5-2019

Stability in Government, Emerging Technology, and Decentralized Economies: An Analysis of Alternative Uses of Cryptocurrencies

Mickayla Stogsdill
mstogsdi@vols.utk.edu

Stability in Government, Emerging Technology, and Decentralized Economies:

An Analysis of Alternative Uses of Cryptocurrencies

Mickayla Stogsdill

May 21st, 2019

Abstract

This project serves to analyze and investigate the emerging influence of cryptocurrencies in business, government, and global economies as a whole. Cryptocurrency use began in 2008 and has since found both widespread media attention and personal consumer interest. Cryptocurrencies such as Bitcoin, Ethereum, and Z-cash lead the way in innovative approaches to business transactions yet remain largely unregulated by the public sector. The literature review on past public policy related to cryptocurrencies is both a small sample and is mostly reactionary. It is crucial to analyze the effects and future implications of the risks of cryptocurrencies against possible different metrics to provide proactive policy.

In this project, I look to summarize the role of current cryptocurrencies and the role of a monetary system as a whole while leveraging the risks of cryptocurrency usage against different environments. To do this, I first examine six potential risks: risk 1: market capitalization, risk 2: private key knowledge, risk 3: transaction irreversibility, risk 4: account anonymity, risk 5: infrastructure distribution, and risk 6: market manipulation. Existing literature has explored the first five risks and has found mixed results looking backward on the effect of cryptocurrencies. In this project, I will be focusing on looking at forward projections in addition to risk six involving market manipulation. This project will utilize case studies and background cryptocurrency calculations against country stability to attempt to add to the growing body of knowledge that government, business, and ultimately the world will need in order to respond appropriately to the emerging world of crypto commodity and currency.

Author's Note: *This project is being submitted in Partial Fulfillment of the Requirements for the Chancellor's Honors Program Degree of Bachelor of Science and the Howard Baker Scholars Program.*

Table of Contents

BACKGROUND: WHAT ARE CRYPTOCURRENCIES?

It is significant to note that the average user and consumer of cryptocurrencies, most commonly Bitcoin, never has to understand the technical details and mathematical functions that are used to perform cryptocurrency transactions in order to utilize the technology for themselves. There are far longer papers detailing just how exactly cryptocurrencies work, so for this project the focus will remain on what aspects will be significant to the central thesis questions:

1.) How can cryptocurrencies affect underdeveloped, developing, and developed economies when treated as a currency rather than a commodity?

2.) To what extent can public policy be used to manipulate or incentivize the process of the emergence of crypto-currencies?

A general overview of cryptography and cryptocurrency technology will be useful in answering these questions. Cryptocurrency ("crypto") is the generic name for a collection of protocols which use a private key and public key pair to facilitate transactions between users. The reason they are called cryptocurrencies is because they use a mathematical technique called cryptography which can be used to hide data in plain sight (Nakamoto 1).

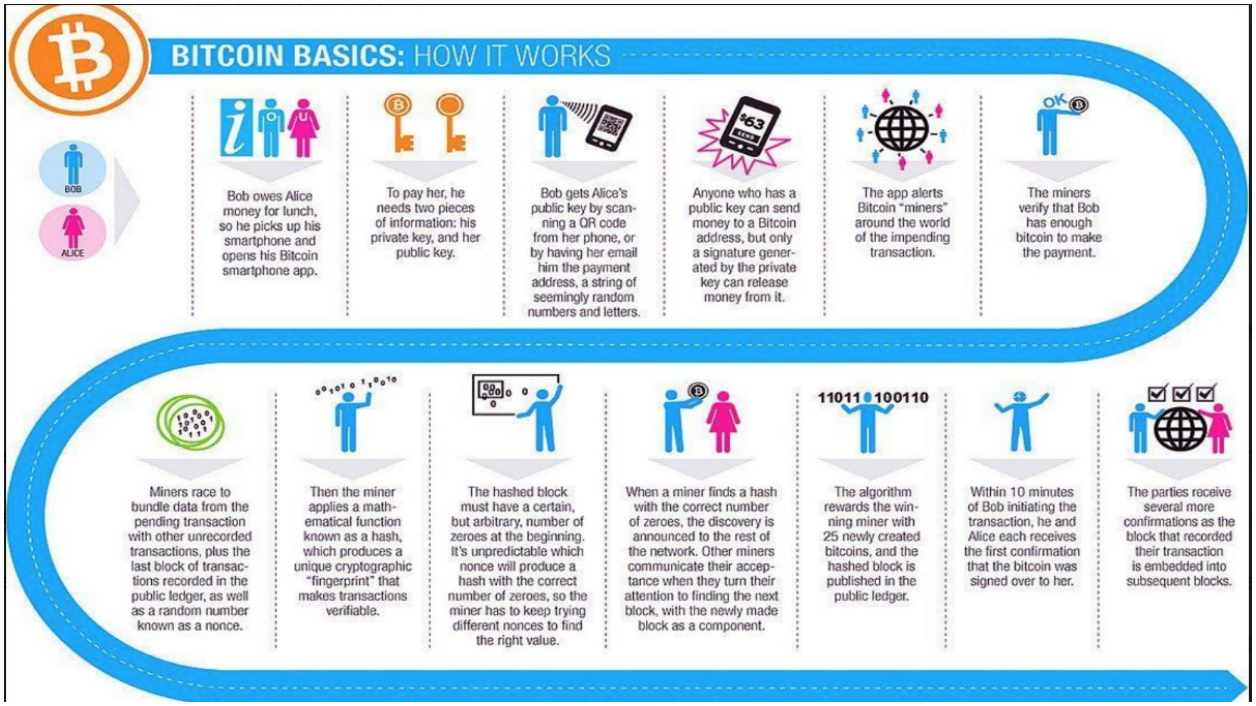
Release	Currency	Market Cap (April 23rd)	Hash Algorithm	Mechanism	Supply	Deflationary	Theoretical Long Term Inflation	Source
Jan-09	Bitcoin	$3,312,281,631	SHA-256	POW	21,000,000	yes		[2]
Sep-13	Ripple	$255,536,445	ECDSA	Byzantine Consensus	100,000,000,000	yes		[3]
Oct-11	Litecoin	$55,662,783	Scrypt	POW	84,000,000	yes		[15]
Jan-14	Dashcoin	$19,482,137	X11	POW & POS	22,000,000	yes		[16]
Aug-14	Stellar	$13,115,557	Undefined	Byzantine Consensus	Unlimited	no	1%	[13]
Jul-14	Bitshares	$11,688,038	Undefined	Undefined				[17]
Dec-13	Dogecoin	$10,841,501	Scrypt	POW	Unlimited	no	0%	[18]
Nov-13	Nxt	$9,606,282	Curve25519 and SHA-256	POS	1,000,000,000	yes		[19]
Aug-12	Peercoin	$5,073,573	SHA-256	POW & POS	Unlimited	no	1%	[4]
May-14	Monero	$4,433,105	CryptoNight	POW	18,400,000	yes		[20]
Jul-12	Bytecoin	$4,199,290	CryptoNight	POW	184,470,000,000	yes		[21]
Apr-11	Namecoin	$3,845,575	SHA-256	POW	21,000,000	yes		[22]
Jun-13	Ybcoin	$2,991,777	Scrypt	POW & POS	3,000,000	yes		[23]
Jan-14	Counterparty	$2,402,854	SHA-256	POB	2,650,000	yes		[24]
Aug-14	NuShares/NuBits	$3,901,430	Undefined	POS	1,000,000,000	yes		[5]
Dec-14	Paycoin	$2,294,250	SHA-256	POW & POS	12,500,000	yes		[25]
Sep-14	ARCHcoin	$2,228,501	Scrypt	POS	16,200,000	yes		[26]
Mar-14	Monacoin	$1,798,198	Scrypt	POW	105,120,000	yes		[27]
Nov-14	Faircoin	$1,201,450	Undefined	POS	Unlimited	no	1.50%	[28]
Jul-14	BitcoinDark	$1,133,283	SHA- 256	POW & POS	22,000,000	yes		[29]
Feb-14	Blackcoin	$1,113,916	SHA- 256	POS	Unlimited	no	1%	[30]

Farell, Ryan. *"An Analysis of the Cryptocurrency Industry."* p. 10

There are thousands of different kinds of cryptocurrencies, although Bitcoin is the most commonly considered (Sovbetov 3). Each crypto has its own pros and cons and should be analyzed and used in different contexts; there are also variations within the same kinds of cryptocurrencies called “forks” (Sovbetov 7). The overarching theme here is that cryptocurrency characteristics can change depending on the type - Bitcoin, Etherium, Z-cash, etc. - but there are critical attributes that are inherent to this peer-to-peer cash system. We will discuss each of these characteristics in detail below.

