Strategic Analysis of Griefing Attack in Lightning Network

Subhra Mazumdar, Prabal Banerjee, Abhinandan Sinha,
Sushmita Ruj, *Senior Member, IEEE*, and Bimal Kumar Roy

SUPPLEMENTAL MATERIAL

I. DEFINING OPPORTUNITY COST

In Section *3.1 System Assumption* of main paper, we define a function $O : \mathbb{R}^+ \times \mathbb{W} \times \mathbb{R}^+ \to \mathbb{R}^+ \cup \{0\}$, where $O(r_U, t, val)$ is the expected revenue a node U would have earned had it utilized the amount val for processing transactions in period of t units given that r_U is the rate of payments processed by U per unit time. In other words, O defines the *opportunity cost* [1]. The primary source of revenue for a routing node in the Lightning Network is the fee obtained by processing transactions [2]. Also, the arrival of payment in a channel follows a Poisson process [1] [3], [5], [6]. U expects each transaction size to be per_tx_val. Given the number of coins locked is val, the number of transactions U expects to receive in period of t units is $J = \frac{val}{per\_tx\_val}$. Given X is the number of transactions in that interval or $X \sim Poisson(r_U t)$, we have.

$$P(X = x) = \frac{e^{-r_U t}(r_U t)^x}{x!} \tag{1}$$

where $0 \leq x \leq J$. Expected number of transactions in t unit of time

$$E(X) = \sum_{x=0}^{J} x P(X = x) \tag{2}$$

Subhra Mazumdar was with Cryptology and Security Research Unit, Indian Statistical Institute Kolkata, India. She is now with TU Wien and Christian Doppler Lab Blockchain Technologies for the Internet of Things, Vienna, Austria. Email: subhra.mazumdar@tuwien.ac.at

Prabal Banerjee is with Cryptology and Security Research Unit, Indian Statistical Institute Kolkata, India and Polygon (previously Matic Network). Email: mail.prabal@gmail.com

Abhinandan Sinha was with Economic Research Unit, Indian Statistical Institute Kolkata, India. He is now with Ahmedabad University, India. Email: abhinandan.sinha@ahduni.edu.in

Sushmita Ruj was with CSIRO's Data61, Sydney, Australia. She is now with University of New South Wales, Sydney, Australia. Email: sushmita.ruj@unsw.edu.au

Bimal Kumar Roy is with Applied Statistics Unit, Indian Statistical Insitute Kolkata, India. Email: bimal@isical.ac.in

[1] All the papers assumed arrival of transaction in Bitcoin blockchain as a Poisson process but the validity of the assumption was not verified. It was first analyzed in [3], [4] and the authors have reported that transactions' inter-arrival times can be approximately fitted with an exponential distribution, which partially supports the Poisson arrival assumption but with noticeable deviation. In our paper, we consider the arrival of transaction in Bitcoin blockchain following a Poisson process and the same holds true for transactions arriving in Lightning Network.

The fee earned by processing a transaction of size per_tx_val is defined as [7], [8]:

$$Fee_{per\_tx\_val} = base\_fee + fee\_rate \times per\_tx\_val \tag{3}$$

Thus, the revenue U expects to earn within period t or in other words, the opportunity cost $O(r_U, t, val)$ is

$$O(r_U, t, val) = E(X) Fee_{per\_tx\_val} \tag{4}$$

II. ANALYSIS OF GRIEFING ATTACK IN HTLC-GP

HTLC-GP starts from U_n, with the locking of penalty in the first round. U_n locks penalty in the contract formed with U_{n-1} but the former has the power to unlock the coins anytime by releasing the preimage of the cancellation hash. U_{n-1} will accept the contract if it thinks that the expected payoff upon forwarding the payment contract in the second round will be greater than the expected payoff on not forwarding the same. Only then it will lock the penalty in the off-chain contract with U_{n-2}. This holds for any pair U_{i-1} and U_i in path P. If U_{i-1} accepts to form a contract with U_i in the first round of *HTLC-GP*, it implies that it will forward the conditional payment to U_i in the second round as well. Thus we merge both the first and second round while studying the interaction between any two parties U_{i-1} and U_i. We analyze the payoff assuming both parties lock their coins in a single off-chain contract instead of two separate contracts. We adapt the model Γ_{HTLC} and propose the two-party game model $\Gamma_{HTLC-GP}$ for griefing attack in *HTLC-GP*. The extensive form of the game $\Gamma_{HTLC-GP}$ is shown in Fig. 1.

