

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: Australia digital IDs to slash scams and crimes, Institutional crypto custody in Australia, New bill proposes seizure powers over digital assets, Cryptopia lays distribution plans, Immutable and King River back \$100m Web3 games fund

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.

Australia identity docs driving to digital to slash scams and crime

The [Digital ID Bill 2023](#), introducing a digital identity verification scheme, passed the Australian Senate with a 33 to 26 vote this week. Accredited businesses [will be able to apply to trial the scheme within two years](#) of commencement of the Act, with banks and credit card operators expected to be the first to access the scheme.

The new legislation will broaden the availability of digital ID in Australia, which is currently limited to government services lacking sophisticated user interfaces and including MyGov and Centrelink, to include State and Territory governments and private businesses. The changes are aimed at streamlining online ID verification processes, preventing businesses from holding copies of primary documents which are then susceptible to hacks and theft. Under the system, individuals will be able to use smart wallets to link credentials to the chosen identity app.

Not all were pleased with the Bill, with former fish and chip shop owner and conservative senator Pauline Hanson throwing shade:



Pauline Hanson  
 @PaulineHansonOz · [Follow](#)



BREAKING NEWS: Anthony Albanese's Labor Government has just rammed Digital ID legislation through the parliament. No debate was allowed, and no questions were allowed to be asked of ministers.

Labor, Greens, Pocock, Lambie, Tyrrell and Van all voted to pass this legislation.... [Show more](#)

Wednesday, 27 March 2024 (05.50pm) Division no. 907

Digital ID Bill 2023 and a related bill

Remaining stages

Question—That the remaining stages of the bills be agreed to and the bills be now passed

The Senate divided—

AYES, 33

Senators—

Allman-Payne
 Ayres
 Bilyk
 Brown
 Chisholm
 Ciccone
 Cox
 Faruqi
 Ghosh

Green
 Grogan*
 Hanson-Young
 Lambie
 Lines
 McKim
 Payman
 Pocock, Barbara

Pocock, David
 Polley
 Pratt
 Rice
 Sheldon
 Shoebidge
 Smith, Marielle
 Steele-John

Sterle
 Stewart
 Tyrrell
 Urquhart
 Van
 Walsh
 Waters
 Whish-Wilson

NOES, 26

Senators—

Antic
 Ashew
 Babet
 Bragg
 Brockman
 Cadell*
 Canavan

Cash
 Chandler
 Colbeck
 Davey
 Duniam
 Fawcett
 Hanson

Hume
 Liddle
 McDonald
 McGrath
 McLachlan
 Nampijinpa Price

O'Sullivan
 Rennick
 Roberts
 Ruston
 Scarr
 Smith, Dean

* Tellers

Question agreed to.

Although the passage was met with concerns from critics that the bill 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.

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 is budgeting AUD\$145.5M to

implement regulation and oversight of the scheme.

Large-scale data breaches in recent years, including Optus, Medibank and Challenger hacks highlights the problems of records of identity being kept in servers for years as mandated by law.

New South Wales has had a very successful digital driver's licence in place for a number of years, but it has not been accepted as valid ID at the federal level. A move to reduce friction and prevent copies of identification being kept where they aren't needed is hoped to lead to greater efficiencies for businesses that must check ID, and reduce identity theft and other problems.

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 Michael Bacina and Kelly Kim

Is your crypto Safu? Institutional crypto custody in Australia

After the US approved its' [first spot Bitcoin exchange traded funds](#) earlier this year (**ETF**), Bitcoin has soared to historical high prices. The successful ETF launch has led to increased interest among Australian fund managers in exploring new crypto-asset specialised funds, or extending their asset portfolio to crypto-assets in order to provide their customers regulated pathways to invest in the asset class. One of the key issues for investors and asset managers to consider are custody obligations for holding this unique asset class.

Crypto-assets raise unique custody considerations under existing laws and regulatory guidance. Crypto-assets are recorded on blockchains and transfers are generally irreversible. The bearer nature of these assets requires an enhanced focus on security measures and internal compliance. Moreover, the need for asset managers to hold crypto-assets securely and compliantly is vital to instil confidence in customers to invest in their funds.

While [the Australian government is currently considering a new legal framework](#) to regulate crypto custody activities, it will be some time before these laws and accompanying rules come into force. Before then and under the current legal framework, asset managers must determine whether the assets they propose to custody are financial products and, in any event, their custody obligations under regulatory guidance published by the Australian Investments and Securities Commission (**ASIC**).

ASIC Regulatory Guide 133

Regulatory Guide 133—Fund management and custodial services: Holding assets (RG 133) was published by ASIC in June 2022, it applies to certain licensed entities under the Australian Financial Services Licence (**AFSL**) regime and other asset holders holding assets under the AFSL umbrella of their client.

When ASIC published RG 133, it likely did not have crypto-asset custody in mind, hence RG 133 does not establish bespoke requirements specific to the custody of crypto-assets. Nevertheless, RG 133 sets out general minimum standards that apply to AFSL holders who hold custody of assets, or third parties that the AFSL holders engage to hold assets for their clients which may apply to custody of crypto-assets.

