FOCUS

Cryptocurrencies: revolution or illusion?

Vendredi, 06/08/2018

The blockchain technology is revolutionary and could be a game changer in many industries. Bitcoin is the first visible application of the blockchain, and is one way to be exposed to the technology. However, trying to value it today is almost impossible. 'Investing' in a cryptocurrency is a bet on it being accepted as a global monetary standard and used on a wide scale.

Reto Gehring
Senior Analyst

Executive summary

- Blockchain technology is revolutionary and could be a game changer in many industries.
- Bitcoin is the first visible application of the blockchain, and is one way to be exposed to the technology. However, trying to value it today is almost impossible.
- 'Investing' in a cryptocurrency is a bet on it being accepted as a global monetary standard and used on a wide scale.
- As one allocation in a portfolio of different assets, cryptocurrencies offer diversification benefits, thanks to the low correlation to traditional assets.

Blockchain vs Cryptocurrency

Before discussing the main cryptocurrencies, we first analyse and explain the underlying technology: the blockchain. We also pinpoint the main differences between the first decentralised cryptocurrency, the bitcoin, and a second generation one, the ethereum.

Is a cryptocurrency a 'currency'?

There is a debate concerning whether a cryptocurrency can be designated a currency or if it shows characteristics of an asset, a commodity, or is simply a new asset class. The three main functions a currency must fulfil are as a) a medium of exchange, b) a unit of account and c) a store of value. Taking bitcoin as an example, these functions have not been fulfilled and we believe it is unlikely to become a currency in future.

Fair value of a cryptocurrency

Price does not mean value. To invest in a cryptocurrency, there must be a rationale behind its price, denominated in an understood measurement standard like the US dollar or the euro. The factors influencing the price of a cryptocurrency are numerous and in this section we try to determine a fair price for bitcoin.

Investing in cryptocurrencies

There are several routes to investing in cryptocurrencies either directly or indirectly. This section gives an overview of the main alternatives to acquiring cryptocurrencies directly - mining, barter, ATMs, trading platforms - or indirectly through futures, ETFs and ETNs, structured products and funds.

I. INTRODUCTION

During 2017, the price of the bitcoin, the most well-known cryptocurrency, multiplied by a factor of about 13. This attracted much attention not only from the investment community, but also from the general public. Indeed, the magnitude of the appreciation sparked strong appetite for this 'thing' and many jumped on the bandwagon in a bid not to miss this 'never-seen-in-history' investment opportunity[1]. However, the exuberant returns came hand-in-hand with unparalleled volatility, as the last weeks of 2017 and the first few months of 2018 demonstrated. This popularity also generated a heated debate about the economic fundamentals of bitcoin and other cryptocurrencies. Academics, investment professionals, government officials and even celebrities have voiced their views on this subject. Supporters put forward the disintermediation and efficiency gains cryptocurrencies allow, while detractors claim that the fundamental value of bitcoin is zero. The goal of this paper is to give some historical and technological background on cryptocurrencies and bitcoin in general. This will help establish whether a cryptocurrency is a currency or any other type of asset. With this foundation, we can discuss a potential fair value of cryptocurrencies such as the bitcoin and analyse the risks and opportunities of the different investment opportunities.

[1] www.marketwatch.com/story/why-bitcoin-is-now-the-biggest-bubble-in-history

II. BLOCKCHAIN VS CRYPTOCURRENCY

Blockchain, definition and history

1. Definition

To fully understand cryptocurrencies, we first need to address the underlying technology: the blockchain. The blockchain is a continuously-growing electronic record of transactions, called blocks, which are linked and secured using cryptography. For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks.

2. History

The creation of the blockchain is linked to that of the bitcoin. Bitcoin written with a capital 'B' refers to the technology, in lower case to the currency. Indeed, the bitcoin is the first application of the Bitcoin blockchain. They were both created in 2009 by an expert in cryptography, known under the pseudonym Satoshi Nakamoto. This individual or group of persons – his/their true identity remains unconfirmed to date – is close to the cyberpunk movement, which emphasises the need for privacy. Initially, the use of Bitcoin and blockchain remained confined to cryptography enthusiasts with no real-world utility. In 2010, bitcoin was used for its first transaction for a real-life good, a pizza. In October 2011, a second cryptocurrency, the Litecoin, was launched. The blockchain is still the underlying technology, but the mining algorithm is different. We waited until June 2012 for the launch of the third cryptocurrency, the Ripple.

However, the most significant evolution came with the development and release of the Ethereum protocol in August 2015. It allowed for the creation of smart contracts (transactions that settle automatically when predefined conditions are met) and opened a whole new world of applications. It also allowed for the creation of tokens (digital assets created on top of Ethereum, released typically through crowd sales), further increasing the number of cryptocurrencies. Since then, many other cryptocurrencies have been released and there are currently 1,560 cryptocurrencies[1]. Not all of them use the original blockchain behind the bitcoin, but the technology has the same foundations.

[1] Source: coinmarketcap.com, April 2018

Basic principles of the blockchain technology

1. Distributed database

Each party on a blockchain has access to the entire database and its complete history. No single party controls the data or the information. Every party can verify the records of its transaction partners directly, without an intermediary.

2. Peer-to-peer transmission

Communication occurs directly between peers, instead of through a central node. Each node (computer connected to the network) stores and forwards information to all other nodes.

3. Transparency with 'pseudonymity'

Every transaction and its associated value is visible to anyone with access to the system. Each node, or user, on a blockchain has a unique 30-plus-character alphanumeric address that identifies them. Users can choose to remain anonymous or provide proof of their identity to others. Transactions occur between blockchain addresses.

