Article Information

Author: Michael Bacina, Steven Pettigrove
Service: Blockchain, FinTech
Sector: Financial Services, IT & Telecommunications

Blockchain Bites: FTX reports additional asset recoveries and past control failures, EU approves new AML/CTF rules for digital assets, BoE hiring for Digital Pound Development, Germany wilkommens legislation for blockchain based shares, Polygon Launches Use Case Collection, The End for Genesis Markets

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

FTX reports additional asset recoveries and past control failures

The US bankruptcy administrators of collapsed crypto-exchange FTX issued a report this week detailing widespread management and control failures at the exchange once led by Sam Bankman-Fried (**SBF)**. The administrators' lawyers also said in a hearing that they have recovered US$7.3 billion of "distributable assets".

In the report, the debtor entities, now led by veteran restructuring advisor John Ray III, said:

> *while the FTX Group's failure is novel in the unprecedented scale of harm it caused in a nascent industry, many of its root causes are familiar: hubris, incompetence, and greed.*

Ray filed the report in the US Bankruptcy Court for the District of Delaware. It contains damning details about FTX's alleged control failures.

1. *Lack of management and governance control*

The report states that management of the FTX Group was largely limited to a small group led by SBF and which included Nishad Singh and Gary Wang (who have already pled guilty to criminal charges).

According to the report:

> *These individuals, not long out of college and with no experience in risk management or running a business, controlled nearly every significant aspect of the FTX Group*

and

> *FTX Group lacked independent or experienced finance, accounting, human resources, information security, or cybersecurity personnel or leadership, and lacked any internal audit function whatsoever. Board oversight, moreover, was also effectively non-existent.*

Further, the company did not maintain an organizational structure nor a complete list of employees at the time of its bankruptcy filing.

2. *A lack of financial and accounting controls*

Ray says that the FTX Group did not have an appropriate accounting system noting that 56 entities did not produce financial statements of any kind and 35 entities used QuickBooks – an accounting software designed for small businesses and freelancers – as their accounting system.

The report further criticizes the firm's external accountants:

> *There is no evidence that the FTX Group ever performed an evaluation of whether its outside accountants were appropriate for their role given the scale and complexity of the FTX Group's business, or whether they possessed sufficient expertise to account for the wide array of products in which the FTX Group transacted*

Another issue cited in the report was the submission of expenses and invoices on Slack, which were then approved with emoji.

These informal, ephemeral messaging systems were used to procure approvals for transfers in the tens of millions of dollars, leaving only informal records of such transfers, or no records at all

3. *A lack of digital asset management, information security, and cybersecurity controls*

Ray alleges that FTX:

> *failed to implement basic, widely accepted security controls to protect crypto assets.*

The failure by FTX to enforce the simple security measure of multi-factor authentication (or MFA) among its staff and corporate infrastructure is particularly ironic, given that

