Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 2145

A survey on approaches to anonymity in Bitcoin and other cryptocurrencies

Felix Konstantin Maurer[1]

Abstract: Bitcoin is a crypto currency with several advantages over previous approaches. Transactions are confirmed and stored by a peer-to-peer network in a blockchain. Therefore, all transactions are public and soon solutions where designed to increase privacy in Bitcoin Many come with downsides, like requiring a trusted third-party or requiring modifications to Bitcoin. In this paper, we compare these approaches according to several criteria. Based on our findings, CoinJoin emerges as the best approach for anonymizing Bitcoins today.

Keywords: Bitcoin, cryptocurrencies, coin mixing, anonymity, transaction linkability

1 Introduction

Bitcoin [Na08] is a new cryptocurrency with several advantages over previous approaches. A peer-to-peer network is used to confirm the validity of transactions. However, the network stores all valid transactions which are therefore always public. Even though Bitcoin uses pseudonyms, it does not provide anonymity. Each transaction is linked to previous transactions and thus only one pseudonym must be known to infer other pseudonyms.

Consequently, employers paying in bitcoins might be able to track your spending and stores, landlords or anyone receiving payments could be able to know your balance. In currently used monetary systems this is not possible. Therefore, anonymity is going to be an requirement for any crypto currency in the future that tries to replace existing systems.

For Bitcoin, there already exist services that allow performing transactions through a third party. These are called mixers as they try to conceal a transaction in a large amount of unrelated transactions. Depending on the design, several problems can arise. For example, the mixing service might learn which addresses are connected. Therefore, other concepts were developed, even new cryptocurrencies which provide more privacy than Bitcoin.

2 Related Work

In Bitcoin, transactions are confirmed and preserved by being inserted into a chain of transaction blocks. As part of the chain they can not be modified, as the blocks are linked to their precursor by embedding its cryptographic hash. This block chain forms the public ledger of the Bitcoin network and represents the consensus about all performed transactions. Each transaction can consists of many inputs and outputs. An output is an amount

[1] Karlsruhe Institute for Technology, Institute of Telematics, felix.maurer@student.kit.edu

of bitcoins and a small program, called output script, that is used to verify if a person can spent the coins. Each input references an output and provides the input for the script. Usually, the output script verifies that the input was created with a specific private key.

Regal Reid and Martin Harrigan [RH13] are able to demonstrate that multiple pseudonymous addresses can be linked to a single user. They construct an graph of Bitcoin transactions (T) and a graph of Bitcoin addresses (U). Assuming that all inputs of a transaction belong to the same user, they then contract the graph nodes of U by merging addresses that appear in the inputs of a single transaction. Furthermore, they include temporal and and external information to link more addresses to real identities.

Florian Tschorsch and Björn Scheuermann [BdL13] extensively discuss Bitcoin. They provide a section on enabling privacy where they present several approaches, also discussed in our work. However, they do not compare them or provide recommendations.

Bonneau et al. [Bo15] also cover various aspects of Bitcoin. They discuss privacy and anonymity in a short section including a comparative table. The approaches are divided into peer-to-peer mixing protocols, distributed mix networks and altcoins. As the first survey, the do not draw conclusions from their comparison.

3 Taxonomy

In this paper, we assume an honest but curious adversary. It could be for example a credit institute, that wants to learn about the spending habits of its clients, or a landlord that would like to know whether her tenant is financially stable. The adversary will conduct transactions with the user and therefore knows at least one of her pseudonyms addresses. To protect the privacy of the user, public information of the cryptocurrency should not allow the adversary to infer other pseudonyms or transactions of the user. We assume that he or she will not try to gain additional information that is not part of the blockchain.

We compare existing work based on several criteria. Most important to us is *Bitcoin compatibility* meaning whether the Bitcoin protocol would have to be modified or not. Right now, Bitcoin is the largest crypto currency[1] by value and transaction volume and is actively developed and well understood. Therefore, it is likely that Bitcoin remains the dominant cryptocurrency and an incompatible mixing approach might not be adopted. The approach should make *theft impossible* as loss of reputation might be acceptable for a mix as long as it gains enough Bitcoins. Different protocols use different *architectures* for mixing coins. Like Bonneau et al. [Bo15], we will distinguish between peer-to-peer mixing protocols, mixing services and altcoins. Furthermore, most approaches need more than a *single transaction* to anonymously send an arbitrary amount of Bitcoins. This increases the time it takes to complete the mix, the amount of transaction fees payed and the energy needed by the network. In cases of peer-to-peer mixing protocols or services, *anonymity against the mixer* will be compared. We also distinguish whether it is *reliant on new cryptographic methods* not used in Bitcoin as it might lessen the confidence in the solution.

[1] `https://coinmarketcap.com/`

4 Survey

As we can not cover all existing approaches, we chose relevant and representative ones.

