Bip300: Getting to 100% Bitcoin Dominance and Collecting Every Transaction Fee on Earth

Paul Sztorc
Anduro Maker Space
7.25.2024

My 1000+ Pages About Bitcoin

2012-2014 | Statistician, Yale Econ
→ Bitcoin Researcher

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

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

My Big Break

Dec 2014 – Adam Back links to my blog

ada
Sr. Member

Activity: 404
Merit: 318

in bitcoin we trust

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

What You Should Do (I think)

- Try the testnet software yourself – to figure out what is going on.
  - LayerTwoLabs.com/download
- Consume some drivechain.info content
  - Including a huge YouTube playlist with 35+ hours of content
  - Read the FAQ
  - Read the misinformation section
  - Read about CUSF, as well -- Bip300cusf.com
- If you agree –
  - get 51% of hashrate to run the Activator client.
  - Plan out which sidechain to adopt first (zCash clone)

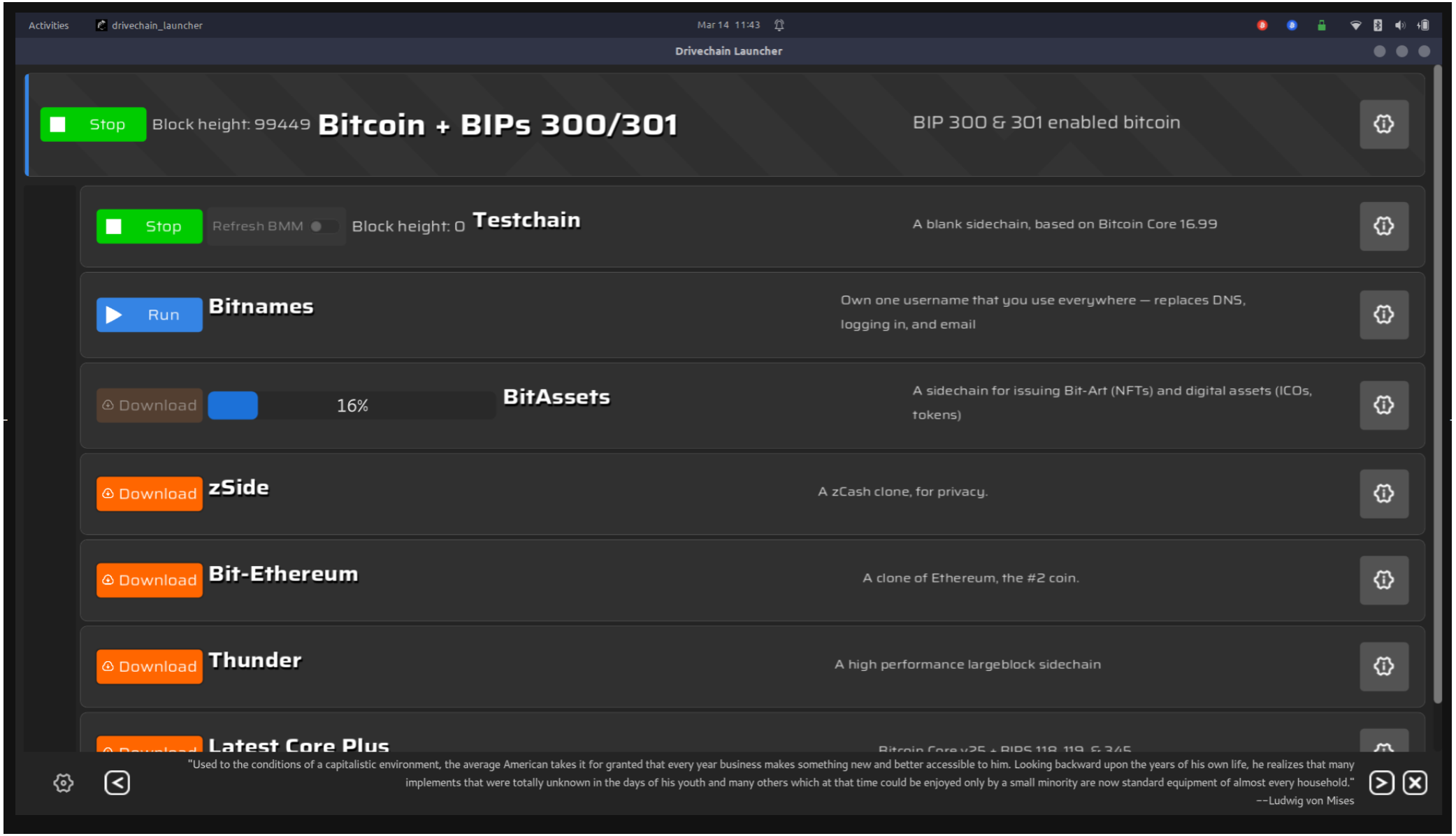
https://layertwolabs.com/download

Download Drivechain Launcher

Download for Linux

Download for Windows

Download for Mac


Activities
drivechain_launcher
Mar 14 11:43
Drivechain Launcher
Stop
Block height: 99449
Bitcoin + BIPs 300/301
BIP 300 & 301 enabled bitcoin
Stop
Refresh BMM
Block height: 0
Testchain
A blank sidechain, based on Bitcoin Core 16.99
Run
Bitnames
Own one username that you use everywhere — replaces DNS, logging in, and email
Download
16%
BitAssets
A sidechain for issuing Bit-Art (NFTs) and digital assets (ICOs, tokens)
Download
zSide
A zCash clone, for privacy.
Download
Bit-Ethereum
A clone of Ethereum, the #2 coin.
Download
Thunder
A high performance largeblock sidechain
Download
Latest Core Plus
"Used to the conditions of a capitalistic environment, the average American takes it for granted that every year business makes something new and better accessible to him. Looking backward upon the years of his own life, he realizes that many implements that were totally unknown in the days of his youth and many others which at that time could be enjoyed only by a small minority are now standard equipment of almost every household."
--Ludwig von Mises

Drivechain (BIPs 300+301)

WHEN DEVS COMPETE, USERS WIN

"DRIVECHAIN ... ARGUABLY COULD HAVE BEEN MORE IMPORTANT OR USEFUL THAN TAPROOT."

- **Adam Back**, Baltic Honeybadger 2022

LEARN via YouTube – DOWNLOAD our Software

PEER-TO-PEER BITCOIN SIDECHAINS

Drivechain allows Bitcoin to *create*, *delete*, *send BTC to*, and *receive BTC from* "Layer-2"s called "sidechains". Sidechains are Altcoins that lack a native "coin" – instead, pre-existing coins [from a different blockchain] must first be sent over.

"Sidechains" boils down to allowing consenting individuals to:

1. choose their own security models
2. spend their bitcoin how they like
3. permissionlessly create voluntarist technology

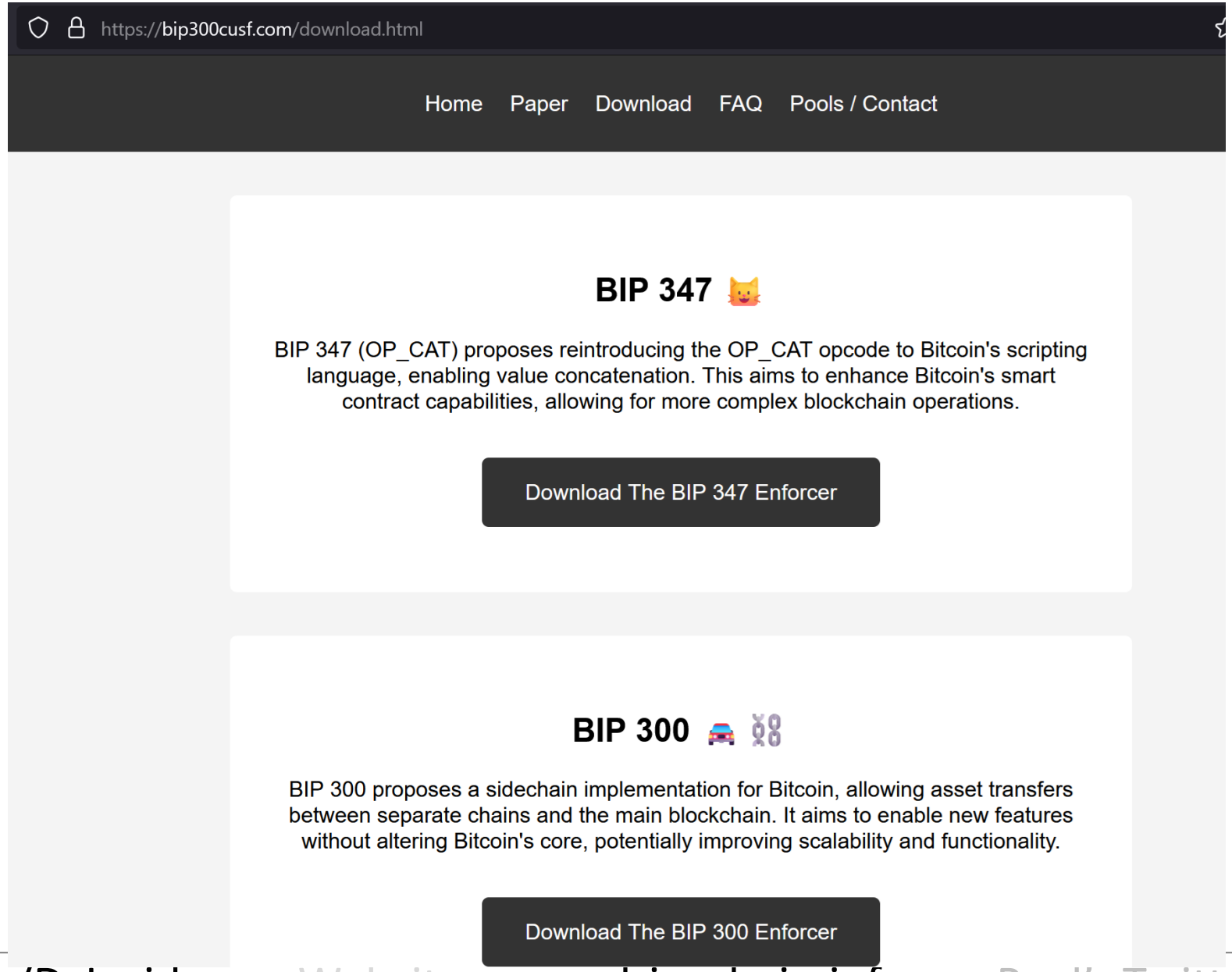
Once on a sidechain, coins can change hands an unlimited number of times, and in an unlimited number of *new ways*. Thus, BTC-owners can opt-in to new features or tradeoffs. Meanwhile, the Bitcoiners who don't opt-in, never need to care what any

LINKS

- Home
- Github
- Releases
- Block Explorer
- Articles
- Literature
- FAQ
- Friends of Drivechain
- Misinformation
- Telegram
- Twitter
- Reddit
- Sidechain Projects

Truthcoin.Info

Bitcoin Hivemind

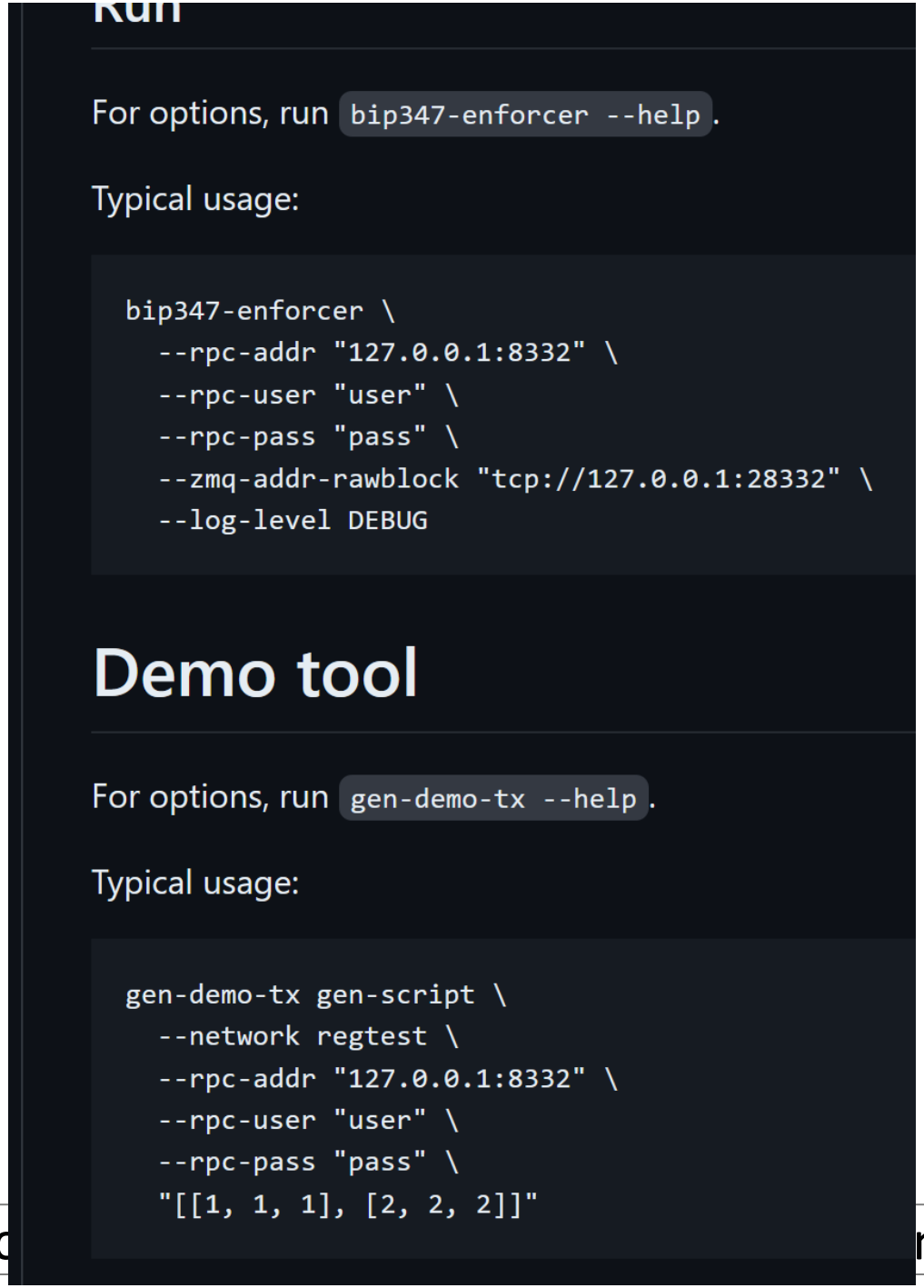

https://bip300cusf.com/download.html
Home
Paper
Download
FAQ
Pools / Contact
BIP 347
BIP 347 (OP_CAT) proposes reintroducing the OP_CAT opcode to Bitcoin's scripting language, enabling value concatenation. This aims to enhance Bitcoin's smart contract capabilities, allowing for more complex blockchain operations.
Download The BIP 347 Enforcer
BIP 300
BIP 300 proposes a sidechain implementation for Bitcoin, allowing asset transfers between separate chains and the main blockchain. It aims to enable new features without altering Bitcoin's core, potentially improving scalability and functionality.
Download The BIP 300 Enforcer

This is how easy it is to activate soft forks

(no modification to Bitcoin Core)

51% hashrate needed

also: reversible



Run

For options, run `bip347-enforcer --help`.

Typical usage:

```
bip347-enforcer \
  --rpc-addr "127.0.0.1:8332" \
  --rpc-user "user" \
  --rpc-pass "pass" \
  --zmq-addr-rawblock "tcp://127.0.0.1:28332" \
  --log-level DEBUG
```

Demo tool

For options, run `gen-demo-tx --help`.

