Nexa Center for Internet & Society
Politecnico di Torino

Bitcoin: la moneta senza autorità

Marco Conoscenti
Ricercatore postdoc in Ingegneria Informatica

Crittografia: dalla teoria alle applicazioni, Anywhere, 17 aprile 2020

Indice

- Bitcoin e la blockchain
  - Concetti chiave
  - Funzionamento
  - Demistificazione
- Le payment channel network
- La mia ricerca

Bitcoin e la blockchain

Concetti chiave

Bitcoin

Bitcoin è una cripto-moneta decentralizzata

Rete di Bitcoin

Rete i cui nodi sono computer che eseguono il software di Bitcoin

Chiunque può eseguire il software di Bitcoin e diventare parte della rete

Transazione

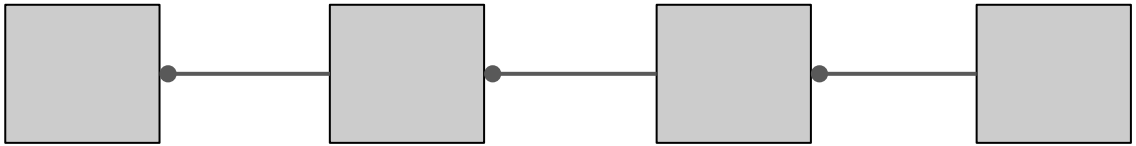
Trasferimento di cripto-moneta da una parte a un’altra

Ogni transazione va
registrata in un libro mastro
per prevenire la doppia spesa

Blockchain

Il libro mastro che memorizza le transazioni di Bitcoin

Blockchain



- Le transazioni vengono registrate in blocchi
- Struttura a catena: difficile da manomettere
- Pubblica: tutti possono accedervi
- Distribuita: ogni nodo di Bitcoin ne possiede una copia

Miner

Nodi che registrano blocchi di transazioni nella blockchain

Funzionamento

Ogni nodo ha una copia della blockchain

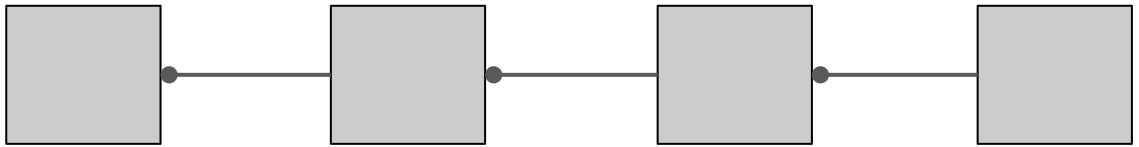
È necessario un protocollo di consenso distribuito per sincronizzare le copie

Protocollo di consenso distribuito

1. Le nuove transazioni vengono mandate alla rete di Bitcoin per essere inserite nella blockchain
2. Ogni miner prepara un blocco di transazioni
3. Viene selezionato il miner che inserisce il prossimo blocco nella blockchain

Selezione del blocco

Blockchain



Nuovi blocchi candidati

Alice Berto Carola

Selezione del blocco

Serve un metodo di selezione non monopolizzabile per garantire la decentralizzazione

Selezione del blocco

Il miner che inserisce il prossimo blocco è il primo che risolve un puzzle crittografico (Proof of Work)

Proof of Work (PoW)

- La probabilità che un miner inserisca un blocco è direttamente proporzionale alla sua potenza di calcolo
- Difficile da risolvere
- In media si produce un blocco ogni 10 minuti

Protocollo - Riepilogo

1. Le nuove transazioni vengono mandate alla rete di Bitcoin per essere inserite nella blockchain
2. Ogni miner prepara un blocco di transazioni e prova a risolvere la PoW
3. Il blocco del miner che per primo ha risolto la PoW viene mandato alla rete di Bitcoin
4. Ogni nodo aggiunge il blocco alla sua copia della blockchain

Incentivi economici

Il miner che inserisce il blocco nella blockchain riceve in compenso nuova moneta

