Bip300: Getting to 100% ~~Bitcoin~~ Litecoin (?) Dominance (and Beyond)

Paul Sztorc

7.24.2024

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
- Plan to dethrone BTC (or just have some harmless fun)
- If you agree –
  - get 51% of hashrate to run the Activator client.
  - Plan out which sidechain to adopt (zCash clone)

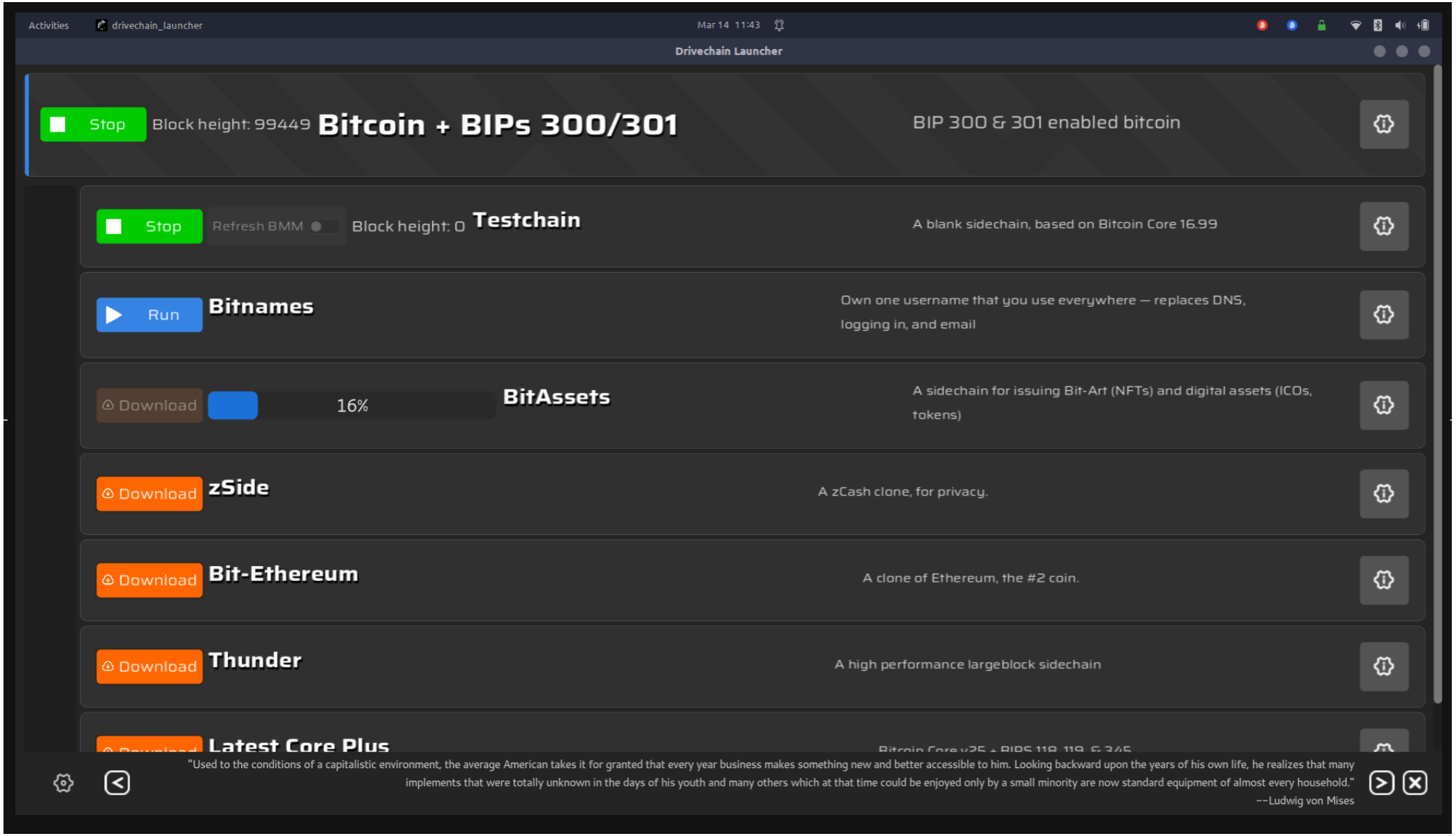
https://layertwolabs.com/download

Download Drivechain Launcher

Download for Linux

Download for Windows

Download for Mac



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

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

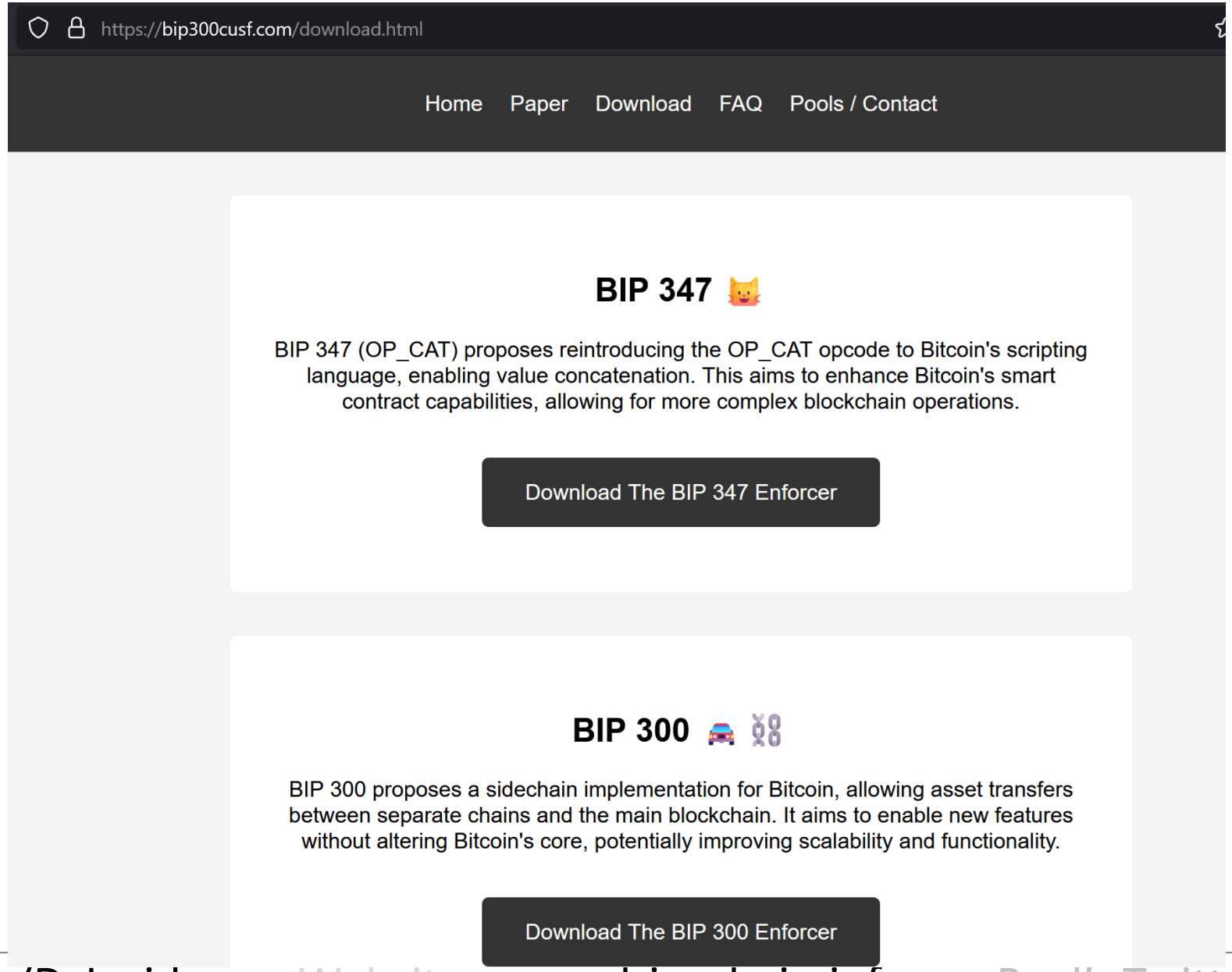
Once on a sidechain, coins can change hands an unlimited number of times, and in an unlimited number of *new ways*. Thus, BTC-owners can opt-in to new features or tradeoffs. Meanwhile, the Bitcoiners who don't opt-in, never need to care what any

LINKS

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

Truthcoin.Info

Bitcoin Hivemind

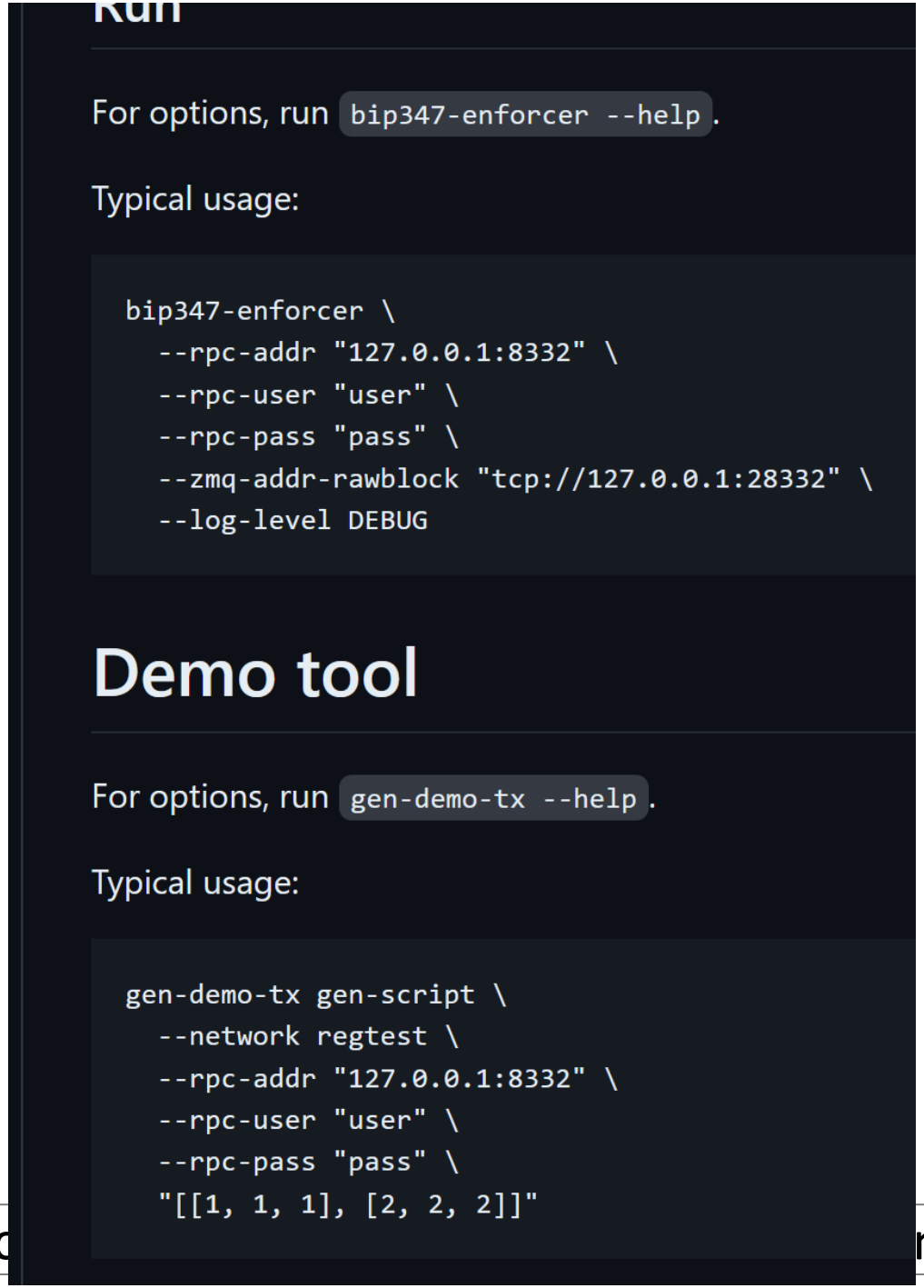

https://bip300cusf.com/download.html
Home
Paper
Download
FAQ
Pools / Contact
BIP 347
BIP 347 (OP_CAT) proposes reintroducing the OP_CAT opcode to Bitcoin's scripting language, enabling value concatenation. This aims to enhance Bitcoin's smart contract capabilities, allowing for more complex blockchain 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

If Litecoin can do this, then you can use the activator TODAY

(no modification to the Litecoin code)

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:

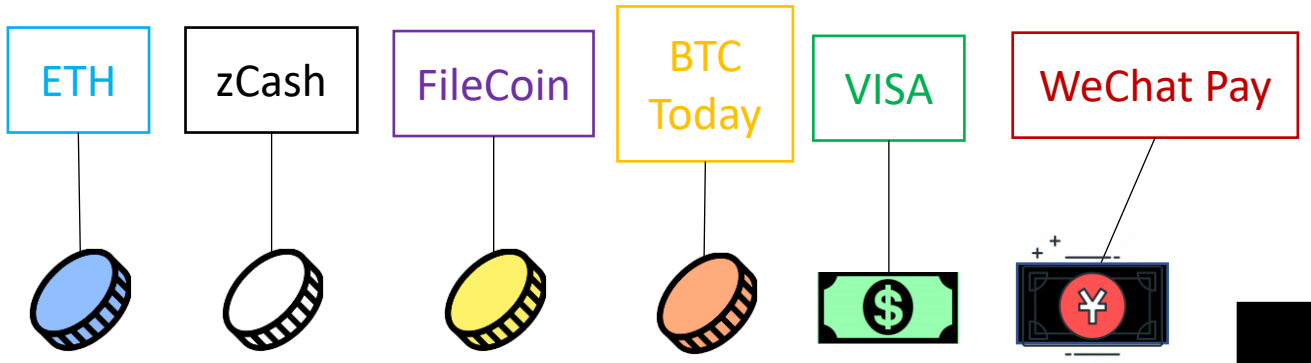
```
gen-demo-tx gen-script \
  --network regtest \
  --rpc-addr "127.0.0.1:8332" \
  --rpc-user "user" \
  --rpc-pass "pass" \
  "[[1, 1, 1], [2, 2, 2]]"
```

