# HTLC-Griefing Penalty protocol

Final project of course 67513 - Introduction to cryptocurrencies

Aviv Baru & Yakir Oz

# What is HTLC-GP protocol?

- One of the problems of Lightning Network is Griefing Attack.
- HTLC Griefing Penalty is a new protocol to replace the current HTLC.
- The protocol require users that participates in a payment to lock funds to ensure compensation to honest users in case of griefing.

# Why is it interesting?

- Lightning Network aimed to improve the scalability problem of Blockchain.
- Problem with the Lightning Network like Griefing attack might prevent people from adopting the Network.
- HTLC-GP protocol might make the attack not profitable and help to make the Network more widespread.

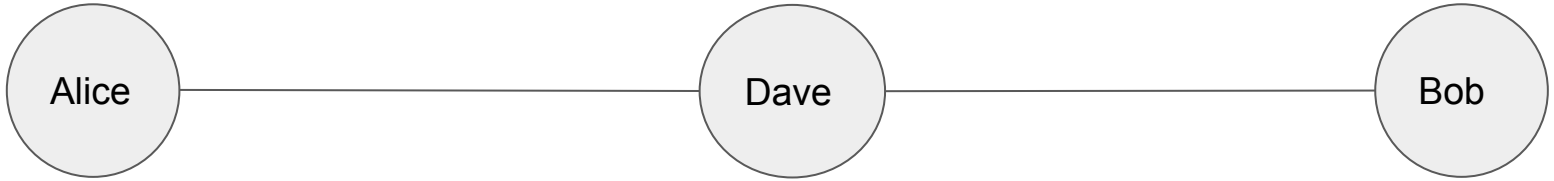
# What is the project about?

- In this project we created a simulation to run Lightning Network with the current HTLC protocol and the new HTLC-GP protocol.
- We compare the effects of the new HTLC-GP protocol against the HTLC protocol.
- Examine the effectiveness of the new protocol against old and new attacks.

# How HTLC-GP work?

Suppose Alice has Lightning channel with Dave, that has channel with Bob.

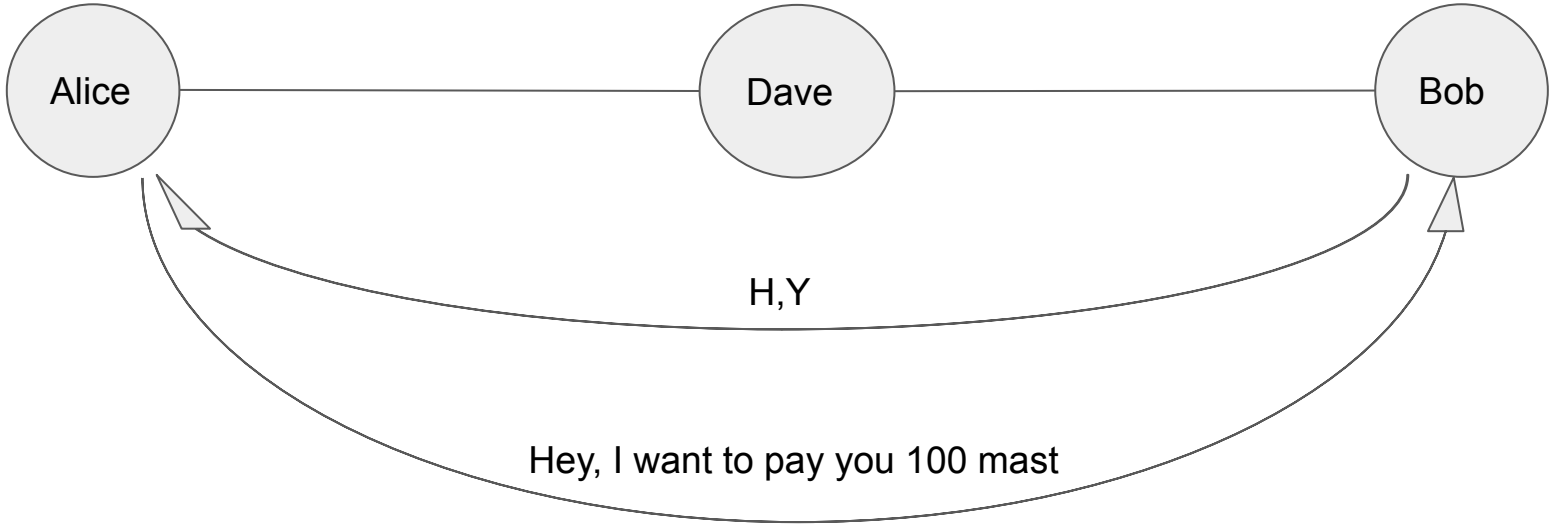
Alice want to transfer to Bob 100 msat.



