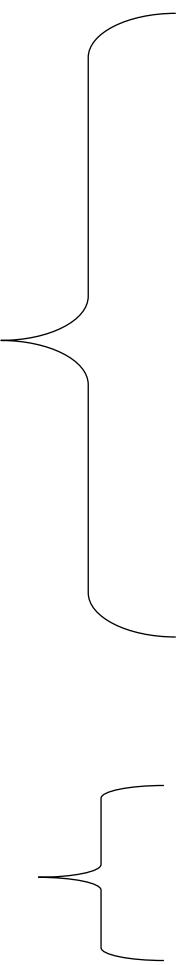


Victory, Unity, and Freedom – via Sidechains

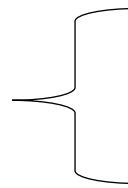
Paul Sztorc
Feb 14, 2024
Anarchapulco

Agenda

30 min

- 
1. Introduction
 2. The Title (“Victory, Unity, and Freedom – via sidechains”)
 3. What is the Sidechain,
 1. Visual Aids
 2. Try it Today
 3. Why this will win
 4. Bip300 for Miners
 4. How You Can Help

10 min

- 
- Q&A, or – Appendix Slides

My 1000+ Pages About Bitcoin

2012-2014 | Statistician, Yale Econ
→ Bitcoin Researcher

AUGUST 2015	MARCH 2016	OCTOBER 2017	SEPTEMBER 2018	JANUARY 2021
Nothing is Cheaper than Proof of Work 04 Aug 2015	The Peer Database ("Private Blockchains" Done Right) 17 Mar 2016	Fork Futures (via the Exchanges) 12 Oct 2017	Expensive Privacy is Useless Privacy 11 Sep 2018	OpenVote - Auditable, Fast, Private, Secure Voting 10 Jan 2021
The Win-Win Blocksize Solution 14 Jul 2015	Private Blockchains, Demystified 16 Mar 2016	Proof of Stake is Still Pointless 07 Jul 2017	Five Lies and the Truth 11 Sep 2018	APRIL 2023
JULY 2015	DECEMBER 2015	JULY 2017	JUNE 2018	Small Transactions 08 Apr 2023
The Win-Win Blocksize Solution 14 Jul 2015	Salvaging the Blocksize Discussion, in Two Questions 28 Dec 2015	Blind Merged Mining 30 Jan 2017	BitAssets - A Digital Assets Sidechain 21 Jun 2018	JUNE 2022
MAY 2015	NOVEMBER 2015	JANUARY 2017	APRIL 2018	The "Sidechain Vision" for Bitcoin 27 Jun 2022
Bitcoin and Deflation, The Last Word 15 May 2015	Drivechain - The Simple Two Way Peg 24 Nov 2015	Mining - Threat Model and Equilibrium Analysis 29 Jan 2017	Meditations on Fraud Proofs 14 Apr 2018	APRIL 2022
JANUARY 2015	OCTOBER 2015	The Mirage of Miner Centralization 28 Jan 2017	Blockchain Fusion (via Compensated Sidechains) 07 Apr 2018	Lightning Network -- Fundamental Limitations
BitUSD Isn't Worth The Trouble 29 Jan 2015	The Hashing Heart Attack 28 Oct 2015	Upgrading 'Smart Contracts' to 'Wise Contracts' 11 Jan 2017	Bitcoin Post-Maximalism 07 Apr 2018	OCTOBER 2021
NOVEMBER 2014	SEPTEMBER 2015	Two Types of Blockspace Demand 10 Jan 2017	GigaChain 20 Mar 2018	Security Budget II, Low Fees, and Merged Mining
The Limits of Blockchain Tech 28 Nov 2014	PSA - Linking to a Blog Section 05 Oct 2015	DECEMBER 2016	2021	FEBRUARY 2021
Altcoins Aren't Money, They're Bitcoin's Casino/Laundromat	Oracles are the Real Smart Contracts 21 Sep 2015	Against the Hard Fork 06 Dec 2016	NOVEMBER 2017	Sidechain For BitNames/Logins/DNS, Taking
Long Live Proof-of-Work, Long Live Mining 16 Nov 2014	Measuring Decentralization 09 Sep 2015	Better Fork Terminology 05 Dec 2016	The UASF Contradiction 02 Nov 2017	Sidechains for Scaling -- Thunder Network
Active Decentralization 09 Nov 2014	The Drivechain OP Code 14 May 2016	MAY 2016	The MAHF And Replay "Protection" 02 Nov 2017	Sidechains for Privacy -- zSide and Melt/Cast
Three Basics 06 Nov 2014	BTC Codex - The Digital Identity Sidechain 21 May 2016	More Terminology -- Forks and Splits 02 Nov 2017	NOVEMBER 2018	Gradually Activated Replay Protection (GARP) - Toward Hard Forks that Don't Suck
		Miners Don't Control Tx-Selection 02 Nov 2017	Deniability - Unilateral Transaction Meta-Privacy 09 Nov 2018	
		ASICBoost is Worthless 02 Nov 2017		

My Big Break

Dec 2014 – Adam Back links to my blog

ada

Sr. Member



Activity: 404

Merit: 318



in bitcoin we trust



December 29, 2014, 12:21:39 AM

#1

Some hypothetical thoughts about price stability, (lack of) price/supply feedback & long run electrical cost

Some hypothetical thoughts about price stability, (lack of) price/supply feedback and long run electrical cost.
Not a call to change anything just some thoughts.

One observation people often make about the difference between bitcoin & gold is that gold reacts to price changes, by rate of supply increasing when price is high, and rate of supply decreasing when price is low. This effect has some positive feedback loop in the direction of stabilising gold price.

Products with an inelastic supply function (like bitcoin or farming with long production lead times) result in gluts and shortages which take longer to self-correct than something with an elastic supply function.

While bitcoin cant directly know its price as that is an externality, one related thing it does know is the rate of difficulty change. An indication that supply is too high would be that difficulty is slowing, or similarly an indication that supply is too high difficulty increasing too fast.

So we could (hypothetically) change bitcoin to decrease subsidy per block if difficulty increase is above 10% per 2016 block period (2 week retarget).

What could we do with the unclaimed subsidy? We could defer it so that bitcoin subsidy lasts for longer, and/or we could bring it forward again if difficulty slowed, eg for example increase the subsidy per block if difficulty increase falls below 0%.

If subsidy is not deferred, just deleted, that saves electricity and reduces the supply.

One might even speculate that the absence of price or rate of difficulty change feedback is currently causing price drops as mining difficulty is falling for the first time while the production cost (mining) is efficient (close to market price of coins) even for the most efficient operators. Or put it another way miners in todays market would be happy to get another 5% at 13.125 btc/block over 12.5 btc/block.

A second question is if bitcoin is \$10,000/btc or \$100k or \$1mil which would be supported by various real-life uses eg see page 5 of report comparing to different aspects of gold ownership <https://cdn.panteracapital.com/wp-content/uploads/Bitcoin-vs-Gold.pdf> then at those prices, what happens to electrical use and mining investment. Is the result sustainable.

Now one argument is more security is needed for higher market cap \$21 tril? [And another argument is you cant have mining cost artificially pulled below market price or people will expend that amount of money anyway to bypass, bribe, hack etc the artificial factor. \(eg Paul Sztorc makes that argument in his blog post http://www.truthcoin.info/blog/pow-and-mining/\)](#) I notice Nick Szabo made a similar point in an old blog post also. The cynic may like to think of the lack of mining for USD (or other fiat) leading to huge expended effort for people to lobby, bribe etc to get access to government funds, where those funds partly come from inflation (which is a form of taxation) and also quantitative easing and bailouts. The resources arent actually saved, they just go into lobbying efforts and create cost via inefficient allocation of capital that arises as a cost of moral hazard.

Since Then...

- 2013/2014 -- wrote code/whitepaper for P2P oracle (BitcoinHivemind.com)
- Technical Talks
 - Scaling Bitcoin 1 2 & 3 -- Program Committee for #4
 - TabConf every year – keynoted in 2018
 - BitDevs – Summer 2014 (NYC), Austin (May 2018)
 - Bitcoin Wednesday – all around the globe (Toronto, Chicago, Amsterdam, etc)
 - Consensus Construct (2017, 2019); American Banker ; Qcon London (2017)
 - Bitcoin Miami 2019/2021/2022/2023 & Amsterdam (all years)
 - Countless podcasts, spaces, etc.
- Wrote BIPs 300 and 301.
- Raised \$3M to start LayerTwo Labs & help Bitcoiners dominate the world.

The Title

Victory

“Crypto” defeats “fiat”

The Title

Victory

The government can create as much money as they like, destroy as much money as they like, take ... , spend . And also observe (and eventually, censor) every mutually beneficial transaction between any two citizens.

“Crypto” defeats “fiat”

Open source software that
protects the user’s rights

8 billion people use it, everyday

The Title

Victory

=

Unity

+

Freedom

Open source software that
protects the user's rights

8 billion people use it, everyday

Only one coin should win.

- “Crypto” defeats “fiat”
- 1) New coins = inflation = annoying
 - 2) Worry about coin-replacement (ie coin-failure)
 - 3) Contradiction / Regress to barter
 - 4) Network effects

Victory = (Unity + Freedom) = Sidechains = Drivechain = Bip300

The government can create as much money as they like, destroy as much money as they like, take ... , spend . And also observe (and eventually, censor) every mutually beneficial transaction between any two citizens.

The Title

Victory

=

Unity

+

Freedom

“Crypto” defeats “fiat”

Only one coin should win.

- 1) New coins = inflation = annoying
- 2) Worry about coin-replacement (ie coin-failure)
- 3) Regress to barter / contradiction
- 4) Network effects

Competition

Choice of blockchain software.
Easy to create a new choice.
Easy for user to switch.

Solves problems of unity:

- 1) Mistakes in any piece of software
- 2) Laziness/corruption of devs
- 3) Disagreement among users
- 4) Heterogenous users

Victory = (Unity + Freedom) = Sidechains = Drivechain = Bip300

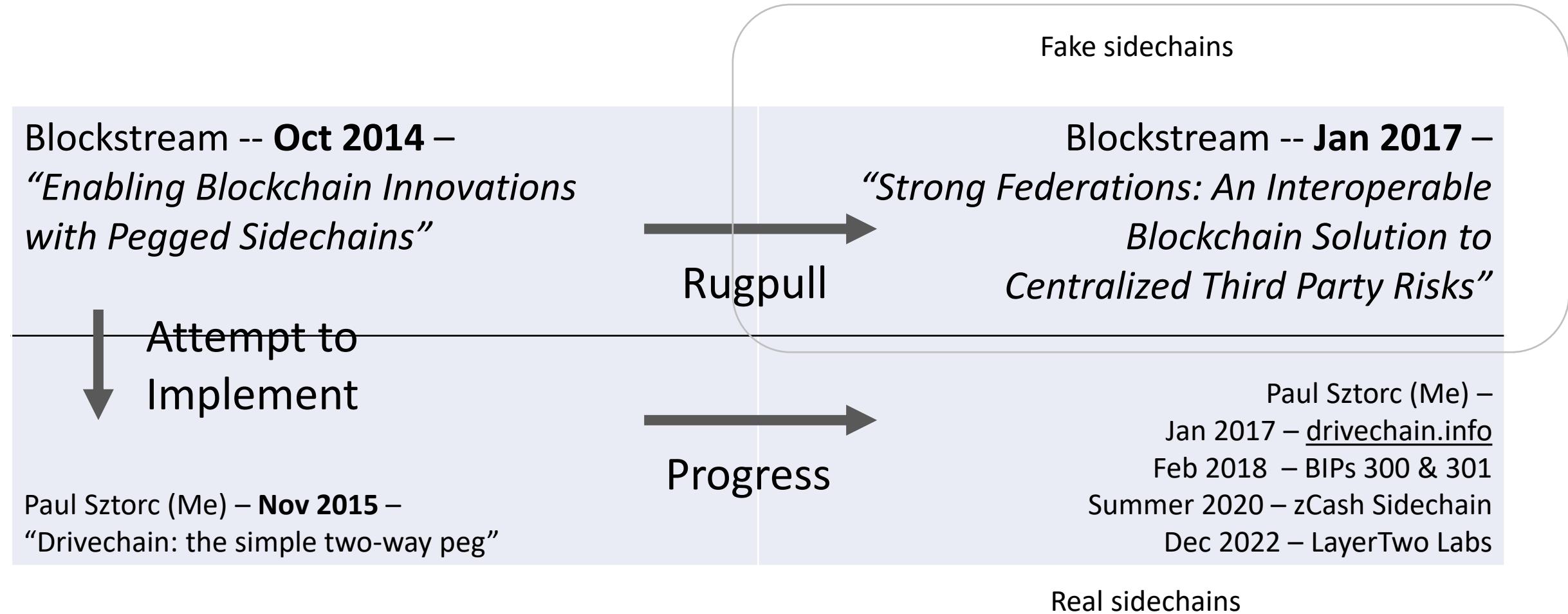
N00bs / poor people: txn fees
activists: privacy
normal people: UX

We want:

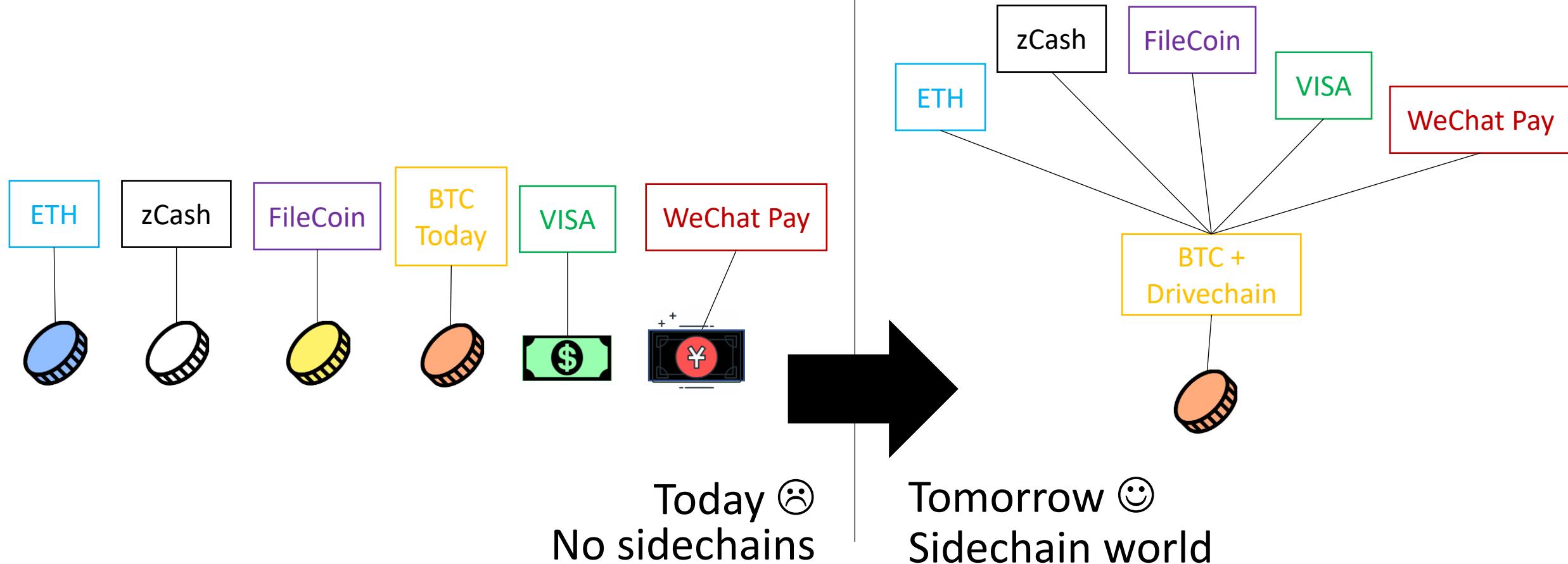
- One cryptocurrency (ie, “21 million coins” only)
- Multiple blockchains, run by different people who all hate each other
- The ability to always add more new blockchains.
- The ability for users to always switch between these as they like.

... getting one of the two, is easy. But how to get both?
...that is what sidechains (BIP300, “Drivechains”) provide.

