The Case Against Lightning

tions///Security to the interesting and the contract of the security of the contract of the co

是"大利的"的"大利",在1945年,在1945年,1945年,1945年,1945年,1945年,1945年,1945年,1945年,1945年,1945年,1945年,1945年,1945年,1945年,1945年,

La 18 2A 19 Transfeld and the Strain Carlo Strain Carlo Strain Carlo Strain Carlo Strain Carlo Strain Carlo Str

Notes to the parish the said

ear and a process of the second

"在我的事情不是我们是

Short talk + Long Q&A

HARM TRANSPORTED AND THE RESIDENCE AND ADDRESS OF A STATE OF THE STATE

Paul Sztorc – CEO LayerTwo Labs

@truthcoin on X | @psztorc on Telegram
truthcoin.info | drivechain.info | LayerTwoLabs.com

TabConf - Oct 15, 2025 - (12:30 - 1:30 PM)

Overview

Thesis: Lightning is a waste of time (and money).

People will regret associating with it.

Talk: (15 minutes)

- Just a review of everything I've said since 2022

Q&A: (45 minutes)

- Take your best shot!

In A Nutshell

The "channels" idea is fundamentally unworkable.

- There is not enough blockspace (on L1) for even 1% of the Earth's population to use Bitcoin via Lightning.
- The "Channels" themselves are difficult to operate and maintain. They offer a poor UX and are unreliable in practice.
- It matter who you open a channel with this steers the idea toward "brands" and away from cypherpunkism.
- The cost/benefit ratio does not meet the required standard.

Demonstrations of it "worked" are rooted in misunderstanding.

- Most testimony comes from laypeople (easily duped, and their testimony is worthless).
- Payment networks have network effects (ie, "Venmo me") so scaling to 8 billion is mandatory (for LN).

Lightning insiders are already abandoning it.

- Quotes from experts, especially Burak (the creator of ARK).
- From Lightning to Covenants.
- The stragglers are fools (or dupes) who have no idea what they are shilling.

• The hype of lightning is mostly rooted in deception (and self-deception).

- Lightning was born out of Blocksize War politics, and never left.
- The cultural relevance of lightning is rooted in peer pressure / conformity / emotion it is a cult, not a scientific idea.
- Lightning has skillfully evaded and suppressed criticism, in ways that make "Shitcoins" look honorable by comparison.

• Lightning creates a "developer grift".

- A parallel "prestige world" where developers use technobabble to impress gullible investors, and take their money.
- The arcane vocabulary is just another tool for muddying the waters and painting Lightning with an illusion of respectability.
- Lightning damages Bitcoin by "crowding out" good ideas.

