

(Source:Hilarski from steemit.com)

## CRYPTO-CURRENCIES: BITCOINS

# CRYPTO-CURRENCIES: BITCOINS

**Suryansh Panwar**

*G.D. Public School, Dwarka*

---

## INTRODUCTION

The purpose of this paper is to address the strengths and weaknesses of bitcoin, which is the first and most valuable crypto-currency in the market, and examines its opportunities in the future. Particularly, the paper emphasizes on the advantages of using bitcoin specifically and crypto-currencies generally in gaining economic benefits, e.g. hedging from inflation; or points out disadvantages of bitcoin and crypto-currencies compared with national currencies with real examples of bitcoin hacks in different countries that allow to trade bitcoin on exchanges.

## BACKGROUND

Bitcoin is designed as a means of exchange. It can be considered as a synthetic commodity money (Selgin, 2015). It has a commodity money sharing feature that presents a combination of commodity money and fiat money. It is clearly seen that naturally, commodity money is usually scarce for example gold and it is used for another uses other than being a means of exchange, while fiat money is not totally scarce, and is issued by the bank with the main purpose of exchange.

**THE CRYPTO UNIVERSE**  
COMPARING SIX MAJOR CURRENCIES

**BITCOIN**  
Bitcoin is the original cryptocurrency, and was released as open-source software in 2009.

Using a new distributed ledger known as the blockchain, the Bitcoin protocol allows for users to make peer-to-peer transactions using digital currency while avoiding the "double spending" problem.

No central authority or server verifies transactions, and instead the legitimacy of a payment is determined by the decentralized network itself.

**KEY FEATURES**

- Blockchain - Foundational Technology
- Fast P2P Payments Worldwide
- No Double Spend Problem
- Low Processing Fees
- Decentralized
- Available To Anyone
- Anonymity (Partial)
- Transparent

**INTERESTING FACT**  
In 2010, a programmer bought two pizzas for 10,000 BTC in one of the first real-world bitcoin transactions.

Today, 10,000 BTC is equal to roughly \$38.1 million - a big price to pay for satisfying hunger pangs.

**1** **10,000**

While regrettable, it is also forgivable. No one knew Bitcoin would be accepted by hundreds of thousands of merchants just years later.

Now cryptocurrency enthusiasts around the world celebrate "Bitcoin Pizza Day" every year on May 22nd, the date the transaction took place.

**BOTTOM LINE FOR BITCOIN**  
Bitcoin is the original cyptocurrency with the most liquidity and significant network effects. It also has brand name recognition around the world, with an eight year track record.

**ETHEREUM**  
Ethereum is an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications.

In the Ethereum blockchain, instead of mining for bitcoin, miners work to earn ether, a type of crypto token that fuels the network. Beyond a tradeable cryptocurrency, ether is also used by application developers to pay for transaction fees and services on the Ethereum network.

**KEY DIFFERENTIATIONS FROM BITCOIN**

- Platform For Making Blockchain Applications
- Multiple Industry Uses
- Uses Smart Contracts
- Ether Powers The Network

**INTERESTING FACT**  
Ethereum has quickly skyrocketed in value since its introduction in 2015, and it is now the 2nd most valuable cryptocurrency by market cap.

It's increased in value by 2,226% in just the last year - a huge boon for early investors.

**BOTTOM LINE FOR ETHEREUM**  
Ethereum serves a different purpose than other cryptocurrencies, but it has quickly grown to displace all but Bitcoin in value. Some experts are so bullish on Ethereum that they even see it becoming the world's top cryptocurrency in just a short span of time - but only time will tell.

