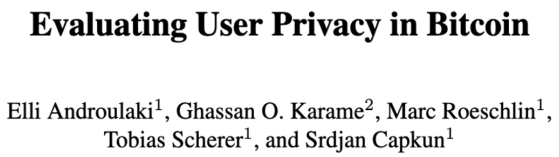
An Empirical Analysis of Privacy in the Lightning Network

George Kappos [1] **Haaroon Yousaf** [1] Ania M. Piotrowska [1,2] Sanket Kanjalkar [3]

Sergi Delgado-Segura [1,5] Andrew Miller [3,6] Sarah Meiklejohn [1]

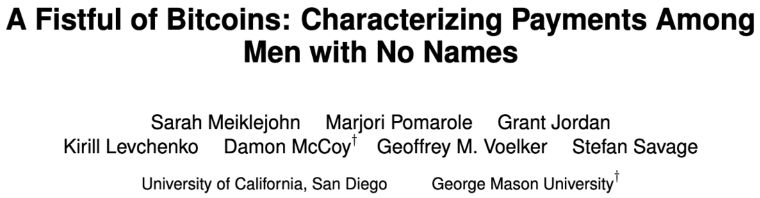
[1] University College London
[2] Nym Technologies
[3] University of Illinois Urbana-Champaign
[5] PISA Research
[6] IC3

Privacy Issues in Cryptocurrencies



Evaluating User Privacy in Bitcoin

Elli Androulaki[1], Ghassan O. Karame[2], Marc Roeschlin[1],
Tobias Scherer[1], and Srdjan Capkun[1]



A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy† Geoffrey M. Voelker Stefan Savage
University of California, San Diego George Mason University†

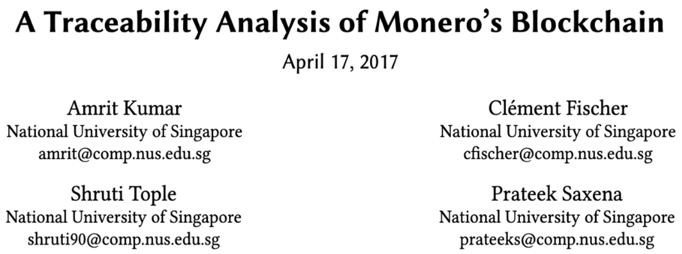
An Analysis of Anonymity in the Bitcoin System

Fergal Reid
Clique Research Cluster
University College Dublin, Ireland
fergal.reid@gmail.com

Martin Harrigan
Clique Research Cluster
University College Dublin, Ireland
martin.harrigan@ucd.ie

Quantitative Analysis of the Full Bitcoin Transaction Graph

Dorit Ron and Adi Shamir



A Traceability Analysis of Monero's Blockchain

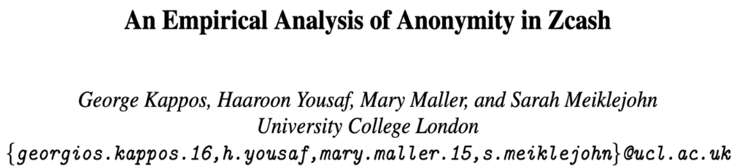
April 17, 2017

Amrit Kumar
National University of Singapore
amrit@comp.nus.edu.sg

Clément Fischer
National University of Singapore
cfischer@comp.nus.edu.sg

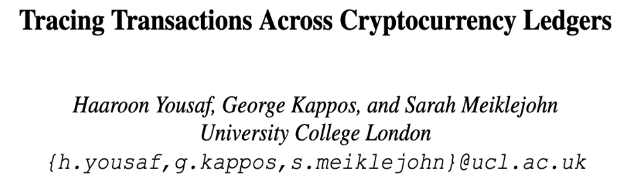
Shruti Tople
National University of Singapore
shruti90@comp.nus.edu.sg

Prateek Saxena
National University of Singapore
prateeks@comp.nus.edu.sg



An Empirical Analysis of Anonymity in Zcash

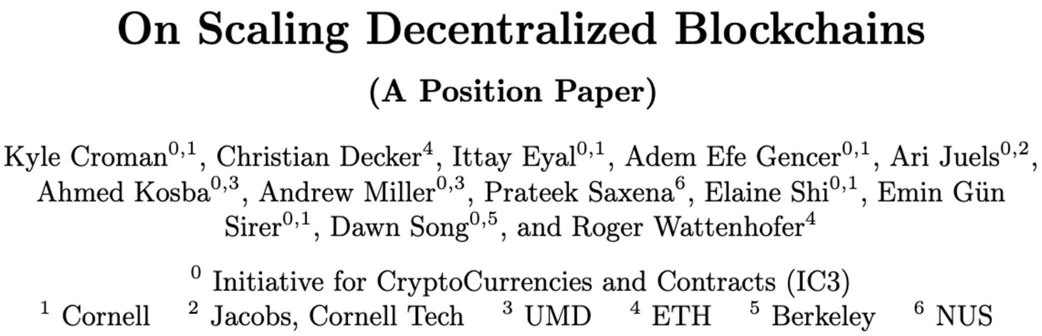
George Kappos, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn
University College London
{georgios.kappos.16,h.yousaf,mary.maller.15,s.meiklejohn}@ucl.ac.uk



Tracing Transactions Across Cryptocurrency Ledgers

Haaroon Yousaf, George Kappos, and Sarah Meiklejohn
University College London
{h.yousaf,g.kappos,s.meiklejohn}@ucl.ac.uk

Scalability Issues in Cryptocurrencies



On Scaling Decentralized Blockchains

(A Position Paper)

Kyle Croman[0,1], Christian Decker[4], Ittay Eyal[0,1], Adem Efe Gencer[0,1], Ari Juels[0,2], Ahmed Kosba[0,3], Andrew Miller[0,3], Prateek Saxena[6], Elaine Shi[0,1], Emin Gün Sirer[0,1], Dawn Song[0,5], and Roger Wattenhofer[4]

[0] Initiative for CryptoCurrencies and Contracts (IC3)
[1] Cornell [2] Jacobs, Cornell Tech [3] UMD [4] ETH [5] Berkeley [6] NUS

On the Security and Performance of Proof of Work Blockchains

Arthur Gervais
ETH Zurich, Switzerland
arthur.gervais@inf.ethz.ch

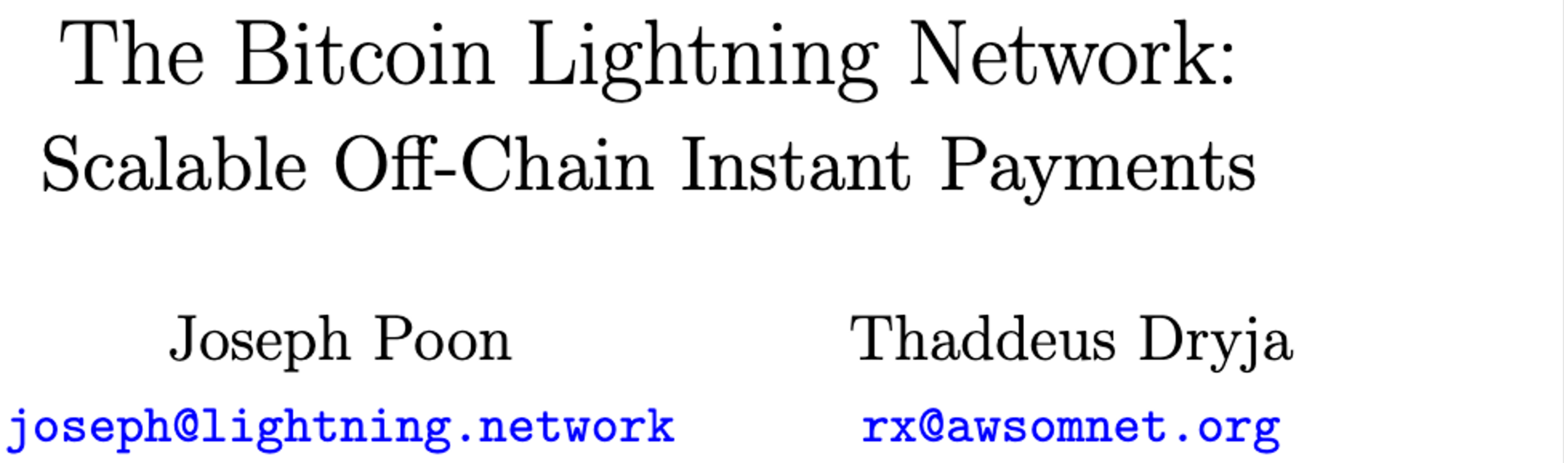
Ghassan O. Karame
NEC Laboratories, Europe
ghassan.karame@neclab.eu

