**An Analysis of Cryptocurrency, Bitcoin, and the Future**

**Abstract**

**ـــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــ**

*Cryptocurrency, an encrypted, peer-to-peer network for facilitating digital barter, is a technology developed thirteen years ago. Bitcoin, the first and most popular cryptocurrency, is paving the way as a disruptive technology to long standing and unchanged financial payment systems that have been in place for many decades. While cryptocurrencies are not likely to replace traditional fiat currency, they could change the way Internet-connected global markets interact with each other, clearing away barriers surrounding normative national currencies and exchange rates. Technology advances at a rapid rate, and the success of a given technology is almost solely dictated by the market upon which it seeks to improve. Cryptocurrencies may revolutionize digital trade markets by creating a free flowing trading system without fees. A SWOT analysis of Bitcoin is presented, which illuminates some of the recent events and movements that could influence whether Bitcoin contributes to a shift in economic paradigms.*

ـــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــ

# Introduction

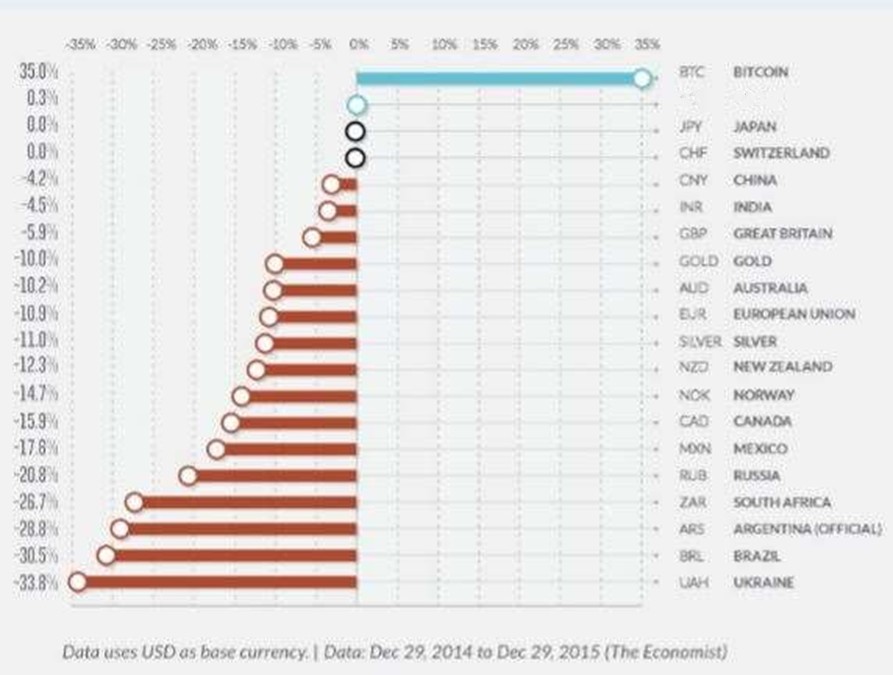
**Bitcoin**, the world’s most common and well known cryptocurrency, has been increasing in popularity. It has the same basic structure as it did when created in 2008, but repeat instances of the world market changing has created a new demand for cryptocurrencies much greater than its initial showing. By using a cryptocurrency, users are able to exchange value digitally without third party oversight. Cryptocurrency works on the theory of solving encryption algorithms to create unique hashes that are finite in number. Combined with a network of computers verifying transactions, users are able to exchange hashes as if exchanging physical currency. There is a finite number of bitcoin that will ever be generated, preventing an overabundance and ensuring its rarity. Water, despite its requirement as a life giving material, is generally accepted as being free or of little cost because it is so abundant. If water was rare, it would be more valuable than diamonds. Value exists for bitcoin because its users have trust that if they accept it as payment, they would could use it elsewhere to purchase something they want or need (Kelly, 2014). As long as the users maintain this faith, the valued object can be anything. Bitcoin’s value exists in its ecosystem much in the same way that wampum, a seashell, was the currency of the land for Native Americans (Kelly, 2014). Bitcoin does not have intrinsic value like gold in that it cannot be used to make physical objects like jewelry that have value. Nevertheless, value continues to exist due to trust and acceptance. Current legal and financial structures are not designed with a technology like this in mind. Financial institutions are built off of much older forms of currency. In some ways, it is comparative to the computing industry. The baseline of computing still relies on transmitting and processing 1‟s and 0‟s, providing only two dimensions of input. Yet all of our current technology uses this technologically archaic system due to adoption, cultivation, and lack of need for newer systems. If cryptocurrencies became the global norm for transactions, long standing systems for trade would need to be completely reformed to deal with this type of competition. For this reason, cryptocurrencies could possibly be the single most disruptive technology to global financial and economic systems.

