SMITH+CROWN

ORIGINAL RESEARCH

The Lightning Network

The Lightning Network is a system of bi-directional payment channels that enables users to securely send fast, low-cost cryptocurrency payments. Lightning gained initial traction with Bitcoin as a layer 2 scaling solution by enabling efficient micropayments and instant transactions, which allows Bitcoin to function more effectively as a medium of exchange.

Overview

The Lightning Network builds on early Bitcoin technology to create an overlay network that functions as a scalable payment system. Lightning transactions offer considerably lower fees and faster settlement times than do Bitcoin base chain transactions. Considered in the context of Bitcoin's history of attempts to create scaling solutions, Lightning emerges as a promising initiative in furthering Bitcoin as a general purpose cryptocurrency.

NOTABLE DEVELOPMENTS

Q2 2013
Bitcoin Core contributor Matt Corallo develops a payment channel implementation for the bitcoinj library.

Q2 2015
Corné Plooy develops a network of payment channels, Amiko Pay, which requires backwards incompatible changes to the Bitcoin protocol.

Q1 2016
Joseph Poon and Thaddeus Dryja publish the Lightning Network's whitepaper, proposing a design fully backwards compatible with the existing Bitcoin network.

Q2 2017
Lightning is released on the Litecoin mainnet.

Q4 2017
Decred mainnet activates new OP codes necessary for future Lightning support through a token holder vote.

Q1 2018
Lightning is released on the Bitcoin testnet.

Q2 2018
Lightning is released on the Bitcoin mainnet.

Q4 2018
Lightning users lock $1 million in BTC into payment channels across 1,800 nodes.

Q2 2019
Lightning is released on the Decred testnet.

Lightning's Technology

Understanding the Lightning Network requires considering its underlying technology and cryptoeconomic incentivization structure. The network's design builds on earlier work in payment channel development, utilizing cryptography to trustlessly route payments without counterparty risk. As a layer 2 scaling solution, Lightning facilitates high throughput by taking transactions off chain, thus mitigating the constraint of a fixed block size.

PAYMENT CHANNELS

Though the Lightning Network design emerged in 2016, the basic concept of payment channels is not new—channels were supported in version 0.1 of Bitcoin, released in 2009. These payment channels allowed two parties to send off-chain transactions between one another and settle on the base blockchain when necessary. Payment channels are established and funded through an on-chain transaction, after which the two channel parties may send portions of the locked tokens between themselves without having to wait for external consensus. Payment channels afford users a degree of privacy in their transactions: the individual payments within the channel are only visible to the two parties participating in the channel, although the transactions opening and closing the channel are visible on-chain. Thus, pinpointing the exact value or timing of economic activity is difficult, particularly if that channel is open for an extended period of time.

These individual payment channels are particularly useful for parties who know in advance that they will frequently transact; for parties conducting one-off transactions, the base blockchain is typically more efficient. Further, individual channels offer potential gains in scalability. Payment channels lower the overall number of base blockchain transactions, since numerous transactions that would be processed on the chain occur on the channel instead and the channel closing is processed as a single transaction on the chain. In theory, millions of micropayments could be transferred back and forth between the two parties over the course of multiple years, and the only transactions recorded on-chain would be the channel opening and the channel closing. These scalability gains are potentially attractive to users of such blockchains—mainstream payment processors, such as Visa, can process ~1700 TPS, whereas Bitcoin's architecture facilitates only ~7 TPS.

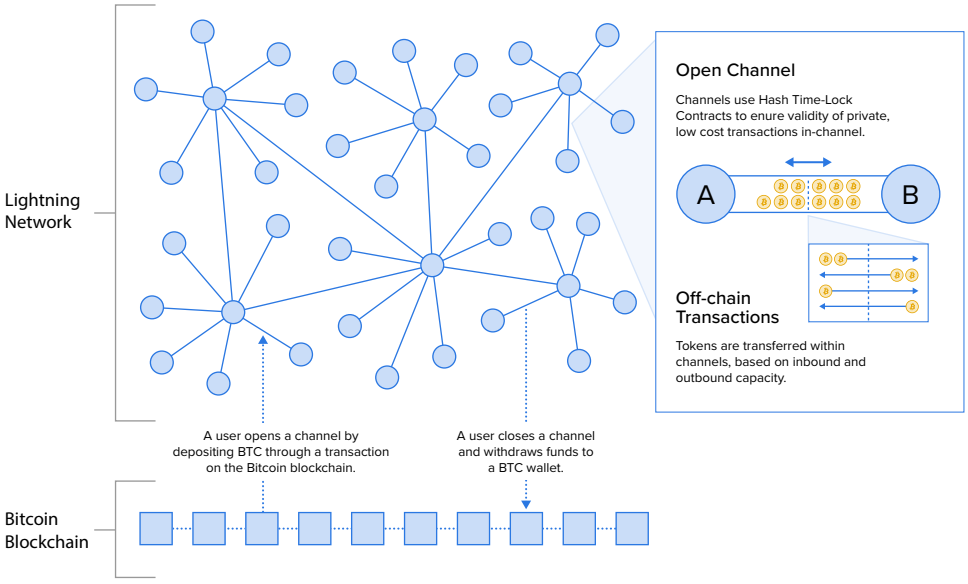
> The practical benefit of this system is that there is no counterparty risk in the routing process and users can access the entire network while only being directly connected to a small subset.

