The New World Order of Cryptocurrencies and 'The Blockchain'

What does this all mean for investors and why all the hype?

Research Analyst: Daniel Stojanovski

1 February 2018

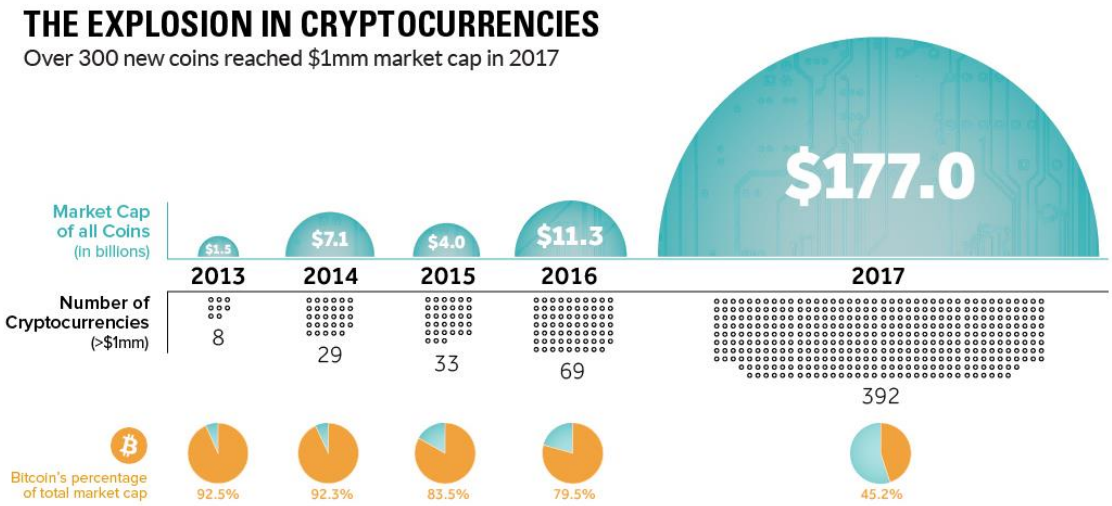
The concept of cryptocurrency was first conceived in January 2009 by a researcher going by the name Satoshi Nakamoto. Satoshi started the open source project known as Bitcoin.

Since 2009 the world has seen the prominence and popularity of cryptocurrencies as well as the technology that underpins them 'The Blockchain', as a new means to store and transfer wealth. The crypto market started originally with Bitcoin, but today there are hundreds of coins on offer for investors, with some of those coins experiencing some gigantic highs and some very volatile lows.

Like traditional currency, cryptocurrencies have no intrinsic value (it is not redeemable for another commodity such as gold), but unlike traditional currency they have no physical form (only existing in the network), and supply is not determined by a central bank (the network is decentralised).

Cryptocurrencies are physically precomputed files which use a 'public/private key' pair which are generated around a specific encryption algorithm (the public key tells the block chain your anonymous holding and the private key holds your private identification. The key assigns ownership of each 'key pair' or 'coin' to the person who is in possession of the private key. These key pairs are stored in a file names 'wallet.dat', which resides in the blockchain. The wallet.dat file is the most important file of cryptocurrency software architecture, as that is where the physical cryptographic private key file is stored. Much like cash in a physical wallet, if a user loses their wallet.dat file, or has it stolen, then the cryptocurrency is lost.

