Drivechains (BIP 300 + 301)

Paul Sztorc

May 16th, 2023

Agenda

1. Paul Sztorc / LayerTwo Labs
2. BIP 300 – A Bold Claim
3. I will quickly show you all the other slides:
    1. Details of the Bold Claim -- Heterogeneity, Namecoin, Truthcoin
    2. Prison Metaphor
    3. Actual zCash Example w/ Screenshots
    4. The BIP – The Six Messages of BIP 300 , Explained
    5. Theory: How to Police a [Chain] We Can't See
    6. Two Critiques of Bip300
    7. Appendix: Fees
4. Q&A – You tell me, what if anything , you actually want to see.

Paul's 1000+ Pages About Bitcoin

AUGUST 2015
- Nothing is Cheaper than Proof of Work 04 Aug 2015

JULY 2015
- The Win-Win Blocksize Solution 14 Jul 2015

MAY 2015
- Bitcoin and Deflation, The Last Word 15 May 2015

JANUARY 2015
- BitUSD Isn't Worth The Trouble 29 Jan 2015

NOVEMBER 2014
- The Limits of Blockchain Tech 28 Nov 2014
- Altcoins Aren't Money, They're Bitcoin's Casino/Laundroma
- Long Live Proof-of-Work, Long Live Mining 16 Nov 2014
- Active Decentralization 09 Nov 2014
- Three Basics 06 Nov 2014

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

DECEMBER 2015
- Salvaging the Blocksize Discussion, in Two Questions 28 Dec 2015

NOVEMBER 2015
- Drivechain - The Simple Two Way Peg 24 Nov 2015

OCTOBER 2015
- The Hashing Heart Attack 28 Oct 2015
- PSA - Linking to a Blog Section 05 Oct 2015

SEPTEMBER 2015
- Oracles are the Real Smart Contracts 21 Sep 2015
- Measuring Decentralization 09 Sep 2015

OCTOBER 2017
- Fork Futures (via the Exchanges) 12 Oct 2017

JULY 2017
- Proof of Stake is Still Pointless 07 Jul 2017

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

DECEMBER 2016
- Against the Hard Fork 06 Dec 2016
- Better Fork Terminology 05 Dec 2016

MAY 2016
- BTC Codex - The Digital Identity Sidechain 21 May 2016
- The Drivechain OP Code 14 May 2016

SEPTEMBER 2018
- Expensive Privacy is Useless Privacy 11 Sep 2018
- Five Lies and the Truth 11 Sep 2018

JUNE 2018
- BitAssets - A Digital Assets Sidechain 21 Jun 2018

APRIL 2018
- Meditations on Fraud Proofs 14 Apr 2018
- Blockchain Fusion (via Compensated Sidechains) 07 Apr 2(
- Bitcoin Post-Maximalism 07 Apr 2018

MARCH 2018
- GigaChain 20 Mar 2018

2021

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

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

JUNE 2019
- The Consent of the Governed 21 Jun 2019
- 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

FEBRUARY 2019
- Security Budget in the Long Run 14 Feb 2019

DECEMBER 2018
- Imposed Mutual-Exclusivity (IMEX) for Hard Forks 20 Dec 2018

NOVEMBER 2018
- Gradually Activated Replay Protection (GARP) - Toward Hard Forks that D
- Suck 13 Nov 2018
- Deniability - Unilateral Transaction Meta-Privacy 09 Nov 2018

APRIL 2023
- Small Transactions 08 Apr 2023

JUNE 2022
- The "Sidechain Vision" for Bitcoin 27 Jun 202

APRIL 2022
- Lightning Network -- Fundamental Limitatic

OCTOBER 2021
- Security Budget II, Low Fees, and Merged Mi

FEBRUARY 2021
- Sidechain For BitNames/Logins/DNS, Taking
- Sidechains for Scaling -- Thunder Network
- Sidechains for Privacy -- zSide and Melt/Cast

Telegram: t.me/DcInsiders Website: www.LayerTwoLabs.com Paul's Twitter: @truthcoin

My Big Break

Adam Back links to my blog – Dec 2014

ada [illegible] (OP)
Sr. Member

Activity: 404
Merit: 318

in bitcoin we trust

[illegible], lack of price/supply feedback & long run electrical cost
December 29, 2014, 12:21:39 AM #1

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 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 Stable ....and therefore loyal to Nobody!! Bwahaha!!

  (My loyalty is to Bitcoin only.)
- Raised $3M to start LayerTwo Labs & help Bitcoiners dominate the world.

BIP300 – A Bold Claim

Part 2 – Why Bip300

My Three Favorite Endorsements

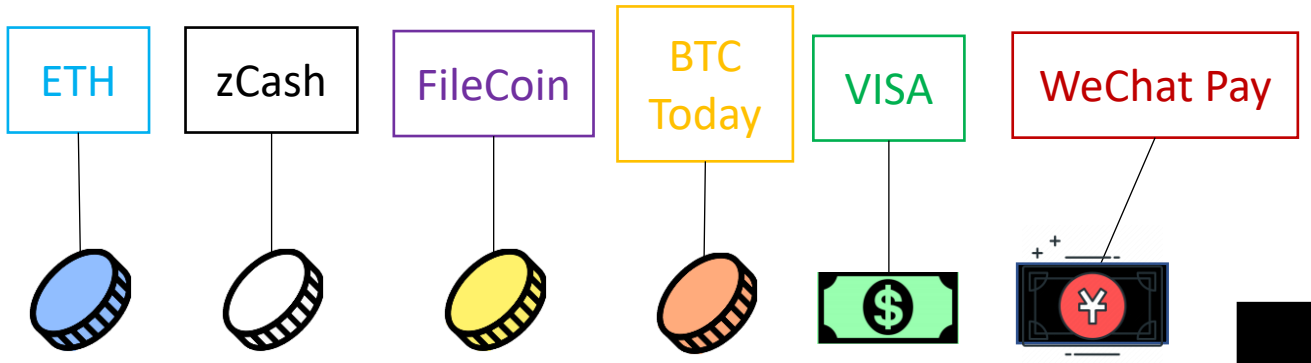
- "Drivechains…are pretty cool…and arguably could have been more important or useful than let's say Taproot."
  - **Adam Back**, Baltic Honeybadger 2022, Live on stage in front of everyone
- "We need Drivechain or all the work of thousands in the last 13 years will be in vain." ... "Drivechain is our 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

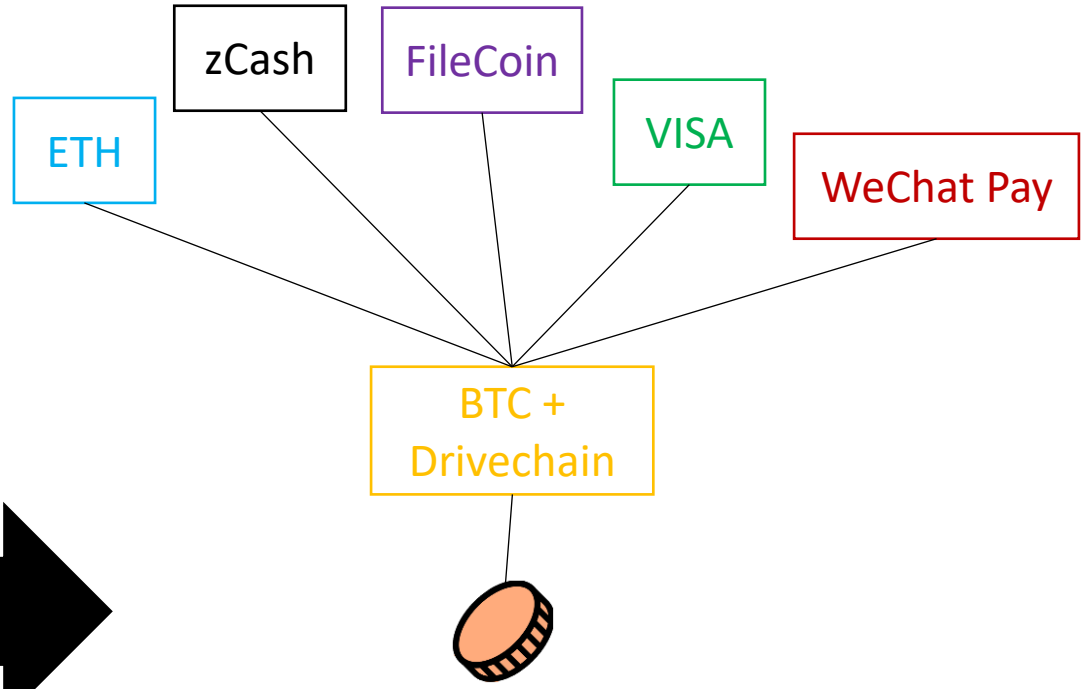
Visit www.LayerTwoLabs.com/friends for 47 more!

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

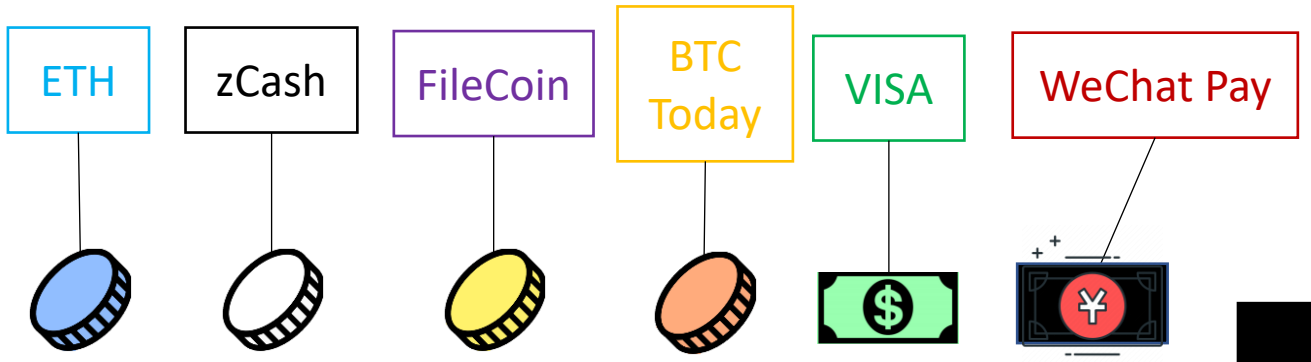




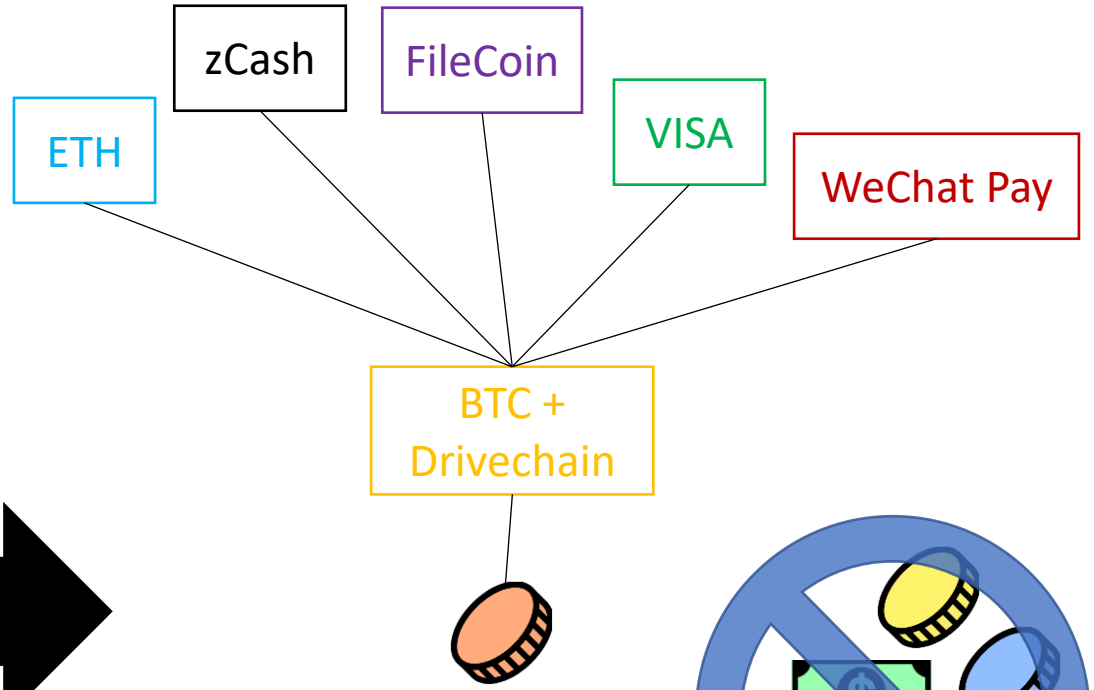
Today ☹

Tomorrow ☺

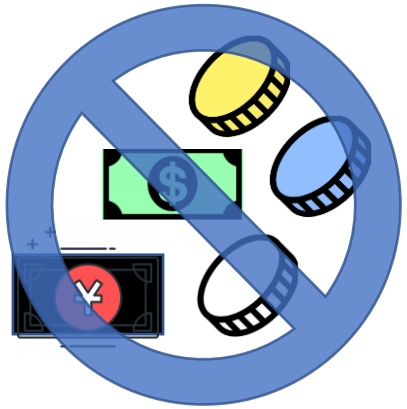
BIP300: Everything on Top of Bitcoin



Today ☹



Tomorrow ☺



The Coming Death of Bitcoin's Competitors

BTC
Today

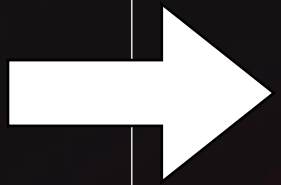
WeChat Pay

VISA

zCash

ETH

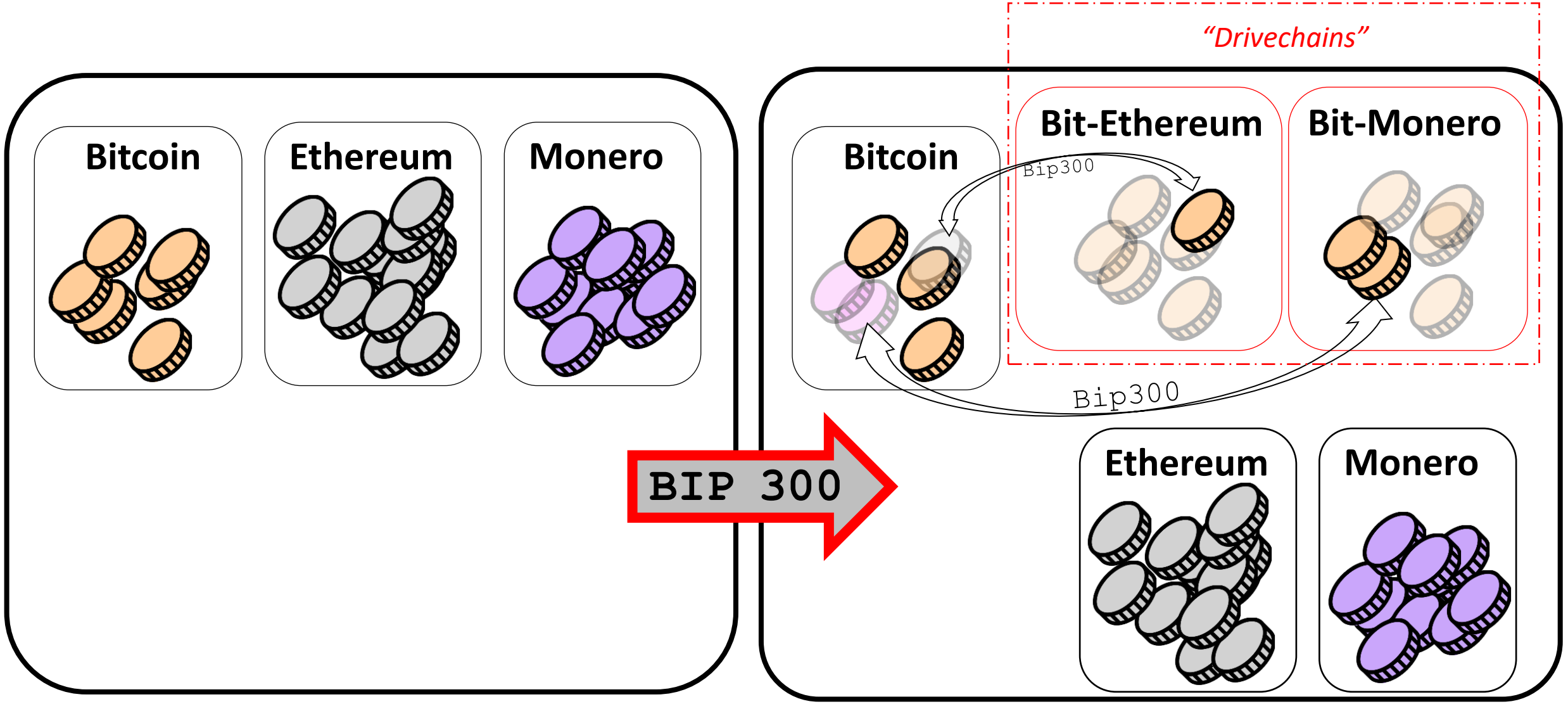
FileCoin



BTC +
Drivechain

* Network effects of Money
* Universality of Computation
* Tech/Culture Kick People Out

Drivechain = Altcoin Tech, BTC Coin Only



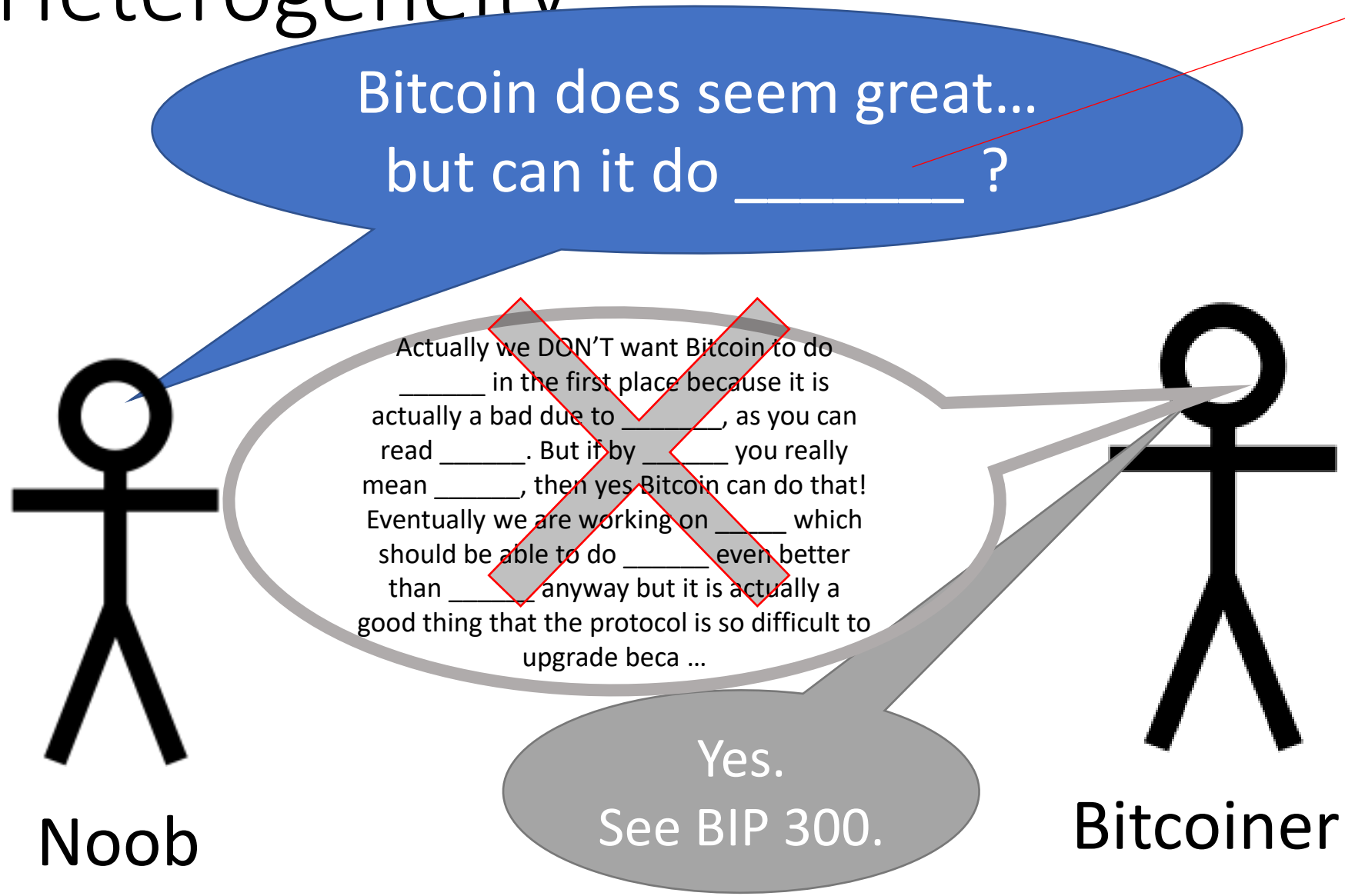
7 Sections

1 - Details of the Bold Claim

A Bold Claim

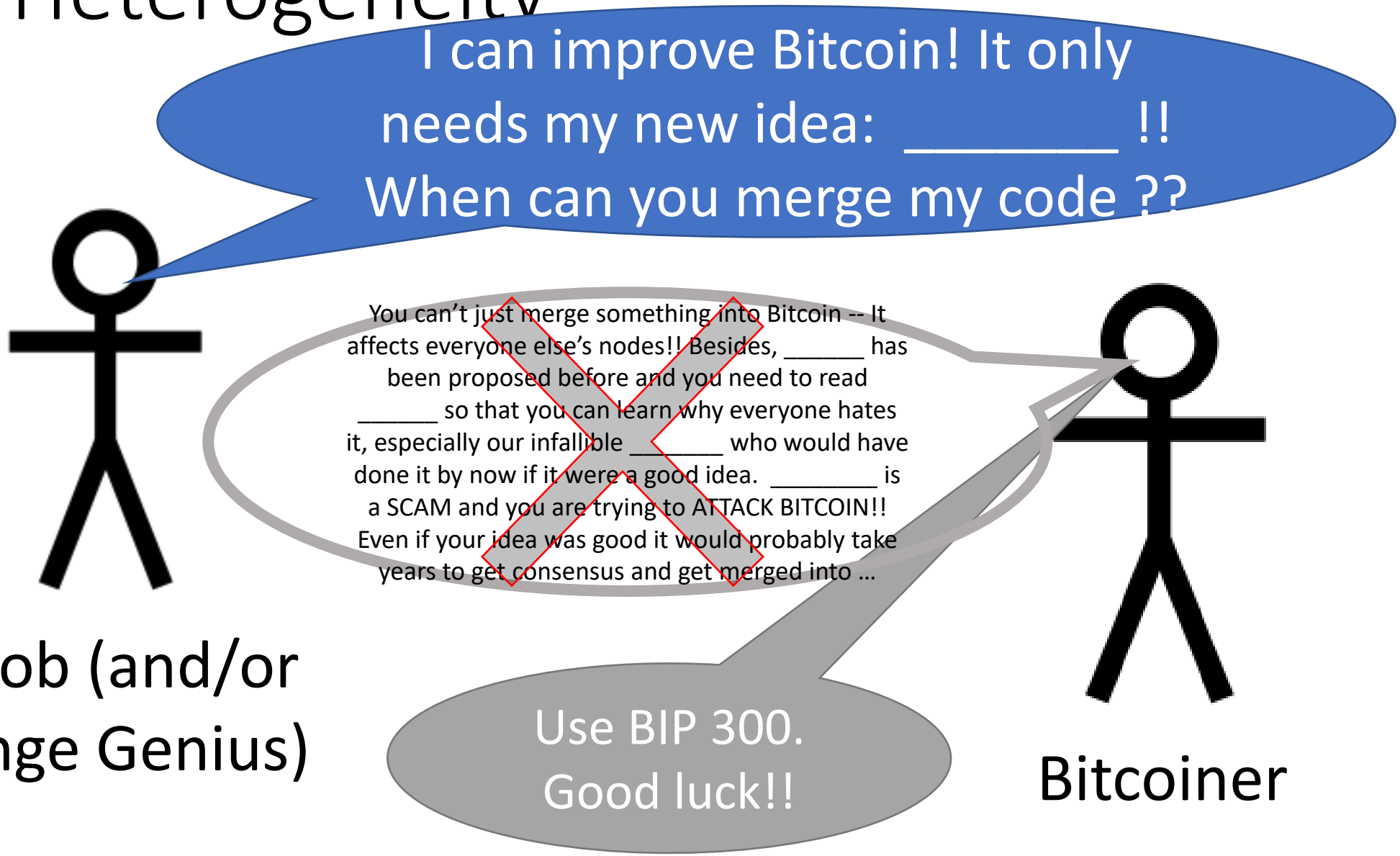
- BIP300 Solves All of Bitcoin's Biggest Problems
  A. Heterogeneity Problem
  B. Scalability
  C. Privacy
  D. Scams – Eliminating ScamCoins ; Domesticating the Token Casino
  E. Security Budget
  F. Decentralization
  G. "Fundamental Value" of Bitcoin
- With...
  H. ...zero risk to Bitcoin!

A. Heterogeneity

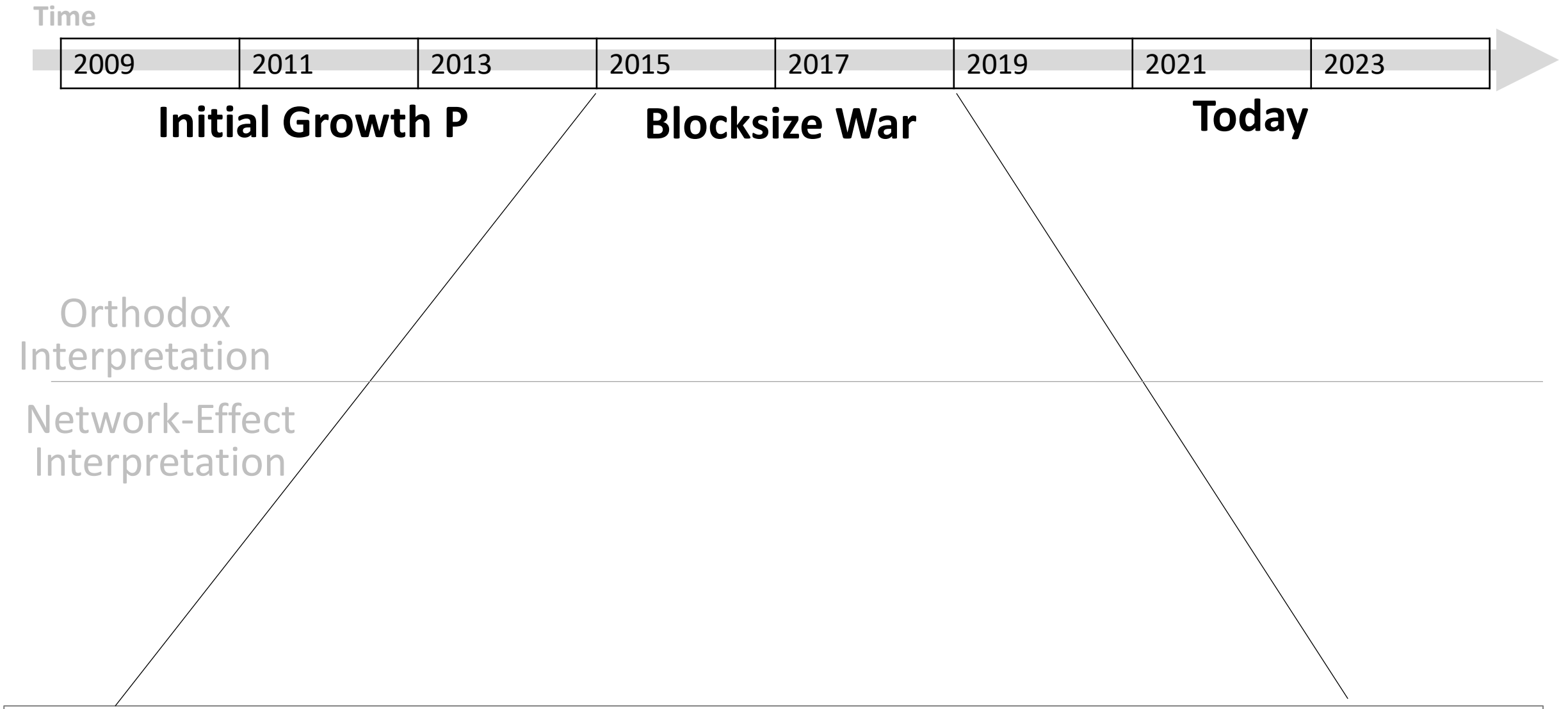


Smart Contracts
DeFi
Turing Completeness
Ring Signatures
zk-Snarks
Large Blocksizes
NFTs
Oracles
Mimblewimble
…(etc)

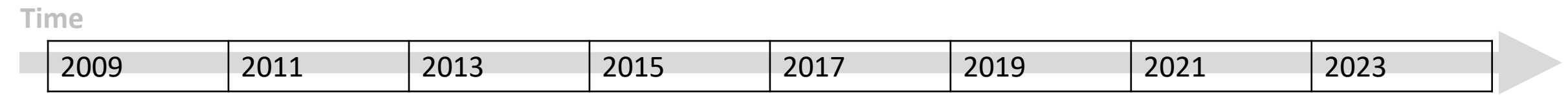
A. Heterogeneity



Why Hasn't Bitcoin *Already* Conquered the World?



Why Hasn't Bitcoin *Already* Conquered the World?



Initial Growth P

Blocksize War

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

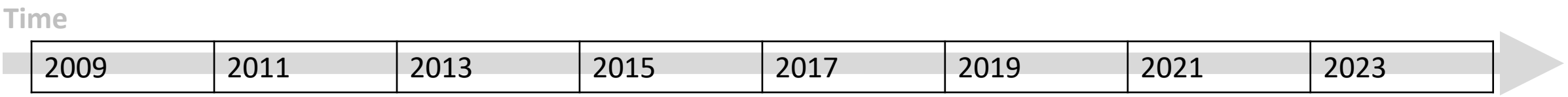
Today

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

Orthodox Interpretation

Network-Effect Interpretation

Why Hasn't Bitcoin *Already* Conquered the World?



Initial Growth P

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).

Orthodox Interpretation

Network-Effect Interpretation

- Community no longer a welcoming / pro-growth place.
- Gave pretext / justification to Ethereum / other competitors.
- Demonstrates our abandoning our core mission (world domination, "bitcoin vs the banks"), so that we can play internal political games amongst ourselves.

- Complacency / Flippening / 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: @truthcoin

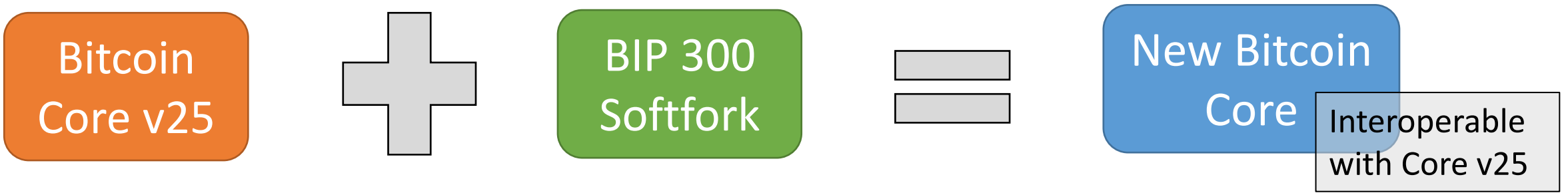
A Bold Claim

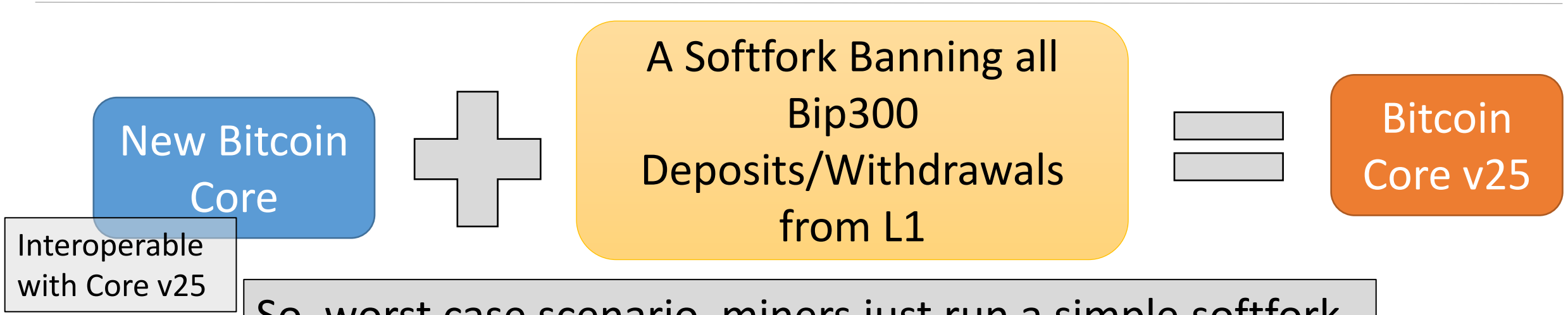
Different strokes for different folks.

