

April 14th, 2023

Hong Kong

LayerTwo Labs – A Drivechain Company

Paul Sztorc

Creator: BIPs 300/301 ; truthcoin.info
Presenter: Scaling Bitcoin I-IV, MIT Bitcoin Club,
Bitcoin 2019-2023, Baltic Honeybadger, etc.

CryptAxe

Bitcoin Core Dev: 0.14, 0.15, 0.16.
Infrastructure engineer: BIPs 300/301.
Creator: sidechain template, DeFi/BitAsset sidechain.

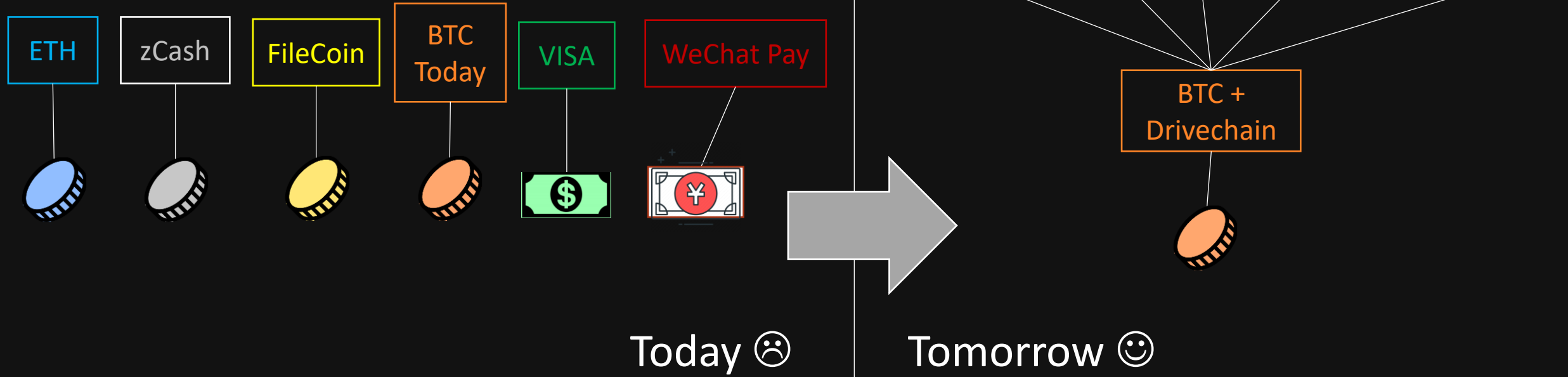
Austin Alexander

Sales & Biz Dev @ Kraken (2014-2022)
CEO @ Kraken MENA (2019 -2021)
Co-Founder @ Bitcoin Center NYC (2013)

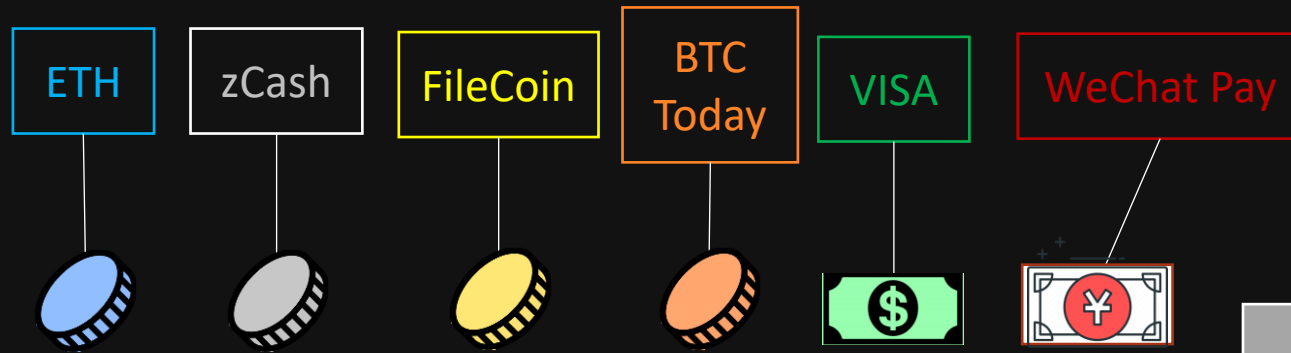
Nikita Chashchinskii

Creator of the zCash Sidechain, Bip300
Bridge Module, EVM Sidechain, &
switchboard launcher.