# How HTLC-GP work?

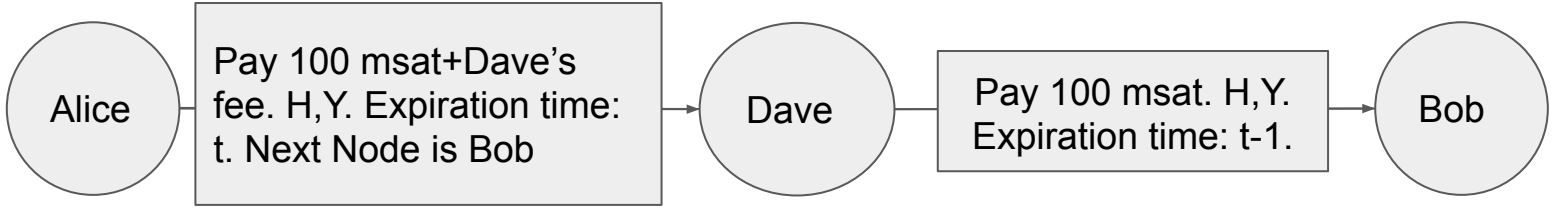
Alice sends message to Bob stating that she wants to send him some money.

Bob replies with H and Y s.t H=h(x) and Y=h(r), and keeps x and r (h is a hash function).



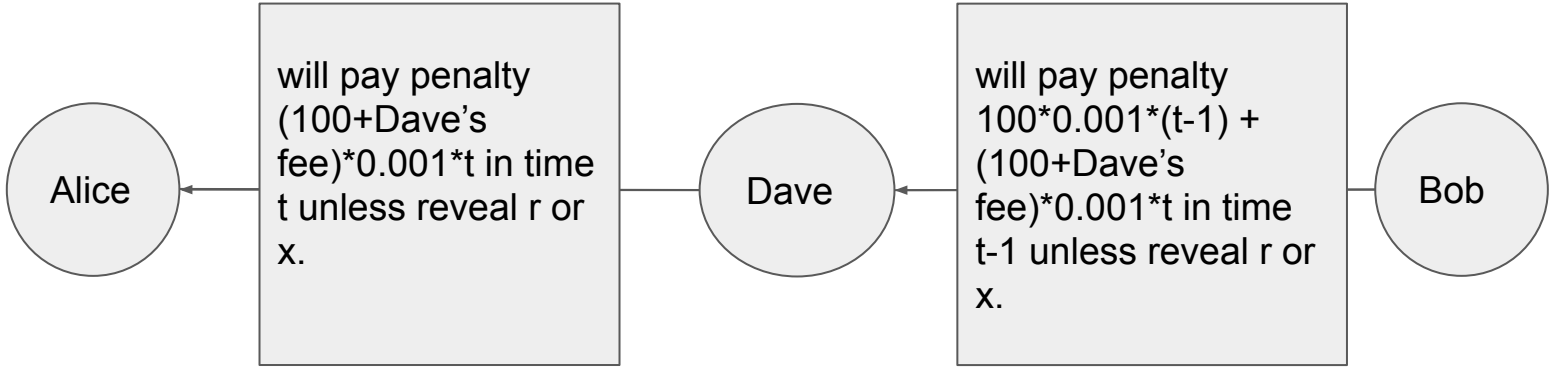
# How HTLC-GP work?

