

British Virgin Islands Blockchain Chapter (Mondaq)

Briefing Summary: This guide to blockchain regulation in the British Virgin Islands covers the legal and enforcement framework, market, cryptocurrencies, smart contracts, data and privacy, cybersecurity, intellectual property and trends and predictions.

Sector: Blockchain, Digital Assets and Tokenisation, Fintech and Regtech

Location: British Virgin Islands

Created Date: 21 November 2024

1. Legal and enforcement framework

1.1 What general regulatory regimes and issues should blockchain developers consider when building the governance framework for the operation of blockchain/distributed ledger technology protocols?

Fintech legislation and guidance notes: The British Virgin Islands (**BVI**) introduced the Financial Services (Regulatory Sandbox) Regulations 2020 to encourage technological innovation in financial services, under a lighter-touch regulatory regime. The regulations were introduced to assist:

- start-ups that wish to provide new financial services solutions that involves a fintech business model which is not currently covered (whether explicitly or implicitly) under current BVI legislation;
- start-ups that wish to test an innovative technology to deliver a licensable financial service; and
- current licensees that wish to test an innovate technology as a part of their already approved financial service offering (together, "**sandbox users**").

The regulations were introduced so that new and innovative fintech products could be trialled for a limited time by sandbox users, without the need to comply with the more onerous licensing requirements set out in more mainstream financial services regulations. Under the regulations, sandbox users can test products or services under the supervision of the BVI Financial Services Commission, which applies specified rules and appropriate regulatory oversight, to reduce the risk of financial disruption and instability to the economy.

The commission has also issued guidance notes on the regulation of virtual assets in the BVI.

Key Contacts



Chris Duncan
PARTNER,
CAYMAN ISLANDS
+1 345 749 2057

[EMAIL CHRIS](#)



Elizabeth Killeen
PARTNER,
BRITISH VIRGIN ISLANDS
+1 284 394 4022

[EMAIL ELIZABETH](#)

OFFSHORE LAW SPECIALISTS

BERMUDA BRITISH VIRGIN ISLANDS CAYMAN ISLANDS GUERNSEY JERSEY

CAPE TOWN HONG KONG SAR LONDON SINGAPORE

careyolsen.com

Anticipated virtual asset legislation: The BVI does not have specific legislation in place that governs and regulates virtual assets and other digital property, but it is expected to pass the following legislation soon:

- legislation to regulate the issue of virtual assets and certain services related to them, such as trading and exchange virtual assets (the proposed Virtual Asset Service Providers Act). This legislation is not expected to impose restrictions on virtual assets themselves or limit the ability of any person to deal with virtual assets for its own account; and
- anti-money laundering and combating the financing of terrorism (**AML/CFT**) legislation, to adopt the Financial Action Task Force recommendations on virtual asset services providers.

Current general regulatory regimes: Until the proposed legislation is enacted, the general regulatory regimes that need to be considered in the BVI are as follows:

- Securities and Investment Business Act, 2010 (**SIBA**): SIBA regulates, among other things, the provision of investment services from within the BVI. All partnerships and companies that are formed or incorporated in the BVI ("**BVI entities**") must therefore have a licence (issued by the Financial Services Commission) to carry on 'investment business'. It is therefore important to determine whether a virtual assets or other digital property is an 'investment'. Usually, a virtual asset or other digital property is merely a medium of exchange, with no benefits or rights (other than ownership of the asset) and therefore it is not considered an 'investment'. As such, we would expect such asset to fall outside the scope of SIBA regulation – a position confirmed in the Financial Services Commission's guidance notes. However, if the value of a virtual asset or other digital property is determined by reference to the performance of some other asset or business (such that it becomes a form of derivative), it may be considered an 'investment' and therefore caught by SIBA. We therefore recommend that specialist advice be sought to determine:
 1. whether a virtual asset or other digital property is caught by the SIBA licensing requirements; and/or
 2. whether the business activities fall in-scope of any of the excluded activities listed in SIBA, which are carved out of the licensing requirement.
- Banks and Trust Companies Act, 1990 (**BTCA**): The BTCA regulates deposits of money (ie, fiat currency) and how it can be withdrawn or repaid. If a BVI entity provides loans to borrowers outside the BVI and accepts deposits, it will need to be licensed under the BTCA. If a BVI entity provides loans to borrowers are based in the BVI, it will also need to be licensed under the BTCA.
- Financing and Money Services Act, 2009 (**FMSA**): The FSMA regulates the provision of 'money services business' in the BVI, which includes:
 - a. money transmission;
 - b. money dispensing; and
 - c. currency exchange.