TRANSACTIONS

First, it is easiest to describe a cryptocurrency transaction compared to a Venmo or Cash App transaction with key differences italicized. Below is a simplified graphic detailing how a common transaction would take place using Bitcoin between two individuals, Bob and Alice.



Main, Ovan Ray. "Bitcoin Basics: How It Works."

Step 1: Similar to millions of daily transaction that occur today, two individuals named Bob and Alice may go to lunch and one party, Alice, offers to pay for the lunch in total via cash while the other individual, Bob, will pay her back via an cryptocurrency app on his phone. The

most common Bitcoin wallet is called Coinbase and can be used like an app similar to Venmo or Cash App (Rosenberg).

Step 2: In order for the individual to pay the other individual back, he will need two key pieces of information: his private key and her public key. A public key is similar to one's username; it is needed for Bob to pay Alice directly because it is the address to which Bob will send his Bitcoins. Bob's private key is loosely similar to his password in the fact that Bob ***should never tell anyone his private key***: "The sender's digital signature is an encryption using the private key, which can be unencrypted using the sender's public key. In this way, the sender is verified and the address of the recipient is known" (Dwyer 84).

Step 3: Bob can get Alice's public key by her telling him or commonly through scanning her QR code via the app Coinbase. The person in possession of the private key should be considered the owner of the Bitcoin. The list of all private keys a user possesses is called their wallet and is generally stored in a file labeled wallet.dat. This file is stored on a local device such as a hard drive.

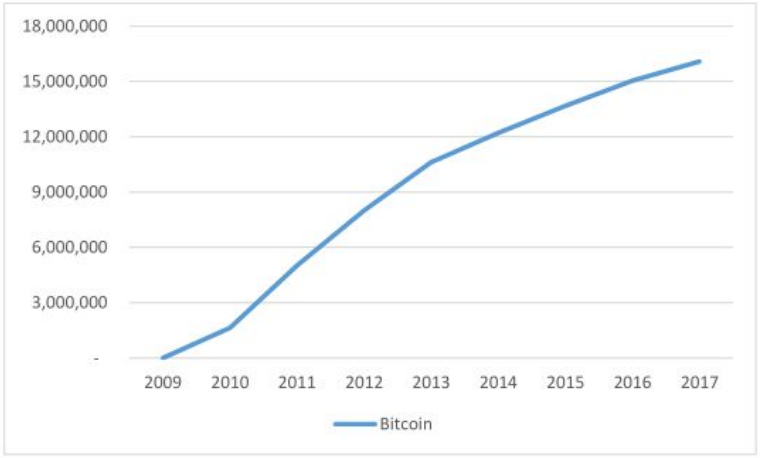
Step 4: This is where the cryptographic mathematics begin coming into question. Once Bob attains Alice's public key, there must be a unique signature generated by the secret private key in order to send Bob's Bitcoins to Alice. This press of a button on Bob's phone will alert Bitcoin miners globally of the transaction.

Step 5: Incentivized by the prospect of being the first miner to complete the hash function that will release the money from Bob's account to Alice's and in turn give that miner a small cut of Bitcoin to keep for themselves, the miners first verify that Bob has enough Bitcoin to pay Alice and then to bundle data from Bob's potential transaction and other transactions

happening globally. This bundle will be added to the public ledger, which is simply a long list of every transaction, and this public ledger leads to two very important traits of Bitcoin: 1.) its decentralization and 2.) its extraordinarily low likelihood of being counterfeit.

Step 6: Applying a mathematical function called a hash, miners create a cryptographic hash block which is singularly unique to each bundle of transactions. This hash block is a list of zeros, but it is unpredictable to foresee which nonce, or random number, can produce the correct number of zeros. This forces the miners to keep verifying different nounces; this leads to one miner discovering the correct number of zeros and it is subsequently announced to the entirety of the network. This block, once accepted by other miners, is added to the public ledger and rewards the fastest miner with a designated amount of ***new*** Bitcoins.

Exhibit 1 Bitcoin Supply over Time

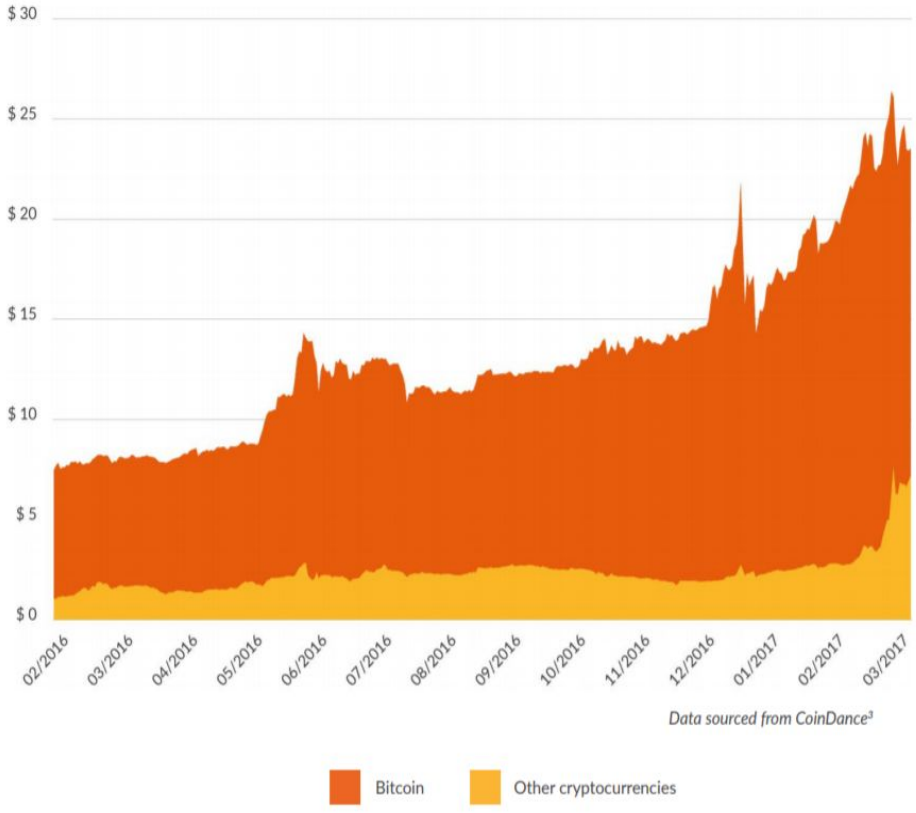


Kuo Chuen, David Lee and Guo, Li and Wang, Yu. *Cryptocurrency: A New Investment Opportunity?*

Step 7: Steps five and six are completely unseen by Bob and Alice who continue eating lunch. Within ten minutes of Bob sending Alice her Bitcoins, Alice is notified that the transaction went through and each of their transactions blocks are embedded with that transaction. This leads to another important characteristic: transactions using Bitcoin are virtually final and irreversible.

On every network there is a finite amount of possible coins available to any user. When initially released, not all Bitcoins were available. The new Bitcoins are available from the finite set which are accessed by facilitating new transactions, hence the name *mining*.

Figure 2: The total cryptocurrency market capitalisation has increased more than 3x since early 2016, reaching nearly $25 billion in March 2017



Hileman, Garrick, and Michel Rauchs. *"2017 Global Cryptocurrency Benchmarking Study."*

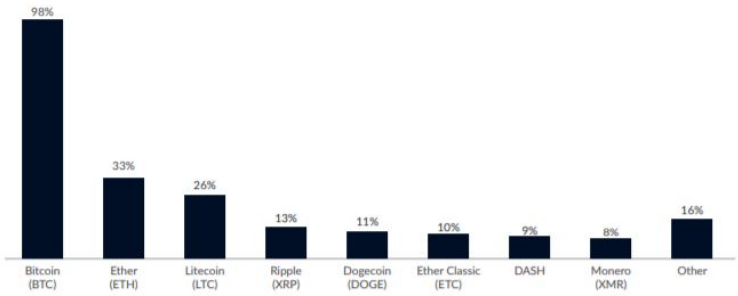
As a result of this finiteness and the speed at which transactions can be facilitated, the value of a cryptocurrency is decided by the market forces of supply and demand (Hileman 16). Additionally, all coding for the system is available and visible to any user meaning the control over the currency remains in the hands of the users and is nearly entirely decentralized. Transactions and their security falls to the general user and *eliminates* the need for centralized institutions such as banks (Hileman 20). This is why the currency is called decentralized; unlike a credit card, Venmo or Cash app, or even a dollar bill, peer-to-peer cash systems like Bitcoin do not need a central bank to give value nor regulate value over it; the USD and any other currency that is not a cryptocurrency is inherently tied to a centralized system of valuation. Rather than using single servers or as clients of other services, cryptocurrency data is sent directly across users who are connected to close-by networks.

