Article Information

Authors: Steven Pettigrove, Jade McGlynn, Jordan Markezic, Luke Misthos, Michael Bacina
Service: Blockchain, FinTech
Sector: Financial Services, IT & Telecommunications

Blockchain Bites: Second bipartisan crypto bill, Tornado cash, RBA's CBDC announcement, Voyager to return US$270M to customers, Alexander Vinnik extradited

Michael Bacina, Steven Pettigrove, Jade McGlynn, Luke Misthos and Jordan Markezic of the Piper Alderman Blockchain Group bring you the latest legal, regulatory and project updates in Blockchain and Digital Law.

Second bipartisan crypto bill released

Following the Department of Justice (**DOJ**) and Securities and Exchange Commission (**SEC**) announcement of enforcement action against a former Coinbase employee, crypto industry leaders and participants criticised regulators' 'regulation by enforcement' approach.

Noting these views in the crypto community, a bipartisan group of Senators introduced the Digital Commodities Consumer Protection Act 2022 (**DCCPA**) which gives the Commodity Futures Trading Commission (**CFTC**) the exclusive jurisdiction to regulate 'digital commodity' trading. Importantly, popular cryptocurrencies such as Bitcoin and Ether were expressly defined as digital commodities.

A key DCCPA supporter, Senator John Boozman, described the current crypto regulatory environment as a 'patchwork of regulations at the state level.' The DCCPA clearly intends to resolve that patchwork, with Senator Debbie Stabenow commenting:

> *closing regulatory gaps and requiring that these markets operate under straightforward rules that protect customers and keep our financial system safe.*

The Bill provides a definition of digital commodity that covers fungible digital forms of personal property that can be possessed and transferred from person-to-person without necessary reliance on an intermediary. The Bill also excludes certain financial instruments including securities, as well as amending the definition of a commodity in the *Commodity Exchange Act* to include a digital commodity.

The Bill also introduces novel categories of registration including through a digital commodity broker or custodian or through a digital commodity trading facility and associated persons of digital commodity dealers. The Bill does clearly state that mining activity alone is insufficient to trigger registration as a digital commodity platform.

Critically, section 3 of the Bill grants the CFTC the exclusive jurisdiction over digital commodity trades, save for transactions in which a merchant or consumer is using a digital commodity solely for the purchase or sale of a good or service. The Bill also purports to prohibit fraud with respect to any digital commodity trade.

Section 4 of the Bill deals with digital commodity platforms. Pursuant to proposed subsection (a), any entity that is acting as a digital commodity platform must register with the CFTC in one or more of the applicable categories: i) digital commodity broker; ii) digital commodity dealer; and iii) digital commodity trading facility.

Proposed subsection (b) of Section 4 also provides core principles for digital commodity platforms. They generally require

digital commodity platforms to comply with all applicable core principles, which are designed to protect customers and the integrity of the digital commodity marketplace. There are two primary obligations placed upon digital commodity platforms:

1. Digital commodity trading facilities are only permitted to facilitate transactions that are not readily susceptible to manipulation, and are required to provide a competitive, open and efficient market for executing transactions.
2. Digital commodity dealers and brokers are required to establish fair and objective prices; and keep records of all digital commodity transactions and provide information to the CFTC upon requisition. Importantly, the dealers and brokers are required to confirm with business conduct standards, and establish risk management systems.

Proposed subsections (c)-(o) of section 4 also explicitly deal with: rules governing margined or leveraged trading, contract listings, rules and rule amendments for trading facilities, product listing for digital commodity brokers and dealers, customer protections, energy consumption publication and examinations, general prohibitions on fraud, deception and manipulation, self-regulation, dual registration, education and outreach, as well as preemption of State Laws.

The Bill also provides additional amendments in proposed Section 5, notably including an anti-money laundering obligation in accordance with the *Bank Secrecy Act*. The Bill provides that it will apply to registrants until such time as the date of effectiveness of the final rule requiring registration under the Act accrues.

With a range of legislation being introduced to the US Congress, it might be that we see definitions becoming law in the US sooner rather than later.

Tornado Cash: can Smart Contracts weather a sanction storm?

The US Treasury has announced it has sanctioned the collection of smart contracts known as Tornado Cash. In 2018, the Office of Foreign Asset Control (**OFAC**) indicated they were considering sanctioning digital wallet addresses and now 4 years later OFAC have moved to include the Tornado Cash wallet addresses in the Specially Designated Nationals (**SDN**) list.

The list names both the Tornado Cash website and a raft of wallet addresses, meaning that US citizens and residents will be breaking the law should they interact with those addresses. Disturbingly, some of the addresses were those accepting donations for ongoing development of Tornado Cash and would appear to have no possible connection whatsoever with illicit activity. As one researcher put it seems to include *"every (Tornado Cash)-related wallet they could find"*.

Transactions on the Ethereum public blockchain are pseudonymous, and transactions are entirely traceable, but it is not easy to identify the owner of an individual wallet. As more wallet addresses are connected to identities through services such as Chainalysis and Elliptic, and technology such as soulbound tokens bring more identification to wallets, that traceability becomes greater.