The FSMA was designed to cover fiat currency – that is, currency that is legal tender – and does not expressly deal with cryptocurrencies (and there is no case law on this point). Tokens and cryptocurrencies are not usually fiat currency, so it is generally accepted that they do not constitute a ‘money services business’. However, if a virtual currency is traded as a contract for difference and a BVI entity could be regarded as a broker, the BVI entity will need to be licensed under the FSMA.

- Data Protection Act, 2021 (**DPA**): The DPA regulates how personal data can be processed. If a BVI entity processes, has control over or authorises the processing of any personal data in respect of a commercial transaction, it will be caught by the DPA. Under the DPA, a data controller cannot process personal data without first obtaining the data subject’s express consent (which can be withdrawn at any time). The DPA also restricts the use of sensitive personal data and the transfer of personal data outside the BVI, unless there are adequate safeguards in place. Data controllers must:
 1. take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure; and
 2. not retain personal data for longer than necessary.
- While there are limited exceptions to these restrictions, we recommend that specialist assistance be sought to advise in relation to the same.
- The existing AML/CFT regime: This comprises:
 1. the Proceeds of Criminal Conduct Act;
 2. the Anti-Money Laundering Regulations; and
 3. the Anti-Money Laundering and Terrorist Financing Code of Practice (together, the **"AML laws"**).
- The AML laws provide a comprehensive set of rules and safeguards, which are in line with international standards, designed to minimise (and ideally eliminate) money laundering and terrorist financing. If a BVI entity is regulated, it must:
 1. maintain know-your-client information and documents on its clients;
 2. have internal AML/CTF systems and controls in place; and
 3. provide copies of these to the Financial Services Commission.

If a BVI entity is not regulated, we still recommend that it familiarise itself with the AML laws as a matter of general good governance. Even though the AML laws may not directly apply now, developers should consider whether changes in the technology or upcoming changes in law under the proposed AML Act may bring it them scope soon.

1.2 How do the foregoing considerations differ for public and private blockchains?

The Financial Services Commission guidance notes and the current legislation do not differentiate between public and private blockchains.

The essential difference between a public and private blockchain is participant access. Public blockchains are publicly distributed so that anyone can effectively set up their own node and 'mine' for cryptocurrency by creating blocks for the transactions requested on the network by solving cryptographic equations. Anyone can read all the data contained within the ledger and use it to send transactions and contribute towards authorising transactions and achieving consensus. Given the nature of a public blockchain, it may be difficult to control the data protection requirements under the DPA.

Private blockchains only give the public restricted access. They are controlled by a central authority, which determines who can be a node and what rights each node can have (it does not necessarily grant each node equal rights). Given the nature of the structure of a private blockchain, it may be easier to control the data protection requirements under the DPA.

Part II of SIBA sets out a requirement for a formal offering prospectus to be produced and registered when an offer of securities is made to the public. However, Part II of SIBA is not yet in force. No guidance has been issued as to when Part II will be implemented.

1.3 What general regulatory issues should users of a blockchain application consider when using a particular blockchain/distributed ledger protocol?

A user of a blockchain or protocol should consider:

- the security of the blockchain or protocol; and
- the recourse it might have in the event of a loss due to hacking or some event negative event.

1.4 Which administrative bodies are responsible for enforcing the applicable laws and regulations? What powers do they have?

The BVI courts have jurisdiction where an unlawful activity has occurred and have demonstrated a readiness to ensure this includes cybercrime and unlawful activity involving virtual assets. In May 2022 (*Chanswap Limited v The Owner of Digital Wallet*), the BVI Commercial Court granted a worldwide freezing order against persons unknown (being those allegedly responsible for cybercrime consisting of the theft of digital assets) and granted an applicant permission to serve its claim on the persons unknown out of the jurisdiction and by alternative means. The BVI Commercial Court also confirmed it would issue a letter of request to the Croatian authorities to seek evidence from a crypto exchange that could identify the persons unknown.

