BitMEX Research

The Lightning Network

25 January 2018

(Source: Flickr)

Abstract

In this piece, we explain the motivation behind the creation of the Lightning Network and why its scaling characteristics are superior to what we have today, potentially resulting in a transformational improvement. We describe some of the basic technical building blocks that make Lightning possible. We then examine some of its limitations, including the downsides of inferior security compared to transacting on-chain and why this makes Lightning potentially unsuitable for larger-value payments.

BitMEX Research

Filtering out the hype with unbiased, evidence-based reports on the crypto-coin ecosystem.

BitMEX Research is also active on Twitter and Reddit.

research.bitmex.com

Previous reports:

Mining Incentives, Part 3: Short Term vs. Long Term
(17/01/2018)

A Complete History of Bitcoin's Consensus Forks
(28/12/2017)

Bitcoin Gold: Investment Flow Data
(21/12/2017)

Public Companies with Exposure to the Crypto Space
(13/12/2017)

Update: Bitcoin Cash Investment Flow Data
(01/12/2017)

The motivation behind the Lightning Network

Blockchain-based payment systems typically work in a "broadcast to everyone" mode, in that when one makes a payment, one needs to broadcast the transaction to all participants in the network.

Nodes in such a system must:

- Store the transaction indefinitely,
- Verify the transaction, and
- Relay the transaction.

Miners, meanwhile, are required to engage in an energy-intensive competitive process to determine if the transaction makes it into the ledger, just in case a conflicting transaction occurs.

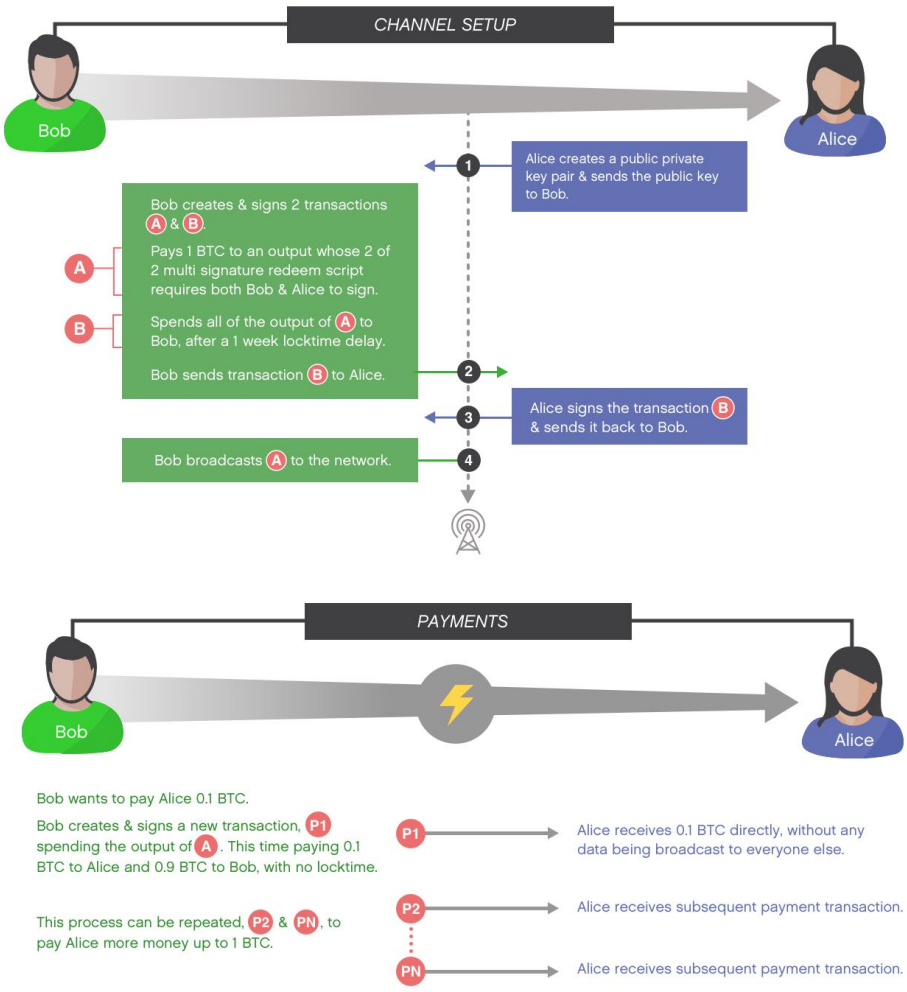
There isn't even special treatment for the recipient of the payment. For example, if one buys a coffee using Bitcoin, the transaction is broadcast to the entire Bitcoin network without prioritising propagation of the transaction data to the coffee shop or the coffee shop's payment processor. Many consider this process to be inefficient. If the objective is to build a payment system used by millions of people across the globe, this method does not seem logical.