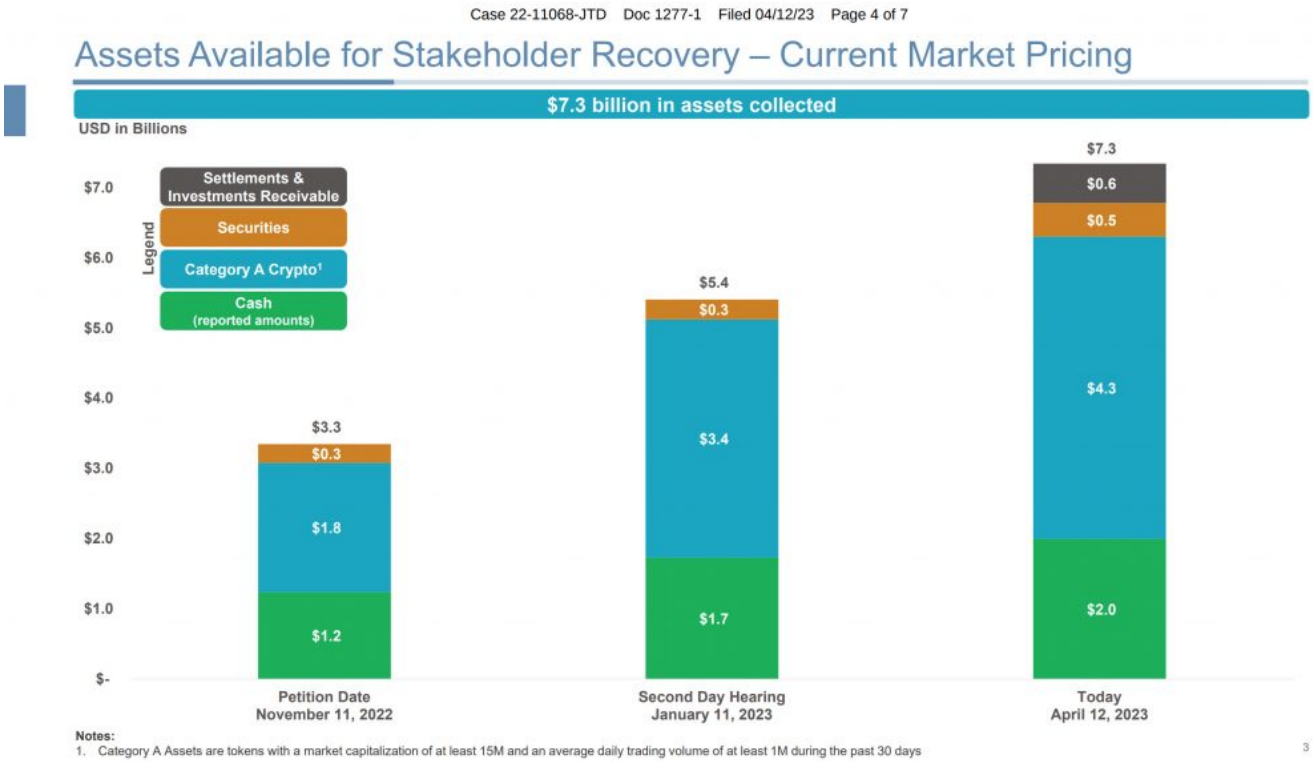
> *the FTX Group recommended that customers use MFA on their own accounts, and Bankman-Fried, via Twitter, publicly stressed the importance of…MFA, for crypto security*

The report further states that FTX Group did not have any mechanism to identify promptly if someone accessed the private keys of central exchange wallets holding hundreds of millions or billions of dollars in crypto assets. Due to the lack of such controls, Ray's team first learned of a US$ 3.5 billion breach of the exchange last November from Twitter.

On a more uplifting front, Ray's team has identified:

> *recovered and secured in cold storage over $1.4 billion in digital assets, and have identified an additional $1.7 billion in digital assets that they are in the process of recovering.*

At a hearing this week, the debtors' lawyers Sullivan & Cromwell said the total assets available for recovery now sit at US$7.3 billion, as shown in the chart below:



The bankruptcy administrators are targeting a preliminary restructuring plan by July and a final plan approved by the Court in the middle of 2024.

The additional recoveries by the US bankruptcy administrator will boost hopes of increased payouts to creditors of FTX Trading. The interim report nevertheless provides a depressing list of traditional control failures and mismanagement which are not exclusive or exceptional to cryptocurrency exchanges or start-ups. It increasingly appears that the spectacular collapse of FTX was largely due to these failures rather than crypto specific business risks.

EU approves new AML/CTF rules for digital assets

The EU is continuing to progress new anti-money laundering and counter-terrorist financing (**AML/CTF**) for digital assets, with parliamentary committees approving positions on three pieces of AML/CTF related legislation last week.

The draft legislation contains strict requirements on cryptoasset service providers (**CASPs**) to identify the users of unhosted wallets. Under the proposals, where a CASPs customers' transact with an unhosted wallet, the CASP would need to identify the counterparty behind the unhosted wallet for all transfers over a threshold of €1,000.

This is a step further to a similar provisional deal struck by the EU Partliament and EU council last July, which only requires CASP to verify whether the un-hosted wallet is effectively owned or controlled by the customer.

CASPs would be forbidden under the rules from processing transactions greater than €1,000 if they cannot identify a counterparty, or unless another regulated CASP is counterparty to the transfer.