The Information Commissioner's Office can assist in the event of breach of the DPA, but the administrators of the blockchain should be contacted in the first instance.

In addition, where a BVI entity is regulated, the Financial Services Commission can assist, to ensure that the requirements under SIBA, BTCA or the FSMA have not been breached.

1.5 What is the regulators' general approach to blockchain?

The Financial Services (Regulatory Sandbox) Regulations and the proposed legislation (see question 1.1) demonstrate the BVI's commitment to:

- encourage the development of new financial services solutions;
- attract people that wish to leverage existing or new technology in an innovative way and deliver new products/services in the financial services industry (or improve existing business processes); and
- provide regulatory clarity for sandbox users.

The Financial Services Commission's approach to blockchain has been open and friendly. The commission recognises the importance of new technologies used to provide or support financial services business and the potential impact on financial services being offered in or from within the BVI.

1.6 Are any industry or trade associations influential in the blockchain space?

The most influential industry bodies are:

- the Securities and Investment Act Committee; and
- the Proposed Virtual Asset Service Providers Act Review Focus Group.

2. Blockchain market

2.1 Which blockchain applications and protocols have become most embedded in your jurisdiction?

The principal blockchain applications which have become embedded in the BVI relate to digital assets and cryptocurrencies – specifically:

- governance and utility tokens;
- trading and exchange platforms; and
- decentralised finance and non-fungible tokens.

2.2 What potential new applications/protocols are most actively being explored?

A wide range of applications and protocols are being explored, with matters involving decentralised autonomous organisations being the most popular, given the ability to incorporate companies limited by guarantee in the BVI.

2.3 Which industries within your jurisdiction are making material investments within the blockchain space?

Many service providers (eg, lawyers, accountants, corporate service providers) are investing time and resources in being able to understand, advise on and facilitate newer blockchain applications and streamline any Securities and Investment Business Act (**SIBA**) applications for the purposes of registering certain blockchain entities with the Financial Services Commission. There are also specific anti-money laundering and compliance services for cryptocurrency-related projects, particularly for entities that require a SIBA licence from the commission to operate.

2.4 Are any initiatives or governmental programmes in place to incentivise blockchain development in your jurisdiction?

The current initiative in place in the BVI to incentivise blockchain development is the finalisation and enactment of the anticipated proposed legislation (see question 1.1).

3. Cryptocurrencies

3.1 How are cryptocurrencies and/or virtual currencies defined and regulated in your jurisdiction?

The Financial Services Commission guidance notes (see question 1.1) use the Financial Action Task Force (**FATF**) definition of a 'virtual asset', being a digital representation of value that can be digitally traded or transferred and that can be used for payment or investment purposes. 'Virtual assets' do not include digital representations of fiat currencies. It is the commission's position that virtual assets and their related products:

- have value;
- exhibit the attributes of property; and
- meet the definition of intangible property.

The guidance notes do not define the term 'cryptocurrency'.

3.2 What anti-money laundering provisions apply to cryptocurrencies?

The BVI expects to introduce new AML/CFT legislation, which adopts the FATF recommendations on virtual asset services providers, in the near future. In the meantime, all BVI entities should adhere to existing AML laws.

3.3 What consumer protection provisions apply to cryptocurrencies?

Individuals who invest in unregulated cryptocurrencies will be limited to seeking assistance from the BVI courts if an unlawful activity has occurred. The Financial Services Commission can only assist where a BVI entity is regulated.

3.4 How are cryptocurrencies treated from a tax perspective?

The BVI tax authority has not issued any formal statement in relation to the taxation of cryptocurrencies. However, the BVI is a tax-neutral jurisdiction and its income tax is set at 0%, which means that there is no income tax actually levied or paid to the BVI government. As such, there is no requirement for BVI entities to file an income tax return, although they must submit an annual economic substance declaration. In addition, there are no capital gains taxes, gift taxes, profits taxes, inheritance taxes or estate duty in the BVI.

For tax purposes, BVI entities may become resident in any jurisdiction, based on such tests as 'management and control'. All BVI entities are exempt from tax in the BVI and can obtain a certificate from either the BVI registrar or the Inland Revenue to that effect. Moreover, the BVI operates a source-based tax system under which BVI entities will be taxed in the BVI on their BVI net income after all BVI expenses. Consequently, BVI entities operating outside of the BVI, if tax resident in the BVI, will not have their foreign source income taxed in the BVI.

