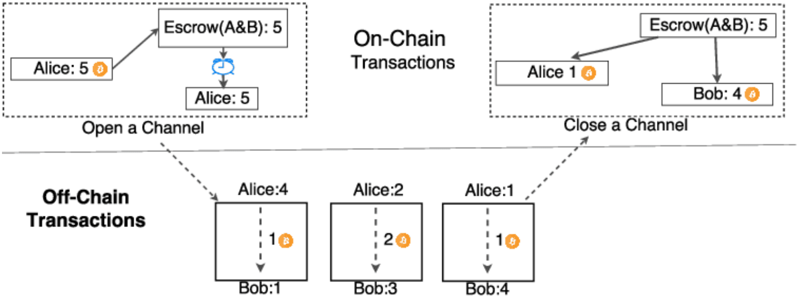
Countermeasure for Griefing Attack in Lightning Network & and its Strategic Analysis

Subhra Mazumdar, Prabal Banerjee, Abhinandan Sinha, Sushmita Ruj and Bimal Kumar Roy

February 10, 2022

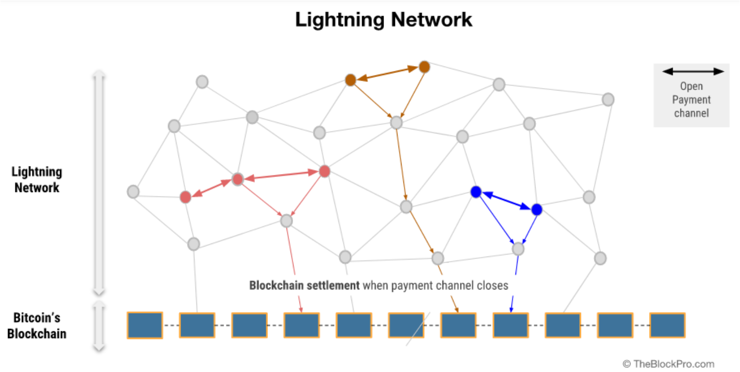
Off-Chain payments using Payment Channel



Avoids recording all the transactions, except opening and closing of channel, in the Blockhain.

Payment Channel Network

- Several Payment Channels are interconnected to form the Payment Channel Network (PCN).

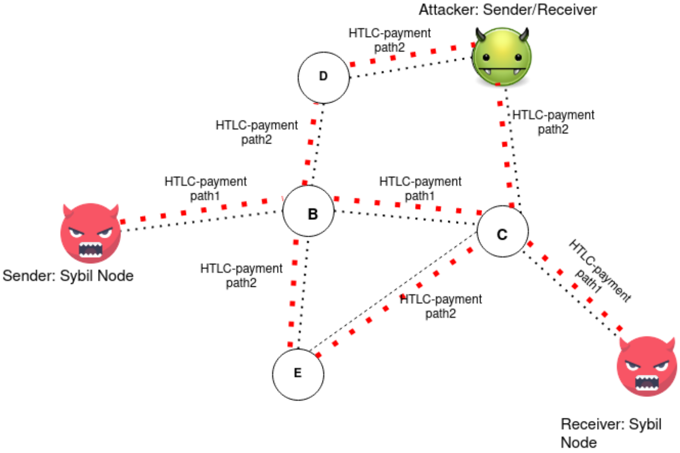


Griefing Attack in Lightning Network

- Lightning Network is the PCN for Bitcoin.
- Payments are finalized using HTLC
- Conditional payments are forwarded till it reaches the recipient
- *Griefing Attack*: If any party in between denies to forward the payment or recipient does'nt respond

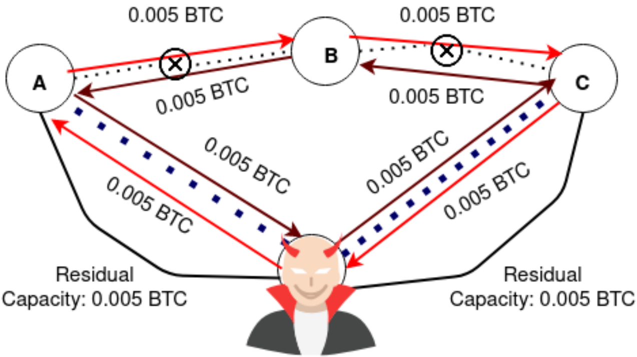
Motivation of Griefing Attack (I)