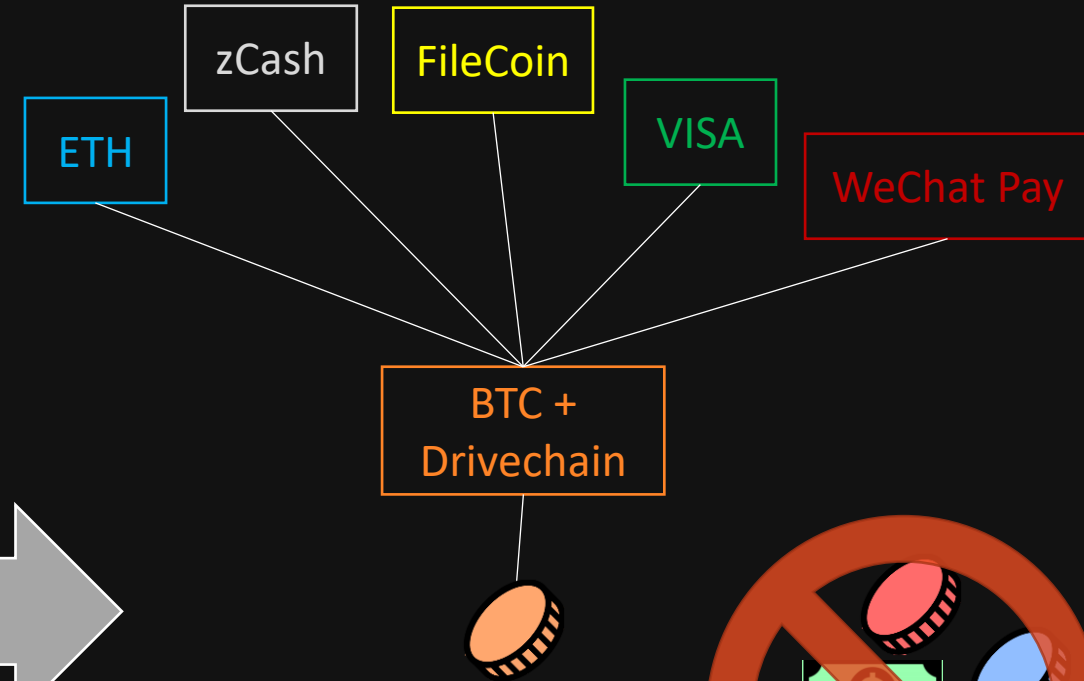
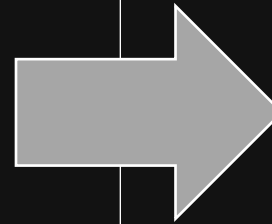
Everything on Top of Bitcoin



Everything on Top of Bitcoin



Today ☹️



Tomorrow 😊



The Coming Death of Bitcoin's Competitors



BTC
Today

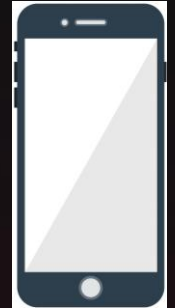
WeChat Pay

zCash

VISA

ETH

FileCoin



BTC +
Drivechain

“

**Drivechain
arguably
more useful
than
Taproot.**

Adam Back,
Founder of Blockstream



“

**Drivechain is our only
hope.
... We need Drivechain
or all the work of
thousands in the last 13
years will be in vain.**



Fiatjaf,
Creator of Nostr

Friends of Drivechain

Olaoluwa Osuntokun,
CTO of Lightning Labs

"In the past year, the drivechain specs seem to have come a long way."



Ruben Somsen,
Bitcoin Sorcerer and Creator of
Spacechains

"I would like to see Drivechains happen and run it as an experiment and see how it goes."



Anton Kumaigorodski,
LN developer

"Here's another project which I think is more critical than LN for bitcoin's long term survival"



Hampus Sjöberg,
Creator of Blixt Lightning
Wallet, Programmer, EDM producer,
Bitcoin fanatic

"We better work on actual real solutions (BIP300 drivechains) rather than nonsensical ones."



visit LayerTwoLabs.com for more

Friends of Drivechain

Brad Mills,
Host of the Magic Internet Money
podcast

"I think it's time the Bitcoin community took a more serious look at @Truthcoin's drivechain proposal."



Eric Wall,
Investor and Software Engineer

"it's been 7 years since @Truthcoin wrote the original drivechain blog post. if you went back in time and told me that 7 years later no effort has been made towards merge-mined sidechains but that the same people who opposed them were upset ethereum existed i'd laugh in your face"



Nic Carter,
Founder and General Partner,
Castle Island Ventures

"I agree with all of this"



Ari Paul,
Founder and Chief Investment
Officer of BlockTower Capital

"...Drivechains are at least 4 years old. The LN whitepaper was 2016. If there had been aggressive innovation (from the user functionality perspective) on this stuff, I'd agree it would have taken the wind out of many altcoin sails, but there wasn't so it didn't."



visit LayerTwoLabs.com for more

Friends of Drivechain

Hampus Sjöberg,
Creator of Blixt Lightning
Wallet, Programmer, EDM producer,
Bitcoin fanatic

"We better work on actual real solutions (BIP300
drivechains) rather than nonsensical ones."



CalleBTC,
Physicist, Programmer, Lightning
dev

"I support BIP-300."



Checkmate,
Lead On-chain Analyst at
Glassnode

"When will people start taking Drivechains seriously?"



Aaron van Wirdum,
Journalist at Bitcoin Magazine

"Surely you wouldn't prefer off-chain custodial accounts
(eg. Coinbase) over sidechain balances (eg. Drivechain)?"



"Custodial services can steal your bitcoin successfully 100%
of the time. How can sidechains be worse than that?"



visit LayerTwoLabs.com for more

Friends of Drivechain

Peter McCormack,
Host of the What Bitcoin Did
podcast

"I like that fact that it just gives me one currency to go around and do all these other things, I like that a lot so that's cool."



Edan Yago,
Cheerleader-In-Chief of Sovryn

"The only thing missing from Bitcoin is that ability to adopt any feature or technology without changing main chain. BIP 300 fixes this."