- 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 – Eliminatin — 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*.
    - BitNames + Truthcoin ; examples
- 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.





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

Scalability – Comparison to LN

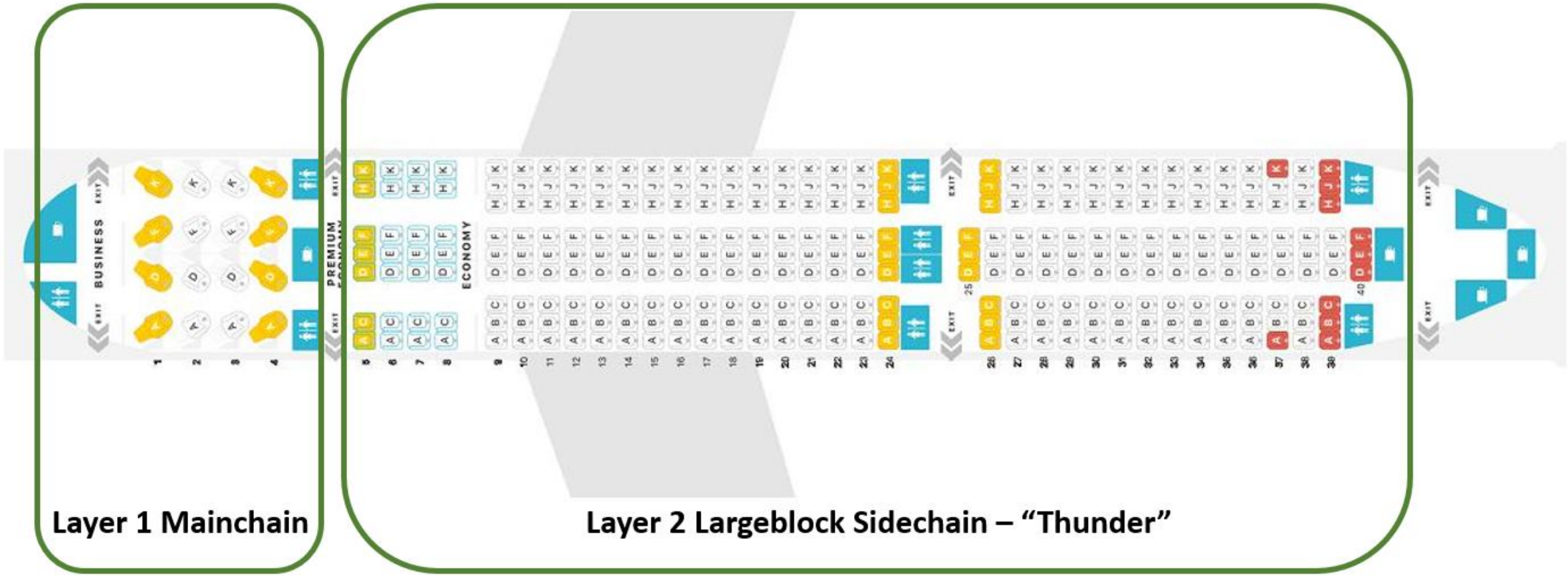
* I assume that an automated hot-wallet is out of the question!

	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.

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.

Fundamental Value – Namecoin

Satoshi co-invents Namecoin in 2010

Why does today's internet suck so much??

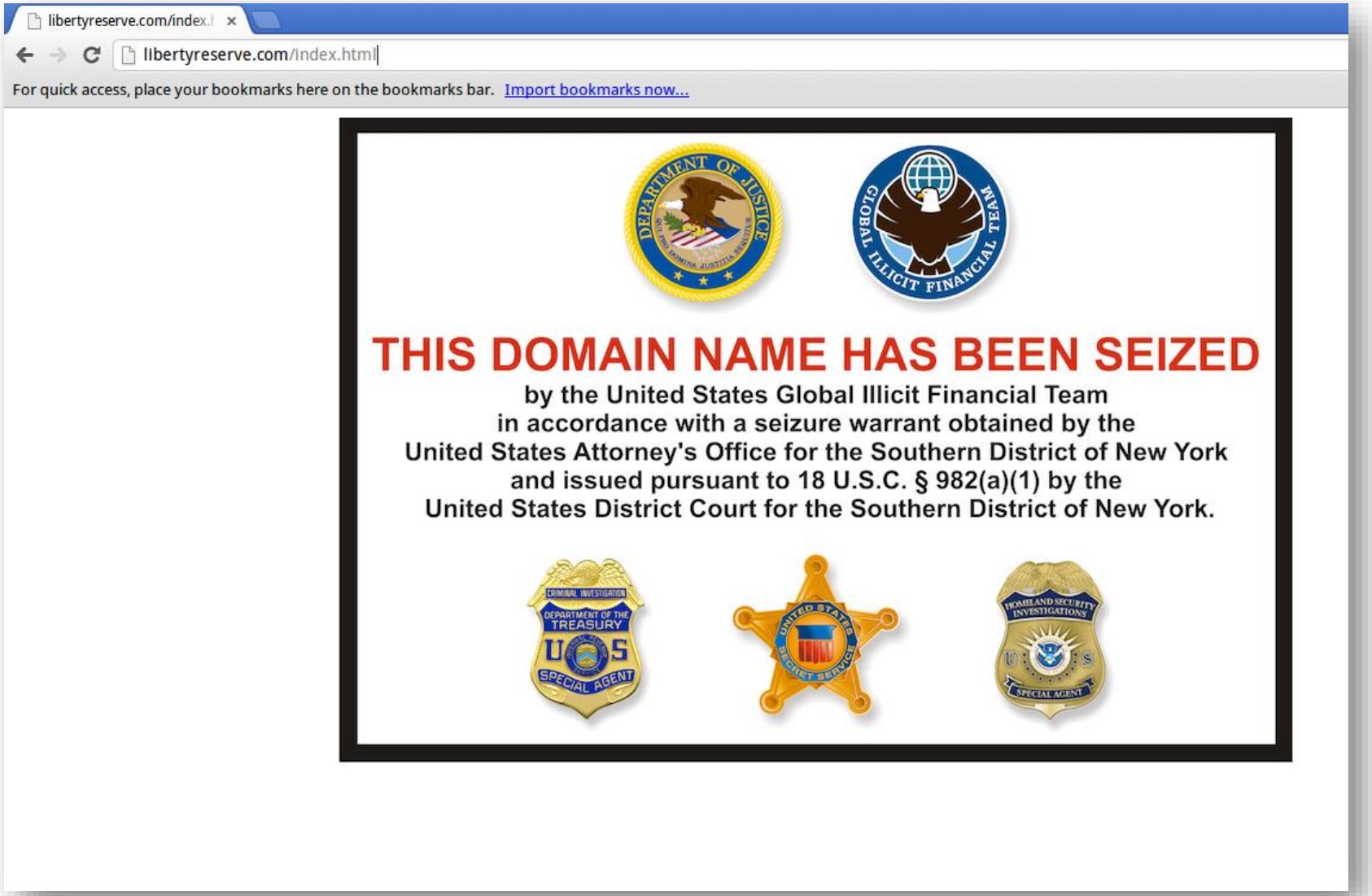
- Namecoin Enables:
  - One Username – Own a single username, that works everywhere, on every site.
  - No more passwords! -- Login by being "pinged" with PIN via open protocol.
  - Easy to keep different online identities separate.
  - "PayMail" – Special inbox where people must pay you $ in order for 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/

Screenshot #2 from

www.truthcoin.info/blog/bitnames/



Screenshot #3 from

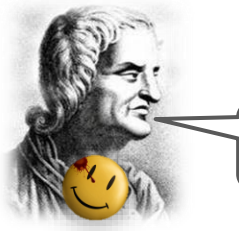
www.truthcoin.info/blog/bitnames/

Fundamental Value – Truthcoin

Paul (me) invents Truthcoin in 2013/14

Why does today's internet suck so much??

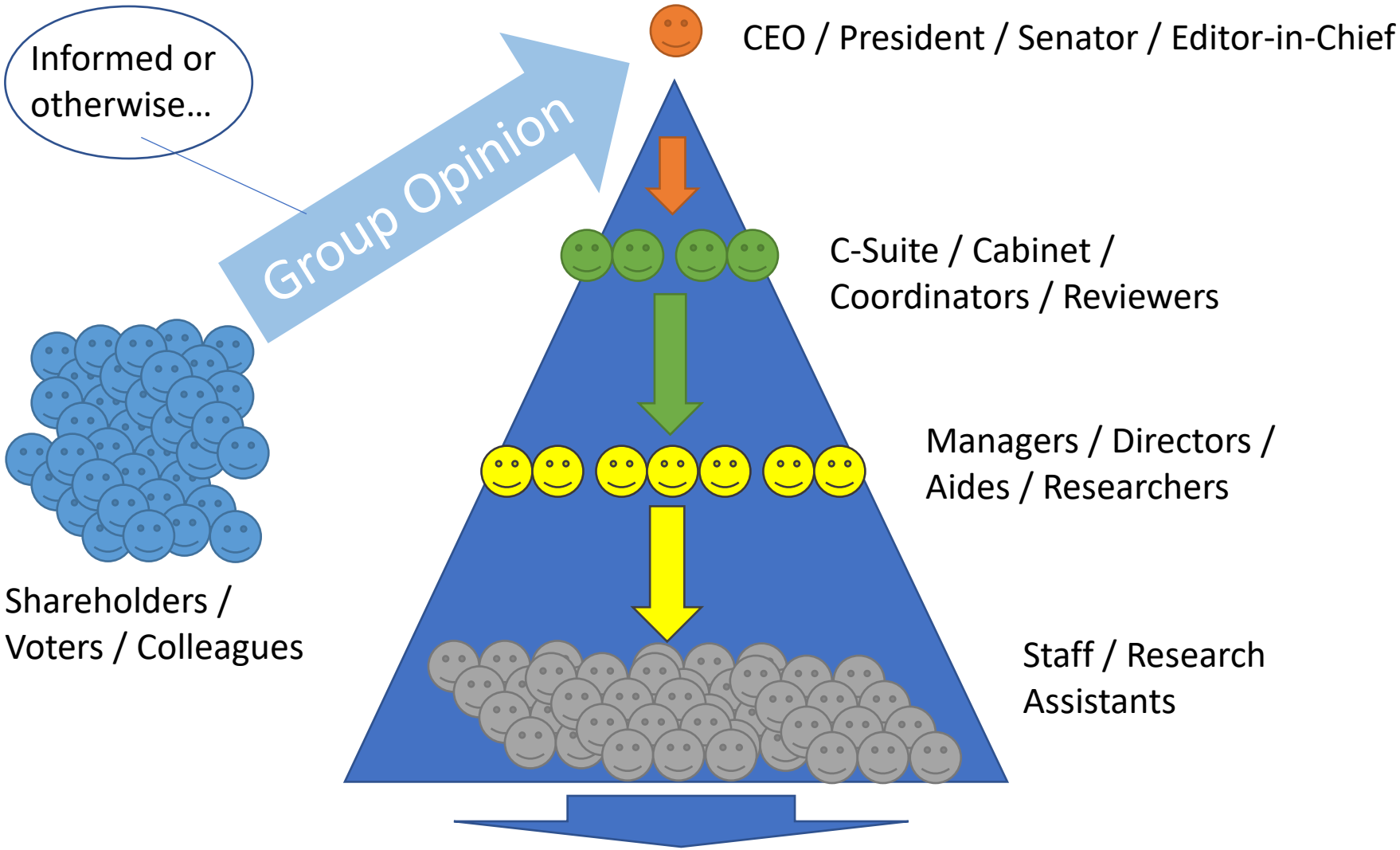
- Truthcoin Enables:
  - Prediction Markets – prevents politicians/CEOs from lying.
    - Prevents politicians/CEOs from lying
    - Each voter/shareholder/whatever can become optimally informed, with zero effort.
    - Will *counteract* "rational ignorance" and Caplan-esque "rational irrationality".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



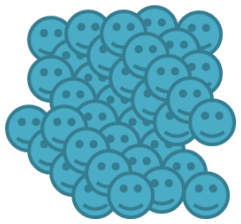
Quis custodiet ipsos custodes? – "But who is in charge of those who are in charge?"

  - 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.

Rot From Above: Who controls what?



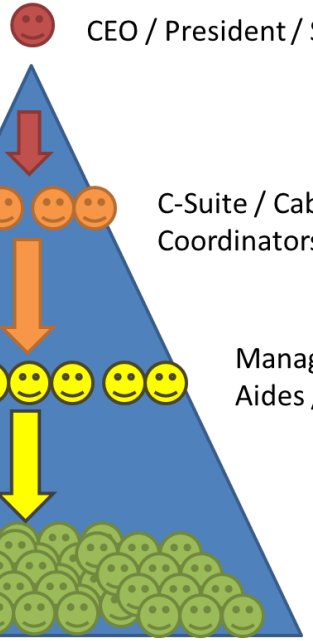
Prediction Markets fix this.



Shareholders / Voters / Colleagues

1. How to we **combine** the many preferences of this group into one request?
2. Do we each have to **monitor** the leader's work? If not, who do we trust (and why)?
3. If I don't like this leader, how do I find out if others agree? How do we **fire the leader**?

Bad



CEO / President / Senator / Editor-in-Chief

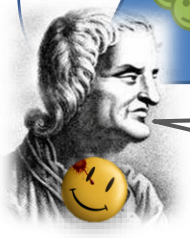
C-Suite / Cabinet / Coordinators / Reviewers

Managers / Directors / Aides / Researchers

Staff / Research Assistants

Can easily…
…make requests.
…observe work/results.
…fire insubordinates.

Good

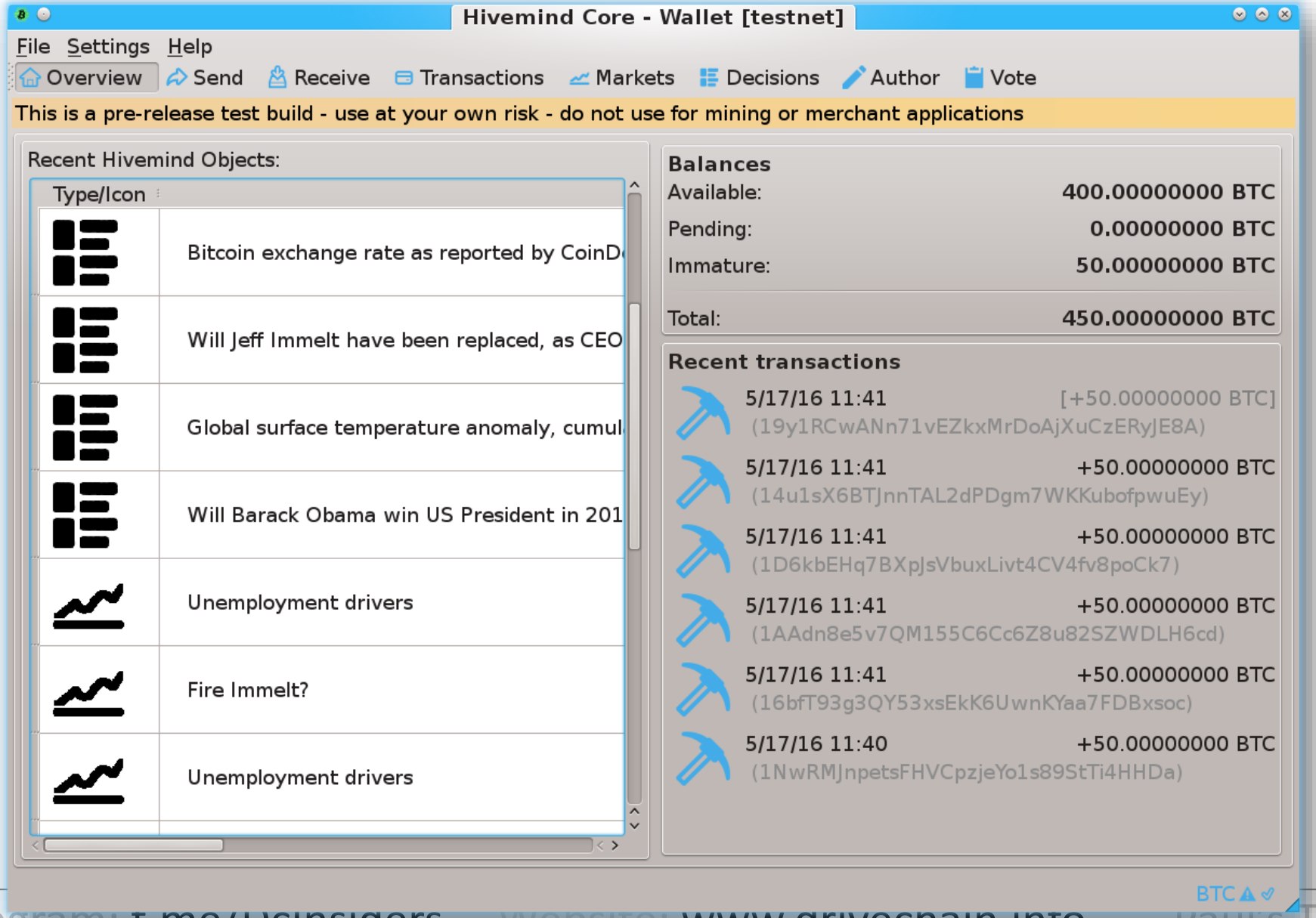


Quis custodiet ipsos custodes? – "But who is in charge of those who are in charge?"

Prediction Markets

- Screenshots from my own BTC sidechain project

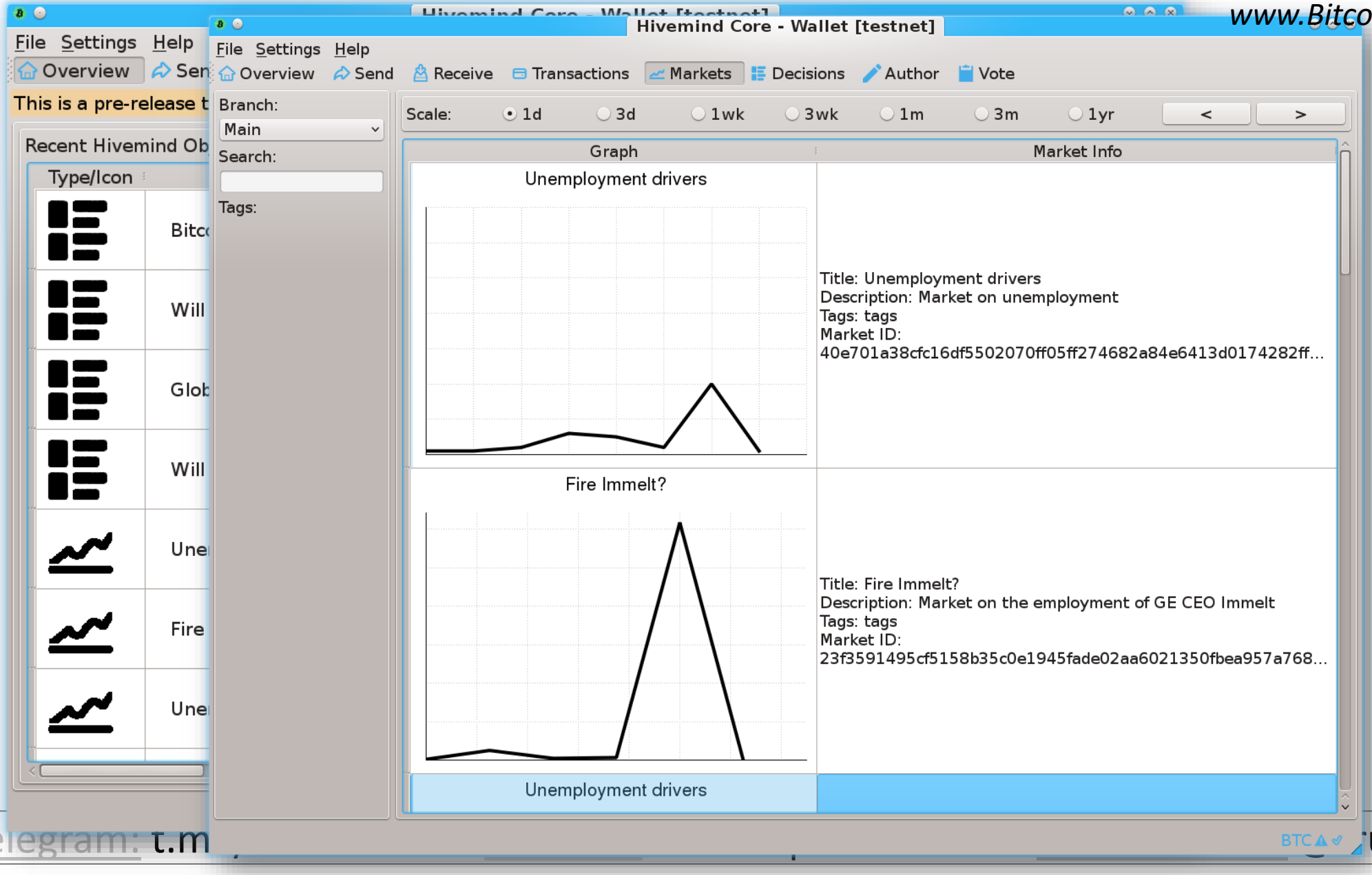
www.BitcoinHivemind.com



Prediction Markets

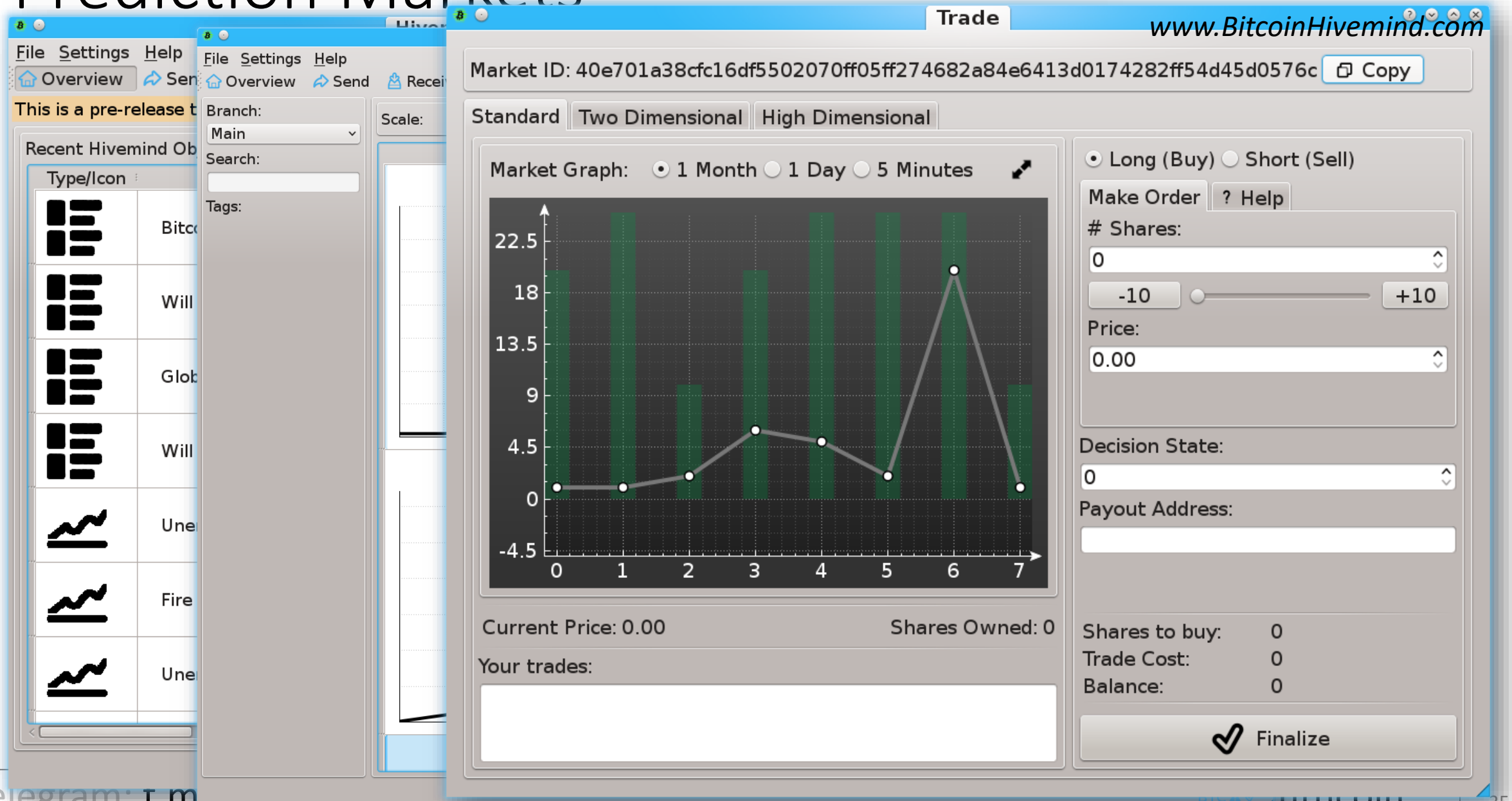
- Screenshots from my own BTC sidechain project

www.BitcoinHivemind.com



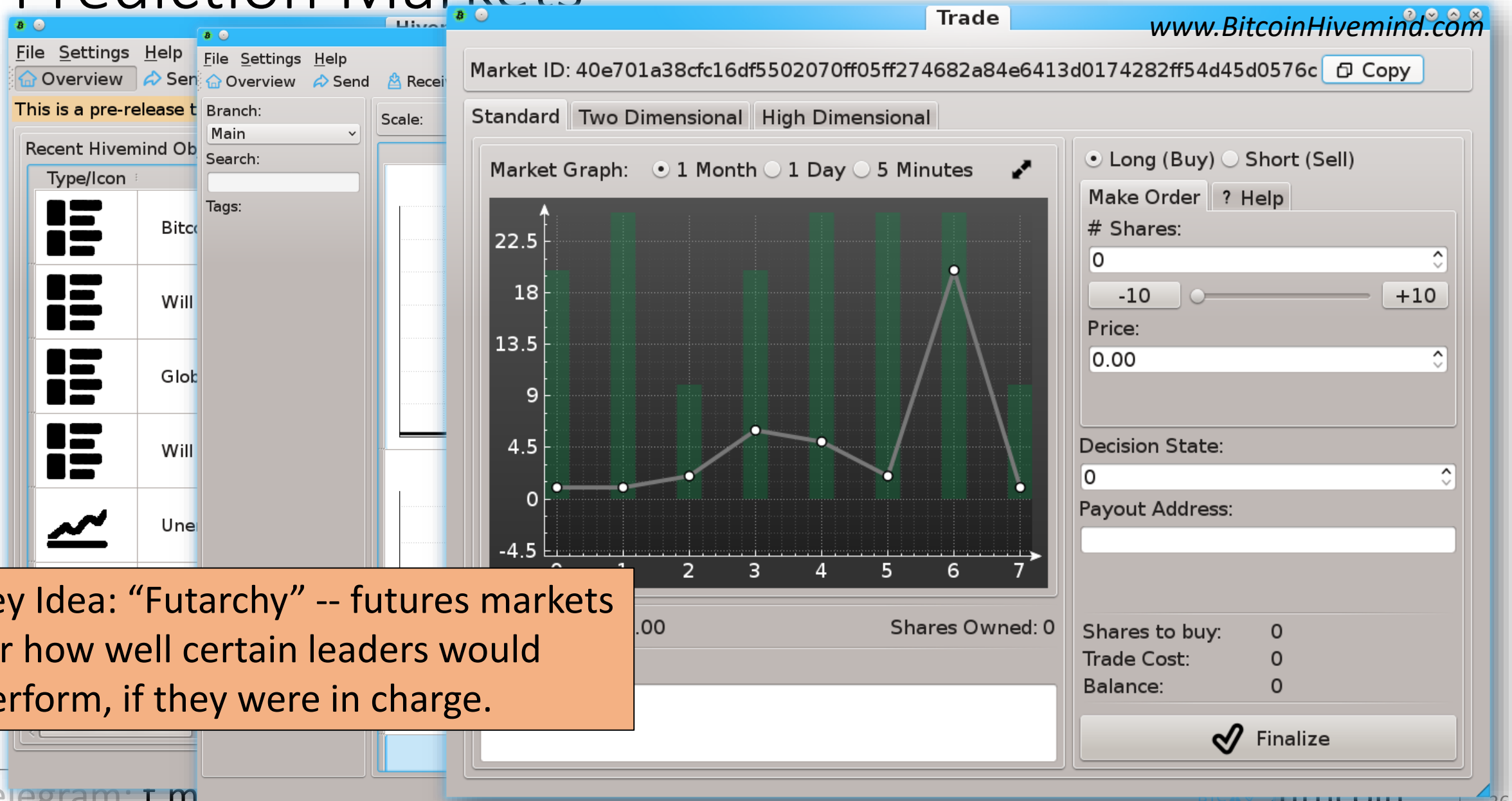
Prediction Markets

- Screenshots from my own BTC sidechain project



Prediction Markets

- Screenshots from my own BTC sidechain project

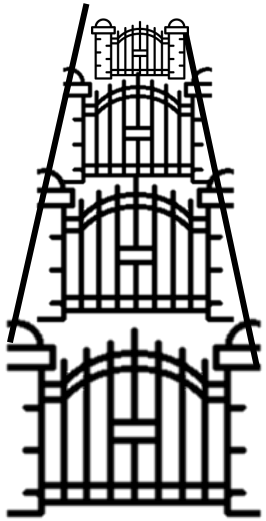


Key Idea: “Futarchy” -- futures markets for how well certain leaders would perform, if they were in charge.

2 - Prison Metaphor

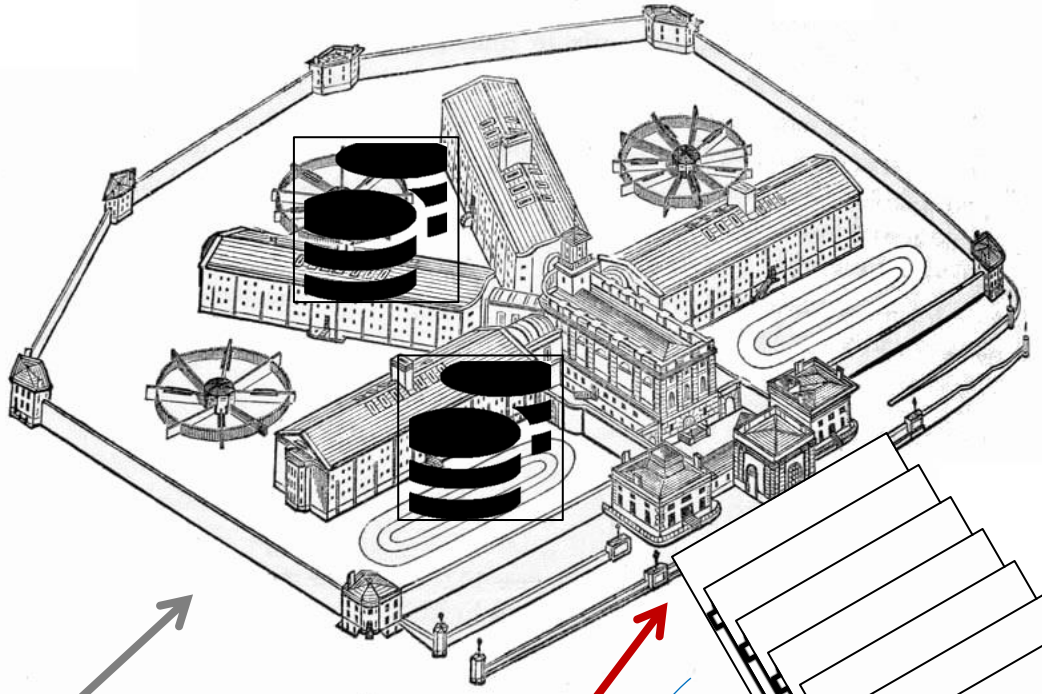
How it Works

- New Kind of Output: “Hashrate Escrow”
- Anyone can *deposit to it* at any time.
- But *withdrawals* are very slow.