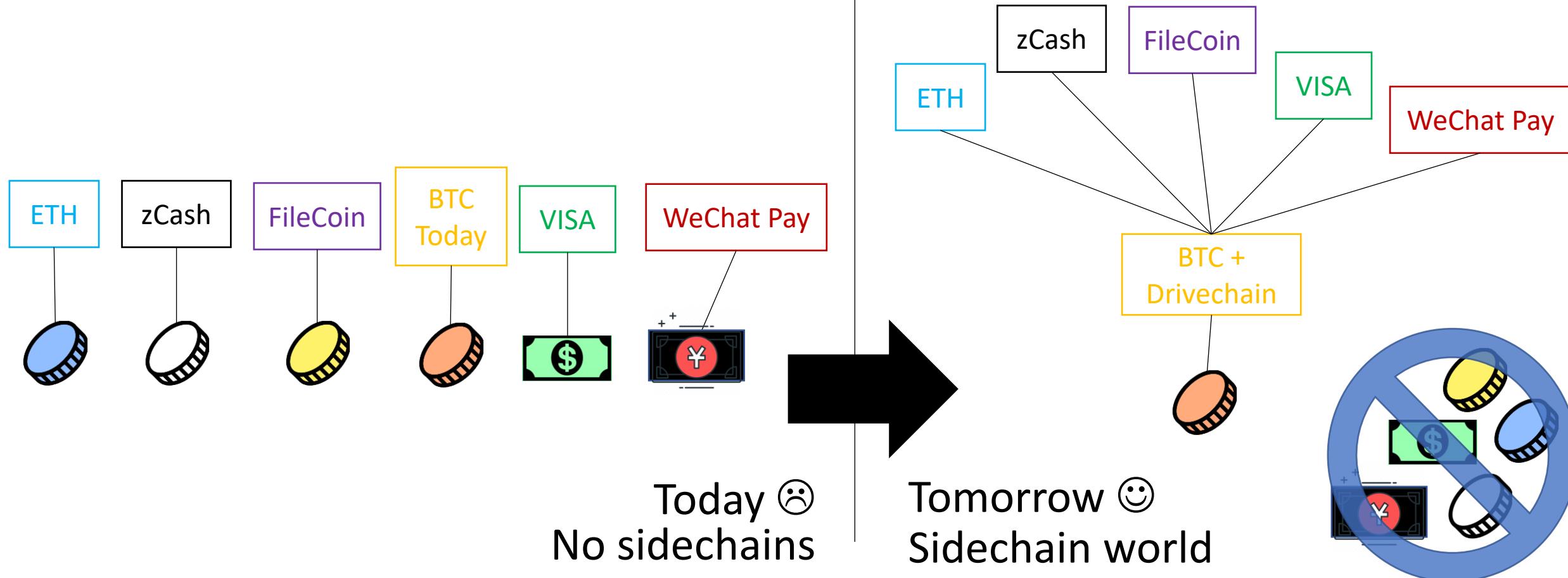
History Lesson



BIP300: Everything on Top of Bitcoin

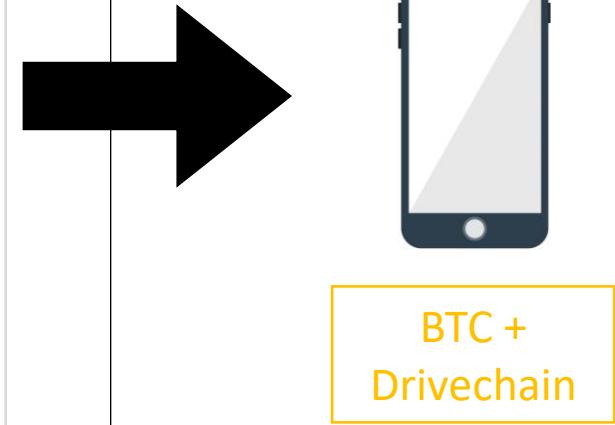
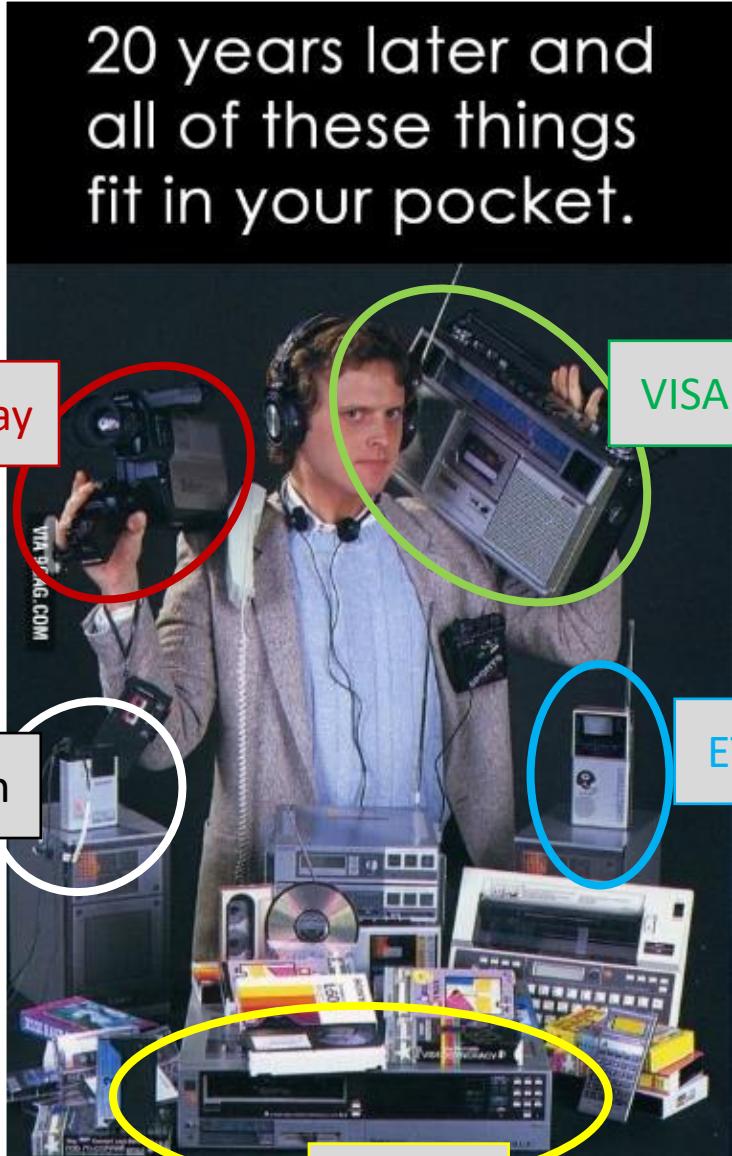


BIP300: Everything on Top of Bitcoin

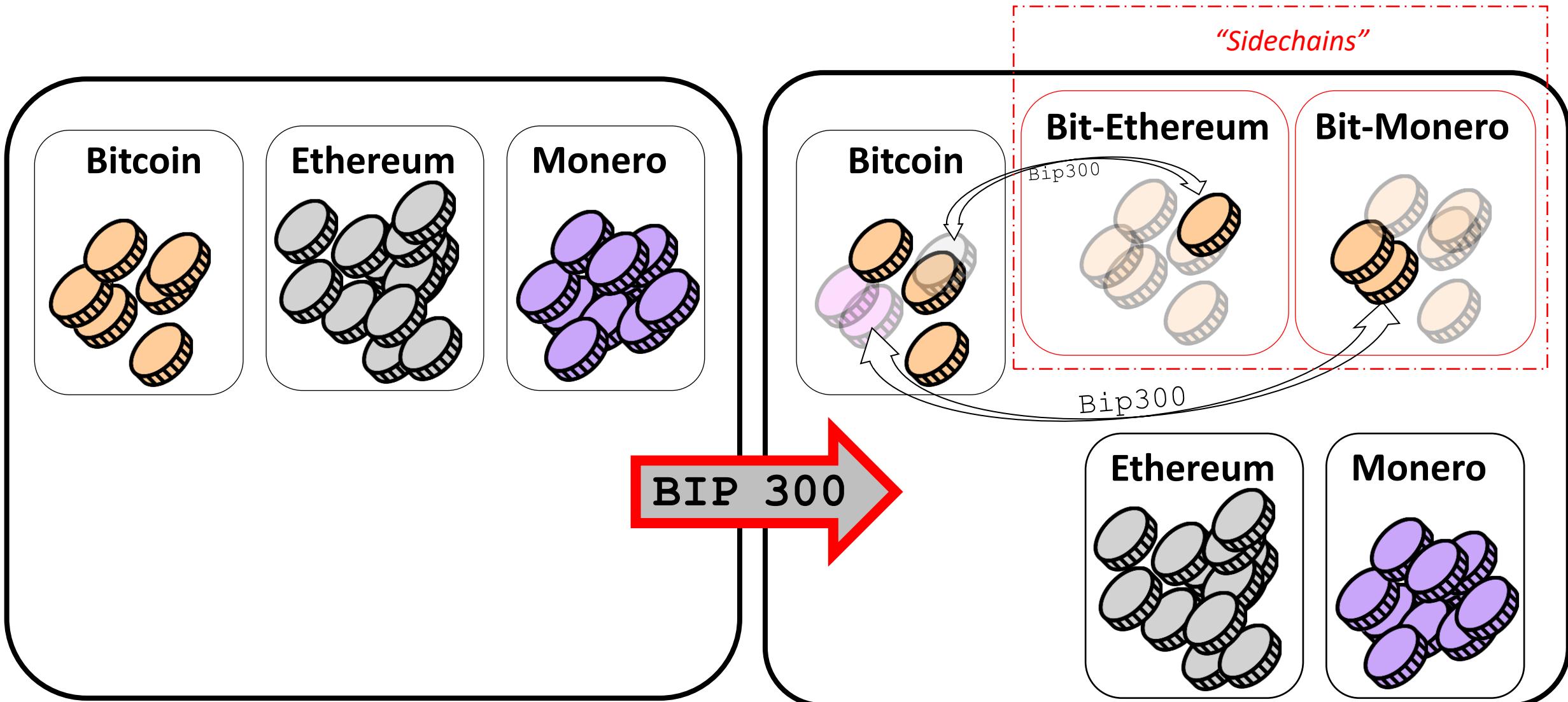




BTC
Today



Drivechain = Altcoin Tech, BTC Coin Only



1.1) The Basic Sidechain Concept



20 years later and
all of these things
fit in your pocket.



Expert Validation

see LayerTwoLabs.com/friends for links, context, & *43 more*

Fiatjaf

creator of Nostr

"Drivechains solve many different problems"

"Drivechain is our only hope."

"...I support Drivechain..."

Anton Kumaigorodski

inventor of hosted channels and creator of the Simple Bitcoin Wallet, the Bitcoin Lightning Wallet, the Lightning Network Wallet, and the Scala IMMORTAN library

"I fully support Drivechain because I want Hivemind since about 2018 when I first heard about them. In 2023 I want to add the following: neither hard-fork (obviously) nor a series of half-assed soft-forks will do. Soft-forks are not free, they add complexity to software code in nothing else. Throw 2-3 more soft-forks of Segwit scale and no one could be bothered figuring out what is going on there. We need one more soft-fork to end all soft-forks which is Drivechain. Another option is change nothing at all but it is a fragile solution which leaves BTC vulnerable to unknown future challenges and does not seem like an attractive investment offer to me."

Super Testnet

freelance software developer specializing in Bitcoin, Lightning, and Nostr

"I support drivechain (bip300 and bip301)"

CalleBTC

creator of Cashu

"I support BIP-300."

"I optimistically support Drivechains and haven't changed my mind about it. I believe it's the easiest way to give Bitcoin "infinite abilities" and it fits my vision of Bitcoin as the base layer of everything else. I'll ignore it from now on until there is code ready for review."

Adam Back

Co-Founder and CEO of Blockstream, inventor of Hashcash

"props to @Truthcoin and team for implementing and validating drivechain design."

"Drivechains...are pretty cool...and arguably could have been more important or useful than let's say Taproot."

"i think we're gonna need a big p2p sidechain for the next billion users to benefit from unseizable, censor-resistant #bitcoin. opcodes to support p2p sidechains like drivechain @LayerTwoLabs, p2p @liquid, @rootstock_io rootstock."

Robin Linus

Co-Founder ZeroSync, inventor of BitVM and BitStream

"The brain drain is real though. I know dozens of bright researchers and engineers who left the bitcoin community because it takes more than a decade of pointless drama to activate even the most simple updates like covenants. We should activate BIP300 and then ossify the baselayer"

Bruce Fenton

CEO of Chainstone Labs, Host of the Satoshi Roundtable, and GOP Senate Candidate

"BIP 300 🚀⚡👍"

Edan Yago

Cheerleader-In-Chief at Sovryn

"The only thing missing from Bitcoin is that ability to adopt any feature or technology without changing main chain. BIP 300 fixes this."

Guy Swann

Host of the Bitcoin Audible podcast

"I feel like sidechains are an inevitable part of the ecosystem for multiple reasons, & I simply see BIP300 as a hashrate based sidechain rather than a federated multisig. I 100% agree on the alts issue, but that's not why i am interested in it."

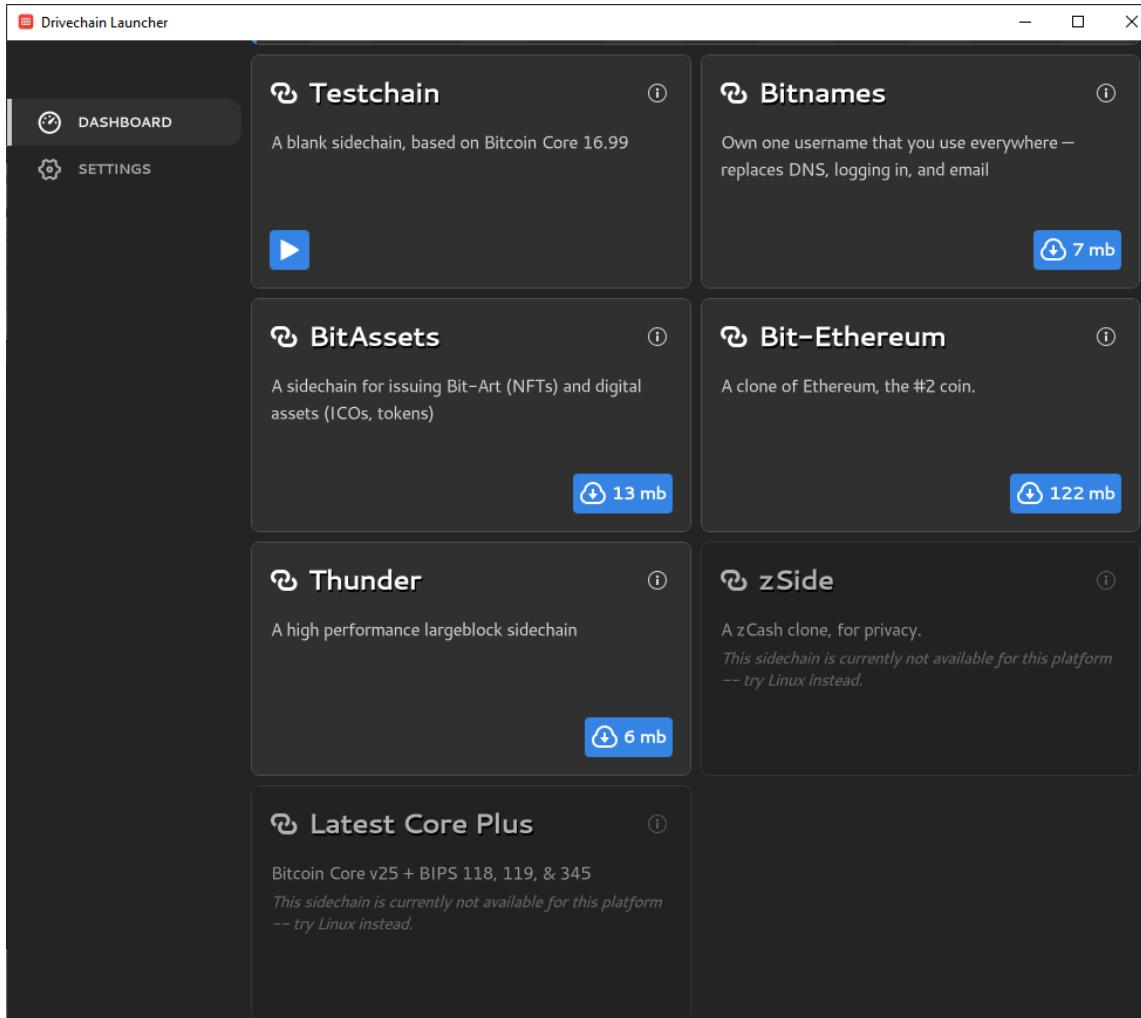
Jameson Lopp

Co-Founder and Chief Technology Officer at Casa

"I'm generally in favor of finally fulfilling the promise of 2-way pegged sidechains. I've yet to see a convincing concern of how it could be dangerous to the main chain. Some folks have said it could be dangerous if a sidechain became more valuable than the base chain, but seems to me that would be a signal that perhaps the base chain should implement that sidechain's features."

Try Our Software

Visit releases.drivechain.info -- it's always improving!



The Drivechain software interface shows a deposit screen for the Testchain sidechain:

- Overview**: Shows 12.0000,0000 BTC available for deposit.
- Send**: Send BTC to another address.
- Receive**: Receive BTC from another address.
- Transactions**: View recent transactions.
- Sidechains**: Manage deposits to other sidechains.

