

A Contribution to Blockchain Privacy

MALIKA YAICI, FERIEL LALAOUI, LYDIA BELHOUL

Computer Department

University of Bejaia

Route de Targa Ouzemour, Bejaia, 06000

ALGERIA

Abstract: - As a new distributed point-to-point (P2P) technology, blockchain has become a very broad field of research, addressing various challenges including privacy preserving as is the case in all other technologies. In this work, a study of the existing solutions to the problems related to private life in general and in blockchains in particular is performed. User anonymity and transaction confidentiality are the two main challenges for the protection of privacy in blockchains. Mixing mechanisms and cryptographic solutions respond to this problem but remain subject to attacks and suffer from shortcomings. Taking into account these imperfections and the synthesis of our study, we present a mixing model without trusted third parties, based on group signatures allowing reinforcing the anonymity of the users, the confidentiality of the transactions, with minimal turnaround time and without mixing costs.

Key-Words: - Blockchain, Privacy, Anonymity, Mixing coins

Received: May 19, 2024. Revised: March 16, 2025. Accepted: April 21, 2025. Published: July 16, 2025.

1 Introduction

As Blockchain technology, introduced in 2009 [1], has undergone a spectacular evolution in the last ten years. It is considered to be a revolutionary technique for carrying out transactions without a trusted third party while protecting users' identity through the use of pseudonyms. More and more businesses and organizations are eager to deploy Blockchain technology for record keeping and business management.

However, the public nature of the Blockchain poses a major problem of preserving user privacy and data confidentiality. Indeed, many research works have been able to highlight the main shortcomings and weaknesses of this technology. Some studies have succeeded in de-anonymizing users, which is a major question of the interest of using blockchains. These criticisms have rightly prompted researchers to propose different solutions aimed at improving the preservation of the privacy of blockchain users.

In this paper a study on the problem on how to improve the protection of privacy in Blockchains as well as the various proposed solutions is undergone and a method based on coin mixing is proposed.

After this brief introduction, section 2 is about Privacy principle and technologies both in Internet and blockchains. Section 3 is a thorough study on related works with a synthesis and a comparison. The contribution is detailed in section 4 with a validation. A conclusion and perspectives finish the paper.

2 Privacy

Privacy is a general concept, which has different meanings according to people and varies according to each individual and context. This concept can encompass several notions such as: the right to be alone, the right to freedom of thought, the right to one's own family life, the right to protect one's reputation, etc. Moreover, these notions may vary from one context to another [2]. On the Internet, privacy encompasses a range of issues relating to the ability of Internet users to ensure control and transparency over the use of their personal data when it is collected and used by private or public entities.

2.1 Privacy principles

Several fundamental principles can be deployed to ensure the protection of privacy. These principles should be implemented in any privacy-enabled

system or architecture. There are principles relating to data and others to the identity and activities of the individual.

1. Data protection [3]:

- Data Minimization: This principle requires that the data collected must be used only for specific, legitimate purposes and limited to what is necessary with regard to the purposes for which they are collected.
- Explicit consent: This principle requires that any collection or processing of personal data must not take place without the explicit and prior authorization of the owner of this data.
- Data Sovereignty (right to be forgotten): This principle gives an individual the right to access, correct and delete their personal information.
- Transparency: This principle requires that a user has the right to be informed about the personal information collected, and how and why their data is used and with whom it is shared.
- Security: an organization that holds personal information must ensure security measures against loss, unauthorized access, misuse or disclosure.

2. Identity and Business Protection [4]:

- Anonymity: This principle allows a user to carry out an action without it being able to be linked to his identity.
- Pseudonymity: This principle defines the fact that a system offers its users the possibility of acting under a pseudonym instead of their real identities.
- Unlinkability: This principle defines the fact that in a system, an attacker is unable to link two anonymous actions that were carried out by the same individual.
- Unobservability: This principle defines the fact that an attacker is unable to know, at a given moment, whether a particular action is taking place or not.

2.2 Privacy threats

All privacy threats relate to unauthorized or malicious use of collected data. The most common threats are:

- Disclosure of personal data: finding and accessing personal information has become a very simple operation due to the emergence of social networks and content sharing services.
- Identity theft and usurpation: Identity theft is one of the fastest growing crimes. It can be considered identity theft; any time a criminal steals some of a person's data and uses it for their own benefit.
- Profiling: Profiling refers to the fact of compiling information files on individuals in order to deduce interests and characteristics by correlation with other profiles and data.

2.3 Internet privacy technologies

There exist many developed techniques to manage private information.

2.3.1 Anonymous accreditations

It is a set of cryptographically based techniques, allowing a user to present proof of qualification, competence or access authorization issued by an authority for an individual without revealing anything about him, other than the accreditation.

1. Blind signature: This concept offers the possibility of having a message signed, without the signatory being able to read the content of this message. The basic principle for achieving this type of signature is to use a blinding function (which encrypts the content of a message) and its inverse.
2. Group signature: Analogous to the digital signature, this technique is generally used to verify the membership of an individual in a group (which may have access to resources) without revealing their identity. Each person belonging to the group has a private key specific to him, and a unique public key for all the members (public key of the group).
3. Ring signature: Introduced in 2001[5], it is a process of forming a ring by network participants and creating a simplified group signature that divulges secrets anonymously. This signature is based on the private key of the ring initiator, the public keys of the members of the ring, random numbers and other technologies. The verifier can just verify that this signature comes from this group of signatories

without ever being able to know who the initiator is. Anonymity is thus preserved.

