The Lightning Network - Deconstructed and Evaluated

Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) professionals, especially those working in the blockchain and cryptocurrency environment, may have heard of the second layer evolution of Bitcoin's blockchain - the Lightning Network, (LN). This exciting new and rapidly deploying technology offers innovative solutions to solve issues around the speed of transaction times using bitcoin currently, but expandable to other tokens. Potentially however, this technology raises regulatory concerns as it arguably makes, (based on current technical limitations), bitcoin transactions truly anonymous and untraceable, as opposed to its current status, where every single bitcoin can be traced all the way back to its coinbase transaction[1] on the public blockchain.

This article will break down the Lightning Network - analyzing how it works and how it compares to Bitcoin's current system, the need for the technology, its money laundering (ML) and terrorist financing (TF) risks, and some thoughts on potential regulatory applications.

Refresher on Blockchain

Before diving into the Lightning Network, a brief refresher on how the blockchain works - specifically the Bitcoin blockchain (referred to as just "Bitcoin" with a capital "B" herein) - is required.

For readers with no knowledge or those wishing to learn more about Bitcoin, Mastering Bitcoin by Andreas Antonopoulos[2] is a must read, and for those wishing to make their knowledge official, the Cryptocurrency Certification Consortium, (C4) offers the Certified Bitcoin Professional (CBP) designation.[3]

Put simply, the blockchain is a growing list of records that can be visualized as a series of blocks linked by chains. Each block contains specific information - in Bitcoin's case, a list of transactions and their data, which includes the time, date, amount, and the counterparties[4] of each transaction. At a high level, these transactions are verified by miners before being added to a block, which is subsequently broadcasted to the blockchain. On average, a new block is generated every 10 minutes and added to the chain (the public ledger), and includes a new list

[1] The "coinbase transaction" is the transaction inside any block that pays the miners their block reward (As of November 21, 2019, the block reward is 12.5 bitcoin). This is not to be confused with the Genesis block, which is the name of the first block of Bitcoin ever mined by Satoshi Nakamoto in 2009.
[2] https://bitcoinbook.info/
[3] https://cryptoconsortium.org/
[4] The counterparties are identified by public keys (also known as "addresses"). There is no personal identifiable data tied to these addresses.

of bitcoin transactions[5]. It is important to note for the purpose of this article that each block can only process a total of 1 MB worth of transactions, (currently approx. 1400-2800 transactions).[6]

New bitcoins are created when blocks are mined, and are given to the miner(s) as a reward for maintaining the blockchain. They can be exchanged for other currencies, products, and services through intermediaries, (e.g. exchanges, merchants, payment processors, etc).

There is much more to how the blockchain and Bitcoin functions than as explained above, but at this point readers should have sufficient knowledge to understand the Lightning Network at a high level.

Bitcoin as a Medium of Exchange

Bitcoin, including it's distributed ledger technology, (DLT) lead to a new payment system, creating a true digital currency that could be used as a medium of exchange. Bitcoin is a peer-to-peer (P2P) electronic 'cash' system, and is not centralized (not governed or controlled by a central authority). Instead, the technology is maintained by its users through the use of a peer-to-peer consensus protocol. This means all peers (referred to as "nodes") must agree on all changes - including validating transactions.

As such, many see Bitcoin as a payment system that revolutionizes traditional financial institutions and systems, and allows cheaper, easily auditable, borderless, and faster transactions.

However, for mass adoption to take place of this new payment system, Bitcoin needs to a viable and scalable medium of exchange instead of simply a store of value.

Transaction Processing Times

The Table below although dated, compares Bitcoin's transaction processing times (in seconds) to other online payment processors[7]:

Transactions per Second (TPS) Comparison Between Bitcoin and Other Payment Processors	
Visa	1700 TPS

[5] All transactions, including newly mined blocks, can be seen on a block explorer (ex: https://www.blockchain.com/explorer)
[6] https://www.blockchain.com/en/charts/n-transactions-per-block
[7] https://steemit.com/cryptocurrency/@steemhoops99/transaction-speed-bitcoin-visa-iota-paypal

Paypal	115 TPS
Bitcoin	7 TPS

The numbers above for VISA and Paypal were obtained based on the reported number of processed transactions per day. As such, these numbers are much bigger if we take into account the number of transactions per second VISA and Paypal are *capable* of processing. For instance, at its peak VISA processed 47,000 transactions per second in 2013[8]. On the other hand, due to Bitcoin's 1 MB limit per block, it can only at maximum process 7 transactions per second. Although this capacity was more than enough in 2009, the system has become increasingly congested over time.

This means users can end up waiting hours, if not days and weeks, for their transaction to be processed if transaction volumes were to match those of VISA. In fact, in late 2017 to early 2018, some users reported a wait time of 4 days for their transaction to be confirmed on the blockchain[9].

Transaction Fees

To understand how Bitcoin fees are determined, we need to keep in mind that a block can only contain 1 MB of transactions and that one block is generated every 10 minutes. Users can choose how much in fees they are willing to pay to the miners as an incentive to have their transaction included in the next block[10]. As such, when there are more than 1 MB of transactions waiting to be verified by miners[11], users have to increase the fee they are willing to pay to guarantee that their transaction will be processed quickly.

During the same period (late 2017 - early 2018) where transactions were taking upwards of 4 days to process, transaction fees averaged $52.18 USD per transaction[12]. For perspective, this means that if a user were purchasing a coffee of 2$ using bitcoin during a peak of high volume, the user's total would be $54.18 USD - a highly unrealistic price for a cup of coffee. If the average wait time of 4 days is included, the user would be theoretically standing at the coffee shop up to 4 days, waiting for their payment to be processed.

[8] https://www.visa.com/blogarchives/us/2013/10/10/stress-test-prepares-visanet-for-the-most-wonderful-time-of-the-year/index.html

[9] https://bitcointalk.org/index.php?topic=2586875.0

[10] When broadcasting a new block, the miner receives both the block reward and the sum of fees users include in their transactions. As such, miners will always include transactions with the highest amount of fees.

[11] The pending transactions are placed in queue, known as the mempool.

[12] A chart showing historically the average bitcoin transaction fee https://bitinfocharts.com/comparison/bitcoin-transactionfees.html

Transaction Transparency

As previously mentioned, no personal identifiable data is included in bitcoin transactions. A typical bitcoin transaction looks like the following[13]:

<table>
<tr><td colspan="3">Transaction Hash: 74dd5db962a23de77ce376dbf77fcf7437b2ae50b7f17643d0365ab2bcf8f409</td></tr>
<tr><td><b>18RQ6VrUjMib836GuiQkDRHGGWHL3J7Q1k</b>
0.003 BTC</td><td>></td><td><b>15FkFe35yeiumdBphDXXAgki8cGWctQ4j2</b>
0.003 BTC</td></tr>
</table>

The only information that can be used in this transaction to identify the involved users are the public keys (or commonly called "addresses"). The sender in this transaction is 18RQ6VrUjMib836GuiQkDRHGGWHL3J7Q1k, and the receiver is 15FkFe35yeiumdBphDXXAgki8cGWctQ4j2.

