

CKB Fiber Network

the best thing you may have never heard of about bitcoin lightning
network

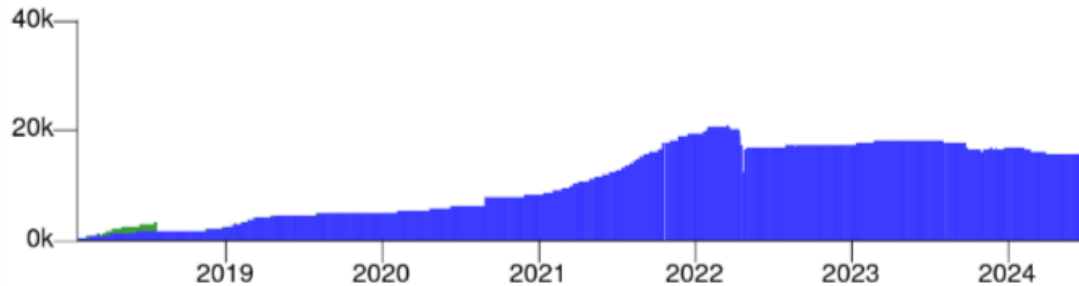
Mass adoption

Everyone is anticipating it, but can we live long enough to witness it?

2024, the year of BTC L2? All quiet on the LN front

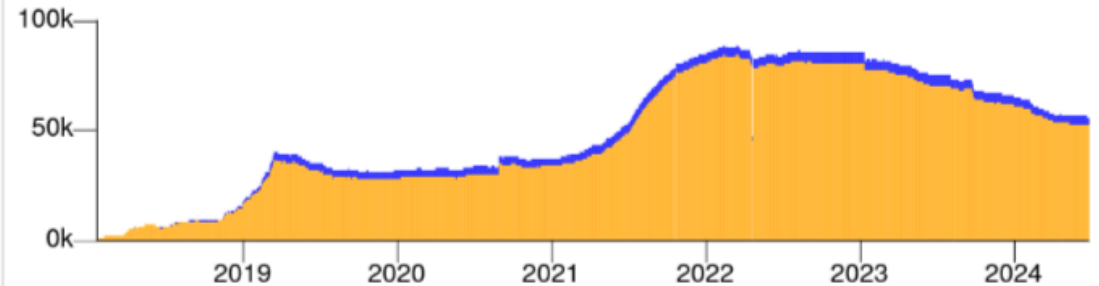
Nodes

Number of nodes with and without channels.



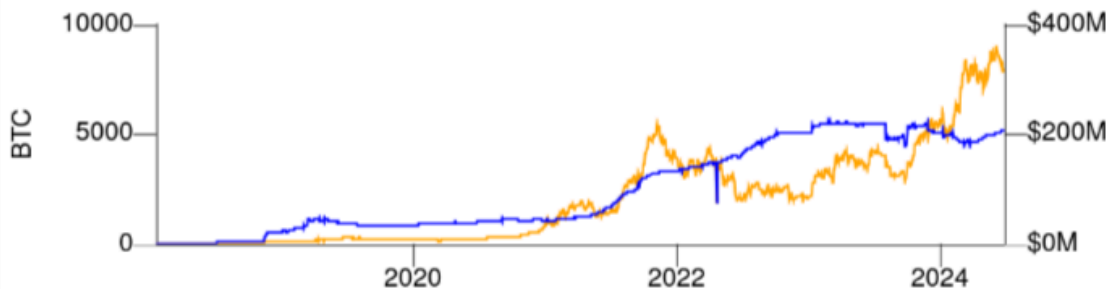
Channels

Unique = channels connecting nodes directly for the first time. Duplicate = channels between nodes that are already connected.



