BLOCKCHAIN FOR THE PUBLIC SECTOR

By

Turner Francis Stanton

A capstone project submitted for
Graduation with University Honors

May 11, 2017

University Honors
University of California, Riverside

APPROVED

_____
Dr. Ronald O. Loveridge
Department of Political Science

_____
Dr. Richard Cardullo, Howard H Hays Jr. Chair and Faculty Director, University Honors
Interim Vice Provost, Undergraduate Education

Abstract

Blockchain is an up and coming technology that will be the next evolution of the current digital world we live and operate in. Currently, most people aren't aware of blockchain, but are aware of the digital currency, bitcoin. Bitcoin is a decentralized monetary system that relies on public verification to bypass the traditional need for intermediaries such as banks and other financial institutions. Blockchain serves as the underlying ledger for Bitcoin to operate. Despite the general publics' limited awareness of blockchain, major corporations, academics, and governments are paying attention to its development and are attempting to be at the forefront. To conduct research into the blockchain, interviews with leaders in technology and the public sector were conducted coupled with independent research through books, databases, and articles.

As a result of this cutting edge development, this senior thesis will focus on two core components. The first component will be an attempt to grasp the operations and potentials of the blockchain ledger. The purpose of this will be to serve as a foundation for educating the public and public officials on the technology. The second and final core component will be to explore the possible application of blockchain to the public sector, specifically, campaign finances and voting. The hope of this exhaustive feasibility study and proposal will be to serve as a model for the public sector to be the leader of the new technology, instead of the inhibitor. Blockchain's implications are the next evolution of the digital world and could impact every aspect of our public and private lives and it is the aim of this project to educate those in leadership positions to appropriately embrace its abilities.

Acknowledgements

A special thank you to Dr. Ronald O. Loveridge who served as the faculty mentor for this senior thesis project. Without Dr. Loveridge's support and guidance, this final project would not have been possible. Dr. Loveridge committed significant time to ensuring research got off the ground and that the excitement for the project remained through fruition. Dr. Loveridge is a visionary and always goes above and beyond his role as a professor as shown by his commitment to this project. Additional thanks are in order for everyone that helped contribute ideas and insights into my quest to learn about the blockchain and its application to the public sector.

The individuals, organizations and institutions that significantly helped in the development of this thesis are: Lea Deesing and Chris Tilden (City of Riverside), The University of Nicosia (Antonis Polemitis & George Papageorgiou), Jim Balistreri, Rob Ewing (Town of Danville) Kazi Mamun, Steve Reneker (County of Riverside), CA Office of the Lieutenant Governor, CA Office of the Secretary of State, San Francisco Ethics Commission, and the Fair Political Practices Commission. Finally, a thank you to my family for being with me throughout the process and bearing through countless conversations about blockchain.

Table of Contents

Lists of Figures

Introduction

Blockchain is a distributed ledger technology that removes intermediaries to streamline processes and transactions for a significantly lower cost than traditional methods. This ledger has the potential to transform every industry and every facet of the digital world we live and operate in today by increasing transparency, accountability, and functionality. Instead of an escrow closing in 30 days and instead of paying significant fees to wire money, blockchain puts the power in the publics' hand to streamline such services by utilizing randomization, mining, and public verification to carry out traditional transactions instead of the existing intermediaries such as Venmo, Bank of America, and others. As shown in *Figure 1: Timeline of Digital Evolution,* we are at the next phase of the digital technology evolution and distributed ledger technologies (blockchains) are the catalysts for this next evolutionary phase. It is important to note that the next evolution is based on blockchain, not the more commonly known bitcoin. Bitcoin is a cryptocurrency that utilizes the blockchain to operate and will not be explored in this thesis. However, it was in large part thanks to understanding that bitcoin operated off of the blockchain that inspired this thesis and that revealed the foundational components' transformative ability. It is critical for the public and leaders in the public sector to be aware of what blockchain is. Awareness will ensure that rules or regulations are not created out of the fear of not knowing the possible applications this new technology could have.

