SMU FinTech Publication

Research – Blockchain and Cryptocurrencies

Saturday, 26 January 2019
By: Gabriel Tan, Research Director

The Flash of Bitcoin

You will not see technological progress until it hits you.

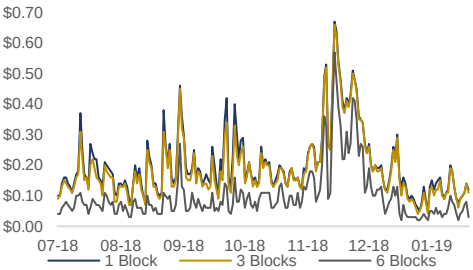
Preface: "Bitcoin" refers the blockchain, technology and general concept of Bitcoin. "bitcoin" or "BTC" refers to the actual currency that underlies "Bitcoin". 1 BTC = 1,000,000 satoshis (sats).

Ten years ago, one bitcoin (BTC) was worth almost nothing. Today, one BTC stands at USD $3,600. To many who jumped on the bandwagon in late 2017, this is the only thing that matters.

With the crash in prices, so did general interest in Bitcoin. Criticisms were thrown around more frequently and harshly— "mother of all bubbles", "scam", "fraud", "facilitates illegal activity". If Bitcoin is as flawed and worthless as detractors claim, odds are that Bitcoin will no longer be around. It is a testament to the strength of this technology, chugging along towards adoption. This is because Bitcoin represents the democratization of money, giving rise to its 2 main use-cases: as a currency and as a store-of-value dubbed Gold 2.0. Where Bitcoin is yet to be widely adopted, recent developments have made leaps and bounds, paving the way for an interesting future.

Cost arguments No Longer as Valid

With the peak in prices end 2017, came peak network traffic, causing transaction costs to soar: average of $0.30; high of $40. Due to this, many argued that Bitcoin would never be usable as a currency or means of value-transfer.



**Historical highs not shown in this chart, only recent averages.*
Source: Bitcoinfees.info, 2019

Historically, fees—along with volatility—have been considered too high by most analysts to allow for adoption of Bitcoin as a viable medium for general retail payments.

However, that has changed with the launch of the Lightning Network and implementation of the SegWit network upgrade. Today, transaction fees have fallen to their lowest in over 3 years: median of $0.02 per transaction, even though the number of transactions has doubled since last October 2015. The falling trend in transaction fees appears to represent a positive, long-term trend in favour of the utility and adoption of Bitcoin as an everyday-payments mechanism, as opposed to a store of value.

A Brief Overview on Bitcoin

The following sections operate on the assumption that you already have a fair understanding on how Bitcoin transactions work. However, as an extremely brief recap: normal Bitcoin transactions (first-layer transactions) are recorded on-chain, and thus carries with it significant fees paid to miners. At current rates, the fastest and cheapest transaction (20 sats/byte) at median size of 250 bytes, carries with it a 5,000 sat ($0.172) fee, no matter the amount of BTC sent or received. At this level of fees, Bitcoin will never be able to operate as a micropayments system, for it is extremely cost inefficient to send small amounts of BTC.

Enter the Lightning Network

The Lightning Network (LN) represents a strong solution for the great Bitcoin scaling issue. Today, the network surpassed $2M in BTC Capacity with 5,600 nodes. It proposes in the whitepaper[1]:

"…using a network of these micropayment channels, Bitcoin can scale to billions of transactions per day…"

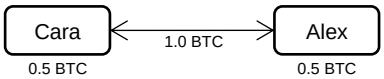
This is done by operating as a secondary layer (off-chain) on top of Bitcoin's base network, creating a way to carry out transactions between several users without recording them on the blockchain (on-chain) until the moment the channel is closed[2]. The significance of this is that off-chain transactions boast extremely low transaction costs and fast confirmation times. Depending on the scenario, users can instantaneously send 10 sats to another user for the low fee of 1 sat ($0.0000345538) or even send 1 sat at sub-sat rates (sometimes even for free). Paying such small sums was impossible prior to the LN.

