Bitcoin and Other Cryptocurrencies: A Review

Andrew Hencic

September 20, 2019

1 Bitcoin and Other Cryptocurrencies

This paper will provide some background on Bitcoin and other cryptocurrencies. A large appreciation of prices in late 2017/early 2018 along with the accompanying news stories generated much interest and discussion in the currencies. Recent developments in the literature are addressed here.

1.1 Cryptocurrencies

Researchers at the European Central Bank (2015) define cryptocurrencies as virtual currency schemes which can be readily converted to a national currency and bought and sold according to an exchange rate. Of these, the most popular is Bitcoin. Originally unveiled in 2009 by a pseudonymous developer under the moniker Satoshi Nakamoto, it has provided the blueprint and inspiration for a new generation of cryptocurrencies.

Of the more than 2000 cryptocurrencies in existence [1] four stand apart from the rest in terms of market capitalization and volume. These are Bitcoin, Ethereum, XRP and Litecoin. As of March 27, 2019 their market capitalizations stand at $71.9 Billion, $17.8 billion, $13.0 Billion and $3.8 Billion, respectively. Each has its own unique features and purpose, which makes them an interesting case study and introduction into the world of cryptocurrencies.

1.2 Bitcoin

Bitcoin is the original cryptocurrency. Created in 2009 by Satoshi Nakamoto it became famous for its distributed ledger technology (called the Blockchain), fixed lifetime supply and guiding philosophy to create a financial system that ensures anonymity (Nakamoto 2009).

The basic building block of Bitcoin is the Blockchain. Bitcoin seeks to create a system where payments can be sent and received without the need for an intermediary. In order to do this, the Blockchain was developed as a "distributed ledger", so that all participants in the ecosystem can trust that payments are being processes accurately and no double spending is occurring. Chapter 2 will provide a more detailed description of the mechanism behind the Blockchain, but a brief discussion here will follow.

Owners of bitcoin download an electronic wallet where they will store their bitcoins. Each wallet is assigned a unique id. As users make payments in bitcoin, they are transferred from one wallet to another. In order to track these transactions the blockchain records them in a public ledger. Importantly, even though the ledger is public the anonymity of the users is preserved.

Members of the network compete to be able to add transactions to the ledger. In order to win the right to add to the ledger they have to solve a cryptographic problem.

[1] The website Coin Market Cap has a complete list: https://coinmarketcap.com/all/views/all/

The difficulty of this problem adjusts such that a new 'block' is added to the blockchain every 10 minutes. Whichever participants solves the problem first is rewarded with newly created bitcoins (this is how the supply of bitcoins is increased). However, as the total supply of bitcoins is limited to 21 million units, eventually the participant that adds the new block will be able to charge a transaction fee.

1.3 Litecoin

Much like Bitcoin, Litecoin's stated mission is to facilitate peer-to-peer payments around the world[2]. Its creator, Charlie Lee, sought to improve upon Bitcoin so as to make a currency more suitable for use in many transactions. As with Bitcoin, it is built using the blockchain. However, rather than blocks being added every 10 minutes, Litecoin has blocks added every 2.5 minutes. Along with the faster transaction times, it also has a finite supply of 84 million Litecoins.

1.4 Ether

Ethereum itself is not a cryptocurrency, but a platform upon which applications looking to use blockchain technology can be built[3]. It was originally proposed by a developer by the name of Vitalik Buterin [4], and is currently the project of the Ethereum Foundation[5].

The basic premise of Ethereum is like that of Bitcoin. The blockchain still exists as a public ledger that is the official record of transactions and balances on the Ethereum network. However, unlike the Bitcoin blockchain which is essentially a list of the transactions on the network, the Ethereum blockchain contains both the list of transactions and the state of the blockchain (in the simplest case, the balances of all the accounts).

The Ethereum whitepaper provides a list of potential use cases for the platform, but the primary one is the ability to build 'smart contracts' that will execute themselves, eliminating the need for counterparties to rely on each others trustworthiness.

Ether (ETH) is the unit of account employed by the Ethereum network. For the Ethereum network to process a smart contract (or any other application) it charges a transaction fee in Ether based on how computationally complex the task is. The user whose transaction is being executed compensates the network with Ether taken from their digital wallet.