Typical usage:

```
gen-demo-tx gen-script \
  --network regtest \
  --rpc-addr "127.0.0.1:8332" \
  --rpc-user "user" \
  --rpc-pass "pass" \
  "[[1, 1, 1], [2, 2, 2]]"
```

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

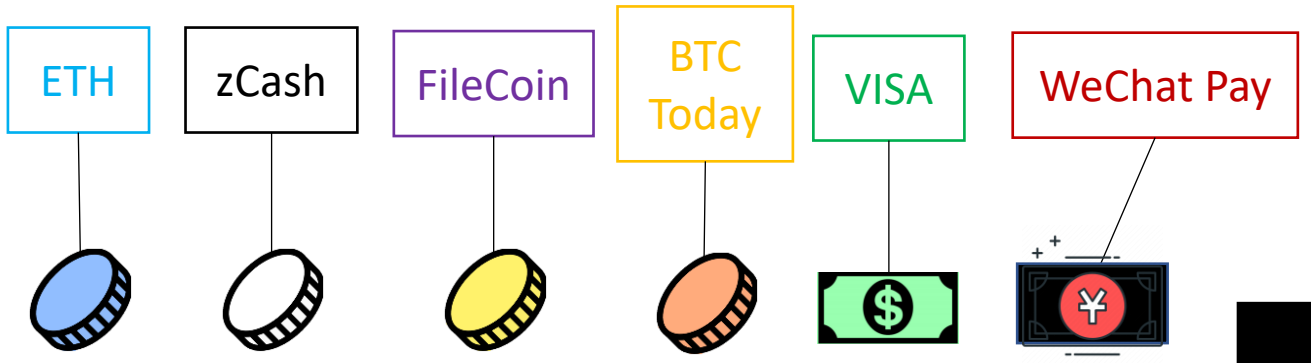
Visit www.LayerTwoLabs.com/friends for 49 more!

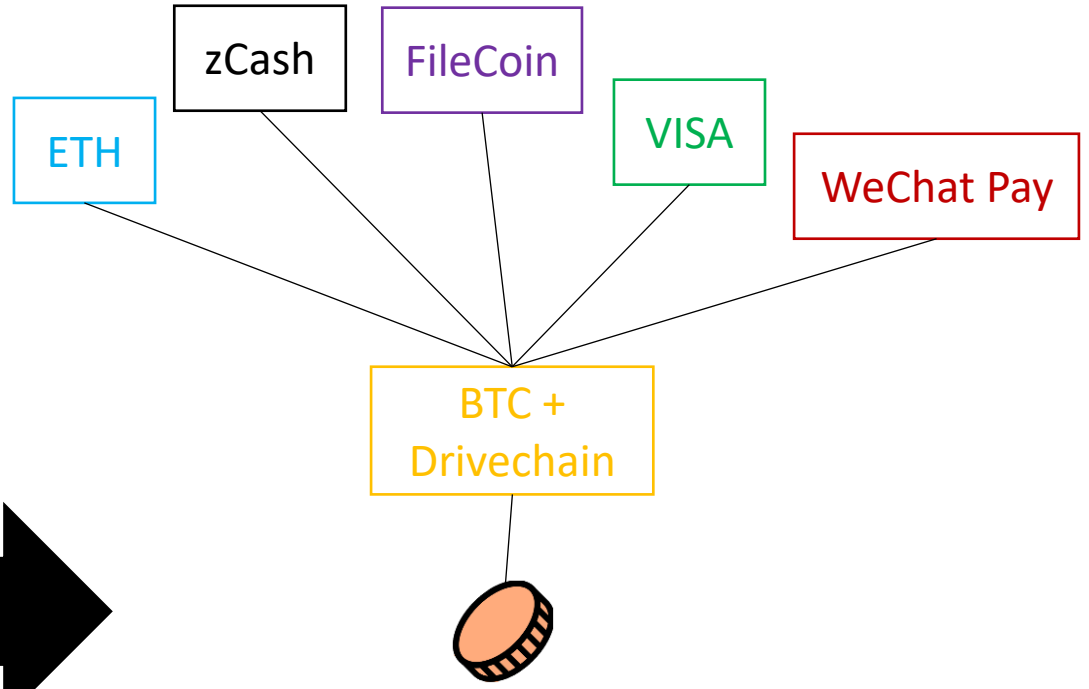
My Three Favorite Endorsements

- "Drivechains…are pretty cool…and arguably could have been more

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

BIP300: Everything on Top of Bitcoin

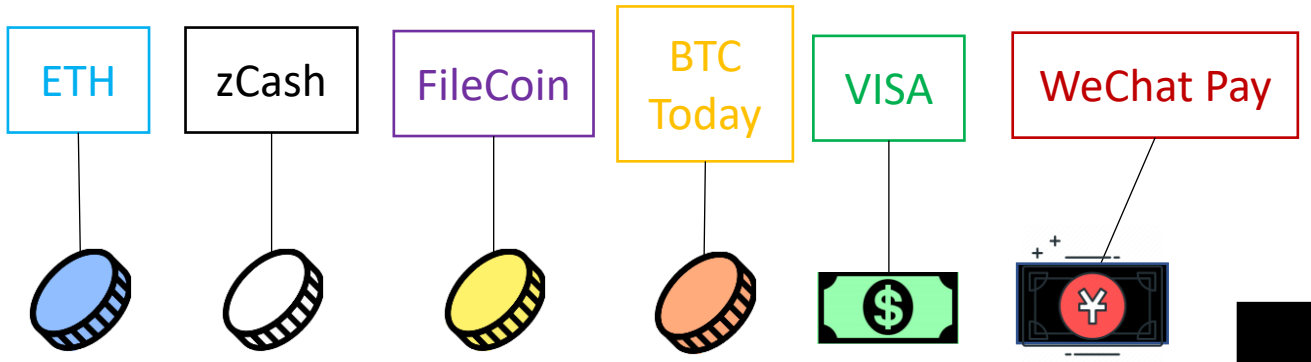




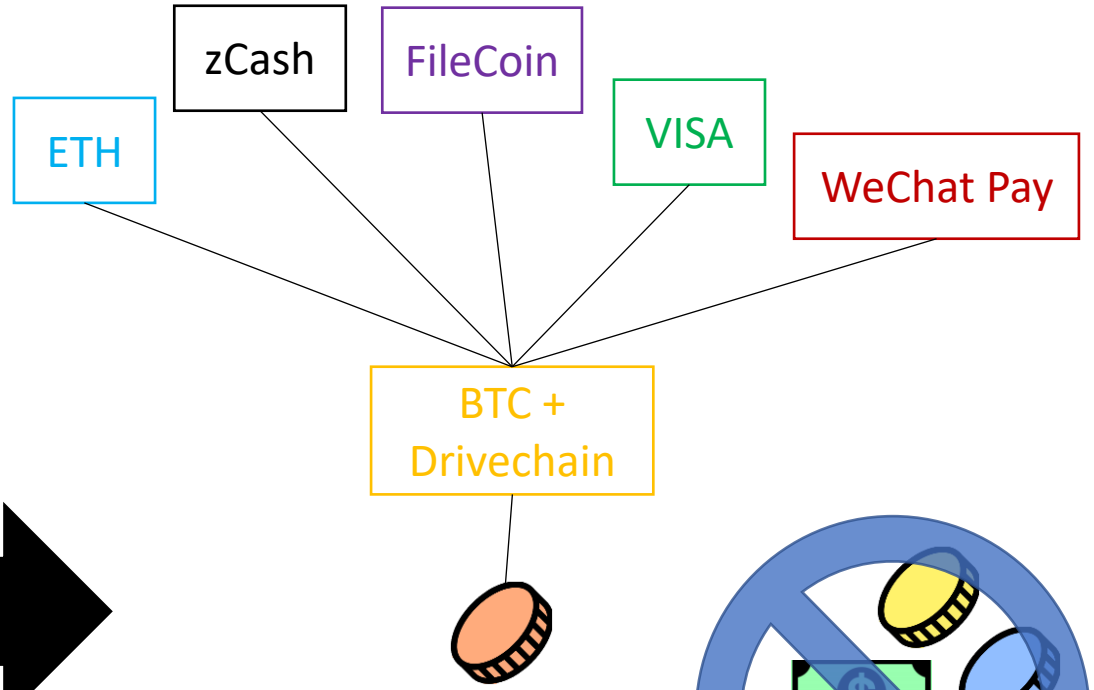
Today ☹

Tomorrow ☺

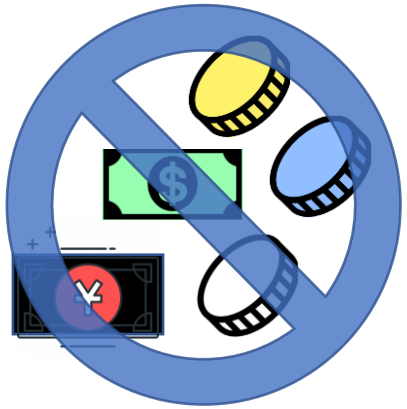
BIP300: Everything on Top of Bitcoin



Today ☹



Tomorrow ☺



The Coming Death of Bitcoin's Competitors

BTC
Today

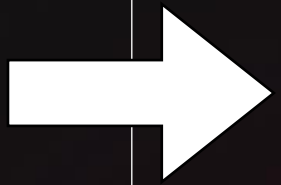
WeChat Pay

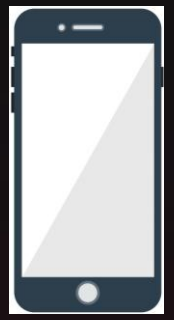
VISA

zCash

ETH

FileCoin

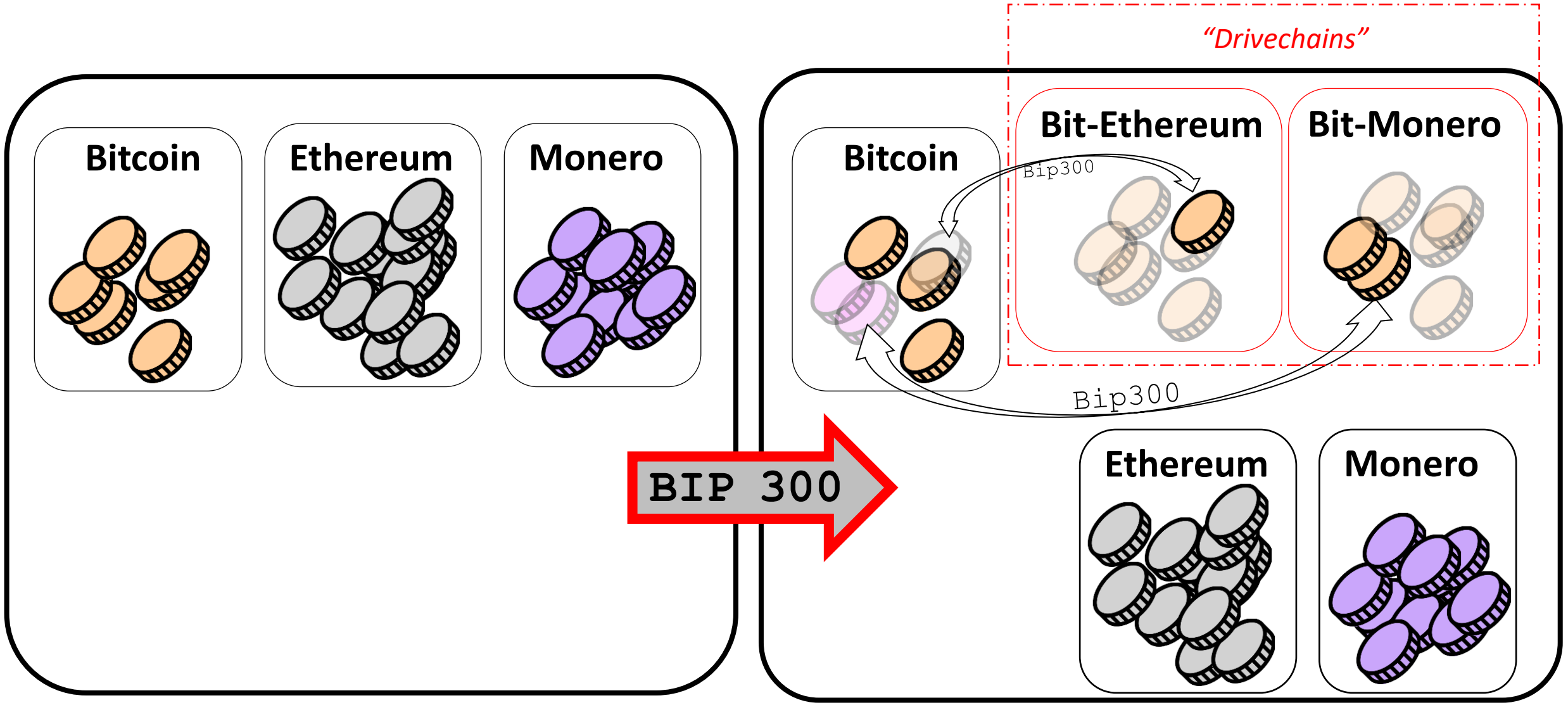




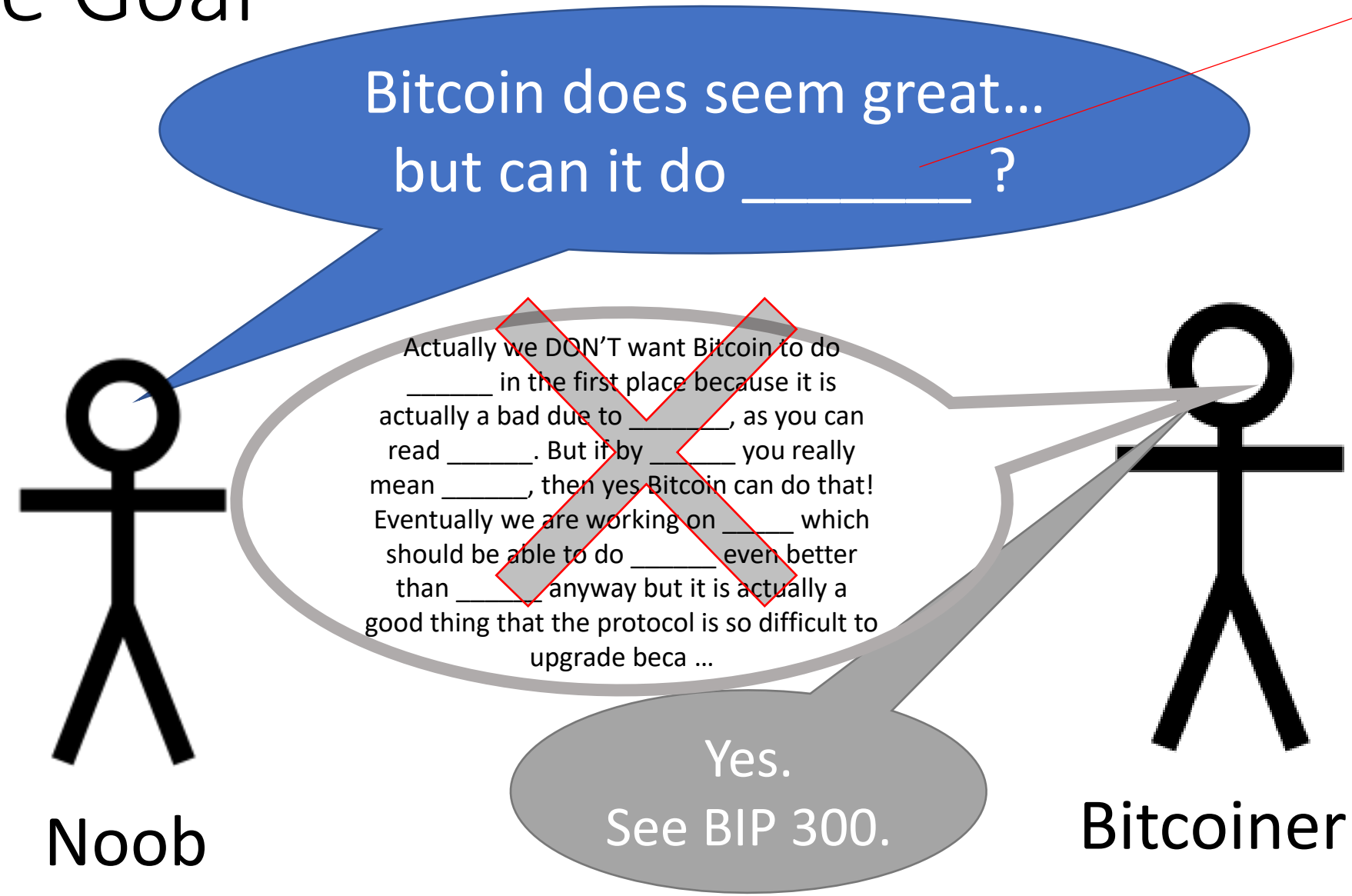
BTC +
Drivechain

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

Drivechain = Altcoin Tech, BTC Coin Only



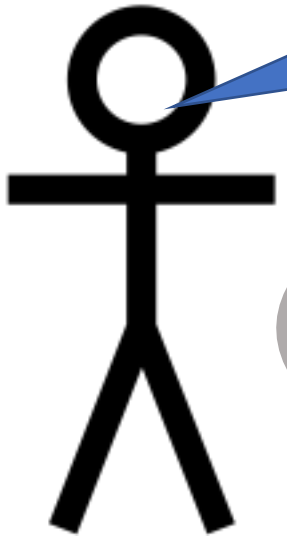
The Goal



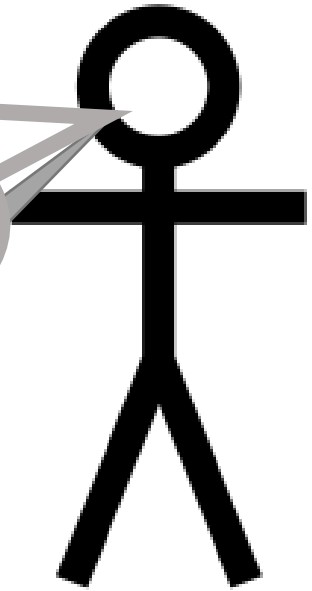
Smart Contracts
DeFi
Turing Completeness
Ring Signatures
zk-Snarks
Large Blocksizes
NFTs
Oracles
Mimblewimble
…(etc)

