Why Crypto Assets Should Be Part of Your Portfolio

Authors
Zev de Zeeuw (l)[1]
Alex Fauvel (m)
Amadeo Brands (r)

The aim of this paper is to introduce crypto assets and motivate to include crypto assets in your portfolio. Blockchains and cryptocurrencies have become the buzzwords of this decade. From a practical point of view, however, their use cases are still not widely adopted. With over a thousand crypto assets on the market, only a select few have the potential to live up to the hype. Last year the industry went through a bubble cycle. In the past seven years, this pattern has occurred four times, once in 2011, twice in 2013, and once in 2017. The only difference being the time frames, market size and number of people involved.

The Beginning

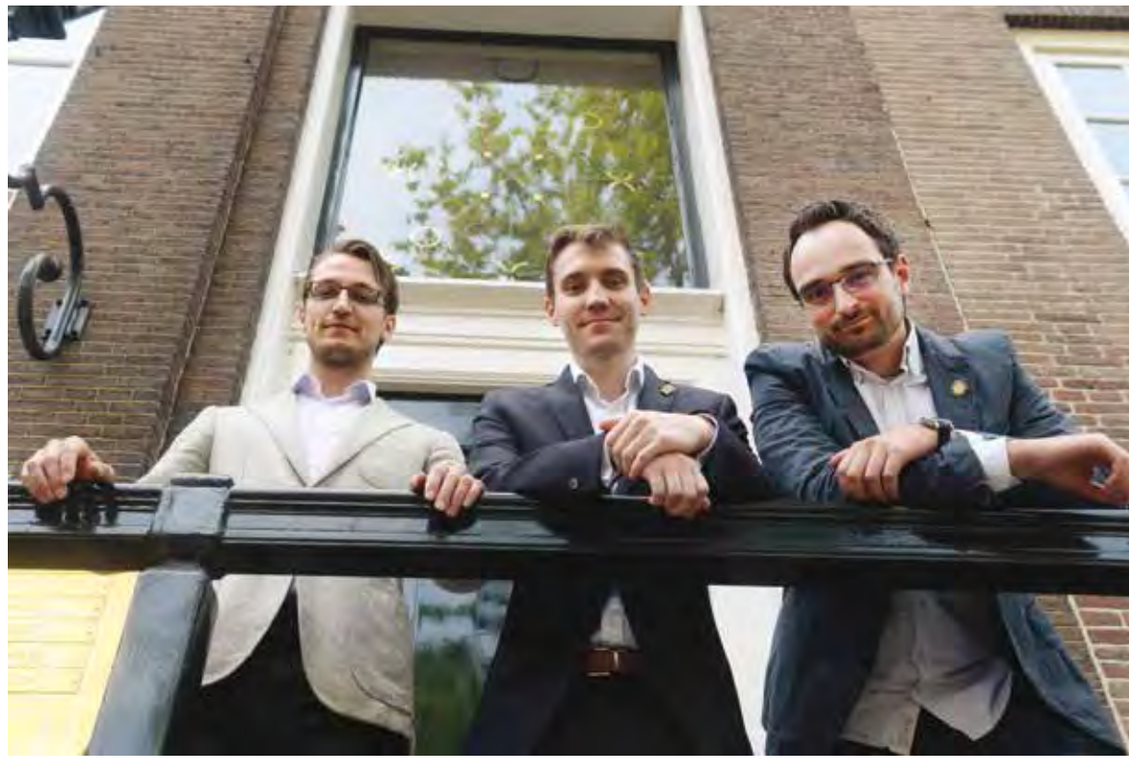
What crypto assets are is as complex as a topic gets. As broadly and succinctly as possible: a crypto asset is a digital representation of value on a distributed tamper proof registry, that no single entity controls yet everyone has access to.

