h_da

HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Hochschule Darmstadt

– Fachbereich Informatik–

Atomic Cross-Chain Swaps and interoperability of Blockchains

Exposé der Abschlussarbeit zur Erlangung des akademischen Grades

Bachelor of Science (B.Sc.)

vorgelegt von

Christopher Glißner

Matrikelnummer: 732978

Referent	:	Lars-Olof Burchard
Korreferent	:	Alexander del Pino

CONTENTS

1 EXPOSÉ

1.1 PROBLEM DEFINITION

Today's blockchain ecosystem has spread into multiple chains using different consensus algorithms and architectures. After a decade of blockchain applications and development there appears the need for interoperability between upcoming and current blockchain innovations. Interoperability presents a complex task towards a wider uptake of blockchain technologies to swap assets and tokens between chains in a steadily growing environment. Implementing and analyzing atomic cross-chain swaps might be mandatory to enable cross-chain transactions in a safely manner towards an internet of blockchains.

1.2 CURRENT STATE OF RESEARCH

Decentralization and scaling of blockchains is a widely addressed topic by many researchers. Bitcoin [7] was the first successful blockchain application which decentralizes money, combining the well-known concepts of Proof-of-Work algorithms and the distributed ledger concept. Based on previous work by Wood [9], Buterin described the next-generation Smart Contract and decentralized application platform known as Ethereum [2]. While most present blockchains still remain unconnected, pegged sidechains are formally defined by [1] and serve as foundation for many proposals towards blockchain interoperabilty [4] [8]. Herlihy proposed the concept of atomic cross-chain swaps to exchange tokens and assets between blockchains safely [3]. Kiayas and Zindras constructed a new primitive called Non-Interactive Proofs of Proof-of-Work [5] which they use in their work on Proof-of-Work sidechains to enable communication between two blockchains without intermediaries [6].

1.3 MOTIVATION

Exchanging assets or tokens between different blockchains still brings up some security issues for end users. With current state of the blockchain ecosystem it is not possible to exchange information between blockchains without an intermediate, which leaves several attack vectors open to malicious actors. Motivation of this thesis is to review current state of the art, both in terms of blockchain interoperability and atomic swap technologies and an outlook to what future and present implementations offer.

1.4 RESEARCH OBJECTIVES

Main focus of this thesis is to implement a smart contract on both the main- and sidechain and execute an atomic swap forth and back between two blockchains. Since touring complete languages like solidity which runs on Etherum's Virtual Machine it remains an open question if atomic swaps are possible with the current architecture of Bitcoin's script language. Another objective is to evaluate if atomic swaps can be done between different consensus algorithms e.g. between Proof-of-Stake and Proof-of-Work, towards a heterogenous internet of blockchains. Therefore this thesis will gather information on current state of the art research and involve aspects like data privacy that is essential for enterprise processes.

1.5 RESEARCH METHODOLOGY

Part of this thesis is to review currently operational blockchains and forthcoming cryptocurrency systems in terms of interoperability and potential directions of research. Since there are several consensus algorithms this work will discuss the challenges of connecting blockchains with different architectures and features. In order to implement atomic cross-chain swaps two separate blockchains will be set up and build the foundation to deploy the main- and side chain smart contract to approach the challenge towards an atomic swap of tokens. Another part is to gather information if current cryptocurrencies in circulation can cover the requirements for interoperability.

1.6 OUTLINE

1. Abstract
2. Introduction
3. General Principles
    - 3.1 Proof-of-Work Private and Public Sidechains
    - 3.2 Atomic Cross-Chain Swaps
    - 3.3 Non-Interactive Proofs of Proof-of-Work
    - 3.4 Interoperability
4. Related Work
5. Requirement Analysis and Concept
6. Implementation
    - 6.1 Main- and Sidechain Smart Contracts
    - 6.2 Comparing present Blockchain implementations
7. Outlook and Future Research
8. Conclusion and Outlook
9. Bibliography

BIBLIOGRAPHY

[1] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille. "Enabling blockchain innovations with pegged sidechains." In: (2014), p. 72.

[2] Vitalik Buterin. "Ethereum: A next-generation smart contract and decentralized application platform, 2013." In: *URL {http://ethereum. org/ethereum. html}* (2017).

[3] Maurice Herlihy. "Atomic cross-chain swaps." In: *Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing*. ACM. 2018, pp. 245–254.

[4] Sandra Johnson, Peter Robinson, and John Brainard. "Sidechains and interoperability." In: *arXiv preprint arXiv:1903.04077* (2019).

[5] Aggelos Kiayias, Andrew Miller, and Dionysis Zindros. "Non-Interactive Proofs of Proof-of-Work." In: *IACR Cryptology ePrint Archive* 2017 (2017), pp. 1–42.

[6] Aggelos Kiayias and Dionysis Zindros. "Proof-of-Work Sidechains." In: *IACR Cryptology ePrint Archive* 2018 (2018), p. 1048.

[7] Satoshi Nakamoto et al. "Bitcoin: A peer-to-peer electronic cash system." In: (2008).

[8] Gavin Wood. "Polkadot: Vision for a heterogeneous multi-chain framework." In: *White Paper* (2016).

[9] Gavin Wood et al. "Ethereum: A secure decentralised generalised transaction ledger." In: *Ethereum project yellow paper* 151.2014 (2014), pp. 1–32.