The old "broadcast to everyone" announcement method at sporting events, during Arsenal's 3-3 draw at home to Sheffield Wednesday in May 2000. Prior to the widespread adoption of mobile phones, stadium announcers broadcast messages for individuals over the public-address system to all those in attendance. Mobile phones have made this process faster and more efficient, as messages can be sent directly to the intended recipient.

The Lightning Network represents an improvement in efficiency and uses a more logical payment-network structure. Instead of broadcasting a transaction to everyone, the transaction can be sent more directly to the payment recipient. Only when parties to the transaction are dishonest does one need to resort to the cumbersome process, which distributed censorship-resistant systems require to maintain consensus. In this way, one can achieve performance and efficiency almost equivalent to that of direct communication between the parties over the Internet, while retaining some of the security characteristics of Bitcoin's blockchain.

However, building such a payment system, in which all parties can always revert to the blockchain and reclaim their funds if there is a problem, is complex and has some significant risks and limitations.

Lightning's basic technical building blocks



Unidirectional micropayment channel.
(Source: BitMEX Research**)**

The diagram above depicts the traditional way to set up a basic unidirectional payment channel. Although setting up the channel involves broadcasting a transaction to everyone, once the channel is set up, multiple payments from Bob to Alice can occur by simply sending data from Bob to Alice, avoiding a broadcast to the entire network. The payment process can be repeated again and again until the funds in the channel, in this case 1 BTC, have been exhausted.

In theory, the above channel is secure for the following reasons:

- If Bob tries to renege on his payment, all Alice needs to do is sign and broadcast to the network transaction P1, which Bob signed when he initially made the payment. As long as this gets confirmed before the one-week locktime in transaction B, Alice safely receives her 0.1 BTC regardless of what Bob does.
- If Alice refuses to sign anything in order to frustrate Bob, all Bob needs to do is wait one week for transaction B to become valid, and he is then able to move the money from the channel to himself by broadcasting transaction B, which Alice has already signed.

This process is more secure if transaction A cannot be malleated by a third party (the TXID changing), otherwise Bob could have created transaction B only for it to become invalid as transaction A changes, thereby enabling Alice to hold the funds hostage indefinitely.

According to an e-mail that Satoshi sent to Bitcoin developer Mike Hearn, this basic structure was Satoshi's idea:

> *"One use of nLockTime is high frequency trades between a set of parties. They can keep updating a tx by unanimous agreement. The party giving money would be the first to sign the next version. If one party stops agreeing to changes, then the last state will be recorded at nLockTime. If desired, a default transaction can be prepared after each version so n-1 parties can push an unresponsive party out. Intermediate transactions do not need to be broadcast. Only the final outcome gets recorded by the network. Just before nLockTime, the parties and a few witness nodes broadcast the highest sequence tx they saw."*

(Source: tinyurl.com/y9km2xy5**)**

How the Lightning Network actually works

This micropayment construction can be considered the core building block for the Lightning Network, which is essentially a network of these payment-channel-like constructions. Payments find a path along channels which are already directly connected to each other until they reach the final recipient.

The channel construction used in Lightning builds on this basic structure with more advanced and complex technologies. The above construction is unidirectional, while in order to be useful, payments need to be made in both directions. For example, one can think of making payment channels bidirectional by constructing two channels between Alice and Bob, each in the opposite direction. More precisely, Lightning uses Poon-Dryja channel construction. This has lower liquidity requirements than simply setting up a network of unidirectional payment channels in opposite directions, which would require twice the amount of funds to be locked up inside the channel. However, Poon-Dryja channel construction has significant weaknesses compared to the other approach. Poon-Dryja channels require each party to sign a new transaction every time the channel is updated (a payment is made) while a unidirectional channel only requires the sender to sign when the channel is updated.

The old locktime feature can be replaced with more advanced functions:

- Check locktime verify (BIP65) can prove that the output cannot be spent until a certain date rather than ensuring a particular spend of the output is invalid until a certain date, which is what locktime does.
- Relative locktime (BIP68) can replace a specific end date with a date relative to the corresponding output. This can allow payment channels to remain open for indefinite periods, with a closure transaction triggering a time window during which the other party has a finite period of time (e.g., two weeks) to broadcast their reclaim transaction and recover the funds.
- Hashed timelock contracts (HTLC) can require the receiver of a payment to provide a string that hashes to a certain value by a certain date or returns the funds to the payer. This same hash can be used to trigger other payments in the channel network, enabling payments to be made across a chain of channels.