Alice finds a path to Bob through Dave and send message about the amount, time lock, H, Y and the next node to Dave, that sends a similar message to Bob.



# How HTLC-GP work?

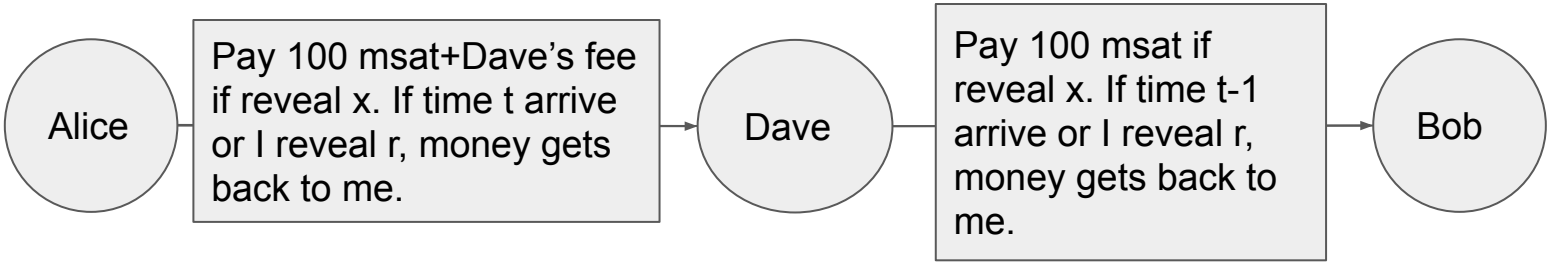
In order to receive the money, Bob establishes a cancellation contract with Dave and after Dave receives the contract, he establishes a similar contract with Alice.



# How HTLC-GP work?

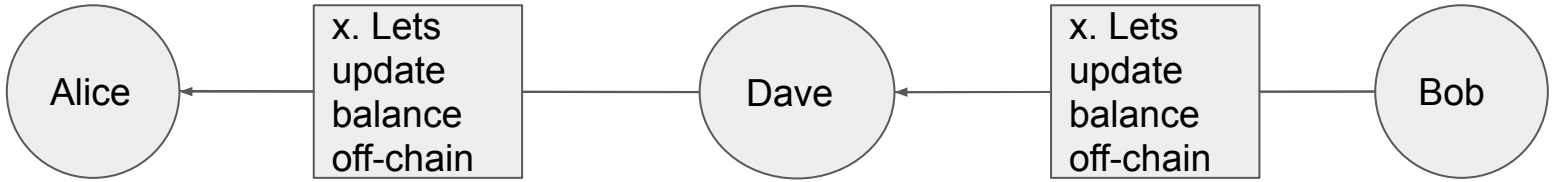
Alice now sends a Forward contract to Dave that sends one to Bob.

A Forward contract is similar to a regular HTLC contract.



# How HTLC-GP work?

In order to receive the money, Bob reveals x. Dave would reveal x to Alice. All parties would prefer now to update balance off-chain and cancel the Cancellation and Forward contract.



