Article Information

Authors: Steven Pettigrove, Katrina Sharman, Luke Higgins, Will Deeb, Sophie Nguyen, Tahlia Kelly
Service: Banking & Finance, Banking & Finance Litigation, Blockchain
Sector: Financial Services, FinTech

Blockchain Bites: Unpacking contract law in DeFi; Trump takes on banks over the CLARITY Act; SEC delivers regulatory clarity on tokens; Deep freeze as FATF urges new stablecoin AML controls

The Piper Alderman Blockchain Group bring you the latest legal, regulatory and project updates in Blockchain and Digital Law.

The Agony of AAVE – How to lose US $50M with one click...

AAVE is a large player in the crypto DeFi space, enabling lending, borrowing and swapping of crypto tokens, usually on Ethereum. It has become well known for a liquidity pool model and enabling flash loans (which enable a borrower to borrow and repay crypto within the same transaction).

Users can access the Aave protocol either through direct smart contract interactions or through open source front ends, the most popular of which is operated by Aave Labs.

This week, an as-yet unidentified user entered a trade on AAVE's front end using their mobile phone. The user sought to swap US$50M of USDT for AAVE tokens. This is a pretty large trade and definitely a very large trade to be done from a mobile phone.

One important technical detail is that the trade did not involve the standard USDT and AAVE tokens directly, but rather Aave's interest-bearing tokens: **aEthUSDT and aEthAAVE**. These "aTokens" represent deposits into the Aave lending protocol and accrue yield over time. While they are designed to remain redeemable for their underlying assets, secondary markets for swapping aTokens directly against each other are often significantly thinner than markets for the underlying tokens themselves.

This means that large swaps between these assets can produce extreme price impact if routed through on-chain liquidity pools rather than being unwound through the underlying tokens first. In particular, the liquidity available for direct swaps between aEthUSDT and aEthAAVE appears to have been relatively limited, meaning a transaction of this size would be highly sensitive to the routing path chosen during execution.

In this case, the user was provided a warning that the trade could lead to unexpected pricing on the tokens but clicked through to confirm the swap anyway. They received $36K worth of AAVE Tokens in return for their US$50M...

Stani, Founder and CEO of AAVE labs, said in an X post:

the Aave interface, like most trading interfaces, warned the user ... and required confirmation via a checkbox. The user confirmed the warning on their mobile device and proceeded with the swap, accepting the high slippage, which ultimately resulted in receiving only 324 AAVE in return [worth $36,297].

The transaction could not be moved forward without the user explicitly accepting the risk through the confirmation checkbox.

Events like this do occur in DeFi, but the scale of this transaction was significantly larger than what is typically seen in the space.

Stani noted that AAVE Labs would return the $600,000 in fees AAVE received from the trade if they can identify the person involved. CoW DAO, the DAO which operates CoW Protocol, which is a decentralised aggregator that routes transactions to find liquidity for trades, said:

No DEX, DEX aggregator, public liquidity pool, or private liquidity pool (or combination thereof) would have been able to fill this trade at anywhere near a reasonable price.

and confirmed that:

The transaction executed according to the parameters of the signed order.

They took the position that CoW Protocol would not build guardrails or limits on user trades as:

Preventing users from making trades removes choice and can lead to terrible outcomes in some situations (e.g. a market crash).

CoW DAO accepted that *"DeFi UX still isn't where it needs to be"* and confirmed that they would refund any fees from the transaction which were received by CoW DAO.

Some users on X are suspicious of the whole transaction, with @Zacodil asserting that it was likely money laundering. Many were questioning how this could possibly happen in a front end given the wildly unreasonable price, which can be seen as having been inserted into the rate of the swap that the user confirmed.

So where did the $50M go? The way AAVE works, every swap is sent through CoW Protocol. CoW Protocol has a network of 'solvers' who are responsible for finding the best execution path for a trade, with the transaction settling in one transaction, instead of a series of transactions. Unlike traditional DEX swaps where the execution path is fixed at the time the users signs the transaction, CoW Protocol operates on an 'intent-based' model. The user signs an order expressing an intent to sell one asset for another, with a minimum acceptable output, and third-party 'solvers' compete to produce a settlement that satisfies those constraints. This can protect users from Maximum Extractable Value (MEV) attacks, where someone sees an order and pays higher fees to front run that order.