Karl Wüst
ETH Zurich, Switzerland
kwuest@student.ethz.ch

Vasileios Glykantzis
ETH Zurich, Switzerland
glykantv@student.ethz.ch

Hubert Ritzdorf
ETH Zurich, Switzerland
hubert.ritzdorf@inf.ethz.ch

Srdjan Čapkun
ETH Zurich, Switzerland
srdjan.capkun@inf.ethz.ch



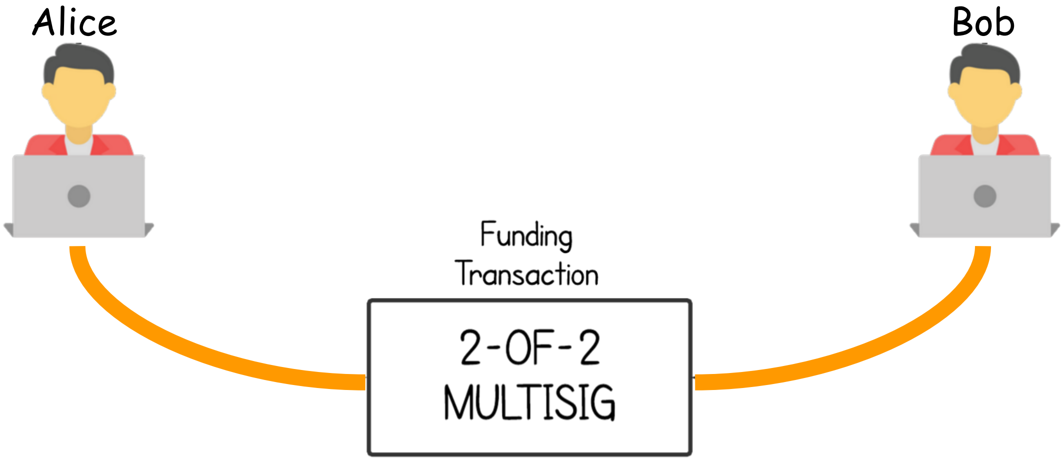
The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments

Joseph Poon
joseph@lightning.network

Thaddeus Dryja
rx@awsomnet.org

Lightning Network Background

Lightning Network Background



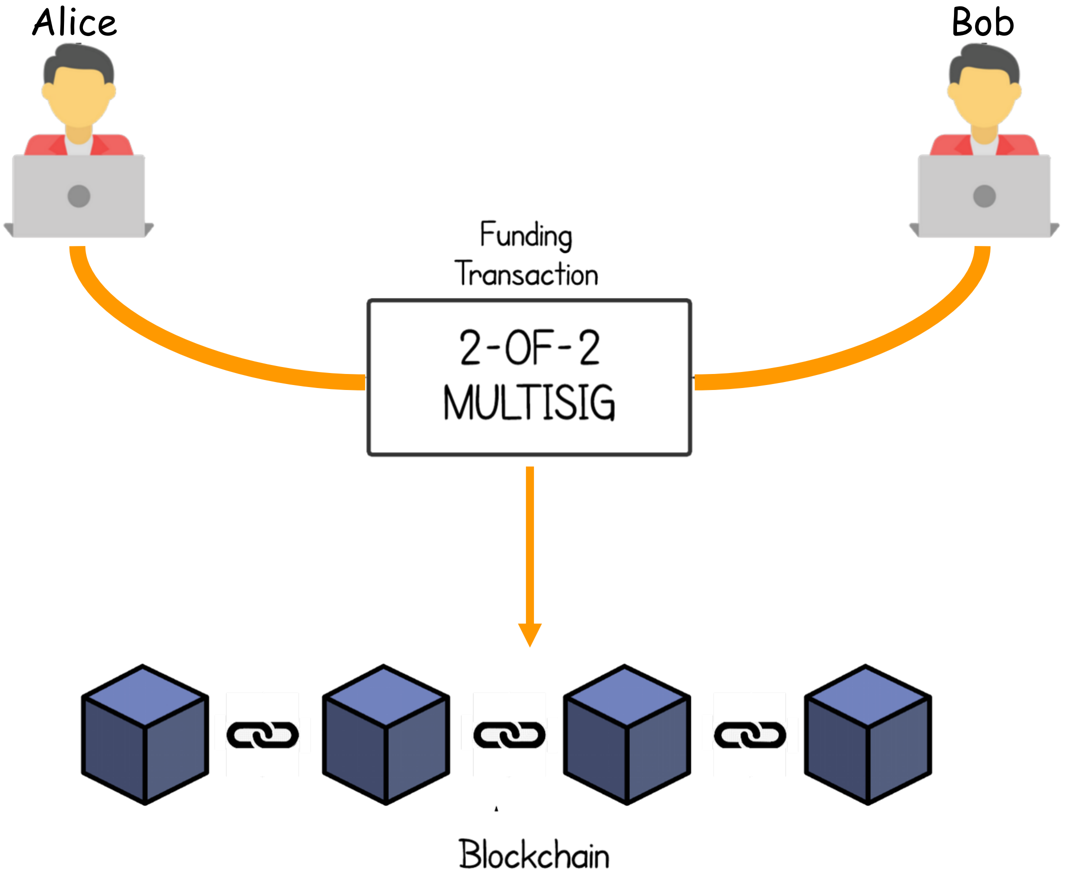
Alice

Bob

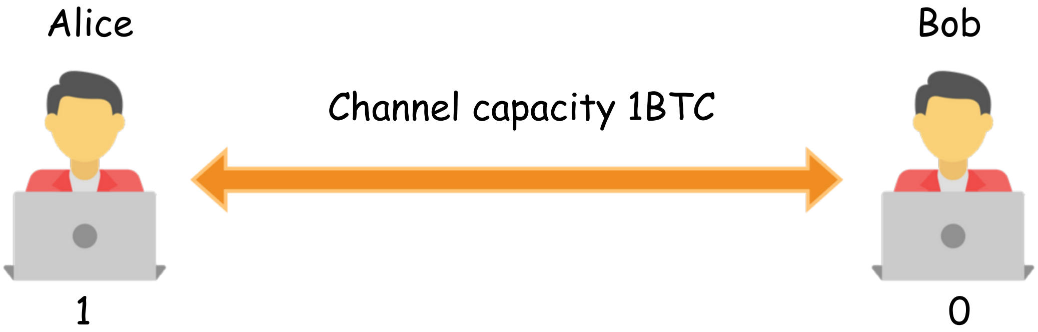
Funding Transaction

2-OF-2 MULTISIG

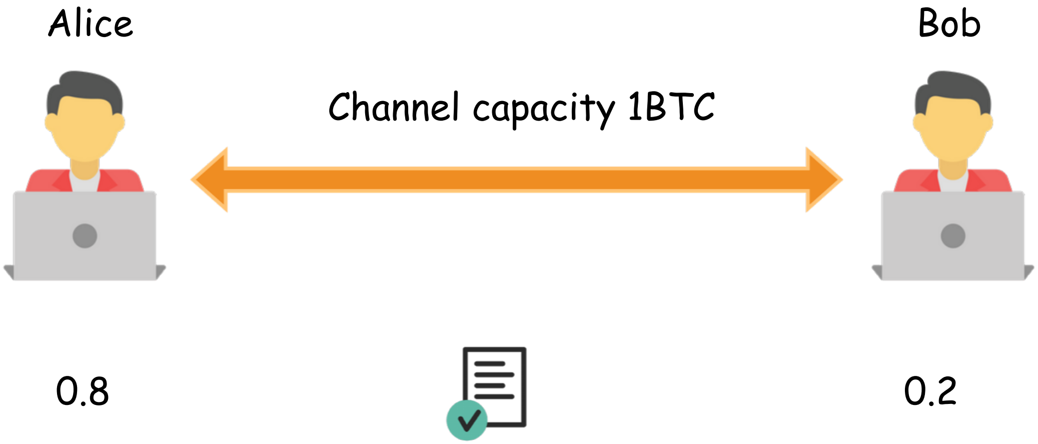
Lightning Network Background



Lightning Network Background



Lightning Network Background



Alice

Bob

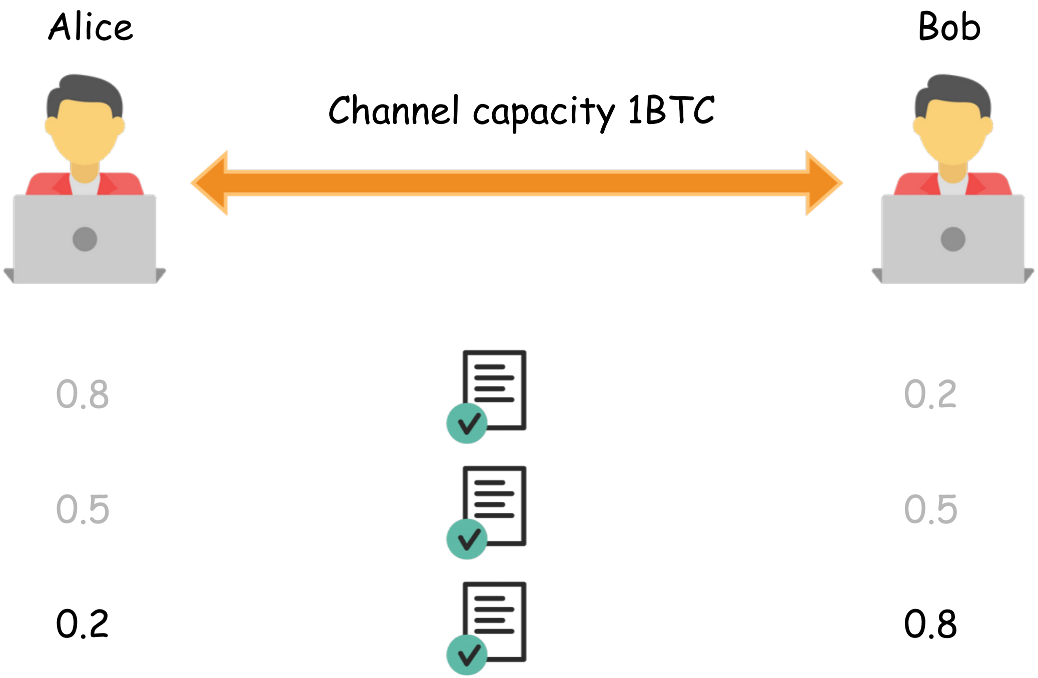
Channel capacity 1BTC

0.8

0.2

Off-Chain