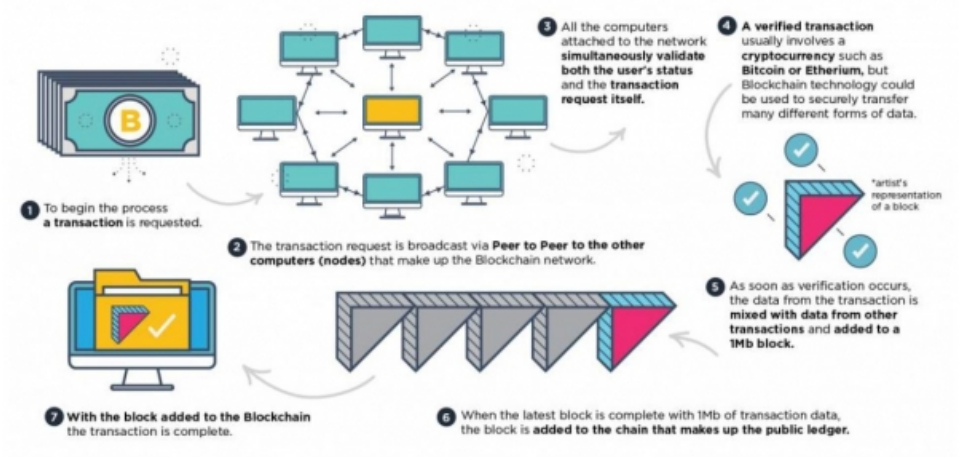
4. Irreversibility of records

Once a transaction is entered in the database and the accounts are updated, the records cannot be altered, because they are linked to every transaction record which took place before them. Hence the term 'chain'. Various computational algorithms and approaches are deployed to ensure that the recording on the database is permanent, chronologically ordered, and available to all others on the network.

5. Computational logic

The digital nature of the ledger means that blockchain transactions can be tied to computational logic and, in essence, programmed. So, users can set up algorithms and rules that automatically trigger transactions between nodes.

How does a blockchain work?



Source

Illustrated by the chart above, bitcoin is the first application of a blockchain. Bitcoins can be transferred from A to B without the help of any bank or usual money transfer channel. Everything is generated in the blockchain and is transparent to all participants. Source: BestVPN.com

First generation cryptocurrency: Bitcoin

1. Definition

Bitcoin is a cryptocurrency – a digital unit of exchange operating on a decentralised, peer-to-peer network. As already stated, bitcoin is the first application of the blockchain. The first block was mined by Satoshi Nakamoto in January 2009, after he published his white paper titled 'Bitcoin: A Peer-to-Peer Electronic Cash System' in October 2008.

2. How it works

Participants on the network transmit data that allow the proof and transfer of ownership, without the need for a trusted third party. Instead of owning coins, bitcoin users possess two unique strings of characters or 'keys': a public key, much like a bank account number for sending/receiving bitcoins, and a private key, comparable to a PIN that allows the owner to spend their coins. Every bitcoin transaction is recorded in a string of data containing details including the addresses of the sender/receiver and the value being transferred. These details are transmitted to the network for inclusion in a public ledger known as the blockchain. Network participants called 'miners' then use computing power and cryptography to repackage data from verified transactions into a "block" that is uniquely identifiable to everyone else on the network and linked to the prior block in the chain. The first miner to complete this process is awarded with new bitcoins, and he also receives the transaction fee associated to all transactions in that block. Once transactions become part of the ledger, it is almost impossible for them to be modified or reversed (see section Fork).

3. Market capitalisation

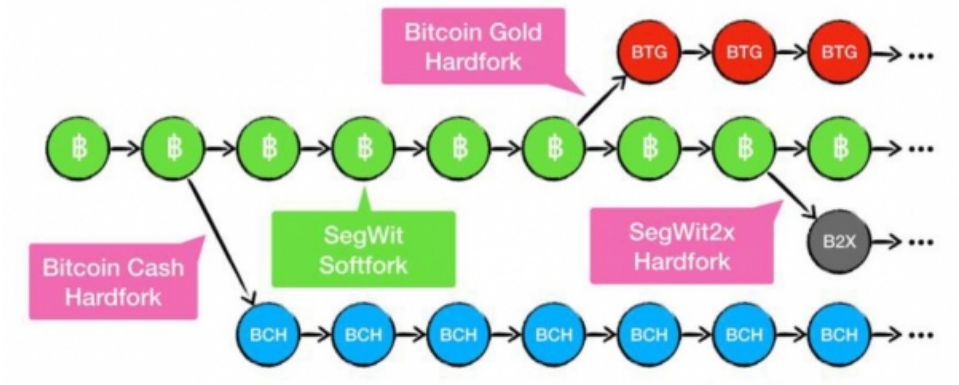
The theoretical total supply of bitcoins is fixed at 21m coins. The limit of 21m bitcoins is 'hard-coded' into the protocol. Theoretically, this quantity will have been completely mined circa by year 2140. However, it was estimated in 2017 that up to 25% of the bitcoins mined so far have been lost for good, due to accidental losses and willful destruction. The total supply of bitcoins outstanding is currently 16,985,700[1].

4. Fork

For a cryptocurrency, a 'fork' is a change of the original protocol at a specific point in time. A fork can be implemented to correct important security issues found in older versions of the software, to add new functionalities, or to reverse transactions. Once a fork is implemented, the blockchain of a cryptocurrency is split into two different blockchains with identical histories before the fork date. A fork is a permanent divergence from the previous version of the blockchain, and nodes running previous versions will no longer be accepted by the newest version. A hard fork creates two valid blockchains, whereas a soft fork results in keeping the original blockchain. To create a fork, the majority of miners must agree on the proposed protocol changes. In bitcoin history, the first hard fork happened in August 2017, resulting in the creation of the Bitcoin Cash, and the second one was effective in October 2017, creating the Bitcoin Gold. In February 2018, the Bitcoin Private was created as a merge fork of Bitcoin and Zclassic, another cryptocurrency. At the end of 2017, there was a hard fork proposal called SegWit2x to double the capacity of every block in the blockchain to two megabytes and to adopt the soft fork SegWit (Segregated Witness). But, this was ultimately cancelled by the miners who proposed this change.