Figure 1: The unparalleled explosion in cryptocurrencies



Source: Visual Capitalist, Coinmarketcap.com, August 2017

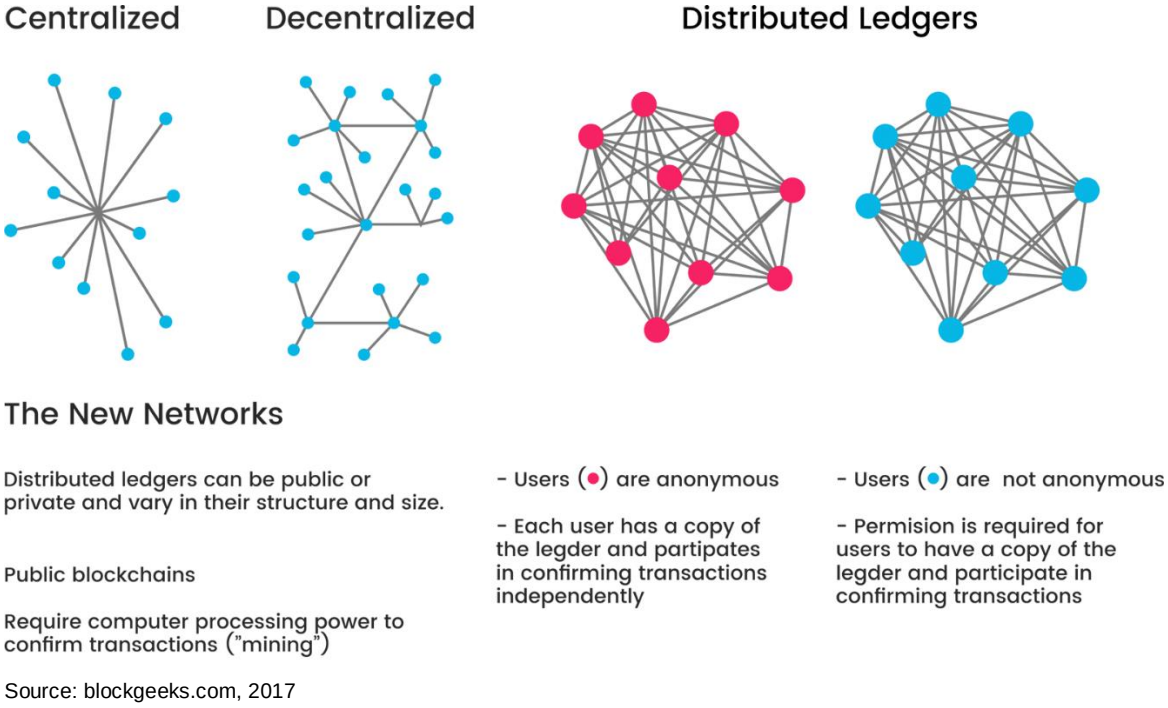
What do we mean by 'The Blockchain'?

Blockchain, also known as the public ledger is the technology that underpins all cryptocurrencies. According to the 'University of Cambridge, Centre for Alternative Finance' the blockchain is defined as a "*record of all validated transactions grouped into blocks, each cryptographically linked to predecessor transactions down to the genesis block, thereby creating a 'chain of blocks*'". What is this definition saying?

Picture a spreadsheet that is duplicated thousands of times across a network of computers. Computers like your own, at work and around the world. Then imagine, that the sole purpose of this network, is to update regularly this one spreadsheet. When people buy coins, sell, and transact (via their wallet.dat) this is all recorded on the spreadsheet and agreed upon by all computers in the network. Similar to EFTPOS which facilitates point of sale payments, and CHESS which facilitates trade authorisation on the ASX, blockchain facilitates the transfer of coins and the maintenance of public ledger that identifies who holds what, this is what you call a distributed ledger. Now you might say what stops people from manipulating the ledger? When people make changes to the ledger the network checks the spreadsheet, if it does not match up, that manipulated ledger is rejected. Participants who hold the blockchain ledger are incentivised by being paid fractions of coins over time.

This technology is extremely effective and has the ability to safely store records, legal documents, transactions and payments. Figure 1 shows graphically the difference of current networks (centralised and decentralised) vs the distributed ledger. Companies and stock exchanges alike are all investing heavily to use a blockchain in order to store and transfer. Which can possibly replace the traditional methods we use today.

Figure 2: The blockchain



Source: blockgeeks.com, 2017

Coins on offer – The Cryptocurrency overview

There are hundreds of cryptocurrencies on the market, the top 4 currencies by market cap are;

Bitcoin is the original cryptocurrency, and undoubtedly the most popular/prominent. It was designed with the idea of being a new form of digital money in order to allow users to make peer-to-peer transactions. It uses cryptography to control its creation/money supply, rather than a central authority, making this currency decentralised. Bitcoin uses the blockchain technology as a tool that keeps a record of every transaction and holding. The decentralised structure means that the Bitcoin network is owned and controlled by users, which must follow a set of rules. Users are rewarded for maintaining the network via the computing power of their devices, tasks such as "mining" adds to the supply of bitcoins. Bitcoin will have 21 million coins in total circulation, which is the maximum amount that can be mined. Cryptocurrencies are tradable in fractions out to multiple decimal places which could be increased if needed. An interesting fact about bitcoin is, in 2010 a programmer bough two pizzas for 10,000 BTC (bitcoins), which was one of the first real-world bitcoin transactions. Today that same transaction would roughly equal $80 million USD, which is why on the 22nd of May 'Bitcoin pizza day' is celebrated worldwide by the crypto community. The programmer can be forgiven for his transaction since no one knew bitcoin would be accepted by hundreds of thousands of people in a few short years (since 2012 bitcoin is made roughly 67,000% return).

