THE DEVELOPING CRYPTOASSET LANDSCAPE IN THE UAE

Spotlight on distributed ledger technology

Ravinder Mattu and Victoria Ferres

Victoria: Welcome to this Allen & Overy podcast. My name is Victoria Ferres and I'm a senior associate in Allen & Overy's Middle East Financial Services Regulatory group. I'm joined by fellow senior associate Ravinder Mattu who is part of our Middle East Technology and Data Protection team ["Hello"].

This podcast forms part of a series where we will be focusing on key considerations relevant to the emerging cryptoasset landscape in the UAE, so we do recommend that you check out the full series. The series will be of interest to anyone already involved in the crypto space, or anyone who is seeking to become involved in the crypto sector in the UAE, or in the broader GCC region.

In this episode we are going to focus on distributed ledger technology, which itself forms the basis of blockchain.

Before we get started, Ravi, perhaps you'd briefly like to introduce yourself to our listeners?

Ravi: Thanks, Victoria. Hello everyone. As Victoria mentioned, my name is Ravinder Mattu and I'm a senior associate in our Middle East Technology and Data Protection team. I've been in the region with A&O for over four years now and we're certainly the busiest we've ever been given the explosion of interest in both technology and data protection matters over the past 18 months.

Victoria: Understandably. So, I guess the question on everyone's lips is, what is distributed ledger technology?

Ravi: Distributed ledger technology, or DLT, is a way of enabling the secure functioning of a decentralised digital database and is the building block of "internet of value". "Value" refers to any record of ownership of asset – for example, money, securities or land titles – and also ownership of specific information like identity, health information and other personal data, which obviously has data protection implications, which we'll come on to in a bit.

Victoria: It sounds like a good idea in theory, but what are the key advantages of DLTs?

Ravi: One of the key advantages of distributed networks is that they eliminate the need for a central authority to keep a check against manipulation.

For example, traditional ledgers do maintain data at different locations and each location is typically on a connected central system, which updates each one of them periodically, making the central database vulnerable to cyber-crime and prone to delays since a central body has to update each distantly located ledger.

Whereas for a DLT, the very nature of a decentralised ledger makes them immune to cyber-crime, as all the copies stored across the network need to be attacked at the same time for the attack to be successful, which is practically impossible. Additionally, the simultaneous, or peer-to-peer, sharing and updating of records make the whole process much faster, more effective, and cheaper.

Victoria: Ok. You've convinced me that DLTs are a good idea in principle, but how do they work?

Ravi: Distributed ledgers use independent computers, referred to as nodes, to record, share and synchronise transactions in their respective electronic ledgers, instead of keeping data centralised as would be the case in a traditional ledger. This is what we mean by a peer-to-peer network.

More specifically, blockchain technology then builds on these decentralised ledgers. In other words, each block of the ledger contains data about transactions that have been executed on the platform. In order to add a block to the ledger, every computer node of the network needs to verify and validate it, meaning the overall system does not need an intermediary to check transactions. Importantly, information stored in a blockchain can never be deleted and serves as a verifiable and accurate ledger of every transaction made within the system, which is why it is potentially so attractive.

The technology can also be used to sign contracts automatically. For example, smart contracts can be coded to be self-signing, so if conditions A and B occur and are verified by the blockchain, then cryptocurrency is automatically unlocked and becomes controlled by the other party. Such a transaction would be virtually irreversible and demonstrably verifiable. We anticipate that these type of contracts would have particular application for more commodity-based transactions.

Victoria: You mentioned that blockchain networks are based on DLTs. Can you tell us a bit more about what blockchains are?

Ravi: Blockchain networks are broadly categorised as either:

- public chain (or "permissionless"): where any person can become a participant to a public network and can access information stored in the network database; or
- private chain(or "permissioned"): where only invited persons can participate in a private network or access information stored in the network database.

Typically, the categories of public/private or permissionless/permissioned blockchains are used interchangeably, as they both describe the amount of access a particular blockchain provides to its underlying data. However, there is a technical distinction between the two.

The public/private networks technically refer to transaction content, in that a public blockchain's transactions are available publicly (that is, anyone can view the contents of the ledger or verify their legitimacy), whereas a private blockchain's transactions are not.

In contrast, whether a blockchain is a permissioned/permissionless network refers to restrictions around its transaction processing; a permissioned blockchain restricts the right to validate and store transactions on the blockchain to invited participants only, whereas a permissionless blockchain enables anyone to write data to the blockchain.

