BIP 300/301 — Collecting every txn fee on Earth

Paul Sztorc

Nov 17, 2023 North American Blockchain Summit

In One Slide

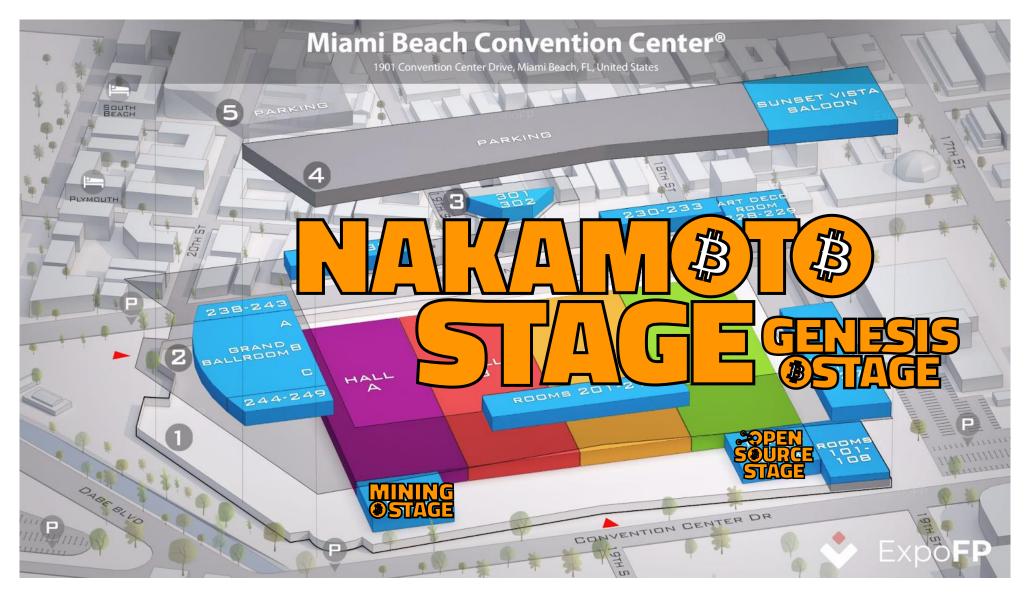
- 1. Paul Sztorc (me), author of BIPs 300/301 ...
 - ... I'm saying that you (Miners), can earn Billions more revenues...
 - ...if you do the right thing, which is: become more educated on technical issues.
- 2. BIPs 300/301 ...
 - ... 300: Altcoin txns → BTC txns ...
 - ... 301: gives all those txn fees to you (the L1 Bitcoin miners).
 - Other benefits and details.
- 3. How to Get It
 - Easy! 51% Hashrate updates.
 - But, it is a touchy subject. You must research the issues.
 - Warning fail to act, and there may be future mismatch between L1/L2 fees.

When Worlds Collide...



Site: www.LayerTwoLabs.com www.drivechain.info Paul's Twitter: @truthcoin

When Worlds Collide...



Site: www.LayerTwoLabs.com www.drivechain.info Paul's Twitter: @truthcoin

When Worlds Collide...



