



# Crypto and the Courts: A Global Case Law Analysis

January 2024





# Crypto and the Courts: A Global Case Law Analysis

January 2024

## Authors

Ateesh Nandi and Siva Bhargavi Nori

## Acknowledgement

The authors thank Shri Dhritiman Murti and Ms Perna Mathur for their insight and support.



# Contents

<b>5</b>	<b>Summary</b>	
<b>7</b>	<b>Introduction and Scope</b>	
<b>9</b>	<b>Background into key web3 concepts</b>	
9	Trustless validation on decentralised ledgers	
9	Immutability of records and self-custody of digital assets	
<b>11</b>	<b>Judicial perspectives on Web3</b>	
11	Crypto assets and property rights	
18	Governance of Web3 service providers	
25	The nature of decentralisation	
<b>29</b>	<b>Key Takeaways for India</b>	
<b>33</b>	<b>Way forward</b>	

# List of Abbreviations

<b>AML</b>	: Anti-Money Laundering
<b>CFT</b>	: Combating the Financing of Terrorism
<b>BCBS</b>	: Basel Committee on Banking Supervision
<b>BIS</b>	: Bank of International Settlements
<b>BUSD</b>	: Binance USD token
<b>DAO</b>	: Decentralised Autonomous Organisation
<b>DeFi</b>	: Decentralised Finance
<b>DLT</b>	: Distributed ledger technology
<b>DoJ</b>	: United States Department of Justice
<b>EWHC</b>	: England and Wales High Court
<b>FATF</b>	: Financial Action Task Force
<b>FinCEN</b>	: United States Department of Treasury Financial Crimes Enforcement Network
<b>FSB</b>	: Financial Stability Board
<b>G20</b>	: Group of Twenty
<b>HKCFI</b>	: Hong Kong Court of First Instance
<b>IEEE</b>	: Institute of Electrical and Electronics Engineers
<b>IEEPA</b>	: International Emergency Economic Powers Act
<b>IEC</b>	: International Electrotechnical Commission
<b>IRS</b>	: Internal Revenue Service
<b>ISO</b>	: International Organization for Standardization
<b>IMF</b>	: International Monetary Fund
<b>IOs</b>	: International Organizations
<b>IOSCO</b>	: International Organization of Securities Commissions
<b>KYC</b>	: Know-Your Customer
<b>NASSCOM</b>	: National Association of Software and Service Companies
<b>NFTs</b>	: Non-Fungible Tokens
<b>OECD</b>	: Organization for Economic Cooperation and Development
<b>OFAC</b>	: United States Department of the Treasury, Office of Foreign Assets Control
<b>SSBs</b>	: Standard Setting Bodies
<b>SEC</b>	: United States Securities and Exchange Commission
<b>UAE</b>	: United Arab Emirates
<b>UKJT</b>	: United Kingdom Judicial Taskforce
<b>USDT</b>	: United States Dollar Tether
<b>USDCC</b>	: United States District Court for the District of Columbia



# Summary

Courts play a pivotal role in clarifying the contours of consumer rights and corporate responsibility in web3. Discussions in courts broaden the public understanding around web3 as opposing perspectives are deliberated in the backdrop of contemporary legal developments.

In this paper, we review key case laws that have shaped the discourse around web3 in recent years. We divide our analysis within three thematic heads, as described below.

## **A. Crypto assets and property rights**

Courts worldwide recognize crypto assets as property. Crypto assets meet the common law test for 'property', in that they are definable, identifiable, transferable, and have a degree of permanence. However, there is a debate on classifying different crypto assets as specific types of property - whether as a security, a means of payment or some other kind of intangible property.

## **B. Governance of web3 service providers**

The principles underlying the existing prudential and corporate governance rules governing traditional finance can address key regulatory challenges in web3. However, there is a need for greater information sharing and international coordination in cases involving non-compliance by market leaders.

## **C. The nature of decentralisation.**

There is a lack of clarity around the concept of decentralisation in web3. Courts have taken conflicting positions in holding decentralised web3 service providers responsible for market activity on their platforms. In some cases, they were treated akin to intermediaries having safe-harbour protection. In others, these service providers, along with their founders were held responsible for the actions of third-parties on their platforms. Global consensus on this issue is yet to be achieved.



We conclude with the following recommendations for Indian policymakers to consider:

- **Need to follow global case law developments.** Policymakers need to consider the outcomes of cases from United Kingdom, Singapore and Hong Kong because they serve as precedents across common law jurisdictions. Cases from US courts become important elements of the global narrative around decentralisation, corporate governance etc.
- **Need to avoid a one-size fits all approaches in classification.** The Securities and Exchange Commission's (SEC) 'Howey Test' to determine whether a crypto asset is a 'security' can be applied in Indian jurisprudence - however, it is critical that Indian lawmakers avoid a one-size fits-all approach to regulation. The different kinds of crypto assets such as unbacked crypto assets, stablecoins, non-fungible tokens (NFTs) etc. must be treated as different asset classes. The SEC's limited success in applying the 'Howey Test' underlines the diverse nature of crypto assets and their varying rights.
- **Need to adopt detailed taxonomies.** India should consider adopting a taxonomy to classify various crypto assets. Standard-setting bodies (SSBs) like the International Monetary Fund (IMF) and the Financial Stability Board (FSB) have provided relevant baselines which can be used as point of reference.
- **Existing prudential and corporate governance principles** can be applied to address frauds and scams in web3. There is a need for baseline standards for know-your customer (KYC) processes, Anti Money Laundering / Combating the Financing of Terrorism (AML/CFT) programs and Suspicious Transaction Reporting (STR) as a global common minimum.
- **Need for participatory models of governance.** The web3 ecosystem stands at the intersection of several sectors, markets and disciplines including engineering, mathematics, and economics. No one public authority is equipped to manage this emerging sector. It is important that regulatory architectures recognise the need for a diversity of perspectives, and adopt participatory models of governance.
- **Industry should proactively adopt best practices and technical standards.** Web3 players should seek to align on best practices to ensure market integrity, consumer protection and systemic resilience. They should adopt emerging standards and global best practices for critical audit, consumer protection, cybersecurity, etc.

## 2.

# Introduction and Scope

The discourse around web3 products, services, and markets (web3 ecosystem) has matured considerably in recent years. Today, countries across the world have set up regulatory frameworks and even bespoke laws to govern the sector. While states typically empower their anti-money laundering agencies and financial regulators to govern crypto assets, some markets such as the United Arab Emirates (UAE) have set up specialised regulators and frameworks for classifying crypto assets and licensing web3 service providers. Others like Japan have also adopted self-regulatory models of governance.

These developments are the result of an in depth understanding of web3 fundamentals. SSBs and International Organizations (IOs) have played a key role here. Their advisories on key aspects of web3 (*see table 1*) furthers global consensus around taxonomies, regulatory approaches, and governance standards.

IOs / SSBs	OECD	BCBS & BIS	FSB	IOSCO	IMF	FATF
Thematic domain	Tax Reporting standards	Prudential standards for traditional financial institutions	Financial stability risks	Market integrity & investor protection	Macro financial vulnerabilities	AML/CFT standards

Source: Author's own

Courts have played an equally important role in clarifying the contours of rights and responsibilities available to various stakeholders in web3.

Discussions in courts broaden the public understanding around web3 as opposing perspectives are deliberated in the backdrop of contemporary interpretations of consumer rights and corporate responsibility. Courts around the world have dealt with disputes related to smart contracts, digital assets, and decentralised autonomous organisations (DAOs). This facilitates legal certainty for individuals and businesses building value in Web3.

Courts have notably tried to balance the interests of aggrieved users and investors without stifling innovation. For instance, in November 2023, the Supreme Court of India dismissed a petition seeking regulatory guidelines around crypto asset trading in India. It highlighted that the legal relief sought by the petitioner fell within the domain of the Indian Parliament.<sup>1</sup> Case law developments and formulations of legal and regulatory guardrails often go hand in hand.



In this paper, we analyse key judicial rulings that have had a seminal impact on the public understanding around web3. We also discuss landmark cases that deal with the nature of crypto assets and the responsibility of service providers in web3, including issuers of crypto assets, operators of exchanges, and trading venues, providers of wallet services, etc.

In the following sections, we first provide a brief background into some concepts that are fundamental to the web3 ecosystem. We then discuss court rulings under three thematic heads: (a) crypto assets and property rights, (b) governance of web3 service providers, and (c) the nature of decentralisation. In conclusion, we discuss some learnings and implications for Indian policymakers to consider.

# 3.

## Background into key web3 concepts

Web3 has numerous value propositions and long-term use cases that can transform the manner in which humans interact and exchange value with each other. At its core, the web3 ecosystem is about the ownership of digital artefacts. Most SSBs and IOs define crypto assets as digital representations of value that rely on cryptographically secure distributed ledgers to validate and secure transactions.

Global consensus is that private crypto assets are not 'fiat currency', i.e. sovereign-backed money. However, as digital products, they can represent value through their inherent characteristics, the rights conferred onto holders or through the forces of supply and demand in the market.

For instance, holders of the crypto asset 'Filecoin'<sup>2</sup> have the right to access a digital storage and data retrieval system. On the other hand, non-fungible tokens (NFTs) such as the Bored Ape NFTs<sup>3</sup> derive value from their inherent characteristics as pieces of art as well as market factors such as scarcity and uniqueness. We discuss some key web3 concepts below.

### Trust less validation on decentralised ledgers

Distributed ledger technology (DLT) systems are those that allow multiple participants to maintain and update a shared digital database, or ledger, without the need for a central authority. It is a digital record-keeping system that is distributed across many computers or nodes.

The validation of transactions and data is done through consensus mechanisms. Instead of a central authority, peer-to-peer networks of nodes agree on the state of a blockchain. This decentralised validation process means that there is no single entity that nodes must trust to validate transactions.

DLT systems have significant implications for decentralised applications, decentralised finance, and other use cases enabled by web3 technologies. The promise of web3 lies in its ability to create digital systems and economies that are open, inclusive, and owned by their participants.

### Immutability of records and self-custody of digital assets

Information stored on DLTs are mathematically tamperproof because no one entity controls the network. This ensures that the historical accuracy, transparency, and integrity of information remains intact, making DLTs auditable and a useful tool for establishing provenance. For instance, each NFT has a unique identifier recorded on the blockchain, which allows NFT holders to prove and verify ownership.

Further, web3 products and services gives users custody and control over their digital assets. Users own their account credentials giving them exclusive access to digital assets, identity, and information. However, self-custody also means users alone are responsible for safeguarding their keys because if they are lost or stolen, funds can be permanently inaccessible.

