

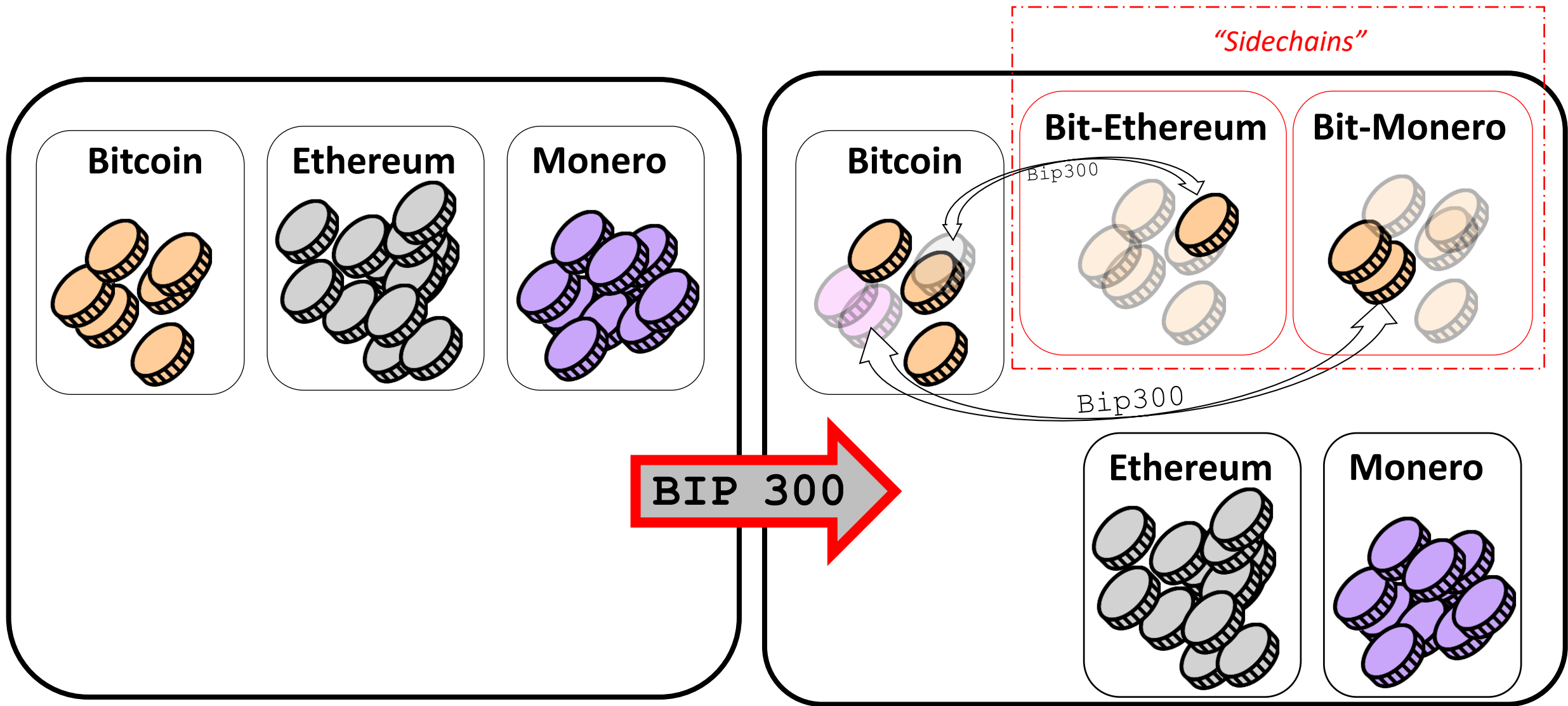
Bip300: Getting to 100% Bitcoin Dominance (and Beyond)

Paul Sztorc

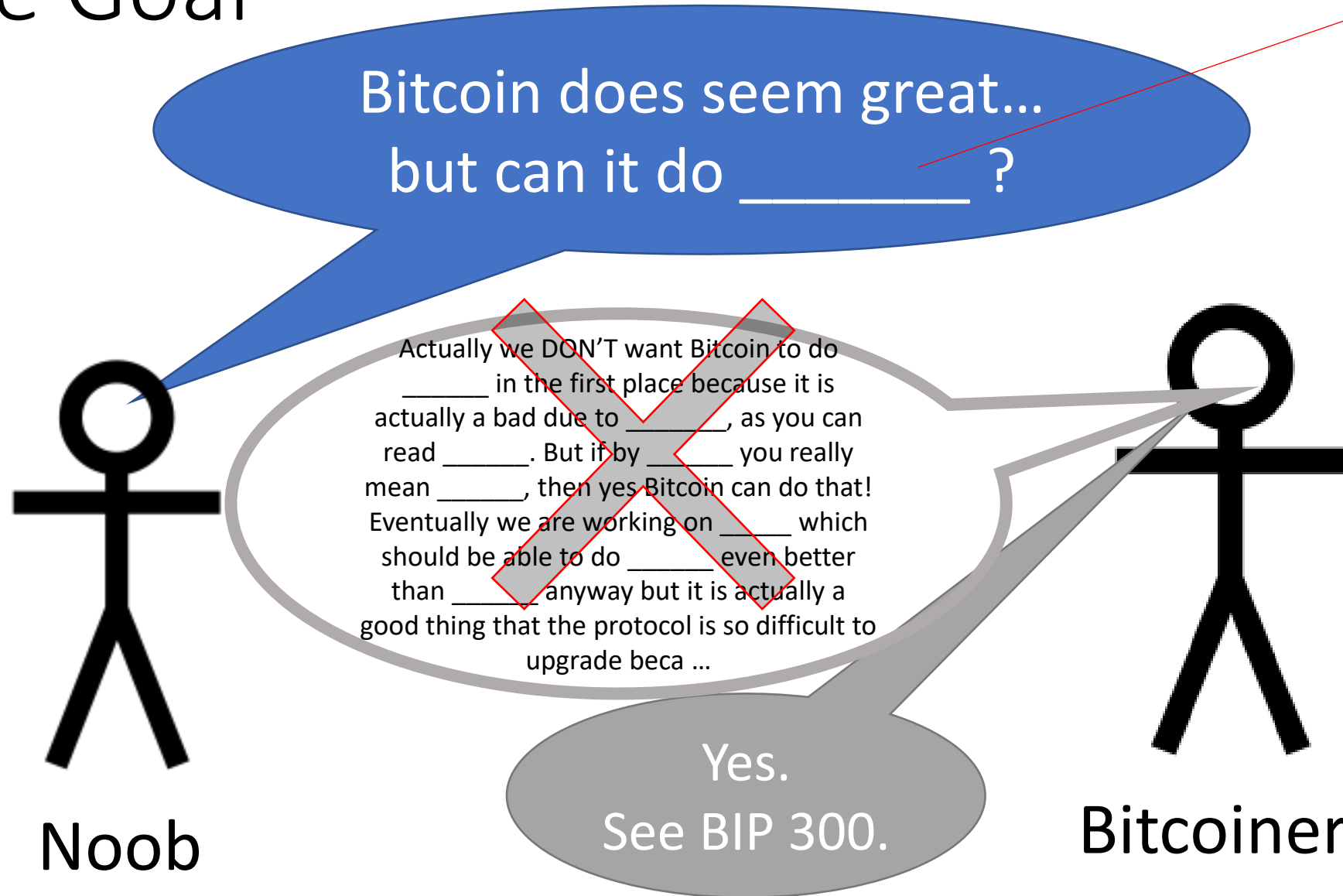
TabConf 2021 -- November 5th



The Concept, in One Slide



The Goal



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

Fringe Ideas

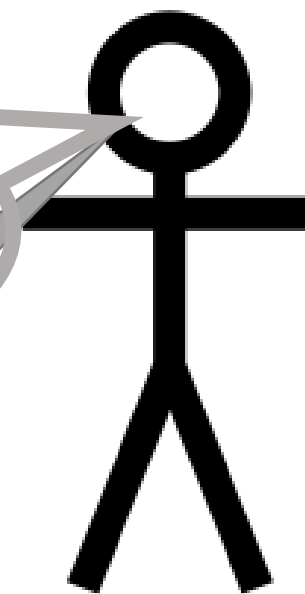
I can improve Bitcoin! It only
needs my new idea: _____ !!
When can you merge my code ??



Noob (and/or
Fringe Genius)

~~You can't just merge something into Bitcoin -- It affects everyone else's nodes!! Besides, _____ has been proposed before and you need to read _____ so that you can learn why everyone hates it, especially our 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 ...~~

Use BIP 300.
Good luck!!



