Blockchain Technology

BLOCKCHAIN TECHNOLOGY

From cryptocurrencies to tokenisation, the level of discussion, perceived potential and interest from regulators in regards to blockchain solutions is at an all time high.

To assist in considering how and when this new technology could be utilised, we take a look at past learnings, current experiences, AUSTRAC's recent activities and potential AML/CTF applications.

The underlying principle of blockchain technology includes:

- A distributed database that is available to all parties and is not controlled by a single party;

- To determine whether a transaction is legitimate, the review process is untaken on a consensus basis as opposed to relying on a central regulator such as a clearing house/central banking institution;

- Peer-to-peer communication instead of information being held by a central party;

- Transaction transparency, where transactions that occur in the database are visible to all; and

- Immutability, transactions that are added to the blockchain cannot be altered without leaving a record.

One application of this transformative technology, and potentially the most well-known and publicised at present, is in the cryptocurrency space.

An overview of this, along with some practical aspects arising from the developing regulatory and operational landscape, is provided below. This is followed by:

- An overview of other potential real-world solutions including smart contracts and tokenisation;

- Examples of applications currently in actual development; and

- How we at RSM can assist in assessing, exploring and harnessing a blockchain inspired solution for your organisation.

WHAT ARE CRYPTOCURRENCIES?

Cryptocurrencies are a new asset class that allows one user to transfer a "coin" to another using blockchain technology, which in turn uses both encryption and open distributed ledger technology to facilitate the process. There are more than 1,300 cryptocurrencies currently available; the best known is bitcoin.

While some cryptocurrencies are built on the same blockchain protocols, they are not all alike. Bitcoin is often compared to gold, Ethereum allows for smart contracts, Monero is built on highly anonymised transactions and Civic is designed to provide government identity data.

RSM

Cryptocurrencies are becoming increasingly popular with investors as they are highly volatile and in some cases, appreciate or depreciate rapidly. For instance, at the beginning of 2017, Bitcoin was trading at about $850 (USD). It then reached an all-time high at almost $20,000 (USD) in the middle of December 2017 and settled at over $13,000 (USD) at year-end. Most currencies have a limited supply, which is one of the reasons the price has appreciated rapidly.

When a cryptocurrency transaction is executed via blockchain technology, the transaction of sending a coin from one person to another is placed in a virtual "block," and that block is then broadcast to participating parties ("miners") on a blockchain network.

Miners are paid a reward (similar to a commission) to ensure that the transactions are valid. Once the transactions are validated, the block is added to the "chain," providing a transparent record of the transaction. A transaction is typically completed in 10 to 15 minutes. In this sense, it is more comparable to a banking transaction than a credit card transaction, which takes place in seconds.
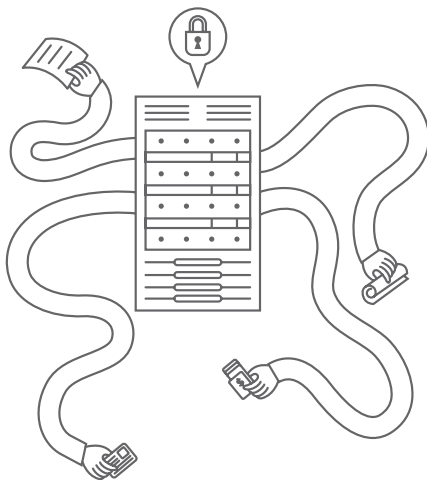
A large, complex cryptocurrency ecosystem has been created, consisting of currencies, exchanges for trading, financial and legal advisors, venture capitalists and hedge funds, market-makers and market researchers, and offline methods for storing the currencies known as "cold storage."

Operational security
The immutability factor means that transactions in the cryptocurrency space are final and cannot be reversed. This can raise some concerns from an operational security perspective as, for example, if an individual:

- Transfers coins to the wrong account, or "wallet," they are gone and cannot be returned.

- Is running a trading operation and an unscrupulous trader moves coins into their own wallet and not the corporate wallet, there is little that can be done to get them back.

- Trades on an exchange that gets hacked or they lose the username/password, the coins are lost.

- Stores coins on a laptop and a hacker breaks in and steals them, they are gone as well.

For these reasons, security in this space is extremely important. Therefore, it is common for users to balance the currencies kept on an exchange, a local computer and in cold storage, explained further below:

Cold storage typically uses a USB key-like device to store the private keys which allow users to send currency.

As with all new technology, certain groups are intrigued by the potential to discover and exploit vulnerabilities in the infrastructure of the software to either bypass or break perceived safety measures. As the potential consequences of a digital wallet being "broken in to" is as severe as in the real world, this is an area which requires constant monitoring — with no central regulator, the question arises as to whether this responsibility resides with the user?

