Layer 2, HTLC, SegWit

Campbell R. Harvey

Duke University and NBER

Transactions per Second

https://en.bitcoin.it/wiki/Scalability

- Visa processes about 2,000 transactions per second
- Mastercard similar
- Visa peak daily is about 4,000 tps and the capacity is 56,000 tps
- Bitcoin can handle about 7 transactions per second: (assuming current blocksize 1mb); Ethereum can do 10-20 transactions per second*
- **Lightning Network** possible solution for bitcoin https://lightning.network/
- **Raiden Network** possible solution for ethereum https://raiden.network/

*https://etherscan.io/chart/tx and https://medium.com/@FEhrsam/scaling-ethereum-to-billions-of-users-f37d9f487db1

Transactions per Second

Bitcoin itself cannot scale to have every single financial transaction in the world be broadcast to everyone and included in the block chain. There needs to be a secondary level of payment systems which is lighter weight and more efficient." -Hal Finney, Dec 2010

- At 1,200 transactions per MB every 10 minutes and 7 billion people do two on-chain transactions per month, blocksize would have to be 5.7gb.
- Need Layer 2 or L2.

https://www.reddit.com/r/Bitcoin/comments/7pi58z/bitcoin_itself_cannot_scale_to_have_every_single/?st=jcatanmi&sh=dea66153

Lightning Network

- Take small transactions out of the main blockchain (off chain)
- The same intuition applies to Coinbase where it is fast and cheap to transfer among all of those whom have Coinbase wallets. Coinbase is not putting all of the small transactions on the bitcoin blockchain
- LN is a much more general approach

Lightning Network

The Washington Post
Democracy Dies in Darkness

The Fix • Analysis

Howard Schultz is looking at an independent presidential bid. Would he have a shot?

- Suppose Cam buys a coffee regularly at Starbucks
- It is inefficient to use the main blockchain for small transactions
- The solution is to set up a multi-signature address that is shared by Cam and Starbucks

CNBC

BITCOIN

Starbucks' Howard Schultz: A 'trusted' digital currency is coming, but it won't be bitcoin

- "One or a few legitimate" cryptocurrencies are coming, but bitcoin is not one of them, according to the Starbucks executive chairman.

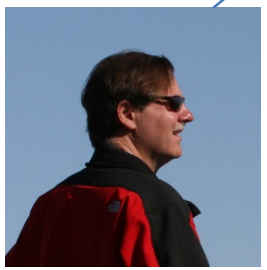
https://www.cnbc.com/2018/01/26/starbucks-schultz-a-digital-currency-is-coming-but-wont-be-bitcoin.html

Lightning Network

Multi-signature address is like a vault that can only be opened when both parties agree. This is a "payment channel".

Multi-signature address

Cam deposits 0.05BTC



Payment Channel Ledger	
Cam	0.05
Starbucks	0.00

Starbucks deposits 0.00BTC

Lightning Network

- Payment Channel is established on main blockchain by two on-chain transactions
- Cam can see his 0.05 BTC
- Starbucks can see that Cam has 0.05 BTC of spending power
- Initial seeding of the channel is “on chain”

Lightning Network

- Cam goes to Starbucks and orders an expresso which costs 0.005 BTC
- Payment channel ledger is updated off chain

Payment Channel Ledger	
Cam	0.045
Starbucks	0.005

- Cam and Starbucks sign the updated balance sheet and each keep a copy of the ledger

Lightning Network

- Cam can continue to buy coffee until balance is exhausted
- There is no limit on the number of transactions per second because these transactions are happening off chain

Payment Channel Ledger	
Cam	0.015
Starbucks	0.035

Lightning Network

- Payment Channel can be closed at any time
- Either party simply needs to take the latest ledger which is signed by both parties and broadcast it to the network
- Miners verify the signatures on the ledger and then release the funds (single transaction to close). This is an on-chain transaction.

0.015 to Cam

Payment Channel Ledger	
Cam	0.015
Starbucks	0.035

0.035 to SB

Lightning Network

- Important 1: Any party can release the funds – even if one party does not want to release the funds. There is no way for Cam to hold Starbucks hostage for the funds.