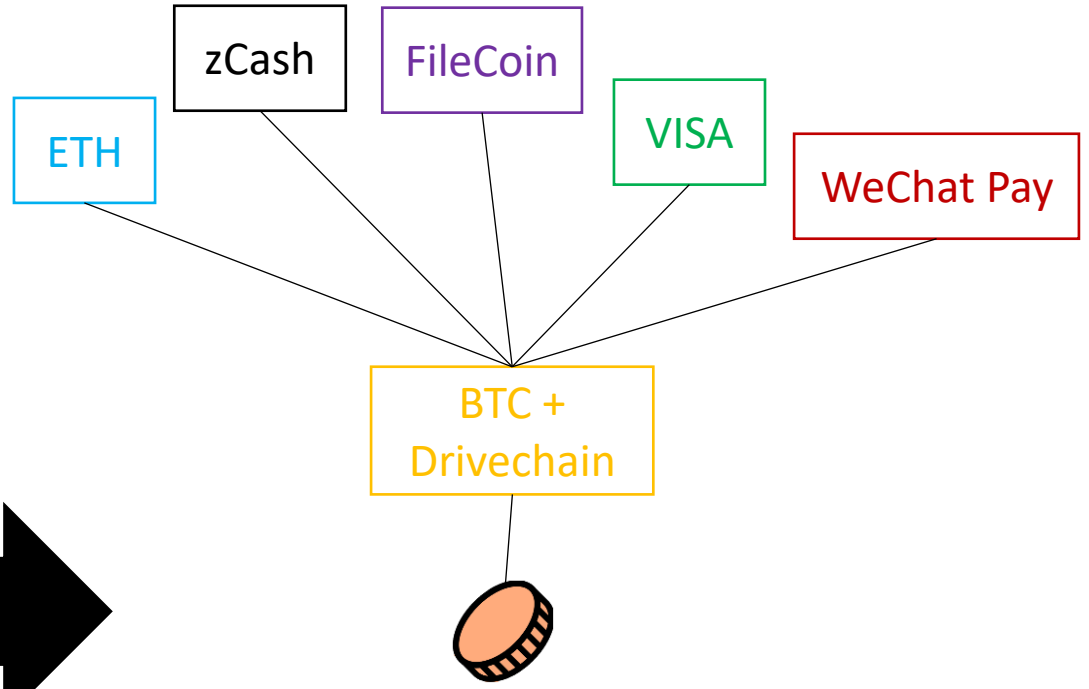
Bip300: Getting to 100% ~~Bitcoin~~ Litecoin (?) Dominance (and Beyond)