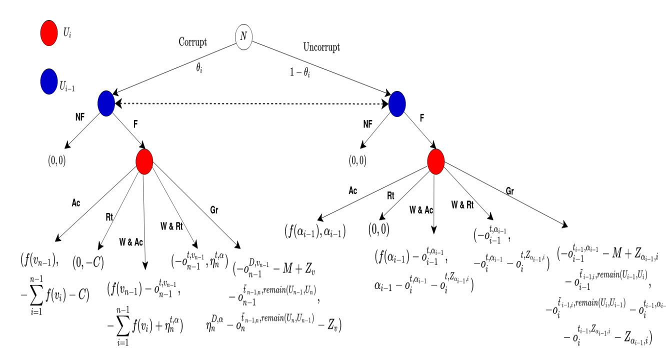
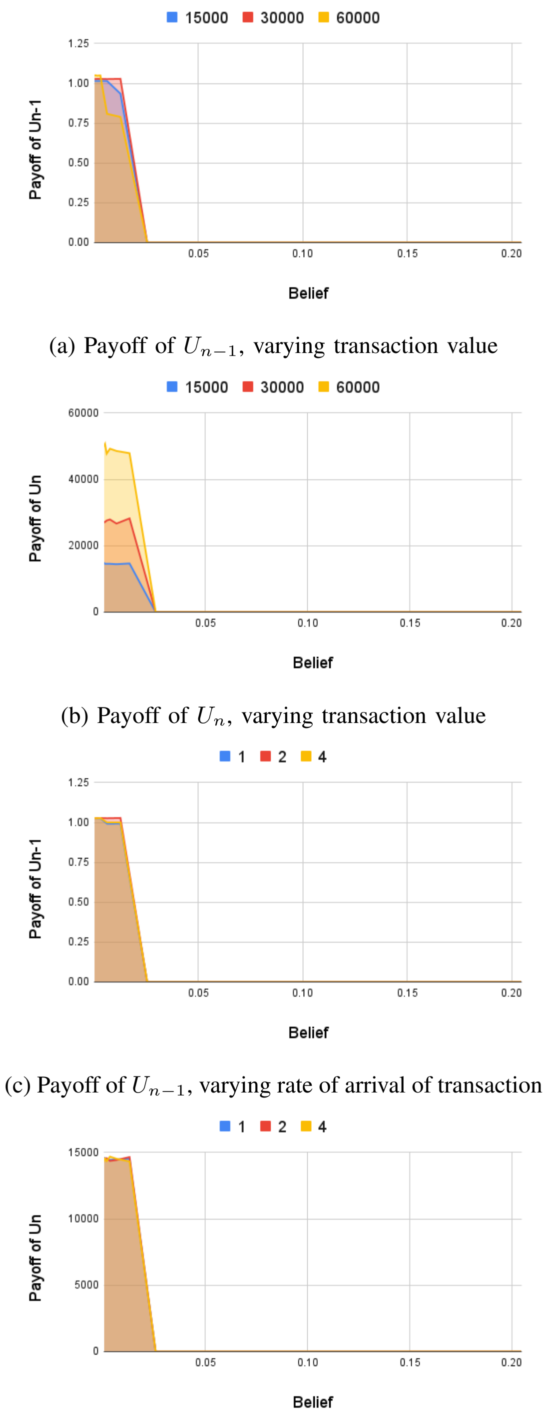