If asset holders fail to satisfy the minimum standards, the AFSL holder (such as the fund manager of a retail managed fund, called a Responsible Entity) would be in breach of RG 133 for failing to "do all things necessary" to ensure compliance. This may lead to legal, financial and reputational liabilities for the AFSL holder. It is for this reason that AFSL holders should expect and seek assurance that the third parties they engage to hold crypto assets are complying with RG 133.

Information Sheet 225 and Response 705

In addition, ASIC has issued guidance that is specifically related to the custody of crypto-assets in Information Sheet 225 (**INFO 225**) and in *Report 705 - Response to submissions on CP343 Crypto-assets as underlying assets for ETPs and other investment products* (**REP 705**).

INFO 225 and REP 705 should be read together as the latter seeks to clarify the former. Together they offer good practice guidance for operators of registered managed investment schemes that are authorised to hold and deal in crypto-assets. Some of the key guidance include:

- methods and solutions to safeguard private keys;

- segregation of crypto-assets on a blockchain;
- signing approaches;
- physical and cyber security practices;
- competency and resourcing; and
- compensation arrangements.

In particular, ASIC has emphasised that the security of private keys is of critical importance, as private keys are necessary to sign transactions that assign crypto-assets to new addresses. If private keys are compromised, unauthorised parties can use them to transfer the scheme's crypto-assets to addresses (and parties) that are outside the control of the fund manager. Accordingly, retail fund managers and their custodians should ensure that the private keys used by the scheme are protected from unauthorised access – both online and offline. They may need to consider using hot and cold wallets, or a combination of them.

Interestingly, INFO 225 and REP 750 do not impose any requirement on retail fund managers to engage an Australian domiciled custodian to hold crypto-assets.

Though the guidance in INFO 225 and REP 750 are not legal requirements, when a retail fund manager engages a third party to hold crypto-assets, they should expect the third party to have considered this good practice guidance in establishing key systems and processes for holding crypto-assets as fund property.

Conclusion

While many fund managers are eager to add crypto-assets to their fund portfolio, they must do so carefully to comply with regulatory requirements. Given the unique nature of crypto-assets, some fund managers may find it more time-efficient and cost-effective to seek professional custodians who can hold crypto assets securely and compliantly on their behalf. When choosing the right crypto custodian, Australian fund managers should consider whether the custodians have measures comparable to those outlined in RG 133, INFO 225 and REP 750.

Written by Jake Huang and Steven Pettigrove and Michael Bacina

New bill proposes broad seizure powers over digital assets

The Australian Parliament will debate whether to enact a bill giving criminal authorities broad powers to seize digital assets. The [Crimes and Other Legislation Amendment \(Omnibus No. 1\) Bill 2024 \(the Bill\)](#) moved to a second reading yesterday and Parliament is currently considering amendments before a final vote.

The Bill proposes amending the *Crimes Act 1914 (Crimes Act)* and the *Proceeds of Crime Act 2002 (Proceeds of Crime Act)* by introducing a framework for the seizure of digital assets, reflecting a significant, and powerful shift in law enforcement's focus on digital assets.

The Bill proposes a broad definition of “digital assets” to encompass digital representations of value or rights, including those held and transferred electronically via distributed ledger technology or similar structures.

The proposed amendments would enable law enforcement to seize digital assets under warrant in specific conditions. This includes the provision that digital assets can be seized if they are suspected to be evidential material related to indictable offences and that the seizure of the digital assets is necessary to prevent the digital asset's concealment, loss or distribution, or use in committing an offence.

Interestingly, the Bill permits the use by the authorities of a computer or a data storage device found in the course of a search, a telecommunications facility operated by the Commonwealth or a carrier, or any other electronic equipment in order to seize a digital asset under a search warrant or for the purposes of obtaining access to data that is held in a computer or device in order to determine whether that data suggests the existence of a digital asset that may be seized.

Authorities also have the power to add, copy, delete or alter other data in a computer or device if necessary to obtain that data which relates to digital assets the subject of a warrant.

The enforcement powers proposed by the Bill, while designed to protect digital assets from being used for illicit purposes, will enable authorities broad power to control, manipulate, destroy and add any data as they see fit so long as it relates to the existence of digital assets which are the subject of a search warrant. In effect, the Bill would give criminal authorities broad power to interfere with digital property rights where they suspect criminal activity has or may occur.

The Bill also includes amendments to the Proceeds of Crime Act which would extend law enforcement authorities'

information gathering powers and freezing orders that currently apply to financial institutions to digital currency exchanges.

Proposed amendments to the bill will be circulated before a final vote by Parliament. The proposed changes follow on the heels of [legislation adopted in the UK which giving UK criminal authorities enhanced powers to seize and “destroy” crypto-assets](#) linked to alleged criminal activities without a criminal conviction. A former Australian Federal Police officer [appeared in Court in February to fight allegations](#) that he stole more than \$6 million in cryptocurrency following a raid in Hoppers Crossing in 2019.

