Security and Privacy of Bitcoin's *Lightning Network*

UNIVERSITÉ DU LUXEMBOURG

Prince Yaw Gharbin
Yann Hoffmann
Supervisor: Sergei Tikhomirov

Table of contents

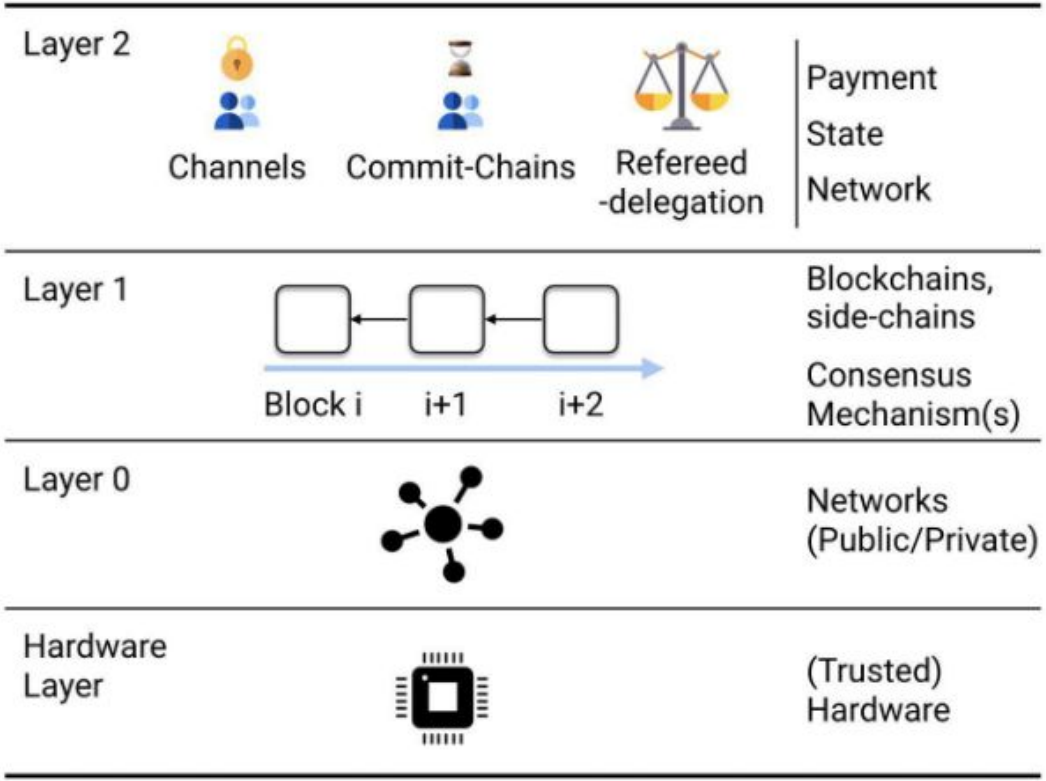
Introduction: Bitcoin

Bitcoin is a collection of rules and software specifications that enables distributed networks to conduct transactions anonymously and irreversibly.

- Bitcoin relies on the **blockchain** consensus mechanism to validate transactions.

- Bitcoin comes with a significant speed constraint (1MB + 10min):
  - *SWIFT* → 33.6 million per day
  - *Bitcoin* → 604,800 per day, 55 times less

- **Lightning Network** addresses the problem of speed and capacity by letting users settle transactions among themselves in trustless off-chain channels.



