Master Thesis Exposé - Adaptor Signature Based Atomic Swaps Between Bitcoin and a Mimblewimble Based Cryptocurrency

Jakob Abfalter, 01126889

Security and Privacy Group https://secpriv.tuwien.ac.at/

1 Introduction

In 2008 an anonymous identity with the name Satoshi Nakomoto published a paper with the title "Bitcoin: A peer-to-peer electronic cash system" [12]. The document outlines the building blocks of a digital currency managed by means of a decentralized multi-party protocol. This approach gained increased interest over the years leading to the development of many other Cryptocurrency and Blockchain projects with different goals.
Some of these alternative Cryptocurrency projects are very similar to Bitcoin. For instance, Litecoin [1] and Dogecoin [2] have forked off the Bitcoin codebase and were released with only slightly modified parameterization and algorithms compared to Bitcoin. Other projects like Ethereum tried to create a more expressive way of constructing transactions by introducing Smart Contracts, which allow the execution of arbitrary program code on the Blockchain [3]. Other projects attempted to solve problems that exist in the Bitcoin Blockchain. Zerocoin [10] and Zerocash [15], for instance, are attempts to enhance Bitcoin's weak privacy, resulting from its open nature. In 2016 another anonymous entity published a paper called Mimblewimble [8]. In this paper, another privacy-enhancing Cryptocurrency is proposed. In this protocol, transaction unlinkability is achieved by cleverly pruning already spent transactions, making its Blockchain uniquely space-efficient. The protocol was later layed out in more detail by Andres Poelstra [13] and implemented in the Cryptocurrencies Beam [3] and Grin [4], which both launched in early 2019.

2 Problem Description

At present, there exist a few thousand Cryptocurrencies [5], which are mostly incompatible with each other, as they are running different protocols and cryptography. If Cryptocurrency holders want to exchange their coins for other digital

[1] https://litecoin.com/en/
[2] https://dogecoin.com/
[3] https://beam.mw/
[4] https://grin.mw/
[5] https://coinmarketcap.com/

assets, this can be done using a centralized exchange service such as Binance [6] or Coinbase.[7] When using such a service, the user needs to send his funds to a trusted service, as the exchange is in full control of the funds private keys, at least for the exchange duration. Many of such exchanges have a history of losing funds to hacking attacks [8] [9] [10]; therefore, using such a service comes with a significant risk.

One attempt to create a trustless coin exchange system are Cross-Chain Atomic Swaps. By utilizing so-called hash-time locked contracts (HTLC), we can build transactions on two Blockchains, exchanging coins between two parties, which will only be executed if both parties successfully retrieve their traded coins [7]. So far, such protocols have mostly been implemented on Bitcoin and currencies similar to Bitcoin, as well as Ethereum.[11] [12] [13] A particular challenge is to implement such a swap protocol on privacy-enhancing Blockchains, such as Zerocash, Monero, or Mimblewimble based Grin and Beam, as these systems lack scripting capabilities and only rely on basic cryptographic primitives.

3 Motivation & Objectives

In this thesis, a generic trustless Atomic Swap protocol between Bitcoin and Grin, a privacy-enhancing Cryptocurrency based on the Mimblewimble protocol, should be designed. In the construction two users, one owning Bitcoin and the other owning Grin should be able to exchange their coins without the need for a trusted third party.

To make the coin swap possible, a new notion of a generalized multiparty Adaptor Signature system will be introduced. The security of the system should be given by providing game-based security definitions compatible with the definitions found for Mimblewimble transactions by Fuchsbauer et al. [5].

Mimblewimble is of particular interest for this topic as its transaction construction process already requires interaction between the sender and receiver, making it particularly suitable for the introduction of Adaptor Signatures. The Grin implementation was chosen because it uses the same signature scheme as Bitcoin, and, in contrast to Beam, is developed fully open source without a company owning the codebase. As both Bitcoin and Grin are based on the ECDSA signature scheme, we can leverage the advances made by A. Poelstra [14] and Moreno-Sanchez et al. [11] and build a construction based solely on cryptographic signatures.

[6] https://www.binance.com/en

[7] https://www.coinbase.com/

[8] https://www.bloomberg.com/news/articles/2019-05-08/crypto-exchange-giant-binance-reports-a-hack-of-7-000-bitcoin

[9] https://www.bloomberg.com/news/articles/2014-02-28/mt-gox-exchange-files-for-bankruptcy

[10] https://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know

[11] https://comit.network/

[12] https://www.airswap.io/

[13] https://github.com/dogethereum

We further implement a prototype of the solution, test it on the Bitcoin and Grin testnets, and evaluate its efficiency.
Additionally, we will explore the possibility of similar topics that can be achieved using the protocol. These include Payment Channels on top of Grin, conditional payments, as well as tumbler-based Atomic Swaps. Through this thesis, we will gain some significant insights on the viability and security of trustless coin swap protocols built on privacy-based Blockchains lacking scripting capabilities and thereby contribute to improving interoperability between these systems.