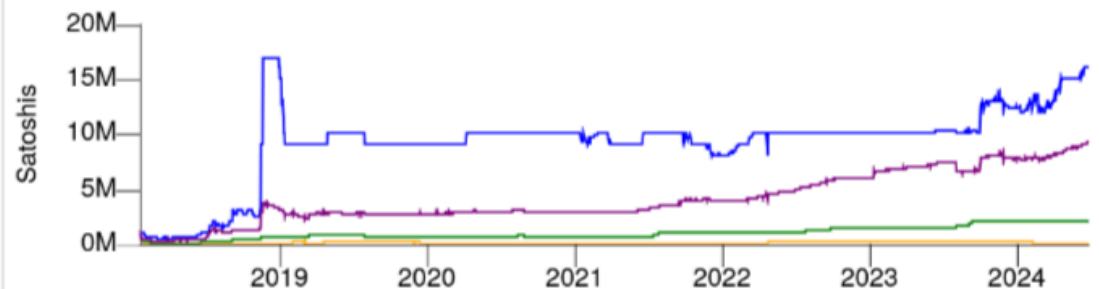
Network Capacity

Cumulative bitcoin capacity across all channels.



Capacity Per Channel

Channel capacity statistics.






User experience
of lightning
network (or
crypto currency
in general)




Rethinking lightning

Source: Rethinking Lightning <https://stacker.news/items/379225>



\$60766

@ar

 Rethinking Lightning

51.5k sats \ 133 comments \ @benthecarman 7 Jan bitcoin ...

Over the last few months it feels the bitcoin community has gotten more and more jaded on lightning. To be honest, for good reason, back in 2017 we were promised a decentralized payment network that would always have cheap payments and everyone would be able to run their own node. Nowadays, the average lightning user actually isn't using lightning, they are just using a custodial wallet and the few of that do run lightning nodes often find it a burdensome. For us at Mutiny Wallet, we are trying to make this better by creating a lightweight self-custodial wallet and in my opinion we have been executing on that dream fairly well. In this post, I'll analyze these issues and present a new way to view lightning and what that means for bitcoin going forward.

First and foremost one of the hardest UX challenges of lightning is channel liquidity. No other payment system has these problems today besides lightning so this often confuses lots of users. To make matters worse, there aren't any practical hacks that we can do to get around this. Muun Wallet used an on-chain wallet + submarine swaps to get around the channel liquidity problem, this worked very well until fees went up and everyone realized it wasn't actually a lightning wallet. The better solution is JIT liquidity like we do in Mutiny or splicing like that is done in Phoenix. These solutions abstract some of it away but not enough, we often get support questions confused on why some payments have failed

- Nowadays, the average lightning user actually isn't using lightning, they are just using a custodial wallet and the few of that do run lightning nodes often find it a burdensome task.
- First and foremost one of the hardest UX challenges of lightning is channel liquidity.
- The other major pain point of lightning is the offline receive problem.
- Combining existing large scale lightning infrastructure with self-custodial solutions sadly, isn't totally possible.
- So how do we scale ownership? Simply put, the answer today is custody, whether that is pure custodial like a Wallet of Satoshi or in the grey area like fedimints and liquid, the only way to do it today



“ Are we doomed then? Is there no way to scale bitcoin in a self-sovereign way? Luckily, the answer is no, but we need some soft-forks. Covenants are the way to scale bitcoin ownership.

”

What covenants can do?

Source: <https://covenants.info/overview/summary/>

use case	apo	ctv	txhash	tluv	intro	vault	catt	matt
Lightning Symmetry	yes	csfs*	csfs*	?	yes	no	yes	yes
Vaults	yes*	yes*	tap*	yes	tap*	yes	yes	yes
Payment Pools	yes	yes	tap*	yes	tap*	~ctv	yes	yes
Ark	no	yes	yes	no	yes	~ctv	yes	yes
Fraud Proofs	no	no	no	no	no	no	yes	yes
Statechains	yes	csfs*	csfs*	?	yes	no	yes	yes
Spacechains	yes	yes	yes	?	?	~ctv	?	?
Congestion Control	no	yes	yes	no	yes	~ctv	yes	yes

Two major problems in lightning network

- Use case 1 Lightning Symmetry: async receiving
- Use case 2 Payment Pools: inbound liquidity

Think every merchants needs to run their own node 7*24 hours and always check their inbound liquidity to receive money normally.

When can we use covenants on BTC?



Join BTC by CKB



Wait, does CKB have covenants already?

They have always been there. Just too trivial to give a dedicated term.



And can CKB do that?