Although no personal identifiable data is tied to these public keys, blockchain intelligence tools (such as Chainalysis, CipherTrace, Elliptic, Crystal and Qlue) and clustering algorithms have been developed to try and identify the identity of the operators (individuals and entities) of public keys, which allows users of these tools to identify the source and destination of bitcoins. This can include identifying which exchanges, services, merchants, and illicit sources from which the funds originated, or to which they are being sent.

In a scenario where Bitcoin was mass adopted, this would mean that users and companies would potentially be able to see where and how users are spending their funds. As a comparison, this would be the equivalent of the transactions on an individuals bank statement being published online. The risks associated with this are numerous and highly debated, especially in terms of privacy and potential for theft - users holding large amounts of cryptocurrency are often the target of hacks and illicit actors.

Another problem surfaces with this level of transparency: the lack of fungibility. An asset or a good is considered fungible if an individual unit of the asset or good is interchangeable for another unit, (e.g. one dollar bill for another). An asset's ability to be fungible can make or break its potential as a viable medium of exchange.

With Bitcoin, one bitcoin is not interchangeable for another unit due to the ledger's transparency - thus, it is not fungible. This is because public keys/addresses of the following examples have been identified by blockchain intelligence tools: darknet markets, terrorist financing, OFAC sanctions, child abuse, stolen coins, ransomware, and scams. As such, currencies sent to or withdrawn from these source have essentially been 'tainted'. Therefore, if a user purchases

[13] https://www.blockchain.com/btc/tx/74dd5db962a23de77ce376dbf77fcf7437b2ae50b7f17643d0365ab2bcf8f409

bitcoins directly from another user, there is a risk that they have been given “tainted coins” that were obtained from a darknet market by the previous user. When the new owner of these funds attempts to ‘cash out’ through an exchange or equivalent service provider, there is a risk that the users account and funds becomes frozen, or the deposit blocked, due to the receiving exposure of the funds.

As such, ‘tainted coins’ are arguably not as valuable as ‘clean coins’, and users may hesitate in accepting funds known to be tainted to avoid triggering enhanced due diligence (EDD) requirements and potential asset seizure. These ‘tainted funds’ may then need to be sold under their market value to incentivize potential buyers.

In summary, Bitcoin, in its current state, is **not practicably scalable** and arguably as a consequence, not a viable medium of exchange.

The Lightning Network

In theory greater minds than the authors’ believe that Bitcoin’s scalability issue could be fixed by implementing an overlay network (a second layer) on its blockchain. This second layer would allow transactions to be processed ‘offchain’[14] directly between peers through payment channels.

The Lightning Network, whose white paper[15] was published on January 14, 2016, “is a decentralized system for *near* instant, high-volume micropayments that removes the risk of delegating custody of funds to trusted third parties.” The Lightning Network currently only functions with Bitcoin. We’ll break down how this technology functions by analyzing its key features while using an example (i.e. Alice buying a coffee from her favorite coffee shop) to provide context and clarity.

Scenario: Everyday, Alice purchases a coffee from the local coffee shop, BittCoffee. The coffee house has recently started accepting bitcoin as a payment option. As Alice owns 0.02 bitcoins (about $150 USD), she decides to use these to make her purchase.. However, when she approaches the counter to pay, she is advised by the barista that her payment needs to be confirmed on the blockchain before her coffee is prepared. In order to guarantee that her transaction would be chosen by the miners to be included in the next block (one block is added every 10 minutes), Alice will also need to pay a higher amount of transaction fees, which could end up costing her an additional $20 (approx). Furthermore, anyone who knows Alice’s and the coffee shop’s public key (their Bitcoin addresses) will now also be able to see that Alice purchased something from the coffee shop by consulting Bitcoin’s public ledger.

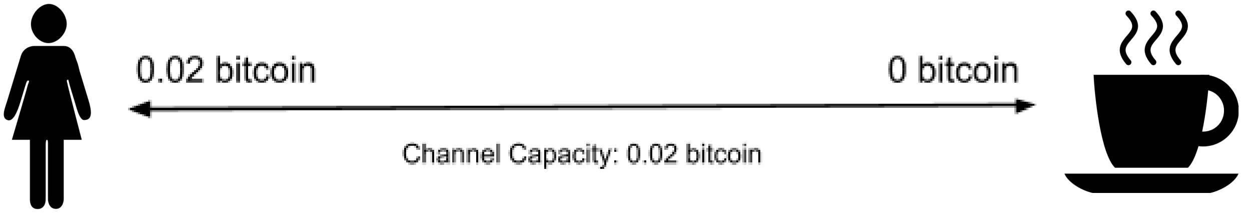
[14] Offchain: term used to describe cryptocurrency transactions that are not published to the public ledger (the blockchain).

[15] https://lightning.network/lightning-network-paper.pdf

Bidirectional Payment Channels

Running parallel to the blockchain, a payment channel is an offchain network that allows two or more parties to perform multiple transactions between each other, without having these transactions included (or “committed”) on the public blockchain[16]. The payment channels are considered bidirectional as assuming they are funded, both parties can send funds to each other through a single payment channel.

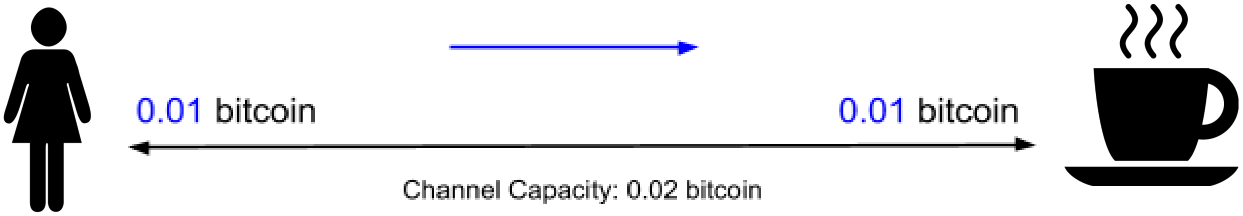
Using our example, Alice could open a payment channel with the coffee shop using the Lightning Network. To do this, Alice would scan the coffee shops Lightning public key using the Lightning Network wallet on her mobile phone and would enter the amount of satoshis (units of bitcoin) to fund the channel. In this case, Alice would fund the channel using her 0.02 bitcoin (2,000,000 satoshis). This is known as the “funding transaction” and is broadcasted (visible) to the blockchain. The coffee shop would enter 0 bitcoin as their funding capacity.