Victoria: And what are the advantages and disadvantages to these types of networks?

Ravi: There are advantages and disadvantages to both types of networks. It is expected that most commercial blockchain applications will utilise a private (and permissioned) chain, at least initially, principally due to concerns over privacy and control, but, as I mentioned, there are advantages and disadvantages to both approaches.

For example, private and permissionless blockchains give users confidence that a counterparty controls the asset which is the subject of a transaction meaning that the transaction in relation to that asset has properly occurred, making it less important to know the identity of one's counterparty. Users can therefore transact on a blockchain in relative anonymity without impeding the blockchain's effectiveness. This anonymity may raise issues for regulators in relation to money laundering and terrorism financing.

Use of a public blockchain is generally described as pseudonymous rather than strictly anonymous, as users are required to transact using a public key. If this public key otherwise becomes associated with the user's personal identity (for example, because it is used for other transactions), it may become possible to identify the user, in which case the public key would be deemed the personal data of the relevant individual, which will have data protection law implications; something we'll discuss in a bit. A user's identity may also be established when the user is required to interact with other institutions for verification purposes.

Victoria: Finally, what can you tell us about tokenisation, which is a word that is being bandied around increasingly frequently?

Ravi: Tokenisation is the process of turning a meaningful piece of data, such as an account number, into a random string of characters called a token that has no meaningful value if breached. In other words, tokens serve as reference to the original data, but cannot be used to guess those values. That's because, unlike encryption, tokenisation does not use a mathematical process to transform the sensitive information into the token. There is no key, or algorithm, that can be used to derive the original data for a token. Instead, tokenisation uses a database, called a token vault, which stores the relationship between the sensitive value and the token. The real data in the vault is then secured, often via encryption.

Essentially, therefore, tokenisation can turn almost any asset, either real or virtual, into a digital token, enabling its digital transfer, ownership and storage without needing an intermediary. These transfers can then be made on distributed ledger technology.

So practically, the value of a token can be used in various applications as a substitute for the real data. If the real data needs to be retrieved – for example, in the case of processing a recurring credit card payment – the token is submitted to the vault and the index is used to fetch the real value for use in the authorisation process. To the end user, this operation is performed seamlessly by the browser or application nearly instantaneously. They're likely not even aware that the data is stored in the cloud in a different format.

Victoria: That's fascinating. Are you able to tell us how a token can be transferred on a DLT by way of a smart contract?

Ravi: From a technical perspective, there are four steps to turn an asset into a token that can be transferred on a DLT by way of a smart contract. Firstly, the interface standard of the token needs to be chosen – ie the interface to be used with the DLT. There are different standards for different assets. For example, ERC20 is a standard interface for interchangeable tokens like voting tokens or virtual currencies; ERC721 is a standard interface for non-interchangeable tokens, like a deed for artwork or a song; and ERC777 allows people to build extra functionality on top of tokens, such as extra data protection, privacy or an emergency recovery function to bail you out if you lose your private keys.

The second step is to consider the asset that is being transferred and decide on the design of the token accordingly. For example, the last four digits of a payment card number can be preserved in the token so that the tokenised number (or a portion of it) can be printed on the customer's receipt so he can see a reference to his actual credit card number. The printed characters might be all asterisks plus those last four digits. In this case, the merchant only has a token, not a real card number, for security purposes.

Step 3 is to audit the code to be used for the smart contract on the DLT to minimise security risks, and then step 4 is finally to issue the code and token on the DLT for transfer.

Victoria: So if you had to very briefly summarise the advantage of tokenisation, what would you say?

Ravi: The advantage of tokens is that there is no mathematical relationship to the real data they represent. If they are breached, they have no meaning. No key can reverse them back to the real data values. And, of course, being exchanged on DLT makes such transactions even more secure and efficient.

Victoria: Thanks Ravi for your insights, this is definitely a very interesting space and I'm excited to see how it develops on both a practical and regulatory level.

Well, that brings us to the end of this episode. As we mentioned at the outset, this does form part of a series of podcasts we are releasing on all things crypto, so do look out for the other episodes. Thanks for listening and please do get in touch if you have any thoughts or comments on this podcast.

Ravinder Mattu
Senior Associate
Technology and Data Protection
– Middle East
Tel + 971 2 418 0434
ravinder.mattu@allenovery.com

Victoria Ferres
Senior Associate
Financial Services Regulatory –
Middle East
Tel + 971 4 426 7274
victoria.ferres@allenovery.com