[1] Source: https://blockchain.info 18 April 2018

Bitcoin Forks 2017



Source
The chart below explains how a fork works: a new bitcoin version keeps the history of the original bitcoin and adds the new properties in its own blockchain. Bitcoin Cash and Bitcoin Gold have their own price and trade independently from the original bitcoin. Source: BestVPN.com

Second generation of cryptocurrencies: Ethereum

1. Definition

Ethereum is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract (scripting) functionality. Ether is the name of the cryptocurrency used on the Ethereum platform or, in other words, the blockchain. Ethereum was proposed in late 2013 by Vitalik Buterin, a cryptocurrency researcher and programmer. Development was funded by an online crowd sale that took place between July and August 2014. The system went live in July 2015, with 11.9m coins 'pre-mined' for the crowd sale. This accounts for approximately 13% of the total circulating supply. As opposed to the bitcoin, the total maximum supply is not capped for the ether.

2. Main differences with bitcoin

- Shorter time to mine a new block (14-15 seconds versus 10 minutes)
- Consistent rate of mining new coins and no hard cap on the total supply of ethers
- Distributed ledger of smart contracts, not just coins

3. Smart contracts

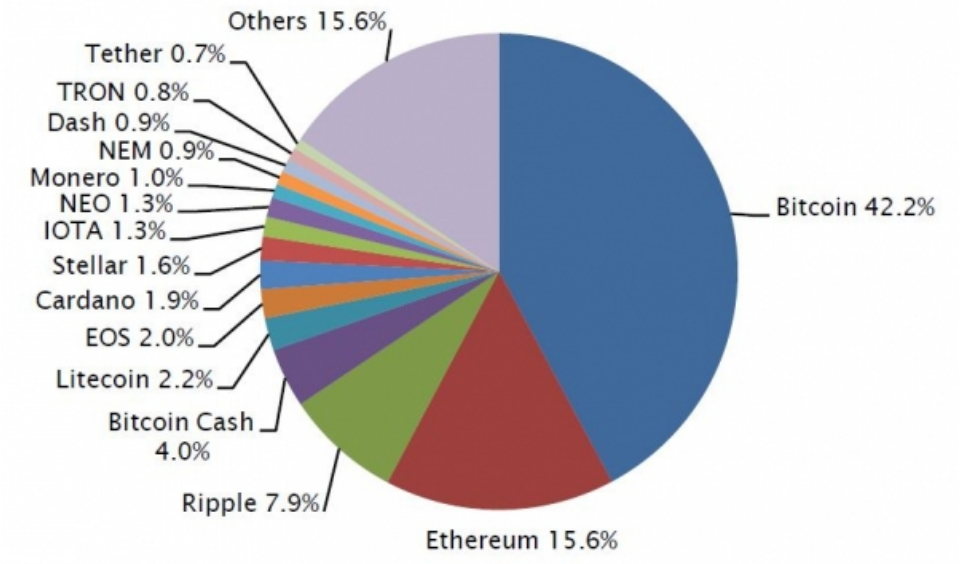
A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible. Proponents of smart contracts claim that many kinds of contractual clauses may be made partially or fully self-executing, self-enforcing, or both. The aim of smart contracts is to provide security that is superior to traditional contract law and to reduce other transaction costs associated with contracting. The first cryptocurrency associated with these contracts was the ether, but since then various cryptocurrencies have implemented types of smart contracts.

Other currencies

Many other cryptocurrencies do exist and have been created in recent months and years. There are currently c.1,560 currencies available, but the market is still dominated by very few of them in terms of market capitalisation and size. Bitcoin is by far the largest cryptocurrency in terms of market capitalisation and traded volume, followed by Ethereum. The next largest and most traded are Ripple, Bitcoin Cash, Litecoin, EOS, Cardano, Stellar, NEO, IOTA. The total market capitalisation of all cryptocurrencies is around USD325bn and the largest, bitcoin, accounts for 42% (USD137bn) of this[1].

[1] Source: https://coinmarketcap.com, April 2018.

Current breakdown of cryptocurrencies by market capitalisation



Source
https://coinmarketcap.com, April 2018

Initial Coin Offering

An Initial Coin Offering ('ICO') is a means of crowdfunding centered on cryptocurrencies. It is used by digital entrepreneurs to fund their future projects. Tokens, which are generally tied to a cryptocurrency, typically ether, are distributed to investors in exchange for their investment. They are supposed to become functional currencies when the project is completed or the funding goal is reached. ICOs are popular because they allow entrepreneurs to avoid costs and regulatory hurdles when raising cash for their projects. However, this comes at the expense of investor safety due to a lack of legal and regulatory framework.

III. IS A CRYPTOCURRENCY A CURRENCY?

Main features of a currency

1. Medium of exchange

A medium of exchange is an intermediary instrument used to facilitate the sale, purchase or trade of goods between parties. For an instrument to function as a medium of exchange, it must represent a standard of value accepted by all parties. Bitcoin as an example is accepted as a medium of exchange as a growing number of merchants accept it as payment, it does therefore fulfil this criterion, even if not at a wide scale.

2. Unit of account

A basic function of money is providing a unit of measurement for defining, recording, and comparing value. For instance, one dollar signifies not only a one dollar bill, but also a dollar's worth of money in other forms (deposits, loans, mortgages), of wealth in forms other than money, and of any good or service with a market value. No lenders use cryptocurrencies as the unit of account for consumer credit, auto loans or mortgages, and no credit or debit card is denominated in a cryptocurrency. This main principle of a currency is not fulfilled by any cryptocurrency. Money must be a standard of deferred payment, meaning that if people borrow today, they can pay back their loan in the future in a way that is acceptable to the person who issued the loan – this is not possible with cryptocurrency.