This characteristic of web3 products and services has several implications for sectors where information integrity and permanence are crucial, such as legal contracts, digital identity, and historical records.

### **Smart contracts and decentralised decision making**

DLT systems embody smart contracts which self-execute when predefined conditions are met. The terms of the contract and triggers for its execution are written into the code on a blockchain layer, which makes them auditable and hard to manipulate. For example, developers write smart contracts on the Ethereum blockchain using a programming language called Solidity.<sup>4</sup>

Smart contracts have several applications in the financial sector, healthcare, real estate, among others. A key application of smart contracts in the context of web3 is in decentralised decision-making. Decentralised Autonomous Organisations (DAOs) are decision-making systems, which operate on the basis of defined rules and operations. Decision-making in DAOs is based on ownership of relevant governance tokens that confer voting rights and decision-making power.<sup>5</sup>

While there are no easy answers to questions around legal classification, governance, tax residency, etc., there is a growing body of knowledge and understanding around DAOs. Wyoming state in the US, for instance, enacted a law that permits DAOs to register as limited liability companies, provided they maintain a registered agent in the state.<sup>6</sup>

In the following paragraphs, we discuss how courts have furthered the development of these Web3 concepts.

# 4.

## Judicial perspectives on web3

Having examined ideas around decentralised ledgers, and how decision making and agency can be exercised, we examine the judicial precedents that have been set around these concepts.

Courts have examined various ideas around ownership of crypto assets and accountability of web3 service providers such as centralised and decentralised exchanges. Judicial observations have also raised fundamental questions around the nature of decentralised decision-making in web3.

In this section, we explore how courts have approached the following questions.

- *Crypto assets and property rights.* What are crypto assets, and what rights do their holders have? Can investors exercise property rights over their holdings? Can these assets be held in trust?
- *Governance of web3 service providers.* What kind of safety and governance mechanisms are necessary for centralised service providers in web3? Can existing legal concepts like intermediary liability and safe harbours apply over decentralised trading platforms?
- *The nature of decentralisation.* How should decentralised decision-making arrangements be classified and governed? What is the duty of developers of blockchains?

### A. Crypto assets and property rights

#	Year	Court	Case
1	2019	England and Wales High Court	AA v Persons Unknown [2019] EWHC 3556 (Comm) ( <i>AA v. Persons Unknown</i> )
2	2022	United States District Court, Southern District of New York	SEC v. Ripple Labs, 20 Civ. 10832 (AT)(SN) ( <i>SEC v. Ripple</i> )
3	2022	High Court of Singapore	Janesh s/o Rajkumar v Unknown Person [2022] SGHC 264 ( <i>Janesh v. Unknown Person</i> )
4	2023	High Court of Singapore	ByBit Fintech Ltd v Ho Kai Xin and others [2023] SGHC 199 ( <i>ByBit case</i> )
5	2023	United States District Court, Southern District of New York	SEC v. Terraform Labs. Pte. Ltd., 23-cv-1346 (JSR) (S.D.N.Y.) ( <i>SEC v. Terraform</i> )
6	2023	NA	Wells Notice <sup>7</sup> to Paxos, 2023

## 1. AA v Persons Unknown, 2019

### Brief facts

A Canadian insurance company's security systems were infiltrated by hackers who installed malware that prevented the company from accessing its IT systems. They demanded that the Company transfer Bitcoins to a specified account in exchange for the decryption software.

The Company was insured against certain cyber-related incidents by an English insurance firm. After the ransom was paid, the insurer hired consultants who tracked the Bitcoin payments to a specific address linked to the crypto asset exchange Bitfinex. While some had been transferred, 96 Bitcoins remained in the account. The insurer therefore sought a proprietary injunction to recover the Bitcoins.<sup>8</sup>

The issue before the England and Wales High Court (EWHC) was whether Bitcoin can be treated as a form of property.

### Analysis

The EWHC stated that while a crypto asset might not fit the traditional definition of property in UK law, it could nonetheless be treated as property.

The traditional definition of property in UK law is narrow. It includes: 'things in possession' i.e., capable of being possessed, or 'thing in action' i.e., capable of being enforced by legal action. The EWHC observed that as intangible assets which did not confer legally enforceable rights, crypto assets do not meet this definition.

However, the EWHC found crypto assets to be a kind of property because they meet Lord Wilberforce's classic definition of the term which was laid down in the landmark case of *National Provincial Bank v Ainsworth* [1965] 1 AC 1175 (*Ainsworth case*). The EWHC held that crypto assets are "definable, identifiable by third parties, capable in their nature of assumption by third parties, and having some degree of permanence."<sup>9</sup>

The EWHC thus adopted the reasoning of the UK Judicial Taskforce's (UKJT) 2019 legal statement on crypto assets and smart contracts, which stated that the *Ainsworth* case served as "an important and authoritative description of the necessary characteristics of property".<sup>10</sup> The UKJT stated that although crypto assets are not strictly a "thing in possession", nor a "thing in action", they represent more than mere information – which is not treated as property under English law.<sup>11</sup>

Thus, crypto assets can be treated as a novel kind of intangible asset which amounts to "property".<sup>12</sup>

## 2. SEC v Ripple labs, 2022

### Brief Facts

Ripple, a blockchain company, launched a crypto asset XRP in 2012 to enable cost-effective cross border transactions.<sup>13</sup>

In December 2020, the SEC had filed a lawsuit before the US District Court for the Southern District of New York against Ripple and two of its executives, Bradley Garlinghouse and Christian Larsen for alleged violations of US law by selling unregistered securities.<sup>14</sup>

The SEC claimed that XRP is a security under US law, and that Ripple illegally raised \$1.3 billion by selling unregistered securities.<sup>15</sup> The issue before the court was whether XRP tokens sold by Ripple constituted a “security”, and therefore in violation of the US Securities Act, 1933.

## **Analysis**

The SEC relied on the ‘Howey test’ to claim that XRP is a security under US law. The Howey test is a four-pronged judicial test that was established by the US Supreme Court in SEC v. W.J. Howey Co. in 1946. It is used to determine whether a transaction qualifies as an ‘investment contract’ under the US Securities Act, 1933.<sup>16</sup>

The court found that XRP was not an unregistered security offering when sold to the public. However, it held that arrangements between Ripple and institutional investors to sell XRP tokens, pursuant to written agreements, amounted to ‘investment contracts’ under US law. In the latter context, the XRP transactions involved an investment in a common enterprise with a reasonable expectation of profits based on the efforts of others; they were thus liable to be regulated as securities.

Many crypto assets are designed and structured in a manner similar to XRP; (unlike Bitcoin, or even Ethereum). The court’s ruling that XRP sold to the public does not amount to an investment contract sets a crucial precedent for all such tokens, especially in US courts.

In October 2023, the SEC dropped claims of aiding and abetting the company in violating federal securities laws in its XRP transactions against the two executives of Ripple.<sup>17</sup>

## **3. Janesh v Unknown Person, 2022**

### **Brief Facts**

The claimant, Janesh, owned a Bored Ape NFT (the Bored Ape Yacht Club (BAYC) ID #2162). The claimant sought a loan from the defendant with the NFT as a collateral under an escrow mechanism. The loan period was 30 days, with interest payable at 45 percent per annum.

Janesh requested that the loan period be extended briefly, and sought to restructure the loan arrangement. Though the defendant was cooperative at first, they later changed their stance and issued an ultimatum - that they would foreclose the Bored Ape NFT if the claimant failed to make a full repayment within two days.

Following the claimant's failure to do so the defendant took possession of the Bored Ape NFT. The claimant, therefore sought an injunction from the High Court of Singapore to restrain the defendant from dealing with the NFT.

## Analysis

The High Court of Singapore found that NFTs could be regarded as property since they met the criteria set out in the Ainsworth case.

- **Definable** – Once a piece of art is minted into an NFT, it gets a unique identification code on the blockchain which is verifiably distinguishable from that of other NFTs.
- **Identifiable by third parties** – The presumptive owner is the one controlling the wallet linked to the NFT. Like other crypto assets, exclusivity is achieved because one cannot access an NFT without the owner's private key.
- **Capable of assumption by third parties** – The owner of an NFT has the exclusive ability to transfer it to a third party. NFTs are the subject of active trading in web3 marketplaces and trading venues.
- **Possessing some degree of permanence or stability** – NFTs stored in DLT systems of different types have the same degree of permanence and stability as money in bank accounts.

## 4. ByBit case, 2023

### Brief Facts

The claimant, a Seychelles company, owned and operated a crypto asset exchange. It paid its employees in fiat currency, crypto assets, or a combination of both. The claimant engaged WeChain Fintech Pte. Ltd. (WeChain) as its payroll service provider. The Defendant, an employee of WeChain, was responsible for processing the payroll of the Claimant's employees.

The dispute arose when the claimant discovered that irregular payments were made to four crypto addresses controlled by the defendant. The irregular payments totalled 4,209,720 in United States Dollar Tether (USDT), a widely adopted stablecoin. The claimant alleged that the defendant manipulated the account information on claimant's payroll files, and consequently caused the claimant to transfer USDT to wrong addresses. The claimant alleged that an institutional constructive trust<sup>18</sup> was created by virtue of the defendant's fraudulent act.

The issue before the High Court of Singapore was whether USDT is property which is capable of being held on trust.

### Analysis

The High Court of Singapore declared a constructive trust over the USDT, and held the claimant to be the legal owner of such assets. The court observed that crypto assets can be defined, identified, and possessed by humans, and can be traded and valued as holdings.

The court made a significant deviation from the earlier position set in common law by UK courts. It classified crypto assets within one of the two traditional definitions of personal property i.e., 'things in action', and 'things in possession'.

It referred to common law jurisprudence about property rights and observed that "all personal things are either in possession or action. The law knows no '*tertium quid*' (unidentified third element) between the two."<sup>19</sup> The court held that a holder of a crypto asset has "in principle an incorporeal right of property recognisable by the common law as a thing in action."<sup>20</sup> Thus, although crypto assets can be transferred without the assistance of the legal system, they nonetheless are 'things in action'.

## 5. SEC v. Terraform Labs, 2023

### Brief Facts

The SEC sued Terraform Labs and its co-founder, Kwon Do-hyung (Do Kwon) in February, 2023. SEC alleged that the defendants engaged in fraudulent conduct, made misleading statements, and committed fraud by deceiving investors about the stability of their stablecoin TerraUSD (UST). TerraUSD (UST) is a decentralised and algorithmic stablecoin of the Terra blockchain built by Terraform Labs.

