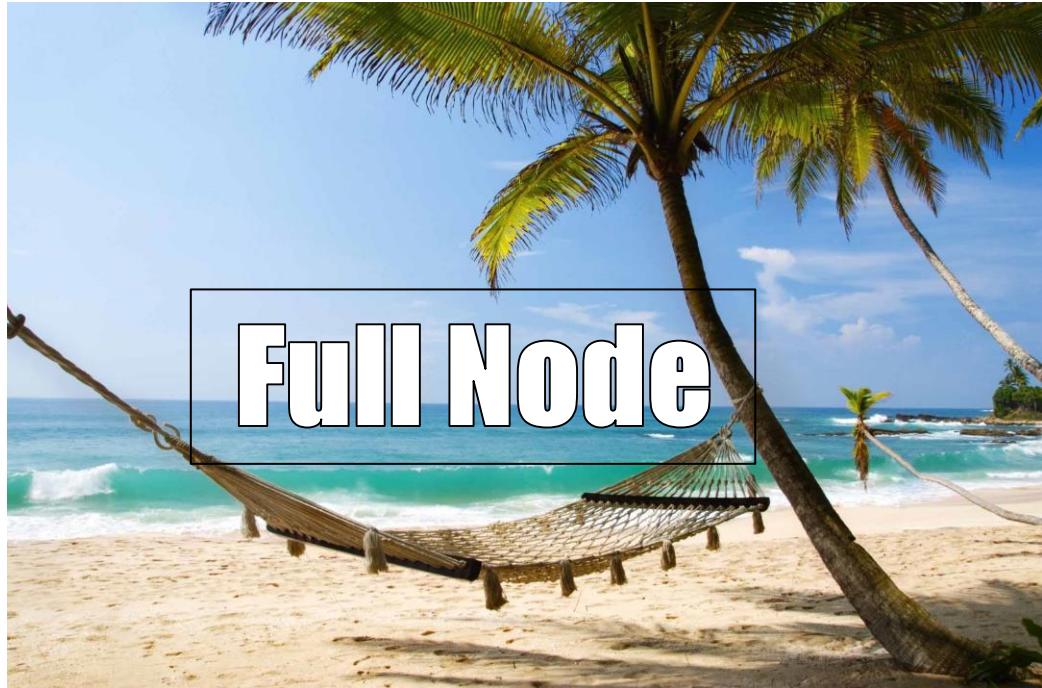


Bip300: How we Police Sidechains Without Looking at Them

Paul Sztorc

Bitcoin++ -- April 29th, 2023

bitcoin++



Full Node

Validating L1

+ counting to 13,150



+ add/remove/validate Sidechains

Agenda

1. Paul Sztorc / LayerTwo Labs
2. Review: Why BIP 300
3. An Example – zCash
4. The BIP Text – The Six Messages of BIP 300
5. Theory: How to Police a [Chain] We Can't See
6. Q&A

Paul's 1000+ Pages About Bitcoin

AUGUST 2015 Nothing is Cheaper than Proof of Work 04 Aug 2015	MARCH 2016 The Peer Database ("Private Blockchains" Done Right) 17 Mar 2016 Private Blockchains, Demystified 16 Mar 2016 The Trusted 3rd Party Doesn't Scale (But Blockchains Do) 08 Mar 2016 One Chain to Rule Them All 07 Mar 2016	OCTOBER 2017 Fork Futures (via the Exchanges) 12 Oct 2017	SEPTEMBER 2018 Expensive Privacy is Useless Privacy 11 Sep 2018 Five Lies and the Truth 11 Sep 2018	JANUARY 2021 OpenVote - Auditable, Fast, Private, Secure Voting 10 Jan 2021	APRIL 2023 Small Transactions 08 Apr 2023
JULY 2015 The Win-Win Blocksize Solution 14 Jul 2015	DECEMBER 2015 Salvaging the Blocksize Discussion, in Two Questions 28 Dec 2015	JULY 2017 Proof of Stake is Still Pointless 07 Jul 2017	JUNE 2018 BitAssets - A Digital Assets Sidechain 21 Jun 2018	JUNE 2019 The Consent of the Governed 21 Jun 2019	JUNE 2022 Map-Territory Epistemology (Part 5) 21 Jun 2019 Map-Territory Epistemology (Part 4) 21 Jun 2019 Map-Territory Epistemology (Part 3) 21 Jun 2019 Map-Territory Epistemology (Part 2) 21 Jun 2019 Map-Territory Epistemology (Part 1) 21 Jun 2019
MAY 2015 Bitcoin and Deflation, The Last Word 15 May 2015	NOVEMBER 2015 Drivechain - The Simple Two Way Peg 24 Nov 2015	JANUARY 2017 Blind Merged Mining 30 Jan 2017 Mining - Threat Model and Equilibrium Analysis 29 Jan 2017 The Mirage of Miner Centralization 28 Jan 2017 Upgrading 'Smart Contracts' to 'Wise Contracts' 11 Jan 2017 Two Types of Blockspace Demand 10 Jan 2017	APRIL 2018 Meditations on Fraud Proofs 14 Apr 2018 Blockchain Fusion (via Compensated Sidechains) 07 Apr 2018 Bitcoin Post-Maximalism 07 Apr 2018	APRIL 2022 Lightning Network -- Fundamental Limitations	OCTOBER 2021 Security Budget II, Low Fees, and Merged Mining
JANUARY 2015 BitUSD Isn't Worth The Trouble 29 Jan 2015	OCTOBER 2015 The Hashing Heart Attack 28 Oct 2015 PSA - Linking to a Blog Section 05 Oct 2015	DECEMBER 2016 Against the Hard Fork 06 Dec 2016 Better Fork Terminology 05 Dec 2016	MARCH 2018 GigaChain 20 Mar 2018	FEBRUARY 2019 Security Budget in the Long Run 14 Feb 2019	FEBRUARY 2021 Sidechain For BitNames/Logins/DNS, Taking
NOVEMBER 2014 The Limits of Blockchain Tech 28 Nov 2014 Altcoins Aren't Money, They're Bitcoin's Casino/Laundromat	SEPTEMBER 2015 Oracles are the Real Smart Contracts 21 Sep 2015 Measuring Decentralization 09 Sep 2015	MAY 2016 BTC Codex - The Digital Identity Sidechain 21 May 2016 The Drivechain OP Code 14 May 2016	NOVEMBER 2017 The UASF Contradiction 02 Nov 2017 The MAHF And Replay "Protection" 02 Nov 2017 More Terminology -- Forks and Splits 02 Nov 2017 Miners Don't Control Tx-Selection 02 Nov 2017 ASICBoost is Worthless 02 Nov 2017	DECEMBER 2018 Imposed Mutual-Exclusivity (IMEX) for Hard Forks 20 Dec 2018	DECEMBER 2018 Sidechains for Scaling -- Thunder Network
Long Live Proof-of-Work, Long Live Mining 16 Nov 2014 Active Decentralization 09 Nov 2014 Three Basics 06 Nov 2014				NOVEMBER 2018 Gradually Activated Replay Protection (GARP) - Toward Hard Forks that Don't Suck 13 Nov 2018 Deniability - Unilateral Transaction Meta-Privacy 09 Nov 2018	NOVEMBER 2018 Sidechains for Privacy -- zSide and Melt/Cast

My Big Break

ada

Sr. Member



Activity: 404

Merit: 318



in bitcoin we trust



price stability, lack of price/supply feedback & long run electrical cost

December 29, 2014, 12:21:39 AM

#1

Adam Back links to my blog – Dec 2014

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 can't 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 today's 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 can't 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 aren't 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

- Wrote “Truthcoin” whitepaper (decentralized oracle)
- Technical Talks
 - Scaling Bitcoin 1 2 & 3 -- Program Committee for #4
 - TabConf every year – keynoted in 2018
 - Bitcoin Wednesday – all around the globe (Toronto, Chicago, Amsterdam, etc)
 - BitDevs – Summer 2014 (NYC), Austin (May 2018)
 - Consensus Construct (2017, 2019); American Banker ; Qcon London (2017)
 - Bitcoin Miami 2019/2021/2022/2023 & Amsterdam
- Wrote BIPs 300 and 301.
- Countless Podcasts
- Financially Stableand therefore loyal to Nobody!! Bwahaha!!
(My loyalty is to Bitcoin only.)

Part 2 – Why Bip300

My Three Favorite Endorsements

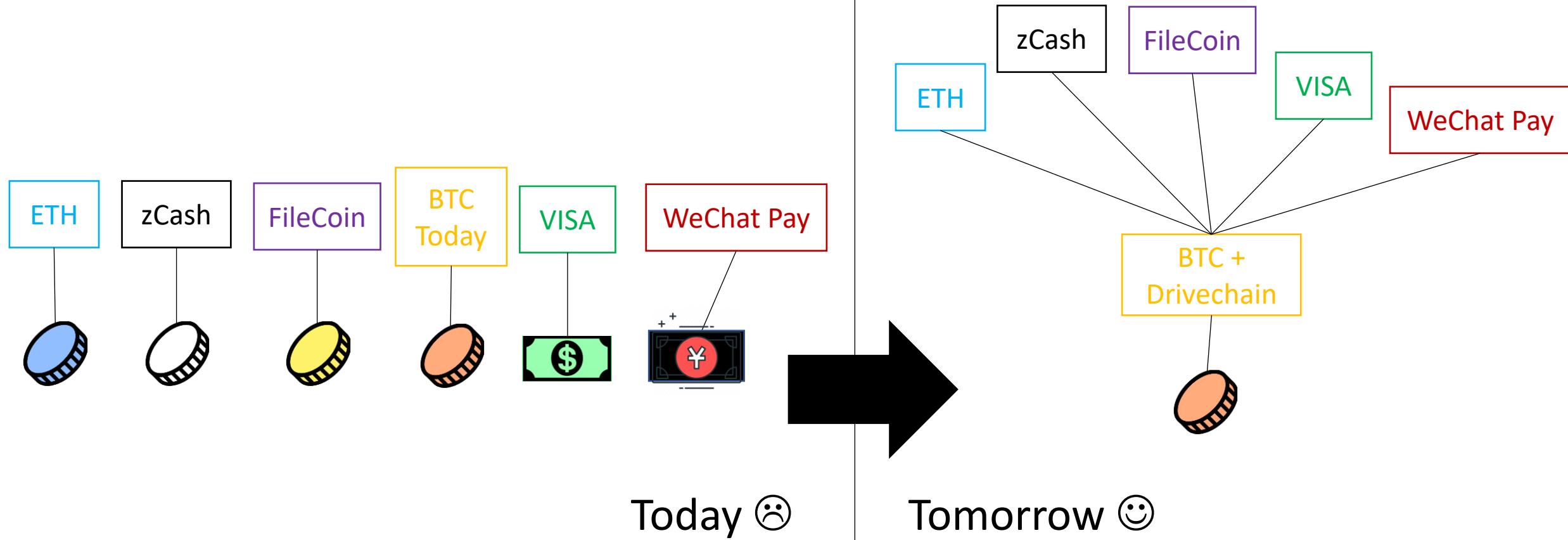
- "Drivechains...are pretty cool...and arguably could have been more important or useful than let's say Taproot."
- **Adam Back**, Baltic Honeybadger 2022, Live on stage in front of everyone
- “We need Drivechain or all the work of thousands in the last 13 years will be in vain.” ... “Drivechain is our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

Visit www.LayerTwoLabs.com/friends for 47 more!

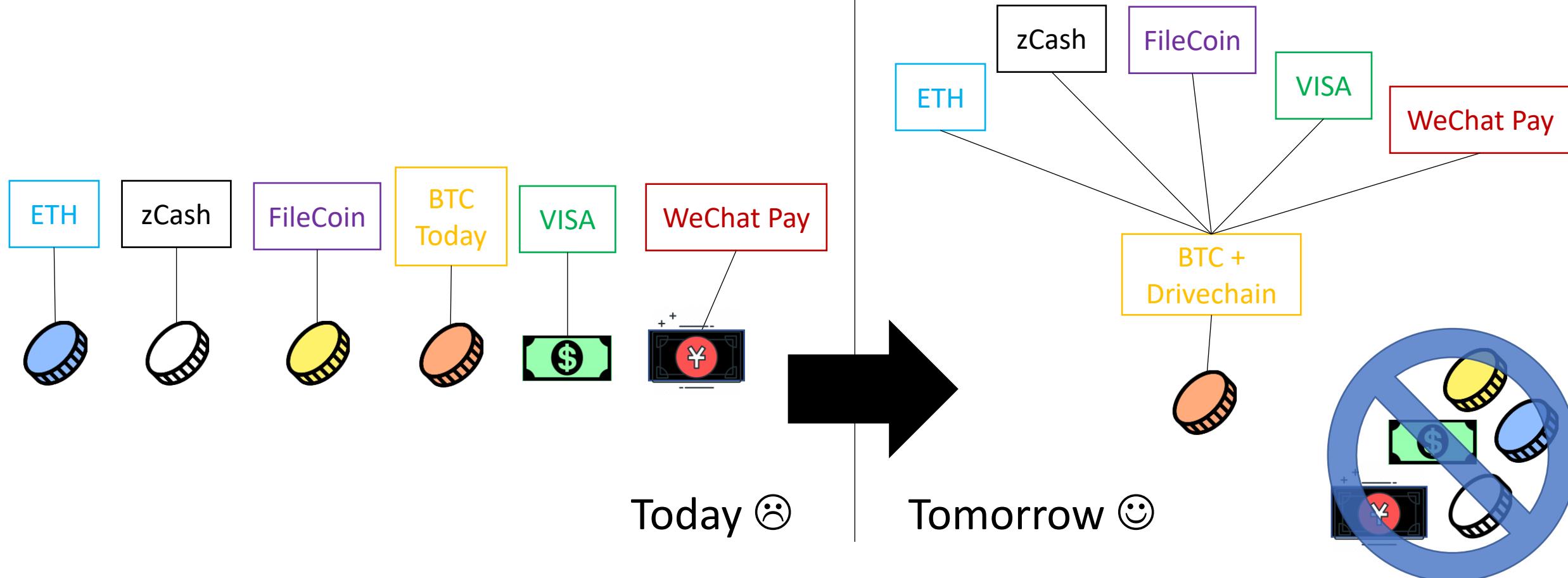
A Bold Claim

- 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!

