|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
|  |  |  | |  |
| Business Report ON MONERO | | |
| MINH DUC DINH NGUYEN – 103502978  DATE: | | FIN20016 – ETHICS AND INTERNATIONAL FINANCE |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
|  |  |  | |  | |
|  | 1. EXECUTIVE SUMMARY   This report will focus and analyze a cryptocurrency with enhanced aninomity feature known as Monero. Monero, unlike other cryptocurrencies, comes with a privacy-centric protocol that protects users in their transactions. Despite paling in value in comparison to mainstream cryptocurrencies such as Bitcoin and Ethereum, Monero has proven itself to be a promising currency for privacy-centric users. | |  | |

|  |  |
| --- | --- |
|  |  |
| INTRODUCTION Cryptocurrency is a system that issues tokens which are meant to be used as a general medium of exchange and maintained by a digital ledger (Pernice & Scott 2021). The “crypto” in the name stands for cryptography, which provides currencies such at Bitcoins cryptographic proofs for verifiability purposes (Pernice & Scott 2021). The “currency” nature of cryptocurrencies was a controversial issue, as it implies the tokens are money tokens (Pernice & Scott 2021).  With a baseline understanding of cryptocurrencies, this report seeks to provide an overview of an emerging cryptocurrency known as Monero to provide not only financial and statistics to enhance understanding of the currency’s position in the market; but also to introduce and explain new ethical and legal dilemmas relating to Monero’s privacy-centric features. | |

|  |  |
| --- | --- |
|  |  |
| Information about moneroThe reason why cryptocurrencies are favored over traditional centralized currency system such as the cash market is due to its decentralized nature, which allows parties to trade trade with each other without the intervention of a third party. Transactions are done using the the Blockchain, which is a public ledger with all participants in a collective system (Li et al. 2021, p.69), and all cryptocurrencies follow this mechanism to enable transactions. However, the public nature of the Blockchain enables a crucial privacy flaw in most cryptocurrencies, which is that external parties can view all transactions of other parties with the right identifier, for example: a blockchain explorer known as Blockchain.com; which allows all users to see all transactions and mining activities that occur within the blockchain (Blockchain.com n.d.), which would deter privacy-focused shareholders from engaging in crypto trading activities.  Monero (XMR) was created as an open-source, decentralized cryptocurrency with a prime focus on privacy and anonymity, launching in 2014 (Li et al. 2021. P.679). Monero differs from other cryptocurrencies based on a protocol known as the CryptoNote, which allows senders and recipient to mask the transaction by generating a new stealth address for senders and delivering the address to the recipient through a one-time generated destination address for recipients (Clack & Courtois 2019, p.31).    *Figure 1: The principle of CryptoNote*  The inherent problem with Monero is that its key feature regarding anonymity opens up legal dilemmas as criminal elements can exploit the currency to perform money laundering or any other illegal financial activities. Since Monero obfuscates any transaction with the given CryptoNote protocol above, investigation of any financial activity into Monero transactions proves difficult to perform. (Li et al, p.679). This would require creators of this currency to implement a seemingly oxymoronic solution of implementing traceable anonymity features into Monero, which will be detailed in Section 7. | |

|  |  |
| --- | --- |
|  |  |
| HIstorical data and company performance This report will utilize Coinmarketcap to provide insights regarding the historical data of Monero since its introduction so as to have a better overview of the currency’s performance. This report will utilize the period between 2020-2022 as the cryptocurrency market experiences wild fluctuations during this period due to COVID-19 outbreak. (Hong & Yoon 2022, p.1). From an overall view of Monero during the given period, the lowest price Monero experienced during this period was on 17th March 2020 at the price of $36.22, and in a span of one year and two months Monero experienced a wild fluctuation that would reach an all-time peak on 9th May 2021 at price $483.58 (CoinMarketCap n.d.), which would net a total increase of 1335.12% in just a span of one year. But just within ten days on 19th May 2021, the currency dropped to $200.03, resulting in a freefall of over 41.36% in just ten days (CoinMarketCap n.d.). As of the time of writing, the currency has dropped to only $140.49 and has only reached over $300 in value 4 subsequent times after the aforementioned drop from all-time peak. The current market cap for Monero in 2022 is also at the $2.7 billion figure, making Monero the 28th largest bitcoin regarding market cap. (CoinMarketCap n.d.) | |