3. Store of value

A commodity, currency or other type of capital that is tradable and can be stored for future use is thus a store of value. It is a fundamental component of the economic system, because it allows trade to occur with items that have inherent value. A currency is an example of a store of value, which can be exchanged for goods and services. If the value of currency becomes unpredictable, such as in times of hyperinflation, investors and consumers will shift to alternative stores of value, such as gold, silver, precious stones and real estate. The high volatility in the 'translated value' of cryptocurrencies into common units of account like the US dollar, euro, and Swiss franc make them difficult to store due to their unpredictability. On top of this, a cryptocurrency has no interest rate attached to it. This criterion is not fulfilled at this stage. As by definition there is no central authority backing a cryptocurrency, one aspect of the cryptocurrency universe is unclear: what happens if a cryptocurrency stops working for some reason? Who will deal with its 'death' and how will users be treated? Moreover, a traditional currency can be deposited in a bank account, which is not possible for now with cryptocurrencies that must be held in digital wallets. This raises the issue of security and technological mishandling, as digital wallets have been vulnerable to hacking.

Finally, a limited money supply does not apply to all cryptocurrencies. Bitcoin currently has a fixed money supply of 21m units. If bitcoin becomes widely accepted and used as a means of payment, this limit would not be compatible with a growing economy and an increasing number of transactions. No fiat money – a currency without intrinsic value like USD, EUR, CHF – has constrained money supply. This is where central banks intervene, as many economic variables do affect the value and the behaviour of a currency.

Not yet and maybe never a currency - but what instead then?

Looking at these various factors, it is clear cryptocurrencies cannot yet be considered a currency (as defined in this text) like the US dollar or the euro. However, governments and regulators will probably need to define them in future. Is a cryptocurrency a currency, an asset, a commodity, a new asset class or something else? Determining the nature of a cryptocurrency is important as it will, among other factors, define the fiscal treatment for an investor. In the United States alone, the positioning is unclear: on 6 March 2018 a Federal judge stated that cryptocurrencies such as bitcoin are commodities and should therefore be regulated by the US Commodity Futures Trading Commission (CFTC). Since 2015, the CFTC has behaved as though cryptocurrencies are commodities, but this was the first time a federal judge confirmed this assumption.

The following day, the US Securities and Exchange Commission (SEC) issued a statement on potentially unlawful online platforms trading digital assets.A number of these platforms where investors can buy and sell digital assets - including coins and tokens offered and sold in ICOs – provide a mechanism for trading assets that meet the definition of a 'security' under the federal securities laws. If a platform offers trading of digital assets that are securities and operates as an 'exchange', as defined by federal securities laws, then the platform must register with the SEC as a national securities exchange or be exempt from registration. Some claim that bitcoin's most profitable use is in the overseas remittance business which is estimated at USD 600bn. Bitcoin could be a major threat for the money transfer operators, such as Western Union, if the cryptocurrency becomes the new standard for international money transfers and payments.

Defining the nature of cryptocurrencies has become a pressing concern. Cryptocurrencies were created to operate globally with no interference from central authorities. In reality, cryptocurrencies are being categorised differently between jurisdictions, and receiving different fiscal treatment as a result. As a result, something that was intended to be global, untouchable and above the law has become local and regulated.

IV. DEFINING THE FAIR VALUE OF A CRYPTOCURRENCY

Price vs. value of a cryptocurrency

Like any other traded asset, commodity or currency, a cryptocurrency has value because market participants think it has value. But how can the value of a cryptocurrency be defined using objective metrics and how is it priced? For bonds or equities, earnings of the issuer/company give some substance and fundamental value to the asset. Is this also true for bitcoin?

Factors that impact the price of a cryptocurrency

Many factors have an impact on the price of a currency, an asset or a commodity. And as for any financial instrument, an exact determination of its value is hardly achievable as it is subject to perception and interpretation. Its traded price might therefore be very different from its fundamental value. In the following section we explore the factors that can have a direct or indirect influence on the price of a cryptocurrency:

1. Supply and demand

The value of a commodity is mainly defined by its utility and limited supply. The price is often linked to the asset's supply and demand dynamics. Bitcoin, for example, has a limited supply as it is capped at 21m of units. If bitcoin were to be adopted by the worldwide population it would, of course, have a massive influence on its price due to scarcity.

2. Energy needed to secure the blockchain

The energy put into securing blockchains is intensive. The proof of work (PoW) blockchains, which are the most popular form – in contrast to proof of stake ones (PoS) – use extensive electricity. In the case of bitcoin, the blockchain currently uses as much energy to secure it as a country like Denmark. This has a factor on the price, as it takes a certain amount of energy on average to 'mine' one new block and this requirement grows as the difficulty increases.

3. Difficulty level of the blockchain

The more secure the blockchain and more difficult the mining, the higher the perceived value. This can have an impact on the price and is closely tied to the usage of energy in the case of proof of work blockchains.

4. Utility of the currency and simplicity to use and store

The utility of a cryptocurrency is a key factor in its price. If you cannot use it for payment, an investment or cash it in, then it would have little perceived value. As bitcoin is usable for payments on a reasonable and increasing scale, its utility is high.

5. Public perception of its value

The public perception of a cryptocurrency has an important impact on its value. The innovation behind the bitcoin and the creation of a new way to complete transactions can be positive factors. On the other side, it can also instigate negative reactions because the technology is often associated with criminal funding. Cases of robbery and hacking also have a negative impact on investors' perception.

6. Price of bitcoin

Bitcoin is often seen as the 'reference currency' of the cryptocurrency world. Rises and falls in the price of bitcoin often have a knock-on effect with other cryptocurrencies. The correlation between bitcoin and the other main cryptocurrencies is on average higher than 0.85[1], illustrating the synchronised behaviour of the 'asset class'.

