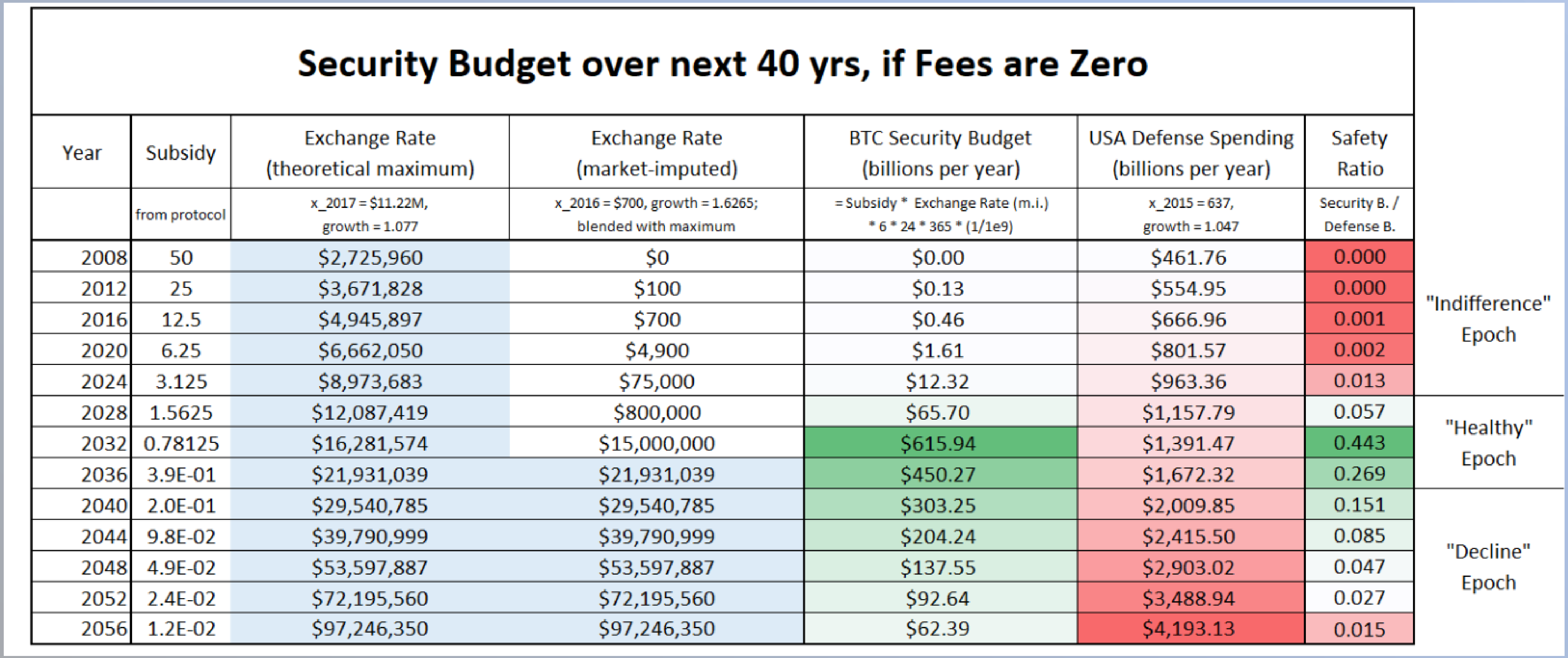
Layer Two Labs Inc. &

MainChain – A BIP300 Fork of Bitcoin

1. Problem:

- Bitcoin's security is uncertain：
    - declining block rewards
    - bull market not giving insane returns
    - low use (USDT since 2018 has been more widely used compared to BTC)
    - therefore low transaction fees
    - lack of any innovation (BTC can't run smart contracts, no functions besides Store-of-Value and Medium-of-Exchange)
    - eventually BTC will reach a plateau where new investors don't want to mine, existing investors won’t invest in faster machines, and hashrate will not increase
    - the 1% of useful features in altchains will not be possible on btc
    - We estimate in two more BTC halvings, the “security budget” of Bitcion will become a major concern



Security Budget over next 40 yrs, if Fees are Zero

Year	Subsidy	Exchange Rate (theoretical maximum)	Exchange Rate (market-imputed)	BTC Security Budget (billions per year)	USA Defense Spending (billions per year)	Safety Ratio	
	from protocol	x_2017 = $11.22M, growth = 1.077	x_2016 = $700, growth = 1.6265; blended with maximum	= Subsidy * Exchange Rate (m.i.) * 6 * 24 * 365 * (1/1e9)	x_2015 = 637, growth = 1.047	Security B. / Defense B.	
2008	50	$2,725,960	$0	$0.00	$461.76	0.000	"Indifference" Epoch
2012	25	$3,671,828	$100	$0.13	$554.95	0.000	
2016	12.5	$4,945,897	$700	$0.46	$666.96	0.001	
2020	6.25	$6,662,050	$4,900	$1.61	$801.57	0.002	
2024	3.125	$8,973,683	$75,000	$12.32	$963.36	0.013	
2028	1.5625	$12,087,419	$800,000	$65.70	$1,157.79	0.057	"Healthy" Epoch
2032	0.78125	$16,281,574	$15,000,000	$615.94	$1,391.47	0.443	
2036	3.9E-01	$21,931,039	$21,931,039	$450.27	$1,672.32	0.269	
2040	2.0E-01	$29,540,785	$29,540,785	$303.25	$2,009.85	0.151	"Decline" Epoch
2044	9.8E-02	$39,790,999	$39,790,999	$204.24	$2,415.50	0.085	
2048	4.9E-02	$53,597,887	$53,597,887	$137.55	$2,903.02	0.047	
2052	2.4E-02	$72,195,560	$72,195,560	$92.64	$3,488.94	0.027	
2056	1.2E-02	$97,246,350	$97,246,350	$62.39	$4,193.13	0.015	

- Governments and central banks with their unlimited money supply can 51% brute-force attack the BTC chain

- BTC needs to take back lost marketcap from altcoins and allow for innovations to be built on top of BTC

- increase the amount of transaction fees earned and make BTC mining much more attractive, therefore increasing Bitcoin’s security budget/hashrate continuously

- Drivechain (aka Bitcoin Improvement Proposal 300 (BIP300) upgrade) is the answer. Drivechain/BIP300 will allow Bitcoin to dominate the entire "Web3" space, making altcoins irrelevant and Bitcoin the defacto platform to develop decentralized applications on

No Bip300

One Sound

Many Sounds

Yes Bip300

2. Technology:

- Drivechain & Sidechain upgrades to the Bitcoin protocol. Created and developed by L2L's founder Paul Sztorc, top-level Bitcoin OG researcher and developer since 2011 and economist from Yale University

- Drivechain enables permissionless sidechains (Layer 2) on Bitcoin, allowing anyone to develop whatever token, smart contract, DApps, etc. they want on their own sidechain (Layer 2), no permission needed, with zero risk to the mainchain (Layer 1)

- Bitcoin miners (Layer 1) will earn transaction fees from every sidechain, with zero new cost overheads and zero need for new equipment. The more and better the sidechains (applications) are, the more the Bitcoin miners will earn

- Dr Adam Back – creator of Proof-of-Work consensus (cited multiple times in Satoshi's Bitcoin Whitepaper), Founder/CEO of Blockstream, Prime Satoshi Nakamoto Candidate

"Drivechain is arguably better than Taproot (an inferior BTC Layer2 Tech) "

- Fiatjaf – Creator of Nostr Protocol

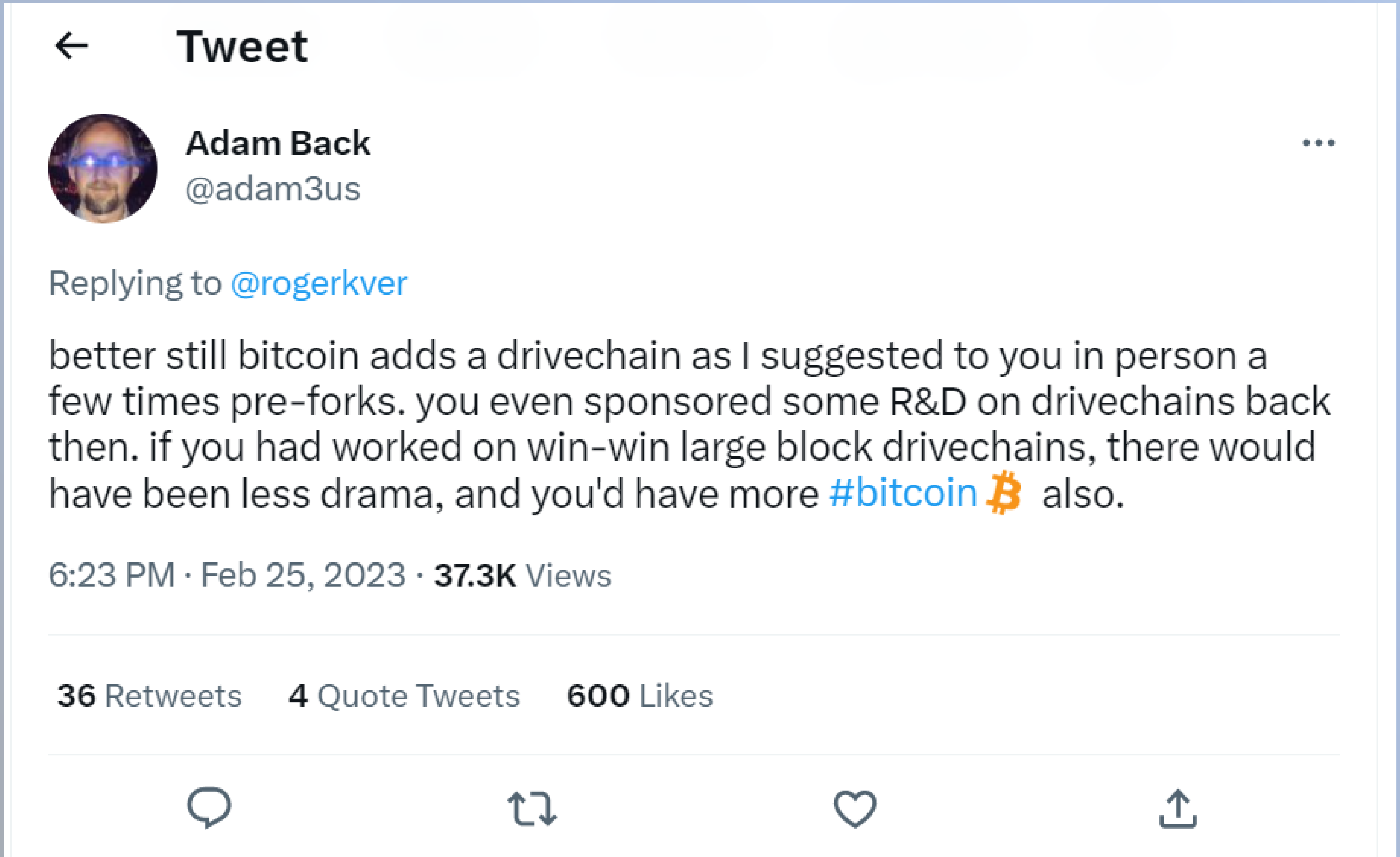
"Drivechain is our only hope. ... We need Drivechain or all the work of thousands in the last 13 years (referring to Bitcoin) will be in vain"

Dr Adam Back (Blockstream)

Paul Sztorc (Drivechain Creator, CEO of LayerTwo Labs)

Dr Adam Back and Paul Sztorc into what the future of sidechains
will look like and how they will be connected to Bitcoin (Adam
Back endorses Paul Sztorc's Drivechain),
at the Bitcoin Amsterdam Conference: Oct 2022

https://www.youtube.com/watch?v=CuKPIUO1pVA



Tweet

Adam Back
@adam3us

Replying to @rogerkver

better still bitcoin adds a drivechain as I suggested to you in person a few times pre-forks. you even sponsored some R&D on drivechains back then. if you had worked on win-win large block drivechains, there would have been less drama, and you'd have more #bitcoin ₿ also.

6:23 PM · Feb 25, 2023 · **37.3K** Views

36 Retweets **4** Quote Tweets **600** Likes

Dr Adam Back replying to Roger Ver (big backer of Bitcoin Cash, pro large block sizes, against Adam Back’s vision of Bitcoin (small blocks)). Adam Back endorsing Drivechain as the way to give everyone exactly any and all functionalities/specifications they’d want from Bitcoin

3. New Bitcoin Fork:

- Layer Two Labs will release its own Proof-of-Work chain in 2023 with Drivechain enabled. It will be a fork of Bitcoin. We are calling it “Mainchain”

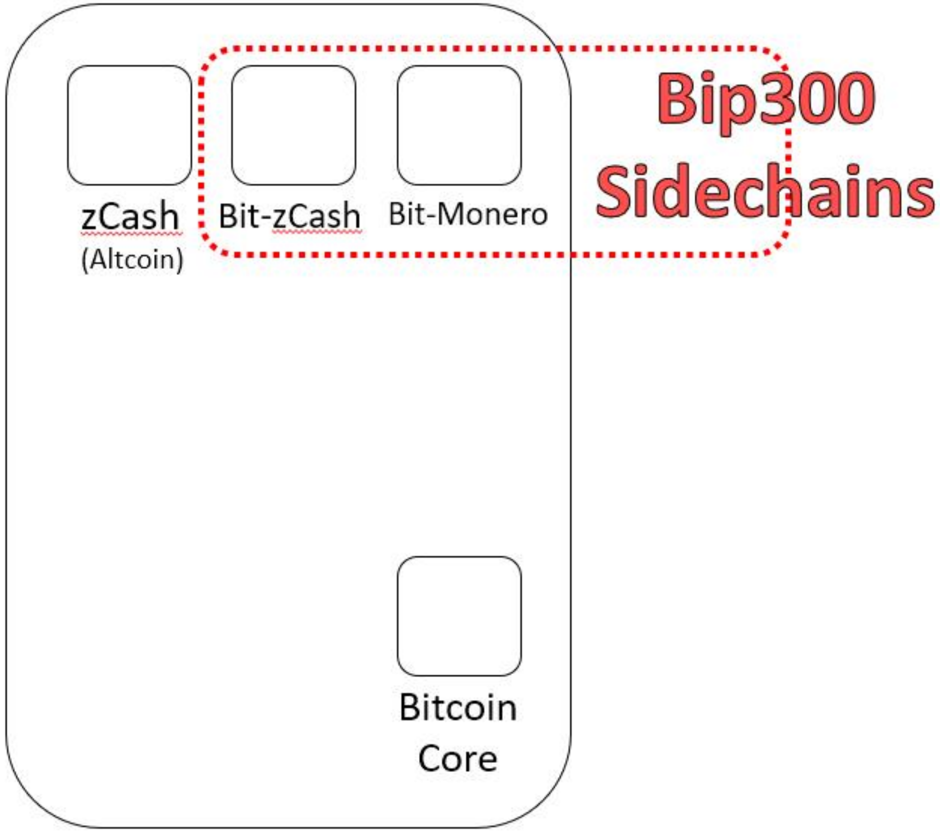
- Several sidechains (“decentralized applications") will be ready at launch

- Developers create Sidechains (L2) on Mainchain (L1) to experiment with whatever ideas and concepts they want

- Think of Mainchain as a permissionless iOS: you can make whatever app you want on Mainchain, just go ahead and create your own sidechain and start innovating. You don’t need permission from anyone and nobody can stop you even if they wanted to

(#1) Full Autonomy

Metaphor



- Launch Dapps/Sidechains include:

a. **Truthcoin** - Decentralized Prediction Market that allows users around the world to use crypto to bet on outcomes of events (who will be the next US president). Trillion dollar market. Decentralized. Been in development by Paul Sztorc since 2010. See intrade.com’s history for a glimpse about Prediction Market (https://en.wikipedia.org/wiki/Intrade)

b. **ZCash**: our version of a high privacy token. Bitcoin has long since lost its lunch to Monero (XMR) and ZCash on the darkweb. Our ZCash sidechain will take back some of this lost revenue for PoW miners

c. **BitAsset:** a NFT sidechain that's more economical/viable than Ordinals

d. **BitNames**: potential to challenge ICANN for domain registration

e. and more

Project	**What We'd Have to Do…**	**TAM** (NPV valuation)	**Notes**
BitAsset Sidechain	Develop the sidechain, and auction off the first asset for collectible value.	**$ 5-50 M**	a16z values **NFT marketplace** at $1.5B (July 2021).
Validation Service	Just run all the sidechain nodes, and provide APIs. We have a unique advantage as the originators/creators.	**$ 50 M**	An industry insider estimated that **Infura** was worth $50 M. Acquired in Oct 2019.
Truthcoin Sidechain	Finish software (MVP already developed), use $$ for liquid markets, educate customers.	**$ 2-200 B**	See presentations at BitcoinHivemind.com for details.
Withdrawal Service	Sell layer1 coin in exchange for layer2 coins. Has all the benefits/drawbacks of running an exchange. Might be better to partner w/ one.	**$ 10-50 M**	Volume will likely be immense, but so will competition. We have a unique "edge" as being the software creators/originators.
BitNames Sidechain	Develop the software (already spec'ed out), test, add infrastructure, promote.	**$ 4-5 M**	Most value is in the kudos for replacing **ICANN**. ICANN "value" unclear but they blocked a relatively small 1.1 B sale in May2020.

4. Advantages:

Layer Two Labs' Mainchain allows for the creation of truly decentralized DApps, smart contracts, new tokens, and other novel ideas to exist on a truly decentralized network.

- Each sidechain ("Layer 2") poses no technical risk to Mainchain ("Layer 1"), even when a sidechain breaks apart due to bad programming, flaws, hacks, and etc.
- When a sidechain is successful, the Mainchain miners automatically earn more in transaction fees from the success of that sidechain (we called this “Blind Merge Mining”). Mainchain (which has Drivechain/BIP300 enabled) allows for this plus-plus/win-win scenario
- Miners won’t need to participate/gamble/mine alts to gain any benefits; all benefits will flow to miners automatically

5. Who benefits?

a. Miners: miners with SHA256/BTC mining equipment switch from mining BTC to Mainchain. Earn block rewards from Mainchain, MC transaction fees, and transaction fees from MC sidechain

- If BTC eventually upgrades to BIP300/301 due to MC's success, MC’s sidechains can easily migrate to BTC, and miners can earn more from these now-BTC sidechains
- If more applications are developed on sidechains, BTC miners get all the rewards without needing to gamble on altcoins or mine altcoins instead of Bitcoin. No extra mining costs, no downsides, only benefits
- This has the potential to increase attractiveness of Bitcoin mining, thereby exponentially increasing Bitcoin's "security budget" against future 51% attacks. Making Bitcoin magnitude more secure, even if no one is using BTC for transactions and are just hodling BTC

b. Developers & Users: MC and (potentially) Drivechain-enabled BTC will be the only defacto Proof-of-Work chain that supports DApps and other creations

- Anyone can experiment on their own sidechain

- Anything remotely prone to government intervention (like intrade.com) will have a better chance of surviving, e.g. Prediction Market applications

- Our Mainchain is a much stronger base to build real apps with utility, compared to Ethereum (PoS), BSC, Tron, Solana (centrally controlled VC chain that breaks every other week) and what have you.

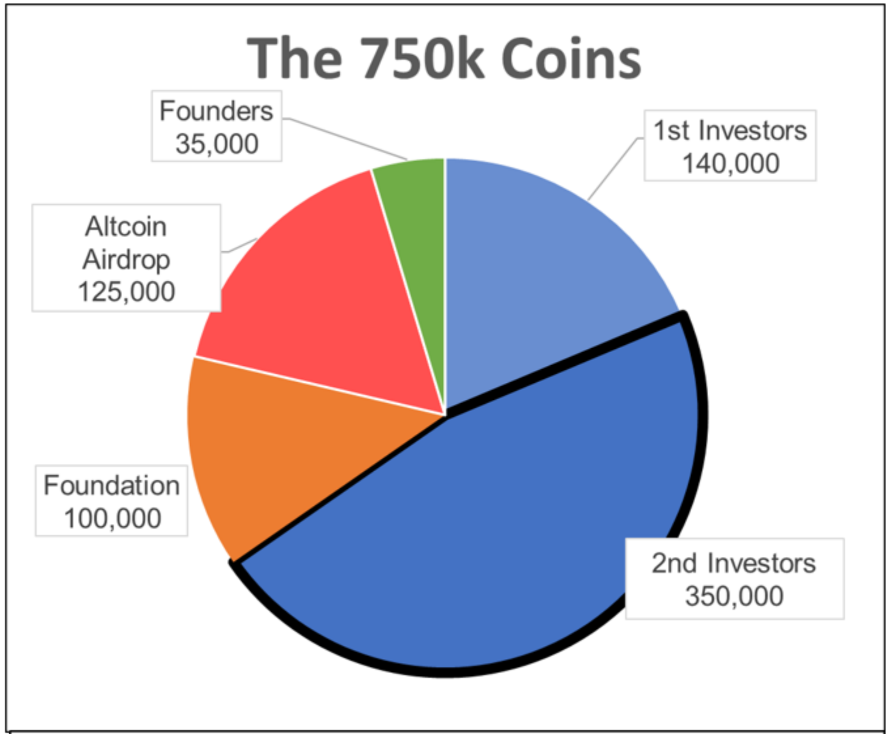
6. Tokenomics/Investment:

- Seed round (2022): $4M USD was raised for 140,000 Mainchain (MC) coins and 4% of the company's shares
- Second round (2023): $100M USD target for 350,000 MC coins and 20% of company's shares
- 50% of investment will go towards MC, 50% will go towards the company's shares
- MC's mining, total supply, and halving schedule will follow BTC: 10 minute per block, 21 million total MC, and halving every 4 years. No ICO
- All existing BTC addresses will receive MC coins 1:1
- Mainchain will fork from BTC at BTC Block Height ~805,000
- All existing SHA256 (BTC's PoW algo) mining equipment can mine MC
- Sidechains (L2) poses no risk for Mainchain (L1)
- Miners can choose to kill sidechains but need majority (51%) consensus (very difficult). Essentially all sidechains will be truly uncensorable, unstoppable

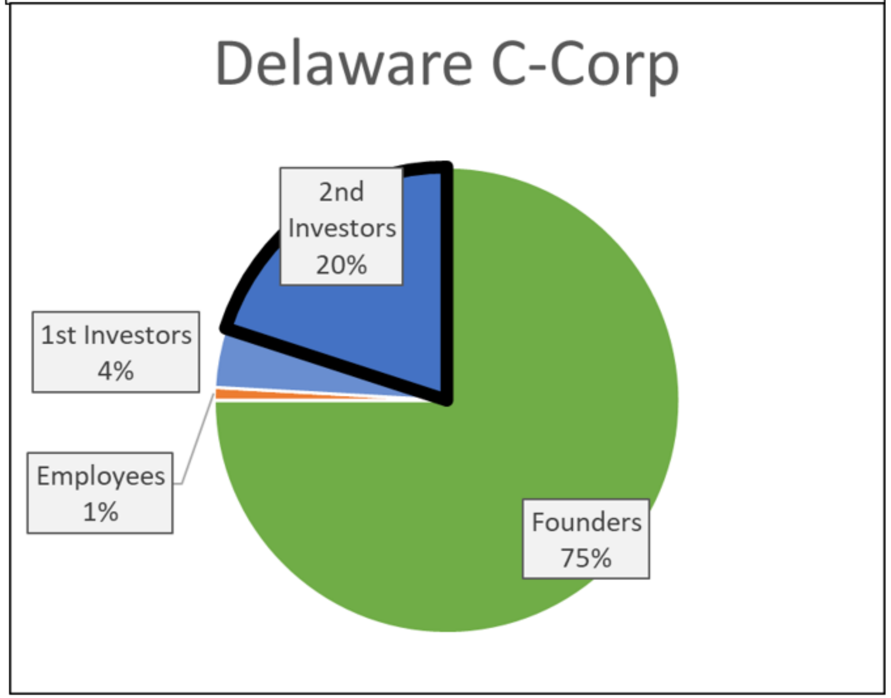
Terms – USD for Coins & Shares

100M
USD
(from you)

$50M
for
350k coins



$50M
for
2,133,333 shares



Valuations

$142.8 per coin

1.81% of a
2.76 B
coin
(@19.3M coins)

...plus...

20% of a
$250 M
company.

7. Different From Other Bitcoin Forks:

- Bitcoin Cash (BCH) and other Bitcoin forks were very political and had no technical improvements. Frivolous at best
- They encouraged certain types usage (e.g. buying coffee with your BCH) and developed closed-off communities with cult-like leaders (e.g. Craig Wright, Jihan Wu)
- They didn’t encourage innovation towards utility by developers and didn't have any real technology like Drivechain and sidechains

Mainchain is NOT political:

- it's an open, permissionless system for anyone who wants to start their own sidechains. L2L will encourage people to innovate on Mainchain, to experiment as they wish.

Craig Wright, BSV

Jihan Wu, BCH

Mainchain is NOT political:

- Mainchain is an open, permissionless system for anyone who wants to start their own sidechains. There will be no dictators in MC like in other Bitcoin Forks

- Layer Two Labs will encourage developers to innovate on Mainchain, to experiment as they wish, and we will provide support and funding to promising developers who focus on novel ideas and utility

8. Mainchain/Drivechain vs. Other Layer 2’s:

- **Stacks: STX** is a scam, it does not "run applications on Bitcoin" as it claims https://www.youtube.com/watch?v=AgZoNYpBh-o

- **Rootstock: RSK** (which actually received consulting from Paul Sztorc as early as 2015: RSK uses some elements of Drivechain) did not launch with any applications. They were just waiting for people to develop something on top. Also their foundation has bad management. No hackathon. The “managers” of their foundation are not very creative people

- **Lightning Network: LN** is not ideal for making applications, it's merely a way to allow faster and cheaper transfers of BTC between users, while cutting out revenue to the BTC miners. Very hyped. But no real world use (nobody wants to spend BTC)

- **Taproot：** Adam Back: “*Drivechain is arguably better than Taproot (an inferior BTC Layer2 Tech)*”

9. Potential Outcomes :

a. Mainchain fails, but investors make a "small" return

b. Layer Two Labs is successful and achieves milestones Blockstream couldn’t:

- L2L grows in valuation close or exceeding Blockstream's current $3.2bn USD
- Many DApps/sidechains with real-life utility proliferate on Mainchain
- Eventually BTC upgrades to BIP300 due to pressures to “save” BTC
- MC's DApps easily migrates to BTC
- MC may die in the process, but our stakes in the DApps continue to live on upgraded-BTC
- Great returns to investors

c. BTC never upgrades. MC's ecosystem is wildly successful and thriving:

- BTC dies in obscurity, MC overtakes BTC, can rename itself BTC
- MC completely destroys the altcoin spaceand becomes the strongest marketcap chain by far and the most ideal platform for any decentralized application development
- Insane returns for investors

The Three Scenarios

We win either way!

Scenario 1 – We Fail	Scenario 2 – We Are Copied	Scenario 3 – We Conquer
Bip300 fails to work as expected. Or users don't like it.	Bip300 is proven "in the wild", and then BTC copies it. Bip300coin loses.	The Bip300coin triumphs! And BTC falls into obsolescence.
We learn from that failure, and try to make something better.	We are the heroes who saved Bitcoin!	We save Bitcoin *and* are early adopters in the $100T hyper-coin!
The coins and the shares are worth very little. (Perhaps a BCH "fail valuation", of **130 $/coin**.)	Our company "LayerTwo Labs" becomes comparable to Blockstream (valued at **$3.2 Billion** in Aug 2021, via Series B raise). *(Except vastly superior, having succeeded exactly where they failed.)* Our coin would be worth $0, as the Bip300-BTC would crush all other coins.	Our coin destroys all rivials an reaches the "hyper-bitcoinization" optimum price (~ **$15M per coin**). *(Our company also becomes worth more than Blockstream, but this is a drop in the bucket in terms of ROI.)*
Seed coins (115,000): **$ 3 million → $15 million**	**Seed shares (2.5%):** **$ 3 million → $80 million**	**Seed coins (115,000):** **$ 3 million → $1.73 trillion**
Round A coins (300,000): **$ 100 million → $39 million**	**Round A shares (10%):** **$ 100 million → $320 million**	**Round A coins (300,000):** **$ 100 million → $4.5 trillion**

This math is correct.

10. Roadmap:

- **H1 2023:** Raise second round, $100m USD. PR and marketing

- **H2 2023:** Create a developer community for Mainchain, encourage, educate, support, and invest into projects that will develop useful sidechains on MC, work with governments and institutions on encouraging the use of MC

- **H2 2023:** Encourage PoW miners to try and mine MC

11. Our People:

- Paul Sztorc can be considered as "the next Dr. Adam Back (creator of PoW consensus)".

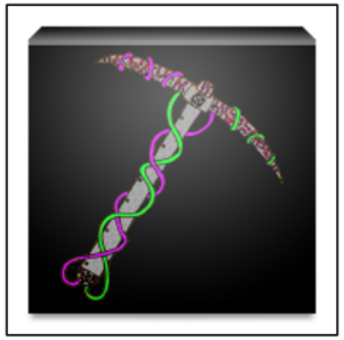
- Paul is the inventor of several profound technologies such as Drivechain and Truthcoin

- Layer Two Labs’ team and seed round investors are veterans in the space, with many having more than 10+ years of experience in crypto

- L2L's core founding team have experience from Bitcoin development, altcoin development, smart contracts, to holding key positions at Kraken Exchange and BlockFi

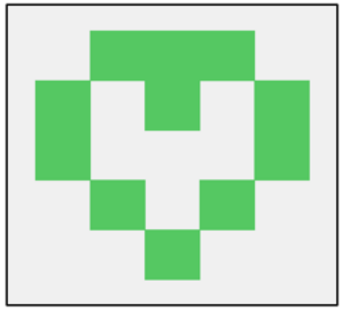
Team

- 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).

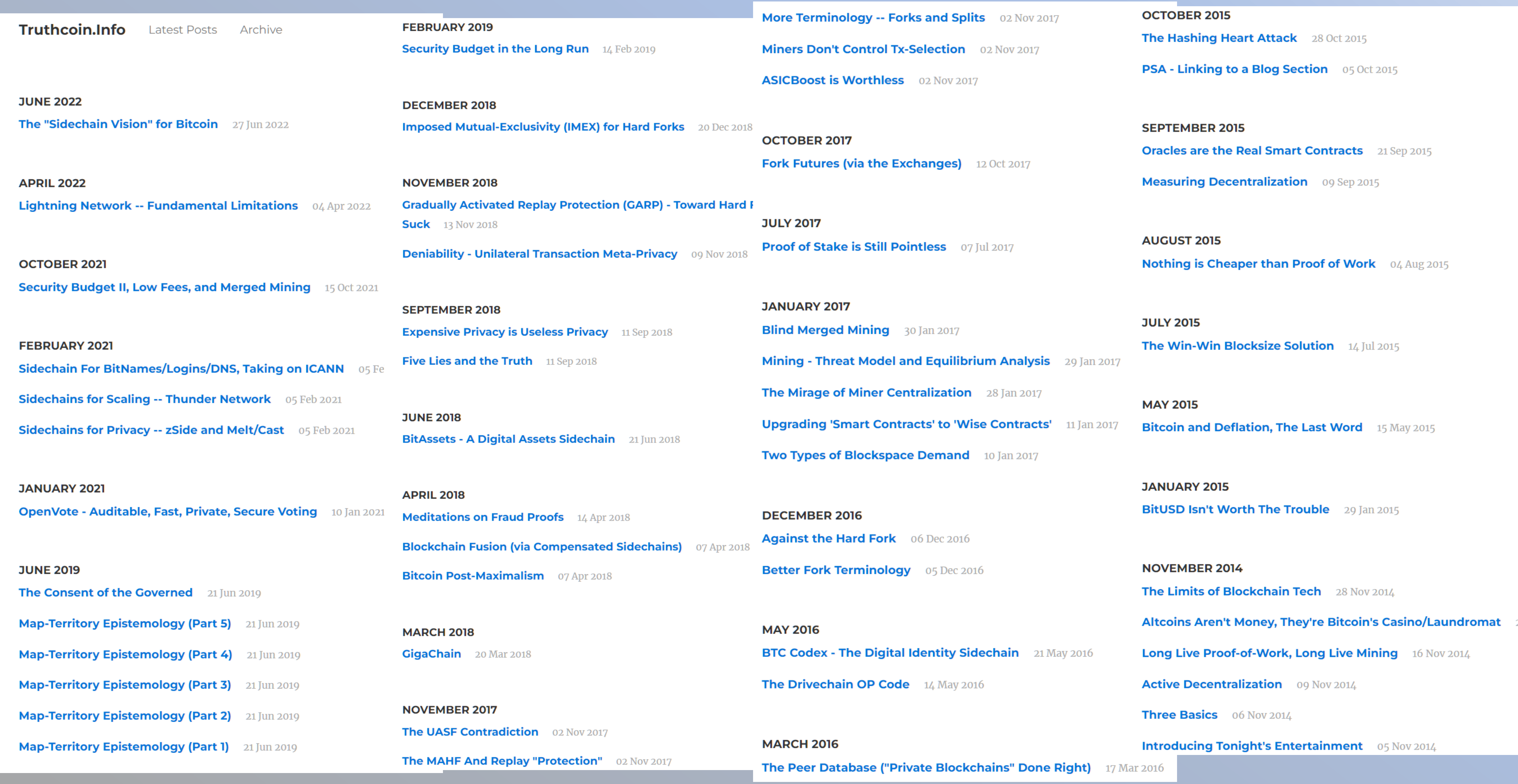


- CryptAxe
  - Bitcoin Core developer (2016-Present; 0.14, 0.15, 0.16). Infrastructure engineer BIPs 300/301. Creator of sidechain template, BitAsset sidechain, zCash sidechain GUI.

- 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.



Truthcoin.Info Latest Posts Archive

JUNE 2022

The "Sidechain Vision" for Bitcoin 27 Jun 2022

APRIL 2022

Lightning Network -- Fundamental Limitations 04 Apr 2022

OCTOBER 2021

Security Budget II, Low Fees, and Merged Mining 15 Oct 2021

FEBRUARY 2021

Sidechain For BitNames/Logins/DNS, Taking on ICANN 05 Fe

Sidechains for Scaling -- Thunder Network 05 Feb 2021

Sidechains for Privacy -- zSide and Melt/Cast 05 Feb 2021

JANUARY 2021

OpenVote - Auditable, Fast, Private, Secure Voting 10 Jan 2021

JUNE 2019

The Consent of the Governed 21 Jun 2019

Map-Territory Epistemology (Part 5) 21 Jun 2019

Map-Territory Epistemology (Part 4) 21 Jun 2019

Map-Territory Epistemology (Part 3) 21 Jun 2019

Map-Territory Epistemology (Part 2) 21 Jun 2019

Map-Territory Epistemology (Part 1) 21 Jun 2019

FEBRUARY 2019

Security Budget in the Long Run 14 Feb 2019

DECEMBER 2018

Imposed Mutual-Exclusivity (IMEX) for Hard Forks 20 Dec 2018

NOVEMBER 2018

Gradually Activated Replay Protection (GARP) - Toward Hard F
Suck 13 Nov 2018

Deniability - Unilateral Transaction Meta-Privacy 09 Nov 2018

SEPTEMBER 2018

Expensive Privacy is Useless Privacy 11 Sep 2018

Five Lies and the Truth 11 Sep 2018

JUNE 2018

BitAssets - A Digital Assets Sidechain 21 Jun 2018

APRIL 2018

Meditations on Fraud Proofs 14 Apr 2018

Blockchain Fusion (via Compensated Sidechains) 07 Apr 2018

Bitcoin Post-Maximalism 07 Apr 2018

MARCH 2018

GigaChain 20 Mar 2018

NOVEMBER 2017

The UASF Contradiction 02 Nov 2017

The MAHF And Replay "Protection" 02 Nov 2017

More Terminology -- Forks and Splits 02 Nov 2017

Miners Don't Control Tx-Selection 02 Nov 2017

ASICBoost is Worthless 02 Nov 2017

OCTOBER 2017

Fork Futures (via the Exchanges) 12 Oct 2017

JULY 2017

Proof of Stake is Still Pointless 07 Jul 2017

JANUARY 2017

Blind Merged Mining 30 Jan 2017

Mining - Threat Model and Equilibrium Analysis 29 Jan 2017

The Mirage of Miner Centralization 28 Jan 2017

Upgrading 'Smart Contracts' to 'Wise Contracts' 11 Jan 2017

Two Types of Blockspace Demand 10 Jan 2017

DECEMBER 2016

Against the Hard Fork 06 Dec 2016

Better Fork Terminology 05 Dec 2016

MAY 2016

BTC Codex - The Digital Identity Sidechain 21 May 2016

The Drivechain OP Code 14 May 2016

MARCH 2016

The Peer Database ("Private Blockchains" Done Right) 17 Mar 2016

OCTOBER 2015

The Hashing Heart Attack 28 Oct 2015

PSA - Linking to a Blog Section 05 Oct 2015

SEPTEMBER 2015

Oracles are the Real Smart Contracts 21 Sep 2015

Measuring Decentralization 09 Sep 2015

AUGUST 2015

Nothing is Cheaper than Proof of Work 04 Aug 2015

JULY 2015

The Win-Win Blocksize Solution 14 Jul 2015

MAY 2015

Bitcoin and Deflation, The Last Word 15 May 2015

JANUARY 2015

BitUSD Isn't Worth The Trouble 29 Jan 2015

NOVEMBER 2014

The Limits of Blockchain Tech 28 Nov 2014

Altcoins Aren't Money, They're Bitcoin's Casino/Laundromat

Long Live Proof-of-Work, Long Live Mining 16 Nov 2014

Active Decentralization 09 Nov 2014

Three Basics 06 Nov 2014

Introducing Tonight's Entertainment 05 Nov 2014

sensus
20:07

THE FUTURE OF SIDE CHAINS
36:13

$10 MILLION BITCOIN PRICE?
PAUL SZTORC
KITCO NEWS
16:02

bitcoin2021
MIAMI
DRIVECHAIN DEMO
swipe
END FIAT
15:58

Website:

www.layertwolabs.com

Important YouTube Videos:

https://www.youtube.com/watch?v=C14V03682Sg
https://www.youtube.com/watch?v=CuKPIUO1pVA

https://www.youtube.com/watch?v=xweFaw69EyA

Paul Sztorc's Blockchain/Crypto/Web3 Blog 2014 to Present (click on right hand side "blog archive"):

https://www.truthcoin.info/

LinkedIn:

www.linkedin.com/company/layertwo-labs/