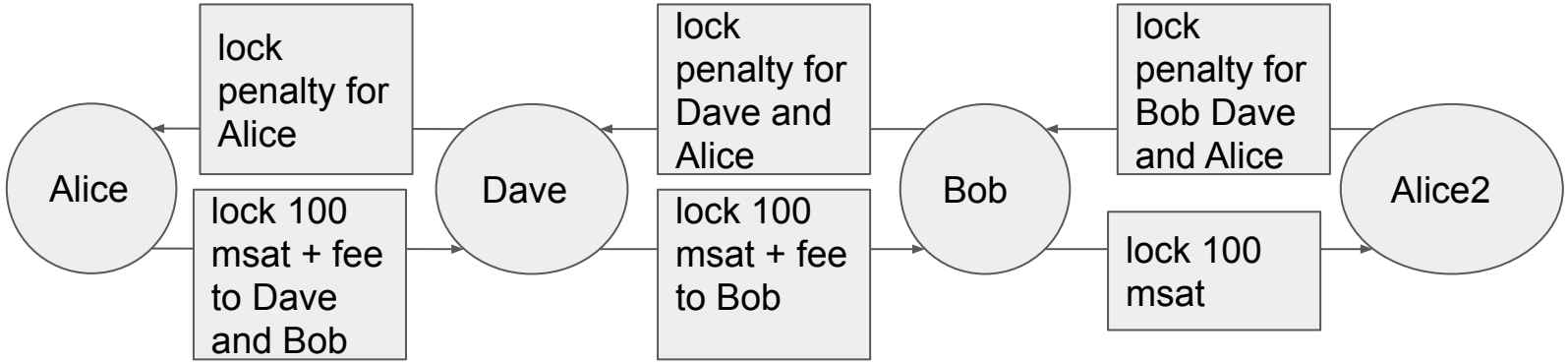

Overall Alice pays 100+Dave’s fee to Dave, and Dave pays 100 to Bob.

# How Soft Griefing in HTLC-GP work?

Alice wants to attack Bob and locks funds in the Bob-Dave channel. Alice connected with 2 nodes to Dave and to Bob (it even could be the same node).

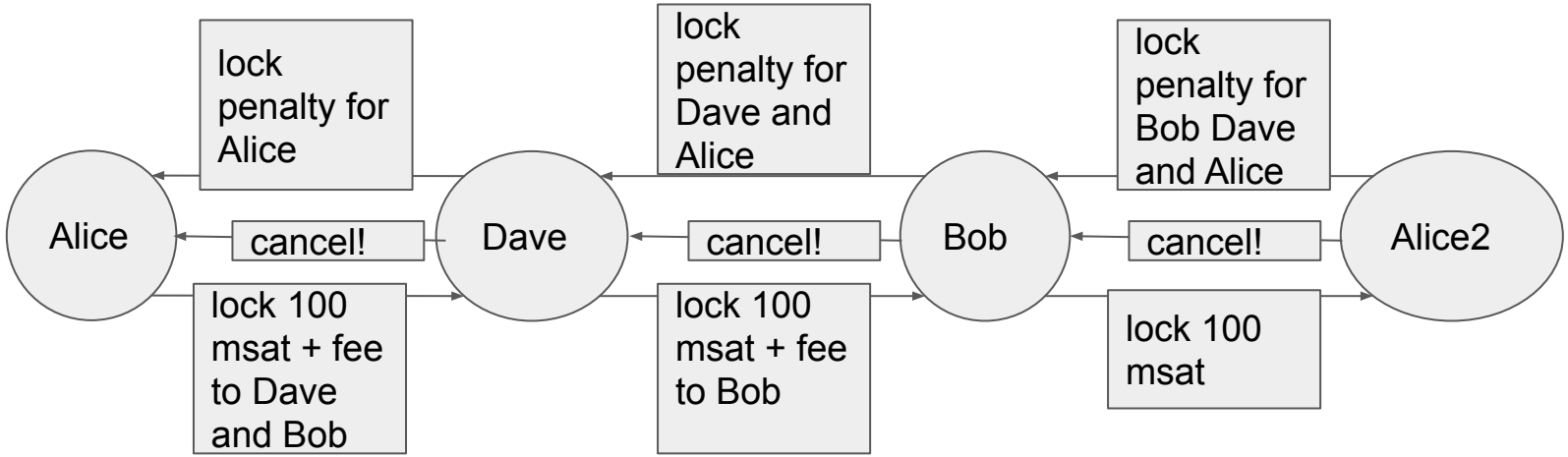
# How Soft Griefing in HTLC-GP work?