This thesis is inspired by the major shifts of the internet today and focuses on applying the next evolution, the blockchain, to the public sector. The first focus is for the researcher to gain a grasp on the blockchain to then promote the knowledge of blockchain

to educate the public and specifically, to educate public officials. The purpose of this is to discourage regulations from being passed out of fear for not knowing the technology and with a goal of getting government at the forefront, instead of behind the technological development. Secondly, with the newfound knowledge of what the blockchain is and how it operates, this thesis will outline a feasible way to apply the blockchain to the public sector with a priority on campaign finances and voting. It is believed that the blockchain holds as much promise for the public sector as it does for the private sector. Form 700s that disclose a public official's financial holdings and assets and campaign donations from individuals, corporations, and PACs can be published on the blockchain in an immutable format. This would give anyone the opportunity and ability to see such holdings and donations to prevent these forms and disclosures from being edited. Furthermore, votes can be cast and counted in a matter of moments while ensuring no voter fraud has occurred. The applications are limitless for blockchain and this thesis focuses on the applications in the public sector.

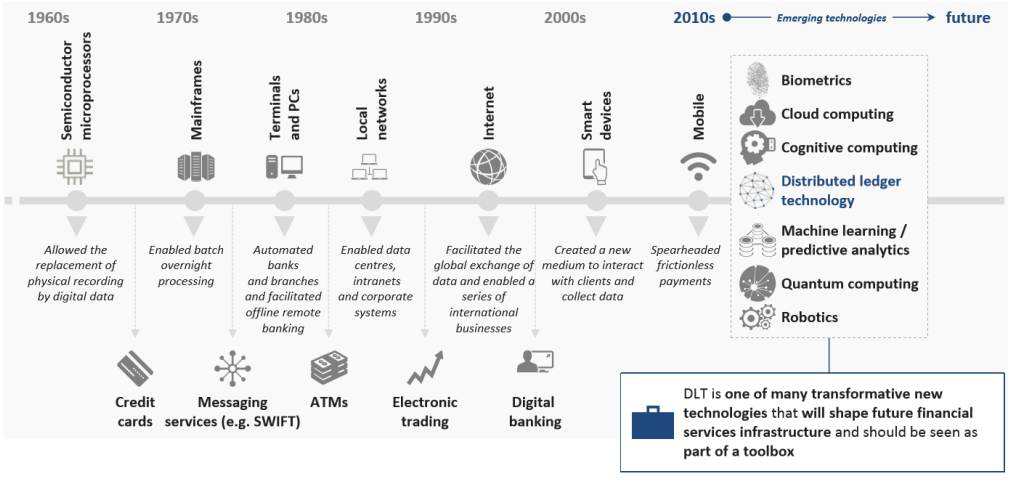

Figure1: Timeline of Digital Evolution (Source: World Economic Forum, 2016)

Main Research Question: What is the blockchain and how can it be applied to the public sector?

Objectives

1. Educate the public and particularly bring the blockchain to the attention of public officials and educate them about the technology with an aim to discourage any unnecessary or potentially stifling rules and regulations.

2. Provide a feasible application of the blockchain to campaign finance reform, specifically campaign donations and financial disclosure forms submitted by public officials and to voting.

Method and Methodology

Independent research focused on articles, databases, books, and an online course with the University of Nicosia was the primary method of research. To complement and strengthen independent research, the use of participants was used in an interview and dialogue based setting with the intent of learning more about blockchain from individuals in the field of technology and the public sector to formulate ideas for public applications. Members from the City of Riverside, County of Riverside, CA Office of the Secretary of State, CA Office of the Lieutenant Governor, General Counsel's Office for the Fair Political Practices Commission, the San Francisco Ethics Commission, and those aware of blockchain were consulted. Internal Review Board (IRB) approval was granted on 02/10/2017.

This method was optimal because it enabled the researcher to understand the blockchain technology, formulate ideas for its application, and test those ideas on individuals interviewed. Those interviewed aware of the technology could provide further insights into its application and individuals a part of the public sector could provide insights into any current use of blockchain and the feasibility of proposed idea(s).

Current Digital Landscape

Blockchain is a distributed ledger technology that has the potential to restore the openness and security that was originally envisioned when the internet went live. The many innovations and applications enabled by the web have exposed major concerns regarding data security and your claim to owning your own data. Target Corporation is the perfect case example of the increasing concerns regarding data security when hackers in 2013 stole, "up to 40 million customers credit and debit information" (Yang and Jayakumar, Washington Post). Target's case was only the beginning of major public hacking incidents. As shown in *Figure 2: Number of Cyber Security Incidents*, not only has United States Federal Agencies had their vulnerabilities exploited by hackers, the number of attacks is on a significant rise, increasing by over 71,000 in a nine year period. Personal data stored online, or used to carry out transactions, is increasingly vulnerable to hackers because hackers are becoming more sophisticated and companies are unable to keep up with the volume of attacks. Beyond the growing concerns over security online, there is growing concern revolving around individual rights to privacy and data control.

