

Layer Two Labs Inc. &

MainChain – A BIP300 Fork of Bitcoin

1.問題:

比特幣安全性的未來是不確定的:

- 減少的區塊獎勵（每4年減少新比特幣）。
- 牛市不會帶來瘋狂的回報。
- 作為交易媒介的使用率較低（2022年USDT的使用範圍比BTC更廣泛，至少是BTC的兩倍）。
- 交易費用低。
- 缺乏創新:沒有智能合約，沒有價值存儲和交易媒介之外的功能。
- 最終BTC會達到一個平台期，新的投資者不願意挖礦，因為回報很差，哈希率也不會增加。
- 替代鏈的最佳功能在比特幣上是不可能的。
- 在未來BTC的兩次減產中，比特幣的“安全預算”將成為主要擔憂。

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
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
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
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

"Indifference"
Epoch

"Healthy"
Epoch

"Decline"
Epoch

- 擁有無限貨幣供應的政府和央行可以51%攻擊比特幣的區塊鏈。
- BTC需要從替代幣中奪回失去的市場份額，並允許在BTC上建立創新。
- 我們需要一種方法來提高礦工的交易費用，讓比特幣挖礦更具吸引力。
- Drivechain（又名比特幣改進提案BIP300）是答案。它將允許比特幣升級並主導整個“Web3”空間。



2.技術:

比特幣協議的 Drivechain 和Sidechain升級——由Layer Two Lab的創始人Paul Sztorc創建，他自2011年以來一直是頂級比特幣的OG研究員和開發人員，也是耶魯大學的經濟學家。

- Drivechain在比特幣上實現了無許可Sidechain，允許任何人在自己的Sidechain上開發任何token、智能合約、DApp和其他概念-驅動鍊是由。每個側鏈的開發人員可以確定鏈的塊大小、每個塊的分鐘數以及任何參數。一切都可以根據開發人員的喜好進行調整
- **Dr Adam Back--PoW共識的教父和創造者**，Blockstream的創始人和首席執行官
 - “Drivechain可以說比Taproot更有用。”
- Fiatjaf是2022年和2023年最熱門、最受關注的去中心化新技術**Nostr**的創造者。
 - “**Drivechain是我們唯一的希望**，我們需要Drivechain，否則過去13年成千上萬人的工作（指BTC）將付之一炬。”



Dr Adam Back (Blockstream CEO)


Paul Sztorc (Drivechain Creator, CEO of LayerTwo Labs)


Adam Back 博士和 Paul Sztorc 在 2022 年 10 月的比特幣阿姆斯特丹會議上探討了側鏈的未來以及它們將如何連接到比特幣（Adam Back 支持 Paul Sztorc 的驅動鏈）

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



Roger Ver  @rogerkver · Feb 24

If **#BTC**  ever raises the block size, it will prove that the **#BCH** camp was right all along.

If **#BTC**  never raises the block size, it will never be permissionless cash for the world.



302



132



606




231.3K



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

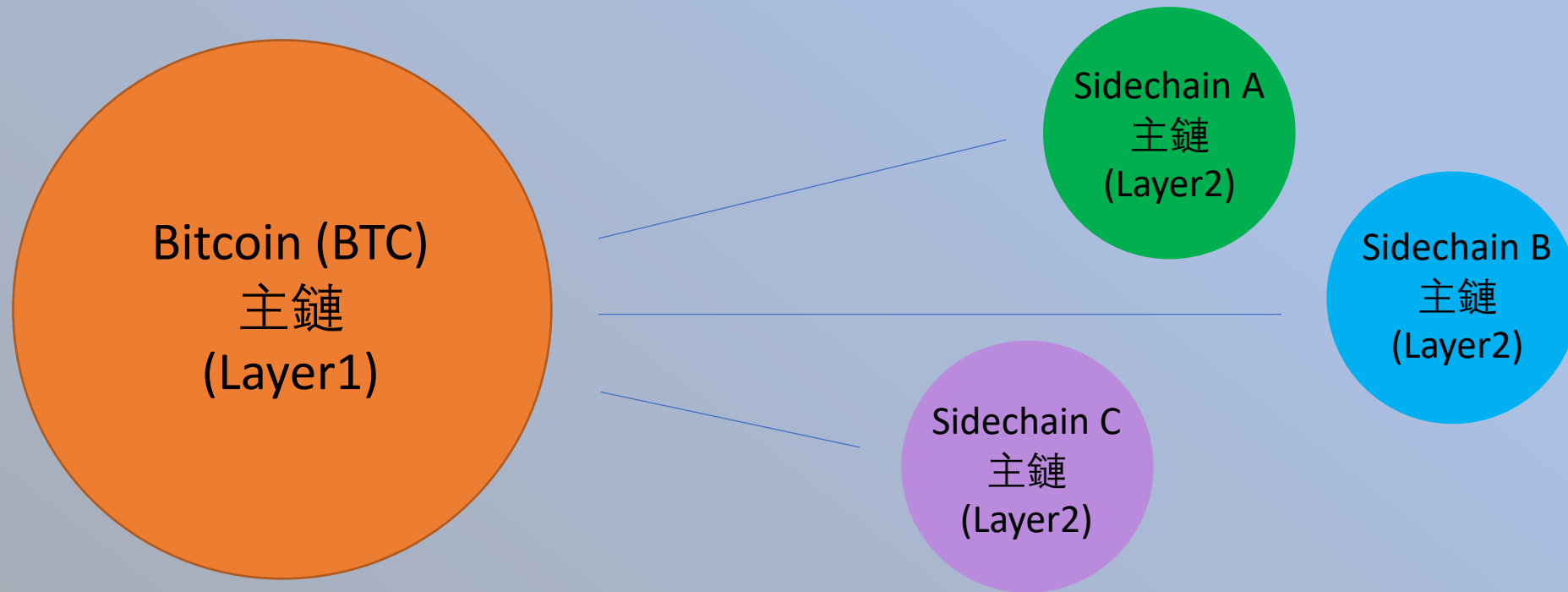
36 Retweets

4 Quote Tweets

600 Likes

Adam Back 博士回复 Roger Ver（比特幣現金的大支持者，贊成大塊大小，反對 Adam Back 對比特幣（小塊）的看法）。Adam Back 認可 Drivechain 作為向每個人提供他們想要從比特幣獲得的任何和所有功能/規格的方式

一旦比特幣升級到 BIP300 (“Drivechain” 軟件)，你可以在比特幣的主鏈 (Layer1) 之上製作你想要的任何側鏈 (Layer2)。

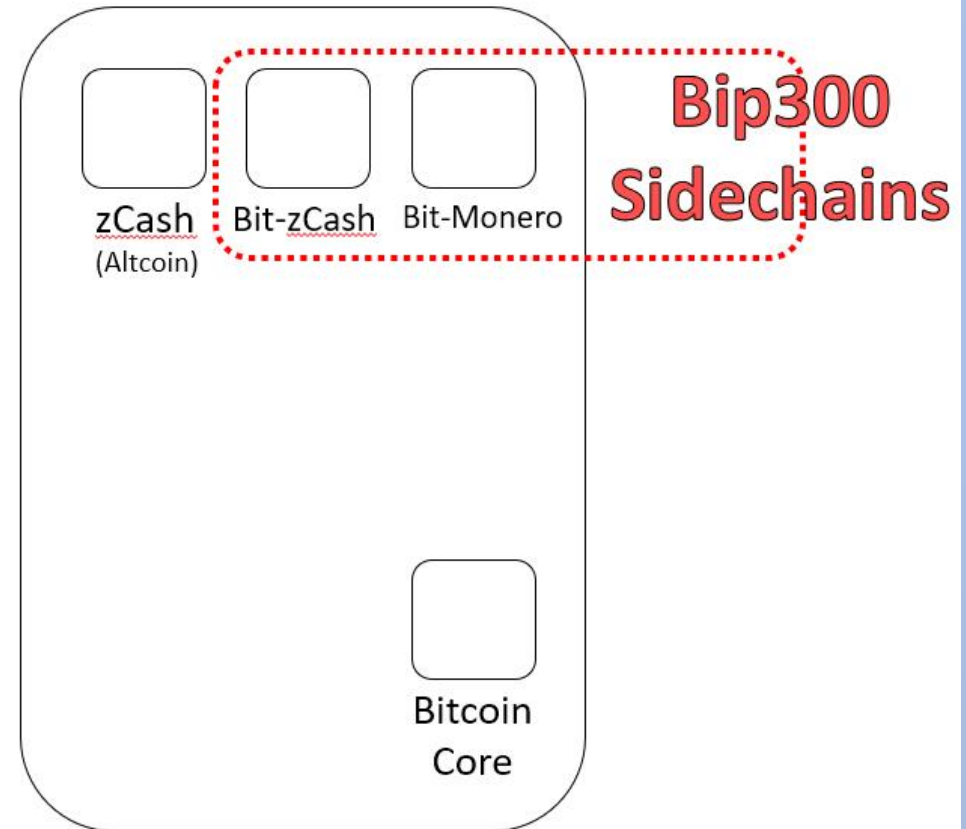
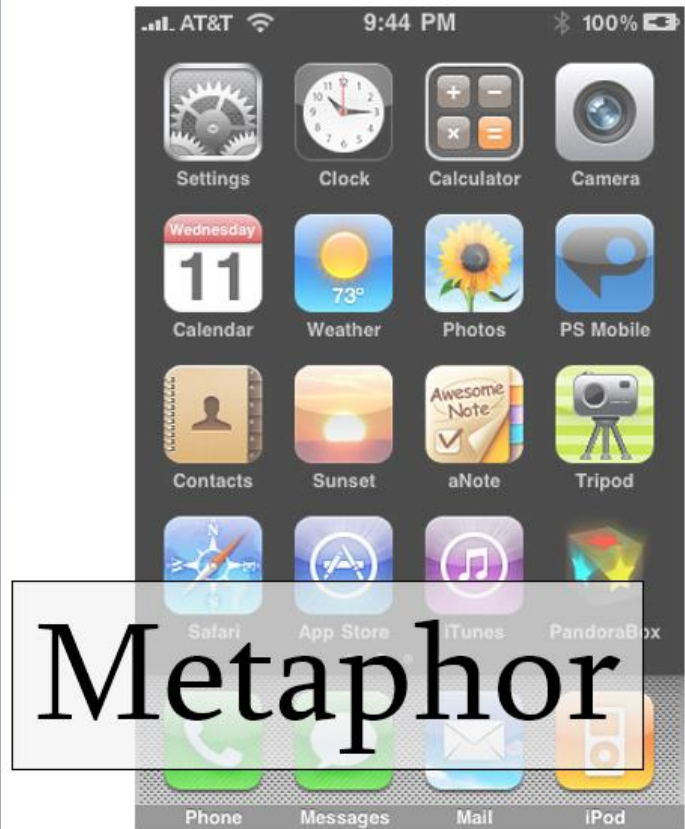


- 比特幣 = PoW 鏈: 需要硬件和電力
- 礦工正在使用特殊的硬件和電力來挖掘和維護比特幣的主鏈 (Layer1)
- 礦工只是周期性地為每條側鏈計算一個小的哈希值 (每3個月一次)，基本上沒有任何額外成本，並從每條側鏈的經濟活動中獲得收益 (交易費，智能合約費等全部捆綁起來)
- 側鏈及其應用因此與PoW綁定，比PoS更值得信賴。只要有一條成功的側鏈，礦工就能賺到更多的錢

- 每個側鏈 (第 2 層) 本質上都是它自己的區塊鏈: 您可以使用任何塊大小、任何代幣、任何智能合約、DApp 功能、任何您想要的規則和功能來配置它
- 側鏈 (Layer2) 不受比特幣主鏈 (Layer1) 的限制。任何人都可以啟動側鏈並開始試驗想法，無需許可。本質上，可以存在 N 個側鏈。每個側鏈都是自己的應用程序和生態系統。把它想像成微信: 微信是Layer1, 所有的小程序都是Layer2 (側鏈)。

- 一旦比特幣升級到 BIP300/Drivechain 標準，比特幣本質上可以通過側鍊為開發者和用戶提供他們想要的任何功能。
- 在你的側鍊中，你不會被迫使用比特幣的小塊大小或比特幣的任何規則。你可以讓你的區塊和你希望它們在你的側鍊中的大小一樣大，並為你的側鍊提供任何功能、代幣和任何你想要的東西。
- 所有的好處，沒有缺點，比特幣礦工的豐厚回報，整個網絡的安全性更高。
- 比特幣（Layer1）礦工不需要關心側鍊（Layer2）在做什麼。側鍊如何運作和產生費用不是礦工關心的問題。就像商場經營者收取租金一樣。
- 無風險：任何製作不當、被黑客攻擊或無能的側鍊（Layer2）都不會影響比特幣主鏈（Layer1）的安全。

(#1) Full Autonomy



20 years later and
all of these things
fit in your pocket.



我們曾經有許多不同的設備，每個功能和用例都有一個。現在，計算機和智能手機可以在一台設備上完成所有工作。一旦升級到 Drivechain，比特幣將成為各種應用程序的基礎層

3.新的比特幣分叉:

Layer Two Labs將在2023年發布自己的PoW區塊鏈，並安裝所有的Drivechain升級。我們稱之為Mainchain:

- 幾個Sidechains (DApp) 會在發佈時準備好。
- 加密開發者可以使用Mainchain來實驗他們自己的DApp。
- 把Mainchain想像成一個沒有許可的iOS:你可以在Mainchain上做任何你想做的應用，只要繼續創建你自己的Sidechain，然後開始創新。

- 啟動DApp需要包括:

a. Truthcoin -去中心化預測市場，允許世界各地的用戶使用加密貨幣下注事件的結果（eg：誰將是下一任美國總統）。萬億美元的市場。自2010年開始開發。

b. ZCash:我們版本的高隱私令牌。在暗網上，比特幣早已被門羅幣和ZCash搶走了午餐。我們的Zcash Sidechain將為礦工挽回部分損失的收入。

c. BitAssets: 一個比Ordinals更經濟的NFTSidechain。

d. BitNames: 有可能取代ICANN進行域名註冊。

e.以及和更多的迭代更新。

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.優勢:

Layer Two Labs的Mainchain允許創建真正去中心化的DApp、智能合約、新代幣和其他新穎的想法，以存在於真正去中心化的網絡上。每個側鏈的開發人員可以確定鏈的塊大小、每個塊的分鐘數以及任何參數。一切都可以根據開發人員的喜好進行調整。

- 每個Sidechain（Layer 2）對Mainchain（Layer 1）不構成技術風險，即使有Sidechain斷裂。
- 礦工挖礦Mainchain將從每個Sidechain獲得所有交易費用。Sidechain越多，使用這些Sidechain的人越多，礦工的收入就越多。

5.誰受益？

a) 礦工:擁有SHA256/BTC挖礦設備的礦工從挖礦BTC切換到Mainchain。從Mainchain中自動獲得區塊獎勵，MC交易費用，以及每個MC Sidechain的交易費用。不需要額外的硬件，不需要額外的成本來賺取額外的利潤。

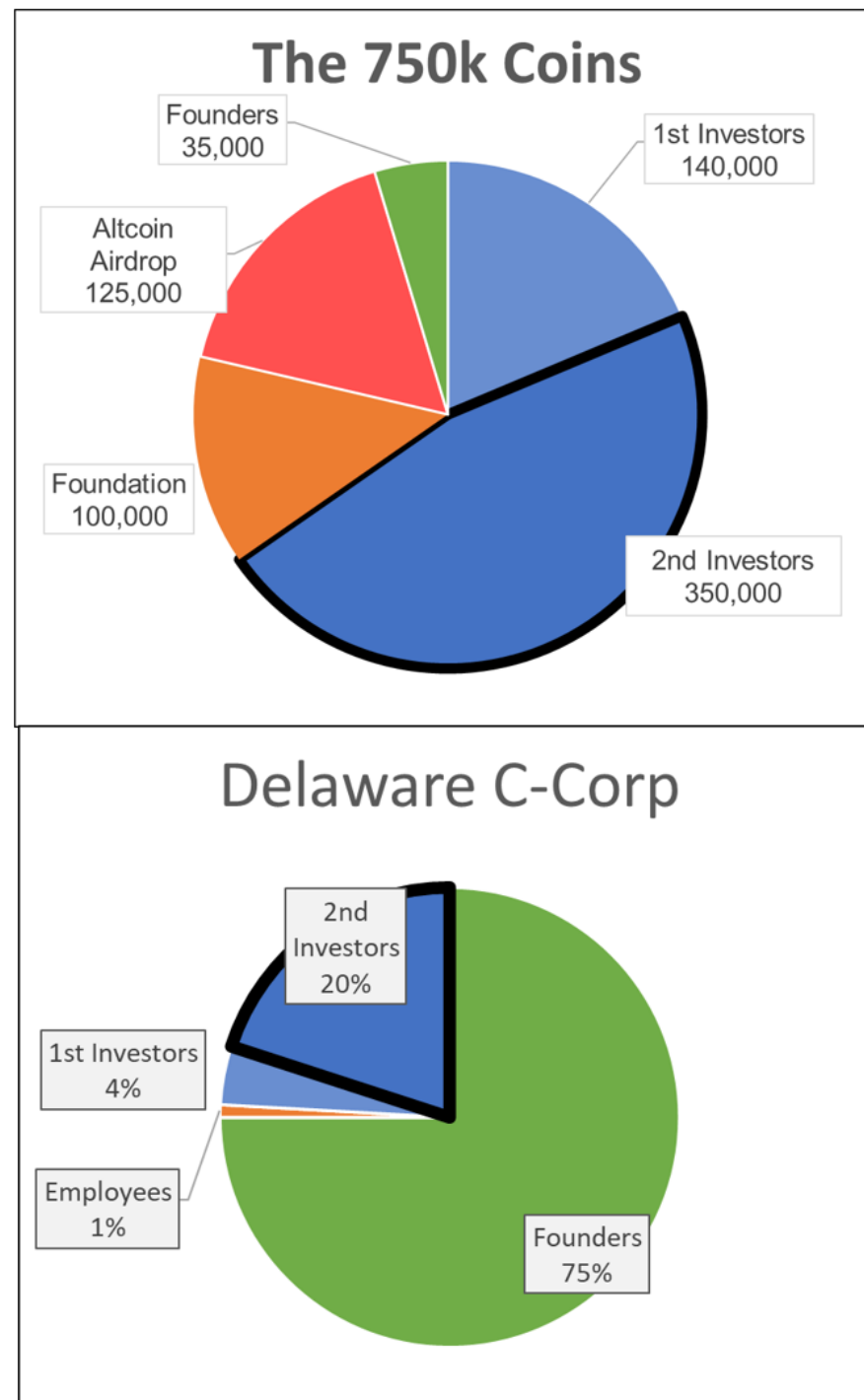
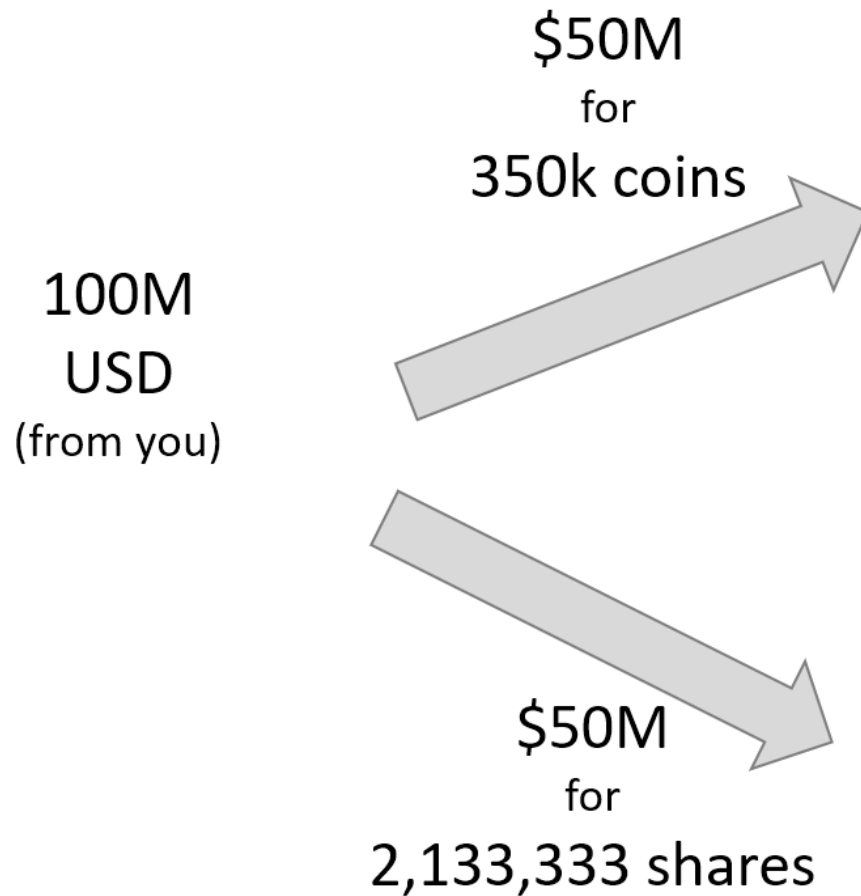
-如果由於MC的成功，BTC最終升級到BIP300/301, BTC礦工可以從BTC側鏈中獲得更多收益。如果在Sidechain上開發更多的代幣和應用程序，BTC礦工就可以獲得所有的獎勵，而不需要在替代幣上賭博或挖掘替代幣而不是比特幣。沒有額外的開採成本，沒有負面影響，只有好處。這有可能增加比特幣挖礦的吸引力，從而成倍增加比特幣的“安全預算”，以抵禦未來51%的攻擊。

- 開發者和用戶：MC和（可能）支持驅動鏈的BTC將是唯一事實上支持DApp和其他創作的工作量證明鏈。
- 任何人都可以在自己的Sidechain上進行實驗。不需要許可。
- 任何容易受到政府乾預的東西都有更好的生存機會，例如預測市場應用。
- 與以太坊（PoS）、Solana（每天都要休息）、BSC、Tron等相比MC是一個更強大的基礎，可以構建有用的應用程序。

6. 代幣經濟學/投資:

- 種子輪（2022年）:籌集了400萬美元，用於140,000個Mainchain（MC）幣和4%的公司股份。
- 第二輪（2023年）:1億美元的目標，獲得350,000個MC幣和20%的公司股份。
- 50%的投資將用於MC, 50%將用於公司股份。
- MC的挖礦，總供應和減半計劃將跟隨BTC:每個區塊10分鐘，總MC 2100萬，每4年減半。
- 所有現有的BTC地址將1:1接收MC幣。
- Mainchain將在BTC區塊號~805,000處從BTC分叉。
- 所有現有的SHA256（BTC的PoW算法）挖礦設備都可以挖MC。
- Sidechain（L2）對Mainchain（L1）無風險。
- 礦工可以選擇殺死Sidechain，但需要多數人達成共識:基本上所有的側鍊及其應用都是不可審查的，不可阻擋的。只有當一個巨大的問題出現，大多數礦工同意停止Sidechain時才有可能。

Terms – USD for Coins & Shares



Valuations

\$142.8 per coin

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

...plus...

20% of a
\$250 M
company.

History / Timeline

- 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.
- Mar 2023 – **\$100M** to build our coalition (branding, promotion, education).

Fundraising History	
1 of 2	2 of 2
\$3 M completed Sep 2022	\$100 M today
Today: 2 nd and Final Round	

7.不同於其他比特幣分叉：

- Bitcoin Cash (BCH) 和其他比特幣分叉是非常政治化的，沒有技術上的改進。
- 他們鼓勵某些類型的使用（例如用你的BCH買咖啡），並與類似邪教的領導人（例如 Craig Wright, Jihan Wu）建立了封閉的社區。
- 他們不允許開發者進行太多創新，也沒有像Drivechain和Sidechain樣的新技術。
- Mainchain不是政治性的：
 - 這是一個開放的，無需許可的系統，任何人都可以開始自己的Sidechain。
 - L2L將鼓勵和支持那些想要在Mainchain上創新的開發人員，按照他們的意願進行實驗。



Craig Wright, BSV



Jihan Wu, BCH

8. Mainchain/Drivechain如何比其他比特幣Layer 2第二層技術更好:

- Stacks: STX是一個騙局，它並不像它聲稱的那樣“在比特幣上運行應用程序”。
- Rootstock: RSK在發佈時沒有為終端用戶提供任何應用程序，只是等著人們在上面開發一些東西。基金會管理不善。沒有單獨的。沒有公關。經理們並不是真正有創造力的人。不知道投資什麼和不投資什麼。
- 閃電網絡Lightning Network: LN並不適合製作應用程序，它只是一種允許用戶之間更快、更便宜地傳輸BTC的方式，同時減少BTC礦工的收入。過度炒作。但沒有實際用途導致沒有人想花他們的比特幣。
- Taproot: Adam Back: “Drivechain可以說比Taproot更有用。”

9. 潛在的結果:

- a. Mainchain失敗，但投資者獲得“少量”回報。
- b. Layer Two Lab是成功的，實現了Blockstream無法實現的里程碑。
 - 公司估值接近或超過Blockstream目前的32億美元。
 - 最終BTC因為拯救BTC的壓力升級到BIP300。
 - MC的DApps很容易遷移到BTC。
 - MC可能會終止在這個過程中。
 - 但是給投資者帶來巨大回報。
- c. BTC從不升級。MC的生態系統是成功和繁榮的。
 - BTC在默默無聞中死去。
 - MC摧毀了競爭，成為最強的PoW鍊和任何去中心化應用開發的最理想平台。
 - 投資者瘋狂的回報。

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 <u>and</u> are early adopters in the \$100T hyper-coin!
The coins and the shares are worth very little. (Perhaps a BCH "fail valuation", of <u>130 \$/coin</u> .)	Our company "LayerTwo Labs" becomes comparable to Blockstream (valued at <u>\$3.2 Billion</u> in Aug 2021, via Series B raise). <i>(Except vastly superior, having succeeded exactly where they failed.)</i> Our coin would be worth \$0, as the Bip300-BTC would crush all other coins.	Our coin destroys all <u>rivals</u> and reaches the "hyper-bitcoinization" optimum price (~ <u>\$15M per coin</u>). <i>(Our company also becomes worth more than Blockstream, but this is a drop in the bucket in terms of ROI.)</i>
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.

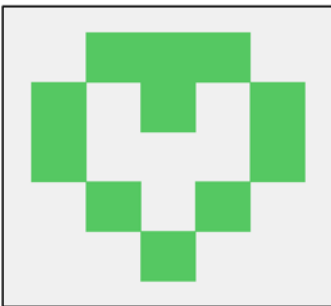
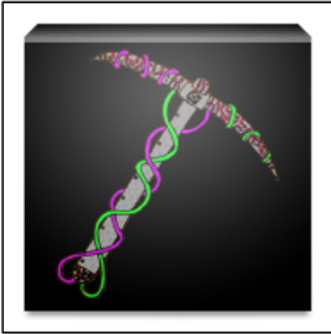
10. 路線圖:

- H1 2023: 第二輪融資, 1億美元。
- H2 2023: 為Mainchain創建開發者社區, 鼓勵和支持在MC上開發有用Sidechain的項目, 與政府 合作鼓勵使用MC。
- H2 2023: 鼓勵更多PoW礦工挖MC。

11. 關於創始人：

- Paul Sztorc可以被認為是“下一個Adam Back博士（PoW共識的創造者）”。
- Paul是Drivechain和Truthcoin等幾項重要技術的發明者。
- L2L的團隊和種子輪投資者是該領域的老手，其中許多人在加密領域擁有超過10年 的經驗。
- L2L的核心創始團隊擁有比特幣開發、替代幣開發、智能合約，以及在Kraken Exchange和BlockFi擔任關鍵職位的經驗。

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.

JUNE 2022

The "Sidechain Vision" for Bitcoin27 Jun 2022

APRIL 2022

Lightning Network -- Fundamental Limitations04 Apr 2022

OCTOBER 2021

Security Budget II, Low Fees, and Merged Mining15 Oct 2021

FEBRUARY 2021

Sidechain For BitNames/Logins/DNS, Taking on ICANN05 Feb 2021

Sidechains for Scaling -- Thunder Network05 Feb 2021

Sidechains for Privacy -- zSide and Melt/Cast05 Feb 2021

JANUARY 2021

OpenVote - Auditable, Fast, Private, Secure Voting10 Jan 2021

JUNE 2019

The Consent of the Governed21 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 Run14 Feb 2019

DECEMBER 2018

Imposed Mutual-Exclusivity (IMEX) for Hard Forks20 Dec 2018

NOVEMBER 2018

Gradually Activated Replay Protection (GARP) - Toward Hard Fork Suck13 Nov 2018

Deniability - Unilateral Transaction Meta-Privacy09 Nov 2018

SEPTEMBER 2018

Expensive Privacy is Useless Privacy11 Sep 2018

Five Lies and the Truth11 Sep 2018

JUNE 2018

BitAssets - A Digital Assets Sidechain21 Jun 2018

APRIL 2018

Meditations on Fraud Proofs14 Apr 2018

Blockchain Fusion (via Compensated Sidechains)07 Apr 2018

Bitcoin Post-Maximalism07 Apr 2018

MARCH 2018

GigaChain20 Mar 2018

NOVEMBER 2017

The UASF Contradiction02 Nov 2017

The MAHF And Replay "Protection"02 Nov 2017

More Terminology -- Forks and Splits02 Nov 2017

Miners Don't Control Tx-Selection02 Nov 2017

ASICBoost is Worthless02 Nov 2017

OCTOBER 2017

Fork Futures (via the Exchanges)12 Oct 2017

JULY 2017

Proof of Stake is Still Pointless07 Jul 2017

JANUARY 2017

Blind Merged Mining30 Jan 2017

Mining - Threat Model and Equilibrium Analysis29 Jan 2017

The Mirage of Miner Centralization28 Jan 2017

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

Two Types of Blockspace Demand10 Jan 2017

DECEMBER 2016

Against the Hard Fork06 Dec 2016

Better Fork Terminology05 Dec 2016

MAY 2016

BTC Codex - The Digital Identity Sidechain21 May 2016

The Drivechain OP Code14 May 2016

MARCH 2016

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

OCTOBER 2015

The Hashing Heart Attack28 Oct 2015

PSA - Linking to a Blog Section05 Oct 2015

SEPTEMBER 2015

Oracles are the Real Smart Contracts21 Sep 2015

Measuring Decentralization09 Sep 2015

AUGUST 2015

Nothing is Cheaper than Proof of Work04 Aug 2015

JULY 2015

The Win-Win Blocksize Solution14 Jul 2015

MAY 2015

Bitcoin and Deflation, The Last Word15 May 2015

JANUARY 2015

BitUSD Isn't Worth The Trouble29 Jan 2015

NOVEMBER 2014

The Limits of Blockchain Tech28 Nov 2014

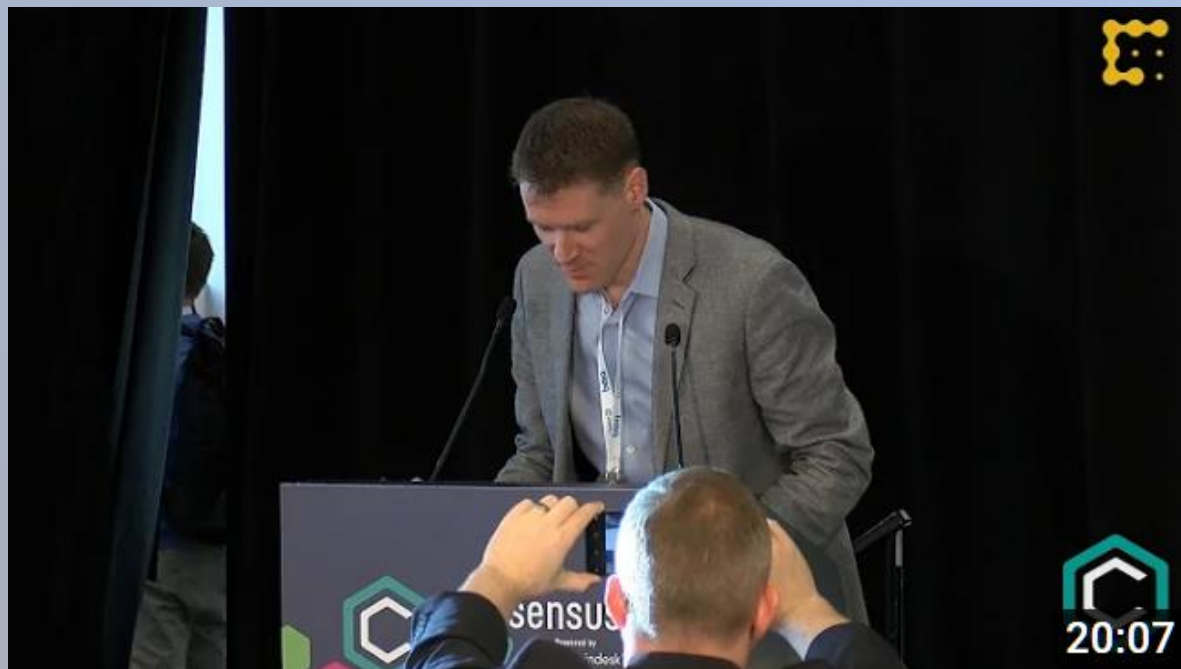
Altcoins Aren't Money, They're Bitcoin's Casino/Laundromat28 Nov 2014

Long Live Proof-of-Work, Long Live Mining16 Nov 2014

Active Decentralization09 Nov 2014

Three Basics06 Nov 2014

Introducing Tonight's Entertainment05 Nov 2014



Website:

www.layertwolabs.com

Downloads:

<https://github.com/LayerTwo-Labs>

<https://layertwolabs.com/download>

<https://www.drivechain.info/releases/>

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/