Make Deposits section:

- Address: s0_S55rbAish7NevXYbBP7WxsE196JWP5nwRy_c8cae6
- Deposit: 7.0000,0000 BTC
- Fee: 0.0001,3000 BTC
- Deposit button: Deposit

Your Recent Deposits:

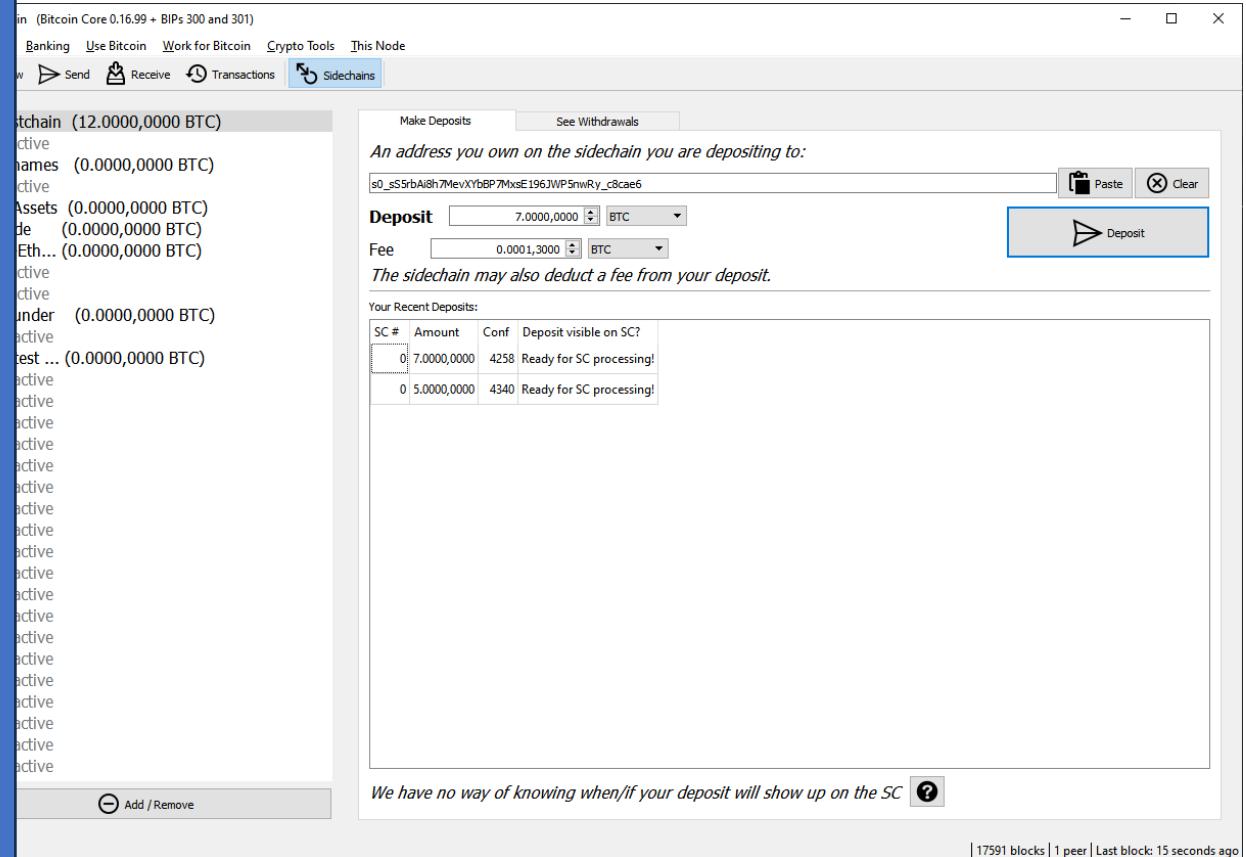
SC #	Amount	Conf	Deposit visible on SC?
0	7.0000,0000	4258	Ready for SC processing!
0	5.0000,0000	4340	Ready for SC processing!

We have no way of knowing when/if your deposit will show up on the SC

Try Our Software

- Bit-zCash
- Bit-Ethereum
- Largeblock payments sidechain
- BitNames (version of Namecoin)
- BitAssets (version of ordinals/NFTs/XCP)
- Blank sidechain for testing
- Bit-Core + CTV / APP / OP Vault activated
- Bit-Solana (work in progress)
- Bit-FileCoin (work in progress)
- Bit-Truthcoin (aka Bitcoin Hivemind, WIP)

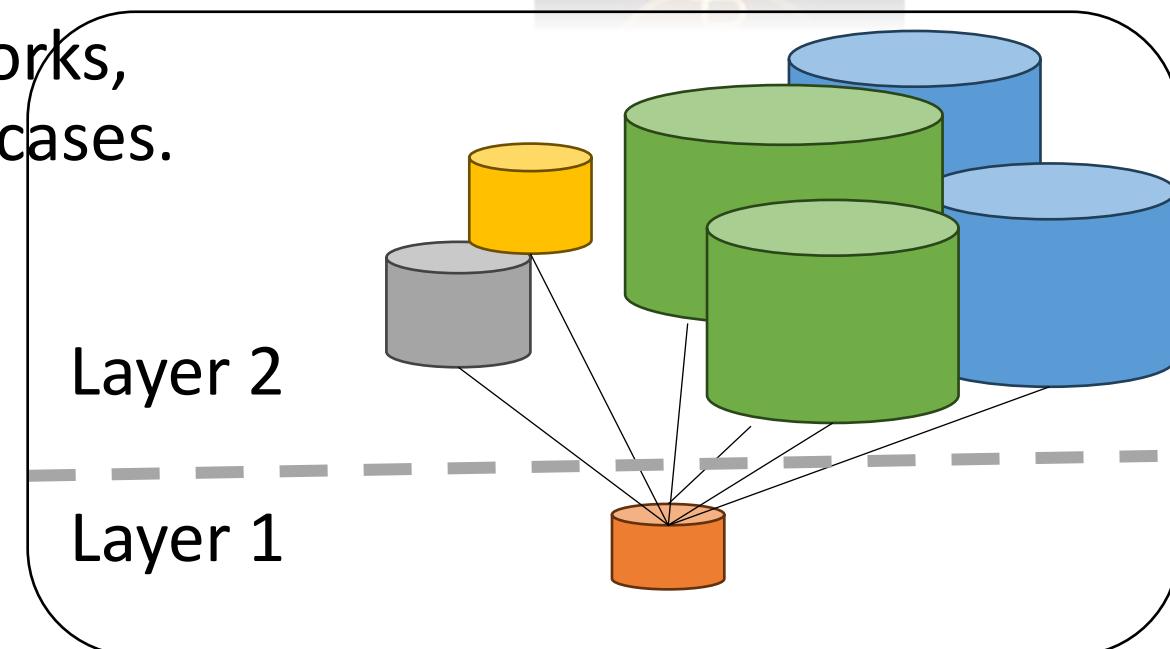
fo -- it's always improving!



Sidechains – Miner Perspective



- 1) Every transaction, in the world, is a Bitcoin txn, and each contributes to miner-revenues.
- 2) There are many different Bitcoin Networks, to accommodate different people /usecases.
- 3) Competition among networks/devs, ie – they all hate each other.



All the world's txns are already on some network or another.
They all pay some kind of fee to someone. (VISA, Venmo)

Goals of BIP 300/301

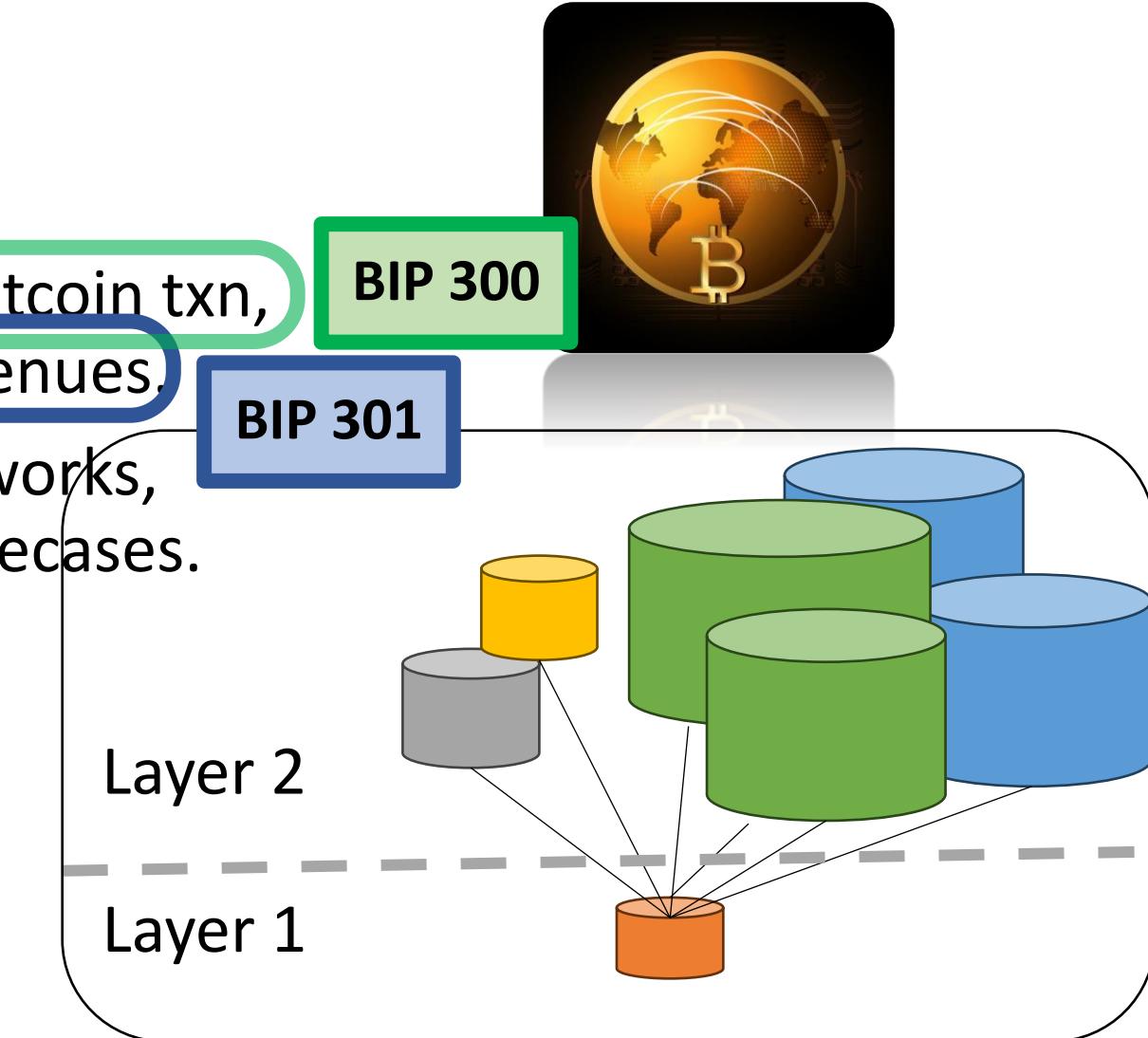
- 1) Every transaction, in the world, is a Bitcoin txn,
and each contributes to miner-revenues.

BIP 300

BIP 301

- 2) There are many different Bitcoin Networks,
to accommodate different people /usecases.

- 3) Competition among networks/devs,
ie – they all hate each other.



All the world's txns are already on some network or another.
They all pay some kind of fee to someone. (VISA, Venmo)

The Goal

Crypto Fees

There's tons of crypto projects.

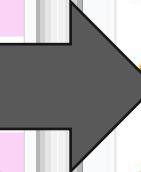
Which ones are people actually paying to use?

Share Bundle Filters Yesterday

Name	▼ 1 Day Fees	7 Day Avg. Fees
♦ Ethereum	\$8,795,834.82	\$9,711,635.45 ▼
Bitcoin	\$5,168,923.49	\$5,201,946.75 ▼
🦄 Uniswap	\$1,687,967.90	\$2,030,906.67 ▼
BNB Smart Chain	\$370,845.41	\$397,688.93 ▼
Aave	\$259,709.22	\$237,702.49 ▼
GMX	\$208,979.03	\$897,156.72 ▼
Arbitrum One	\$205,965.44	\$243,570.22 ▼
MakerDAO	\$203,306.44	\$196,858.37 ▼
Synthetix	\$137,334.86	\$152,790.36 ▼

Share Bundle Filters Yesterday

Name	▼ 1 Day Fees	7 Day Avg. Fees
Bitcoin	\$8,795,834.82	\$9,711,635.45 ▼
Bitcoin	\$17,000,000	\$5,201,946.75 ▼
Bitcoin	\$1,687,967.90	\$2,030,906.67 ▼
Bitcoin	\$370,845.41	\$397,688.93 ▼
Bitcoin	\$259,709.22	\$237,702.49 ▼
Bitcoin	\$208,979.03	\$897,156.72 ▼
Bitcoin	\$205,965.44	\$243,570.22 ▼
Bitcoin	\$203,306.44	\$196,858.37 ▼
Bitcoin	\$137,334.86	\$152,790.36 ▼



The Goal

Crypto Fees

There's tons of crypto projects.

Which ones are people actually paying to use?

Share Bundle Filters Yesterday

Name	▼ 1 Day Fees	7 Day Avg. Fees
Ethereum	300	
Bitcoin	\$5,168,923.49	\$5,201,946.75 ▾
Uniswap	\$1,687,967.90	\$2,030,906.67 ▾
BNB Smart Chain	\$370,845.41	\$397,688.93 ▾
Aave	\$259,709.22	\$237,702.49 ▾
GMX	300	
Arbitrum One	\$205,965.44	\$243,570.22 ▾
MakerDAO	\$203,306.44	\$196,858.37 ▾
Synthetix	\$137,334.86	\$152,790.36 ▾

Name	▼ 1 Day Fees	7 Day Avg. Fees
Bit-Ethereum	\$8,795,834.82	\$9,711,654.55 ▾
Bitcoin	301	\$17,000,000 ▾
Bit-GMX	\$1,687,967.90	\$2,030,906.67 ▾
Bit-BNC	\$370,845.41	\$397,688.93 ▾
Bit-Aave	\$259,709.22	\$237,702.49 ▾
Bit-Arbitrum	\$208,979.03	\$243,570.22 ▾
Bit-MakerDAO	\$205,965.44	\$196,858.37 ▾
Bit-Synthetix	\$203,306.44	\$152,790.36 ▾
Bitcoin	\$137,334.86	\$152,790.36 ▾

Not limited to Existing Altcoins

- Can include other networks, including centralized ones.
- Or new blockchain networks we build from scratch.
- Earth's 1.1 trillion txns
 - At \$0.10 = \$100B per year in revenue. From payments alone.
 - Doubles roughly every ~ 5 years.
- Chase revenues, instead of cutting costs.
- More users = more Bitcoin adoption = higher price.

Not limited to Existing Altcoins

- Can include other networks, including centralized ones.
 - Or new blockchain networks we build from scratch.
 - Earth's 1.1 trillion txns
 - At \$0.10 = \$100B per year in revenue. From payments alone.
 - Doubles roughly every ~ 5 years.
 - Chase revenues, instead of cutting costs.
 - More users = more Bitcoin adoption = higher price.
-
- **Important because:** BIP 300/301 can be activated by 51% hashrate alone ... without any change to the Bitcoin Core software.

Final Thoughts -- Why BIP300 Guarantees Success

- 1) Commanding Heights – Capture these, and the rival currencies will surrender.
- 2) Batting Cleanup – Fundamental Value, “Mining Decentralization”, Anti-Scam, Security Budget, Small blocks, Creativity
- 3) Culture – Why static cultures always fail, how to combine progress with stability.

1) The Commanding Heights

- Capture these 3 dimensions, and you have an insurmountable advantage:
 - **Scalability** – money has network effects. So whoever can't scale, is at a permanent, fatal disadvantage. Bip300 allows a team of larger-block sidechains to reach planetary scale immediately, giving 8 billion people their own UTXO. See:
<https://www.truthcoin.info/blog/thunder/>
 - **Privacy** – It is difficult to openly innovate privacy – at least, privacy of the truly subversive kind that matters. That is why it is best to just copy the already existing zCash sidechain. This was *already done*, back in 2020. Try it!
 - **Ossification** – It is difficult to “compete on ossification”. Whoever has gone the longest without changing, is the most ossified, no matter what the rivals do later. So, this advantage goes to whoever can ossify first. Bip300 allows us to ossify immediately – no L1 changes are ever needed ever again. Instead, they take place on L2 where they belong.

2) Batting Cleanup

- BIP300 also solves these problems (as a kind of side-effect):
 - **Security Budget** – Miners automatically collect *all txn fees from all chains*, without doing any additional work. Last year ~1.1 trillion txns on Earth, @ \$0.10/tx = **\$100B** per year in miner revenue. (And this figure doubles every ~5 years.)
 - **Fundamental Value** – BIP300 focuses on fees – aka building chains that people use. See: truthcoin.info/blog/bitnames/ + truthcoin.info/blog/bit-assets/ + bitcoinhivemind.com/ This drives *real* adoption – loyal users, not speculators.
 - **Mining Decentralization** – Reduce the bargaining power of pools! The best way, is to support: (1) inter-pool competition, (2) PPS/FPPS, (3) frequent on-chain pool2hasher payments. Thunder (one of our sidechains) facilitates this already. We are building optimized open source pool software, to further this use-case and set a good example.
 - **Anti-Scam** – Scams plague our industry. Bad PR and regulatory headaches. After Bip300, all innovation will be absorbed into the winning coin, not compete with it. This removes the justification for creating new coins – which is the basis of the scams.

3) Culture as Suicide

- “[Easter Islanders] may have arrived on the island as early as the fifth century CE. They developed a complex Stone Age civilization, which suddenly collapsed over a millennium later. By some accounts there was starvation, war and perhaps cannibalism. The population fell to a small fraction of what it had been, and their culture was lost.

The prevailing theory is that the Easter Islanders brought disaster upon themselves, in part by chopping down the forest which had originally covered most of the island. They eliminated the most useful species of tree altogether.

...
Of the hundreds of statues on the island, built over the course of several centuries, fewer than half are at their intended destinations. The rest, including the largest, are in various stages of completion, with as many as 10% already in transit on specially built roads. Again there are conflicting explanations, but, according to the prevailing theory, it is because there was a large increase in the rate of statue-building just before it stopped for ever. In other words, as disaster loomed, the islanders diverted ever more effort not into addressing the problem – for they did not know how to do that – but into making ever more and bigger (but very rarely better) monuments to their ancestors. And what were those roads made of? Trees.”

-David Deutsch, *The Beginning of Infinity*

vs.

- Bip300 *fosters* L1 openness to change, & innovation. But this change is opt-in and reversible. Thus, Bip300 also fosters ossification.



See Appendix 3

How You Can Help

- Learn and spread the word
 - Join the Telegram – t.me/DclInsiders
 - Try the software – releases.drivechain.info
 - Read the BIPs / read drivechain.info, to absorb the ideas
 - Follow me, @truthcoin on Twitter
- Specifically, we eventually need either:
 - Bitcoin to take this idea
 - Core to merge the Bip300 pull request (will take years), OR
 - 51% BTC hashrate to run the Bip300 software (MASF)
 - An Altcoin / Fork must take this idea



Thank You For Your Attention

Fundamental Value – Namecoin

Satoshi co-invents Namecoin in 2010

- Namecoin Enables: Why does today's internet suck so much??