Paul Sztorc

7.24.2024

BIP300: Everything on Top of Bitcoin

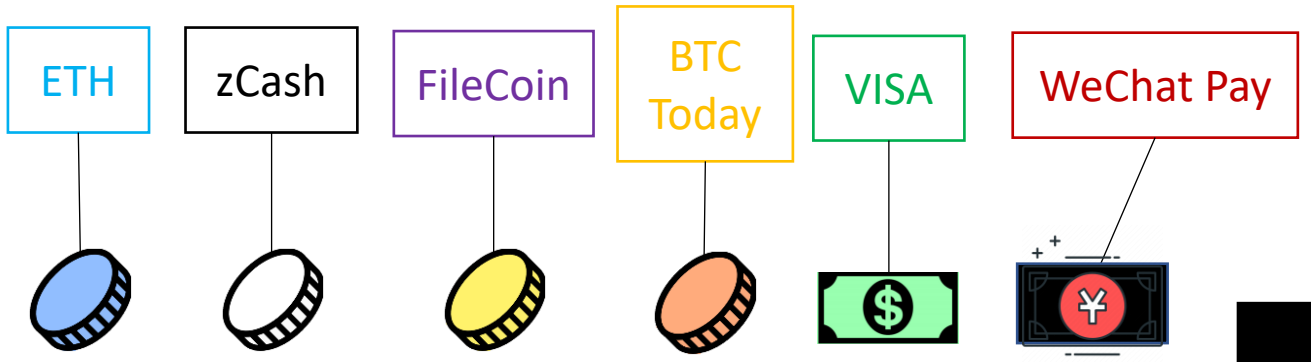




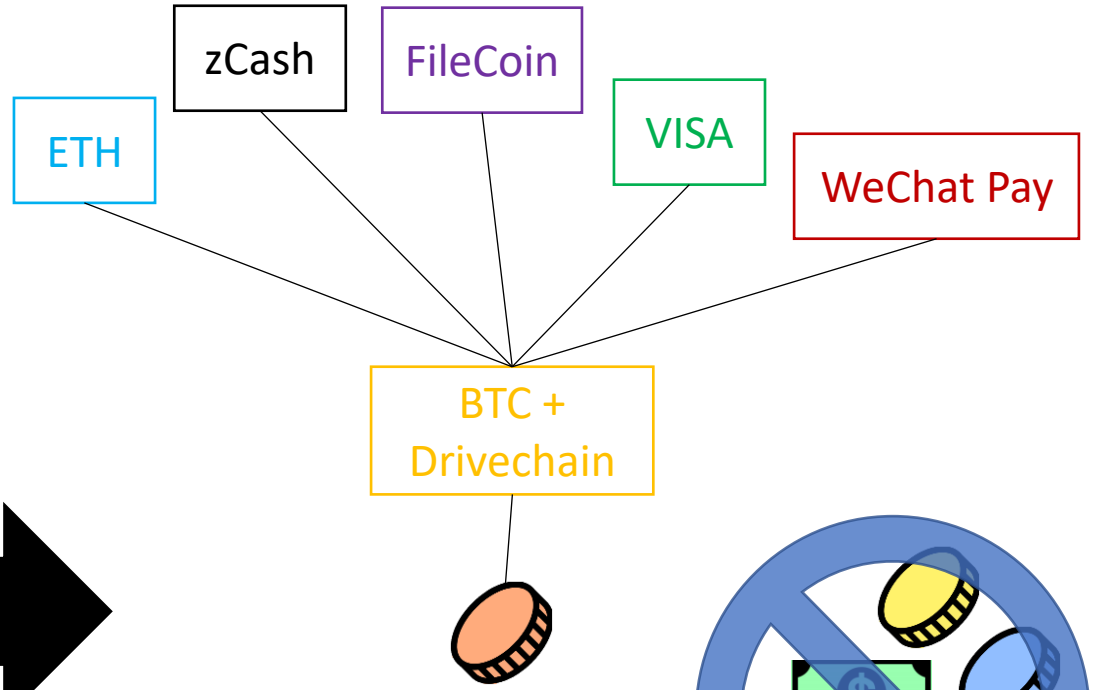
Today ☹

Tomorrow ☺

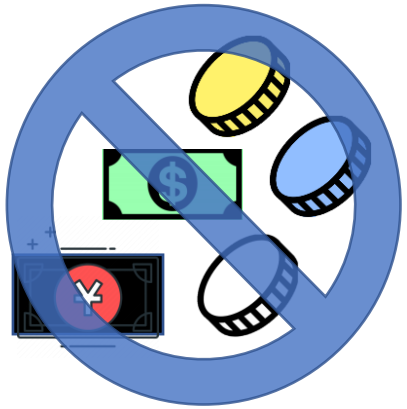
BIP300: Everything on Top of Bitcoin



Today ☹



Tomorrow ☺



The Coming Death of Bitcoin's Competitors

BTC
Today

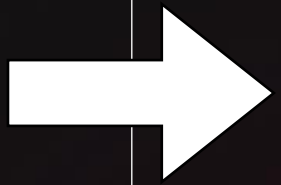
WeChat Pay

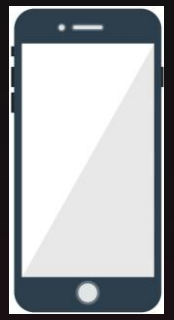
VISA

zCash

ETH

FileCoin

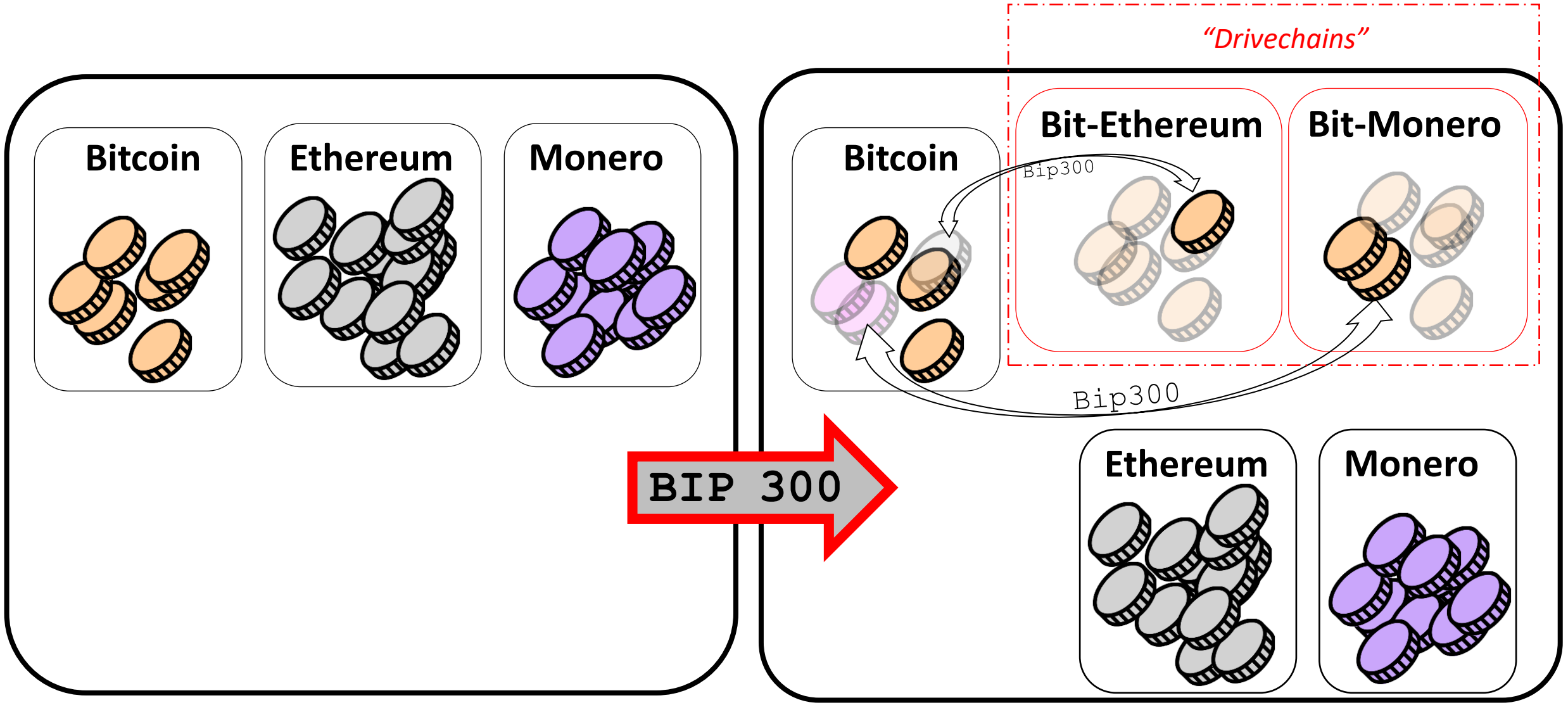




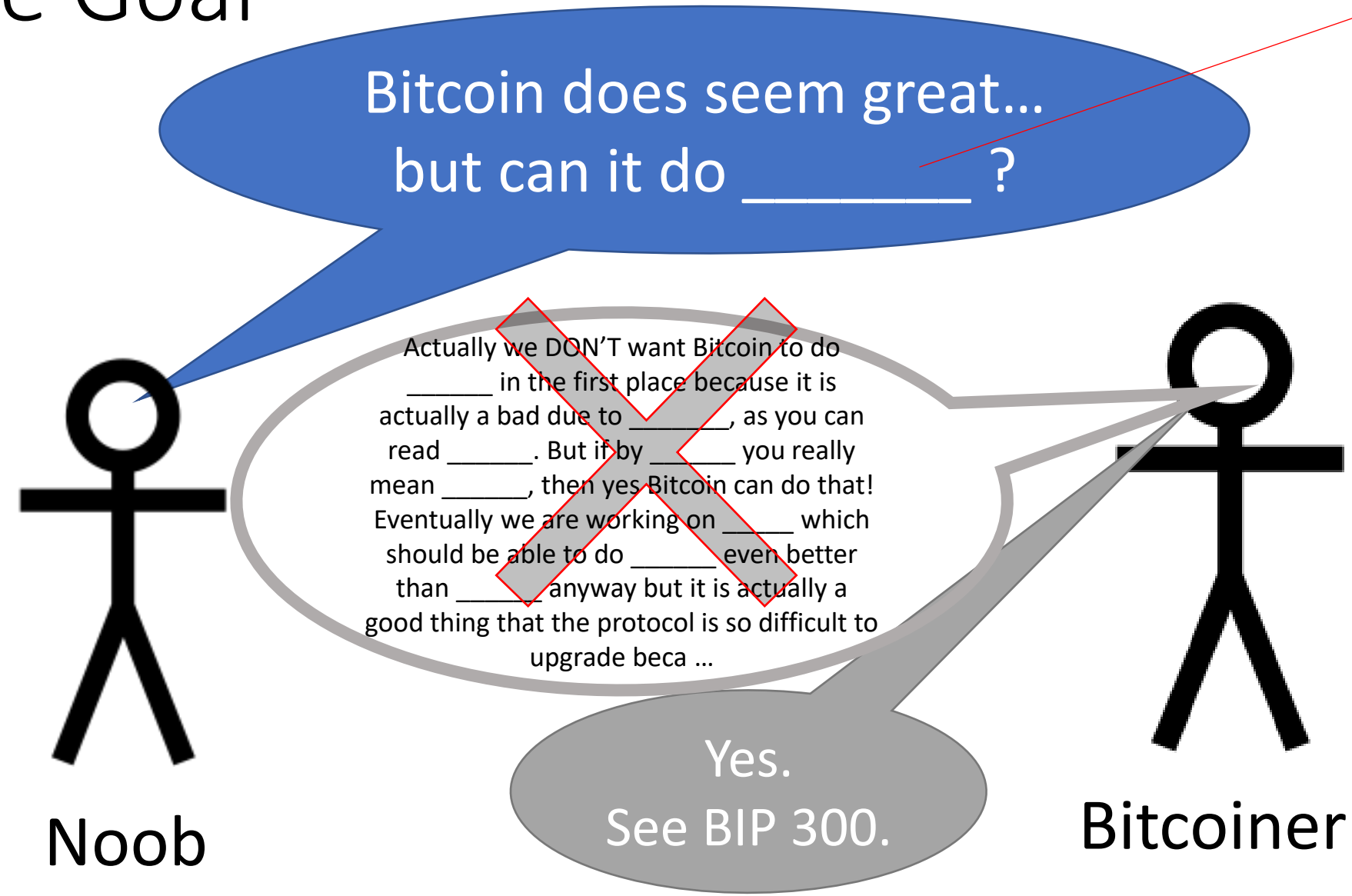
BTC +
Drivechain

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

Drivechain = Altcoin Tech, BTC Coin Only

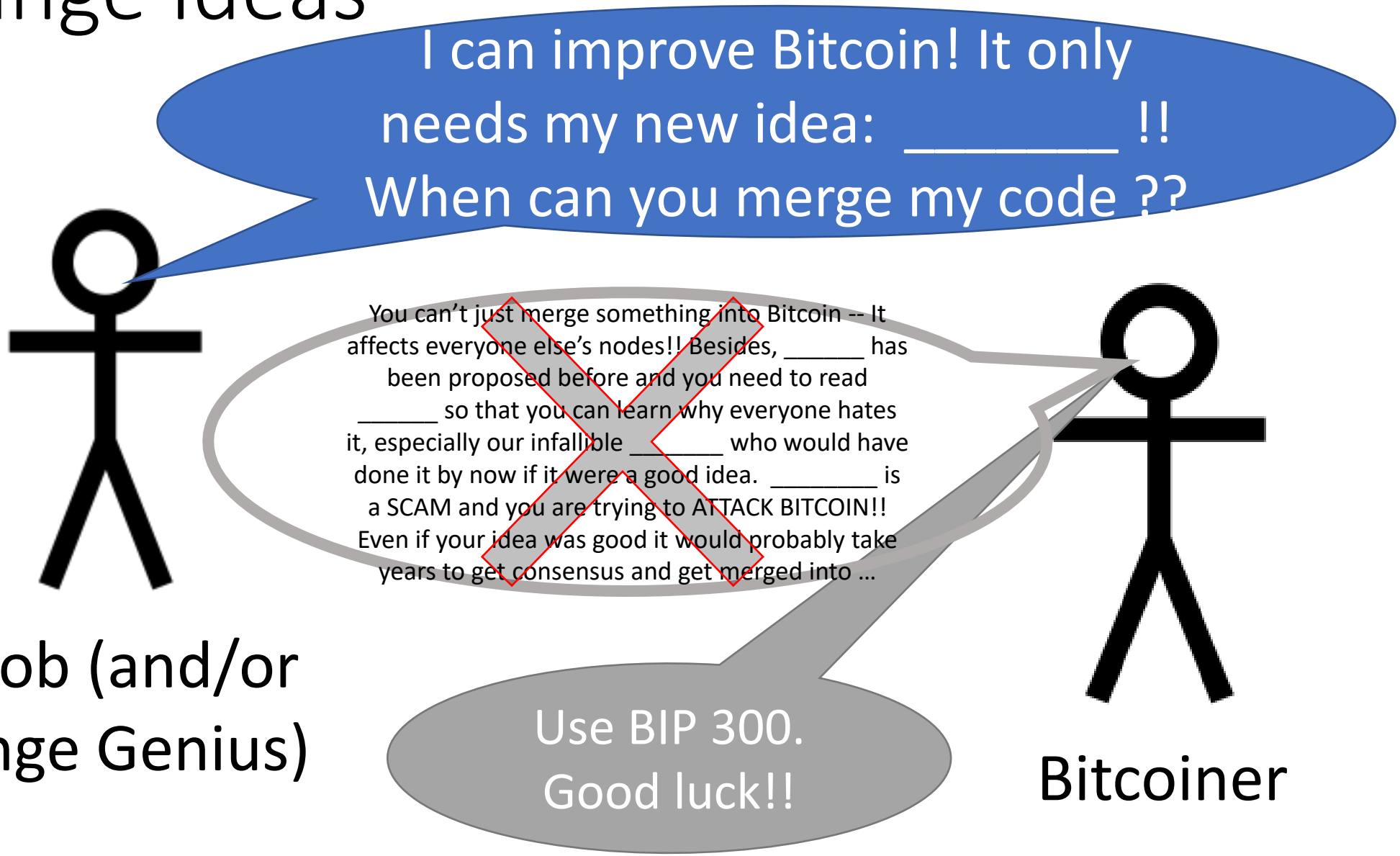


The Goal



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

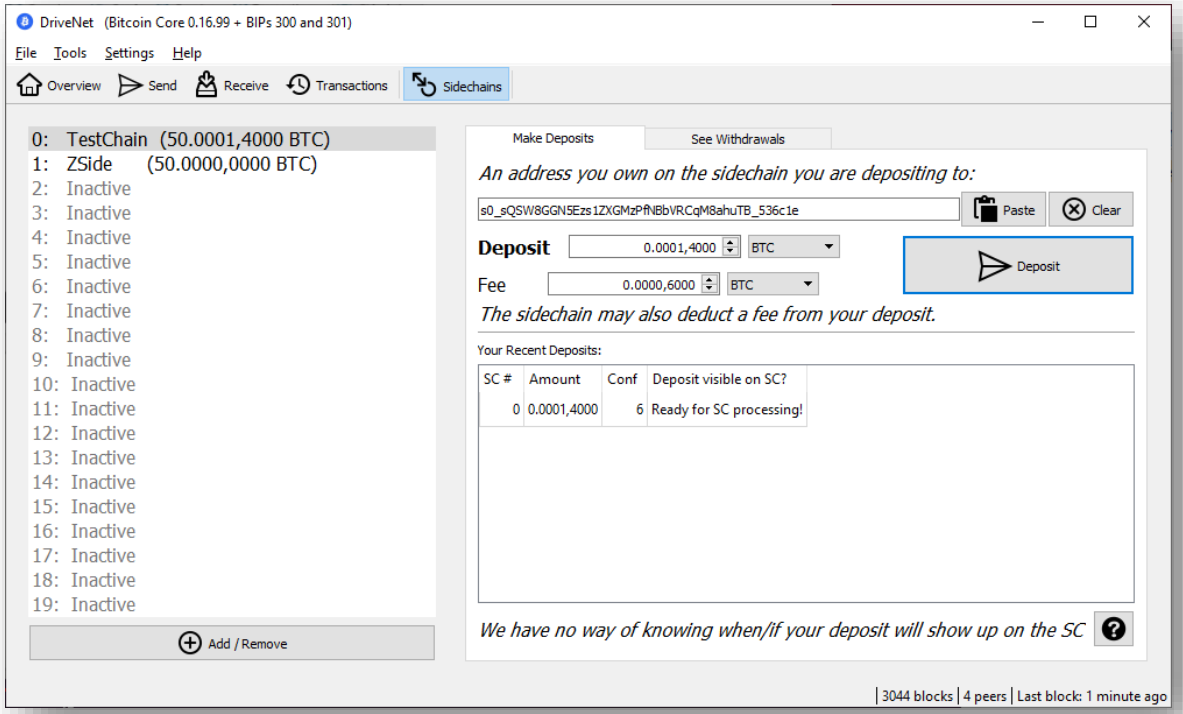
Fringe Ideas



Three Aspects

1. Full Autonomy
2. Protect Base Layer
3. Improve Miner Incentives

Not Vaporware



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

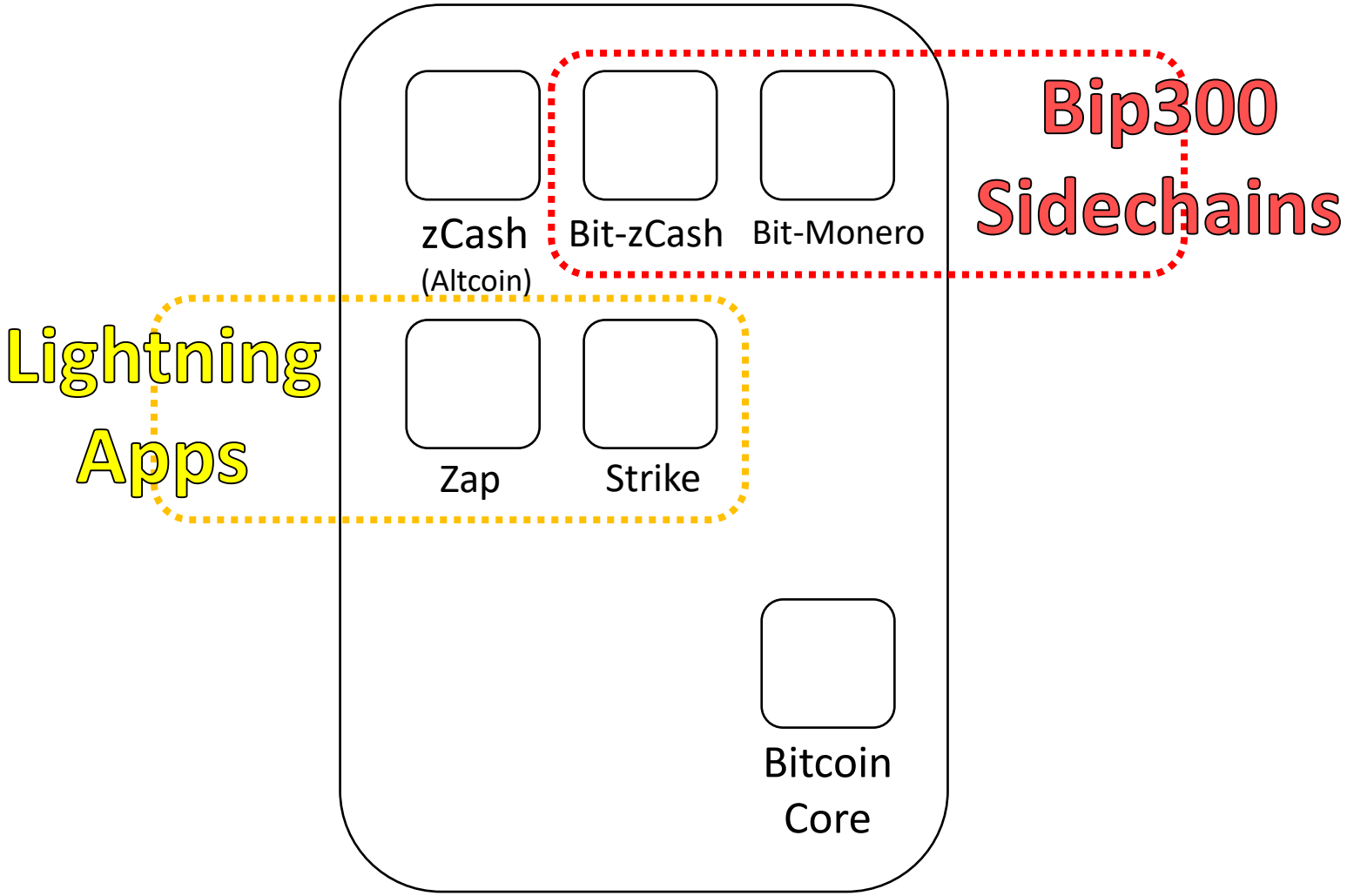
YouTube

Bitcoin-ZCash Sidechain (Regtest Demo)