Key features

- Uses blockchain technology
- Low processing fees
- Decentralised
- Available to anyone
- Partial Anonymity
- Transparent
- Only has 21 million bitcoins of capacity.

Ethereum was officially launched in 2015 and is a decentralised computing platform which features its own Turing-complete programming language. Ethereum was developed in an effort to improve bitcoin, through the expansion of its capabilities. The defining feature of Ethereum is around the use of 'smart contracts' (decentralised, self-executing agreements which are coded into the blockchain, essentially financial agreements similar to options contracts, coupon-paying bonds or swaps). The blockchain records scripts or 'smart contracts', which are then executed by every participating node (a node is a piece of software that connects to other nodes, thus participating in the formation of the network), these nodes are then activated through payments into the cryptocurrency 'ether'. Ethereum has attracted significant interest since its creation from many developers and institutional players, thus increasing its size and use. The Ethereum blockchain works differently to that of bitcoin, where instead of mining for coins, miners in Ethereum work to earn 'ether' (a type of crypto token, which fuels the network). This ether is used by developers to pay for transaction fees and services in the Ethereum network. An interesting fact around Ethereum is, due to its increasing value since its launch in 2015, it has quickly become the second most valuable cryptocurrency by market capitalisation. It has increased by 2,226% in the past year.

Key differentiators to bitcoin

- Platform for producing blockchain applications
- Has multiple uses for a range of industries
- Uses smart contracts

Ripple was officially launched in 2012, and unlike the other cryptocurrencies was created as a global settlement network for currencies such as USD, EUR, GBP and BTC (bitcoin), it is also the

only cryptocurrency that does not use a blockchain. Instead Ripple uses a 'global consensus ledger'. Ripple is used by a number of institutional players such as large banks and money service businesses. A function of the Ripple native token is to serve as a bridge currency between national currency pairs that are rarely traded, and to prevent spam attacks. One of the most interesting facts about Ripple is that it is intended to be a new global settlement system for the exchange of currencies and other assets, some of the early supporters of Ripple include the Royal bank of Canada, UBS, UniCretit and Santander. Another interesting fact is that Ripple does not have 'miners' – instead there is an existing supply of 100 billion Ripples which are mostly held by the company (Ripple Labs Inc.), and are released at a set rate on a monthly basis.

Key differentiators to bitcoin

- Global settlement network
- Can be exchanged into any store of value
- Backed by large institutional players
- Has no mining
- Does not use Blockchain technology

Litecoin was launched in 2011 by a former google employee and MIT graduate named Charlie Lee as an early substitute to bitcoin. Litecoin is considered as the 'silver' to bitcoin's 'gold' due to its larger total supply of coins which is 84 million compared to bitcoins 21 million coins in supply. Litecoin borrows some of the main concepts from bitcoin, however has some altered key parameters in order to reduce the increasingly expensive hardware requirements to mine bitcoins (where anyone with a regular computer can mine). The Litecoin mining algorithm is based off Scrypt instead of bitcoin's SHA-265.

Key differentiators to bitcoin

- Uses a simpler cryptographic algorithm
- Is considered to be 4x fast in generating new block (coins)
- Has much faster transaction processing (bitcoin can take anyway from 40mins to 1 hour to transact/transfer coins to another participant or merchant)
- Litecoin has 84 million coins in total supply (whereas bitcoin has 21 million)