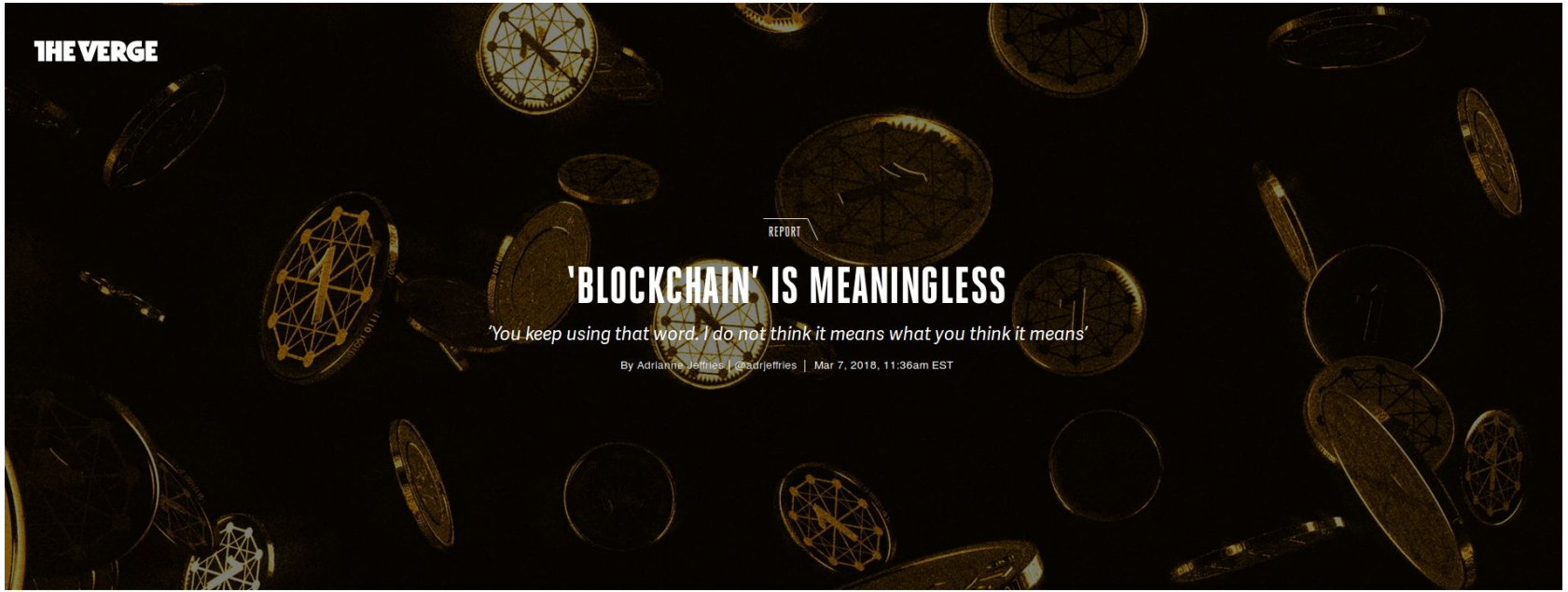
Incentivi economici

- Incentivano i miner a produrre blocchi validi
- Incentivano i miner a risolvere la PoW
- Viene coniata nuova moneta

La novità di Bitcoin

Un sistema aperto e decentralizzato, garantito dalla combinazione di PoW e incentivi economici

Demistificazione



https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning

La novità della blockchain è la decentralizzazione

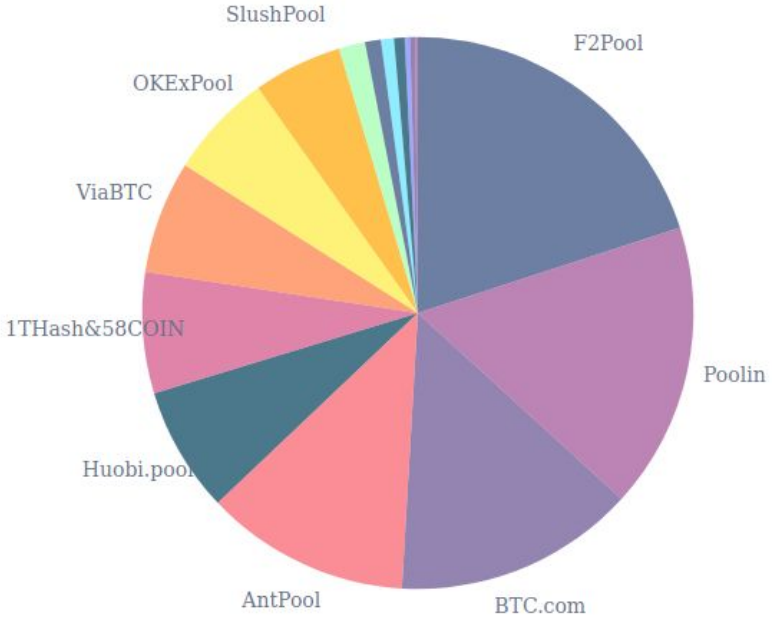
Le blockchain private o chiuse sono solo database distribuiti
(una tecnologia che esiste dagli anni 80)