Fig. 1: Extensive form of the game $\Gamma_{HTLC-GP}$



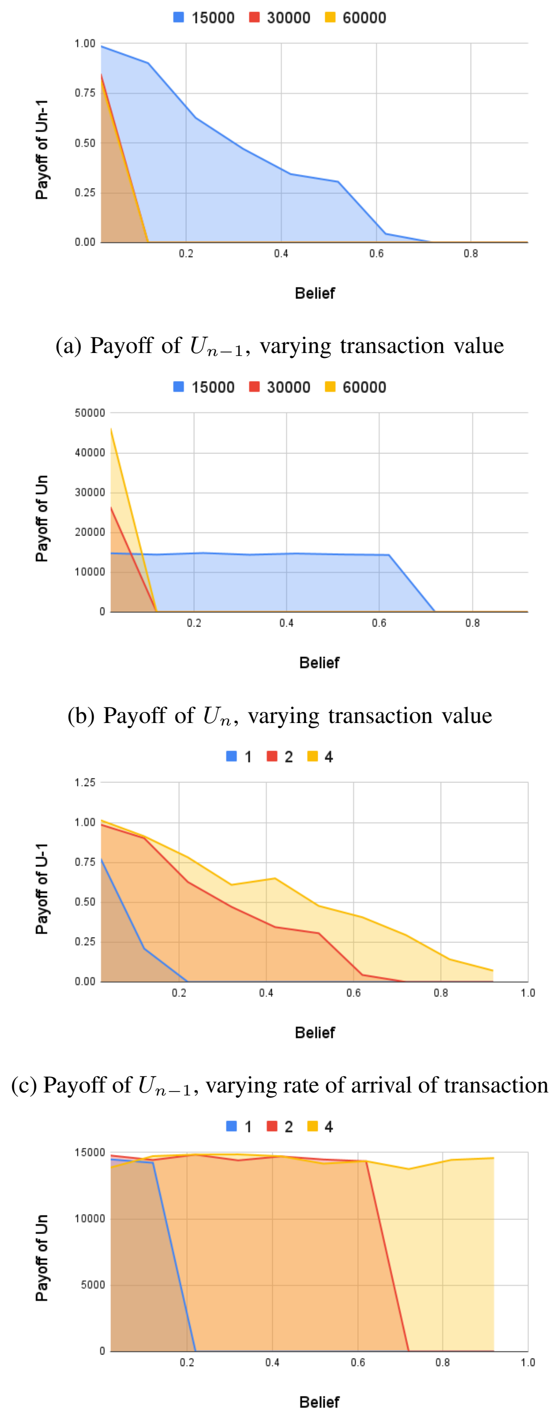
(a) Payoff of U_{n-1}, varying transaction value

(b) Payoff of U_n, varying transaction value

(c) Payoff of U_{n-1}, varying rate of arrival of transaction

(d) Payoff of U_n, varying rate of arrival of transaction

Fig. 2: Simulation of Γ_{HTLC}



(a) Payoff of U_{n-1}, varying transaction value

(b) Payoff of U_n, varying transaction value

(c) Payoff of U_{n-1}, varying rate of arrival of transaction

(d) Payoff of U_n, varying rate of arrival of transaction

Fig. 3: Simulation of $\Gamma_{HTLC-GP}$

III. Simulating the Game Model for Griefing Attack in HTLC and HTLC-GP

A. Dataset and Parameters

Simulation of sequential Bayesian games: The first part analyzes the payoff of each party involved in the games Γ_{HTLC} and $\Gamma_{HTLC-GP}$. We simulate the games Γ_{HTLC} and, $\Gamma_{HTLC-GP}$ respectively, and estimate the payoff of U_{n-1} and U_n. We consider a *Poisson distribution* for the arrival of transaction in a given channel [6]. The rate of arrival of the transaction is varied between 1 and 4 for the next 10 *blocks*. The path length is set 20 and $D = 100$. The transaction amount is varied between 15000 satoshis to 60000 satoshis.

The mining fee for closing a channel is $0.00000154\ BTC^2$. q is set to 0.7. If the coins remaining unutilized are C, the party tries to estimate the fee earned in the future had it utilized the coins. We set per_tx_val to 1000 satoshis, thus a party will earn by processing $\frac{C}{1000}$ transactions.

