5-2018

Cryptocurrency's Unique Emergence: An Industry Analysis on the Factors Behind a Meteoric Rise and Uncertain Future

Spencer Finney
University of Arkansas, Fayetteville

Cryptocurrency's Unique Emergence: An Industry Analysis on the Factors Behind a Meteoric Rise and Uncertain Future

by

Spencer M. Finney

Advisor: Kim Petrone

An Honors Thesis in partial fulfillment of the requirements for the degree Bachelor of Science in Business Administration in Finance and Accounting.

Sam M. Walton College of Business
University of Arkansas
Fayetteville, Arkansas

May 11, 2018

1 Introduction

The world of cryptocurrency is a fascinating assortment of paradoxes. A world of digital currencies largely built for electronic transactions but with seemingly few vendors to transact with. A world that everyone seems to be talking about but no one can seem to easily define. A world where titans of financial industry publicly lambast the product while having their companies prepare to monetize it in the next room. A world whose digital attributes cause it to be decried as "fake" or "not real" currency while only 24% of Americans still use actual cash for most of their purchases.[1] A world that was literally named for its security but has become infamous for some of its hacks. It is a world where an interesting creation story and atypical market factors have blended to make something wholly unique. This point is very important. To truly understand why cryptocurrencies have performed the way they have and gain insight into how they might look in the future, you have to approach the situation knowing that it is different from any other.

The cryptocurrency marketplace unequivocally had its best year ever in 2017. This holds true from a variety of different vantage points. Financially, it was by far the strongest year to date as the market cap for cryptocurrencies grew a record 3,362% during the year from $17.7 billion to just under $613 billion.[2] Technologically, the past 12 months brought along some of the most exciting and potentially impactful innovations since the industry's inception. Socially, cryptocurrencies gained widespread and mainstream attention for the first time, finally breaking free of its common "underground" and "futuristic" labels for the first time. But this meteoric year has brought along with it a myriad of new challenges for the industry. In this thesis, I examine the commercial and sociological environment that bred the emergence of the cryptocurrency market, analyze the major problems it now faces going forward,[3] and investigate which currencies are best positioned for long term success[4] in a unique and evolving industry.

2 Background and Emergence of the Cryptocurrency Market

2.1 Brief Origin of Cryptography and Digital Cash

As the name might suggest, cryptocurrencies are a form of digital asset that use cryptographic techniques to form and secure transactions. Renowned computer scientist and cryptographer Nick Szabo breaks the cryptography definition down further by simplifying it to "keeping secrets through mathematics".[5] Contemporarily, this means using computer algorithms to electronically encrypt information. These techniques first reached widespread public awareness in March of 1975 when a team of IBM researchers published their proposal for the Data Encryption Standard (DES), an algorithm developed at the request of the National Bureau of Standards and in accordance with National Security Agency (NSA) demands.[6] DES then became the government standard for unclassified documents and was internationally adopted for securing non-government documents as well. It was met with a large amount of academic

[1] Swift and Ander (2016)
[2] Per coinmarketcap.com
[3] From a business' perspective
[4] The varying definitions and metrics of success within the industry will be discussed in depth later, but I am broadly defining long term success as an ideal combination of currency value/market cap, stability, widespread adoption, and utility.
[5] Ferris (2017)
[6] Burr (2001) pg. 250-251

scrutiny and condemnation, mostly focused on the NSA's involvement and the potential of a backdoor.[1]

Over the coming decades, growing distrust of the government and a deeper understanding of cryptography led to the Cypherpunk Movement that originated in the late 1980s. This was an "activist movement whose participants seek to engineer social and political change and subvert the status-quo by enhancing security and privacy through cryptographic techniques".[2] One of the cypherpunks was cryptologist David Chaum, who had researched anonymous financial transactions as a doctoral student at the University of California Berkeley in the early 1980s. By 1990, he had created the company Digicash and was working on an electronically encrypted currency called E-cash. Soon after, similar projects like Peppercoin,[3] NetBill,[4] and B-money[5] were underway.

While none of these endeavors were ultimately successful, they had important implications for the future of cryptocurrency. First, they were emblematic of the somewhat anti-establishment spirit that many crypto founders still hold today. They were also valuable learning lessons for those future founders of other currencies, revealing existing flaws in cryptocurrency theory and other potential pitfalls of an electronic payment system. Lastly and maybe most importantly, they were pivotal for their role in proposing concepts like proof of work functions[6] and decentralized networks, which are foundational concepts underlying many of the biggest cryptocurrencies in the current market.

2.2 Bitcoin

Creation and Foundational Concepts

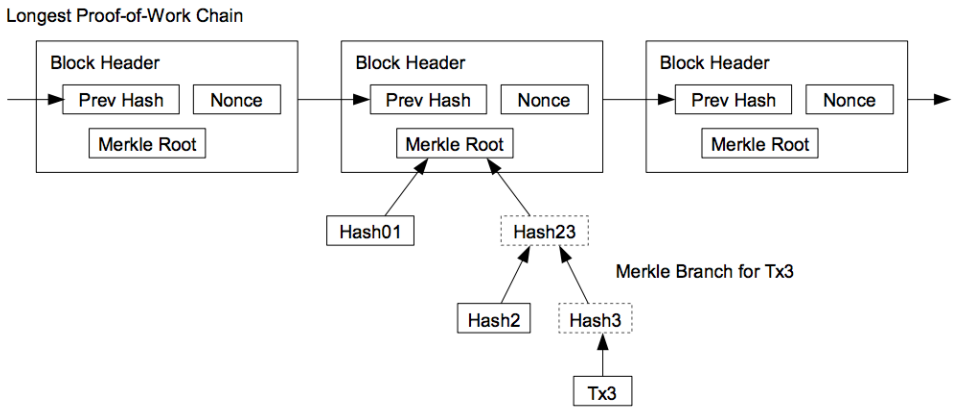
The term "Bitcoin" was first mentioned in a white paper that was published under the name Satoshi Nakamoto to a cryptography mailing list in the fall of 2008.[7] The paper was more of a general proposal than a detailed description, with little to no actual code included. Nakamoto's identity was also vague, and it is generally accepted that the name is a pseudonym for another individual or even a group.[8] In early 2009, the Bitcoin software was made available to the public for the first time. It was revolutionary in its field, becoming the first decentralized cryptocurrency. That means that there was no central authority having to approve or back transactions in order for them to be verified. Instead, Bitcoin introduced blockchain technology and used the concept of a distributed ledger. A blockchain is a "series of blocks that are made up of computations done by computers all over the world that use cryptography."[9] The computations that make up those blocks are series of transactions that are grouped together and

[1] Subramanian (2015) pg. 26
[2] Subramanian (2015) pg. 27
[3] A payment processing software vendor designed to help companies avoid costly micropayment fees by lumping them into a single, larger transaction. Wolfe pg. 10
[4] Another micropayment system developed by a team at Carnegie Mellon University, Cox
[5] B-money was a proposal for an "anonymous, distributed electronic cash system" that was mentioned by Bitcoin founder Satoshi Nakamoto in his famous initial white paper. Nakamoto (2008) pg. 9
[6] Proof of work is the computing power used in a system designed to help secure a decentralized blockchain by having miners compete to be the first one to "define an expensive computer calculation" in order to add a block to the chain. Rosic (2017)
[7] Nakamoto (2008)
[8] Whoever it is, with over a million bitcoins linked to Nakamoto's known accounts, they would be worth several billion dollars today. Bearman (2017)
[9] Szabo, on the Tim Ferris Show (2017)

recorded across all of the computers on the network in order for the chain to remain consistent and secure without one entity maintaining everything. This is the idea of a distributed ledger.

It wasn't until 2010 that Bitcoin was valued for the first time by being exchanged for something-a user swapped 10,000 units for two pizzas.[1] What was happening with the currency for the year in between the launch of the software and the first use of the currency? It was being mined. Mining is another foundational concept to Bitcoin and many other cryptocurrencies. A Bitcoin miner uses powerful computer hardware and advanced software to compete against other miners to be the first to solve complex mathematical problems. The problems deal with grouping transactions together in a "block" in order to be added to the blockchain. The miner's other main role is in studying the transactions to make sure each one meets certain criteria that are laid out in the Protocol Rules[2] so that the transaction will be consistent with the previous ones on the blockchain.[3] The whole process was set up to be challenging, complex, and competitive so that significant proof-of-work is used in creating each new block.

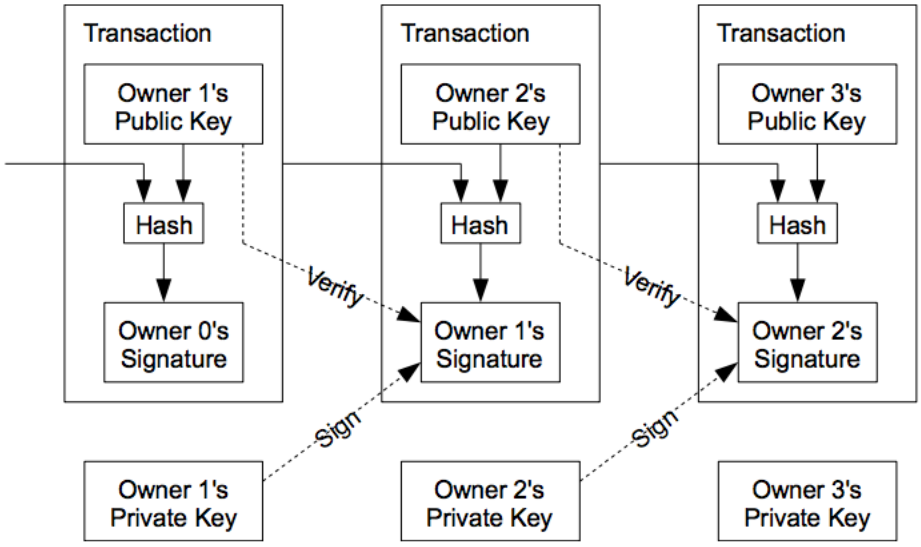
A broad overview of the process is a miner starts creating a new block that contains the hash[4] of a previously approved block that already exists on the blockchain, then adds a hash of the group of transactions that are needed to be added to the blockchain (known as the Merkle Root), and then finally selects a nonce[5]. That new block is only accepted if the hash is smaller than the target hash generated by the system. If that is not the case, the other nodes in the blockchain network recognize the chain as invalid and the miner must try again with another combination. The difficulty in achieving this is also varied so that the overall competition remains fierce; the system is constantly recalibrating to where a new block is created about every ten minutes after the transaction is released into the network.[6] If successful, the correct hash is easy to verify by other hackers and the successful miner is compensated with 12.5 bitcoin (BTC) units as of today. This is the miner's incentive for continuing their role in the building of the blockchain and verifying its transactions. There is a finite number of BTC that can be mined, 21 million units. By the end of 2017, just under 17 million of the possible units had been mined and were in circulation.[7]



[8]

[1] per Marr (2017). That comes out to about $40 million per pizza at today's prices.
[2] en.bitcoin.it (2017)
[3] Subramanian (2015) pg. 29
[4] A hash function is a cryptographic technique that turns any amount of data into a standard, but random new output of a fixed length. Bitcoin uses the hashing algorithm SHA-256.
[5] Nonce (abbreviation of number used once) is a random number that for Bitcoin must be between 0 and 4,294,967,296 and is added to try and achieve the target hash. Acheson (2016)
[6] Subramanian (2015) pg. 30
[7] Per blockchain.info/
[8] Diagram from Nakamoto's original white paper overview of Bitcoin's architecture

Clearly, like you would expect from any currency or payment system, Bitcoin is centered around transactions. Specifically, transactions of a certain number of units[1] of bitcoin currency from one party to another. These transactions work using a combination of public and private keys that are generated by the Bitcoin software for each user. The public key is like a user's address, a code that other users can see in order to send and receive payment from that user. The private key is the user's "signature" when sending bitcoin to another user's public key. This allows the receiving user to verify the authenticity of the bitcoin that the other user is sending based on their prior transactions. The private key is stored in a device called a Bitcoin wallet. There are many different types[2] of wallets that a user can choose from to create addresses and store their private key. The type of wallet a user chooses will help determine the security and accessibility of their own funds. After a transaction takes place and is part of the blockchain ledger, it cannot be undone. Anyone's public key can be viewed by the general public, but because the key is just code generated by an algorithm the users themselves remain anonymous.