Lightning's key innovation is trustlessly routing payments among parties not directly connected by a payment channel. Despite the above in-channel scaling advantages, traditional payment channel technology is unsuitable for connecting every pair of Bitcoin users; such a network could require N^2 channels where N is the number of Bitcoin users. By trustlessly routing payments through third parties, Lightning reduces the number of channels necessary to connect the entire network, potentially enabling transaction throughput in line with Visa. Alice can pay Bob without needing to open an Alice-Bob channel, as long as a third party Carol has an open channel with both of them. Whereas, in Bitcoin, each node must verify all transactions, each Lightning node only must verify transactions in their own open channels. This significantly reduces the computational requirements for Lightning nodes, which consumer hardware easily runs.

Figure 1

How The Lightning Network Works

Lightning transactions are processed in payment channels, collectively forming an overlay network for the base blockchain.



The resulting network of bi-directional payment channels functions as an overlay onto a base blockchain, with each channel opening and closing being recorded on the base chain. This design is displayed in the above Figure 1.

HASH TIME-LOCK CONTRACTS (HTLCS)

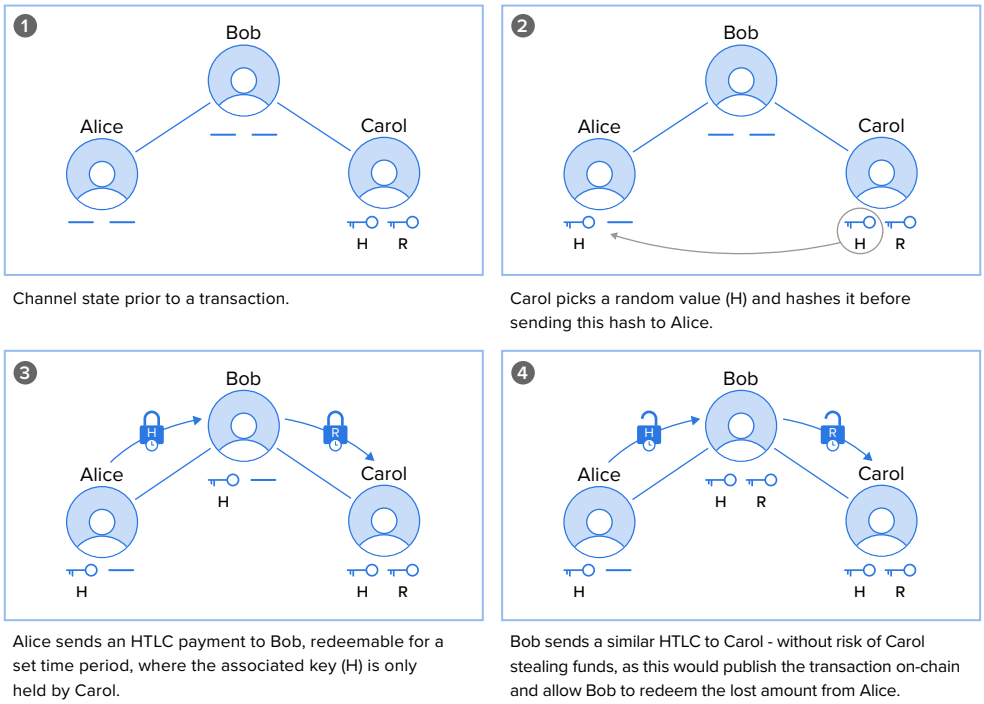
Lightning uses an architecture known as Hash Time-Lock Contracts (HTLCs) to ensure that intermediary nodes cannot intercept a transaction and that each party in a transaction can withdraw their funds at any time. HTLCs essentially allow one transaction to be made conditional on another, meaning that the intermediary is punished if they fail to correctly route the payment. If Alice wishes to send Carol

a payment via the Lightning Network and there exists no direct payment channel connecting Alice and Carol—as will frequently be the case—then intermediary payment channels can be employed. In the simplest case, Bob opens channels with Alice and Carol and routes payments between them. The practical benefit of this system is that there is no counterparty risk in the routing process and users can access the entire network while only being directly connected to a small subset.