B. Observations

We discuss our observation in this section:

- Γ_{HTLC}: For transaction value ranging $15000 - 60000$ (in satoshis) and rate of arrival of transaction fixed to 10 within 10 blocks , the plots in Fig. 2(a) and 2(b) shows the expected payoff of U_{n-1} and expected payoff of U_n varying with the belief θ. U_{n-1}'s payoff decreases with increase in θ. Payoff of U_n remains more or less constant for a fixed transaction amount, but increases with increase in the transaction amount. For $\theta \geq 0.025$, U_{n-1} acts cautious and chooses *not forward*, as forwarding will lead to negative payoff. Both U_{n-1}'s and U_n's payoff drops to 0 from this point onwards.
  In Fig. 2(c) and 2(d), the rate of arrival of transaction is varied between 1 and 4 within a period of 10 blocks and transaction amount is 15000 satoshi. We observe that for $\theta < 0.025$, payoff of U_{n-1} and U_n remains positive and invariant.
- $\Gamma_{HTLC-GP}$: The plots in Fig. 3(a) and 3(b) shows that for $\theta \geq 0.1$, U_{n-1} acts cautious and chooses *not forward* for transaction varying between 30000 satoshi and 60000 satoshis. For transaction amount 15000, expected payoff of U_{n-1} and U_n remains positive till $\theta < 0.7$.
  In Fig. 3(c) and 3(d), given the rate of arrival of transaction is 1, U_{n-1} chooses to *forward* till $\theta \leq 0.2$. When the rate of arrival of transaction is 2, U_{n-1} chooses to *forward* till $\theta \leq 0.7$ and when rate of arrival is 4, $\theta \leq 0.9$.

C. Discussion of Results

Expected Payoff in Γ_{HTLC} and $\Gamma_{HTLC-GP}$:

- *Transaction amount is varied*: We see that expected payoff of U_{n-1} in $\Gamma_{HTLC-GP}$ remains positive for a higher value of θ compared Γ_{HTLC}. The reason being that in the first game, U_n can choose not to respond, forcing U_{n-1} to go on-chain and close the channel. Since the mining fee for closing the channel is quite high, the stakes are higher. Thus U_{n-1} tends to stop forwarding payment for θ as low as 0.025. In the second game, U_n will always resolve the payment just before the lock time elapses to avoid paying penalty. This prevents abrupt closure of the channel. It is observed that the cutoff value of θ is higher for transaction amount 150000 satoshis. This is because the capacity locked is higher when the transaction amount increases, hence the risk is higher.
- *Rate of the arrival of the transaction is varied*: In Γ_{HTLC}, varying the rate of arrival of the transaction has no impact on the payoff of both U_{n-1} and U_n because mining fee of channel closure dominates the result. In $\Gamma_{HTLC-GP}$, the value of θ increases with an increase in the rate of arrival of transaction. The reason behind this is that the distribution is positively skewed for a lower arrival rate. As the rate increases, the Poisson distribution becomes more symmetric and less peaked.

[2] We have considered the data for mining fee observed for one particular channel closure https://blockstream.info/tx/c0471c9ff72a883aa45058029049ffa12b92d7379f44447bc1df52382c725c01, the mining fee can vary as observed for various closed channels in https://1ml.com/channel?order=closedchannels

IV. Effectiveness of HTLC-GP

***Claim** 1: 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 corrupt 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 $\frac{\gamma n(\frac{D}{2}+\frac{\Delta(n-2)}{6})}{1+\gamma n(D+\frac{(n-1)\Delta}{2})}$*

Proof: In *HTLC*, a given instance of attack locks $(n-1)\alpha$ coins in the path routing payment. The capacity locked in $\frac{\mathcal{B}_{EX}}{L}(n-1)\alpha$.