But what exactly happened here:-

1. The wallet routed 50.43M USDT, which had been received from Binance 20 days earlier, into AAVE Cow Protocol / CowSwap.
2. The 'solver' swapped USDT for 17,958 WETH, losing $13.6M due to slippage).
3. The WETH was then routed into a small SushiSwap AAVE/WETH pool, which delivered only 331 AAVE (worth $36K) in return to the user.

The settlement appears to have involved flash-loan liquidity and MEV-style execution strategies. Flash loans allow large amounts of capital to be borrowed and repaid within a single transaction, enabling complex arbitrage and routing strategies that would otherwise require significant capital.

In this case, priority fees appear to have been paid to block builders or validators to ensure the transaction was included in a block, capturing a large portion of the value created by the execution. This route was facilitated by an automated MEV bot which borrowed $29M of WETH with a flash loan from Morpho Protocol and paid priority fees (known as tipping) to miners to the tune of $20M to have the transaction included in a block, leaving the bot with a $9M profit and miners with $20M of tips.

An interesting analysis has been posed by @Ehsan1579 which suggests something more serious may have occurred:

Aave's CoW adapter quote path did not include the flash-loan and hook metadata that actually defines execution. The UI emphasized an optimistic receive amount.

This analysis suggests that the quote presented to the user and the transaction that ultimately executed may have been produced in different execution contexts. The front-end interface generated a quote based on observable liquidity routes, but the final settlement produced by a solver could incorporate additional mechanisms such as flash-loans and custom routing logic. These additional execution components were not necessarily reflected in the original quote displayed to the user.

The author here suggests that the solver deliberately chose a small liquidity pool which could not handle the order size, while ignoring a deep liquidity pool which could have provided the correct amount of AAVE to the user. The suggestion is that AAVE's use of CoW Protocol enabled one of the 'solvers' to deliberately choose a routing which they could take advantage of, and the user was not aware of this in the UX:

The user is looking at a quote produced in one context. The system later posts an order in a different context entirely.

Under the CoW Protocol model, solvers are not obligated to find the best possible execution path, but rather a valid execution path that satisfies the minimum constraints defined in the signed order. The analysis was that once the user had selected a minimum floor number of AAVE (here 324 AAVE) then any solver in CoW Protocol could 'solve' the transaction to complete the order (which does not have to be the best solution or best price). Once that minimum output threshold was set, a solver could validly settle the order using any routing strategy capable of delivering at least that amount. In practice, this meant the order could be routed through extremely thin liquidity while still satisfying the signed order parameters.

This transaction raises a raft of possible legal issues, including in relation to contractual assent and the law of mistake, which we will explore in a bit more detail in a subsequent post.

Written by Steven Pettigrove and Will Deeb

Interest-ing times: Trump goes toe-to-toe with banks over CLARITY Act

Whether firms should be permitted to issue stablecoins that provide interest-like returns has emerged as a key point of contention in Congress's consideration of the Digital Asset Market Clarity Act of 2025 (**CLARITY Act**), the U.S. crypto market structure bill.

In late February, U.S. stablecoin policy has moved back into focus following a series of White House-brokered meetings between banks and crypto industry participants, alongside a further instance of direct public intervention by President Trump.

The central issue is whether, and in what form, stablecoin interest or yield should be permitted under U.S. law. Notably, the stablecoin provisions in section 404 of the draft are largely unrelated to market structure. Instead, the proposed revisions aim to close a gap left by last year's Guiding and Establishing National Innovation for U.S. Stablecoins Act (**GENIUS) Act**). The issue has emerged as a key obstacle to passage of the CLARITY Act.

Although the debate is often presented in political terms, the underlying issues are fairly simple. The question is whether stablecoins that offer interest or rewards start to look like bank deposits, which should be regulated like banking, and how far lawmakers want to limit non-banks from competing with traditional banks by offering returns to customers.