4. Zero-knowledge proof (ZK proof): It is used to prove the validity of a declaration without having to disclose any information. Another variant of zk proofs known as NIZK proof (non iterative zero-knowledge) is widely used since it drastically reduces the complexity of communication [6].
5. Homomorphic encryption: It is a cryptographic technique that allows calculations to be performed directly on encrypted data; the result of the calculation is the same as that performed on the original data [7].
6. Multi-party computation (MPC): Security Multi-Party Computation (SMPC) is a cryptographic protocol that allows mutually suspicious distributed parties to jointly compute arbitrary functionality without having to reveal their own private inputs and outputs [8].

2.3.2 Anonymous communication networks

It is a technology which allows protecting the identity of the sender and/or the receiver of the message among a group (or the whole population), ensuring unlinkability and unobservability.

1. Mix network: It is a family of routing modes that promote anonymity by preventing traffic analysis, hiding the link between incoming and outgoing messages by message encryption and swapping mechanism. The mixer receives as input several pairs of type (message; recipient's address) which have been previously encrypted, then decrypts an encryption layer and relays the message to the recipient [9].
2. The Onion Router (TOR): It is a decentralized, anonymous global network organized in layers around routers that play the role of nodes; it allows anonymizing any type of communication made on the Internet. The Tor network consists of a group of servers (onion routers), its operating principle is very similar to that of the Mix-nets, apart from the mixing stage which does not exist. Security in TOR is based primarily on the choice of routes that are difficult for an adversary to predict.

However, and unlike mix networks, TOR is unable to withstand an attack from an adversary able to see the full path of the servers [10].

3. Crowds Anonymous: It is a communication protocol that protects the anonymity of the sender of a message by routing it randomly, to groups of similar users. The main idea is to hide the origin of a message by scattering it. The nodes are grouped in "Crowds". Only nodes of the same Crowd can connect to each other to relay traffic. When a user wants to access a website, he will forward the request to a random node. This one will choose randomly if it transfers the package to another node or if it sends it directly to the web server. The process is repeated until the request arrives at its destination [11].

2.4 Privacy technologies in Bigdata

Today, big data is used in all fields of science, technology and social-economic activities, the protection of this data is therefore essential to maintain the privacy of individuals.

2.4.1 K-anonymity

A publication of data is said to be anonymous if the information relating to each person contained in the publication cannot be perceived by at least $k-1$ people whose information appears in the publication. In the context of k -anonymity problems, a database is a table that consists of n rows and m columns, where each row of the table represents a record relating to a particular individual in a population, there are two techniques to achieve k -anonymity for some value of k in a table [12]:

- Deletion: This technique generates an anonymous table where all the data of the original table sources of a risk of re-identification are removed. A deletion can concern both the deletion of tuples in their entirety and the deletion of some tuple data (replacement by the null value). In the first case, we speak of global deletion and the second case is called local deletion.
- Generalization: It consists in diluting information so that it can no longer be attached to a person or a small group of people.

2.4.2 L-diversity

It reinforces k-anonymity by avoiding, in the event that a victim's QIT is known, targeting a record from a published table and therefore, as a result, directly revealing the victim's sensitive data. An equivalence class respects the l-diversity constraint if it contains at least l "representative" values for the sensitive attribute [13].

2.4.3 T-proximity

Although l-diversity protects the tables, it is still possible for an adversary to obtain information about a sensitive attribute when he has information about the global distribution of this attribute. To counter this, t-proximity has been proposed. This model ensures that the distribution of the sensitive attribute within any equivalence class is close to the global distribution of the attribute. In other words, he introduces the concept of distance between these two distributions and proposes that this distance does not exceed a threshold t. Thus, the smaller t is, the more the adversary's possibility of inference is reduced [13].

2.4.4 Differential privacy

Differential Privacy has been a very fashionable method in computer research circles for a few years, because unlike previous methods, it is the only one to give formal guarantees on the possibility of limiting the information that can be learned about individuals. It makes it possible to obtain useful information from databases that contain personal data, without revealing the personal identity of individuals [13], [14].

2.5 Blockchain privacy

Privacy protection has been widely studied in blockchains, as a distributed database, blockchain technology has significant privacy protection advantages, such as data inviolability and user anonymity. However, the decentralized architecture mechanism and data storage adopted by blockchain technology also bring some negative effects on privacy protection. The two main issues are the identity privacy (anonymity) challenge and the user transaction (data) privacy challenge.

2.5.1 Identity privacy (anonymity)

User privacy is the ability to convert a blockchain user's real identity into something that cannot be identified, and further ensuring that the original identity also remains impossible to be obtained. Anonymity hides the real identity of the user by masking the users' real network address with a computer generated address [7].

2.5.1 Data privacy (confidentiality)

Data privacy in blockchains is all about hiding the content of a transaction. At the most basic level, the data content of a transaction is usually encrypted to maintain confidentiality in the network. In blockchains, although users exchange transactions directly using pseudonyms, anyone can track those transactions, see the exact amount of exchanges, and by which pseudonyms those exchanges were made. This has resulted in successful attempts to link these pseudonyms to real-world entities as shown in [15].

