Contents

Chapter 1

Introduction

Chapter 2

Background

2.1 Blockchain

2.2 Bitcoin

2.3 Privacy

2.4 Private Schemes

2.4.1 Tumblers

2.4.2 Zcash

2.4.3 Monero

2.4.4 Quisquis

Chapter 3

Auditability in Private Payment Systems

Auditability plays a pivotal role in ensuring the integrity, transparency, and regulatory compliance of payment systems. In financial transactions, where trust and security are paramount, regulatory functions serve as critical safeguards to protect against fraud, money laundering, and other illicit activities. These regulatory functions that appear in the literature can be categorized in transaction and user level.
On the transaction level regulatory functions can include data such as: *value limits* (e.g. a threshold in the transfer amount), *tracing tags*, that provide links between transactions, *revealing the transaction value and/or participants*, *tax rate*, deducting a transaction's value portion towards a predetermined account.
On the user level regulatory functions can include: *information of user's sum of values* (e.g. total amount of funds received/spent in a specific period of time), *user revocation*, meaning that specific policies are applied only to users in a "blacklist", *deriving statistical information* (e.g. learning th average transacted value in a time from user's past transactions), *revoking a non compliant user's anonymity.*

There are two approaches in order these regulation to be enforced, *auditability* and *accountability.* On the one hand, auditability refers to a protocol where an external auditor can learn the requested information through the data that are stored on the blockchain. This protocol could be either interactive with the users, meaning their consent is required, or non-interactive. On the other hand, accountability refers to recurrently execution of policies by system fucntionalities when certain predicate is satisfies. In other words, transactions that does not comply with system's policies will never be verified and stored in the blockchain. Therefore, there is no need of active

participation of an external auditor, since the policies are enforced during the verification phase of the transaction.

Afterwards, an overview of existing distributed payment systems which combines both privacy and auditability is presented. Following the structure of [1] these systems are divided into two categories depending on the power given to the auditors from the disclosed information: There are systems that requires a centralized trusted desingated athority to perform the regulation functions and the systems that does not assume any explicit auditor.

3.1 Trusted desingated Auditor

3.1.1 Zcash extension

3.1.2 PRCash

3.1.3 ACCDET

3.2 General Auditor

3.2.1 zkLedger

3.2.2 PGC

Chapter 4

Proposed Scheme

Chapter 5

Implementation

Chapter 6

Evaluation

Chapter 7

Conclusion

Bibliography

[1] Panagiotis Chatzigiannis, Foteini Baldimtsi, and Konstantinos Chalkias. "SoK: Auditability and Accountability in Distributed Payment Systems". In: *Applied Cryptography and Network Security: 19th International Conference, ACNS 2021, Kamakura, Japan, June 21–24, 2021, Proceedings, Part II*. Kamakura, Japan: Springer-Verlag, 2021, 311–337. ISBN: 978-3-030-78374-7. DOI: 10.1007/978-3-030-78375-4_13. URL: https://doi.org/10.1007/978-3-030-78375-4_13.