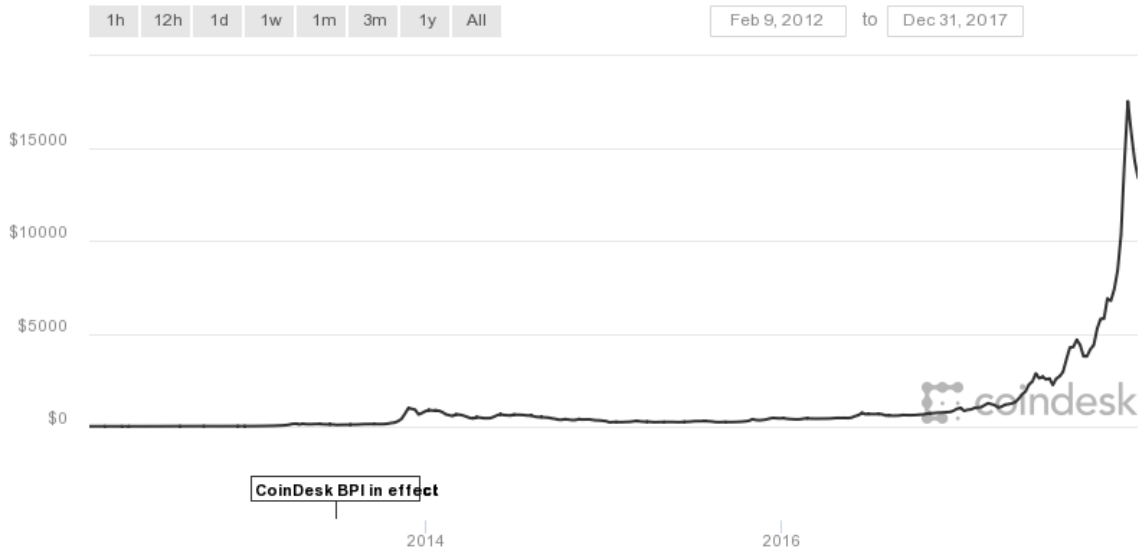
[3]

One important thing to note about Bitcoin is that it is open source software, so anyone can download the code and try to modify or improve it. Nakamoto was involved in development until 2010, and the project has since been led by a group of five "core developers": Gavin Andresen, Jeff Garzik, Mike Hearn, Matt Corallo, and Pieter Wiuelle.[4]

[1] A single unit of bitcoin can be broken down into many different denominations to facilitate smaller transactions. The most common are bitcoin (BTC, which is one full unit), millibitcoin (mBTC, which is one thousandth of a BTC), and microbitcoin (uBTC, which is one millionth of a BTC).
[2] The four main types are desktop, mobile, web, and hardware according to cointelegraph.com
[3] Diagram from Nakamoto's original white paper overview of Bitcoin's architecture
[4] Gregerson (2017)

Growth and Adoption of Bitcoin

A second cryptocurrency (Namecoin) followed in April 2011, but Bitcoin's first-mover advantage allowed it to establish dominant control of the market early on.[1] A large part of its initial appeal was the (relative) anonymity it promised and the possibility that opened for trading illegal goods online.[2] The most publicized place for this kind of activity was the infamous Silk Road, a dark net site that was primarily used for drug trafficking and was shut down by the FBI in 2013. Bitcoin was the currency used for all exchanges on the site. According to one study that looked at Silk Road sales over a period of eight months,[3] computer engineering professor Nicolas Christin conservatively estimated that 4.5% of all Bitcoin transactions were attributed to the site and admitted it could be double that. While its use on illegal sites like Silk Road was largely unintentional, it nevertheless did not help Bitcoin gain mainstream traction. As a result, the price of one bitcoin unit stayed fairly stable for several years before the recent rapid growth of the last 12 or so months.



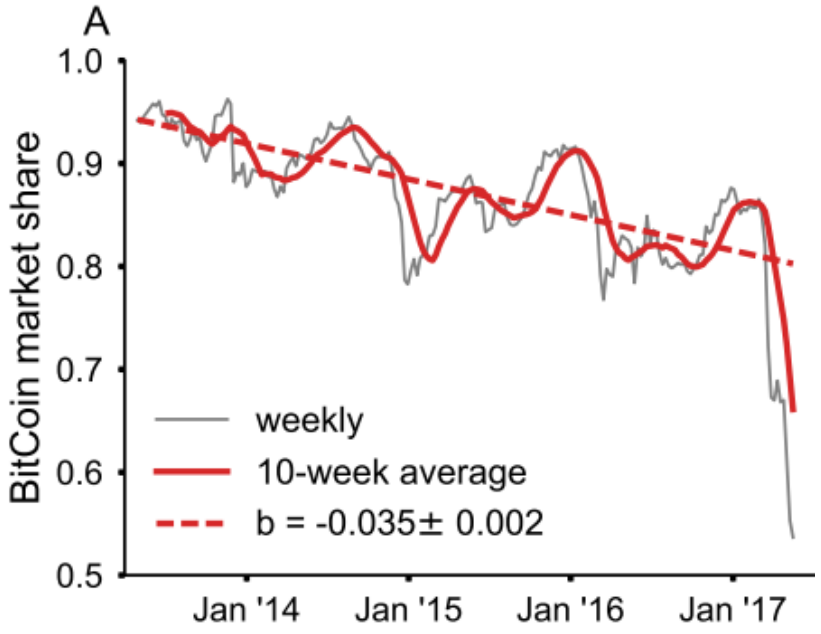
[4]

Not all of Bitcoin's relatively slow start can be attributed to its affiliation with illegal activity, however. The cryptocurrency also had several setbacks in its more public markets as well. Like any currency, bitcoin can be traded for another currency at a specific rate on any exchange platform that is willing to facilitate the transaction. For the first several years of its existence, the main exchange handling bitcoin trades was the Tokyo-based Mt. Gox, which at its peak was handling over 70% of all bitcoin exchanges worldwide.[5] In early 2014, Mt. Gox was hacked and approximately 850,000 bitcoins were stolen, valued at about $460 million at the time. Inside the cryptocurrency community, Mt. Gox had become known for unreliability so the

[1] ElBahrawy, et al (2017) pg.3
[2] Gandal and Halaburda (2016) pg. 16
[3] Christin (2012) pg. 19
[4] Chart from coindesk.com
[5] Vigna (2014)

hack was more of a source of anger than a referendum on the security of bitcoin itself. But outside of that still largely underground community, the hack was more damaging. To many potential major investors and even more causal entrepreneurs that had been looking into the currency, the Mt. Gox hack was a clear example that Bitcoin was not ready for heavy investment yet. As technology writer Robert McMillan of *Wired* put it in his profile of the incident, "A new wave of entrepreneurs may bring the digital currency a new level of respectability, but over its first several years, Bitcoin has been driven largely by computer geeks with little experience in the financial world."[1]

While not catastrophic to Bitcoin's long-term outlook and the underlying software was still solid, the negative attention did help open the door for competition in the cryptocurrency market. I will look at various altcoins[2] in depth in the next section, but while examining Bitcoin's rise it is important to note its simultaneous loss of market share. An in-depth study from the University of London on the trends in market cap of the cryptocurrency market revealed Bitcoin's decline in crypto dominance. [3]



None of this is as somber for Bitcoin as it may sound. An influx of strong competition was inevitable, and Bitcoin is still the largest cryptocurrency by over $60 billion as of this writing.[4] It just enjoyed its best year to date in 2017, ending the year with a price of $13,791 per coin. It has finally seemed to find its way into the consciousness of the general public,[5] even if the majority of people still do not have a firm understanding of what it is.

---

[1] McMillan (2014)
[2] Any cryptocurrency other than Bitcoin.
[3] ElBahrawy, et al (2017) pg. 3. The chart is also from this study.
[4] Per coinmarketcap.com
[5] Popular think pieces like Lance Ulanoff's, "How to Talk to Your Mom and Dad About Bitcoin on Thanksgiving" became common throughout the fall of 2017, as well as seeing Bitcoin discussed on platforms like the evening news. (Ulanoff, 2017)

There are several probable reasons for Bitcoin's huge growth in 2017. First, although previous growth had been much slower, there had been steady (if volatile) momentum in Bitcoin's price in the previous 18 months before 2017 so a natural continuation could be partially attributable. The biggest factor, however, is probably the legitimization of Bitcoin by important financial institutions. The world's largest crypto exchange bitFlyer expanded into the US in 2017 and received the elusive bitLicense from the state of New York to trade there, something only four other digital currency companies had attained.[1] This led to larger US financial interest in Bitcoin and cryptocurrency at large because bitFlyer's more sophisticated trading tools made it appealing to some high worth clients for the first time. Never ones to miss out on an opportunity to add a new profitable sector, major US investment banks and exchanges soon began exploring ways to get in on the Bitcoin movement. Goldman Sachs began looking into setting up a cryptocurrency trading desk,[2] more than a hundred hedge funds were created for the same purpose,[3] and NASDAQ released that some type of Bitcoin investment would probably hit their exchange in 2018.[4] The world's largest marketplace for futures[5], the Chicago Mercantile Exchange, began offering Bitcoin futures near the end of 2017 after getting a "tentative go ahead"[6] from the US Commodity Futures Trading Commission.[7]

As a lot of banks and corporations started looking into cryptocurrency seriously for the first time, they also grew enamored with some of the technology backing Bitcoin and other industry leaders. Major players like all "Big 4" accounting firms quickly put together teams to look into harnessing some of the concepts in their own fields. This optimism around ideas like blockchains and smart contracts was another driver of growth for the cryptocurrency market.

All of these moves helped to raise the price of the currency, which obviously made the people holding bitcoin a certain amount of money. This led to a final main factor in Bitcoin's meteoric 2017, word-of-mouth. As Bitcoin slowly became more mainstream and more Average Joes started to net a profit on its appreciation, the word-of-mouth on this new source of "easy wealth" snowballed through urban areas, college campuses, and suburbs alike. Stories like one I heard from a wife whose husband had told her out of the blue one day, "just so you know, if I die, most of our money is now in bitcoin" became if not common, then at least not abnormal in 2017. The combination of extreme hype and a widespread lack of understanding of the actual technology can be a sometimes dangerous combination for a currency as I will examine later, but it is impossible to ignore the growth affect that word-of-mouth in a social media age had for Bitcoin last year.

2.3 Proliferation of Competition

Motivation

When looking at the cryptocurrencies that followed in the wake of Bitcoin, it is certainly noteworthy to look at the motivation behind their entry into the market. But, I believe it is of far greater importance to examine what factors have allowed various projects to separate themselves

[1] Patrick (2017) pg. 183
[2] McLellan (2017)
[3] Patrick
[4] Yang (2017)
[5] Futures are financial contracts where a buyer or seller agrees to a predetermined future price at which to buy or sell an asset (in this case, Bitcoin). They are often used to hedge or speculate on the potential price movement of the asset.
[6] Small regulatory wins like this were also key to legitimizing Bitcoin in 2017.
[7] Meyer (2017)

and grow into legitimate competitors. That will be the main focus of this section[1] but I will briefly look at motivation as well.

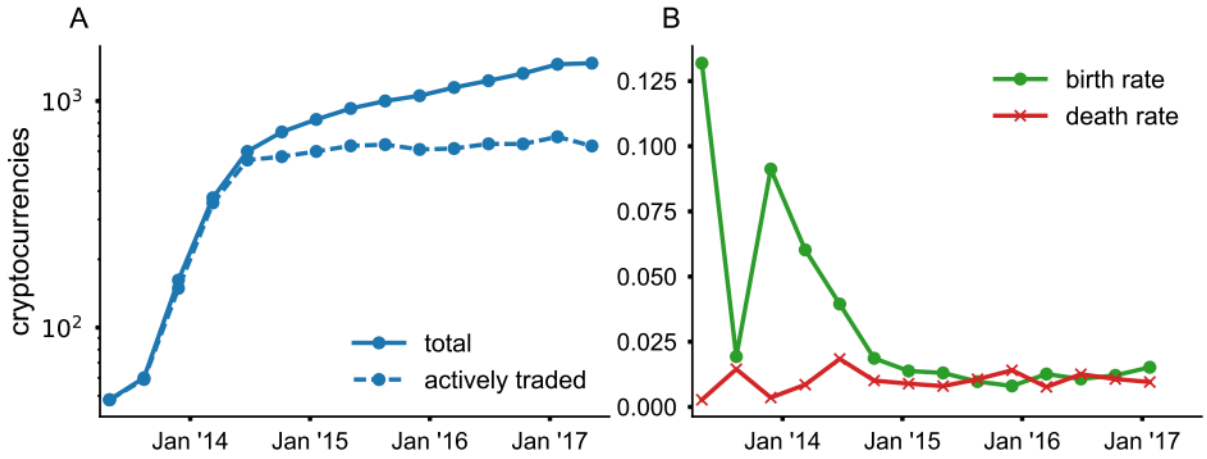
There are several broad reasons that a company or group of individuals join the cryptocurrency marketplace. One logical angle to look at any time a company follows another successful company's lead is that they did it to make money (especially when dealing with a currency market). That is undoubtedly true of some cryptocurrencies, but especially early on was not a driving factor. It would have taken extreme long-term faith in the technology for that to be true, since early after its inception even Bitcoin was experiencing serious price stagnation. Even then, since Bitcoin has always been open source and mining has always yielded bitcoin, there was a greater opportunity for any computer engineer to make money by simply mining the industry leader's currency than trying to recreate their own. This has changed some lately since the overall cryptocurrency market exploded over the last 18 months, and usually takes the form of Initial Coin Offerings (ICO's). ICO's are when a cryptocurrency is trying to raise capital for their project (often while avoiding the traditional rigors of venture capital campaign) and so they essentially auction off a percentage of their cryptocurrency in exchange for a currency like dollars that has real current value. Most large ICO's would still go through some form of a vetting process and have to demonstrate some value from their technology, but smaller ICO's that are essentially fraudulent attempts to get donations for a currency that will never enter the market were an unfortunate result of this system. Either way, I am not treating getting rich as a motivation (or at least an effective one) behind the emergence of other cryptocurrencies.