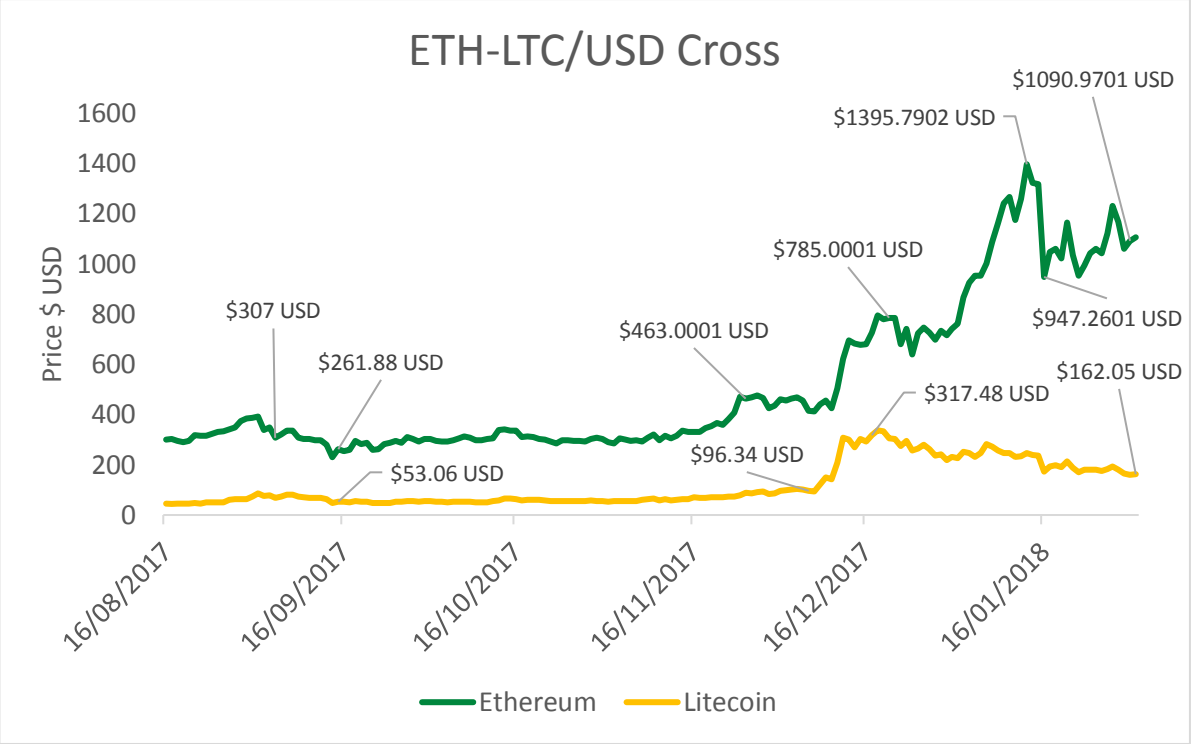
Figure 3: Metrics by coin and Price peaks of other coins

	Bitcoin	Ethereum	Ripple*	Litecoin
Market Capitalisation	$173,194,008,818	$109,881,674,316	$44,747,971,252	$9,121,632,614
Volume (24hrs)	$8,039,830,000	$3,803,060,000	$1,240,170,000	$366,974,000
Daily Transactions**	287,549.00	1,086,500.00	1,119,500.00	102,211.00
Circulating Supply	16,837,675	97,333,446	38,739,142,811	55,011,233

