@qut.edu.au

ABSTRACT

The concept of virtual currencies is an emerging, and perhaps unexpected development in the modern financial world. Bitcoin can be regarded as the first successful virtual currency, followed by many other implementations. Analogous to paper currencies, it is apparent that privacy and anonymity are two pivotal considerations that affect the adoption of virtual currencies by users. However, many studies have identified several problems associated with the privacy and anonymity of Bitcoin. Consequently, a large number of attempts have been made to address these issues, yet it has been proven that many such solutions do not provide an acceptable level of anonymity. This survey presents an account of the level of anonymity achieved through those and attempts to provide a comparative evaluation across different constructions.

CCS CONCEPTS

• **Security and privacy** → *Security protocols*; Pseudonymity, anonymity and untraceability.

KEYWORDS

Anonymity, Privacy, Bitcoin, Cryptocurrency

ACM Reference Format:
Niluka Amarasinghe, Xavier Boyen, and Matthew McKague. 2019. A Survey of Anonymity of Cryptocurrencies. In *Proceedings of the Australasian Computer Science Week Multiconference (ACSW '19), January 29–31, 2019, Sydney, NSW, Australia.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3290688.3290693

1 INTRODUCTION

Anonymity is a property that is paramount to any currency scheme. The simplest meaning of anonymity in this context implies that any entity cannot be distinguished from any other entity. It is important for every stakeholder in a currency scheme such as users, merchants, policy makers and governments. If a transaction can be traced back to its corresponding sender and recipient, such a scheme will lose credibility, as the nominal and actual worth of a coin will deviate based on the coin's history. The absence of an acceptable level of anonymity could cause various hindrances such as violating the privacy of users and merchants, and undesirable consequences of a non-fungible currency, such as the possibility of ostracising participants.

Bitcoin, being the first and most widely adopted true cryptocurrency, has drawn much attention in relation to its anonymity and privacy. As many studies have proven, Bitcoin does not provide an acceptable level of anonymity in its present framework. This has led to many improvements to the existing Bitcoin framework as well as other independent constructions. Although a large number of solutions have been proposed in this context, the level of anonymity achieved by those varies significantly from one another. Moreover, it has been proven that many such constructions are not yet able to provide an acceptable solution to the problem.

In this paper, we attempt to evaluate the level of anonymity achieved across several constructions of cryptocurrencies. Our main contributions include: (1) Identification of a set of suitable properties that can be used to model anonymity across different constructions; (2) A critical evaluation of cryptocurrencies, and their strengths and weaknesses with respect to anonymity; (3) Identification of gaps in the current literature in this context; and (4) Recommendations for future research.

A related study has been published recently by Khalilov et. al. [14], that presents an evaluation of the level of anonymity achieved by different cryptocurrency schemes, drawing comparisons based on their technical implementations. In contrast, our findings are grounded in a set of conceptual models, and presented from a theoretical perspective. Herein, we initiate a discussion on unified evaluation of anonymity across different constructions.

The remainder of this paper is organised as follows. In the background section, we present a high-level overview of the Bitcoin framework. We then propose a set of anonymity properties applicable to cryptocurrencies based on several theoretical models as presented by many studies in this context. In the next section, we discuss the implications of the present Bitcoin framework in relation to its anonymity. Thereafter, we analyse several solutions proposed to improve anonymity of Bitcoin and other cryptocurrencies, and present their strengths and weaknesses as evaluated in the literature. Subsequently, we summarise the findings of our survey, while highlighting the gaps identified during this process. Finally,

Xavier Boyen is a Future Fellow of the Australian Research Council supported under ARC grant number FT140101145.

ACSW '19, January 29–31, 2019, Sydney, NSW, Australia

ACM ISBN 978-1-4503-6603-8/19/01…$15.00
https://doi.org/10.1145/3290688.3290693

we conclude the paper by proposing recommendations for future research.

2 BACKGROUND

Advances in technology have transformed the way that financial transactions take place. The concept of decentralised virtual currencies or cryptocurrencies has become one of the emerging modes of fund transfers in the highly connected world today, mainly due to their inherent decentralised nature and convenience [14]. Moreover, if their full potential can be realised in practice, the use of virtual currencies could be more beneficial as an alternative to traditional currency schemes.

Virtual currency implementations rely on cryptographic methods to achieve features such as privacy, decentralisation and anonymity, which are essential for the anonymity of digital currencies. The privacy aspects of a cryptocurrency are analogous to paper currencies in the sense that an outsider cannot link a particular transaction to the individual users who are involved in the transaction. On the other hand, many virtual currencies eliminate the need for a central trusted party as opposed to the traditional system, which not only helps with privacy, but also improves soundness by reducing exposure to unilateral institutional policy decisions.

The emergence of blockchain technology has made a significant breakthrough in virtual currencies, providing a public ledger service to hold the information related to transactions in a transparent manner. Bitcoin can be regarded as the first cryptocurrency that has been widely accepted around the world and uses a public blockchain structure to store transaction data. Since the inception of Bitcoin, a number of other virtual currencies have emerged and many such currencies are constructed based on the Bitcoin framework and blockchain technology.

2.1 A Brief Overview of the Bitcoin Framework

Bitcoin is a decentralised cryptocurrency scheme, which was first proposed by Nakamoto [25]. It consists of a public ledger (blockchain), where the history of all Bitcoin transactions are stored, which helps prevent double spending of any given coin (spending the same coin twice). Due to the Bitcoin architecture, no central authority is required to manage the transactions and hence the system functions as a decentralised scheme. The Bitcoin blockchain is shared with participants in a Peer-to-Peer(P2P) network where they are connected with each other without a central server. This blockchain is constructed by the participants based on a Proof-of-Work (PoW) system. PoWs create an artificial competition between the otherwise unvetted and untrusted peer participants that purport to maintain and grow the blockchain. This competition comes with corresponding rewards, all based on computing power, and ensures the integrity of the blockchain, as long as a majority of the computing power in the system is in the hand of honest users [25].

In the Bitcoin system, users maintain Bitcoin Wallets which are identified by addresses instead of the real identities of the users. Bitcoin transactions take place between these wallets using cryptographic keys and signatures to ensure privacy. The PoW system allows verification of transactions by the participating nodes in the Bitcoin network and to create new blocks in the blockchain to store verified transactions. This process (also termed as mining) generates Bitcoins as rewards to participating nodes [3, 14, 34]. In this construction, the complete history of the transactions is transparent to the network participants, yet they are not related to specific identities, but addresses. Hence, Bitcoin is regarded as "pseudonymous" [7, 14].