How are stablecoins treated under the current law?

In July 2025, Congress enacted the GENIUS Act, establishing a federal framework for "payment stablecoins," digital assets pegged to a fixed monetary value and fully backed by high-quality liquid assets such as U.S. currency or Treasury bills. Issuance is limited to licensed entities, which are subject to reserve, disclosure, and risk-management requirements. Critically, the Act explicitly prohibits approved issuers from paying interest, yield, dividends or other returns to holders solely for holding a payment stablecoin.

The GENIUS Act did not, however, clearly address whether third parties, such as crypto exchanges or wallet providers, could offer rewards or incentives linked to stablecoin use. That gap has fuelled the current debate. Crypto firms argue that incentives are a legitimate tool for customer engagement, while banking groups contend that third-party yield-bearing stablecoin arrangements closely resemble interest-bearing deposits and risk eroding the bank deposit base. That balance has shifted following a proposed implementing rule from the Office of the Comptroller of the Currency, which suggests that these third party reward structures may be inconsistent with the statute's intent.

Will stablecoin rewards be permitted under the CLARITY Act?

At a White House meeting on 19 February 2026, administration officials signalled support for a compromise that would allow limited stablecoin rewards under the CLARITY Act, provided they are tied to transactional use or support for crypto infrastructure, rather than passive holding. The White House reportedly urged banks to accept this compromise to allow the legislation to advance.

Banks have so far resisted. In subsequent discussions with crypto firms and White House officials, banking lobbyists have argued that the administration does not control the Senate process and have maintained that most forms of rewards should be prohibited. That position has gained traction among lawmakers from both parties, stalling progress on the CLARITY Act and raising the prospect that resolution could slip into 2027.

On 3 March 2026, President Trump publicly called on Congress to pass the CLARITY Act "ASAP," accusing banks of seeking to undercut the GENIUS Act by blocking market-structure reform over the stablecoin rewards issue.

Crypto negotiators have grown increasingly frustrated with what they see as the banking sector's inflexible stance, even as

digital asset firms signal a willingness to forgo rewards on stablecoins that are merely held rather than used. Industry leaders such as Coinbase CEO Brian Armstrong and Ripple CEO Brad Garlinghouse have nevertheless expressed confidence that an eventual deal remains achievable.

In the weeks ahead, attention will focus on whether targeted adjustments to stablecoin reward models are sufficient to unlock passage of the CLARITY Act, or whether the GENIUS Act will continue to define the market's practical limits. The direction of this debate may also foreshadow discussions in Australia as stablecoins are brought within a new payments-licensing regime.

In Australia, regulatory uncertainty and pending litigation have largely curbed the offer of yield by exchanges in any form. Upcoming regulatory reforms promise an opportunity to offer limited staking services under the AFSL framework, but it remains to be seen whether new types of yield offerings will emerge as banks and exchanges compete more closely in the years ahead.

Written by Steven Pettigrove, Katrina Sharman and Tahlia Kelly

The Last Chapter in the Book of Howey? SEC and CFTC Draw the Lines on Crypto

For a decade or more, web3 founders structuring projects out of the Cayman Islands which had any US token holders have had to live with a particularly uncomfortable question: is my token a security under US based laws? For projects with a substantial US token holder base or development team, the answer could mean the difference between regulatory clarity and an enforcement action or Wells notice. That question has now received its clearest answer yet.

On March 17, 2026, the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) issued a joint 68-page interpretive release clarifying how both regulators consider that federal securities laws apply to certain crypto assets and transactions.

This followed hot on the heels of a Memorandum of Understanding (MoU) announced on March 11, 2026, under which the two agencies committed to coordinate on oversight, reduce duplication, and align their regulatory frameworks. This represents one of the most important changes to digital asset treatments globally, as much of the world follows the US regulatory lead. Presently the Gensler era decisions have influenced IOSCO and other international digital asset treatment, and this change will take some time to filter though to the international bodies.