There are three main motivations that seem to drive new entrants into the cryptocurrency market; the first is to improve or address perceived flaws in Bitcoin itself, the second is to service a market that is currently overlooked,[2] and the third is to create or incorporate new technology that is not being used by another cryptocurrency. An example of the first motivation is the altcoin Litecoin, which was "made in the image of Bitcoin in its early days" (so is technically addressing the flaw that Bitcoin has evolved too far) but with a few other changes.[3] Ripple is emblematic of the second motivation, carving out a niche by focusing almost exclusively on the banking industry. Finally, IOTA is a cryptocurrency that was notably created for using technology other than the blockchain.

Before jumping into a specific breakdown of some of the most important altcoins and the factors behind their emergence, I want to touch on the notion of time being a critical determiner of success for this industry. As mentioned earlier, other cryptocurrencies imitating Bitcoin's decentralized model started emerging as early as 2011. But, getting in early on the heels of Bitcoin's release was not a guarantee or even a harbinger of future success in the crypto market. Of the other nine cryptocurrencies that make up the top 10 largest in market cap after Bitcoin,[4] the average release date was the middle of 2014, with three of those nine being launched within the last twelve months. Although possibly a little surprising, that fact makes sense for a couple of reasons. One is that Bitcoin already took the first-mover advantage and there was not a significant edge to be gained by being among the first in a second wave of currencies. Because of Bitcoin's initially slow adoption among a wider community, potential flaws and oversights that

[1] I acknowledge that the two ideas are not mutually exclusive and that sometimes what motivates a group to enter a marketplace (ex: to fill a niche that is currently overlooked by a dominant project) can also be what allows it to thrive. But if that is the case, I want to analyze further why that motivation was so important in the first place.
[2] Motivation two is similar to motivation one but is different and large enough that I believe it qualifies as its own category.
[3] Liebkind (2017)
[4] data from coinmarketcap.com

could be corrected by a new cryptocurrency were not immediately apparent. There was simply no scale to reveal some of them.[1] Another reason why early new entrants did not gain as big of an advantage is because more recent entrants have not faced as stiff of competition as one might think. As the market cap for cryptocurrencies rose throughout the decade and awareness grew, it would make sense if more and more projects were started to ride the growing wave. But that has not been the case. The same University of London study that examined Bitcoin's diminishing market share also yielded interesting insights on the relative stability on the number of competitors in the overall cryptocurrency market.[2]



Starting around the middle of 2014 there seems to be a saturation point that the market has reached where cryptocurrencies enter and exit the market at a remarkably similar rate. This has naturally led to the number of overall cryptocurrencies (especially those actively traded) to stay within a small range for the last several years. This means that a cryptocurrency that entered the market in 2017 has had to compete with a similar number of currencies as one that entered nearly 3 years prior. A newer entrant would be behind in terms of market share and awareness, but has not been facing continually stiffer competition[3] like one might expect from such a growing industry. This ability for new projects not to face significant barriers of entry into the marketplace while still being able to remain lean and modern like traditional startups is an interesting dynamic in the cryptocurrency world.

The Other Major Players

Ethereum

One of Bitcoin's biggest rivals is called Ethereum and was introduced in 2015 by a researcher named Vitalik Buterin. Ethereum is an open source software platform that is also built on blockchain technology. While that may sound very similar to Bitcoin, the two projects are significantly different in their purposes. Bitcoin created blockchain technology and then used that technology in a very specific way, to build an electronic cash system that was decentralized.

[1] A helpful comparison could be when Apple releases new software for its iPhones. Although they have done significant testing of the software (the idea behind beta versions), they consistently release software updates that run into issues once a much larger population gets their hands on it.
[2] ElBahrawy, et al (2017) pg. 4. The graphs are also from this study.
[3] At least in terms of the number of competitors

Ethereum, on the other hand, was proposed and created to utilize the blockchain technology to build a platform that allows users to create their own decentralized applications.[1] It is a far broader project. But, the reason Ethereum is a rival to Bitcoin and being examined in this thesis is that it also has a cryptocurrency component too. The digital currency used on Ethereum's platform to be distributed for miners and as a means of payments for other apps on the network is called Ether and is often used interchangeably with Ethereum. It is the second largest cryptocurrency in the world, with a market cap of $85 billion.[2] Part of what makes Ethereum so interesting is the seeming lack of interest in promoting the currency.[3] In fact, the main page of Ethereum's own website invites developers to use the network to design and build their own cryptocurrencies.[4]

The project's focus is clearly on the decentralized platform and smart contracts. Smart contracts "take a human aspect of something and code it into a computer" and primarily are used to do two things 1) verify transactions 2) automate transactions.[5] They are similar to a computer program that is executed on the blockchain. The appeal of smart contracts is that they are automated, efficient, and immutable. They allow a developer to take a task that is often manually intensive (and therefore usually leads to higher costs) and cut out most of the work and intermediaries. A good example is an insurance policy.[6] In most cases, there are quantifiable parameters that can be input as code and if an event triggers those parameters, an insurance payment could be sent automatically. This is a broad example, but think of how much paperwork and how many man-hours would be saved with a large-scale implementation of a task like that or say, the execution of a will. Ethereum's primary market advantage is as the premier network for the building and execution of these decentralized smart contracts.

Ripple

As mentioned earlier, Ripple is a project that arose to service a specific industry (banking) in ways that Bitcoin was not optimized to do. Ripple is more similar to Bitcoin than Ethereum, it is a payment network built on a blockchain that specializes in global financial transactions. The cryptocurrency native to its network, XRP, was the #1 performing cryptocurrency asset of 2017, with market cap growth of 36,018%.[7] The purpose of the currency is to use an open source protocol to operate as a settlement system for payments across the world on a secure, distributed network. In other words, "to allow anyone to transfer money in any currency to any other currency in a matter of seconds."[8] International money transfers can often take days or weeks depending on the bank, so Ripple was designed to utilize a blockchain to increase global liquidity. It enjoyed such large growth in 2017 as a result of its acceptance and legitimization by an array of financial service providers. It has partnered with American Express and with large banks around the world because many bankers see Ripple's underlying platform having multiple advantages over Bitcoin and other cryptocurrencies.[9] It is also being used in

[1] Rosic, Ameer "What is Ethereum" (2017)
[2] per coinmarketcap.com
[3] As an open source project, there is no real corporate leadership but the project is headed by the Ethereum Foundation, a non-profit council that has shown that the currency is not their primary goal.
[4] www.ethereum.org
[5] Szabo, on the Tim Ferris Show (2017)
[6] Dikusar (2017)
[7] Korosec (2017)
[8] Description from financial services information site finder.com
[9] Todd (2015)

other ways in the financial market. A hedge fund founded by prominent tech entrepreneur Michael Arrington was recently set up that will be the denominated in XRP.[1] It is the first hedge fund to ever be denominated in cryptocurrency instead of a fiat currency. Ripple's reach has extended to venture capital as well. The start-up company Omni recently elected to receive a $25 million round of funding in XRP instead of dollars. Part of Ripple's broader appeal to more casual cryptocurrency investors can be attributed to its low prices. Although the market cap has exploded over the last year, the currency was not valued at $1 per unit until December 21st of 2017. For average people looking to get into the market that are interested in owning whole units of a cryptocurrency, it is a common option.

Bitcoin Cash

Bitcoin Cash is the most prominent example of what is called a hard fork in blockchain terminology. A hard fork is when a blockchain (in this case the original Bitcoin blockchain) duplicates at a certain point in time and then the two resulting blockchains operate independently.[2] In other words, the two blockchains will have a shared history of all of the transactions up until a certain date, but then all future transactions on the respective blockchains will be unique. This means that although no new work is really done, a new cryptocurrency is essentially formed. When Bitcoin Cash (BCC) split off from Bitcoin classic (BTC) on August 1, 2017, for every one unit of BTC that a user owned, they now owned one unit of BCC as well. The reasons behind a hard fork can differ, but in this case it was a long-stand ideological debate within the Bitcoin community that led to the creation of Bitcoin Cash. Bitcoin has a size limit of one megabyte per 10 minutes on its network that has been around nearly since its creation as a security measure and as far back as 2010 this limit was creating tension.[3] One faction of the Bitcoin community wanted the limit raised or abolished to decrease transaction times[4] and help with scalability. The other faction thought that action would lead to too rapid of growth and centralization.[5] The divide did not come to a head until 2016 when Bitcoin's growth led to the 1 MB limit being tested for the first time, leading to a de facto bidding war of transaction fees in order for users to get their transactions processed.[6] The hard fork was eventually decided upon and was implemented last year. The primary difference between them is the block size limit, Bitcoin Cash has not seemingly settled on a final limit size but has hovered around 8 MB. The long-term implication is that because these are two distinct cryptocurrencies now, any changes or adaptions that are made to Bitcoin will not be reflected on the Bitcoin Cash network.[7] In the short term, both currencies have seemingly done well. At the time of this writing, Bitcoin Cash had the fourth largest market cap at around $22 billion, and the hard fork never caused a serious dip in Bitcoin's prices in 2017.[8]

---

[1] John Roberts (2017)
[2] Tepper (2017)
[3] Smith (2017)
[4] A typical bitcoin transaction takes about 500 bytes, so this limit meant there could only be around 2,000 transactions per block, and with a block being mined about every 10 minutes this means that the Bitcoin network could only handle 3-7 transactions per second. Lee (2017)
[5] This is an example of the same anti-establishment, distrustful sentiment that was described earlier that many people behind the evolution of digital currency similarly held.
[6] Smith (2017)
[7] Or vice versa, but it is more likely that due to its size and reach that the original Bitcoin will undergo the more substantive changes.
[8] per Coinmarketcap.com

Litecoin

Commonly described as the silver to Bitcoin's gold, Litecoin is one of Bitcoin's oldest and most similar competitors. It was created by Charlie Lee, formerly a software engineer at Google and the Director of Engineering at Coinbase,[1] and was one of the first projects to imitate Bitcoin's technology with only minor modifications. It was "made in the image of Bitcoin in its early days", but there are still a couple of important technological differences between the two.[2] For starters, Litecoin uses a different algorithm on its blockchain (Scrypt instead of BTC's SHA-256). This is important because it makes it hard for miners to switch over from another currency, allowing it to remain more decentralized. Scrypt's code is also less optimized for use with customized mining rigs that are becoming more and more common with large-scale mining groups.[3] Litecoin's blockchain also allows for larger blocks (more transactions grouped together) and faster confirmation times (2.5 minutes compared to 10 minutes for Bitcoin).[4] Other minor differences are things like a greater total amount of coins[5] and slightly less volatility than Bitcoin.[6]

Cardano

Most of the cryptocurrencies examined already have been derivatives of Bitcoin in style, function, or both. Cardano is unique because it is largely based off of Ethereum instead of Bitcoin. In fact, one of Ethereum's original founders, Charles Hoskinson, is behind the Cardano project.[7]The project is similar to Ethereum in its basis as a platform for smart contracts instead of a "pure" cryptocurrency, although the platform does have its own dedicated cryptocurrency, Ada. A development firm based out of Honk Kong backed the project, and it was funded through an ICO in Asian markets so that it could create more interest and avoid some of the regulation that was starting to appear in more Western countries.[8] The unique attributes of Cardano are its programming language (Haskell)[9] and its use of proof of stake (PoS) to verify transactions instead of the more common proof of work (PoW) that Bitcoin uses. In proof of stake, a miner is chosen based on some randomized criteria such as wealth and receives the transaction fees as payment.[10] This method is significantly more cost and energy efficient that proof of work.

