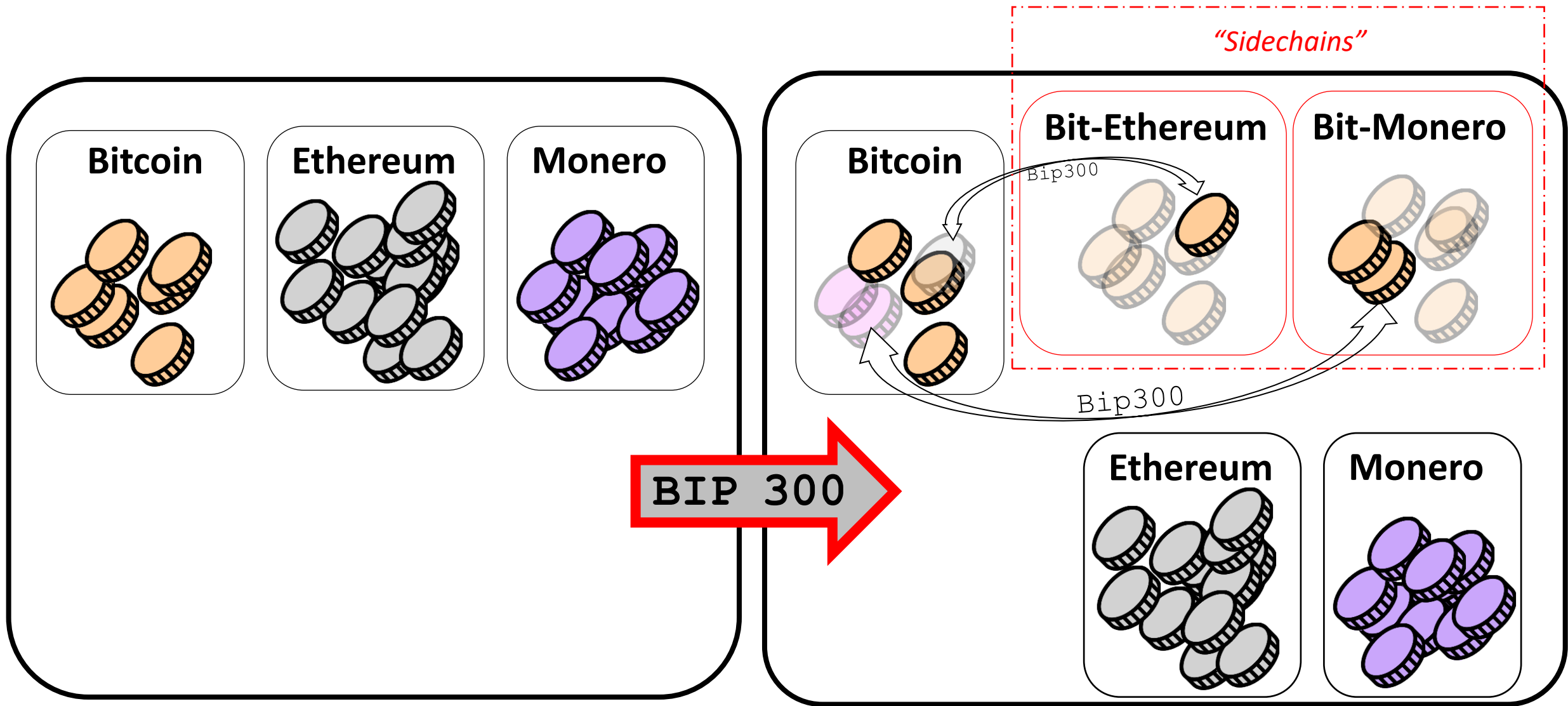


# Bip300: Getting to 100% Bitcoin Dominance (and Beyond)

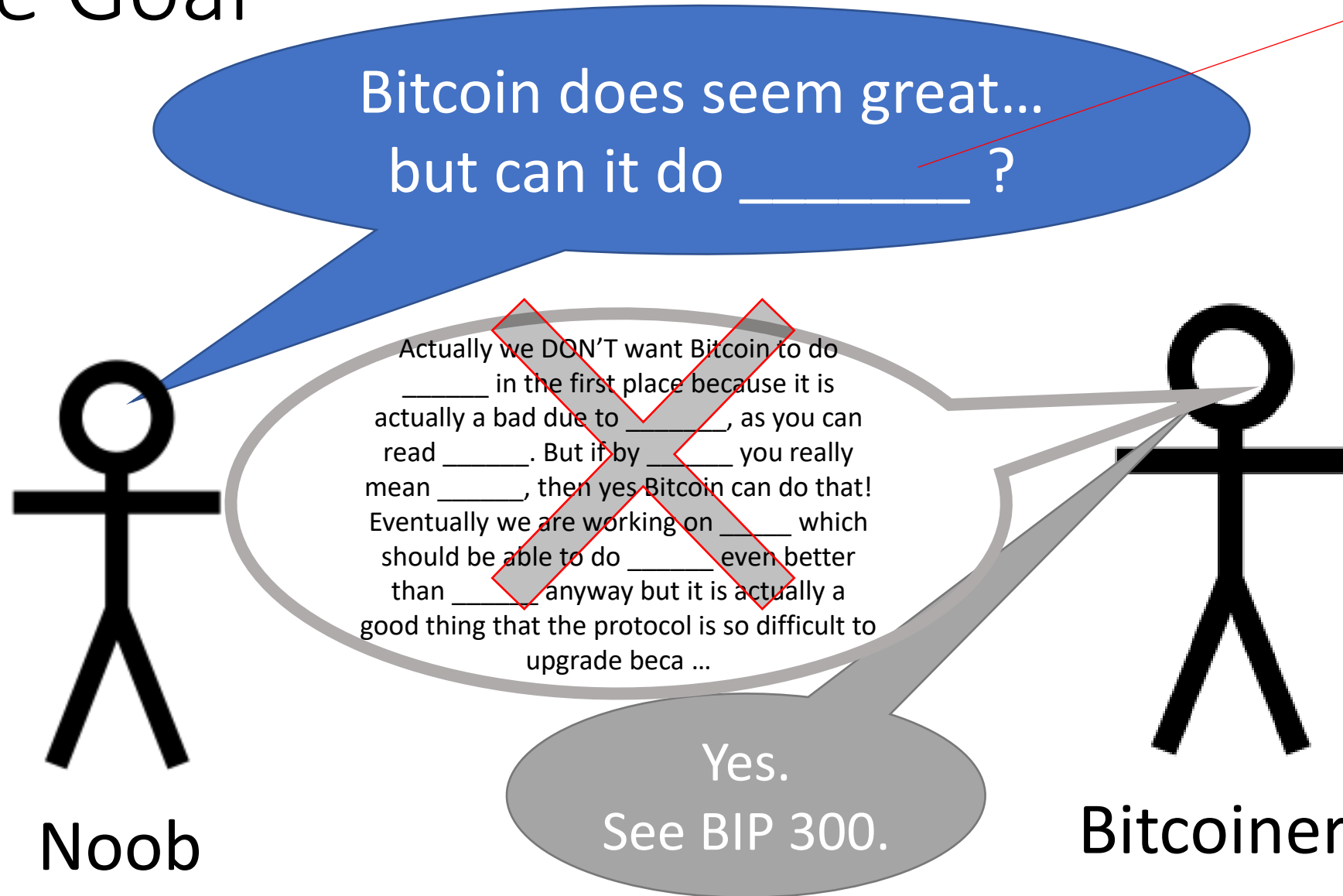
Paul Sztorc

Bitcoin2021 – June 4<sup>th</sup>

# The Concept, in One Slide



# The Goal



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

