Bitcoin: The Newest Form of Money

Shayan Mollahassani, Dario Tao, Lana Tang

ECO349: Money, Banking, and Financial Markets

Faculty of Arts and Science, Department of Economics, University of Toronto

Abstract:

As a relatively new retail payment instrument, Bitcoin is now considered the most popular decentralized cryptocurrency around the globe. A better understanding of this digital currency is necessary to help evaluate whether or not central banks should introduce their own electronic retail payment instrument. A variety of sources were used to gather the information within this report. This list includes news articles, web articles, textbooks, research studies, textbooks, the Bitcoin user agreement, and a literature review. Bitcoin logistics, including the pros and cons of using this cryptocurrency, are examined in this report. In conclusion, central banks should issue a regulated CBDC to regulate an unregulated market.

Section 1: Introduction to Bitcoin

Bitcoin is a cryptocurrency; a digital currency that relies on decentralized blockchain technology. This technology acts as a communal ledger that records all transactions in chronological order. Asymmetric cryptography is used to ensure each Bitcoin has a unique public key and an associated private key, both of which are stored in a database known as a Bitcoin wallet. To successfully add a transaction to the blockchain, the digital signature, private key, and the public key must match. As well, within a transaction, a Bitcoin address acts as a digital fingerprint of the recipient's address.[1] To extract Bitcoins, computer algorithms solve a complex mathematical puzzle, also known as a hashing puzzle.

This currency operates autonomously, free from the influence of any central control system such as financial institutions or government organizations. However, governments have been implementing policies and regulations to protect those Bitcoin users. Bitcoin, unlike fiat currency, offers users a certain amount of anonymity; Bitcoin addresses do not necessarily have to be linked with personal information.[2]

Its value comes from scarcity, as there can only be a maximum of 21 million Bitcoins in existence.[3] Meanwhile, Bitcoin price fluctuations are based on supply and demand. Since it is currently the most popular cryptocurrency, many third party vendors are now accepting Bitcoin as a form of accepted currency.

---

[1] The logistics of how Bitcoin operates and is transacted is listed in detail in Antonopoulous (2017).
[2] Acuant (2020) highlights how users have an additional degree of anonymity when using Bitcoin.
[3] Hayes (2021) reflects on the scarcity of Bitcoin and what happens after all 21 million are mined.

Section 2: Bitcoin Terms & Conditions

Below, is a list of economically important terms and conditions for Bitcoin:

1. Compliance with Applicable Law (2)

Many governmental authorities are now taking legal precautions against Bitcoin in the form of increased laws and regulations. This will decrease Bitcoin usage and adoption rate in the countries where there are excessive laws pertaining to the use of this cryptocurrency.

2. Risk of Digital Assets (4)

This clause warns consumers that Bitcoin is an extremely volatile cryptocurrency. The price of Bitcoin constantly changes depending on demand and supply. Therefore, Bitcoin scares off investors who are risk averse and thus, decreases their adoption rate.

3. Limitation of Liability (6.3)

As Bitcoin is a digital currency, there are possible issues that arise such as network failure, hackers, government policy changes, and more. This poses a large risk to investors, as they are not liable for any monetary compensation in the case of these unexpected events.

4. Dispute Resolution (8)

This term forces users to sign away their rights to a jury and to participate in a class action lawsuit. By only entertaining individual lawsuits, this decreases Bitcoin's liability in terms of payout. One individual versus Bitcoin will decrease the chances of the sole individual winning the case, and in the case of winning, decrease the overall payout that is owed to them.[4]

Section 3: Consumer and Retailer Costs & Benefits of using Bitcoin

[4] The outlined terms and agreements found in Bitcoin's User Agreement, last updated March 9, 2021.