The resulting Lightning Network and its advantages

The Lightning Network should then, in theory, allow all participants in the network to make near instant and cheap transactions in all directions by finding a path among the nodes. This therefore avoids broadcasts to the Bitcoin network, as long as there are no problems, and results in a scalable network. The architecture even allows microtransactions and improves the privacy of payments.

Channels can stay open indefinitely due to the relative-locktime feature and there should be no counterparty risk; if anyone tries to steal funds through a hostile channel closure, the other participants to the transaction will have a significant time window in which to issue their own redemption transaction and get their money back.

Network functionality and user experience

A big unknown is how people and businesses will actually use the network, and commentators have different visions. Some see the Lightning Network as eventually being ubiquitous for small payments, with complexities handled in an automated way. Others more sceptical of Lightning typically envision the various components of the network requiring more of a manual construction when the system is used and a poor user experience plagued by unexpected channel closures and periods of Lightning Network downtime.

	Sceptical view of Lightning	Ambitious view of Lightning
Channel setup	In order to set up a Lightning channel, a user must manually create a new expensive on-chain transaction.	Setting up a Lightning channel will be a seamless process built into existing wallets and systems. When receiving a payment or purchasing Bitcoin, the funds need to go somewhere. Funds could immediately go into a Lightning channel as they are received and therefore setting up the channel requires no additional steps or costs.
Channel closure	Once the payment is complete, one needs to close the channel, with a manually created, expensive on-chain transaction.	There may be no need to close the channel and users can keep their wallet funds in channels indefinitely or for long periods of time.
Network routing	Routing is likely to be a significant problem, since finding a short path between parties is a difficult problem to solve algorithmically. If no route is found, the user and merchant will have to engage in the cumbersome process of selecting an on-chain transaction by manually changing the payment process.	1. The existing P2P network already requires a network topology and the relaying of messages, with nodes typically having eight connections. The Lightning Network topology is simply an extension of that. 2. Routing is not a significant problem, since even in massive networks the average number of steps in a path between users is small. 3. Even if there is a problem with routing, a payment could simply be made on-chain without the user even noticing the difference. 4. A small number of large channel operators can prevent routing problems.

Centralisation of payment channels	The network will centralise around a few large hubs as this is the most efficient model. This centralisation increases the risk of systemic channel failure, which is when a few large channels fail, resulting in a simultaneous mass exodus from payment channels and on-chain congestion, ensuring that some are unable to exit the channels before expiry.	Economic incentives act against centralisation; anyone can set up a node as there are low barriers of entry. In addition, there is an incentive to undercut other nodes by charging lower fees. Even if the network does centralise around a few large hubs, the Lightning Network still provides a useful and interesting system. Bitcoin already has a few large entities such as Coinbase that take custody of a large amount of funds. Under Lightning, the entities do not have custody of funds and merely act to relay data used for payments.
Liquidity	Payment channels will have insufficient liquidity and therefore the scope of payments will be limited. Payments of any reasonable size can almost instantly drain the liquidity of an entire channel, such that Lightning payments will need to be suspended.	Users will be incentivised to run Lightning nodes and provide liquidity in order to receive fees. The network will be used for small payments, far smaller in value than the maximum channel capacity, ensuring sufficient liquidity.
Requirement to be online when receiving a payment	With an on-chain transaction, all a sender needs is a payment address to make a payment; the recipient does not need to be online. In contrast to this, as explained above, a recipient in Lightning will need to sign a reclaim transaction before receiving a payment. This significant limitation means that recipients are required to keep their private keys exposed in a hot wallet. This makes Lightning impractical in many scenarios, such as making high-value payments, at ATMs, at in store PoS systems, or paying those with limited Internet connectivity.	Although a recipient is required to be online to receive a payment, this does not result in significantly different dynamics to most on-chain payments, since if the recipient is not online, they don't know about or cannot verify the payment anyway. It is also not necessary that the user or device directly receiving the payment needs to store the private keys. For example, an in-store PoS terminal or a crypto ATM machine could receive the signed redemption transaction over the Internet from the firm's HQ prior to receiving payments, communication that is necessary when making payments anyway.
Potential requirement to monitor the channel	Lightning Network participants may be required to monitor payment channels and then take action by a certain deadline in order to safeguard their funds. For example, a hostile reclaim transaction could trigger the start of a period in which the other party must also issue a reclaim transaction to protect their funds, before a certain deadline. This is a significant burden on users.	Channels do not need to be monitored at all times, as this depends on the window provided by the relative locktime. Channel-monitoring services (watchtowers) could mitigate this risk by monitoring channels on behalf of users: these services could either warn users in the event of a hostile reclaim transaction or could issue reclaim transactions themselves, if they were pre-signed and supplied beforehand by the users.

