

Fighting over nothing: Cryptocurrency litigation issues

Leigh Sagar, New Square Chambers, Lincoln's Inn
leigh.sagar@newsquarechambers.co.uk

1. In my talk this afternoon I do not intend to discuss in any detail how cryptocurrency systems operate. That would take far more time than is available and would not really assist with what I really want to say. I will explain as necessary and everyone in the room should understand what I am talking about, even if some of you do not understand some of the words that I use.

Introduction

2. There are four points that I want to raise at the outset.

(1) The first is that cryptocurrencies generally operate without any intermediary, like a bank or a government, so if something goes wrong you cannot write a letter to anyone and complain.

- (2) Secondly, the currencies function over a network of many thousands of computers around the world, each running network software known as a “protocol”, connecting them directly or indirectly.
- (3) Thirdly, I will refer to cryptocurrencies as “crypto”, “digital cryptographic tokens”, “DCT” or “tokens”.
- (4) Fourthly, as in other cases that lawyers deal with, the key to success is properly analysing the transactions in which DCTs play a part and apply the law, as you would in any other matter. But there are issues that might currently be insurmountable in certain cases.

3. Since I offered to give this talk, there has been an explosion in the tokenisation of crowdfunding and crowdsales around the world and I want to talk about this as well. Tokens are acquired through an "Initial Coin Offering" (“ICO”) and a substantial number of ICOs have been part of fraudulent schemes; so much so that China and South Korea have banned them altogether. Many jurisdictions, including Gibraltar,¹ have published warnings about contributing to these schemes without due diligence. This new phenomenon is, in my view, the beginning of what has been called “Web 3.0” or the “Financial Web” or “the future of the financial internet”. Just as internet giants such as Facebook and Google rose out of the collapse of the dot com bubble, new titans will rise out of the taming of this new ICO exuberance. People are experimenting with these arrangements and, although the amounts involved are large by the standards of the average person, they are proportionately small when compared to amounts regularly being transferred by credit cards.

4. The best way to think about cryptocurrencies is to imagine a children’s tea party, at which the miniature tea pot, milk jug and tea cups are all empty of any liquid and, although the participants appear to be drinking, they are actually drinking nothing. They believe, at least at some level, that they are drinking something and are enjoying it. It is the same with crypto. There is nothing in the software that can be identified as a crypto token. It exists and functions because

¹ By the Gibraltar Financial Services Commission; see <http://www.fsc.gi/news/statement-on-initial-coin-offerings-250>

the participants in the system share the view that it does; by holding tokens, they believe that they have something and that that something has value. The law recognises that such a belief can confer a property interest. A crypto token can be held on trust.