Where there is an initial token/coin offering, the exchange operators will need to be cognisant of the impact of the Foreign Account Tax Compliance Act (**FATCA**) and Common Reporting Standards (**CRS**). FATCA and the CRS will not be immediately relevant at the launch of the initial token/coin offering, but they will need to be considered when a BVI issuer starts to conduct business more generally.

3.5 What regulatory requirements apply to a cryptocurrency trader/exchange?

No regulatory requirements apply to individuals who trade cryptocurrencies on their own behalf, provided that they are not offering any regulated or investment services under SIBA. However, where a cryptocurrency provides a benefit or right beyond a medium of exchange (eg, because it grants rights to shares or creates or acknowledges a debt), SIBA can apply. Some cryptocurrencies can provide other benefits to the holder, such as rights to:

- vote on different protocol proposals;
- be eligible for part of the protocol profits or fees; or
- take part in a decentralised autonomous organisation.

BVI entities that hold fiat currency on behalf of their clients and invest the same will need to consider whether they need to apply for a licence under the Banks and Trust Companies Act. Advice should therefore always be taken prior to engaging in activities involving cryptocurrencies in or from within the BVI, to determine whether it needs to be regulated by the Financial Services Commission.

3.6 How are initial coin offerings and securities token offerings defined and regulated in your jurisdiction?

These terms are not currently defined in the BVI and there is no specific regulation in relation to the same. Whether an initial coin offering or securities token offering needs to be regulated in the BVI will depend on how it is structured and what the token subsequently represents. If the token is merely a medium of exchange, with no benefits or rights other than ownership of the asset, it will not be considered an 'investment'. As such, we would expect such asset to fall outside the scope of SIBA regulation – a position confirmed in the Financial Services Commission guidance notes (see question 1.1). However, if the value of a token is determined by reference to the performance of some other asset or business, such that it becomes a form of derivative, it may be considered an 'investment' and therefore caught by SIBA. We therefore recommend that specialist advice be sought to determine whether a token is caught by the SIBA licensing requirements.

4. Smart contracts

4.1 Can a smart contract satisfy the legal requirements of a legal contract under the laws of your jurisdiction? What will be considered when making this determination?

BVI law does not normally require contracts (other than deeds) to be in any particular form. It will enforce any promise (or at least award damages for breach), as long as:

- the common law requirements for formation of a contract are met; and
- there are no vitiating factors (eg, duress, misrepresentation or illegality).

The common law requirements are that there must be:

- offer and acceptance;
- valid consideration;
- an intention to create legal relations; and
- sufficient certainty.

As such, if a smart contract satisfies these common law requirements, it should have legal effect. This view is supported by the recent decision of the Commercial Court in *Chanswap Limited v The Owner of Digital Wallet*. In this decision, the BVI Commercial Court recognised crypto assets as property and the transfers of tokens between blockchains via a smart contract, as a set of pre-determined rules, and under which relief may be granted.

4.2 Are there any regulatory or governmental guidelines or policies within your jurisdiction which provide guidance on regulating/defining smart contracts?

There are no regulatory or governmental guidelines regarding the enforceability of smart contracts in the BVI. However, the Electronic Transactions Act, 2019 helpfully provides that the offer and acceptance of a contract may be expressed by means of electronic record. This, coupled with the recent decision in *Chanswap Limited v The Owner of Digital Wallet*, indicates that smart contracts are enforceable under BVI law.

On 18 November 2019, the UK Jurisdiction Taskforce issued a Legal Statement on Cryptoassets and Smart Contracts. The paper concluded that smart contracts are capable of being legally binding in the normal way. While this paper is not binding in the BVI, it is persuasive.

4.3 What parts of traditional contract might smart contracts be able to replace?

Aspects of contracts which require third-party involvement may be replaceable by smart contracts. Examples of contracts that could be replaced by smart contracts are:

- the payment of goods and services on delivery;
- the payment of royalties in relation to IP assets;
- the automatic ordering of stock when supplies are low;
- the automatic payment of insurance when particular events have occurred;
- escrow arrangements; and
- notification provisions.

In these examples, payments can trigger events can be hardcoded.

