Article Information

Authors: Barbara Vrettos, Jade McGlynn, Michael Bacina
Service: Blockchain
Sector: Financial Services, FinTech, IT & Telecommunications

Blockchain Bites: US Regulators Divided on Defi Regulation, Colonial Pipeline ransomware recovered, El Salvador promotes BTC to legal tender

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.

US Regulators Divided on Defi Regulation

The US has arrived at a crypto-crossroads. Recently we've seen US regulators either pushing hard to update and increase America's rules on engaging with cryptocurrencies, or expressing concern that too much red tape will suffocate innovation. This difference of opinion is apparent across regulators.

Hester Peirce, one of the five commissioners at the Securities and Exchange Commission, believes in honouring and accommodating the differences of the digital asset space to encourage new business and ideas.

In a recent interview with the Financial Times Peirce said:

> I am concerned that the initial reaction of a regulator is always to say 'I want to grab hold of this and make it like the markets I already regulate…I am not sure that's going to be great for innovation.

These comments mirror the words of Australia's own Financial Services Minister Jane Hume who recently recognised the profound opportunity posed by digital currencies and the Australian Government's need to reject calls for undue restrictions of digital asset marketplaces. Yet both of these leading views stand in stark contrast to the Chair of the SEC, Gary Gensler who reportedly " s*pearheads an effort to bring the fast-growing cryptocurrency market more in line with other types of financial assets*."

Gensler has told Congress members there are "gaps" in the regulatory system and a need for lawmakers to clarify which regulator should oversee digital asset exchanges in particular. He has also touted his desire for crypto holders to be offered similar protections to those investors need dealing with centralised counter parties like the New York Stock Exchange or Nasdaq.

This split of opinion is further highlighted in recent comments of Commissioner Dan Berkovitz of the CFTC (Commodity Futures Trading Commission). In his keynote address at the FIA and SIFMA AMG, Asset Management Derivatives Forum 2021, Commissioner Berkovitz ballyhooed that "*unlicensed decentralized finance (DeFi) markets may be illegal*", urging other regulators to focus more attention to DeFi derivatives as a growing area of concern and to address regulatory violations appropriately.

In summary, Berkovitz takes issue with the 'counterparty risk' involved in Defi. Similar could be said of Gensler who seemed to paint digital asset holders as defenceless without the protection of increased regulation overseen by clearly elected supervisors.

Berkovitz commented:

> In a pure "peer-to-peer" DeFi system, none of the benefits or protections (in traditional finance) exist. There is no intermediary to monitor markets for fraud and manipulation, prevent money laundering, safeguard deposited funds, ensure counterparty performance, or make customers whole when processes fail.

He continued:

> A system without intermediaries is a Hobbesian marketplace with each person looking out for themselves. Caveat emptor—"let the buyer beware."

Any financial transaction carries risk, the concern expressed by Gensler and Berkovitz appear to mis-apply what is traditionally considered as counterparty risk.

In a traditional transaction, intermediaries are required because of the opaque nature of a marketplace where certain parties can have information advantages over others, and where the risk of counter-party risk (that is one party defaulting on their promises) poses a real and systemic threat to confidence in the entire marketplace.

A significant part of existing financial services laws are designed to deal with counterparty risk and the safety of deposited funds given the incentives to bad actors to take risks or cheat customers.

The entirely open nature of blockchain based systems, upon which DeFi is built (in this case principally the Ethereum blockchain) by design has radical transparency so that parties can transact on a peer-to-peer basis with trust in the computerised system, rather than in a person, to complete a transaction. This is of course only possible by smart contract code being open source and visible, so that users can see (or more realistically rely upon auditors who have reviewed) the code of those contracts.

A smart contract can never do something the code doesn't permit, and so can provide mechanisms previously at risk of bad actors mishandling or stealing funds. Escrow smart contracts with release only upon performance by a counterparty in many cases today entirely eliminate the counterparty risk and the permanent nature of blockchain transactions with tracking of the transactions publicly available renders money laundering a foolish endeavour.

The biggest risks which have crystalised to date in DeFi projects are either "rug pulls", where a project is a scam and the price of the tokens in the project have been hyped up by bad actors, something just as illegal in DeFi as it is in regular commerce or indeed in a financial market, and in hacks or smart contracts being manipulated due to a bug in the code or exploit not previously uncovered.

The Hobbesian nature of DeFi which Berkovitz referred to is viewed by some as a strength, as smart contracts with poor code *will* be exploited and weeded out over time and only the strongest and most reliable code should survive. That is, of course, cold comfort to those who have lost funds in such exploits.