In *HTLC-GP*, U_n executes self-payment of amount v. It cancels the contract at time $t' = D - \delta$. Capacity locked is $((n-1)v + \sum_{i=1}^{n-1} Z_{v_{i-1},i})\frac{\mathcal{B}_{EX}}{L}$. In both the cases, we exclude the coins locked by the corrupt node while computing the unusable capacity and fee charged by the intermediate parties. Thus we substitute $Z_{v_{i-1},i}$ with $Z_{v,i}$. We measure the difference in capacity locked to judge the effectiveness.

$$\begin{aligned}
&\frac{\mathcal{B}_{EX}}{L}(n-1)\alpha - \big(\frac{\mathcal{B}_{EX}}{L}(n-1)v + \frac{\mathcal{B}_{EX}}{L}\sum_{i=1}^{n-1} Z_{v,i}\big)\\
&= \frac{\mathcal{B}_{EX}}{L}((n-1)\alpha - (n-1)v - \sum_{i=1}^{n-1} Z_{v,i})\\
&= \frac{\mathcal{B}_{EX}}{L}((n-1)\alpha - (n-1)v - \gamma v\sum_{i=0}^{n-1}\sum_{j=0}^{i} t_j)
\end{aligned} \tag{5}$$

Substituting $v = \frac{\alpha}{1+\gamma\sum_{j=0}^{n-1} t_j}$,

$$= \gamma\frac{\alpha}{1+\gamma(nD+\frac{n(n-1)\Delta}{2})}n(n-1)\frac{\mathcal{B}_{EX}}{L}(\frac{D}{2}+\frac{\Delta(n-2)}{6}) \tag{6}$$

The loss percent is ratio of difference of capacity locked in *HTLC* and *HTLC-GP* and capacity locked in *HTLC*.

$$\begin{aligned}
&\frac{\gamma\frac{\alpha}{1+\gamma(nD+\frac{n(n-1)\Delta}{2})}n(n-1)\frac{\mathcal{B}_{EX}}{L}(\frac{D}{2}+\frac{\Delta(n-2)}{6})}{\frac{\mathcal{B}_{EX}}{L}(n-1)\alpha}\\
&= \frac{\gamma n(\frac{D}{2}+\frac{\Delta(n-2)}{6})}{1+\gamma n(D+\frac{(n-1)\Delta}{2})}
\end{aligned} \tag{7}$$

The loss percent of capacity locked by the attacker is $\frac{\gamma n(\frac{D}{2}+\frac{\Delta(n-2)}{6})}{1+\gamma n(D+\frac{(n-1)\Delta}{2})}$. The value is greater than 0 for $n \geq 2$. This proves that attacker ends up locking less capacity when HTLC-GP is used as a payment protocol. ■

V. Guaranteed minimum compensation

A. Calculation the maximum cumulative griefing-penalty

If the probability of remaining live is h and $(1-h)$ is the probability of suffering crash fault, then the payee would be willing to lock a maximum cumulative griefing-penalty $Z_{\alpha,max} = k\alpha$, such that the expected profit is greater than 0. Given that it gains α when it remains live, and loses $k\alpha + o_n^{D,k\alpha} + o_n^{D,\alpha} + o_n^{\tilde{t}_{n-1,n},remain(U_n,U_{n-1})}$ if there is a crash fault, the expected profit if the payee participates in the game is $h\alpha - (1-h)\big(k\alpha + o_n^{D,k\alpha} + o_n^{D,\alpha} + o_n^{\tilde{t}_{n-1,n},remain(U_n,U_{n-1})}\big)$ and the expected profit if it does not participate is 0. If a payee participates in the game, then the following relation must hold:

$$h\alpha - (1-h)\big(k\alpha + o_n^{D,k\alpha} + o_n^{D,\alpha} + o_n^{\tilde{t}_{n-1,n},remain(U_n,U_{n-1})}\big) \geq 0 \tag{8}$$

From the above equation, the payee calculates the maximum value of k for which it would be safe to participate in the game.

B. Adjusting Maximum Path Length

***Proposition** 1: Given the maximum cumulative griefing-penalty for a payment α is $k\alpha$, and the guaranteed minimum compensation ζ, the maximum allowed path length $\tilde{n}^{\zeta,k}$ is $\frac{k}{\zeta}$.*