489 views • Mar 1, 2021

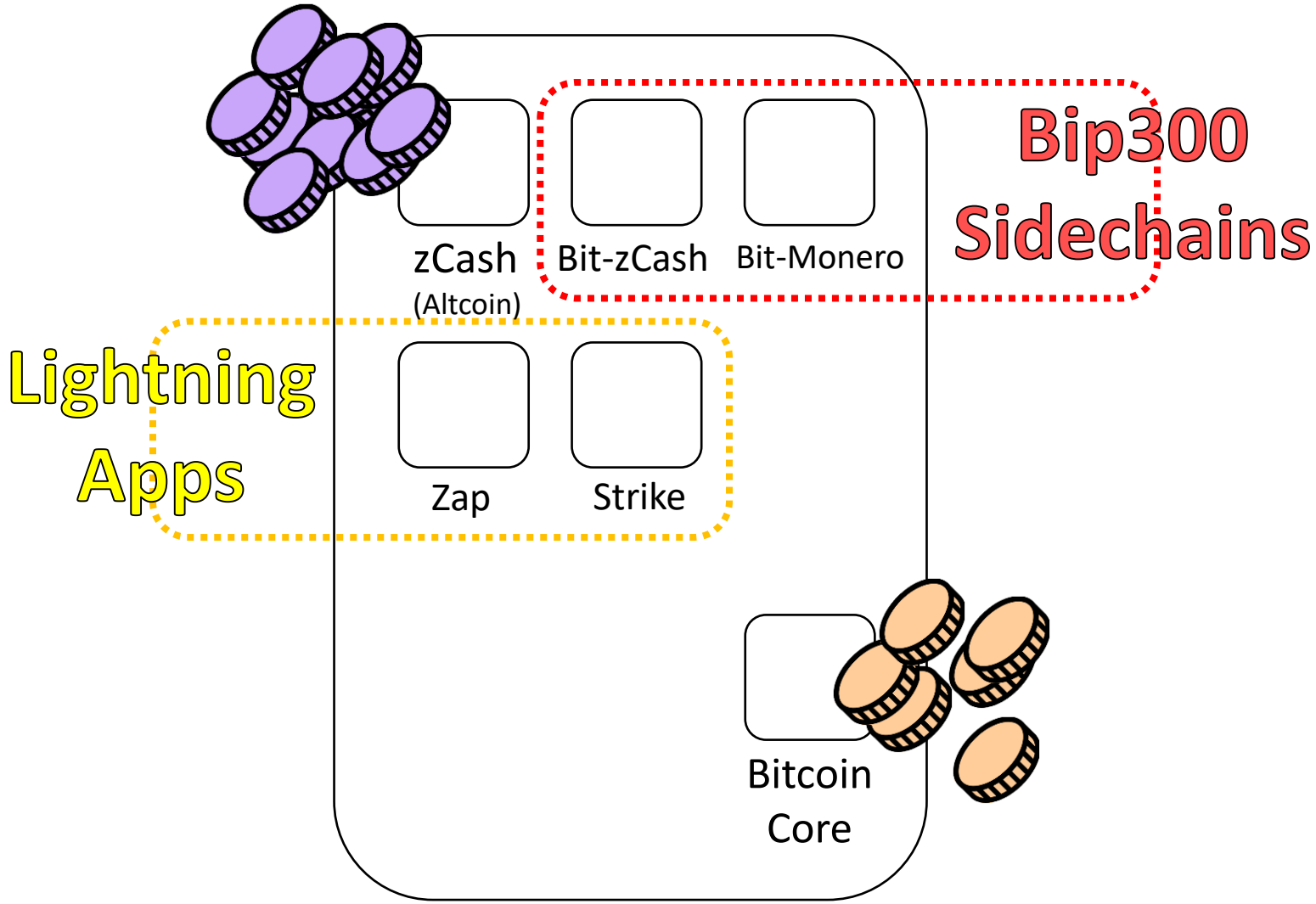
(#1) Full Autonomy

Metaphor



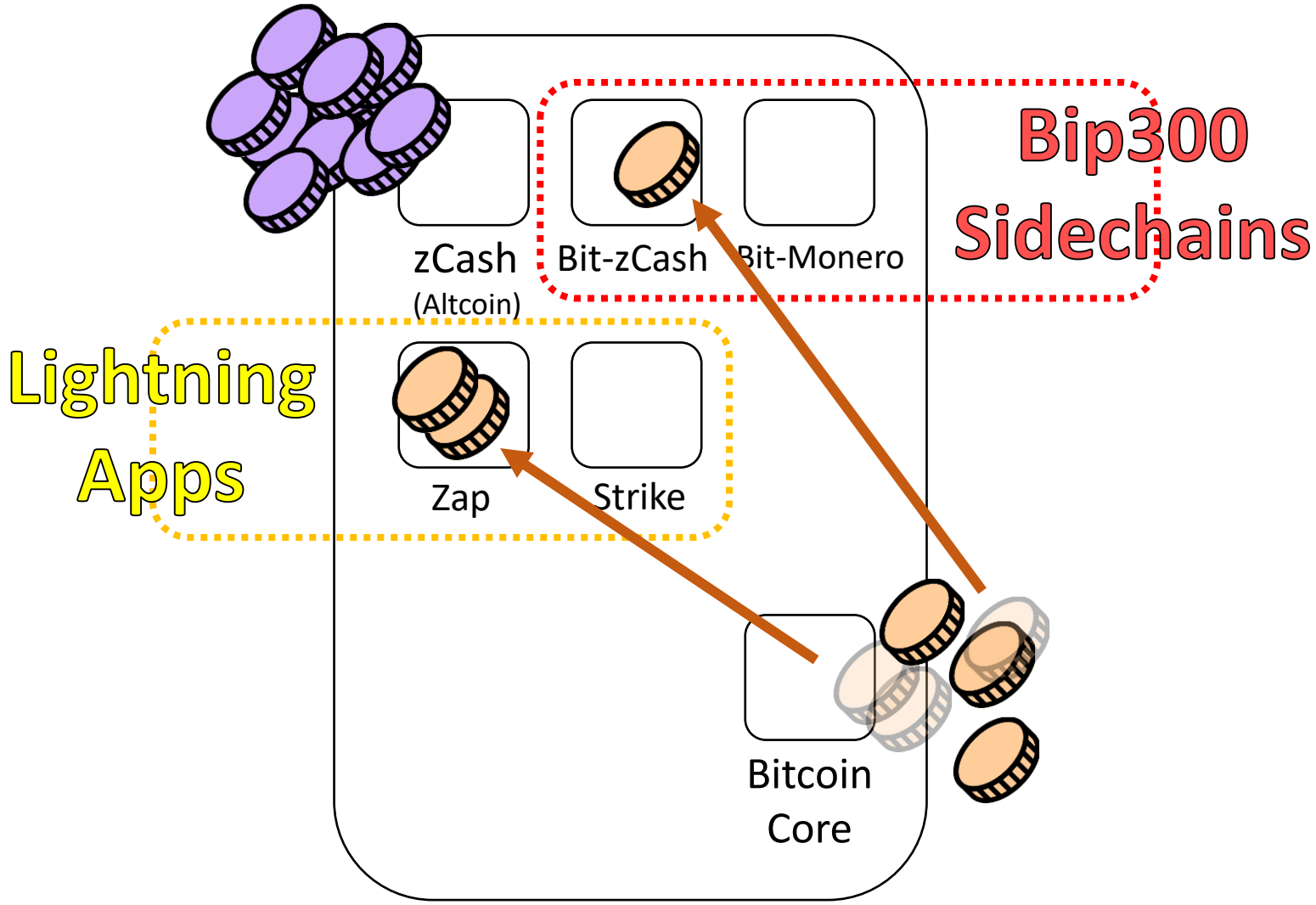
(#1) Full Autonomy

Metaphor

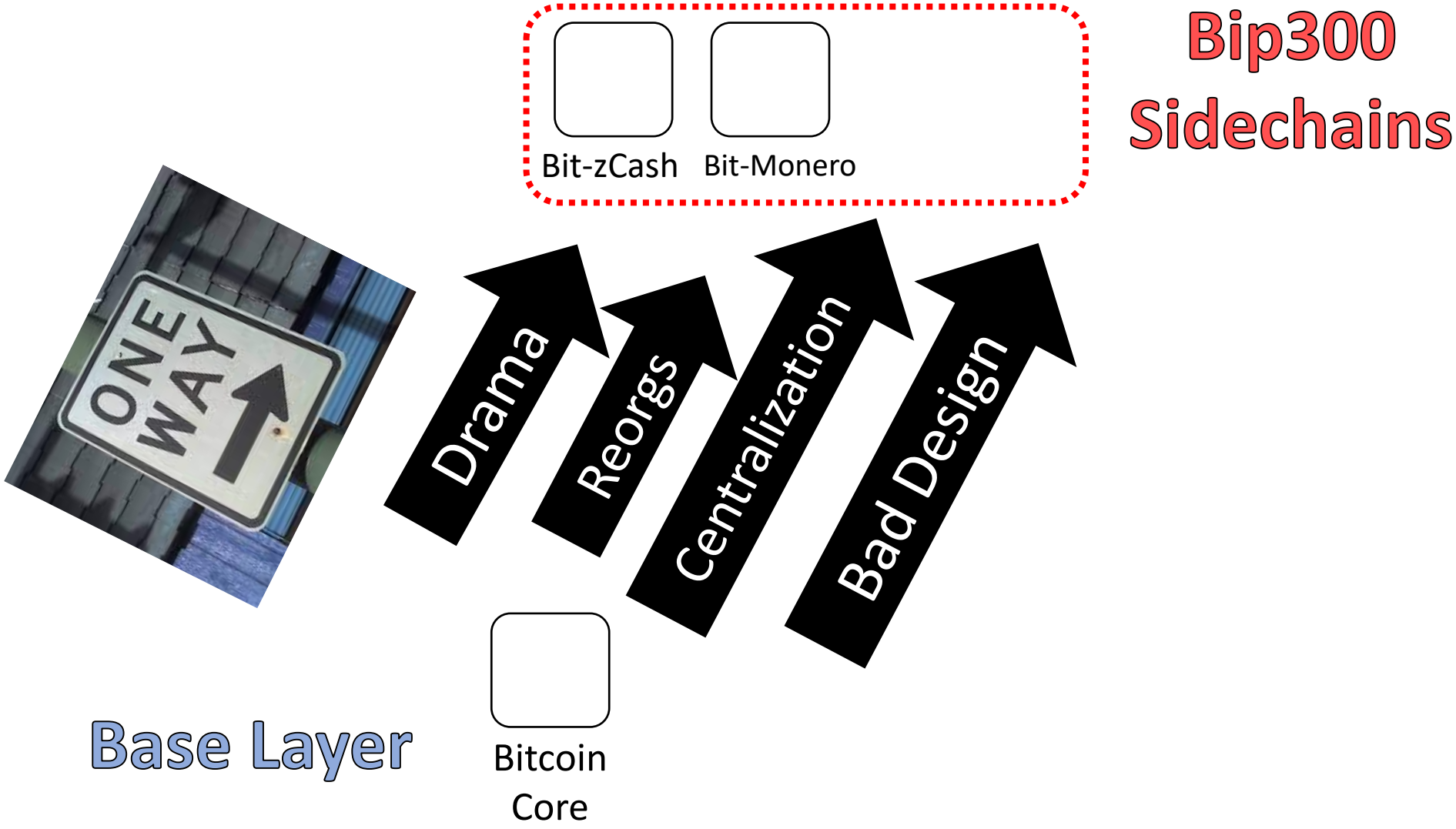


(#1) Full Autonomy

Metaphor



(#2) Base Layer is Safe



(#2) Base Layer is Safe

= Block Header

= List of transactions

December 2020 January 2021 February 2021 March 2021 April 2021

Base Layer (Bitcoin Core)

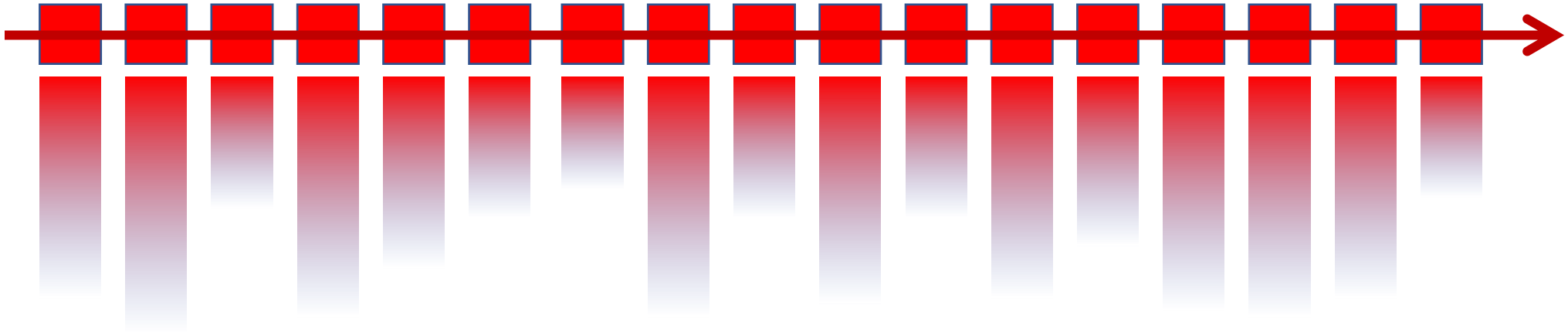
(#2) Base Layer is Safe

= 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

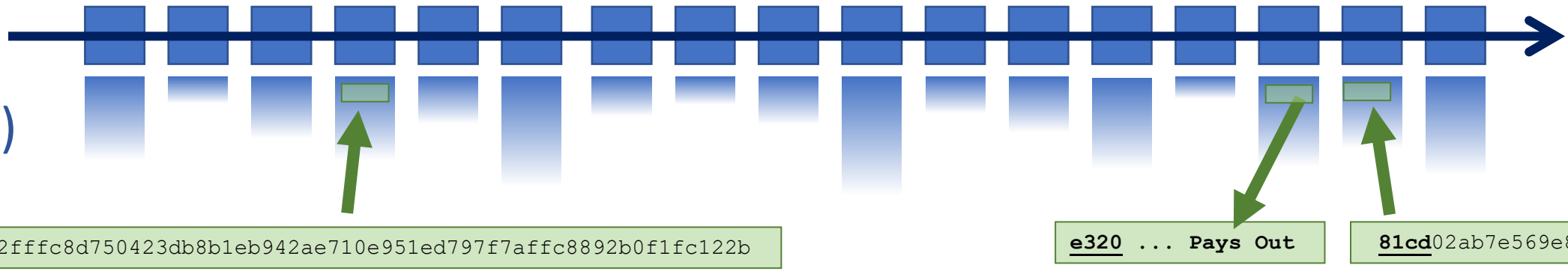
Base Layer
(Bitcoin Core)

e320 ... Pays Out

(#2) Base Layer is Safe

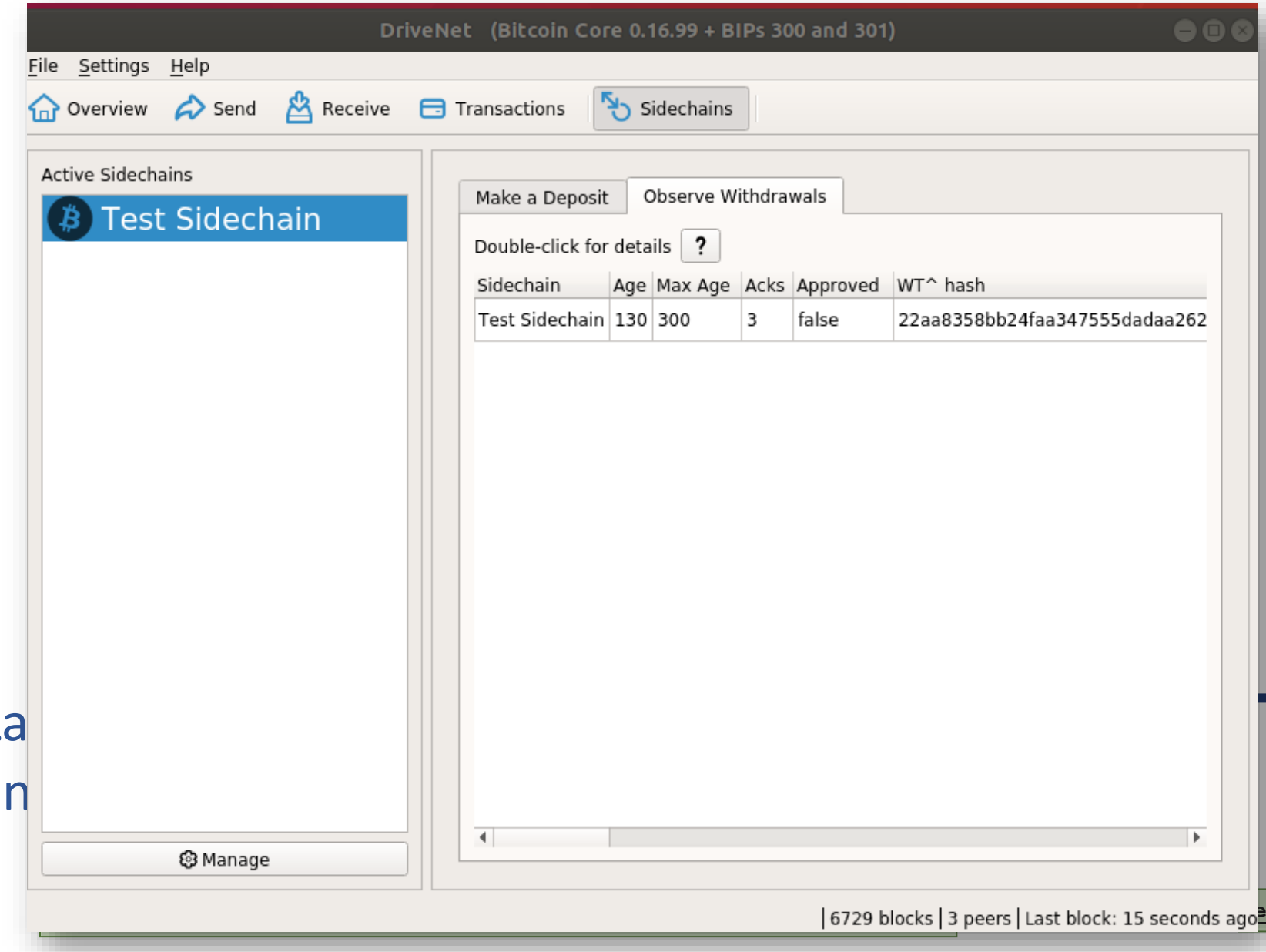
Your Layer 1 Node Sees…

Base Layer
(Bitcoin Core)