My Lightning Timeline

- May 2015 Tadge / Joseph SF Bitcoin Meetup LN Presentation I watched it on Youtube. Over this year, there would be thousands of reddit posts (pro and anti lightning) yet, this one video never had more than 350 views (at that time). The people who argue about lightning, don't know about lightning.
- Dec 2015 Scaling II in Hong Kong wide agreement that Lightning is the thing to try. (+ soft forks, + scaling in layers). Mar 2016 I research the technology, and post a variant: "Lightning Network for Hivemind" (P2P oracle + prediction market thing basically PolyMarket on Bitcoin). I knew exactly how Lightning Worked, in 2016.
- **Feb 2019** Bitcoin Meetup in Mexico <u>everyone</u> is thrilled by a new "Lightning Wallet" (BlueWallet) I download it and instantly receive 8 satoshis from the person next to me I ask "is it custodial?" this room (full of 25 people) has no idea what I'm even talking about. **All lightning supporters are dupes.**
- Feb 2022 On bitcoin-dev, "ZmnSCPxj" incorrectly says that L2 blockchains don't scale, because "you have to show your transaction to everyone" (both false and irrelevant). I point out that you must "show everyone" an LN channel open txn, and there is not enough space. No Response April 2022 I publish "Lightning Network: Fundamental Limitations" It is a bullet point at the large Miami BitDevs (coincident with the large conference), but again there is no response. In fact, two high-level lightning engineers, messaged me to say "until I read your 2022 article, I didn't realize how lightning works". Even the "experts" / mailing list crowd, cannot show us how the Lightning Network might work, at scale.
- Late 2022 While doing fundraising for L2L I had one solitary slide (of like 60) about how LN doesn't work and we deserve better. People often reacted badly to this slide and suggested I take it out. Telling the truth about LN will hurt your career.
- June 2023 Burak (who crashed the entire public LN for fun a few times), inventing ARK "I've always been a big critic of Lightning. I had severe objections, right? ..from inbound liquidity, to inbound receiving interactivity ... I wanted [with ARK] to address the inbound liquidity problem, but I really couldn't find a cure for it. ... I fail to see Lightning scaling." April 2023 a very big LN name, pulls me aside in the hallway and complains "If I try to present honestly about problems at Lightning Conferences, then I get disinvited." Mar 2024 I collect <u>many</u> quotes and publish "the LN Blackpill" again <u>no response</u>. The experts all know Lightning is doomed and are covering it up.
- June 2025 I "debate" Alex Gladstein his argument for lightning boiled down to "I have an email from someone in Keyna who says they used it once" I "debate" Harsha Goli, he basically says "the hype is more important than the technology" and when pressed about technical issues says "take it to the mailing list" unaware that I already did that 3.5 years before. I'm an idiot for even still talking about LN. I should just move on.

What is Lightning?

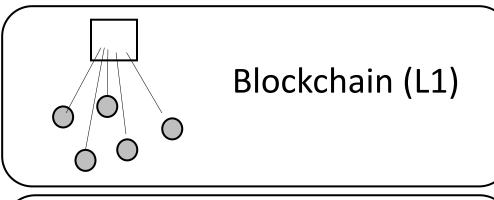
- "Scalable off-chain instant payments"
 - Don't transact on L1
 - (Scale without Blocksize increase)
- "via a network of channels"
 - Offload txns <u>away from L1</u>
 - Onto: a <u>network of micropayment channels</u>
 - Using: the <u>HTLC</u>

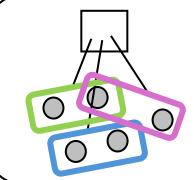


Payer wants to pay.

Receiver wants to receive. (\$)

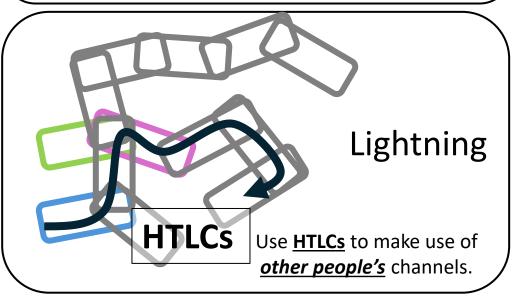
How to entice 3rd parties to facilitate your txn? HTLC.





Channels

2 people = 1 channel



The Channel Idea & the HTLC Idea Both Don't Work

Lightning Network -- Fundamental Limitations

04 Apr 2022

I use basic arithmetic to derive limitations of the Lightning Network. Because the analysis is so basic, I hope it will [1] stand the test of time, and [2] be easier for everyone to understand.

SUMMARY

- Channel-open transactions must be broadcast on L1, but there is simply not enough L1-space.
- "Factories" can onboard more users per L1 txn. Unfortunately, they can be sabotaged for free. CoinPool has the same problem (when it comes to LNonboarding). The limitation is fundamental.
- There are scenarios where LN-users consume *more* bytes than L1 "onchain" users. These are interesting, especially when it comes to use of HTLCs.