Bitcoiner

Three Aspects

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

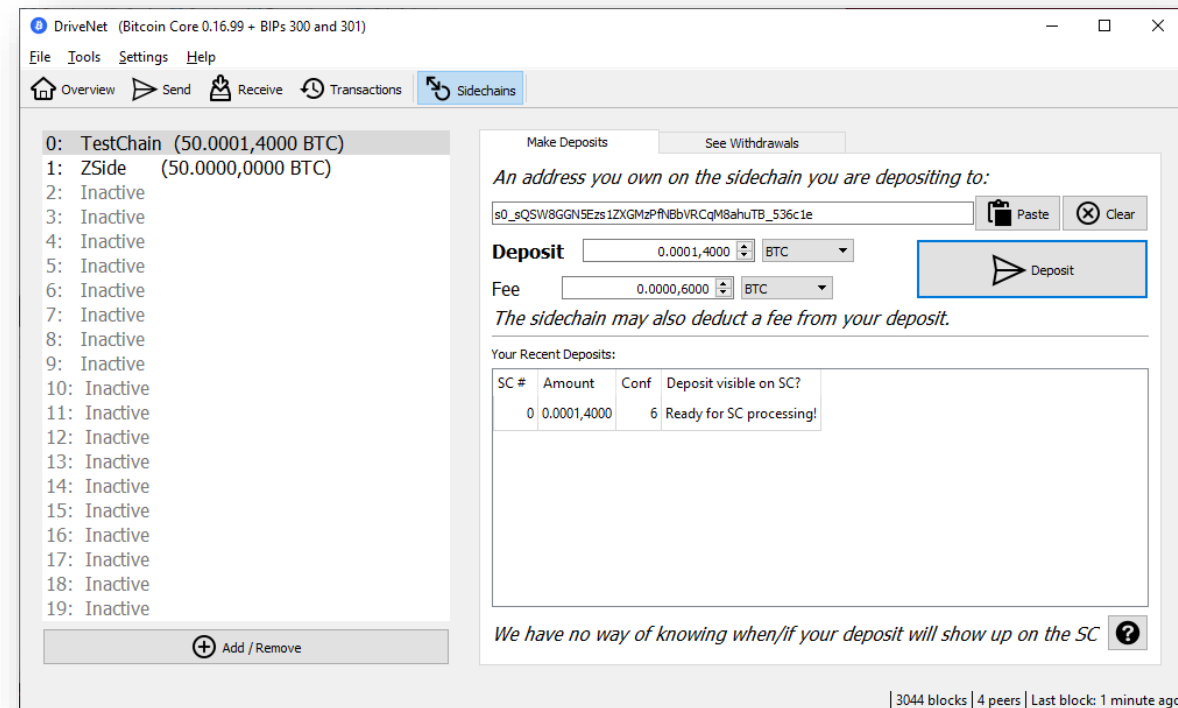
Releases

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

Te Click [here](#) for CHECKSUMs

Not Vaporware



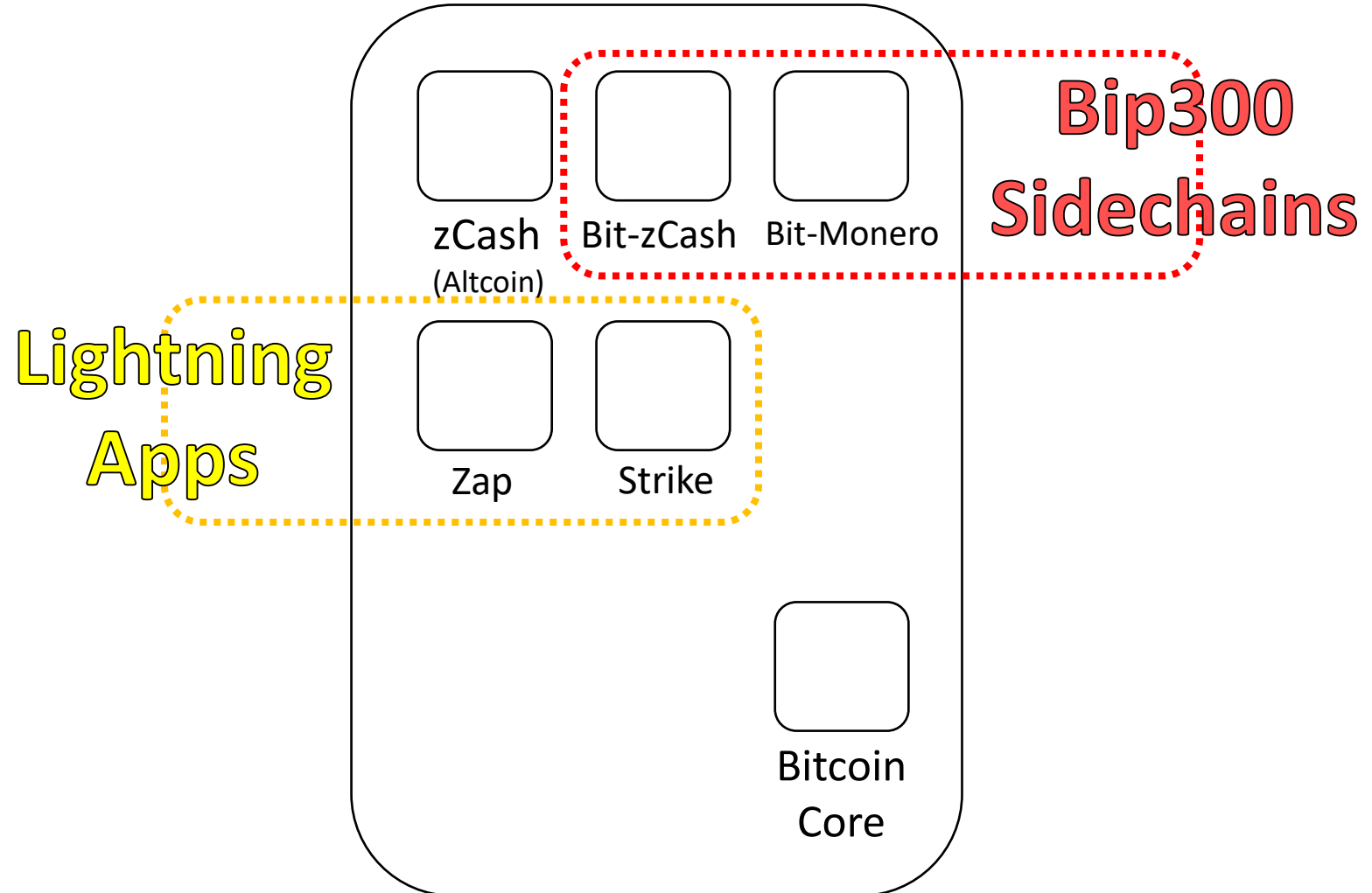
Bitcoin-ZCash Sidechain (Regtest Demo)

489 views • Mar 1, 2021

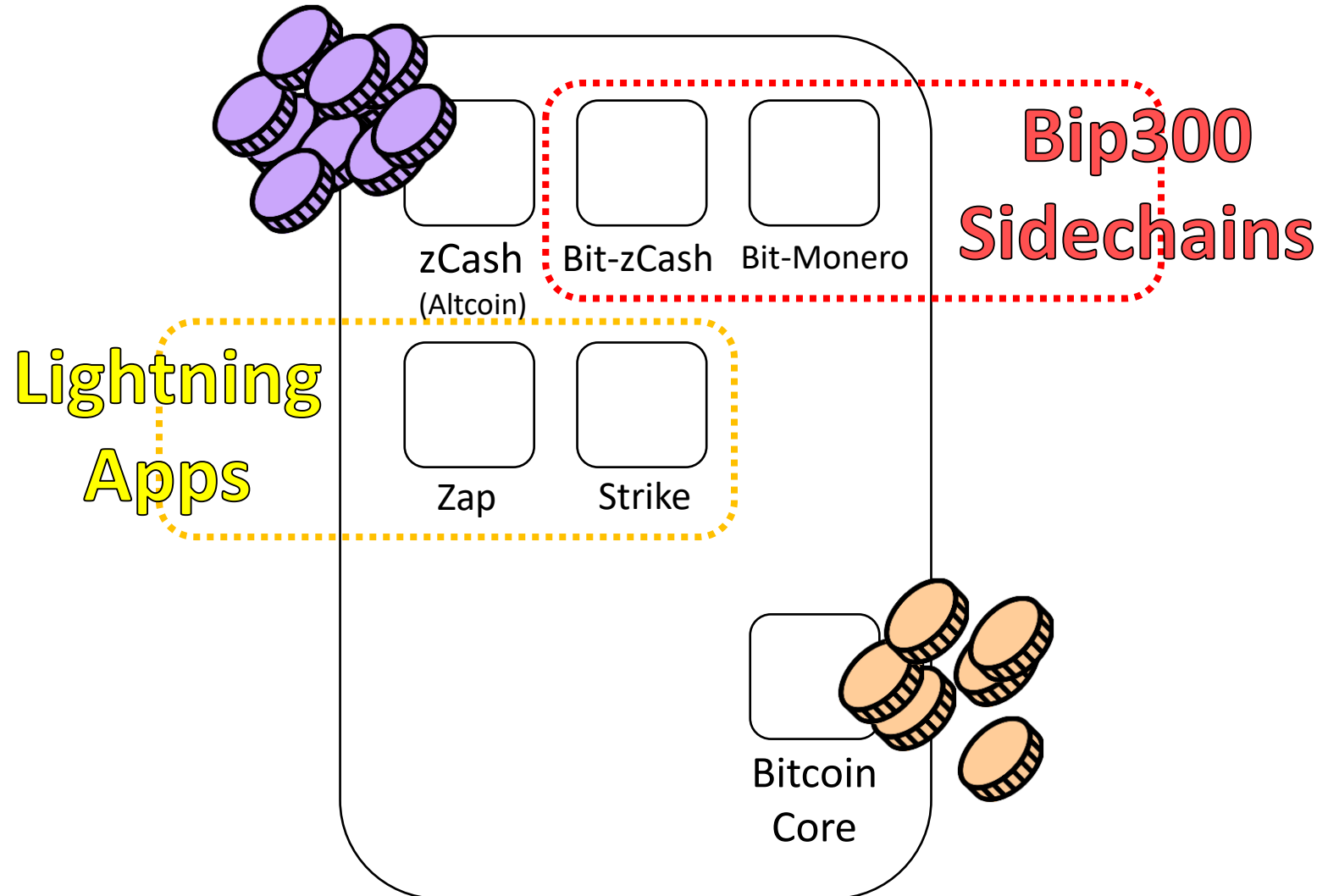
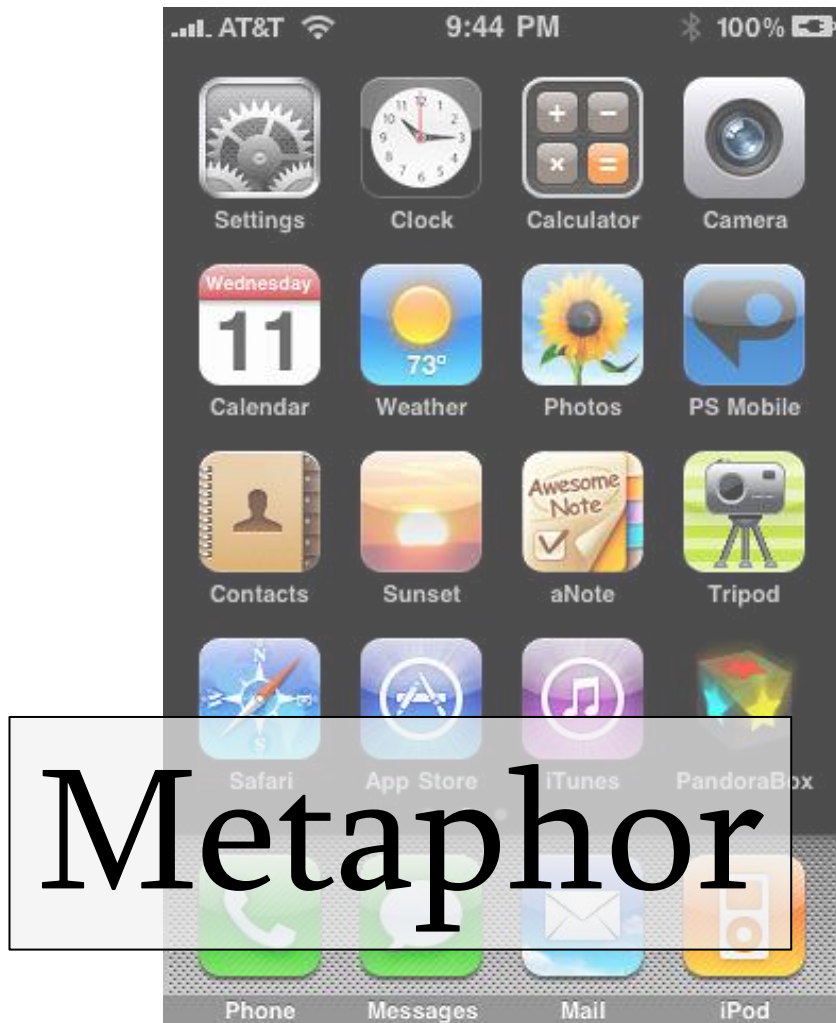
ivechain.info