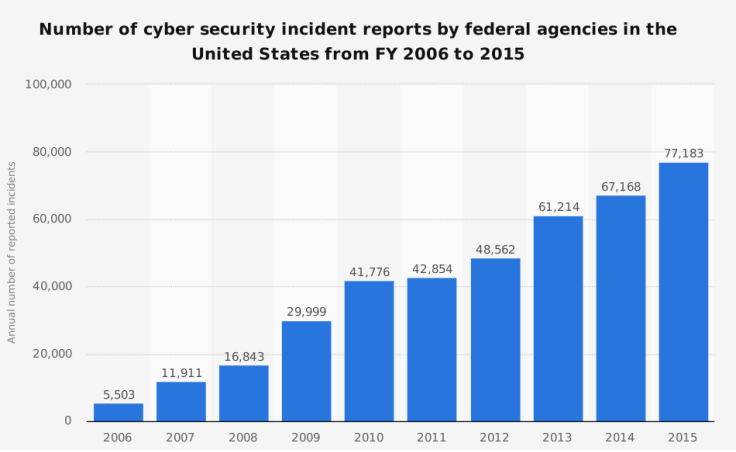

Figure 2: Number of Cyber Security Incidents

(Source: US Office of Management and Budget, US Department of Homeland Security; GAO, Statista, 2017)

The more we utilize the internet and mobile applications, the more public our private lives become. The data we create through searches on the internet, or mobile applications downloaded on our devices gives companies a near limitless freedom to do anything they want with our data. This reveals the second major concern with online privacy and the ability (or growing inability) for an individual to own their own data. An example of the near complete lack of control we have over our online behavior history stems from the terms of service agreements we are required to acknowledge before using any "free" service or before downloading a "free" app. The word free is in quotation marks, because the famous saying "there's no such thing as a free lunch" applies to the digital world today because we are all paying for those "free" applications and "free" web services by giving the companies and developers near complete control over our data to use and sell at their discretion. Due to terms of service agreements required to be acknowledge before using free services such as Google Docs, Marc Goodman in his book *Future Crimes,* gives the vivid example of the costs of free services by stating, "If J.K. Rowling had written Harry Potter in Google Docs Instead of Microsoft Word, she would have granted Google the worldwide rights to her work…" (Goodman, 59). This extreme, but real possibility shows that we are often forced to 'agree' to a terms of service that grants the service provider limitless rights to our data and work, removing the openness and privacy to our online interactions.

These cases are alarming because they reveal the flaws in data security and the loss of privacy online through the increasing connectedness of applications and web services. As a result, the blockchain has emerged to be the next evolution of the internet. Blockchain's implementation can help establish rigorous data security that is often overlooked and can

place the individual user back in control of their data and information. Because of the blockchain's many applications to increasing security, transparency, and accountability, the blockchain can be leveraged to create a transparent and public system of campaign finance reform and a streamlined voting process. To understand the basics of blockchain, the industry leading and accepted definition must be outlined, accompanied by a real-life example (without the technological jargon) of what a blockchain looks like.

What Is Blockchain?

What is the blockchain? This is the single most important question given the aforementioned growing concerns associated with the present digital world, the blockchain proving to be the next evolution of technology and the scope of this thesis. The blockchain, in the simplest sense, is a distributed ledger technology. What is a distributed ledger? A distributed ledger (blockchain) is a network that removes traditional intermediaries or central managers such as mobile payment services like PayPal or more traditional intermediaries such as Bank of America, Wells Fargo, and others to facilitate and verify transactions by operating off of a pooling of computing power from various computers to streamline transactions. This pooling of computing power is known as a Peer-to-Peer (P2P) system.

