

BRITISH VIRGIN ISLANDS

Nia Statham & Shaun Reardon-John
Baker & Partners

This chapter forms part of:

CRYPTOASSETS
Law Over Borders Comparative Guide 2026

www.globallegalpost.com/lawoverborders

1. Are cryptoassets (including, for example, cryptocurrencies, stablecoins and non-fungible tokens) defined and, if so, what are the major elements?

Distinctions between various cryptocurrency and virtual asset types are not explicitly drawn under the Virtual Assets Service Providers Act, 2022 (VASP Act), which is the British Virgin Islands' (BVI) primary piece of legislation for regulating virtual asset activity. Instead, a digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes, will be regarded as a "virtual asset".

However, digital representations of fiat currencies, other assets or matters specified in the applicable guidelines and digital records of a credit against a financial institution of fiat currency, securities or other financial assets that can be transferred digitally are excluded from the "virtual assets" definition. Stablecoins also fall within the definition of virtual assets (see also the Financial Action Task Force (FATF) report titled Targeted Report on Stablecoins and Unhosted Wallets, published in March 2026).

2. What are the major laws/regulations specifically related to cryptoassets?

The BVI Financial Services Commission (FSC) is the key regulatory body in the BVI with respect to virtual assets service providers (VASPs), which are profiled in response to Question 4 below.

As noted earlier, the VASP Act is a cornerstone of the BVI's regulatory framework for the virtual assets sector and is applicable to all entities operating in or from within the BVI that qualify and are registered as VASPs. The VASP Act also permits entities (upon obtaining regulatory approval) to participate in a regulatory sandbox. This regulatory sandbox is governed by the Financial Services (Regulatory Sandbox) Regulations, 2020 and the Regulatory Sandbox Guidelines.

Additionally, section 3(2) of the VASP Act expressly states that the provisions of the: Proceeds of Criminal Conduct Act (as Revised); Proliferation Financing (Prohibition) Act, No. 20 of 2021; Counter Terrorism Act, No. 33 of 2021; Anti-money Laundering Regulations (as Revised) (AML Regulations); Anti-money Laundering and Terrorist Financing Code of Practice (as Revised) (AMLTF COP); and other enactments relating to money laundering, terrorist financing and proliferation financing generally apply to virtual assets and VASPs as they apply to other BVI entities (subject to any necessary modifications to ensure an appropriate application to virtual assets and VASPs). Further guidance which has been issued specifically with respect to VASPs also includes the Guidance on Regulation of Virtual Assets in the Virgin Islands, July 2020 (Virtual Asset Guidance), the VASP Guide to the Prevention of Money Laundering, Terrorist Financing and Proliferation Financing (VASP AML Guide), the BVI FSC's Guidance on Application for Registration of a Virtual Assets Service Provider (VASP Registration Guidance) and the VASP Travel Rule Guidance.

Other ancillary legislation that virtual asset service providers may engage includes:

- the Securities and Investments Business Act (as Revised) (SIBA);
- the BVI Business Companies Act (as Revised);
- the Financing and Money Services Act (as Revised); and
- the Economic Substance (Companies and Limited Partnerships) Act (as Revised).

3. How are different types of cryptoassets regulated?

As mentioned above, the VASP Act does not regulate specific categories of virtual assets but, similarly to other offshore jurisdictions, is focused on regulating the activities of virtual asset service providers.

For example, several activities are not caught by the VASP Act in the BVI, which generally speaking includes the issuance of virtual assets. However, it is worth noting that certain activities associated with issuance may be caught by the VASP Act, and that issuance as an activity may engage other regulations; in each case, advice should be sought.

Issuing is a core function of any Web3 project which can go to the project's ability to fundraise (i.e. via the launch of meme coins and NFTs and in the context of decentralised autonomous organisations (DAOs) its governance tokens that attach voting rights, which can all be acquired for value). Additionally, tokens which are issued can have repatriation functions built into their architecture to mitigate against token loss, which can greatly assist with digital asset recovery and enforcement efforts (although incorporating such repatriation functions is not legally required – but see also the FATF's targeted report on stablecoins).

Issuers can direct (on instruction) the allocation of a token supply, the concentration of which can impact the token's overall value if bulks of tokens held by a few holders are sold all at once. Centralised token supplies can also predetermine the outcome of a vote put to a community of token holders in the context of a DAO.

Votes may be cast to (for example) influence the development of a DAO's protocol and/or signal a DAO community's agreement to the outbound transfers of the DAO's virtual assets stored in its treasury wallets.

The mining of virtual assets is also generally considered to be excluded from regulatory oversight (which is the case in other offshore jurisdictions) subject to relevant provisions of the Virtual Asset Guidance. Mining is the means of generating new virtual assets (i.e. which enables a private entity or other legal persons to generate and privately amass virtual asset wealth without the need for any regulated intermediaries) which can then be used to directly invest, trade, store, transfer or exchange (i.e. for other virtual assets or for goods and services with payment deposited into a seller's wallet).

In its Virtual Asset Guidance, the FSC has also adopted the position that, where virtual assets are used solely as payment for goods and services which provide the purchaser with an ability to only purchase goods and services (such as utility tokens), these will not be captured by financial services legislation. This would also extend to airline miles and credit card awards.

There is also a recognition that virtual asset activity can overlap with other regulated activities, such as investment activities, which risks engaging other regulatory licensing regimes at once. To prevent duplicating regulatory oversight, the VASP Act expressly states that a person registered as a VASP under the VASP Act is not required to obtain a licence under SIBA, the FMSA or the Business Licensing Act, 2022.