Site: www.LayerTwoLabs.com www.drivechain.info Paul's Twitter: @truthcoin

My 1000+ Pages About Bitcoin

OCTOBER 2017

Fork Futures (via the Exchanges) 12 Oct 2017

2012-2014 | Statistician, Yale Econ

→ Bitcoin Researcher

The Peer Database ("Private Blockchains" Done Right) 17 Mar 2016 Five Lies and the Truth 11 Sep 2018 Small Transactions 08 Apr 2023 Nothing is Cheaper than Proof of Work 04 Aug 2015 Private Blockchains, Demystified 16 Mar 2016 **JUNE 2019** JULY 2017 The Consent of the Governed 21 Jun 2019 The Trusted 3rd Party Doesn't Scale (But Blockchains Do) 08 Mar 2016 **JUNE 2018** Proof of Stake is Still Pointless 07 Jul 2017 JUNE 2022 BitAssets - A Digital Assets Sidechain 21 Jun 2018 Map-Territory Epistemology (Part 5) 21 Jun 2019 The "Sidechain Vision" for Bitcoin 27 Jun 201 One Chain to Rule Them All 07 Mar 2016 The Win-Win Blocksize Solution 14 Jul 2015 Map-Territory Epistemology (Part 4) 21 Jun 2019 **JANUARY 2017 APRIL 2018** Map-Territory Epistemology (Part 3) 21 Jun 2019 Blind Merged Mining 30 Jan 2017 **APRIL 2022** DECEMBER 2015 Meditations on Fraud Proofs 14 Apr 2018 Lightning Network -- Fundamental Limitation Salvaging the Blocksize Discussion, in Two Questions 28 Dec 2015 Mining - Threat Model and Equilibrium Analysis 29 Jan 2017 Map-Territory Epistemology (Part 2) 21 Jun 2019 Bitcoin and Deflation, The Last Word 15 May 2015 Blockchain Fusion (via Compensated Sidechains) 07 Apr 20 The Mirage of Miner Centralization 28 Jan 2017 Map-Territory Epistemology (Part 1) 21 Jun 2019 Bitcoin Post-Maximalism 07 Apr 2018 **OCTOBER 2021 NOVEMBER 2015** Upgrading 'Smart Contracts' to 'Wise Contracts' 11 Jan 2017 JANUARY 2015 Security Budget II, Low Fees, and Merged M Drivechain - The Simple Two Way Peg 24 Nov 2015 Two Types of Blockspace Demand 10 Jan 2017 **FEBRUARY 2019** BitUSD Isn't Worth The Trouble 29 Jan 2015 **MARCH 2018** Security Budget in the Long Run 14 Feb 2019 GigaChain 20 Mar 2018 OCTOBER 2015 DECEMBER 2016 NOVEMBER 2014 Sidechain For BitNames/Logins/DNS, Taking The Hashing Heart Attack 28 Oct 2015 Against the Hard Fork 06 Dec 2016 The Limits of Blockchain Tech 28 Nov 2014 **NOVEMBER 2017** Sidechains for Scaling -- Thunder Network PSA - Linking to a Blog Section 05 Oct 2015 Imposed Mutual-Exclusivity (IMEX) for Hard Forks 20 Dec 2018 Better Fork Terminology 05 Dec 2016 Altcoins Aren't Money, They're Bitcoin's Casino/Laundroma The UASF Contradiction 02 Nov 2017 Sidechains for Privacy -- zSide and Melt/Cas Long Live Proof-of-Work, Long Live Mining 16 Nov 2014 The MAHF And Replay "Protection" 02 Nov 2017 **MAY 2016** Active Decentralization 09 Nov 201/ Oracles are the Real Smart Contracts 21 Sep 2015 Gradually Activated Replay Protection (GARP) - Toward Hard Forks that De More Terminology -- Forks and Splits 02 Nov 2017 BTC Codex - The Digital Identity Sidechain 21 May 2016 Three Basics 06 Nov 201/ Measuring Decentralization 09 Sep 2015 Miners Don't Control Tx-Selection 02 Nov 2017 The Drivechain OP Code 14 May 2016

SEPTEMBER 2018

Expensive Privacy is Useless Privacy 11 Sep 2018

ASICBoost is Worthless 02 Nov 2017

OpenVote - Auditable, Fast, Private, Secure Voting 10 Jan 2021

Deniability - Unilateral Transaction Meta-Privacy 09 Nov 2018

APRIL 2023

My Big Break

Dec 2014 – Adam Back links to my blog

Sr. Member



Activity: 404 Merit: 318



in bitcoin we trust





y, lack of price/supply feedback & long run electrical cost December 29, 2014, 12:21:39 AM

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 selfcorrect 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 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.

Part 2 - BIP 300/301

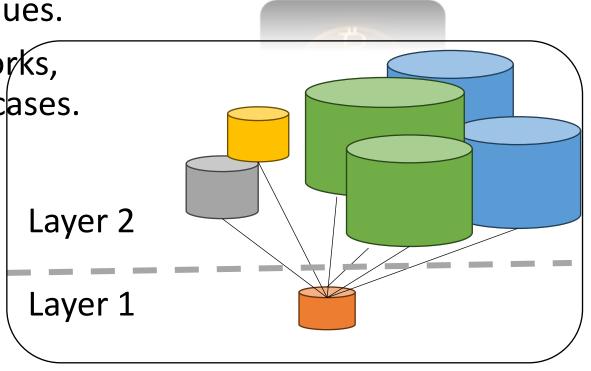
(also called "Drivechain")

- 1. The idea
- 2. Timeline of Progress
- 3. Supporters / Detractors
- 4. More details

Goals of BIP 300/301

- **1) Every** transaction, in the world, is a Bitcoin txn, and <u>each</u> 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 <u>already</u> on some network or another. They all pay some kind of fee to someone. (VISA, Venmo)