Transaction integrity in this system is achieved through a cascading series of unlocked transactions, essentially forming a basic smart contract. Figure 2 demonstrates one such cascading series. In the depicted event, Carol picks a random value and hashes it before sending this hash to Alice. Expanding on this simplified three user case, HTLCs can also be used to route payments with several intermediaries, creating a payment network than can effectively route globally without requiring every user to be directly connected with every other user.

Figure 2

Anatomy of a Hash Time-Lock Contract



Channel state prior to a transaction.

Carol picks a random value (H) and hashes it before sending this hash to Alice.

Alice sends an HTLC payment to Bob, redeemable for a set time period, where the associated key (H) is only held by Carol.

Bob sends a similar HTLC to Carol - without risk of Carol stealing funds, as this would publish the transaction on-chain and allow Bob to redeem the lost amount from Alice.

ROUTING FEES

Lightning nodes can earn fees for routing transactions between two non-connected parties. Whereas, in Bitcoin, transaction fees are set by the payment sender and miners choose to include in blocks transactions with the highest fees, in Lightning, the routing node operators set fees and the payment sender chooses the most efficient path. Lightning software performs this process and does not require manual user input. Any Lightning node can opt in to route payments and earn

fees—there is no formal distinction between routing and non-routing nodes. Fees are separated into base fees paid per transaction and a fee based on liquidity used. Lightning nodes can manually set both these parameters. Because of these fees, routing nodes effectively act as BTC liquidity providers. One aspect of the Lightning Network's architecture is a routing protocol that finds the most efficient path between two transacting nodes, so as to minimize these routing fees. Currently, an average of five hops are needed to route a payment between any two nodes. The ability to passively earn routing fees introduces a protocol-level holding incentive for Bitcoin users who participate in the Lightning Network.

Lightning nodes may send and receive funds based on their available channel capacity. There are two types of channel capacity:

- **Inbound Capacity** - The amount of funds that third party nodes have added to connected channels; third party nodes own these funds. This is the total amount of funds that a node can receive; increasing it requires other nodes to open and fund new channels.
- **Outbound Capacity** - The amount of funds available for the node operator to send others; the node owner controls these funds. For a node operator, adding outbound capacity requires locking more funds within channels. These funds can be considered temporarily locked in Lightning and are the primary capital cost for node operators.

> A recent study by BitMEX Research experimented with varying fee rates, finding that nodes maximize revenue by setting the variable fee (paid by amount of liquidity used) at approximately 0.1 BPS. Running a routing node with this fee structure would yield estimated annual returns of 2.75%.

Providing routing capabilities requires nodes to fund Lightning channels that are well-connected to the rest of the network with both inbound and outbound capacity. For example, if node A sends its entire available outbound capacity to node B, A can only send further payments to B if it has outbound capacity with a node C that also has outbound capacity to B. To provide an efficient service in routing payments, nodes must frequently rebalance inbound and outbound channel capacity so that they can both receive and send large quantities from around the network. This rebalancing is presently done manually.

A recent study by BitMEX Research experimented with varying fee rates, finding that nodes maximize revenue by setting the variable fee (paid by amount of liquidity used) at approximately 0.1 BPS. Running a routing node with this fee structure would yield estimated annual returns of 2.75%. While the network may trend toward a higher fee rate if widely adopted and liquidity is in high demand, this may be mitigated on the supply side if managed liquidity pooling services emerge that allow a wide user base of BTC holders to provide channel capacity through a third party. Broadly, the fact that any node can earn routing fees by providing BTC channel liquidity arguably makes managing the Lightning Network a more widely participatory protocol than the base Bitcoin blockchain, as it lowers the barriers to network engagement and earning economic rewards. While users require specialized hardware—ASICs—to meaningfully participate in Bitcoin's consensus process, consumer hardware is sufficient for managing Lightning routing.