- One Username – Own a single username, that works everywhere, on every site.
- No more passwords! -- Login by being “pinged” with PIN via open protocol.
- Easy to keep different online identities separate.
- “PayMail” – Special inbox where people must pay you \$ in order for the message to go through.
 - PayMail for introductions + Whitelists = eliminates all spam from the internet. This breaks the chokehold of Google.
 - On-chain PayMail is completely, 100% untraceable if you run a full node. No TOR required.
- Everyone has end-to-end encryption. Everyone has a TOR / i2p website.
- No seizing of ICANN domain names.
- (Through Bip47 / similar), eliminates the need for Bitcoin addresses.

Screenshot #1 from
[www.truthcoin.info/
blog/bitnames/](http://www.truthcoin.info/blog/bitnames/)



Elon Musk @elionsmusks · 4h
Replies to [@EmZIp1dp7EGKf3A](#) @elonmusk
Amazing emoji. I'm in the mood for a giveaway.
Just send me from 0.6 to 5 ETH and get 6 to 50 ETH.
Address goo.gl/wo9eH5

11 97 845

Jack @jackforth1984 · 4h
works perfect. i have 6 Ether now, but i want more.

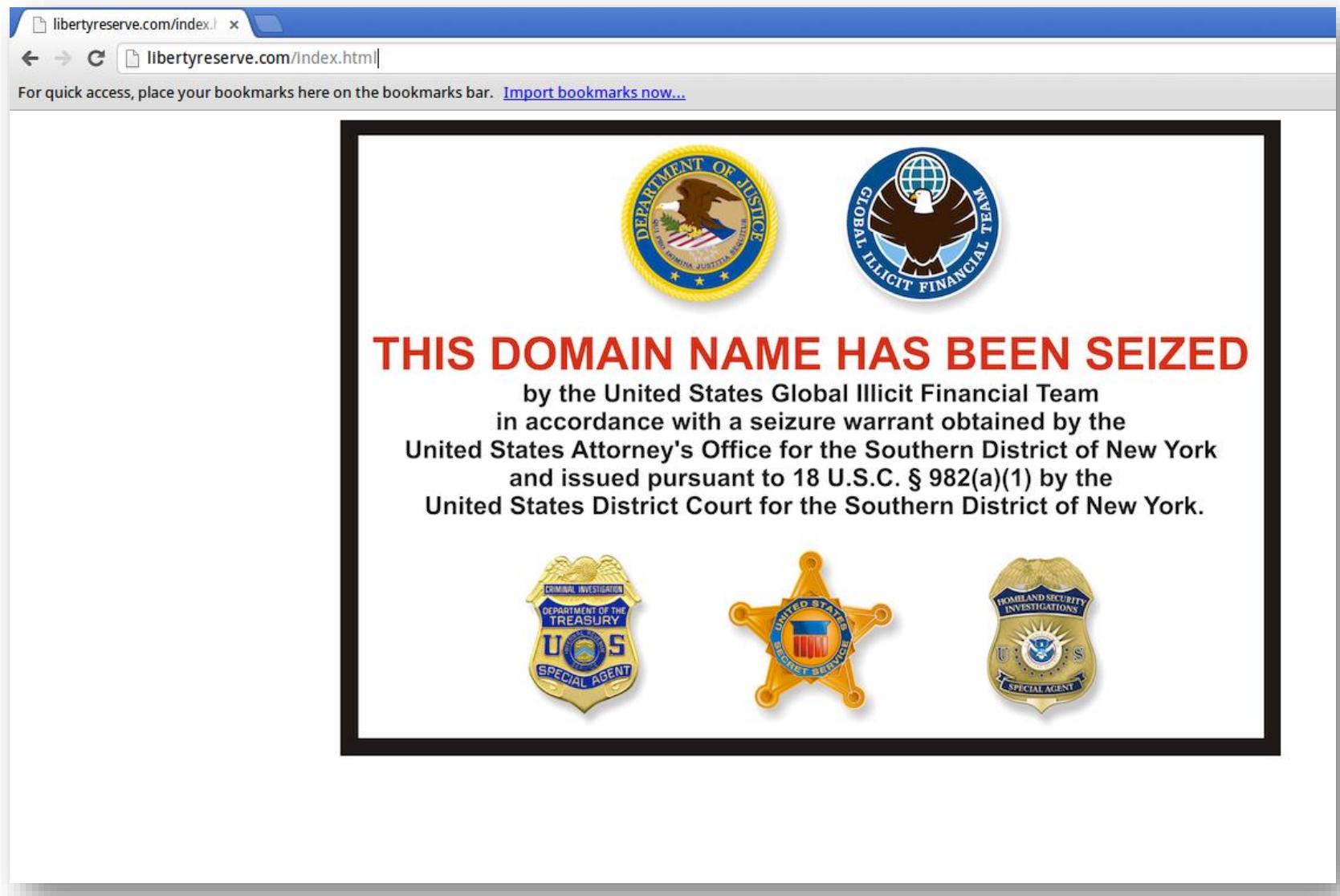
1 100 638

bay @bayta1982 · 4h
Initially I thought "maybe not", but then tried it and - woot - it works. gj

2 100 633

Screenshot #2 from

[www.truthcoin.info/
blog/bitnames/](http://www.truthcoin.info/blog/bitnames/)



Screenshot #3 from

[www.truthcoin.info/
blog/bitnames/](http://www.truthcoin.info/blog/bitnames/)

Info corner

"If you think less of yourself after doing it... don't do it again."

The Stoic Emperor

John Owen

Paul Charles Morphy

Use #suggestion when suggesting a game for me to analyze. Thank you :)

How to Support the channel?
Donation link is in the description

Kaveh Allahmadi \$20.00
Tim Tully \$20.00
Jeffrey Turner \$25.00
Kevin Clark \$25.00
Austin Breidenthal \$25.00

Top: Mystery \$9.590.26 (1BTC)
Nathan Baker \$5.000.00
Scott McKay \$2.750.00

Lichess:agadmator
Chess.com:agadmator
Twitter:agadmator
Instagram:agadmator
Facebook:agadmatoryoutube

#MorphySaga
BARNES Power! || Morphy vs Owen (1858)

Fundamental Value – Truthcoin

Paul (me) invents Truthcoin in 2013/14

- Truthcoin Enables:

Why does today's internet suck so much??

- Prediction Markets – prevents politicians/CEOs from lying.
 - Prevents politicians/CEOs from lying
 - Each voter/shareholder/whatever can become optimally informed, with zero effort.
 - Will counteract “rational ignorance” and Caplan-esque “rational irrationality”.
- Eliminates the entire “misinformation” pipeline / food chain. (Lobbyists, pollsters, etc).
- Thus, politicians will have to work as hard as possible.



Quis custodiet ipsos custodes? – “But who is in charge of those who are in charge?”

- Fork futures -- would have prevented the Blocksize war.
- Portfolio replication – allows for stablecoins/anything-coins... *no backer needed!*
- Paves the way for land-value-Futarchy / nirvana.

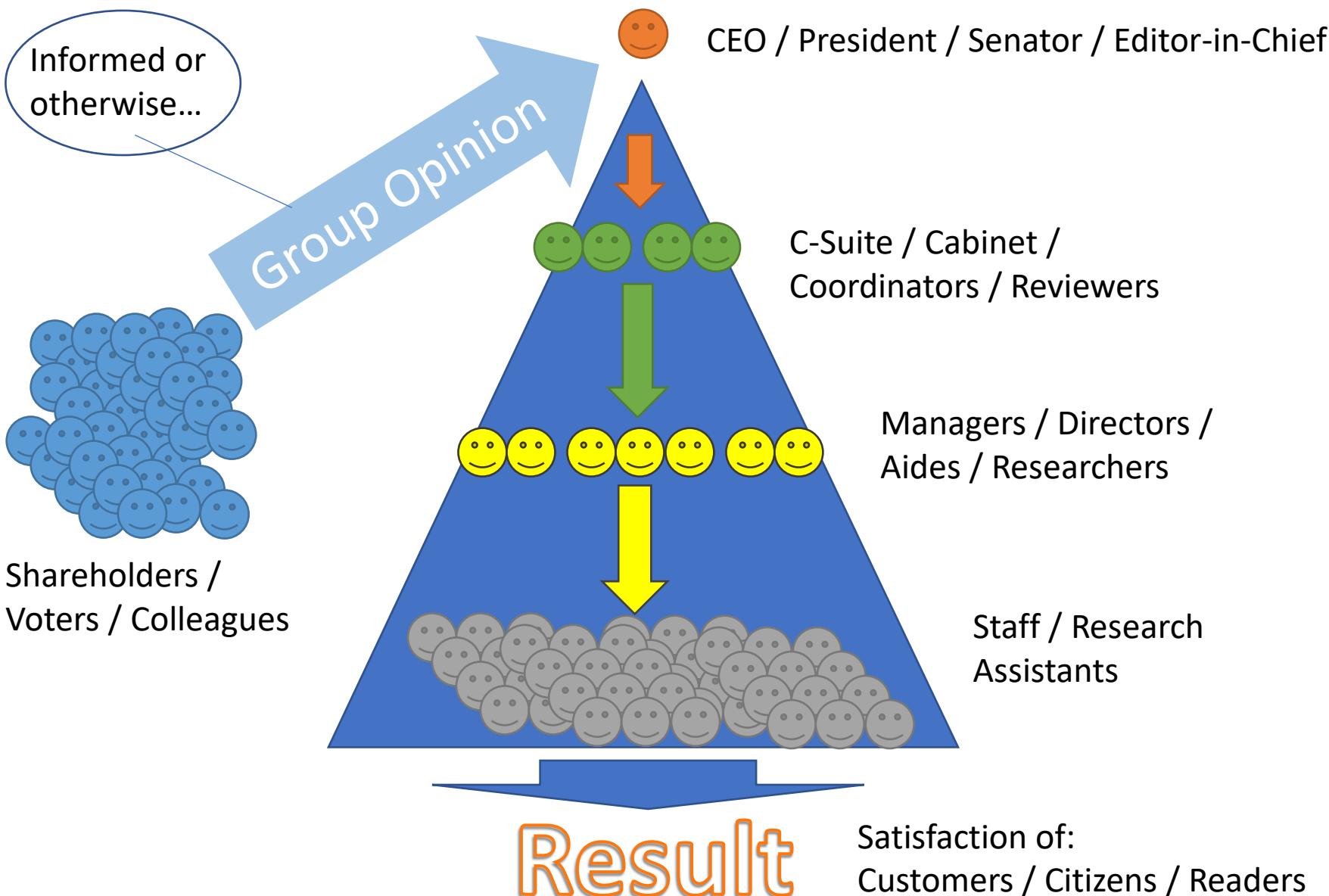
Telegram: t.me/DcInsiders

Website: www.LayerTwoLabs.com

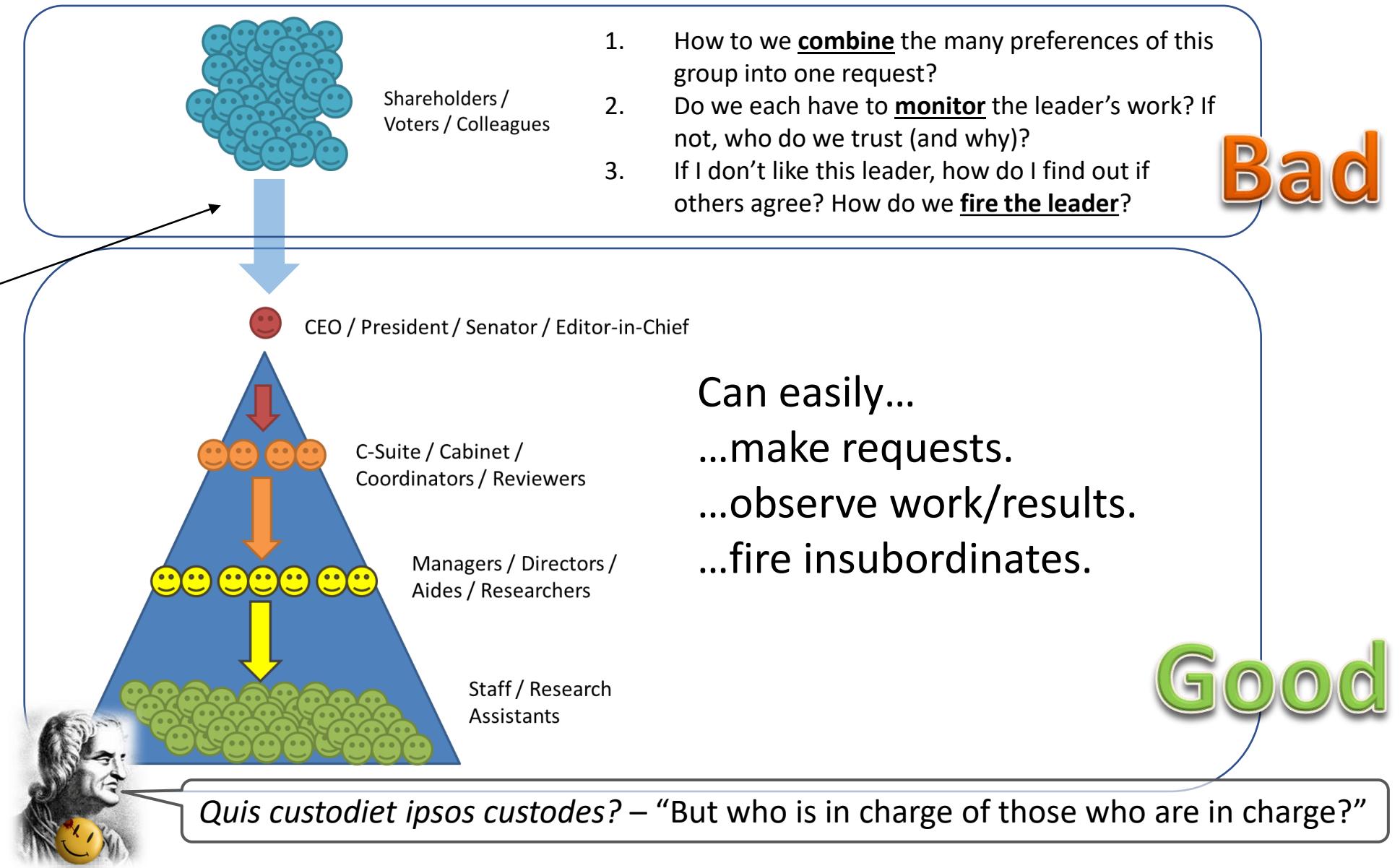
Paul's Twitter:

@truthcoin

Rot From Above: Who controls what?



Prediction
Markets fix
this.



Prediction Markets

- Screenshots from my own BTC sidechain project

Hivemind Core - Wallet [testnet]

This is a pre-release test build - use at your own risk - do not use for mining or merchant applications

Recent Hivemind Objects:

Type/Icon	Description
	Bitcoin exchange rate as reported by CoinDesk
	Will Jeff Immelt have been replaced, as CEO
	Global surface temperature anomaly, cumulative
	Will Barack Obama win US President in 2012?
	Unemployment drivers
	Fire Immelt?
	Unemployment drivers

Balances

Available:	400.00000000 BTC
Pending:	0.00000000 BTC
Immature:	50.00000000 BTC
Total:	450.00000000 BTC

Recent transactions

	5/17/16 11:41	[+50.00000000 BTC] (19y1RCwANn71vEZkxMrDoAjXuCzERyJE8A)
	5/17/16 11:41	+50.00000000 BTC (14u1sX6BTJnnTAL2dPDgm7WKKubofpwuEy)
	5/17/16 11:41	+50.00000000 BTC (1D6kbEHq7BXpjsVbuxLvt4CV4fv8poCk7)
	5/17/16 11:41	+50.00000000 BTC (1AADn8e5v7QM155C6Cc6Z8u82SZWDLH6cd)
	5/17/16 11:41	+50.00000000 BTC (16bfT93g3QY53xsEkK6UwnKyaa7FDBxsoc)
	5/17/16 11:40	+50.00000000 BTC (1NwRMJnpetsFHVCpzjeYo1s89StTi4HHDa)

