

Revelio: A Network-Level Privacy Attack in the Lightning Network

Theo von Arx

Muoi Tran

Laurent Vanbever

July 6, 2023

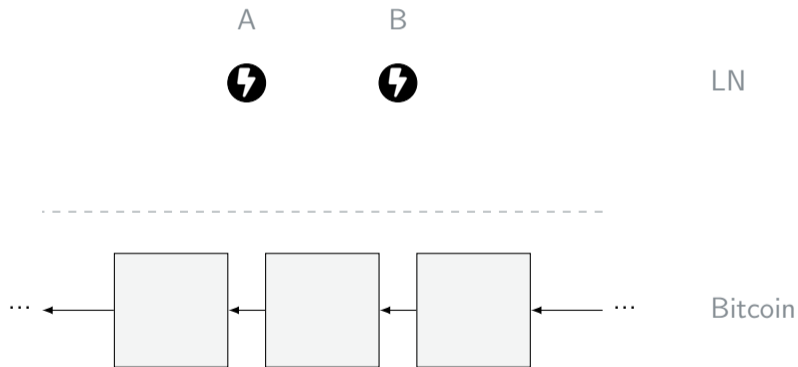
Sometimes a change of perspective is all it takes to see the light.

– Dan Brown, *The Lost Symbol*

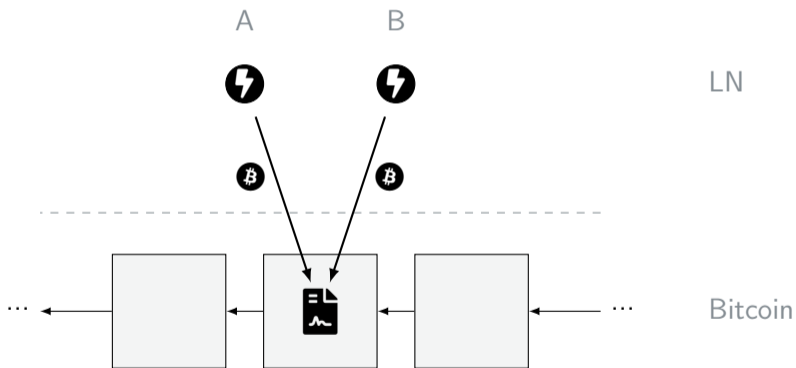
Sometimes a change of perspective is all it takes to see the lightning network payments.

| from application to network

The Lightning Network (LN) enables **faster** Bitcoin payments



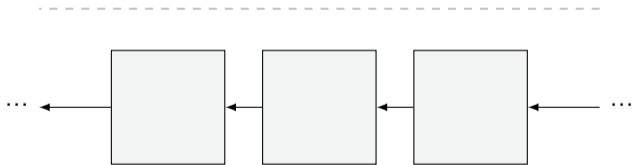
The Lightning Network (LN) enables **faster** Bitcoin payments



The Lightning Network (LN) enables **faster** Bitcoin payments



LN



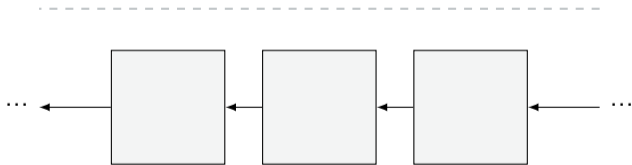
Bitcoin

The Lightning Network (LN) enables **faster** Bitcoin payments



LN

fast (ms)



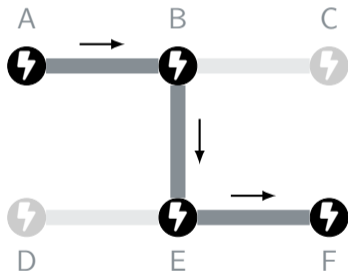
Bitcoin

slow (h)

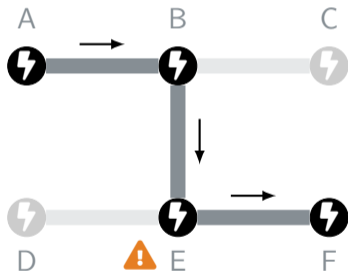
LN provides **anonymity** for **single-hop** payments