BIP300: Everything on Top of Bitcoin



BIP300: Everything on Top of Bitcoin

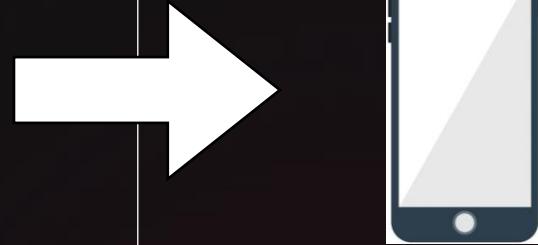


The Coming Death of Bitcoin's Competitors



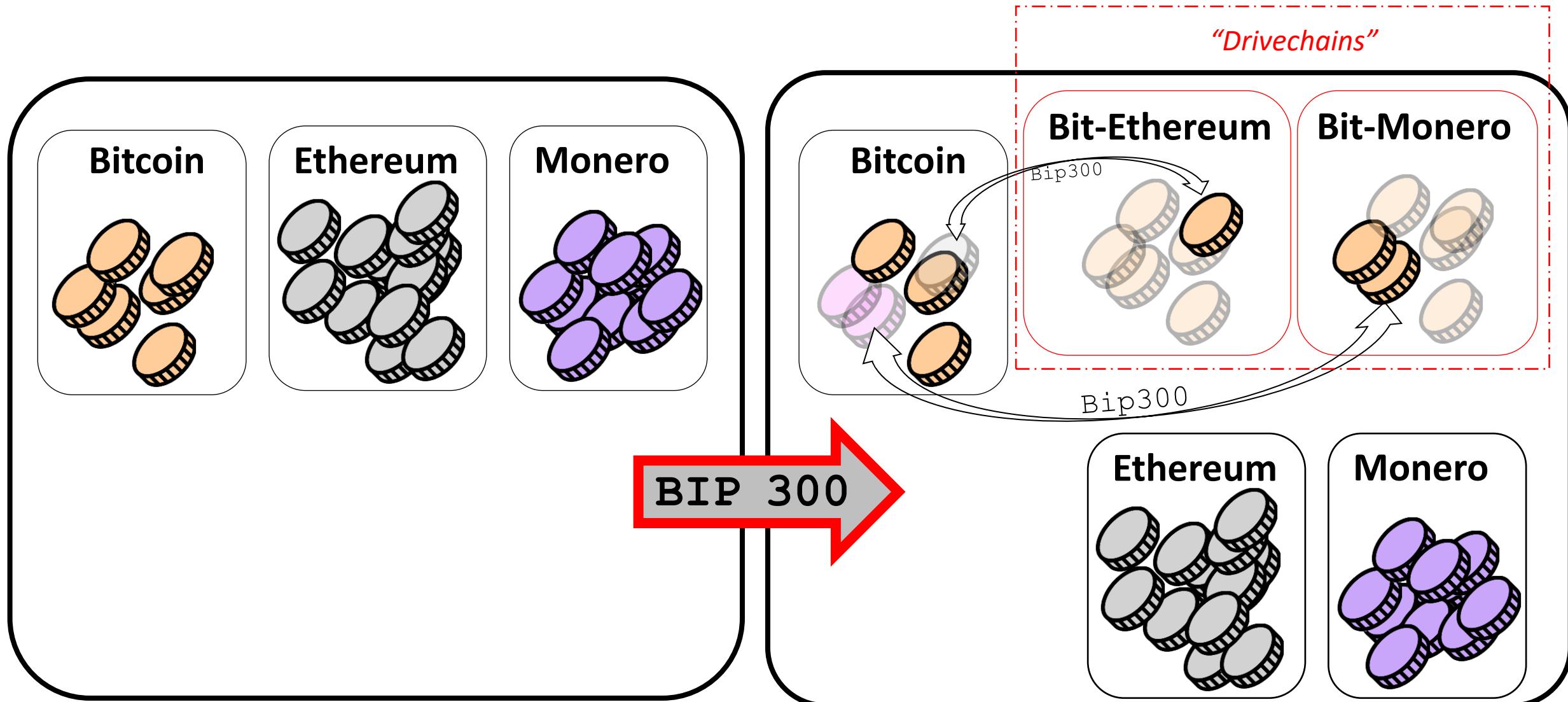
BTC
Today

WeChat Pay



BTC +
Drivechain

Drivechain = Altcoin Tech, BTC Coin Only



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!

A. Heterogeneity



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

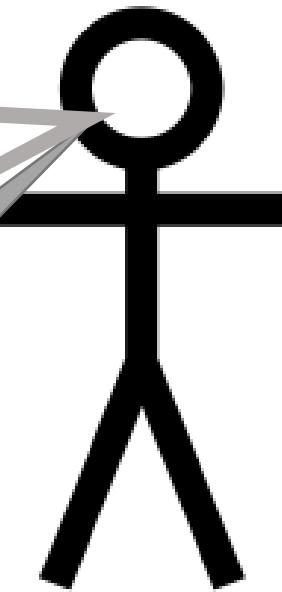
A. Heterogeneity



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

Different strokes for different folks.

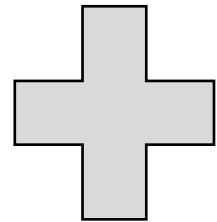
- BIP300 Solves All of Bitcoin's Biggest Problems

- 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... BitNames + Truthcoin ; examples
- H. ...zero risk to Bitcoin!

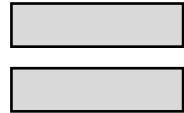
That “Zero Risk” Part

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

Bitcoin
Core v25



BIP 300
Softfork

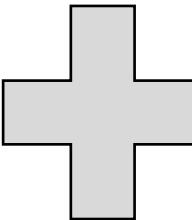


New Bitcoin
Core

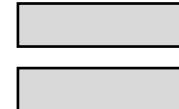
Interoperable
with Core v25

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.

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!

Scalability – Comparison to LN

* I assume that an automated hot-wallet is out of the question!

	Lightning N.	LB Drivechain
Onboard without Layer-1	No	Yes
Receive Payments while Offline*	No	Yes
Recover Wallet From Seed	No	Yes
Unlimited Liquidity	No	Yes
Option to use SPV Mode	No	Yes
Reckless	Yes	Yes
Txn Settles Instantly	Yes	No

...the primary advantage of LN is **fast settlement**, especially when both buyer and seller are online.
So, LN probably best for in-person retail; DC better for online shopping, perhaps.

Scalability – Fees

Onboard n users, each makes m payments, stay on L2.

	Lightning Network	Largeblock Drivechain
Extra Software	LN Node	SC Node (SPV option)
Onboard n Users	n Layer-1 txns	n Layer-2 txn
m Payments	..on LN	..on DC
L1 Base Fee	3*m	1
L2 Base Fee	0	1 + (n*m)
L2 Routing Fee	n*m	0

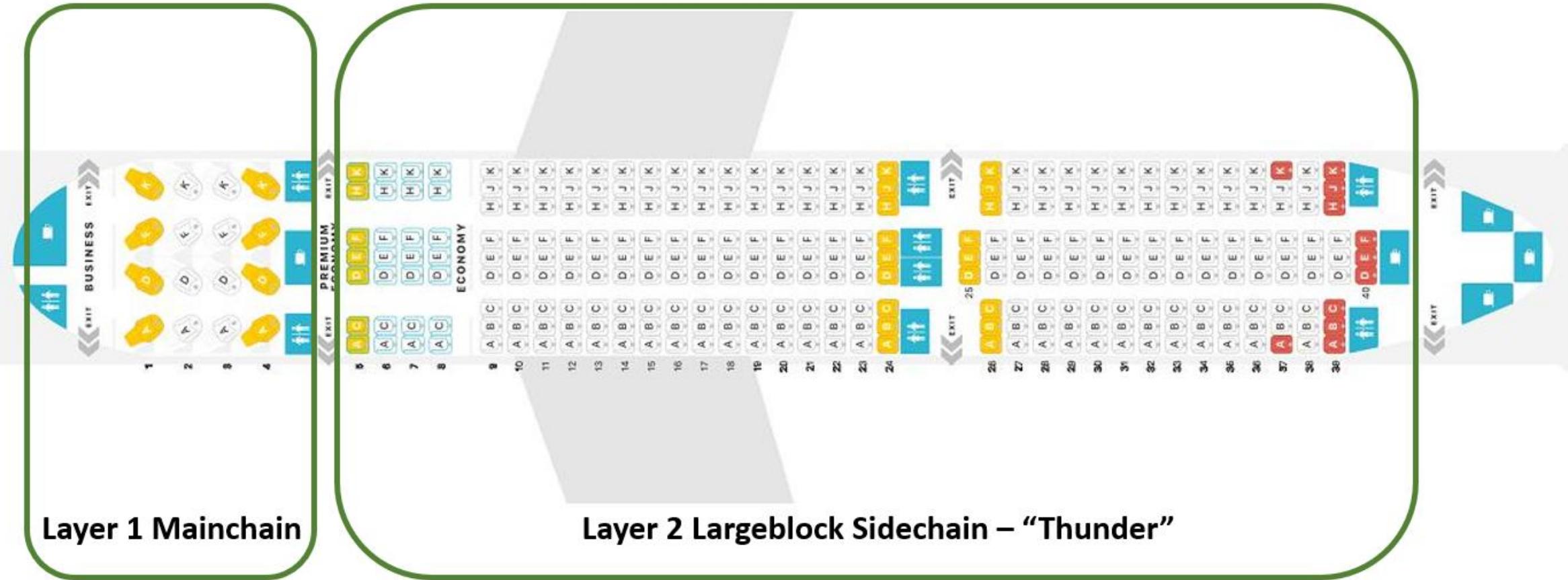
So, LN is only cheaper when there are many low-value payments. ie, LN is cheaper than BP, for **micropayments**.

Scalability – Fees

Onboard n users, each makes m payments, stay on L2.

	Lightning Network	Largeblock Drivechain
Extra Software	LN Node	SC Node (SPV option)
Onboard n Users	n Layer-1 txns	n Layer-2 txn
m Payments	..on LN	..on DC
L1 Base Fee	3*m	1
L2 Base Fee	0	1 + (n*m)
L2 Routing Fee	n*m	0
LN's micropayments require L1 fee-rates to be low, DC's do not.		
Smallest Payment	90% of L1 \$/txn fee	0% of L1 \$/txn fee

LargeBlocks?? What about Decentralization??



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

Fundamental Value – Namecoin

- Namecoin Enables:
 - 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.

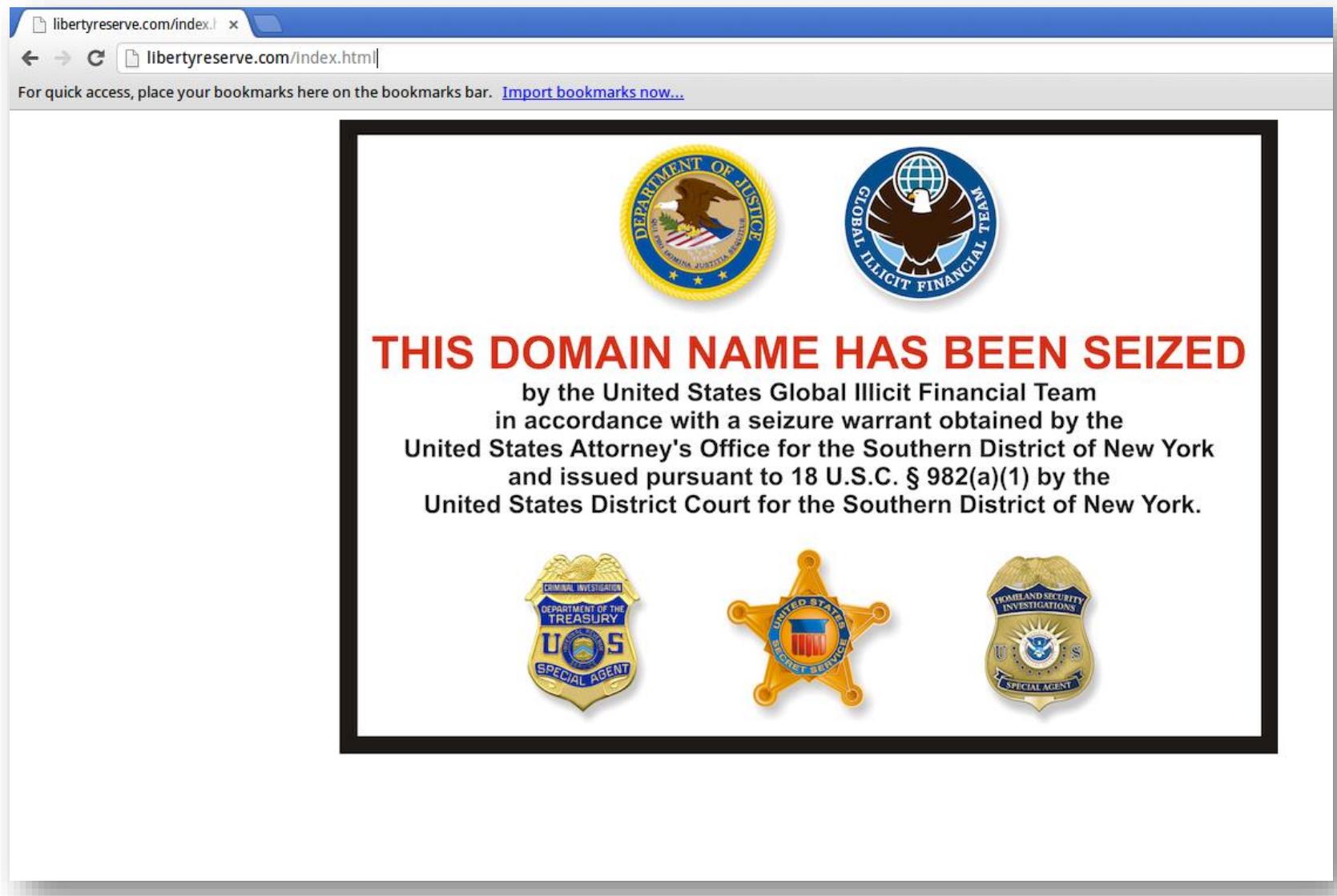
1 100 638

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

2 100 633

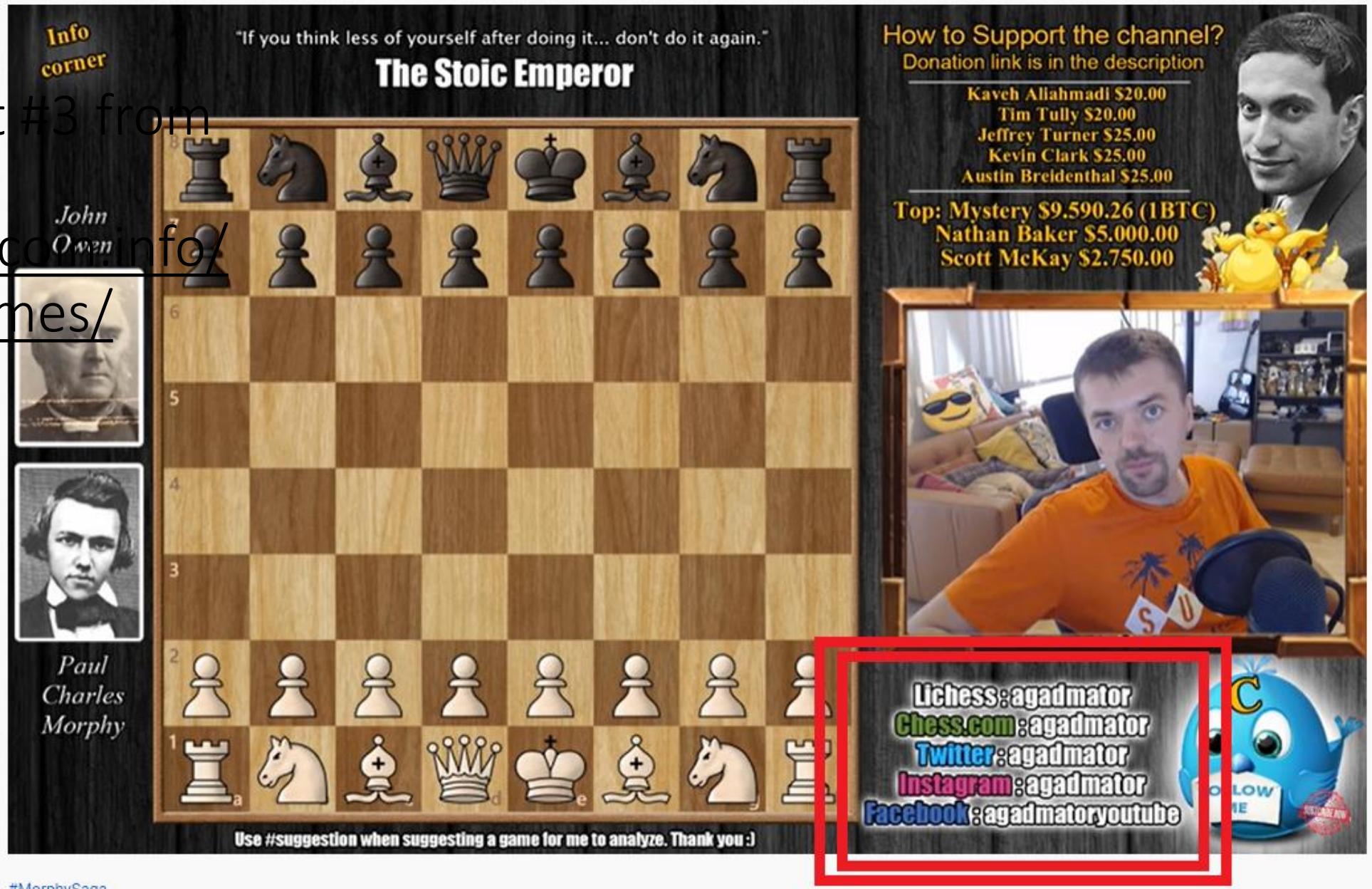
Screenshot #2 from

[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/)



