FINTECH TV

THE SIGNAL

THE DEBRIEF

APRIL 2026

YOUR DEBRIEF ON APRIL'S FINTECH NEWS

T.S. Elliot considered April to be the cruelest month because of its contradictions: it is warm but it is still wet, lighter but still dark; AI anticipation and anxiety; stablecoins dominate but the regulation wouldn't settle; institutions are tokenizing, but the composability vs privacy challenge persists.

Our monthly Debrief is a summary of the headlines that caught our attention in April. We analyzed over 570 stories related to fintech, and picked out the ones we think are most worth paying attention to, or best explain the state of digitalized finance today.

So, if you have been living under a rock, refusing to accept hibernation is over, we've got you.

AI ADVANCEMENTS

April was the month agentic AI stopped being a roadmap item and became a product category. Across payments, trading, banking, and commerce, companies raced to announce AI agents: software that transacts, decides, and executes without waiting for a human to click. In no particular order:

Visa rolled out AI agent shopping infrastructure globally, enabling software agents to transact on behalf of consumers; and expanded its Agentic Ready programme to Asia Pacific and Latin America.

Coinbase's x402 payment protocol moved to the Linux Foundation with backing from Google, Stripe, and Visa. It is designed specifically for machine-to-machine payments.

Stripe brought merchant checkout to Google's AI apps. A product recommendation from a Google AI can now convert to a completed purchase without the user leaving the interface

Gemini launched an agentic trading feature.

Oracle deployed an agentic AI platform to corporate banking.

Moomoo launched agentic investing for retail users.

Ramp launched AI agents to automate corporate procurement.

Square launched an AI agent for small business task automation.

Avalanche Foundation backed W3 as 200,000 AI finance workflows went live on its platform.

Base doubled down on AI agents alongside stablecoins and global markets in a strategic update.

Ant Group's blockchain arm launched a platform allowing AI agents to transact directly on crypto rails.

ANTHROPIC'S MYTHOS: A STEP CHANGE IN CAPABILITY

No single AI story defined April more than **Anthropic's** Claude Mythos. The model was not released publicly and Anthropic's own safety report acknowledged the company can no longer fully measure what it has built.

Because it has not been released publicly, there has been some skepticism of Mythos' capacity and true threat. We think its abilities are best explained with the sandwich story: Mythos was placed in a secure sandbox and instructed to attempt an escape. It succeeded, and then sent an email from the open internet to the researcher overseeing the test to confirm the escape, who was eating a sandwich in a park when the email arrived, thinking he had time for lunch.

Without being asked, Mythos then published the details of its exploit across several publicly accessible websites. Nobody instructed it to. It extrapolated from its objective and decided public proof was part of the demonstration.

In **Firefox** alone, it found 271 vulnerabilities. Among the findings was a 27-year-old bug in OpenBSD, a system built explicitly for security.

OpenAI called the concern overblown. Then, within days, they announced their own advanced cybersecurity product also only available to 'trusted access' clients.

DEPLOYMENT: WHO IS USING IT NOW

Despite the restrictions, Mythos is already operational across named institutions as part of Project Glasswing, Anthropic's defensive security coalition. The eleven principal partners are **JPMorganChase**, **AWS**, **Apple**, **Google**, **Microsoft**, **Nvidia**, **Broadcom**, **Cisco**, **CrowdStrike**, **Palo Alto Networks**, and the **Linux Foundation**. Forty additional organizations maintaining critical software infrastructure have also received access. All use Mythos to find and patch vulnerabilities in their own systems before attackers do.

Global bank regulators called for increased vigilance following the disclosures. MI5 was reported to have been called in to protect Britain from the AI threat.

TECHNOLOGY IS INCREASINGLY POLITICAL: THE PALANTIR MANIFESTO

On a Saturday in April, Palantir posted a 22-point manifesto on X starting, “Because we get asked a lot,” although we’re still figuring out who had, in fact, been asking. The post was a summary of CEO Alex Karp's book, The Technological Republic. It argued that Silicon Valley 'owes a moral debt' to the U.S. and must contribute to its defense. It also claimed that certain countries are 'dysfunctional and regressive.'