(Source:Hilarski from steemit.com)

Additionally, two types of money can be used for value storage. Bitcoin is a combination of two money types, bitcoin is scarce due to its design and foundation. The scarcity of bitcoin can be determined by an automatic, determined rule by assessing the level of competition as commodity money. However, Bitcoin is not exactly the same as fiat money that it has no intrinsic value. Besides that, Bitcoin also has a similarity with commodity money that is semi-focused. Forms of commodity money often do not meet the threats from competitors, which is not consistent with the bitcoin payment network. The assessment of the potential and acceptability of bitcoin should address the analysis of the rate of development of bitcoin supplies. The supply of Bitcoins can be totally predictable and keep increasing in downward steps until 2040 and remain at

an extremely high level of 2040. Due to the demand of Bitcoin in contrast to supply, it is difficult to predict the near future of Bitcoin, leading to potential value judgments and widespread use of Bitcoin in the future. Nevertheless, if the demand increases steadily, the demand eventually becomes larger than the supply that drives up Bitcoin prices and thus deflation. These integrated deflationary effects help Bitcoins to be used as an investment rather than a means of exchange. If virtual currency gradually developed as a form of exchange and slowly became an accepted alternative similar to the fiat currency, one would issue a dual currency or multi-currency structure where that fiat money and virtual currency in parallel exist. History has recorded many examples of the existence of dual currency or multi-currency. There are a variety of currencies used for exchange including cigarettes, alcohol, barley and many others. In the Middle Ages, gold, silver, and bronze coins were popularized and circulated at the same time at pre-determined exchange rates. In the 1800s, commodity money as well as fiat money issued by the government coexist and circulate simultaneously. In the United States, there were many currencies used as a means of communication, especially in the 1930s, when even the privately-issued banknotes was used concurrently with fiat money and commodity money.

**LITECOIN**  
 Litecoin was launched in 2011 as an early alternative to Bitcoin.  
 Around this time, increasingly specialized and expensive hardware was needed to mine bitcoins, making it hard for regular people to get in on the action. Litecoin's algorithm was an attempt to even the playing field so that anyone with a regular computer could take part in the network.

**KEY DIFFERENTIATIONS FROM BITCOIN**

- A Simpler Cryptographic Algorithm
- 4x Faster Block Generation
- Faster Transaction Processing
- 84M / 21M (84 Million Coin Max [Bitcoin: 21 million])

**INTERESTING FACT**  
 Litecoin's creator is a former Google employee and MIT grad named Charlie Lee. He wanted to make cryptocurrency more accessible - and for Litecoin to be the "silver" to Bitcoin's "gold".

**BOTTOM LINE FOR LITECOIN**  
 Other altcoins have taken away some of Litecoin's market share, but it still has an early mover advantage and some strong network effects.

---

**ETHEREUM CLASSIC**  
 In 2016, the Ethereum community faced a difficult decision: The DAO, a venture capital firm built on top of the Ethereum platform, had \$50 million in ether stolen from it through a security vulnerability.  
 The majority of the Ethereum community decided to help The DAO by "hard forking" the currency, and then changing the blockchain to return the stolen proceeds back to The DAO.  
 The minority thought this idea violated the key foundation of immutability that the blockchain was designed around, and kept the original Ethereum blockchain the way it was. Hence, the "Classic" label.

**KEY DIFFERENTIATIONS FROM BITCOIN**

- Platform For Making Blockchain Applications
- Multiple Industry Uses
- Uses Smart Contracts
- Ether Powers The Network

**INTERESTING FACT**  
 Because Ethereum and Ethereum Classic stem from the same code, they run in parallel, doing virtually the same thing.  
 The DAO hacker still holds over 3 million of Ethereum Classic, which could be "dumped" somewhere along the line - a baked in risk that could drag on price.

**BOTTOM LINE FOR ETHEREUM CLASSIC**  
 As time goes on, Ethereum Classic has been carving out a separate identity from its bigger sibling. With similar capabilities and a different set of principles, Ethereum Classic could still have upside.

---

**DASH**  
 Dash is an attempt to improve on Bitcoin in two main areas: speed of transactions, and anonymity.  
 To do this, it has a two-tier architecture with miners and also "masternodes" that help the network perform advanced functions such as near-instant transactions and coin-mixing to provide additional privacy.

**KEY DIFFERENTIATIONS FROM BITCOIN**

- Two-Tier Architecture
- Advanced Transactions
- Decentralized Autonomous Organization (DAO)
- Improved Anonymity

**INTERESTING FACT**  
 For each block mined, a 10% reward goes to the treasury to help fund improvements and projects around Dash.  
 Dash is the first ever Decentralized Autonomous Organization (DAO), a type of organization run through rules encoded in computer programs and smart contracts.

