Mental blocks

Blockchain technology presents users with enhanced security and efficiency, but it is not without its challenges – including overcoming the ingrained habits of its users

BY ALEXANDER LARSEN AND FAISAL ALNAHDY

The last couple of years has seen a real buzz around a new technology called blockchain, which in essence is just a decentralised public database (the chain) of digital information (the block). Transactions are recorded into this public database through consensus across a network of decentralised computers, which is achieved by a proof-of-work system called mining.

Many organisations are implementing it already including IBM, Google, American Express, Oracle, Facebook, Ford, Amazon and Nestlé. There are also blockchain-specific companies offering blockchain solutions for supply chain, social media and stock control. These companies often use crypto-utility tokens within their ecosystem. There are also blockchain-based coins with no other use than that they seek to behave in a similar way to traditional currency and to potentially replace it. Whether a utility token or currency coin, both of which fall into the category of cryptocurrency, most are available for purchasing as investment or as a way of speculating on various exchanges globally.

> “Dhofar Bank in Oman has already implemented the Ripple blockchain

Hacking incidents and vulnerabilities

There has already been a number of major and high-profile hacking incidents which has government regulators concerned. When it comes to hacking, it is not so much

> When it comes to hacking, it is not so much the cryptocurrencies that are the problem, but rather the exchanges on which they are traded and the digital wallets where many of them are held

the cryptocurrencies that are the problem, but rather the exchanges on which they are traded and the digital wallets where many of them are held.

Many exchanges are unregulated or loosely regulated at best. Their governance standards and cybersecurity measures are severely lacking, which is where the problems lie. Some exchanges have been hacked in recent years. Interestingly, hacking risk is also one of the main concerns for the existing banking system, which means fiat and cryptocurrencies have the same security concern. For instance, online banking apps can be exposed to hacking which aims to steal users' login data and debit or credit card information.

A potential solution to hacking incidents on exchanges is the introduction of decentralised exchanges, essentially a cryptocurrency exchange on the blockchain. This would reduce hacking significantly. Unfortunately, it is not currently practical, due to poor user interfaces, but it could become the standard of the future, especially if regulation supports this innovation.

While it is difficult to govern cryptocurrency itself, and due to the fact that cryptocurrency is apparently unhackable, what policymakers should focus on is the regulation of the services associated with the use of cryptocurrencies. Regulation should focus on stricter business practices within exchanges to avoid fraud and scams, as well as introducing minimum but high standards of cyber risk requirements in order to protect against hacking, phishing and other cyber-related attacks.

Most people involved with the technology agree that blockchain networks are virtually unhackable although some argue that all "software" is vulnerable. The one vulnerability that everyone agrees on is that blockchain technology can be hacked through a mechanism called 51 per cent attacks. This happens when 51 per cent of a network is owned by the same group of people, enabling them to manipulate transactions on what is effectively no longer a decentralised network. While this is possible on some of the very low market cap coins and tokens, it is highly expensive, and some would suggest impossibly expensive, on larger market cap coins such as Bitcoin. According to the CEO of a new blockchain company in Oman, who we interviewed, aside from a 51 per cent attack, no one can hack a blockchain. The CEO echoes the sentiment that vulnerabilities tend to exist in the applications that use blockchain technology such as exchanges and wallet.

Blockchain and financial services

Various studies suggest that implementing blockchain in the banking industry alone could decrease expenses by $20 billion by 2022.

opportunity to offer a more secure gift card and loyalty programme that is not exposed to the same data breaches from hacking incidents that has plagued the industry for years. Many suggest that blockchain could also be the solution that Elon Musk needs to get autonomous cars on the road. The threat of terrorists hacking self-driving cars, robots, drones or automated transportation systems in itself is a scenario that would strike fear in any government. Blockchain could provide a solution not only to the hacking threat but also to potential accidents arising from other challenges too, such as the current lack of accuracy of verifying of data collected from the surrounding environment and potential downtimes and systems failures that are inherent in a centralised network.

Challenges

One of the major drawbacks of the technology is the need for mining, which essentially requires computing power. It has been estimated that during a week, the entire blockchain network consumes energy on a par with the total amount of electricity used by Hungary – or 0.25 per cent of the entire planet's energy needs. Recent research estimated that mining could account for 1 per cent of global energy usage by 2020, an amount that would increase rapidly through mass adoption.

Blockchain technology is improving and a number of updates have already made many blockchains more energy efficient. Nonetheless, it should be a concern for governments looking to reduce carbon emissions. Regulation could be introduced to ensure that mining companies adhere to strict renewable energy requirements, although this will also potentially shift mining activities to countries who have less stringent rules on mining activity (and cheaper electricity).

A fully decentralised system would enable users to trade, transfer and receive money directly without intermediaries. It could be argued that some intermediaries may be seriously exposed financially or resist the technology. As a result of this, and in countries or cities largely reliant on the financial sector, unemployment rates could rise, and policymakers therefore need to think about whether creating new roles for intermediaries may be possible in order to avoid this scenario.

There is also the matter of investor and customer protection to consider. The existing centralised financial system has a level of trust built into it that protects money in events such as bankruptcy, fraud or in the event of the death of a family member. This level of protection does not exist in a decentralised system. It seems as though the most likely scenario is a semi-decentralised system, which could therefore still be potentially more vulnerable to cyberattack.

What about GDPR?

A major area of concern for all businesses over the past couple of years has been the General Data Protection Regulation (GDPR), introduced in May 2018 to increase people's data privacy. It presents a possible stumbling block for blockchain implementation. The major areas of conflict include the fact that blockchain would hold personal data that is publicly accessible at the same time as not allowing for changes, such as deletion as per requirements of GDPR under "the right to be forgotten".

This is a direct clash of function. However, by ensuring that the blockchain does not hold any personal details, such as individual names, there may be a way to get around this problem. Additionally, GDPR does not aim at regulating technologies as such, but regulates how organisations use these technologies.

Both GDPR and blockchain's main focus is the protection of data, something which blockchain does very well as we have already discussed, and as a result, while initially it may seem that they are incompatible, blockchain could actually be a potential solution to meeting the GDPR requirements of encryption. Additionally, one of the reasons for the existence of GDPR was the misuse of data by major corporations, something that the decentralised nature of blockchain totally removes from the equation.

The same, but different

A blockchain future with levels of security we have previously not been used to seems difficult to imagine. We have grown accustomed to major cyberattacks and breaches. While blockchain, if embraced and implemented properly, is certain to reduce these attacks significantly, we will still be faced with a fact not yet mentioned in this article. Ninety per cent of cyberattacks come from human error and social engineering – a risk that blockchain would be unable to remove. As technology moves forward, humans seem to be unable to adapt quickly enough. The staggering speed of innovation could mean that while the future may turn out to be very different to today, many of the same old threats could remain.

This article was written by Alexander Larsen $^{\text{CFIRM}}$, president of Baldwin Global Risk Services Ltd, and Faisal Alnahdy, senior auditor at the State Audit Institution in Oman. It is based on Alnahdy's MSc dissertation, "Evaluation of risks associated with cryptocurrency: case study on Oman", which he wrote at Glasgow Caledonian University.

> “ It has been estimated that during a week, the entire blockchain network consumes energy on a par with the total amount of electricity used by Hungary