— lang: it frontespizio: true facolta: Facoltà di Ingegneria corsoDiLaurea: Corso di Laurea in Ingegneria Informatica titoloTesi: Studio dell'architettura payment channel per blockchain basate su smart contract con linguaggi turing completi nomeLaureando: Federico Ginosa matricolaLaureando: 457026 annoAccademico: 2017-2018 relatore: Alberto Paoluzzi correlatore: Federico Spini dedica: Questa è la dedica toc: true toc-depth: 1 lof: true documentclass: book fontsize: 12pt linestretch: 1.25 bibliography: bibliography.bib csl: template/transactions-on-computer-systems.csl —

\chapter*{Ringraziamenti}

\chapter*{Introduzione} ![Blockchain con blocchi non manomessi](./figure/blocks-green.pdf){width=400}

State channel e payment channel

State channel

Payment channel

Progetti esistenti

1. Lightning Network
2. Spirites
3. Perun
4. Nocust
   (a) Descrizione dell'architettura
   (b) Analisi della sicurezza
   (c) Interruzione del servizio da parte dell'hub
   (d) Hub compromesso porta in catena root hash errato

Inextinguishable payment channel

Introduzione

Schema propose/accept

1. Introduzione
2. Transazioni off-chain

Schema detach/attach

1. Introduzione
2. Hot withdraw
3. Hot refill

Threat model

1. Double spending di un token
2. Token non speso
3. Gestione della free-option
4. Threat modeling tool

Fulgur Hub

Introduzione

Obiettivi di progettazione

Pagamenti ibridi

Trustless

Non censurabile

Anonimato

Scalabilità

Schema detach/attach esteso

Pagamenti omogenei

Pagamenti misti

Pagamenti esterni

Chiusura di un canale

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

Modello di incentivi

Proof of concept

2. Solidity

Database

1. Redis
2. LevelDB

Prove sperimentali

Introduzione

Transazioni OffChain-OffChain seriali

Transazioni OffChain-OffChain concorrenti

\chapter*{Conclusioni e sviluppi futuri}