The Bitcoin Lightning Network

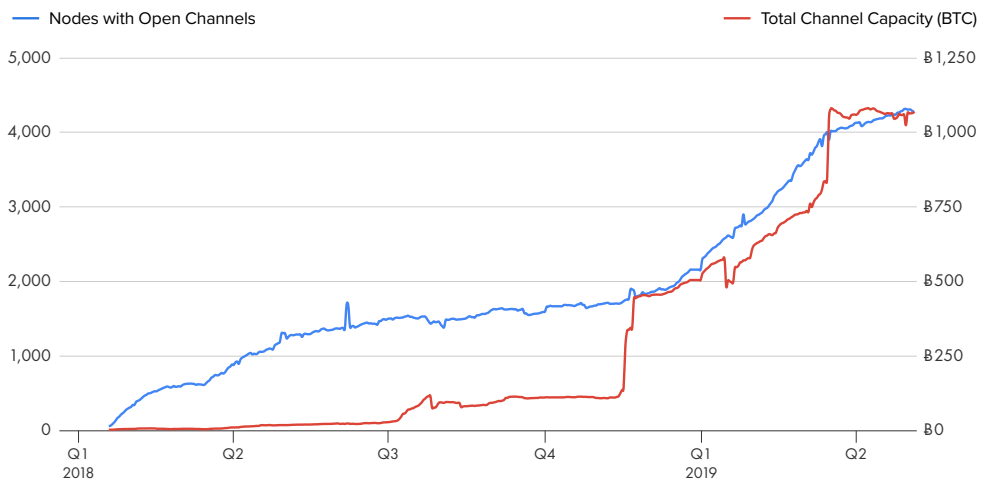
Bitcoin is the first blockchain to implement the Lightning Network, launching the mainnet in early 2018 and subsequently gaining significant traction. Bitcoin transactions that open or close a Lightning network channel appear identical to other Bitcoin transactions in block explorers and payments within Lightning Network channels do not appear in block explorers. The Litecoin network also operates a small Lightning Network and Decred aims to implement it in the future. Each of these networks would be distinct, but development progress is underway to enable cross-chain atomic swaps between each network.

Since launching, the Bitcoin Lightning Network has grown significantly as displayed in Figure 3, with over 4000 nodes holding nearly $6 million in BTC in channels.

Figure 3

Lightning Network Nodes & Capacity

Source: Bitcoin Visuals



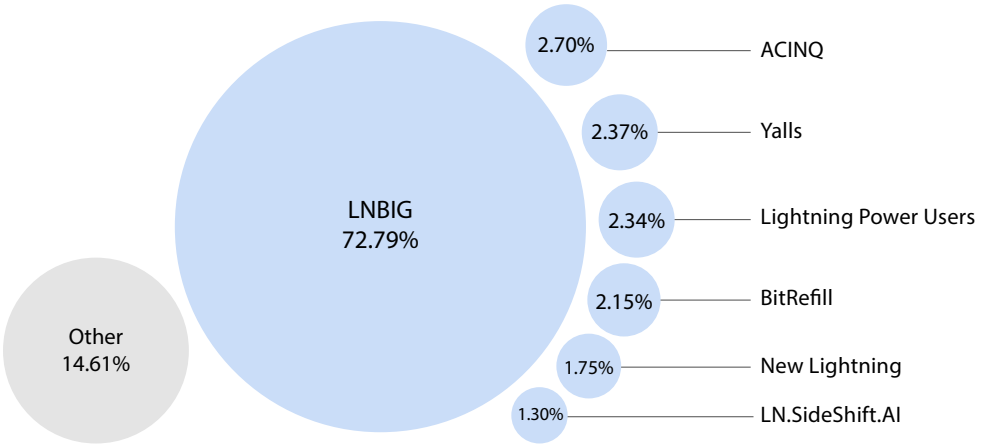
While there are a large number of Bitcoin Lightning nodes, a small number own the vast majority of the channel capacity. This distribution is displayed in Figure 4. These large capacity nodes are typically applications or service providers using the Lightning Network as a payment rail, such as the Twitter micropayments service Tippin.me. One provider, LNBIG, operates dozens of nodes and controls nearly 75% of the total channel capacity. While the network is still in its relative infancy and dynamics surrounding such payment hubs are likely to evolve over time—particularly as the routing fee market matures—centralization of capacity ownership is a trend that bears watching for its potential centralizing influence, partially analogous to the concentration of Bitcoin mining hash rate in a small number of mining pools. Such topology of Lightning network routing capacity creates central

points of failure were the network to gain widespread adoption; disrupting a small number of nodes could have considerable security and usability impacts on both Lightning and the underlying Bitcoin network. The fact that Lightning nodes are effectively hot wallets with more attack vectors (such as DDoS attacks) than cold storage heightens the risk of a more centralized network. The Prospects and Challenges section below discusses this issue further.

Figure 4

Bitcoin Lightning Network Channel Capacity Distribution

Source: 1ML



The above chart considers the total capacity across all operating nodes, not single nodes; ie, LNBIG operates over forty Lightning nodes, with each accounting for less than 4% of total network capacity.