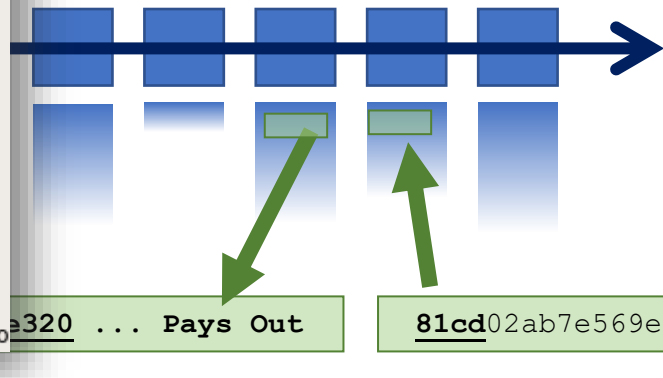


(#2) Base Layer is Safe

Your Layer 1 Node Sees…



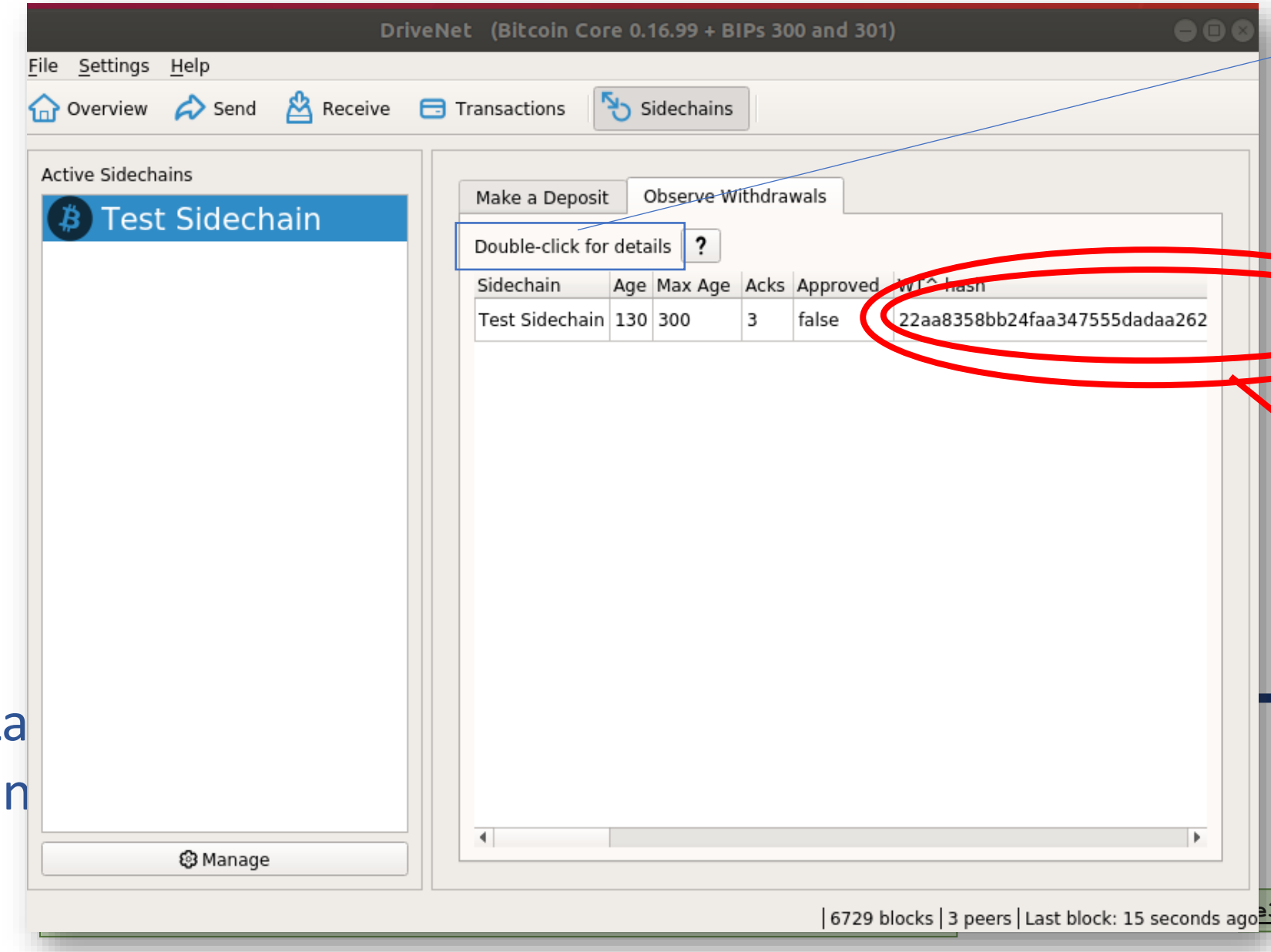
Base La
(Bitcoin



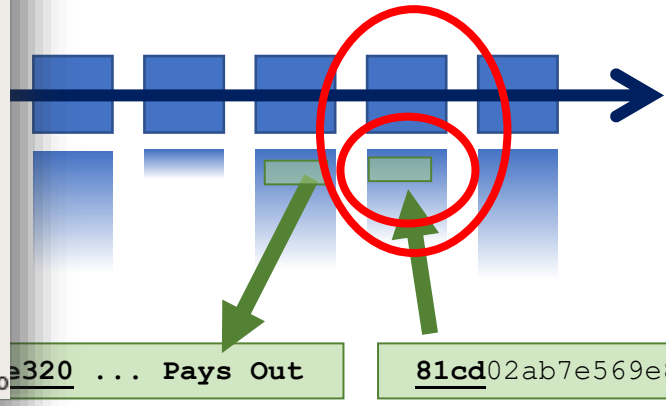
(#2) Base Layer is Safe

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

(#3) Improve Mining Incentives (Bip 301)

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

Upon finding a sidechain block worth $2000...

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

Security Budget in the Long Run

14 Feb 2019 https://www.truthcoin.info/blog/security-budget/

Security Budget II, Low Fees, and Merged Mining

15 Oct 2021 https://www.truthcoin.info/blog/security-budget-ii-mm/

(#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	$13,051.22	$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 ca

Outline

- Title / Summary (2)
- Bip300 -- Goal, Three Aspects (16)
- Outline (1) -- *YOU ARE HERE*
- Altcoins We Should Copy (15)
- The Supposed "Drawbacks" of Bip300 (2)
- Ending (1)

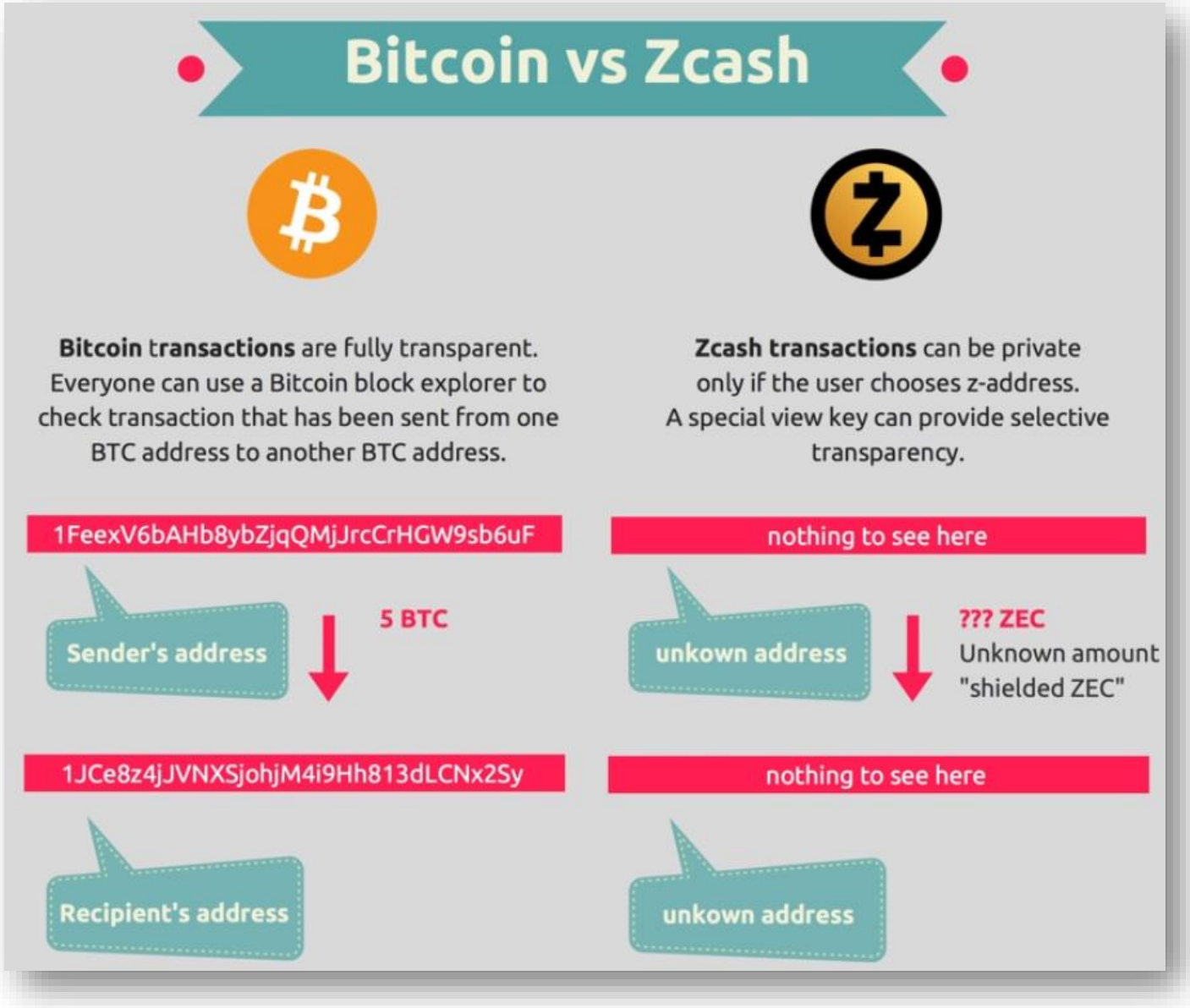
What do we use BIP 300 for…?

(In other words: Which altcoins are worth copying?)

