

# Cryptocurrency - A Brief Review

Nafeesa Khader Syed

Department of Finance and Banking, College of Business Administration Girls, Jizan University, Jizan, KSA

Email: syedanafeesaali[at]gmail.com

**Abstract:** *Cryptocurrencies are internet-based virtual currencies and exist without centralized regulating authorities. They are launched in the internet ecosystem and are used primarily outside of the traditional banking system. They are used for transfer and exchange of value over the internet. This brief review aims to give an introduction of the most commonly used cryptocurrencies.*

## 1. Introduction

Cryptography is an old science that is based on allowing hidden and secure communications. In the modern-day technological era, it is widely used for everyday tasks. (Drainville, 2012) Cryptocurrencies are a revolutionary modern medium of digital exchange. (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016) Cryptocurrency (CC) is "a digital currency secured with encryption". (Medeiros & Chau, 2016) They are virtual decentralized currencies, which are primarily online, are entirely independent of government or any central authority control and provide double-spending attack protection. (Gandal & Halaburda, 2016) (Lansky, 2018). CCs lack a central issuing authority and regulatory bodies and are primarily based on cryptography and are hence called cryptocurrency. They exist as an entirely independent entity and the transactions do not pass a bank. It acts as a medium of exchange, secures the transactions as well as controls the creation of new units. (Popuri & Gunes, 2016) Since the introduction of bitcoin in 2008, the use of CCs often for online transactions has increased enormously. (Abbasi, Chen, & Salem, 2008; Böhme, Christin, Edelman, & Moore, 2015; Kim et al., 2016) Furthermore, currently, a broad ecosystem of CCs has grown, and their usage has increased every year since their introduction (Gandal & Halaburda, 2016) Jan Lansky, a CC researcher, described CC as a system that meets the following six criteria: (Lansky, 2018)

- 1) "The system does not require a central authority; its state is maintained through distributed consensus".
- 2) "The system keeps an overview of cryptocurrency units and their ownership".
- 3) "The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units".
- 4) "Ownership of cryptocurrency units can be proved exclusively cryptographically".
- 5) "The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units".
- 6) "If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them".

Difference between cryptocurrency and blockchain & how they work together:

A blockchain consists of a sequential list of transactions in a unit of value (called a digital asset, cryptocurrency, coin, or token). They act as platforms that float the CCs. Hence blockchain is a distributed ledger, maintains a list of data records that grow continuously. They are designed against tampering and revision, even by operators of the data store's nodes. It mirrors a public ledger where all transactions executed are recorded. It continually grows as completed blocks are added to previous blocks thus forming a chain. The blocks in the blockchain are added in a linear, chronological order. (Fanning & Centers, 2016)

Sovbetov defined as "a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency". (Sovbetov, 2018)

CCs work in the platform provided by Blockchains, which act as a network and creates the means for transaction and transfer of value and information. CCs are coins or tokens used within these networks to send value and pay for these transactions. They digitize the value of the asset. Hence CCs are part of the ecosystem of Blockchain technology. (Kaplan, Aslan, & Bulbul, 2018) (Wu, Wheatley, & Sornette, 2018)

### Types of cryptocurrency

A number of cryptocurrencies are available over the internet as a cryptocurrency can be created at any time. (Chohan, 2017) (Fernández-Villaverde, 2018) Since its inception, the cryptocurrency market has seen substantial growth. (Wu et al., 2018) By market capitalization, Bitcoin remains the largest blockchain network with speculations of rise in Bitcoin price. (Wilmoth, 2019) This review deals with notable cryptocurrencies that are currently influential in the market.

#### Zcash (ZEC):

Zcash (Zero cash protocol) is a cryptocurrency template that is in many ways comparable to Bitcoin. It achieves greater efficiency and is based on a digital ledger of transactions called a blockchain. (Peck, 2016) (Zhong, 2002) (Sasson et al., 2014). It provides highly anonymous transactions as it maintains the privacy of the details of the sender, recipient and amount and hence offers enhanced security. Moreover, it does not use range-bounded commitment schemes. (Zhong, 2002) ("Privacy-protecting digital currency | Zcash," n.d.)