DEVELOPMENT AND SERVICE PROVIDERS

A variety of service providers and development groups support the Bitcoin Lightning Network. There is no built-in protocol funding mechanism, similar to Bitcoin itself. Groups such as Lightning Labs, Blockstream, and the MIT Digital Currency Initiative serve as the de facto primary developers for the network, with each releasing a new Lightning client library in various programming languages. ACINQ is a French Bitcoin technology company that operates several large routing nodes and has developed user interfaces such as the Strike Lightning API for businesses and the Eclair mobile wallet. Casa offers pre-synced Bitcoin and Lightning full node setups that reduce the technical complexity for new users, while retaining self custody. BitFury, a manufacturer of Bitcoin mining hardware, offers merchant payment processing APIs and is developing a watchtower service to reduce the need for nodes to be online to verify transactions in their open channels. Lightning Loop offers channel liquidity management and automated channel setups to new users.

USE CASES

MICROPAYMENTS

Micropayments can be a significant cost for both retailers and web applications, with credit card transaction fees of roughly 1.5-2% plus a fixed cost of $0.11. Such fees can reduce profit margins for high volume, low unit price businesses. The problem is even more persistent in developing countries, as there are fewer all-purpose retail stores—a consumer often goes to several sellers to buy groceries, with each transaction amounting to less than a dollar. Since most credit card companies take $0.11 out of that dollar, traditional finance was often out of reach for small merchants, leading many to retain more traditional methods such as collecting cash. The Lighting Network enables micropayments with fees per transaction less than $0.0001 and may offer a compelling alternative for businesses affected by credit card processing fees.

> ...the instant settlement times and low transaction fees of Lightning transactions are potentially compelling for merchants and consumers. Customer experience could be very similar to that of credit cards and merchants could integrate Lightning within existing point-of-sale systems.

INSTANT TRANSACTIONS

Transactions on the Bitcoin blockchain take at least ten minutes to confirm and even longer during periods of high network use. This is a significant barrier for retail payment processor adoption; users are accustomed to the instant transaction finality of credit cards and do not want to wait ten minutes after buying a cup of coffee. Here, the instant settlement times and low transaction fees of Lightning transactions are potentially compelling for merchants and consumers. Customer experience could be very similar to that of credit cards and merchants could integrate Lightning within existing point-of-sale systems. Two examples of crypto projects leveraging this functionality are Lightning Peach and BTCPay. Existing payment processors such as Square are exploring integrating the Lightning Network into its Cash App and merchant payment services.

Prospects and Challenges

INCENTIVIZING ROUTING NODE LIQUIDITY

A key determinant of the Lightning Network's success is its ability to incentivize routing nodes to provide sufficient channel liquidity. Given the current relative difficulty of rebalancing inbound and outbound capacity and the capital costs in holding BTC within a channel, it is likely more efficient for a small number of nodes to emerge as payment hubs. These nodes would have significant channel capacity and be well-connected to the rest of the network. Indeed, such a network topology emerged in the early days of the Bitcoin Lightning Network, with eight entities managing over 75% of the total network capacity.

> Incentives to provide channel capacity are partially dependent on alternative passive returns that held BTC can generate, considering other consumer lending options such as BlockFi or institutional alternatives such as Genesis Capital.

The long run challenge for the network is incentivizing this liquidity provisioning by paying such routing nodes enough in routing fees to cover their operating and capital expenses, but not so much as to create high fees for users, which would reduce a core value proposition of the network. As noted above, BitMEX Research estimates that a routing node can earn 2.75% annually, though, in this nascent stage of the network, that may change significantly with more merchant demand for liquidity. Incentives to provide channel capacity are partially dependent on alternative passive returns that held BTC can generate, considering other consumer lending options such as BlockFi or institutional alternatives such as Genesis Capital.

Beyond the immediate investment returns that running a Lightning node may generate, payment processors or other heavy users of the network might operate nodes to support their core business line. Presently, the biggest barriers to providing liquidity is the technical and custodial risk, and the lack of tools to automatically rebalance channels—auxiliary services may emerge to mitigate these factors. If demand for the use of the Lightning Network continues to grow, supply (channel capacity) is likely to grow, assuming channel and node management becomes easier and more secure, and assuming investment returns are comparable on a risk adjusted basis with other lending or staking opportunities. This creates a dynamic fee market equilibrium for use of the Lightning network, somewhat similar

to transaction fees in base layer Bitcoin. As the Lightning Network matures and gains adoption, this will be a rapidly evolving issue to watch, one highly intertwined with broader crypto market forces.

CENTRALIZATION OF PAYMENT HUBS

Presently, providing significant routing capacity is technically challenging and has significant capital costs. Most channel liquidity is governed by a small number of nodes, often those that are using Lightning as a payment processor for an application or business. Thus, the network is relatively centralized, which presents a variety of potential risks. Since Lightning nodes are functionally hot wallets and more open to various forms of attack, this centralization of network functionality to just a few nodes presents a meaningful risk to Lightning. If only a few high-capacity nodes are disrupted, either through technical bug or malicious attack, the network may lose significant functionality. Such an attack could also have cascading effects on the base Bitcoin chain. While this risk may be mitigated with the development of third-party security tools that reduce the technical overhead of running secure personal Lightning nodes, it is unlikely to be eliminated entirely.