However, in its Virtual Asset Guidance, the FSC has taken the view that, where a virtual asset conveys additional investment rights (e.g. profit share, debt, interest, a mutual fund, which in a virtual assets context may take the form of staking, yield farming or participating in an investment or for-profit DAO), this virtual asset

arrangement may fall under SIBA. On the face of it, this guidance would appear to exclude digital asset treasury companies (DATCs), as DATCs are generally publicly listed or private companies, and the share price and overall valuation of the company can be heavily influenced by the performance of the underlying digital assets held in the company's digital asset treasuries. However, digital asset treasuries may, in some cases, fall within the scope of a custodian arrangement and in the event of any uncertainty, the FSC should be approached for guidance.

A discussion on the anti-money laundering (AML) regimes applicable to virtual assets is found below.

4. Is there an authorisation/licensing regime applicable to cryptoasset issuers/providers/exchanges and, if so, what are the requirements?

As mentioned above, there is no licencing regime applicable to cryptoasset issuers in the BVI. However, the FATF has recently recommended that entities involved in stablecoin arrangements, such as issuers, are subject to clear and enforceable AMC/CFT obligations, that they limit issuance on high risk blockchains and they incorporate repatriation functions into a stablecoin token's architecture. The VASP Act also establishes a comprehensive registration regime for all entities carrying on a virtual asset service which operates in or from within the BVI (as outlined below) which is supported by the VASP Registration Guidance. As of July 2025, 14 VASPs have been registered with the FSC and it is estimated that as many as 80 applications may currently be before the FSC for consideration. According to the VASP Registration Guidance, the FSC will endeavour to process an application and provide initial comments within six weeks of receipt, with a view to concluding the application process within six months of the initial submission date. However, this timeline will be dependent on the quality of the application and supporting information submitted.

Under the VASP Act, a VASP provides, as a business, a virtual assets service and is registered under the VASP Act to conduct one or more of the following activities or operations for or on behalf of another person:

- exchange between virtual assets and fiat currencies;
- exchange between one or more forms of virtual assets;
- transfer of virtual assets between addresses or accounts;
- safekeeping or administration of virtual assets, or instruments allowing control over them;
- participation in and provision of financial services related to an issuer's offer or sale of a virtual asset; or
- any other activity specified in the VASP Act or by regulations.

Engaging in virtual asset services on behalf of another person under the VASP Act will include:

- hosting wallets or maintaining custody or control over another person's virtual assets, wallets, or private keys;
- providing kiosks (such as ATMs, Bitcoin teller machines, or vending machines) that facilitate virtual asset transactions, including exchanges between virtual assets for fiat currency or other virtual assets; and
- engaging in any other activity classified as a virtual asset service or virtual asset issuance under future guidelines.

This means entities operating a virtual asset exchange or offering custody services must register as a VASP in the BVI.

To register as a VASP, applicants must use the FSC's prescribed form, and must clearly indicate the specific category of registration being sought. The application must also be accompanied by, among other things:

- a business plan outlining the virtual asset activities to be undertaken, the knowledge and expertise of the person applying for registration and information on how the VASP will be marketed;
- information (together with supporting evidence to demonstrate that the FSC's "fit and proper" requirements have been satisfied) on the proposed directors, senior officers, and compliance officer;
- the applicant's proposed policies and procedures for complying with its obligations under the VASP Act and the applicable AML, Countering Terrorist Financing and Proliferation of Weapons of Mass Destruction Financing legislative framework; and
- payment of the required application fee.

Upon approval, the FSC will issue a certificate of registration, and may impose any conditions it deems appropriate, such as a requirement to obtain professional indemnity insurance.

All entities must be registered with the FSC before engaging in any activities governed by the VASP Act.

5. Is the promotion of cryptoassets to consumers or investors regulated and, if so, how? Are there specific rules for crypto advertising and influencer promotion?

There are no specific requirements with respect to the deployment of paid internet and social media influencers in support of a VASP's marketing activities. However, section 24 of the VASP Act makes provisions for dealing with misleading advertisements and statements which apply where a VASP is conducting any activity that involves the exchange, transfer, safekeeping, administration, participation in or provision of virtual assets or in relation to any virtual asset business (regardless of whether or not those activities are carried on by the VASP and whether or not the activity is one that the VASP is authorised to carry on). Under those circumstances, the VASP is prohibited from causing or permitting to be made, a statement, promise or forecast which the VASP either knows, or is reckless as to whether it is false, misleading or contains incorrect statements of fact, or dishonestly conceals a material fact.

Similar prohibitions apply to VASPs when issuing, or causing or permitting to be issued, an advertisement, brochure or similar document relating to virtual asset activities. If the FSC is of the opinion that an advertisement, brochure, similar document, statement, promise or forecast (issued or to be issued/made by or for a VASP) breaches these prohibitions or is contrary to public interest, it may:

- direct the VASP in writing not to issue (or to withdraw) the document or statement, promise or forecast;
- approve issuance/the making of the document, statement, promise or forecast, but with such changes as specified by the FSC.

Additionally, and subject to some limited exceptions, registered VASPs are prohibited from engaging in marketing activities with respect to any virtual assets for its own benefit which may be detrimental to the interests of its clients.

Contravening the relevant provisions of the VASP Act which concern misleading advertisements and statements is an offence punishable by a pecuniary penalty and/or imprisonment under certain circumstances.