SEC claimed that they falsely credited UST's algorithm for its price stabilisation which was marketed as pegged to US dollar though another crypto asset - Luna.<sup>21</sup> It also claimed that Terraform Labs made misleading claims about the efficiency of the price stabilisation algorithm used in UST.<sup>22</sup>

Terra collapsed in May 2022, destroying billions of dollars in investor wealth, particularly for investors residing in emerging markets and developing economies.<sup>23</sup>

The issue before the United States District Court in the Southern District of New York was whether Terraform Labs and Do Kwon sold unregistered securities and engaged in fraudulent conduct to deceive investors.

### Analysis

Do Kwon and the SEC have sought summary judgements from the court in October and November of 2023 respectively. Terraform and Do Kwon claimed that the SEC had not proved that the company was selling securities, even after a two-year investigation.<sup>24</sup> Whereas the SEC claimed that Terraform was indeed selling securities as there was: (a) pooling of money in a common enterprise, (b) with an expectation of profit, and (c) predominantly due to the efforts of promoters – thereby satisfying Howey test.<sup>25</sup>

## 6. Wells Notice to Paxos, 2023

### Brief facts

Paxos Trust Co., is an issuer of stablecoins such as Paxos Dollar (USDP). It partnered with Binance, a leading web3 service provider, in September 2019 to build BUSD, a US Dollar-collateralized stablecoin. However, Paxos operations came under scrutiny when the SEC reportedly planned to initiate regulatory action against the company for violating investor protection laws. In February 2023, the SEC issued a Wells Notice to Paxos, alleging that BUSD is an unregistered security.

Paxos in response “categorically disagreed” with the SEC's position that BUSD is a security and expressed its preparedness to “vigorously litigate” if necessary.<sup>26</sup> Further, Paxos announced it would stop minting new BUSD tokens and would end its relationship with Binance, while ensuring that customers could still redeem the stablecoin for at least a year.



## Analysis

The SEC's prospective lawsuit against Paxos represents a significant moment in the regulatory oversight of stablecoins. It underscores the operational complexities and regulatory challenges in managing stablecoins like BUSD, and highlights the increasing uncertainty with classifying them as securities.

Specifically, the Wells Notice flags discrepancies in maintaining collateral for the stablecoins. Representatives from Binance reportedly stated that the alleged inconsistencies were due to delays in gathering appropriate capital and that the process behind maintaining collateral has since been improved.<sup>27</sup>

This lawsuit could have far-reaching implications for investor protection and the stability of the crypto-asset market. It might set a precedent for the treatment of similar crypto-assets under US securities law, potentially influencing the regulatory approach towards other stablecoins and digital assets. The case could also be a catalyst for clearer regulatory guidelines, which are critical for the continued growth and stability of the web3 ecosystem.

## Takeaways

### **Crypto assets are increasingly recognised as property around the world**

Common law courts have established that crypto assets are property, and holders of crypto assets have legally enforceable property rights over the same. The High Court of Singapore as well as the UKJT aligned on the position that crypto assets are 'property' in that they are "definable, identifiable by third parties, capable in their nature of assumption by third parties, and have some degree of permanence."

Moreover, the High Court of Singapore also ruled that crypto assets meet the traditional definition of property in common law.

### **There is an ongoing discussion on whether crypto assets are securities or payments mechanism**

The SEC has asserted its jurisdiction<sup>28</sup> over different kinds of crypto assets by classifying them as 'investment contracts' under the US Securities Act of 1933. SEC v. Ripple Labs, and SEC v. Terraform Labs, underline the challenge in transplanting traditional legal tests, such as the Howey test, to determine the nature of and classify crypto assets.

Regulators like the SEC treat crypto assets under securities laws because of the way they are marketed to the public – as profit-bearing instruments without adequate disclosures – and not based on inherent characteristics. On the other hand, countries such as the Bahamas, Cayman Islands, Gibraltar, and Japan recognize crypto assets as modes of payments mechanisms,<sup>29</sup> which adds another layer of complexity to the discourse.

Consensus on the nature of crypto assets is crucial since it affects how they are taxed and regulated. For example, if crypto assets are property, they may be subject to capital gains tax and stamp duties around the world. Governments and policymakers should provide clarity on the issue of taxonomy and classification. In this regard, they should refer to proposals forwarded by SSBs such as the IMF.

### **Stablecoins are treated separately owing to their characteristics**

Circle, the issuer of a popular stablecoin USD Coin (USDC) highlights that asset pegged to the US dollar, such as BUSD or USDC are not securities. Stablecoins do not amount to 'investment contracts' under US law since there is no expectation of profit among holders.<sup>30</sup> According to Circle, payment stablecoins do not have the "features of an investment contract" on their own.

Stablecoins maintain price stability either through reserve assets or via algorithms. Governments and regulators pay special attention to stablecoins due to their potential to act as a currency equivalent.

The IMF notes how USD-denominated stablecoins might be used as a hedge against inflation or store of value in some emerging markets and developing economies.<sup>31</sup> The stablecoins that hold safe and liquid assets as reserves and offer direct legal claims on the issuer can indeed serve this purpose. However, many algorithmic stablecoins have proven to be volatile.<sup>32</sup>

It remains to be seen how the jurisprudence around stablecoins develops. Currently, the BCBS prudential standards recommend that banks deploy more conservative capital treatment restrictions in respect of algorithmic stablecoins with ineffective stabilisation mechanisms.<sup>33</sup>

### **NFTs have implications in intellectual property law as copyrightable works**

NFTs can be regarded as property, as illustrated in *Janesh v. Unknown Person*. However, their legal treatment must be aligned with other legal concepts such as copyright law. In India, copyright vests with the author of an artistic work. Even if the artistic work is sold as an NFT, the copyright would vest with the original author or artist, unless it is assigned. Authors of artistic works must explicitly and unconditionally assign the copyright to a purchaser of the work under a written agreement.<sup>34</sup> Once the assignment is duly made, the assignee is treated as the owner of the copyright under the Indian Copyright Act, 1957.

The mode of assignment of a copyright varies across jurisdictions. The requirement to execute a signed written agreement in India may pose challenges especially where an NFT changes hands multiple times. In cases where NFTs are acquired without the corresponding copyright, the purchaser may have a valid title to the NFT, but will lack the right to commercialise it by, say issuing merchandise containing the artistic work.

## Governance of web3 service providers

#	Year	Court	Case
1	2014	Tokyo District Court	Bankrupt Entity: MtGox Co., Ltd; (Tokyo District Court 2014 (fu) No. 3830) (Mt.Gox bankruptcy)
2	2023	United States District Court, Western District of Washington at Seattle	United States of America v. Binance Holdings Limited (CR23-178 RAJ) (USA v. Binance, 2023)
3	2023	United States District Court, Southern District of New York	United States v. Bankman-Fried, 22-cr-0673 (LAK) (S.D.N.Y.) (FTX case, 2023)
4	2023	Hong Kong Court of First Instance	Re Gatecoin Limited [2023] HKCFI 91, (Gatecoin case)

### 1. Mt.Gox bankruptcy, 2015

#### Brief facts

Launched in 2010, Tokyo-based Mt. Gox quickly became the largest Bitcoin exchange globally - handling over 70 percent of all Bitcoin transactions by 2014. However, in February 2014, the crypto asset exchange suspended trading, shut down its website, and filed for bankruptcy protection owing to a cyber-attack which caused it to lose a substantial amount of Bitcoin holdings (both proprietary and client holdings). In April that year, an investigation revealed that most of the missing bitcoins were stolen from it over multiple years - beginning late 2011.<sup>35</sup>

CEO Mark Karpelès was arrested on charges of fraud and embezzlement in August 2015. He was accused of misappropriating funds from Mt. Gox investor accounts and manipulating the company's internal systems to inflate account balances. In March 2019, the Tokyo District Court found Karpelès guilty of falsifying data to inflate Mt. Gox's holdings but acquitted him of more severe charges like embezzlement and aggravated breach of trust.

The aftermath of the Mt. Gox collapse has been a protracted process for creditors awaiting reimbursement. Nobuaki Kobayashi, the Mt. Gox trustee, announced several delays in repayment plans due to logistical challenges. As of late 2023, creditors, who have been awaiting payments for nearly nine years, were informed that repayments in BTC, BCH, and yen were pushed to the following year, with the possibility of some receiving payments by the end of 2023.<sup>36</sup>

#### Analysis

The Mt. Gox bankruptcy shaped much of the early regulation and policymaking around web3 service providers. As the host, Japan responded to Mt Gox's collapse by implementing stricter regulations to enhance the security and reliability of crypto-asset exchanges. It eventually took web3 service providers into confidence by adopting a self-regulatory model of governance.<sup>37</sup> The Japanese Financial Services Agency

(JFSA) officially recognised Japan Virtual and Crypto Assets Exchange Association (JVCEA), a self-regulatory organisation (SRO) set up by crypto asset exchanges operating in Japan, to coordinate with public authorities and ensure regulatory agility.

Regulatory authorities also confronted the complex and interconnected nature of the web3 ecosystem. Funds stolen from Mt.Gox allegedly passed through BTC-e, a Russia-based crypto asset exchange before they reached the hackers' accounts.<sup>38</sup> The Mt. Gox bankruptcy thus underlined the need for international cooperation towards a more resilient and responsible web3 ecosystem by adopting standards that prioritise investor protection and market stability.

Several positive outcomes also emerged from this incident. Web3 service providers upgraded their security practices, by adopting robust measures to safeguard crypto assets in their custody. There was also a heightened awareness of the need for regulatory frameworks to protect investors and ensure market integrity.

Mt.Gox bankruptcy remains the seminal case for financial fraud and corporate mismanagement in the crypto asset exchange space – and has served as a benchmark for regulators around the world. With repayment to creditors finally within reach, it also shows that even in the most difficult cases, with minimal information, oversight and infrastructure, existing laws can be applied effectively to reach an equitable resolution.

## 2. USA v. Binance, 2023

### Brief Facts

Binance, a leading web3 service provider has been subject to two prosecutions, one with the SEC and another against the US Department of Justice (DoJ).

Binance Holdings Ltd., (offshore holding company) BAM Trading Services Inc., BAM Management US Holdings Inc., (*collectively*: US subsidiaries) and their founder Changpeng Zhao (Zhao) together ran Binance.com, a global crypto asset exchange, and Binance.US, a crypto asset trading platform for US residents (US trading platform).