Series of gates.

Prison Metaphor



Prison

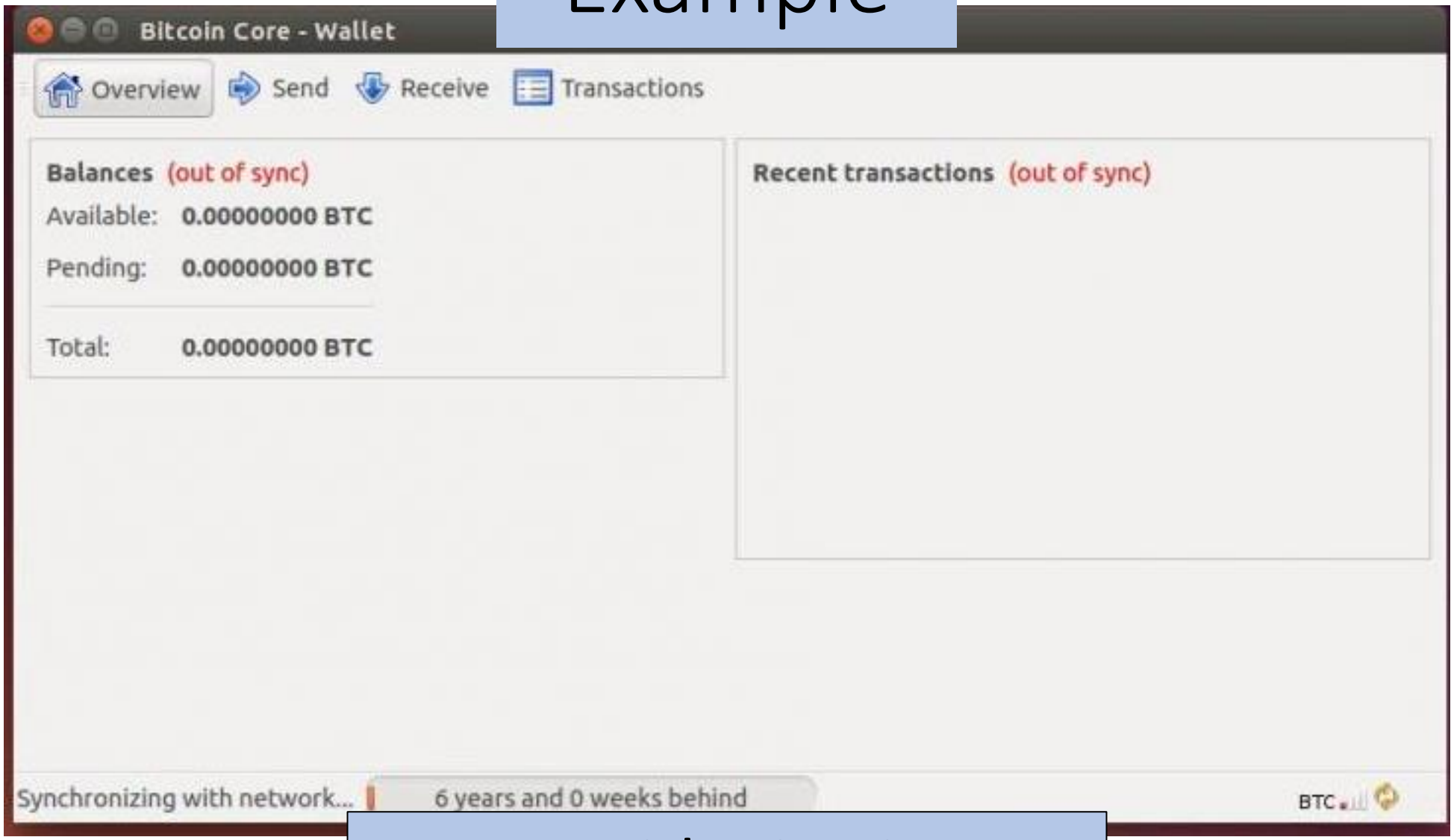
Only way out.

13,150 Gates

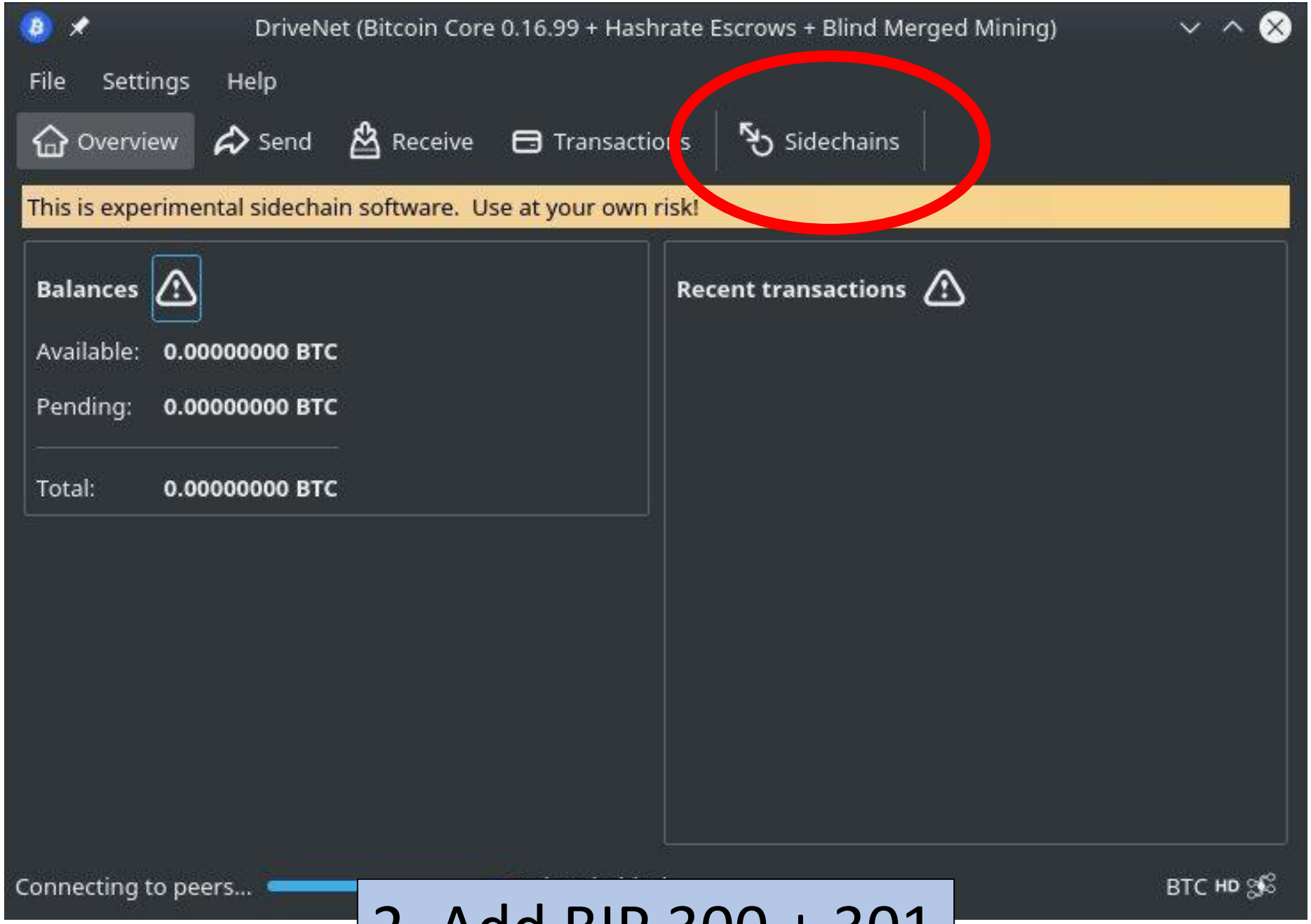
...

BTC

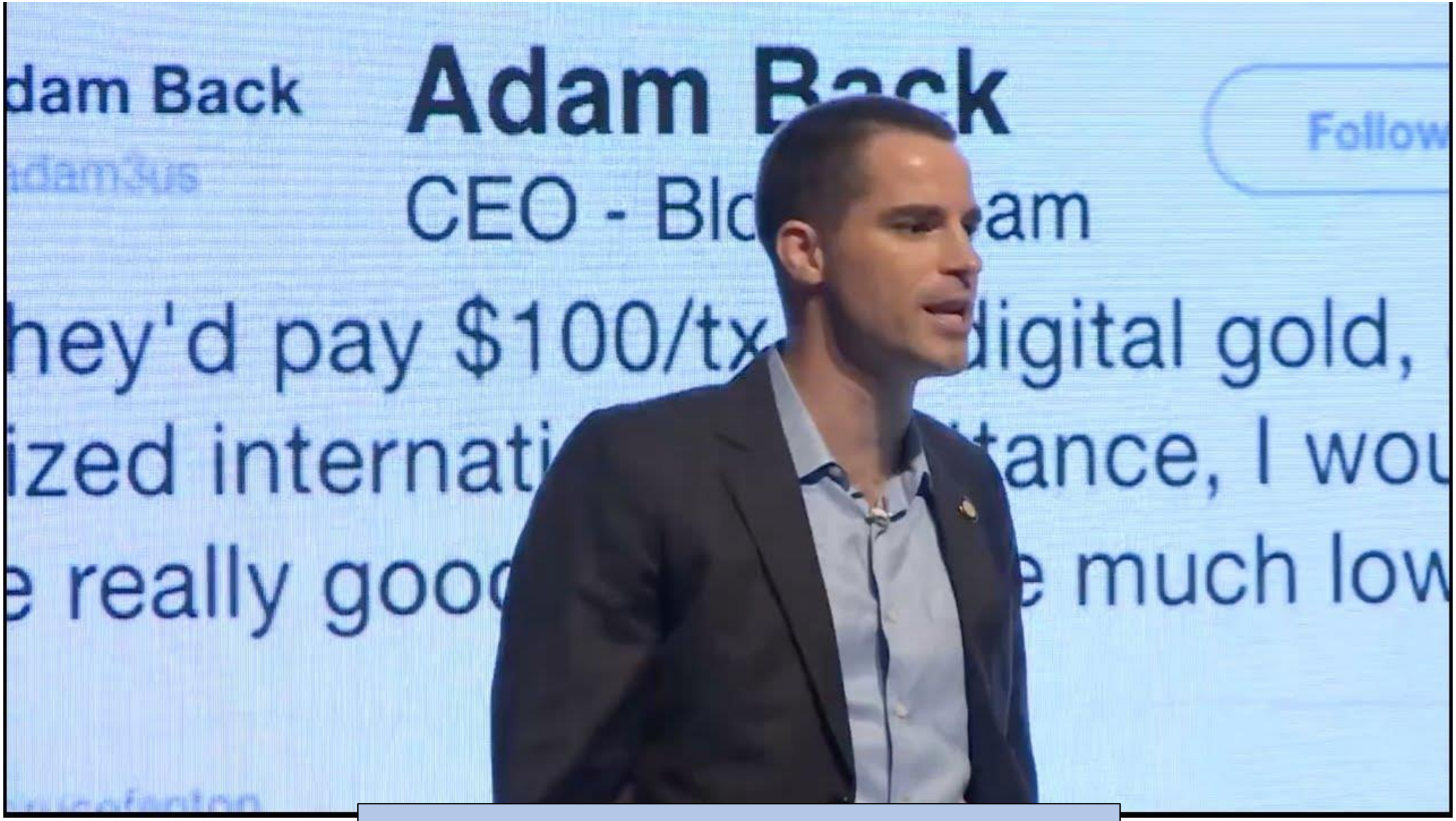
Example



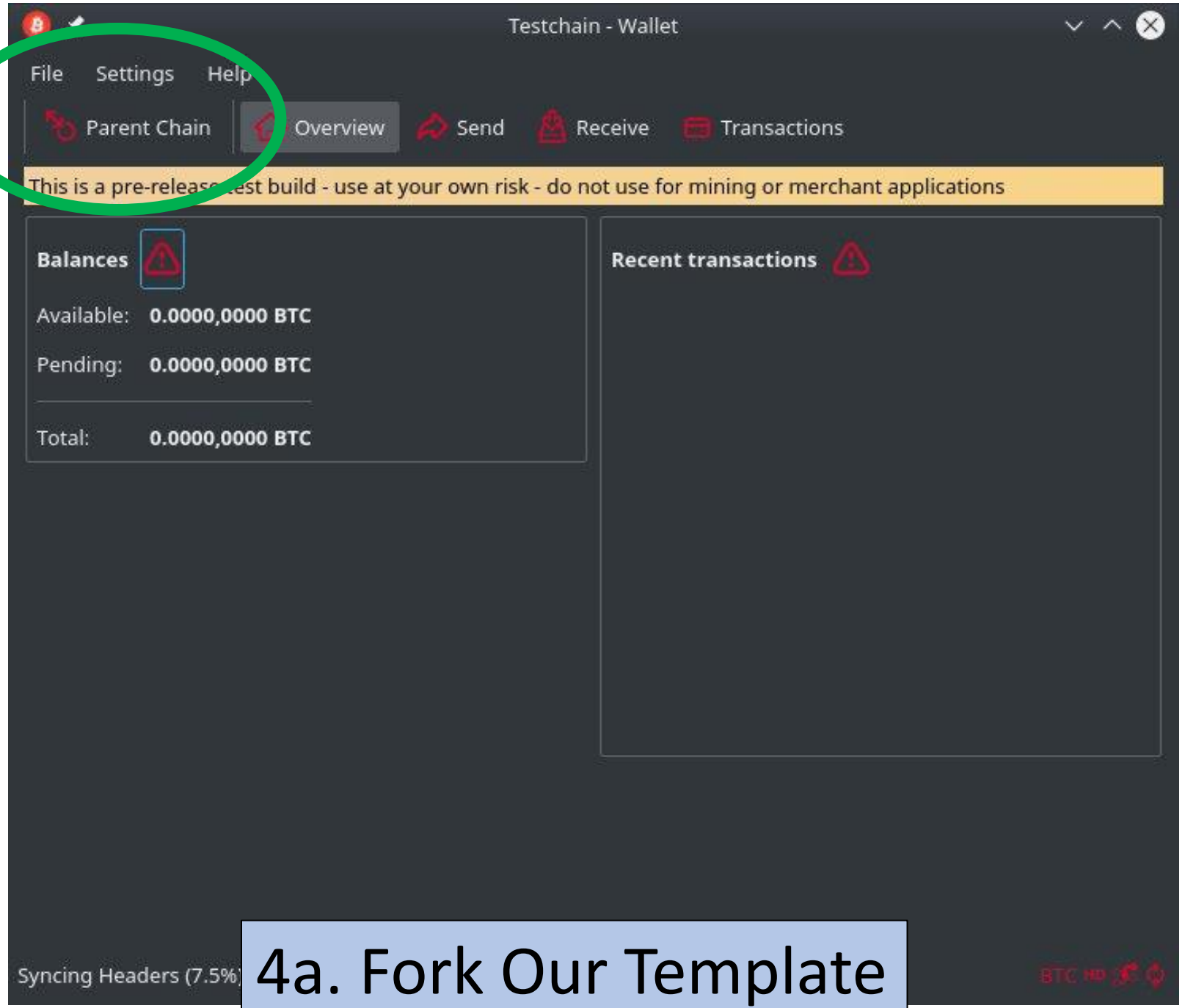
1. Start with Bitcoin Core



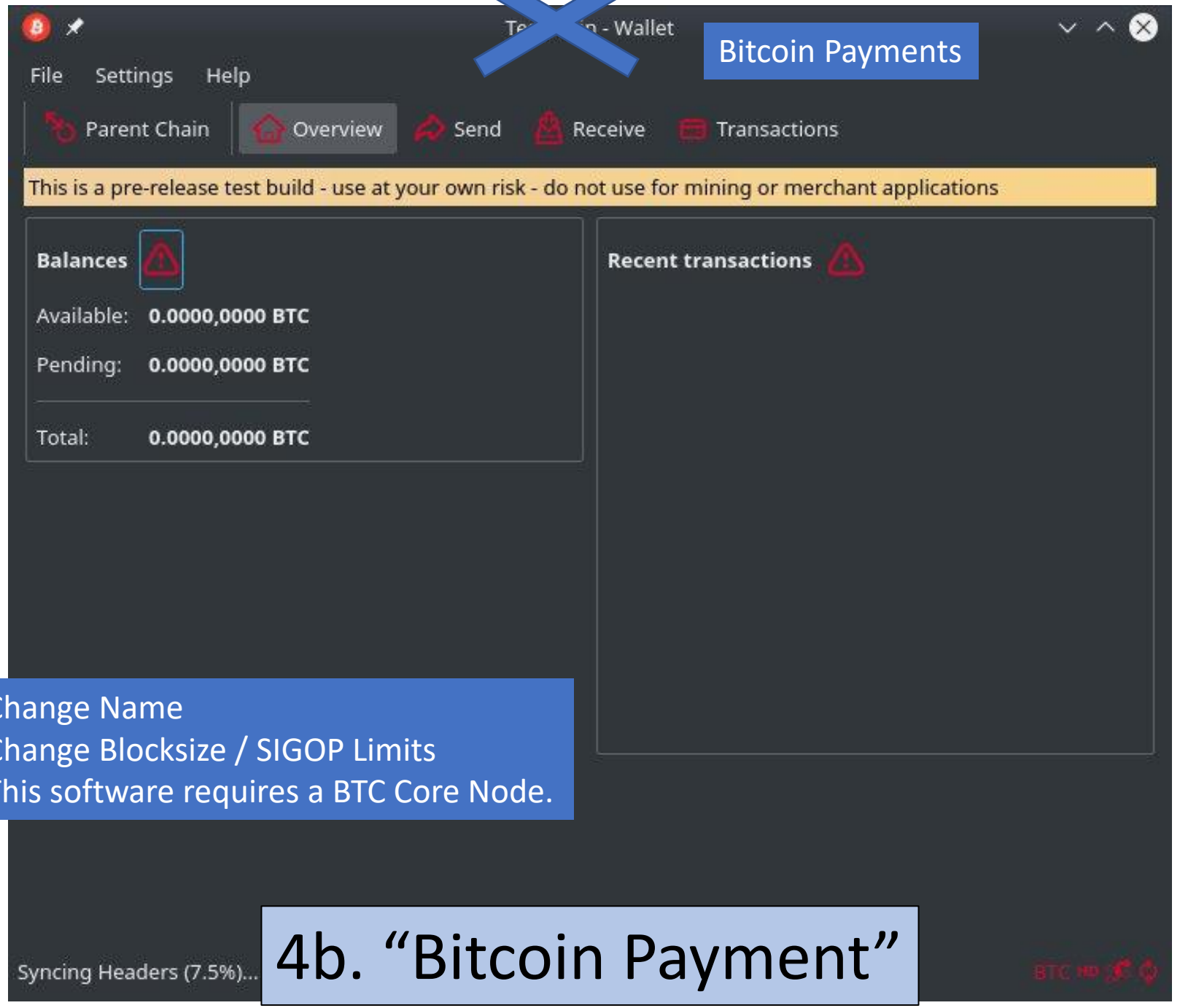
2. Add BIP 300 + 301



3. Meta-Consensus Problem



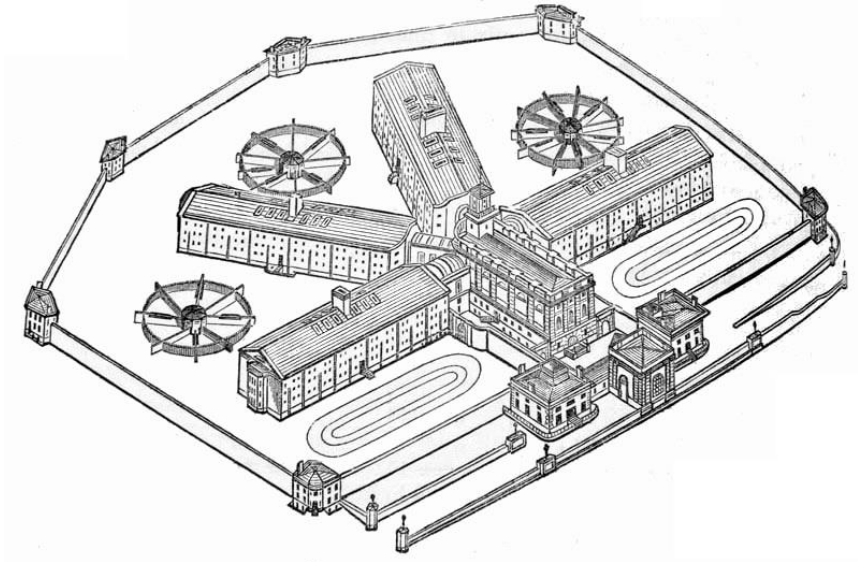
4a. Fork Our Template



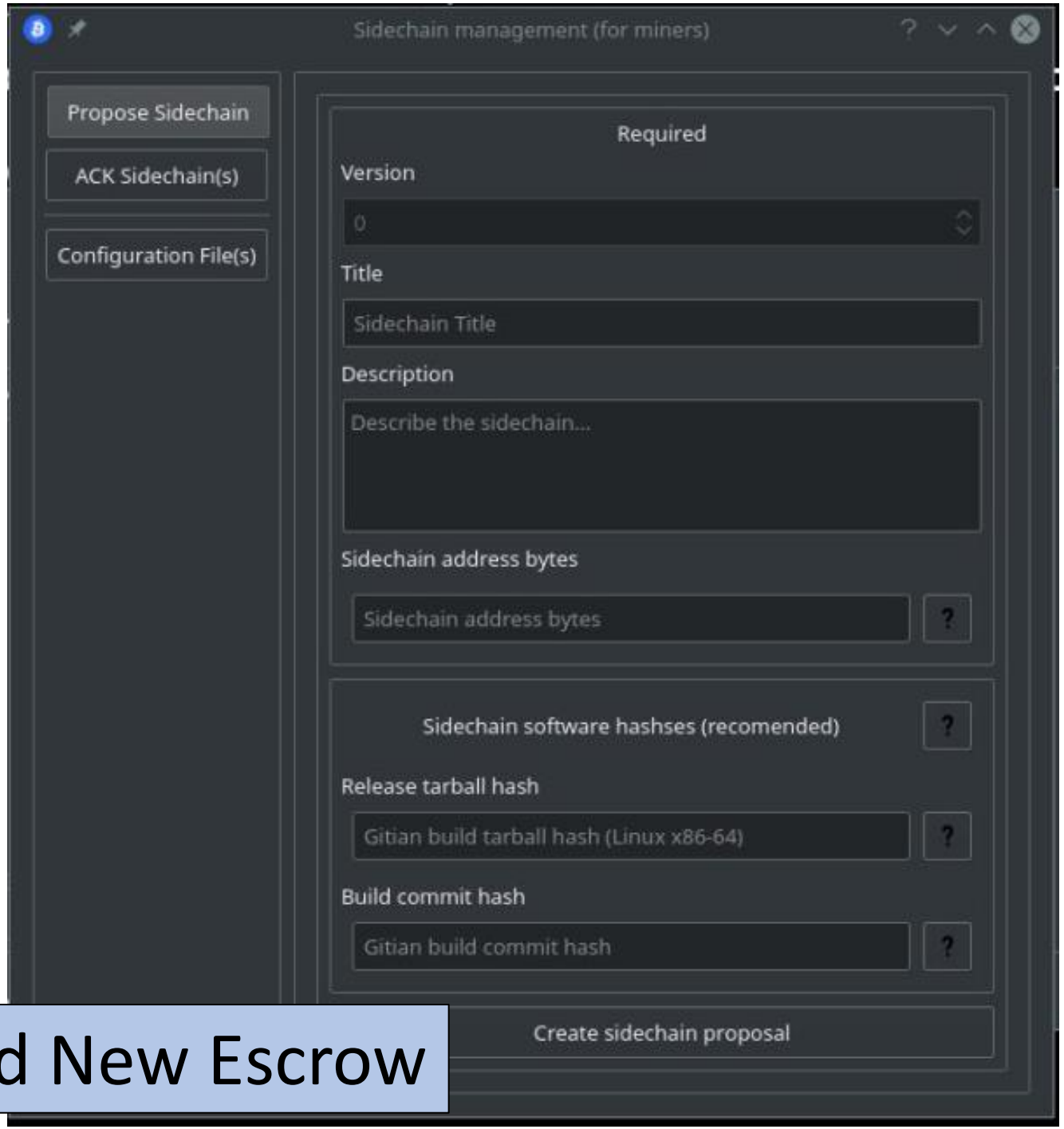
- Change Name
- Change Blocksize / SIGOP Limits
- This software requires a BTC Core Node.

4b. “Bitcoin Payment”

“Bitcoin Payments”

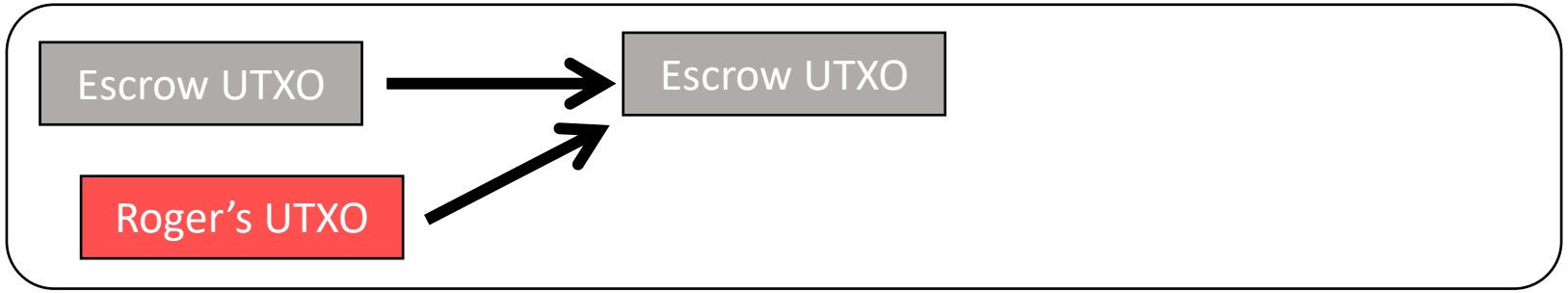


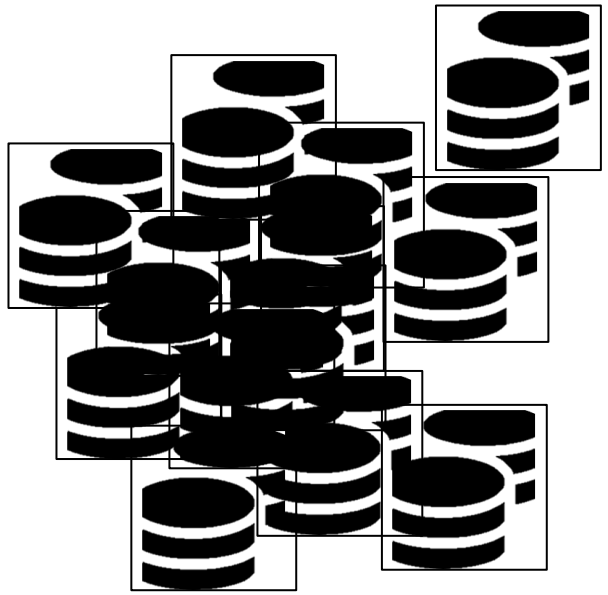
Now Open For Business



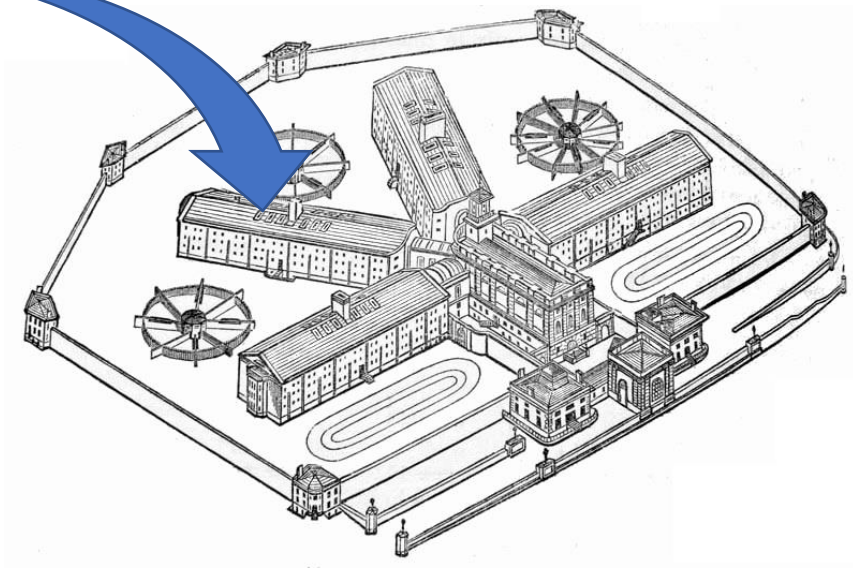
5. Add New Escrow

On layer-1:





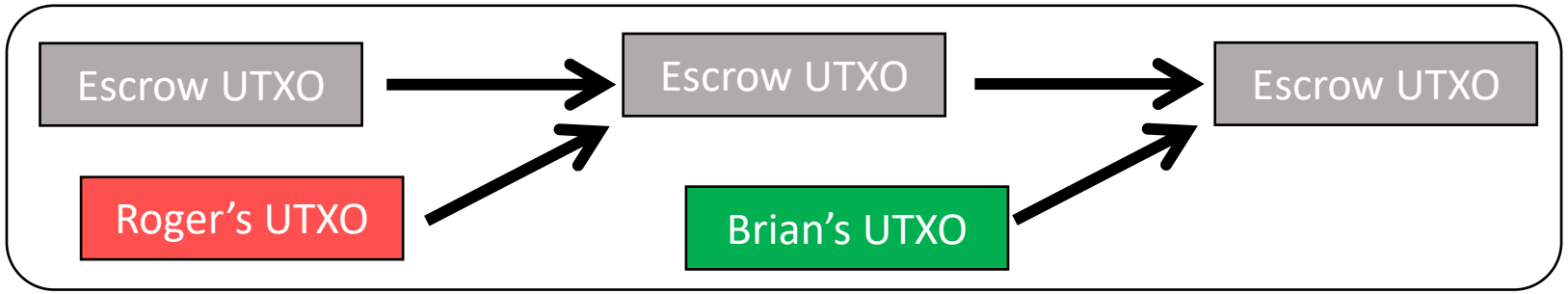
Roger's 50,000 BTC

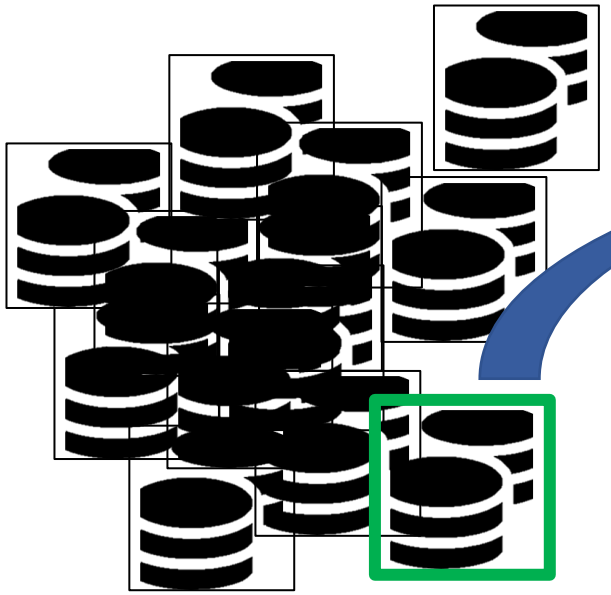


"Bitcoin Payments"