Art: “When I paint my masterpiece” – Nick Kenrick (?) - Creative commons license

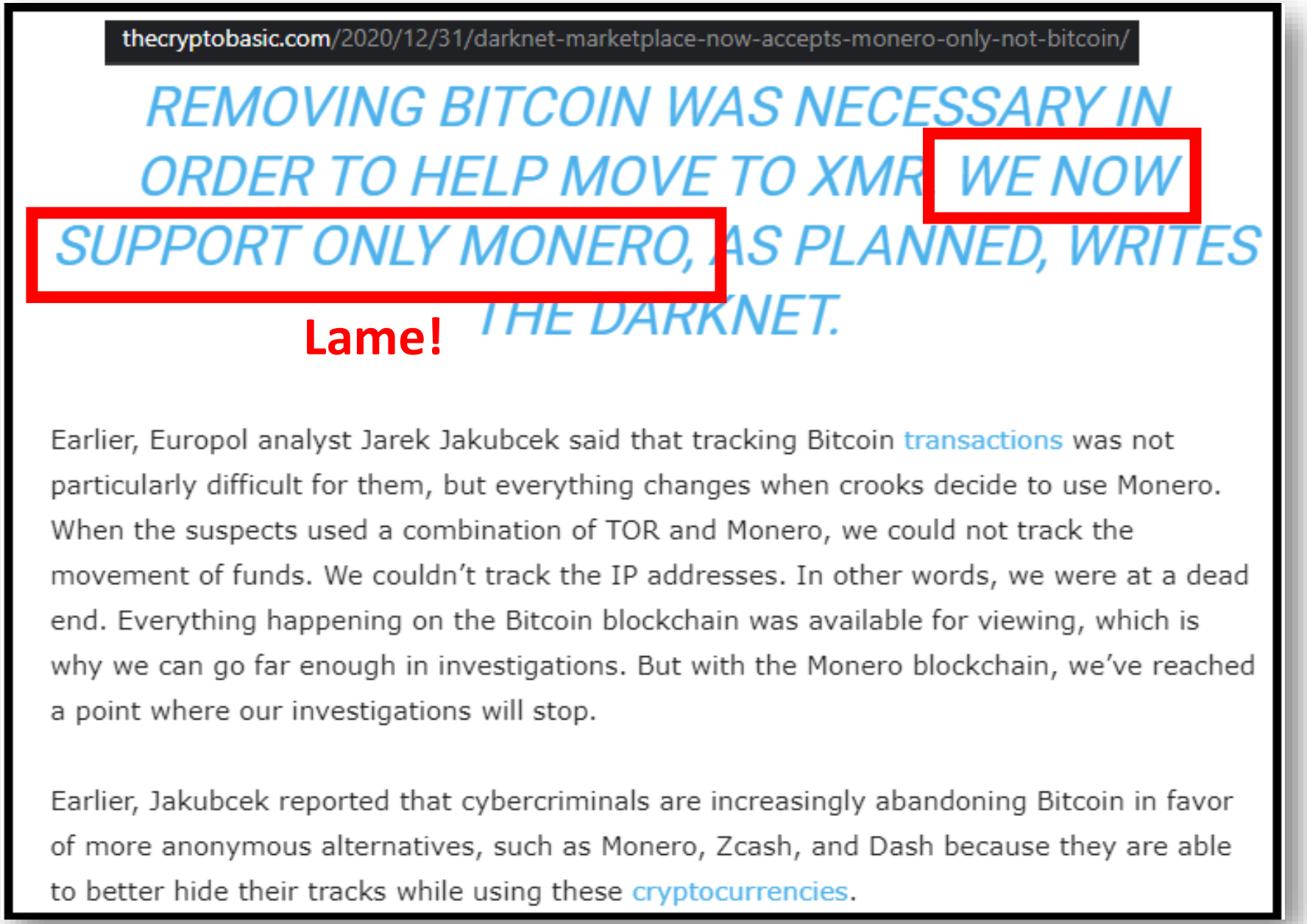
Altcoins we should copy (?): zCash

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

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

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:

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) ?

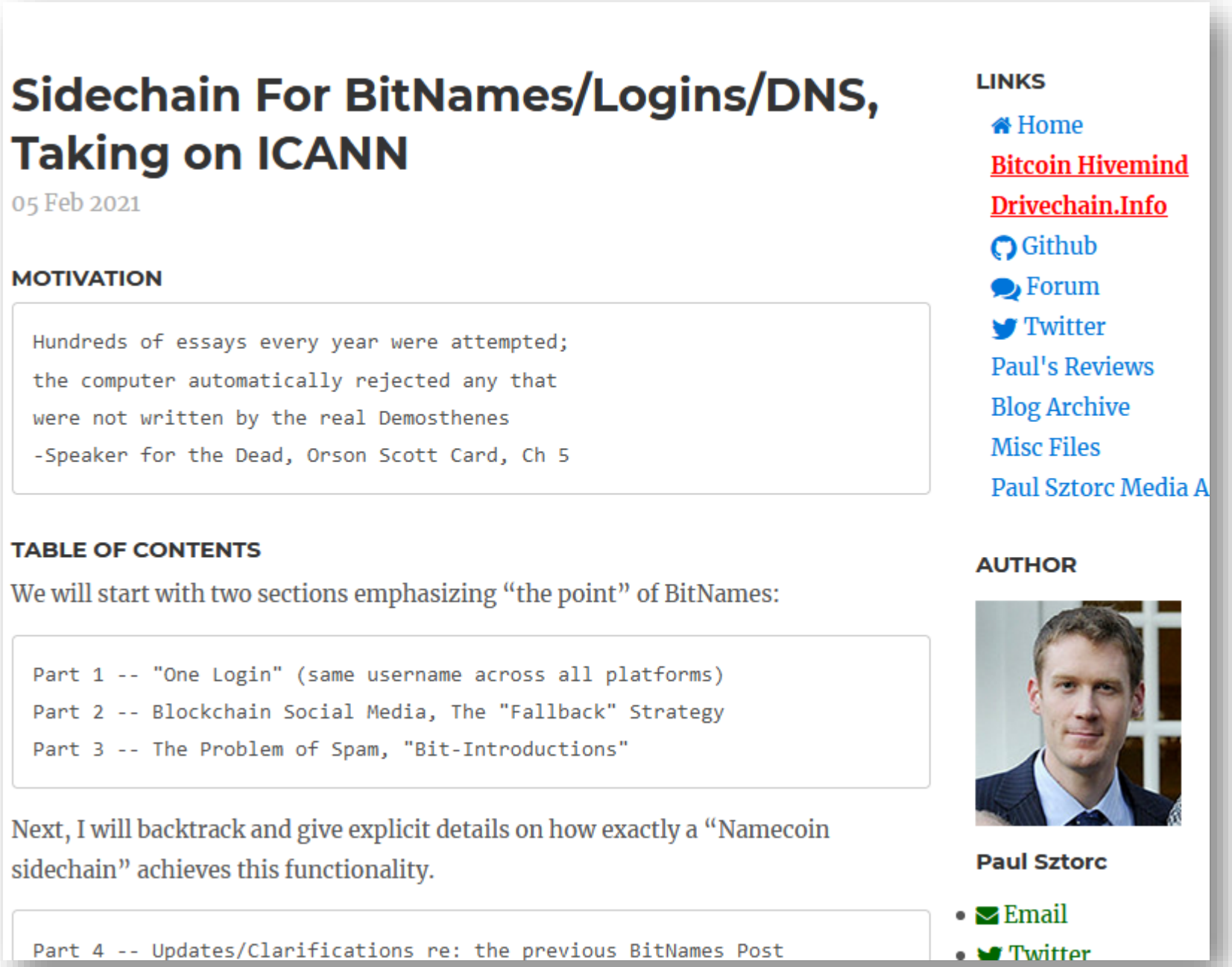
The incentive is to get the rewards from the extr side chains also fo

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

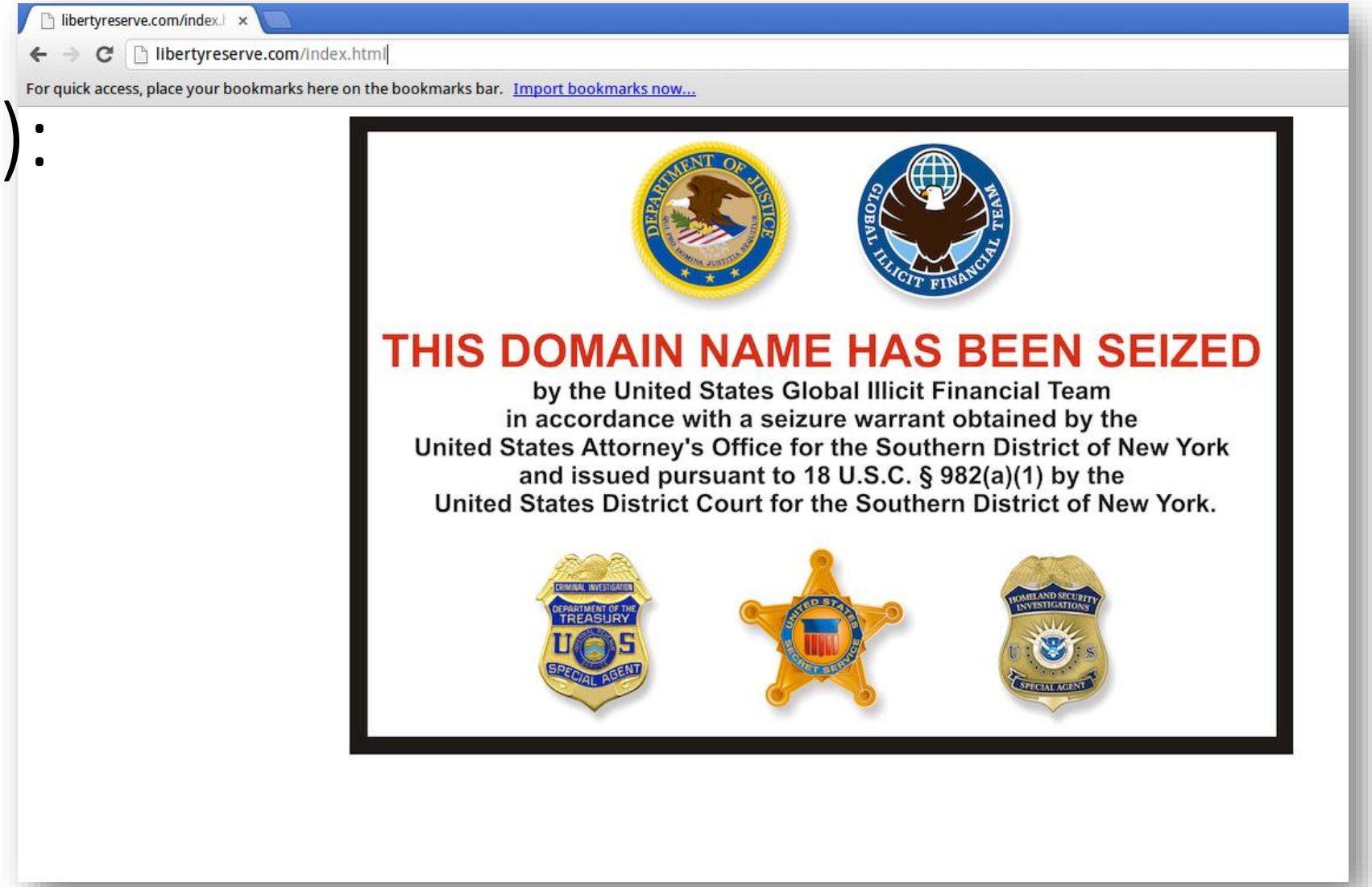
Screenshot #1 from

www.truthcoin.info/blog/bitnames/

Altcoins we should copy (?): NameCoin

Screenshot #2 from

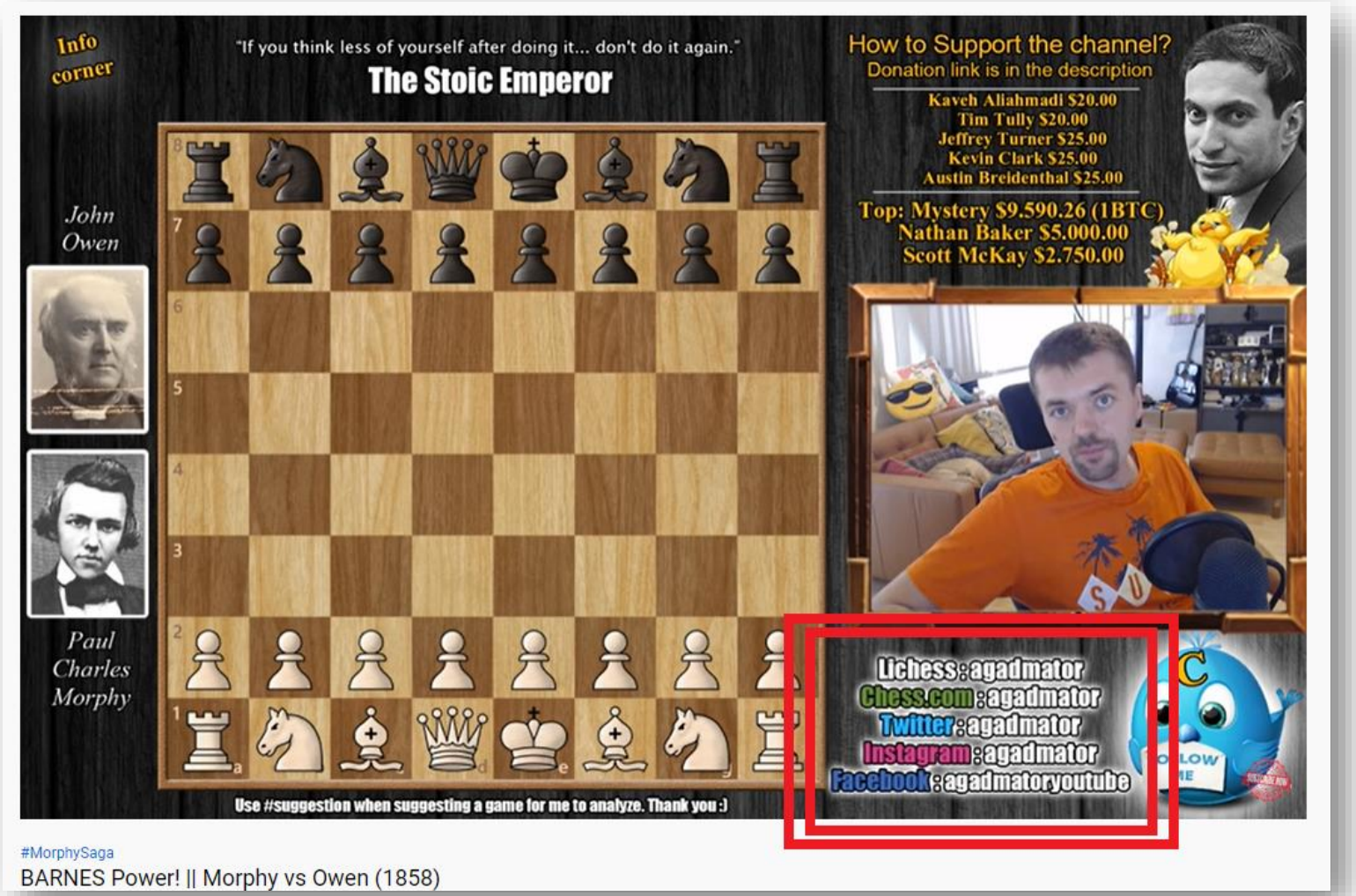
www.truthcoin.info/blog/bitnames/



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]

