Blockchain and Crypto Currencies

Blockchain and Crypto Currencies

LNB News 17/11/2017 24

Published Date

17 November 2017

Jurisdiction

United Arab Emirates
Relevant Companies

Afridi & Angell

Abstract

Blockchain technology is attracting the attention of Governments, business people and consumers. The headline-grabbing cryptocurrency, ‘Bitcoin’, is the best known application, but the implications and potential uses of Blockchain technology and, more broadly, distributed ledger technology (DLT), are much broader than Bitcoin and other crypto currencies.

Analysis

What is Blockchain Technology?

A Blockchain application is a distributed database which records information in a ledger format. The information recorded on any Blockchain is copied across the network of computers who choose to run a particular application (each a node). The software records a continuous and complete ‘chain’ of entries or transactions, each cryptographically linked to the last. Blockchain applications use cryptography to protect the integrity of the information recorded.

Why use Blockchain?

The advantages of Blockchain are broadly considered to be the reliability and immutability of information the technology offers as well as virtually unbreakable security and an ability to facilitate peer-to-peer transactions at a significantly reduced cost compared to traditional centralised systems. Blockchain applications are said to be decentralised, as they do not rely on any owner or administrator to run or govern or maintain the application. This feature improves their security since there is no central database to hack.

Bitcoin

The best known and largest Blockchain application is Bitcoin which is a type of (but not the only form of) ‘cryptocurrency’, which is essentially a form of digital money. This digital money has tended to be most attractive to speculative investors. No merchant has to accept it and as at the time of writing it is not widely accepted in mainstream business. Crypto currencies are generally treated as commodities by regulators.

The Bitcoin Blockchain is an example of an open Blockchain network which any individual can be a part of. Open Blockchain networks of this type are often referred to as ‘un-permissioned Blockchains’. Conversely, a Blockchain network can also be private and, in the case of private networks, there is someone who controls the network and the controller can limit participants. Private Blockchain networks are also referred to as ‘permissioned Blockchains’. This is an important difference to take note of.

Can we trust the data on a Blockchain application?

In both permissioned and un-permissioned Blockchains, the ledger is copied on every computer which forms part of the network, meaning there is complete transparency across the user base because all nodes in the network have an independent copy of the data in the ledger. Therefore, two questions from a legal perspective are: how is the data on a Blockchain protected and should we trust it?

As the term already suggests, one of the essential characteristics of a Blockchain application is the concatenation of blocks. Those blocks of date are interconnected and encrypted in a way which ensures data cannot be manipulated or deleted after the data has been entered into a block. Therefore, we can trust the data to be accurate from the beginning. However, whilst the data may be accurate because it correctly reflects the input, the data may not be reliable, because the input might not have been accurate. It is therefore critical to understand the source and quality of input in order to assess its level of trustworthiness.

It is also worth noting any node’s (i.e. user’s) access to a Blockchain application will probably be password protected, so if the password is stolen and misused, abuse or fraud can occur through credential theft just as it can with non-Blockchain applications. Blockchain technology itself may therefore be secure and reliable, but the elements of human input and access remain subject to the usual cautions.

Are there privacy concerns?

Arguably, Blockchain applications have data protection by design, as the entries stored on them are encrypted in a way which makes changing or deleting them virtually impossible. Privacy questions can arise because all information recorded on a Blockchain application is visible to all users on the Blockchain, so everyone can see everyone else’s transactions. Most Blockchains will not show personally identifiable information as individual users are identified by their so-called public key (a string of numbers), so at first blush anonymity may be maintained. However, the parties to a transaction will likely know the identity of one another and they could disclose publicly the identity behind the other's public key and once known, anyone who was interested would be able to identify all transactions by a person, which could indeed be very personal. In addition, it is easily foreseeable more and more data which could reside on Blockchains may be of a personal nature, thanks to advances in digital identity and the internet of things. Where the data is instantly made available to a wide network of participants across many jurisdictions, data protection concerns become a real issue and must be analysed in the context of existing laws which will not have contemplated Blockchain.

What recourse do we have if something goes wrong?

The first consideration in relation to what recourse you may have when using a Blockchain application is whether the Blockchain is permissioned or un-permissioned. In the case of un-permissioned Blockchain networks, no-one is accountable if something goes wrong. The peer-to-peer relationships are governed by the general 'rules' of the Blockchain (i.e. the underlying code). For this reason, participants must either simply trust the application or make themselves comfortable with the code from a technical perspective, because there is no person or centralised body to which a participant can seek recourse for failures in the software.