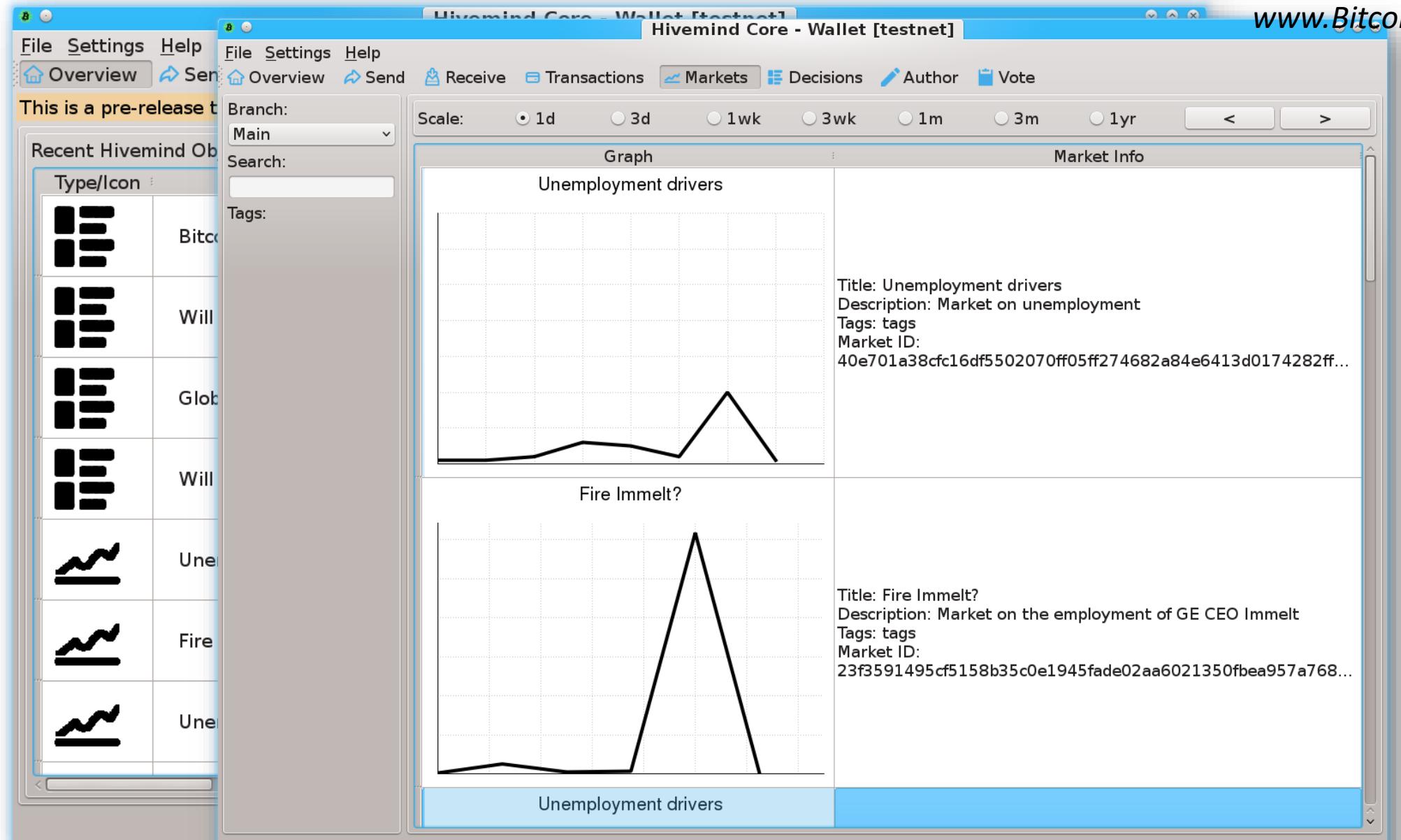
BTC ▲▼

www.BitcoinHivemind.com

Paul's Twitter:

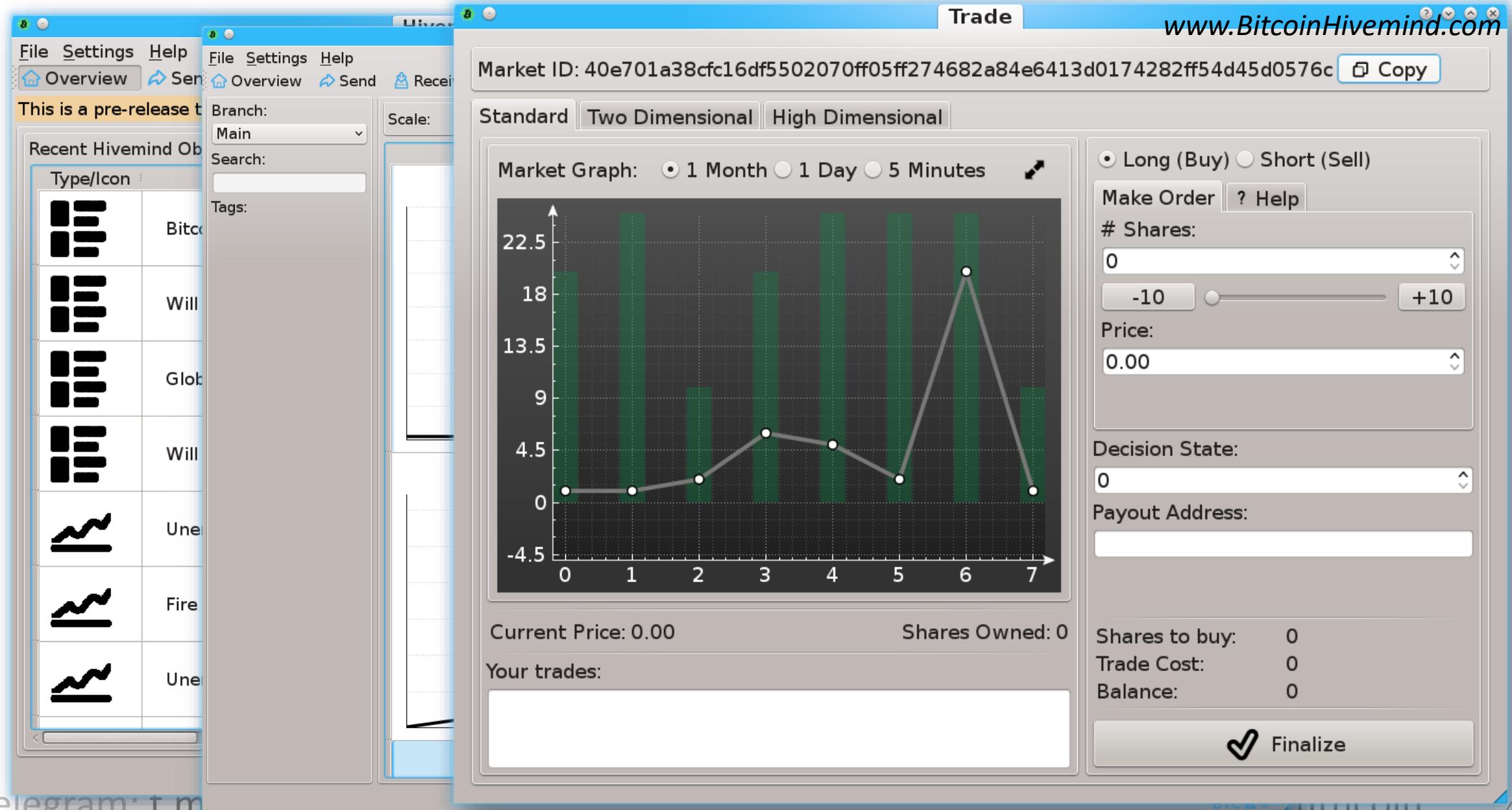
Prediction Markets

- Screenshots from my own BTC sidechain project



Prediction Markets

- Screenshots from my own BTC sidechain project



Prediction Markets

- Screenshots from my own BTC sidechain project

The screenshot shows a desktop application window titled "Trade" with the URL "www.BitcoinHivemind.com" at the top right. The window has two panes. The left pane is a "Hivemind Overview" window showing a table of recent objects. The right pane is a "Market Graph" window.

Market Graph Window:

- Market ID:** 40e701a38cf16df5502070ff05ff274682a84e6413d0174282ff54d45d0576c [Copy](#)
- Branch:** Main
- Scale:** Standard (selected), Two Dimensional, High Dimensional
- Market Graph:** Shows a line graph with vertical error bars. The x-axis ranges from 0 to 7, and the y-axis ranges from -4.5 to 22.5. The line starts at (0, ~1.5), dips to (1, ~1.5), rises to (2, ~2.5), dips to (3, ~4.5), rises to (4, ~4.5), dips to (5, ~2.5), rises sharply to (6, ~20), and ends at (7, ~1.5). A white dot is placed on the line at x=6.
- Time Period:** 1 Month (radio button selected), 1 Day, 5 Minutes
- Decision State:** 0
- Payout Address:** [Empty field]
- Shares to buy:** 0
- Trade Cost:** 0
- Balance:** 0
- Finalize** button

Left Pane (Hivemind Overview):

- Recent Hivemind Objects:**
- Type/Icon:** Bitcoin (with icon of a stack of coins)
- Will (with icon of a stack of coins):** Will, Will, Will
- Glob (with icon of a stack of coins):** Glob
- Une (with icon of a line graph):** Une

Bottom Left: Telegram: t.me/BitcoinHivemind

Bottom Right: 42

Text Overlay:

Key Idea: “Futarchy” -- futures markets for how well certain leaders would perform, if they were in charge.

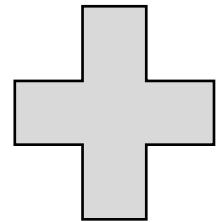
A Bold Claim

- BIP300 Solves All of Bitcoin's Biggest Problems
 - A. Heterogeneity Problem
 - B. Scalability
 - C. Privacy
 - D. Scams – Eliminating ScamCoins ; Domesticating the Token Casino
 - E. Security Budget
 - F. Decentralization
 - G. “Fundamental Value” of Bitcoin
- With...
 - H. ...zero risk to Bitcoin!

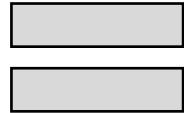
That “Zero Risk” Part

Bip300 is an easy soft fork to add to Bitcoin... And an easy soft fork to remove.

Bitcoin
Core v25



BIP 300
Softfork

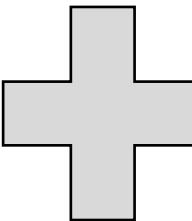


New Bitcoin
Core

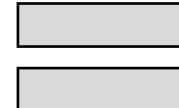
Interoperable
with Core v25

New Bitcoin
Core

Interoperable
with Core v25



A Softfork Banning all
Bip300
Deposits/Withdrawals
from L1



Bitcoin
Core v25

So, worst case scenario, miners just run a simple softfork,
and we are exactly back to where we are today.

Telegr

ter:

A Bold Claim

Different strokes for different folks.
Flexibility to grow and change as needed.

- BIP300 Solves All of Bitcoin's Biggest Problems

- A. Heterogeneity Problem Different chains for different users.
- B. Scalab A team of region-specific chains, each with a large growing Blocksize – onboard users directly to L2.
- C. Privacy zCash drivechain.
- D. Scams – Eliminating Have a dedicated NFT/ERC/Ordinals chain. Pay all txn fees in BTC. Clear coin roles.
- E. Security Budget Merged Mining = miners collect ALL fees from ALL chains. For free.
- F. Decentralization Shrink L1 Bitcoin Core Blocksize, and ossify (the spec at least). No more politics.
- G. “Fundamental Value” of Bitcoin Chains are actually useful for *real world tasks*.
- With...
 - H. ...zero risk to Bitcoin!

A. Heterogeneity



Smart Contracts
DeFi
Turing Completeness
Ring Signatures
zk-Snarks
Large Blocksizes
NFTs
Oracles
Mimblewimble
...(etc)

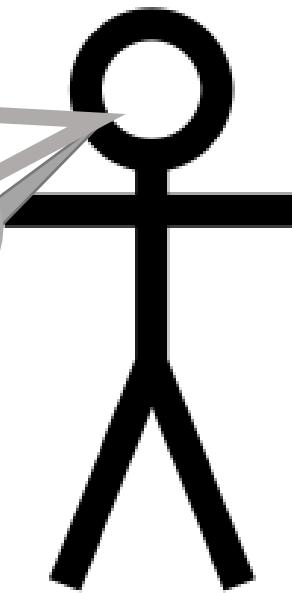
A. Heterogeneity



Noob (and/or
Fringe Genius)

I can improve Bitcoin! It only
needs my new idea: _____ !!
When can you merge my code ??

You can't just merge something into Bitcoin -- It
affects everyone else's nodes!! Besides, _____ has
been proposed before and you need to read
_____ so that you can learn why everyone hates
it, especially our infallible _____ who would have
done it by now if it were a good idea. _____ is
a SCAM and you are trying to ATTACK BITCOIN!!
Even if your idea was good it would probably take
years to get consensus and get merged into ...



Bitcoiner

Use BIP 300.
Good luck!!

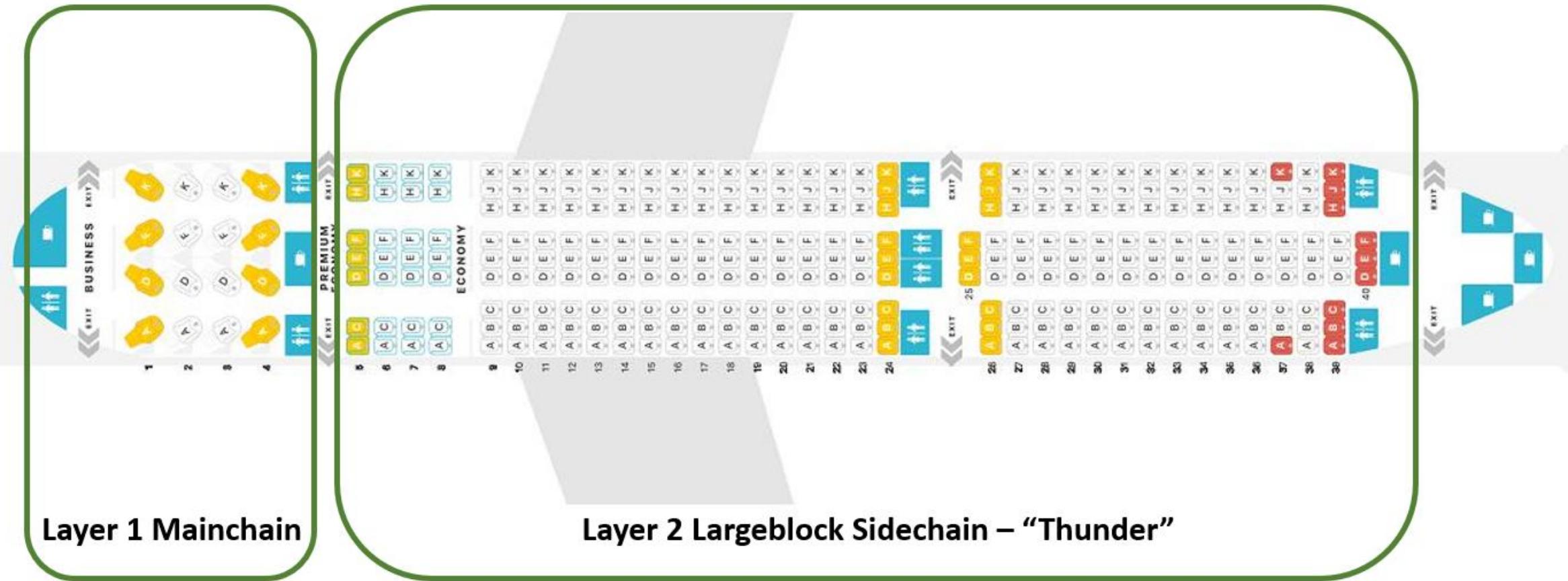
A Bold Claim

- BIP300 Solves All of Bitcoin's Biggest Problems

- A. Heterogeneity Problem Different chains for different users.
- B. Scalability A team of region-specific chains, each with a large growing Blocksize – onboard users directly to L2
- C. Privacy zCash drivechain.
- D. Scams – Eliminating Have a dedicated NFT/ERC/Ordinals chain. Pay all txn fees in BTC. Clear coin roles.
- E. Security Budget Merged Mining = miners collect ALL fees from ALL chains. For free.
- F. Decentralization Shrink L1 Bitcoin Core Blocksize, and ossify (the spec at least). No more politics.
- G. “Fundamental Value” of Bitcoin Chains are actually useful for *real world tasks*.
- With... BitNames + Truthcoin ; examples
- H. ...zero risk to Bitcoin!

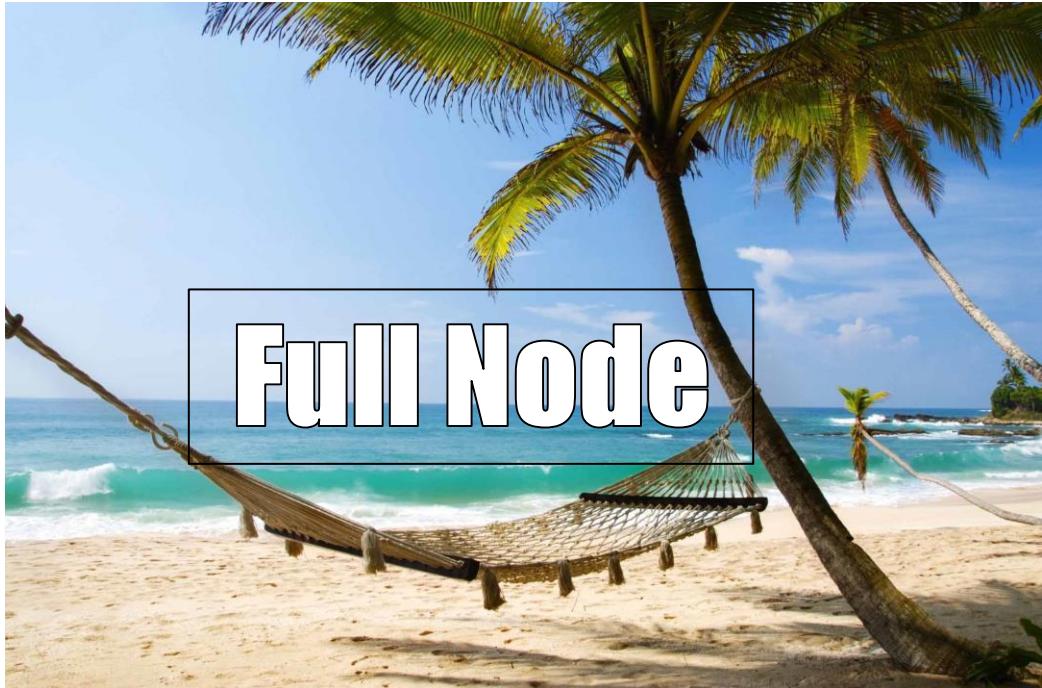
LargeBlocks?? What about Decentralization??

A Scalability Paradigm Shift



Remember: Heterogeneity! People are different!
“Coffee txn” does not need as much decentralization as other txns.
Bitcoin must compete, today, with Venmo.