B. REALISTIC ASSUMPTIONS

Let's get some more realistic assumptions:

- The effective onboard rate will NOT be 43 vbytes per onboard (via a laughably implausible single 1-input-23250-output txn). Instead, there will be roughly one input per output (for the "rich guy" story to play out, we must also include a second "change output"). So the effective rate would be closer to 143.5 vbytes ([41 + 66/4] + [43] + [43], see P2TR here) per onboard. (Even this assumes that we never need more than 1 input, which is highly optimistic.)
- Similarly, each user will need at least 5 channels, in practice. And these will not be permanent they will last (on average) perhaps 1 year²:.
- Moreover, when channels close and reopen (sometimes un-cooperatively³),
 they will consume blockspace, leaving less for LN-onboarding. So, 99.97%
 onboarding block portion is not realistically achievable, let's go with 90%. (Still very optimistic.)

Channels

So, if we redo the analysis with non-absurd numbers, we get:

```
900,032 / 143.5 = 6,272 channels opened, per block [see above]
6,272 / 5 channels per user = 1255 users onboarded per block
6*24*365 = 52,560 blocks per year [6 blocks/hour]
-----
65,962,800 users onboarded per year

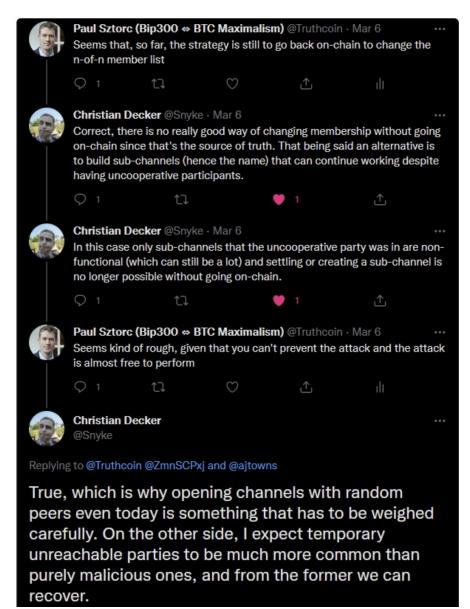
8 billion people per Earth,
divided by 65,962,800 onboards/year

= 121.28 years
```

In other words, each year we'd only onboard 0.82% of the world⁴.

Worse: if channels last merely one year, then by Jan 1 2025, we will need to re-onboard the people who joined on Jan 1 2024. In *that* world, *only* 0.82% of Earth's population, max, can be *bona fide* Bitcoin users (at any one time).

Do channel factories help? No



nel by splicing out the red party, after it has become unresponsive. The other three parties can merge their current outputs of the allocation into a new shared account. Broadcasting the old allocation and the new hook will remove the unresponsive party from the channel.

Fig. 10. A multi-party channel of eight parties, which are divided into three overlapping subgroups of four parties each. Only signatures from four parties are needed to move money between channels inside one of the subgroups, but all eight nodes can be connected at least indirectly.

The new hook must replace the other commitments from the replaced subchannels. This is possible using either a lower or no timelock for timelocked commitments or by disclosing any secrets of revocable commitments. It is not necessary to broadcast the new hook transaction right away, so the group can hope that the crashed node eventually recovers and a new allocation can be created or a regular settlement be executed. If it is not the case the allocation has to be broadcast to the blockchain, which makes all subchannels occupy blockchain space.

With splice out, it is feasible to wait for crashed nodes to return, thus good partners for a group may be offline occasionally, but if they do not intend to return, they should leave the group in cooperation with the other parties.

3.5 Higher Order Systems

With larger groups, the coordination work required to sign a new allocation

Above: Conversation between Christian Decker (inventor of channel factories, and Researcher at Blockstream), and myself. Also: excerpt from the Factories paper.

In channels, you only have one counterparty who might become unresponsive – in factories, you have many.