After 3 confirmations of the funding transaction (approximately 30 minutes), the payment channel between Alice and the coffee shop would be considered open, and the 0.02 bitcoin is now locked into the channel until the latter is closed. The payment channel operates like a “tab” at a bar - a credit card (the funding transaction and promise of payment) is given to the bartender. The client can then order as many drinks as their credit card allows, but the transaction is not processed until the credit card is swiped by the bartender when the client wants to close out their tab (closing transaction). Similarly, every time Alice purchases a coffee through her payment channel, the transaction is not published on the public ledger, but is committed by the payment channel.

[16] https://www.mdpi.com/2076-3417/9/12/2519

For the sake of simplicity, Alice purchases a coffee for 0.01 BTC.



As seen in the above illustration, 0.01 bitcoin is sent from Alice to the coffee shop. Alice's sending potential is now 0.01 bitcoin, and the coffee shops sending potential is now 0.01 bitcoin, with the total channel capacity remaining unchanged. This means that Alice can only send a total of 0.01 bitcoin, while the coffee shops can now send Alice 0.01 BTC in the event of a refund.

If Alice's sending potential reaches 0 and she no longer has any funds to spend, she can choose to close the channel. When closing the payment channel, the current balance of both parties (0 bitcoin for Alice, and 0.02 bitcoin for the coffee shop) is visibly settled on the public ledger in the form of a "closing transaction".

It should be noted that both the funding transaction and the closing transaction that are published on the blockchain are not labelled as Lightning Network transactions. Some indicators can be seen, but it cannot be confirmed with certainty if published transactions were part of a payment channel on the Lightning Network.

Feeless/Quick micropayments

As per the Lightning Networks official website, once a payment channel is opened, the transactions taking place in the channel are completed near instantly, measured in seconds to milliseconds[17]. Using our example, this means Alice no longer has to wait for a block confirmation for her purchase to be confirmed, as the funding transaction already locked her funds in the payment channel when it was created.

As the transactions are processed offchain, little to no resources are required to process the funds. As such, transactions processed through the Lightning Network payment channels can cost as little as nothing to fractions of a penny.

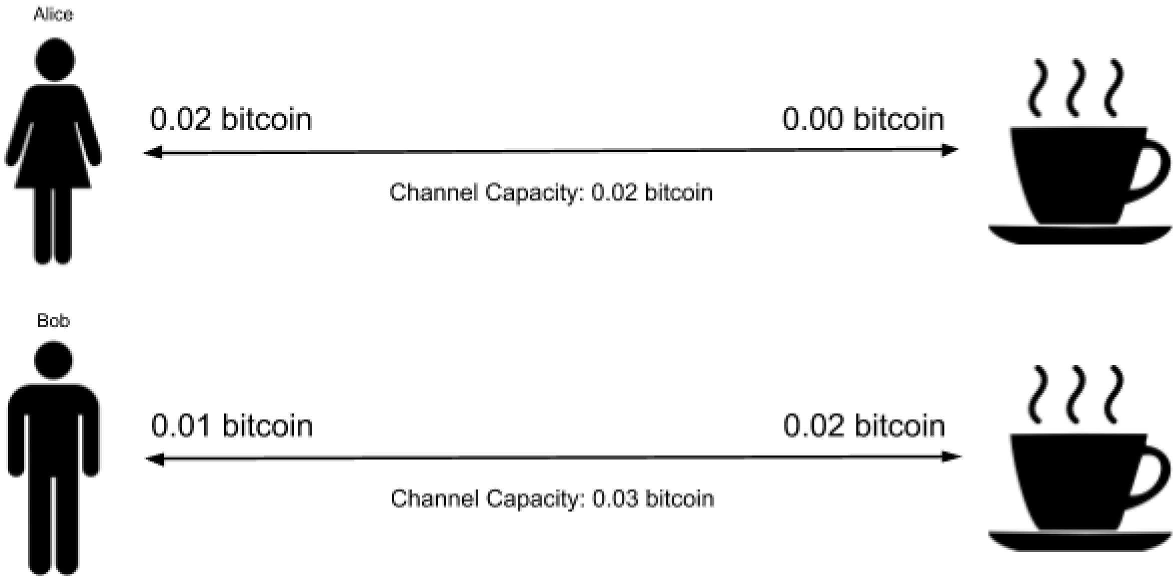
As such, the technology allows for instant, and next to no cost micropayments. Additionally, due to the speed of Lightning transactions, it is estimated that millions to billions of transactions can be processed per second.

[17] https://lightning.network/

Routing Functionality

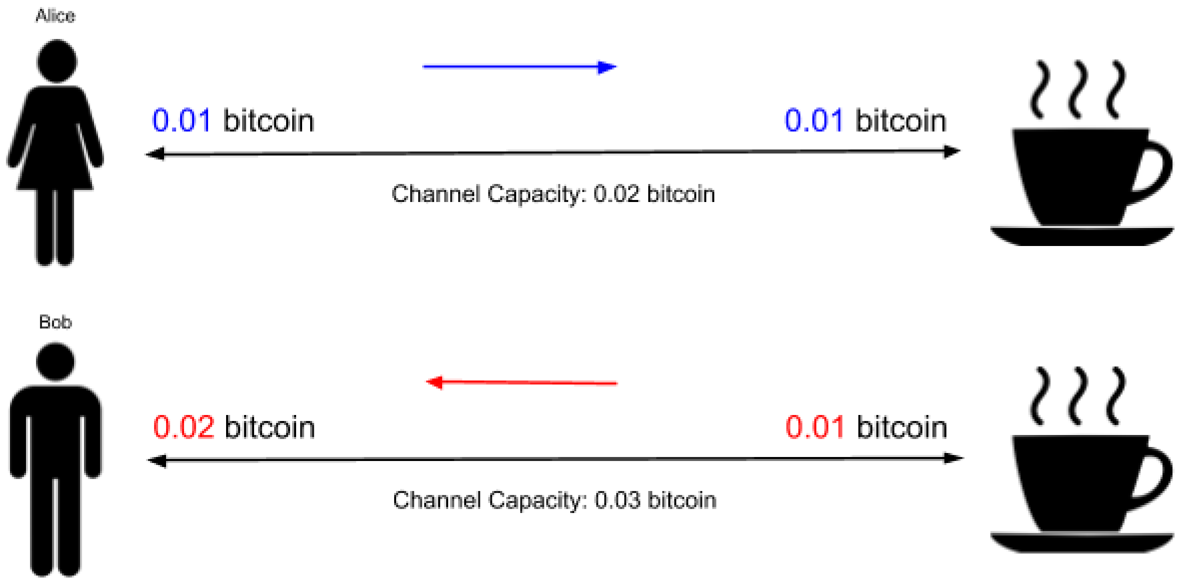
What is arguably seen as the truly revolutionary feature of the Lightning Network is the routing functionality between payment channels. Essentially, users can send payments through Lightning Nodes to other users without having to create a payment channel with the destined counterparty.