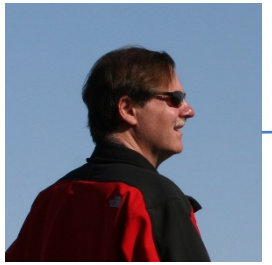
0.015 to Cam

Payment Channel Ledger	
Cam	0.015
Starbucks	0.035

0.035 to SB

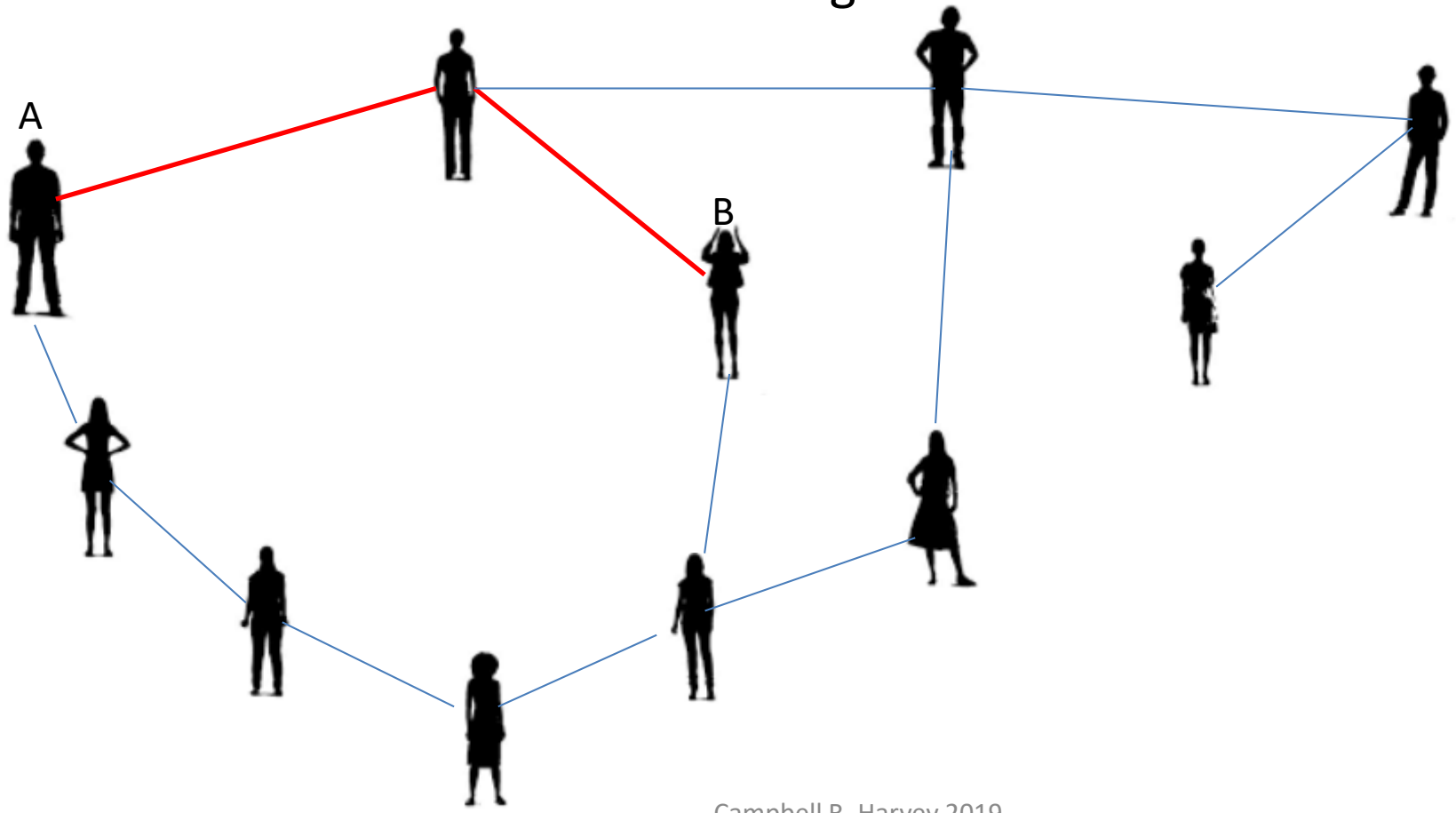
Lightning Network

- Important 2: You do not need to set up a separate payment channel for Starbucks – you can use the network.
- Suppose Amber and Cam have a payment channel. Suppose Amber wants a cup of coffee at Starbucks and she knows that Cam has a payment channel



Lightning Network

- Important 2: Network finds the fastest and cheapest way to connect A to B. It is also important that the channels have enough funds to do the transaction.