Written by Steven Pettigrove and Luke Misthos

Easter tidings as Cryptopia lays distribution plans

Cryptopia, a New Zealand-based cryptocurrency exchange, has received Court approval to begin returning cryptocurrencies to its users after [being hit by a cyberattack in 2019](#). The now defunct exchange plans to distribute bitcoin (BTC) and Dogecoin (DOGE) to qualifying users within three months, with more distributions expected to follow.

This development follows a [recent ruling in the company’s bankruptcy case by a New Zealand Court](#). Cryptopia detailed the claims process in an email to users, outlining steps to reclaim their assets. After the initial distribution, efforts will continue to return remaining cryptocurrencies by the end of 2024.

The exchange failed in 2019, losing USD\$15.5 million of user holdings to a cyberattack. Trading services were suspended and a police investigation commenced. It was later revealed that the hacking took place between 14 to 17 January 2019.



Four months after the hack, the exchange announced it had [appointed Grant Thornton as liquidator](#). A series of court hearings followed, including a [landmark New Zealand High Court](#) case brought by the liquidators to determine the legal status of cryptocurrencies held by Cryptopia and whether the assets were held on trust by the exchange. It was ultimately decided by the Court that crypto-assets were “a species of intangible personal property” and “an identifiable thing of value” that was capable of being held on trust.

During the liquidation phase in 2021 further losses occurred [when a former employee pilfered USD \\$170,000 worth of crypto](#), adding salt to the wound. In the recent hearing, Cryptopia stated that it was exploring avenues to recover these stolen funds, including assets traced by the FBI.

The Court detailed the distribution plan in its orders at paragraph [58] of the decision:

1. The claim valuation date for accountholders would be 14 May 2019 (the date the exchange went into liquidation);
2. The liquidators are permitted to make distributions to accountholders who have registered their claim by a specific cut-off date;
3. In relation to unclaimed holdings, the liquidators be permitted to make distributions to accountholders an amount by way of reimbursement of costs charged to such accountholders;

4. A review process be established for accountholders unsatisfied with their claims (Order 3);
5. There is no requirement to take any steps in relation to cryptocurrencies that have no or nominal realisable value (Order 4); and
6. The liquidators be permitted to treat account holders who have an account balance equivalent or less than the actual or anticipated cost of the trust administration of the distribution as having no right to participate in the distribution (i.e. nominal claims) (Order 5).

After a journey down the rabbit hole marred by a cyberattack, theft and court proceedings, the hunt for returns looks to be nearing a close for Cryptopians users with distributions expected to commence this year.

Written by Luke Higgins, Steven Pettigrove and Michael Bacina

Immutable and King River backs \$100m Web3 games fund

Immutable, Polygon Labs and King River Capital [have united to back the Inevitable Games Fund \(IGF\)](#), to encourage growth and innovation in blockchain based video games.

The strategic partnership combines King River Capital's investment prowess with Immutable's deep web3 gaming expertise, and Polygon Labs' international reach. The collaboration underscores its backers confidence in web3 gaming's potential and their commitment to nurturing innovation within this dynamic space.

Head of Investments at Immutable, Brendan Ma, [took to LinkedIn](#) to announce the flagship venture.



Brendan Ma • 1st
Chief of Staff & Head of Investments at Immutable | ex-Goldman Sachs
1w • 

...

They said it was impossible - we said it was inevitable. Delighted today to announce the launch of the Inevitable Games Fund (IGF), a flagship global venture fund that will invest across web3 gaming and infrastructure opportunities.

IGF is backed by [Immutable](#) and our deep partnerships with [Polygon Labs](#) and [King River Capital](#), as well as commitments from [Alpha Wave Global](#) (backed by the Abu Dhabi Royal Group), [Merit Circle](#), [Arrington XRP Capital](#), [Steven Kokinos](#) (Sonic Boom Ventures), [Sandeep Nailwal](#), [Robbie Ferguson](#), [James Ferguson](#) and more investors.

Immutable and Polygon Labs launch Inevitable Games Fund with hopes of raising \$100M

The fund has already secured \$30 million from various investors in the Web3 space

BY BESSIE LIU / MARCH 18, 2024 06:00 PM



The IGF has a cap size of \$100 million. The fund has already raised \$30 million from its first close and secured anchor commitments from Alpha Wave Ventures, part of the global investment company Alpha Wave Global, and several other investors.

The IGF reflects increasing momentum in the development of Web3 games. With [Sony and Microsoft recently filing patents](#) pointing to blockchain technology gaming integrations and [France's NFT gaming law](#), NFT based games are continuing to receive attention as a logical use case for blockchain technology, allowing gamers to own virtual game currencies and in-game assets. The IGF enables game developers to access the financial resources and tools to build the future of Web3 games.

Written by Michael Bacina, Steven Pettigrove and Luke Misthos