Stalling the Network

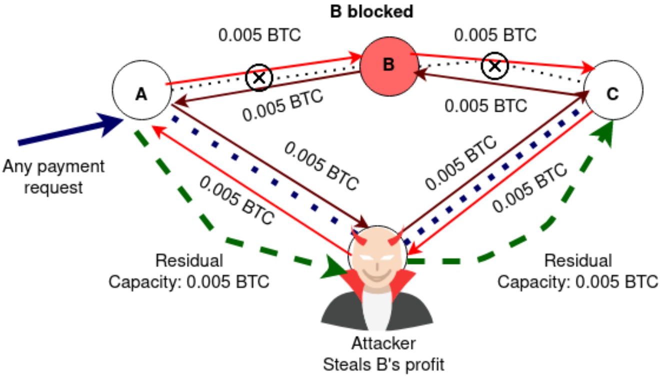


Motivation of Griefing Attack (II)

Eliminating a competitor



Motivation of Griefing Attack (III)



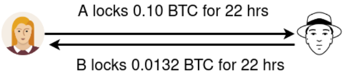
State-of-the-Art

- Up-front Payments: Economic barrier for payer
- Reverse Bonds: Violates payer privacy, not well defined
- Proof-of-Closure: Fails to penalize attacker

Objective of Countermeasure

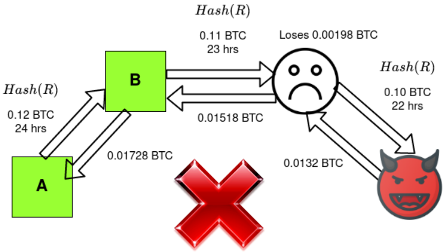
- Penalize Attacker for locking funds
- Compensate honest parties affected by Griefing Attack
- No honest party must incur any loss
- Ensure that privacy of payment isn't violated

Proposed Countermeasure: Griefing-Penalty



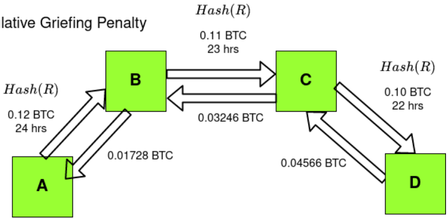
- Rate of Griefing-Penalty γ: 0.0001 per minute.
- B locks $0.0001 \times 60 \times 22 \times 0.1\ BTC = 0.0132\ BTC$ as penalty
- *Terms of the contract: If B resolves payment before 22 hrs, it gets 0.1 BTC, else A will get a compensation of 0.0132 BTC*

Incorporating Griefing-Penalty in HTLC

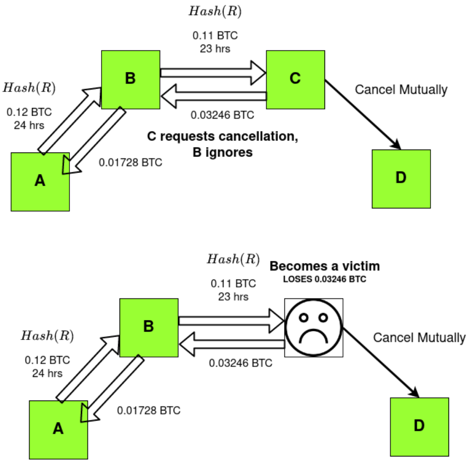


Rate of penalty per minute: 0.0001

Cumulative Griefing Penalty



Problem of Reverse Griefing

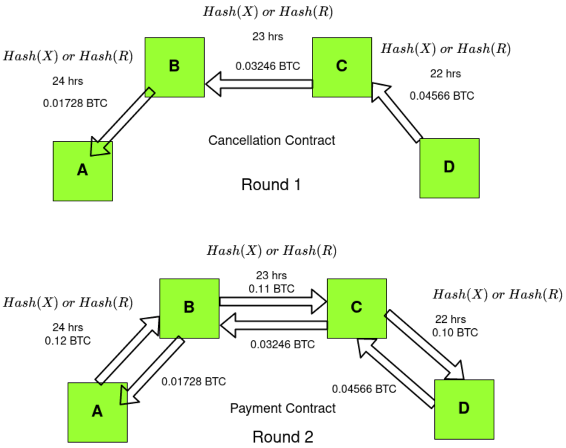


HTLC-GP Construction (I)