1. The Token Taxonomy

The release introduces a five-category taxonomy for digital assets:-

- **Digital commodities**— assets intrinsically linked to a functional network, whose value derives from the programmatic operation of a system and ordinary supply and demand, not from the managerial efforts of others. Bitcoin, Ether, Solana, Cardano, Avalanche, XRP, Dogecoin, Litecoin, Chainlink, Polkadot, Hedera, Bitcoin Cash, Shiba Inu, Stellar, Tezos and Aptos are among those expressly named. These fall primarily under CFTC oversight as commodities.
- **Digital collectibles**— not securities.
- **Digital tools**— not securities.
- **Stablecoins**— not securities, provided they are structured consistently with the GENIUS Act definition.
- **Digital securities (or tokenised securities)**— are considered securities.

The guidance also provides welcome clarity on a number of specific activities: protocol mining, protocol staking, and wrapping a non-security crypto asset do not involve the offer or sale of a security.

Importantly, airdrops do not constitute an "investment of money" under the Howey test.

The release addresses the lifecycle of investment contracts in the web3 space. A non-security crypto asset can *become* subject to an investment contract (where it is accompanied by representations or promises about managerial efforts that satisfy the *Howey* test), but it can equally *cease* to be subject to one — a critical acknowledgment for mature, decentralised networks. This was a key point of debate under the Gensler SEC, where the position taken by the regulator was, in effect, that something sold as a security under US law was always a security. The web3 industry's position in a number of cases has been vindicated in this new SEC/CFTC position.

What the Agencies Said

SEC Chairman Paul S. Atkins, announcing the interpretive release, was direct about the significance of the change:

After more than a decade of uncertainty, this interpretation will provide market participants with a clear understanding of

how the Commission treats crypto assets under federal securities laws. This is what regulatory agencies are supposed to do: draw clear lines in clear terms.

Chairman Atkins also took the opportunity to acknowledge what had been a long-standing point of contention:

It also acknowledges what the former administration refused to recognize – that most crypto assets are not themselves securities.

CFTC Chairman Michael S. Selig, who prior to his confirmation as CFTC Chairman played a leading role as Chief Counsel of the SEC's Crypto Task Force, matched the tone:

For far too long, American builders, innovators, and entrepreneurs have awaited clear guidance on the status of crypto assets under the federal securities and commodity laws. With today's interpretation, the wait is over.

The MoU itself drew similarly emphatic language from Chairman Atkins, who noted that:

For decades, regulatory turf wars, duplicative agency registrations, and different sets of regulations between the SEC and CFTC have stifled innovation and pushed market participants to other jurisdictions.

The Director of the SEC's Division of Corporation Finance titled his speech on the day "The Last Chapter in the Book of Howey" — capturing the sentiment that after 80 years of the *Howey* investment contract test dominating the analysis, the agencies now have a workable, modern framework.

Is This Really the Last Chapter?

The interpretive release carries significant practical weight. Writing in Forbes, former banking regulator Jason Brett noted that Ryne Miller, partner at Morrison & Foerster, put it plainly:

A Commissioner-level interpretation is a big deal. Even in a post-Loper Bright world without Chevron-style deference, its practical and persuasive power will shape industry behavior, judicial analysis, and enforcement policy for the foreseeable future — shifting us from regulation-by-enforcement to a rules-based framework.

Notably, this interpretive release is expressly not the "innovation exemption" that Chairman Atkins has separately flagged as forthcoming — meaning further clarity is still on the way for certain limited trading activities.

The latest guidance will have important implications for US-based projects. However, given the global nature of crypto-asset projects, it will also have implications for overseas projects which have a US-jurisdictional nexus. However, the guidance does not displace local law requirements. Start-ups operating in other jurisdictions will need to continue to carefully monitor local regulatory frameworks and ensure that they manage legal compliance at the local and global level.

We will very likely see several more chapters before the book of Howey is truly closed, but at least one unsatisfying cliffhanger has moved substantially closer to a satisfying ending.