Table 1: Average daily number of transactions for largest cryptocurrencies

	Bitcoin	Ethereum	DASH	Ripple	Monero	Litecoin
Q1 2016	201,595	20,242	1,582	N/A	579	4,453
Q2 2016	221,018	40,895	1,184	N/A	435	5,520
Q3 2016	219,624	45,109	1,549	N/A	1,045	3,432
Q4 2016	261,710	42,908	1,238	N/A	1,598	3,455
January - February 2017	286,419	47,792	1,800	N/A	2,611	3,244

Data sourced from multiple block explorers[a]

Figure 6: Bitcoin is the most widely supported cryptocurrency among participating exchanges, wallets and payment companies



Hileman, Garrick, and Michel Rauchs. *"2017 Global Cryptocurrency Benchmarking Study."*

By crowdsourcing transactions, verification, data transfer, and the coding processes, cryptocurrencies completely eliminate the need for any third party other than the users of the coins themselves. Although this description applies to most of the common cryptocurrencies, part of the advantage of the open source model is that it allows users to create alternative protocols which can use different mechanism and even serve completely different purposes. This basic background leads to both some fairly universal pros and cons about the usage of cryptocurrencies:

Pros	***Cons***
Cryptos are decentralized: no central bank is needed to ensure value nor verification	There is a smaller community that uses cryptos: it would be nearly impossible to complete transactions as fast as the status quo
Cryptos are more "anonymous" due to the decentralized nature and some cryptos such as Z-cash truly are "anonymous" because of its zero knowledge proof verification process	Must have internet to use cryptocurrency technology: mining, Coinbase app, etc.
Transactions are final, irreversible*	Transactions are final, irreversible*
Disputes in transactions can be disputed faster due to the public ledger	There is a slower verification process
Cryptos are cash-like and are near impossible to counterfeit	There is a slow adoption rate to cryptos
Cryptos have ubiquity: an individual can send Bitcoin to anyone, anywhere	Cryptos are easily manipulated and are largely unregulated

* This characteristic can easily be both a benefit and harm so it is included in both columns

COMMODITIES VERSUS CURRENCY

Although this paper and most other scholars will refer to Bitcoin and other cryptos as crypto*currency*, the term currency for today's societal use of Bitcoin and other cryptos is a heated debate. Some basic background of the differences in use and impact between the terms commodity and currency is vital. There are key differences between commodity money and fiat money: the biggest being that fiat money is only worth what we assign to it (like a $100 bill), while commodity money has some kind of scarcity tied to it (like a bar of gold). In society, individuals trade commodities, like gold or agricultural products, in order to turn those commodities in for fiat money. Individuals do not, however, trade $100 dollar bills in hopes that those $100 bills will increase in value; the value of fiat money is completely what financial actors decide to value it at: the physical piece of paper that says $100 on it *isn't actually worth that.* But in theory, commodity money in the form of gold or wheat is actually worth that $100 value due to the scarcity of the product (Khan Academy).

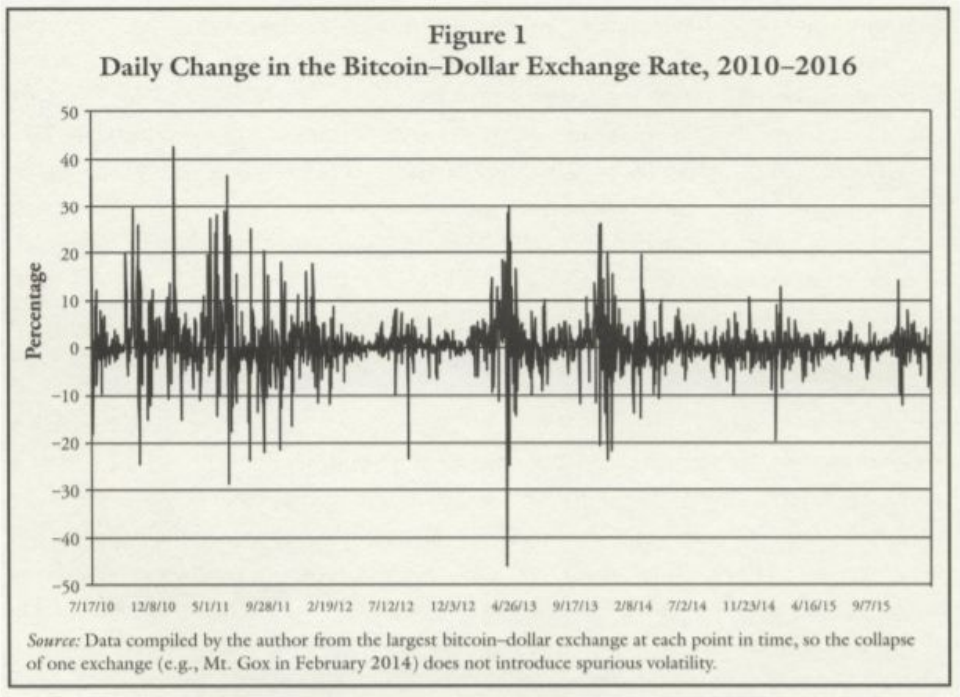
Money is something that:	***Money works best when it is:***
Stores Value	Durable
Medium of Exchange	Stable
Unit of Account or Standard of Value	Acceptable

LEGALITY OF CRYPTO-"CURRENCIES"

Currently in the status quo, cryptocurrencies, with an emphasis on Bitcoin, are practically and legally treated as commodities in the United States (U.S. Commodity Futures Trading Commission). According to Senior Judge Rya W. Zobel of the U.S. District Court for the District of Massachusetts who ruled on this specific case in September 2018, this was an important step for the US Commodity Futures Trading Commission (CFTC) to begin investigating crimes related to cryptocurrencies. However, this began a complicated legal battle between who, what, and how agencies regulate an entity that is socially treated like a quasi-currency and quasi-commodity. Although Bitcoin, which is considered the "original" cryptocurrency, specifically was always intended to be a means of exchange and another alternative for cash (Nakamoto 1). This ruling has serious consequences to the fate of Bitcoin and many other cryptocurrencies: "cryptocurrencies are here to stay" says US CFTC Chairman Christopher Giancarlo, one of the top derivatives regulators in America (Wilmoth). Both the financial sector and the basis for this thesis came from Giancarlo's at the time controversial statement in October 2018:

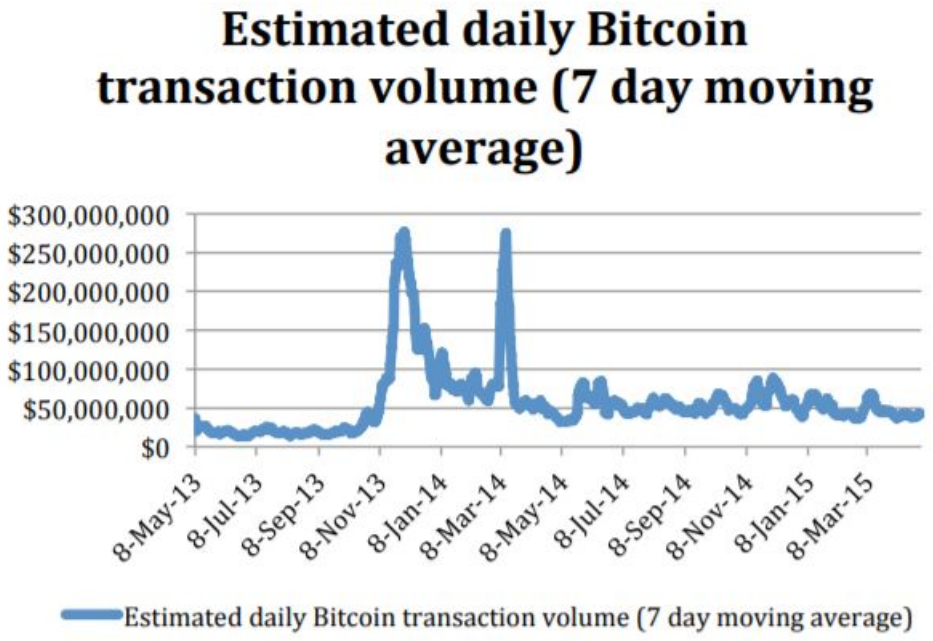
> "*there's a whole section of the world that really is hungry for functioning currencies that they can't find in their local currencies. There's 140 countries in the world, every one of them has a currency. Probably two-thirds are not worth the polymer or the paper they're written on, and those parts of the world rely on hard currencies. Bitcoin [or another] cryptocurrency may solve some of the problems."*

Not only did this statement send the financial sector into a frenzy, it began the conversation about the stability these crypto-commodities could be if used as crypto-currencies. At the time, day-to-day trades of Bitcoin were common, but could we ever imagine day trading a common dollar bill? Never. This assessment by a powerful actor in the United States financial regulation team began the shift of cryptos as a commodity toward a currency.