5 Theory – Policing a [Chain] We Can't See



Full Node

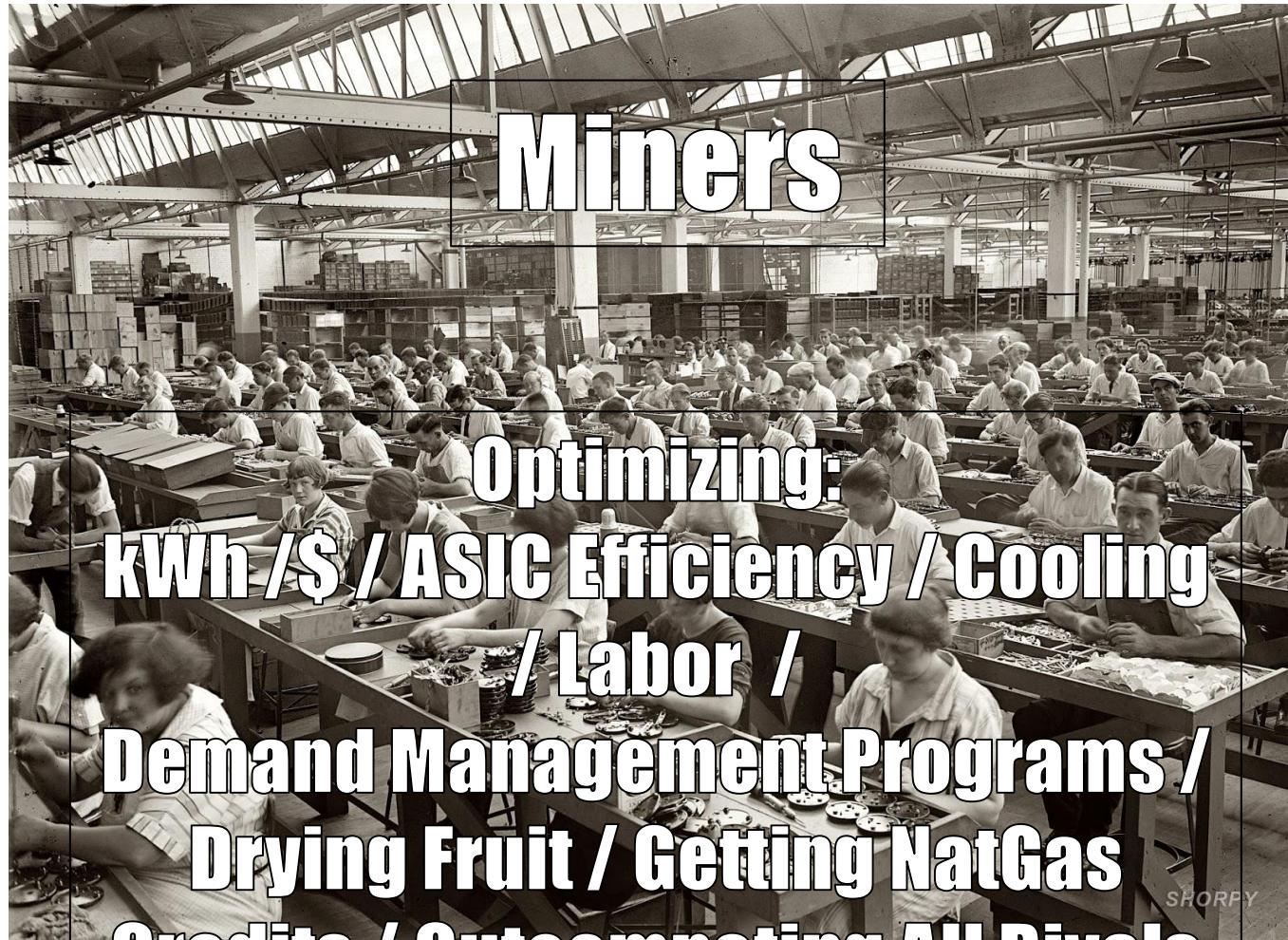
Validating L1

+ counting to 13,150

Telegram: t.me/Dclnsiders

Website: www.LayerTwoLabs.com

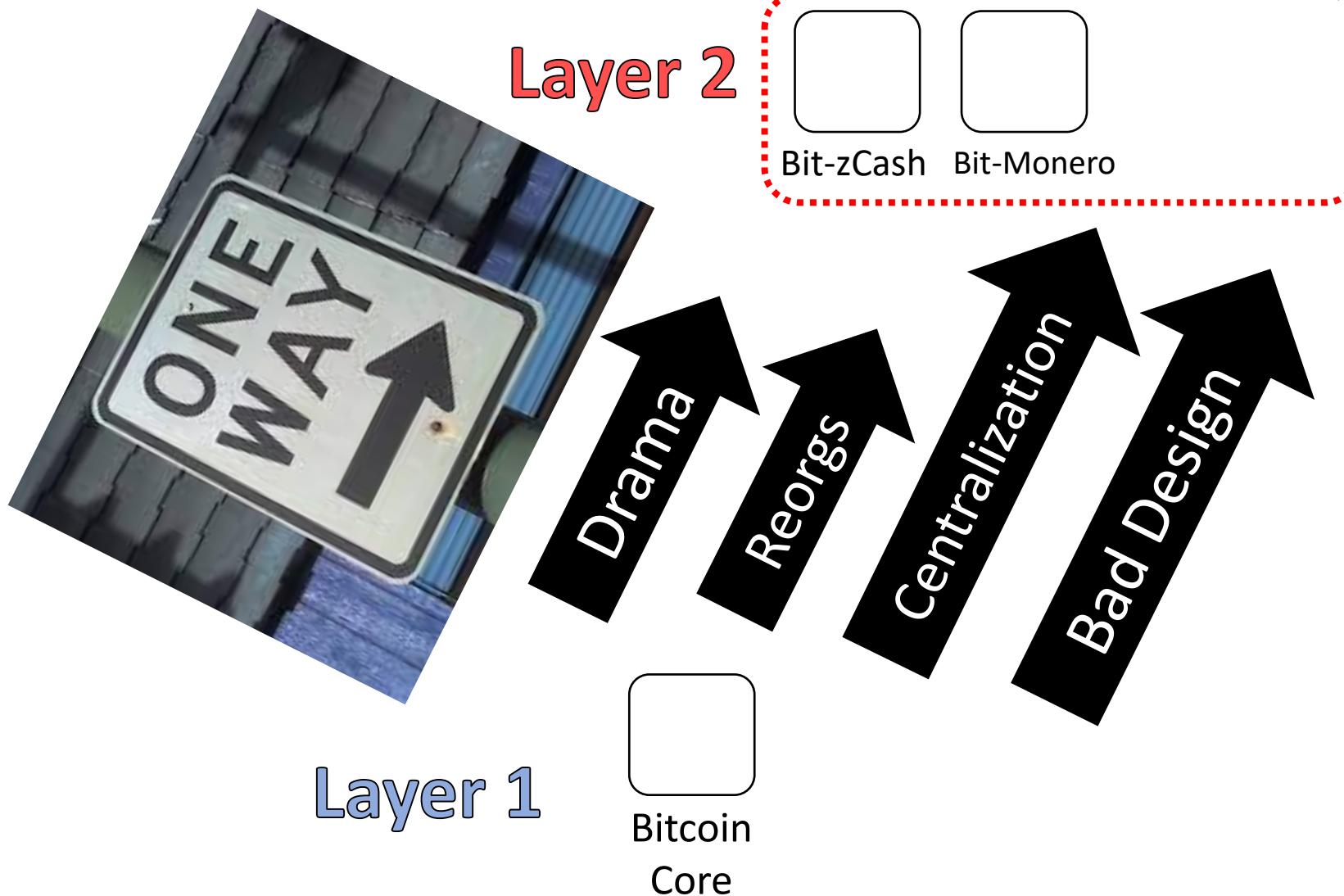
@truthtcoin



+ add/remove/validate Sidechains

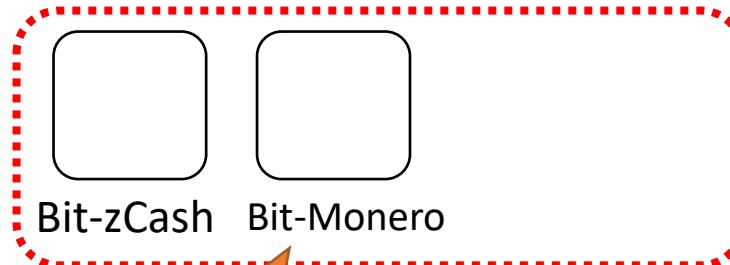
Paul's Twitter:

The “One Way Street”



Bip300
Drivechains
L2 node must
have access to
an L1 node

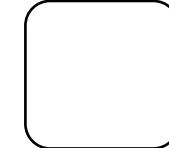
The “One Way Street”



Bip300
Drivechains

Layer 2

Layer 1

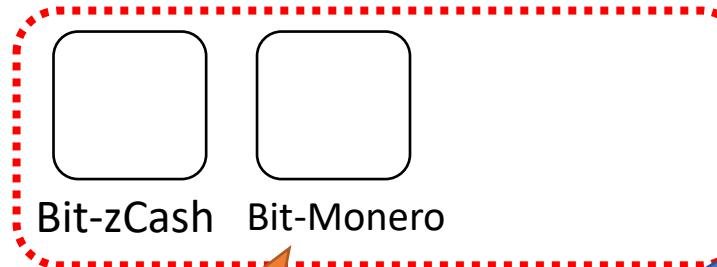


Bitcoin
Core

“I’m having a problem
with my ring signature---”



The “One Way Street”



Bip300
Drivechains



Layer 2

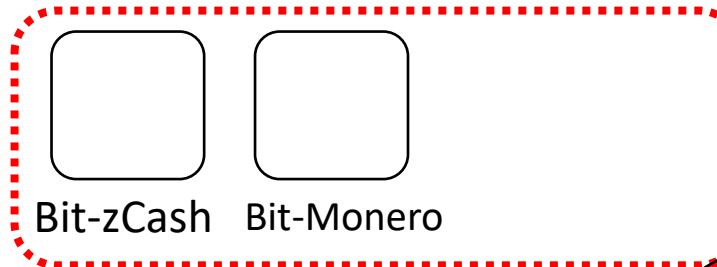
Layer 1

“I’m having a problem
with my ring signature---”

Can’t hear you,
sorry.



The “One Way Street”



Bit-zCash Bit-Monero



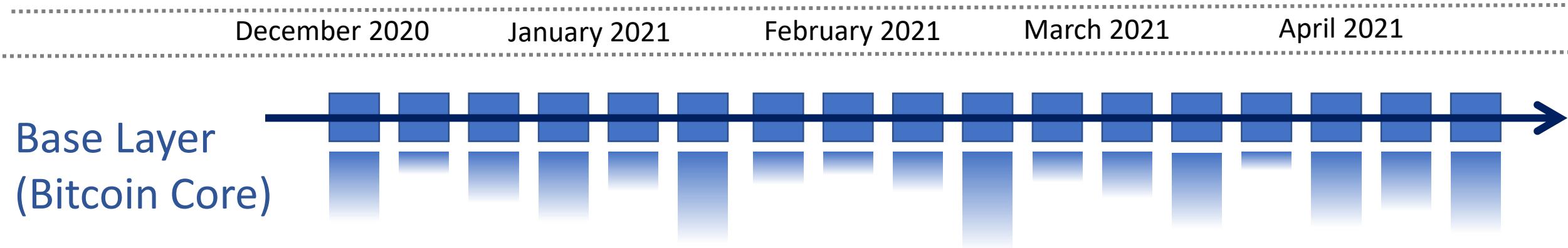
What's that??
Oh Sorry can't hear you.
Enjoying my music over
here.



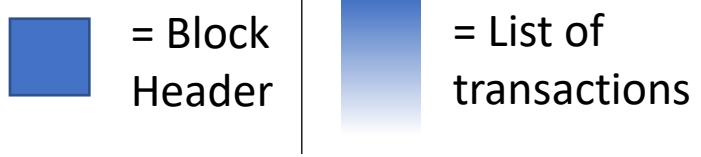
Bip300
Drivechains
Layer 2

ayer 1

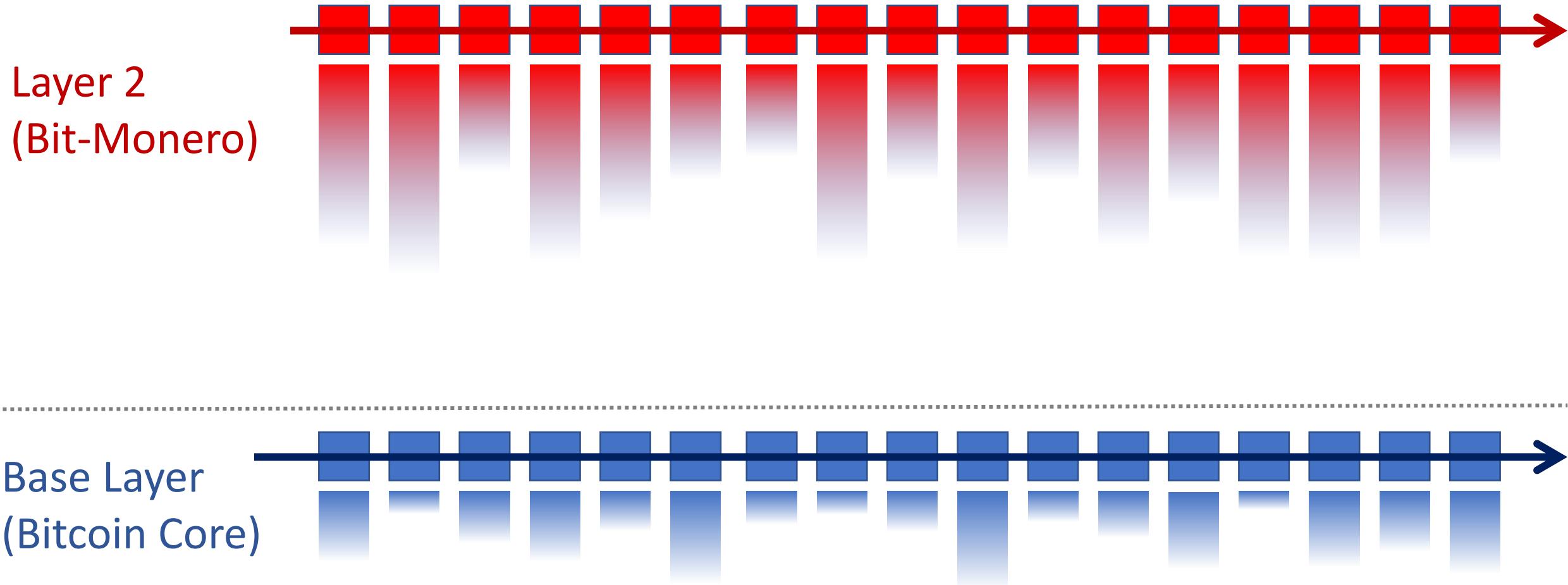
Putting Hash(L2) into L1



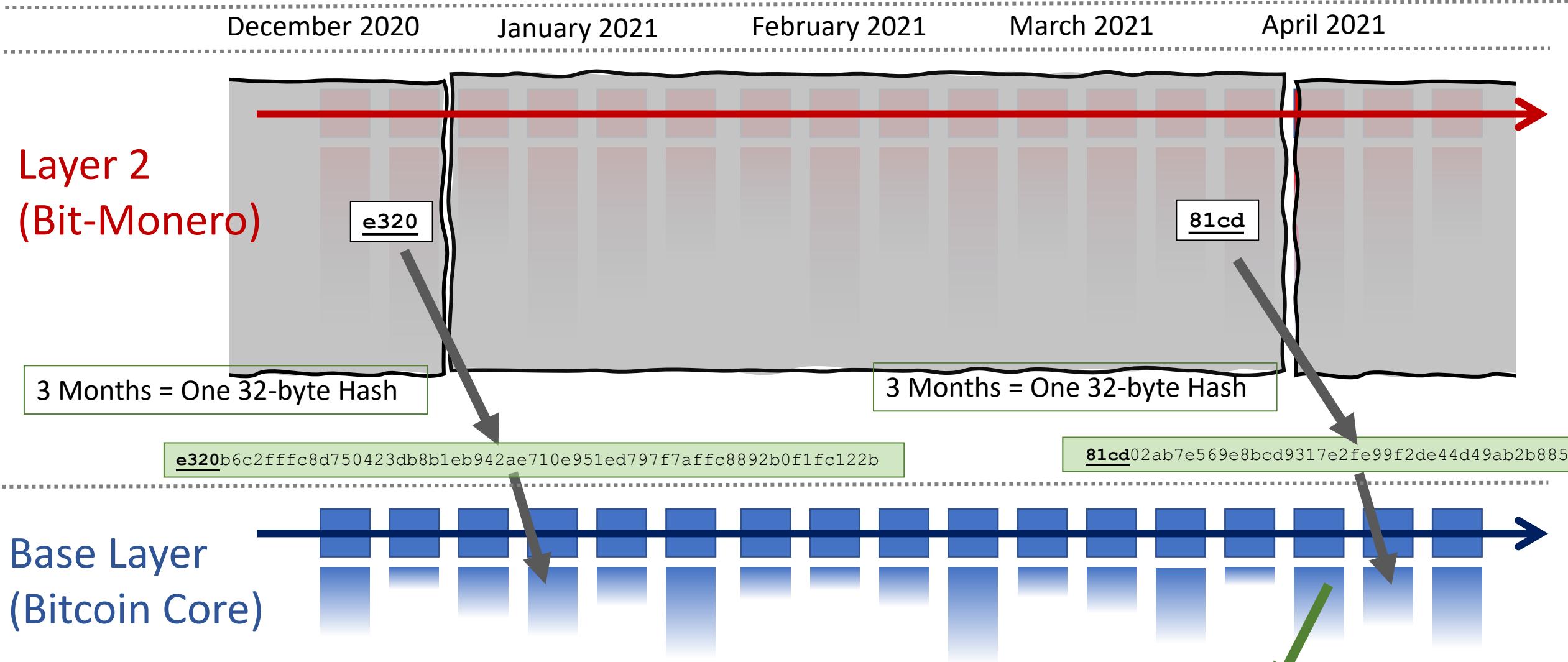
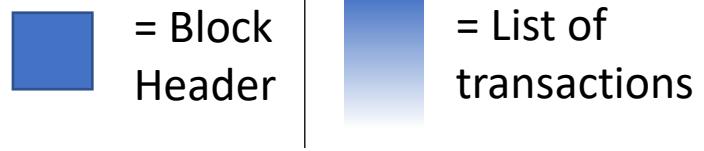
Putting Hash(L2) into L1



December 2020 January 2021 February 2021 March 2021 April 2021

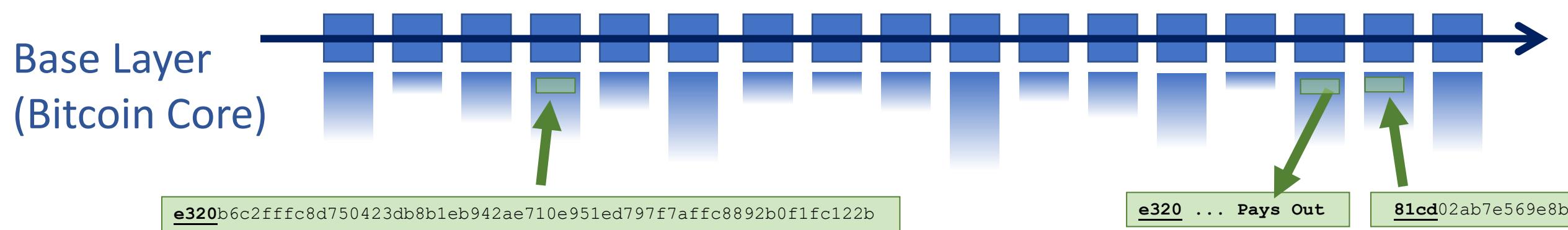


Putting Hash(L2) into L1



Putting Hash(L₂) into L₁

Your Layer 1 Node Sees...



