Exchanging Views

# Introducing cryptocurrencies – what are they good for?

Industry Overview

Bank of America Merrill Lynch

Equity | 16 October 2017

TransformingWorld
Thematic Research

Pan-Euro
Other Financials


**Philip Middleton** >>
Research Analyst
MLI (UK)
+44 20 7996 1493
philip.middleton@baml.com

**Francisco Blanch**
Commodity & Deriv Strategist
MLPF&S
francisco.blanch@baml.com

**Vadim Iaralov**
FX Strategist
MLPF&S
vadim.iaralov@baml.com

**Adithya Metuku, CFA** >>
Research Analyst
MLI (UK)
adithya.metuku@baml.com

**Hubert Lam** >>
Research Analyst
MLI (UK)
hubert.lam@baml.com


## Evolving technology which investors want to understand

Cryptocurrencies ("coins") have proliferated over the past couple of years and have been highly volatile. Many come with associated businesses and technologies. Understandably, investors want to know how this innovation has been created. We also think that the technologies underpinning this development could resonate into mainstream finance and beyond. This note doesn't try to value the coins – they are surrounded by uncertainty. It tries to give an overview to explain how they work, how they differ and how they may develop.

## Bitcoin, Ethereum, Ripple +1,000

Bitcoin (currently valued at $80bn) is the original and largest coin, however in our view, it is struggling to fulfil its objective of facilitating decentralised payments. Its costs, lack of speed and tax treatment in some key jurisdictions, make it hard to use for payments. It can be seen as "digital gold", but lacks gold's track record. Ethereum ($28bn), the next largest, allows users to write code within its blockchain. These "smart contracts" enable a plethora of applications to be built. Ethereum has hosted a lot of coin offerings ("ICOs"). The future adoption of ICOs is important to Ethereum's success. Ripple ($10bn) is looking to provide FX infrastructure. Its software has been adopted by some large FX players. For its coin to be valuable, it needs to carve out a niche in trading the less liquid currencies. These are only three of over a thousand coins. Unless a coin has some distinctive feature, we think it may struggle to gain mass adoption. We think the proliferation of bitcoin-like coins also suggests a lack of scarcity value.

## Going mainstream?

There are signs that coins are crossing over into mainstream finance; CBOE and LiquidX plan to offer futures, and CBOE also aims to list an ETF. Cryptocurrency futures could be a significant revenue stream for the exchanges, but plenty of hurdles remain.

## Diversifying asset?

Bitcoin has, technically, been a diversifying asset in the past. It correlates with a number of other coins, though it doesn't correlate with ether. It has not correlated with mainstream assets; its volatility is high, and this is a challenge for a range of uses.

## Disrupting status quo?

Coins may potentially disrupt existing businesses; Bitcoin could undermine both payment processors and gold, Ethereum the exchanges and Ripple some FX infrastructure providers. We do not see any of these as likely, but investors need to be alert to this.

## Overall – look out for broker/dealers

The coin universe is dynamic and innovative and volatile; while a true value for cryptocurrencies may be impossible to assess, one factor which we believe could affect their liquidity and market capitalisation would be if one or more global broker/dealers decided to offer institutional-like products.




Timestamp: 16 October 2017 12:30AM EDT

# Contents

# What's in a name?

We have adopted the following conventions for naming the various coins we have discussed. We note that naming conventions, like so much else with the area, are still evolving. We have also added in a few definitions for the various abbreviations we use throughout the note.

**Bitcoin**
Bitcoin has a lower case "b". It is often called BTC (though we have seen XBT used).

**Ethereum**
Ethereum seems to have an uppercase "E". The coin is called ether (usually, but not always, with a lower case "e") or ETH. The unit used to measure computational effort in Ethereum is "gas"; one unit of gas is currently worth around 20bn Wei, or 0.00000002 ETH (the Wei is the smallest subdivision of ETH; $10^{18}$ Wei are an ETH).

**Ripple**
Ripple is the parent company for a token, which seems almost always to be called XRP; this is the terminology that Ripple itself uses.

**Bitcoin Cash**
Bitcoin Cash seems to have upper case "B" and "C" – at least, this is what its website employs. It is called BCC.

**Litecoin**
Litecoin, a coin, has an upper case "L" (as per the Litecoin website). It is called LTC.

**IOTA**
IOTA, a coin, is all upper case. For some reason, the coin is often called MIOTA.

**Coin and token**
We use coin to mean the tradable currency or the various systems we discuss. Token tends to mean "coin issued by ICO", though again, people use different terminology.

**Altcoin**
An alternative to bitcoin; ether, XRP and so on are alt coins.

**ICO**
An ICO is an "Initial Coin Offering", a way of offering new coins, typically using the Ethereum system; we discuss these later.

**IoT**
The "Internet of things", essentially the idea that an increasingly large number of devices can be linked together using the Internet. IOTA has set out its stall to appeal to IoT developers.

**CCP**
A central counterparty, part of the mainstream finance world which stands between buyers and sellers in a lot of mainstream markets (cash equities, futures, many wholesale derivatives and so on).

**DApp**
A DApp is a decentralised application, which tends to be built on Ethereum.

**ETF/ETP**
Exchange Traded Fund/Product, listed vehicles which provide exposure to an underlying asset.

# Coin, huh, yeah, What is it good for?

Edwin Starr's question, "what is it good for?" is the right one, we think, at least as far as cryptocurrencies are concerned[1]. This note tries to answer it for bitcoin and some of the larger cryptocurrencies that are currently traded.

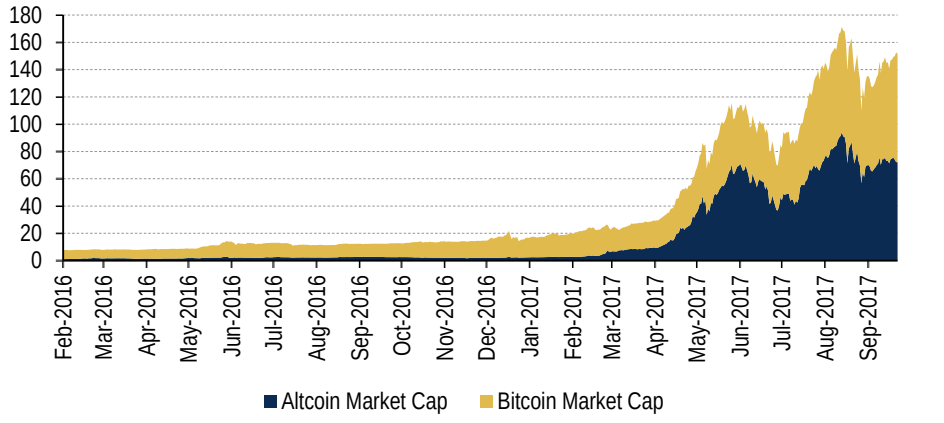
**How did we get here?**

The way people exchange value has gone through many evolutions. People moved from commodity backed currencies to metal backed ones. Silver formed the basis of the world's monetary system for nearly 400 years, after which gold filled a similar role. Policy shifted a bit following the Great Depression, a bit more during the Vietnam War and finally in 1971 Nixon announced that the US would no longer exchange Dollars for gold in the international markets, effectively ending the gold backing of currency. Since then, most countries have moved towards locally constructed fiat currencies.

The cryptocurrencies are, in some people's view, the next evolution of money. A group of developers created bitcoin in 2009, following a pioneering paper from Satoshi Nakamoto. The first known use of bitcoin to actually buy something came in May 2010, when a programmer paid 10,000 bitcoins for two Papa John's pizzas[2]. Since then, bitcoin has appreciated by several orders of magnitude, and over a thousand other cryptocurrencies have emerged, many looking like bitcoin, others using different technologies.

To start with, we show how the market caps of bitcoin and the altcoins have grown (the price and market cap data here and throughout the note is as at 9th October '17, but please note, these data points are highly volatile). This has been a dramatic year for the assets, with overall market cap growing over 12x. We show a lot more statistics later in this note.

**Chart 1: Cryptocurrencies market cap ($bn)**




Source: Coin Dance

There are two plausible ways to analyse coins, we think. You could approach the matter quantitatively or technically, as some do with more traditional FX products, looking for past statistical relationships, chart patterns etc. Both of these approaches are based on taking precisely zero notice of what underpins the prices being analysed. However, coins have a very short trading history, making it hard to say too much here.

[1] Yes, we know he didn't write it, nor was his the first version. But it's the one most people know.

[2] 22nd May 2010 is known as "Bitcoin Pizza Day" in the coin world, according to Coindesk ("Bitcoin Pizza Day: Celebrating the Pizzas Bought for 10,000BTC", 22.5.2014)

Our commodity and FX analysts have examined at least bitcoin in these terms, and we draw upon their work in this piece. In brief, they see clear issues with bitcoin, but also clear positives, including liquidity and diversification.

## What sets coins apart?

The bulk of this note focuses on a completely different approach. We try to look at what individual coins, and the cryptocurrency movement overall, are actually good for. Once you work out what distinguishes each coin, it becomes easier to understand what conditions might, or might not, lead to it being worth more than its current market value and how it may disrupt the current market. Perhaps the most important thing to understand about coins, we think, is that this is a less straightforward question than it sounds.

### Bitcoin – not a great P2P platform

When bitcoin was first launched, it was probably seen as a mix of an interesting intellectual experiment, a political statement and an alternative to playing World of Warcraft. It was, for a time, seen as a vehicle for peer to peer payments, and then other payments, before becoming more akin to "digital gold". We think it's important to recognise that actually, in its current implementation, bitcoin's not really very good at making payments, especially smaller payments.

### Ethereum – smart contracts at the core

Within the increasing menagerie of coins, Ethereum's key characteristic is that it is a Turing complete smart contract platform. It therefore allows people to perform a multitude of functions which are not practicable on the bitcoin blockchain. It hosts a lot of DApps and ICOs. It is moving towards a different validation mechanism to bitcoin and its relatives.

### Ripple – FX, IOTA – IoT

Ripple is different again, in that it clearly is targeting a more institutional audience, especially banks and other financial institutions who need to transfer money across borders. Bitcoin Cash and Litecoin aim to be faster than bitcoin. IOTA employs a radically different approach to cryptography, and is designed to work with IoT.

### Our focus

The list goes on. Our objective is to begin to explain what has to happen, for more fundamental factors to drive value, rather than current drivers which seem more momentum-based. We also look at what needs to happen to the whole ecosystem to make coins a more investible asset.

## Tinker Bell school of value – don't let bitcoin die

We don't try to value the various coins. We think the whole area is too new to allow for any precision here. As the sector develops it may become more susceptible to valuation. At present, we are to an extent in Tinker Bell territory: "Every time a child says 'I don't believe in fairies' there is a little fairy somewhere that falls down dead", according to JM Barrie in *Peter Pan*. "Do you believe in fairies? If you believe clap your hands. Don't let Tinker die". In a similar vein, we think that there is some of the digital equivalent of hand clapping required with coins at the moment. Simply put, we don't know yet whether a lot of the conditions we set out will be met. There is a possible universe where bitcoin is undervalued, as well as one where it is grossly expensive; ditto for Ethereum and the rest.

## Our views

This note is largely an attempt to provide a framework for thinking about the coins in a mainstream way. We do not provide investment recommendations anywhere in the note, rightly so as the field is too new and the uncertainty too great. Nor do we provide valuations.

### Bitcoin – brilliant, innovative, showing its age

We think that bitcoin (BTC) is an extraordinary intellectual achievement. To have a $71bn asset, trading several billions of dollars a day with virtually no budget, and without an obvious founder, CEO or anything, is remarkable.

However, we think that bitcoin is at the moment struggling to find a role beyond the brand name. In particular, the mining construct and the fee load make it an expensive way of moving value from one party to another.

Nor is it unique. Bitcoin Cash (BCC) only recently split from the main bitcoin chain. In many ways similar, it aims to address bitcoin's scaling issue by allowing higher block sizes, and its moving spirit is also looking to build other services on top of the chain. Litecoin (LTC) is also relatively similar to bitcoin.

There is an undoubted value in having a pre-eminent market position, and BTC has this. It may be able to parley this into a position of economic strength. It may be able to evolve to be a mighty payment platform (some argue that Lightening Network can do this). However, our view is that its time to do so is limited, as it is not unique, and that its somewhat anarchic governance makes it difficult for it to change.

### Ethereum – smart contract pioneer

Ethereum is the number two cryptocurrency, but it has a number of advantages over bitcoin. It is cheaper to run. It has in Vitalik Buterin[3] a founder and figurehead who seems relatively successful in steering the platform and dealing with the inevitable challenges it faces.

Ethereum's USP[4] is that it offers a Turing-complete programming language which permits "smart contracts" to be executed on the Ethereum blockchain. In turn, this has allowed Ethereum to be used for ICOs (see later). An early ICO, the DAO, provided a major challenge to the system, but one which it survived. Because Ethereum's coin, ether (ETH), is heavily used to fund ICOs, we think a large part of the potential value of Ethereum is its role as the money supply for ICOs.

### Ripple – FX transactions made easy?

Ripple is a venture funded company whose coin, the Ripple (XRP), can be used to facilitate FX dealing. Ripple offers enterprise software for banks and financial institutions. This aims at simplifying FX transactions. This has been taken up by a number of credible institutions. You don't need to use of XRP to use Ripple's software, but the company believes that the coin can have a role to play in FX transfers especially in the less liquid currency markets.

If this is right, given the size and volumes of the FX markets, it's not hard to see how you can justify XRP's valuation. This is, though, quite a big if.

We note that XRP does not rely on mining, and so it is a much cheaper service to run than bitcoin or Ethereum.

## Other coins – let a thousand flowers bloom

There are plenty of other coins in the digital universe. We know that the "thousand flowers" is a misquote for a hundred; the fact is, though, that there are more than a thousand flowers blooming, or at least coins digitally clinking, at present. We've profiled three, two which look like bitcoin and one, IOTA, which aims to be the ledger of choice for the Internet of Things ("IoT").

[3] Somewhat appropriately for someone who may be presiding over a future tech giant, he dropped out of University to promote Ethereum.

[4] Unique selling point – we try to define the various TLAs we unleash in the note, as well as the coin names.

We think that it is probably good to have a large number of flowers blooming, or more precisely competing. However, the ease by which coins multiply, divide and evolve suggests to us that scarcity is likely to be very hard to impose. Importantly, the key achievements which underpin the coin movement are open source and not copyrighted. In our view, the best strategy in these circumstances is to try to be Amazon like, and capture enough "mind share" to act as a moat.

### Coin versus company

One last complexity. With bitcoin, although there is a Bitcoin Foundation, it's hard to see much economic value in this. At the other end of the spectrum, Ripple could be a major success without XRP being used much; XRP's value depends, we think, on how people choose to use Ripple's software. We are still in the foothills of trying to work out how IOTA's coin benefits if IOTA itself manages to gain significant share of IoT. It is important when looking at both the larger coins, and the ICOs, to differentiate between the coin and operating business which may be associated.

## Through difficulty to the stars

The focus of this note is on understanding what impact today's coins, and more generally, the whole technology behind coins, could have on mainstream finance. To begin, though, we discuss in outline some of the technological background to the topic. We think it's important to understand the general outline of the technology, as without this, it's hard to gauge its potential impacts.

# Crypto what? Alt delete?

Cryptocurrencies are now capitalised at around $138bn. This represents significantly more than the amount of notes and coins in circulation in Korea[5]. Ten years ago, the equivalent figure was zero.

Clearly, zero to $138bn is a growth rate which will not likely be repeated, on simple mathematical grounds. But many remain big believers in the future of cryptocurrencies. Over the past few years, bitcoin has gone from its first real world transaction – two Papa John's pizzas for 10,000 coins (implying a value of give or take 0.3 cents per coin) to around $4,800 a coin now.

## What is a cryptocurrency?

Cryptocurrency "refers to a math-based, decentralised convertible virtual currency that is protected by cryptography.—i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy[6]", according to the Financial Action Task Force.

This is a bit of a mouthful, but actually quite helpful. To unpack it:

### Decentralised

That is, there is no central issuing authority, as there is with, say, the US Dollar.

### Convertible

This means the currency can be converted into real world money; this is in opposition to non convertible currencies like the ones you find in some role playing games.

### Virtual currency

This is a digital representation of value which "is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency"[7].

So, the Dollar is the Dollar because the US Government says so. Bitcoin is bitcoin because the bitcoin community agrees it to be so. This actually brings us to the heart of bitcoin, and a lot of altcoins, the "dispersed trust function".

### Protected by cryptography

The blockchain, hashing and mining are the means by which bitcoin is protected, but other coins use different methods. We will look at Ethereum and Ripple later, and each of these has its own approach. IOTA is radically different to all these.

### Distributed

This means that there is no one canonical database, as there is with, say, the data underpinning our various bank accounts. There are instead a number of "nodes" with full copies of the data.

### Decentralised

Not only are there more than one instances of the database, the decision as to which version is "right" is for the overall community not one trusted entity.

### Secure

This is as a result of the cryptographic work underpinning the currency.

---

[5] Source: CMPI

[6] "Virtual Currencies Key Definitions and Potential AML/CFT Risks", FATF report June 2014, available on their website.

[7] Ibid

### Information economy

Just a way of saying that the coin is based on "information" – i.e. it's digital, and to do with the economy – i.e. you can sometimes use it to buy things.

### More detail in our primer

If you want more details on the mechanics of blockchain, please see "Blockchain: exploring the potential".

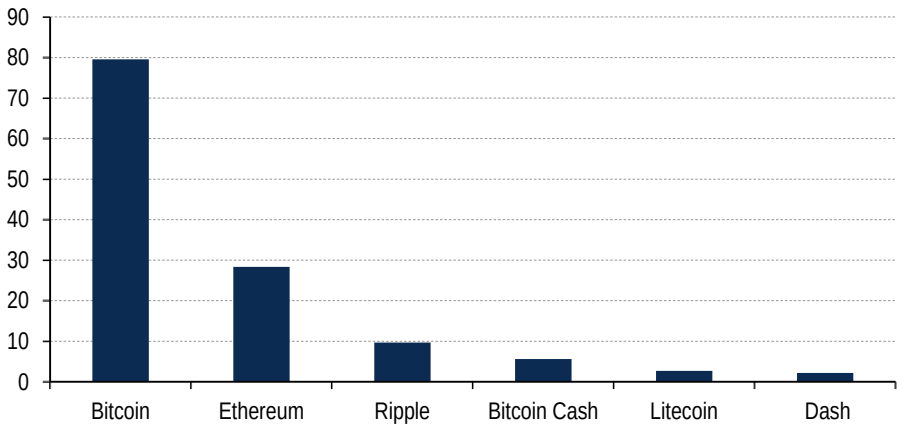
### Large number of potential coins

This actually is a good definition. Importantly, though, it delimits a very broad (we would argue infinite) set of possible coins. We have tended to use Dogecoin as an example of a midsized coin, because it is a reasonable size (number 54 in coinmarketcap's list of coins at present, with a market value of ~$111m), and seemingly good natured. The name puns on "dog", its logo is a Shiba Inu, and it brands itself as "the fun and friendly internet currency…with an amazing, vibrant community made up of friendly folks just like you". Its community has raised funds for the Jamaican Bobsled team and a Kenyan irrigation project. We could quite as easily have picked Bytecoin (BCN), which is larger (~$245m), or Mooncoin, which is much smaller (~$12m) but claims to be "faster than bitcoin"[8]. Overall, there are over a thousand to choose between.

## Larger coins – market cap, performance

We show below the six largest coins. Bear in mind that these prices tend to be very volatile.

**Chart 2: Cryptocurrencies - market cap ($bn)**

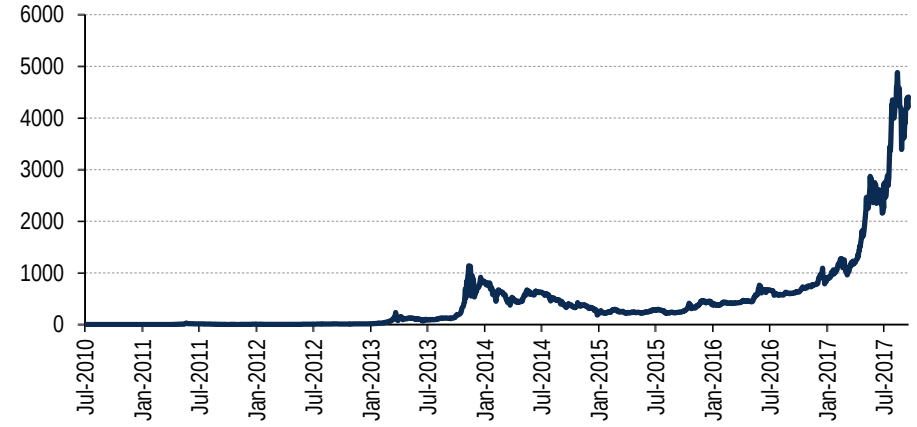



Source:CoinMarketCap

The coin world has had a heady 2017. We show below the prices of bitcoin, Ethereum and Ripple.

[8] According to its website, it has a block time of 90 seconds, which is faster than bitcoin, which adds a block around every 9 minutes.

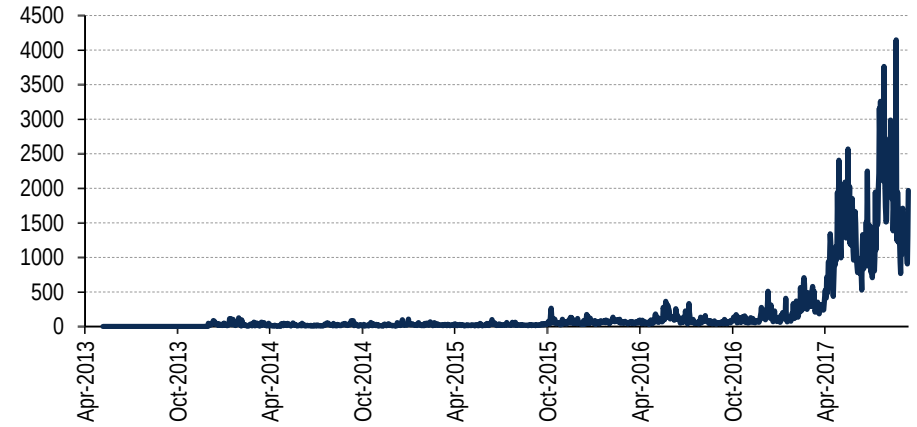
**Chart 3: Bitcoin - price in US$**




Source: Bloomberg

Ae well as performing strongly, bitcoin has also seen volumes grow dramatically, as the chart below suggests.