3 ANONYMITY OF CRYPTOCURRENCIES

In the traditional banking system, banks act as intermediaries to transfer funds between their customers and they are bound by regulation, and only by regulation, to preserve the privacy of customer information. Therefore, it is a centralised environment where the users rely upon trusted third parties to process their transactions and to preserve the privacy of related information. If it is possible for an outsider to track the transaction history of users or merchants and link the same to real world identities, such information could be misused for various purposes such as analysing spending patterns of users, violating user privacy, tracking physical locations of users, gaining competitive advantage in businesses etc. [14]. Moreover, if cryptocurrency coins are associated with history, genuine transactions could also end up with undesirable consequences with linkage to illegal activities such as money laundering, which could 'taint' those coins and make them lose their value after the fact, even to an unsuspecting recipient. As such, it is important to preserve the anonymity of transaction data in any currency system.

In the context of virtual currencies, most implementations rely on a decentralised approach to eliminate the need for a central trusted third party. However, the public ledgers store all the transaction data and these are publicly available to anybody. Hence, the anonymity of virtual currency systems should be such that an outsider cannot link the transaction data to the participants involved in corresponding transactions.

3.1 Theory of Anonymity

The theory of anonymity in data communication has been discussed widely in academic literature and many theoretical frameworks exist in this context [2, 19, 41]. However, these models cannot directly be applied to virtual currencies. Hence, some researchers have come up with new constructions to model anonymity, specifically in cryptocurrencies. In the case of cryptocurrencies, many attributes have been considered to construct definitions and models to measure anonymity. We summarise below, a set of such attributes that have been widely referred to in the literature, and these properties can be used together to capture different aspects of anonymity.

- **Anonymity of an entity** is defined such that an outsider is not able to adequately identify that entity within a group of entities, which is known as the **anonymity set**

[31]. The larger the anonymity set is, the higher the level of anonymity becomes.

- **Unlinkability** of two or more entities means that an outsider cannot adequately identify whether these entities are related [31]. In other words, given any two transactions, it is not possible to conclude that both transactions were delivered to the same user [15].
- **Recipient anonymity** implies that it is impossible to link a given transaction to its corresponding recipient and for any given recipient, no transaction can be linked [31].
- **Untraceability** property is such that for each transaction, there is an equal probability for every possible sender in the system to be considered as a probable sender [42]. In other words, untraceability holds if any given incoming transaction cannot be traced back to its sender, which is the sender anonymity.
- **Fungibility** of a currency refers to the property that every currency unit in a currency system should be identical [3]. As such, no currency unit should be blacklisted based on its past history and this could be regarded as an important attribute of anonymity of cryptocurrencies.
- **Hidden Transaction Values** also play a vital role in ensuring anonymity. If the transaction values are visible, one can analyse the transaction flow patterns and eventually link the transactions to corresponding addresses. Khalilov et al. [14] claimed that such linking could be achieved through behavior-based clustering in the Bitcoin system. Behavior-based clustering involves grouping Bitcoin addresses with similar behavior patterns based on characteristics such as transaction values.
- **Metadata Unlinkability**, such as unlinkability of IP addresses to Bitcoin payment addresses, can be considered as another attribute in anonymity. If an outsider can link a transaction to corresponding IP addresses, it is possible to identify real world identities and geographical location information of related users, which could violate user privacy. Khalilov et al. [14] argued that many experimental studies have shown that real world data about Bitcoin users could be revealed in its current implementation.
- **Deniability** is also regarded as another factor affecting true anonymity. Deniability refers to the users' ability to deny that they have participated in a particular transaction or a transaction mixing instance [43, 45]. Ziegeldorf et al. [45] argued that early centralised mixing services did not satisfy the deniability requirements.

Furthermore, Androulaki et al. [2] presented an adversarial model to quantify the privacy in the Bitcoin framework in terms of unlinkability of activities and indistinguishability of user profiles. Based on these metrics on the actual Bitcoin network, it has been shown that addresses corresponding to Bitcoin transactions can be extracted from the information that is publicly available on the blockchain and hence Bitcoin does not satisfy the property of unlinkability.

In a separate study, Saberhagen [42] argued that a digital currency scheme possessing untraceability and unlinkability properties could be regarded as a fully anonymous virtual currency system and claimed that Bitcoin does not satisfy either of these properties.

The notion of k-anonymity proposed by Sweeney[41] has also been used in the literature to analyse the level of anonymity of cryptocurrencies. In a system of k users, for any given user in the system, if the actions of any of the remaining $k-1$ users cannot be differentiated from said user, then that user is regarded as k - anonymous [30]. k represents the size of the anonymity set and a larger k value corresponds to a higher level of anonymity.

Meiklejohn et al. [19] proposed a definition for anonymity with respect to taint analysis, in an attempt to formalise a theoretical framework in this context. Taint analysis of Bitcoin transactions refers to the analysis of the relationships among Bitcoin addresses based on the transaction history corresponding to those addresses [44]. This framework mainly focuses on overlays of Bitcoin and creates a formal definition for virtual currencies in terms of taint resistance. Taint resistance is a measure of the identifiability of the ownership of a Bitcoin by analysing its past transactions and hence is related to the properties of traceability and fungibility.

It is noteworthy that a majority of the above attributes have been referred to in isolation across a vast number of studies, yet with different interpretations. Hence, it is a complex task to model the anonymity of diverse cryptocurrency implementations in terms of a standardised theoretical framework.

3.2 Summary of Proposed Anonymity Properties

As it was evident from the literature, the level of anonymity achieved by each cryptocurrency construction has been evaluated against different attributes. As a result, one cannot draw a comparison across different implementations. As a solution to this discrepancy, we propose a set of parameters, which can be commonly used to assess every aspect of anonymity applicable to various cryptocurrency schemes and protocols, as summarised below.