In June 2023, the SEC filed charges against the offshore holding company, its US subsidiaries, and Zhao before the US District Court for the District of Columbia (USDCC). The SEC alleged that the group engaged in unregistered offer and sale of a crypto asset called Binance Coin (BNB), a stablecoin called Binance USD (BUSD) along with other crypto lending products without proper disclosures to investors. The US subsidiaries also misled investors about trading and market integrity controls over the American trading platform. SEC also alleged that the defendants deliberately sidestepped geo-restrictions by allowing US users to trade on its international platform. Further, it alleged that Zhao and the offshore holding company, exercised control of investor holdings in the US trading platform. This allowed them to divert billions of dollars to entities owned and controlled by Zhao called Sigma Chain and Merit Peak.<sup>39</sup> Sigma Chain allegedly engaged in manipulative trading that artificially inflated the platform's trading volume according to the SEC. These proceedings are still ongoing.<sup>40</sup>

In parallel, a multi-year investigation by the DoJ led to a three-count indictment for violations of US laws. The charges brought by the DoJ against the offshore holding company included failure to register with the

US Department of Treasury Financial Crimes Enforcement Network (FinCEN) as a Money Service Business, failure to institute appropriate AML/CFT and KYC checks, and violations of US economic sanctions under the International Emergency Economic Powers Act (IEEPA).

## **Analysis**

Binance's US operations were structured in a way as to preserve the technical separation between the offshore holding company and the two Delaware incorporated US subsidiaries' earnings from the US business were sent to the main exchange in the form of licence and service fees without threatening their legal separation. While the Delaware incorporated subsidiaries obtained licences from US regulators - particularly registration with FinCEN - the offshore holding company did not obtain licences or registrations in the US.

Despite announcing that US-based users would not be able to participate in the offshore holding company, large US investors and market makers were nonetheless allowed. The DoJ charged Binance to have developed and executed strategies to allow some high-volume 'VIP' users to continue to access the offshore holding company's platform.<sup>41</sup> An API plugin allowed some users located in the US (with American IP addresses) to provide non-US KYC information and access Binance.com.<sup>42</sup>

Since American users were allowed to transact on the unregulated offshore Holding Company's platform, Binance.com and Zhao were charged with the following:

- ***Failure to register as a Money Service Business***

Binance is an offshore crypto asset exchange that did business wholly or in substantial part within the United States, including by serving US customers. As such, it would qualify as a money transmitter and be required to register with FinCEN as a Money Service Business. As a Money Service Business, Binance would have been required to institute KYC checks, transaction monitoring controls (such as systems for suspicious transaction reporting) and implement an effective anti-money laundering program under the US Bank Secrecy Act.

- ***Violations of US economic sanctions***

Binance facilitated transactions for individuals located in jurisdictions subject to US economic sanctions. The US Department of the Treasury Office of Foreign Assets Control (OFAC) administers and enforces economic sanctions pursuant to the IEEPA. OFAC sanctions prohibit US persons from engaging in transactions with designated countries/ regions including but not limited to regions such as Cuba, North Korea, Iran, Syria, Crimea, Luhansk, and Donetsk.

Binance facilitated transactions worth millions of dollars between US users and users located in the sanctioned above regions. This included transactions for users who operated illegal mixing services, thereby facilitating the laundering of proceeds from darknet market transactions, hacks, ransomware attacks and scams.

On November 21, 2023, Binance.com, pleaded guilty to the above charges and agreed to pay over \$4 billion to resolve the Justice Department's investigation. Zhao also admitted to a deficient Anti-Money Laundering (AML) program, violating the Bank Secrecy Act, and resigned as CEO of Binance.<sup>43</sup> Under the plea deal, Zhao faced a \$50 million individual penalty and possible jail time. A sentencing hearing against Zhao is scheduled for February 2024.<sup>44</sup>

### 3. FTX case, 2023

#### Brief Facts

In November 2022, FTX, a crypto asset marketplace, filed for bankruptcy due to surge in customer withdrawals from concerns over undisclosed related-party transactions.<sup>45</sup> When reports of the same surfaced,<sup>46</sup> investors rushed to withdraw their funds and crypto asset holdings which resulted in a liquidity and solvency crisis for FTX.<sup>47</sup>

Sam Bankman-Fried, the founder of FTX, was indicted in December 2022 for alleged manipulation of funds between FTX and Alameda Research, a hedge fund he founded. SBF was accused of being part of a conspiracy to extract over \$8 billion from FTX customers and redirect it to his trading firm, Alameda Research.

According to the SEC, Bankman-Fried raised over \$1.8 billion from equity investors, with around \$1.1 billion coming from approximately 90 investors based in the United States. Bankman-Fried marketed FTX as a secure and responsible crypto asset trading platform, emphasising its advanced automated risk measures for safeguarding customer assets. However, the SEC complaint contends that Bankman-Fried engaged in a multi-year fraudulent scheme. SEC's allegations against Bankman-Fried from a corporate governance perspective include:<sup>48</sup>

- Diversion of investor funds from FTX to his privately-held crypto hedge fund, Alameda Research LLC, without disclosures.
- Providing undisclosed preferential treatment to Alameda Research on the FTX platform, including: (a) an almost limitless line of credit funded by FTX customers and (b) exemptions to Alameda from FTX risk safeguards.
- Withholding disclosures around risks associated with FTX's exposure to Alameda's holdings of overvalued, illiquid assets like FTX-affiliated tokens.

SBF extracted more than \$8 billion from FTX customers, funnelled it to his trading firm Alameda Research and then spent it for various purposes, including on Bahamian real estate, startup investments and political donations. The SEC claimed a jury trial before the United States District Court of the Southern District of New York had to determine questions of mismanagement and breach of trust with respect to FTX, and laundering investors' funds.<sup>49</sup>

#### Analysis

On November 2, 2023, the jury found Bankman-Fried guilty on all seven counts of fraud and conspiracy.<sup>50</sup> SBF violated the anti-fraud provisions under the Securities Act of 1933 and the Securities Exchange Act of 1934, which make defrauding, holding of money by use of misstatements or omissions in the course of business to defraud or deceit a person in transacting securities unlawful. The exact prison sentence will be determined at a hearing on March 28, 2024.

The FTX collapse, and the subsequent guilty verdict against Bankman-Fried by the New York jury, highlights the importance of corporate governance checks by web3 service providers.

Centralised crypto exchanges serve as repositories of investor trust. Investors trust that the custodial wallet provider that accesses their public and private keys will (a) not get hacked and lose the funds, (b) not misuse or abscond with the funds and (c) allow investors to withdraw their holdings upon demand.

Exchanges should therefore separate corporate funds from customer deposits, separate the crypto assets in their custody and funds / assets used for proprietary trading. Industry players should disclose transparency and audit reports, including via proof-of-reserves audit reports which establish that investor holdings in their custody are not misused or misstated as reserves in their accounts.

## 4. Gatecoin case, 2023

### Brief Facts

Gatecoin, a crypto asset exchange platform based in Hong Kong underwent liquidation in 2019. Kroll, a financial advisory solutions provider, was appointed as liquidators. The liquidators sought directions under the Hong Kong Companies (Winding Up and Miscellaneous Provisions) Ordinance (Winding Up Ordinance) on how to treat the crypto assets held by Gatecoin in the liquidation proceedings. The issue before the court of Hong Kong Court of First Instance (HKCFI) was whether Gatecoin held the crypto assets in trust on behalf of its customers, or whether it held the crypto assets in its own right.

The terms and conditions of the Gatecoin platform stated that:

- Gatecoin does not have any fiduciary duties towards its investors.
- Gatecoin does not segregate client assets from its own assets but rather mixed them together (both crypto assets and fiat currency);
- Gatecoin would use customer assets for proprietary trading and other purposes;
- Gatecoin would treat customer assets as its own assets, and customer deposits as liabilities, on its balance sheet.

After reviewing the terms and conditions, the HKCFI held that Gatecoin did not hold crypto assets in trust, and thus, it did not give directions on the mechanics of allocating assets in the liquidation proceedings.

### Analysis

In the Gatecoin case the HKCFI expressly recognised that crypto assets are property, following the position taken by the EWHC in *AA v Persons Unknown*. The court stated that crypto assets satisfy the four criteria laid down in the *Ainsworth* case and can form the subject matter of a trust.

In cases of fraud, liquidators will be able to recover or preserve crypto assets as though they were any other form of property belonging to the company for the benefit of creditors. However, the Gatecoin case highlights the importance of the language used in the terms and conditions of a service. Had the terms and conditions not disclaimed Gatecoin's responsibility towards investor funds and holdings, it would have had to return the same during the liquidation proceedings.

Investors should be aware of the risks of depositing assets with entities that do not ensure clear segregation of investor holdings and proprietary assets, and do recognize their ownership rights over crypto assets held in custodial wallets.

## Takeaways

### Existing rules can address key regulatory challenges surrounding centralised service providers in web3

Mismanagement, lack of accountability and governance controls stands out as a common thread across cases involving FTX and Binance. This manifests in the form of commingling of investor holdings for proprietary trades, externalisation of corporate structures for regulatory arbitrage, and issuance of misleading advertisements to investors and users. Implementation of baseline prudential controls and corporate governance standards can go a long way in addressing these issues.

The developments in USA v. Binance, and the FTX case, exemplify the efficacy of existing AML/CFT controls and corporate governance standards on centralised web3 service providers. For instance, Indian law has clear standards on corporate reporting, treatment of related party transactions, and conduct of intra-group lending. The principles underlying the above standards and rules would be effective to tackle the issues that arose in USA v. Binance and the FTX case.

The above cases indicate that adoption of global standards such as FATF guidance on AML/CFT standards, the FATF travel rule, and the OECD reporting framework for crypto assets can assuage regulatory concerns around KYC, AML/CFT, and capital flight. At the same time, it underlines the need for traditional financial institutions to adopt prudential controls over crypto asset exposures, including by adopting the recommendations issued by BIS.<sup>51</sup>

### How these issues are handled on an international level remains unclear

Authorities have been successful in taking enforcement action against non-compliances in the above cases – in particular those involving bankruptcy claims, like the Mt.Gox case and the FTX case. However, questions remain about how losses faced by customers can be restored, what the standards should govern such processes.

