Blockchain Bites: ASIC updates strategic priorities, Mastercard offers self-custody debit card as Apple opens NFC transactions, ACCC targets Facebook scam ads, Europe surveys smart contracts, Binance clipped with class-action lawsuit

Michael Bacina, Steven Pettigrove, Jake Huang, Luke Higgins and Luke Misthos of the Piper Alderman Blockchain Group bring you the latest legal, regulatory and project updates in Blockchain and Digital Law.

ASIC updates strategic priorities for 2024-2028

The Australian Securities and Investment Commission (**ASIC**) has announced its 2024-2025 Corporate Plan outlining its strategic priorities for the next four years.

As Australia's integrated corporate, markets, financial services and consumer credit regulator, ASIC's vision is to foster a fair, strong and efficient financial systems for all Australians through regulatory activities.

Underpinning this vision is ASIC's 5 strategic priorities:

1. Improve consumer outcomes
2. Address financial system climate change risk
3. Better retirement outcomes and member services
4. Advance digital and data resilience and safety
5. Drive consistency and transparency across markets and products

Each of these pillars consists of several focus areas which ASIC is going to direct its resources towards.

OUR VISION

A fair, strong and efficient financial system for all Australians

STRATEGIC PRIORITIES

1	2	3	4	5
Improve consumer outcomes	Address financial system climate change risk	Better retirement outcomes and member services	Advance digital and data resilience and safety	Drive consistency and transparency across markets and products

FOCUS AREAS

The design and distribution of financial products	Climate-related disclosure	Improved services for superannuation fund members	Technology-enabled scams and misconduct, and the poor use of artificial intelligence (AI)	Outcomes in public and private markets
Predatory sales and lending	Greenwashing	Driving industry progress towards improving retirement outcomes	Business, cyber and operational resilience	Existing and emerging financial products and services, including new market participants
Financial hardship assistance	Integrity and fairness in energy and carbon credit markets			
Insurance claims handling	Insurer claims and complaints handling following severe weather events	Compliance by superannuation trustees, and providers of managed investments and financial advice		
Dispute resolution				

Compared to last year's ASIC Corporate Plan, there have been some notable changes. First, ASIC has kept all of last year's strategic priorities but rephrased them to cover a broader range of issues. For example, the first pillar "Product Design and Distribution" has become "Improve consumer outcomes", which covers a broader range of issues, such as predatory sales practices and dispute resolution.

Second, within the 4th pillar, rather than "supervise", ASIC now says it will:

> hold ASX (*note: the Australian Securities Exchange*) to account on the safe and efficient implementation of the CHESS replacement program

This change may well refer to ASIC's headline lawsuit against the ASX, accusing the exchange of misleading and deceptive conduct over an ill-fated attempt to replace the CHESS settlement system with a blockchain-based solution.

Third, ASIC has added a new 5th pillar (see above) covering public and private markets and emerging financial products. Key activities within this pillar now include monitoring digital assets, tokenisation and decentralised finance. ASIC has committed to create a central coordination function to monitor and engage entities on these emerging trends within an expected time frame of 2 years+. It will be interesting to see how this will align with Treasury's plan to establish a new

custody and licensing framework to regulate digital asset platforms, with draft legislation expected late this year.

In ASIC Chair Joe Longo's announcement of the Corporate Plan, he placed particular emphasis on the last pillar:

> The integrity of our markets is fundamental to maintaining trust in Australia's financial system which is core to ASIC's remit.

Mr Longo also trumpeted the number of enforcement actions that the regulator has commenced.

> In the last year alone we commenced around 170 new investigations – an increase of about 25%, and we filed 33 new civil proceedings in the Federal Court – an increase of 27% in civil proceedings on the previous year.

ASIC's recent enforcement actions involving crypto-asset related offerings against Finder, BPS Financial (i.e. Qoin) and Block Earner have garnered significant attention, each of which is now on appeal by ASIC. The case against BPS Financial could also have important implications for the scope of the corporate authorized representative regime.

