2021 September

George Kaloudis

A Deep Dive Into Lightning as a Bitcoin Scaling Solution

CoinDesk research

Content

CoinDesk research

Introduction

The Lightning Network is an overlay network powered by Bitcoin smart contracts – it is NOT a blockchain.

Bitcoin was introduced as a "purely peer-to-peer version of electronic cash" that "would allow online payments to be sent directly from one party to another without going through a financial institution." In the early days, it was exactly that; for a small group of people. Twelve years and 100 million users later, Bitcoin is prohibitively expensive for casual transactions and only capable of confirming up to roughly seven transactions per second. The latter point is not completely fair since Bitcoin provides final settlement versus a promise of payment later, but it still constrains bitcoin's ability to act as cash without adding functionality.

As such, the Bitcoin narrative shed the "electronic cash" use case in recent years and replaced it with "store of value" and "digital savings technology" use cases, likening it to a type of digital gold. But that does not mean the dream of bitcoin as a peer-to-peer version of electronic cash has died.

After El Salvador made bitcoin legal tender in June 2021, a common critique was that this was a bad idea since the entire Bitcoin blockchain only has enough transactional throughput to allow every Salvadoran to do one Bitcoin transaction every 20 days, assuming no one else in the world uses it at all.

There is, of course, a solution. El Salvador has implemented the Lightning Network to allow bitcoin payments to flow through its economy.

The Lightning Network is an overlay network or "second layer" built on top of the Bitcoin blockchain that uses user-generated micropayment channels to conduct transactions instantaneously. It was introduced in 2016 as an idea by Thaddeus Dryja and Joseph Poon and eventually implemented in 2018 as an open-source software solution.

In short, Lightning allows multiple transactions to occur away from the blockchain (or off-chain) and then keeps track of the state of the channel which is then confirmed on the Bitcoin blockchain with a tidy, single transaction. In practice, this leads to less congestion on the blockchain and makes transfer of value cheaper on a per-use basis because the fee structure of Lightning differs from Bitcoin.

This report will aim to give an introduction to what Lightning is, the metrics that can be used to characterize the current condition of Lightning, potential attack vectors developers are working to mitigate and the future of Lightning. Combined, these topics provide a primer to help individuals and investors learn about the Lightning Network and Lightning Network Finance or "LiFi."

Throughout, we capitalize the blockchain (Bitcoin) and use lowercase or trading symbols (bitcoin/BTC) for the asset. Dollars are U.S. dollars ($USD). Nothing in this report should be considered investment advice.

Lightning Network: A Quick Primer

There are entire books on this topic, but the following section can act as a brief overview of the important aspects of the Lightning Network. We assume the reader has a basic understanding of how Bitcoin works (for more on that, check out CoinDesk's Learn content here).

The Lightning Network is an overlay, peer-to-peer network that operates alongside Bitcoin and uses the Bitcoin blockchain to secure its transactions. Lightning does not have its own coin or token.

Lightning uses Bitcoin smart contracts, self-executing digital contracts with the terms and execution written as code or scripts, in order to build its network. To do this, Bitcoin nodes, computers that validate transactions and maintain the network, include additional software to also act as nodes for the Lightning Network. From there, the Lightning nodes open up channels with other nodes by executing a 2-of-2, bilateral Bitcoin smart contract and committing bitcoin to the payment channel. The channel setup effectively moves the committed bitcoin "off-chain" or on top of the Bitcoin blockchain, making the Bitcoin blockchain layer 1 and Lightning layer 2.

From there, the rules of the Lightning Network apply to that payment channel. Each side of the payment channel is now able to send bitcoin back and forth without having to wait for confirmation on the Bitcoin blockchain, which you must do for layer 1 transactions. Instead, the channel acts like a sliding scale with the balance at each end changing as bitcoin gets sent across the channel between nodes. When both parties choose to close the channel, the rules of the smart contract determine the final balance due to each node and settle that final state on the Bitcoin blockchain. So, while the Bitcoin blockchain will only see two transactions – the original commitment transaction and the channel-closing transaction – there could be any number of transactions that have happened in between.

This is hardly exciting in a two-node, one-channel world. However, the technical specifications of Lightning also allow payments to be routed through multiple nodes via channels. This is where the network effect kicks in. Node A can send a Lightning payment to Node C even if they do not have a channel opened together. If Node A has a channel open with Node B, and Node B has a channel open with Node C, Node A can send a payment to Node C by routing through Node B. For its trouble, Node B would be compensated with a nominal "routing fee."

On top of that, Node B does not have to be directly connected to Node C either. There just must be a path of channels between nodes that ***eventually*** connect Node A to Node C.

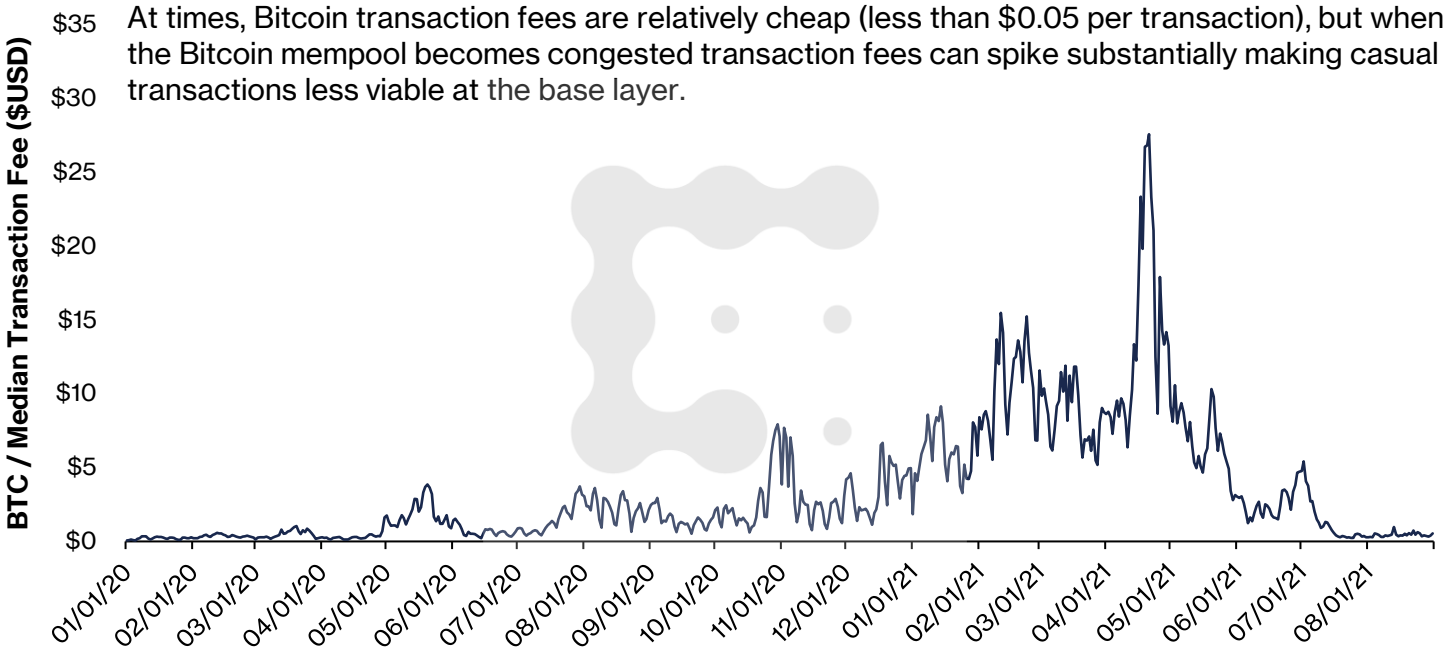
To wrap this section, we should point out two important characteristics of the Lightning Network.