However, these robust regulatory protections with respect to marketing may not guarantee equivalent protections against possible pump-and-dump or rug-pull scams, as they do not extend to token issuances (which is not a licenced activity). In addition, these protections will also not extend to the issuance of DAO governance tokens, and the associated advertisements concerning the purpose of the DAO or Web3 project and how it will ultimately apply the community's funds (in the event that the DAO's governance token supply is centralised or there is unilateral control over the DAO's treasury wallets). In each case, these tokens can be sold both publicly and privately to facilitate fundraising or govern investment activity (see Question 2 above).

6. How are cryptoasset custodians regulated?

A custodian under the VASP Act is anyone who accepts for safekeeping virtual assets or instruments that enable a VASP to exercise control over them, and is a regulated activity (see Question 4, above). No person may provide virtual asset custody services in or from within the BVI without being registered by the FSC.

To provide custodial services, the BVI entity when applying to the FSC for a VASP licence must provide additional information with its application that (for example): confirms the facilities it has to enable the safekeeping of virtual assets; confirms the measures it has in place to ensure the segregation of clients' virtual assets; and discloses information about the risks associated with the VASP's safekeeping arrangements in addition to the security measures it has in place to ensure the integrity of those safekeeping arrangements.

The VASP Act also requires that custodians take appropriate steps to safeguard virtual assets against theft and loss, and take steps to limit or mitigate against any risks that may be associated with the safekeeping arrangements of those virtual assets. This includes ensuring that the custodian has adequate security measures in place for safeguarding purposes and has the organisational and management resources to safeguard clients' virtual assets.

Custodians are also required to enter into safekeeping arrangements with the owner of the virtual assets being custodied with respect to the duration of the safekeeping arrangement, the manner in which the client's virtual assets are to be held, the transactions that the VASP can engage in, and how those transactions are to be conducted. Custodians must also disclose any risks associated with these safekeeping arrangements to the client. Disclosures with respect to fee arrangements, the manner in which the client's virtual assets may be accessed and the remedies available to clients in the event that their virtual assets are lost or stolen, also form part of the minimum requirements that apply to safekeeping arrangements between regulated custodians and their clients under the VASP Act.

Sourcing and adopting best practices in information technology for virtual asset safekeeping is also expected of custodians, in addition to ensuring: (a) that any ancillary or subsidiary proceeds from the virtual assets accrue to the virtual asset owner unless agreed otherwise; and (b) that custody providers do not encumber or cause client assets to be encumbered without specific agreement from those clients.

There are also general and continuing compliance duties, as well as obligations to maintain and keep sufficient records. Whilst there are no provisions under the VASP Act which impose a strict obligation on a custodian to maintain insurance, obtaining insurance may be a condition imposed by the FSC before issuing a licence (per the VASP Registration Guidance). These custodian rules may apply to a DAO's and project's treasury wallets when managed by a BVI entity (depending on the circumstances of each case). In the event of uncertainty, the FSC should be approached for guidance.

7. What anti-money laundering requirements apply to cryptoassets?

The AML Regulations and the AMLTFCOP were amended to bring VASPs within the scope of the BVI's AML/CFT framework.

The VASP AML Guide provides (amongst other things) that VASPs are required to conduct comprehensive risk assessments and maintain robust Client Due Diligence (CDD) (otherwise known as Know Your Customer) procedures. They must also appoint a compliance officer to develop and implement a compliance framework and, more topically (given increased reports at the time of writing concerning threat and state actors infiltrating FinTech companies through recruitment processes), VASPs must screen employees to ensure their suitability for handling AML/CFT controls, in addition to allowing for immediate sanctions screening.

The VASP Travel Rule Guidance also applies to registered VASPs when a transaction involving virtual assets is valued at USD 1,000 or more. The FATF's Travel Rule essentially mandates that VASPs assess the regulatory risks posed by counterparty VASPs and perform due diligence assessments of those counterparties. Where a transaction amounts to less than this, the VASP Travel Rule Guidance will not apply unless the aggregate of any linked transactions exceeds this value, or there is a suspicion of money laundering.

Together, the AMLTFCOP, the VASP AML Guide and the Travel Rule Guidance emphasise the importance of monitoring transactions, especially those involving foreign VASPs, and highlight the risks associated with privacy coins, cryptocurrency mixers, and the use of decentralised platforms (such as decentralised cryptocurrency exchanges and bridging services) in connection with illicit activity. Additionally, VASPs must implement mechanisms for filing suspicious activity reports to the BVI's Financial Investigations Agency, and ensure compliance with sanctions screening requirements.

8. How is the ownership of cryptoassets defined or regulated?

The ownership of virtual assets is not expressly dealt with under BVI statute but is rather informed by the BVI courts' common law approach, which has

confirmed that cryptocurrencies are a form of property (see *Philip Smith and Jason Kardachi v. Torque Group Holdings Limited (in liquidation)* BVIHC(COM) 0031 of 2021).

In *Torque*, the range of virtual assets that were subject to the decision included virtual assets which had been issued by a centralised issuer (such as Tether) and virtual assets which had been mined (including Bitcoin and Ether). In total, Bitcoin, Ether, Tether, Litecoin, Ripple, Tron, Bitcoin Cash and Torque were all subject to the determination in *Torque*.

The BVI court did not draw a distinction between the characteristics of each virtual asset in the judgment at the time it was made. This blanket approach taken by the BVI court signals that ownership rights can arguably attach to any virtual asset regardless of how it was created. In the context of fraud, it is also important to note that “ownership” of virtual assets does not necessarily correlate with its control or *lex situs* (i.e. its location), which are issues that are frequently considered together by the BVI courts in digital asset recovery cases.