**BOTTOM LINE FOR DASH**  
 The innovations behind Dash are interesting, and could help to make the coin more consumer-friendly than other alternatives.

---

**RIPPLE**  
 Ripple is considerably different from Bitcoin. That's because Ripple is essentially a global settlement network for other currencies such as USD, Bitcoin, EUR, GBP, or any other units of value (i.e. frequent flier miles, commodities).  
 To make any such a settlement, however, a tiny fee must be paid in XRP (Ripple's native tokens) - and these are what trade on cryptocurrency markets.

**KEY DIFFERENTIATIONS FROM BITCOIN**

- Global Settlement Network
- Works With Any Store of Value
- Backed By Many Banking Institutions
- No Mining Involved

**INTERESTING FACT**  
 Because Ripple is intended as a new global settlement system for the exchange of currencies and other assets, many banks are experimenting with the technology.  
 Banks counted as early supporters include: Royal Bank of Canada, Santander, UBS, and UniCredit.  
 There is no "mining" on the Ripple network - instead, there is an existing supply of 100 billion ripples, with many still being held by the company. In mid-2017, the company announced they'd lock up billions of dollars worth of ripples in escrow smart contracts, to decrease any fears of the market being "flooded".

**BOTTOM LINE FOR RIPPLE**  
 Ripple runs on many of the same principles of Bitcoin, but for a different purpose: to serve as the middle man for all global FX transactions. If it can successfully capture that market, the potential is high.

(Source:Hilarski from steemit.com)

Today, dual currency economies start to appear in developed and developing countries such as Liberia, Cuba and some Latin American states. One example is Switzerland, which has the world's most advanced industry, accepts both euro and Swiss franc even though the Swiss franc are globally accepted. When multiple currencies coexist in a national economy, Gresham's law states that regardless of the nature of the currency, "good" and "bad" money, they are equally valid under the legal tender. Good money is defined as a currency with no big difference between real

value and nominal value. Meanwhile, according to research by Rolnick and Weber (1986), it shows that bad money can help make good money a premium rather than pushing it out of the money market entirely. Although the two researchers have ignored bid rules for the peer value of bilateral currencies, the dollarization in countries with underdeveloped economies and how money works is opposite to Gresham's law (Guidotti and Rodriguez, 1992), where strong currencies like the US dollar have removed bad currencies according to Mundell (1998).

## **STRENGTHS**

The design, the nature of operation, and the future limit source of bitcoin make it a viable currency for the world and elevate its position over traditional currencies such as money and gold over recent years. The returns from mining bitcoin will be diminished every four years until the number of bitcoin reaches the maximum limit of 21 million (King, 2013). The scarcity of bitcoin is important factor as it determines the value of this crypto-currency, meaning bitcoin will never be inflated from an overabundance due to the limited amount. Moreover, the most outstanding advantage of bitcoin over national currencies is that it hedges against inflation originating from national government changes or restrictions (Magro, 2016). Thus, bitcoin has been perceived as a safe place to store money, i.e. money stored in the form of bitcoin is not affected by the effect of "time value of money". Thus, people buy bitcoins because of its strength as a refuge against inflating national currencies. The Ellington's head of systematic strategies - Rasheed Sabar also believed that cryptocurrencies can be the safe havens in the next crisis that protect against high inflation and capital controls, and bitcoin can be considered as an insurance policy against low-trust states of the world. The fact that the number of hedge funds used bitcoin to hedge against risks is small but growing (figure 1) (Zuckerman, 2017). Nevertheless, price of bitcoin, is like most commodities, is wildly subject to external factors. For example, bitcoin was the best performing currency of 2015 using the US Dollar Index due to market demand for a safe option to store wealth and its price volatility (Desjardins, 2016), which made this crypto-currency the most valuable currency in the world at the end of 2015. United States and China witness this feat in the global economy; South America, in particular, is a hotbed for increased cryptocurrency usage, e.g. bitcoin transactions increased by 510% within only one year from 2014 to 2015 (Bitcoin: A New Global Economy, 2015).