When exploring a new frontier like Bitcoin, there are often unknown dangers, coupled with substantial incentives and advantages. To both individual consumers and retailers, it is apparent that Bitcoin's advantage lies within the fact that it is a decentralized currency with low fraud risk and high transparency, while also being fast and inexpensive.[5] To begin, the transaction costs associated with moving money across the world using banks are immense; as Bitcoin has no geographical limitations, investors can trade Bitcoin from any place and time with minor costs and no restrictions. The lack of restrictions is attributable to the decentralized issuance of Bitcoin disallowing it from being valued, created, regulated, and distributed by the government and central bank. Moreover, using blockchain technology, confidential information is not disclosed and transparency is guaranteed by allowing consumers to conduct trades at any given time[6].

To retail institutions, the rising notoriety of Bitcoin represents an incentive to penetrate a new market—demographic groups with a high level of technology that value transparency. Bitcoin's extraordinary performance over the past few years has led to many companies viewing it as an investable asset that could potentially be a balancing asset to cash without the drawdown of inflation.[7]

For both individual investors and retail institutions, Bitcoin's advantages are often also its most significant costs/risks. For instance, while the lack of government regulation provides freedom to users, it is also one of the biggest downsides of the currency because different cryptocurrency laws and low buyer protection see users susceptible to fraud. Moreover, consumers and retailers alike put extensive consideration to the substantial volatility risks associated with Bitcoin such as built-in deflation and lack of a valuation guarantee. As the number of Bitcoins cannot exceed 21 million, the market for this currency is heavily demand-based and can see large fluctuations in its valuation from users collectively dumping and buying currency collectively.[8] Lastly, as Bitcoin uses relatively new and advanced technology, there are many counterparty risks involved that could potentially lead to heavy losses such as a system malfunction causing one to lose their entire wallet. As stated

[5] Abramova (2016) Appendix table 1 lists benefits of BTC, table 2 lists risks of BTC
[6] Kulkarni (2021) details the pros and cons of Bitcoin
[7] Deloitte (2021) business benefit of using cryptocurrency and a study regarding new demographic access
[8] Bambrough(2021) Forbes article indicating BTC prices dropped 15% from a dump

by Abramova (2016) " ...bitcoins might be lost due to users' inadvertence, such as typos in the transaction, forgotten passwords or security flaws of devices used".[9] Considering all of the costs and benefits in a relatively speculative market, consumers and retail institutions must decide whether or not to use Bitcoin as a payment instrument that best suits their risk profile and needs.

Section 4: Bitcoin and the Three Functions of Money

According to Mishkin and Serletis (2020), for something to be considered money, it must satisfy three primary functions in an economy. It must be: a medium of exchange, a unit of account, and be a store of value.

Bitcoin has shown potential to be used as a medium of exchange, defined as money used to pay for goods and services. An increasing number of companies now accept Bitcoin as a form of payment, and many more have plans to accept the cryptocurrency in the future.[10] Bitcoin is also immediately transferable from one account to another, therefore is economically efficient and also minimizes time spent in exchanging goods and services, a feature of money listed by Mishkin and Serletis (2020). However, a study conducted in 2018 by Baur et al. found that around a third of Bitcoins are held by investors who only receive, but never send Bitcoins to others. Only a small portion of Bitcoins appear to be used as a medium of exchange. They conclude that Bitcoins are mainly held for investment purposes, rather than being used as a medium of exchange.

In terms of being a unit of account, meaning money used to measure value of goods in an economy, Bitcoin has struggled due to its volatility.[11] Yermack (2015) proposed that the bitcoin-dollar exchange rate volatility was too high to be used as a unit of account. He found that the exchange rate volatility of Bitcoin in 2013 was 142%, while exchange rate volatility of other currencies lie around 7% to 12% in the same year. In comparison, Gold's exchange rate volatility in the same year was 22%. If Bitcoin were used, businesses would have to adjust prices hourly. This is because the exchange rate between Bitcoin and today's popular fiat currencies is constantly

[9] Abramova (2016) explanation of the risks of BTC in table 2 appendix
[10] Companies that now accept Bitcoin include Paypal, Xbox, and Coca-Cola Amatil.
[11] The definition of unit of account according to Mishkin and Serletis (2020).

changing. Constantly recalculating prices is costly for businesses. This issue would only subside if Bitcoin was the primary currency used in an economy.