Fringe Ideas

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 …



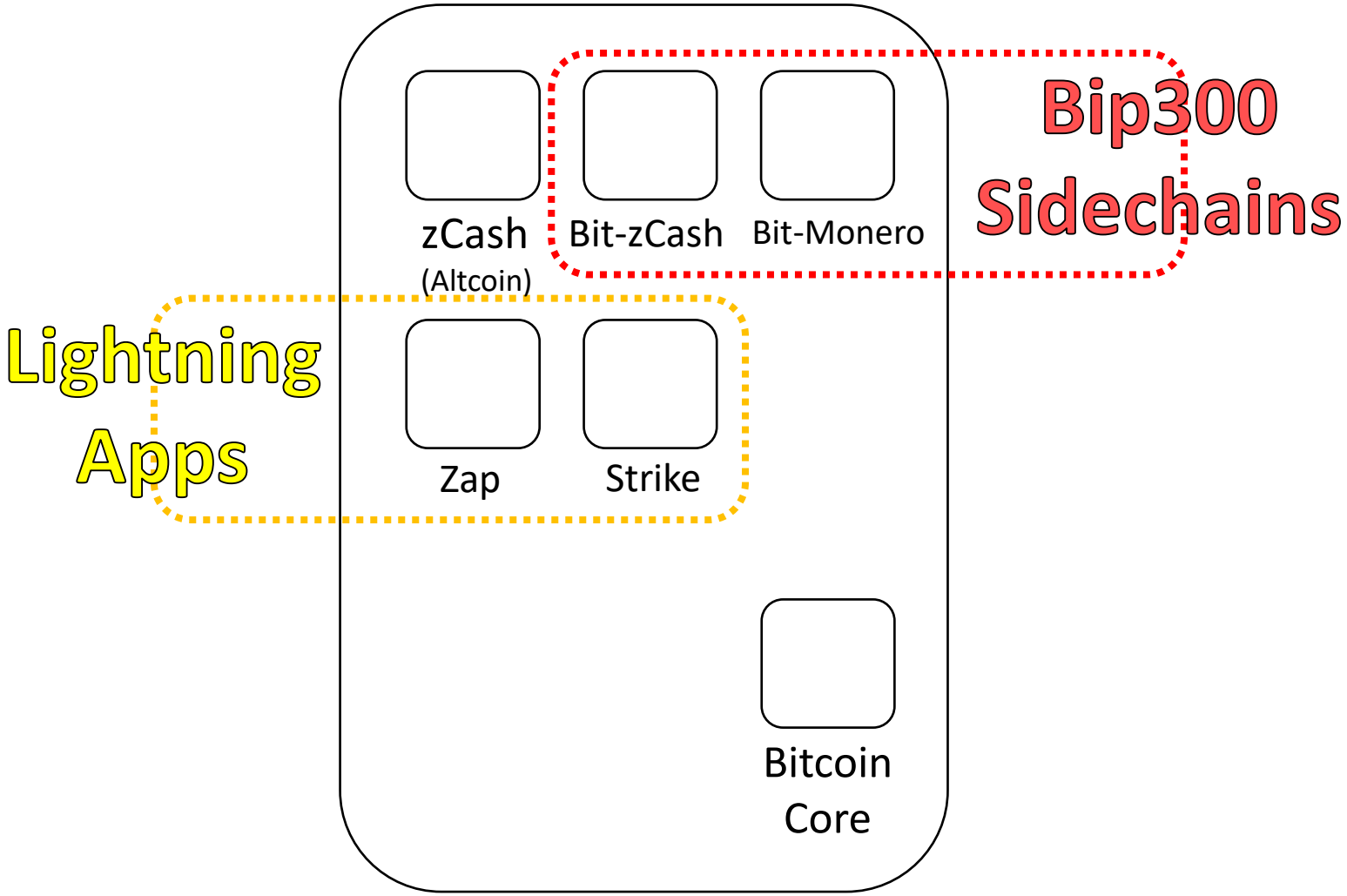
Noob (and/or Fringe Genius)

Use BIP 300.
Good luck!!