Telegram: t.me/DclInsiders

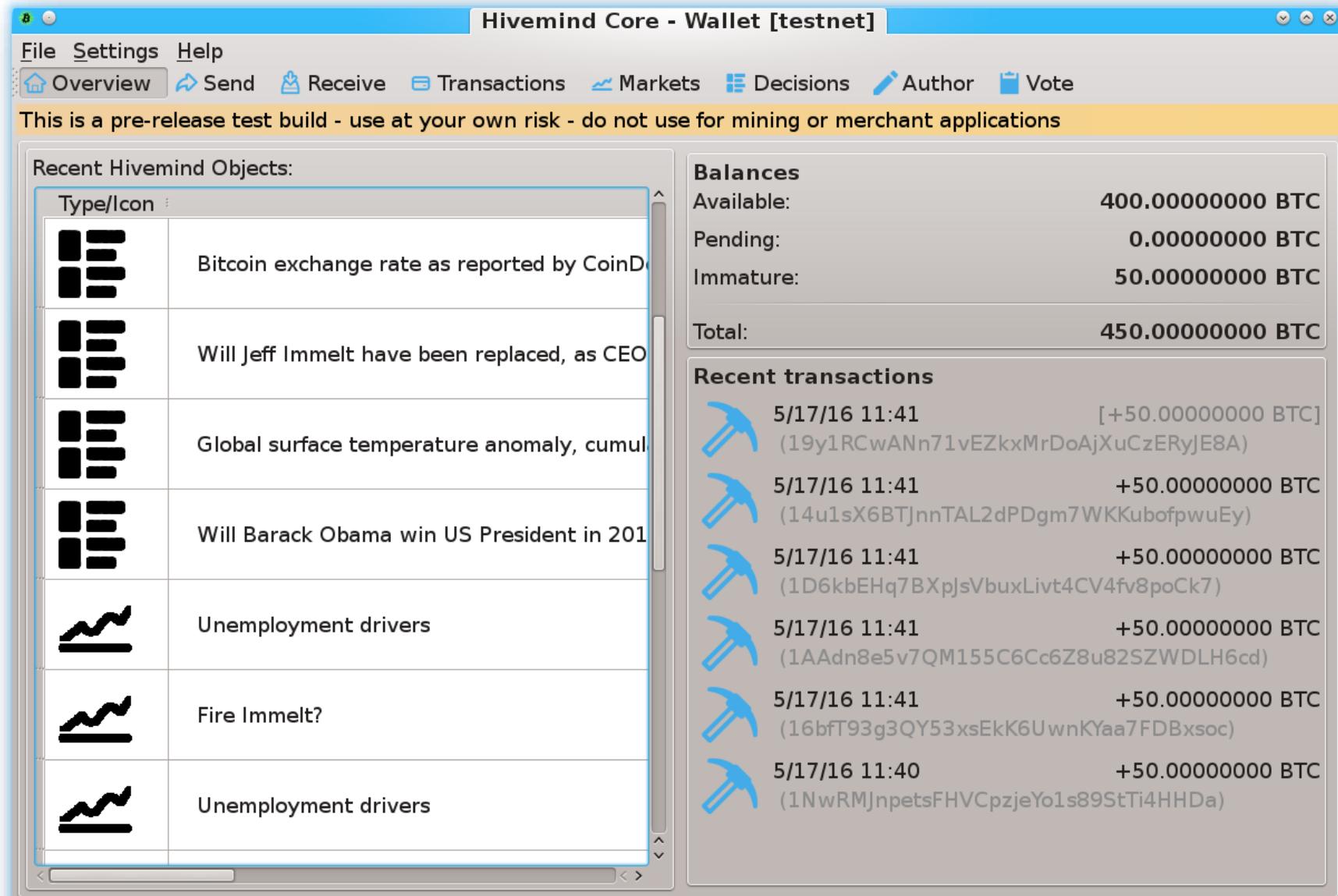
Website: www.drivechain.info

Paul's Twitter: [@truthcoin](https://twitter.com/truthcoin)

Prediction Markets

- Screenshots from my own BTC sidechain project

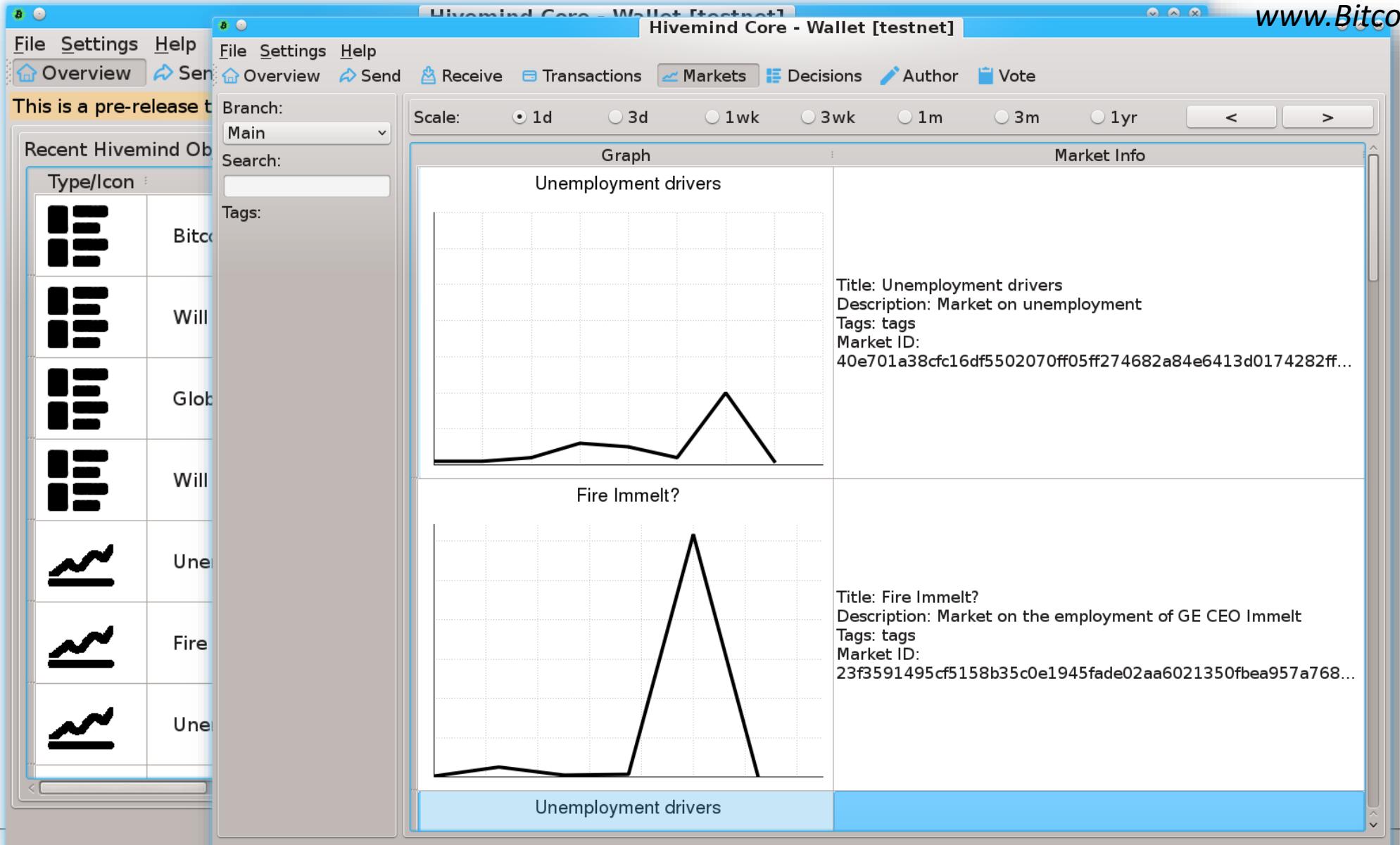
www.BitcoinHivemind.com



Prediction Markets

- Screenshots from my own BTC sidechain project

www.BitcoinHivemind.com



Prediction Markets

- Screenshots from my own BTC sidechain project

Trade www.BitcoinHivemind.com

Market ID: 40e701a38cf16df5502070ff05ff274682a84e6413d0174282ff54d45d0576c

Recent Hivemind Objects

Type/Icon	Name
	Bitcoin
	Will
	Glob
	Will
	Une
	Fire
	Une

Branch: Main

Scale:

Market Graph: 1 Month 1 Day 5 Minutes

Current Price: 0.00 Shares Owned: 0

Your trades:

Decision State: 0

Payout Address:

Shares to buy: 0 Trade Cost: 0 Balance: 0

Long (Buy) Short (Sell)

Make Order

Shares: 0

Price: 0.00

Telegram: t.m

Prediction Markets

- Screenshots from my own BTC sidechain project

The screenshot shows a software interface for a prediction market. On the left, there are two windows: one titled "Overview" and another titled "Send". The main window is titled "Trade" and displays a "Market Graph" for a specific market ID. The graph plots price against time, showing a series of green vertical bars representing price ranges and a grey line connecting circular markers representing price points. The x-axis is labeled with integers from 0 to 7, and the y-axis has labels at -4.5, 0, 4.5, 9, 13.5, 18, and 22.5. Above the graph, there are three radio buttons for "Market Graph": "1 Month" (selected), "1 Day", and "5 Minutes". Below the graph, there are input fields for "Shares Owned" (0.00) and "Shares to buy" (0). To the right of the graph, there is a section for placing an order, including fields for "Price" (0.00), "Decision State" (0), and "Payout Address". At the bottom right is a "Finalize" button with a checkmark icon. The URL "www.BitcoinHivemind.com" is visible at the top right of the main window.

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

File Settings Help
Overview Send Receive
This is a pre-release test build.
Recent Hivemind Objects

File Settings Help
Overview Send Receive
Branch: Main
Search:
Tags:

Market ID: 40e701a38cf16df5502070ff05ff274682a84e6413d0174282ff54d45d0576c

Standard Two Dimensional High Dimensional

Market Graph: 1 Month 1 Day 5 Minutes

Shares Owned: 0.00 Shares to buy: 0

Trade Cost: 0 Balance: 0

Long (Buy) Short (Sell)

Make Order ? Help

Shares: 0

-10 +10

Price: 0.00

Decision State: 0

Payout Address:

Finalize

Telegram: t.me/autonome

Part 4 – zCash Example

My hope: going through screenshots now, makes it easier to understand the BIP later.

The screenshot shows the DriveNet software interface. At the top, there is a menu bar with "File", "Tools", "Settings", and "Help". Below the menu is a toolbar with icons for "Overview", "Send", "Receive", "Transactions", and "Sidechains". The "Sidechains" tab is currently selected, indicated by a blue border around its icon. On the left side of the main window, there is a vertical list of 18 items, each consisting of a small icon followed by the text "Inactive". The items are numbered from 0 to 17. At the bottom of this list is a button labeled "Add / Remove". In the center of the main window, there is a message: "Sorry, no sidechains have been activated yet. Please check back later!". At the very bottom of the screen, there is a footer bar with the text "Make sidechain transfers and manage sidechain settings" on the left and "101 blocks | 0 peers | Last block: 0 seconds ago" on the right. The background of the main window is light gray, and the overall interface has a clean, modern look.

Take a “Slot”

A coinbase message announcing that we want to assign Slot 1: a global name, and some optional info to identify the L2 node software

Create Sidechain Proposal

Required

Slot # 21 Title ZSide

Optional but recommended

Description
ZCash as a Bitcoin sidechain

Version
0

Release tarball hash (256 bits)
8c2a146ad3b464e16e5065f84c6c54905b16ae97c72d8f

Build commit hash (160 bits)
7af8c02db761ffc05f240d02b03ad131c3307728

Propose Sidechain

DriveNet [regtest](Bitcoin Core)

File Tools Settings Help

Overview Send Receive Transactions Sidechains

0: Testchain 1: zSide 2: Inactive 3: Inactive 4: Inactive 5: Inactive 6: Inactive 7: Inactive 8: Inactive 9: Inactive 10: Inactive 11: Inactive

Make Deposits See Withdrawals

Sidechain Activation Management

Escrow Status (Active Sidechains)

#	Active	Name	Address	CTIP TxID	CTIP Index	Private Key
0	true	Testchain	sYXjof1Db8TFNLJ7dyQwWWnWAbhB99r	NA	NA	91jbRcYNm4Rpdy4u9
1	true	zSide	sh9xmjmHfUxrhy7Fyh8wjxoCb8me29YXQ	NA	NA	92jrVFaoWPBOr9ojeIN

Pending Sidechain Proposals

Vote	Title	Description	Age	Fails	Key	Script Hex

ACK NACK Create Sidechain Proposal

Drivechains are Proposed, and ACKed on L1
Each proposal / Ack is a message in a L1 coinbase txn

Deposit

- 1 -- Get destination address from zCash-Drivechain
- 2 -- Give that to L1
- 3 -- L1 broadcasts the deposit
- 4 -- After the deposit confirms on L1, L2 credits user the coins.

The screenshot shows two windows of the DriveNet testnet application. The left window is titled 'DriveNet [regtest](Bitcoin Core 0.16.99 + BIPs 300 and 301)' and shows a 'Sidechains' tab selected. It lists several sidechains, with 'zSide' highlighted. The main area shows a 'Make Deposits' form with the following details:

- An address you own on the sidechain you are depositing to: `51_tnE3CzZUjR16R76fMnUYdTbam3CLgN9kdEf_2386a3`
- Deposit: `1000.0000,0000` BTC
- Fee: `0.0040,0000` BTC
- Deposit button

The right window is titled 'zSide - Wallet [regtest]' and shows a 'Deposit to Sidechain' form. It includes a QR code and the same deposit details as the left window. A status message at the bottom says 'Connecting to peers...'.

zCash Features

Now we have a z-address to use!

The screenshot shows the ZSide - Wallet [regtest] interface. At the top, there is a menu bar with File, Settings, Help, and several tabs: Parent Chain, Overview, Send, Receive, Transactions, ZCash, and Melt / Cast. The ZCash tab is currently selected. Below the tabs, a yellow box highlights the text "Your Z Address: zregtestsapling13gh808t3fh6x3fd9leg0argk0q03uqkkjrhtermv7gnz62kc7uz0cp5rtxmlze2t9crk5veq6q".