These five cryptocurrencies, along with Bitcoin, are the six largest in terms of market cap and all possess unique capabilities that have enabled them to become market leaders. Below are a

[1] Coinbase is one of the largest cryptocurrency exchanges in the world.
[2] Liebkind (2017)
[3] Fernando (2017)
[4] Martindale (2018)
[5] The difference in total number of potential coins (84 million compared to 21 million BTC) is mostly psychological because the units can be broken up into such small amounts to facilitate transactions.
[6] Liebkind (2017)
[7] Castor (2017)
[8] Castor (2017)
[9] Haskell is a functional language that is known for its similarity to mathematics, creating a more secure protocol. *A Dictionary of Computer Science* (2016)
[10] Rosic (2017)

quick breakdown of a couple smaller cryptocurrencies that were selected because of their own defining characteristics that could be impactful in the cryptocurrency industry going forward.

IOTA

IOTA was founded in 2015 and is best known for being one of the few cryptocurrencies that does not incorporate blockchain technology. Instead, IOTA uses the Tangle, a distrubted ledger system that is supposed to be more scalable and faster than blockchain, while allowing for many more transactions.[1] Tangle is based on directed acyclic graph technology which does away with a dependence on miners and makes transactions free.

Monero

The appeal of Monero is its commitment to privacy and security. It is completely open source and uses a cryptographic technique called "ring signatures" where a real address from a transaction is mixed with other addresses to obfuscate the identity of the actual person involved in the transaction.[2]

Overview of the Cryptocurrencies in this Study

CURRENCY	BITCOIN	ETHEREUM	RIPPLE	BITCOIN CASH	LITECOIN	CARDANO	IOTA	MONERO
ABBREVIATION	BTC	ETH	XRP	BCH	LTC	ADA	MIOTA	XMR
LAUNCHED	2009	2015	2012	2017	2011	2017	2015	2014
MARKET CAP (GROSS)	$157B	$85B	$44B	$22B	$11B	$10B	$5B	$4B
MARKET CAP (RANK)	1	2	3	4	5	6	10	13
Blockchain	PoW	PoW	Consensus	PoW	PoW	PoS	Other (DAG)	PoW
Notable Characteristics	First, most liquid	Smart contracts	Partnerships w/ financial services	Hard fork from BTC in late 2017	Modeled after original BTC	Smart contracts	Not blockchain based	Privacy and security
2017 Growth	1,318%	9,162%	36,018%	513%	5,046%	2,782%	501%	2,959%

[3]

[1] Reiff (2017)
[2] Bajpai (2017)
[3] I created this table with data pulled from coinmarketcap.com.
Acronyms: Proof of Work (PoW), Proof of Stake (PoS), Directed Acyclic Graph (DAG)

3 Identifying Problems Facing the Cryptocurrency Market and Possible Solutions

After giving a brief background and overview of the cryptocurrency market while examining some of the major players, this section will transition into identifying and describing the main problems facing the market today. While some of the issues discussed will apply to some cryptocurrencies more than others, all are macro issues that apply to the market at large. The main criteria for selecting the issues for this section were obstacles or questions that could plausibly slow or derail cryptocurrency from its growth in becoming a dominant global technology. After detailing each problem, possible solutions will be laid out and then a "winner" will be awarded. The selection of each winner is based on their ability to combat each individual problem with (i) how they might be currently positioned in the market and (ii) with any upgrades they are implementing.

3.1 External Identity

As previously shown, 2017 was a year of enormous growth for the industry and served to launch cryptocurrency to a certain level of mainstream vernacular. But, there remains a lot of advancement to be made if crypto is to become the world-changing currency and technology force that it is often billed as by its creators and some optimistic pundits.[1] Now that terms like cryptocurrency and blockchain and Bitcoin have become common enough to be recognized by the average individual, the next step for the industry is to have people understand the terms and feel comfortable being associated with them. When experts have a difficult time coming to any kind of consensus on a definition,[2] it is easy to understand why so many laypeople are uncertain in their thoughts and feelings on the topic. They simply do not have a clear grasp of what exactly cryptocurrency is and this identity question is obviously a hindrance to a product or technology hoping to be adopted across a wide market. The public's lack of understanding over cryptocurrency can be broken down further by looking at some key drivers of the confusion and uneasiness.

Reputation

Cryptocurrency has certainly legitimized itself in major ways through some of the deals that individual currencies have made with major companies, but the "shady" stigma from its earlier days still remains. This is particularly true of older generations that seem to have vague recollections of the FBI's takedown of Silk Road and the Mt. Gox hack making the national news. This is where the longstanding lack of clarity around cryptocurrency is particularly harmful. Because instead of understanding and remembering negative events as isolated or rendered irrelevant by advances in technology, many potential users have blurred timelines and facts to where, to their knowledge, the responsible parties are still actively involved in cryptocurrency and the criminal issues must still be pervasive (even if that is largely untrue). This is also a problem because of the lack of differentiation in the minds of many consumers between cryptocurrencies. For example, new cryptocurrencies can often still be negatively associated with things like the underground dealings of the Silk Road even if the site was shut down years before their creation just because they fall under the same broad cryptocurrency moniker as the currency involved, Bitcoin.

[1] Bereznak (2017)
[2] Ferriss (2017)

Technological Complexity

It is human nature to not fully trust anything that we do not understand, and it is safe to say that many people in the US and around the world do not have a good understanding of the technology involved in cryptocurrency. Any new advancement in technology is going to generate a learning curve for its terms and concepts, but cryptocurrency's is especially steep. While a deep understanding of blockchains or modern cryptographic techniques is certainly not necessary to use a cryptocurrency, it is almost undoubtedly hurting its rate of adoption among the population at large. This is not a problem that is confined to older generations either. Younger, more technologically savvy age groups may be able to exchange or transact with cryptocurrencies easier because of their overall comfort level with apps or other digital mediums, but their understanding of major underlying concepts like mining and smart contracts is also very limited. The difficulty in understanding cryptocurrency is not completely isolated to just technology though. Based on conversations I've had across multiple age groups, it is the combination of complex computing ideas with the financial aspects that is the largest source of people's naiveté. When a person already has a hard time describing items like currency or ledgers, adding in an unfamiliar technological component for cryptocurrency creates a very foreign situation to try and understand.

Negativity from Thought Leaders

The mixed identity of cryptocurrency to users or potential users is not solely due to past scandals or the technology being difficult to understand. It also is heavily influenced by prominent figures in multiple industries coming out with less than optimistic opinions and sometimes even sharp criticism of the new digital currencies. Thought leaders can have an outsized impact on complex topics that they are perceived to be experts in, and cryptocurrency certainly fits the bill. When consumers are unfamiliar with names like Cardano or Ripple, it makes sense that they would trust in the words of various captains of industry from established companies like Vanguard or Goldman Sachs on those cryptocurrencies. The table on the next page gives a sample of some of these leaders and their views, all from the past year. While their views may evolve with time, there seems to be a consensus among many banking and finance executives that cryptocurrency is not currently viable as a currency, and several of them use the word "bubble" to describe the rapid growth and speculative nature of the current crypto market. It is important to note that although Bitcoin is mentioned specifically in several of the comments, that is more of a reflection of either questions being asked phrased around that cryptocurrency or as an example of how Bitcoin is often used interchangeably with cryptocurrency at large.

Negativity on Cryptocurrency from Thought Leaders

Name	Company/ Organization (Industry)	Notable Quotes	Date of Comment
Jack Bogle	Founder of The Vanguard Group (Investment Mgmt.)	"Avoid Bitcoin like the plague"[1]	Nov. 27, 2017
Randal Quarles	Vice Chairman of Supervision-Federal Reserve (Banking)	"More serious financial stability issues may result if they achieve wide-scale usage" Change in payments systems "measured in decades, not years"[2]	Nov. 30, 2017
Jamie Dimon	Chairman and CEO of JPMorgan Chase (Banking)	"(Bitcoin) is a fraud…worse than tulip bulbs" "If you're stupid enough to buy it, you'll pay the price for it one day"[3]	Sept. 12, 2017 Oct. 13, 2017
Lloyd Blankfein	Chairman and CEO of Goldman Sachs (Finance)	"(Bitcoin) is too volatile to be a good currency"[4]	Nov. 30, 2017
Tidjame Thiam	CEO of Credit Suisse (Finance)	"(Banks) in the current state of regulation have little or no appetite to get involved in a currency which has such anti-money laundering challenges"[4] "(Bitcoin) is the very definition of a bubble"[5]	Nov. 2, 2017

[1] Grant (2017)
[2] Heltman (2017)
[3] Cheng (2017)
[4] Yurcan (2017) pg. 182
[5] Foerster (2017)

Possible Solutions to External Identity Problems

The saying "any publicity is good publicity" might have been true while cryptocurrencies were aggressively trying to make headway in grabbing the public's attention, but as competition has grown it is now more prudent for each cryptocurrency to actively cultivate a more positive public image. This is a tough problem for the industry to address because that is a lot easier said than done. Time will be a very important element in building trust with consumers. There are steps that projects can take to positively evolve their identity, however. Making a clear delineation between a current project and the troubled ones of the past would be a good place to start. This could apply to more traditional powers like Bitcoin doing a bit of rebranding to emphasize their more legitimate standing or to new startups that want to known that they should not be lumped in with hacks or crimes committed while they were not around.

Another helpful idea addresses the technological complexity and requires a little more systemic change from the cryptocurrency community itself. Many in that community (especially more traditional members) see themselves as purists who have created a product that is impactful and contrarian, taking pride in harnessing complex technology to accomplish their goals. They do not wish to compromise or dumb down anything for the sake of business growth. A pop-culture example of this is depicted on HBO's acclaimed comedy series *Silicon Valley*[1], which is focused on a fictional technology start-up called Pied Piper. One story arc tracks Pied Piper as they launch a revolutionary app, only to see it fail because it was designed by computer engineers who could or would not effectively build something for "regular people". To steal the show's solution, one way to combat this is with an aggressive marketing campaign that is based around the idea of helping educate the public through simplified ads, pop-up shops, and other flash retailing strategies.

A final solution to this problem deals with generating less negative reviews from prominent figures. Like the public at large, many of the objections raised by these leaders are rooted in their lack of understanding as to what the cryptocurrencies are or are going to be. Partnering with large companies that are run by these figures, even on a limited basis so that they can gain a better understanding of the technology, would be a major step forward. This is easier said than done, but most companies have a very real interest in at least blockchain technology so a group project could be mutually beneficial. It will be a lot less likely for a CEO to make disparaging remarks when there is money on the line for his company.

Current Winner: Ripple

Picking who might win out in the court of public opinion can be fickle, and this problem as a whole is a little more imprecise than others. But I am selecting Ripple as the cryptocurrency best positioned to overcome this problem for a couple of reasons. First, although it is by no means one of the newer cryptocurrencies, its slower rise and lack of negative incidents means that it has been able to avoid some of the connotations that follow other currencies that rose amongst scandal. It is also a project that is led by a company with an actual corporate structure, which is extremely advantageous for organizing a marketing strategy and brokering deals. Speaking of, Ripple has already secured deals with major banks and financiers which lend it (no pun intended) credibility with consumers and thought leaders alike.

[1] To be fair, it is a pop-culture example that is firmly grounded in reality. *Silicon Valley* is famed for its verisimilitude, with tech giants like Marc Andreeseen, Dick Costolo, and Sheryl Sandberg all contributing ideas and issues they see in the real world Valley. (Rose, 2018)

3.2 Internal Identity

Cryptocurrency's identity problem is clearly an important issue that needs to be clarified for consumers, but the problem also has another side that is equally if not more important for the future of the industry; many cryptocurrencies themselves seem to be having a difficult time establishing what their identity is or should be going forward. These ideas are obviously heavily intertwined. How can the public know definitively what something is supposed to be used for if the creators seem to be unsure? Conversely, how does a company or board of overseers reckon with their creation being used for something entirely different than how it was intentioned?