Tornado Cash is a mixing service which enables the law-abiding and criminals alike to enjoy privacy over their transactions. It is non-custodial, meaning no third party takes control over funds, but rather transfers are placed into a pool and payments are made from that pool, breaking the link between any specific transfers of digital currency.

Tornado Cash smart contracts (known collectively as a Dapp, or decentralised application) have been used by a number of high profile ransomware and hacking groups to obscure the trail of stolen funds and ransoms. That usage is reportedly in excess of US$7BN, including the North Korean state-sponsored hacking group Lazarus putting over USD$96M through Tornado Cash after hacking the Harmony Bridge in June of this year, and criminals allegedly used Tornado Cash to obscure the destination of US$7.8M from the Noman Bridge hack last week. It is possible to see this because of the traceable nature of digital currency transactions on public ledgers, and not due to any particular investigatory powers of any regulators.

The developers of Tornado Cash announced in April that there were using a Chainalysis oracle to block OFAC sanctioned addresses from accessing the Dapp, saying:

> *Maintaining financial privacy is essential to preserving our freedom, however, it should not come at the cost of non-compliance.*

This seems to not be enough, but the move by OFAC raises a series of questions (many of which were raised in 2018 when the announcement first was made) such as:

- Can OFAC even sanction a piece of code? Some in the US are already arguing code is "speech" and protected under the US Bill of Rights;

- If an address is improperly added to the list, a review process exists, but requires the applicant to disclose their identity, and will likely lead to the applicant being investigated.
- How will the sanctions be enforced in a permissionless blockchain world where OFAC isn't able to turn off smart contracts or block at a technology level specific wallet addresses?
- What level of association with the sanctioned addresses will amount to dealing with 'tainted' digital currency?
- How will DeFi addresses which interact with Tornado Cash be dealt with?
- If tainted ETH or an ERC-20 is deposited into a liquidity pool with billions of dollars of other coins – are those coins or any associated pairs now tainted as well?
- what about a spray attack where tainted ETH is sent to addresses (which can't refuse the transactions) and create unintended breaches?
- Do miners and node operators now have obligations (in the US at least) to block these addresses?
- Could crypto which once touched Tornado Cash be forever marked as dirty?
- What does this mean for other privacy enabling tools and entirely legitimate privacy protection?

Increasing regulation over crypto-assets will lead to more collisions between fundamental blockchain features like unstoppable smart contracts, and regulation designed for a centralised world being applied to a decentralised world. Blockchain businesses in the meantime need to be carefully advised to meet their compliance obligations. The broader debate of privacy as a human right should be taken up by the legislature or courts to give clarity on the matter.

Reserve Bank of Australia to launch CBDC pilot

The Reserve Bank of Australia (**RBA**) has announced it is working with the Digital Finance Cooperative Research Centre (**DFCRC**) to launch a limited-scale CBDC pilot that will operate in a ring-fenced environment and involve a pilot CBDC that is a real claim on the Reserve Bank.

The RBA has identified a 'gap' between Australia's well-functioning payment and settlement system, and the use cases and potential economic benefits of CBDCs. Innovative use cases and business models that may benefit from the introduction of a CBDC will be reviewed as part of the project.

In a media release, the RBA and DFCRC indicate further exploration in the space:

> *The project will also be an opportunity to further understanding some of the technological, legal and regulatory considerations associated with a CBDC.*

The project, which is expected to take a year to complete, will call on industry participants to develop specific use cases that demonstrate how a CBDC can be used in Australia to provide innovative and value-added payment and settlement services to households and businesses.

A range of different interested industry participants will be considered as part of the pilot based on their potential to provide insight to the project. Once concluded, a findings report that assesses the various use cases will be published. The RBA has undertaken 'considerable research' into the feasibility and technical design of a CBDC with particular attention being given to innovative technology such as distributed ledger technology.

Dr. Andreas Furche, CEO of the DFCRC affirmed the likelihood of a CBDC in Australia is dependent on the economic benefits it could provide:

> *CBDC is no longer a question of technological feasibility. The key research questions now are what economic benefits a CBDC could enable, and how it could be designed to maximise those benefits.*

It's been two years since the RBA's Australian Senate FinTech & RegTech Inquiry Submission confirmed that its internal 'Innovation Lab', established in late 2018, had been considering the merits of a CBDC in the context of the RBA's responsibilities.

A year later, in September 2021, the RBA posted a job advertisement for a CBDC team to research whether there is a case for CBDC in Australia. It appears now that the working group has decided there is enough merit in CBDCs, and the underlying technology, to welcome submissions from interested participants.

Australia will join the United States, France, Cambodia, England, United Arab Emirates, Singapore and China as one of the countries exploring and testing CBDCs as a way to innovate the financial space.

CBDCs can provide notable benefits to the Australian economy, the blockchain-based technology allows for more efficient and cost-effective cross-border payments, transaction transparency and innovation such as being able to establish a programmable payment system.