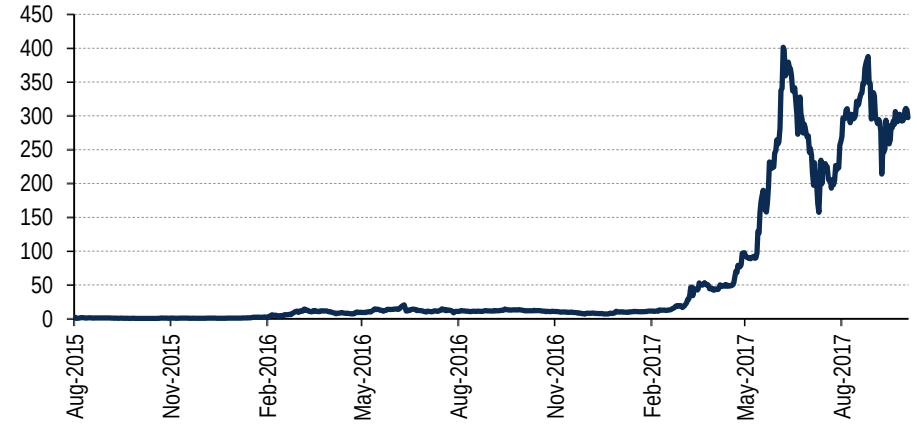
**Chart 4: Bitcoin - Daily volume ($m)**




Source: CoinMarketCap

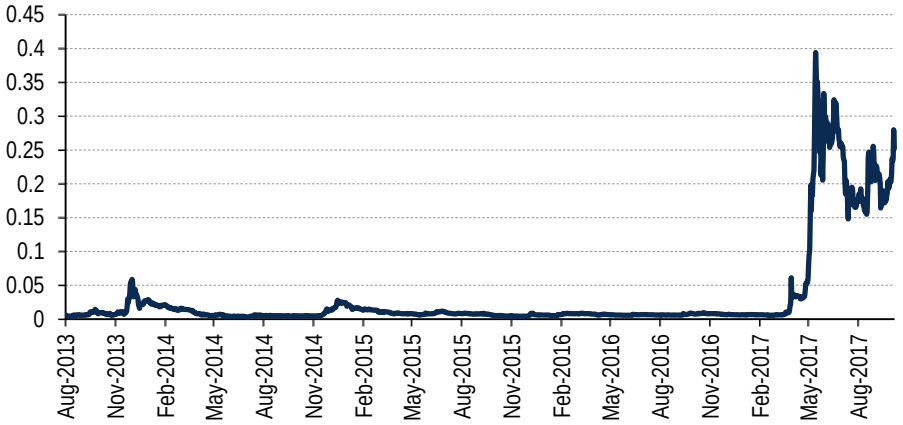
This increase in volumes in itself suggests that bitcoin could be taken more seriously by the financial community.

**Chart 5: Ether - price in US$**




Source: CoinMarketCap

**Chart 6: Ripple - price (US$)**




Source: CoinMarketCap

These graphs aren't the easiest to read, so we show below some static performance data.

**Table 1: Price performance**

| | Ether | Ripple | Bitcoin |
|---|---|---|---|
| 2015 | | -76% | 38% |
| 2016 | 762% | 7% | 133% |
| YTD 2017 | 3540% | 3855% | 170% |

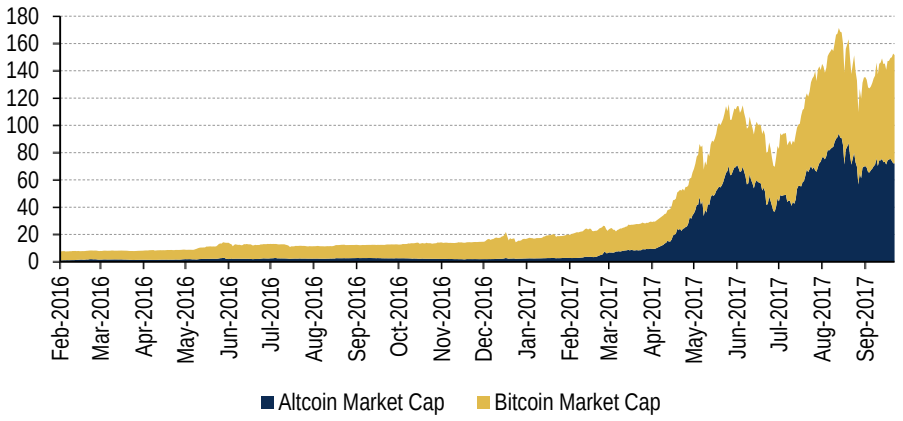
Source: CoinMarketCap

These are big moves and even these don't tell the whole story, as they do not reflect large intra-day swings.

### Bitcoin, altcoin market caps

More generally, it's interesting to look at the performance of bitcoin, the best known cryptocurrency, and the alt coins. We show this below.

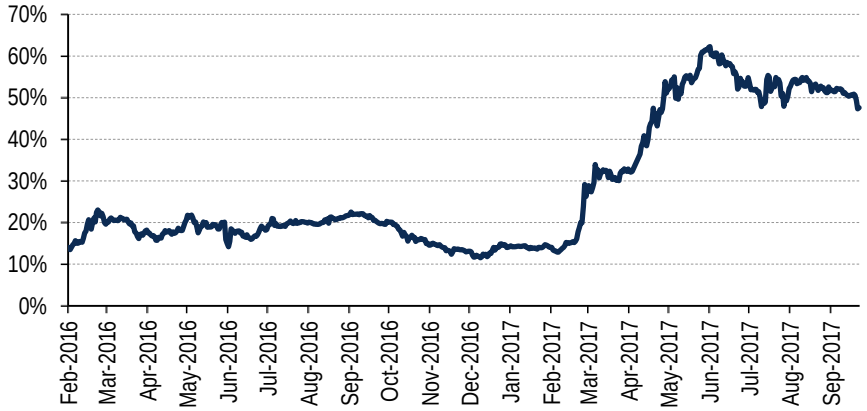
**Chart 7: Cryptocurrencies market cap ($bn)**




Source: Coin Dance

Total coin market cap is about $150bn. Within this, the altcoins have gained significant share. We show below how much of total market cap it represented by altcoins.

**Chart 8: Altcoins as a percentage of total market cap**




Source: Coin Dance

This year has overall seen a major increase in the share of value represented by altcoins. This underlines the importance of looking at the whole coin universe, not just bitcoin.

## Understanding bitcoin

To recap, bitcoin is a "cryptocurrency", that is, a "currency" created and transferred by cryptographic means, in this case, the bitcoin blockchain.

Bitcoin was invented by Satoshi Nakamoto[9] who published the invention in 2008 and released it as open-source software in 2009. However, it built on a number of existing technologies. People had been building distributed ledgers for decades before bitcoin. The bitcoin, though, provided some intriguing answers to the obvious questions which distributed ledgers posed.

Here's how Nakamoto's paper starts.

*Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.*

*What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.* [10]

[9] A pseudonym; the internet will provide a range of theories about who Satoshi Nakamoto really is, if s/he is a single person.

[10] "Bitcoin: A Peer-to-Peer Electronic Cash System", Nakamoto, 2008, bitcoin.org.

Bitcoin transactions occur when somebody decides to send a bitcoin (or fraction of a bitcoin) to another, presumably in payment for some good or service. Person A will already have obtained some bitcoins, and will store these in a digital "wallet". If A wants to pay B $10, they simply open their "wallet" (which in reality is likely to be a smartphone app[11]), and enter an amount and a destination bitcoin address. B will provide this. In retail transactions, this is often done by scanning an icon which looks like a QR code. Once A has hit send, this will create a record, containing A and B's addresses and the amount transferred. This record is sent to the ledger, which is "distributed" – that is, here, there and everywhere.

To make this payment, A will use a digital "key" (maintained in the "wallet"); the key process ties into another branch of cryptography.

**Linking up to the chain - mining**

At this point, the transaction is not actually part of the blockchain. What makes the blockchain so powerful is the process of creating blocks. A block is often likened to a page on a ledger. It contains a discrete number of transactions. The innovation of the blockchain, which we think has genuine applicability in finance, is that the blocks are made incredibly hard to change once created ("impossible" is the word usually used here, in fact – this is a question well beyond our competence, but we would simply point out that it is not impossible to change fraudulently the records which current finance depends upon – this is what some types of hacking do).

A block lumps together a number of time-stamped transactions together. It does this by taking the transaction data[12] and adding some other standard fields, including the hash of the number of the preceding block.

**What is a hash?**

A hash is an alphanumeric representation of a particular message. No two messages can have the same hash, and you cannot modify the hash without changing the message. You cannot work from the hash to the message, but if you know the message, you can check that an individual hash corresponds to that message.

Starting from this material, the bitcoin "miner" manipulates the data by changing the "nonce", some random alphanumerics added at the end of the block. If the core message is, for example, "Adi, Philip, Francisco [13]", this would generate a certain hash. "Adi, Philip, Francisco1" would generate a different hash, as would "Adi, Philip, Francisco2" and so on. To be successfully "mined", the data has to have a nonce which leads to a hash starting with a certain number of zeros. Both the number of zeros and the fact that it's zeros at all are simply social conventions of the bitcoin. You could choose to require ten "Z"s instead, and the same principle would apply.

This is a non-trivial problem. Miners typically have a "mining rig" of specially configured computers which churn through possible solutions until a hash appears which meets the requirements of the chain. At this point, a new block has been created, and the ecosystem can move onto the next set of transactions. In passing, mining has become a material industry. For instance, our US Semiconductor analysts have produced an interesting note looking that he impact of mining demand on semiconductor manufacturers.

[11] Plenty are available for both Android and iOS.

[12] Well, OK, not actually the transactions themselves but the "Merkel root" of a "Merkel tree" containing the transactions.

[13] The authors of this note

In theory, two different miners can come up with a new block at the same time. In this case, the block which is most used by subsequent miners will "win" over time. We presume that geography is a factor here. If you are a miner in New York, you are likely to be close to a lot of other miners. A miner in a small Pacific atoll will be less close, and so disadvantaged by latency. Whatever, this "branching" of the chain is, apparently, very rare, and resolvable. The block which is used least will become an "orphan".

### Quantum computing

We have seen some articles worrying that quantum computing will undermine bitcoin's security, because the power these could deploy would enable them to calculate bitcoin owners, private keys from their public keys. In turn, this would undermine the whole dual key approach which underpins bitcoin. We have also read about services which seek to link people's bitcoin addresses to other known data about people, making bitcoin transactions potentially less private than they are often assumed to be[14].

### Why mine?

Although we suspect that some people would mine just because they enjoy the challenge (after all, people do crosswords and run marathons), bitcoin incentivises people to mine by paying them. The reward for mining a block is ownership of a certain number of bitcoins. The reward halves roughly every four years; by around 2041, it is estimated that the limit in the number of bitcoins of 21m will be reached, and the reward for mining will be zero. The last number we saw was 12.5 bitcoins per block. Based on this and the value of the bitcoin, you can work out profitability metrics for mining, driven by the cost of the kit you need, electricity etc, and the expected number of coins you will mine. In passing, mining is often seen as being pretty non-green, as it demands a lot of computer power which in turn demands a lot of electricity to drive the computers, and also to keep the mining rigs cool.

The mining process is how new bitcoins are created. Bitcoins are viewed as non-inflationary because the number reaches an asymptote at 21m. Some other coins have built in inflation.

### How do you acquire bitcoins?

The classic example of using bitcoins is buying coffee in Seattle. Before you can do this, assuming you are not a miner, you have to buy bitcoins. You can buy bitcoins in a similar way to how you can buy other digital goods (e.g. books for your Kindle) – with proper money. There are a range of exchanges which will effect this swap for you.

The biggest bitcoin-related issue we have seen actually related to this process, not the bitcoin itself. Mt. Gox was a bitcoin exchange operating out of Tokyo which, in its prime, was one of the biggest venues from swapping between bitcoin and proper money. In February 2014, it suspended trading, and subsequently liquidated, having announced that around 850,000 bitcoins belonging to the company and its customers had disappeared.

This account highlights some of the issues with the bitcoin, as well as some of its strengths.

## Key strength – it is operational

The key strength is simply that bitcoin is operational – people are using it to transfer value. Although there have been issues, these seem to do with interfaces between bitcoin and the rest of the world (exchanges, wallets etc), not the bitcoin itself.

It is also global (you can buy your latte-in-Seattle from Singapore, Sunderland, Stockholm or Sudan, without hassle and without the various fees which beset proper currencies when they venture outside their currency areas). Also, the bitcoin system

[14] See, for example, "US Law Enforcement Have Spent Hundreds of Thousands on Bitcoin Tracking Tools", Joseph Cox, "Motherboard", 25.5.17

prevents the bane of transaction systems, people using the same funds to pay for two or more different items (so-called "double spending"), at last as long as you are prepared to wait for your transaction to form part of a block.

## Weaknesses – regulation, volumes, real world interface

However, we think there are substantial challenges that would need to be overcome before bitcoin could end up as the core of some kind of new financial system. Obvious issues include:

- Lack of an interface with the rest of the world – the issue of exchanges is symptomatic here. Unless there is a robust interface between bitcoin and "real" money, it will remain of limited interest to financial companies.
- No guarantee of mining.
- Relatively low volume - (there are around 200,000 transactions a day, according to blockchain.info).
- Blockchain "bloat" – the chain keeps getting bigger.
- No clear entity to regulate – the "here, there and everywhere" nature of the bitcoin appeals to some, but present difficulty to regulators, who want to know who is responsible for any issues and malfeasance.
- Tax status unclear or unhelpful. For example, in the US, bitcoin is viewed as a commodity, and so subject to taxation, rather than a currency.

## Three coins in a digital fountain – consensus mechanisms

Bitcoin, ether and Ripple are all clearly cryptocurrencies, but they use (or are about to use) different consensus mechanisms. To recap, cryptocurrencies do not have a central authority determining the canonical version of the truth. Instead, truth emerges out of a consensus mechanism. The idea behind coins is that they could work if you assume no trust between the various market participants (this is sometimes expressed as the mechanism would work if you assumed a community of bandits). Mainstream finance works on the basis of having a central trusted party, which is then scrutinised, regulated and so on.

### Proof of work

Bitcoin's approach is to use "Proof of Work" (POW). As we have already described, POW involves some cryptographic task being fulfilled. Broadly, if over 50% of the processing power present on the chain arrives at a version of the truth, that is the truth. As Nakamoto put it:[15]

*The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers.*

There are various different types of consensus algorithms used, but the idea is the same.

### Proof of stake

Ethereum also uses POW at present, but it is looking to migrate to a different consensus system, Proof of Stake (POS). Here, rather than defining truth as the account supported by a majority of computing power, consensus is determined by obtaining a majority of stakeholders. Ethereum is planning to move to a version of its software called "Casper", at which point one block in a hundred will be generated using POS, the

[15] Nakamoto, ibid, P1

rest POW. According to Vitalik Buterin, a prototype of "Casper the Friendly Finality Gadget" was "close to being finished" in the beginning of July.[16]

The advantage of POS is that it should be much cheaper than POW. POW weighs computing power, which in reality is also weighing electricity. In POS, typically there is no seigniorage. Instead, the miners just receive transaction fees. This can be regarded as an interest rate paid on the funds the miners (worryingly, POS miners are also called "forgers"). According to Buterin, in a Reddit post, the interest rate will be "somewhere around 2-15%".

Ethereum's proposed implementation of POS includes what it calls "slashing conditions", which means stakeholders losing the funds they have deposited should they violate the pre established rules.

### Validation

Ripple does away with both mining and forging. It instead has a group of validators who validate transactions. According to Ripple, validation is costless to the node.

### DAG

Bubbling under, there is a wholly different approach, the DAG, which we describe in the context of IOTA. This does away with the whole idea of a blockchain in favour of the "directed acyclic graph".

## Three blockchain incidents

The whole technology behind the coins is new and innovative. It is hardly surprising that some things have, to put it one way, worked better than others. In the interests of balance, we have described three incidents which form part of the "others", as examples of when the blockchain system did not work as planned.

### Number 3 – Bitfinex hack

Bitfinex is a cryptocurrency exchange. Since the demise of Mt. Gox (see below), it has typically seen the largest market share of the exchanges[17]. In August 2016 it announced that 119,756 bitcoins, worth around $72m at the time, had been stolen. According to Wikipedia, "Significant hacker funds transactions were signed off by Bitfinex's security provider, without full security".

To its credit, Bitfinex both survived, and paid back the clients who had their assets stolen, although this took a few months.

In spite of this, the fact that clients of a leading piece of infrastructure lost $72m to start with does highlight why we talk later about enhanced infrastructure being important for the coins universe.

### Number 2 – the DAO

This was a major incident in the world of coins, but it is also arguably contributed mightily to Ethereum's development. The DAO ("Decentralised autonomous organization") was intended as a community directed venture capital fund. It was crowdfunded via a token sale in May 2016. The idea was that individual investors would vote on proposed investments chosen by a nominated manager[18]. This whole process was to be executed via smart contracts, taking advantage of Ethereum's capabilities.

Sadly, in June 2016, some malefactors moved a third of the DAO's funds into a subsidiary account. This was clearly contrary to the intentions of the DAO's promoters, but it was in keeping with the DAO's coding. This set off a vigorous debate about how to respond. Some argued that "the code is the law" and therefore although the action was evidently abusive, it was nonetheless valid. Others took the contrary view; Vitalik

[16] "Roundup Q2", in Ethereum Blog, 8.7.17

[17] Bitcoinity has useful data here.

[18] The SEC's Release No 81207, available on its website, provides a lot of detail.

Buterin, the moving spirit behind Ethereum, fell into the latter camp, and he prevailed on the community to deploy a hard fork restoring the state of the Ethereum chain to how it was before the DAO hack.

This was not universally supported; some coin owners rejected this fork, and instead opted to move into "Ethereum Classic", a system with in essence the same code as Ethereum, but without the hard fork. Both versions of Ethereum implemented software patches which would stop future attacks such as the one suffered by the DAO.

Although this was not a glowing endorsement of Ethereum, the leadership the community showed seemed to have been reassuring, and certainly it has not damped enthusiasm for subsequent ICOs. However, this does show that code can do odd things, and that, in our view, the code isn't the law; the law is the law, and the code is at best a useful way of automating certain processes.

**Number 1 – Mt. Gox**

The undisputed world heavyweight coin fiasco, Mt. Gox was the largest coin exchange globally, handling over 70% of bitcoin transactions[19] by 2014. Prior to 2014, it had experienced a few "teething troubles": namely a security breach in 2011 and a legal dispute with CoinLab.

On 7th February 2014, Mt. Gox suspended all withdrawals from its accounts.

At the end of February, it filed for bankruptcy in Japan (where it was based), saying that it had lost almost 750,000 of its customers' bitcoins, and around 100,000 of its own bitcoins, totaling around 7% of all bitcoins, and worth around $473 million near the time of the filing.[20] Its CEO at the time said he was working to recover the missing coins. In April 2016 it officially filed for liquidation. Perhaps unsurprisingly, the CEO subsequently has had various encounters with the legal authorities in both Japan and the US. On 11th September 2015 he was accused of embezzlement by the Japanese authorities. His case has yet to come to trial.

**So what?**

In a way, so nothing. Mainstream finance is not without its lawsuits, and few industries are immune from both questionable behaviour and fiascos. However, we think it is important to acknowledge that the coin world has certainly attracted its fair share of these. Its suggestion of an environment where security is guaranteed by consensus has yet to materialise. In fairness, the bulk of issues we have seen are to do with the interface between bitcoin and the "real world" – both Mt. Gox and Bitfinex were probably issues with the traditional cybersecurity of entities providing a link between cryptocurrencies and traditional finance. The DAO is different – it was wholly an internal issue. We are impressed by how effectively Ethereum has recovered from this but it does highlight how radically new systems can behave in strange ways when put under stress.

## Looking at coins fundamentally

Having set out some general background to the coin world, we now look at the three largest coins by market value in detail, followed by a quick tour through some of the more interesting coins inhabiting the next few slots in the market value list.

[19] Bitcoinity

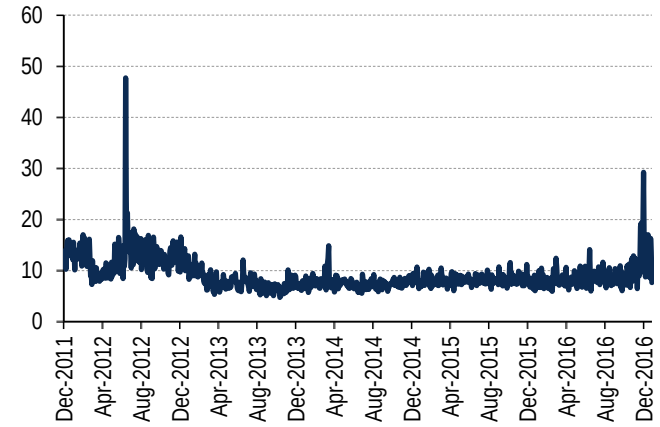
[20] A lot of this account comes from Wikipedia, some from Coindesk.

# Bitcoin

Bitcoin is the best known digital currency, we think, and definitely the largest. It has a long record of operating, at least compared to its competition. We have discussed some of the issues surrounding bitcoin already. The most important technical issue, we think, is to do with the coin's capacity to scale.

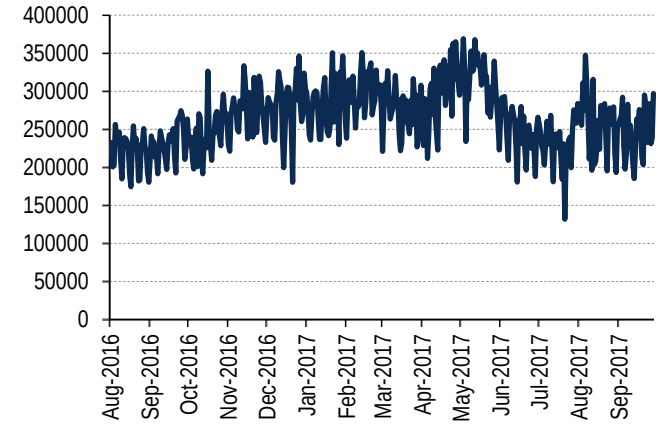
Bitcoin, for all its technical elegance, is not a fast, high volume system. Below we show the average confirmation time for a transaction and the number of transactions per day.

**Chart 9: Median confirmation time (mins)**




Source: Blockchain.info

**Chart 10: Transactions per day**




Source: Blockchain.info

Thirty minutes seems a very normal average wait time for confirmation, with peak transaction volumes representing around four transactions a second. Nor, as we show later, is it cheap, with transactions fees averaging $2.40 in Q2 17, ignoring mining revenues. In addition, as we've already shown, although it was the first cryptocoin to gain much publicity, it is now competing with a wide range of coins, including the schismatic Bitcoin Cash.

## Forking

The recent bitcoin split ("fork"), which created Bitcoin Cash, poses important questions for those looking to value bitcoin.

**What is a fork?**

Bitcoin operates with a "blockchain" – a chain of blocks. In a chain, one link follows form another. However, on occasion, the chain can split into two. This is a fork.

A fork is normally a bad thing; it suggests that there are two versions of reality. However, there are occasions where a fork is deliberate, and arguably positive. The split of Ethereum into Ethereum and Ethereum Classic is one example. The split of bitcoin into bitcoin and Bitcoin Cash is another.

There are two types of fork; a soft fork is a backwards compatible change, something like a software upgrade. A hard fork introduces a new rule into the system which isn't compatible with the existing software.