In *Torque*, the virtual assets in question were held to be assets for the purposes of Torque’s liquidation, and the ownership of those assets was attributed to Torque where it could evidence that it had both exclusive control over those assets and knowledge of the private keys to the wallets which the digital assets were assigned to. The BVI court’s approach was guided by the UK Jurisdiction Taskforce’s (UKJT) Legal Statement on Cryptoassets and Smart Contracts (“Legal Statement”). However, on its face this approach would arguably have left victims of frauds and thefts in the cold who would typically have no knowledge of a bad actor’s whereabouts or identities, and no knowledge of the bad actors’ private keys to wallets which held misappropriated virtual assets, but would still want to assert ownership rights in them.

For the purposes of establishing jurisdiction, in *Russell Crumpler and Christopher Farmer v. Cheong Jun Yoong and Three Arrows Capital Ltd (in liquidation)* BVIHC(COM) 2023/003/BVIHCCOM 2022/0119, the BVI court determined that despite Three Arrows being domiciled in the British Virgin Islands and asserting ownership rights in disputed virtual assets, the *lex situs* of the virtual assets in dispute was tethered to their central management and control. This was held to be in Singapore on the basis that the company’s directors, its fund management and administrators, its headquarters, its operations and the preparation of its financial statements were all conducted from there. In addition, the sole holder of the private keys to the wallets which stored a high proportion of disputed virtual assets, was also located in Singapore.

The issue of ownership v. control in a virtual asset context is multi-faceted as the way in which a virtual asset is created can also sometimes mean that control is not only limited to which wallet address a virtual asset is assigned to (and therefore limited to those who possess knowledge of the private key to that wallet address), but rather whether the virtual asset has a centralised issuer which can (a) control its onward transfer; and (b) burn and re-issue it to the correct wallet address as a means of repatriation on the blockchain.

This issue was before the BVI court when it was asked to consider the *lex situs* of virtual assets in the context of whether to grant a freezing injunction against a “well-known” operator and issuer of cryptocurrency.

In *AQF v. XIO and Ors* BVIHCCOM 2023/0239, *ex parte* proceedings were brought against a non-cause of action respondent token issuer with respect to a virtual asset investment scam. The applicant was seeking to obtain a freezing injunction against the token issuer, who had the capability of centrally controlling the token supply it had issued. This control could extend to freezing certain tokens that it had issued, despite those tokens allegedly having been misappropriated from the victim and assigned to a bad actor's wallet addresses.

When considering whether to grant the injunction against the BVI token issuer, the *lex situs* of the virtual assets was examined by the BVI court, which again, informed by the UKJT Legal Statement, was guided by whether there was any "centralised control" of those tokens in the jurisdiction. Because the issuer was domiciled in the BVI and could control the functions and onward travel of the virtual assets it had issued, the BVI court accepted at the *ex parte* hearing that the *lex situs* of those virtual assets was the BVI (despite these virtual assets being assigned to wallets on a decentralised blockchain controlled by persons unknown who possessed knowledge of the private keys to those wallets and likely resided outside of the jurisdiction).

Where available, this alternative recovery strategy helps remove some of the limitations which the reasoning in *Torque* may inadvertently have placed on victims of fraud, hacks and thefts. In addition to token issuers, the approach adopted in *AQF v. XIO and Ors* could arguably also extend to other intermediaries which exert control over third parties' virtual assets, including any operators of a BVI-domiciled protocol (such as a bridging protocol, which locks or vaults native virtual assets in wallets under its control), any BVI-domiciled custodians and BVI-domiciled cryptocurrency exchanges, which control the virtual assets that are deposited with it.

9. How are Decentralised Autonomous Organisations (DAOs) treated?

DAOs are virtual associations of anonymous or pseudo-anonymous token holders which typically enjoy voting rights and operate on a decentralised and open-source blockchain ledger. DAOs, as a virtual community of voters, can sit adjacent to an automated protocol, the development of which the DAO's voting community may be able to influence but not directly control without the intervention of others (such as hiring software developers via a legal wrapper (see below) to maintain or upgrade it). They can also behave as decentralised fundraising vehicles.

Whether a DAO is truly decentralised will depend on whether the allocation of the DAO's supply of governance tokens has been sufficiently diluted amongst a pool of unrelated and independent token holders, or whether the token supply has been concentrated in the wallet addresses controlled by a few of the DAO's insiders or participants.

DAOs can have many varied functions, ranging from charitable fundraising, philanthropic, non-profit and operational to commercial, for-profit and investments, but often they issue community or governance tokens native to each, which carry voting rights that can be acquired for value or allocated to holders

at the token's launch. Votes are needed to pass proposals put to the DAO's community to, for example, decide on how a DAO's protocol should develop, or how a DAO's funds stored in a DAO's treasury wallet(s) (akin to a publicly viewable bank account hosted on a blockchain network) should be spent and/or transferred away. For that reason, the allocation of tokens that carry voting rights can pre-determine the outcome of votes which have financial consequences for token holders and investors alike.

There is no bespoke regulatory regime which applies to DAOs in the BVI but the VASP Act and possibly other legislation mentioned above may be engaged depending on the activities of the DAO and any BVI corporate intermediary that either engages with, or represents it (generally referred to as a legal wrapper). These interactions may extend to the DAO's underlying protocol, treasury wallet(s) and virtual assets stored therein.

By themselves, DAOs cannot produce "know your customer" information, which prevents them from accessing regulated services. They also risk failing to achieve legal recognition, which impacts the DAO's ability to validly enter into legally enforceable contracts, and/or courts may infer that they have formed a general partnership or association (which would result in anonymous holders of tokens being jointly and severally responsible for the actions of the other). Although whether a BVI court would make such an inference in the case of a native DAO has yet to be determined.