The Corporate Plan provides important insights into the regulator's priorities in the next few years and how it will deploy its limited resources. The impact of last year's Corporate Plan was demonstrated by ASIC's active enforcement of design and distribution obligations, including publishing Report 770 for the OTC derivatives sector and issuing 10 interim stop orders in this sector.

While crypto and digital assets no longer receive an honourable mention as ASIC's "core strategic project", the Plan seems to reflect an increasing convergence of digital assets with regulated markets encompassing cryptocurrency, tokenisation and DeFi.

Written by Jake Huang and Steven Pettigrove

Mastercard offers self-custody debit card, as Apple opens NFC transactions

Mastercard has partnered with popular decentralized finance (**DeFi**) wallet, MetaMask, and digital payments company, Baanx, to launch a self-custody debit card pilot program for select users in the United Kingdom and the European Union, with plans to roll out the product in other regions over time.

The MetaMask Mastercard allows users of self-custody wallets to make card purchases everywhere Mastercard is accepted — while retaining personal custody of the funds until the moment of purchase, and with greater security provided by Mastercard's existing systems and controls.

MetaMask's self-custody wallet will support the Mastercard debit card. Self-custody wallets are also referred to as "non-custodial wallets". They're different from the crypto wallets offered by centralized exchanges in that the owner of a self-custody wallet maintains control over their digital assets, rather than entrusting them to an intermediary.

Lorenzo Santos, the senior product manager for Consensys, the blockchain company behind MetaMask self-custody wallets, says

> It's like having cash in your wallet instead of your bank account…You're responsible for safeguarding that cash, and you can access it anytime.

Historically, it has been hard for people to easily spend self-custodied digital assets on anything beyond the crypto world. For example, if someone wants to spend their digital assets, they would first need to move them to an exchange and convert them to fiat currency before transferring them to a traditional bank account. This has made self custodied crypto assets hard to spend for everyday purchases.

Some centralised crypto exchanges have addressed the problem by working with issuing banks, payment networks like Mastercard and other technology enablers to launch branded debit or prepaid cards, with the same safeguards required by local regulators. MetaMask's Mastercard for self-custody wallets breaks new ground by allowing crypto users to custody and spend directly.

Meanwhile, [Apple has announced that it will open up its NFC chips to third-party app developers](#), potentially paving the way for crypto developers to integrate blockchain-based contactless payments using Apple devices such as iPhones and iPads.

[Jeremy Allaire, the CEO of stablecoin firm Circle](#), said on X that his firm is planning to introduce tap-and-go USDC payments on iPhones:

> Jeremy Allaire – jda.eth / jdallaire.sol ✓
> @jerallaire
>
> Tap to pay using USDC on iPhones incoming soon. Wallet devs, start your engines.

Apple to Open Payment Chip to Third Parties and Charge Fees

He later added that,

> This would allow a [point of sale] to tell an iPhone what blockchain address it will accept USDC on, or the amount to pay, and then the iPhone-based wallet app could prompt the user to confirm a payment (like with FaceID) and initiate a transaction over the blockchain to settle the USDC,

Apple's move could open up a powerful pathway for direct to merchant USDC payments. Additionally, Allaire explained that Apple's opening up access to its NFC chip would apply to "lots of things" outside of USDC, including non-fungible tokens (NFTs) for tickets, other certificates, and other stablecoins.

Notably, Apple said the APIs would be made available to developers in Australia, Brazil, Canada, Japan, New Zealand, the United Kingdom, and the United States but made no mention of the European Union.

The latest announcements by Mastercard and Apple could pave the way for a wave of new payments product which utilise blockchain infrastructure and digital assets like stablecoins to make faster and cheaper payments by bypassing traditional payment rails, and significantly broadening the scope to use and spend digital currency in everyday transactions.

Written by Steven Pettigrove and Jake Huang

Meta in the middle as ACCC targets Facebook scam ads

Australia's consumer watchdog, the Australian Competition and Consumer Commission (ACCC), is pursuing Meta, the parent company of Facebook, over its handling of cryptocurrency-related advertisements on the platform. The ACCC alleges that a significant portion of these ads are either scams or violate Meta's advertising policies, raising critical questions about the role of social media platforms in safeguarding users from online fraud.

