PLATINUM

QUINLAN &ASSOCIATES

JANUARY 2018

FOOL'S GOLD?

UNEARTHING THE WORLD OF CRYPTOCURRENCY

THE AUTHORS

BENJAMIN QUINLAN
CEO & MANAGING PARTNER
BCom (Hons 1) / LLB (Hons), *Macquarie*

HUGO CHENG
CONSULTANT
BA (Hons), *Cambridge*,
MSc (Distinction), *Imperial*

.

SPECIAL THANKS

We would like to thank our interns:

Antti Viitala (BSc, Risk Management and Business Intelligence at The Hong Kong University of Science and Technology),

Charles Yau (BBA, Global Business and Information Systems at The Hong Kong University of Science and Technology),

Edwin Morris (BSc, International Business and Management at Aston University), and

Tommy Wong (BBA, Finance and Information Systems at the Hong Kong University of Science and Technology)

for their help in the preparation of this report.

CONTENTS

EXECUTIVE SUMMARY

Cryptocurrencies have been heralded as the revolution of the financial system since its proof of concept by Wei Dai and Nick Szabo in 1998, followed by Satoshi Nakamoto's whitepaper detailing a 'peer-to-peer electronic cash system' and open source code, which is now known as Bitcoin.

Underpinned by blockchain technology, cryptocurrencies promised an end to third party institutions and barriers to financial transactions. And in recent years, they have exploded onto the scene at an exponential rate. At its 2017 peak, there were over 1,300 cryptocurrencies in existence, with a combined market capitalisation of nearly USD 650 billion, rivalling the GDP of nations such as Saudi Arabia. Bitcoin (BTC) itself, the most popular cryptocurrency, has touched market capitalisations similar to economies such as Malaysia and Vietnam.

The sudden rise of the cryptocurrency market has generated heated debate by both believers and critics alike for its value, future potential, and use cases. At the centre of this discussion is BTC, with its meteoric price rise capturing daily headlines in mainstream and social media alike, with speculators rushing to the market in the hopes of joining the wave of overnight millionaires. A plethora of inter-related industries have also been spawned, including wallets and payment services, crypto exchanges, and mining, as entrepreneurs across the globe look to capitalise on new revenue pools that have opened up on the back of this technological revolution.

To appreciate the recent rise of cryptocurrencies and their future potential, one must understand the underlying technology, surrounding ecosystem, and the place of cryptocurrencies in financial markets (and the wider economy). Our report details the aforementioned criteria, utilising BTC as the exemplar for current cryptocurrencies in place at the time of writing. We also drew further insights from interviews with a wide range of industry stakeholders, as well as survey responses from over 1,500 individuals working predominantly in financial services, FinTech, consulting, and technology.

Most current iterations of cryptocurrencies are, at their core, meant to operate as currencies (be it fiat replacements or within their own ecosystem). However, currencies have, for many centuries, needed to meet a number of specific criteria to be recognised as such – namely, acting as a unit of account, a medium of exchange, and a store of value. Despite fulfilling most of the characteristics of a traditional fiat currency, cryptocurrencies are largely being utilised as speculative investment assets, leading to considerable volatility in their value. This lack of stability, together with soaring valuations, means they are rarely used for payments. In order to achieve status as a legitimate currency, the public must spend cryptocurrencies widely to determine a credible benchmark for their actual value, encouraging businesses to accept them as a medium of payment (hence making them more liquid in the long run). Until then, most cryptocurrencies, including BTC, will continue to exist in a speculative capacity, with all the undertones of being a bubble.

2017 saw the price of BTC surpass the asset price inflation of the 17th century tulip mania, while rendering "bubbles" such as dotcom a mere blip by comparison. Its strong – albeit slowly unwinding – correlation to alternative cryptocurrencies also indicates a collapse in the price of BTC could lead to a rapid downfall for the broader non-fiat cryptocurrency market.

A number of factors underpinned BTC's price rise in 2017. In the earlier part of the year, many of the gains could be tied to ongoing discourse around its potential regulatory legitimacy. Since then, however, its popularity – and infamy – has

appeared to fuel a widespread “fear of missing out” (FOMO), a classic characteristic of most bubbles. Yet, consensus regarding its future value remains literally non-existent, with valuations ranging from USD 0 to as high as USD 1,000,000. Moreover, the majority of these predictions do not appear to be based on any robust, quantitative methods, but are more a reflection of individual opinion.

To determine whether BTC is indeed a bubble, we looked to calculate its value using two overarching approaches: (1) as an asset; and (2) as a currency.

As an asset, we valued Bitcoin using a cost of production approach and a store of value approach, resulting in values of USD 2,161 and USD 687 respectively. To value BTC as a currency, we estimated its utilisation for both legal, retail transactions payments and payments in the black market, as well as functioning as an international FX reserve. After significant testing, we calculated the price of BTC 1 to be USD 1,780.

Irrespective of the valuation methodology employed, we found the price of BTC deviates significantly from its current price of ~USD 14,000. For the longer-term, we are even less optimistic around the future price of BTC and believe it will ultimately be ruled out as a mainstream form of payment. We see this exerting greater downward pressure on its price and forecast it to trade at ~USD 810 by 2020, if not even lower. We therefore believe that BTC, at its current valuation, is a bubble waiting to burst.

While our views on the price (and future applications of BTC) remain muted, our outlook for the broader cryptocurrency industry remains much more sanguine. Existing cryptocurrencies that were designed to replace fiat currencies, such as BTC, are unlikely to act as viable substitutes to the money or currency system we have in place today, due to their inherent challenge to central bank and government functions – namely, fiscal and monetary policy. However, cryptocurrencies with associated utility applications (such as Ethereum’s ETH), as well as fiat cryptocurrencies attached to a sovereign nation, are likely to grow in significance, given the ability of the underlying blockchain technology to provide meaningful enhancements to current payment systems, as well as their broader applications beyond being used as speculative assets (e.g. facilitating the execution of smart contracts).

Although a sharp decline in the price of BTC in 2018 is likely to take the value of other non-utility cryptocurrencies with it, we see the correlation with utility cryptocurrencies being much less pronounced. While we anticipate valuations to decline in the short-term in response to the widespread unwinding of the digital currency space, valuations of utility cryptocurrencies are likely to recover and dominate the market in the long-term. We forecast total market capitalisation of private cryptocurrencies to be USD 407 billion by 2020. We also see fiat cryptocurrencies gaining momentum as governments accelerate their research and piloting efforts, with potential to be a USD 150 billion market by 2020.

While we believe BTC can largely be viewed as fool’s gold at present, digital currencies will continue to unearth major enhancements to the global payments system in years to come.

SECTION 1

THE EMERGENCE OF CRYPTOCURRENCIES

INTRODUCTION

In October 2008, an entity known as Satoshi Nakamoto published a paper entitled *Bitcoin: A Peer-to-Peer Electronic Cash System*,[1] proposing a revolutionary money and payment system in which transactions are conducted using cryptocurrencies and recorded on a public ledger, called the blockchain, eliminating the need for a trusted third party. Because of the characteristic of not requiring a third party or central administrator, these cryptocurrencies are sometimes called decentralised digital currencies.

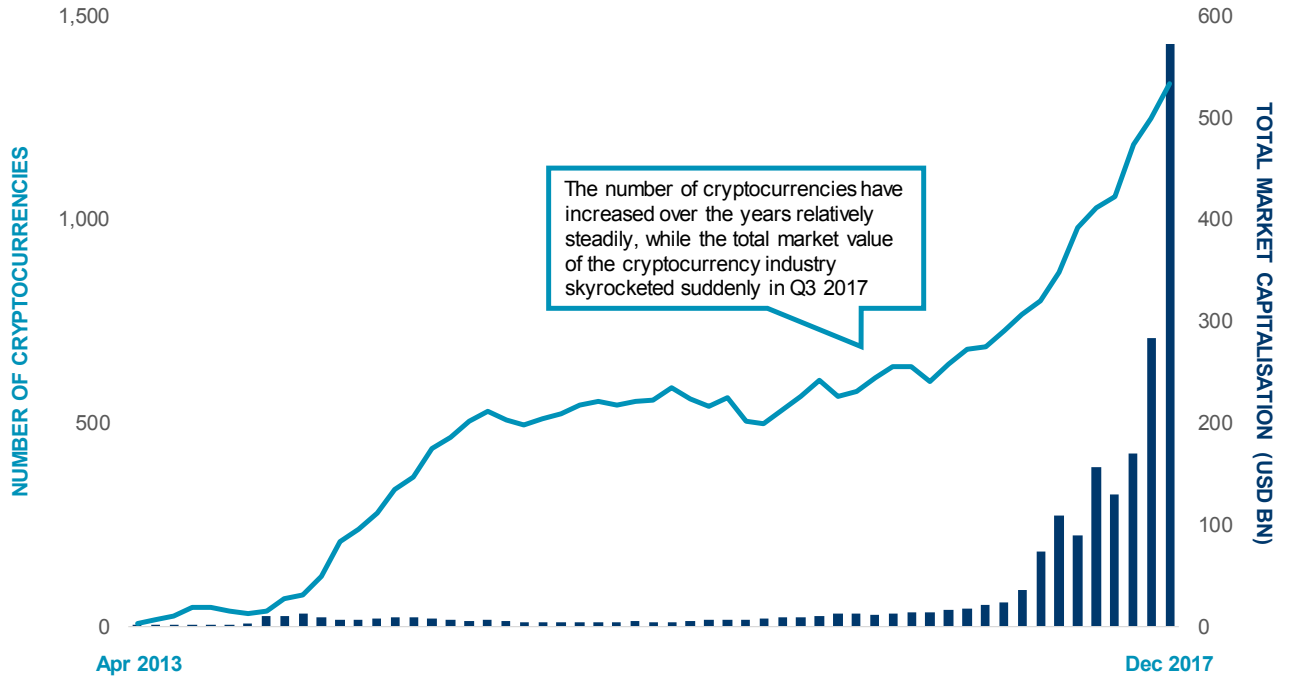
Instead of using a third party, a network of computers, which serve as interconnected "nodes" within the network, maintains and verifies a record of consensus of transactions. These transactions are then encrypted and stored in linked blocks on the nodes, creating a cryptographic audit trail. As a result, all nodes in the network have access to the distributed ledger, a shared, single source of truth.[2]

Following the release of the paper, Satoshi Nakamoto released Bitcoin as an open-source software on 3 January 2009, marking the start of a new era in the money and transaction space. Since then, a plethora of cryptocurrency enthusiasts and companies created their own cryptocurrencies, known as altcoins (short for "alternative coins"), which are alterations or enhancements of Bitcoin.

As at 31 December 2017, there were over 1,300 cryptocurrencies with a combined market capitalisation of USD 569 billion listed on CoinMarketCap[3] (see Figure 1). At its 2017 peak, the market capitalisation of all cryptocurrencies neared USD 650 billion,[4] higher than the 2016 GDP of countries such as Saudi Arabia (USD 646 billion) and Sweden (USD 514 billion).[5]

[1] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', 31 October 2008, available at: https://bitcoin.org/bitcoin.pdf
[2] Quinlan & Associates, 'From KYC To KYT', available at: http://www.quinlanandassociates.com/wp-content/uploads/2016/12/Quinlan-Associates-From-KYC-to-KYT.pdf
[3] CoinMarketCap, 'Cryptocurrency Market Capitalizations', available at: https://coinmarketcap.com/
[4] CoinMarketCap, 'Total Market Capitalization', available at: https://coinmarketcap.com/charts/
[5] The World Bank, 'World GDP', available at: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?end=2016&start=2016&view=bar&year_high_desc=true

FIGURE 1: NUMBER AND VALUE OF CRYPTOCURRENCIES (2013-17)

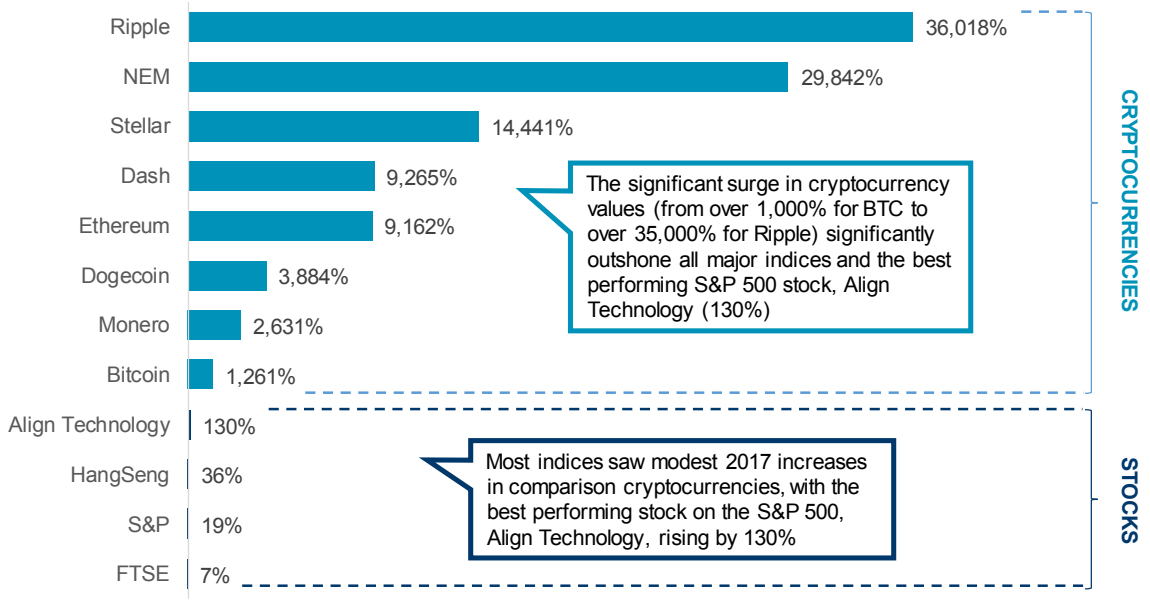


Source: CoinMarketCap, Quinlan & Associates analysis

In addition, the value of many cryptocurrencies increased significantly during 2017, with some experiencing over 10,000% gains (see Figure 2). By comparison, the gains in the stock markets, with the best performing S&P 500 stock gaining "only" 130%, look abysmal. Note that the price of XRP (the native cryptocurrency of Ripple) increased from ~USD 0.006 to ~USD 2.3 in 2017, representing a nearly 400-fold increase.[6]

[6] CoinMarketCap, 'Ripple', available at: https://coinmarketcap.com/currencies/ripple/

FIGURE 2: PERCENTAGE GAINS OF SELECT CRYPTOCURRENCIES AND STOCKS (2017)



Note that the best performing S&P 500 stock in 2017 was Align Technology[7]

Source: CoinMarketCap, Nasdaq, Quinlan & Associates analysis

For clarity, this report will use Bitcoin when referring to the system or technology based on Satoshi Nakamoto's paper, and BTC when referring to the digital currency itself. Note also that BTC 1 can be divided into 100,000,000 parts, called satoshi (i.e. 100,000,000 satoshi = BTC 1).

The two most famous blockchain systems at present are arguably Bitcoin and Ethereum, with Bitcoin simply being a cryptocurrency system, while Ethereum aims to use blockchain technology to create a system for decentralised applications (Ethereum does have its own cryptocurrency, named Ether). In addition, Ethereum has also led to the emergence of Initial Coin Offerings (ICOs).

Due to the significant hike of the price of BTC in 2017, from just under USD 1,000 at the beginning of year to over USD 20,000 on some cryptocurrency exchanges in December 2017 (representing a ~2,000% increase), interest in cryptocurrencies has erupted, and it is not surprising to see daily headlines on BTC prices breaking previous records and retail investors with little technological knowledge discussing investments in BTC.

[7] CNBC, 'The best-performing stock in the S&P 500 this year was the company behind Invisalign clear braces', 27 December 2017, available at: https://www.cnbc.com/2017/12/27/align-technology-2017-top-performer-on-sp-500.html

Despite cryptocurrencies and blockchain being related, and less-informed media or entities treating them as the same thing, they are two very different concepts. Blockchain is a technology with many applications, and cryptocurrency is one of these applications. Taking an analogy with internet, the internet has different uses, with social media/networking being just one of many applications.

This report will review in detail the usage, applications, and effects, of cryptocurrencies, as well as their longer-term outlook.

To enhance our perspectives, we conducted a survey of over 1,500 people to understand the market's broader views and perspectives on Bitcoin and other cryptocurrencies. All results from the survey are outlined in Section 7, and are also referenced throughout the body of the report.

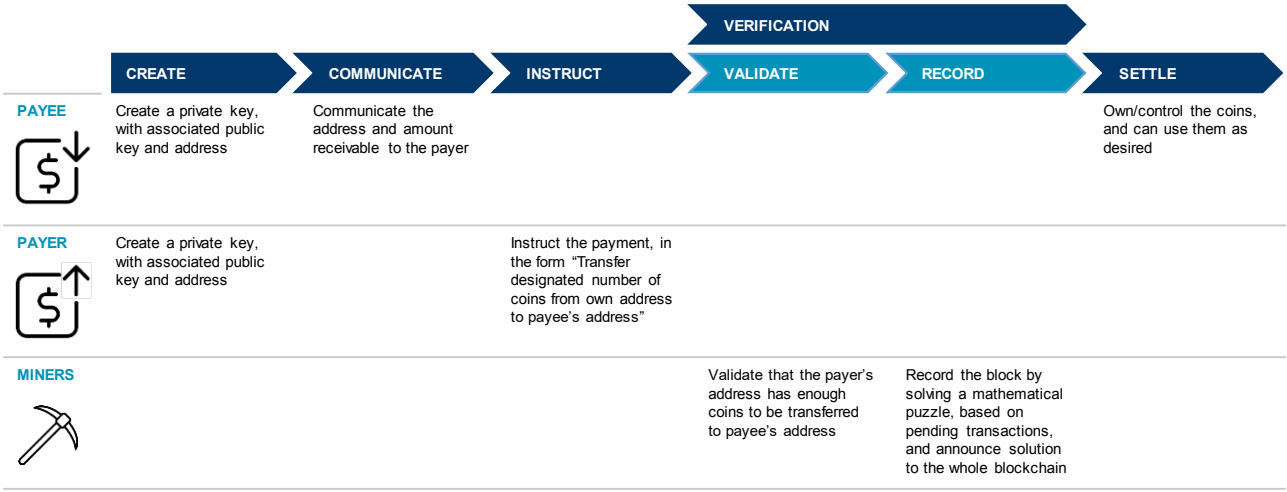
BLOCKCHAIN IS A TECHNOLOGY WITH MANY APPLICATIONS, AND CRYPTOCURRENCY IS ONE OF THESE APPLICATIONS

HOW IT WORKS

Even though news headlines have been awash with stories on cryptocurrencies and blockchain systems, we still find that very few people know how their mechanics truly work.

The following segment uses Bitcoin, currently the most well-known cryptocurrency system, as an example of how the blockchain payment system works in practice (see Figure 3).

FIGURE 3: CRYPTOCURRENCY PAYMENT FLOW



Source: Quinlan & Associates analysis

A. CREATE (PAYER & PAYEE)

Both the payer and payee create new addresses respectively (or use existing addresses). This is done by randomly choosing a private key, out of ~2^{256} possible combinations,[8] which is then used to calculate a public key. The public key is subsequently used to calculate the address.

Calculations are conducted through trapdoor functions, which are functions that are easy to do in one direction, but difficult to revert (i.e. it is easy to calculate the public key using the private key, but virtually impossible to use the public key to calculate the private key).

The address can be shown to everyone and anyone, while the private key is treated as a password and should be kept confidential. Because there is no centralised party, there is no "forgot my password" option. Hence if the private key is lost, access to the wealth at the address is also lost.

The private and public key mechanics are similar to a bank account's, in which the address is the account number and the private key is the account password, with the private key needed to initiate a fund transfer. However, in the case of Bitcoin, anyone can view the wealth of an address (whereas the public does not know how much one holds in a bank account) and an individual can generate as

[8] This is equivalent to ~1.15×10^{77} possible combinations; there is a non-zero probability of choosing a private key that is already in use, however the probability is so low that the feat is treated as practically impossible

many addresses as desired without providing any information (whereas one needs to provide personal information to the bank to open a bank account).

B. COMMUNICATE (PAYEE)

The payee communicates the address and the number of coins payable to the payer.

C. INSTRUCT (PAYER)

Using the Bitcoin client or payment services, the payer provides instructions in the form of "transfer specified amount of coins from payer's address to payee's address", and signs this instruction using the private key.

Note that the signature is not the private key, but is generated mathematically using both the transaction details and the private key. This means that changing any details of the payment (such as the amount to be transferred and the payee's address) will result in a different signature.

The payer also has the option to include a transaction fee in this payment to incentivise quicker validation.

D. VERIFICATION (MINERS)

VALIDATE

After the payment instructions are received, the payer's address is checked to ensure there are sufficient funds for the payment. In addition, the transaction is checked against the signature to verify the authenticity of the instructions (as a signature associated to the transaction cannot be faked practically, having the correct signature means the instructions are sent by the owner of the private key).

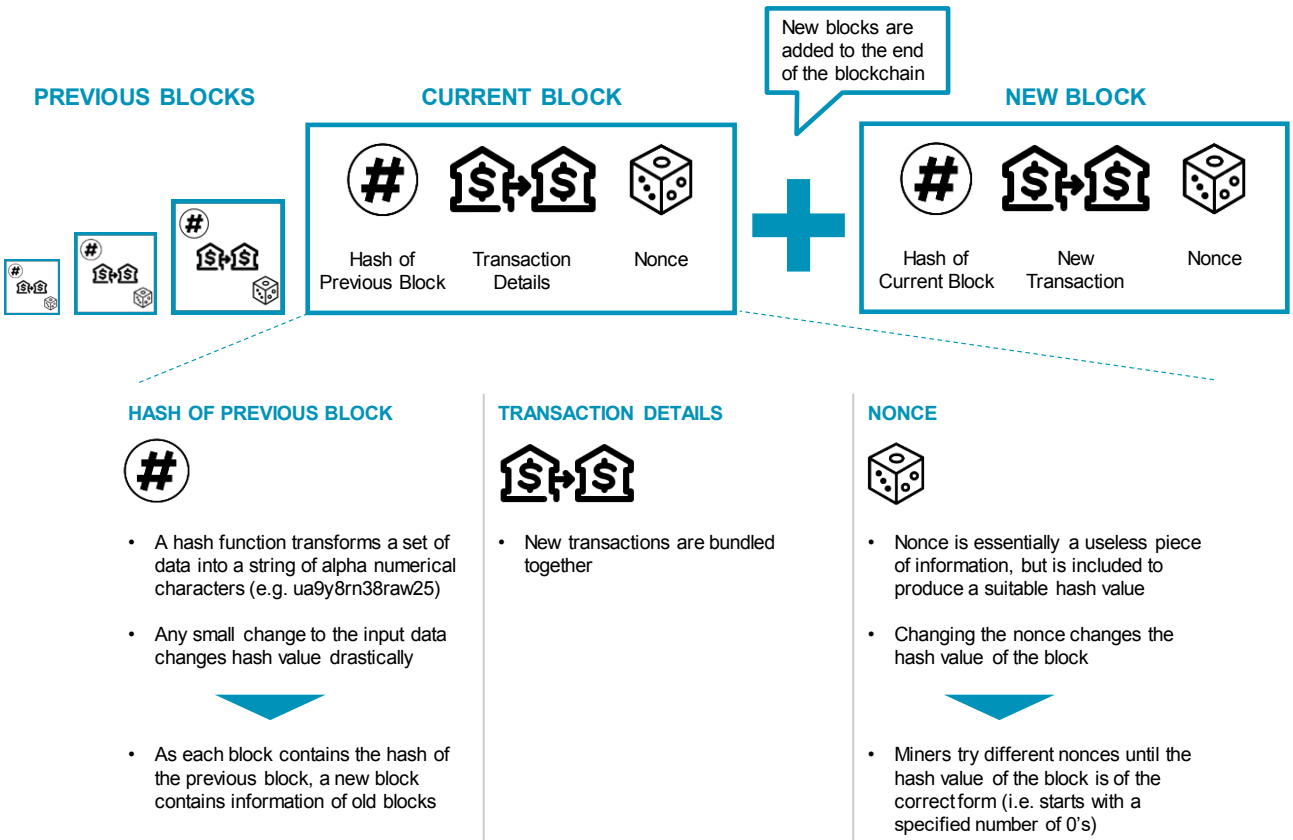
RECORD

The blockchain is a growing sequence of blocks, and each block has a hash value, which is calculated using a hash function. Hash functions transform a set of data into a string of alpha numerical characters.

A key feature of hash functions is that any tiny change made to the input (i.e. the set of data) will result in significant changes in the resulting hash value, which means it is impossible to predict the hash value of any given data.

New and pending transactions are bundled together, preceded by the previous block's hash value and succeeded by a nonce (which is an arbitrary number, see below), forming a new block (see Figure 4).

FIGURE 4: HOW MINING WORKS



Source: Quinlan & Associates analysis

The aim of the miners is to be the quickest to identify a suitable nonce against all other competing miners, based on the previous block's hash value and the pending transactions, such that the new block's hash value is of an acceptable form. An acceptable hash value starts with a certain number of 0's, with the number of 0's updated every 2016 blocks to ensure difficulty. As it is impossible to predict the hash value of any given data, miners must try a huge amount of nonces[9] (requires ~8 sextillion[10] tries on average,[11] as at 31 December 2017) to identify one that results in the acceptable form. The difficulty of any one miner finding this nonce is dynamically adjusted every 2016 blocks (~ 2 weeks) to ensure a consistent block time of ~10 minutes.

Taking a very simple analogy, imagine having the first 10 digits of an 11-digit phone number (with a three-digit area code and eight-digit number), and one must guess the correct phone number (see Figure 5). The first ten digits are given, similar to the previous block's hash value along with the bundled transactions. The final unknown digit is the nonce, and the process of dialling the number to check whether it reaches the target person is similar to hashing the block to check whether the hash value is of the desired form.

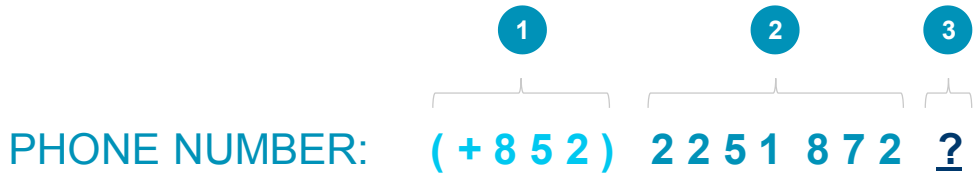
In both cases, the result cannot be predicted (one cannot predict who will pick up the phone unless one calls, and one cannot predict the hash value of any data unless one calculates the value), and the solution can only be found through trial and error. The major difference is that one only needs to try 10 digits (i.e. 0, 1, 2, …, and 9) for a phone number compared with sextillions of different nonces for Bitcoin mining.

[9] The number of nonces miners have to try depends on the "difficulty", which is set by the system and updated every 2016 blocks (i.e. two weeks, given the blocktime of 10 minutes) based on the time required to generate the previous 2016 blocks, in order to keep blocktime at 10 minutes

[10] 8 sextillion is 8,000,000,000 trillion, or 8 billion trillion; 8 sextillion seconds is over 250,000 billion years (note the universe is only ~14 billion years old)

[11] The expected number of tries required is roughly $\mathrm{DIFFICULTY} \times 2^{32}$; as at 31 December 2017, the difficulty was ~1.9 trillion

FIGURE 5: ANALOGY TO BITCOIN MINING



	GIVEN INFORMATION		ACTION REQUIRED	
	1 AREA CODE	2 KNOWN DIGITS	3 UNKNOWN DIGIT	CALLING
BITCOIN MINING EQUIVALENT	• Hash value of previous block	• Transaction details for the block	• Nonce	• Hashing
PHONE NUMBER	• Two different sets of data – namely, the country code and the first seven digits of a number		• Trying different digits	• Calling the number to see if desired person is reached
DETAILS	• Two different sets of data provided by the system (i.e. the hash value of the previous block and transaction data)		• Trying different nonces	• Hashing the value to see if targeted form is reached

Note that the number displayed is Quinlan & Associates' phone number (the final digit is 5); please call us if you would like to further discuss this topic or other opportunities where we can help

Source: Quinlan & Associates analysis

When a miner finds a suitable nonce, called a "golden nonce", this block is added to the blockchain and the information is delivered to the network. Once a block is added to the blockchain, the payment from the payer to the payee is completed, and the payee can spend the coins received.

Note that as each block contains the hash value of the previous block, the new block contains information on old transactions.

The miner who finds the suitable solution the fastest is subsequently rewarded with a specific number of BTC (currently BTC 12.5 per block). In addition to this reward, some payment instructions may include transaction fees, and the miner who mines the block including this transaction earns the transaction fee. Therefore, miners are incentivised to prioritise processing transactions with higher fees than those with no transaction fees.

Bitcoin has a transaction capacity limit of 7 transactions per second. As a consequence, transaction fees are essentially required if one needs quick confirmation. In fact, it costs USD 28, on average, to execute transactions using BTC.[12]

E. SETTLE (PAYEE)

When a block is added, the payment is said to have one confirmation. After one subsequent block is added onto the blockchain, the payment is said to have two confirmations. For large payments, it is currently recommended that the payee wait for six confirmations (i.e. after five more blocks have been added onto the chain subsequent to the block containing the payment), as at this point, the payment is practically secured.

Once the payment is completed and confirmed, the payee now owns the coins transferred and can use them as desired. The transaction is settled.

[12] CNBC, 'Big transaction fees are a problem for bitcoin – but there could be a solution', 19 December 2017, available at: https://www.cnbc.com/2017/12/19/big-transactions-fees-are-a-problem-for-bitcoin.html

PROOF-OF-WORK VS PROOF-OF-STAKE

Bitcoin uses a proof-of-work system, which is essentially a mechanism that requires miners to identify a piece of data that is costly (in terms of electricity consumption) and time-consuming to produce but easy for others to verify (i.e. the golden nonce), to ensure the validity of the blockchain.

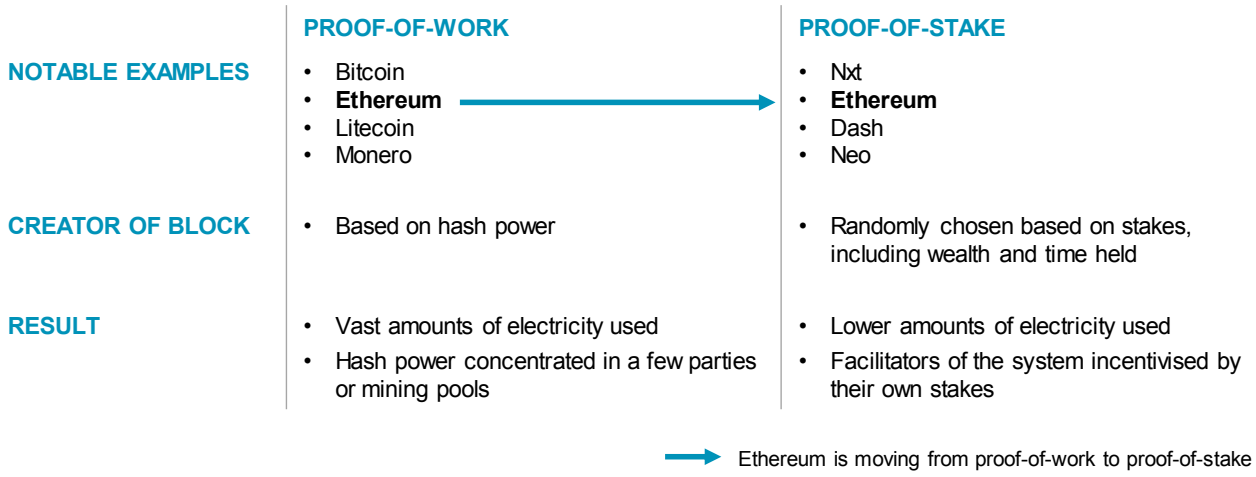
To briefly explain how this works, the network considers the longest blockchain to be the valid one. Therefore, if a hostile entity wishes to cheat the system (e.g. double-spend BTC), this entity needs to create a block containing the fake transaction information, and race against other miners to create subsequent blocks, such that the fake version of the blockchain which contains invalid transaction information is the longest chain. However, given the proof-of-work system, the hostile entity must compete against all other miners to constantly identify each golden nonce quicker than the non-hostile miners, which is virtually impossible unless the hostile entity controls over 50% of the mining power (which is economically unviable). Therefore, the proof-of-work system ensures the integrity of the blockchain.

Notwithstanding this, the proof-of-work system requires a huge amount of electricity and is biased towards parties with high mining powers. This centralises power within mining pools (i.e. syndicates of miners – see Section 2 for more detail), which partially defeats the purpose of Bitcoin being a decentralised system. In addition, many miners will be attempting to add the same block of transactions onto the blockchain, though only the fastest one (as verified by the nodes in the system) will succeed. This means the electricity consumed by all other miners is essentially wasted. In fact, it was reported that globally, Bitcoin mining operations are estimated to consume more energy annually than 20 European countries, including Ireland and Morocco.[13]

Proof-of-stake is an alternative type of system in which the creator of the next block is randomly chosen, typically based on wealth (wallets with higher amounts of cryptocurrency are more likely to be chosen) or age (wallets which have held funds for a longer amount of time are more likely to be chosen) (see Figure 6).

[13] The Guardian, 'Bitcoin mining consumes more electricity a year than Ireland', 27 November 2017, available at: https://www.theguardian.com/technology/2017/nov/27/bitcoin-mining-consumes-electricity-ireland

FIGURE 6: PROOF-OF-WORK VS PROOF-OF-STAKE



Source: Quinlan & Associates analysis

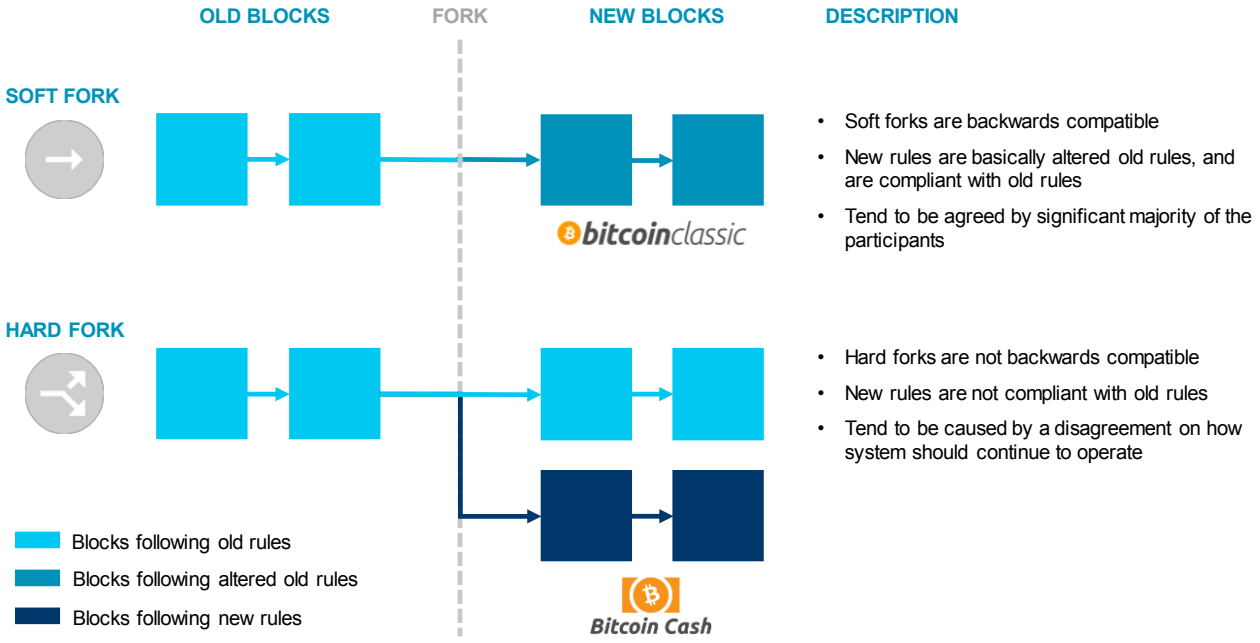
In contrast to proof-of-work, in which the incentive for mining is to gain block rewards, miners in the proof-of-stake system are facilitating a system in which they themselves hold stakes (as they hold large amounts of the cryptocurrency and for a long period of time), and are rewarded through transaction fees.

Instead of competing for block rewards through constantly running calculations, and therefore consuming energy, the proof-of-stake system reduces the amount of electricity wasted, and is considered a more sustainable mechanism for validating transactions.

FORKING

A fork occurs when network participants want to change, influence, or upgrade the system. When a significant majority agrees with the change and, a soft fork occurs. By contrast, a hard fork occurs when there is a split in opinion on how the system should continue to operate (see Figure 7).

FIGURE 7: SOFT FORK AND HARD FORK



Source: Quinlan & Associates analysis

For a soft fork, the new blocks follow a set of new rules that are essentially an altered version of the set of old rules (but are still compliant with the set of old rules). Therefore, the new blocks are still valid under and accepted by the old system. This results in one chain, with new rules for the new blocks. This tends to happen when a significant majority of the participants in the system agree to a change or update, which will likely improve the blockchain system.

In a hard fork, a group of the new blocks follow a set of new rules that are incompatible with the set of old rules, which means the old system will not accept the new blocks. On the other hand, another group of the new blocks will follow the same set of old rules, which will be accepted by the old system. These two sets of blocks will create two chains in parallel, and share the same information up to a certain point (as they share old blocks). This tends to occur when the participants split into two factions regarding an incident or impending protocol. After the hard fork, each faction can continue operations on their preferred chain.

The main difference between a hard fork and a soft fork is backwards compatibility of the new protocol. The new protocol is backwards compatible for a soft fork, which means older versions of the system will accept new blocks; and the new protocol is not backwards

compatible for a hard fork (i.e. older versions of the system will not accept new blocks). In a distributed ledger system, it is necessary for users and their nodes to remain compatible after the fork, and therefore the node has no need to be upgraded after a soft fork. In a hard fork, those preferring to remain on the original chain do not need to upgrade their software. However, an upgrade is required for those who want to move onto the new chain.

An example of a soft fork for Bitcoin was the incorporation of Segregated Witness (a.k.a. SegWit) into the system, which aims to increase the transaction speed. Some hard forks of Bitcoin include Bitcoin Cash (which emerged due to disagreements on how to improve the transaction speed) and Bitcoin Gold (which emerged due to debates regarding the centralisation of mining power).

Another example of a hard fork occurred on the Ethereum blockchain, which split into Ethereum and Ethereum Classic, due to conflicts regarding how to resolve an exploit.

The DAO (decentralised autonomous organisation) is essentially a venture capital fund for projects on the Ethereum platform. Participants would spend Ether to purchase DAO tokens, which act as voting rights, and vote on projects or dapps (decentralised apps, which are applications on the Ethereum network) to fund.

However, there was a loophole which was exploited, and on 17 June 2016, an attacker took away tokens equivalent to USD 50 million from the DAO's funds. Fortunately, the code dictates that funds withdrawn from the DAO are inaccessible for 28 days, during which the community discussed options. One group proposed a hard fork from the moment before the exploit was executed, and refunding DAO token holders with Ether. This would create a new chain, essentially reversing the exploit.

However, another group believed that "code is law" and that a vital value of a decentralised system is that it cannot be tampered with and is resistant against human bias, meaning a hard fork to reverse the incident was against the philosophy of the system. Those that agreed with the hard fork moved onto the new chain, which is currently known as Ethereum (ETH), and those that disagreed with the hard fork stayed with the original chain, called Ethereum Classic (ETC).[14]

[14] Blockgeeks, 'What is Ethereum Classic? Ethereum vs Ethereum Classic', available at: https://blockgeeks.com/guides/what-is-ethereum-classic/

EXAMPLES OF CRYPTOCURRENCIES

According to CoinMarketCap, as at 31 December 2017, there were over 1,300 cryptocurrencies in existence, with 30 having a market capitalisation of over USD 1 billion, 19 having a market capitalisation of USD 500 million to USD 1 billion, and 615 having a market capitalisation of USD 1 million to USD 500 million.

The following are examples of the better-known cryptocurrencies and some of their key features (see Figure 8). For more examples of popular or interesting cryptocurrencies, please refer to the appendix (see Appendix A).