More broadly, payment hub centralization is only one such risk within the Bitcoin ecosystem, and users should consider the relative balance of enabled features with other approaches to scaling. A Lightning Network with a hub and spoke topology comprising of a limited number of payment hubs may provide sufficient network security for most users, particularly if the switching cost between hubs is low for users and the barrier to entry for new hubs is minimal. By leveraging returns to scale of operational and capital costs, payment hub operators may be able to offer smaller Lightning users lower routing fees and enhanced usability relative to a more equally distributed network. Such a network would represent a tradeoff of some degree of decentralization for scalability; in a context such as high volume digital payments where transaction fees and user experience are key distinguishing features, this may be reasonable. Further, since funds in payment channels can be easily reverted to the base Bitcoin chain, users can inherit some degree of its decentralization and security for cases where censorship from a Lightning hub is of particular concern.

Alternative approaches to scaling Bitcoin throughput also introduce forms of centralization risk. By significantly increasing the base block size, Bitcoin Cash raises the hardware requirements to run full nodes; this can also be seen as a centralizing force. Thus, while the centralization risks associated with Lightning payment hubs are meaningful, they may be considered in the context of other approaches to scaling and the relative importance of each facet of the blockchain scalability trilemma for a payment network.

MASS CHANNEL CLOSINGS

From a technical perspective, a key attack vector is the rapid closing of many Lightning channels. Each closing would post a new transaction in the Bitcoin mempool, potentially overwhelming the chain and preventing it from properly confirming transactions. While this is only one form of a Bitcoin transaction spam attack, in a scenario of a robust Lightning with a significant portion of the total BTC supply locked in payment channels, it does represent a single, concentrated trigger point for a spam attack. Such a scenario could delay Bitcoin transaction confirmations, increase base chain fees, and potentially delay other locktimed transactions until they become valid. That is, invalid channel balance states could be committed to the base chain.

> ...this issue highlights how security vulnerabilities in layer 2 blockchain protocols can affect not just themselves, but also the layer 1 networks in which they are rooted.

This scenario could occur either through a malicious attack of the Bitcoin network, or through a mass exodus of channel liquidity away from Lightning, in cases ranging from a codebase bug or broader movements within the crypto markets. This issue is highlighted in the original whitepaper (section 9.2) as 'possibly the greatest systemic risk when using the Lightning Network'. The effects of such a scenario may include: extreme delays in users accessing their bitcoin on the main chain, high transaction fees for all Bitcoin users, and/or invalid settlement of locktimed transactions if the attack is extended. In effect, movement of funds on and off Lightning is constrained by the Bitcoin block space available to confirm such transactions.

Considered more broadly, this issue highlights how security vulnerabilities in layer 2 blockchain protocols can affect not just themselves, but also the layer 1 networks in which they are rooted. These networks do not exist in a vacuum; Bitcoin users may be indirectly affected by a growing Lightning Network, even if they do not themselves use Lightning. While it is difficult to evaluate the prospects for individual networks in this early stage of layer 2 development, it is plausible that networks only loosely coupled in functionality with one another present less of a security vulnerability. In any case, evaluating the interplay between such networks presents a key design consideration moving forward.

USER EXPERIENCE & SECURITY

As an experimental, early stage technology, Lightning presently requires a significant degree of technical knowledge and security-awareness from its users. Typically, a user must run their own full Bitcoin node client, the Lightning client, and manage channel capacities manually while maintaining high network uptime. The requirement to be online to securely send or receive a payment (to ensure a channel with an invalid balance is not committed to the main chain), presents a significant usability barrier for many. While such issues are non-trivial barriers to adoption, they likely represent only a short, not long, run issue. In Bitcoin's early years, many users operated full nodes; today, most use a third party service.

Indeed, the Lightning community has already developed a variety of tools to improve the user experience. Watchtowers are third-party services that monitor the Bitcoin blockchain for discrepancies between on-chain transactions and closed channels with invalid states, reducing the need for every user to run their own Bitcoin full node to ensure the validity of channel balances. Such watchtowers could charge a small transaction fee and are presently in the early stages of development. Node Launcher is an integrated Bitcoin/Lightning node management app that abstracts command line technical complexity from the user. Joule is a web browser extension for managing Lightning payments, similar to MetaMask. Zap is a user-friendly GUI wallet that abstracts details around setting routing fees and managing channel capacity. Initiatives such as the Peach Wallet allow users to connect to a remote Bitcoin node with a local Lightning wallet, thus eliminating the storage requirements of hosting a full Bitcoin node. The Lightning Labs app utilizes the Neutrino protocol to run a lightweight Bitcoin client as a backend to a Lightning node; such an architecture could eliminate the need for Lightning users to run full Bitcoin nodes. The pace at which such solutions are developed will be an important factor in Lightning's adoption potential.