AUSTRAC and the changing regulatory status
Bitcoin was designed, and other cryptocurrencies followed, around the idea of an ecosystem where no one entity is in charge. Changing functions in Bitcoin requires consensus among miners to agree rather than a monetary authority to make policy.

Therefore, many would say that these currencies can't be regulated. Certainly, governments try. The most common regulation in this space is entering and exiting the marketplace — converting fiat currency (dollars, pounds, euros) to cryptocurrency.

RSM
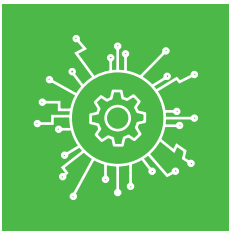
In April 2018, new laws for digital currency exchange (DCE) providers operating in Australia were implemented by AUSTRAC, Australia's financial intelligence agency and anti-money laundering and counter-terrorism financing (AML/CTF) regulator.

The new AML/CTF laws cover, for the first time, regulation of service providers of cryptocurrencies, including bitcoin.

AUSTRAC CEO, Nicole Rose PSM, said the new laws will strengthen the agency's compliance and intelligence capabilities to help DCEs implement systems and controls that can minimise the risk of criminals using them for money laundering, terrorism financing and cybercrime.

Effective immediately, DCEs with a business operation located in Australia must now register with AUSTRAC and meet the Government's AML/CTF compliance and reporting obligations including the collection of information to:

- Establish a customer's identity;

- Monitor transactional activity; and

- Report to AUSTRAC transactions or activity that is suspicious or involves large amounts of cash over $10,000.

In addition to AUSTRAC, the Australian Securities and Investments Commission (ASIC) have published, within information sheet 219, that their approach to developments in the fintech sector is to work to harness opportunities and economic benefits, not stand in the way of innovation and development. At the same time, they have communicated a need to mitigate any potential risks of new business models through the use of new technologies.

At present, it seems ASIC believe that the existing regulatory framework can accommodate blockchain and cryptocurrencies. As this technology matures, they anticipate that additional regulatory considerations may arise.

Interestingly, one of the contributing reasons for rapid price fluctuations in this space result from the changes in regulations throughout the world that impact an investor's ability to buy and sell cryptocurrencies. Whether these continue to evolve in a similar fashion, or pre-empt a period of stability, is still to be seen.

Anti-money laundering issues and KYC opportunities

With both the reports from the Financial Services Royal Commission, and the introduction of the General Data Protection Regulation (GDPR), in 2018, there is significant emphasis on financial institutions to have appropriate processes in place to monitor their internal controls, particularly those that relate to client data security, and to provide comfort over their robustness to regulators and boards.

Assessing the extent to which controls are effective can be challenging to monitor, especially in large and complex organisations with inherently high risks surrounding data security and privacy with respect to the collection and storage of client information.

Because of its anonymous or pseudonymous nature, cryptocurrencies are a natural place for criminals to launder money.

Following the Know Your Customer (KYC) requirements of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML Act) is critical to making sure that organisations are not facilitating criminal activity. While any transaction can be used to launder money, transactions where a cryptocurrency is used as the source of funds or capital is often a higher risk transaction. Determining how or where a person received their cryptocurrency is much more difficult than with a fiat currency.

Blockchain as a platform has the potential for multiple uses within financial services, in addition to disrupting a number of the more 'traditional' processes, one example being KYC.

The benefits of customising and utilising this technology supports the efforts of the financial services industry to mitigate the risk of KYC whilst increasing operational efficiency, reducing complexity and reinforcing a positive customer experience.

RSM

Immutability

An immutable object is *one whose state cannot be modified after it is created.*

This is a key attribute of blockchain technology, especially in its practical application within the financial services, and other, industries. Although it would be impossible to completely protect a system or database, blockchain offers a larger and more distributed network which is currently thought to offer increased levels of security.

The systems which utilise this technology are also able to contain specific applications to detect any unauthorised changes to records.

Further attributes of the technology which all support potential integration in to the systems, process and controls of organisations include all of those mentioned at the start of this article:

- A distributed database that is available to all parties and is not controlled by a single party;
- To determine whether a transaction is legitimate, the review process is untaken on a consensus basis as opposed to relying on a central regulator such as a clearing house/central banking institution.
- Peer-to-peer communication instead of information being held by a central party;
- Transaction transparency, where transactions that occur in the database are visible to all; and
- Immutability, transactions that are added to the blockchain cannot be altered without leaving a record.