The interface is divided into two main sections:

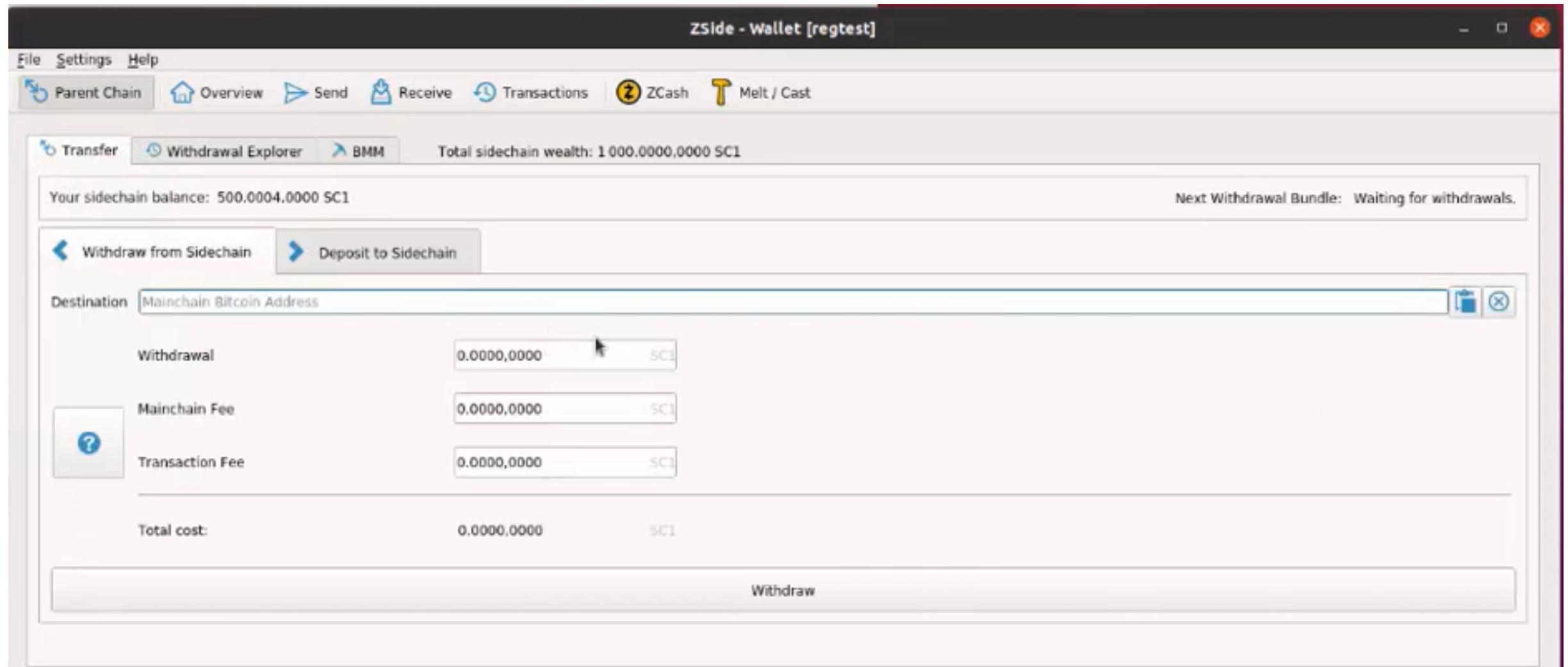
- Melt:** A section titled "Melt" with the sub-instruction "Click here to Melt ALL of your transparent Coins". It displays a table of available coins for melting:

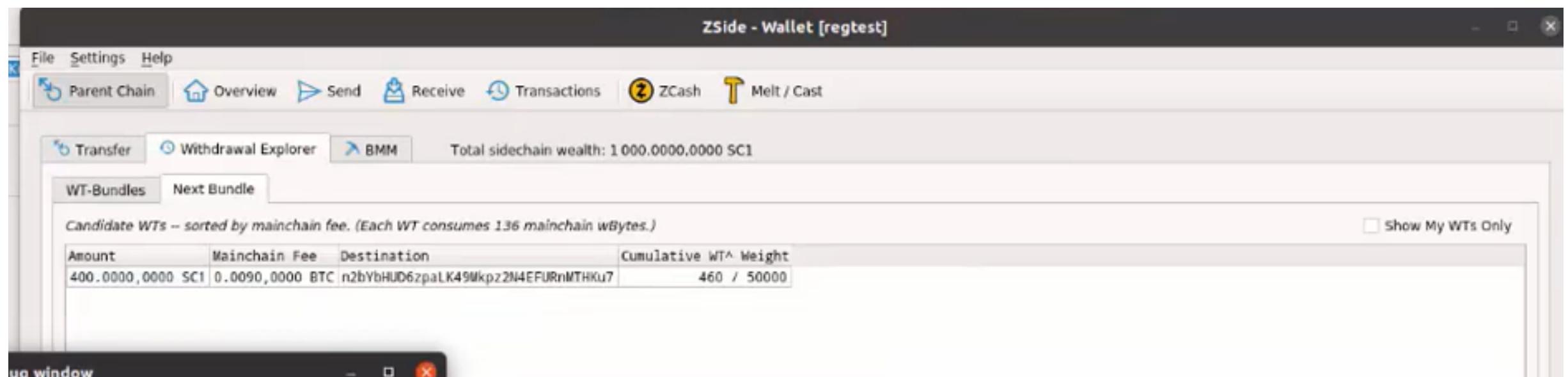
	Amount	Address	Date	# Conf
Melt	14.0000, 0.0000	t2NzaZerkhnQLEYjANV93aRKDCILH8nteUt	2/28/21 18:49	2
Melt	0.0000, 0.0000	tnTgeQD9u524XbftWFx4fDBCVCJcdkvAf76C	2/28/21 18:47	10
Melt	0.0001, 0.0000	tnELaa11GVH538R29trw4mn6gabBHfuKxyW	2/28/21 18:48	10
Melt	0.0001, 0.0000	tnQjDvvrVdwwzoaNsBJwGkcX69Yb3ZaJuW46	2/28/21 18:47	12
Melt	0.0001, 0.0000	tnT49oBjf4T97Gp01f5rNspZYfbraKJ4DDZ	2/28/21 18:50	2
- Cast:** A section titled "Cast" with the sub-instruction "Click here to Cast 95-100% of your z-value as 4 new Coins". It displays a table of scheduled casts:

	Bill	Amount	Broadcast Day	ETA
Cast		85.8993,4592	Monday	Tomorrow
Cast		21.4748,3648	Wednesday	3 Days
Cast		10.7374,1824	Thursday	4 Days
Cast		5.3687,0912	Friday	5 Days

At the bottom, it shows the current UTC time as Sun Feb 28 23:54:01, and indicates that no withdrawals are pending. There are also buttons for "What's Going On?", "Bills", and "Cancel".

Withdrawing Bit-Zcash to Layer1 BTC





ZSide - Wallet [regtest]

File Settings Help

[Parent Chain](#) [Overview](#) [Send](#) [Receive](#) [Transactions](#) [ZCash](#) [Melt / Cast](#)
[Transfer](#) [Withdrawal Explorer](#) [BMM](#)

Total sidechain wealth: 1 000.0000.0000 SC1

[WT-Bundles](#)[Next Bundle](#)

Candidate WTs -- sorted by mainchain fee. (Each WT consumes 1.36 mainchain wBytes.)

 Show My WTs Only

Amount	Mainchain Fee	Destination	Cumulative WT [^]	Weight
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu	460	/ 50000
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu	596	/ 50000
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu	732	/ 50000
400.0000,0000 SC1	0.0090,0000 BTC	n2bVbHUD67paLK49Wkpz2N4EFURnMTIKu7	868	/ 50000
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu	1004	/ 50000
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu	1140	/ 50000
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu	1276	/ 50000
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu	1412	/ 50000
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu	1548	/ 50000
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu	1684	/ 50000
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu	1820	/ 50000
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu	1956	/ 50000

A- A+

WT[^]: None yet. Waiting for withdrawals. | 29 blocks | 0 peers | Last block: 8 seconds ago

ZSide - Wallet [regtest]

File Settings Help

[Parent Chain](#) [Overview](#) [Send](#) [Receive](#) [Transactions](#) [ZCash](#) [Melt / Cast](#)
[Transfer](#) [Withdrawal Explorer](#) [BMM](#) Total sidechain wealth: 1 000.0000,0000 SC1
WT-Bundles [Next Bundle](#) Automatically update to latest

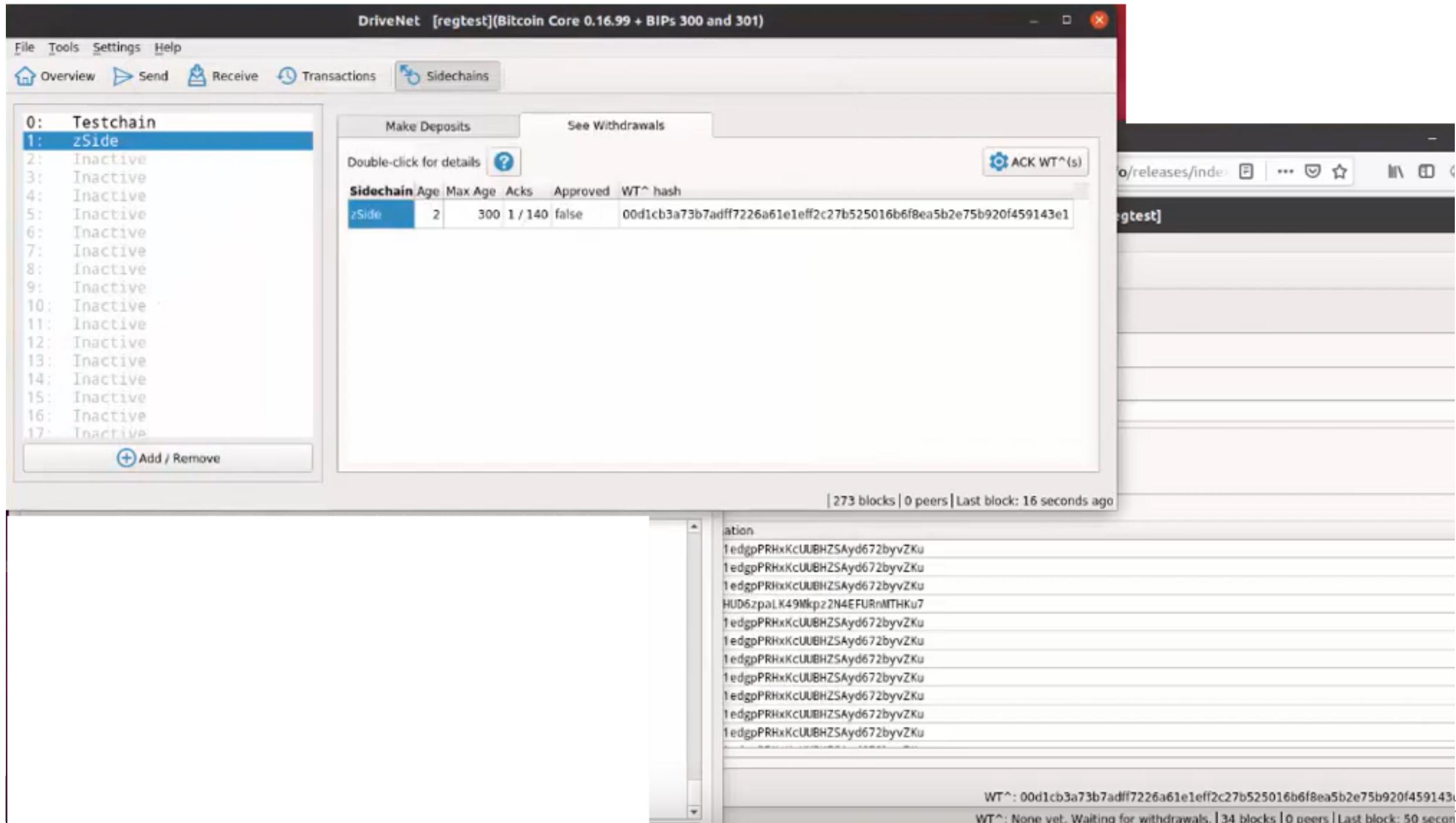
00d1cb3a73b7adff7226a61e1eff2c27b525016b6f8ea5b2e75b920f459143e1

[Withdrawal History](#)

Mainchain status: Created Total withdrawal amount: 411.1080,0000 SC1
 Numer of WT(s): 12 Total mainchain fees: 0.1080,0000 BTC
 Height created: 30 Total transaction size: 1964 / 50000 wBytes

WT(s) included:

Amount	Mainchain Fee	Destination
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu
400.0000,0000 SC1	0.0090,0000 BTC	n2bYbHUD6zpalK49Mkpz2N4EFURnMTHKu7
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu
1.0000,0000 SC1	0.0090,0000 BTC	n1gKa1edgpPRHxKcUUBHZSAyd672byvZKu



DriveNet [regtest](Bitcoin Core 0.16.99 + BIPs 300 and 301)

Coin Selection



Quantity: 0

Amount: 0.0000,0000 BTC

Fee: 0.0000,0000 BTC

After Fee: 0.0000,0000 BTC

Bytes: 0

Dust: NO

Change: 0.0000,0000 BTC

 (un)select all Tree mode List mode

	Amount	Received with label	Received with address	Date	Confirmations
<input type="checkbox"/>	25.0000,6240	(no label)	mpXp6jCUZaPXAyAcwosDA75WSBsVsX51id	2/28/21 18:49	166
<input type="checkbox"/>	0.0002,0000	(no label)	mpXp6jCUZaPXAyAcwosDA75WSBsVsX51id	2/28/21 18:49	166
<input type="checkbox"/>	49.9942,8300	(change)	2NDzs6s5bK5vPbgBBy7voLTuk3AcqB3xjHV	2/28/21 18:49	165
<input type="checkbox"/>	25.0000,6700	(no label)	n3gyMajMCHQYsXhKpAKCd1Z5v29FpYw5jt	2/28/21 18:50	165
<input type="checkbox"/>	0.0002,0000	(no label)	n3gyMajMCHQYsXhKpAKCd1Z5v29FpYw5jt	2/28/21 18:50	165
<input type="checkbox"/>	25.0000,6700	(no label)	mnutTNEqx9ppEnNzmf8wWYM6SP8rXM1Csf	2/28/21 18:50	164
<input type="checkbox"/>	0.0002,0000	(no label)	mnutTNEqx9ppEnNzmf8wWYM6SP8rXM1Csf	2/28/21 18:50	164
<input type="checkbox"/>	25.0000,6240	(no label)	mqkMRWyQDXL1tCUoCzcA5eWpEb9jVvymx9	2/28/21 18:50	163
<input type="checkbox"/>	0.0002,0000	(no label)	mqkMRWyQDXL1tCUoCzcA5eWpEb9jVvymx9	2/28/21 18:50	163
<input type="checkbox"/>	25.0000,3120	(no label)	mu5o5XaH5pZYSGmSbHVD41kX77AwNH4nA	2/28/21 18:54	162
<input type="checkbox"/>	0.0001,0000	(no label)	mu5o5XaH5pZYSGmSbHVD41kX77AwNH4nA	2/28/21 18:54	162
<input type="checkbox"/>	25.0000,6700	(no label)	mhrtYsHQ2LvScqTHmmdhYEj4d6bZTeb5jc	2/28/21 18:54	161
<input type="checkbox"/>	0.0002,0000	(no label)	mhrtYsHQ2LvScqTHmmdhYEj4d6bZTeb5jc	2/28/21 18:54	161
<input type="checkbox"/>	25.0000,6240	(no label)	mkXsujQ68La25iftEWbAN77m1ghLRZwNBS	2/28/21 18:54	160
<input type="checkbox"/>	0.0002,0000	(no label)	mkXsujQ68La25iftEWbAN77m1ghLRZwNBS	2/28/21 18:54	160
<input type="checkbox"/>	25.0000,6240	(no label)	myqcLangw8XCr5YdnZzQycBgEPgfoC47UE	2/28/21 19:01	159
<input type="checkbox"/>	0.0002,0000	(no label)	myqcLangw8XCr5YdnZzQycBgEPgfoC47UE	2/28/21 19:01	159
<input type="checkbox"/>	25.0000,6240	(no label)	n1sVjM6XDQDSrkkiZfQbKdtEvG5bqjcwXZ	2/28/21 19:01	158
<input type="checkbox"/>	0.0002,0000	(no label)	n1sVjM6XDQDSrkkiZfQbKdtEvG5bqjcwXZ	2/28/21 19:01	158
<input type="checkbox"/>	25.0000,3120	(no label)	mfZAQ2RczNFMMjrwytvgKijXMfuXKVRdAF	2/28/21 19:01	157
<input type="checkbox"/>	0.0001,0000	(no label)	mfZAQ2RczNFMMjrwytvgKijXMfuXKVRdAF	2/28/21 19:01	157

 OK

BIP300 – The Six Messages

BIP: 300

Layer: Consensus (soft fork)

Title: Hashrate Escrows (Consensus layer)

Author: Paul Sztorc <truthcoin@gmail.com>

CryptAxe <cryptaxe@gmail.com>

Comments-Summary: No comments yet.