First, it is cheap to send transactions on Lightning right now. Transactions can even be routed for 1 satoshi, which is 1/100,000,000th of a bitcoin or about $0.0005. Second,

because single Lightning payments are not dependent on the Bitcoin blockchain for transaction finality, payments are effectively instantaneous. Cheap and instantaneous payments is why many proponents are excited about the Lightning Network.

Bitcoin Transaction Fees

At times, Bitcoin transaction fees are relatively cheap (less than $0.05 per transaction), but when the Bitcoin mempool becomes congested transaction fees can spike substantially making casual transactions less viable at the base layer.



Source: Coin Metrics

Lightning Network: Metrics

The following section outlines several metrics to determine the overall growth, health and viability of the Lightning Network as a technology worth investing in or paying attention to.

There is an important limitation to note here. Not all Lightning nodes need to be announced to the entire network. When starting a node or opening a channel, there is an option to announce yourself to the entire network or to remain private and known only to those you are connected to. Therefore, the following metrics will represent, at worst, a lower bound to actuals. As a reference point, in 2020 BitMEX estimated that 28% of Lightning Channels were private.

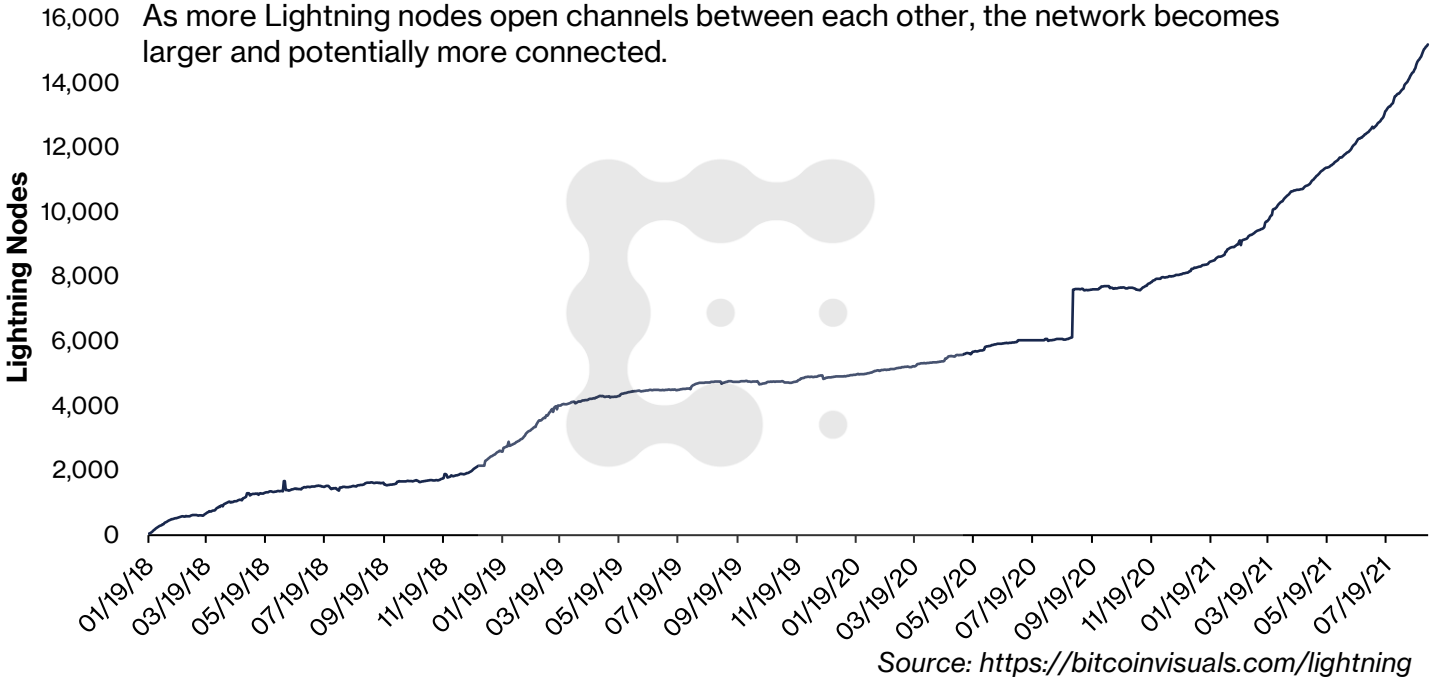
Public Lightning nodes with channels

As outlined in the previous section, the Lightning Network is an overlay network that routes payments through payment channels that are maintained by nodes. These channels are connected through nodes, and payments are routed through the channels until they reach a specified endpoint.

The first step in setting up a channel is to set up a node. One could stop after setup and just act as a node for the overlay network, which does not allow for anything functionally useful. It is more powerful to take it a step further and set up a payment channel with another node. To that point, a network with fewer nodes is less connected than a network with more nodes. There is not a number that is "good enough" for individuals to pay attention to, but an increasing number over time is generally a good trend. On Aug. 31, 2021, there were 15,203 public Lightning nodes with channels, up 30.3%, 63.8% and 99.5% over the trailing three-month, six-month and twelve-month period, respectively.

Public Lightning Nodes with Channels

As more Lightning nodes open channels between each other, the network becomes larger and potentially more connected.



Source: https://bitcoinvisuals.com/lightning

Lightning Network capacity

As described in the previous Nodes subsection, in order to open a Lightning channel, node operators must commit bitcoin to provide liquidity to their channels. The total amount of bitcoin committed to all channels combined is known as the Lightning Network capacity.

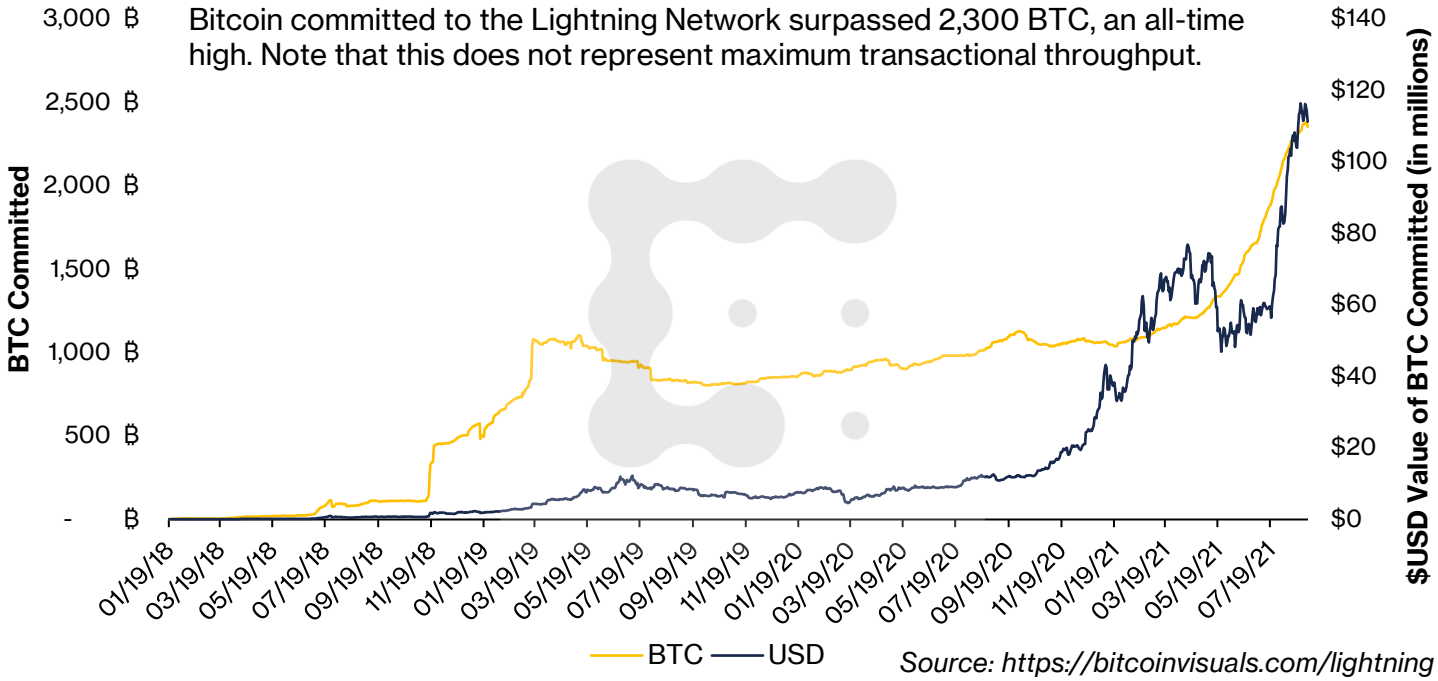
This is an important metric, but we should clarify that the total value of bitcoin committed should not be viewed as a maximum on the amount of value that can be transferred over Lightning over a unit of time. If anything, it is really a theoretical maximum on the amount that could be sent **at one time in one direction**.