Bitcoiner

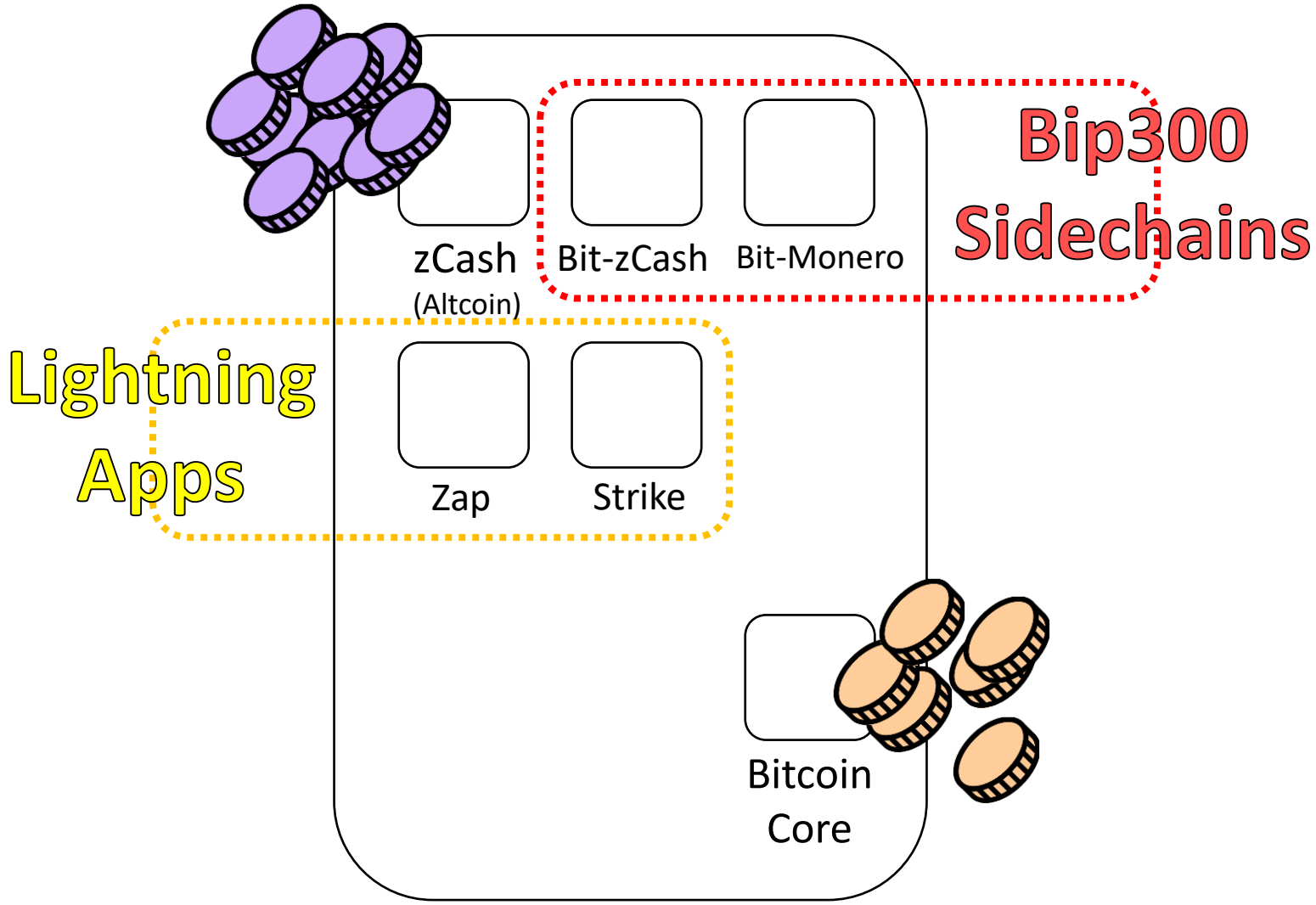
(#1) Full Autonomy

Metaphor



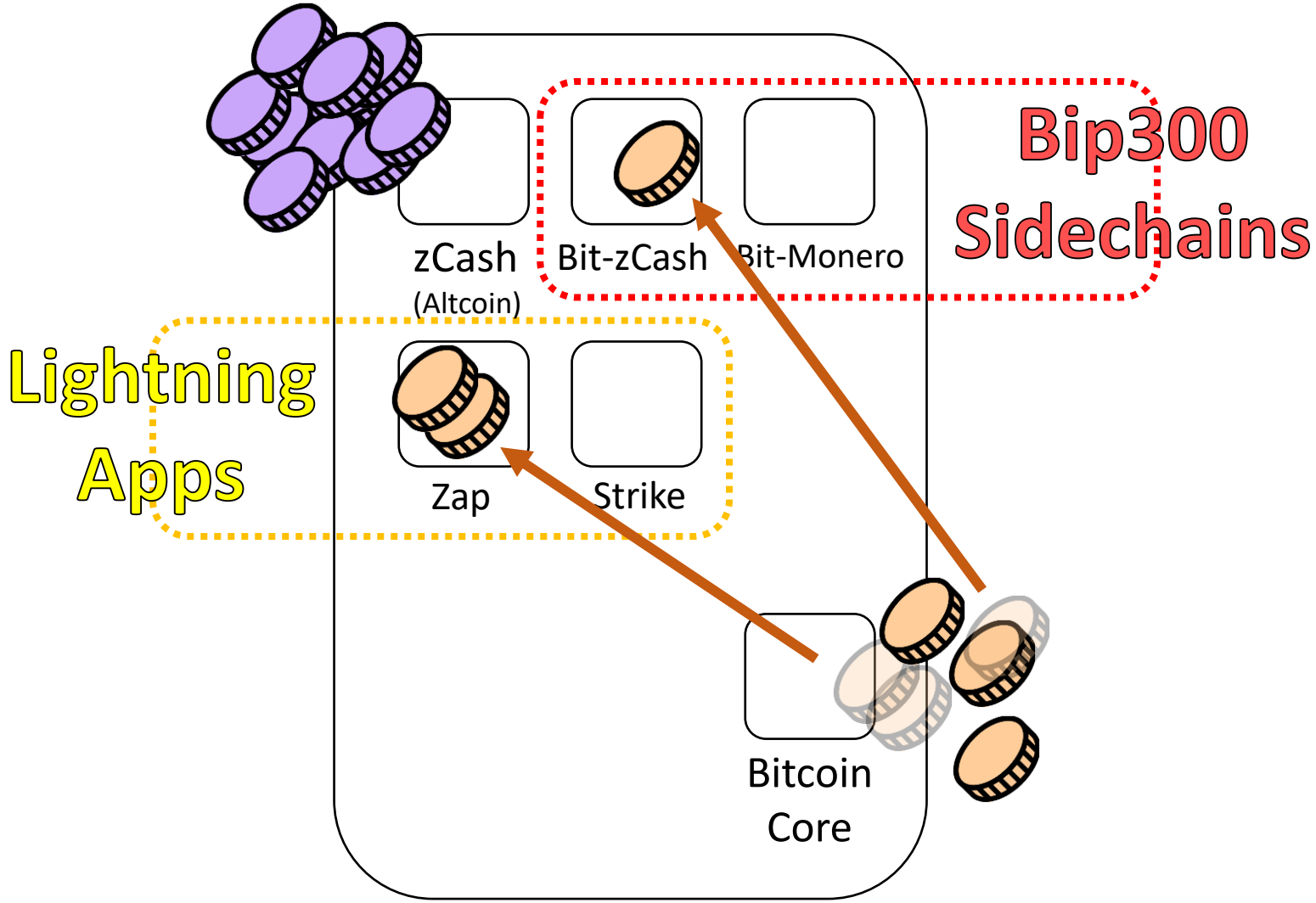
(#1) Full Autonomy

Metaphor

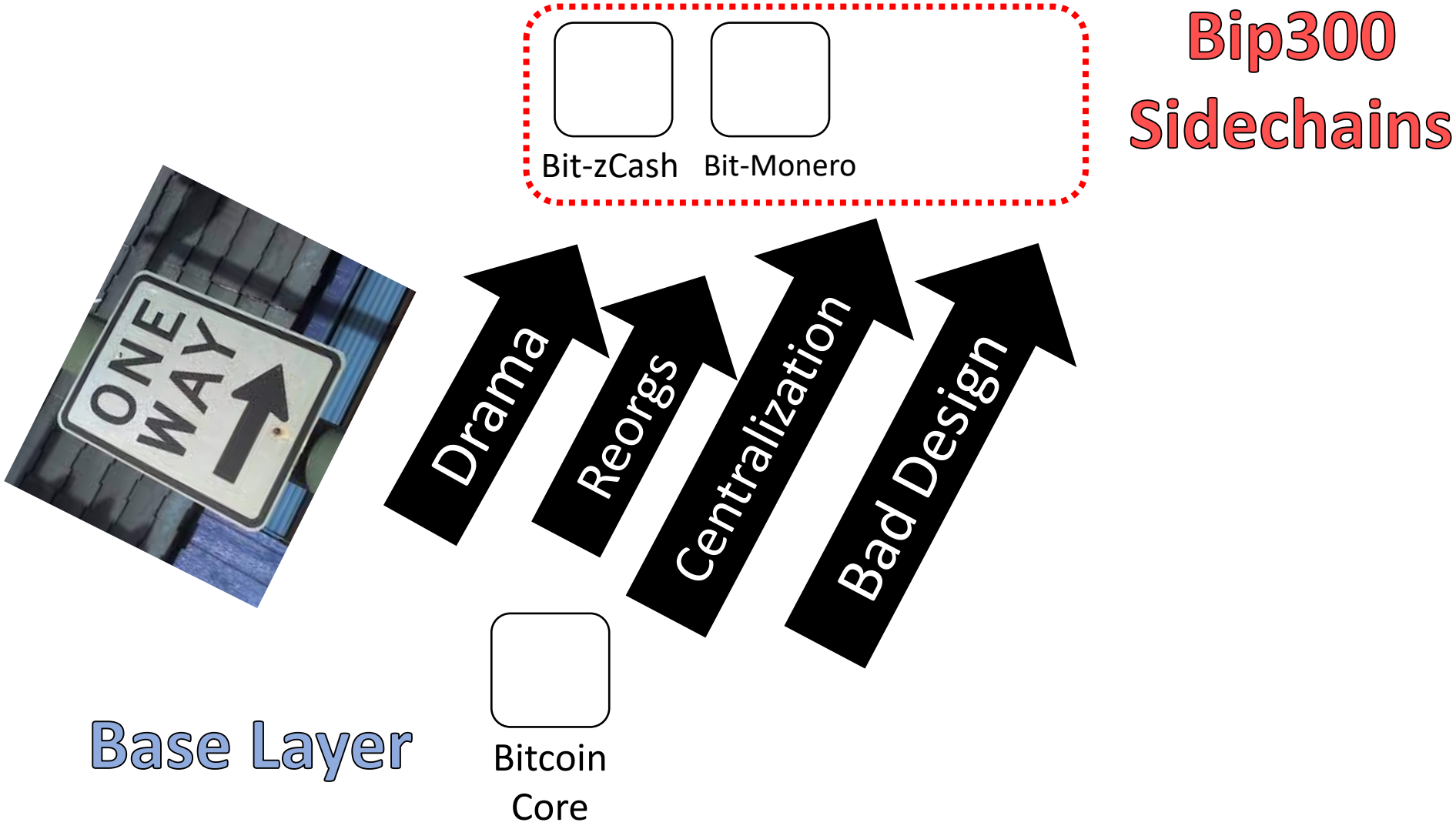


(#1) Full Autonomy

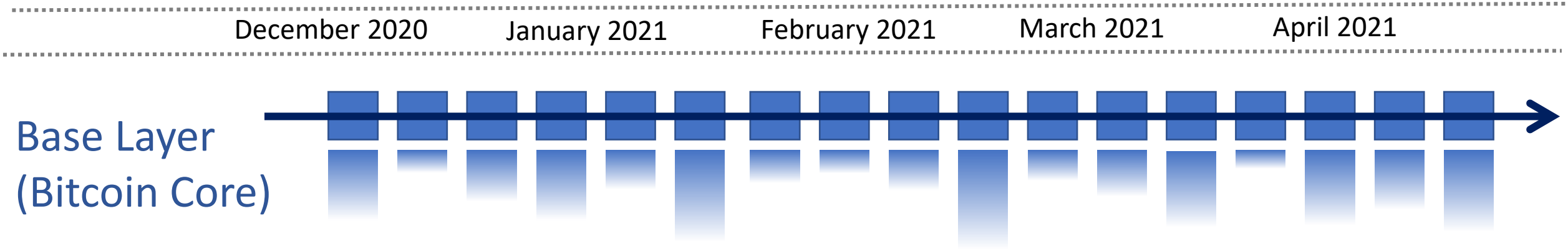
Metaphor



(#2) Base Layer safely ignores L2s



(#2) Base Layer safely ignores L2s



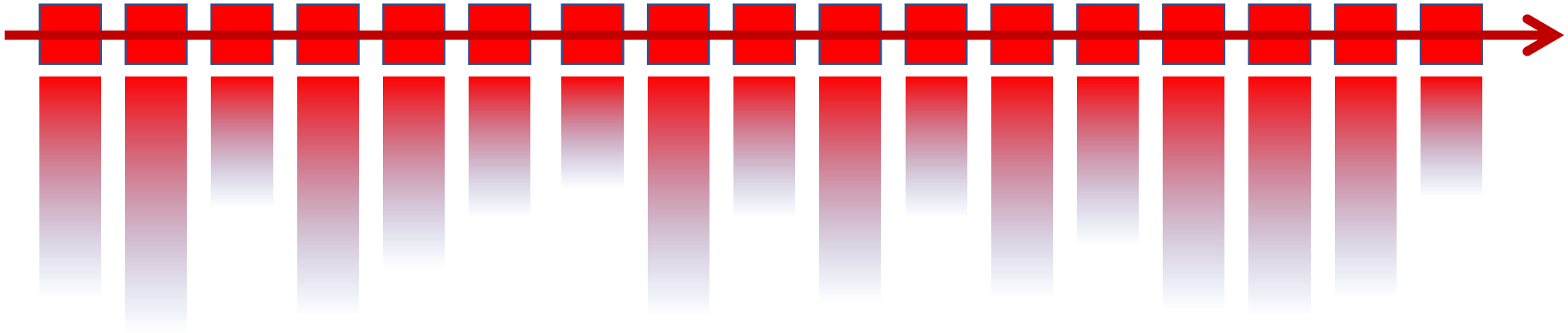
(#2) Base Layer is Safe

= Block Header

= List of transactions

December 2020 January 2021 February 2021 March 2021 April 2021

Layer 2
(Bit-Monero)



Base Layer
(Bitcoin Core)

Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

(#2) Base Layer is Safe

= Block Header

= List of transactions

December 2020 January 2021 February 2021 March 2021 April 2021

Layer 2
(Bit-Monero)

e320

81cd

3 Months = One 32-byte Hash

3 Months = One 32-byte Hash

e320b6c2fffc8d750423db8b1eb942ae710e951ed797f7affc8892b0f1fc122b

81cd02ab7e569e8bcd9317e2fe99f2de44d49ab2b885

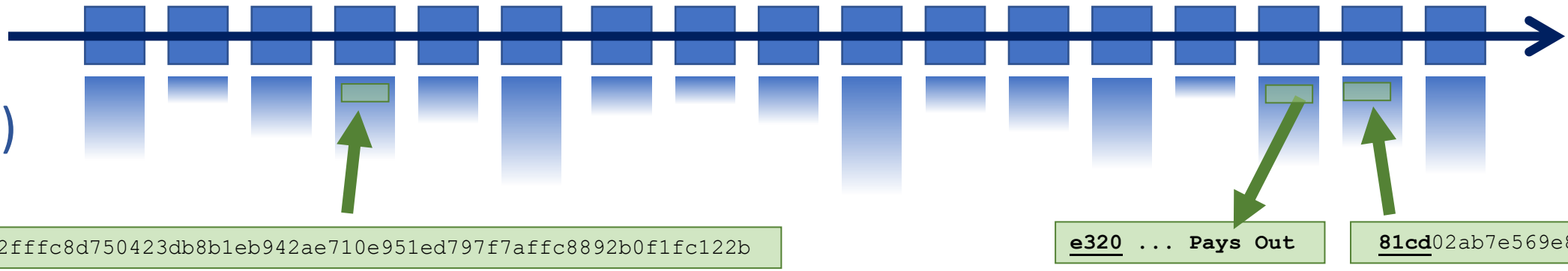
Base Layer
(Bitcoin Core)

e320 ... Pays Out

(#2) Base Layer is Safe

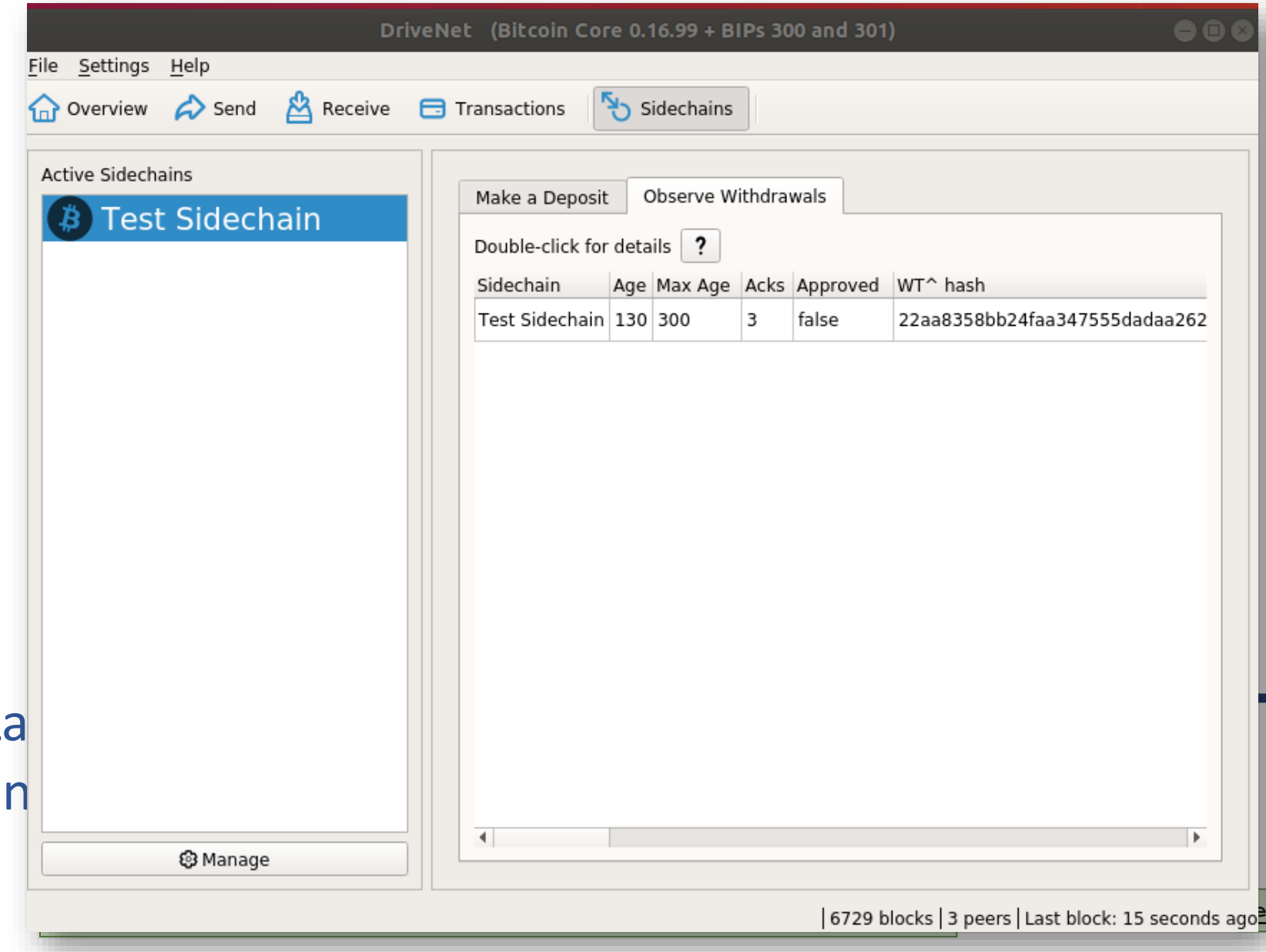
Your Layer 1 Node Sees…

Base Layer
(Bitcoin Core)

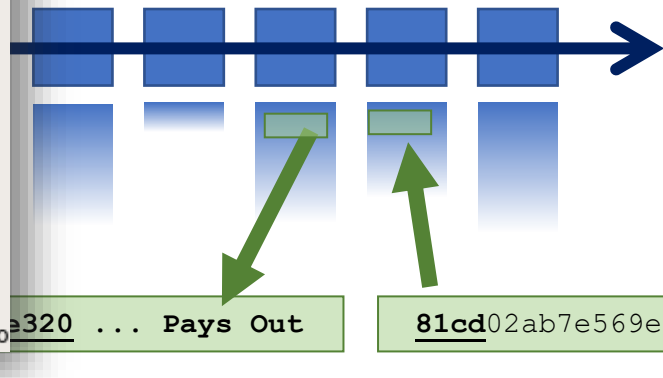


(#2) Base Layer is Safe

Your Layer 1 Node Sees…



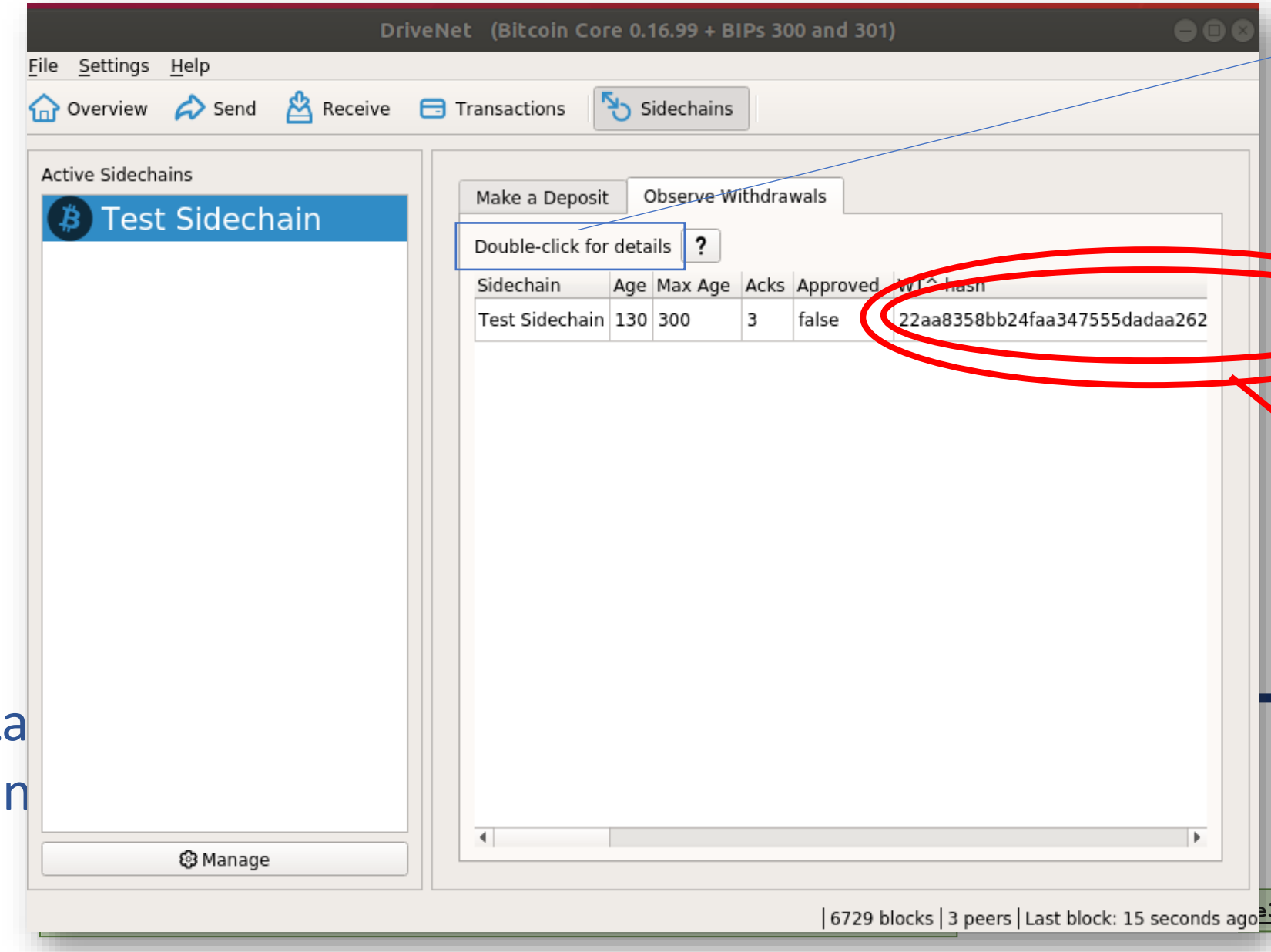
Base La
(Bitcoin



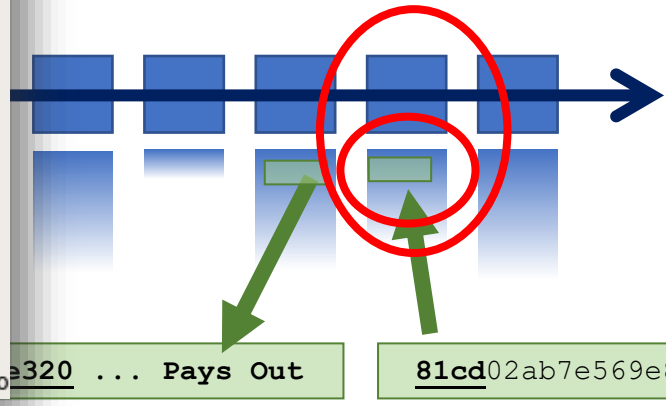
(#2) Base Layer is Safe

Your Layer 1 Node Sees…

Software will *look* for a sidechain node, on your computer, (to ask it questions).
But if it can't find one it will report back nothing.



