MixEth: efficient trustless coin mixing service for Ethereum

István András Seres[1], Dániel A. Nagy[1], and Péter Burcsi[1]

[1]Department of Computer Algebra, Eötvös Loránd University

October 23, 2018

Note: this is an early-stage work-in-progress! Security proofs, implementation and many more are yet to come!

Abstract

Cryptocurrencies enable users to transact with each other without relying on trusted parties or intermediaries. These transactions are recorded in an immutable, publicly verifiable ledger. Due to this transparent nature of the ledger, privacy is notably reduced. If the link between users' public key and their physical identity is exposed their pseudonymity is lost. One way to increase users' privacy is to deploy coin mixing services. In this paper, we present MixEth, which is a trustless coin mixing service. MixEth is more efficient than any proposed trustless coin tumbler. It requires only 3 on-chain transactions at most per user and 1 off-chain. It achieves strong notions of anonymity and is able to resist denial-of-service attacks.

Keywords: Cryptography, Verifiable shuffle, Cryptocurrency, Ethereum, Coin mixer

1 Introduction

Bitcoin [14] and other cryptocurrencies are pseudonymous. Users' public keys are used as pseudonyms in these systems. Transactions essentially record a flow of cryptocurrency from one (or more) public keys to another public key (or more). Flow of cryptocurrency can be easily tracked due to the open and transparent nature of cryptocurrencies' transaction ledger. Moreover, coherent public keys, which are used by the same user, can be clustered merely by analyzing the ledger. Recently several tools and algorithms were proposed to diminish users' privacy ([11],[13], [12]). Such deanomyzation attacks are extremely harmful to user privacy, especially in the case when any of the users' pseudonyms, public keys, are linked to their real world identity.

One of the methods to increase users' privacy is coin mixing or tumbling. This technique provides *k-anonymity* or *plausible deniability*. The idea is that k users deposit 1 coin each and then in the course of a coin shuffling protocol either a centralized trusted third party or a smart contract mixes the coins and redistributes them to designated fresh public keys. This powerful technique gives users superior privacy and anonimity since their new received coins can not be linked to them.

Several coin mixing protocols were proposed in the literature both centralized ([5], [17], [8]) and decentralized ([9], [16], [1], [10], [4]). A major drawback of centralized coin mixing is that the availability of the tumbler is entirely dependent on the trusted party and in most cases theft prevention can not be guaranteed ([5], [17]). On the other hand decentralized tumblers achieve availability, theft prevention and satisfy strong notions of anonymity although they are considerably heavier computationally. In the following we will solely focus on the problem of coin mixing on Ethereum [18].

The two major techniques to provide mixing services for Ethereum are Möbius, a ring-signature-based solution [10] and Miximus, a zkSNARK-based proposal [1]. Both of them burn tremendous amounts of gas to withdraw funds, which could be prohibitive for many use cases. Möbius requires $335{,}714n$ gas (n is the ring size) while Miximus consumes 1,903,305 gas to verify a zkSNARK proof [2].

Our contributions. In this paper, we present MixEth, to overcome the above mentioned efficiency issues while retaining strong notions of anonymity already achieved by previous proposals. MixEth requires as few off-chain messages and on-chain transactions as Möbius and Miximus,

meanwhile it burns significantly less gas. Game-theoretical analysis of incentives in MixEth is also enclosed.

2 Background

2.1 Notations

In most cases if it is possible we will stick to the notations used in [10] for sake of uniformity. Let [] denote the empty tuple. For a tuple $t = (x_1, \ldots, x_n)$ we denote as $t[x_i]$ the value stored at x_i. The cardinality of a finite set X is denoted as $|X|$. In the following let $\lambda \in \mathbb{N}$ be the security parameter and its unary representation is 1^λ. If x is uniformly randomly sampled from a set A we write $x \xleftarrow{\$} A$. The symmetric group of degree n is written as S_n. In a cyclic group $\mathbb{G}$, the standardized generator is denoted as G and we use the additive notation. Secret keys and public keys are denoted as sk and pk respectively (or often times s and sG), while the user the corresponding key belongs to is indicated in subscript. Let PK_i denote the set of public keys belonging to receivers at a particular shuffling round i.