Like other cryptocurrencies, Ether relies on the blockchain to record and verify transactions. There are two major differences between Ether and Bitcoin. First, unlike Bitcoin who's total supply is capped at 21 million units, there is no fixed supply of Ether. Secondly, blocks are added to the Ether blockchain every 15 seconds (on average), unlike the

[2]https://litecoin.org/

[3]https://www.ethereum.org/

[4]Whitepaper: https://github.com/ethereum/wiki/wiki/White-Paper

[5]www.ethereum.org

approximately 10 minutes for Bitcoin[6].

The block reward for mining Ethereum (i.e. the payment received for adding transactions to the blockchain) is currently set at 5.0 ETH plus whatever the transaction cost charged was, plus and extra reward for including an orphaned chain as part of the block [7].

1.5 XRP

Unlike other cryptocurrencies, XRP was developed by the for profit firm Ripple. Ripple [8] looks to facilitate payments for institutions and XRP is a component of their payments processing system. Rather than looking to create a financial system that operates outside of the establishment, Ripple is looking to exploit blockchain technology to reduce frictions in the global payments system.

Amongst their clients Ripple lists, Santander, a major European bank. They are using the Ripple platform for a mobile application that allows users execute cross border transactions with much shorter transaction times [9].

XRP is not only limited to financial institutions but is available for purchase by the general public on cryptocurrency exchanges. In addition, it XRP not mined like other cryptocurrencies. 100 Billion XRP coins were created and this supply is to be held fixed going forward[10].

1.6 Bitcoin News and Awareness

Bitcoin was on the radar of Fed officials far before its recent price appreciations. In a working paper (Yermack 2013) Fed researchers explored its merits as a currency by discussing how well it fulfils the three functions of money: (1) a medium of exchange, (2) a unit of account, and (3) a store of value.

Yermak finds that there are serious limitations to its usefulness as a medium of exchange. At the time of writing, the author finds that registered merchants(roughly 24,000 of them) averaged less than one Bitcoin transaction per day. Additionally, the author highlights that acquiring Bitcoin is not very easy as they either have to be mined, or acquired on an exchange which exposes the user to another set of risks. Finally, Yermack notes that there are no credit products available to consumers, resulting in all transactions having to be conducted on a cash basis.

When Bitcoin is examined through the lens of a unit of account. Yermack notes the volatility in the Bitcoin/Dollar exchange rate would negatively impact price stability in

[6] www.ethdocs.org/en/latest/mining.html

[7] The orphaned chains are called 'uncles'. For more details as to why they are included please see: www.ethdocs.org/en/latest/mining.html

[8] A description of the firm is available at: https://ripple.com/company/

[9] `https://ripple.com/files/case_study_santander.pdf`

[10] `https://bitcoinmagazine.com/guides/what-ripple`

the market and is ultimately, "costly to the merchant and confusing to the consumer". Citing the summary of research on consumer prices by Thomas and Morwitz (2009), Yermack notes the challenges faced by consumers in comparing prices. Extending this notion to Bitcoin, whose divisibility is often cited as a feature, Yermack remarks that these issues could very well be exacerbated when prices are listed in scientific notation.

Lastly, Yermack notes two limitations in Bitcoin's usefulness as a store of value. First, is the very high volatility relative to gold and national currencies. Secondly, there is no real form of deposit insurance. Given the relatively frequent security lapses and robberies of Bitcoin exchanges (notably that of Mt.Gox in 2014), it seems the latter point is crucial to long term viability of Bitcoin as a currency.

Schilling and Uhlig (2018b) develop a model to derive the fundamental value of Bitcoin in a world where agents can decide which currency they transact in. The authors present a model of an exchange economy with two infinitely lived agents who alternate their consumption and production between even and odd periods. The pricing equation for Bitcoin is shown to be a martingale if conditions for no speculation are satisfied. Schilling and Uhlig (2018a) then present a model for currency choice in the presence of transaction costs (in the case of Bitcoin) and value added taxes (for traditional currencies). The relative costs of transacting in the currencies determine the choice of the medium of exchange for agents.

