



Informatics

Adaptor Signature Based Atomic Swaps Between Bitcoin and a Mimblewimble Based Cryptocurrency

MASTER'S THESIS

submitted in partial fulfillment of the requirements for the degree of

Master of Science

in

Software Engineering Internet Computing

by

Jakob Abfalter, BSc

Registration Number 01126889

to the Faculty of Informatics

at the TU Wien

Advisor: Univ. Prof. Dr. Matteo Maffei

Assistance: Dr. Pedro Moreno Sanchez

Vienna, 6th April, 2020

Jakob Abfalter

Matteo Maffei

Erklärung zur Verfassung der Arbeit

Jakob Abfalter, BSc

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 6. April 2020

Jakob Abfalter

Danksagung

Ihr Text hier.

Acknowledgements

Enter your text here.

Kurzfassung

Ihr Text hier.

Abstract

Enter your text here.

Contents

Kurzfassung	ix
Abstract	xi
Contents	xiii
1 Introduction	1
2 Motivation & Objectives	3
3 Preliminaries	5
3.1 Bitcoin	5
3.2 Privacy-enhancing Cryptocurrencies	5
3.3 Hash-time-locked Contracts	5
3.4 Adaptor Signatures	5
4 Adaptor Signature Based Atomic Swaps Between Bitcoin and Grin	7
4.1 General Notation	7
4.2 Cryptographic Primitives	7
4.3 Generalized multiparty Adaptor Signature	7
4.4 Atomic Swap Construction	7
5 Implementation	9
5.1 Implementation Bitcoin side	9
5.2 Implementation Grin side	9
5.3 Performance Evaluation	9
6 Implementation Security and Privacy Evaluation	11
6.1 Security Evaluation	11
6.2 Privacy Evaluation	11
7 Related and Future Work	13
7.1 Payment Channel Networks on Grin	13
7.2 Payment Channel Networks on Monero	13
	xiii

7.3	Atomic Swaps With Related Cryptocurrencies	13
7.4	Tumbler Based Atomic Swaps	13
8	Conclusion	15
	List of Figures	17
	List of Tables	19
	List of Algorithms	21
	Bibliography	23

CHAPTER 1



Introduction

TODO

CHAPTER 2

Motivation & Objectives

TODO

CHAPTER 3

Preliminaries

3.1 Bitcoin

3.1.1 Bitcoin Transaction Protocol

3.1.2 Bitcoin Scaling and Layer Two Solutions

3.2 Privacy-enhancing Cryptocurrencies

3.2.1 Zero Knowledge Proofs

3.2.2 Range Proofs

3.2.3 Mimblewimble (Grin)

3.3 Hash-time-locked Contracts

3.4 Adaptor Signatures

3.4.1 Schnorr Signature Construction

3.4.2 ECDSA Signature Construction

Adaptor Signature Based Atomic Swaps Between Bitcoin and Grin

- 4.1 General Notation
- 4.2 Cryptographic Primitives
- 4.3 Generalized multiparty Adaptor Signature
- 4.4 Atomic Swap Construction
 - 4.4.1 Construction Bitcoin side
 - 4.4.2 Construction Grin side
 - 4.4.3 Security Definitions

CHAPTER 5



Implementation

5.1 Implementation Bitcoin side

5.2 Implementation Grin side

5.3 Performance Evaluation

CHAPTER 6

Implementation Security and Privacy Evaluation

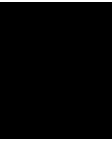
6.1 Security Evaluation

6.2 Privacy Evaluation

Related and Future Work

- 7.1 Payment Channel Networks on Grin
- 7.2 Payment Channel Networks on Monero
- 7.3 Atomic Swaps With Related Cryptocurrencies
- 7.4 Tumbler Based Atomic Swaps

CHAPTER 8



Conclusion

List of Figures

List of Tables

List of Algorithms

Bibliography