7. Legal/political issues

Legal and governmental issues can also influence the price. If a government has particularly oppressive tax or asset laws, it can be tempting to hide assets in a cryptocurrency. A country could positively impact a cryptocurrency by making it an official currency or means of payment. On the flipside, banning it could have a negative effect.

[1] Source: SYZAM, https://coinmetrics.io/data-downloads/, Jan 2017-April 2018

Limited transaction capacity

As discussed above, many of the factors that have an impact on the price of a cryptocurrency are difficult to quantify and value accurately; they rely on herd behavior and investor perception, rather than on fundamentals. Bitcoins were originally created to reward "miners" and validate pending transactions by adding a block to the blockchain. The reward must economically cover the cost associated to mine a block: including the energy required to run very powerful computers and skilled IT specialists to operate them.

Assuming that a miner receives 12.5 bitcoins to validate a block (a new block is mined every 10 minutes) and that a bitcoin trades at approximately USD 7,000, this means a miner receives the equivalent of USD 87,500 every 10 minutes for validating pending transactions. The bitcoin blockchain is able to perform seven transactions per second, i.e. 4,200 transactions every 10 minutes. Taking our example of a bitcoin worth US$7,000, a miner receives the equivalent of USD 20.8 per transaction he validates – no matter the size of the transaction - plus the transaction fee associated with each trade. As a comparison, VISA, the largest transaction servicer, processes 24,000 transactions per second, i.e. 14.4m transactions every 10 minutes. If VISA charged USD 20.8 per transaction, they would earn USD 300mn every 10 minutes or USD 43.1bn every day.

The comparison with VISA is probably unfair, but it puts the transaction capacity and speed of the bitcoin blockchain technology into perspective. This limited transaction volume capacity is also one of the most widespread criticisms of the bitcoin technology. Multiple improvements have been proposed by users and could be implemented in the future with a newer version of the bitcoin, through the adoption of a fork.

Fair value of the bitcoin

What if the fair value of a bitcoin was the cost of mining a bitcoin? This metric is used in the gold industry, where the extraction of one ounce of gold from the ground has a certain cost and no one would be willing to extract gold if they were not rewarded for it. The cost of mining a bitcoin, just as the cost of extracting gold, is not the same in each country. Nevertheless, one question remains: by 2140, no new bitcoins will be issued as new blocks are mined and so miners will no longer be rewarded with bitcoins. Their only source of revenue would then be collecting the transaction fees associated with the transactions validated in that block. If by 2140 the current limited transaction processing capacity of the bitcoin blockchain is solved and becomes unlimited, the price of bitcoin should gradually run its course to zero. Miners would receive no revenue from mining and almost no revenue from transaction fees. If the current processing congestion persists until then and the bitcoin becomes a true market standard, then the transaction fees will have to increase substantially, simply as a function of the supply and demand mechanism.

V. CRYPTOCURRENCIES AS AN INVESTMENT OPPORTUNITY

DIRECTLY ACQUIRING CRYPTOCURRENCIES

Mining

The genuine way to access bitcoin or any other cryptocurrency is to receive them as reward for mining them. Inversely to fiat currencies which are controlled and issued by central banks, cryptocurrencies are created by the participants of the blockchain who validate pending transactions: the miners. Money creation and supply is coded in the algorithm of the blockchain. For bitcoin for example, the rhythm of money creation and total money supply are already predefined, and the final number of 21m units of bitcoins will be reached somewhere by 2140. Many participants saw in mining an opportunity to make easy money when the price of bitcoin started to increase rapidly. The competition for resolving the 'crypto-puzzle' in order to get rewarded with bitcoins became fierce. Farms of super-computers were set-up all around the world, which created high barriers to entry in mining. It quickly became impossible for private participants with personal computers to compete for the mining reward every ten minutes. Along with the increased technological capability required, the amount of energy needed to mine bitcoins also grew substantially. Although it is difficult to assess the cost of putting together enough computing resources to mine bitcoins, the energy cost is not negligible and may vary immensely from one country to the other. According to research conducted by Elite Fixtures, the cost of mining a bitcoin varies significantly around the world, from as little as USD 531 in Venezuela to a stunning USD 26,170 in South Korea. The average stands at USD 4,758. If the market price drops below the marginal cost of mining a bitcoin, the number of miners will also suddenly decrease. The access to bitcoins through mining is limited to a tiny part of the population, as it is subject to high barriers to entry. It will never be the easiest way to acquire bitcoins.

Barter

It is also possible to buy or sell bitcoins over-the-counter. This was probably the first way to exchange cryptocurrencies when trading platforms did not exist. The meeting points were defined between the buyer and the seller, and so was the price of the transaction.

ATMs

An alternative way to buy and sell bitcoins is to use a kind of 'cash machine', which can be found mainly in larger cities around the globe. Just over 2,600 of these machines have already been installed, but their number continues to grow at a pace of 6 ATM/day [1]. ATMs are not the most efficient way to transact bitcoin, but they offer a 'physical' buy and sell facility for people who struggle to transact exclusively via the web.

[1] Source: Coin ATM Radar

Trading platforms

Cryptocurrencies can be bought and sold against traditional currencies or other cryptocurrencies on specialised websites called platforms. They also allow for the transfer of ownership of cryptocurrencies from one person to another. There are two types of trading platforms:

1. Cryptocurrency exchanges

These connect buyers and sellers for a fee, and most of them allow the trade of many cryptocurrencies. The most popular are Coinbase, Binance, Bittrex, Kraken, Cex.io, GDAX, Bitfinex, and Poloniex, among many others.

2. Online forex brokers

These are similar to foreign exchange dealers. Unlike cryptocurrency exchanges, the investor trades bitcoin CFD's (contract for difference) – a kind of financial derivative instrument - requiring less initial capital than buying bitcoins directly. The investor does not hold the bitcoin but they have an exposure to it. The most popular platforms are eToro, Avatrade and FXTM.