Alice starts HTLC-GP transaction to Alice2 in order to pay 100 msat (for example).



# How Soft Griefing in HTLC-GP work?

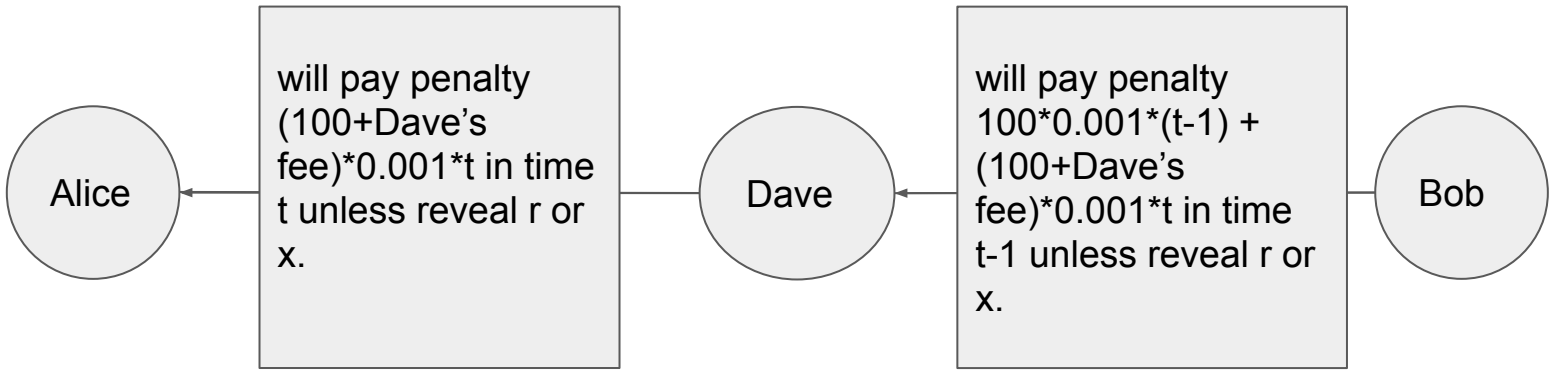
Now Alice2 wait for the last moment, and reveals r to cancel the cancellation contract and the transaction.



# How Dos Attack in HTLC-GP work?

Alice would tell Bob that she wants to send him some money.

Bob will now create a cancellation contract with Dave, locking up funds, when Dave tries to establish a cancellation contract with Alice, she ignores him and locks the funds for delta amount of time.



# Simulations Runs

Ran the following simulations (all compares made on the exactly same run):

- A few levels of possible delays in the network, compared the HTLC and the HTLC-GP.
- DIfferent values of Delta parameter with Dos attacking a specific node. Compare HTLC-GP with the attack and without.
- Soft griefing attack a specific node. Compare HTLC-GP with the attack and without.
- Soft griefing attack all network - trying to lock as mush funds as possible. Compare HTLC-GP with the attack and without.