The back story to these forks is that the bitcoin blockchain has become increasingly slow and unwieldy. This is because as bitcoin ages, so its history grows. Remember, the system works because every note has the entire blockchain. Each block makes this bigger.

There have been a number of suggestions about how to prune the bitcoin blockchain. The current consensus approach is SegWit2x.

**OK. SegWit2x?**

There are two parts to this proposal.

Firstly, the bitcoin blockchain will implement "Segregated Witness", or SegWit. This means that more transactions can be included in a block without raising block size. It does this by stapling "Segregated Witnesses" containing signature data to the blockchain, without them forming part of the blockchain. The chain contains a pointer to these "Witnesses". The pointers are smaller than the "Witnesses", which therefore shrinks the chain.

The second change is a bit more direct. It is simply to double the size of allowable blocks, to 2MB.

The two components are phased. SegWit has been agreed and implemented. The 2MB hard fork is supposed to take place around 1st November. It requires 100% miner support, according to Coindesk.

The rollout of SegWit was the proximate cause of the fork between bitcoin and Bitcoin Cash. Bitcoin Cash (BCC) boosts bitcoin's capacity by increasing the maximum block size to 8MB, and doesn't implement SegWit. So, although BCC very much follows Nakamoto's original design, it and bitcoin are incompatible. They run different, incompatible software. The bitcoin equivalent of the assassination of Archduke Franz Ferdinand was the mining of a block larger than 1MB, which happened at 6.14pm UTC on 1st August 2017. At this point, there were two different chains in existence. In theory, BCC could have withered on the vine after the block was mined[21], but in reality, more blocks were produced.

As a result of the fork, someone who owned 100 bitcoin before the fork owned 100 bitcoin and 100 BCC after the fork. This is because both coins have exactly the same ownership history, and it is the history which generates an ownership claim.

There are a range of practical issues surrounding this. Chris Skinner, a well regarded fintech expert, discussed them in a useful article "Forking hell"[22]. He points to two knotty issues:

- Replay Attack – where a transaction meant for one network might get sent to another one. Given the two coins have very different prices, this would be potentially difficult.
- Support from exchanges – a number of exchanges have said that if clients have coins stored with them, the BCC will effectively be lost.

Mr. Skinner says of the second "It is yet another sign of how flaky this cryptocurrency market is – the DAO hack, the Mt. Gox debacle, the Bitstamp affair, the Bitfinex loss, the Parity Wallet breach … the list is endless". This is a fair point; the coin ecosystem is, in our view, improving but is not yet where it needs to be.

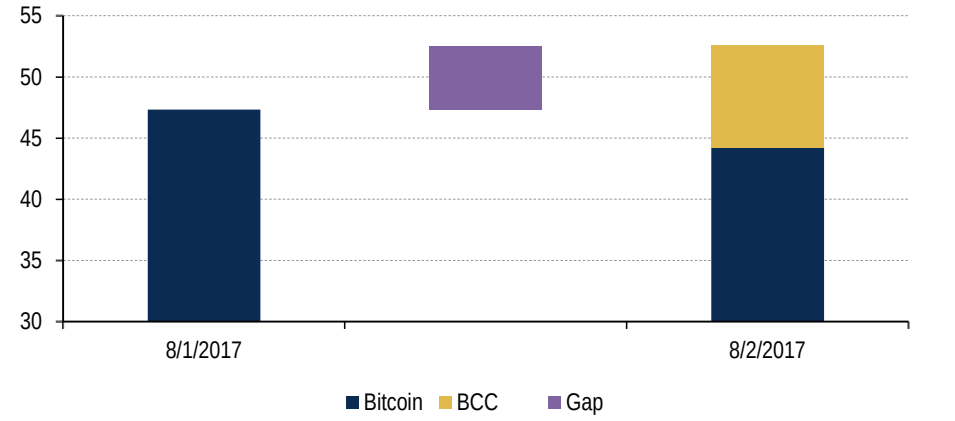
However, let's park practical issues. These can always be fixed with enough effort. The fork raises an important theoretical issue, too. The number of coins in circulation doubled as a result of the fork; this is an inevitable consequence of the mechanics (the

[21] The blockchain mechanism occasionally generates orphan blocks, which disappear if further blocks aren't added to them.
[22] "Forking hell --- the bitcoin split", available on his website, 24.7.17

fact that the two chains by definition have the same history). To state the obvious, gold is not like this. You do not suddenly find that your ounce of gold is now an ounce of gold and an ounce of silver.

Theoretically, the hard fork is like a company distributing an asset in specie. The total package of assets before and after distribution should be worth the same. Pricing in coins is less reliable than pricing in equities, but it seems pretty clear that this law of parity has been broken by the bitcoin hard fork. We show below the price of bitcoin on the day of the fork, and the next day, when BCC was trading.

**Chart 11: Bitcoin fork arbitrage ($bn)**




Source: CoinMarketCap

We know that coins are volatile, and a price move of 11% (the arbitrage spread) over a day is conceivable. However, the 2nd doesn't look to have been a particularly volatile day for other coins. Ether, hardly a low vol asset itself, was up around 0.5%, Ripple by 1.5%. So, it's reasonable to believe that the fork generated money for nothing, which is not the sign of a mature market.

Granted, there was a material technical reason for the fork – the difference of opinion about whether to proceed with SegWit2x or raise the maximum block size. However, we find it worrisome that a relatively large, liquid asset can seem to allow for the creation of $5bn of value out of thin air. The ability to generate new coins is a worry for valuation of existing assets, as we discuss below. The ability of existing coins to create valuable fission products is if anything more worrisome.

## What is bitcoin good for?

We think there are four elements to bitcoin's potential value.

- It was originally seen as a method of making peer to peer payments, cutting out a lot of middlepeople and avoiding government interference.
- It is also often viewed as a store of value, somewhat like digital gold.
- It is also in some quarters seen as a speculative asset.
- It also can be used to subscribe to many ICOs.

## A payment system

The first of these is clearly in Nakamoto's mind; s/he writes

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other[23]

[23] Quoted earlier

### Bitcoin is expensive as a payment system

The problem with bitcoin as a peer to peer payment system is that it's expensive, relative to conventional alternatives. This comes from the mining process. Mining isn't a zero sum game. The economics of mining are pretty simple. There is a fixed reward per block mined. At present, each block generates 12.5BTC. So, each block mined produces in Dollars around 12.5*bitcoin/dollar rate. At present, this is around $60k per block. This is a function of the bitcoin price. There are roughly 2000 transactions in a block, give or take. This implies that around $30 of bitcoin are created per transaction at present. Economically, we would regard this as a cost of the transaction, although this is not how people always view it. This cost should fall as the amounts of BTC per block continues to halve, but is also a function of the BTC price.

In addition to the creating bitcoins, the rough equivalent of seigniorage in "real" money[24], people pay fees alongside transactions. Like many things to do with bitcoin, fees sound a bit weird at first, but the system is roughly that people transacting bitcoins may "choose" to add a fee along to a transaction. Fees are optional, but in the words of "Blockchain blog",

*Bitcoin transactions are in place as an incentive to miners when validating bitcoin blocks. One of the reasons there is a fee is because the larger the transaction data size, the longer and more energy it will take miners to validate the data. Transactions with higher transaction fees tend to be validated faster in the blockchain.*

#### 240c per transaction in Q1 17 (plus mined bitcoins)

A key variable here is how many bytes each transaction represents. The more complex the transaction, the more bytes. Fees are not strictly enforced like transaction fees in normal banking, but if you don't include appropriate fees, there is a serious risk that a transaction won't be processed by a miner. According to Coindesk, the average fee for mining in Q1 17 amounted to 240c per transaction. This is easily the highest average fee recorded (Q4 16 was 24c, Q4 15 was 6c).

So, even ignoring the bitcoin earned by miners, fees alone make bitcoin unsuited to many retail transactions.

Ah, people sometimes say, that may be expensive for a small transaction, but it is highly competitive for larger transactions (like buying a car). And this is true. The issue is that for larger transactions, counterparties are highly likely to wait for a transaction to be validated before parting with goods (a variation on "cash on delivery"). Typically, blocks are mined every 10 minutes, but there is no guarantee that any individual transaction will be included in a newly mined block.

So, at present, people are faced with a mixture of financial and administrative impediments to using blockchain as a payment mechanism.

Also, blockchain's irreversibility is a two edged sword. All kinds of functionality which normal retail payment systems allow, especially reversing a transaction, simply aren't possible in bitcoin.

The upshot is that as presently constituted, we think it is hard to see bitcoin becoming a mass payment channel. Some argue that the "Lightening Network" can solve these issues.

### The size of the problem

Before looking at this, it's worth setting out the scale of these issues which a genuine retail payments system faces.

[24] You could argue that the real seigniorage is the profit made by the miners.

### Visa – 56,000 transactions per second capacity

To illustrate, Visa's payment system processes 2,000 transactions per second, on average, and can handle up to 56,000 per second, if needed. Assuming similar transaction handling capabilities at other large payment schemes such MasterCard, UnionPay, AliPay etc, total digital payment transaction volume in the retail space can be an order of magnitude higher than the aforementioned 2,000 transactions per second. Assuming 20,000 retail transactions are processed every second, it would take about 100 minutes for one second's worth of transactions to be recorded on the bitcoin blockchain.

### Online payments – 20bps for a large, mainstream merchant

Similarly, coming to payment economics, online merchants pay payment processors anywhere between 20bps to 5% depending on various factors such as merchant size, charge back risks involved, additional value added services provided, location of the merchant (US and APAC higher than Europe), type of payment method and so on. 20bps would represent a large merchant in a low risk domicile. The upper end of 5% would represent a potentially risky counterpart. We believe looking at online payment processors is more relevant than instore payment processors as we believe bitcoin payments are more likely to be used in online payments than in instore payments, as we explained in our Blockchain primer.

### $1200 breakeven

If you take 240c as a fee for processing a bitcoin transaction (and bear in mind, we think the real economic cost is much higher, due to the seigniorage component), and a 20bps fee, this suggests that for a merchant, you need a transaction in the order of magnitude of $1200 for bitcoin to break even. This is, to state the obvious, rather more than either a latte even in Seattle or two Papa John's pizzas.

In addition, payment processing prices have been falling, due to a multitude of factors but mainly regulation (Interchange fees in Europe, fee waivers for SMEs in India etc) and volume based discounts as digital payments grow. Given the strong opportunity from increasing adoption of digital payment methods, we believe incumbents may be inclined to further reduce pricing if they see any significant risk from blockchain based retail payment methods.

### Peer to peer payments

A lot of commentary involves Alice sending bitcoins to Bob, which is nice of her. We understand that there are situations where this is difficult using conventional means. If Alice lives in London and Bob in New York, this can often be an expensive and painful process. Were Alice to live a range of developing nations, the problem could be worse. We think there is a real opportunity for some kind of alternative cross border FX service to develop (we are modestly pro Ripple because of this, though there are issues with Ripple here). To be fair, there are other attempts at solving this issue which seem to transfer money more cheaply than the mainstream banks, too; Transferwise and Currencyfair are potential examples.

However, if Alice and Bob are both Londoners, the existing banking system allows P2P transfers rapidly, even if they don't share the same bank, and costlessly for normal sums. Were they Indian, they could send cash up to a certain limit[25] between each other for nothing via bank enabled smartphone apps. Were they Swedish, they could use Swish, a well accepted, free P2P payment system which has even become a verb – "I'll Swish you"[26]. Yes, we know that typcially nothing is costless in banking, but if you have a mainstream bank account to start with, there is typically nil marginal cost.

[25] 1000 Rupees, which at about $17 covers a lot of small transactions.

[26] "Jag swishar dig", actually.

### Other issues

We also see a number of other hindrances to adoption of public blockchain based retail payment methods as we noted in our Blockchain primer.

## Lightening network – clever, will it work?

Lightening Network is sometimes suggested as an answer to bitcoin's scaling issues. Lightening required Segwit2x to be operational, so could be implemented now that the hard fork has been solidified. We are unaware of any implementation timescale, though according to media reports a number of companies are looking to build Lightening applications for bitcoin.

### Bilateral, off chain "channels"

As with many things to do with bitcoin, Lightening is clever. The basic idea, though, is simple. Rather than blasting every transaction out into the ether, you set up dedicated "micropayment channels" between entities, and every so often report net settlement transactions to the network. It's not a million miles away from equity clearing[27], where counterparties only settle net balances. The benefit of this is that it would reduce the number of transactions written to the blockchain, hence reduce blockchain bloat, mining costs and fees.

This seems straightforward.

*If Alice and Bob commit funds into a 2-of-2 multisignature address (where it requires consent from both parties to create spends), they can agree on the current balance state. Alice and Bob can agree to create a refund from that 2-of-2 transaction to themselves, 0.05 BTC to each. This refund is not broadcast on the blockchain. Either party may do so, but they may elect to instead hold onto that transaction, knowing that they are able to redeem funds whenever they feel comfortable doing so. By deferring broadcast of this transaction, they may elect to change this balance at a future date.*[28]

The issue here is that setting up channels between every participant is a cure which arguably is as bad as the disease. It works fine in equity clearing because there are relatively few clearing members of a CCP, and by definition, each clearing member has only a relationship with the CCP, not the other members (it is a "hub and spoke" design). However, in a bilateral environment, the number of connections increases rapidly, in a non linear way[29].

Instead, Lightening proposes a much broader set of off chain payments. The precise details here are intricate, and feel at first sight somewhat overworked. Visa does not rely on hashed timelock contracts, commitment transactions and other exotica. The idea, though, is that if Alice wants to send Carol a payment, and Bob also has a channel open with Carol, he can be used as an intermediary; the setup becomes a cryptographic version of the "six degrees of Kevin Bacon" game[30]. The network relies on a series of automated game-theory like arguments to incentivise A, B and C to cooperate in the transfer. The mechanics sound complex, but presumably can be automated in some kind of wallet.

### Applying to retail transactions complex

We shall see. The A and B version is pretty straightforward, although some of the mechanics strike us as unwieldy. For instance, one of the enforcement mechanisms involves A and B effective committing collateral to the channel. This can be redeemed,

[27] Traiana does something very similar in FX.

[28] "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments", Poon and Dryja, 14.1.16, available on Lightening website, P5

[29] It's actually a combination. There are n!/(k!(n-k)!) combinations of k members from a set of n. In this case, k is 2 and n is the total set of users. 1000 users in theory call for almost 0.5m channels.

[30] This account has benefitted from "Understanding the Lightening Network" by Aaron van Wirdum for Bitcoin Magazine.

but only after a certain number of bitcoin blocks have been mined. Also the process relies on prefunding the channel from existing bitcoin resources. Presumably, the network would be used to make payments, which would involve relatively frequent topping up of the channel. If you assume that Alice actually wants to use her Lightening channel to, you know, buy stuff, rather than shunt BTC between her and Bob, then she will have to add BTC to the channel when necessary, which means that she will be generating normal BTC transactions. Also, if we assume that B is, say, Boots or Ben and Jerry's or any other retailer (Overstock famously accepts various coins as payment now), it will also want to crystallise its payments frequently. Maybe the fact that Alice's payment to retailer B may end up going via a range of other alphanumerics, with Z making some kind of net payment to B, may reduce the number of on chain transactions. However, netting procedures in finance typically work because you have a small number of counterparties who make payments to each other. Retail involves a large number of participants (Adi, Philip, Vadim etc) making by and large unidirectional payments to retailers.

### Still conceptual

So, Lightening may work. We understand the excitement it is generating. But at the moment, it is very conceptual, and at the moment, we think that bitcoin suffers from structural impediments to becoming a mass payment channel.

Anecdotally, coin enthusiasts sometimes prefer Ethereum as a payment mechanism, as its mining costs are cheaper than bitcoin. We would tend to prefer Ripple to both of them, albeit in its limited use case of cross border transfer, because this seems an efficient piece of enterprise software. Lastly, Lightening is not specific to bitcoin. If it adds some extra efficiency to payments, it could be deployed in a range of coins.

### Taxes – potential complexity

We are not tax experts, nor can we offer tax advice. However, it's worth noting that in at least some countries, using bitcoin (or other coins) as a payment method may have tax implications. For example, in the US, the IRS considers coins to be like property. If you pay for goods using coins, you may generate a tax liability.

*Q-6: Does a taxpayer have gain or loss upon an exchange of virtual currency for other property?*

*A-6: Yes. If the fair market value of property received in exchange for virtual currency exceeds the taxpayer's adjusted basis of the virtual currency, the taxpayer has taxable gain. The taxpayer has a loss if the fair market value of the property received is less than the adjusted basis of the virtual currency.*[31]

In other words, if you were to buy a bitcoin, have it sitting in your digital wallet for a week, during which time its price appreciates, then use it to buy something, you may have realised a gain which may be taxable. The UK appears to take a roughly analogous view:

*"Gains and losses incurred on Bitcoin or other cryptocurrencies are chargeable or allowable for CGT if they accrue to an individual"*[32]

This does not seem ideal for a payment medium. In theory, assuming that this reading is correct, somebody who pays for a string of small ticket items using bitcoin or other coins may in fact be generating a string of taxable gains and losses.

## Digital gold

Another potential source of value for bitcoin is as a store of value. In this context, it is often called "digital gold". Bitcoins and gold have three important common attributes:

[31] IRS Notice 2014-21

[32] Revenue and Customs Brief 9 (2014): Bitcoin and other cryptocurrencies

neither pays any interest, the supply of both is limited, and both are more difficult to trace than most financial assets (except cash).

That said:

- Bitcoins are much more volatile than gold, which makes bitcoins a riskier asset to own.
- The reputation of gold as a unique and safe store of value has been growing for the past ten thousand years. It will take some time for bitcoins to acquire that reputation.

One benefit of bitcoin over gold and silver (and indeed paper money) in that it is easier to transfer. Although bitcoin is more traceable than either paper money or bullion, it offers a degree of anonymity. It is also harder than these assets to confiscate.

## Unit of account

This is a pretty straightforward no. We do see a lot of coin prices quoted against bitcoin, but its volatility makes bitcoin a poor unit of account, we think. Eventually, volatility may subside and so this might become a more viable role for the currency, but at present, we wouldn't ascribe much value to this role.

## ICOs

Although ICOs are generally part of the Ethereum ecosystem (see our discussion of Ethereum), many ICOs allow people to fund them with bitcoin as well as ether.

## Means of exchange

For now bitcoin remains the predominant cryptocurrency because of its first-mover advantage. It remains to be seen if it will be displaced in payments by newer, cheaper-to-send currencies.

## "One chain to bind them"

The remaining source of value lies in what we would jargonise as "optionality". We have pointed out already that a lot of gold's value probably lies in its history and track record. Whilst bitcoin hasn't been around for long, it has been around for a lot longer than most other coins, has the best known "brand name" in the area and genuinely has a history of technology that works, within its limitations (which we have explored already).

A number of people we have talked to in our work have likened coins to the early days of the internet. We doubt if anyone properly understood exactly what the internet would end up doing, or the uses to which it would be put. However, it could well have seemed valuable, simply because it had so much unspecified potential.

In the same way, it is very hard precisely to pinpoint what makes bitcoin valuable. However, there must be some worth in being the best known coin with the longest track record and technology with the longest history. We have talked about the "Tinker Bell" theory of value – if enough people believe something is valuable, it is. However, another way of looking at bitcoin is to say that bitcoin is perhaps like Amazon in its earlier years. Until the early to mid-2000s, the company either lost money, or made very little. However, it was judged valuable, and this judgement seems to have been validated.

What Amazon did in the 90s and early 2000s was build its reach, footprint, mindshare or whatever piece of jargon you feel like choosing. It has increasingly used the position it built to add extra services, and geographies, and to enhance profitability. Similarly, you could argue that bitcoin at the moment could be investing in building footprint, mindshare and so on. At some point, the world will want a cryptocurrency, and will find a major use for it. At this point, bitcoin will be the obvious first port of call.

**Do we believe this?**

Bitcoin's history and visibility are a differentiator for it. However, it faces issues.

### Governance a problem

The key problem it faces, in our view, is governance. A range of people from Jeff Bezos down have been intensely focused on making Amazon valuable. Ripple has a visible CEO and management structure, as well as a business development team.

Bitcoin has a founder whose gender is unknown, who may in fact be more than one person, and who seems to have disappeared regardless. Who or whatever Satoshi Nakamoto is, she, he or they is/are not dynamically driving forward value creation at bitcoin in a Bezos-like way.

Similarly, conventional payment systems employ salesforces who try to get merchants to use their services. Conventional channels also tend to invest in attracting customers, too. Bitcoin doesn't, largely because it can't.

### Now or never

Our guess, and it is a guess, is that unless something as yet undetermined catapults bitcoin into the big league soon, even if coins in general become an increasingly large part of finance, it is likely that the winner will be a less idealistic coin. Ethereum offers the ability to execute Turing complete code on its system. The Ethereum Foundation may not be Jeff Bezos, but it has a significant role. Ripple is a classic piece of enterprise software. Bitcoin Cash aims to offer bitcoin with fewer bottlenecks, as does Litecoin. IOTA is radically cheaper, assuming the cryptography works.

In the Cambrian explosion of coins we are now witnessing, is it obvious that the long term winner will be early entrants like an organic walled tube or a sponge? Or will the scene end up being dominated by entities which build on the undoubted advances made by these organisms to develop legs, eyes and suchlike?

BlackRock CEO Larry Fink has raised the same issues in a slightly different way, telling "Bloomberg" that he is "a big believer in the potential of what a cryptocurrency can do. You see huge opportunities, but what we're talking about today, it's much more of a speculative platform"[33].

### Has bitcoin missed the tide?

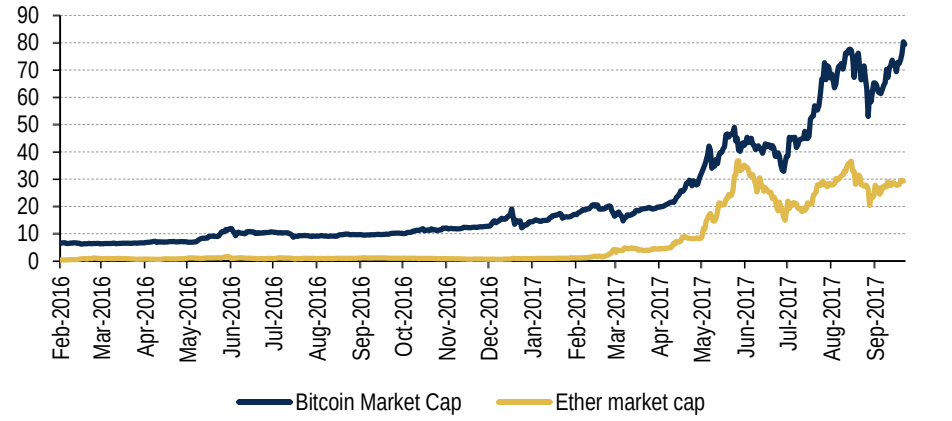
Bitcoin is a magnificent proof of concept that something like its blockchain can work. However, so far it looks to have not made much headway in its obvious agenda, to provide a "purely peer-to-peer version of electronic cash". Unless Lightening proves to be a massive success, we think bitcoin is simply too expensive to fill this role. Even if Lightening works, we think it can equally work on cheaper, faster networks (there is talk of rolling Lightening out in Ethereum, too, for example).

