mondaq
Connecting knowledge & people

Mondaq Comparative Guides

Blockchain 2024

Jersey

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?

As a matter of policy, Jersey has chosen not to regulate cryptocurrencies (the most obvious application of blockchain technology) within its existing regulatory framework.

Accordingly, the principal laws relating to digital assets are:

- the Financial Services (Jersey) Law 1998; and
- the Control of Borrowing (Jersey) Order 1958 (Jersey's principal statute concerning the raising of capital).

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

Jersey's regulator, the Jersey Financial Services Commission (**JFSC**), does not differentiate between private and public blockchains.

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

The most common application of blockchain technology in Jersey is to cryptocurrencies and any other digital assets.

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

Jersey's regulator is the JFSC, which has regulatory responsibility for overseeing the conduct of businesses and ensuring compliance with Jersey's anti-money laundering legislation.

If an activity comes within the jurisdiction of the JFSC, its enforcement teams will investigate and, where appropriate, take action against businesses and individuals that do not comply with Jersey's regulatory and legal requirements. The JFSC has statutory powers to impose a range of sanctions, including:

- restricting or preventing people from working in Jersey's finance industry;
- revoking or placing condition on a business licence;
- issuing public statements;
- imposing civil financial penalties; and
- referring cases to the States of Jersey Police for consideration of criminal prosecution.

1.5 What is the regulators' general approach to blockchain?

Jersey is certainly open to blockchain applications and to cryptocurrencies in general. The JFSC approved the world's first regulated Bitcoin fund, GABI Plc, in 2015 and since then, a number of blockchain businesses have established themselves in Jersey. However, Jersey is fiercely protective of its reputation as a well-regulated financial services jurisdiction and the island is certainly not a 'crypto free-for-all'. The application to establish a blockchain business in Jersey will be subject to a degree of scrutiny from the JFSC.

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

The Digital Assets Working Group was established in 2017 during the height of the Individual Savings Account boom to assist the JFSC in understanding the emergence of blockchain and cryptocurrencies as an asset class. Representatives from the legal, accounting and corporate service provider sit on the committee, as well as representatives from blockchain businesses.

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 Jersey relate to digital assets and cryptocurrencies – specifically:

- utility tokens;
- defined platforms; and
- stablecoins.

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

We are seeing some enquiries as to how decentralised organisations can be established in Jersey.

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

As a financial services hub, Jersey understands that many are trying to make use of blockchain technology in the financial services industry. Accordingly, all 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.

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

Jersey has an independent organisation called Digital Jersey, which is government backed and facilitates the development of new technologies to help Jersey become a digital-friendly economy.

As part of Digital Jersey's remit, it can facilitate discussions between blockchain developers on the one hand and the Jersey Financial Services Commission on the other. It also has some business licences which new companies can take advantage of.

Continued

3. Cryptocurrencies

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

Virtual currencies: Jersey's principal anti money laundering law, the Proceeds of Crime (Jersey) Law 1999 (**POC(J)L**), defines 'virtual currency' as:

any currency which (whilst not itself being issued by, or legal tender in, any jurisdiction) –

- digitally represents value;
- is a unit of account;
- functions as a medium of exchange; and
- is capable of being digitally exchanged for money in any form.

For the avoidance of doubt, virtual currency does not include any instrument which represents or stores (whether digitally or otherwise) value that can be used only to acquire goods and services in or on the premises of, or under a commercial agreement with, the issuer of the instrument.

Any person that provides to third parties the business of a 'virtual currency exchange' (ie, the exchange of virtual currency for money or vice versa) must register with the Jersey Financial Services Commission (JFSC) under the POC(J)L and will be subject to Jersey's anti-money laundering regime.

The Initial Coin Offering (**ICO**) Guidance Note published by the JFSC sets out various categories of tokens (of which a cryptocurrency is one such type) as follows.

Security token: This will typically have characteristics that are usually associated with an equity or debt security in the traditional capital markets sense, including one or more of the following such characteristics (whether contractual or implied):

- a right to participate in the profits/earnings of the ICO issuer or a related entity;
- a claim on the issuer or a related party's assets;
- a general commitment from the ICO issuer to redeem tokens in the future;
- a right to participate in the operation or management of the ICO issuer or a related party; and
- the expectation of a return on the amount paid for the tokens.

A utility token (see below) will not be regarded a 'security' solely by reason of being traded on a secondary market (eg, via a cryptocurrency exchange).

Non-security token: a token which is deemed not to be a 'security' will typically be either:

- a utility token, which confers on the holder merely a usage right or the right to access a product or service. Such a token has no economic rights attached to it, there is no expectation of a return; or
- a cryptocurrency token, which is designed to behave like a currency, being a store of value and medium of exchange and referred to in some jurisdictions as a payment token.

See question 3.6 for more information on the regulatory treatment of ICOs.

3.2 What anti-money laundering provisions apply to cryptocurrencies?

Any person that provides to third parties the business of a 'virtual currency exchange' (ie, the exchange of virtual currency for money or vice versa) must register with the JFSC under the POC(J)L and will be subject to Jersey's anti-money laundering regime.
The anti-money laundering requirements relating to an ICO/token issuance are stated in question 3.6.