# Fringe Ideas

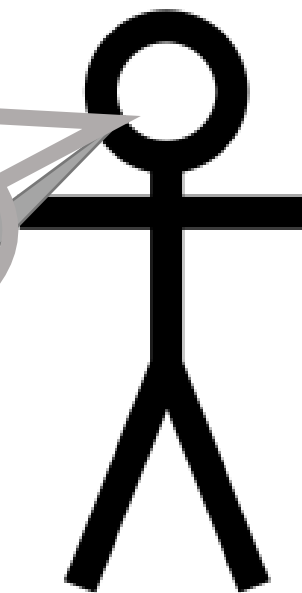
I can improve Bitcoin! It only  
needs my new idea: \_\_\_\_\_ !!  
When can you merge my code ??



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!!

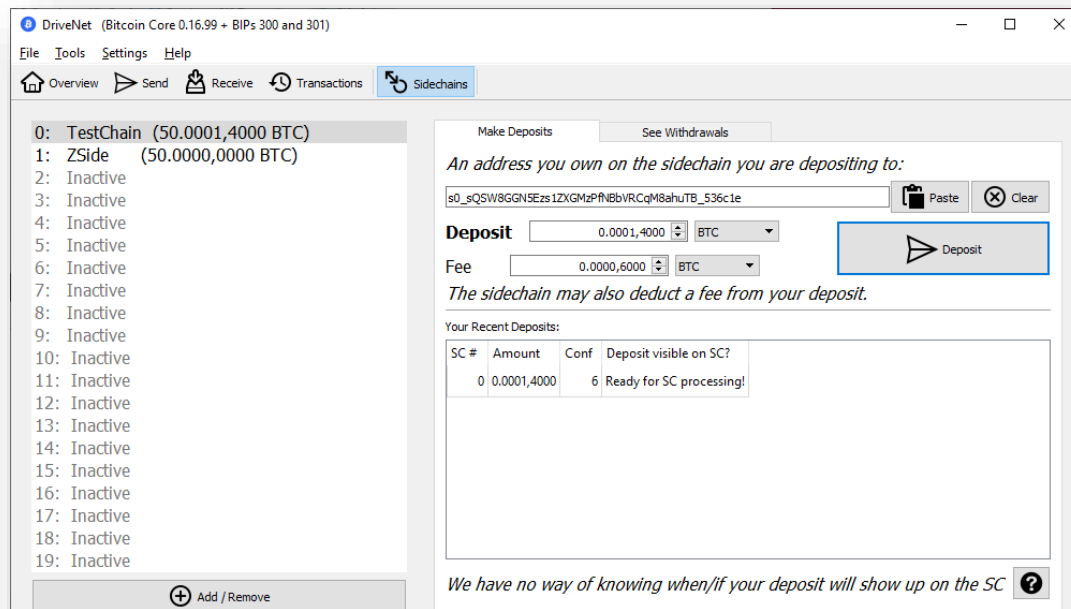
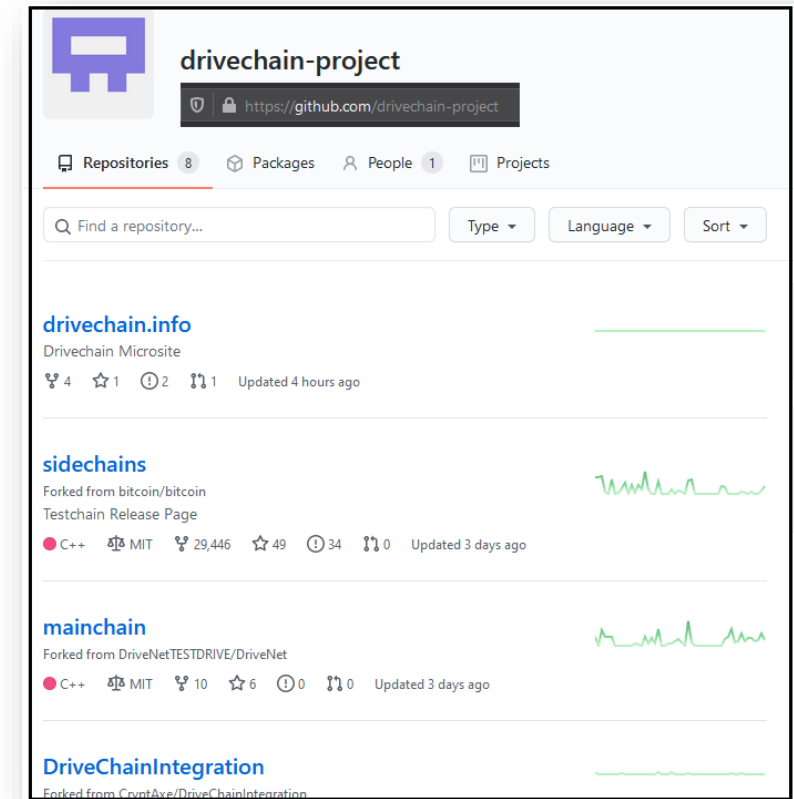