Alternative Designs

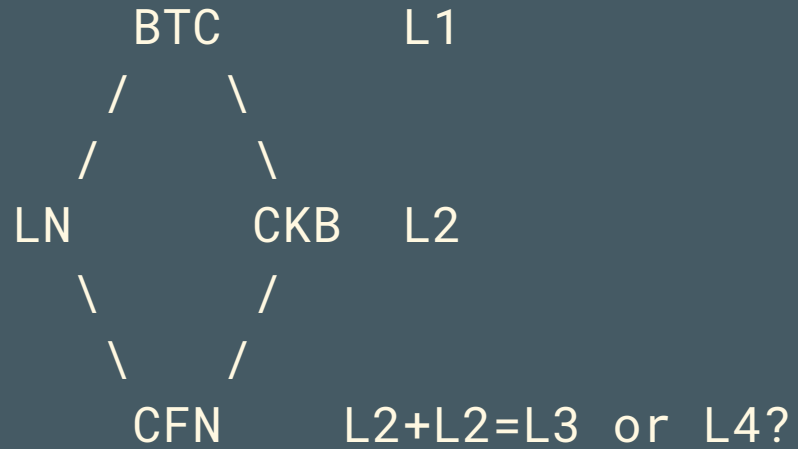
use case	apo	ctv	txhash	tluv	intro	vault	catt	matt	tplk	CKB
Lightning Symmetry	yes	csfs*	csfs*	?	yes	no	yes	yes	yes	yes
Vaults	yes*	yes*	tap*	yes	tap*	yes	yes	yes	tap*	yes
Payment Pools	yes	yes	tap*	yes	tap*	~ctv	yes	yes	tap*	yes
Ark	no	yes	yes	no	yes	~ctv	yes	yes	yes	yes
Fraud Proofs	no	no	no	no	no	no	yes	yes	no	yes
Statechains	yes	csfs*	csfs*	?	yes	no	yes	yes	yes	yes
Spacechains	yes	yes	yes	?	?	~ctv	?	?	yes	yes
Congestion Control	no	yes	yes	no	yes	~ctv	yes	yes	yes	yes
ETA	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	2019

- yes*: CTV/APO enable better vaults than are currently possible, but not nearly as good as OP_VAULT ones.
- tap*: yes if combined with something that allows turning a script into a Taproot, plus often also OP_CAT
- csfs*: yes if combined with OP_CHECKSIGFROMSTACK
- ~ctv: yes but only because the OP_VAULT proposal also includes OP_CTV

Request for fact-checking

- You are welcome fact-check my hasty conclusion above (it's backed by only over-confidence).
- I will not fix any inaccuracy in my slides, as CKB is easily fixable.

Introducing CKB Fiber Network (CFN)



$$2 + 2 = \infty$$

- Lightning network: Instant, Infinitely Scalable P2P Payment System
- CKB: Unmatched Flexibility and Interoperability

Call this L_∞ instead of L_3 or L_4 .