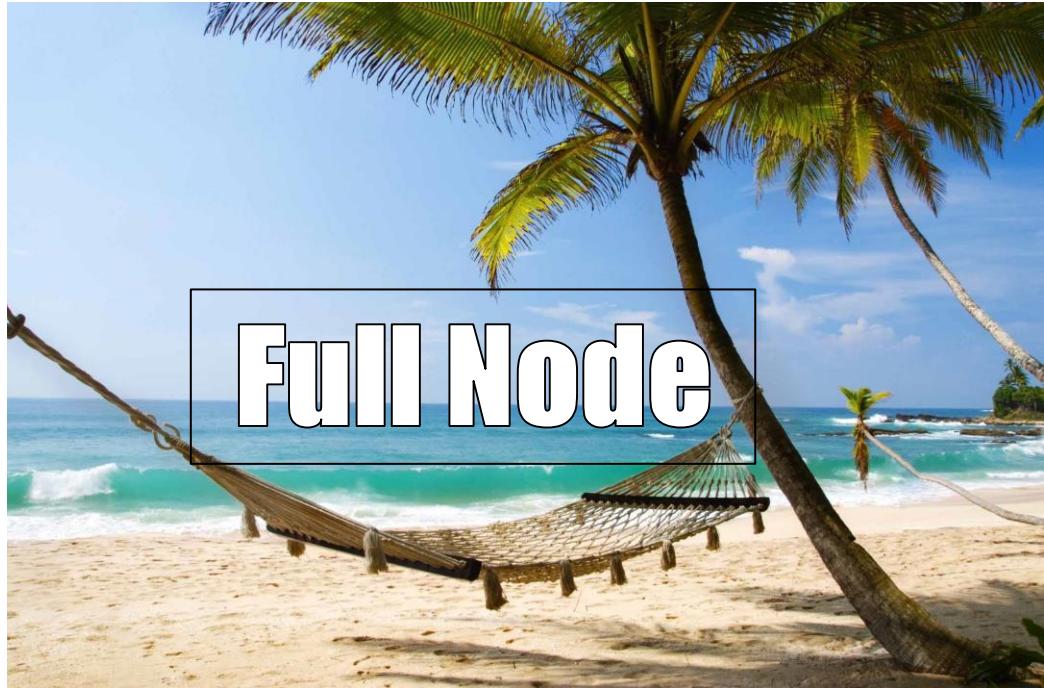
But then how is it secure??

Telegram: t.me/DcInsiders

Website: www.LayerTwoLabs.com

@truthtcoin

Paul's Twitter:



Full Node

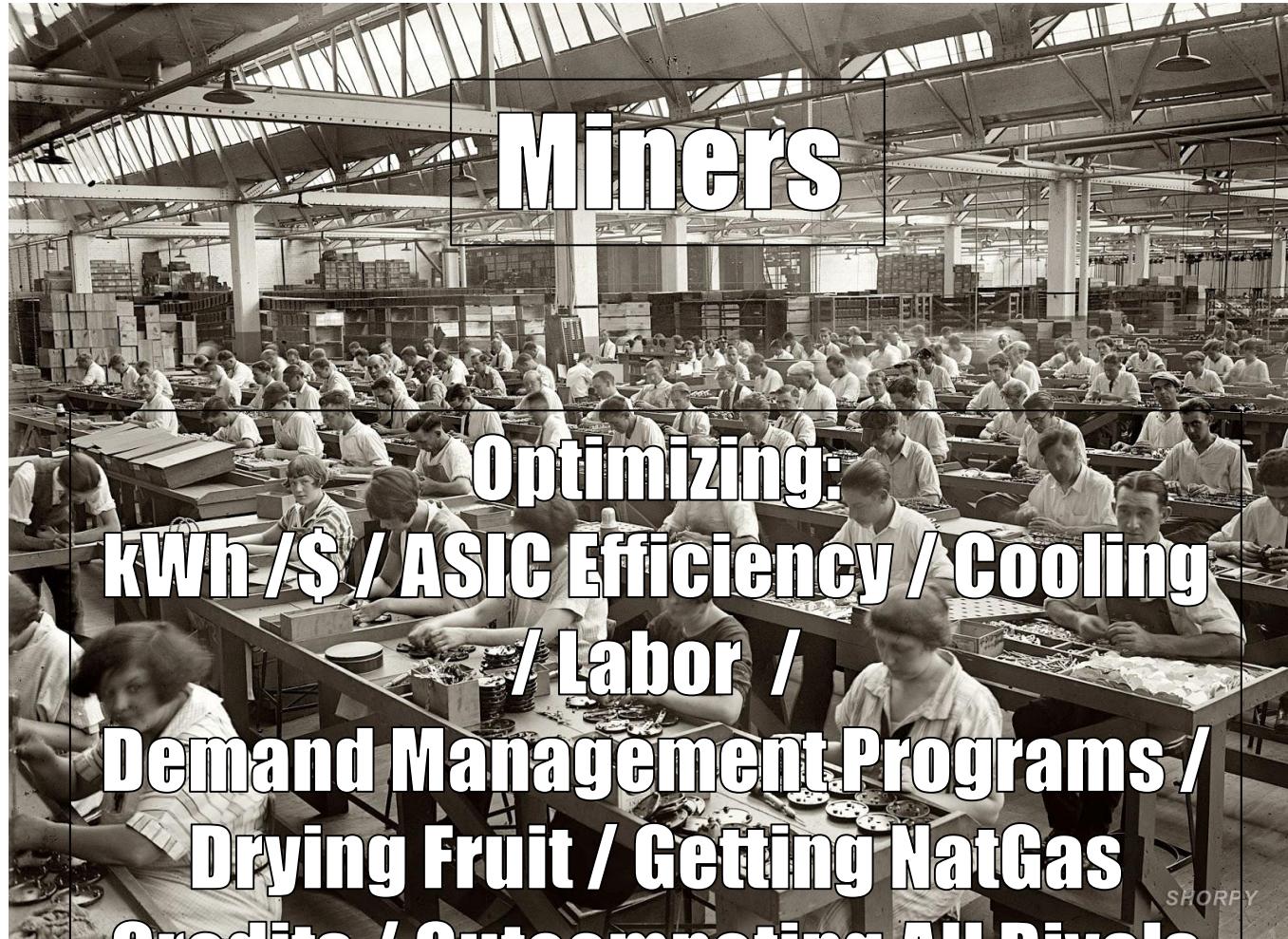
Validating L1

+ counting to 13,150

Telegram: t.me/Dclnsiders

Website: www.LayerTwoLabs.com

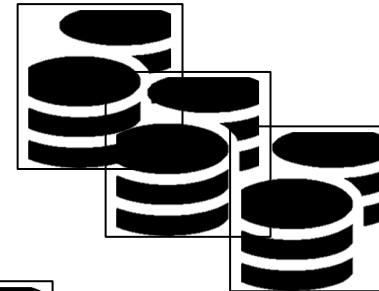
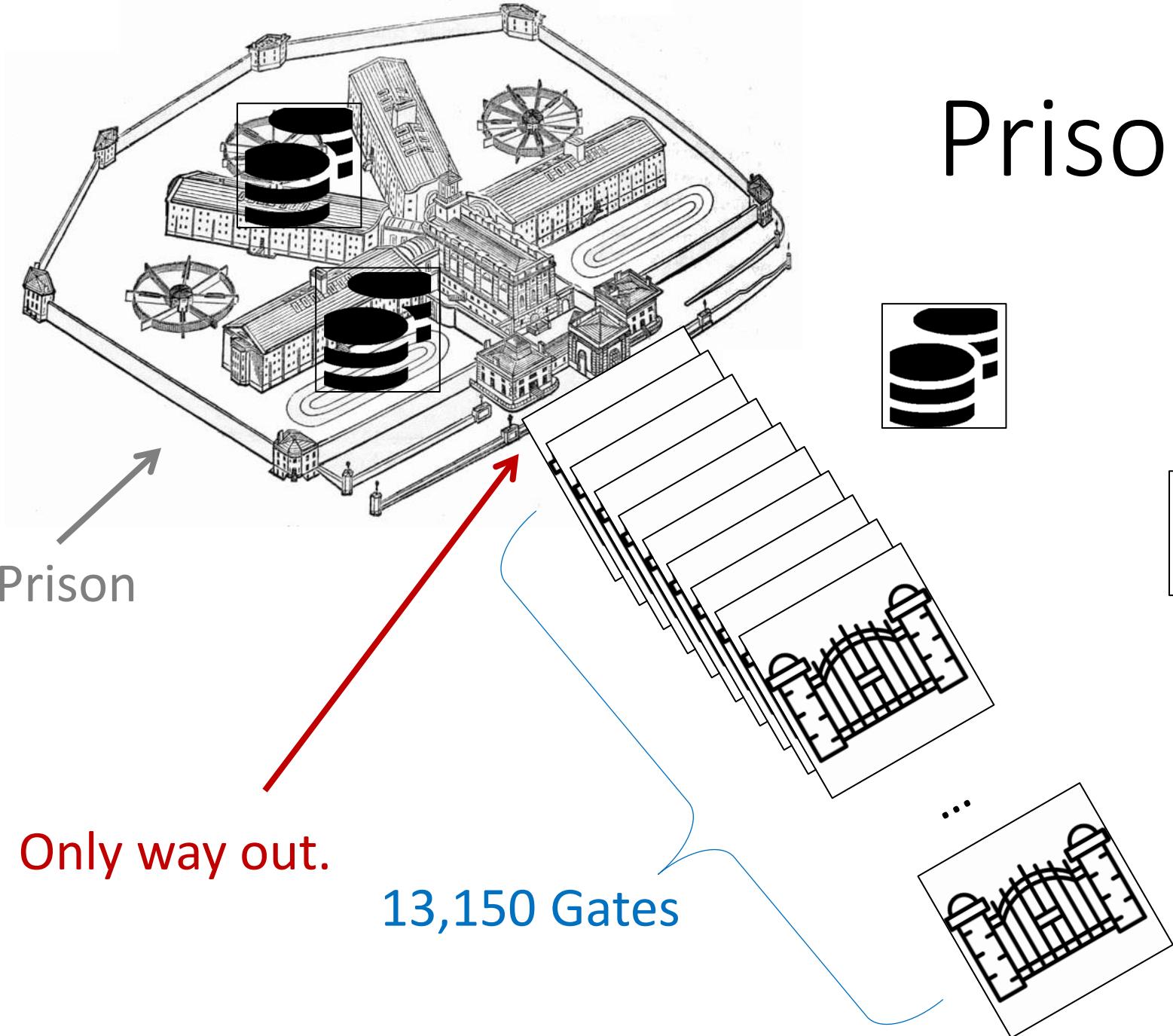
@truthtcoin



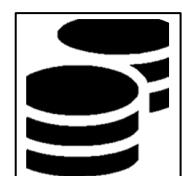
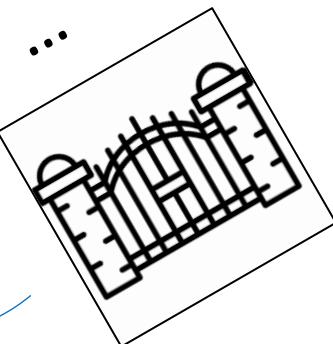
+ add/remove/validate Sidechains

Paul's Twitter:

Prison Metaphor

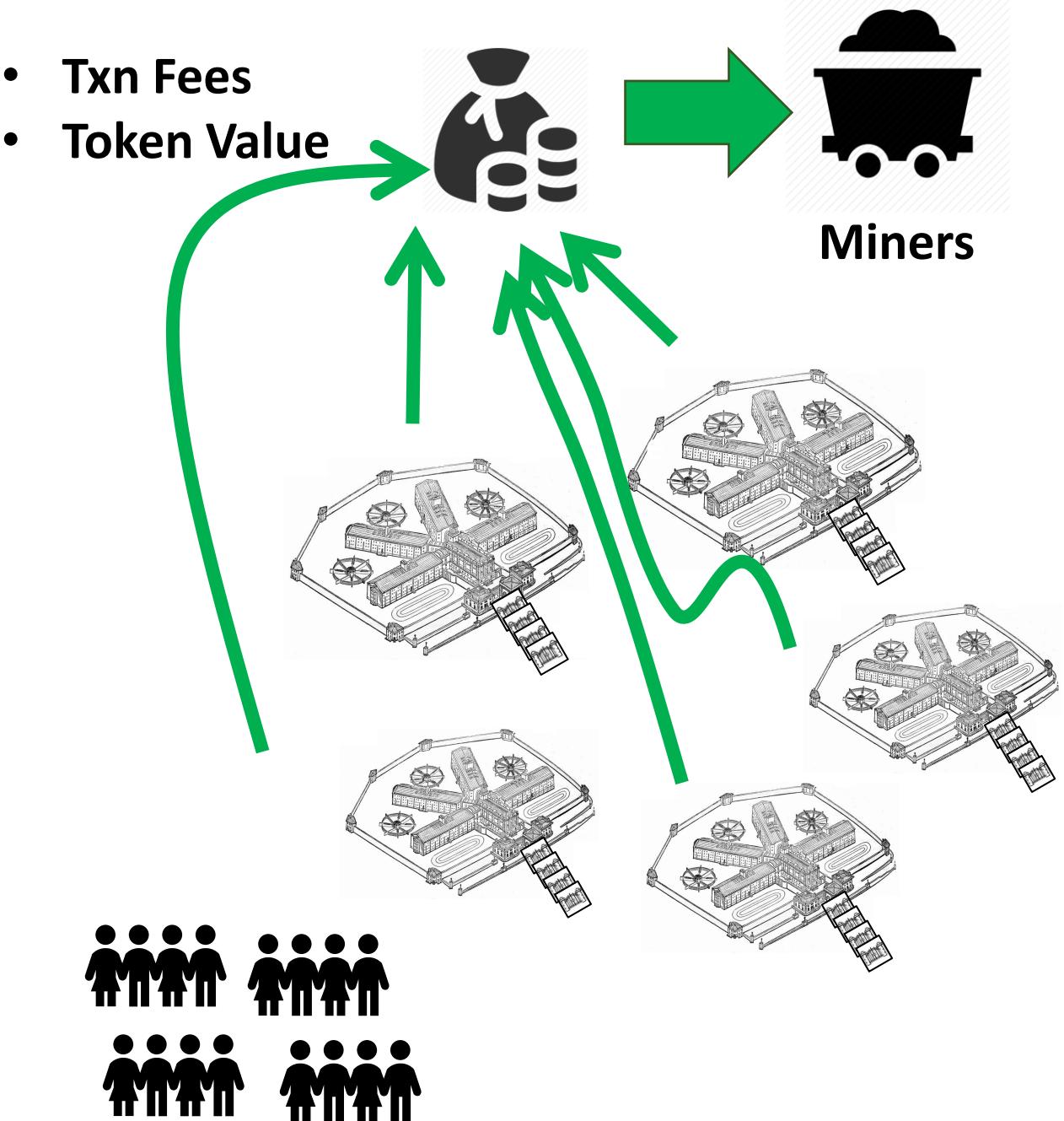


BTC



Summary

1. New source of miner-profits.
2. Miners choice: claim this revenue, or destroy it.
3. High-Auditability:
 - a) Reducing “all txns” down to “net transfers”.
 - b) Crunching all xfers down to 32 bytes.
 - c) One transfer at a time.
 - d) Transfers take 3 months to settle.