We use games in definitions and proofs of security. At the end of each game, the main procedure of game G outputs a single bit. $\Pr(\mathsf{G})$ denotes the probability that the output is 1.

2.2 Cryptographic keys in Ethereum

Ethereum uses Elliptic Curve Cryptography (ECC) to secure users' funds. More specifically, it uses the secp256k1 curve, the same one as used in Bitcoin. If a user wants to create an Ethereum address, first she needs to generate a secret key $s \xleftarrow{\$} \mathbb{Z}_n$, where n is the order of secp256k1 over a finite field $\mathbb{F}_p$. The corresponding public key will be sG. Note that any multiples of G is also a generator of curve points since n, the order of the group is also a prime. Accounts in Ethereum are identified by their addresses which can be obtained by taking the right most 20 bytes of the Keccak hashed public key [18].

2.3 Verifiable shuffle

Neff introduced the notion of verifiable shuffle [15]. It is a cryptographic protocol allowing a party to verifiably shuffle a sequence of k modular integers. The output of the shuffle is another k modular integers raised to the same secret exponent only known to the shuffler. The shuffler can generate a publicly verifiable zero-knowledge proof to convince the public that the shuffle was done correctly.

Neff's mathematical construct is extremely powerful, since it only relies on the intractability of the Decisional Diffie-Hellman (DDH) problem. Therefore, Neff's verifiable shuffle can also be applied in groups over elliptic curves.

Verifiable shuffle can be used to shuffle a set of public keys, $PK = (s_1G, s_2G \ldots, s_kG)$. Note that secret keys are not known to the shuffler.

1. Shuffler commits to $C = cG$, publishes

$$PK^* = (c(s_{\pi^{-1}(1)}G), c(s_{\pi^{-1}(2)}G), \ldots, c(s_{\pi^{-1}(k)}G))$$

   where π is a random permutation. Shuffler additionally computes and publishes a zero-knowledge proof about the correctness of the shuffle. This proof can be made non-interactive via the Fiat-Shamir heuristic. Let us call C as the shuffling constant.

2. Assuming the proof verifies users gain new public keys with respect to another generator element, namely cG.

For verifying the proof one needs to compute $8k + 5$ exponentiations, however later this result was ameliorated to $3,5k$ exponentiations by Bayer and Groth [3].

So far verifiable shuffles were only applied in voting schemes, we argue that they are useful in trustless coin mixers as well.

2.4 Chaum-Pedersen protocol

The language $\mathcal{L}_{DDH}$ is defined to be the set of all tuples (G, aG, bG, abG) where $G \in \mathbb{G}$ is of order prime q. The Chaum-Pedersen protocol enables a prover $\mathcal{P}$ to prove to a verifier $\mathcal{V}$ that $(G, A, B, C) \in \mathcal{L}_{DDH}$ in zero-knowledge for groups of prime order [7]. The protocol is organized as follows:

1. $\mathcal{V}$: $s \xleftarrow{\$} \mathbb{Z}_q$, then sends $commit(s)$
2. $\mathcal{P}$: $r \xleftarrow{\$} \mathbb{Z}_q$, then sends $y_1 = rG$, $y_2 = rB$.
3. $\mathcal{V}$ opens commitment by sending s
4. $\mathcal{P}$ sends $z = r + as \pmod q$
5. $\mathcal{V}$ checks $zG = y_1 + sA \pmod q \wedge zB = y_2 + sC \pmod q$

Note that in the following a non-interactive version of this protocol will only be considered that can be achieved by applying the Fiat-Shamir heuristic.

2.5 Ethereum

2.6 Ethereum account abstraction

Unfortunately, neither Möbius nor Miximus can be deployed on the present-day Ethereum. When users of the coin mixing contract, either Möbius or Miximus would like to withdraw their funds they can not do this from a fresh address, since it does not hold any ether. Since as of now only the sender of a transaction can pay for the gas fee, users can not withdraw their funds unless they ask someone to fund their fresh address.