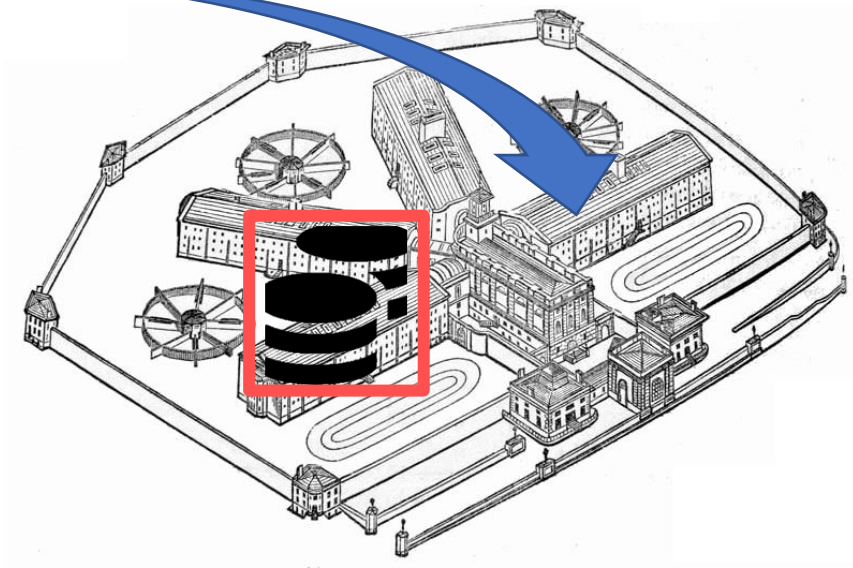
6a. Spend from Layer-1 to Layer-1.5

On layer-1:





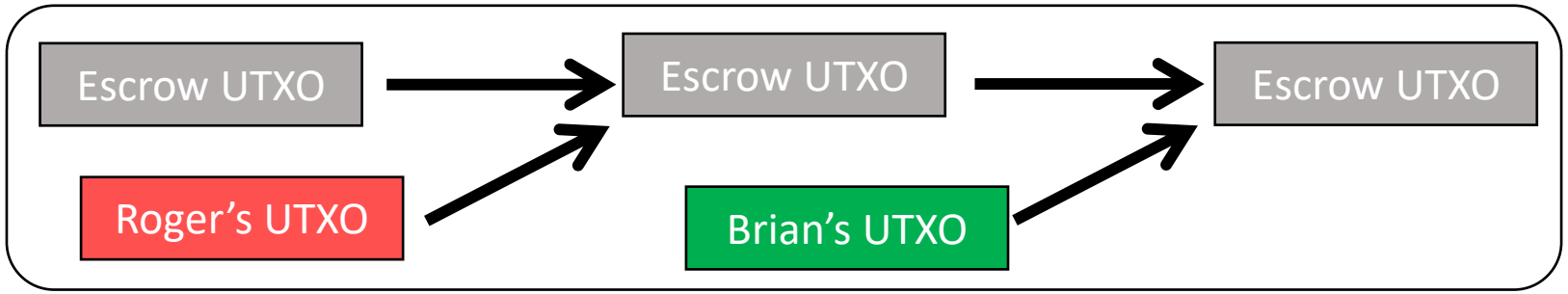
Brian's 7,000 BTC

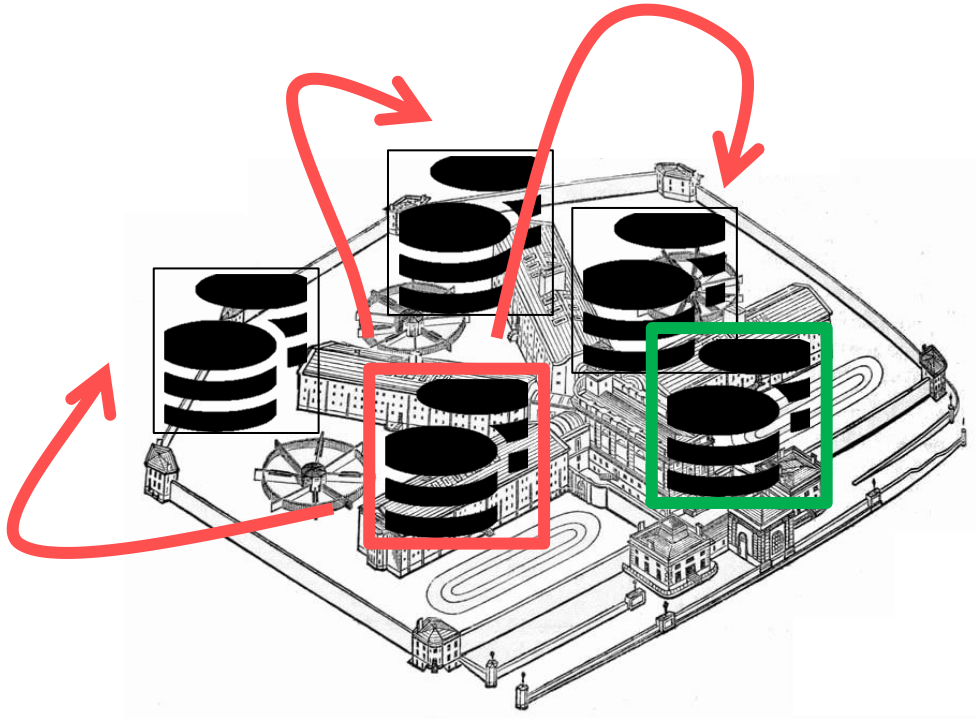


"Bitcoin Payments"

6b. Spend from Layer-1 to Layer-1.5

On layer-1:





"Bitcoin Payments"

7. Spend within the Escrow

Generates txn fee revenues for miners

Sideshift, Shapeshift, Atomic Swaps, Etc

SIDESHIFT.AI

TEST PILOT STAGE

Become An Affiliate: Shill friends, get money

Choose conversion

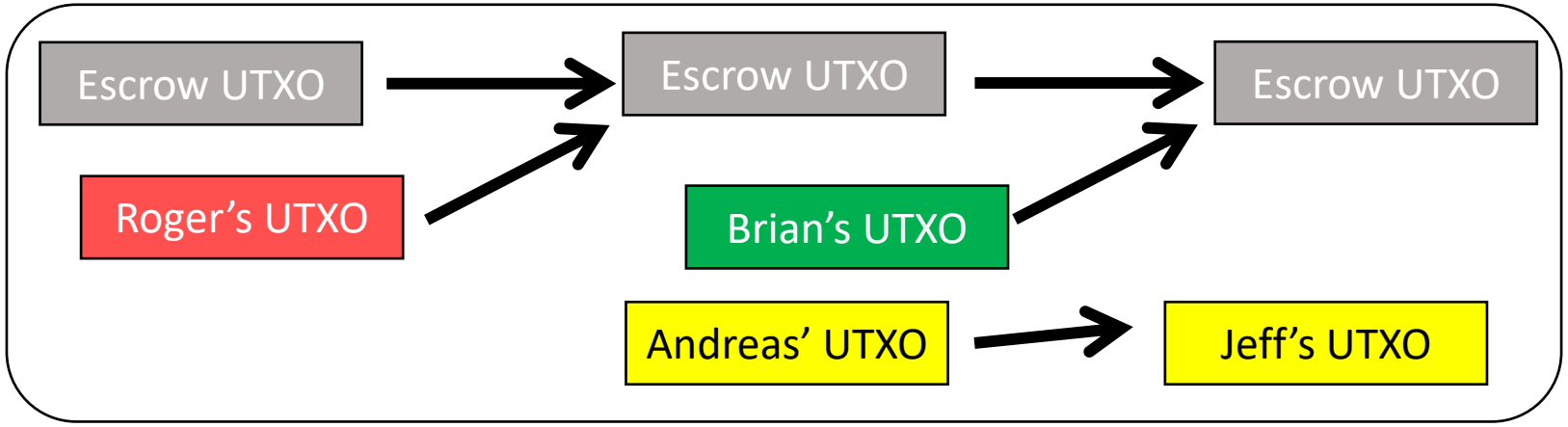
Bitcoin (Lightning) → Tether USD

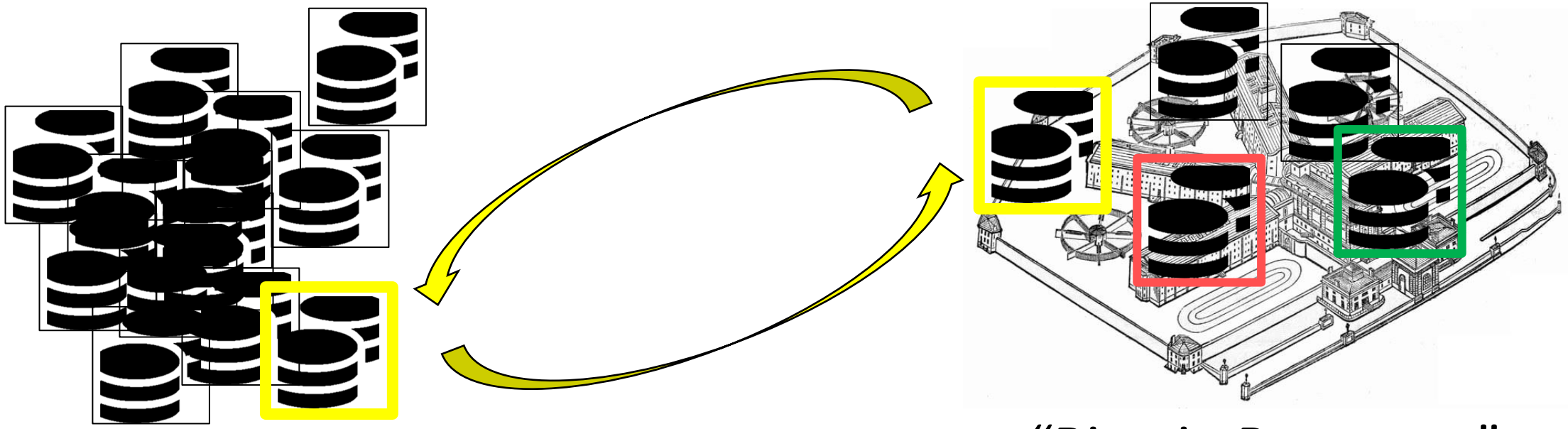
SHIFT

Time	From	To
7 hours ago	⚡0.0003 BTC	0.008601 ETH
16 hours ago	0.0149022 BTC	0.9805 ZEC
17 hours ago	⚡0.00001 BTC	0.03671 USDT
17 hours ago	⚡0.00001 BTC	
17 hours ago	0.00868722 BTC	

8a. Swapping to Instant Freedom

On layer-1:

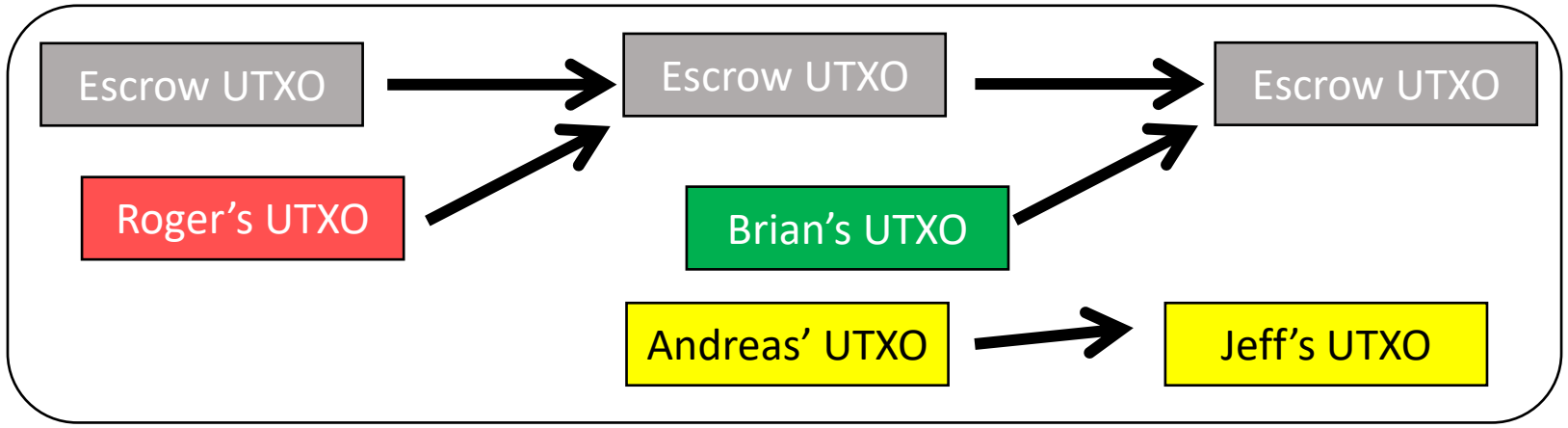


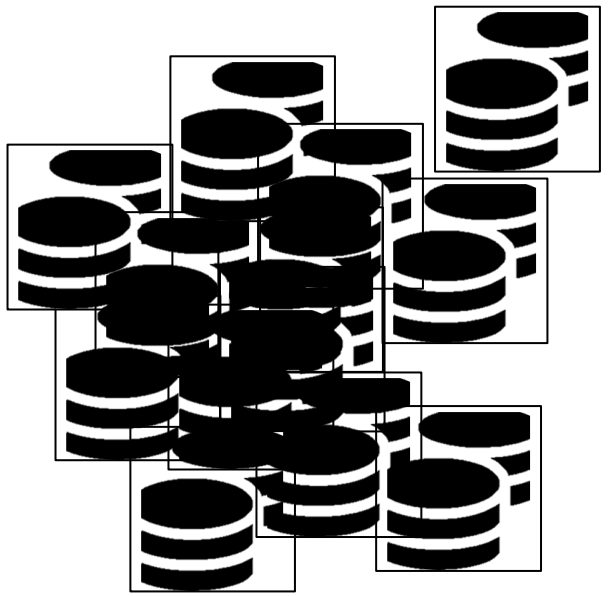


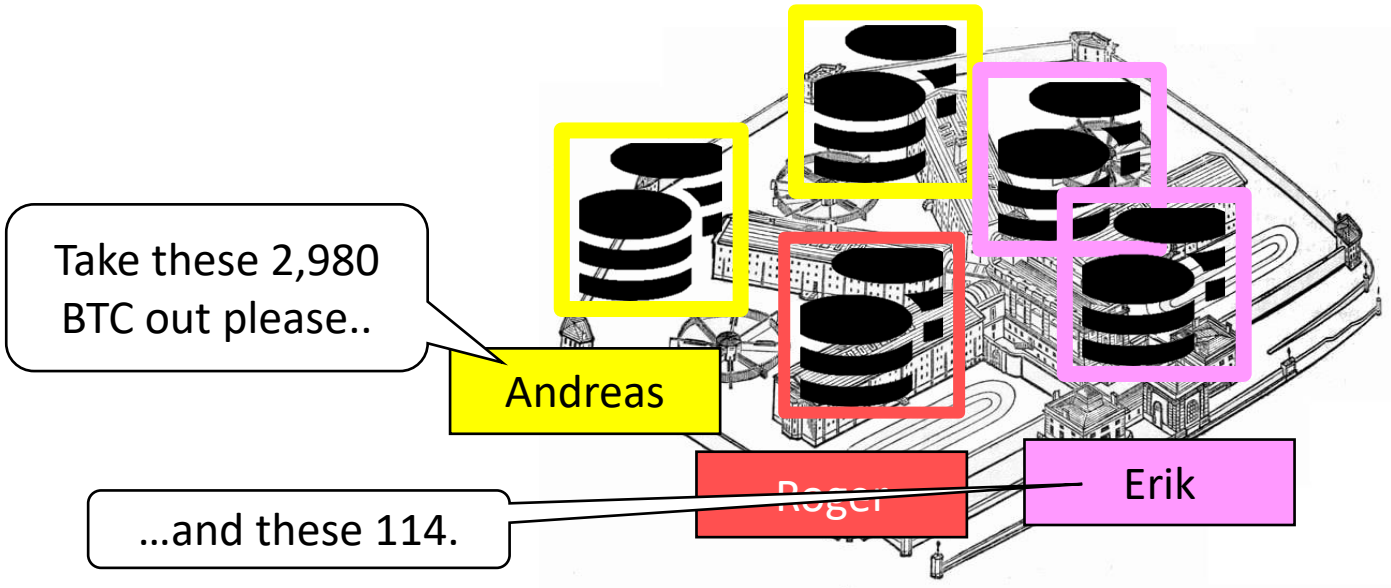
"Bitcoin Payments"

8b. Prisoner Exchange

On layer-1:

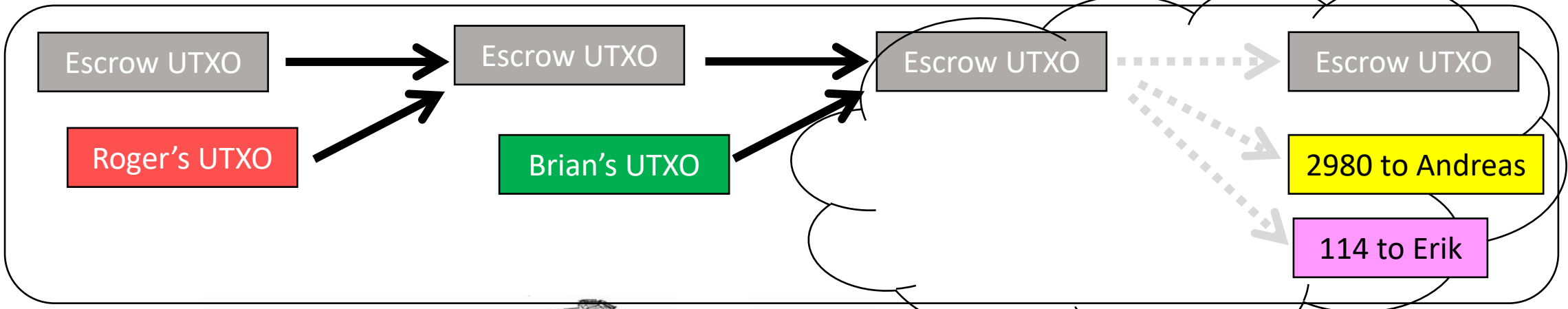




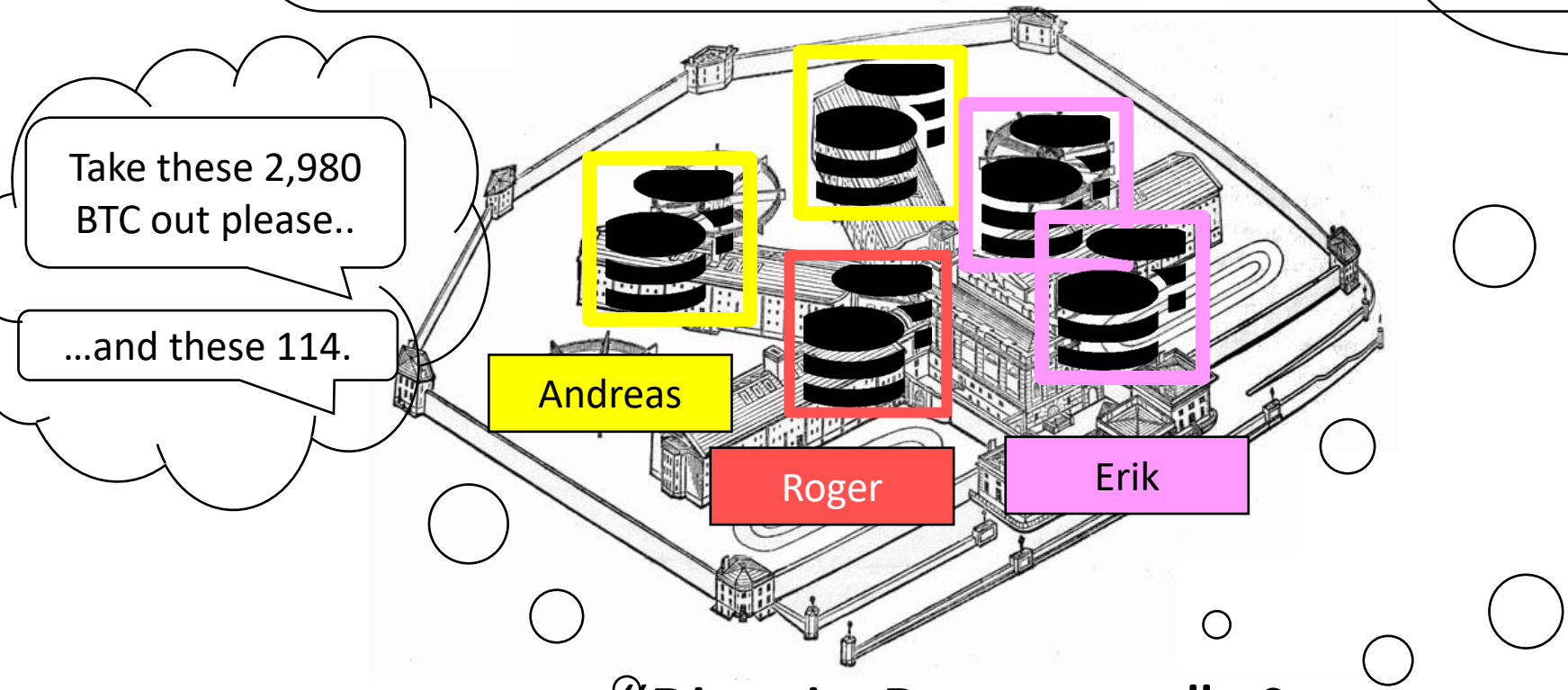


"Bitcoin Payments"

9. Leaving Prison



32 bytes



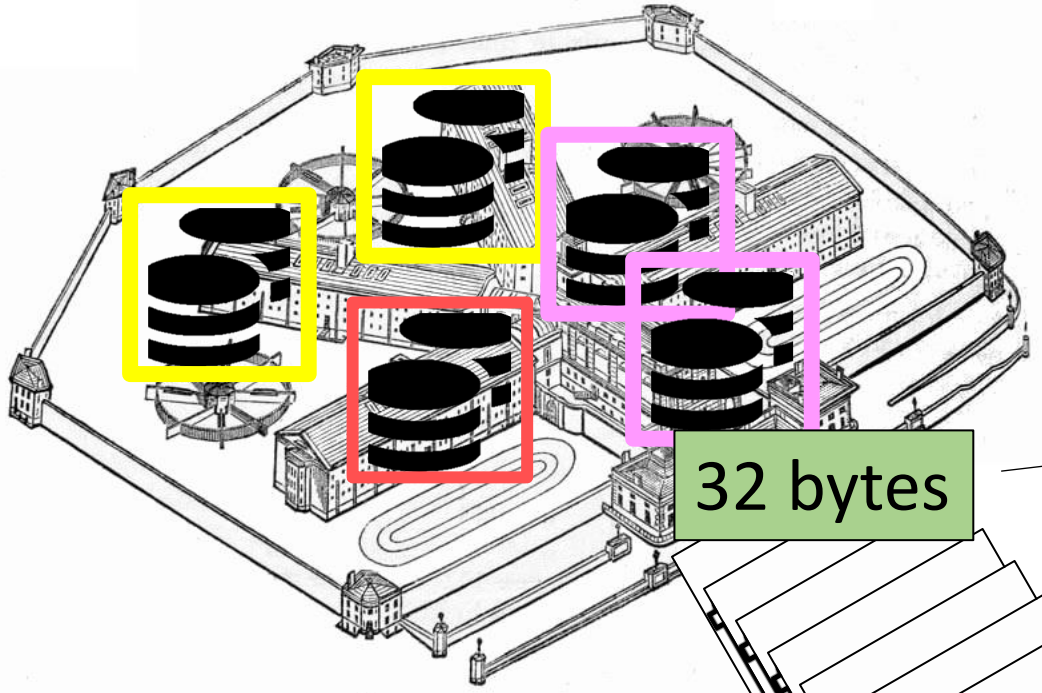
What do I need?

@"Bitcoin Payments"

10. The Withdrawal Txn

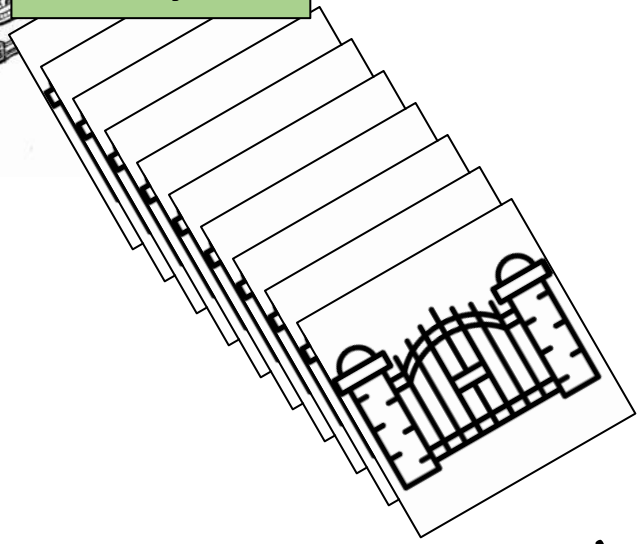

Debug window
Information
Console
Network Traffic
Peers
getblockheader
00:27:47
getblockheader
00:27:47
{
"hash":
"84e51e142b7410dad573e0b63225cc935c27a29ca3fd1c1fe147d9b03e89a5ce",
"confirmations": 1,
"height": 83,
"version": 536870912,
"versionHex": "20000000",
"merkleroot":
"6fb20a8389a1442abd4b7d540e9c68c0e7bbb9bdb42b2d243c5d40d33deed605",
"time": 1556522344,
"mediantime": 1556522316,
"nonce": 0,
"bits": "207fffff",
"difficulty": 4.656542373906925e-10,
"chainwork":
"hashwtprime":
"0000000000000000000000000000000000000000000000000000000000000000",
"previousblockhash":
"4fb9bd41b134fda5638a4c9da2f8419eefb7dae5ab9e70c621c5fe1dc86115cf"
}
32 bytes
10. The Withdrawal Txn

Prison Metaphor



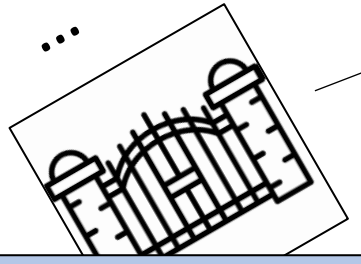
32 bytes

1st gate



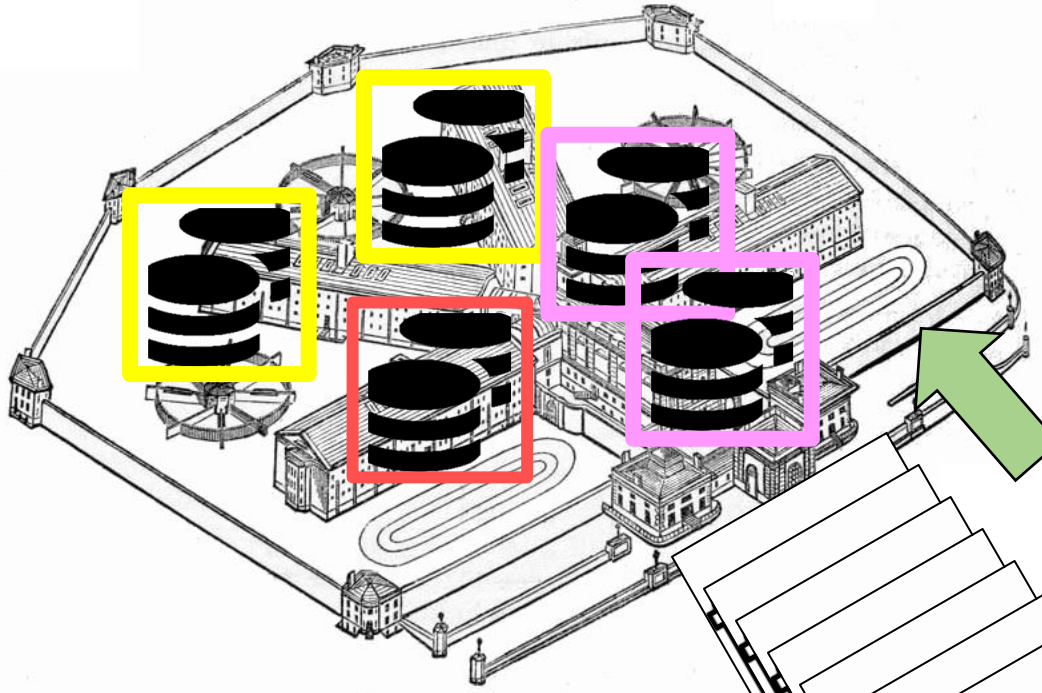
...