Paul's Twitter: @truthcoin

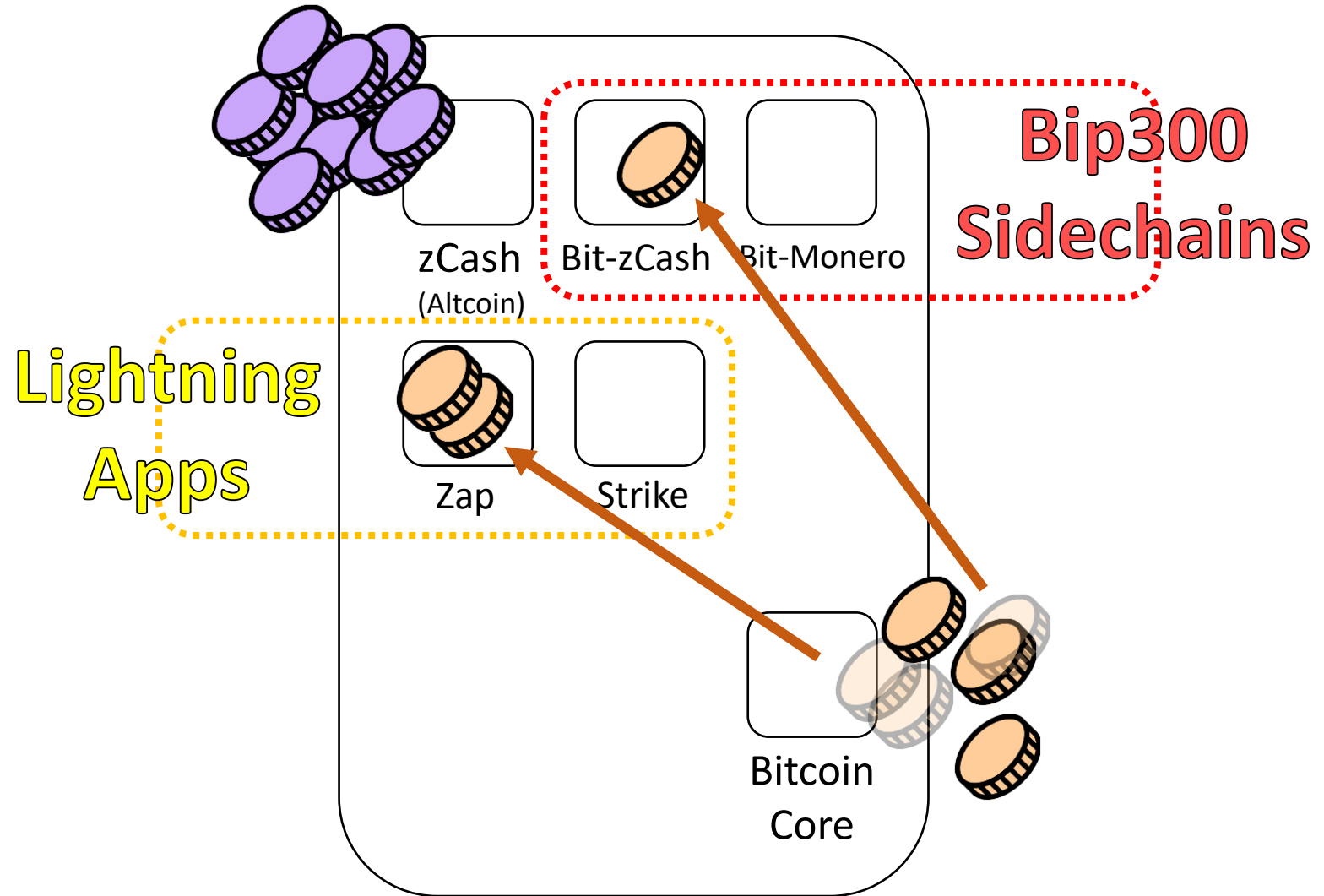
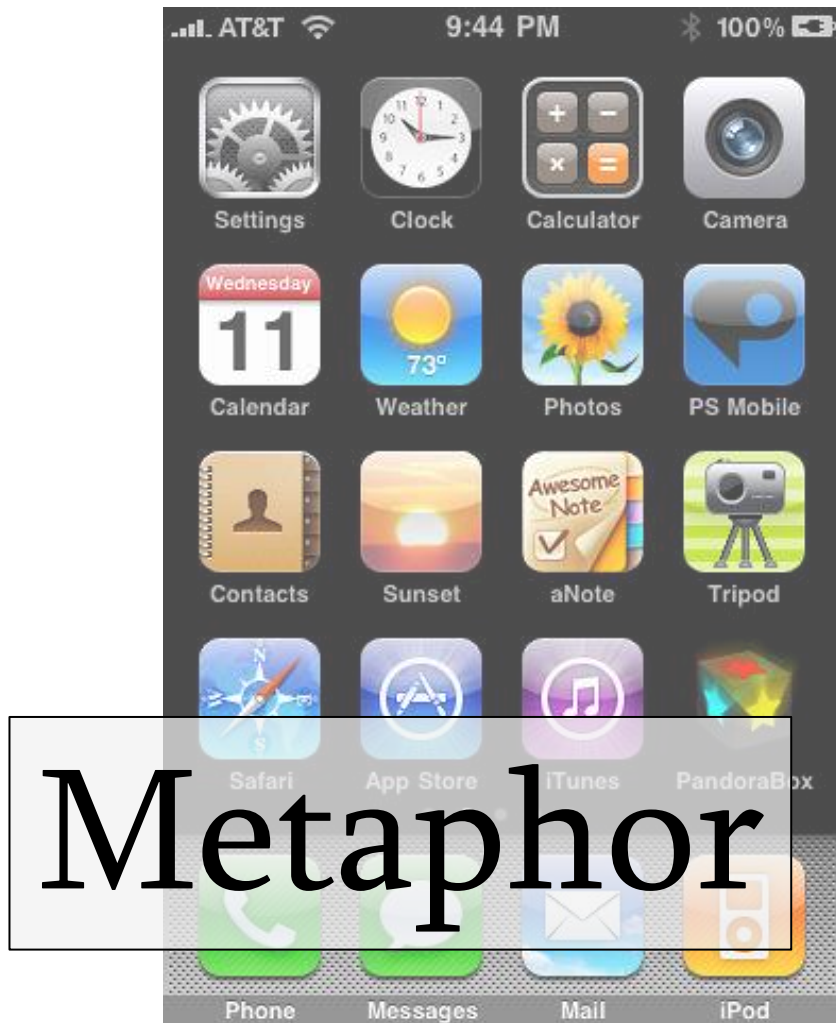
(#1) Full Autonomy