[33] "BlackRock CEO Larry Fink Is a 'Big Believer' in Cryptocurrency", Nikhilesh De, CoinDesk, 3.10.17

# Ethereum

Although ether has been a strongly performing coin, at one point coming close to bitcoin's market cap, it is in theory a very different entity.

**Chart 12: Bitcoin, Ether market caps ($bn)**




Source: Coin Dance

To quote the Ethereum Foundation's website,

*Ethereum would never be possible without bitcoin—both the technology and the currency—and we see ourselves not as a competing currency but as complementary within the digital ecosystem. Ether is to be treated as "crypto-fuel", a token whose purpose is to pay for computation, and is not intended to be used as or considered a currency, asset, share or anything else.*

Ethereum sees itself as an environment in which users can create a range of applications using blockchain and smart contracts. Ether is the currency needed to pay for smart contract functionality, and also for a range of Initial Coin Offerings ("ICOs") also hosted on the Ethereum platform. On this reading, ether is more like a season ticket for the underground than a currency.

### Smart contracts

Smart contracts are, in our view, a neat idea, without being a unique selling point for Ethereum. A smart contract is a piece of code embedded within a distributed ledger. The concept of using a piece of code to achieve a particular effect on certain conditions isn't new. These used to be called "sprites" in the "good old days"; "they are effectively little "ghosts" or "geists" that act autonomously"[34].

**Smart contracts**

In our view, smart contracts are neither smart, nor contracts. They are, typically "if…then" statements. "If the price of gold is over $1,300, pay the owner the difference" would represent a call option on gold. "If the date is either 30/6 or 31/12, pay the bearer $5" would represent a fixed income security. As a result, smart contracts are often seen as having applicability to finance. However, they have many other applications, too.

They aren't smart because they are simply an exercise in following orders, however daft the orders might me – we discussed the DAO fiasco earlier. And they aren't contracts, as in themselves they have no particular legal status; they can of course derive legal status if people agree to be bound by the outcome of smart contracts.

[34] "Why Smart Contracts Need Shrewder People", Mainelli and McDowall, coindesk, 2.4.2016

Ethereum is a distributed ledger built to support and facilitate using smart contracts.

**Can smart contracts eradicate default risk?**

No, as we argued in our note on distributed ledgers and finance. A smart contract can automate an instruction to make a payment in a given situation, but it can't actually make that payment unless there are funds available for it to do so. Unless the party to a contact is willing to place adequate funds in an escrow account, which would work ex smart contracts too, the credit risk remains the same as before.

Ethereum has, in our view, done well in developing an ecosystem which others both want and feel able to use. There is an argument that the Ethereum Foundation has done a better job than its bitcoin counterpart in providing a common front to the outside world and in managing the Ethereum infrastructure. That said, Ethereum has had a range of issues, which we talk about below.

If you look at Ethereum from our perspective of what is it good for, though, it seems as if there are two components to ether's value:

- Payment for using the Ethereum applications platform.
- Potential upside from "Initial Coin Offerings".

### Value of Ethereum software

Ethereum has, in our view, established a smart contract platform and environment which many find useful. You can see that from the number of partnerships which are being announced with Ethereum. For example, there is the "Enterprise Ethereum Alliance", set up to provide "a clear roadmap for enterprise features and requirements" whilst using Ethereum. Members here, according to the Alliance's website, include BNY Mellon, Cisco, CME, Credit Suisse, DTCC, J.P.Morgan, Microsoft, Santander and UBS.

It has also a wide range of third party built DApps, decentralised applications built using Ethereum technology. People who are interested can browse these at their leisure.

### Initial Coin Offerings ("ICOs").

An ICO is a process whereby typically a startup or very early stage company issues coins to investors to fund the company's development. Investors in ICOs are hoping (expecting?) that the venture will be a success, and that this will cause the coins to rise in value.

Ethereum is actually a great example of an ICO. Ethereum was first described by Vitalik Buterin, who produced a white paper in late 2013 (ICOs tend to produce a white paper, a kind-of unregulated sort-of prospectus). There was a sale of coins in July-August 2014, with investors buying coins using bitcoin. As we've already seen when we discussed the price of ether, it would have been good, in retrospect, to have bought ether at its initiation, or at any point last year, to be fair. Of course, Ethereum could also have turned out to be useless, over buggy or in some other way unattractive, and the coins would have gone nowhere.

According to Smith + Crown, a research firm who specialises in ICOs, 2016 saw around $100m raised in tokens (i.e. ICOs). This was a multiple of funds raised in2013-5. Q1 17 saw just under $40m, a notable pick up in the pace of issuance, and in Q2, amounts raised "dwarfed" all previous quarters. "In June alone, more funds were raised … than in every other month…to 2013". Coinschedule, another data source, suggested that total funds raised were around $560m.

## Why do companies opt for ICOs?

ICOs provide funds with funding (in the form initially of coins) in exchange for some kind of ownership rights, although the exact nature of these can be obscure. Why do companies opt for this method, rather than the obvious other routes of looking for venture funding or listing on any of the various SME markets which target small tech companies around the globe?

There are, we think, a number of reasons. Clearly, different reason will motivate different issuers, and more than one may apply.

### Culture

For some, we suspect that an ICO just "feels right". If you are a company looking to produce a distributed ledger solution to, say, selling groceries (maybe some kind of IoT approach linked to a bluetooth enabled fridge), you will probably feel culturally aligned to obtaining capital through some kind of distributed ledger. This is probably quite persuasive, especially if you also believe that the ICO route is a viable one.

### Valuations

We have already shown recent price performance data for ether. Someone who had invested $30,000 in ether a couple of years ago could easily now be a paper millionaire. One natural response to this would be to cash out some ether. Another would be to diversify away from the coin, whilst remaining within the ecosystem, zeitgeist and so on. ICOs provide a clear way of doing this. An early ether owner could easily commit to a few ICOs, take a significant profit in Dollars and retain a decent exposure to ether.

We understand that a fully rational economic person would treat both paper profits which almost certainly exceeded someone's wildest dreams and their salary in precisely the same way. We also understand that most people won't!

### Regulation

ICOs are not in general subject to the attentions of the SEC, ESMA, the FCA and so on. This has its attractions. The requirements of a listing even on the light touch growth markets in Europe are relatively significant (see our note on equities). Being able to publish a white paper, then issue a coin is a much easier route to follow than meeting the diligence requirements of a regulated market. Venture money has a different set of standards, but also is in its own way a very demanding environment. Venture investors, too, tend to want to have at least the ability to interfere bigly in the running of their investees.

To be clear, the white papers we have looked at are often interesting, sometimes quite detailed but usually not overflowing with financial details.

Because ICOs aren't securities, at least in the minds of their promoters, and not therefore under the ambit of the SEC, they are not bound by the SEC's requirements about qualified investors and the like. To be qualified to invest in an ICO, broadly, you have to own directly some coins.

To provide some context, we show below an extract form the Gnosis white paper (which has a lot of details about what sound like an interesting if as yet unbuilt platform)

*GNO tokens are functional utility tokens within the Gnosis platform. GNO tokens are not securities. GNO tokens are non-refundable. GNO tokens are not for speculative investment. No promises of future performance or value are or will be made with respect to GNO, including no promise of inherent value, no promise of continuing payments, and no guarantee that GNO will hold any particular value. GNO tokens are not participation in the Company and GNO tokens hold no rights in said company. GNO tokens are sold as a functional good and all proceeds received by Company may be spent freely by Company*

*absent any conditions. GNO tokens are intended for experts in dealing with cryptographic tokens and blockchain-based software systems.*[35]

### For how long?

The SEC itself has recently expressed views (or even Views) on the matter of ICOs. We recommend the whole judgement[36] , but the Commission's press release gives a decent summary.

*The Securities and Exchange Commission issued an investigative report today cautioning market participants that offers and sales of digital assets by "virtual" organizations are subject to the requirements of the federal securities laws. Such offers and sales, conducted by organizations using distributed ledger or blockchain technology, have been referred to, among other things, as "Initial Coin Offerings" or "Token Sales." Whether a particular investment transaction involves the offer or sale of a security – regardless of the terminology or technology used – will depend on the facts and circumstances, including the economic realities of the transaction.*

*The SEC's Report of Investigation found that tokens offered and sold by a "virtual" organization known as "The DAO" were securities and therefore subject to the federal securities laws. The Report confirms that issuers of distributed ledger or blockchain technology-based securities must register offers and sales of such securities unless a valid exemption applies. Those participating in unregistered offerings also may be liable for violations of the securities laws. Additionally, securities exchanges providing for trading in these securities must register unless they are exempt.* [37]

In other words, it all depends, but the SEC has ruled that at least one high profile ICO (which we will talk about further in a few paragraphs) was a security. The SEC's report sets out a number of tests for being counted as a security in the US, and shows how, in its view, the DAO satisfied these. These include[38]

1. Securities law applies to virtual organisation
2. Investors in the DAO invested money
3. With a reasonable expectation of profits
4. Derived from the managerial efforts of others.

In passing, we would highlight 2, as in fact, investors invested ether. In the words of the SEC, "'money' need not take the form of cash".

### Europe?

We have seen a reasonable amount of discussion from Europe about distributed ledger technology, and some mention of coins and ICOs, but no regulatory guidance. In the words of a lawyer specialising in blockchain technology:

*What follows from the above is that there is very little certainty on whether and how to apply the EU securities law to tokens and ICOs.*[39]

### China?

Finally, China has recently decided to ban ICOs. According to Coindesk, the Chinese regulators' statement translates as:

---

[35] Section 8.1 – white paper available on company website

[36] The SEC's Release No 81207, available on its website.

[37] SEC press release 2017-131, available on its website.

[38] SEC's release, III B refers.

[39] "ICOs in the EU: How Will the 'Slow Giant' Regulate Tokens?" Jacek Czarnecki, Coindesk, 24.7.17

*ICO financing refers to the activity of an entity raising virtual currencies, such as bitcoin or Ethereum, through illegally selling and distributing tokens. In essence, it is a kind of non-approved illegal open fund raising behavior, suspected of illegal sale tokens, illegal securities issuance and illegal fund-raising, financial fraud, pyramid schemes and other criminal activities.*[40]

Those who persist with ICOs will be "investigated and severely punished according to the law".

The Chinese announcement at least coincided with a noticeable sell-off of the larger cryptocurrencies, in our view reflecting the economic importance of the ICO model to them.

## Will these conditions last?

Our view is that typically, regulations catch up with technology. It may be unwise to expect ICOs to remain outside regulations for the medium term; indeed, the recent SEC release would suggest that this is indeed the case for at least the US, and clearly the format now is extremely risky in China, which has historically seen a lot of coin trading activity, judging by both the location of some large exchanges and the prevalence of the BTC/CHY cross. It may be that as ICOs become more regulated, their appeal diminishes.

The cultural argument seems a decent one, but ultimately will probably be dominated by the question of whether ICOs are seen as representing an effective means of raising funds. This is likely to depend on regulations, but also on how successful and scandal free the current crop of ICOs proves to be. Zeitgeist is all well and good, and we can quite understand people who have found themselves to have made material paper gains on ether being willing to invest some of these on less than fully formed schemes. We are less sure, to put it mildly, that people would continue to do so were their current investing experience to be overwhelmingly negative.

### SEC taking enforcement action

In this context, we note that there are attempts at self-regulation here in the form of the SAFT standards. The SEC is also "cautiously optimistic" on its ability to get to grips with ICOs.[41] To underline this, it has also laid what seem to be its first ever charges against an ICO:

*According to the SEC's complaint, investors in REcoin Group Foundation and DRC World (also known as Diamond Reserve Club) have been told they can expect sizeable returns from the companies' operations when neither has any real operations.*[42]

## Why do ICOs matter to Ethereum (and bitcoin)?

Let's assume that within the coin assets trading or being issued today there are next decade's FAANG stocks. Further, let's assume that the regulators broadly leave well alone, and that there are no massive scandals within the ICO universe (to be fair, existing capital markets have their own scandals).

On this basis, which represents what we regard as a best realistic case, coin issuance could provide a considerable support to the value of ether, and potentially other coins. This is simply because the "money supply" required to fund coin issuance will be significant. That said, we would highlight a couple of issues.

### Plenty of smart contract environments

Smart contracts are hardly "secret sauce". Ethereum has provided a distributed ledger which allows people to develop smart contact applications easily, but we continue to

[40] China Outlaws ICOs: Financial Regulators Order Halt on Token Trading, Coindesk 4.9.17

[41] Hon. Jay Clayton, SEC Chair to the House Financial Services Committee, 4.10.17 – see Committee's website

[42] SEC press release 2017-185

read about smart contracts being employed in a range of applications without Ethereum's involvement. For example, a lot of derivative applications in derivatives use smart contracts.

### Competition

Ethereum is not alone in looking to use a distributed ledger to raise funds for companies. Bitcoin has fulfilled a similar role in ICOs (including ether's). We talk about this in our section on bitcoin. In addition, more conventional venues are looking to adopt distributed ledgers for issuance. For example, the LSE has worked with IBM to build a distributed ledger to digitise issuing SME private securities. The system uses Hyperledger's blockchain framework.

#### Exchanges – a lot of advantages

The LSE, and other mainstream exchanges, offer considerable advantages to the ICOs in terms of access to mainstream investors, regulation, due diligence and so forth. They have significant marketing teams to recruit potential IPOs. Importantly, we continue to believe that any kind of distributed ledger is likely to prove unsuitable for many trading applications. The higher volume markets (cash equities, FX, futures) tend to operate with latencies which any system with nodes in, say, London and New York will be unable to match simply because of the laws of physics[43].

Also, the exchanges are exploring the use of distributed ledger technology in issuance, as well as in a range of registry functions. So they are well placed to employ similar technology, if in a very different ecosystem.

## Ethereum as a transaction medium

On the numbers, Ethereum actually offers a better way of transferring funds than bitcoin.

#### Speed

Ethereum tends to produce a block in well under a minute. This is significantly faster than bitcoin's ten minutes average per block.

#### Cost

The average fee on an Ethereum transaction is much lower than on bitcoin, too. Fees per transaction are routinely a tenth of those paid on bitcoin (source: bitinfocharts).

#### Seigniorage

This is perhaps a bit lower than bitcoin, but still pretty significant. We calculate that on a typical day, this could amount to something in the range of $12.5 per transaction.

[43] The time it takes for light to travel from London to New York is greater than the time you can transact on Turquoise – see our previous note on distributed ledgers and capital markets.

# Ripple

Ripple is a very different entity to bitcoin and Ethereum. In essence, it is a piece of enterprise software with a coin attached, whose objective is to simplify cross border FX. It isn't mined, and appears to be genuinely a cheap alterative to the status quo. It is neither the product of a few devotees coding, nor of a Foundation; it's a mainstream, venture funded corporate. The most recent funding round we are aware of is a Series B funding, which raised $55m. Overall, Ripple has received funding from a range of prestigious names, including Andreesen Horowitz, Google Ventures, Seagate technologies, Santander (via their innovation fund) and the CME.

## Fast, scalable, cheap, what's not to like?

Ripple's website lists its virtues as "Fast, Scalable, distributed". In terms of speed, the website cites payments settling in 4 seconds and that although it consistently handles 1,500 transactions a second, it can scale to handle "the same throughput as Visa" (50k+ transactions a second). Ripple isn't mined, so its transfer is relatively cheap (a few fractions of an XRP disappear with each transaction, but these don't go to the company).

### Consensus by validation

Instead of mining, Ripple works with "validator nodes", which, as well as distributing transaction data, also play a part in building the ledger. Validators don't receive any fees. According to Ripple, running a validator "is comparable in cost to running an email server in terms of electricity". It argues that being a validator has essentially zero added cost to running a Ripple server to process transactions. In terms of validators' motivations, according to Ripple "the primary incentive to run a validator is to preserve and protect the stable operation and sensible evolution of the network". The list of validators in the first instance is set by Ripple, but individuals can choose their validators. To quote the company: "Currently, Ripple provides a default and recommended list which we expand based on watching the history of validators operated by Ripple and third parties. Eventually, Ripple intends to remove itself from this process entirely by having network participants select their own lists based on publicly available data about validator quality."

So, Ripple's consensus mechanism is neither proof of work nor proof of stake. It has the benefit of being pretty cheap to run, and presumably is also effective, as we haven't read any complaints about the integrity of Ripple's ledger.

## What does it do?

Crudely, Ripple offers a piece of enterprise software and a coin.

### The enterprise software

This is a messaging system for banks (xCurrent), which isn't a million miles away from Swift in functionality. In the company's words "xCurrent is Ripple's enterprise software solution that enables banks to instantly settle cross-border payments with end-to-end tracking. Using xCurrent, banks message each other in real-time to confirm payment details prior to initiating the transaction and to confirm delivery once it settles." This seems to be gaining support from the banking community, judging by the logos featured on the company's website (which include Santander, UniCredit, UBS, Standard Chartered, BMO. RBC, Bank of Tokyo Mitsubishi and CIBC).

In a similar vein, there is xVia, which is "for corporates, payment providers and banks who want to send payments across various networks using a standard interface. xVia's simple API requires no software installation and enables users to seamlessly send payments globally with transparency into the payment status and with rich information, like invoices, attached."

### The coin

XRP, Ripple's coin, is a potential bridge between currencies. Ripple is clear that nobody needs to own XRP, apart from a pretty nominal holding, but XRP can be useful in moving funds between less liquid currencies. Ripple often talks about "corridors" between currencies. Their point here is that sometimes the cheapest route from A to B may be via C and D. On occasion, they argue that XRP can be a useful part of the corridor.

In addition, the company believes that XRP can be especially useful for currencies where the underlying liquidity is not massive. Currently, it is looking at the Mexican market, where it believes it has an opportunity to use XRP to facilitate FX trades.

### Coin doesn't benefit from parent company

However, bear in mind that Ripple is a venture owned enterprise. It is not an ICO, or anything like. We can have views on how much the parent company might eventually be worth (leaving aside its balance sheet holdings of XRP), but this doesn't really make any difference to the worth of the underlying coin.

### XRP in the context of FX market

So, the question for the coin is how much XRP do we think investors will want to hold to facilitate FX transactions?

### Possible payment engine?

In theory, XRP is also much better suited to a lot of payment uses than bitcoin or ether, as it's so much cheaper to run. Oddly, we haven't really seen it talked about in these terms, probably because it simply doesn't market itself as a payment rail. However, something with a confirmation time of a few seconds and no mining sounds a decent place to start.

### But not unique – look at SETL and its peers

Of course, if you want a settlement rail based on a distributed ledger run by a third party software company, rather than a funky, anarchistic, zeitgeisty thing like bitcoin, then SETL would, we presume, be happy to oblige. According to its website, SETL "was launched in July 2015 to deploy a multi-asset, multi-currency institutional payment and settlements infrastructure based on blockchain technology. The SETL system will enable market participants to move cash and assets directly between each other, facilitating the immediate and final settlement of market transactions. The SETL system maintains a permissioned, distributed ledger of ownership and transaction records, simplifying the process of matching, settlement, custody, registration and transaction reporting." And, it was named the "Hottest Blockchain Startup" in the 2017 TechCrunch Europas awards. It has run a successful test of a retail payment card using distributed ledger technology, alongside Metro Bank and Deloitte. The obvious difference between SETL and Ripple is that Ripple uses a consensus mechanism, whereas SETL curates its distributed ledger. There are, it goes without saying, a number of hurdles in the implementation of any such system – please see our blockchain primer, referenced already, for more details.

The point is not that we have any great insight about SETL's likely success (we have simply come across its founders, although the factual claims about awards, tests etc are, well, facts). There are other, similar, companies looking to provide alternatives to the current payment system using new technology. The point is that as with coins, there is nothing unique about having a quick, cheap, scalable distributed ledger platform.

## FX the key

What Ripple has done well is build a system which appears to deliver appreciable benefits to a clear segment of the financial world. Its associated coin potentially has a useful role to play here, and given the size of the FX marketplace,

# The rest

There are over a thousand coins in existence. We have picked three relatively sizeable ones to focus on.

## Litecoin

Litecoin is pretty much like bitcoin. It's USP has been that it has adopted various technological improvements, such as Segwit. Technically, it also uses a different proof of work algorithm. It has also hosted a Lightening Network transaction.

### The data

Litecoin adds a block roughly every 2.5 minutes, making it around four times faster than bitcoin. Fees seem a lot lower, with a median fee of around 3c.

As it is a mined currency, there is seigniorage. Each block currently generates 25 LTC, or give or take $1,250. There are roughly 44 transactions per block, which suggests $28 per transaction, which is a material amount.[44]

### The future

Charlie Lee created Litecoin in 2011. He now works for the Litecoin Foundation. Whilst Litecoin's future development ultimately depends on what "the market" will accept, his perspective is interesting. He argues that the most important agenda item is increasing Litecoin's adoption. "I want to make sure that Litecoin is traded everywhere first, then make a convincing case why companies and merchants should use Litecoin when they need fast and cheap payments."[45]

This seems perfectly rational if you want to be used as a payment mechanism. Given the similarity between bitcoin and Litecoin, though, it also underline the lack of uniqueness of bitcoin (bitcoin and Litecoin are sometimes referred to as the cryptocurrency world's gold and silver).

Technologically, Litecoin is looking to add smart contract functionality, and a Lightening Network implementation.

### Atomic swaps?

Lee also talks positively about "atomic swaps". This seems a digital version of bimetallism. Using Lightening Network, the idea of an atomic swap is that two people can exchange bitcoin and Litecoin instantaneously and risklessly. Crudely, this works by the parties having Lightening channels open in both bitcoin and Litecoin, and using cryptography to ensure that the two opposing transactions either happen together or not at all. Clearly, this requires Lightening to be operational on both chains.

We can see why people would find this interesting – it looks prima facie quicker, cheaper and less risky than going via an exchange. However, we also think that making the two coins more fungible begins to chip away at one of the properties of bitcoin which its supporters point to – its fixed supply. This was the point of bimetallism, after all!

### Overall

To us, Litecoin highlights the lack of exclusivity of bitcoin, has some interesting features but is also grappling with the issues which bitcoin faces.

## Bitcoin Cash

Bitcoin Cash (BCC) is the smaller of the two coins which have resulted from the recent hard fork. BCC's selling point is that it increased scalability by increasing the maximum block size to 8mb (bitcoin's current limit is 1mb, rising to 2mb as part of Segwit2x).