To be a store of value requires Bitcoin wallets to be secure and for Bitcoin to hold its value over time.[12] Those who receive currency expect to be able to save and spend it later with the same purchasing power. We have seen that Bitcoin wallets are often compromised, therefore they may not be secure and available at a future time.[13] The volatility as given previously also means that receivers of Bitcoin payments are not guaranteed to preserve the same purchasing power in the future either. Therefore, Bitcoin does not satisfy the function of being a store of value.

Bitcoin can be used as a medium of exchange but lacks in being an effective unit of account and store of value.

Section 5: The Central Banks and Digital Currency

Given Bitcoin's global adoption, with hundreds of thousands of daily transactions, the Central-Banks need to be abreast with the developments of digital forms of currency. With nearly 80% of Central Banks "conducting work" on a CBDC[14] (exhibit 1), no country has formally issued one to retail consumers but proof of concepts have been created. However, with its limitations causing it to be touted as a store of value rather than a means of transaction, the opportunity arises for the Central banks to introduce a stabilized Digital Currency, a form of electronic retail payment. A Central Bank issued Digital Currency (CBDC) is similar to a stablecoin, otherwise known as "collateralized cryptocurrency", a digital currency which pegs its value to a unit of an underlying asset, backing wholly or partially with state-issued tender, very liquid reserves, or commodities[15] with the difference being that the CBDC is regulated whilst a stablecoin is not.

Here we consider the various benefits of a CBDC and why we believe that it is a sensible undertaking. We review a study on two recent developments involving digital currencies by BIS, Bitcoin, and the venture of Big

[12] Yermack (2015) explains the difficulty of ensuring secure "digital wallets" in the Bitcoin industry.
[13] McMillan (2014) for Wired, details the security breach of Mt. Gox, a formerly popular Bitcoin exchange, where hackers stole around $460 million dollars worth of Bitcoin.
[14] De Bode, Higginson & Niederkorn (2021) for McKinsey, Central Bank adoption of CBDCs
[15] Calle & Eidan (2020) for R3, describes what a CBDC is and how its stability is hedged

Tech into digital payment services. With cash transactions declining across the globe further accelerated by the pandemic, a lack of a CBDC causes consumers to seek an alternative source for digital payment (exhibit 2). With few benefits in the interest of the public, while being commonly used for financial crimes, Bitcoin has been a premier alternative to a regulated Digital-Currency[16]. Another option is the use of payment services provided by Big Tech companies which can reduce public welfare as a result of market concentration. Digital payment options such as Debit- and Credit-cards have greater costs than cash which are indirectly levied to the consumer in the form of merchant fees.[17] With the emergence of Big Tech and their dominant market power, the consumer may bear even greater fees up to 4%.[18] There lies significant opportunities for the central banks to address the issues with Bitcoin as a CBDC will become a substitute, and will also prevent Big Tech companies from having too much market dominance and charging consumers more. There are many approaches that the government has proposed for the architecture of the CBDC. This brings us to our next point where we look at the different types of architecture and analyze the benefits, inherent risks, and costs associated with each.

There are currently 4 potential types of CBDCs, being Hybrid, Indirect, Direct, and Intermediate. The Hybrid CBDC involves the Central-Bank being the only entity permitted to create or destroy a token of the core ledger, a ledger holding the CBDC reserves. This forces Payment Interface Providers (PiPs) to interact with end-users and maintain the know your customer checks [19]. This however provides significant risks as with a digitized form of currency, where all the coins are both created and destroyed through the core ledger with a single controlling entity, a security breach could deplete reserves or cause an over-circulation of coins in the market to destroy underlying-value. This risk is also associated with the Direct CBDC as the Central Bank is still the main creator/destroyer of the coin; however, the Direct CBDC is offered to consumers in 2 ways, through a value model or through Central Bank accounts. Indirect CBDC functions slightly differently as the CB provides a non-CB entity with the ability to issue a stablecoin backed by the Central Bank's reserves where the asset, the coin, held by retail participants is a liability of the private sector intermediary. This could cause a similar risk