(1) Unlinkability
(2) Recipient anonymity
(3) Untraceability - Sender anonymity
(4) Fungibility - Indistinguishability of coins
(5) Confidentiality - Hidden transaction values
(6) Unlinkability of Metadata
(7) Deniability - Ability to deny the participation in a transaction

In addition, the degree of anonymity could be characterised by the following parameters: (1) Size of the anonymity set; (2) Average transaction processing time; and (3) Transaction block size. These parameters, together with the metrics of anonymity properties could be used to derive the level of resistance attributed against de-anonymisation attacks, that could be used to benchmark the level of anonymity across all currency schemes.

In the following section, we discuss the anonymity considerations of Bitcoin and related enhancements and also of

other cryptocurrency schemes, with respect to the proposed set of anonymity properties, wherever applicable.

3.3 Anonymity of Bitcoin

The privacy of Bitcoin users and transaction data has been widely spoken about in both academia and in the industry, showing that Bitcoin transactions are not anonymous. It is claimed that Bitcoin transactions are pseudonymous rather than being anonymous since Bitcoin users are represented by public keys instead of their real identities [2, 11, 14, 19, 22, 34]. Many research studies have proved that Bitcoin transactions can ultimately be linked to real world identities and they are not anonymous as it was claimed at the outset [2, 11, 14, 22, 34]. Ober et al. [30] analysed the dynamics of the Bitcoin transaction graph and claimed that the usage of multiple public addresses concurrently could pose a threat to the anonymity of the Bitcoin system. In a separate study, Reid et al. [34] constructed two networks; a transaction network and a user network, based on the data extracted from public Bitcoin data and showed that it is possible to gather details about Bitcoin users including their behaviour patterns from publicly available data. Accordingly, it can be concluded that Bitcoin does not satisfy the properties of unlinkability, recipient anonymity or untraceability.

Meiklejohn et al. [19] also claimed that it is impossible to achieve unlinkability in the Bitcoin framework since two different Bitcoins can be easily distinguishable, which is also a violation of the property of fungibility. Hence, it is argued that anonymity can only be considered with respect to the ownership of Bitcoins rather than the coins themselves [3].

A recent study by Khalilov et al. [14] presented a comprehensive survey of similar literature in terms of five properties of anonymity of Bitcoin namely; *i*) discovering Bitcoin addresses, *ii*) discovering identities, *iii*) mapping Bitcoin addresses to IP addresses, *iv*) linking Bitcoin addresses and *v*) mapping Bitcoin addresses to geo-locations. The results of the study showed that the transaction flow can be traced and user identities can be linked to transactions by combining both network and off-network information thus the Bitcoin framework does not provide metadata unlinkability.

Conti et al. [7] conducted an exhaustive study on the security and privacy properties of Bitcoin and argued that the transparent nature of the Bitcoin transactions affects the fungibility of coins. The study also evaluated security and privacy properties of other cryptocurrency implementations and claimed that security and privacy measures need to be improved further in order to achieve their full potential.

Consequently, many solutions have been proposed to improve the anonymity of Bitcoin and cryptocurrencies in general, and some have resulted in live implementations. Some of the solutions are based on heavy cryptographic techniques whereas the others focus mainly on mixing coins or transactions [5]. On the other hand, some protocols have decentralised constructions while others are more centralised in their architecture. Moreover, some of these solutions have been implemented as improvements to the existing Bitcoin protocol whereas others have led to the emergence of new cryptocurrencies (Altcoins). We group these solutions under two main categories; Mixing and Cryptographic approaches, and discuss their strengths and weaknesses in the following section.

3.4 Mixing Protocols

The simplest solution for the anonymity problem is to mix coins or transactions of multiple users thereby making it difficult to establish a direct link between users and corresponding coins or transactions. Many early solutions were focused on using intermediary mixing services such as **BitLaundry**, **MixCoin** and **Bitcoin tumblers** to achieve anonymity [22]. They are not fully decentralised as the Bitcoin network and depend on centralised third parties to achieve the mixing, often by charging a fee. If the coins involved in a mix are of similar values, then it makes it harder to link the coins to respective users, thus it increases the degree of anonymity. In addition, the level of anonymity also increases with the number of users and transactions involved in the mix, which is the anonymity set. Hence, mixing solutions in general possess a slightly higher level of unlinkability, recipient anonymity and untraceability when compared to Bitcoin. However, users have to trust the central mixing party not to retain any trace of their coins and also to return their coins after mixing [16]. Dependency on a centralised system is also a negative aspect as it could lead to a single-point of failure. Decentralised mixing approaches have been proposed and implemented recently as improvements to Bitcoin as well as Altcoins, while addressing these issues [14].

MixCoin is a mixing protocol which is compatible with the existing Bitcoin architecture and provides an accountable mixing method. It assumes the availability of multiple mixes, each trusted by the sender through a signed warranty [5]. This warranty allows a sender to publish any misbehaviour of a mix and hence damage the reputation of the mix. For a given sender, the MixCoin protocol allows splitting of the funds into multiple blocks and mixing each block several times consecutively, based on parameters decided by the sender. However, it does not provide any assurance as to whether transaction data are being stored by the mixing service, which could lead to linking them back to the sender [16].

CoinJoin Protocol is one of the widely accepted implementations that has been proposed to overcome the anonymity issue of Bitcoin and has led to several other anonymous protocols. In the CoinJoin implementation, a client-side application forms a single transaction by combining multiple inputs and outputs from multiple users, which is signed by those users and then sent to the network [18, 44]. In this arrangement, there is no involvement of a third party and thus it eliminates the need to trust a third party which is a drawback in many mixing protocols. However, if the Bitcoin amounts are different, then it compromises the anonymity to some extent [18]. In addition, the availability of users who

are willing to combine their coins/transactions at a given time may also affect the achievable level of anonymity.

Dash is a cryptocurrency that has been built with a privacy-focus, and has been implemented based on the CoinJoin protocol. Dash uses a secondary network of full nodes on the Bitcoin network to mix transactions without using a centralised third party [8]. Known as the Dash Masternode Network, this network acts as a trust-less implementation to provide the required privacy in mixing. Dash uses a PrivateSend function which extends from the initial CoinJoin protocol and improves on decentralisation and denominations [8]. However, Dash still has some limitations such as requiring at least 3 participants to initiate a PrivateSend transaction and facilitating only common denominations. Further, it is still a centralised system to some extent due to its dependency on the Masternode network, and given enough time, transactions can be linked to respective users.