Comments-URI: <https://github.com/bitcoin/bips/wiki/Comments:BIP-0300>

Status: Draft

Type: Standards Track

Created: 2017-08-14

License: BSD-2-Clause

Post-History: <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-May/014364.html>

Specification

Overview

Bip300 allows for six new blockchain messages (these have consensus significance):

- M1. "Propose New Sidechain"
- M2. "ACK Proposal"
- M3. "Propose Bundle"
- M4. "ACK Bundle"
- M5. Deposit -- a transfer of BTC from-main-to-side
- M6. Withdrawal -- a transfer of BTC from-side-to-main

Nodes organize those messages into two caches:

- D1. "The Sidechain List", which tracks the 256 Hashrate Escrows (Escrows are slots that a sidechain can live in).
- D2. "The Withdrawal List", which tracks the withdrawal-Bundles (coins leaving a Sidechain).

M1

Create Sidechain Proposal

Required

Slot # 21 Title ZSide

Optional but recommended

Description
ZCash as a Bitcoin sidechain

Version
0

Release tarball hash (256 bits)
8c2a146ad3b464e16e5065f84c6c54905b16ae97c72d8f

Build commit hash (160 bits)
7af8c02db761ffc05f240d02b03ad131c3307728

Propose Sidechain

Create Sidechain Proposal

Required

Slot # Title

Optional but recommended

```

cryptaxe@hal:~/Drivechain$ ./src/drivechain-cli help createsidechainproposal
createsidechainproposal
Generates a sidechain proposal to be included in the next block mined by this node.
Note that this will not broadcast the proposal to other nodes. You must mine a block which includes your proposal to complete the process.
Pending proposals created by this node will automatically be included in the soonest block mined possible.

Arguments:
1. "nsidechain" (numeric, required) sidechain slot number
2. "title" (string, required) sidechain title
3. "description" (string, optional) sidechain description
4. "version" (numeric, optional) sidechain / proposal version
5. "hashid1" (string, optional) 256 bits used to identify sidechain
6. "hashid2" (string, optional) 160 bits used to identify sidechain

Examples:
> drivechain-cli createsidechainproposal 1 "Namecoin" "Namecoin as a Bitcoin sidechain" 0 78b140259d5626e17c4bf339c23cb4fa8d16d138f71d9803ec394bb01c051f0b 90869d013db27608c7428251c6755e5a1d9e9313

> curl --user myusername --data-binary '{"jsonrpc": "1.0", "id":"curltest", "method": "createsidechainproposal", "params": [1 "Namecoin" "Namecoin as a Bitcoin sidechain" 0 78b140259d5626e17c4bf339c23cb4fa8d16d138f71d9803ec394bb01c051f0b 90869d013db27608c7428251c6755e5a1d9e9313]}' -H 'content-type: text/plain;' http://127.0.0.1:8332/

```

```

cryptaxe@hal:~/Drivechain$ ./src/drivechain-cli createsidechainproposal 1 "Namecoin" "Namecoin as a Bitcoin sidechain" 0 78b140259d5626e17c4bf339c23cb4fa8d16d138f71d9803ec394bb01c051f0b 90869d013db27608c7428251c6755e5a1d9e9313
{
  "nSidechain": 1,
  "title": "Namecoin",
  "description": "Namecoin as a Bitcoin sidechain",
  "privatekey": "5JPj0snCe69m5S6JFahcc6AQsDEoRadje4LZj4dmGkv2EfPFKma",
  "keyid": "c6fb9b51c3883fb3d5f41a3d930fadca7ca3483",
  "version": 0,
  "hashID1": "78b140259d5626e17c4bf339c23cb4fa8d16d138f71d9803ec394bb01c051f0b",
  "hashID2": "90869d013db27608c7428251c6755e5a1d9e9313"
}

```

Propose Sidechain

M2

M2 -- ACK Sidechain Proposal

M2 is a coinbase OP_RETURN output containing the following:

```
1-byte - OP_RETURN (0x6a)
4-byte - Message header (0xD6E1C5BF)
32-byte - sha256D hash of sidechain's serialization
```

Notes

The new M1/M2 validation rules are:

1. Any miner can propose a new sidechain (M1) at any time. This procedure resembles BIP 9 soft fork activation: the network must see a properly-formatted M1, followed by "acknowledgment" of the sidechain (M2) in 90% of the following 2016 blocks.
2. Bip300 comes with only 256 sidechain-slots. If all are used, it is possible to "overwrite" a sidechain. This requires vastly more M2 ACKs -- 50% of the following 26300 blocks must contain an M2. The possibility of overwrite, does not change the Bip300 security assumptions (because we already assume that the sidechain is vulnerable to miners, at a rate of 1 catastrophe per 13150 blocks).

Notes on Withdrawing Coins

Notes on Withdrawing Coins

Bip300 withdrawals ("M6") are very significant.

In Drivechain, "Bundles" are very important!

For an M6 to be valid, it must be first "prepped" by one M3 and then 13,150+ M4s. M3 and M4 are about "Bundles".

What are Bundles?

Sidechain withdrawals take the form of "Bundles" -- named because they "bundle up" many individual withdrawal-requests into a single rare layer1 transaction.

Sidechain full nodes aggregate the withdrawal-requests into a big set. The sidechain calculates what M6 would have to look like, to pay all of these withdrawal-requests out. Finally, the sidechain calculates what the hash of this M6 would be. This 32-byte hash identifies the Bundle.

This 32-byte hash is what miners will be slowly ACKing over 3-6 months, not the M6 itself (nor any sidechain data, of course).

A bundle either pays all its withdrawals out (via M6), or else it fails (and pays nothing out).

Bundle Hash = Blinded TxID of M6

The Bundle hash is static as it is being ACKed. Unfortunately, the M6 TxID will be constantly changing -- as users deposit to the sidechain, the input to M6 will change.

To solve this problem, we do something conceptually similar to AnyPrevOut (BIP 118). We define a "blinded TxID" as a way of hashing a txn, in which some bytes are first overwritten with zeros. These are: the first input and the first output. Via the former, a sidechain can accept deposits, even if we are acking a TxID that spends from it later. Via the latter, we can force all of the non-withdrawn coins to be returned to the sidechain (even if we don't yet know how many coins this will be).

M3

M3 -- Propose Bundle

M3 is a coinbase OP Return output containing the following:

```
1-byte - OP_RETURN (0x6a)
4-byte - Commitment header (0xD45AA943)
32-byte - The Bundle hash, to populate a new D2 entry
```

The new validation rules pertaining to M3 are:

1. If the network detects a properly-formatted M3, it must add an entry to D2 in the very next block. The starting "Blocks Remaining" value is 26,299. The starting ACKs count is 1.
2. Each block can only contain one M3 per sidechain.

Once a Bundle is in D2, how can we give it enough ACKs to make it valid?

M4

M4 -- ACK Bundle(s)

M4 is a coinbase OP Return output containing the following:

```
1-byte - OP_RETURN (0x6a)
4-byte - Commitment header (0xD77D1776)
1-byte - Version
n-byte - The vector describing the "upvoted" bundle-choice, for each sidechain.
```

Version 0x01 uses one byte per sidechain, and applies in most cases. Version 0x02 uses two bytes per sidechain and applies in unusual situations where at least one sidechain has more than 256 distinct withdrawal-bundles in progress at one time. Other interesting versions are possible: 0x03 might say "do exactly what was done in the previous block" (which could consume a fixed 6 bytes total, regardless of how many sidechains). 0x04 might say "upvote everyone who is clearly in the lead" (which also would require a mere 6 bytes), and so forth.

If a sidechain has no pending bundles, then it is skipped over when M4 is created and parsed.

The upvote vector will code "abstain" as 0xFF (or 0xFFFF); it will code "alarm" as 0xFE (or 0xFFFFE). Otherwise it simply indicates which withdrawal-bundle in the list, is the one to be "upvoted". For example, if there are two sidechains, and we wish to upvote the 7th bundle on sidechain #1 plus the 4th bundle on sidechain #2, then the vector would be 0x0704.

The M4 message will be invalid (and invalidate the block), if it tries to upvote a Bundle that doesn't exist (for example, trying to upvote the 7th bundle on sidechain #2, when sidechain #2 has only three bundles). If there are no Bundles at all (no one is trying to withdraw from any sidechain), then *any* M4 message present in the coinbase will be invalid. If M4 is NOT present in a block, then it is treated as "abstain".

The ACKed withdrawal will gain one point for its ACK field. Therefore, the ACK-counter of any Bundle can only change by (-1,0,+1).

Within a sidechain-group, upvoting one Bundle ("+1") requires you to downvote all other Bundles in that group. However, the minimum ACK-counter is zero. While only one Bundle can be upvoted at once; the whole group can all be unchanged at once ("abstain"), and they can all be downvoted at once ("alarm").

Finally, we describe Deposits and Withdrawals.

M5 – Depositing Coins

M5 -- Deposit BTC to Sidechain

Both M5 and M6 are regular Bitcoin txns. They are distinguished from regular txns (non-M5 non-M6 txns), when they select one of the special Bip300 CTIP UTXOs as one of their inputs (see D1).

All of a sidechain's coins, are stored in one UTXO, called the "CTIP". Every time a deposit or withdrawal is made, the CTIP changes. Each deposit/withdrawal will select the sidechains CTIP, and generate a new CTIP. (Deposits/Withdrawals never cause UTXO bloat.) The current CTIP is cached in D1 (above).

If the **quantity of coins**, in the from-CTIP-to-CTIP transaction, goes **up**, (ie, if the user is adding coins), then the txn is treated as a Deposit (M5). Else it is treated as a Withdrawal (M6). See [here](#).

As far as mainchain consensus is concerned, all deposits to a sidechain are always valid.

M6

M6 -- Withdraw BTC from a Sidechain

We come, finally, to the critical matter: where users can take their money *out* of the sidechain.

First, M6 must obey the same CTIP rules of M5 (see immediately above).

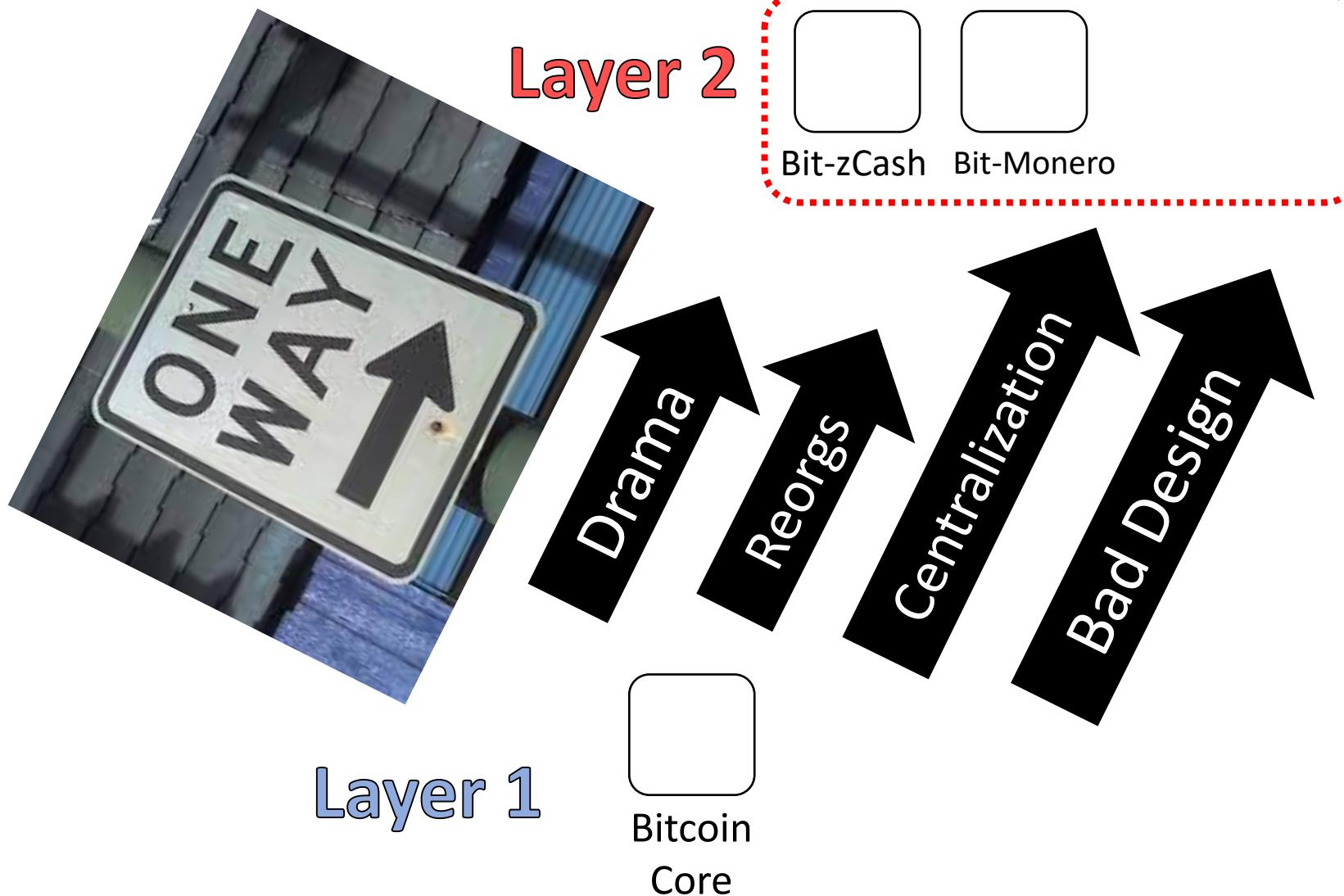
Second, an M6 is only valid for inclusion in a block, if its blinded TxID matches an "approved" Bundle hash (ie, one with an ACK score of 13150+). In other words, an M6 can only be included in a block, after the 3+ month (13150 block) ceremony.

Third, M6 must meet two accounting criteria, lest it be invalid:

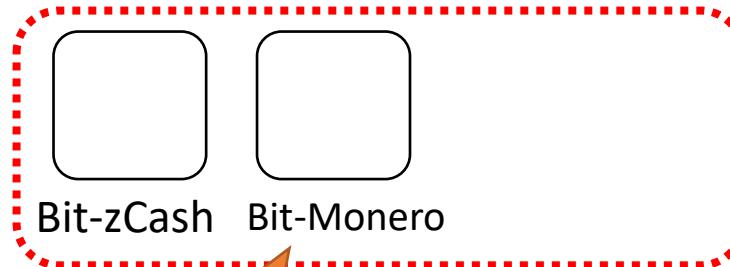
1. "Give change back to Escrow" -- The first output, TxOut0, must be paid back to the sidechain's Bip300 script. In other words, all non-withdrawn coins must be paid back into the sidechain.
2. "No traditional txn fee" -- For this txn, the sum of all inputs must equal the sum of all outputs. No traditional tx fee is possible. (Of course, there is still a txn fee for miners: it is paid via an OP TRUE output in the Bundle.) We want the withdraw-ers to set the fee "inside" the Bundle, and ACK it over 3 months like everything else.