La blockchain funziona solo con la cripto-moneta alla base

La blockchain è inefficiente:
Bitcoin supporta al massimo 7 transazioni al secondo

Bitcoin tende alla centralizzazione

Miner in Bitcoin



https://www.blockchain.com/charts/pools

Gli sviluppatori di Bitcoin esercitano il controllo sulle modifiche al software

The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure, De Filippi P. e Loveluck B., Internet Policy Review, Vol. 5, Issue 4

Le payment channel network

La blockchain non scala

Per mantenere Bitcoin decentralizzato, viene limitata la crescita della blockchain

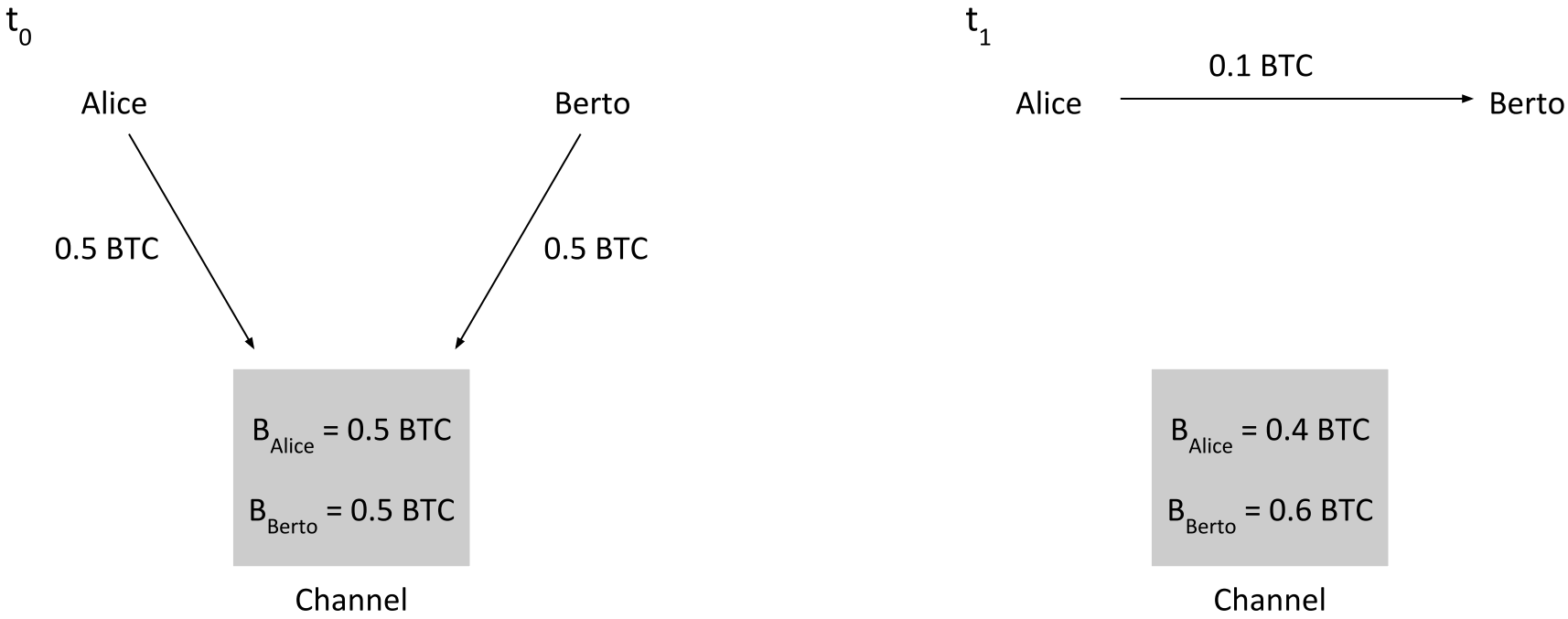
Bitcoin supporta al massimo 7 transazioni al secondo

Le payment channel network sono la soluzione più promettente, in quanto preservano la decentralizzazione