Commitment Transactions

Lightning Network Background



Alice	Bob
0.8	0.2
0.5	0.5
0.2	0.8

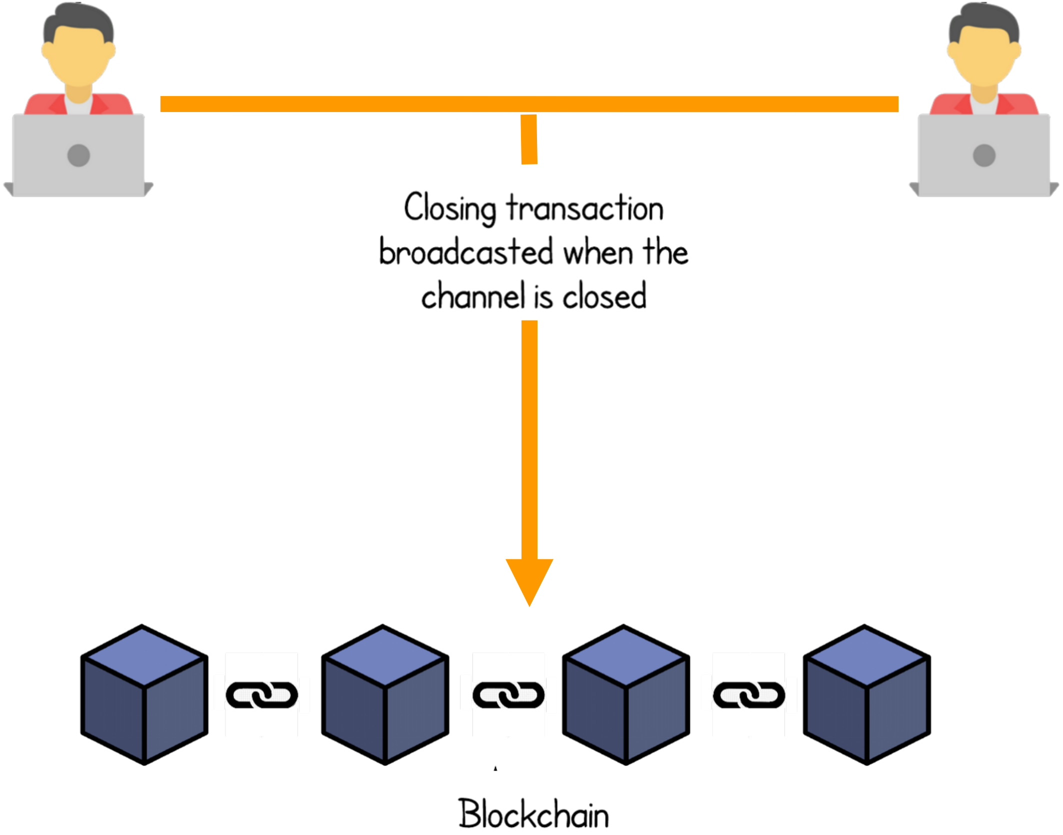
Channel capacity 1BTC

Off-Chain
Commitment Transactions

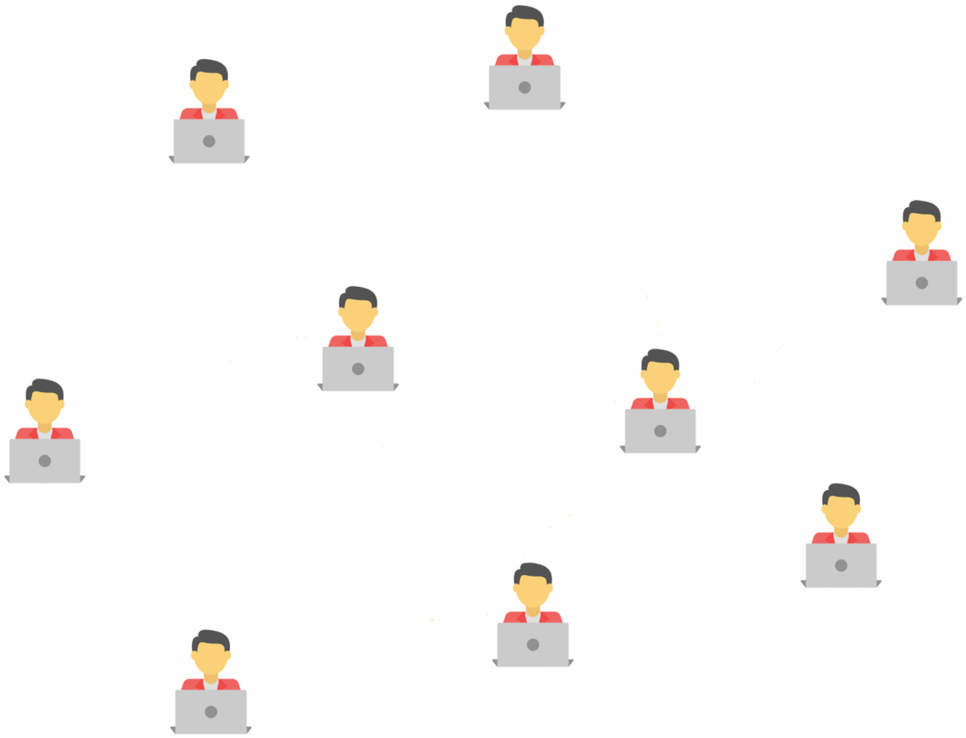
Lightning Network Background

Closing transaction

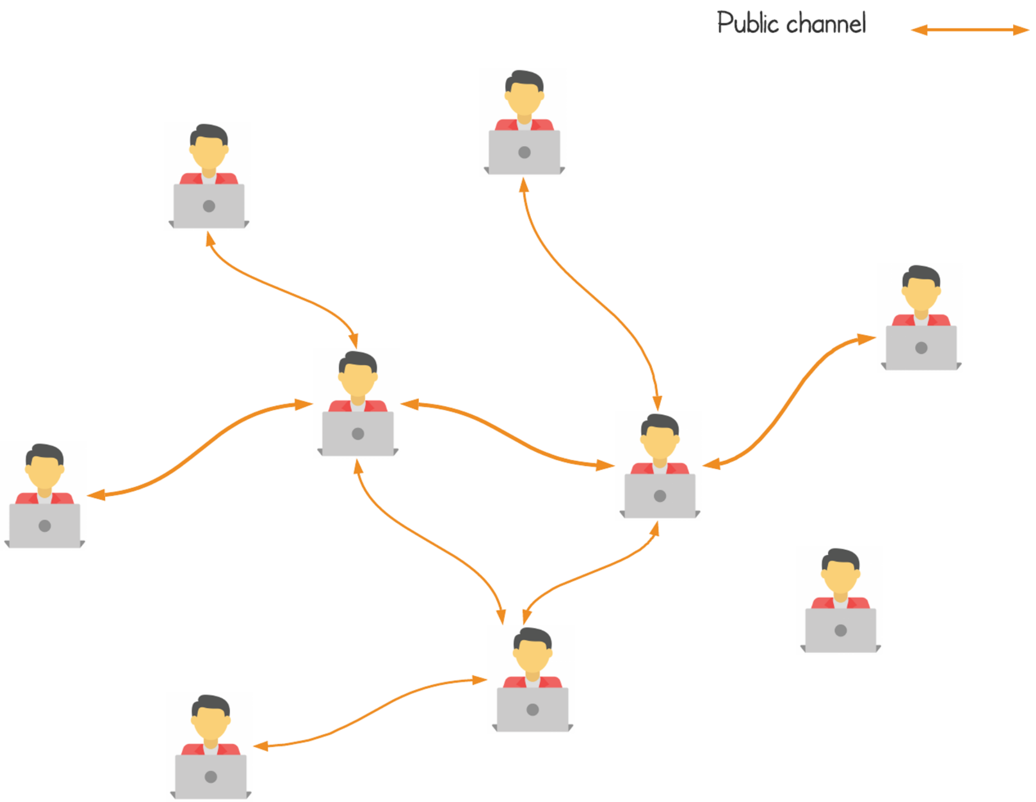
Lightning Network Background



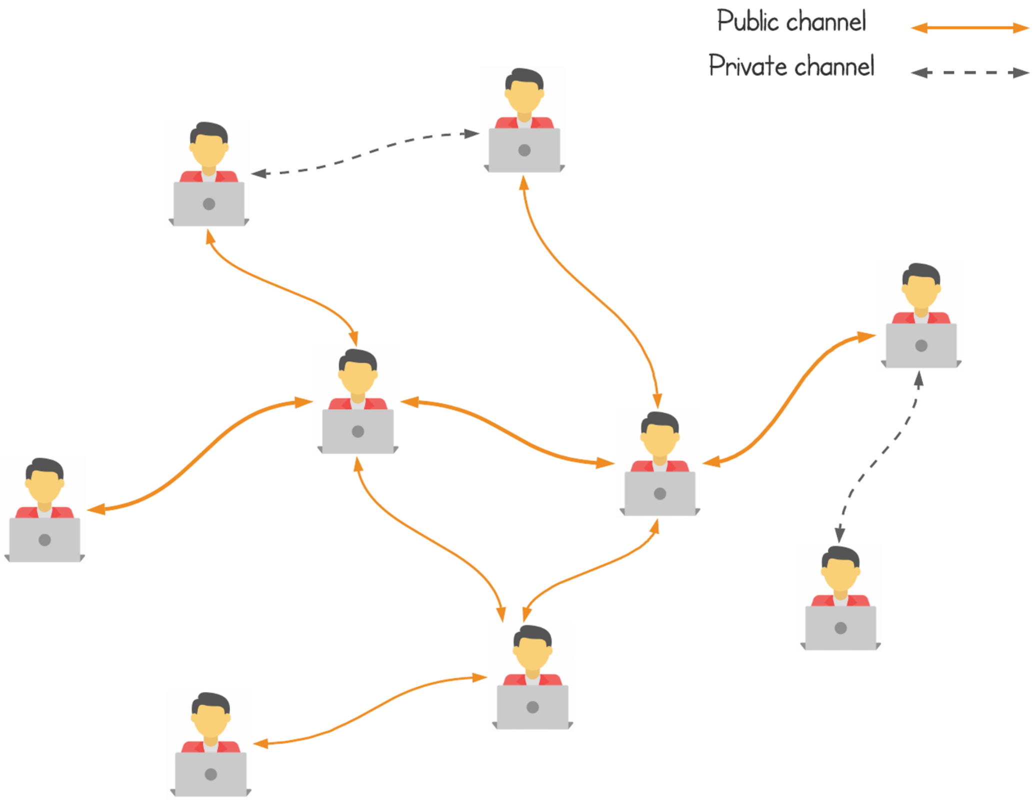
Lightning Network Background



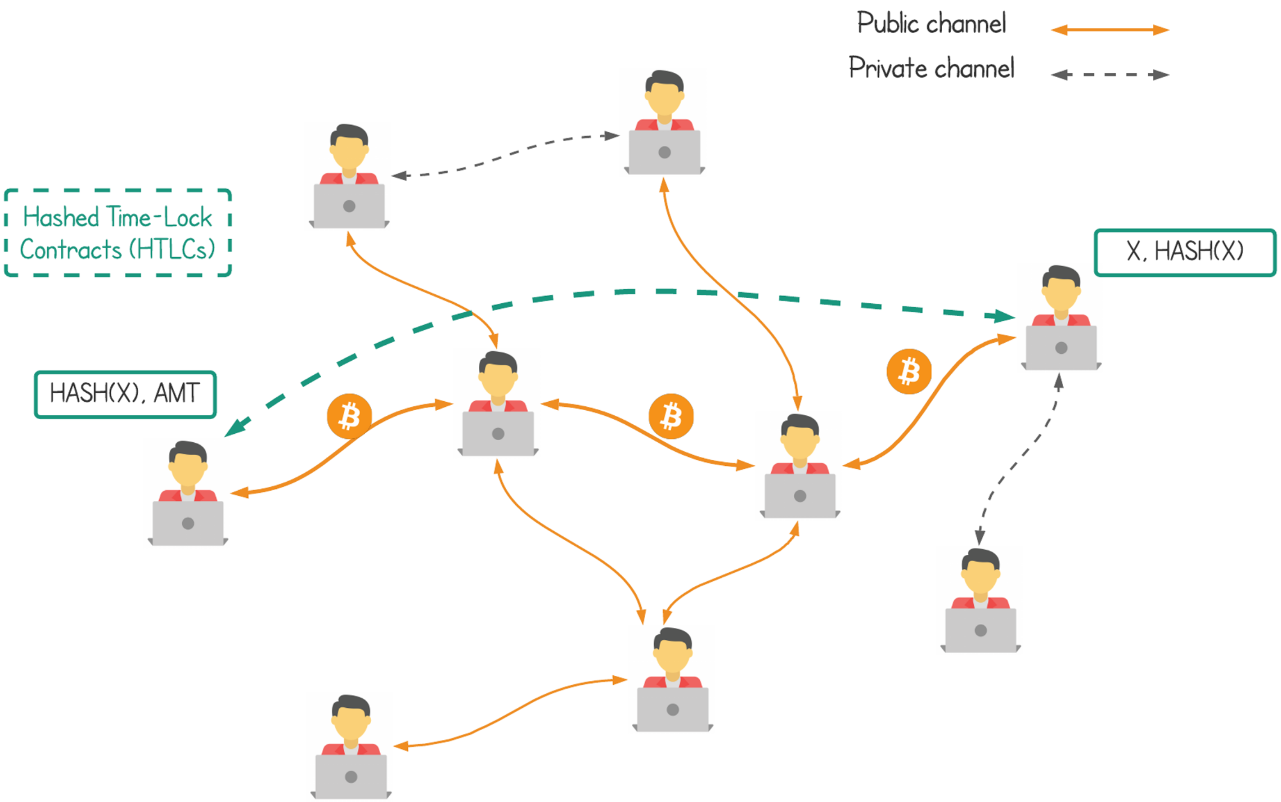
Lightning Network Background