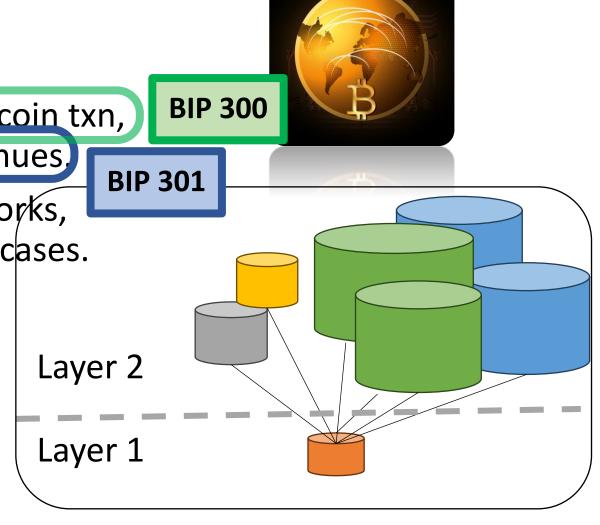
Goals of BIP 300/301

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

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

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





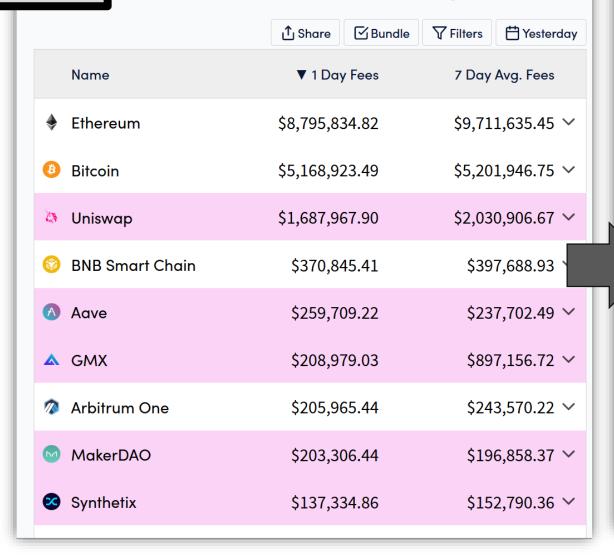
All the world's txns are <u>already</u> on some network or another. They all pay some kind of fee to someone. (VISA, Venmo)

The Goal

Crypto Fees

There's tons of crypto projects.

nich ones are people actually paying to use?



Crypto Fees

There's tons of crypto projects.

Which ones are people actually paying to use?

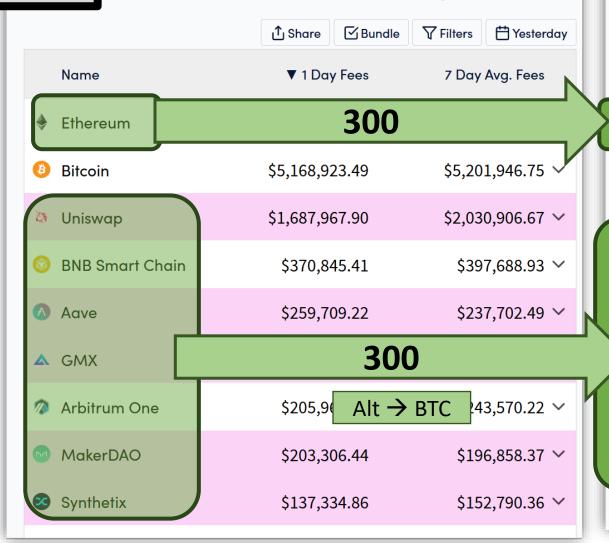
	1 Share	☑ Bundle	∀ Filters	Yesterday		
Name	▼ 1 Day	/ Fees	7 Day Avg. Fees			
Bitcoin	\$8,795,83	34.82	\$9,711,635.45 \			
Bitcoin	\$17,000	0,000	\$5,201,946.75 ~			
Bitcoin	\$1,687,96	67.90	\$2,030,906.67 ~			
3 Bitcoin	\$370,84	45.41	\$39	7,688.93 ×		
Bitcoin	\$259,709.22			\$237,702.49 \(\times		
Bitcoin	\$208,979.03			\$897,156.72 ∨		
Bitcoin	\$205,965.44			\$243,570.22 ~		
Bitcoin	\$203,30	06.44	\$196,858.37 ×			
Bitcoin	\$137,33	34.86	\$15	2,790.36 ×		

The Goal

Crypto Fees

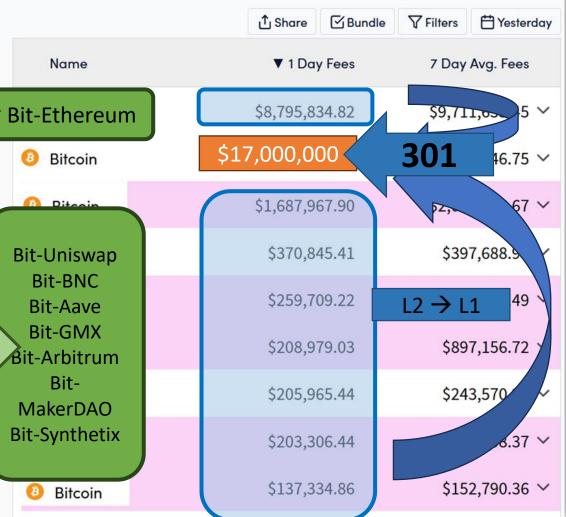
There's tons of crypto projects.

nich ones are people actually paying to use?



Crypto Fees

There's tons of crypto projects.
Which ones are people actually paying to use?



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.