Another solution for this problem is the Ethereum Improvement Proposal (EIP) 86 suggested by Nick Johnson and Vitalik Buterin [6]. EIP86 permits receivers of a transaction paying the gas fee. This would certainly enable a functional Möbius and Miximus as well, since the tumbling contract could pay for the withdrawal transactions' gas fee, eliminating the previous workaround to unlinkably fund freshly mixed addresses. Additionally, EIP86 also allows contracts and accounts to define their own digital signature algorithms. This means that users are no longer required to sign transactions with Elliptic Curve Digital Signature Algorithm (ECDSA). Moreover if EIP86 or something similar is implemented, which is expected in 2019, MixEth is also made viable.

3 Threat model

3.1 Participants and interactions

In a decentralized tumbler, we have 3 distinct entities: the tumbling smart contract, a set of senders and a set of receivers. A sender, whom we will call Alice, sends funds to the receiver, Bob, through the mixer contract in order to break direct links between their public keys. Interactions of these entities can be summarized as follows:

$tx \xleftarrow{\$} Deposit(sk_A, pk_B)$: The sender runs this algorithm to deposit some ether to the receiver's public key.

After some period of time no more deposits are allowed to the tumbling contract. Let PK_0 denote the set of public keys after the depositing period to be mixed. Every recipient of the mix is allowed to shuffle the public keys at most once:

$PK_{i+1}, C^*_{i+1} \xleftarrow{\$} Shuffle(PK_i, C^*_i, c_i, \pi_i)$. Let us call C^* as the shuffling accumulated constant, which can be obtained by $C^*_{i+1} = c_i C^*_i$. The shuffling accumulated constant is needed for receivers to audit shuffling and to collect their funds at the end of the final shuffling period. The permutation π and the secret multiplier c_i from the new shuffling accumulated constant should be kept private after shuffling, otherwise it is trivial to track how public keys are shuffled. All the outputs of the $Shuffle$ algorithm are public and written into the tumbling contract.

$0 \vee 1 \leftarrow ChallengeShuffle(PK_i, C^*_i, PK_{i-1}, C^*_{i-1}, pk_B)$: receiver B with public key $pk_B = s_B G$ can challenge an incorrect shuffle at the ith round by giving two Chaum-Pedersen zero-knowledge proofs that the following two tuples are DDH-tuples: $(G, s_B G, C^*_{i-1}, s_B C^*_{i-1})$ and

$(G, s_B G, C^*_{i-1}, s_B C^*_i)$. If both of the proofs are verified and $s_B C^*_i \notin PK_i$, while $s_B C^*_{i-1} \in PK_{i-1}$, then the challenge is accepted, otherwise rejected. These proofs and checks allow one to check that indeed the ith round is the first round in which the corresponding public key to s_B is shuffled incorrectly.

$tx \xleftarrow{\$} Withdraw(sk_B)$: after the end of the shuffling period users are allowed to withdraw their funds. Note that here withdraw transactions will be signed with a modified version of ECDSA, where not the original generator element G is used as generator rather the final shuffling accumulated constant.

3.2 Security goals

We are aiming to achieve and prove the same notions of security as the ones defined in [10]. We are going to assume that at most $k-2$ recipients are malicious (k is the number of recipients). Otherwise, no meaningful notion of security can be achieved. Furthermore presume that participants are on-line during the entire course of mixing in order to be able to monitor and potentially challenge any incorrect shuffle. Finally we assume that honest recipients will always exercise their rights to shuffle and they do not disclose any private information used in their shuffles.

In this early version of the MixEth paper we only restrict ourselves to give informal security definitions.

3.2.1 Anonymity

Sender anonymity is achieved if an adversary can not determine to whom honest miners are sending funds, assuming that honest senders' deposits are indistinguishable.