OTHER POTENTIAL REAL-WORLD APPLICATIONS

In addition to cryptocurrencies, discussed previously, other extensions of the technology include smart contracts and the ability to "tokenise" assets. The theory behind each of these is as followed:

- Smart Contracts — with the ability to define and embed the rules and penalties of an agreement within blockchain technology, smart contracts allow parties to automatically execute, witness (by hundreds of people)

and enforce the terms of an arrangement which would have historically required the involvement of a lawyer or notary.

- Asset Tokenisation — a methodology which converts an asset which is traditionally "whole", such as a property, into many pieces, or tokens, which can then be traded on an individual basis. In theory, this would enable smaller capital amounts to be invested in to assets which would otherwise be outside the capabilities of the individual. As well as property, this could be extended to works of art, precious stones, or even unlisted businesses. However, as noted previously, without a fully developed, and stable, regulatory environment the question as to who has legal right over the asset, and the consequence of a sale, may require resolution before wide scale adoption.

With a focus on improving the efficiency of existing processes, a number of organisation are in the early stages of piloting real-world applications of blockchain technology using a combination of factors from the key attributes and cryptocurrency learnings already noted. The following are three examples of this.

Walmart
Following the US and Canada's 2017 outbreak of Shiga toxin-producing E.coli, which resulted in 2 deaths and 60 people falling ill, and the 2018 recall of nearly 15,000 pounds of imported beef and pork, Walmart has implemented a blockchain solution which is being used to track pork (China's most popular meat), from farm to supermarket shelf.

After the success of the first pilot in addressing the food safety risk, a second was launched with mangoes in Central America. Frank Yiannas, Vice President of Food Safety and Health, said that blockchain was also able to reduce the time it took to track produce from six days to two seconds.

Coca-Cola
Coca-Cola, in collaboration with the US State Department and two other companies, are using blockchain technology to create a secure registry for workers. This is intended to prevent the use of forced labour worldwide and especially in countries where sugarcane is sourced. The system is designed to create a validated chain of evidence that will encourage compliance with employment contracts.

RSM

Maersk

In early 2018, Maersk, a global leader in container logistics, and IBM announced their intent to establish a joint venture to provide more efficient and secure methods for conducting global trade using blockchain technology.

Their aim will be to offer a jointly developed global trade digitisation platform built on blockchain standards and designed for use by the entire global shipping ecosystem. It will address the need to provide more transparency and simplicity in the movement of goods across borders and trading zones.

By applying the technology to digitise global trade processes, a new form of command and consent can be introduced into the flow of information, empowering multiple trading partners to collaborate and establishing a single shared view of a transaction without compromising details, privacy or confidentiality.

FINAL THOUGHTS

Just as with any new and disruptive technology, the ecosystem around cryptocurrencies is evolving fast.

It is likely that a number of the exchanges will fail, currencies will collapse and people will lose money. That said, this is also still a very big market and it is equally likely that exchanges will flourish, currencies will appreciate and investors make significant gains.

At a time where the appetite for wealth, technology and process improvement are aligned, being prepared and informed will become key especially in regards to the changes to come from an industry, investment, AML, and regulatory perspective.

For further assistance in identifying risks and opportunities within your organisation, reach out to one of our specialised assurance and professional services experts.
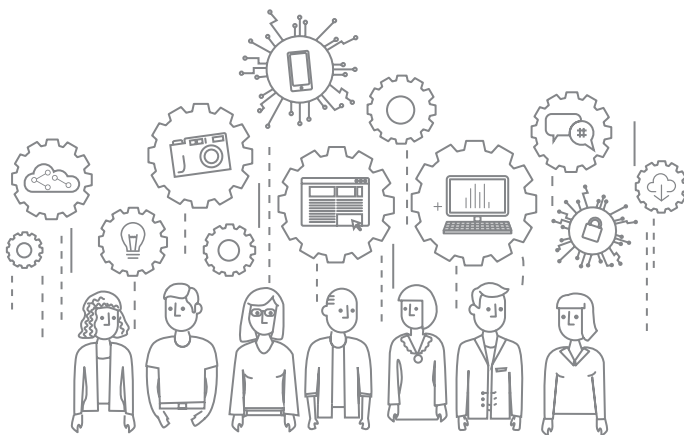
HOW WE CAN HELP

By asking the right questions, RSM can assist in developing future strategic initiatives and operational priorities.

- Why blockchain?
- What is the current state of this technology?
- Is blockchain the right answer?
- If so, what are the risks and opportunities from adopting this technology?
- Will it introduce new risks?

For more information

Our blockchain National Solution Set Leader, Paul Joseph, assisted by Michael Shatter in Melbourne and Jeremy Elman in Sydney, are available to discuss with you the nature, timing and extent of how we can assist in achieving your organisational goals, ensure the effective use of investment funds and time, and appropriately manage financial, technical and operational risk.