# Simulations Parameters

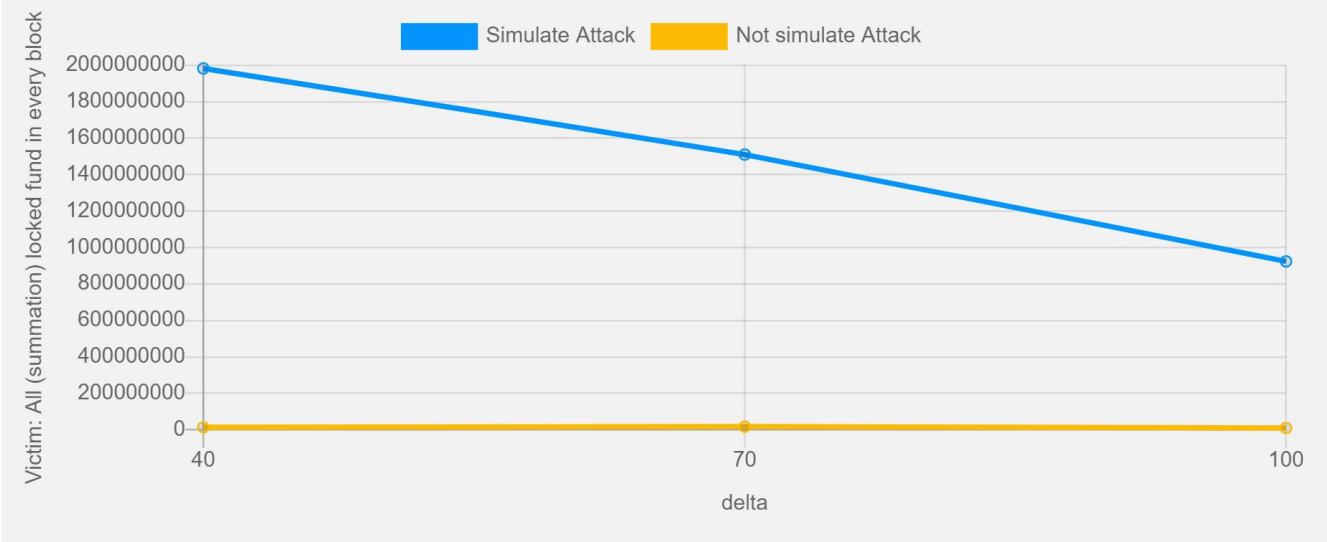
- Network with 1000 nodes connected between with redundancy topology, each node has 6 channels and can reach to any other node with not a lot of hops.
- Simulate 15 days, each block runs 1 transaction.
- Fee, amount to send, capacity of channel, Griefing penalty rate are all constant numbers.

# Not all is great

- We wanted to run the simulation on a real snapshot of Lightning Network (the code still exists) but it ran for too long, and it was hard to see significant difference within few iterations.
- At first we used parameters (fee, amount to send, capacity) distributed like a in the real snapshot of Lightning, but it had a big variance in the results, and the long running time was making it hard to show the difference along many runs.