CoinShuffle is a Bitcoin mixing protocol that uses the Dissent (Dining-cryptographers Shuffled-Send Network) Protocol to achieve accountable group anonymity [37]. The Dissent protocol provides anonymous message transmission with shuffling that is consistent with the current Bitcoin framework and does not require a third party to do the mixing. In addition, it does not involve any mixing fees. However, when the number of participants is small, the linkability becomes higher. Selij [40] simulated CoinShuffle transactions on a test Bitcoin network and analysed the linkability of those transactions. According to the results of this study, those transactions were identifiable among other transactions. Further, it is proposed that anonymity can be improved by splitting the transactions into several smaller amounts.

CoinShuffle^{++} is a cryptocurrency based on P2P mixing that was proposed by Ruffing et al. to facilitate unlinkable transactions in the Bitcoin system [38]. It is built on CoinJoin and the DiceMix P2P mixing protocol and achieves faster transaction times compared to CoinShuffle. The DiceMix protocol allows the broadcast of messages sent by a group of users anonymously in a decentralised manner [38]. However, the protocol assumes the existence of at least two honest users within the group to achieve an acceptable level of anonymity.

Research of Maurer et al. [18] claimed that initial CoinJoin transactions having common denominations can be linked to pseudonyms and thus proposed a solution to improve the unlinkability of CoinJoin transactions. This study examined how knapsack mixing can be implemented to split outputs and how it could be combined with an input shuffling algorithm to reduce the linkability, while allowing different values of coins to be mixed together. Their evaluation results showed an increase in the difficulty in linking transactions in the new framework compared to the original CoinJoin transactions.

As it was evident from the literature, mixing protocols have several limitations with respect to the anonymity of cryptocurrencies as listed below.

- Centralised nature of the implementation
- The need to trust a third party mixing service not to store any record of transaction data and also to return the coins after mixing
- Restrictions on denominations
- Anonymity set is often limited to the number of participants involved in the mixing
- Longer transaction processing times due to mixing delays
- Requirement of a least number of honest participants in the mix to realise an acceptable level of anonymity

Despite the slight increase in the level of unlinkability etc., mixing solutions have not been able to achieve acceptable levels of fungibility, confidentiality or metadata unlinkability. Hence, they exhibit a low resistance to deanonymisation attacks. It is also important to note that deniability of these solutions has not been discussed much in the literature.

3.5 Cryptographic Solutions

As previously mentioned, mixing protocols have inherent limitations that degrade the achievable level of anonymity. In addition, the involvement of malicious mixes could also significantly affect the anonymity of transactions. Hence, research on anonymity has diverted towards cryptographic solutions and many practical implementations can be seen at present.

Zerocoin relies on cryptographic methods to achieve anonymity while eliminating most of the problems faced by mixing protocols. It is regarded as one of the first anonymous electronic cash systems [1, 20]. The Zerocoin system uses one-way accumulators for storing values and zero-knowledge proofs for spending coins while breaking the link between transactions [20, 22]. Using one-way accumulators, participants can combine a set of values to generate a single block of data with a constant size and prove that a specific data value exists in this block [20]. A zero-knowledge proof allows a user in a system to prove the existence of some specific information without revealing that information to other users in the system. The Zerocoin implementation improves the anonymity considerably in comparison with the mixing methods. However, it does not hide the transaction values and uses only fixed coin values [1, 39]. In addition, the size of transactions increases due to the cryptographic content that needs to be stored, and therefore transaction processing takes longer than mixing protocols. Further, it requires modifications to the existing Bitcoin architecture to be able to realise its practical implementation [20].

ZeroCash provides improvements to the original Zerocoin e-cash system with enhanced assurance of anonymity. This system uses zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs) for verification of transactions and Decentralised Anonymous Payment (DAP) schemes, which enables users to pay directly to each other privately [39]. Using zk-SNARKs, not only one can prove the existence of some specific information, but also can prove the possession of that information, without revealing it or without interacting with the verifiers. Further, DAP transactions

conceal the sender, recipient and also the values of transactions, as opposed to Zerocoin. Moreover, transaction sizes are also smaller compared to Zerocoin (however, they are still larger than that of Bitcoin), which makes it more efficient than Zerocoin [39]. It also allows transactions of variable amounts. Despite the benefits over Zerocoin, the ZeroCash protocol does not hide IP addresses of end users. In order to achieve this anonymity, an anonymity network such as Tor, which facilitates anonymous transmission of data among users via tunnelling through a large network of distributed nodes, should be used [39]. Considering these facts, Zerocash can be regarded as having a moderate resistance against deanonymisation compared to Bitcoin. Moreover, ZeroCash is not compatible with the existing Bitcoin network and performance of the payment scheme is still affected by the heavy cryptographic computation involved.

Zcash is a virtual currency that was implemented recently based on the ZeroCash framework. This scheme uses a shielded payment scheme with zk-SNARKs to provide an anonymous, decentralised currency system [12]. Transaction values in Zcash can be either shielded or transparent, and it works similar to Bitcoin in the latter case. In comparison with ZeroCash, Zcash uses only the original Bitcoin transaction type with additional operations to handle shielded transactions. Although there are several advantages over the anonymity of shielded transactions, it is claimed that Zcash transactions are still linkable to some extent due to the fact that it supports both transparent and shielded transactions at the same time [33]. Thus, Zcash possesses a slightly higher level of anonymity than Zerocash with respect to confidentiality and the size of anonymity set. Nevertheless, both seem to have similar level of resistance to deanonymisation since a majority of Zcash transactions are transparent.

CryptoNote protocol was developed by Saberhagen [42] with an aim to address the weaknesses of Bitcoin, mainly the inflexibility of the system which resists the addition of new features to the Bitcoin framework. The CryptoNote protocol achieves both untraceability and unlinkability through the use of one-time ring signatures with non-interactive zero-knowledge proofs. Ring signatures allow a user in a group of users (a ring of users) to sign a message on behalf of the group, without revealing the identity of the signer [16]. This protocol also can be regarded as a form of non-interactive mixing [21]. Instead of one public key, the set of public keys belonging to all the users in the group is used to verify the signature. Several cryptocurrencies such as ByteCoin, DigitalNote, DarknetCoin and Aeon have been developed based on the CryptoNote architecture[14]. In spite of the claims for unlinkability, Noether [26] mentions that CryptoNote transactions may still be linkable as proven through some targeted attacks. Further, transaction values are not hidden and the transactions are larger in size compared to Bitcoin due to the size of cryptographic keys used. Therefore, Cryptonote can be considered as having similar levels of resistance to deanonymisation as Zcash.