P2P increases transparency because information on the blockchain or transactions that occur on the blockchain are publically available on an immutable thread, and cheaper because intermediaries cannot charge significant transaction fees. The notion of a P2P system and the underlying blockchain ledger was developed in the midst of the 2008 financial recession in the United States of America when Satoshi Nakamoto published his white paper, *Bitcoin: A Peer-to-Peer Electronic Cash*. Nakamoto established in large part as a result of the hard hit financial services sector that, "What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party" (Nakamoto, 1). The blockchain's ability to facilitate transactions and record information without a third party, thanks to complicated algorithms that can only be solved (or

"mined") by intensive computing systems on the distributed network is the truly evolutionary component of blockchain and its many promises for the future.

To highlight why blockchain is evolutionary and extremely applicable, *Figure 3: Traditional Process for a Credit Card Transaction* shows how cumbersome a traditional credit card transaction is today. The time and costs involved simply to verify a person has the necessary funds to make a purchase is too intensive and costly given the technological advances. Instead of this process, blockchain's three core operating components as outlined by Don and Alex Tapscott in their book *Blockchain Revolution,* distributed, public, and encryption could be applied instead.

- "Distributed: no central data base for hacking, runs on computers provided by volunteers around the world
- Public: anyone can view it at any time because it resides on the network, not within a single institutions database
- Encrypted: public and private keys…to maintain virtual security (Tapscott, 6-7)".

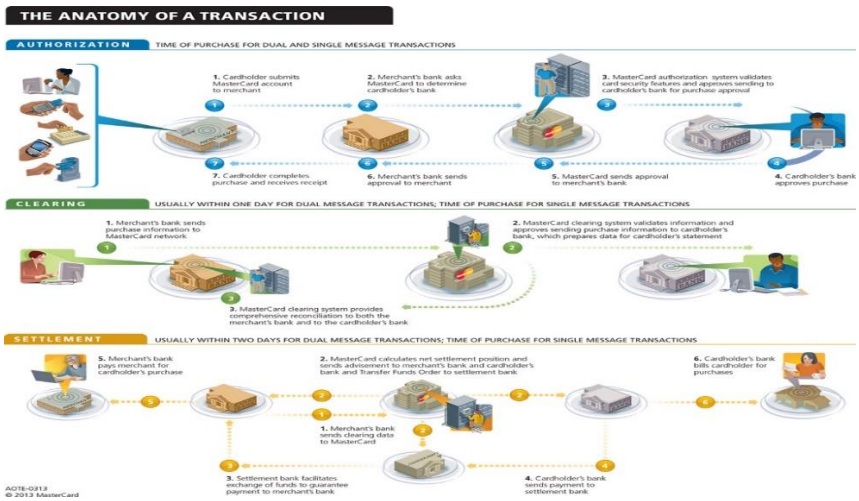

Figure 3: Traditional Process for a Credit Card Transaction (Source: unibulmerchantservices.com)

With these core components of the blockchain underlying a transaction, the operation will be distributed, public, and encrypted as Tapscott outlined above. On the blockchain, a credit card (or digital payment) transaction would take place across a distributed network. Everyone would be able to see the transaction occur, anyone could verify the payment based on their central processing units' ability to solve an algorithm proving necessary funds exist, and personal data of the card holder and shop would be encrypted through public and private keys making it much more secure than present centralized databases or clouds. Most importantly, the shop would receive the money almost instantly and not be required to pay significant transaction fees. As Tsukerman provides in his work *The Block Is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future*, "Merchants must pay a variety of authorization fees, transaction fees, statement fees, interchange fees, and customer service fees, to name a few. These fees amount to 2 to 3 percent of the transaction" (Tsukerman, 1140). 2 to 3 percent is a significant amount of a sale for small businesses, thus as a result of blockchain, small business would be able to retain greater profits by paying less money to process digital payments.

To further develop what a blockchain transaction would look like, *Figure 4: Typical Blockchain Process* provides a strong depiction of a current transaction utilizing a cryptocurrency, which is a fancy term for digital money. This outline shows how a transaction (in this case, a bitcoin payment) is exchanged from one user to another utilizing the blockchain ledger. The process of a blockchain transaction highlighted in this illustration are:

1. A transaction is sent over the peer to peer (P2P) network.

2. Everyone can see this transaction taking place on the public ledger.
    a. The message is sent encrypted via a private key that belongs to the sender of the bitcoin, only a public key by the individual it is sent to, can decrypt the message and enable the user to access the bitcoins that were sent (University of Nicosia).
3. Miners verify the message by establishing the longest block.
    a. Miners are not what is traditionally thought of when the term miner is read. Miners for blockchains are the "nodes", or the computers that are distributed throughout the P2P network. These nodes are running intensive algorithms to verify the transaction. The node that completes the longest algorithm/block provides the verification.
4. The transaction is deposited into the intended receiver's wallet with a small amount being provided to the miner who created the longest block.
    a. A block is the immutable record of the transaction that occurred, no one can alter the block once it is published, thus the record will be forever available for any member of the public to see and review.