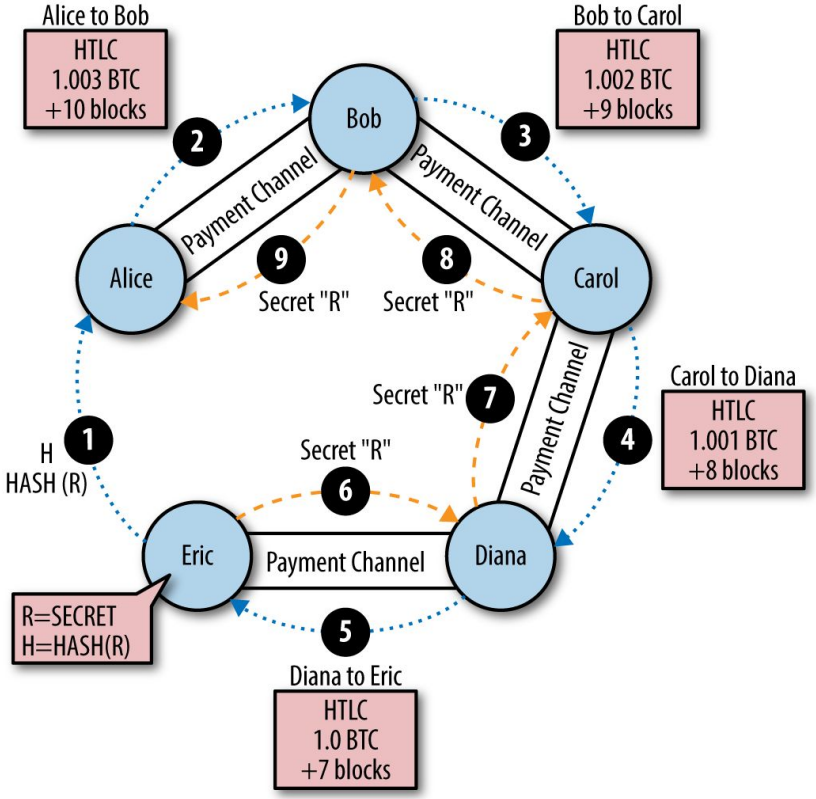
SoK: Layer-Two Blockchain Protocols Lewis Gudgeon et alii

Scaling Bitcoin?

The Lightning Network

1. Two nodes can create a channel by committing BTC to a **shared address**.
2. Two characteristics: **capacity** and **distribution of funds**.
3. A payer and payee can then transact together even if they do not share a channel by **rerouting** through Lightning.
4. Lightning resorts to the blockchain only in case of **disputes**.
5. Lightning Network then becomes independent from the blockchain and unlocks the transfer rates.

Payment Channels



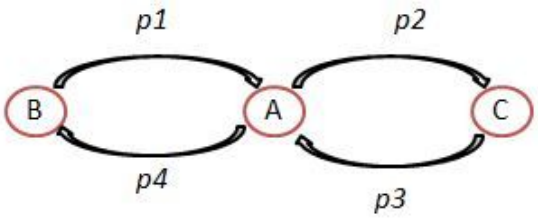
Key features:

- Privacy
- Speed
- Capacity
- Flexibility
- Security

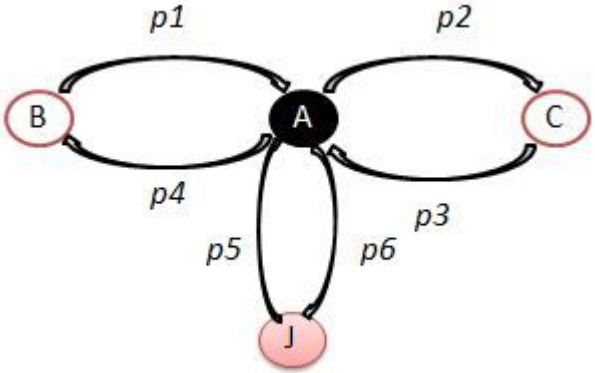
New Security Threats

1. Lockdown
2. Eclipse
3. Probing

- ➔ Victim **A** is a hub between two users, **B** and **C**.
- ➔ Capacity values ***AB = p1 + p4***.
- ➔ Capacity values ***AC = p2 + p3*** being ***pi*** the balances in each direction for each channel.
- ➔ Objective of adversary James (J) is to disrupt the availability of **A** by either blocking incoming links or outgoing ones.
- ➔ By rendering ***p1 = 0*** and ***p3 = 0*** or ***p2 = 0*** and ***p4 = 0***