Using our example, Alice wants to send her friend, Bob, 0.01 bitcoin. Alice does not have a payment channel established with Bob, but both Bob and Alice have a payment channel with the coffee shop.

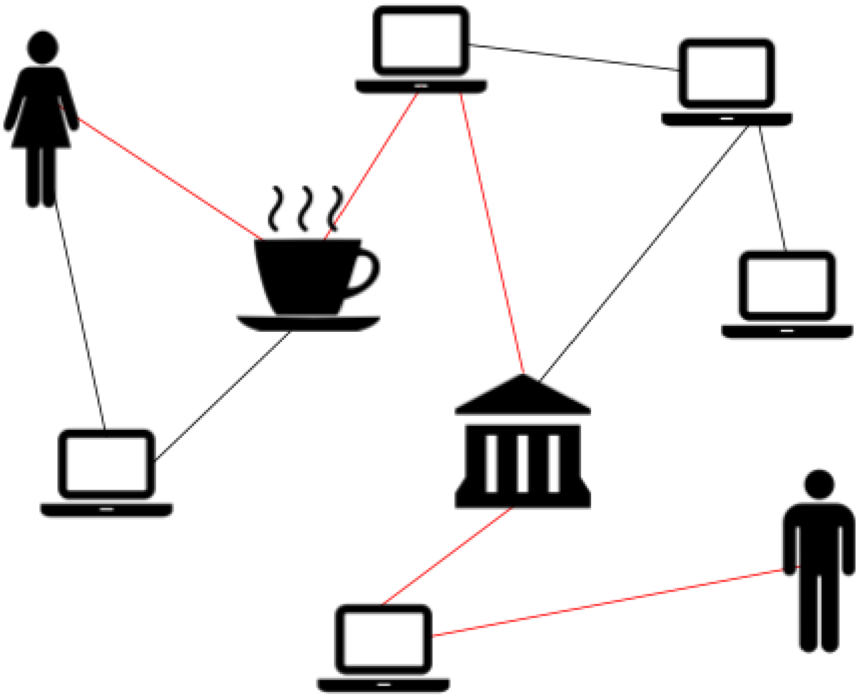

Alice
0.02 bitcoin
0.00 bitcoin
Channel Capacity: 0.02 bitcoin
Bob
0.01 bitcoin
0.02 bitcoin
Channel Capacity: 0.03 bitcoin

Due to the routing functionality of the Lightning Network, Alice can send funds to Bob through the coffee shop as both counterparties have an open channel with the coffee shop. As per the illustration below, Alice's 0.01 bitcoin would be sent to the coffee shop, whose Lightning Node would route the payment to Bob.

It should be noted that the funds do not 'leave' the payment channel. Instead, similarly to the Hawala system, the Lightning Node of the coffee shop would accept the funds from Alice and note that Bob is owed 0.01 bitcoin. The Lightning Node of the coffee shop would then send Bob 0.01 bitcoin using the funds available on their respective payment channel.


Alice
0.01 bitcoin
0.01 bitcoin
Channel Capacity: 0.02 bitcoin
Bob
0.02 bitcoin
0.01 bitcoin
Channel Capacity: 0.03 bitcoin

Payments can be routed through **unlimited** intermediaries, as long as there is a direct connection between the sender and receiver. The Lightning Node of the sender will automatically find the path of least resistance (quickest or lowest fees).



The type of routing used is similar to Onion Routing[18] on Tor, where the information - in this case payments - is transmitted in a way that the intermediary nodes on the transaction path between the sender and receiver only know the identity of the immediate predecessor and successor in the route. They do not know who is the sender or receiver, even if they are the node connected directly to one of the counterparties.

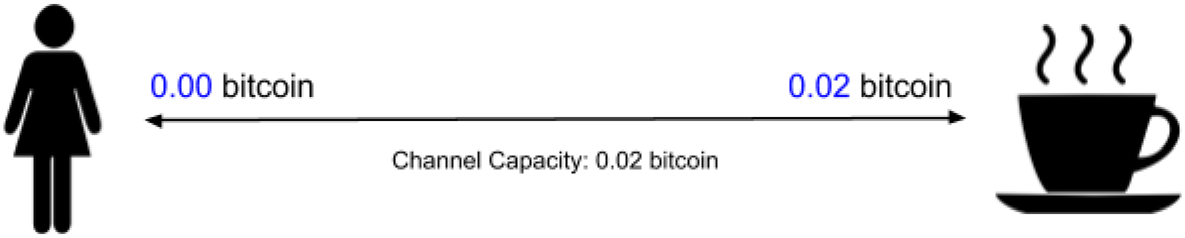
The Lightning Node of the sender is responsible to both select the route of the funds and apply Onion Routing. This ensures that the routed payments are private and censor-resistant.

Trustless and Secure

When a user deposits their funds in an account with a Virtual Asset Service Provider (VASP), they are delegating custody of their funds to the service. Between hacks, exit scams, loss of funds, and theft of funds held on various VASPs, it's understandable that users are seeking to transact securely without relinquishing custody of their funds and placing trust in a service's security.

The Lightning Network allows users to create channels and transact without delegating custody of their funds. These "trustless" transactions are made possible through the use of a two-party, multisignature "channel" bitcoin address (the funding transaction), and through a Hash Time Locked Contract (HTLC). In order to close the channel, thus spending funds from the address, all counterparties need to sign a new "exit transaction" where they all need to agree on the most current channel balance, which is recorded as the most recent transaction signed by both parties.

To ensure that funds do not remain locked in payment channels indefinitely due to a counterparty being unresponsive, either party can choose to close the channel at any time without the consent of the other party. The most recent transaction signed by both parties will be taken as the final balance.



Returning to our example, this would mean that in order to close their channel, Alice and the coffee shop would need to sign a transaction where both agree that Alice now has 0.00 bitcoin,

[18] https://blog.lightning.engineering/posts/2018/05/30/routing.html

and the coffee shop has 0.02 bitcoin. Alice can then, if she so chooses, open a new payment channel with the coffee shop to continue paying using Lightning transactions.

The watchtower is a security mechanism for connecting to another node, which monitors lightning channels for the user and prevents a dishonest counterparty from stealing funds, even when the user is offline[19]. We will continue to use the Alice and Bob analogy to simulate a Fraudulent Channel Close scenario.

Alice and Bob both open a transaction and each put 5,000 satoshis on the table, making a total of 10,000 satoshis. Alice decides to pay Bob for a coffee for 2,000 satoshis. Now Alice has 3,000 satoshis and Bob has 7,000. Bob then gets preoccupied or loses his internet connection. Alice can now choose to close the channel and broadcast the first state of the channel, instead of the final state, leaving Alice and Bob both with the original 5,000 satoshis contributed, making the coffee purchase free. This is what is known as a fraudulent channel close.