This problem has two major considerations to examine when looking at it. The first is the unique environment at work in the cryptocurrency world by having some major players be privately funded companies and others that are open source projects that are largely being produced by unconnected developers across the globe. I will touch more on the pros and cons of these two primary options later, but for the relevance of this section it seems clear that the projects created and run by companies instead of open sourced developers have an advantage in forging a united identity for the project. A company with an executive team that has a product (in this case a cryptocurrency or platform) they are wanting to market will have a top-down directive for what they want being produced. For an open source project like Bitcoin, the community at large may have stronger feelings about what they want the currency to look like and function as, but constant suggestions from thousands of sources of improvements or changes they would like to see made tends to muddy the waters a little bit. In short, these projects have a harder time presenting a unified front on the identity of the project.[1]

This leads into the second main consideration for this issue, that this is a problem more on a macro scale than a micro scale. Yes, it may be more difficult for an open source project to come to a consensus on the direction of a project in the future, but by and large there is a good amount of agreement within each community on what that direction should generally look like. The question of what cryptocurrency as an industry is going to be from the developer's point of view is where this becomes a bigger unknown. A good way to think about this might be to use traditional money as an example.[2] Money serves a multitude of different roles in society, and depending on what type of person you ask, you will usually get a different answer for what it is. A lawyer's definition of money might be an official government currency, while an economist might say that it is something used as a medium of exchange or store of value.[3]

In the same way, cryptocurrency is a broad term that is used to describe technology that is being used for many different purposes. Ripple is being primarily used to facilitate international money transfers. Cardano and Ethereum's currencies are built around them being used on their own platform to pay for smart contracts and other transactions. Bitcoin is a digital payment system created to facilitate transactions between users and merchants. These all being so different is not bad, and is a natural result of competition. The issue occurs because at this point most of their differences are still highly speculative. It is a positive sign of market maturation that these variations of cryptocurrency have been created, but most of the currencies

[1] This is something that is often cited as one of the benefits of open source software, that there is more brainpower looking to improve a cryptocurrency. I am not disagreeing with that sentiment at all, but merely pointing out a downside that the system has created.

[2] The inspiration for this train of thought comes from Nick Szabo on the Tim Ferriss Show (2017).

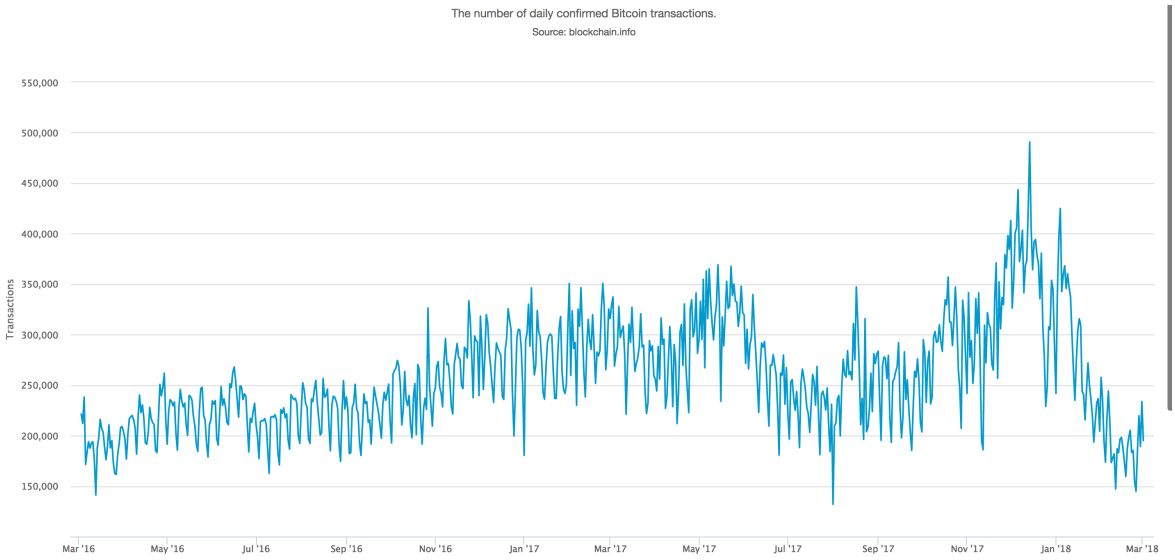
[3] Oxford's Dictionary of Business and Management lists the functions that money fulfills as being a medium of exchange, a unit of account, and a store of value. Law (2016)

are not doing a very effective job of executing their goals in differentiation. NYU Professor Aswath Damordan argued in a blog post[1] that the cryptocurrency market will be dependent on its currencies seeing their creations as "a transaction medium and acting accordingly" if they want to successfully move from being a speculative asset to a bona fide currency.

Cryptocurrency as a Speculative Asset

There is little disagreement that, by and large, cryptocurrency was being treated as a speculative asset in 2017. Back in November, Credit Suisse CEO Tidjane Thiam said that, "from what we can identify, the only reason today to buy or sell Bitcoin is to make money, which is the very definition of speculation and the very definition of a bubble."[2] Talk of a crypto bubble really picked up steam at the end of the year. UBS Wealth Management's Global Chief Economist Paul Donovan wrote in a post that his company believed there was definitely a bubble.[3] He also pointed out that just realizing there is a bubble does not mean much. "Being able to short a bubble does not make the bubble burst at once," he said, "bubbles are by definition irrational. Predicting when a bubble will burst cannot use rational analysis. Ignoring a bubble is the best course of action."[4] Nick Szabo has a different opinion though, one that traces back to cryptocurrencies previously discussed relationship with traditional money. He notes that even if there is a crypto bubble that "money is the bubble that never pops."[5]

Bubble or not, it is fair to say that speculation drove most of the growth in market cap among cryptocurrencies last year. It was based on currencies being used as a capital asset, with investors holding units of the currencies and hoping for appreciation. While you could generously chalk up some of the investing to optimism in the future of the technology, there was simply not enough underlying growth in the usage of the currencies to justify some of the price appreciation.



6

[1] "The Crypto Currency Debate: Future of Money or Speculative Hype?" Damordan (2017)
[2] Revill (2017)
[3] Donovan (2017)
[4] Donovan (2017)
[5] Ferris (2017)
[6] Table from blockchain.info

This chart shows that although there was a slight bump in the daily number of Bitcoin transactions, major growth was not there. Damordan looked at the data from a longer timeline and noted that "while the price of bitcoin has increase more than a thousand fold, since the start of 2012, the number of transactions involving bitcoin was only about thirty two times larger in July 2017 than what it was at the start of 2012."[1] This holds true for almost all of the major currencies as well. Some of them like Ethereum show solid transaction growth, but this is more reflective at how little they were being used before and still only accounts for a fraction of the growth in its market cap. As the crypto industry moves away from its infancy, it must figure out how to shift away from being a purely speculative asset to many people. There has not been enough interest from consumers to motivate businesses to accept crypto payments, with a recent study showing that only three out of the top 500 online retailers are accepting Bitcoin payments.[2] This current situation is already turning off major investors, as people like Jack Bogle argue that if it is operating primarily based on capital appreciation then it does not even have the same underlying rate of return like bonds or stocks since there are no dividends or payouts.

Possible Solutions to Internal Identity Problems

This is a major issue that has led to a lot of the recent bearish reports on cryptocurrency. Some, like Vanguard's chief economist Joe Davis, believe that "even if cryptocurrencies qualify for niche purposes, their prospects seem dubious."[3] Whether that turns out to be true will play out over time, but there are definitely steps to be taken that will increase a cryptocurrencies chances in carving out a lasting role.

The main fix for this problem is for each cryptocurrency to identify their lane within the market and pursue that aggressively. Practically, this means either the community or the parent company will have to come together to make definite decisions on how the currency will best be used and then take steps in evolving the currency to meet that use more effectively. The often times fractured groups that make up a community like Bitcoin can make this difficult, but some currencies are already taking proactive steps to combat this infighting. Tezos is a cryptocurrency that has been struggling to find a balance between listening to contributions from its community and moving on with decision making at a foundational level. Their developers have recently started working on modifying the system to push out updates to the network automatically to avoid quibbling over each new update, a process that has led to inertia in other currencies.[4]

Some improvement will come naturally as well. As time and competition eliminates many currencies, it will become more clear to the remaining ones which niche is allowing them to survive. From that point, it is imperative that they continue to hone their strategy instead of staying broad. A less crowded marketplace with more defined competitors should help with speculation and price volatility a little bit too. There will be less incentive to throw money at a wide range of currencies and more consistent use will allow a more steady price range to form.

Current Winner: Ethereum (and Bitcoin)

Ethereum is an easy winner here because it has stuck to its guns as a platform for enabling smart contracts from the very beginning and has been recognized as such almost universally. This isn't to say that the currency is without flaws or will monopolize that domain,

[1] Damordan (2017)
[2] Toplin (2017)
[3] Fuscaldo (2018)
[4] Hackett (2017)

but that Ethereum stands out for having a clear target that it is pursuing with its strategy and updates.

The inclusion of Bitcoin here is more complex. In many ways it has been a poster child for some internal identity problems. But I am selecting winners in these categories by looking at both the current and near future status of the cryptocurrency, and Bitcoin has taken steps to more clearly follow its original purpose as an electronic payment platform. Its slow processing times and higher transaction costs have often been cited as unacceptable drawbacks to widespread adoption of the network, but Bitcoin is responding to these challenges (albeit in a slow and heavily debated way).

One solution that Bitcoin is pursuing, called Segregated Witness (SegWit), is a protocol upgrade that took effect on the network in 2017 that allows for reduced malleability and changed the network's block size limit to a block weight limit.[1] All of this is supposed to allow for more transactions, which would in turn lower transaction costs. The issue has been adoption. Not all cryptowallets and exchanges currently are utilizing the changes, although there is supposedly more hope for change in 2018.[2]

Another step that Bitcoin is taking to further signify itself as the premier transactional cryptocurrency is the adoption of a second-layer solution to scalability and transaction concerns. Bitcoin is currently testing beta versions of one of these called the Lightning Network, which uses SegWit to operate on top of a blockchain network. The Lightning Network is designed to drastically reduce fees and could solve Bitcoin's scalability issues.[3] These benefits would be massive in reducing many altcoins advantages over Bitcoin, even though neither SegWit or the Lightning Network is exclusive to Bitcoin. Rather, they would simply level the playing field in major areas, seemingly allowing Bitcoin's brand recognition to lead it to be a more dominant and effective transaction medium.

These changes have yet to produce many tangible results for Bitcoin, but it is still early and they are signs of change that the project is becoming more decisive in its position in the cryptocurrency market.

3.3 Security and Privacy Concerns

Hacks

As its name suggests, cryptocurrency gets a lot of billing for its security but it has not been without its fair share of troubling incidents. Before I detail some of the most prominent hacks and the important takeaways, it is important to note that no cryptocurrencies' blockchain itself has ever been hacked. It has always been a failure in implementation or storage from one of the parties involved. That in itself is a huge selling point for the future of the industry. But, clearly even hacks by association are very damaging, so here are a few in-depth looks at some of the largest thefts.

Mt. Gox

This 2014 attack was described earlier, but it was the first major hack involving cryptocurrency and was the largest until very recently with around 850,000 bitcoins stolen. It is notable not only for its scale but for also being the attack that brought cryptocurrency security under scrutiny for the first time and setting back adoption. The vulnerabilities were on the front

[1] van Wirdum (2018)
[2] van Wirdum (2018)
[3] Torpey (2017)

end at the exchange and through a loophole called transactional malleability. Transactional malleability is when data is tampered with before it reaches the blockchain and then becomes immutable.[1]

Coincheck

The hack of Japanese exchange Coincheck in January of 2017 now holds the notorious title of being the largest hack in crypto history, with an estimated $524 million worth of the coin NEM being stolen.[2] NEM was the tenth-largest cryptocurrency at the time of the attack. The cause of the hack is still being investigated, but it is rumored to be at least partially attributable to the level of sophistication (or lack thereof) of the wallets that the coins were being stored in. This event reminded the crypto community and investors that these types of large-scale hacks are not things of the past and should be factored into the current market view of cryptocurrency.

DAO Attack

Now that the largest overall and largest Bitcoin hack have both been examined, the next major hack here was the largest Ethereum theft to date. The DAO attack took place in June 2016, and approximately $50 million worth of ether was siphoned away. The eponymous DAO[3] was the title of a smart contract system that was being used to crowdsource funding and decision making for an organization. The hacker was able to use a "recursive call bug"[4] to exploit the system in the middle of the fundraising and steal around a third of the funds. The very loophole that the hacker used had been brought up as a potential problem by members of the community before the attack but was dismissed. [5] This is emblematic of a more systemic flaw; a group or community rushes into a cryptocurrency idea without fully considering all of its implications or vulnerabilities and unknowingly seems to create opportunities for hackers. The more concrete takeaway from the incident was the exploration of a soft fork option before settling for a hard fork of Ethereum that created the resulting two blockchains, Ethereum and Ethereum Classic.