3 Related Works

In order to propose a solution improving the preservation of anonymity in Blockchain, we began by studying the works that have dealt with this subject. In [16], the authors discussed privacy issues related to user identity and transaction privacy in Blockchain systems, this study covered privacy protection techniques in Blockchain technology like the mixing mechanism, zero-knowledge proof, ring signature, hidden address, homomorphic encryption, stealth address, pawning, secure multiparty computation and trusted execution environment. They also carried out a detailed comparative analysis of the latter on the technical and anonymity side. The authors concluded that centralized mixing and hidden address mechanisms have the lowest privacy followed by decentralized mixing and ring signing, while the other four techniques have better privacy and improved anonymity in blockchains.

Although each of the studied works presents a mix of different technologies to achieve the much sought-after privacy preservation, one could try to distinguish them. The methods can be classified into: Coin mixing solutions and Cryptographic solutions. The first class consists of centralized and decentralized coin mixing techniques. The second class consists of techniques based on signatures, Zero-knowledge proof, homomorphic cryptography, Security Multi-Party Computation, etc.

3.1 Cryptographic solutions

3.1.1 Signatures based solutions

Inspired and built from the Bitcoin protocol, the authors in [17] present a private decentralized token-based P2P system named PriWatt. The goal of PriWatt is to ensure the security of transactions as well as the confidentiality of user identities in smart grid systems in the energy field. This system consists of blockchain-assisted distributed smart

contracts, multi-signatures, and anonymous encrypted messaging streams. Following the agreements written in the smart contract, PriWatt allows sellers and buyers to securely bid and negotiate energy prices. To be done anonymously, the technique of anonymous mail flow is used. The multi-signature scheme is deployed to provide protection against theft; while to validate a transaction, a minimum of M of the N parties must sign the transaction in order to complete it. The signature is done using an Elliptic Curve Digital Signature Algorithm (ECDSA). In the event that there are problems during a transaction, the Distribution Network Manager (DNM) is responsible for solving the problem. Moreover, for the consensus, PoW is used to avoid certain attacks, like the Byzantine fault attack and the double-spend attack.

In [18], a framework named Attrichain, that implements transactions with anonymous sender identity and threshold traceability used in permissioned blockchain, is proposed. Attrichain realizes on-chain access control and distributed identity governance by allowing users to create transactions anonymously using their transaction keys and their attributes. The identity management or tracing of misbehaviors is distributed on multiple independent spontaneous tracing members.

3.1.2 Zero-knowledge proof

In [19], an investigation on usage of multi-blockchain Zero Knowledge Proof mixers by adversarial actors is undergone. More specifically, using coin flow tracing, the deposit and withdrawal behavior is studied. Five on-chain data heuristics to measure Mixer Anonymity Set Size are proposed, and the impact of Anonymity Mining on privacy is evaluated.

- Zerocoin: In [20], the authors extended Bitcoin to improve user anonymity and protect their privacy. The principle is to break the links between Bitcoin transactions and to hide the origin of the latter, by replacing a coin with a new one which has the value of the first plus the fees in bitcoins generated by this operation. The resulting coin must have a value corresponding to a transaction and be correctly constructed. This protocol relies on zero-knowledge proof to certify that the coins generated belong to a list of valid coins.
- In Zerocash [21], the authors criticized the functionalities of Zerocoin and brought an

improvement by relying essentially on the advances of zero-knowledge proof and more precisely the zk-SNARK. It is considered to be a decentralized electronic payment system which allows anonymous payments of any amount. Just like Zerocoin, the principle of replacing one coin by a new one is also adopted, except that the values are not fixed.

- Hawk [22]: It is based on the concept of smart contracts introduced by Ethereum to ensure privacy-preservation in blockchain technology Hawk is offered to users even if they are not proficient in programming or cryptography because it compiles the program into a cryptographic protocol using cryptographic primitives such as zero-knowledge proof and secure multi-party computation SMPC. It is made up of two parts, a private part which takes into account the contribution of the parties to the contract and a public part which does not concern money or private data.
- Privacy Pools [23] is a novel smart contract-based privacy-enhancing protocol. The protocol is based on a mechanism where users can reveal certain properties of their transaction without having to reveal the transaction itself. The users publish a zero-knowledge proof on the origin of their funds, without publicly revealing their entire transaction history. This is achieved by proving membership in custom association sets, which are designed to demonstrate compliance with regulatory frameworks or social consensus.

3.2 Coin mixing solutions

This mechanism, commonly used in blockchains, consists in adding intermediate transit information to hide the link between the input address and output address of a transaction, thus ensuring the confidentiality of transactions.

3.2.1 Centralized coin mixing

This method consists in using an intermediate node (server) to play the role of a trusted third party and perform the mixing of the funds thanks to an adequate mixing algorithm; the objective is to

scramble the addresses and the link between the entry and the output of a transaction.

- Mixcoin [24] is a protocol proposed to facilitate anonymous payments using the Bitcoin monetary system, it uses a central mixing server to mix transaction addresses and offer mixing services to users. The links between the input and output addresses are then masked. To improve anonymity, MixCoin requires users to choose the same amount to mix simultaneously and they are not allowed to choose the number of corresponding transactions, so the mixing server must be honest enough to record the identities and information contained in transactions.
- BlindCoin [25] is based on the idea of adding to MixCoin a blind signature and an append-only property associated with an access log that monitors the mix server. The data and transactions manipulated by the Mixing Server are added and recorded on the log but cannot be overwritten or deleted, making the Mixing Server responsible and its theft attempts detectable. Blind signing in BlindCoin hides the relationship between the input address and the output address of a transaction from the mix server itself. However, it is still impossible to prove the honesty of the log and becomes a target of possible attacks, which weakens the anonymity of BlindCoin.
- Blind-Mixing: The authors of [13] tried to improve the BlindCoin protocol with a blind-signature mixing algorithm based on an elliptic curve that prevents mixing servers from binding an input address to an output address. Blind-Mixing offers better anonymity protection than BlindCoin and a very high overall blind signature calculation speed performance.
- LockMix [12] also offers an improvement to the BlindCoin protocol; in fact, it is a protocol that uses a blind signature algorithm to hide the link between the input address and the output address of a transaction from the server, as well as a multi-signature scheme which prevents from funds theft by the mixing server. To ensure the protection of data in the IP layers of the network, protocol Tor [10] has been