To illustrate this, let us introduce a simple example. Think of Lightning channels like bilateral lines of credit with a collateral pool. If we both put $50 down to open a channel, then our channel capacity is $100 ($50 + $50), and we have a claim to $50 each. Suppose then I want to buy something from you for $25. We then change the balance of our channel to $25 for me ($50 – $25), $75 for you ($50 + $25). Suppose then, you want to purchase something for $10 from me. The channel balance would then move to $35 for me ($25 + $10), and $65 for you ($75 – $10). This can go on ad infinitum until we decide we are ready to close our channel and settle up. Over the life of a channel, value throughput can easily exceed the amount contributed to a channel.

This is exactly what occurs when a Lightning Channel is opened. A Bitcoin transaction is effectuated to commit value to the Lightning overlay network; that transaction is validated by the Bitcoin blockchain; Lightning payments are routed through the channel keeping track of the balance on each end; and then the channel is programmatically closed and validated on the Bitcoin blockchain. The blockchain only sees two transactions for a value *x*. In practice, more than two transactions can be effectuated and **far more value than** *x* could be transferred. With that understanding, we should view an increase in Lightning Network Capacity as a positive and a decrease as a negative.

Lightning Network Capacity

Bitcoin committed to the Lightning Network surpassed 2,300 BTC, an all-time high. Note that this does not represent maximum transactional throughput.



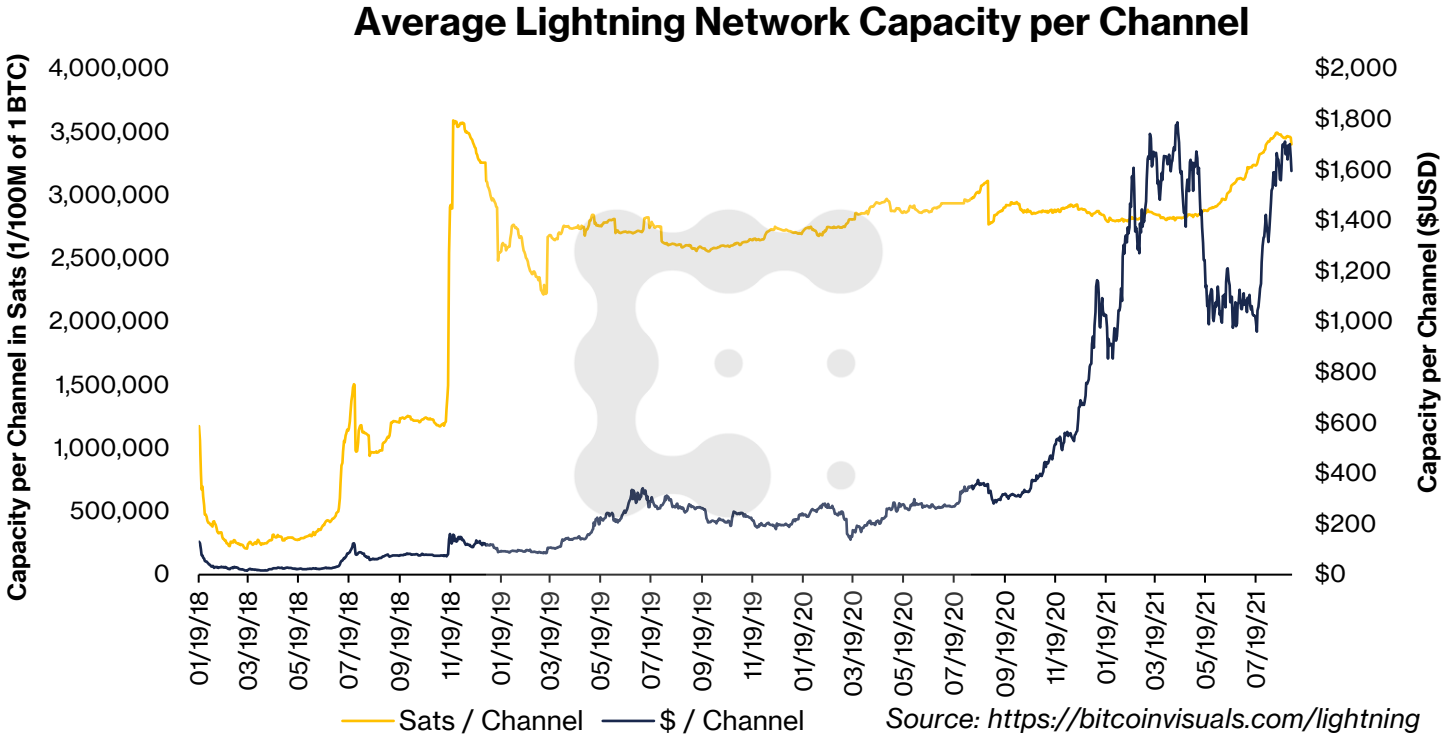
Source: https://bitcoinvisuals.com/lightning

As a quick aside, the amount of payment volume flowing through the Lightning Network would be a useful metric to look at. Unfortunately, that is not data that is publicly available to all nodes on the overlay network. However, there are some Lightning node operators that periodically provide volume data, which could be a decent proxy for Lightning transaction demand. We do not have network-wide data now, but as the network grows we may eventually be able to accurately approximate Lightning payment volume if large node operators begin reporting volume data consistently.