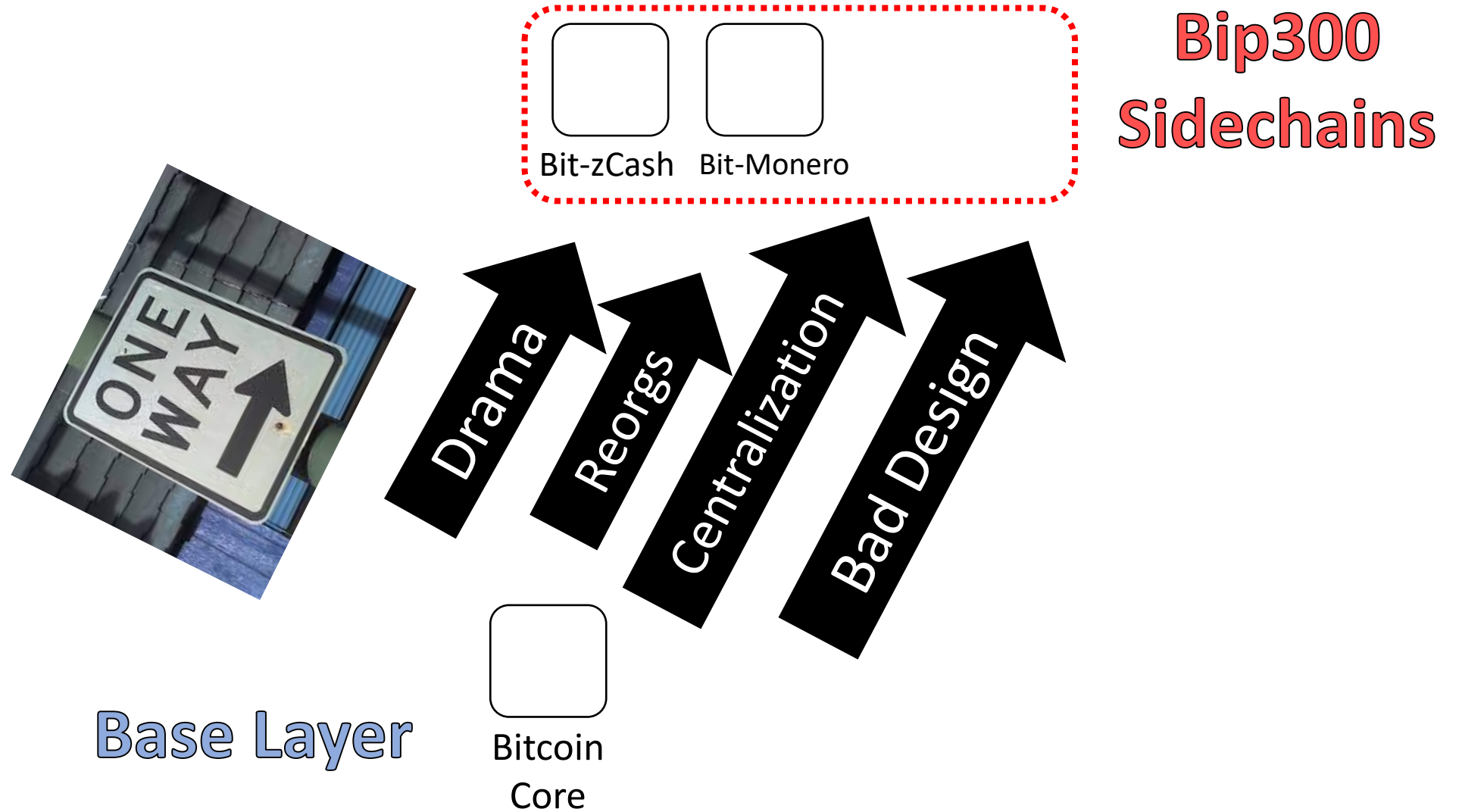
(#1) Full Autonomy



(#1) Full Autonomy



(#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



December 2020

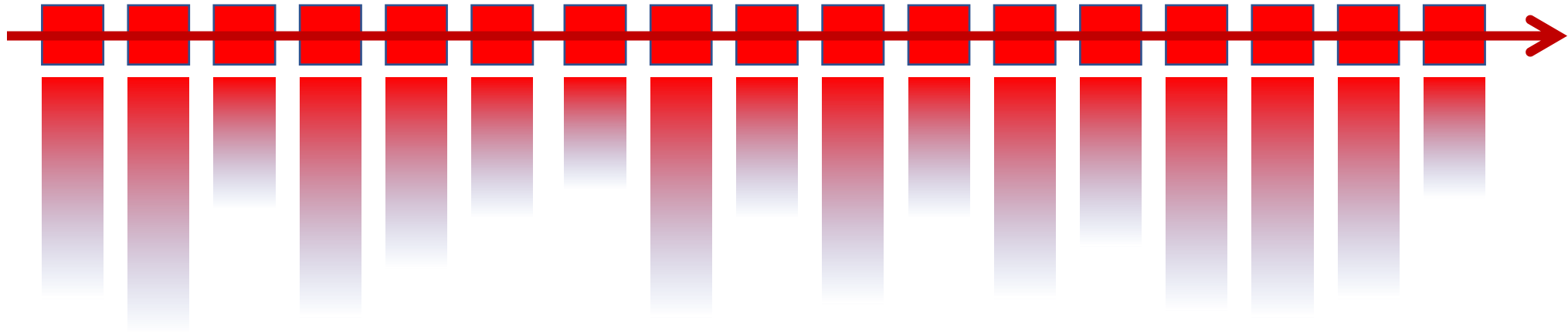
January 2021

February 2021

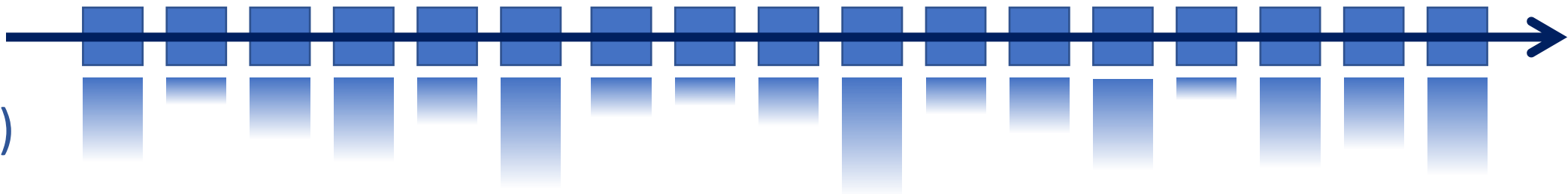
March 2021

April 2021

Layer 2
(Bit-Monero)



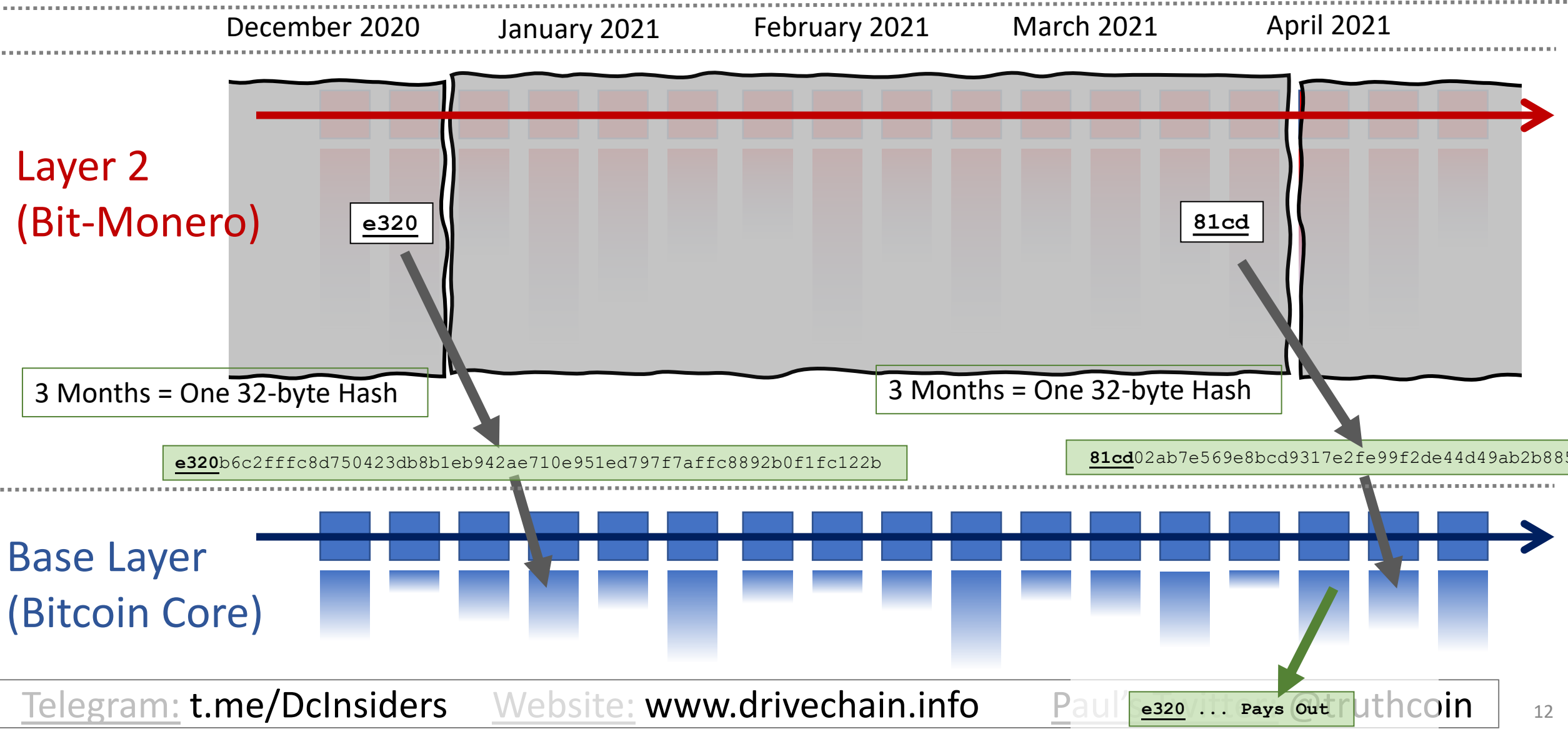
Base Layer
(Bitcoin Core)



(#2) Base Layer is Safe

= Block Header

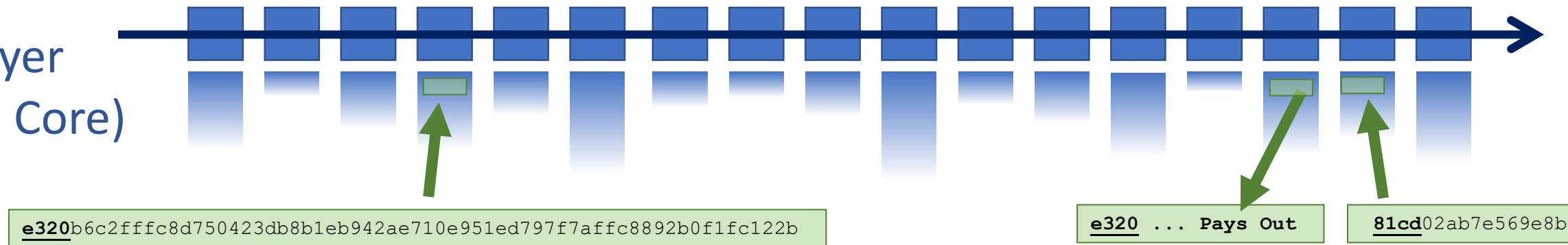
= List of transactions



(#2) Base Layer is Safe

Your Layer 1 Node Sees...