It is generally thought that, in order for token holders to limit their liability in a DAO, and particularly to purchase real-world assets, access regulated services, open accounts at banks and regulated cryptocurrency exchanges and enter into legally binding agreements (i.e. to hire software developers to maintain the protocol or engage the services of signatories to approve outbound transfers from a DAO's treasury wallet where multiple authorisations are required), DAOs will adopt a legal wrapper(s) to represent them. These can be bespoke vehicles (some of which have been introduced in the United States), but more often than not they will be regular corporate entities and/or "ownerless" companies (which are gaining traction in the Web3 space). These entities will present as a regular corporate client to regulated institutions and businesses and there will often be no suggestion that they represent a project or DAO, particularly where there is no requirement for legal wrappers to: (a) disclose that they represent a DAO or Web3 project; (b) record which projects and DAOs they represent; and (c) do not need to share the same name as the project or DAO that they represent – making it difficult to link them together.

In *Hector Enterprises Inc v. Hector DAO & Ors* BVIHCCOM 2024/0072, the BVI court determined for the purposes of a receivership application, that the *lex situs* of the DAO's virtual assets was the BVI, on the basis that its legal wrapper, which was used for off-chain transactions and contracting with service providers, was domiciled in the BVI. In addition, multiple signatories were required to authorise outbound transactions from the DAO's treasury wallet and notably, those signatories had been contracted by the BVI legal wrapper to provide signatory services to the DAO. Therefore, despite these signatories being located outside of the jurisdiction, as a whole, the BVI was considered to have the closest nexus with the DAO's digital assets.

Where a BVI corporate entity (such as a company limited by guarantee, a company limited by shares, or a charitable trust) is adopted as a legal wrapper, guidance should be sought by the FSC where that BVI entity may be caught by the VASP Act, SIBA or other BVI regulations, depending on the activities and purpose of the DAO, the BVI entity's nexus to the DAO it has agreed to represent and the functions it will perform on the DAO's behalf.

10. Are there any particular laws or rules which apply in the event of the crypto bankruptcy or insolvency?

At the time of writing, there are no bespoke insolvency or asset recovery regimes which apply to the virtual asset sector or DAOs in the BVI. As such, the BVI's usual insolvency framework will apply, which comprises the following legislation: the Insolvency Act (as revised and amended), the Insolvency Code of Practice (as amended), the Insolvency Practitioners Regulations (as amended) and the Insolvency Rules.

As mentioned above in *Torque*, virtual assets have been held to be property, although as our adoption of virtual assets becomes increasingly sophisticated and mainstream, the BVI's general approach to how certain categories of virtual assets may be classified in law could gradually change (and in the absence of any statutory developments or interventions in the interim).

Where creditors can claim and sufficiently demonstrate a proprietary right in those virtual assets, they should obtain a higher priority claim in a BVI liquidation.

When an entity enters a regular (rather than voluntary) liquidation, the BVI court will appoint regulated insolvency practitioners to take command of the liquidation, gather in the entity's assets (both real world and virtual, which may necessitate an investigation using blockchain analytics tools to trace those virtual assets) and make distributions to admitted creditors (which may require special software solutions in order to verify that distributions are being made to the correct creditors, where they were only previously known as anonymous holders of virtual assets to the entity during its lifespan).

Liquidators may also encounter challenges in identifying the Centre of Main Interest (COMI) of both a DAO or a VASP where: a BVI entity's virtual asset activities take place outside of the jurisdiction and/or where the control and administration of the entity's virtual assets and/or where the group's operations were performed outside of the BVI, and/or where the group's operations were performed outside of the BVI and/or in an anonymous and seemingly decentralised manner (i.e. through employing remote contractors who use virtual personal networks when conducting business on behalf of the BVI entity and/or its group).

Liquidators may also apply for Chapter 15 recognition in the United States. In the case of *Hector DAO* and following the appointment of receivers to its treasury wallet (see *In re Hector DAO* (Bankr. D.N.J. July 15, 2024)) the BVI receivership was recognised as a foreign main proceeding and the DAO was treated as a "debtor" under the U.S. Bankruptcy Code. This was the first cross-border insolvency of a DAO to obtain Chapter 15 recognition in the United States, where all of the debtor's management functions existed only in smart contract code, a blockchain address and token holder votes, rather than a bricks and mortar company with offices, headquarters and a memorandum and articles of association.

11. Is a smart contract enforceable as a legal contract?

As the BVI recognises common law principles of contract (i.e. offer, acceptance, consideration and intention), it follows that should a smart contract be formed in accordance with these established legal requirements, the BVI courts would likely entertain arguments that such smart contracts are legally binding and enforceable as standard contracts are in the usual course.

12. What recourse does a victim of crypto fraud have?

Actions

Victims of virtual asset fraud may bring the same types of civil recovery claims as victims in a regular fraud could otherwise bring, including:

- civil remedies such as breach of trust and breach of fiduciary duties;
- personal claims such as unjust enrichment, conspiracy, dishonest assistance and knowing receipt;
- proprietary and tracing claims such as fraudulent disposition, deceit and fraudulent misrepresentation (amongst other things); and
- claims under the BVI's insolvency framework brought by a BVI entity's liquidators, including setting aside transactions.