LN provides **anonymity** for **multi-hop** payments

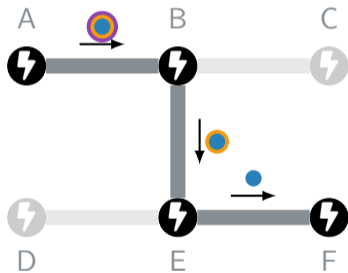


LN provides **anonymity** for **multi-hop** payments

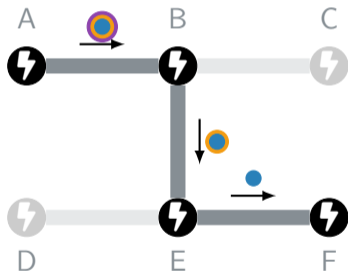


Intermediate nodes could learn endpoints

LN provides **anonymity** for **multi-hop** payments

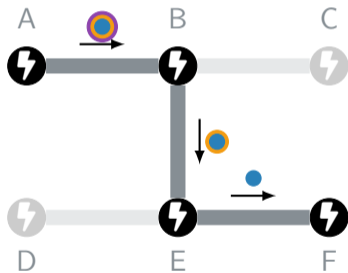


LN provides **anonymity** for **multi-hop** payments



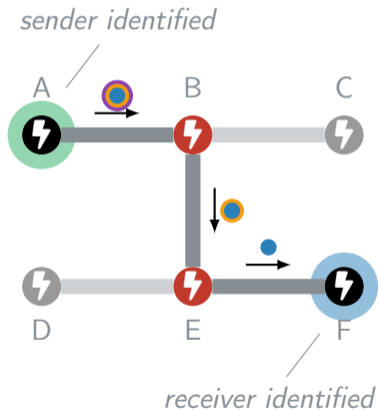
No one can learn the **sender** or the **receiver** of a payment

LN uses **Onion Routing** for anonymous multi-hop payments

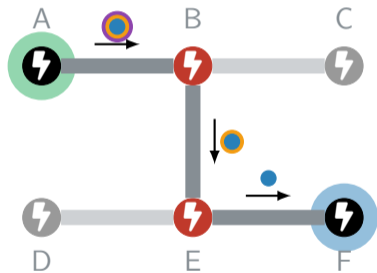


except the sender
No one can learn the **sender**
or the **receiver** of a payment

Colluding intermediate nodes can still deanonymize payments



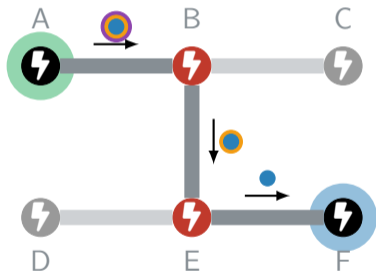
Colluding nodes need to be in a **central position**



Rohrer et al. 2020 30 top central nodes

Sharma et al. 2023 100 top central nodes

Colluding nodes need to be in a **central position**



Rohrer et al. 2020 30 top central nodes

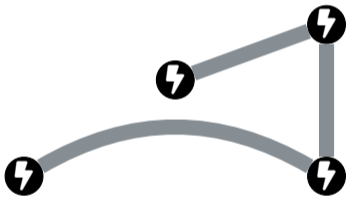
Sharma et al. 2023 100 top central nodes

... require additional **visible attacks**

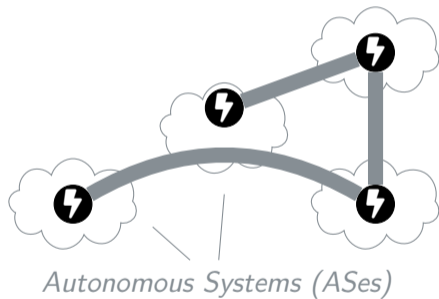
Can we deanonymize payments
without controlling central nodes?

Can we deanonymize payments
without controlling ~~central~~ any node?

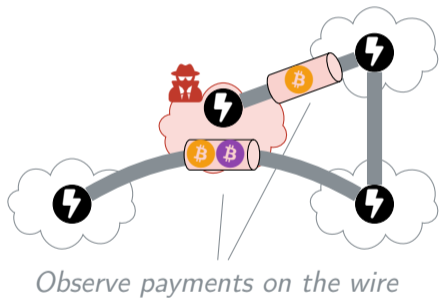
Revelio is a [network-level](#) deanonymization attack



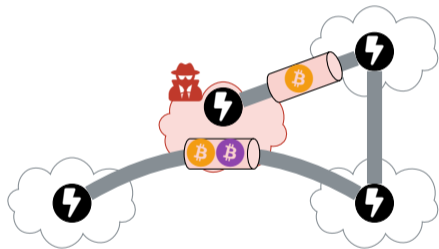
Revelio is a **network-level** deanonymization attack