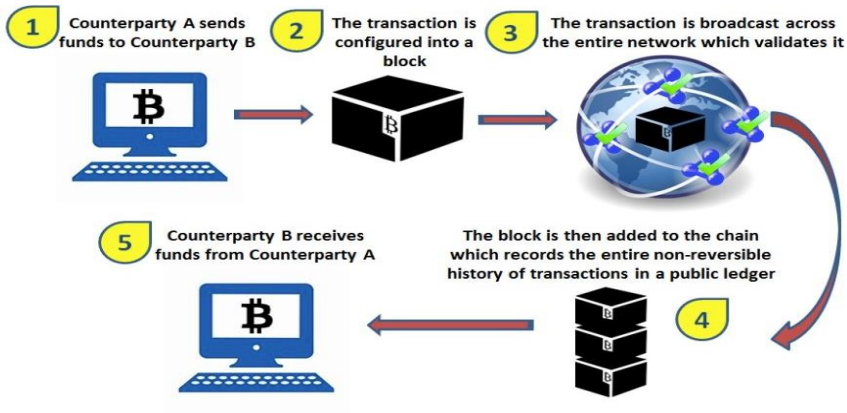

Figure 4: Typical Blockchain Process
(Source: Goldman Sachs Global Investment Research)

Byzantine Generals Problem (BGP)

Another key component of blockchain is its ability to overcome the inherent flaw of original decentralized systems: double spending or malicious actors, also known as the Byzantine Generals Problem (BGP). Alex Tapscott at a Tedx talk in San Francisco explained that, “When you use the internet today, you are sending a copy and retaining an original…except when it comes to things that have value like say money, sending a copy is a bad idea”. This issue of ensuring copies of money are not sent is what led to the rise of intermediaries to verify and prove a transaction occurred. When early digital money platforms emerged, the most difficult thing to create was a system that did not allow someone to act as a malicious actor by retaining the money they spent, the BGP.

BGP showcases the inherent issue with a system when a traitor or malicious actor is present. As *Figure 5: Byzantine Generals Problem (BGP)* shows, lieutenant #2, the yellow oval, is a traitor to the general and communicates the wrong message to lieutenant #1, the two blue ovals. As a result, lieutenant #2 has caused the original message of ‘attack’ to be turned into ‘retreat’. The morning of the attack, the general and his troops will be overwhelmed by the city they have planned to attack because they will realize the two reinforcements have retreated from the battlefield as a result of the traitors falsely communicated message. This illustration of the BGP is exactly what can occur in the digital world when a hacker or malicious actor can attempt to “double spend” and provide false information during a transaction.

This potential hijacking has been the inherent issue with a decentralized system and only increases with the number of users. Blockchain has overcome the BGP difficulty through randomization, mining the longest block and public verification.

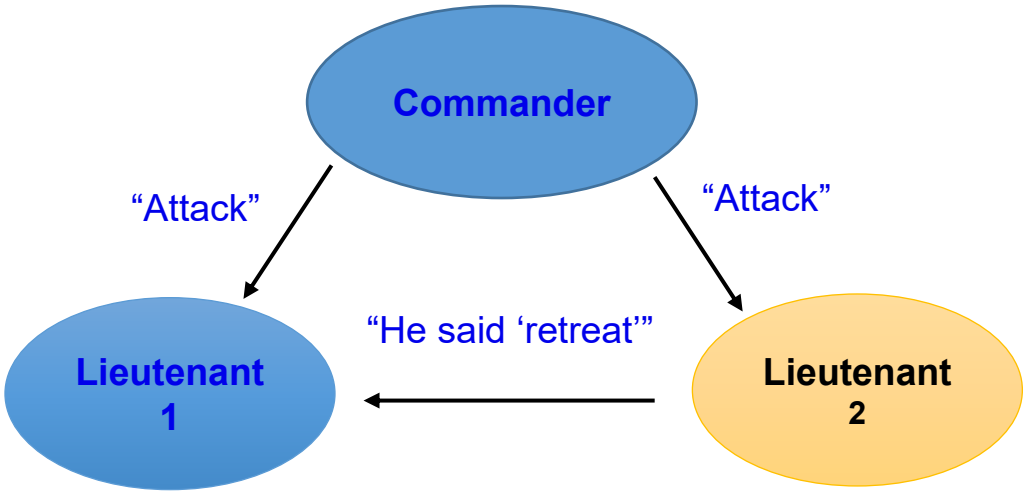

Figure 5: Byzantine Generals Problem (BGP)