Lightning Network

False concerns

- I don’t want to prefund future payments
- I don’t want to lock-up funds so that I can’t use them elsewhere
- I’ll have to close and reopen the channel whenever I want to replenish funds
- I have no idea in advance how many coffees I’ll buy from Starbucks

https://i.imgur.com/kJ94x5u.png

Lightning Network

Allayed concerns

- Your regular LN channel will be just like your hot/spending wallet (think of the difference between your “wallet” and your “savings account”)
- Establishing a channel is analogous to funding a hot wallet
- You don’t need to open a channel with every Starbucks

https://i.imgur.com/kJ94x5u.png

Lightning Network

Real concerns

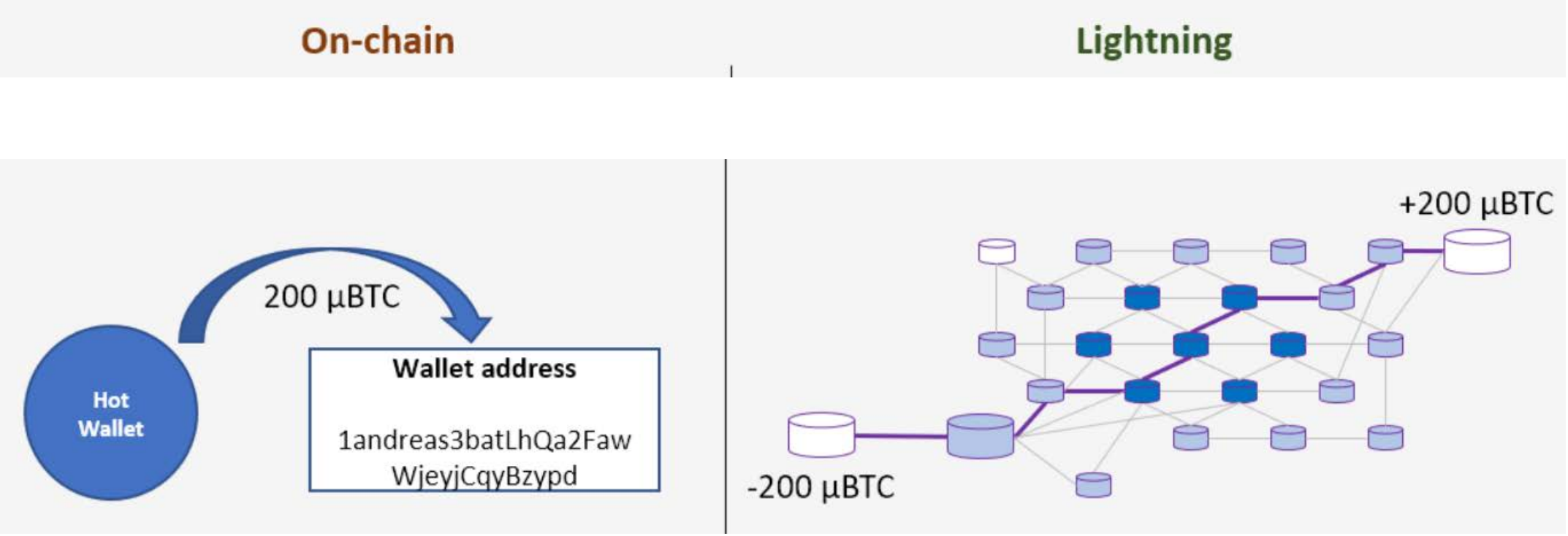
- LN depends on another change in bitcoin protocol called SegWit
- Some are concerned that the payment channels maybe become "centralized" with a few important players
- You need to hold bitcoin in the channel and bitcoin is not a reliable store of value (high volatility)
- Is a second layer, L2, enough? Will there need to be a third level?