Harwick, Cameron. *Cryptocurrency and the problem of intermediation.*

When cryptos are used solely like commodities, there are several pervasive incentives: 1.) because cryptos have no actual internal value like gold or agricultural products, Bitcoin acts extremely volatile when traded and 2.) little to no regulation leads to miners “gaming” systems and reaping benefits that would not be seen if treated like a currency.



Farell, Ryan. *"An Analysis of the Cryptocurrency Industry."* p. 20

Farell, Ryan. *"An Analysis of the Cryptocurrency Industry."* p. 19

There are benefits to both the status quo with cryptocurrencies as commodities and the potential for them to become currencies. However, many countries have already either banned, although this action is largely unenforceable, or tried to restrict use of cryptocurrencies rather than leverage the benefits from blockchain technology.

Content/Scope	Country	Additional Information
Prohibition	China	December 5th, 2013, China's Central Bank prohibited financial institutions from handling Bitcoin transactions. Individuals and private parties can legally trade Bitcoin. [43]
	Russia	In February 2015, Russia's Prosecutor General's Office claimed that Bitcoin "cannot be used by individuals or legal entities." [44]
	Iceland	The Icelandic Central Bank said "it is prohibited to engage in foreign exchange trading with the electronic currency bitcoin, according to the Icelandic Foreign Exchange Act"[3]

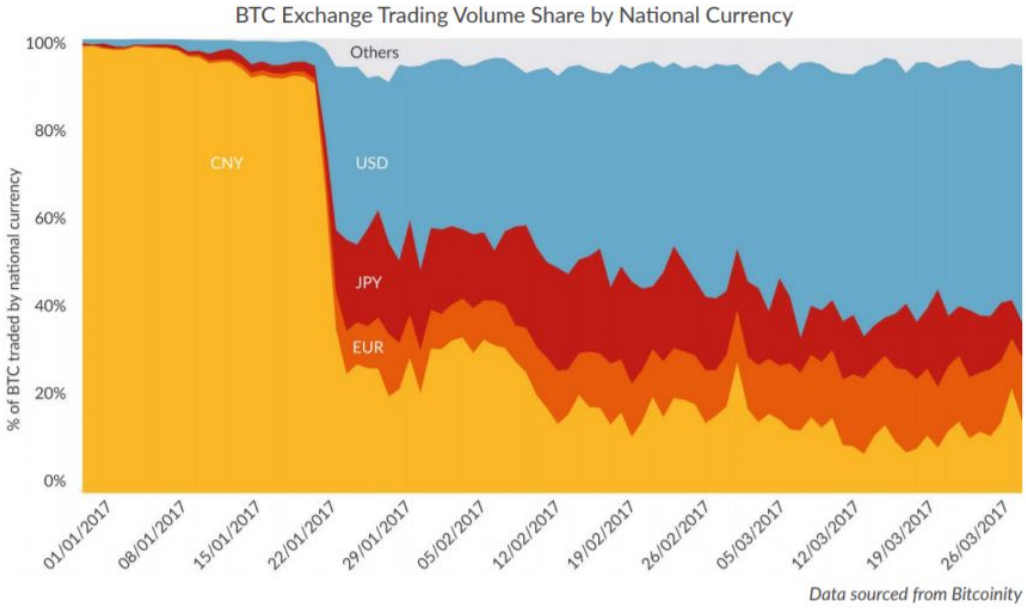
Farell, Ryan. *"An Analysis of the Cryptocurrency Industry."* p. 13

Prohibition of ATM's	Taiwan	Approval for Bitcoin ATMs refused.
Protection from money laundering & illicit activities	Singapore	Financial intermediaries to verify the identities of their customers and report suspicious transactions.
	USA	Bitcoin exchanges and most miners obliged to collect information on potentially suspicious transactions and report these to the federal government
Taxing Bitcoin		The sale, exchange or use of Bitcoin for payment in a real-world economy transaction may result in tax liability.
	Japan	The tax will cover gains from trading bitcoins, purchases made with bitcoins and revenues from transactions. Banks and securities firms will be prohibited from Bitcoin trades.
	Finland	Rules on taxation of capital gains apply when profits are in Bitcoin after it was obtained as payment is also taxable.
	Germany	Profits from mining or trading subject to capital gains tax unless hoarded for at least one year
Unclear	Israel	The Bank of Israel, the Capital Market, Insurance and Savings Department, the Israel Tax Authority, the Israel Securities Authority, and the Israel Money Laundering and Terror Financing Prohibition Authority issued a joint statement warning of the risks cryptocurrencies posed to users. However, no regulation has been established.
	India	The Reserve Bank of India's Secretary General, Ajit Prasad, said "The creation, trading or usage of virtual currencies including bitcoins, as a medium for payment are not authorized by any central bank or monetary authority." However, cryptocurrencies are currently not regulated.

Farell, Ryan. *"An Analysis of the Cryptocurrency Industry."* p. 14

Countries and areas where the government and national currency is unstable, like Chairman Giancarlo mentioned, could truly benefit from the cryptocurrency technology due to its decentralized benefit. Places where anonymous purchasing power and censorship circumvention is important for the safety of the people could also benefit. It is fairly certain at this point that policies and restrictions do have an effect on the use of Bitcoins and act like a deterrence.

Figure 14: Trading in renminbi has plumetted since Chinese authorities tightened regulation



Hileman, Garrick, and Michel Rauchs. *"2017 Global Cryptocurrency Benchmarking Study."*

Multinational corporations which have to convert between currencies frequently or multinational and international contracts which need to kept track of could be settled faster with more ease with the use of cryptocurrencies. The next section of this thesis will focus on the potential use cases of three primary cryptos: Bitcoin, Ethereum, and Z-cash.

LITERATURE ANALYSIS

Before applying any metrics to potential use cases, it is important to review the literature that has been done on the field of cryptocurrencies. This project has had several challenges, with a large and significant issue being the sheer amount of research that is being either privately funded by the private sector or government funding in the form of research grants. These incentives have led to a massive influx in the research available. The potential technology within cryptocurrencies has led to significantly more resources being poured in to study the effects of cryptocurrencies. The topic of a once underground online currency is now popping up in mainstream media like 60 Minutes and online research projects via massive multinational corporations such as Facebook.

Brief summary and timeline on the history of Bitcoin

The focus on research as I began this project in the fall of 2017 was mainly focused on the potential different forks and variations Bitcoin could produce (Kuo Chuen, Dwyer, and

Hileman). As time passed, more research began to surface that delved into the how cryptocurrencies could benefit the private sector regarding transaction time, dispute resolution, and other innovative solutions Ethereum specifically could offer business to business transactions (Dierksmeier and Baur).

The main research found ways to analyze large qualitative research questions which led to the risk-lens approach (Lansky). Some research seemed to question the role of the state if cryptocurrencies were to take flight (Atzori), but research was still lacking that addressed common-sense policy actions that should take place when the adoption of Bitcoins and other cryptocurrencies reached a level beyond mainly the black market.

As expanded upon further in the "Risks" section, the main contribution this project aims to meet is an additional public policy lens to the conversation surrounding cryptocurrencies. This type of lens has been largely untouched by past literature on this issue and perhaps can contribute to a more proactive role in addressing cryptocurrencies rather than reactive.

POTENTIAL USE CASES

Bitcoin, Ethereum, and Z-cash are the three types of cryptos that will be focused on when analyzing the effects of cryptocurrencies on different types of economics and what kind, if any, public policy recommendations should be put in place.