Written by Steven Pettigrove and Luke Higgins

Deep freeze: FATF urges new stablecoin AML controls

The Financial Action Task Force (**FATF**) recently released its Targeted Report on Stablecoins and Unhosted Wallets, positioning stablecoin "freezing" in the secondary market as an emerging AML/CTF control. At the same time, Circle's recent freeze of USDC across 16 operational wallets demonstrates how these controls operate in practice, and why unlimited freeze powers pose market and security risks as financial markets move on-chain and particularly for decentralised finance (**DeFi**).

The FATF Report points to a growing regulatory and technical reality: compliance expectations are expanding beyond intermediaries to stablecoin issuers themselves. This shift could entrench censorship capability, centralised governance and single points of failure, introducing counterparty and security risks under the guise of well intentioned efforts to tackle financial crime.

Freezing moves from theory to practice

FATF's March 2026 report highlights the rapid growth of stablecoins, with more than 250 in circulation and aggregate market capitalisation exceeding USD 300 billion by mid-2025, now accounting for approximately 84% of illicit virtual-asset transaction volume according to FATF data.

FATF's Report observes that illicit stablecoin activity is increasingly occurring in the secondary market, particularly via peer-to-peer transfers using unhosted wallets, where transactions often take place without customer due diligence, transaction monitoring, or a clearly responsible reporting entity.

To address this "secondary-market gap," FATF explicitly points to issuer-level programmable controls, including freezing, deny-listing and similar smart-contract controls, as "good practices" capable of disrupting illicit flows where intermediaries are absent. The report encourages jurisdictions that are developing regulatory frameworks for stablecoins to consider the freezing of stablecoins as part of their AML/CFT toolkit.

What freezing achieves – and what it breaks

From a technical perspective, freezing renders stablecoins economically immobilised but still on-chain, preserving visibility while preventing transfer, redemption or use. FATF notes that freezing may be applied even where wallet holders are unidentified, making it a blunt but effective intervention tool where attribution is incomplete.

However, issuer-level freezing reintroduces asset-level censorship, concentrates governance and legal risk in a single controlling entity, and creates single points of failure, allowing broad or mistaken freeze decisions to disrupt liquidity, protocols and users far removed from any wrongdoing.

Case study: USDC's 16-wallet freeze

Circle's reported late-March 2026 freeze of USDC across 16 "hot wallets," apparently linked to a sealed US civil case, illustrates these risks. The frozen wallets appeared to be ordinary operational business wallets, including infrastructure-linked addresses, not sanctioned or criminal actors. According to reports, at least one wallet was later unfrozen following public scrutiny.

While well-intentioned, issuer-level freezing can spill into protocol infrastructure, disrupt live operations and strand downstream users with no legal or practical recourse – even in civil disputes unrelated to illicit conduct. This could introduce new systemtic risks where end users increasingly rely on on-chain market infrastructure or in the event of a hack or security breach.

GENIUS Act raises the stakes

In the United States, the GENIUS Act establishes a federal regime for payment stablecoins but leaves critical AML rules to be written by FinCEN and Treasury. Those rules could shape how freezing occurs in the on-chain economy. In that context, it is important to balance competing policy objectives by targeting financial crime while not introducing new risks to market integrity or the free flow of capital. These risks are unique to the on-chain economy, where it is possible to identify illicit activity several hops away from the transaction in question. To that end, blockchain software provides a powerful (and potentially all powerful) tool for targeting financial crime but which can also be abused or used as a censorship tool. Similar concerns have been raised in relation to the widespread adoption of central bank digital currencies.

Bottom line

If adopted more broadly, FATF's approach would require stablecoin issues to embed powerful centralised freezing controls. Without close consultation with industry, well-intentioned AML/CTF measures, particularly around freezing, risk inadvertently undermining innovation, market confidence and the resilience of decentralised financial systems at scale. These developments can have downstream effects on decentralised systems, shaping liquidity, settlement and user experience. As expectations around secondary-market freezing continue to evolve, policy makers will need to balance competing policy objectives to ensure secure and robust on-chain financial markets.

Written by Steven Pettigrove, Katrina Sharman and Sophie Nguyen