To use the network, you first need to install and run a Bitcoin node with the LN client. To transact with another user (each user has a node), you (1) initiate a payment channel by creating a multi-signature transaction on the blockchain. At least one party must (2) commit funds (depositing BTC) to this transaction. Once this channel is open and a payment channel is established on the LN, both of you can (3) transfer funds between each other. Each transaction updates a "temporary" balance sheet, signed by each party's private key. This balance sheet can be (4) broadcast as a Bitcoin transaction at any time if either, or both parties want to close the channel.

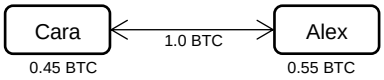
Consider this example between Cara and Alex:

(1) Cara sets up a payment channel with Alex.

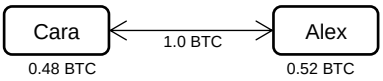
(2) The capacity of this channel is 1 BTC, with Cara and Alex each committing half of that capacity.



(3) They can then transact as many times as they want over the LN. If Cara sends 0.05 BTC to Alex, the "temporary" balance sheet is signed by each person and now states that 0.45 BTC belongs to Cara and 0.55 belongs to Alex (less minor fees).



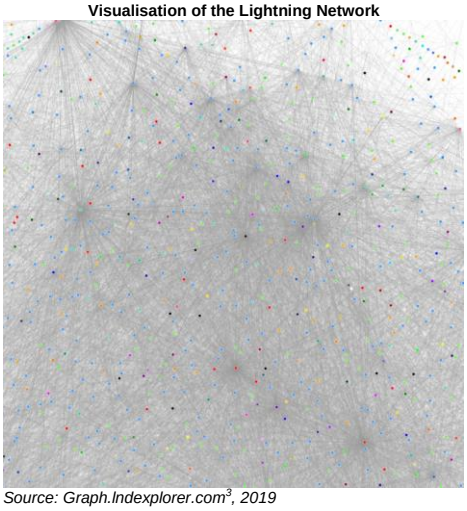
Next, if Alex sends 0.03 BTC to Cara, the balance sheet now reads 0.48 BTC for Cara and 0.52 BTC for Alex. They can do this for a theoretical unlimited amount of times.



(4) When either, or both, decide to close the payment channel, the latest balances are broadcasted as a transaction to the blockchain, carrying with it standard on-chain transaction fees. Each wallet is credited the respective balances in BTC.

The result is an intricate and growing network of connections resembling a dense spiderweb. Visualised below, is a small corner of the LN. Each colored dot represents a node and each line represents an open channel.

Visualisation of the Lightning Network



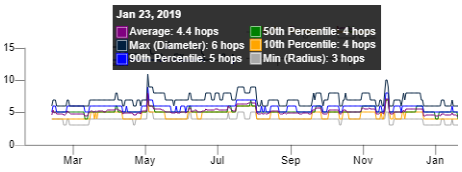
Source: Graph.lndexplorer.com[3], 2019

Due to the costs associated, it is not feasible to open direct channels with every single party to transact. This may only make sense if you foresee yourself making multiple transactions in the future. An example may be opening a channel with a news website, allowing you pay to read individual articles over a long period of time; it defeats the purpose of the Lightning Network to make open and close channels for single transactions. Another thing to note is that in most cases, the liquidity of a channel is limited by the amount of BTC committed to the channel.

This is where the concept of transaction routing comes into play. Since the LN is a network of payment channels, every node is connected to another node and payments can be forwarded to another node (called a "hop") until the payment gets to its intended recipient. In this way, someone can send funds to another user without having a direct channel with them.

One measure of network strength is the number of hops required between indirect nodes—currently an average of 4.4 hops to reach any other node. Some users may charge a small fee to let others route transactions through his node. Thus, fewer hops require less transaction fees and suggests greater connectivity between all nodes. Metcalf's Law states that a network's value is the square of the number of nodes in the network—every node connected and channel created increases the value of the network (which the price per BTC reflects at an inefficient level).