Per-channel and Per-node capacity

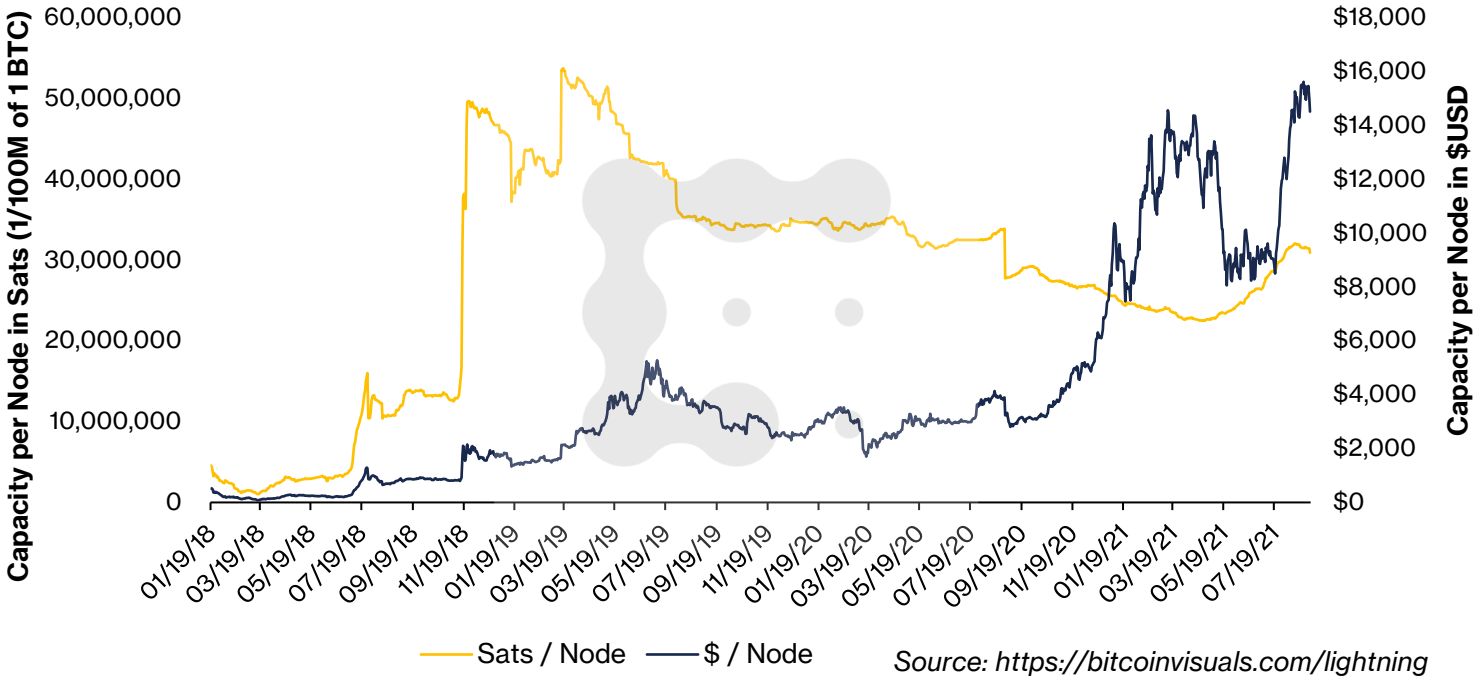
Expanding on the previous subsection, individuals can take Network Capacity a step further and divide by the number of channels or nodes.

Looking at these per-channel or per-node metrics can tell a good story about the condition of the Lightning Network. If the average capacity per channel exceeds ~$1,000 (~2,500,000 satoshis (sats) or ~0.025 BTC), that would imply that an average user who interacts with the Lightning Network will likely be able to make most reasonably priced daily purchases. If average capacity was ~$100 or ~$10, perhaps that would make most channels less viable for daily commerce (remember, per channel capacity is spread across two nodes).



Comparing per-node to per-channel capacity allows us to determine how potentially active node operators are. If the per-node capacity was close to per-channel capacity, that would imply that most nodes operate a small number of channels. As the gap widens, this implies nodes operate more than one channel. More channels per node implies higher demand for channel capacity **once nodes open a channel and "get off of zero."** If most nodes had just one channel, that could imply that the opening of the channel is mostly a novelty that only few customers use.

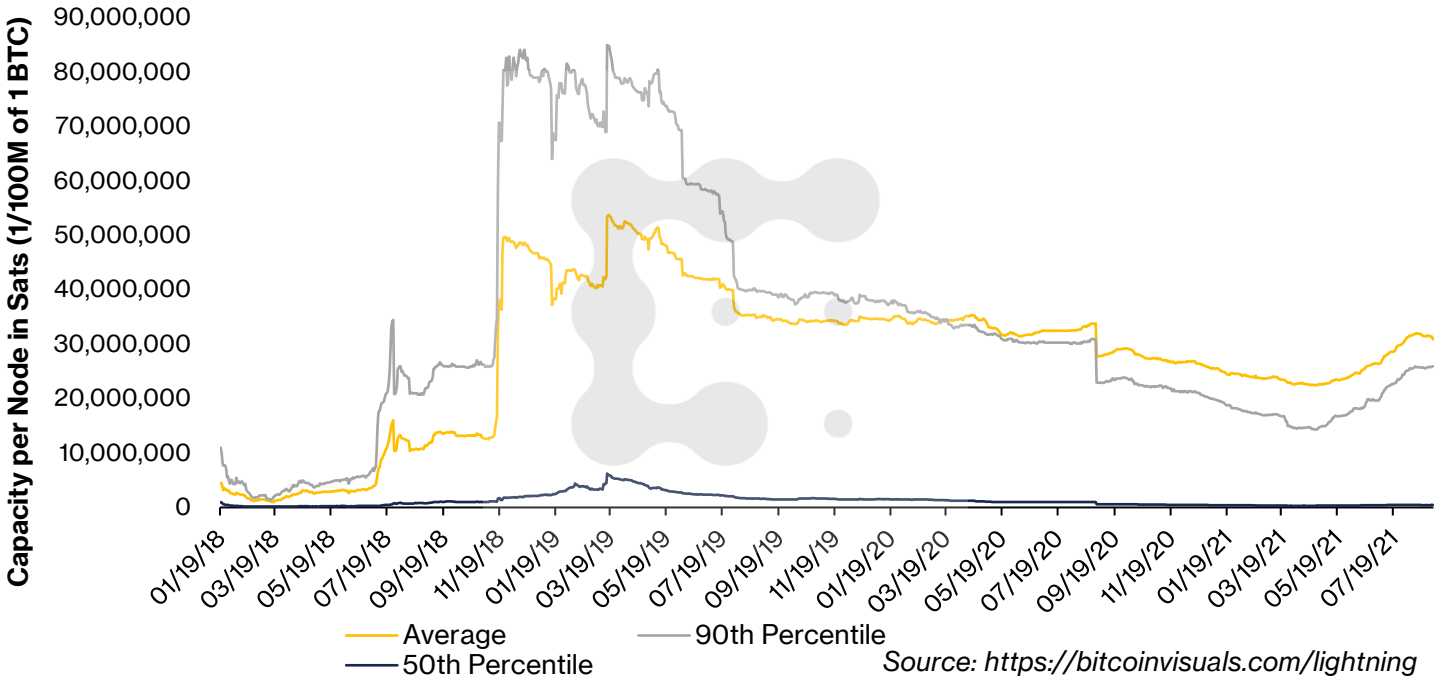
Average Lightning Network Capacity per Node



Source: https://bitcoinvisuals.com/lightning

There are some limitations here. First, these charts show averages, which are affected by outliers. If we look at the percentile breakpoints, we can get a more granular story as to what you can expect from the "average" node.

