UNIVERSITÀ DEGLI STUDI ROMA TRE

Facoltà di Ingegneria
Corso di Laurea in Ingegneria Informatica

Tesi Di Laurea

Studio dell'architettura payment channel per blockchain basate su smart contract con linguaggi turing completi

Laureando

Federico Ginosa

Matricola 457026

Relatore

Alberto Paoluzzi

Correlatore

Federico Spini

Anno Accademico 2017-2018

Questa è la dedica

Indice

Elenco delle figure

Ringraziamenti

Introduzione

Capitolo 1

State channel e payment channel

State channel

Payment channel

Progetti esistenti

Lightning Network

Spirites

Perun

Nocust

Descrizione dell'architettura

Analisi della sicurezza

Interruzione del servizio da parte dell'hub

Hub compromesso porta in catena root hash errato

Capitolo 2

Inextinguishable payment channel

Introduzione

Schema propose/accept

Introduzione

Transazioni off-chain

Schema detach/attach

Introduzione

Hot withdraw

Hot refill

Threat model

Double spending di un token

Token non speso

Capitolo 3

Fulgur Hub

Introduzione

Obiettivi di progettazione

Pagamenti ibridi

Trustless

Non censurabile

Anonimato

Scalabilità

Schema detach/attach esteso

Pagamenti omogenei

Pagamenti misti

Pagamenti esterni

Capitolo 4

Threat model

Introduzione

Recoverable exception paths

B does not send a receipt back to Alice

Myriad of tokens generation

Unrecoverable exception paths

The hub is not cooperative in token attachment

The hub is not cooperative in token detachment

Payment attempt via expired token

Alice refuse to settle the transfer

Malicious pending token redemption attempt

Non-cooperation in payment reception

Capitolo 5

Proof of concept

Introduzione

Scopi della PoC

Apertura di un canale

Transazioni OnChain-OnChain

Transazioni OffChain-OffChain

Transazioni OffChain-OnChain

Transazioni OnChain-OffChain

Riscossione di un pending token

Chiusura di un canale

Capitolo 6

Prove sperimentali

Introduzione

Transazioni OffChain-OffChain seriali

Transazioni OffChain-OffChain concorrenti

Conclusioni e sviluppi futuri

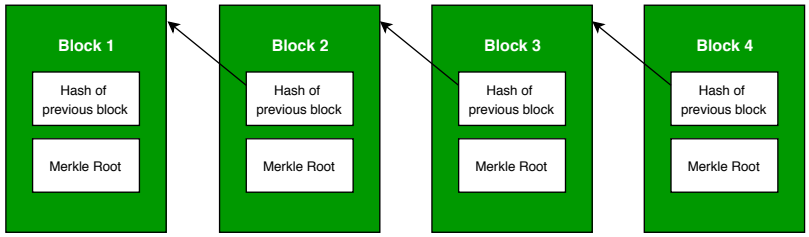

Figura 6.1: Blockchain con blocchi non manomessi