13150th gate



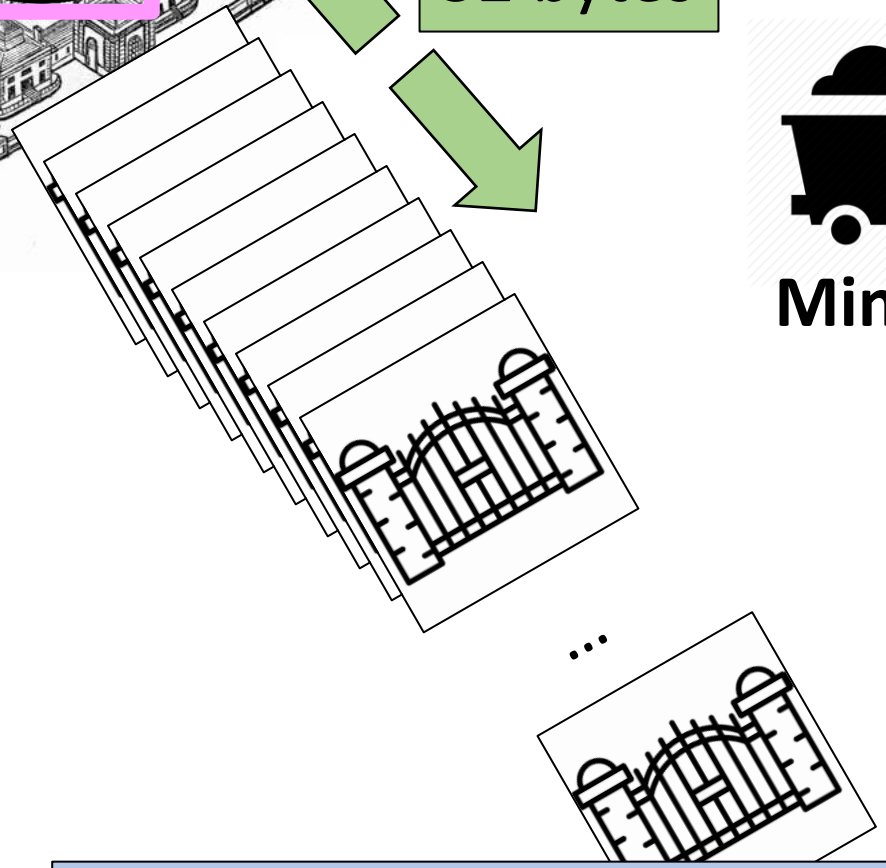
11. Starting Off…

Prison Metaphor



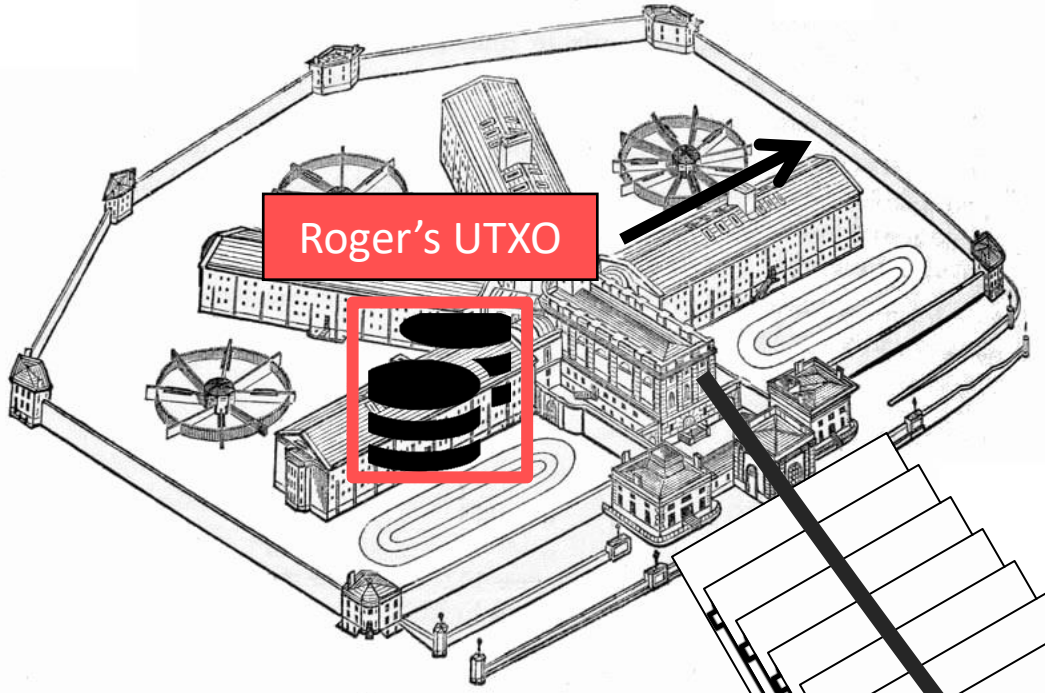
32 bytes

Miners

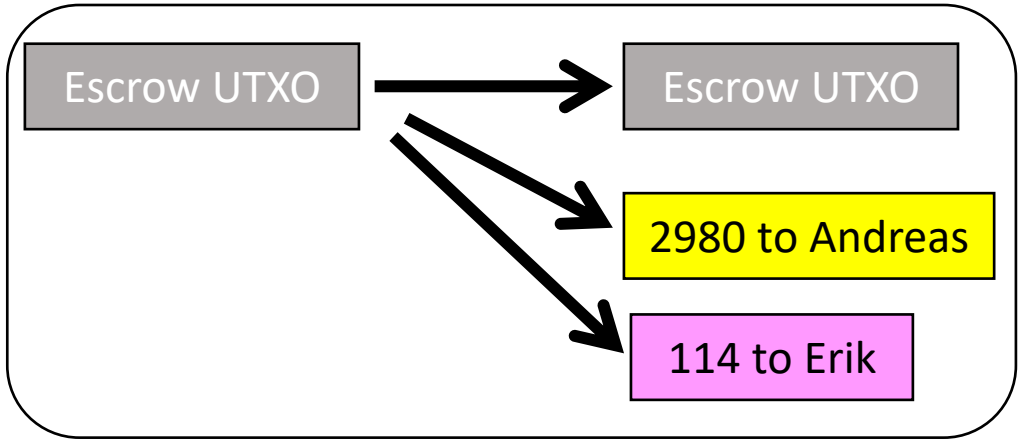


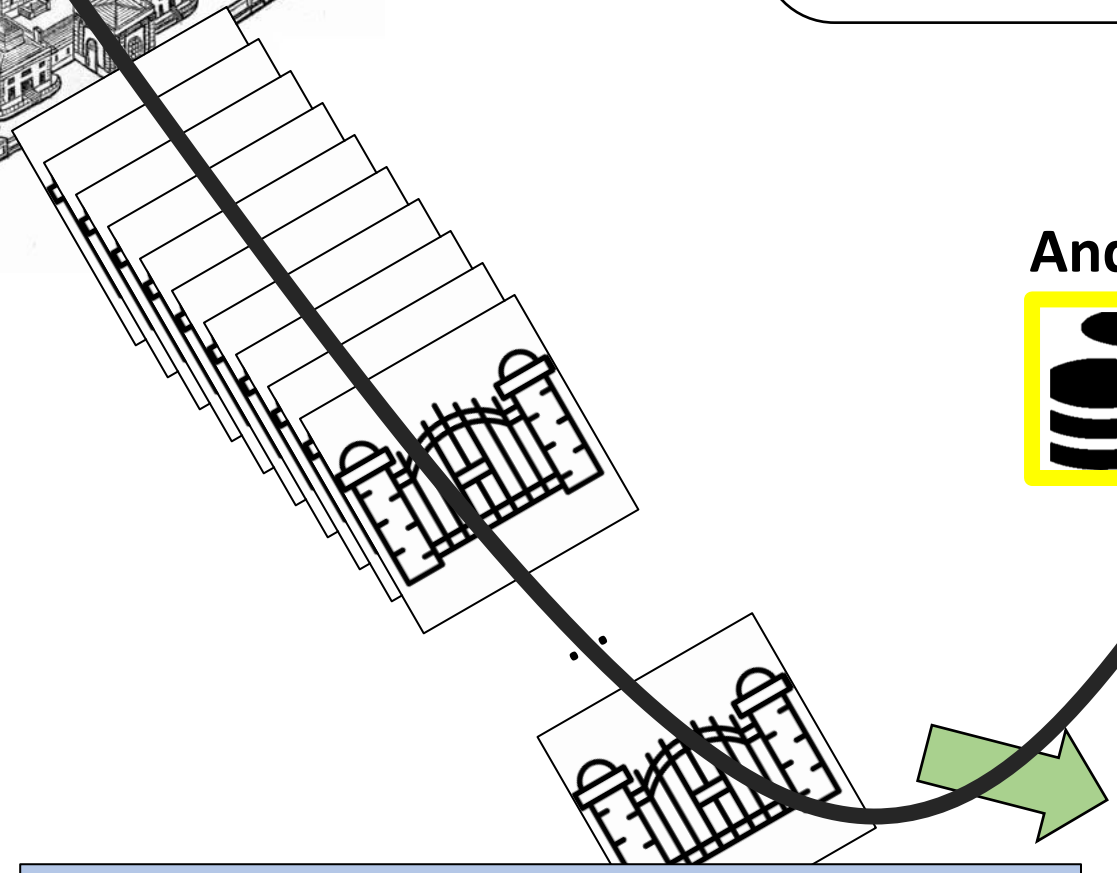
...

12. Making Progress…



On layer-1:



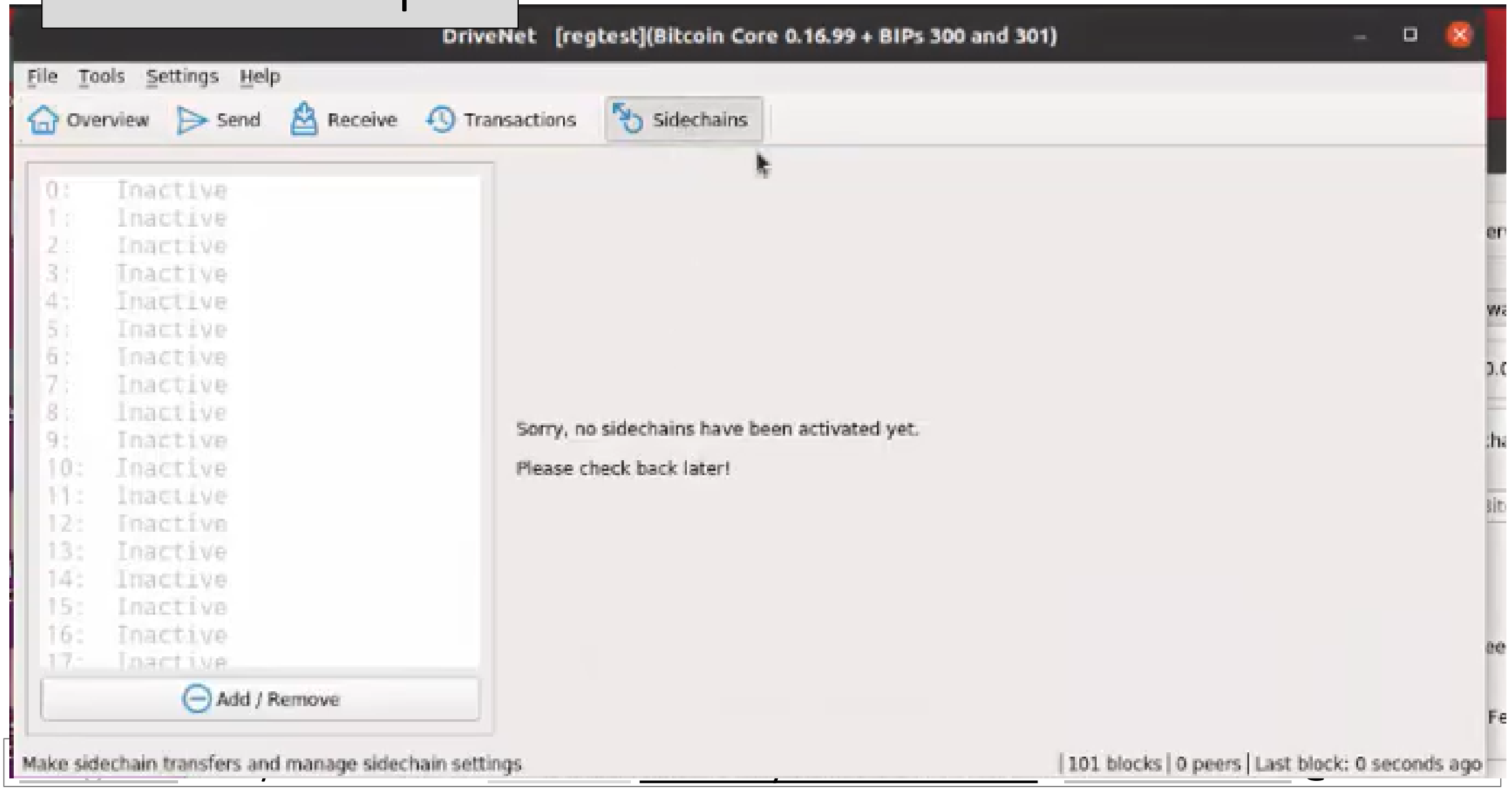


32 bytes

13. Withdrawal Complete

3 - zCash Example

zCash Example

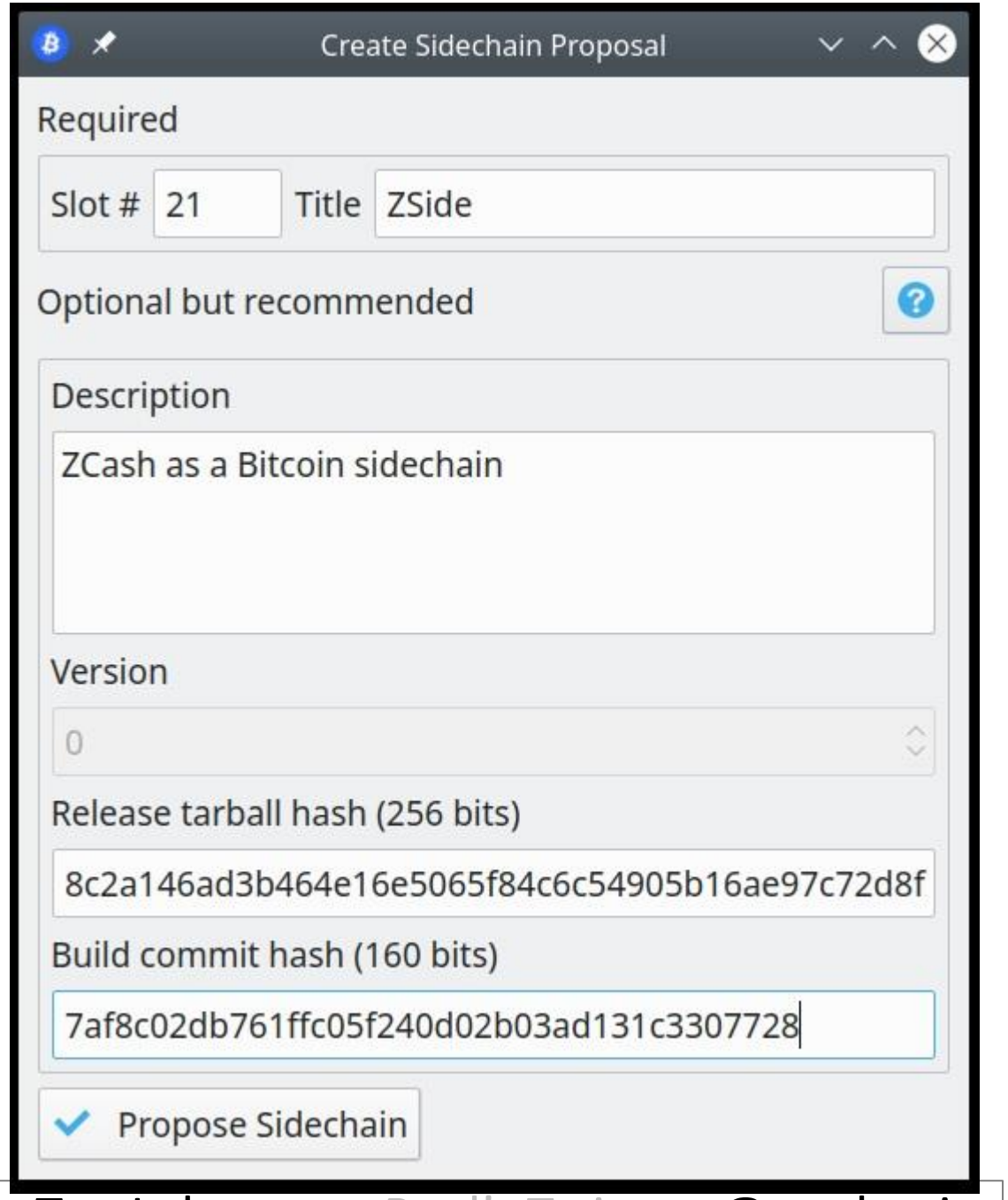


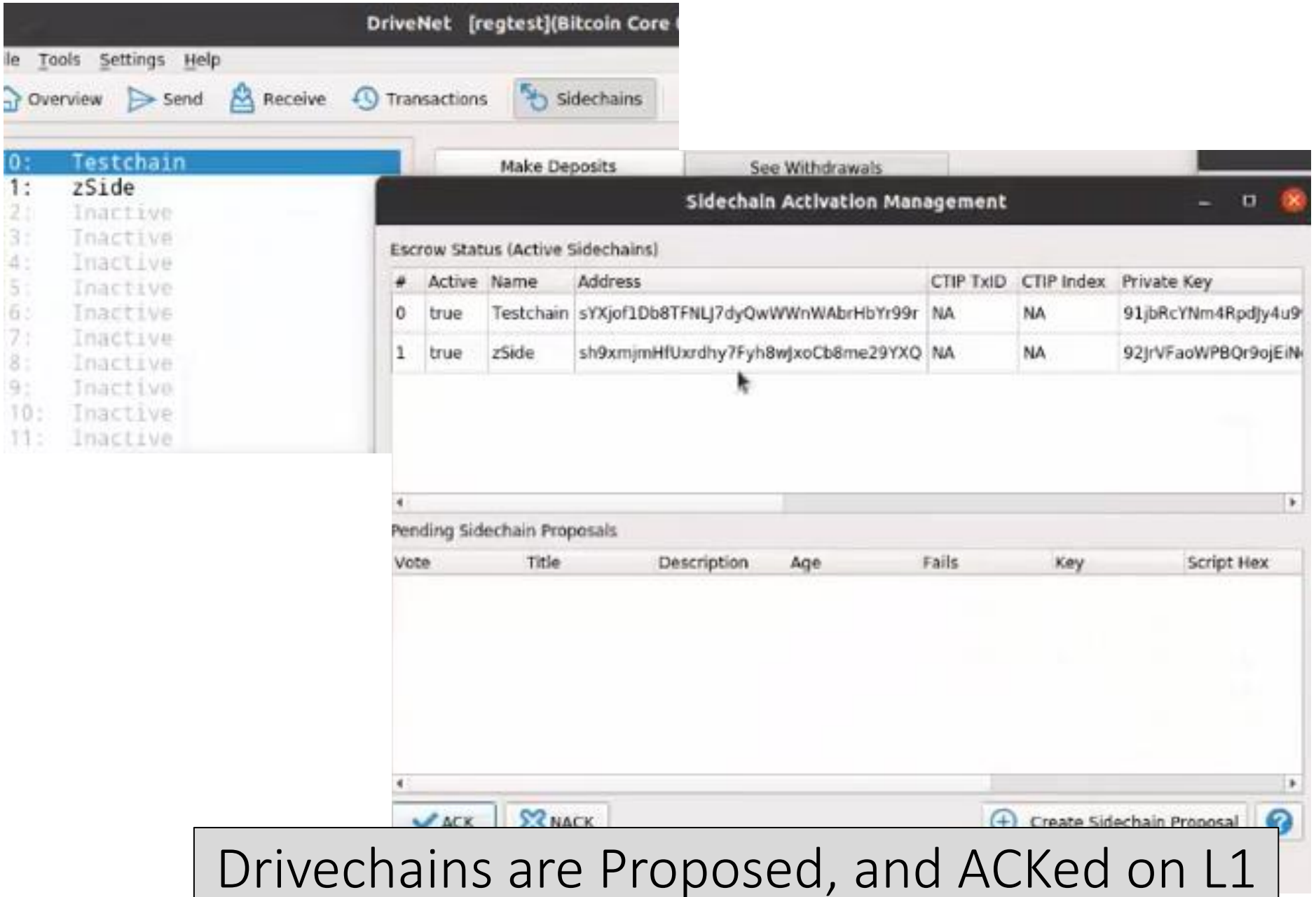
Take a “Slot”

A *coinbase message* announcing that we want to assign Slot 1:

a global name, and

some optional info to identify the L2 node software



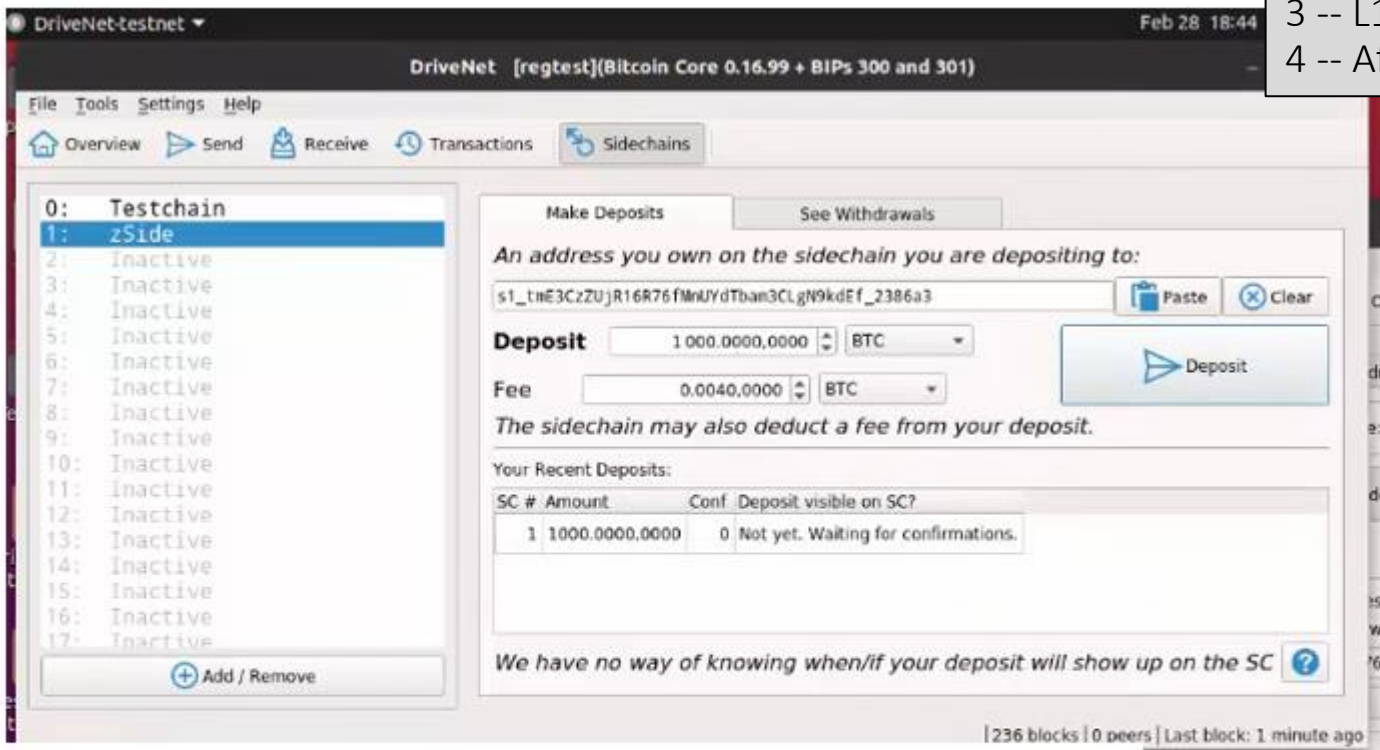


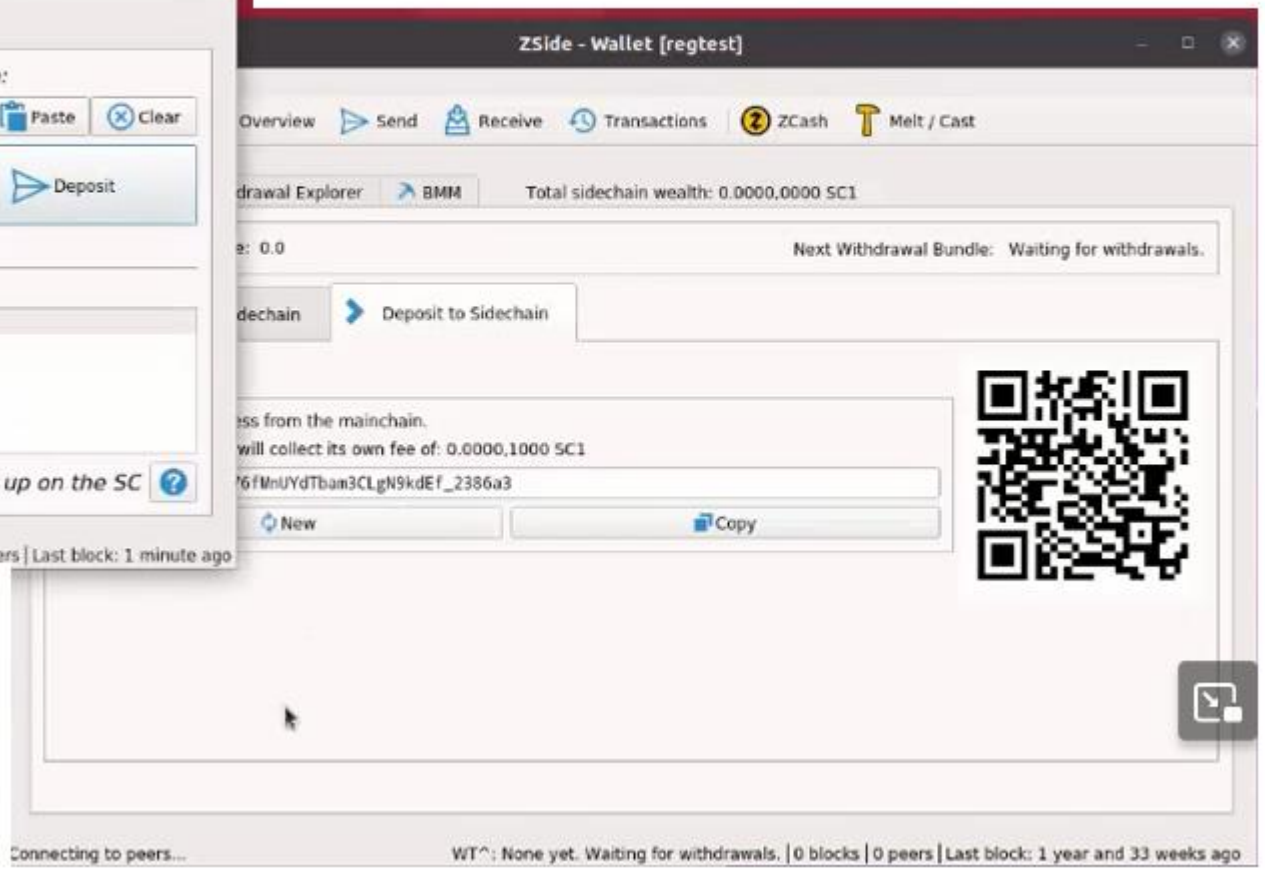
Drivechains are Proposed, and ACKed on L1

Each proposal / Ack is a message in a L1 coinbase txn

Deposit

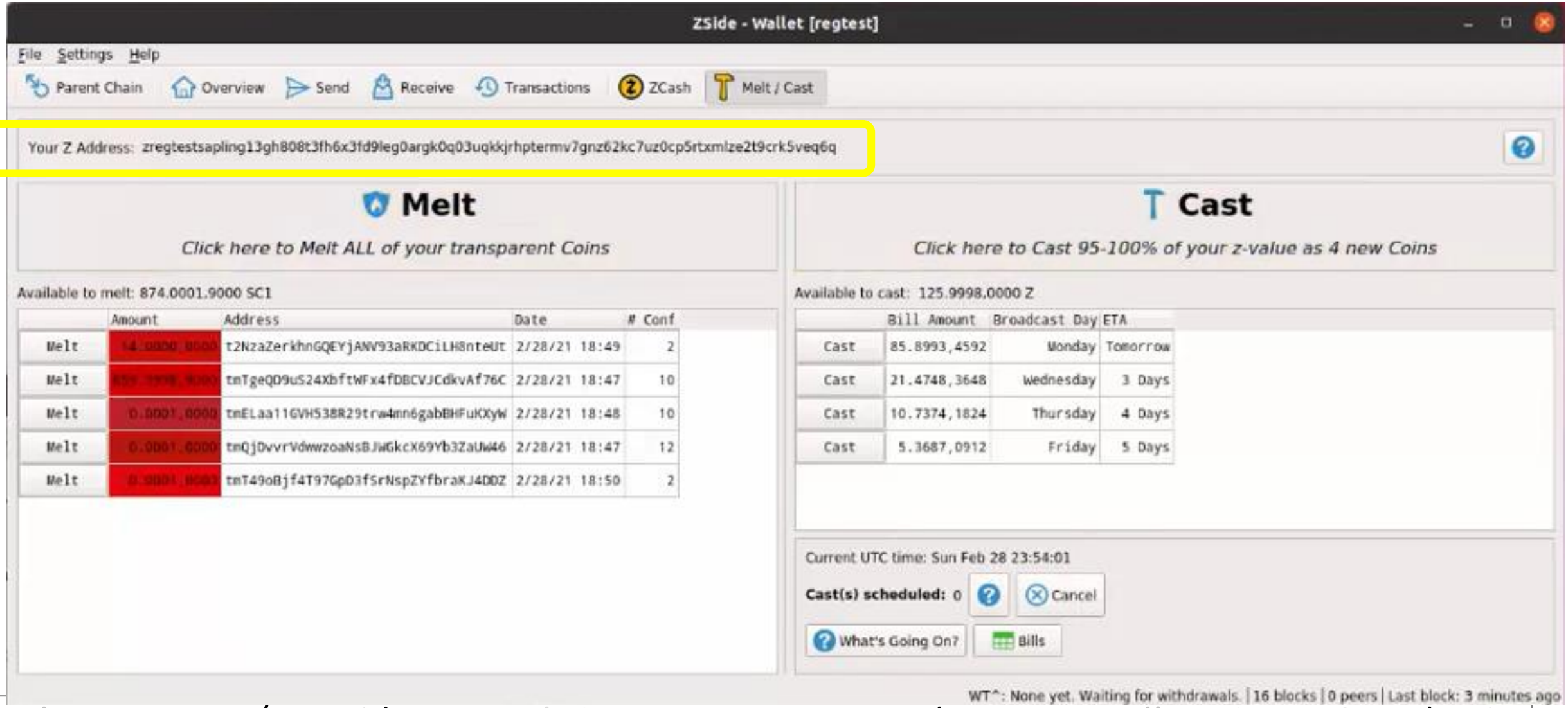
1 -- Get destination address from zCash-Drivechain
2 -- Give that to L1
3 -- L1 broadcasts the deposit
4 -- After the deposit confirms on L1, L2 credits user the coins.



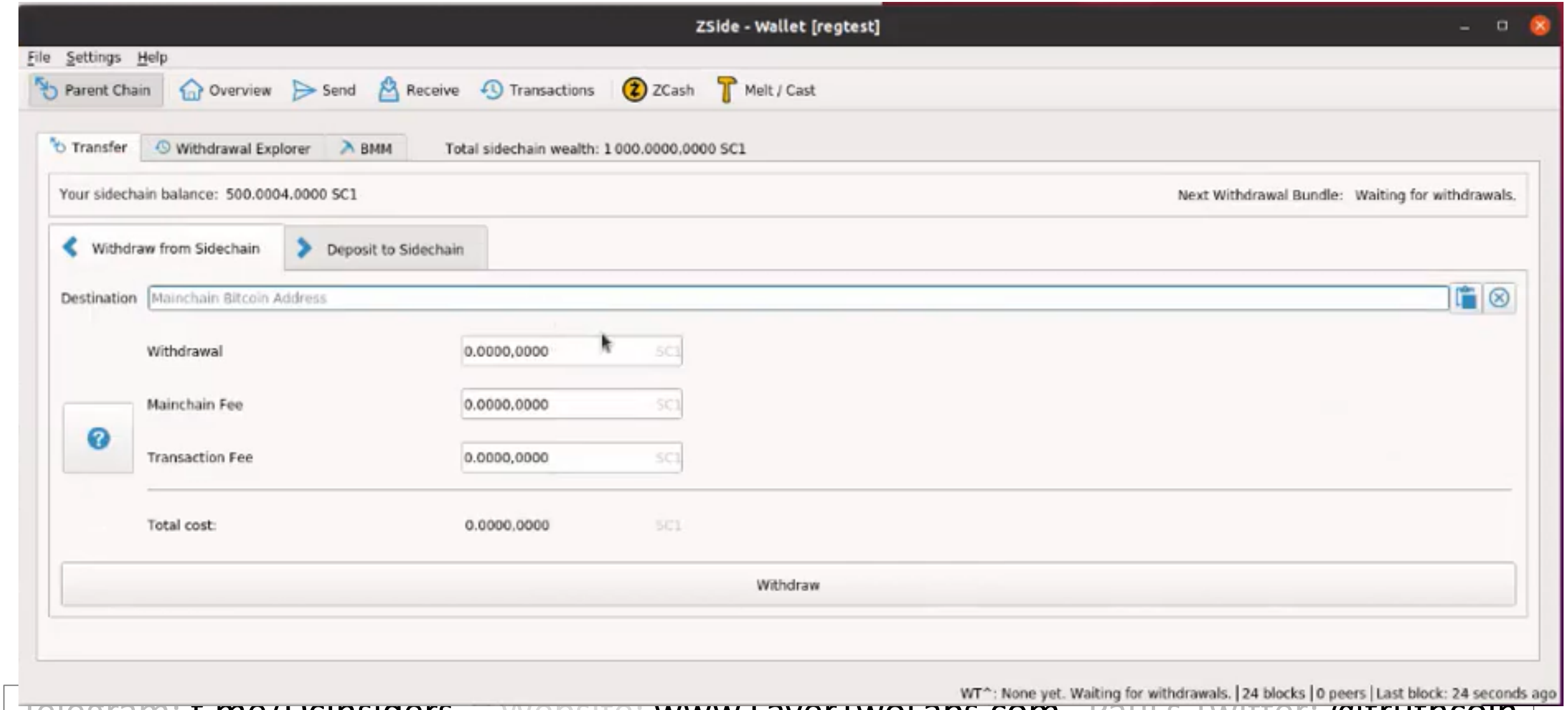


zCash Features

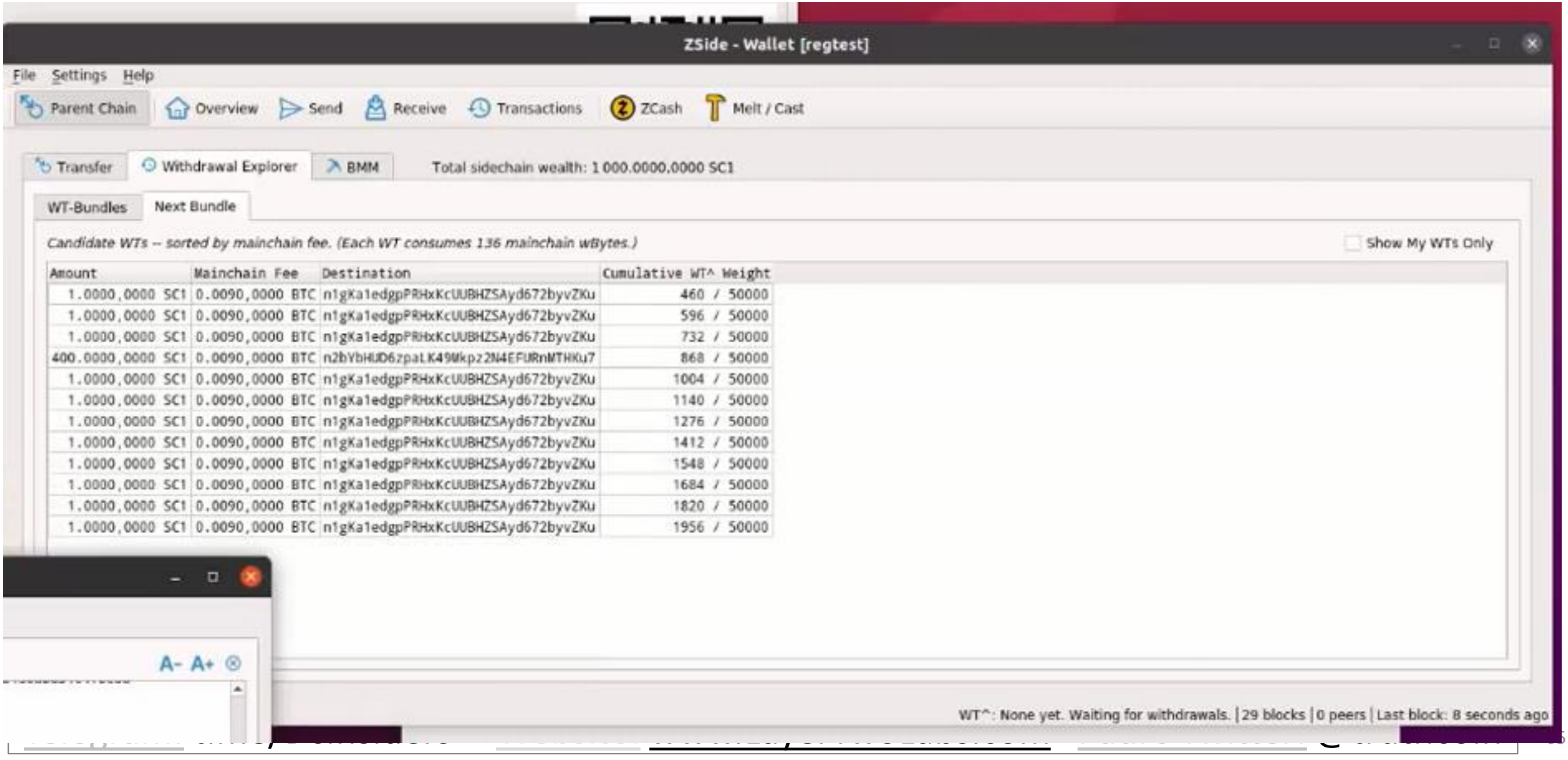
Now we have a z-address to use!