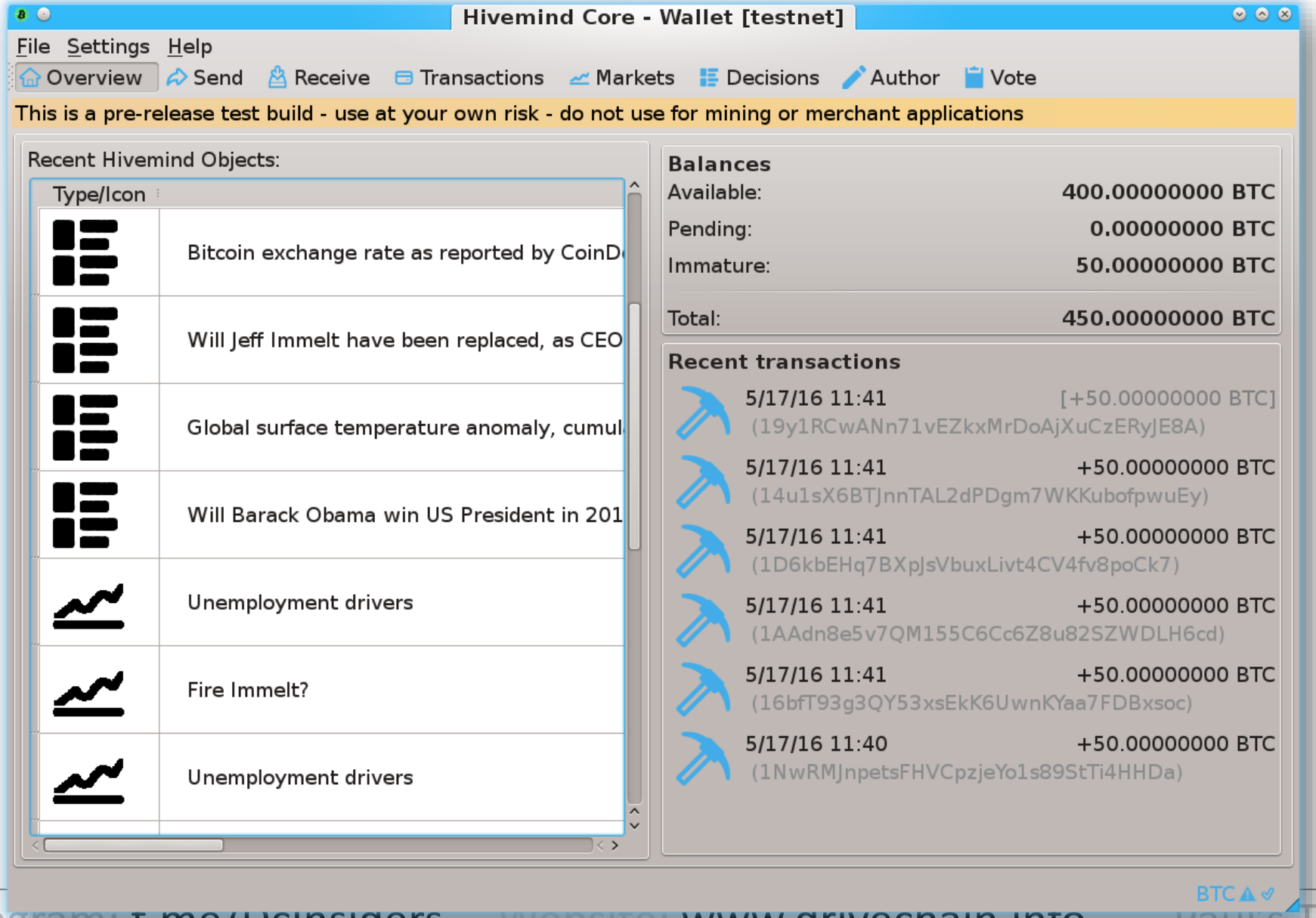
1 Description

Logo used to represent fungible tokens

Prediction Markets

- Screenshots from my own BTC sidechain project

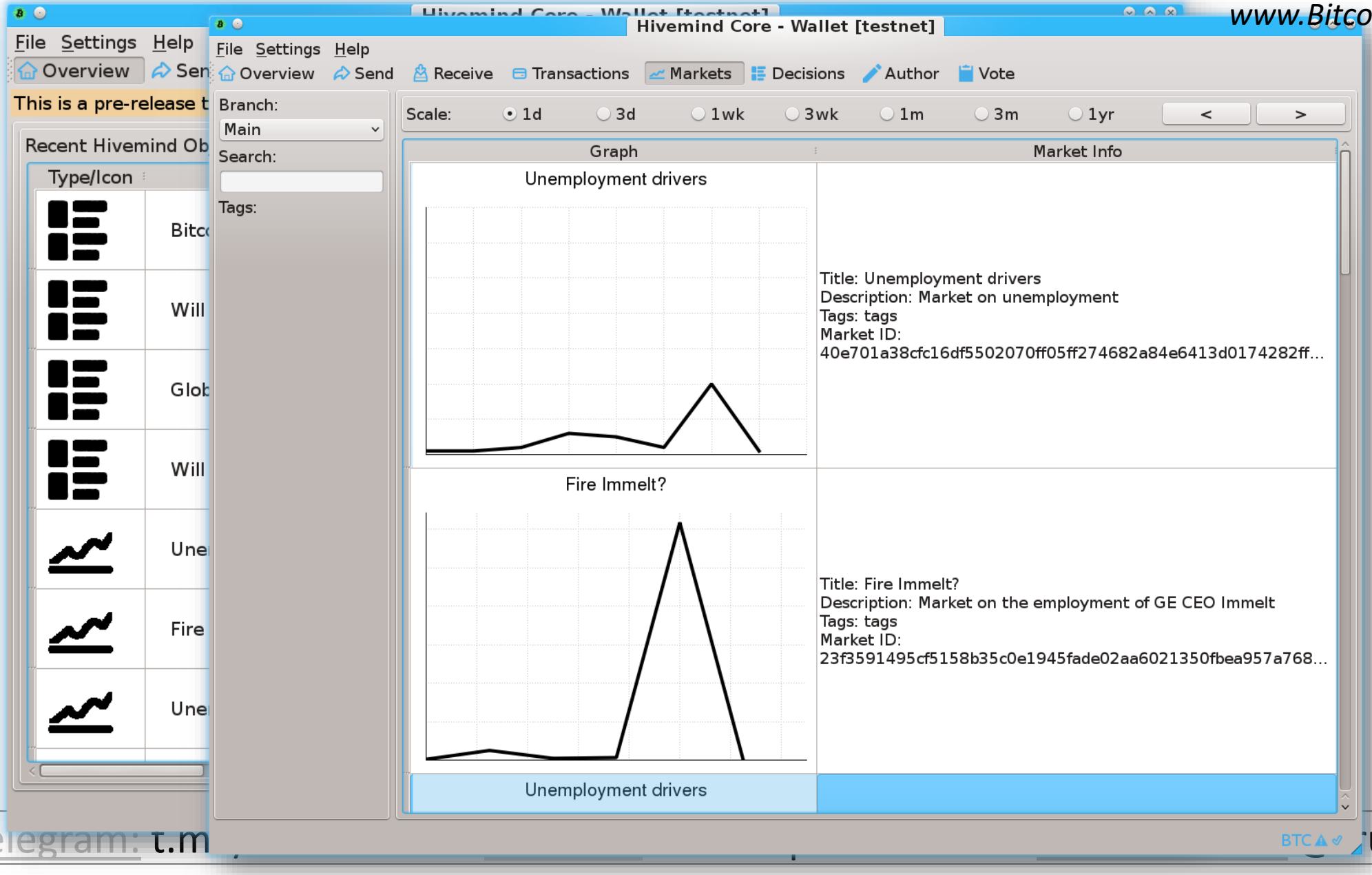
www.BitcoinHivemind.com



Prediction Markets

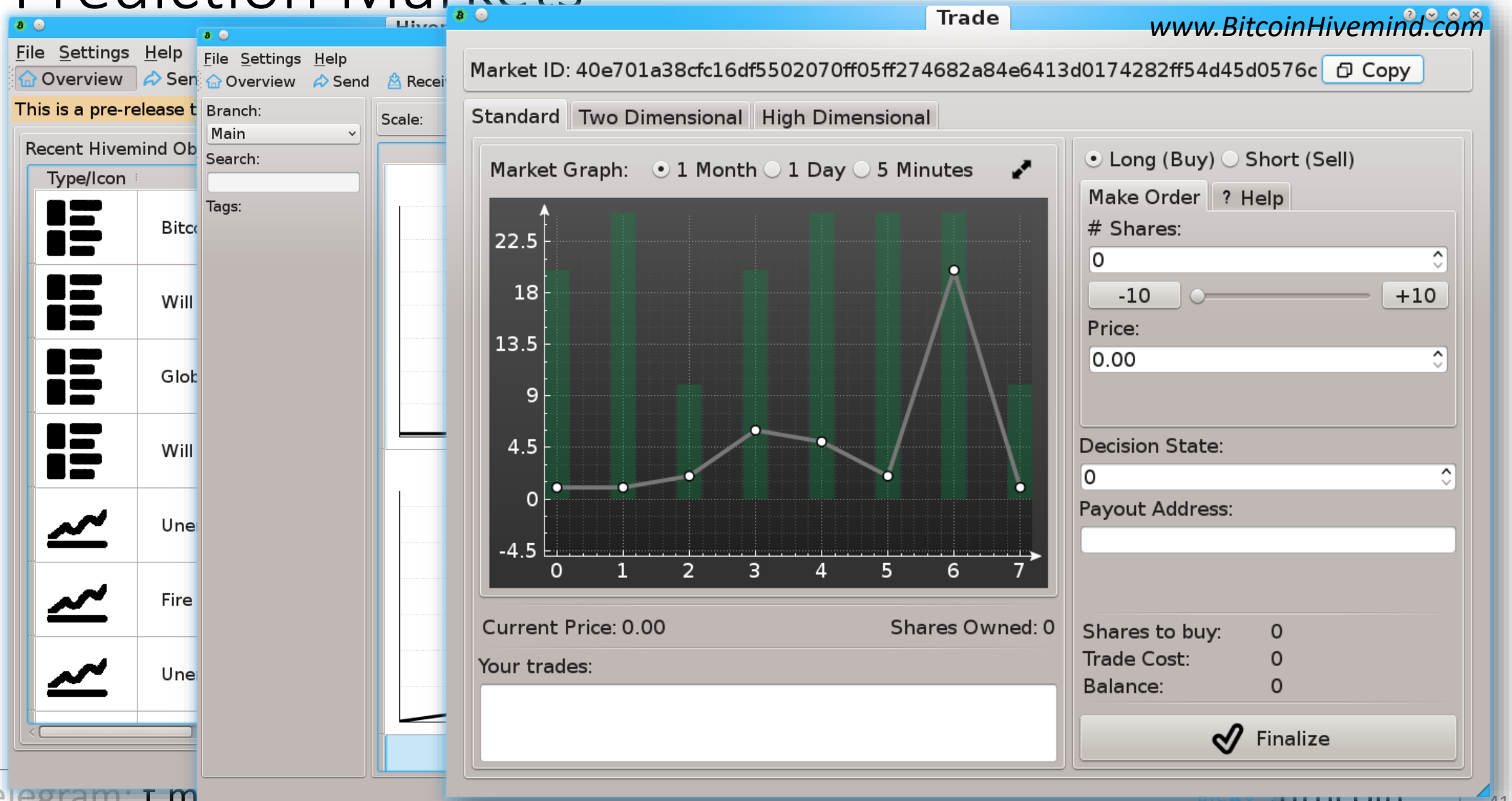
- Screenshots from my own BTC sidechain project

www.BitcoinHivemind.com



Prediction Markets

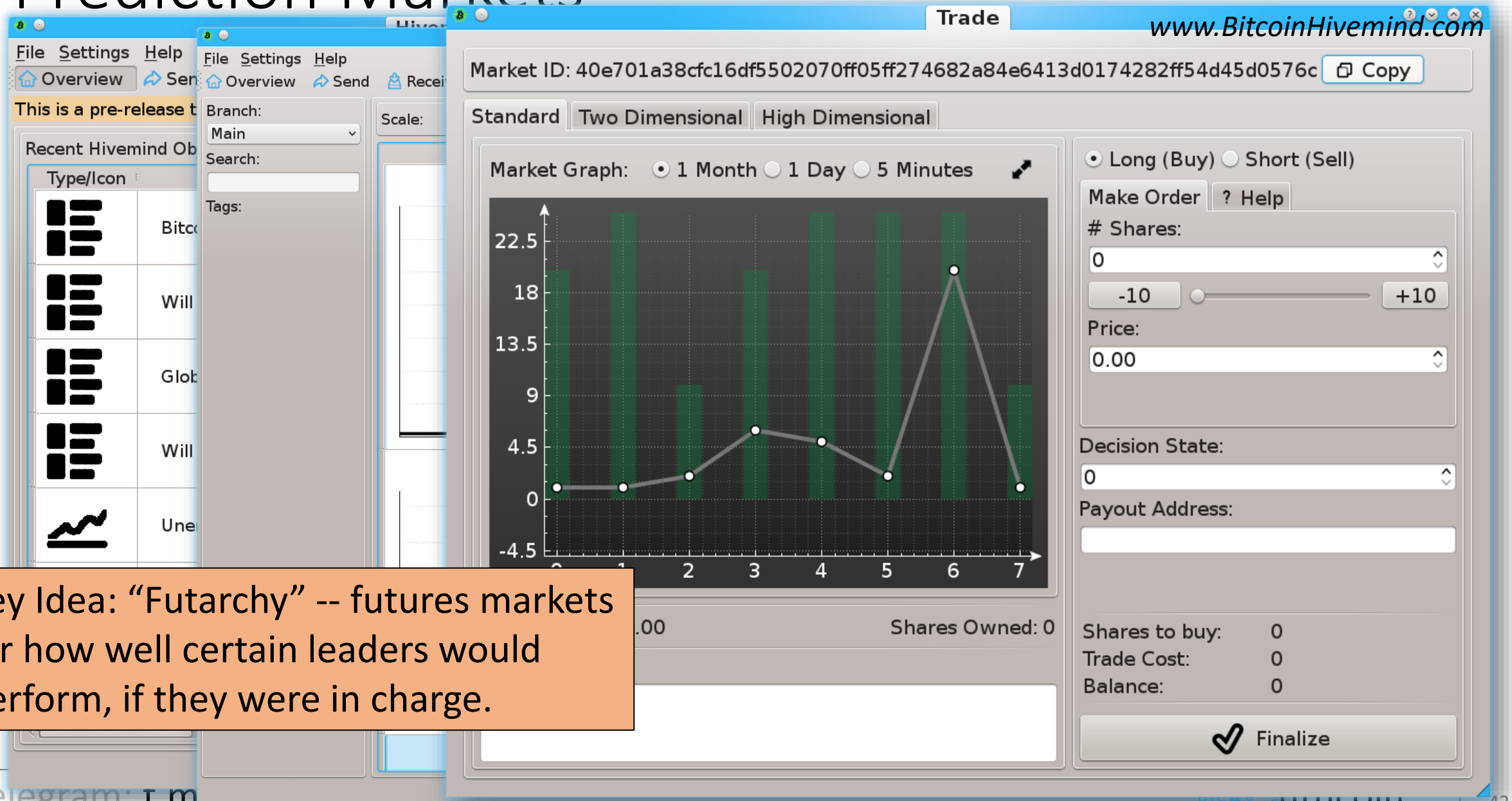
- Screenshots from my own BTC sidechain project