The Cost

- Activate BIP 300 I'll get to that.
- Curate the portfolio of sidechains very easy, since you have all the leverage. Cost ~\$0.
- Moderate disputes.
 - Run a node if there is a dispute.
 - Nodes are cheap, by mining standards. Worst-of-the-worst: Solana, BSV, 1 GB Blocksize node. Cost is 3k-5k \$/year, each.
 - Amortized, 10 days to sync → \$137 per dispute.
 - E(d) = 0
 - Miners can defer to pools; pool admits can defer to a user's node.
 - So cost = \$0.
- 9 of those (or something better), would process the world's txns.
 See my blog post "thunder" for details.

The Cost

- Activate BIP 300 I'll get to that.
- Curate the portfolio of sidechains very easy, since you have all the leverage. Cost ~\$0.
- Moderate disputes.
 - Run a node if there is a dispute.
 - Nodes are cheap, by mining standards. Worst-of-the-worst: Solana, BSV, 1 GB Blocksize node. Cost is 3k-5k \$/year, each.
 - Amortized, 10 days to sync → \$137 per dispute.
 - E(d) = 0
 - Miners can defer to pools; pool admits can defer to a user's node.
 - So cost = \$0.
- 9 of those (or something better), would process the world's txns. See my blog post "thunder" for details.

Timeline of Progress

Timeline:

2015 – A mere blog post

2017 - BIP #s 300 / 301

2019 – 1st Software Release (testnet)

2022 – Cloned zCash and Eth.

2023 – Luke Dashjr's WIP pull request to Bitcoin Core

Highly endorsed by the technical elite – but not everyone.

My Three Favorite Endorsements

- "Drivechains...are pretty cool...and arguably could have been more important or useful than let's say Taproot."
 - Adam Back, Baltic Honeybadger 2022, Live on stage in front of everyone
- "We need Drivechain or all the work of thousands in the last 13 years will be in vain." ... "Drivechain is our only hope".
 - fiatjaf, (creator of nostr), on twitter
- "We need your project, of course, for the obvious reasons..."
 - Rene Pickhardt (Author of <u>Mastering Lightning</u> , #1 stackoverflow (?) contributor for LN questions), MIT Bitcoin Expo, 2023

Visit www.LayerTwoLabs.com/friends for 49 more!

My Three Favorite Endorsements

• "Drivechains...are pretty cool...and arguably could have been more



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

-Robin Linus, Founder of ZeroSync, Creator of BitVM / BitStream

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.

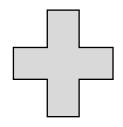
A Bold Claim

- 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!

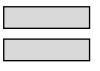
That "Zero Risk" Part

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

Bitcoin Core v25



BIP 300 Softfork

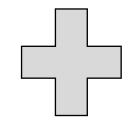


New Bitcoin

Core Interoperable

with Core v25

New Bitcoin <u>Co</u>re



A Softfork Banning all Bip300 Deposits/Withdrawals from L1



Bitcoin Core v25

Interoperable with Core v25

Telegi

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

ter:

22

A Bold Claim

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

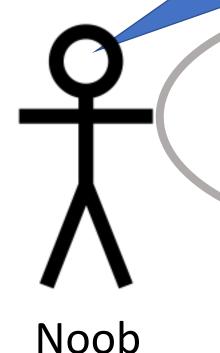
- BIP300 Solves All of Bitcoin's Biggest Problems
 - A. Heterogeneity Problem Different chains for different users.
 - B. Scalab A team of region-specific chains, each with a large growing Blocksize onboard users directly to L2.
 - C. Privacy zCash drivechain.
 - D. Scams Eliminating Have a dedicated 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 <u>real world tasks</u>.
- With...

H. ...zero risk to Bitcoin!

BitNames + Truthcoin ; examples

A. Heterogeneity

Bitcoin does seem great... but can it do



Actually we DON'T want Bitcoin to do in the first place because it is actually a bad due to , as you can . But it by you really , then yes Bitcoin can do that! Eventually we are working on which should be able to do even better anyway but it is actually a good thing that the protocol is so difficult to upgrade beca ...

> Yes. See BIP 300.

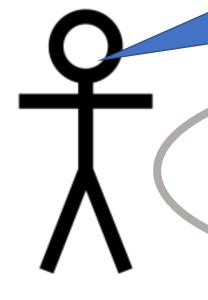
DeFi **Turing Completeness** Ring Signatures zk-Snarks Large Blocksizes **NFTs Oracles** Mimblewimble ...(etc)

Smart Contracts

Bitcoiner

A. Heterogeneity





Noob (and/or Fringe Genius)

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 infall ble ____ 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 ...

> Use BIP 300. Good luck!!



Bitcoiner

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.