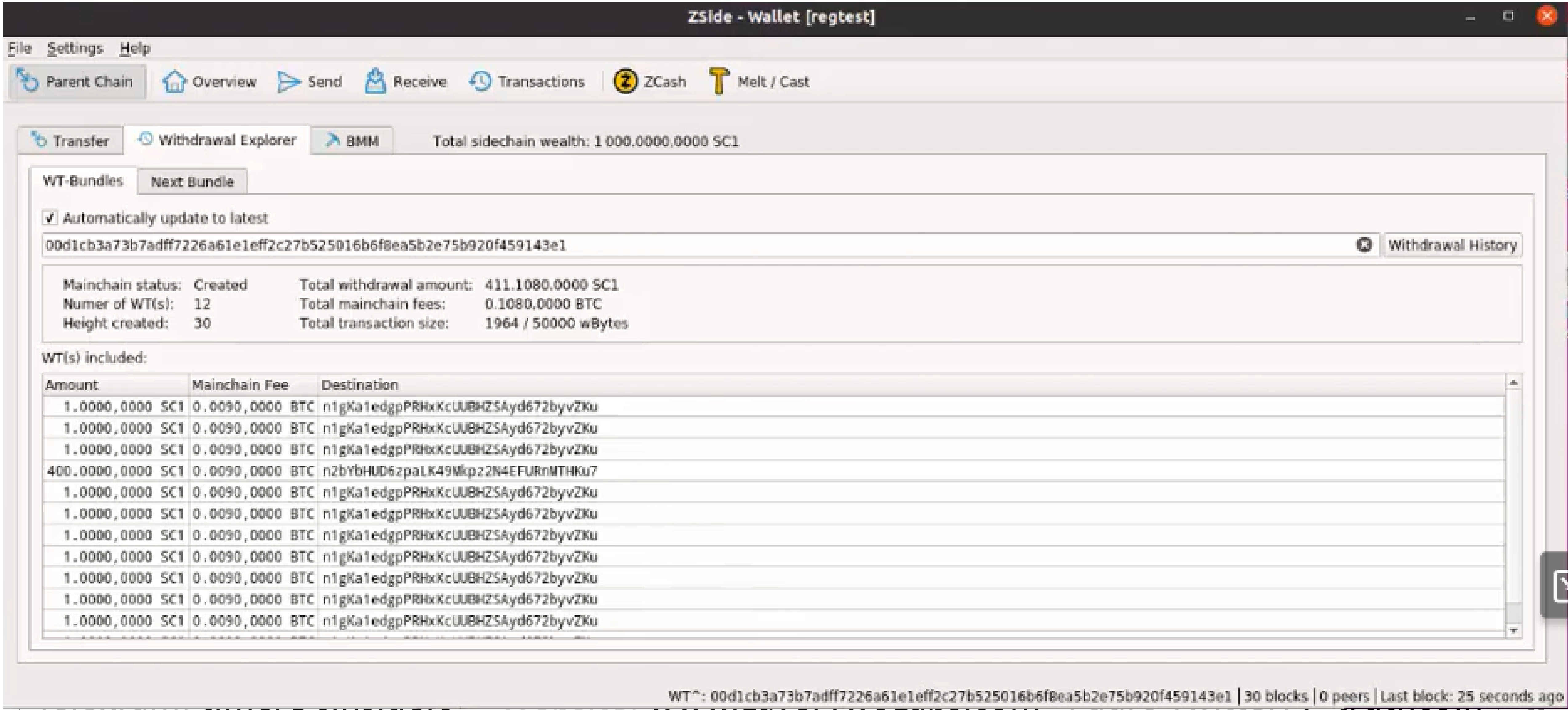


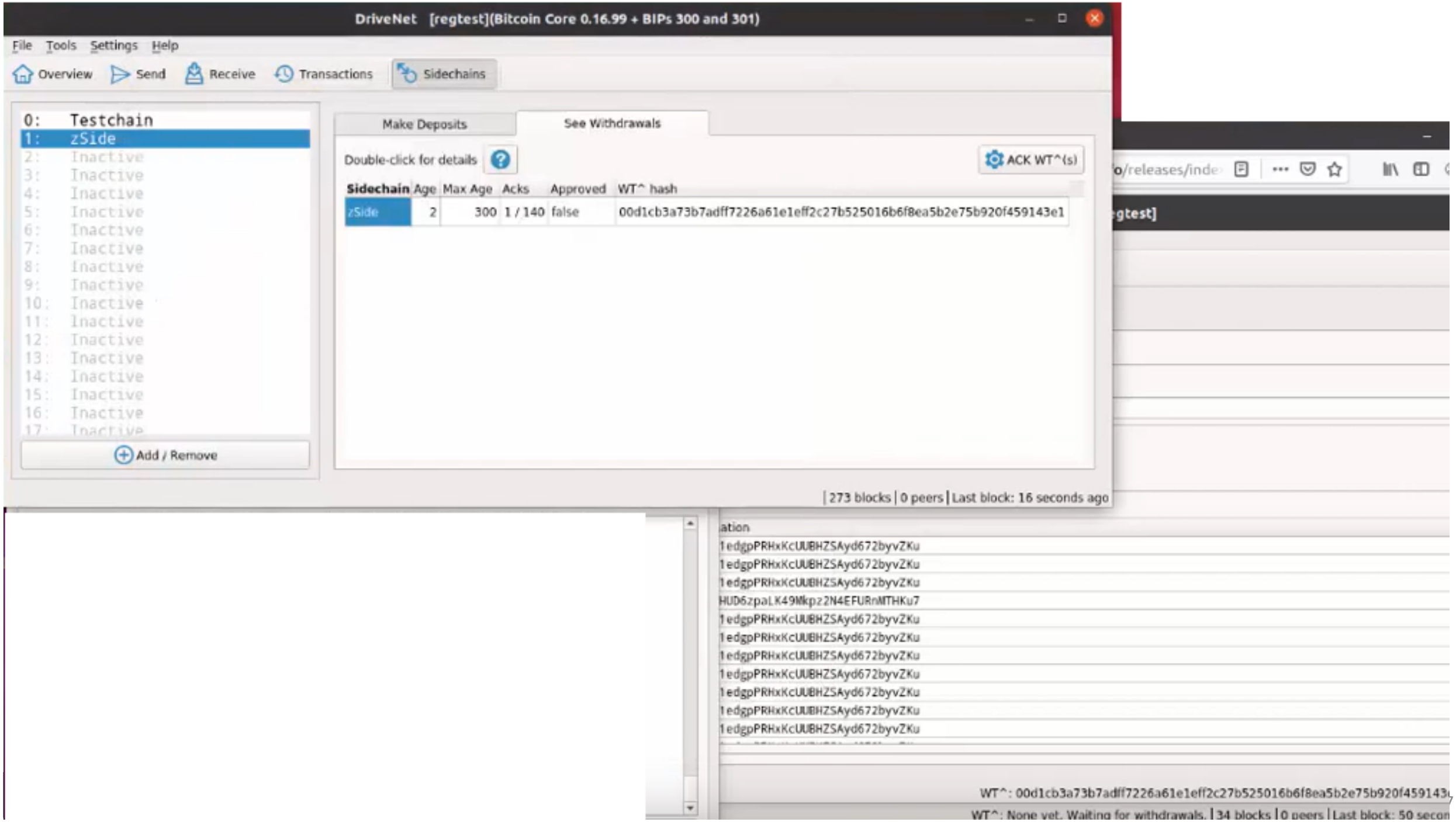
Withdrawing Bit-Zcash to Layer1 BTC

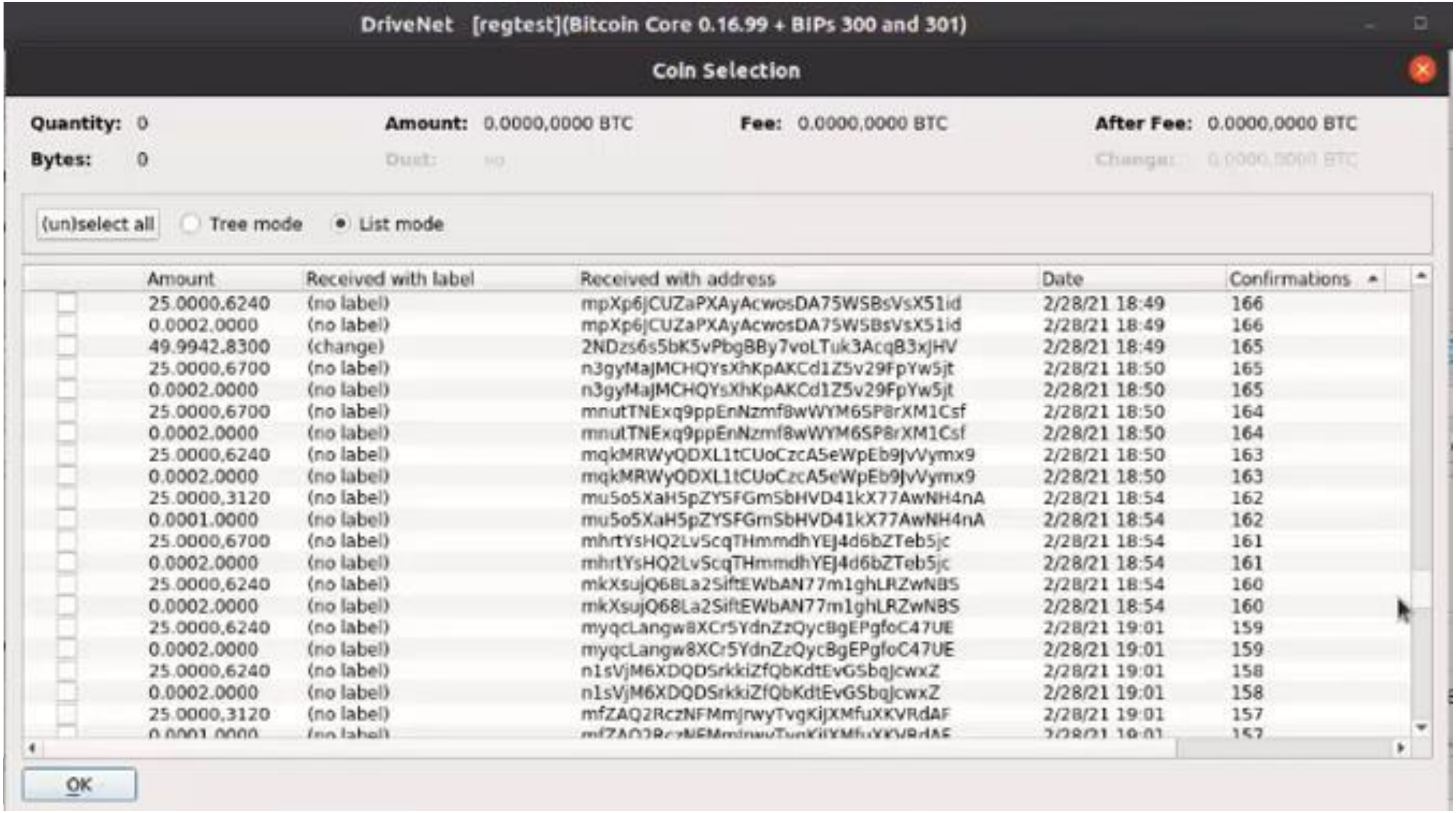



ZSide - Wallet [regtest]
File Settings Help
Parent Chain
Overview
Send
Receive
Transactions
ZCash
Melt / Cast
Transfer
Withdrawal Explorer
BMM
Total sidechain wealth: 1 000.0000,0000 SC1
WT-Bundles
Next Bundle
Candidate WTs -- sorted by mainchain fee. (Each WT consumes 136 mainchain wBytes.)
Show My WTs Only
Amount
Mainchain Fee
Destination
Cumulative WT^ Weight
400.0000,0000 SC1
0.0090,0000 BTC
n2bYbHUD6zpaLK49Wkpz2N4EFURnWTHKu7
460 / 50000


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 136 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 | n2bYbHUD6zpaLK49Wkpz2N4EFURnMTHKu7 | 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
Numer of WT(s): 12
Height created: 30
Total withdrawal amount: 411.1080.0000 SC1
Total mainchain fees: 0.1080.0000 BTC
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 | n2bYbHUD6zpaLK49Nkpz2N4EFURnMTHKu7
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
WT^: 00d1cb3a73b7adff7226a61e1eff2c27b525016b6f8ea5b2e75b920f459143e1 | 30 blocks | 0 peers | Last block: 25 seconds ago


DriveNet [regtest](Bitcoin Core 0.16.99 + BIPs 300 and 301)
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
12: Inactive
13: Inactive
14: Inactive
15: Inactive
16: Inactive
17: Inactive
Add / Remove
Make Deposits
See Withdrawals
Double-click for details
ACK WT^(s)
Sidechain Age Max Age Acks Approved WT^ hash
zSide 2 300 1 / 140 false 00d1cb3a73b7adff7226a61e1eff2c27b525016b6f8ea5b2e75b920f459143e1
| 273 blocks | 0 peers | Last block: 16 seconds ago
ation
1edgpPRHxKcUUBHZSAyd672byvZKu
1edgpPRHxKcUUBHZSAyd672byvZKu
1edgpPRHxKcUUBHZSAyd672byvZKu
HUD6zpaLK49MkpZ2N4EFURnMTHKu7
1edgpPRHxKcUUBHZSAyd672byvZKu
1edgpPRHxKcUUBHZSAyd672byvZKu
1edgpPRHxKcUUBHZSAyd672byvZKu
1edgpPRHxKcUUBHZSAyd672byvZKu
1edgpPRHxKcUUBHZSAyd672byvZKu
1edgpPRHxKcUUBHZSAyd672byvZKu
1edgpPRHxKcUUBHZSAyd672byvZKu
WT^: 00d1cb3a73b7adff7226a61e1eff2c27b525016b6f8ea5b2e75b920f459143
WT^: None yet. Waiting for withdrawals. | 34 blocks | 0 peers | Last block: 50 secon


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
(un)select all
Tree mode
List mode
Amount
Received with label
Received with address
Date
Confirmations
25.0000,6240 (no label) mpXp6jCUZaPXAyAcwosDA75WSBsVsX51id 2/28/21 18:49 166
0.0002.0000 (no label) mpXp6jCUZaPXAyAcwosDA75WSBsVsX51id 2/28/21 18:49 166
49.9942.8300 (change) 2NDzs6s5bK5vPbgBBy7voLTuk3Acq83xJHV 2/28/21 18:49 165
25.0000,6700 (no label) n3gyMajMCHQYsXhKpAKCd1Z5v29FpYw5jt 2/28/21 18:50 165
0.0002.0000 (no label) n3gyMajMCHQYsXhKpAKCd1Z5v29FpYw5jt 2/28/21 18:50 165
25.0000,6700 (no label) mnutTNExq9ppEnNzmf8wWYM6SP8rXM1Csf 2/28/21 18:50 164
0.0002.0000 (no label) mnutTNExq9ppEnNzmf8wWYM6SP8rXM1Csf 2/28/21 18:50 164
25.0000,6240 (no label) mqkMRWyQDXL1tCUoCzcA5eWpEb9JvVymx9 2/28/21 18:50 163
0.0002.0000 (no label) mqkMRWyQDXL1tCUoCzcA5eWpEb9JvVymx9 2/28/21 18:50 163
25.0000,3120 (no label) mu5o5XaH5pZYSFGmSbHVD41kX77AwNH4nA 2/28/21 18:54 162
0.0001.0000 (no label) mu5o5XaH5pZYSFGmSbHVD41kX77AwNH4nA 2/28/21 18:54 162
25.0000,6700 (no label) mhrtYsHQ2LvScqTHmmdhYEJ4d6bZTeb5jc 2/28/21 18:54 161
0.0002.0000 (no label) mhrtYsHQ2LvScqTHmmdhYEJ4d6bZTeb5jc 2/28/21 18:54 161
25.0000,6240 (no label) mkXsujQ68La2SiftEWbAN77m1ghLRZwN8S 2/28/21 18:54 160
0.0002.0000 (no label) mkXsujQ68La2SiftEWbAN77m1ghLRZwN8S 2/28/21 18:54 160
25.0000,6240 (no label) myqcLangw8XCr5YdnZzQyc8gEPgfoC47UE 2/28/21 19:01 159
0.0002.0000 (no label) myqcLangw8XCr5YdnZzQyc8gEPgfoC47UE 2/28/21 19:01 159
25.0000,6240 (no label) n1sVjM6XDQDSrkkiZfQbKdtEvGSbqJcwxZ 2/28/21 19:01 158
0.0002.0000 (no label) n1sVjM6XDQDSrkkiZfQbKdtEvGSbqJcwxZ 2/28/21 19:01 158
25.0000,3120 (no label) mfZAQ2RczNFMmjnwyTvgKijXMfuXKVRdAF 2/28/21 19:01 157
OK

4 - The BIP Text

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):

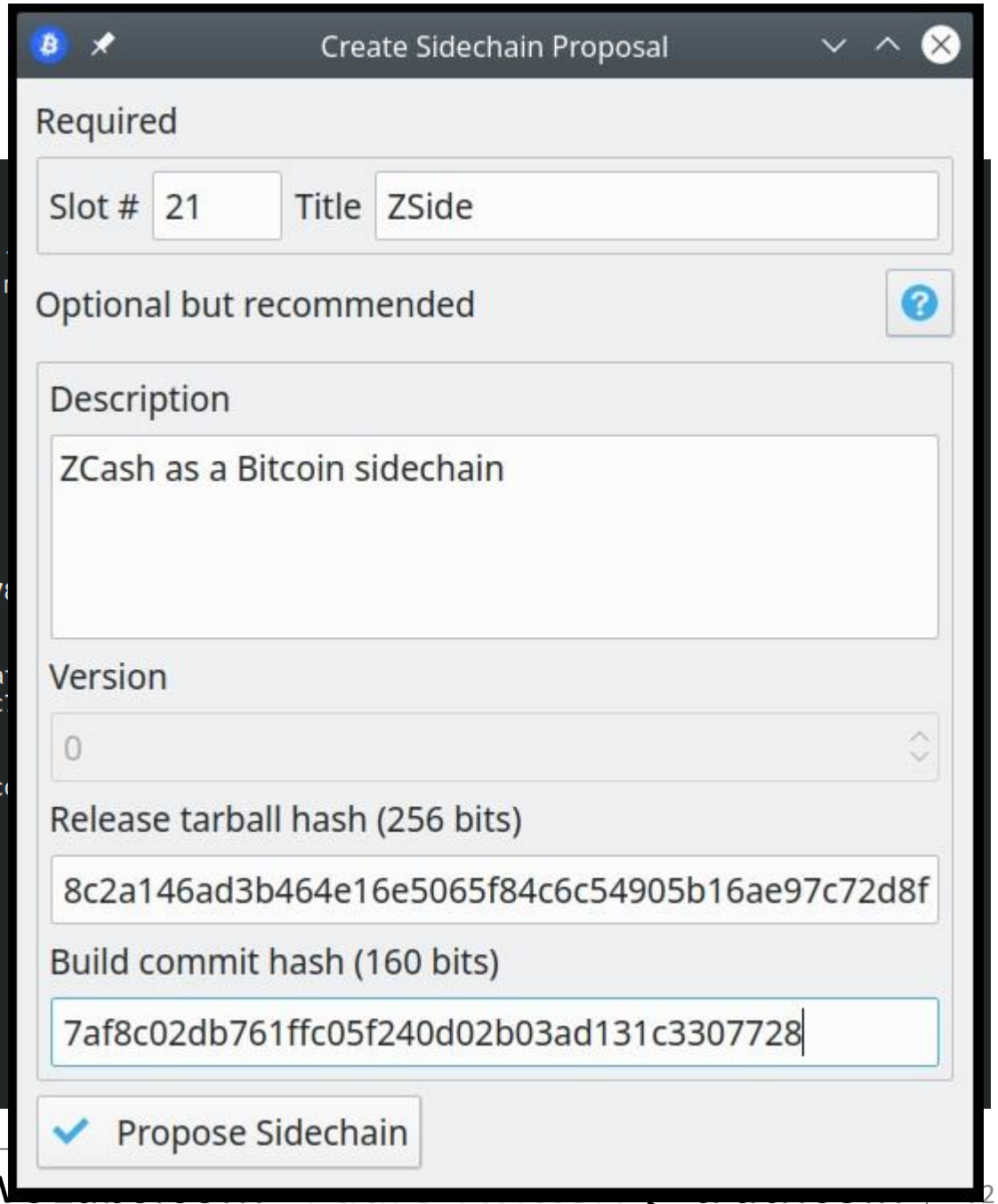
- M1. "Propose New Sidechain"
- M2. "ACK Proposal"
- M3. "Propose Bundle"
- M4. "ACK Bundle"
- M5. Deposit -- a transfer of BTC from-main-to-side
- M6. Withdrawal -- a transfer of BTC from-side-to-main

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

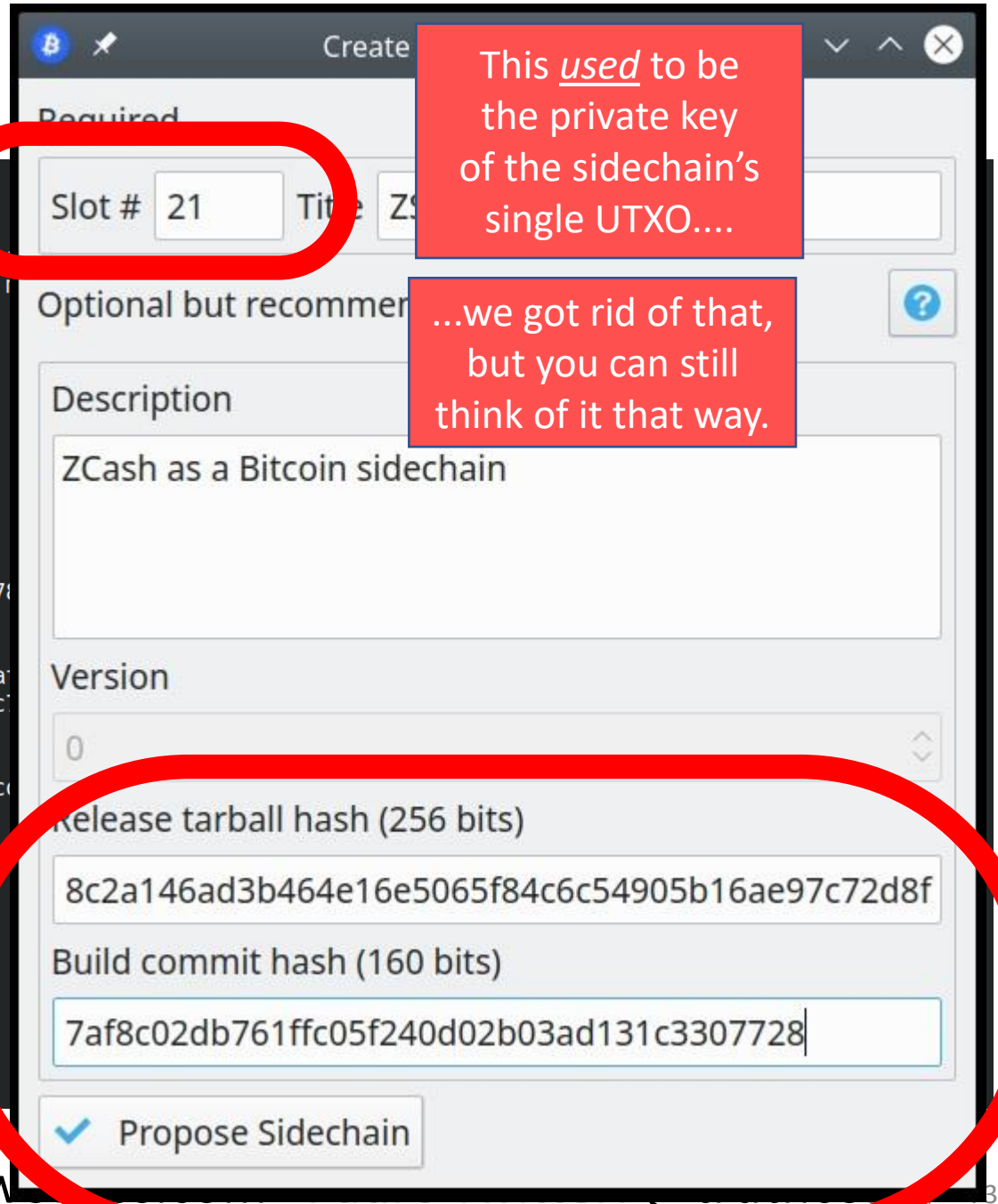
```
cryptaxe@hal:~/Drivechain$ ./src/drivechain-cli help createsidechainproposal
createsidechainproposal
Generates a sidechain proposal to be included in the next block mined by this node.
Note that this will not broadcast the proposal to other nodes. You must mine a block which
Pending proposals created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

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 7
db27608c7428251c6755e5a1d9e9313

> curl --user myusername --data-binary '{"jsonrpc": "1.0", "id":"curltest", "method": "crea
chain" 0 78b140259d5626e17c4bf339c23cb4fa8d16d138f71d9803ec394bb01c051f0b 90869d013db27608c
.1:8332/

cryptaxe@hal:~/Drivechain$ ./src/drivechain-cli createsidechainproposal 1 "Namecoin" "Namec
d9803ec394bb01c051f0b 90869d013db27608c7428251c6755e5a1d9e9313
{
  "nSidechain": 1,
  "title": "Namecoin",
  "description": "Namecoin as a Bitcoin sidechain",
  "privatekey": "5JPjosnCe69m5S6JFahcc6AQsDEoRadjE4LZj4dmGkv2EfPFKma",
  "keyid": "c6fbd9b51c3883fb3d5f41a3d930fadca7ca3483",
  "version": 0,
  "hashID1": "78b140259d5626e17c4bf339c23cb4fa8d16d138f71d9803ec394bb01c051f0b",
  "hashID2": "90869d013db27608c7428251c6755e5a1d9e9313"
}
```



M1

```
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 whi
Pending proposals created by this node will automatically be included in the soonest block

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 78
db27608c7428251c6755e5a1d9e9313

> curl --user myusername --data-binary '{"jsonrpc": "1.0", "id":"curltest", "method": "creat
chain" 0 78b140259d5626e17c4bf339c23cb4fa8d16d138f71d9803ec394bb01c051f0b 90869d013db27608c7
.1:8332/

cryptaxe@hal:~/Drivechain$ ./src/drivechain-cli createsidechainproposal 1 "Namecoin" "Namec
d9803ec394bb01c051f0b 90869d013db27608c7428251c6755e5a1d9e9313
{
  "nSidechain": 1,
  "title": "Namecoin",
  "description": "Namecoin as a Bitcoin sidechain",
  "privatekey": "5JPjosnCe69m5S6JFahcc6AQsDEoRadjE4LZj4dmGkv2EfPFKma",
  "keyid": "c6fbd9b51c3883fb3d5f41a3d930fadca7ca3483",
  "version": 0,
  "hashID1": "78b140259d5626e17c4bf339c23cb4fa8d16d138f
  "hashID2": "90869d013db27608c7428251c6755e5a1d9e9313"
}
```

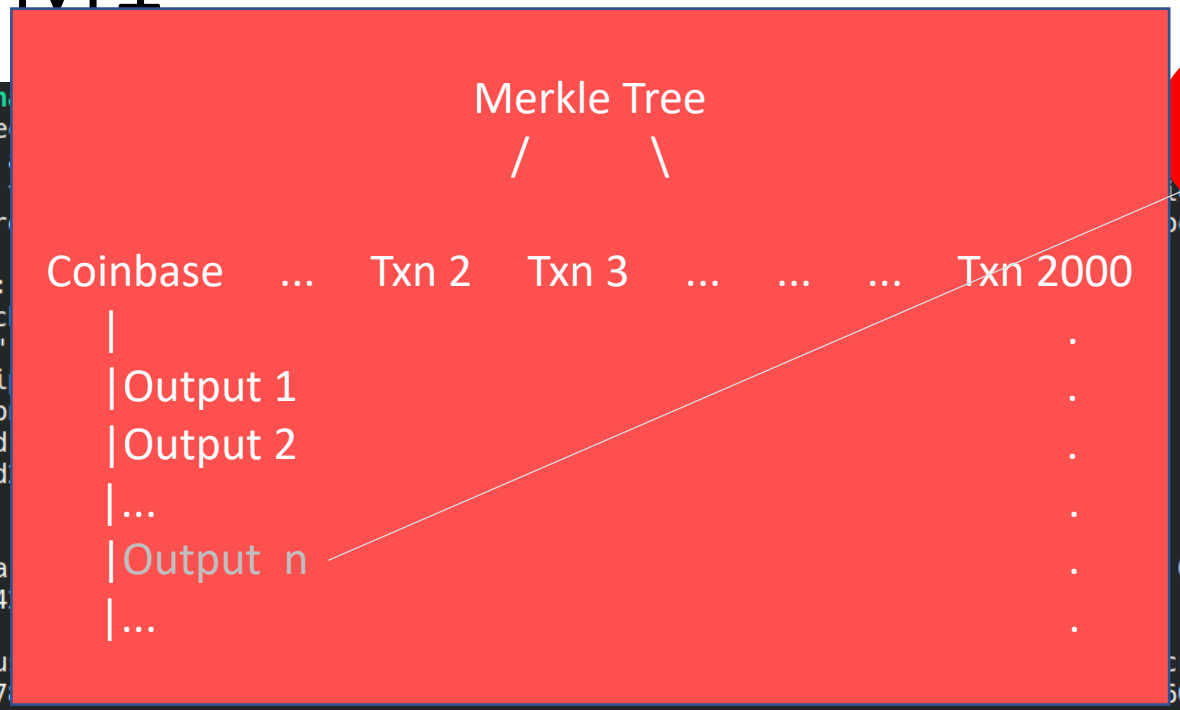
This helps people find (and agree on) the sidechain's full node software.



This *used* to be the private key of the sidechain's single UTXO....

...we got rid of that, but you can still think of it that way.

M1




```
cryptaxe@h
createside
Generates
Note that
Pending pr

Arguments:
1. "nsidec
2. "title"
3. "descri
4. "versio
5. "hashid
6. "hashid

Examples:
> drivecha
db27608c74

> curl --u
chain" 0 7
.1:8332/

cryptaxe@hal:~/Drivechain$ ./src/drivechain-cli createsidechainproposal 1 "Namecoin" "Namec
d9803ec394bb01c051f0b 90869d013db27608c7428251c6755e5a1d9e9313
{
  "nSidechain": 1,
  "title": "Namecoin",
  "description": "Namecoin as a Bitcoin sidechain",
  "privatekey": "5JPjosnCe69m5S6JFahcc6AQsDEoRadjE4LZj4dmGkv2EfPFKma",
  "keyid": "c6fbd9b51c3883fb3d5f41a3d930fadca7ca3483",
  "version": 0,
  "hashID1": "78b140259d5626e17c4bf339c23cb4fa8d16d138f
  "hashID2": "90869d013db27608c7428251c6755e5a1d9e9313"
}
```

This helps people find (and agree on) the sidechain's full node software.