**Etherum (ETH):**

Etherum is an open-source network that is built using blockchain-based technology. (Mathis, 2018; Singh, Suguna, Satish, & My, 2018). It is a project which attempts to build a centralized technology. Etherum also provides a non-bitcoin cryptocurrency called ether which can be transferred between accounts. Etherum in particular has captivated many because of its so-called smart contract features with scripting functionality. (Singh et al., 2018) (Mathis, 2018) ("Etherum Project," n.d.)

**Ripple (XRP):**

Ripple is a digital real-time gross payment system. It is a currency exchange system created to aid the traditional banking sector, and it evolved independently of Bitcoin. It was created by Ripple Labs Inc., a US-based technology company, and holds the highest market cap after Bitcoin. (Armknrecht, Karame, Mandal, Youssef, & Zenner, 2015)

**Bitcoin Cash (BCH)**

Bitcoin is a peer-to-peer distributed digital currency that does not rely on a centralized authority. (Decker & Wattenhofer, 2013; Reid & Harrigan, 2013) It is the most prominent of the cryptocurrencies, and it operates on a set of rules proposed in Nakamoto. (Gandal & Halaburda, 2016; Moore & Christin, 2013) (Easley, O'Hara, & Basu, 2017) Bitcoin relies on a network of participants called miners that collectively implement a replicated ledger and verify transactions in a public log called the blockchain. The users within the system are called clients and are identified only by public-keys. (Decker & Wattenhofer, 2013) (Reid & Harrigan, 2013) (Barber, Boyen, Shi, & Uzun, 2012)

**Cardano (ADA):**

Cardano ADA is a new digital cryptocurrency. It was developed by Charles Hoskinson and was launched in late 2017. In addition to transferring funds digitally, plans are to build a platform that can also run financial applications and smart contracts. It aims at promoting financial inclusion by balancing privacy with regulation. (Guides, 2018e)

**Litecoin (LTC):**

Litecoin is a peer-to-peer decentralized, open-source cryptocurrency created as a fork from bitcoin. (Gibbs & Yordchim, 2014) It offers several key differences especially in areas of payment pattern and payment behavior from Bitcoin. (Haferkorn & Quintana Diaz, 2015) The network claims to process settlement goals quicker than Bitcoin by processing a block every 2.5 minutes rather than 10 minutes.

**NEM**

Nem is a peer-to-peer platform that is looking to help companies and industries improve things like online payments, logistics, and messaging. It provides an alternative for API developers that are looking to develop blockchain-based apps. (Guides, 2018b) As NEM is a blockchain notarization, it makes NEM become the first public/private blockchain combination. (A'fifah, Ritahani, & Ahmad, 2018)

**Stellar (XLM):**

Stellar is a cryptocurrency platform that aims to make swift payments with very low fees, has an eye on the way money

is moved by people, banks, and through payment networks. It was co-founded by Jed McCaleb through the Stellar Foundation and is around since 2014. It was created as a fork of Ripple protocol. Its currency is called lumens and is now the 5th largest coin in the market. It requires a short confirmation time of 3 to 5 seconds and supports thousands of transactions in a second. (Hazar & Yilmaz, 2018) (Guides, 2018d) (Farell, 2015) (Iris, n.d.; "Stellar News," n.d.)