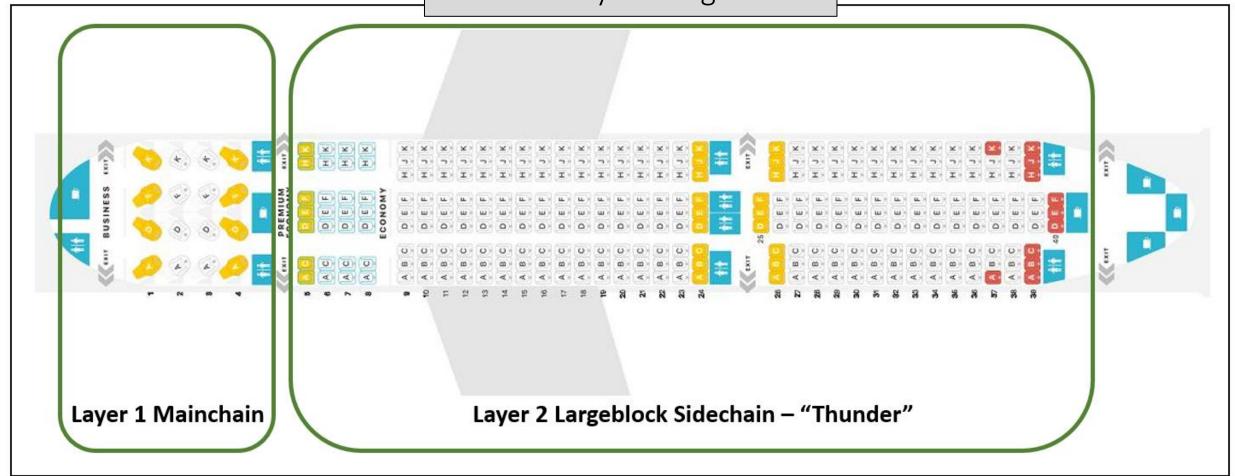
BitNames + Truthcoin; examples

- 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 <u>real world tasks</u>.
- With...

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.

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	16
# of Soft Forks	7	0	2	2	0	2	3	10
Year	2017	2018	2019	2020	2021	2022	2023	2
# of Soft Forks	1	0	0	0	1	0	(Presumably)	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

- 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.
- Requires better Pool ← → 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.

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.

@truthcoin

- 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.

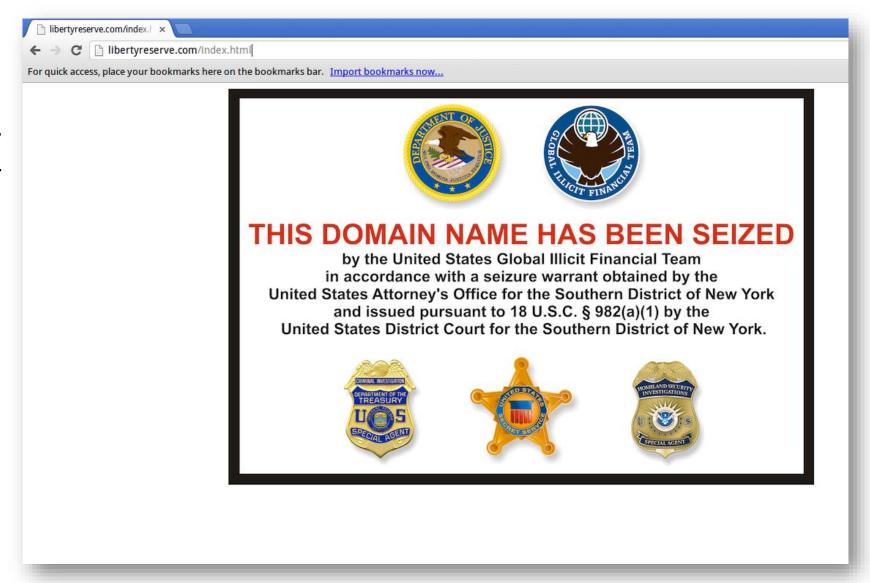
Screenshot #1 from

www.truthcoin.info/ blog/bitnames/



Screenshot #2 from

www.truthcoin.info/
blog/bitnames/





Telegram: t.me/DcInsiders

Paul's Twitter: @truthcoin

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 <u>counteract</u> "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.