Exhibit 3 Market Capitalization of Cryptocurrencies

No.	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)
1	Bitcoin	BTC	$41,008,872,596	$2,498.53	16,413,200	$1,669,970,000
2	Ethereum	ETH	$24,995,499,905	$269.28	92,822,076	$2,046,010,000
3	Ripple	XRP	$10,569,342,023	$0.276024	38,291,387,790*	$279,029,000
4	Litecoin	LTC	$2,109,484,112	$40.78	51,730,682	$547,445,000
5	Ethereum Classic	ETC	$1,881,721,498	$20.24	92,988,807	$285,136,000
6	NEM	XEM	$1,482,417,000	$0.164713	8,999,999,999*	$8,954,510
7	Dash	DASH	$1,249,325,507	$169.13	7,386,908	$44,395,300
8	IOTA	MIOTA	$1,082,988,384	$0.38963	2,779,530,283*	$6,107,400
9	BitShares	BTS	$676,530,938	$0.260568	2,596,370,000*	$103,575,000
10	Stratis	STRAT	$666,034,742	$6.77	98,440,369*	$11,205,900
11	Monero	XMR	$625,404,471	$42.57	14,691,754	$14,801,000
12	Zcash	ZEC	$511,623,362	$329.56	1,552,444	$35,928,300
13	Bytecoin	BCN	$434,915,240	$0.002376	183,065,167,227	$2,490,360
14	Siacoin	SC	$428,467,781	$0.015721	27,254,659,755	$28,877,300
15	Waves	WAVES	$426,407,000	$4.26	100,000,000*	$5,813,100

*Not Mineable

Kuo Chuen, David Lee and Guo, Li and Wang, Yu. *Cryptocurrency: A New Investment Opportunity?*

Bitcoin and Ethereum are the top two cryptocurrencies in terms of market capitalization and are the top and third spot for per-coin price, with Ethereum coming in third only to Z-cash. All three cryptocurrencies have different properties, but the following main characteristics are why these cryptos will be focused on: Bitcoin due to its market share and popularity, Ethereum due to it business capitalisation and unique business-to-business transaction style, and Z-cash for its use of a zero knowledge proof and truly “anonymous” nature.

All three of these currencies also illustrate how capable cryptocurrencies are at presenting solutions to vastly different societal and economics problems in the status quo. This thesis will focus on and present six different potential use cases, each of which highlight a different function in which a cryptocurrency could serve the three overarching types of economies: underdeveloped, developing, or developed.

For the first set of use cases, the focus shall be on two specific underdeveloped nations. Argentina and Sudan. First, Argentina is a potential example of how cryptocurrencies such as

Bitcoin could be used to back the value of a local currency in a time when it is desperately needed (Brown). Prior to America's abolition of the gold standard, the United States kept a stockpile of physical gold to sustain the valuation of the dollar. Since then, most developed nations have done away with a national standard for their currency. However, Argentina, where the national currency is far from stable, a decentralized cryptocurrency could provide a less volatile entity to sustain the value of the currency. While inflation rose by more than 50% in Argentina, the value of Bitcoin remained relatively stable in 2018 (Brown). This indicates a very useful potential case in which Bitcoin could serve a role the local currency simply has not. In nations with unstable governments and by extension unstable currencies, cryptos could serve the role of stabilizing those national valuations. If a currency were to be localized within these potential nations, decentralized cryptocurrencies *could* maintain an average value which *could* outperform the centralized national currency; these *could* statements will be further developed next in the "Risk" section.

Sudan provides another example of a developing nation where this idea that a decentralized currency *could* be more beneficial than the centralized status quo *could* be taken even a step further. The Central Bank in Sudan has recently placed strict restrictions on the national currency and therefore significantly harmed consumer buying power and personal economic freedom (Brown). In response, many Sudanese citizens have acquired and started to use Bitcoin as a form of currency instead (Kantchev). This organic use of Bitcoin as a currency highlights a second potential use case where cryptos *could* replace a currency entirely and *could* end in a scenario with greater benefits than harms. By adopting cryptocurrencies into localized economics, countries such as Sudan *could* begin to see a currency unaffected by centralized

government corruption or instability in large financial actors such as banks. Countries such as Kenya and South Africa have also started to adopt this procedure but have seen mixed results, mainly dependent on the quickness of the local adoption rates (Kantchev). In this way, cryptocurrencies could be used in the way they were originally envisioned as a currency to replace the centralized standard (Nakamoto 1).

Developing nations seem to have more specialized uses for cryptocurrencies than underdeveloped nations. Censorship circumvention, for example, could be very useful in nations such as China or Russia. These countries will serve as the main focus when analyzing the effects of cryptocurrencies on developing nations. In both of these countries, the government has cracked down on freedom of assembly and anti-government activism through internet censorship (Sherman). This includes an inability for many citizens to access or use international services which require online transactions. Since cryptocurrencies work on peer-to-peer networks and cryptos such as Z-cash are completely anonymous, citizens of these countries could circumvent such restrictions if they switch to decentralized cryptocurrencies. The use of cryptos in these developing nations could facilitate more groups to take an active role and improve their abilities to organize due to economic freedom being a major factor in the government's ability to control and suppress. A protocol which was recently developed at Purdue University explores this possibility further. Building off of the currency Z-cash, "R3C3" is a protocol which users can use to organize rendezvous and assemble (Minaie 1). The use of protocols like this could improve the democratic process in other nations by allowing the grassroots movements a means of organizing. Both China and Russia's potential in the world of cryptocurrencies will be assessed compared to the risks of crytos in the next section.

When moving the focus toward developed nations, the need for cryptocurrencies may not be as obvious. However, there is no shortage of potential usage for cryptos in these countries. The use of cryptocurrencies as a commodity to be exchanged is most widespread in developed nations such as the United States, most of Europe, and parts of Japan. With the previous examples, part of the motivation for the use the cryptocurrencies relied on internal instability within the government. Why then would a country with a *stable* currency still switch to a cryptocurrency as its main form of currency? Could it? Should it? Would it?

The two countries that will be the focus when analyzing developed nations will be the United States and Japan. Firstly looking at Japan, the answer to at least the *could* question seems to be yes. Japan currently is attempting to eliminate cash transactions in addition to credit card systems; instead, the country is looking into minting their own cryptocurrency (Orcutt). This development makes Japan quite a different potential case than the others. In Sudan, the potential came from citizens looking for a stable currency and in Russia, the incentive may be to escape some level of censorship. For Japan, the government is taking an *active role* in transitioning the country toward cryptocurrencies. Japan could also provide researchers a genuine case study of whether developed economies could switch to cryptocurrencies. If Japan is successful in this endeavor, the country may be able to acquire all the benefits of cryptocurrencies while sustaining a well regulated economy; however, we will see in the next section mixed results when comparing the different lens of risk.

Regarding the United States, the switch to full adoption of cryptocurrencies may not be as easy considering the market structure of the US banking system. However, America is home to more international corporations than almost any other country, effectively making it a major

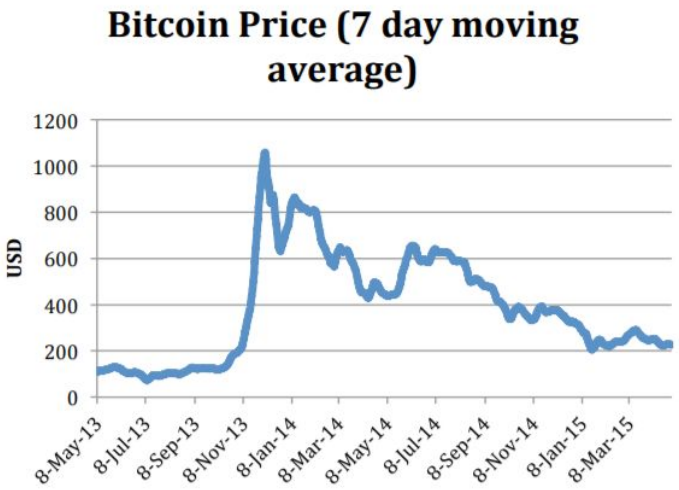
player in global trade. In America's case, Ethereum and Bitcoin prove to be valuable resources in aiding necessary trade. Bitcoin offers multinational corporations a means of exchange which is not constrained by currency conversions. By using cryptocurrencies such as Bitcoin more often, international exchanges *could* be simplified and made cheaper. Additionally, the "Smart Contracts" from Etherium could also serve a unique role in reducing the legal costs of maintaining and adhering to contracts since it can effectively keep track of contractual obligations without a third-party use of a lawyer (Sovbetov). These potential benefits pose great potential for American business worldwide but will require stronger and well-developed regulation to prevent exploitation and tax avoidance. The same type of risk-lens approach will be taken with all three types of economics and potential uses below.