Le payment channel network permettono di eseguire pagamenti off-chain

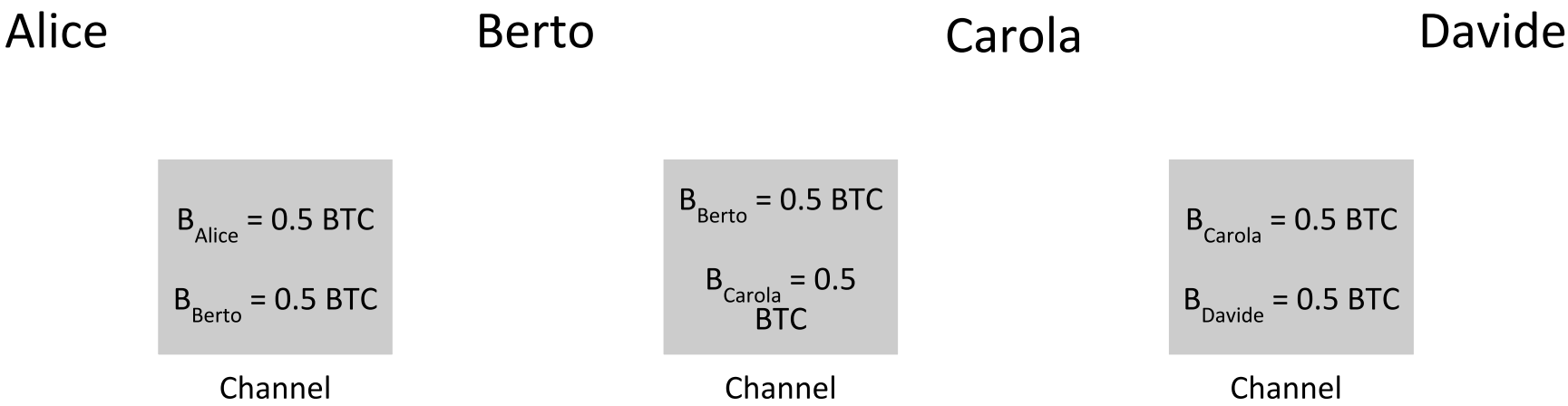
Un payment channel è un canale tra due nodi che permette loro di scambiare pagamenti off-chain

Payment channel - Esempio

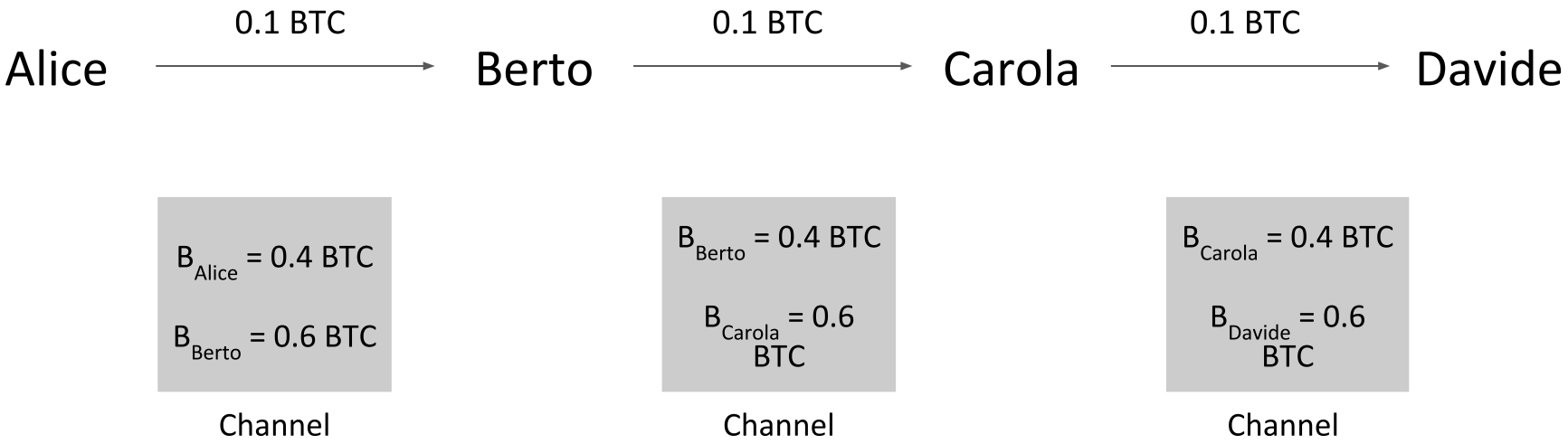


Una payment channel network è costituita da payment channel connessi tra di loro

Payment channel network - Esempio



Payment channel network - Esempio



Lightning Network è la payment channel network principale

Viene utilizzata in Bitcoin

Chiunque può scaricare il software e entrare a far parte di LN

https://play.google.com/store/apps/details?id=fr.acinq.eclair.wallet.mainnet2

LN il 16 aprile 2020

5,046 nodes

31,802 channels

956.17 BTC (~6M $)

https://explorer.acinq.co/?utm_source=bitcoiner.today

Lightning Network usa l'Hashed Timelock Contract (HTLC) per trasferire pagamenti off-chain

