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: Unpacking the lessons earned from the Block Earner v ASIC judgment, AI deepfakes challenge KYC and internal controls, Satoshi Naka-who? UK High Court to determine who is Wright, Sim swapping FTX hackers prosecuted, Regulating DeFi as Critical Infrastructure

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.

Access all areas? Unpacking the lessons earned from the Block Earner v ASIC judgment

The judgment in ASIC v Web3 Ventures Pty Ltd (trading as Block Earner) was released today and has been greatly anticipated. The matter focused on two products offered by Block Earner, "Access" through which customers could send funds through to Aave and Compound, prominent DeFi lending protocols which compensate lenders for depositing cryptocurrency, and an "Earner" product, which paid users interest on crypto, and which was discontinued in November 2022. ASIC alleged that Block Earner should have obtained a financial services license to offer the Access and Earner products as it had created a facility through which a person makes a financial investment, that the products were an unregistered managed investment scheme or were a derivative.

Earner Product

The Earner product operated by users lending cryptocurrency to Block Earner in return for daily interest payments. Block Earner took that cryptocurrency and loaned it to others for higher interest rates than the users were being paid. Importantly Block Earner had published a statement that the yields on Earner were from "pooling customer funds and lending it to our trusted partners" and despite claiming this statement was a mistake the Court found the description reflected reality.

The Court noted the ongoing legal controversy as to whether cryptocurrency is property at common law but sought not to take a position on this question to address the financial services aspects of the case, but later the Court noted that if cryptocurrency is not property there is difficulty in the application of the current regulatory regime to the Earner product.

The Court found that the Earner product met the definition of a managed investment scheme in that:-

1. Investors contribute money or money's worth as consideration to acquire rights to benefits (being payment of interest) produced by the scheme;
2. The contributions are to be pooled, or used in a common enterprise to produce financial benefits, or benefits consisting of rights or interests in property, for the investors who hold interests in the scheme; and
3. The investors do not have day-to-day control over the operation of the scheme.

An acknowledgement in the terms of use that a customer did not "intend for Block Earner to use the loaned [crypto] to generate a financial benefit or act as an investment for you" was considered inconsistent with the representation that contributions would be pooled to generate a financial benefit for users.

The Court also found that the Earner product met the definition of a financial investment, which requires an investor gives money or money's worth to another person, and:

1. The other person uses the contribution to generate a financial return, or other benefit, for the investors; or
2. The investor intends that the contribution will be used to generate a financial return, or other benefit, for the investor (even if no return or benefit is in fact generated); or
3. The other person intends that the contribution will be used to generate a financial return, or other benefit, for the investor (even if no return or benefit is in fact generated).

And the investor has no day-to-day control over the use of the contribution.

The Court dismissed a suggestion that a "Risk Disclosure" and acknowledgements in the terms of use around investment would override an investor's intentions where a prominent representation is made to the contrary. Put another way, disclaimers must be consistent with advertising and representations.

Access Product

The Access product operated by means of an omnibus account, where users who wished to access DeFi protocols pooled their tokens with others and Block Earner's tokens and Block Earner passed the tokens though, tracked returns from the protocols and credited those returns to the customer's accounts.

In relation to the Access product, the Court rejected ASIC's argument that "pooling" in the omnibus account satisfied the pooling requirements of the managed investment scheme definition, finding that ASIC had not properly pleaded this claim in the first instance, but that even if the matter had been the subject of proper pleading, there was no evidence that the pooling itself generated benefits, such as individual account fees being saved, and there was no representations that the omnibus accounts were providing any benefit, such as saving on individual account fees.

The Access product was also found not to meet the definition of a financial investment given the pass-through nature of the service. The Court compared Block Earner to a 'broker' connecting users to smart contracts and referred to the notation in the definition of financial investment to the effect that the giving of money to a broker for the purpose of purchasing shares, in and of itself, is not a financial investment.

ASIC also failed to show the Access product met the definition of a derivative, as the Court accepted it was a "contract for the future provision of services" and so exempted from the definition in the *Corporations Act*. Had it not met that exemption, the Court would have found it was otherwise within the (extremely broad) definition of derivative.

Block Earner has sought to play down the decision, telling the Australian Financial Review that they had "moved on from the Earner product over a year ago".

ASIC Deputy Chair Sarah Court said:

> This important decision provides some clarity as to when crypto-backed products should be considered financial products which require licensing under the law.