Revelio is a **network-level** deanonymization attack



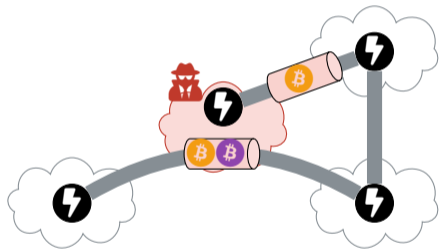
Revelio is a **network-level** deanonymization attack



Prior Attacks

Revelio

Revelio is a **network-level** deanonymization attack



Network traffic

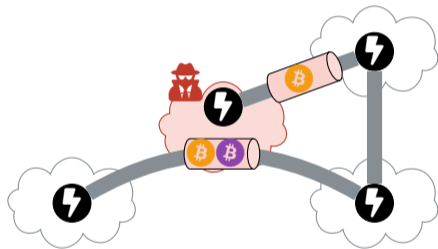
Prior Attacks



Revelio



Revelio is a **network-level** deanonymization attack



Network traffic

Message content

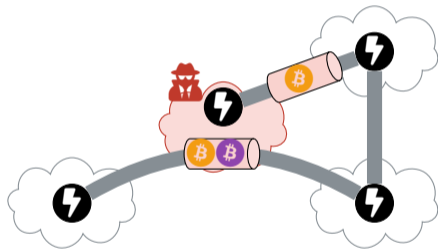
Prior Attacks









Revelio



Revelio is a **network-level** deanonymization attack

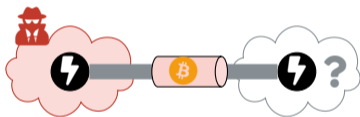


	Prior Attacks	Revelio
Network traffic		
Message content		
P2P topology		

A network-level deanonymization attack is **challenging**

Hidden nodes

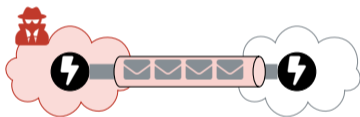
70% have no public IP address



A network-level deanonymization attack is **challenging**

Hidden nodes

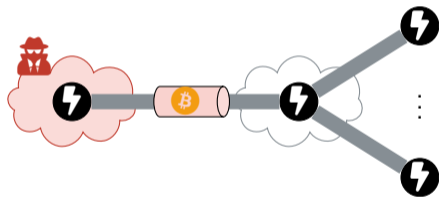
70% have no public IP address



Noisy, encrypted traffic

Payment-related packets mixed with others

A network-level deanonymization attack is **challenging**



Hidden nodes

70% have no public IP address

Noisy, encrypted traffic

Payment-related packets mixed with others

Huge anonymity set

17'600 nodes (as of 2022)

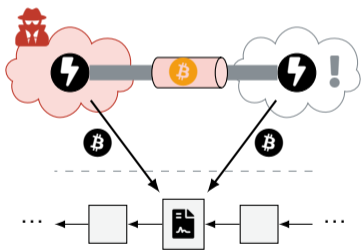
Revelio adversaries can [address](#) these challenges

Hidden nodes

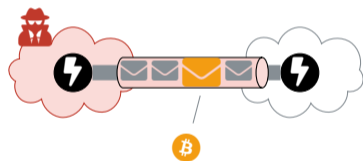
Identify using their network traces

Noisy, encrypted traffic

Huge anonymity set



Revelio adversaries can **address** these challenges



Hidden nodes

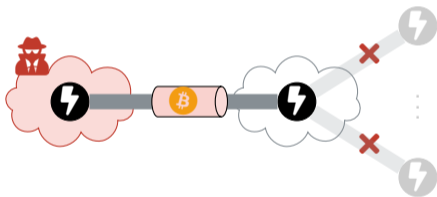
Identify using their network traces

Noisy, encrypted traffic

Filter messages with specific length

Huge anonymity set

Revelio adversaries can [address](#) these challenges



Hidden nodes

Identify using their network traces

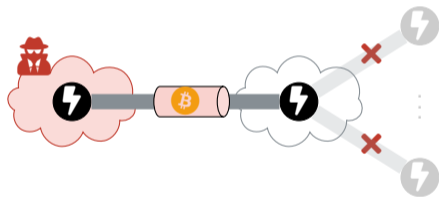
Noisy, encrypted traffic

Filter messages with specific length

Huge anonymity set

Combine network and P2P topology

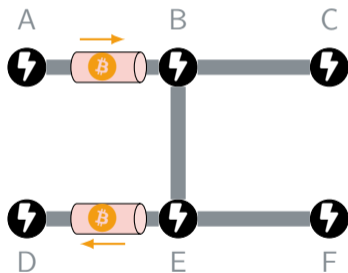
Revelio adversaries can [address](#) these challenges