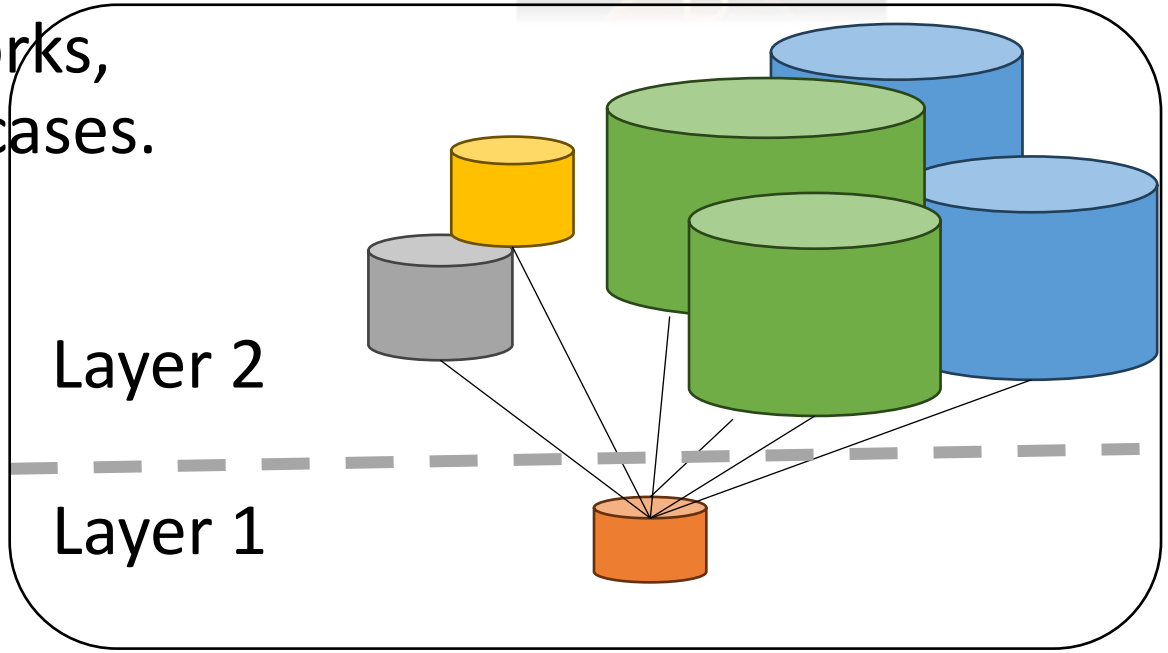
Hash we mentioned before

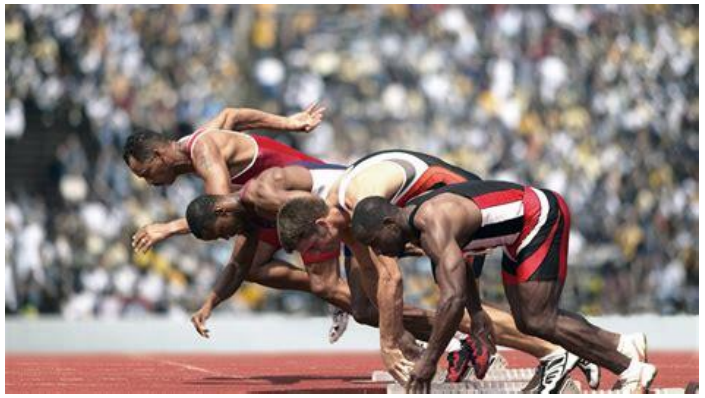


Base La
(Bitcoin

Collect Every Transaction Fee

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





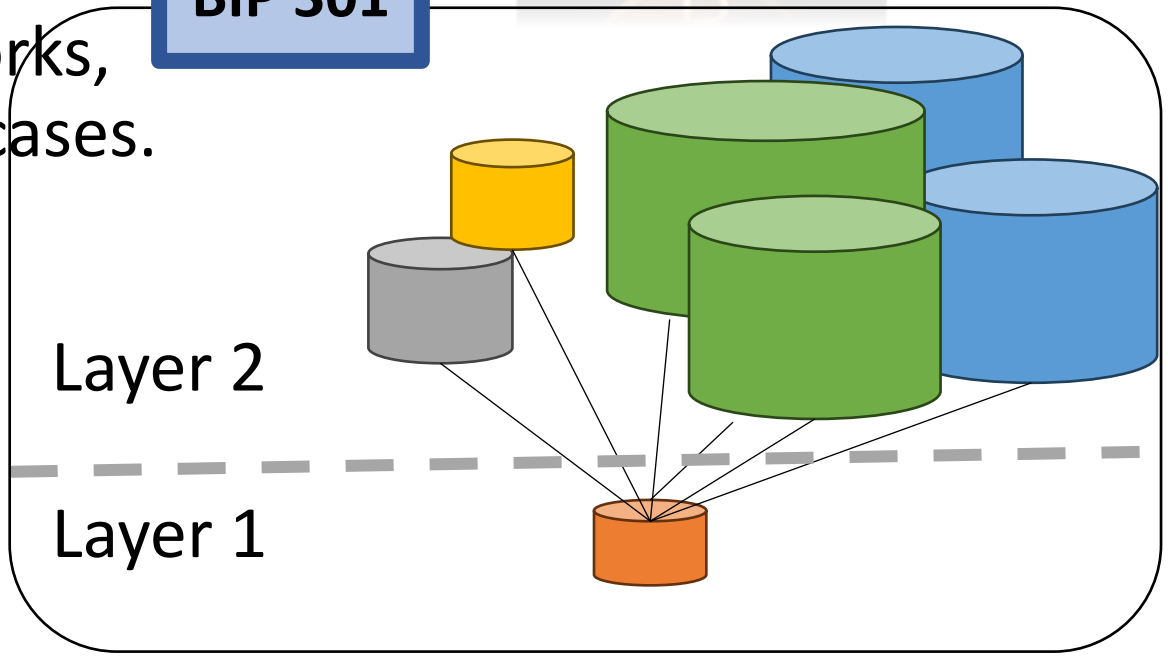
All the world's txns are <u>*already*</u> on some network or another.
They all pay some kind of fee to someone. (VISA, Venmo)

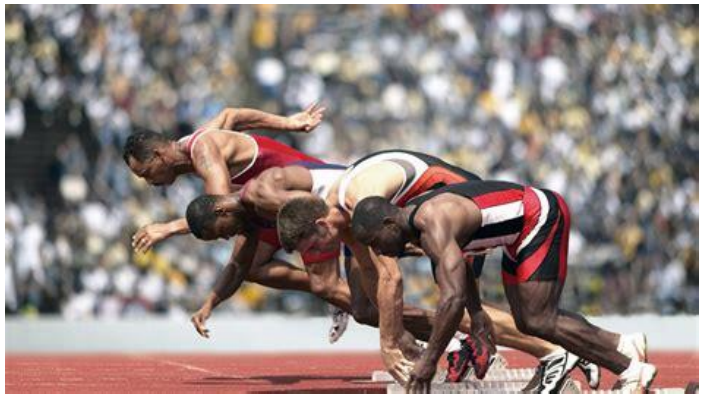
Collect Every Transaction Fee

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

BIP 300

BIP 301





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

The Goal

Crypto Fees

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

Share | Bundle | Filters | Yesterday

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

Crypto Fees

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

Share | Bundle | Filters | Yesterday

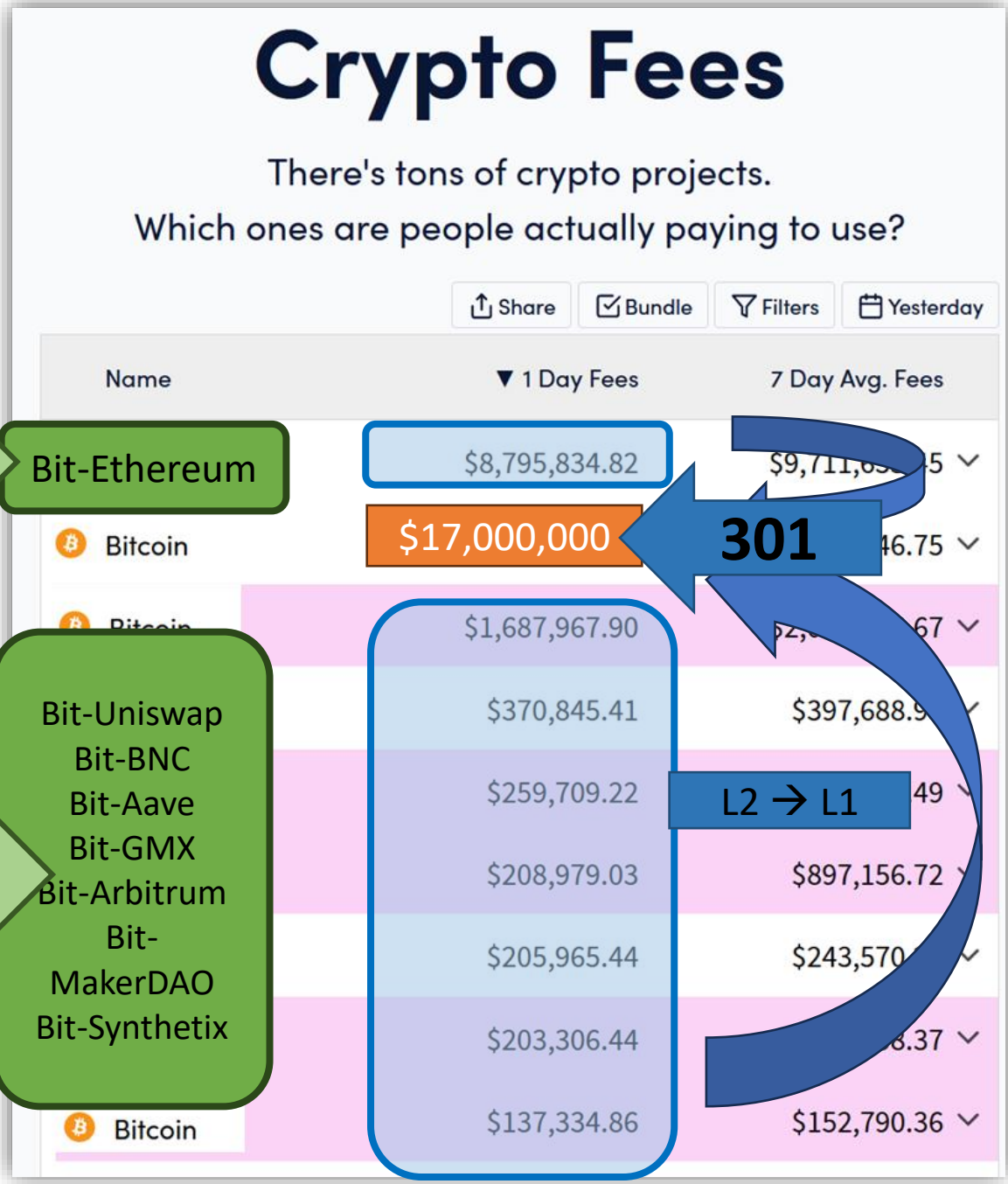
Name	▼ 1 Day Fees	7 Day Avg. Fees
Bitcoin	$8,795,834.82	$9,711,635.45
Bitcoin	$17,000,000	$5,201,946.75
Bitcoin	$1,687,967.90	$2,030,906.67
Bitcoin	$370,845.41	$397,688.93
Bitcoin	$259,709.22	$237,702.49
Bitcoin	$208,979.03	$897,156.72
Bitcoin	$205,965.44	$243,570.22
Bitcoin	$203,306.44	$196,858.37
Bitcoin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

The Goal

300

300

Alt → BTC



Bit-Ethereum

Bit-Uniswap
Bit-BNC
Bit-Aave
Bit-GMX
Bit-Arbitrum
Bit-
MakerDAO
Bit-Synthetix

301

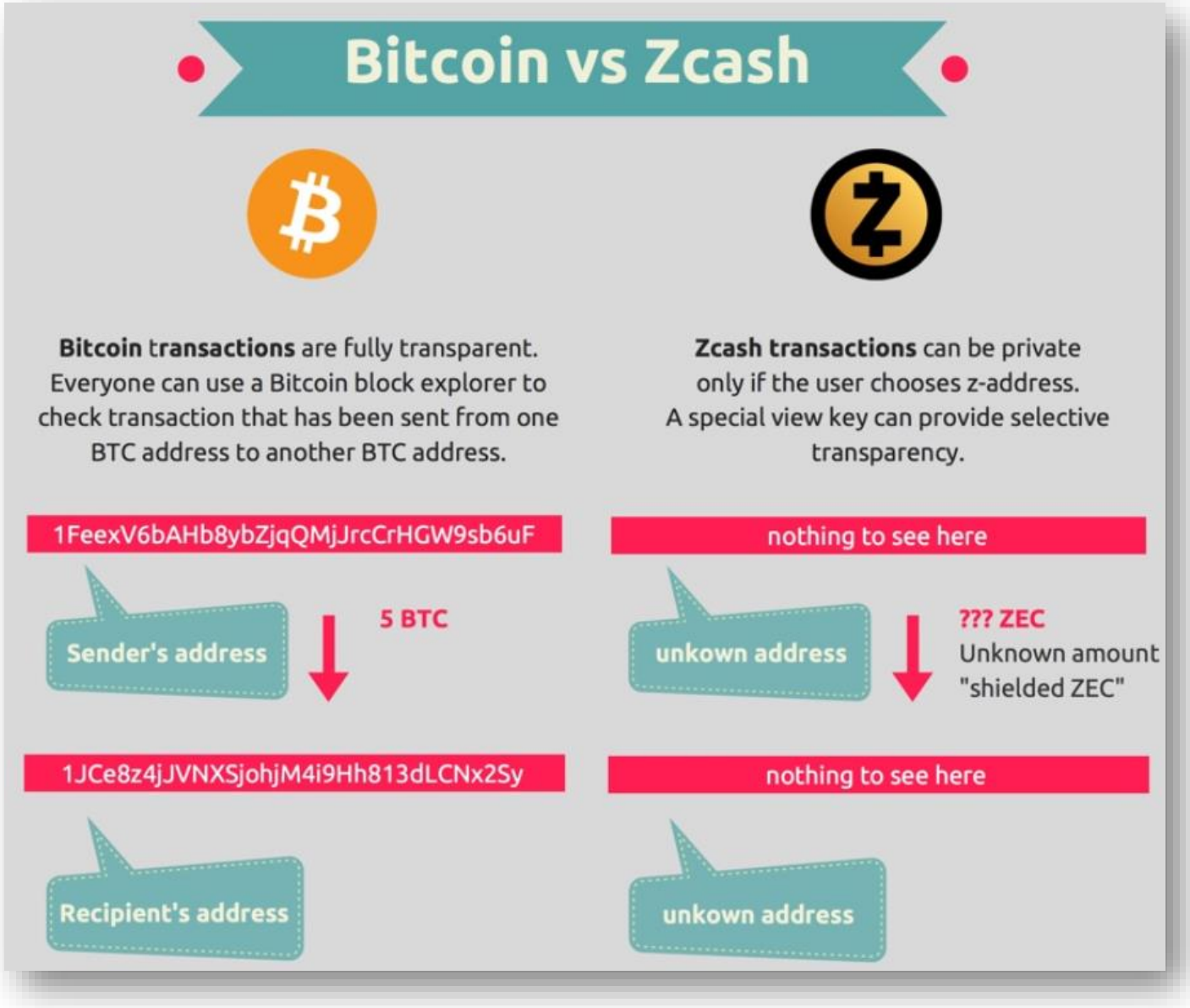
L2 → L1

Not limited to Existing Altcoins

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

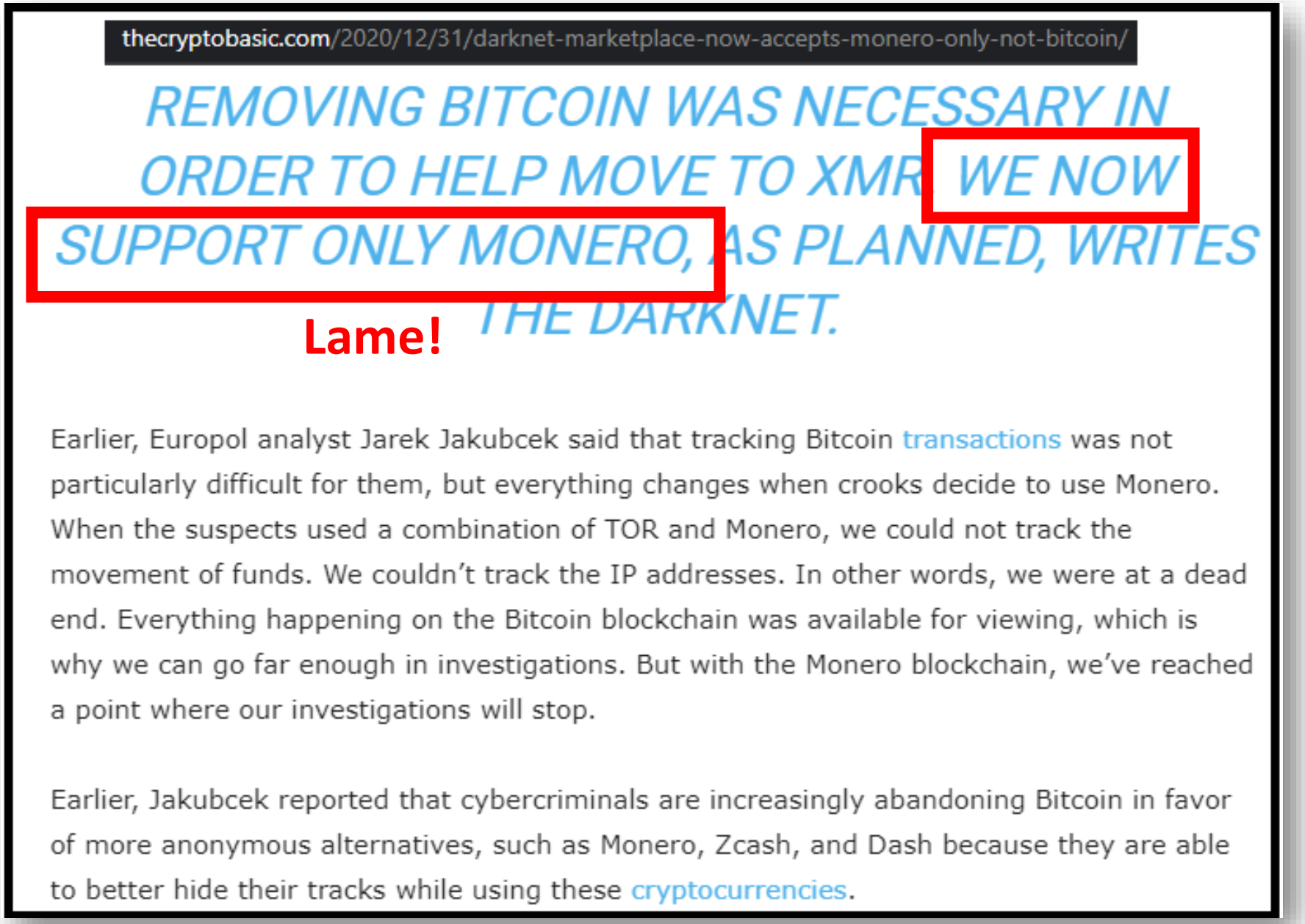
Altcoins we should copy (?): zCash

Image from blockchainhub.net :
https://blockchainhub.net/blog/infographics/zcash-explained/



Losing Customers to Monero (?)