The ACCC's Allegations

According to a [ruling issued by the Federal Court earlier this month](#), the ACCC claims that more than half of the cryptocurrency ads analysed on Facebook were deceptive or violated the platform's rules. According to the regulator, Meta has been aware of this issue since at least January 2018 but failed to take adequate measures to prevent the proliferation of these fraudulent ads.

The Federal Court heard that an initial analysis by the ACCC revealed that 58% of the crypto ads and related landing pages reviewed were either in violation of Meta's policies or were potentially scams. These ads often featured prominent public figures, including celebrities and business leaders (such as Elon Musk), who were falsely portrayed as endorsing the scams. Other scammers have posed as "professors", attempting to deceive people into depositing funds with promises of
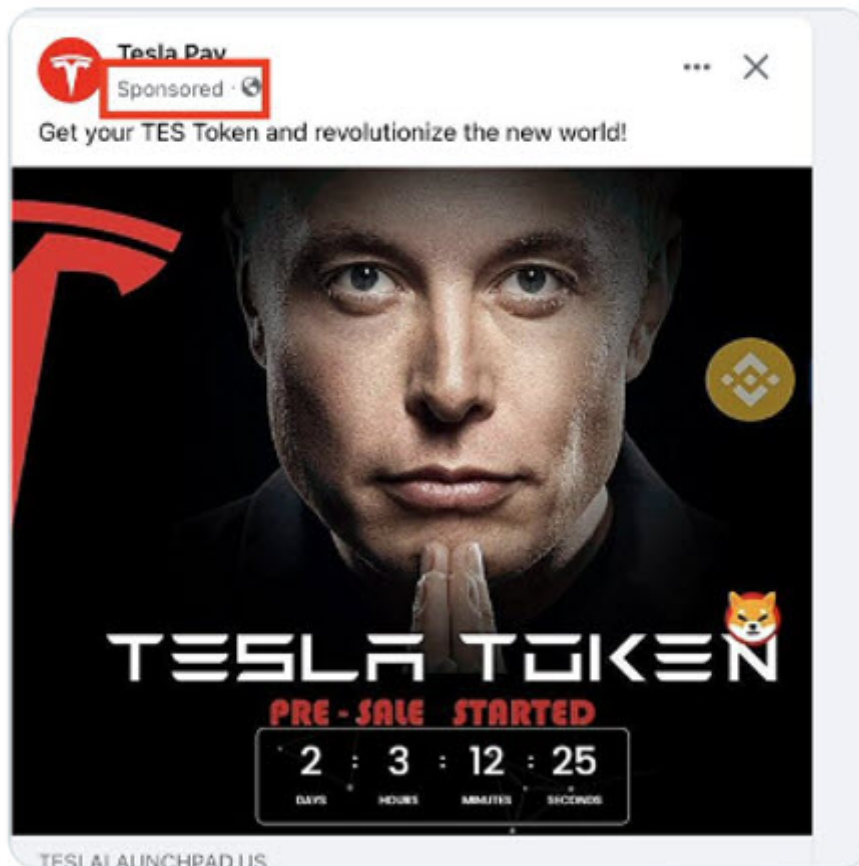
DogeDesigner ✔ 🐕
@cb_doge · Follow

Facebook is running paid crypto scam ads using Elon Musk's name.

Tesla and Elon Musk are not affiliated with any cryptocurrency token and will never launch one.

Tesla Pay
Sponsored · 🌐
Get your TES Token and revolutionize the new world!

TESLA TOKEN
PRE - SALE STARTED
2 : 3 : 12 : 25
DAYS HOURS MINUTES SECONDS

TESLALAUNCHPAD.US

10:29 AM · Jun 5, 2024

❤️ 1.1K   💬 Reply   ↑ Share

Read 229 replies

high returns.