*Figure 2: Performance of Monero during 2020-2022 period.*

# aNALYSIS AND TREND OF DATA

As previously stated in the aforementioned section, Monero peaked at price $483.58, which is explainable by United States’ president Joe Biden’s proposed tax plan for crypto transaction in 2021, which involves any crypto transaction over $10,000 USD to be reported to the tax office (Steven 2021). With this newly proposed tax plan and the lack of privacy present in most other cryptocurrencies, investors swapped to Monero as a mean to minimize the taxation effect caused by the new tax plan. Since Monero’s key features lies in its privacy, users could conduct transactions without said transaction ever written into a crypto ledger, therefore minimizing transfer amount and tax effect. In the whitepaper published by Saberhagen regarding Monero in 2013, the CryptoNote protocol easily outclasses the drawbacks of mainstream cryptocurrencies such as Bitcoin. The privacy feature of Monero also provides comfort for privacy-conscious users. According to a study conducted by Pew Research Center, 81% of U.S. adults feel that they have little control over data collected by them from companies (Auxier et al. 2019). Therefore, the untraceability of Monero through CryptoNote satisfies the concerns of these stakeholders.

After reaching all-time peak, it appears that investors became bearish, and withdrew investment from the coin, resulting in a 41% drop from all-time peak. Inflation also played a major role during the period concerning Monero. According to data collected from the U.S Bureau of Labor Statistics and analyzed through Power BI tool, the median consumer purchase index (CPI) of the United States went from 259.89 to 272.35 (U.S Bureau of Labor Statistics 2022), Which would result in inflation of 2020 being roughly 1% and 2021 being 5.2%, which results in a net increase of 4.2% in inflation rate during 2020-2021 period, which drastically decreases consumer purchasing power. As the U.S. consumer purchasing power decreased, it resulted in a net decrease of trust in the securities of the cash market internationally.

Chart, line chart

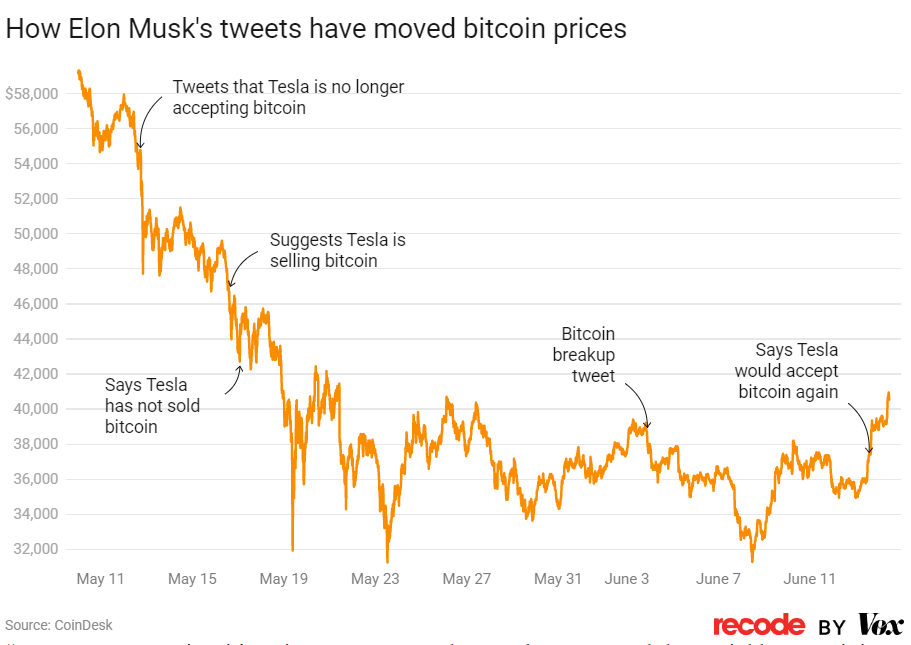
Description automatically generated

*Figure 3: The U.S. dollar inflation rate 2012-2022*

Monero suffered a fall from its peak to the current value of $148.29 could be explained by the impact of Bitcoin in 2022. After the harsh fall of Bitcoin from its $66,971 peak from November 2021 to around $20,000 for Bitcoin in June 2022 (CoinMarketCap n.d.), and the fall of Dogecoin; general trust in the security of the cryptocurrency market dropped, but there are still traders who still believe in the security of Bitcoin. As of the time of writing, the market is still remaining resilient with Bitcoin floating over the $20,000 level, which regains investors’ trusts, and lower trust in “altcoins” – a term referring to any cryptocurrency other than Bitcoin (Frankenfield 2022), which leads to the fall in Monero’s performance.