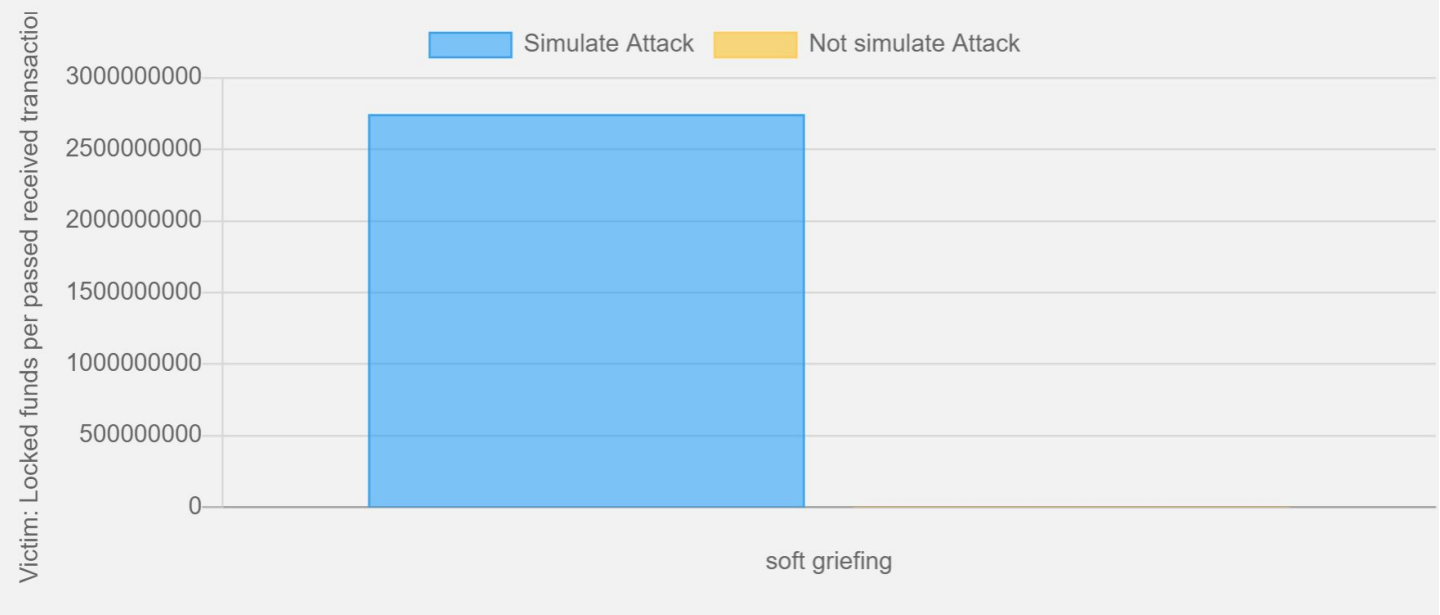
# Results

All results showed in UI we built.