4.1 Mixcoin and Blindcoin

Mixcoin [Bo14] is a mixing service with accountability features. Bitcoin users negotiate a set of parameters with the service, including the address where the coins should be sent to. To provide anonymity, all users must use the same amount when mixing and multiple users must use the service at the same time. The service will provide a signed warranty that can be published in case the service steals the coins.

Mixcoin is compatible with Bitcoin and does not require new cryptographic methods. As a central mixing service, it is easier to protect against DoS attacks by single users compared to p2p mixing protocols. However, the mixer will learn the connection between the input and output address. To protect against this, different providers can be used in sequence. This further increases the number of Bitcoin transaction needed and total transaction costs.

Blindcoin [VR15] improves on Mixcoin by using blind signatures to ensure that the mix can't link the input and output address. Nevertheless, the amount that can be mixed is still fixed and the anonymity depends on the number of simultaneous users. Also, the user must be able to anonymously publish the output address to a public log which might result into a bootstrapping problem. Furthermore, while theft will be detected and can be proven, it is not prevented and Bitcoins might still be "lost" [2].

4.2 CoinJoin

CoinJoin [Ma13a] is a concept by Gregory Maxwell of mixing transactions by joining them into a larger transaction. It exploits the fact that a transaction can have multiple inputs and outputs that do not need to belong to the same person. This increases the anonymity of a single transaction, but also can increase the anonymity of Bitcoin in general. As theses join transactions are in principle indistinguishable from other transactions, the assumption that inputs of a transaction belong to a single person does no longer hold.

However, an actual implementation still has to overcome some challenges. First, linking of inputs and outputs might still be possible, based on the value. This can be fixed by requiring each user to transmit the same amount. However, this is unpractical and might make join transactions distinguishable from regular transactions. Then, depending on how the transactions is constructed, all participants learn the connection between input and output addresses. If the transaction joining is performed by a service, it might be required to trust a third-party. On the other hand, if the transaction is created in peer-to-peer network, it might be susceptible to DoS attacks. In any case, it works without modifications to Bitcoin and without necessarily relying on new crypto-graphic methods.

[2] https://en.wikipedia.org/wiki/Mt._Gox

A popular centralized implementation is the **SharedCoin**[3] service. While it can not steal coins from users, it can link the input and output addresses. Thus, if the service is compromised, all anonymity gains are lost.

CoinShuffle [RMSK14] provides a decentralized solution based on a peer-to-peer network. Similar to Tor[4], users encrypt their output address multiple times with the keys of their participants. This ensures, that no one learns the connection between input and output addresses. An optional blame phase is used to protect against DoS attacks.

4.3 CoinSwap

CoinSwap [Ma13b] is another proposal of Gregory Maxwell to perform a transaction through a third party. Instead of Alice transferring coins directly to Bob, she sends the coins to Carol who in turn sends them to Bob. The transactions between Alice and Carol and Carol and Bob are escrow transactions that can be spent with a redeeming transaction that is protected by a hash-lock. This ensures that neither Alice nor Carol can steal coins.

CoinSwap is usable on Bitcoin today. It can even be used to perform transactions across different chains. However, the anonymity does depend on all 2of2 escrow transactions going on at the same time. Furthermore, it increases the number of needed transactions.

4.4 CrytoNote and Monero

CryptoNote [vS13] describes a new crypto currency concept. While the basic structure of transactions and the block-chain is the same as in Bitcoin, address derivation and signature generation make use of new cryptographic methods. When transferring coins, the sender A calculates a new receiver address based on the public key B of the receiving party. The matching private key can only be calculated by the owner of the private key B. To spent coins, the transaction output is signed with a one-time ring signatures. These signatures can be verified against a set of public keys without revealing the actually used private key. The most successful implementation to date is **Monero**[5].

CryptoNote provides anonymity for the sender and the receiver. As it is not a mixing service but a completely new currency, it is not susceptible to DoS attacks. However, it is not compatible with Bitcoin without introducing breaking changes. Furthermore, it relies on new cryptographic methods like one-time key pairs and one-time ring signatures.

4.5 Zerocoin and Zerocash

Zerocoin [Mi13] implements a new crypto currency atop of Bitcoin. It extends Bitcoin by new transaction types, that mint and spent a new sort of coins. The spending of these new

[3] `https://sharedcoin.com/`
[4] `https://www.torproject.org/`
[5] `https://getmonero.org/`

	Bitcoin compatible	architecture	Bitcoin cryptography	theft impossible	single transaction	remarks
Mixcoin	✓	service	✓	✗	✗	anonymity depends on simultaneous users, mixer can link addresses
Blindcoin	✓	service	✓	✗	✗	anonymity depends on simultaneous users
CoinJoin	✓	-	-	✓	✗	details left to implementation, improves overall anonymity in Bitcoin
SharedCoin	✓	service	✓	✓	✗	mixer can link addresses
CoinShuffle	✓	p2p	✓	✓	✗	-
CoinSwap	✓	p2p	✓	✓	✗	allows transactions across chains/altcoins
CryptoNote	✗	altcoin	✗	✓	✓	needs transactions with same amount
Zerocoin	✗	altcoin	✗	✓	✗	large transaction overhead compared to Bitcoin
Zerocash	✗	altcoin	✗	✓	✓	also anonymizes the transaction amount

Tab. 1: Comparison of existing approaches

coins can not be linked to the minting and thus provides anonymity. To prevent double spending, an accumulator of commitments is used. When a coin is spent, a non-interactive zero knowledge proof is used to proof that one such commitment is known. A serial number linked to the commitment ensures that each commitment can only be spent once.