Currently, the only way Bob could prevent Alice from defrauding him would be to remain online, raising the alarm in case he suspects Alice has stolen funds. However, this is not realistic from a user experience point of view and in situations where networks are unreliable.

Watchtowers were conceptualized in the lightning network white paper, however, implementations are still being tested. Watchtowers would act as a third party monitor overseeing Alice and Bob's exchange and alerting Bob to retrieve his funds in case foul play is taking place. Recent iterations mean that watchtowers are essentially lightning nodes with a different dedicated algorithm run by anyone. So a business accepting payments on the lightning network can run its own watchtower or connect to external towers to protect its transactions. Watchtowers in the future could be equipped with incentive models.

Atomic Swaps & Submarine Swaps

Before we explore Atomic and Submarine swaps, an explanation of Hash Time Locked Contracts (HTLC) is required. This type of smart contract is what allows the security and the trustless nature of the Lightning Network. It allows the secure transfer of funds across multiple hops of the network of channels (routing).

A HTLC is a time-bound conditional agreement - in this case, conditional payment - between 2 or more counterparties that removes the risk of a counterparty stealing funds, while removing the need for a trusted third party[20].

Let's say Alice has 1 bitcoin, and wants to exchange it for 100 litecoin. On the other hand, Bob has 100 litecoin, and wants to exchange them for 1 bitcoin. In a normal scenario and without

[19] https://www.theglobeandmail.com/investing/markets/stocks/IBT-X/pressreleases/3219700/
[20] https://liquality.io/blog/hash-time-locked-contracts-htlcs-explained/

using trusted third party, Alice would have to send Bob her 1 bitcoin and hope that Bob sends her the 100 litecoin instead of running off with her funds. To remove this risk, Alice can program a HTLC. Simply put, the HTLC would enforce that both parties have a specified amount of time to process their transactions. Once Alice has received 100 litecoin, and Bob has received 1 bitcoin, both would sign the contract stating that they have received the funds, and enough block confirmation have taken place to ensure the transactions are not reversible. The contract would then give each person access to the funds. If either party fails to uphold their end of the agreement, the funds are automatically returned to their respective holders. This example

Atomic swaps are the exchange of different cryptocurrencies through the use of a Hash Time Locked Contract (HTLC) without the use of centralized intermediaries. The above example is an example of an Atomic Swap.

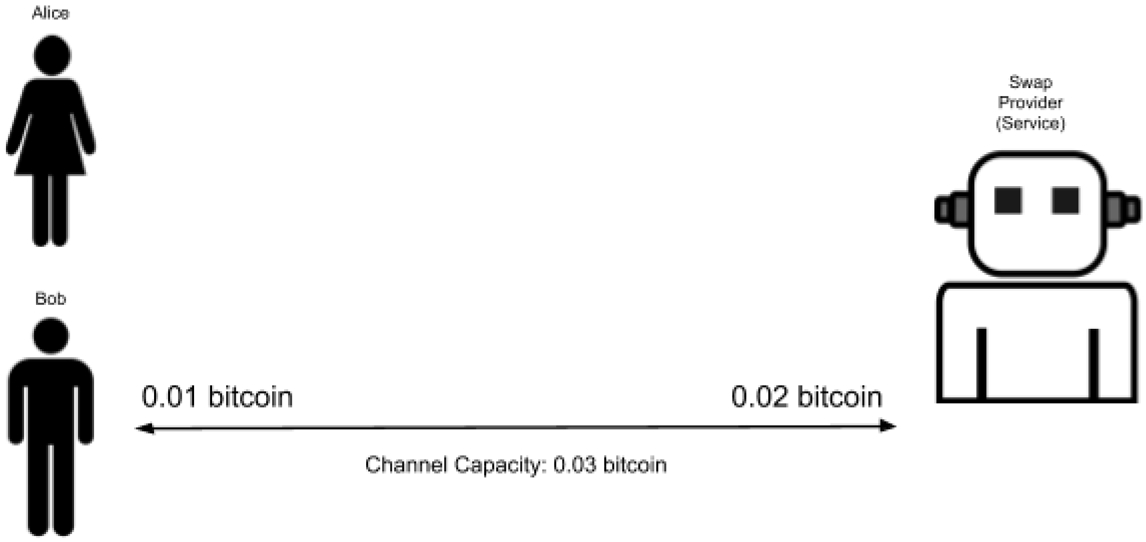
Although a viable solution, Hash Time Locked Contracts (HTLC) would need to be programmed every time an Atomic Swap were to take place and can be difficult to understand for those not familiar with the technology. Moreover, Alice would need to be able to find a counterparty who specifically wants her 1 bitcoin and has 100 litecoin they wish to trade.

Although the Lightning Network currently only operates on Bitcoin, there are plans to incorporate the technology on other blockchains whose scripting language allows for Hash Time Locked Contracts (HTLC) (this would include Bitcoin Cash, Litecoin and other Bitcoin based currencies, Ethereum, other Ethereum based currencies, Dash, Zcash, Monero, etc). Currently, The Raiden Network[21] is being built and plans to offer the same technology as the Lightning Network, but will be layered on Ethereum. In addition to offering offchain payment channels, it is expected to allow for atomic swaps between Ethereum and ERC-20 tokens.

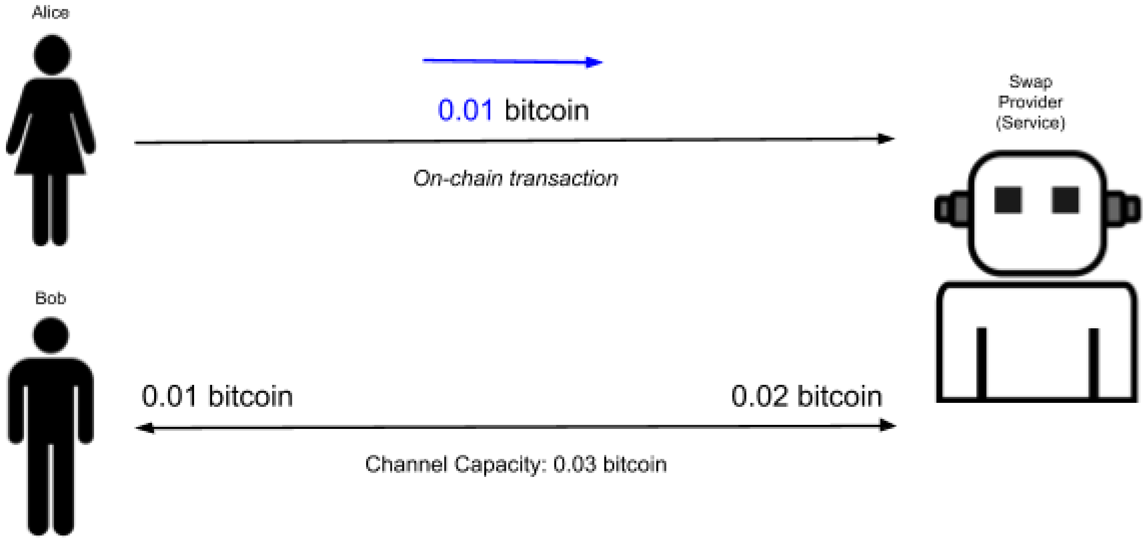
In theory, if the Lightning Network or similar technology were to be implemented across other blockchains, Atomic Swaps could easily be made through payment channels without users having to use a third party intermediary. This would mean Alice could simply exchange her bitcoin for litecoin from her mobile phone by using the power of the peer to peer network and routing function of the Lightning Network