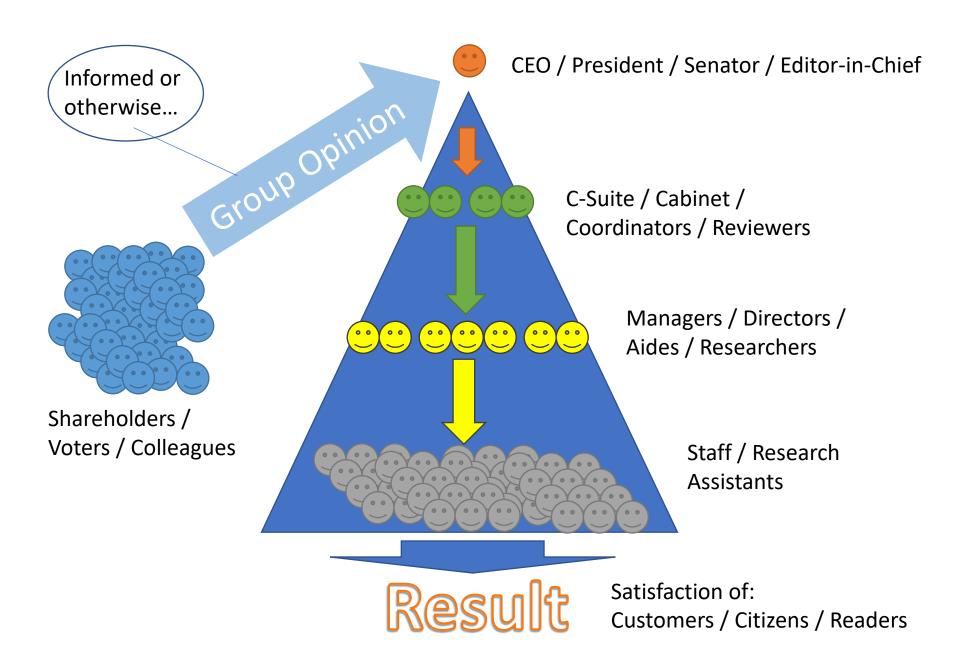
Quis custodiet ipsos custodes? – "But who is in charge of those who are in charge?"

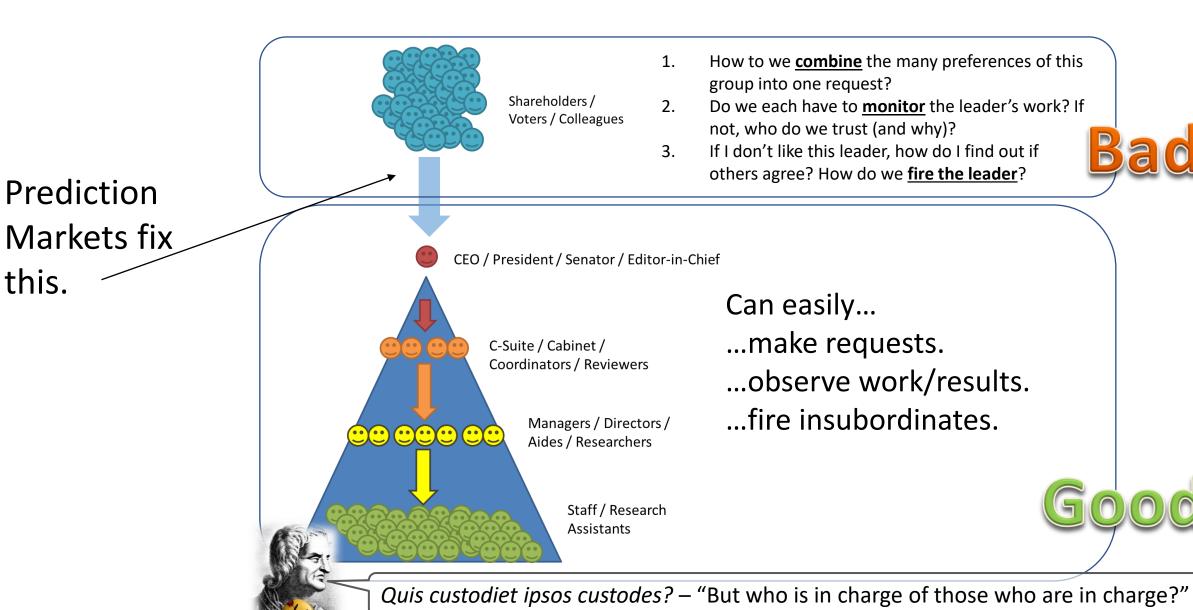
- Fork futures -- would have prevented the Blocksize war.
- Portfolio replication allows for stablecoins/anything-coins... no backer needed!

@truthcoin

Paves the way for land-value-Futarchy / nirvana.

Rot From Above: Who controls what?