Bitcoiner

# Three Aspects

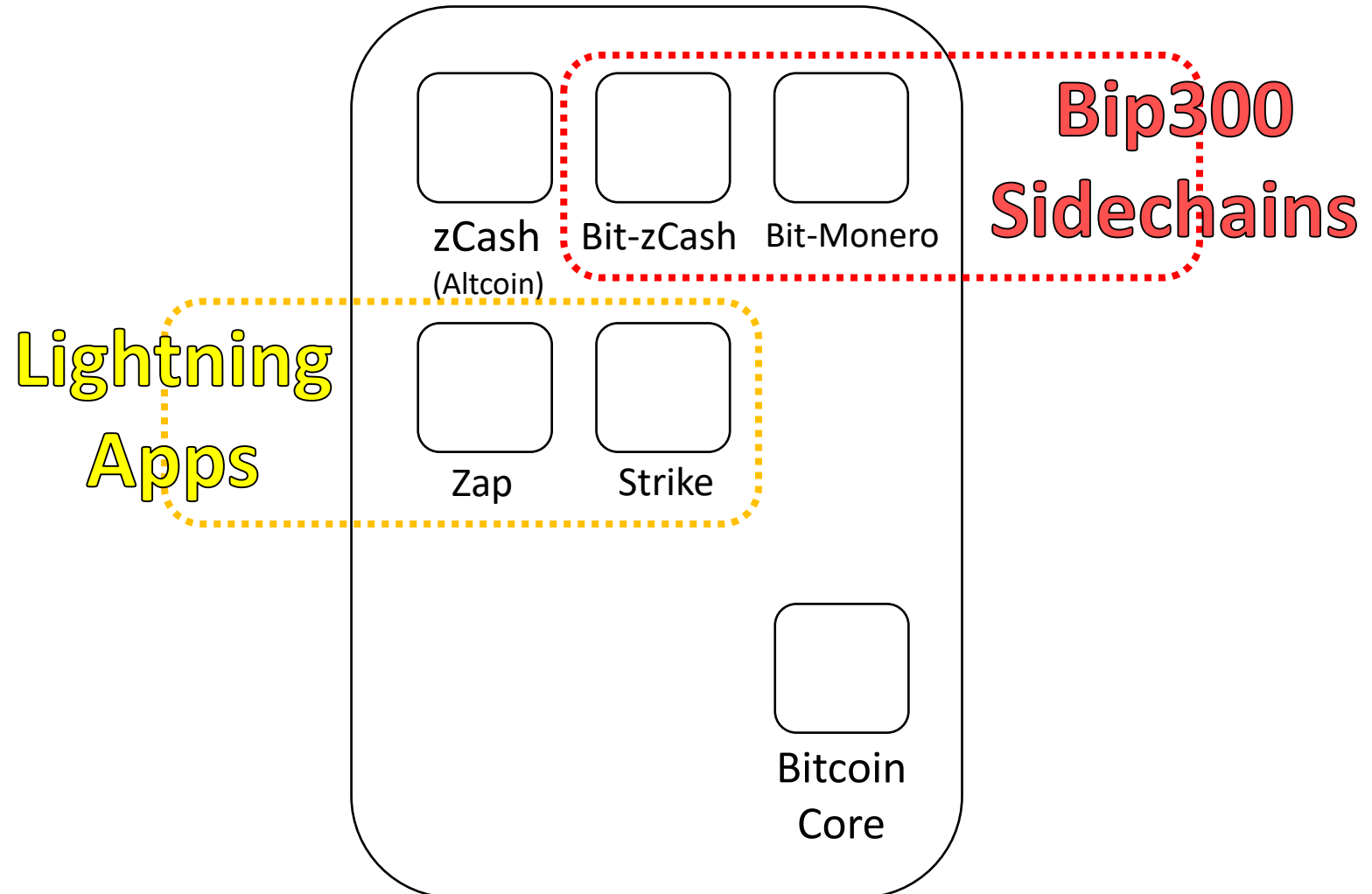
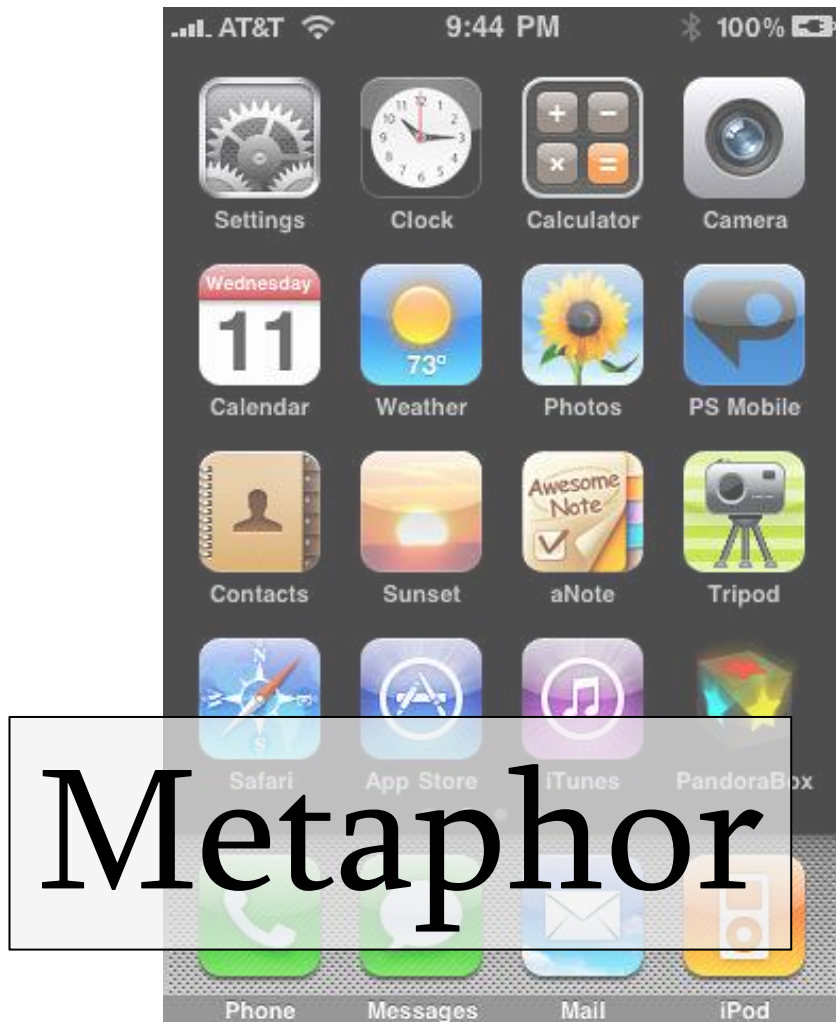
1. Full Autonomy
2. Protect Base Layer
3. Improve Miner Incentives