"White House Market" Retired (not exit scam) on Oct 4, 2021 [last month]



thecryptobasic.com/2020/12/31/darknet-marketplace-now-accepts-monero-only-not-bitcoin/

REMOVING BITCOIN WAS NECESSARY IN ORDER TO HELP MOVE TO XMR, WE NOW SUPPORT ONLY MONERO, AS PLANNED, WRITES THE DARKNET.

Lame!

Earlier, Europol analyst Jarek Jakubcek said that tracking Bitcoin transactions was not particularly difficult for them, but everything changes when crooks decide to use Monero. When the suspects used a combination of TOR and Monero, we could not track the movement of funds. We couldn't track the IP addresses. In other words, we were at a dead end. Everything happening on the Bitcoin blockchain was available for viewing, which is why we can go far enough in investigations. But with the Monero blockchain, we've reached a point where our investigations will stop.

Earlier, Jakubcek reported that cybercriminals are increasingly abandoning Bitcoin in favor of more anonymous alternatives, such as Monero, Zcash, and Dash because they are able to better hide their tracks while using these cryptocurrencies.

Altcoins we should copy (?): NameCoin

satoshi
Founder
Sr. Member

Activity: 364
Merit: 2754

Re: BitDNS and Generalizing Bitcoin
December 10, 2010, 05:29:28 PM
Merited by BitcoinFX (1), darosior (1)
#246

Piling every proof-of-work quorum system in the world into one dataset doesn't scale.

Bitcoin and BitDNS can be used separately. Users shouldn't have to download all of both to use one or the other.
BitDNS users may not want to download everything the next several unrelated networks decide to pile in either.

The networks need to have separate fates. BitDNS users might be completely liberal about adding any large data features since relatively few domain registrars are needed, while Bitcoin users might get increasingly tyrannical about limiting the size of the chain so it's easy for lots of users and small devices.

Fears about securely buying domains with Bitcoins are a red herring. It's easy to trade Bitcoins for other non-repudiable commodities.

If you're still worried about it, it's cryptographically possible to make a risk free trade. The two parties would set up transactions on both sides such that when they both sign the transactions, the second signer's signature triggers the release of both. The second signer can't release one without releasing the other.

Re: BitDNS and Generalizing Bitcoin
December 10, 20
Merited by Aveatr

Quote from: Hal on De

additional block chain
on exchanges? These
purchase some kinds

Right, the exchange

satoshi
Founder
Sr. Member

Activity: 364
Merit: 2754

Re: BitDNS and Generalizing Bitcoin
December 09, 2010, 10:46:50 PM
Merited by ImHash (1)

Quote from: nanotube on December 09, 2010, 09:20:40 PM

seems that the miner would have to basically do "extra work". and if there's no
(which of course, slows down the main bitcoin work), what would be a miner's
chains) ?

The incentive is to get the rewards from the extr side chains also fo

A longer interval than 10 minutes would be appropriate for BitDNS.

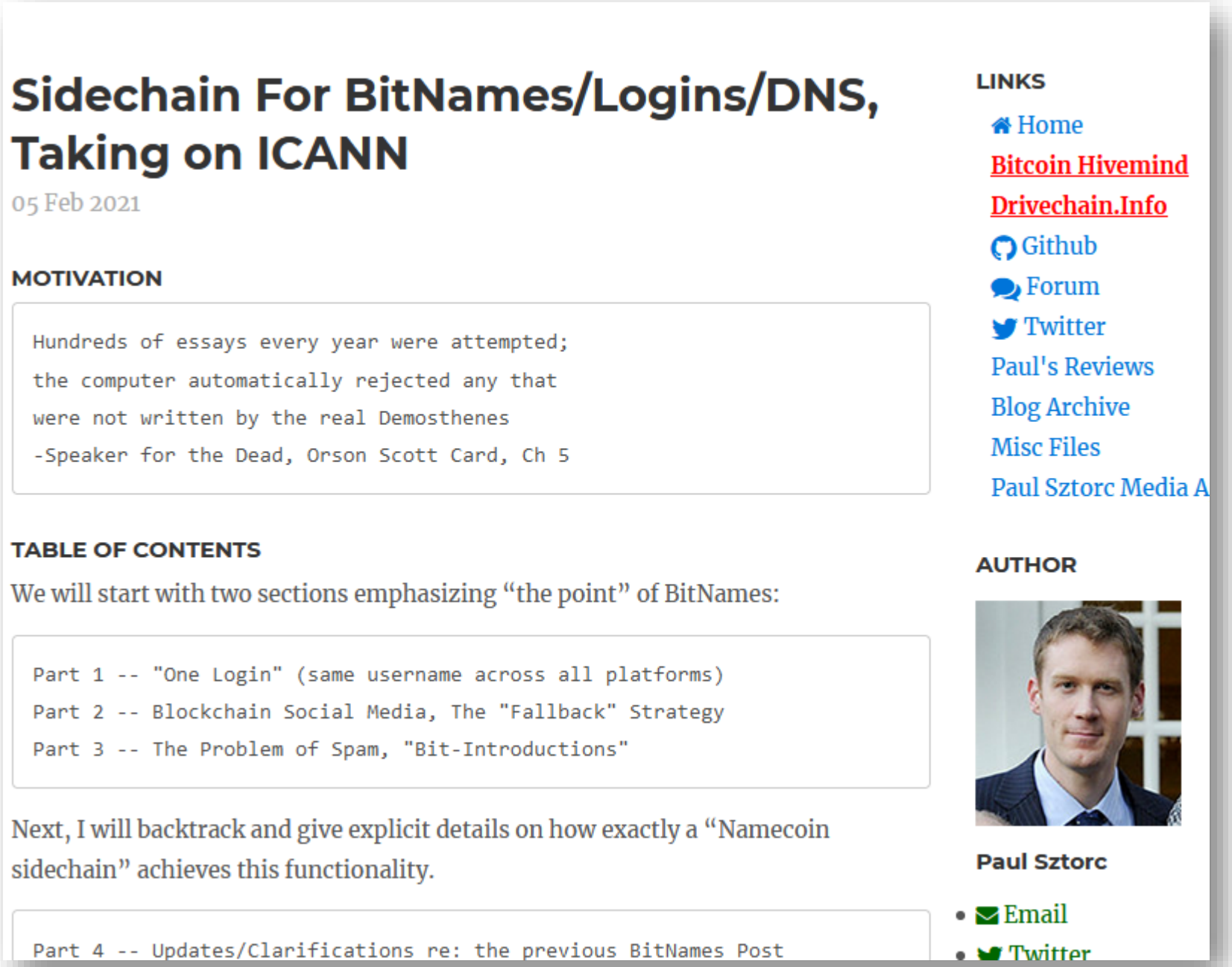
So far in this discussion there's already a lot of housekeeping data required. It will be
much easier if you can freely use all the space you need without worrying about paying
fees for expensive space in Bitcoin's chain. Some transactions:

Fun facts -- in this thread, Satoshi:
* Invents what is now known as Merged Mining.
* Assumes that there will be many separate blockchains that pay different fees (as if this were non-controversial!).
* The term “side chain” is used numerous times!

Altcoins we should copy (?): NameCoin

Screenshot #0 from

www.truthcoin.info/blog/bitnames/



Sidechain For BitNames/Logins/DNS, Taking on ICANN

05 Feb 2021

MOTIVATION

```
Hundreds of essays every year were attempted;
the computer automatically rejected any that
were not written by the real Demosthenes
-Speaker for the Dead, Orson Scott Card, Ch 5
```

TABLE OF CONTENTS

We will start with two sections emphasizing "the point" of BitNames:

```
Part 1 -- "One Login" (same username across all platforms)
Part 2 -- Blockchain Social Media, The "Fallback" Strategy
Part 3 -- The Problem of Spam, "Bit-Introductions"
```

Next, I will backtrack and give explicit details on how exactly a "Namecoin sidechain" achieves this functionality.

```
Part 4 -- Updates/Clarifications re: the previous BitNames Post
```

LINKS

Home
Bitcoin Hivemind
Drivechain.Info
Github
Forum
Twitter
Paul's Reviews
Blog Archive
Misc Files
Paul Sztorc Media A

AUTHOR

Paul Sztorc

Email
Twitter

Altcoins we should copy (?): NameCoin

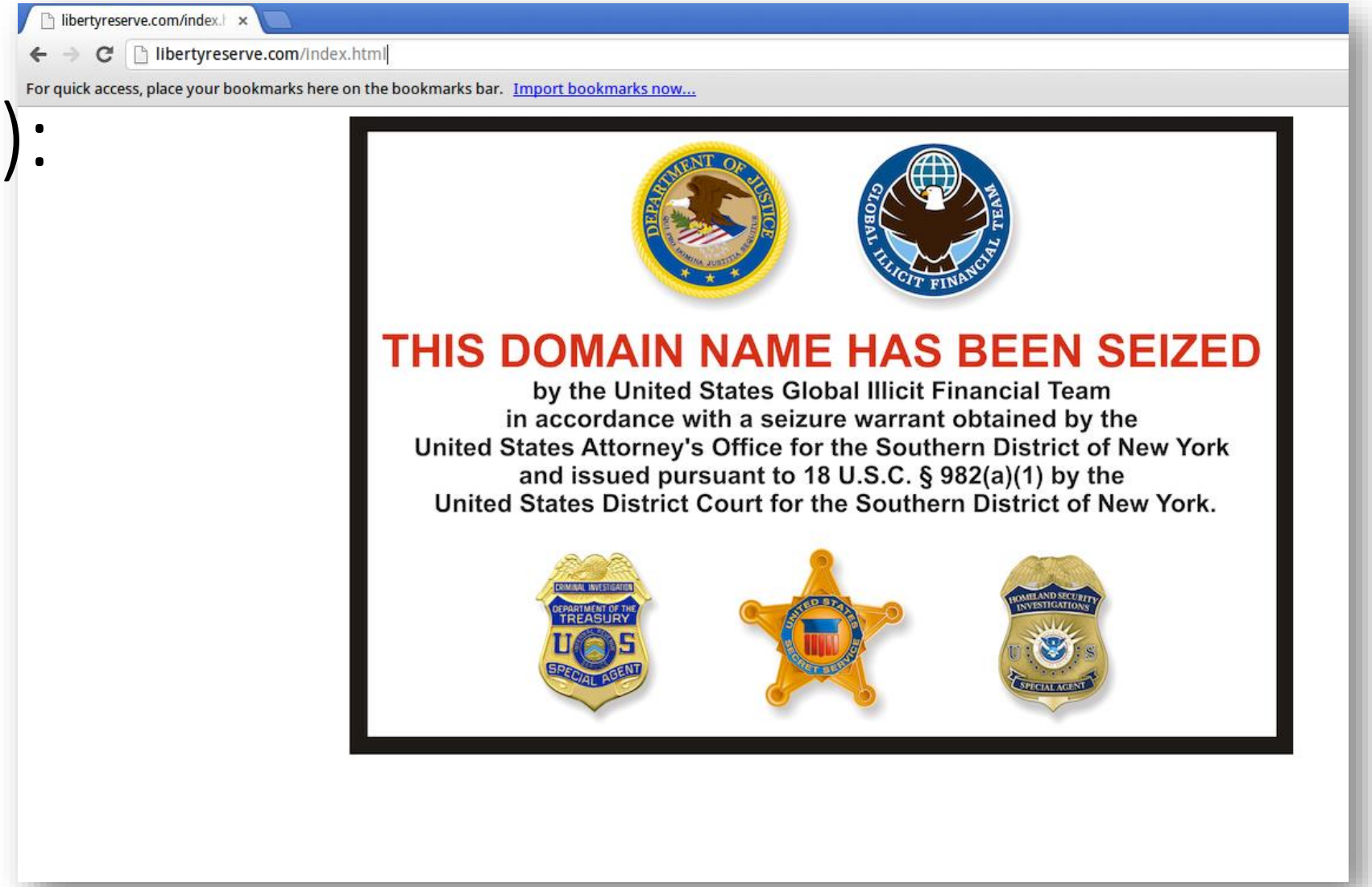
Screenshot #1 from

www.truthcoin.info/blog/bitnames/

Altcoins we should copy (?): NameCoin

Screenshot #2 from

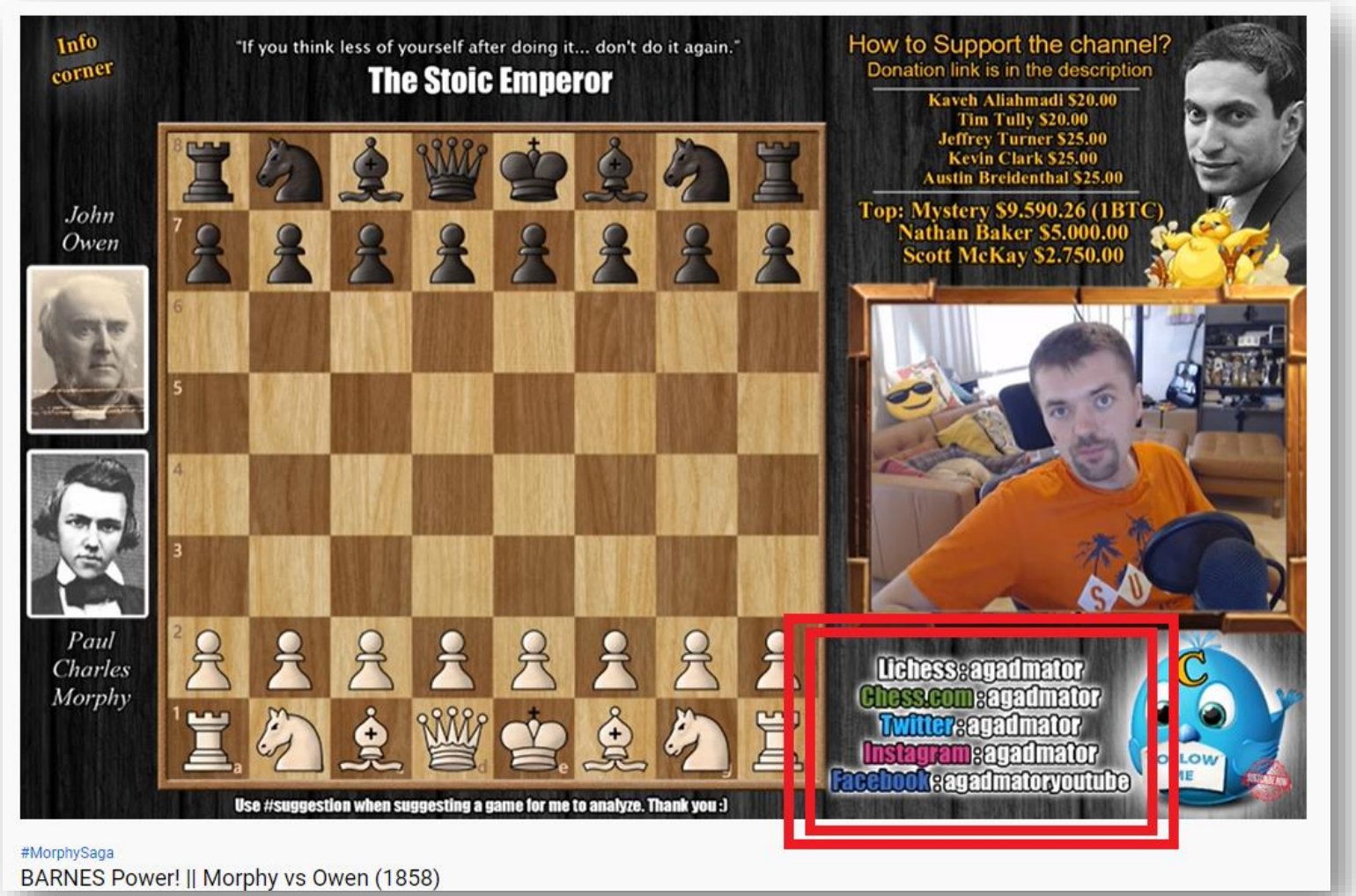
www.truthcoin.info/blog/bitnames/



Altcoins we should copy (?): NameCoin

Screenshot #3 from

www.truthcoin.info/blog/bitnames/



Altcoins we should copy (?): XCP / BitAssets / ERC20

Non-fungible token

From Wikipedia, the free encyclopedia

"NFT" redirects here. For other uses, see NFT (disambiguation).