FIGURE 8: SELECT CRYPTOCURRENCIES

	MARKET CAPITALISATION (AS AT 31 DECEMBER 2017)	PRACTICAL ENHANCEMENT OF BITCOIN?	DETAILS
BITCOIN	**USD 217.2 billion**	• N/A	• The original cryptocurrency • Arguably the most well-known cryptocurrency at present • Blocktime of 10 minutes
ETHEREUM	**USD 69.3 billion**	• Yes	• Allows development of applications • Allows usage of smart contracts • Blocktime of under 20 seconds
RIPPLE	**USD 85.0 billion**	• Yes	• Released with an open payment network • Network used by multiple global banks • Blocktime of 3.5 seconds
MONERO	**USD 5.2 billion**	• Yes	• Enhances privacy, masking details of transactions • Hides wealth of addresses • Blocktime of 2 minutes
DOGECOIN	**USD 887.2 million**	• No	• Used as a "joke currency" • Based on the popular meme, "doge"

Source: CoinMarketCap, cryptocurrency website, Quinlan & Associates research

BITCOIN

Bitcoin was introduced in late 2008 in the whitepaper, *Bitcoin: A Peer-to-Peer Electronic Cash System*, written by Satoshi Nakamoto. It was launched as an open-source software on 3 January 2009.

Transactions are verified by miners and recorded on the blockchain, a public distributed ledger (see previous Section – HOW IT WORKS). As a central, trusted party is not needed for the facilitation of the system, Bitcoin is regarded as a decentralised digital currency.

One of the biggest challenges of Bitcoin is the scalability problem. Bitcoin can only handle seven transactions per second, severely hindering its transaction speed and increasing transaction fees. Conflicts within the community regarding how to solve the scalability problem have led to several hard forks, such as Bitcoin Cash.

As at 31 December 2017, BTC 1 was priced at USD 12,948.7, with a market capitalisation of USD 217.2 billion.[15]

ETHEREUM

Ethereum was introduced in 2013 by Vitalik Buterin and launched in 2015.

The blockchain of Ethereum is a shared global infrastructure, which moves value around and represents ownership of property, enabling the usage of smart contracts, which are self-executing programs that represent contracts between users in the system. Different inputs can be used to trigger the execution of contracts, meaning that transactions are conducted as agreed – as coded in the smart contract – automatically and securely, without the need for a third-party escrow.

Ethereum also challenges the current internet model, by storing data and information on a network of nodes from across the world, as opposed to in servers owned by websites, therefore creating a decentralised internet infrastructure. Ethereum has a native cryptocurrency, named Ether, for transactions and to incentivise the facilitation of the network.

Ethereum was forked into Ethereum (the subject of this section) and Ethereum Classic in 2016, due to a dispute regarding an exploit against the system.

As at 31 December 2017, one Ether was priced at USD 716.8, with a market capitalisation of USD 69.3 billion.[16]

RIPPLE

Released in 2012, Ripple is a payment protocol with a native cryptocurrency, XRP.

The Ripple network aims to enhance the current payment infrastructure, which Ripple claims is slow, expensive, and unreliable. Ripple network enables instant and secure transactions without chargebacks, and supports tokens representing fiat currencies, other cryptocurrencies, and other tokens, such as loyalty points and frequent flier miles. The network is mainly used by financial institutions, including MUFG, UBS, and AMEX.

As at 31 December 2017, one XRP was priced at USD 2.2, with a market capitalisation of USD 85.0 billion.[17]

MONERO

Monero was introduced in 2014, and is a secure, private, and untraceable cryptocurrency.

Monero boasts an enhanced level of privacy compared to other cryptocurrencies, via mechanisms including ring signatures, ring confidential transactions, and stealth addresses to hide transaction details, including payer address, payee address, and amount transferred. In addition, unlike Bitcoin, where the amount of coins in an address is visible to the public, Monero hides the owners' wealth.[18]

[15] CoinMarketCap, 'Bitcoin', available at: https://coinmarketcap.com/currencies/bitcoin/
[16] CoinMarketCap, 'Ethereum', available at: https://coinmarketcap.com/currencies/ethereum/
[17] CoinMarketCap, 'Ripple', available at: https://coinmarketcap.com/currencies/ripple/
[18] CoinMarketCap, 'Monero', available at: https://coinmarketcap.com/currencies/monero/

DOGECOIN

Dogecoin is an example of a “joke currency”, evidenced by the official website claiming that Dogecoin is ‘favo[u]red by Shiba Inus worldwide.’

Usage of Dogecoin is limited to Doge-related goods, such as clothing apparel and miscellaneous gifts. Dogecoin is most popularly used as a tip for internet content creators who create good content, similar to “Likes” on Facebook.

As at 31 December 2017, one Dogecoin was priced at USD 0.008, with a market capitalisation of USD 887.2 million.[19]

[19] CoinMarketCap, ‘Dogecoin’, available at: https://coinmarketcap.com/currencies/dogecoin/

SECTION 2

DEVELOPMENT OF RELATED INDUSTRIES

OVERVIEW

With BTC and other cryptocurrencies gaining significant traction, related industries are prospering, as entrepreneurs attempt to capture opportunities from this revolution.

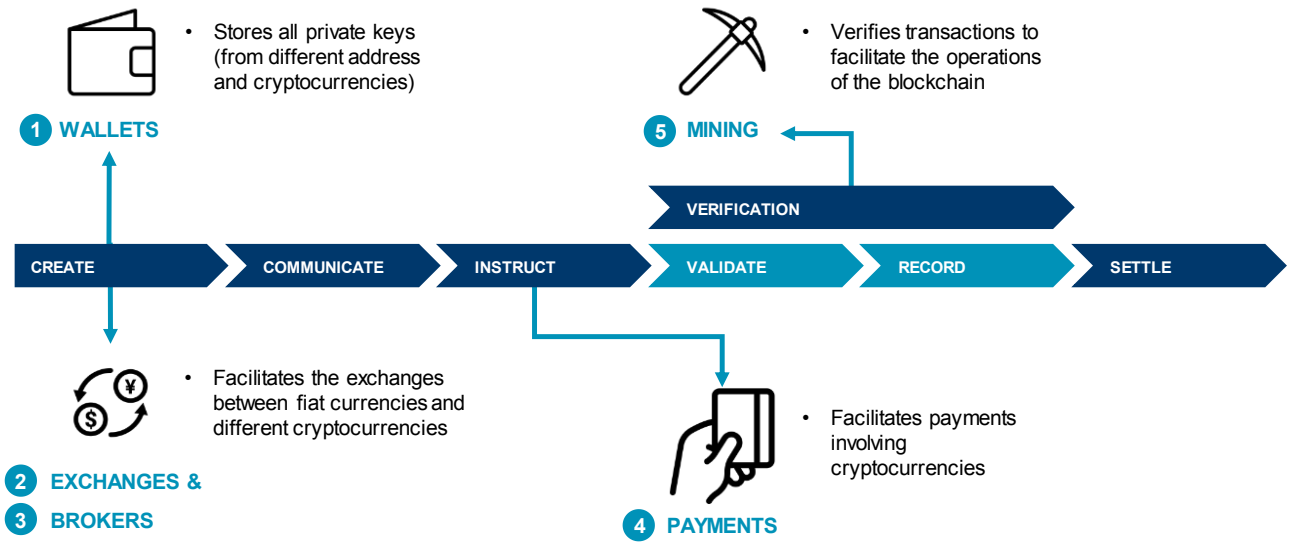
The five main industries that support and facilitate the operations of the blockchain are (see Figure 9):

1. Wallets;
2. Exchanges;
3. Brokers;
4. Payments; and
5. Mining.

Wallets, exchanges, brokers, and payments companies provide services to enhance the experience of cryptocurrency users, and can be treated as add-ons to the cryptocurrency, charging users for their services. There are an increasing number of companies which provide services in more than one industry – for example, some cryptocurrency exchanges provide wallet services to their users, and most wallet providers also offer payment services.

On the other hand, mining services are necessary for the operations and maintenance of the system, and are incentivised by rewards provided by the system itself (block rewards) and transaction fees provided by the users.

FIGURE 9: CRYPTOCURRENCY RELATED INDUSTRIES



Source: Quinlan & Associates analysis

WITH BTC AND OTHER CRYPTOCURRENCIES GAINING SIGNIFICANT TRACTION, RELATED INDUSTRIES ARE PROSPERING, AS ENTREPRENEURS ATTEMPT TO CAPTURE OPPORTUNITIES FROM THIS REVOLUTION

1. WALLETS

Unlike day-to-day wallets which hold banknotes and coins, cryptocurrency wallets do not hold or contain the cryptocurrencies.

Anyone who controls the private key controls the wealth in the associated address, and therefore anything storing the private key can be treated as the wallet holding the cryptocurrency. Some users may hold multiple addresses for a single cryptocurrency (for example, Bitcoin recommends its users to create a new address for every transaction for privacy). As such, having a wallet that holds all the addresses and associated private keys is extremely convenient.

Some popular choices are online wallets, desktop wallets, mobile wallets, hardware wallets, and paper wallets. The following are some examples of cryptocurrency wallets and their key features (See Figure 10).

FIGURE 10: EXAMPLES OF CRYPTOCURRENCY WALLETS

ONLINE	DESKTOP	MOBILE	HARDWARE	PAPER
GreenAddress	*Exodus*	*Electrum*	*Trezor*	*bitaddress.org*
• Can be accessed through Chrome as an extension • Improves security using a 2-layer validation for transactions, needing both the user's approval and the website's approval (given only if transactions satisfy predetermined conditions)	• Supports BTC and other cryptocurrencies, including Dash and Ether • Provides details on the users' cryptocurrency portfolio • Also provides exchange services	• Private keys are encrypted and stored in the users' device, and the users can view the address details online using a watch-only wallet (private keys are not uploaded or used) • Also provides desktop wallet services	• Supports BTC and other cryptocurrencies, including Ether and Litecoin • Also provides password management for different websites • Costs EUR 89 according to the official website	• A website which helps generate a private key and the associated address • Website displays the private key and address as alphanumerical characters and as QR codes • Users then write down or print out the details

Source: Quinlan & Associates analysis

Two main criteria for choosing the type of wallet are access (i.e. how easy it is to access the cryptocurrency wealth and conduct transactions) and security (i.e. the protection of private keys) (see Figure 11).

FIGURE 11: TYPES OF CRYPTOCURRENCY WALLETS

WALLET TYPE	DESCRIPTION	ACCESS	SECURITY
ONLINE	• Acts like an online account • Holds private keys on the server		
DESKTOP	• An application on the desktop • Holds private keys locally		
MOBILE	• An application on the mobile phone • Holds private keys locally		
HARDWARE	• An external and portable hardware • Holds private keys locally		
PAPER	• A piece of paper • Printed with private key (the private key and QR code of the private key)		

Source: Quinlan & Associates analysis

ONLINE WALLETS

Online wallets are similar to online accounts, which can be accessed by users through the internet. Some online wallets can also be linked to mobile or desktop wallets.

Due to its web-based nature, online wallets can be accessed from virtually anywhere. However, the details of the users (including the address and associated private key) are typically kept with the service provider, which means the service providers have easy access to the users' cryptocurrencies.

Online wallets are prime targets for hackers, as gaining access to the list of private keys gives hackers the ability to move all cryptocurrency fortunes to their own addresses.

DESKTOP/MOBILE WALLETS

Desktop wallets and mobile wallets are similar, both being an application installed on the users' electronic devices.

Desktop wallets tend to provide extra features, such as better security or a higher level of privacy, while mobile wallets are more portable and therefore provide better access. Both wallet types store the users' details locally, and are therefore more secure than online wallets, provided there is no malware present. However, hardware failure of the desktop or mobile phone will lead to the loss of private keys, and therefore backups are recommended.

Note also that there are online wallets which offer associated desktop or mobile applications, and in these cases, the service providers may have access to the users' private keys, compromising security.

HARDWARE WALLETS

A hardware wallet is similar to a USB stick, and is used by plugging into a desktop computer.

Hardware wallets are highly secure as the private key is stored on an external device and cannot be transferred out of the wallet, making them immune to computer viruses.

Furthermore, given their small size, hardware wallets are easily portable, and hence provide a high level of access. However, as with desktop wallets and mobile wallets, hardware failure is the major concern for hardware wallet users.

PAPER WALLETS

A paper wallet is simply a piece of paper with the address and associated private key written or printed on it.

Sometimes the address and private key are also translated into QR code form for easier transactions. This can be done using online services which generate the keys for users randomly, after which the result is printed. If a user does not trust online services, the process of generating a QR code of a private key, followed by the associated public key and address, can be conducted on an offline computer, or by hand (which is extremely time consuming).

Paper wallets can be stored and hidden easily (given it is literally a piece of paper). As there is little digital trace (only at creation using online services), paper wallets are considered extremely secure. However, users need to input the details into a client during transactions, which can be inconvenient, and pieces of paper are easily damaged or destroyed.

2. EXCHANGES

Cryptocurrency exchanges facilitate the buying or selling of cryptocurrencies using other cryptocurrencies or fiat currencies. There are currently over 150 cryptocurrency exchanges in operation. More than 70 of these exchanges have a daily transaction volume of over USD 10 million, the majority of which are situated in Asia Pacific (see Figure 12).

FIGURE 12: DISTRIBUTION OF CRYPTOCURRENCY EXCHANGES

AMERICAS		EMEA		APAC			
Bittrex	US	**CoinsBank**	UK	***Coincheck***	Japan	***Bithumb***	South Korea
GDAX	US	**Exmo**	UK	***bitFlyer***	Japan	***Coinone***	South Korea
Poloniex	US	**CEX.IO**	UK	***BTCBOX***	Japan	***Coinnest***	South Korea
Kraken	US	**Tidex**	UK	***Zaif***	Japan	***Korbit***	South Korea
Gemini	US	**CoinEgg**	UK	***LakeBTC***	Japan	***Coinrail***	South Korea
itBit	US	**Luno**	UK	***Quoine***	Japan	***BTC Markets***	Australia
BitShares	US	**CoinFalcon**	UK	***Fisco***	Japan	***CoolCoin***	Australia
QuadrigaCX	Canada	**Mercatox**	UK	***Neraex***	Japan	***Bitfinex***	Taiwan
Allcoin	Canada	**Paribu**	Turkey	***Bitbank***	Japan	***Bitcoin Indonesia***	Indonesia
Coinsquare	Canada	**BTCTurk**	Turkey	***Binance***	Hong Kong	***Cryptopia***	New Zealand
Foxbit	Brazil	**Koinim**	Turkey	***HitBTC***	Hong Kong	***Bits Blockchain***	Macau
Mercado Bitcoin	Brazil	**WEX**	Russia	***EXX***	Hong Kong	***BX Thailand***	Thailand
Bitso	Mexico	**YoBit**	Russia	***Bit-Z***	Hong Kong	***Koinex***	India
GetBTC	Saint Vincent and the Grenadines	**Bitonic**	Netherlands	***Gate.io***	Hong Kong		
		LiteBit	Netherlands	***ACX***	Hong Kong		
		BitBay	Poland	***Lbank***	Hong Kong		
		BitMarket	Poland	***Gatecoin***	Hong Kong		
		BitMEX	Seychelles	***OKEx***	China		
		Bitstamp	Luxembourg	***Huobi***	China		
		Liqui	Ukraine	***BTCC***	China		
		RightBTC	Dubai	***ZB.com***	China		
		Exrates	Armenia	***OKCoin***	China		

Note this only includes exchanges where daily transaction volume >USD 10 million as at 31 December 2017

Source: CoinMarketCap, exchange websites, Quinlan & Associates research

Examples of better-known cryptocurrency exchanges with the highest trading volumes include Bitfinex, Bithumb, BitMEX, GDAX, and Binance (see Figure 13). For a more comprehensive list of cryptocurrency exchanges, please refer to the appendix (see Appendix B).

FIGURE 13: EXAMPLES OF CRYPTOCURRENCY EXCHANGES

	Country/Base	Trading Volume (24h)	Cryptocurrency	Fiat Currency	Transaction Fees	Deposit / Withdrawal Fees	Additional Features
BITFINEX	• Taiwan	• USD 2.7 billion	• BTC • Ether • Litecoin • Dash • Etc.	• USD • EUR	• Maker: 0.0-0.1% • Taker: 0.1-0.2%	• Deposit: 0.1% • Withdrawal: 0.1%	• Leveraged margin trading through P2P funding • Associated with Tether (a cryptocurrency)
bithumb	• Korea	• USD 2.6 billion	• BTC • Ether • Litecoin • Zcash • Etc.	• KRW	• Maker: 0.15% • Taker: 0.15%	• Withdrawal: 1,000 KRW	
BitMEX	• Seychelles	• USD 2.4 billion	• BTC • Ether • Monero • Zcash • Etc.	• USD • JPY	• Maker: -0.25%-0.0% • Taker: 0.075%-0.25%	• Deposit: 0 • Withdrawal: 0	• Provides futures and swaps
GDAX	• US	• USD 1.4 billion	• BTC • Ether • Litecoin	• USD • EUR • GBP	• Maker: 0.0% • Taker: 0.1%-0.25%	• Deposit: USD 10 • Withdrawal: USD 25	• Insurance of up to USD 250,000 per customer
BINANCE	• Hong Kong	• USD 1.0 billion	• BTC • Ether • Litecoin • Binance coin		• Maker: 0.1% • Taker: 0.1%		• Has own cryptocurrency, Binance Coin

Note empty cells mean information is not available by the time of publication

Source: CoinMarketCap, exchange websites, Quinlan & Associates research

We believe there are multiple factors to take into consideration when choosing which cryptocurrency exchange to use. These criteria can generally be separated into two categories: (1) offering and (2) ease-of-use (see Figure 14).

FIGURE 14: CRITERIA FOR CHOOSING CRYPTOCURRENCY EXCHANGE

	CRITERIA	DESCRIPTION
OFFERING	REPUTATION	• External market reputation / customer reviews
	VOLUME	• Order book volume, especially for target cryptocurrency
	EXECUTION	• Speed of execution
	RANGE	• Range of cryptocurrencies and fiat currencies supported
	FEES	• Amount of fees charged
	SECURITY	• Cybersecurity of the exchange, especially those providing wallet services
	INFRASTRUCTURE	• Ability of the system to handle operations
	PROTECTION	• Customer protection mechanisms
EASE-OF-USE	DEPOSIT METHODS	• Range of deposit methods supported
	VERIFICATION	• Requirement of ID verification for account registration
	ACCESS	• Geographical restrictions
	INTERFACE	• User interface of the exchange and related applications

Source: Quinlan & Associates analysis

OFFERING

REPUTATION

In general, an established exchange with a good reputation has a larger user base, leading to higher order book volumes. This contributes to greater levels of liquidity, which is vital given the volatile nature of cryptocurrency prices.

VOLUME

Cryptocurrency exchanges with better reputations tend to attract higher trading volumes. However, users should focus their attention on the volume of the cryptocurrency they want to trade rather than total traded volumes, given this directly impacts the liquidity of the target cryptocurrency.

EXECUTION

Due to the volatile nature of cryptocurrency prices (e.g. BTC price dropped by almost 2% within a minute on 3 December 2017, according to Coindesk data), speed of execution is of utmost importance. The reputation of an exchange contributes to its liquidity, which in turn allows for faster execution speed.

RANGE

Range refers to both the cryptocurrencies provided – as well as the fiat currencies supported – by the particular exchange.

The most well-known cryptocurrencies, such as BTC, Ether, and Litecoin, and fiat currencies (including USD, GBP, and JPY), are generally supported by most exchanges. However, some cryptocurrency exchanges distinguish themselves by providing exchange services for relatively unknown cryptocurrencies with significantly lower market capitalisations, such as BlueCoin and eBitcoin, or by providing related products, including derivatives for more sophisticated investors (e.g. BTC swaps and futures).

FEES

Exchanges charge different fees based on the users' activities. These can include trading/transaction fees, deposit fees, and withdrawal fees.

Trading fees can be separated into maker fees and taker fees, with maker fees typically lower than taker fees, but both ranging around 0.2%. Deposit fees tend to be waived for cryptocurrencies, but users are charged for fiat currencies. Finally, withdrawal fees (typically <1%) are charged when users withdraw fiat currencies from their accounts.

SECURITY

Internal security and cybersecurity are extremely important for cryptocurrency exchanges, especially those that hold users' funds on behalf of the users and those that provide associated wallet services.

One of the most notable examples of a security breach was the liquidation of Japan-based Mt. Gox, which was once the world's largest Bitcoin exchange. In early 2014, Mt. Gox filed for bankruptcy and announced that ~BTC 850,000 (~750,000 owned by users and 100,000 by Mt. Gox), then valued at USD 480 million, was stolen.[20] Another example is Youbit, a South Korean cryptocurrency exchange, which filed for bankruptcy in December 2017 after losing 17% of its assets in a cyberattack.[21]

INFRASTRUCTURE

On 14 December 2017, one of the largest Bitcoin exchanges, Coinbase's GDAX, was non-functional on 10 separate occasions due to heavy web traffic. As a result, 10 million customers were unable to reach the exchange or the Coinbase wallet.[22]

The rapid increase in BTC price has led to a high level of interest from the market. As such, cryptocurrency exchanges need stable infrastructure and capacity to handle rapidly increasing transaction volumes.

PROTECTION

Other than internal security measures, customer protection mechanisms provided by cryptocurrency exchanges are also important.

These could include 2-step verifications, e-mail notifications for suspicious account access, analysis of data to detect unusual activities, and withdrawal protections.

[20] Reuters, 'Mt. Gox files for bankruptcy, hit with lawsuit', 28 February 2014, available at: https://www.reuters.com/article/us-bitcoin-mtgox-bankruptcy/mt-gox-files-for-bankruptcy-hit-with-lawsuit-idUSBREA1R0FX20140228
[21] BBC, 'Bitcoin exchange Youbit shuts after second hack attack', 19 December 2017, available at: https://www-bbc-co-uk.cdn.ampproject.org/c/s/www.bbc.co.uk/news/amp/technology-42409815
[22] New York Times, 'Bitcoin Fever Exposes Crypto-Market Frailties', 14 December 2017, available at: https://www.nytimes.com/reuters/2017/12/14/business/14reuters-markets-bitcoin-risks-insight.html

EASE-OF-USE

DEPOSIT METHODS

Different deposit or payment methods include debit/credit cards, bank transfers, Paypal, and cryptocurrency payments. A cryptocurrency exchange may charge different fees based on the payment method used.

VERIFICATION

Some cryptocurrency exchanges require users to provide ID verification during registration, and personal details are also linked to the account if the users adopt payment methods such as bank transfers.

While providing more information to a cryptocurrency exchange is beneficial for anti-money laundering (AML) and/or counter-terrorist financing (CTF) reasons, this compromises one of cryptocurrencies' key functions as an anonymous, private payment method.

Most exchanges have instituted vigorous Know Your Customer (KYC) and AML/CTF protocols, with the expectation that they will be subject to such regulatory requirements in future.

ACCESS

Due to different regulations, some cryptocurrency exchanges are geographically limited and may require different levels and forms of customer identification.

As a result, the level of demand and supply for cryptocurrencies may differ between exchanges, leading to price differences and arbitrage opportunities. For example, on 28 November 2017, BTC was listed at USD 10,026 and USD 9,748 on CEX (South Korea) and Kraken (US) respectively, representing a difference of nearly 3%.[23]

INTERFACE

This criterion simply refers to how easy it is to use the interface of the exchange, and is highly personal and subjective. Some cryptocurrency exchanges also offer mobile applications, allowing seamless trading across platforms.

[23] Business Insider, 'The 'immature' global bitcoin market is ripe for arbitrage', 28 November 2017, available at: http://www.businessinsider.com/bitcoin-cryptocurrency-arbitrage-2017-11

3. BROKERS

Similar to cryptocurrency exchanges, cryptocurrency brokers facilitate trades between cryptocurrencies with other cryptocurrencies or fiat currencies.

The main difference between exchanges and brokers is the counterparty of the transaction; while an exchange matches a willing buyer with an appropriate willing seller and charges transaction fees, the broker is a market maker and buys or sells cryptocurrencies at specified prices to generate a profit. One can view brokers as foreign exchange firms, which buy foreign currencies at a low price and sell them at a high price, taking the spread as profit.

Some examples of cryptocurrency brokers include eToro, Plus500, 24option, and AVA (See Figure 15).

FIGURE 15: EXAMPLES OF CRYPTOCURRENCY BROKERS

BROKER	HEADQUARTERS	CRYPTOCURRENCIES	NOTABLE FEATURES
eToro	• Israel	• BTC • Bitcoin Cash • Dash • Ether • Ethereum Classic • Litecoin • Ripple	• Regulated by CySEC (Cyprus) and FCA (UK) • Spread ranges from 0.7% to 5% for cryptocurrencies • Signed a sponsorship deal with West Ham United in 2015
Plus500	• Israel	• BTC • Bitcoin Cash • Ether • Litecoin • Ripple • IOTA	• Regulated by ASIC (Australia) and FCA (UK) • Operates continuously, except on Sundays from 1200 to 1400 UTC • Signed a sponsorship deal with Atlético de Madrid in 2015
24option.com	• Belize	• BTC • Ether • Dash • Litecoin	• Regulated by IFSC (Belize) • Held a Christmas campaign, giving a chance to win BTC 1 • Signed a sponsorship deal with Juventus in 2014
AVATRADE	• Ireland	• BTC • Dash • Ether • Litecoin • Ripple	• Regulated by CBI (Ireland), ASIC (Australia), FSA (Japan), and FFAJ (Japan) • Continuous customer service available in 14 languages • Offers zero commissions and no bank fees for Bitcoin trading

Source: Service provider websites, Quinlan & Associates research

Another major difference between cryptocurrency exchanges and cryptocurrency brokers is that cryptocurrency brokers also tend to operate foreign exchange services, which means they have been authorised by financial regulators and are regulated entities. While their cryptocurrency businesses may not be regulated, their longer track record of operations, existing infrastructure, tested KYC/AML processes, and reputation, may provide a safer option for retail investors.

At the time of writing, the number of investment banks that have partaken in official cryptocurrency trading is zero. This is in part due to the highly volatile nature of the cryptocurrency space and regulations from governments who have sought to restrict financial institutions from entering such a trade (for example, China banning cryptocurrency trading and ICOs).[24] However, Goldman Sachs recently announced they would be setting up a cryptocurrency trading desk in New York by June 2018.[25] While there are many issues which have yet to be resolved – such as security, internal processes, and where to house the desk – this suggests that traditional financial institutions are getting serious about entering the cryptocurrency trading space in coming years.

.

[24] The Wall Street Journal, 'China's Interference on Bitcoin Tests Currency's Foundation', 18 September 2017, available at: https://www.wsj.com/articles/china-widens-bitcoin-crackdown-beyond-commercial-trading-1505733976?mod=e2tw
[25] Bloomberg, 'Goldman Is Setting Up a Cryptocurrency Trading Desk' 22 December 2017,, available at: https://www.bloomberg.com/news/articles/2017-12-21/goldman-is-said-to-be-building-a-cryptocurrency-trading-desk

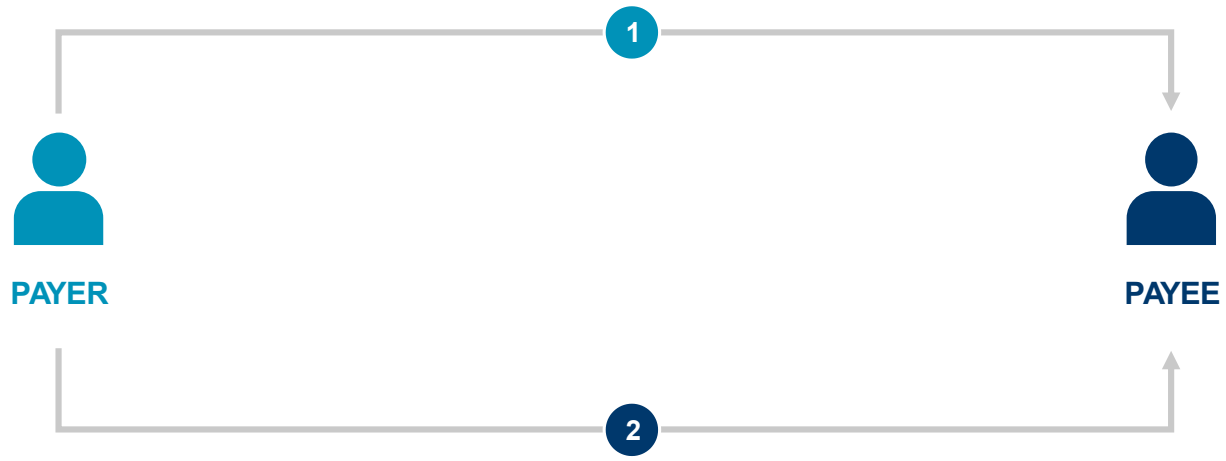
4. PAYMENTS

This section looks at the development of cryptocurrency payment facilitators.

Even though cryptocurrencies are created with an inherent payment system to handle transactions for their users, payment facilitators provide add-on features, such as an easy-to-use user interface, management of public and private keys, management and documentation of payment and receipt, additional security or privacy, and instant exchange between fiat currencies and cryptocurrencies.

There are two types of payment facilitators, and they focus on one of the two different parties of a transaction – the payer or the payee (see Figure 16).

FIGURE 16: PAYMENT FACILITATORS



1

SERVICE PROVIDED TO PAYER

- Helps the payer pay with cryptocurrencies
- The payer transfers cryptocurrencies to the payment facilitator, which are then exchanged for fiat currencies and transferred to the payee

2

SERVICE PROVIDED TO PAYEE

- Helps the payee receive cryptocurrencies
- The payment facilitator provides tools (physical for brick and mortar stores and virtual for online businesses) to receive cryptocurrencies

Source: Quinlan & Associates anaylsis

SERVICE PROVIDED TO PAYER

These payment facilitators help individuals spend their cryptocurrencies. This is typically done through cryptocurrency debit cards, like a Visa or MasterCard, that converts cryptocurrencies into fiat currencies.

The users can deposit cryptocurrencies into the cryptocurrency wallet that comes with the cryptocurrency debit card, and the deposited cryptocurrencies will be converted into fiat currency as the card is used.[26] This essentially allows users to pay for goods and services in stores that accept debit cards with cryptocurrencies. It also helps tourists by removing the need to convert foreign fiat currencies into local ones.

Despite being extremely helpful and practical for cryptocurrency payments, Visa and MasterCard seem relatively hesitant towards the idea. In fact, in October 2017, Visa suspended all cryptocurrency debit cards outside of the EEA, and MasterCard followed suit.[27]

There are upcoming projects with the aim of creating cryptocurrency debit cards, such as Centra, TenX, Monaco, and Pillar.[28] However, their services are currently unavailable or restricted geographically (due to the lack of support from global payment facilitators, Visa and MasterCard). The industry is hence still in its infancy.

SERVICE PROVIDED TO PAYEE

These payment facilitators typically provide applications and tools to businesses for accepting payments in cryptocurrencies from customers. For physical stores, the tools can include physical terminals and mobile phone apps, while for online retailers, the tools may include website plugins and APIs.

Retailers normally have two options after receiving payments; they can choose to simply hold the cryptocurrencies in a digital wallet or exchange them for fiat currencies, which will then be deposited into their bank account.

In terms of pricing, payment services may charge users based on a subscription model, through transaction fees, or withdrawal fees (for withdrawing cryptocurrencies or fiat currencies). The more prominent payments service providers tend to charge a 1% transaction or processing fee, which is arguably cheaper than traditional payment services, such as ~3% for PayPal.

Because of the management of public and private keys, some payments service providers also provide wallet services.

A few examples of payments service providers are BitPay, Coinbase, and CoinGate, each with their own distinct features (see Figure 17).

[26] Cryptoincome.io, 'Crypto Debit Cards: Spending Cryptocurrency in the Read World', 30 November 2017, available at: http://cryptoincome.io/crypto-debit-cards/
[27] The Merkle, 'MasterCard Removes Cryptocurrency Debit Card Availability Outside EEA', 12 October 2017, available at: https://themerkle.com/mastercard-joins-visa-in-removing-cryptocurrency-debit-card-availability-outside-of-the-eea/
[28] Cryptoincome.io, 'Crypto Debit Cards: Spending Cryptocurrency in the Read World', 30 November 2017, available at: http://cryptoincome.io/crypto-debit-cards/

FIGURE 17: EXAMPLES OF PAYMENT SERVICE PROVIDERS

PROVIDER	LOCATION	FEES	NOTABLE CLIENTS	KEY FEATURES
bitpay	• US	• 1% transaction fee	• Microsoft • Shopify • Virgin Galactic	• Provides retail and eCommerce tools to help accept payments • BTC is converted into fiat currency and deposited into bank account • Also provides wallets service
coinbase	• US	• 1% for exchanging BTC into fiat currency	• Bloomberg • Expedia • Paypal	• Provides website plugins and APIs to help accept payments • BTC can be sold immediately to Coinbase through "Instant Exchange" function to eliminate risk of price fluctuations • Also operates a cryptocurrency exchange
COINGATE	• Lithuania	• 1% transaction fee	• UnrankedSmurfs (sells League of Legends accounts) • Mineshop (sells cryptocurrency miners)	• Provides mobile phone apps, website plugins, and APIs to help accept payments • Accepts other cryptocurrencies, such as Ether, Litecoin, and Dash • Other cryptocurrencies are instantly converted to BTC, EUR, or USD

Source: Company websites, Quinlan & Associates research

5. MINING

Mining is an essential component of the blockchain, and is vital for smooth operations and the facilitation of transactions.

Due to the explosive increase in the price of multiple cryptocurrencies in 2017, mining has transformed from being a hobby to a full-scale business. According to Cambridge's Global Cryptocurrency Benchmarking Study, Bitcoin miners earned over USD 2 billion in revenue up to 2016.[29] There is also an increasing number of hardware manufacturing firms which specialise in providing tailored machines, called Application-Specific Integrated Circuits (ASICs), which are essentially computers specialised in Bitcoin mining, providing superior hash power (mining power) while using less electricity.

There are three main mining groups:

1. Individual mining;
2. Mining services; and
3. Mining pools.

INDIVIDUAL MINING

As the name suggests, individual mining is when individuals use their own hardware (such as their own desktop computer or a purchased ASIC) to mine cryptocurrencies.

It is extremely difficult for individual miners to compete against large mining pools (see later). The most important consideration for individual miners is the efficiency of their mining rigs (i.e. number of cryptocurrencies mined per price of a unit of electricity). If individual miners successfully mine a block, they receive the full payment (for Bitcoin, it is currently BTC 12.5 per block).

MINING SERVICES

Mining services, cloud mining, or mining contracts, provide mining power with capacity specified by contract. This is done through renting out specified mining power or mining rigs for a duration at a price.

The obvious advantage of this is that individuals do not need to invest in the hardware and do not have to deal with issues such as excess heat, noise, and electricity bills. However, the individual is simply renting mining power and it is possible that the specific rig does not successfully mine any block, resulting in zero payout. In fact, there have been cloud mining scams, in which the company advertises non-existent hash power to attract individuals to pay and rent their service.

MINING POOLS

Running mining pools is currently the most dominant approach to Bitcoin mining, and occurs when multiple miners share their processing power over a network (so that the pool has a higher hash power). The block reward is then split based on the amount of power contributed.

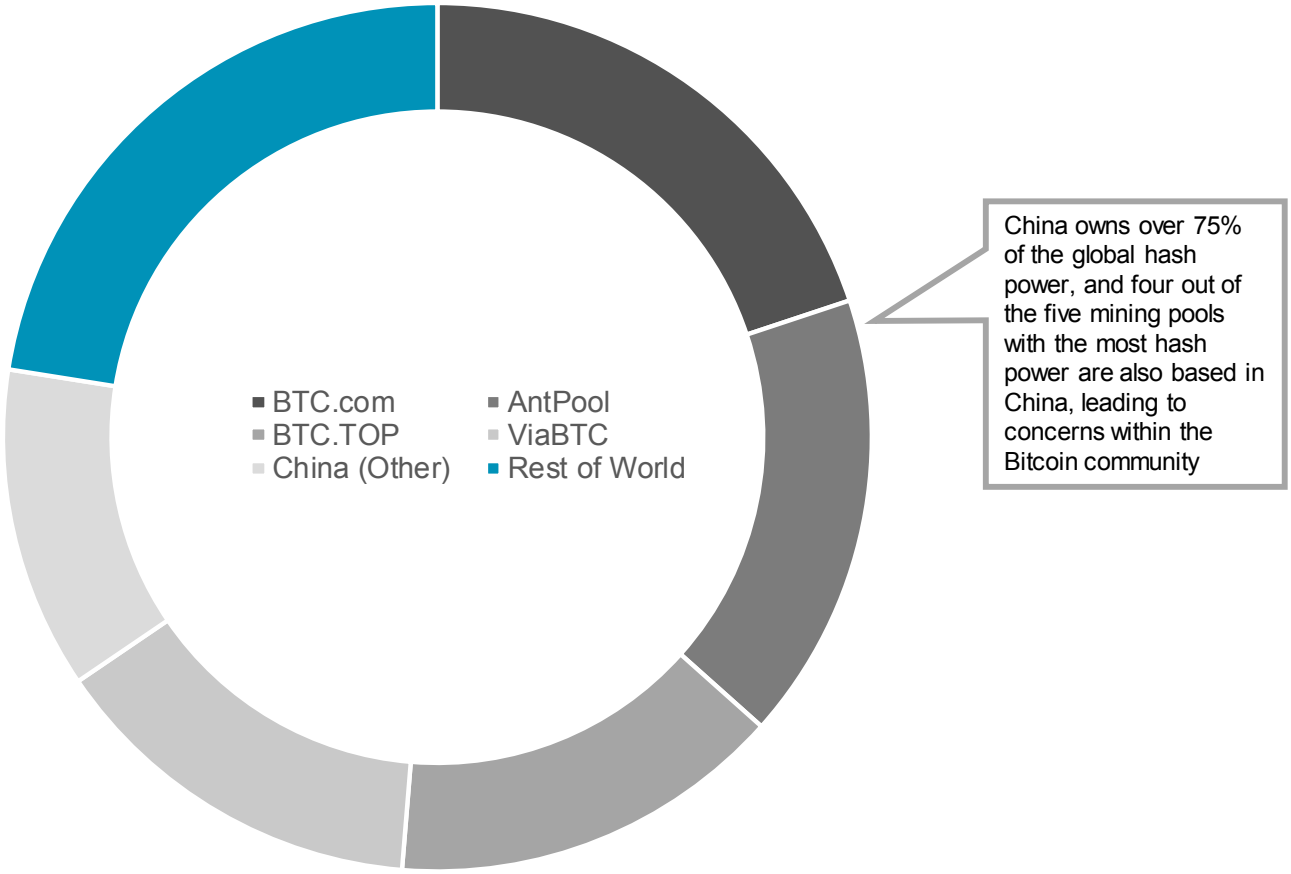
Mining pools came into existence when the difficulty of mining increased to the point where individual miners or slower miners were unable to mine any blocks. Pooling together resources provides a more consistent stream of lower rewards, instead of hoping to get lucky every once in a while. However, in addition to the lowered rewards, mining pool operators also charge pool fees for managing the pool.

[29] Cambridge Centre for Alternative Finance, 'Global Cryptocurrency Benchmarking Study', Dr. Garrick Hileman & Michel Rauchs

HASH POWER

As at 31 December 2017, the five Bitcoin mining pools with the most hash power were BTC.com (19.9%), AntPool (16.7%), BTC.TOP (14.7%), ViaBTC (14.2%), and SlushPool (9.1%),[30] with the top four mining pools based in China. In fact, by the end of 2017, China held over 75% of Bitcoin's collective hash power, mainly due to the extremely low electricity prices in the country (see Figure 18).