.**2Strengths**

Bitcoin has strength by design to make it a viable currency that has elevated it in status over the years, more notably the fixed limit of bitcoin that will exist. Bitcoin will be mined with diminishing returns every four years until the maximum number of bitcoins are reached: a total of 21 million (King, 2013). This aspect of Bitcoin is important for its value. Due to the limited amount of bitcoins, it will never become inflated from an overabundance of bitcoins. Also, bitcoin and other cryptocurrencies are generally regarded as being protected from inflation originating from national government changes or restrictions (Margo, 2016). This creates a “safe haven” for investors to put their wealth into, as it generally does not lose value based on inflation. Bitcoin is quickly showing its strength as a refuge against inflating national currencies. However, as is the case with most commodities, the price can fluctuate wildly based on many other external factors. The combination of demand for a safe haven option and its price volatility helped Bitcoin to become the best performing currency of 2015 using the US Dollar Index (Desjardins, 2016). This means that Bitcoin was the highest valued currency in the entire world at the end of last year. This is no small feat in a global economy with powerhouses like China and the United States running the landscape.

**Figure 1**: **The Best Performing Currency of 2015**

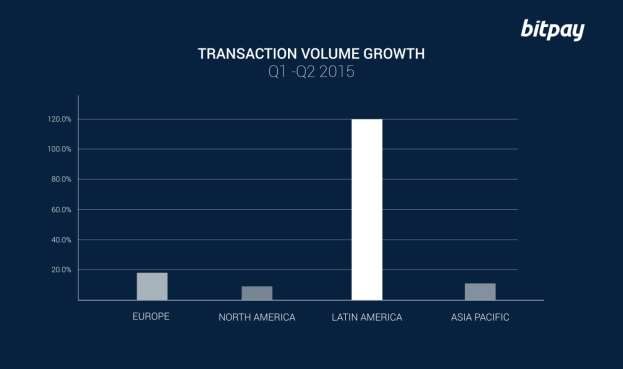
*Source*: Desjardins, J. (2016, January 5)



South America has seen a huge increase in bitcoin transactions, increasing 510% from 2014 to 2015 (Bitcoin: A New Global Economy, 2015). Argentina is a hotbed for increased cryptocurrency usage due to its extremely high inflation rate and high population of unbanked citizens (Magro, 2016). In the past, Argentinians would convert their currency into US dollars to preserve their value. However, Argentina has recently put restrictions on how many US dollars its citizens can convert. As a result, both a black market for purchasing USD at a higher price and increased bitcoin adoption has arisen (Magro, 2016). The demand for Argentinians to keep their currency value has made itself very apparent, and cryptocurrencies are prominent legal vehicles to meet that demand.

**Figure 2: Bitcoin Transaction Volume Growth**

*Source:* Bitcoin: A New Global Economy (2015)



**3. Weaknesses**

Bitcoin has quite a few internal weaknesses that are part of its design and cannot easily be modified. The public ledger, or block chain, means that every user can see every transaction. There is semi-anonymity, in that the owners of bitcoin wallets cannot be identified outright, but it is slightly nerve-wracking for some potential adopters. The public block chain is shared with all users, which means that it is susceptible to attacks due to easy access (King, 2013). So far, the Bitcoin network has been subjected to multiple “stress tests” that were essentially DDoS attacks (Hileman, 2016). These “tests” were launched by exchanges and miners to attempt to prove a point about Bitcoin’s design: that the network cannot handle a high load transaction rates. The mere fact that the participants of Bitcoin’s operation can bring the network down to prove a point is an unfortunate design feature of the code. These two aspects of Bitcoin’s design are integral to operation, and cannot be changed. Adoption by reluctant users must be in spite of these attributes.