Lightning in Context

Broadly, Lightning is a key approach to scalability, an issue the blockchain community has long grappled with. Considered in the context of other layer 2 approaches to scalability, the Bitcoin block size debate, and its impact on cryptocurrencies outside of Bitcoin, Lightning emerges as an influential initiative touching key themes across much of the industry.

LIGHTNING WITHIN THE BLOCK SIZE DEBATE

The development of the Bitcoin Lightning Network is directly related to the Bitcoin/Bitcoin Cash fork in 2017. While Bitcoin Cash aims to scale transaction throughput by a larger base blockchain size, Bitcoin aims to scale throughput by taking small value transactions off-chain with solutions such as Lightning. This represents a broad philosophical divide within the respective communities, manifesting in differing views on optimal block sizes, SegWit, and, more broadly, the core value proposition of Bitcoin. Broadly, this debate can be framed as a disagreement over which layer represents the optimal venue to address transaction scalability issues.

The Bitcoin Cash developers point to Satoshi's supposed original vision where he or she intends for Bitcoin to be used as a means of payment without the use of financial intermediaries. In order to achieve this, the original Bitcoin capacity of seven transactions per second must be increased, either by increasing the base block size to accommodate more transactions at the base blockchain layer or by utilizing alternative means, such as SegWit and Lightning. As a result, two major factions formed, one advocating for an increase in block size and the other for SegWit, which changes how the transaction is assembled thus giving extra space for more transactions and enabling a transaction malleability protection that makes a Lightning implementation more secure. Ultimately, a majority of developers sided with SegWit and the advocates of an increased block size created Bitcoin Cash in mid 2017. However, even with SegWit implemented, Bitcoin transaction capacity effectively only doubled—Lighting is seen as a potential solution for adding orders-of-magnitude more capacity without changing features of the base Bitcoin chain.

The potential downside of scaling through increasing the block size (a la Bitcoin Cash) is that it significantly increases the hardware requirements to run full nodes and may centralize the network consensus process to only those who can afford to run nodes, arguably representing an approach at odds with Bitcoin's original appeal as an accessible P2P currency with a broad user base. A related objection could be levied against Lightning's approach, as discussed previously in the Prospects & Challenges section; given the technical and security complexity associated with running a Lightning node, the network could (and in these early stages of

development, has) centralize the majority of channel capacity to a small number of routing nodes.

While this also presents a meaningful risk of centralization, it should be noted that attacks on Bitcoin Cash nodes more directly interfere with security of the main network than do attacks on Lightning nodes, which are separate from Bitcoin nodes. Third parties could attack Lightning without significantly harming the base Bitcoin chain. Thus, while both approaches present centralization risks, the consensus centralization risks on the core chain of Bitcoin Cash are perhaps more critical.

> ...the median Bitcoin transaction fee peaked at $25 in late 2017; in contrast, Lightning Network transactions cost < $0.0001. The Lightning network could alleviate the base chain from having to process many small transactions, and instead reserve the limited block space for large or highly security-conscious transactions.

BITCOIN W/ LIGHTNING VS. OTHER GENERAL PURPOSE CRYPTOCURRENCIES

In evaluating Lightning's impact within the broader cryptocurrency landscape, perhaps the most salient comparison is between a Bitcoin network with a robust Lightning implementation and other scalability-focused general purpose cryptocurrencies, such as Dash and Bitcoin Cash. Broadly, a robust Bitcoin w/ Lightning represents a meaningful challenge to such cryptocurrencies, as it combines the security, adoption, extended history, and consistent monetary policy of Bitcoin with the scalable payment system of Lightning. All else equal, applications needing a 'money' will prefer the network with the most liquidity and consistent monetary policy. Without a Lightning network or other scalability solution, Bitcoin alone faces frequently noted challenges in becoming adopted as a means of payment for low value transactions, given the high transaction fees during periods of high network demand. For example, the median Bitcoin transaction fee peaked at $25 in late 2017; in contrast, Lightning Network transactions cost < $0.0001. The Lightning network could alleviate the base chain from having to process many small transactions, and instead reserve the limited block space for large or highly security-conscious transactions.