Huge anonymity set

Combine network and P2P topology

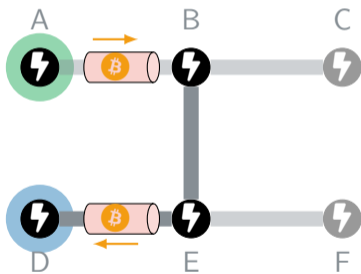
Revelio in a simple example



Sender anonymity set: A B C D E F

Receiver anonymity set: A B C D E F

Revelio in a simple example

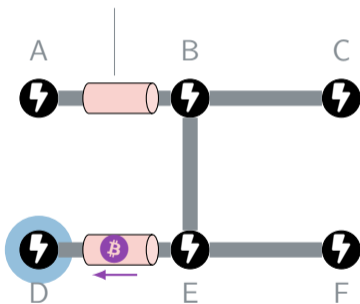


Sender anonymity set: A B C D E F

Receiver anonymity set: A B C D E F

Revelio in a **more complex** example

nothing observed

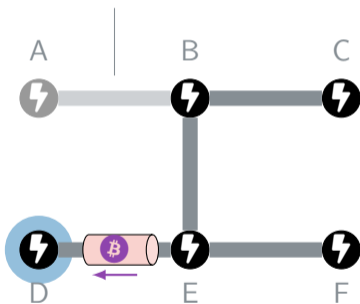


Sender anonymity set: A B C ~~D~~ E F

Receiver anonymity set: ~~A~~ ~~B~~ ~~C~~ D ~~E~~ ~~F~~

Revelio in a **more complex** example

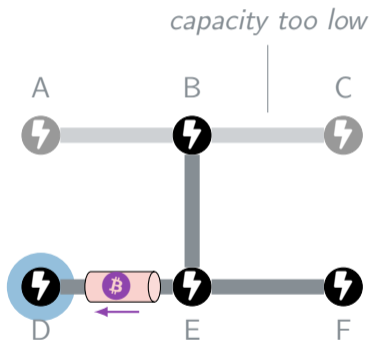
nothing observed



Sender anonymity set: $A B C \bar{D} E F$

Receiver anonymity set: $A \bar{B} \bar{C} D \bar{E} \bar{F}$

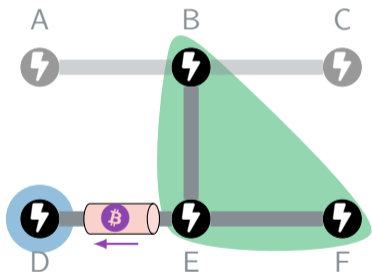
Revelio in a **more complex** example



Sender anonymity set: A B ~~C~~ D E F

Receiver anonymity set: A ~~B~~ C D ~~E~~ F

Revelio in a more complex example



Sender anonymity set: A B C D E F

Receiver anonymity set: A B C D E F

We evaluate Revelio using large-scale [simulations](#)

Captured snapshot of [LN topology](#)
consisting of 18K nodes & 81K channels

We evaluate Revelio using large-scale **simulations**

Captured snapshot of **LN topology**
consisting of 18K nodes & 81K channels

Simulated AS-level **Internet routing**
of 1000 randomly crafted LN payments

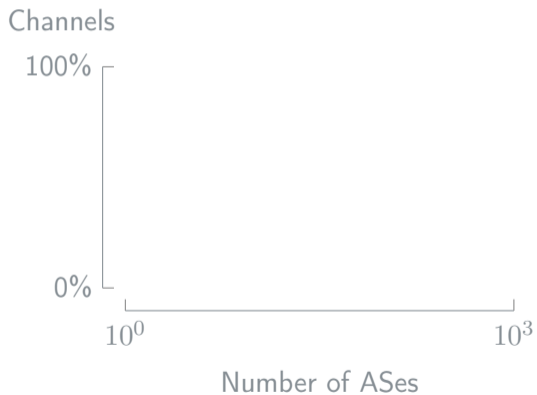
We evaluate Revelio using large-scale **simulations**