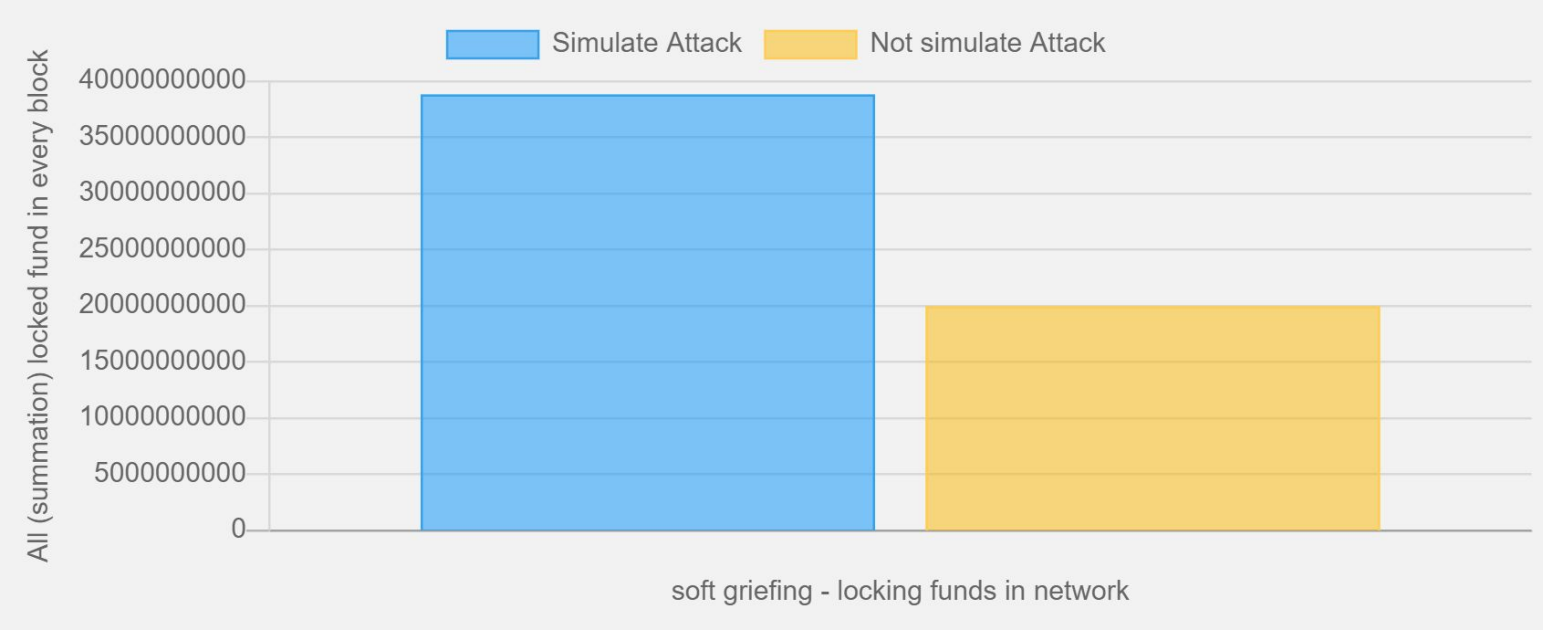

Delta parameter effect how Dos attack on specific node locked many more funds

# Results



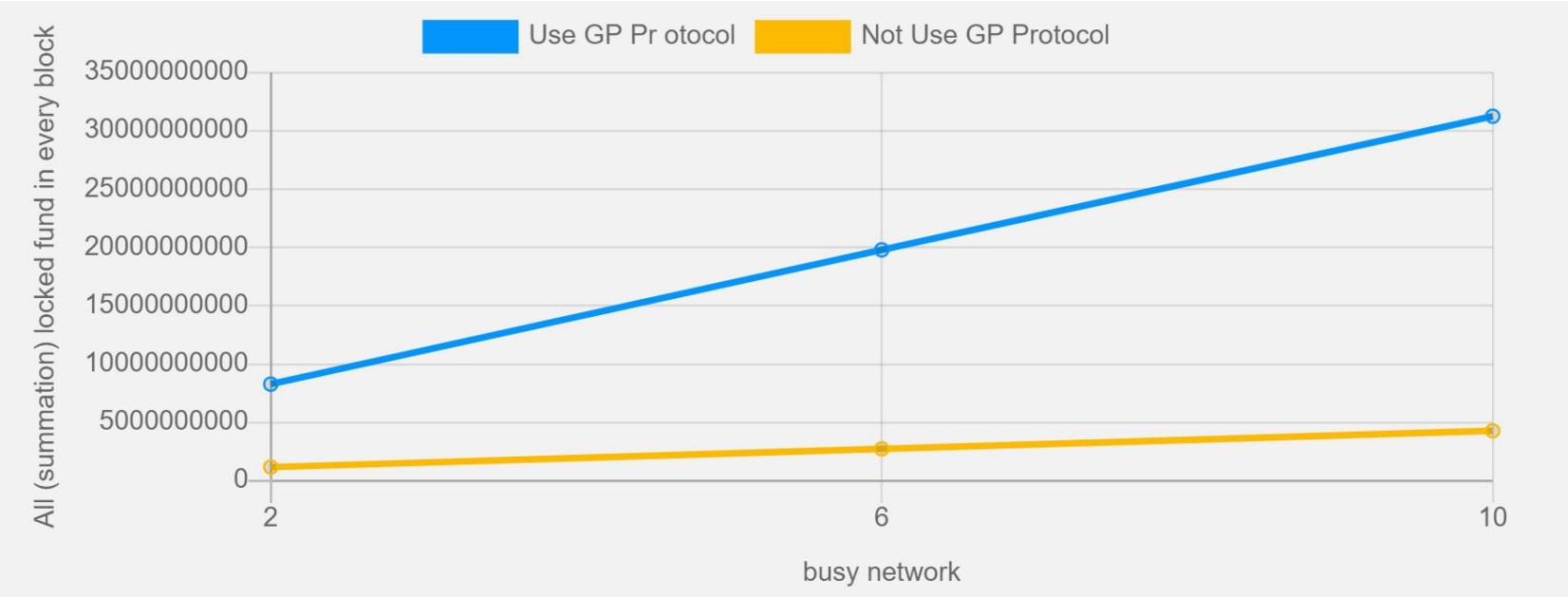

Soft Griefing affect the locked fund of the victim

# Results




Soft Griefing attack on network affect sum locked funds of all the network.

# Results




Busy network parameter show how HTLC-GP locked many more fund along the simulation as we increase the parameter

# The End

Thanks!

The code is hiding here:
https://github.com/avivbaru/cryptocurrencies_final_project