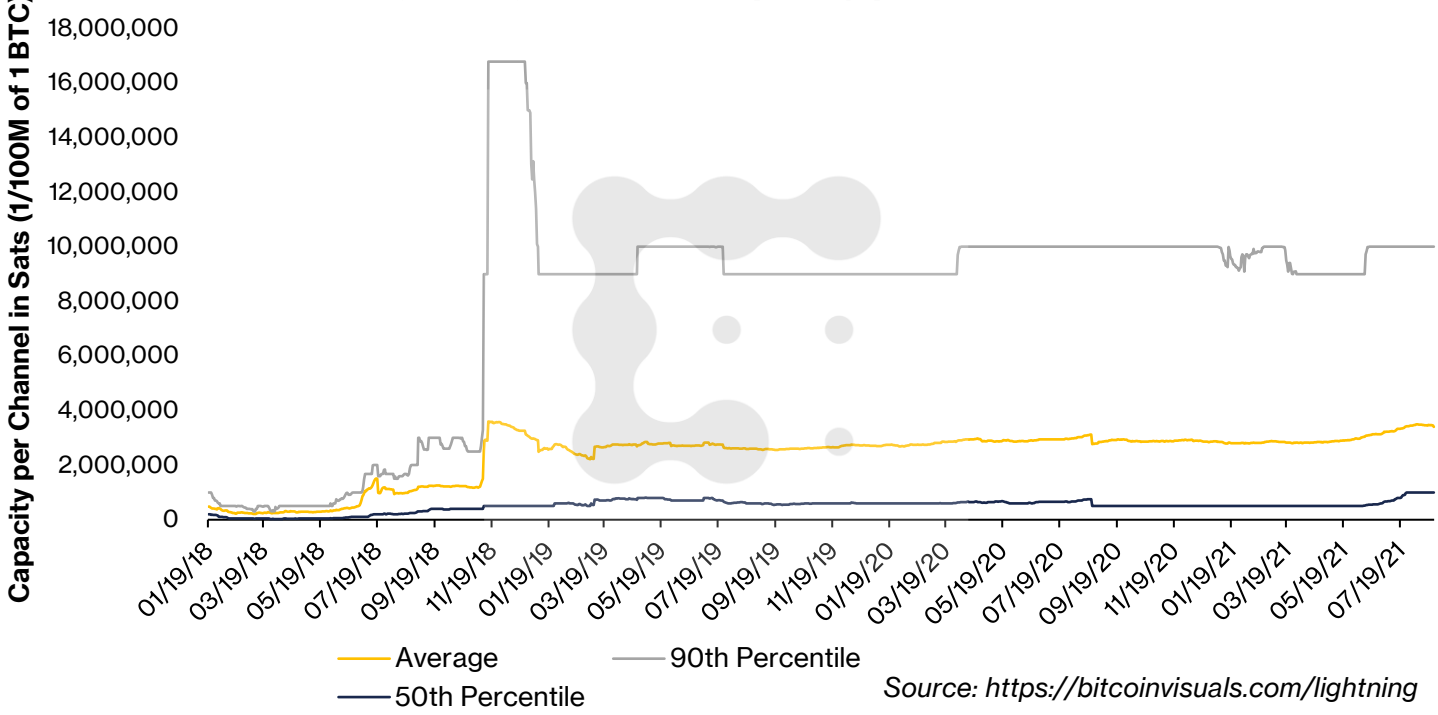
Lightning Network Capacity per Node



Source: https://bitcoinvisuals.com/lightning

Second, there is an arbitrary limit on the size of regular channels determined by the Lightning protocol of 16,777,215 satoshis (there are channels known as "wumbo" channels that support channels of unlimited size, but they are less common). That phenomenon reveals itself with the 90th percentile per channel data maxing out at 16,777,215 in August 2018, before coalescing around 9,000,000–10,000,000 satoshis.

Lightning Network Capacity per Channel



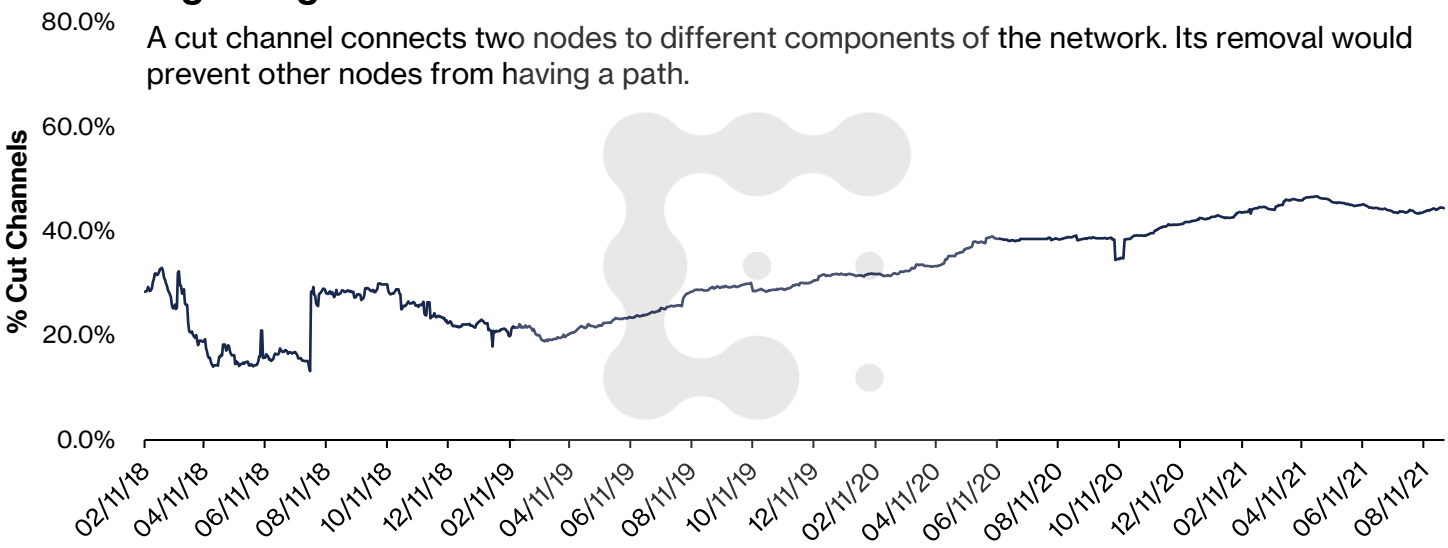
Source: https://bitcoinvisuals.com/lightning

Lightning Network cut channels and nodes

Cut channels are a means to measure the overall connectivity of a network. A cut channel is a channel between two nodes that connects different components of the network. This channel's removal would prevent other nodes from having a path. As such, cut channels are also referred to as bridges.

Lightning Network Cut Channels

A cut channel connects two nodes to different components of the network. Its removal would prevent other nodes from having a path.