L'HTLC fa sì che non sia necessario fidarsi degli altri nodi

Durante un pagamento, i fondi in trasferimento sono bloccati fino a quando il pagamento ha avuto successo;
o fino a quando scade un timeout

I problemi di LN

- La capacità dei payment channel limita l’ammontare dei pagamenti
- I payment channel sono soggetti a sbilanciamento
- I nodi che si disconnettono causano il blocco di fondi

La mia ricerca

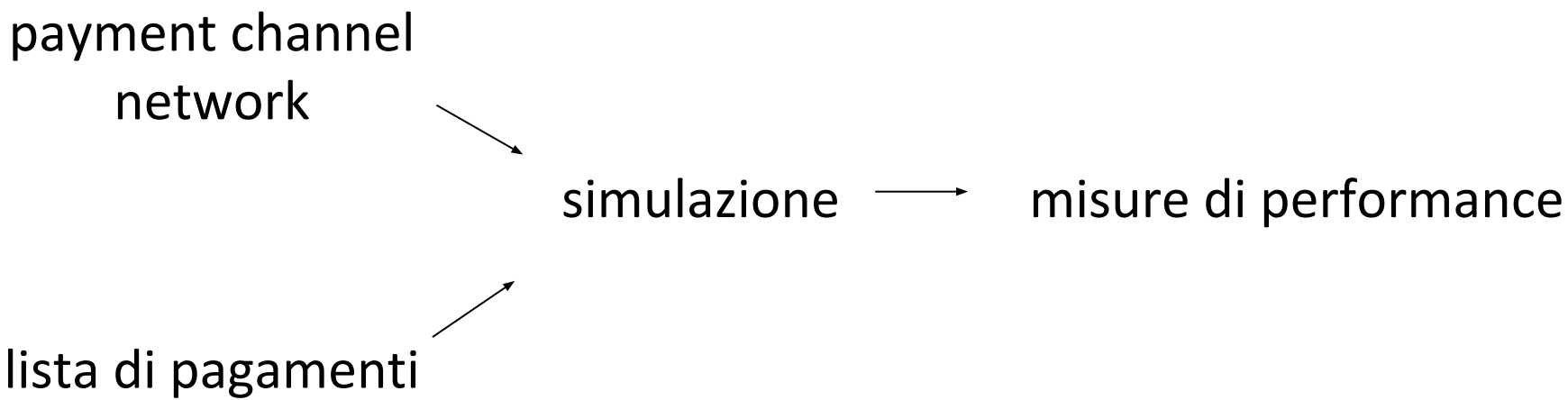
L’obiettivo di ricerca è analizzare possibilità e limiti delle payment channel network

Ho sviluppato CLoTH, un simulatore di Lightning Network (scritto in C e python)

CLoTH simula pagamenti in una payment channel network e produce misure di performance

(ad es. probabilità di successo, tempo medio di pagamento)

Flusso di CLoTH



CLoTH permette di:

- identificare problemi delle payment channel network
- testare miglioramenti del protocollo
- simulare attacchi
- studiare l’evoluzione delle payment channel network

Simulazioni

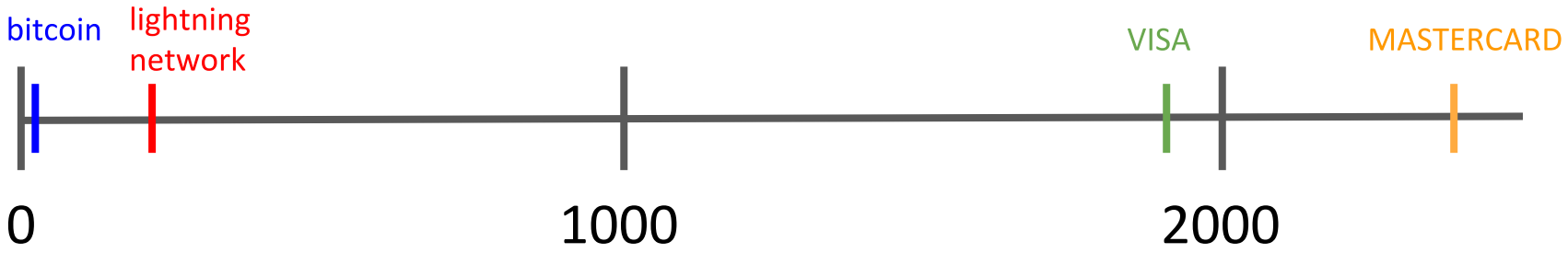
- su Lightning Network (x2)
- su payment channel network sintetiche
- su hubs in Lightning Network
- su approcci di ribilanciamento
- su service provider in Lightning Network