Overall, these hacks and others like them signify that the cryptocurrency industry still has a lot of progress to be made in terms of security. Many of the incidents are a result of a user or institution simply not following effective practices for securing the data. How the various cryptocurrencies decide to enforce stricter security in conjuncture with third parties or in spite of them will be a very important step in building public trust in their currencies.

Fraud

Initial Coin Offerings (ICO's) were touched on briefly earlier as a popular new source of fundraising for cryptocurrency startups. Essentially these projects will exchange a certain amount of their new currency's coins for capital investment from either venture capital firms or even the public itself. This strategy allows the startups to avoid the typical funding process and giving away equity or leadership positions. But it has also led to one of the largest sources of fraud in the cryptocurrency world. Criminals will simply raise funds for their new cryptocurrency that does not exist and will never exist. It is a very 21st century take on the classic confidence scheme. The technical complexity of crypto and the still sometimes underground nature of the market combine to all too often make the scam relatively easy to sell and difficult to trace.

---

[1] "5 High Profile Cryptocurrency Hacks" (Rosic, 2017)
[2] Shen (2017)
[3] DAO stands for Decentralized Autonomous Organization
[4] Siegel (2016)
[5] "5 High Profile Cryptocurrency Hacks" (Rosic, 2017)

This is a problem that even those within the crypto world acknowledge and are obviously eager to solve because it brings negative attention to their currencies as well. Ripple CEO Brad Garlinghouse told *Fortune* there is shady stuff going on within the industry and that "frauds are happening."[1] Investor Peter Smith admitted that he believes "market manipulation and insider dealing is rampant among purveyors of initial coin offerings" and that it is an unfortunate downside of any emerging technology.[2]

The good news is that regulators are starting to take notice. In October the Securities and Exchange Commission (SEC) brought its first charges against a company for a fraudulent ICO.[3] The charges deal with anti-fraud and failure to register regulations. The scams are not only a monetary theft, but can also be a way for a proverbial internet boogeyman to steal a person's personal information. This is an area that the SEC has stated they are looking to crack down in, and the extent to which they do so could help solve a problem that is a black eye for the entire cryptocurrency industry.

Possible Solutions to Security and Privacy Concerns

This may be the current problem set with reason for the most optimistic outlook. Part of the reason for optimism is because the projects themselves have high interest in seeing it addressed, especially when compared to some other issues. By and large, the people behind cryptocurrencies are far more likely to spend time working on addressing security weaknesses than they are in tracking the latest in potential policy changes across the world. The huge benefit that it would bring to their currencies is obvious, but this is also an area that inspired many of them to join the cryptocurrency field in the first place and continues to drive them.

Another small cause for optimism is that although this is a problem with several infamous incidents, those incidents are deeper than they are wide. Losing half a billion dollars in a hack is bad no matter how you look at it, but it being the result of one organization's negligence shows the silver lining that there may not be as many security holes to plug as one might assume. It has been mentioned before, but cryptocurrency security breaches are continually the result of external weaknesses from third parties. Cryptocurrencies themselves can help curb this by partnering with exchanges and vendors to make sure their security matches a certain standard. They cannot exactly stop their currencies from trading on those platforms, but it is mutually beneficial for those in the cryptocurrency community to help each other with security issues especially as it moves away from its infancy.

More concrete solutions are becoming increasingly available as well. A Schnorr signature is a type of cryptographic signature that has been heavily discussed for integration with Bitcoin and several other currencies because it has great side effects like lowering transaction capacity and quicker verification.[4] But this type of signature also has big security benefits. It is "considered by many cryptographers to be the best type cryptographic signatures in the field" and does not suffer from malleability concerns that have led to some fraud cases.[5]

New technologies have been developed in the privacy sector concurrently. One proposal from a team of university researchers is called TumbleBit. As Bitcoin and other cryptocurrencies began to seem less anonymous and private than they were initially billed as, TumbleBit was

[1] Hackett (2017)
[2] Hackett (2017)
[3] McLellan (2017)
[4] van Wirdum (2017)
[5] van Wirdum (2017)

created as essentially an extension to a blockchain network that mixes transactions together before redistributing the funds so that the trail of ownership is lost.[1] It can also be used with wallets. An older but similar project called ZeroLink has started to gain traction too. Instead of scrambling transactions together, it creates a layer of anonymity by using a central server to combine them all into a single transaction.[2] This makes the process even cheaper than TumbleBit while achieving a similar level of privacy protection.

Current Winner: Monero

Monero has established itself as the premier cryptocurrency concerning security and privacy matters. Instead of allowing users that are transacting to use the knowledge of the other party's public address to see the amount of coins in their account like other currencies do, Monero blocks that information and uses one-time addresses to make the transactions untraceable. Additionally, its ring signatures feature creates another layer of obfuscation by using a randomization algorithm in mixing transactions together.[3] All of this has made it rapidly grow in popularity, for both legal and illegal transactions.

3.4 Regulation

State Level

Putting 'regulation' within a section identifying problems for the cryptocurrency market may be a bit of a misnomer, but I believe it adequately fits and is definitely of significant importance to the future of the industry. It is no secret that governments across the world are in the process of forming or drafting legislation that applies to this previously unrestricted area, and some laws have already passed. How a cryptocurrency fits within or adapts to a freshly regulated world will have a defining impact on its ability to be viable over the long run.

One of the earliest actions to regulate cryptocurrency was the introduction of the BitLicense by the state of New York in 2014.[4] Billed as "first comprehensive virtual currency regulatory regime proposed in the United States", a BitLicense is essentially just a business license that allows the company to conduct business involving virtual currencies within the state.[5] Here is a summary of requirements that was compiled by international law firm Davis Polk after reviewing the proposed bill that eventually passed.

[1] Heilman, et al (2016) pg. 1
[2] van Wirdum (2017)
[3] Bajpai (2017)
[4] Subramanian (2015) pg. 33
[5] Polk (2014) pg. 3

Summary of Requirements for BitLicense Proposal

Covered Activities	• Most business activities, excluding mere merchant/consumer activities; • involving centralized or decentralized virtual currencies (excluding in-game / rewards points); and • involving New York or New York customers.
BitLicense Application / Revocation	• Must submit detailed applications to NYDFS & become licensed *before* undertaking covered activities. • Existing businesses will have transition period to apply; if denied, must cease activities. • NYDFS has broad discretion to approve/deny, revoke/suspend licenses. • Material change of activities or change of control requires an application to NYDFS.
Consumer Protections	• Initial and per-transaction disclosures of risks, terms and conditions. • Complaint policies & disclosures. • Advertising and marketing requirements (e.g., no false, misleading or deceptive representations or omissions).
Safeguarding Assets	• Capital requirements at NYDFS's discretion. Licensed entity must invest "earnings and retained profits" in enumerated high-quality assets (e.g., CDs, not Bitcoin), but dividends not prohibited. • Bond/trust account at NYDFS's discretion. • Full reserves for custodial assets — selling / encumbering prohibited. • Books and records requirements (generally 10 years).
Cyber Security Program	• Board-approved cyber security policy & program to protect electronic systems and sensitive data. • Qualified Chief Information Security Officer. • Annual reports to NYDFS. • Annual penetration testing/audits. • Maintain business continuity and disaster recovery plan, to be independently tested annually.
Anti-Money Laundering	• Largely consistent with federal AML requirements. • Initial & annual risk assessments to inform AML program. Board-approved policy. • 10-year records of all transactions. • Report within 24 hours to NYDFS ≥ $10,000 one-day transactions by one person. • Suspicious Activity Reports required. • Customer Identification Program. • OFAC checks and compliance. • Annual internal or external audit. No structuring to evade reporting, or obfuscating identity.
Exams, Reports and Oversight	• NYDFS examines at least every two years, and may examine affiliate of licensee in its discretion (not limited to virtual currency activity). • Submit quarterly financials within 45 days, audited annual GAAP financials within 120 days of fiscal year end (including management certifications). • Have overall compliance program and officer(s).

[1]

The requirements are obviously quite stringent, and only four such licenses have been issued to date.[2] Many firms are undoubtedly opting for non-compliance because of some of the burdens placed on businesses operating under the license and because the broad language of the bill has made government repercussion difficult. There was also strong pushback from the crypto community during the process of drafting the original license requirements that led to a few revisions that have been met with mixed reviews. Some of this negativity (along with less incentive)[3] has made states slow to follow in New York's footsteps on licensing cryptocurrency, perhaps waiting on the federal government to wade into the tricky landscape first.

State legislatures have not been totally inactive involving cryptocurrency, however. In March of last year, Arizona passed a law that granted smart contracts the "same legal effect, validity, and enforceability" as normal contracts.[4] Although this type of law is not radically different from others like the Uniform Electronic Transactions Act that deal with electronic contracts, it is an important step forward because it specifically is written based around blockchain technology and helps to continue legitimizing the technology.

Another state-backed program is the Delaware Blockchain Initiative (DBI). DBI was initiated by the state's Governor's office and is a project dedicated to working with businesses in the state to make sure they are not being unfairly regulated over the new technology and to uphold the legality of any shares that are issued by corporations on a blockchain network. Notable not only because of its early mover mentality, DBI is also extremely practical for its

[1] Polk (2014) pg. 3
[2] Brennan (2018)
[3] As the heart of the US financial markets and home to a fast emerging tech scene, New York acted swiftly to regulate the industry because of all the advantages it could purportedly bring to the state. Other states would reasonably not feel such an urgent need if they were mostly home to casual traders or investors.
[4] de Ridder (2017) pg. 17-19

deployment in a state that is "widely regarded as the corporate capital of the US", with almost a million businesses being incorporated there.[1]

Federal Level

Things get more complex at the federal level of cryptocurrency regulation because the government is expected to take a more serious and comprehensive position on a potentially game changing industry. Adding a bit of murkiness to the situation is the fact that no one seems to be quite sure which government agency should be taking charge on the issue. Several entities like the SEC and Commodity Futures Trading Commission (CFTC) have already met with Capitol Hill officials, but some of their angling may be in an attempt to extract additional resources for their budgets.[2] Both agencies have already attempted to wade into the cryptocurrency waters. The SEC has primarily stuck to cases like the ICO fraud discussed earlier as they feel they clearly fall under their purview. The CFTC draws its jurisdiction from the Dodd Frank Act which describes its influence as extending to "leveraged, margined, or financed retail commodity transactions" and which the CFTC interpreted as including cryptocurrencies in 2015.[3] The problem is that companies are exempt from the CFTC if they provide "actual delivery" of the commodity within 28 days. And the head of the CFTC himself is having difficulty defining what "actual delivery" means for a virtual currency.[4] William Michael Cunningham of *American Banker* has argued that the Department of the Treasury should be the government office leading the regulatory charge because of its "clear and historical role in the area of the U.S. currency."[5]

Clearly there is a lot that is still to be decided on U.S. government regulation of cryptocurrency, including not just who will be regulating the industry but how strict they will be over companies or projects that are less formal than many they are used to dealing with. While politicians debate over how to settle the issue, the impending cloud of regulation hangs over the cryptocurrency market. Companies are having a hard time building for the now and planning for the future because they are so unsure over what kind of regulatory structure will ultimately be put into place.