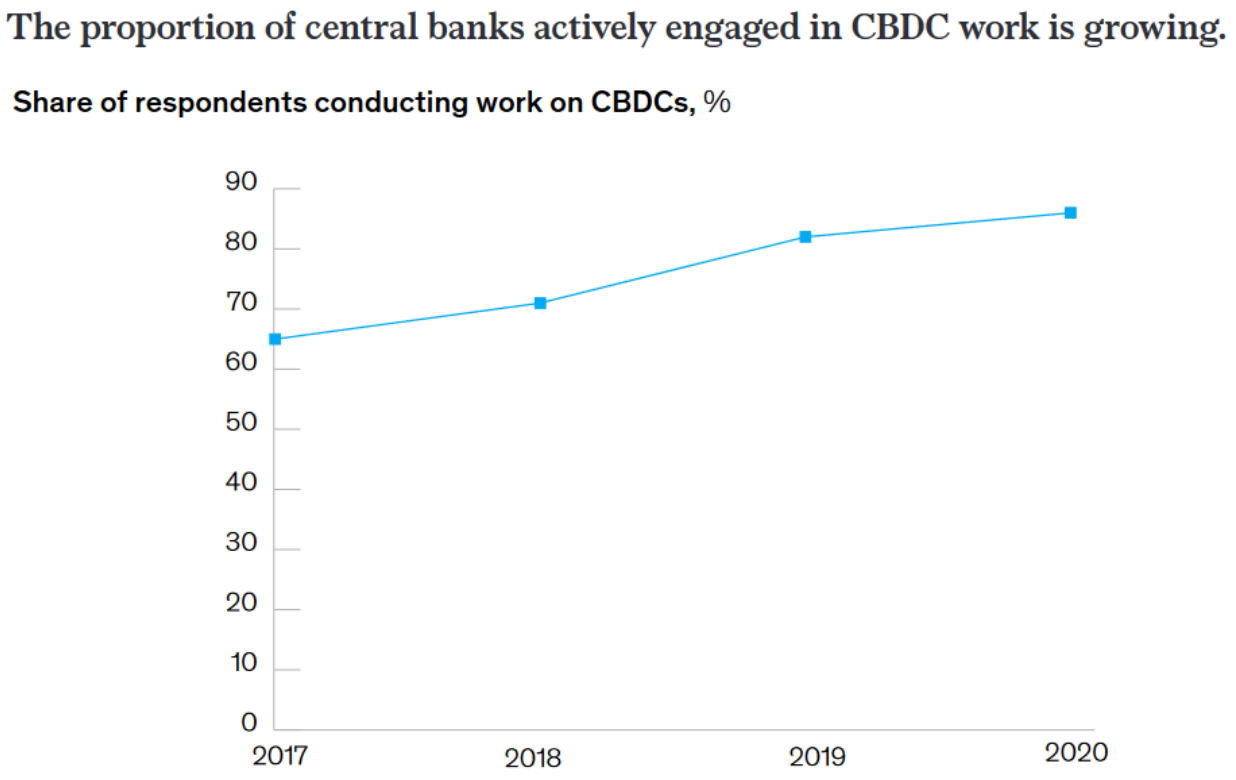
[16] BIS (2021), Bitcoin is commonly used for financial crimes, ransomware attacks and operating on top of a massive energy footprint.
[17] BIS (2021), The costs of these credit and debit card fees are not directly seen by the consumer, but are charged indirectly through merchant fees and higher prices
[18] BIS (2021), description of highest recorded merchant fee
[19] Calle & Eidan (2020) for R3, description on the types of CBDC, Hybrid, Direct, and Indirect

associated with the Direct and Hybrid methods as with a security breach in the issuing firm, the stablecoin could be over-circulated which would place strains on the intermediary, with it being a liability for the private sector intermediary. The final type of CBDC the central bank may consider is the Intermediated CBDC, where the CB will not collect all payment data, rather, only wholesale balances. This addresses users' needs for privacy while protecting the CB from exposure to harmful data breaches. The Intermediated model is compromised due to the CB not having the necessary data to honour claims, which as a result, would require it to verify through third parties. Effectively, this adds an extra layer of complexity as PiPs will need active verification of accounts, in which each wholesale account equates to the aggregate of the retail accounts associated with it.