adapted. The LockMix protocol works in two phases: payment deposit phase and mixing phase including a mixing fee.

3.2.2 Decentralized coin mixing

Decentralized mixing uses techniques that do not require a trusted third party. In addition, they can prevent theft and eliminate mixing fees in most of the techniques offered.

- CoinJoin [26] is the oldest of the decentralized mixing protocols, published on the bitcoin forum. CoinJoin uses a central server at zero cost. In the CoinJoin system, it is necessary for several network users to establish the decision to use this method, then each user, signs and sends his request to the central server individually and simultaneously. When receiving all the requests, the server then changes the input addresses, performs the mixing of the funds, gathers the transactions and generates a many-to-many type transaction, then transfers the funds to the corresponding output addresses.
- CoinShuffle [27] is considered a complete decentralized mixing protocol, which allows Bitcoin to be used in an anonymous way, it is inspired by the two protocols CoinJoin and Dissent [28], which is the first general messaging protocol that offers provable anonymity with responsibility for medium-sized groups and manages unbalanced loads where few members wish to transmit data in a specific round. The multi-signature scheme is used to encrypt the exit address of each transaction with the public keys of the other members of the group. If the nodes of the group suspect a node of being dishonest, they just have not to sign its transaction and will be excluded from the group, the protocol will be re-executed. The use of a trusted third party is eliminated, which does not entail mixing costs. This protocol was improved in 2017 and gave birth to CoinShuffle++ which integrates DiceMix [29], to perform mixing in parallel and not in sequential order.
- Xim [30] is an approach proposed to resist known attacks against mixing, notably Sybil, DOS and inference attacks (data analysis to extract information). Xim is a bipartite multi-turn protocol; it includes an

anonymous decentralized partner search system to perform the mixing using FairExchange [31] which is a protocol allowing two users to exchange funds by swapping their exit addresses. It can support up to four transactions at the same time unlike CoinJoin which only supports one. No external party can confirm or find evidence regarding partners who match. Miners take care of partnership requests in exchange for fees paid by the requester and the responder. The transaction is then validated and executed, if and only if the two partners match.

- ValueShuffle [32] is an extension of CoinShuffle++, it combines the protocols CoinJoin, Confidential Transaction (CT) [33] and Stealth Addresses (SA) [34], thus, during a transaction with ValueShuffle the anonymity of the payer, the anonymity of the beneficiary and the confidentiality of the amount to be transferred are significantly improved compared to other protocols.
- Möbius [35] was the very first trustless coin mixer based on an Ethereum smart contract. The Möbius authors provided formal definitions of various security notions such as anonymity, theft prevention, and mixer availability. These properties could be used to evaluate and compare future proposals from a security point of view. This is what MixEth has done, which we will discuss shortly. Möbius uses ring signature and stealth addresses, it is relatively resistant to DOS attacks.
- Miximus [36] is a zk-SNARK based mixer for Ethereum. It uses zk-SNARK to hide the correspondence between senders and receivers. An emitter creates a leaf in a Merkle tree. The sender must exchange the preimage of the leaf with the receiver. Later, a recipient could prove to the Miximus contract that they know one of the preimages of a certain undisclosed leaf, called cancellers; they allow recipients to withdraw funds once and only once.
- MixEth [37] is a decentralized multi-turn protocol that uses Neff's verifiable mixes [38] in the context of Ethereum coin mixes. MixEth users take turns mixing public keys using a secret multiplier that is known only

to the mixer, in an effort to break the ties between the public keys of the sender and the receiver. Next, a challenge round is imposed on the mixer to generate a publicly verifiable ZK-proof to convince other participants in the mix that the mix was done correctly, without disclosing the secret multiplier.

3.3 Synthesis

Mixing services are relatively simple methods for privacy protection in the blockchain. Most are compatible with existing blockchain protocols and require few resources to implement. The privacy protection they propose is acceptable and remains an interesting area of research for future work, in particular to improve:

- Waiting times: the user waiting for other participants to participate in the mixing leads to a high waiting time for a transaction to be validated.
- Malicious Mixing Servers: Although Mixing Servers hides the relationship between inputs and outputs of a transaction, however, the server itself can be dishonest and hence the confidentiality becomes prone to breaches.
- Mixing Fees: Mixing services usually incur fees and can be very expensive.

Mixing services and ring signatures may provide confidentiality of user identity but do not guarantee confidentiality of transaction data. Similarly, cryptographic solutions, such as anonymous credential systems and anonymous communication networks, aim to ensure the confidentiality of transaction data but do not ensure the confidentiality of the user's identity and are costly in terms of resource consumption and execution time. Additionally, although ZKPs provide both types of privacy in blockchains, this comes at the expense of system performance and high cost. These technologies are applied to various digital currencies and other applications, such as Zerocoin, Zerocash and Hawk. A common characteristic brings them together, decentralization, which avoids attacking malicious third-party nodes as well as transaction analysis. Therefore, the protection of privacy in the blockchain must be improved, especially since many users and sectors adapt it to their systems.

