Article Information

Authors: Michael Bacina, Steven Pettigrove, Tim Masters, Jake Huang, Luke Higgins, Luke Misthos, Kelly Kim
Service: Blockchain, FinTech
Sector: Financial Services, IT & Telecommunications

Blockchain Bites: Treasury consult to modernise Australia's payment system, Sony and Microsoft point to NFT gaming, Europe leading the charge on AI governance, FSB says "crypto contagion" a limited threat to real economy, Capitol Hill dances between innovation and regulation in crypto clash, Buterin backs Zk-rollup centric roadmap

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

Treasury consult to modernise Australia's payment system

On 8 September 2023, Treasury released a second consultation paper (**Consultation Paper**) to update Australia's payments regulatory framework. This follows Treasury's first consultation in June, and a draft bill introduced in October to reform the *Payment System (Regulation) Act 1998* (Cth) (**PSRA**). The new Consultation Paper marks another significant stride by Australia to implement its ambitious Strategic Plan for a future ready payment system.

The Consultation Paper sets out a new framework for multiple regulators and industry bodies to oversees different payment services, depending on their potential impacts on the payment system.

Multi-layered regulatory framework

This "multi-layered" regulatory framework is visualised in the table below:

Table 1: Proposed regulatory framework

Prudential regulation Major stored-value facilities and designated PSPs	APRA	Manage financial and stability risks
Prudential regulation Common access requirements for payments clearing and settlement		Improve access to payment systems
Financial services regulation All PSPs performing a payment function	ASIC	Protect payment service users
Technical industry standards All payment system participants and payment system operators where a standard applies	Industry body authorised by RBA	Broad and consistent adoption of core standards

As shown by the table, the regulatory framework consists of four separate, but interconnected layers which apply to different aspects of the payment system. They are:

1. *Australia financial services licensing (**AFSL**) regime* – upheld by the Australian Securities and Investments Commission (**ASIC**), will apply to all payment service providers (**PSPs**). PSPs are entities that perform a payment function, such as issuing payment stablecoins, providing a stored-value facilities (e.g. a pre-paid card), providing a payment instrument (e.g. debit and credit cards) or facilitating payments (e.g. direct debit services).
2. *Prudential regulation* – administered by the Australian Prudential Regulation Authority (**APRA**), will apply to major stored-value facility (**SVF**). Major SVF are proposed to include SVF with more than $100 million in customer funds. Major SVF, and certain designated payment facilitation service will require an APRA licence to operate.
3. *Common access requirements* – another form of prudential regulation, will be set and overseen by APRA. This is intended to provide a new pathway for non-bank PSPs to directly access payment systems, something that they currently cannot do.
4. *Technical industry standards* – mandatory technical standards, which could include a revised ePayment Code that is currently non-mandatory, will be approved by the Reserve Bank of Australia and apply to a broad range of PSPs.

Payment functions and PSPs

Central to this regulatory framework is the scope of payment functions, which underpins the definition of PSPs. Absorbing feedback from the previous consultation, Treasury has proposed in this Consultation Paper a revised list of payment functions:

Table 3: List of payment functions

Payment function	Description	Illustrative examples
Stored-value Facilities ('traditional SVFs')	Funds loaded onto an account or facility. Customers are able to direct the movement of these funds, for the purposes of paying for goods or services, transferring to another person, or withdrawing the funds.	Current Purchased Payment Facilities, digital wallets that store value, value stored on online accounts, virtual and physical pre-paid cards.
Issuance of Payment Stablecoins ('Payment Stablecoin SVFs')	Issuers of payment stablecoins that store value and control the total supply of payment stablecoins through issuance and redemption activities.	Payment stablecoin issuers.
Payment Instruments	A personalised or individualised set of procedures that allows a payer to instruct an entity with which its funds are held to initiate a transfer of funds to a payee.	Issuers of digital and physical cards (e.g. debit and credit cards, Buy Now Pay Later cards), cheques.
Payment Initiation Services	The initiation of payments from a payer to a payee by a third-party entity, at the request of a customer. The entity initiating a payment is a third party to the payment account where the payer's funds are held.	PayTo services, recurring payments initiated by a third party, direct debit or credit services.
Payment Facilitation Services	The process of entering into the possession of funds for the purpose of facilitating a transfer between a payer and payee. This includes for the purpose of acquiring, aggregating, disbursing, or otherwise transferring of funds within Australia.	Merchant acquirers, payment facilitators and aggregators, certain marketplaces and platforms, payout providers, certain payment processors, domestic money transfer service providers.
Payment Technology and Enablement Services	Payment specific services provided by third parties that enable payments to be made. These services enable a transfer of funds to occur but do not enter into possession or control of the funds.	Passthrough digital wallets, payment gateways.
Cross-border Transfer Services	A service that transfers or enables the transfer of funds from Australia to a payee outside of Australia, and/or of funds from outside of Australia to a payee in Australia.	Certain remittance providers, or international money transfer service providers.

ASIC's AFSL regime will generally apply to all PSPs that perform a payment function. Traditionally, the AFSL regime only apply when a business involves financial products or financial services. To take PSPs into the regulatory perimeter of the AFSL regime means that these payment functions will effectively become either financial products or financial services.

Transition issues

The Consultation Paper proposes the payments AFSL licensing requirements will come into force 18 months after the passage of legislation, to allow sufficient time for businesses to transition to the new arrangements. To obtain the benefit of the 18-month transitional relief, the Consultation Paper proposed that entities lodge an AFSL application within 6 months from the passage of legislation.

Further information on APRA's licensing expectations on Major SVFs will be released once APRA commences its consultation process.

Next Steps

Building on Treasury's previous consultation, this Consultation Paper improves and develops the proposed payment regulatory regime in multiple aspects, including refining the scope of payment functions that fall under the regime.

This proposed framework will likely bring the majority of Australia's payment industry participants, including those not currently requiring a licence, within the scope of the multi-layered regulation. Payment and payment related businesses should watch developments closely.

This consultation closes on **2 February 2024**. Please reach out to us if you wish to discuss any of the above or to make a submission.

Written by J Huang, M Bacina and S Pettigrove

Sony and Microsoft patents point to NFT gaming future

Sony and Microsoft, the two biggest video game publishers and console producers in the world, have both been reportedly making significant moves to integrate blockchain technology with gaming in recent years.

A series of big strides made by Sony include:

- filing a patent for a system allowing players to transfer digital assets (e.g. non-fungible tokens, or NFTs) between games on its PlayStation console using blockchain technology. This could enable digital asset ownership across different games rather than having assets locked to individual games;
- exploring tokenising in-game assets, allowing players to sell and trade them on secondary markets;
- announcing in October that it was partnering with Web3 builder Startale Labs to build their own blockchain; and
- in a recent blog post on the Sony Group portal, Sony announced plans to leverage blockchain beyond the confines of cryptocurrency, echoing a transformative belief in blockchain's potential to reshape social systems.

As for Microsoft, leaked documents show that it is planning to add crypto wallets to Xbox. This would allow players to trade digital assets across different platforms securely. Microsoft's is also pursuing the acquisition of Activision Blizzard and acquiring Savage Game Studios for mobile. This suggests that Microsoft is serious about expanding its gaming presence and that blockchain could play a role.

Video games and the "metaverse" have long been considered significant use cases of blockchain technologies, digital assets and NFTs. Some of the main drivers of the growth of the blockchain gaming market include:

- the increasing popularity of play-to-earn games;
- the growing demand for more immersive and engaging gaming experiences; and
- the increasing adoption of blockchain technology by game developers and publishers.

Sony and Microsoft are definitely not alone in eyeing a NFT gaming future. Companies like Disney are also increasing stepping onto the blockchain stage. Closer to home, Sydney based Immutable recently signed a deal with UbiSoft to bring Web3 into that studio's games.