Base Layer
(Bitcoin Core)



(#2) Base Layer is Safe

Your Layer 1 Node Sees...

DriveNet (Bitcoin Core 0.16.99 + BIPs 300 and 301)

File Settings Help

Overview

Send

Receive

Transactions

Sidechains

Active Sidechains

Test Sidechain

Manage

Make a Deposit

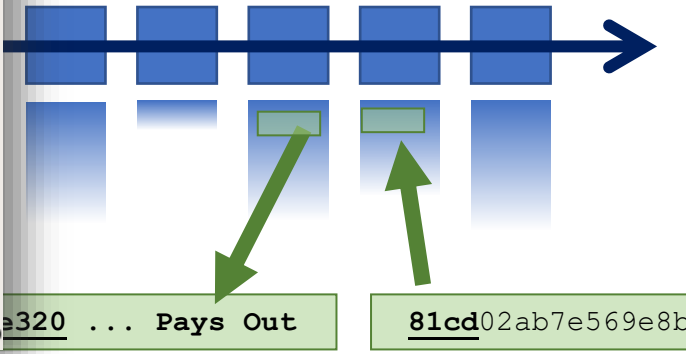
Observe Withdrawals

Double-click for details ?

Sidechain	Age	Max Age	Acks	Approved	WT^ hash
Test Sidechain	130	300	3	false	22aa8358bb24faa347555dadaa262

6729 blocks | 3 peers | Last block: 15 seconds ago

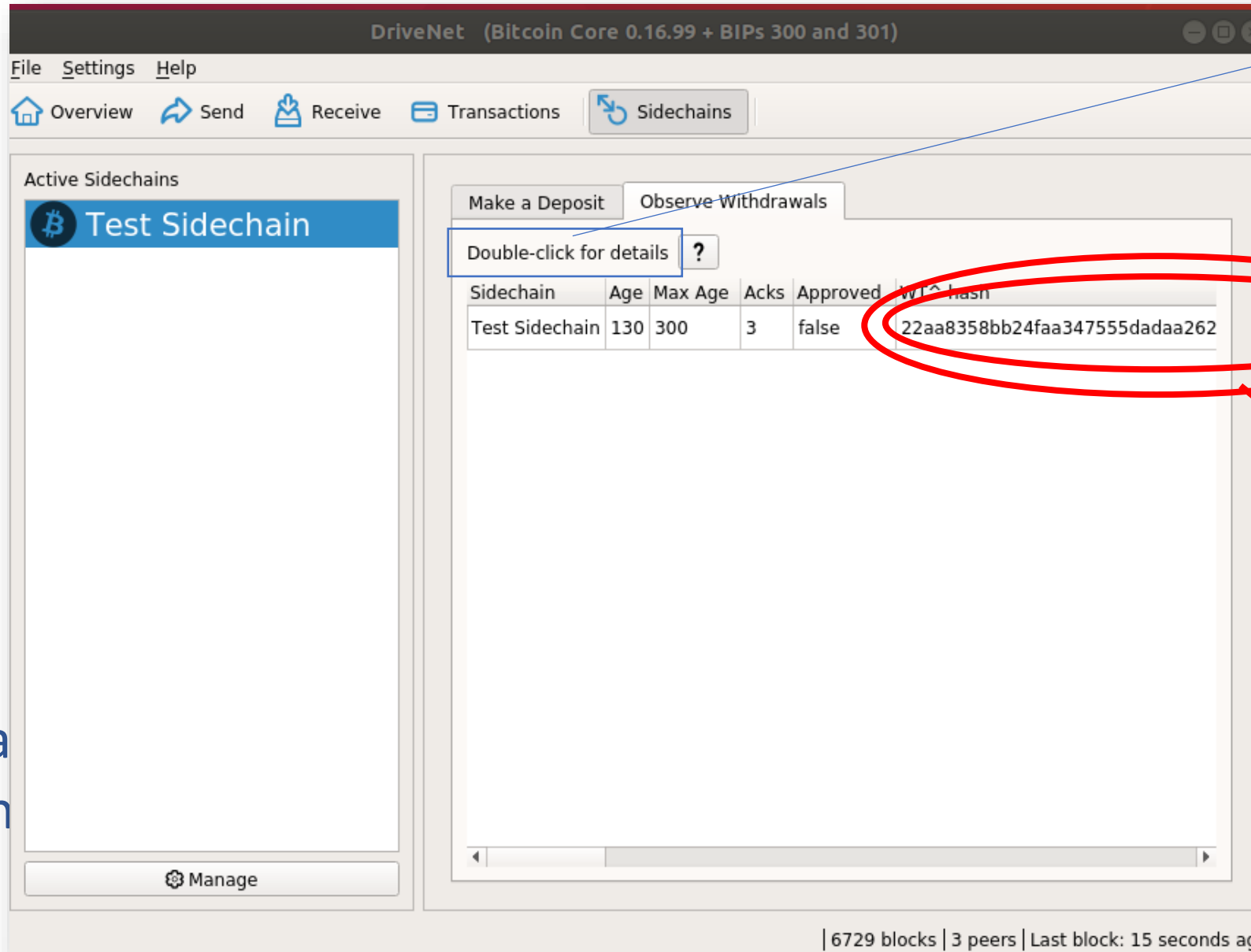
Base Layer
(Bitcoin)



(#2) Base Layer is Safe

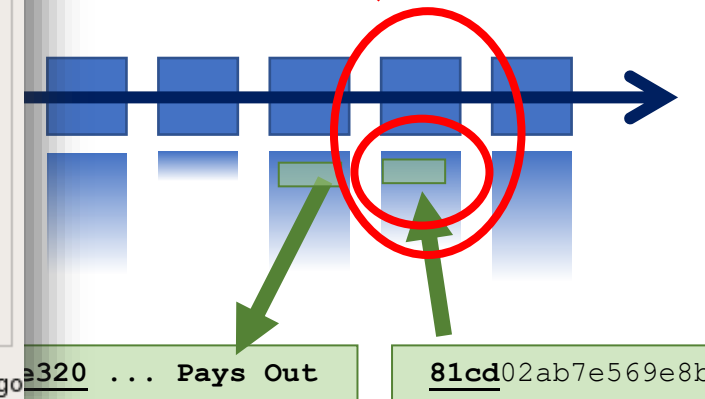
Your Layer 1 Node Sees...

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 Layer
(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

Crypto Fees

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

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 ∨
● xDei	\$12,051.22	\$27,636.72 ∨

Security Budget in the Long Run

14 Feb 2019

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

WWW.

Security Budget II, Low Fees, and Merged Mining

15 Oct 2021

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

4, 2021

coin

(#3) Improve Mining Incentives (Bip 301)

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

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	\$12,051.22	\$27,636.72 ∨

Security Budget in the Long Run

14 Feb 2019

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

WWW.

Security Budget II, Low Fees, and Merged Mining

15 Oct 2021

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

4, 2021

coin

(#3) Improve Mining Incentives (Bip 301)

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

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

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...?

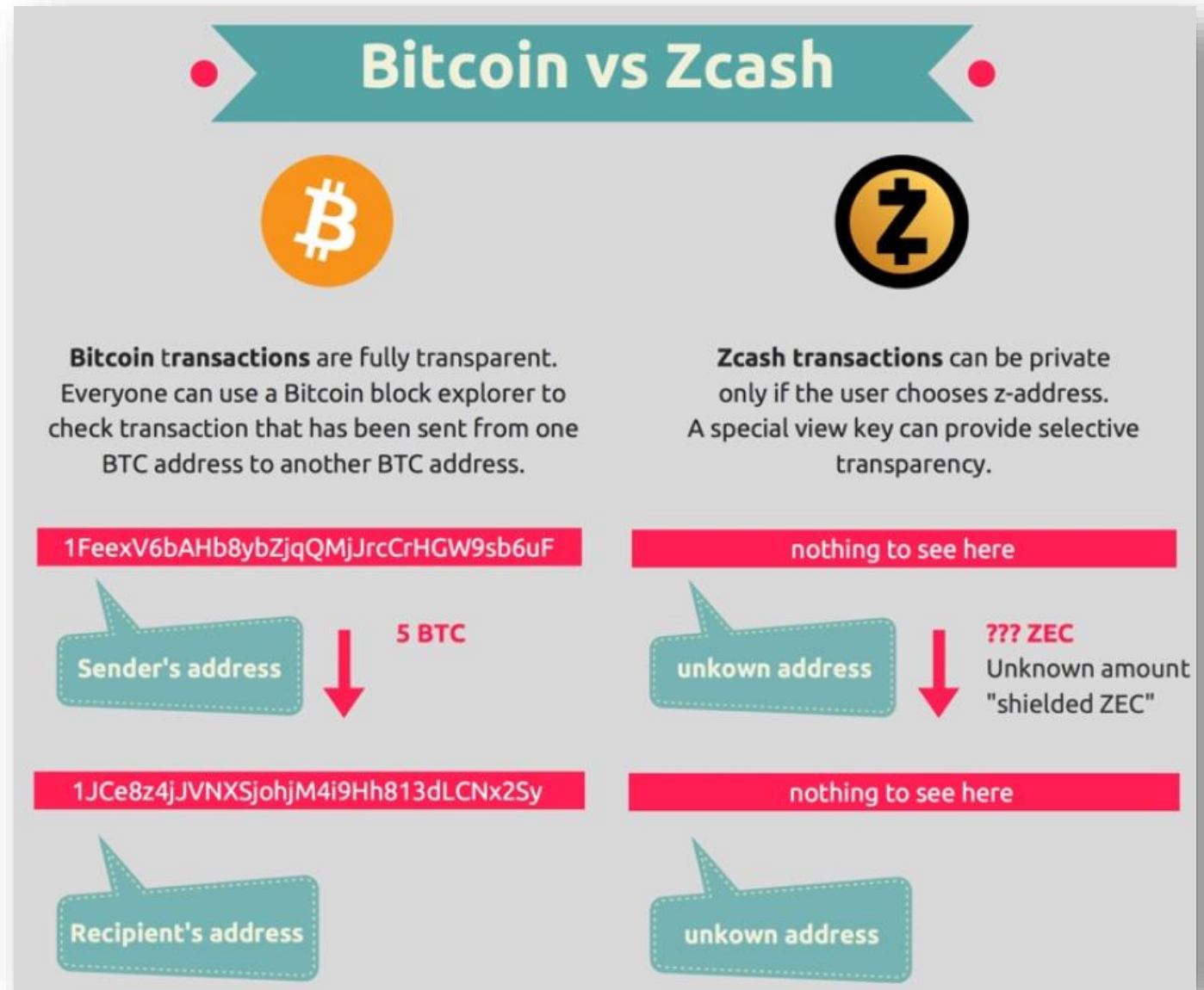
(In other words:
Which altcoins are
worth copying?)