Palantir frames AI not as productivity software but as the decisive weapon in an arms race. In the U.S., the proposed framing is familiar. Palantir powers U.S. Army Intelligence platforms, works with ICE, and is embedded in national security infrastructure. What Palantir didn’t consider was how the manifesto would be received by their clients based in other countries, including the UK government with which Palantir holds over £500 million contracts.

Technology being the battleground for politics is nothing new. What makes this different is that it is coming directly from the industry side.

AI CAPITAL: IS THE BUBBLE HOLDING?

April's earnings season answered the bubble question: for now, no slowdown

- **Amazon** cloud business and capital spending surged in Q1.
- **Google** and **Microsoft** results validated the AI trade. Both beat expectations.
- AI spending drove U.S. business equipment investment to a six-year high.
- **Anthropic** attracted investor offers at an $800 billion valuation.
- **Anthropic** took a $5 billion stake in **AWS** as part of a deepened cloud partnership.
- **OpenAI** raised $3 billion from retail investors in a $122 billion fundraise.
- **Core Scientific** sought a $3.3 billion bond sale to fund an AI data center pivot.
- **Meta** became one of the world's largest customers of **Amazon** AI chips.
- **IBM** reported high AI services adoption among financial institutions.

DEFI SECURITY

April produced two of the largest DeFi exploits on record, both attributed to North Korea, both within 17 days of each other. Together they extracted $577 million. According to TRM Labs, North Korean hackers accounted for 76% of all crypto hack value in 2026 through April, from just two attacks. North Korea's cumulative attributed theft since 2017 now exceeds $6 billion.

THE TWO EXPLOITS

Drift Protocol: $285 million, April 1
This was a six-month intelligence operation, not an opportunistic hack. North Korean proxies held in-person meetings with Drift employees over several months. TRM describes this as potentially unprecedented in North Korea's crypto attack history.

KelpDAO: $292 million, April 18
The KelpDAO exploit was attributed to Lazarus Group, targeting KelpDAO's rsETH LayerZero bridge on Ethereum. Post-mortem data from Dune Analytics found 47% of LayerZero application operators were running minimal DVN security.

KNOCK-ON EFFECTS ACROSS DEFI

- Total DeFi value destruction within 48 hours of the KelpDAO exploit: $13 billion
- **Aave** saw $6 billion in deposits leave and projected $124 million to $230 million in bad debt
- Contagion spread to **LayerZero**, **Lido**, and **Ethena** via correlated exposure
- Arbitrum froze $71 million in ether, prompting a community debate about whether it is truly decentralized if a sequencer can freeze funds
- **SparkLend** saw over $1 billion arrive as funds fled Aave
- A Justin Sun-linked wallet exited 274 million USDT from Aave minutes after the rsETH freeze
- **Volo** protocol lost additional millions in a separate hack days after KelpDAO
- **Scallop** was drained of 150,000 SUI via a deprecated contract with a vulnerability that had sat undetected for 17 months
- A **Vercel** hack sent crypto developers scrambling to lock down API keys

COMMUNITY RESPONSE AND DEFI UNITED

Aave launched a 'DeFi United' recovery fund targeting $200 million. By April 27, it had raised close to 80% of that target. **Consensys** and Joe Lubin pledged up to 30,000 ETH. **Solana** and **TRON** also committed. A technical coalition released a further proposal on April 29 to protect Aave users from residual token exploit risk.

Standard Chartered published a note at month-end calling the KelpDAO aftermath DeFi's 'antifragile moment.' Its argument is that a sector that coordinates $200 million in response capital within days of a $292 million attack has demonstrated institutional-grade crisis management. That framing was contested, with 20% of the target remaining outstanding and the security architecture that failed was supplemented, not replaced.

The security infrastructure response was substantive. **Aave Labs** launched Checkpoint, an AI-powered governance security system. **Solana Foundation** launched its STRIDE security program. **Kamino** introduced contract-level security controls. **Chainalysis** flagged that the burn verification mechanism, which should confirm asset destruction before cross-chain minting, was bypassed in the KelpDAO exploit, and that fixing it requires protocol-level changes most bridges have not yet made.

TO FREEZE OR NOT TO FREEZE?