Monero is an Altcoin with strong anonymity features and it was initially built on the CryptoNote protocol [29]. The anonymity of Monero has been strengthened continuously since its inception and the current framework uses Ring signatures to hide the sender details. This provides a way of mixing Monero coins with garbage coins named "mixins" [21]. Further, Ring Confidential Transactions (Ring CT) are used to hide transaction values which was not possible with CryptoNote [14, 28]. Confidential Transactions (CTs) provide a means of hiding transaction amounts while still allowing the transaction verification by other participants whereas Ring CT incorporates CTs with Ring signatures to improve on the original CryptoNote protocol [27]. This introduces a minor overhead in terms of block size in comparison to CryptoNote. In addition, unique one-time addresses (also known as Stealth Addresses) are used to hide the recipient. However, it may still be possible to link the addresses to network level IP addresses. Monero developers are working on an anonymous payment network named Kovri, which will provide facility to hide the IP addresses in Monero transactions.

Although Monero is claimed to be one of the most anonymous cryptocurrencies, recent studies have proved that Monero transactions can be de-anonymised [15, 21]. Miller et al. [21] showed that Monero transactions can be linkable due to the mixin sampling strategy used. In a separate study, Kumar et al. [15] developed three attack scenarios and proved that Monero's untraceability feature can be breached. Thus, the resistance of Monero against deanonymisation can be regarded as similar to CryptoNote and Zcash.

3.6 Recent Approaches

As already discussed, both mixing solutions and cryptographic solutions have limitations with respect to the achievable level of anonymity in cryptocurrencies. Recent research studies in this area have proposed solutions by combining mixing together with cryptographic techniques to achieve the best of both approaches.

CoinParty is an improved mixing service which uses decryption mixnets together with threshold signatures to achieve strong anonymity measures [45]. Decryption mixnets consist of a set of mixing nodes, which mix the inputs that are passed through them and provide required encryption and decryption [14]. Threshold signatures enable claiming funds upon agreement of a majority of mixing nodes. In this construction, mixing happens in a distributed manner, thereby eliminating the problems associated with traditional mixing schemes. Further, CoinParty is considered as one of the first mixing protocols to achieve plausible deniability [45]. This construction assumes the existence of at least two honest mixing nodes to establish the unlinkability of transactions. In addition, it takes longer to complete the mixing and to process the transaction, in comparison to the closest implementation, CoinShuffle.

ValueShuffle is a recent protocol which has been developed as an extension to CoinShuffle^{++} protocol with an aim to overcome the problems of early approaches such as difficulties in integrating to the existing Bitcoin framework [36]. The ValueShuffle specification has been constructed from

the CoinJoin protocol to achieve sender anonymity through decentralised coin mixing. Confidential Transactions are integrated in the protocol to hide the transaction values. Sender anonymity has been realised through the use of stealth addresses. Further, it is compatible with the Bitcoin architecture and is claimed to achieve a high level of anonymity when integrated with Bitcoin [36]. ValueShuffle transactions have lower transaction sizes compared to other cryptographic solutions and therefore the protocol improves on the efficiency with respect to space and time. In addition, these transactions incur comparatively lower fees among other protocols based on CoinJoin [36]. However, it may be possible to link input addresses to IP addresses at the network level unless an anonymous payment network is used.

Liu et al. [16] proposed an **unlinkable coin mixing scheme** which provides unlinkability without a trusted third party. This mixing scheme uses ring signatures with Elliptic Curve Digital Signature Algorithm (ECDSA) to achieve anonymity and it can be integrated to the existing Bitcoin framework. ECDSA is the algorithm used to generate and verify signatures in the Bitcoin network. This algorithm generates shorter key lengths and ring signatures provide anonymity of the sender. A mixing server is used to construct mixing transactions. Although this scheme achieves anonymity and scalability, the reliance on a central server degrades the decentralised implementation of cryptocurrencies.

Mimblewimble is an alternative cryptocurrency which proposes a novel idea to achieve privacy through the aggregation of confidential transactions, without storing individual transaction data [13, 32]. Although this provides better scalability, unlinkability cannot be assured among the participants who undertake the aggregation [36].

Wang et al. [43] proposed the concept of a **secure escrow address** to mix Bitcoin transactions without a trusted third party in a decentralised environment. In this scheme, participants use a temporary escrow address generated through a secure distributed key generation process and they transfer some Bitcoins to this address. Then each participant creates a set of output addresses of all participants which are then shuffled to form a list of output addresses. Bitcoins are then transfered from the escrow address to the list of output addresses. Moreover, this scheme also achieves strong deniability. However, malicious participants could have an impact on the system.

Chator et al. [6] proposed a novel technique to improve the efficiency over mixing protocols through an enhanced means of sampling obfuscating transactions. This solution proposes a recoverable sampling scheme constructed based on programmable hash functions and it is claimed that it can be integrated to many existing cryptocurrency implementations. Such strategies can be used to leverage anonymity properties of existing mixing protocols.

Although many anonymity constructions have achieved acceptable levels of anonymity with respect to the attributes such as unlinkability and untraceability, it is noteworthy that the unlinkability of IP addresses has not been realised as a whole. Many studies have proposed the use of anonymous communication channels to achieve this [39]. Hence, many research studies are now focusing on those aspects. **Bolt** is one such scheme and it presents a network level approach to facilitate an anonymous payment channel which could be used by existing anonymous cryptocurrencies. Blind Off-chain Light-weight Transactions (BOLT) provide a basis for defining payment channels that ensure the anonymity of transactions in decentralised cryptocurrencies while storing a part of the transaction data outside the blockchain [10].

Another network level approach was proposed by Fanti et al. [9] with an aim to strengthen the protection of the existing Bitcoin network against de-anonymisation attacks. They proposed a network protocol, **Dandelion**$^{++}$, a modified construction of a previously proposed protocol Dandelion, through the use of randomised routing algorithms and graph topologies.

Table 1 presents a comparative evaluation of cryptocurrency schemes that we discussed in this work versus Bitcoin, in terms of the proposed set of anonymity properties. It should be noted that some areas have not been addressed adequately in the literature, in which case, a comparison has been made on theoretical grounds. Further, deniability is not considered in Table 1 since it has not been studied in detail for a majority of the solutions. As a whole, these findings suggest that a single implementation that meets all the anonymity requirements does not exist as yet.