However, the nature of the interest in the virtual assets being recovered will vary as will the availability of tracing information (as some issuers maintain their own internal ledgers which clearly show where a token they have issued is at any one time). How digital assets have been laundered and whether they have travelled through a cryptocurrency exchange or mixer will also impact tracing and proprietary claims. Together, all these factors will affect whether a victim has a proprietary or equitable claim in the virtual assets, and how they can be traced in law. It is also possible to bring claims for regulatory breaches, and filing a criminal complaint is usually the first step taken by victims of a virtual asset fraud or theft.

Recovery tools

Third party disclosure orders – virtual asset tracing challenges

Where virtual assets are traced to a centralised cryptocurrency exchange (regardless of whether it is regulated or not, but depending on the type of virtual asset being traced) tracing cannot generally be performed beyond this point as the virtual assets are often co-mingled in omnibus wallets hosted by that exchange, and only the exchange will know how those assets were administered and whether they have left the exchange.

Under those circumstances, the liquidators and claimants alike will likely need to apply for a third-party disclosure order (otherwise known as a Norwich Pharmacal order) against the exchange for:

- information on whether the virtual assets are still housed there;
- information on the identities of any account holders (to the extent that any CDD is required to open an account at that exchange); and
- further tracing information where the virtual assets have left the exchange.

If virtual assets have been traced to a registered account held by a Cayman Islands "ownerless" Foundation Company (Cayman Foundation), or if the account has been registered to a BVI entity which has a Cayman Foundation as its parent, then

the ultimate beneficial ownership information housed at a regulated centralised cryptocurrency exchange will typically be limited to the Register of Directors and Register of Supervisors of the Cayman Foundation. This will be the case when the Foundation Company has become “ownerless,” as no current shareholder information will be available where those shares have been cancelled. As directors and supervisors can be the same legal person (i.e. a corporate service provider which offers both types of services) which also provided the company’s formation services, then this same legal person may also be the only recorded shareholder on the Register of Members of the Cayman Foundation prior to its shares being “cancelled”. Under those circumstances, the CDD taken by a regulated cryptocurrency exchange (or any other regulated service provider for that matter which onboards ownerless vehicles or subsidiaries of ownerless vehicles) may have very little tracing value and could be limited to just the details of the corporate service provider. The CDD will not reveal, for example, who founded the ownerless company, or who ultimately gives instructions to the directors and supervisors where the Cayman Foundation acts as a legal wrapper/parent of a legal wrapper and/or issuer for DAOs or Web3 projects, and may be dealing with the DAO’s virtual assets on its behalf. Under those circumstances, a further Norwich Pharmacal order may be required and served on the corporate services provider which will increase the costs of civil recovery efforts. Combined with the fact that companies in most jurisdictions are not required to disclose or keep a record of which Web3 projects and DAOs they represent, limited information is being collected by regulated cryptocurrency exchanges and regulated service providers alike, which poses a barrier to digital asset tracing and recovery efforts.

Freezing orders/tokenised freezing orders/Anton Piller orders

It is also possible to obtain freezing orders against cryptocurrency exchanges, protocols, issuers, directors and signatories to wallets (amongst others). In *Chainswap Limited v. The Owner of Digital Wallet & Ors* BVIHC(COM) 2022/0031, the BVI court granted a worldwide freezing order against persons unknown, permission to serve out by alternative means and a letter of request to Croatian authorities seeking evidence from a cryptocurrency exchange domiciled in Croatia. It is also worth noting that courts in other jurisdictions (such as Singapore and Hong Kong; see *M31 Capital Partners, LP and another v. Various Defendants* HC/OC 371/2023 and *Worldwide A-Plus Investments Ltd v. A-Plus Meta Technology Ltd* [HCA2417/2024], respectively) have made orders for tokenised worldwide freezing orders to be served directly on target wallet addresses. Whilst these tokens (which are Airdropped to wallet address(es) subject to the freezing order) do not freeze the wallet or prevent the onwards transfer of virtual assets contained therein, tokenised freezing orders can be detected upon screening by some cryptocurrency exchanges and other DeFi services when monitoring transactions. To this end, these service providers may be able to impose an informal freeze on the virtual assets received from a wallet subject to a tokenised freezing order and/or file a suspicious activity report and/or contact the party with the benefit of the freezing order, where the provider is on notice that those virtual assets are subject to it and where they may be in breach of the freezing order themselves by having received those virtual assets.

In some cases, the whereabouts of the private keys to wallets containing misappropriated virtual assets may be known and/or the private keys (or their shards) may be stored or recorded in some physical and/or partitioned by a virtual medium. In those cases, Anton Piller orders can be obtained to effect a physical or virtual seizure for analysis and investigation.

Alternative service – NFT airdrops and chat boxes

Alternative service has also been ordered by the BVI courts in virtual asset cases, which extends to service of proceedings by way of a non-fungible token airdrop (see *AQF v. XIO and Ors*). With respect to DAOs, in *CFTC v. Ooki DAO*, C.A. No. 3:22-cv-5416, the United States District Court for the Northern District of California granted a motion to serve proceedings on the Ooki DAO by electronically depositing it in the DAO's help chat box, as well as posting it contemporaneously on the DAO's online forum. Whilst the issue of effecting service on a DAO has not been publicly considered by the BVI courts at the time of writing, this case serves as a helpful precedent when trying to effect traditional legal processes in a Web3 environment.

Appointment of receivers and liquidators

It is also permissible in the BVI to make an application for the appointment of interim receivers to a wallet or treasury wallet address (see *Hector DAO*). If there has been a fraud on a DAO, the DAO's token holders may, subject to the terms of the smart contract governing the DAO's protocol and any applicable voting thresholds, pass a resolution authorising the appointment of BVI receivers to the DAO's treasury wallet and/or to transfer the DAO's virtual assets to a more secure wallet address under the control of the receivers.