4.4 What parts of traditional contracts might smart contracts be unable to replace?

Due to their self-executing nature, the possible outcomes of a smart contract are typically limited to being binary. The risks of an unintended outcome can be high if the smart contract itself contains errors or has not been properly coded. In addition, common yet subjective terms (eg, 'good faith', 'sufficient cause' and 'reasonable/best efforts') cannot be implemented in code and are therefore incapable of being incorporated into smart contracts.

4.5 What issues might present themselves in your jurisdiction with regard to judicial enforcement of smart contracts?

No specific issues have presented themselves before the courts in the BVI. However, issues that might arise are likely to centre on the way in which a smart contract might be undone or amended. There may also be jurisdictional issues, where it is not easy to identify the location of a particular virtual asset or other digital property. Also, many smart contracts are written in code, rather than in a particular spoken language. This may give rise to translation issues should a dispute arise.

4.6 What are some practical considerations that parties should consider when drafting a smart contract?

Given that smart contracts are immutable, it is extremely important to consider in detail all aspects of the contract before executing it. Such considerations include:

- performance measures;
- pricing metrics;
- notice;
- execution authority; and
- wallet addresses.

Like any form of technology, smart contracts may be subject to human errors (incorrect initial coding) and other bugs/system upgrades which unintentionally impact the smart contract.

4.7 How will the foregoing considerations differ when smart contracts are running on a private versus public blockchain?

Private blockchain will be more amenable to change and alteration, and therefore issues which could arise may be more easily resolved for a private blockchain compared with a public blockchain (which will likely require the consensus of a much larger group).

5. Data and privacy

5.1 What specific challenges or concerns does blockchain present from a data protection/privacy perspective?

The British Virgin Islands has implemented the Data Protection Act, which is based on the UK/EU standards of the General Data Protection Regulation (**GDPR**).

The GDPR and other data protection laws are constructed around the notion that centralised entities should control and process personal data, with statutory obligations relating to attributed to 'data controllers' and 'data processors'.

This approach is fundamentally at odds with blockchain's decentralised nature, making it hard to reconcile current data protection laws with blockchain's other principal characteristics – that is:

- the lack of centralised control and storage;
- the immutability of the blockchain; and
- the storage of data forever.

The following principal issues arise:

- It is often difficult (if not impossible) to identify within a blockchain application who the data controllers and data processors actually are, for the purposes of compliance with data protection legislation.
- Stakeholders in the blockchain space may have a different attitude to anonymity and pseudonymity, which has an impact on how data protection and privacy laws can (or should) apply.
- Global participation in blockchain applications (eg, in the trading of cryptocurrencies) means that transactions are often conducted on a cross-border basis, which raises questions of:
 1. whether any restrictions might apply to the transfer of personal data to another jurisdiction; and
 2. whether that other jurisdiction has equivalent data protection or privacy legislation.
- It must further be considered whether, in a blockchain application, the use of personal data is for legitimate purposes.
- An individual's 'right to be forgotten' is difficult to reconcile with the blockchain's immutable nature – a data subject could find his or her personal data encased onto a blockchain forever.

5.2 What potential advantages can blockchain offer in the data protection/privacy context?

The area of data protection/privacy on which blockchain will likely have the biggest positive impact is the recording and retention of anonymised data. The ability to continuously update and record important records and statistics (eg, medical journals, government statistics) could offer the ability to ensure that such information is public, easily accessible, auditable and at the same time secure and uneditable. This has many potential benefits – including that a person need not rely on a third party to provide safekeeping of important records.

6. Cybersecurity

6.1 What specific challenges or concerns does blockchain present from a cybersecurity perspective?

Private keys: Private keys are used for interacting with the blockchain and, in contrast to user passwords, cannot be restored. If a user loses a private key, all data encrypted with it will most likely be impossible to recover. This can be mitigated by the use of third-party custody services; albeit that in reality, this passes the responsibility of ensuring safekeeping to the third party.

Hacking: Like all technology, blockchain applications are at risk of ‘hacking’ or being compromised. Again, this risk can be mitigated by the use of third-party custody solutions; however, those providers can themselves be hacked.

Out-of-date software/vulnerability coverage: The fast pace of the blockchain space means that it is often difficult to keep blockchain software updated. In the same vein, it is hard to keep track of security updates to enterprise blockchain software because there is a lack of coverage on relevant national databases.