3.7 Other Related Studies

In addition to the literature focusing on anonymity constructions, there are other studies that assessed the strengths and weaknesses of such constructions through various types of de-anonymisation attacks. Morris [22] provided a critical evaluation of early implementations such as LiteCoin, MixCoin and Zerocoin by constructing transaction graphs from the public blockchain data. A similar evaluation done by Bonneau et al. [4] compared several mixing protocols as well as Zerocoin, ZeroCash and CryptoNote with respect to various aspects of anonymity and provided predictions for BitCoin's future. Maurer [17] conducted a survey on several mixing protocols and cryptographic methods and claimed that implementations like CoinJoin will have more potential towards achieving better anonymity compared to other cryptocurrencies. In a separate study, Moser et al. [23] surveyed and compared Fair Exchange, CoinJoin, CoinSwap and Stealth Addresses, which they considered as second generation anonymisation techniques, and provided a detailed account of each protocol and its anonymity considerations. A recent study by Khalilov et al. [14] presented a comprehensive analysis of nearly all anonymity constructions that have been proposed up to April, 2017 and classified them based on underlying techniques. Based on the outcomes of their analysis, they argued that a considerable amount of research should still be focused on improving the level of anonymity.

The level of anonymity achieved by different implementations as evaluated by these studies are only relative measures of anonymity among a set of implementations, that are often

Table 1: Comparative Evaluation of Current Anonymity Constructions

Anonymity Construction	Construction Attributes		Anonymity Properties					Degree of Anonymity Compared to Bitcoin			Resistance to Deanonymisation
	Protocol Type	Decentralised System	Fungibility	Level of Unlinkability[1]	Level of Untraceability[1]	Confidentiality	Metadata Unlinkability	Size of Anonymity Set	Average Transaction Processing Time[1]	Transaction Block Size[1]	
MixCoin	Mixing	X	X	Slightly high	Slightly high	X	X	No. of users in the mix	Moderately high	Similar	Low
CoinJoin	Mixing	√	X	Slightly high	Slightly high	X	X	No. of users in the mix	Moderately high	Similar	Low
Dash	Mixing	√	X	Slightly high	Slightly high	X	X	No. of users in the mix	Moderately high	Similar	Low
CoinShuffle	Mixing	√	X	Slightly high	Slightly high	X	X	No. of users in the mix	High	Similar	Low
CoinShuffle++	Mixing	√	X	Moderately high	Moderately high	X	X	No. of users in the mix	Slightly high	Similar	Low
Zerocoin	Cryptographic	√	X	Moderately high	Moderately high	X	X	No. of coins minted between mint and spend of a coin [2]	Moderately high	Large	Low
ZeroCash	Cryptographic	√	X	Moderately high	Moderately high	√	X	No. of coins minted between mint and spend of a coin	Moderately high	Large	Moderate
Zcash	Cryptographic	√	X	High	High	√	X	All users	Moderately high	Large	Moderate
CryptoNote	Cryptographic	√	√	Moderately high	Moderately high	√	X	No. of users in a group	Slightly high	Very Large	Moderate
Monero	Cryptographic	√	√	High	High	√	X	No. of users in a group	Slightly high	Large	Moderate
CoinParty	Mixing	√	X	High	High	X	X	All transactions with same value as chosen mixing value	Slightly high	Similar	Moderate[5]
ValueShuffle	Combined	√	X	High	High	√	X	No. of users in the mix	Moderately high	Similar	Moderate[5]
Mimblewimble	Cryptographic	√	X	Moderately high	Moderately high	√	X	No. of users in aggregation	Moderately high	Slightly large[3]	Moderate[5]
Secure Escrow Addresses	Mixing	√	X	Moderately high	Moderately high	X	X	No. of participants[4]	Slightly high	Slightly Large	Moderate[5]

[1] These measures are with respect to corresponding properties of Bitcoin.
[2] This is the minimum value. The maximum is the total set of minted coins.
[3] But the overall size of the blockchain is considerably smaller compared to Bitcoin.
[4] Can be extended to all Bitcoin users.
[5] Theoretically moderate resistance but no proven studies are available, yet.

grouped based on the techniques used. In contrast, our analysis focuses on evaluating the level of anonymity of these constructions in a unified manner in terms of a set of anonymity attributes. Outcomes of our analysis show that there is no theoretical model up to now, which could model anonymity across different cryptocurrency schemes in a systematic way.

4 DISCUSSION

The domain of cryptocurrencies is rapidly developing and it is significant from our study that a vast number of research studies have focused on improving the adaptability of cryptocurrencies. In this section, we summarise the findings of our survey, further supported in Table 1, and present our recommendations.

4.1 Current landscape of Anonymity of Cryptocurrencies

Existing anonymity protocols can be broadly categorised into two groups based on the method of implementation; centralised and decentralised. Centralised implementations are often realised through coin mixing protocols whereas cryptographic techniques have mainly led to decentralised implementations. These protocols can be classified further according to the techniques used. One group of protocols use various mixing schemes to achieve anonymity while another

group relies heavily on cryptographic methods. In addition, there is another set of constructions which combine both mixing and cryptographic methods.

In comparison with general mixing protocols, cryptographic solutions can be regarded as more effective in terms of the achievable level of anonymity. However, cryptographic solutions also have limitations such as higher transaction processing times and larger transaction block sizes due to cryptographic computations involved. Our findings show that despite the rapid development, many cryptocurrency schemes do not exhibit acceptable levels of anonymity. According to Table 1, a majority of mixing protocols have inherent limitations such as dependency on third parties, decentralised nature and smaller anonymity sets whereas cryptographic solutions try to achieve a compromise between anonymity and performance. In spite of having comparatively higher degree of anonymity compared to Bitcoin, these currency schemes are also susceptible to de-anonymisation attacks. Hence, there is much to improve on almost all current constructions.

With regard to the evaluation of the level of anonymity, there is no universal model that could be used to assess the anonymity of different cryptocurrency implementations. Modelling anonymity of cryptocurrencies involves a complex process of studying different notions of anonymity and their relationships and dependencies, which certainly requires further study.

