UK Outlook sponsored briefing: ‘Hodl’, ‘Hit the moon’, ‘Lambo’, ‘Miners’

17 May 2018 09:30am | Guest Blog

Disputes Yearbook 2018 Brown Rudnick Cyber security

Brown Rudnick’s Jane Colston considers asset tracing and enforcement across the blockchain

As comedian John Oliver recently said: ‘Cryptocurrencies and blockchain [are] everything you don’t understand about money combined with everything you don’t understand about computers.’

The technology behind blockchain is complicated, but on top of that, there is the cryptocurrency jargon to get to grips with.

Litigators, especially fraud litigators, need to be conversant with the terminology, the technology and the issues that arise when seeking to trace across the blockchain. Also, bitcoins are the fifth most valuable global currency which, as a new asset class, makes cryptocurrencies relevant to judgment enforcement.

What is the blockchain?

The blockchain is a public and online cash ledger that records in real time all purchases and transactions regarding cryptocurrencies.

The blockchain can be used to record almost any transaction, including assets like art, diamonds and land, as well as intangible assets such as electronic money (eg bitcoins),

securities transactions and other financial instruments.

A key feature of the blockchain is that there is no central administrator (like a bank), server or centralised data storage, which authenticates and updates the ledger with new transactions. Instead, the ledger is stored on many record keepers’ computers (in cryptocurrency speak: ‘miners’). A transaction is only entered on the ledger/the blockchain if all the miners agree it is authentic, eg if they have validated that the bitcoin being used in the trade exists and is owned by the spending party. Once entered on the blockchain, information can never be erased, as each time a new block (a bundle of transactions) is created it is hashed back to the previous block, extending the chain.

The blockchain can do this because of the work of the miners who are located across the globe (many are in China) and have access to considerable computing power. The miners are ‘paid’ with bitcoin. The miners are not concerned with the actual exchange of value taking place on the blockchain, but the authentication of each transaction. As a consequence of the miners’ activity, an identical ledger recording all transactions is held on the computers of each of the miners. The creation of the ledger in this way means that it is a secure and permanent record of every single transaction ever made using the blockchain.

This structure, coupled with the sheer number of miners participating in transactions, helps to protect the integrity of the ledger against cyber attacks.

As the blockchain offers a decentralised way of carrying out transactions, banks or other intermediaries are not needed to authenticate and process the transactions. The blockchain therefore allows you to ‘cut out the traditional middle person’ and any fees that come with their services.

What are bitcoins?

The blockchain was originally developed to enable bitcoin transactions to take place. Bitcoin is a type of virtual currency. It is the most well-known cryptocurrency, but there are hundreds more. Numerous companies now accept bitcoins as payment, eg Expedia and Microsoft.

How do you acquire bitcoins?

- As payment for goods or services.
- You can earn bitcoins through competitive mining.
- You can purchase bitcoins at a bitcoin exchange, which is a place to buy and sell cryptocurrencies with traditional currency or to trade between different cryptocurrencies.
- Lastly, ownership of a bitcoin ‘wallet’ where bitcoins are stored, can be passed – on a flash drive or electronically – to another person.

What is a wallet?

Once a user buys cryptocurrency, eg via an exchange, those coins stay on that exchange until they are removed into a person’s password-protected digital ‘wallet’.

The wallet can be held in a secure cloud environment, on a computer, in a hardware wallet, on a USB or app. A wallet is a personal interface to the bitcoin network.

Bitcoin wallets contain bitcoins, the ‘public key’ and the ‘private key’. The public key is a series of unique numbers and letters that is visible to other users on the blockchain (like an email address would be) and allows a user to receive cryptocurrency. The private key (a password) is known only to the cryptocurrency owner and is required to deal with/spend the coin or complete a transaction (like a digital signature). If you have the password/the private key, you own the bitcoin.

> Disclosure and search orders obtained from the courts can be used to identify if a defendant has any cryptocurrency and/or has received stolen monies in the form of, for example, bitcoins.
> *Jane Colston, Brown Rudnick*

The bitcoin network will not recognise any other evidence of ownership than the possession of the public key and the private key.

What are the challenges when seeking to trace stolen monies or enforce a judgment?

The fact that the owner of the private key remains hidden gives rise to challenges when seeking to trace stolen monies or enforce a judgment.

Disclosure and search orders obtained from the courts of England and Wales can be used to identify if a defendant has any cryptocurrency and/or has received stolen monies in the form of, for example, bitcoins. Such orders should specifically seek disclosure of cryptocurrency. If disclosure is not made, the challenge is finding out about any cryptocurrency owned by the defendant. Norwich Pharmacal orders may assist, but there is no immediate, identifiable intermediary from which to seek such disclosure. The defendant should be compelled therefore by court order to disclose, eg bank account statements, in order to see if bitcoin-related purchases have been made from a cryptocurrency exchange or online merchants.

Further, the imaging and forensic analysis of data obtained from a search order may show if cryptocurrency software has been installed; or if the bitcoin wallet or public/private keys are stored on the defendant’s computer or elsewhere (thereby allowing you to view all their transactions on the blockchain); or if they are using a particular exchange. Without using an exchange it is difficult to realise gains made in the bitcoin economy, lawful or otherwise.

Finally, analysis can also be done by blockchain investigators, to identify digital trails left by bitcoin transactions, eg by user’s behaviour patterns and publicly-available information. This technique can be used to follow the flow of bitcoins from a transaction to a cryptocurrency exchange. Once you have identified an exchange, a court order might then be obtained against it to get information about the bitcoin owner as exchanges often require proof of address before a person can convert between conventional currencies and bitcoins.

Jane Colston, partner, Brown Rudnick
T: 020 7851 6059
E: jcolston@brownrudnick.com

Jane Colston is one of the award-winning, 14 litigation-partner team at Brown Rudnick London, combining cross-border civil fraud, criminal and regulatory experience under one roof. In 2018 the team won The Legal 500 award for civil fraud litigation. Colston has acted in numerous complex, cross-border fraud cases and has extensive experience of forensic investigations. She has managed numerous cases involving freezing, search, disclosure, gagging and delivery-up injunctions.

Return to the Disputes Yearbook 2018 menu