Submarine Swaps, on the other hand, is another feature that results from the use of Hash Time Locked Contracts. As HTLCs can be used for both on-chain and off-chain transactions, they can also be used to *chain payments* between on-chain senders and off-chain receivers, and vice versa, through the use of a swap provider[22]. This means that a user can pay for something on the Lightning Network using an on-chain transaction without needing to open a single channel.

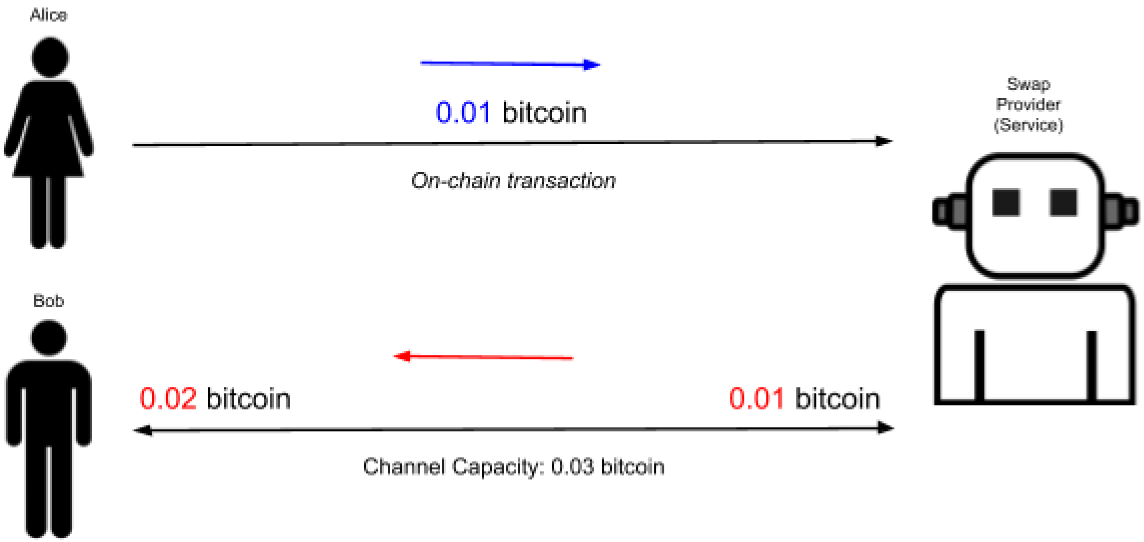
[21] https://raiden.network/
[22] https://blog.muun.com/a-closer-look-at-submarine-swaps-in-the-lightning-network/



In the illustration above, Alice wants to send 0.01 to Bob who owns a bookstore to pay for her purchase. However, Alice does not have a single Lightning Network channel, and does not want to wait the amount of time needed to make a funding transaction to create a channel with Bob. Alice can instead use a Swap Provider - a service uses HTLCs to chain off-chain and on-chain payments.



After receiving the Lightning Network payment invoice, she sends 0.01 bitcoin to the swap provider along with the payment invoice.



The swap provider then sends 0.01 bitcoin using the sending potential from their payment channel they have open with Bob, completing the payment. Depending on the implementation and service, the swap provider could send the funds instantaneously to Bob without waiting for a block confirmation from Alice's payment.

Submarine swaps can also be done using other cryptocurrencies. For instance, alice could send the equivalent of 0.01 bitcoin using litecoin, and Bob will still received the funds in the designated cryptocurrency of their channel.

Limitations

Although the Lightning Network offers many solutions to many of Bitcoin's most notable issues, it does come with some drawbacks.

For one thing, Lightning Nodes (including private wallets on mobile phones) need to be connected to the internet to complete transactions or to route payments. If the coffee shop Alice frequents has a temporary internal blackout, she cannot send funds through her channel until the coffee shop re-establishes its internet connection.

Two drawbacks also come in the form of channel funding limits and refills.

As it stands, the maximum amount a user can use to fund a channel is approximately $150 USD. As such, the maximum channel capacity is approximately $300 USD. Additionally, a channel cannot be "refilled". Once Alice has a sending potential of 0 bitcoin, she cannot add to this balance herself without closing the channel and creating a new one. There is an argument that submarine swaps can be used to "refill" channels, but this can become a time consuming and costly process with the current channel amount limit.

It should be noted that the payment channel amount limit is in place by default for security purposes, as the technology is still very young.

Lastly, funds placed in a channel are considered "locked" until the channel is closed. As such, the user cannot access the funds to use for another purpose until its closure, which can be a disadvantage for services and users with multiple channels.

Social and Economic Benefits - Case Study: Venezuela

According to a UN report, it is estimated that 57% of the world's population do not have access to the internet and over 90% of people in the 48 UN-designated Least Developed Countries (LDCs) do not have any form of internet access[23]. In developing countries, there is limited infrastructure in place to allow citizens reliable access to the internet, let alone afford subscription-based private access to the internet. Even amongst some of the largest economies, there is a great discrepancy in internet adoption between rural and urban areas. The areas simply lack the presence of the state infrastructure required to provide reliable and affordable internet access.

These jurisdictions also tend to have volatile currencies and an unstable economic environments, making citizens' purchasing power unpredictable. Along with weak domestic currencies and high inflation rates, citizens and merchants will often rely on stronger currencies to complete a transaction - it is not uncommon to be able to pay in US dollars, British pounds, or Sterling in the same mom-and-pop shop in a developing country.

Other countries suffer from long-term political instability and dictatorial regimes that enforce internet blackouts while others experience electricity blackouts has part of everyday life. However, enthusiasts are currently developing technical solutions to tackle the issues of economic instability, lack of access to the internet, and government censorship.

The **mesh network**, a decades-old technology with origins in the military, allows users to surf the internet without using a traditional internet service provider (ISP) or landline[24]. A transaction could bounce across the mesh until it reaches a user with an internet connection[25]. It provides a cost-efficient solution; mesh networks dynamically self-organize and self-configure, enabling dynamic distribution of workloads even in the event that a few nodes fail[26].