On a different note, some argue that cryptocurrency schemes should be auditable so that misuses of cryptocurrencies leading to illegal activities such as money laundering could be traced and culprits could be identified by law enforcement authorities. In other words, relevant legal authorities should be able to de-anonymise transactions which could then lead to the loss of fungibility. Further, Reynolds et al. [35] argued that cryptocurrencies should be subject to a universal regulation setup in order to be able to trace illegal transactions. In that regard, Nagamuna et al. [24] proposed a method to allow authorised parties extract transaction information in Zerocoin without letting others access the same. The proposed scheme deploys a non-interactive zero-knowledge proof of knowledge (NIZKP) to achieve auditability. Nevertheless, this is not our position, since such implementations will inevitably result in weakening the level of anonymity. As it was claimed at the outset, non-fungibility can lead to instabilities because some coins may lose value based on their histories, compromising the integrity of the currency system.

4.2 Recommendations for Future Research

Although there are numerous studies into the problem of anonymity, originating from the inception of Bitcoin up to now, several significant gaps still prevail in related research.

With respect to the evaluation of anonymity levels, it was evident that each protocol deploys its own theoretical framework to prove the level of anonymity due to the absence of a common evaluation framework. As such, the perceived level of anonymity is only a relative measure and cannot be compared across different platforms. This opens up a new research direction towards formulating a common rigorous theoretical framework, which can be used to effectively capture every attribute of anonymity of different currency schemes.

In relation to different aspects of anonymity, almost all cryptocurrency schemes focused on improving unlinkability, recipient anonymity and untraceability, yet the majority have failed to achieve acceptable levels of unlinkability of metadata such as IP addresses. In addition, very few constructions give consideration to improving fungibility and deniability. Hence, these areas need to be explored further to enhance privacy and anonymity in these perspectives.

5 CONCLUSION

In this work, we examined different theoretical frameworks that are used to model anonymity and surveyed a number of solutions proposed to address anonymity issues of cryptocurrencies. Then we evaluated their effectiveness against a set of anonymity properties identified through the studied theoretical models. Our findings showed that despite numerous attempts to achieve complete anonymity and privacy of cryptocurrencies, limitations exist in their practical implementations and hence they had been unable to realise true anonymity in practice. It was also evident that there was no unified theoretical framework available to measure the level of anonymity across different anonymity constructions. Therefore, one cannot gain a proper understanding of the anonymity of cryptocurrencies from a broader perspective. As such, our work leads to several future research directions. More importantly, the adoption of an acceptable framework to model anonymity in the context of cryptocurrencies would help understand the areas that need to be improved in order to realise the full potential of cryptocurrencies.

REFERENCES

[1] Elli Androulaki and Ghassan O. Karame. 2014. Hiding Transaction Amounts and Balances in Bitcoin. In *Trust and Trustworthy Computing*, Thorsten Holz and Sotiris Ioannidis (Eds.). Springer International Publishing, Cham, 161–178.

[2] Elli Androulaki, Ghassan O Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. 2013. Evaluating user privacy in bitcoin. In *International Conference on Financial Cryptography and Data Security*. Springer, 34–51.

[3] Simon Barber, Xavier Boyen, Elaine Shi, and Ersin Uzun. 2012. Bitter to better - How to make bitcoin a better currency. In *Financial Cryptography and Data Security. FC 2012. Lecture Notes in Computer Science*, Vol. 7397. 399–414.

[4] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. 2015. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In *2015 IEEE SYMPOSIUM ON SECURITY AND PRIVACY SP 2015 (IEEE Symposium on Security and Privacy)*. IEEE Comp Soc Tech Comm Security & Privacy, 104–121. https://doi.org/{10.1109/SP.2015.14} IEEE Symposium on Security and Privacy SP, San Jose, CA, MAY 18-20, 2015.

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

[6] A. Chator and M. Green. 2018. How to Squeeze a Crowd: Reducing Bandwidth in Mixing Cryptocurrencies. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. 40–49. https://doi.org/10.1109/EuroSPW.2018.00012

[7] Mauro Conti, Sandeep Kumar, Chhagan Lal, and Sushmita Ruj. 2018. A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials* (2018).

[8] Evan Duffield and Daniel Diaz. 2014. Dash: A PrivacyCentric CryptoCurrency.

[9] Giulia Fanti, Shaileshh Bojja Venkatakrishnan, Surya Bakshi, Bradley Denby, Shruti Bhargava, Andrew Miller, and Pramod Viswanath. 2018. Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees. *Proceedings of the ACM on Measurement and Analysis of Computing Systems* 2, 2 (2018), 29.

[10] Matthew Green and Ian Miers. 2017. Bolt: Anonymous Payment Channels for Decentralized Currencies. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*. ACM, New York, NY, USA, 473–489. https://doi.org/10.1145/3133956.3134093

[11] Jordi Herrera-Joancomartí. 2015. Research and Challenges on Bitcoin Anonymity. In *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*, Joaquin Garcia-Alfaro, Jordi Herrera-Joancomartí, Emil Lupu, Joachim Posegga, Alessandro Aldini, Fabio Martinelli, and Neeraj Suri (Eds.). Springer International Publishing, Cham, 3–16.

[12] Daira Hopwood, Sean Bowe, Taylor Hornby, and Nathan Wilcox. 2016. *Zcash protocol specification*. Technical Report. Tech. rep. 2016-1.10. Zerocoin Electric Coin Company.

[13] Tom Elvis Jedusor. 2017. MIMBLEWIMBLE. (2017). https://scalingbitcoin.org/papers/mimblewimble.txt

[14] M. C. K. Khalilov and A. Levi. 2018. A Survey on Anonymity and Privacy in Bitcoin-like Digital Cash Systems. *IEEE Communications Surveys Tutorials* (2018), 1–1. https://doi.org/10.1109/COMST.2018.2818623

[15] Amrit Kumar, Clément Fischer, Shruti Tople, and Prateek Saxena. 2017. A Traceability Analysis of Monero's Blockchain. In *Computer Security – ESORICS 2017*, Simon N. Foley, Dieter Gollmann, and Einar Snekkenes (Eds.). Springer International Publishing, Cham, 153–173.