6.2 What potential advantages can blockchain offer in the cybersecurity context?

Blockchain applications offer the following major advantages in the cybersecurity context:

- Secure data storage and processing: blockchain records are immutable and any change recorded on the blockchain is transparent and non-removable. Therefore, data stored on a blockchain is protected better than traditional digital or paper-based records.
- Transfer of data in a secure manner: blockchain facilitates fast and secure transactions of data and finances. Features such as smart contracts allow for the automatic execution of agreements between several parties.
- Traceability/transparency: all blockchain transactions are digitally signed and time stamped, so participants can trace transaction history and track accounts at a point in time.
- User confidentiality: the confidentiality of blockchain network participants is high due to the public key cryptography that authenticates users.

- No single point of failure: permissionless blockchains are decentralised, so the failure or compromise of a single node will not compromise the operation or security of the blockchain as a whole.

6.3 What tools and measures could be implemented to mitigate cybersecurity risk?

The most effective tool we are aware of that can help to mitigate cybersecurity risk (in all blockchains, but specifically in new and therefore more centralised chains) is a security audit. In short, this is a process whereby a blockchain security entity is contracted to run a rigorous analysis of a blockchain's code, identifying weak points and allowing the developers to patch them prior to (or after) a public launch. Many of the recent decentralised finance hacks and exploits could have been prevented by a thorough security audit.

7. Intellectual property

7.1 What specific challenges or concerns does blockchain present from an IP perspective?

One challenge is that different protocols can involve intellectual property in different ways, from coding to branding. For decentralised projects, it is not always clear where the ownership of the relevant intellectual property sits and where (and how) it can be protected.

7.2 What type of IP protection can blockchain developers obtain?

Blockchain developers can take advantage of the Trade Marks Act, 2013, which uses the international classification of goods and services provided by the Nice Agreement, which is used by more than 150 countries. Any BVI entity looking to register intellectual property in the BVI will also need to consider the potential impact of the Economic Substance (Companies and Limited Partnerships) Act, 2019, and whether this registration would mean it must demonstrate that it:

- has substance in the BVI;
- has both adequate employees and appropriate premises in the BVI;
- is managed and directed from the BVI;
- incurs adequate expenditure in the BVI; and
- carries on its core income-generating activities in the BVI.

7.3 What are the best open-source platforms that could be used to protect developers' innovations?

We cannot recommend any specific open-sourced platforms.

7.4 What potential advantages can blockchain offer in the IP context?

It is predicted that blockchain technology is already transforming the way in which IP rights are recorded or evidenced. An example of this is the popularity of non-fungible tokens. While they were initially used to represent digital artwork, their use in other industries is increasing as a way of providing digital identifiability and authenticity for property of all varieties.

8 Trends and predictions

8.1 How do you think the regulatory landscape in your jurisdiction will evolve in the blockchain space over the next two years? Are any pending changes currently being considered?

The enactment and implementation of the anticipated proposed legislation in this space (see question 1.1).

8.2 What regulatory changes would you like your jurisdiction to implement to further advance the blockchain industry?

The enactment and implementation of the anticipated proposed legislation in this space (see question 1.1).

8.3 What is the largest impediment within your jurisdiction to the adoption of blockchain technology?

Blockchain is complicated and comes with challenging technical concepts and much jargon; all stakeholders (advisers, service providers, government and the Financial Services Commission) are therefore on a continued learning curve. It is also difficult for persons that are completely unfamiliar with blockchains to enter the space and to trust it, given that it is largely unregulated. Given how quickly blockchain technology develops, it is inevitable that the law any regulation (in any jurisdiction) will lag behind.

9. Tips and traps

9.1 What are your top tips for effective use of blockchain technologies in your jurisdiction and what potential sticking points would you highlight?

Seek specialist advice to ensure that your activities do not need to be regulated by the Financial Services Commission, and so you can keep up to date when the proposed legislation in this space (see question 1.1) comes into force.

Carey Olsen (BVI) L.P. is registered as a limited partnership in the British Virgin Islands with registered number 1950.

Please note that this briefing is only intended to provide a very general overview of the matters to which it relates. It is not intended as legal advice and should not be relied on as such. © Carey Olsen (BVI) L.P. 2026.