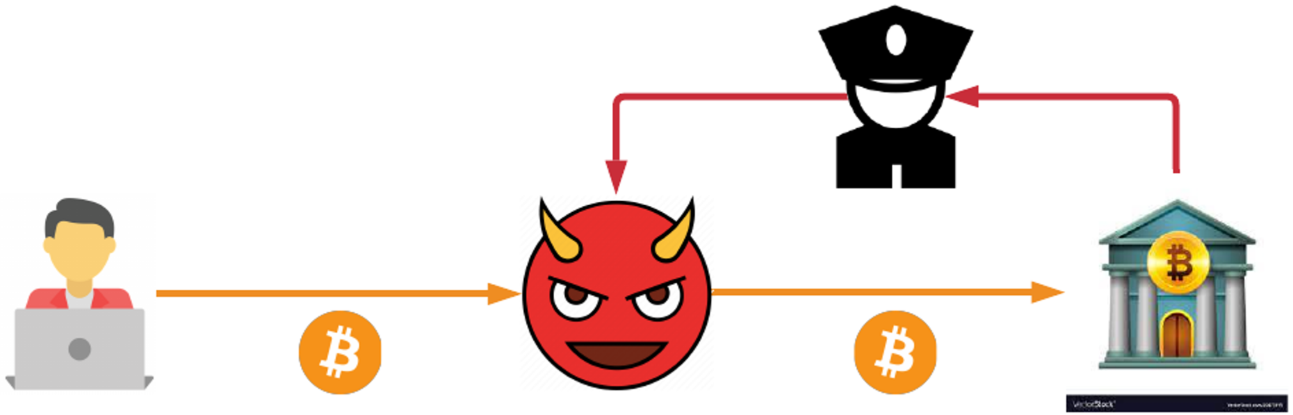
Lightning Network Background



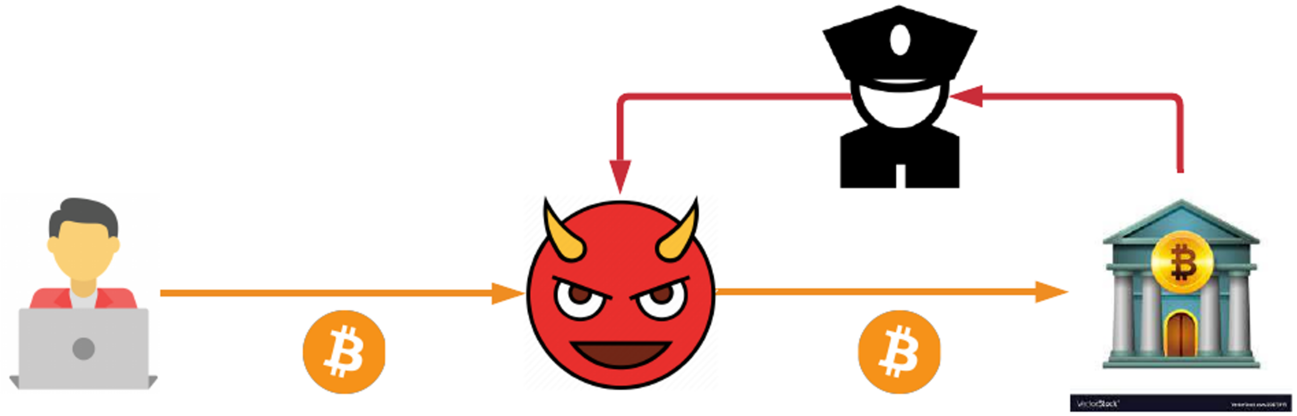
Lightning Network Background



Tracing illicit activities in Bitcoin

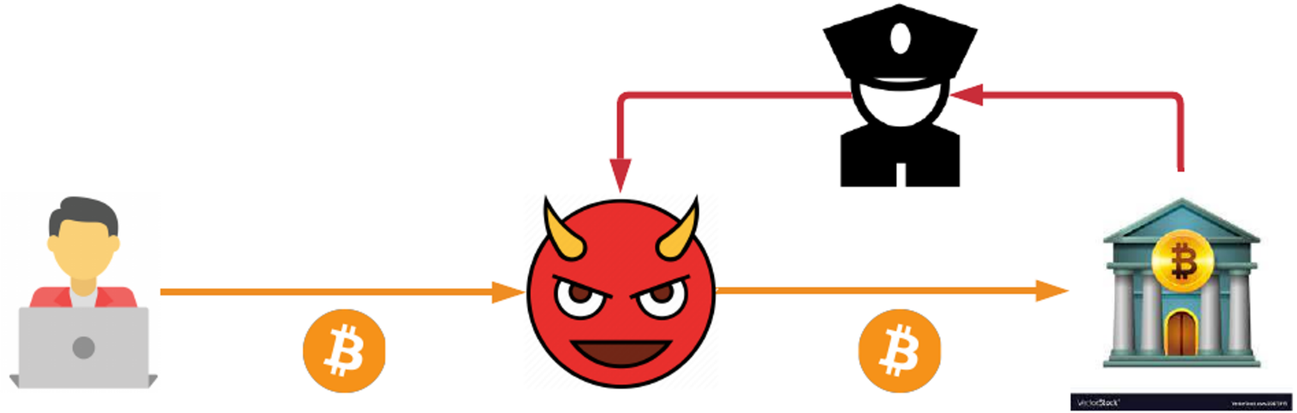


Tracing illicit activities in Bitcoin



1. Bob gets hacked by Eve and sends her ransomware

Tracing illicit activities in Bitcoin

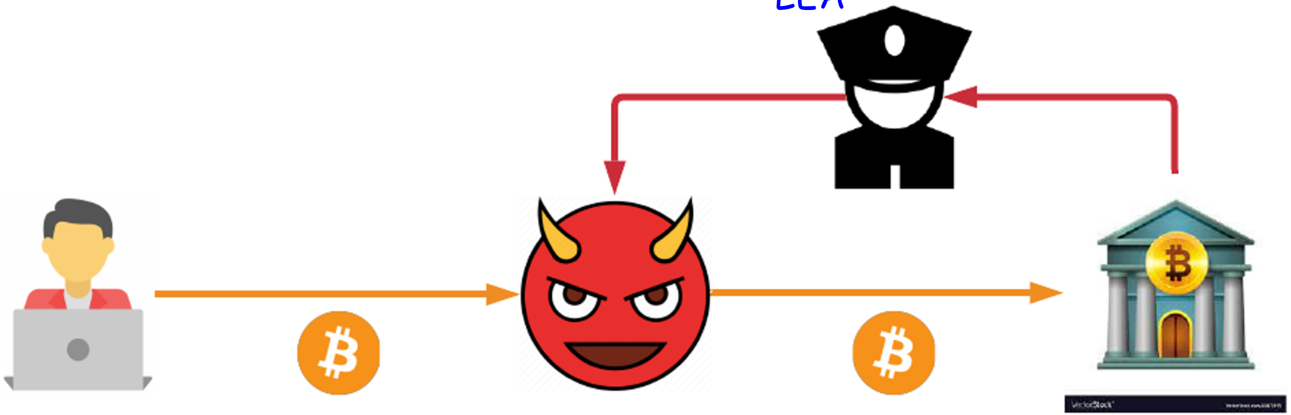


1. Bob gets hacked by Eve and sends her ransomware

