
mondaq
Connecting knowledge & people
Mondaq Comparative Guides
Blockchain 2024
Cayman Islands
CAREY OLSEN

Contents

At Carey Olsen, we always look at the bigger picture. In the face of opportunities or challenges, our clients know that the advice and guidance they receive from us will be based on a complete understanding of their goals and objectives combined with outstanding client service, technical excellence and commercial insight.

BIGGER PICTURE

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?

The primary regulatory regime to consider in the Cayman Islands is the Virtual Assets (Service Providers) Act ("**VASP Act**"). The VASP Act regulates certain blockchain-related activities and therefore may be relevant for certain protocols.

The other regulatory regime that may be relevant for protocols with an associated token or which enable trading of securities is the Securities and Investment Business Act (**SIBA**).

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

The Cayman Islands regulator, the Cayman Islands Monetary Authority (CIMA), does not differentiate between public and private blockchains. However, the VASP Act and SIBA could be relevant for public and private blockchains, depending on their characteristics and operation. For example, both a private and public blockchain could involve the issuance of a token which could be captured under the VASP Act and may also be considered a security under SIBA. Specialist advice is recommended.

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

The 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?

CIMA (as defined above) is the government body tasked with enforcing the VASP Act and retains wide-reaching powers to regulate persons and entities regulated pursuant to the VASP Act.

1.5 What is the regulators' general approach to blockchain?

CIMA has generally been fairly open and friendly in its approach to blockchain, while at the same time adopting a degree of caution in order to maintain the very high standards of the financial services industry.

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

The most influential industry body is the Cayman Islands Blockchain Association, whose stated goal is to "*promote everything blockchain related in the Cayman Islands*".

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 Cayman Islands 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?

In the Cayman Islands, a wide range of applications and protocols are being explored, with decentralised autonomous organisations the most popular given the existence of the Cayman Islands foundation company.

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 through the provision of crucial infrastructure and support. There are also specific anti-money laundering and compliance services for cryptocurrency-related projects.

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

Aside from the VASP Act discussed in question 1, there are various organisations and bodies looking to attract talent in the Cayman Islands, including:

- Cayman Enterprise City, which facilitates entry into the special economic zone; and
- Tech Cayman.

3. Cryptocurrencies

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

The VASP Act governs any entity that issues virtual assets or provides certain virtual asset services.

The VASP Act's implementation is occurring over two phases and began in October 2020. Phase 1 brought into force the anti-money laundering, counter-terrorist financing of terrorism, compliance and supervision provisions of the VASP Act.

Phase 2 has yet to come into force. When implemented, Phase 2 will introduce additional licensing requirements applicable to custody services and trading platforms and will provide for sandbox licences.

Continued

The VASP Act defines 'virtual assets' as "a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes but does not include a digital representation of fiat currencies". In this regard, the VASP Act distinguishes between virtual assets and 'virtual service tokens', which are defined as "digital representations of value which are not transferable or exchangeable with a third party at any time and includes digital tokens whose sole function is to provide access to an application or service or to provide a service or function directly to its owner".

The VASP Act requires all virtual asset service providers (**VASPs**) to register or obtain a licence (as applicable). A 'virtual asset service' is defined as the issuance of virtual assets or the business of providing one of more of the following services or operations for or on behalf of a natural or legal person or legal arrangement:

- exchange between virtual assets and fiat currencies;
- exchange between one or more other forms of convertible virtual assets;
- transfer of virtual assets;
- virtual asset custody service; or
- participation in, and provision of, financial services related to a virtual asset issuance or the sale of a virtual asset.

3.2 What anti-money laundering provisions apply to cryptocurrencies?

Under the Proceeds of Crime Act (2020 Revision) and the Anti-Money Laundering Regulations (2020 Revision), and their applicable guidance notes (together, "**the AML laws**"), any person, formed, registered or based in the Cayman Islands conducting "relevant financial business" is subject to various obligations aimed at preventing, identifying and reporting money laundering and terrorist financing. VASPs must comply with the AML laws.

The requirements include (but are not limited to) the following:

- appointing a managerial level employee as an AML compliance officer (who must be approved by the Cayman Islands Monetary Authority (CIMA) under the VASP Act);
- appointing a managerial-level employee as the money-laundering reporting officer and a deputy for the same; and
- implementing comprehensive procedures to ensure that clients are properly identified, risks assessed and requisite records maintained.

3.3 What consumer protection provisions apply to cryptocurrencies?

Aside from the requirements of the VASP Act, which provides a level of consumer protection, CIMA has in the past made statements concerning the operation of certain exchanges from the jurisdiction where those exchanges may have been operating without licences or registration.

3.4 How are cryptocurrencies treated from a tax perspective?

No Cayman Islands taxes currently apply to cryptocurrencies.

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

No regulatory requirements apply to an individual who is trading cryptocurrencies on his or her own behalf, provided that he or she is not offering any virtual asset services as defined under the VASP Act. An exchange operating as a business may be subject to the VASP Act and therefore will need to register as a 'registered person' or obtain a licence under the VASP Act.

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

On the basis that the coin being offered falls within the definition of a 'virtual asset' as defined in question 3.1, and that the initial coin offering falls within the definition of an 'issuance of virtual assets' as set out in question 3.1, the entity conducting the issuance will be required to register as a 'registered person' under the VASP Act.

A securities token offering may be regulated by both the VASP Act and the Securities and Investment Business Act ("**SIBA**"). This will be the case where the token falls within the definition of a 'virtual asset' as set out in question 3.1 and the definition of a 'security' as set out in Schedule 1 of SIBA. Currently this would require the issuing entity to become regulated under both acts; however, a waiver process is expected to be introduced whereby regulation under both regimes should not be required.