In [39], a study on blockchain-based mixing services, particularly on theoretical propositions (CoinJoin, CoinShuffle, MixCoin, etc.) compared to

real implementations solutions (BitcoinFog, BitLaundry, Blockchain.com, etc.), is undergone. The author proposes a set of evaluation criteria for mixing services (Centralized, Mixing fee, Attack resistance, etc.) and provides a detailed analysis on what are the weaknesses and strengths of different mixing solutions.

A comparison of different privacy protection techniques has been established in terms of many criteria, almost the same as in [mixing]; it is summarized in table1 and table2. As for malicious Behavior Penalty only Coin Shuffle and Coin Shuffle++ protocols integrate suspicious nodes suppression.

Table 1 Resistance to attacks

Resistance to attacks	Protocols
Resistance to DoS attacks	ZeroCoin, ZeroCash, MixEth, Hawk, Privacy Pools, Mobius, Coin Shuffle++, Xim, Value Shuffle, LockMixing
Vulnerable to DoS attacks	CoinJoin, Coin Shuffle
Resistance to Sybil attacks	ZeroCash, Xim, LockMixing
Vulnerable to Sybil attacks	CoinJoin, Coin Shuffle
Resistance to Inference attacks	ZeroCash, Xim
Resistance to theft	MixEth, Mobius, LockMixing
Minimal risk of theft	ZeroCoin, ZeroCash, Xim, Hawk, Privacy Pools, CoinJoin, Coin Shuffle++, Value Shuffle, Coin Shuffle
Vulnerable to theft	Miximus (very)
High Anonymity	ZeroCoin, MixEth, Mobius, Value Shuffle

Additional fees: +fees
 Trusted Third Party: TTP
 Type of Protection: Type
 Used Technology: Used Tec

Table 2 Comparative table

Protocol	Used Tec	Type	TTP	+fees
MixCoin	Cent. Mixing	Data	Yes	Yes
BlindCoin	//	Identity	Yes	Yes
Blind Mixing	//	Identity	Yes	Yes

Lock Mixing	//	Identity	Yes	Yes
CoinJoin	Decent. Mixing	Identity	No	No
Coin Shuffle	//	Identity	No	No
Coin Shuffle++	//	Identity	No	No
Value Shuffle	//	Identity	No	No
Xim	//	Identity	Yes	Yes
Möbius	//	Identity	No	No
Hawk	Smart Contract SMPC ZK SNARK	Identity Transaction	Yes	Yes
Privacy Pools	Smart Contract ZK SNARK	Identity Transaction	No	No
ZeroCoin	ZK Proof	Identity	No	Yes
ZeroCash	ZK SNARK	Identity	Yes	Yes
Miximus	Decent. mixing ZK Proof	Identity	No	No
MixEth	Decent. mixing Verifiable mixing	Identity Data	No	No

4 Contribution

In order to strengthen the protection of privacy in Blockchains, the mixing of coins can be an effective mean, especially if it is reinforced by other cryptographic means; our model is based on the creation of a mixing group, a group signature to perform mixing operations to improve the anonymity of users and the confidentiality of their transactions.

The following assumptions are made:

- A Blockchain network consisting of ten nodes.
- A bulletin board.
- A node wishing to perform mixing publishes a request for a mixing group on the bulletin board.

Our study was limited to processing one group creation request at a time.

The general idea is the proposition of a mixing model allowing a node of the Blockchain network to mix coins with other nodes of the network by forming a temporary mixing group that would ensure the anonymity of members and the confidentiality of transactions. Our model is based on:

- A mix request published on a bulletin board.
- An ephemeral group creation process.
- The generation of a final transaction.
- Verification of the validity of the final transaction by the members of the group.
- The execution of the final transaction. The recording of the transaction on the Blockchain.

4.1 How the model works

The operation of our model is detailed in the following steps:

Step1. Creation of the mixing group: A Node A in the Blockchain network posts a request, $ReqGr$, to create a coin mixing group on the bulletin board. This request includes the following fields:

- The old transaction address of node A .
- A nonce: $Nonce$.
- A minimum number of group members: $MinMember$, of type integer.
- A mix request.
- A time stamp T_A of A 's clock.
- A maximum delay for creating the group: D (Seconds).
- A number of turns authorized for the creation of the group: Tr of type integer.
- A signature $SIGN_A$.

The $ReqGr$ request is then broadcast by the bulletin board in the network. The network nodes, say $node_i$, wishing to participate in the coin mixing group, respond to the request, with $ReqRep$ response, containing the following fields:

- The address of the old transactions of the $node_i$.
- An instantaneous timestamp T_i of the $node_i$'s clock.
- The Nonce of $ReqGr$.
- A request for mixing.
- A signature $SIGN_i$.

At the end of the delay D , node A performs the following checks on the number of participants m :

- If $m > MinMember$ then the number of turns Tr is decremented and it continues to step 2.
- If $m < MinMember$ then, Tr is decremented and verified: if $Tr > 0$ then it tries again to create a group from step 1, otherwise the group is dissolved and the request dismissed.

