Poster: Mixing Confidential Transactions: Comprehensive Transaction Privacy for Bitcoin*

Tim Ruffing
Saarland University
tim.ruffing@mmci.uni-saarland.de

Pedro Moreno-Sanchez
Purdue University
pmorenos@purdue.edu

***Abstract*—The public nature of the blockchain has been shown to be a severe threat for the privacy of Bitcoin users. Even worse, since funds can be tracked and tainted, no two coins are equal, and fungibility, a fundamental property required in every currency, is at risk. With these threats in mind, several privacy-enhancing technologies have been proposed to make Bitcoin more private. However, they either require a deep redesign of the currency, breaking many currently deployed features, or they address only specific privacy issues and consequently provide only very limited guarantees when deployed separately.**

The goal of this work is to overcome this trade-off. Building on CoinJoin, we design ValueShuffle, the first coin mixing protocol compatible with Confidential Transactions, a proposal to hide payment values in transactions. ValueShuffle ensures a mixing participant's anonymity and the confidentiality of her payment values not only against an attacker observing the blockchain but also against the other possibly malicious mixing participants and against network attackers. By combining ValueShuffle with the proposal for Confidential Transactions and additionally Stealth Addresses, our solution provides *comprehensive privacy* (payer anonymity, payee anonymity, and payment value privacy) without breaking with the design or the features of Bitcoin. We demonstrate that the combination of these three privacy-enhancing technologies creates synergies that overcome the two major obstacles which so far have prohibited the deployment of coin mixing in practice, namely that users need to mix funds of the same value, and need to do so before they can actually spend the funds. As a result, our approach unleashes the full potential of coin mixing as a privacy solution for Bitcoin.

I. Introduction

In Bitcoin's initial design, privacy plays only a minor role. The initial perception of Bitcoin providing some built-in anonymity has been refuted by a vast set of academic works by showing many different privacy weaknesses with the current Bitcoin protocol. This state of affairs has led to a plethora of privacy-enhancing technologies aiming at overcoming these shortcomings while not breaking with the fundamental design of the Bitcoin system [3].

Yet, current available proposals and deployments offer only partial solutions, focusing typically just on one aspect of privacy. First, Confidential Transactions (CT) [7] is a proposal for a transaction format that hides the payment value. Second, Stealth Addresses (SA) [11] defines a mechanism for payers to generate unique one-time addresses, which improves payee anonymity. Finally, coin mixing is the most prevalent approach to ensure payer anonymity while keeping compatibility with Bitcoin. In fact, Bitcoin supports CoinJoin [6] transactions, which enables the users to atomically transfer their money from potentially tainted inputs to fresh untainted output addresses. Additionally, if users exchange their output accounts by means of an anonymous broadcast protocol [4], [9], [10], inputs cannot be linked to outputs even by malicious users in the mixing, and such malicious users cannot prevent the honest users from successfully completing the protocol.

A. Challenges

It is highly desirable to combine all these privacy-enhancing technologies but this approach poses several challenges.

First, current P2P coin mixing protocols [9] suffer from the problem that users are required to mix their funds (in a CoinJoin transaction) by sending them to a fresh address of their own first, which removes the trace to the owner. Only afterwards users can spend the now mixed funds to a recipient (in a normal transaction). This two-step process renders mixing expensive for users, who pay additional fees and need to wait longer, and for the entire Bitcoin network, which has to process the additional CoinJoin transactions. Trustless centralized mixing solutions share this limitation [5]. As a result, privacy comes with an large expense. This is highly undesirable and creates a conflict between privacy and efficiency.

Second, all forms of coin mixing are traditionally heavily restricted to mixing funds of the same amount, because otherwise it is trivial for an observer to link inputs and outputs together just based on their monetary amount, no matter how the mixing is organized. Adding value privacy to coin mixing, e.g., by means of CT, removes this restriction entirely but comes with a challenge. While CT is compatible with CoinJoin at first glance, the design of CT assumes that a transaction is created by just a single user, who proves to the network that no money is created by performing the transaction. In P2P coin mixing, however, it is a group of *mutually distrusting* users who jointly must create a CoinJoin transaction.

This leads to the following question: *Can we design a P2P mixing protocol that enables a group of mutually distrusting users to create a confidential CoinJoin transaction without revealing the relation between inputs and outputs or their payment values to each other?*

* This work has been accepted for publication at the 4th Workshop on Bitcoin and Blockchain Research (BITCOIN'17). A full draft is available at https://people.mmci.uni-saarland.de/~truffing/papers/valueshuffle.pdf.

II. Our Approach: Mixing Confidential Transactions

We answer this question affirmatively. We design ValueShuffle, the first coin mixing protocol compatible with CT. ValueShuffle is an extension of CoinShuffle++ [9], the most efficient P2P coin mixing protocol in the literature, which is based on the DiceMix paradigm [9].