HTLC-GP Construction

- One pass for lock phase fails!
- Needs 2 pass for locking collateral.
- First pass *Cancellation Round* - Establish Cancellation Contract from payee to payer.
- Second Pass *Payment Round* - Establish Payment Contract from payer to payee.

HTLC-GP Construction (II)



Security Analysis (I)

Theorem

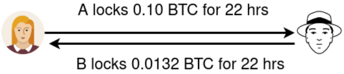
(Guaranteed compensation for an honest node). *Given a payment request* (U_0, U_n, α_0) *to be transferred via path* $P = \langle U_0, U_1, \ldots, U_n \rangle$*, if at least one party* $U_k, k \in [1, n]$ *mounts griefing attack then any honest party* $U_j \in P, j \in [0, k-1]$ *will earn compensation, without losing any funds in the process.*

Security Analysis (II)

Theorem

(Payer and Payee's Privacy). *Given the information of griefing-penalty in the off-chain contract, an intermediate node cannot infer its exact position in the path for routing payment.*

Problem with Bitcoin Scripts



B will pay if it doesn't respond with 22 hrs.

But what if it responds at the 21^{th} hr? B need not pay any penalty
Wait, isn't he still locking A's money uselessly?

Thus HTLC-GP's security analysis was not enough! Works under assumption that attacker will not respond.
In reality, each party is rational.

Can we solve it Cryptographically?

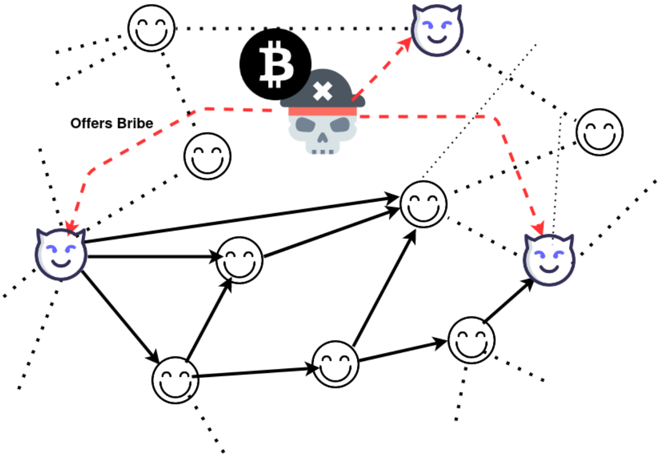
- Given that D is the contract timeout period and total penalty charged is P, let us consider that a party charges penalty after d interval.
- The timeout period is divided into $\frac{D}{d}$ slots. There must be total $\frac{D}{d}$ cancellation contracts denoted as $C_1, C_2, \ldots, C_{\frac{D}{d}}$.
- In each contract C_j, the penalty locked is $\frac{d}{D}P$ and each contract's timeout period is $jd, j \in [1, \frac{D}{d}]$.

Multiple contracts on a single channel for a single payment. Each cancellation contract has a very short timeout period. Risky!

Solution

- Bitcoin scripts has limitation!
- Security proofs of these protocols typically concentrate on the cryptographic aspects.
- Rewards and punishment mechanism needs to be analyzed from Game Theoretic point of view.