Lightning Network

Lightning advantages

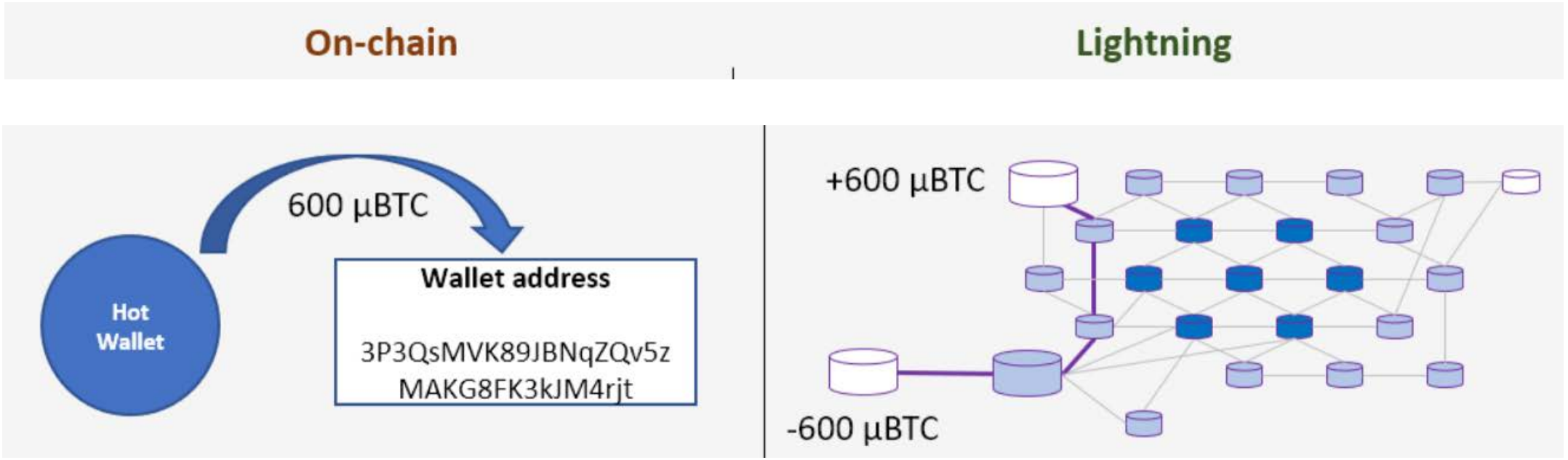
- Reduces number of on chain transactions which will reduce transactions fees (good for users not good for miners)
- Illustration: https://www.robtex.com/lnemulator.html

Lightning Network



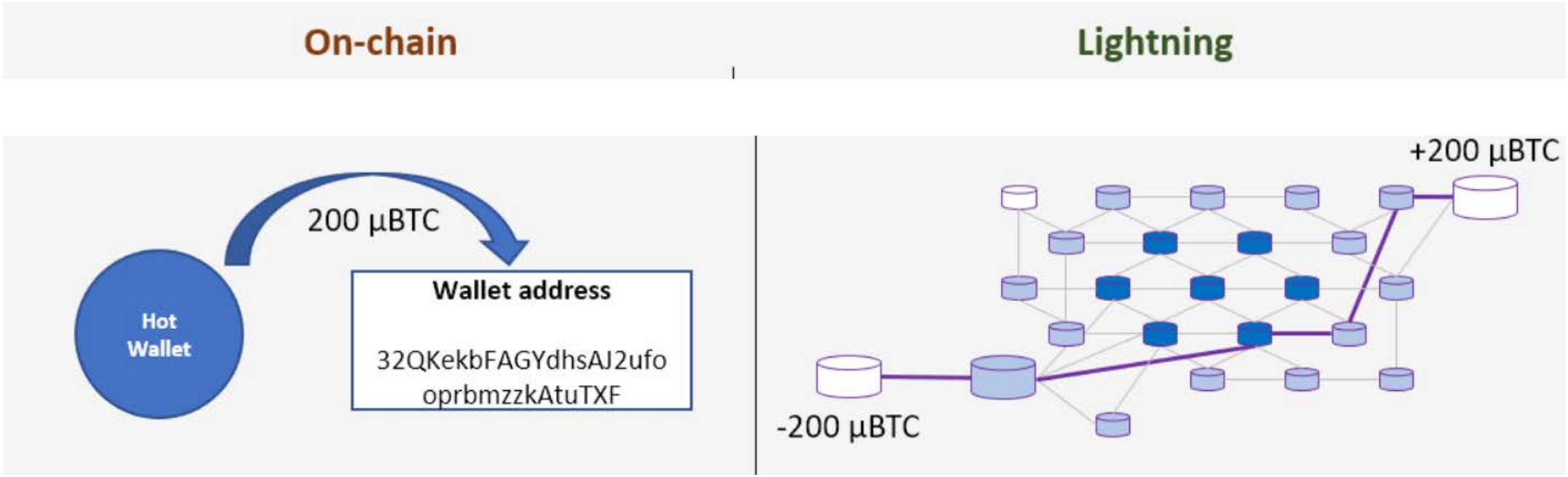
https://i.imgur.com/kJ94x5u.png

Lightning Network



https://i.imgur.com/kJ94x5u.png

Lightning Network



- Three on-chain transactions
- Miners' fees for each
- Long confirmation times

- Three off-chain transactions optimally routed through channel network
- No on-chain transactions
- Minimal fees; forwarding nodes get very small fee
- Instant settlement