**NEO**

NEO is a decentralized, open-source blockchain crypto technology. It was launched in China in 2014 and is seen by many as the Chinese version of Ethereum. NEO is not entirely a cryptocurrency. It, along with the NEO coins also has a crypto token called Gas. It facilitates the development of easily movable digital assets, safe digital identity and smart contracts. (Lehner, Hunzeker, & Ziegler, 2017) (Van Den Broek, 2018) (Guides, 2018c; Van Den Broek, 2018) (Smith, 2018)

**IOTA (MIOTA):**

The primary communication form that occurs on the internet is human-human. However, with newer ways of identification, developing objects will eventually get connected. It is estimated that by 2020 as many as 20 billion physical objects will be connected to internet. The forms of communication will then encompass human to human, human to things and things to things through the internet. (Lu Tan & Neng Wang, 2010) This abetting of connected devices explains the Internet of Things Application. Hence Internet of Things Application is molding things, which formerly were blind and mute, talk, hear, and even think. (Ouaddah, AbouElkalam, & AitOuahman, 2016) As these connections increase exponentially to billions, so will the number of micropayments and IOTA claims to deliver this without fees. (Smith, 2018) The use of a blockchain-IoT combination will be powerful and it is predicted to cause significant transformations across several industries, paving the way for new business models and novel, distributed applications. (Conoscenti, Vetro, & De Martin, 2016) (Christidis & Devetsikiotis, 2016)

**Dash (DASH):**

Dash is one of the first attempts to provide privacy-focused cryptocurrency. It was launched in 2014 and is similar to bitcoin. It anonymizes the transaction process by mixing coins. Its market shares have risen significantly since 2017. It is intended for use by people to buy goods and services. Its block rewards are equally shared between miners and 'masternodes'. Only 10% of revenues go to the treasury. (Hileman & Rauchs, 2017; Smith, 2018; Sun, Au, Liu, & Yuen, 2017)

**Monero (XMR)**

Monero is a privacy-centric anonymous cryptocurrency that uses Ring confidential Transaction (RingCT) protocol. It has high levels of anonymity and hence provides good user privacy. It is popular on the dark web. It allows users to obscure their transaction graph by including chaff coins, called "mixins," along with the actual coins they spend. (Sun et al., 2017) (Miller, Mo ser, Lee, & Narayanan, 2017)

**Mintchip:**

MintChip is dubbed as Canada's cryptocurrency as it was created by the Royal Canadian Mint a government agency. It is supported by Canadian dollars. It is a smartcard chip system launched in 2012. The card stored electronic value and the system allowed transfers of value across cards. It was later sold to a private loyalty and payments company, nanoPay Corp., ("Royal Canadian Mint's digital cash platform 'MintChip' sold to Toronto payments company nanoPay," 2016) (Hazar & Yilmaz, 2018) (Mas, 2015)

**TRON (TRX):**

TRON is a blockchain-based decentralized protocol. It was founded by Justin Sun and it primarily aims to make entertainment available to masses around the globe. It is also called as the Bitcoin of China as the CEO of TRON is Chinese. (TradingStrategyguides, 2018) (Kaplan et al., 2018)

**EOS:**

EOS cryptocurrency was launched in 2017 that supports the effortless creation of decentralized Apps. This new cryptocurrency has gained attention and is one of the largest coins in the market. (Guides, 2018a) (Risberg, 2019)

**2. Discussion and Conclusion**

In the long history of human coins (Howgego, 2002) (Kagan, 1982), CC is in its infancy. Furthermore, CC is digital and holds no inherent value. (Barnes, 2018). They are characterized by exponential price spikes and explosivity. (Bouri, Shahzad, & Roubaud, 2018). Research on CC is generally restricted to single CCs. Moreover, research on technological advancement in CCs, minimal accountability and disclosure requirements and its effects on cryptocurrency manipulation, government participation in market regulation as well as their possible impact if intertwined with real economy still remains unknown. (A'fifah et al., 2018) (Barnes, 2018) Though a cautious approach towards the use of CCs is recommended a rise in the use and the number of CCs is expected.