Distance Measures: the maximum number of hops required to reach another node (among the shortest paths)



Source: BitcoinVisuals.com/lightning[4], 2019

Bolstering Network Infrastructure

Reducing the number of hops is possible in 2 ways: by increasing the number of nodes in general and by increasing channel density. The latter will only realistically possible with the formation of liquidity providers (Hubs).

Hubs are generally BTC-rich nodes that have a high number of open channels. The main benefit is that small nodes only have to open a channel with the Hub in order to route transactions to other users (who have also connected). Where these can be run by individuals, Hubs are more likely to be businesses such as an e-commerce website e.g Amazon. This will be discussed in greater detail in the following section. Overall, chances are that we will see large concentrations of nodes around Hubs; the max number of hops should eventually tend towards 2.

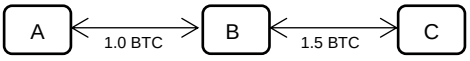
Critics of the LN believe that eventually this will decrease decentralisation and privacy, against the ethos of Bitcoin. All payments will end up routing through a few Hubs, where they will act like banks. Government regulation may step in to require Hubs do KYC using passports or utility bills, or even applying for money transmission licenses.

Alternatively, proponents believe that the LN will in-fact improve decentralisation. Since more transactions will be handled off-chain, Bitcoin mining cartels will be given less power. Privacy will not be undermined due to the use of multi-hop payment channels and even the Tor network.

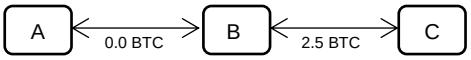
Opportunities: Liquidity Providing (Hubs)

Where a limitation of the LN is that it is likely to tend towards centralization, it does propose a unique business opportunity for first-movers who wish to bet big and build a network of Hubs.

For small users, funds in their channels may be limited. Should their channels be constantly used by indirect peers for routing, this may cause a misbalancing of BTC in the channels. For instance, consider 3 nodes each: A, B and C.



Should A attempt to route more than 1.0 BTC to C through B, the A-B channel balance will become 0.



Funds must be restored between A and B for them to transact again. Either C has to pay A by re-routing through B or the channel has to be re-opened (incurring fees). Therefore, users can choose to charge a routing fee. The current market rate is currently extremely low within the 1 sat range, but will definitely grow with the network (not to on-chain fee levels).

With large reserves of BTC, a network of Hubs will have the economies of scale to provide fees than individuals would; the name of the game is volume and market share. The costs of providing such a service include: opportunity costs from locking up BTC in channels, electricity costs for running nodes 24/7 (significantly less than BTC mining), on-chain fees for opening and closing channels and marketing expenses, among others.

In a future where the Lightning Network is used for a substantial portion of day-to-day transactions, running a sizeable network of Hubs may prove to be a highly profitable venture.

Opportunities: Micropayments as a Service

Blockstream introduced the micropayment processing API "Lightning Charge"[5] for the LN that utilizes Blockstream's c-lightning implementation. Lightning Charge makes it easy for web developers to accept payments for their content, goods, and service through the LN.

Satoshis.place[6] is an excellent proof-of-concept for micropayments on the LN: an online collaborative artboard that pays homage to Milliondollarhomepage.com. It allows you to paint over any of the 1 million pixels for merely 1 sat.

Source: Satoshis.place, 25 Jan 2019

Launching around 11 June 2018, it managed to clear over 8,000,000 pixels in just a few days for a cool 8 BTC profit (1 BTC ≈ $6,500, June 2018). At 28,555 pixels drawn per day, according to the website, it has generated close to 6 BTC since 1 July 2018. The only associated costs are paying for channel updates and website hosting—quite a profitable venture.

Should adoption catch on, major e-commerce platforms such as Taobao, Alibaba and Amazon will definitely begin accepting LN payments. Customer turnover and revenue will likely increase since payment processing fees will not be factored into prices. Taking the rate sellers are charged by PayPal as an example[7]: US fees are 2.9% + $0.30 per transaction; micropayments (transactions under $10) are charged at 5% + $0.05 per transaction. Instead, with the LN, prices of goods across the board may be lowered and boost consumer surplus. Established payment processors such as Visa and PayPal will have to evolve to stay relevant.