This article **may contain wording that promotes the subject through exaggeration of unnoteworthy facts**. Please help improve it by removing or replacing such wording. *(May 2021) (Learn how and when to remove this template message)*

A **non-fungible token** (**NFT**) is a unit of data stored on a digital ledger, called a blockchain, that certifies a digital asset to be unique and therefore not interchangeable.[1] NFTs can be used to represent items such as photos, videos, audio, and other types of digital files. Access to any copy of the original file, however, is not restricted to the buyer of the NFT. While copies of these digital items are available for anyone to obtain, NFTs are tracked on blockchains to provide the owner with a proof of ownership that is separate from copyright.

In 2021, there has been increased interest in using NFTs. Blockchains like Ethereum, Flow, and Tezos have their own standards when it comes to supporting NFTs, but each works to ensure that the digital item represented is authentically one-of-a-kind. NFTs are now being used to commodify digital assets in art, music, sports, and other popular entertainment. Most NFTs are part of the Ethereum blockchain; however, other blockchains can implement their own versions of NFTs.[2] The NFT market value tripled in 2020, reaching more than $250 million.[3]

So lame!!

Contents [hide]

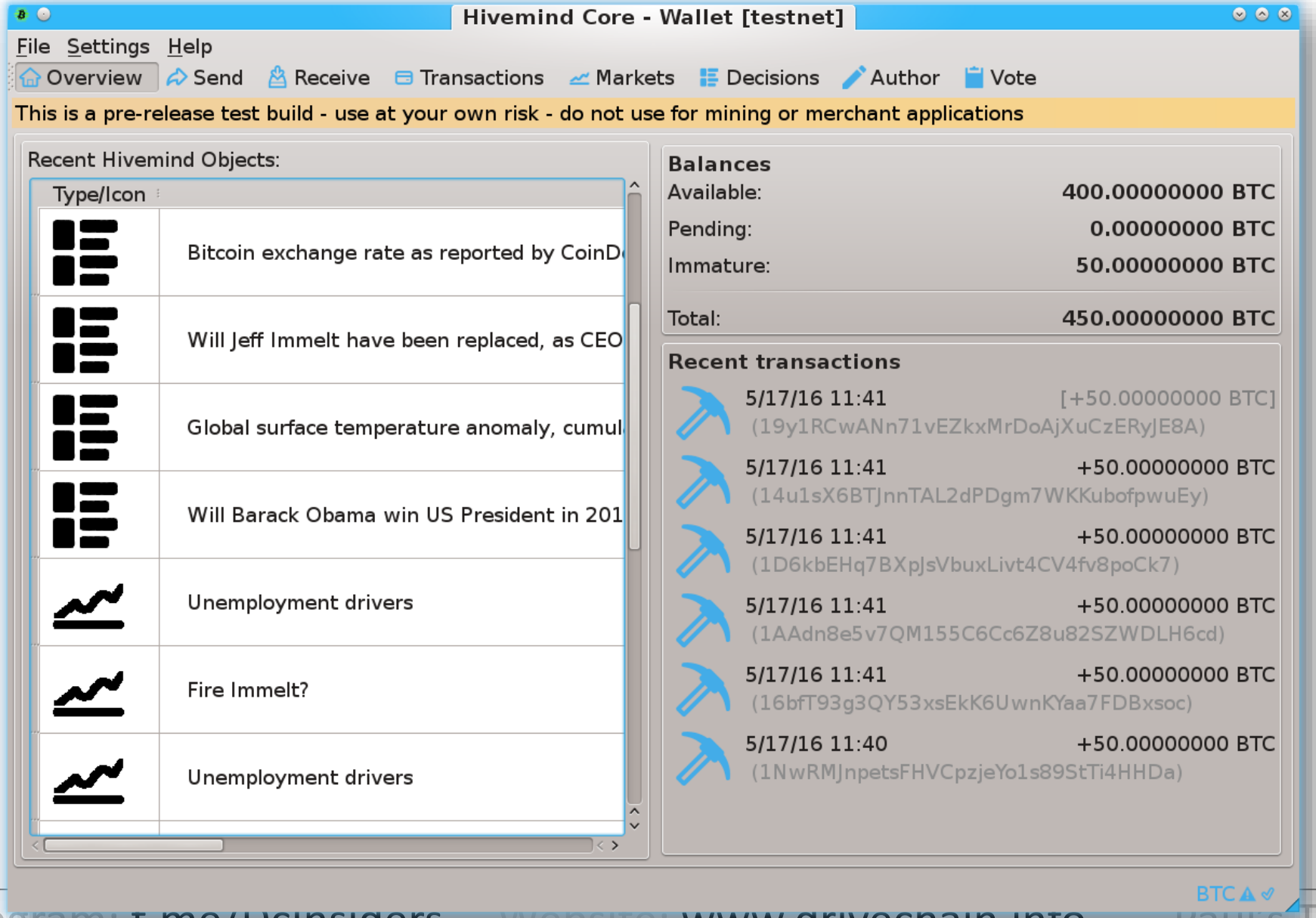
1 Description

Logo used to represent fungible tokens

Prediction Markets

- Screenshots from my own BTC sidechain project

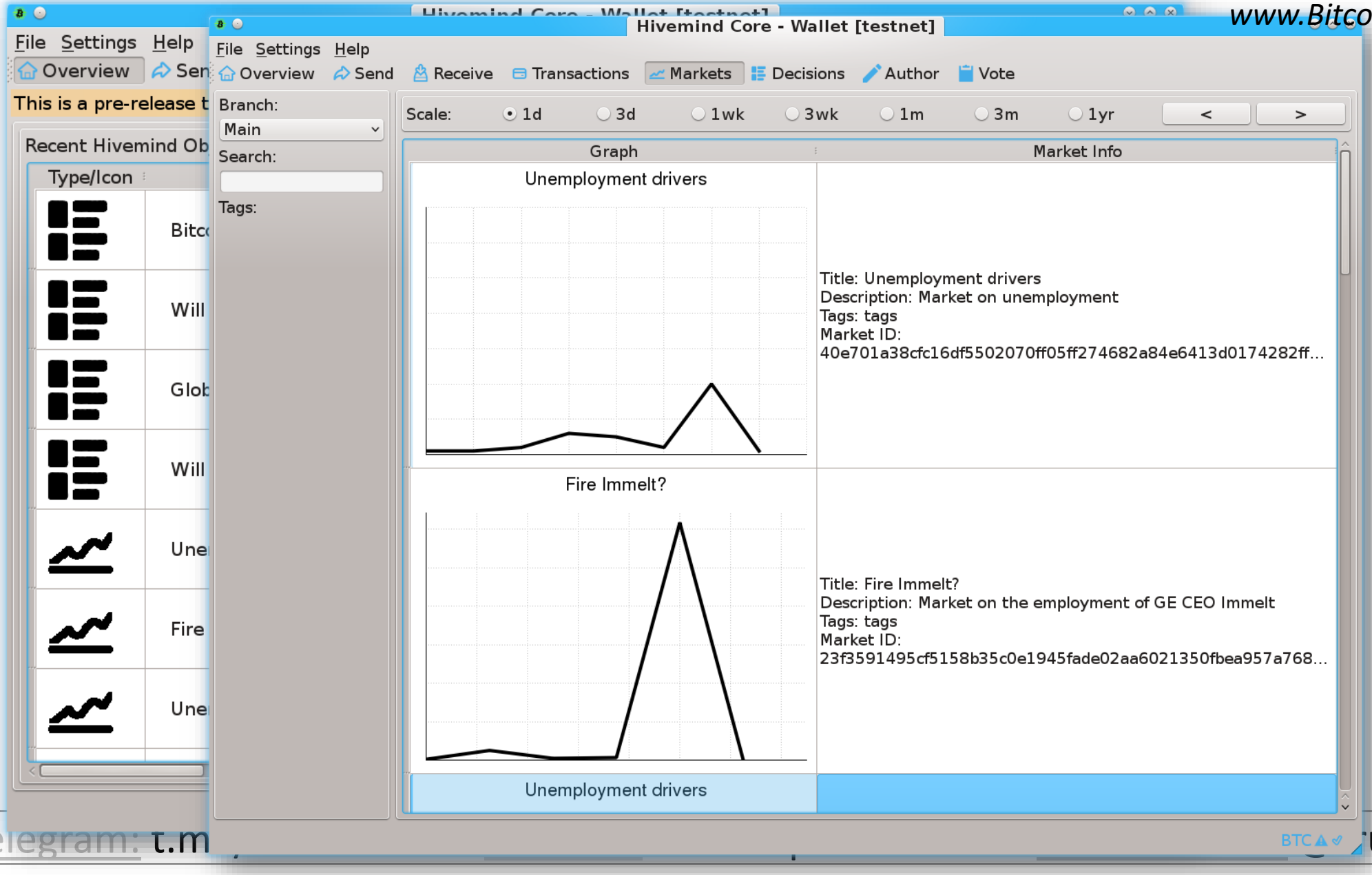
www.BitcoinHivemind.com



Prediction Markets

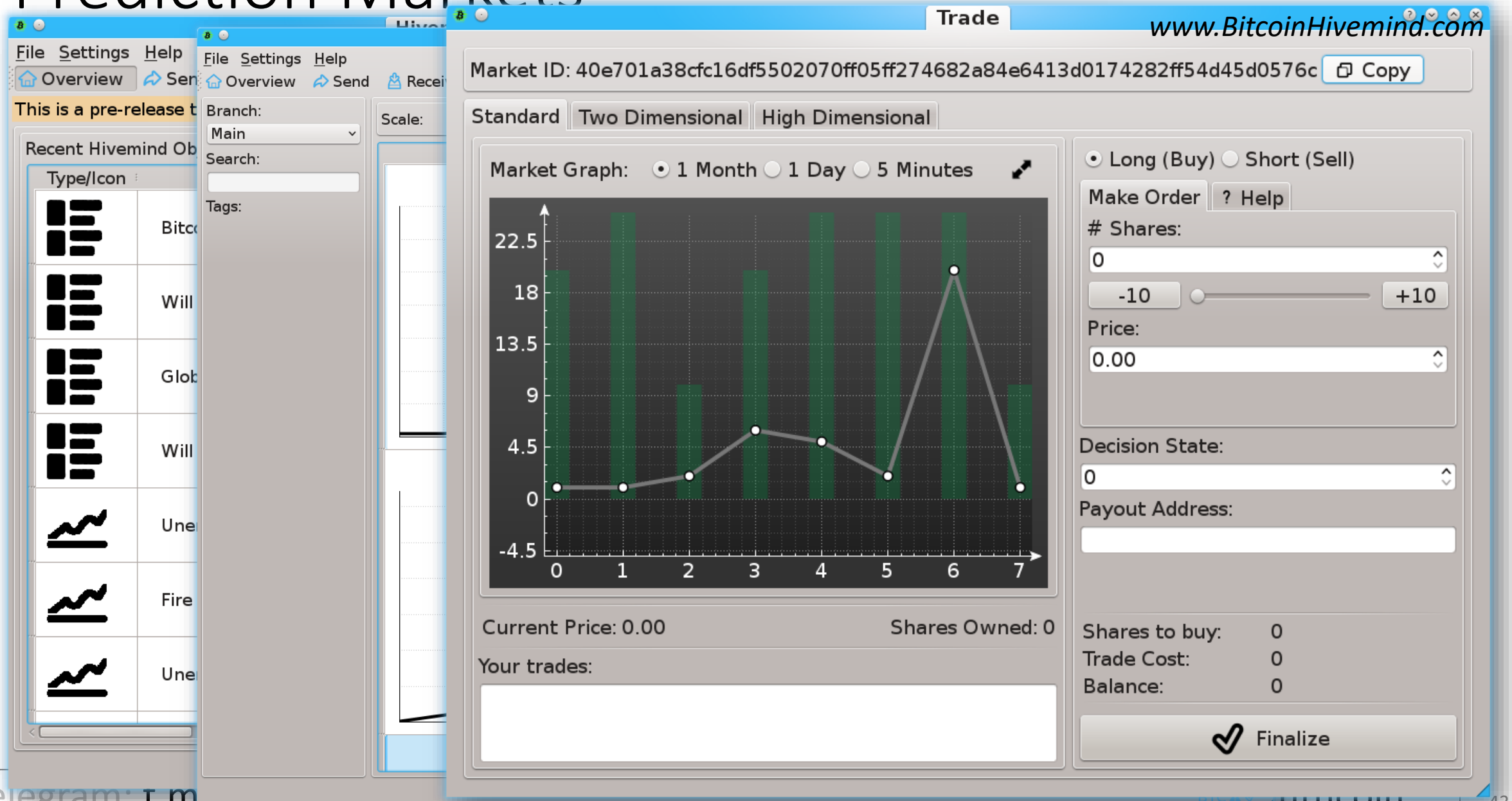
- Screenshots from my own BTC sidechain project

www.BitcoinHivemind.com



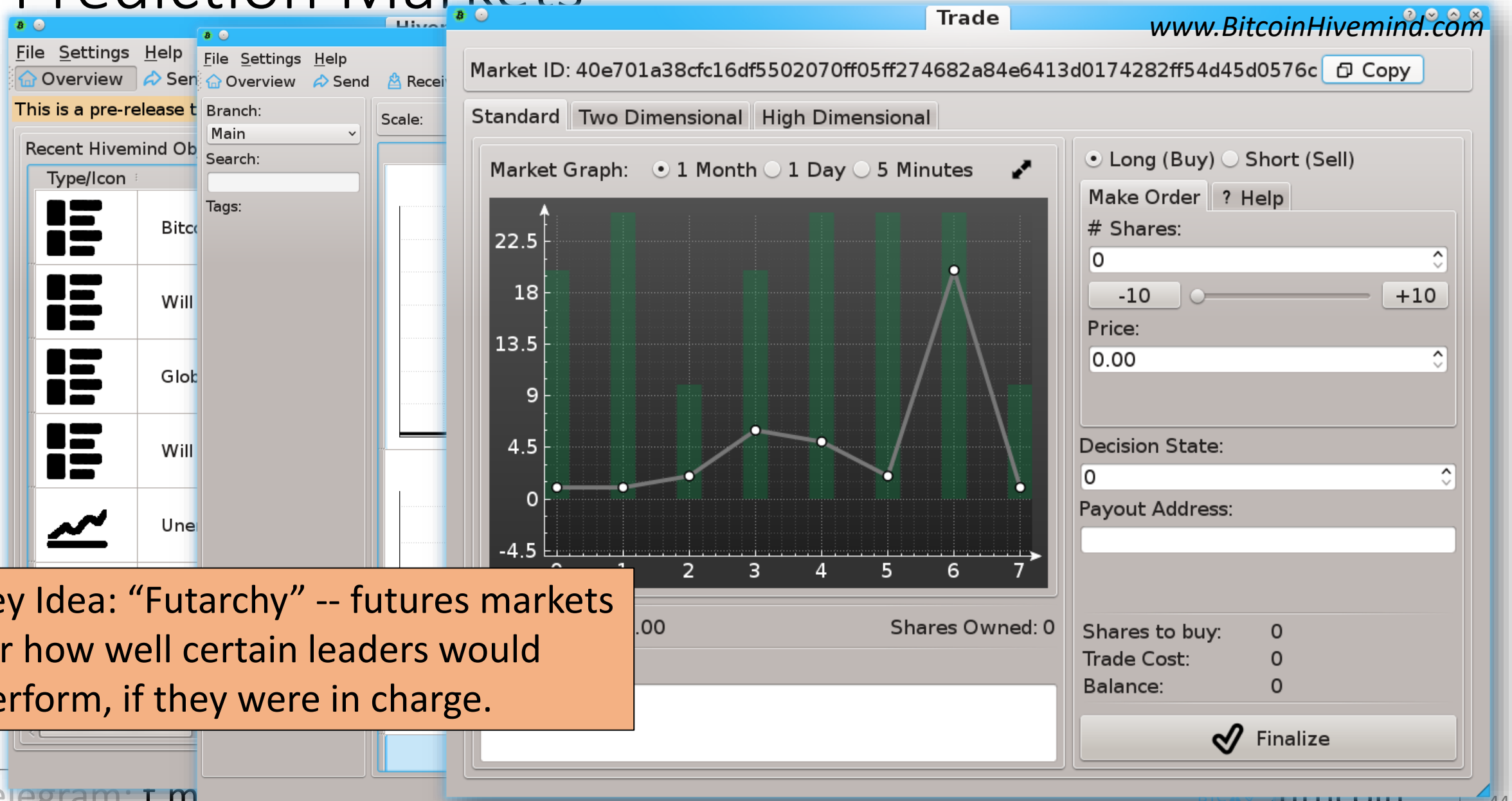
Prediction Markets

- 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.