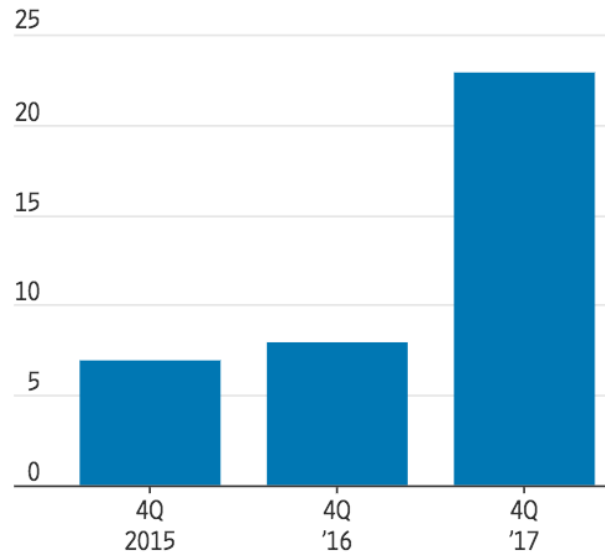


Figure 1

Moreover, Argentina has seen a tremendous increase in bitcoin demand due to its extremely high inflation rate and high population of unbanked citizens. Before the existence of bitcoin, Argentinian citizens would prefer to convert the peso to U.S. dollars to avoid losses in monetary value. Nevertheless, strict restrictions that are imposed on the amount of U.S. dollars that Argentinian citizens can convert encourages people to switch to crypto-currencies; bitcoin has changes the situation. Bitcoin adoption arose and people started to trade bitcoin in black market with the increasing price (Magro, 2016). Literally, the demand of every individual in the world is to preserve their money value is apparent, and the existence of cryptocurrencies meet that demand by providing prominent legal vehicles. Argentina is not the only country that has demand of cryptocurrencies to protect value of national currencies. Global markets crashes due to political conflicts are another reason that increase value and demand of cryptocurrencies. For example, prior to the Brexit, or the United Kingdom has recently removed itself from the European Union, price of bitcoin declined by around 15% (Bovaird, 2016). However, after the U.K successfully walked away from the European Union, bitcoin's price skyrocketed by over 18% from \$550 to \$650 in the following day. The Brexit further adversely affected the globally traded markets because investors lost confidence in what the Brexit vote would mean financially. In this situation, bitcoin presents itself is the safest currency that can be traded expeditiously, especially worldwide; whereas other fiat currencies requires in-person exchanges if people wish to and that money cannot be used if it is not accepted locally. On the other hand, bitcoin does not deal with this problem. People who want to buy bitcoin only need to create an online account with an online exchange, quote their bid and wait for the transaction to be completed in a few minutes. Then,

people can use bitcoin in digital wallet to make global purchases without the complication of currency convert and without any fees of converting different currencies. Thus, bitcoin is an ideal solution that offers users unique benefits such as quick entry and exit quick entry and exit for a currency that can quickly gain value. Although fiat money can appreciate against other currencies and gains more value, fiat money cannot beat the agility of bitcoin. To conclude, the disruptive technology of bitcoin is the most valuable option for investors who simply wants a tool to hedge against sinking global markets and protect their wealth (DeVries, 2016).

## **WEAKNESSES**

Bitcoin has a few shortcomings in the design phase and is difficult to modify. For example, every transaction on the ledger or block chain is open to the public that everyone can see it, which means being attacked easily due to easy access (King, 2013). According to Hileman 2016, so far, the Bitcoin network has been subjected to a series of checks to address DDos attacks. These tests aim to demonstrate the design of bitcoin that its network can't handle a large amount of transactions. The fact that Bitcoin participants collapse the system is one of the most damaging aspects of bitcoin. Bitcoin has expanded and disseminated dubiously over time through a number of events. Silk Road is a black market, demonstrating the negative image of using digital money, not just bitcoin. In this market, publicly traded prohibited items such as weapons, drugs, ... and a million of illegal transactions are paid by bitcoin mainly by the manipulation of the hidden bosses due to lack of state management. This has taken place from 2011 to 2013. According to Bearman 2015, the figure could have reached one billion dollars. Bitcoin has become a popular tool of ransomware, like the Wannacry virus attack in 2017. This has made it difficult for the government to track down the people behind the transactions (Virgna, Demos, and Hoffman, 2017). Thus, without positive marketing, digital money can be misunderstood as being used only for criminals.