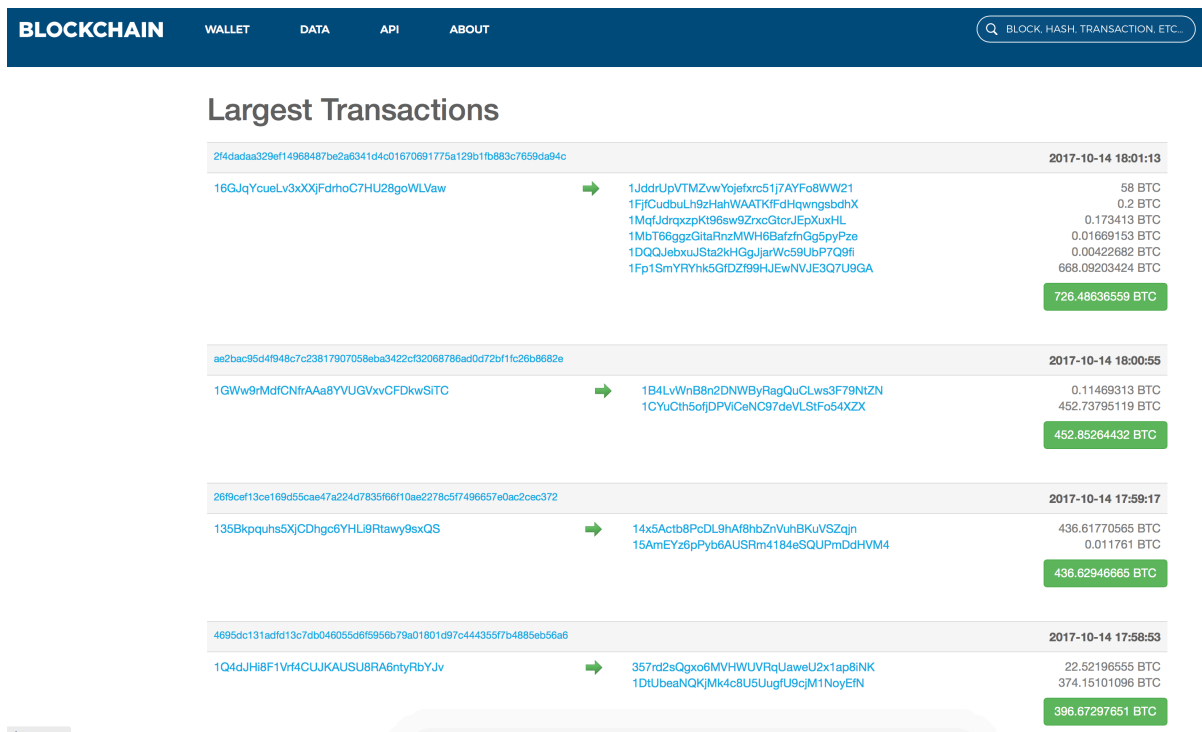


Figure 1: Largest bitcoin transactions on 14th October 2017

5. I have inserted the image in Figure 1 as a matter of interest. It shows the four largest bitcoin transactions that took place on 14th October 2017. The first one is a transfer of more than 700 bitcoin (worth over \$4m at the time) from a public key starting 16GJqYcuel, split into a number of different amounts and going to different public keys, with the largest amount being transferred to the number beginning 1Fp1SmYRY.

Issues

6. There are three main types of issue to consider: regulatory, substantive and procedural.

Regulatory

7. There has been a consultation paper in Gibraltar, setting out proposals for the regulation of activities using distributed ledger technology for the transmission or storage of value belonging to others.² This is about people using blockchain technology, which underpins the security and processing of cryptocurrencies, for various purposes, some of which are yet to be thought of and, of those that have been, most are currently no more than proof of concept. The most important business to which the regulations will apply is the crypto exchange, which exchanges DCT for fiat (government) currency and vice versa, as well as providing facilities for holding tokens on trust for users. I think that the consultation paper presents an excellent approach to the regulation of blockchain innovation but, like other regulation around the world, it does not cover ICO tokens. I will not mention regulation further but clearly Gibraltar is keen, and seems able, to offer a home to distributed ledger technology.

Substantive

8. Substantive issues that I will look at are the nature of DCTs and causes of action that might arise with their use.

Nature

9. Because a DCT does not actually exist, except in the minds of those who believe, understanding the nature of a DCT is counter-intuitive. It is a property interest with no rights or obligations attached to it. There is a protocol network that can be used to transfer it and receive it but no one can be forced or ordered by a court to process the transfer and no one can be forced or ordered not to process it. The process is carried out in a network of thousands of independent computing devices situation around the world and there is no way to predict in advance which of those devices will process and confirm the next transfer that is sent into the network. Once the “transfer” button in a user’s wallet (a software utility to hold the public and private keys necessary

² http://www.gibraltarfinance.gi/downloads/20170508-dlt-consultation-published-version.pdf?dc_%3D1494312876; see also **Uniform Regulation of Virtual - Currency Businesses Act**, the legislation offered by the National Conference of Commissioners on Uniform State Laws at http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/URVCBA_Final_2017oct9.pdf

to send and receive bitcoin) is clicked or pressed, the transaction will almost certainly go through (I have never heard of a transaction not going through).

10. There are currently three main types of token being used, although this list is not exclusive and is likely to increase as more and different arrangements are conceived.

Coin token

11. This is the simplest manifestation of the DCT, and an example is bitcoin. It exists as a property interest and its value is speculative and variable according to market conditions.

Utility token

12. This is crowdsale token, which is transferred to a contributor in an ICO. It enables the contributor to participate in the implementation of a project, which may be the development of software or the manufacture of a hardware item. It is a property interest that can be bought and sold once it has been issued, but there is also a contract between the promoter and the contributor. It can be argued that such a token is like a share—a bundle of rights and obligations—but that ignores the nature of the token itself. The better view is that the token carries with it no rights and obligations and, subject to the terms and conditions of the offering, that the initial agreement was made for benefit of token holders for the time being. One of the benefits of issuing a token, rather than something in the nature of a cause of action, is that the token is divorced from the issuer and an independent market for the sale and purchase of the tokens can develop. The formalities of an assignment of the benefit of the associated agreement may therefore in some cases be an issue.

Tokenised security

13. This is a crowdfunding token that is transferred to a contributor in an ICO. It can represent shares or equity in an existing business that is raising funds or in a business that will come into existence on the completion of the ICO. Issuing such a token generally requires compliance with financial services regulations. Again, it is a property interest that can be bought and sold once it has been issued, but there is also a contract between the promoter and the contributor, which might also benefit successors.

Causes of action

14. The bitcoin network has existed for some years without any successful attack. The code has been resilient. There can, however, still be loss: for instance, by mistake (such as entering the wrong number for the public key of the recipient) or fraud (such as breaking into a computing device and using the wallet to transfer the owner's crypto (a "protocol claim"). On the other hand, the encryption of some associated websites has been successfully breached and cryptocurrency has been lost. This has occurred in attacks on bitcoin exchanges, which buy and sell crypto in return for fiat currency and provide web-based wallets (a "gateway claim").

