Poster: Towards Blockchain Transaction Privacy

Matthew Di Ferrante[1]
mdf@clearmatics.com
[1]clearmatics
London, UK.

Rebekah Mercer[1, 2]
rebekah.mercer.15@ucl.ac.uk
[2]University College, London
London, UK.

***Abstract*—Blockchains allow users to transfer money securely to possibly unknown and untrusted counterparties, without requiring a trusted intermediary. Transactions contain the value being transferred, and sender and recipient identifiers (known as *addresses*) in the clear, meaning that although on-chain addresses are unlinked from off-chain identities, monetary movements are easily traceable. We explore methods offering transaction privacy, which include ring signatures, with which users can produce a signature that verifies against a set rather than an individual public key, and combine with *stealth addresses*. We construct a scheme that is compatible with current blockchain platforms, but unlinks sender and recipient address pairs in a way that payee addresses are unknown even to the payer of the transaction in question.**

1. Introduction

The launch of the bitcoin blockchain in 2009 allowed mutually distrusting parties to securely transfer money to one another, for the first time, without reliance on a trusted third party [4]. This is achieved by storing the entire transaction history, replicated on all nodes in the Peer-to-Peer network, so that all transactions can be publicly verified. Transactions are initially verified by *miners*, who perform a *Proof of Work* algorithm so that nodes can reach consensus on which block of transactions is taken as valid and appended to the chain [4].

Blockchains provide users with pseudonymity, meaning that the on-chain identifiers (known as *addresses*) of all parties are ideally unlinked with their off-chain identities. However, in practice, address reuse and the transparency of monetary movement allows for very revealing statistical analysis to be performed on the blockchain [3].

Deanonymising account holders, tracing money through the blockchain, or creating graphs of connected addresses are attractive endeavours for both adversaries looking for easy and lucrative hacking targets and law enforcement looking to trace possible criminal activity.

Transaction privacy is desired in many blockchain use-cases – on public blockchains, users may wish for increased levels of privacy in order to avoid revealing their financial situation to every curious blockchain participant. In a permissioned blockchain setting, such as consortium-controlled blockchains, this property is essential – blockchain participants who are not directly involved in a given transaction are not permitted to learn any information about such transactions. As a result, consortia have generally chosen one of the solutions given in Section 2.3, or moved away from the blockchain model, deeming the transparency of blockchain transactions an insurmountable problem.

2. Background

2.1. Bitcoin

Bitcoin uses an 'unspent transaction output' (UTXO) model, and transactions are irreversible. The order in which the on- and off-chain interactions occur is based on the risk profile of the pair of interacting parties.

Several mixes or tumblers to offer users the ability to 'unlink' sender and recipient pairs within bitcoin transactions, by joining their transaction input and output addresses with other parties wishing to perform a similar valued transactions at a similar time [2]. In order to remain compatible with bitcoin and its restricted set of on-chain operations, solutions have multiple off-chain communications, multiple on-chain transactions (for example, four on-chain messages are sent per transaction in [2]) or reliance on a trusted server.

2.2. Ethereum

Ethereum is a blockchain platform which extends the ability to transfer money between on-chain accounts with its Turing-complete virtual machine. This allows users to create incorruptible applications and functions with transparent executions, and even decentralised autonomous organisations (DAOs), all termed 'smart contracts' [5].

Accounts in Ethereum are controlled either by a private key, as with bitcoin accounts, or by the code that resides at the address in question. Rather than using a UTXO model, each address in Ethereum is associated with a state, which is updated as a result of transactions and contract executions. The incorruptability of smart contracts allows us to construct a mixer that cannot act adversarially.

This work was supported by Clearmatics Technologies LTD.

2.3. Permissioned blockchains

In permissioned blockchains, the network is constructed of known, semi-trusted participants. Methods considered to increase privacy in this situation include transaction encryption with a trusted third party (TTP), where all transactions are sent to a trusted third party who checks that the actions performed are valid, then encrypts and broadcasts to the network. This removes the public verifiability of transactions, means blockchain liveness depends on the availability of the TTP, and makes incorrectly or maliciously formed transactions undetectable.