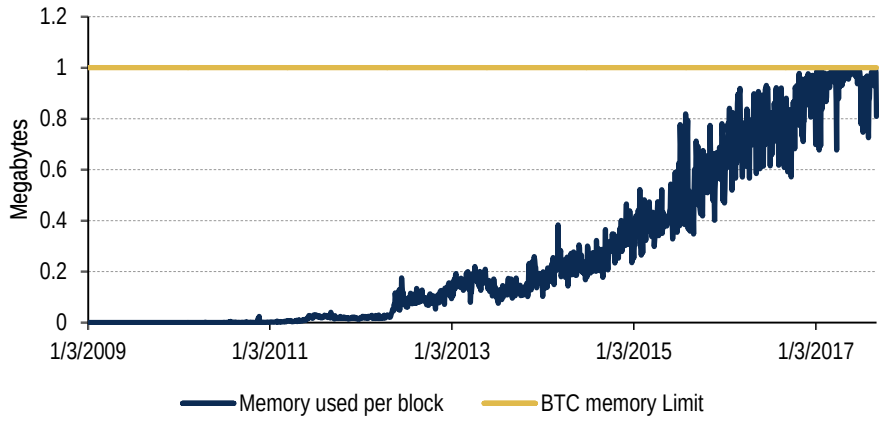
[44] These figures are all approximate BofAML estimates, as there is a lot of variability. They come from reviewing BitInforCharts' data.

[45] "Life After Coinbase: Can Charlie Lee Keep Litecoin's Revival Alive?" Coindesk, Alyssa Hertig, 7.7.17

BCC argues that the 1mb capacity limit was a severe issue for BTC. "In 2017, capacity hit the 'invisible wall'. Fees skyrocketed, and bitcoin became unreliable, with some users unable to get their transactions confirmed, even after days of waiting. Bitcoin stopped growing. Many users, merchants, businesses and investors abandoned bitcoin."[46]

It claims to be the "best money in the world", which if nothing else displays a sense of ambition.

**Chart 13: Bitcoin hit 1MB memory limit per block earlier in 2017, leading to transaction delays**




Source: BofA Merrill Lynch Global Research, Blockchain.info

**Data**

Some of BCC's claims seem more realistic than others. The median transaction fee, at 6c, is lower than BTC's. The mining reward is the same as BTC's, reflecting the fact that it is a recent outgrowth of the bitcoin blockchain. However, because BCC's price is materially lower than BTC's, the seigniorage is lower, but because the number of transactions per block is lower than bitcoin, the seigniorage per transaction is somewhat higher than for BTC. At the moment, it produces fewer blocks per hour than BTC, which makes its claims to "transact in seconds. Get confirmation in minutes" technically true (they don't say how many minutes) but not totally helpful.

**Overall**

BCC is looking to be a better bitcoin. It will be interesting to see if it is able to change its offering more nimbly than BTC; we presume this is its game plan. At the moment, though, we think that BCC underlines our argument that the scarcity value in BTC, and coins in general, is overstated.

## IOTA

And now for something completely different. IOTA is a relatively new coin. Litecoin and BCC are obviously close relatives of bitcoin, but IOTA is only a distant cousin. Like Ripple, it transacts without mining, employing a much cheaper validation system.

The idea behind IOTA is set out early on in its white paper.[47]

*Among these drawbacks, an especially notable one is the impossibility of making micro-payments, which have increased importance for the rapidly developing Internet-of-Things industry. Specifically, in the currently available systems one must pay a fee for making a transaction; so, transferring a very small amount just makes no sense since one would have also to pay the fee which is many times larger. On the other hand, it is not easy to get rid of the fees since they serve as an incentive for the creators of the blocks.*

[46] Bitcoin Cash FAQ, on its website

[47] "The tangle", Serguei Popov, 3.4.16, available on IOTA website.

Instead of a blockchain, IOTA uses a "DAG" (directed acyclic graph). It looks a bit like the sort of graphic people use to demonstrate bilateral trading relationships, and Popov, author of the IOTA white paper, calls it a "tangle". The system works by requiring that to issue a transaction, a node has to validate two other transactions, checking they do not conflict. The great benefit of this as a system is that there is no distinction between miners and users. To use the system is to validate it. As a result, the system has no fees (you could argue that the computational power needed to perform the validation is an implicit fee), no seigniorage and according to its authors no scalability issues.

As a result, they argue it is well suited to Internet of Things applications. IoT involves a lot of transactions, which would render even the cheaper mined blockchains prohibitively expensive.

IOTA is therefore positioning itself as a backbone for IoT blockchain development. We can well understand why this is an attractive concept. It's not obvious to us exactly how this development benefits IOTA coin holders, but this is leading edge stuff. The positive case for IOTA is that by buying into the coin, you are buying into "the community of developers building on top that then go on to use this token as the unit of value within the system"[48]. In a way, this is a similar argument as that for Ethereum; rather than smart contracts, IOTA has a structure aimed at IoT. The issue we have is that there is a clear link between the Ethereum community and ether – it's used to pay for computations on Ethereum and to buy into ICOs. It is less clear where the coin itself fits in with IOTA.

As with many coins, IOTA has experienced some teething troubles. Recently, researchers at Boston University and MIT found vulnerabilities in its hash function, which is a crucial piece of cryptography[49].

**Differentiated vision**

As with so much of the coin world, we would also point out that there are other coins using DAG, and that there are other potential distributed ledger solutions for IoT. For example, if a white goods manufacturer wanted to promote the bluetooth enabled fridge, it could curate a permissioned ledger itself. Nevertheless, we will continue to watch IOTA, as it has a clear, differentiated vision.

[48] VC investor Jamie Burke, quoted in "IOTA's Bitfinex Listing Surges To $1.5B Record-Breaking 'Crypto' Capitalization On Market Debut", Forbes, 15.6.17

[49] See "Cryptographic vulnerabilities in IOTA", Neha Narula, Director, Digital Currency Initiative at the MIT Media Lab, available on Medium

# Moving mainstream

What would it look like if cryptocurrencies moved into the mainstream?

## Institutional owners/liquidity providers

We think that by and large, cryptocurrencies are owned and traded by retail investors. There have been some attempts to bring them more into the mainstream, especially via proposals for various bitcoin ETFs (from the Winklevoss Brothers and SolidX). There is already an ETP traded on Nasdaq Nordic and cleared via Euroclear, although this is not massive. We are unaware, though, of major institutions investing in the asset class. Equally, although exchanges talk about liquidity providers and marketmakers, we do not think that either the large dealers or the electronic marketmaking community is committed to the area. Without support from the dealer and buy side community, we think the area will remain a quirky one.

### Venture capital – some interest

The one counterexample to this is venture capital investment. Venture investors have committed materially to a range of bitcoin related entities. Historically, venture capital has funded investments in blockchain and bitcoin related developments. According to Coindesk, around $500m was invested in blockchain by VCs in 2016, with around $100m being committed in Q1 17 and $240m in Q2. Anecdotally, some VCs are also beginning to commit to ICOs, although we think that this market would benefit from being tidied up before VCs overall will feel comfortable with it.

### Specialist cryptocurrency investment funds

We have also read commentary about some specialist cryptocurrency oriented funds being raised, some by ICO, with others using more conventional means (Polychain Capital has received funding from Andreessen Horowitz and Union Square Ventures). There is also a "Secretive Cryptocurrency hedge fund", MetaStable.[50] A strong roster of VC investors have, apparently, committed to the company, including Sequoia Capital, Bessemer Venture Partners and Founders Fund, on top of Andreessen Horowitz and Union Square.

## Industrial strength post trade

The first sign of a move into the mainstream would, in our view, be to see a significant upgrade of the post trade environment. Coins are currently held in "wallets". There are a range of wallets available, some provided by "exchanges", some not. There are occasional stories of wallets being hacked. There is also the possibility of people losing their digital keys, without which they cannot access their coins.

### Custody

This just wouldn't work for an institutional client base. Institutions demand third party custodians to look after and validate their assets. We have not heard of any of the major custodians accepting any of the cryptocurrencies as assets. This would be a major step forwards in the mainstreaming of cryptocurrencies.

Bear in mind that this is not only important in allowing institutions to access assets like bitcoin and Ethereum. The same issue pertains to ICOs. Here again, the current post trade environment is a bit free form.

### Clearing and settlement

As far as we know, cryptocurrency transactions aren't cleared and settled in the same way as mainstream financial assets. In a sense, settlement happens on chain. Alternatively, if you want to move from the crypto to the fiat world, settlement occurs with the exchanges, a process which has in the past occasionally been vulnerable to hacking, and there is no clearing.

[50] The description comes from Bitcoin.com, 28.7.17. It is **SO** secretive that it has a website with a "contact us" page.

Settlement is as important as custody in the institutional world (understandably – people want their money back). Clearing is a bit more optional; spot FX isn't cleared, but this settles on a 24 hour cycle and benefits from a lot of post trade netting, both via CLS and its JV with Traiana.

If institutional cryptocurrency volumes are going to grow meaningfully, progress is needed here, too.

### Exchanges

This is an easier fix, but we think that institutions would also welcome overall a more sophisticated exchange presence. Our understanding is that although there are a wide number of exchanges, which provide execution, price feeds and post trade, by and large these do not offer the same quality of technology as the large global exchange groups.

## Collateral?

If coins were taken as collateral by lenders, it would mark another big step forwards in mainstreaming the asset class. At present, we don't think mainstream lenders will take coins as collateral, in the way they will with bonds, equities, art and so on.

If this changed, it would have two obvious impacts:

- It would underline that cryptocurrencies have become, to a degree, mainstream financial assets.
- It would free up a lot of capital which at present may be hard to mobilise.

## On the horizon – derivative markets

Derivative markets for cryptocurrencies may be easier to bring into the mainstream than cash markets. There are some existing venues which offer cryptocurrency derivatives – Plus500, the £1bn London listed trading platform firm offers "The Hottest Virtual Coins with No Commissions! CFD service" according to its advertising. Helpfully, it adds "Capital at risk", perhaps reflecting the idea that a derivative over something as volatile as a coin may indeed not prove to be the safest of investments.

However, we are aware of two initiatives to bring cryptocurrencies into a more institutional setting.

The reason this may be relatively straightforward is that there is no conceptual difference between running a futures market on bitcoin (or technically some cross rate involving bitcoin) and oil. With coins, there is a reference price (although you would need careful rules about exactly how this is determined, given the absence of a central price feed), and an underlying asset. Oil futures can be deliverable or cash settled ("non deliverable"). In the case of the former, in theory an investor can be involved in the messy business of actually owning a tanker full of oil. In the latter, the contracts are settled by cash payments reflecting the profit or loss.

A cleared non deliverable BTC/USD contract would, in our view, be a very mainstream looking entity. It would have similar execution and post trade to a host of other institutional contracts. You could also use short dated swaps as a cash substitute – this is, in our view, one of the roles which currency swaps currently fill.

### Clearing and hedging

The big issues, we think, are clearing and hedging. For a CCP to be prepared to clear a coin contract, it would have to believe it could both manage the risks associated with the open interest and unwind the contract if needs be. This is arguably the greatest challenge which the move to cryptocurrency derivatives faces, we think. Allied to this, although in theory a futures market can exist simply by matching natural buyers and sellers, in practice all but the most liquid contracts benefit from some kind of dealer support, and the dealers will want to be able to hedge back to the cash market. So, a

derivative market doesn't get rid of the need for an improved cash market infrastructure, but it does push the issue away somewhat.

### Reducing volatility

Derivatives markets might play some role in reducing the volatility of cash markets. We would not overstate this, as a material reduction in volatility would require there to be a large community of speculators prepared to provide liquidity to the natural owners of the various coins, but given the volatility of the coin markets, maybe there already exists a cadre of participants who would look to short coins on strong days and vice versa, which could overall reduce volatility.

## CBOE, LedgerX

Two entities have recently set out concrete plans to trade coin derivatives (with both looking to start with BTC/USD).

### CBOE

The CBOE is by far the more mainstream of the two. It is diversified US exchange, with a market cap of around $11bn. As well as the eponymous options markets, it also owns BATS, the global trading platform which is heavily represented in cash equities.

The CBOE has announced that it intends to list bitcoin derivatives, starting in Q4 17 or Q1 18. It intends to begin with USD/BTC, but will consider other contracts later. It is discussing registration with the CFTC. It will clear at the OCC, as all CBOE's derivative products do today. The OCC is a well established US derivatives clearer which, inter alia, clears US options.

### Partnership with Gemini, Winklevoss

CBOE is partnering with Gemini, a digital currency exchange, and the Winklevoss team (who founded Gemini, and have been pretty vocal bitcoin proponents). The CBOE will use Gemini's cash trading experience and data set. Gemini holds auctions twice daily; the CBOE will use their end of day New York auction for settlement. We don't want to over use the word "mainstream", but this, like the use of OCC, is a very mainstream solution.

Gemini is regulated as a New York trust company, which subjects it to a lot of the regulations that New York banks face. According to CBOE, Gemini did this to build credibility; according to CBOE, Gemini runs a thorough KYC process for every member, and complies fully with AML checks. This gave them comfort. Gemini's process is mostly just ledger transfer. They work with pre funded wallets and most trades on exchange settle that day by transferring funds from one account to another.

### Products

The CBOE contracts are designed as cash settled, but the Gemini auction provides a bridge between being cash and physically settled. This is designed to hold appeal to people looking for exposure to physical bitcoin as well as those who want to stay in the futures environment. They aim to list monthly expirations, with one contract on the March quarterly cycle.

### US listed ETF

CBOE is also working with the Winklevoss team to list a bitcoin ETF. In the US, it is the listing exchange's responsibility to advocate for the approval of innovative ETPs, and CBOE has been working with the SEC over the past year on the application. The ETF and futures contracts do not depend on each other, but clearly, they would be reinforcing.

### Who are the customers?

From a very high level perspective, there are three constituencies for futures.

- Retail customers who are currently trading FX. Physical bitcoin has uncertain security and is more cumbersome than trading traditional currencies. The CBOE product though sits alongside other retail traded products. The ability to short the contract could also be attractive.

- Institutional players, who again security concerns may deter from the cash market. It will, presumably, take time to build institutional liquidity, but at least the format is very well understood.

- Marketmakers, as a lot of such firms are already active in cash bitcoin (we think these tend to be smaller commodity trading businesses). A broader set of proprietary trading firms may find the volatility of bitcoin appealing but also like the plug and play aspect of a CBOE product.

Anecdotally, some existing participants have told CBOE they are already active in cash bitcoin.

**LedgerX**

At the other end of the spectrum, LedgerX is a venture funded exchange. Its largest investor, and a strategic partner, is Miami International Holdings, which owns the Miami International Securities Exchange, an existing US options market. The management team is headed by two ex Goldman Sachs employees, and it also has Mark Wetjen, an ex CFTC Commissioner, on its Board. LedgerX has received CFTC approval to open up a SEF to trade cryptocurrency derivatives and a clearinghouse.

**Products**

LedgerX is looking to offer standard options contracts. It will start with 1-6 month contracts. It has also decided to offer a day ahead swap, settling T+1. LedgerX sees this as an institutional product set; they think institutions at present cannot be involved in coins as they usually can't trade on unregulated exchanges. It also should also be attractive to miners who are naturally long bitcoin as well as trading companies, especially commodity trading shops. The company intends to start trading in September/October 2017.

Over time, LedgerX will consider ETPs, to be listed through Miami (which has cash equity capability).

**Clearing model**

Because of the volatility of bitcoin they have applied for a fully collateralised model. No margin will be allowed. At the start, all positions will be 100% collateralised; LedgerX will take cash from one side, bitcoin from the other. The products will be deliverable. Counterparties will receive bitcoin or cash, depending on which side of a trade they are on.

**IRAs**

We are aware of at least one service which offers some coins as part of a US IRA (Investment Retirement Account). Bitcoin, ether, XRP, Litecoin and Bitcoin Cash appear currently available.[51]

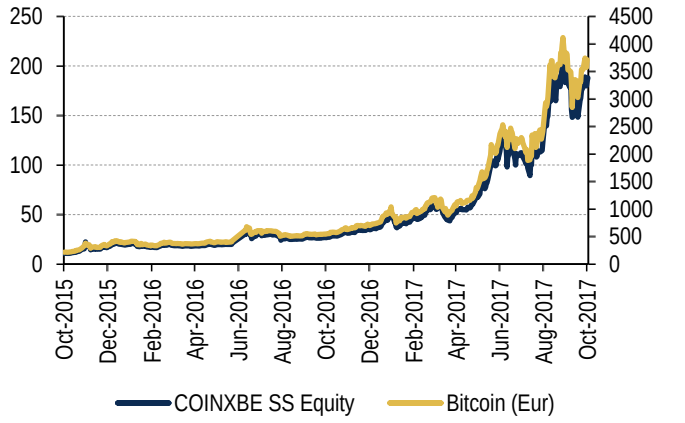
## Swedish ETP

Sweden has boasted a fully regulated ETP tracking Bitcoin for over two years, although it has generated far fewer column inches than its putative US peers. There are products denominated in SEK (COINXBT SS, market cap SEK 1.2bn) and Euros (COINXBE SS, market cap €95m). To underline the products' mainstream credentials, they are traded on Nasdaq Nordic market, cleared at Euroclear Sweden and regulated by the Swedish financial regulator, the Finansinspektionen. This looks extremely mainstream, reputable

[51] BitcoinIRA

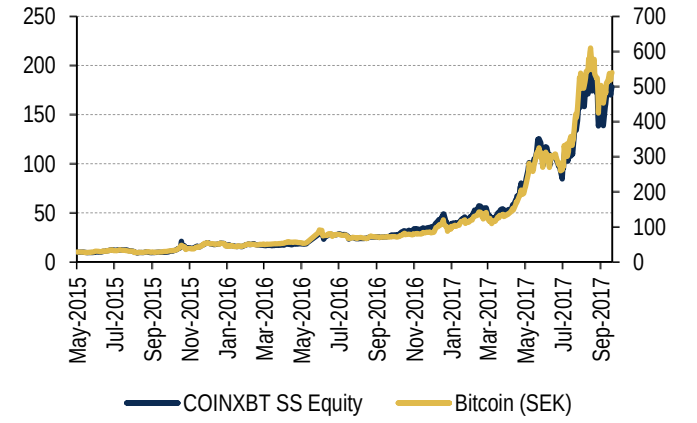
and normal. The fund takes pricing from a selection of bitcoin exchanges, and collateralises itself by holding bitcoin against its liabilities.

**Chart 14: Bitcoin Tracker Euro vs bitcoin**




Source: Bloomberg

**Chart 15: Bitcoin Tracker One vs bitcoin**




Source: Bloomberg

The ETPs seem to have tracked the underlying pretty closely. Given the product carries a 2.5% fee load, it's not surprising that overall, its price performance has somewhat lagged the underlying.

## Positive steps

Taken together, we see some highly positive steps for the adoption of some form of cryptocurrencies in the mainstream financial system. CBOE has the advantage in terms of familiarity, connectivity and brand names. If the long-running bitcoin ETF saga reaches a positive conclusion, this would sit well alongside the CBOE contracts, as a mainstream cash instrument to sit alongside a suite of mainstream derivatives. We also think the Gemini link-up is sensible, as it provides a relatively liquid cash market. Lastly, there could be arbitrage opportunities with the Swedish ETP, although liquidity here is pretty limited.

LedgerX's plans seem more imminent. However, it lacks the current market power of CBOE, and its product offering looks a little less mainstream than CBOE's.

### Market wants mainstream products?

Ultimately, the market will decide what it wants. Our view is that the market is likely to use mainstream products which fit into the existing regulatory and operational infrastructure. We think people often underestimate how important operational questions are in determining what does, and does not, get adopted by mainstream financial institutions. Neither the dealers nor their clients have infinite budgets for middle and back office technology, and they aim to spend the bulk of the budgets they have on fixing a range of legacy issues.

### Range of crosses to widen

We understand why both CBOE and LedgerX are starting with BTC/USD. However, we note that current bitcoin volumes are in multiple currencies, including ether; the dollar is often not the biggest cross in the various cryptocurrency exchanges. So, over time we think the market would benefit from a wider range of products. That said, we think these two regulated derivatives markets mark a fairly momentous step into the mainstream. This underlines, in our self-interested view, the importance of investors taking increasingly detailed views on the value of the various coins.

# Coins and financials

We have talked about how the coins could go mainstream. How could this impact existing financial companies?

This is clearly speculative. We have stressed that there is a wide cone of possible outcomes for the various coins we have covered, and by extension the whole universe. However, there are some directional impacts.

## Payments – no obvious impact

The argument which runs through this note is that certainly bitcoin is a poor medium for making payments, as it is expensive. We think that the mainstream payment processing infrastructure (Visa, MasterCard and so on) are much quicker and cheaper than bitcoin, and so we struggle to see a role for the coins in the developed world. Our blockchain primer, referenced above, argues this case in more detail. Potentially, coins could find more of an audience where the existing infrastructure is underdeveloped.

### Distributed ledger technology offers potential

As we have continually stressed, though, there is considerable potential for distributed ledger technology to form part of the future payments infrastructure. However, we think that such solutions are likely to be permissioned, and managed by a trusted provider. This is partly due to regulation. Typically, financial infrastructure is heavily regulated, and this provides a barrier to disruption. There is also a cost issue. Bitcoin is an expensive system, due to its reliance on mining. It is also extremely slow, for the same reason.

Other validation mechanisms may be cheaper and/or faster, but have yet to be fully tested in the real world, in our view.

### But likely to be permissioned

On the other hand, we can see either an existing infrastructure provider, or a consortium of existing companies, using a permissioned distributed ledger solution. SETL, which we have already mentioned, is one such potential system, but there are others. The advantages of this would be in terms of reduced cost, as well as increased ease of use. Distributed ledgers can be straightforward to link to a company's existing system, as there is no particular requirement to use a designated interface.

## Exchanges

There are potential positives and negatives for the exchanges.

### Positives – futures and cash trading

We have already described a few attempts to take coins into the mainstream. If these efforts to apply existing exchange technology to coins work, then this creates a new revenue pool for the exchange industry. The CBOE has taken a lead in this, although there is no guarantee that their offering is successful.

Given current cash volumes, our working assumption would be that coin derivative markets would be helpful but not transformational in terms of revenues. For example, Deutsche Börse (B-1-7, EUR91.97) earned €438m from index futures last year (its highest margin product range). This is a market where the equivalent cash asset turned over €46bn a day in 2016. Simply applying this ratio to bitcoin could suggest a top line of €20m, assuming a similar yield. This reflects the fact that bitcoin volumes since the beginning of August (when they have been extremely high compared to their history) were around $2.1bn a day.

Bear in mind that this scenario includes a range of crosses, including some with other coins as well as the fiat currencies. Over time, we think that if USD/BTC takes off, you could see a much broader range of crosses being traded. To be generous, you could then double the $20m, to reflect the fact that bitcoin is, give or take, about half the coin total market cap.

### Key sensitivities

To get above the $40m a year, you would have to assume one of three things, we think.

- **A material increase in coin market cap.** This is possible, but bear in mind that overall coin market cap has gone up 11x over the past year.
- **Significantly higher velocity of circulation.** However, annualizing the $2.1bn bitcoin ADV suggests $770bn a year. This is, give or take, ten times the market value of bitcoin. This is already a much higher velocity than seen in mainstream equity markets.
- **The rate per contract could be much higher.** However, index products are Eurex' highest margin, and benefit from IP protection over the STOXX and DAX contracts. There are higher margin contracts in the market (some CME contracts have a higher RPC, for instance). To be generous, were you to double the RPC, you would arrive at around $80m a year for all coins.