2. Eve uses an exchange to monetize her coins

Tracing illicit activities in Bitcoin

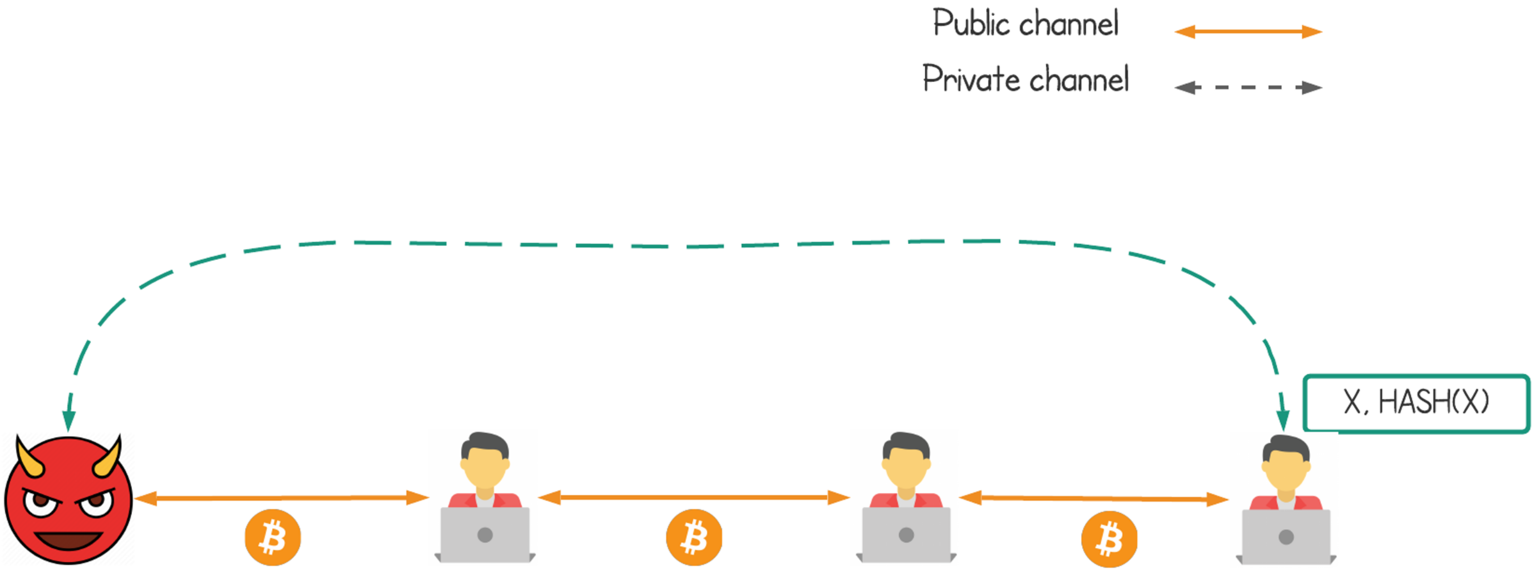
3. The exchange implemented AML policy and informed an LEA



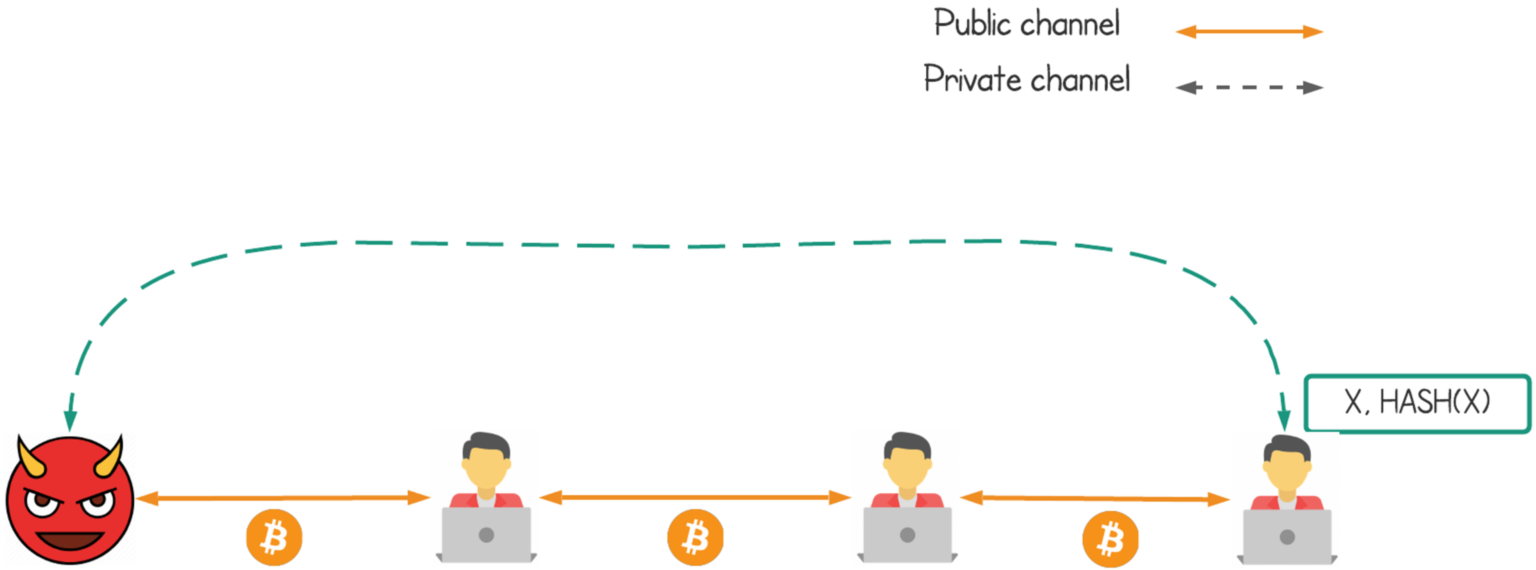
1. Bob gets hacked by Eve and sends her ransomware

2. Eve uses an exchange to monetize her coins

Tracing illicit activities in the Lightning Network

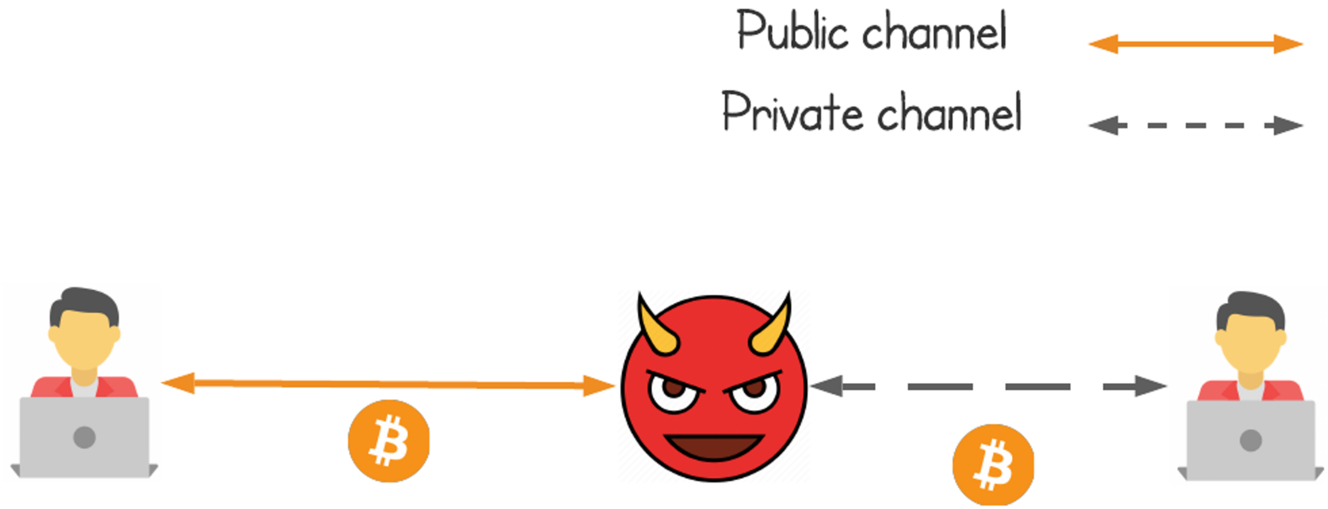


Tracing illicit activities in the Lightning Network



Who is the sender of this payment?