Once the waiver provisions are brought into force, CIMA may grant a waiver to any person already licensed under another regulatory act (eg, SIBA). Section 16 of the VASP Act expressly provides that CIMA may issue such waiver if it determines that:

- the virtual asset service does not materially change the nature of the activity for which the existing licensee is already licensed; and
- the supervision and oversight in relation to that licensee is sufficient to include the virtual asset service carried on by it.

The aforementioned waiver provision in the VASP Act appears designed specifically to address a securities token offering situation and in that context, were the entity already regulated by SIBA, it could apply for a waiver from the VASP Act (or vice versa).

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?

While there is no Cayman Islands precedent addressing this question, we see no reason why a smart contract could not be enforceable as a legal contract under the laws of the Cayman Islands.

Continued

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. However, the Electronic Transactions Act (2003 Revision) helpfully provides that that the offer and acceptance of a contract may be expressed by means of electronic record. On the face of it, this would suggest that smart contacts are enforceable under Cayman Islands law.

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 contract. Escrow arrangements and notification provisions are two obvious examples. Certain insurance contracts can also be improved upon by the use of smart contracts where trigger events and pay-outs 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') are 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 Cayman Islands. However, issues that might arise are likely to centre on the way in which a smart contract might be undone or amended.

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 (including the potential use of multi-signature mechanisms for additional security); and
- wallet addresses.

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

Presumably a 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 Cayman Islands has implemented data protection legislation largely 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.
- The 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:
    a. whether any restrictions might apply to the transfer of personal data to another jurisdiction; or
    b. 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 may 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

Continued

at the same time secure and uneditable. This has many potential benefits – one of which is that a person need not rely a on a third party to provide safe keeping 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 to interact with the blockchain and, in contrast to user passwords, cannot be restored. If a user loses the 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. 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 blockchains 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 for intellectual property is that different protocols can involve intellectual property in different ways, from code to branding. For decentralised projects, it is not always clear where the ownership of the relevant intellectual property sits.

7.2 What type of IP protection can blockchain developers obtain?

Blockchain developers can take advantage of the UK Copyright, Design and Patents Act 1988, which has been extended to apply (in part) in the Cayman Islands. This can, for example, afford automatic copyright protection for code. However, anyone looking to register any kind of intellectual property in the Cayman Islands should consider the potential impact of the International Tax Co-operation (Economic Substance) Act.

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

Not applicable.

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

It is predicted that blockchain technology will transform the way in which IP rights are recorded or evidenced.

An example of this trend in action is evidenced by the meteoric rise in popularity in 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 most obvious change will be the implantation of Phase 2 of the Virtual Assets (Service Providers) Act ("**VASP Act**"), discussed in question 3.1. Aside from that, it is hoped that the process for becoming registered (and licensed when Phase 2 has been implemented) will become more streamlined and certain with regard to timing.

Continued

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

The VASP Act as drafted is a solid piece of legislation and gives certainty to persons wishing to operate in the crypto space in the Cayman Islands. One change that may be helpful would be to streamline processes so that an applicant can have some level of certainty as to how long it may take for an application to be approved.

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. It can therefore be difficult for persons that are completely unfamiliar with these to enter the space. That is likely to slow the adoption overall as service providers come up to speed.

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?

The most important factor when considering offering blockchain technology to the public from the Cayman Islands is to understand the potential impact of the Virtual Assets (Service Providers) Act. We would always recommend obtaining product-specific advice as a first step to understand the regulatory implications of the product before undertaking any blockchain-related activities.

Author

Chris Duncan
Partner

D +1 345 749 2057
E chris.duncan@careyolsen.com

Our offices

Jurisdictions

Bermuda

Carey Olsen Bermuda Limited
Rosebank Centre
5th Floor
11 Bermudiana Road
Pembroke HM08
Bermuda

T +1 441 542 4500
E bermuda@careyolsen.com

British Virgin Islands

Carey Olsen
Rodus Building
PO Box 3093
Road Town
Tortola VG1110
British Virgin Islands

T +1 284 394 4030
E bvi@careyolsen.com

Cayman Islands

Carey Olsen Cayman Limited
PO Box 10008
Pavilion East
Cricket Square
Grand Cayman KY1-1001
Cayman Islands

T +1 345 749 2000
E cayman@careyolsen.com

Guernsey

Carey Olsen (Guernsey) LLP
PO Box 98
Carey House
Les Banques
St Peter Port
Guernsey GY1 4BZ
Channel Islands

T +44 (0)1481 727272
E guernsey@careyolsen.com

Jersey

Carey Olsen Jersey LLP
47 Esplanade
St Helier
Jersey JE1 0BD
Channel Islands

T +44 (0)1534 888900
E jerseyco@careyolsen.com

International offices

Cape Town

Carey Olsen
Protea Place
40 Dreyer Street
Claremont
Cape Town 7708
South Africa

T +27 21 286 0026
E capetown@careyolsen.com

Hong Kong SAR

Carey Olsen Hong Kong LLP
Suites 3610-13
Jardine House
1 Connaught Place
Central
Hong Kong SAR

T +852 3628 9000
E hongkong@careyolsen.com

London

Carey Olsen LLP
Forum St Paul's
33 Gutter Lane
London EC2V 8AS
United Kingdom

T +44 (0)20 7614 5610
E londonco@careyolsen.com

Singapore

Carey Olsen Singapore LLP
10 Collyer Quay #29-10
Ocean Financial Centre
Singapore 049315

T +65 6911 8310
E singapore@careyolsen.com