https://i.imgur.com/kJ94x5u.png

Lightning Network

Overall

- No locking up of funds. It is that it is trustless. If the other party goes offline or tries anything shady, you can broadcast your transactions to the blockchain immediately and get your money out yourself.
- Minimizes on-chain transactions (low fees)
- Unlimited, instant payments
- Microtransactions possible
- End user behavior is exactly like an on-chain hot wallet. Intuition similar to Venmo – every so often you need to replenish your wallet.
- Makes more sense with stablecoins

https://i.imgur.com/kJ94x5u.png

Lightning Network

Early days

- Mainly an idea with a test net in early 2018.

https://explorer.acinq.co/#/

Lightning Network

Sudden growth

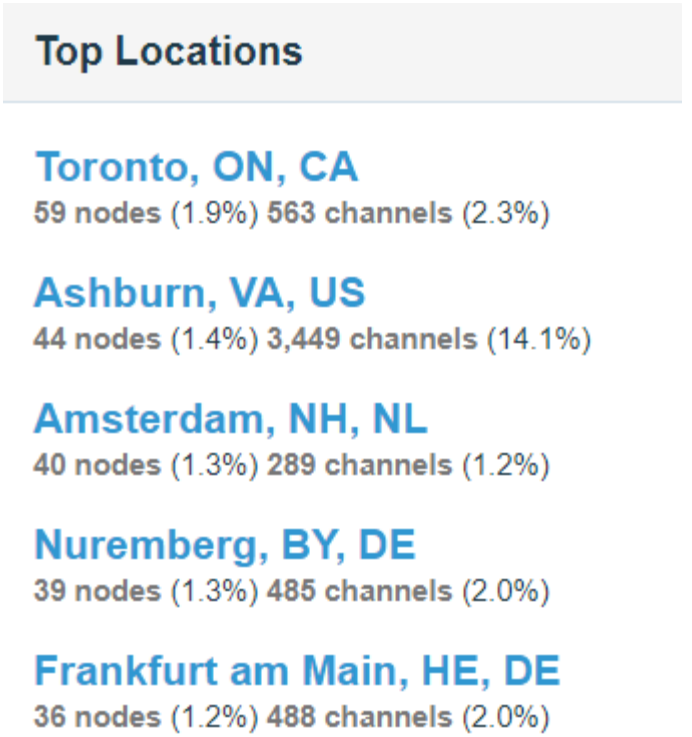
- February 9, 2019: 3,075 public nodes, 24,618 channels

https://explorer.acinq.co/#/

Lightning Network

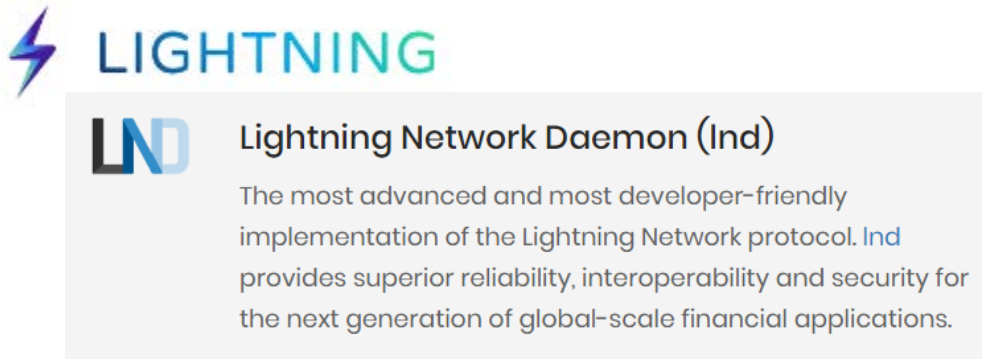
Sudden growth

- Lightning Network Search and Analysis Engine
- Support for bitcoin, litecoin, stellar
- Protocol can also work for private channels as well as TOR



https://1ml.com/

Lightning Network



https://github.com/lightningnetwork/lnd

Three main implementations (developers)