The Problem It Solves

To answer this, we introduce two concepts which are central to explaining why crypto assets are important:

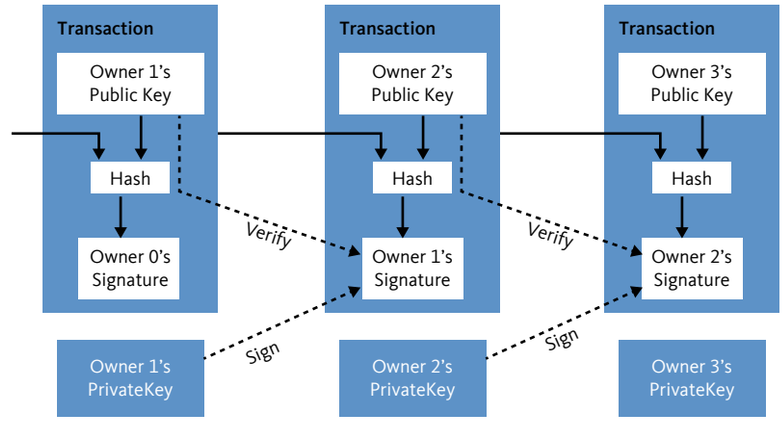
1. Computers can copy digital things perfectly.
2. Anything of value that is easily copied is practically worthless.

When one combines these two facts it becomes apparent that having a digital currency that exists entirely on computer networks might have some drawbacks. After all, how can information on a computer not simply be copied? This is also known as the double-spend problem or the Byzantine Generals problem.



Ever since the entertainment industry went through its digital transformation, it has been involved in a never-ending battle with piracy. It simply cannot stop anyone from copying and distributing intellectual property (e.g. music and films). Once content has reached a computer outside of the industry's control, it can be easily duplicated and redistributed. This form of reproduction and distribution, which is considered such a nuisance to the entertainment industry, is prohibitive to the existence of a digital currency. The essential difference between information and value, is that value cannot be in two places at once. As a result, the consequences of allowing unchecked copying and reproduction of value are dire for any monetary system.

Figure 1: Transfer and control of a digital asset using a private key



Solution

Bitcoin as invented by Satoshi Nakamoto (the pseudonymous person or group that invented the blockchain protocol for Bitcoin) allows different untrusted parties to reach consensus on a common historical truth. Cryptocurrencies have different methods of reaching consensus and thus solving the double-spend problem. In this section we will outline the original design, best exemplified by the Bitcoin blockchain.

It is important to point out that everyone who owns the currency is only able to modify the entry on the blockchain that corresponds to the value they possess. They control this value with a 'private key', which allows them to publish transactions to the blockchain.

Transactions on a blockchain are combined in pages of a ledger, called blocks. These pages or blocks are mathematically linked together so that they must occur in the order they are created and therefore remain unchanged. Consequently, everyone producing blocks has access to identical information. Blocks take computational work to create, requiring the consumption of resources (e.g. energy), thus incurring a cost to create. Block producers or the miners get rewarded for updating the ledger with transaction fees and newly created coins (block reward).

If anyone wishes to undo or change a particular transaction within any of these blocks they must invalidate all blocks that come after. To make the change valid, they must remake all the blocks following the change and create more blocks than the rest of the network. This is known as a 51% attack. The act of recalculating blocks (i.e. attacking the network) is economically irrational when compared with the profit that there is to be made by simply acting honestly. Honest miners can also choose to ignore malicious blocks and continue from the last-known valid point, introducing an additional risk to acting against the network. This cost-benefit analysis is the security mechanism of the blockchain. It is not that it is impossible to attack the network but that doing so is economically irrational.

The concept of a blockchain is not a new one, it was first described in the book Policing Online Games in 2003. Blockchains as we know them today are an elegant implementation of computer science and economics. Public decentralised blockchains operate because its maintainers have a greater economic incentive to stay honest than to attack the network. In other words they are working to acquire a coin of value, in this way crypto assets are inseparable from blockchains.

A Store of Value or Medium of Exchange?

For the past number of years, Bitcoin especially has been touted as digital gold. This is not only misleading, but also completely incorrect. Gold is gold, Bitcoin is Bitcoin. Bitcoin was designed as a peer-to-peer digital cash system as implied by the original whitepaper. The total value of the gold market is quite small when compared to that of cash. As of today, the total market capitalisation of gold is $7.5 trillion, while the total amount of M1 cash is $34.61 trillion. Furthermore, displacing gold is insurmountable when compared with displacing fiat currencies. The average lifespan of a fiat currency is 27 years, while gold has been highly valued by virtually every human civilisation since the dawn of trade.