Protocol claim

15. The rights and obligations that arise out of something that went wrong with the transfer of a token are in the field of restitution. Someone may have received an unjust enrichment, or there may be a proprietary restitutionary claim.

Gateway claim

16. Here, the tokens are simply stolen by hacking into the computers of the gateway host. If a currency exchange is involved, it almost certainly holds tokens on trust for any customers that leave them in their custody and a breach of trust claim (subject to the terms and conditions of the agreement between the user and the exchange) may be available. Usually, there is also a fraud claim.

Smart contracts

17. Smart contracts are processes that are designed to occur automatically on the occurrence of an event.³ Most currently run on the Ethereum blockchain.⁴ For instance, there may be smart contract that directs that, on the notification of Alice's death, her DCTs will be transferred

³ Some computer developers believe that the code of the smart contract can be made to govern the contract itself—code is law—possibly with tragic results. See for example, the promotion document of the ill-fated DAO, <https://archive.fo/0trrl>

⁴ ICOs are generally conducted through smart contracts.

automatically to Ben, Christopher and Donald equally.⁵ An analysis of the rights and obligations that arise out of smart contracts can be interesting and complex and they need careful examination.

Procedural

Self-help

18. There are examples of the individuals involved in a cryptocurrency sorting out a mess without outside interference, but it needs the cooperation of many individuals who are primarily interested in their own financial advancement and is rare. But can be an effective exercise. Examples are the hard fork remedying the DAO fiasco,⁶ and the Bitfinex hack in August 2016, after which the company issued tokens that could be redeemed for its own shares.⁷

Jurisdiction

19. With coin tokens, there are no contractual provisions and the transaction processing takes place in many jurisdictions around the world. No jurisdiction or governing law is selected by the participants. It is necessary, therefore to look at the applicable European Regulations.

(1) Article 10 of Rome II deals with unjust enrichment and the governing law is that of any associated contract, as determined by habitual residence or close connection. Article 4 of Rome II determines the law in connection with fraud: place of damage or close connection.

(2) Article 4 of Rome I determines the governing law of a contract claim: habitual residence, place of performance or close connection.

Parties

20. As demonstrated in Figure 1 above, transactions on the blockchain are between numbers. Although each number is uniquely linked with a person or persons, it is extremely difficult to

⁵ This would probably be a trust arrangement but might be arranged as a testamentary gift

⁶ See the analysis of the SEC at <https://www.sec.gov/litigation/investreport/34-81207.pdf>

⁷ See the Wikipedia article at https://en.wikipedia.org/wiki/Bitfinex_hack

identify those persons: this is known as pseudonymity. There are available techniques that might result in some success.

- (1) Chainalysis.com is a company that has an extensive experience in analysing transactions in blockchains, primarily for money laundering purposes. There are other such companies.
- (2) If a person can be found who was innocently caught up in the wrongdoing of another, that person can be compelled to disclose the identity of the actual wrongdoer.⁸ So, for instance, in appropriate circumstances identification might be possible from k.y.c. information given to a bitcoin exchange.⁹
- (3) Proceedings will be properly constituted if the defendant is named by description, such as “the bitcoin-holder with the public key ‘02a1633cafcc01ebfb6d78e39f687a1f0995c62fc95f51ead10a02ee0be551b5dc’”.¹⁰ This is unlikely to cure the problem; enforcement then becomes the hurdle because the defendant will need to be identified eventually.

Service

21. For the same reasons, service is a difficulty. Substituted service, or service by an alternative method,¹¹ is unlikely to very useful if the identity of the defendant is not known; the public key holder might live in Uzbekistan and there is at present no way to send messages through the protocol to a public key holder. An order to dispense with service is not likely to be made if the identity of the holder is not known.¹²

⁸ *Norwich Pharmacal Co v Customs and Excise Commissioners* [1974] AC 133

⁹ For instance, Bitstamp in the UK

¹⁰ *Bloomsbury Publishing Group plc and another v News Group Newspapers Ltd* [2003] 1 WLR 1633; The FBI is currently involved in an application in the US against Coinbase, for information about its clients: see <https://www.coindesk.com/bitcoin-judge-approved-irs-coinbase-users/>

¹¹ CPR 6.27

¹² CPR 6.28

United Nations model law adoption

22. What is necessary is a model law that can be adopted around the world, so that injunctions can be ordered to prevent processing of transactions that originate from hackers or so that identification information can be sought from anyone that does have it.¹³

Evidence

23. Apart from the issue of pseudonymity, there is plenty of evidence available. In almost every blockchain the information is in the clear (is not encrypted) and can be viewed. An example is in the statistics gleaned from transactions over 24 hours and shown in Figure 1. Figure 2 shows a transaction on the Ethereum blockchain, for an instance of a smart contract by which 10 QTUM tokens were transferred.¹⁴ Figure 3 shows statistics about the last 5 blocks on the bitcoin blockchain as at the time of writing and Figure 4 shows the formation about a transaction that has not yet been confirmed by the transaction processors (known as “miners”).