Relative to Bitcoin Cash, Bitcoin w/ Lightning offers a potential advantage of lower hardware requirements to run a full node. With its current 32mb block size, the Bitcoin Cash blockchain will grow quickly under a heavy transaction volume, making it more costly for the average user to participate in the network. With

Bitcoin w/ Lightning, users could validate their own transactions by running a Lightning node on consumer hardware, assuming that secure third party Bitcoin node providers emerge. Further, if Bitcoin Cash were to be adopted widely as a means of payment, the fixed block size still constrains scalability as a function of the number of payments, presuming all transactions were completed on chain with no intermediaries. This is in contrast to the Lightning Network, which faces some scalability constraints in the movement of funds on/off the network, but can support an arbitrary number of transactions once the channels exist. Whereas the scalability of Bitcoin Cash is constrained by the number of payments, the scalability of the Lightning Network is constrained by the supplied BTC liquidity in payment channels.

Bitcoin w/ Lightning offers similar scalability prospects as Dash and both architectures have the potential to centralize payment processing to a small set of nodes, given the capital costs in each. Bitcoin w/ Lightning arguably obviates one potential benefit of using Dash over just Bitcoin, as Dash was developed and adopted partially in reaction to Bitcoin's lack of scalability and appeal to merchants. While both projects have a similar value proposition and could each continue to find future use, the extended history and network effect of Bitcoin offers a compelling alternative to Dash. Dash's governance system offers a structured decision making and network funding process; no such analog exists in Lightning. Additionally, Bitcoin w/ Lightning offers different privacy features than Dash; channel closings and opening are non-private but transactions within a channel are private, whereas all Dash transactions are private.

> Lightning provides the option of using Bitcoin as an efficient payment mechanism (by reducing transaction costs and settlement times) without changing any of the monetary characteristics—deflationary emission and credibly fixed long-run supply—that arguably render Bitcoin an effective store of value.

A narrative has emerged over the past few years that Bitcoin's deflationary monetary policy and scaling issues render it more suitable as a savings than as a transactional instrument; that is, it functions more effectively as a store of value ('digital gold') than a medium of exchange ('buying coffees'). To some extent, Lightning challenges this narrative. Lightning provides the option of using Bitcoin as an efficient payment mechanism (by reducing transaction costs and settlement times) without changing any of the monetary characteristics—deflationary emission and credibly fixed long-run supply—that arguably render Bitcoin an effective store of value.

An analogy can be made to prior developments in gold-backed monetary regimes. Physical gold is expensive to move. Thus, governments issued gold-backed paper notes. Such notes had non-zero redemption risk and required an intermediary (a bank) to mediate the settlement. Base layer Bitcoin is also relatively expensive to move, motivating the development of the Lightning Network. However, Lightning's design aims to eliminate similar redemption risk by anchoring all in-channel BTC with base chain BTC, secured by the protocol without the need to trust an intermediate party. Thus, the development of the Lightning Network arguably moves the narrative beyond Bitcoin as primarily a store of value and towards Bitcoin as also a more effective medium of exchange.

LIGHTNING AS A LAYER 2 APPROACH

Outside of the Bitcoin Lightning Network, other projects are using many of Lightning's technologies and concepts in an effort to scale other protocols' transaction throughput. Raiden is a layer 2 scaling approach for Ethereum, utilizing a similar network of bidirectional state channels for transacting any Ethereum-based token. State channels are effectively a generalization of payment channels, allowing channel parties to monitor and update the state of any smart contract, not just the particular case of token transfers. A key design difference between Lightning and Raiden is the latter's use of a native payment token (RDN) to pay routing fees and incentivize node participation, in contrast to the Bitcoin Lightning Network's use of BTC. This introduces a degree of friction for users of Raiden, as they must also acquire and manage RDN to transfer other tokens. Connext Network is taking a similar approach in building a network of payment channels for Ethereum, though unlike Raiden does not use a native payment token and instead uses ETH or ERC20 tokens in channels. StarkWare is another layer 2 payment processing solution emphasizing scalability through STARK proofs, lower capital requirements than Lightning, and no liveness requirements for nodes.

Though technologically distinct from Lightning, other layer 2 scaling approaches also seek to increase transaction throughput by moving consensus formation off chain. Such examples include Loom Network, a Delegated Proof of Stake sidechain framework for Ethereum focused on gaming applications, and PoA Network, an Ethereum side chain utilizing a Proof of Authority consensus mechanism. While each of these projects, including the Lightning Network, are in relatively early development stages, the proliferation of layer 2 scaling approaches to major base blockchains represents a trend as such blockchains gain public adoption and face increased demand for limited block space. Blockstream's Liquid sidechain is another approach to scaling Bitcoin's transaction throughput, as a consortia network for inter-institutional settlement.

Base chain BTC can be transferred 1-1 with the sidechain's L-BTC, with the consortia members responsible for validating transactions. This approach is potentially useful for institutional entities, such as exchanges using Bitcoin as a settlement network for large transactions amongst (relatively) trusted parties without utilizing the limited block space of the Bitcoin base chain.