Captured snapshot of **LN topology**
consisting of 18K nodes & 81K channels

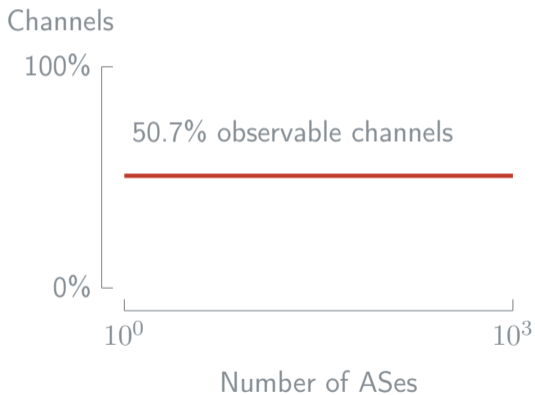
Simulated AS-level **Internet routing**
of 1000 randomly crafted LN payments

Emulated **deanonymization attack**
for the top ASes observing most channels

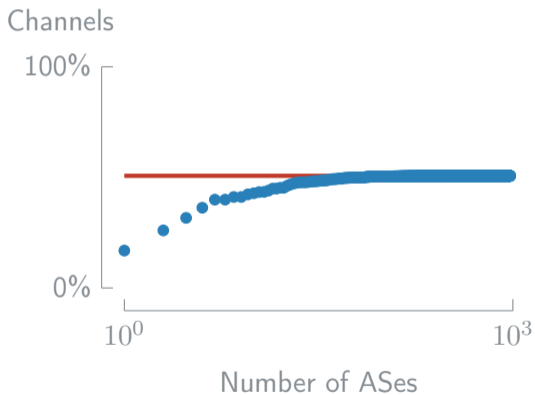
LN is centralized at the network level



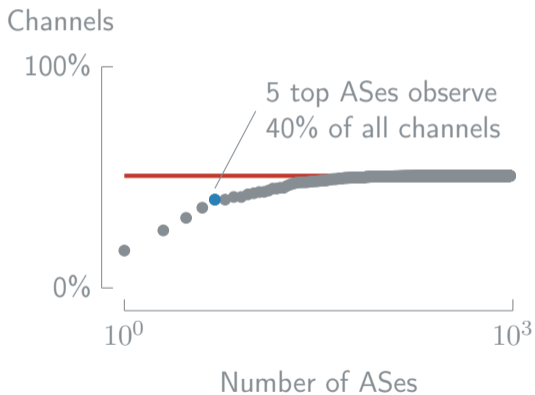
LN is centralized at the network level



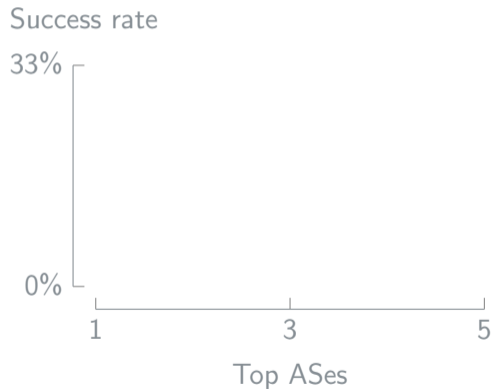
LN is centralized at the network level



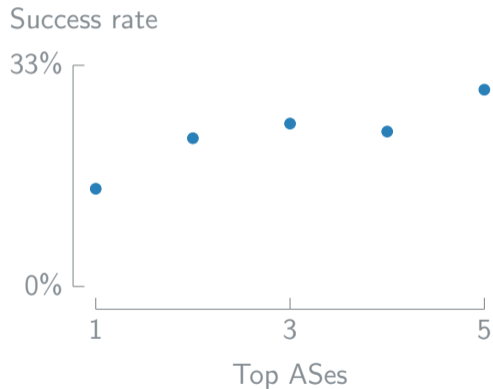
LN is centralized at the network level



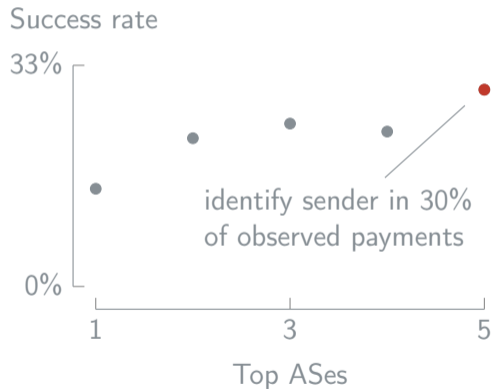
Revelio **deanonymizes a third** of the endpoints of observed payments