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, 2010
Merited by Aveat

Quote from: Hal on Dec

additional block chain
on exchanges? These
purchase some kinds

Right, the exchange

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:~~

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 extra side chains also for

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/](http://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](#)

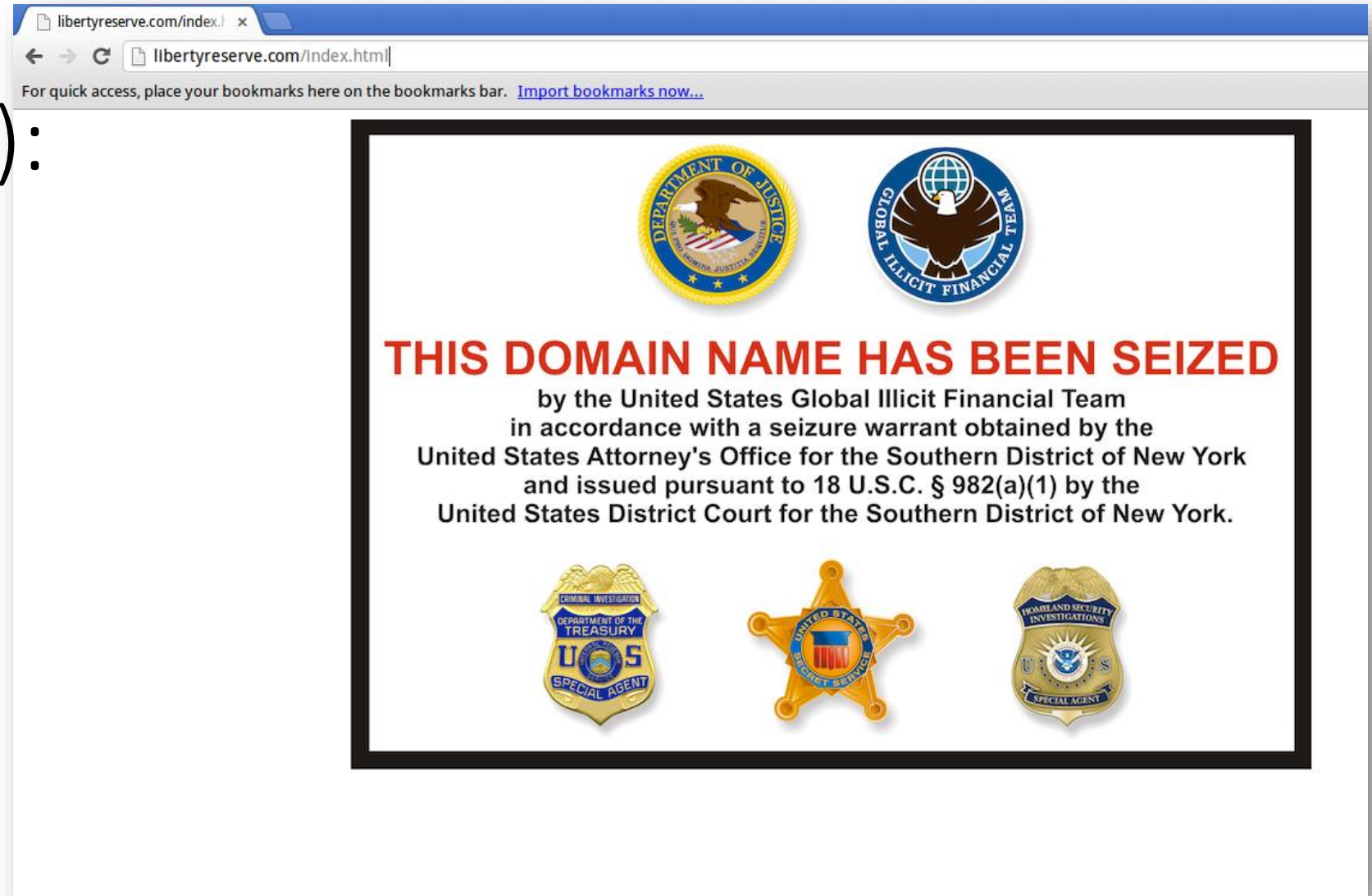
Altcoins we
should copy (?):
NameCoin

Screenshot #1 from
[www.truthcoin.info/
blog/bitnames/](http://www.truthcoin.info/blog/bitnames/)



Altcoins we
should copy (?):
NameCoin

Screenshot #2 from
[www.truthcoin.info/
blog/bitnames/](http://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!!



Logo used to represent non-fungible tokens

Contents [\[hide\]](#)

1 [Description](#)

Prediction Markets

- Screenshots from my own BTC sidechain project

www.BitcoinHivemind.com

The screenshot shows the Hivemind Core - Wallet [testnet] interface. The top menu bar includes File, Settings, and Help. Below it is a navigation bar with icons for Overview, Send, Receive, Transactions, Markets, Decisions, Author, and Vote. A yellow warning banner states: "This is a pre-release test build - use at your own risk - do not use for mining or merchant applications".

Recent Hivemind Objects:

Type/Icon	Description
	Bitcoin exchange rate as reported by CoinD
	Will Jeff Immelt have been replaced, as CEO
	Global surface temperature anomaly, cumul
	Will Barack Obama win US President in 201
	Unemployment drivers
	Fire Immelt?
	Unemployment drivers

Balances

Available:	400.00000000 BTC
Pending:	0.00000000 BTC
Immature:	50.00000000 BTC
Total:	450.00000000 BTC

Recent transactions

	5/17/16 11:41	[+50.00000000 BTC]
	(19y1RCwANn71vEZkxMrDoAjXuCzERyJE8A)	
	5/17/16 11:41	+50.00000000 BTC
	(14u1sX6BTJnnTAL2dPDgm7WKKubofpwuEy)	
	5/17/16 11:41	+50.00000000 BTC
	(1D6kbEHq7BXpJsVbuxLivt4CV4fv8poCk7)	
	5/17/16 11:41	+50.00000000 BTC
	(1AAdn8e5v7QM155C6Cc6Z8u82SZWDLH6cd)	
	5/17/16 11:41	+50.00000000 BTC
	(16bfT93g3QY53xsEkK6UwnKYaa7FDBxsoc)	
	5/17/16 11:40	+50.00000000 BTC
	(1NwRMJnpetsFHVCPzjeYo1s89StTi4HHDa)	

Prediction Markets

- Screenshots from my own BTC sidechain project

www.BitcoinHivemind.com

The screenshot displays the Hivemind Core - Wallet [testnet] interface. The main window is titled "Hivemind Core - Wallet [testnet]" and features a menu bar with "File", "Settings", and "Help". Below the menu bar is a navigation bar with tabs: "Overview", "Send", "Receive", "Transactions", "Markets", "Decisions", "Author", and "Vote". The "Markets" tab is currently selected.

On the left side, there is a sidebar with a "Recent Hivemind Objects" section. It includes a "Type/Icon" column and a list of objects with their corresponding icons and names. The objects listed are:

- Bitcoin
- Will
- Glob
- Will
- Une
- Fire
- Une

The main content area is divided into two sections: "Graph" and "Market Info". The "Graph" section displays two line charts. The top chart is titled "Unemployment drivers" and shows a line graph with a peak. The bottom chart is titled "Fire Immelt?" and shows a line graph with a sharp peak. The "Market Info" section provides details for the selected market, including the title, description, tags, and market ID.

Below the graphs, there is a table with two columns: "Unemployment drivers" and "Fire Immelt?". The table contains the following data:

Unemployment drivers	Fire Immelt?
Title: Unemployment drivers Description: Market on unemployment Tags: tags Market ID: 40e701a38cfc16df5502070ff05ff274682a84e6413d0174282ff...	Title: Fire Immelt? Description: Market on the employment of GE CEO Immelt Tags: tags Market ID: 23f3591495cf5158b35c0e1945fade02aa6021350fba957a768...