Many believe that the fall of the US dollar, British pound, European euro, Japanese yen, Chinese renminbi or any other established fiat currency is unlikely. However, if we recognise that there is a possibility that weaker currencies such as the Venezuelan bolívar, Argentine peso, or Zimbabwean dollar may fail and be replaced by a kind of cryptocurrency, then we must also recognize that it is possible that more established currencies may someday be replaced by crypto assets.

Competitive Money

Financial systems often represent the natural progression of a civilization. All great civilizations in history started with a robust economic foundation of hard money, most often precious metals. Just before the end of World War Two, the majority of the allied nations world agreed to the Bretton Woods Accord, a scheme where nations pegged

their currencies to the US dollar and trusted the US to not violate the gold standard that was in place at the time. A few decades later during the Vietnam War US president Nixon removed the gold standard to avoid bankrupting the US, commonly known as "The Nixon Shock". Many people would argue the consequences of the US going bankrupt when the majority of the first world backed their own currency with it, would have been a disaster.

Each money or currency has its own benefits and drawbacks, they can mutate, and they can fail. If currencies evolve due to for example, competition, what would the next generation of currencies look like in this digital information age? Permission-less, decentralised crypto assets could be that next generation, and the central monetary authorities of the world are starting to take notice. In a recent report, Dong He, deputy director of the IMF's Monetary and Capital Markets Department, wrote:

> *"If central bank money no longer defines the unit of account for most economic activities – and if those units of account are instead provided by crypto assets – then the central bank's monetary policy becomes irrelevant."*

If there is even a slight chance that this scenario occurs, then the benefit of being exposed to crypto assets by far outweigh the risks that they currently present. If cryptocurrencies truly succeed, modern macroeconomics will have to be revisited.

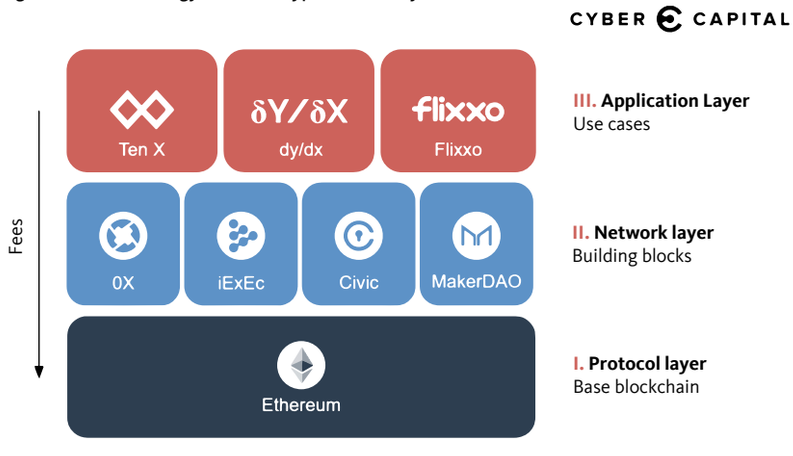
Different Crypto Asset Categories

So far, we have covered the money aspect of this new technology. Money maybe the first recognisable application, but it is not the only one. Entirely new business models and practices can be established causing the disruption of many industries.

Technology Stack

In this section we will map the technology stacks by defining three different layers and outline their economic models, as to understand the potential future of this technology.

Figure 2: The technology stack of a crypto asset ecosystem



1. Protocol Layer

The first layer acts as the foundation of the crypto asset sector and can be identified as the protocol layer, which provides the actual blockchain. Many protocols have modified the core architecture of the original Bitcoin protocol. However, they often have different advantages and disadvantages such as: Ease of use, transaction cost, scalability, accessibility, technology architecture, and differences in economic designs. Protocol layers always have a native token with common examples being Bitcoin, Ethereum and EOS. Crypto-ecosystems utilize these native tokens, as the network and application layers are both built on top of the base protocol. Typically, these protocol tokens are also competing to become world currencies.