# Market performance and competitiveness in the markets

During the period between 2020 to 2022, the cryptocurrency market has experienced massive fluctuations regarding its performance, and draws the attention of major financial institutes and key shareholders of the cash market. Despite its rapid increase in market capitalization, the cryptocurrency market has proven itself to be quite fragile, as exemplified by how a single tweet from billionaire Elon Musk caused the fall of Bitcoin. In graphics produced by Molla (2021), a single tweet from Elon Musk about the breakup of Bitcoin caused the currency to immediately drop by 5%, which also drops investors’ trust in the entire market.

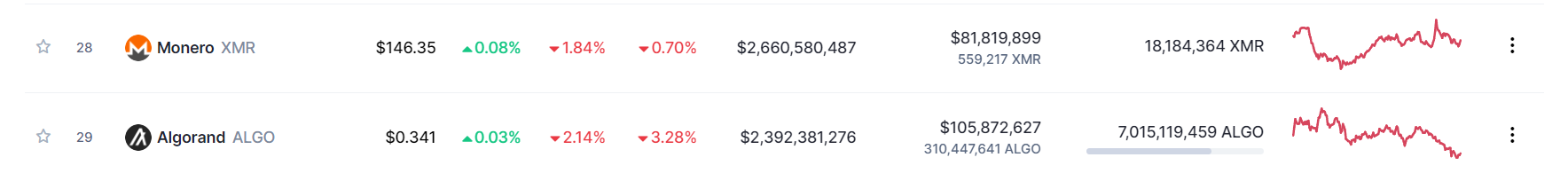


*Figure 4: How Elon Musk’s tweets have moved bitcoin prices*

This wild fluctuation in the cryptocurrency market drastically affects Monero, as its performance hinges on the market capitalization of Bitcoin to succeed. As Monero belongs to the altcoin umbrella, its creation comes from developers leaving to create new coins which seeks to improve upon perceived limitations of Bitcoin, which is its user privacy (Frankenfield 2022). Therefore, as an open-source fork of Bitcoin, the performance of Monero performs as a parallel to Bitcoin. When confidence in Bitcoin and the cryptocurrency drops, the performance and market capitalization of Monero also drops.

As of the time of writing, Monero currently stands as the 28thrd largest coin in the cryptocurrency market with a market capitalization of $2.49 billion USD, which is higher than Algorand, another altcoin with approximately $2.394 billion USD in market cap (CoinMarketCap n.d.). Although not high in market capitalization, Monero’s advantage of anonymity appeals to investors who have gotten past Bitcoin and are looking for serious investments in the cryptocurrency market.

The table below illustrates Monero and its competitors’ change in price during the last 7 days. (CoinMarketCap n.d.) Monero’s change in price during the last 24 hours and the last 7 days performs better than that of Alogrand at -1.84% and -0.7% respectively, compared to Algorand’s -2.14% drop during the last 24 hours and -3.28% during the last 7 days. The performance chart of Monero and Algorand appears to have an inverse relationship, which could be deduced that investors are pulling away from Algorand in favor of Monero.



*Figure 5: Monero’s performance against Algorand*

For seasoned crypto investors that has operational security concerns, Monero proves to be the most viable choice as its market capitalization sits on the top of privacy-preserving altcoins (Wijaya et al. 2019, p. 621). It seems to be heavily affected by the recent Bitcoin bubble crash which leads to the crash of the cryptocurrency market, but future prospects for the coin remains positive.

# future prospects and recommendation

As users become more concerned about Opsec and data privacy, more and more financial investors are looking forward to Monero to trade. But with the significantly volatile nature of the market, Monero is facing a challenging future as Bitcoin’s performance will impact the performance of the entire market.

As stated in section 3, the anonymity feature of Monero functions as more a double-sided blade as illegal financial users are using the currency to circulate illegal money and conduct cyberattacks on the digital space (Li et al. 2021, p. 679). A notable example of this came from the Colonial Pipeline ransom where hackers breached the Colonial Pipeline and held ransom, demanding payment in Monero (Turton & Mehrotra 2021). The risk that Monero poses to the circulation of the cryptocurrency market demands that a seemingly backwards feature to be implemented into the currency, which involves a traceable solution to the coin where tracing authorities are responsible for tracing payer in dubious transactions with his private key (Li et al. 2021, p.681).