There remain many centralised parties involved in DeFi who may well be sensible targets for light touch regulatory treatment (we're looking at you CeFi lenders and centralised chains like Binance Smart Chain), but it seems to these writers that Berkovitz and Gessler need to improve their understanding of Blockchain, Crypto and DeFi considerably before making such sweeping misstatements as to the risks posted by DeFi generally. Blockchain and crypto have a hard enough time with myths abound without new myths being spread and leaders of regulators should ensure they are informed and speak accurately and with nuance about new technologies. In the meantime, Commissioner Peirce continues to lead the way.

Colonial Pipeline ransomware recovered

The Colonial Pipeline cyberattack was reportedly the largest cyber attack on the American energy system and caused multiple US states to feel the shockwaves of surged gas prices and gas shortages. Now the US Department of Justice says it has recovered millions of dollars in cryptocurrency paid to hackers to mitigate the disruption.

The Colonial Pipeline company, which operates a 5,500 mile pipeline transporting gas and diesel from Texas to New Jersey, succumbed to the cyber attack on 7 May 2021 and, against recommendations, paid USD$4.4 million in BTC as ransom to the Eastern European hackers known as Darkside. Joseph Blount, Colonial Pipeline's CEO, told the Wall Street Journal that he authorized the ransom payment because executives were unsure how badly the cyberattack had breached Colonial's systems, and consequently, how long it would take to bring the pipeline back. Tom Robinson, co-founder of cryptocurrency tracking firm Elliptic, reported that the ransomware payment was paid the day after the hackers had locked the Colonial Pipeline network.

The US Department of Justice however has said it has recovered USD$2.3 million in cryptocurrency of the ransomware paid. Deputy Attorney General Lisa Monaco stated that the Justice Department has found and recaptured a majority of the ransomware, saying:

> Following the money remains one of the most basic, yet powerful tools we have.

The DoJ's approach consisted of identifying the wallet that Darkside had used to collect the payments, tracking the payments to a wallet with a private key "controlled by hte FBI" then lodging a warrant to seize the funds in that wallet and secure court approval from a judge in the Northern District of California.

According to the Sydney Morning Herald, the operation to recover the ransomware is the first feat of the specialised ransomware task force created by the Biden administration. The perception that cryptocurrency is anonymous and cannot be traced is refuted time and time again. However, it continues to persist in the financial press, in close correlation to authors skeptical or critical of digital currencies.

There has been no word on whether the US taskforce is collaborating with private digital currency tracing companies such as Elliptic or Chainalysis with whom the DoJ has collaborated with previously in relation to high profile takedowns.

It's unclear whether this was a case of Darkside returning some funds under an undisclosed deal, or a genuine infiltration of the group or wallets by FBI white-hat hackers. But the example stands to show that blockchain and digital currency remains a terrible way for criminals to transfer value, unless they want to get caught.

Bitcoin got the job! El Salvador promotes Bitcoin to legal tender

A moment in Bitcoin history was made when President Nayib Bukele's proposal to make Bitcoin legal tender was recently approved by El Salvador's Congress.

With 62 out of 84 votes cast in favour, it Bukele's reasoning – that "*it will bring financial inclusion, investment, tourism, innovation and economic development for our country*", seems to have been accepted by the lawmakers.

Under this new law *"bitcoin must be accepted by firms when offered as payment for goods and services (and) tax contributions can also be made with it."*

Long time digital currency community members will recall Japan was reported to have made Bitcoin legal tender in 2018, which was swiftly clarified to confirm Japan only recognised it as property. El Salvador is now the first country in the world to recognise a digital currency as legal tender. El Salvador also recognises the US dollar as legal tender and will use the US dollar as the reference price for any accounting using Bitcoin.

Before the vote was put to Congress there were some reservations expressed around what this could mean for El Salvador's International Monetary Fund participation and program. Bukele is with the IMF and believes there will be no change to El Salvador's macro economics as a result of this move.

Bukele further gave reassurances that:

> The use of bitcoin will be optional for individuals and would not bring risks to users, with the government guaranteeing convertibility to dollars at the time of transaction through a trust created at the country's development bank BANDESAL.

The country has 90 days to roll out infrastructure to support the use of Bitcoin, as many businesses will be unlikely to have software in place to accept payments. Bitcoin can of course continue to be used by ex-patriots for remittances back to El Salvador, and depending on what kind of infrastructure is to be offered, adoption on the ground will need to overcome matters such as current on-chain transaction fees (which at the time of writing are ~AUD$10 – making Bitcoin payments impractical for small transactions).

This bold experiment will be closely examined by fans and foes of Bitcoin alike as a natural experiment in Bitcoin adoption now progresses.