C. FACTORY SABOTAGE

This is particularly bad for *onboarding* via factory, since the Ideal Onboard is going to look something like this:

```
Rich Guy Input 80 Coins ---> [43 byte Taproot Output]: Rich Guy -- Factory S

Newbie #1 -- Factory S

Newbie #2 -- Factory S
```

HTLCs

- HTLCs hurt your bottom line
- They <u>expand the size</u> of two transactions you need to broadcast in order to claim the money.
- Catch-22
 - When fee-rates are high, you can't use HTLCs. And the "network" of channels is useless.
 - When fee-rates are low, you can just use on-chain txn. LN is uncompetitive.

B. HTLCS

i. The Concept (of this section)

Imagine a world where it costs \$20 to take someone to court. Even if *you knew you would win*, you would **never** sue someone for <\$20. By "winning" the lawsuit, your net worth would decrease. If instead you let them get away with it, you would be wealthier.

ii. The Cost of Justice, in LN

Each HTLC costs 172 wbytes, or (172/4) = 43 vbytes.

How much does that cost, in txn fees?

Let's assume that txn fees are 5/txn, and txns are ultra-compact size of 141 vbytes. Then, *merely the HTLC part* (of the LN-channel-txn) will cost *the broadcaster* (43/141)*\$5 = \$1.52. That is the cost of the "ink", needed to write the HTLC part-of-the-txn into the blockchain.

Worse – you aren't truly "done", until you spend that HTLC money. In its current, unspent form, it is an "accounts payable" to the miners – a liability against your net worth. When you spend the HTLC, you will need to select it as an input, *and* provide the hash, *and* provide your signature. This will cost [32+4] + [32] + (64/4) = 84 vbytes. So the total cost is 43+84 = 127 vbytes. The total USD cost, of enforcing the HTLC, (in a world of \$5 fees), is (127/141)*\$5 = \$4.50.