**References**

- [1] Abbasi, A., Chen, H., & Salem, A. (2008). Sentiment analysis in multiple languages: Feature selection for opinion classification in Web forums. *ACM Transactions on Information and System Security*, 26 (3), 1–34.
- [2] A'fifah, A., Ritahani, A., & Ahmad, A. (2018). Comparative Performance of Deep Learning and Machine Learning Algorithms on Imbalanced Handwritten Data. *International Journal of Advanced Computer Science and Applications*, 9 (2). <https://doi.org/10.14569/ijacsa.2018.090236>
- [3] Armknecht, F., Karame, G. O., Mandal, A., Youssef, F., & Zenner, E. (2015). Ripple: Overview and Outlook. In M. Conti, M. Schunter, & I. Askoxylakis (Eds.), *Trust and Trustworthy Computing* (Vol. 9229, pp. 163–180). Cham: Springer International Publishing.
- [4] Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to Better — How to Make Bitcoin a Better

- Currency. In A. D. Keromytis (Ed.), *Financial Cryptography and Data Security* (Vol. 7397, pp. 399–414). Berlin, Heidelberg: Springer Berlin Heidelberg.
- [5] Barnes, P. (2018). Cryptocurrency and its susceptibility to speculative bubbles, manipulation, scams and fraud. Retrieved from <https://mpr.ub.uni-muenchen.de/90241/>
- [6] Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *The Journal of Economic Perspectives: A Journal of the American Economic Association*, 29 (2), 213–238.
- [7] Bouri, E., Shahzad, S. J. H., & Roubaud, D. (2018). Co-explosivity in the cryptocurrency market. *Finance Research Letters*. <https://doi.org/10.1016/j.frl.2018.07.005>
- [8] Chohan, U. (2017). Cryptocurrencies: A Brief Thematic Review. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3024330>
- [9] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4, 2292–2303.
- [10] Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. In 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA) (pp. 1–6). Agadir, Morocco: IEEE.
- [11] Decker, C., & Wattenhofer, R. (2013). Information propagation in the Bitcoin network. In *IEEE P2P 2013 Proceedings* (pp. 1–10). Trento, Italy: IEEE.
- [12] Drainville, D. (2012, December 21). An Analysis of the Bitcoin Electronic Cash System. Retrieved January 26, 2019, from <https://pdfs.semanticscholar.org/f7e3/3271bc73b1ae8501aa3776f9fb72695edffe.pdf>
- [13] Easley, D., O'Hara, M., & Basu, S. (2017). From Mining to Markets: the Evolution of Bitcoin Transaction Fees. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3055380>
- [14] Ethereum Project. (n.d.). Retrieved December 30, 2018, from <https://www.ethereum.org/>
- [15] Fanning, K., & Centers, D. P. (2016). Blockchain and Its Coming Impact on Financial Services. *Journal of Corporate Accounting & Finance*, 27 (5), 53–57.
- [16] Farrell, R. (2015). An Analysis of the Cryptocurrency Industry. Wharton school, University of Pennsylvania. Retrieved from [https://repository.upenn.edu/wharton\\_research\\_scholars/130](https://repository.upenn.edu/wharton_research_scholars/130)
- [17] Fernández-Villaverde, J. (2018). Cryptocurrencies: A Crash Course in Digital Monetary Economics. *The Australian Economic Review / Institute of Applied Economic Research*, 51 (4), 514–526.
- [18] Gandal, N., & Halaburda, H. (2016). Can We Predict the Winner in a Market with Network Effects? Competition in Cryptocurrency Market. *Games*, 7 (3), 16.
- [19] Gibbs, T., & Yordchim, S. (2014). Thai Perception on Litecoin Value. *International Journal of Economics and Management Engineering*, 8 (8), 2634–2636.
- [20] Guides, T. S. (2018a). EOS Cryptocurrency Trading Strategy – Turtle Soup Pattern. Retrieved from