Strategic Analysis of HTLC (I)



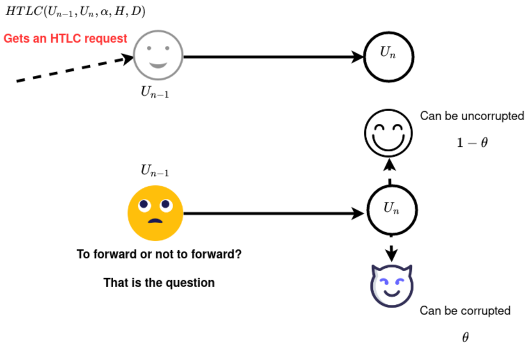
Attacker corrupts some nodes in the network. *Corrupt party griefs*

Strategic Analysis of HTLC (II)

- Sender node U_0 wants to transfer α coins to node U_n through path $P = \langle U_0 \rightarrow U_1 \rightarrow U_2 \ldots \rightarrow U_n \rangle$, each node U_i charging a processing fee $f(\alpha)$.
- Any node U_i forwards an amount $\alpha + (n-1-i)f(\alpha)$ to U_{i+1}. U_n generates a payment condition $H = \mathcal{H}(x)$ and shares it with U_0.
- The *HTLC* timeout period in the contract between U_i and U_{i+1} is set to $D + (n-1-i)\Delta, i \in [0, n-1]$, Δ being the worst-case time taken to settle a transaction on-chain.

Strategic Analysis of HTLC (III)

Two party interaction: *Formulate a Dynamic Game of Incomplete Information*



Strategic Analysis of HTLC (IV)

Opportunity Cost of locked coins

- Expected revenue a node would have earned had it utilized the locked coins for processing transactions in a given time period.
- The arrival of payment in a channel follows a Poisson process
- Opportunity cost is calculated as per that

Strategic Analysis of HTLC (V)

Attacker Budget and Strategy

- An attacker with a given budget has the objective of locking as many coins as possible in the network.
- *Bribe offered per attack*. The attacker bribes a party. The amount is sufficient to cover cost of attack.
- If U_n is corrupted, it executes a self-payment of amount α (where it acts as both payer and payee) via a route of the maximum allowed path length.

Strategic Analysis of HTLC (VI)

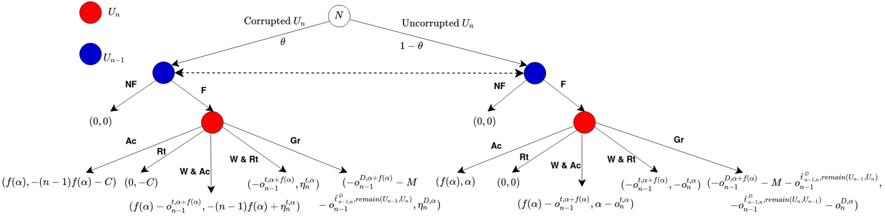
Action Set of U_{n-1}: Forward payment, Not forward payment

Action Set of U_n: Accept, Reject, Wait & Accept, Wait & Reject, Grief
Corrupted U_n can select either of the strategies for mounting the attack:

- Reject the payment just before lock time elapses
- Do not respond

Strategic Analysis of HTLC (VII)

Extensive Form of Game



U_n
U_{n-1}
N
Corrupted U_n
θ
Uncorrupted U_n
$1-\theta$
NF
F
$(0,0)$
NF
F
$(0,0)$
Ac
Rt
W & Ac
W & Rt
Gr
$(f(\alpha), -(n-1)f(\alpha) - C)$
$(0, -C)$
$(f(\alpha) - o_{n-1}^{t,\alpha+f(\alpha)}, -(n-1)f(\alpha) + \eta_n^{t,\alpha})$
$(-o_{n-1}^{t,\alpha+f(\alpha)}, \eta_n^{t,\alpha})$
$(-o_{n-1}^{D,\alpha+f(\alpha)} - M - o_{n-1}^{\tilde{t}_{n-1,n}^D, remain(U_{n-1},U_n)}, \eta_n^{D,\alpha})$
Ac
Rt
W & Ac
W & Rt
Gr
$(f(\alpha), \alpha)$
$(0,0)$
$(f(\alpha) - o_{n-1}^{t,\alpha+f(\alpha)}, \alpha - o_n^{t,\alpha})$
$(-o_{n-1}^{t,\alpha+f(\alpha)}, -o_n^{t,\alpha})$
$(-o_{n-1}^{D,\alpha+f(\alpha)} - M - o_{n-1}^{\tilde{t}_{n-1,n}^D, remain(U_{n-1},U_n)}, -o_{n-1}^{\tilde{t}_{n-1,n}^D, remain(U_n,U_{n-1})} - o_n^{D,\alpha})$

Figure: Extensive form of game Γ_{HTLC}

Strategic Analysis of HTLC (VIII)

- Uncorrupted U_n will choose *Accept*
- Corrupted U_n can choose either *Wait and Reject at* $D - \delta : \delta \to 0$ or *Grief*. It selects the first method with probability q and the second method with probability $1 - q, q \in [0, 1]$.