Proof: In *HTLC-GP*, $Z_{\alpha,max} = k\alpha$ when payment is routed via the maximum allowed path length $\tilde{n}^{\zeta,k}$. Upon introduction of *guaranteed minimum compensation*, any node routing a payment α is entitled to a minimum compensation $\zeta\alpha$ upon being affected by the griefing attack. If the compensation falls below this amount, the node will refuse to forward the contract. Thus, the recipient must bear a cumulative penalty of at least $\zeta\tilde{n}^{\zeta,k}\alpha$ for a path of length $\tilde{n}^{\zeta,k}$. Thus, the following criteria must hold:

$$\begin{aligned} &\tilde{n}^{\zeta,k}\zeta\alpha \leq Z_{\alpha,max} \\ &or, \tilde{n}^{\zeta,k}\zeta\alpha \leq k\alpha \\ &or, \tilde{n}^{\zeta,k} \leq \tfrac{k}{\zeta} \end{aligned} \tag{9}$$

Thus the maximum path length in HTLC-GP$^\zeta$ is $\frac{k}{\zeta}$. ■ From the expression, we observe that $\tilde{n}^{\zeta,k}$ is inversely proportional to ζ.

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

***Proposition** 2: 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 $\frac{2\zeta^2}{2\zeta D+\Delta(k-\zeta)}$.*

Proof: For ease of analysis, we ignore the processing fee charged by each intermediate party. The cumulative penalty locked by the recipient is summation of the compensation of each intermediary and the source node forwarding the conditional payment. Given that $Z_{\alpha,max} = k\alpha$ and maximum path length for routing is $\tilde{n}^{\zeta,k}$, we estimate $\gamma^{\zeta,k}$:

$$\begin{aligned} k\alpha &= \gamma^{\zeta,k}\textstyle\sum_{i=1}^{\tilde{n}^{\zeta,k}}(D + (\tilde{n}^{\zeta,k} - i)\Delta)\alpha \\ or, \quad \gamma^{\zeta,k} &= \frac{k}{\Delta\tilde{n}^{\zeta,k}(\frac{D}{\Delta} + \frac{\tilde{n}^{\zeta,k}-1}{2})} \end{aligned} \tag{10}$$

Replacing $\tilde{n}^{\zeta,k}$ by the expression given in Proposition 1, we have $\gamma^{\zeta,k} = \frac{2\zeta^2}{2\zeta D+\Delta(k-\zeta)}$. ■

Procedure 1: Release_Phase for U_κ

Input: Message M, time bound μ
if $M \stackrel{?}{=} Payment\_Contract(H, Y, \alpha', t')$ *and* $current\_clock\_time - t_\kappa^{form} \leq \mu$ **then**
  Parse M and retrieve (H, Y, α', t')
  if $t' \geq t_{now} + \Delta$ *and* $\alpha' = \alpha$ **then**
    $z = x$
  end
  else
    $z = r$
  end
end
else
  $z = r$
end
Release z to $U_{\kappa-1}$
if $current\_time < t_{\kappa-1}$ **then**
  if U_κ *and* $U_{\kappa-1}$ *mutually agree to terminate* Payment Contract and Cancellation Contract **then**
    if *z*=*x* **then**
      $remain(U_\kappa, U_{\kappa-1}) = remain(U_\kappa, U_{\kappa-1}) + \alpha + \text{cgp}_{\kappa-1}$
    end
    else
      $remain(U_\kappa, U_{\kappa-1}) = remain(U_\kappa, U_{\kappa-1}) + \text{cgp}_{\kappa-1}$
      $remain(U_{\kappa-1}, U_\kappa) = remain(U_{\kappa-1}, U_\kappa) + \alpha$
    end
  end
  else
    U_κ goes on-chain for settlement by releasing preimage z.
  end
end
else
  $U_{\kappa-1}$ goes on-chain for settlement, claims $(\alpha + \text{cgp}_{\kappa-1})$.
  $z = null$
end
Call Release_Phase$(U_{\kappa-1}, z)$