Prediction Markets

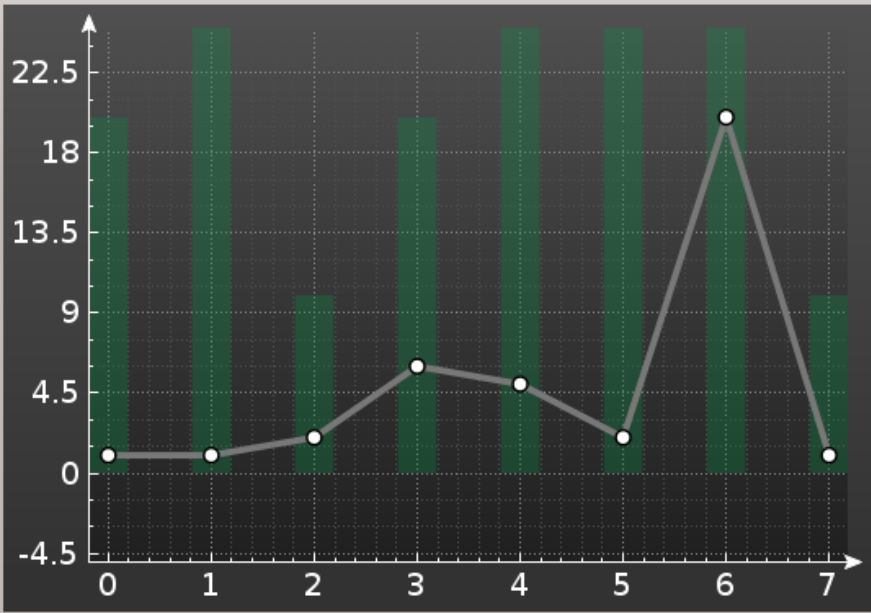
- Screenshots from my own BTC sidechain project

Trade www.BitcoinHivemind.com

Market ID: 40e701a38cfc16df5502070ff05ff274682a84e6413d0174282ff54d45d0576c [Copy](#)

Standard Two Dimensional High Dimensional

Market Graph: ☒ 1 Month ☐ 1 Day ☐ 5 Minutes



Period	Price
0	1.0
1	1.0
2	2.0
3	6.0
4	5.0
5	2.0
6	20.0
7	1.0

Current Price: 0.00 Shares Owned: 0

Your trades:

Decision State: 0

Payout Address:

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

[Finalize](#)







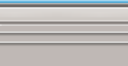
File Settings Help
Overview Send Receive

Branch: Main

Search:

Tags:

Type/Icon

Type/Icon	Item
	Bitcoin
	Will
	Glob
	Will
	Une
	Fire
	Une

Prediction Markets

- Screenshots from my own BTC sidechain project

The screenshot displays the BitcoinHivemind.com Trade interface. The top bar shows the website name and a 'Copy' button for the Market ID: 40e701a38cfc16df5502070ff05ff274682a84e6413d0174282ff54d45d0576c. The interface is divided into several sections:

- Left Panel:** Contains a 'File Settings Help' menu, a 'Recent Hivemind Objects' list with icons and names (e.g., Bitcoin, Will, Glob, Will, Une), and a 'Type/Icon' dropdown.
- Market Graph:** A line graph showing price over time. The x-axis is labeled 1 through 7, and the y-axis ranges from -4.5 to 22.5. The graph shows a series of green bars and a line connecting points. The points are approximately at (1, 1), (2, 2), (3, 6), (4, 5), (5, 2), (6, 18), and (7, 1).
- Trading Controls:** Includes a 'Make Order' button, a '# Shares' input field (set to 0), a 'Price' input field (set to 0.00), and a 'Decision State' dropdown (set to 0). There are also buttons for '-10' and '+10' to adjust the share count.
- Summary:** A section showing 'Shares Owned: 0', 'Shares to buy: 0', 'Trade Cost: 0', and 'Balance: 0'.
- Finalize:** A button with a checkmark and the text 'Finalize'.

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

Storage Capacity

556

Storage Providers

913TB

Used Storage

1.2M

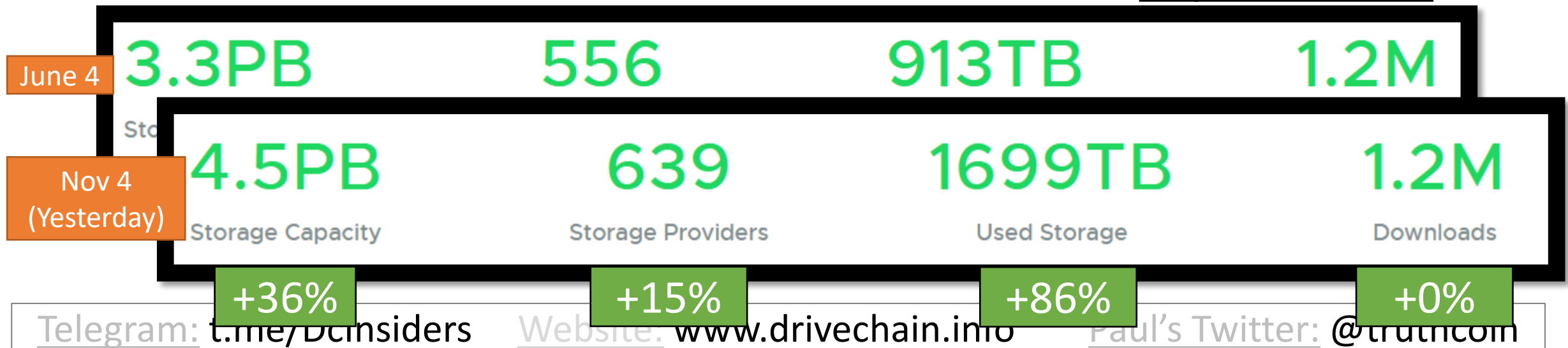
Downloads

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

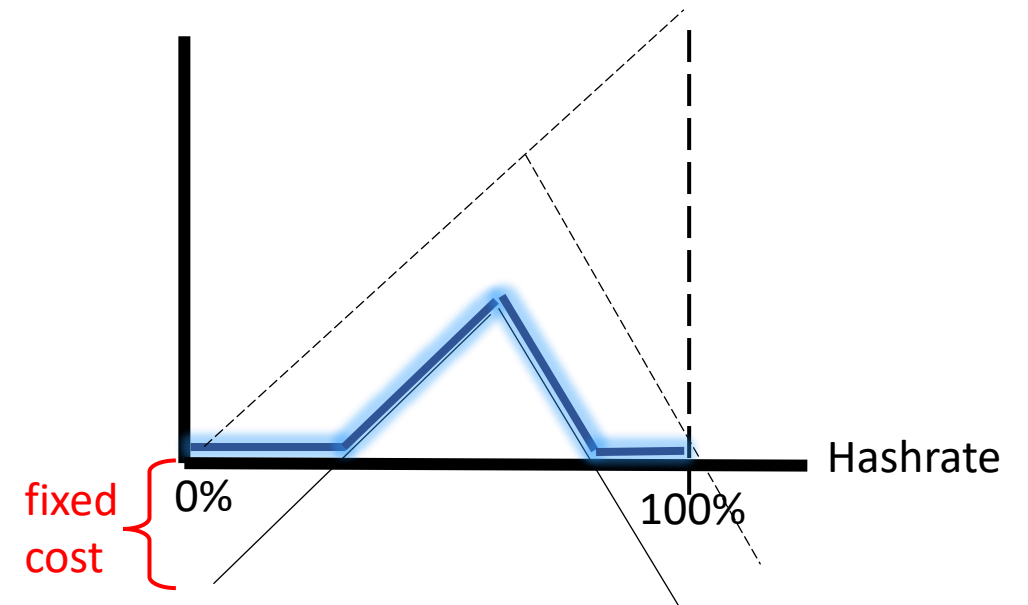
1. Never Change Layer 1 Again
 - “Protocol Ossification”
 - No “drama”.
 - No “mob rule”.
2. Shrink Layer1 Blocksize.
 - Improves Decentralization.
 - Protects your node.



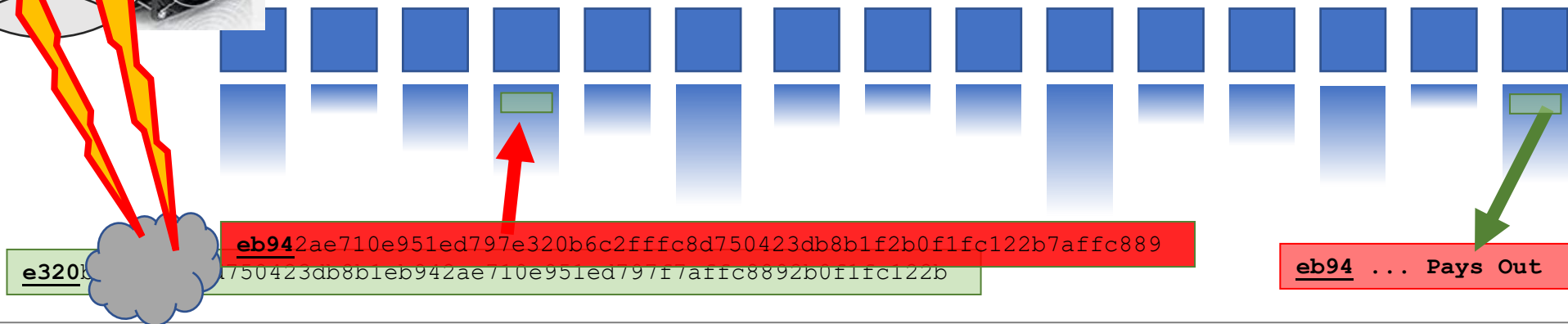
“Frozen Bitcoin” - Marco Verch , Creative Commons License

Two Supposed Drawbacks

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



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



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

The free market allows entrepreneurs to go bankrupt – this is an essential part of creativity. True: not every SC will succeed. But those few that do, will pay fees to miners and boost BTC's appeal (since BTC can now easily do everything). The failures will serve as a warning to lazy or incompetent developers.

Bip300 has multiple safeguards in place to make “stealing” difficult. Stealing requires 3-6 months of openly dishonest mining activity. Humans can audit theft, by checking just 32 bytes.