The Rules also provides provisions on customer due diligence process, transparency of beneficial owners, the use of anonymous transaction mechanisms including crypto assets and crowdfunding platforms and a prohibition on 'golden' passports/visas which previously enabled individuals to gain passports/visa via investment programs.

6th Anti-Money Laundering directive

The proposal introduces safeguards such as establishing a Financial Intelligence Unit (**FIU)** in each member state and having a Fundamental Rights Officer in every FIU to prevent, report and address ML/TF issues. It aims at increasing access to quality data by national authorities and regulatory bodies by mandating sharing of information between FIUs and encouraging cooperation with AMLA, Europol, Eurojust and the EU Public Prosecutor's office. The draft proposal ultimately looks to promote transparent, cross-border sharing of AML/CTF information across the EU.

Regulation establishing the European Anti-Money Laundering Authority

Described as the 'heart' of the legislative package, the proposed Anti-Money Laundering Authority (**AMLA**) has been

assigned supervisory and investigative powers to enforce compliance with AML/CTF measures. This new central authority is expected to ensure consistent enforcement of the new regulations and the MEPs have reflected their intention to further extend the AMLA's power to draw up lists of high-risk non-EU countries and mediate and settle disputes between national financial supervisors. The full extent of the power of AMLA will be determined during the negotiations between the Parliament and Council.

The EU Parliament is planning to commence negotiations on the full legislation following a confirmation during a plenary round scheduled in April.

Bank of England on a hiring spree for Digital Pound Development

The digital currency arm of the Bank of England is poised to grow with the announcement that the United Kingdom's Central Bank will be hiring as many as 30 new staff members to assist in developing a central bank digital currency (**CBDC**), months after the Federal Reserve Bank of New York launched its CBDC pilot.

The digital pound, also known as the 'digital sterling' or 'Britcoin', is to be denominated in sterling and function just like any other stablecoin, with its value pegged 1:1 to the price of sterling. According to the Bank of England, the digital pound will not be a cryptocurrency or a crypto asset, but will be proper digital money that is backed by the government.

The careers page of the Bank of England currently only lists two jobs that appear relevant to the digital pound, these being a Digital Pound Security Architect and a Digital pound Solution Architect, both added on 29 March 2023.

The hiring spree by the bank suggests a firm intention to build a substantial team responsible for effective integration of a CBDC into the United Kingdom's existing financial framework.

Several international and domestic financial institutions have started on a path to utilise the benefits that CBDCs can offer. Faster and cheaper transactions, enhanced security and more accurate data analytics, among other things, have led to a spike in CBDC adoption and research.

In New Zealand, the Reserve Bank is currently seeking public consultation on a NZ digital currency, in the United States the US Federal Reserve has released its CBDC insight and in Australia the Reserve Bank of Australia's CBDC pilot project is underway.

The future of currencies is looking more and more digital with mainstream adoption of CBDCs becoming seemingly inevitable but governments may need to take note of the concerns voiced regarding surveillance and tracking of citizens using CBDCs, the Digital Pound is expressly promised to provide privacy to users and not to let the government monitor what is being spent by holders, which would appear an essential element of any true digital money.

Germany wilkommens 'technology enabling' legislation for blockchain based shares

The German government is planning to introduce a 'Future Financing Act' to improve financing for future investments and to facilitate capital market access for startups, growth companies, and SMEs. The German government believes the Future Financing Act is necessary to strengthen the German capital market and increase its attractiveness to national and international companies and investors.

In particular, Germany plans to advance the digitalisation of the capital market in Germany by enabling companies to issue shares using blockchain technology. Rules already in place allowing the tokenisation of bonds and fund units will be extended to also capture 'normal' securities. Tokenisation is the current hot topic in the Web3 space, with many believing it to be one of the most compelling use cases. The Act also aims to improve the transferability of crypto assets, and reduce the formal/legal requirements of digitisation.

In December 2022, Germany's top regulator (**BaFin**) called for global regulation of the cryptocurrency industry to protect consumers, prevent money laundering, and preserve financial stability. The president of BaFin, Mark Branson, said a 'hands-off' approach would simply not work for the industry. The Future Financing Act is a positive move for Germany and hopefully marks a change in tone, given the German Minister of Finance's dim view of stable coins, calling them previously "wolf in sheep's clothing". Germany has been involved in the European Union's development of the Markets In Crypto Assets Regulation (**MiCA**), which aims to establish harmonised rules for crypto-assets at the European Union level.