* Circulation - not mineable, ** 30 day simple moving Average

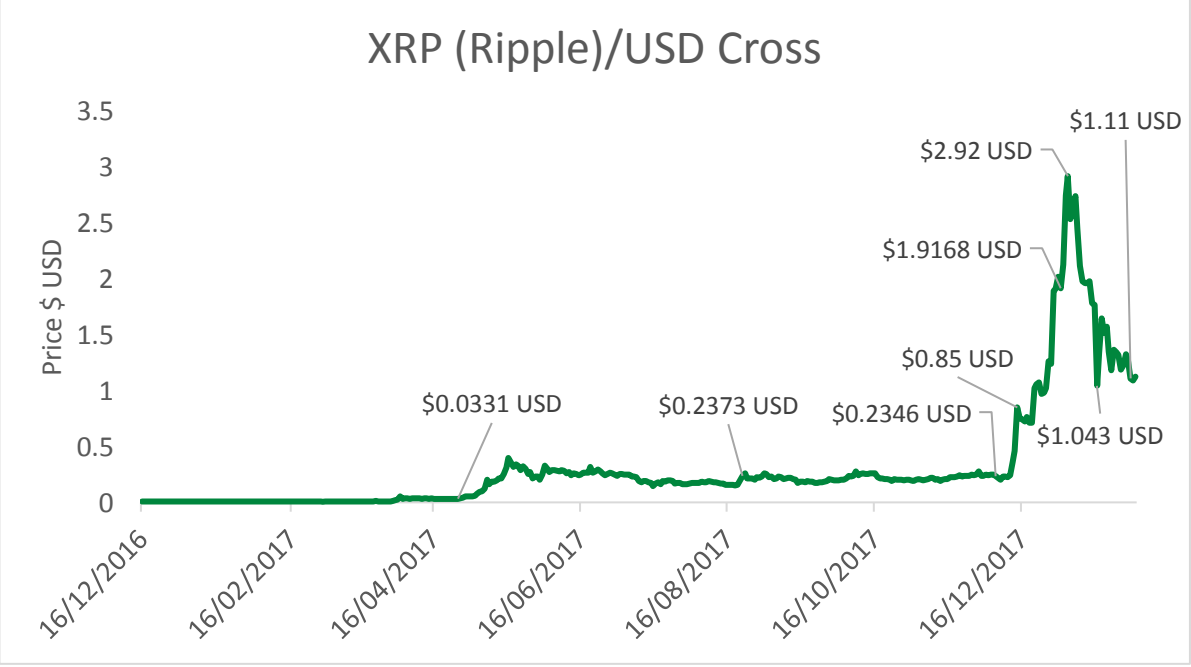
Source: Coinmarketcap, bitinfocharts, IOOF Research, Feb 2018

Figure 4: Price of Ethereum and Litecoin in USD



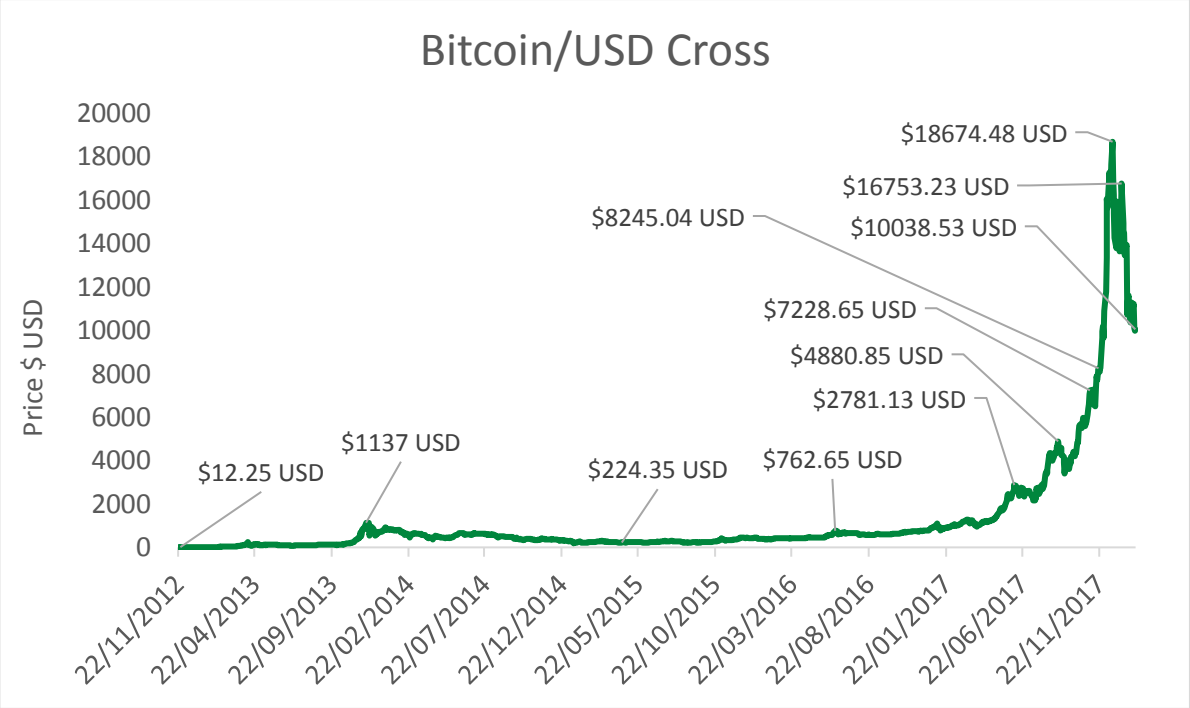
Source: Bloomberg, IOOF Research, Feb 2018