4 Related Work

Herlihy et al. [7] were one of the firsts to mention Atomic Swaps in the scientific literature. Han et al. [6] have evaluated the fairness of Atomic Swamp protocols, and Borkowski et al. [2] give a scientific overview of the current state of the art of this topic. Bennink et al. mainly focus on Atomic Swaps with or on Ethereum [1] and Deshpande et al. construct Atomic Swaps with a focus on protecting the user's privacy [4]. Teutsch et al. [16] managed to lay out and build a bridge network between Ethereum and Dogecoin (A Bitcoin fork) with which coins can be swapped trustlessly. The already mentioned paper by Fuchsbauer et al. [5] did an extensive cryptographic investigation of the Mimblewimble protocol, which security definitions will be highly relevant for this thesis. Recent work, such as [14], [11], [9], made clear that we can build a swap protocol only by utilizing simple Schnorr or ECDSA signatures.
Apart from scientific literature, there exist several production grade or prototype implementations of different Atomic Swap protocols. Comit[14] by CoBloX[15] tries to connect many different Cryptocurrencies, currently supporting Bitcoin and Ethereum, and actively trying to add others to this list. Of particular interest for this thesis is a prototype implementation called grinswap [16] in which Atomic Swaps between Grin Testnet and Ethereum Ropsten testnet were successfully executed.

5 Outline

1. Introduction
2. Motivation & Objectives
3. Preliminaries
   (a) Bitcoin
      i. Bitcoin Transaction Protocol
      ii. Bitcoin Scaling and Layer Two Solutions
   (b) Privacy-enhancing Cryptocurrencies
      i. Zero Knowledge Proofs

[14] https://comit.network/
[15] https://coblox.tech/
[16] https://github.com/vault713/grinswap

        ii. Rangeproofs
        iii. Mimblewimble (Grin)
    (c) Hash-time-locked contracts
    (d) Adaptor Signatures
        i. Schnorr Signature Construction
        ii. ECDSA Signature Construction
4. Adaptor Signature Based Atomic Swaps Between Grin and Bitcoin
    (a) General Notation
    (b) Cryptographic Primitives
    (c) Construction Bitcoin Side
    (d) Construction Grin Side
    (e) Security Definitions
5. Implementation
    (a) Implementation Bitcoin Side
    (b) Implementation Grin Side
    (c) Performance Evaluation
6. Implementation Security and Privacy Evaluation
    (a) Security Evaluation
    (b) Privacy Evaluation
7. Related & Future Work
    (a) Payment Channel Networks on Grin
    (b) Payment Channel Networks on Monero
    (c) Atomic Swaps With Other Cryptocurrencies
    (d) Tumbler Based Atomic Swaps
8. Conclusion

References

1. Bennink, P., Gijtenbeek, L.v., Deventer, O.v., Everts, M.: An analysis of atomic swaps on and between ethereum blockchains using smart contracts. Tech. rep., Tech. report (2018)
2. Borkowski, M., McDonald, D., Ritzer, C., Schulte, S.: Towards atomic cross-chain token transfers: State of the art and open questions within tast. Distributed Systems Group TU Wien (Technische Universit at Wien), Report (2018)
3. Buterin, V., et al.: A next-generation smart contract and decentralized application platform. white paper **3**(37) (2014)
4. Deshpande, A., Herlihy, M.: Privacy-preserving cross-chain atomic swaps
5. Fuchsbauer, G., Orrù, M., Seurin, Y.: Aggregate cash systems: a cryptographic investigation of mimblewimble. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 657–689. Springer (2019)
6. Han, R., Lin, H., Yu, J.: On the optionality and fairness of atomic swaps. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies. pp. 62–75 (2019)
7. Herlihy, M.: Atomic cross-chain swaps. In: Proceedings of the 2018 ACM symposium on principles of distributed computing. pp. 245–254 (2018)
8. Jedusor, T.E.: Mimblewimble (2016)

9. Malavolta, G., Moreno-Sanchez, P., Schneidewind, C., Kate, A., Maffei, M.: Anonymous multi-hop locks for blockchain scalability and interoperability. In: NDSS (2019)
10. Miers, I., Garman, C., Green, M., Rubin, A.D.: Zerocoin: Anonymous distributed e-cash from bitcoin. In: 2013 IEEE Symposium on Security and Privacy. pp. 397–411. IEEE (2013)
11. Moreno-Sanchez, P., Kate, A.: Scriptless scripts with ecdsa
12. Nakamoto, S., et al.: Bitcoin: A peer-to-peer electronic cash system (2008)
13. Poelstra, A.: Mimblewimble (2016)
14. Poelstra, A.: Scriptless scripts (2017)
15. 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. pp. 459–474. IEEE (2014)
16. Teutsch, J., Straka, M., Boneh, D.: Retrofitting a two-way peg between blockchains. arXiv preprint arXiv:1908.03999 (2019)