[16] Y. Liu, X. Liu, C. Tang, J. Wang, and L. Zhang. 2018. Unlinkable Coin Mixing Scheme For Transaction Privacy Enhancement of Bitcoin. *IEEE Access* (2018), 1–1. https://doi.org/10.1109/ACCESS.2018.2827163

[17] Felix Konstantin Maurer. 2016. A survey on approaches to anonymity in bitcoin and other cryptocurrencies. *Informatik 2016* (2016).

[18] F. K. Maurer, T. Neudecker, and M. Florian. 2017. Anonymous CoinJoin Transactions with Arbitrary Values. In *2017 IEEE Trustcom/BigDataSE/ICESS*. 522–529. https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.280

[19] Sarah Meiklejohn and Claudio Orlandi. 2015. Privacy-Enhancing Overlays in Bitcoin. In *Financial Cryptography and Data Security*, Michael Brenner, Nicolas Christin, Benjamin Johnson, and Kurt Rohloff (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 127–141.

[20] I. Miers, C. Garman, M. Green, and A. D. Rubin. 2013. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In *2013 IEEE Symposium on Security and Privacy*. 397–411. https://doi.org/10.1109/SP.2013.34

[21] Andrew Miller, Malte Moeser, Kevin Lee, and Arvind Narayanan. 2017. An Empirical Analysis of Linkability in the Monero Blockchain. (2017).

[22] Liam Morris. 2015. *Anonymity Analysis of Cryptocurrencies*. Ph.D. Dissertation.

[23] M. Möser and R. Böhme. 2017. Anonymous Alone? Measuring Bitcoin's Second-Generation Anonymization Techniques. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. 32–41. https://doi.org/10.1109/EuroSPW.2017.48

[24] K. Naganuma, M. Yoshino, H. Sato, and T. Suzuki. 2017. Auditable Zerocoin. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. 59–63. https://doi.org/10.1109/EuroSPW.2017.51

[25] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008). https://bitcoin.org/bitcoin.pdf

[26] Surae Noether. 2014. Review of CryptoNote white paper. (2014).

[27] Shen Noether. 2015. Ring Signature Confidential Transactions for Monero. Cryptology ePrint Archive, Report 2015/1098. https://eprint.iacr.org/2015/1098.

[28] Shen Noether, Adam Mackenzie, and the Monero Research Lab. 2016. Ring Confidential Transactions. *Ledger* 1, 0 (2016), 1–18. https://doi.org/10.5195/ledger.2016.34

[29] Shen Noether and Sarang Noether. 2014. Monero is not that mysterious. *Technical report* (2014). https://lab.getmonero.org/pubs/MRL-0003.pdf

[30] Micha Ober, Stefan Katzenbeisser, and Kay Hamacher. 2013. Structure and Anonymity of the Bitcoin Transaction Graph. *Future Internet* 5, 2 (2013), 237–250. https://gateway.library.qut.edu.au/login?url=https://search-proquest-com.ezp01.library.qut.edu.au/docview/1524881011?accountid=13380 Copyright - Copyright MDPI AG 2013; Last updated - 2014-07-30.

[31] Andreas Pfitzmann and Marit Hansen. 2010. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. Http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf V0.34.

[32] Andrew Poelstra. 2016. Mimblewimble. (2016).

[33] J. Quesnelle. 2017. On the linkability of Zcash transactions. *ArXiv e-prints* (Dec. 2017). arXiv:cs.CR/1712.01210

[34] Fergal Reid and Martin Harrigan. 2013. *An Analysis of Anonymity in the Bitcoin System*. Springer New York, New York, NY, 197–223. https://doi.org/10.1007/978-1-4614-4139-7_10

[35] Perri Reynolds and Angela S.M. Irwin. 2017. Tracking digital footprints: anonymity within the bitcoin system. *Journal of Money Laundering Control* 20, 2 (2017), 172–189. https://doi.org/10.1108/JMLC-07-2016-0027 arXiv:https://doi.org/10.1108/JMLC-07-2016-0027

[36] Tim Ruffing and Pedro Moreno-Sanchez. 2017. ValueShuffle: Mixing Confidential Transactions for Comprehensive Transaction Privacy in Bitcoin. In *Financial Cryptography and Data Security*, Michael Brenner, Kurt Rohloff, Joseph Bonneau, Andrew Miller, Peter Y.A. Ryan, Vanessa Teague, Andrea Bracciali, Massimiliano Sala, Federico Pintore, and Markus Jakobsson (Eds.). Springer International Publishing, Cham, 133–154.

[37] Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate. 2014. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. In *Computer Security - ESORICS 2014*, Mirosław Kutyłowski and Jaideep Vaidya (Eds.). Springer International Publishing, Cham, 345–364.

[38] Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate. 2016. P2P Mixing and Unlinkable Bitcoin Transactions. *IACR Cryptology ePrint Archive* 2016 (2016), 824.

[39] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. 2014. Zerocash: Decentralized Anonymous Payments from Bitcoin. In *2014 IEEE Symposium on Security and Privacy*. 459–474. https://doi.org/10.1109/SP.2014.36

[40] Jan-Willem Selij. 2015. CoinShuffle anonymity in the Block chain. (2015).

[41] LATANYA SWEENEY. 2002. k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10, 05 (2002), 557–570. https://doi.org/10.1142/S0218488502001648 arXiv:https://www.worldscientific.com/doi/pdf/10.1142/S0218488502001648

[42] Nicolas Van Saberhagen. 2013. Cryptonote v 2. 0. https://cryptonote.org/whitepaper.pdf

[43] Q. Wang, X. Li, and Y. Yu. 2018. Anonymity for Bitcoin From Secure Escrow Address. *IEEE Access* 6 (2018), 12336–12341. https://doi.org/10.1109/ACCESS.2017.2787563

[44] Dimaz Ankaa Wijaya, Joseph K. Liu, Ron Steinfeld, Shi-Feng Sun, and Xinyi Huang. 2016. Anonymizing Bitcoin Transaction. In *Information Security Practice and Experience*, Feng Bao, Liqun Chen, Robert H. Deng, and Guojun Wang (Eds.). Springer International Publishing, Cham, 271–283.

[45] Jan Henrik Ziegeldorf, Roman Matzutt, Martin Henze, Fred Grossmann, and Klaus Wehrle. 2018. Secure and anonymous decentralized Bitcoin mixing. *Future Generation Computer Systems* 80 (2018), 448 – 466. https://doi.org/10.1016/j.future.2016.05.018