Figure 5: Price of Ripple in USD



Source: Bloomberg, IOOF Research, Feb 2018

Figure 6: Price of Bitcoin in USD

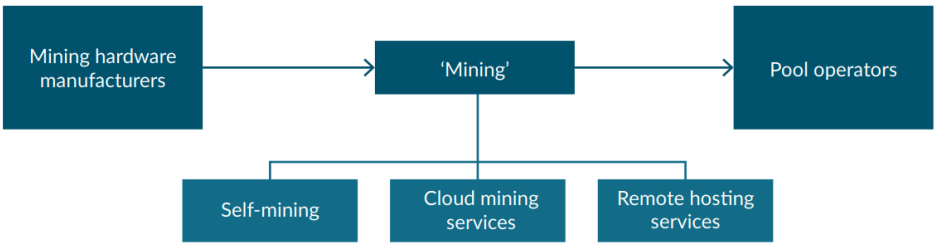


Source: Bloomberg, IOOF Research, Feb 2018

Exchanges and Mining?

Mining for cryptocurrencies has gone from being a simple hobby performed by early adopters on ordinary PCs into a capital-intensive industry that uses and array of custom hardware equipment.

Figure 7: The mining industry value chain



Source: Global Cryptocurrency Benchmarking Study, 2017

Miners play a crucial role in any cryptocurrency system. They are responsible for grouping unconfirmed transactions into new blocks and adding them to the global ledger (blockchain). For each addition of block the miner creates for the blockchain, they are rewarded with tokens. These tokens can be used to purchase coins or make transactions. By adding an additional block, it makes it difficult for an attacker to reorganise the ledger and double spend already confirmed transactions. Miners provide the necessary computing power to secure a blockchain, which is done by computing vast numbers of hashes to find a valid block.

There are various exchanges that investors can purchase their coins on, all seem to be extremely expensive relative to trading equities and other financial securities. Security is another growing concern with these crypto exchanges, where investors are not advised to leave their coins on the exchange but to transfer to their "wallet" (a web service or piece of hardware or a physical document, from a provider, that has details to access your coins). Off line solutions (hardware and paper wallets) are most secure.

Investment implications and risks

There are various implications and risks surrounding cryptocurrencies. Although the decentralised nature offers many advantages, such as being free from government control and regulation, this can also present a disadvantage. Apart from the users of cryptocurrencies, there are no real overarching set of controls or institutions to help overlook the whole system when there is a crisis. We have seen values hit sky high with no real news present to explain why, in which case some see no value in Bitcoin and/or other cryptocurrencies.

This space is extremely speculative and volatile, and has added vulnerabilities around security and hacking. An example of this was in 2016 where $50 million USD was stolen from investors in Ethereum.

There is always the risk that this whole space could be a bubble, the price of bitcoin and its associated costs/transaction times go against why it was developed in the first place. Without wider acceptance by merchants and governments, cryptocurrency will be unable to evolve into a stable useful currency.

Figure 8: Level of concerns regarding general challenges affecting the cryptocurrency industry

Respondents Scored these Categories on a 1 - 5 Scale

1: Not concerned at all 2: Concerned 3: Moderately concerned 4: Highly concerned 5: Extremely concerned

Lowest average score — Highest average score

	Weighted average	Small miners	Large miners
Centralisation of hashing power in the hands of a few (control)	**3.77**	3.89	3.30
Centralisation of hashing power in a particular geographical area (location)	**3.59**	3.70	3.11
Scaling	**3.41**	3.44	3.30
Mining fees not compensating for decreasing block rewards in the long run	**3.17**	3.41	2.22
Centralisation of mining equipment production in a particular geographical area	**3.09**	3.35	2.10
Implementation bugs in mining firmware/ hardware	**2.98**	3.11	2.55
Design bugs/weaknesses at the protocol level	**2.83**	2.92	2.55
Lack of liquidity in cryptocurrency markets	**2.57**	2.72	2.09