The footsteps of global gaming titans certainly sends a resounding signal to the world—the era of blockchain isn't just a digital spectacle, but has the power to reshape entire industries.

By J Huang and M Bacina

Europe leading the global charge on AI governance

In a marathon of closed-door negotiations, the EU has etched a deal for the world's first comprehensive laws for artificial intelligence (AI), a groundbreaking move with repercussions echoing far beyond the continent's borders. Simply named the "Artificial Intelligent Act", the legislation aims to ensure that the fundamental rights of democracy are protected from high risk AI whilst boosting innovating and making Europe a leader in the field.

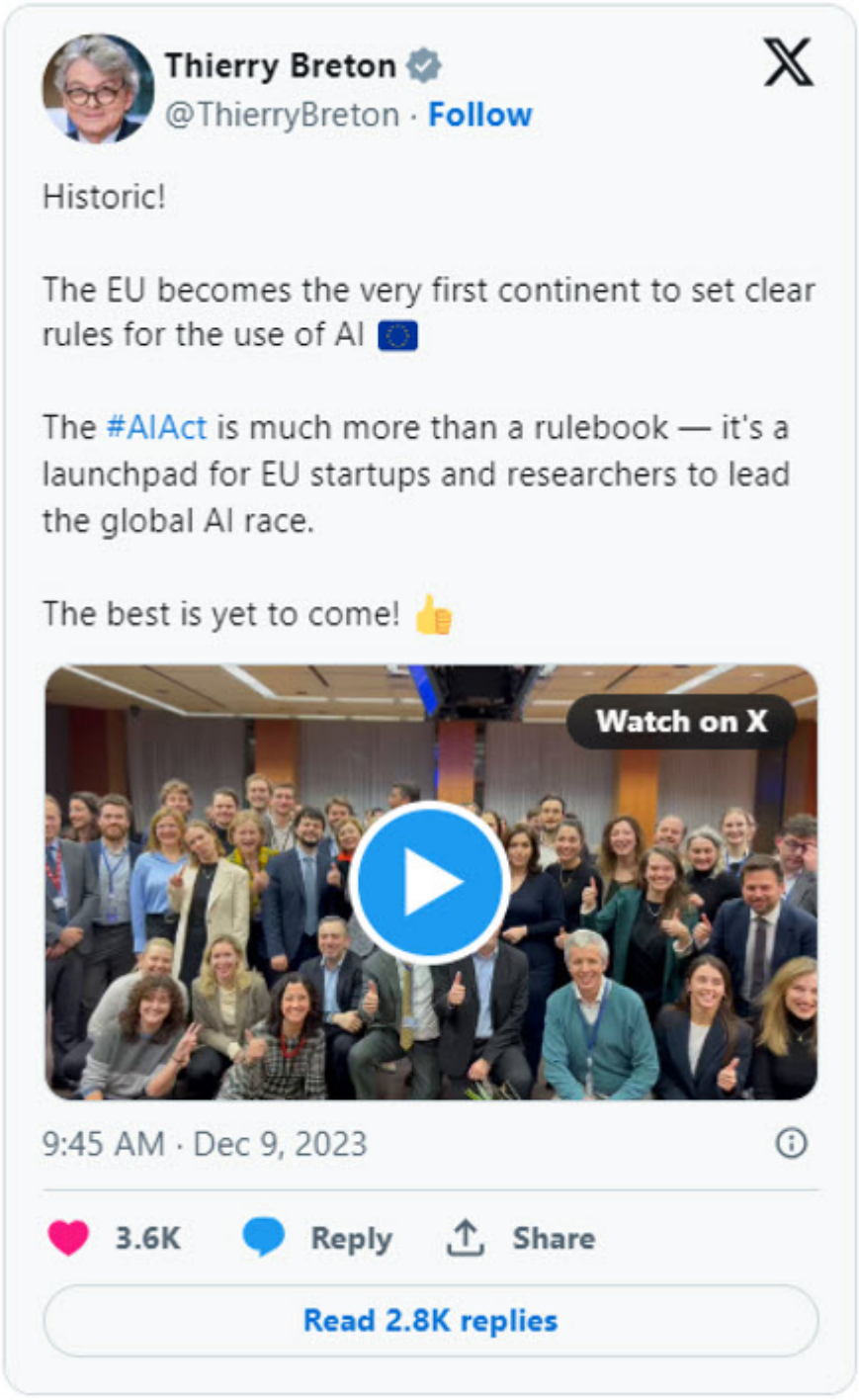
The deal, a meticulous dance between ambition and caution, puts the most advanced AI foundation models under a magnifying glass. These models, like OpenAI's ChatGPT and Google's Bard, bred by tech titans, carry the potential to shape society. Accordingly, heightened scrutiny will be applied to these models that pose significant "systemic risks". EU regulators caution that such AI models could be harnessed for disinformation, cyberattacks, or even the development of bioweapons. Given the current lack of regulatory oversight, the EU noted that the developers of such models should be