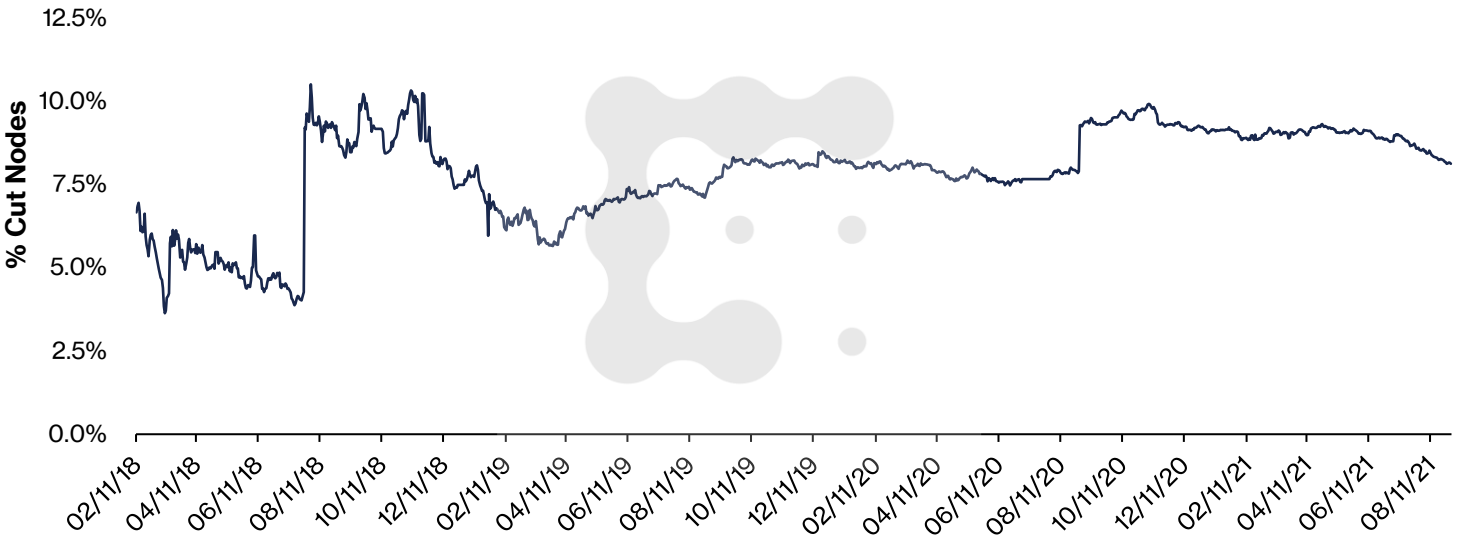
Source: https://bitcoinvisuals.com/lightning

As with the other metrics, there is not an optimal percentage of cut channels in the network. If the percentage is lower, then the network is theoretically better-connected than when the percentage is higher.

A cut node is the same concept as a cut channel, except it represents a node that connects two parts of the network.

Lightning Network Cut Nodes

A cut node connects nodes to different components of the network. Its removal would prevent other nodes from having a path.



Source: https://bitcoinvisuals.com/lightning

Intuition would suggest that we would prefer to see cut channels and nodes trend downward since that would indicate that the network is becoming more connected and less dependent on centralizing forces. Many users, developers and proponents herald the Bitcoin protocol as decentralized and hold that in high esteem, so that it would make sense that this holds for the Lightning Network as well.

That said, those who know about Lightning in that same group are not necessarily concerned about a potential Lightning "hub-and-spoke" construction – a phenomenon where large nodes run by merchant services own a large share of channel capacity that a large portion of the network must run through.

The expectation that the channel an individual opened with friends will be just as connected as channels run by a merchant service is far-fetched. Capital has to be allocated to open channels which will naturally lead to Lightning Network traffic flowing through bigger channels that will act as a hub. The value proposition of Lightning is that you need not use the centralizing hubs to route payments if you do not want to. Nothing stops an individual from setting up private, smaller channels with people they want to transact with. Lightning is still permissionless and does not require permission from big centralizing forces to use.

Lightning is the ability to choose.

Vulnerabilities, Attack Vectors and a Path Forward – A Developer's Viewpoint

Much literature and media content has been wildly polarizing when it comes to discussion around the Lightning Network. It is either characterized as a perfect product ready to fix all of Bitcoin's scaling problems or as a terrible idea that would best be set aside for some other coin to act as peer-to-peer cash.

Of course, reality lies somewhere in the middle and investors would be well served looking at the Lightning Network through the eyes of developers. In general, the Lightning developer community views Lightning as an exciting technology with massive potential. However, they also understand that there are vulnerabilities that need to be reckoned with if Lightning is to become widely implemented, and as the group with the most intimate understanding of the "nuts and bolts," their opinion and views should be taken into consideration.

In writing this section of the report, we had discussions with Lightning Network developers about attack vectors and their views on the future of Lightning. The findings are presented in the following subsections.

Attack Vectors

Before we dive into the specific attack vectors, we need to define a handful of Lightning terms.

Lightning uses Hash Time Locked Contracts (HTLCs) to route payments which contain two fundamental pieces: a hash lock and a time lock. This basically means that there is a secret (hash) that can be revealed for payments to be successfully routed – like a passcode – which is commonly referred to as **the preimage**. There is also a concept of a time-out where a payment can be claimed by either party after a certain amount of time passes. This time-out is used to avoid problems with negligent channel operators, but it can be taken advantage of by bad actors with a sophisticated understanding of Bitcoin and Lightning. When a node sends a payment, they do so by sending HTLCs. We will use Lightning payments and HTLCs interchangeably in the following subsections.

Also note that attackers can take advantage of their knowledge of how layer 1 works since Bitcoin nodes play an important role in the proper operation of the Lightning Network.

Griefing

A griefing attack involves freezing bitcoin committed to Lightning channels by spamming the channel with small payments. Lightning channels are only able to accommodate 483 in-flight or pending HTLCs at a time. Thus, an attacker can send 483 micropayments to another node they control through channels maintained by other nodes and then hold onto the HTLCs long enough to incapacitate those channels. This could cause funds to be held up for up to two weeks, at which point the time-out would cancel the contracts.

This attack cannot be used to steal funds, but it can be used for sabotage or to demand ransom from channel operators. Malicious actors could also shut down meaningfully large channels with little capital, some scripting knowledge and a bit of luck.

Griefing attacks can also lead to inadvertent loss of funds due to channel force closes that griefing attacks might instigate. A force close occurs when one channel partner attempts to close a channel without the other channel partner's consent. Typically, a force close is not ideal since funds will be locked for longer than a consensual channel closure, and the partner who opened the channel will have to pay a higher on-chain fee than usual given the design of Lightning that implemented a fee structure to discourage closing of channels for arbitrary reasons.

There has never been a big push from Lightning's maintainers to fix griefing. Joost Jager, however, is working on a concept known as Circuit Breaker. Circuit Breaker allows for node operators to assign a maximum number of in-flight HTLCs on a per-peer basis, making it impossible for a bad actor to flood a node with the max number of HTLCs. In order to be effective, Circuit Breaker would have to be implemented across the entire network, so this change will need buy-in from the broader community.

Eclipse Attack

An Eclipse Attack, aka a time-dilation attack, involves a Sybil attack on Lightning Network nodes. To carry this out, an attacker launches hundreds of nodes in order to swarm a victim's node such that the victim is not connected to any honest nodes. This effectively blocks the victim from the actual peer-to-peer network and the attacker can dictate what the victim sees.

From there, an attacker can close Lightning channels, and since the victim is not able to know what the network is actually doing, the attacker can steal funds.

At first blush, this does not seem to be a big deal. If you are running a full node, then it is likely that you would be too widely connected to honest nodes to be adequately attacked. However, there are many "lightweight" implementations of Lightning Network that are used by some wallet providers. These implementations only receive data from the Bitcoin blockchain one block at a time and do not always have a copy of the blockchain's transaction history. Note that although Lightning Network is separate from Bitcoin, knowledge of the blockchain is still paramount. These light clients use the back end of blockchain processing to save space on resource-constrained devices – mainly mobile devices.

Herein lies the real issue. An eclipse attack would take advantage of those using a lightweight implementation of Lightning and Bitcoin, which likely means these are the users who are less sophisticated and well-capitalized. That clearly runs counter to the ethos and end goal of Bitcoin and Bitcoin-enabled services.