- <https://tradingstrategyguides.com/eos-cryptocurrency-trading-strategy/>
- [21] Guides, T. S. (2018b). Nem (XEM) Cryptocurrency Strategy – Momentum Pinball Setup. Retrieved from <https://tradingstrategyguides.com/nem-xem-cryptocurrency-strategy/>
- [22] Guides, T. S. (2018c). NEO Cryptocurrency Strategy – Scalping with BB and AO. Retrieved from <https://tradingstrategyguides.com/neo-cryptocurrency-strategy/>
- [23] Guides, T. S. (2018d). Stellar Cryptocurrency Strategy – The Future of Banking. Retrieved from <https://tradingstrategyguides.com/stellar-cryptocurrency-strategy/>
- [24] Guides, T. S. (2018e). Why Cardano ADA Deserves your Attention – Cardano Cryptocurrency Strategy. Retrieved from <https://tradingstrategyguides.com/cardano-cryptocurrency-strategy/>
- [25] Haferkorn, M., & Quintana Diaz, J. M. (2015). Seasonality and Interconnectivity Within Cryptocurrencies - An Analysis on the Basis of Bitcoin, Litecoin and Namecoin. In A. Lugmayr (Ed.), *Enterprise Applications and Services in the Finance Industry* (Vol. 217, pp. 106–120). Cham: Springer International Publishing.
- [26] Hazar, H. B., & Yilmaz, N. K. (2018). Predicting future cryptocurrency investment trends by conjoint analysis. *Pressacademia*, 5 (4), 321–330.
- [27] Hileman, G., & Rauchs, M. (2017). Global Cryptocurrency Benchmarking Study. Retrieved January 26, 2019, from <https://cdn.crowdfundinsider.com/wp-content/uploads/2017/04/Global-Cryptocurrency-Benchmarking-Study.pdf>
- [28] Iris. (n.d.). Stellar - Develop the world's new financial system. Retrieved January 5, 2019, from <https://www.stellar.org/>
- [29] Kaplan, C., Aslan, C., & Bulbul, A. (2018). Cryptocurrency Word-of-Mouth Analysis via Twitter. In II. International Conference on Theoretical and Applied Computer Science and Engineering 2018-Summer. Retrieved from <http://dx.doi.org/>
- [30] Kim, Y. B., Kim, J. G., Kim, W., Im, J. H., Kim, T. H., Kang, S. J., & Kim, C. H. (2016). Predicting Fluctuations in Cryptocurrency Transactions Based on User Comments and Replies. *PloS One*, 11 (8), e0161197.
- [31] Lansky, J. (2018). Possible State Approaches to Cryptocurrencies. *Journal of Systems Integration*, 9 (1), 19–31.
- [32] Lehner, E., Hunzeker, D., & Ziegler, J. R. (2017). Funding Science with Science: Cryptocurrency and Independent Scientific Funding. *The Journal of Cryptocurrency and Blockchain Technology Research*. Retrieved from [https://academicworks.cuny.edu/bx\\_pubs/21](https://academicworks.cuny.edu/bx_pubs/21)
- [33] Lu Tan, & Neng Wang. (2010). Future internet: The Internet of Things. In 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE) (pp. V5–V376 – V5–V380). Chengdu, China: IEEE.
- [34] Mas, I. (2015). Strains of Digital Money. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.1728125>
- [35] Mathis, T. (2018). *Ethereum: Your Guide To Understanding Ethereum, Blockchain, and Cryptocurrency*. Level Up Lifestyle Limited.
- [36] Miller, A., Moser, M., Lee, K., & Narayanan, A. (2017, April 13). An Empirical Analysis of Linkability in the MoneroBlockchain. Retrieved January 26, 2019, from <https://maltemoeser.de/paper/monerolink.pdf>
- [37] Moore, T., & Christin, N. (2013). Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. In A.-R. Sadeghi (Ed.), *Financial Cryptography and Data Security* (Vol. 7859, pp. 25–33). Berlin, Heidelberg: Springer Berlin Heidelberg.
- [38] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.
- [39] Ouaddah, A., AbouElkalam, A., & AitOuahman, A. (2016). FairAccess: a new Blockchain-based access control framework for the Internet of Things: FairAccess: a new access control framework for IoT. *Security and Communication Networks*, 9 (18), 5943–5964.
- [40] Peck, M. (2016). A blockchain currency that beat bitcoin on privacy [News]. *IEEE Spectrum*, 53 (12), 11–13.
- [41] Popuri, M. K., & Gunes, M. H. (2016). Empirical Analysis of Crypto Currencies. In H. Cherifi, B. Gonçalves, R. Menezes, & R. Sinatra (Eds.), *Complex Networks VII* (Vol. 644, pp. 281–292). Cham: Springer International Publishing.
- [42] Privacy-protecting digital currency | Zcash. (n.d.). Retrieved November 17, 2018, from <https://z.cash/>
- [43] Reid, F., & Harrigan, M. (2013). An Analysis of Anonymity in the Bitcoin System. In Y. Altshuler, Y. Elovici, A. B. Cremers, N. Aharony, & A. Pentland (Eds.), *Security and Privacy in Social Networks* (pp. 197–223). New York, NY: Springer New York.
- [44] Risberg, J. (2019, January 14). What Is EOS? | Everything You Should Know. Retrieved January 26, 2019, from <https://coincentral.com/what-is-eos/>
- [45] Royal Canadian Mint's digital cash platform "MintChip" sold to Toronto payments company nanoPay. (2016, January 12). Retrieved January 26, 2019, from <https://business.financialpost.com/news/economy/royal-canadian-mints-digital-cash-platform-mintchip-sold-to-toronto-payments-company-nanopay>
- [46] Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. In 2014 IEEE Symposium on Security and Privacy (pp. 459–474). San Jose, CA: IEEE.
- [47] Singh, S., Suguna, R., Satish, D., & Mv, R. K. (2018). Survey on Surging Technology: Cryptocurrency. *International Journal of Engineering & Technology*, 7 (3.12), 296.
- [48] Smith, K. A. (2018, August 30). 13 Types Of Cryptocurrency That Aren't Bitcoin | Bankrate.com. Retrieved January 5, 2019, from