FIGURE 18: HASH POWER DISTRIBUTION



Source: Blockchain Luxembourg S.A., mining pool website, Quinlan & Associates analysis

[30] Blockchain Luxembourg S.A., 'Hashrate Distribution', available at: https://blockchain.info/pools

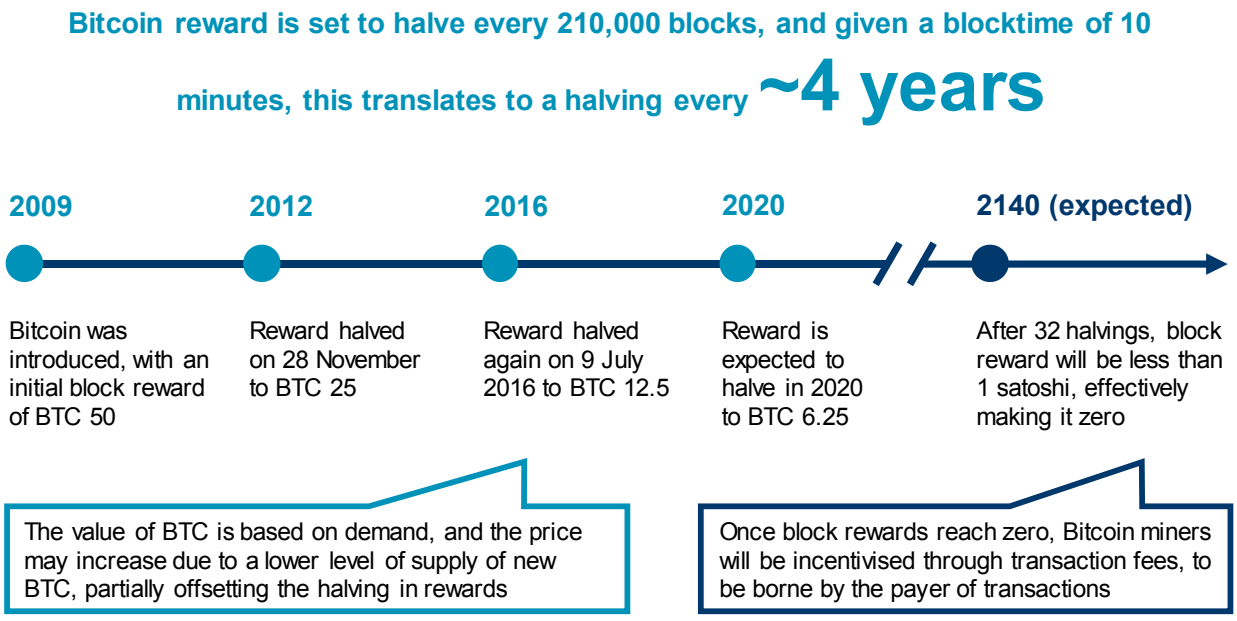
This concentration of hash power has led to concerns among the Bitcoin community regarding a 51% attack. This occurs when a single party holds over 50% of the hash power, enabling them to prevent new transactions, halt payments, and even reverse transactions (i.e. they can double spend their cryptocurrency). Any mining pool with over 50% of the total hash power can exert significant influence onto the cryptocurrency. In fact, in 2014, GHash.IO briefly exceeded 50% of the hash power, leading to Ghash.IO voluntarily limiting their hash power to 39.99% to appease the community's concerns.[31]

BLOCK REWARDS

Bitcoin is designed to halve the block reward every 210,000 blocks (roughly every four years).

The block reward started at BTC 50 per block in 2009. It halved in 2012 to BTC 25, and halved again in 2016 to BTC 12.5 per block, and eventually, after 32 divisions, the reward will be less than 1 satoshi (effectively making it BTC 0), resulting in the limit of a total of BTC 21 million in circulation (see Figure 19).

FIGURE 19: BITCOIN BLOCK REWARD TIMELINE



Source: Quinlan & Associates analysis

Halving the block reward essentially means the number of BTC received by miners is halved, on average, every four years, which may discourage some miners from continuing operations. However, some have argued that the value of BTC is based on demand and

[31] Coindesk, 'GHash Commits to 40% Hashrate Cap at Bitcoin Mining Summit', 16 July 2014, available at: https://www.coindesk.com/ghash-commits-40-hashrate-cap-bitcoin-mining-summit/

supply, and if the demand for BTC stays at the same level, the price of BTC will increase to counteract the halving of new supply. This means that the halving of the block reward does not directly translate into a halving of revenues for miners. Accordingly, the price of BTC and the size of the reward will need to be weighed against the cost of mining.

Due to the decreasing BTC rewards available for mining in future years, miners are likely to be increasingly incentivised by transaction fees, paid by the user initiating the transactions. However, this will inevitably push out smaller miners who will find it less profitable to stay in business, leading to a reduction in the number of miners. This will subsequently increase the risk of concentration and the threat of a 51% attack.

SECTION 3

STAKEHOLDER PERSPECTIVES

OVERVIEW

Despite cryptocurrency being a revolutionary system, developed to create a decentralised digital currency and to be used as one, it is clear that it is not currently used for its intended purpose, especially by the general public (see Figure 20).

FIGURE 20: INTENDED USAGE VS ACTUAL USAGE

	STAKEHOLDER	KNOWLEDGE	CURRENT USAGE/VIEW
1	GENERAL PUBLIC	✗	• Used as a speculative investment • Illegal/grey area use
2	GENERAL BUSINESSES	✗	• Relatively few businesses accept cryptocurrencies as payment • Technology firms are generally more enthusiastic
3	FINTECH START-UPS	✓	• Create new tokens during ICOs to raise capital • Emergence of FinTech firms providing services based on blockchain technology
4	BANKS	✓	• Majority of banks denounce the usage of and investments in cryptocurrency • High degree of interest in blockchain technology
5	EXCHANGES AND FUND MANAGERS	–	• Used as a speculative investment • High degree of interest in blockchain technology
6	GOVERNMENTS AND REGULATORS	✓	• Some have banned the usage of private cryptocurrencies • Generally strong interest in blockchain technology • Some have expressed interest in or intention to launch national cryptocurrency

✗ Weak – Dependent ✓ Strong

Source: Quinlan & Associates analysis

Knowledge in Figure 20 refers to in-depth understanding of the blockchain technology and its potential, instead of a general knowledge (i.e. a quick Googling) of what cryptocurrencies are and how they can be used.

Overall, the general public and businesses tend to have a superficial understanding of cryptocurrencies, as interest originally sparked from the explosive growth in the price of BTC. Banks and governments, on the other hand, have been researching and experimenting with blockchain technology for a considerable period of time, providing them with a much deeper understanding and appreciation of its uses and applications.

1. GENERAL PUBLIC

The general public rarely uses cryptocurrencies to pay for goods and services. Reasons for this include a lack of businesses that accept cryptocurrencies, higher cost compared to using fiat currencies (businesses tend to charge more due to price fluctuations), and high transaction costs.

The majority of the wider population uses cryptocurrencies, and most famously BTC, for speculative and investment purposes. However, it is important to note that the level of investment does not appear to be supported by a commensurate level of knowledge. For example, it was reported that retail investors in Hong Kong are participating in the Bitcoin market, without actually understanding the product, opportunity, or situation.[32]

We spoke with William Piquard, the COO of Hong Kong-based cryptocurrency exchange Gatecoin, who told us that the majority of investors in BTC before 2017 were IT or financial professionals with a good understanding and knowledge of the cryptocurrency and its underlying technology. However, with the substantial price increase in most cryptocurrencies in late 2017, there was a new wave of investors, who have little understanding of the technology and risks involved.

In fact, based on our 1,500 survey respondents who had investments in cryptocurrencies, 13% indicated their knowledge was weak, and 40% claimed to have only a moderate level of knowledge (see Section 7). This problem is further magnified by the risk involved in trading BTC. Emil Oldenburg, co-founder of Bitcoin.com, said that 'investment in BTC is right now the riskiest investment [one] can make.' He has also sold all his BTC and invested in Bitcoin Cash.[33]

This phenomenon is especially prominent in Japan and South Korea. Deutsche Bank believes that Japan is the major source driving the surge in BTC prices, while a Nikkei report says that 40% of cryptocurrency trading during October and November 2017 was JPY denominated.[34]

[32] SCMP, 'Hongkongers are going big on bitcoin, but some don't understand what they are getting into', 16 December 2017, available at: http://www.scmp.com/news/hong-kong/economy/article/2124598/hongkongers-are-going-big-bitcoin-some-dont-understand-what
[33] The Sydney Morning Herald, ''Extremely high risk': bitcoin.com co-founder has sold all his bitcoins' 21 December 2017, available at: http://www.smh.com.au/business/markets/bitcoin-as-good-as-useless-says-bitcoin-com-co-founder-20171218-p4yxty.html
[34] Bloomberg, 'Deutsche Bank Says Japan's Retail Investors Are Behind Bitcoin's Surge', 14 December 2017, available at: https://www.bloomberg.com/news/articles/2017-12-14/deutsche-bank-says-mrs-watanabe-behind-the-surge-in-bitcoin

In South Korea, the government issued a statement that noted the trading prices of most cryptocurrencies were higher on South Korean exchanges than on foreign exchanges.[35] In fact, the head of business development at BitMex (a cryptocurrency exchange), Greg Dwyer, said that 'every crypto[currency] is priced at a 30 percent premium in South Korea',[36] demonstrating the South Koreans' level of enthusiasm for cryptocurrency investments.

South Korean prime minister, Lee Nak-yeon, has expressed his concerns about such speculative behaviour 'lead[ing] to serious distortion or social pathological phenomena'. Mr. Lee is particularly worried about young people investing in BTC, with a 16-year-old high school student saying 'he had been drawn to Bitcoin because it has gone up so quickly, and doesn't require the same amount of knowledge as stock investing.'[37] Regrettably, this seems to be the norm for retail investors, in which the constant media coverage of the rocketing price of BTC has sparked intense interest, leading to high levels of investment without sufficient research or analysis.

[35] Reuters, 'South Korea to impose new curbs on cryptocurrency trading', 28 December 2017, available at: https://uk.reuters.com/article/uk-southkorea-bitcoin/south-korea-to-impose-new-curbs-on-cryptocurrency-trading-idUKKBN1EM05K
[36] Reuters, 'Bitcoin slides as website drops South Korea prices from virtual currency rates', 8 January 2018, available at: https://www.reuters.com/article/uk-global-bitcoin/bitcoin-slides-as-website-drops-south-korea-prices-from-virtual-currency-rates-idUSKBN1EX1DB
[37] The New York Times, 'In South Korea, the Virtual Currency Boom Hits Home', 3 December 2017, available at: https://www.nytimes.com/2017/12/03/technology/virtual-currency-south-korea.html

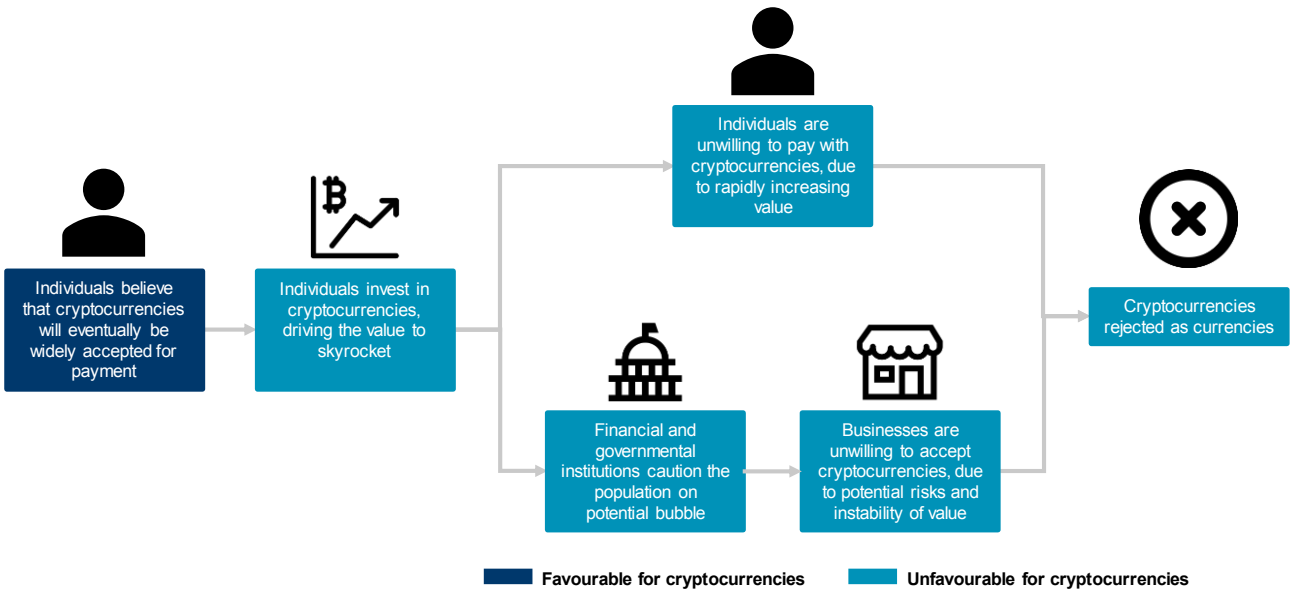
Furthermore, as the cryptocurrency space remains largely unregulated, retail investors are susceptible to "pump and dump" activities, which are illegal in traditional markets. It was reported that cryptocurrency traders use a secure messaging app, Telegram, to co-ordinate large purchases for a cryptocurrency, artificially inflating the price to attract investors, then bulk selling the cryptocurrency for profit.[38]

It is worth noting that, similar to fiat currency, the value of cryptocurrency stems from the population's trust and confidence in it. The population believes a USD 1 banknote provides value equivalent to USD 1 because the US government, a trusted party, says so. In contrast, the value of cryptocurrency originates from investors' confidence in the blockchain system and their belief that cryptocurrencies will eventually be recognised and widely accepted. However, this confidence leads to higher levels of investment, pushing up prices. As a result, consumers are less likely to purchase goods and services with cryptocurrencies due to their seemingly ever-inflating values.

In addition, the rapid surge in prices has led to prominent financial and governmental figures cautioning about the potential of a bubble, leading to reluctance by businesses to accept cryptocurrencies as a form of payment.

Taken together, this all creates an interesting paradox, as the very belief that cryptocurrencies can be used as currencies has in fact led to actions that discourage their acceptance as currencies (see Figure 21).

FIGURE 21: CRYPTOCURRENCY PARADOX



Source: Quinlan & Associates analysis

[38] Business Insider, "Market manipulation 101': 'Wolf of Wall Street'-style 'pump and dump' scams plague cryptocurrency markets', 14 November 2017, available at: http://uk.businessinsider.com/ico-cryptocurrency-pump-and-dump-telegram-2017-11

THE VERY BELIEF THAT CRYPTOCURRENCIES CAN BE USED AS CURRENCIES HAS IN FACT LED TO ACTIONS THAT DISCOURAGE THEIR ACCEPTANCE AS CURRENCIES

Cryptocurrencies have also been used as tools for illegal or grey area activities, with the most famous example being the Silk Road. Silk Road was an online black market known for selling illegal drugs, and the founder and then-owner, Ross Ulbricht, was arrested on 2 October 2013,[39] with the FBI seizing BTC 26,000 (then valued at ~USD 3.6 million) from Silk Road accounts[40] and BTC 144,000 (then valued at ~USD 28.5 million) from Ross Ulbricht.[41]

Other illegal activities cryptocurrencies have been associated with include tax evasion and money laundering, due to their highly private and anonymous nature.

[39] Forbes, 'Who Is Ross Ulbricht? Piecing Together The Life Of The Alleged Libertarian Mastermind Behind Silk Road', 2 October 2013, available at: https://www.forbes.com/sites/ryanmac/2013/10/02/who-is-ross-ulbricht-piecing-together-the-life-of-the-alleged-libertarian-mastermind-behind-silk-road/#303ee9023a74

[40] Forbes, 'The FBI's Plan For The Millions Worth Of Bitcoins Seized From Silk Road', 4 October 2013, available at: https://www.forbes.com/sites/kashmirhill/2013/10/04/fbi-silk-road-bitcoin-seizure/#1b0c71bc2848

[41] Forbes, 'FBI Says It's Seized $28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road', 25 October 2013, available at: https://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/#6b8923af2765

2. GENERAL BUSINESSES

The first transaction using BTC to pay for goods and services occurred on 22 May 2010, when Laszlo Hanyecz paid BTC 10,000 for two pizzas.

Under the alias “laszlo”, Laszlo Hanyecz started a post on 18 May 2010 on Bitcoin Forum offering to trade BTC 10,000, which was worth USD 41 at that time according to a reply to the post[42], for ‘a couple of pizzas... like maybe 2 large ones.’[43] The request was completed by Jeremy Sturdivant, under the alias “jercos”, on 22 May 2010.

To commemorate the landmark transaction, Bitcoin Pizza Day (22 May) is celebrated by Bitcoin enthusiasts, with some businesses using the day as a promotion opportunity. For example, in 2014, eGifter (a gift card platform) gave extra points to customers using BTC, Litecoin, or Dogecoin to pay for Domino’s and Papa John’s gift cards.[44]

Since then, popularity of cryptocurrencies, especially BTC’s, has significantly increased, and an increasing number of businesses are accepting BTC as a form of payment (see Figure 22). However, acceptance still remains extremely limited.

[42] Note this would be equivalent to ~USD 200 million at the height of BTC’s valuation in 2017
[43] Bitcoin Forum, ‘Pizza for bitcoins?’, 18 May 2010, available at: https://bitcointalk.org/index.php?topic=137.0
[44] Coindesk, ‘Bitcoin Pizza Day: Celebrating the Pizzas Bought for 10,000 BTC’, 22 May 2014, available at: https://www.coindesk.com/bitcoin-pizza-day-celebrating-pizza-bought-10000-btc/

FIGURE 22: EXAMPLES OF BUSINESSES ACCEPTING BTC

COMPANY	IT BACKGROUND	DESCRIPTION
MICROSOFT	✓	• Tech giant, known for Microsoft Office and Windows System • Accepts BTC as deposits into Microsoft account for Windows and Xbox stores
VALVE	✓	• Largest digital distribution platform for computer games • Accepts BTC for Steam purchases (e.g. computer games) • Stopped accepting BTC on 7 December 2017, citing volatility and increasing transaction fees as reasons
EXPEDIA	✓	• Online marketplace for flight and hotel bookings • Partnered with Coinbase, a cryptocurrency exchange, to accept BTC as payment
OVERSTOCK	✓	• Online retailer selling home goods (e.g. furniture) • Partnered with Coinbase to accept BTC as payment
NEWEGG	✓	• Online retailer selling computer hardware and electronics • Supports payments from online, desktop, and mobile cryptocurrency wallets
EGIFTER	✓	• Online retailer selling gift cards • Partnered with BitPay, a payment service provider, to accept BTC as payment
WIKIPEDIA	✓	• Online encyclopaedia • Partnered with Coinbase to accept BTC as donation
REDDIT	✓	• Online social forum • Accepts BTC as payment for Reddit Gold, a premium membership programme
ZYNGA	✓	• Video game developer • Accepts BTC as payment for games or in-app purchases
OKCUPID	✓	• Online dating website • Accepts BTC as payment for subscription
NAUGHTY AMERICA	✓	• Adult entertainment • Accepts BTC as payment for subscription
ALPHABAY	✓	• Online marketplace on the Darknet, selling illegal products (e.g. drugs, fake IDs) • Accepted BTC for transactions • Shut down in July 2017
VIRGIN GALACTIC	✗	• Company under Virgin Group to develop commercial spaceflight • Accepts BTC as payment for future tickets
SUBWAY	✗	• Fast food franchise, specialising in submarine sandwiches • Several Subway restaurants in Buenos Aires accept BTC as payment
SAVE THE CHILDREN	✗	• Charity focusing on children in developing countries • Partnered with BitPay to accept BTC as donation

Source: Quinlan & Associates analysis

Given their deeper understanding of and interest in technology, technology companies appear more willing to accept cryptocurrencies as a form of payment than companies in other industries. In addition, an increasing number of businesses are using payment services to accept cryptocurrencies, most likely due to ease-of-use, as the businesses themselves do not need to concern themselves with technological issues.

There is a tendency for businesses to charge higher for cryptocurrency payments than credit card or cash payments, due to the volatility in price. For example, the adult website, Naughty America, charges USD 24.95 for a 1-month subscription and USD 71.4 for a 1-year subscription for credit card payments, but quotes USD 29.95 and USD 119.95 respectively for BTC payments, representing differences of 20% and 68%.

Some businesses also require customers to initiate the cryptocurrency payment within a certain timeframe during the checkout process, after which the price will be updated based on the exchange rate.

Other than the volatility of cryptocurrency prices, another reason why businesses, especially those selling subscription services, are reluctant to accept cryptocurrencies as payment, is the “push mechanism”. Typically, subscribers pay for subscription services using credit cards or automatic bank transfers. Due to the automatic and recurring nature of such payments, this provides a relatively stable income stream for the service provider. However, cryptocurrency payments require the payer to initiate a payment, demanding more time and effort from the subscriber and therefore discouraging the subscriber from regular payments. The push mechanism also makes it easier for the subscriber to cancel the subscription anytime. Therefore, businesses tend to charge customers paying with cryptocurrencies more than those paying via traditional methods.

In addition, tax authorities are also cautious of businesses receiving payments and individuals earning investment gains respectively through cryptocurrencies. Given the anonymous and private nature, cryptocurrency transactions can lead to inaccurate or dishonest accounting practices (including the misreporting of income), resulting in lower tax revenue.

3. FINTECH START-UPS

Blockchain technology provides FinTech start-ups with an alternative means to access capital, through Initial Coin Offerings (ICOs), also known as token sales.[45]

The process normally begins with the start-up producing a whitepaper, similar to a business plan, which provides details about a specific business or project, including aim of project, goods or services provided, and team's experience. Along with the details of the project, information on the ICO is also provided, such as amount of capital targeted, proportion of tokens made available and kept within the start-up, accepted currencies, and duration of the ICO.

ICOs can be treated as a mechanism to raise funds with just a "promise".

Typically, if the capital raised meets the target, then the project proceeds as stated in the whitepaper. Otherwise, money is returned to the investors and the ICO is deemed unsuccessful. However, this is simply a common practice, and is not always the case.

Even though both ICOs and Initial Public Offerings (IPOs) are aimed at providing public investments into companies, they have significant differences (see Figure 23).

FIGURE 23: DIFFERENCES BETWEEN ICO AND IPO

CRITERIA	ICO	IPO
STAGE OF COMPANY	• Typically young/seed company	• Well-established company
PURCHASE	• Access to service/proportion of ownership	• Proportion of ownership
RETURNS	• Based on performance of company	• Based on performance of company
LIQUIDITY	• Relatively difficult to find counterparties to buy or sell tokens	• Shares can be easily bought and sold through exchanges
REGULATION	• Very few, if any, regulations currently • Banned in certain countries	• Highly regulated for initial listing • Ongoing monitor

Source: Quinlan & Associates analysis

ICOs are relatively easy to conduct – a company simply needs to publish a whitepaper, detailing its aims, with an address to receive the funds – and are therefore favoured by companies during the seed stage, and even those with solely a concept and no working product or service. On the other hand, companies seeking an IPO need to satisfy different targets based on the jurisdiction, such as revenue, profit, cash flow, and market capitalisation requirements for a period of time (upwards of a year), and therefore tend to be well-established.

In terms of the purchase, investors are paying for ownership of the company in an IPO. However, there are different types of tokens investors can receive in an ICO. The two main types of tokens are utility tokens and equity tokens.

[45] To gain a deeper understanding of token sales, and their applications and implications, please read our upcoming thought leadership report on ICOs, which will be published in H1 2018

Utility tokens provide investors with access to services provided by the start-up company holding the ICO, after the project is operational, while equity tokens give investors ownership of the start-up company. One can consider utility token sales as early-bird or pre-order purchases, while equity token sales are more reflective of a digital version of IPO for the start-up. Utility tokens are currently more popular in ICOs. However, an increasing number of start-ups we spoke to stated that equity tokens will soon be the norm.

Due to the more established and facilitated nature of IPOs, liquidity of shares is considerably higher, and investors will find it easy to buy and sell their shares in the company. By contrast, ICOs are less well-known with fewer participants, meaning the tokens may not be as liquid as investors would expect, especially for less well-known token sales.

Some recent examples of successful ICOs include Ethereum, Filecoin, and Bancor, which raised USD 18.4 million,[46] USD 257 million[47], and USD 153 million[48] respectively. Filecoin aims to create a decentralised market for cloud storage, enabling renting or trading of excess storage space (using Filecoin tokens as the currency for transactions).[49] On the other hand, Bancor aims to facilitate the conversion of one type of Ethereum tokens to another, using the Bancor Network Token as an intermediate.[50]

However, there have been numerous joke or scam ICOs, which undermined investors' confidence in the ecosystem. For example, Confido raised nearly USD 375,000 through an ICO, claiming to use the capital to develop smart contracts which will act as escrows between counterparties. However, after the ICO, the Confido team disappeared, and the firm's online presence (including website, Twitter account, and Facebook page) was erased.[51] In addition, a joke token, Useless Ethereum Token, received over USD 200,000, despite being completely transparent and stating that investors are literally giving money 'to someone on the internet and getting completely useless tokens in return.'[52]

[46] Coindesk, 'Ethereum: Bitcoin Price Decline Created $9 Million Funding Shortfall', 28 September 2015, available at: https://www.coindesk.com/ethereum-bitcoin-decline-9-million-funding-shortfall/
[47] ICOBench, 'Filecoin', available at: https://icobench.com/ico/filecoin
[48] ICOBench, 'Bancor', available at : https://icobench.com/ico/bancor
[49] Filecoin, 'Filecoin: A Decentralized Storage Network', available at: https://filecoin.io/filecoin.pdf
[50] Bancor, 'Bancor Protocol', available at: https://www.bancor.network/static/bancor_protocol_whitepaper_en.pdf
[51] CNBC, 'Cryptocurrency start-up Confido disappears with $375,000 from an ICO, and nobody can find the founders', 21 November 2017, available at: https://www.cnbc.com/2017/11/21/confido-ico-exit-scam-founders-run-away-with-375k.html
[52] Useless Ethereum Token, available at: https://uetoken.com/

One does not need a working product, but simply a plausible concept, to conduct an ICO. As a result, there have been warnings from regulatory bodies about potential ICO scams, with several countries now paying more attention to the space. Despite ICOs being on a decentralised system, countries can restrict the activities within their jurisdiction. In fact, the Cyber Unit of the Securities and Exchange Commission (SEC) filed its first charges in the ICO space on 4 December 2017 against a company called PlexCorps, which raised USD 15 million from selling its tokens, PlexCoin, claiming that the investment would produce profits of over 1,300% within a month. Cyber Unit, on the other hand, said this 'hits all of the characteristics of a full-fledged cyber scam' and took action against PlexCorps.[53]

[53] Forbes, '$15 Million ICO Halted By SEC For Being Alleged Scam', 4 December 2017, available at: https://www.forbes.com/sites/laurashin/2017/12/04/15-million-ico-halted-by-sec-for-being-alleged-scam/#4f3a3fe31569

4. BANKS

Global investment banks, in general, have expressed concerns against Bitcoin, but are interested in the underlying technology, blockchain, as well as the potential developments and uses of cryptocurrencies (see Figure 24).

FIGURE 24: INVESTMENT BANKS' VIEW ON BITCOIN

BANK	PERSON	POSITION	VIEW ON BITCOIN
Goldman Sachs	**Lloyd Blankfein**	CEO	–
Morgan Stanley	**James Gorman**	CEO	–
J.P.Morgan	**Jamie Dimon**	CEO	✗
Bank of America Merrill Lynch	**Brian Moynihan**	CEO	✗
CREDIT SUISSE	**Tidjane Thian**	CEO	✗
UBS	**Sergio Ermotti**	CEO	✗
SOCIETE GENERALE	**Lorenzo Bini Smaghi**	Chairman	✗
SOCIETE GENERALE	**Severin Cabannes**	Deputy CEO	✗

✗ **Negative** – **Neutral** ✓ **Positive**

Source: Bloomberg, Quinlan & Associates analysis

Prominent figures that have criticised Bitcoin include the CEO of J.P. Morgan, Jamie Dimon, Credit Suisse's CEO, Tidjane Thiam, and the Deputy CEO of Société Générale, Severin Cabannes.

Jamie Dimon called Bitcoin 'a fraud'[54], that 'it's worse than tulip bulbs', and that he would 'fire in a second' any J.P. Morgan trader trading BTC. Jamie Dimon has since retracted his statement.[55]

Tidjane Thiam stated that 'the only reason today to buy or sell BTC is to make money, which is the very definition of speculation and the very definition of a bubble.'[56] Severin Cabannes said in an interview that 'Bitcoin today is […] very clearly in a bubble.'[57]

Lloyd Blankfein, Goldman Sachs' CEO, is one of the few with a relatively neutral view, saying he isn't 'willing to pooh-pooh it'.[58] In fact, Goldman Sachs seems to be the most enthusiastic bulge bracket regarding cryptocurrencies; as outlined in Section 2, the bank is looking to set up a trading desk to make markets in cryptocurrencies, in order to serve clients' interests in the market.[59] We expect a number of other investment banks to follow this move in 2018.

Despite the criticism against Bitcoin, the banking industry has openly expressed its support for – and interest in – blockchain, and has investigated, researched, and invested into related technologies to enhance its systems or service offerings.

Goldman Sachs has been reported to be one of the two (the other one being Google) most active corporate investors in blockchain companies.[60] J.P. Morgan set up an in-house Blockchain Center of Excellence to 'lead efforts for applications of distributed ledger technology within J.P. Morgan.' As of 11 August 2017, Bank of America has filed over 20 blockchain and cryptocurrency-related patent applications.[61] UBS is in a partnership with IBM to use blockchain technology for international transactions, and the initiative has been joined by other banks, including Bank of Montreal and Commerzbank.[62] Despite calling Bitcoin a bubble, Severin Cabannes said Société Générale is 'very keen to invest in the blockchain technology'.[63]

[54] CNBC, 'JPMorgan CEO Jamie Dimon says bitcoin is a 'fraud' that will eventually blow up' 12 September 2017, available at: https://www.cnbc.com/2017/09/12/jpmorgan-ceo-jamie-dimon-raises-flag-on-trading-revenue-sees-20-percent-fall-for-the-third-quarter.html
[55] CNBC, 'Jamie Dimon says he regrets calling bitcoin a fraud and believes in the technology behind it', 9 January 2018, available at: https://www.cnbc.com/2018/01/09/jamie-dimon-says-he-regrets-calling-bitcoin-a-fraud.html
[56] Bloomberg, 'Bitcoin Is the 'Very Definition' of a Bubble, Credit Suisse CEO Says', 2 November 2017, available at: https://www.bloomberg.com/news/articles/2017-11-02/bitcoin-is-very-definition-of-a-bubble-credit-suisse-ceo-says
[57] Bloomberg, 'SocGen Stokes Bitcoin Bubble Talk as Bank Eyes Blockchain', 3 November 2017, available at: https://www.bloomberg.com/news/articles/2017-11-03/bitcoin-is-very-clearly-in-a-bubble-says-deputy-socgen-ceo
[58] Bloomberg, 'Blankfein Says Don't Dismiss Bitcoin', 3 November 2017, available at: https://www.bloomberg.com/news/articles/2017-11-02/blankfein-says-don-t-dismiss-bitcoin-while-still-pondering-value
[59] Bloomberg, 'Goldman Is Setting Up a Cryptocurrency Trading Desk', 22 December 2017, available at: https://www.bloomberg.com/news/articles/2017-12-21/goldman-is-said-to-be-building-a-cryptocurrency-trading-desk?lipi=urn%3Ali%3Apage%3Ad_flagship3_feed%3BOJzKRFhFS7ypPySfHRb1cQ%3D%3D
[60] CNBC, 'Google and Goldman Sachs are two of the most active investors in blockchain firms: Report', 19 October 2017, available at: https://www.cnbc.com/2017/10/18/google-goldman-sachs-investors-blockchain.html
[61] Coindesk, 'Bank of America Has Filed for Over 20 Blockchain Patents Already', 11 August 2017, available at: https://www.coindesk.com/bank-america-filed-20-blockchain-patents-already/
[62] Coindesk, 'New Banks Join UBS-Backed Blockchain Trade Finance Platform', 4 October 2017, available at: https://www.coindesk.com/new-banks-join-ubs-backed-blockchain-trade-finance-platform/
[63] Bloomberg, 'SocgGen Stokes Bitcoin Bubble Talk as Bank Eyes Blockchain', 3 November 2017, available at: https://www.bloomberg.com/news/articles/2017-11-03/bitcoin-is-very-clearly-in-a-bubble-says-deputy-socgen-ceo

Some Bitcoin enthusiasts have argued that banks, as incumbents, have a vested interest in the traditional currency system and are therefore criticising Bitcoin, given they profit from transaction fees or commission fees during transactions, such as credit card .

payments and bank transfers. Nonetheless, banks will continue their research and investments in blockchain in order to incorporate the distributed ledger technology into their operations

5. EXCHANGES AND FUND MANAGERS

A handful of key financial institutions affected by cryptocurrencies and blockchain are exchanges, fund managers (asset managers and hedge funds), and venture capitalists. For a more comprehensive list on how different prominent figures view cryptocurrencies, please refer to the appendix (see Appendix C).

EXCHANGES

Some exchanges are currently operating or planning to launch cryptocurrency futures.

The first ones to gain approval from the US Commodity Futures Trading Commission (CFTC) were the Chicago Mercantile Exchange (CME Group) and Chicago Board Options Exchange (CBOE).[64] CBOE launched its Bitcoin Futures on 10 December 2017, and the CME Group launched its on 18 December 2017. Nasdaq has also expressed its intention to introduce Bitcoin Futures as early as Q2 2018.[65]

The price of CBOE's Bitcoin Futures is based on the price of BTC on Gemini,[66] a cryptocurrency exchange owned by the Winklevoss twins, while CME's is derived from the CME CF Bitcoin Reference Rate, which takes into account the BTC trading activities from a number of exchanges, including Bitstamp, GDAX, itBit, and Kraken.[67] One key feature of these Bitcoin Futures is that they are financially settled, providing exposure to the cryptocurrency without the need to own a digital wallet or the cryptocurrency itself, enabling those without the technical knowledge to participate in the market.

According to Greg Dwyer, BitMEX's head of business development, some major concerns regarding Bitcoin Futures include potential manipulations, DDoS (distributed denial-of-service), and potential hard forks.[68] For CBOE's Bitcoin Futures, the price is based on one cryptocurrency exchange which only represents a small portion of the Bitcoin market, and is therefore susceptible to manipulation by wealthy BTC holders. As discussed in Section 2, the system of the largest cryptocurrency exchange crumpled under intense traffic, and it is uncertain whether the cryptocurrency exchanges, which provide the reference for Bitcoin Futures, can operate during an organised DDoS attack. In addition, there is currently no clear guidance on how potential hard forks will be treated, leading to a level of uncertainty regarding settlement

.

[64] Bloomberg, 'Bitcoin Heads to Wall Street Whether Regulators Are Ready or Not', 1 December 2017, available at: https://www.bloomberg.com/amp/news/articles/2017-12-01/bitcoin-futures-to-start-trading-as-regulators-rush-to-catch-up
[65] Bloomberg, 'Nasdaq Plans to Introduce Bitcoin Futures', 30 November 2017, available at: https://www.bloomberg.com/news/articles/2017-11-29/nasdaq-is-said-to-plan-bitcoin-futures-joining-biggest-rivals
[66] CBOE, 'XBT-Cboe Bitcoin Futures', available at: http://cfe.cboe.com/cfe-products/xbt-cboe-bitcoin-futures
[67] CME, 'CME Bitcoin Futures Frequently Asked Questions', available at: http://www.cmegroup.com/education/cme-bitcoin-futures-frequently-asked-questions.html
[68] Business Insider, 'The 5 issues to consider before trading bitcoin futures', 14 December 2017, available at: https://amp-businessinsider-com.cdn.ampproject.org/c/s/amp.businessinsider.com/bitcoin-futures-price-cboe-cme-issues-2017-12

We spoke to Leonhard Weese, the President of the Bitcoin Association of Hong Kong, who believes that Bitcoin Futures 'show that Bitcoin is not inherently incompatible with the traditional financial world' and 'create hope that an ETF can be approved soon'.

Outside of the US, Australia is on track to have its own cryptocurrency exchange, The National Currency Exchange (NCX), in early 2018, which will trade well-known cryptocurrencies, such as BTC and Ether, and adding lesser-known cryptocurrencies and ICOs later in 2018.[69]

The introduction of futures, and potentially other derivatives and funds in the future, provides investors, both retail and institutional, with hedging tools for their BTC investments, and in some sense, legitimises Bitcoin's existence. If other cryptocurrencies gain popularity, it would not be surprising to see a further introduction of other derivatives.

FUND MANAGERS

Due to the potential upside of cryptocurrency investments, an increasing number of asset managers and hedge funds are joining the group of cryptocurrency enthusiasts.

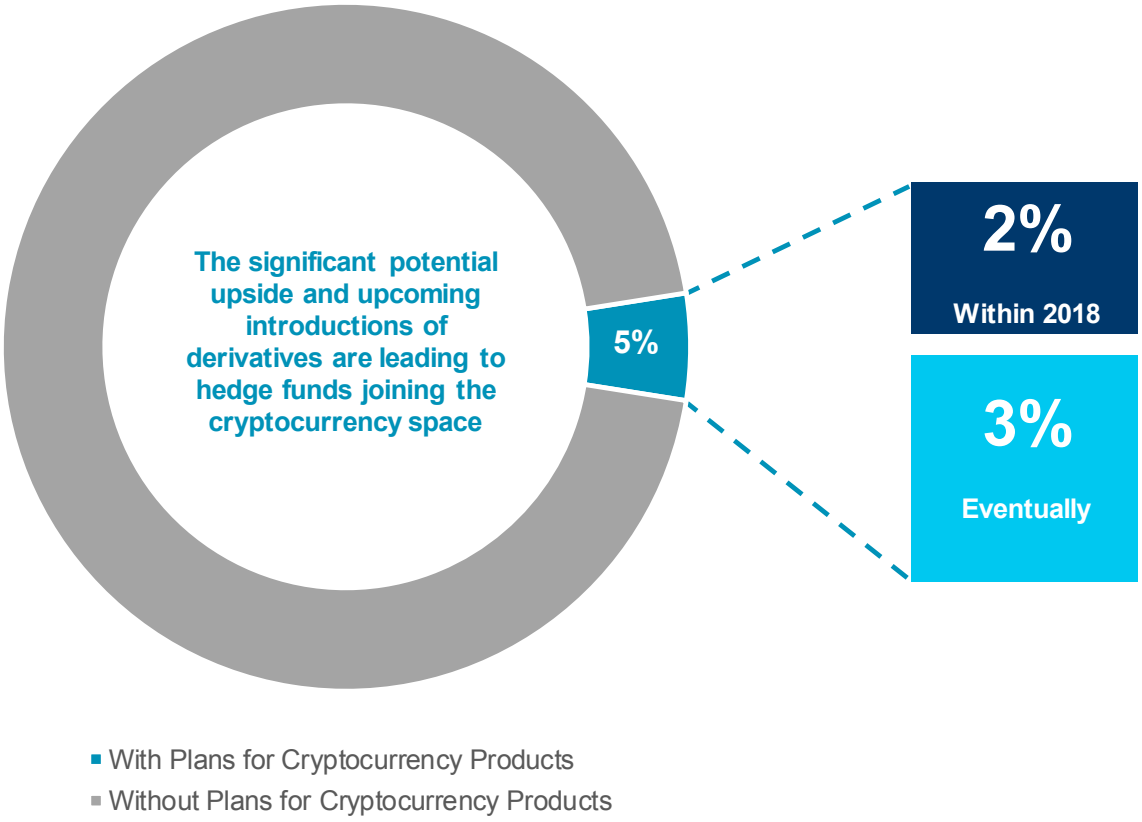
Tobam, a French asset management firm with USD 10 billion in assets under management (AuM), launched Europe's first BTC mutual fund in November 2017. The fund is classified as an alternative investment fund, and required the approval of Autorité des Marchés Financiers, the French financial regulator. In addition, Rafferty Asset Management and Exchange Traded Concepts shelved plans to launch Bitcoin ETFs in early 2018 amid concerns from the SEC regarding liquidity and valuations.[70] Nonetheless, this shows interests from fund managers to capitalise opportunities presented by cryptocurrencies.

By October 2017, there were over 120 hedge funds focusing on investing solely in BTC and other digital currencies.[71] It was reported that over 90 funds focusing on digital assets, such as cryptocurrencies and BTC, were launched in 2017, bringing the total to 124, with a combined USD 2.3 billion in AuM.

It was also reported that 2% of hedge fund managers are planning to launch cryptocurrency products in 2018, with a further 3% with plans to do so eventually (see Figure 25).[72]

[69] The West Australian, 'Perth tech firm to open Australian cryptocurrency exchange', 21 December 2017, available at: https://thewest.com.au/business/money/perth-tech-firm-to-open-australias-first-cryptocurrency-exchange-ng-b88697655z
[70] Reuters, 'Fund managers say bitcoin ETF proposals withdrawn due to SEC concern', 9 January 2018, available at: https://www.reuters.com/article/us-bitcoin-funds/fund-managers-say-bitcoin-etf-proposals-withdrawn-due-to-sec-concern-idUSKBN1EY045
[71] CNBC, 'There are now more than 120 hedge funds focused solely on bitcoin, digital currencies', 27 October 2017, available at: https://www.cnbc.com/2017/10/27/there-are-now-more-than-120-hedge-funds-focused-solely-on-bitcoin.html
[72] Preqin, '2018 Global Hedge Fund Report'

FIGURE 25: HEDGE FUNDS WITH PLANS FOR CRYPTOCURRENCY PRODUCTS



Source: Preqin, Quinlan & Associates analysis

Following the introduction of Bitcoin Futures, hedge funds are also able to bet against BTC, leading to bearish hedge funds joining in on the action. The most enthusiastic hedge funds have already sprung into action; BlackTower Capital was reported to have purchased USD 1 million worth of call options, which will expire in December 2018, providing it with the option to buy BTC 275 at USD 50,000 each.[73]

A number of managers see the explosive rise in cryptocurrency valuations as providing an opportunity to launch index products, offering considerable investment gains through beta capture alone. Two notable examples of such funds include Hong Kong-based CryptAM and Cryptomover. CryptAM provides a passive fund product, with the proportion of cryptocurrencies in its fund broadly based on their respective market capitalisations. It is also looking to

[73] Business Insider, 'We now know who was behind the $1 million bet that bitcoin will soar to $50,000', 22 December 2017, available at: https://amp-businessinsider-com.cdn.ampproject.org/c/s/amp.businessinsider.com/blocktower-capital-behind-1-million-bet-bitcoin-could-soar-to-50000-2017-12

develop active products. Cryptomover offers cryptocurrency index funds, with selection criteria including market capitalisation, liquidity, and trading history.