The rising popularity of cryptocurrencies has caught the attention of monetary authorities around the world. A European Central Bank (2015) research paper provides a comprehensive review of virtual currency schemes (and the cryptocurrencies that form a subset of them). Of the roughly 500 cryptocurrencies operating at the time of writing the report notes that only Bitcoin had emerged as being used for payments. Bitcoin is also credited as being important to the emergence of other cryptocurrencies as it is an open-source project whose protocol forms the basis for many of the new "altcoins", including other major cryptocurrencies Ethereum, XRP, and Litecoin.

The report provides four main characteristics along which virtual currency schemes can be differentiated. First, the transaction validating system they employ. The two main methods are proof of work systems, like that used by Bitcoin, and proof of stake systems [11]. The proof of stake system purports to be more energy efficient and process transactions faster than the proof of work system. Secondly, the algorithms used by the currencies can be differentiated by the type and quality of hardware required to execute the algorithm. Thirdly, the supply of coins differs across products. Some, like Bitcoin and Litecoin, have a fixed total supply, while others do not. Lastly, some virtual currency schemes don't necessarily operate as currencies, but rather offer services that employ

[11]The biggest difference between the two is that the proof of work system relies on participants to compete to, in essence, solve mathematical problems in order to verify transactions. These participants are then rewarded with newly created cryptocurrency. In a proof of stake system transactions are verified by predetermined members of the network who already have established stakes in the cryptocurrency. These members can then collect a transaction fee, rather than receiving newly created cryptocurrency.

the blockchain technology. More detail in the measure of differentiation and about the potential applications and pitfalls of virtual currency schemes can be found in the 2015 report.

The Bank of Canada has also been conducting research on the applications and awareness of cryptocurrencies. Given its leading position in the market place the BoC has run a so called "Bitcion Omnibus Survey" of the general public to ascertain their awareness of, and involvement with, Bitcoin. The first edition was conducted in 2016, while the 2017 edition cointains an addendum with a questionnaire to gauge the knowledge of the participants.

In line with the rapid price appreciation from 2016 to 2017 the authors find that the awareness of Bitcoin grew by 21 percentage points, with the highest levels of awareness amongst those with incomes over $ 70,000. The knowledge test showed that both owners and non-owners showed an increase in average test scores. The authors computed two test scores, including one that deducted points for wrong answers to discourage guessing, and in both instances the average score was higher for owners of Bitcoin than for non-owners. This indicates an increased familiarity for those who have a monetary investment in the cryptocurrency. It is important to note that the authors attribute an increase in scores from year to year to the improved readability of the questionnaire. Finally, the authors find that though ownership of Bitcoin had increased from 2016, that increase was attributable to newly aware individuals.

At the shorter time frequency, Urquhart (2018) employed Google Trends data that describes search popularity to examine what causes attention to Bitcoin. They construct three vector autoregressive models. The first includes search queries and realized volatility of Bitcoin returns, the second includes search queries and Bitcoin trading volume, and the third search queries and Bitcoin returns. Ultimately the author finds that after splitting the Bitcoin price sample (using a Bai and Perron (2003) test) the reaction of search queries to trading volume, returns, and realized volatility differ across subperiods. In the first period (pre October 28, 2013) none Granger cause search queries. In the second subperiod realized volatility of Bitcoin returns, Bitcoin trading volume and Bitcoin returns all Granger cause search queries at various lags.

For all of its attention there are still issues with Bitcoin markets. In their presentation to the Securities and Exchange Commission in support of their application for a Bitcoin ETF, Bitwise Asset Management illustrates one. Their report shows that up to possibly 95% of current trading volumes may not be real (slide 62) and, potentially, only 10 exchanges have actual volumes (slide 61).

1.7 Bitcoin Return Research

Much of the academic literature on Bitcoin has focused on its merits as a financial asset. Specifically, there has been a significant amount of research about the efficiency of Bitcoin prices and whether the behaviour of the price can be said to satisfy the Efficient Market

Hypothesis (EMH).

Urquhart (2016) was amongst the first to examine the efficient market properties of Bitcoin. Treating it as an asset, Urquhart looks to examine whether Bitcoin returns satisfy the weak form of market efficiency proposed by Fama (1970). Urquhart calculates Bitcoin log returns at the daily frequency by taking the volume weighted average price across exchanges. Then, the author conducts a variety of tests on these returns to test the EMH.