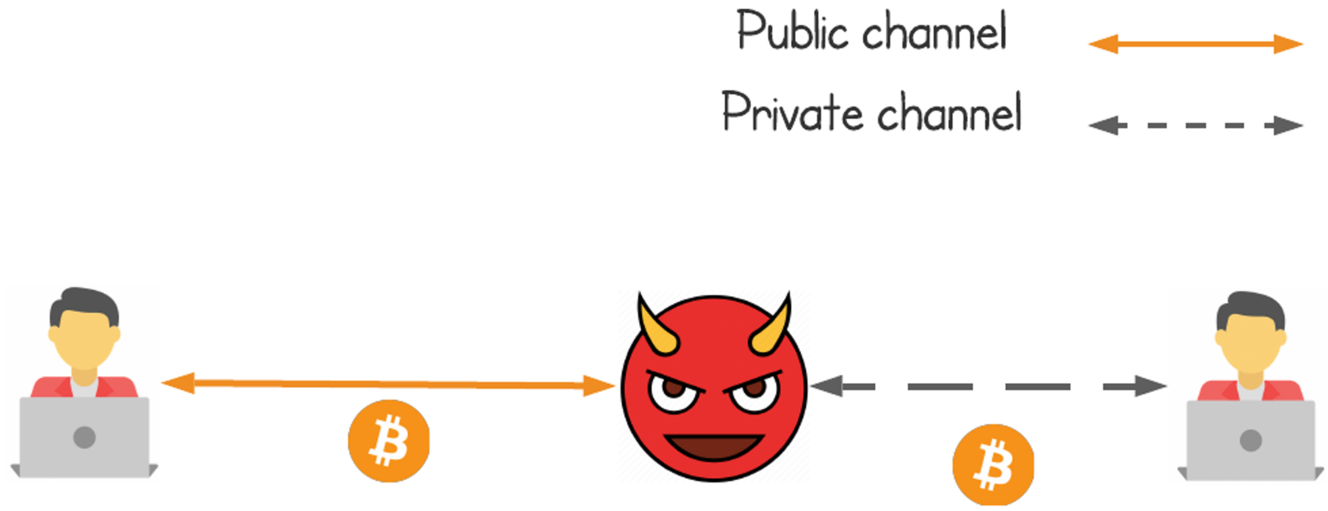
Tracing illicit activities in the Lightning Network



Public channel

Private channel

Tracing illicit activities in the Lightning Network



Public channel

Private channel

Who is interacting with Eve?

Lightning Network’s Privacy Properties

- Channels secrecy
- Third party balance secrecy
- Off-path payment privacy
- On-path relationship anonymity

Channels secrecy

Privacy properties of channels

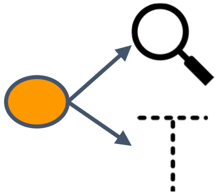
Public channel

- Everyone knows
- Known capacity
- Anyone can use it for routing
- User who takes funds is anonymous

Private channel

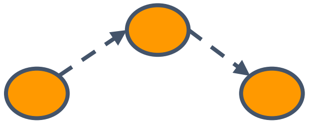
- Only participants know
- Hidden capacity
- Only participants/allowed third-parties can use
- User who takes funds is anonymous

Channel secrecy heuristics



Two heuristics
(Property & Tracing)