Tax Regulation

One final, major agency that is not being shy about jumping into the fray and that will impact users as well as companies is the Internal Revenue Service (IRS). In the second half of 2017, the IRS sued one of the world's largest crypto exchanges, Coinbase, for customer information so that they could search for underreported income.[6] Coinbase fought the suit but recently lost and handed over the information. It is a safe bet that the IRS will find what they are looking for in the data. According to a TIME Money report, Credit Karma released that of the 250,000 people who had already filed their 2017 taxes through their service, less than 100 of them (under .04%) reported cryptocurrency transactions.[7] This is hardly surprising because the IRS "has not provided comprehensive guidance for tax reporting of virtual currency trading"[8]

---

[1] Klayman, Peck, and Wojciechowski (2017)
[2] Cunningham (2018)
[3] Mourselas (2017)
[4] "Would someone here like to tell me how to define the "actual delivery" of a virtual commodity? The CFTC is working very hard to provide a suitable response to that question." - Commissioner Brian Quintenz (Mourselas)
[5] Cunningham (2018)
[6] Prieto (2017) pg. 60-61
[7] Derousseau (2018)
[8] Prieto, *Journal of Accountancy* pg. 60-61

beyond releasing that stocks and virtual currencies are taxed the same when held as capital assets. Convertible virtual currencies like cryptocurrencies are of interest to the IRS because they create a tax event and a tax liability. The agency is still trying to flesh out its policies on the topic though. It is unclear whether the rules for like-kind exchanges will apply to trading different cryptocurrencies (they do not apply to stocks) and the introduction of futures contracts on cryptocurrencies will complicate the issue even further.[1]

Possible Solutions to Regulation Concerns

It is difficult to outline specific solutions for this situation until it crystallizes in the coming years. Drafting and implementing regulations for an industry as global and complex as cryptocurrency is going to take time, so both projects themselves and consumers have a window to diligently research the implications of proposed legislation. That would be a wise first step for all involved. The Financial Stability Board of the G-20 just set a July 2018 deadline for compiling data and information before moving forward with proposed regulations for its members.[2] In the interim, it will be interesting to see which cryptocurrencies opt to try and work with legislators as they explore options and which ones carry on with business as usual because of their longstanding desire to "circumvent government regulation and financial institutions."[3]Working alongside legislators could be very beneficial for some of the major cryptocurrencies because their expertise in the issues involved could help legislators better understand how to classify the currencies and avoid them unintentionally enacting a piece of legislation with dire consequences.

Conversely, some governments will look to impose strict regulations in order to curb illegal transactions and tax evasion while there are already a few nations that are preparing to become a haven for cryptocurrencies. Countries like Switzerland, Singapore, and Estonia are pursuing this strategy as they seek to "become hubs for a new wave of business financing".[4] This will present cryptocurrencies with an interesting option. They can theoretically relocate to one of these countries or one like it and continue to operate as they please, and may even see tax or operational advantages because of it.

The trickier part concerns users. Although the IRS has not issued comprehensive official policies yet on cryptocurrencies, there is already precedent for them taxing oversees investments if that is what digital currencies based abroad end up being classified as. The Foreign Tax Credit would offset some of an American taxpayer's tax liability but there would be no dodging of taxes like there has been for many years. This has already been shown to be hurting some cryptocurrencies. Recently, a drop in the price of bitcoin was attributed to investors selling their holdings to avoid paying taxes from 2017.[5]

All of the concern and anxiety could be for naught though. After a short decline from imposed regulations, both Japan and Australia saw their markets rise again.[6] While not the size of the US market, Japan especially has a large cryptocurrency market that gives hope to the idea that a similar situation could occur here. Regulation would also bring a couple reasons for optimism to cryptocurrencies. Many consumers would feel more assured in interacting with a

[1] Prieto (2017) pg. 60-61
[2] Rooney (2018)
[3] Vanian (2018)
[4] Hackett (2017)
[5] Chung (2017)
[6] Hosp (2018)

currency that has been vetted by a government, and that added sense of credibility could go a long way in legitimizing the industry.

Current Winner: Ripple

Ripple is already being proactive in addressing policy concerns (another example of the advantages of its strong leadership structure). Its CEO, Brad Garlinghouse, believes that it is best to "work within the system" instead of fighting inevitable change and hopes that doing so will allow Ripple and other forward thinking currencies to enter the mainstream.[1] Ripple also benefits from its software being used largely by institutional investors, avoiding a bulk of the illegal transactions that will undoubtedly burden other currencies. There is a final angle that will be interesting to watch with Ripple that could afford it an even more advantageous position. Because of its growing relationships with some of the world's largest banks, it would not shock me to see some of them try and use their considerable legislative influence to assist Ripple in securing a positive regulatory outcome.

3.5 Quick Hitters

There are a few other topics that I wanted to mention as problematic without going in-depth on. While the main focus of this thesis is to explore the most impactful areas on the current and future viability of individual cryptocurrencies in the marketplace, these additional areas warrant general review. The reason for their concision may be that they are less important or urgent for the future of the cryptocurrency, outside the scope I wanted to focus on, or because there is still not enough data or research to expound on them in detail.

-**International Law**-The US is far from the only country interested in regulating this market, and is in fact behind many other nations. Many Asian countries in particular have been aggressive in regulating and even banning some currencies or exchanges.

-**Price Volatility-**this issue has been mentioned throughout this paper and is still a major concern among many investors. To make major headway as a commonly accepted currency, a cryptocurrency will have to demonstrate that it can be redeemed for a fairly stable price over lengths of time.

-**Speed/Scalability-**the speed of a blockchain network in verifying transactions is dependent on multiple factors, but there is legitimate concern that as the number of transactions on the network grows that the process will become a bottleneck. For perspective, Visa handles around 1,700 transactions per second (and has the capability to handle 24,000) while Bitcoin can currently handle seven transactions per second.[2]

-**Energy Usage-**This problem relates mostly to the mining that is required on some networks, so it does not apply to all cryptocurrencies. Because mining is competitive and more energy intensive mining rigs can give miners an advantage, energy costs have been soaring as the industry has grown. It was estimated in 2017 that Bitcoin mining accounted for .14% of all of the world's energy consumption.[3]

[1] Vanian (2018)
[2] Frankenfield (2018)
[3] Gregerson (2018)

4 Conclusion

Success is not a concrete idea in any industry, but is particularly difficult to pinpoint in the cryptocurrency market. For example, some altruistic creators might consider a cryptocurrency a success if it gives users a more secure and intermediary-free alternative to fiat currency, even if there are only a dozen of those users. Others might consider a cryptocurrency successful if many use it to make money through capital appreciation, even if it is providing little to no real utility while doing so. So with that caveat that the definition of success will always be a source of debate, here are my proposed criteria for evaluating the success of a cryptocurrency.

-Currency Price/Market Cap-This is an easy one. It is useful because it is easily quantified and can be used for comparison, and is the simplest reflection of the value that users attribute to a particular currency.

-Price Stability-In its short history, the cryptocurrency market has always been known for its extreme price volatility. In order to continue moving forward toward increased legitimization, it will be necessary for a cryptocurrency to show users (and large institutional investors especially) that it can be traded for a relatively stable rate that is at least consistent in a certain range over time like fiat currencies.

-Widespread Adoption-This is referring to attracting a deep and diverse user base to undergird growth and allow a currency to more easily overcome negative events. It is somewhat reflected in market cap, but that does not totally account for the number of users and does not reveal anything about the type of users. Only by building a currency that appeals to and services people from all walks of life will a cryptocurrency be able to reach the billing of world changing technology.

-Utility-These are all interrelated and a product that offers greater utility should reach a wider audience in theory. But some cryptocurrencies may provide a game changing advantage to some industries that does not have much usefulness outside of that industry; or a currency might hold the promise of impactful technology but fail because of poor marketing. Providing utility will not guarantee a cryptocurrency staying power, but a cryptocurrency that does not provide any new use will not survive for long.

-Adaptability-The market is still very young for cryptocurrencies, but change has been one of the few constants. The ability to adapt and pivot to continue providing a useful currency to consumers is going to be a necessity as more change is assured, at the very least by impending regulation.

Using my proposed criteria, I will conclude by selecting an overall "winner" or "leader" in the cryptocurrency market. To be clear, this title is who I believe has the best combination of these necessary attributes to have sustained success into the near future.[1]

[1] I am setting an arbitrary timeline of 2-4 years on this. Even that may be far too long in an industry this volatile, but it provides enough time for changes to occur and the market to adapt.

Based on a combination of all factors, **Ripple (XRP)** stands out as being poised to carve out a dominant position among cryptocurrencies. XRP rose a meteoric 2017 to take the third place spot in market cap among all cryptocurrencies at just over $27 billion. There is not a widely accepted volatility index for cryptocurrencies yet like there is for stocks, but one analysis rates Ripple as one of the least volatile in the market.[1] It is traded on most major exchanges, but still has opportunities to grow its user base, as it is still not featured on a few large exchanges like Coinbase.[2]

Its partnerships with American Express and Western Union (and rumored to be in talks with Google Pay) reflect how promising many large scale institutions see the technology as and have helped legitimize XRP more than its competitors. As mentioned in earlier sections discussing solutions to current problems, Ripple's strong leadership team has already demonstrated their ability to proactively read the market and be out front on necessary changes. Ripple's strong market presence in the present and positive positioning for the future all point toward it being able to emerge as one of the dominant cryptocurrencies for the foreseeable future.

As you can hopefully now see, the world of cryptocurrency is nearly as complex as it seems to be at first blush. The market is still developing, and there is plenty of reason for both optimism and pessimism, creating a wide variance in potential outcomes. External factors in the market will play an outsized role in determining the ceiling of the marketplace, but there is still much that individual cryptocurrencies can and should be doing to increase their chances of a successful future.

[1] "Price Volatility in Cryptocurrencies—Beta Analysis for Altcoins" (2017)
[2] https://www.coinbase.com/

Works Cited

Acheson, Noelle. "**How Does Proof of Work, um, Work?**." June 6, 2016 Web. <https://decentralize.today/how-does-proof-of-work-um-work-f44642b24215>.

Bajpai, Prableen. "**The 6 Most Important Cryptocurrencies Other Than Bitcoin**." December 7, 2017 Web. <https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/?utm_source=personalized&utm_campaign=www.investopedia.com&utm_term=11948183&utm_medium=email>.

Bearman, Sophie. "**Bitcoin's Origin Story Remains Shrouded in Mystery**." October 27, 2017 Web. <https://www.cnbc.com/2017/10/27/bitcoins-origin-story-remains-shrouded-in-mystery-heres-why-it-matters.html>.

Bereznak, Alyssa. "**"I'm Not Worried About the Price": A Recent Visit to Silicon Valley's Unofficial Bitcoin Headquarters**." December 27, 2018 Web. <https://www.theringer.com/tech/2017/12/28/16825892/crypto-castle-december-2017-profile>.

"**Bitcoin Wallets for Beginners: Everything You Need to Know**." Web. <https://cointelegraph.com/bitcoin-for-beginners/what-is-bitcoin-wallets#why-you-need-a-bitcoin-wallet>.

Bitcoins in Circulation. Blockchain Info, 2017. Print.

Brennan, Sarah. "**Contortions for Compliance: Life Under New York's BitLicense**." January 21, 2018 Web. <https://www.coindesk.com/contortions-compliance-life-new-yorks-bitlicense/>.

Browne, Ryan. "**Banks are Staying Away From Bitcoin 'Bubble' Due to Money Laundering, Credit Suisse CEO says**." November 2, 2017 Web. <https://www.cnbc.com/2017/11/02/credit-suisse-ceo-banks-staying-away-from-bitcoin-bubble.html>.

Burr, William E. "**Data Encryption Standard**." *In A Century of Excellence in Measurements, Standards and Technology - A Chronicle of Selected NBS/NIST Publications 1901-2000.*, 2001. 250-251-253. Print.

Butterfield, Andrew, and Gerard Ekembe Ngondi, eds. *A Dictionary of Computer Science* . Oxford University Press, 2016. Print.

Castor, Amy. "**IOHK Launches Cardano Blockchain; Ada Now Trading on Bittrex**." October 2, 2017 Web. <https://bitcoinmagazine.com/articles/iohk-launches-cardano-blockchain-ada-now-trading-bittrex/>.

Cheng, Evelyn. "**Jamie Dimon says if you're 'stupid' enough to buy bitcoin, you'll pay the price one day**." October 13, 2017 Web. <https://www.cnbc.com/2017/10/13/jamie-dimon-says-people-who-buy-bitcoin-are-stupid.html>.

Christin, Nicholas. *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace*. Carnegie Mellon University, 2012. Print.

Chung, Samantha. "Bitcoin Price Crashed in Mass Selloff as Crypto Owners Try to Avoid Taxes." March 16, 2018 Web. <https://www.investopedia.com/news/bitcoin-price-crashed-mass-selloff-crypto-owners-try-avoid-taxes/?utm_source=personalized&utm_campaign=www.investopedia.com&utm_term=12584923&utm_medium=email>.

Cox, B., Tygar, J. D., & Sirbu, M. (1995). NetBill security and transaction protocol. In Proceedings of the First USENIX Workshop on Electronic commerce (Vol. 13). Retrieved from http://static.usenix.org/publications/library/proceedings/ec95/full_papers/cox.ps

Cunningham, William Michael. American Banker; New York, N.Y. [New York, N.Y]23 Feb 2018.

Damordan, Aswath. ***The Crypto Currency Debate: Future of Money Or Speculative Hype?***. Musings on Markets:, 2017. Print.

de Ridder, C. A., Tunstall, M. K., & Prescott, N. (2017). Recognition of Smart Contracts in the United States. *Intellectual Property & Technology Law Journal*, *29*(11), 17-19.