Along the same vein, e-commerce businesses will also become immense Hubs[8] due to the sheer size of their userbases. Large deposits of BTC and numerous open channels, with well-connected nodes and small nodes alike make them natural Hubs. This creates an opportunity to capitalise on it by doubling up as liquidity providers, helping users route payments. These make for compelling arguments as to why e-commerce businesses may end up being more competitive than Hubs who purely provide liquidity-as-a-service

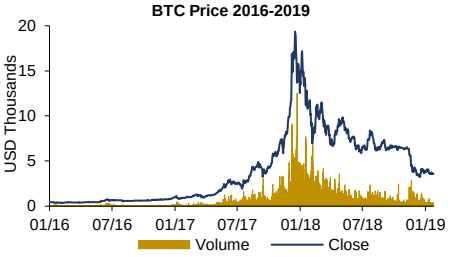
Other compelling uses of micropayments on the LN include: pay-per-call API access, streaming videos, IOT-applications, machine-to-machine payments, pay-as-you-go insurance and "leased" wi-fi portals.

Wait, When Did That Happen?

Despite what is said and heard, the future of Bitcoin is extremely bright. Here is a little story:

"This one-time, bitcoin went from $0.06, all the way to $0.36, and then it crashed down to $0.21. Another time, bitcoin went all the way to $1100, before it crashed right down to $213. And then another time, bitcoin went to $20,000, before it crashed all the way down to $3200. Moral of the story? Don't buy bitcoin because it's going to crash."

BTC Price 2016-2019



Source: Coinmarketcap[9], 2019

Sure, we may say that the price of Bitcoin is not important, and that the technology is what really matters. However, with a decent understanding of the mechanisms that underlie the technology, one would realise that the market mechanism and thus price is what makes Bitcoin strong. Price comes with security and robustness, and security and robustness come with price.

Those in the know are quietly working hard and breaking new grounds. Following an adoption S-Curve, the next 10-15 years could very well see Bitcoin permeating into our everyday lives very slowly at first, then suddenly all at once, absolutely changing the global landscape; money and assets will be able to move faster and with less friction on a global scale. With the creation of more user-friendly innovations, most of these changes will happen in the background. Majority of people will not even realize that they are using Bitcoin and the Lightning Network.

Contact: Gabriel Tan, Research Director
yhtan.2017@business.smu.edu.sg

Sources:

---

[1] Poon, J., & Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Retrieved from https://lightning.network/lightning-network-paper.pdf

[2] Pham, J. (2019). Lightning Network — how does it work? Retrieved from https://medium.com/coinmonks/lightning-network-how-does-it-work-ceeeda8ad21e

[3] bmancini55. (2019). Lightning Network Visualizer. Retrieved from https://graph.lndexplorer.com/

[4] Bitcoinfees.info. (2019). Bitcoin Transaction Fees. Retrieved from https://bitcoinfees.info/

[5] Najera, J. (2018). An Introduction to Lightning Network Apps (LAPPs): Scaling Bitcoin. Retrieved from https://coincentral.com/an-introduction-to-lightning-network-apps-lapps-scaling-bitcoin/

[6] Lightning K0ala. (2019). Satoshi's Place. Retrieved from https://satoshis.place/

[7] PayPal. (2018). Credit Card Fees, Send Money Fees & Other Charges - PayPal US. Retrieved from https://www.paypal.com/us/webapps/mpp/paypal-fees

[8] Brekken, A. (2018). Bitcoin Lightning Network #2: We must first become the Lightning Network. Retrieved from https://medium.com/andreas-tries-blockchain/bitcoin-lightning-network-2-we-must-first-become-the-lightning-network-49c46953c1d7

[9] CoinMarketCap. (2019). Bitcoin (BTC) price, charts, market cap, and other metrics | CoinMarketCap. Retrieved from https://coinmarketcap.com/currencies/bitcoin/