Bitcoin has developed a questionable reputation through recent events. Stories like Silk Road can portray a negative image of digital currency in general, not just Bitcoin. Silk Road was an online marketplace buried in the dark-net, which allowed thousands of drug dealers and nearly a million customers to make illegal drug deals. Bitcoin was their primary means of transaction, due to the lack of government tracking and semi-anonymity. It ran from 2011 to 2013, and racked up nearly one billion USD in sales (Bearman, 2015). People want criminals to have justice meted against them, so the semi-anonymity attribute of bitcoin seems negative to law abiding citizens. Without positive marketing towards the value of semi-anonymity for normal users, the general user base will think that cryptocurrencies are only used by criminals.

Cryptocurrencies have also developed a reputation of having questionable security. Mt Gox, short for Magic the Gathering Online Exchange, was the world’s primary bitcoin exchange until it went bankrupt after it was robbed by hackers in 2011 of approximately 460 million USD (McMillan, 2014). The CEO and main programmer, Mark Karpeles, was not using version control for new code. He also would allow bug and security fixes to languish for weeks (McMillan, 2014). These security flaws and oversights allowed hackers to skim bitcoin from the exchange. This breach severely dropped Bitcoins value when users sold their bitcoin for fear of it getting stolen. Etherium, another form of digital currency, just recently suffered a similar form of theft to the tune of a 50 million USD hack (Price, 2016). These hacks are generally targeted at large holders of cryptocurrency that do not keep their security standards up to date. They are the main reason that the value of these currencies plummet, and do the most damage to the image of cryptocurrency. Until future organizations who exchange cryptocurrency understand how security flaws can lead to these attacks, these events will continue to hinder adoption.

Investors are beginning to realize that the bitcoin network has begun to stabilize, and immediate returns on investment are not guaranteed. The source code makes solving the algorithm more difficult starting in June 2016, increasing the cost of bitcoin mining. This is called a “halving event”, and it cuts the number of bitcoin returned to miners by half. This could effectively push out 25% of the bitcoin network that is running older computer hardware, as it would cost more to operate the machines than would be earned from mining (Kar, 2016). This shift in the mining community could make the network less secure and more vulnerable to attack. It also makes it less likely for new miners to enter the network due to the higher overhead required and limited returns on mining. The halving events continue, only the largest miners will exist until all of the bitcoin has been mined.

Cryptocurrencies‟ ability to be traded like a commodity can also be a weakness. Commodity based markets show a huge fluctuation in value from various events in the marketplace. This value fluctuation ultimately limits investor trust in the commodities. An unforeseen event could cause an investor to lose huge portions of money, decreasing investor trust. Also, determinates of bitcoin price have not truly been meted out, which creates an uncertain trading environment. Commodities are also prone to being traded by investors with a “buy low, sell high” mentality, which has overreaching effects to those who are using bitcoin for currency and create value fluctuations. Price volatility generates risk, which discourages both merchants and consumers from holding cryptocurrency for any significant length of time (PwC, 2015). Too much risk in lower’s consumer trust, which limits validation of legitimacy. Bitcoin’s price is also at risk from being in a shallow market, even though it has the highest capacity of all cryptocurrencies.

An individual who desires to purchase a large amount of bitcoin would not be unable to without affecting the current price (Kasiyanto, 2016). This is exponentially greater for other cryptocurrencies, who have a much smaller capacity. Cryptocurrencies do not seem to be a mature form of currency in its current market and state. Further growth in capacity and adoption would theoretically alleviate this problem.