Game Analysis

U_{n-1} chooses *Forward*
if $\theta < \frac{f(\alpha)}{o_{n-1}^{D,\alpha+f(\alpha)}+f(\alpha)+(1-q)(o_{n-1}^{\tilde{t}^{D}_{n-1,n},remain(U_{n-1},U_n)}+M)}$, else it chooses *Not Forward*; *corrupted* U_n can either choose *Grief* or *Wait & Reject* at time $D - \delta$; *uncorrupted* U_n chooses *Accept*; is a perfect Bayesian equilibrium.

Strategic Analysis of HTLC-GP (I)

- For payment of α from U_0 to U_n via $(n-1)$ intermediaries, cumulative compensation offered to node U_i by node U_{i+1} upon forwarding an amount $\alpha_i = \alpha + (n-i-1)f(\alpha)$ as $Z_{\alpha_i,i+1}, i \in [0, n-1]$.
- An off-chain contract between node U_i and U_{i+1} requires U_i locking an α_i coins and U_{i+1} must lock $Z_{\alpha_i,i+1}$ coins.
- Uncorrupted U_n will choose *Accept*
- Corrupted U_n can choose *Wait and Reject at* $D-\delta : \delta \rightarrow 0$. *Griefing* leads to loss of coins, not selected

Game Analysis

U_{n-1} chooses *Forward* if $\theta < \frac{f(\alpha)}{f(\alpha)+o_{n-1}^{D,v+f(v)}+o_{n-1}^{D,Z_{v+f(v),n-1}}}$, else it chooses *Not Forward*; *corrupted* U_n chooses *Wait & Reject* at time $D-\delta$; *uncorrupted* U_n chooses *Accept*; is a perfect Bayesian equilibrium.

Effectiveness of HTLC-GP (I)

Measuring success rate of attack: *Capacity locked* in a path routing payment is the summation of the coins locked in the off-chain contract instantiated on the channel forming the path. Assuming all the payments

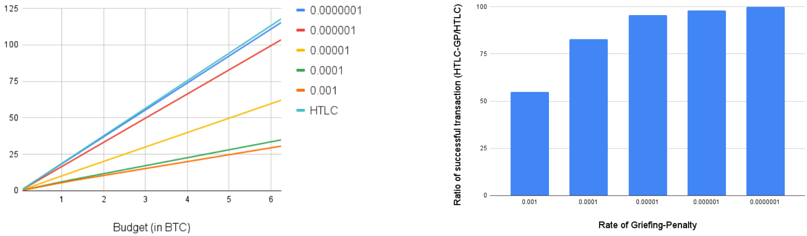
executed are of value α and the bribe offered per instance is L, the attacker can corrupt $\frac{\mathcal{B}_{EX}}{L}$ nodes in the networks.

Effectiveness of HTLC-GP (II)

Claim

Given the total budget of the attack is $\mathcal{B}_{EX}$, incentive per attack being L, transaction value per payment being α, HTLC timeout period is D, time taken to settle a transaction on-chain being Δ, n is the maximum allowed path length and a corrupted recipient rejects the payment at time $t' = D - \delta$, where $\delta \to 0$, the capacity locked upon using HTLC-GP is less than the capacity locked in HTLC, the loss percent being $\frac{\gamma n(\frac{D}{2}+\frac{\Delta(n-2)}{6})}{1+\gamma n(D+\frac{(n-1)\Delta}{2})}$

Effectiveness of HTLC-GP (III)



(a) Capacity locked (in BTC) vs Adversary's Budget

(b) Ratio of successful transaction (HTLC-GP/HTLC) upon varying γ

Figure: γ is varied between 10^{-3} to 10^{-7}

Dependent on γ, cannot be set too high. HTLC-GP is Weakly Effective!