- lnd (Lightning Labs), c-lightning (Blockstream), éclair (ACINQ)
- Developers have worked out a set of standards, BOLT, (Basis of Lightning Technology) that allow for interoperability [the same way it is easy to send an Outlook email to a Gmail user]

https://github.com/ElementsProject/lightning

https://github.com/ACINQ/eclair

http://bitcoinist.com/bitcoin-fees-mainnet-lightning-network/
https://medium.com/@lightning_network/lightning-protocol-1-0-compatibility-achieved-f9d22b7b19c4
https://www.youtube.com/watch?v=vPnO9ExJ50A&feature=youtu.be

Lightning Network

Routing

- Implements the Onion routing protocol
- Each node only sees the immediate hop before and after
- Called Onion because routing information is wrapped in layers. You peel the onion to figure out where to send it for the next hop. Nodes have no idea how many hops have happened or how many are needed to get to the recipient
- Same protocol used in TOR (The Onion Routing)

https://www.youtube.com/watch?time_continue=1&v=D-nKuInDq6g

HTLC

Hashed Timelock Contracts (HTLC)

- Payments that use hashlocks and timelocks to require that the receiver of a payment either acknowledge receiving the payment prior to a deadline by generating a cryptographic proof of payment – or forfeit the ability to claim the payment – returning it to the payer
- Technique allows for conditional payments in cryptocurrency

https://en.bitcoin.it/wiki/Hashed_Timelock_Contracts

HTLC

Hashed Timelock Contracts (HTLC)

- Ideal for payment channels because it makes payments routable across many payment channels
- It is also possible to use this type of contract for cross-chain trading, so called atomic cross-chain trading

https://en.bitcoin.it/wiki/Hashed_Timelock_Contracts

HTLC

Hashed Timelock Contracts (HTLC)

- Example of cross-chain trade
- Alice wants to buy 1BTC from Bob for 10ETH. She does not want to use an exchange
- She could just send the 10ETH to Bob. But Bob might not fulfill his side. So Bob keeps the 1BTC and 10ETH!

https://en.bitcoin.it/wiki/Hashed_Timelock_Contracts

HTLC

Hashed Timelock Contracts (HTLC)

- Alice opens a payment channel to Bob, and Bob opens a payment channel to Charlie.
- Alice wants to buy something from Charlie for 1000 satoshis.
- Charlie generates a random number and generates its SHA256 hash. Charlie gives that hash to Alice.
- Alice uses her payment channel to Bob to pay him 1,000 satoshis, but she adds the hash Charlie gave her to the payment along with an extra condition: in order for Bob to claim the payment, he has to provide the data which was used to produce that hash.
- Bob uses his payment channel to Charlie to pay Charlie 1,000 satoshis, and Bob adds a copy of the same condition that Alice put on the payment she gave Bob.
- Charlie has the original data that was used to produce the hash (called a pre-image), so Charlie can use it to finalize his payment and fully receive the payment from Bob. By doing so, Charlie necessarily makes the pre-image available to Bob.
- Bob uses the pre-image to finalize his payment from Alice

https://en.bitcoin.it/wiki/Hashed_Timelock_Contracts

Transaction malleability

Problem

- In bitcoin, transactions are signed. However, the signature does not cover all of the data in a transaction. That is, the signature does not cover all of the data that is reflected in the transaction hash. This is a well known problem for years.
- Hence, it might be possible for a nefarious node to change a transaction in a subtle way (not the outputs) causing a change in the transaction hash.

https://en.bitcoin.it/wiki/Transaction_malleability

Segregated Witness (SegWit)

Solution

- SegWit establishes a new structure called a “witness” that is separated (or segregated) from the transaction Merkle tree.
- Signatures are moved to this new structure
- An added benefit is that the new structure does not count towards the blocksize
- Four times as many transactions can be fit on a block. This is, in addition, to solving the transaction malleability problem
- Already implemented in Litecoin

https://en.bitcoin.it/wiki/Segregated_Witness https://en.wikipedia.org/wiki/SegWit

Segregated Witness (SegWit)

Solution

- Known as BIP141 and was backward compatible
- Already implemented in Litecoin (#5 crypto, early 2011 fork of bitcoin, same code but 84 million coin limit, Scrypt hash not SHA-256, larger effective blocksize because blocks every 2.5 minutes)
- Note: SegWit should not be confused with SegWit2x which was a combination of SegWit plus a hard fork to increase blocksize to 2mb. SegWit2X was abandoned November 8, 2017 due to lack of consensus