VI. Effectiveness of HTLC-GP$^\zeta$

***Claim** 2: 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, $\tilde{n}^{\zeta,k}$ is the maximum allowed path length for HTLC-GP$^\zeta$ for a given pair of ζ and k, and a corrupt recipient rejects the payment at time $t' = D - \mu$, where $\mu \to 0$, the capacity locked in HTLC-GP$^\zeta$ is less than the capacity locked in HTLC, the loss percent being* $\frac{n-\tilde{n}^{\zeta,k}}{(n-1)\left(1+\gamma^{\zeta,k}nD+\gamma^{\zeta,k}n\Delta\frac{n-1}{2}\right)} + \frac{\gamma^{\zeta,k}\tilde{n}^{\zeta,k}\left((n-1)(D+\frac{(\tilde{n}^{\zeta,k}-1)\Delta}{2})-\frac{\tilde{n}^{\zeta,k}-1}{2}(D+\frac{(2\tilde{n}^{\zeta,k})\Delta}{3})\right)}{(n-1)\left(1+\gamma^{\zeta,k}nD+\gamma^{\zeta,k}n\Delta\frac{n-1}{2}\right)}$

Procedure 2: Release_Phase for $U_i, i \in [1, \kappa - 1]$

Input: z
Release z to U_{i-1}
if $z \neq null$ *and* $current\_time < t_{i-1}$ **then**
  if U_i *and* U_{i-1} *mutually agree to terminate* Payment Contract and Cancellation Contract **then**
    if z=x **then**
      $remain(U_i, U_{i-1}) = remain(U_i, U_{i-1}) + \alpha_{i-1} + \mathrm{cgp}_{i-1}$
    end
    else
      $remain(U_i, U_{i-1}) = remain(U_i, U_{i-1}) + \mathrm{cgp}_{i-1}$
      $remain(U_{i-1}, U_i) = remain(U_{i-1}, U_i) + \alpha_{i-1}$
    end
  end
  else
    U_i goes on-chain for settlement by releasing preimage z.
  end
end
else
  U_{i-1} goes on-chain for settlement after elapse of locktime t_{i-1}, claims $(\alpha_{i-1} + \mathrm{cgp}_{i-1})$.
end
Call Release_Phase(U_{i-1}, z)

Proof: In HTLC-GP$^{\zeta}$, the capacity locked is $((\tilde{n}^{\zeta,k} - 1)v + \sum_{i=1}^{\tilde{n}^{\zeta,k}-1} Z_{v,i})\frac{\mathcal{B}_{EX}}{L}$. In both the cases, we exclude the coins locked by the corrupt node while computing the capacity locked. We measure the difference in capacity locked in *HTLC* and HTLC-GP$^{\zeta}$.

$$\begin{aligned}
&\frac{\mathcal{B}_{EX}}{L}(n-1)\alpha - \frac{\mathcal{B}_{EX}}{L}((\tilde{n}^{\zeta,k}-1)v + \sum_{i=1}^{\tilde{n}^{\zeta,k}-1} Z_{v,i}) \\
&= \frac{\mathcal{B}_{EX}}{L}\Big((n-1)\alpha - ((\tilde{n}^{\zeta,k}-1)v + \sum_{i=1}^{\tilde{n}^{\zeta,k}-1} Z_{v,i})\Big) \\
&= \frac{\mathcal{B}_{EX}}{L}\Big((n-1)v(1+\gamma^{\zeta,k}\sum_{j=1}^{\tilde{n}^{\zeta,k}} t_j) - ((\tilde{n}^{\zeta,k}-1)v + \sum_{i=1}^{\tilde{n}^{\zeta,k}-1} Z_{v,i})\Big) \\
&= v\frac{\mathcal{B}_{EX}}{L}\Big((n-\tilde{n}^{\zeta,k}) + \gamma^{\zeta,k}\tilde{n}^{\zeta,k}((n-1)(D+\frac{(\tilde{n}^{\zeta,k}-1)\Delta}{2}) \\
&\quad - \frac{\tilde{n}^{\zeta,k}-1}{2}(D+\frac{(2\tilde{n}^{\zeta,k}-1)\Delta}{3}))\Big)
\end{aligned} \tag{11}$$

The loss percent is ratio of difference of capacity locked in *HTLC* and HTLC-GP$^{\zeta}$ and capacity locked in *HTLC*.

$$\frac{v\frac{\mathcal{B}_{EX}}{L}\Big((n-\tilde{n}^{\zeta,k})+\gamma^{\zeta,k}\tilde{n}^{\zeta,k}((n-1)(D+\frac{(\tilde{n}^{\zeta,k}-1)\Delta}{2})-\frac{\tilde{n}^{\zeta,k}-1}{2}(D+\frac{(2\tilde{n}^{\zeta,k}-1)\Delta}{3}))\Big)}{\frac{\mathcal{B}_{EX}}{L}(n-1)\alpha} \tag{12}$$