Step2. Negotiating a mixing transaction: Node A of the group, formed in the previous step, generates output addresses $AdresSort_{A_i}$ to whom it wants to send amounts $amount_{A_i}$. Then chooses a number h randomly, such that: $1 \leq h \leq m$, and h random nodes of the group to send them h sub-requests $ReqMix_{A_h}$, which contain: $AdresSort_{A_i}$ and a division of the amounts $Amount_{A_i}$: $Amount_{A_h}$.

Upon receipt of a $ReqMix_{A_h}$ request by a node j among the h selected nodes, it evaluates whether it has enough coins to satisfy it. Here we distinguish three cases:

- Case 1: node j does not have any coins, so it relays the received request to another node in the group.
- Case 2: node j can satisfy the received request, so it responds with a satisfaction message $MessageSat_j$ which contains: the old transaction address of j , $AdresSort_{A_h}$, $Amount_{A_h}$, then broadcasts it in the group.
- Case 3: node j can only satisfy part of the request, so it responds with a partial satisfaction message $MessageSatPart_j$ which contains: the old transaction address, $AdresSort_{A_h}$, $Amount_j$. Then it generates a new request $ReqMix'_{A_h}$ which contains: $AdresSort_{A_i}$ and $Amount'_{A_h}$ such that: $Amount'_{A_h} = Amount_{A_i} - Amount_j$, which it sends to other members of the group to satisfy the amount missing.

All group members who responded with a satisfaction or partial satisfaction message updated their amounts.

Step3. Generation of the final transaction: Each node in the group assembles all the received messages and checks whether each output address can receive the appropriate amounts, i.e.: $AdresSort_{A_i}$ can receive at least $amount_{A_i}$. If this is the case, the final transaction $TransFinal$ is generated and broadcast to the group. It will

contain: all input addresses, all output addresses, the new coin division and the TransFinal hash. Otherwise, Tr is decremented and checks if Tr>0 then it tries again to create a group from step 1, otherwise the group is dissolved.

Step4. Signature of the final transaction: Each node of the group signs *TransFinal* and broadcasts the result in the group. If it is signed by all the members of the group then the transaction is valid and added to the Blockchain, if not, the transaction is cancelled and the group will be dissolved.

Step5. Adding transaction to the Blockchain: Only the node A which initiated the mixing adds the transaction to the Blockchain if it is signed.

4.2 Illustrative example

If Node A wants to perform a transaction with any member of the blockchain where he belongs, in order to hide their addresses and the details of the transaction (amount), Node A needs to mix his information with a certain number of other nodes who want also to perform transactions. The mixing process is simplified and explained in the following.

Let Node A wants to create a mixing group to mix coins such that: m=10. Node A generates three output addresses AdresSort_{Ai}: X, Y and Z, to which it wants to send 1, 2 and 3 coins respectively.

Node A randomly chooses a number h such that $1 \leq h \leq 10$, and h nodes of the group. Let h=4, and N1, N2, N3 and N4 the four nodes of the group.

Node A generates the following requests: ReqMix_{AN1}(X,1), ReqMix_{AN2}(Y,2), ReqMix_{AN3}(Z,1), and ReqMix_{AN4}(Z,2). Suppose nodes N1, N2, N3, and N4 respond respectively with the following messages:

- MessageSat_{N1}(hash(1),X,1),
- MessageSat_{N2}(hash(2),Y,2),
- MessageSatPart_{N3}(hash(3),Z,0.4) and
- MessageSat_{N4}(hash(4),Z,2).

Since node N3 has responded with a partial satisfaction message, then it generates another request ReqMix'_{AN3}(Z,0.6) which it sends to another node of the group, i.e. N5, which, in turn, responds to Z with a message MessageSat_{N5}(hash(5), Z, 0.6).

Each of the nodes N1, N2, N3, N4 and N5 updates their amounts, collects all the received messages and checks that the requests are satisfied, which is the

case in this example because X, Y and Z can receive the amounts requested by node A.

Only then can the final transaction be generated and broadcast to the group to be signed by all group members. At the end of this step the final transaction is validated and added by node A to the Blockchain.

4.3 Simulation results

A simulation program, using Python, has been implemented to measure the convergence rate (Conv_rate) of the protocol and the average mixing time (Mix_time) over a number of simulations runs. We consider this value over the maximum time obtained. For each simulation run, either a mixing group is found (mixing success and mix time) or not.

$$Conv_{rate} = \frac{\text{number of mixing success}}{\text{number of runs}}$$

$$Mix_{time} = \frac{\sum_{i=1}^{\text{number of mixing success}} \text{mix_time}_i}{\text{number of runs}}$$

The size of the blockchain (Block_size) and the numbers of turns Tr are fixed; the simulation is run for size=10 Tr=1, then size=100 TR=3 and finally size=1000 Tr=5. The requester node and the responders are generated randomly. The results are given in Table1.

Table 1. Simulation results

Block size	Mix time %	Conv rate %
10	0.30	0.51
100	0.58	0.62
1000	0.69	0.85

Mix time is bounded by D*Tr*m where D: delay, Tr: number of tries and m: number of participants (size of the mixing group). If the size of the blockchain is small (around 10) Tr may be initialized to 1. All the members are quickly reachable, and if no mixing group is found, it is futile to try again another turn! For greater blockchains, Tr=3 is sufficient to reach convergence.

4.4 Analysis

The fact that the final transaction is only generated after signature by all group members checks the following criteria:

- A decentralized mixing scheme without a trusted third party or mixing server.