Guy Swann,
Host of the Bitcoin Audible
podcast

"I feel like sidechains are an inevitable part of the ecosystem for multiple reasons, & I simply see BIP300 as a hashrate based sidechain rather than a federated multisig. I 100% agree on the alts issue, but that's not why i am interested in it."



visit LayerTwoLabs.com for more

How it Works



= Block
Header



= List of
transactions

December 2020

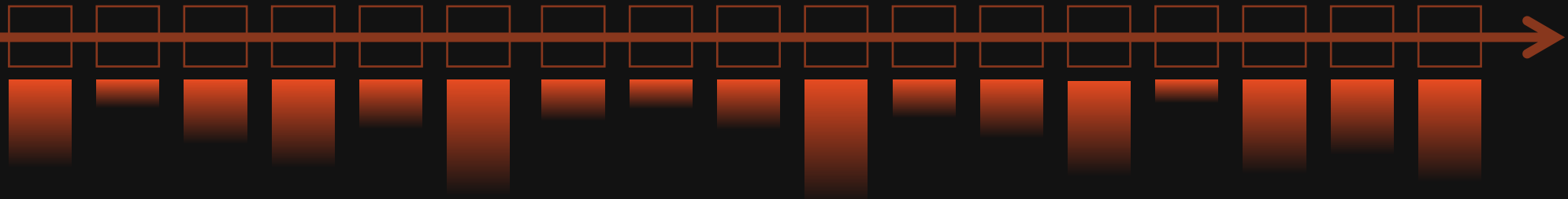
January 2021

February 2021

March 2021

April 2021

Base Layer
(Bitcoin Core)



How it Works



= Block
Header



= List of
transactions

December 2020

January 2021

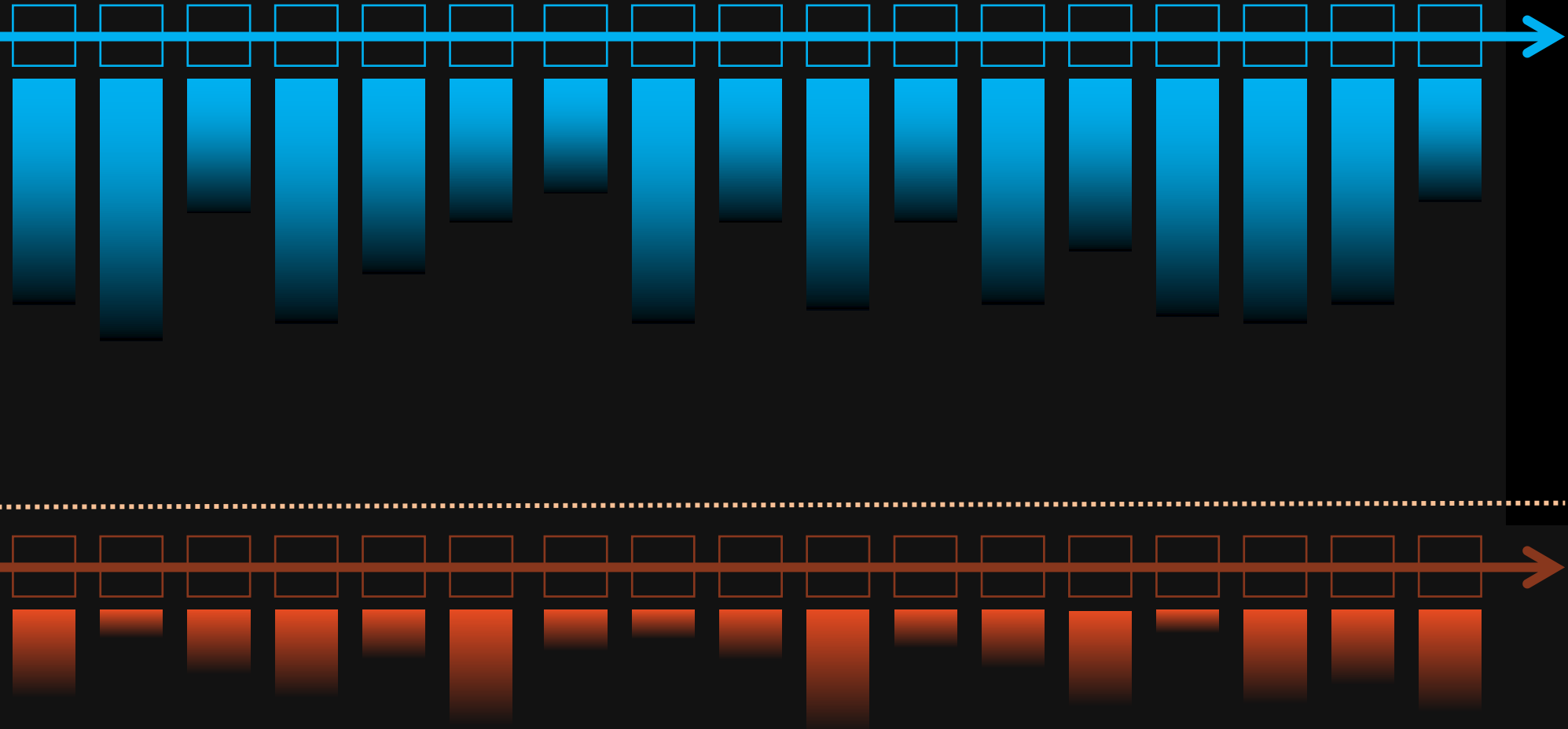
February 2021

March 2021

April 2021

Layer 2
(Bit-Monero)

Base Layer
(Bitcoin Core)



How it Works



= 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

Your Layer1 Node, Sees...

= Block Header

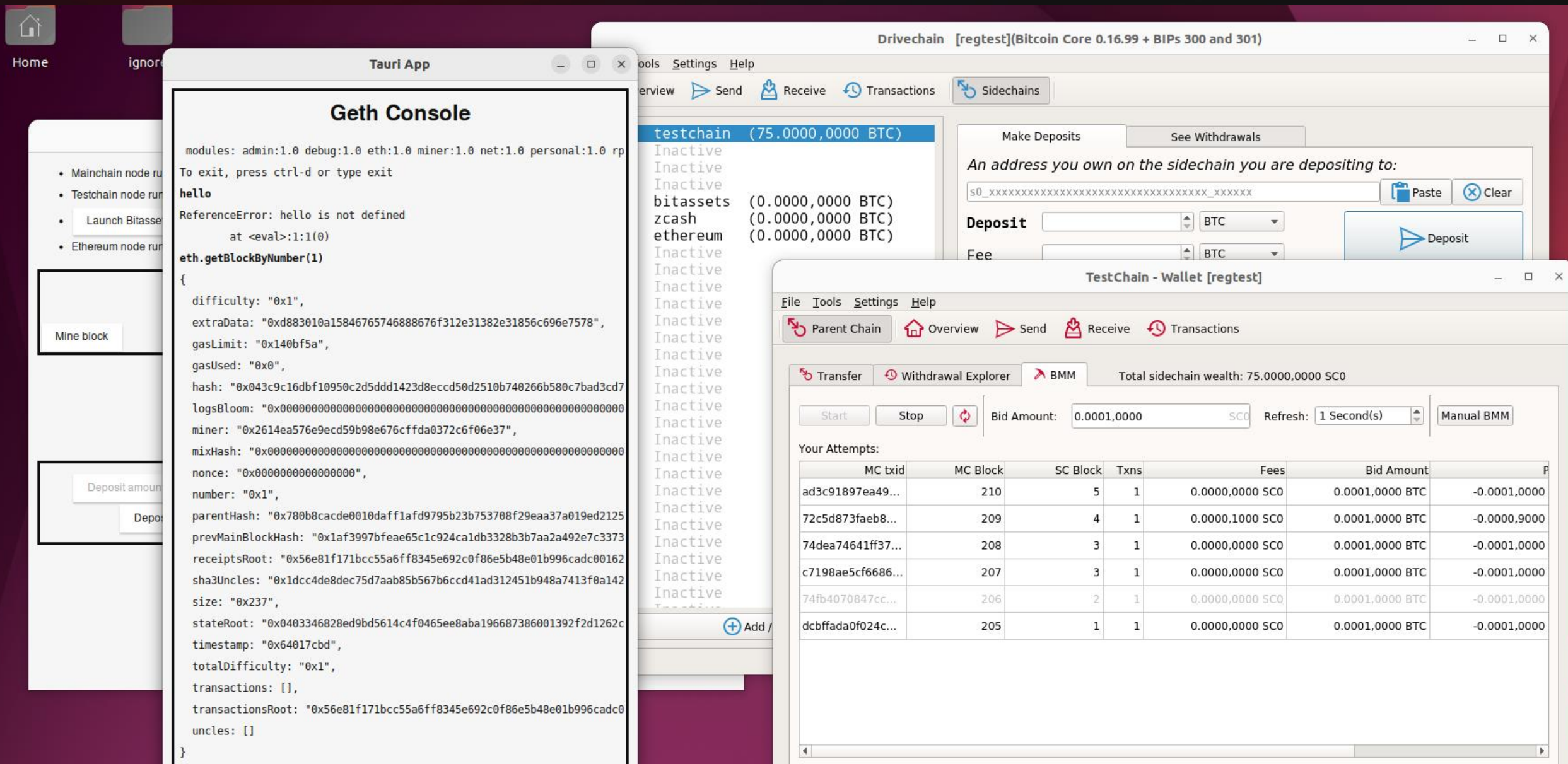
= List of transactions

December 2020 January 2021 February 2021 March 2021 April 2021

Base Layer
(Bitcoin Core)



Try Our Software -- see for yourself!



Try Our Software -- see for yourself!



drivechain.info

Six years of:

- Slides
- Me as a Podcast Guest
- Technical Documentation
- Software
- Endorsements
- Peer Review
- FAQ
- Memes

Individual Binaries and Sources

MAINCHAIN (V44.00)

Software	Linux	Windows
Mainchain v44	tar.gz	.exe

SIDECHAINS BASED ON TEMPLATE

Software	Linux	Windows
Sidechain Template v18.00	tar.gz	.exe
zCash-DC v9.0.0	tar.gz	.exe
BitAssets v4.00.0	tar.gz	.exe
Thunder v8.00.00	tar.gz	.exe
Trainchain v81	tar.gz	.exe

SIDECHAINS BASED ON CLONING ALTCOIN

Software	Linux
Latest Ethereum	Guide, Video
Latest zCash	Guide, Video

 [Github](#)

 [Releases](#)

 [Block Explorer](#)

 [Articles](#)

 [Literature](#)

 [FAQ](#)

 [Friends of Drivechain](#)

 [Telegram](#)

 [Twitter](#)

 [Reddit](#)

 [Sidechain Projects](#)

BIPS

Drivechain is made of two BIPs:

1. [BIP 300 \(Hashrate Escrows\)](#) – “Container UTXOs” that compress 3-6 months of transaction data into a fixed 32-bytes.
2. [BIP 301 \(Blind Merged Mining\)](#) – A technique to replace the act of running a sidechain node with the act of including a single high-fee transaction.

SELECTED RECENT PODCASTS

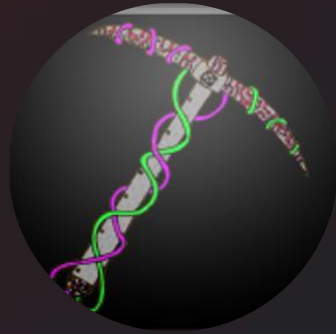
1. [Van Wirdum Sjorsnado #23](#) – (see my [comments](#))
2. [51 Minutes \(0:26:00 to 1:17:40\)](#) during an Oct 14 Whalepool Talk on Bitcoin, Drivechain, and Hivemind

TEAM



Paul Sztorc

Creator of BIPs 300/301, Bitcoin Consultant & Presenter (Scaling Bitcoin, Bitcoin 2019/2021/2022, Consensus NYC, TABconf, Qcon etc). Fmr Software Engineer @ Yale Econ dept (2012 - 2015).



CryptAxe

Bitcoin Core developer (2016-Present; 0.14, 0.15, 0.16). Infrastructure engineer BIPs 300/301. Creator of sidechain template, BitAsset sidechain, zCash sidechain GUI.



Austin Alexander

Kraken - Business development (2014-2022)
*Kraken MENA - CEO (2019-2021) *NYC Bitcoin Center - co-founder (2013-2014)



Nikita Chashchinskii

Creator of the zCash Sidechain, Bip300 Bridge Module, & EVM Sidechain.

TEAM



Each 10+ Years Bitcoin Experience

Paul Sztorc

Creator of BIPs 300/301, Bitcoin Consultant & Presenter (Scaling Bitcoin, Bitcoin 2019/2021/2022, Consensus NYC, TABconf, Qcon etc). Fmr Software Engineer @ Yale Econ dept (2012 - 2015).



CryptAxe

Bitcoin Core developer (2016-Present; 0.14, 0.15, 0.16). Infrastructure engineer BIPs 300/301. Creator of sidechain template, BitAsset sidechain, zCash sidechain GUI.



Austin Alexander

Kraken - Business development (2014-2022)
*Kraken MENA - CEO (2019-2021) *NYC Bitcoin Center - co-founder (2013-2014)



Nikita Chashchinskii

Creator of the zCash Sidechain, Bip300 Bridge Module, & EVM Sidechain.

The Benefits

- The 21M coins, can travel to/from other blockchains. Or stay on L1.
- Blockchains become sort of like optional plug-ins. One à la carte super-coin.

Investors:

- Technical innovation never threatens your coin-investment.
- All investors united in one team, against fiat.
- No need to “fund development” – just copy other’s code.
- Safely ignore all technical squabbles, & enjoy all innovation.

Users:

- Get every feature of every crypto-coin. (Plus: no gas fees.)
- Competition ensures rapid progress on whatever *problem du jour* – MEV, Censorship, etc.
- Culture no longer rewards *toxicity* – there is no need to feel threatened by change/novelty.
- Rewards creativity & innovation, instead of stasis & defense.

Development:

- Devs do as they like, no bureaucracy.
- Users switch blockchains like switching from Chrome to Firefox. Can “fire” / “hire” devs at will.
- Each dev is CEO/dictator of their own private realm, accountable only to their customers/users (who can leave at any time). Perfect incentive alignment.

Miners:

- Collect all fees from all blockchain transactions everywhere, while doing zero additional work.
- Ensures *maximum* security budget, with minimal per-txn fees, and no violations of 21M coin limit.

Our Goals

- BTC gets immediate global scale & unbreakable privacy.
- Fees (on “per txn” basis) are always near-zero.
- Miner revenues grow exponentially, forever.
- L1 never changes again – maximum decentralization, zero bickering.
- Immediate, total creative freedom for devs – no lobbying, no toxicity.
- End of scam coins, scam marketing (& other distractions).
- Devs make useful blockchains – no to Ponzi-nomics, yes to coin-use.
 - NameCoin -- Revolution in Media / Free Speech / Social Media.
 - Prediction Markets – Prevent CEOs/Politicians from lying, double wGDP_g
- All this with zero risk to Bitcoin – 100% optional & reversible.

Our Goals

- BTC gets immediate global scale & unbreakable privacy.
- Fees (on “per txn” basis) are always near-zero.
- Miner revenues grow exponentially, forever.
- L1 never changes again – maximum decentralization, zero bickering.
- Immediate, total creative freedom for devs – no lobbying, no toxicity.
- End of scam coins, scam marketing (& other distractions).
- Devs make useful blockchains – no to Ponzi-nomics, yes to coin-use.
 - NameCoin -- Revolution in Media / Free Speech / Social Media.
 - Prediction Markets – Prevent CEOs/Politicians from lying, double wGDP_g
- All this with zero risk to Bitcoin – 100% optional & reversible.
- Our investors **make a fortune**.

The Last Slide!

- Nov 2015 | “Drivechain” blog post written
- Jan 2017 | Drivechain.info created
- Feb 2018 | Assigned BIP #s (300/301)
- Mar 2019 | 1st Bip300 sidechain
- June 2021 | zCash sidechain
- May 2022 | 4 sidechains total
- June 2022 | Eth Sidechain (5th sidechain)
- May 2022 | Gather co-founders, Retain Fenwick, Incorporate, 409A Valuation
- Sept 2022 | \$3M seed for product, legal, overhead, basic marketing.
- Apr 2023 | Second (and FINAL) round of Fundraising

END

Thank You

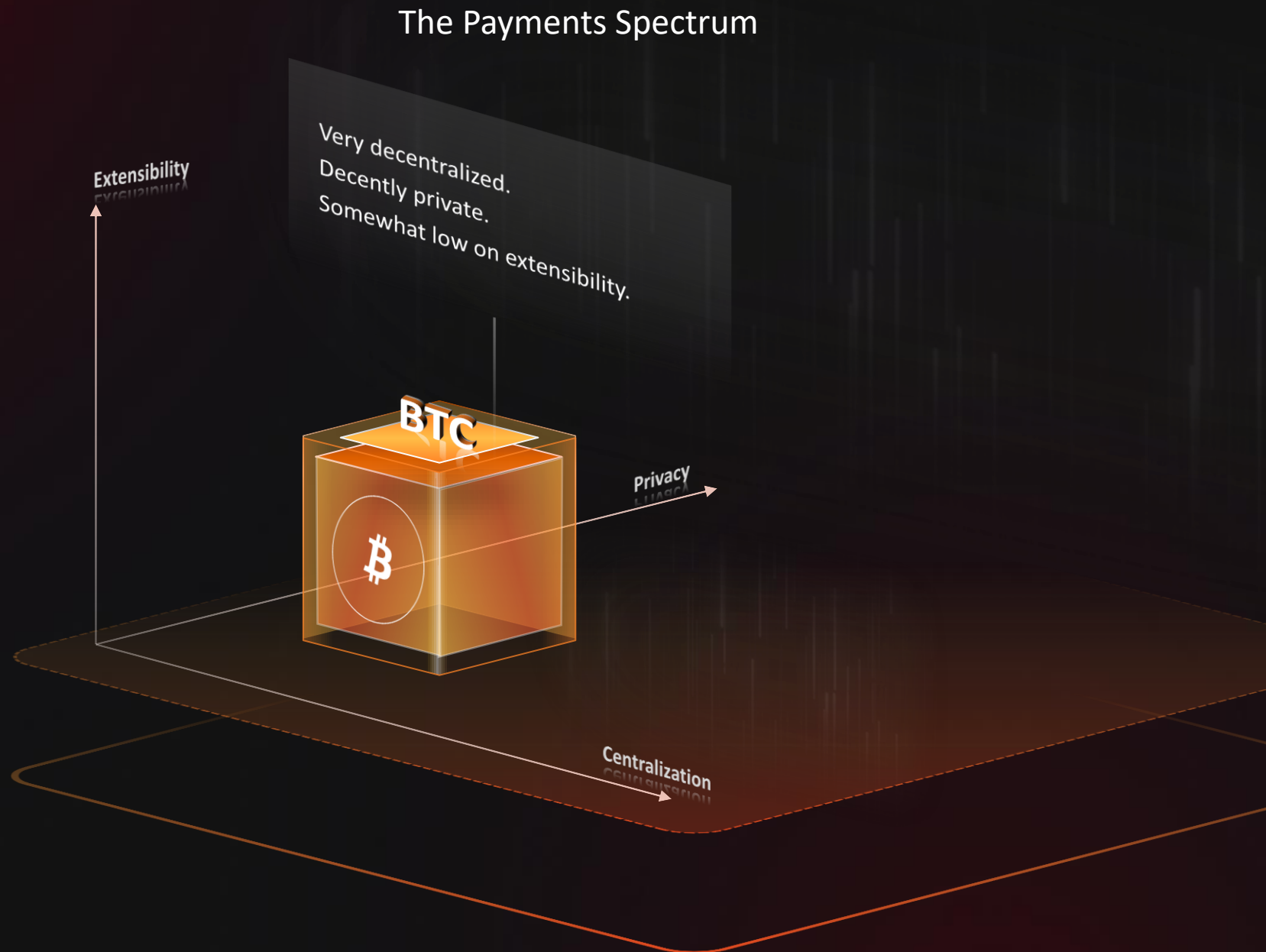
visit LayerTwoLabs.com
Drivechain.info
for more

Paul Sztorc
@truthcoin on Twitter
@psztorc on Telegram

Why Bip300

Bitcoin

One coin, one blockchain

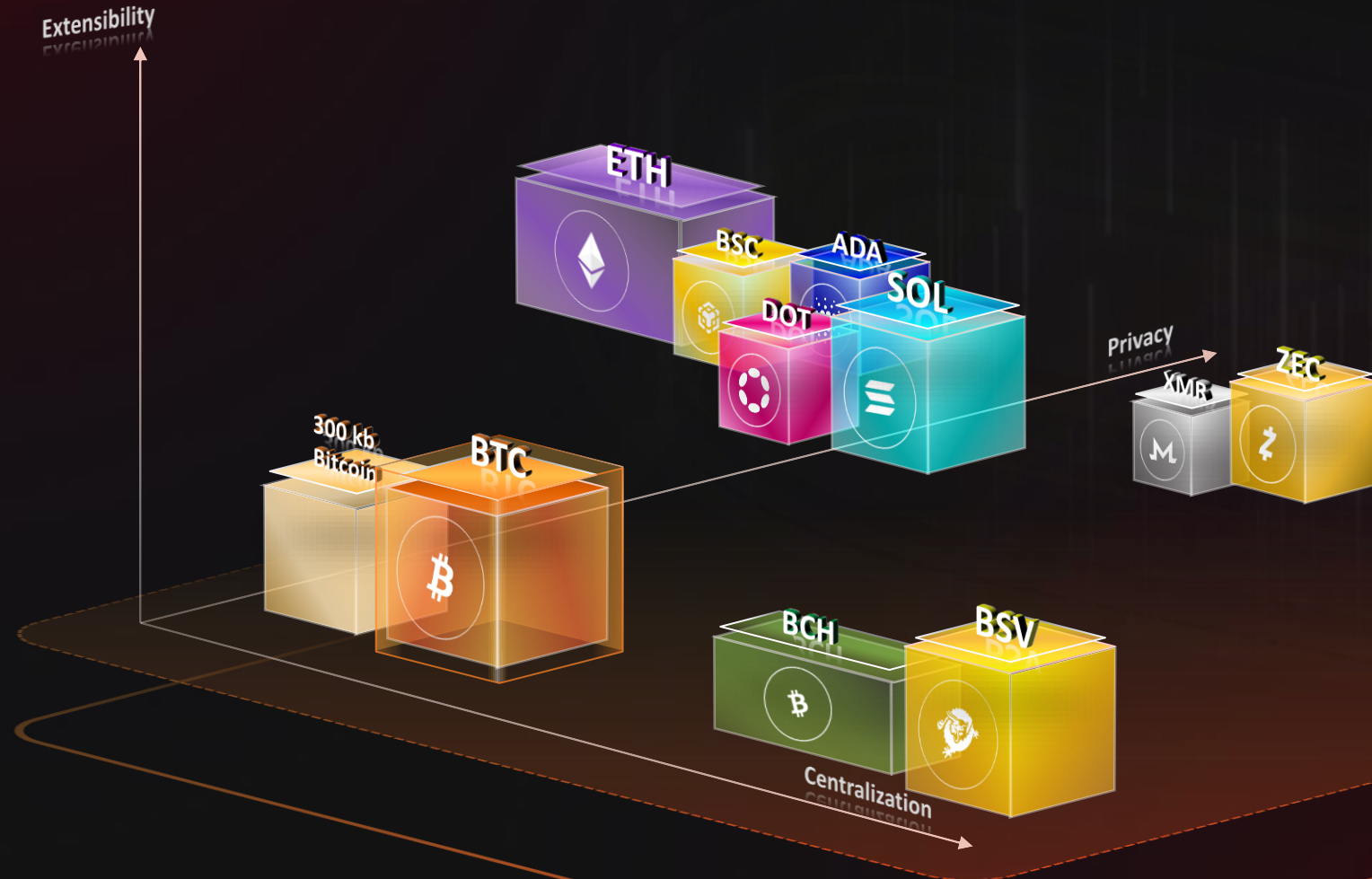


Why Bip300

Altcoins

Rival coins -- different protocol,
different blockchain

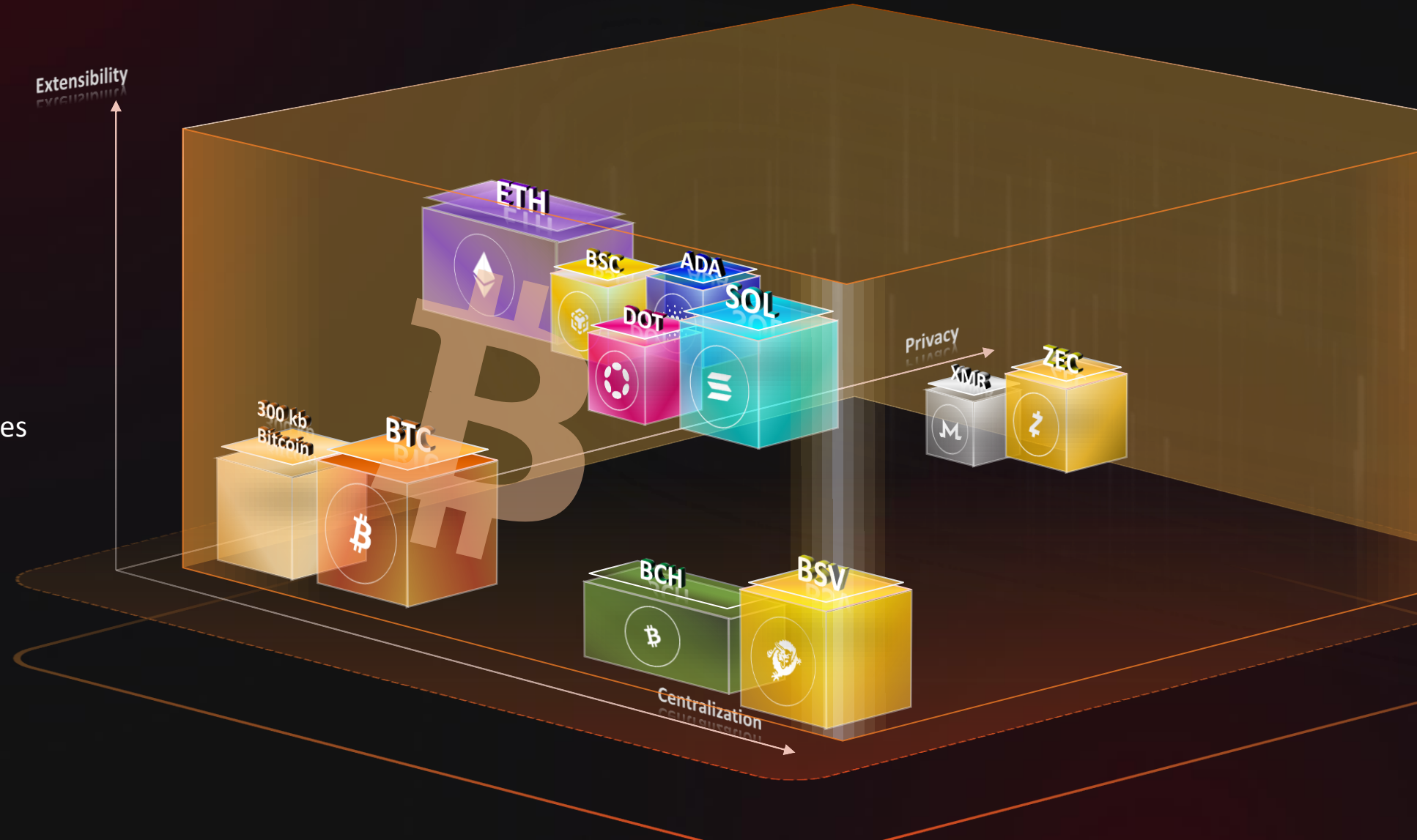
The Payments Spectrum



One Coin, Many Blockchains

Bip300

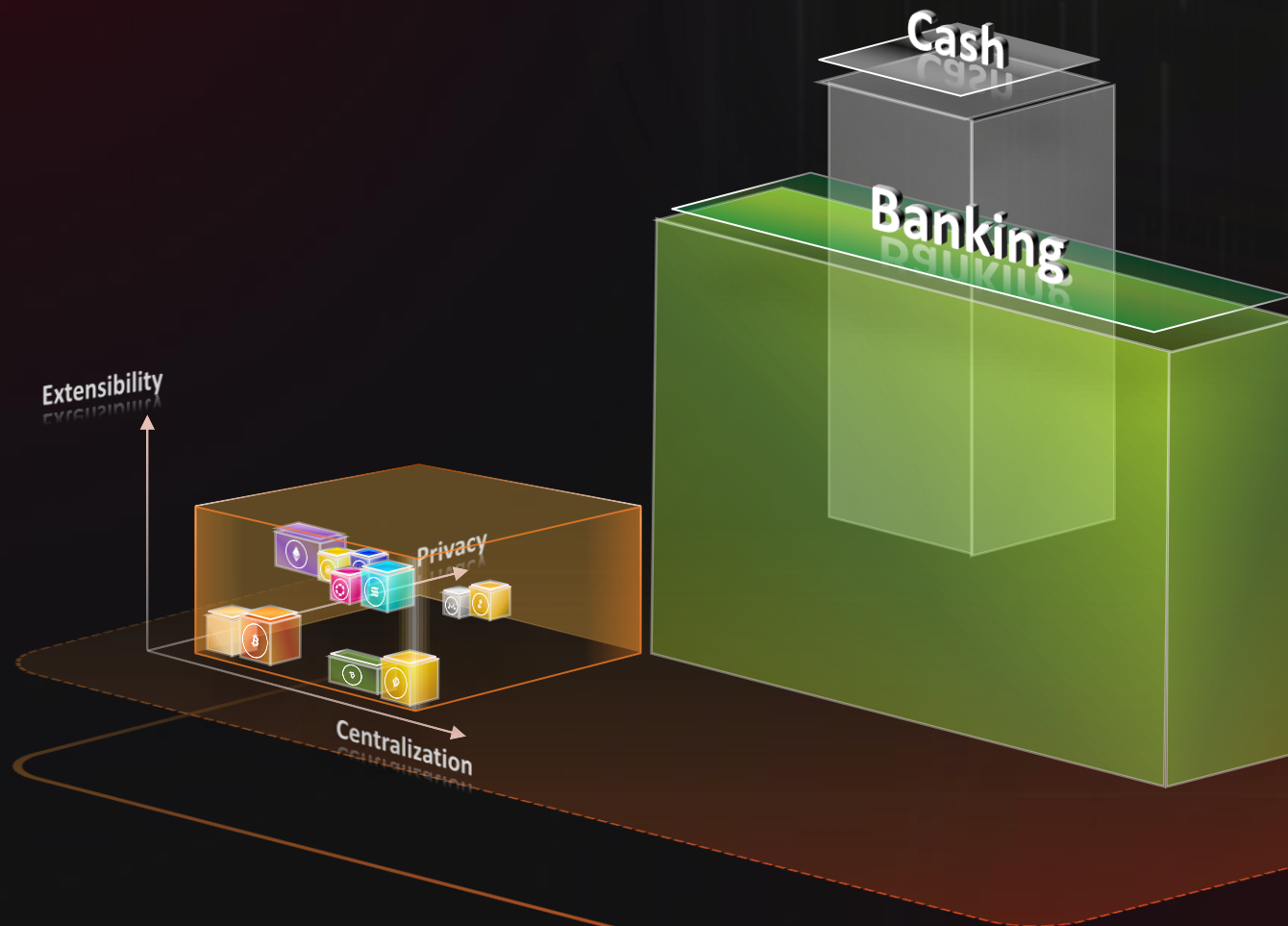
Allows BTC to Cover
the *Entire Spectrum* of Use-Cases



Also Copy Non-Blockchain Systems

Fiat

Non-blockchain,
centralized...



One Coin, Entire Payments Spectrum

Bip300

...just more for
Bip300 to copy!

