Article Information

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

Blockchain Bites: Blockchain Australia becomes DECA, Australia bans crypto payments to gambling sites, Hong Kong greenlights 11 crypto licence applicants (for now), EU criticises crypto privacy tools

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

Embracing the Digital Future: Blockchain Australia becomes DECA

Blockchain Australia, Australia's preeminent Web3 professional group, has announced it is rebranding to the Digital Economy Council Australia (**DECA**). This rebrand, unveiled during the highly anticipated Blockchain Week 2024, underscores the organisation's commitment to a broader spectrum of digital innovations.

The announcement was made by Amy-Rose Goodey, the newly appointed Managing Director of DECA (previously serving as COO of Blockchain Australia), during her opening speech at the annual Blockchain Week 2024 event held in Sydney.

Commenting on the rebranding, Ms. Goodey emphasised that the organisation needed to broaden its scope to be more inclusive, addressing the rapidly evolving demands of the digital economy.

> The term 'blockchain', while central to our inception and growth, now represents only a segment of the vast digital ecosystem in which we operate. Our repositioning to the Digital Economy Council of Australia marks an important re-alignment for our organisation, to one that encompasses all verticals of the digital economy.

DECA aims to encapsulate the diverse and expanding range of digital technologies transforming Australia. Its new identity signals an inclusive approach, focusing on fostering growth and collaboration across various facets of the digital economy.

The rebranding announcement was strategically timed with Blockchain Week, an event that has grown to become a cornerstone of the digital technology calendar in Australia. This year's event, held from 11-14 June, drew industry leaders, policymakers, and innovators from around the globe and marks the tenth year of the organisation's founding.

Written by Steven Pettigrove and Luke Misthos

All crypto bets are off: Australia bans crypto payments to gambling sites

On 11 June 2024, the Australian government implemented a sweeping new ban on most regulated interactive gambling services (e.g. interactive wagering services) accepting digital currency and credit cards payments. The ban follows amendments to the *Interactive Gambling Act 2001* (**Act**) enacted in December last year, which make it a criminal offence for interactive wagering services to accept credit card and digital currency payments punishable by criminal and civil penalties.

This means Australians will no longer be able to use their credit cards or digital currency (such as Bitcoin) to place bets online, as the government moves to tighten industry regulations to "stamp out harms" caused by gambling.

If an online gambling platform breaches the prohibition, it could face severe criminal or civil liabilities. They may also commit a separate offence in respect of each day during which the contravention continues, which could result in the imposition of significant cumulative penalties.

Furthermore, these offences do not require the interactive wagering service to be physically based in Australia – which basically means it has extraterritorial effect. The Act offers only limited defences to interactive wagering services.

The new amendments also pose risks to digital currency exchanges (**DCEs**). While the Act does not directly prohibit DCEs from facilitating digital currency payments to interactive wagering services, DCEs could become complicit in the commission of an offence by facilitating digital currency transfers to interactive wagering services (e.g. by dealing in the instrument or proceeds of crime). DCEs also risk breaching anti-money laundering and counter-terrorism financing (**AML/CTF**) obligations by facilitating crypto payments to interactive wagering services.

Crypto users are known to like a punt and in recent years there has been a proliferation of gambling websites which accept crypto payments. On 11 January 2024, users of the betting platform Polymarket gambled USD$12 million on the outcome of Bitcoin Spot ETF approvals. Similar bets on ETH ETFs approvals reached USD$2.4 million in March.

Given the serious financial and reputational consequences of breaching criminal and AML/CTF laws, it is important for both online gambling services and DCEs to assess their payments offerings and identify steps to mitigate legal risks arising from the new prohibition on credit and crypto payments.

The genesis of the new prohibitions was the Parliamentary Joint Committee on Corporations and Financial Services' 2021 inquiry into Regulation of the use of financial services such as credit cards and digital wallets for online gambling. The policy rationale for restricting the use of credit to gamble are well known and new restrictions on credit cards appear to be targeted at gaps in the existing law. The focus on digital currency payments appears to have come later with little by way of published policy analysis or debate supporting the ban. In any event, the prohibition on crypto payments is now law of the land Downunder for interactive wagering services, so all crypto bets are off for the foreseeable future.

Written by Steven Pettigrove and Jake Huang

Hong Kong greenlights 11 crypto licence applicants to continue trading (for now)

This week Hong Kong's Securities and Futures Commission (**SFC**) published a list of 11 virtual asset trading platforms (**VATPs**) applicants who can continue to operate under Hong Kong VATP regulatory regime pending determination of their licence applications. According to the SFC's website, these applicants are now "deemed to be licensed" as of 1 June 2024.

Major exchanges such as Crypto.com are among this list of 11, which can now continue to operate in Hong Kong pending formal decisions on their licence applications. Exchanges were given a 1 June deadline to submit an application, otherwise they must close down business in Hong Kong, and stop actively marketing their services to Hong Kong investors.