Trusted notaries distribute this TTP behaviour across transaction verifiers selected from a set of validators that the network trusts. This is more robust than a single trusted third party, but still prevents public verifiability of transactions, and the availability of the blockchain is restricted by the availability of the validators.

2.4. Linkable ring signatures

Ring signatures verify against a set of public keys, allowing parties to prove that they are part of a group, without revealing exactly which public key corresponds to the private key that they possess. Any two signatures produced by the same party are indistinguishable from signatures produced by two different parties in the ring. Linkable ring signatures subvert this property and are appended with a linking tag, which is the same across any signatures produced by the same party in the same ring. These tags do not reveal the identity of the signer, but simply show whether or not the signer has already produced a signature for that ring. Using linkable ring signatures, we can construct a transaction mixer, which several parties can deposit funds into, and either withdraw themselves, in order to obfuscate the trail of their transactions, or allow a recipient party to withdraw from, in order to transfer funds in an unlinkable manner. We use unique ring signatures [1].

2.5. Stealth addresses

Stealth address derivation produces addresses that are indistinguishable from random, with the guarantee that only the holder of the master private key is able to spend funds from any address derived from the master public key.

For a long-term, or *master*, ECDSA public key pair mpk and msk, derived stealth keys spk and ssk are constructed as explained below.

With elliptic curve group $E(\mathbb{F}_q)$, generator G, H a hash function with output in $\mathbb{Z}_q$, long-term master key pair mpk, msk and secret v shared between the sender and recipient, a stealth address and its key pair spk, ssk are constructed as follows:

$$\implies spk = mpk + H(v) \cdot G \tag{1}$$

$$\implies ssk = msk + H(v) \tag{2}$$

In dual-key stealth addresses, the secret v is formed by the payer producing an ephemeral key pair b, B, and broadcasting B to the intended recipient. The secret is then formed $v = b \cdot mpk = msk \cdot B$.

Stealth addresses with one amortised communication (in which v is communicated), with n a sequence number, mpk the long-term public key of the recipient, are constructed $spk = mpk + H(vmpk||n) \cdot G$.

Here, v acts as a viewing key, allowing the account owner to give others the ability to deanonymise specific transactions, without the ability to spend the funds in the given account.

For $\mathcal{A}$ wishing to make a transfer to $\mathcal{B}$, interactions are as follows:

1) $\mathcal{A}$ uses $\mathcal{B}$'s long term $mpk_\mathcal{B}$, nonce m and secret v, to form $spk_\mathcal{B}$.
2) $\mathcal{A}$ forms the transaction to deposit $spk_\mathcal{B}$ and the agreed denomination of funds into the smart contract.
3) When the required number of participants have joined, or a predefined number of blocks have been mined, the smart contract broadcasts a notification processed by $\mathcal{A}$. $\mathcal{A}$ tells $\mathcal{B}$ (off-chain) that the contract is ready, and sends him the contract address.
4) $\mathcal{B}$ fetches ring description pk_i from the contract, derives $ssk_\mathcal{B}$, using v and m, and constructs the linkable ring signature.
5) $\mathcal{B}$ creates a new address and sends the correctly formed ring signature to the contract, triggering the withdrawal of funds.

3. Conclusion and Limitations

We have introduced a ring signature mixing scheme with a deterministic ‘stealth address’ method of constructing new addresses and keys. These operations are very expensive on Ethereum currently, with rings of more than 3 parties having to be spread across multiple blocks. However, it provides users with anonymity with respect to an anonymity set, and mixes can be chained (similarly to a mix network) to increase this anonymity set to the level desired by the user.

This solution covers only the case of *transaction* privacy – extending the scheme to cover general computation is non-trivial.

References

[1] M. K. Franklin and H. Zhang. A Framework for Unique Ring Signatures. *IACR Cryptology ePrint Archive*, 2012:577, 2012.

[2] E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro and S. Goldberg. TumbleBit: An untrusted Bitcoin-compatible anonymous payment hub, *IACR Cryptology ePrint Archive*, 2016:575, 2016.

[3] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. 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.

[4] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Oct. 2008.

[5] G. Wood. Ethereum: A Secure Decentralised Generalised Transaction Ledger – Homestead Revision. Jan. 2016.