Scalability of Lightning with different BIPs

Some back-of-envelope estimates

Thaddeus Dryja <tadge@lightning.network>

Scaling Bitcoin 2015.2, Hong Kong

Lightning Intro

No time for a detailed description of how the Lightning Network works (will work) here but documented, or ask me ?s after the talk

Helps a lot with scalability by keeping some transactions off the blockchain

When things fail, falls back to the efficiency and security of standard bitcoin transactions.

Can Lightning work today?

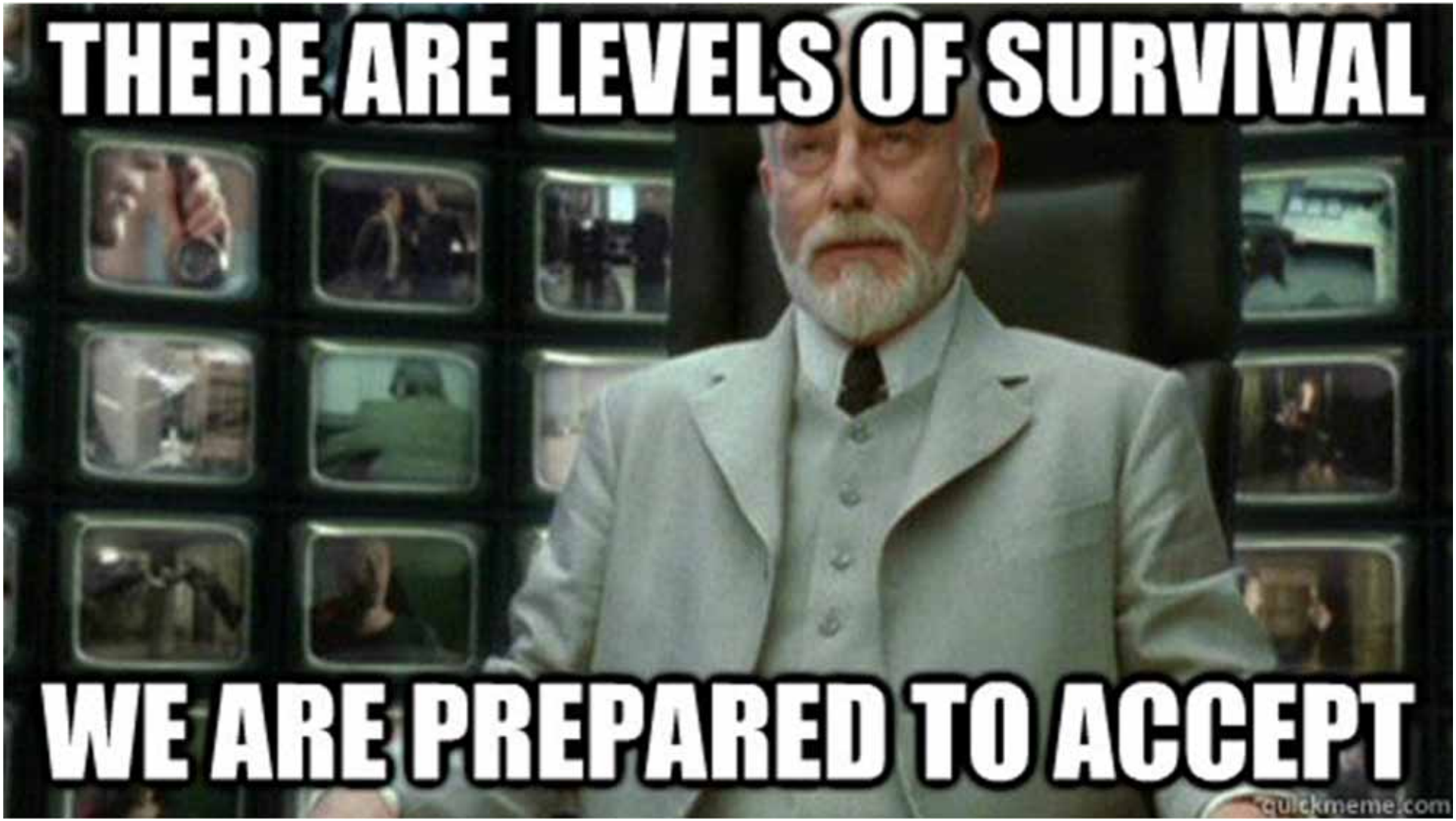
Not today, but check back in a week!

Efficient lightning channels need time locks, relative time locks, and reliable spends from unconfirmed txs.

OP_CLTV is almost active

OP_CSV may be soon

Minimum Viable Lightning



Minimum Viable Lightning

Channels can work with *only* OP_CLTV
So next week!
But much less efficient
Lightning models, least to most efficient

LightningLevel 1

LLvl 1: OP_CLTV only

Channel Open	Channel Close	Channel Duration	Channel Monitoring	Generalized Channel Awesomeness
1 input, 1 sig 3 outputs 350 Bytes	2 inputs, 4 sigs 2 outputs (PKH) 700 bytes	1 Week	Must be done by user	Low

(note that these numbers are approximate, and **minimums**)

LightningLevel 2

LLvl 2: OP_CSV (or OP_MATURITY or whatever is the coolest name)

Channel Open	Channel Close	Channel Duration	Channel Monitoring	Generalized Channel Awesomeness
1 input, 1 sig 3 outputs 350 Bytes	2 inputs, 4 sigs 2 outputs (PKH) 700 bytes	**Indefinite**	Must be done by user	**Medium**

LightningLevel 3

Channel Open	Channel Close	Channel Duration	Channel Monitoring	Generalized Channel Awesomeness
1 input, 1 sig 3 outputs 350 Bytes	1 inputs, 2 sigs 2 outputs (PKH) **350 bytes**	Indefinite	**Maybe be anonymously / kindof untrustedly outsourced**	**High**

SigHash_NoInput / SegWit

- SegWit is cool as sipa just said
- Also kind of weird. (In a good way)
- May want some more time to test it out
- SigHash_NoInput is very simple, doesn't "fix" malleability (txid still changes) but makes it irrelevant (sig is still OK even with new txid)
- Can be done with a soft fork, multisig only; OP_MULTISIG2
- Could also get rid of 0 bug in multisig
- More efficient sigs (less to hash)

Back of Envelope

3 LN levels, 1, 2, 3 for different BIPs

3 Blocksizes for different BIPs:

- 1 MB (BIP 0: Inertia)
- 8 MB (BIP248: 2MB, then 4MB, then 8MB)
- 32 MB (BIP100: Miners vote, max 32MB)

3x3 matrix

Assumptions and extrapolations

½ of txs are LN opens and closes
½ of LN closes and opens are merged
No non-cooperative closes
3 Channels per user
When indefinite, channels last 6 months

LLvl 1: 150 chan / year, 150 close, 75 open
LLvl 2: 6 chan / year, 6 close 3 open
LLvl 3: 6 chan / year, 6 close 3 open

Scalability Matrix

# of LN users	LLvl 1 1.25 MB / user / year	LLvl 2 5KB / user / year	LLvl 3 3KB / user / year
1 MB 52GB / y (25GB for channels)	20K	5M	8.3M
8 MB 420GB / y 210 GB for channels	168K	42M	70M
32 MB 1.7TB / y 840GB for channels	672K	168M	280M

Conclusion

Lightning can help a lot w/ scaling
Relative locktime helps a lot
NoInput or SegWit pushes scalability even further, also improves usability
Can support a significant fraction of humans with reasonable block sizes
Further research is required (lots of guesses about how people will use it)

Thanks!