# Not Vaporware

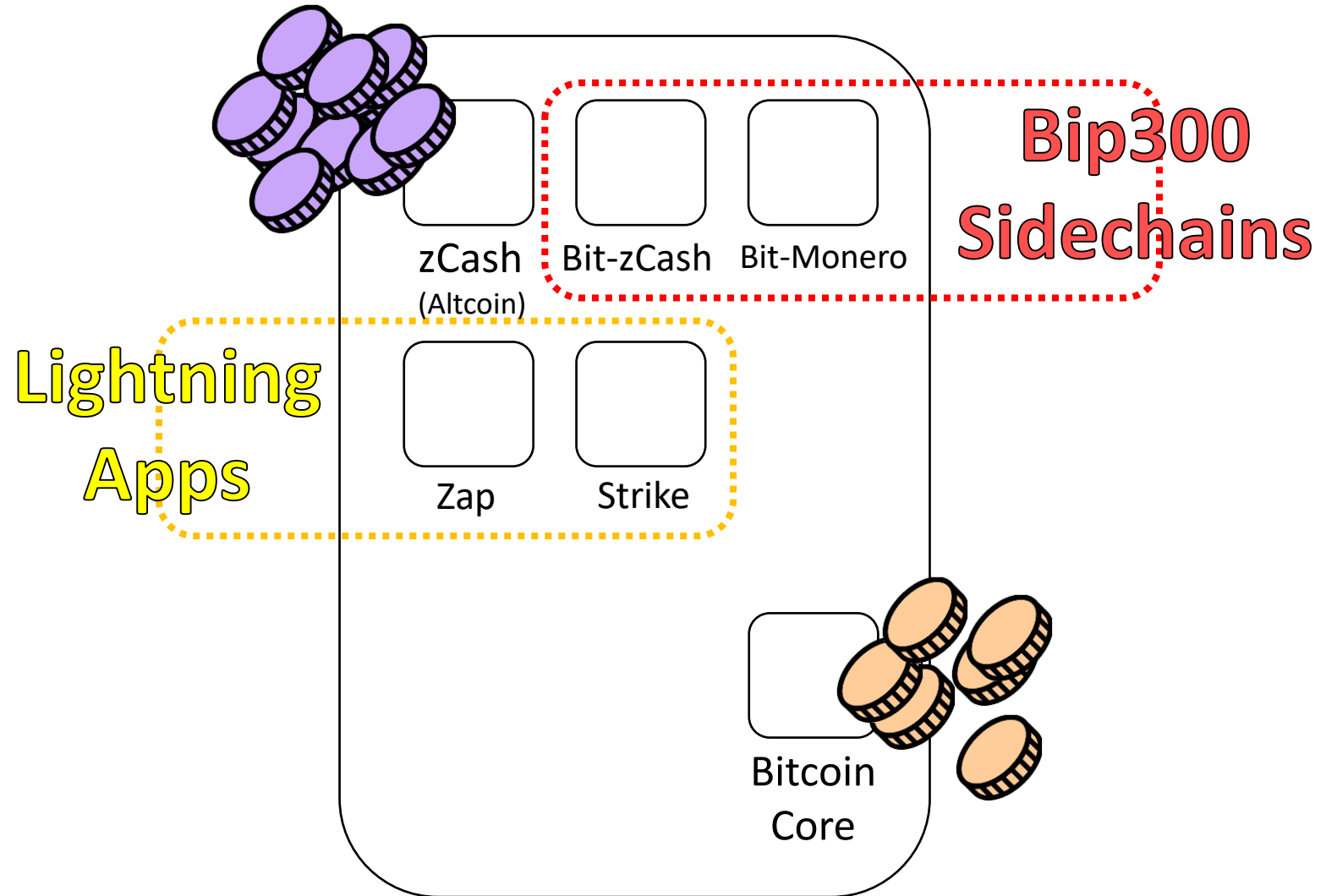




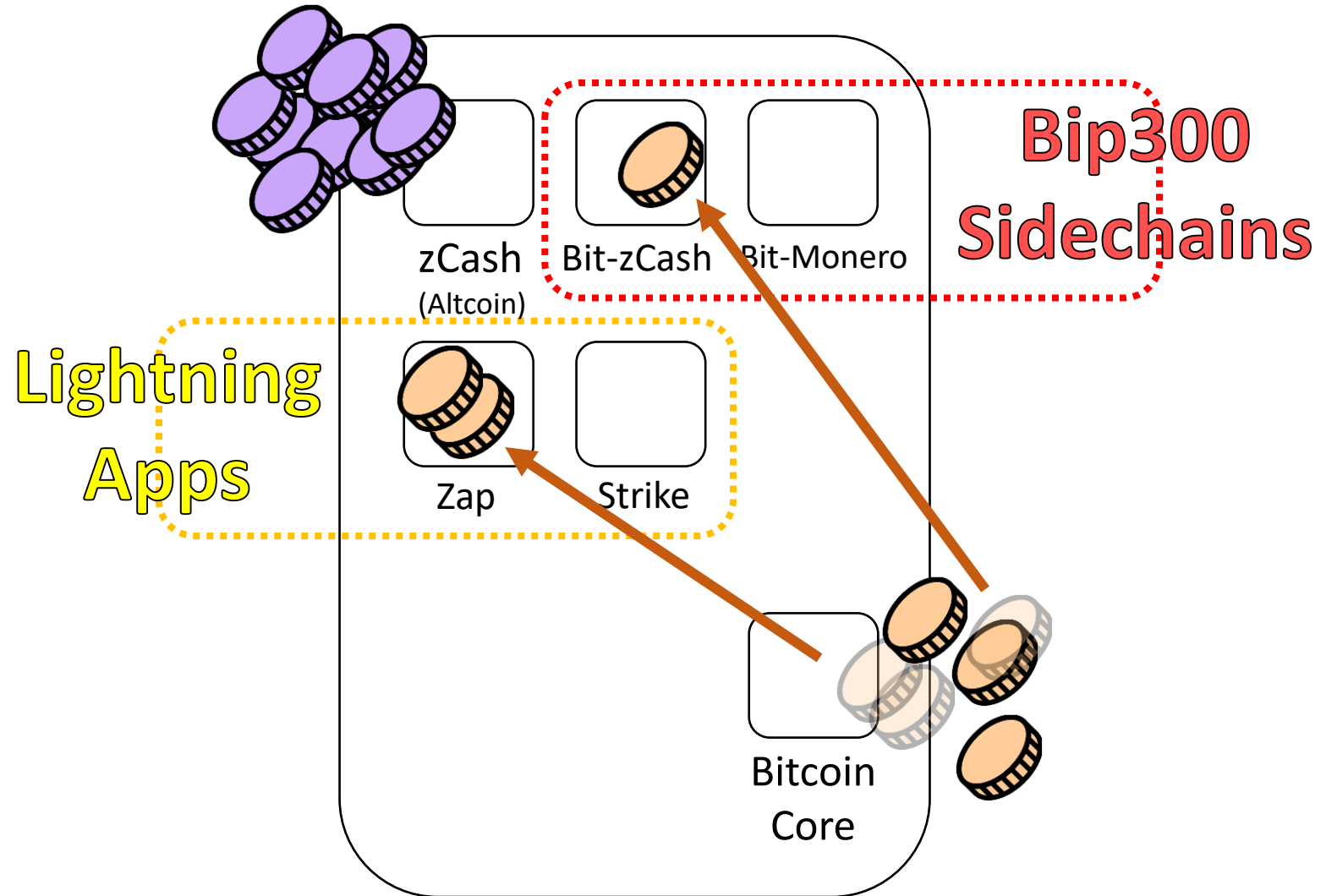
