

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: Digital ID bills passed, Australia's Budget Allocation for Crypto, Finance Regulation and Tech Innovation, Kraken wrestles SEC over regulatory waterline, Tornado Cash judgment yields whirlwind for developers, Sheriff of Wall St issues Wells Notice to Robinhood

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

Digital ID bills passed

The much-anticipated [Digital ID bill](#), together with the Digital ID Bill (Transitional and Consequential Provisions) has finally passed the Australian Parliament this week.

The new legislation will broaden the availability of digital ID in Australia, which is currently limited to government services, many of which are lacking sophisticated user interfaces, including MyGov and Centrelink, to include State and Territory governments and private businesses. The changes are aimed at streamlining online ID verification processes, and preventing businesses from holding copies of primary documents which are then susceptible to hacks and theft.

Under the new system, individuals will be able to use smart wallets to link credentials to the chosen identity app.

The Government expects the Bills will:

- strengthen a voluntary Accreditation Scheme for digital ID service providers that wish to demonstrate compliance with best practice privacy, security, proofing and authentication standards;
- enable expansion of the Australian Government Digital ID System for use by the Commonwealth, state and territory governments and eventually private sector organisations; and
- embed strong privacy and consumer safeguards, in addition to the Privacy Act, to ensure users are protected

The Bills are expected to receive Royal Assent in coming weeks and to commence by November 2024. Accredited businesses [will be able to apply to join the Australian Government Digital ID System within two years of commencement](#), with banks and credit card operators expected to be the first to access the scheme.

From commencement, the Australian Competition and Consumer Commission (**ACCC**) will be the Digital ID Regulator alongside the Office of the Australian Information Commissioner (**OAIC**), who will regulate the privacy aspects of the Australia's Digital ID System. At this stage there is no indication that blockchain technology will be used for Australia's digital ID system which may be a missed opportunity, but interfaces with digital ID and smart contract services in future will be needed to unlock the benefits of the technology.

While some critics previously [complained](#) that the bills was expedited through the Parliament without proper debate, [Katy Gallagher, the Minister for Finance said](#):

Improving safety online is a priority for us and legislation will ensure strong independent oversight is in place to support the expansion of the Australian Government Digital ID System from mid-2024.

And:

We've spoken with business, community and privacy groups to ensure the Bill will deliver the privacy safeguards, accreditation options and consumer safeguards they expect

Gallagher also highlighted that the digital ID scheme will remain voluntary and alternative methods will be available for those that do not wish to use digital identity verification processes. The Government has budgeted AUD\$145.5M to implement regulation and oversight of the scheme.

The danger of Australia becoming a "digital papers please" environment may be overblown, but concerns of creeping surveillance will remain and it is hoped the Government keeps a careful review and limit on just what information is needed to be collected from citizens to keep our privacy and freedom protected.

Written by Jake Huang, Michael Bacina and Steven Pettigrove

Australia's Budget Allocation for Crypto, Finance Regulation and Tech Innovation

The [Australian Federal Budget for FY24-25](#) was announced last night with broad changes across key areas and new funding allocation for regulators and initiatives. The changes are sweeping with some noteworthy priorities sure to affect Australia's developing crypto regulation. We've set out some of those priorities below:

Modernising Digital Assets and Payments Regulation

\$7.5 million is being allocated to the development of digital asset regulation and licensing frameworks. This funding comes on the back of previous moves the Australian Government has made to understand the crypto space and develop regulation.

The Government will provide \$7.5 million over four years from 2024-25 (and \$1.5 million per year ongoing) to modernise regulatory frameworks for financial services to improve competition and consumer protections for services enabled by new technology, including to:

- develop and consult on legislation to licence and regulate platforms that hold digital assets and progress related reforms, including continuing exploratory work on Central Bank Digital Currencies, asset tokenisation and decentralised finance
- introduce a new regulatory framework for payment service providers (including digital wallets and electronic stored value providers), including licensing and a mandated ePayments Code.

The Government will consider future funding requirements to implement the proposed reforms informed by the development of legislation.