required to provide information on the data used to train the programs.

One of the most challenging points of negotiation in the deal was AI-powered facial recognition surveillance systems, with EU politicians calling for a blanket ban on its public use due to privacy concerns, with three specific exceptions. The police would be able to use the "invasive" technologies only in the event of:

1. an unexpected threat of a terrorist attack;
2. the need to search for victims; or
3. in the prosecution of serious crimes.

As European Commissioner Thierry Breton declares success with the "Historic!" development in a Tweet, the EU positions itself at the vanguard, setting a global precedent for AI governance. Unfortunately, the world will have to wait longer for the fine print of the legislation, expected to take effect no earlier than 2025.



The European Parliament still needs to vote on the Artificial Intelligence Act next year, but with the deal in place, approval

seems likely.

In the past year, generative AI has been the showstopper of the tech world, capturing our imaginations while stoking fears of job loss, privacy invasion, and copyright conundrums. In a recent case, AI has found itself in the legal hot seat. In the UK case of Felicity Harber v The Commissioners for His Majesty's Revenue and Customs [2023] TC09101, the First Tier Tribunal (FTT) uncovered that nine cases presented before Tribunal Judge Redstone were nothing but fabrications or "hallucinations" generated by an AI system akin to ChatGPT.

The appeal, which revolved around Harber's failure to notify the HMRC of Capital Gains Tax (CGT) on a property disposal, took an unexpected turn when it was revealed that the cases relied upon by Harber in her submissions were AI-generated. HMRC had assessed Harber for underdeclared gains related to undeclared rental income, slapping penalties on her for her failure to notify.

This isn't AI's first foray into legal fiction. The FTT highlighted a case across the pond, Mata v Avianca, Inc. 22-cv-1461(PKC), where barristers attempted to slip AI-generated fictitious cases past the Judge. They sought to rely on summaries that had "some traits that are superficially consistent with actual judicial decisions." The Judge was quick to sniff out the deception, identifying "stylistic and reasoning flaws that do not generally appear in decisions issued by United States Courts of Appeals."

Returning to the FTT case, the AI displayed a lack of legal acumen, failing to distinguish between the offences of failure to notify and late filing. The generated defense included a mishmash of cases, complete with American spellings in British judgments and suspiciously repetitive phrases. The FTT concluded that Harber was blissfully unaware that her defense was a product of AI creativity and otherwise dismissed her matter.

This case serves as another cautionary tale of using AI. While the technology has made remarkable strides in various fields, including law, relying blindly on its outputs may lead to legal misadventures that not even the best legal minds can untangle. That is why legislative and regulatory efforts like that of the EU's recent deal are positive steps toward an AI-assisted future, which at this stage, is looking inevitable.

By S Pettigrove, M Bacina and L Higgins

FSB says "crypto contagion" a limited threat to real economy

The Financial Stability Board (**FSB**), a multi-international financial standard-setter, said in its recent report that crypto firms that engage in multiple activities only pose a limited threat to the "real" economy.