Recipient anonymity is achieved if honest recipients withdrawal transactions are indistinguishable.

3.2.2 Availability

It is essential for a coin mixer to provide availability, meaning that honest recipients can always withdraw their money from the mixer.

3.2.3 Theft prevention

We would like to ensure that neither coins can be withdrawn twice, nor withdrawn by anyone other but the intended recipient.

4 MixEth

4.1 Overview

MixEth is a coin mixing smart contract allowing parties to efficiently tumble coins in a trustless manner on Ethereum.

4.2 Initializing the tumbler

A MixEth contract living on the Ethereum blockchain at $id_{contract}$ address must be initialized with the following parameters:

- amt: denomination of ether to be mixed;
- $senders[]$: list of all the sender addresses;
- $initPubKeys[]$: list of all the recipients' public keys;
- $shuffles[][]$: list of all the shuffles with corresponding shuffling accumulated constants.
- $withdrawn[]$: list of all the shuffled public keys who had already withdrawn their coins.

4.3 Depositing period

Every sender must deposit exactly *amt* ether to a specific public key. Deposits with incorrect ether value are rejected.

4.4 Shuffling period

After the depositing round, shuffling and challenging rounds are coming after in turns. Each shuffling round is followed by a challenging round when the correctness of the preceding shuffle can be challenged by anyone. If a challenge is accepted, then shuffler's deposit is lost, her shuffle is discarded and shuffling continues from the set of public keys prior to the discarded shuffle. In the course of a shuffle an honest shuffler should raise all the public keys to a secret exponent c and then permute all the transformed public keys. Honest shuffler commits to c by sending back to MixEth the new shuffling accumulated constant and the shuffled public keys.

Shuffle is done off-chain, however the result and the updated shuffling accumulated constant is loaded into the MixEth contract enabling anyone to verify the shuffle's correctness and to continue public key shuffling after the corresponding challenging round.

Procedure 1 Off-chain public key shuffling algorithm for the ith shuffling round

$PK_i \leftarrow []$
$c \xleftarrow{\$} \mathbb{Z}_n$
$C^*_{i-1} \leftarrow read\ from\ MixEth\ contract$
$PK_{i-1} \leftarrow read\ from\ MixEth\ contract\ the\ current\ sequence\ of\ shuffled\ public\ keys$
$\pi \xleftarrow{\$} S_{|PK_{i-1}|}$
for $j = 0; j < |PK_{i-1}|; j++$ **do**
    $PK_i[\pi(j)] = c * PK_{i-1}[j]$
$C^*_i = cC^*_{i-1}$
Output: (PK_i, C^*_i)

4.5 Challenging period

Every participant should check the correctness of incoming shuffles, therefore sufficient time should be provided for each challenging round. These are the actions Bob as a receiver needs to perform to check the correctness of the shuffle at ith round if Bob has secret key s_B. In this case Bob should check whether $s_BC^*_i \in PK_i$ or not. If not, Bob should prove to MixEth that the ith round is indeed the first round, where the shuffled public key corresponding to s_B is compromised. The first Chaum-Pedersen ensures that the integrity of the shuffled public key in round $i-1$st is intact, while the second proves that it is compromised in round ith.

Procedure 2 On-chain verification algorithm of incoming shuffle challenges

Input$(PK_i, PK_{i-1}, proof_{DDH}(G, s_BG, C^*_{i-1}, s_BC^*_{i-1}), proof_{DDH}(G, s_BG, C^*_i, s_BC^*_i)$

$b \leftarrow verifyChaumPedersen(proof_{DDH}(G, s_BG, C^*_{i-1}, s_BC^*_{i-1})$
$b' \leftarrow verifyChaumPedersen(proof_{DDH}(G, s_BG, C^*_i, s_BC^*_i)$
$b^* \leftarrow 0$
if $b \wedge b' \wedge s_BC^*_{i-1} \in PK_{i-1} \wedge s_BC^*_i \notin PK_i$ **then**
    $b^* \leftarrow 1$
else
    $b^* \leftarrow 0$
Output: b^*

Note that every recipient should perform this check after each shuffling. Noone can check the inclusion and correctness of shuffled public keys for recipients other than themselves. This task is non-outsourcable unless one reveals her own private key, which would obviously lead to loss of funds at the end of the MixEth protocol, since anyone can claim the funds knowing the corresponding secret key.