Funding for Regulators

A number of regulators get a big shot in the arm across a variety of different priorities including the development of the "Scams Code Framework", measures to promote and enforce sustainable financial markets and Data Capability. Some of the highlights:

- \$37.3 million over four years from 2024-25 to administer and enforce mandatory industry codes for regulated businesses to address scams on their platforms and services. Telecommunications, banks and digital platforms services related to social media, paid search engine advertising and direct messaging will be initially targeted. The funding is allocated to the Australian Competition and Consumer Commission (**ACCC**), the Australian Securities and Investments Commission (**ASIC**) and the Australian Communications and Media Authority (**ACMA**).
- \$6.3 million in 2024-25 for the ACCC to improve public awareness of scams and help the public to identify, avoid and report scams

- \$1.6 million over two years from 2024–25 for the Treasury to develop and legislate the overarching Scams Code Framework. [Budget Measures Paper No.2](#) notes:

Partial funding for this measure will be held in the Contingency Reserve pending development of the preferred legislative approach for the Scams Code Framework.

- \$10.0 million over four years for resourcing for ASIC to investigate and take enforcement action against market participants engaging in greenwashing and other sustainability-related financial misconduct
- \$5.3 million over four years to deliver the sustainable finance framework, including issuing green bonds, improving data and engaging in the development of international regulatory regimes related to sustainable finance with funding allocated to for the Treasury, ASIC and the Australian Prudential Regulation Authority (APRA)
- \$206.4 million over four years to ASIC and APRA to improve the data capability and cyber security of those regulators.
- \$160.8 million over two years for the Australian Transaction Reports and Analysis Centre (AUSTRAC) to expand its regulatory, intelligence and data capabilities and provide guidance to newly regulated entities.
- \$7.0 million over four years to support implementation of the anti-money laundering and counter-terrorism financing (AML/CTF) legislative reforms capable of delivery in the Pacific.
- \$145.4 million over two years from 2024–25 to maintain the National Measurement Institute’s core scientific measurement and ICT capabilities and to support current site operations and future planning.

Taxation

The paper is silent on funding for the much hoped for reforms following the [Board of Taxation’s report to the Australian government on the tax treatment of digital assets and transactions in Australia](#).

However, amongst a plethora of tax concessions and cuts for small businesses and individuals the paper also details that the ATO will receive additional funding to beef up its compliance capabilities to counter fraud and other instances of non-compliance by taxpayers. This includes:

- \$78.7 million for upgrades to information and communications technologies to enable the ATO to identify and block suspicious activity in real time.
- \$24.8 million to improve the ATO’s management and governance of its counter-fraud activities, including improving how the ATO assists individuals harmed by fraud.

Responsible AI

The government also turns its attention to the development of AI policy with some target funding on several initiatives in this space including:

- \$21.6 million over four years to establish an AI advisory body within the Department of Industry, Science and Resources – the National AI Centre (NAIC).
- \$15.7 million over two years to support industry analytical capability and coordination of AI policy development, regulation and engagement activities across government.
- \$2.6 million over three years from 2024–25 to respond to and mitigate against national security risks related to AI.

Quantum Computing

Finally, we have some noteworthy support for Psiquantum, the Brisbane-based tech company building what is reportedly the “world’s first” quantum computer who receive \$466.4 million for a financing package of equity and loans provided on the National Interest Account.

The budget papers report that:

Additional funding of \$27.7 million over 11 years from 2023–24 will also be provided for the Department of Finance, the Department of Foreign Affairs and Trade, the Department of Industry, Science and Resources and the Department of the Treasury to manage and provide oversight of this investment.

Budget Takeaways

Reading the Federal Budget tea-leaves gives us only broad insight into the allocation of funds but it is clear that the Australian Government intends to press ahead with the [proposed regulatory reforms](#) for regulating digital asset platforms. The Government are clearly hedging their bets on future funding which does seem to suggest a lack of clarity in

anticipating required funding for regulators to implement any proposed reforms. However, the funding statement for AUSTRAC, who currently impose a registration requirement on digital exchanges, does include a mention of “guidance to newly regulated entities” which may provide some insight into the expectations Government have as to which entities will be involved in the proposed regulatory reforms.

There is a lot to be learned from the budget, but it is difficult to have certainty on the direction these initiatives will take. On a general overview, more funding for digital innovation and tech is a very good thing. The government just has to be cautious in finding the balance between promoting innovation, and taking enforcement actions against true harm to Australians.

Regulation need not be heavy, nor light. It should be smart.

Written by Tim Masters, Luke Higgins and Michael Bacina

Kraken wrestles SEC over regulatory waterline

Global crypto exchange Kraken has pushed back in litigation with the US Securities and Exchange Commission (SEC), [which alleges Kraken operated an unregistered securities exchange, clearing agency, and broker](#).

In a [filing on 9 May, Kraken argues that the SEC](#):

has not identified any investment contracts that were (or could be) traded, brokered, or settled on Kraken.