Don't Take My Word For It

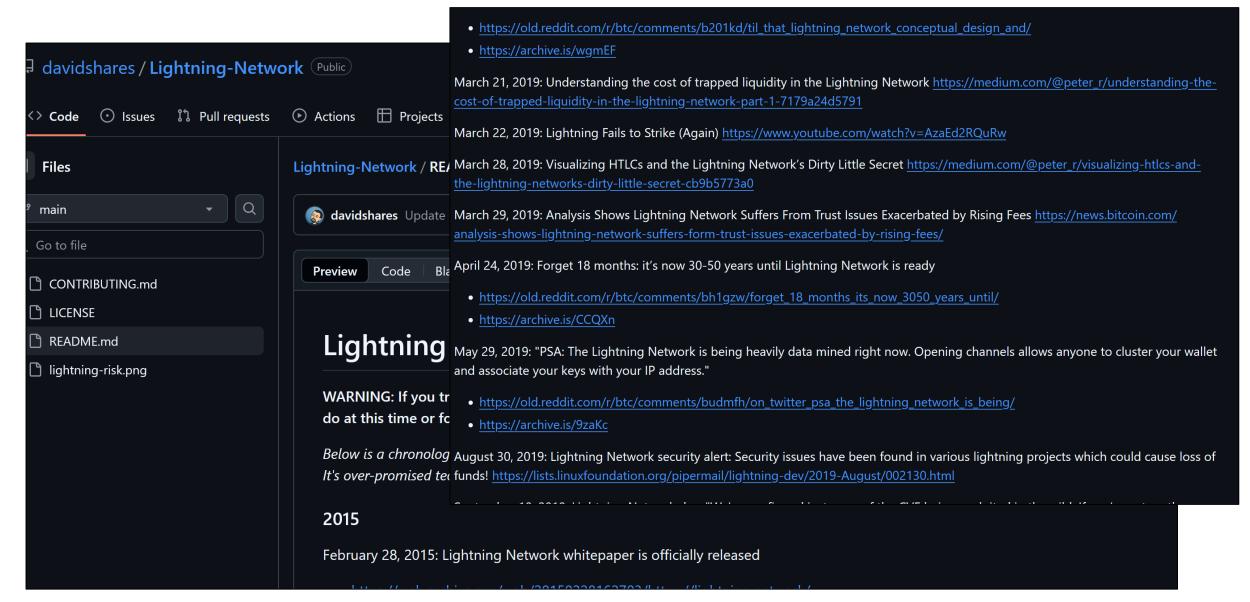
FROM ELITE LIGHTNING DEVS

- Tadge Dryja Creator of LN, 2019,
- "Everyone's like: 'LN is the gonna be the best thing ever'. Wait, uh, [LN] can't actually do that." (43:20 // 27:50)
- Matt Corallo, 10th known contributor to Bitcoin Core
- Nov 2022, Presentation, "Lightning is Broken (AF) .. but we can fix it (I hope)"
- May 2023 "Honestly, lightning today is kinda a joke, look at BTCPayServer

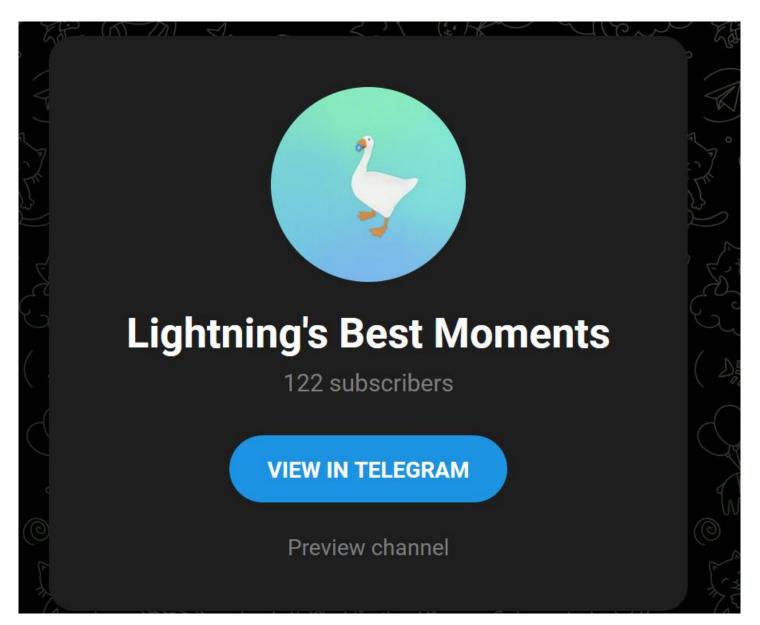
 you can install lightning with one click, and then you will generate
 invoices that are unpayable cause you have no inbound liquidity! Never
 heard of inbound liquidity? I dunno google it or something..."
- Burak Keceli inventor of ARK, and hacker who crashed most of the Lightning Network for fun in 2022
- June 2023, 1:25 "I've always been a big critic of Lightning. I had severe objections, right? ..from inbound liquidity, to inbound receiving interactivity ... I wanted [with ARK] to address the inbound liquidity problem, but I really couldn't find a cure for it. ... I fail to see Lightning scaling."
- Alex Bosworth head of Lightning Liquidity at Lightning Labs
- July 2021, "No algorithm can ever solve LN pathfinding/peering, because it
 is a 2 sided market system, just like no spam filter can ever get every spam
 and no targeted ad system can ever only show you only what you will buy.
 Heuristics can move the needle a long ways but they can never solve"
- • This image I made
- Dec 2022, "I worry whichever way you slice it things could all end in tears"