2. Network Layer

The idea that every token has its own blockchain is a widespread misconception. Services within the network layer are actually built on top of an existing blockchain i.e. the protocol layer. Under a set of very narrow circumstances they might require their own unique token. These network services facilitate the application layer by adding functionality to the protocol in such a way that it allows others to create applications. Example use cases of such network layer services can be data storage, computation, identity management and exchange solutions. This layer is not what consumers will normally be interacting with on a daily basis.

3. Application Layer

The third layer is the application layer. This is the layer that consumers mostly interact with. These applications look very much like traditional businesses that provide a service to consumers. At the time of writing, there are only a few functional applications, as the market is still very immature. Yet examples would be businesses like Coinbase, Binance, Facebook, Airbnb, Amazon or Uber.

Economic Models

When looking at the complete technology stack, transaction fees are charged whenever layers interact with each other. This starts a chain reaction down the technology stack, where value is captured within each of the underlying layers. When looking at each individual service or token within the layers, they have different value propositions for token/coin holders and maintainers of the ecosystem's infrastructure. As such there are several different economic models (tokenomics). However, we can segment the different models into just two fundamental categories:

Currency

The currency model (i.e. cryptocurrency) makes the most sense for protocol layers, due to its security and network effect. Its value proposition is simply a global currency for use anywhere that accepts it as a form of payment.

To bring a currency into circulation, certain mechanisms exist to determine how and to whom it is distributed. Most mechanisms for protocol layers will distribute the coins to those that contribute resources typically known as miners, stakers or block producers. This is comparable to traditional money creation by a central bank.

Some of these currency models do not have any money creation, or only use monetary growth to support maintenance of the network in its early stages. The incentives to continue maintaining the infrastructure would eventually transition into transaction fees, allowing the system to continue.

Securities

Some crypto assets act more like traditional securities, commonly known as security tokens. A share of the revenue or profit, generated by the entity behind the asset, is distributed to the investors in the token. Due to the efficient and transparent nature of the blockchain, this distribution can be done in real time. These more complex security tokens can also sometimes represent a vote on a subject related to the token's function, just like traditional voting rights of a company. Furthermore, a security token could also represent a real asset, such as gold, fiat currency, or even a share in real estate.

Security, Hacks and Fraud

Traditional assets typically go hand in hand with custodial counterparty risks. The infrastructure required for such schemes is vast. Fiat currency for example: If a company would wish to store more than 10 million USD, they are unable to do so without oversight and management. However, with crypto assets, security can be as much or as little as one would like it to be. Since the security is based upon randomness of numbers, one of the most secure methods simply utilises some dice and an offline computer. Best practices are still being developed since this is an immature ecosystem. One such development is custodial services for institutions and individuals that do not wish to take on such overhead risk. This is the freedom that crypto assets provide, they do not force people to have a custodian and allow them to maintain their financial sovereignty.

Mt.Gox

Sometimes the risks of being one's own custodian present themselves in a very real way. Many people are typically familiar with the Mt. Gox scandal of 2014. Mt. Gox the largest Bitcoin exchange at the time was hacked and lost around 850,000 bitcoins. Headlines around the world highlighted the risk of being your own custodian, while at the same time illustrating the issue of counterparty risk. If security is breached and the attacker accesses the private keys, there is no one to call that can help. Once it is gone it is gone, even if the perpetrator is caught, reclaiming the value may still not be possible unless they give it back of their own volition.

DAO Hack

Ethereum has had several high-profile hacks; The DAO (Distributed Autonomous Organisation) hack was one of the largest and most dangerous hacks in the history of cryptocurrencies. The consequences of the hack called into question many of the beliefs and practices of the community.

The DAO was an Ethereum smart contract designed to organise both commercial and non-profit enterprises. At the time, it was the largest crowd funded project in history, totalling 14% of all Ethereum coins in existence (150 million USD at the time). The hackers managed to move a portion of the funds into a subsidiary account without proper authorisation. Although this was immediately noticeable, recourse was limited, the only immediate mitigation possible was to take the remaining money at the same rate as the attacker. The aftermath caused the community to split in ideologies which caused a subsequent real split in the cryptocurrency itself. The result was two protocol layers sharing a common blockchain history, but now with their individual blockchain and currency; Ethereum (ETH) and Ethereum Classic (ETC). The former, returned the victim's funds, the latter allowed the attackers to keep their spoils.