We spoke to Kevin Loo, co-founder of CryptAM, who told us they intend to focus on institutional clients over the longer term. However, most of their current clients include smaller family offices and High Net Worth Individuals (HNWIs). Only a few hedge funds have expressed interest, with long-only funds steering clear.

In terms of fees, CryptAM has a 2% management fee for their passive products and a "2 and 10" model for their active products. Understandably, some may believe that a 2% management fee for passive products and the pricing model for active products are unjustified, given traditional asset managers are facing significant price pressures. However, given the potential upside of cryptocurrency investments and rapid growth in demand for cryptocurrencies, Kevin Loo said that, given the current complexities of investing, he would not be surprised if fees for cryptocurrency asset managers actually increase in 2018.

With the introduction and continuous enhancements to the cryptocurrency infrastructure and ongoing clarifications from regulators, it is likely that more fund managers will be able to actively participate in the cryptocurrency market in coming years. Fund managers have also been experimenting with blockchain technology – for example, Vanguard is considering implementing blockchain in the process of updating index data for mutual funds, while BlackRock has experimented with using blockchain with its custodian bank clients.[74] We expect more institutions to make their way into cryptocurrencies from 2018 onwards.

[74] Reuters, 'Vanguard looks to blockchain for index data', 12 December 2017, available at: https://www.reuters.com/article/us-vanguard-group-blockchain/vanguard-looks-to-blockchain-for-index-data-idUSKBN1E61HR

VENTURE CAPITALISTS

As ICOs allow start-ups to raise capital through token sales, venture capitalists are finding themselves competing against this new fundraising trend. ICOs are relatively easy to conduct, and as current ICOs are prominently based on utility token sales, the start-ups do not lose ownership of their companies, in contrast to the traditional venture capital funding route.

ICOs have shifted power from venture capital firms to start-ups. Mangrove Capital Partners' partner, Michael Jackson, stated that '[t]his is going to turn arrogant venture capitalists on their heads' and that 'venture capitalists are going to have to enter into the ICO game to prove their value to companies'.[75] Traditionally, start-ups had to court venture capitalists for capital, which was a long, demanding, and tedious process. Now, start-ups are able to turn to the general public, which is arguably easier to coax, allowing them to focus their time and resources on more important aspects of the business.

Notwithstanding this, venture capitalists do provide a number of value-add services in addition to capital, such as strategic recommendations and/or operational support, as well as a level of confidence for the start-up (due to the rigorous due diligence process required to fund them). Co-founder of Index Ventures, Neil Rimer, stated that venture capitalists 'bring a lot of other help and advice' and thinks 'there will continue to be demand for that.'[76]

In addition, except in countries such as China and South Korea where ICOs are completely banned, ICOs remain largely unregulated, which means start-ups are able to spend relatively few resources on conducting ICOs. However, as the popularity of ICOs grows and more ICO scams emerge, regulators are likely to step in and implement more stringent compliance obligations, which will inevitably curb the interest in, and therefore the number of, ICOs. As such, despite challenging more traditional fundraising models, ICOs are unlikely to completely replace venture capitalists as a source of funding over the longer-term.

Besides ICOs, some venture capital firms are showing interest in cryptocurrency-related products and companies. For example, Founders Fund[77] (co-founded by Peter Thiel[78]) has invested in Metastable Capital, a cryptocurrency-focused hedge fund, and Polychain Capital, a hedge fund focusing on blockchain companies.[79] Given the promising applications of blockchain and the rise of cryptocurrencies, it is likely that more venture capital firms will be looking to join the space in coming years.

[75] Financial Times, 'Venture capital investors urged to wake up to ICOs', 3 October 2017, available at: https://www.ft.com/content/68c795ca-a680-11e7-ab55-27219df83c97
[76] Financial Times, 'Venture capital investors urged to wake up to ICOs', 3 October 2017, available at: https://www.ft.com/content/68c795ca-a680-11e7-ab55-27219df83c97
[77] Founders Fund's notable investments include Facebook, Airbnb, and Lyft
[78] Peter Thiel is a co-founder of Paypal
[79] The Wall Street Journal, 'Peter Thiel's Founders Fund Makes Monster Bet on Bitcoin', 2 January 2018, available at: https://www.wsj.com/articles/peter-thiels-founders-fund-makes-big-bet-on-bitcoin-1514917433

6. GOVERNMENTS AND REGULATORS

Governmental organisations, including central banks and financial regulators, have been paying close attention to BTC and other cryptocurrencies. Some of the major concerns regarding cryptocurrencies is their role in facilitating illegal transactions, money laundering, and tax evasion.

In the UK and Europe, multiple countries are considering a crackdown on BTC, and plan to regulate cryptocurrencies to ensure they are compliant with AML and CTF laws.[80] In addition, France Finance Minister, Bruno Le Maire, stated that he will propose discussions on BTC during the G20 summit in April 2018, to explore options for the regulation of cryptocurrencies.[81]

There are also concerns regarding tax implications on holding or trading cryptocurrencies, and there is a lack of indication on how cryptocurrencies are or should be taxed: as an asset, income, or capital gains. However, some tax regulators have already taken action. For example, the Indian government has initiated a probe against over half a million individuals who have BTC holdings, and stated that BTC are taxable assets and therefore gains from Bitcoin trading are taxable gains.[82] In the US, the new Republican tax bill means that cryptocurrency trading will be subject to taxation, starting from 1 January 2018.[83] South Korea has also announced plans to tax cryptocurrency trading gains, which is also a move by the government to curb the risk of excessive speculation.[84]

Moreover, due to the anonymised nature of cryptocurrency transactions, businesses can hide their actual revenue and income, and therefore pay less tax than they should.

To address such concerns, regulators are considering identity disclosure obligations, essentially ending anonymity of cryptocurrency transactions. In fact, the EU has agreed on requiring cryptocurrency exchange platforms and wallets service providers to identify users, which will be implemented and written into national laws within 18 months.[85] South Korea has also announced a ban on anonymous cryptocurrency accounts.[86] Some other potential regulations include restricting the use of cryptocurrencies as a payment method and completely banning cryptocurrencies.

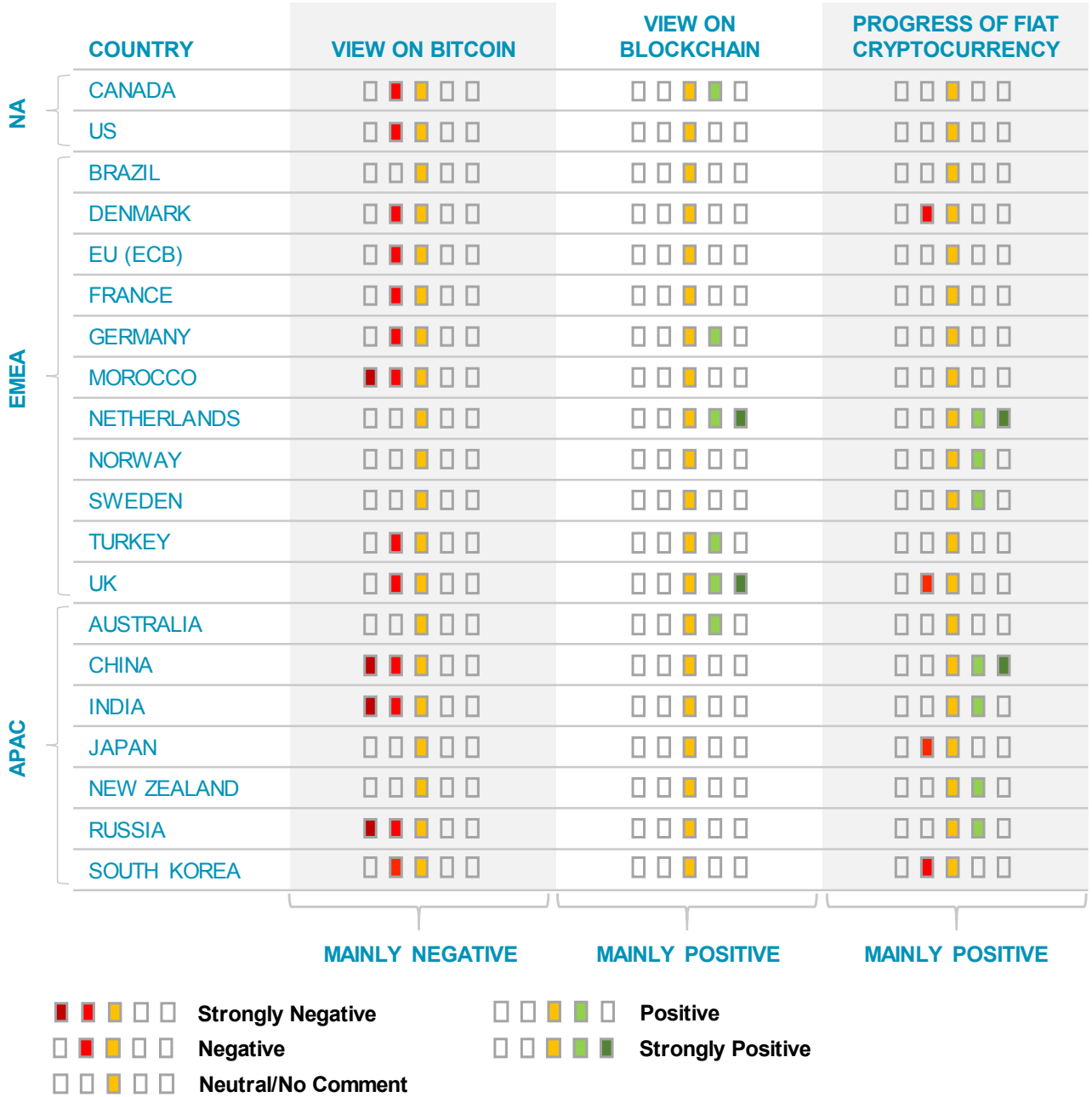
In addition, regulators are still debating how to classify cryptocurrencies, with some believing that cryptocurrencies should be a currency (which is typically regulated by the central bank) and others thinking that cryptocurrencies should be considered a security (which is typically regulated by the securities regulator).

Irrespective of their treatment, governments around the world have generally cautioned

[80] The Guardian, 'Bitcoin: UK and EU plan crackdown amid crime and tax evasion fears', 4 December 2017, available at: https://www.theguardian.com/technology/2017/dec/04/bitcoin-uk-eu-plan-cryptocurrency-price-traders-anonymity
[81] Reuters, 'French finance minister calls for bitcoin regulation debate at G20', 18 December 2017, available at: https://www.reuters.com/article/uk-markets-bitcoin-g20/french-finance-minister-calls-for-bitcoin-regulation-debate-at-g20-idUSKBN1EB0SZ
[82] Sputnik, 'Indian Tax Authorities Probe 500K Bitcoin Traders for Alleged Tax Evasion', 19 December 2017, available at: https://sputniknews.com/business/201712191060129734-indian-bitcoin-traders-evade-tax/
[83] Bloomberg, 'Tax-Free Bitcoin-to-Ether Trading in U.S. to End Under GOP Plan', 21 December 2017, available at: https://www.bloomberg.com/news/articles/2017-12-21/tax-free-bitcoin-to-ether-trading-in-u-s-to-end-under-gop-plan
[84] Reuters, 'South Korea to impose new curbs on cryptocurrency trading', 28 December 2017, available at: https://uk.reuters.com/article/uk-southkorea-bitcoin/south-korea-to-impose-new-curbs-on-cryptocurrency-trading-idUKKBN1EM05K
[85] Reuters, 'EU agrees clampdown on bitcoin platforms to tackle money laundering', 16 December 2017, available at: https://www.reuters.com/article/uk-eu-moneylaundering/eu-agrees-clampdown-on-bitcoin-platforms-to-tackle-money-laundering-idUSKBN1E928M
[86] Reuters, 'South Korea to impose new curbs on cryptocurrency trading', 28 December 2017, available at: https://uk.reuters.com/article/uk-southkorea-bitcoin/south-korea-to-impose-new-curbs-on-cryptocurrency-trading-idUKKBN1EM05K

investors against the potential cryptocurrency bubble (especially BTC), while expressing interest in blockchain technology (see Figure 26). A few countries that are more enthusiastic about the blockchain technology have indicated an intention to launch their own fiat cryptocurrency. For a more comprehensive list of view on cryptocurrencies by country, please refer to the appendix (see Appendix D).

FIGURE 26: COUNTRIES'/CENTRAL BANKS' VIEW ON CRYPTOCURRENCIES



Source: Bloomberg, Reuters, Telegraph, Quinlan & Associates analysis

Some of the countries that are strongly opposed to private cryptocurrencies are China (which has banned the Chinese population from trading cryptocurrencies and all ICOs), Morocco and India (where transactions involving cryptocurrencies are deemed as violations of law), and Russia (which referred to cryptocurrencies as 'pyramid schemes', and that Russia is 'totally opposed to private money').[87] A securities regulator we spoke to also said that monetary policy is a key tool of central banks, and that widespread adoption of private cryptocurrencies could interfere with its workings.

Despite this, most countries remain generally excited by the prospects of blockchain technology, citing reasons such as the ability of distributed ledger technology to enhance the financial system by making it more efficient, strengthening cybersecurity efforts, and enhancing payment methods. The most aggressive countries in experimenting with the blockchain system and exploring the concept of a fiat cryptocurrency include China, where a digital fiat money research team was set up in 2014, Netherlands, whose central bank created the DNBcoin in 2015 for internal use to gain an in-depth understanding of the technology, and New Zealand, which is evaluating the feasibility of replacing the New Zealand fiat currency with a digital alternative. In addition, we spoke to the Hong Kong Monetary Authority (HKMA), who indicated that they have commenced a research and a proof-of-concept work on the issuance of central bank digital currency over a distributed ledger technology network.

In the UK, the Bank of England (BoE) also considered a GBP-linked cryptocurrency,[88] but recently announced they would scrap such plans due to fears about its impact on the wider financial system, including an inability to maintain fiscal stability through the use of interest rates policies.[89]

Similar to banks, central banks are criticised by cryptocurrency enthusiasts as having a vested interest in rejecting BTC and its peers. Given that the power of central banks stems from the population's choice to believe in the government, and hence the central bank, to back up the value of fiat currency, a widespread adoption of decentralised cryptocurrencies will render central banks, and perhaps even governments, powerless.

Leonhard Weese believes that countries 'will be trying to restrict' private or decentralised cryptocurrencies, 'but with as much success as their attempts to restrict the flow of information around the internet [,] only very powerful and authoritarian states will dare, and only few of them [will] succeed.' However, unlike banks, governments and central banks have the ability, through legislation, to ban the use of current cryptocurrencies or enforce the adoption of fiat cryptocurrencies, which can be controlled by the government (e.g. through controlling all miners or through forcing hard forks).

Despite Bitcoin inspiring a revolutionary money system challenging the incumbent model, the promotion of a decentralised currency will likely be a struggle against governments, which rarely ends well for the counterparty (i.e. cryptocurrency enthusiasts).

[87] Bloomberg, 'Here's What the World's Central Banks Really Think About Bitcoin', 27 November 2017, available at: https://www.bloomberg.com/news/articles/2017-11-26/what-the-world-s-central-banks-are-saying-about-cryptocurrencies
[88] The Telegraph, 'Bank of England plots its own bitcoin-style digital currency', 30 December 2017, available at: http://www.telegraph.co.uk/news/2017/12/30/bank-england-plots-bitcoin-style-digital-currency/
[89] CryptoCoinsNews, Bank of England drops plans for its own cryptocurrency, fearing instability', available at: https://www.ccn.com/bank-of-england-drops-plans-for-its-own-cryptocurrency-fearing-instability/

SECTION 4

CRYPTOCURRENCIES: CURRENCY OR ASSET?

INTRODUCTION

Regulators have different viewpoints on cryptocurrencies, treating them as different concepts, such as currencies, commodities, or assets.

For example, the Financial Services Agency in Japan allows citizens to pay for goods and services with BTC,[90] treating BTC as a currency, while in US, the Commodity Futures Trading Commission said BTC is 'a commodity unlike any the Commission has dealt with in the past.'[91] The US Inland Revenue Service treats virtual currencies as 'property for US federal tax purposes',[92] effectively treating cryptocurrencies as assets.

In fact, as discussed in Section 3, currently available cryptocurrencies are generally not used as currencies, but as a financial asset.

This section explores whether a theoretically perfect cryptocurrency or existing cryptocurrencies can be treated as a currency and/or as an asset. We will mainly use BTC as an exemplar for current cryptocurrencies, given that it is arguably the most well-known and widely used cryptocurrency at present.

[90] Financial Times, 'Bitcoin gets official blessing in Japan', 18 October 2017, available at: https://www.ft.com/content/b8360e86-aceb-11e7-aab9-abaa44b1e130
[91] U.S. Commodity Futures Trading Commission, 'CFTC Statement on Self-Certification of Bitcoin Products by CME, CFE and Cantor Exchange', 1 December 2017, available at: http://www.cftc.gov/PressRoom/PressReleases/pr7654-17
[92] Inland Revenue Services, 'IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply', 25 March 2014, available at: https://www.irs.gov/newsroom/irs-virtual-currency-guidance

1. CRYPTOCURRENCY AS A CURRENCY

It is evident from the name that cryptocurrencies were created to be used as currencies, instead of investment assets.

In the envisioned world of cryptocurrency creators, where the general population has adopted cryptocurrency as the norm, cryptocurrency does generally better satisfy the three requirements of money: (1) unit of account, (2) medium of exchange, and (3) store of value, than known currencies, such as gold and fiat currency (see Figure 27). However, in the current environment, cryptocurrencies lack certain key characteristics or features, which makes them less desirable than fiat currencies.

FIGURE 27: CRYPTOCURRENCY AS A CURRENCY

		GOLD	FIAT CURRENCY	PERFECT CRYPTO	CURRENT CRYPTO
UNIT OF ACCOUNT	COUNTABLE	✓	✓	✓	✓
	DIVISIBLE	–	✓	✓	✓
	FUNGIBLE	✓	✓	✓	–
MEDIUM OF EXCHANGE	LIQUID	–	✓	✓	✖
	RECOGNISABLE	✖	✓	✓	–
	BACKING	✓	✓	✓	✖
	TRANSFERABLE (PHYSICAL)	–	✓	✓	–
	TRANSFERABLE (REMOTE)	✖	–	✓	✓
	COUNTERFEIT-PROOF	✓	–	✓	✓
STORE OF VALUE	DURABLE	✓	✓	✓	✓
	INHERENTLY VALUABLE	✓	✖	✖	✖
	STABLE	✓	–	✓	✖
	SECURE STORAGE	–	✓	✓	–

✖ Unfavourable – Dependent ✓ Favourable

Source: Quinlan & Associates analysis

UNIT OF ACCOUNT

A currency needs to act as a measure of worth, providing a numerical value for goods and services. To this end, the currency needs to be countable, divisible, and fungible.

COUNTABLE

A currency needs to be easily countable, providing numerical value to items and can undergo basic arithmetic operations (i.e. addition, subtraction, multiplication, and division). The value of goods and services can be measured in weight for gold, and numerical value for fiat currencies and cryptocurrencies.

DIVISIBLE

Related to the above criteria (i.e. countable), the currency itself needs to be able to be divided and combined without any loss in value.

Theoretically, if one splits a block of gold into smaller blocks, the total weights of these smaller blocks will equal the original weight. And if one melts these smaller blocks and combines them, it should result in a block of gold with the exact same weight as the original block. In practice, however, when gold is melted and reformed, some gold may be lost during the process, meaning gold is not perfectly divisible.

Fiat currency and cryptocurrency, on the other hand, can be divided and re-combined based on their numerical values, without any loss in value.

FUNGIBLE

A currency is fungible if any one unit is the same as any other one unit. One block of gold weighing 10 kilograms is exactly as valuable as any other block of gold weighing 10 kilograms (provided they are of the same purity). Similarly, any USD 10 banknote is valued at USD 10, just as any one unit of cryptocurrency should have the same value.

In reality, some cryptocurrencies are fungible, while others are not. The Bitcoin blockchain is public and transparent, and the history of each BTC can be traced and tracked. Some people may value certain BTC lower than others if they have been involved in illegal or grey-area transactions (e.g. the “dark web”), due to potential legal consequences.[93] For example, some cryptocurrency exchanges and wallets trace the history of each BTC, and freeze accounts if anything is associated with Silk Road.

Other cryptocurrencies, such as Monero, use various mechanisms to hide transaction details, making the history of any coin impossible to identify. These cryptocurrencies are fungible, while BTC is not.

[93] DecentralizeToday, ‘Bitcoin Fungibility: The Most Important Feature?’, 9 October 2016, available at: https://decentralize.today/bitcoin-fungibility-the-most-important-feature-of-bitcoin-4b87a381f21a

MEDIUM OF EXCHANGE

A currency needs to act as an intermediary in the system to facilitate trade, and this group of criteria is therefore highly related to the ease-of-use during daily transactions for goods and services.

LIQUID

A currency is liquid when a buyer can easily purchase goods and services with the currency and when sellers are willing to accept the currency as payment.

Currently, cash is one of the most liquid forms of currency. In the envisioned world of cryptocurrency creators, cryptocurrency will also be liquid.

However, even the most popular cryptocurrency, BTC, is hardly used to purchase goods and services. In fact, it was reported that out of the top 500 online merchants tracked by Internet Retailer (an eCommerce news and analytics publication), only three accept BTC.[94] Some people have argued that due to the majority of public not understanding the technology underpinning Bitcoin, they are reluctant to accept it as currency. However, it is arguably the case that the majority of the population does not understand the current money system, and yet they are still willing to accept cash and banknotes, which defeats the aforementioned argument.

RECOGNISABLE

To facilitate trade, a currency and its value need to be easily recognisable.

Even though one can recognise gold with relative ease, the exact weight of a block of gold is virtually impossible to determine at a glance. Conversely, fiat currency and cryptocurrency, and their associated values, can be identified easily, given their numerical nature.

In practice, cryptocurrencies are not recognised by everyone due to their short history, intangible nature, and a plethora of less well-known coins.

BACKING

People use certain currencies because the currency either has intrinsic value or is promised by a reliable entity to provide value.

Gold is backed by its own physical and chemical properties, aesthetics, and scarcity, while fiat currency is backed by a government, presumably a trustworthy party. Conversely, cryptocurrency is not backed by any organisation due to its decentralised nature, and is arguably backed by potential adoption (functional value) and its supposed scarcity. Due to the fact that current cryptocurrencies are rarely used to facilitate transactions, they are not backed by any utility or functional value.

TRANSFERABLE (PHYSICAL)

This criterion refers to local, face-to-face, transfer of the currency, as opposed to remote transfer or transactions (the next criterion).

Gold is arguably the most difficult to transfer physically, given its weight. Fiat currency can be transferred using banknotes or cheques, while cryptocurrencies can be transferred using an application, which are both very easy to do.

[94] Bloomberg, 'Bitcoin Acceptance Among Retailers Is Low and Getting Lower', 13 July 2017, available at: https://www.bloomberg.com/news/articles/2017-07-12/bitcoin-acceptance-among-retailers-is-low-and-getting-lower

In reality, however, the receivers of cryptocurrencies are recommended to wait for a certain period of time to confirm the transaction. Taking Bitcoin as an example, users are recommended to wait for six confirmations, or six blocks, which translates to one hour (given the current rate of 10 minutes per block), before accepting large payments. On the other hand, Ethereum aims to have a blocktime of under 20 seconds, while Ripple has a blocktime of ~3.5 seconds, meaning transaction confirmation is much quicker. However, this is still markedly slower than gold and fiat currency, given that the payment is confirmed the moment the payer hands the payee the gold or banknote.

TRANSFERABLE (REMOTE)

For remote transactions, such as cross-border trades, it is very impractical to use gold as a currency, given the time required to transfer and the potential for it to be lost and/or stolen. Fiat currency is the current norm, but this requires the service of a third party, such as a bank or payment service provider, such as Paypal.

Cryptocurrency has a strong edge over gold and fiat currency in this criterion, as the payers can simply send funds using their own private key and the payee's wallet address, without relying on a third party.

In this case, the confirmation time of cryptocurrencies can be quicker than that of fiat currencies. Cryptocurrency confirmation can be done in under an hour, while bank transfers may take several business days to complete.

COUNTERFEIT-PROOF

Currency needs to be impossible to counterfeit, or so difficult to counterfeit such that the cost of creating a counterfeit does not justify the operations.

Gold and cryptocurrency are virtually impossible to counterfeit, due to their unique characteristics and cryptography features respectively. On the other hand, counterfeit money is relatively common, and news of fake banknotes are not unheard of. Some fake banknotes have been of such high quality that they were accepted by not just common citizens, but also bank tellers on multiple occasions. In response, several governments have introduced new security features to their banknotes to make them harder to counterfeit.

STORE OF VALUE

A currency needs to retain its value over time, in order to retain purchasing power into the future for the holder. Therefore, the currency itself needs to be durable, without significant deterioration, and its value needs to stay relatively constant.

DURABLE

A currency has to tolerate wear and tear, and if it is unable to do so, its value needs to be retained somehow. Due to its chemical composition and structure, gold is chemically unreactive. Combined with its physical properties, gold is a highly durable material.

On the other hand, banknotes and paper money themselves are not very durable, and can be easily damaged. But in most cases, their value is retained, because the countries' central bank or note-issuing banks will replace damaged banknotes, provided a sufficient portion of the note remains. Therefore, even though the banknote itself is not durable, it does retain its value.

Cryptocurrencies are virtual, and hence do not suffer from wear and tear, or other damages, and are therefore highly durable.

INHERENTLY VALUABLE

A currency needs to have an intrinsic worth to back is value, in order for people to believe in the value it promises.

As discussed in the former criterion (BACKING), gold's inherent value stems from its physical and chemical properties, aesthetics, and scarcity. Fiat currency, represented by banknotes, are simply pieces of paper with special painting and patterns, and therefore have very low inherent value. However, fiat currencies are backed by supposedly trustworthy governments, such that people are willing to believe in their value.

Similarly, cryptocurrencies are not inherently valuable, as they do not have any extra features or uses that provide value, and cryptocurrency enthusiasts argue that cryptocurrencies are backed by potential adoption (which provides them with a function, and therefore value) and their supposed scarcity.

It is worth noting that despite scarce objects tending to be more valuable, scarcity alone does not provide value to the object. Scarce items, such as paintings by Vincent van Gogh, Leonardo da Vinci's manuscripts, and collector's edition toys, have other intrinsic value, such as aesthetics, cultural value, or nostalgic value, providing subjective worth, which is then inflated by scarcity.

Taking an example, one can create a token, named OneCoin, and make it indivisible and limiting its supply to one coin only. This OneCoin will be even more scarce than BTC, as there is only one of OneCoin and a supply limit of 21 million BTC. However, this coin will not be valued too highly given its lack of use or intrinsic value, and its scarcity alone is unable to provide it with any worth.

Currently with little acceptance during transactions and widespread use as a speculative asset, cryptocurrencies like BTC have virtually no function, and hence have little utility and value. This means that despite their scarcity, their intrinsic value is almost non-existent.

Note that new cryptocurrencies can be easily created, meaning there is no limit on the number of all cryptocurrencies; and despite some individual currencies having a cap, the cap can be increased through forks. These factors severely weaken the scarcity argument.

STABLE

Currencies that are stable in value are preferred to those whose value fluctuates widely, as stability provides confidence to the preservation of purchasing power.

Because gold has an inherent value, its worth can be derived based on its function relatively easily. In terms of fiat currency, its stability stems from the confidence people have in the government. In most cases and under normal circumstances, fiat currencies are relatively stable, though hyper-inflation is not unheard of during times of crisis or when people lose faith in their government.

In the world where cryptocurrency is widely used as a currency, its value should be relatively stable, as people believe in the value it promises. However, in reality, the stability of the value of different cryptocurrencies varies. In 2017, the value of BTC experience a near-parabolic rise, starting from ~ USD 1,000 at the beginning of the year to ~USD 13,000 by 31 December 2017, representing a 1,200% increase. As discussed previously (see Figure 21 – CRYPTOCURRENCY PARADOX), this rapid inflation of value leads to cryptocurrencies being unstable, such that they are rarely used for transactions.

In addition, in early 2018, when CoinMarketCap excluded data from South Korean cryptocurrency exchanges (where cryptocurrencies are priced at a 30% premium), this led to confusions in investors and a broad selloff.[95] Within the day, the total market capitalisation of cryptocurrencies fell by nearly 20%, with BTC price falling by nearly 10% and XRP price falling more than 30%.[96] An HKMA spokesperson told us that as current cryptocurrencies do not have any backing and their pricing is highly volatile, they do not qualify as electronic money.

Note that there are cryptocurrencies, such as Tether, which aim to be stable through backing the tokens by holding fiat currencies, such as USD, in a 1:1 rate in reserves. However, this requires users to place trust in the party holding the fiat currencies in reserves, defeating the purpose of eliminating a trustworthy party. In addition, this cryptocurrency is backed by USD, which is in turn backed by the US government. This means Tether is technically backed by the US government, albeit indirectly, and can be made redundant if the US government decides to issue its own fiat cryptocurrency (which is obviously backed by the US government itself).

SECURE STORAGE

The currency needs to be held in a secure place, for the holder to use it in the future.

Gold is relatively harder to store, simply due to its size and weight. Fiat currency can easily be stored in a bank or a safe, while cryptocurrency can be stored securely in a cryptocurrency wallet.

Despite this, there have been cases of theft of cryptocurrency, with one of the most famous incident being the theft from Mt. Gox (the largest Bitcoin exchange in 2014), which led to its liquidation. However, this is due to consumers allowing an online exchange to store their private key. If users keep their private keys confidential, such as by storing them offline or locally on a secure computer, the possibility of theft is extremely low.

[95] Reuters, 'Bitcoin slides as website drops South Korea prices from virtual currency rates', 8 January 2018, available at: https://www.reuters.com/article/uk-global-bitcoin/bitcoin-slides-as-website-drops-south-korea-prices-from-virtual-currency-rates-idUSKBN1EX1DB

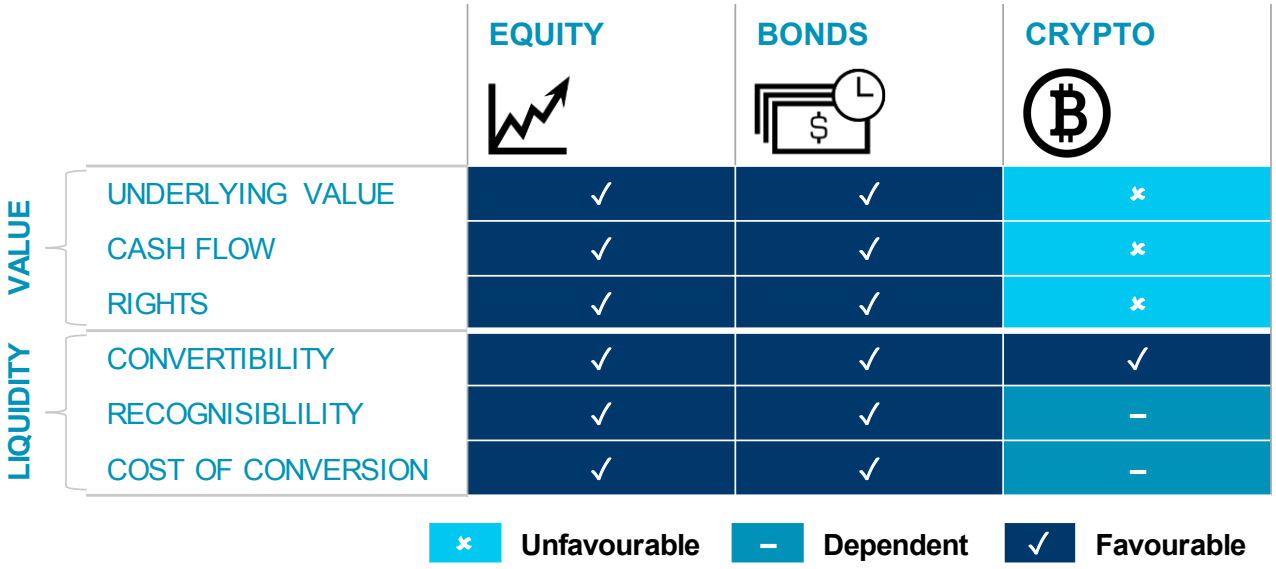
[96] CoinMarketCap, 'Cryptocurrency Market Capitalizations', available at: https://coinmarketcap.com/

2. CRYPTOCURRENCY AS A FINANCIAL ASSET

A financial asset is a resource whose value is derived from contractual claims. Unlike physical assets, such as properties and commodities, financial assets may not hold any physical value.

The two most common types of financial assets are equities and fixed income/bonds. The following discussion does not include a theoretically perfect cryptocurrency, as the intended use is as a currency, not a financial asset. Unsurprisingly, cryptocurrencies do not fare well against generally accepted criteria for assets (see Figure 28).

FIGURE 28: CRYPTOCURRENCY AS AN ASSET



Source: Quinlan & Associates analysis

VALUE

Value refers to the derivation of value of the asset. As financial assets do not have a physical worth, the value is derived from contractual claims, which are normally based on the underlying value of the claim, future cash flow, or contractual rights.

UNDERLYING VALUE

Equities represent a claim of ownership of companies, and therefore the underlying value is a proportion of the value of the company. Bonds are loans, are therefore the underlying value stems from the promise of repayment of the debt. As discussed previously, cryptocurrencies' value stems from their potential functionality, suggesting they have no underlying value.

CASH FLOW

Equities typically pay holders dividends while bonds pay holders interest coupons, providing them with a regular stream of cash flow. On the other hand, holders of cryptocurrencies gain no additional cash flow from their exposure.

RIGHTS

As equity holders own a proportion of the company, the owners have the right to vote and to share profit. Bond holders, on the other hand, gain the right to be compensated first during a company's liquidation and are prioritised to receive cash or securities first in the event of a re-organisation. Cryptocurrencies provide no extra rights, and therefore no value, to holders.

LIQUIDITY

The value of an asset is meaningless, unless the asset can be converted into money or other assets of equal value.

CONVERTIBILITY

All equities, bonds, and cryptocurrencies can be converted into money on respective exchanges or markets.

RECOGNISIBILITY

Equities and bonds have a long history, and are recognised by virtually everyone. On the other hand, cryptocurrencies are a new concept and, despite a sharp rise in media attention, are not widely-known or understood.

COST OF CONVERSION

In addition to convertibility, an asset is liquid if the cost of conversion (i.e. cost of purchase and cost of sale) is relatively low, such that it can be exchanged without a significant loss in value. For cryptocurrency exchanges, the cost of conversion is in line of equities' and bonds', typically ~0.2%. However, there are ways of cryptocurrency purchase and sale, such as Bitcoin ATMs, that charge upwards of 5% for transactions.

FROM SPECULATIVE ASSET TO LEGITIMATE CURRENCY

While cryptocurrencies are currently being used as speculative assets, they barely meet any basic criteria for being assets. On the other hand, current cryptocurrencies arguably meet more criteria for being currencies, with the theoretically perfect cryptocurrency being a better currency than today's most widely accepted fiat currencies. Despite this, they are not used as currencies.

The main challenge for current cryptocurrencies to be accepted as a currencies is their price instability. If the price of cryptocurrencies stabilises, they will become liquid, as the wider population and businesses will be willing to use them to facilitate transactions. This helps in making them recognised and provides cryptocurrencies with utility (i.e. functional value to back their worth). Gatecoin's William Piquard believes that the value of cryptocurrencies will stabilise once regulators step in to limit or restrict speculative activities, after which they will become mainstream.

It appears that the current situation can be summarised as, "no one knows its value because no one is using it to purchase goods and services, and no one uses it to purchase goods and services because no one knows its value". This is akin to the well-known joke, 'I don't have a job because I don't have experience, and I don't have experience because I don't have a job.'

We believe this cycle will only be broken when one party chooses to assume the risk of a first-mover (e.g. a company decides to take a leap of faith to hire someone without experience or the individual taking unpaid internships to gain experience). Similarly, the value of a cryptocurrency can be agreed upon if a significant proportion of users sacrifice the potential upside of value inflation, and spend the cryptocurrency on transactions for goods and services, providing a rough guide or standard to measure the value of a unit of the cryptocurrency. In this case, the value of the cryptocurrency will be agreed upon, encouraging businesses to accept them as payment, further enhancing the standard of value agreed upon. This would help to stabilise the value of the cryptocurrency, making it more liquid (and hence more widely accepted as a form of currency).

Note that other drawbacks of current cryptocurrencies as an effectively functioning currency (i.e. criteria that are unfavourable in the CURRENT CRYPTO column but favourable in the PERFECT CRYPTO column in Figure 27 – CRYPTOCURRENCY AS A CURRENCY), including fungible and secure storage, are easily solved. As previously mentioned, some cryptocurrencies, such as Monero and Dash, mask transaction details, and are therefore fungible. Secure storage can also be achieved through education while exercising diligence and care.

THE MAIN CHALLENGE FOR CURRENT CRYPTOCURRENCIES TO BE ACCEPTED AS A CURRENCY IS THEIR PRICE INSTABILITY

SECTION 5

IS BITCOIN A BUBBLE?

BTC PRICE RISE IN CONTEXT

As outlined in Section 4, although cryptocurrencies were originally designed to be used as currencies and not assets, cryptocurrencies are primarily used as speculative assets or investment vehicles.

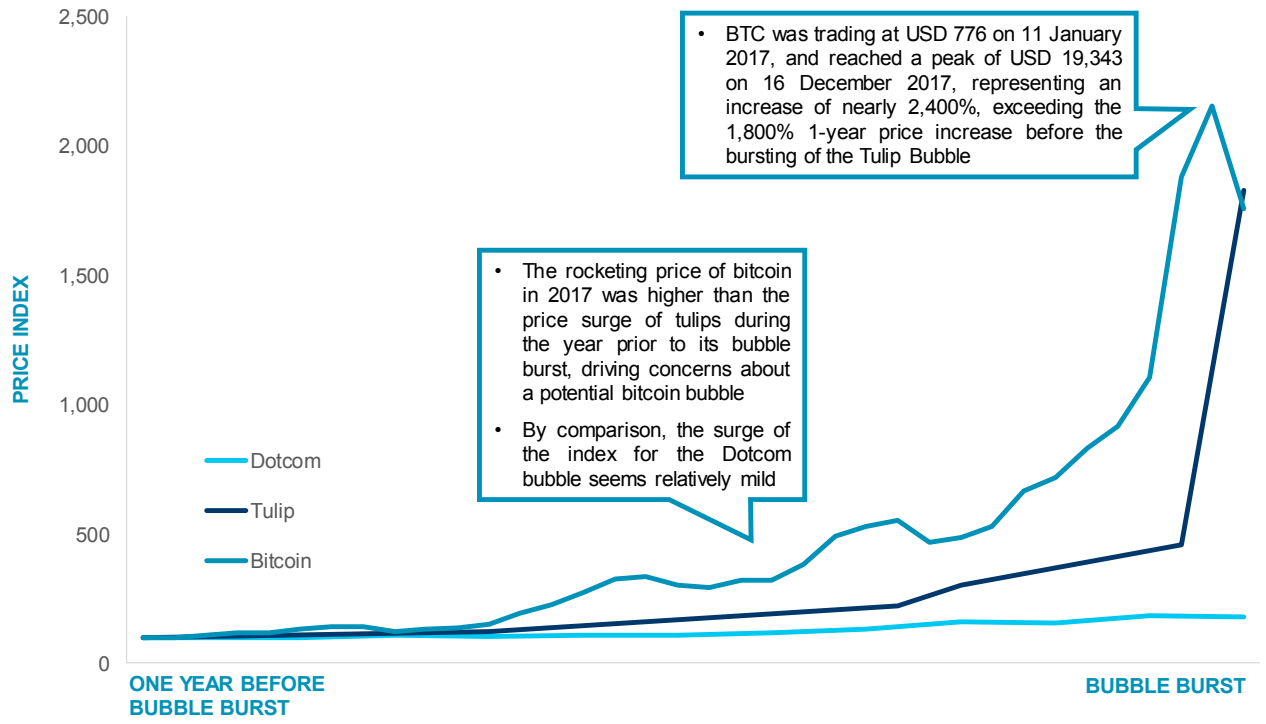
Because of the rapid surge in price of BTC, there have been numerous warnings about Bitcoin being a bubble from a range of stakeholders, including financial regulators, leading academics, and finance heavyweights. Even cryptocurrency business leaders, including Brian Armstrong, CEO of Coinbase (one of the largest cryptocurrency exchanges), told investors in December 2017 to 'invest responsibly.'[97] In fact, 55% of our survey respondents think that Bitcoin is a bubble, while 31% remain unsure (see Section 7).