- Antonie Riard
- Oct 2023, "Effective now, I'm halting my involvement with the development of the lightning network and its implementations"
- Oct 2023, "On the culture crisis compromising the future of the Lightning Dev Kit project... they're trying to cover up their ethical past misbehaving or do "virtue signaling" to cover their inner softness in term of personal values. I understand the spiral team is under strain... to yield back value on the \$\$\$ which have been burnt in Spiral salaries since 2019, though this doesn't justify their behaviors."
- Dec 2023, Twitter Space where I interview Antonie
- Rene Pickhardt Author of "Mastering Lightning" and top contributor to LN StackOverflow
- Aug 2020, "The more I study the lightning network the more I realize with shock that there are so many misconceptions about the privacy of Lightning in the wild for which often just the opposite seems to be true // I am scared that even in Mastering lightning we won't be able to fix that :("
- Dec 2022, next paper: "Principle limitations of the #LightningNetwork for #Bitcoin payments"
- April 2023, 2023, MIT Bitcoin Expo Fundamental Limits of Lightning "bitcoin often ... is being very much hyped ... and we should also discuss
 the shortcomings ... creating p2p cash is very hard."
- CalleBTC, creator of Cashu (LN Chaumian e-cash)
- Sept 2023, "He asked why he needed a new channel. He already had one! ...
 Fvck"
- Jameson Lopp, Creator of Statoshi and Casa
- "we dropped lightning support later as a result of re-evaluating the tech and business."

Other People Have Made Similar Lists



t.me/LightningFantasy



Lightning's Best Moments

https://morehouse.github.io/lightning/ldk-invalid-claims-liquidity-griefing/

Matt Morehouse

LDK: Invalid Claims Liquidity Griefing

Discussion of a bug in LDK that can be exploited to lock up funds



● 171 4:01 PM

January 28

Lightning's Best Moments

https://njump.me/nevent1qqsrcpuja390k455csf7p8x9xxtr4gpngz7z 55f66mryap2wt00metcppemhxue69uhkummn9ekx7mp0qgsrm3rn g9975n0pmu03wtp3j65zquvahdvt4tu8vju7m2s8cm27nhqrqsqqqq palht3p

Brian of London (npub18h...wfmgv)

Short Text Note by Brian of London seen on nos.lol

Stuff nobody seems to know about Lightning....



How do you clear a stuck In-Flight payment which failed 1002 days ago?

Seriously? I'm working on some new code for my node and both the LND nodes I have have stuck payments like this. Obviously this node has been rebooted and upgraded numerous times in the last 1002 days!

February 3

st Moments

me/nevent1qqsrwqc4lyaajqnzuywm0kjqd6syr44xcct xv5smxcppemhxue69uhkummn9ekx7mp0qgsrm3rn 3wtp3j65zquvahdvt4tu8vju7m2s8cm27nhqrqsqqqqq

don (npub18h...wfmgv)

don on Nostr:

y Alby appears to be geo blocking Israel. This of the functioning of the so-called self sovereign y hard to access. Full details on my blog. https://p...

≯ INSTANT VIEW

● 177 7:13 PM

February 4

st Moments shtningd/35695

n Core Lightning (CLN)

tlc that expired over 3000 blocks ago for a forcediel. My clightning logs are showing *BROKEN* No .56. Channel state is ONCHAIN, but I've not receiv...

VIEW MESSAGE

201 6:14 AM

February 18

Lightning's Best Moments

https://fixupx.com/pavolrusnak/status/1891967156104954164



Pavol Rusnak (@PavolRusnak)

If you are running LND older than 0.18.5 and/or Lightning Terminal older than 0.14.1, stop what you are doing and upgrade immediately. Thieves are draining funds using exploit...



≯ INSTANT VIEW







● 154 6:51 PM

February 19

Lightning's Best Moments

Forwarded from Indomitus | 不屈の 夕



A Tweet



Nikita Zhavoronkov 🤡 @nikzh · Oct 31, 2023



Nostr creator: "Lightning is a scam" 🤪



[-] fiatiaf *** 8likes • 8 hours ago

Lightning is a scam.

reply tip permalink quote repost 1reposts



Merrcurr *** 1 likes • 8 hours ago

Glitchy, unpolished but how is that a scam?

[814595]

reply tip permalink quote repost



[-] fiatjaf *** 3likes • 8 hours ago

It is scamming bitcoiners out of their time and energy and money for 6 years.