UK Law Commission recommends recognition of digital assets as property

In a consultation paper issued last week, the Law Commission of England and Wales (the **Commission**) recommended that the British Government expand the scope of recognition and legal protections currently in place for digital assets, including cryptocurrencies and non-fungible tokens (**NFTs**).

Commenting on the new proposals, Professor Sarah Green, the Law Commissioner for Commercial and Common Law, said:

> *Digital assets such as NFTs and other crypto-tokens have evolved and proliferated at great speed, so it's vital that our laws are adaptable enough to be able to accommodate them.*

The Commission's paper argues that digital assets do not fit neatly into the existing categories of personal property (things in possession and things in action) and recommends the implementation of a third category of personal property called "data objects", which could include a wide variety of digital assets including cryptocurrencies and NFTs.

The Commission's key proposals include:

1. providing explicit recognition of a distinct category of personal property known as "data objects" that is better able to accommodate the unique features of digital assets;
2. options on how this third category of "data objects" could be developed and implemented under the current law;
3. clarifying the law around ownership and control of digital assets; and
4. clarifying the law around transfers and transactions involving digital assets.

The Commission's proposals are intended to ensure that the law remains flexible and progressive towards new and emerging technologies. Professor Green noted:

> *It's important that we focus on developing the right legal foundations to support these emerging technologies, rather than rushing to impose structures that could stifle their development. By clarifying the law, England and Wales could reap the potential rewards and position itself as a global hub for digital assets.*

The Commission's recommendations are a positive step in developing a strong legal framework to support ownership of digital assets and further innovation in this space. If adopted, the Commission's proposals could pave the way for other jurisdictions to follow suit and recognise digital assets as a unique form of property.

The deadline for public responses to the Commission's consultation paper is 4 November 2022.

Bankrupt crypto firm Voyager to return USD$270M in customer cash

Voyager Digital Holdings Inc, a cryptocurrency brokerage firm has received approval from a New York Bankruptcy court to return USD$270 million in customer cash leaving a significant portion of client assets still frozen.

Judge Michael Wiles of the U.S. Bankruptcy Court in New York ruled that the recently bankrupt firm made out "a sufficient basis" for its argument that customers should not be allowed access to the custodial account held at New York-based Metropolitan Commercial Bank following Voyager filing for bankruptcy.

The Wall Street Journal said:-

> *Voyager is looking for ways to pay back customers, its largest creditor base, through a restructuring that turns them into owners or a possible sale of the business*

While Voyager has filed for bankruptcy and is in the process of assessing how it can reunite customers with their deposits (both crypto and cash based), the firm is allegedly not in a position to honour the volume of withdrawal requests being made.

Voyager held approximately USD$270 million in cash in their bank account when they filed for bankruptcy, with close to $1.3 billion in digital assets. These volume of digital assets means there will be much more work done before customers can find out what they will receive, which in part justified the Court finding that only cash withdrawal requests, which are presently reconcilable, should be honoured.

According to Voyager, their motivation behind the resumption of a proportion of some withdrawals is to:

> *to avoid material(ly) harming customer moral*

This may be too late given redemptions have been frozen for some time. This serves as a reminder of pre-emptive planning of client custody for digital currency exchanges and the importance of client funds not being used for business purposes. As regulation of digital currency exchanges draws nearer, standards seen in the traditional financial world will continue to be applied to digital currency exchanges.

FTX, together with trading firm Alameda Research, continues to press an offer to buy most of Voyager's digital assets and digital asset loans as a way for Voyager customers to move forward without waiting for the bankruptcy process to slowly move through the Courts. Voyager has resisted what they call a "low ball bid" for the assets, but so far there seems to be no better offers coming forward.

Alexander Vinnik reportedly being extradited to US

Alexander Vinnik – a Russian national accused of running BTC-e, a multibillion-dollar cryptocurrency exchange implicated in the MtGox hack – has been reportedly extradited from Greece and is currently in transit to the US, according to his legal representative, Frédéric Bélot.

In 2017, Vinnik was arrested in Greece and extradited to France. He was then sentenced to five years in prison in 2020 for money laundering offences. Critically, Vinnik had also been under indictment in the US since 2017, with the US and Russia filing duelling extradition requests from Greece.

It is alleged that BTC-e profited from various hacking and extortion schemes, including doing business with ransomware gangs, drug dealers and identity thieves, according to the Justice Department.

Vinnik is facing charges in the US Northern District Court of California for allegedly engaging in money laundering activities, as well as operating an unlicensed money services business in the US. The extradition demonstrates US regulatory authorities and prosecutors propensity to pursue notable Russian criminals accused or suspected of cybercrime.

According to CNN, Vinnik's extradition demonstrates:

> *how US prosecutors have continued to pursue high-profile Russian cybercrime suspects at a time when any faint hopes of cooperation with Moscow on the issue have dimmed.*

According to the Justice Department, BTC-e received in excess of US$4 billion worth of bitcoin while it was trading. The US Treasury levied a US$110M fine against the exchange for allegedly willfully violating US anti-money laundering laws, as well as imposing an individual fine of US$12M against Vinnik.