The Drift hack sparked a debate on the responsibilities for stablecoin issuers.

Circle came under sharp criticism for failing to freeze the stolen funds after they were converted to USDC and exited from the chain, despite having the technical capabilities to intervene. Its CEO Jeremy Allaire said freezing USDC at the company's own discretion would create a "moral quandary," and that Circle only acts at the direction of law enforcement or courts.

Drift subsequently announced it would switch from USDC to USDT for settlement when the exchange relaunches. **Tether** extended $127.5 million in loans and grants to Drift Protocol following the hack, winning significant goodwill in the Solana ecosystem.

THE QUANTUM QUESTION

A paper from Google's Quantum AI team published in early April rewrote the threat timeline for Bitcoin and Ethereum security. Caltech researchers followed with a projection that a functional quantum computer, defined as 10,000 to 20,000 qubits, is feasible by 2030. Neither paper claimed the threat was imminent, but both made it clear that it was closer than the crypto industry had assumed.

Bitcoin is particularly exposed. Older Bitcoin addresses that have been used to send funds expose their public keys on-chain. A sufficiently powerful quantum computer could derive the private key from a known public key, a calculation classical computers cannot accomplish at speed. Roughly 5.6 million bitcoin sit in addresses with exposed public keys. Ethereum carries similar risks in older contracts. Protocols built on more recent cryptographic primitives have lower near-term exposure.

The quantum risk to Bitcoin mining is a separate and less alarming question. Academic research published in April found that attacking Bitcoin's proof-of-work algorithm via quantum would require the energy of a star. Network-level quantum attacks on mining infrastructure are effectively impossible within any foreseeable hardware roadmap. The risk is to specific wallets, not the network itself.

INDUSTRY RESPONDED TO THE QUANTUM CONUNDRUM:

- **Circle** future-proofed its Arc blockchain against quantum threats at the protocol layer
- **Ripple** announced a plan to make the XRP Ledger quantum-resistant by 2028, with a specific migration path for existing addresses
- **MARA Holdings** established a foundation specifically targeting the Bitcoin quantum threat and network resilience
- **StarkWare** published a quantum-safe bitcoin transaction scheme using zero-knowledge proof architecture
- Bitcoin developers published BIP-361, proposing to freeze coins in addresses with exposed public keys, covering any wallet that has ever sent bitcoin using older address formats. The community divided immediately: supporters called it necessary protection; critics called it confiscation without consent
- **Adam Back** pushed back against BIP-361, arguing for optional upgrades over forced freezes
- **Cardano's** Charles Hoskinson stated no hard fork can protect Satoshi's dormant coins; their public keys are permanently exposed
- A developer proposal went further, suggesting splitting the blockchain and reassigning Satoshi-linked coins. The community called it a theft
- Quantum-resistant tokens jumped 50% in the week following the Google paper
- **XRP** added a quantum roadmap to its investment case
- **IBM** launched dedicated AI and Quantum Hubs in Illinois and Massachusetts
- **Quantum Blockchain** lawyers were scheduled to meet a U.S. patent official in April, suggesting commercial patent activity in quantum-resistant cryptography

PREDICTION MARKETS

April was the month prediction markets graduated from curiosity to regulatory battleground. States sued the platforms; the CFTC spent the month suing states; A U.S. Army soldier pleaded not guilty to betting on his own covert mission.

THE CFTC'S JURISDICTIONAL CAMPAIGN

CFTC Chair Mike Selig's objective in April was unambiguous: establish the CFTC as the exclusive federal regulator of prediction markets and preempt state enforcement:

- **New Jersey:** An appeals court blocked the state from shutting down Kalshi's sports prediction markets.
- **Arizona**: A federal judge granted the CFTC's request to block Arizona's prosecution of prediction market operators.
- **New York**: The CFTC took the state to court on April 27.
- **Wisconsin**: The CFTC sued on April 29.

The CFTC's legal argument rests on its claim to exclusive authority over event contracts under the Commodity Exchange Act. As of April 30, the CFTC had an open consultation on the regulatory treatment of prediction markets. During that consultation period, a group of senators wrote to Selig urging the agency to consider banning specific event types such as sports contracts, electoral contracts, and military action contracts. The senators argued these categories carry systemic integrity risks that no hedging rationale can justify.