In reality, the truth may lie somewhere between these two visions, with the network potentially moving to the more ambitious vision over time. What this disagreement appears to come down to is that Lightning sceptics see it as a complex, incomplete, and impractical payment system based on the channel-construction system alone. Proponents see Lightning more as a scalable building block for a second layer on top of Bitcoin's blockchain, which will eventually be supplemented by wallets, payment protocol systems and channel-servicing companies, resulting in a simple and seamless user experience. Ultimately, wallets may be able to communicate with each other and then automatically, dynamically decide which payment methodology is best, on-chain or the most practical method via Lightning, without the user even knowing or caring.

The increased security risks of Lightning

- **Requirement to be online when receiving a payment:** As explained above, before receiving a payment, the recipient needs to sign a reclaim transaction so that the sender knows they can reclaim their funds in the event of hostile channel closure or a refusal to sign. Therefore, to receive money requires a hot wallet, meaning that private keys are potentially exposed if a security incident occurs.
- **Requirement to monitor the channel:** Lightning Network participants or watchtowers may be required to actively monitor the payment channels. This could place a burden on users or watchtowers and potentially reduces the security of funds inside a channel relative to Bitcoin stored on-chain. There is a risk of missing a reclaim-transaction deadline, either due to a failure to appropriately monitor the channel or perhaps because of on-chain network congestion.
- **Miners could censor channel-closing transactions:** 51% of the hashrate may have the ability to steal funds from Lightning users by censoring a channel-closure transaction, in which the miner is the other party. Although the potential consequences of this type of attack are already devastating without Lightning, the Lightning Network potentially offers hostile miners a slightly larger attack surface.

While each of these three factors alone may not be significant, the need to potentially expose one's private keys to the Internet when receiving payments, the risk of a hostile channel closure, and the risk of miners censoring channel-redemption transactions combined result in significantly inferior security — although all these risks can be managed to some extent.

There is a risk that lazy or poorly informed users keep too much money in a channel and funds are lost or stolen due to one of these failure scenarios. There is also the risk that price volatility results in users keeping more funds in payment channels than they would otherwise have intended.

Conclusion

The Lightning Network does appear to potentially offer significant and transformational improvements with respect to scalability. As a result, transaction speeds and transaction fee rates should dramatically improve, without impacting the underlying security of the core protocol. Crucially, however, the inferior security properties of Lightning payments may make the Lightning Network unsuitable for larger payments (or, at least, it may be irresponsible to use it for larger payments). Speculation and investment flows, which require these larger payments, currently appear to be the major driving force in the cryptocurrency space, with the volume of retail payments being relatively small in comparison. Because of that, Lightning may not be as big a game changer as some imagine, at least in the medium term. While enthusiasts appear likely to adopt this technology quickly, widespread adoption may take considerable time.

Disclaimer

Transacting on BitMEX is not offered or available to any resident of (I) the United States of America, (ii) Cuba, Crimea and Sevastopol, Iran, Syria, North Korea, Sudan, or any other sanctioned jurisdiction, or (iii) any jurisdiction where the services offered by BitMEX are restricted.

This material should not be the basis for making investment decisions, nor be construed as a recommendation to engage in investment transactions and is not related to the provision of advisory services regarding investment, tax, legal, financial, accounting, consulting or any other related services, nor is a recommendation being provided to buy, sell or purchase any good or product.

Any views expressed are the personal views of the authors of the report. BitMEX (or any affiliated entity) has not been involved in producing this report and the views contained in this report may differ from the views or opinions of BitMEX.

The information and data herein have been obtained from sources we believe to be reliable. Such information has not been verified and we make no representation or warranty as to its accuracy, completeness or correctness. Any opinions or estimates herein reflect the judgment of the authors of the report at the date of this communication and are subject to change at any time without notice. BitMEX will not be liable whatsoever for any direct or consequential loss arising from the use of this publication/communication or its contents.