ICO Frauds

The typical path for launching a crypto asset is the following: founding, private sale, pre-sale, Initial Coin Offering (ICO), building, platform launch and adoption. The issue with this process is the accelerated funding rounds before the product has even begun its construction. ICO's have been the most popular funding method for startups in 2017. An EY report estimated that approximately $4 billion was raised through ICO's compared with only $1.8 billion via traditional VC investments for blockchain start-ups.

Projects currently worth hundreds of millions or even billions of dollars have no product, no customers or are outright frauds. It is likely that the majority of these projects will fail, while some may well be prosecuted for securities fraud. This environment is the result of a global market with hyper-inflated expectations of a new technology. Start-ups rarely fail due to a lack of funding, they fail due to mismanagement, ill-advised teams, unworkable products or simply lack of market demand. No amount of money can fix any of these issues. As high-profile projects start to fail, investors with a high-risk appetite may experience capital exhaustion and be unable to continue participating in the market. This would reduce the size of the ICO market dramatically potentially making many of these assets comparable to penny stocks.

If due diligence is done with correct understanding, all risks discussed can be mitigated. If projects are not willing to provide information to prove their claims then there is no reason to trust or invest in them. Crypto assets allow investors to do more thorough due diligence, from code analysis to transparent on-chain audits. A project that refuses

to prove its claims or is ignorant of the underlying mechanics should immediately cause concern to investors and users alike. Unsurprisingly the crypto asset industry has seen a resurgence in use of the phrase 'caveat emptor', in English: 'Let the buyer beware'.

Regulation

Most current crypto assets have no purpose other than to raise funds for the development of new business initiatives and would therefore fall under classic securities law. To circumvent this, the 'utility token' was introduced, which has none of the technical mechanics of a security token as outlined previously. Despite this, the objective of raising capital remains the same. Therefore, classic regulation still applies. New classifications are unlikely to be created for these offerings, which makes it likely that most utility tokens available today will be classified as non-compliant securities.

The Commodity Futures Trading Commission (CFTC) and the Securities and Exchange Commission (SEC) have made statements detailing their initial intentions to regulate crypto assets. These intentions seem to be that ICOs will be treated like classic IPOs, i.e. security offerings, whereas sufficiently decentralised protocol layers could be classified as commodities. It is as of yet unclear how a sufficiently decentralised protocol layer that previously performed an ICO will be treated within this legal framework.

Metrics, Performance & Risk

We believe the crypto asset class has the potential to be the best performing asset class for the next five years in terms of return on investment. However, such potential does not come without risk. In this section the equitability of the crypto asset risk premium will be evaluated. It should be noted, that the immaturity of this market means that there is a limited amount of data. Bitcoin, being the most mature asset, will be the focus of the following analysis.

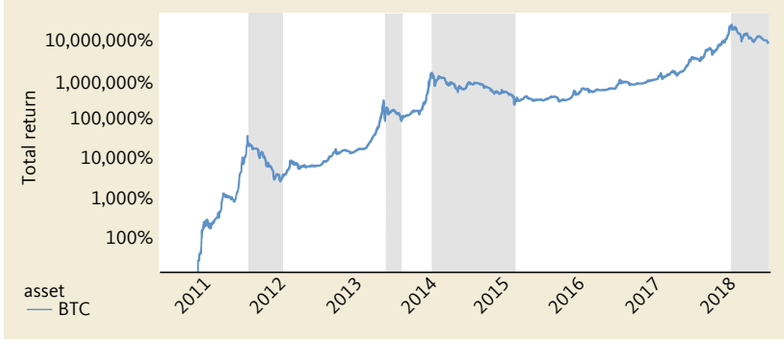
Returns

Bitcoin has increased considerably in value since it first started trading in 2010. This historic rise has not been without its corrections. Below we have highlighted market reversals and shown that even when buying bitcoin at the peak of each cycle, substantial returns have been made.