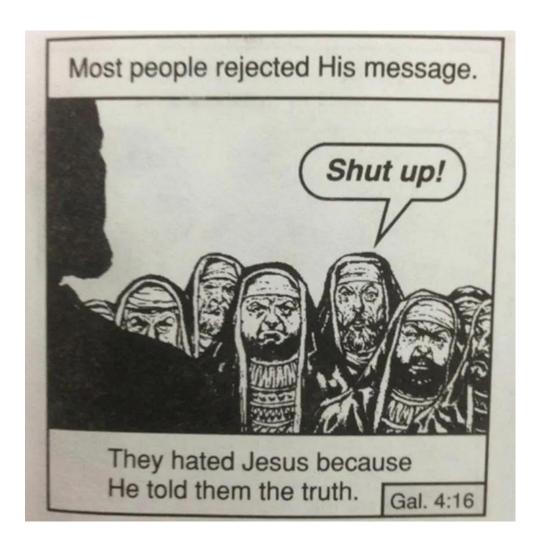


The problems with LN are:

- 1) onboarding -- everyone now admits that you cannot onboard 8 billion people to LN
- 2) (Now) need for op expire; enormous "channel risk" -- it matters who you open a channel with. They can lock your funds for 2 weeks, or even steal from you
- 3) inbound liquidity expensive, counterintuitive, bad UX
- 4) HTLCs consume too many bytes (L1 feerate dust effect), making them useless
- 5) routing / payment fail rate -- must be near zero
- 6) the use of the abominable and outrageous phrase "custodial lightning". Either we purge this term, or we admit to ourselves that Venmo is actually the best "lightning wallet". Since words don't mean anything anymore.
- 7) the culture around LN has warped the kinds of ideas one is allowed to express. We are now 20% meritocracy at most, and 80% LN propaganda factory at least. This is a runaway death spiral, for ancient Rome and for Bitcoin.
- 8) almost everyone who actually uses the real thing, dislikes it. Current coin uptake is microscopic 00.025%. Payments usecase has moved to USDT. Senior LN people, all move on to other things, including inventors Dryja/ Poon.
- 9) privacy is terrible, according to LN experts
- 10) 51% hashrate can steal from any LN channel, by censoring the justice txn. Moreover they have an incentive to do this, since LN siphons fees from miners.

Some Other Points (Quickly I Hope)....

Lightning Derangement Syndrome



- Lightning Sucks
- 2. You <u>tell the truth</u> about how it sucks.
- 3. People get angry, and defensive, and they say: *you suck*.

- As a result: lightning evades future criticism – because people don't want to put up with being harassed by idiots.
- We are all *lying to ourselves*.

Custodial Lightning

- Imagine getting in a "driverless Waymo"...
- ...and yet lo and behold a human driver, is in the front seat.
 - He drives the car to your destination (with his eyes and hands).
- Finally, as you leave...the driver says: "Waymo is the future of taxis; because a computer can drive cheaper and safer than any human driver".

Meet Waymo

The world's first autonomous ride-hailing service

⇒ Be one of the first



You would immediately think:

"Wow, this guy is SO stupid, that it's a waste of my time to even talk to him."

And what would you say? Out loud? Probably:

"Yeah – thank you. See you later! Bye."

Custodial = all the proof of work, blockchain, key management – it is all a waste.

When we are born, we cry – that we are come to this great stage of fools. – William Shakespeare

Types of Problems

- Every new technology has problems.
- Examples of <u>unrelated</u> (normal) problems:
 - "We hired the wrong guy, he had a bad work ethic. We fired him, but it has set us 4 months behind schedule."
 - "The idea is new, and our customers aren't used to it yet."
 - "I underestimated how much work it would be to finish."
- In contrast, these are examples of a problem <u>related to the heart of the idea</u>:
 - "Hi everyone, we just noticed that it is possible to attack a lightning channel by doing New Thing XYZ. This attack imposes a new cost (or risk) on the channel-owner. Luckily, we can fix the problem (I think) with New Complex ABC solution (which is also brand new and you're all hearing about it for the first time, right now)."
- The LN problems (pinning, liquidity, flood-and-loot, etc) are this second type.
- "Vitalik has said he will fix it" | BitShares technical whack-a-mole.