A. Core Features of ValueShuffle

Comprehensive Privacy. Since ValueShuffle successfully combines coin mixing, SA and CT, the resulting currency provides comprehensive privacy, i.e., unlinkability, payee anonymity and value privacy. In particular, ValueShuffle ensures that no attacker observing the blockchain or the network, or even participating in the protocol, can link inputs and outputs of the CoinJoin transaction created in an execution of ValueShuffle. That implies that given an output of this transaction, the payer's input address cannot be identified among the honest input addresses in the mixing (payer anonymity). Additionally, SA provides one-time addresses for receiving payments preventing linkage to known addresses (payee anonymity), and CT provides value privacy.

Single Transaction. ValueShuffle can be used to pay recipients directly without any form of premixing required by current P2P coin mixing solutions, and without requiring interaction with the recipient. As a result, private payments can be performed with just one single transaction on the blockchain.

DoS Resistance. ValueShuffle succeeds in the presence of denial-of-service attacks by disruptive users aiming to prevent honest users from completing the mixing. While disruptive users can delay the protocol, they cannot stop it. Since ValueShuffle is based on the efficient DiceMix protocol, it terminates in only $4 + 2f$ communication rounds in the presence of f disruptive users. That is, an undisrupted run of ValueShuffle completes in four communication rounds.

No Anonymous Channel Required. For providing unlinkability of inputs and outputs in a CoinJoin transaction, ValueShuffle does not rely on any external anonymous channel such as the Tor network. (However, to avoid that an observer is able to link inputs of the CoinJoin transaction with network-level identifiers such as IP addresses, using an external means of anonymous communication is highly recommended.)

B. Features Inherited from CoinJoin

Since ValueShuffle is based on the CoinJoin paradigm, it additionally inherits all of its practical advantages.

Theft Resistance. Since honest users will check the final CoinJoin transaction before signing it, no money can be stolen from them.

Script Compatibility. While ValueShuffle does not keep the scripts confidential, it is compatible with transactions outputs that use complex scripts, e.g., advanced smart contracts, and provides meaningful privacy guarantees for them.

Reduced Fees and Space Requirements. Unlike ring signatures as for instance deployed in Monero [8] that require to add a signature with size proportional to the anonymity set, our approach—while requiring interaction between users—provides anonymity without putting an additional burden in terms of blockchain space or verification time on the Bitcoin network. Taking this one step further, CoinJoin makes Bitcoin in fact more efficient assuming the availability of Schnorr signatures, which are planned to be deployed by Bitcoin Core in the future [2]. The introduction of Schnorr signatures will enable aggregate signatures using a interactive two-round protocol among the users in a CoinJoin transaction [12]. This protocol can easily be integrated in ValueShuffle, and since we can exploit parallelism, the resulting protocol will have the same number of rounds as the non-interactive variant $(4f + 2)$. This enhancement greatly reduces the size of transactions, thereby providing large saving in terms of blockchain space and verification time compared to individual transactions, and hence also reduces fees compared to individual transactions.

Incentive for Privacy. Due to the reduced fees, users save money by performing privacy-preserving transactions. This provides an unprecedented incentive for deployment and usage of privacy-enhancing technologies in Bitcoin.

Compatibility with Pruning. Unlike in Zerocash [1] or in Monero [8], using CoinJoin it can be publicly observed which transaction outputs are unspent. While this releases some information to the public, it allows to prune spent outputs from the set of (potentially) unspent transaction outputs. This helps to mitigate the scaling problems in Bitcoin.

Overlay Design. The unlinkability provided by ValueShuffle through the use of CoinJoin is built as a separate layer on top of Bitcoin, which avoids additional complexity and risk in the underlying Bitcoin protocol.

References

[1] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from Bitcoin," in *S&P'14*.

[2] Bitcoin Core, "Segregated witness: the next steps," https://bitcoincore.org/en/2016/06/24/segwit-next-steps/#schnorr-signatures.

[3] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies," in *S&P'15*.

[4] H. Corrigan-Gibbs and B. Ford, "Dissent: Accountable anonymous group messaging," in *CCS'10*.

[5] E. Heilman, F. Baldimtsi, L. Alshenibr, A. Scafuro, and S. Goldberg, "TumbleBit: An untrusted tumbler for Bitcoin-compatible anonymous payments."

[6] G. Maxwell, "CoinJoin: Bitcoin privacy for the real world," Post on Bitcoin forum, 2013, https://bitcointalk.org/index.php?topic=279249.

[7] ——, "Confidential transactions," 2015, https://people.xiph.org/~greg/confidential_values.txt.

[8] S. Noether and A. Mackenzie, "Ring confidential transactions," *Ledger*, vol. 1, 2016.

[9] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "P2P Mixing and Unlinkable Bitcoin Transactions," in *NDSS'17*.

[10] ——, "CoinShuffle: Practical decentralized coin mixing for Bitcoin," in *ESORICS'14*, 2014.

[11] P. Todd, "Stealth addresses," Post on Bitcoin development mailing list, https://www.mail-archive.com/bitcoin-development@lists.sourceforge.net/msg03613.html.

[12] P. Wuille, *Schnorr-SHA256 module*, Documentation for Bitcoin Core, 2016, https://github.com/sipa/secp256k1/blob/968e2f415a5e764d159ee03e95815ea11460854e/src/modules/schnorr/schnorr.md.