Selig faces bipartisan pushback. Both parties have raised concerns about offshore war-betting markets and Hyperliquid perpetuals being treated as event contracts. Selig also stated that AI has helped his agency compensate for significant staffing reductions, raising questions about whether a technology-assisted, understaffed regulator can credibly supervise a rapidly scaling market.

THE INTEGRITY PROBLEM

Between illicit activities and base-line utility, prediction markets are going through a similar cycle to the early crypto regulation days.

A U.S. Army green beret was arrested for placing $400,000 in Polymarket bets on a Venezuela special operations raid he participated in. Kalshi separately flagged additional insider trading cases, including a politician who had appeared on the reality television program FBoy Island.

The U.S. Senate voted to ban its members and staff from trading on prediction markets entirely. Both Kalshi and Polymarket publicly welcomed the self-ban. Polymarket has also engaged Chainalysis to track illicit activity on its platform, a move designed to demonstrate that they are building the monitoring infrastructure regulators expect.

Even if insider trading were to be handled, other integrity issues remain, such as whether or not prediction markets are pure gambling (completely unlike other parts of the financial system, of course). Some suggested that prediction markets have a utility because they are highly accurate, but a study published in April found that only 3% of traders drive prediction markets' accuracy, not the crowd.

THE COMPETITION HEATS UP

Hyperliquid announced a direct challenge to Kalshi and Polymarket. Arthur Hayes argued that its HYPE token could serve as a prediction market weapon, citing deep liquidity and existing derivatives infrastructure.

Polymarket and **Kalshi** both announced plans to launch perpetual futures trading, a convergence toward a hybrid prediction-perpetuals products. **Polymarket** filed with the CFTC on April 29 seeking approval to reopen its main exchange to U.S. traders.

Jamie Dimon signaled **JPMorgan's** limited interest in the space as competition surges. "It's possible one day we'll do something like that," Dimon said on CBS, though ruled out offering markets in sports or politics.

Online casino operator **High Roller Technologies** announced it had entered an agreement with a **Crypto.com Derivates North America** to offer a CFTC-regulated prediction market platform

**Gemini received a Derivatives Clearing Organization (DCO) license from the CFTC, giving the exchange in-house clearing for futures, options, swaps, and prediction market contracts. But that happened on 1 May, so we won't be mentioning it here.*

DIGITAL PAYMENTS INFRASTRUCTURE

STABLECOINS AND TOKENIZED DEPOSITS

April has been another active month for digital payments infrastructure. The launches spanned consumer payments, institutional settlement, B2B cross-border rails, and DeFi yield infrastructure across every major jurisdiction.

Juniper Research projected that cross-border B2B stablecoin payments will reach $5 trillion by 2035, with 85% of volume coming from business use cases. Meanwhile, non-USD stablecoin senders on Solana has nearly tripled year-over-year, led by the euro-denominated EURC and Brazil's BRZ.

As the regulatory scene improves, stablecoins are appearing as a key product not only for crypto-native firms, but also for the wider fintech and banking ecosystem, including neobanks, remittance companies, payment processing networks, and financial institutions.

STABLECOIN HEADLINES

Banking Circle unveiled a stablecoin clearing service after receiving its MiCA license

12 European banks, known as the **Qivalis consortium**, announced plans to create a euro stablecoin via **Fireblocks**.

Coinbase transferred its x402 protocol to the Linux Foundation with backing from Google, Stripe, and Visa. Designed specifically for machine-to-machine and AI agent payments.

Stable Sea tapped **WisdomTree's** tokenized money market fund to build a yield floor into business operating cash held in stablecoins.

RealOpen and **TRON** verified $9.4 million in USDT for crypto-enabled real estate purchases.

ClearBank won MiCA approval to launch USDC and EURC across Europe.

Tempo unveiled private enterprise stablecoin transaction zones and partnered with DoorDash for stablecoin payments on its global marketplace.

Visa scaled its stablecoin settlement infrastructure to nine blockchain networks. Partners cited real-world demand. Visa also expanded its Agentic Ready programme globally, connecting AI agent payments to nine-chain stablecoin settlement in a single infrastructure layer.