**.4Opportunities**

Cryptocurrency is in a unique position as a forerunner in a possibly transformative technology to long standing financial systems. By its very nature, it is able to fill gaps in current financial technologies and be able to help solve traditional banking problems by being a peer-to-peer system. Napster, another peer-to-peer system, transformed the music industry by cutting out the middle man (Kelly, 2014). Transformative technologies start by solving a specific problem in an industry. For instance, cryptocurrencies are poised to help remediate the problems related to unbanked consumers. Significant portions of the population in developing countries are unbanked. In Latin America, 60% of 600 million inhabitants have no access to bank accounts (Magro, 2016). Bitcoin’s technology allows for individuals to exchange currency without needing a third trusted party, like a bank, to oversee the transaction. All that is needed to use Bitcoin is a mobile phone, which 70% of Latin Americans do have access to (Magro, 2016). Due to bitcoin’s ad-hoc networking capability, two users can trade bitcoin with each other by scanning QR codes displayed on their phones printed out by the application. This is a truly unique solution to a problem that has existed for many years for some people. This would invariably increase as the user base grows, so the demand for better cryptocurrency network and applications will come to the forefront. There is an enormous market for potential developers to create these applications, as this technology could affect any industry that relies on a trusted third-party clearing system (PwC, 2015). Any developers who increase usability through application and GUI improvements to bitcoin would be very successful. Bitcoin’s progression into becoming a transformative technology is driven by its ability to solve long standing problems, combined with a supportive and growing community of developers and users.

Businesses are beginning to see the value in using cryptocurrencies for international transactions, especially when transactions need to occur quickly in response to an emergency. Cryptocurrencies are solely positioned to solve this problem thanks to the speed and ease of transaction in the peer-to-peer system. Money can be wired internationally, but typically arriving days after being sent and not for the full amount (Team, 2016). The transaction can be hit with any number of unexplained fees as it crosses borders, making it difficult to send the correct amount to another business. A good example of this type of emergency need is an online company who is suffering from a denial-of-service attack and is looking to get immediate protection from a network security company (Team, 2016). In this scenario, speed is of transaction is of the essence, for every minute that the company’s website is down, profits are being lost. Cryptocurrency has a major advantage over traditional currencies thanks to its agility in making fast peer-to-peer transactions, especially in international business-to- business scenarios.

Internet marketplaces have been thriving and are true contenders to traditional brick-and-mortar stores. Amazon.com has grown to a degree that seems almost unexpected. They have even begun to hire “on-demand” delivery drivers, who use their own personally owned vehicle to deliver standard packages (Saito, 2016). This type of growth shows an attempt to further tighten control of the company’s logistics costs, which expand exponentially with increased business. Ebay.com already uses a paying system that is similar to Bitcoin called PayPal, and has been very successful in using it to facilitate all purchases made on its site. Silk Road was another example of a thriving online market, albeit it’s very illegal nature. It connected buyers and sellers who mostly used bitcoin to complete transactions. This marketplace showed how a digital currency can connect buyers and sellers without much interference by presiding governments and still succeed. Online shopping is thriving, and bitcoin is poised to extend its reach with efficient and easy payments for both vendors and customers. General purpose online shopping for individuals accounted for nearly 23 percent of transactions processed by Bitpay in the second quarter of 2015 (Kasiyanto, 2016). Cryptocurrency has the advantage over traditional card-based for the vendor in that it eliminates those fees.

International laws regarding taxation have been passed recently, creating validity for cryptocurrency as a mainstream device. Laws regarding the taxation of cryptocurrencies are required before digital currency could be considered a truly valid form of transactions. Towards the end of 2015, the European Court of Justice announced that it viewed bitcoin transactions as exempt from value-added tax (Hileman, 2016). Steps like this will significantly increase cryptocurrency flow.

Some users would refuse to use currency without knowing how it would affect their tax statements, regardless of what positive light in which they are viewed.

One of Bitcoin’s largest opportunities is that it can also act as a sort of commodity, similar to gold. The value of gold can spike considerably whenever an event threatens the balance of the global market, as we have seen with the Brexit vote. The precious metal saw an increase in value to a two-year high as investors became uncertain as to how the markets would react to the vote, using it as a safe haven (Reuters, 2016). The commodity market is a widely accepted form of trade worldwide, and cryptocurrency has seemingly begun to mimic the characteristics of gold. Gold has been a long standing holder of value, and that is based on the universal acceptance and trust of its value. Cryptocurrencies could potentially become a big player in the commodity market. They have a unique attribute of being purchased through a direct online mechanism, which creates easy entry for buyers. If bitcoin continues to be a valid refuge for inflating currencies, it will gain validity to investors and push deeper into becoming more mainstream.