@truthcoin

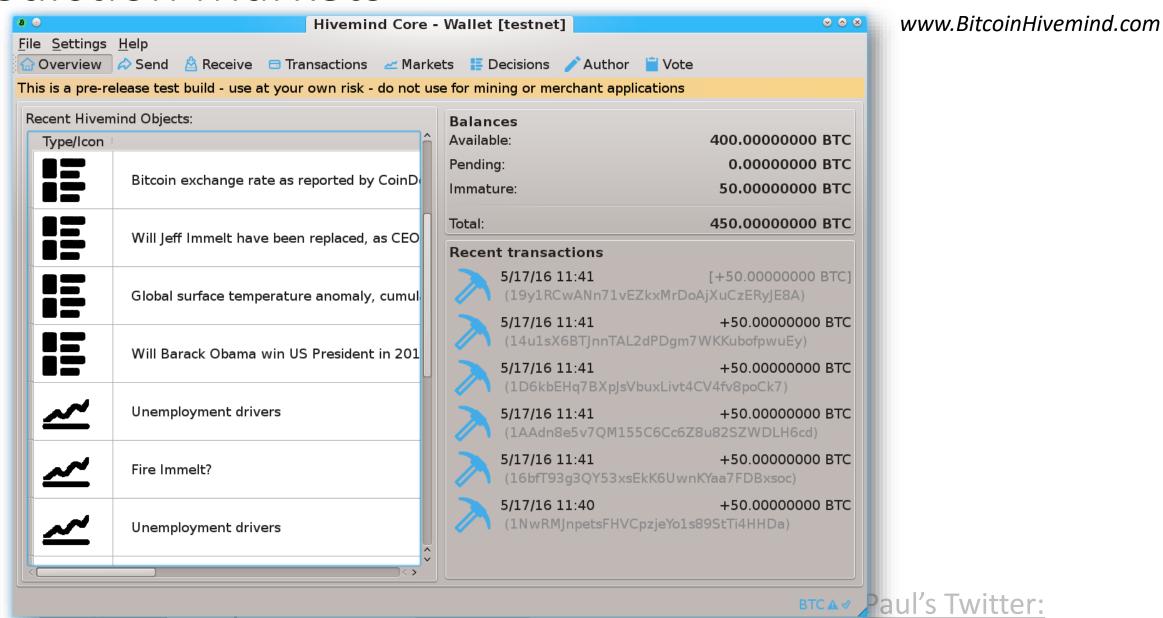
Telegram: t.me/DcInsiders

Prediction

this.

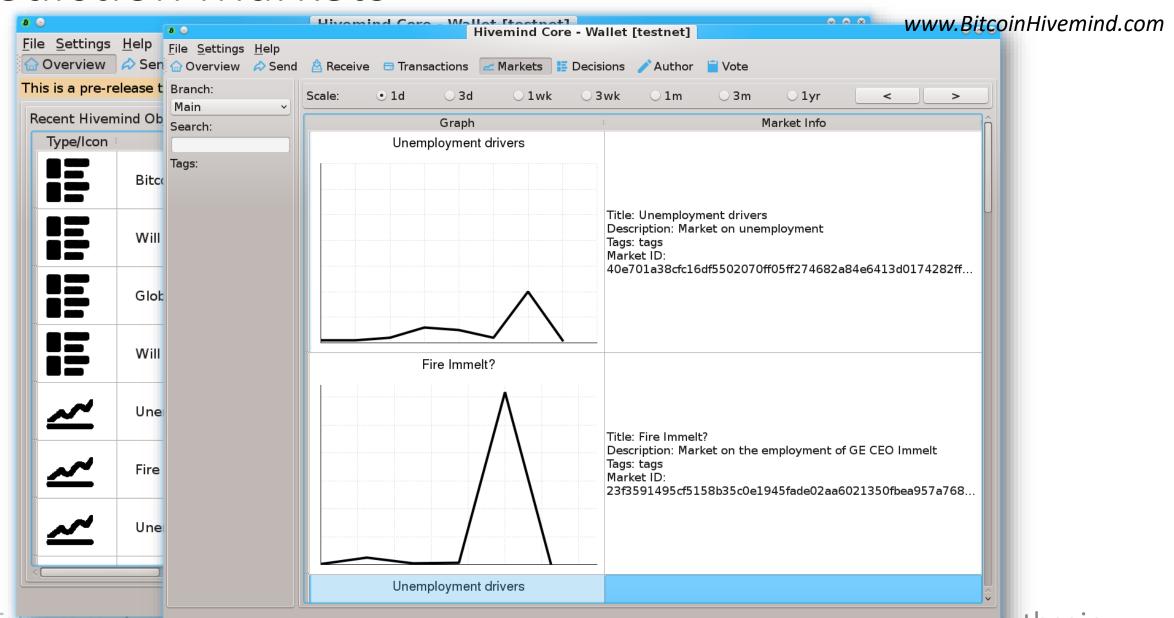
Website: www.LayerTwoLabs.com Paul's Twitter:

Screenshots from my own BTC sidechain project

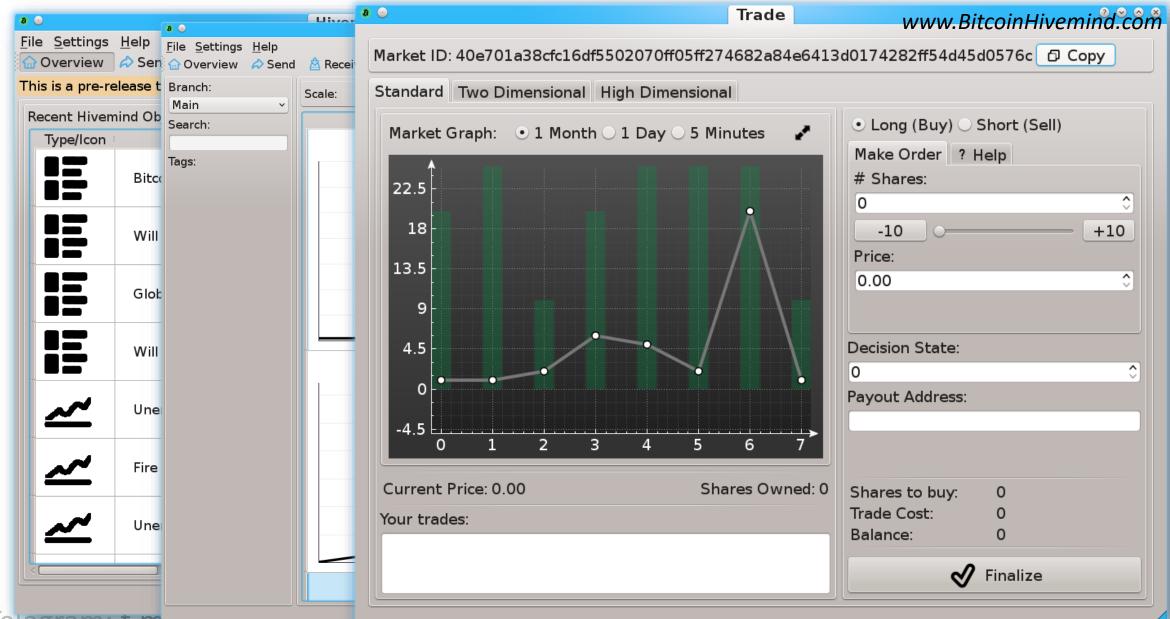


40

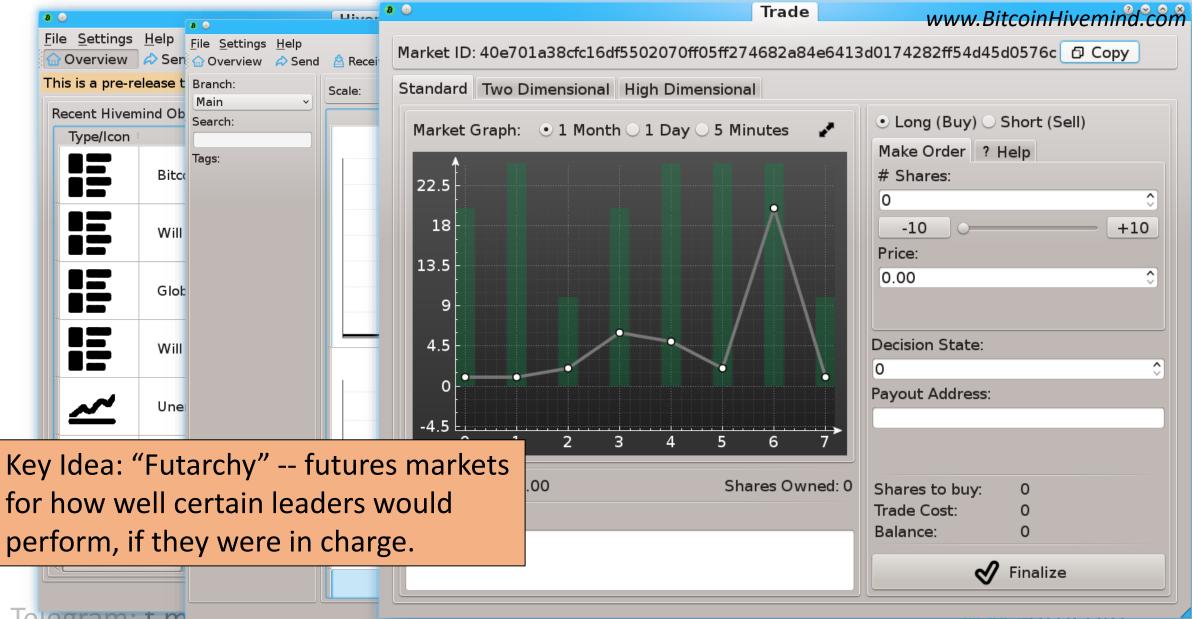
Screenshots from my own BTC sidechain project



• Screenshots from my own BTC sidechain project



• Screenshots from my own BTC sidechain project



Supporters and Detractors

	Supporters	Detractors
Theorists		Hopelessly Confused
	Many Tech Elite (visit LayerTwoLabs.com/friends)	The main concern is Billions of Revenue, may cost miners \$40k, which may harm small miners.
		(None of that is true.)
Builders	Reluctant Altcoiners	The Death Cult
	ETH, Monero, BCH, Namecoin, Sia – all created by Bitcoiners. Published comments of regret, re Bitcoin's non-extensibility All will be cloned, by me! So we will steal	 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.
	back their work.	

In One Slide

More revenues (10x 20x) are possible, but only if Miners <u>educate themselves on the tech</u>. 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 <u>take responsibility</u> for educating self on BIPs.
 - Fix softfork deadlock issue. Force responsibility onto someone.
 - Fix Pool Hasher communication.

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.