Virtual money has also evolved with concerns about security. Magic the Gathering Online Exchange, was one of the world's major bitcoins until it officially went bankrupt by hacker attacks in 2011, stealing approximately 460 million USD (McMillan, 2014). The CEO, Mark Karpeles, did not use the management version of the new code, along with allowing for bug fixes and security maintenance for several weeks to accidentally create a security hole that allows hackers to exploit it. This incident caused a severe drop in the price of bitcoin as the users quickly sold off bitcoin for fear of being stolen. Ethereum, another form of digital currency, has undergone similar theft with an estimated \$ 50 million loss (Price, 2016). The target of hackers is one who holds large amounts of electronic currency but not follows the rules of security. These are the main reasons that the value of cryptocurrency is falling and damaging to the image of virtual currency. Since 2016, the cost of mining bitcoin significantly increases due to changes in source code in solving algorithms. As a result, half the amount of bitcoin returned to the miners. This increases the efficiency by pushing 25% of the bitcoin network running on the older hardware, because it



will cost more to operate than earning from mining (Kar, 2016). Moreover, transition in the mining community can make the network less safe and vulnerable to attack. It also hinders miners access to the network due to high costs and low profits. Only some miners survive until bitcoin is mined. Virtual currency is traded as a commodity that can be considered a weakness. Commodity-based markets for trading show continuous volatility. Volatility reduces investor confidence in commodities. In addition, the difficulty in determining the bitcoin price creates uncertainty. Value fluctuations create a lot of risks, which prevents investors from holding Cryptocurrency for any period of time (PWC, 2015).

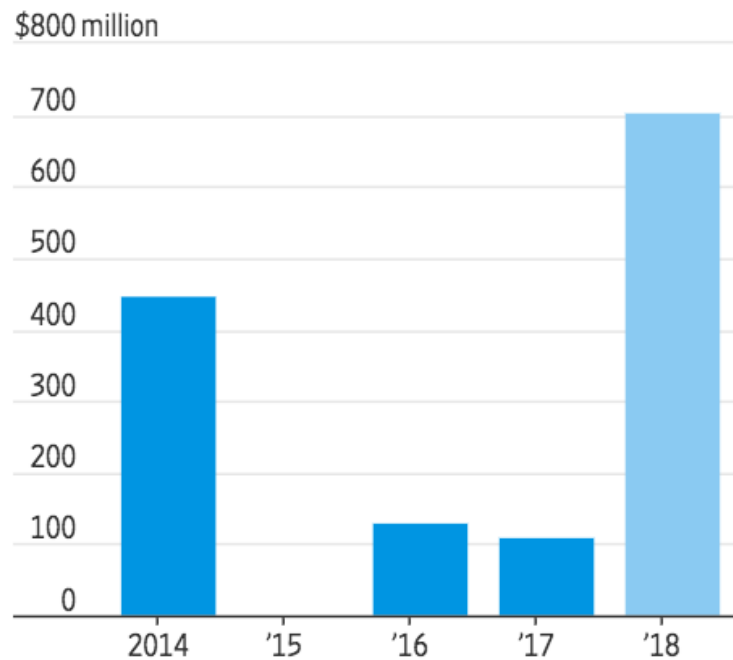


Figure 2. Losses due to hacks on crypto-currencies platforms

As can be seen from figure 2 that losses due hacks on crypto-currencies platforms are extremely high compared with previous years. These losses are attributable to several scandal occurs across the globe. One of the scandals of cryptocurrencies cyberattack is the case of Tokyo Coindeck Inc. in Japan. This cryptocurrency trading platform operator spent ¥46.3 billion (\$435 million) to compensated 260,000 losses of its customers affected by the hacking and resumed some exchange services. These customers kept their money in a digital currency called NEM whose 523 million units was stolen. Particularly, the victims were compensated for 88.549 yen per NEM which was the rate promised by Coincheck. Although the compensating rate exceeded the

current market rate but below the value of one NEM in terms of yen at the time NEM was stolen, which was ¥110 per NEM.