Security

Platforms are relatively underregulated, which means that the protection offered to the investor is very limited. Indeed, cryptocurrency holdings on platforms are not insured by any state, and in case of a loss investors will not be reimbursed automatically. This lack of regulatory monitoring means that theft is particularly problematic. Indeed, over the history of cryptocurrencies there have been plenty of examples of hacking and digital theft. More than 980,000 bitcoins have been stolen in the cryptocurrency's history, and few have been recovered. Security is a crucial issue here, particularly regarding the private key used to execute transactions. This private key is the main target of theft, as taking possession of it gives access to the entire bitcoin wallet of that wallet owner. As a result, the key requires specific security measures, which many users are unaware of. Stories of stolen or lost private keys abound. Even the physical safety of people in charge of private keys can be at stake. On top of this, practical issues like geographical restrictions, ID verification, or depositing funds into the account on the platform (among others) can prove cumbersome.

Regulators are behind the curve

The use and exchange of cryptocurrencies present real regulatory challenges and risks for participants. Exchanging fiat currencies for cryptocurrencies, exchanging cryptocurrencies for other cryptocurrencies or transferring ownership of cryptocurrencies from one person to another involve complex issues of ownership and trust. The main challenges for the regulator are:

- **Privacy and data security:** stakeholders such as the police, financial authorities or sophisticated criminals could link anonymous wallet addresses to real life addresses.
- **Anti-money laundering:** Australia, for example, requires digital currency exchanges to comply with their anti-money laundering regime, including KYC (know your customer) obligations and more.
- **Taxation issues:** at the investor level, should an investment in a cryptocurrency be taxed as income, as good and services, as capital gains, or not at all?
- **Financial services regulation:** a cryptocurrency may fall under the scope of laws regulating financial services and products.
- **Jurisdictional issues:** where a country's jurisdiction starts and ends in a digital world is not very clear.
- **Crime risk:** a lot of people have the 'fear of missing out' syndrome regarding the cryptocurrencies boom and so do not assess the risk of an investment adequately. Investors do not have enough protection legally or financially.
- **Political risk:** country regulators are cracking down on cryptocurrencies and can change the regulatory framework overnight.

Despite all these risks, cryptocurrency trading exchanges are the most common way to invest in digital currencies. Once governments and regulators have addressed the challenges outlined above, these trading platforms will be much safer for investors. But, they will also be more constrained, like a trading platform for traditional assets.

VI. INDIRECT WAYS TO INVEST IN CRYPTOCURRENCIES

One of the main objectives of the 'cyberpunks' when creating cryptocurrencies was to exclude governments – or more precisely central banks – and traditional financial stakeholders like banks from the economic cycle of currency creation, transfer and storage. The idea was to develop a decentralised, self-managed, autonomous currency with very different foundations and no true links to fiat currencies. Among the main contradictions of investing indirectly into cryptocurrencies – via structured product structures, ETFs/ETNs or futures – is that investors do not hold bitcoins per say and so only participate in its price developments, in terms of its value against a fiat currency. This goes against the genuine philosophy behind cryptocurrencies, but is an easy way for an investor to get exposure to the most liquid cryptocurrencies and in particular bitcoins.

Futures

1. Creation

The first bitcoin futures opened for trading on the CBOE Futures Exchange (Chicago Board Options Exchange) mid-December 2017. One week later, bitcoin futures were also available for trading on the CME (Chicago Mercantile Exchange). Bitcoin futures are supposed to offer more transparency, more liquidity, efficient price discovery (a mechanism by which buyers and sellers determine the price of a security) and risk transfer capabilities. Futures also provide a risk management tool for investors who want to hedge their underlying bitcoin holdings or short them. Financial futures allow exposure to bitcoin without having to hold any of the cryptocurrency and are settled in fiat currencies. Given the volatility of bitcoin, the initial margin requirement needed to trade cryptocurrencies futures is high, respectively 40% for the CBOE and 35% for the CME. In comparison, the S&P 500 futures contract requires an initial margin of approx. 5%, enabling much higher leverage.

2. Market development and broader usage

In a January 2018 fund manager survey by BarclayHedge, it was revealed the majority of CTAs are unconvinced by bitcoin futures, although nearly one third said it was too early to determine their view. "73% of respondents from a wide range of firms located in Switzerland, Canada, Japan and the UK, as well as the majority in the USA, did not believe that bitcoin futures were a valuable or useful addition to a diversified futures portfolio and only 5% said they were already trading these contracts. The biggest concerns of CTA managers regarding bitcoin futures are, in order of importance:

- Not enough volume/liquidity
- Bitcoin is too volatile
- Cryptocurrencies futures are a bad idea and should not be encouraged
- Contracts are too new
- Margin requirements are too high

Only 30% of CTA managers believe that in one year's time, cryptocurrencies futures will be high volume, successful contracts. 60% believe they will be inconsequential/low volume and 10% think cryptocurrencies futures will no longer exist. Some of the headwinds to investing in bitcoin futures are that they can only be traded by a limited number of institutional investors and the roll-over costs are high. On a more technical note, the futures do not fully incorporate bitcoin 'forks', like Bitcoin Cash or Bitcoin Gold.

Exchange Traded Funds/Exchange Traded Notes

1. US regulation not ready for crypto ETFs

The hype around cryptocurrencies quickly raised the appetite of the passive investment industry, which sought to replicate the active routes to investing in cryptocurrencies. Various providers proposed bitcoin ETFs for registration and approval to the Security and Exchange Commission (SEC) in the US by the end of 2017, but every filing has been rejected so far. The SEC and ETF companies cannot agree on how to bring a bitcoin ETF to the market. Some Issuers even decided to withdraw their filings for new funds tracking the digital currency as the SEC had concerns about liquidity and valuation of underlying bitcoin futures

2. Sweden as pioneer

The first index product tracking the bitcoin was launched in Sweden by XBT Provider back in 2015, approved by the FSA, the Swedish Financial Supervisory Authority. It really acts as a precursor in this space. In 2017, XBT Provider created a similar product tracking the performance of ethereum, the second-largest and second most-liquid cryptocurrency.