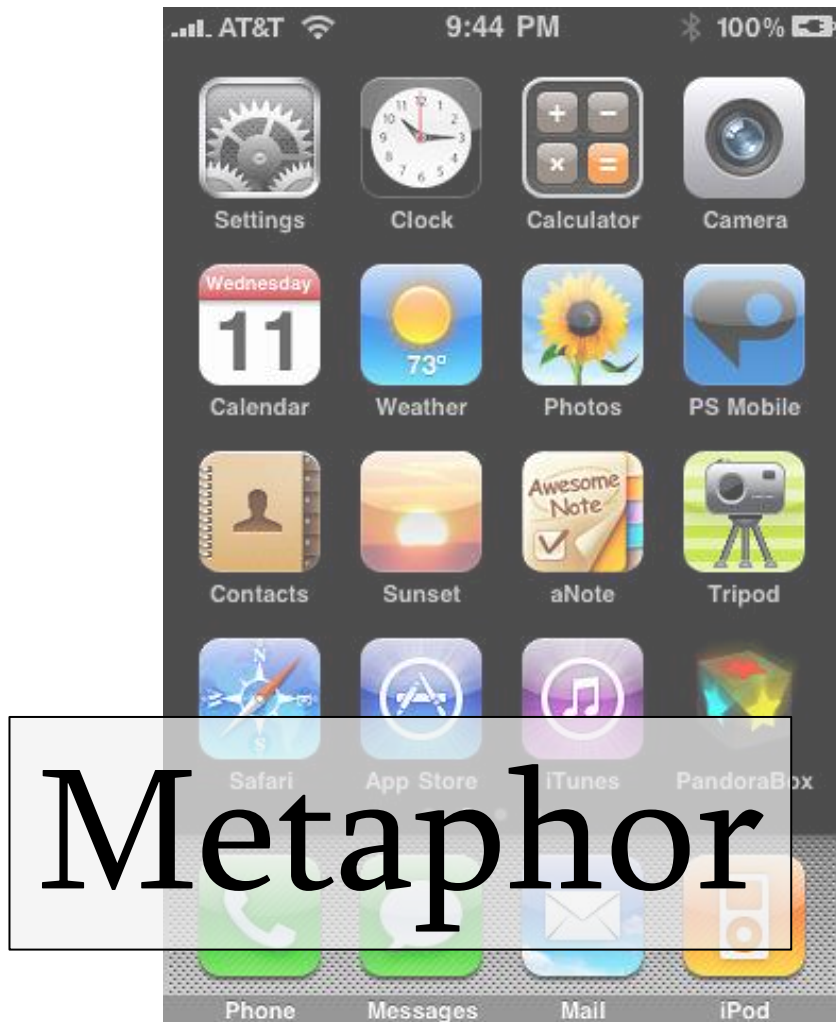
# (#1) Full Autonomy