Most of what can be done to mitigate this attack vector comes from the user side, although there are some potential solutions developers are working on as follows:

- Higher connectivity and number of honest reachable nodes. Honest users should be encouraged to provide more resources to the network and make use of those resources more efficiently on the Bitcoin network, as Lightning Network is tied to layer 1. The more honest nodes committed to the network, the more difficult it becomes to hurt network participants as a dishonest node.
- Peer diversity with proactive topology improvements through peer rotation. This would increase the cost of a Sybil attack and therefore act as an effective countermeasure.
- The implementation of watchtowers which act as monitors of the network who send "breach remedy" or "justice" transactions as punishment when they detect a user who is attempting to broadcast incorrect channel states in order to cheat the protocol. Watchtowers in effect probe the network for bad behavior.

Pinning

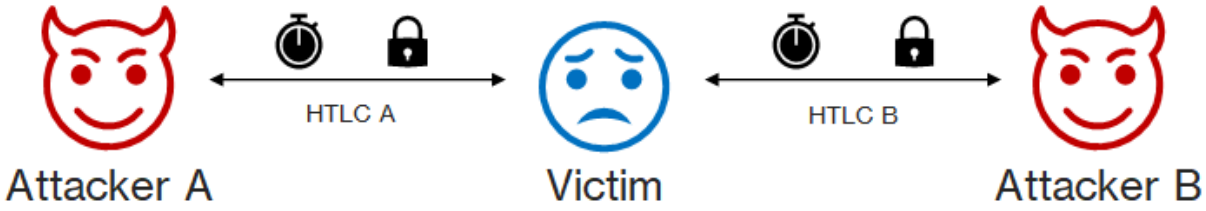
Pinning takes advantage of dissimilar transaction mempools and an inability for Child Pays For Parent (CPFP) transactions to be bumped when the parent transaction's fee rate is too low or when the transaction does not allow for Replace-By-Fee (RBF) (the latter two are related but slightly different concepts).

When Bitcoin transactions are initiated, they are aggregated into a collection called a "mempool" where miners look for transactions to include in blocks. CPFP refers to a transaction that references a previous transaction in order to increase the effective fee rate to speed up its addition to the blockchain, in the situation where the fee for the original transaction is too low to be carried out as quickly as desired. RBF refers to a transaction policy that allows an unconfirmed transaction in the mempool to be replaced with the same transaction but with a higher fee. Where CPFP and RBF differ is that CPFP transactions can always be attempted, while RBF transactions can only occur if the original transaction opted in to RBF.

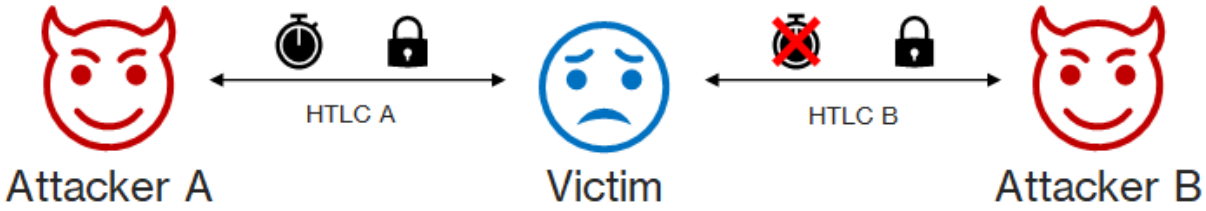
With these concepts in mind, a sophisticated attacker can use the Bitcoin and Lightning protocols to their advantage to carry out a pinning attack on pending Lightning transactions. There are many forms of pinning, but the simplest example is outlined in the visuals below. The visuals also illustrate how a time lock and hash lock effectively "wall-in" pending transactions between nodes (time lock at the left or before and hash lock at the right or after) until they are ready to go.

- The attacker sets up two channels with the target victim.

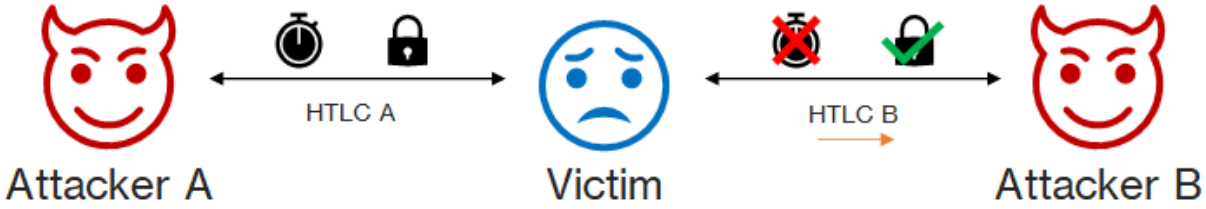
- The attacker then sends a transaction from Attacker A to Attacker B through these channels.



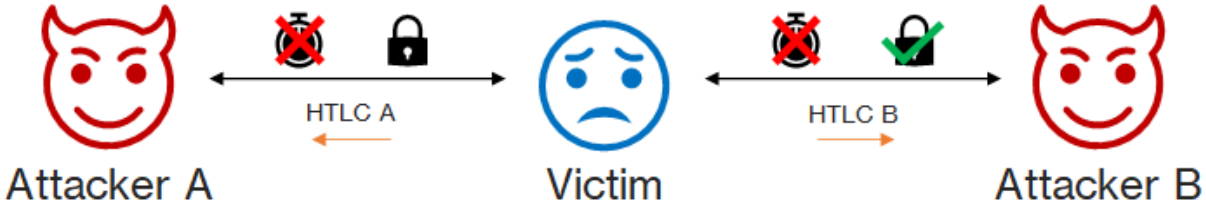
- When Attacker B receives the HTLC, they do not respond and wait for the timeout to pass. This forces the victim to publish a commitment transaction that contains a “HTLC-timeout transaction” in order to claim their funds contained in HTLC B between Victim and Attacker B.



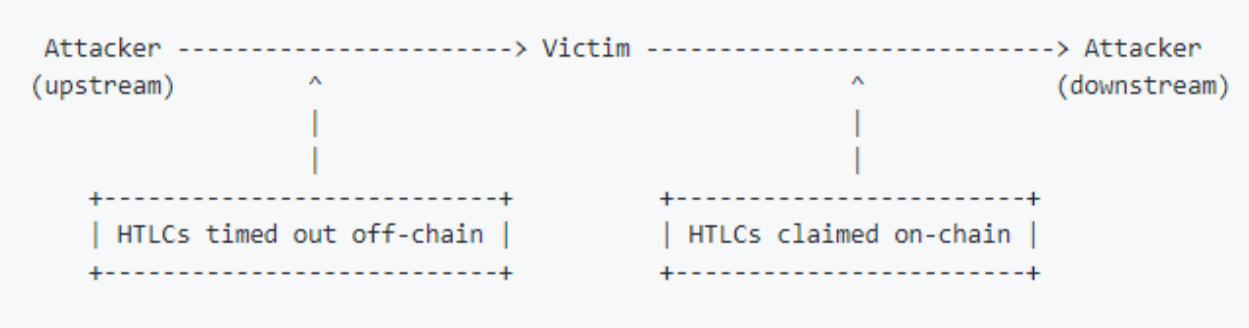
- The attacker then broadcasts a transaction to claim HTLC B between Victim and Attacker B – revealing the hash lock secret – with an intentionally low fee with RBF disabled. The fee is set intentionally low as the transaction must not confirm before Attacker A is able to pull HTLC A. Otherwise the attacker's HTLC B is mined successfully, allowing the victim to see it and the requisite preimage, allowing them to pull the funds from HTLC A – which stops the attack. If the attacker’s transaction gets into miners' mempools before the victim's HTLC-timeout transaction, the victim will not be able to claim the funds back and HTLC B value would flow from Victim to Attacker B. The victim can attempt to increase the fee of its HTLC-timeout transaction with RBF, but they would not be able to replace the **attacker's transaction** because it has RBF disabled. The victim gets “pinned” in place, unable to do anything as they see the HTLC-timeout transaction in their own mempool, but it does not get mined.