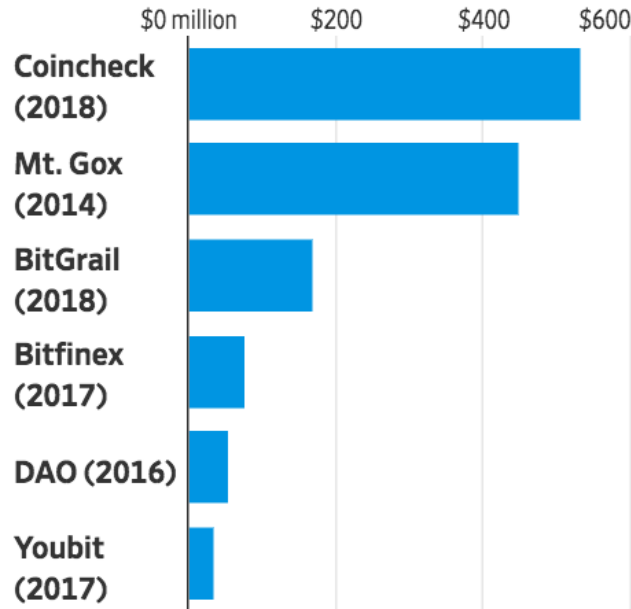


Figure 3. Selected losses from cyberattacks on trading platforms

Figure 3 illustrates that Coincheck is the most damaged exchange with the largest amount of losses of reverses compared with Mt.Gox, Bitgrail, Bifinix, DAO and Youbit. More importantly, despite several investigation to the hack were conducted by the Japanese authorities, significant progress in identifying the hackers was not reported. This may be explained by the design of the cryptocurrencies in which many of them offer a high degree of anonymity to their owners (Mochizuki, 2018). South Korea is also a victim of cryptocurrency attacks. Within eight months, Youbit suffered from two hacks that forced it to shut down and went bankrupt. The large amount of its digital-currency reserves was lost raised concerns about security in trading in bitcoin and other virtual currencies, which made South Korea faced a collapse of cryptocurrency exchanges (South Korean cryptocurrency, 2017). 17% of its total assets was lost in the latest security breach. However, the exchange neither announced the name of coin that was stolen nor specified the financial value of its losses to the public. When the price of bitcoin have significantly climbed up and international speculators have come to this market looking for speculative opportunities, especially in Asia, the risk of being attacked online in cryptocurrency markets is raised (Jeong and Russolillo, 2017). Experts warn that cryptocurrencies and the trading platforms are constantly exposed to the risk of being attacked by cyber-hackers. The typical disadvantage of trading bitcoin is that several crypto exchanges do not consider safeguard investors' virtual tokens is the highest priority, whereas traditional stock and futures exchanges offer traders a higher level

of security despite that they take away a small proportion of gains as trading fees. Recent hacks and considerable losses from crypto-currency exchanges illustrate the vulnerability of this digital money. Investors are exposed to risks when virtual assets they trade are unproven, especially on startup unregulated exchanges since these new exchanges are often flooded with a large number of new, untested currencies. Although bitcoin has the largest capacity in the crypto market, its price is also exposed to risks due to the shallow market.

After severe fluctuation in prices and huge publicity, the debate over the replacement of bitcoin as the future currency and its advantages against the dollar has arisen. The common question is if bitcoin differs from the dollar. The fact that bitcoin is not backed by any government, meaning people are not forced to use it as a payment method, e.g. the U.S. government requires payment in dollars to create direct demand for dollars and remove replication by Bitcoin (Whelan, 2013). Moreover, monetary systems are always in control of states that generates revenue from seigniorage over its national currency and unlikely to permit other sources of money to replace it. According to Goodhart (1998), the private inefficiencies of barter has little historical backing can be solved by the emerge of private money. For instance, precious metals was adopted as a payment method due to its scarcity; however, the supply of metallic content of coins is not guarantee to be limited as claimed by advocates of bitcoin. Goodhart (1998) questions the credibility of the private suppliers of money in committing to limit the source. Goodhart (1998) claimed that the promise to limit the source of coin is against the interest of currencies' controllers, thus the credibility is low.