The Mt.Gox case has progressed for about a decade, and even now there is a lack of certainty around repayment to investors.<sup>52</sup> Given the global nature of the exchange, it serves as the first, and perhaps still, the most important case in the industry. The FTX case is perhaps equally significant. FTX had a large number of international clients, including about 5 lakh Indians.<sup>53</sup> The above developments highlight an urgent need for an international information sharing and dispute resolution mechanism for large cases involving market leaders.

Alternatively, the developments also suggest that strict regulatory guardrails should be placed on web3 offshore service providers, i.e., those that serve a market without establishing registered offices in that country / region. To illustrate, FTX Japan customers did not lose money (even though the platform wound down), due to a separate subsidiary and segregated offices.



## The nature of decentralisation.

#	Year	Court	Case
1	2021	United States District Court, District of Columbia	United States v. Sterlingov Criminal Action No. 21-399 (RDM) ( <i>Bitcoin Fog arrest</i> )
2	2022	United States District Court, Southern District of New York	Risley v. Universal Navigation Inc., 22 Civ. 2780 (KPF) (S.D.N.Y.) ( <i>Uniswap case</i> )
3	2023	United States District Court, Western District of Texas, Austin Division	Joseph Van Loon, et al. v. Department of Treasury, et. al., No. 1:2023cv00312 (W.D. Tex.) ( <i>Tornado cash case</i> )
4	2023	Court of Appeal of England and Wales	Tulip Trading Limited v Bitcoin Association For BSV & Ors [2023] 4 W.L.R. 16 ( <i>Tulip Trading case</i> )

### 1. Bitcoin Fog arrest, 2021

#### Brief Facts

The Internal Revenue Service (IRS) Criminal Investigations division arrested Roman Sterlingov, a Swedish-Russian national in 2021. He was accused of creating and operating Bitcoin Fog, a bitcoin “mixing” service on the dark web that took in coins from its users and returned others with the intention of preventing forensic accountants from following that money’s trail.<sup>54</sup>

The US DoJ accused Sterlingov of laundering more than 1.2 million Bitcoin worth \$336 million through Bitcoin Fog since 2011.<sup>55</sup> A major share of crypto assets traded on the platform came from darknet marketplaces and was linked to the narcotic trade and other illegal activities.<sup>56</sup>

An arrest warrant<sup>57</sup> for Bitcoin Fog’s founder, Roman Sterlingov, was successfully executed in April 2021.<sup>58</sup> Sterlingov filed a motion to revoke his pretrial detention before the USDCC. The issue before the Court was whether Sterlingov is liable for money laundering, operating an unlicensed money transmitting business, and money transmission without a licence in the District of Columbia.

#### Analysis

The Court noted that Bitcoin Fog’s advertised purpose was to enable users to evade detection by legal authorities and that Sterlingov allegedly went to extraordinary lengths to evade detection as Bitcoin Fog’s administrator.<sup>59</sup>

US authorities relied on blockchain forensics and tracing tools to identify Sterlingov’s culpability in the charges around money laundering and operation of unlicensed money transmitting business. USDCC denied Sterlingov’s motion to revoke pretrial detention in Nov, 2021.

## 2. Uniswap case, 2022

### Brief Facts

In April 2022, a class action lawsuit was filed against decentralised crypto exchange, Uniswap and its creator, Hayden Adams before the United States District Court Southern District of New York.<sup>60</sup>

The lawsuit alleged that Uniswap violated US securities laws by allowing scam tokens like EthereumMax (EMAX), Bezoge (BEZOGGE), and Alphawolf Finance (AWF) to be issued and traded on its platform. The claimants alleged that Uniswap caused harm to investors by not registering as an exchange or broker-dealer and sought accountability for losses incurred due to these 'scam tokens'.

The issue before the court was whether Uniswap was liable for the scam token issuance over its platform.

### Analysis

The court dismissed the lawsuit, stating that the actual defendants should be the issuers of the scam tokens, not Uniswap.<sup>61</sup>

The decentralised nature of Uniswap made identifying these issuers impossible, leading to the dismissal. The court also rejected the argument that Uniswap was liable for facilitating trades involving scam tokens, likening it to holding a payment application accountable for illegal transactions facilitated through its platform.

The court emphasised the absence of relevant crypto asset regulations and suggested that concerns regarding such issues should be addressed by Congress, highlighting the challenges posed by the current state of crypto asset regulation.<sup>62</sup>

The court ruling in the case was also significant as it classified popular crypto assets, specifically ether (ETH) and bitcoin (BTC), as 'commodities'.<sup>63</sup>

## 3. Tornado cash case, 2023

### Brief Facts

In August 2022, pursuant to an amendment to an Executive Order, the OFAC sanctioned Tornado Cash pursuant to an Executive Order for laundering \$7 billion worth of crypto assets since its creation in 2019 which included diversion of funds to Lazarus Group, a North Korean state-sponsored hacking group.<sup>64</sup>

The plaintiffs instituted a lawsuit against the US Department of Treasury and contested the legal authority of OFAC's decision to designate Tornado Cash as a sanctioned entity, arguing that it not only surpassed statutory limits but also infringed upon constitutional rights and posed a threat to the citizens for freedom and privacy of financial transactions.<sup>65</sup>

They argued that the sanctioning of Tornado Cash was unlawful under the IEEPA and the North Korea Sanctions and Policy Enhancement Act, 2016,<sup>66</sup> because Tornado cash was not a foreign 'national' or 'person'; the immutable smart contracts were not 'property'; and that even if Tornado Cash were a person, it

did not have an 'interest in property' with respect to the smart contracts. The plaintiffs further contended that the designation of Tornado Cash violates the First Amendment's Free Speech Clause.<sup>67</sup>

The co-founders of Tornado Cash, were also charged with conspiracy to commit money laundering, conspiracy to commit sanctions violations, and conspiracy to operate an unlicensed money transmitting business later that same month. The charges arose from creation and operation of Tornado Cash which was allegedly used to launder more than \$1 billion, including hundreds of millions that went to Lazarus Group.<sup>68</sup>

## Analysis

In August 2023, the Federal District Court for the Western District of Texas granted summary judgement for the US Department of Treasury and addressed the plaintiff's contentions:

- Designation as a 'Person' - The court determined that Tornado Cash, via its founders and participants in its DAO, qualified as a 'body of persons' pursuing a common objective, justifying its designation as a "person" under IEEPA.
- Property Interest in Smart Contracts - It held that Tornado Cash possesses a property interest in its immutable smart contracts, disagreeing with plaintiffs' arguments by deferring to OFAC's regulatory definitions. Those definitions encompassed "contracts of any nature whatsoever" supporting OFAC's determination that the smart contracts constitute property, or an interest in property.
- Beneficial Interest in Smart Contracts - The court concluded that Tornado Cash derived ongoing benefits from the smart contracts in the form of transmitted fees to the DAO.
- Constitutional Implications - Dismissing First Amendment concerns, the court ruled that the designation did not impede users' rights to donate anonymously or publish source code, as the right to privacy in transactions through any specific service is not constitutionally protected.

The court upheld OFAC's sanctions against Tornado Cash to include Tornado Cash on its Specially Designated Nationals and Blocked Persons List.

## 4. Tulip Trading case, 2023

### Brief Facts

Tulip Trading Limited (Tulip Trading) lost access to its Bitcoin valued at approximately \$4.5 billion following a hack on the computer of its CEO, Dr Craig Wright, during which the private keys needed to control the Bitcoin were deleted. Dr Wright had no other record of the private keys.

Dr. Wright filed suit against the developers of 16 blockchains including those associated with the BTC and BCH blockchains. Dr. Wright argued that the software engineers in charge of the relevant blockchains owed him a duty to prevent the hackers from dealing in the stolen property. That it would be simple for the developers to secure the inaccessible Bitcoin through a software patch and transfer it to a new wallet that Tulip could control.<sup>69</sup>

The EWHC declared that Tulip Trading had failed to establish a serious issue to be tried on the question of whether blockchain developers are under a legal duty to return lost or stolen digital assets to their rightful owners.<sup>70</sup> On appeal, the issue before the Court of Appeal of England and Wales was whether Bitcoin

software developers owed fiduciary or common law duties of care to those that use the code to trade or store their crypto assets.

The Court of Appeal found it conceivable that developers should, at least, have a ‘negative’ legal duty not to act in their own self-interest when acting in their capacity as network developers and, taking that a step further, owe a positive duty to actively fix system bugs when drawn to their attention. However, the Court noted that it would be a significant step to characterise positive duties as amounting to fiduciary duties. The court also observed that Bitcoin developers are a fluctuating body of individuals with the lack of an established structure. They aren’t bound by ongoing commitments to sustain their roles as developers or to implement future updates that might align with the interests of owners.<sup>71</sup>

Overall, the Court of Appeal found that the case raised a serious issue to be tried. Importantly, it did not go into the merits of Tulip Trading’s case, the Court of Appeal only examined whether it was serious enough an issue to allow an appeal. As things stand absent any further appeal by the developers, Tulip Trading’s case will proceed to trial.

## Analysis

Pinpointing responsibility on a particular developer or a group of developers is challenging given that they typically constitute a globally dispersed and constantly evolving group of individuals across various jurisdictions.

However, not all DLT systems are comparable in terms of decentralisation (or the lack of it) of control. For instance, in October 2022 Binance’s blockchain ‘BNB Chain’ was attacked by hackers. Binance promptly paused its network and thereby managed to avoid ~ \$400 million in losses.<sup>72</sup> This swift resolution was possible only due to the collaboration of its 26 validators, which triggered concerns regarding centralised control and vulnerabilities in its consensus mechanism.

## Takeaways



### **There is a lack of clarity around the concept of decentralisation in web3.**

In the Uniswap case, the US court differentiated between the decentralised trading platform and issuers of scam tokens thereon. On the other hand, in the Tornado Cash case and Bitcoin Fog arrest, the court held decentralised service providers responsible for violating OFAC sanctions and AML/CFT controls.

These developments indicate growing levels of regulatory stringency on platforms that enhance anonymity or obfuscate traceability. There should be clarity around what really is a decentralised platform to effectively affix responsibility and accountability on the various actors interacting thereon.

Interestingly, a report by Ciphertrace, financial intelligence entity in web3 states that *“blockchain forensics and tracing tools used in this case were misused to erroneously conclude that Mr. Sterlingov was the operator of Bitcoin Fog when no such evidence exists on-chain.”* It highlights the need for data and models used in blockchain analyses be reviewed, independently audited and transparent.<sup>73</sup> The discussion around the efficacy of the forensics and investigation processes underlines the need for greater research and development into how decentralised systems are built, operated, and managed.