Until the regulator or government provides a pathway to compliance for crypto products of this kind, the decision stands to highlight:

- The importance of extremely careful analysis and design of products involving crypto-assets, particularly those offering yields; and
- The need to ensure careful consideration and alignment of representations and ongoing marketing and terms and conditions.

By Michael Bacina and Steven Pettigrove

AI deepfakes challenge KYC and internal controls

From Barack Obama calling Donald Trump a "complete dipshit", Mark Zuckerberg bragging about having "total control of billions of people's stolen data", to explicit images circulating on X, artificial intelligence (**AI**) technologies are being used to create fake but convincing materials proliferating online challenging KYC and internal governance controls. Some call the technology "21st century's answer to Photoshopping", using AI to create ever more convincing fakes.

Now deepfakes are posing a serious threat to financial institutions and crypto exchanges. A website called OnlyFake offers

cheap services claiming to use AI "neural networks" and "generators" to create fake driver licenses and passports. Some claim they have successfully used the website to bypass Know-Your-Customer (**KYC**) checks on multiple crypto exchanges.

OnlyFake reportedly generates realistic fake driver's licenses and passports from 26 countries, including the United States, Canada, Britain, Australia and multiple European Union countries, and takes payment in multiple cryptocurrencies.

404 Media said that it successfully bypassed the KYC verification of a global crypto exchange using a fake photo of a British passport generated with the site, where the ID appeared to be laid on a bedsheet as if a picture of it was taken.

Other media reported stories of the site's users generating fake IDs to onboard leading crypto exchanges and financial services providers.

It is worrying that the site could possibly be used by crypto scammers and hackers as a power tool to fake documents and open exchange or bank accounts, protecting their real identity and making them more difficult to track. This will likely escalate the risks of money laundering, terrorism financing and sanction evasion, which already pose severe challenges to the technological capacity and resources of financial institutions and crypto firms.

It is reported that generating a fake document on OnlyFake takes less than a minute and costs $15 only. Users can upload their own photo or one chosen randomly from a "personal library of drops and not using a neural network".

Meanwhile, deepfakes could also pose challenges for internal governance and compliance controls with generative AI technologies used to manipulate employee identity to commit fraud. CNN reported this week that a finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call, according to Hong Kong police.

> (In the) multi-person video conference, it turns out that everyone [he saw] was fake,

senior superintendent Baron Chan Shun-ching told RTHK.

The case is apparently one of several where criminals have used AI to manipulate publicly available video to perpetuate fraud and scams.

With the ever-escalating challenges of deepfakes and AI technologies, traditional financial institutions and crypto firms alike should ensure that they adopt robust measures, whether internal or third-party controls, to identify and prevent fabricated ID documents. Along with tackling a constant wave of phishing attacks, corporates will also need to scrutinize their internal compliance controls, including payment authorities and procedures, to tackle the increasing risk of deepfakes intended to manipulate employees into parting with money and sensitive corporate information.

By Jake Huang and Steven Pettigrove

Satoshi Naka-who? UK High Court to determine who is Wright

The trial to determine whether Australian computer scientist Craig Wright is the pseudonymous creator of bitcoin, Satoshi Nakamoto, commences in the UK High Court this week.

Wright faces a claim by the Crypto Open Patent Alliance (COPA), a crypto and tech consortium. COPA contends that Wright's history of filing intellectual property lawsuits – which are predicated on his claim of being the inventor of the bitcoin cryptocurrency and Bitcoin network – has had the effect of "scaring" off developers from building and integrating projects onto the network. Accordingly, COPA is asking the court for a declaration that Wright is NOT Satoshi Nakamoto.

Any verdict will likely impact the many cases Wright is currently disputing against companies and developers that are, in his opinion, unlawfully using and adapting "his" software. The COPA claim is unique in the sense that its focus is on the identity issue, that is, who is Satoshi Nakamoto.

Wright first claimed to be Nakamoto sometime in late 2015, with a Wired article stating that Wright "either invented bitcoin or is a brilliant hoaxer who very badly wants us to believe he did". This article has since been updated to reflect the opinion of much of the cryptocurrency community and the media; that Wright's claims are false. Members of the community have taken to social media to share their views (in various humorous ways):

The identity of Satoshi Nakamoto has been a hotly debated and researched topic since the inception of the Bitcoin network in January of 2009, by enthusiasts and critics alike. Despite numerous claims and self-proclamations throughout the years (in addition to Wright's claims), no individual has conclusively proven to be the elusive genius. However, as time continues to pass, many believe that we will never unmask the enigmatic figure of Satoshi Nakamoto definitively.