3.3 What consumer protection provisions apply to cryptocurrencies?

In relation to a token issued by a Jersey issuer, the JFSC's ICO Guidance Note requires the Jersey issuer to have procedures and processes in place to:

- mitigate and manage the risk of retail investors investing inappropriately in the ICO; and
- ensure that retail investors understand the risks involved.

This is usually achieved by bolstering risk warnings in the white paper which purchasers must specifically acknowledge (usually by checking a box on the token portal) prior to purchase.

More generally, in the past, the JFSC has published announcements warning the general public about the risks of investing in cryptocurrencies.

3.4 How are cryptocurrencies treated from a tax perspective?

The Jersey tax authorities have not issued any formal statement in relation to the taxation of cryptocurrencies. However, Jersey has a zero rate of corporate income tax and a personal rate of income tax of 20%. There are no capital taxes in Jersey.

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

An exchange which facilitates the exchange of fiat money for (non-security tokens) cryptocurrencies must register with the JFSC as a virtual currency exchange (see question 3.2).

Any person or exchange that facilitates the exchange by third parties of fiat money for security tokens will need to obtain an 'investment business' licence from the JFSC under Jersey's financial services legislation, the Financial Services (Jersey) Law 1998, and will be subject to the full regulatory regime.

Continued

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

The JFSC's basic position regarding token launches is that it welcomes properly thought-out token launches with a good governance structure. Its two principal concerns are consumer protection and anti-money laundering/combating the financing of terrorism.

To address these issues, the JFSC imposes a set of conditions on a Jersey company that issues a utility token or security token, which are summarised below and can be found in the JFSC's ICO Guidance Note. The conditions are imposed on the consent issued to the Jersey issuer (so-called 'COBO consent') under the (oddly named) Control of Borrowing (Jersey) Order 1958 – the island's principal regulation controlling the raising of capital by Jersey entities.

The JFSC does not like tokens or Jersey companies which issue the tokens to be described as 'regulated'. However, some language may be included in any marketing material (as set out in Appendix 1 of the ICO Guidance Note) to give potential token purchasers the comfort that a Jersey issuer has been scrutinised by the JFSC (and which might not be available in other jurisdictions.)

In addition to obtaining COBO consent from the JFSC, the other major item on the critical path is for the Jersey issuer to appoint a Jersey-regulated administrator to provide certain services. In essence, if things go wrong with the token issuance, the JFSC will go after the administrator.

The conditions imposed on a Jersey issuer by the JFSC are as follows:

- to appoint and maintain a Jersey resident director on the board of the Jersey issuer;
- to appoint a Jersey-regulated administrator to act as administrator to the Jersey issuer;
- not to change either the Jersey issuer's administrator or the Jersey resident director without the JFSC's prior approval;
- to prepare and file annual audited accounts with the Jersey Companies Registry irrespective of whether the Jersey issuer is a public or private company;
- to maintain and adopt systems, controls, policies and procedures for the customer take-on, profiling and transaction monitoring at enhanced levels, ensuring reporting of suspicions and money-laundering and financing of terrorism activities (this obligation effectively falls on the Jersey licensed administrator);
- to prepare and issue an information memorandum which complies with certain content requirements required of a prospectus issued by a company under the Jersey Companies Law;
- to include in any marketing material (including the information memorandum) clear consumer warnings highlighting that the token is unregulated; and
- if and to the extent that any crypto-to-fiat exchange (or vice versa) takes place in Jersey, to require the Jersey issuer to register as a virtual currency exchange pursuant to the POC(J)L (see question 3.1), which imposes certain additional anti-money laundering obligations on the exchange.

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?

There is no reason why a smart contract could not be enforceable as a legal contract under the laws of Jersey.

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 Communications (Jersey) Law 2000 helpfully provides that the offer and acceptance of a contract may be expressed by means of electronic communication. On the face of it, this would suggest that smart contacts are enforceable under Jersey law.

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

It is generally accepted that smart contracts are well suited to agreements between parties without any trusted intermediary or third-party validation, such as:

- peer-to-peer financial transactions such as trading in over-the-counter derivatives; and
- changes in public ownership records, because the time of change of ownership can be measured digitally (eg, when payment can occur directly from wallet to wallet).

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

Due to their self-executing nature, the outcome of a smart contract is very binary. Subjective terms relating to contractual performance (often referred to as 'deliberate ambiguity'), such as 'good faith' or 'reasonable efforts', cannot be implemented in code and thus cannot be part of a smart contract.

In addition, the requirements under Jersey contract law relating to an 'agreement between the parties' – that is, that there has been a valid offer which has been validly accepted – should align with the technical nature of a smart contract.

Continued

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

Stakeholders have identified some headline issues relating to the enforceability of smart contracts generally, which will also likely arise in Jersey. These are as follows:

- A contract performed under a smart contract cannot be reversed, modified or undone – therefore, attempting to void a smart contract as a matter of law will be difficult.
- Smart contracts cannot be modified because they are formed pursuant to computer code.
- One of the requirements under Jersey contract law is 'cause' – akin to the Anglo-Saxon concept of 'consideration'. Where a smart contract automatically executes in the absence of identifiable 'cause', this may render it unenforceable as a matter of Jersey law.