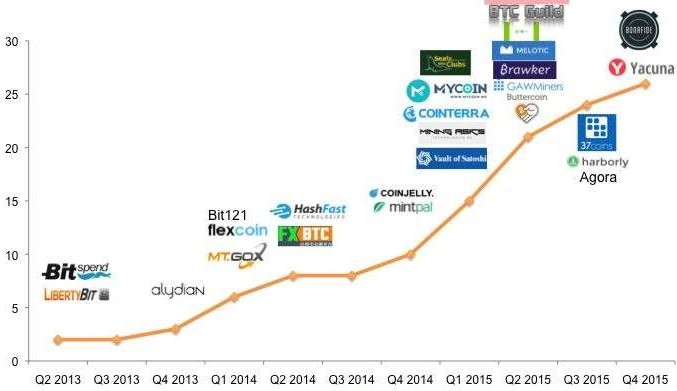
**.5Threats**

Bitcoin has quite a few hurdles to clear for user acceptance to become widespread. The value fluctuations that plague cryptocurrencies puts doubt in users, as well as investors. Ultimately a limiting factor in cryptocurrency is general acceptance. [PWC]. Value fluctuations reduce trust that a consumer’s value would be retained on a day to day basis, limiting faith in the currencies overall worth. In a survey performed by PwC, 83% of those surveyed had little to no familiarity of bitcoin (PwC, 2015). The lack of central ownership of cryptocurrencies means that any attempt to remediate this marketing problem using advertisements could theoretically help the investing company’s competition. This is not an ideal situation for a marketing plan. Cryptocurrencies have also seen fraud and theft, generally due to faulty system setups by exchange companies. These hacks generally make the news, and can easily convince the layman that they are unsafe locations to put their money. There is also a large gap in laws that cover the use of cryptocurrency. As long as cryptocurrencies remain in an area not generally covered by law, user acceptance will be limited. User’s need to trust that any transactions using cryptocurrencies are legal and binding. Markets and governments are slow to react to the new technology. Ultimately, all of these factors limit consumer’s trust in bitcoin and cryptocurrency.

This lack of trust leads to issues with investors as well. The dead pool of failed startups has increased to 24, mostly citing „security‟ as the main reason for closure (Hileman, 2016). This metric could be considered a watermark for future investors to consider before investing in bitcoin. The Mt Gox and DAO hack shows how inattentive organization can not only lose millions of dollars‟ worth of digital currency, but can drop the value significantly. New startups now know that a haphazard and unplanned launch is ill-advised at best, and new market entry will be limited. This could ultimately hurt bitcoin, as development of better software is important to improve security and user acceptance. As obvious of a concern as it may seem, security implementation and fixes are both generally slow to adapt for any new technology. Even the DAO hack exploit was documented as a potential problem weeks before the attack (Price, 2016). One of the issues with security is that the decentralized nature prevents a unified effort to completely secure every server that runs the code. A unified front in the realm of cryptocurrency may need to rise before the peer-to-peer network would become truly secured. A standards committee similar to ANSI, the American National Standards Institute, may need to be appointed for cryptocurrencies to develop security standards beyond the bitcoin application requirements. This type of regulation could only be implemented at the cost of the freedom of peer-to-peer networks, and may cause independent miners to exit the market.

# Figure 3: Bitcoin ‘Dead pool’ Grows to 26 Startups

*Source:* Hileman, G. (2016)



**.6 Conclusions**

Cryptocurrency seems to have move past the early adoption phase that new technologies experience. Even motor vehicles experienced this phenomenon. Bitcoin has begun to carve itself a niche market, which could help advance cryptocurrencies further into becoming mainstream; or be the main cause of it failing. Cryptocurrencies are still in their infancy, and it is difficult to see if they will ever find true mainstream presence in world markets.