Kraken also argues that the agency failed to satisfy elements of the Howey Test, a 1946 US Supreme Court case frequently cited by the SEC, to determine if an asset qualifies as an investment contract and, therefore, a security.

These issues are central to the SEC’s case against Kraken, which is premised on Kraken operating a trading platform for securities.

Kraken’s filing follows its motion to dismiss the SEC’s lawsuit, which is now set for hearing 12 June. Kraken previously [moved to dismiss](#) the lawsuit in February, to which [the SEC responded by way of filing in April](#).

Kraken has also sought to rely on the “major questions doctrine” in its most recent filing. The doctrine, which has been often cited by crypto firms, asserts that if an agency wants to decide on an issue that has major national significance, it has to be supported by “clear congressional authorisation”.

In the April filing, the SEC asserted that it is not “assuming new powers”:

To argue that the SEC is assuming new powers in doing so here suggests that new technologies are beyond the scope of traditional securities law. They are not... Congress does not need to enact bespoke laws for each new technology that emerges.

Kraken is not alone in its woes with the SEC. [Coinbase](#) and [Binance](#) have both faced charges from the SEC, with the latter also being slapped with a US\$4.3 billion dollar fine by the Department of Justice and Commodity and Futures Trading Commission, as well as a personal US\$50 million dollar fine for its CEO, Changpeng Zhao. Zhao subsequently resigned his role and [was sentenced to four months in prison](#) over anti-money laundering violations.

Kraken [issued a response to the SEC action in a blog](#), stating its unwavering commitment to provide its services:

We disagree [with the SEC’s complaint against Kraken], and intend to vigorously defend our position in court. [The news] has no impact on the products we offer and we will continue to provide services to our clients without interruption.

Kraken also [asserts SEC registration is impossible](#) and there is no path to compliance.

The stage is now set for a hearing on Kraken’s motion in June. The outcome of this case will likely set important precedents on the SEC’s regulatory perimeter and on future enforcement actions against other crypto exchanges.

Tornado Cash judgment yields whirlwind for developers

[Alexey Pertsev, one of the core software developers of the sanctioned crypto-mixer service, Tornado Cash](#), has been convicted of laundering over USD\$1.2 billion and sentenced to 64 months in jail by a Dutch criminal court.

In the [judgment \(in Dutch\)](#) and the [media release \(in English\)](#) published by the court, the court labelled Tornado Cash as “no legitimate tool” that

combines maximum anonymity and optimal concealment techniques with a serious lack of functionalities that make identification, control or investigation possible.

The court rejected arguments that Tornado Cash was unintentionally abused by criminals, suggesting that it was created for criminal use only. It also found the defendant (and his co-developers) leveraged blockchains and DeFi and that Tornado Cash:

automatically performs the concealment acts that are needed for money laundering.


As for Pertsev’s subjective state of mind in relation to the crimes, the court said he was aware that Tornado Cash was being used for money laundering – which the court called “common knowledge” – while he kept developing the software. The court also cited damning evidence in group chats discussing Ether hacks and how cryptocurrency with a criminal origin was deposited into Tornado Cash.

The court sentenced Pertsev to imprisonment for 5 years and 4 months. It also ruled that his Porsche and cryptocurrency worth 1.9 million euros, which had been seized, will not be returned to him.

Many fear that this judgement will set a dangerous precedent for software developers, including two other Tornado Cash co-developers Roman Storm and Roman Semenov, who are currently [facing money laundering and sanction violation charges](#) in the US.

Peter Van Valkenburg, the Director of Research at Coin Center (which previously [sued the US Treasury Department over privacy concerns](#) relating to their sanctioning of Tornado Cash), voiced disappointment with the judgement on X.



Peter Van Valkenburgh  · May 14



@valkenburgh · [Follow](#)

Replying to @valkenburgh

This part of the Pertsev verdict is just factually incorrect. The trusted setup generates parameters for the zero knowledge proof. That activity has nothing to do with setting the smart contract update capability to the zero address. These events may have occurred around the same...

is transported to the [crypto system] team, during the trusted setup ceremony, the [crypto system] team also gratefully embraced by the user with criminal intentions.

ated Setup ceremony will take place at the initiative of the [crypto system] team, during the address of the smart contracts of the pools was set to 0. This gave up any form of smart contracts. [§5](#) The verifier, a smart contract that checks whether the recording of [zero-knowledge proof], could no longer be changed from that moment on. [§6](#) Users are sure of complete anonymity, without the risk of human interference. The suspect is one of attributed to this. [§7](#)