The 'finalised' version of MiCA is expected sometime this year, with jurisdictions around the world sure to take inspiration from MiCA in their own legislative approaches. EU country-specific legislation like the Future Financing Act will likely be heavily influenced by MiCA.

The Act is also an interesting point when 'tech neutrality' is raised around legislation and regulation of digital assets.

Forward thinking jurisdictions are recognising that foundational technologies like blockchain require technology-enabling regulatory changes, and a 'technologically neutral' approach, which simply requires meeting rules, including through the use of technology (irrespective of what that technology is) will not be sufficient to harness the benefits which come from a technology like blockchain and distributed ledgers.

Polygon Launches Use Case Collection

Polygon has launched a community initiative to showcase a use case collection that aims to champion the best of what Web3 has to offer, aiming to show policymakers globally that the Web3 ecosystem is filled with blockchain-based applications that have a positive impact on the way in which we engage and transact with the new era of the Internet, and providing a valuable counterpoint to narratives that denigrate web3 and blockchain.

The showcase is seeking applications built or under construction, which positively influence and impact Internet users socially, sustainably, from an education perspective, from a Web3 social and Web3 gaming perspective, as well as enabling transactions involving payments, remittances and DeFi. The collection will gather all the use cases in one place, making it easy for the community, policymakers and regulators to locate, without getting lost in an ever-evolving space of new designs and emerging technologies.

This crowdsourcing initiative involves compiling a use case database, based on contributions from the community tapping into their knowledge of what is happening in the ecosystem. The database of new and innovative applications, which will be open-source, will emphasise how the Internet and web3 are being utilised fundamentally for good.

Contributions can be made via a Google form that will collect information about an application but also permit submitters to leave out certain information about the developers or operators of projects.

The database will be published when an unspecified number of use cases have been collected with an intention to further update the database regularly as more use cases are collected.

If you would like to contribute to this community initiative, see here.

The End for Genesis Markets

Genesis Market, one of the world's largest cybercrime facilitation websites and a marketplace for trading personal information, was home to almost 80 million sets of digital fingerprints for sale by 2023. Founded in 2017, and operating simultaneously on both the dark and open web, with a convenient user interface, Genesis Markets quickly gained popularity with online fraudsters as an all-in-one destination to purchase digital fingerprints. Login credentials, browser histories, autofill data, IP address and location information from the site has been leveraged by criminals to log into victim's accounts on platforms including PayPal, Amazon, online banking as well as numerous cryptocurrency exchanges.

Depending on the quality of the data, personal information was sold for as low as $1. In the 2021 hack of Electronic Arts, a $10 bot purchased from the Genesis Market allowed hackers access into EA's internal Slack account. Due to the association with profit motivated cybercriminals, the Genesis Market has been on the radar of numerous global authorities for some time.

Robert Jones, the director general of the National Economic Crime Centre at the NCA said:

> *It was a very sophisticated website, very easy to use…you just needed to be able to use a search engine, and then you could start committing crime.*

After a combined effort by law enforcement agencies across 17 countries, the 'enormous enabler of fraud' was officially shut down on Tuesday, 4 April 2023 with 120 people arrested globally. The global law enforcement crackdown was led by the US FBI, Dutch National Police, NCA in the UK, Australian Federal Police and other countries across Europe.

The NCA estimated that sales from Genesis Markets led to frauds involving over 2 million victims worldwide, with both individuals and companies impacted by way of fraud and ransomware attacks. The FBI believes that Genesis has generated at least USD$8.7M from illicit transactions of stolen data but also noted the possibility of total financial losses surpassing tens of millions of dollars.

The domains for Genesis Market have been seized by the FBI, with a takedown notice available on Genesis' normal login page, encouraging users to contact the authorities regarding information on the operators of the platform. So far, officials have identified approximately 59,000 users of the marketplace. While continued efforts are made to identify and detain the owners and administrators of the fallen Genesis Market, the seizure nevertheless marks a 'meaningful blow in the fight

against online identity theft’.