- No mixing fees: as the mix is performed by the members of the group.
- User anonymity: even though the transaction is added by the requester node, it is performed by other members.
- Protection against theft: we suppose the members are trustworthy. But this criterion may be improved.
- Protection of transaction content: again other members perform the transaction and we suppose them trustful.

The solution works correctly for a small amount of coins, thus a small group ($m < 10$) and has been validated for this, but can be enlarged to a greater group and so be used in large blockchains. Small blockchains include private or permission blockchains, such as universities or companies; and large blockchains include public blockchains such as Bitcoin, Ethereum etc.

Mixing time is bounded and should not exceed the maximum time of messages propagation, but can be considered as a drawback because it also means that the mixing is not as complicated as it should be.

5 Conclusion

The objective here consists in the proposition of a model which can manage to improve the protection of private life in the Blockchain networks.

We proposed a coin mixing model with a temporary group creation phase which ensures the protection of the anonymity of users and transactions, this specific phase makes it possible to circumvent the need for a trusted third party as well as mixing fees. The model offers a wide scope for possible improvements in future work.

Theoretically, our model meets the expectations of privacy preserving; formal validation will be one of our future goals.

A practical study could shed light on some weaknesses, which would allow us to make the necessary adjustments in order to arrive at the ultimate goal, which is to achieve strong anonymity in Blockchain networks. These improvements can be:

- Limitation of the maximum number of group members to reduce complexity especially for small transactions.
- Choose the members of the group according to predefined parameters (level of confidence, reliability, etc.) by the requester of the mix.

- Define a criterion for stopping the sending of requests to avoid flooding the network in the event that the amount is never satisfied.
- Define a criterion for the choice of amounts to be accepted in case the requested amount is exceeded.
- Define a penalization system for members who do not sign the final transaction.

Finally, introducing artificial intelligence techniques in Blockchains is the new trendy approach either in security, data privacy or smart contracts. In our case using classifiers to detect and isolate malicious members or to choose members of the mixing group before starting any transaction would be a possible improvement.

Declaration of Generative AI and AI-assisted Technologies in the Writing Process

The authors wrote, reviewed and edited the content as needed and they have not utilised artificial intelligence (AI) tools. The authors take full responsibility for the content of the publication.

References:

- [1] S. Nakamoto, 'Bitcoin: A peer-to-peer electronic cash system', 2008, available at <https://bitcoin.org/bitcoin.pdf> (last access 14/02/2023)
- [2] A.D. Moore, Privacy, *Library Hi Tech*, Vol. 25, 2007, pp. 58-78.
- [3] B. Gerber, OECD Privacy Principles, 2010, available at <http://oecdprivacy.org/>, (last access 10/02/2023)
- [4] A. Belabed, A. La protection de la vie privée sur Internet, PhD thesis, University of Tlemcen, Algeria, 2018.
- [5] R.L. Rivest, A. Shamir, and Y. Tauman, How to Leak a Secret, in *Proc.ASICRYPT*. New York, NY, USA: Springer-Verlag, 2001, pp. 552-565.
- [6] D. Lavrenov, A Zero-Knowledge Proof: Improving Privacy on a Blockchain, 2019, available at <https://www.altoros.com/blog/zero-knowledge-proof-improving-privacy-for-a-blockchain/> (last access 14/02/2023)
- [7] X. Yan, Q. Wu and Y. Sun, A Homomorphic Encryption and Privacy Protection Method Based on Blockchain and Edge Computing. *Wirel. Commun. Mob. Comput.* Vol. 2020, No 8832341, 2020 <https://doi.org/10.1155/2020/8832341>