## Takeaways

### **Questions around responsibility of developers are linked to the understanding of decentralisation in web3.**

The Tulip Trading It raised questions around whether developers' have discretionary decision-making authority in public blockchains such as Bitcoin, which justifies the existence of fiduciary duties.<sup>74</sup>

Developers play an indispensable role in shaping web3. Their decisions, coding choices, and updates directly impact the functionality and security of a DLT system or blockchain protocol. The role of developers extends beyond mere code creation; it encompasses ensuring the integrity of the network, addressing vulnerabilities, and responding to community concerns.

Developers often collaborate with each other for decentralised builds. This is a major departure from traditional notions of centralised authority and responsibility frameworks, and paves the way for greater emphasis on community governance through transparent and equitable consensus mechanisms. At the same time, this decentralised decision making also raises ethical considerations for developers. The decisions they make can have widespread implications, particularly if there are deliberate loop-holes or security vulnerabilities in the build. There is a growing need for the crystallisation of ethical coding practices, security audits, and adherence to community values.

Nevertheless, it is important to realise developers have as much control over a functioning public blockchain platform as miners, node operators, and even end users and investors. For example, in the case of bitcoin, anyone can verify and suggest alternatives to the open-source code. Developers cannot unilaterally enforce changes because miners, nodes, and end users can reject changes to the software if deemed undesirable. Unresolved disagreements among the various stakeholders results in hard-forks – such as Bitcoin Cash and BSV.

# 5.

## Key Takeaways for India

Having reviewed some of key case laws that shaped web3 over the last decade, we discuss some learnings for policymakers in India to consider.

First, crypto assets are a unique asset class consisting of heterogeneous tokens such as NFTs, stablecoins etc. The diverse opportunities they present, and the varying risks they pose should be harnessed and mitigated respectively under proportionate rules. Second, that existing money laundering, KYC and suspicious transaction reporting rules can go a long way in bringing regulatory visibility over the web3 ecosystem. Third, that the nuances of decentralised and interconnected DLT systems and platforms is yet to be understood in its entirety. India should look to foster global cooperation in this regard. And fourth, that adoption of emerging international web3 standards around information privacy, network security etc., should be encouraged to ensure that the Indian web3 ecosystem remains competitive and aligned with evolving global best practices.

### Box - Snapshot of legal and regulatory guardrails over the web3 ecosystem in India

**Taxation.** In India, centralized exchanges are subject to tax and money laundering regulations to operate legally and securely. The Finance Act, 2022, introduced a new provision in the Income Tax Act, 1961, that requires the person responsible for paying any sum to a resident seller as consideration for the transfer of a virtual digital asset to deduct tax at source (TDS) at the rate of 1% of the amount paid. The TDS is applicable only if the value or aggregate value of the consideration exceeds Rs. 10,000 in a financial year, except for a specified person, for whom the limit is Rs. 50,000.

---

**Anti-money laundering.** The Ministry of Finance, via a notification dated March 07, 2023, brought crypto assets under the ambit of the Prevention of Money Laundering Act, 2002, (PMLA).<sup>75</sup> The notification brings the exchange of crypto assets for fiat money, the exchange of one or more types of crypto assets, the transfer of crypto assets, the storage or management of crypto assets or tools that allow control over crypto assets, as well as involvement in and the delivery of financial services associated with an issuer's offer and sale of a crypto assets under the provisions of the PMLA. This means that centralized exchanges and other crypto-asset service providers have to register as reporting entities under the PMLA and comply with the anti-money laundering and counter-terrorism financing norms, such as maintaining an effective AML program, filing suspicious activity reports, and conducting customer due diligence.

---

**Cybersecurity.** The Indian Computer Emergency Response Team (CERT-In), a national agency under the Ministry of Electronics and Information Technology, issued cybersecurity directions for web3 service providers.<sup>76</sup> These primarily include requirements to maintain records, and report suspicious transactions and cybersecurity incidents.

**Advertising.** The Advertising Standards Council of India (ASCI), a self-regulatory organisation of the advertising industry issued 'Guidelines for advertising of Virtual Digital Assets and Linked Services' which focus on consumer awareness and empowerment. The ASCI guidelines are an important development towards standardisation of advertising norms in the web3 ecosystem.

## **1. Crypto assets have different properties to traditional assets and financial instruments, and should therefore have a unique taxonomy.**

Indian authorities highlight that the global nature of crypto assets necessitates common policy and regulatory frameworks. It is important therefore to trace the development of jurisprudence on the issue – particularly, developments in common law jurisdictions such as the UK, Hong Kong, and Singapore.

Common law courts have held that crypto assets meet the classic definition of 'property', based on their definability, identifiability, transferability, and permanence on the blockchain. They have also accepted the possibility of crypto assets being held on trust. In particular, the high court of Singapore in the ByBit case, 2023, declared a 'constructive trust' over the USDT that was siphoned off by the defendant for unjust enrichment. This suggests the possibility of adapting traditional legal concepts in property law and the law of trusts to accommodate the unique features of crypto assets. For instance, users who hold crypto assets in custodial wallets offered by web3 service providers can be treated akin to beneficial owners of traditional securities held by depositories. These recognitions provide a foundation for developing legal frameworks around ownership, transfer, and protection of crypto assets. Further, by recognizing the use of crypto assets as collateral, the high court of Singapore allowed the possibility for jurisprudence to develop around integrating crypto assets into financial systems, creating new avenues for traditional finance to intersect with crypto lending and DeFi.

However, SEC's application of the Howey test in cases like SEC v. Ripple Labs and SEC v. Terraform Labs. underlines the inherent heterogeneity among crypto assets. Not all crypto assets carry and confer the same rights – just as not all types of physical property are the same.

It is therefore important to develop a unique taxonomy for classifying crypto assets as different types of property.

## **2. It is possible to enforce existing legal and corporate governance principles on perpetrators of frauds and scams in web3.**

Centralised web3 service providers can be regulated using established principles from existing regulations. Recent cases such as the FTX Case, and USA v. Binance shows that enforcement of regulatory principles is possible even against the largest web3 enterprises. The impact of these cases

could have been mitigated had baseline corporate governance standards – such as arm’s length dealing of related party transactions been in place. Given the gulf in consumer trust as a result, web3 service providers must prioritise ethical governance practices and ensure transparency in the management of investor holdings.

The above cases highlight the criticality of well-defined regulatory frameworks, and the ensuing predictability it allows for businesses. While courts have granted emergency relief, including by repatriation of customer assets and restrictions on asset transfers, it is important that legislative and regulatory standards set out clear guardrails relating to registration, reporting and disclosure norms, investor protection standards and AML/CFT compliances.

In doing so, policymakers should avoid broad brushstrokes approaches to regulation. Distinctions between centralised and decentralised enterprises, between active and passive intermediaries, as well as onshore and offshore enterprises should be baked into the law.

As things stand, web3 service providers in India should adopt global best practices in terms of compliance measures and forge partnerships with other industry players to establish baseline standards on a proactive basis and adapt as technology progresses.

### **3. Global coordination to understand nuances around decentralisation should be a priority**

The nature of decentralisation, and decentralised entities is unique to web3. Traditional legal concepts around corporate governance may not apply neatly to these frameworks, and therefore need revisiting.

Decentralisation is a key facet of web3. However, some commentators argue that decentralisation on most blockchains and DLT systems is illusory because voting power is concentrated with only a small group of validators. These validators tend to act like gatekeepers in decision making and oversee the implementation of updates to the ledgers.<sup>77</sup> While the Tulip Trading case can have implications for how questions around developers’ responsibility will be addressed, UK courts are yet to examine the merits of the issue in appeal.

Be that as it may, web3 service providers have a duty of care to adopt while working on the blockchain networks. The responsibilities include ensuring that the users’ interest is at the forefront by building secure systems and acting in a positive manner by helping trace the actors during a hack or a fraud. At this juncture, policymakers in India should devise regulatory frameworks for entities and activities that can be regulated, particularly centralised service providers and issuers of crypto assets. They should in addition look to foster global consensus on how decentralised decision making, governance and issuance of assets should be regulated.

### **4. Industry should proactively adopt emerging international standards**

Policymakers should encourage web3 service providers to pre-emptively comply with global best practices around data security, investor protection, fraud-risk assessments etc. These best practices should be concretised through the adoption of standards, and self-declarations before industry associations such as the Bharat Web3 Association. To this end, developers, web3 service providers and stakeholders such as rights organisations in India should collaborate on identifying key technical standards that should be adopted by industry players irrespective of legislative or regulatory mandates.



Global organisations such as the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and Open Standards bodies like the Institute of Electrical and Electronics Engineers (IEEE) have developed critical technology standards relevant to blockchain and web3 service providers.<sup>78</sup> These standards encompass a range of aspects including information security management system standard that evaluates an organisation's ability to safeguard sensitive data (ISO 27001:2013), privacy and personally identifiable information protection considerations within blockchain systems (ISO/TR 23244:2020), technical aspects of smart contracts, discussing their functionality and interactions within blockchain systems (ISO/TR 23455:2019), security management for digital asset custodians, covering threats, risks, and controls related to custodian services (ISO/TR 23576:2020) and others.<sup>79</sup> Complementing these ISO standards, IEEE 2140.1-2020 emerges as a standard aimed at ensuring quality, transparency, fairness, and security within crypto asset exchanges.

This IEEE standard places emphasis on consumer protection, ethical business practices, and technical requirements for exchanges. Though these standards do not comprehensively cover core blockchain security controls, digital asset custodian business risks, asset segregation, or governance aspects, the businesses in web3 can comply with these standards to begin with. Risk based approach could be taken to deal with other aspects.

In the light of maintaining standards and transparency, web3 service providers should aim to have their technical systems audited by independent agencies proactively. They should develop IT policy, third party risk assessment policy, hold training and awareness among its members and ensure that vendors and third parties maintain the standards through an audit when dealing with their systems as far as possible. Periodic audits can provide users with confidence in the integrity and accountability of the centralised platforms within the ecosystem.

# 6.

## Way forward

Our discussion highlights the increasing sophistication in the discourses surrounding the treatment of crypto assets and web3 service providers. Development of judicial precedents compliments the commitments made at the G20 level towards global cooperation on policy frameworks, enforcement, outreach, and data collection.

Indian law implicitly treats crypto assets as a form of property through the levy of capital gains tax on crypto assets. It governs web3 service providers as reporting entities under PMLA from a KYC and AML/CFT perspective. However, challenges remain, particularly around the treatment of offshore service providers and technology that obfuscates regulatory visibility. These challenges are heightened by existing transaction taxes over crypto transactions in India - which have resulted in an increase in offshore trading activity by Indian investors.