A bubble occurs when an asset is traded at a price significantly higher than its value. Eventually, investors are unwilling to purchase the asset at this inflated price, leading to a massive sell-off and the price of the asset plummeting. Some famous examples of bubbles include Tulip Mania in the 17th century and the Dotcom Bubble at the turn of the millennium, with Tulip Mania having the largest asset price inflation (~1,800%) in the one-year period before its burst. However, the relative surge in the price of BTC during 2017 already surpassed that of the tulips one year before the tulip bubble burst (see Figure 29).

THE RELATIVE SURGE IN THE PRICE OF BTC DURING 2017 ALREADY SURPASSED THAT OF THE TULIPS

[97] CNBC, 'The Coinbase Founder sent a warning to bitcoin investors: 'Please invest responsibly'', 9 December 2017, available at: https://www.cnbc.com/2017/12/09/coinbase-ceo-sends-warning-to-bitcoin-investors-invest-responsibly.html

FIGURE 29: PRICE INDICES OF TULIPS, DOTCOM, AND BTC



Note bubbles are only identified after their burst, and therefore Bitcoin is not yet defined as a bubble, and its price index data is for 2017

Source: Nasdaq, Convoy Investments, Quinlan & Associates analysis

By comparison, the Dotcom bubble seems relatively insignificant, with the Nasdaq Composite Index increasing by less than 100% during the one-year period prior to its burst. However, unlike recent financial bubbles, the underlying asset, BTC, is not strongly correlated to or involved in other industries or the wider economy. Hence, if Bitcoin does burst, it will likely have less of a contagion effect – and associated impact – to the world economy when compared to other recent crashes, such as the 2008 Global Financial Crisis. Paul Donovan, Chief Economist at UBS Wealth Management, supports this view, saying that the damage will be 'spread quite thinly' if the bubble bursts.[98]

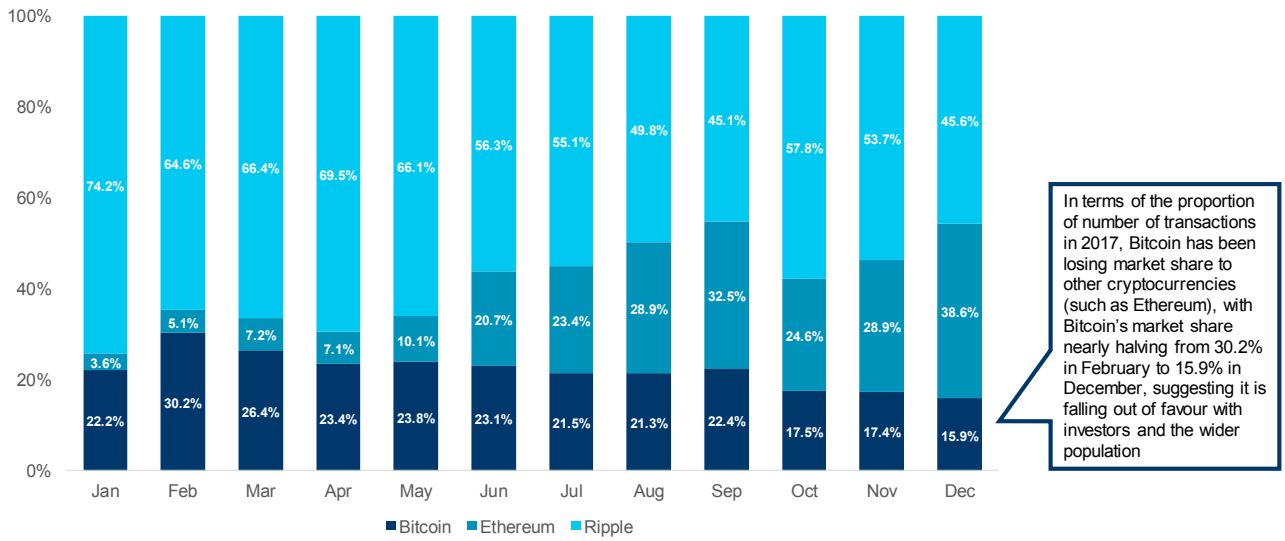
[98] CNBC, 'Bitcoin bubble could lead to 'destructive' consequences, UBS says', 12 December 2017, available at: https://www.cnbc.com/2017/12/12/bitcoin-bubble-destructive-consequences-ubs-says.html

Despite Bitcoin being, arguably, the most well-known cryptocurrency, its dominant status is mainly due to it having a first-mover advantage. There are other cryptocurrencies which function better as currencies, with shorter transaction time, lower transaction cost, or higher level of privacy, as well as blockchain systems with extra utility, such as Ethereum (facilitating a decentralised internet ecosystem) and Ripple (enhancing interbank and international payments). In fact, BTC is rapidly losing its market share, not just in terms of market capitalisation, but also in terms of number of transactions per day (see Figure 30).

Despite a number of pending upgrades to Bitcoin, such as the Lightning Network (which enhances its function as a currency) and MAST (which provides it with extra utility by enabling smart contracts), we believe Bitcoin will lag behind altcoins technologically. Without the founding entity guiding or leading upgrade discussions (such as Vitalik Buterin for Ethereum and Ripple Labs for Ripple), reaching consensus may be more difficult (this led to discussions of a hard fork caused by SegWit2x) and any change may take longer to be implemented – for example, Lightning Network was proposed in February 2015,[99] and is yet to be implemented as of January 2018. We therefore expect Bitcoin to be a technological laggard, leading to users and investors migrating to altcoins.

[99] Coindesk, 'Lightning, Duplex and the Search for Scalable Bitcoin Micropayments', 7 October 2015, available at: https://www.coindesk.com/lightning-duplex-scalable-bitcoin-micropayments/

FIGURE 30: NUMBER OF TRANSACTIONS FOR BITCOIN, ETHEREUM, AND RIPPLE



Source: Blockchain Luxembourg S.A., Etherscan, XRPcharts, Quinlan & Associates analysis

In addition, it was reported that the correlation between BTC price and other cryptocurrencies' price, including Ether's and Ripple's, has changed from strongly positive at 0.9 (from August 2015 to December 2017) to 0.1 for Ether and -0.6 for Ripple (in the final two weeks of 2017).[100]

Therefore, we believe the burst of the Bitcoin bubble will have a noticeable effect on similar cryptocurrencies (i.e. those without extra utility), but lessened effect on others. Subsequent to the bubble burst, we also feel users are unlikely to return to Bitcoin, given its relative weakness compared to technologically superior altcoins.

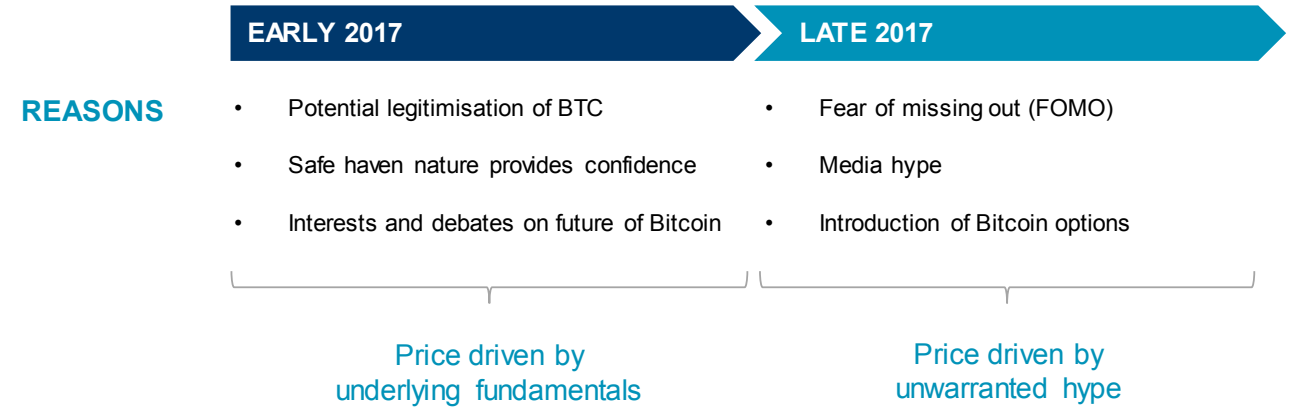
[100] Bloomberg, 'Second-Tier Crypto Coins Are Starting to Catch Up to Bitcoin', 4 January 2018, available at: https://www.bloomberg.com/news/articles/2018-01-03/bitcoin-loses-some-dazzle-as-second-tier-crypto-coins-catch-up

DRIVERS OF BTC PRICE (2017)

During early 2017 and late 2017, the underlying forces that were driving the surge in the price of BTC were markedly different (see Figure 31).

In early 2017, investors placed confidence in BTC due to the potential regulatory legitimisation of BTC and growing political uncertainty (i.e. BTC was seen as a relative safe haven, uncorrelated from all other asset classes). However, much of the rapid price surge that occurred in late 2017 was driven by a flood of investors rushing into BTC due to a fear of missing out ("FOMO"). And, as the mass market began to act irrationally, a bubble began to form.

FIGURE 31: DRIVERS OF BTC PRICE



Source: Quinlan & Associates analysis

EARLY 2017

In April 2017, Japan legitimised the use of BTC, allowing businesses to accept BTC as legal currency.[101] In addition, despite Russia being strongly against BTC, the country's Deputy Finance Minister, Alexey Moiseev, stated that authorities hope to recognise BTC and other cryptocurrencies in 2018, in order to enforce rules against illegal transfers.[102]

In addition to potential regulatory legitimisation, its properties as an investment asset were also being recognised. Brian Kelly, CEO of BK Capital Management, explained that BTC could be used 'as a hedge against political chaos'.[103] Due to its decentralised nature, BTC was seen as a safe haven against potential scandals in the US and Brazil in May 2017. The growing recognition of BTC as a currency, financial instrument, or safe haven asset, appears to have provided it with functional value.

[101] CNBC, 'Bitcoin value rises over $1 billion as Japan, Russia move to legitimise cryptocurrency', 12 April 2017, available at: https://www.cnbc.com/2017/04/12/bitcoin-price-rises-japan-russia-regulation.html
[102] Bloomberg, 'Russia Caves In on Bitcoin to Open Front on Money Laundering', 11 April 2017, available at: https://www.bloomberg.com/news/articles/2017-04-10/russia-caves-in-on-bitcoin-to-open-new-front-on-money-laundering
[103] CNBC, 'Bitcoin jumps to fresh record near $1,900 amid increased political risk', 18 May 2017, available at: https://www.cnbc.com/2017/05/18/bitcoin-jumps-to-fresh-record-near-1900-amid-increased-political-risk.html

The first half of 2017 saw a huge amount of debate and discussion surrounding the technology of Bitcoin, such as the scaling potential and transaction time, leading to growing interest and confidence in potential adoption, further driving up the price of BTC. Given the value in early 2017 appeared to be supported by actual usage or function of, as well as interest and confidence in, the cryptocurrency, one could argue the gradual and steady price increases were more reflective of BTC longer-term, underlying fundamentals.

LATE 2017

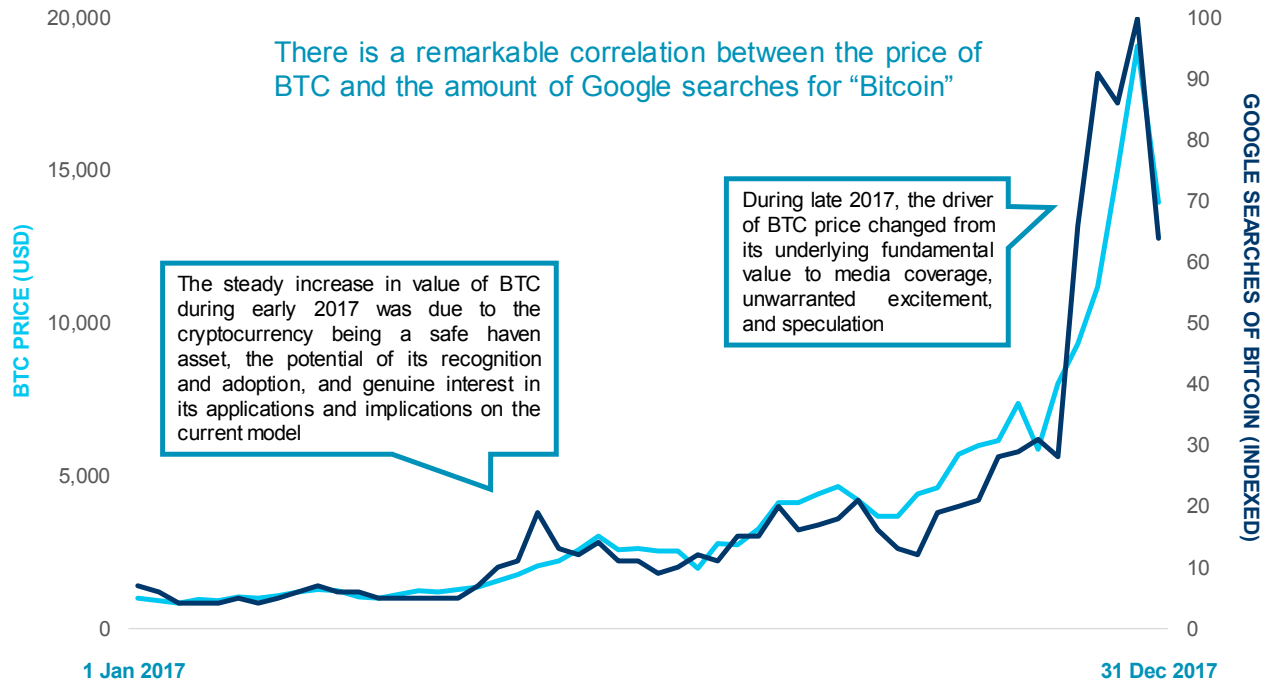
In late 2017, the rhetoric around BTC took a marked turn, with press coverage and social media posts on the soaring price of BTC leading to a flood of interest from retail and institutional investors alike.

One of the biggest examples of the craze was the renaming of an unprofitable, non-alcoholic beverage business (which arguably has nothing to do with cryptocurrencies and blockchain) from Long Island Iced Tea Corp to Long Blockchain Corp, after which it saw its share price rose as much as 289% on the day of its name change.[104] This example provides a clear example of how anything cryptocurrency or blockchain-related can attract significant hype, whether warranted or not, which is a tell-tale sign of a bubble.

Despite arguably not conducting sufficient research and analysis, retail investors are pouring into BTC due to FOMO and the potential price upside. In fact, BTC's price movements are highly correlated to the number of Google searches on Bitcoin (see Figure 32). This wave of retail interest has been exacerbated by the advent of Bitcoin ATMs (allowing retail investors to buy BTC in shopping malls and convenience stores etc.) and the fact that BTC is highly divisible (unlike a share, BTC 1 can be divided into 100,000,000 parts called satoshis), allowing the mass market with low levels of liquid assets to participate.

[104] Bloomberg, 'Long Island Iced Tea Soars After Changing Its Name to Long Blockchain', 21 December 2017, available at: https://www.bloomberg.com/news/articles/2017-12-21/crypto-craze-sees-long-island-iced-tea-rename-as-long-blockchain

FIGURE 32: BTC PRICE VS GOOGLE HITS



Note the number of Google searches is indexed to the week with the most searches (w/c 17 December 2017)

Source: Coindesk, Google, Quinlan & Associates analysis

While the number of Google searches is not 100% indicative of the level of hype or public excitement, it serves as a good proxy of the public's broader interest in BTC and how FOMO appears to be highly correlated with its price.

In addition to the rush of retail investors, institutions have been paying increasingly close attention to the cryptocurrency space. As mentioned in Section 3, just under 100 new funds focusing on digital assets were launched in 2017. The introduction of Bitcoin Futures by CBOE, CME, and potentially Nasdaq in Q2 2018, contributed to the recognisability of BTC, and attracted even more institutional money flow.

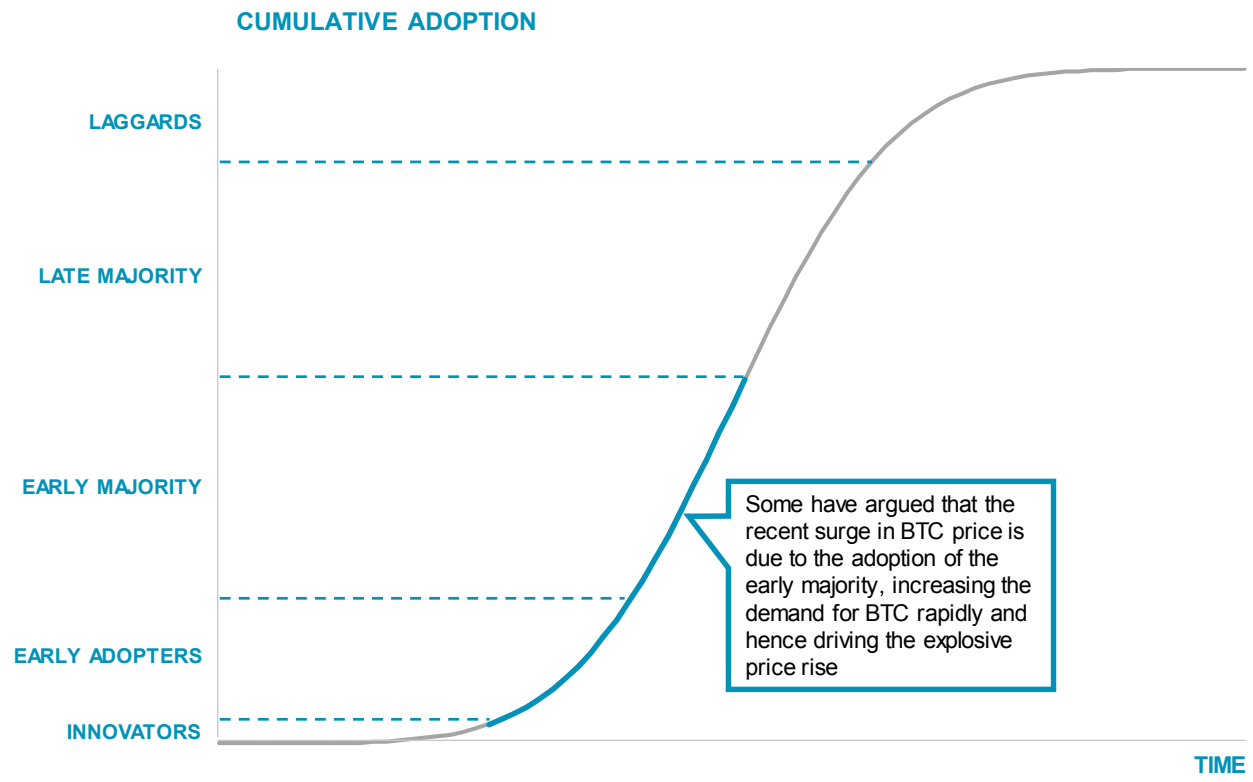
More traditional asset managers, especially long-only funds, are unlikely to invest in BTC, due to the lack of basis on which its value can be evaluated. On the other hand, hedge funds, HNWIs, and family offices, tend to be more interested in the opportunity, given their more speculative nature. Gatecoin's William Piquard said most of the institutional interest in recent months came from smaller family offices prepared to make more speculative investments, rather than institutions such as hedge funds with more established investment processes. Investment into BTC appears to be largely underpinned by hype and expectations of supernormal profits, rather than investors having an actual understanding of the potential usage of the cryptocurrency. As such, we believe that the price of BTC is likely to deviate from its true underlying value.

It is also worth noting that prior to the introduction of Bitcoin Futures, bearish investors had been unable to participate in the space. It is likely that this inability to short BTC further contributed to the cryptocurrency's largely one-way price hike throughout much of 2017.

TECHNOLOGY ADOPTION CURVE

Some have argued that the surge in BTC price in late 2017 is due to the population learning more about the cryptocurrency and starting to use it, and that the rate of adoption is increasing rapidly (see Figure 33).

FIGURE 33: BITCOIN ADOPTION ARGUMENT



Source: Quinlan & Associates analysis

According to the theory, as the proportion of the population using a new technology hits critical mass, the rate of adoption increases significantly as the early majority begin to use it. Given BTC's nature as a cryptocurrency, one must buy BTC to use it, meaning the increase in adoption led to greater demand for the cryptocurrency, driving its price higher. This can be explained by network effect, where the value of the BTC increases as the number of people adopting BTC increases, providing it with utility.

However, only three out of the top 500 online merchants tracked by Internet Retailer accept BTC.[105] Furthermore, conversations in online forums, such as Bitcoin forum and Reddit, highlight a general consensus of holding BTC as an investment asset, instead of using BTC for payments for goods and services, which has led to the saying “HODL” (i.e. hold on for dear life).

This suggests the rate of adoption for BTC as a form of payment is not increasing, rejecting the argument that the surge in price is caused by growth in its usage.

[105] Bloomberg, ‘Bitcoin Acceptance Among Retailers Is Low and Getting Lower’, 13 July 2017, available at: https://www.bloomberg.com/news/articles/2017-07-12/bitcoin-acceptance-among-retailers-is-low-and-getting-lower

MINSKY'S FIVE STEPS OF A BUBBLE

Economist, Hyman Minsky, proposed a 5-stage model of a bubble, namely: (1) displacement, (2) boom, (3) euphoria, (4) profit taking, and (5) panic (see Figure 34).

Stages 2 and 3 (boom and euphoria) happen during the boom stage of a bubble, while stages 4 and 5 (profit taking and panic) make up the bust stage of a bubble.

FIGURE 34: MINSKY'S 5-STAGE BUBBLE MODEL AND BITCOIN

		BOOM		BUST	
	DISPLACEMENT	BOOM	EUPHORIA	PROFIT TAKING	PANIC
DETAILS	• New product or technology comes into existence	• Interest level increases, along with significant media coverage, attracting participants/investors	• Greater fool theory applies • Investors try to buy the assets as quickly as possible	• Sophisticated investors notice warnings, leading to shorting or closing of positions	• Investors try to sell the assets as quickly as possible, at any price they can get
ASSET PRICE	• Typically low	• Increases slowly, and gains momentum	• Skyrockets	• Slightly decreases	• Plummets
TYPICAL BEHAVIOUR		• Public excitement • Constant media coverage	• Constant success stories • Justification theories	• Shorting and closing of positions ignored or ridiculed	• Panic and despair
BITCOIN	• Satoshi Nakamoto published Bitcoin whitepaper • Bitcoin software introduced	• Enthusiasts excited about potential adoption of Bitcoin • Daily media coverage on Bitcoin	• Stories on social media on rocketing wealth, and reasons why the Bitcoin bubble is not a bubble	• Smart money holding short positions through Bitcoin futures	• N/A
TIME	• 2009	• Early 2017	• Late 2017	• January 2018	• N/A

Source: Hyman Minsky, Quinlan & Associates analysis

The current situation for Bitcoin appears to mimic the Boom, Euphoria, and Profit Taking stages of Minsky's model.

BOOM

As discussed earlier (see earlier Section – DRIVERS OF BITCOIN PRICE), the gradual increase in BTC price in early 2017 appeared to be more reflective of its underlying fundamentals and investor confidence around its widespread adoption. However, as BTC price increased and repeatedly broke records, the media regularly reported about BTC and other cryptocurrencies, generating considerable public interest and excitement around the potential gains on offer.

EUPHORIA

In late 2017, the price of BTC surged from USD 4,950 on 1 September 2017 and touched USD 20,000 in December 2017 on some cryptocurrency exchanges (an increase of over 300%). One can easily read stories about sudden wealth and success stories through trading BTC on social media, such as Facebook, and even LinkedIn. On social media

and online forums, when comments challenged the price and value of BTC, they were often followed by theories and explanations justifying why BTC is not a bubble.

Note that a significant amount of vocal BTC supporters are also holders of BTC, meaning they have a vested interest in promoting the cryptocurrency. For example, Cameron Winklevoss, who is thought to be one of the largest BTC holders along with his twin brother, claimed on 10 December 2017 that BTC will rise as much as 20-fold.[106] During the euphoria stage, an investor needs a "greater fool", who is willing to purchase the asset at a higher price. It is, of course, quite natural that BTC holders talk up the cryptocurrency to encourage others to participate and purchase it at a high price.

It is important to note that the increase in BTC price (over 300% within three months from September to December 2017) is significantly higher than the surge in the Nasdaq Composite Index three months before the crash of the Dotcom Bubble (the index increased by ~25% from ~4,000 to ~5,000 from January to March 2000, the 3-month period before the bubble burst). It also exceeds that of the Tulip Mania in 1637 (there is no detailed price data, but tulip prices were indexed at just over 100 in December 1636 and just under 200 in February 1637 when the bubble burst, which is just shy of a 100% increase).

PROFIT TAKING

It was reported that during the first week of 2018, the big players in Bitcoin futures at CBOE (defined to be those holding more than 25 contracts, and likely to be institutional investors) primarily held short positions. CFTC data also showed that hedge funds and money managers placed 40% more short bets than long bets.[107] However, some have argued that these investors are simply hedging against a price fall, and the short positions do not indicate an expectation for the crash of Bitcoin. Nonetheless, these behaviours are remarkably similar to the Profit Taking stage of Minsky's framework.

While much of the analysis in this section indicates the price of BTC is indeed a bubble, we believe a more robust conclusion can only be made from better understanding its true underlying value.

'YOU KNOW IT'S TIME TO SELL WHEN SHOESHINE BOYS GIVE YOU STOCK TIPS. THIS BULL MARKET IS OVER.' – JOSEPH PATRICK KENNEDY SR.

---

[106] Bloomberg, 'Bitcoin Billionaire Winklevoss Sees Surge of as Much as 20 Fold', 10 December 2017, available at: https://www.bloomberg.com/news/articles/2017-12-09/a-winklevoss-sees-bitcoin-surging-as-much-as-20-times-higher
[107] The Wall Street Journal, 'Little Guys and Big Trading Firms Square off in Bitcoin Futures Arena', 7 January 2018, available at: https://www.wsj.com/articles/little-guys-and-big-trading-firms-square-off-in-bitcoin-futures-arena-1515326400

SECTION 6

VALUING BTC

MARKET PREDICTIONS

The current situation, both in terms of BTC price and behaviour of the population, appears to fit with Minsky's model of a bubble. However, simply because a situation fits with a model does not mean it will evolve according to the model.

If one can determine the value of BTC 1, then one can identify whether Bitcoin is a bubble by comparing its value with the current BTC price. In fact, quite a few figures within the cryptocurrency space have tried to predict the future price of BTC 1 (see Figure 35 and 36).

FIGURE 35: BTC PRICE PREDICTIONS (TABLE)

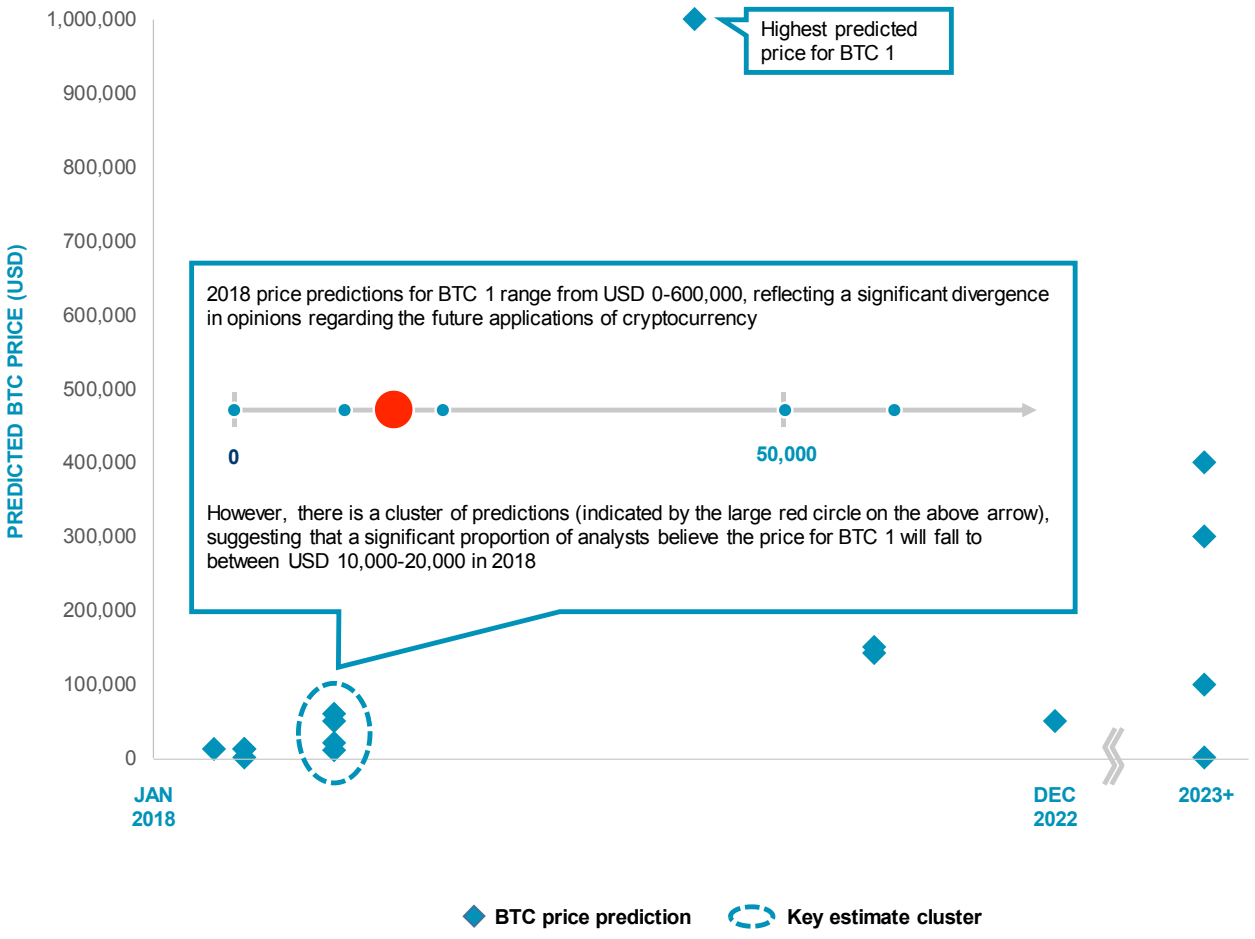
NAME	ROLE	FIRM	DATE OF PREDICTION	PRICE AT PREDICTION (USD)	PREDICTION FOR	PREDICTED PRICE (USD)
James Faucette	Analyst	Morgan Stanley	25 Dec 2017	13,917	N/A	0
Michael Novogratz	Manager	Fortress Hedge Fund	23 Dec 2017	14,549	Dec 2018	50,000
Dhaval Joshi	Chief European Investment Strategist	BCA Research	21 Dec 2017	15,561	Apr 2018	12,750
Victor Dergunov	Founder	Albright Investment Group	18 Dec 2017	18,961	2022	50,000
Ronnie Moas	Founder	Standpoint Research	17 Dec 2017	19,086	All time high	300,000
Jordan Hiscott	Chief Trader	Ayondo Markets	16 Dec 2017	19,343	End of 2017	20,000
Michael Bryant	Contributor	SeekingAlpha	10 Dec 2017	15,037	2021-2027	142,000
Marc van der Chijs	Founder	First Block Capital	8 Dec 2017	16,057	2021	150,000
John Hardy	Head of FX Strategy	Saxo Bank	7 Dec 2017	16,858	Peak of 2018	60,000
Mark Yusko	Founder & CIO	Morgan Creek Capital Management	6 Dec 2017	13,709	All time high	400,000
David Drake	Founder & Chairman	LDJ Capital	29 Nov 2017	9,816	2018	20,000
James Altucher	Managing Director	Formula Capital	29 Nov 2017	9,816	2020	1,000,000
John McAfee	CEO	MGT Capital Investments	29 Nov 2017	9,816	2020	1,000,000
Jerry Brito	Founder & Executive Director	Coin Center	27 Nov 2017	9,739	Nov 2017	10,000
Shane Chanel	Adviser	ASR Wealth Advisers	27 Nov 2017	9,739	Mid 2018	12,000
Tom Lee	Managing Partner & Head of Research	Fundstrat Global Advisors	22 Nov 2017	8,231	Mid 2018	11,500
Sheba Jafari	Technical Head	Goldman Sachs	6 Nov 2017	6,958	Dec 2017	8,000
John Spallanzani	Chief Macro Strategist	GFI Group	21 Aug 2017	4,055	2018	10,000
Paul Veradittakit	Vice President	Pantera Capital Managementt	21 Aug 2017	4,055	Dec 2017	6,000
Roy Sebag	Founder & CEO	Goldmoney	21 Aug 2017	4,055	Foreseeable future	0
Kay Van-Petersen	Analyst	Saxo Bank	31 May 2017	2,330	2027	100,000

Note James Faucette did not give a target price, and was commenting on the real value of BTC

Note that the price at prediction is based on the 00:00 price on the date listed on Coinbase, and not the price at the moment of prediction

Source: CNBC, Bloomberg, Business Insider, CNN, Fortune, CCN, The Motley Fool, Seeking Alpha, Express, Coinbase, Quinlan & Associates analysis

FIGURE 36: BTC PRICE PREDICTIONS (SCATTER)



Source: CNBC, Bloomberg, Business Insider, CNN, Fortune, CCN, The Motley Fool, Seeking Alpha, Express, Coinbase, Quinlan & Associates analysis

Most individuals were rather vague in their rationale behind their BTC price predictions, with some of the quoted reasons including increasing interest from traders and mainstream finance, as well as limited supply.

An arguably more well-thought-out reasoning came from Kay Van-Petersen, an analyst at Saxo Bank, who valued BTC based on the factors including percentage of average daily volumes of fiat currency, the relationship between market capitalisation and the average daily volumes, and the supply of BTC a decade from now.[108]

Nonetheless, there are huge discrepancies regarding BTC future price estimates, which is unsurprising due to considerable uncertainty surrounding its potential adoption and usage.

THERE ARE HUGE DISCREPANCIES REGARDING BTC FUTURE PRICE ESTIMATES, DUE TO CONSIDERABLE UNCERTAINTY SURROUNDING ITS POTENTIAL ADOPTION AND USAGE

[108] CNBC, 'Bitcoin could hit $100,000 in 10 years, says the analyst who correctly called its $2,000 price', 31 May 2017, available at: https://www.cnbc.com/2017/05/31/bitcoin-price-forecast-hit-100000-in-10-years.html

OUR VALUATION OF BTC

AS AN ASSET

Given the fact that BTC is mainly used as an investment asset at present, one obvious way to value BTC would be the discounted cash flow valuation method (DCF). However, given that BTC does not provide holders with any cash flow (unlike dividends from equities and interest coupon payments from bonds), this would suggest an underlying value of zero.[109]

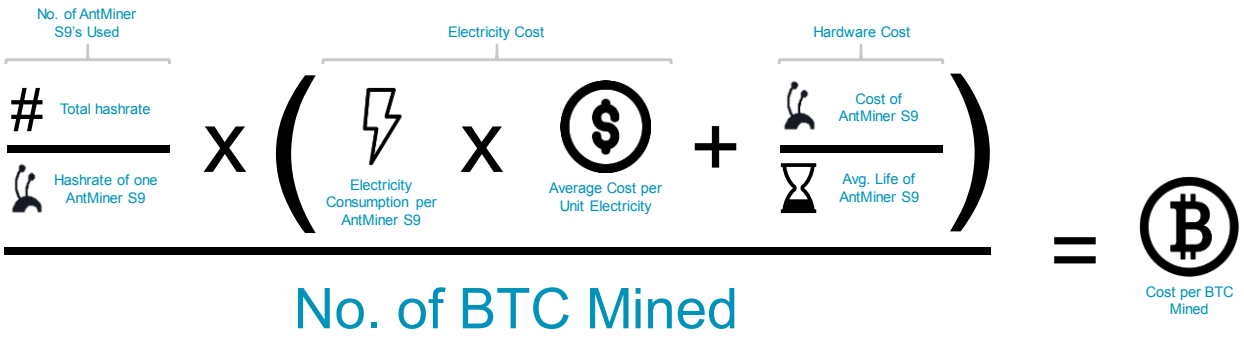
However, given the value of an asset like gold (which also offers no cash flows), using a DCF valuation methodology is obviously flawed.

We therefore employed two methods to determine the value of BTC 1 as an asset, namely: (1) cost of production and (2) store of value.

COST OF PRODUCTION

By considering the cost of mining, including electricity cost and hardware cost, and the block reward available to miners, one can calculate the current cost of mining BTC 1 (see Figure 37). Note that our calculations are based on the AntMiner S9, which is one of the most efficient ASICs at present (in terms of hashrate per unit electricity).

FIGURE 37: CALCULATION OF COST PER BTC MINED



Note that we incorporated indirect costs such as rent, equipment upgrades/maintenance costs, through adding a 30% profit margin.

Source: Quinlan & Associates analysis

[109] Using the DCF model gives: $\mathrm{DCF} = \sum_{i=0}^{\infty} \frac{\text{Cash Flow}_i}{(1+\text{Discount Rate})^i} = \sum_{i=0}^{\infty} \frac{0}{(1+\text{Discount Rate})^i} = 0$

The AntMiner S9 provides a hashrate of 13.5 TH/s,[110] with a power consumption of 1323W (+10%).[111] The average total Bitcoin hashrate throughout 2017 was ~6 million TH/s,[112] indicating that ~446,000 AntMiner S9s were used during the year, translating to a total power consumption of ~5.68 billion kWh.

As mining pools provide close to 100% of the hashrate, by considering the location or origin of these pools and calculating the weighted average for electricity cost,[113] we found that the average cost of electricity for mining is ~USD 0.085 per kWh for 2017. Note that the electricity cost is heavily skewed towards the Chinese figure, USD 0.09 per kWh,[114] due to mining pools in China contributing to nearly 80% of the total hashrate. This translates to a total electricity cost of ~USD 484 million for all mining activities and a cost of USD 737 per BTC mined in 2017.

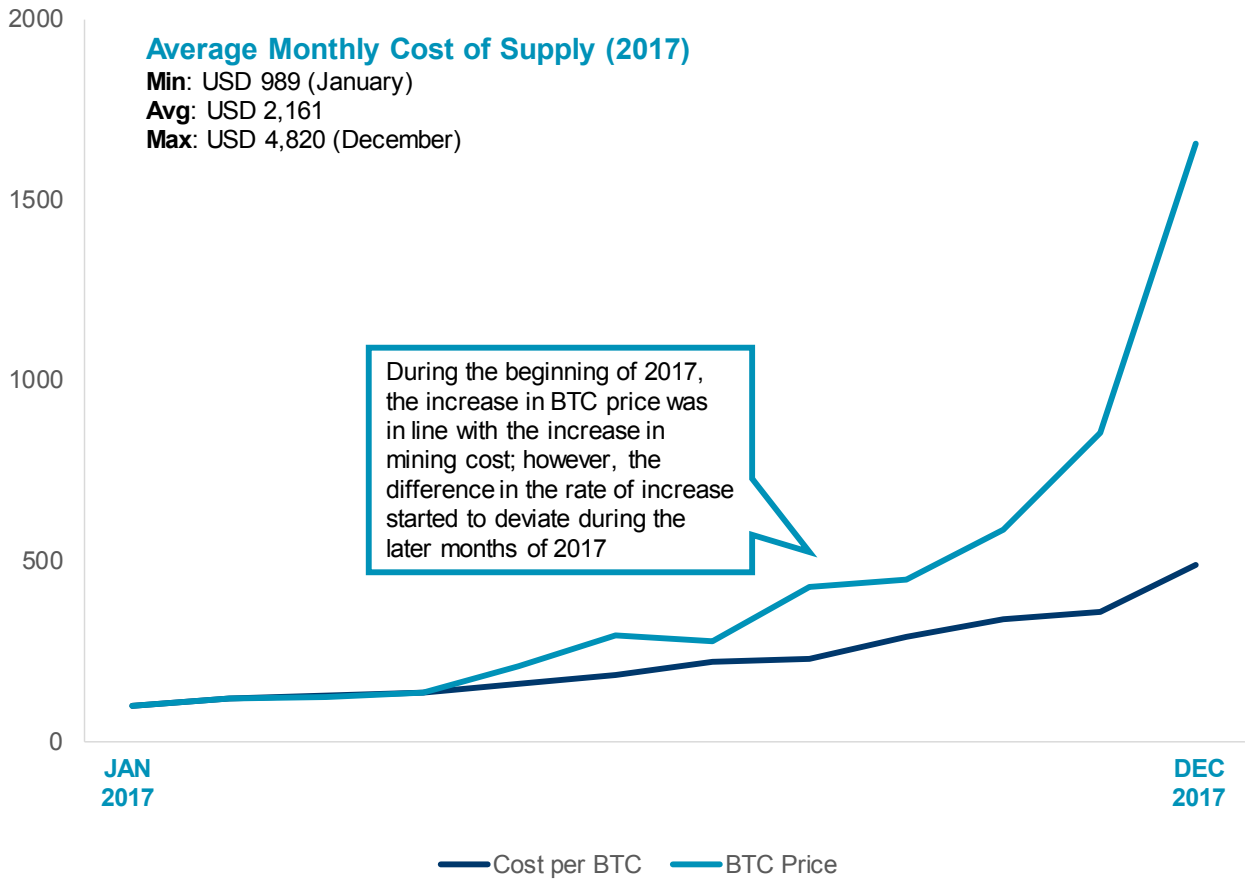
Besides operations cost (i.e. the electricity cost of running AntMiner S9s constantly), the major cost is the cost of the AntMiner S9 or cost of the hardware. The AntMiner S9 is quoted at USD 2,725 on Bitmain.[115] Assuming an average lifespan of two years, the total cost of AntMiner S9s per year is ~USD 608 million, or USD 925 per BTC mined in 2017.