3. ETF vs ETN

The structures offered by XBT Provider are not Exchange Traded Funds, but Exchange Traded Notes. The main difference is that this introduces a notion of counterparty risk, as the ETN is a kind of unsecured bond issued by the investment solution provider. If the issuer goes bankrupt, the investor loses their money, independently of the performance of the underlying tracked asset. One of the other features of buying an ETN is that the investor does not own bitcoins – they hold a financial instrument that returns the performance of the bitcoin. Just like futures, ETNs do not incorporate the management of bitcoin 'forks'. However, they are very easy to buy and investors do not face the challenge of storing bitcoins.

Structured products

Delta-one certificates have been issued by banks and financial services companies to provide investors with directional exposure to bitcoin. Vontobel, Leonteq, Swissquote were the first in Switzerland to offer such products, which are an easy way for end investors to get access to the performance of bitcoin, without having to trade the cryptocurrency. A simple deposit is sufficient to trade these certificates for a trading and/or subscription fee. Structured products have a counterparty risk (the issuer) and do not deal with bitcoin 'forks'. On top of that, they are currently limited to only a few cryptocurrencies. On the other hand, they are easy to buy and as with ETNs, there is no security issue with storing bitcoins safely.

Funds

A fund is a hybrid way to invest in cryptocurrencies: the fund owns cryptocurrencies directly, but the investor owns shares of a fund and thus, has indirect exposure to cryptocurrencies. The main advantage associated with holding shares of a fund, instead of dealing directly on a cryptocurrency exchange, is that the investor does not have the security hassle of owning the private key themselves. On top of this, a fund structure has by definition a segregation of assets, as clients' assets are kept independent from the company's assets. If the company goes out of business, the client's assets can be returned easily. Of course, this comfort has a price – a management fee and often a performance fee.

1. Available structures

Many funds investing in cryptocurrencies were launched in the last couple of months, while some were launched earlier by pioneers in the asset class. The most common structures that can be found on the market are offshore funds, mainly Cayman or Jersey-domiciled or Delaware LPs. Some are open-ended and others that invest in less-liquid assets were set up as closed-end private equity-type funds. The first bitcoin mutual fund in Europe was launched in France. A second is in the process of being registered in Switzerland, and an open-ended fund of funds is applying for registration in Luxembourg. Countries and regulators are slowly opening-up to funds in this new 'asset class'.

2. Strategies: buy & hold, arbitrage, venture

There are already plenty of available strategies in the cryptocurrency space, including:

- Traditional buy & hold, tracking the return of one single digital asset (mainly bitcoin).
- Directional investing in a diversified, actively-managed portfolio of the most liquid cryptocurrencies.
- Market neutral, using cross-market arbitrage (taking advantage of mispricing between exchanges), carry arbitrage and digital currency lending.
- Quant arbitrage strategies, using exchange arbitrage, OTC block trading, triangular arbitrage (exchanging cryptocurrencies against others on various platforms), and relative value trading.
- Venture funds investing in ICOs, pre-ICOs and pre-sale SAFTs (Simple Agreement for Future Tokens).

3. Liquidity and fees

The liquidity offered by the available funds is dictated by the investment approach, i.e. daily for the mono-cryptocurrency long-only funds, monthly to quarterly

for market neutral and arbitrage strategies, and up to 10 years for private equity-like closed-end fund structures in the venture space. Fees are generally high in the asset class, even for long-only buy and hold funds. Clients may choose between a flat 2.5% p.a. management fee or a 1% p.a. management fee and a 20% performance fee over cash for the French bitcoin fund. An investment manager in the United States charges 0.75% for their bitcoin fund, but it is open only to US clients. Lastly, a USD 2bn Delaware-domiciled investment trust charges 2% p.a. management fee without a performance fee. One of the actively-managed funds investing in several cryptocurrencies charges 2% p.a. management fee and a 25% performance fee. The same company manages a market neutral arbitrage strategy, which charges 2% p.a. management fee and a 30% performance fee. Paying 2% plus 20% is probably the average in this space, which is not very different from a usual hedge fund fee structure. At this fee level, an investor is entitled to ask for active management. Funds that offer longer-term less-liquid strategies like pre-ICOs or pre-sale SAFTs can charge up to 3% p.a. management fee and a 30% performance fee. In short: a high-risk strategy with a high-return potential means high fees.

4. Diversification

Diversification can be handled in two ways: diversification within the funds and diversification of cryptocurrencies in a broad portfolio.By definition, a single cryptocurrency investment like a bitcoin fund is not diversified and investors probably invest for its innovative features and high return potential, without worrying too much about its undiversified nature. Holding a fund that invests in several cryptocurrencies is not much different, as most cryptocurrencies follow the same direction. Nevertheless, investing in a basket of cryptocurrencies will always be less risky and volatile than a single line, even if volatility is much higher in this space in general than in any other traditional asset. Instead, let's focus on the diversification benefits of an investment in cryptocurrency in a broader investment portfolio. Despite its volatility, an addition of a bitcoin allocation in a wider portfolio has diversification benefits and can enhance the portfolio risk/return. This is only possible through an adequate sizing and the low correlation of bitcoin against all the main traditional asset classes – cash, currencies, sovereign bonds, corporate bonds, equities, commodities, gold, real estate and volatility – as it ranges between -0.08 and +0.08[1].