The ongoing appeal in Tulip Trading case reflects a significant development in common law jurisprudence around the responsibility of developers of blockchain and DLT systems. While more accountability should be placed on developers and service providers, they should also be made active stakeholders in the development of standards and regulation.

The web3 ecosystem stands at the intersection of several sectors, markets and disciplines including engineering, mathematics, and economics. No one public authority is thus equipped to manage this space. It is important that regulatory architectures recognise the need for a diversity of perspectives, and adopt participatory models of governance.

Co-regulatory or self-regulatory models of governance take the developer community and service providers into confidence in establishing and enforcing best practices at an industry wide level. These include existing ISO standards on web3, along with specialised codes of conduct for the novel aspects of web3 such as voting and governance of decentralised autonomous organisations, and operation of initial coin offerings. Many industry players such as onshore web3 service providers in India proactively follow global standards in terms of KYC, transaction monitoring, security, suspicious transaction reporting etc. Recognition of these steps under co-regulatory or self-regulatory frameworks can reduce the legal vacuum caused by the absence of a parliamentary law over crypto assets and web3. Such measures are more attuned to the globally pervasive character of the web3 ecosystem than regulatory models that try to circumscribe crypto markets within jurisdictional free zones.

Looking ahead, while courts have provided clarity on questions around corporate governance, liability of decentralised platforms, etc. it will be interesting to see how the discourse matures even further into the nuances of the web3 ecosystem. In the meanwhile, governments should focus on creating level playing fields in the market, and allowing participatory models of governance so those who are held accountable in web3 are made responsible for developing rules and standards.

# Endnotes

- 1 Staff Report, The HinduBusinessLine, "Supreme Court refuses to entertain plea to frame guidelines for regulation of trading of cryptocurrencies," November 11, 2023, Available at: <https://www.thehindubusinessline.com/money-and-banking/supreme-court-refuses-to-entertain-plea-to-frame-guidelines-for-regulation-of-trading-of-cryptocurrencies/article67524077.ece>.
- 2 Filecoin is an open-source cloud storage marketplace, protocol, and decentralised storage network. See <https://filecoin.io/>.
- 3 Bored Ape Yacht Club. See <https://boredapeyachtclub.com/>.
- 4 Solidity is a powerful programming language which allows developers to define the rules and behavior of decentralized applications (DApps) on the Ethereum blockchain. Available at <https://soliditylang.org/>.
- 5 Staff report, Coinbase Research & insights, "How DAOs can reshape business foundations," February 25, 2022, Available at: <https://www.coinbase.com/institutional/research-insights/resources/education/how-daos-can-reshape-business-foundations>.
- 6 State of Wyoming Bill No. SF0038, Wyoming Decentralized Autonomous Organization Supplement, Available at: <https://www.wyoleg.gov/Legislation/2021/SF0038>.
- 7 A Wells Notice is a notification issued by regulators to inform individuals or companies of completed investigations where infractions have been discovered.
- 8 Jenna Rennie, "Recovering the ransom: High Court confirms Bitcoin status as property" White & Case, February 10, 2020, Available at: <https://www.whitecase.com/insight-alert/recovering-ransom-high-court-confirms-bitcoin-status-property>.
- 9 Staff report, "Crypto assets case law: How far have we come?," Addleshaw Goddard, August 18, 2022, Available at: <https://www.addleshawgoddard.com/en/insights/insights-briefings/2022/dispute-resolution/crypto-assets-case-law-how-far-have-we-come/>.
- 10 UK Jurisdiction Taskforce, "Legal statement on cryptoassets and smart contracts," November 2019, Paragraph 39, Available at: [https://www.blockchain4europe.eu/wp-content/uploads/2021/05/6.6056\\_JO\\_Cryptocurrencies\\_Statement\\_FINAL\\_WEB\\_111119-1.pdf](https://www.blockchain4europe.eu/wp-content/uploads/2021/05/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf).
- 11 *Ibid* Paragraph 63.
- 12 Staff report, "UKJT Legal Statement on Cryptoassets and Smart Contracts aims to give market confidence that England & Wales is a crypto-friendly jurisdiction," Herbert Smith Freehills, December 16, 2019, Available at: <https://hsfnotes.com/tm/2019/12/16/ukjt-legal-statement-on-cryptoassets-and-smart-contracts-aims-to-give-market-confidence-that-england-wales-is-a-crypto-friendly-jurisdiction/>.
- 13 Emi Lacapra, "What is Ripple: Overview, history and XRP cryptocurrency" CoinTelegraph, Available at: <https://cointelegraph.com/learn/what-is-ripple-a-beginners-guide-for-understanding-ripple>.
- 14 Scott Mascianica, et al., "SEC v. Ripple: When a Security Is Not a Security," Holland & Knight Alert, July 20, 2023, Available at: <https://www.hklaw.com/en/insights/publications/2023/07/sec-v-ripple-when-a-security-is-not-a-security>.
- 15 Jody Godoy, "US SEC drops claims against two Ripple Labs executives," Reuters, October 20, 2023, Available at: <https://www.reuters.com/markets/us/sec-dropping-claims-against-ripple-executives-court-filing-2023-10-19/>.
- 16 US Securities and Exchange Commission, "Framework for "Investment Contract" Analysis of Digital Assets," Available at: <https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets>
- 17 *Supra* Note 15.
- 18 An institutional constructive trust is a trust that arises through operation of law, regardless of the parties' intentions, where it would be unconscionable to allow a legal owner to retain beneficial ownership of property.
- 19 ByBit Fintech Ltd v Ho Kai Xin and others [2023] SGHC 199, July 25, 2023, Paragraph 35, Available at: [https://www.elitigation.sg/gd/s/2023\\_SGHC\\_199](https://www.elitigation.sg/gd/s/2023_SGHC_199).
- 20 *Ibid*, Paragraph 36.

- 21 US Securities and Exchange Commission Press Release, “SEC Charges Terraform and CEO Do Kwon with Defrauding Investors in Crypto Schemes” February 16, 2023, Available at: <https://www.sec.gov/news/press-release/2023-32>.
- 22 Sam Reynolds, “SEC Asks Court for Summary Judgement Against Do Kwon, Terraform,” CoinDesk, November 3, 2023, Available at: <https://www.coindesk.com/policy/2023/11/03/sec-asks-court-for-summary-judgement-against-do-kwon-terraform/#:~:text=Terraform%20and%20Kwon%20also%20engaged,while%20secretly%20arranging%20third%2Dparty>.
- 23 Camomile Shumba, Sandali Handagama, “Retail Crypto Investors in Emerging Economies Hit Hardest by FTX, Terra Collapses: BIS,” CoinDesk, February 21, 2023, Available at: <https://www.coindesk.com/markets/2023/02/20/retail-crypto-investors-in-emerging-economies-hit-hardest-by-ftx-terra-collapses-bis/>.
- 24 Jesse Coghlan, “Do Kwon and Terraform Labs ask judge to toss SEC’s lawsuit,” CoinTelegraph, October 31, 2023, Available at: <https://cointelegraph.com/news/do-kwon-terraform-labs-request-sec-suit-dismiss-district-court>.
- 25 *Supra* Note 22.
- 26 Nelson Wang, “Paxos ‘Categorically Disagrees’ With SEC That BUSD Is a Security, Says It Will Litigate if Needed,” CoinDesk, February 14, 2023, Available at: <https://www.coindesk.com/policy/2023/02/13/paxos-categorically-disagrees-with-sec-that-busd-is-a-security-says-it-will-litigate-if-needed/>.
- 27 André Beganski, “Paxos Says It’s ‘Prepared to Vigorously’ Fight SEC Lawsuit,” Decrypt, February 14, 2023, Available at: <https://decrypt.co/121225/paxos-says-its-prepared-to-vigorously-fight-sec-lawsuit>.
- 28 US Securities and Exchange Commission, Crypto Assets and Cyber Enforcement Actions, November 19, 2022, Available at: <https://www.sec.gov/spotlight/cybersecurity-enforcement-actions>.
- 29 PricewaterhouseCoopers, PwC Global Crypto Regulation Report 2023, December 19, 2022, Available at: <https://www.pwc.com/gx/en/new-ventures/cryptocurrency-assets/pwc-global-crypto-regulation-report-2023.pdf>.
- 30 Teuta Franjkovic, “Circle Steps into Binance vs SEC Case — Asserts Stablecoins Aren’t Securities,” CCN, September 29, 2023, Available at: <https://www.ccn.com/news/circle-says-stablecoins-are-not-securities-binance-sec/>.
- 31 International Monetary Fund, Elements of Effective Policies for Crypto Assets, February 23, 2023, Available at: <https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-Assets-530092?cid=pr-com-PPEA2023004>.
- 32 *Ibid.*
- 33 Financial Stability Board, “Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of “Global Stablecoin” Arrangements,” October 11, 2022, Available at: <https://www.fsb.org/wp-content/uploads/P111022-4.pdf>.
- 34 Section 19, Indian Copyright Act, 1957.
- 35 Robert McMillan, “The Inside Story of Mt. Gox, Bitcoin’s \$460 Million Disaster”, WIRED, March 3, 2014, Available at: <https://www.wired.com/2014/03/bitcoin-exchange/>.
- 36 Jamie Redman, “Mt Gox Repayment Delayed Again: Creditors Await BTC, BCH, and Yen Payments Until 2024,” Bitcoin.com, September 22, 2023, Available at: <https://news.bitcoin.com/mt-gox-repayment-delayed-again-creditors-await-btc-bch-and-yen-payments-until-2024/>.
- 37 William Suberg, “Japan Finally Gets Self-Regulatory Body For Cryptocurrency Exchanges,” CoinTelegraph, April 24, 2018, Available at: <https://cointelegraph.com/news/japan-finally-gets-self-regulatory-body-for-cryptocurrency-exchanges>.
- 38 Emma Roth, “Feds charge two men for the \$400 million Bitcoin hack that took down Mt. Gox,” The Verge Jun 9, 2023, Available at: <https://www.theverge.com/2023/6/9/23755376/mt-gox-bitcoin-hack-russians-charged>.
- 39 Staff Report, “Binance CEO’s trading firm received \$11 billion via client deposit company: US SEC,” Economic Times, June 08, 2023, Available at: <https://economictimes.indiatimes.com/tech/technology/binance-ceos-trading-firm-received-11-billion-via-client-deposit-company-us-sec/articleshow/100838165.cms>.
- 40 SEC v. Binance Holdings Limited, Bam Trading Services Inc., Bam Management Us Holdings Inc., And Changpeng Zhao, Civil Action No. 1:23-cv-01599, Available at: <https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf>.