Property
77,245 closed private
channels

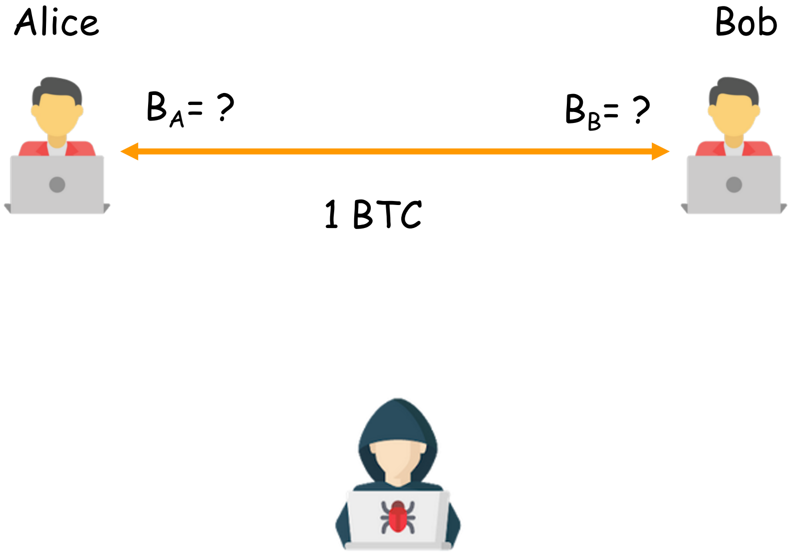


Tracing
27,183 channels
79.3% identified one
participant

Public
155k found opening node
143k found who got
closing funds

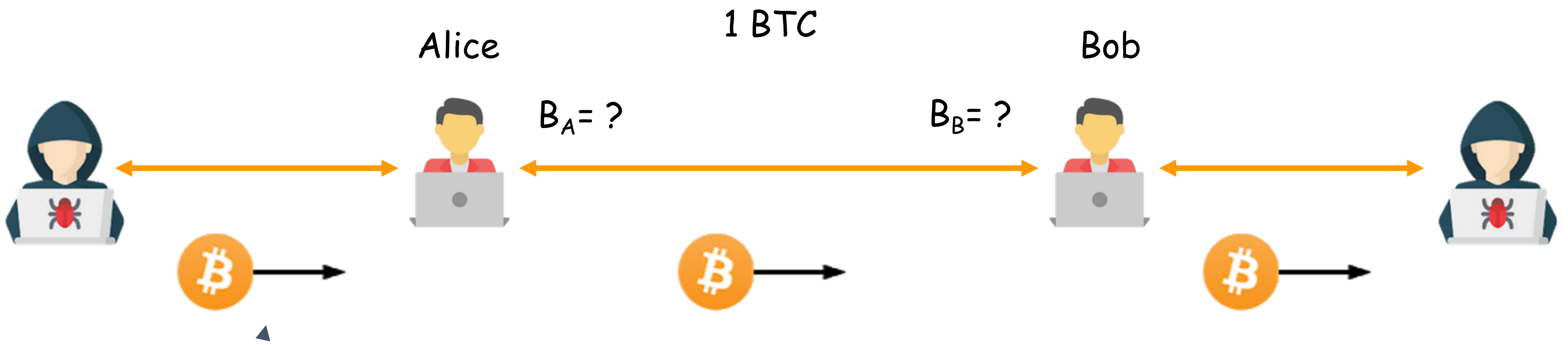
Third party balance secrecy

Third party balance secrecy



Third party balance secrecy

Generic balance inference attack



Route payment *amt* to attacker node with fake pre-image H

✓ Received pre-image, sufficient balance

✗ Repeat with binary search

Third party balance secrecy

Generic balance inference attack

Full *testnet* attack

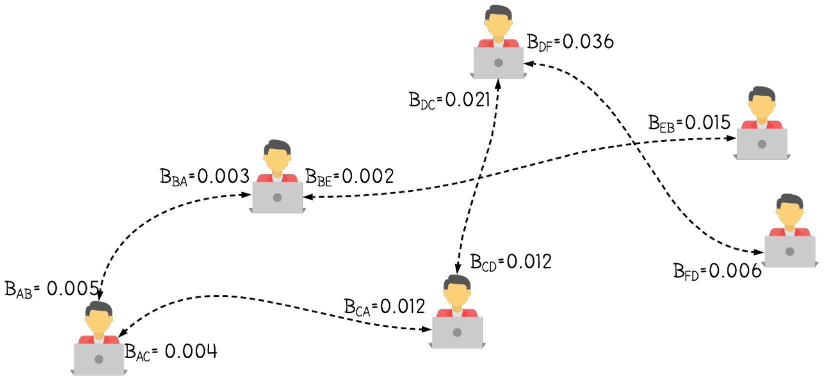
103 nodes, 1,017 channels

65% of the channels were one-sided

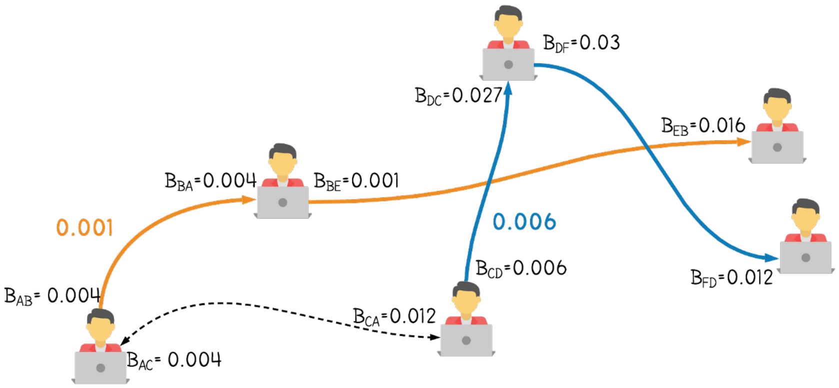
Attacker cost

Off-path payment privacy

Off-Path Payment Privacy



Snapshot 1
12:00

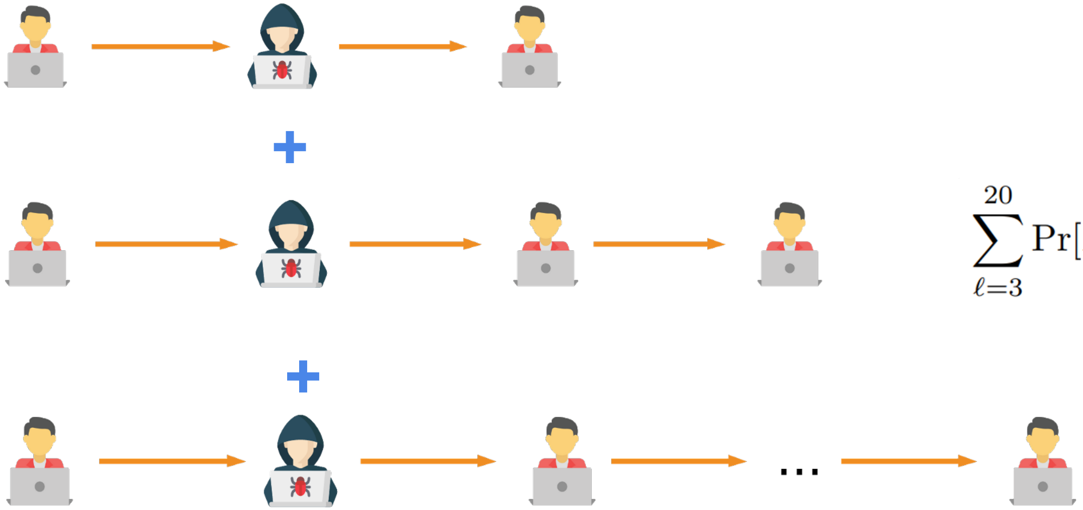


Snapshot 2
12:05

On-path relationship anonymity

On-Path Relationship Anonymity

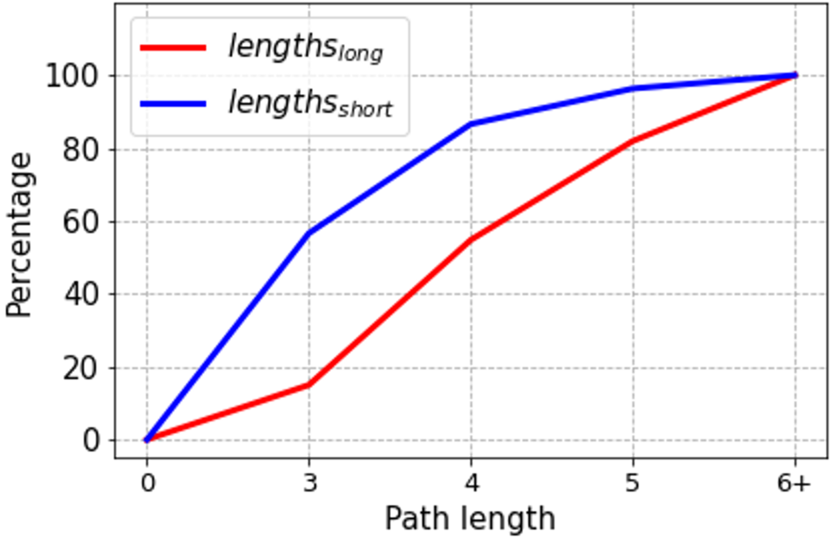
When does an intermediate node knows who the Sender is



$$\sum_{\ell=3}^{20} \Pr[L = \ell | \text{success}] \cdot \Pr[H = 1 | L = \ell, \text{success}]$$

Lightning Network Simulator

Average Lengths - How long is each path?

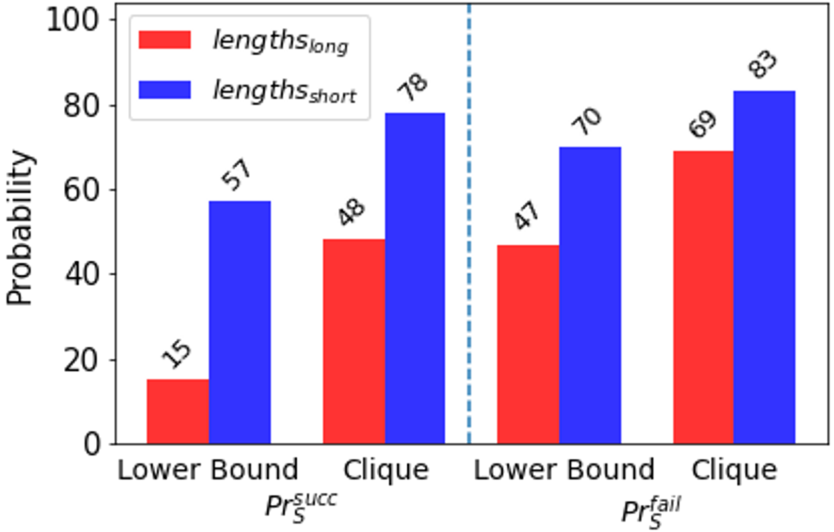


lengths$_{long}$: We maximize the lengths | **lengths$_{short}$** : We minimize the lengths

For **lengths$_{long}$** 14.98% of paths consist of only one hop.

In **lengths$_{short}$**, 56.65% of paths consisted of a single hop.

On-Path Relationship Anonymity - Results



In the worse case scenario the intermediate now has a 14.98% probability of being right

In the best case scenario, where paths are short, failures happen oftenly and the nodes in a path form a clique the probability is 83% !

Summary and Keypoints

- Private channels → Property & Tracing Heuristics
- Third party balance secrecy → Balance inference attacks
- Off-path payment privacy → Payment detection attack
- On-path relationship anonymity → Path discovery attack

Contact: g.kappos@ucl.ac.uk h.yousaf@ucl.ac.uk

THE END

UCL

THANK YOU

QUESTIONS?

Contact: g.kappos@ucl.ac.uk h.yousaf@ucl.ac.uk