### Bull case scenario – 10% of FX volumes

As a bull case, you could assume that cryptocurrency volumes end up at around 10% of fiat volumes. The FX market is highly liquid. For example, spot FX volumes were $1.65tr as of the most recent BIT Triennial survey in April 2016. If these volumes were to materialise, with the same relationship between spot market and futures, and he same revenue per contract, the revenue pool would be about $1.6bn. Bear in mind, though, that were this to happen, we suspect volumes would be split between more than one exchange, and also that RPC would come under pressure. Finally, this also assumes that there is no substitution of coin volumes for other contracts. This may well be optimistic.

The CBOE seems to have established a first mover advantage. However, if the market develops, we would assume that other major derivative players like DB1's Eurex and the CME would try to become involved. There would also be at least the potential for LCH to offer clearing, as there may be cross margining benefits with the Group's current FX clearing. This is a long way away, though.

In the short term, the key data point to watch for will be the CBOE's futures listing, followed by the Winklevoss ETF. Successful outcomes here would be positive for the market infrastructure providers, we think.

### Negatives – potential competition for tech listings

On the other hand, ICOs are at least in part a competitor product to exchange listings (as well as potentially competing with venture funding). The listing markets aren't massive drivers of exchange volumes. For illustration, the LSE overall earned £91m from issuance overall. Again, to be generous, potentially a revenue pool of this magnitude may be available if ICOs simply displace exchange listings (bear in mind the LSE figure is for all listings, including more mature companies). (LSE, B-1-7, 3858p).

The potential revenue impact might in fact be somewhat greater than this, as listings in turn lead to future trading revenues. However, cash equities in total are not a major revenue source for the exchanges. For example, 15% of the LSE's revenues come from equities. We would not see anything like all of these revenues under threat. Bear in mind, amongst other things, that we have demonstrated in our note on distributed ledger technology and capital markets that blockchain type technology is structurally too slow for equities trading.

### Investment banks – potential impact on FX

The mainstream banking community is at present working with Ripple on cross border FX. The industry sees it as a potential cost saving product. If Ripple does achieve a significant market share, we think this is probably benign for the incumbents, as the XRP

is positioned to aid FX trading where there is limited liquidity. There is a potential risk that over time, XRP might disintermediate the mainstream system, but XRP at present relies on mainstream banks to provide an interface with the fiat currencies. This is a key aspect of all the existing coins – the interface with the fiat world is the area of greatest vulnerability, in our view.

This may in fact be an opportunity for mainstream banks. If they were to generate a natural business in XRP and other coins, they could also provide money exchange services between coins and other currencies. Again, though, this is dependent upon the coin environment maturing.

### Trading opportunities

Lastly, some banks have ruminated about the possibility of trading coins; Goldman Sachs is the most up front of these[52]. "As digital coins proliferate and draw interest from professional investors, though, they become harder for Wall Street trading desks to ignore ... Its [Goldman's] effort could eventually entail a team of traders and salespeople making markets in bitcoins much as they do Japanese yen or Apple Inc. shares", according to the WSJ.

If the exchanges develop futures products, over time these, too could attract dealer involvement and generate revenues.

### ICOs

If ICOs become more prevalent, we assume that they will begin to involve the advisory community, leading to some potential added revenues for the investment banks, as well as the legal, accounting and PR industries.

## Overall

We retain our existing ratings on the market infrastructure providers. We think it is important for investors in these stocks to keep informed about what is happening with the cryptocurrencies, as at some point these may impact the mainstream world, for good or ill. We hope this note forms part of this process. However, at present, these impacts are too far off, and too unpredictable, to form part of an estimate or an investment recommendation.

[52] "Goldman Sachs Explores a New World: Trading Bitcoin", Paul Vigna, Telis Demos and Liz Hoffman WSJ, 2.10.17

# The commodity perspective on cryptocurrencies

Our commodity team, headed by Francisco Blanch, francisco.blanch@baml.com, has recently produced an extremely useful note on cryptocurrencies, focusing largely on bitcoin. This section is heavily based on that note, with some updated statistics and modestly different emphasis.

**We would especially highlight from this analysis:**

- Bitcoin is a strongly diversifying asset, at least based on the historical record.
- Bitcoin correlates with a number of other coins, though it doesn't correlate with ether; you could view this as reflecting the differences in business model between the two.
- Bitcoin's volatility is high, and this is a challenge for a range of applications, but it seems to be falling and a range of fiat currencies can also display significant volatility.

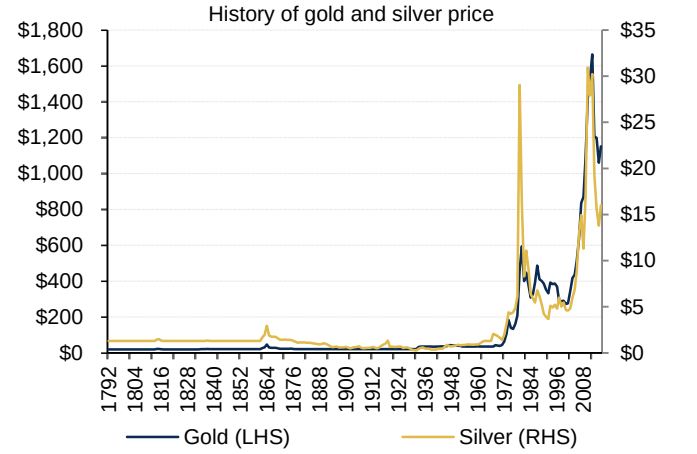
### From metal-backed to fiat to crypto, money keeps evolving

The world economy has used different types of currencies as a means of exchange for millennia. From commodity-backed to precious metal-backed to fiat to crypto, the meaning of currency has changed with varying economic needs, political trends, and technological change. For example, salt was once mined and treasured in the ancient world and used a means of exchange. However, commodity-backed currencies were often neither a practical nor a durable means of exchange. So the global economy moved on. Governments coined currency to create standard economic units of account using either precious metals like gold or industrial metals like copper, a practice that continues to this date.

### Huge deposit discoveries preceded the advent of silver currency

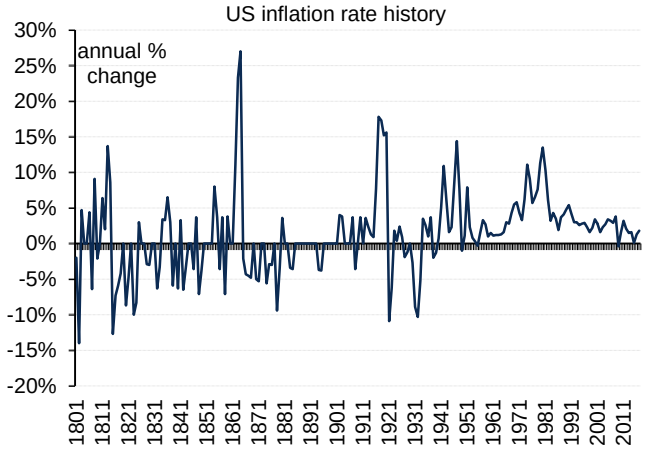
The discovery of large silver deposits in Bolivia by the Spanish in the 16th century set the basis for the world's monetary system until late in the 19th century (Chart 16). These silver dollars were the international trading currency of choice for nearly 400 years and kept a stable value relative to gold. The Spanish milled dollar was even used as a standard to set up the US dollar by the Federal Government. However, carrying large amounts of silver or gold was not practical. So the world started to move steadily to paper money, particularly in the last 200 years. At first, most governments maintained an asset or precious metal-backed currency system where paper currency could be exchanged for hard metal at a fixed rate. However, the supply of this money was fixed, creating huge inflationary and deflationary waves in the economy as the business cycle fluctuated every few years (see US example in Chart 17).

**Chart 16: Silver dollars were the international trading currency of choice for nearly 400 years and kept a stable value relative to gold**




Source: Kitco, Bloomberg

**Chart 17: However, the supply of this money was fixed, creating huge inflationary and deflationary waves every few years**

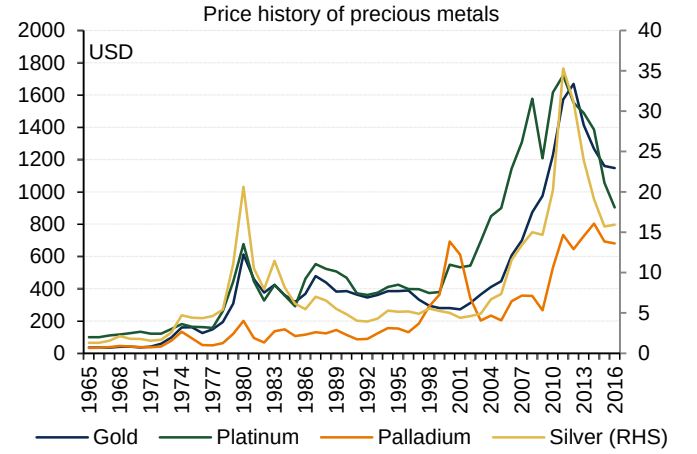



Source: Minneapolis Fed

## Macro financial stability considerations propelled fiat currencies

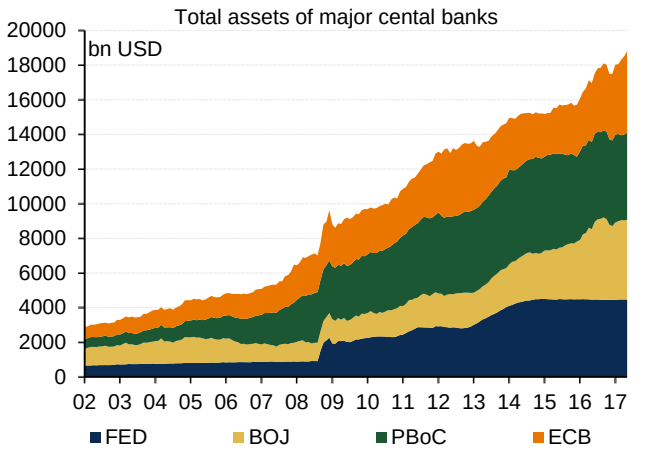
Following the Great Depression in 1933, the US government moved away from the gold standard domestically and left the economy running solely on silver, in effect a quantitative easing of sorts. Still, international payments were settled in gold. The domestic silver standard was eventually constrained by Kennedy in 1963, as inflation caught up with dollar silver certificates issued by the Treasury. Then Nixon announced in 1971 that the US government would no longer redeem US dollar currency for gold in international markets. A major spike in precious metals prices followed (Chart 18)As of today, most countries have moved to locally minted fiat currencies that have no intrinsic international value other than the full faith of the issuing government. In effect, central banks safeguard the value of the fiat currency mainly by complying with their inflation mandate. However, central banks have the ability to create fiat currency at will as long as the pre-established inflation target has not been met (Chart 19).

**Chart 18: The end of dollar/gold convertibility in 1971 led to a major spike in precious metals prices**




Source: Bloomberg, BofA Merrill Lynch Global Research

**Chart 19: Central banks safeguard the value of a fiat currency by mainly complying with their inflation mandate, but can create currency at will**




Source: FRED - St. Louis Fed, Bloomberg

## Technological advancements have enabled cryptocurrencies

Decentralized digital cryptocurrencies first came about at the depth of the Global Financial Crisis in 2009 when a group of developers created Bitcoin. The idea of a virtual means of exchange that is controlled by an algorithm and escapes government control certainly has appeal to many. What turns a digital token into a proper store of value? We would argue that a reserve currency has to meet three "must have" criteria: safety, liquidity, and return. Also, there are "nice to have" criteria such as diversification

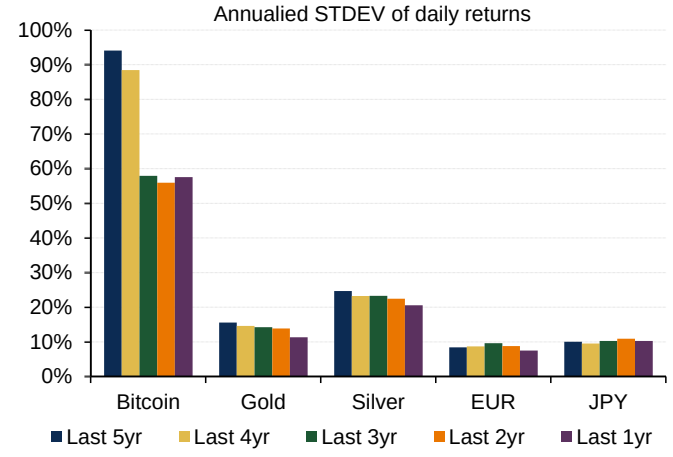
benefits. Bitcoin and other cryptocurrencies score well on some, and not so well on others.

### Bitcoin does not score well on the safety parameter

On the first parameter, safety, it is hard to argue that a crypto token meets the criteria of a reserve currency. On the one hand, the system creates enough incentives for miners to guarantee settlement of bitcoin transactions within hours, compared to 2 or 3 days for conventional securities such as equities or bonds. On the other, the lack of a centralized decision-making process or authority creates risks such as a currency split, such as the recent fork (see "Forking hell" above).

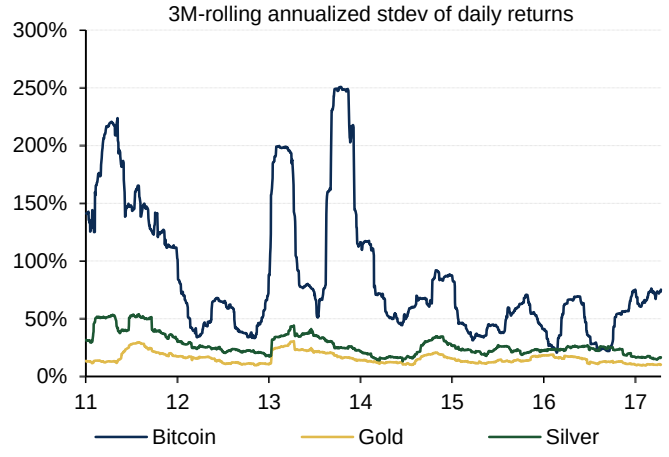
Also, risks such as hacking, identity theft, or outright scams are a recurring problem (for instance, see "Your top three cryptocurrency fiascos" above). But you could also argue that fiat currency holdings are exposed to these issues. Most importantly, volatility is the key parameter to understand the concept of safety in a reserve currency, in our view. In that regard, bitcoin's score has improved in recent years as volatility has continued to drop (Chart 20). Still, bitcoin's volatility is very high compared to the euro, the yen or even gold. But it fell twice last year below the volatility of silver (Chart 21), the world's currency for 400 years.

**Chart 20: Volatility is a key parameter for safety in a reserve currency and bitcoin vols have been falling for a while**




Source: Bloomberg, BofA Merrill Lynch Global Research

**Chart 21: True, bitcoin's volatility is very high compared to the euro, the yen or even gold, but it is starting to approach silver**




Source: Bloomberg, BofA Merrill Lynch Global Research

### Don't forget the risks

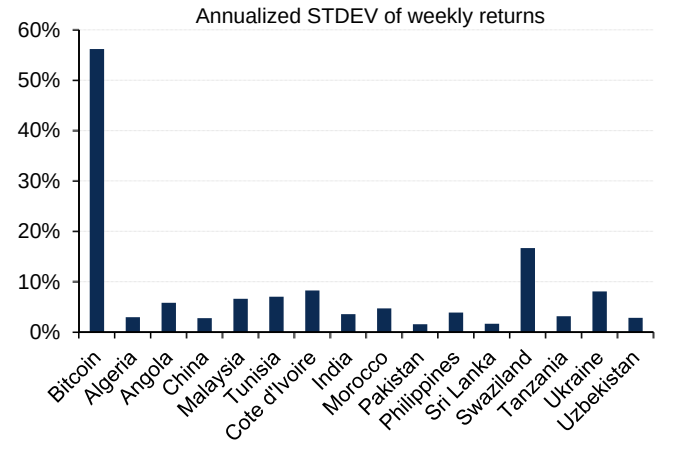
When examining the safety of any asset, volatility is not the only source of concern. In the case of bitcoin and other virtual tokens, worries are magnified given that its regulatory status is still moot in many domiciles. We have already discussed the issues relating to the interface between coins and the "real world", and of ICOs. Lastly, it is worth noting that cryptocurrency transactions are taxable in many jurisdictions, presenting additional challenges to users that are unfamiliar with the fiscal implications of using bitcoin (although you could say the same of other instruments).

### Yet, EM currency pegs and capital controls encourage bitcoin use

True, bitcoin is still volatile compared to even Emerging Market currencies. But it is also worth noting that EM FX volatility tends to be artificially suppressed by controls. When looking at 16 countries with severe capital controls based on IMF indicators (Algeria, Angola, China, Malaysia, Tunisia, Cote d'Ivoire, India, Morocco, Pakistan, Philippines, Sri Lanka, Swaziland, Tanzania, Togo, Ukraine, and Uzbekistan), we find that bitcoin is more volatile than these currencies (Chart 22). However, it is not uncommon for these EM currencies to suffer from high inflation rates (Chart 23). When pegged or semi-pegged FX regimes face high inflation or sharp FX reserve drawdowns, steep exchange rate adjustments eventually follow. So the more official and black market exchange rates diverge, the more attractive bitcoin may appear to some as a means of payment and

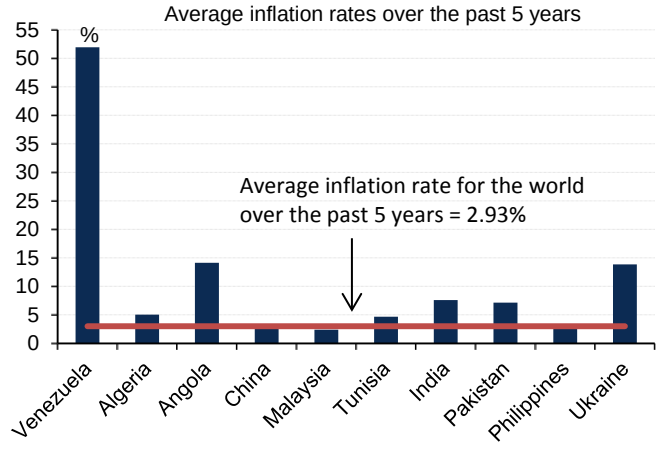
store of value. And the more liquidity and scale bitcoin builds to, the lower the volatility over time, in our view.

**Chart 22: We find that bitcoin is more volatile than the currencies with severe capital controls**




Source: Bloomberg, BofA Merrill Lynch Global Research

**Chart 23: However, it is not uncommon for these EM currencies to suffer from high inflation rates**

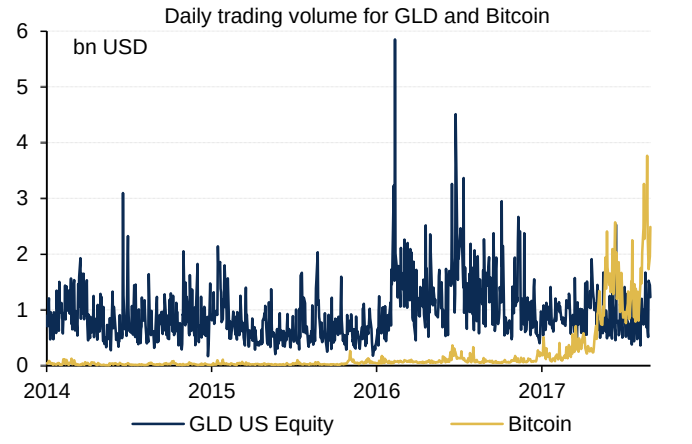



Source: FRED - St. Louis Fed, Bloomberg, BofA Merrill Lynch Global Research

## Liquidity, however, keeps increasing at a very fast rate

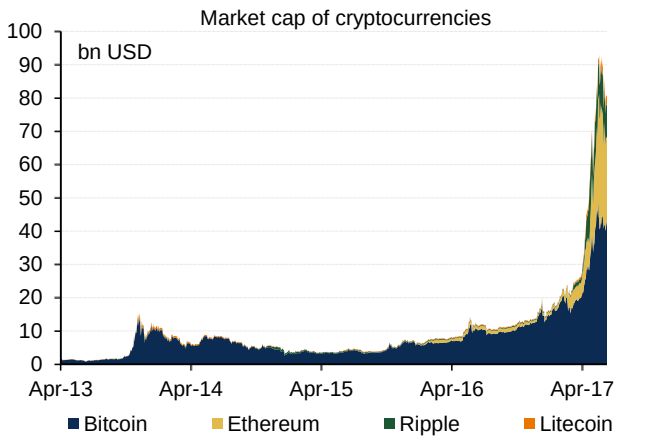
Moving on to our second parameter, liquidity, it is hard to ignore that trading volumes for major digital currencies like bitcoin and Ethereum have skyrocketed in recent years. For example, daily trading volumes for bitcoin were $40mn in 2014 and have now moved up to about $1bn a day at present (Chart 24). Meanwhile, Ethereum had daily trading volumes of $1.5mn when it first launched in 2015 and it is now experiencing daily trading of about $1bn. Most importantly, for a digital token to become a currency, it must build to a certain scale. In some ways, this is exactly what has been happening in recent quarters, with the total market value of digital tokens growing exponentially from $1.5bn to around $87bn at present (Chart 25). Put differently, cryptocurrencies have built scale rapidly and are now accepted as a means of payment by some corporations and individuals.

**Chart 24: Daily trading volumes for bitcoin were $0.04bn in Jan. 2014 and have now moved up to about $1bn a day at present**




Source: coinmarketcap.com

**Chart 25: The total market value of bitcoin exploding growing exponentially from $1.5bn to around $43bn at present**



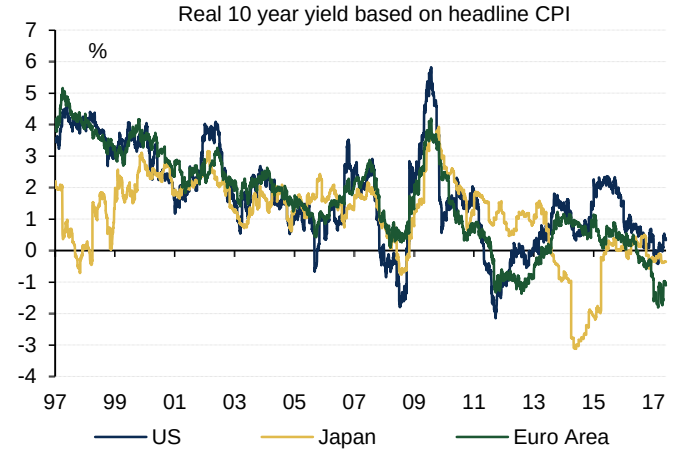

Source: coinmarketcap.com

## Returns of cryptocurrencies depend mostly on price appreciation...

On our third parameter, there are several ways to look at the return produced by a reserve currency. Because a government issues both debt and currency simultaneously, perhaps the most important measure of value for a reserve currency is the real interest rate (Chart 26). Then there is the term premium, as fixed income markets typically make

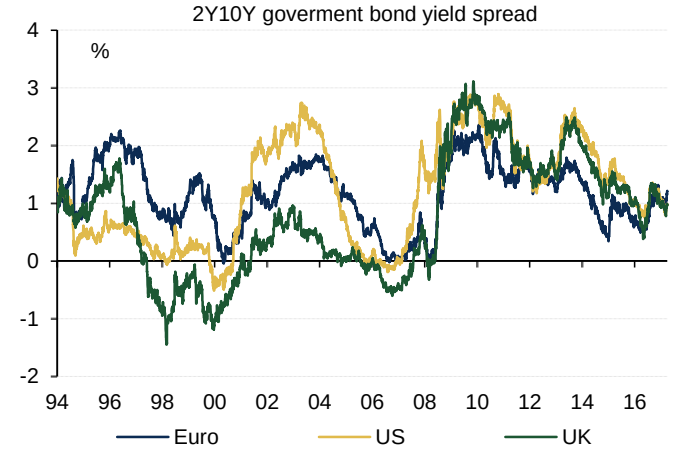
it more expensive to borrow for longer periods of time. In fact, despite quantitative easing, most major currencies like the EUR, the USD, or the GBP maintain a positive spread between their 2 year and their 10 year interest rate (Chart 27Yet, there are some widely accepted reserve assets like gold or even the JPY that do not pay a yield.