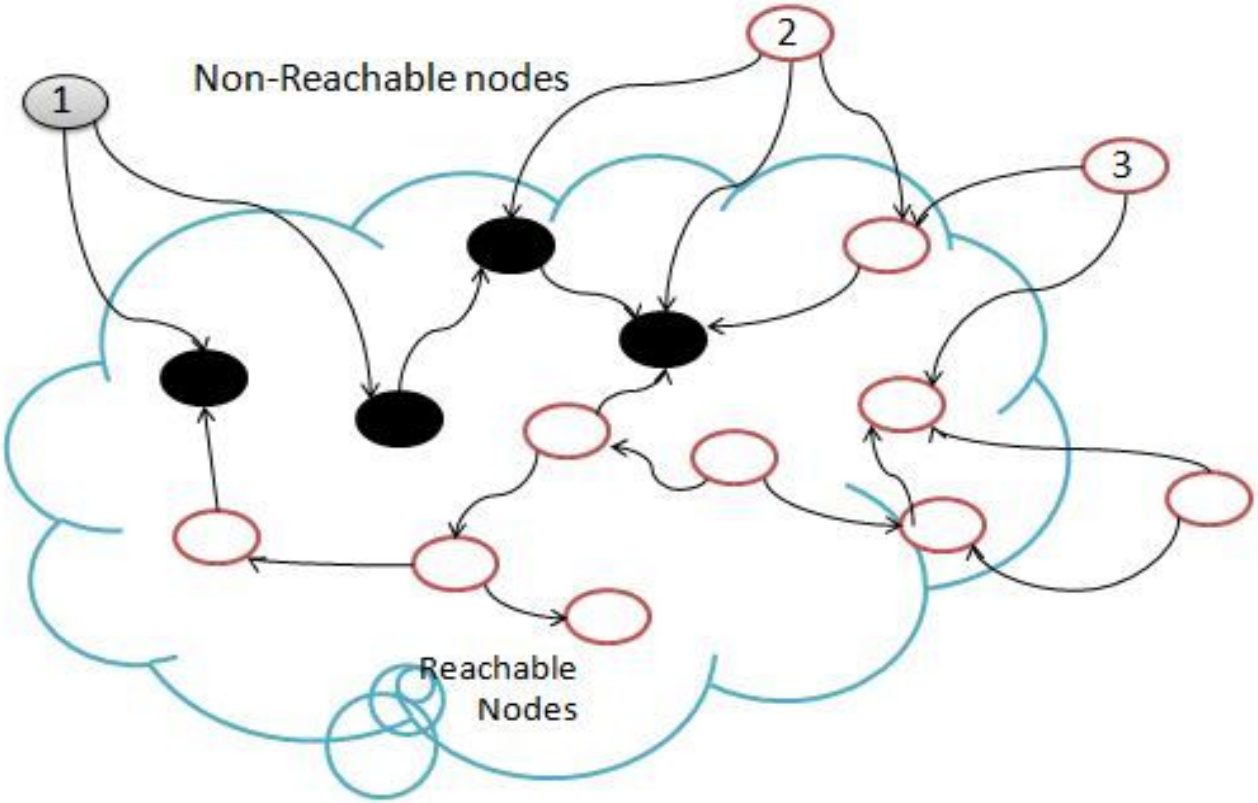


Scenario 1

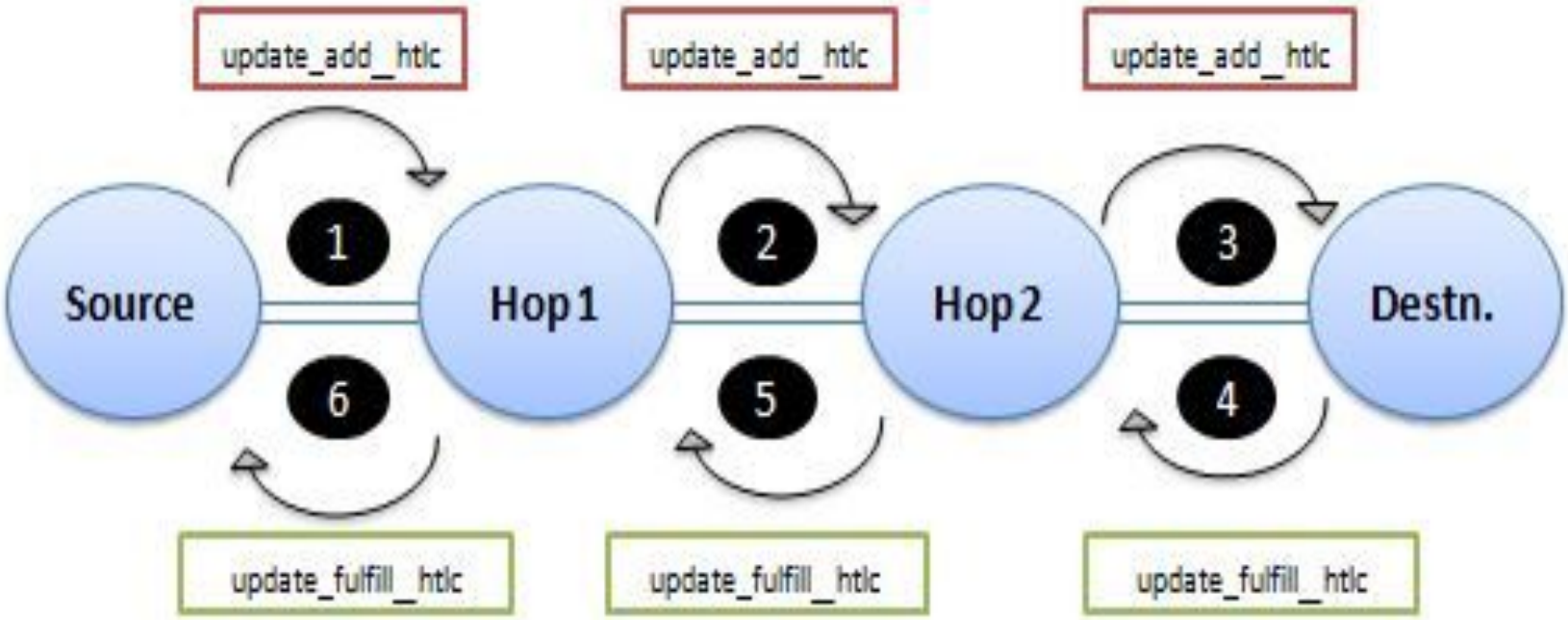


Scenario 2

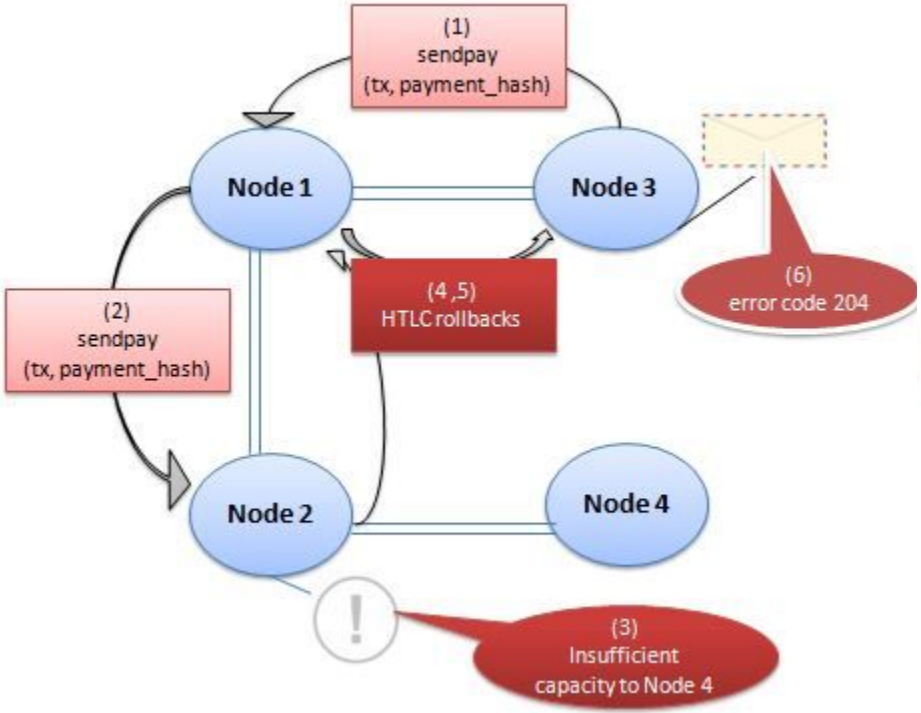
Lockdown Attack



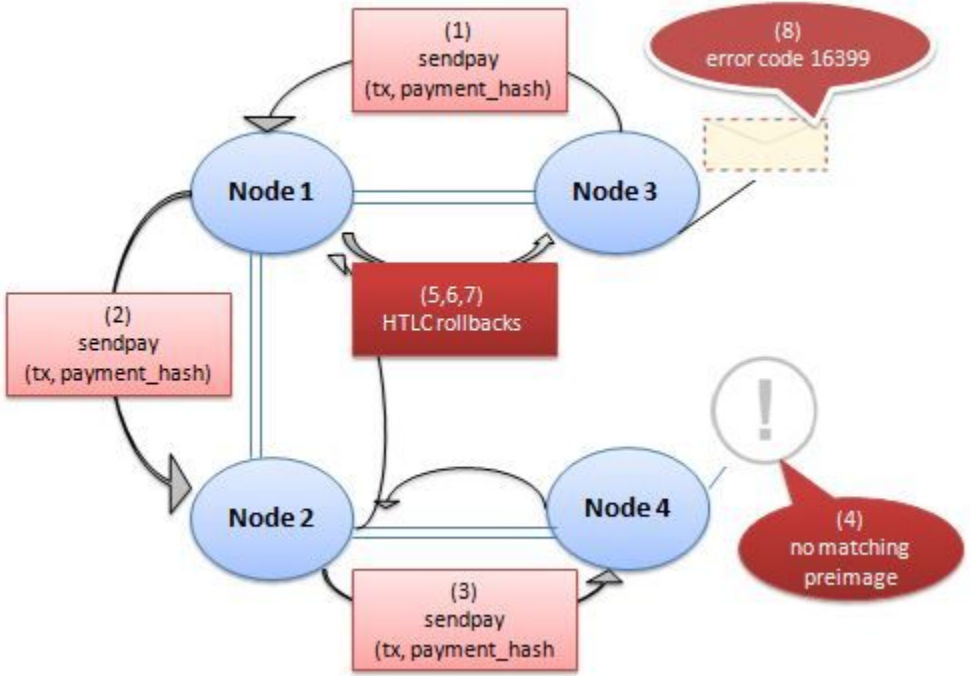
Eclipse attack: Only node 1 is eclipsed because all of its connections lead to the attacker.



Lightning Channel: Probing attack



Error 204

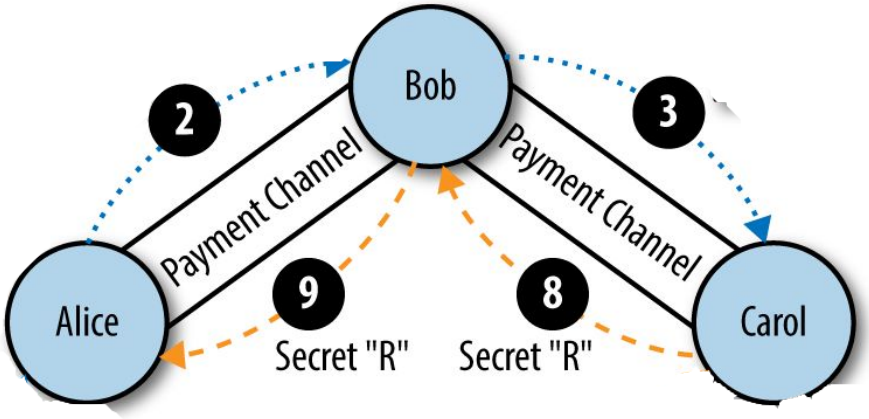


Error 16399

Probing attack in practice

Walkthrough:

- Setting up a route {attack, intermediary, node, target}