Derousseau, Ryan. "**The IRS Is Cracking Down On Cryptocurrency Transactions. Here's What That Means For You**." March 5, 2018 Web. <http://time.com/money/5178950/the-irs-is-cracking-down-on-cryptocurrency-transactions-heres-what-that-means-for-you/>.

Dikusar, Aleksandra. ***Smart Contracts: Industry Examples and use Cases for Business***. https://xbsoftware.com/blog/smart-contracts-use-cases/: XB Software, 2017. Print.

Donovan, Paul. *The Long and the Short of it*., 2017. Print.

ElBahrawy, Abeer, et al. "Evolutionary Dynamics of the Cryptocurrency Market." *Royal Society Open Science* (2017)Print.

"Ethereum." 2018. Web. <www.ethereum.org>.

Fernando, Jason. "Bitcoin vs. Litecoing: What's the Difference?" December 22, 2017 Web. <https://www.investopedia.com/articles/investing/042015/bitcoin-vs-litecoin-whats-difference.asp?utm_source=personalized&utm_campaign=www.investopedia.com&utm_term=11759005&utm_medium=email>.

Ferriss, Tim. "The Quiet Master of Cryptocurrency-Nick Szabo." *The Tim Ferriss Show* , 2017.

Foerster, Jan-Henrik. "**Bitcoin Is the 'Very Definition' of a Bubble, Credit Suisse CEO Says** ." November 2, 2017 Web. <https://www.bloomberg.com/news/articles/2017-11-02/bitcoin-is-very-definition-of-a-bubble-credit-suisse-ceo-says>.

Frankenfield, Jake. "Bitcoin vs. Bitcoin Cash: What's the Difference?" November 6, 2017 Web. <https://www.investopedia.com/tech/bitcoin-vs-bitcoin-cash-whats-difference/?utm_source=personalized&utm_campaign=www.investopedia.com&utm_term=11906542&utm_medium=email>.

Fuscaldo, Donna. "Bitcoin Price More Likely $100 Than $100K in a Decade: Harvard Economist." March 6, 2018 Web. <https://www.investopedia.com/news/bitcoin-price-more-likely-100-100k-decade-harvard-

economist/?utm_source=personalized&utm_campaign=www.investopedia.com&utm_term=12518652&utm_medium=email>.

Gandal, Neil, and Hanna Halaburda. “Can We Predict the Winner in a Market with Network Effects? Competition in Cryptocurrency Market.” *Games* 7.3 (2016): 16. *Crossref*. Web.

Grant, Nico. "Vanguard Founder Jack Bogle Says 'Avoid Bitcoin Like the Plague'." November 28, 2017 Web. <https://www.bloomberg.com/news/articles/2017-11-28/vanguard-founder-jack-bogle-says-avoid-bitcoin-like-the-plague>.

Gregerson, Erik. "Bitcoin." (2017)Print.

Hackett, Robert. "**7 Cryptocurrency Predictions From the Experts**." July 25, 2017 Web. <http://fortune.com/2017/07/25/bitcoin-ethereum-cryptocurrency-predictions/>.

Heilman, Ethan, et al. "TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub." Boston University, 2016. Print.

Heltman, J. (2017). Wider cryptocurrency use could harm system stability: Fed’s Quarles. *American Banker*, *182*(230), 1.

Hosp, Julian. "**Five reasons 2018 could be the best year yet for cryptocurrencies**." February 23, 2018 Web. <https://www.cnbc.com/2018/02/23/bitcoin-ethereum-other-cryptocurrency-five-positive-factors-for-2018.html>.

John Roberts, Jeff. "Michael Arrington Has a New $100 Million Hedge Fund That Will Be Valued In Ripple's XRP." November 28, 2017 Web. <http://fortune.com/2017/11/28/arrington-xrp/>.

Klayman, Joshua Ashley, Geoffrey Peck, and Mark and Wojciechowski. "**Why The Delaware Blockchain Initiative Matters To All Dealmakers**." September 20, 2017 Web. <https://www.forbes.com/sites/groupthink/2017/09/20/why-the-delaware-blockchain-initiative-matters-to-all-dealmakers/#13f53e087550>.

Korosec, Kirsten. "The Rise of Ripple." December 27, 2017 Web. <http://fortune.com/2017/12/29/ripple-cryptocurrency-surge/?utm_source=fortune.com&utm_medium=email&utm_campaign=term-sheet&utm_content=2018010214pm>.

Law, Jonathan, ed. *A Dictionary of Business and Management*. 6th ed. ed. Oxford University Press, 2016. Print. "Functions of Money" .

Lee, Timothy. "**Bitcoin Fees are Skyrocketing**." December 11, 2017 Web. <https://arstechnica.com/tech-policy/2017/12/bitcoin-fees-are-skyrocketing/>.

Liebkind, Joe. "Is Litecoin the Future of Cryptocurrency?" December 11, 2017 Web. <https://www.investopedia.com/news/litecoin-future-cryptocurrency/?utm_source=personalized&utm_campaign=www.investopedia.com&utm_term=11582082&utm_medium=email>.

Marr, Bernard. "**A Short History Of Bitcoin And Crypto Currency Everyone Should Read**." December 6, 2017 Web. <https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/2/#7dee7bf3533c>.

Martindale, John. "**What is Litecoin? Here's everything you need to know**." January 28, 2018 Web. <https://www.digitaltrends.com/computing/what-is-litecoin/>.

McLellan, L. (2017). "The Crypto Market is Growing Up". *Globalcapital*, 1.

McMillan, Robert. "**The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster**." *Wired* March 30, 2014Print.

Meyer, David. "The Dangerous Reason Why Bitcoin Just Hit Yet Another New High." 2017. Web. <http://fortune.com/2017/11/01/bitcoin-6600-high-cme-futures/?utm_source=fortune.com&utm_medium=email&utm_campaign=term-sheet&utm_content=2017113014pm>.

Mourselas, C. (2017). "CFTC: Crypto Regulation Needs Clarity". *Globalcapital*, 1.

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. bitcoin.org, 2008. Print.

Patrick Eha, B. (2017). World's biggest bitcoin exchange launches in U.S. as currency nears $10K. *American Banker*, *183*(228), 1.

Polk, Davis. *"New York July 2014 "BitLicense" Proposal: Visual Memorandum"*. Davis Polk & Wardwell LLP, 2014. Print.

Prieto, T. (2017). Trading Virtual Currencies. *Journal Of Accountancy*, *224*(5), 60-61.

"Protocol Rules." August 25, 2017 Web. <https://en.bitcoin.it/wiki/Protocol_rules>.

Reiff, Nathan. "3 Obscure Cryptocurrencies to Watch." December 1, 2017 Web. <https://www.investopedia.com/news/3-obscure-cryptocurrencies-watch/?utm_source=personalized&utm_campaign=www.investopedia.com&utm_term=11750772&utm_medium=email>.

Reuters. "**Europe Is Pouring a Staggering Amount of Cash Into New Cryptocurrencies**." 2017. Web. <http://fortune.com/2017/11/30/ico-initial-coin-offering-bitcoin-europe/?utm_source=fortune.com&utm_medium=email&utm_campaign=term-sheet&utm_content=2017113014pm>.

Revill, John. "**Credit Suisse CEO skeptical about Bitcoin 'bubble'**." November 2, 2017 Web. <https://www.reuters.com/article/us-creditsuisse-bitcoin/credit-suisse-ceo-skeptical-about-bitcoin-bubble-idUSKBN1D2189>.

Rooney, Kate. "**Bitcoin moves above $8,400 after news that 'could have been worse' from G-20 regulators**." March 18, 2018 Web. <https://www.cnbc.com/2018/03/19/bitcoin-moves-above-8400-after-news-from-g-20-regulators.html>.

Rose, Lacey. "**'Silicon Valley' Confronts a "Darker Side" of Tech Culture (and T.J. Miller's Messy Exit)**." March 7, 2018 Web. <https://www.hollywoodreporter.com/features/silicon-valley-confronts-a-darker-side-tech-culture-tj-millers-messy-exit-1092493>.

Rosic, Ameer. "5 High Profile Cryptocurrency Hacks." 2017. Web. <https://blockgeeks.com/guides/cryptocurrency-hacks/>.

---. "Proof of Work vs. Proof of Stake: Basic Mining Guide." 2017. Web. <https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/>.

---. "What is Ethereum? A Step-by-Step Beginner's Guide." 2017. Web. <https://blockgeeks.com/guides/ethereum/>.

Russell, Jon. "**Ripple turns investor as execs lead $25M round for storage and rental startup Omni**." January 16, 2018 Web. <https://techcrunch.com/2018/01/16/ripple-turns-investor-omni/>.

Shen, Lucinda. "**Bitcoin Prices Rebound Following Possibly the Largest Cryptocurrency Hack Yet**." January 26, 2017 Web. <http://fortune.com/2018/01/26/bitcoin-price-coincheck-nem-mt-gox/>.

Siegel, David. "Understanding the DAO Attack." June 26, 2016 Web. <https://www.coindesk.com/understanding-dao-hack-journalists/>.

Smith, Jake. "**The Bitcoin Cash Hard Fork Will Show Us Which Coin Is Best**." August 11, 2017 Web. <http://fortune.com/2017/08/11/bitcoin-cash-hard-fork-price-date-why/>.

Subramanian, Ramesh, and Theo Chino. "The State of Cryptocurrencies, their Issues, and Policy Interactions." *Journal of International Technology and Information Management* 24.3 (2015): 25-40. Print.

Swift, Art, and Steve Ander. ***Americans using Cash Less Compared with Five Years Ago***. http://news.gallup.com/poll/193649/americans-using-cash-less-compared-five-years-ago.aspx:, 2016. Print.

Tepper, Fitz. "**WTF is bitcoin cash and is it worth anything?**." August 2, 2017 Web. <https://techcrunch.com/2017/08/02/wtf-is-bitcoin-cash-and-is-it-worth-anything/>.

Todd, Sarah. "**Banks can Cherry-Pick the Best Bits from Bitcoin: Report**." *American Banker* (2015): https://www.americanbanker.com/news/banks-can-cherry-pick-the-best-bits-from-bitcoin-report. Print.

Toplin, Jaime. "**Merchants aren't accepting bitcoin**." July 14, 2017 Web. <http://www.businessinsider.com/merchants-arent-accepting-bitcoin-2017-7>.

Torpey, Kyle. "**Will Bitcoin's Lightning Network Kill Off Altcoins Focused On Cheap Transactions?**." December 28, 2017 Web. <https://www.forbes.com/sites/ktorpey/2017/12/28/will-bitcoins-lightning-network-kill-off-altcoins-focused-on-cheap-transactions/#627b74d67dab>.

Tu, Kevin V., and Michael W. Meredith. "Rethinking Virtual Currency Regulation in the Bitcoin Age." *Wash.L.Rev.* 90 (2015): 271. Print.

Ulanoff, Lance. "How to Talk to Your Mom and Dad About Bitcoin on Thanksgiving." November 22, 2017 Web. <https://mashable.com/2017/11/22/how-to-explain-bitcoins-to-your-parents/#O_JLG_P4bmqH>.

van Wirdum, Aaron. "Keep an Eye Out for These Bitcoin Tech Trends in 2018." January 2, 2018 Web. <https://bitcoinmagazine.com/articles/keep-eye-out-these-bitcoins-tech-trends-2018/>.

Vanian, Johnathan. "**Ripple CEO Brad Garlinghouse Talks Bitcoin, Banks, and Payments**." February 14, 2018 Web. <http://fortune.com/2018/02/13/ripple-bitcoin-banks-brad-garlinghouse/?utm_source=fortune.com&utm_medium=email&utm_campaign=term-sheet&utm_content=2018021415pm>.

Vigna, Paul. "5 Things About Mt. Gox's Crisis." February 25, 2014 Web. <https://blogs.wsj.com/briefly/2014/02/25/5-things-about-mt-goxs-crisis/>.

"What is Ripple?" February 8, 2018 Web. <https://www.finder.com/ripple>.

Wolfe, Daniel. **American Banker; New York, N.Y.** [New York, N.Y]18 Oct 2005: 10

Yang, Stephanie, and Alexander Osipovich. "**Nasdaq Plans to Launch Bitcoin Futures in First Half 2018**." 2017. Web. <https://www.wsj.com/articles/nasdaq-plans-to-launch-bitcoin-futures-in-first-half-2018-1511968313>.

Yurcan, B. (2017). Is it Time for Bankers to Rethink Bitcoin?. *American Banker*, *182*(230), 1