Totalling these figures gives a cost of USD 1,662 per BTC mined in 2017. Assuming miners expect a profit margin of 30% (to cover rent, equipment maintenance, etc.), the cost to supply BTC 1 was, on average, USD 2,161 in 2017.

[110] Hashrate is the rate of computation, with 1 TH/s meaning 1 trillion hashes per second
[111] Bitmain, 'AntMiner S9', available at: https://shop.bitmain.com/antminer_s9_asic_bitcoin_miner.htm?flag=specifications
[112] Blockchain Luxembourg S.A., 'Hash Rate', available at: https://blockchain.info/charts/hash-rate
[113] Weighted Average of Electricity Cost = $\sum_{\text{Country}} \frac{\text{Hashrate Contributed by Mining Pools}}{\text{Total Hasrate}} \times \text{Electricity Cost}$
[114] Statista, 'Global electricity prices by select countries in 2017', available at: https://www.statista.com/statistics/263492/electricity-prices-in-selected-countries/
[115] Bitmain, 'Antminer S9-13.5TH/s', available at: https://shop.bitmain.com/productDetail.htm?pid=00020171219125505438 8vvfMz1v06F0

Using a similar method, we identified the average cost of mining BTC 1 for each month in 2017, and plotted the data against the average price of BTC 1 for the month (see Figure 38).

FIGURE 38: COST OF BTC VS BTC PRICE IN 2017



Note that the data values are indexed to January 2017

Source: Blockchain Luxembourg S.A., Bitmain, CoinDesk, Quinlan & Associates analysis

By indexing the values to those in January 2017, it is clear that the increase in BTC price was in line with the rise in mining costs for the earlier part of the year. However, as the year progressed, the price of BTC increased significantly (~16.5x) relative to the cost of mining (~5x, from USD 989 to USD 4,820) from January to December 2017.

This can be attributed to the fact that the cost of mining only reflects new BTC production while the price of BTC takes into account all BTC in existence. In addition, the value of BTC won't be determined solely by the cost of supply; demand considerations must also be taken into account.

The majority of mining pools currently operate in China. However, the Chinese government has plans to clamp down on the mining industry in the country, through limiting electricity usage and guiding an orderly exit. Some mining pools are considering moving operations to other countries, including Canada, Iceland, and US.[116] Given that most of these target countries have higher electricity costs than China, the cost of mining will increase. However, given the current value of BTC and the sizeable profit margins on offer at present to miners, the increase in cost is unlikely to discourage new miners from entering the industry in the short-term.

[116] Bloomberg, 'Bitcoin Miners Are Shifting Outside China Amid State Clampdown', 5 January 2018, available at: https://www.bloomberg.com/news/articles/2018-01-05/bitcoin-miners-are-shifting-outside-china-amid-state-clampdown

Analogies can be drawn between gold mining and Bitcoin mining, and some have argued that a similar valuation method can be used. However, despite there being similarities between them, a key difference is that the probability of any gold miner finding gold is constant and independent of the number of total miners, while the probability of a Bitcoin miner finding the golden nonce changes with the total hashrate which is affected by the number of Bitcoin miners (see Figure 39). In fact, if the number of gold miners doubles, one can expect the rate of finding gold to double, while for BTC, the number of BTC mined will stay constant (at BTC 12.5 per 10 minutes until 2020) regardless of the number of Bitcoin miners.

FIGURE 39: ILLUSTRATIVE COMPARISON BETWEEN GOLD MINING AND BITCOIN MINING

	GOLD MINING	BITCOIN MINING
		
EQUIPMENT USED	• Shovel	• AntMiner S9
MINING POWER	• 10 shovels per minute	• 10 hashes per minute
PROBABILITY OF SUCCESS	• Constant	• Varies depending on total hashrate
DETAILS	• The probability of hitting gold per shovel does not change, as the gold mine does not increase its difficulty in locating gold, no matter how many shovels there are	• The probability of obtaining a nonce per hash changes depending on how many AntMiners there are, as the Bitcoin protocol increases the difficulty according to the hashrate

Note the figures are changed for illustrative purposes

Source: Quinlan & Associates analysis

To put this simply, imagine a 10 x 10 grid (i.e. 100 tiles), with the gold or golden nonce hidden under 1 tile, hence there is a 1% chance of success for each shovel or hash.

For gold mining, if there is one miner, it will take 10 minutes on average to find the gold (assuming a rate of 10 shovels per minute). If there are two miners, the time required on average to hit gold will halve, to 5 minutes. The rate of finding gold increases accordingly with the increase in number of miners.

On the other hand, if there is only one Bitcoin miner, it will take 10 minutes, on average, to find the golden nonce (assuming a rate of 10 hashes per minute). However, if the number of miners doubles (which doubles the hashrate, assuming all miners have the same mining power), the algorithm doubles the difficulty of finding the golden nonce. Instead of a 10 x 10 grid, the system now requires the miners to mine on a 10 x 20 grid (i.e. 200 tiles, and a 0.5% chance of finding the golden nonce per shove), which keeps the rate of finding a golden nonce constant. The Bitcoin system is configured in a manner such that the level of new supply stays constant, regardless of the total number of miners and hashrate.

Therefore, we recognise that this valuation method can only provide a value for BTC at a

particular point in time, and cannot be used to accurately predict a future price. This is because the valuation involves the usage of several interlinked and interdependent variables. Based on this valuation method, the value of BTC drives the supply of miners in the industry, which in turns affects the hashrate and the average supply cost of BTC, subsequently changing the value of BTC, forming a self-reinforcing cycle.

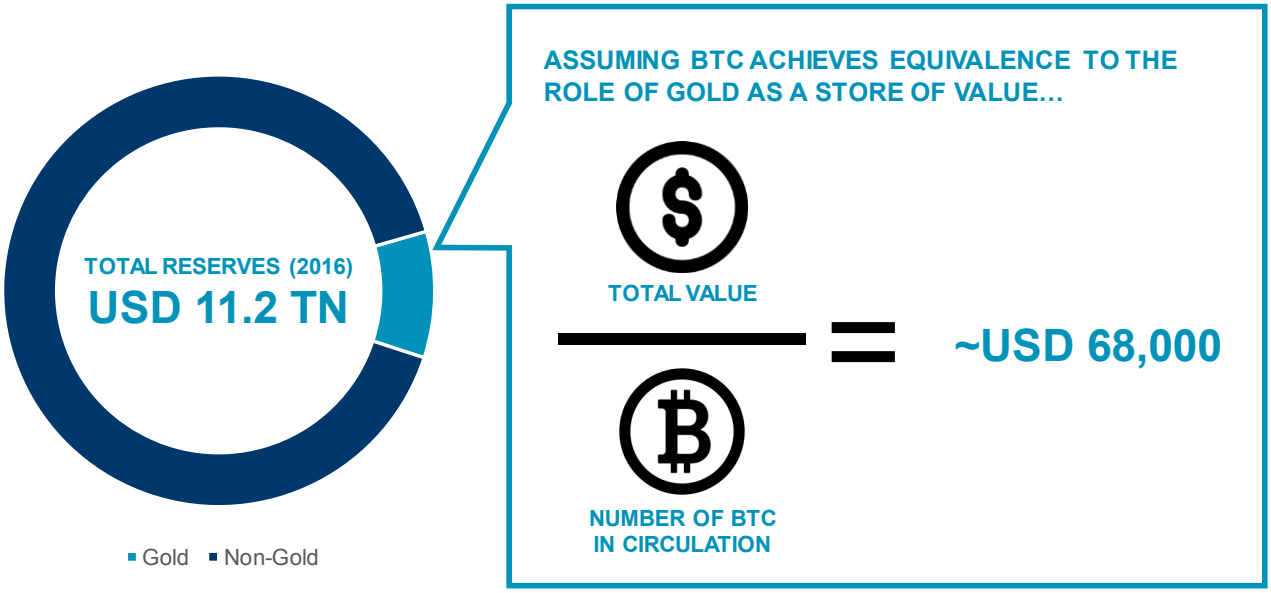
Therefore, while a cost-plus valuation is useful for estimating the value of commodities and gold, this valuation method is essentially incapable of providing an accurate valuation for BTC.

STORE OF VALUE

Following on the comparisons between gold and BTC, BTC has largely been referred to as the digital version of gold, with its lack of price correlation to other assets making it an effective inflation hedge and store of value. According to World Bank data, total international reserves (including gold) in 2016 were ~USD 11.2 trillion,[117] and total international reserves (excluding gold) in 2016 were ~USD 10.1 trillion.[118] Gold makes up ~9.5% of the total international reserves, as a store of value.

There were ~15.6 million BTC in circulation on average in 2016.[119] Assuming BTC was considered equivalent to gold as an inflation hedge and a store of value in 2016, BTC 1 would be worth ~USD 68,000 (see Figure 40).

FIGURE 40: STORE OF VALUE METHOD



Source: World Bank, Quinlan & Associates analysis

[117] The World Bank, 'Total reserves (includes gold, current US$)', available at: https://data.worldbank.org/indicator/FI.RES.TOTL.CD
[118] The World Bank, 'Total reserves minus gold (current US$)', available at: https://data.worldbank.org/indicator/FI.RES.XGLD.CD
[119] Blockchain Luxembourg S.A., 'Bitcoins in circulation', available at: https://blockchain.info/charts/total-bitcoins

From World Bank data, we see that the value of total international reserves has been decreasing for the past few years. In addition, fiat currencies (foreign exchange currencies) are currently the most dominant store of value, and this is likely to remain unchanged. Using a CAGR rate of ~-3% for international reserves (based on 2014 to 2016 figures) and an average proportion for reserves in the form of gold, while also considering the average number of BTC in circulation, we estimate the value of BTC 1 to be USD 69,000 in 2017 and USD 55,000 in 2020 if it is deemed a perfect substitute for gold in terms of acting as an inflation hedge and store of value. However, we see these as theoretically maximum values for BTC 1.

The following table illustrates the different values of BTC 1 based on its level of equivalence to gold (see Figure 41).

FIGURE 41: SENSITIVITY ANALYSIS

EQUIVALENCE TO GOLD AS INFLATION HEDGE AND STORE OF VALUE (%)

	1	5	10	15	20	25	30	35	40	45	50
2017	687	3,433	6,866	10,298	13,731	17,164	20,597	24,030	27,463	30,895	34,328
2020	548	2,741	5,482	8,223	10,965	13,706	16,447	19,188	21,929	24,670	27,411

Likely Movements

Source: Quinlan & Associates analysis

Given our negative evaluation of BTC as a store of value in Section 4 (as it has no inherent value, and no utility value as an asset), we believe it is virtually impossible for BTC to mimic gold as a store of value.

We expect BTC to, at best, achieve 1% (or even less) of gold's function as a store of value, giving it a value of USD 687 in 2017 and USD 548 in 2020, if not considerably less.

AS A CURRENCY

Given that Bitcoin was invented with the intention for it to be used as a currency, one way to value BTC 1 is through using the Quantity Theory of Money.

QUANTITY THEORY OF MONEY

The Quantity Theory of Money states that:

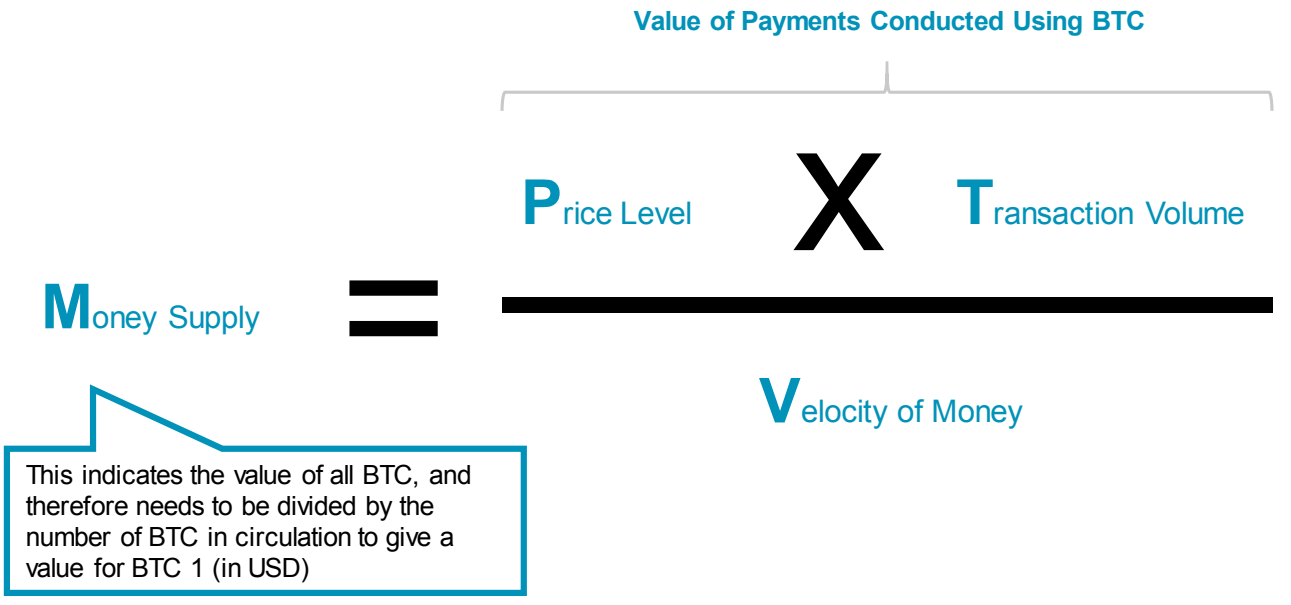
$M \times V = P \times T$, where:

M represents money supply,
V represents velocity of money,
P represents average price level, and
T represents volume of transactions.

The right side of the equation, $P \times T$, is essentially the total value of payments or spending using BTC. We used various data points and assumptions (see later) to calculate V and $P \times T$, which were used to determine M (i.e. the value supplied by all BTC). This value, in turn, needs to be divided by the number of BTC in circulation to give the value of BTC 1 (see Figure 42 and 43).

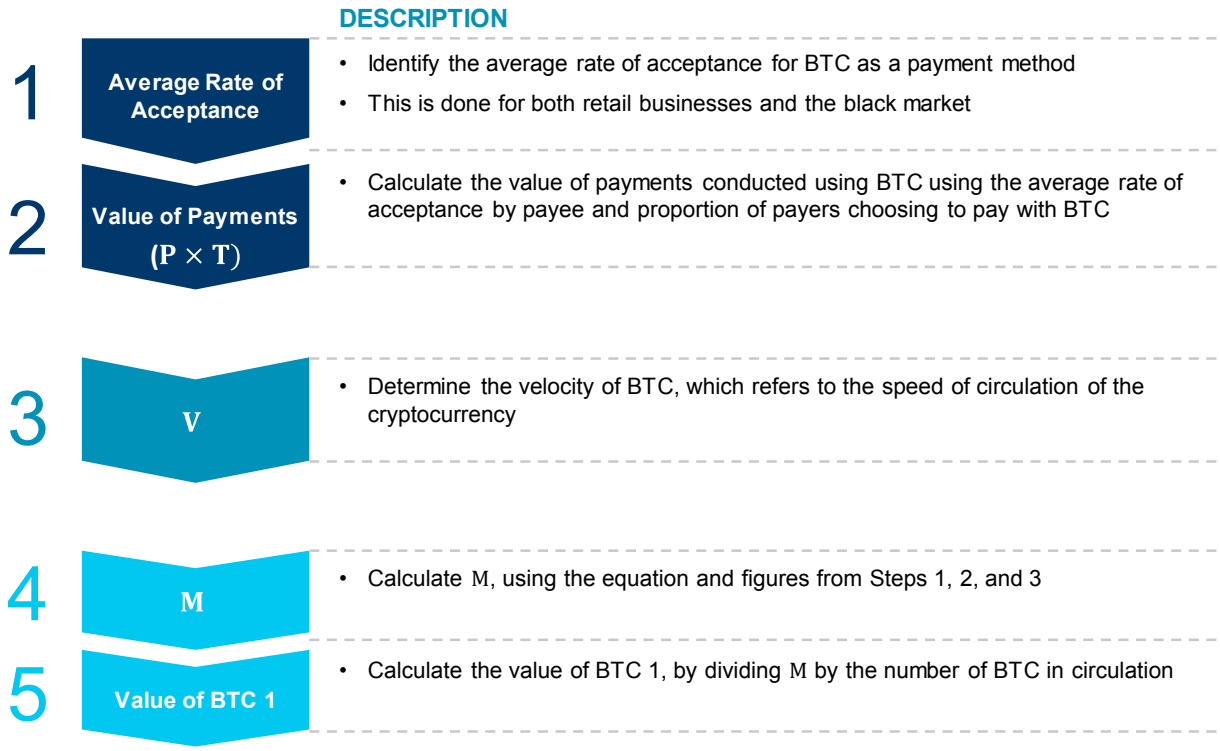
Note that we valued BTC in Q3 2017 using macroeconomic data from the United States, given its availability.

FIGURE 42: QUANTITY THEORY OF MONEY



Source: Quinlan & Associates analysis

FIGURE 43: OUR METHODOLOGY



Source: Quinlan & Associates analysis

VALUE AT Q3 2017

In terms of payments for goods and services, BTC are mainly used for retail sales and illegal or black-market transactions at present.

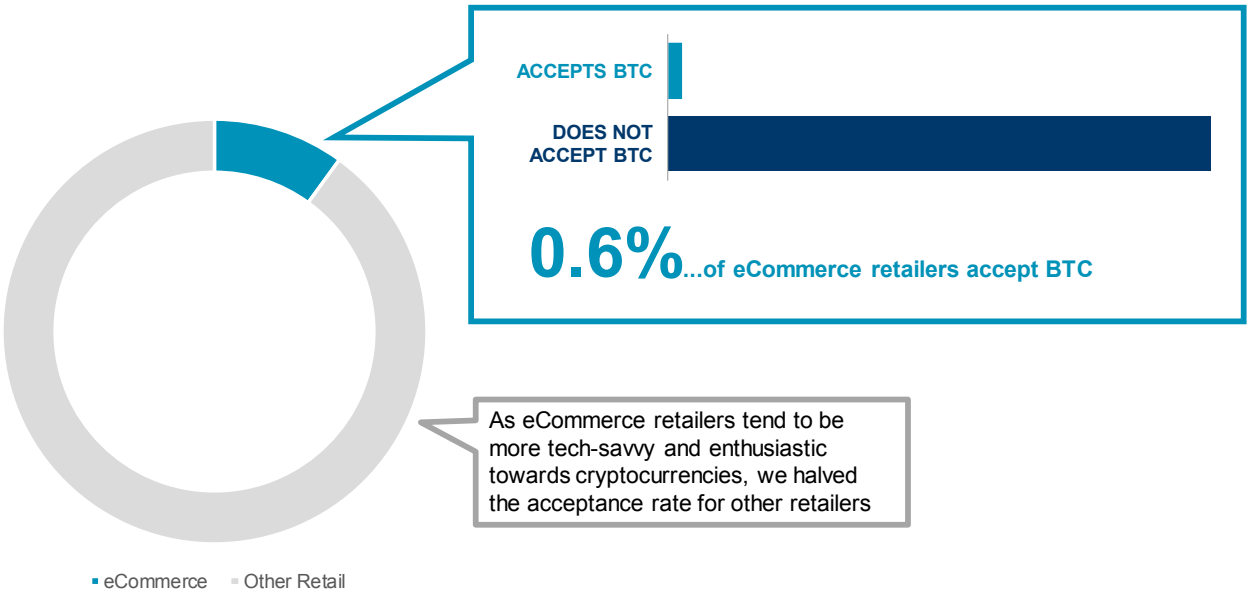
STEP 1 (RETAIL)

According to data from the US Census Bureau, retail eCommerce sales were estimated to be USD 115.3 billion in Q3 2017, accounting for ~9% of total retail sales.[120] As outlined in Section 4, only 3 out of the top 500 online merchants accept BTC as payment (an acceptance rate of ~0.6%). Provided that online merchants represent a group of more tech-savvy group of businesses (given their technological background), online merchants should have a higher level of adoption of BTC payments than other industries.

[120] U.S. Census Bureau News, 'QUARTERLY RETAIL E-COMMERCE SALES 3RD QUARTER 2017', 17 November 2017, available at: https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf

Assuming, on average, other retail businesses are 50% less inclined to accept BTC payments (i.e. an acceptance rate of 0.3%), this suggests ~0.3% of all retail businesses currently accept BTC as payment (see Figure 44). Accordingly, out of the ~USD 1.3 trillion in US retail sales during Q3 2017, we estimate ~USD 4.2 billion worth of goods and services could have been paid for in BTC.

FIGURE 44: AVERAGE RATE OF ACCEPTANCE



On average, we estimate that ~0.3% of all retailers accept BTC payments

Note that the bar chart is for illustrative purposes, and is not drawn to scale

Source: US Census Bureau News, Quinlan & Associates analysis

STEP 2 (RETAIL)

However, BTC is not the preferred transaction method, due to its lack of liquidity, high transaction costs, slow transaction time, and volatile price. As such, we assume just 1% of consumers choose to pay for goods and services using BTC, giving a value of ~USD 42 million for total value of payments using BTC (see Figure 45).

FIGURE 45: VALUE OF PAYMENT USING BTC IN Q3 2017

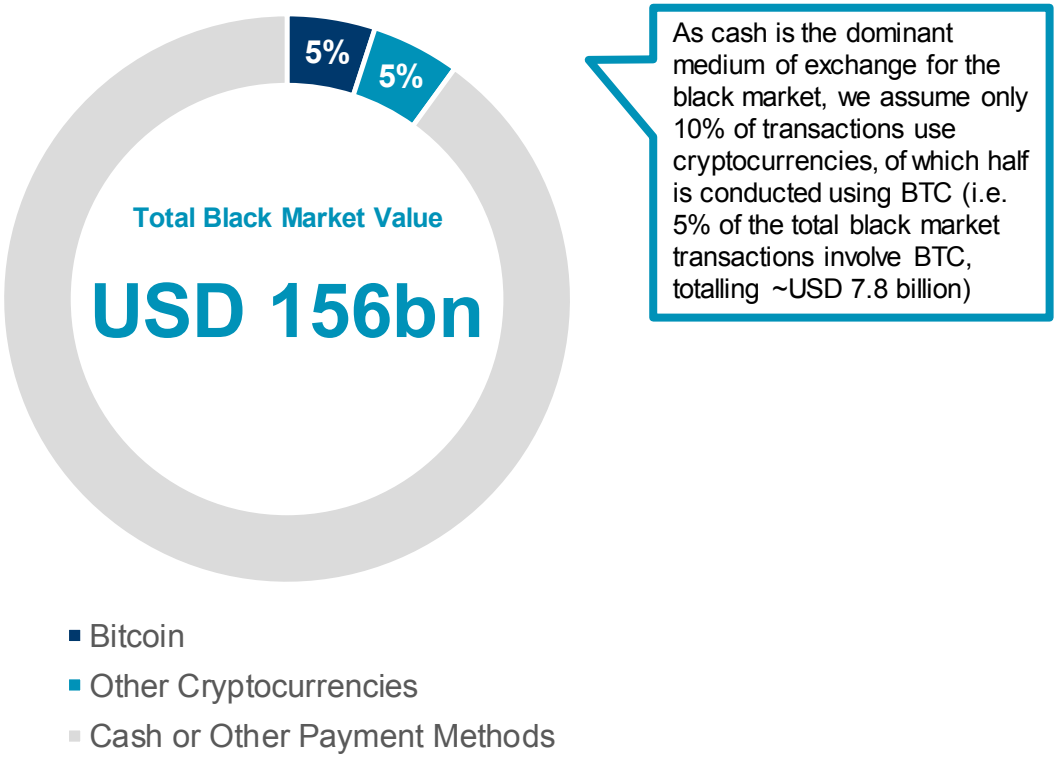
Note that our assumption is based on extensive interviews with the general public, with <1% saying they would pay for good and services with their BTC, given its high transaction costs and price volatility

Source: Quinlan & Associates analysis

STEP 1 & 2 (BLACK MARKET)

We also need to consider the use of BTC in the black market. In terms of the US black market, the annual market size is estimated to be USD 626 billion,[121] which translates to ~USD 156 billion for a quarter. We assume the majority of illegal transactions are conducted in cash, and only 10% conducted using cryptocurrencies (a higher rate than retail sales due to the privacy and anonymity provided by cryptocurrencies). In order to be accepted as a payment, the cryptocurrency needs to be relatively well-known, and the market capitalisation of BTC is ~50% of the total market capitalisation of the top 10 cryptocurrencies in Q3 2017. We therefore assumed 50% of these black-market cryptocurrency payments involved BTC. This gives a value ~USD 7.8 billion for black market BTC payments (see Figure 46).

FIGURE 46: VALUE OF BLACK MARKET PAYMENTS USING BTC IN Q3 2017



Source: Statistic Brain, Quinlan & Associates analysis

[121] Statistic Brain, 'Black Market & Illicit Trade Statistics', available at: https://www.statisticbrain.com/black-market-illicit-trade-statistics/

Summing the two values gives ~USD 7.9 billion for the total value of payments or spending using BTC (i.e. $P \times T$).

STEP 3

Currently, BTC is not used as cash and match better with the characteristics of M2 money supply (i.e. liquid assets that are not cash), being unsuitable as medium of exchange but able to be converted into cash relatively quickly.[122, 123] Using US data once again, the velocity of M2 was 1.427 in Q3 2017.[124] This means the left side of the equation becomes $M \times 1.427$.

STEP 4

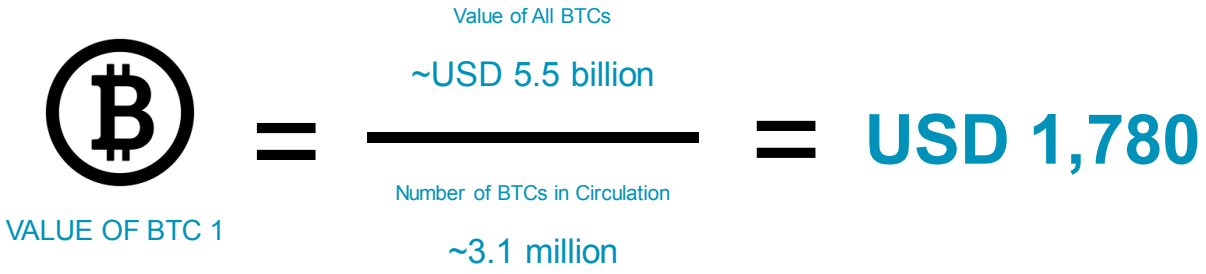
Solving the equation gives M a value of ~USD 5.5 billion, which means, in Q3 2017, BTC in the US should provide ~USD 5.5 billion in value.

STEP 5

On average, there was a global total ~16.5 million BTC in circulation in Q3 2017.[125] By comparing the volume of BTC usage for the world[126] and the US,[127] we calculated the percentage of BTC usage in the US, which gives ~3.1 million BTC in the US.

Dividing the value provided by BTC by the number of BTC in circulation in the US in Q3 2017 gives a value of USD 1,780 per BTC (see Figure 47), notably close to its valuation based on its cost of production.

FIGURE 47: VALUE OF BTC 1 IN Q3 2017 (UNITED STATES)



Source: Coin Dance, Quinlan & Associates analysis

[122] Investopedia, 'M2', available at: https://www.investopedia.com/terms/m/m2.asp
[123] Note that Woobull estimated BTC's velocity (calculated by dividing the 90-day estimated USD transaction volume by 90-day average USD market cap), and found that it is similar to the velocity of USD M2, available at: chart.woobull.com/bitcoin-velocity/
[124] Federal Reserve Bank of St. Louis, 'Velocity of M2 Money Stock', 21 December 2017, available at: https://fred.stlouisfed.org/series/M2V
[125] Blockchain Luxembourg S.A., 'Bitcoins in circulation', available at: https://blockchain.info/charts/total-bitcoins
[126] Coin Dance, 'LocalBitcoins Volume (Global)', available at: https://coin.dance/volume/localbitcoins/ALL
[127] Coin Dance, 'LocalBitcoins Volume (USA)', available at: https://coin.dance/volume/localbitcoins/USD

From our calculations, we see that the contribution from the black market significantly outweighs that of legal, retail figures. Therefore, we conducted a sensitivity analysis on the value of BTC, by changing the percentage of black market payments using cryptocurrencies, and the percentage of these cryptocurrency payments that use BTC (see Figure 48).

FIGURE 48: SENSITIVITY ANALYSIS

…% OF WHICH USE BTC	% OF BLACK MARKET PAYMENTS WITH CRYPTOCURRENCIES									
	5	10	15	20	25	30	35	40	45	50
5	98	186	275	363	452	541	629	718	806	895
10	186	363	541	718	895	1,072	1,249	1,426	1,603	1,780
15	275	541	806	1,072	1,337	1,603	1,868	2,134	2,400	2,665
20	363	718	1,072	1,426	1,780	2,134	2,488	2,842	3,196	3,550
25	452	895	1,337	1,780	2,222	2,665	3,108	3,550	3,993	4,436
30	541	1,072	1,603	2,134	2,665	3,196	3,727	4,259	4,790	5,321
35	629	1,249	1,868	2,488	3,108	3,727	4,347	4,967	5,586	6,206
40	718	1,426	2,134	2,842	3,550	4,259	4,967	5,675	6,383	7,091
45	806	1,603	2,400	3,196	3,993	4,790	5,586	6,383	7,180	7,976
50	895	1,780	2,665	3,550	4,436	5,321	6,206	7,091	7,976	8,862

Base Case Likely Movements

Note% of which use BTC refers to the value of transactions that use BTC

Source: Quinlan & Associates analysis

The value of BTC 1 ranges from USD 98 to USD 8,862, based on the different assumptions. The higher valuations require BTC to be used in a majority of the cryptocurrency transactions in the black market, which is plausible but unlikely due to cash being the prominent payment method (which is anonymous and relatively secure) and BTC price volatility. In addition, it was reported that criminals are turning to Monero, which provides a higher level of privacy and anonymity. Founder of security firm Comae Technologies, Matt Suiche, said that Monero is now 'one of the favourites, if not the favourite' for ransomware attacks.[128] Therefore, we believe even though the black market will increasingly use cryptocurrencies for transactions, the proportion which uses BTC will decrease, leading to the top right values in Figure 48.

[128] Bloomberg, 'The Criminal Underworld Is Dropping Bitcoin for Another Currency', 2 January 2018, available at: https://www.bloomberg.com/news/articles/2018-01-02/criminal-underworld-is-dropping-bitcoin-for-another-currency

VERDICT

We believe BTC current price of ~USD 14,000 deviates significantly from its true value, USD 2,161 (based on our cost of production valuation), USD 687 (from our store of value method), and USD 1,780 (as a currency).

It is clear from data that during October and November 2017, there was a massive surge in the level of public interest in BTC, along with a significant spike in BTC price (see Figure 32 – BTC PRICE VS GOOGLE HITS). Prior to this, both the level of interest in and price of BTC were relatively stable, experiencing a gradual and steady rate of increase.

It is therefore not unreasonable to believe that during Q1 to Q3 2017, BTC's value stemmed more from its potential future utility, while in the last quarter of 2017, the price of BTC was largely a function of outright speculation. All of this suggests that Bitcoin, in its current form, is a bubble waiting to burst.

We expect a significant price correction in the short-term as the speculative furore around the price of BTC subsides. However, it's longer-term value will largely depend on how regulators and the wider market choose to accept it in coming years.

BITCOIN IN ITS CURRENT FORM, IS A BUBBLE WAITING TO BURST

2020 PRICE FORECASTS

For 2020, we forecasted two scenarios. For our BULL SCENARIO, we valued BTC based on its potential as a currency and national FX reserve. For the BEAR SCENARIO, we valued it with a view it is largely ruled out as a mainstream currency (and hence mostly a black-market medium of exchange) (see Figure 49).

Note that for 2017, our calculations are based on US data and ignore BTC's utility as an FX store of value, given it was not being used as an FX reserve. Global data has also been used for 2020 (given availability of forecasts). However, the final results are comparable, as data can be extrapolated proportionally.

FIGURE 49: VALUE OF BTC 1 IN 2020

	BULL SCENARIO (<1% Probability) 	**BEAR SCENARIO** (>99% Probability) 
DESCRIPTION	• BTC widely accepted as a form of payment • Used by governments as an FX reserve	• BTC ruled out as a form of payment • Not used by governments as an FX reserve
RETAIL USAGE	• 95% of eCommerce retailers accept BTC • 75% of other retailers accept BTC	• 1% of eCommcerce retailers accept BTC • 0.5% of other retailers accept BTC
BLACK MARKET USAGE	• 20% involves cryptocurrencies • Of which 1% uses BTC	• 20% involves cryptocurrencies • Of which 5% uses BTC
VELOCITY OF BTC	• Similar to M1 money supply	• Similar to M2 money supply
FX STORE OF VALUE	• 10% of 'other' currency reserves (non-USD, EUR, GBP, JPY, CAD, AUD, RMB, & CHF)*	• None
# BTC IN CIRCULATION	• ~18.6 million BTCs (2020)	• ~18.6 million BTCs (2020)
VALUE OF BTC 1	**USD 56,750**	**USD 810**

MV = PT assumptions | FX store of value assumptions

*Note that data is based on Q4 2016 figures

Source: IMF, Quinlan & Associates analysis

BULL SCENARIO

In our BULL SCENARIO, BTC is widely accepted as a mainstream currency, and is used as (A) a medium of exchange (for retail payments); and (B) a store of value (as global FX reserves).

A. MEDIUM OF EXCHANGE

STEP 1 (RETAIL)

The 2020 world GDP is estimated to be USD 93.5 trillion,[129] which translates to ~USD 24.3 trillion in retail sales globally, assuming the same proportion as 2017 Q3 US data. Given that BTC is accepted as a form of payment, we assumed 95% of eCommerce businesses and 75% of other retail businesses accept BTC. In addition, as the world shifts towards digital and online business, we assumed that out of all retailers, 15% will be eCommerce businesses. This gives an average adoption rate of ~78%.

STEP 2 (RETAIL)

However, 85% of transactions are still carried out using cash in 2017,[130] and we believe cash will still be the prominent medium of exchange. Assuming 30% of consumers choose to pay with BTC, this gives a value of ~USD 5.7 trillion.

STEP 1 & 2 (BLACK MARKET)

The global black market was estimated to be worth USD 1.81 trillion in 2017,[131] and assuming the same growth rate as the world GDP, the total value of the black market in 2020 would reach ~USD 2.1 trillion.

We assumed 20% of transactions are conducted using cryptocurrencies (increasing from 10% in 2017). For Bitcoin to be a mainstream currency, it cannot be prominently used in the black market, and therefore out of the cryptocurrency payments, we assumed only 1% uses BTC (down from 50% in 2017). This gives a value ~USD 4.3 billion for black market BTC payments.

Summing the two values gives ~USD 5.7 trillion for the total value of payments or spending using BTC (i.e. $\mathrm{P} \times \mathrm{T}$).

STEP 3

Given the assumption that BTC is a widely accepted form of payment, it should behave like cash, and therefore will be similar to M1 money supply. We used a value of 5.496 for the velocity of M1,[132] based on Q3 2017 US data.

STEP 4

This gives a value of ~USD 1.0 trillion for M.

STEP 5

The block reward is expected to be halved on 8 June 2020 to BTC 6.25, and the average number of BTC in circulation in 2020 will be ~18.6 million.

Dividing the value of M by the number of BTC in circulation in 2020 gives a value of USD 55,772 for BTC 1, this gives a value for BTC 1 if it is solely used as a medium of exchange (for payments).

[129] Statista, 'Global GDP at current prices from 2010 to 2022', available at: https://www.statista.com/statistics/268750/global-gross-domestic-product-gdp/
[130] International Monetary Fund, 'Cash Is Dead, Long Live Cash', June 2017, available at: http://www.imf.org/external/pubs/ft/fandd/2017/06/wheatley.htm
[131] Havocscope, 'Havocscope Market Value', available at: http://www.havocscope.com/market-value/
[132] Federal Reserve Bank of St. Louis, 'Velocity of M1 Money Stock', 21 December 2017, available at: https://fred.stlouisfed.org/series/M1V

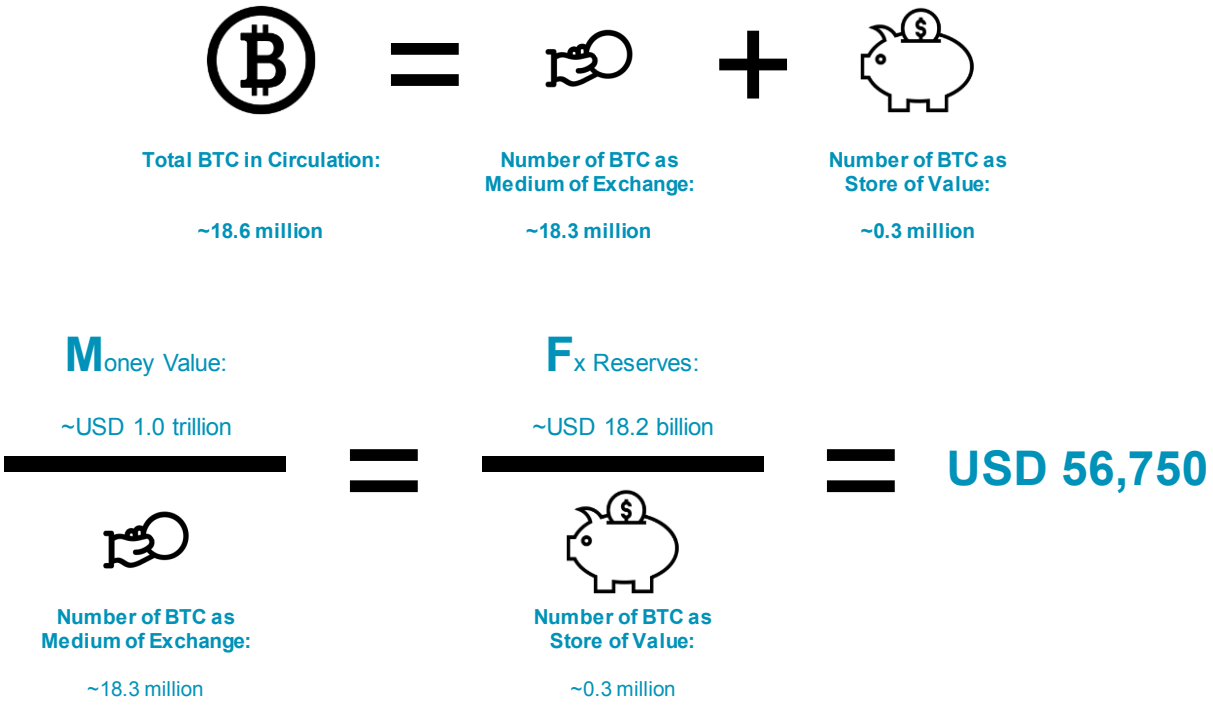
B. STORE OF VALUE

In this BULL SCENARIO, we assume that, in addition to being used as a medium of exchange, BTC will be equivalent to 10% of "other" currencies (i.e. currencies that are not USD, EUR, GBP, JPY, CAD, AUD, RMB, and CHF) in terms of its place as an international FX reserve. Using a CAGR rate of ~-3% for reserves projection (based on 2014 to 2016 World Bank data), and fiat currency proportions (based on Q4 2016 IMF data), we calculate that BTC would represent ~USD 18 billion worth of international FX reserves (i.e. ~0.2% of total) by 2020.