This happened in the case of the Hector DAO, where BVI receivers were appointed following a community DAO vote. Following the vote, the receivers took positive steps to ensure that any orders sought from the BVI court stipulated that the receivership served the collective interests of the Hector DAO's token holders. These steps likely helped the Hector DAO to secure the world's first Chapter 15 recognition in the United States (as discussed above), which confirms that a receivership could be considered a collective process under the U.S. Bankruptcy Code.

It is also open for victims of fraud to apply to wind up a BVI entity on a just and equitable basis for the purposes of installing either provisional or official liquidators to investigate the affairs of the BVI entity and its involvement in any potential fraud.

Insolvency processes

More inexpensive options may include filing a proof-of-debt claim if the BVI entity is in liquidation, or filing a statutory demand in certain cases (which, if unchallenged or if unsuccessfully resisted) could result in the BVI entity being placed into liquidation.

Delivery up

It is also important to note that, given the prevalence of protocols and issuers in the BVI, it may be possible (subject to obtaining a judgment confirming the

victim's proprietary or equitable rights to certain virtual assets under their control) to make an application for an order of delivery up against certain issuers and protocols as a non-cause defendant, in the event that misappropriated tokens are capable of being transferred, "burned" and/or "re-issued".

Practical considerations of digital asset recovery

Where virtual assets are accessible and capable of being secured, those pursuing a digital asset recovery may also need to consider transferring the entity's virtual assets into third-party custodian wallets in order to mitigate the possibility of a potential hack, exploit or theft. In addition, this arrangement helps protect against the risk that the integrity of wallets formerly operated by staff or controllers of the BVI entity in liquidation or subject to a recovery action may have been compromised, where copies of the private keys may have been made.

Some custodian wallets may also need to be established on different blockchains as not all virtual assets are supported on the same blockchain networks. In that case, claimants and liquidators alike will need to be mindful of the hidden costs of paying for multiple custodian wallet addresses across different blockchain networks during the lifespan of any proceedings, and/or may consider converting these digital assets into fiat currencies and/or stablecoins in order to lower the running costs of taking custody of virtual assets that are subject to the conclusion of an uncertain legal process.

In the context of liquidations, the liquidators in *Torque* sought to convert various virtual asset types into the stablecoin Tether, which required an application for sanction from the BVI court before doing so.

A similar sanction application would also be required when the time comes for liquidators to distribute the entity's virtual asset holdings, but no case law has been publicly handed down in the BVI as to the valuation of creditor claims where the virtual assets in question are susceptible to market volatility.

Some creditors may also wish for proceeds to be distributed *in specie* where their virtual assets may have appreciated in value over the course of the liquidation. However, should the liquidators obtain sanction to liquidate an entity's virtual asset stockpile into fiat or a stablecoin, care must be taken to ensure that there will be no adverse impacts on the wider crypto markets (which may be the case in very large bankruptcies). Certain debt restructuring options may also be considered (which has been known to involve a part payment of virtual assets and tokens through the creation of a DAO) but this is not considered further here. There is also the possibility that recovery targets in the BVI operated as an unauthorised VASP, in which case it may be possible to involve the FSC.

Cross-border enforcement

Due to discords in how virtual assets are treated in law by various jurisdictions, cross-border enforcement and insolvency with respect to both virtual assets and DAOs may prove highly problematic. For example, where virtual assets which are subject to a BVI judgment are traced to a cryptocurrency exchange in a civil law jurisdiction which has not yet codified virtual assets into its legal framework, novel, untested and therefore higher-risk legal strategies may be required in an attempt to persuade those local courts that virtual assets, protocols, cryptocurrency exchanges, DAOs and

their respective innovative functions are comparable to traditional institutions and the codified legal principles that apply to them (such as banking and trust law).

Additionally, cross-border enforcement may be highly dependent on enforcing a BVI judgment or Order against the signatories to a wallet containing the virtual assets which are subject to the judgment or Order. Where a wallet requires more than one person to authorise the transfer out of virtual assets (i.e. a quorum of signatories, say four out of six) then being able to identify those signatories is important, otherwise an Order which attaches a penal notice will have little effect, where there is no one identifiable to fine or imprison in the event of contempt. Although not always the case, signatories may be dispersed around the globe and are known to use pseudonyms as there are relevant safety issues which apply to individuals who are administering high value wallets. This means their real identities may also not be verified or securely recorded. As such, compelling the transfer out of virtual assets from wallets administered by persons unknown and outside the BVI is another barrier to digital asset recovery due to the absence of verifiable information taken from signatories.

Global unharmonised approaches to the legal treatment of digital assets pose a serious challenge to cross-border digital asset recovery, and increases the risk that judgments obtained in the BVI (or any other jurisdiction which recognises virtual assets as a form of property) may be very hard to enforce in jurisdictions which have not considered the issue before or have reached a different determination. These disparities in cross-border enforcement give threat and state actors the opportunity to play virtual asset recovery arbitrage, by purposefully moving virtual assets, conducting operations and/or adopting legal wrappers for off-ramping purposes in jurisdictions with no or little regulation and/or regulated jurisdictions which have weak legal arrangements (i.e. lightly regulated corporate vehicles which can evade registering as a VASP) in order to evade digital asset recovery.

Without an international insolvency and cross-border recovery regime for virtual assets and DAOs, the field of digital asset recovery will remain an uneven one for victims of virtual asset fraud and theft.