Guaranteed Minimum Compensation ζ (I)

- Compensation offered to a party may be too low for a given rate of penalty in HTLC-GP.
- For a given rate of penalty, the maximum cumulative penalty, denoted as $Z_{\alpha,max}$ that U_n is required to lock, is $\gamma\alpha\sum_{i=1}^{n}(D+(n-i)\Delta)$.
- We consider $\gamma\sum_{i=1}^{n}(D+(n-i)\Delta)$ as k, where $k \in \mathbb{R}^+$. Thus, $Z_{\alpha,max} = k\alpha$.
- ζ is the Guaranteed Minimum Compensation and $\zeta \in [0,1)$.

Guaranteed Minimum Compensation ζ (II)

Adjusting the maximum path length

Proposition

Given the maximum cumulative griefing-penalty for a payment α is $k\alpha$, and the guaranteed minimum compensation ζ, the maximum path length for routing transaction is $\frac{k}{\zeta}$.

Follows from $\tilde{n}\zeta\alpha \leq Z_{\alpha,max}$

Guaranteed Minimum Compensation ζ (III)

Estimating Rate of Griefing-Penalty $\gamma^{\zeta,k}$

Once the maximum path length is adjusted, the rate of griefing-penalty γ is no more a free variable. We call this new rate of griefing-penalty $\gamma^{\zeta,k}$.

Proposition

Given ζ as the guaranteed minimum compensation, ratio of maximum cumulative griefing penalty and the transaction amount is k, and the least timeout period of the off-chain contract being D, the rate of griefing-penalty $\gamma^{\zeta,k}$ is $\frac{2\zeta^2}{2\zeta D+\Delta(k-\zeta)}$.

Follows from $k\alpha = \gamma^{\zeta,k}\sum_{i=1}^{\tilde{n}}(D + (\tilde{n} - i)\Delta)\alpha$

HTLC-GP$^{\zeta}$ (I)

- For relaying funds from U_0 to $U_{\tilde{n}}$, both of them decides on k for a given ζ and sets $\tilde{n}$.
- The rate of griefing-penalty $\gamma^{\zeta,k}$ is calculated accordingly for a given HTLC timeout period D.
- Parties are rational and will take a decision based on the belief θ.

HTLC-GP$^{\zeta}$ (II)

Effectiveness of HTLC-GP$^{\zeta}$

Claim

Given the total budget of the attack is $\mathcal{B}_{EX}$, incentive per attack being L, transaction value per payment being α, HTLC timeout period is D, time taken to settle a transaction on-chain being Δ, n is the maximum allowed path length for HTLC, $\tilde{n}$ is the maximum allowed path length for $HTLC\text{-}GP^{\zeta}$ and a corrupted recipient rejects the payment at time $t' = D - \mu$, where $\mu \to 0$, the capacity locked in $HTLC\text{-}GP^{\zeta}$ is less than the capacity locked in HTLC, the loss percent being

$$\frac{n-\tilde{n}}{(n-1)\left(1+\gamma^{\zeta,k}nD+\gamma^{\zeta,k}n\Delta\frac{n-1}{2}\right)}+\frac{\gamma^{\zeta,k}\tilde{n}((n-1)(D+\frac{(\tilde{n}-1)\Delta}{2})-\frac{\tilde{n}-1}{2}(D+\frac{(2\tilde{n})\Delta}{3}))}{(n-1)\left(1+\gamma^{\zeta,k}nD+\gamma^{\zeta,k}n\Delta\frac{n-1}{2}\right)}$$

HTLC-GP$^\zeta$ (III)

- The loss percent is dominated by the factor $\frac{n-\tilde{n}}{n-1}$. For a given k, the higher the factor ζ, lower is the maximum path length $\tilde{n}$, greater is the loss incurred.
- For a fixed value of k, ζ can be increased, reducing the maximum path length available for routing. This will increase the cost of the attack.