Some Theory

The “One Way Street”



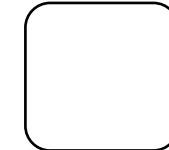
The “One Way Street”



Bip300
Drivechains

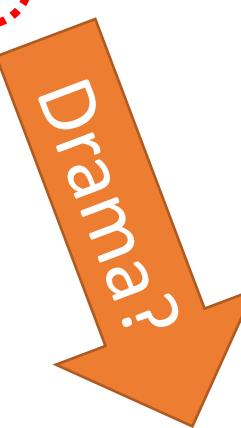
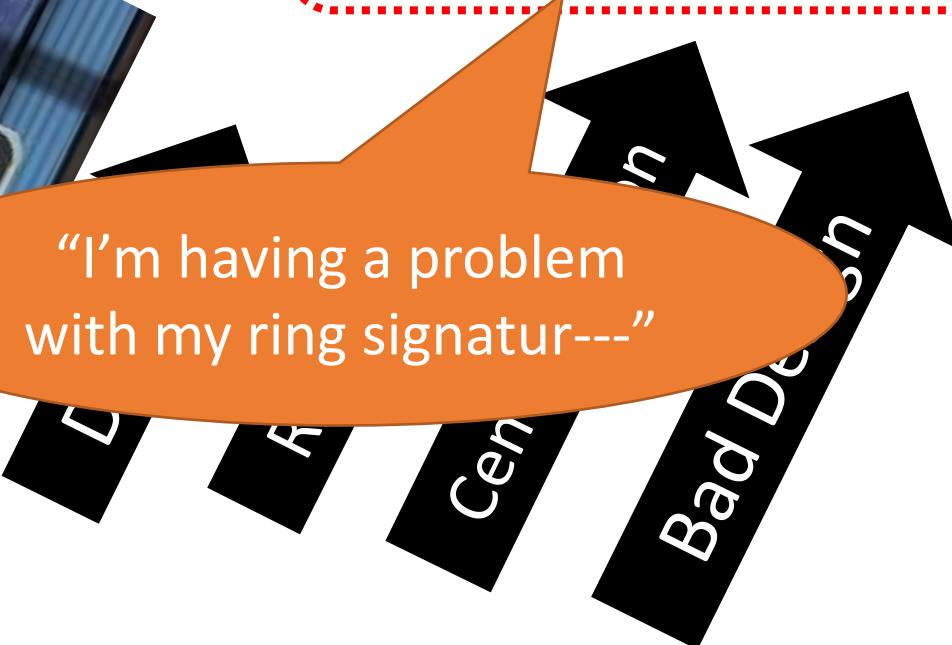
Layer 2

Layer 1

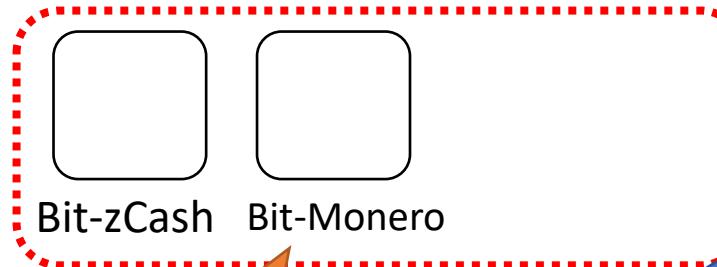


Bitcoin
Core

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



The “One Way Street”



Bip300
Drivechains



Layer 2

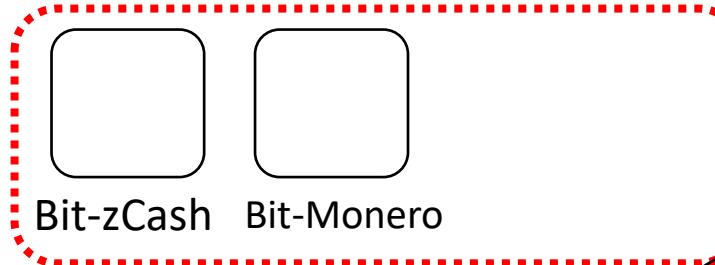
Layer 1

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

Can’t hear you,
sorry.



The “One Way Street”



Bip300
Drivechains
Layer 2

Sigma
args
Centralization
Bad Design

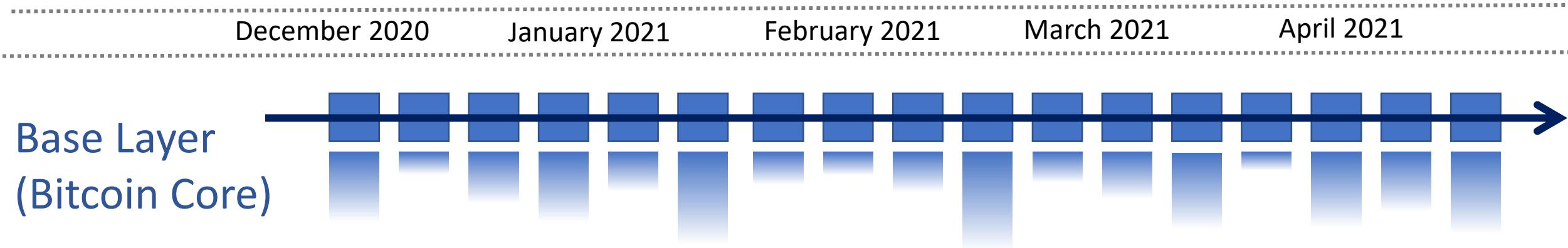


What's that??
Oh Sorry can't hear you.
Enjoying my music over
here.



Layer 1

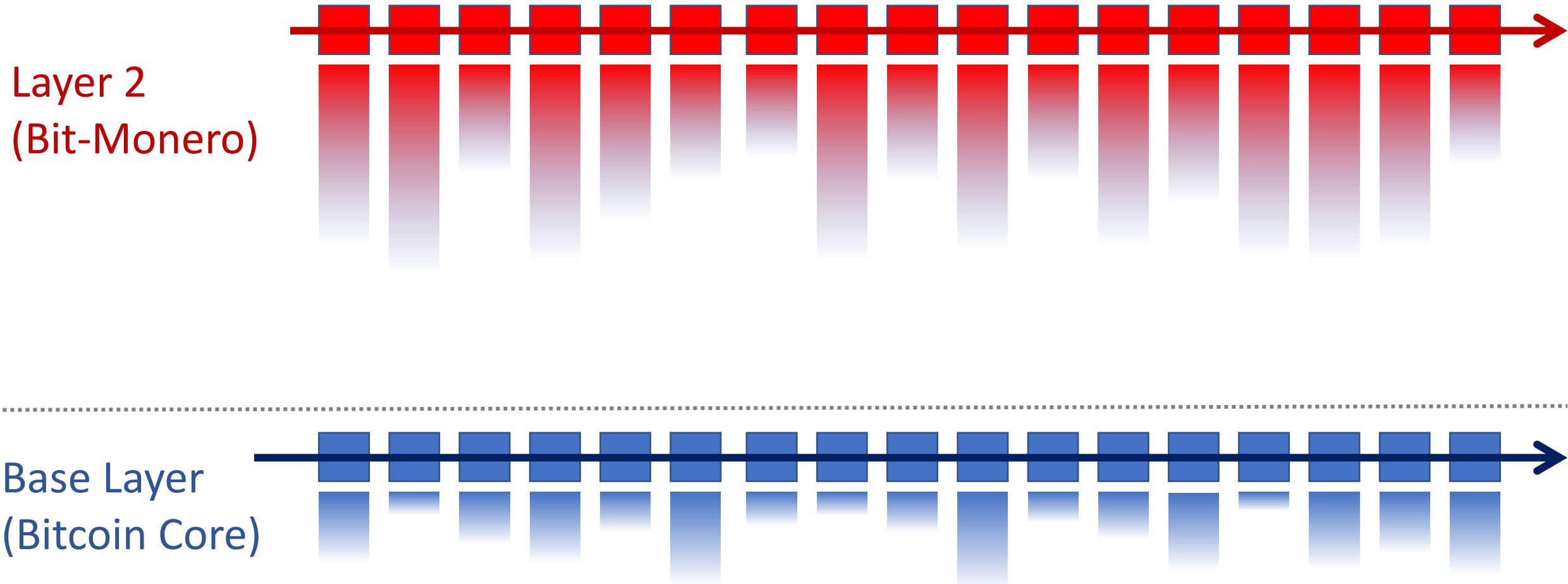
Putting Hash(L2) into L1



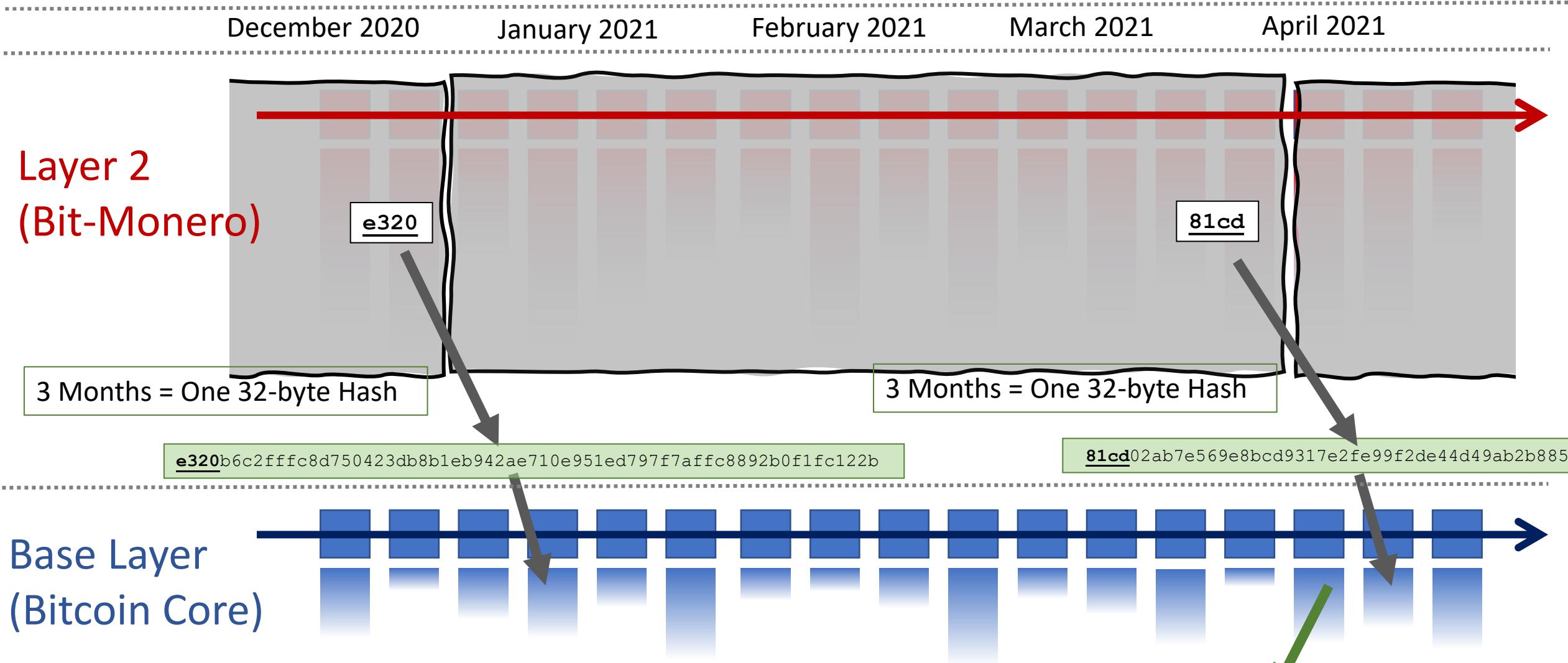
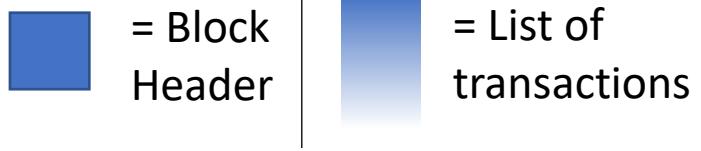
Putting Hash(L2) into L1



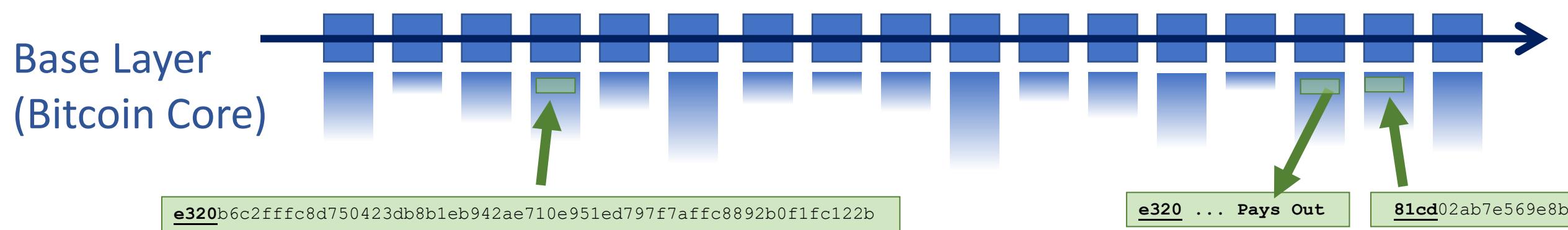
December 2020 January 2021 February 2021 March 2021 April 2021



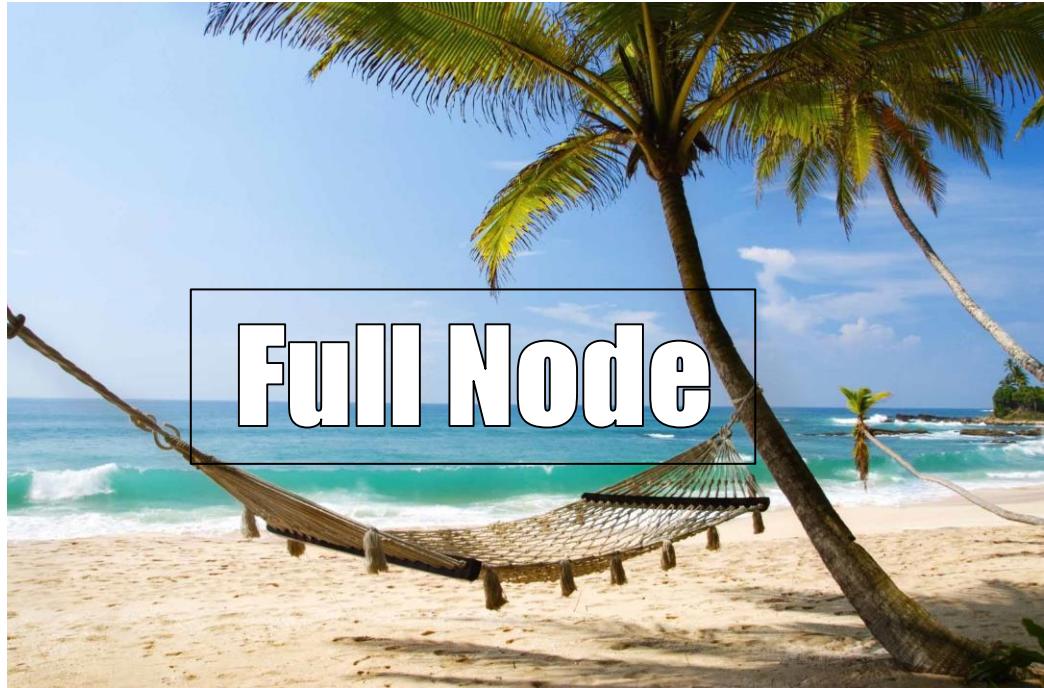
Putting Hash(L2) into L1



Putting Hash(L2) into L1 Your Layer 1 Node Sees...



But then how is it secure??