RISKS

The vast majority of reliable past research has concluded that there are at least five major risks to consider when measuring any potential benefits or harms associated with Bitcoin, Ethereum, and Z-cash (Lansky 24-26). These fives risks include:

1.) ***Market capitalization: how many coins are there and who has them?***

In general, Bitcoin, Ethereum, and Z-cash along with all other cryptocurrencies have a low market capitalization, meaning not a lot of the potential actors that could be using cryptos actually are using them. Because of this low market capitalization and treatment of cryptocurrencies like commodities, this creates an environment rich of volatility.

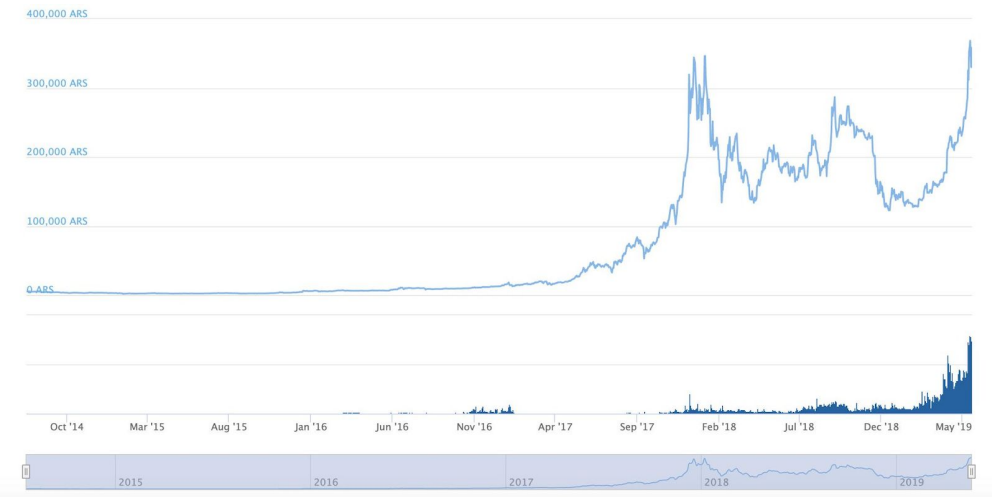


Farell, Ryan. *"An Analysis of the Cryptocurrency Industry."* p. 20

Moreover, The result of legal commodification is that adoption as a currency seems less likely and now can be more easily regulated. This regulation could prevent further adoption.

2.) ***Private key knowledge: what if someone steals an individual's private key?***

As stated earlier, if an individual loses their private key, it is similar to sharing their unchangeable password. Although the impact depends on the type of crypto, this can still be a costly mistake. Even looking at a particularly volatile week, Bitcoin prices fluctuated from a low of around 1BTC:$100 USD to a high of around 1BTC:$1,300 USD. In the US, Bitcoin has its all time high of 1BTC:$19,891 USD in 2017. But in countries with poor fiat currency value such as Argentina, 1BTC:$375,000 ARS (Brown).



Brown, Ben. *"Bitcoin Price Hits All-Time Highs in These Countries, Thanks to Crippling Fiat."*

Combined the risk of transaction irreversibility, this risk is especially impactful in that it can potentially destroy and empty entire accounts (Lansky 25). This risk in dependent on consumer awareness and knowledge and is one of the biggest risks that perhaps public policy regulation can address.

3.) ***Transaction irreversibility: what happens when a legitimate mistake is added to the public ledger?***

The vast majority of cryptos, including Bitcoin, Ethereum, and Z-cash, have transactions that cannot be reversed. There was a famous case of an Ethereum fork, which in turn created Ethereum Classic, which changed the new public ledger to allow the stolen funds back to its rightful owners; however, 10% of the community disagreed with the fork and remained as Ethereum Classic (Lansky 25 and Castilo). It is helpful to remember that a fork is simply a computational split of the public ledger which in turns creates two versions of the same cryptocurrency, now with two separate and distinct public ledgers.

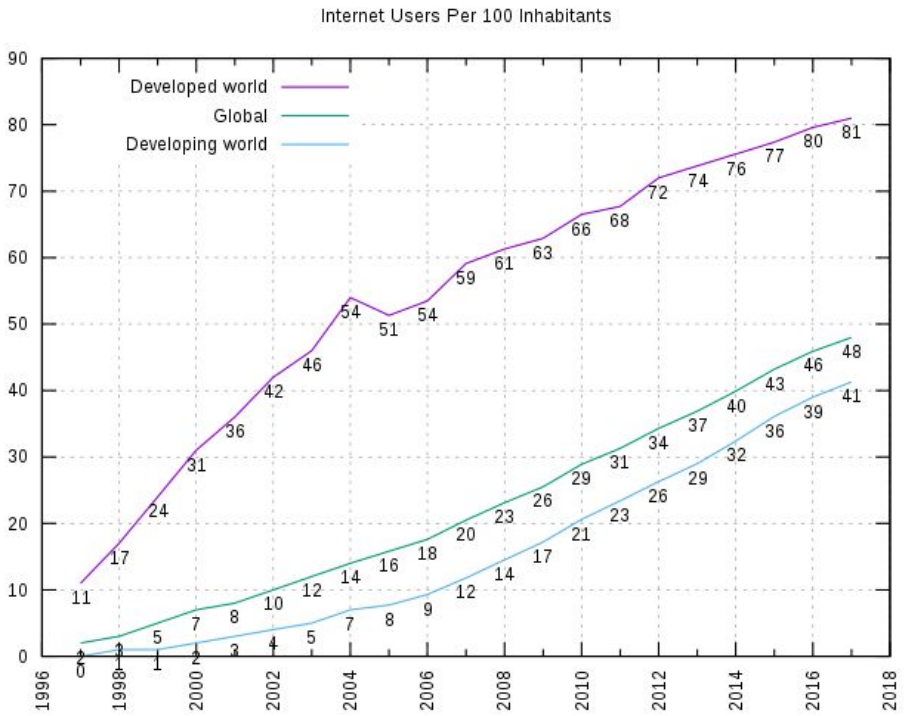
4.) ***Account anonymity: what defines anonymity and can the transactions be as anonymous as cash?***

Although there is some level of a spectrum when it comes to how anonymous cryptocurrencies can be, cryptocurrencies are typically viewed as more "anonymous" than say an average American bank. However, this discussion truly depends on the framing and definition of the word "anonymous." If one is discussing the viewpoint of anonymous as the ability to track someone's *name and identity,* cryptos in general will shield better than a centralized banking system. This is because no name needs to be associated with a transaction using Bitcoin or Ethereum or Z-cash; an American bank transaction typically requires some level of documentation and most likely an account which include private details such as one's identity. When discussing the anonymity of transactions, the result is flipped. Because of the use of a public ledger, it is very possible for any Bitcoin user to track any transaction made; privacy laws and confidential transactions would prevent this type of open information via an American centralized bank.

5.) ***Infrastructure distribution: can everyone have a computer and internet?***

As of April 2019, only 56% of the world has internet access and over 80% of the developed work can access the internet (Miniwatts Marketing Group). This means the part of the world US CFTC Chairman Giancarlo predicts would most benefit from the cryptocurrency technology is disproportionately disconnected from blockchain altogether. There are various businesses, such as SpaceX or Google, which are launching

long-term initiatives to provide internet to all people (Mosher). It is definitely worth noting the potential political backlash that intensifies the risk of infrastructure distribution. Many countries may not ***want*** to see the benefits that come from a decentralized and less volatile currency than that country's status quo and therefore may thwart efforts towards adoption, affecting both risk one and risk five.



ICT Statistics *"Global ICT Developments."*

In addition to these five risks, this project will add a sixth risk in an attempt to address the public policy recommendations and challenges. This sixth lens of risk has largely remained untouched in conjunction with the other lens of risk.