Sharpe ratios

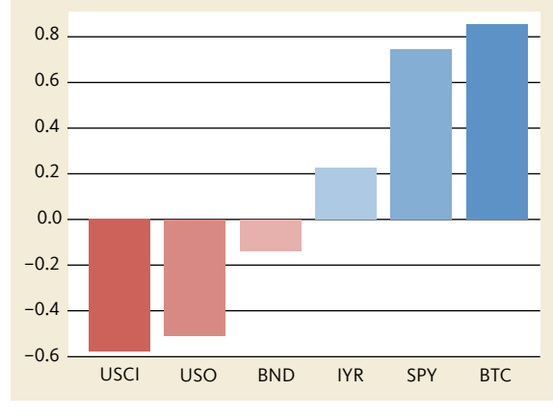
To evaluate the crypto asset risk premium, we use the most popular risk-adjusted performance metric, namely the Sharpe ratio. In figure 4, the Sharpe ratio is provided for five traditional asset classes and Bitcoin (BTC) based on daily log returns from the June 8th 2011, the inception date of the first indicated bear market, until June 19th 2018. The other five assets are the United States Commodity Index (USCI), United States Oil Fund (USO), Vanguard Total Bond Market ETF (BND), iShares US Real Estate ETF (IYR), and SPDR S&P 500 ETF (SPY). The figure shows that BTC has an excellent Sharpe ratio similar to that of the S&P 500. Thus, from an investment perspective Bitcoin's high volatility is transcended by its annual performance.

Figure 3: Bitcoin returns 2010-09-30 to 2018-06-19 with bear markets indicated in grey on a log-scale since. The historic price levels show extended downward market trends, but in the long term, unfortunately timed buys have yielded considerable profits. Price data provided by CoinDesk and Cyber Capital



Date of market reversal	Bear market drawdown	Retrun from market high to 2018-06-19
2011-06-08	-93%	22,661%
2013-04-24	-57%	4,269%
2013-12-04	-85%	487%
2017-12-16		-65%

Figure 4: Annualised Sharpe ratio based on daily log returns from 2011-6-8 (start BTC bear market) to 2018-06-19. The risk-free rate is assumed to equal 0%. Price data provided by CoinDesk, Yahoo Finance, and Cyber Capital

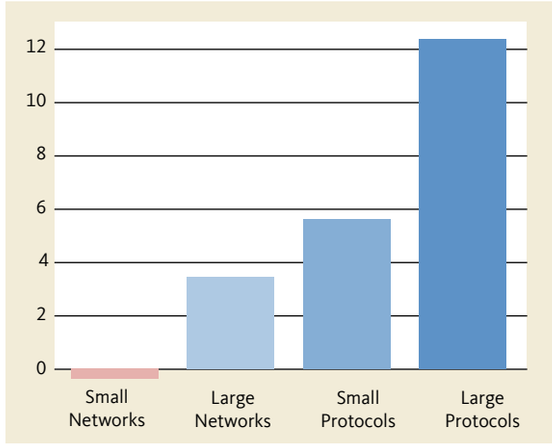


Protocol and Network Layers

In Figure 5, we have analysed the difference in the network and protocol layer's annualized Sharpe ratio. As of 2017-1-1 the application layer is only very meagrely represented in the top 100 crypto asset market capitalisations. Therefore, we have elected to omit this layer completely. We also separated large and small projects by respectively the top 20 and 21 to 100 in market capitalization. Clearly, protocol layer coins appear to perform better. This is in line with the perspective that this market is young, and the foundations of the tech-

nology still need to be solidified before further constructs are built on top. It can also be observed, that smaller assets perform worse on average. There seem to have been a large number of low quality projects in the top 100. But they are likely being identified as such by investors before reaching the top 20.