## REFERENCES

Desjardins, J. (2016). It's Official: Bitcoin was the Top Performing Currency of 2015. The Money Project. Retrieved from <http://money.visualcapitalist.com/its-official-bitcoin-was-the-top-performing-currency-of-2015/>

Guidotti, P. E. and C.A. Rodriguez, 1992, Dollarization in Latin America – Gresham law in reverse. International Monetary Fund Staff Papers 39, 518–544.

Hileman, G. (2016). State of Bitcoin and Blockchain 2016: Blockchain Hits Critical Mass. Coindesk. Retrieved from <http://www.coindesk.com/state-of-bitcoin-blockchain-2016/>

King, R. S. (2013). By reading this article, you're mining bitcoins. Quartz. Retrieved from <http://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins/>

Kar, I. (2016, June 30). Everything you need to know about the bitcoin „halving“ event. Retrieved from Quartz website: <http://qz.com/681996/everything-you-need-to-know-about-the-bitcoin-halving-event/>

- Jeong, E-Y., & Russolillo, S. (2017). Cryptocurrency Exchange Collapses, Files for Bankruptcy After Second Hack. Wall Street Journal. Retrieved from [https://www.wsj.com/articles/cryptocurrency-exchange-collapses-files-for-bankruptcy-after-second-hack-1513683519?mod=article\\_inline](https://www.wsj.com/articles/cryptocurrency-exchange-collapses-files-for-bankruptcy-after-second-hack-1513683519?mod=article_inline)
- Magro, P. (2016). What Greece can learn from bitcoin adoption in Latin America. International Business Times. Retrieved from <http://www.ibtimes.co.uk/what-greece-can-learn-bitcoin-adoption-latin-america-1511183>
- McMillan, R. (2014, March 3). The Inside Story of Mt. Gox, Bitcoin's \$460 Million Disaster. Retrieved from Wired.com Website: <http://www.wired.com/2014/03/bitcoin-exchange/>
- Mochizuki, T. (2018). Hacked Japanese Cryptocurrency Exchange Pays Back Customers. Wall Street Journal. Retrieved from <https://www.wsj.com/articles/hacked-japanese-cryptocurrency-exchange-pays-back-customers-1520917328?mod=searchresults&page=1&pos=3>
- Mundell, R., 1998, Uses and Abuses of Gresham's Law in the History of Money, Zagreb. Journal of Economics, 2(2), 3 – 38.
- PwC. (2015). Money is no object: Understanding the evolving cryptocurrency market. PricewaterhouseCoopers, LLP.
- Rolnick, A. J. and W.E. Weber, 1986, Gresham's Law or Gresham's Fallacy. Journal of Political Economy, 94 (1): 185–199.
- Selgin, G., 2015, Synthetic commodity money, Journal of Financial Stability, 17, 92-99.
- Vigna, P., Demos, T., & Hoffman, .L. (2017). Goldman Sachs Explores a New World: Trading Bitcoin. Wall Street Journal. Retrieved from <https://www.wsj.com/articles/goldman-sachs-explores-a-new-world-trading-bitcoin-1506959128>
- South Korean cryptocurrency exchange to file for bankruptcy after hacking. (2017). Reuters. Retrieved from <https://www.reuters.com/article/us-bitcoin-exchange-southkorea/south-korean-cryptocurrency-exchange-to-file-for-bankruptcy-after-hacking-idUSKBN1ED0NJ>
- Whelan, K. (2013). How is bitcoin different from the dollar?. Forbes. Retrieved from <https://www.forbes.com/sites/karlwhelan/2013/11/19/how-is-bitcoin-different-from-the-dollar/#3dc70f5d398f>
- Zuckerman, G. (2017). Big Hedge Funds Want In on Bitcoin. Wall Street Journal. Retrieved from <https://www.wsj.com/articles/big-hedge-funds-want-in-on-bitcoin-1513765802>