# (#1) Full Autonomy



# (#1) Full Autonomy





# (#2) Base Layer is Safe



December 2020

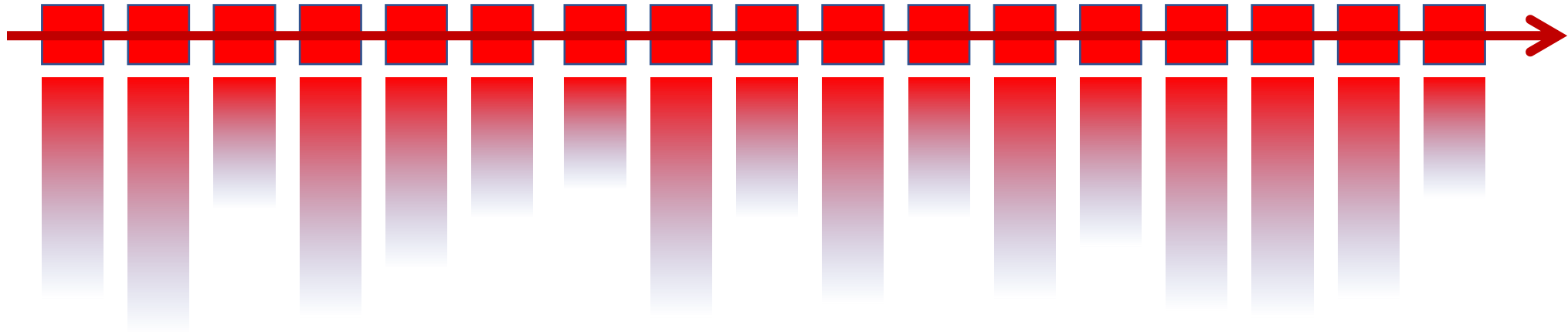
January 2021

February 2021

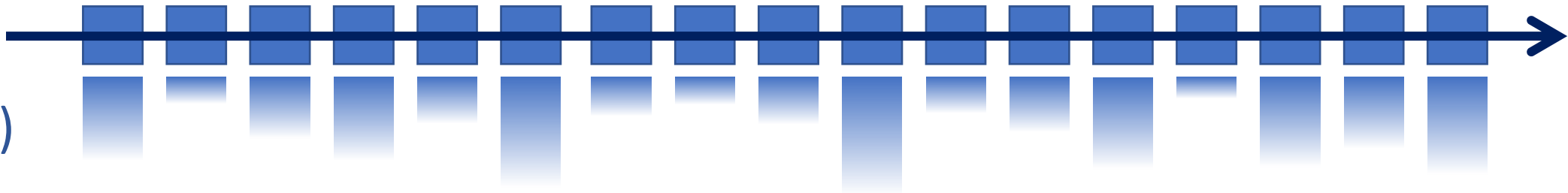
March 2021

April 2021

Layer 2  
(Bit-Monero)



Layer 1  
(Bitcoin Core)



# (#2) Base Layer is Safe



December 2020

January 2021

February 2021

March 2021

April 2021

Layer 2  
(Bit-Monero)

3 Months = One 32-byte Hash

3 Months = One 32-byte Hash

e320b6c2fffc8d750423db8b1eb942ae710e951ed797f7affc8892b0f1fc122b

81cd02ab7e569e8bcd9317e2fe99f2de44d49a

Layer 1  
(Bitcoin Core)

Inserted into Layer1 coinbase txn

# (#3) Improve Mining Incentives (Bip 301)

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

TrainChain - Wallet

File Settings Help

Parent Chain Overview Send Receive Transactions

Transfer Withdrawal Explorer BMM Total sidechain wealth: 3 480.1356,0000 SC1

Start Stop Bid Amount: 0.0001,0000 SC1 Refresh: 1 Second(s) Manual

Your Attempts:

MC txid	MC Block	SC Block	Txns	Fees	Bid Amount	Profit	Status
0993d15f0a7...	5323	515	1	0.0000,0000 SC1	0.0001,0000 BTC	-0.0001,0000 SC1	Trying...
551b9f0128d...	5322	515	1	0.0000,0000 SC1	0.0001,0000 BTC	-0.0001,0000 SC1	Success
a72505eadd2...	5321	515	1	0.0000,0000 SC1	0.0001,0000 BTC	-0.0001,0000 SC1	Failed
90fc56a2af8c...	5319	515	1	0.0000,0000 SC1	0.0001,0000 BTC	-0.0001,0000 SC1	Failed
f08d7b77789...	5319	515	1	0.0000,0000 SC1	0.0001,0000 BTC	-0.0001,0000 SC1	Failed
2f0d3c687ee...	5319	514	1	0.0000,0000 SC1	0.0001,0000 BTC	-0.0001,0000 SC1	Failed
d8bce6afac9...	5318	513	1	0.0000,0000 SC1	0.0001,0000 BTC	-0.0001,0000 SC1	Success
688eaa74193...	5317	513	1	0.0000,0000 SC1	0.0001,0000 BTC	-0.0001,0000 SC1	Success
56b5127deb...	5316	513	1	0.0000,0000 SC1	0.0001,0000 BTC	-0.0001,0000 SC1	Failed

WT^: None yet. Waiting for withdrawals. | 515 blocks | 0 peers | Last block: 1 minute ago

## Crypto Fees

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

Layer 1 x Share Filters 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/> this morning.