We also highlight the necessity of two Chaum-Pedersen proofs for challenging a shuffle. If only one Chaum-Pedersen proof is enclosed in the challenging transaction, MixEth can not be sure that the integrity of the problematic public key indeed in the ith shuffling round was compromised. This could be abused by a malicious shuffler who deliberately corrupts their own public key in their shuffling round and afterwards they could blame any other shuffler for the compromise. This could have been led to losses of honest recipients' deposit.

4.6 Withdrawing

Let C^* be the final shuffling accumulated constant. For a recipient B, whose public key $s_B G \in initPubKeys[]$, in the final shuffle there will be $s_B C^*$. The recipient can prove to MixEth that she knows secret key s_B by using a modified ECDSA, which uses C^* as the generator element instead of the standardized G.

4.7 MixEth pseudocode

```
contract MixEth {
  uint256 amt;
  address[] senders;
  CurvePoint[] initPubKeys;
  Shuffle[] Shuffles;

  struct CurvePoint {
    uint256 x; //x coordinate
    uint256 y; //y coordinate
  }
  struct Shuffle {
    //describes a shuffle
    // contains the shuffled pubKeys and the shuffling accumulated constant
  }

  constructor() public {
   //sets amt
  }

  function uploadShuffle(Shuffle newShuffle) public {
    //needs to be ensured that recipient has not shuffled yet
    Shuffles.append(newShuffle);
  }

  function challengeShuffle(CurvePoint[] challenge, uint256 i) public {
    bool accepted;
    //contract checks the correctness of the i-th shuffle which is stored at
        Shuffles[i]. If challenge accepted malicious shuffler's deposit is slashed.
    return accepted;
  }

  function withdraw() public {
    //receivers can withdraw funds at most once
  }
}
```

Figure 1: MixEth contract pseudocode

5 Security

This section is going to demonstrate security proofs for the notions of security introduced in Section 3.2.

In this early version of the MixEth paper, we only restrict ourselves to give intuition and informal proofs for certain security properties.

5.1 Recipient anonymity

The withdrawing transaction for recipient B sends funds to the public key $s_B C^*$. This public key does not reveal any links to the original $s_B G$ in case if at least one honest sender shuffled and

the DDH assumption holds. Adversary can only distinguish between honest recipients public keys with negligible probability.

5.2 Availability

If an adversary is able to destroy an honest recipient's funds' availability, it implies that adversary either breaks the soundness of the Chaum-Pedersen protocol or successfully launched an eclipse attack against the honest recipient, who can not send any transactions to the Ethereum transaction ledger.

5.3 Theft prevention

If an adversary is able to steal funds from other users than it would imply that they broke discrete logarithm problem on the secp256k1 curve.

Table 1: Security properties achieved by each coin mixing protocol.

	Anonimity against			Availability		Theft prevention
	outsiders	senders	recipients	sender	tumbler	
Centralized						
Mixcoin [5]	TTP	✗	✓	✓	✗	TTP
Blindcoin [17]	✓	✗	✓	✓	✗	TTP
TumbleBit [8]	✓	✓	✓	✓	✗	✓
Decentralized						
Coinjoin [9]	✓	✗	✓	✗	n.a.	✓
Coinshuffle [16]	✓	✗	✓	✗	n.a.	✓
XIM [4]	✓	✗	✓	✓	n.a.	✓
Möbius [10]	✓	✓	✗	✓	✓	✓
Miximus [1]	✓	✓	✗	✓	✓	✓
MixEth	✓	✓	✗	✓	✓	✓

6 Implementation

7 Related work

As Table 2 demonstrates, both Möbius and Miximus require 2 on-chain transactions, while MixEth requires 3. In spite of this seemingly added complexity, we are confident that these 3 (deposit, shuffle, withdraw) transactions consume significantly less gas than those (deposit, verify linkable ring signature/zkSNARK) of Möbius and Miximus.