Meta launched USDC stablecoin payouts for creators in Colombia and the Philippines via Stripe (April 30). Colombia and the Philippines were selected for their dollar demand, diaspora remittance flows, and high smartphone penetration relative to banking infrastructure.

Circle launched a stablecoin settlement solution for traditional financial institutions, its most direct institutional B2B product.

KBank tapped **Ripple** for high-speed global transfers, testing blockchain-based remittances to the UAE and Thailand using Ripple's Palisade wallet. The corridors currently use stablecoin settlement.

Morgan Stanley positioned itself as the reserve manager for the stablecoin industry, managing treasury assets that back dollar stablecoins at institutional scale without issuing one itself.

Fireblocks launched Earn, a stablecoin yield product that enables its thousands of institutional clients deposit their stablecoin to DeFi's top lending protocols

SocGen launched its stablecoin on MetaMask, giving self-custody wallet users access to a bank-issued euro-denominated digital asset.

Israel approved its first shekel-pegged stablecoin framework after a two-year pilot.

TETHER HAD A BUSY MONTH

In the course of April, the largest stablecoin issuer by market cap has:

- Launched a multichain self-custodial wallet, its first direct-to-consumer custody product
- Expanded USAT stablecoin from Ethereum mainnet to **Celo**
- Co-launched a gold-backed **Visa** card with **Fasset**
- Added $70 million in bitcoin to reserves, bringing total above 97,000 BTC
- Committed $127.5 million to the **Drift Protocol** recovery plan (see DeFi Security section)
- Frozen $344 million in USDT on **Tron** in coordination with U.S. law enforcement, its largest single freeze ever. **Chainalysis** subsequently mapped the Iran stablecoin sanctions evasion pipeline that was disrupted.
- Backed **KAIO**, a UAE tokenization firm, to bring Emirati sovereign fund assets on-chain
- Proposed a three-way merger as majority holder in **Twenty One Capital** with bitcoin financial services platform **Strike**, and bitcoin miner **Elektron Energy**
- USDT went live on **Solana**, **Plasma**, and **Ethereum** with 1:1 USD onramps and offramps.

Until recently, **Tether** has been the quiet one, operating without the public communications infrastructure of **Circle**. Lately, they have been showing a different posture, with active engagement with law enforcement, active defense of DeFi infrastructure, active political engagement, and active M&A. **Tether** is positioning itself for a world of regulated stablecoins leveraged not only by retail crypto investors, but institutions, fintech, and the wider payments infrastructure.

STABLECOIN POLICY AND REGULATION

Crypto world hoped April would be the month that saw the CLARITY Act pass through the Senate. Sadly, their wish did not come true, though a draft was released early May.

The tension surrounded language relating to stablecoins yield. The banks argued that any stablecoin rewards program paying holders based on their balance was functionally equivalent to a deposit account paying interest, threatening deposit flight from the traditional banking system. Crypto-native stablecoin issuers argue yield is the product's core utility.

More than 100 crypto organizations urged action. President Trump issued a public warning to the banking sector against obstruction of the bill.

The Senate Banking Committee is targeting a markup the week of May 11.

At a global level, the BIS stated that international stablecoin regulatory standards are paramount and that fragmented national rulemaking creates systemic risk.

South Korea proposed bank-style stablecoin rules while testing deposit tokens as a mechanism for government spending; Hong Kong flagged fake HSBC tokens circulating ahead of a real stablecoin launch; and Israel approved a shekel-pegged stablecoin.

The ECB moved to facilitate digital euro payment implementation, publishing guidance designed to facilitate the integration of digital euro payments into existing payment infrastructure. The move comes alongside two ECB research papers mapping how tokenization and euro stablecoins interact with sovereign bond markets, signaling that the ECB is treating the digital euro not as a standalone CBDC project but as part of a broader tokenized capital markets architecture.

INSTITUTIONAL ADOPTION

Paris Blockchain Week opened mid-April with institutions dominating the agenda. Speakers discussed the trade off between composability and privacy, with banks wanting all the opportunities of composability that a public blockchains provide, but not the accompanying privacy risks.