🚨 **NEW CRYPTO SCAM ALERT: FAKE PROFESSORS HUSTLING INVESTORS**

Watch out for fraudsters posing as "professors," tricking people into depositing funds with promises of sky-high returns.

They use Facebook ads to lure victims into WhatsApp or Telegram groups, offering phoney loans... Show more

3:57 PM · Jul 17, 2024

♥ 52   💬 Reply   ⬆ Share

Read 6 replies

The ACCC advances allegations of misleading and deceptive conduct and false or misleading representations against Meta

under the Australian Consumer Law and the *Australian Securities and Investments Commission Act 2001* (Cth).

Despite Meta's actions to remove specific ads and ban accounts after receiving complaints, the ACCC alleges that the company has continued to allow similar ads to appear, earning revenue from these misleading promotions. The ACCC also claims that Meta could have developed technology to warn users about the risks of such ads but chose not to do so.

Meta's Defence

Meta's has noted the complexity of tackling online scams, as scammers continuously adapt their methods to avoid detection. [According to The Guardian](#), a spokesperson for Meta stated that the company is committed to preventing scams on its platforms and protecting users, despite the challenges involved.

Despite methods implemented by Meta, including a new requirement for advertisers introduced in June of this year to verify a phone number associated with their account, the ACCC remains sceptical of Meta's efforts. The regulator believes that while these actions address individual cases, they do not sufficiently tackle the broader issue of systemic fraud on the platform.

In the current Federal Court application, Meta sought to strike out certain parts of the ACCC's pleaded case. On this occasion, it was successful in obtaining orders requiring the ACCC to replead parts of its case against the firm.

Implications for Social Media Regulation

The ACCC's case against Meta has broader implications for the regulation of social media platforms. The ACCC's actions reflect a growing expectation that companies like Meta must be more proactive in preventing the spread of fraudulent content.

The financial impact of these scams is considerable. According to Scamwatch, investment scams promoted on social media have led to over $13 million in reported losses in 2024 alone. This figure is part of a larger trend of rising scam-related losses, with $134 million reported across various channels during the same period.

As the legal proceedings continue, the outcome could set a precedent for how social media platforms are held accountable for the content they host, not just in Australia but globally.

A hearing date has yet to be set, but the stakes are high. For users, the case underscores the importance of being vigilant when encountering online investment opportunities, particularly those that seem too good to be true.

The case also highlights the need for a robust licensing framework for cryptocurrency businesses to help consumers differentiate between licensed and unscrupulous fraudsters who seek to exploit blockchain technologies and cryptocurrency to induce consumers to part with their hard earned funds.

Written by Luke Higgins and Steven Pettigrove

Just how smart? Europe surveys smart contracts

Europe's financial markets regulator, the European Securities and Markets Authority (**ESMA**), has [published a working paper on the categorisation of smart contracts on the Ethereum blockchain](#), in which the authors acknowledge smart contracts' significant potential for financial innovation, while noting their risks to financial stability and investor protection.

In this paper, smart contracts are defined as

> Immutable computer programs that run deterministically on the blockchain and execute automatically, interacting with other accounts on the blockchain according to the code that defines their actions.

Since smart contracts were introduced on the Ethereum blockchain in 2015, they have garnered significant interest, as demonstrated by a surge of google searches:

Chart 1

Google searches for the terms 'decentralized finance' and 'smart contract'
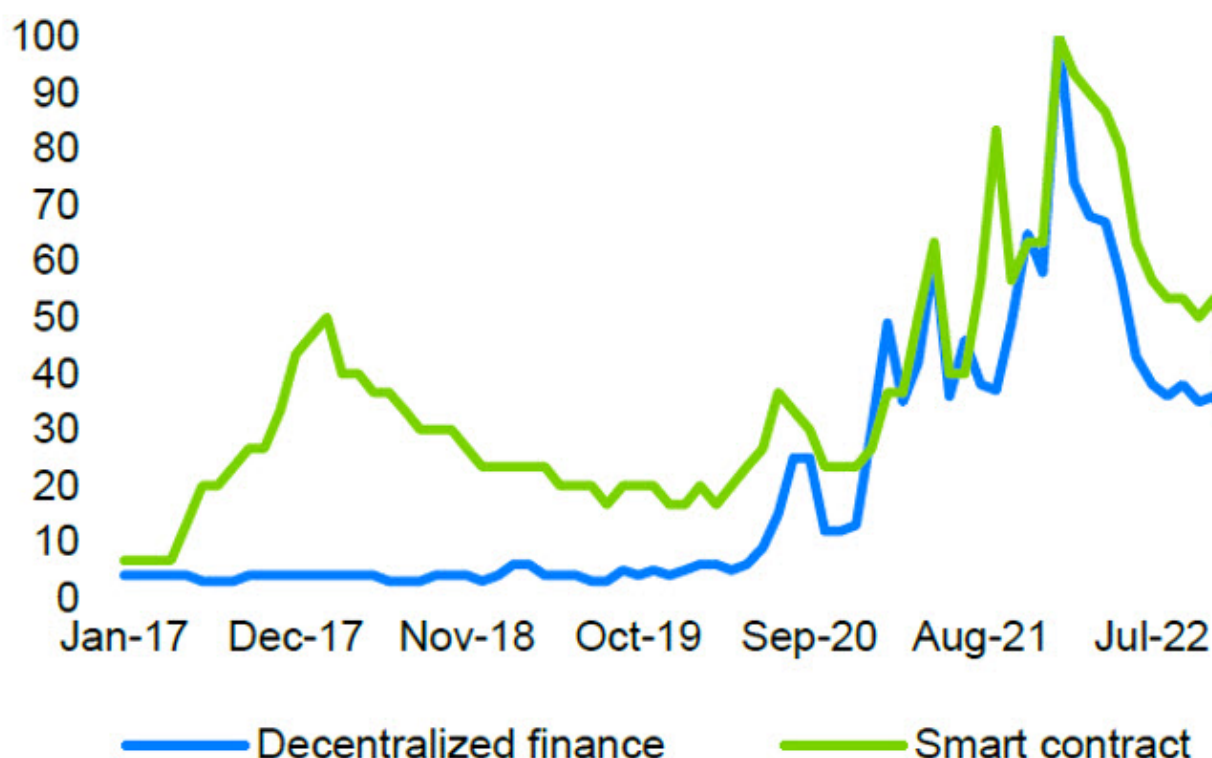
Note: Interest for 'smart contract' and 'decentralized finance' over time, measured by the number of Google searches. Note that a value of 100 represents the peak in popularity for the given term.
Sources: Google, ESMA

Many DeFi (decentralised finance) advocates argue that the 'trustless' nature of smart contracts is set to alter the financial landscape – by eliminating the need for intermediaries such as banks and brokers, smart contracts could potentially grant individuals complete autonomy over their finances, lessening their reliance on centralised agencies and making central institutions, including supervisors and standard setters, obsolete.

However, the paper points out that these features, coupled with the immutability of smart contracts, can have both positive and negative impacts – the latter include potential threats to investor protection and to financial stability. To better study the issues, the paper identified five categories of smart contracts: *Financial*, *Operational*, *Token*, *Wallet*, and *Infrastructure*.

- Financial: smart contracts belonging to this category serve primarily to gather and redistribute funds, thus enabling basic financial operations. They include:
    - simple borrowing and lending protocols to initial coin offerings (**ICOs**);
    - complex DAO (decentralized autonomous organizations) project;
    - airdrop smart contracts;
    - contracts that serve insurance purposes (since they are able to store funds and release them upon the fulfilment of predefined conditions);
    - contracts that enable ponzi schemes, lotteries, and other sort of 'gambling' activities on the blockchain concern the storing and redistribution of funds;
    - financial smart contracts are usually the infrastructure of automated market makers (AMMs) and pools for decentralised exchanges (DEXs).
- Operational: this category comprises smart contracts that, performing general purpose operations, facilitate the

functioning of other smart contracts or the interaction between other smart contracts. For instance, operational smart contracts are deployed onto the blockchain to host libraries. These smart contracts play crucial role in optimising resource allocation and utilisation, as well as in handling errors.