Table 2: Number of on-chain transactions and off-chain messages required to run a certain coin mixer protocol.

	#Off-chain messages	#Transactions
Centralized		
Mixcoin [5]	2	2
Blindcoin [17]	4	2
TumbleBit [8]	12	4
Decentralized		
Coinjoin [9]	$\mathcal{O}(n^2)$	1
Coinshuffle [16]	$\mathcal{O}(n)$	1
XIM [4]	0	7
Möbius [10]	2	2
Miximus [1]	1	2
MixEth	1	3

8 Extensions and improvements

MixEth is not fully compatible with the current EVM, however it could be deployed with a workaround. A recipient could ask another party or service to send a signed transaction including a signature which uses the modified version of ECDSA, where the generator element is the shuffling accumulated constant. MixEth could check this signature and send out funds to a fresh Ethereum address given in the withdraw transaction.

9 Conclusion

10 Future work

We are going to implement and deploy MixEth on Ethereum and evaluate its performance. We are also going to give formal security proofs for the claimed security properties. An important and crucial research question is whether it is possible to design and implement an efficient and trustless Ethereum-based coin mixer with strong security guarantees which do not rely on any workaround and upcoming EIP implementation and is ready to be deployed on present-day Ethereum.

References

[1] barryWhiteHat. Miximus. https://github.com/barryWhiteHat/miximus, 2018.

[2] barryWhiteHat. Miximus gas costs. https://www.reddit.com/r/ethereum/comments/8ss53z/miximus_zksnark_based_anonymous_transactions_is/, 2018.

[3] Stephanie Bayer and Jens Groth. Efficient zero-knowledge argument for correctness of a shuffle. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 263–280. Springer, 2012.

[4] George Bissias, A Pinar Ozisik, Brian N Levine, and Marc Liberatore. Sybil-resistant mixing for bitcoin. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, pages 149–158. ACM, 2014.

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

[6] Vitalik Buterin and Nick Johnson. Eip86: Account abstraction. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-86.md, 2017.

[7] David Chaum and Torben Pryds Pedersen. Wallet databases with observers. In *Annual International Cryptology Conference*, pages 89–105. Springer, 1992.

[8] Ethan Heilman, Leen Alshenibr, Foteini Baldimtsi, Alessandra Scafuro, and Sharon Goldberg. Tumblebit: An untrusted bitcoin-compatible anonymous payment hub. In *Network and Distributed System Security Symposium*, 2017.

[9] Greg Maxwell. Coinjoin: Bitcoin privacy for the real world. In *Post on Bitcoin forum*, 2013.

[10] Sarah Meiklejohn and Rebekah Mercer. Möbius: Trustless tumbling for transaction privacy. *Proceedings on Privacy Enhancing Technologies*, 2018(2):105–121, 2018.

[11] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 127–140. ACM, 2013.

[12] Pedro Moreno-Sanchez, Muhammad Bilal Zafar, and Aniket Kate. Listening to whispers of ripple: Linking wallets and deanonymizing transactions in the ripple network. *Proceedings on Privacy Enhancing Technologies*, 2016(4):436–453, 2016.

[13] Malte Moser, Rainer Bohme, and Dominic Breuker. An inquiry into money laundering tools in the bitcoin ecosystem. In *eCrime Researchers Summit (eCRS), 2013*, pages 1–14. IEEE, 2013.

[14] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[15] C Andrew Neff. A verifiable secret shuffle and its application to e-voting. In *Proceedings of the 8th ACM conference on Computer and Communications Security*, pages 116–125. ACM, 2001.

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

[17] Luke Valenta and Brendan Rowan. Blindcoin: Blinded, accountable mixes for bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 112–126. Springer, 2015.

[18] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151:1–32, 2014.