Ultimately, the author finds that all of the tests reject the weak form of informational efficiency over the full sample (August 1, 2010 to July 31, 2016). However, when the author splits the sample, with the second sample period starting in August 2013, the Ljung-Box (Ljung and Box (1978)) and automatic variance test (Choi (1999)) tests fail to reject the null hypothesis indicating some efficiency.

Bariviera (2017) looks to investigate the inconclusive market efficiency results of Urquhart (2016) by examining the long memory properties of Bitcoin return volatility. In order to conduct the analysis, Bariviera employs the Hurst exponent statistic using two methods; (1) the R/S method and (2) the Detrended Fluctuation Analysis method. The Detrended Fluctuation analysis method is better at avoiding detection of spurious long rang dependence. The author examines both daily returns and intraday volatility for dependence (i.e. the violation of the weak form of the Efficient Markets Hypotehsis).

Similar to Urquhart, Bariviera (2017) finds that Bitcoin returns exhibited dependence earlier in the sample, but lost these features after 2014. Meanwhile, the volatility clustering at the intraday level is found to be present over the whole sample.

Katsiampa (2017) looks to apply a single model of conditional heteroscedasticity to the whole Bitcoin historical time series. In order to accomplish this, the author computes the log returns of a Bitcoin price index provided by Coindesk. Then, using the log returns, an autoregressive model of the conditional mean and various forms of the conditional variance are modelled. Ultimately, amongst the whole suite of potential conditional variance models (GARCH, EGARCH, TGARCH, Asymmetric Power ARCH, Component GARCH, Asymmetric Component GARCH), the empirical exercise identifies that the AR(1)-CGARCH(1,1) model has the best in sample properties as measured by the maximized value of the log-likelihood function, the Akaike information criterion, Bayesian information criterion and Hannan-Quinn information criterion. The implication of these finding, like those of Bariviera (2017) are that there is information in the long run components of the historical time series, in this case directly related to the conditional variance.

Another branch of literature examines potential other drivers of bitcoin returns. Panagiotidis, Stengos and Vravosinos (2018) estimate four types of vector autoregressive processes (VAR), over two time periods, to examine the effects of shocks to explanatory variables on bitcoin returns [12]. The four frameworks they employ are; (1) the standard

[12]The authors provide a very extensive review of the literature on econometric research into the empirical determinants of bitcoin returns. This background forms the basis for the explanatory variables

VAR; (2) a factor augmented VAR; (3) a VAR with factor analysis; (4) a VAR with principal component analysis. The reason for the variety of methods is that there are a large number of potential explanatory variables, so the authors use various methods to reduce the dimensions of the VAR. Ultimately they find find that popularity (as measured by Google trends data and Wikipedia searches) has a reduced impact on bitcoin returns, while there exists a connection between shocks in traditional financial markets and bitcoin. Additionally, the factor analysis allowed the authors to examine the effects of geographic markets on Bitcoin returns. In the initial period (which begins in 2010 and ends in 2016) the authors find that shocks in the Asian region (measured by a combined China and Japan factor) had the largest impact, followed by the US and then Europe. However, over the sample that begins in 2010 and ends in 2018, the US becomes the most important. The authors note that this is likely due to the regulatory clampdown by Chinese authorities in late 2017 that saw a large reduction in the share of Bitcoin trading done with Renminbi.

1.8 Investment Strategies

Investors have begun examining the merits of inclusion of Bitcoin in their personal portfolios. Two papers, Bouri, Molnar, Azzi, Roubaud Hagfors (2017) and Timborn, Li and Hardle (2017), introduce methods for incorporating cryptocurrencies into investment portfolios.

Bouri et. al. (2017) examine the usefuleness of Bitcoin as a hedge or diversifier against conventional asset (equity, bonds and commodities) returns. To examine which of these functions Bitcoin can fulfil, the authors employ the Dynamic Conditional Correlation (DCC) model proposed by Engle (2002). The DCC model involves modelling the bivariate return equation of Bitcoin and the other asset as an autoregressive process and the conditional variance of the returns processes as a GARCH(1,1). Then, the time-varying unconditional correlation matrix of the standardized residuals from the initial GARCH estimation is then modelled as a bivariate system.

