

Article Information

Authors: Barbara Vrettos, Jade McGlynn, Michael Bacina

Service: Blockchain, FinTech

Sector: Financial Services, IT, IT & Telecommunications

Blockchain Bites: Australia as a Technology and Finance Hub, BTC Markets ISO 27001 certified, Roll ransacked by rogue hacker, India indicates no blanket ban on digital assets coming

Michael Bacina, Barbara Vrettos and Jade McGlynn of the Piper Alderman Blockchain Group bring you the latest legal, regulatory and project updates in Blockchain and Digital Law.

Positioning Australia as a Technology and Finance Hub

Senator Bragg has [unveiled exciting news](#) that the Senate recently approved an expansion of the scope and length of the [FinTech Select Committee on RegTech and FinTech](#) to capitalise on the technology opportunities available to Australia.

Coming with a rebrand to the '*Select Committee on Australia as a Technology and Financial Centre*' the expansion gives the Committee until October 2021 to prepare its report. Senator Bragg's announcement singles out [opportunities in](#):

1. Cryptocurrency and digital assets;
2. Neobanking, and
3. Instances of corporate law holding back investment.

Senator Bragg said:

I fully expect the Committee to focus on removing more barriers to Australian growth as a technology and finance centre.

and:

This is a golden opportunity to bolster Australia's economic growth and I want to ensure we take full advantage of it.

After already publishing [two issues papers](#), receiving [217 submissions](#) and holding [13 days of public hearings](#) it is clear that the Senate Committee's focus has harnessed the key issues raised in the hearings, that Australia needs work to improve it's position "[as a global financial and technology hub](#)" and to stop businesses leaving Australia and taking their innovation and jobs with them.

The Senate Committee will deliver a further report in April about the existing mandate on RegTech and FinTech which may reveal further factors influencing the decision to expand the scope of the Committee.

We welcome the increased scope and specific identification of the challenges facing Australia in becoming a hub for digital assets and blockchain and look forward to the Committee's work and report

BTC Markets ISO 27001 certified

The [ISO 27001 Information Security Management Systems Standard](#) sets the bar for the best practice information security management. [BTC Markets](#), one of Australia's largest digital currency exchanges, has [announced](#) it been awarded the certification by a world leading standards body, the [British Standards Institution](#).

BTC Markets [reports](#):

The ISO 27001 certificate is highly sought-after by banks and other institutions within the financial services sector. It signifies that the entity in question has a robust information security management system that meets the highest of industry standards at a global level.

Having transacted over AUD\$14.1 billion in trades for over 300,000 customers, security and risk management is at the forefront of mind for BTC Markets. The ISO standard aims to protect against the risks of "[fraud; espionage; sabotage; and natural causes](#)" via controls implemented in the business. [CoinSpot](#), another of Australia's top exchanges by trading volume, received ISO 27001 accreditation a year ago.

A certification of this level demonstrates the increasing sophistication of digital currency exchanges which need to mitigate against the risk they face, including scams and hacks. The rise of digital currency exchange certification is only a further

indicator of confidence in the digital asset space, which we hope this will continue to dispel the myths and critiques about scams that often are raised by media.

Roll ransacked by rogue hacker

Social token platform [Roll](#), built to be an “[infrastructure for social money](#)” has been the subject of a USD\$5.7 million attack. The platform sought to host a range of tokens to allow “[creatives to launch and manage their own Ethereum blockchain based money systems](#)”. The hack has diminished the value of many of the tokens hosted.

The hacker reportedly gained access to the digital asset management platform [MyCrypto's](#) private keys for the Roll hot wallet. This means that the hacker could transact the tokens within that wallet at will, which they did and the tokens were swiftly sold. The hacker then quickly moved those funds into a mixer, which is a [platform that obscures digital currency transactions](#) often used by hackers to make it harder (but not impossible) to track transactions.

This kind of hack is a key risk of projects which rely upon ‘hot wallets’ – named as the private keys for the wallets are able to be obtained via internet access – rather than a ‘cold wallet’ which stores private keys entirely offline. Cold wallets are considerably more secure as it is inherently harder to obtain a private key which is not accessible via the internet.

The hacker is reported to have stolen “[11 different social tokens, including \\$WHALE, \\$RARE, and \\$PICA](#)” which subsequently plummeted in value. [Coin Telegraph reported](#) that:

As a result of the attack, the market cap of social tokens on the platform fell from \$1.5 billion as of March 12 to \$365 million ...

Roll has announced the creation of a \$500,000 fund to help the creators affected by the hack but has not yet [announced](#) a refund to users despite acknowledging that “[the attacker has already sold all the tokens.](#)”

Creator of the \$WHALE token [reported](#) that 2.17% of the token was compromised but the rest of the tokens are fully secured in cold storage.

This is an unfortunate lesson in security and that hot wallets, by their very nature, are more susceptible to hacks compared to sensible cold storage solutions.

India indicates no blanket ban on digital assets coming

[India's agenda to ban private digital currencies and provide a framework for its own central bank digital currency](#) has caused alarm, being called “[one of the worlds strictest policies against cryptocurrencies](#)” and calls that India is going to “[miss the bus](#)” on the opportunities posted by digital assets. Under the proposed Bill, anyone trading or even holding digital assets may find themselves subject to fines, [perhaps even jail terms](#).

While further details have not been shared, a government official is [now walking back earlier comments](#) to reassure digital asset users that “*the government was not going to block all options regarding cryptocurrency*” and that experimentation with digital assets is likely to remain acceptable.

Finance Minister, Nirmala Sitharaman [commented](#):

We are very clear that we are not shutting all options off. We will allow a certain amount of window for people to use, so that experiments in blockchain, bitcoin, whatever you may want to call it, the cryptocurrency experiments and fintech which depends on such experiments will have that window of element for them; they are not going to shut it all off.

While hesitant on digital currencies, the Indian government sought to clarify its positive intentions for Blockchain technology.

The Finance minister [added that](#):

On fintech, on blockchain, there is a lot of work going on in India and we would certainly encourage them.

It is unclear what holdings, individuals or companies will be inside or outside the ban's ‘window’. If the bill passes any individuals trading or holding digital assets in India will need to actively review the scope of the law as the [6 month clock](#)

will begin for those captured to liquidate their assets.

The Indian government's approach of "blockchain not Bitcoin" remains one of the most skeptical approaches of a democratic government and it remains to be seen whether it is informed by a lack of understanding, or a fear of disruption to monetary sovereignty, given the popularity of electronic payments in a country which is still [heavily cash dependent](#).