- 41 Binance’s VIP users were granted a set of special privileges, including an early heads-up from the crypto exchange if they were under investigation by law enforcement, according to the US Treasury’s Financial Crimes Enforcement Network. See MacKenzie Sigalos, “Binance warned VIP customers about law enforcement investigations, Treasury says,” CNBC, November 21, 2023, Available at: <https://www.cnn.com/2023/11/21/binance-warned-vip-customers-about-investigations-treasury-says.html>.
- 42 United States of America v. Binance Holdings Limited, CR23-178 RAJ, Paragraph 33, Available at: <https://storage.courtlistener.com/recap/gov.uscourts.wawd.328551/gov.uscourts.wawd.328551.1.0.pdf>.
- 43 US Department of Justice, Office of Public Affairs, Press Release, “Binance and CEO Plead Guilty to Federal Charges in \$4B Resolution,” November 21, 2023, Available at: <https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution>.
- 44 James Morales, “CZ Prison Term: How Long a Sentence Will Binance Founder Face After Guilty Plea?,” CCN, November 22, 2023, Available at: <https://www.ccn.com/news/cz-prison-term-binance/>.
- 45 Alex Hern and Dan Milmo, “What do we know so far about the collapse of crypto exchange FTX?,” The Guardian, November 18, 2022, Available at: <https://www.theguardian.com/technology/2022/nov/18/how-did-crypto-firm-ftx-collapse>
- 46 Ian Allison, “Divisions in Sam Bankman-Fried’s Crypto Empire Blur on His Trading Titan Alameda’s Balance Sheet,” CoinDesk, November 2, 2022, Available at: <https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/>
- 47 Sage D. Young, Bradley Keoun, “The Epic Collapse of Sam Bankman-Fried’s FTX Exchange: A Crypto Markets Timeline,” CoinDesk, November 12, 2022, Available at: <https://www.coindesk.com/markets/2022/11/12/the-epic-collapse-of-sam-bankman-frieds-ftx-exchange-a-crypto-markets-timeline/>.
- 48 US Securities and Exchange Commission Press Release, SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX, December 13, 2022, Available at: <https://www.sec.gov/news/press-release/2022-219>.
- 49 United States v. Bankman-Fried, Civil Action No. 22-cv-10501. Available at: <https://www.sec.gov/files/litigation/complaints/2022/comp-pr2022-219.pdf>.
- 50 Eli Tan and Tory Newmyer, “Bankman-Fried convicted on all charges after weeks-long criminal trial”, The Washington Post, November 2, 2023, Available at: <https://www.washingtonpost.com/business/2023/11/02/sbf-bankman-fried-trial-ftx/>.
- 51 Basel Committee on Banking Supervision, “Prudential treatment of cryptoasset exposures,” December 2022, Available at: <https://www.bis.org/bcbs/publ/d545.pdf>.
- 52 Parikshit Mishra, “Infamously Hacked Crypto Exchange Mt. Gox Delays Repayment Deadline by a Year,” CoinDesk, September 21, 2023, Available at: <https://www.coindesk.com/business/2023/09/21/mt-gox-pushes-repayments-by-a-year/>.
- 53 Laxitha Mundhra, “FTX Collapse Has Impacted Nearly 5 Lakh Indians: Crypto Exchange Giottus,” Inc42, December 3, 2022, Available at: <https://inc42.com/buzz/ftx-collapse-has-impacted-nearly-5-lakh-indians-crypto-exchange-giottus/>.
- 54 US Department of Justice, Office of Public Affairs, Press Release, “Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency “Mixer,” April 28, 2021, Available at: <https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer>.
- 55 Nikhilesh De, “US Officials Arrest Alleged Operator of \$336M Bitcoin Mixing Service,” CoinDesk, April 28, 2021, Available at: <https://www.coindesk.com/markets/2021/04/27/us-officials-arrest-alleged-operator-of-336m-bitcoin-mixing-service/>.
- 56 Andy Greenberg, “Feds Arrest an Alleged \$336M Bitcoin-Laundering Kingpin,” WIRED, April 27, 2021, Available at: <https://www.wired.com/story/bitcoin-fog-dark-web-cryptocurrency-arrest/>.
- 57 United States v. STERLINGOV, 1:21-mj-00400, (D.D.C. Apr 27, 2021) ECF No. 5, April 27, 2021, Available at: <https://www.courtlistener.com/docket/59856080/5/united-states-v-sterlingov/>.
- 58 *Supra* Note 55.
- 59 United States v. Sterlingov Criminal Action No. 21-399, Criminal Action No. 21-399 (RDM), Available at: [https://www.govinfo.gov/content/pkg/USCOURTS-dcd-1\\_21-cr-00399/pdf/USCOURTS-dcd-1\\_21-cr-00399-0.pdf](https://www.govinfo.gov/content/pkg/USCOURTS-dcd-1_21-cr-00399/pdf/USCOURTS-dcd-1_21-cr-00399-0.pdf).
- 60 Risley v. Universal Navigation Inc., 22 Civ. 2780 (KPF) (S.D.N.Y.), Available at: <https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2022cv02780/577791/90/>.

- 61 Sandali Handagama, “U.S. Court Calls ETH a Commodity While Tossing Investor Suit Against Uniswap,” CoinDesk, August 31, 2023, Available at: <https://www.coindesk.com/policy/2023/08/31/us-court-calls-eth-a-commodity-while-tossing-investor-suit-against-uniswap/>.
- 62 André Beganski, “Uniswap Lawsuit Dismissed: DeFi Crypto Exchange Not Liable for ‘Scam Tokens,’” Decrypt, August 31, 2023, Available at: <https://decrypt.co/154312/uniswap-lawsuit-dismissed-defi-crypto-exchange-not-liable-for-scam-tokens>.
- 63 *Supra* Note 62.
- 64 US Department of the Treasury, Press Release, “U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash,” August 8, 2022, Available at: <https://home.treasury.gov/news/press-releases/jy0916>.
- 65 Staff Report, “Tornado Watch: Popular Cryptocurrency Mixer “Tornado Cash” Dealt Two Major Blows in a Week,” Dechert LLP, September 7, 2023, Available at: <https://www.dechert.com/knowledge/onpoint/2023/9/tornado-watch--popular-cryptocurrency-mixer--tornado-cash--dealt.html>.
- 66 North Korea Sanctions and Policy Enhancement Act of 2016, As Amended Through P.L. 116–92, Enacted December 20, 2019, Available at: <https://www.govinfo.gov/content/pkg/COMPS-11985/pdf/COMPS-11985.pdf>.
- 67 Joseph Van Loon, et al. v. Department of Treasury, et. al., 1:23-CV-312-RP, Available at: <https://cases.justia.com/federal/district-courts/texas/txwdce/1:2023cv00312/1211705/94/0.pdf>.
- 68 United States Attorney’s Office, Southern District of New York, Press Release, “Tornado Cash Founders Charged With Money Laundering And Sanctions Violations” August 23, 2023, Available at: <https://www.justice.gov/usao-sdny/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations>.
- 69 Jordan Atkins, “Landmark coin recovery settlement set to usher in a new era for digital assets,” CoinGeek, June 10, 2022, Available at: <https://coingeek.com/landmark-coin-recovery-settlement-set-to-usher-in-a-new-era-for-digital-assets/>.
- 70 Sophie Nappert, “Tulip Trading Limited v Bitcoin Association & Others: What Duties for Blockchain Platforms and Core Developers?,” Kluwer Arbitration Blog, June 1, 2022, Available at: <https://arbitrationblog.kluwerarbitration.com/2022/06/01/tulip-trading-limited-v-bitcoin-association-others-what-duties-for-blockchain-platforms-and-core-developers/>.
- 71 Graham Lovett and Michael Stewart, “Tulip Mania—Do Blockchain Developers Owe Duties to the Owners of Crypto Assets?,” Akin, April 12, 2022, Available at: <https://www.akingump.com/en/insights/alerts/tulip-mania-do-blockchain-developers-owe-duties-to-the-owners-of-crypto-assets>.
- 72 Josh Adams, Michael Washburn, “Crypto Needs to Confront Its Decentralization Myth, Say Experts”, BeinCrypto, September 8, 2023, Available at: <https://beincrypto.com/crypto-confront-decentralization-myth/#:~:text=The%20Decentralization%20Myth%20is%20a%20Running%20Concern%20in%20Web3&text=Lido%20Finance%20now%20holds%20almost,%2C%20with%20Lido%20holding%2032.5%25>.
- 73 Defense Expert Report, United States v. Roman Sterlingov 21-CR00399 (RDM), Ciphertrace, August 7, 2023, Available at: <https://storage.courtlistener.com/recap/gov.uscourts.dcd.232431/gov.uscourts.dcd.232431.159.1.pdf>.
- 74 Staff Report, “Is the decentralised governance of Bitcoin a myth? Court of Appeal finds real issue to be tried as to whether developers owe fiduciary duties to Bitcoin owners,” Herbert Smith Freehills, February 13, 2023, Available at: <https://hsfnotes.com/litigation/2023/02/13/is-the-decentralised-governance-of-bitcoin-a-myth-court-of-appeal-finds-real-issue-to-be-tried-as-to-whether-developers-owe-fiduciary-duties-to-bitcoin-owners/>.
- 75 Aanchal Magazine and Soumyarendra Barik, “Finance Ministry brings crypto assets under Prevention of Money Laundering Act: What are the implications?,” The Indian Express, March 10, 2023, Available at: <https://indianexpress.com/article/explained/explained-economics/crypto-assets-pmla-explained-8486629/>.
- 76 Staff Report, “New CERT-In Rules On Crypto, VPN, Cloud Service Providers Comes Into Effect From June 2022,” Outlook Money, May 5, 2022, Available at: <https://www.outlookindia.com/business/new-cert-in-rules-on-crypto-vpn-cloud-service-providers-comes-into-effect-from-june-2022-news-195061>.
- 77 *Supra* Note 70.
- 78 Global Blockchain Business Council, Technical Standards, Available at: <https://gbbccouncil.org/gsmi/technical-standards/>.
- 79 International Organization for Standardization (ISO) Standards for Blockchain and distributed ledger technologies. Available at: <https://www.iso.org/search.html?q=blockchain>.



KOAN CoinDCX