6.) ***Market manipulation: how susceptible to bad actors is the cryptocurrency in the status quo and after any proposed policy change?***

This risk, along with others, is further exacerbated when combined with the effects of other risks. In general, cryptos are more susceptible to market manipulation when adoption rates and government regulation is low (Coleman). However, because cryptocurrencies are based somewhat on a level of trust - 50+% of the community must tell the truth when verifying the public ledger in order for the ledger to publish - there will always be a potential for some level of manipulation. Mining, due to economies of scale, will inevitably become profitable to the largest mining firms due to more computational speed and power given to each set of transactions. Moreover, without any level of proactive regulation, there is little to stop third-party wallets such as CoinBase from extorting and manipulating their account, sometimes without the consumer ever knowing.

Below is a simplified table detailing each of the six risks along potential solutions to ease or completely eliminate each risk. The solution in the left column is typically less preferred while the solution in the right column is more preferred.

Risks	***Solutions to Ease Risks***	
Low Market Capitalization	Movement Away from Commodity Use and Movement Toward Strict Currency Use	Gradual Adoption Rate Increases through incentives

Private Key Knowledge	Public Government Regulation (widely varies)	Private Company Regulation (widely varies)
Transaction Irreversibility	Hard Fork Reversals (similar to Ethereum's 2016 fork which cost Ethereum 10% of its community)	Third-party (perhaps governmental) oversight and use of a third-party arbitrator
Account Anonymity	Less Anonymous: government regulation requiring names to be associated with private keys in a national database	More anonymous: cryptos should move toward zero knowledge proofs (like Z-cash) which allow complete anonymity via its inherent mathematical attributes
Infrastructure Distribution	Third-party private attempts to bring internet access globally (Ex. SpaceX's Starlink internet satellite plan or Google's global internet cable progression)	Global foreign aid attempts to encourage countries to increase their internet infrastructure; countries would be less likely to destroy work their own government and people paid partly for
Market Manipulation	Forced Adoption Increase in order to allow more actors into the community	Government Regulation of Markets similar to regulation of the stock market

RISK-LENS APPROACH

Below are three tables which detail how each of the six risks affect the six different potential use cases. The overall effects are qualitative and will inevitably be debatable; this risk-lens approach will be used to construct the overall policy recommendations used in the next and final section of this project.

Underdeveloped Nation Cases

	Argentina	*Sudan*	*Overall Effect (+,-,~)* *+ Positive* *- Negative* *~ Neutral*
Low Market Capitalization	At the point in time that Argentina's currency is **more** volatile than the current crypto market in Argentina (Brown), the low market capitalization effects would be a more **positive** effect than remaining in the status quo	At the point in time that Sudan's currency is **more** volatile than the current crypto market in Sudan (Brown), the low market capitalization effects would yield more **positive** effect than remaining in the status quo	*Argentina:* + *Sudan:* +
Private Key Knowledge	Although the damages would be significantly impactful due to Argentina's currency valuations, there do not seem to be outside influences that would worsen this risk within these two countries	Although the damages would be significantly impactful due to Sudan's currency valuations and previous government intervention, there do not seem to be outside influences that would worsen this risk within these two countries	*Argentina:* ~ *Sudan:* ~
Transaction Irreversibility	Argentina faces no significant outlying effect that would hold dispute resolution as a	Sudan faces no significant outlying effect that would hold dispute resolution as a	*Argentina:* + *Sudan:* +

	major factor in their economy (Ex. US will face disproportionate effects of this risk) and ability for transaction to be final eliminate possible government corruption or intervention (Kantchev)	major factor in their economy (Ex. US will face disproportionate effects of this risk) and ability for transaction to be final eliminate possible government corruption or intervention (Kantchev)	
Account Anonymity	There are not significant factors that sway the risk of account anonymity either way in Argentina	There are not significant factors that sway the risk of account anonymity either way in Sudan	*Argentina:* ~ *Sudan:* ~
Infrastructure Distribution	Argentina's internet infrastructure is above the world's average yet below the developed country average making infrastructure distribution a generally neutral issue (Internet World Statistics) that can be improved on in the future but would not likely stop adoption of cryptocurrencies alone	Sudan faces some of the worst internet access in the world, with only 37.3% of African nations currently having free ability to the internet (Internet World Statistics), but private entities may alleviate this risk in the future (Mosher); the status quo infrastructure would make for a difficult adoption of cryptos	*Argentina:* ~ *Sudan:* -
Market Manipulation	Argentina faces a volatile government which has manipulated the national currency in the past (Brown) and has a disproportionately higher likelihood than other countries of national market manipulation when trying to adopt cryptocurrencies	Sudan also faces a volatile government (Brown) and has a disproportionately higher likelihood of market manipulation when trying to adopt cryptocurrencies	*Argentina:* - *Sudan:* -

Developing Nations Cases

	China	*Russia*	*Overall Effect (+,-,~)* *+ Positive* *- Negative* *~ Neutral*
Low Market Capitalization	China's currency, the yuan, is valued at $1USD:$.14YEN. Although the currency is not as prone to extreme level of volatility and inflation as the underdeveloped counterparts, there are concerns that low market capitalization would yield the same results as the current state of the yuan	Russia's currency, the ruble, is valued at $1USD:$.016RUBLE Although the currency is not as prone to extreme level of volatility and inflation as the underdeveloped counterparts, there are concerns that low market capitalization would yield the same results as the current state of the ruble	*China: ~* *Russia: ~*
Private Key Knowledge	China's government poses a real threat to individual safety within their own country (Sherman) so private key safety may be a concern for this type of government (Lansky)	Russia's government, although more hands-off than China, poses a real threat to individual safety within their own country (Sherman) so private key safety may also be a concern for this type of government (Lansky)	*China: -* *Russia: -*
Transaction Irreversibility	Due to the governmental control discussed above, transaction irreversibility probably will work in favor of citizens in China so that no transaction may be	Due to the governmental control discussed above, transaction irreversibility probably will work in favor of citizens in Russia so that no transaction may be	*China: +* *Russia: +*

	reversed in light of political motivations	reversed in light of political motivations	
Account Anonymity	Due to the governmental control discussed above, account anonymity probably will work in favor of citizens in China so that no transaction may be traced to a single individual in light of political motivations	Due to the governmental control discussed above, account anonymity probably will work in favor of citizens in Russia so that no transaction may be traced to a single individual in light of political motivations	*China:* + *Russia:* +
Infrastructure Distribution	China faces somewhat worse conditions than Russia, in that only a little over 50% of Asia has internet access (World Internet Statistics) . However, China's internet infrastructure is fairly modernized and could be utilized if allowed	Russia is split between Europe and Asia; due to Siberia's vast amount of land and harsh condition, Russia faces some gaps in internet infrastructure that also pose risks to adoption; however, most of the nation is centralized in the cities which enjoy higher quality internet access	*China:* ~ *Russia:* ~
Market Manipulation	China in 2013 banned all transactions involving Bitcoin (Farrel); this law has been enforced and the Chinese government would likely manipulate any large-scale adoption trends (Lansky)	Russia banned the use of cryptocurrencies in 2015 (Farrel) yet has largely left the issue unenforced (Sherman)	*China:* - *Russia:* ~

Developed Nation Cases

	Japan	*United States*	*Overall Effect (+,-,~)* + *Positive* - *Negative* ~ *Neutral*
Low Market Capitalization	The Japanese Yen remains a strong currency with little volatility; low market capitalization would near likely cause significant economic disruptions	The United States dollar remains a strong currency with little volatility; low market capitalization would near likely cause significant economic disruptions	*Japan:* - *US:* -
Private Key Knowledge	There are not significant factors that sway the risk of account anonymity either way in Japan	There are not significant factors that sway the risk of account anonymity either way in the US	*Japan:* ~ *US:* ~
Transaction Irreversibility	Japan faces a complex developed economy rich in white collar contract disputes that would make the risk of irreversible transition more harmful (Orcutt)	The United States faces a complex developed economy rich in white collar contract disputes that would make the risk of irreversible transition more harmful (Sovbetov)	*Japan:* - *US:* -
Account Anonymity	Japan, due to its very welcoming nature of cryptocurrencies (Orcutt), will not face significant harms from the risk account anonymity	The majority of the US Bitcoin market is within the black market (Hileman); the United States government is not as open toward cryptocurrency adoption and will likely find account anonymity a harm	*Japan:* ~ *US:* -

Infrastructure Distribution	Japan's internet infrastructure has high integrity and is accessible to the vast majority of the nation	The United States' internet infrastructure has high integrity and is accessible to the vast majority of the nation	*Japan:* + *US:* +
Market Manipulation	Although there remains cases on individual and private market manipulation within Japan, regulatory forces are advanced and could manipulate the market in fair and equitable ways if adopted	Although there remains cases on individual and private market manipulation within the US, regulatory forces are advanced and could manipulate the market in fair and equitable ways if adopted	*Japan:* + *US:* +

PUBLIC POLICY RECOMMENDATIONS

There are two primary types of policy a government can pursue in the world of cryptocurrencies that were shown through this thesis project: growth policies and protectionist policies. Growth policies are mainly concerned with the following four criteria: the promotion of cryptocurrencies and incentives toward adoption, recognizing cryptos in the market, reducing restrictions on cryptocurrency usage, and increasing overall access to needed technology in order to reap full potential of the blockchain. Protectionist policy is mainly focused on the following four criteria: increasing government ability to regulate specific cryptocurrencies, research faults and failures through public grants and research funding, increasing the restrictions on

cryptocurrency usage, and creating financial protections for users of cryptos. The central question remains: should there be more creation of growth or protection policies? The answer probably lies in between and depends on the conditions facing the community. The idealistic goal is to create growth policies that make it a realistic and viable option for average consumers to use the benefits of cryptocurrencies while also developing protection policies which reduces risk to consumers and lowers volatility in the national financial market.