1-byte - OP_RETURN (0x6a)
4-byte - Header (0xD5E0C4AF)
N-byte – SC serialization....
- 1-byte nSidechain
- 4-byte nVersion
- x-byte strKeyID
- x-byte strPrivKey
- x-byte scriptPubKey
- x-byte title
- x-byte description
- 32-byte hashID1
- 20-byte hashID2

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
```

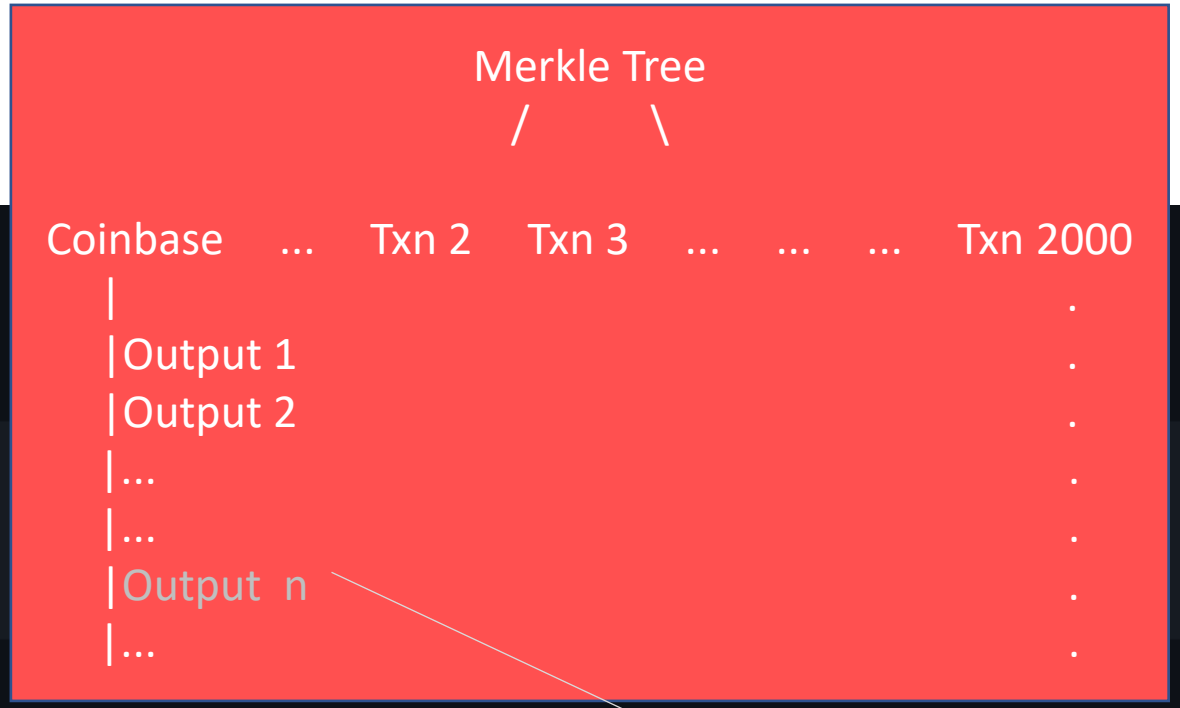
Notes

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

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

In Drivechain, “Bundles” are very important!

Bip300 withdrawals ("M6") are very significant.

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?

0x6AD45AA9435DE475C54F292D357B4665C4A06673354D0AF583ABEC2AC51B752FDF06FCDBBD

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 0xFFFE). 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.

Telegram: t.m

M4

M4 -- ACK Bundle(s)

M4 is a coinbase OP Return output containing the followin