Considering $t_{n-1} = D$ and $t_i = D + (n-i-1)\Delta, i \in [0, n-1]$, where $\sum_{j=0}^{n-1} t_j = nD + \frac{n(n-1)}{2}\Delta$ and substituting $\alpha = v(1+\gamma^{\zeta,k}\sum_{j=0}^{n-1} t_j)$, the loss percent is

$$\begin{aligned}
&\frac{v\frac{\mathcal{B}_{EX}}{L}\Big((n-\tilde{n}^{\zeta,k})+\gamma^{\zeta,k}\tilde{n}^{\zeta,k}((n-1)(D+\frac{(\tilde{n}^{\zeta,k}-1)\Delta}{2})-\frac{\tilde{n}^{\zeta,k}-1}{2}(D+\frac{(2\tilde{n}^{\zeta,k}-1)\Delta}{3}))\Big)}{\frac{\mathcal{B}_{EX}}{L}(n-1)v(1+\gamma^{\zeta,k}\sum_{j=0}^{n-1} t_j)} \\
&= \frac{n-\tilde{n}^{\zeta,k}}{(n-1)\Big(1+\gamma^{\zeta,k}nD+\gamma^{\zeta,k}n\Delta\frac{n-1}{2}\Big)} + \\
&\frac{\gamma^{\zeta,k}\tilde{n}^{\zeta,k}((n-1)(D+\frac{(\tilde{n}^{\zeta,k}-1)\Delta}{2})-\frac{\tilde{n}^{\zeta,k}-1}{2}(D+\frac{(2\tilde{n}^{\zeta,k})\Delta}{3}))}{(n-1)\Big(1+\gamma^{\zeta,k}nD+\gamma^{\zeta,k}n\Delta\frac{n-1}{2}\Big)}
\end{aligned} \tag{13}$$

■

ACKNOWLEDGEMENT

We thank our anonymous reviewers for their valuable feedback. The work was partially supported by the European Research Council (ERC) under the European Union's Horizon 2020 research (grant agreement 771527- BROWSEC), by the Austrian Science Fund (FWF) through the projects PROFET (grant agreement P31621), and the project W1255- N23, by the Austrian Research Promotion Agency (FFG) through the COMET K1 SBA and COMET K1 ABC, by the Vienna Business Agency through the project Vienna Cybersecurity and Privacy Research Center (VISP), by the Austrian Federal Ministry for Digital and Economic Affairs, the National Foundation for Research, Technology and Development and the Christian Doppler Research Association through the Christian Doppler Laboratory Blockchain Technologies for the Internet of Things (CDL-BOT).

REFERENCES

[1] J. M. Buchanan, "Opportunity cost," in *The world of economics*, pp. 520–525, Springer, 1991.

[2] O. Osuntokun, C. Fromknecht, W. Paulino, O. Gugger, and J. Halseth, "Lightning pool: A non-custodial channel lease marketplace," 2020.

[3] B. G. Gebraselase, B. E. Helvik, and Y. Jiang, "Transaction characteristics of bitcoin," in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 544–550, IEEE, 2021.

[4] B. G. Gebraselase, B. E. Helvik, and Y. Jiang, "An analysis of transaction handling in bitcoin," in *2021 IEEE International Conference on Smart Data Services (SMDS)*, pp. 162–172, IEEE, 2021.

[5] P. Guasoni, G. Huberman, and C. Shikhelman, "Lightning network economics: Channels," *Available at SSRN 3840374*, 2021.

[6] Y. Kawase and S. Kasahara, "Transaction-confirmation time for bitcoin: A queueing analytical approach to blockchain mechanism," in *International Conference on Queueing Theory and Network Applications*, pp. 75–88, Springer, 2017.

[7] "Lightning 101: Lightning network fees." https://blog.bitmex.com/the-lightning-network-part-2-routing-fee-economics/, 2019. Accessed: 2019-01-22.

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