The SFC emphasised that applicants who are "deemed-to-be-licensed" have not yet been formally approved:

> All VATP applicants on this list are NOT licensed by the SFC, and may NOT be in compliance with the SFC's requirements. It should also be noted that the SFC has NOT formally licensed the deemed-to-be-licensed VATP applicants.

The SFC clarified its purpose of publishing the list is:

> to enable any member of the public to ascertain whether a virtual asset trading platform has made untrue or misleading misrepresentations regarding its licence application status with the SFC.

It also said that VATP applicants which appear on this list may not eventually be granted licences. SFC may update the list at any time if:

1. licence applications have been returned by the SFC due to them being incomplete and/or having unresolved

fundamental issues; and
2. licence applications have been refused by the SFC or withdrawn by the VATP applicants.

It was reported that the conditional approval comes as a relief to many industry watchers one week after several other major global exchanges withdrew their applications from consideration, which led observers to question whether Hong Kong would offer a hospitable environment to cryptoasset firms. So far, only two VAPTs have received full approval from the SFC – being OSL Exchange and HashKey Exchange.

In the past two years Hong Kong has taken significant strides towards regaining Asia's crypto crown. Notable efforts by the Hong Kong government include establishing the VATP regulatory framework and formulating guidance on asset tokenisation.

The SFC's comprehensive regulatory framework and world-renowned financial regulators have been held up by many observers as an example of a regulatory ecosystem that could facilitate the growth of a mature crypto industry in Asia. The latest licensing developments however underscore some of the challenges that many of exchanges will face in transitioning their business to new licensing frameworks being developed around the world.

Written by Steven Pettigrove and Jake Huang

Crypto's double-edged sword: EU criticises crypto privacy tools

The EU Innovation Hub, a collaborative venture involving various European Union agencies and member states, recently unveiled its first ever report on encryption. The report spotlights the "dual-use" nature of cryptographic technologies, underscoring their potential for both privacy protection and exploitation by bad actors.

In the digital realm, encryption has applications for privacy, and also poses a potential threat to collective security by concealing financial crime and other threats. The dichotomy between privacy and security in technology has been a battleground since the 1990s when the "encryption/crypto war" started, noting that but crypto referred to cryptography generally and not cryptocurrency specifically.

Cryptocurrencies are reliant on cryptography for their core security, including storage, mining, validation, and transfers and for privacy coins encryption protects the privacy of those using them from easy observation. The technology is neutral and may be used for good of illicit purposes, and the report highlights the concerns around illicit use of privacy coins, mixers, and layer-2 platforms, which can obscure the linear visibility of transactions on the blockchain. The report contends that these privacy-enhancing applications of blockchain technology can assist in facilitating money laundering. It should of course be noted that the amount of illicit use involving crypto assets is vastly lower than that in the cash economy and is more easily traced.

The controversial mixer 'Tornado Cash' recently came under scrutiny again when its developer, Alexey Pertsev, was sentenced to over five years in jail by a Dutch court. The court ruled that the platform, which allows users to exchange tokens while concealing wallet addresses, was created for money laundering purposes. This verdict was handed down despite Tornado Cash being a non-custodial crypto mixing protocol, which implies it never assumes control of the funds processed through it. The service has been caught up in a broader crackdown on mixing services led by US law enforcement.

The report also expressed concerns with privacy coins (e.g., Monero) which have privacy mechanisms built into their protocols, concealing the identities of the sender, receiver, and the actual amount being sent. Also in the firing line are layer-2 solutions such as the Lightning Network, which the report stated could be misused by criminals to make payments without revealing the times and amounts of transactions. The report also foreshadowed that new wallet encryption schemes may further complicate lawful access by law enforcement.

Following the publishing of the report, crypto enthusiasts took to social media to highlight comparisons to other technologies with good or bad applications:

Bitcoin News · Jun 11
@BitcoinNewsCom · **Follow**
NEW: "#Bitcoin ⚡ Lightning Network might be abused by criminals and create problems for law enforcement investigations," says EU Innovation Hub for Internal Security in their First Report on Encryption.

Henry Scavacini(BTC FAM)
@Scavacini777 · **Follow**

Fiat is abused and used by criminals much more than anything.

So are g-ns and hammers,

So are cars and dogs, should We ban all this too?

10:50 PM · Jun 11, 2024

7 Reply Share

Read more on X

Coincidentally, France's Autorité des Marchés Financiers (AMF) also warned in a report that crypto remains a high risk for money laundering due to its popularity, cross-border nature, and the anonymity provided by platforms like mixers, echoing the sentiment of the EU Innovation Hub but it appears from a translation of the report that it focuses mainly on the

theoretical risks of illicit use.

Despite regulators' increasing concerns over the privacy of our data, the status of financial data remains heavily contested. The importance balance between individual privacy and the fight against financial crime continues to play out in the cryptocurrency landscape and is clearly a hot topic in the EU (and the rest of the world). As regulators around the globe continue to grapple with these issues, a new wave of innovators is attempting to thread the needle by developing novel applications which embrace zero knowledge proofs and related technologies to preserve user privacy while curbing financial crime.

Written by Steven Pettigrove, Michael Bacina and Luke Higgins