Source: Global Cryptocurrency Benchmarking Study, 2017

Wider merchant adoption and the ability for the average person to trade goods and services on a daily basis is one of the key challengers for cryptocurrency. Currently less than 1% of the global population actually owns cryptocurrency, where the average user fits into the category of either 'programming enthusiast', 'speculative investor', 'criminal' or 'libertarian'. The average consumer and merchant is usually deterred due to their lack of technological understanding, volatility, hacking concerns or the daunting prospect of creating a wallet. However as more companies start accepting cryptocurrencies (to name a few; Microsoft, Subway (US), Expedia, Bloomberg, Webjet, and dominos US-via PizzaForCoins.com), scalability could improve some of the issues cryptocurrencies have around transaction times for confirming transfer of funds to merchants (which can range from 10 mins to 2 hours on average), volatile and security. If wider merchant adoption is not possible it would be very difficult to find a specific use for cryptocurrencies besides being a speculative investment for traders.

Conclusion

While the potential for a big payday from trading and investing into cryptocurrencies may look enticing for certain investors. The truth of the matter is, with such violent volatility, it is hard to see when broad adoption can occur or where the value relative to Australian dollars will settle toward. There is the chance that these currencies are accepted widely and the price continues to rise, or they are they are banned (such as the China ban on bitcoin) and the price takes a huge hit, or trades to zero. There is a great deal that is unknown.

Cryptocurrency 'investing' and 'trading' is still considered as a new market. For those who trade it, it requires specialised knowledge that may be inscrutable to the inexperienced. The rapid growth has led to a lot of volatility which has attracted investors of all kinds. Most investors use these digital currencies as punting tools. It is hard to tell where the future will take us with cryptocurrency. Blockchain technology on the other hand is one aspect from digital currencies that can be applied widely and expanded to various industries.

Research Analyst – Daniel Stojanovski

Approved By – Paul Saliba

Research Analyst Disclosures:

I, Daniel Stojanovski, hereby certify that all the views expressed in this report accurately reflect my personal views about the subject investment theme and/or company securities. I also certify that no part of my compensation was, is, or will be, directly or indirectly, related to the specific recommendations or views expressed in this report.

I, Daniel Stojanovski and/or entities in which I have a pecuniary interest, have an exposure to the following securities and/or managed products mentioned in this report: Ripple (XRP)

Important Information

This report is prepared by Bridges Financial Services Pty Limited ABN 60 003 474 977 AFSL 240837 (Bridges). Bridges is an ASX Market Participant and part of the IOOF group of companies.

Bridges and/or its associated entities, directors and/or its employees may have a material interest in, and may earn brokerage from, any securities or other financial products referred to in this document, or may provide services to the company referred to in this report. The document is not available for distribution outside Australia and may not be passed on to any third person without the prior written consent of Bridges. Bridges and associated persons (including persons from whom information in this report is sourced) may do business or seek to do business with companies covered in its research reports. As a result, investors should be aware that the firms or other such persons may have a conflict of interest that could affect the objectivity of this report. Investors should consider this report as a single factor in making an investment decision.

The document is current as at the date of issue but may be superseded by future publications. You can confirm the currency of this document by checking the intranet site (links below).

The information contained in this report is for the sole use of advisers and clients of AFSL entities authorised by Bridges in writing. This report may be used on the express condition that you have obtained a copy of the Bridges Financial Services Guide (FSG) from the website www.bridges.com.au/fsg

Disclaimer: The information in this report is general advice only and does not take into account the financial circumstances, needs and objectives of any particular investor. Before acting on the advice contained in this document, you should assess your own circumstances or seek advice from a financial adviser. Where applicable, you should obtain and consider a copy of the Product Disclosure Statement, prospectus or other disclosure material relevant to the financial product before making a decision to acquire a financial product. It is important to note that investments may go up and down and past performance is not an indicator of future performance.

The contents of this report should not be disclosed, in whole or in part, to any other party without the prior consent of Bridges. To the extent permitted by the law, Bridges and its associated entities are not liable for any loss or damage arising from, or in relation to, the contents of this report.

For information regarding any potential conflicts of interest and analyst holdings; IOOF Research Team's coverage criteria, methodology and spread of ratings; and summary information about the qualifications and experience of the IOOF Research Team please visit https://www.ioof.com.au/adviser/investment_funds/ioof_advice_research_process