- Binary search



Epsilon (msat):	10	100	1000	10000
Nb. of iterations	27	23	20	17
Convergence (msat)	153,890,003	153,889,988	153,889,845	153,890,990
Probe #1 (s)	42.991	44.291	32.674	29.092
Probe #2 (s)	43.243	39.725	31.589	31.745
Probe #3 (s)	47.818	41.849	32.375	31.538
Probe #4 (s)	46.289	37.218	36.379	33.076
Probe #5 (s)	44.44	34.29	37.111	31.742
Mean probe duration (s)	1.67	1.72	1.70	1.85

Experimental Results

References

- U. Nisslmueller, K.-T. Foerster, S. Schmid & C. Decker – "Toward active and passive confidentiality attacks on cryptocurrency off-chain networks", *arXiv preprint arXiv:2003.00003* (2020).
- C. Pérez-Solà, A. Ranchal-Pedrosa, J. Herrera-Joancomartí, G. Navarro-Arribas & J. Garcia-Alfaro – "Lockdown: Balance availability attack against lightning network channels", in *International Conference on Financial Cryptography and Data Security*, Springer, 2020, p. 245–263.
- A. Riard & G. Naumenko – "Time-dilation attacks on the lightning network", *arXiv preprint arXiv:2006.01418* (2020).