5. Custody and security

Segregation of duties, segregation of assets and management of the security aspects are key when investing in cryptocurrencies via a fund rather than directly on a crypto-exchange, and these requirements do partly explain the higher cost. The role of the independent custodian seems pretty obvious – it guarantees the isolation of the assets held in the name of a client from the rest of the company's assets. It also prevents the assets from being stolen or hacked, or at least makes the exercise more challenging. Since security is one of the main concerns when buying cryptocurrencies on an exchange, the private keys that allow the transactions should be handled with the highest care. As such, the true 'assets' in a cryptocurrency fund are the private keys, and secure storage of these keys is paramount. At the current stage, there is no custody solution in the marketplace that meets the SEC's qualified custodian rule. Several custody solutions have nevertheless been tested:

- **Multi-signature wallet:** having multiple signatures on a wallet is a pre-requisite when dealing in the name of a fund, as this prevents one person from being able to steal the assets from the fund. It makes a hacker's task more difficult as he would need to steal multiple keys to take ownership of the fund's wallet. The fund's custodian could be one of the signatories, which would further reinforce the security.
- **Cold storage:** it is possible to secure bitcoins or cryptocurrencies by storing them offline, away from any internet access. There are several methods of cold storage like paper wallets, USB drives, sound wallets (compact or vinyl discs) and hardware wallets. Cold storage is probably the safest way to store cryptocurrencies - its disadvantage, however, is that it can take a while to process a transaction.
- **Account limitations:** putting transaction limitations on a digital wallet can be an effective way of reducing risk. These restrictions can be placed on the number of tokens that can be dealt in a single transaction or on the maximum number of tokens that can be distributed in a certain period of time.

  Some fund managers use a combination of these custody solutions. The management of security risk is certainly the key risk for investor's to assess when doing due diligence on the fund manager. It is as important as the fund management skills, if not more so. Recent cryptocurrency fund launches have been plentiful. However, only a few of them can show long track-records, demonstrating the quality of their management skills. The cryptocurrency fund industry has a long way to go to meet global fund management standards.

[1] Source: SYZ Asset Management, Bloomberg, Nov. 2012-April 2018

VII. CONCLUSION

The blockchain, even if it is still an emerging technology, is revolutionary and innovative. It is likely to change industry standards in many economic sectors.

- In the financial sector for instance, real applications will probably be seen in the international payments space; for banking access in remote areas as a stable form of currency; in B2B payments as a threat to the SWIFT system; in securities trading and settlement; to manage bank guarantees, among many more.
- At a wider scale, the blockchain can speed up and securitise many areas like supply chain tracking in the logistics business or become the base technology in the cybersecurity space using keyless signatures, replacing logins and passwords.

Getting exposure to the blockchain technology itself is not easy and one of the best ways is to invest in companies that develop or provide blockchain-based solutions. Those companies tend to be start-ups and venture capital-type investments and would require a private equity approach with a long-term investment horizon. Investing directly in cryptocurrencies is another way to get exposure to the growth of the blockchain technology and, indirectly, to its underlying infrastructure. Bitcoin is the first visible application of the blockchain but trying to value it proves very difficult. Investing in bitcoin or any cryptocurrency is, at this stage, an uncertain bet on the future. The technology is likely to see many applications in the coming years, but the utility of a wider range of cryptocurrencies, and especially bitcoin, is questionable due to scalability limits. However, if one cryptocurrency becomes a new global standard and a 'reserve currency' adopted by all market participants, then its price is likely to rise further. We are still far from this scenario. The key question is: will bitcoin be that currency? Despite these uncertainties, the good news for people willing to invest in one or a basket of cryptocurrencies in a global portfolio is that they offer diversification benefits thanks to very low correlations with traditional assets, without requiring a significant allocation due to high volatility and high expected return. Among the available investment alternatives, a diversified multi-cryptocurrency fund is probably the least risky way to invest in this area. Nevertheless, selecting such a fund requires particular skills in terms of technological understanding and, even more importantly, a detailed assessment of the operational setup and security risk. The due diligence exercise is made even more challenging as very few managers have long and proven track-records.

VIII. BIBLIOGRAPHY

https://www.technologyreview.com/s/524666/bitcoin-lacks-the-properties-of-a-real-currency/

https://bitconnect.com/bitcoin-information/10/how-is-the-price-of-cryptocurrency-defined/

https://coinmarketcap.com/all/views/all/

http://bitcoins.net/investing/limits-of-supply.asp

https://seekingalpha.com/article/4082979-much-bitcoin-lost-forever

https://bitinfocharts.com/

http://www.bilan.ch/yves-bennaim/crypto-actifs-mieux-comprendre-icos

https://www.theodysseyonline.com/cryptocurrency-exchange-forex-broker-trading-bitcoin

https://bravenewcoin.com/news/36-bitcoin-exchanges-that-are-no-longer-with-us/

https://www.reuters.com/article/uk-markets-bitcoin-factbox/factbox-things-you-might-not-know-about-bubbly-bitcoin-idUSKBN1DT30L

https://www.unisuper.com.au

https://blockchain.info/

https://www.barclayhedge.com/research/hedge-fund-manager-survey

https://www.cnbc.com/2018/01/17/sec-frets-over-bitcoin-etfs-but-swedes-figured-it-out-years-ago.html

https://www.marketwatch.com/story/heres-how-much-it-costs-to-mine-a-single-bitcoin-in-your-country-2018-03-06

https://coinatmradar.com

https://digiconomist.net/bitcoin-energy-consumption

https://blockexplorer.com/

https://www.fintechbusiness.com/blogs/993-the-risks-of-cryptocurrency-exchanges

http://blockassetmanagement.com/

https://www.cryptofinance.ch/

http://www.tobam.fr/

https://grayscale.co/

https://hbr.org/2017/01/the-truth-about-blockchain

“Monpoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System”.
G. Huberrman, J.D. Leshno, C.C. Moallemi, Columbia Business School, October 2017

https://coinmetrics.io/data-downloads/

Disclaimer