Full Node

Validating L1

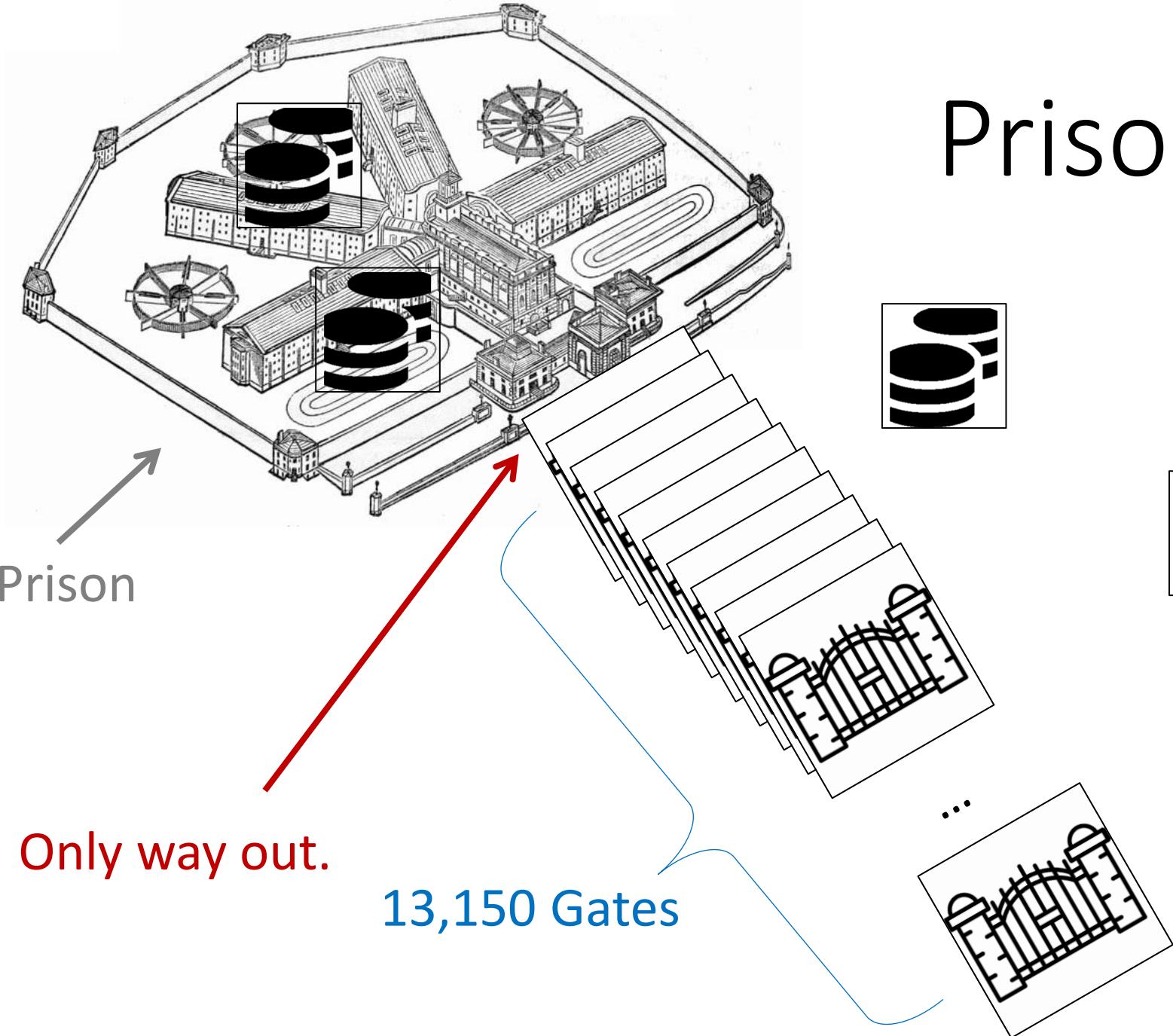
+ counting to 13,150



Miners
**Optimizing:
kWh / \$ / ASIC Efficiency / Cooling
/ Labor /
Demand Management Programs /
Drying Fruit / Getting NatGas
Credits / Outcompeting All Rivals**

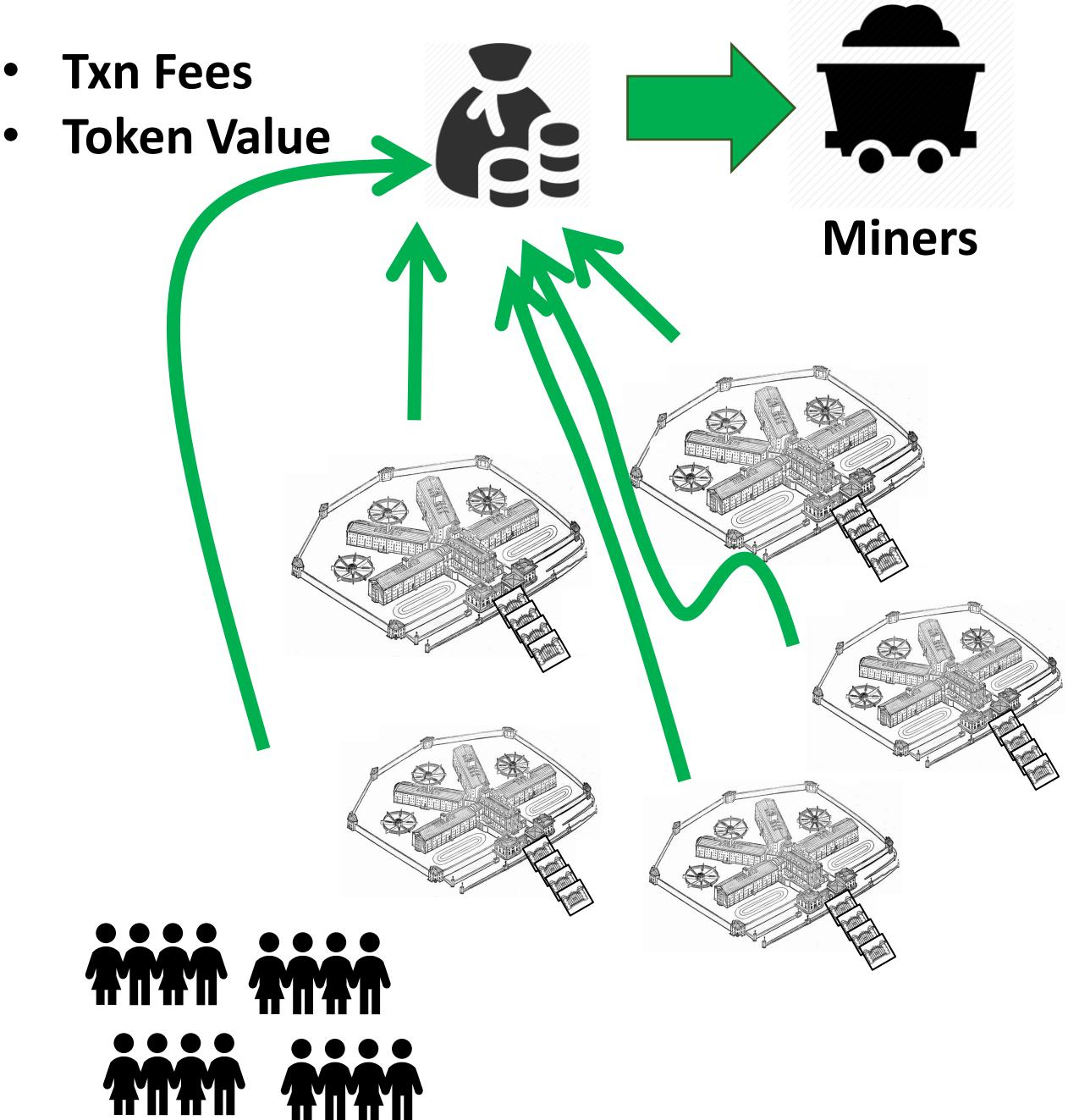
+ add/remove/validate Sidechains

Prison Metaphor



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:

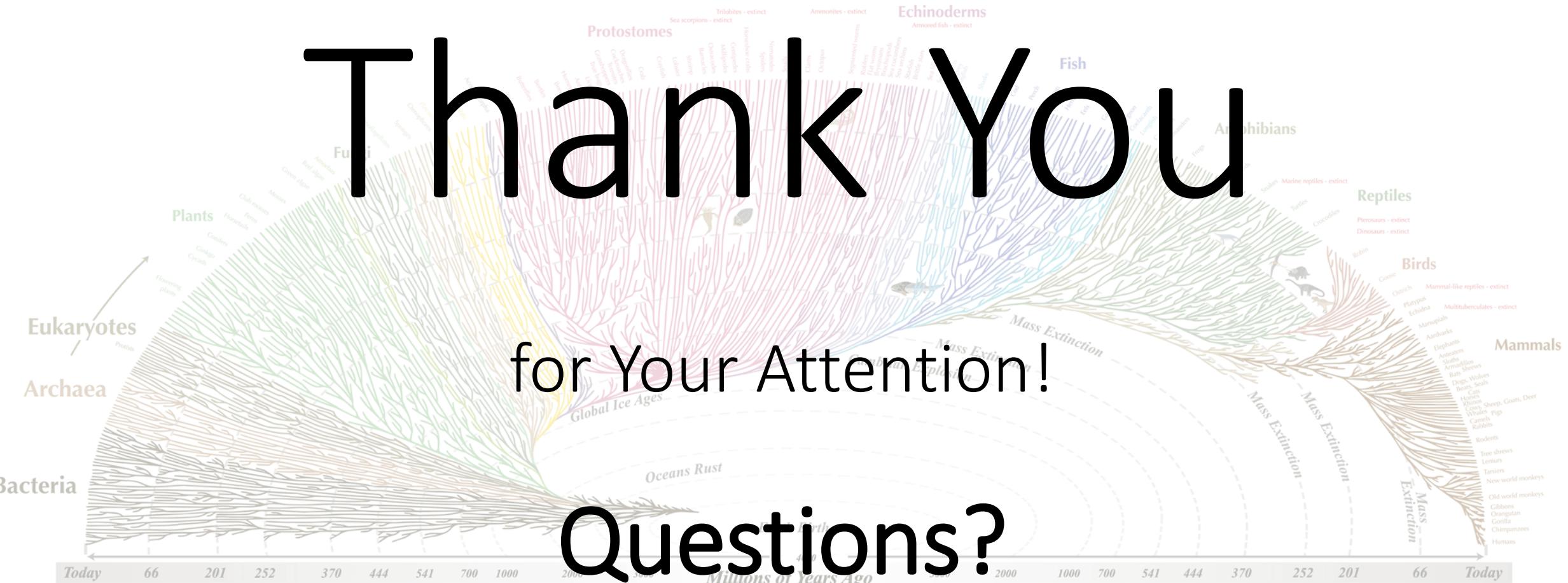
- Steal from LN channels – by censoring the justice txn
- Reorg mainchain Bitcoin txns out, and hold them hostage
- Block any message from L1 – including zk-proofs

- So, marginally, it is not actually very large an assumption.

The image features a large, bold, black 'Thank You' text centered in the foreground. Behind the text is a detailed phylogenetic tree of life, showing the evolutionary relationships between various organisms. The tree is color-coded by clade, with major groups like Protostomes (pink), Ecdysozoans (yellow), and Deuterostomes (blue) clearly visible. Numerous scientific names of organisms are written along the branches of the tree, including Cnidarians, Bilateria, Annelids, Molluscs, Crustaceans, Insects, Fish, and Vertebrates. The tree extends from a central root node at the bottom left towards the top right, with labels for specific species and groups placed near their respective branches.

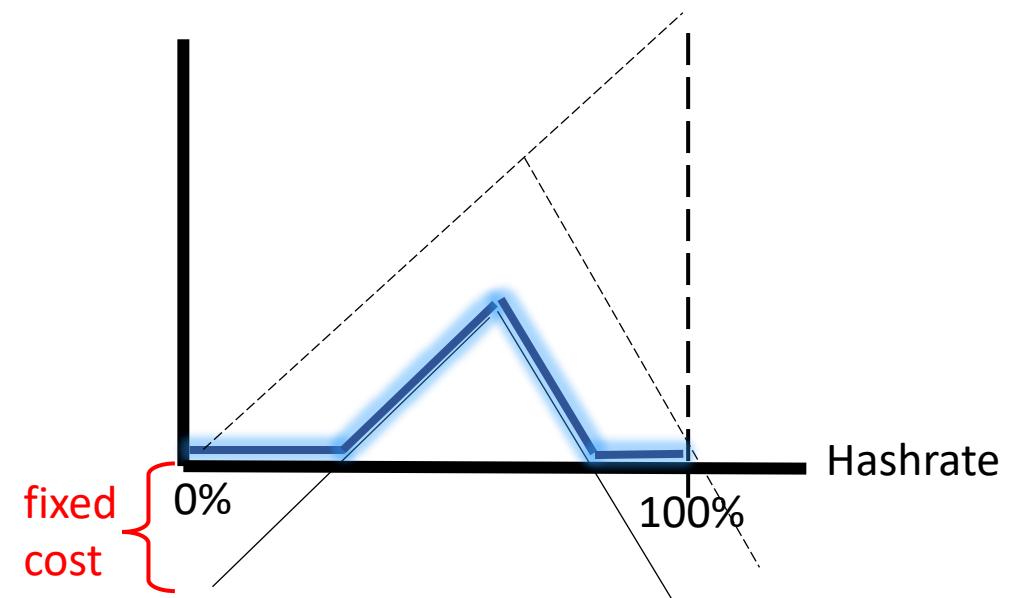
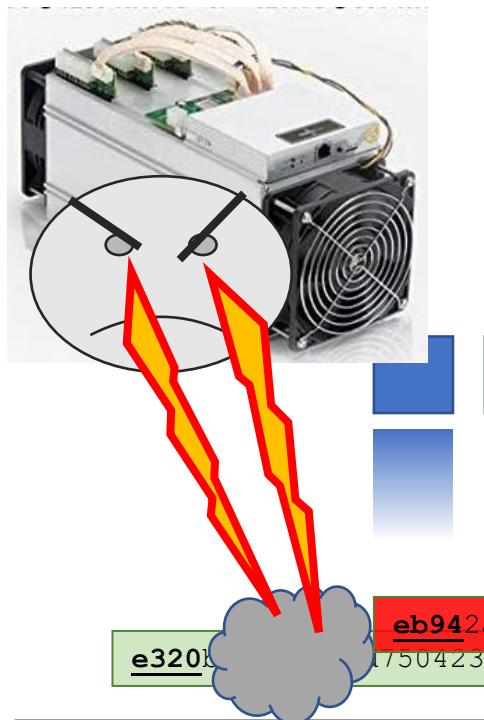
for Your Attention!

Questions?

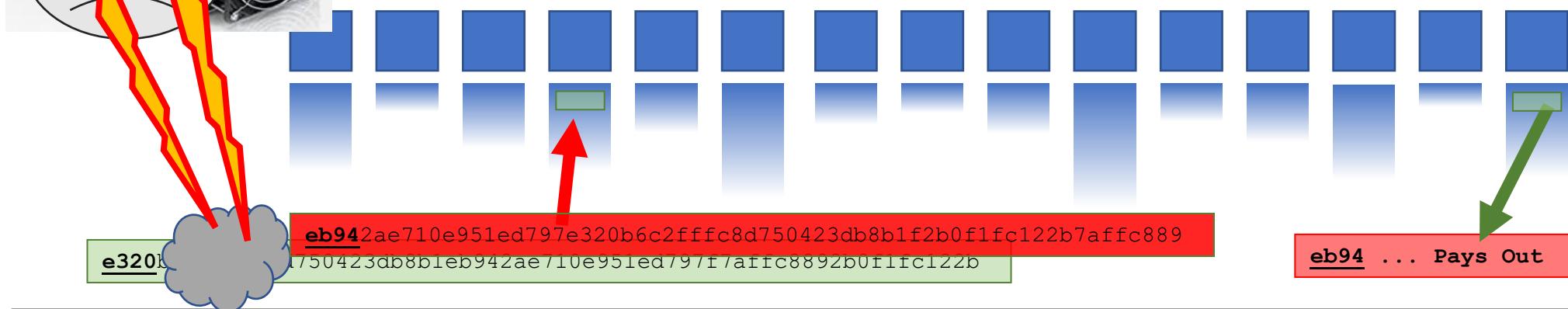


Two Supposed Drawbacks

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



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



(#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.