[23] https://news.un.org/en/story/2015/09/509292-billions-people-developing-world-still-without-internet-access-new-un-report

[24] https://www.pastemagazine.com/articles/2017/12/cryptocurrency-is-fighting-back-against-the-fccs-n.html

[25] https://www.coindesk.com/gotenna-bitcoin-wallet-mesh-network

[26] https://beincrypto.com/what-are-mesh-networks-and-why-are-they-making-a-comeback/

Venezuela is one economy that has been innovative in the adoption and advancement of Lightning Network solutions. Many of the solutions currently being developed in Venezuela are largely dependent on the mesh network and focus on being able to provide connectivity in spite of not being connected to the internet. Transactions are processed off-grid only temporarily until a device gets connected to the internet. For example, a device a little larger than an SD adapter, the Turpial mesh node device, requires only a battery to enable anyone to send off-grid messages or Bitcoin transactions until a device in the network is connected[27].

Another hardware tool currently in the development phase is the Harpia device that eliminates the need to rely on local state infrastructure as it acts as a mesh node. With a Harpia device, transactions can be initiated and broadcasted to the network, it can run a full Bitcoin and Lightning Network node, and connect to Blockstream Satellite[28]. Lastly, txTenna is an app in the proof-of-concept phase that promises off-grid broadcasts of signed Bitcoin transactions using the the goTenna Mesh network or standard SMS network[29]. A limitation of the txTenna app is that it needs to be roughly within a mile of another goTenna device in order to broadcast a message across the mesh network[30].

Lighting Network solutions can also benefit developed countries by providing secure notification systems, personal messaging, and payment solutions in cases of natural disasters. However, it can be argued that because the Lightning Network is meant to facilitate microtransactions, the technology will have the biggest impact and adoption rate in developing countries.

Technologies such as the ones previously mentioned have the potential for mass-adoption due to the low transaction fees and fungible nature of the Lightning Network. This can, in turn, drive economic development in developing countries by immediately providing a currency that won't be influenced by an unstable political or economic climate, provide solutions that are relatively immune to internet and electricity blackouts, and are unhindered by lack of state infrastructure and resistant to government censorship.

Money Laundering and Terrorist Financing Risk

Although the technology offers revolutionary functionality to Bitcoin and has several socio-economic benefits, the risks of abuse of the Lightning Network for the purposes of money laundering, terrorist financing or other crimes cannot be overlooked. There are several characteristics of the lightning network that make second layer payment solutions inherently susceptible to being abused for money laundering and terrorist financing; the level of privacy, the lack of traceability, the ease of access to the technology, and the lack of recourse to conduct enhanced due diligence on any of its transactions.

[27] https://bitcoinist.com/bitcoin-venezuela-mesh-network/
[28] https://bitcoinist.com/bitcoin-venezuela-mesh-network/
[29] https://github.com/MuleTools/txTenna
[30] https://www.coindesk.com/gotenna-bitcoin-wallet-mesh-network

Privacy Risks

Although the Lightning Nodes themselves who have/had active channels can be seen through several online tools[31], the identity of the operators, and the operators of the nodes to which they are connected, remain hidden. Nodes can have "nicknames" associated with them to assist users in identifying the correct nodes with which they wish to connect. However, these nicknames can be misleading as they are chosen by the operator. As such, the identity of the sender and receiver is generally obscured to outside parties, especially when considering that payments can be routed across multiple nodes. Routed transactions, as well as general transactions in a payment channel, are also private. This increases the risk of a user creating a payment channel with a legitimate node for the purpose of using the routing feature to anonymously send funds to an illicit source/actor who also has a payment channel with the legitimate node.

Furthermore, although Lightning Nodes can be placed geographically using their IP address[32], it is possible to have the Node use a Virtual Private Network (VPN) to obscure the true location of the Node. However, when considering sanction risks, this risk is somewhat mitigated by the fact that a VPN location can not be set to a sanctioned country (North Korea, Syria, Iran, for example). However, if a Node in a sanctioned country is connected to a Node outside the area, it is possible for users to send funds to the Node through the routing feature - this transaction would be completely private, and even the routing node (the intermediary) would not be aware of the destination of the transaction due to Onion Routing.

Traceability Risks

The origin and ultimate destination of a transaction is untraceable, and geolocation of a transaction is not visible. Furthermore, current blockchain intelligence tools do not currently have the ability to trace Lightning transactions and identify high risk activities or positively name services on the Lightning Network. The Lightning Network related transactions that have the potential to be identified using currently-available technology would be the transactions associated with channel creation and closure; although, this is difficult and does not have a high degree of certainty. The transactions that occurred while the channel was open would not be viewable nor traceable.

Ease of Access

Any individual with an internet connection can obtain access to the Lightning Network, either by buying a Lightning Node like the Casa Node, or by downloading a Lightning wallet. Neither of these require user identification, and provide immediate access to the Network, and users do

[31] Example of Lightning Node Explorer: https://explore.casa/nodes
[32] To see location of Lightning Nodes https://explorer.acinq.co/

not need to be verified to create a channel with another node. The ease of access and lack of barriers of the technology allows widespread use and adoption, which can include illicit actors.

Money Laundering Risks

On the surface, it may seem that the micropayment limitation (maximum of approximately $300 USD channel capacity) of the lightning network may hinder criminal networks from being able to use the lightning network to maintain anonymity in an efficient manner. While the lightning network in its current state may not be suitable for the movement of millions of dollars in criminal proceeds, or efficiently move any meaningful amount of funds, microstructuring is still part of a number of AML typlogies connected to high risk activities including drug trafficking, human trafficking, and various fraud tactics. This risk is further increased when considering services that allow accept Lightning payments in exchange for gift cards and other goods that have their own money laundering risks.

For example, many drug trafficking cases involve the use of email money transfers, which has transaction limits of its own, to collect micropayments from hundreds of users per dealer. These funds are then accumulated and funneled up through a pyramid-like structure. The accumulation of these funds can be significant, even in the millions of dollars per month. In the case of mass-adoption, the lightning network can very well be used to process the transactions for a drug trafficking store-front. The funds will eventually have to be integrated in the traditional financial system, however the origin of these funds will not only be obscured, it'll be extremely difficult for a financial institution to observe and detect drug trafficking-related red flags and the patterns that make up known typologies. The lack of recourse available to perform enhanced due diligence on these transactions is also a concern.

Human trafficking also has the potential to find its place on the lightning network as it becomes more adoptable. Commonly, payments as little as $50 are observed in a victim's account by way of email money transfer. As the funds accumulate, most or all the funds are transferred to the main illicit actor. Human trafficking-related expenses are also small-value transactions and often are debited from the vitcim's account, usually controlled by the main illicit actor. If the lightning network becomes user-friendly, it might be the ideal payment processor for perpetrators of human trafficking as a direct result of the anonymity it provides.