The Bitcoin community is striving to push into the mainstream through innovation and solving old problems. Other forms of cryptocurrency have already emerged and have gained followings of their own, and each slightly different from Bitcoin and arguably as valid. Some nations like Iceland have even begun to start their own national cryptocurrencies (Hofman, 2014). It possible that the future holds a place for cryptocurrency as a major currency solution, and Bitcoin will be instrumental in paving the way for those currencies to flourish. The European and Latin America markets are exploding with Bitcoin transactions, signifying true validity. Further topics to explore regarding Bitcoin and cryptocurrencies are quite numerous. Extensive studies should be performed on the economic effects of Bitcoin’s effect on long standing fiat currency performance, and compare the results to countries that are beginning to adopt state-sponsored cryptocurrencies. The ability for cryptocurrency to perform micro transactions may allow it to bridge an economic gap that traditional state sponsored currencies would not be able to solve, but requires a much deeper market and economic analysis to determine. Also, the block chain technology that acts as Bitcoin’s backbone has potential uses in other ways, such as smart contracts (Hileman, 2016). These contracts are programmed payments that occur when a set condition occurs. Predetermined payment contracts are normally carried out by an entire accounting department of a company, making this an extremely interesting topic of further transformation. Lastly, cryptocurrency is a product of using cryptography to create a digital property. The frontier of digital property was popularized by the music industry’s shift to a cloud-based infrastructure. This frontier is still fairly new and unexplored, mainly populated by different types of media. Other forms of digital property may become as popular as music and cryptocurrency. Eight years ago, digital money was completely unheard of, and the creator of Bitcoin single handedly changed that. Cryptology, the root science beneath bitcoin and all cryptocurrencies, may be the mechanism behind the frontier for new and exciting digital inventions.

1. **References**

Bearman, J. (2015, May). The Untold Story of Silk Road, Pt. 1. Retrieved from Wired.com Website: https://[www.wired.com/2015/04/silk-road-1/](http://www.wired.com/2015/04/silk-road-1/)

Bitcoin: A New Global Economy. (2015, August 4). Retrieved July 2016, from BitPay, Inc. Website: https://blog.bitpay.com/bitcoin-a-new-global-economy/

Bovaird, C. (2016, June 24). Bitcoin Rollercoaster Rides Brexit As Ether Price Holds Amid DAO Debacle. Retrieved June 2016, from CoinDesk Website: <http://www.coindesk.com/bitcoin-brexit-ether-price-> rollercoaster/

Desjardins, J. (2016, January 5). It‟s Official: Bitcoin was the Top Performing Currency of 2015. Retrieved from The Money Project Website: <http://money.visualcapitalist.com/its-official-bitcoin-was-the-top-> performing-currency-of-2015/

Gerber, R. (2015, January 29). Why Apple Pay And Dollars Are Killing Bitcoin. Retrieved from Forbes Investing Website: <http://www.forbes.com/sites/greatspeculations/2015/01/29/why-apple-pay-and-dollars-are-> killing-bitcoin/#23ac58a0b4b6

Hileman, G. (2016, January 28). State of Bitcoin and Blockchain 2016: Blockchain Hits Critical Mass. Retrieved from Coindesk Website: <http://www.coindesk.com/state-of-bitcoin-blockchain-2016/>

Hofman, A. (2014, March 6). The Dawn of the National Currency – An Exploration of Country-Based Cryptocurrencies. Retrieved from Bitcoin Magazine Website: https://bitcoinmagazine.com/articles/dawn- national-currency-exploration-country-based-cryptocurrencies-1394146138

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/>

Kasiyanto, S. (2016). Bitcoin's potential for going mainstream. Journal Of Payments Strategy & Systems, 10(1), 28-39.

Kelly, B. (2014). The Bitcoin Big Bang: How Alternative Currencies Are About to Change the World.

King, R. S. (2013, December 17). By reading this article, you‟re mining bitcoins. Retrieved from Quartz.com Website: <http://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins/>

Magro, P. (2016, July 16). What Greece can learn from bitcoin adoption in Latin America. Retrieved July 2016, from International Business Times Website: <http://www.ibtimes.co.uk/what-greece-can-learn-bitcoin-> adoption-latin-america-1511183

**Team Members:**

**1- Fawy Tag ElDein Fawy**

* **Section 4 (General)**
* **Level 4 (batch 2017)**
* **ID: 162017109**
* **Team 51**

**…GitHub Link:**

* [**https://github.com/linuex007/FinalProject.git**](https://github.com/linuex007/FinalProject.git)

**The End.**