Performance Analysis

k	ζ	$\gamma^{\zeta,k}$	Maximum Path Length	Ratio of capacity locked	
				$\frac{HTLC-GP^{\zeta}}{HTLC}$	$\frac{HTLC-GP}{HTLC}$
0.005	0.00025	2.4×10^{-7}	20	96.89%	96.89%
	0.0005	9.1×10^{-7}	10	46.3%	89.86%
	0.0025	1.4×10^{-5}	2	5.21%	50.7%
0.05	0.0025	2.4×10^{-6}	20	78%	78%
	0.005	9.1×10^{-6}	10	38.2%	54%
	0.025	1.6×10^{-4}	2	4.7%%	33%
0.25	0.0125	1.2×10^{-5}	20	53%	53%
	0.025	4.5×10^{-5}	10	28%	40%
	0.1125	6.9×10^{-4}	2	4.2%	32%
0.5	0.025	2.4×10^{-5}	20	44%	44%
	0.05	9.1×10^{-5}	10	22.1%	38.5%
	0.2	1.1×10^{-3}	2	3.8%	31.5%
0.75	0.0375	3.6×10^{-5}	20	41%	41%
	0.075	1.36×10^{-4}	10	21.2%	35.6%
	0.3	1.7×10^{-3}	2	3.51%	30.04%
1	0.05	4.8×10^{-5}	20	38%	38%
	0.1	1.8×10^{-4}	10	20%	34%
	0.5	3.3×10^{-3}	2	3.4%	29.98%
2	0.1	10^{-4}	20	35%	35%
	0.2	3.6×10^{-4}	10	18%	32%
	0.95	6.1×10^{-3}	2	3.34%	29.01%

Table: Capacity Locked when k and ζ is varied

Future Works

- Extend routing algorithm for handling dynamic networks.
- Combine routing and payment protocol by allowing dynamic split of payments - reduce the computation overhead of the sender.
- Extend the concept of griefing-penalty to *Atomic Cross Chain Swap*. We would like to study the impact of exchange rate volatility, locktime of contract on the cumulative griefing-penalty, with each party locking collateral in different contracts belonging to different blockchains.
- We want to propose a fair compensation protocol for griefing attack considering different routing nodes have different estimates of loss suffered. We would like to study the attack in presence of both Byzantine and rational participants and analyze the effectiveness of the countermeasure in the new model.

References (I)

[1] Poon, Joseph, and Thaddeus Dryja. “The bitcoin lightning network: Scalable off-chain instant payments.” (2016).

[2] Daniel Robinson. 2019. HTLCs considered harmful. In Stanford Blockchain Conference.

[3] "A proposal for up-front payments", https://lists.linuxfoundation.org/pipermail/lightning-dev/2019-November/002282.html, November 2019.

[4] "A proposal for up-front payments: Reverse bond payment," https://lists.linuxfoundation.org/pipermail/lightning-dev/2020-February/002547.html, February 2020.

[5] "Proof-of-closure as griefing attack mitigation," https://lists.linuxfoundation.org/pipermail/lightning-dev/2020-April/002608.html, April 2020.

References (II)

[6] Lightning 101: Lightning network fees, https://blog.bitmex.com/the-lightning-network-part-2-routing-fee-economics/, accessed: 2019-01-22 (2019).

[7] The lightning network (part 2) - routing fee economics, https://blog.bitmex.com/the-lightning-network-part-2-routing-fee-economics/, accessed: 2019-03-27 (2019).

[8] P. Guasoni, G. Huberman, C. Shikhelman, Lightning network economics: Channels, Available at SSRN 3840374 (2021).

[9] A. Mizrahi, A. Zohar, Congestion attacks in payment channel networks, in: International Conference on Financial Cryptography and Data Security, 2021.

[10] Z. Lu, R. Han, J. Yu, General congestion attack on htlc-based payment channel networks, in: 3rd International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2021), 2021

References (III)

[11] P. Zappal'a, M. Belotti, M. Potop-Butucaru, S. Secci, Game theoretical framework for analyzing blockchains robustness, in: Proceedings of the 4th International Symposium on Distributed Computing, Leibniz International Proceedings in Informatics (LIPIcs), Freiburg (virtual conference), Germany, 2020.

Thank You
Any Questions?