# What do we use BIP 300 for...?

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

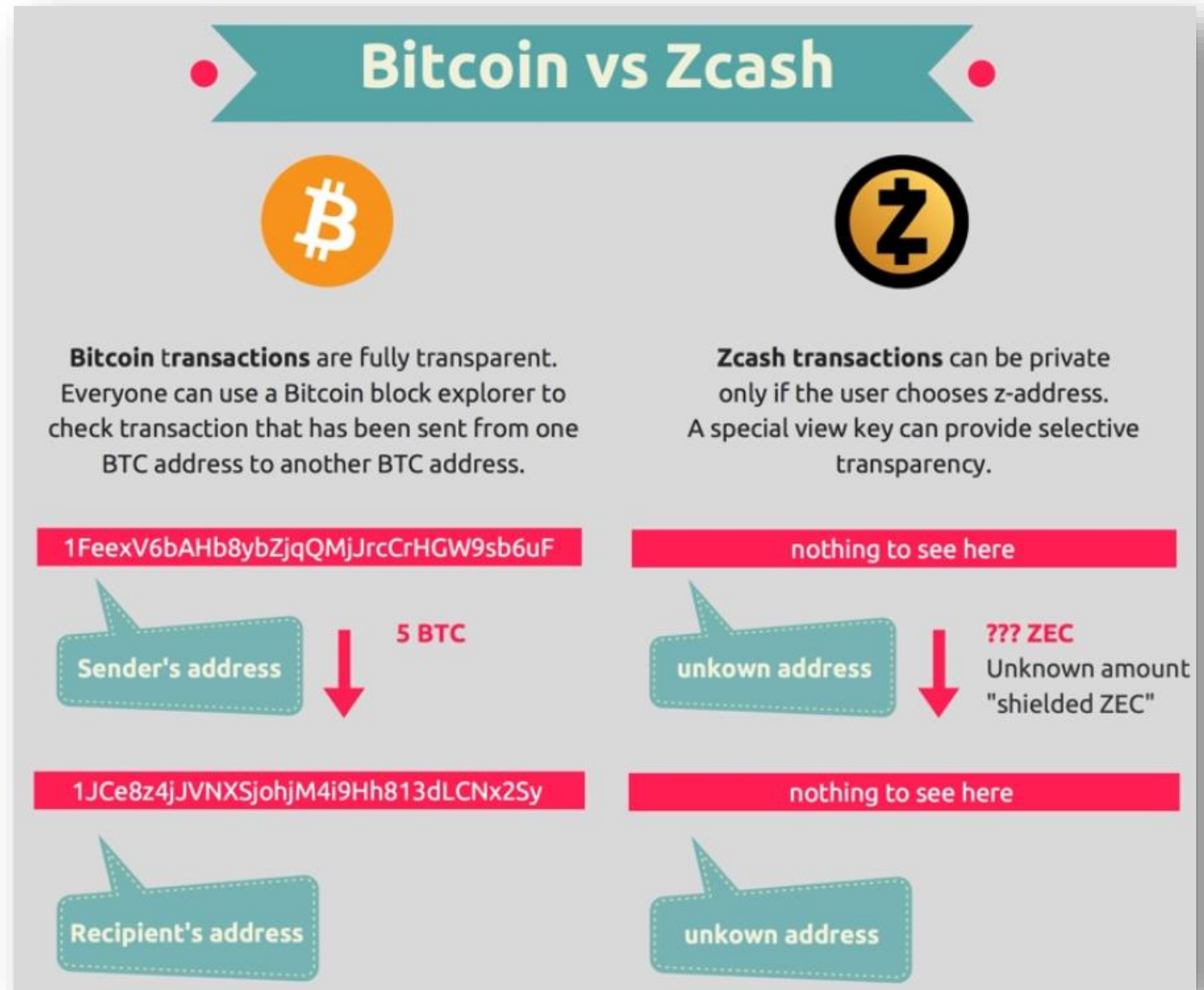


Art: "When I paint my masterpiece" – Nick Kenrick (?) - Creative commons license



# Altcoins we should copy (?): zCash

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





# Losing Customers to Monero (?)

[thecryptobasic.com/2020/12/31/darknet-marketplace-now-accepts-monero-only-not-bitcoin/](https://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

Fun facts -- in this thread, Satoshi:

- \* Invents what is now known as Merged Mining.
- \* Assumes that there will be many different blockchains that pay different fees (as if this were non-controversial!).
- \* The term "side chain" is used numerous times!

**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)*



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.

**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 reward from the bitdns n (which of course, slows down the main bitcoin work), what would be a miner's incentive to include bitdns chains) ?

The incentive is to get the rewards from the extra side chains also for the same work.

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](#)

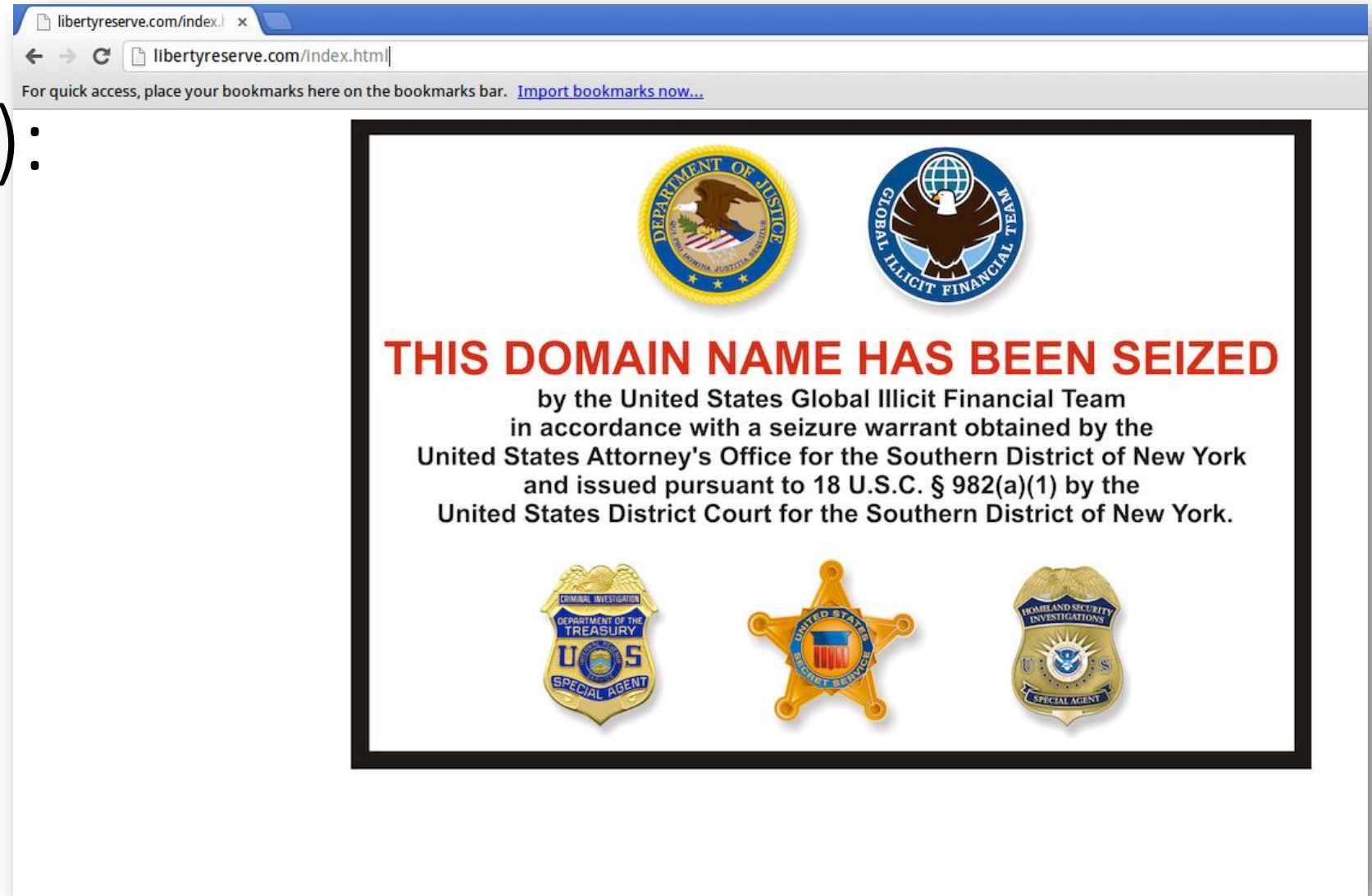
Altcoins we  
should copy (?):  
NameCoin

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/](http://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.<sup>[1]</sup> 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.<sup>[2]</sup> The NFT market value tripled in 2020, reaching more than \$250 million.<sup>[3]</sup>

So lame!!