The report, titled *The Financial Stability Implications of Multifunction Crypto-asset Intermediaries,* was published by the FSB on 28 November 2023. As its title suggests, the report focused on the financial stability risks associated with multifunction crypto-asset intermediaries (**MCIs**).

FSB defined MCIs as:

> individual firms, or groups of affiliated firms, that combine a broad range of crypto-asset services, products, and functions typically centred around the operation of a trading platform.

Many MCIs also have proprietary trading and investment functions, while some are also involved in issuing, promoting, and distributing crypto-assets including stablecoins. FSB raised several examples of MCIs: Coinbase, Binance and FTX (pre-collapse) – all got into various troubles with regulators, and the last being one of the reasons that prompted FSB to conduct this report.

FSB said MCIs vulnerabilities are not very different from those of traditional finance – common vulnerabilities include leverage, liquidity mismatch, technology and operational vulnerabilities, and interconnections.

However, some combinations of functions – which are typically separated in traditional finance – within a single MCI could exacerbate these vulnerabilities. Vulnerabilities are further also amplified by:

- a lack of effective controls and operational transparency,
- poor or no disclosures, and
- conflicts of interest.

Additionally, there are vulnerabilities stemming from the concentration of MCIs and their market power.

FSB concluded that:

> The collapse of a major MCI could have significant contagion effects for the crypto-asset ecosystem, but limited effects on the financial sector and the real economy.

In addition, FSB said further assessments are required because "significant information gaps remain."

As an international standard-settler that monitors financial systems and proposes rules to help prevent financial crises, FSB has been consistently focusing on the crypto sector. This report follows another FSB report in July advising on implementing a global regulatory framework for crypto-asset activities.

FSB's reports will provide valuable information and statistics that could inform governments around the world to come up with their regulatory framework for the crypto industry.

Written by J Huang and M Bacina

Capitol Hill dances between innovation and regulation in crypto clash

In a dynamic week on Capitol Hill, the cryptocurrency industry has watched competing approaches with the US House of Representatives endorsing a pro-blockchain bill and a bipartisan group of senators proposing measures to allegedly curb terror financing through crypto transactions.

In a unanimous vote, the House Committee on Energy and Commerce has given the nod to the Deploying American Blockchains Act, a 13-page legislative instrument aiming to propel the United States into a better position regarding blockchain technology. While not among the headline-making bills, it signifies another positive stride in Congress's attitude towards the blockchain industry.

The legislation directs the US Secretary of Commerce to champion the competitiveness of the US in the deployment, use, and application of blockchain and other distributed ledger technology. Ron Hammond, the Blockchain Association's Director of Government Relations, emphasised the non-partisan support for the bill within the committee in an interview with CoinDesk, highlighting its potential to either be combined with other legislative efforts or lead to agency action at the Department of Commerce:

> …[The House Committee on] Energy and Commerce is unanimously in support, and there's nothing partisan about it.
>
> [T]hese bills have either gotten looped together into larger bills or lead to agency action at [the Committee], which has been very open to conversation.

However, life will not be easy for this bill as it will face an uphill battle in the US Senate, where the cautious approach of the Democrat-controlled Senate towards digital asset bills presents a significant hurdle. It may be the case that merging these bills with broader, "must pass" legislation might be the key to navigating the Senate's undulating landscape.

Simultaneously, a bipartisan group of senators, led by Mitt Romney, has introduced the Terrorist Financing Prevention Act of 2023. This legislation expands existing sanctions to foreign entities supporting all groups designated as terrorists by the US, including those leveraging crypto transactions. The proposed act seeks to equip law enforcement with additional tools to counter terrorism financing, purporting to address the continued overemphasised role that digital assets play in the battle against global money laundering and terrorism financing.