13. Are there tax implications specific to cryptoassets?

At the time of writing, the BVI government does not impose or collect tax on income (unless that income has arisen in the BVI), capital gains tax or value-added tax, and does not impose tax or duties on gifts, profits, inheritance or estates. As a result, the taxation of virtual assets and decentralised finance activities is, for the most part, not a practical concern under current BVI law and no guidance with respect to the tax treatment of virtual assets has been issued. However, the BVI International Tax Authority announced on 23 October 2025 that it will be implementing the Crypto-Asset Reporting Framework with reporting to begin in 2027. In addition, where a BVI subsidiary is held by a Cayman Foundation (which is a quasi-trust legal arrangement) as its parent, the Cayman Foundation can extinguish or elect not to designate any beneficiaries (despite the existence of a beneficial interest in tokens or other assets it may handle on behalf of others), which may avoid triggering a tax obligation in certain jurisdictions altogether.

14. What are the data privacy and cybersecurity obligations for cryptoasset businesses?

The VASP Act establishes explicit disclosure requirements for VASPs where client assets have been unlawfully interfered with or otherwise compromised. Upon the VASP first becoming aware of such a failure, the VASP must immediately notify the client and the FSC, and inform them both of the steps the VASP intends to take to restore the client's assets and protect those assets from further compromises.

The Data Protection Act, 2021 also imposes clear obligations for individuals and entities processing personal data in the BVI, including those using equipment in the BVI for processing data. Under this legislation, several key principles apply which determine the data privacy rights of data subjects, including the Notice and Choice Principle, the Disclosure Principle, the Security Principle, the Retention Principle, the Data Integrity Principle and the Access Principle. However, as the Information Commissioner has not yet been established, the relevant enforcement regime is not fully operational.

Cybersecurity concerns are also addressed under the Computer Misuse and Cybercrime Act, 2014 (as amended; CMC Act), which was enacted in the BVI to secure computer material and prohibit unauthorised access, modification, or interference with such material, as well as the misuse of computers. The CMC Act applies to any person, regardless of nationality or citizenship, within or outside the BVI, and covers offences committed partly or wholly outside the BVI.

15. How are staking, yield farming, and other DeFi activities regulated?

Engaging in derivative transactions linked to investment assets may constitute a regulated investment activity under SIBA. Accordingly, a BVI entity carrying on such business will typically need to obtain the appropriate authorisation. That said, where a derivative-related activity falls within the regulatory perimeter of the VASP Act, it may be exempt from separate authorisation under SIBA (as noted above). In any case, the FSC should be approached for guidance.

16. Are there any other ongoing legal or regulatory consultations or other legal frameworks in the pipeline relating to cryptoassets?

Whilst not specifically related to VASPs, but still relevant to them, an amendment to the BVI Business Companies and Limited Partnerships (Beneficial Ownership) Regulations 2024 came into effect on 2 January 2025. Beneficial ownership information in the BVI was stored centrally and privately on the BOSS system, which was established under the Beneficial Ownership Secure Search System Act, 2017. The BOSS system has since been replaced with a new regime to collect beneficial ownership using an existing system known as VIRRGIN, which is relied upon for company filings and searches in the BVI. Beneficial ownership information will now be made available under a new "legitimate interest" regime which came into force on 1 April 2026 and makes beneficial ownership information available based on demonstrable legitimate interest. As mentioned above, the BVI International Tax Authority has also announced on 23 October 2025 that will be implementing the Crypto-Asset Reporting Framework, with reporting set to begin in 2027.

AUTHOR BIOGRAPHIES**Nia Statham**

Nia Statham is a Senior Associate admitted in the BVI, Cayman Islands, and England and Wales. Nia specialises in cross-border digital asset recovery, fraud and asset tracing, with a focus on crypto laundering, DAOs and the Cayman Foundation Company, insolvency and investigations.

Nia is experienced in advising on crypto recovery strategies arising from high-value hacks and thefts. She has acted for two petitioning retail investors in the first winding-up of a Cayman-domiciled holding company behind a defunct cryptocurrency exchange and in a synchronised cross-border receivership petition for the ringfencing of circa USD 800 million in digital assets. She has also been involved in recovery efforts connected with the theft of over 11,000 Bitcoin from a cryptocurrency trading platform and USD 7.65 billion stolen from a Malaysian sovereign wealth fund amid global corruption investigations.

Nia regularly provides training on DAOs, digital asset recovery and crypto laundering, and has spoken extensively on the topic for panels hosted by the American Bankruptcy Institute, the New York State Bar International Section, The Association of Women in Cryptocurrency, and the Crypto Fraud and Asset Recovery network (amongst others).

**Shaun Reardon-John**

Shaun Reardon-John leads the Baker & Partners BVI office. He is a solicitor-advocate and experienced BVI dispute resolution lawyer, who was admitted to practice in the BVI in 2012. He is recognised by the Legal 500 as a Leading Partner in the jurisdiction.

Shaun specialises in commercial disputes that often involve civil fraud and asset recovery. Most of his work involves cross-border disputes. He has been involved in a synchronised cross-border receivership petition in respect of entities where circa USD 800 million digital assets were alleged to have been misappropriated from various corporate entities controlled by a high-net-worth UBO. He has also acted for the founders of a well-known crypto hedge fund that was placed into liquidation. He has extensive experience with Ponzi schemes, having acted for liquidators on some of the largest matters in recent memory. He has experience of investor-state arbitration disputes, such as the enforcement of an ICSID award against the government of Pakistan.

Where appropriate, Shaun is an advocate for alternative dispute resolution, having secured advantageous outcomes for clients via arbitration and mediation. Clients appreciate his pragmatic approach to disputes.