Miners “can” steal from Lightning Network (by broadcasting old state + censoring Justice Txns), but this criterion is never held against LN.

The user is sovereign. Users are allowed to sell their BTC for USD; or use BTC to buy “bad” products (ie “drugs”). Or invest in Alts / scams. Bip300 allows users to spend BTC to a script.

This supposed “flaw” is actually a pro, as it gives miners motive and opportunity to destroy “parasite sidechains” (SC which antagonize other SCs). I am not aware of any other way of efficiently accomplishing this. And I believe it is prerequisite for high-quality smart contracts.

The whole point of SCs is that Layer1 nodes ignore them. With federations, you trust a fixed committee of law-abiding people. With Bip300 you trust a decentralized P2P process.

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

The fixed cost in question...
...is zero under BMM.
...was already microscopic, vs other miner fixed costs.
...must always be small enough for non-mining nodes to exist (since their revenue is the smallest of all, \$0.)

Mining is a complex task involving many “sub-tasks” (getting cheap power / sourcing good ASICs / etc). Each has its own incentives, innovation, and fixed costs. No stopping those.

Bizarre implications: if BitFury sold t-shirts on the side, for profit, then t-shirts = bad for BTC. If Saylor altruistically paid miners \$0.10 per year, then MS = bad for Bitcoin.

MM is the opposite of bad – it is good and necessary. MM alone can boost BTC's fee revenues by 10,000x or more. Without MM, long run hashrate may be too low.

What is probably happening is that people are confusing node costs with mining costs. Node costs *must* be low, for decentralization. But mining costs have no such requirement. In fact, if we wanted mining costs to be low we could remove the upward difficulty adjustments.

MM is already unblockable. Satoshi invented MM in 2010, and envisioned many independent MM chains. We have been MM since 2011, with no end in sight.

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

The free market allows entrepreneurs to go bankrupt – this is an essential part of creativity. True: not every SC will succeed. But those few that do, will pay fees to miners and boost BTC's appeal (since BTC can now easily do everything). The failures will serve as a ~~warning to lazy or incompetent developers.~~

Bip300 has multiple safeguards in place to make “stealing” difficult. Stealing requires 3-6 months of openly dishonest mining activity. Humans can audit theft, by checking just 32 bytes.

Miners “can” steal from Lightning Network (by broadcasting old state + censoring Justice Txns), but this criterion is never held against LN.

The user is sovereign. Users are allowed to sell their BTC for USD; or use BTC to buy “bad” products (ie “drugs”). Or invest in Alts / scams. Bip300 allows users to spend BTC to a script.

This supposed “flaw” is actually a pro, as it gives miners motive and opportunity to destroy “parasite sidechains” (SC which antagonize other SCs). I am not aware of any other way of efficiently accomplishing this. And I believe it is prerequisite for high-quality smart contracts.

The whole point of SCs is that Layer1 nodes ignore them. With federations, you trust a fixed committee of law-abiding people. With Bip300 you trust a decentralized P2P process.

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

The fixed cost in question...
...is zero under BMM.
...was already microscopic, vs other miner fixed costs.
...must always be small enough for non-mining nodes to exist (since their revenue is the smallest of all, \$0.)

Mining is a complex task involving many “sub-tasks” (getting cheap power / sourcing good ASICs / etc). Each has its own incentives, innovation, and fixed costs. No stopping those.

Bizarre implications: if BitFury sold t-shirts on the side, for profit, then t-shirts = bad for BTC. If Saylor altruistically paid miners \$0.10 per year, then MS = bad for Bitcoin.

MM is the opposite of bad – it is good and necessary. MM alone can boost BTC's fee revenues by 10,000x or more. Without MM, long run hashrate may be too low.

What is probably happening is that people are confusing node costs with mining costs. Node costs *must* be low, for decentralization. But mining costs have no such requirement. In fact, if we wanted mining costs to be low we could remove the upward difficulty adjustments.

MM is already unblockable. Satoshi invented MM in 2010, and envisioned many independent MM chains. We have been MM since 2011, with no end in sight.

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

The free market allows entrepreneurs to go bankrupt – this is **an essential part of creativity**. True: not every SC will succeed. But those few that do, will pay fees to miners and boost BTC's appeal (since BTC can now easily do everything). The failures will serve as a warning to lazy or incompetent developers.

Bip300 has multiple safeguards in place to make “stealing” difficult. Stealing requires **3-6 months** of openly dishonest mining activity. Humans can audit theft, by checking just 32 bytes.

Miners “can” **steal from Lightning Network** (by broadcasting old state + censoring Justice Txns), but this criterion is never held against LN.

The user is **sovereign**. Users are **allowed** to sell their BTC for USD; or use BTC to buy “bad” products (ie “drugs”). Or invest in Alts / scams. Bip300 allows users to spend BTC to a script.

This supposed “flaw” is actually a pro, as it gives miners motive and opportunity to **destroy “parasite sidechains”** (SC which antagonize other SCs). I am not aware of any other way of efficiently accomplishing this. And I believe it is prerequisite for high-quality smart contracts.

The **whole point** of SCs is that Layer1 nodes ignore them. With federations, you trust a fixed committee of law-abiding people. With Bip300 you trust a decentralized P2P process.

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

The fixed cost in question...
...is **zero** under BMM.
...was already **microscopic**, vs other miner fixed costs.
...**must always be small** enough for non-mining nodes to exist (since their revenue is the smallest of all, \$0.)

Mining is a complex task involving many “sub-tasks” (getting cheap power / sourcing good ASICs / etc). Each has its own incentives, innovation, and fixed costs. **No stopping those.**

Bizarre implications: if BitFury sold t-shirts on the side, for profit, then **t-shirts = bad for BTC**. If Saylor altruistically paid miners \$0.10 per year, then MS = bad for Bitcoin.

MM is the opposite of bad – it is good and necessary. MM alone can **boost BTC's fee revenues by 10,000x** or more. Without MM, long run hashrate may be too low.

What is probably happening is that people are **confusing node costs** with **mining costs**. Node costs *must* be low, for decentralization. But mining costs have no such requirement. In fact, if we wanted mining costs to be low we could remove the upward difficulty adjustments.

MM is **already unblockable**. Satoshi invented MM in 2010, and envisioned many independent MM chains. We have been MM since 2011, with no end in sight.

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

The free market allows entrepreneurs to go bankrupt – this is an essential part of creativity. True: not every SC will succeed. But those few that do, will pay fees to miners and boost BTC's appeal (since BTC can now easily do everything). The failures will serve as a warning to lazy or incompetent developers.

Bip300 has multiple safeguards in place to make “stealing” difficult. Stealing requires 3-6 months of openly dishonest mining activity. Humans can audit theft, by checking just 32 bytes.

Miners “can” steal from Lightning Network (by broadcasting old state + censoring Justice Txns), but this criterion is never held against LN.

The user is sovereign. Users are allowed to sell their BTC for USD; or use BTC to buy “bad” products (ie “drugs”). Or invest in Alts / scams.
Bip300 allows users to spend BTC to a script.

This supposed “flaw” is actually a pro, as it gives miners motive and opportunity to destroy “parasite sidechains” (SC which antagonize other SCs). I am not aware of any other way of efficiently accomplishing this. And I believe it is prerequisite for high-quality smart contracts.

The whole point of SCs is that Layer1 nodes ignore them. With federations, you trust a fixed committee of law-abiding people. With Bip300 you trust a decentralized P2P process.

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

The fixed cost in question...
...is zero under BMM.
...was already microscopic, vs other miner fixed costs.
...must always be small enough for non-mining nodes to exist (since their revenue is the smallest of all, \$0.)

Mining is a complex task involving many “sub-tasks” (getting cheap power / sourcing good ASICs / etc). Each has its own incentives, innovation, and fixed costs. No stopping those.

Bizarre implications: if BitFury sold t-shirts on the side, for profit, then t-shirts = bad for BTC. If Saylor altruistically paid miners \$0.10 per year, then MS – bad for Bitcoin.

MM is the opposite of bad – it is good and necessary. MM alone can boost BTC's fee revenues by 10,000x or more. Without MM, long run hashrate may be too low.

What is probably happening is that people are confusing node costs with mining costs. Node costs *must* be low, for decentralization. But mining costs have no such requirement. In fact, if we wanted mining costs to be low we could remove the upward difficulty adjustments.

MM is already unblockable. Satoshi invented MM in 2010, and envisioned many independent MM chains. We have been MM since 2011, with no end in sight.

Future of Bip300 – Depends on You!

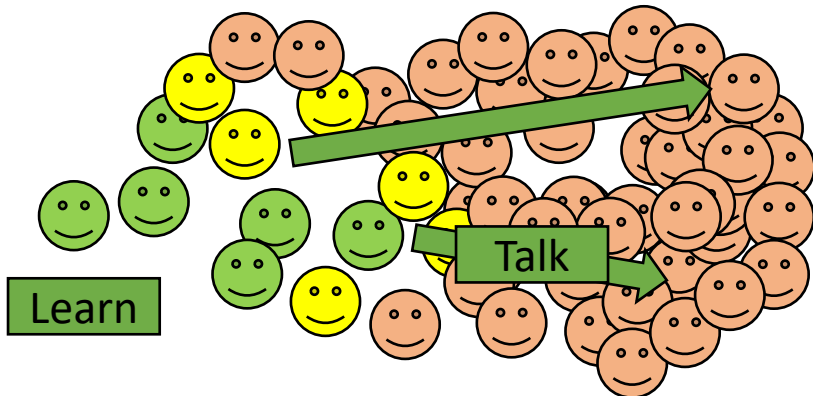
1. Learn !

- Download the software
- Read drivechain.info

2. Talk

- Soft forks need consensus
- Invite on podcasts/whatever

3. View Altcoins Differently



Releases

drivechain.info/releases/

Drivechain = Bip 300+301

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](#)

Thank You

for Your Attention!

(Find me and talk to me!)