<https://www.bankrate.com/investing/types-of-cryptocurrency/>

- [49] Sovbetov, Y. (2018). Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, Litecoin, and Monero. *Journal of Economics and Financial Analysis*, 2 (2), 1–27.
- [50] Stellar News. (n.d.). Retrieved January 5, 2019, from <https://cointelegraph.com/tags/stellar>
- [51] Sun, S.-F., Au, M. H., Liu, J. K., & Yuen, T. H. (2017). RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero. In *Computer Security – ESORICS 2017* (pp. 456–474). Springer, Cham.
- [52] Trading Strategy guides. (2018, May 2). TRON the new Bitcoin of China – Tron TRX Cryptocurrency Strategy. Retrieved January 26, 2019, from <https://tradingstrategyguides.com/tron-trx-cryptocurrency-strategy/>
- [53] Van Den Broek, L. (2018). Cointegration-based pairs trading framework with application to the Cryptocurrency market (Bachelor General Economics). (Z. Sharif, Ed.). Erasmus University Rotterdam. Retrieved from <https://thesis.eur.nl/pub/43392/Broek-L.-vd-4037271b-.pdf>
- [54] Wilmoth, J. (2019, January 21). Bitcoin Price Could Crack \$10 Million, Become New Gold Standard: Asset Management Firm. Retrieved January 27, 2019, from <https://www.ccn.com/bitcoin-price-could-crack-10-million-become-new-gold-standard-asset-management-firm/>
- [55] Wu, K., Wheatley, S., & Sornette, D. (2018). Classification of cryptocurrency coins and tokens by the dynamics of their market capitalizations. *Royal Society Open Science*, 5 (9), 180381.
- [56] Zhong, M. (2002). A faster single-term divisible electronic cash: ZCash. *Electronic Commerce Research and Applications*, 1 (3-4), 331–338.