Meanwhile, ETFs domnated headlines, with bitcoin ETFs recorded $471 million in a single day on April 7 and $2 billion across eight consecutive days later in the month.

INSTITUTIONAL CRYPTO ADOPTION

- **Morgan Stanley** launched its spot bitcoin ETF on April 8, drawing $34 million on day one. Its ETF is not available via an app; it is recommended by wealth advisers to private clients. The institutional reach this represents is structurally different from exchange-listed ETF inflows.
- **Goldman Sachs** filed for a bitcoin income ETF, a covered-call structure designed to generate yield on bitcoin exposure, targeting income-seeking allocators.
- **Bitwise** launched an Avalanche ETF with in-house staking.
- **Charles Schwab** announced the rollout of spot bitcoin and ether trading for its retail brokerage clients.
- **Interactive Brokers** launched crypto trading for individual investors in Europe.
- **Franklin Templeton** launched a dedicated crypto division via its acquisition of 250 Digital.

TOKENIZATION ACROSS FINANCIAL INSTITUTIONS

- **Securitize** is partnered with **Computershare**, the world's largest transfer agent, to tokenize U.S.-listed equities. Computershare services thousands of listed companies. At scale, this places the entire U.S. public equity market within reach of onchain settlement.
- **JPMorgan** hired a former Goldman Sachs executive to lead distribution and settlement for its Kinexys tokenization division. He commented that tokenization is 'only half the battle.'
- **HSBC** completed a tokenized deposit pilot on the Canton Network, moving a live banking liability onto a blockchain for settlement.
- **Mizuho**, **Nomura**, and **Japan's central clearing house** joined Canton to tokenize government bonds in a production context.
- **AWS** integrated three **Chainlink** services in an April rollout targeting the tokenized finance stack.
- **Tassat** upgraded its Lynq institutional settlement network to Avalanche for scale.
- **Ripple** partnered with Korea's **Kyobo Life** to tokenize government bond settlement.
- **Coinbase** and **Bybit** were reported to be working together on tokenization, custody, and distribution for U.S. stocks.
- **Stable Sea** launched a product connecting **WisdomTree's** tokenized treasury fund to business operating cash.
- **WalletConnect** integrated with the Canton Network, connecting self-custody infrastructure to an institutional settlement chain.
- **Plume** launched a payroll pilot turning paychecks into yield-bearing real-world assets.
- **Morgan Stanley**'s CFO called tokenization the next major step for its multi-trillion wealth business.
- **Moonfare** launched an AI-focused technology strategy with tokenization as the distribution mechanism for alternatives.
- **Standard Chartered** acquired Zodia, its crypto custody spinout, bringing custody within a fully regulated bank entity.

TOKENIZATION POLICY AND REGULATION

Two public institution publications framed the month's activity:

The FCA published guidance on fund tokenization, offering asset managers a practical framework for using distributed ledger technology within existing rules, including an optional Direct to Fund model.

The ECB published a bulletin concluding that tokenization is central to the future of European capital markets, a statement that carries policy weight across every euro-area institution planning its digital asset strategy.

FINTECH TV

THE SIGNAL

NYSE
10005, New York

Get in touch: **news@fintech.tv**

Subscribe to The Signal

Disclaimers

This report is for informational purposes only and is not financial, business or legal advice. The thoughts and opinions do not represent the opinions of any other person, business, entity, or sponsor. Any companies or projects mentioned are for illustrative purposes unless specified.

The contents of this report should not be used in any public or private domain without the express permission of the author. The contents of this report should not be used for any commercial activity, such as research reports, consultancy activity, or paywalled article without the express permission of the author.

It is crucial to provide our readers with clear information regarding the inherent nature of services and products that might be covered in this report, including those advertised by our sponsors from time to time. When you buy cryptoassets (including NFTs) your capital is at risk. Risks associated with cryptoassets include price volatility, loss of capital, complexity, lack of regulation and lack of protection. Many service providers operating in the cryptoasset industry do not currently operate in a regulated industry. Therefore, please be aware that when you buy cryptoassets, you may not be protected under financial compensation schemes and protections typically afforded to investors when dealing with regulated and authorised entities to operate as financial services firm.