COMPILATION

Logically, the value of BTC 1 as a medium of exchange has to be equal to the value of BTC 1 as a store of value. By compiling these values together, we estimate that the value of BTC 1 to be USD 56,750 (see Figure 50)

FIGURE 50: COMPILATION OF FIGURES FOR BTC 1 VALUE IN 2020



Source: IMF, Quinlan & Associates analysis

We have also considered different cases, where BTC replaces the top six FX global reserves as a store of value, resulting in different values for BTC 1 in 2020 (see Figure 51).

FIGURE 51: VALUE OF BTC 1 FOR DIFFERENT CASES IN 2020

COUNTRY	CURRENCY	% OF GLOBAL RESERVES	BTC 1 PRICE (USD)
United States	USD	46.8	301,512
European Union	EUR	14.4	131,603
United Kingdom	GBP	3.2	72,761
Japan	JPY	3.1	71,955
Canada	CAD	1.5	63,593
Australia	AUD	1.4	62,878
10% of all others	N/A	0.2	56,750
None	N/A	0.0	55,772

Note that proportions are based on IMF data for Q4 2016

Source: IMF, Quinlan & Associates analysis

Note that if the value of BTC as an FX reserve store of value is relatively small, the final BTC price is skewed towards USD 55,772 (i.e. if the FX reserve store of value function is ignored, the functional value of BTC as a medium of exchange is USD 55,772, a floor for the BULL SCENARIO). However, if BTC can replace a large proportion of international FX reserves, then its price as a store of value dominates the calculations, inflating accordingly (e.g. BTC 1 is worth USD 301,512 if it completely replaces USD in terms of its proportion of international FX reserves, i.e. a ceiling for the BULL SCENARIO).

Even if we take the theoretically most bullish scenario for BTC by 2020, where 100% of retail and black-market payments are conducted using BTC, and BTC also achieves an equivalent status as to the USD in terms of its proportion of international FX reserves, this gives a value BTC 1 at ~USD 505,000. However, we believe this scenario is virtually impossible.

BEAR SCENARIO

In our bear scenario, BTC is widely ruled out as a mainstream form of payment by governments, and is mainly used for illegal transactions in the black market or as a safe haven asset.

Given that BTC is largely ruled out as a form of payment, it is extremely unlikely that governments will hold BTC as part of their FX reserves. As such, BTC has no value as an FX reserve. Therefore, in the BEAR SCENARIO, only the Quantity Theory of Money method is used.

STEP 1 & 2 (RETAIL)

Assuming 1% of eCommerce businesses and 0.5% of other retail businesses accept BTC, and 0.1% of consumers choose to pay with BTC, this gives a value of ~USD 140 million for payments for goods and services using BTC.

STEP 1 & 2 (BLACK MARKET)

We assumed 20% of black market trade is conducted using cryptocurrencies in 2020, similar to the BULL SCENARIO, of which 5% involved BTC (as there are other, more private, anonymous, and secure cryptocurrencies), giving a value of ~USD 21.4 billion for black market trade using BTC.

Summing the two values gives ~USD 21.5 billion for the total value of payments or spending using BTC (i.e. $P \times T$).

STEP 3

BTC, in this case, behaves similarly to M2, given that it is not used as the main form of payment and behaves like an asset that can be converted to cash easily, which again gives a value of 1.427 for V.

STEP 4 & 5

This gives a value of ~USD 15.1 billion for M. Dividing by the average number of BTC in circulation in 2020, we arrive at a value of ~USD 810 for BTC 1.

‘THE MARKET CAN REMAIN IRRATIONAL LONGER THAN YOU CAN REMAIN SOLVENT’
– JOHN MAYNARD KEYNES

FUTURE VALUE

Our calculations for the future value of BTC (in 2020) under a BEAR and BULL SCENARIO range from USD 810 to USD 56,750 respectively, which is a significantly large range. However, we believe this is unsurprising due to the uncertainties surrounding its potential adoption, competing cryptocurrencies, and upcoming regulations, which have also been contributing to its considerable volatility during 2017.

Nonetheless, it is our opinion that the BEAR SCENARIO is considerably more likely to play out, given we believe BTC will be ruled out as a mainstream form of payment and will not be utilised by governments as an FX reserve. As such, we forecast BTC 1 to trade at or below USD 1,800 by December 2018, based on our valuation methodology.

We see the value likely to gradually decline to our BEAR SCENARIO value (USD 810) and potentially lower by 2020 as it falls out of favour relative to other cryptocurrencies, such as Monero (especially for black market transactions), which have better privacy/security features and faster transaction processing times.

Note that Quinlan & Associates and the authors of this report do not hold any positions (be it long or short) in BTC or any other cryptocurrencies. In addition, Quinlan & Associates is not a financial institution, and therefore our business model does not benefit or suffer from the development and level of adoption of BTC or other cryptocurrencies (be it positive or negative). As such, Quinlan & Associates has no vested interest in either talking up or talking down BTC and/or other cryptocurrencies.

SECTION 7

CRYPTOCURRENCY SURVEY

In order to corroborate the research, interviews, and opinions in previous sections, we conducted a global survey on Bitcoin and other cryptocurrencies. The purpose of the survey was to understand the perspective of the mass population on current cryptocurrencies and their view on the outlook for the wider industry.

We received over 1,500 online survey responses across the Americas, EMEA, and APAC. Our survey respondents worked in a wide range of industries, with the majority being in financial services, technology/IT, FinTech, and consulting (including IT consulting). As cryptocurrencies arguably impact these industries most directly, we believe our survey respondents had a relatively in-depth understanding of the effects and implications of cryptocurrencies, providing us with practical insights.

Given Quinlan & Associates is headquartered in Hong Kong, it is no surprise that the largest proportion of respondents were located in the APAC region and work in the financial services industry. Some of the respondents from financial services work for regulators, which was extremely helpful in providing a more comprehensive view on upcoming regulations, and therefore the outlook for current cryptocurrencies.

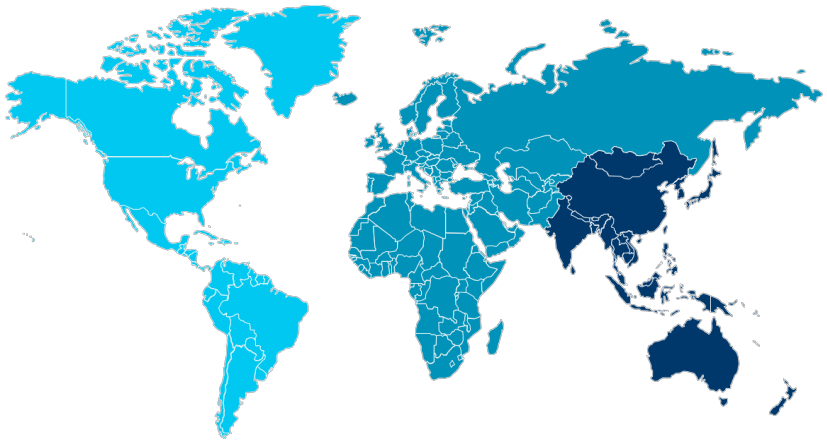
We asked survey respondents about the value of their cryptocurrency holdings. Some of this data was cut to better identify the perspectives of those who hold cryptocurrencies (and are, therefore, arguably more supportive and confident in the outlook) and those who do not.

Survey respondents were also asked about their view on current cryptocurrencies, including their potential to replace fiat currencies, upcoming regulations, and whether Bitcoin is a bubble.

Finally, respondents were given the opportunity to freely provide their own comments around their views on cryptocurrency and blockchain.

Q&A SURVEY: DEMOGRAPHICS

GEOGRAPHICAL BREAKDOWN



9%
AMERICAS

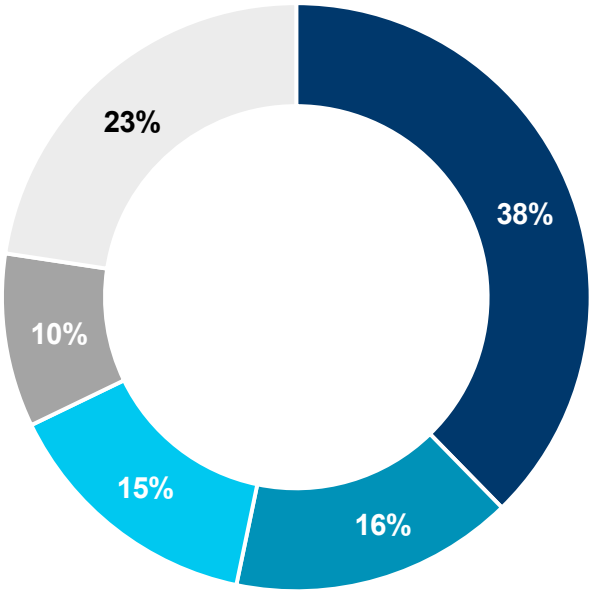
25%
EMEA

66%
APAC

INDUSTRY BREAKDOWN

- Financial Services
- Consulting
- FinTech
- Technology
- Others

Note: numbers may not sum to 100% due to rounding



Within financial services, 49% of respondents work in fund management (e.g. asset management, hedge fund, private equity), 26% are in investment banking, and 7% are regulators

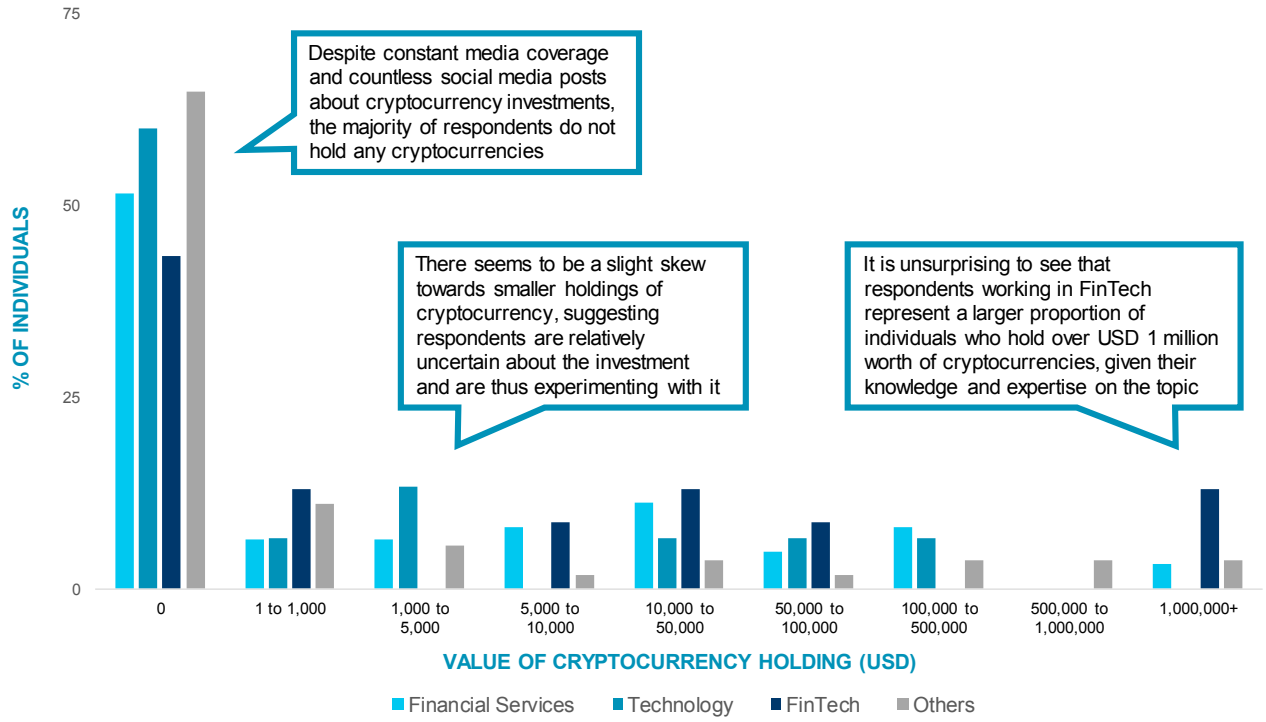
Within consulting, 13% of respondents work in IT consulting

Of all FinTech respondents, 24% indicated that they work for cryptocurrency/ blockchain-related firms

Source: Quinlan & Associates survey and analysis

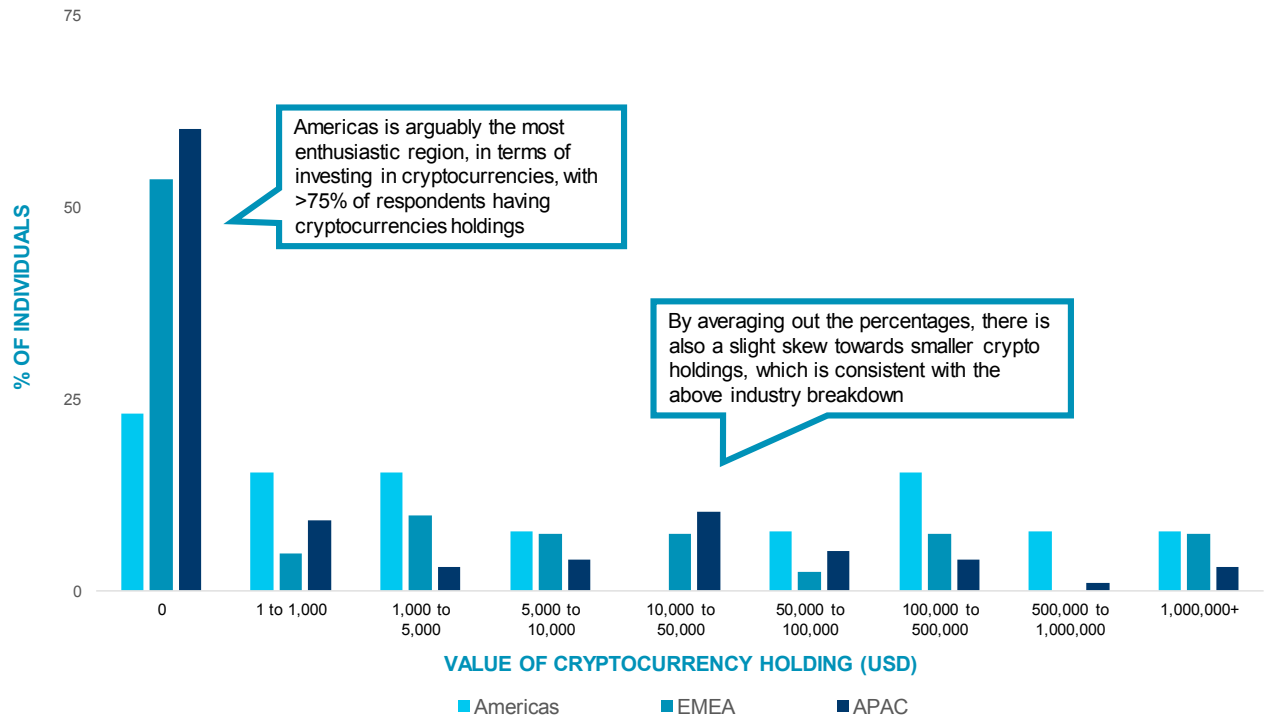
We asked our respondents for the value of their cryptocurrency holdings. Understandably, a small group of respondents were unwilling to disclose the value of their cryptocurrency holdings.

Q&A SURVEY: CRYPTOCURRENCY HOLDINGS



Source: Quinlan & Associates survey and analysis

Q&A SURVEY: CRYPTOCURRENCY HOLDINGS (CONT.)

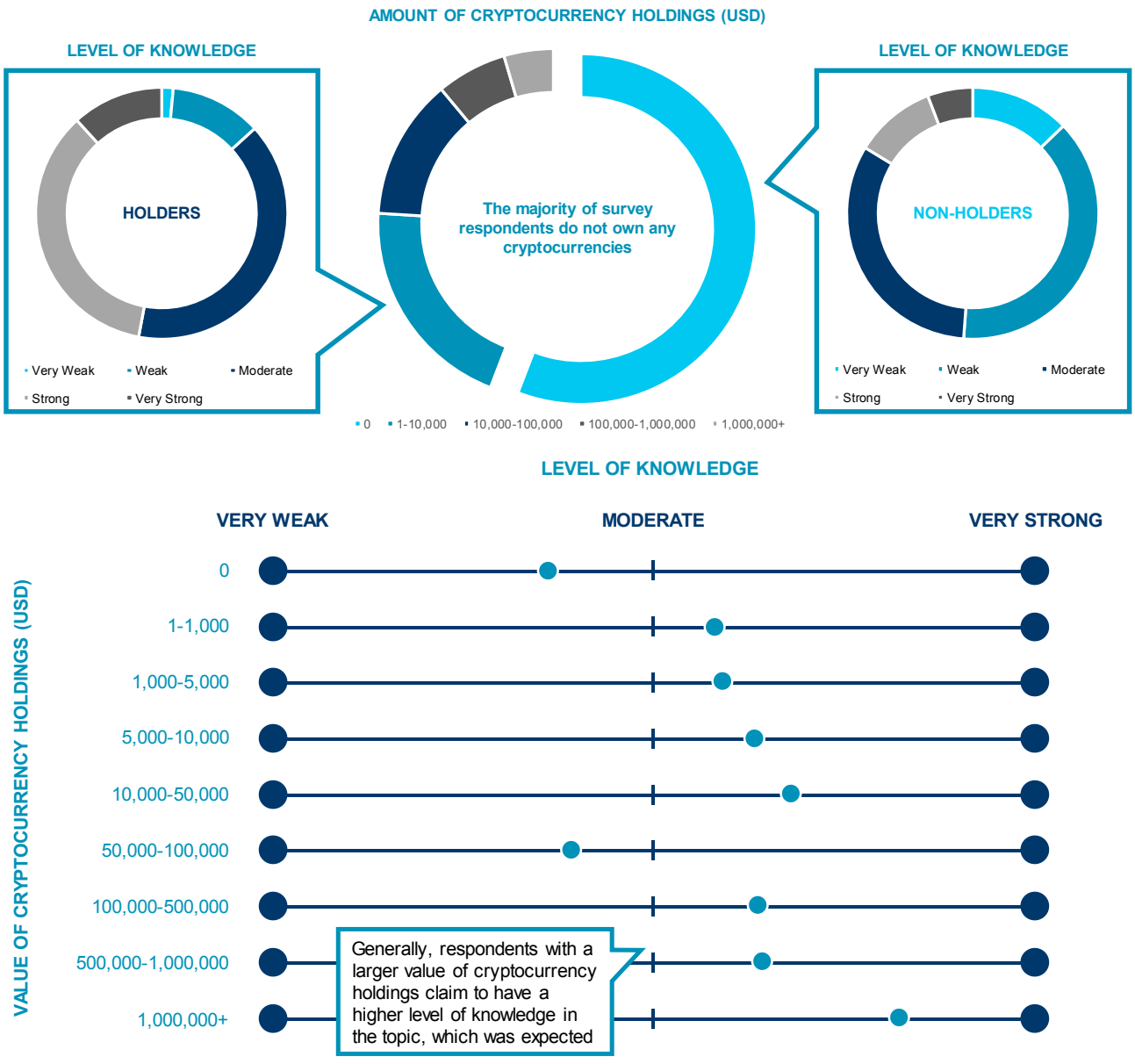


Source: Quinlan & Associates survey and analysis

Most of our respondents did not hold any cryptocurrencies; for those that did, there was a tendency to hold smaller values of cryptocurrencies instead of larger sums. This indicates a relatively experimental stance towards cryptocurrencies as an investment. We also asked our respondents to rate their own level of knowledge around cryptocurrencies, from very weak to very strong.

It was not surprising to see that, on average, cryptocurrency holders believed they have a stronger knowledge in cryptocurrencies than non-holders. In general, we noted that individuals with larger cryptocurrency holdings reported greater levels of knowledge. There was also a clear gap in the reported level of knowledge between those with holdings of over USD 1 million and all other respondents. It was also somewhat surprising to see respondents with cryptocurrency holdings of USD 50,000-100,000 reporting a relatively weak understanding around the topic.

Q&A SURVEY: KNOWLEDGE IN CRYPTOCURRENCIES

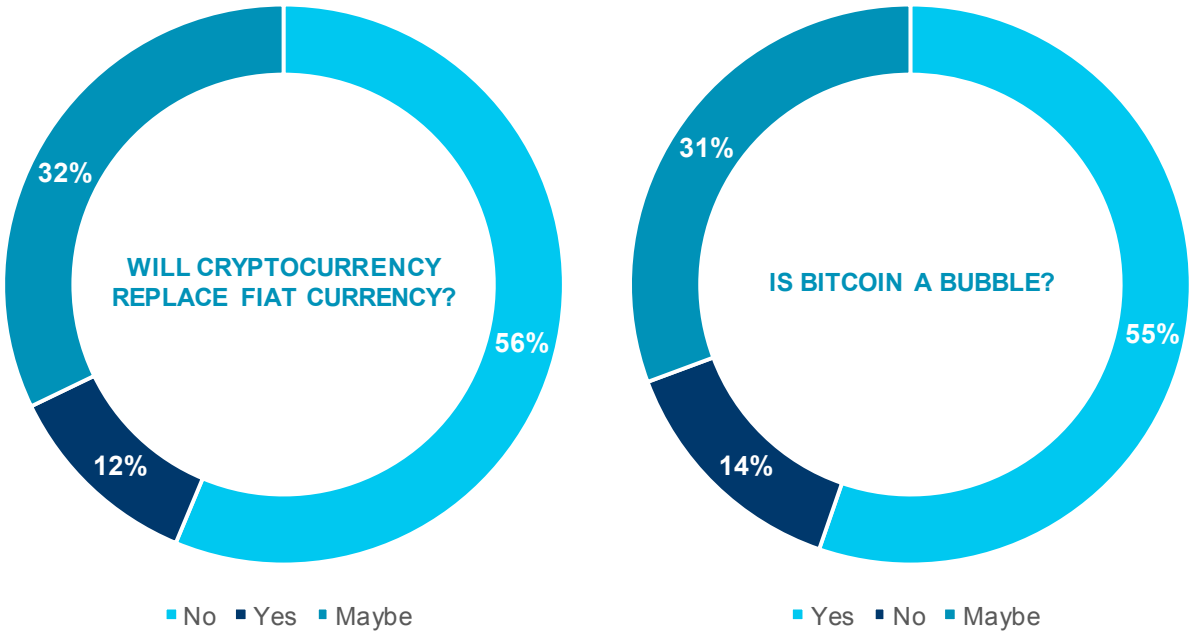


Source: Quinlan & Associates survey and analysis

We also asked our respondents about their views on the outlook for current cryptocurrencies in terms of: (1) their ability to replace fiat currency; and (2) whether BTC was a bubble.

Q&A SURVEY: VIEWS ON OUTLOOK

Generally, those that believed cryptocurrency will not replace fiat currency also thought Bitcoin was a bubble, and vice versa



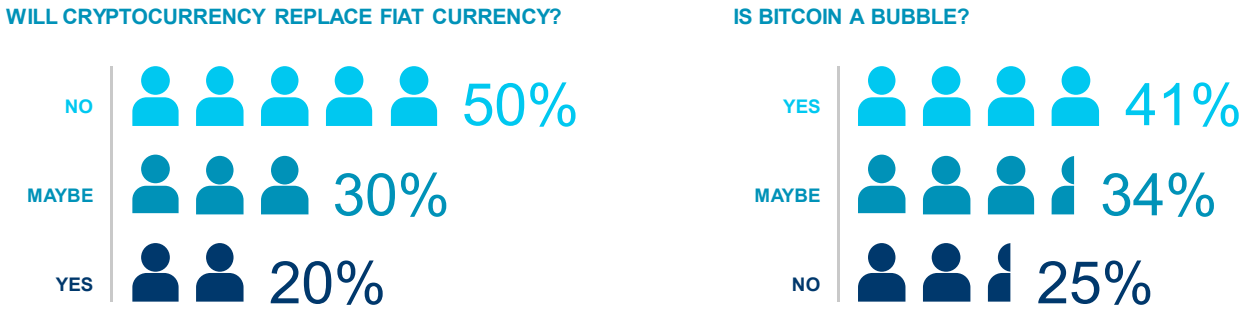
Note that dark blue is favourable for Bitcoin and other cryptocurrencies, while light blue is unfavourable

Source: Quinlan & Associates survey and analysis

Remarkably, there was a high correlation between those that believed cryptocurrencies would not replace fiat currencies and those that thought BTC was a bubble. This is most likely due to the fact that if cryptocurrencies do not replace fiat currencies, they will never be a mainstream medium of exchange, and therefore never have utility value. This implies the value of BTC is indeed deviating substantially from its true value, reinforcing our view that it is a bubble. A majority of respondents agree, with two individuals saying that 'the bulk of activity in cryptocurrencies right now is speculative' and Bitcoin is 'a big scam and will burst sooner or later.'

Even amongst respondents with cryptocurrency holdings, 50% thought that cryptocurrencies would not replace fiat currencies, and 41% believed BTC was a bubble, suggesting a substantial number of holders had a negative view on the outlook of current cryptocurrencies.

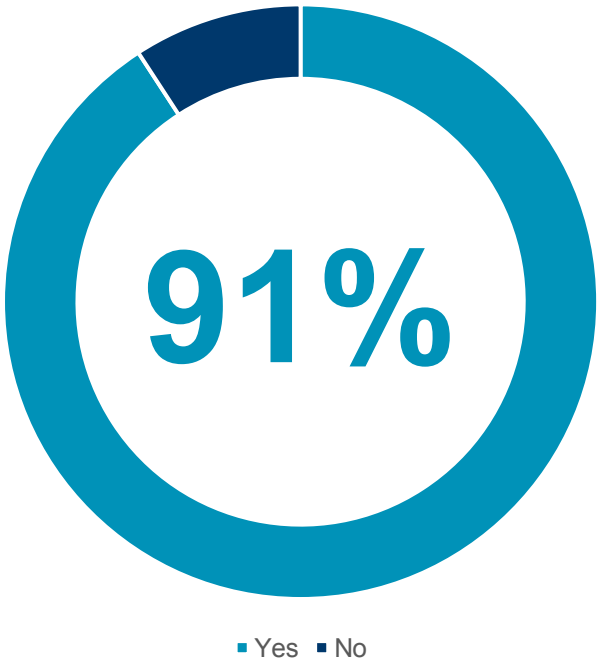
Q&A SURVEY: VIEWS FROM THOSE WITH CRYPTOCURRENCY HOLDINGS



Source: Quinlan & Associates survey and analysis

When asked about their views on upcoming regulations, 91% of respondents believed Bitcoin and other cryptocurrencies would be subjected to greater regulatory scrutiny. The result was similar for respondents that worked for financial regulators; one regulator respondent said that 'with how the cryptocurrency world is evolving, regulations will definitely come.'

Q&A SURVEY: REGULATIONS FOR BITCOIN AND OTHER CRYPTOCURRENCIES



% of respondents who believed that Bitcoin and other cryptocurrencies would be subject to greater regulatory scrutiny

Source: Quinlan & Associates survey and analysis

SUMMARY

The majority of our respondents maintained a relatively negative view on the outlook for current cryptocurrencies, regardless of the value of their cryptocurrency holdings and their level of knowledge in the underlying technology.

The survey responses support our view that cryptocurrencies will likely be further restricted through greater regulation, and are thus incapable of challenging the role of fiat currencies. This further suggests that Bitcoin, in its current form, is a bubble waiting to burst.

THE MAJORITY OF OUR RESPONDENTS MAINTAINED A RELATIVELY NEGATIVE VIEW ON THE OUTLOOK FOR CURRENT CRYPTOCURRENCIES, REGARDLESS OF THE VALUE OF THEIR CRYPTOCURRENCY HOLDINGS AND THEIR LEVEL OF KNOWLEDGE IN THE UNDERLYING TECHNOLOGY

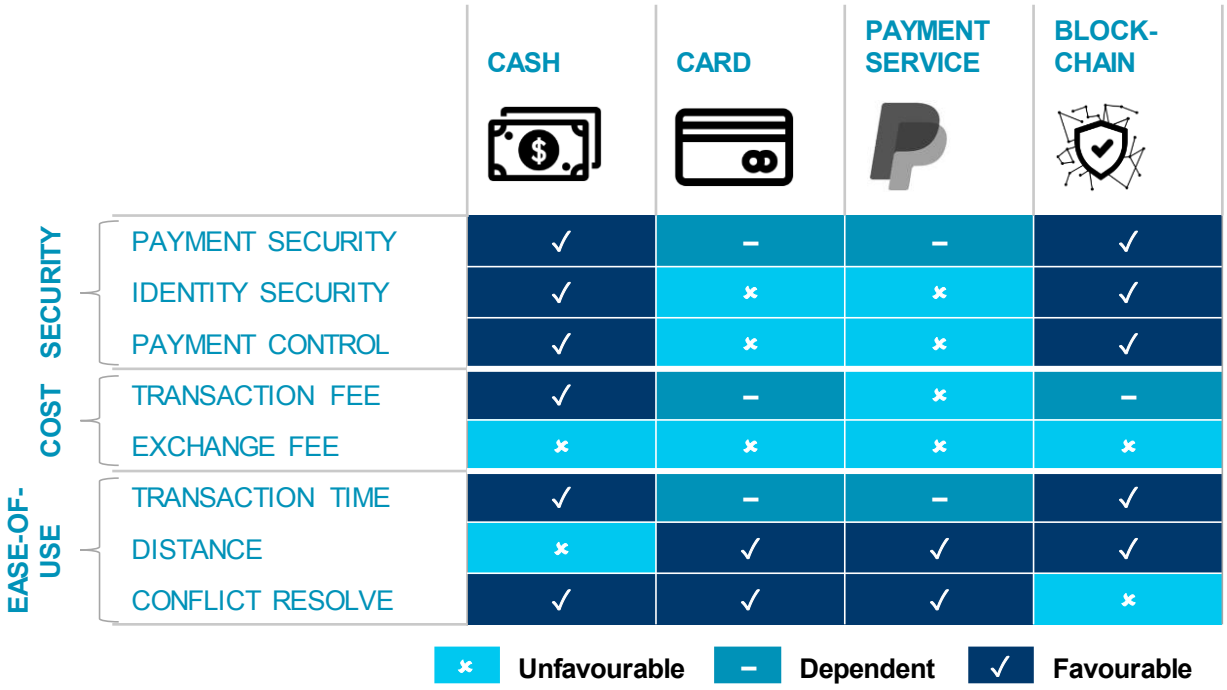
SECTION 8

BLOCKCHAIN AS A PAYMENT SYSTEM

INTRODUCTION

No matter the view on cryptocurrency (i.e. whether it is a currency or an asset, or whether it is a bubble or not), the consensus is that blockchain technology can enhance current payment systems (see Figure 52). Note that the discussion uses a decentralised blockchain system, such as Bitcoin's blockchain, instead of a bank-developed or country-developed system, in which a party (i.e. the bank or the country) has significance influence over the system.

FIGURE 52: BLOCKCHAIN AS A PAYMENT SYSTEM



Source: Quinlan & Associates analysis

SECURITY

This refers to both the security of the payment and the level of privacy involved.

PAYMENT SECURITY

Payment security mainly refers to the chargeback mechanism, aimed at protecting the payer.

Due to the face-to-face nature of cash payments, transactions are settled and secured once the cash is handed over to the payee. By contrast, payees that accept credit card payments or use payment services run the risk of chargebacks, especially those dealing with international transactions.

Cryptocurrency payments avoid this problem, as transactions are pushed, meaning the payer has to initiate the payment. Moreover, given the lack of third parties, the payment received by the payee is secured and cannot be reversed (unless the payee does so voluntarily).

IDENTITY SECURITY

Identity security is the level of privacy one experiences when using a payment method.

When using cash, the payee is not required to reveal any personal information, ensuring their privacy is protected. With credit cards and payment services, both require the setting up of an account, which involves ID verification. Therefore, the central party can determine the identify of both the payer and the payee, reducing the level of privacy.

The blockchain system provides a high level of privacy, and properly using the system (e.g. choosing blockchains which mask transaction details, using a different wallet address for each transaction, etc.) can make it virtually impossible for an observer to pinpoint the parties involved in any transaction.

PAYMENT CONTROL

Payments through cash and the blockchain use a push mechanism. This means the payer has full control over the payment, and can cancel subscriptions at any time. On the other hand, cards and payment services use a pull mechanism, allowing the payee to incur recurring charges.

Note that this criterion uses the perspective of the payer (or consumer), in which case a push mechanism is preferred to a pull mechanism.

COST

The cost of transactions is an important consideration for consumers when choosing which payment method to use.

The main contributors to cost are transaction fees and exchange fees. At present, due to the volatility of cryptocurrencies valuations, businesses charge customers paying with cryptocurrencies higher than those paying with traditional payment methods, therefore increasing the cost of transactions involving cryptocurrencies.

TRANSACTION FEE

Paying with cash does not involve a transaction fee, as this payment method does not require a third party. However, payments with credit cards may require transaction fees, depending on the service provider. Payment services firms generate their revenue stream from transaction fees, with most levying these fees on the payee.

Similar to credit cards, whether a blockchain system charges transaction fees depends on the blockchain itself.

Some blockchain systems, such as Bitcoin, do not charge transaction fees, even though there is a choice for the payer to include transaction fees in the payment to speed up the transaction verification process. However, in practice, it was reported that BTC transaction fees are doubling every three months.[133] Other blockchain systems, such as Ethereum, charge transaction fees for all transactions.

Note that the Bitcoin miners will be incentivised only by transaction fees once all 21 million BTC are in circulation (see Section 2).

EXCHANGE FEE

For cross-border transactions, all payment methods require the payer to exchange their currency to the payee's currency, and therefore incur foreign exchange costs for the transaction. This is, however, inevitable, and can only be solved by having a global currency.

[133] The Sydney Morning Herald, ''Extremely high risk': bitcoin.com co-founder has sold all his bitcoins', 21 December 2017, available at: http://www.smh.com.au/business/markets/bitcoin-as-good-as-useless-says-bitcoin-com-co-founder-20171218-p4yxty.html

EASE-OF-USE

Generally, the easier it is to use a payment method, the more willing people are to adopt it.

TRANSACTION TIME

Cash payments, due to their face-to-face nature, are instantaneous. For cards and payment services, the verification time varies, and can range from virtually instant to a few business days.

Blockchain systems have the potential to conduct and verify transactions extremely quickly. For example, transactions through Ripple take only a few seconds. This contrasts with Bitcoin's system, which has a blocktime of 10 minutes, and recommended waiting time of an hour (6 confirmations) for large transactions.

It is important to note that the capacity of the system contributes to the transaction time required. One of the most popular payment methods, Visa, handles roughly 2,000 transactions per second and has the capacity to handle up to 56,000 transactions per second. Bitcoin can handle seven, which severely lengthens its transaction time, and there are occasions where a single transaction takes up to five hours to be confirmed.[134] Ripple's CEO, Brad Garlinhouse, stated that Ripple can handle 70,000 transactions per second.[135]

An interesting incident regarding the capacity of a blockchain occurred in December 2017, when CryptoKitties, a game on the Ethereum network which allows players to breed and trade virtual cats (with some selling for upwards of USD 100,000), clogged the Ethereum network, causing over 30,000 transactions to be stuck, with some requiring over 20 hours to be verified.[136]

DISTANCE

Other than cash payments, all other payment methods are able to handle long-distance, cross-border transactions.

CONFLICT RESOLUTION

Due to the centralised nature of cash, cards, and payment services, all conflicts can be resolved through the central party (e.g. complaining to the bank).

On the other hand, decentralised blockchains have no central party and all payments are irreversible, meaning there is no way to resolve payment conflicts other than negotiating with the counterparty. This also means that thefts are irreversible, unlike other payment methods where the central party can potentially reimburse victims.

[134] The Sydney Morning Herald, ''Extremely high risk': bitcoin.com co-founder has sold all his bitcoins', 21 December 2017, available at: http://www.smh.com.au/business/markets/bitcoin-as-good-as-useless-says-bitcoin-com-co-founder-20171218-p4yxty.html
[135] Business Insider, 'The value of the world's third biggest cryptocurrency has risen by almost 3,000% this year', 24 July 2017, available at: http://uk.businessinsider.com/ripple-cryptocurrency-has-risen-by-almost-3000-this-year-2017-7
[136] Coindesk, 'Cat Fight? Ethereum Users Clash Over CryptoKitties', 7 December 2017, available at: https://www.coindesk.com/cat-fight-ethereum-users-clash-cryptokitties-congestion/

VERDICT

Despite cash having a significant advantage over other payment methods, its use is limited to face-to-face and short-distance transactions, while the other three methods allow long-distance and cross-border transactions.

In terms of face-to-face transactions, cash is still the superior payment method, given that it is secure, free, and easy to use. For transactions involving greater distance, however, the blockchain system provides an enhanced mechanism to improve upon current offerings.

The blockchain system is extremely secure for both the payee and the payer, protecting the payee as transactions are irreversible and protecting the payer's identity and wealth (in the sense that payments must be pushed). On the other hand, this means that erroneous payments cannot be reversed, and that the payee may need to carry out substantial onboarding processes for AML/CFT reasons.

The level of transaction fee is dependent on the blockchain system itself. Some are completely free to use (e.g. IOTA), some use an optional transaction fee model (e.g. Bitcoin, but at present transaction fees are essentially required), and some will always require a transaction fee (e.g. Stellar). However, given the existence of blockchain systems which charge zero transaction fees, there is pressure on all blockchains to decrease transaction costs. We believe it is likely that the transaction cost of using blockchain systems will be lower than that of current offerings in coming years.

In terms of customer experience or ease-of-use, blockchain systems have the potential to significantly outperform current models. Blockchain systems like Ripple are able to confirm and validate transactions within seconds, which is arguably quicker than cards and payment services, which may take hours (or even days). However, due to their decentralised nature, conflicts can only be resolved through discussions with the counterparties, which may be time consuming and ultimately fruitless.

Banks have been experimenting with incorporating blockchain technology into their operations, and this will be highly similar to the current blockchains, but with an "unfavourable" IDENTITY SECURITY and a "favourable" CONFLICT RESOLVE. Nonetheless, a bank-controlled blockchain system will likely be an enhancement to their current bank offerings (e.g. wire transfer and cards), providing shorter transaction times and potentially lowering transaction fees.

FOR TRANSACTIONS INVOLVING GREATER DISTANCE, THE BLOCKCHAIN SYSTEM PROVIDES AN ENHANCED MECHANISM TO IMPROVE UPON CURRENT OFFERINGS

SECTION 9

THE FUTURE OF CRYPTOCURRENCIES

INDUSTRY OUTLOOK

Although the concept of cryptocurrency was introduced nearly a decade ago, it has only caught the attention of the mass population over the past year, with new revolutions in technology and regulations being implemented. These will all have different effects and implications, generating considerable public interest in the future of cryptocurrencies – both private and fiat ones.

THE FUTURE OF BITCOIN

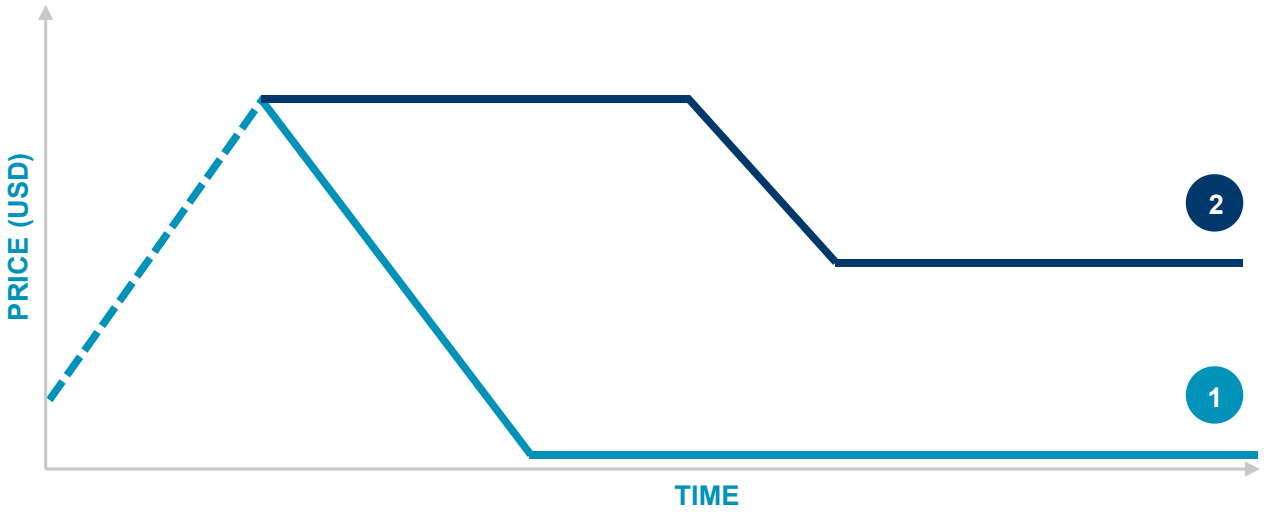
As outlined in Section 6, the significant surge of Bitcoin does appear to be a bubble, deviating considerably from its true underlying value. Our view is supported by a number of commentators in the market, and is also backed by a study by Anglia Ruskin University, Trinity College Dublin, and Dublin City University, with Larisa Yarovaya, a co-author of the report, stating that '[their] evidence finds that the price of Bitcoin has been artificially inflated by speculative investment, putting it in a bubble.'[137]

We believe there are two possible scenarios for BTC in coming years, depending on how its investors use the cryptocurrency in the future (see Figure 53).