Auer and Bohme illustrate an imperative trade-off model between the amount of information held by the CB being inversely related with the required level of PiP supervision (exhibit 3). If the CB wishes to implement the Direct CBDC, they would reduce the need to rely on third parties on top of their PiP-supervision and prevent crimes, with the tradeoff of tapping into highly sensitive user information as they monitor each retail transaction as mentioned by Auer and Bohme (2021). Conversely, an Intermediated CBDC approach possesses the benefits of returning user privacy at the expense of requiring complex technological infrastructure to verify transactions by PiPs. Fundamentally, this trade-off model recognizes the costs and benefits regarding each type of CBDC approach where we believe an implementation of the Direct CBDC would be the optimal solution.

Exhibits

Exhibit 1:



Source: Codruta Boar and Andreas Wehrli, "Ready, steady, go? – Results of the third BIS survey on central bank digital currency," Bank for International Settlements, January 2021, bis.org.

Exhibit 2:

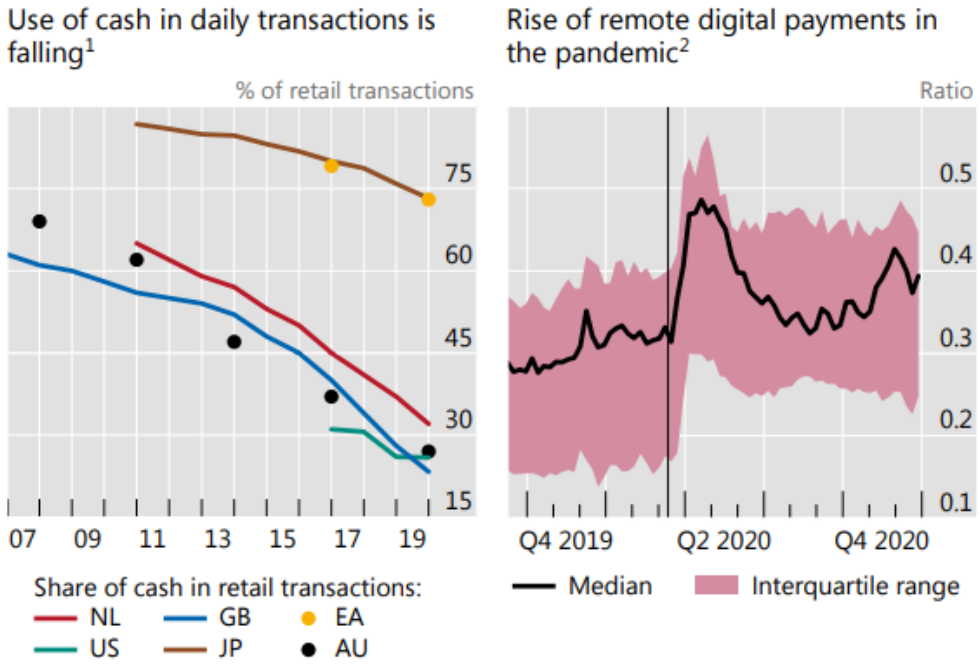


Exhibit 3:

A new trade-off for the central bank of the future — Graph 5

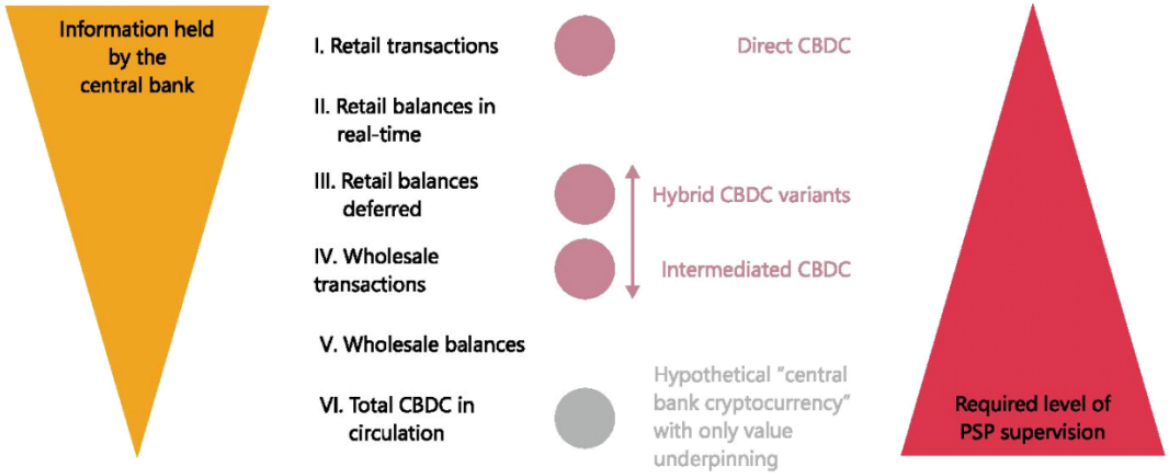


Table 1: Benefits of BTC

Perspective	Benefit	References
Technology	Decentralization	(Ali et al. 2014), (Barber et al. 2012), (Böhme et al. 2015), (Krombholz et al. 2016), (Nakamoto 2008), (Zohar 2015)
	Faster transaction speeds	(Gao et al. 2015), (Zohar 2015)
	Security and control of money	(Gao et al. 2015), (Van Alstyne 2014)
Economics	Lower transaction fees	(Ali et al. 2014), (Barber et al. 2012), (Beer and Weber 2014), (Böhme et al. 2015), (Gao et al. 2015), (Van Alstyne 2014), (Zohar 2015)
	Speculating opportunities	(Ali et al. 2014), (Böhme et al. 2015), (Gao et al. 2015), (Glaser et al. 2014), (Hur et al. 2015)
	Mining rewards	(Barber et al. 2012)
Policy	Transaction irreversibility	(Barber et al. 2012), (Beer and Weber 2014), (Zohar 2015)

Table 2: Risks of BTC

Risk	Risk determinant	References
Market risk	Price volatility and exchange rate risk	(Bohr and Bashir 2014), (Brezo and Bringas 2012), (Gao et al. 2015), (Glaser et al. 2014), (Grant and Hogan 2015), (Van Alstyne 2014)
Counterparty risk	Security breaches or malfunction of exchanges / wallet providers	(Bohr and Bashir 2014), (Grant and Hogan 2015), (Meiklejohn et al. 2013), (Moore and Christin 2013), (Van Alstyne 2014)
Transaction risk	Irreversibility of transactions	(Beer and Weber 2014), (Meiklejohn et al. 2013)
	Possible cancelation of a confirmed transaction	(Eyal and Sirer 2014), (Karame et al. 2012), (Sapirshtein et al. 2016)
	Potential blacklisting of bitcoins of dubious origin	(Möser et al. 2013), (Möser et al. 2014)
Operational risk	Security flaws or incidents (e.g., forgotten or stolen passwords)	(Brezo and Bringas 2012), (Gao et al. 2015), (Grant and Hogan 2015), (Vasek et al. 2016)
	Potential vulnerabilities in the protocol design	(Eyal and Sirer 2014), (Karame et al. 2012)
Privacy risk	Linking Bitcoin addresses to real identifiers	(Androulaki et al. 2013), (Brezo and Bringas 2012), (Meiklejohn et al. 2013), (Reid and Harrigan 2013), (Ron and Shamir 2013)
Legal and regulatory risk	Uncertain legal and regulatory status of Bitcoin	(Bohr and Bashir 2014), (Grant and Hogan 2015), (Grinberg 2011), (Reid and Harrigan 2013)

References:

Antonopoulos, Andreas M. “Mastering Bitcoin, 2nd Edition.” O'Reilly Online Learning, O'Reilly Media, Inc., Retrieved from https://www.oreilly.com/library/view/mastering-bitcoin-2nd/9781491954379/ch04.html.