Logo used to represent non-fungible tokens

### Contents [\[hide\]](#)

#### 1 [Description](#)

# 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>

**3.3PB**

Storage Capacity

**556**

Storage Providers

**913TB**

Used Storage

**1.2M**

Downloads

# Prediction Markets

- Screenshots from my own BTC sidechain project

[www.BitcoinHivemind.com](http://www.BitcoinHivemind.com)

The screenshot shows the Hivemind Core - Wallet [testnet] interface. The top menu bar includes File, Settings, and Help. Below it, a navigation bar has 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".

The main content area is divided into two panels. The left panel, titled "Recent Hivemind Objects:", displays a list of objects with their Type/Icon and description:

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

The right panel shows the "Balances" and "Recent transactions".

**Balances**

Available:	400.00000000 BTC
Pending:	0.00000000 BTC
Immature:	50.00000000 BTC
<b>Total:</b>	<b>450.00000000 BTC</b>

**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](http://www.BitcoinHivemind.com)

The screenshot displays the Hivemind Core - Wallet [testnet] interface. The top menu bar includes File, Settings, and Help. Below it, a navigation bar shows Overview, Send, Receive, Transactions, Markets (selected), Decisions, Author, and Vote. The main content area is divided into two columns: Graph and Market Info.

**Graph Section:**

- Unemployment drivers:** A line graph showing a fluctuating trend with a peak.
- Fire Immelt?:** A line graph showing a sharp, isolated peak.

**Market Info Section:**

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



# Prediction Markets

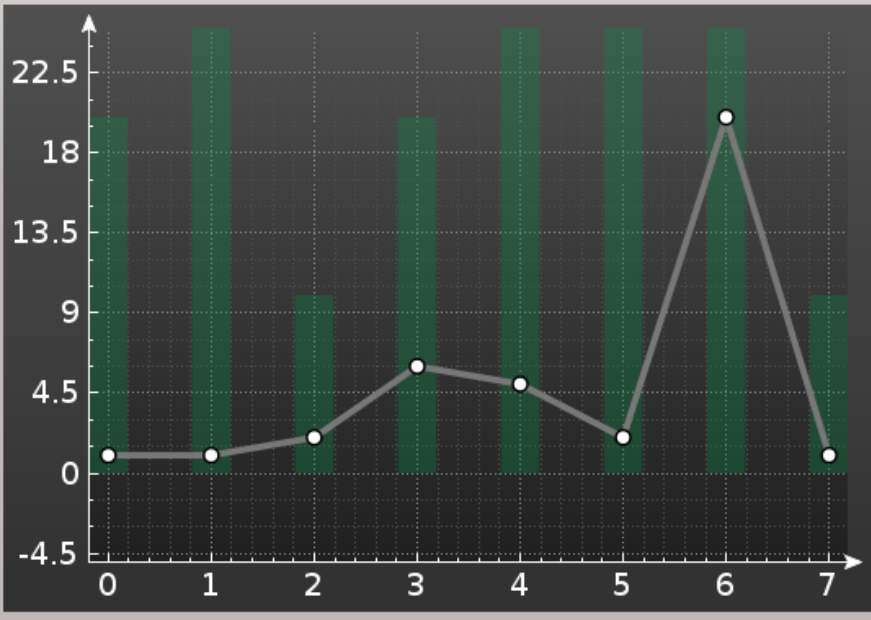
- Screenshots from my own BTC sidechain project

Trade [www.BitcoinHivemind.com](http://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

☒ Long (Buy) ☐ Short (Sell)

Make Order [? Help](#)

# Shares: 0

Price: 0.00

☒ Finalize

# 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 'Recent Hivemind Objects' list with icons and names like 'Bitcoin', 'Will', 'Glob', 'Will', and 'Une'. It also has a 'Type/Icon' dropdown and a 'Tags' input field.
- Market Graph:** A line graph showing price over time. The y-axis ranges from -4.5 to 22.5. The x-axis shows time steps from 0 to 7. The graph is labeled 'Market Graph: 1 Month 1 Day 5 Minutes'. The data points are approximately: (0, 0.5), (1, 0.5), (2, 1.5), (3, 6.5), (4, 5.5), (5, 2.5), (6, 19.5), (7, 1.5).
- Trading Controls:** Includes a 'Long (Buy) Short (Sell)' selector, 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 is also a 'Payout Address' input field.
- Summary:** Shows '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.

# 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*

# How to Get Bip300 Faster

1. Learn !
  - Download the latest version
2. Talk
  - Soft forks need consensus
  - Invite on podcasts/whatever
3. View Altcoins Differently

**[drivechain.info/releases/](https://drivechain.info/releases/)**

Drivechain = Bip 300+301

## Releases

### Download Latest Version (June 1st, 2021)

Software	Linux	Windows	Mac	Source
Mainchain v38	<a href="#">tar.gz</a>	<a href="#">.exe</a>	n/a	<a href="#">Github</a>
Testchain v11	<a href="#">tar.gz</a>	<a href="#">.exe</a>	n/a	<a href="#">Github</a>
Trainchain v2k	<a href="#">tar.gz</a>	<a href="#">.exe</a>	n/a	<a href="#">Github</a>
Thunder v3	<a href="#">tar.gz</a>	<a href="#">.exe</a>	n/a	<a href="#">Github</a>
zSide v3	<a href="#">tar.gz</a>	n/a	n/a	<a href="#">GitLab</a>

Click [here](#) for CHECKSUMs

## LINKS

- [Home](#)
- [Github](#)
- [Release](#)
- [Block Ex](#)
- [Articles](#)
- [Literatu](#)
- [FAQ](#)
- [Peer Re](#)
- [Telegra](#)
- [Twitter](#)
- [Reddit](#)
- [Sidecha](#)
- [Truthcoin](#)
- [Bitcoin Hi](#)





# Thank You

for Your Attention!

(Find me and talk to me!)