```
1-byte - OP_RETURN (0x6a)
4-byte - Commitment header (0xD77D1776)
1-byte - Version
n-byte - The vector describing the "upvoted" bundl
```

Version 0x01 uses one byte per sidechain, and applies in m
situations where at least one sidechain has more than 256 c
possible: 0x03 might say "do exactly what was done in the p
sidechains). 0x04 might say "upvote everyone who is clearly

If a sidechain has no pending bundles, then it is skipped ov

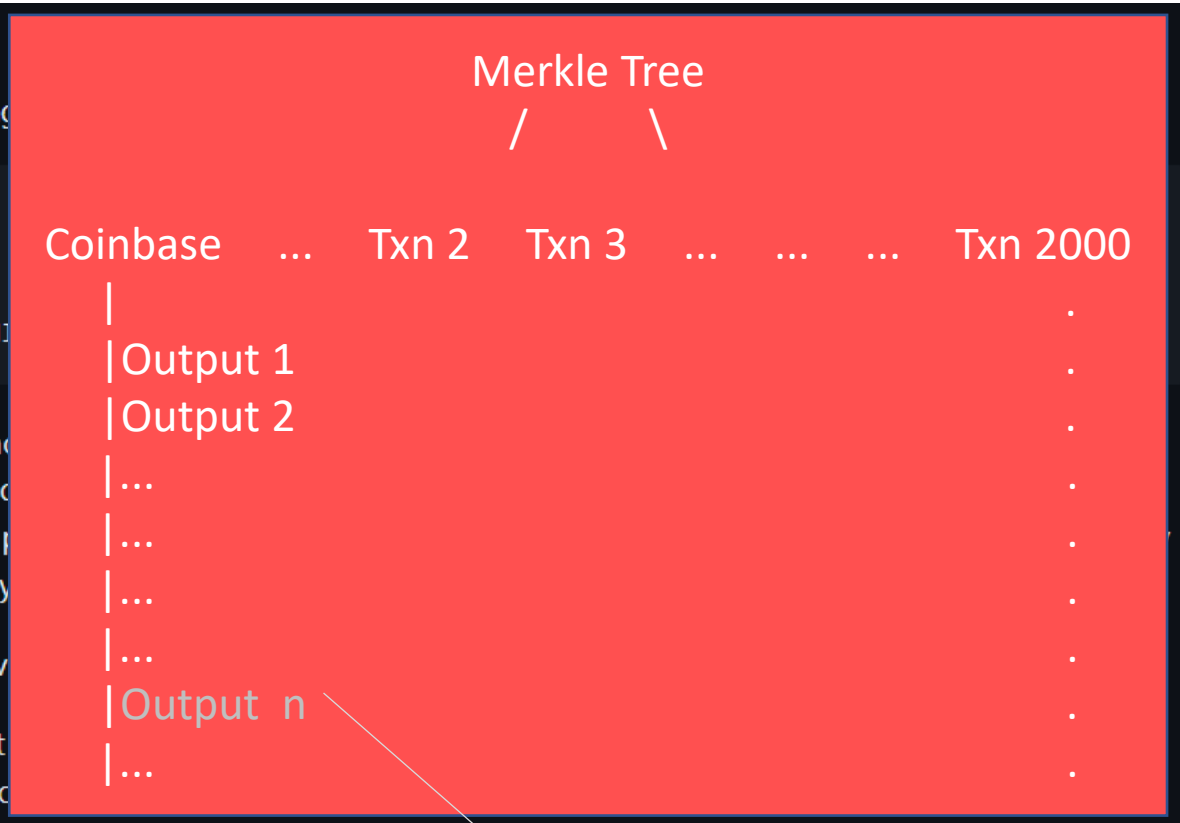
The upvote vector will code "abstain" as 0xFF (or 0xFFFF); it
withdrawal-bundle in the list, is the one to be "upvoted". Fo
sidechain #1 plus the 4th bundle on sidechain #2, then the vector would be 0x0704.

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,

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").

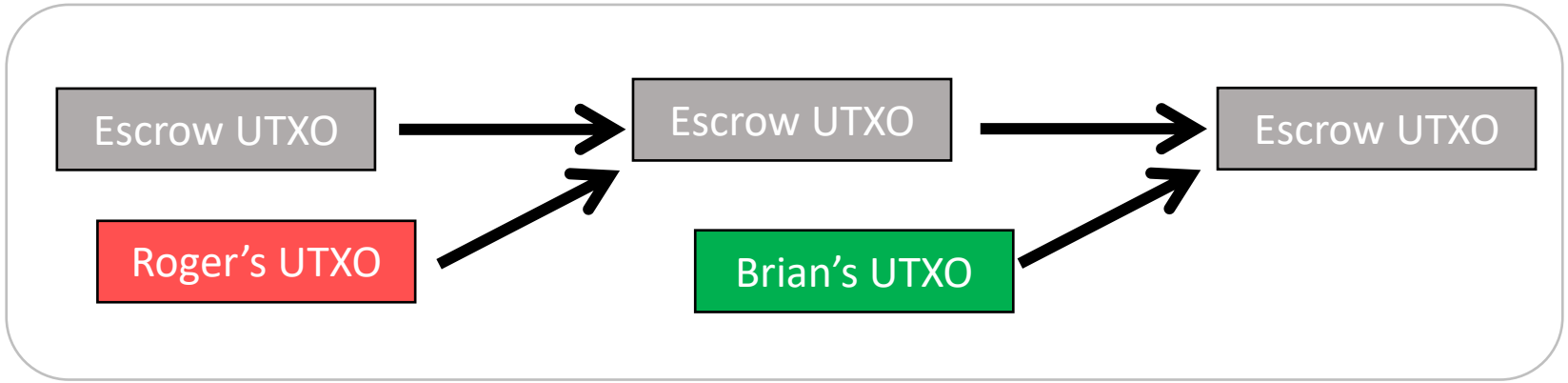
Finally, we describe Deposits and Withdrawals.



0x6AD77D1776000100000300001

M5 – Depositing Coins

Coin Quantity Increasing = Deposit



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).

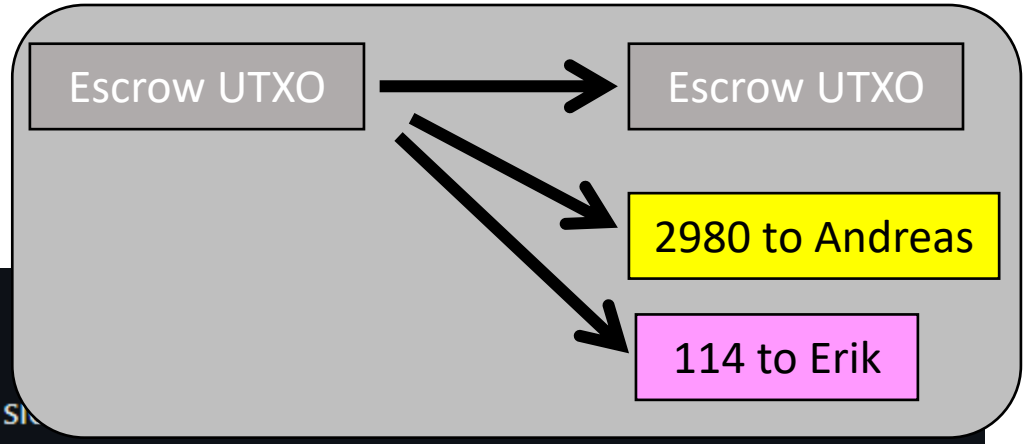
All of a sidechain's coins, are stored in one UTXO, called the "CTIP". Every time a deposit or withdrawal is made, the CTIP changes. Each deposit/withdrawal will select the sidechains CTIP, and generate a new CTIP. (Deposits/Withdrawals never cause UTXO bloat.) The current CTIP is cached in D1 (above).

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

Coin Quantity Decreasing
= Withdrawal



M6 -- Withdraw BTC from a Sidechain

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

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:

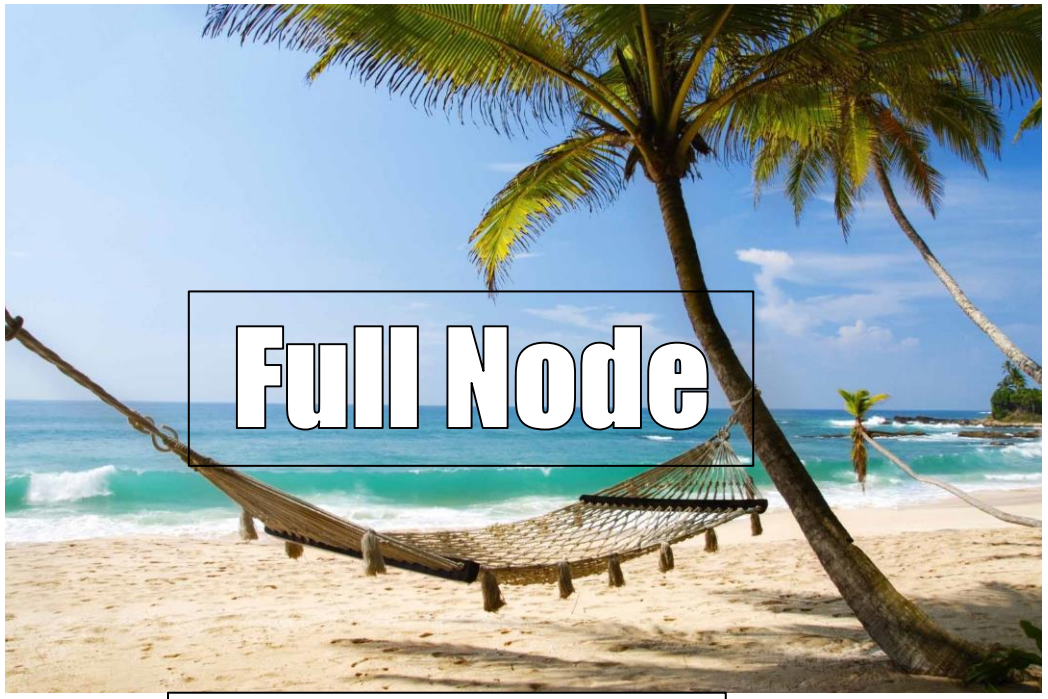
1. "Give change back to Escrow" -- The first output, TxOut0, must be paid back to the sidechain's Bip300 script. In other words, all non-withdrawn coins must be paid back into the sidechain.
2. "No traditional txn fee" -- For this txn, the sum of all inputs must equal the sum of all outputs. No traditional 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.

Only one M6 every three months, max
[per sidechiain].

b_TxID (M6) broadcasted first, the actual M6 only comes later.

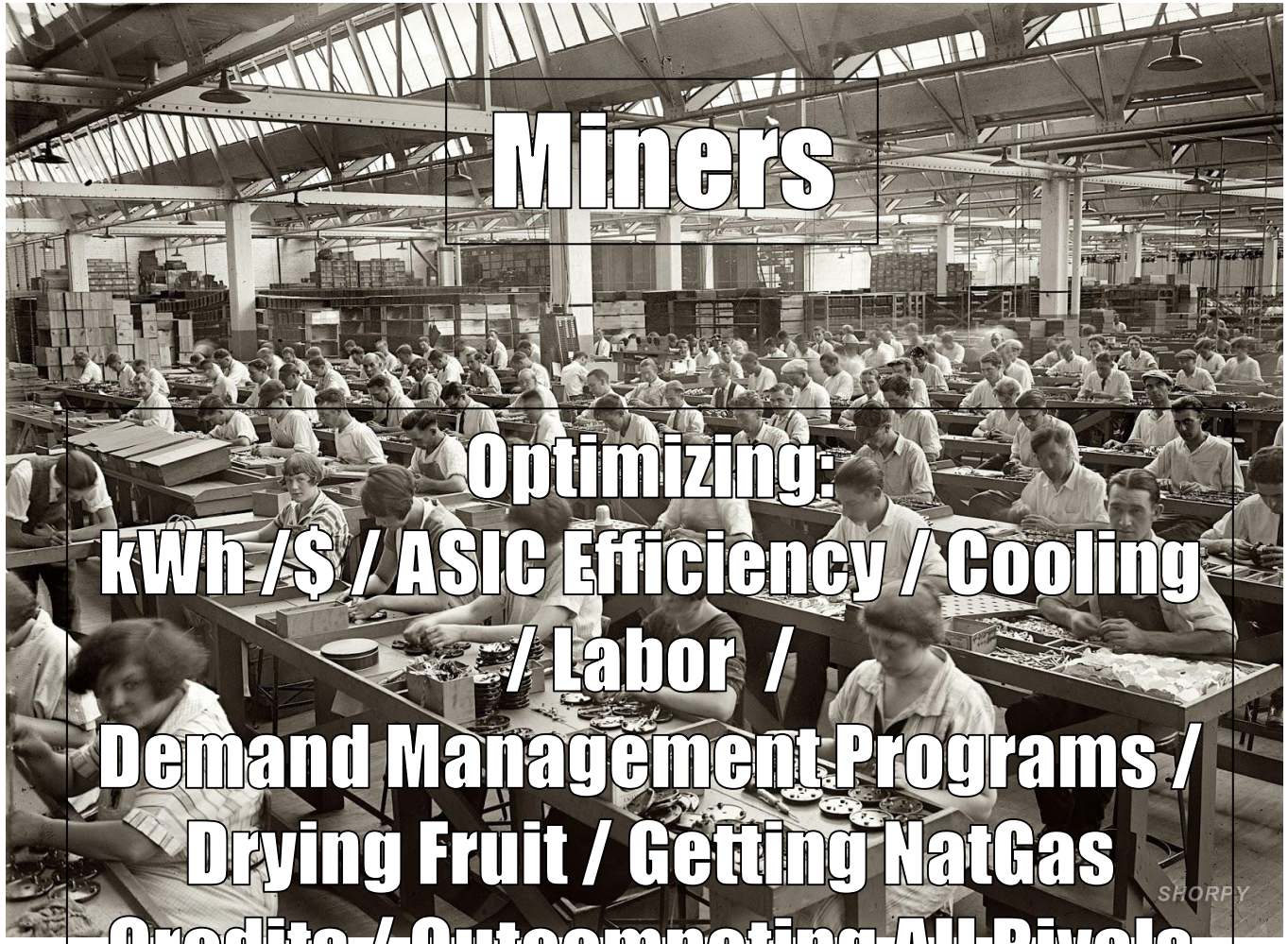
M6 is never in the Mempool.

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



Validating L1

+ counting to 13,150



+ add/remove/validate Sidechains

The “One Way Street”

Layer 2

Bit-zCash Bit-Monero

Drama

Reorgs

Centralization

Bad Design

Layer 1

Bitcoin Core

Bip300 Drivechains

L2 node must have access to an L1 node

The “One Way Street”

Bit-zCash Bit-Monero

Bip300
Drivechains

Layer 2

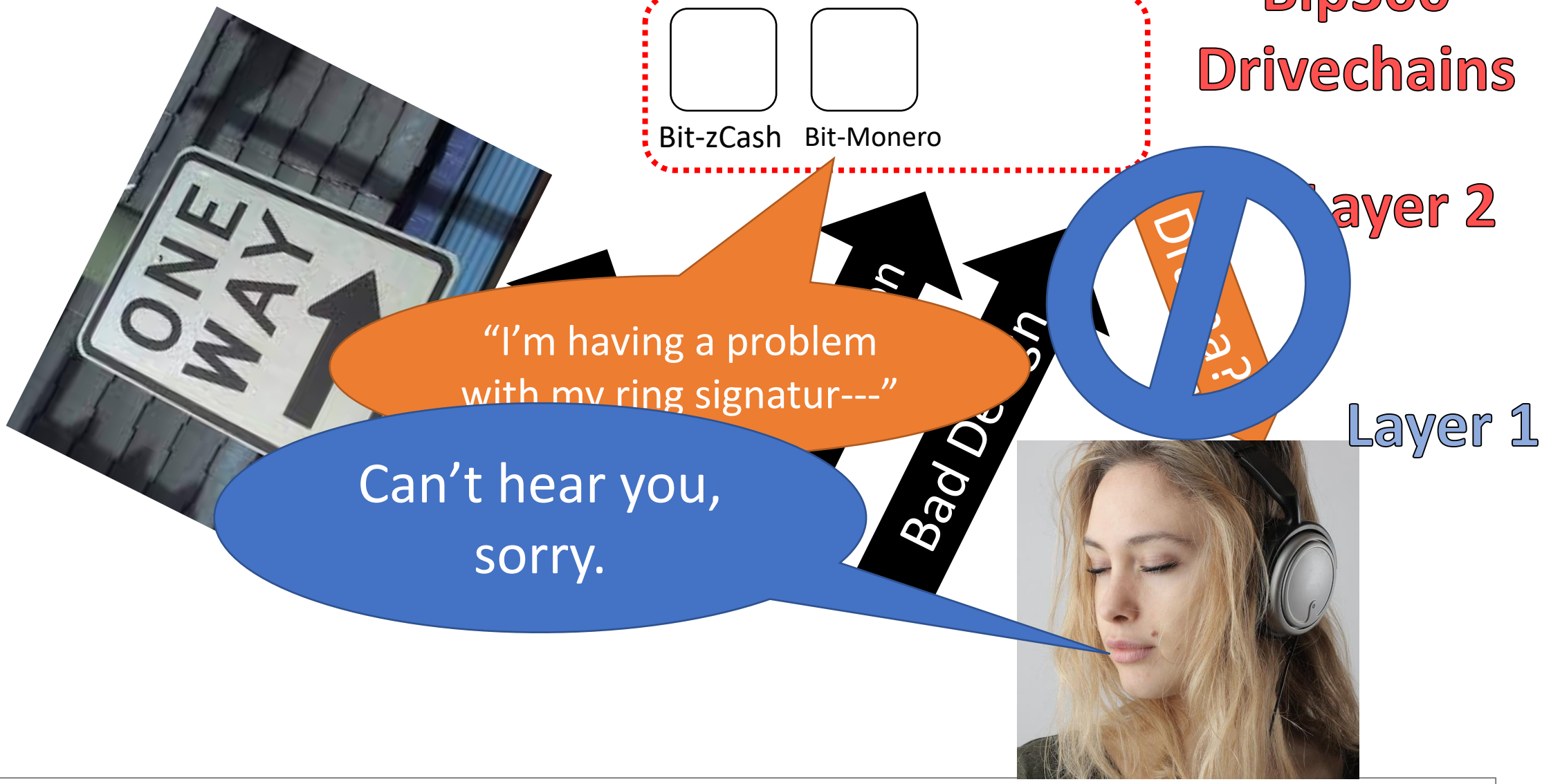
Drama?

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

Layer 1

Bitcoin Core

The “One Way Street”



The “One Way Street”

Bit-zCash Bit-Monero

Bip300
Drivechains
Layer 2

ama

rgs

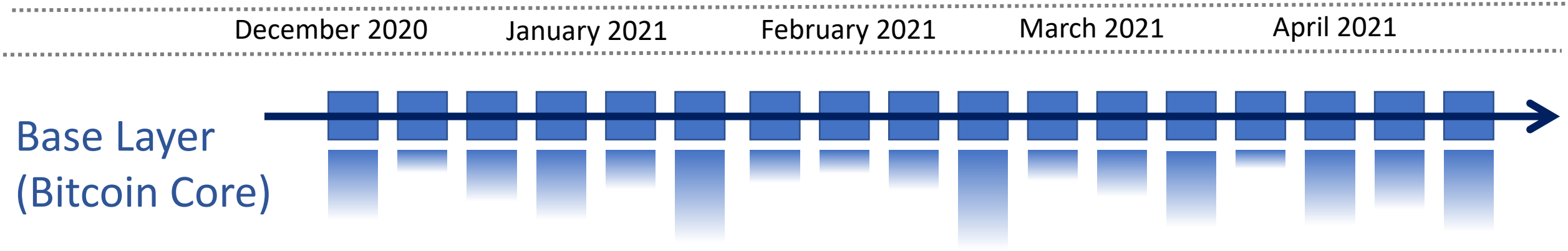
tralization

Bad Design

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

ayer 1

Putting Hash(L2) into L1



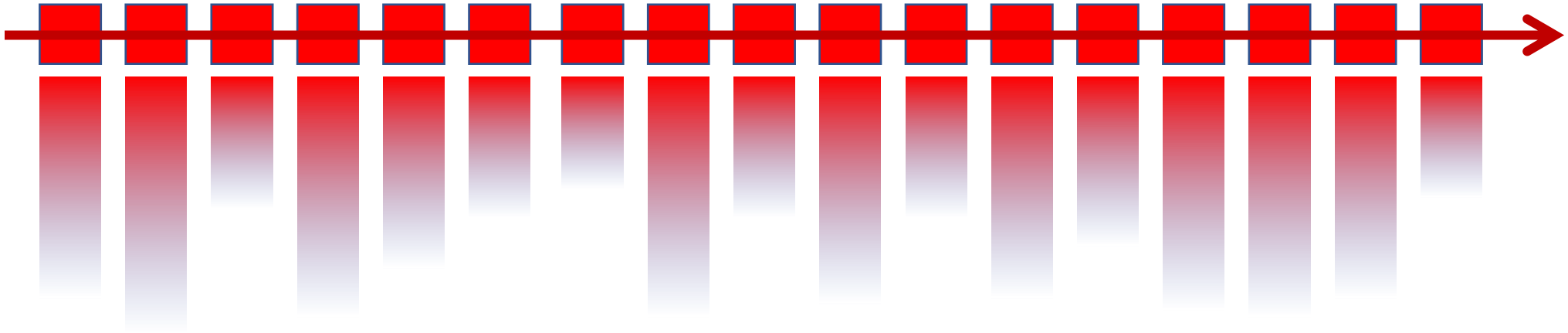
Putting Hash(L2) into L1

= Block Header

= List of transactions

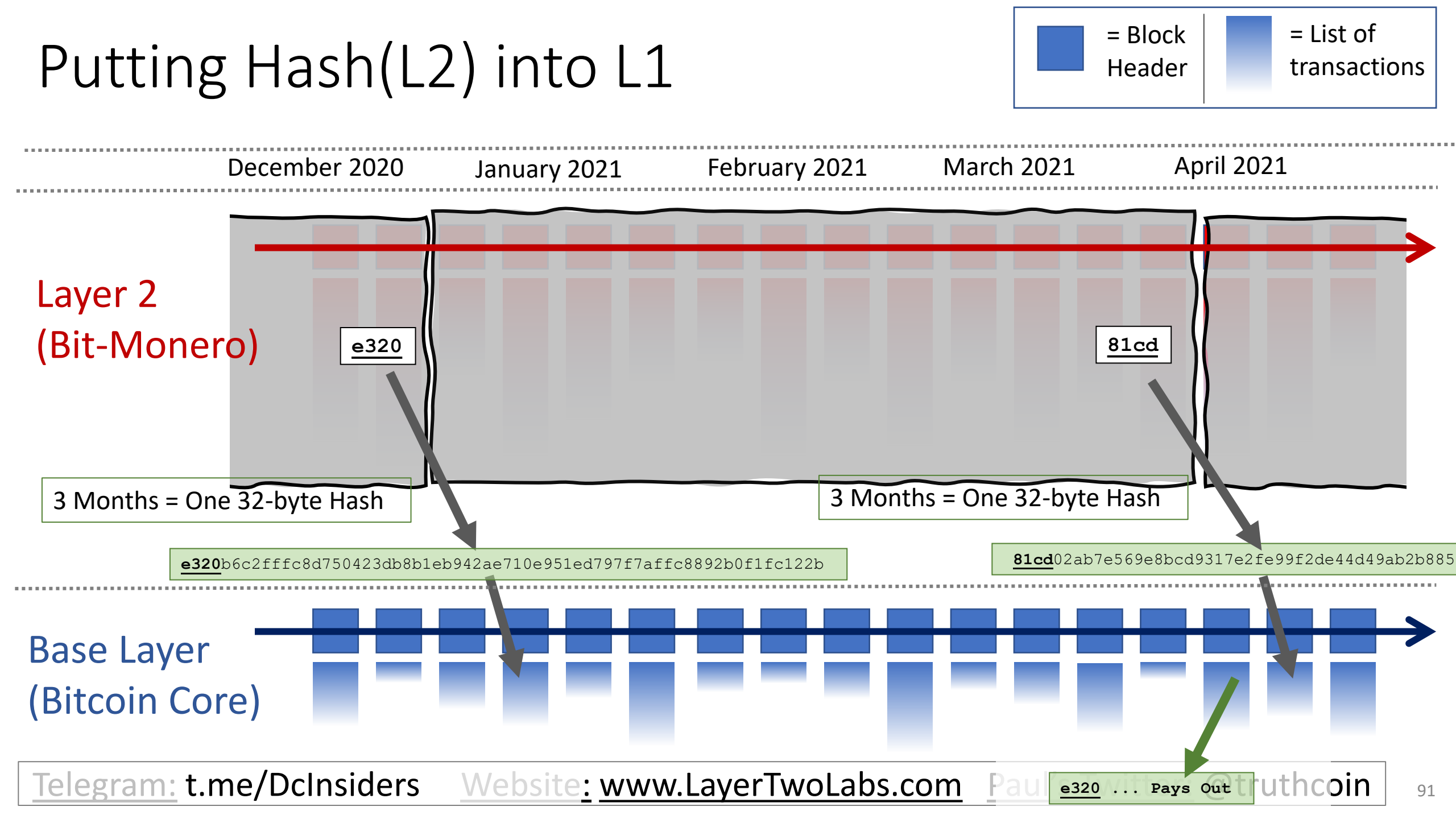
December 2020 January 2021 February 2021 March 2021 April 2021

Layer 2
(Bit-Monero)

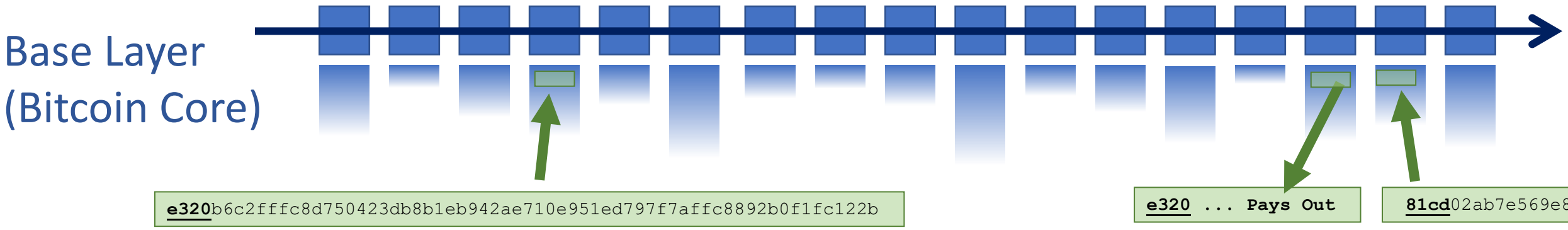


Base Layer
(Bitcoin Core)

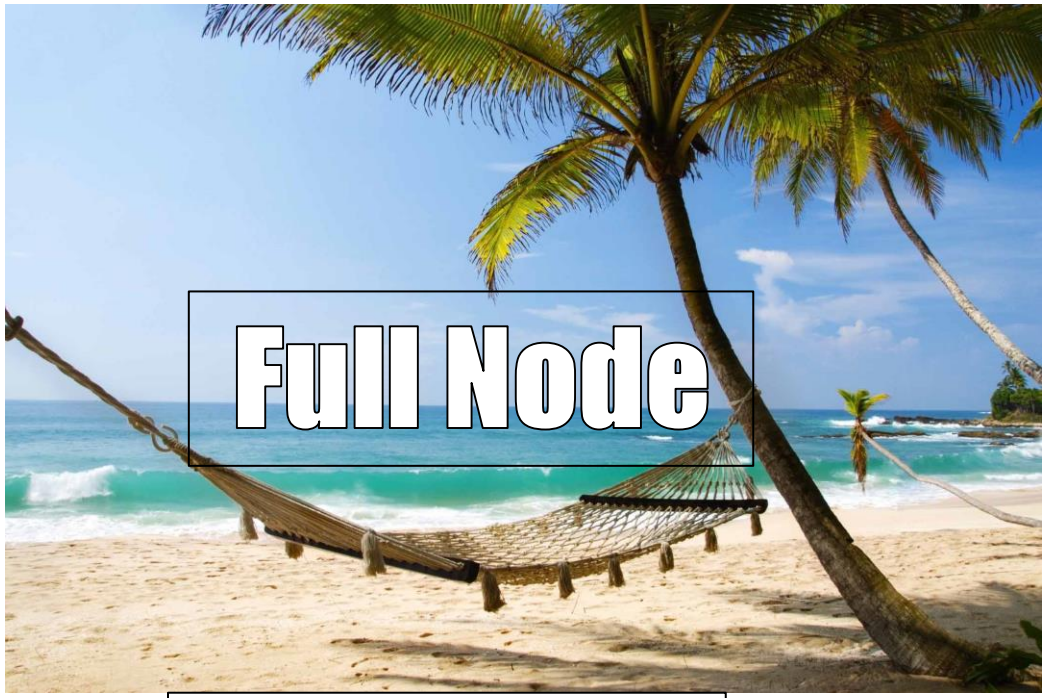
Putting Hash(L2) into L1



Your Layer 1 Node Sees…

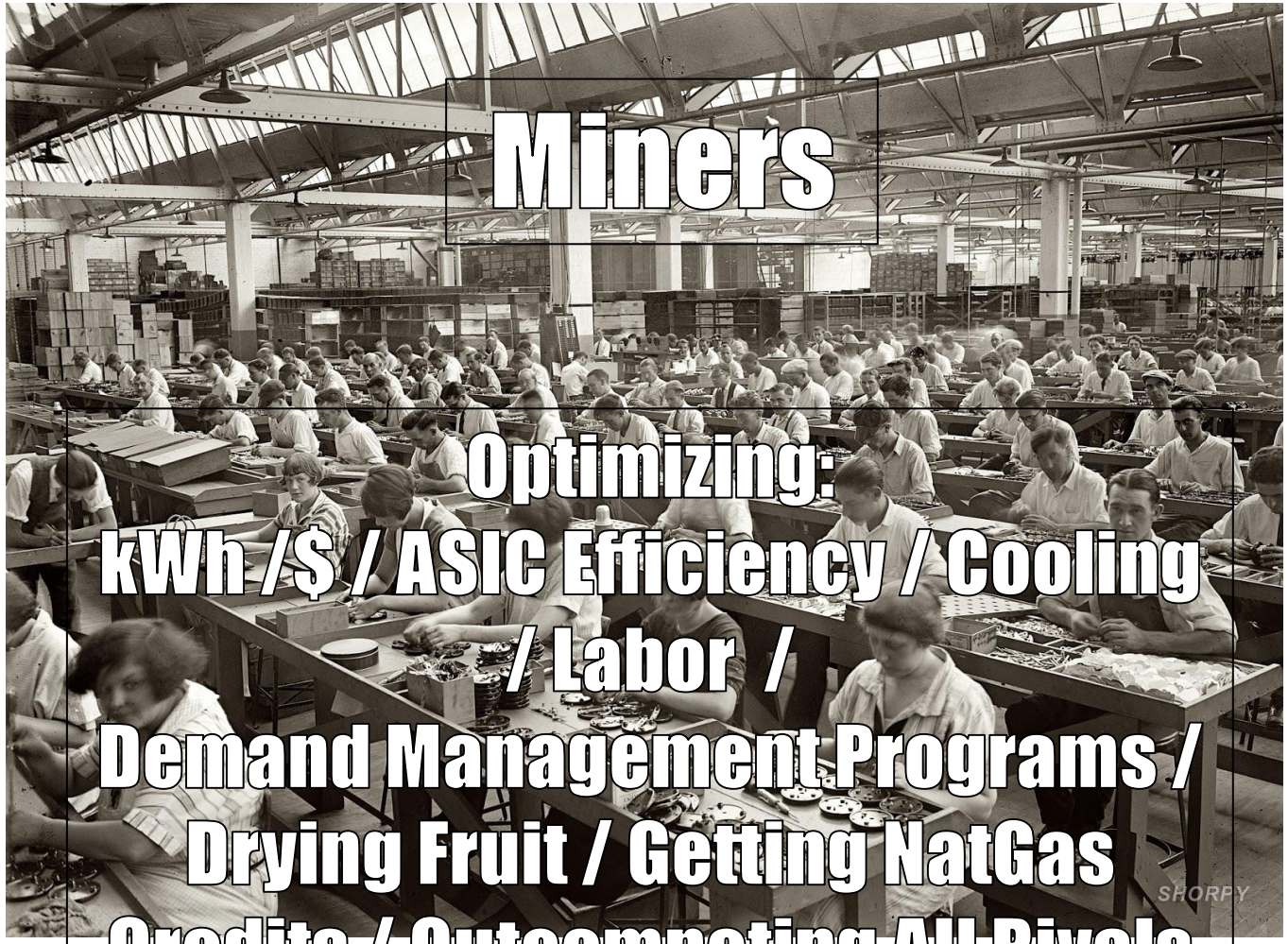


But then how is it secure??



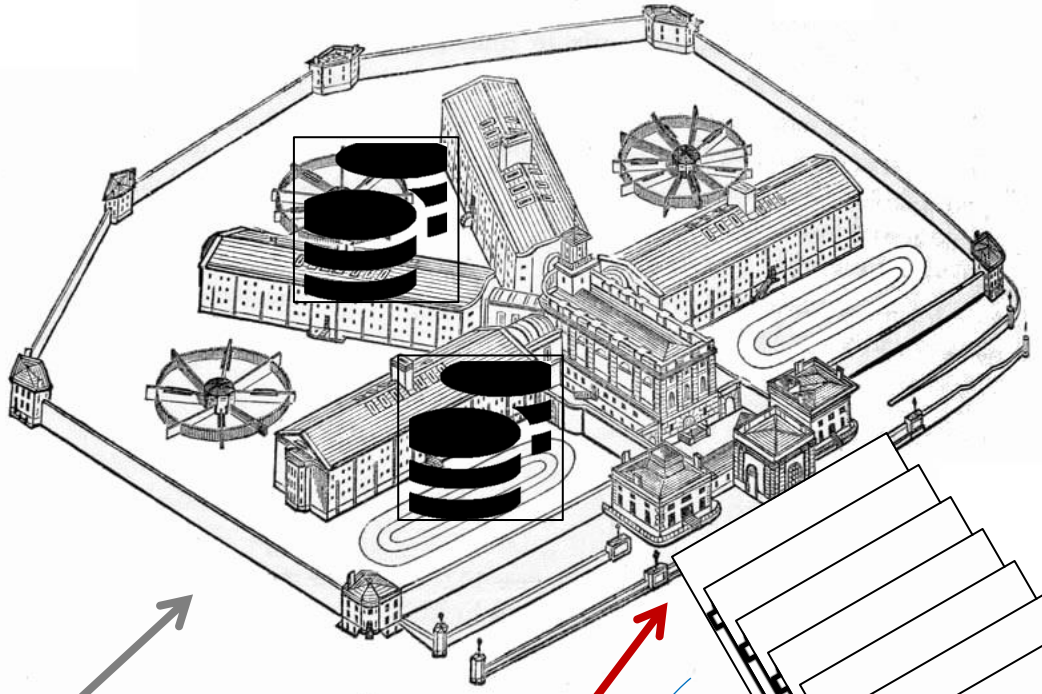
Validating L1

+ counting to 13,150



+ add/remove/validate Sidechains

Prison Metaphor



Prison

Only way out.

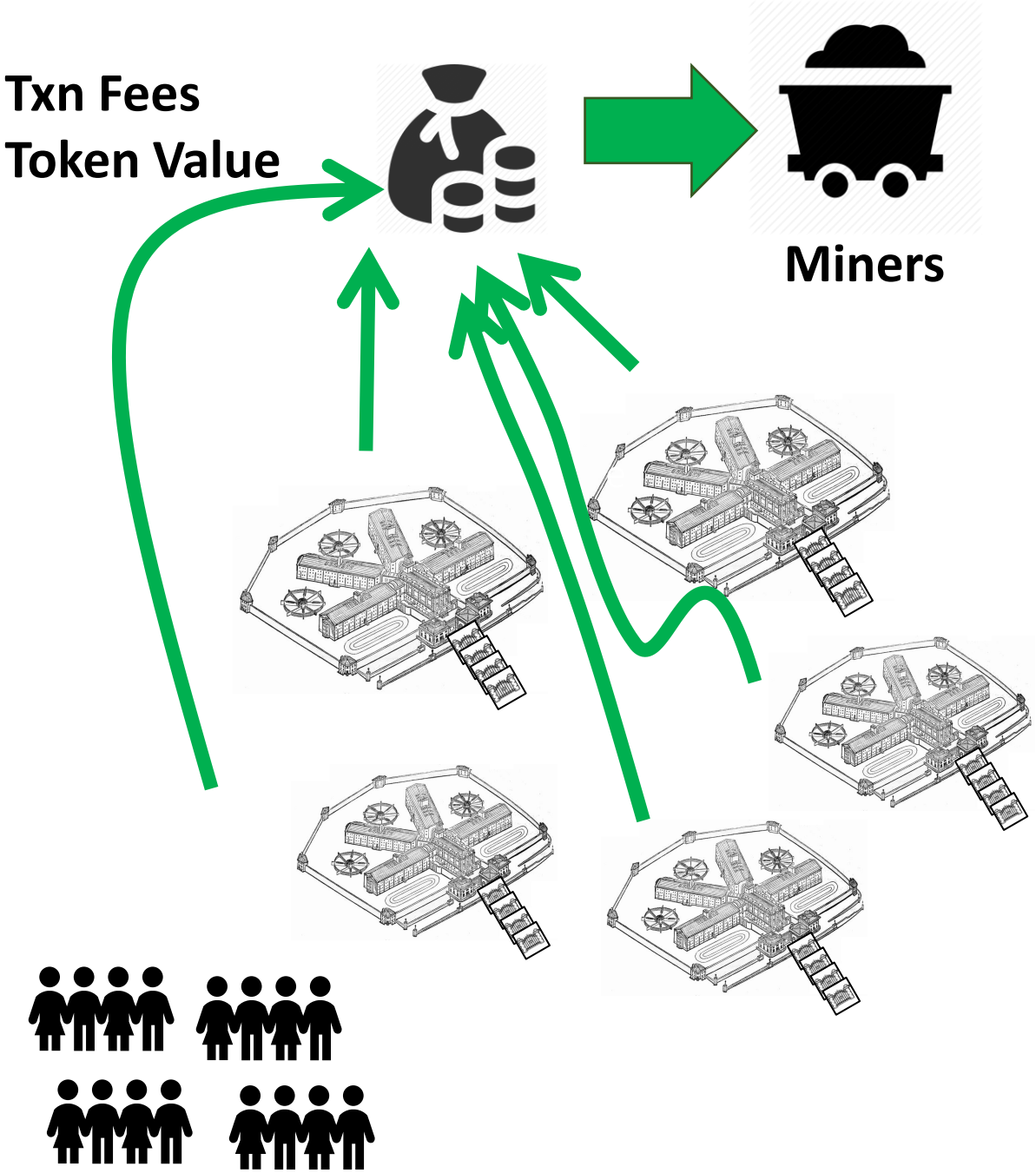
13,150 Gates

...

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:

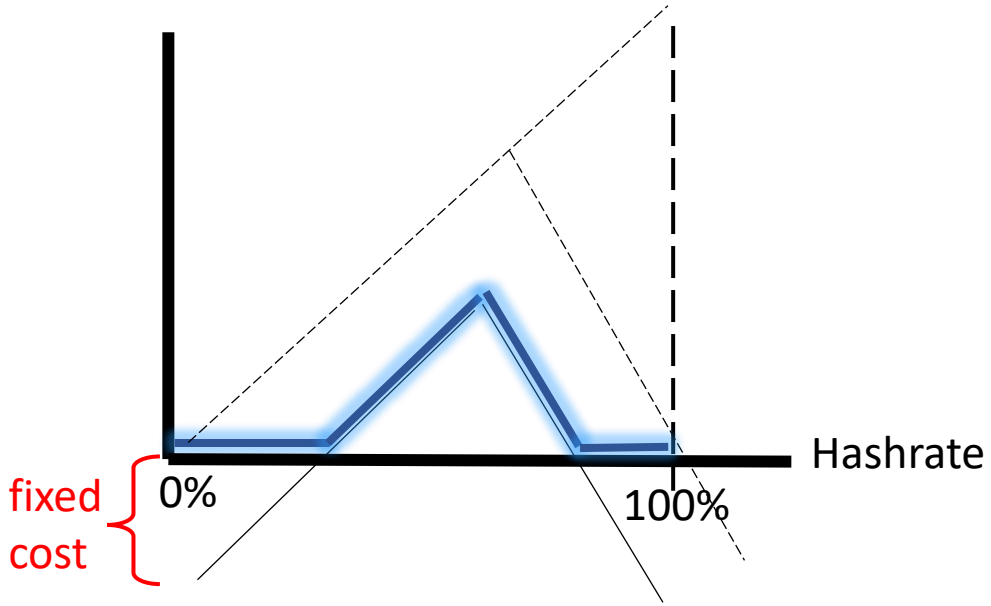
- Steal from LN channels – by censoring the justice txn
- Reorg mainchain Bitcoin txns out, and hold them hostage
- Block any message from L1 – including zk-proofs

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

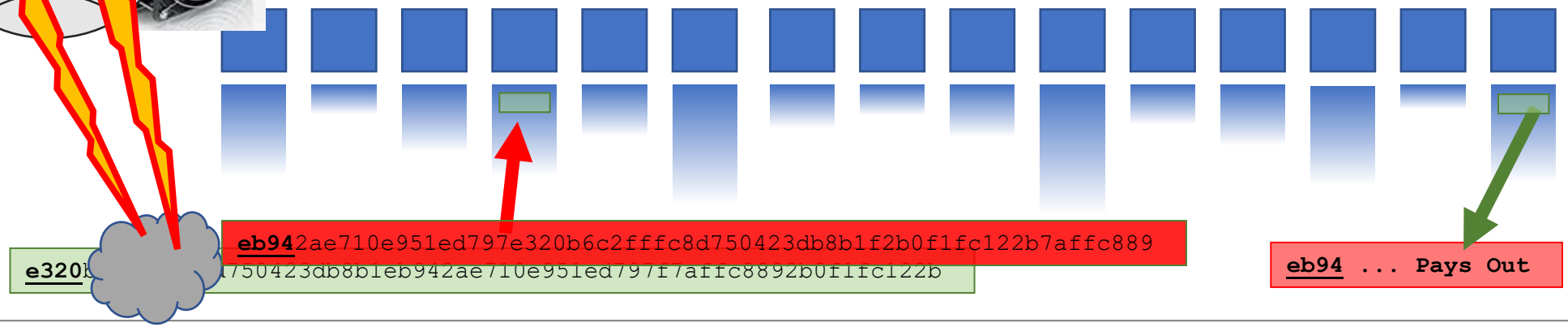
6 - Two Critiques

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)



(#1) **Miners-Can-Steal** from Bip300 Scripts (and this is bad)	(#2) **Merged-Mining is a Side-Hustle** (and those are always 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.	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.)
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.	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.**
Miners "can" **steal from Lightning Network** (by broadcasting old state + censoring Justice Txns), but this criterion is never held against LN.	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.
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.	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.
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.	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.
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.	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)	(#2) **Merged-Mining is a Side-Hustle** (and those are always 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.	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.)
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.	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.**
Miners "can" **steal from Lightning Network** (by broadcasting old state + censoring Justice Txns), but this criterion is never held against LN.	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.
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.	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.
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.	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.
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.	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)	(#2) **Merged-Mining is a Side-Hustle** (and those are always 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.	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.)
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.	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.**
Miners "can" **steal from Lightning Network** (by broadcasting old state + censoring Justice Txns), but this criterion is never held against LN.	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.
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.	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.
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.	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.
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.	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)	(#2) **Merged-Mining is a Side-Hustle** (and those are always 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.	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.)
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.	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.**
Miners "can" **steal from Lightning Network** (by broadcasting old state + censoring Justice Txns), but this criterion is never held against LN.	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.
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.	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.
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.	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.
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.	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.

Thank You

for Your Attention!

Questions?

7 – Alts/Fees

What **does** affect mainchain miners: Altcoins

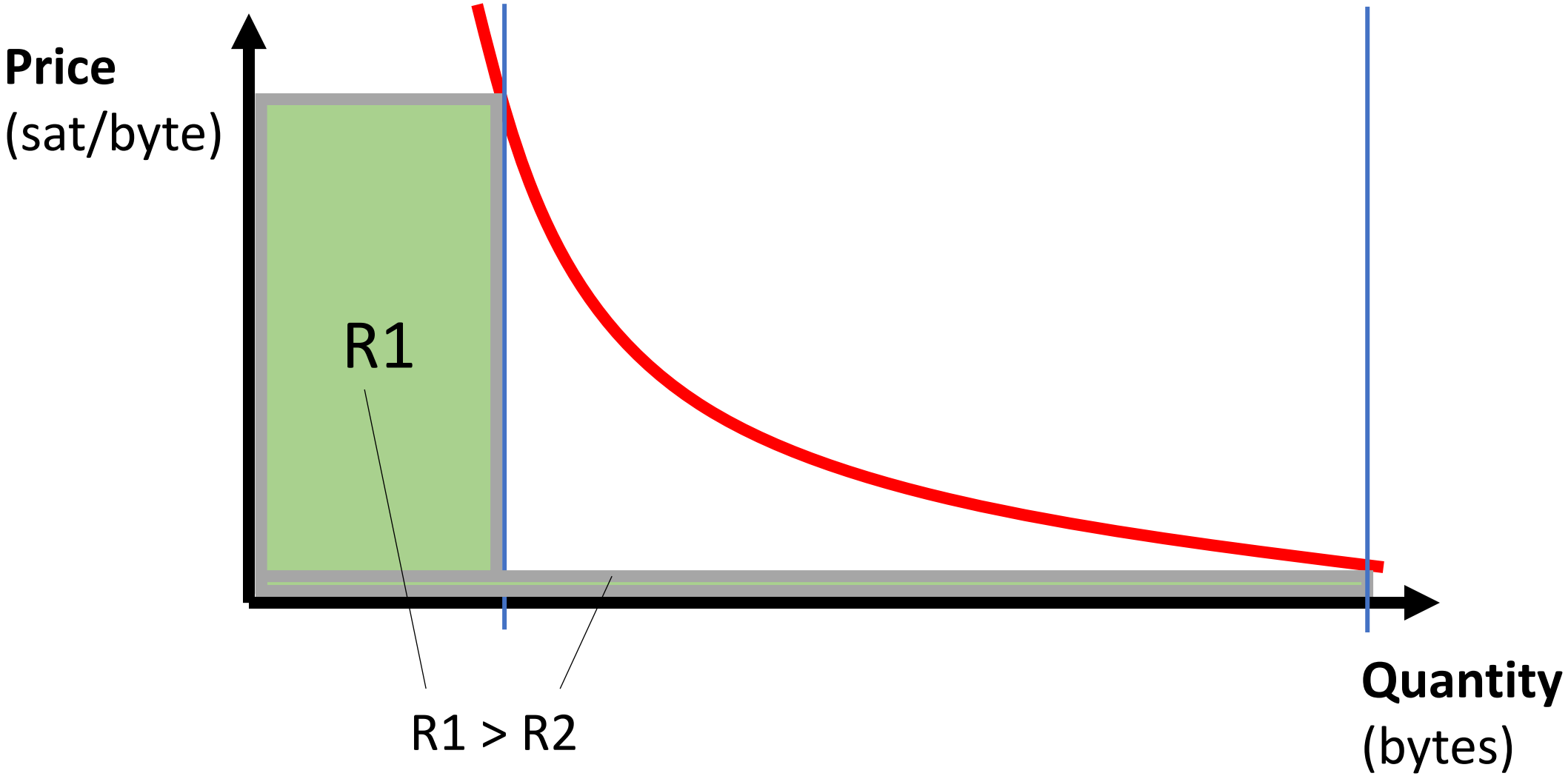
[bitcoin-dev] Total fees have almost c

Gregory Maxwell greg at 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]

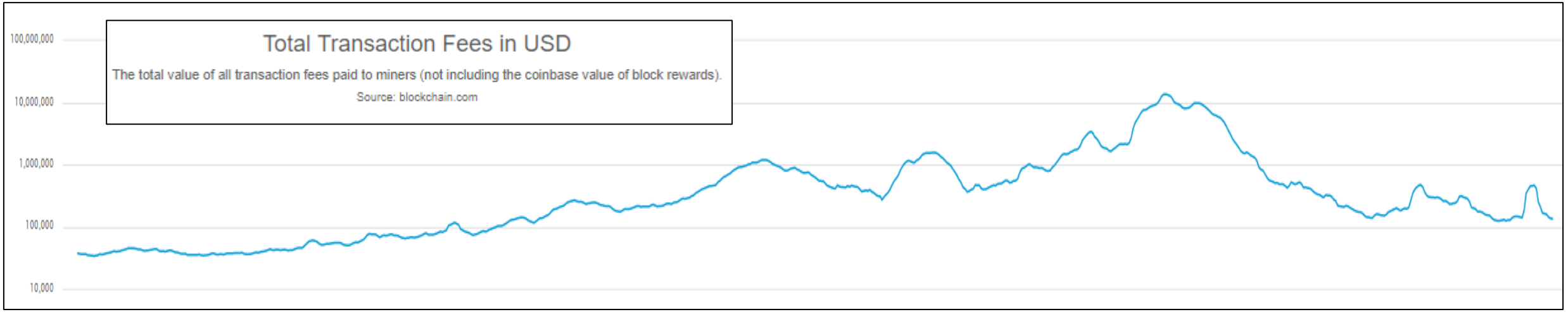
Personally, I'm pulling out the champaign that market behaviour is indeed producing activity levels that can pay for security without inflation, and also producing fee paying backlogs needed to stabilize consensus progress as the subsidy declines.

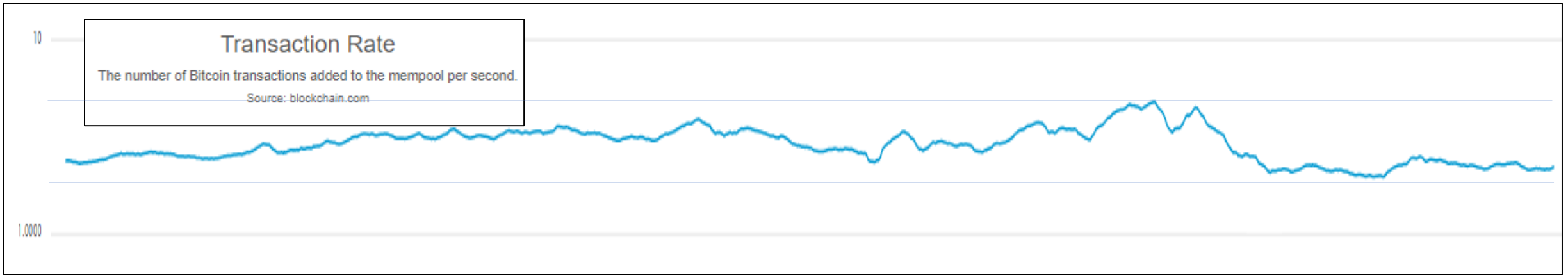
What **does** affect mainchain miners: Altcoins



High Fees → Less Usage

Last 2 Years, Log Scales, 7d average





Fee revenues are important…

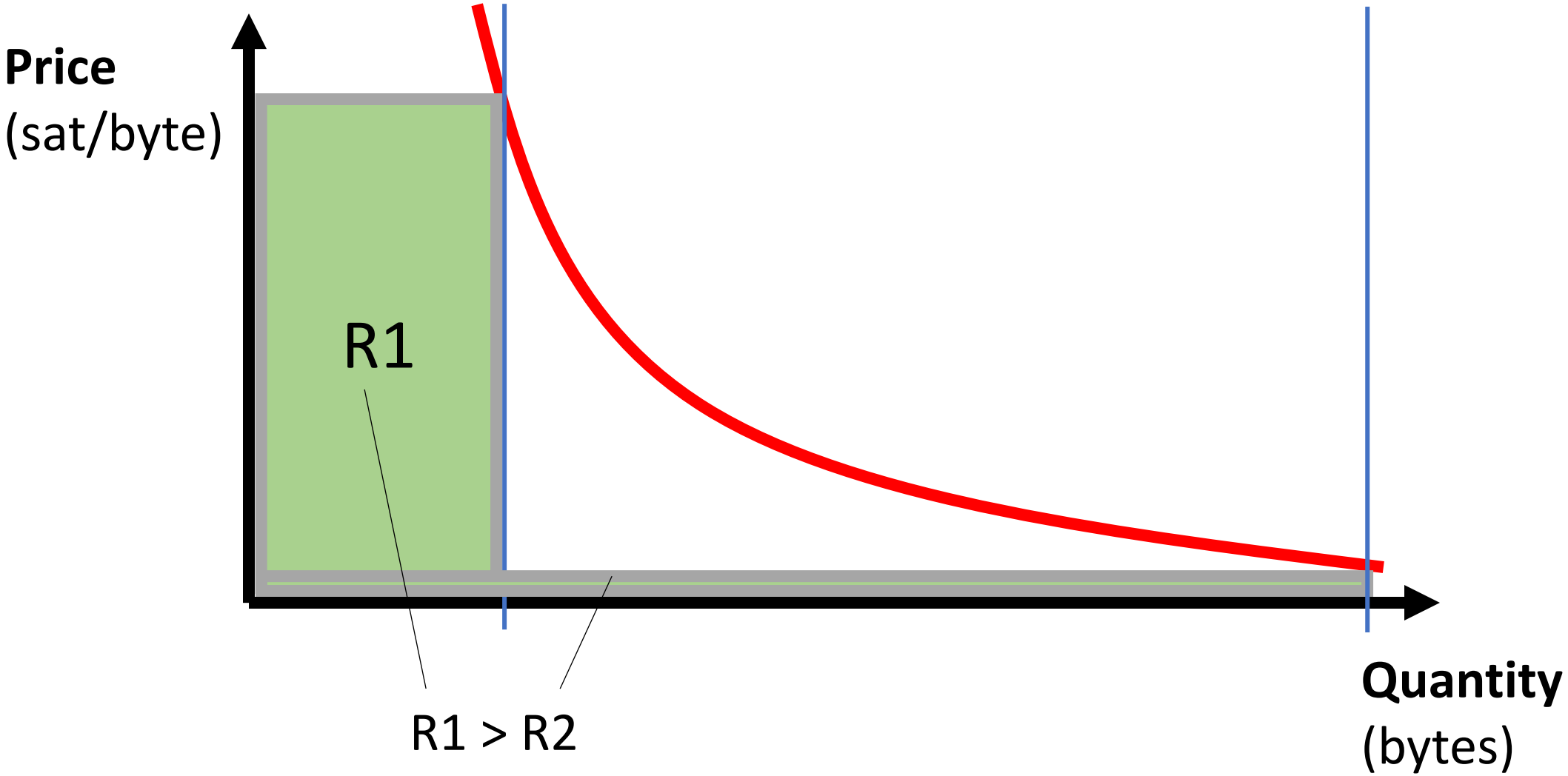
[bitcoin-dev] Total fees have almost c

Gregory Maxwell greg at xiph.org
Thu Dec 21 22:44:32 UTC 2017

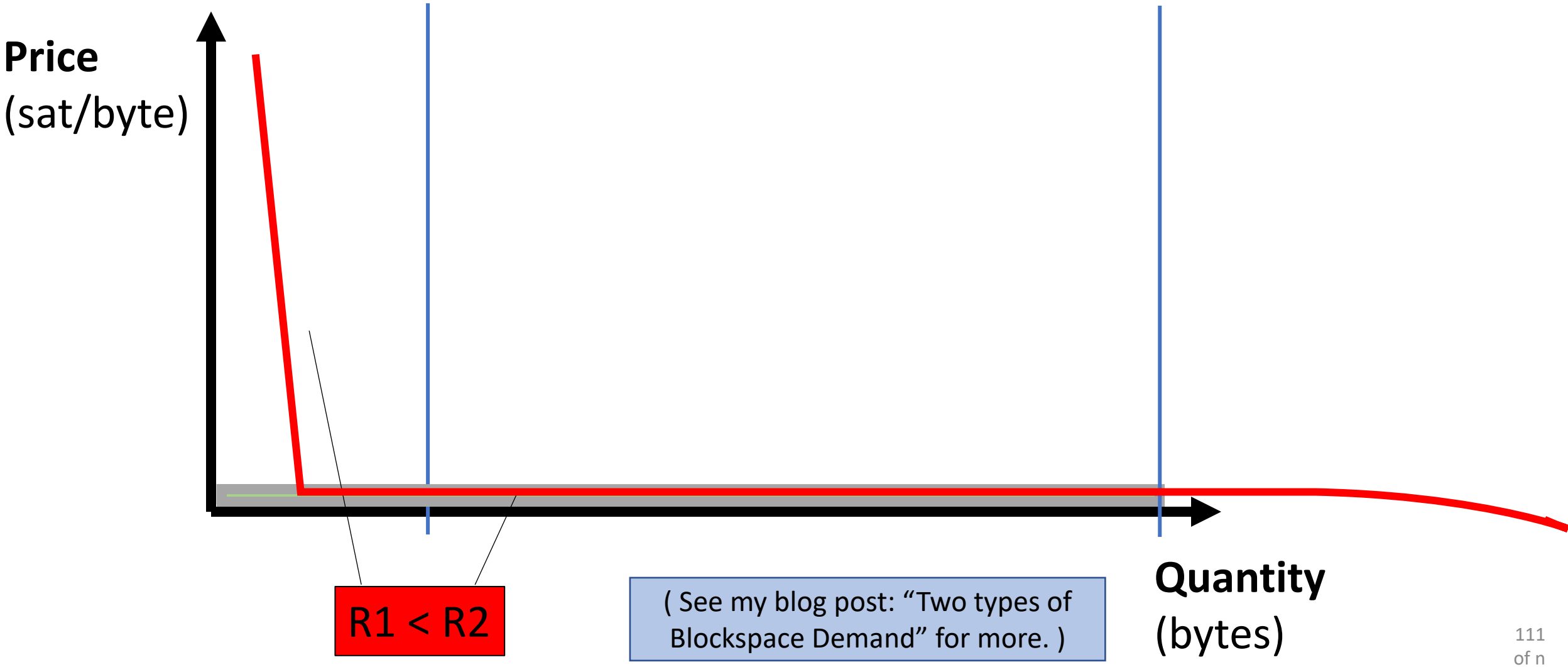
- Previous message: [bitcoin-dev] Total fees have almost crossed the block
- Next message: [bitcoin-dev] Total fees have almost crossed the block rev
- **Messages sorted by:** [date] [thread] [subject] [author]

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

Crypto Fees

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

Layer 1 × | Share | Filters 1 | Yesterday

Name	▼ 1 Day Fees	7 Day Avg. Fees
Ethereum	$8,740,188.92	$7,864,461.27
Binance Smart Chain	$2,033,849.09	$1,643,743.19
Bitcoin	$1,970,350.71	$1,809,454.32
Dogecoin	$32,366.20	$24,394.61
Terra	$18,666.89	$19,434.10
Cardano	$14,645.96	$13,656.48
xDai		$7,636.72

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/

e 4, 2021

www. coin

(#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

Crypto Fees

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

Layer 1 × | Share | Filters 1 | Yesterday

Name	▼ 1 Day Fees	7 Day Avg. Fees
Ethereum	$8,740,188.92	$7,864,461.27
Binance Smart Chain	$2,033,849.09	$1,643,743.19
Bitcoin	$1,970,350.71	$1,809,454.32
Dogecoin	$32,366.20	$24,394.61
Terra	$18,666.89	$19,434.10
Cardano	$14,645.96	$13,656.48
xDai		$7,636.72

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/

(#3) Improve Mining Incentives (Bip 301)

- Get all of the fees, on all of the chains!
- Miners ca

Item

Runs a sidechai

How much hash

Coins collected,

Coins paid out,

Coins rec'd, on

d(Net Worth)

Crypto Fees

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

Layer 1 × | Share | Bundle | Filters 1 | Yesterday

Name	▼ 1 Day Fees	7 Day Avg. Fees
Ethereum	$75,669 +846%	$74,428,911.16
Binance Smart Chain	$5,848 +216%	$5,198,367.48
Bitcoin	$1,035 -52%	$863,839.49
Avalanche	$105,316.62	$86,451.49
Fantom	$92,087.08	$92,517.89
Polygon	$65,296.89	$74,457.60
Terra	$64,095.94	$14,118.19

November 4, 2021

Crypto Fees

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

Layer 1 × | Share | Filters 1 | Yesterday

Name	▼ 1 Day Fees	7 Day Avg. Fees
Ethereum	$8,740,188.92	$7,864,461.27
Binance Smart Chain	$2,033,849.09	$1,643,743.19
Bitcoin	$1,970,350.71	$1,809,454.32
Dogecoin	$32,366.20	$24,394.61
Terra	$18,666.89	$19,434.10
Cardano	$14,645.96	$13,656.48
xDai	$13,951.33	$27,636.72

Taken from https://cryptofees.info/

June 4, 2021

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
Smallest Payment	90% of L1 $/txn fee	0% of L1 $/txn fee

LN's micropayments require L1 fee-rates to be low, DC's do not.