**Chart 26: The most important measure of value for a reserve currency is the real interest rate**




Source: Bloomberg

**Chart 27: The term premium means that currencies maintain a positive spread between their 2 year and their 10 year interest**




Source: Bloomberg

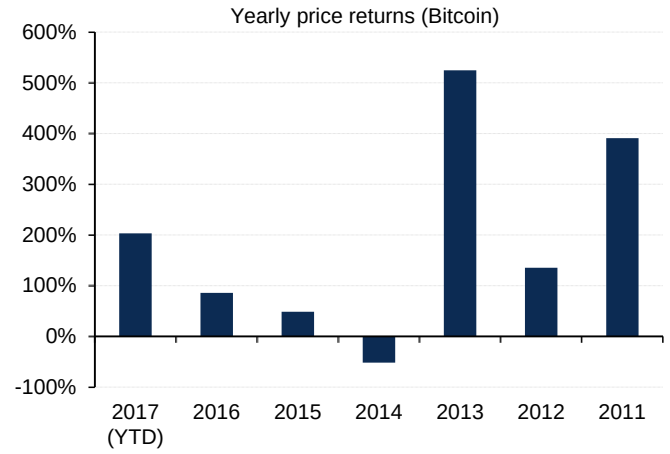
### ...although some exchanges offer a return for borrowing tokens

Bitcoin and other digital currencies do not have an interest rate set by a central bank. And it is hard to calculate a real interest rate, as there is no specific national inflation metric to match it against. However, just like in gold, there is still an interest rate set by the market. After all, bitcoin exchanges need digital currency for short lending purposes. Some of the most popular services offer 1% for 14 days and scales to 5% for 1 year. Even then, returns paid by exchanges are arguably more of a credit spread than a real interest rate. Moreover, with volatility in excess of 50% or higher, a 5% return on a cryptocurrency over the course of 1 year as compensation for lending a bitcoin to an online exchange does not seem like a particularly attractive proposition.

### A key step for bitcoin would be to become pledgeable collateral

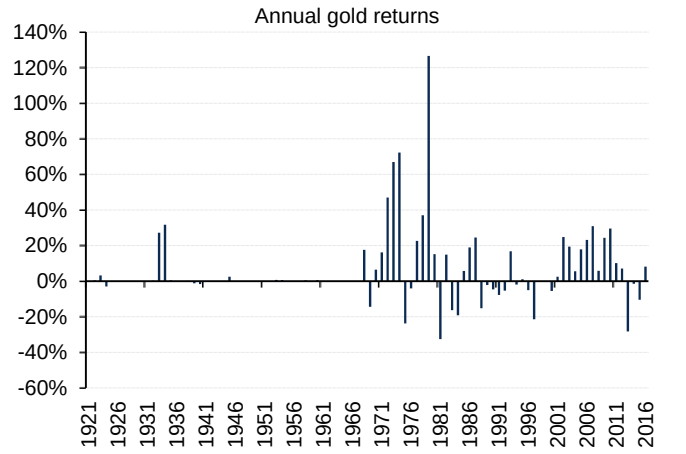
Still, bitcoin and Ethereum have delivered impressive returns so far (Chart 28) as fiat currency flowed into these digital tokens. Is it realistic to assume cryptocurrencies will continue to appreciate over time? The dollar price of gold has appreciated over centuries in line with inflation (Chart 29), but some periods have experienced much faster gold price appreciation than others. Moreover, periods of high real interest rates have been particularly damaging for gold returns in the past. In our view, cryptocurrency returns will mostly depend on the faith placed by individuals, corporations, and financial institutions on this emerging technology. As discussed earlier, there are large inherent risks to digital. Moreover, a crucial hurdle remains. Most regulated financial institutions allow their clients to borrow against financial or physical assets, but we are not aware of any major institution that takes cryptocurrency as collateral at the moment. Thus, in our view, a key step for bitcoin would be for it to become pledgeable collateral.

**Chart 28: So far, bitcoin has delivered exceptional returns as fiat currency flowed into these digital tokens**




Source: Bloomberg
Note: Data available from July 2010 to current. There were almost non price fluctuations before 2011.

**Chart 29: The dollar price of gold has appreciated over centuries in line with inflation, but returns have fluctuated over the cycle**




Source: Bloomberg

### Bitcoin correlations to EM and G10 fiat currencies are near zero…

Lastly, a financial instrument tends to be more attractive if it offers diversification benefits. In that regard, bitcoin and other cryptocurrencies score well. For starters, we find near zero correlation in weekly returns between bitcoin and fiat currencies (Table 2). Remarkably, while some currency like DXY and CHF exhibit a correlation of 0.67, bitcoin returns are uncorrelated to any other major EM or G10 currency in our analysis.

**Table 2: EM and G10 currencies - weekly returns correlation**

| | Bitcoin | DXY | EUR | JPY | GBP | MXN | CNY | KRW | CAD | CHF |
|---|---|---|---|---|---|---|---|---|---|---|
| Bitcoin | | -0.04 | 0.04 | -0.01 | 0.05 | -0.06 | -0.04 | 0.02 | 0.01 | -0.01 |
| DXY | | | -0.96 | 0.45 | -0.69 | 0.33 | 0.25 | 0.35 | 0.53 | 0.67 |
| EUR | | | | -0.30 | 0.59 | -0.28 | -0.20 | -0.25 | -0.42 | -0.62 |
| JPY | | | | | -0.19 | 0.02 | 0.17 | 0.11 | 0.14 | 0.32 |
| GBP | | | | | | -0.26 | -0.22 | -0.34 | -0.44 | -0.43 |
| MXN | | | | | | | 0.19 | 0.43 | 0.55 | 0.19 |
| CNY | | | | | | | | 0.25 | 0.26 | 0.14 |
| KRW | | | | | | | | | 0.49 | 0.26 |
| CAD | | | | | | | | | | 0.26 |
| CHF | | | | | | | | | | |

Source: Bloomberg, BofA Merrill Lynch Global Research
Note: Data available from July 2010 to current. There were almost no price fluctuations before 2011.

### …and bitcoin is also uncorrelated to volatile, inflation prone EM FX

Arguably, bitcoin is not particularly attractive as a means of exchange in a very large and stable economy like the US that boasts the world's pre-eminent trading currency. But what about emerging markets? After all, bitcoin does not face the same capital controls and banking rules as do some currencies in highly constrained economies. It could potentially deliver low cost, fast, cross border transactions. We look again at the correlations between EM FX and bitcoin and we find that bitcoin lacks correlation to a whole range of EM currencies (Table 3).

**Table 3: Inflation prone EM FX - weekly returns correlation**

| | Bitcoin | DZD | AOA | CNY | MYR | TND | XOF | INR | MAD | PKR | PHP | LKR | SZL | TZS | UAH | UZS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bitcoin | | -0.07 | -0.03 | -0.03 | -0.08 | 0.02 | -0.02 | -0.01 | -0.02 | 0.03 | -0.01 | -0.06 | 0.02 | -0.01 | -0.06 | -0.07 |
| DZD | | | 0.03 | 0.32 | 0.31 | 0.40 | 0.49 | 0.17 | 0.54 | 0.06 | 0.13 | 0.05 | 0.27 | 0.01 | 0.05 | -0.15 |
| AOA | | | | 0.25 | 0.12 | 0.00 | 0.01 | 0.02 | -0.01 | -0.03 | -0.01 | 0.00 | 0.13 | 0.16 | 0.01 | -0.07 |
| CNY | | | | | 0.30 | 0.16 | 0.16 | 0.15 | 0.17 | -0.01 | 0.20 | 0.09 | 0.26 | 0.03 | 0.07 | 0.01 |
| MYR | | | | | | 0.15 | 0.23 | 0.43 | 0.26 | 0.02 | 0.56 | 0.14 | 0.45 | 0.03 | -0.10 | -0.07 |
| TND | | | | | | | 0.77 | 0.17 | 0.79 | 0.06 | 0.10 | 0.05 | 0.31 | 0.03 | -0.03 | -0.08 |
| XOF | | | | | | | | 0.22 | 0.95 | 0.10 | 0.16 | 0.04 | 0.34 | 0.03 | -0.03 | -0.09 |
| INR | | | | | | | | | 0.24 | 0.07 | 0.45 | 0.20 | 0.39 | 0.00 | -0.01 | -0.14 |
| MAD | | | | | | | | | | 0.08 | 0.17 | 0.05 | 0.37 | 0.04 | -0.04 | -0.07 |
| PKR | | | | | | | | | | | 0.07 | 0.09 | 0.01 | -0.05 | -0.09 | -0.06 |
| PHP | | | | | | | | | | | | 0.15 | 0.31 | 0.03 | 0.01 | 0.03 |
| LKR | | | | | | | | | | | | | 0.05 | 0.01 | 0.04 | 0.03 |
| SZL | | | | | | | | | | | | | | 0.01 | -0.04 | -0.05 |
| TZS | | | | | | | | | | | | | | | 0.19 | -0.06 |
| UAH | | | | | | | | | | | | | | | | -0.01 |
| UZS | | | | | | | | | | | | | | | | |

Source: Bloomberg, BofA Merrill Lynch Global Research
Note: Data available from July 2010 to current. There were almost no price fluctuations before 2011.

### Bitcoin correlations to gold, oil, or copper are also about zero

The same applies to commodities. While gold and silver maintained a correlation on weekly returns of around 80% since 2011, we do not observe any meaningful correlation between bitcoin and precious, industrial or energy commodities (Table 4

**Table 4: Commodities - weekly returns correlation**

| | Bitcoin | Gold | Silver | Platinum | Palladium | BCOM | Brent | Copper |
|---|---|---|---|---|---|---|---|---|
| Bitcoin | | 0.05 | 0.04 | 0.07 | 0.06 | 0.06 | 0.05 | 0.02 |
| Gold | | | 0.80 | 0.70 | 0.35 | 0.40 | 0.14 | 0.26 |
| Silver | | | | 0.68 | 0.46 | 0.56 | 0.27 | 0.44 |
| Platinum | | | | | 0.60 | 0.50 | 0.28 | 0.43 |
| Palladium | | | | | | 0.44 | 0.27 | 0.48 |
| BCOM | | | | | | | 0.74 | 0.57 |
| Brent | | | | | | | | 0.34 |
| Copper | | | | | | | | |

Source: Bloomberg, BofA Merrill Lynch Global Research
Note: Data available from July 2010 to current. There were almost no price fluctuations before 2011.

### When looking at equities, we also observe minimal correlations

Equity markets, partly because of their interconnectedness, tend to move together with average correlations nearing or exceeding 50%. Once more, bitcoin exhibits near zero correlation with all major equity markets around the world (Table 5).

**Table 5: Equities - weekly returns correlation**

| | Bitcoin | S&P 500 | MSCI World | HSCEI | HSI | NIFTY | EURO STOXX 50 | Nikkei |
|---|---|---|---|---|---|---|---|---|
| Bitcoin | | 0.04 | 0.05 | 0.02 | 0.02 | -0.04 | 0.04 | 0.08 |
| S&P 500 | | | 0.96 | 0.50 | 0.54 | 0.51 | 0.78 | 0.53 |
| MSCI World | | | | 0.58 | 0.65 | 0.57 | 0.85 | 0.61 |
| HSCEI | | | | | 0.93 | 0.60 | 0.49 | 0.50 |
| HSI | | | | | | 0.64 | 0.55 | 0.56 |
| NIFTY | | | | | | | 0.53 | 0.49 |
| EURO STOXX 50 | | | | | | | | 0.58 |
| Nikkei | | | | | | | | |

Source: Bloomberg, BofA Merrill Lynch Global Research
Note: Data available from July 2010 to current. There were almost no price fluctuations before 2011.

### Bitcoin is also uncorrelated to Treasury securities or the VIX

Lastly, we test the correlation of bitcoin to other liquid markets such as Treasuries and the VIX and our own BofA Merrill Lynch GFSI™. Once more, the correlation between bitcoin and both near-term and long-term Treasury bonds and breakevens is near zero

(Table 6). Interestingly, the correlation of bitcoin to the VIX and to other risk indicators such as the BofAML GFSI is also very low, near zero, but negative (Table 7).

**Table 6: Correlation between weekly returns of Bitcoin and weekly changes in rates**

| | Bitcoin | 2YR UST | 10YR UST | 2YR BE | 10YR BE |
|---|---|---|---|---|---|
| Bitcoin | | 0.02 | 0.03 | 0.05 | 0.03 |
| 2YR UST | | | 0.74 | -0.06 | -0.04 |
| 10YR UST | | | | 0.17 | -0.01 |
| 2YR BE | | | | | 0.62 |
| 10YR BE | | | | | |

Source: Bloomberg, BofA Merrill Lynch Global Research
Note: Data available from July 2010 to current. There were almost no price fluctuations before 2011.

**Table 7: Correlation between weekly returns of Bitcoin and weekly changes in BofAML VIX and GFSI**

| | Bitcoin | VIX | BofAML GFSI - Risk | BofAML GFSI - Flow | BofAML GFSI – Skew |
|---|---|---|---|---|---|
| Bitcoin | | -0.05 | -0.08 | -0.06 | -0.05 |
| VIX | | | 0.55 | 0.44 | 0.65 |
| BofAML GFSI - Risk | | | | 0.46 | 0.59 |
| BofAML GFSI - Flow | | | | | 0.45 |
| BofAML GFSI - Skew | | | | | |

Source: Bloomberg, BofA Merrill Lynch Global Research
Note: Data available from July 2010 to current. There were almost no price fluctuations before 2011.

### However, bitcoin returns are correlated to other cryptocurrencies

To complete our correlation analysis, we have also looked at the correlation patterns of the 10 major cryptocurrencies by market value. Our work suggests that bitcoin and other digital currencies are correlated for the most part (Table 8), although nowhere nearly as correlated as equity markets are to each other. Moreover, bitcoin and Ethereum, the two biggest coins, seem uncorrelated to each other.

**Table 8: Cryptocurrencies - weekly returns correlation**

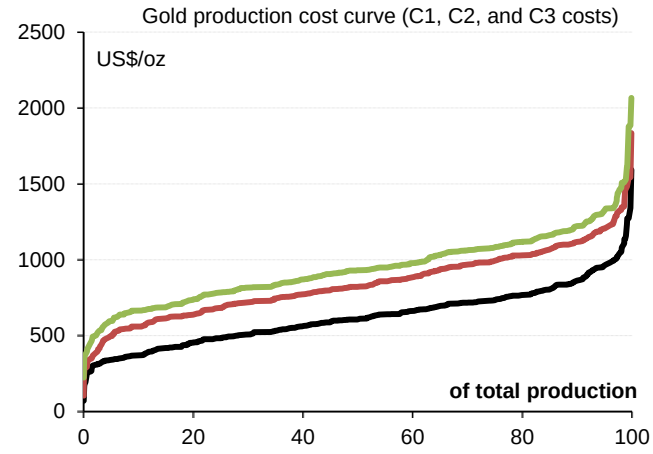
| | Bitcoin | Ethereum | Ripple | Litecoin | Ethereum Classic | Dash | NEM | Monero | Bitshares | Stratis |
|---|---|---|---|---|---|---|---|---|---|---|
| Bitcoin | | 0.01 | 0.21 | 0.56 | 0.14 | 0.19 | 0.27 | 0.23 | 0.31 | 0.34 |
| Ethereum | | | 0.04 | 0.06 | 0.44 | 0.34 | 0.29 | 0.18 | 0.35 | 0.29 |
| Ripple | | | | 0.60 | 0.08 | -0.12 | 0.22 | 0.02 | 0.35 | 0.19 |
| Litecoin | | | | | 0.07 | 0.09 | 0.22 | 0.15 | 0.40 | 0.21 |
| Ethereum Classic | | | | | | 0.18 | 0.24 | -0.07 | 0.17 | 0.18 |
| Dash | | | | | | | 0.27 | 0.20 | 0.22 | 0.13 |
| NEM | | | | | | | | 0.19 | 0.33 | 0.25 |
| Monero | | | | | | | | | 0.19 | 0.02 |
| Bitshares | | | | | | | | | | 0.24 |
| Stratis | | | | | | | | | | |

Source: Bloomberg, BofA Merrill Lynch Global Research
Note: Data available from July 2010 to current. There were almost no price fluctuations before 2011.

### Rising production costs have supported bitcoin prices for now

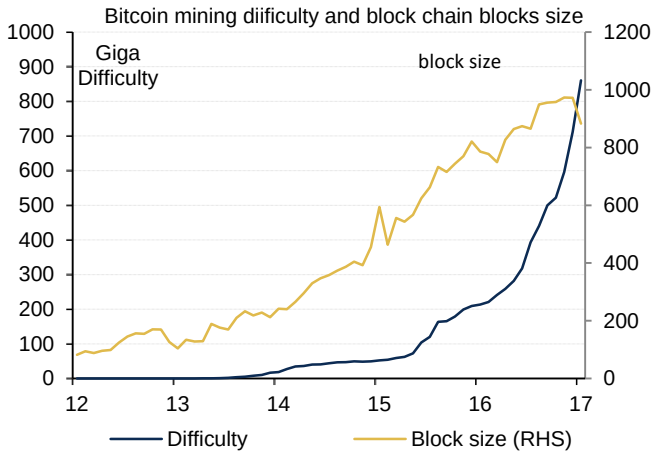
One final consideration in bitcoin and other digital currencies is their cost of production. Unlike gold, which is mined at a high cost (Chart 30), the marginal cost of creating a new digital token is near zero. This is the reason why the number of cryptocurrencies has risen to over 1,000 in recent years. However, the marginal cost of "mining" established cryptocurrencies like bitcoin has increased exponentially (Chart 31) while the rewards for mining are designed to experience a logarithmic decline. The operational and electricity costs required to maintain ledgers have increased as tasks have become more complex. This could change with the advent of quantum computers or through agreements among developers to adopt simpler protocols. Thus, while rising marginal costs of production for bitcoin have been arguably a source of support for prices, falling mining costs for incremental units could also force prices to fall.

**Chart 30: Gold is mined at a high cost, with most companies facing breakevens around $600/oz on average and $1200+/oz on the margin**




Source: Bloomberg, BofA Merrill Lynch Global Research

**Chart 31: The marginal cost of "mining" established cryptocurrencies like bitcoin has increased exponentially**




Source: data.bitcoinity.org
Note: The difficulty is a unit of measurement designed to indicate how difficult it is to find a hash below the given target

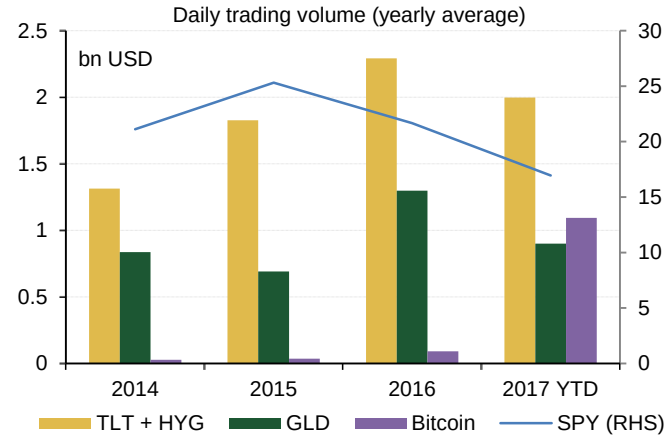
## Bitcoin faces many hurdles and risks, but liquidity keeps growing

So is bitcoin a new liquid market? Certainly, cryptocurrencies score well in terms of liquidity when compared to other assets. But liquidity in equity, fixed income, or currency markets remains a large multiple of bitcoin (Chart 32). Also, while cryptocurrencies are still very volatile and thus not particularly safe, that could change as both their value rises and liquidity increases. We think moves to integrate coins into more mainstream financial systems, such as the various exchange traded derivatives we have discussed already, or an ETF listing, arguably could help to manage volatility.

### Strong diversification benefits

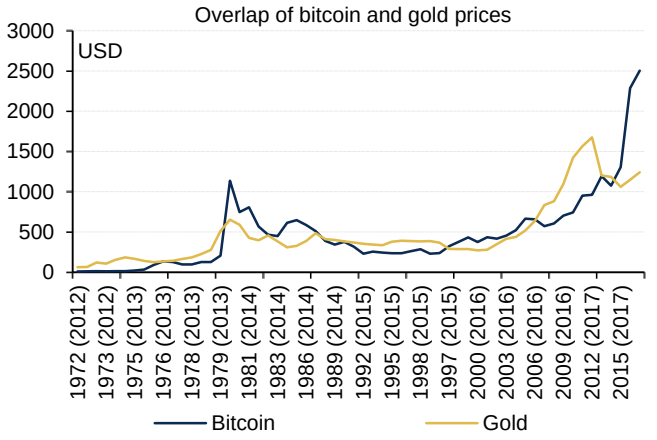
Importantly, cryptocurrencies score well when it comes to diversification, as their correlation to equities, bonds, commodities, FX or selected measures of risk is near zero. A big uncertainty facing bitcoin and other digital tokens we see is their expected real rate of return. So far, early adopters have enjoyed a sharp appreciation in prices. While bitcoin seems to have followed a pattern similar to gold over a much more compressed time period (Chart 33), there is no certainty that that will continue and, most certainly, no way to predict it. Also, there are large inherent risks to digital tokens.

**Chart 32: Liquidity in equity, fixed income, or currency markets is still a huge multiple of bitcoin**




Source: Bloomberg

**Chart 33: It is still early days, but bitcoin seems to have followed a pattern similar to gold over a much more compressed time period**




Source: Bloomberg
Note: Years in parentheses correspond to Bitcoin

# What are they good for?

Ultimately, although some Tinker Bell assets do exist, we think the only secure basis for a financial asset is some kind of fundamental value. In the case of the US Dollar, this reflects the support of the US Government, its economy's productive power, future expected interest and inflation rates and so on. Commodity prices are sensitive to expected supply and demand, as well as the overall financial climate (interest rates, exchange rates and so on). An early stage equity tends to rely upon a vision of future earnings power. A more mature stock is more a matter of how the future cash and dividend flows are likely to behave. We could go on. The underlying point, though, is that if you can't find at least an argument for why a particular coin generates economic value, it is hard to view it as anything other than a trading asset.