The Appearance of Success

Date	Event	The Appearance of Success
2003–2004	Elizabeth Holmes founds Theranos as a 19-year-old Stanford dropout. It promises to perform hundreds of blood tests with just a finger prick of blood.	
2004–2007	Raises \$6.9 million at a <i>\$30 million valuation</i> ; by 2007, raises \$43 million at <i>\$197 million</i> valuation.	
2009–2011	Holmes recruits a star-studded board—former Secretaries of State Henry Kissinger and George Shultz, General Jim Mattis, and former top executives like Richard Kovacevich. This lends enormous credibility to Theranos despite their lack of scientific expertise.	
2010	Theranos achieves a <i>\$1 billion valuation</i> by 2010 as it continued raising funds.	
2013: Public Launch and Media Blitz	Theranos emerged from stealth mode with a strategic PR wave. Holmes appeared in major outlets like Fortune, Forbes, and TEDMED, presenting herself as a visionary. The press mostly echoed the company's claims without peer-reviewed validation.	
2014 (10 years in)	making Holmes one of the Rupert Murdoch, the Devenillions of dollars. Walgre	ost \$9–10 billion valuation, raising over \$400 million in funding and e richest self-made women on paper. High-profile investors such as los family, and the Walton family each invested tens to hundreds of eens and Safeway signed partnerships to bring Theranos tests to retail of of scalability and trustworthiness.
Early to Mid- 2015: Mainstream Acceptance	BlueCross designated The Pennsylvania—one of sev	y was increasingly adopted in pilot programs. Health insurer Capital eranos as a preferred lab provider for 725,000 customers in veral corporate deals suggesting industry validation. The firm advertised is from a few drops of blood.

Simulation

- With drivechain / Bip300 I have actually simulated what the L2 network would look like, with 8 billion daily users.
- As a result, we can actually see:
 - How many coins are on each L2?
 - What Txn fee does each user pay?
 - How does the software perform?
 - What are the bandwidth requirements and full node requirements?
 - What is the ratio of L2 txns to L1 txns?
 - How much revenue is earned by miners?
- Why doesn't lightning do this? (Because it's not even possible.)

"But -- users don't <u>want</u> to use Bitcoin to transact. They use it as a store of v--"

Well just don't talk about lightning then!

Reality: This is cope/lame. Blame the users! For your shitty product. Anything to <u>evade</u> <u>taking responsibility</u>.



Make Your Choice

Orthodox View	My Alternative
Channels work. They are the future of Bitcoin. Problems will be solved with engineering.	They don't work. It's a waste of time. The engineers are playing pretentious games.
Paul is here to FUD lightning and shill Drivechains. Paul wants more clout / attention, so that he can get Bip300 activated.	Tidwell had to practically drag me here, I have very little interest in doing this. LN will collapse on its merits; and Bip300 will activate without code changes to Core – and it will do so because of its affect on miner revenues, ASIC valuations, and UX. I don't need anything from you.
Everyone just can't be wrong! Lightning has all these smart and nice people. Is Paul really smarter than everyone in lightning? Probably not.	LN came from the Blocksize war and is inherently propaganda. It will never shed this baggage. People are emotionally unwilling to admit they are wrong. Leading to peer pressure. Groupthink/ cults are common. The prestige economy / funding bias exacerbates this.
Paul did invent his own Lightning Technology in 2016 – his knowledge is now <u>old</u> and <u>obsolete</u> .	I was <u>early</u> . Both times: in joining LN; and in leaving. You'll be joining me eventually.