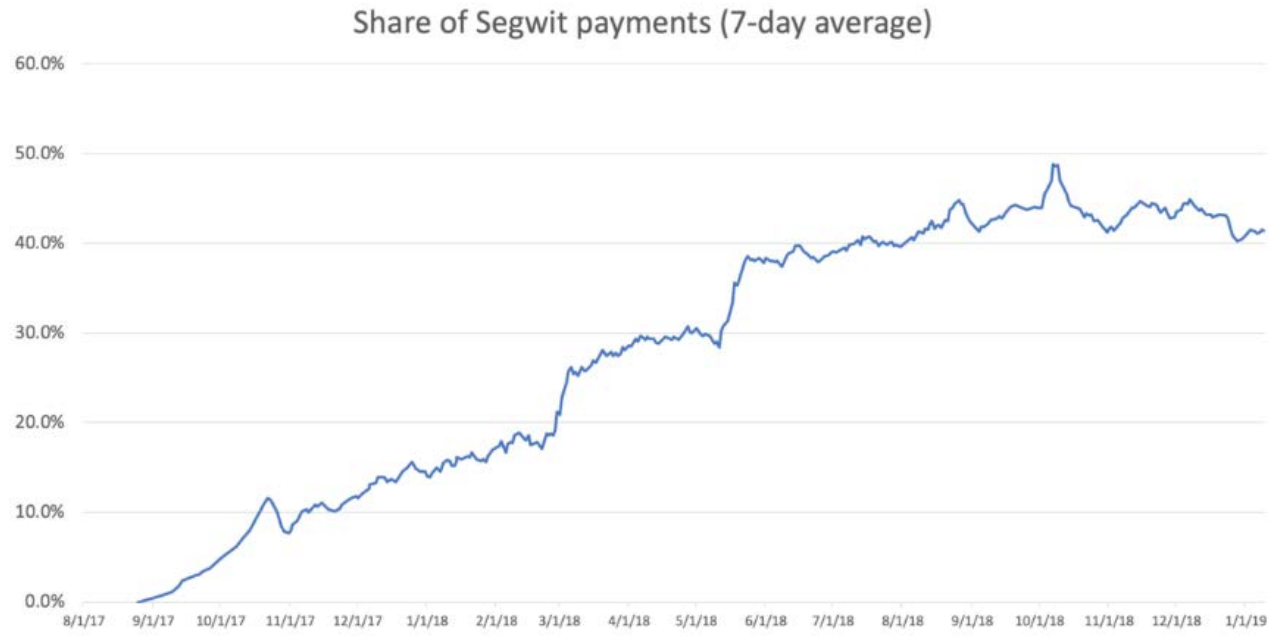
https://en.bitcoin.it/wiki/Segregated_Witness https://en.wikipedia.org/wiki/SegWit

Segregated Witness (SegWit)

Solution

- SegWit is necessary for adoption of Lightning Network

Segwit is a soft fork protocol upgrade to fix all forms of malleability and increase the block capacity. The Segwit transactions use different signatures and redeem scripts that are moved to a new structure, which doesn't count towards a block size limit of 1MB. Depending on the parameters, Segwit transactions are at least 25% smaller in size when compared to legacy transactions. Therefore, the blocks are still the same size but they can fit more Segwit transactions. Since they are smaller and the fee is determined by size, the Segwit transactions naturally cost less. Basically a smaller fee can achieve the same speed as legacy transactions.



https://www.theblockcrypto.com/2019/01/11/segwit-adoption-tapers-off-after-rapid-early-growth/

Segregated Witness (SegWit)

Solution

- Not all exchanges have adopted yet
- More transactions in block mean less congestion and lower transactions fees

Exchange	Segwit
Binance	No
BitMEX	No
Coinbase	Yes
Gemini	No
Bitfinex	Yes
Bitstamp	Yes
Bittrex	No
Kraken	Yes
Poloniex	Yes
HitBTC	Yes
Shapeshift	Yes

https://bitcoincore.org/en/segwit_adoption/

Lightning Network

Key documents

- https://github.com/lightningnetwork/l...
  https://github.com/ElementsProject/li...
  https://github.com/ACINQ/eclair

Videos

- https://www.youtube.com/watch?v=UULNfNjlZ5w