¹³ See, for instance, the UNCITRAL Model Law, in respect of International Commercial Arbitration

¹⁴ It is what is known as an ERC20 token, a standard that has been developed for ease of use in ICOs. QTUM is one of the more successful ICOs.

Sponsored Link: **B Bankera** - the bank for the blockchain era. [Participate in the initial coin offering.](#)

Overview | Event Logs | Comments


Transaction Information Tools & Utilities

TxHash: 0xbe5ad2a016b3d1c62dea300ae6bbc261273d92a8e6dac8234f2880d7d54a4bfc

Block Height: 4365712 (13 block confirmations)

TimeStamp: 6 mins ago (Oct-14-2017 06:10:33 PM +UTC)

From: 0xea3e20c0e1e194b91f485cba126d03f8988ad25e

To: Contract 0x9a642d6b3368ddc662ca244badf32cda716005bc (QtumTokenContract) 
10 Qtum TOKEN Transfer From 0x0ace5887862efc347f2d... to 0xea3e20c0e1e194b91f48...

Value: 0 Ether (\$0.00)

Gas Limit: 43633

Gas Used By Txn: 28633

Gas Price: 0.000000021 Ether (21 Gwei)

Actual Tx Cost/Fee: 0.000601293 Ether (\$0.21)

Cumulative Gas Used: 528977

Nonce: 3787

Input Data:

```
Function: transferFrom(address _from, address _to, uint256 _value)
MethodID: 0x23b872dd
[0]:000000000000000000000000000000000000ace5887862efc347f2d2b141c24fdbb972f447b
[1]:000000000000000000000000000000000000ea3e20c0e1e194b91f485cba126d03f8988ad25e
[2]:0000000000000000000000000000000000000000000000000000000008ac7230489e80000
```

Figure 2

Latest Blocks

Height	Age	Transactions	Mined by	Size
489822	6 minutes ago	2327		933554
489821	9 minutes ago	1453		983377
489820	13 minutes ago	1873		969899
489819	15 minutes ago	2058	SlushPool	988535
489817	34 minutes ago	2170		950172

See all blocks

Latest Transactions

Hash	Value Out
f92277b4ee1086ac109d3fbce38823c466daded05be...	0.01255005 BTC
e6d29a5aa9f2df78ec368dd83dd1485b6d82d479348...	0.04549621 BTC
aa9176eff35bfaa08902cce7957841e6209c1d264bc3...	1.39800999 BTC
d666f467a7dea7f3aad8e3bdc27c25a99cfe350c20de...	0.03745016 BTC
2e72e0438499add9ae1e58ea1b779ef7537d147f0c0...	0.50250719 BTC
a3e6d770928f03bb3aa2a3ba50cc6e6c956447ccd3e...	0.0024428 BTC
408d8e47a8984ff8dc71bd9b341945235cb45f91a35...	14.68751944 BTC

About Block Explorer

Bitcoin Block Explorer is an open source web tool that allows you to view information about [blocks](#), [addresses](#), and [transactions](#) on the Bitcoin blockchain. The [source code](#) is on GitHub.

[What is bitcoin?](#)


Public Bitcoin API: Machine readable stats & blockchain info can be accessed directly through the [REST](#) and [Websockets](#) APIs.

Testnet is Bitcoin's sandbox. Block Explorer supports viewing both the [testnet](#) and [mainnet](#) blockchains.

Thanks to [Private Internet Access](#) for hosting the site. They provide a [VPN Service](#) that accepts Bitcoin.

Figure 3


Transaction

Transaction 01386abd710dec037001dd9418d6e513e5df35927d84b4779da54055a7ac88ef 

Summary

Size	226 (bytes)
Fee Rate	0.00239 BTC per kB
Received Time	Oct 14, 2017 7:18:32 PM
Mined Time	N/A
Included in Block	Unconfirmed

Details

01386abd710dec037001dd9418d6e513e5df35927d84b4779da54055a7ac88ef 

1Fy27ZgKG89b8KnYWuPNoHN473FdC5KSNp	214.6563285 BTC	➤	1NwF9Uj5EdXWgD8YZ65oLmvVZ4IMkjbvUT	30 BTC (U)
			1Fy27ZgKG89b8KnYWuPNoHN473FdC5KSNp	184.65578836 BTC (U)

FEE: 0.00054014 BTC

UNCONFIRMED TRANSACTION! 214.65578836 BTC

Figure 4