Altcoins we should copy (?): Sia

- P2P Cloud Storage – Managed via Blockchain
- Running for 5 years
- No files ever lost?
- $1-2 per TB/month (vs $23 on Amazon S3)

https://sia.tech

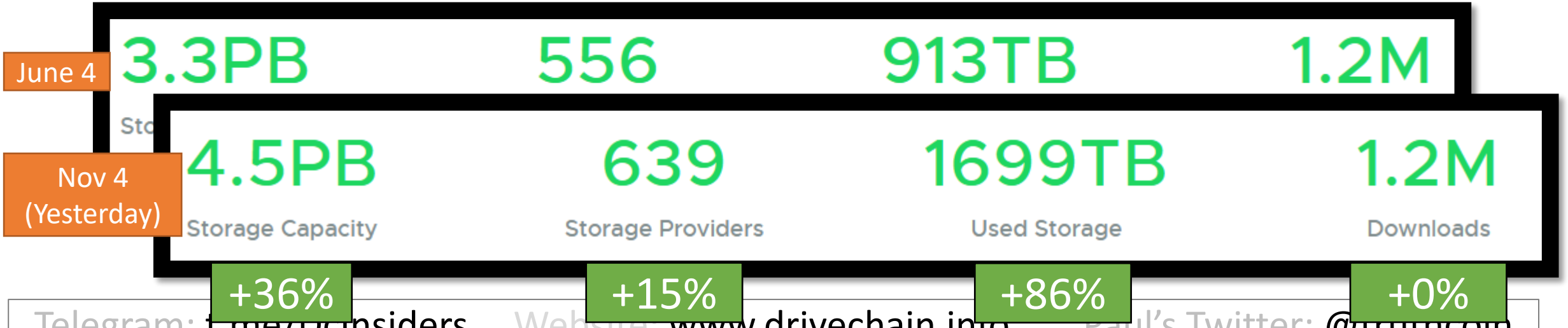
June 4

3.3PB	556	913TB	1.2M
Storage Capacity	Storage Providers	Used Storage	Downloads

Altcoins we should copy (?): Sia

- P2P Cloud Storage – Managed via Blockchain
- Running for 5 years
- No files ever lost?
- $1-2 per TB/month (vs $23 on Amazon S3)

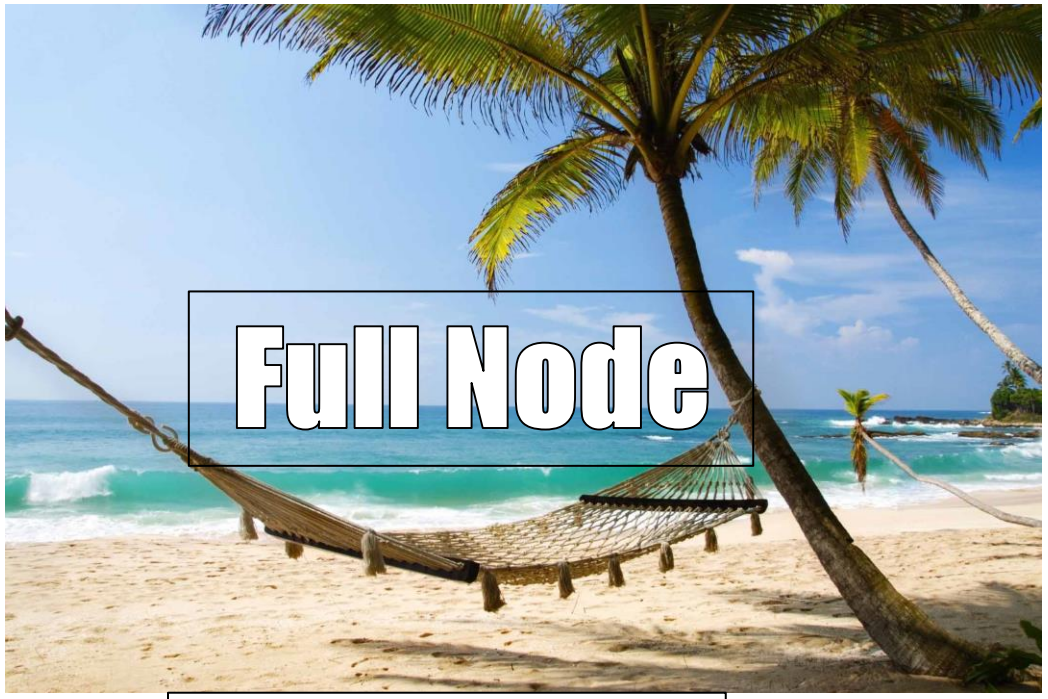
https://sia.tech



Finally: How Bip300 Improves Layer1

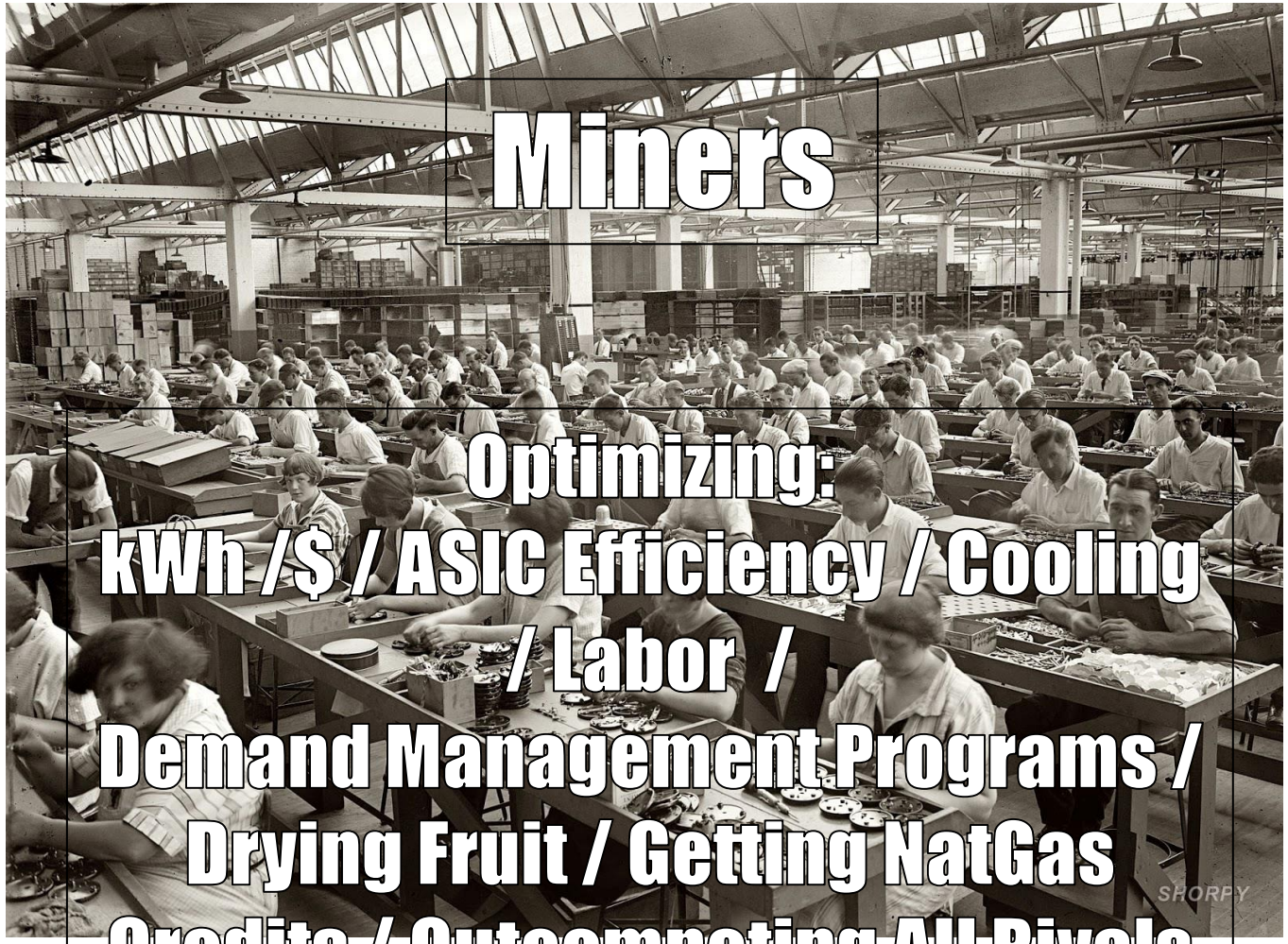
1. Never Change Layer 1 Again
   – “Protocol Ossification”
   - No “drama”.
   - No “mob rule”.
2. Shrink Layer1 Blocksize.
   - Improves Decentralization.
   - Protects your node.

“Frozen Bitcoin” - Marco Verch , Creative Commons License



Validating L1

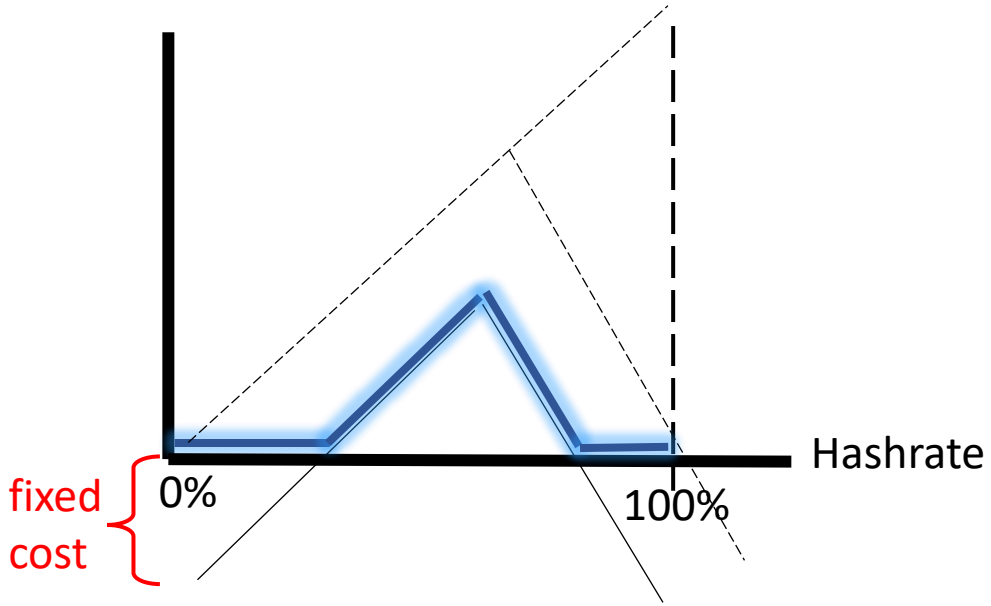
+ counting to 13,150



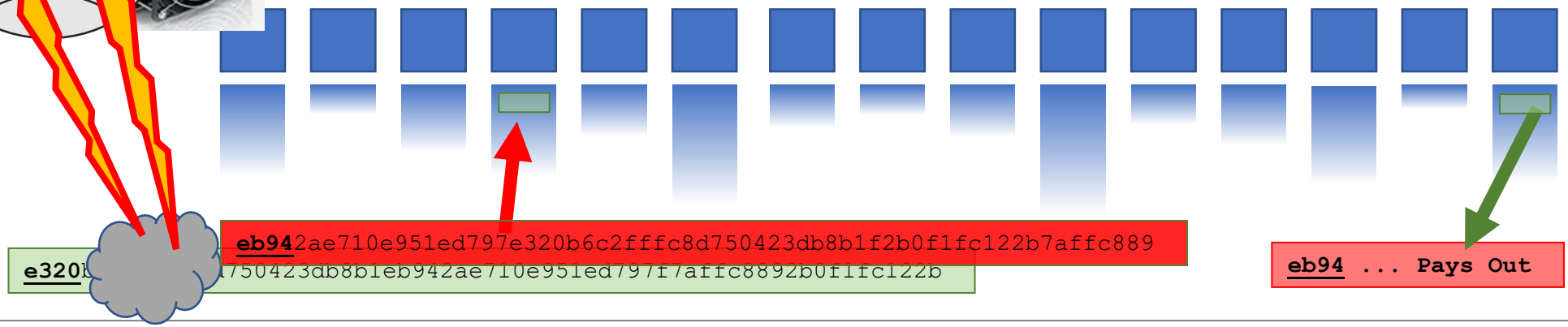
+ add/remove/validate Sidechains

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.

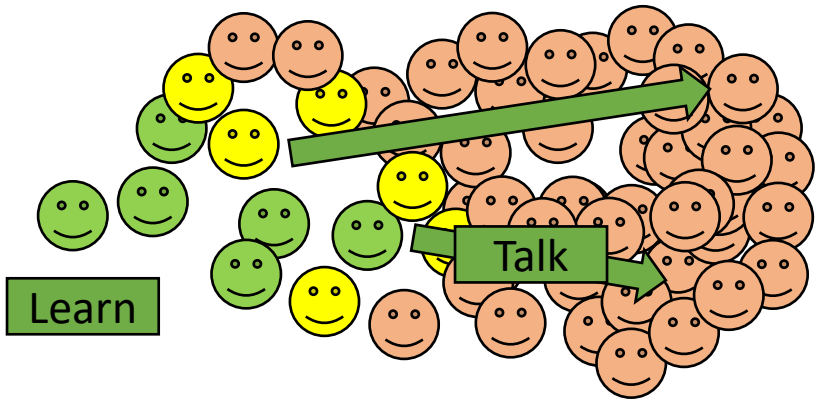
(#1) **Miners-Can-Steal** from Bip300 Scripts (and this is bad)	(#2) **Merged-Mining is a Side-Hustle** (and those are always bad)
The free market allows entrepreneurs to go bankrupt – this is **an essential part of creativity**. True: not every SC will succeed. But those few that do, will pay fees to 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.

Future of Bip300 – Depends on You!

1. Learn !
   - Download the software
   - Read drivechain.info
2. Talk
   - Soft forks need consensus
   - Invite on podcasts/whatever
3. View Altcoins Differently



drivechain.info/releases/

Drivechain = Bip 300+301

Releases

Download Latest Version (v40)

Software	Linux	Windows	Mac	Source
Mainchain v40.01	tar.gz	.exe	dmg, tar.gz	Github
Testchain v14	tar.gz	.exe	n/a	Github
Trainchain v77	tar.gz	.exe	n/a	Github
Thunder v5	tar.gz	.exe	n/a	Github
zSide v5	tar.gz	n/a	n/a	GitLab

Click here for CHECKSUMs

Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

Thank You

for Your Attention!

(Find me and talk to me!)

Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin