Presto Research

Daily Market Brief

May 29, 2025 (UTC -02:00)

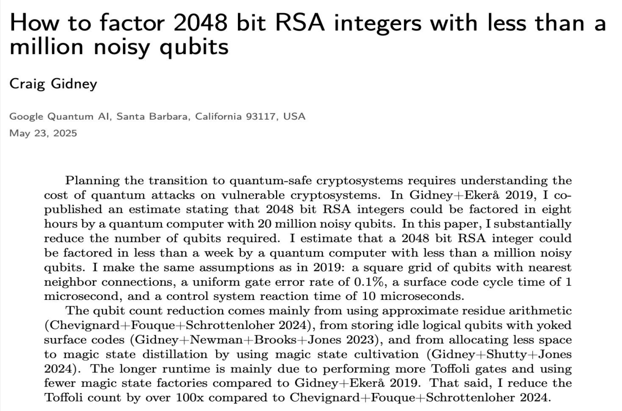
Peter Chung I Head of Research
Min Jung I Research Analyst

BTC	$107,786.70 -1.1%	**S&P500**	5,888.56 -0.6%	**US 10Y**	4.5091% +0.0645PPT	**WTI**	$62.26 +2.2%
ETH	$2,681.20 +0.8%	**Nasdaq**	19,100.94 -0.5%	**DXY**	100.40 +0.9%	**Gold**	$3,282.67 -1.4%

- $BTC is slightly down. As of now, $BTC is trading at $107,786 and $ETH at $2,681. Bitcoin dominance stands at 63.75%.
- NVIDIA reported Q1 FY2026 revenue of $44.1 billion (+69% YoY), slightly beating expectations, with data center revenue surging 73% to $39.1 billion. Meanwhile, the Fed's May minutes showed downgraded GDP growth projections for 2025–2026 due to trade policy drag, with unemployment expected to remain above the natural rate through 2027.
- A few other headlines include: Telegram plans to raise $1.5B via 5-year bonds at a 9% yield, backed by Citadel, BlackRock, and Mubadala; GameStop announced the purchase of 4,710 BTC; and Don Jr. and Eric Trump predicted Bitcoin could surpass $170,000 by the end of 2026.
- During the last 24 hours, the top three gainers were $ZBCN, $SPX, and $TON, while the top three losers were $XMR, $XDC, and $KAITO.

Google Research Signals Quantum Leap's Rapid Rise

The notion that quantum computing is a distant threat is increasingly outdated, as recent advances reveal a faster-than-expected trajectory. A new paper by Google Quantum AI researcher Craig Gidney shows that cracking RSA encryption may require 20 times fewer quantum resources than previously thought. While Bitcoin relies on elliptic curve cryptography, not RSA, this underscores quantum technology's exponential scalability. Ironically, the crypto industry leads in quantum risk awareness – a focus vital for all, given the technology's potential to disrupt banking, military, power grids, and beyond. Yet, the decentralized nature of crypto networks complicates the shift to quantum-safe standards, necessitating urgent coordination. Start exploring quantum computing today, as its impact could rival AI's within five years, rewarding early adopters. Begin with Quantum Computing x Crypto: Everything You Need To Know and Quantum Computing Expert Answers All Your Crypto Questions, by Presto Research analyst Rick Maeda in collaboration with Dr. Isaac Kim at UC Davis.



How to factor 2048 bit RSA integers with less than a million noisy qubits

Craig Gidney

Google Quantum AI, Santa Barbara, California 93117, USA
May 23, 2025

Planning the transition to quantum-safe cryptosystems requires understanding the cost of quantum attacks on vulnerable cryptosystems. In Gidney+Ekerå 2019, I co-published an estimate stating that 2048 bit RSA integers could be factored in eight hours by a quantum computer with 20 million noisy qubits. In this paper, I substantially reduce the number of qubits required. I estimate that a 2048 bit RSA integer could be factored in less than a week by a quantum computer with less than a million noisy qubits. I make the same assumptions as in 2019: a square grid of qubits with nearest neighbor connections, a uniform gate error rate of 0.1%, a surface code cycle time of 1 microsecond, and a control system reaction time of 10 microseconds.

The qubit count reduction comes mainly from using approximate residue arithmetic (Chevignard+Fouque+Schrottenloher 2024), from storing idle logical qubits with yoked surface codes (Gidney+Newman+Brooks+Jones 2023), and from allocating less space to magic state distillation by using magic state cultivation (Gidney+Shutty+Jones 2024). The longer runtime is mainly due to performing more Toffoli gates and using fewer magic state factories compared to Gidney+Ekerå 2019. That said, I reduce the Toffoli count by over 100x compared to Chevignard+Fouque+Schrottenloher 2024.

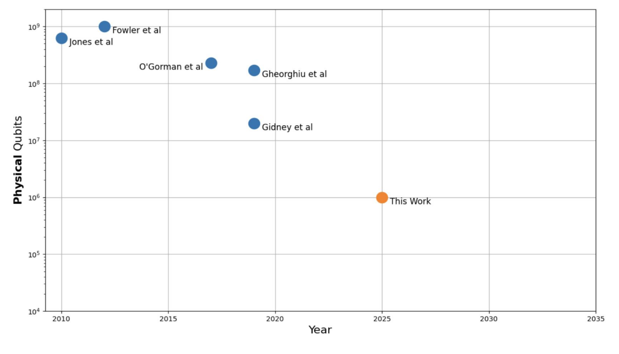
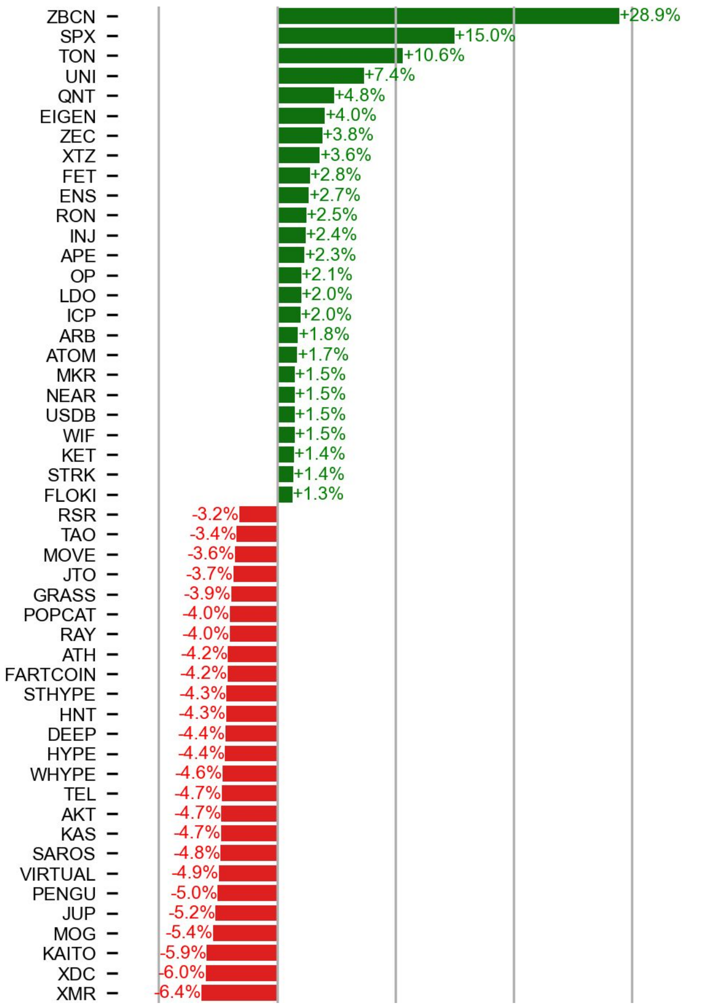


Figure 1: Historical estimates, with comparable physical assumptions, of the physical qubit cost of factoring 2048 bit RSA integers. Includes overheads from fault tolerance, routing, and distillation. Results are from [Jon+12; Fow+12; OC17; GM19; GE21]. Results such as [Van+10] and [LN22] aren't included because they target substantially different assumptions or cost models.

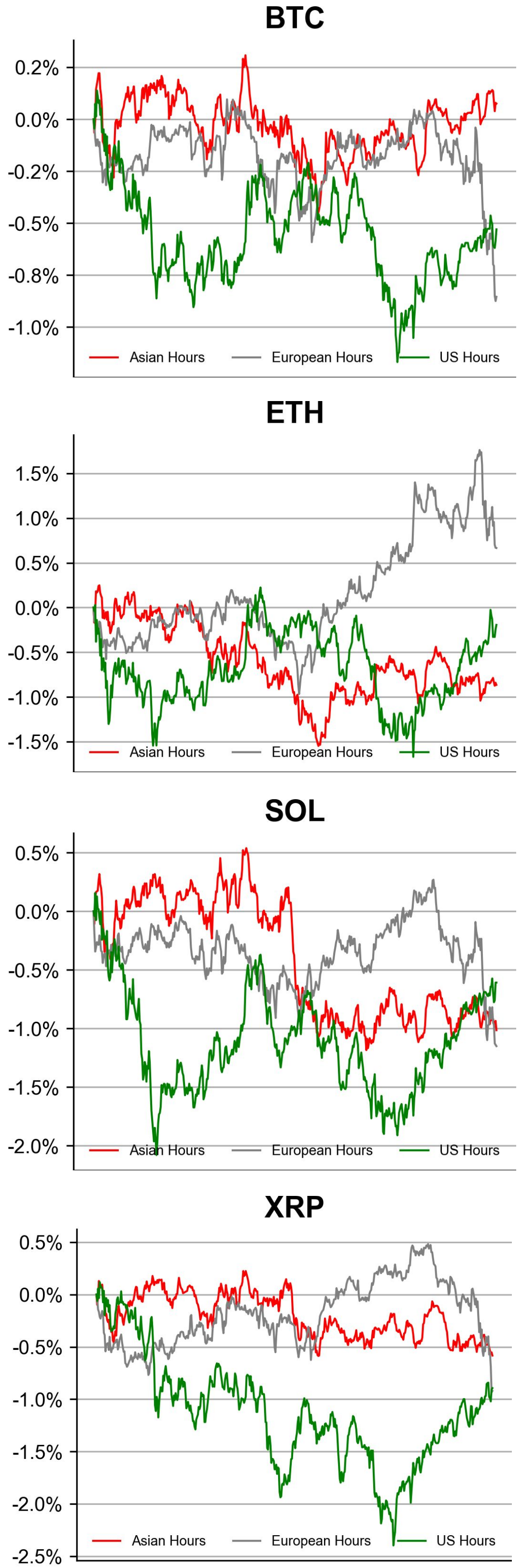
Source: Google Quantum AI

PRICE ACTIONS

24H Price Change (Top/Bottom 25 from Top 200)



Time Zone Analysis

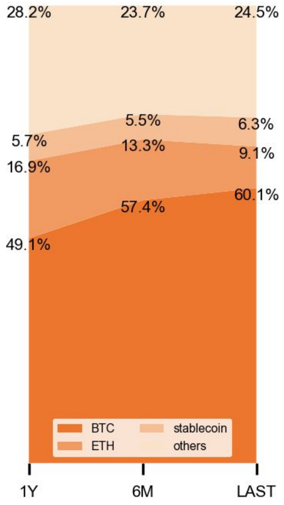

BTC

ETH

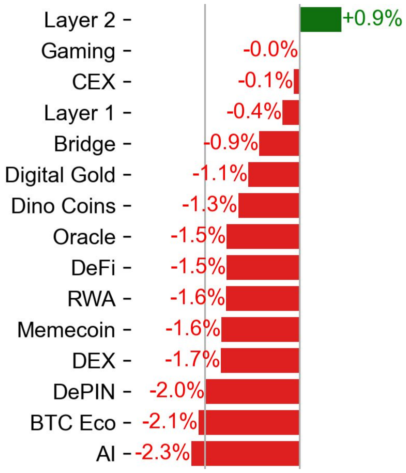
SOL

XRP

Dominance Ratio

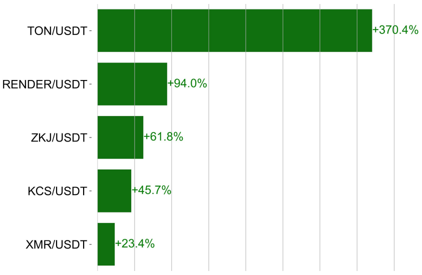


Sector Performance



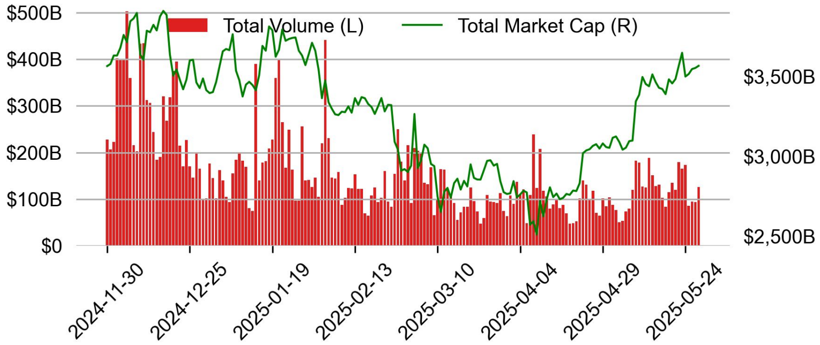
TRADING VOLUME

24H Vol % Chg*

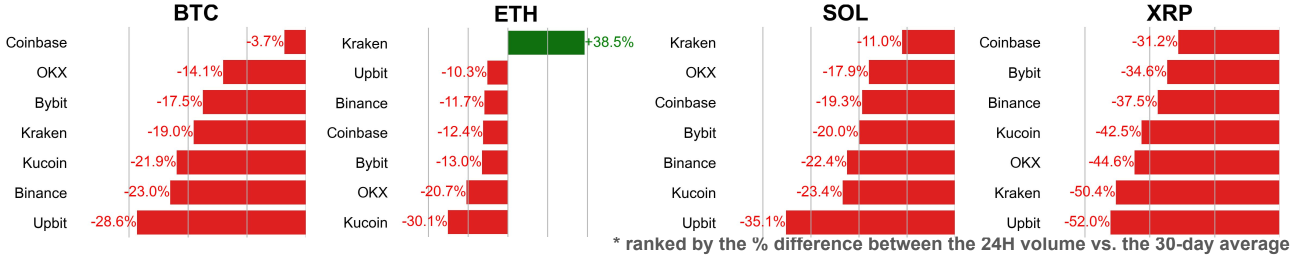


* 5 largest 24H vol. change from the universe of top 50 assets by market cap

Spot Volume



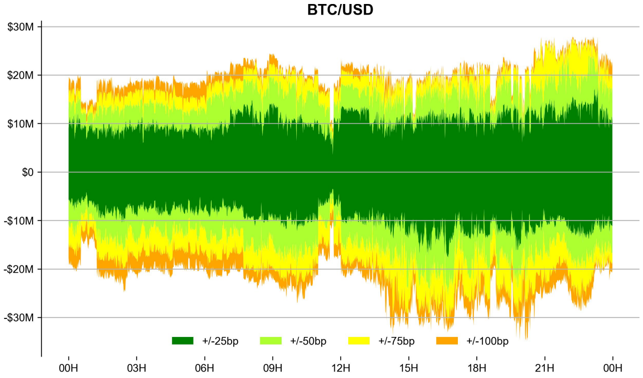
Spot Volume Leaders (% chg vs ave)*

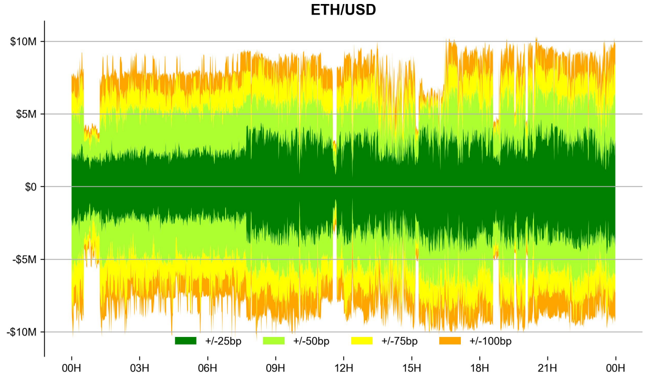


* ranked by the % difference between the 24H volume vs. the 30-day average

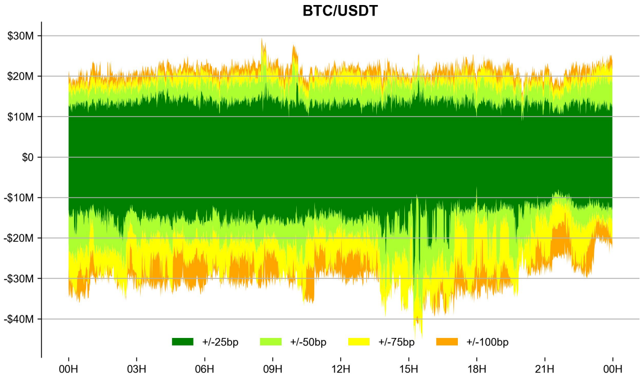
ORDER BOOK DEPTH (within 1% best bid/ask)

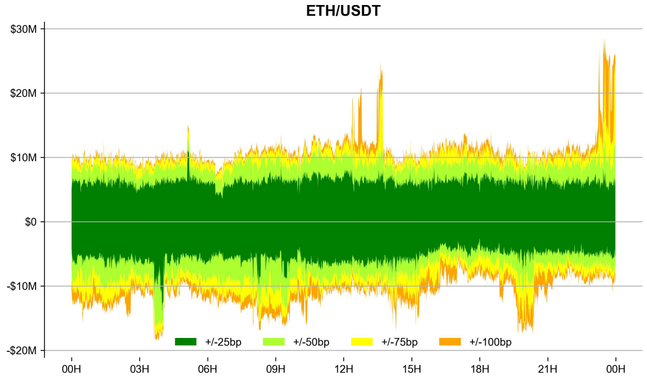
Coinbase





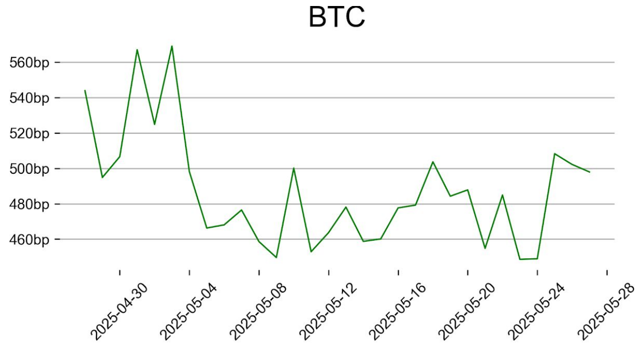
Binance

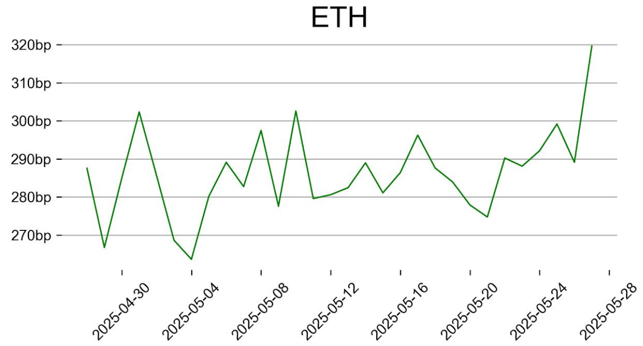




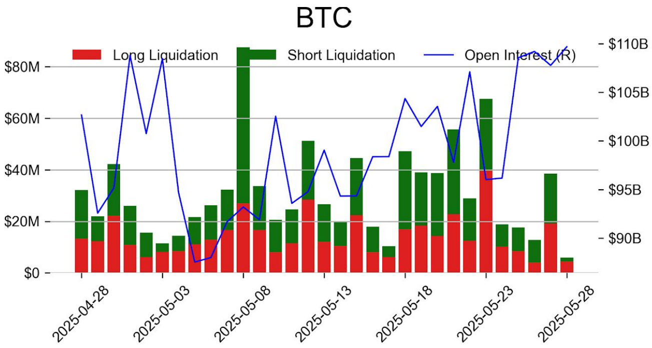
DERIVATIVES

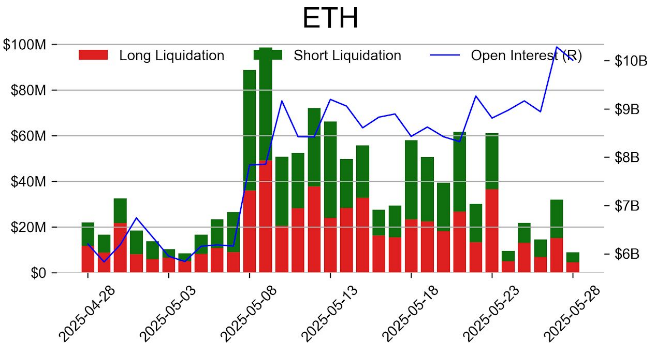
Open Interest / Market Cap


BTC

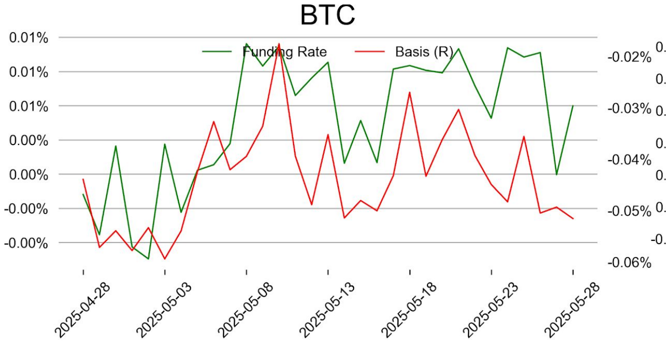

ETH

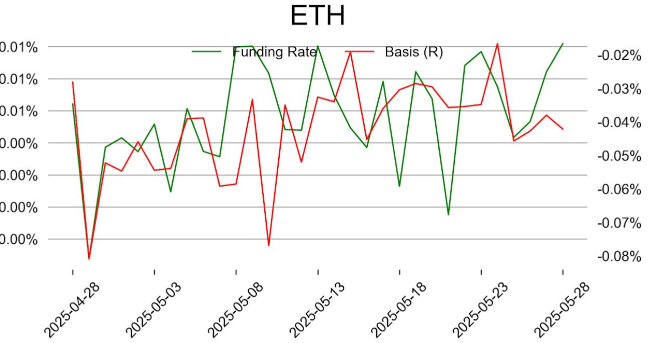
Futures O.I. & Liquidations


BTC

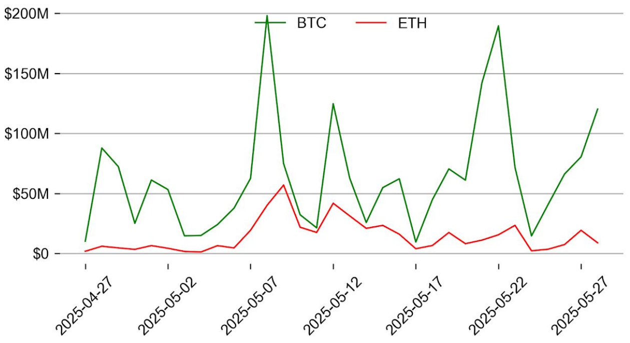

ETH

Perps Funding Rate & Rolling Basis

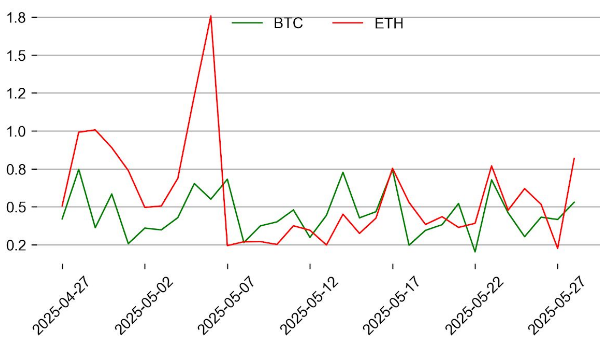

BTC


ETH

Option Volume



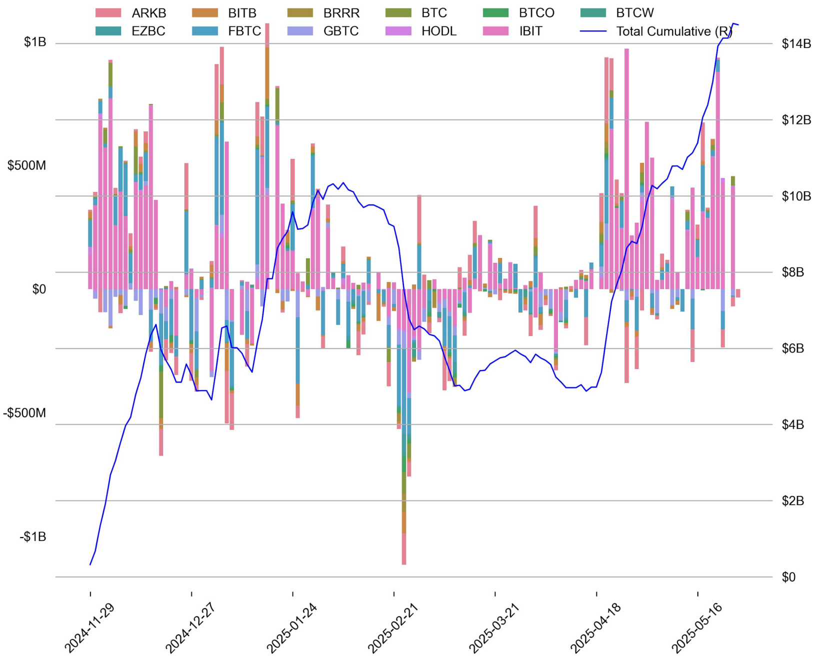
Put Call Ratio



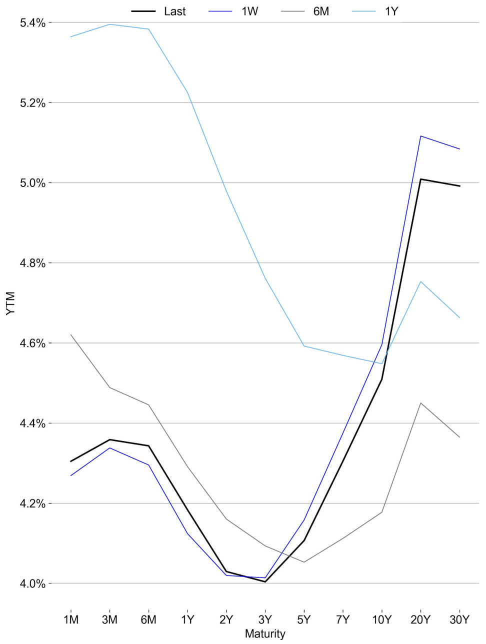
TRADFI

	Stocks					FX				Commodity		Crypto Equity			
	S&P500	Nasdaq	EuroStoxx50	HSI	CSI300	USD/EUR	USD/JPY	USD/CNY	DXY	WTI	Gold	COIN	MSTR	MARA	RIOT
Last	5888.56	19100.94	5376.25	23258.31	3836.24	0.8904	145.72	7.1948	100.40	62.26	3282.67	254.29	364.21	14.86	8.38
1D	-0.6%	-0.5%	-0.7%	-0.5%	-0.1%	0.9%	1.0%	-0.0%	0.9%	2.2%	-1.4%	-4.5%	-2.1%	-9.6%	-8.3%
1M	6.5%	10.0%	4.0%	5.9%	1.4%	1.7%	2.6%	-1.4%	1.4%	0.3%	-1.5%	23.9%	-1.4%	6.1%	9.8%
1Y	11.0%	12.2%	6.9%	23.6%	6.3%	-3.3%	-7.3%	-0.7%	-4.0%	-22.0%	38.7%	3.8%	-78.3%	-28.3%	-19.0%

BTC Spot ETF Flow

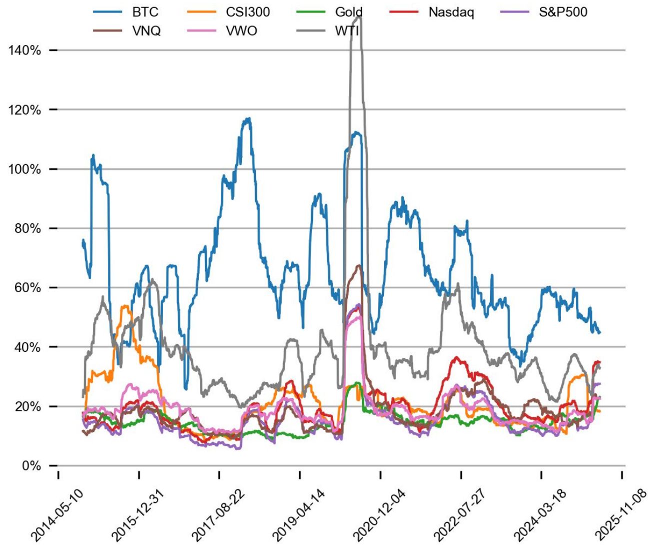


US Treasury Yield Curve

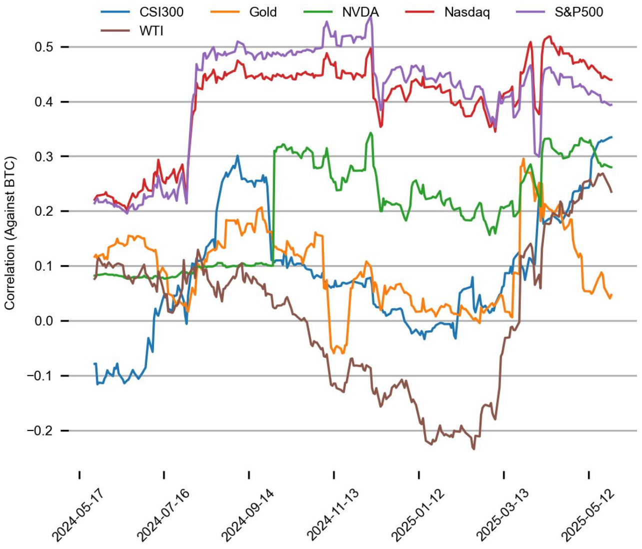


CROSS ASSET METRICS

Volatility



Correlation

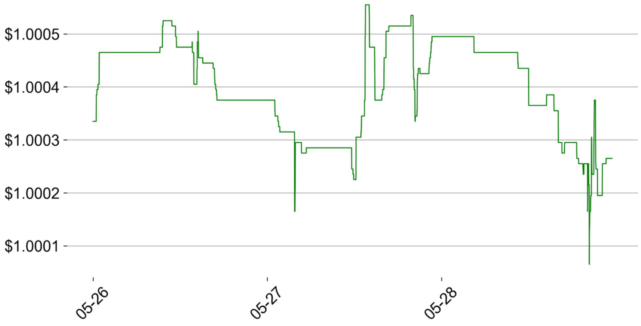


STABLECOIN

Supply Change

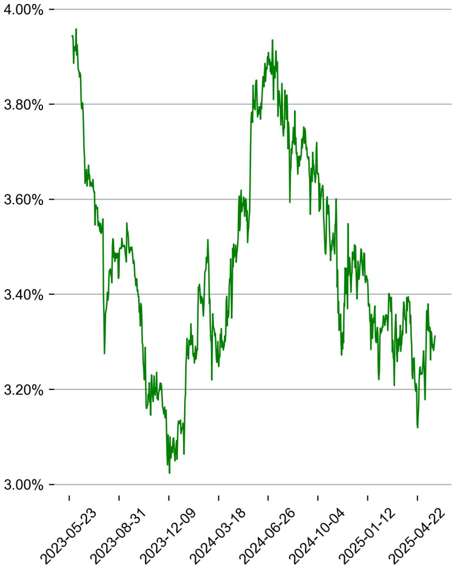
	Market Cap ($mn)	Share	7D Change
USDT_Tron	76,284	31.0%	+1.1%
USDT_Ethereum	62,490	25.4%	+0.4%
USDT_Omni	83	0.0%	0.0%
USDC	60,805	24.7%	+1.3%
DAI	4,576	1.9%	+1.2%
FDUSD	1,366	0.6%	+9.8%
Others	40,337	16.4%	+0.6%
Total	245,942	100.0%	+0.9%

USDT Prem/Disc

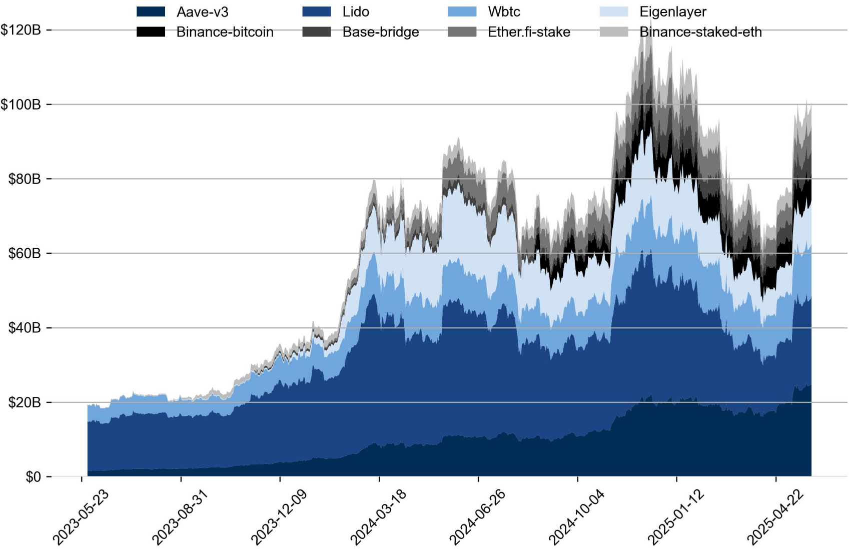


ONCHAIN MOVES

TVL/Crypto MC



Top TVL by Protocol

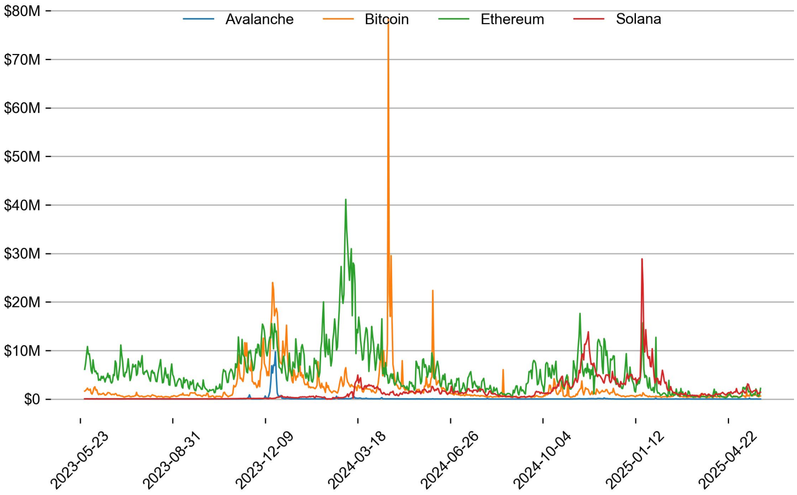


Top TVL Gainers*

#	Name	7D Change
1	ether.fi Liquid	+111.6%
2	Stacks sBTC	+65.2%
3	Solv Strategies	+45.7%
4	Pell Network	+36.4%
5	Unit	+33.9%

* 5 largest 7 day TVL change in % terms from the universe of minimum $100m TVL protocols, according to DefiLlama.