EVIDENCE FINDS THAT THE PRICE OF BITCOIN HAS BEEN ARTIFICIALLY INFLATED BY SPECULATIVE INVESTMENT

[137] Reuters, 'Bitcoin hits new record high as warnings grow louder', 15 December 2017, available at: https://www.reuters.com/article/us-global-markets-bitcoin/bitcoin-hits-new-record-high-as-warnings-grow-louder-idUSKBN1E919T

FIGURE 53: POTENTIAL SCENARIOS



	1 USED AS INVESTMENT ASSET (STATUS QUO)	2 USED AS CURRENCY OR PAYMENT METHOD
DETAILS	• Bitcoin users continue to treat BTC as an investment asset, giving it no utility, and hence no value • A "greater fool" ceases to exist, leading to massive sell-offs	• Bitcoin users change their mindset and use BTC as a currency • Regulators try and clamp down on widespread adoption • Bitcoin users realise BTC will not be a "mainstream" currency, leading to sell-offs
PRICE OF BTC	• Plummets due to massive sell-offs	• Decreases rapidly due to sell-offs • Stabilises after certain levels, due to BTC having utility value
USES AFTER CRASH	• Bitcoin enthusiasts may still trade BTC due to nostalgic value • Criminals may use BTC for illegal/grey area transactions due to anonymous nature	• BTC will be used for some transactions • Investors can use BTC as a safe haven asset during political chaos • Criminals may use BTC for illegal/grey area transactions due to anonymous nature

Note visual is for illustrative purposes and is not drawn to scale

Source: Quinlan & Associates analysis

SCENARIO 1 (STATUS QUO)

This scenario occurs if the market continues to treat BTC as an investment asset.

As discussed previously, BTC does not fare well as an asset, and does not have any value as an investment asset. Since BTC's value stems from its utility, investors will eventually realise this scenario cannot be sustained, and the "greater fool" will cease to exist. This will lead to massive sell-offs, panic among investors, and causes the price to plummet.

After the crash, BTC will be kept by enthusiasts for nostalgic reasons (providing it with subjective value). Despite criminals moving onto more private and secure cryptocurrencies, BTC may still be used to facilitate illegal payment transfers, providing it with a low level of utility.

While our cost-based approach to value BTC 1 suggests a price of USD 2,161 for 2017, for reasons outlined in Section 6 (i.e. a non-static level of difficulty in mining), this approach cannot be used to forecast the price of BTC in the future.

Accordingly, we believe it is more appropriate to evaluate BTC price as an asset from the perspective of being a potential inflation hedge and store of value akin to gold (and not a reserve currency), though only a fraction of gold's potential. Due to its scarcity, BTC users will likely only sell it for fiat currency when necessary (e.g. during emergencies). This would see it being priced at USD 548 by 2020, if not considerably lower (see Section 6).

SCENARIO 2

This scenario occurs when BTC users collectively change their mindset and use BTC as a currency or payment method.

Due to the continuously increasing BTC price, a majority of BTC holders need to sacrifice the potential increase in value and spend BTC in transactions for this to happen. As more transactions are being conducted using BTC, the value stabilises, leading to wider adoption.

However, as discussed in Section 3, governments are unlikely to allow mainstream adoption of a non-fiat currency, leading to strict regulations with regards to the usage of BTC. The utility value of BTC would subsequently decrease, given its inability to be used widely as a form of payment for goods and services, leading to sell-offs, and ultimately decreasing the price of BTC.

However, BTC will still have utility as a non-mainstream currency (especially for grey-area transactions) and as a potential safe-haven asset, which means its price should gradually stabilise and not fall as low as the price in Scenario 1.

We believe this scenario will play out in line with our Bear Scenario in Section 6, and BTC 1 will have a value of USD 810 by 2020.

PRIVATE CRYPTOCURRENCIES

As discussed in Section 4, cryptocurrencies in their current form do not satisfy the three main requirements of currencies, nor do they fit the role of an asset (despite some cryptocurrencies being used as assets). If the status quo continues, we believe this will inevitably lead to the bursting of a bubble, given a lack of inherent value (both intrinsic value and utility value).

Cryptocurrencies will only gain utility value if and when they are actually used as currencies. As such, a change in the mindset of cryptocurrency investors is ultimately required. However, if they become mainstream, we envision governments will inevitably regulate the space and restrict their usage. Notwithstanding this, some stakeholders, such as CryptAM's Kevin Loo, believe that regulations are currently very fragmented, and given the current differences (where some countries have banned cryptocurrencies while others regulate them and legitimise them), the cryptocurrency industry will likely survive.

We believe private cryptocurrencies will not be adopted as mainstream currencies, given they allow the mass public to circumvent governments (e.g. tax evasion, money laundering) and undermine economic policies that fiat currencies support (e.g. monetary policy), and governments are therefore unlikely to allow their widespread adoption. Despite underpinned by a revolutionary decentralised system, private cryptocurrencies are unlikely to challenge the money and currency system that we are familiar with today.

As discussed in Section 6, we believe BTC, at its current price, is a bubble waiting to burst, and expect it to trade at or below USD 1,800 by December 2018. The Bitcoin crash will, inevitably, affect the wider private cryptocurrency industry.

After the Bitcoin bubble bursts, the mass population will realise that cryptocurrencies that are designed to function solely as a currency (i.e. without extra utility) have essentially no functional value, and these cryptocurrencies will crash with Bitcoin, mimicking the magnitude of its price drop of ~95% by 2020.

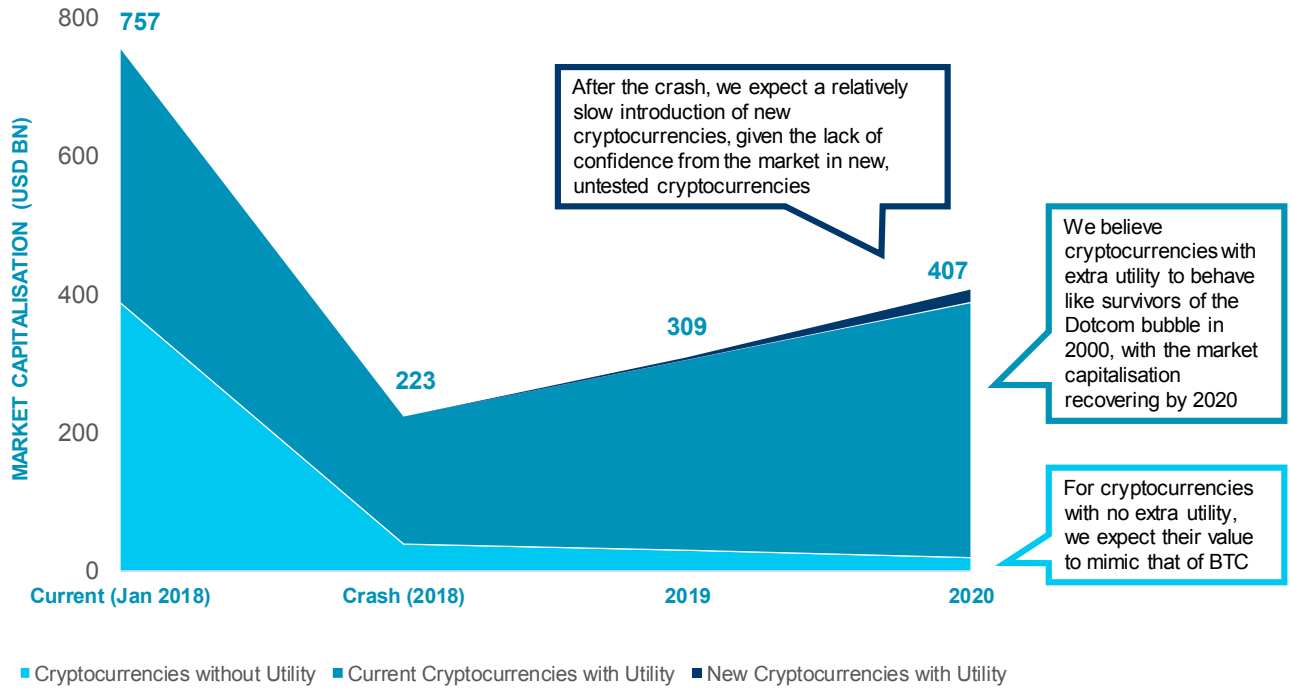
On the other hand, there are cryptocurrencies with added utilities that can be used within their own system. Ether, for example, is used to facilitate the Ethereum system, and therefore has functionality within its own ecosystem (such as the facilitation of smart contracts). Despite having a near zero probability of being mainstream currencies, the utility offered by such cryptocurrencies means they are likely to recover quickly following the burst of the Bitcoin bubble, similarly to eBay, Google, and Amazon post-Dotcom crash. Assuming that these cryptocurrencies behave similarly to surviving technology companies of the Dotcom bubble, we estimate their value to drop by ~50% in 2018, but recovering by 2020.

In addition, there will continue to be new cryptocurrencies coming into the industry. However, we expect cryptocurrencies without significant utility to fall out of favour with the general public. In terms of new cryptocurrencies with utility, we expect a relatively slow introduction due to an extremely low level of confidence in the space by the market (caused inevitably by the bubble burst) and an increased level of caution against new, untested cryptocurrencies. We therefore expect these new cryptocurrencies to add on 1% and 5% of the market capitalisation for cryptocurrencies with utility in 2019 and 2020 respectively.

Based on these values, we arrive at an estimate for the total market capitalisation of private cryptocurrencies in 2020 (see Figure 54).

.

FIGURE 54: PRIVATE CRYPTOCURRENCIES MARKET CAPITALISATION



Source: Quinlan & Associates analysis

By end of 2020, we expect the market capitalisation of private cryptocurrencies to be ~USD 407 billion, representing a ~45% decrease from January 2018. However, a significant proportion of the current private cryptocurrency market is composed of cryptocurrencies without extra utility, and their value is likely to be essentially negligible post-bubble burst. We expect private cryptocurrencies with utility, and hence functional value, to survive the bubble burst, and dominate the private cryptocurrency industry going forward, representing 95% of the market capitalisation.

With our views regarding cryptocurrency and the outlook for BTC, we see an interesting analogy which can be drawn with other realms of technology, such as social media (see Figure 55). While we recognise that internet and blockchain are completely different concepts, their value is built upon network effect (similarly for social media and cryptocurrency).

FIGURE 55: SOCIAL MEDIA AND CRYPTOCURRENCY

UNDERLYING TECHNOLOGY	• Internet	• Blockchain
FUNCTION	• Social media	• Cryptocurrency
EXAMPLES	myspace® a place for friends facebook	bitcoin ethereum

Source: Quinlan & Associates analysis

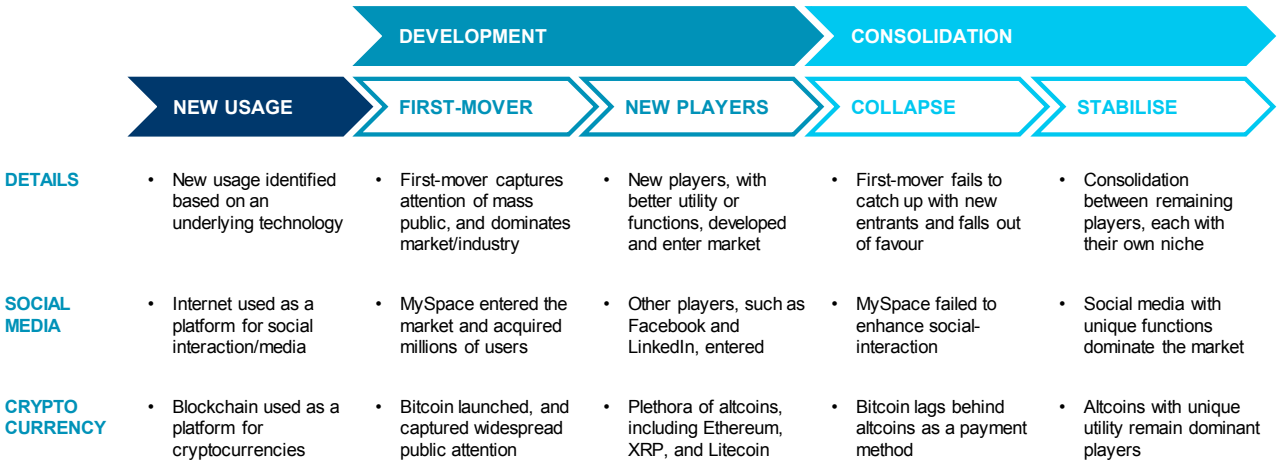
Social media is based on the technology of the internet, while cryptocurrency is based on blockchain technology. Examples of social media sites include MySpace and Facebook, while examples of cryptocurrencies include Bitcoin and Ethereum.

Despite being one of the first-movers and, at its peak, the most dominant player in the market, MySpace now exists as a trailing player within the social media space.[138] Among the main reasons behind its downfall was its failure to keep up with new market entrants, who offered improved functionality and a better user experience.

Similarly, BTC, in its current form, trails behind several altcoins in terms of its function as a medium of exchange, given its slower transaction times, considerable transaction fees (despite technically being optional), and lower levels of privacy and anonymity. It also lacks additional utility beyond acting a medium of exchange, such as the ability to support smart contracts (like Ethereum). Consequently, as a technology, it trails many of its peers, and we believe it will gradually fall out of favour with investors and cryptocurrency users in favour of more technologically advanced altcoins (see Figure 56).

[138] Los Angeles Times, 'How MySpace fell off the pace', 17 June 2009, available at: http://articles.latimes.com/2009/jun/17/business/fi-ct-myspace17

FIGURE 56: SOCIAL MEDIA AND CRYPTOCURRENCY



Source: Quinlan & Associates analysis

If we look more closely at the social media space, we can see it is currently dominated by a handful of major players, who are surrounded by an ecosystem of additional, smaller players, focused on a specific niche.

Facebook, for example, has positioned itself as one of the most dominant players in the social media world, acting as a platform for users to deploy apps or other social media sites, such as dating apps or Instagram (through the "Login Using Facebook" function). Other platforms such as LinkedIn act as the world's professional career and networking site, while Snapchat has carved out a niche as a "cheeky" version of social media.

We see the cryptocurrency space evolving in a very similar fashion. Cryptocurrencies that act as a "platform" for other applications, or those that provide additional utility such as Ethereum (e.g. providing a network for dapps and smart contracts), are likely to take on the role as the Facebook of the cryptocurrency world. Cryptocurrencies like Monero (with its highly private and anonymous usage) and IOTA (with its free usage) will likely make up the market of remaining niche players, akin to the position of LinkedIn and Snapchat in social media, bringing niche functionality to the digital currency space.

As mentioned in Section 5, despite BTC having upgrades lined up, we see their development and implementation being significantly slower than many altcoins'. Therefore, while serving as a first-mover, we believe BTC is likely to become a technological straggler within the broader cryptocurrency ecosystem. As with any technological laggard, this will further reinforce downward pressure on its value, as well as the value of other private cryptocurrencies that fail to provide additional utility.

FIAT CRYPTOCURRENCIES

Several countries have considered or experimented with the idea of a fiat cryptocurrency. The People's Bank of China (PBOC) was the first central bank to test a fiat cryptocurrency,[139] while Venezuela considered launching the petro, a cryptocurrency backed by Venezuelan oil reserves.[140] Some countries trialling cryptocurrencies include Japan, Sweden, and Estonia, with project J-coin, E-Krona, and Estcoin respectively.[141] Singapore will also be experimenting with a digital version of SGD as part of its Project Ubin[142] in 2018.[143]

Even though no country has fully launched its own fiat cryptocurrency, there will be more research, reports, and news of the potential establishment of a central bank digital currency in coming months. However, it will take the population a long time to fully understand and use fiat cryptocurrency. Accordingly, cash will continue to be the dominant currency and payment system over the next few years.

Fiat cryptocurrencies will most likely have a faster adoption rate in cashless societies, as the population is already used to alternative payment methods. We see fiat cryptocurrency starting off as an enhancement to the current payment system, facilitating a small proportion of transactions, and eventually slowly replacing cash and other payment methods through ongoing education and promotion efforts.

To determine the future potential of fiat cryptocurrencies, we sought to estimate the total money supply in the form of government-issued cryptocurrency by 2020.

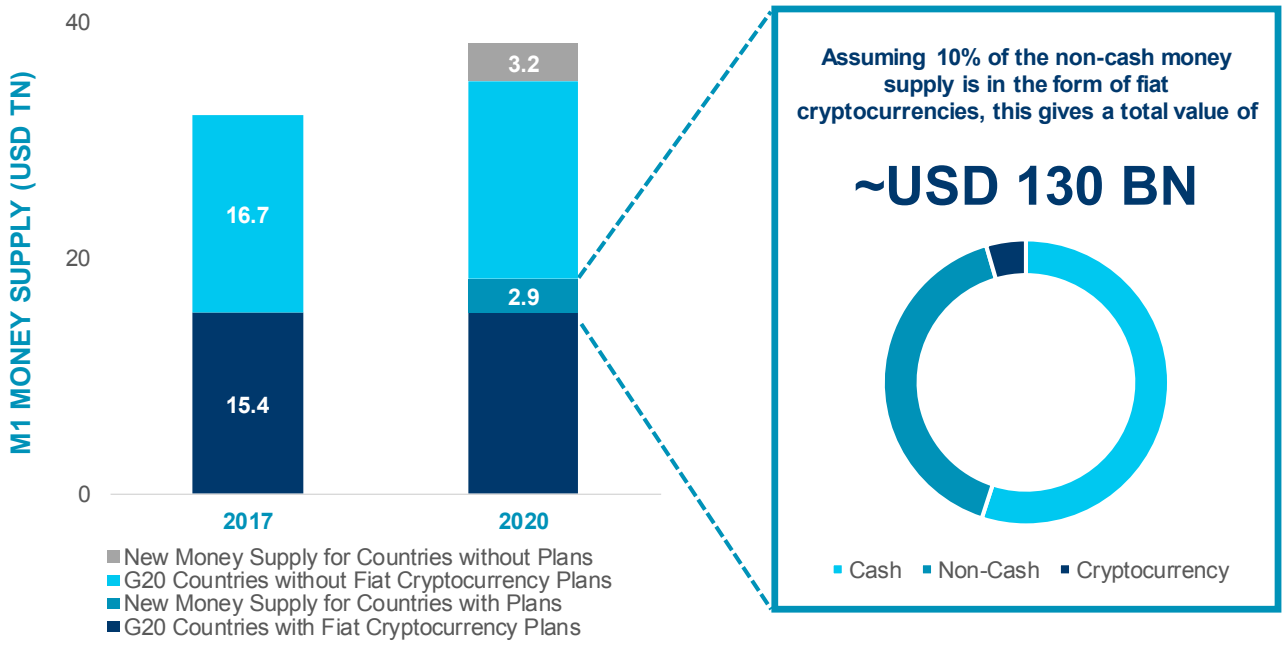
Given the slower speed of government projects relative to private projects, we believe for a country to launch its fiat cryptocurrency by 2020, significant research and experimentation needs to either be in progress or completed by the end of 2017. Within G20, only Canada,[144] China,[145] India,[146] Japan,[147] Russia,[148] and Saudi Arabia,[149] have made such progress.

[139] Caixin, 'PBOC Set to Be First to Issue Digital Bills', 26 January 2017, available at: https://www.caixinglobal.com/2017-01-26/101049103.html
[140] Bloomberg, 'Get Set for Petro, Venezuela's Cryptocurrency Answer to Bitcoin', 29 December 2017, available at: https://www.bloomberg.com/news/articles/2017-12-29/get-set-for-petro-venezuela-s-cryptocurrency-answer-to-bitcoin
[141] CNBC, 'Next stop in the cryptocurrency craze: A government-backed coin', 30 November 2017, available at: https://www.cnbc.com/2017/11/30/cryptocurrency-craze-springboards-government-backed-coin.html
[142] Project Ubin is a 5-stage project, which experiments with using blockchain technology for (1) a proof-of-concept design to conduct inter-bank payments, (2) different models for inter-bank payments, (3) delivery of securities, (4) cross-border payments, and (5) a digital version of SGD
[143] CNBC, 'Singapore aims to finish its own cryptocurrency trial next year', 26 October 2017, available at: https://www.cnbc.com/2017/10/26/singapore-cryptocurrency-blockchain-trial.html
[144] CNC News, 'Bank of Canada weighs merits of creating a digital currency', 30 November 2017, available at: http://www.cbc.ca/news/business/bank-canada-digital-currency-1.4426580
[145] Forbes, 'After Cracking Down On Bitcoin, China Contemplates Its Own Digital Currency', 19 October 2017, available at: https://www.forbes.com/sites/sarahsu/2017/10/19/will-china-host-the-worlds-biggest-state-backed-digital-currency/#2cee40e12319
[146] Coindesk, 'Indian Central Bank Studies 'Fiat Cryptocurrency' for Digital Rupee', 13 September 2017, available at: https://www.coindesk.com/indian-central-bank-studies-fiat-cryptocurrency-for-digital-rupee/
[147] Financial Times, 'Japan's big banks plan digital currency launch', 26 September 2017, available at: https://www.ft.com/content/ca0b3892-a201-11e7-9e4f-7f5e6a7c98a2
[148] The Merkle, 'Russia to Launch Its Own Digital Currency, the CryptoRuble', 17 October 2017, available at: https://themerkle.com/russia-to-launch-their-own-digital-currency-the-crypto-ruble/
[149] TrustNodes, 'Saudi Arabia to Issue a Digital Currency', 5 October 2017, available at: http://www.trustnodes.com/2017/10/05/saudi-arabia-issue-digital-currency

Taking these countries, we estimated and totalled their new money supply by 2020. Within more developed countries in the G20, cash is still the dominant payment method, accounting for ~60% of all transactions.[150]

As the global population continues to migrate to alternative, non-cash payment methods, we assume non-cash to make up 45% of all transactions by 2020, up from 40% in 2017. Of this 45% of new, non-cash money supply, we assume only 10% to be in the form of fiat cryptocurrency (see Figure 57).

FIGURE 57: TOTAL FIAT CRYPTOCURRENCY VALUE



Source: CEIC, Quinlan & Associates analysis

This gives a total value of ~USD 130 billion for fiat cryptocurrencies in G20 in 2020. Extrapolating this to the rest of the world gives a value of ~USD 150 billion for fiat cryptocurrencies globally in 2020.

Note that the estimation for the 2020 value of fiat cryptocurrencies is significantly lower than that of private cryptocurrencies. However, we believe this is due to the head-start that private cryptocurrencies have, as well as the abundance of substitutes that are currently available for fiat cryptocurrencies (e.g. cash, alternative payment methods).

[150] Statista, 'Proportion of cash and non-cash payments worldwide in 2015, by region', available at: https://www.statista.com/statistics/585858/cash-vs-non-cash-payments-by-region/

BLOCKCHAIN

Unlike private cryptocurrencies that lack any associated utility, blockchain technology is here to stay. Governments and financial institutions have already, or are starting to, research, experiment, and incorporate the technology into their operations.

A critical point of difference between current cryptocurrencies and blockchain technology is that current cryptocurrencies are designed to challenge and replace the current system. Blockchain technology, on the other hand, can be utilised to enhance the current system. Consequently, blockchain technology and its applications are actively studied by various stakeholders (from businesses to financial institutions through to governments), while current cryptocurrencies face immense levels of pushback.

Despite being an innovative system and gaining enthusiastic support from the public and investors, current cryptocurrencies are unlikely to be a successful revolution in challenging the position of fiat currencies in the foreseeable future. However, the underpinning blockchain technology will benefit us all, through providing a faster and more secure system, with considerable scope to enhance current offerings.

CONCLUSION

Given the extremely low likelihood of BTC ever being a mainstream currency, and our valuations of BTC (both as an asset and as a currency), we believe Bitcoin, in its current form, is a bubble waiting to burst.

BTC is currently trading at ~USD 14,000, ~10 times higher than our current valuations. We expect to see a large correction in the BTC price in 2018, and we forecast a price at or below USD 1,800 by December 2018.

As mentioned, Bitcoin is currently the most well-known cryptocurrency; not because of its superior functionality, but because it was the first popular cryptocurrency and had a first-mover advantage. A wide range of other cryptocurrencies have since been developed which function better as currencies than BTC.

Moreover, we believe governments are unlikely to allow the widespread adoption of an uncontrollable currency, and the population will eventually realise BTC has virtually no utility as a currency. And when the price of BTC does start to tumble, a fear of holding on (FOHO) will drive a mad rush for the exits as investors look to avoid being caught in a vicious downward price spiral.

After the burst of the Bitcoin bubble, the effects on other cryptocurrencies will depend on the nature of the cryptocurrency itself. We believe cryptocurrencies that compete directly against Bitcoin that are designed solely for the purpose of being a currency (such as the forks of Bitcoin) will follow the crash of Bitcoin, while cryptocurrencies with extra utility (be it within their own ecosystems or within the wider financial industry) will likely survive and continue to co-exist with the current system.

With an extremely unfavourable future forecast for the price of BTC, as well as the fact that Bitcoin is unlikely to ever achieve the status of a mainstream currency, current valuations suggest these digital tulips are very much fool's gold.

WITH AN EXTREMELY UNFAVOURABLE FUTURE FORECAST FOR THE PRICE OF BTC, AS WELL AS THE FACT THAT BITCOIN IS UNLIKELY TO EVER ACHIEVE THE STATUS OF A MAINSTREAM CURRENCY, CURRENT VALUATIONS SUGGEST THESE DIGITAL TULIPS ARE VERY MUCH FOOL'S GOLD

SECTION 10

HOW WE CAN HELP

HOW WE CAN HELP

Our consultants have the capabilities and knowledge to strategise, implement, and monitor systems related to cryptocurrencies.

As outlined in our report, there are several stakeholders who need to be proactive about ongoing changes occurring in the industry.

BANKS AND BROKERS

Position banks and brokers to successfully enter and compete in the crypto trading space:

- Identify appropriate arbitrage and market-making opportunities
- Develop a framework for cryptocurrency trading operations, including detailed risk and compliance controls
- Conduct comprehensive market sizing and shortlisting of potential clients and strategically suitable cryptocurrencies

FINTECH START-UPS

Identify opportunities to leverage technical know-how to outmanoeuvre the competition:

- Assist in preparation of whitepapers and design of token concepts to maximise firm valuation and long-term utility of technology
- Work with firms to facilitate Initial Coin Offerings (ICOs) to both the general public and institutional investors
- Carry out a market landscape analysis including industry and regulatory response

GOVERNMENTS AND REGULATORS

Determine appropriate regulatory stance to ensure sound market practices whilst encouraging continued innovation:

- Analyse uses of cryptocurrencies in conjunction with existing fiat currencies, including effects on monetary policy and the wider economy
- Design a roadmap for the development and deployment of fiat cryptocurrencies
- Evaluate and estimate the effect of different cryptocurrency-related taxation policies

EXCHANGES AND FUND MANAGERS

Identify opportunities for funds to capitalise on rising investor interest in cryptocurrencies:

- Define unique selling points and business models to effectively raise capital and funds
- Provide guidance on crypto-portfolio allocation and construction
- Calculate value of different types of cryptocurrencies to identify investment opportunities

VENTURE CAPITALISTS

Adaptations to business models to remain relevant in the wake of ICOs:

- Develop marketing strategy to attract FinTech start-ups in need of capital or in the process of Initial Coin Offerings (ICOs)
- Design valuation/investment assessment frameworks for FinTech start-ups and their tokens

SECTION 11

APPENDIX

APPENDIX A

EXAMPLE CRYPTOCURRENCIES

	MARKET CAPITALISATION (AS AT 31 DEC 2017)	KEY FEATURES: TRANSACTION TIME	KEY FEATURES: PRIVACY	KEY FEATURES: SMART CONTRACT/ APPLICATIONS	OTHERS FEATURES
CARDANO	• USD 17.9 billion		✓	✓	
LITECOIN	• USD 11.8 billion	✓			
IOTA	• USD 9.3 billion	✓			• Free transactions
NEM	• USD 8.4 billion				• Proof-of-importance
DASH	• USD 7.8 billion	✓	✓		
STELLAR	• USD 5.7 billion	✓			• Asset freeze
NEO	• USD 4.6 billion			✓	• ”Sharding”
LISK	• USD 2.2 billion			✓	
ZCASH	• USD 1.4 billion		✓		
VERTCOIN	• USD 261.8 million				• ASIC-resistant

Source: cryptocurrency website, Quinlan & Associates analysis

CARDANO

Cardano is a blockchain platform, and has a native token, ADA. Cardano has two layers; a settlement layer which facilitates transactions and a control layer which executes smart contracts. The protocol of Cardano is designed to protect the privacy of users while complying with regulations. A treasury system has also been established to ensure sustainability and development for the infrastructure.

LITECOIN

Litecoin was introduced on 7 October 2011, and is a fork of the Bitcoin Core client. Litecoin is very similar to Bitcoin, but has a few key differences, including a shorter blocktime of 2.5 minutes (as opposed to Bitcoin’s 10 minutes), a limit of 84 million Litecoins (as opposed to Bitcoin’s 21 million), and a different proof-of-work algorithm. Nonetheless, the industry often compares Litecoin to Bitcoin due to their similar structure and internal targets set by the system.

IOTA

Introduced on 11 June 2016, IOTA focuses on secure communications and transactions between devices on the "Internet of Things". Instead of using a blockchain, IOTA uses a directed acyclic graph[151] technology (known as the "tangle"). To send out a transaction, a user must validate two previous, random transactions. Because of IOTA's design, its transactions are free, transactions times are short, and the system can scale easily. In addition to transactions, IOTA enables data transfer and voting through the system.

NEM

NEM was released on 31 March 2015, and its main feature is its proof-of-importance system (instead of the more popular proof-of-work and proof-of stake). Despite being highly similar, proof-of-importance takes into account a wallet's wealth and volume of transactions while proof-of stake considers a wallet's wealth and time held. As such, a proof-of-importance mechanism encourages using the cryptocurrency, instead of hoarding it.

DASH

Released in 18 January 2014, Dash, originally XCoin, is designed to be the most user-friendly cryptocurrency available on the market. Dash uses a two-tier network, with the first tier validating transactions (like miners on Bitcoin) and the second tier (called the masternodes) handling add-on functions, including PrivateSend (which makes transactions untraceable) and InstantSend (which allows instant transactions). The masternodes are also responsible for choosing and financing projects with benefit and enhance Dash.

STELLAR

Stellar was launched in 2015, and is used mainly as a payment infrastructure. In fact, Stellar was originally based on Ripple (an arguably more popular decentralised payment network). Stellar's native currency is Lumens, which is used for transaction fees (0.0001 lumens per transaction to prevent spam), to ensure authenticity (all accounts must hold 20 lumens), and to facilitate multi-currency transactions. An interesting feature of Stellar is the function to allow a user to freeze assets the user issued, in order to protect erroneous payments.

NEO

NEO, formally known as Antshares, is sometimes referred to as "Chinese Ethereum. NEO system supports smart contracts (similar to Ethereum), digitised assets, and digital identity, in order to facilitate a smart economy. NEO uses a proof-of-stake system and a "sharding system", which splits up the workload of transaction validation among divided sections of the network to allow quicker handling of transactions.

LISK

Lisk's ICO raised USD 5.8 million, the second most successful ICO at the time, and was subsequently released on 24 May 2016. Lisk is a blockchain platform that helps facilitate decentralised apps and runs each app on a sidechain, which is separated from the main blockchain. Lisk uses a delegated-proof-of-stake mechanism, which differs from proof-of-stake by having only the top 101 delegates secure the network, and is arguably a more efficient and flexible consensus model.

[151] A directed acyclic graph is a collection of interconnected chains, while blockchain is one single chain; note that a blockchain is a special example of directed acyclic graphs

ZCASH

Zcash was introduced on 28 October 2016, and focuses on privacy. Zcash provides users with an option to hide transaction details, including payer, payee, and amount transferred. Zcash also has a selective disclosure feature, which allows users to add notes or details to transactions, which can then be shown to selected people or parties, helping users to comply with tax or anti-money laundering regulations. Zcash uses zero-knowledge proofs, which allow validation of fully encrypted transactions, and therefore protecting the user's privacy.

VERTCOIN

Released on 8 January 2014, Vertcoin is designed to resist centralised mining, with developers pledging to take any steps necessary to protect Vertcoin from ASICs and multipool mining. Vertcoin implements ASIC-resistant proof-of-work mechanisms, allowing individuals to mine Vertcoins with consumer grade hardware. Vertcoin has already forked twice to use different mechanisms, due to the threat of centralised mining.

APPENDIX B

CRYPTOCURRENCY EXCHANGES

EXCHANGE	COUNTRY/BASE	CRYPTOCURRENCY	TRANSACTION FEES	ADDITIONAL FEATURES
COINCHECK	• Japan	• BTC • Ether • Litecoin • (Total 13)	• Maker: 0% • Taker: 0%	• Coincheck Lending • Coincheck Payment; accept BTC and receive JPY • Coincheck exchange
OKEX	• China	• Litecoin • BTC • Ether • (Total 42)	• Maker: 0% • Taker: 0%	
POLONIEX	• US	• Litecoin • Bitcoin • Ether • (Total 99)	• Maker: 0% - 0.15% • Taker: 0.05% - 0.25%	
HITBTC	• Hong Kong	• Bitcoin Cash • BTC • Ether • (Total 344)	• Maker: 0.1% • Taker: 0.1%	• Leading API for trading bot with low latency data ad execution fees
BITSTAMP	• Luxembourg	• BTC • Litecoin • Ether • (Total 14)	• Maker: 0.1% - 0.25% • Taker: 0.1% - 0.25%	• Stop price at certain level
COINONE	• South Korea	• BTC • Ether • (Total 8)	• Maker: 0.02% - 0.1% • Taker: 0.02% - 0.1%	
KRAKEN	• US	• BTC • Ether • Litecoin • (Total 17)	• Maker: 0% - 0.16% • Taker: 0.1% - 0.26%	• Considered to be one of the safest exchanges
HUOBI	• China	• BTC • Ether • Litecoin • (Total 51)	• Maker: 0.2% • Taker: 0.2%	
BITFLYER	• Tokyo	• BTC • Ether • Bitcoin Cash	• Maker: 0.0% • Taker: 0.0%	

EXCHANGE	COUNTRY/BASE	CRYPTOCURRENCY	TRANSACTION FEES	ADDITIONAL FEATURES
GEMINI	• US	• BTC • Ether • Bitcoin Cash • Ripple	• Maker: 0% - 0.25% • Taker: 0.1% - 0.25%	• First US exchange licensed for BTC and ether trading
KORBIT	• Korea	• BTC • Ether • Monero • Zcash	• Maker: 0% - 0.08% • Taker: 0.01 - 0.20%	• Longest running Korean exchange • Stores customers deposits offline in 'cold wallets'
QUOINE	• Japan	• BTC • Ether • Bitcoin Cash	• Maker: 0.1% - 0.25% • Taker: 0.1% - 0.25%	• Quoine has other special features like futures trading, algo trading, and even lending
LAKEBTC	• China	• BTC	• Maker: 0% - 0.15% • Taker: 0.2%	• Big Four exchange in Coindesk
ZAIF	• Japan	• BTC • NEM • Monacoin • (Total 10)	• Maker: -0.05% - 0% • Taker: -0.01 - 0.1%	• Allows margin trading and offers an affiliate program
FISCO	• Japan	• BTC • Monacoin	• Maker: 0% • Taker: 0%	
BTCBOX	• Japan	• BTC • Litecoin • Ether • Bitcoin cash	• Maker: 0% • Taker: 0%	
ZB.COM	• China	• BTC • Bitcoin Cash • Litecoin • (Total 16)	• Maker: 0% - 0.1% • Taker: 0% - 0.1%	• Insurance of up to USD 250,000 per customer
WEX	• Russia	• BTC • Litecoin • Ether • (Total 10)	• Maker: 0.2% • Taker: 0.2%	

Note the aforementioned list focuses on cryptocurrency exchanges with a 24h volume of over USD 100 million at the time of production; empty cells mean information is inapplicable or not available by the time of publication

Source: CoinMarketCap, exchange websites, Quinlan & Associates research

APPENDIX C

STAKEHOLDER PERSPECTIVES

	PERSON	POSITION	INSTITUTION	VIEW ON CURRENT CRYPTO
ASSET MANAGEMER / HEDGE FUND	WARREN BUFFETT	CEO	Berkshire Hathaway	✖
	LARRY FINK	CEO	Blackrock	✖
	ABIGAIL JOHNSON	CEO	Fidelity	✓
	BILL MILLER	Founder	Miller Value Partners	–
	KYLE BASS	Founder	Hayman Capital Management	✓
	RAY DALIO	Co-Chairman and Founder	Bridgewater Associates	✖
	HOWARD MARKS	Co-Chairman and Co-Founder	Oaktree Capital Management	✖
CENTRAL BANK	CHRISTINE LAGARDE	Managing Director	International Monetary Fund	–
	BEN BERNANKE	Former Chairman	Federal Reserve	✖
	VITOR CONSTANCIO	Vice President	European Central Bank	✖
	MARK CARNEY	Governor	Bank of England	–
	HARUHIKO KURODA	Governor	Bank of Japan	–
	RAVI MENON	Managing Director	Monetary Authority of Singapore	–
	ELVIRA NABIULLINA	Governor	Central Bank of Russia	✖
NOBEL PRIZE WINNER	ROBERT SHILLER	Sterling Professor of Economics	Yale University	✖
	PAUL KRUGMAN	Distinguished Professor of Economics	City University of New York	✖
TECH	PETER THIEL	Co-Founder	Paypal	✓
	BILL GATES	Co-Founder	Microsoft	✓
	ERIC SCHMIDT	Chairman	Alphabet	–
	RICHARD BRANSON	Founder	Virgin	✓

✖ Negative – Neutral ✓ Positive

Source: Quinlan & Associates analysis

It is worth noting that on this list, individuals with a financial services background are generally against current cryptocurrencies.

APPENDIX D

VIEWS ON BITCOIN BY COUNTRY

AMERICAS		EMEA				APAC	
COUNTRY	VIEW ON BITCOIN	COUNTRY	VIEW ON BITCOIN	COUNTRY	VIEW ON BITCOIN	COUNTRY	VIEW ON BITCOIN
BOLIVIA		AUSTRIA		JORDAN		AUSTRALIA	
BRAZIL		BELGIUM		JERSEY		BANGLADESH	
CANADA		BULGARIA		KYRGYZSTAN		CHINA	
COLOMBIA		CROATIA		LEBANON		HONG KONG	
ECUADOR		CYPRUS		LUXEMBOURG		INDIA	
MEXICO		CZECH REPUBLIC		MOROCCO		INDONESIA	
UNITED STATES		EU (ECB)		NETHERLANDS		JAPAN	
		FINLAND		POLAND		MALAYSIA	
		GERMANY		PORTUGAL		NEW ZEALAND	
		GREECE		RUSSIA		PHILIPPINES	
		HUNGARY		SERBIA		SINGAPORE	
		ICELAND		SLOVENIA		SOUTH KOREA	
		IRAN		SOUTH AFRICA		TAIWAN	
		IRELAND		SWITZERLAND		THAILAND	
		ISLE OF MAN		U.A.E.		VIETNAM	
		ISRAEL		UNITED KINGDOM			
		ITALY					

Strongly Negative
Negative
Neutral/No Comment
Positive
Strongly Positive

Source: Perkins Coie,[152] Quinlan & Associates analysis

[152] Perkins Coie, 'Digital Currencies: International Actions and Regulations', December 2017, available at: https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html

It is clear that the majority of governments have a negative view on Bitcoin and other cryptocurrencies.

Those with “Strongly Negative” views have generally restricted financial institutions from dealing with BTC, or outright banned the usage (usage is punishable by law). Governments with “Negative” views have mainly issued warnings against the risk of using cryptocurrencies, and expressed concerns in the AML/CFT perspectives.

“Neutral” governments are still investigating and considering potential actions, but BTC.

Governments with “Positive” views have implemented certain regulations, which legitimise the existence and usage of Bitcoins and other cryptocurrencies. Isle of Man is the only “Strongly Positive” country, where BTC can be accepted as cash and the government has expressed an intention to build up a virtual currency infrastructure to promote the business.

QUINLAN
&ASSOCIATES

STRATEGY WITH A DIFFERENCE

QUINLAN
&ASSOCIATES

CONTACT US

@ info@quinlanandassociates.com

www.quinlanandassociates.com

(+852) 2251 8725

Level 19, Two International Finance Centre,
8 Finance Street, Central, Hong Kong SAR