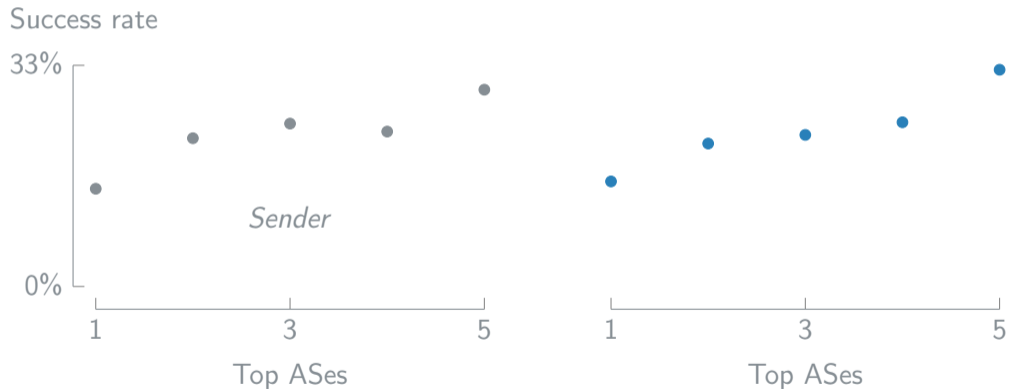
Revelio **deanonymizes a third** of the endpoints of observed payments



Revelio **deanonymizes a third** of the endpoints of observed payments



Revelio [deanonymizes a third](#) of the endpoints of observed payments



Revelio **deanonimizes a third** of the endpoints of observed payments

Success rate

33%

0%

1

3

5

Top ASes

Sender

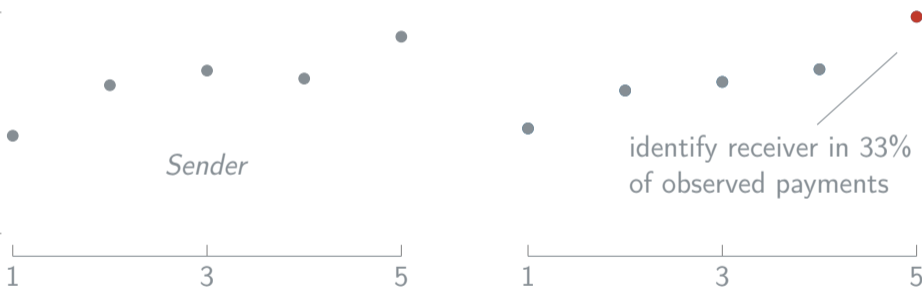
1

3

5

Top ASes

identify receiver in 33%
of observed payments



Revelio requires [countermeasures](#) on multiple layers

Network level

Use Tor/VPN to avoid adversarial ASes

Revelio requires **countermeasures** on multiple layers

End-to-end communication

Random padding to hide message types

Network level

Use Tor/VPN to avoid adversarial ASes

Revelio requires **countermeasures** on multiple layers

Application topology

Select intermediate LN nodes consciously

End-to-end communication

Random padding to hide message types

Network level

Use Tor/VPN to avoid adversarial ASes

Revelio requires **countermeasures** on multiple layers

Application topology

Select intermediate LN nodes consciously

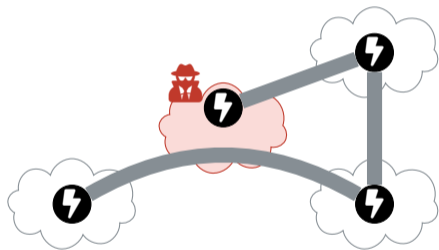
End-to-end communication ✓ **under development**

Random padding to hide message types

Network level

Use Tor/VPN to avoid adversarial ASes

Revelio: A Network-Level Privacy Attack in the Lightning Network



LN is centralized on P2P and network layer

Adversaries deanonymize $\approx 1/3$ of payments

Revelio could potentially apply beyond LN

License

This work is licensed under a Creative Commons “Attribution-ShareAlike 4.0 International” license.



This work uses Font Awesome icons.