Perhaps as a last-ditch effort to avoid legal costs, Wright extended a settlement offer to COPA in the form of an open letter in late January of this year. COPA was quick to offer a blistering retort via X that sent a clear message:

> Hard pass on that "settlement".
>
> Just like Craig Wright forges documents and doesn't quite tell the truth, his description of the settlement offer isn't quite accurate either – it comes with loopholes that would allow him to sue people all over again.

The settlement offer would also effectively require COPA to admit that Wright was Nakamoto. For now, the trial will unfold following COPA's rejection of the settlement offer, with the cryptocurrency world watching with baited breath.

Satoshi Nakamoto has long represented the principles of innovation, decentralisation, and the democratisation of finance. Yet, the prospect of Craig Wright assuming this revered mantle is often met with collective scepticism and disdain, partly due to the nature of Wright's activities over the past decade or so in seeking to claim ownership rights in the network. For many faithful disciples of bitcoin and decentralised technology, the idea of Wright donning the Satoshi crown is unappealing. While the identity of Satoshi may never be proven with certainty, one thing is evident: Wright is not the answer the community has been searching for.

By Luke Higgins and Steven Pettigrove

Call your lawyer! Sim swapping FTX hackers prosecuted

Prosecutors in the United States have charged three individuals with coordinating and executing a hack which saw over USD$400 million removed from FTX wallets the day after the defunct digital currency exchange filed for bankruptcy.

The devastating hack, which was initially thought to be under "suspicious circumstances", was allegedly orchestrated by three individuals using a SIM swap attack. This is where cyber criminals impersonate a victim (in this case an FTX employee) to take over control of their cellular service.

> On or about 11 November, 2022 **POWELL** instructed co-conspirators to execute a SIM swap of the cellular telephone account of an employee of Victim Company-1, which was maintained by AT&T.

Washington D.C. district court federal prosecutors charged Robert Powell, Carter Rohn and Emily Hernandez with carrying out the SIM-swap and related cyber attack.

While FTX is not named in the filing, a company known only as "Victim Company-1" suffered a SIM-swap attack and over USD$400 million worth of digital currency was siphoned from this company. Bloomberg later reported that the USD$400 million was that stolen from FTX, as mentioned in the court's filing.

> On or about November 11, 2022, a co-conspirator sent **HERNANDEZ** a fraudulent document with the PII [Personally Identifiable Information] of Victim Company 1's employee bearing **HERNANDEZ'**s photograph, which **HERNANDEZ** then used to impersonate that person at a mobile service provider store in Texas.

According to CNBC, the arrests came three months after the blockchain intelligence company Elliptic reported that 180,000 units of the cryptocurrency Ether had been dormant after being stolen in the FTX hack, but then was converted into Bitcoin in late September. The Ether by that point was worth $300 million.

If convicted, the hackers may be required to "forfeit to the United States, any property, real or personal, which constitutes or is derived from proceedings traceable to this offence" which includes the stolen virtual currency.

Whether the stolen funds are within the jurisdiction of the court or have been transferred to a third party, for example, is unclear. While there is no certainty that the stolen assets will ever be returned to FTX, which is currently under in Chapter 11 Bankruptcy, creditors have recently been buoyed by the news that eligible customers may be repaid in full. Meanwhile, the alleged sim swapping hackers might be in need of some old fashioned hard currency to call their lawyer.

By Michael Bacina and Luke Misthos

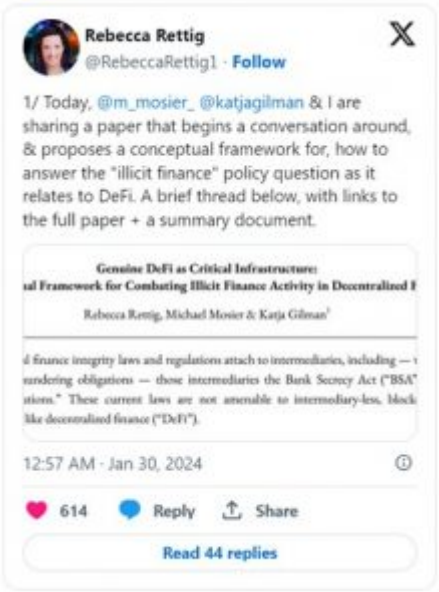
Future proof: Regulating DeFi as Critical Infrastructure

The rise of decentralised finance (**DeFi**), based on smart contract and peer to peer technologies, has highlighted reliance on existing centralized intermediaries in combating illicit financial activities including money laundering, terrorism financing and sanctions violations.