Daily Network Fees



EVENTS CALENDAR		
Date	**Title**	**Coins / Hosts**
May 6, 2025	End of BOYCO	$BERA
May 7, 2025	US FOMC	
May 7, 2025	Pectra Upgrade	$MNT
May 7, 2025	TGE	$OBOL
May 8, 2025	Temporary Ceasefire in the Russia Ukraine	
May 8, 2025	Earnings Call	$COIN
May 8, 2025	Big Announcement	$ZK
May 8, 2025	$12M Unlock	$MOVE
May 12, 2025	US Federal Budget Balance	
May 12, 2025	SEC Virtual Asset TF 3rd Roundtable	
May 12, 2025	$62M Unlock	$APT
May 13, 2025	US CPI	
May 13, 2025	Trump Middle East Visit	
May 15, 2025	US PPI	
May 19, 2025	CME XRP Futures	$XRP
May 22, 2025	Dinner with Trump	$TRUMP
May 28, 2025	Earnings call	$NVDA
May 30, 2025	FTX 2nd Repayment	$FTT

DATA EXPLAINER

Headers	Source	Note
PRICE ACTIONS TRADING VOLUME ORDER BOOK DEPTH DERIVATIVES	Presto Labs	**Time Zone Analysis** separates out the asset's price action according to the business hours in Asia, Europe and US region. This is to identify which geography is responsible for price actions of the last 24hrs. The cut-offs are, - Asia: UTC 22:00 -1 to UTC 6:00 - Europe: UTC 6:00 to 14:00 - US: UTC 14:00 to 22:00 **Sector** constituents are, AI(FET, AGIX, OCEAN), BTC Eco(BCH, BSV, ICP, STX, ORDI), CEX(BNB, CRO, OKB, KCS, BGB), Data(LINK, GRT), DePIN(ICP, FIL, AR, HNT, SIA), DEX(UNI, INJ, RUNE, SNX, DYDX, OSMO, CRV, CAKE, GMX), Digital Gold(BTC), Gaming/Metaverse(IMX, BEAM, SAND, GALA, AXS, WEMIX, RON), L0(AVAX, DOT, TIA), L2(MATIC, OP, MNT, ARB, STRK), Lending(MKR, AAVE, COMP), Liquid Staking(LDO, RPL, JTO), Meme(DOGE, SHIB, FLOKI), NFT(APE, BLUR), Payments(XRP, LTC, XLM, XMR, ZEC), RWA(ONDO, CFG), Smart Contract(ETH, BNB, SOL, ADA, TRX, TON, APT, NEAR, HBAR, VET, ALGO, FTM, SUI, FLOW, MINA). The sector return is market-cap weighted average of the constituents' returns. **Exchanges:** 24H spot price & volume % changes and dominance ratios are from CoinGecko. Time Zone Analysis is based on data from Binance. Spot volume leaders are based on data from Binance Bybit, Coinbase, Kraken, OKX, KuCoin, HTX, Upbit, Gate.io. Futures data are from Binance OKX, Bybit, KuCoin. Options data are from Deribit.
TRADFI	Investing.com Farside Investors	**BTC Spot ETF Flows** are based on data shown on farside.co.uk at UTC 03:00. Due to varying data reporting schedules among ETF sponsors, the figures may not encompass data from all 10 ETFs.
STABLECOIN ONCHAIN MOVES	DefiLlama	**Stablecoin Supply** is a proxy for fiat on/off ramp from TradFi into crypto. **USDT Prem/Disc** reflects the USDT supply/demand imbalance, approximating the market's risk aversion towards USDT specifically, and/or the crypto market more broadly. The data is from Coinbase. **TVL/ Crypto MC Ratio** = Total Value Locked / Crypto Market Cap. The ratio neutralizes the TVL changes caused by asset price fluctuations.
EVENTS CALENDAR	CoinMarketCap Layer GG	**Events Calendar** provides a summary of major events happening throughout the month.

* The Daily Market Brief is published every business day, following the Singapore calendar, excluding public holidays

About Presto

Presto is an algorithmic trading firm where researchers and engineers solve challenging problems in global financial markets. Our core strength lies in combining engineering, mathematics, and science to navigate both digital asset and traditional finance markets with precision. Presto Research, our research unit, provides expert-driven insights to help navigate these markets effectively.

Find out more at https://www.prestolabs.io.
Follow Presto for more content: X, LinkedIn
Follow Presto Research for latest research : X, Telegram

Authors

Peter Chung, Head of Research X, Telegram, LinkedIn
Min Jung, Research Analyst X, Telegram, LinkedIn

Required Disclosures

Any expression of opinion (which may be subject to change without notice) is personal to the author and the author makes no guarantee of any sort regarding accuracy or completeness of any information or analysis supplied. The views and opinions expressed herein are those of the author(s) and do not necessarily reflect the views of Presto or its affiliates. This material by itself, is not and should not be construed as an offer or a solicitation to deal in any investment product or to enter into any legal relations. This material is for informational purposes only and is only intended for sophisticated investors, and is not intended to provide accounting, legal, or tax advice, or investment recommendations, or an official statement of Presto or its affiliates. Presto, its affiliates and its employees make no representation and assume no liability to the accuracy or completeness of the information provided. Presto, its affiliates and its employees also do not warrant that such information and publications are accurate, up to date or applicable to the circumstances of any particular case. Certain statements in this document provide predictions and there is no guarantee that such predictions are currently accurate or will ultimately be realized. Prior results that are presented here are not guaranteed and prior results do not guarantee future performance. Recipients should consult their advisors before making any investment decision. Presto or its affiliates may have financial interests in, or relationships with, some of the assets, entities and/or publications discussed or otherwise referenced in the materials. Certain links that may be provided in the materials are provided for convenience and do not imply Presto's endorsement, or approval of any third-party websites or their content. Any use, review, retransmission, distribution, or reproduction of these materials, in whole or in part, is strictly prohibited in any form without the express written approval of Presto. Presto Research and related logos are trademarks of Presto, or its affiliates.