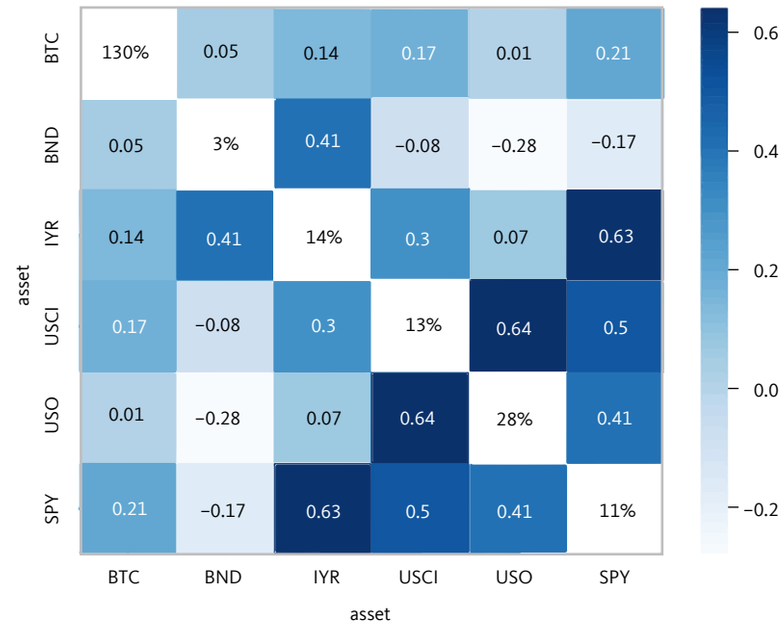
Figure 5: Annualised Sharpe ratio based on daily log returns from 2017-1-1 to 2018-06-19 for four indicated crypto asset categories. The risk-free rate is assumed to equal 0%. Price data provided by CoinMarketCap and Cyber Capital



Correlations and Volatility

When examining the correlation matrix (figure 6), we can see that all traditional asset classes have a correlation of at least 0.41 with at least one other asset. Yet, Bitcoin has a maximum correlation of 0.21. This makes the role of Bitcoin in one's portfolio irreplaceable. As indicated in the Sharpe ratio section, crypto assets provide a good risk-return balance on their own. Furthermore, we can see that the correlation with more traditional investment classes indicate great potential for portfolio diversification benefits.

Figure 6: Correlation matrix based on monthly log returns from 2010-09-30 to 2018-06-19 including annualized volatilities for the compared assets on diagonal. Price data provided by CoinDesk, Yahoo Finance, and Cyber Capital



Conclusion

In this article we have taken a critical look at the current state of crypto assets as an investment from an insider's perspective. In our final performance analysis, we focused on Bitcoin because it is most well-known and has the longest history. This does not mean that we endorse Bitcoin as an investment. Bitcoin has a number of problems such as scalability and ease of use, that it must overcome in order to fulfil its true potential. Its competitors such as Ethereum, Bitcoin Cash, EOS and Dash are catching up in some metrics and have even overtaken it in others.

Finding out the specific problems of crypto assets is a great learning experience. We recommend everyone to do his or her own due diligence on this new and exciting technology. The question one should be asking is which of them will eventually execute and deliver? Caveat Emptor.

Literature and References

- Leslie Lamport, Robert Shostak, and Marshall Paese, 1982, The Byzantine Generals Problem, ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3.
- Peter Wayner, 2003 Policing Online Games
- Satoshi Nakamoto, 2009, Bitcoin: A Peer-to-Peer Electronic Cash System
- Wikipedia, Gold reserve, https://en.wikipedia.org/wiki/Gold_reserve
- CIA, The world factbook, https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html
- Chris Mack. 2011, Is This Time Different for the Dollar?
- John Maynard Keynes, Harry Dexter White, 2013, The Battle of Bretton Woods
- Lewis E. Lehrman, 2011, The Nixon Shock Heard 'Round the World, https://www.wsj.com/articles/SB10001424053111904007304576494073418802358
- Dong He, 2018, Monetary Policy in the Digital Age,, http://www.imf.org/external/pubs/ft/fandd/2018/06/central-bank-monetary-policy-and-cryptocurrencies/he.htm
- EYGM LIMITED, 2018, EY research: initial coin offerings (ICOs), https://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/%24File/ey-research-initial-coin-offerings-icos.pdf
- Frank Chaparro, 2018, Businessinsider, http://www.businessinsider.com/ico-community-should-be-worried-about-a-coming-wave-2018-6?international=true&r=US&IR=T
- William Hinman, 2018, Digital Asset Transactions, https://www.sec.gov/news/speech/speech-hinman-061418

Note

1 Alex Fauvel – *Fundamental Cryptocurrency Analyst at Cyber Capital*
Amadeo Brands – *Fundamental Cryptocurrency Analyst at Cyber Capital*
Zev de Zeeuw – *Quantitative Cryptocurrency Analyst at Cyber Capital*