The goal of growth policies is to grow the cryptocurrency market and make it easier for adoption rates to increase since market size is a major factor in safety and security; growth policies have less of a focus on risk and consumer-driven policies than protectionist policies. On the other hand, protectionist policies put less priority on market capitalization and economic growth within the cryptocurrency market. Below is a table analyzing the differences in growth and protectionist policies:

Growth Policy Examples	***Protectionist Policy Examples***
Allow for certain national programs to accept cryptocurrencies in addition to USD (or equivalent currency)	Incentivizing a gradual increase in crypto adoption rates to decrease market volatility
Promoting access to technology in the US and other countries	Government regulation protecting account anonymity and perhaps providing grants for new cryptos with a focus on account and transaction privacy
Using Smart Contracts in international and large-scale national contracts	Strict regulation to avoid consumer turmoil due to market manipulation

CONCLUSION

With Bitcoin coming into existence in 2008, eleven years of cryptocurrencies have seen massive, extraordinary, and impactful changes that will inevitably continue to affect financial markets and consumer decisions around the world. There is still much research to be done about the effects and risk management of the currently volatile means of exchange; identifying risks against its potential will help develop new ways to understand and innovate the current blockchain technology.

References

1.) 60 Minutes. *"Where in the world is Bitcoin's mysterious creator, Satoshi Nakamoto?"* *Youtube*, 19 May 2019. https://www.youtube.com/watch?v=wQd1CpNzDx4

2.) Atzori, Marcella, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* 1 Dec. 2015. https://ssrn.com/abstract=2709713 or http://dx.doi.org/10.2139/ssrn.2709713

3.) Baur A.W., Bühler J., Bick M., Bonorden C.S. (2015) *Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co. In: Janssen M. et al. (eds) Open and Big Data Management and Innovation.* I3E 2015. Lecture Notes in Computer Science, vol 9373.

4.) Brown, Ben. *"Bitcoin Price Hits All-Time Highs in These Countries, Thanks to Crippling Fiat."* CCN, 20 May 2019, www.ccn.com/bitcoin-price-rockets-all-time-highs-countries-crippling-fiat.

5.) Castilo, M., 2016: *Ethereum Executes Blockchain Hard Fork to Return DAO Funds.* CoinDesk. http://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investorfunds/

6.) Coleman, Lester. *"Bitcoin Price Manipulated by Cryptocurrency Trading Bots: WSJ."* CCN, 2 Oct. 2018, www.ccn.com/bitcoin-price-manipulated-by-cryptocurrency-trading-bots-wsj.

7.) Dierksmeier, C. & Seele, P. J *Bus Ethics* (2018) 152: https://doi.org/10.1007/s10551-016-3298-0

8.) Dwyer, Gerald P. *"The Economics of Bitcoin and Similar Private Digital Currencies."* Journal of Financial Stability, vol. 17, Apr. 2015, pp. 81–91., doi.org/10.1016/j.jfs.2014.11.006.

9.) Farell, Ryan, *"An Analysis of the Cryptocurrency Industry"* (2015). Wharton Research Scholars. 130. http://repository.upenn.edu/wharton_research_scholars/130

10.) *"Federal Court Finds That Virtual Currencies Are Commodities."* Federal Court Finds That Virtual Currencies Are Commodities | U.S. COMMODITY FUTURES TRADING COMMISSION, www.cftc.gov/PressRoom/PressReleases/7820-18.

11.) *"Global ICT Developments."* ICT Statistics, www.itu.int/ITU-D/ict/statistics/ict/.

12.) Harwick, Cameron. (2017). *Cryptocurrency and the problem of intermediation.* 20. 569-588.

13.) Hileman, Garrick, and Michel Rauchs. *"2017 Global Cryptocurrency Benchmarking Study."* SSRN Electronic Journal, 2017, pp. 1–114., doi:10.2139/ssrn.2965436.

14.) Kantchev, Georgi. *"Bitcoin Is a Hit in Countries Where Locals Face Currency Troubles."* The Wall Street Journal, Dow Jones & Company, 4 Jan. 2018, www.wsj.com/articles/bitcoin-is-a-hit-in-countries-where-locals-face-currency-troubles-1515067201.

15.) Khan Academy. *"Commodity money vs. Fiat money | Financial sector | AP Macroeconomics | Khan Academy." Youtube,* 20 June 2016. https://www.youtube.com/watch?v=fs12fX407GU

16.) Kuo Chuen, David Lee and Guo, Li and Wang, Yu, *Cryptocurrency: A New Investment Opportunity?* (August 24, 2017). Available at SSRN: https://ssrn.com/abstract=2994097 or http://dx.doi.org/10.2139/ssrn.2994097

17.) Lansky, Jan. *Possible State Approaches to Cryptocurrencies* - Si-Journal.org. www.si-journal.org/index.php/JSI/article/viewFile/335/325.

18.) Main, Ovan Ray. *"Bitcoin Basics How It Works." Youtube*, 7 Mar. 2017. https://www.youtube.com/watch?v=TGwUpi77bLU

19.) Minaei, Mohsen, et al. *"R3C3: Cryptographically Secure Censorship Resistant Rendezvous Using Cryptocurrencies."* Purdue University., 15 May 2018, pp. 1–34., eprint.iacr.org/2018/454.pdf.

20.) Mosher, Dave. *"Elon Musk Has a 2027 Deadline to Surround Earth with High-Speed Starlink Internet Satellites - but the Service Would Work Far Sooner than That."* Business

Insider, Business Insider, 18 May 2019, www.businessinsider.com/spacex-starlink-satellite-internet-service-when-available-date-2019-5.

21.) Nakamoto, Satoshi. *"Bitcoin: A Peer-to-Peer Electronic Cash System."* Oct. 2008, pp. 1–9., bitcoin.org/bitcoin.pdf.
Rosenberg, Eric. "The 7 Best Bitcoin Wallets of 2019." The Balance, The Balance, 11 Mar. 2019, www.thebalance.com/best-bitcoin-wallets-4160642.

22.) Orcutt, Mike. *"Will People Ditch Cash for Cryptocurrency? Japan Is about to Find Out."* MIT Technology Review, MIT Technology Review, 23 Jan. 2019, www.technologyreview.com/s/611656/will-people-ditch-cash-for-cryptocurrency-japan-is-about-to-find-out/.

23.) Sherman, Justin. *"Emulating China and Russia, More Countries Crack Down on Internet Freedoms."* World Politics Review, 11 Jan. 2019, www.worldpoliticsreview.com/articles/27162/emulating-china-and-russia-more-countries-crack-down-on-internet-freedoms.

24.) Short, J. H., 2014: *The Future of Cryptocurrency.* http://www.harkell.com/TFOC-30-03-14.pdf

25.) Sovbetov, Yhlas, *Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, Litcoin, and Monero* (February 17, 2018). Journal of Economics and Financial Analysis, 2(2), 1-27. Available at SSRN: https://ssrn.com/abstract=3125347

26.) Wilmoth, Josiah. *"Cryptocurrency Is 'Here to Stay': CFTC Chairman Giancarlo."* Yahoo! Finance, Yahoo!, 2 Oct. 2018, finance.yahoo.com/news/cryptocurrency-stay-cftc-chairman-giancarlo-163054434.html.

27.) *"World Internet Users Statistics and 2019 World Population Stats."* Internet World Stats, *Miniwatts Marketing Group.* www.internetworldstats.com/stats.htm.