Another future concern regarding Monero is that it is an energy-consuming coin to mine. According to Li et al. (2019), Monero mining uses approximately 645.62 GWh to mine and emits a carbon intensity of 0.63 – 0.64 kg of CO2.KWh, which could result in over 19.42 thousand tons of carbon dioxide being emitted. If mining efficiency of Monero does not improve in the near future, the environment will take the fall for Monero’s inefficiencies.

Overall, with the volatility in the cryptocurrency market, it would be difficult to recommend investors to trade in Monero. It would be more rational for investors to collect more data regarding Monero’s and the cryptocurrency markets’ performance in the future, as well as the shifting consciousness of stakeholders regarding privacy concerns.

# Conclusion

Monero is one of the pioneers of the cryptocurrency market that prioritizes anonymity for its traders, therefore attracting interest of privacy-conscious stakeholders. Despite having a less than favorable position in the market, future prospects of the coin seems to be promising as modern traders are getting increasingly more concern about the security of their data. Monero still comes with problems regarding illegal circulation and Its high energy consumption, and given the volatile nature of the cryptocurrency market, Monero cannot be recommended to prospective investors at this current moment.

# Reference List

Auxier, B, Rainie, L, Anderson, M, Perrin, A, Kumar, M & Turner, E 2019, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, viewed 8 October 2022, <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

Blockchain.com n.d., *Blockchain Explorer | BTC | ETH | BCH*, Blockchain.com, viewed 2 October 2022, <https://www.blockchain.com/explorer>.

Clack, CD & Courtois, NT 2019, *Distributed Ledger Privacy: Ring Signatures, Möbius and CryptoNote,* Cornell University, pp. 1–47.

CoinMarketCap n.d., *Monero*, coinmarketcap.com, viewed 2 October 2022, <https://coinmarketcap.com/currencies/monero/>.

Frankenfield, J 2022, *Altcoin Explained: Pros and Cons, Types, and Future*, Investopedia, viewed 7 October 2022, <https://www.investopedia.com/terms/a/altcoin.asp#:~:text=Altcoins%20are%20generally%20defined%20as>.

freepik n.d., *Stack of silver coins with monero symbol isolated on white background*., freepik.com, viewed 2 October 2022, <https://www.freepik.com/free-vector/stack-silver-coins-with-monero-symbol-isolated-white-background\_8801369.htm#query=monero&position=33&from\_view=keyword>.

Hong, MY & Yoon, JW 2022, ‘The impact of COVID-19 on cryptocurrency markets: A network analysis based on mutual information’, in AF Bariviera (ed.), *PLOS ONE*, vol. 17, no. 2, p. e0259869.

Li, J, Li, N, Peng, J, Cui, H & Wu, Z 2019, ‘Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies’, *Energy*, vol. 168, pp. 160–168.

Li, Y, Yang, G, Susilo, W, Yu, Y, Au, MH & Liu, D 2021, ‘Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability’, *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 679–691.

Molla, R 2021, *When Elon Musk tweets, crypto prices move*, Vox, viewed 7 October 2022, <https://www.vox.com/recode/2021/5/18/22441831/elon-musk-bitcoin-dogecoin-crypto-prices-tesla>.

Pernice, IGA & Scott, B 2021, ‘Cryptocurrency’, *Internet Policy Review*, vol. 10, no. 2, pp. 1–9.

Saberhagen, N van 2013, *CryptoNote v 2.0*, GitHub, pp. 1–15, viewed 8 October 2022, <https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf>.

Stevens, R 2021, *Privacy Coin Monero Rises 30% After Biden Reveals Tax Plans for Crypto Transactions*, Decrypt, viewed 3 October 2022, <https://decrypt.co/71616/privacy-coin-monero-rises-30-after-biden-reveals-tax-plans-crypto-transactions>.

Turton, W & Mehrotra, K 2021, *Hackers Breached Colonial Pipeline Using Compromised Password*, Bloomberg, viewed 8 October 2022, <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>.

U.S Bureau of Labor Statistics 2022, “All items in U.S. city average, all urban consumers, not seasonally adjusted”, U.S Bureau of Labor Statistics, <https://data.bls.gov/cgi-bin/surveymost>

Wijaya, DA, Liu, JK, Steinfeld, R, Liu, D & Yu, J 2019, ‘On The Unforkability of Monero’, P*roceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, pp. 621–632.