In their 2023 Synthesis Paper: Policies for Crypto-Assets, the Financial Stability Board (**FSB**) and the International Monetary Fund (**IMF**) stated:

> In the case of DeFi…the lack of intermediaries means that the traditional approach…in which AML/CTF requirements are imposed on a private sector entity and compliance is monitored by supervisors, cannot be applied.

In an attempt to address this issue, and recognising the need to balance the benefits of open systems and tackling financial crime, Polygon Labs' Rebecca Rettig, Chief Legal and Policy Officer, and Katja Gilman, Senior Lead in Public Policy, together with Michael Mosier, a former Acting Director of the Financial Crimes Enforcement Network (**FinCEN**) have published a proposal for Combating Illicit Finance Activity in Decentralized Finance.



The paper adopts the concept of 'Genuine DeFi' and proposes a framework to address illicit financial activity. The term "Genuine DeFi" is defined as:

A technological System comprised only of open source software – typically smart contracts where:

1. Users engage in financial transactions in a self-directed manner without intermediaries;
2. Users always maintain independent control over their assets through maintenance of the "private key"; and
3. All elements of the transaction occur on a permissionless blockchain network.

The proposal seeks to address 3 primary issues:

1. Not all DeFi systems are entirely decentralised and may involve points of centralisation that warrant application of existing rules;
2. Existing legal frameworks depend on identifiable intermediary entities and are not fit for purpose in regulating Genuine DeFi;
3. The nature of the risks of illicit financial activity differ between TradFi and DeFi. Main sources of risk in DeFi include cyber risks, system management risk and usage risk.

It then goes on to formulate a three part proposal:

1. Identifying "independent control" in on-chain software systems that do not constitute DeFi

The paper suggests that where a subject is identified as performing functions similar to traditional financial intermediaries, existing regulations may appropriately be applied. However, this assessment must be made on a case-by-case basis, taking into account the unique facts and circumstances of the protocol. The proposed definition of 'independent control' is intentionally broad and technology neutral but excludes DAOs, third party software integrated in the protocol and individuals with significant governance token holdings from being identified as a subject with 'independent control' by reason of their identity alone.

2. DeFi as a 'critical infrastructure'

Critical infrastructure is defined by the Cybersecurity and Infrastructure Security Agency (**CISA**) traditionally as:

> systems and assets that are so vital that their incapacitation or destruction would have a debilitating effect on security, the economy, public health, public safety, or any combination thereof.

While the question of whether Genuine DeFi satisfies this standard at this time remains debatable, there are clear benefits of classifying Genuine DeFi as a Critical Infrastructure subject to oversight by the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (**OCCIP**), including response coordination, implementation of cybersecurity standards and information sharing across government agencies.

3. A multi-tiered approach

In addition to oversight from the OCCIP, the establishment of a new regulated entity named 'critical communications transmitters' (**CCT**) is proposed. The CCT definition does not include those solely involved in the development of the software but does include those providing a service communicating user information about a transaction, responsible for transmitting a material portion of the communications and where the service is offered as a business or for profit. However, it is expected that FinCEN will require new authority to regulate CCTs as existing regulations do not give the Treasury authority to establish risk programs for non-financial institutions. Under the proposal, these CCTs will be responsible for implementing risk management systems and procedures to mitigate illegal activity in DeFi. This may include a wallet risk scoring and blocking system which helps filter wallets with transactional proximity to illegal transactions, sanctioned addresses, historical engagement in suspicious activity and more.

The proposed framework identifies the absence of intermediaries in Genuine DeFi protocols and recognizes the distinctive risks stemming from the technology. A collective effort involving policymakers, industry stakeholders, and experts is imperative in order to ensure DeFi regulation addresses the unique risks and benefits of the technology. The authors' paper is a welcome contribution to the debate over how to mitigate the financial crime risks raised by DeFi which seeks to allow DeFi to flourish and avoid simply reimposing centralisation into open systems.

By Steven Pettigrove and Kelly Kim