## Bitcoin – first mover, ageing

From this perspective, although we understand why bitcoin has tended to hog the headlines, it faces challenges. It is an expensive way of paying for things, and its blockchain doesn't offer any functionality beyond this. We think that unless it can form part of a global payment system, which would entail doing something about speed, scalability and cost, it may struggle to justify its valuation. We would add the whole bitcoin family – Bitcoin Cash, Litecoin etc – to this category.

### Unlikely to disrupt payment infrastructure

We do not see the Bitcoin family disrupting the existing payment processors. The technology strikes us as too expensive, absent dramatic new functionality, and in addition the tax status is problematic in at least the USA. We expect mainstream finance to continue to explore the use of permissioned distributed ledger applications in payments, but this is a very different kettle of fish to bitcoin.

## Ethereum, Ripple – clear use cases

Ethereum and Ripple are somewhat easier to get to grips with. It is moot whether its role in supporting ICOs and smart contract execution makes ether worth its current value, but it is straightforward to set out a scenario where it is fair value, or better.

Similarly, it is an open question whether the global FX market will want to use XRP as an important part of its ecosystem, and indeed whether Ripple's enterprise software wins out in institutional FX transfer, but it is not outlandish to expect that it does. Ripple has the potential to disrupt some incumbent infrastructure providers, but its positioning as an enterprise software provider partnering with existing banks underlines that, in our view, its ambition is not to disrupt the banks themselves but to make them more efficient.

## Moving mainstream

So, the investment case for the various coins exists, even if it strikes us as stronger in some cases than others (as is typical of an investment market). At present, we think a lot of the coins are somewhat like early stage technology companies. There is significant uncertainty about their future economics, but you can at least see the outlines of a discussion.

Importantly, there are signs that the infrastructure surrounding the cryptocurrency world is also improving. We think that if LiquidX and CBOE manage to list bitcoin derivatives the environment could become much more mainstream. In turn, we think this could lead to the exchange world being strengthened. We also would see a US ETF listing as potentially positive to the environment for coins, as it would provide vanilla cash equity investors with a potentially straightforward way of buying and selling coins.

### Potential revenues for exchanges, dealers

If coins do become more mainstream, this suggests that they will become more involved with the existing financial infrastructure. In turn, this implies added revenues for both

the market infrastructure players and the dealers. So far, the most positive commentary from the mainstream industry has come from CBOE and Goldman Sachs.

**Diversification, no yield…**

As investments, statistically coins currently could look very attractive for the diversification they offer. Bitcoin basically only seems to correlate with other coins of its family – it doesn't even correlate well with ether. It has no correlation, overall, with other mainstream asset classes. To a quant, therefore, adding bitcoin (or ether) to a portfolio could improve its risk/reward characteristics.

We understand why this is the case – there is no obvious reason why bitcoin should at present correlate with, say, the S&P 500. The S&P 500 trades on the basis of macro newsflow, earnings surprises and so on; bitcoin does not.

However, if our overall view – that the coins need to be viewed fundamentally – is right, then over time, we could see the various coins behaving a bit like technology shares.

We don't see any way around the lack of yield in the coins. But then again, last time we looked, Tesla didn't yield anything, either, and yet this has a market cap in the same ballpark as bitcoin. Technology companies aren't necessarily where you naturally go for yield.

## Highly volatile, all or nothing, but . . .

There is, we think, no escape from the fact that coins are likely to be highly volatile over the next few years. There is still no accepted consensus for how they are to be valued.

Equally, we think the emergence of some differentiated coins, each embedded within an ecosystem where you can see how value and demand can be created, might point to some coins prospering. The recent moves towards more institutional trading platforms also suggest that coins may well become more normal assets.

Coins face a range of business and regulatory challenges, but they are also a source of creativity and disruptive business models. We think that the case for investors understanding the coins, and so being able to judge their implications for the existing financial world, is becoming ever clearer.

# Disclosures

## Important Disclosures

**FUNDAMENTAL EQUITY OPINION KEY: Opinions include a Volatility Risk Rating, an Investment Rating and an Income Rating. *VOLATILITY RISK RATINGS*, indicators of potential price fluctuation, are: A - Low, B - Medium and C - High. *INVESTMENT RATINGS* reflect the analyst's assessment of a stock's: (i) absolute total return potential and (ii) attractiveness for investment relative to other stocks within its *Coverage Cluster* (defined below). There are three investment ratings: 1 - Buy stocks are expected to have a total return of at least 10% and are the most attractive stocks in the coverage cluster; 2 - Neutral stocks are expected to remain flat or increase in value and are less attractive than Buy rated stocks and 3 - Underperform stocks are the least attractive stocks in a coverage cluster. Analysts assign investment ratings considering, among other things, the 0-12 month total return expectation for a stock and the firm's guidelines for ratings dispersions (shown in the table below). The current price objective for a stock should be referenced to better understand the total return expectation at any given time. The price objective reflects the analyst's view of the potential price appreciation (depreciation).**

| Investment rating | Total return expectation (within 12-month period of date of initial rating) | Ratings dispersion guidelines for coverage cluster* |
|---|---|---|
| Buy | ≥ 10% | ≤ 70% |
| Neutral | ≥ 0% | ≤ 30% |
| Underperform | N/A | ≥ 20% |

* Ratings dispersions may vary from time to time where BofA Merrill Lynch Research believes it better reflects the investment prospects of stocks in a Coverage Cluster.

***INCOME RATINGS*, indicators of potential cash dividends, are: 7 - same/higher (dividend considered to be secure), 8 - same/lower (dividend not considered to be secure) and 9 - pays no cash dividend.** *Coverage Cluster* is comprised of stocks covered by a single analyst or two or more analysts sharing a common industry, sector, region or other classification(s). A stock's coverage cluster is included in the most recent BofA Merrill Lynch report referencing the stock.

BofA Merrill Lynch Research Personnel (including the analyst(s) responsible for this report) receive compensation based upon, among other factors, the overall profitability of Bank of America Corporation, including profits derived from investment banking. The analyst(s) responsible for this report may also receive compensation based upon, among other factors, the overall profitability of the Bank's sales and trading businesses relating to the class of securities or financial instruments for which such analyst is responsible.
BofA Merrill Lynch Global Credit Research analysts regularly interact with sales and trading desk personnel in connection with their research, including to ascertain pricing and liquidity in the fixed income markets.

## Other Important Disclosures

From time to time research analysts conduct site visits of covered issuers. BofA Merrill Lynch policies prohibit research analysts from accepting payment or reimbursement for travel expenses from the issuer for such visits.
Prices are indicative and for information purposes only. Except as otherwise stated in the report, for the purpose of any recommendation in relation to: (i) an equity security, the price referenced is the publicly traded price of the security as of close of business on the day prior to the date of the report or, if the report is published during intraday trading, the price referenced is indicative of the traded price as of the date and time of the report; or (ii) a debt security (including equity preferred and CDS), prices are indicative as of the date and time of the report and are from various sources including Bank of America Merrill Lynch trading desks.
The date and time of completion of the production of any recommendation in this report shall be the date and time of dissemination of this report as recorded in the report timestamp.

This report may refer to fixed income securities that may not be offered or sold in one or more states or jurisdictions. Readers of this report are advised that any discussion, recommendation or other mention of such securities is not a solicitation or offer to transact in such securities. Investors should contact their BofA Merrill Lynch representative or Merrill Lynch Financial Global Wealth Management financial advisor for information relating to fixed income securities.
Rule 144A securities may be offered or sold only to persons in the U.S. who are Qualified Institutional Buyers within the meaning of Rule 144A under the Securities Act of 1933, as amended.
SECURITIES DISCUSSED HEREIN MAY BE RATED BELOW INVESTMENT GRADE AND SHOULD THEREFORE ONLY BE CONSIDERED FOR INCLUSION IN ACCOUNTS QUALIFIED FOR SPECULATIVE INVESTMENT.
Recipients who are not institutional investors or market professionals should seek the advice of their independent financial advisor before considering information in this report in connection with any investment decision, or for a necessary explanation of its contents.
The securities discussed in this report may be traded over-the-counter. Retail sales and/or distribution of this report may be made only in states where these securities are exempt from registration or have been qualified for sale.
This report, and the securities discussed herein, may not be eligible for distribution or sale in all countries or to certain categories of investors.
BofA Merrill Lynch Global Research policies relating to conflicts of interest are described at http://go.bofa.com/coi.
"BofA Merrill Lynch" includes Merrill Lynch, Pierce, Fenner & Smith Incorporated ("MLPF&S") and its affiliates. Investors should contact their BofA Merrill Lynch representative or Merrill Lynch Global Wealth Management financial advisor if they have questions concerning this report. "BofA Merrill Lynch" and "Merrill Lynch" are each global brands for BofA Merrill Lynch Global Research.
Information relating to Non-US affiliates of BofA Merrill Lynch and Distribution of Affiliate Research Reports:
MLPF&S distributes, or may in the future distribute, research reports of the following non-US affiliates in the US (short name: legal name, regulator): Merrill Lynch (South Africa): Merrill Lynch South Africa (Pty) Ltd., regulated by The Financial Service Board; MLI (UK): Merrill Lynch International, regulated by the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA); Merrill Lynch (Australia): Merrill Lynch Equities (Australia) Limited, regulated by the Australian Securities and Investments Commission; Merrill Lynch (Hong Kong): Merrill Lynch (Asia Pacific) Limited, regulated by the Hong Kong Securities and Futures Commission (HKSFC); Merrill Lynch (Singapore): Merrill Lynch (Singapore) Pte Ltd, regulated by the Monetary Authority of Singapore (MAS); Merrill Lynch (Canada): Merrill Lynch Canada Inc, regulated by the Investment Industry Regulatory Organization of Canada; Merrill Lynch (Mexico): Merrill Lynch Mexico, SA de CV, Casa de Bolsa, regulated by the Comisión Nacional Bancaria y de Valores; Merrill Lynch (Argentina): Merrill Lynch Argentina SA, regulated by Comisión Nacional de Valores; Merrill Lynch (Japan): Merrill Lynch Japan Securities Co., Ltd., regulated by the Financial Services Agency; Merrill Lynch (Seoul): Merrill Lynch International Incorporated (Seoul Branch) regulated by the Financial Supervisory Service; Merrill Lynch (Taiwan): Merrill Lynch Securities (Taiwan) Ltd., regulated by the Securities and Futures Bureau; DSP Merrill Lynch (India): DSP Merrill Lynch Limited, regulated by the Securities and Exchange Board of India; Merrill Lynch (Indonesia): PT Merrill Lynch Sekuritas Indonesia, regulated by Otoritas Jasa Keuangan (OJK); Merrill Lynch (Israel): Merrill Lynch Israel Limited, regulated by Israel Securities Authority; Merrill Lynch (Russia): OOO Merrill Lynch Securities, Moscow, regulated by the Central Bank of the Russian Federation; Merrill Lynch (DIFC): Merrill Lynch International (DIFC Branch), regulated by the Dubai Financial Services Authority (DFSA); Merrill Lynch (Spain): Merrill Lynch Capital Markets Espana, S.A.S.V., regulated by Comisión Nacional del Mercado De Valores; Merrill Lynch (Brazil): Bank of America Merrill Lynch Banco Multiplo S.A., regulated by Comissão de Valores Mobiliários; Merrill Lynch KSA Company, Merrill Lynch Kingdom of Saudi Arabia Company, regulated by the Capital Market Authority.
This research report: has been approved for publication and is distributed in the United Kingdom (UK) to professional clients and eligible counterparties (as each is defined in the rules of the FCA and the PRA) by MLI (UK) and Bank of America Merrill Lynch International Limited, which are authorized by the PRA and regulated by the FCA and the PRA, and is distributed in the UK to retail clients (as defined in the rules of the FCA and the PRA) by Merrill Lynch International Bank Limited, London Branch, which is authorized by the Central Bank of Ireland and subject to limited regulation by the FCA and PRA - details about the extent of our regulation by the FCA and PRA are available from us on request; has been considered and distributed in Japan by Merrill Lynch (Japan), a registered securities dealer under the Financial Instruments and Exchange Act in Japan; is issued and distributed in Hong Kong by Merrill Lynch (Hong Kong) which is regulated by HKSFC is issued and distributed in Taiwan by Merrill Lynch (Taiwan); is issued and distributed in India by DSP Merrill Lynch (India); and is issued and distributed in Singapore to institutional investors and/or accredited investors (each as defined under the Financial Advisers Regulations) by Merrill Lynch International Bank Limited (Merchant Bank) (MLIBLMB) and Merrill Lynch

(Singapore) (Company Registration Nos F 06872E and 198602883D respectively). MLIBLMB and Merrill Lynch (Singapore) are regulated by MAS. Bank of America N.A., Australian Branch (ARBN 064 874 531), AFS License 412901 (BANA Australia) and Merrill Lynch Equities (Australia) Limited (ABN 65 006 276 795), AFS License 235132 (MLEA) distribute this report in Australia only to 'Wholesale' clients as defined by s.761G of the Corporations Act 2001. With the exception of BANA Australia, neither MLEA nor any of its affiliates involved in preparing this research report is an Authorised Deposit-Taking Institution under the Banking Act 1959 nor regulated by the Australian Prudential Regulation Authority. No approval is required for publication or distribution of this report in Brazil and its local distribution is by Merrill Lynch (Brazil) in accordance with applicable regulations. Merrill Lynch (DIFC) is authorized and regulated by the DFSA. Research reports prepared and issued by Merrill Lynch (DIFC) are done so in accordance with the requirements of the DFSA conduct of business rules. Bank of America Merrill Lynch International Limited, Frankfurt Branch (BAMLI Frankfurt) distributes this report in Germany and is regulated by BaFin.

This research report has been prepared and issued by MLPF&S and/or one or more of its non-US affiliates. MLPF&S is the distributor of this research report in the US and accepts full responsibility for research reports of its non-US affiliates distributed to MLPF&S clients in the US. Any US person receiving this research report and wishing to effect any transaction in any security discussed in the report should do so through MLPF&S and not such foreign affiliates. Hong Kong recipients of this research report should contact Merrill Lynch (Asia Pacific) Limited in respect of any matters relating to dealing in securities or provision of specific advice on securities or any other matters arising from, or in connection with, this report. Singapore recipients of this research report should contact Merrill Lynch International Bank Limited (Merchant Bank) and/or Merrill Lynch (Singapore) Pte Ltd in respect of any matters arising from, or in connection with, this research report.

**General Investment Related Disclosures:**

Taiwan Readers: Neither the information nor any opinion expressed herein constitutes an offer or a solicitation of an offer to transact in any securities or other financial instrument. No part of this report may be used or reproduced or quoted in any manner whatsoever in Taiwan by the press or any other person without the express written consent of BofA Merrill Lynch.

This research report provides general information only, and has been prepared for, and is intended for general distribution to, BofA Merrill Lynch clients. Neither the information nor any opinion expressed constitutes an offer or an invitation to make an offer, to buy or sell any securities or other financial instrument or any derivative related to such securities or instruments (e.g., options, futures, warrants, and contracts for differences). This report is not intended to provide personal investment advice and it does not take into account the specific investment objectives, financial situation and the particular needs of, and is not directed to, any specific person(s). This report and its content do not constitute, and should not be considered to constitute, investment advice for purposes of ERISA, the US tax code, the Investment Advisers Act or otherwise. Investors should seek financial advice regarding the appropriateness of investing in financial instruments and implementing investment strategies discussed or recommended in this report and should understand that statements regarding future prospects may not be realized. Any decision to purchase or subscribe for securities in any offering must be based solely on existing public information on such security or the information in the prospectus or other offering document issued in connection with such offering, and not on this report.

Securities and other financial instruments discussed in this report, or recommended, offered or sold by Merrill Lynch, are not insured by the Federal Deposit Insurance Corporation and are not deposits or other obligations of any insured depository institution (including, Bank of America, N.A.). Investments in general and, derivatives, in particular, involve numerous risks, including, among others, market risk, counterparty default risk and liquidity risk. No security, financial instrument or derivative is suitable for all investors. In some cases, securities and other financial instruments may be difficult to value or sell and reliable information about the value or risks related to the security or financial instrument may be difficult to obtain. Investors should note that income from such securities and other financial instruments, if any, may fluctuate and that price or value of such securities and instruments may rise or fall and, in some cases, investors may lose their entire principal investment. Past performance is not necessarily a guide to future performance. Levels and basis for taxation may change.

Futures and options are not appropriate for all investors. Such financial instruments may expire worthless. Before investing in futures or options, clients must receive the appropriate risk disclosure documents. Investment strategies explained in this report may not be appropriate at all times. Costs of such strategies do not include commission or margin expenses.

BofA Merrill Lynch is aware that the implementation of the ideas expressed in this report may depend upon an investor's ability to "short" securities or other financial instruments and that such action may be limited by regulations prohibiting or restricting "shortselling" in many jurisdictions. Investors are urged to seek advice regarding the applicability of such regulations prior to executing any short idea contained in this report.

This report may contain a trading idea or recommendation which highlights a specific identified near-term catalyst or event impacting a security, issuer, industry sector or the market generally that presents a transaction opportunity, but does not have any impact on the analyst's particular "Overweight" or "Underweight" rating (which is based on a three month trade horizon). Trading ideas and recommendations may differ directionally from the analyst's rating on a security or issuer because they reflect the impact of a near-term catalyst or event.

Foreign currency rates of exchange may adversely affect the value, price or income of any security or financial instrument mentioned in this report. Investors in such securities and instruments effectively assume currency risk.

UK Readers: The protections provided by the U.K. regulatory regime, including the Financial Services Scheme, do not apply in general to business coordinated by BofA Merrill Lynch entities located outside of the United Kingdom. BofA Merrill Lynch Global Research policies relating to conflicts of interest are described at http://go.bofa.com/coi.

MLPF&S or one of its affiliates is a regular issuer of traded financial instruments linked to securities that may have been recommended in this report. MLPF&S or one of its affiliates may, at any time, hold a trading position (long or short) in the securities and financial instruments discussed in this report.

BofA Merrill Lynch, through business units other than BofA Merrill Lynch Global Research, may have issued and may in the future issue trading ideas or recommendations that are inconsistent with, and reach different conclusions from, the information presented in this report. Such ideas or recommendations reflect the different time frames, assumptions, views and analytical methods of the persons who prepared them, and BofA Merrill Lynch is under no obligation to ensure that such other trading ideas or recommendations are brought to the attention of any recipient of this report.

In the event that the recipient received this report pursuant to a contract between the recipient and MLPF&S for the provision of research services for a separate fee, and in connection therewith MLPF&S may be deemed to be acting as an investment adviser, such status relates, if at all, solely to the person with whom MLPF&S has contracted directly and does not extend beyond the delivery of this report (unless otherwise agreed specifically in writing by MLPF&S). If such recipient uses the services of MLPF&S in connection with the sale or purchase of a security referred to herein, MLPF&S may act as principal for its own account or as agent for another person. MLPF&S is and continues to act solely as a broker-dealer in connection with the execution of any transactions, including transactions in any securities mentioned in this report.

**Copyright and General Information regarding Research Reports:**



Materials prepared by BofA Merrill Lynch Global Research personnel are based on public information. Facts and views presented in this material have not been reviewed by, and may not reflect information known to, professionals in other business areas of BofA Merrill Lynch, including investment banking personnel. BofA Merrill Lynch has established information barriers between BofA Merrill Lynch Global Research and certain business groups. As a result, BofA Merrill Lynch does not disclose certain client relationships with, or compensation received from, such issuers in research reports. To the extent this report discusses any legal proceeding or issues, it has not been prepared as nor is it intended to express any legal conclusion, opinion or advice. Investors should consult their own legal advisers as to issues of law relating to the subject matter of this report. BofA Merrill Lynch Global Research personnel's knowledge of legal proceedings in which any BofA Merrill Lynch entity and/or its directors, officers and employees may be plaintiffs, defendants, co-defendants or co-plaintiffs with or involving issuers mentioned in this report is based on public information. Facts and views presented in this material that relate to any such proceedings have not been reviewed by, discussed with, and may not reflect information known to, professionals in other business areas of BofA Merrill Lynch in connection with the legal proceedings or matters relevant to such proceedings.

This report has been prepared independently of any issuer of securities mentioned herein and not in connection with any proposed offering of securities or as agent of any issuer of any securities. None of MLPF&S, any of its affiliates or their research analysts has any authority whatsoever to make any representation or warranty on behalf of the issuer(s). BofA Merrill Lynch Global Research policy prohibits research personnel from disclosing a recommendation, investment rating, or investment thesis for review by an issuer prior to the publication of a research report containing such rating, recommendation or investment thesis.

Any information relating to the tax status of financial instruments discussed herein is not intended to provide tax advice or to be used by anyone to provide tax advice. Investors are urged to seek tax advice based on their particular circumstances from an independent tax professional.

The information herein (other than disclosure information relating to BofA Merrill Lynch and its affiliates) was obtained from various sources and we do not guarantee its accuracy. This report may contain links to third-party websites. BofA Merrill Lynch is not responsible for the content of any third-party website or any linked content contained in a third-party website. Content contained on such third-party websites is not part of this report and is not incorporated by reference into this report. The inclusion of a link in this report does not imply any endorsement by or

any affiliation with BofA Merrill Lynch. Access to any third-party website is at your own risk, and you should always review the terms and privacy policies at third-party websites before submitting any personal information to them. BofA Merrill Lynch is not responsible for such terms and privacy policies and expressly disclaims any liability for them.
All opinions, projections and estimates constitute the judgment of the author as of the date of the report and are subject to change without notice. Prices also are subject to change without notice. BofA Merrill Lynch is under no obligation to update this report and BofA Merrill Lynch's ability to publish research on the subject issuer(s) in the future is subject to applicable quiet periods. You should therefore assume that BofA Merrill Lynch will not update any fact, circumstance or opinion contained in this report.
Subject to the quiet period applicable under laws of the various jurisdictions in which we distribute research reports and other legal and BofA Merrill Lynch policy-related restrictions on the publication of research reports, fundamental equity reports are produced on a regular basis as necessary to keep the investment recommendation current.
Certain outstanding reports may contain discussions and/or investment opinions relating to securities, financial instruments and/or issuers that are no longer current. Always refer to the most recent research report relating to an issuer prior to making an investment decision.
In some cases, an issuer may be classified as Restricted or may be Under Review or Extended Review. In each case, investors should consider any investment opinion relating to such issuer (or its security and/or financial instruments) to be suspended or withdrawn and should not rely on the analyses and investment opinion(s) pertaining to such issuer (or its securities and/or financial instruments) nor should the analyses or opinion(s) be considered a solicitation of any kind. Sales persons and financial advisors affiliated with MLPF&S or any of its affiliates may not solicit purchases of securities or financial instruments that are Restricted or Under Review and may only solicit securities under Extended Review in accordance with firm policies.
Neither BofA Merrill Lynch nor any officer or employee of BofA Merrill Lynch accepts any liability whatsoever for any direct, indirect or consequential damages or losses arising from any use of this report or its contents.