- Token: these smart contracts enable the generation of new tokens, their indexing, and their dismissal. The most common standards are ERC20 and ERC721:
  - ERC20 defines the standard interface for fungible tokens, which are identical and interchangeable units of value, commonly used for cryptocurrencies and utility tokens;
  - ERC721 specifies the standard for non-fungible tokens (NFTs), which represent unique and indivisible assets like collectibles, digital art, and in-game items.
- Wallet: smart contracts within this category concern the management of fees, sender accounts, balances, public access, requirements, and permission control. They serve primarily to simplify users' interaction with the blockchain, for instance by batching transactions and defining transfer limits.
- Infrastructure: smart contracts belonging to this category can be considered as the underlying infrastructure for other smart contracts. This category comprises contracts that deal with the manipulation and processing of string data, Boolean values, signatures, encoding and decoding operations, ABI (Application Binary Interface) functionality, viewing operations, memory usage, sending operations, and payload handling. Such operations are essential building blocks that contribute to the underlying infrastructure of smart contracts and dApps (decentralised applications).

Overall, the paper observes a shift from predominantly *financial* smart contracts to a broader range of applications, including *tokens*, *operational* and *infrastructure* categories.

While the European Union's *Markets in Crypto Assets Regulation* (**MiCA**) entering into force from June, the paper points out that it does not directly regulate "fully decentralised" crypto-asset services (true DeFI). The paper notes that the OECD has called for closer, consistent monitoring of the DeFi ecosystem, which has been echoed by legislators and the European Commission. The European Commission has acknowledged the limited enforcement power that can be exerted on DeFi, suggesting "a public observatory of DeFi activity operated by a public authority" that "would deploy public investigations and issue opinions and warnings publicly about specific DeFi protocols".

ESMA's paper represents a first step in a deeper research project to understand the risks and benefits of smart contracts in finance and more broadly. The paper's emphasis on the breadth of potential applications for smart contracts is well noted. Having regard to the potential impacts of MiCA on the regulation of smart contracts and dApps, the paper is a welcome contribution in progressing risk-based regulation of decentralised technologies which promise significant consumer and efficiency benefits for markets.

Written by Steven Pettigrove, Jake Huang and Matt Norton

Binance and CZ clipped with class-action lawsuit

Following the massive settlement deal and imprisonment of CZ over money laundering concerns, opportunistic class action lawyers are now seeking to sue Binance and CZ, with a rather novel suggestion that Binance's anti-money laundering failures led to the loss of assets of victims of fraud, specifically that proceeds of fraud were laundered through Binance but due to the exchanges failures the assets could not be traced further.

The lawsuit alleges that:

> Binance.com became a preferred-choice as the "get-away driver" for a large number of bad actors

and goes on to refer to Binance as the "Binance Crypto-Wash Enterprise" as well as seeking to activate the US RICO laws (Racketeer Influenced and Corrupt Organizations Act) which permit triple damages to successful plaintiffs.

The heart of the claim is that Binance is alleged to have "aided and abetted" criminals by failing to have an "adequate" or compliance AML/CTF program.

If not settled (and class actions like these often settle) there may be interesting defences available to Binance including whether a compliant AML/CTF program would have assisted at all in recovering funds. In most scams where a user willingly transfers crypto-assets to an exchange account or wallet which then moves funds to an exchange account, the exchange has little to no ability to identify the scam or fraud until the wallets used are flagged as illicit.

There also may be interesting challenges as to the usefulness of on-chain tracking of transactions, as a core argument of the claim is that, absent Binance being involved, on-chain tracking of the assets could have permitted recovery. This seems a fairly challenging argument to run and likely to be a point of defence for Binance. Prominent lawyer Bill Hughes commented that he thought it was "dubious" that the claim could be made out, but that the case would probably settle before reaching discovery.

Written by Michael Bacina