In contrast, in the case of permissioned Blockchain networks, there will be a centralised controller of the network who is responsible for limiting the participants to the network and ensuring participants only see what they need to see. It is likely permissioned Blockchains will be commercial applications sold by their developer and will be supported by contractual terms and conditions which allocate liability in the event of a fault. For this reason, permissioned Blockchain applications are likely to be the preferred option for mainstream business.

What are the anti-money laundering and Know Your Customer implications?

Crypto currencies are a high risk 'currency' because they have a reputation for being a means by which crime and money laundering is facilitated.

Bitcoin is not a regulated currency or legal tender, which means it is not difficult to purchase Bitcoin with the proceeds of crime and to use those Bitcoins to purchase legitimate goods or services, or exchange them for fiat currency. The anonymity of the participants, the lack of traceability of virtual currency users and the potential ability to circumvent laws and sanctions all raise clear legal issues.

For businesses who do choose to deal with crypto currencies, Know Your Customer (KYC) procedures are important because, in the context of transfers of value, every business has an obligation to confirm the legal identity of the person it is dealing with, as well as the source of funds. This may be difficult in the virtual world because we are not yet at the stage where we have reliable, Government-recognised, digital identities. This will come. However, until then, when businesses are receiving funds from their clients by way of crypto currencies, the solution may be to treat those clients as high risk clients and to carry out well document enhanced KYC.

What are the uses for Blockchain technology?

There is no shortage of blue-sky thinking around the potential applications for Blockchain technology as any cursory search will show. It will be transformative and mainstream and it demands attention by any responsible business, as it is impossible to avoid. Blockchain technology has the potential to be the backbone of many core platforms. One example is smart contracts. A smart contract is software code which creates self-executing and self-fulfilling so-called 'contracts'. They create a very binary 'if this then that' sequence: if 'this' happens, then 'that' will happen automatically. For the time being, lawyers' jobs are in no danger from smart contracts due to limitations on the usefulness of smart contracts. For example, the 'if this' element must be something the smart contract will be aware of, meaning it must be an event which shows as an entry on a Blockchain on which the smart contract resides. If it requires any human intervention whatsoever to confirm the event happened (referred to as an 'external dependency'), the purpose is defeated entirely. Most uses for smart contracts which people tend to think of (like escrow arrangements or insurance payments) are not currently possible for this reason alone. In addition, bear in mind any payment triggered by a smart contract needs to be paid into the contract (using cryptocurrency like Ethereum) at the time of entering into the contract, meaning it is effectively funded upfront, which is not practical and often not possible. Finally, it is also important to note people will enter into smart contracts based on a description of what they purport to do and the description will be in English or whatever (non-code) language applies. The description, which may be in the form of a contractual wrapper and will contain representations and terms, is what people will rely upon in case of a dispute. Without these terms, anyone who does not comprehend software code will not be able to comprehend the smart contract they are entering into.

However, smart contracts and other Blockchain uses are not being developed in a vacuum. This is a fundamental point to bear in mind when considering the potential for smart contracts and for Blockchain generally. The limitations of smart contracts, for example, may be overcome with ever-increasing interconnectedness of networks, the evolution of artificial intelligence and the internet of things, all of which are developing rapidly and in conjunction with Blockchain applications. Many of the limitations noted above will be overcome in the near to medium term.

What are regulators doing?

Regulators across the globe have been closely watching the development of Blockchain applications. Last October the Dubai Government said it will go paperless by 2020 by moving to a Blockchain-based transaction system across Government entities. Meanwhile the Abu Dhabi Global Market (ADGM) is encouraging FinTech developments which include a strong focus on DLT with initiatives like RegLab. The use of Blockchain technology is gradually being embraced as something which is inevitably going to be a part of everyday life in years to come.

Whereas, in the case of crypto currencies, the general feeling amongst regulators has been they are wary of stifling innovation (or appearing outdated) through premature imposition of regulations. For this reason, regulators have been cautiously reactive rather than proactive, which is appropriate. For example, the UAE Central Bank has recently warned against crypto currencies and urged potential investors to proceed with caution, but has refrained from regulation.

Most major markets have been willing to regulate Initial Coin Offerings (ICO), which allow participants to acquire certain rights which are issued on Blockchain applications. The ADGM, for example, issued guidance stating tokens issued through an ICO which represent ‘a traditional regulated issuance, such as share, debenture or units in a collective investment fund’ will be subject to existing financial regulations and fall under the legal classification of ‘securities tokens’. The guidelines state the applicability of the financial regulations will be determined on a case-by-case basis.

So, whilst regulators have steered away from regulating Blockchain as a type of technology, regulators have, in some cases, been willing to regulate the activities which Blockchain facilitates to ensure market integrity and consumer protection.

Written by James Bowden and Alexandra Aikman.