Telegram: t.m

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

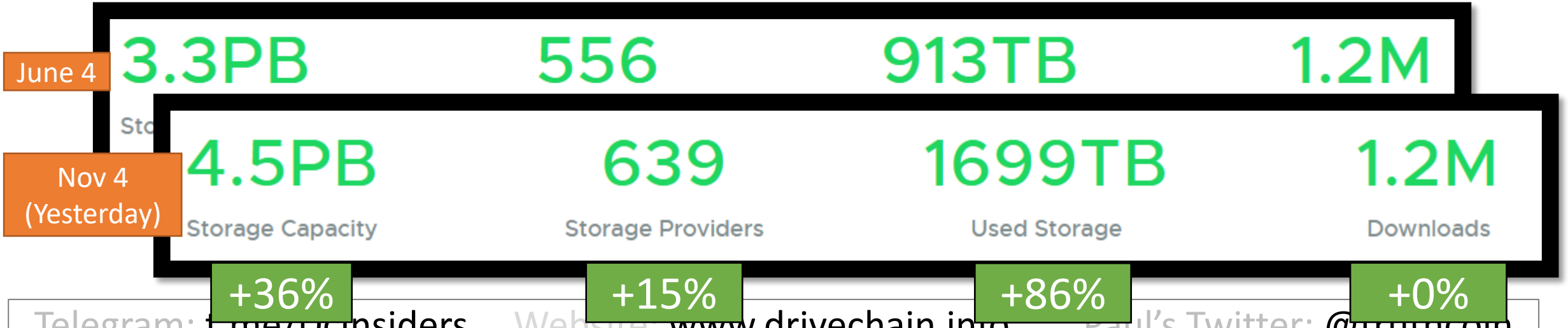
June 4

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)

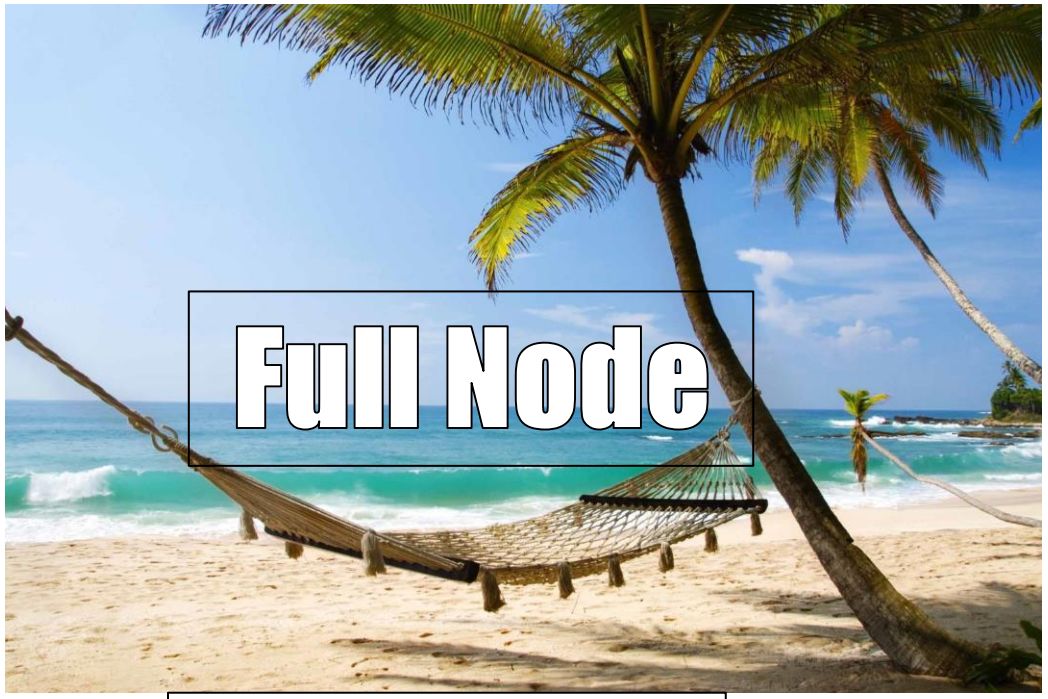
https://sia.tech



Finally: How Bip300 Improves Layer1

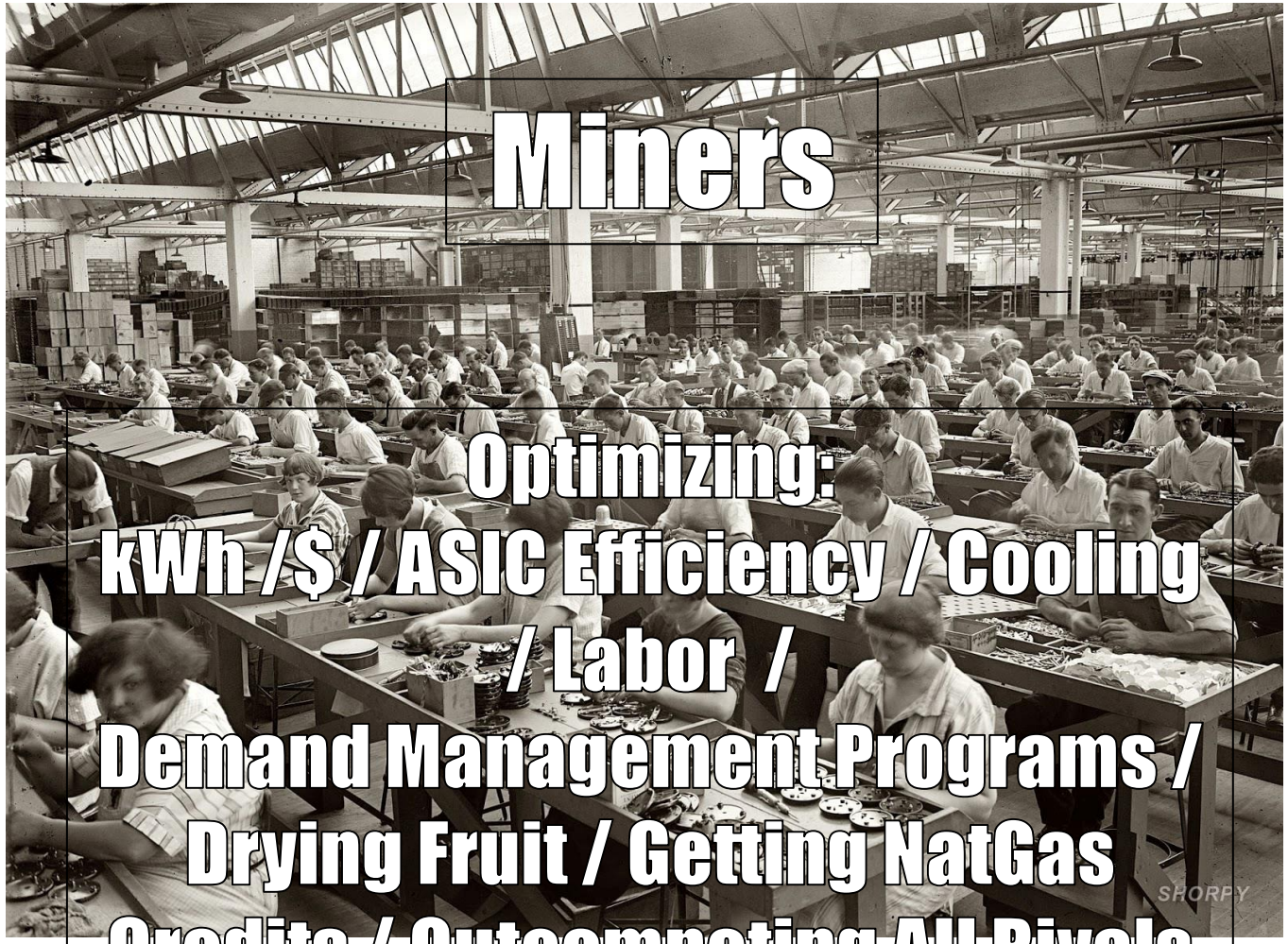
1. Never Change Layer 1 Again
   – “Protocol Ossification”
   - No “drama”.
   - No “mob rule”.
2. Shrink Layer1 Blocksize.
   - Improves Decentralization.
   - Protects your node.

“Frozen Bitcoin” - Marco Verch , Creative Commons License



Validating L1

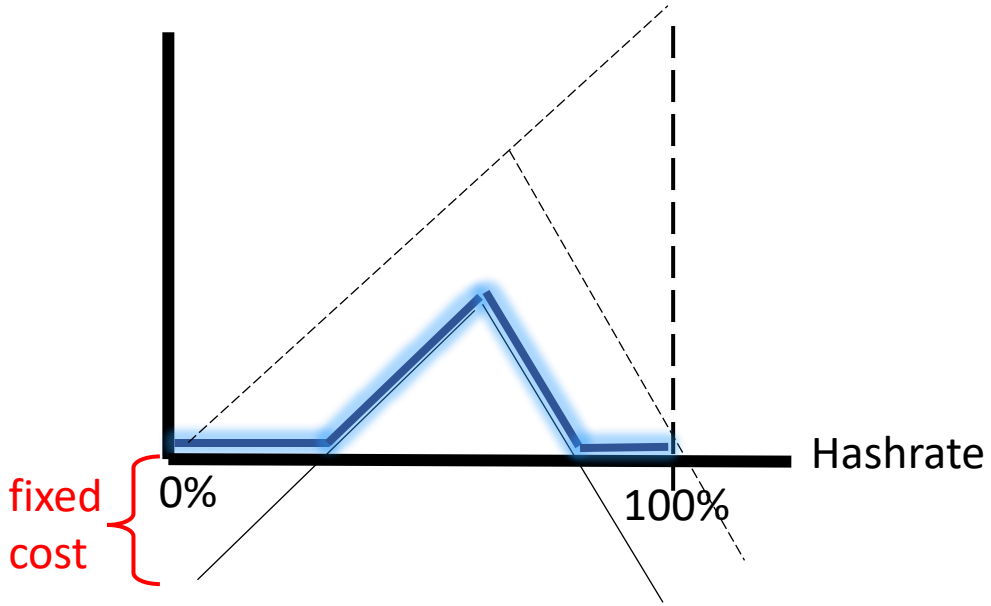
+ counting to 13,150



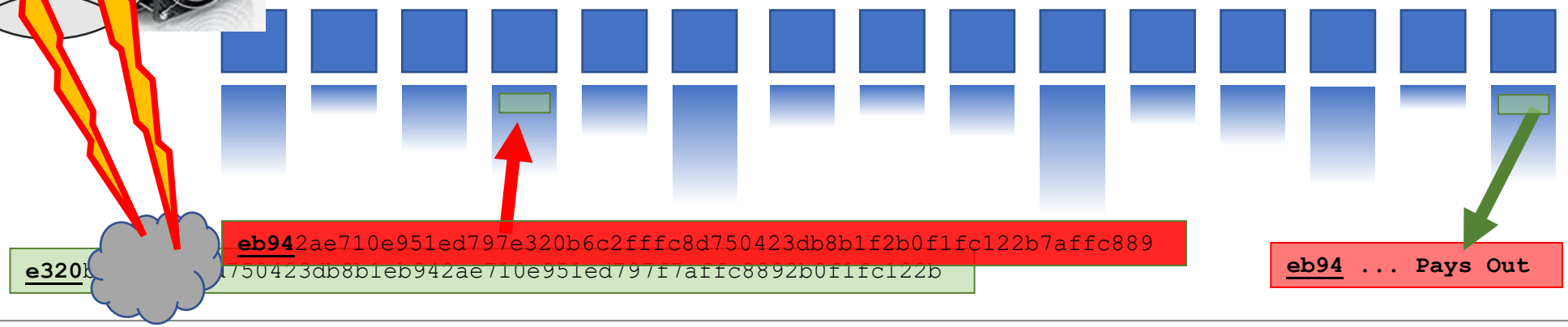
+ add/remove/validate Sidechains

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.

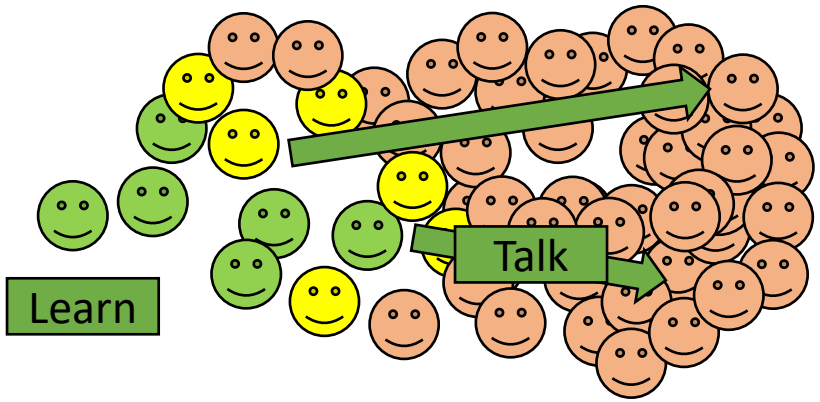
(#1) **Miners-Can-Steal** from Bip300 Scripts (and this is bad)	(#2) **Merged-Mining is a Side-Hustle** (and those are always bad)
The free market allows entrepreneurs to go bankrupt – this is **an essential part of creativity**. True: not every SC will succeed. But those few that do, will pay fees to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