- Meanwhile, the timelock for HTLC A from Attacker A to Victim expires, and Attacker A is able to claim HTLC A for themselves. When the Attacker's transactions get mined, the victim will have paid the HTLC downstream, but not received the corresponding amount upstream.



The following figure provides a summary and outline of the basics of a pinning attack.



Source: Bastien Teinturier
https://github.com/t-bast/lightning-docs/blob/master/pinning-attacks.md

More deeply, for HTLCs, all miners have a "success" transaction in their mempool which reveals the preimage to claim the HTLC and the rest of the network has a time-out transaction. The attacker ensures the preimage transaction has a low enough fee rate to be kept in the mempool (in general, miners will include transactions in blocks that have higher fee rates) so that the upstream channel is able to claim the timed out HTLCs.

If the preceding attack sounds overcomplicated, that is because it is. The good news is that pinning is immensely difficult to carry out. It would take someone with an intimate understanding of the Bitcoin blockchain and Lightning. However difficult, it is still very possible. There are a handful of updates developers are working on to mitigate this attack vector.

First – anchor outputs make this attack more difficult. Anchor outputs are special outputs in Lightning commitment transactions that are designed to allow the transaction to be fee-bumped. Anchor outputs do not stop pinning on their own, but they do make it more difficult. These had been proposed for Lightning for some time and are now live on the Lightning Network.

Second – there is something known as package relays that, when combined with anchor outputs, should make pinning attacks a thing of the past. Package relay is a proposed feature that would allow nodes to send and receive packages of related transactions which would be accepted or rejected based on the fee rate of the overall package, rather than each individual transaction. This buffets the main mechanism by which attackers are able to finish their pinning attack.

Flood & Loot

A Flood & Loot attack takes advantage of the fact that the Lightning Network uses time locks to route payments.

To carry out a Flood & Loot an attacker needs two nodes: a source node and a target node. With the source node, the attacker opens a channel with a victim and with the target node they open other miscellaneous channels. The attacker then sends as many payments or HTLCs as possible through the victim to the target node. The attacker accepts the payments when they reach the target node and sends back preimages for validation to the

source node.

At that point, the attacker's source node stops replying. This means that the victim must wait until the HTLCs time-out to close the channel on the Bitcoin blockchain. However, if the attacker times the channels to all close at the same time, the Bitcoin blockchain will become congested with nodes looking to close their channel at the same time. After the time-out, any past expired HTLCs can be claimed by the attacker using RBF.

This is a damaging attack since it leads to a loss of funds. There are several ways developers are working on mitigating the incidence of Flood & Loot attacks. Before outlining those, the most simple means, especially as an individual, to avoid these attacks is to only open Lightning channels with nodes you know and trust.

Things developers are working on:

- There is a high likelihood that a node is being attacked if it has many pending incoming HTLCs that the other party does not resolve. In this case, the channel should be closed as early as possible to avoid losing funds. There is support around a more sophisticated dynamic closing rules policy that adjusts the "commitment broadcast delta" – the time prior to HTLC expiration that nodes begin to unilaterally close channels – based on the potential loss that this channel may incur.
- Allow for a mechanism that would change the amount of HTLCs that can be sent through channels that nodes are connected to, based on a reputation-based score set by the node operator in response to peer behavior. The more reputable the node, the greater number of HTLCs can be sent through it.
- Anchor outputs had long been proposed as a mitigation technique for Flood & Loot attack – now that they are live on Lightning these attacks are more difficult.

Path Forward and Parting Thoughts

We asked developers what they were most concerned about and what they thought needed to happen to best push Lightning adoption in the future. They all had unique, nuanced answers, but there were a handful of common themes worth sharing in a bulleted list.

- Development on the Lightning Network should be done methodically and carefully in order to maintain consistent uptime – we cannot afford to "move fast and break things" on an open-source network with real funds at stake;
- In addition, the network and its implementations (the actual software that delivers the specifications of a proposed program) must remain committed to the technical specifications of the Lightning Network – we cannot "fall out of spec." If one of the popular implementations, such as Lightning Labs' *lnd*, ACINQ's *eclair* or Blockstream's *c-lightning*, deviate from the spec in order to pursue something they view as superior, that would not only be damaging to Lightning, but it would also be a re-creation of the financial payments system we have now;
- The Lightning Network is still nascent, and we need more users in order to test the network, since ideas that work in a testing environment may not work once real-life incentives come to bear;
- There are people and organizations who will look to "gamify" the network for economic gain – similar to the MEV bots that plague Ethereum – which could potentially become a problem as more value attaches itself to the Lightning Network;
- Theoretical problems we have known about can potentially become real problems as the network grows – an example cited directly from the Lightning white paper is the Forced Expiration Spam, Section 9.2;
- One developer told us that the Lightning Network may not end up working at very large scale – when there are billions of payment channels. The developer pointed to the dependence on the Bitcoin blockchain and its mempool as a reason why Lightning in its current design may not scale to billions of users.

This report and preceding list is not meant to be exhaustive, intentionally pessimistic or urge the reader to use an alternative. It is simply provided as a means to educate the reader on the potential speedbumps the Lightning Network may encounter on the road to scaling Bitcoin. Developers take the tack of "awesome – but what's broken?" toward their products – not because they do not want Lightning to succeed, but because they do. Investors, users and stakeholders would be well served doing the same. Casting a critical eye on breakthrough technologies is important for the long-term success of those projects.

The Lightning Network is promising, but there is still much work to do and a long way to go.

Further Reading and Thanks

There are countless information sources available online about the Lightning Network. We are including a listing of the books, academic papers, research reports and articles we felt were most important for the writing of this CoinDesk Research report. Our attempt with this report was to provide a one-stop-shop for the individual to understand Lightning. The following links provide further reading, education and context for the Lightning Network without which this report would not have been possible.

Andreas Antonopoulos, Olaoluwa Osuntokun and René Pickhardt wrote Mastering Lightning, which is available for free in a GitHub repository. The book is mostly a technical manual of how Lightning works, but the first part of the book is meant to be approachable for anyone regardless of technical background.

In discussions about pinning attacks with Bastien Teinturier of ACINQ, he forwarded us to a GitHub repository he maintains which has a good collection of in-depth articles about Lightning Network.

There is a breadth of shorter Lightning Network pieces, both news articles and technical primers, available on CoinDesk.com, including a two-part article series written by Colin Harper of Luxor Technologies (previously of CoinDesk). Links:

1. https://www.coindesk.com/bitcoin-lightning-network-vulnerabilities-not-exploited-yet
2. https://www.coindesk.com/bitcoin-lightning-network-vulnerabilities-pressure

Lastly, we want to thank Ryan Gentry (Lightning Labs), Antoine Riard (independent developer), Rusty Russell (Blockstream) and Bastien Teinturier (ACINQ) for taking calls from the author to discuss Lightning during the research process.

CoinDesk Research is **George Kaloudis** and **Teddy Oosterbaan**.

CoinDesk Research offers reports and multimedia programming by independent experts on crypto industry trends and assets, to help professional investors make sense of the rapidly evolving concepts and data.

You can see more of our work at www.coindesk.com/research.

Be sure to follow us on Twitter at @coindeskdata. You can reach us at research@coindesk.com.