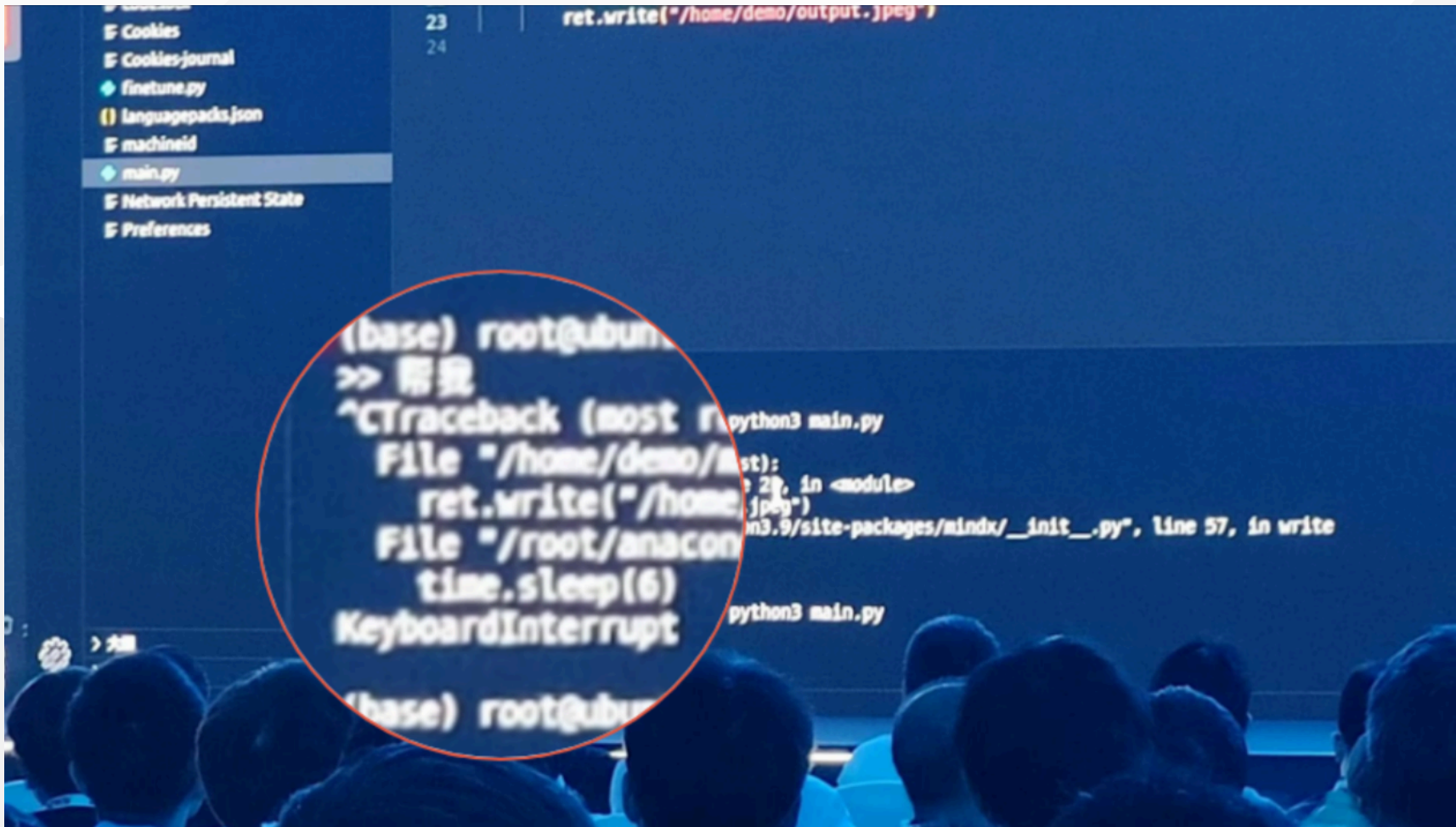
At this point, you may be completely bewildered.



Talk is cheap

Show me
~~the cool~~
~~demos~~

```
time.sleep(6)
```



High level overview of CFN

Before we going down into the details. Here is a high level overview of CFN.

- Use the same building blocks as lightning network (HTLC and revocation)
- Native multiple assets support (with extensibility)
- Cross-chain payment channel network thanks to CKB-VM's flexibility

Demo time and some bad news

We only have time to show some staged animations.

TODO: show some testnet transaction screenshots on the explorer websites.

CFN as of today

- Native multi-assets payment channel network
- Native bitcoin lightning network interoperability with atomic 2-way transfers
- Same secure assumption with bitcoin

TODO: refine the list here.

CFN as of tomorrow

We will be focusing on the infrastructure side that application developers can leverage to change the world.

- Feature parity with bitcoin lightning network (watch tower, multiple-hop network)
- Leverage existing BTC lightning network infrastructure for payment routing
- Rethink lightning network with CKB's extensibility and programmability, e.g. Non Interactive Channels, Ark like payment

Conclusion

- CFN as of today is a LN compatible instant, infinitely scalable payment system.
- Augmented with CKB's Unmatched Flexibility and Interoperability, CFN significantly enhance LN's programmability and unlock a whole new area of use cases.



Join the force

Come and build
For Life is too short
To wait for BIPs to
land