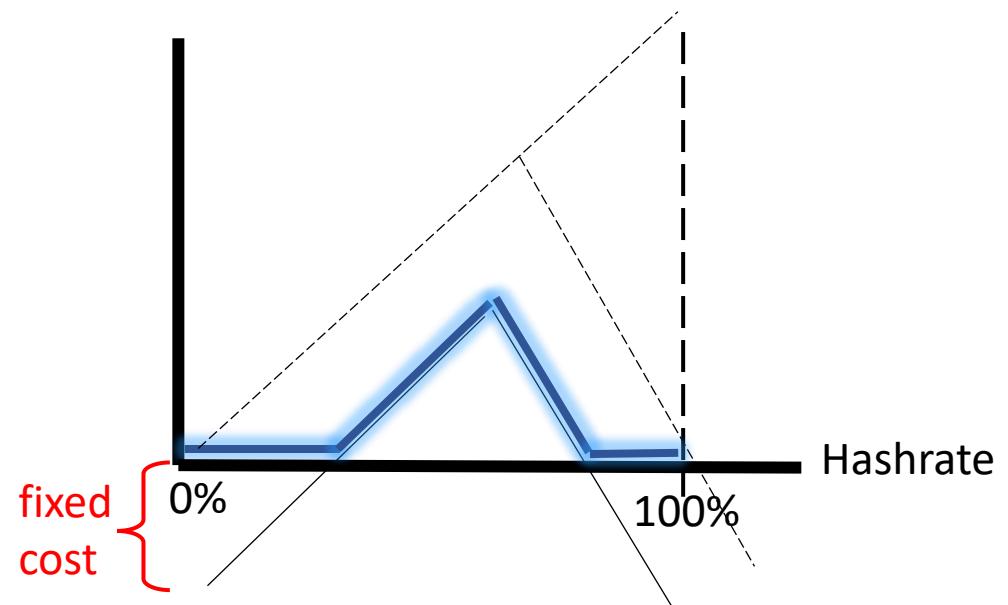
Miners can already:

- Steal from LN channels – by censoring the justice txn
 - Reorg mainchain Bitcoin txns out, and hold them hostage
 - Block any message from L1 – including zk-proofs
-
- So, marginally, it is not actually very large an assumption.

6 - Two Critiques

Two Supposed Drawbacks

(#1) **Miners-Can-Steal** from Bip300 Scripts
(and this is bad)



(#2) **Merged-Mining is a Side-Hustle**
(and those are bad)

Telegram: t.me/DclInsiders

Website: www.drivechain.info

@truthtcoin

Paul's Twitter:

(#1) Miners-Can-Steal from Bip300 Scripts
(and this is bad)

The free market allows entrepreneurs to go bankrupt – this is an essential part of creativity. True: not every SC will succeed. But those few that do, will pay fees to miners and boost BTC's appeal (since BTC can now easily do everything). The failures will serve as a warning to lazy or incompetent developers.

Bip300 has multiple safeguards in place to make “stealing” difficult. Stealing requires 3-6 months of openly dishonest mining activity. Humans can audit theft, by checking just 32 bytes.

Miners “can” steal from Lightning Network (by broadcasting old state + censoring Justice Txns), but this criterion is never held against LN.

The user is sovereign. Users are allowed to sell their BTC for USD; or use BTC to buy “bad” products (ie “drugs”). Or invest in Alts / scams. Bip300 allows users to spend BTC to a script.

This supposed “flaw” is actually a pro, as it gives miners motive and opportunity to destroy “parasite sidechains” (SC which antagonize other SCs). I am not aware of any other way of efficiently accomplishing this. And I believe it is prerequisite for high-quality smart contracts.

The whole point of SCs is that Layer1 nodes ignore them. With federations, you trust a fixed committee of law-abiding people. With Bip300 you trust a decentralized P2P process.

(#2) Merged-Mining is a Side-Hustle
(and those are always bad)

The fixed cost in question...
...is zero under BMM.
...was already microscopic, vs other miner fixed costs.
...must always be small enough for non-mining nodes to exist
(since their revenue is the smallest of all, \$0.)

Mining is a complex task involving many “sub-tasks” (getting cheap power / sourcing good ASICs / etc). Each has its own incentives, innovation, and fixed costs. No stopping those.

Bizarre implications: if BitFury sold t-shirts on the side, for profit, then t-shirts = bad for BTC. If Saylor altruistically paid miners \$0.10 per year, then MS = bad for Bitcoin.

MM is the opposite of bad – it is good and necessary. MM alone can boost BTC's fee revenues by 10,000x or more. Without MM, long run hashrate may be too low.

What is probably happening is that people are confusing node costs with mining costs. Node costs *must* be low, for decentralization. But mining costs have no such requirement. In fact, if we wanted mining costs to be low we could remove the upward difficulty adjustments.

MM is already unblockable. Satoshi invented MM in 2010, and envisioned many independent MM chains. We have been MM since 2011, with no end in sight.

(#1) Miners-Can-Steal from Bip300 Scripts (and this is bad)

The free market allows entrepreneurs to go bankrupt – this is an essential part of creativity. True: not every SC will succeed. But those few that do, will pay fees to miners and boost BTC's appeal (since BTC can now easily do everything). The failures will serve as a warning to lazy or incompetent developers.

Bip300 has multiple safeguards in place to make “stealing” difficult. Stealing requires 3-6 months of openly dishonest mining activity. Humans can audit theft, by checking just 32 bytes.

Miners “can” steal from Lightning Network (by broadcasting old state + censoring Justice Txns), but this criterion is never held against LN.

The user is sovereign. Users are allowed to sell their BTC for USD; or use BTC to buy “bad” products (ie “drugs”). Or invest in Alts / scams. Bip300 allows users to spend BTC to a script.

This supposed “flaw” is actually a pro, as it gives miners motive and opportunity to destroy “parasite sidechains” (SC which antagonize other SCs). I am not aware of any other way of efficiently accomplishing this. And I believe it is prerequisite for high-quality smart contracts.

The whole point of SCs is that Layer1 nodes ignore them. With federations, you trust a fixed committee of law-abiding people. With Bip300 you trust a decentralized P2P process.

(#2) Merged-Mining is a Side-Hustle (and those are always bad)

The fixed cost in question...
...is zero under BMM.
...was already microscopic, vs other miner fixed costs.
...must always be small enough for non-mining nodes to exist
(since their revenue is the smallest of all, \$0.)

Mining is a complex task involving many “sub-tasks” (getting cheap power / sourcing good ASICs / etc). Each has its own incentives, innovation, and fixed costs. No stopping those.

Bizarre implications: if BitFury sold t-shirts on the side, for profit, then t-shirts = bad for BTC. If Saylor altruistically paid miners \$0.10 per year, then MS = bad for Bitcoin.

MM is the opposite of bad – it is good and necessary. MM alone can boost BTC's fee revenues by 10,000x or more. Without MM, long run hashrate may be too low.

What is probably happening is that people are confusing node costs with mining costs. Node costs *must* be low, for decentralization. But mining costs have no such requirement. In fact, if we wanted mining costs to be low we could remove the upward difficulty adjustments.

MM is already unblockable. Satoshi invented MM in 2010, and envisioned many independent MM chains. We have been MM since 2011, with no end in sight.

(#1) Miners-Can-Steal from Bip300 Scripts (and this is bad)

The free market allows entrepreneurs to go bankrupt – this is an essential part of creativity. True: not every SC will succeed. But those few that do, will pay fees to miners and boost BTC's appeal (since BTC can now easily do everything). The failures will serve as a warning to lazy or incompetent developers.

Bip300 has multiple safeguards in place to make “stealing” difficult. Stealing requires 3-6 months of openly dishonest mining activity. Humans can audit theft, by checking just 32 bytes.

Miners “can” steal from Lightning Network (by broadcasting old state + censoring Justice Txns), but this criterion is never held against LN.

The user is sovereign. Users are allowed to sell their BTC for USD; or use BTC to buy “bad” products (ie “drugs”). Or invest in Alts / scams. Bip300 allows users to spend BTC to a script.

This supposed “flaw” is actually a pro, as it gives miners motive and opportunity to destroy “parasite sidechains” (SC which antagonize other SCs). I am not aware of any other way of efficiently accomplishing this. And I believe it is prerequisite for high-quality smart contracts.

The whole point of SCs is that Layer1 nodes ignore them. With federations, you trust a fixed committee of law-abiding people. With Bip300 you trust a decentralized P2P process.

(#2) Merged-Mining is a Side-Hustle (and those are always bad)

The fixed cost in question...
...is zero under BMM.
...was already microscopic, vs other miner fixed costs.
...must always be small enough for non-mining nodes to exist
(since their revenue is the smallest of all, \$0.)

Mining is a complex task involving many “sub-tasks” (getting cheap power / sourcing good ASICs / etc). Each has its own incentives, innovation, and fixed costs. No stopping those.

Bizarre implications: if BitFury sold t-shirts on the side, for profit, then t-shirts = bad for BTC. If Saylor altruistically paid miners \$0.10 per year, then MS = bad for Bitcoin.

MM is the opposite of bad – it is good and necessary. MM alone can boost BTC's fee revenues by 10,000x or more. Without MM, long run hashrate may be too low.

What is probably happening is that people are confusing node costs with mining costs. Node costs *must* be low, for decentralization. But mining costs have no such requirement. In fact, if we wanted mining costs to be low we could remove the upward difficulty adjustments.

MM is already unblockable. Satoshi invented MM in 2010, and envisioned many independent MM chains. We have been MM since 2011, with no end in sight.

(#1) Miners-Can-Steal from Bip300 Scripts (and this is bad)

The free market allows entrepreneurs to go bankrupt – this is an essential part of creativity. True: not every SC will succeed. But those few that do, will pay fees to miners and boost BTC's appeal (since BTC can now easily do everything). The failures will serve as a warning to lazy or incompetent developers.

Bip300 has multiple safeguards in place to make “stealing” difficult. Stealing requires 3-6 months of openly dishonest mining activity. Humans can audit theft, by checking just 32 bytes.

Miners “can” steal from Lightning Network (by broadcasting old state + censoring Justice Txns), but this criterion is never held against LN.

The user is sovereign. Users are allowed to sell their BTC for USD; or use BTC to buy “bad” products (ie “drugs”). Or invest in Alts / scams. Bip300 allows users to spend BTC to a script.

This supposed “flaw” is actually a pro, as it gives miners motive and opportunity to destroy “parasite sidechains” (SC which antagonize other SCs). I am not aware of any other way of efficiently accomplishing this. And I believe it is prerequisite for high-quality smart contracts.

The whole point of SCs is that Layer1 nodes ignore them. With federations, you trust a fixed committee of law-abiding people. With Bip300 you trust a decentralized P2P process.

(#2) Merged-Mining is a Side-Hustle (and those are always bad)

The fixed cost in question...
...is zero under BMM.
...was already microscopic, vs other miner fixed costs.
...must always be small enough for non-mining nodes to exist
(since their revenue is the smallest of all, \$0.)

Mining is a complex task involving many “sub-tasks” (getting cheap power / sourcing good ASICs / etc). Each has its own incentives, innovation, and fixed costs. No stopping those.

Bizarre implications: if BitFury sold t-shirts on the side, for profit, then t-shirts = bad for BTC. If Saylor altruistically paid miners \$0.10 per year, then MS = bad for Bitcoin...

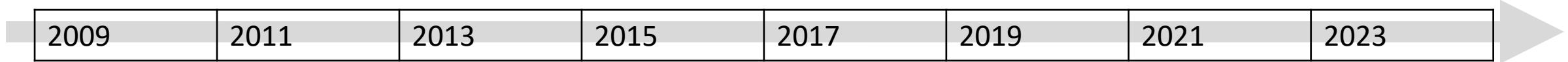
MM is the opposite of bad – it is good and necessary. MM alone can boost BTC's fee revenues by 10,000x or more. Without MM, long run hashrate may be too low.

What is probably happening is that people are confusing node costs with mining costs. Node costs *must* be low, for decentralization. But mining costs have no such requirement. In fact, if we wanted mining costs to be low we could remove the upward difficulty adjustments.

MM is already unblockable. Satoshi invented MM in 2010, and envisioned many independent MM chains. We have been MM since 2011, with no end in sight.

Why Hasn't Bitcoin Already Conquered the World?

Time



Initial Growth P

Blocksize War

Today

Orthodox Interpretation

Network-Effect Interpretation

Telegram: t.me/DlInsiders

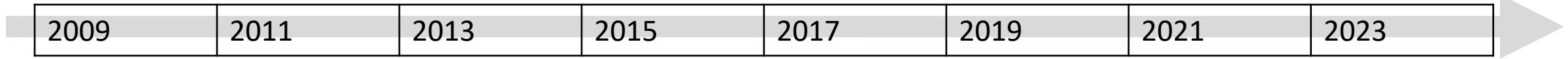
Website: www.LayerTwoLabs.com

Paul's Twitter:

@truthtcoin

Why Hasn't Bitcoin Already Conquered the World?

Time



Initial Growth P

Orthodox Interpretation

Network-Effect Interpretation

Blocksize War

- Culling of the Weak
- Unreliable allies were purged
- Demonstrates our Commitment to Decentralization

Today

- It takes time!
- S**tcoins exist because of moral defects (“greed”, scams, bad marketing).

Telegram: t.me/DlInsiders

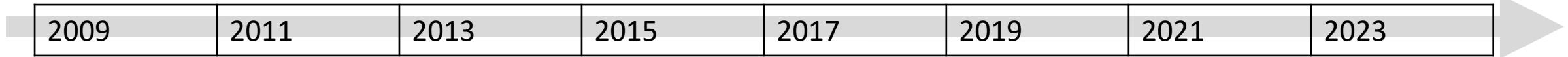
Website: www.LayerTwoLabs.com

Paul's Twitter:

@truthtcoin

Why Hasn't Bitcoin Already Conquered the World?

Time



Initial Growth P

Orthodox Interpretation

Network-Effect Interpretation

Blocksize War

- Culling of the Weak
- Unreliable allies were purged
- Demonstrates our Commitment to Decentralization

Today

- It takes time!
- S**tcoins exist because of moral defects (“greed”, scams, bad marketing).

- Complacency / Flipping / Uncertainty that Bitcoin is “the one”.
- People like the features and cheap fees of other blockchains.

Telegram: t.me/DcInsiders

Website: www.LayerTwoLabs.com

Paul's Twitter:

@truthtcoin

How to Get These BIPs

Soft Fork Deadlock Problem

Bitcoin Development has slowed to a crawl – because of 2017!

Year	2010	2011	2012	2013	2014	2015	2016
# of Soft Forks	7	0	2	2	0	2	3
Year	2017	2018	2019	2020	2021	2022	2023
# of Soft Forks	1	0	0	0	1	0	0 (Presumably)

16

2

- SegWit

- Announced Dec 2015
- Coded Oct 2016
- Activated Aug 2017

20 Months

- Taproot

- Announced Jan 2018
- Coded Oct 2020
- Activated Nov 2021

46 Months

Modern Soft Fork Activation

- The fate of 118
- The fate of 119
- If we always refuse to act, out of fear of making an error – that itself is a pretty grave error.
- If we always defer – it will create politics and chaos.
- Miners must get involved and learn the issues.
- Not everyone can be a specialist – by definition. But you can force 2-3 independent specialists to compete for your attention.

How to Get BIPs 300/301

1. Specifically, **SoftFork deadlock problem** –
2017-era Miners created this problem,
can be solved with leadership from >50% hashpower (a few pools).
Can be solved once-and-for-all.
2. Requires better Pool \leftrightarrow Hasher **communication**.
And willingness to switch pools.
Or even punitively destroy a pool, retroactively.
3. Someone has to take **responsibility** – and its YOU!
Long run, you will suffer the most... if Bitcoin underperforms.

Supporters and Detractors

	Supporters	Detractors
Theorists	<p>Many Tech Elite (visit LayerTwoLabs.com/friends)</p>	<p>Hopelessly Confused</p> <p>The main concern is Billions of Revenue, may cost miners \$40k , which may harm small miners.</p> <p>(None of that is true.)</p>
Builders	<p>Reluctant Altcoiners</p> <p>ETH, Monero, BCH, Namecoin, Sia – all created by Bitcoiners. Published comments of regret, re Bitcoin's non-extensibility</p> <p>All will be cloned, by me! So we will steal back their work.</p>	<p>The Death Cult</p> <ul style="list-style-type: none">○ Unwilling to give Altcoins any credit for innovation. Or adoption.○ Think Bitcoin shouldn't improve / can't improve (since it is perfect).○ Prefer Bitcoin to stay niche.

In One Slide

More revenues (10x 20x) are possible,
but only if Miners educate themselves on the tech.
Including conflicts-of-interest among dev groups.

1. What are BIPs 300/301 ?

- 300 allows for conversion: [Altcoin L1] → [BTC-only L2].
- 301 allows Bitcoin miners (that's you), to collect all the fees of these networks.
- Requires 51% hashrate to activate soft fork + other very small costs.

2. How to get it ?

- Miners take responsibility for educating self on BIPs.
- Fix softfork deadlock issue. Force responsibility onto someone.
- Fix Pool – Hasher communication.

Detractors

The Hopelessly Confused

Believe misinformation about the idea.

For example, Peter Todd mistakenly believes that this idea could cost miners as much as \$40k / year in software, which he says may harm small miners.

(Not true. But also irrelevant since every mining input has fixed/variable costs.)

The Death Cult

People who:

- Think Bitcoin shouldn't improve / can't improve (since it is perfect).
- Think Bitcoin shouldn't compete / doesn't compete for users (since it is perfect).
 - Are uninterested in long run miner revenues.
- Are unwilling to give Altcoins any credit for innovation. Or adoption.
 - Prefer Bitcoin to stay niche.

Conflicts of Interest – Time to get Woke

- Devs , Users, Miners, Investors

Good Luck with Your Decision!

- @truthcoin on twitter
- @psztorc on Telegram
- I know many Pools/Miners, also can contact me through them.