Although the current transaction limits of the lightning network may make it a less-than-ideal gateway for large-scale money laundering, it can be a great anonymizing tool for drug traffickers to avoid detection and help human traffickers conceal the financial connection with their victims as well as help facilitate other types of crimes characterized by microstructuring.

Terrorist Financing Risks

Unlike money laundering, terrorist financing is characterized by the fact that funds can be derived from both legitimate and legitimate sources, such as employment income or student loans. Additionally, terrorist financing often involves micropayments, or very little amounts of funds to conduct the activity. According to a statement by the Section Chief of the Criminal Investigative Division of the FBI, it only takes a few hundred dollars to join a terrorist organization abroad or fund a domestic terror attack[33]. Additionally, the IMF provided the following statement on terrorist financing typology in a 2019 report:

> *"More recent typologies involving ISIS involve micro-financing and individuals with little financial capacity either self-funding attacks or providing financial support to foreign terrorist fighters (usually relatives) abroad,"* - IMF Country Report No. 19/326, October 2019

Commonly-used terrorist financing methods are not hindered by the transaction limits of the Lightning Network. Furthermore, terrorist networks have been known to make use of different online technologies; online marketplaces such as eBay, online gambling sites, crowdfunding, charity campaigns, video games with digital currency and messaging features, internet-based payment services such as PayPal, prepaid cards, and cryptocurrencies. Such transactions are difficult to detect even for the relatively more mature compliance programs of traditional financial institutions as they appear to be normal daily activity on the surface.

Additionally, the fact that the source of funds could be legitimate increases the difficulty of detecting potential terrorist financing activities. However, typologies have been created that are used in training for AML investigators and for creating transaction monitoring scenarios that have helped the detection of potential terrorist financing activities.

The Lightning Network can provide a level of anonymity which surpasses that of traditional Bitcoin and Altcoin channels, and its micropayment structure does not hinder potential terrorist financing. Thus, it is imperative that technical and regulatory solutions are created by both the public and private sectors for the detection and prevention of terrorist financing activities on the Lightning Network.

Transaction Monitoring Considerations

While information on off-chain transactions is difficult to retrieve and won't include routed payments, channel creation and channel closure do leave a footprint on the blockchain; thus some information can be obtained about the channel. For example, it is possible to know how long a channel was active as the value of the inputs used to create the channel will be time stamped and the outputs at channel closure will also be timestamped. Furthermore, it will be possible to view whether there was a single input used to create a channel or whether there were multiple inputs. Multiple inputs could be an indication that funds are derived from multiple users or that the same user funded the channel from multiple sources. Finally, the balance of each counterparty of the channel at the time of creation and closure would also be published.

[33] https://www.fbi.gov/news/testimony/combating-money-laundering-and-other-forms-of-illicit-finance

When the channel is closed, the output will be published, which will indicate the channel's final balance. A study by Mariusz Nowostawski and Jardar Tøn at the Norwegian University of Science and Technology proposes that it is possible to be able to obtain information on which channels are connected and established that at least 75% of all Pay-to-Witness-Script-Hash (P2WSH) transactions are Lightning transactions[34]. While Lightning Network-related footprints on the blockchain will be a focus point of future transaction monitoring solutions, the traceability and monitoring of activities of off-chain Lightning Network transactions, especially routed payments, currently remain a mystery.

The rapid development and burgeoning adoption of new payment technologies have created AML challenges for both regulatory bodies and the private sector. In the next section we will explore potential regulatory applications in the case of mass adoption of Lightning Network applications.

Outlook on Regulatory Applications

Conservative views predict that both the public and private sector will delay adoption until a solution for AML/KYC integration is found. While large, licensed exchanges may shy away from lightning network adoption in the absence of AML controls in order to avoid regulatory risk, there's little regulators can do in terms of halting the development and use of Lightning Network technology. Furthermore, the privacy-enhancing features of the Lightning Network may actually inspire regulatory involvement. So, in the case of mass-adoption, will Lightning Network Nodes be regulated as money service businesses (MSBs)?

FinCEN

Anti-Money Laundering (AML) regulations are often based or influenced on the Bank Secrecy Act (BSA) of the United States. This has included cryptocurrency exchanges and other Virtual Asset Service Providers.

FinCEN makes clear that convertible virtual currencies (CVCs) that conceal information otherwise available through the CVC's native distributed public ledger, providers of anonymized services such as "mixers" or "tumblers", and privacy coins are not exempt from regulatory obligations[35]. On the other hand, software providers are not considered money transmitters; persons providing the delivery, communication, or network access services used by a money transmitter to support money transmission services are exempt from the definition of money transmitter. FinCEN has not yet directly addressed regulatory implications for the Lightning Network. However, given the very broad definition of money transmitters provided by FinCEN, a

[34] https://www.mdpi.com/2076-3417/9/12/2519
[35] https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20CVC%20Guidance%20FINAL.pdf

strong argument can be made for projecting that those running Lightning nodes would be considered MSBs and have to comply with the Bank Secrecy Act (BSA).

Custody Factor

What is often the key factor in deciding if a service is considered a money transmitter or money service business, based on FinCEN guidelines, is the custody/control factor. If those running a Lightning Node that route payments are considered to hold custody of the funds they are routing, this would potentially lead to these Node operators being designated as money transmitters.

FinCEN's 2013 Virtual Currency Guidance established two definitions that are relevant in determining if a person, service or entity is considered a money transmitter:

> ***A user***: a person that obtains virtual currency to purchase goods or services (not considered a money transmitter).
>
> ***An Exchanger***: a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency (considered a money transmitter).

An exchanger takes and holds the funds of a user to facilitate the purchase of other currencies or sale of the currency itself. The key factor in deciding if a service is considered a money transmitter or money service business, based on the FinCEN guidelines, is the custody/control factor. If those running a Lightning Node that route payments are considered to hold custody of the funds they are routing, this would potentially lead to Lightning Node operators being designated as money transmitters.

However, if the decision is made that Lightning Nodes are to be designated as money transmitters, this would impact all Lightning Network users. Enforcement of these regulations would be exceptionally difficult and the resources required would be unreasonable, as every individual user would essentially need to be monitored. Furthermore, as mentioned prior, the technology is a software, which does not fall into the category of a money transmitter.

While regulation threatens pure decentralization, this will not stop financial regulatory authorities from imposing AML and CFT controls to cover any service that facilitates the movement of funds. We see today that large, licensed cryptocurrency exchanges that offer DEX services have migrated to a hybrid solution where activities remain decentralized, but KYC information may still be collected. Similarly, a compromise by Lightning Node operators and application developers may become a reality.

Melanie Lefebvre, CAMS, CBP, AML & Law Enforcement Investigations, Bitfinex

Yasmine Ibrahim, CBP, Compliance Analyst, Tether

Peter Warrack, CAMS, CBP, CCI, CFE, Chief Compliance Officer, Bitfinex -edits and additional content