- [8] C. Zhao, S. Zhao, M. Zhao, Z. Chen, C. Z. Gao, H. Li and Y.A. Tan, Secure Multi-Party Computation: Theory, practice and applications. *Inf. Sci.* vol. 476, 2019, pp. 357-372.
- [9] S. Gambs, Réseaux de communication anonyme, 2015, available at https://www.irisa.fr/prive/sgambs/cours2_pvp.pdf, (last access 10/02/2023).
- [10] P. Syverson, R. Dingledine and N. Mathewson, Tor: The second generation onion router, *Researchgate*, 2004, available at https://www.researchgate.net/publication/2910678_Tor_The_Second-Generation_Onion_Router
- [11] G. Pillot, Anonymat et vie privée sur internet, Master report, University of Laval, Quebec, 2018, available at <https://corpus.ulaval.ca/server/api/core/bitstreams/b80b8e47-882b-402b-9ebb-e21440e1e0bd/content> (last access 10/02/2023).
- [12] Z. Bao, W. Shi, S. Kumari, Z.Y. Kong and C. M. Chen, Lockmix: a secure and privacy-preserving mix service for bitcoin anonymity, *Int. J. of Information Security*, 2019, pp. 1-11.
- [13] Q. Shentu and J. Yu, A Blind-Mixing Scheme for Bitcoin based on an Elliptic Curve Cryptography Blind Digital Signature Algorithm, 2015, available at <https://arxiv.org/ftp/arxiv/papers/1510/1510.05833.pdf> (last access 10/02/2023)
- [14] A. Belkhamisa and M. Yahiaoui, La protection de la vie privée dans le BigData, Master report, University of Bouira, Algeria, 2020.
- [15] R. Solomon and G. Almashaqbeh, SmartFHE: Privacy-Preserving Smart Contracts from Fully Homomorphic Encryption, *Cryptology ePrint Archive*, Paper 2021/133 <https://eprint.iacr.org/2021/133> (last access 10/02/2023).
- [16] Z. Wang, D. Zhao and J. Wang, A survey on privacy protection of Blockchain: The technology and application, *IEEE Access* 8, 2020, pp. 108766-108781.
- [17] N.Z. Aitzhan and D. Sveltinovic, Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams, *IEEE Transactions on Dependable and Secure Computing*, vol.15, no.5, 2016, pp. 840-852.
- [18] W. Shao, C. Jia, Y. Xu, K. Qiu, Y. Gao, and Y. He, Attrichain: Decentralized traceable anonymous identities in privacy-preserving permissioned blockchain, *Computers and Security*, vol. 99, 2020, pp. 102069
- [19] Z. Wang, S. Chaliasos, K. Qin, L. Zhou, L. Gao, P. Berrang, B. Livshits, and A. Gervais, On How Zero-Knowledge Proof Blockchain Mixers Improve, and Worsen User Privacy, in *Proc. of ACM Web Conference 2023 (WWW '23)*, 2023, pp. 2022-2032
- [20] I. Miers, C. Garman, M. Green and A.D. Rubin, Zerocoin: Anonymous Distributed E-Cash from Bitcoin, *IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, 2013, pp. 397-411, doi: 10.1109/SP.2013.34.
- [21] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer and M. Virza, Zerocash: Decentralized anonymous payments from Bitcoin, *IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, 2014, pp. 459-474, doi: 10.1109/SP.2014.36.
- [22] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts, *IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, 2016, pp. 839-858, doi: 10.1109/SP.2016.55.
- [23] V. Buterin, J. Illium, M. Nadler, F. Schar, A. Soleimani, Blockchain privacy and regulatory compliance: Towards a practical equilibrium, *Blockchain Research and Applications*, vol. 5, 2024, pp. 100176
- [24] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J.A. Kroll and E.W. Felten, Mixcoin: Anonymity for Bitcoin with Accountable Mixes, *Lecture Notes in Computer Science*, 2014, pp. 486-504.
- [25] L. Valanta, and B. Rowan, Blindcoin: blinded, accountable mixes for bitcoin, *Int. Conference on Financial Cryptography and Data Security*, Berlin, Heidelberg, 2015, pp. 112-126.
- [26] G. Maxwell, CoinJoin: Bitcoin privacy for the real world, 2013, available at <https://bitcointalk.org/index.php?topic=279249.0> (last access 08/02/2023).
- [27] T. Ruffing, P. Moreno-Sanchez and A. Kate, CoinShuffle: practical decentralized coin mixing for Bitcoin, *European Symposium on Research in Computer Security*, Springer, 2014, pp. 345-364.
- [28] H. Corrigan-Gibbs and B. Ford, Dissent: Accountable anonymous group messaging, *Proc. of the 17th Conference on Computer and Communications Security CCS'10*, USA, 2010, pp. 340-350.
- [29] T. Ruffing, P. Moreno-Sanchez and A. Kate, P2P mixing and unlinkable bitcoin transactions,

- NDSS, 2017, pp. 1-15, 2017, available at <https://eprint.iacr.org/2016/824.pdf>
- [30] G. Bissias, A.P. Ozisik, B.N. Levine and M. Liberatory, Sybil resistant mixing for Bitcoin, *ACM Workshop on Privacy in the Electronic Society Scottsdale, USA*, New York: ACM Press, 2015, pp 149-158.
- [31] S. Barber, X. Boyen, S. She and E. Uzun, Bitter to better-how to make bitcoin a better currency, in Proc. of *Int. Conference on financial cryptography and data security*, Springer, 2012, pp.399-414.
- [32] T. Ruffing and M.S. Pedro, Mixing Confidential Transactions: Comprehensive Transaction Privacy for Bitcoin, 2017, available at <https://eprint.iacr.org/2017/238>
- [33] G. Maxwell, Confidential Transactions, 2015, available at <https://elementsproject.org/features/confidential-transactions> (last access 10/02/2023).
- [34] P. Todd, [Bitcoin-development] Stealth addresses, 2014, available at <http://www.mailarchive.com/bitcoin-development@lists.sourceforge.net/msg03613.html>, (last access 10/02/2023).
- [35] S. Meiklejohn and R. Mercer, Möbius: Trustless tumbling for transaction privacy, Proc. on *Privacy Enhancing Technologies*, 2018, pp. 105-121.
- [36] B. Whitehat, Miximus, 2018, available at <https://github.com/barryWhiteHat/miximus> (last access 10/02/2023)
- [37] I.A. Seres, D.A. Nagy, P. Burcsi and C. Buckland, (2019) MixEth: efficient, trustless coin mixing service for Ethereum, in Proc. of *Tokenomics*, Paris, 2019, DOI:10.4230/OASICS.Tokenomics.2019.13
- [38] C.A. Neff, A verifiable secret shuffle and its application to e-voting, in Proc. of the *8th ACM conference on Computer and Communications Security*, 2001, pp. 116-125.
- [39] A. Arbabi, A. Shojaeinasab, B. Bahrak, and H. Najjaran, Mixing Solutions in Bitcoin and Ethereum ecosystems: A Review and Tutorial, arXiv:2310.04899v1 [cs.CR] 7 Oct 2023 26 pages.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution. The first author wrote the paper.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0

https://creativecommons.org/licenses/by/4.0/deed.en_US