Romney, emphasising the urgency following the October 7 attacks on Israel by Hamas, stated that the legislation aims to cover all terrorist organizations, including Hamas. The bill broadens existing sanctions, originally focused on Hezbollah, to include all US-designated foreign terrorist organisations and their supporting entities.

The use of crypto in financing terrorism has long been a stated concern for regulators and law enforcement, despite there being very limited data on the extent to which it is occurring. Recent debates among Republican presidential candidates have continually framed digital assets as tools for "fraudsters, criminals, and terrorists" without evidence to support the position.

The discussion intensified with a Wall Street Journal report suggesting substantial crypto funds were used to find terrorist Palestinian groups, a claim challenged by blockchain analytics firms like Chainalysis. Shortly after the WSJ publication blockchain security firm Elliptic stated that there was no substantial evidence supporting significant crypto donations to Hamas, noting the transparency of the blockchain and the effectiveness of monitoring tools in tracking and freezing fund flows, leaving the Wall Street Journal with egg on their face.

These events underscore the dynamic nature of cryptocurrency regulation and the battle over the narrative and the Overton Window around such regulation. Even positive developments like the Deploying American Blockchains Act are overshadowed by measures such as the Terrorist Financing Prevention Act with a "risk focus" outweighing an "innovation focus" when the two are not mutually exclusive. In addition to the disparaging comments toward crypto in the recent presidential debates, it is clear the US still has a long way to come on reaching consensus on regulation. As both bills navigate the complex legislative process, the crypto industry watches closely, with a pessimistic view towards the likely future regulatory landscape in the United States for blockchain technology.

By M Bacina and L Higgins

Buterin Backs Zk-rollup centric roadmap

In a blog post on December 13, Vitalik Buterin, the co-founder of Ethereum announced plans of an 'enshrined zkEVM' to address existing layer-2 challenges on Ethereum. It stands for Zero Knowledge Ethereum Virtual Machine and proposes to implement a Zk-rollup directly on the Ethereum mainnet. The disruptive potential of layer-2 blockchain scaling solutions have already been widely recognised in the industry, with notable layer-2 projects from Matter Labs and Polygon attracting billions in user deposits.

In particular, Buterin highlighted 'speed' as the key benefit of the 'enshrined zkEVM', alongside 'basic guarantees of correct functionality and security'. Although the EVM verification functionality will be handled by the protocol natively under this proposal, he emphasised that layer 2 projects will continue to play an important role, including:

- Servicing fast pre-confirmations;
- Overseeing MEV mitigation strategies;
- Incorporating extensions to the EVM, including almost-EVMs; and
- Managing user and developer experience and attracting users and projects.

Buterin summarised the key properties of this 'enshrined zkEVM' as:

- Verifying Ethereum blocks;
- Compatibility with Ethereum's multi-client philosophy – it must meet data availability requirements such that provers using different proving systems may re-prove the execution and clients can verify new proofs;
- Auditability – to ensure users and developers can inspect and audit errors;
- Upgradeability – to prevent and timely address system bugs; and
- Supporting almost-EVMs – by leveraging L2's ability to innovate on the execution layer and make extensions to the EVM.

The proposals are grounded on his vision of an ‘open multi-client system’, in which proofs are placed externally to the block and verifiable by users separately. This means that users enjoy flexibility to engage whatever client they want to verify the blocks given certain conditions are met. Such a proof system which gains influence by ‘convincing users to run them, and not by convincing the protocol governance process’ is likely to foster more client trust and loyalty.

Projects like Loopring and Zksync have already implemented Zk-rollups, with users on mainnets. While Buterin has shown support for Zk-rollups on Ethereum mainnet through this recent announcement, its implementation remains unconfirmed at this stage:

> The upsides of implementing a protocol feature should be weighed against the benefits of leaving things to the ecosystem and keeping the base protocol simple.

This cautious approach is sensible given the ‘engineering challenge’, ‘costs of research and development’ and other unseen ‘complexity costs’ associated with its implementation.

By T Masters and K Kim