While Zerocoin intended to be used with Bitcoin, it would require breaking changes to Bitcoin. Furthermore, the generated transactions are quite large (>10KB) compared to traditional transactions. One instance of Zerocoin can also only support coins of one value. To support more than one value, several instances would have to be run on simultaneously.

Zerocash [Sa14] improves on Zerocoin by allowing any amount. It is able to hide the origin, destination and amount of a transaction. Compared to Zerocoin it also performs better by reducing the transaction size and time spend on verification. However, it still requires breaking changes to Bitcoin and similar to Zerocoin needs a trusted party to setup public parameters of the protocol.

5 Conclusion

Bitcoin is a new successful approach to crypto currency but does not guarantee anonymity. Figure 1 highlights the relevant properties of current approaches for anonymizing Bitcoins.

Services like Mixcoin and Blindcoin do not require modifications to Bitcoin and are easier to implement than decentralized approaches. However, they do not prevent theft like CoinJoin implementations or CoinSwap. All of them are unable to hide the transaction amount and therefore require extra transactions with fixed amounts. This increases transaction delays and costs. It may also require more blocks in the chain and thus raise the

energy needed by the Bitcoin network. More recent altcoins provide higher anonymity but are incompatible with Bitcoin and introduce overhead. Furthermore, they also rely on new implementations of new cryptographic methods, that might not be trusted by everybody.

For current usage with Bitcoin, an implementation of the CoinJoin concept is the most promising approach. A peer-to-peer implementation like CoinShuffle can be added to existing Bitcoin wallets and used opportunistically. This will increase the anonymity of participants and other Bitcoin users by breaking the assumption in [RH13].

We think that future research on CoinJoin transactions with arbitrary values and whether they can increase anonymity is needed. This would allow making payments while simultaneously mixing and therefore reduce the number of overall transactions, fees payed and energy consumed. One such approach could be "confidential transactions" [6] that hide the amount but can currently not be implemented in Bitcoin in a backwards compatible way.

References

[BdL13] Bergstra, Jan A; de Leeuw, Karl: Bitcoin and beyond: exclusively informational monies. arXiv preprint arXiv:1304.4758, 2013.

[Bo14] Bonneau, Joseph; Narayanan, Arvind; Miller, Andrew; Clark, Jeremy; Kroll, Joshua A; Felten, Edward W: Mixcoin: Anonymity for Bitcoin with accountable mixes. In: Financial Cryptography and Data Security, pp. 486–504. Springer, 2014.

[Bo15] Bonneau, Joseph; Miller, Andrew; Clark, Jeremy; Narayanan, Arvind; Kroll, Joshua A; Felten, Edward W: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. Technical report, Cryptology ePrint Archive, Report 2015/452, 2015.

[Ma13a] Maxwell, Gregory: , CoinJoin: Bitcoin privacy for the real world, 2013.

[Ma13b] Maxwell, Gregory: CoinSwap: transaction graph disjoint trustless trading. CoinSwap: Transactiongraphdisjointtrustlesstrading, 2013.

[Mi13] Miers, Ian; Garman, Christina; Green, Matthew; Rubin, Aviel D: Zerocoin: Anonymous distributed e-cash from bitcoin. In: Security and Privacy (SP), 2013 IEEE Symposium on. IEEE, pp. 397–411, 2013.

[Na08] Nakamoto, Satoshi: , Bitcoin: A peer-to-peer electronic cash system, 2008.

[RH13] Reid, Fergal; Harrigan, Martin: An analysis of anonymity in the bitcoin system. Springer, 2013.

[RMSK14] Ruffing, Tim; Moreno-Sanchez, Pedro; Kate, Aniket: CoinShuffle: Practical decentralized coin mixing for Bitcoin. In: Computer Security-ESORICS 2014. Springer, 2014.

[Sa14] Sasson, E. B.; Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M.: Zerocash: Decentralized Anonymous Payments from Bitcoin. In: 2014 IEEE Symposium on Security and Privacy. 2014.

[VR15] Valenta, Luke; Rowan, Brendan: Blindcoin: Blinded, accountable mixes for bitcoin. In: Financial Cryptography and Data Security, pp. 112–126. Springer, 2015.

[vS13] van Saberhagen, Nicolas: Cryptonote v 2.0. 2013.

[6] `https://people.xiph.org/~greg/confidential_values.txt`