What does affect mainchain miners: Altcoins

[bitcoin-dev] Total fees have almost c

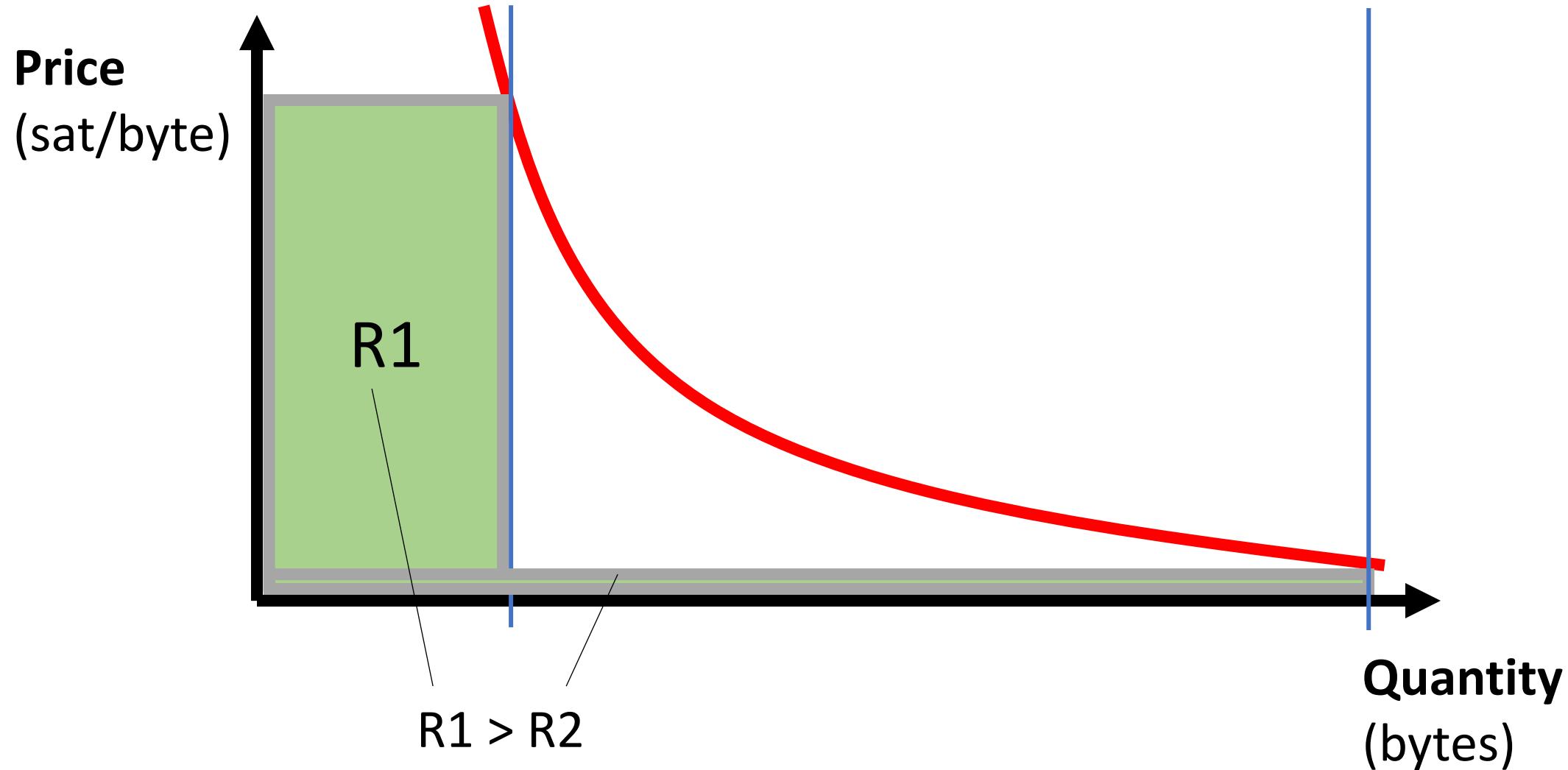
Gregory Maxwell [greg at xiph.org](mailto:greg@xiph.org).

Thu Dec 21 22:44:32 UTC 2017

- Previous message: [\[bitcoin-dev\] Total fees have almost crossed the block](#)
- Next message: [\[bitcoin-dev\] Total fees have almost crossed the block rev](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)

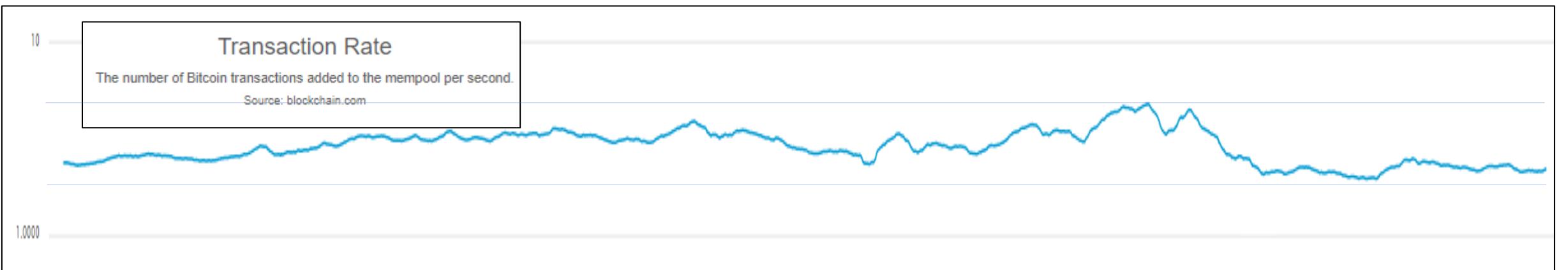
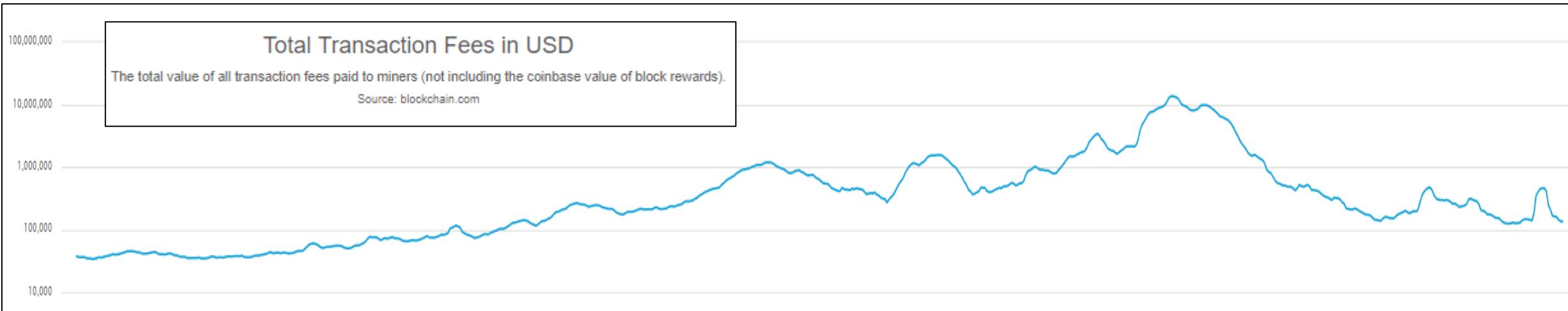
Personally, I'm pulling out the champagne that market behaviour is indeed producing activity levels that can pay for security without inflation, and also producing fee paying backlogs needed to stabilize consensus progress as the subsidy declines.

What does affect mainchain miners: Altcoins



High Fees → Less Usage

Last 2 Years, Log Scales, 7d average



Fee revenues are important...

[bitcoin-dev] Total fees have almost c

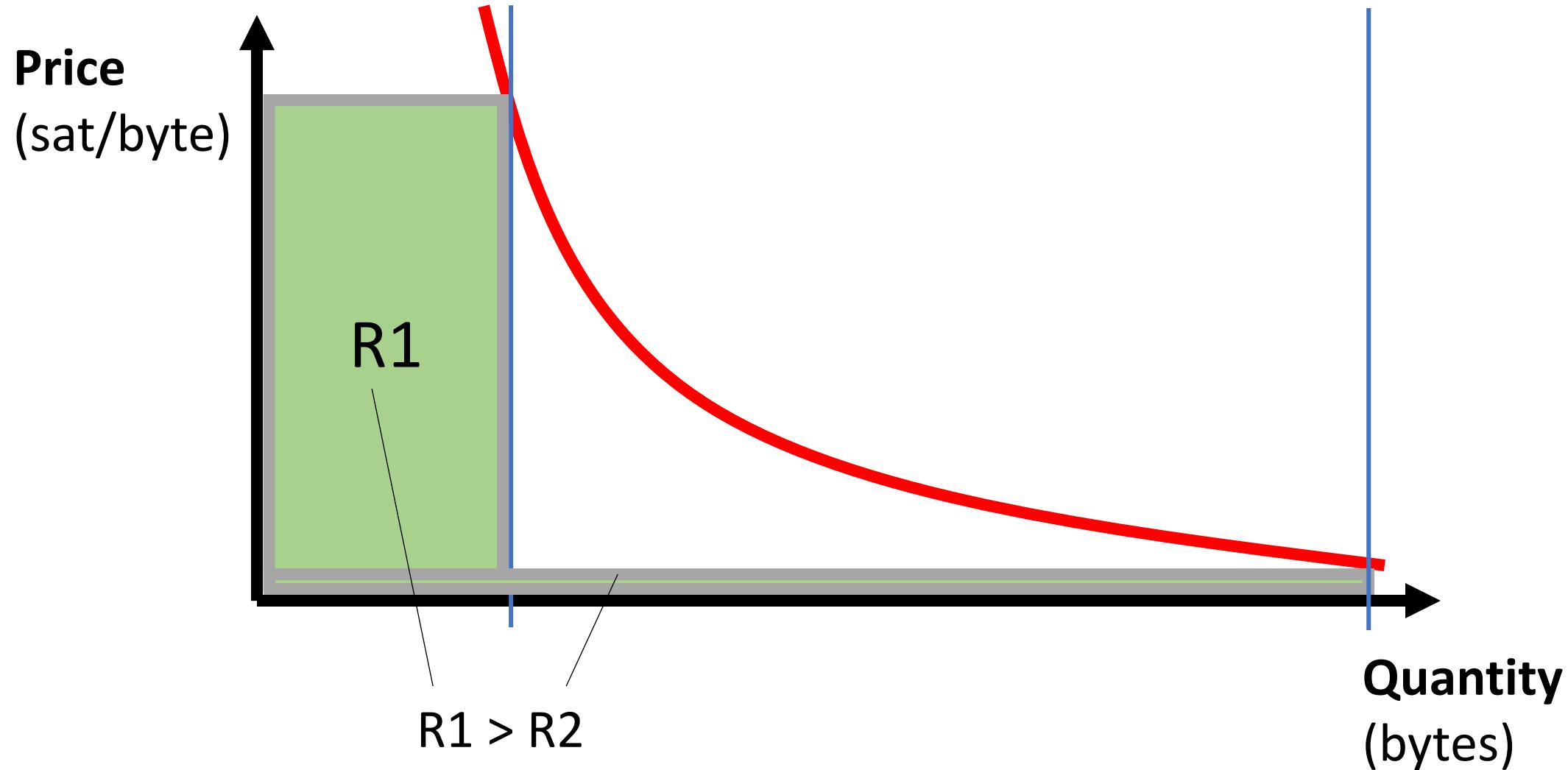
Gregory Maxwell greg@xiph.org.

Thu Dec 21 22:44:32 UTC 2017

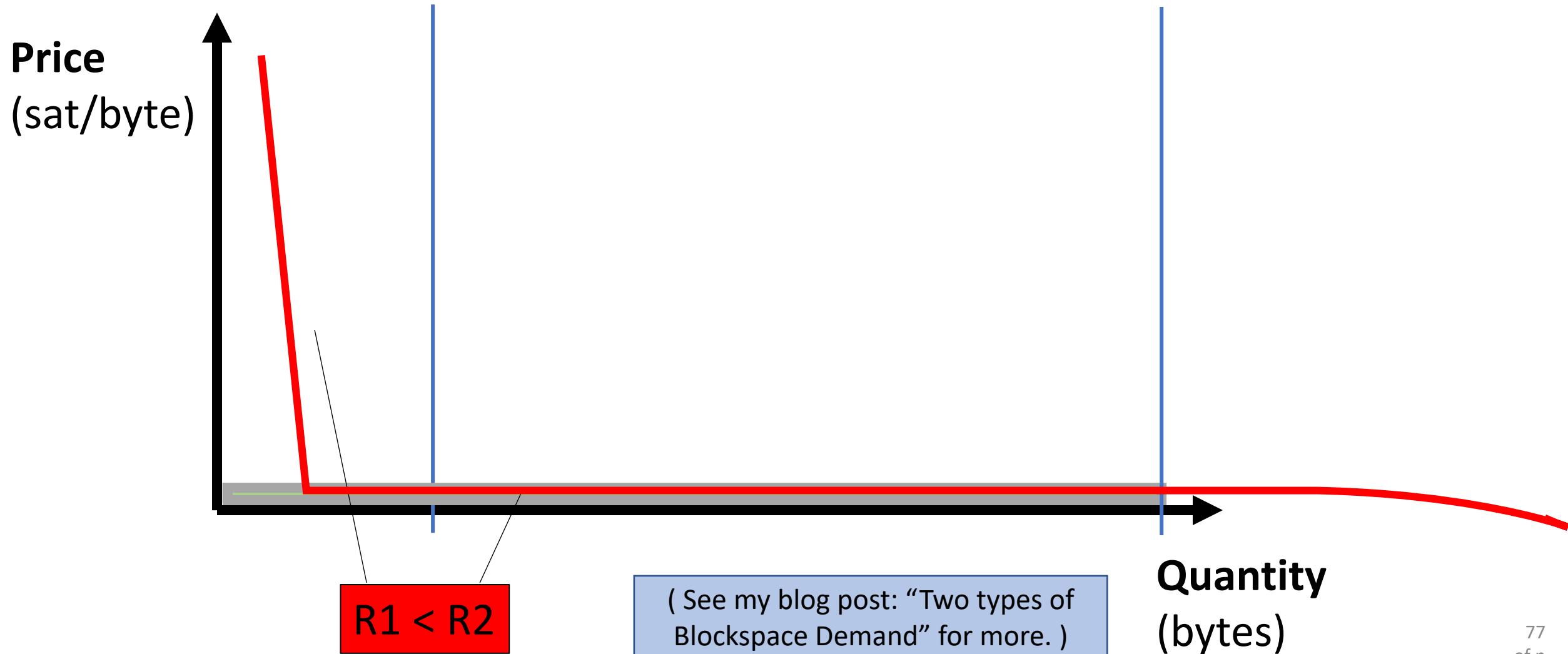
- Previous message: [\[bitcoin-dev\] Total fees have almost crossed the block](#)
- Next message: [\[bitcoin-dev\] Total fees have almost crossed the block rev](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)

Personally, I'm pulling out the champaign that market behaviour is indeed producing activity levels that can pay for security without inflation, and also producing fee paying backlogs needed to stabilize consensus progress as the subsidy declines.

...and supply affects Fee Revenues.



What does affect mainchain miners: Altcoins



(#3) Improve Mining Incentives (Bip 301)

- Get all of the fees, on all of the chains!
- Miners can ignore Sidechain / Altcoin software.

Upon finding a sidechain block worth \$2000...		
Item	Layer1 Miner ("Mary")	Sidechain User ("Simon")
Runs a sidechain node?	No	Yes
How much hashing?	100%	0%
Coins collected, on Layer2	\$0	\$2000
Coins paid out, on Layer1	\$0	\$1999
Coins rec'd, on Layer1	\$1999	\$0
d(Net Worth)	+\$1999	+\$1



Security Budget in the Long Run

14 Feb 2019

<https://www.truthcoin.info/blog/security-budget/>

Security Budget II, Low Fees, and Merged Mining

15 Oct 2021

<https://www.truthcoin.info/blog/security-budget-ii-mm/>

4, 2021

coin

78

(#3) Improve Mining Incentives (Bip 301)

- Get all of the fees, on all of the chains!
- Miners can ignore Sidechain / Altcoin software.

Upon finding a sidechain block worth \$2000...		
Item	Layer1 Miner ("Mary")	Sidechain User ("Simon")
Runs a sidechain node?	No	Yes
How much hashing?	100%	0%
Coins collected, on Layer2	\$0	\$2000
Coins paid out, on Layer1	\$0	\$1999
Coins rec'd, on Layer1	\$1999	\$0
d(Net Worth)	+\$1999	+\$1



Security Budget in the Long Run

14 Feb 2019

<https://www.truthcoin.info/blog/security-budget/>

Security Budget II, Low Fees, and Merged Mining

15 Oct 2021

<https://www.truthcoin.info/blog/security-budget-ii-mm/>

4, 2021

coin

(#3) Improve Mining Incentives (Bip 301)

- Get all of the fees on all of the chains!
- Miners can