Simulazioni su Lightning Network (I)

Uno snapshot di LN (giugno 2018) è stato dato in input a CLoTH per scoprire configurazioni in cui LN è non operativa

Una delle configurazioni di non operatività si è verificata quando il rate di pagamenti è stato settato a 100 pagamenti/secondo

Pagamenti al secondo in diversi sistemi di pagamento



Simulazioni su Lightning Network (II)

Uno snapshot di LN più recente (febbraio 2019) è stato dato in input a CLoTH per studiarne la performance

La probabilità di successo è più bassa del 90% quando vengono simulati pagamenti dell’ordine di 10K satoshi (~10$)

Simulazioni su payment channel network sintetiche

Le payment channel network sintetiche sono reti generate da CLoTH utilizzando la loro descrizione statistica

Sono state generate diverse reti variando il numero di payment channel per nodo

È risultato che sono necessari almeno 5 canali per nodo per avere una rete ben connessa

Sono state provate diverse configurazioni variando la probabilità che i nodi si disconnettano

È risultato che con probabilità al di sotto del 10% non avvengono significativi fallimenti

Simulazioni sugli hub

Simulazioni che studiano la performance di LN quando vengono rimossi gli hub (i nodi con il maggior numero di canali)

Chi sono gli hub

rompert.com - 952 canali - sviluppatori di un explorer di LN

IP Location	- California - San Francisco - Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET - Cloudflare, Inc., US (registered Jul 14, 2010)

acinq.com - 836 canali - sviluppatori di una versione di LN

IP Location	- Hessen - Frankfurt Am Main - A100 Row Gmbh
ASN	AS16509 AMAZON-02 - Amazon.com, Inc., US (registered May 04, 2000)

Chi sono gli hub

lightningpowerusers.com - 812 canali - sviluppatori di un launcher di LN

IP Location	- New York - Hicksville - Verizon Communications Inc.
ASN	AS701 UUNET - MCI Communications Services, Inc. d/b/a Verizon Business, US (registered Aug 03, 1990)

truevision.club - 734 canali - servizio che permette di fare micropagamenti

IP Location	- California - San Francisco - Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET - Cloudflare, Inc., US (registered Jul 14, 2010)

Chi sono gli hub

ln1.satoshi.com - 716 canali - non trovato

IP Location	- California - Mountain View - Google Llc
ASN	AS15169 GOOGLE - Google LLC, US (registered Mar 30, 2000)

1ML.com - 645 canali - sviluppatori di un explorer di LN

IP Location	- New York - New York City - Fdcservers.net
ASN	AS174 COGENT-174 - Cogent Communications, US (registered May 16, 1996)

La probabilità di successo è rimasta invariata quando sono stati rimossi gli hub

Simulazioni sul ribilanciamento

Ho progettato e implementato nel simulatore un paio di approcci per il ribilanciamento dei canali

Uno dei due approcci ha ridotto di un quarto la probabilità di fallimento per sbilanciamento

Simulazioni sui service provider

È stato simulato un tipico caso d’uso di LN: molti pagamenti vengono mandati a pochi nodi che fanno da service provider

I payment channel collegati ai service provider si sono sbilanciati: il 26% dei pagamenti sono falliti a causa dello sbilanciamento

Per riassumere

Punti di forza di LN

- LN è resistente alla rimozione degli hub
- LN è resistente a una moderata disconnessione dei nodi

Punti di debolezza di LN

- L’ammontare dei pagamenti è strettamente limitato (1-10$)
- I canali sono soggetti a sbilanciamento

Lavori in corso

- Simulazioni di scenari di attacco
- Analisi di rete di Lightning Network
- Test di miglioramenti al protocollo

Se siete interessati, contattatemi!

Grazie

marco.conoscenti@polito.it