It has not distanced himself from [crypto system] at any time, despite his knowledge of minimal assets into [crypto system]. He remained actively involved in [crypto system] until at on August 30, 2022. [§8](#)



Peter Van Valkenburgh 

@valkenburgh · [Follow](#)

As an American I find this part of the verdict bizarre. I'm actually not a fan of guns personally but if you told me that Smith and Wesson is obligated under law to emphatically disavow and decry their own products and distance themselves from their promotion and continued usage,... [Show more](#)

self from [crypto system] by no longer promoting its use and abused. However, at no time did the suspect report to authorities deposited in [crypto system] or other measures were taken. On [co-suspect 2] have only drawn up a general message that they help if it appears that their stolen Ether has been deposited into it clear that the [crypto system] team cannot do anything for

has sought legal advice. This would also show that there was no chance. The court determines the following.

11:40 PM · May 14, 2024



81



Reply



Share

[Read 2 replies](#)

With Pertsev's sentence, all eyes are now on the forthcoming US trials. The US Department of Justice recently filed a [111-page-long response rejecting the request to dismiss charges against Roman Storm](#), which is now headed for a jury trial.

The continuing legal battle will likely have broad ramifications for software developers as the US and Dutch governments seek to impose liability on Tornado Cash's developers for the acts of third parties who exploited the autonomous smart contracts underpinning the protocol. The US trial will further define the boundaries of legitimate software development activities and developers' liability where that software facilitates illicit funds flows.

Written by Jake Huang, Steven Pettigrove and Michael Bacina

Sheriff of Wall St issues Wells Notice to Robinhood

The US Securities and Exchange Commission (SEC) has issued another Wells Notice, this time to the crypto unit of the brokerage firm Robinhood Markets. The SEC recently issued a Wells Notice to [Uniswap](#), making this the second Wells Notice issued to Web3 companies in as many months, and rumours abound that further Wells Notices have been issued which haven't seen the light of day.

A Wells Notice is a document used by the SEC to inform a person or entity that it has started an investigation and, unless the target can persuade them not to, that they intend to bring charges for securities laws violations. Wells Notices are typically followed by enforcement action, and almost always have been in the crypto space.

Robinhood had previously attempted to register as a special purpose broker for digital assets with the SEC. Spearheaded by Chief Legal Compliance and Corporate Affairs Officer, Dan Gallagher (who is also a former SEC commissioner), the company sought to effectively collaborate with the regulator to ensure compliance.

According to reports, Robinhood went through a 16-month process under which it supplied documents and information to the SEC, only to be abruptly told the process was over and the registration is unsuccessful. Mr Gallagher was seemingly less than impressed having received the Wells Notice, saying in a [statement](#) that he was disappointed:

After years of good faith attempts to work with the SEC for regulatory clarity including our well-known attempt to 'come in and register,' we are disappointed that the agency has decided to issue a Wells Notice related to our U.S. crypto business,

We firmly believe that the assets listed on our platform are not securities and we look forward to engaging with the SEC to make clear just how weak any case against Robinhood Crypto would be on both the facts and the law.

The SEC has been unrelenting in its unofficial [regulation by enforcement](#) policy over the past few years and has been more and more transparent about seeking to prevent crypto businesses operating in the way that crypto permits, going so far as to allege in an appeal filing that Coinbase "decided to arrange its business affairs in ways that may make it costly to comply with existing law" when it seems obvious that Coinbase could not arrange their affairs in any other way while still using blockchain technology. After targeting [Kraken](#), [Binance](#) and [Coinbase](#), the SEC is seemingly pursuing crypto companies without any rhyme or reason and risking allegations that they are not in fact adhering to technology-neutral principles based regulation, but rather deciding upon the rules without consultation of the public or explaining how their position meets their mandate.

The regulation by enforcement approach has made its way to Australia, with the Australian Securities and Investments Commission (ASIC) recently suing a number of projects over products which were removed when the regulator reached out, but have still been the subject of prosecution, as well as misleading and deceptive representations claims being brought together with alleged financial services law breaches (in the case of [BPS Financial](#)). While ASIC does not have the large enforcement appetite (or budget) of its US counterparts, the absence of clear rules, even within a principles based regulatory approach coupled with enforcement actions without due guidance and prior warning is not a comfortable precedent to protect Australian users of crypto products.

Written by Steven Pettigrove, Michael Bacina and Luke Misthos