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

A smart contract is not a contract in the ordinary sense of the word, so it is perhaps confusing to talk about 'drafting' smart contracts as a lawyer would interpret that phrase. Instead, in a bilateral smart contract, both parties should be confident that the underlying computer code works as both parties intend.

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

On a private (or 'permissioned') blockchain, it is easier to unilaterally amend the smart contract.

5 Data and privacy

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

Jersey has implemented data protection legislation to conform to European standards of the General Data Protection Regulation (**GDPR**) and has been assessed by the European Commission as providing adequate protection for personal data.

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' that determine the purposes for and means of processing the data; and
- 'data processors' that process the personal data on behalf of data controllers.

This approach is fundamentally at odds with blockchain's decentralised nature and it is often difficult 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 (at least in theory).

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:
    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 should also be considered whether, in a blockchain application, the use of personal data is for legitimate purposes (as required by the data protection laws of both Jersey and other jurisdictions).
- 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?

Given the pseudonymous nature of the blockchain, the advantages which it brings in terms of data protection/privacy are well publicised.

6. Cybersecurity

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

Private keys: blockchains rely on the use of private keys – long sequences of random numbers automatically generated by a wallet. 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. There have been several well-publicised examples of individuals losing their private key.

Hacking: like all technology, blockchain applications are at risk of 'hacking' or being compromised. Hacking is carried out for a variety of reasons: financial, political or even just for fun. Blockchain hacking can take three main forms:

- 51% attacks: these are more common on smaller blockchains because it is hard for miners to gain significant control over bigger blockchains. During the decentralised transaction verification process (known as 'mining'), if one or more hackers gain control over half of the mining process, the

Continued

miners can create a second version of the blockchain (also known as a 'fork') where some transactions are not recorded. This allows the miners to create a different set of transactions on the fork and designate the fork as the true version of the blockchain, even though it is fraudulent. This also allows the hackers to double spend cryptocurrency. One sub-set of 51% attacks is the 'sybil attack', where hackers generate numerous fake network nodes and use them to obtain majority consensus.

- Exploiting 'creation errors': Security errors may not be eliminated when a blockchain application is created. In this instance, hackers can identify the error and seek to hack into the blockchain.
- Insufficient security/endpoint vulnerabilities: hackers will attack the blockchain network's endpoint, where users interact with the blockchain – typically via devices where users have not implemented sufficient security measures. Historically, 'hot' wallets on mobile phones have been considered especially vulnerable because of the ease with which such wallets can be created and their mass usage.
- Routing attacks: a blockchain network relies on the real-time movement of massive amounts of data. Hackers can use an account's anonymity to intercept data as it is being transmitted to internet service providers. Participants are usually unaware of the threat because data transmission and operations proceed as usual.

Out-of-date software/vulnerability coverage: the fast pace of the blockchain space means that it is often difficult to keep blockchain software updated. One open-source blockchain platform released 182 upgrades in the space of five years! 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?

No answer submitted for this question.

7. Intellectual property

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

No answer submitted for this question.

7.2 What type of IP protection can blockchain developers obtain?

It is fair to say that Jersey's laws relating to, and the means of registering, IP rights are not as sophisticated as those of certain other jurisdictions. However, there is no reason why a Jersey court would not enforce a valid judgment of a court in other reputable jurisdiction relating to a person's IP rights.

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?

Many predict that blockchain technology will transform the way in which IP rights are recorded and traced. In a 2019 article entitled "How blockchain can impact the intellectual property life cycle", EY Global identified the lifecycle of IP rights through the lens of blockchain as follows:

- Step 1: creating or acquiring IP rights using tokens to represent IP rights assets.
- Step 2: tracking the development of, and contributions to, the IP rights using a blockchain application.
- Step 3: commercial exploitation of the IP rights (whether by licensing, sale or some other means). Transactions and movements of value are shared on the network and a layer of smart contracts alerts third parties with an interest in the IP rights and instantly calculates who on the network has a resulting financial obligation (eg, a licensee of the tokenised IP rights).

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?

Jersey is implementing the Financial Action Task Force's Guidelines on Virtual Asset Service Providers into the domestic anti-money laundering legislation in 2023.

Continued

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

It would undoubtedly be helpful if the enforceability of smart contacts were expressly recognised under Jersey law.

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

All stakeholders (advisers, service providers, government and the Jersey Financial Services Commission) are on a continued learning curve in this very fast-paced evolving landscape. It is inevitable that the law and regulation of any jurisdiction will lag behind the evolution of technology.

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?

Anyone looking to launch a blockchain project in Jersey, particularly in relation to cryptocurrencies, should engage with the JFSC

Author

Christopher Griffin
Partner

D +44 (0)1534 822256
E christopher.griffin@careyolsen.com

Continued

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
PO Box 10008
Willow House
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