These dynamic correlations are then employed to evaluate whether Bitcoin can serve as an effective diversifier, hedge, or safe haven asset against a wide variety of financial assets [13]. By regressing these dynamic conditional correlations against dummies that represent extreme movements in different quantiles of the return distribution of various asset classes, the hedging properties are identified.

Using daily Bitcoin returns, the authors find that Bitcoin is a "strong hedge against movements in Japanese and Asia Pacific stocks". Meanwhile, the weekly returns demonstrate that it can only be a strong hedge for Chinese equities at this frequency. This difference in hedging and safe haven properties stands out. The authors note that this

chosen in the analysis.

[13] These include the S&P 500, a Bond Index, a commodity index and gold among others. See Bouri et. al. (2017) for the full list.

may be a product of the speculative nature of the daily returns. These speculative movements in the price then undermine Bitcoin's safe haven properties at both the daily and weekly frequency.

Finally, the authors conclude by noting that the hedging and diversification benefits of Bitcoin could change profoundly in the future as the time period they study (2011-2015) features very high return variance. Secondly, they note the limited liquidity of Bitcoin is an important caveat for its role in a portfolio, that could be improved with further financial innovation.

On this note, Trimborn et. al (2017) directly address the liquidity issue associated with investing with cryptocurrencies. The authors look to examine potential advantages of including cryptocurrencies in a diversified portfolio while directly addressing the issue of their relative illiquidity.

The authors begin by noting that there exist sufficient liquidity concerns when adding alternative assets to an investment portfolio comprised of the S&P 500 index, the DAX30 index and those listed on the Portuguese stock exchange. The advantages of the added returns and diversification could quickly be offset by an inability to liquidate the assets in time to rebalance the portfolio. In order to address this concern Trimborn et al. introduce the LIBRO (Liquidity Bounded Risk-Return Optimization) method. It is a modification of the traditional Markowitz diversification theory proposed by Markowitz (1952).

To motivate their work Trimborn et al. first present a simulation study to demonstrate that in portfolio construction the incorrect estimation of asset allocation weights is less of a concern than the incorrect estimation of the maximum weight attributable to an individual asset. This problem is, not surprisingly, exacerbated in the cases where the covariance amongst the assets in the portfolio is higher.

To find a proxy for liquidity the authors use Turnover Value. Turnover value is defined as the sum of transaction values over a predefined time interval.

This measure is then scaled by a factor that determines the speed at which the investor wants to clear their position. In turn, dollar amount assigned to any asset is then restricted to be less than or equal to the scaled Turnover value. By implementing this new constraint into the portfolio optimization problem, the performance of a portfolio with liquidity restrictions can be evaluated.

The authors then examine the merits of employing this augmented portfolio optimization strategy to a combination of 39 cryptocurrencies, the S&P 100 Index, the DAX30 index and those listed on the Portugal Stock Exchange. They find that, in sample, the portfolios incorporating cryptocurrencies improve the risk-return trade-off at every level of risk, including at the point of the global minimum variance portfolio. A novel observation is that a greater share of the investment is allocated to altcoins relative to bitcoins.

The cumulative performance of the S&P 100 portfolio with cryptocurrencies and no liquidity constraints shows minor improvements over a small horizon. However, when the liquidity constraints are added, the cumulative returns of the portfolio are 1.12% higher over the 3-year period. Similar results hold for the portfolio comprising of DAX stocks

and cryptocurrencies, with cumulative returns exceeding those of the stock portfolio by 1.5%. Examining the risk-adjusted returns with the Sharpe ratio, a similar story holds, with the liquidity constrained portfolio combining cryptocurrencies and stocks dominating those of the stock only portfolios. Finally, the portfolios comprising of Portuguese stocks and cryptocurrencies the outperformance of the portfolio with liquidity constraints was 3.4%. Therefore, by accounting for the liquidity issues and introducing cryptocurrencies into stock portfolios the authors show that meaningful improvements in the risk-return relationship can be achieved.

Using the portfolio with Portuguese stocks, the authors undertake their simulation study to demonstrate that error in the estimation of the risk of the portfolio remains small even when incorporating their proposed liquidity constraints.

2 Conclusion

The emergence of Bitcoin and other cryptocurrencies have led to an explosion of trading and speculation in once non-traditional markets. Their growing popularity is driving research into their uses and risks. This paper highlighted some of the more recent developments to date.