Auer, B., Bohme, R. (2021). “Central bank digital currency: the quest for minimally invasive technology”, www.bis.org/publ/work948.htm

Bambrough, B. (2021, September 26). JPMorgan Warns Big Investors Are Suddenly Dumping Bitcoin For Ethereum Amid A $150 Billion Crypto Price Crash. Retrieved from https://www.forbes.com/sites/billybambrough/2021/09/26/jpmorgan-warns-big-investors-are-suddenly-dumping-bitcoin-for-ethereum-amid-a-150-billion-crypto-price-crash/?sh=355c095b213f

Baur, D.G., K. Hong and A.D. Lee. 2018. “Bitcoin: Medium of exchange or speculative assets?” Journal of International Financial Markets, Institutions & Money (54): 177-189.

BIS 2021. “III. CBDCs: an opportunity for the monetary system”, www.bis.org/publ/arpdf/ar2021e3.htm

Calle, G., Edian, D. (April, 2020) “Central Bank Digital Currency: An Innovation in Payments”, R3 https://www.r3.com/wp-content/uploads/2020/04/r3_CBDC_report.pdf

Hayes, Adam. “What Happens to Bitcoin after All 21 Million Are Mined?” Investopedia, Investopedia, 13 Oct. 2021, https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/.

Higginson, Matt. “CBDC and Stablecoins: Early Coexistence on an uncertain road” Mckinsey, 13 Oct. 2021 https://www.mckinsey.com/industries/financial-services/our-insights/cbdc-and-stablecoins-early-coexistence-on-an-uncertain-road

Hong, Euny. “How Does Bitcoin Mining Work?” Investopedia, Investopedia, 13 Oct. 2021, Retrieved from https://www.investopedia.com/tech/how-does-bitcoin-mining-work/.

Kashif, Malik. “Cryptocurrency: How Anonymous Is Cryptocurrency?” Sanewnetworks, 8 Sept. 2021, https://sanewnetworks.com/cryptocurrency-how-anonymous-is-cryptocurrency/.

Kulkarni, S. (2021, September 20). Bitcoin: Pros And Cons Of Investing In World's Largest Cryptocurrency.Retrieved from https://www.goodreturns.in/classroom/pros-and-cons-of-investing-in-bitcoin-advantages-and-disadvantages-of-bitcoin-cryptocurrency-1209500.html

Luthi, Ben. (30th, July, 2021) “What is Crypto Lending and How does it Work?”, Bankrate https://www.bankrate.com/loans/personal-loans/cryptocurrency-lending/

McMillan, R. (2014, March 03). The inside story of Mt. Gox, Bitcoin's $460 million disaster. Retrieved from https://www.wired.com/2014/03/bitcoin-exchange/

Mishkin, F.S. and A. Serletis. 2020. “What Is Money?” The Economics of Money, Banking, And Financial Markets. Pearson, pp. 50-62.

Perceived Benefit and Risk as Multidimensional Determinants of Bitcoin Use: A Quantitative Exploratory Study. (2016). Retrieved from https://informationsecurity.uibk.ac.at/pdfs/Abramova2016_Bitcoin_ICIS.pdf

The Business Benefit of Using Cryptocurrency. (2021, September 01). Retrieved from https://www2.deloitte.com/us/en/pages/audit/articles/corporates-using-crypto.html

Yermack, D., 2015. “Is Bitcoin a real currency? An economic appraisal.” Handbook of Digital Currency. Academic Press, pp. 31–43.

---. 2021a. “User Agreement.” Bitcoin.com, https://www.bitcoin.com/legal/user-agreement/.