References

[1] Bitcoin Wiki. Introduction (2013, December 4). Retrieved December 4, 2013, from $https://en.bitcoin.it/wiki/Introduction$

[2] Bitcoin Wiki. Controlled Supply (2013, December 4). Retrieved December 4, 2013, from $https://en.bitcoin.it/wiki/Controlled\_Currency\_Supply$

[3] Bitcoin Wiki. Trade (2013, December 4). Retrieved December 4, 2013, from $https://en.bitcoin.it/wiki/Trade$

[4] Bitwise Asset Management: "Presentation to the U.S. Securities and Exchange Commission". March 19, 2019. Retrieved from: https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf

[5] Blockchain. Bitcoin Market Capitalization. Retrieved from Bitcoin Block Explorer $http://blockchain.info/charts/market\_cap$

[6] Bai, J. and P. Perron(2003): "Computation and Analysis of Multiple Structural Change Models", Journal of Applied Econometrics, 2003, vol. 18, issue 1, 1-22.

[7] Bariviera, A.F., (2017). "The Inefficiency of Bitcoin Revisited: A Dynamic Approach." Economics Letters 161, 1-4.

[8] Bouri, E., Molnar, P., Azzi, G., Roubaud, D., L.I. Hagfors, (2017). "On the Hedge and Safe Haven Properties of Bitcoin: Is it Really More than a Diversifier." Finance Research Letters 20, 192-198.

[9] Choi, I., (1999): "Test the Random Walk Hypothesis for Real Exchange Rates", Journal of Applied Econometrics 14, 293–309.

[10] Engle, R.F., (2002). "Dynamic Conditional Correlation - A Simple Class of Multivariate GARCH Models." Journal of Business and Economics STatistics 20, 339-350.

[11] European Central Bank, (2015). "Virtual Currency Schemes - A Further Analysis" European Central Bank, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

[12] Fama, E.F., (1970). "Efficient capital markets: A review of theory and empirical work." Journal of Finance 25, 383–417.

[13] Gordon, S., "What is Ripple", Bitcoin Magazine, `https://bitcoinmagazine.com/guides/what-ripple`

[14] Henry, C., K. Huynh, G. Nicholls (2018). "Bitcoin Awareness and Usage in Canada: An Update.", Bank of Canada Staff Analytical Not

[15] Katsiampa, P., (2017). "Volatility Estimation for Bitcoin: A Comparison of GARCH Models." Economics Letters, 3-6.

[16] Ljung, G.M., Box, G.E.P., (1978): "On a Measure of the Lack of Fit in Time Series Models." Biometrika 65 (2), 297–303.

[17] Markowitz, H. (1952). "Portfolio Selection", Journal of Finance 7.1, pp 77-91

[18] Nakamoto, S. (2009): "Bitcoin: A Peer-to-Peer Electronic Cash System", `https://bitcoin.org/en/bitcoin-paper`

[19] Panagiotidis, T., Stengos, T., and Vravosinos, O. (2018): "The Effects of Markets, Uncertainty and Search Intensity on Bitcoin Returns", The Rimini Centre for Economic Analysis WP.

[20] Ripple, "Santander Becomes First U.K. Bank to Use Ripple for Real-Time Cross Border Payments", `https://ripple.com/files/case_study_santander.pdf`

[21] Schilling, L.M., Uhlig, H. (2018a): "Currency Substitution under Transaction Costs" forthcoming AEA Papers & Proceedings 109

[22] Schilling, L.M., Uhlig, H. (2018b): "Some Simple Bitcoin Economics", WP

[23] Thomas, M. and V. Morwitz, (2009). "Heuristics in Numerical Cognition: Implications for Pricing" in Vithala R. Rao ed., Handbook of Pricing Research in Marketing (Northampton, MA: Edward Elgar Publishing).

[24] Trimborn S., Li M., Hardle K.M., "Investing with Cryptocurrencies - A Liqduidity Constrained Investment Approach" July 7, 2017

[25] Urquhart, A., (2016). "The Inefficiency of Bitcoin." Economics Letters 148, 80-82.

[26] Urquhart, A., (2018). "What Causes the Attention of Bitcoin." Economics Letters 166, 40-44.

[27] Yermack, D., (2013). "Is Bitcoin a Real Currency?" Fed WP