Blockchain in Place of Venmo, a Current Day Illustration

Without the technological jargon accompanying a typical blockchain process as we have seen in the prior pages, allow me to provide a real world example. The example focuses on what a payment transaction looks like today given existing payment applications and what it could look like if blockchain was used instead of corporations to verify transfers of payments. Let us assume that an individual needs to repay their friend $20 for helping pay for a meal. In this situation, both individuals have the current popular mobile application, Venmo on their smartphones. Venmo allows these two to seamlessly transfer money between each other despite having different banks. Venmo, like many mobile applications is free to download and mostly free to use. When the individual sends the $20 through the Venmo mobile application, $20 is taken out of their account and placed in the account of the receiving individual. This transfer of money would be equivalent to a "chain" in the blockchain, it is the record or history of the transaction. One individual's account shows a debit of $20 and the other shows a credit of $20. However, this process is not as instant and seamless as it appears to be.

As outlined on Venmo's website, "Bank transfers submitted before 7 PM Eastern Time will typically reach your bank account in 1 business day. However, all withdrawals are reviewed by us and may be delayed or blocked if we identify a problem. Bank transfers will not be deposited on weekends or bank holidays" (Venmo.com). This shows that despite the individual transferring $20 to their friend, the $20 will not be available in their bank account for at least one business day. Once the payment has cleared, this is what can be considered a "block" on the blockchain. The $20 has been settled and it has been established that one individual no longer has $20 because $20 was posted to the

other individuals' account in a 'block'. Why is it that given the interconnection of the internet and the seamless ability to share data, that sending money over a mobile application takes at least a full business day to clear? Before showing how blockchain can address that question, we must also see how this "free" application is not as free as it appears to be.

Venmo spells out the actual costs that are incurred by using its service on its terms of service and statement of privacy which can be found on its website and application. According to Venmo's terms of service and privacy statement, "When you visit the website or use one of our mobile applications, we collect your IP address, and standard web log information, such as your browser type and the pages you accessed on our website. We also may collect certain geo-location information. If you do not agree to our collection of this information, you may not be able to use our Service…Venmo charges a 3% fee for payments by credit card" (Venmo.com). These terms of service show that this application is anything but free because Venmo collects important and sensitive personal data collected from your device while also taking a 3% transaction fee. Although Venmo states it does not sell personal information (such as your geolocation) to third parties, can Venmo ensure the data it collects is safe from a potential hacker looking to obtain such data to sell to third parties? When looking under the hood of how Venmo operates, it becomes apparent that it is not as free and instant as it is often believed to be. Let's look at how this entire transaction could be faster and cheaper if blockchain is employed instead.

Using blockchain (a distributed ledger), instead of Venmo to repay an individual $20 would be more secure, cheaper and faster. Instead of downloading a mobile

application, the two individuals would download an open source wallet of their choice to serve as their place of storing their digital money. When one individual needs to repay the other $20, the money is sent in the form of the cryptocurrency of their possession over the network. The transfer is sent fully encrypted and can only be decrypted by the recipient using a public-private key combination. The transfer of the money is verified through the network and the computer that solves the algorithm to confirm the transaction, receives a small transaction fee, much less than 3%. Once the transaction is confirmed, a block is created making the transaction permanently etched on the blockchain for anyone to see, thus showing that the original sender is no longer in possession of the money that had been sent. This is much more secure because no personal information is exchanged or collected in the process, nor is it stored in a database or cloud that could be vulnerable to hackers. Furthermore, bank account information is not accessible by hackers because the wallets used in the transaction are purely based in the system, they are not tied to a bank account. Additionally, this is much cheaper because transaction fees collected for verification are significantly less than the existing fees in place for services like Venmo and other intermediaries. Finally, this transaction is much faster, because once it is confirmed by one of the computers, the transfer is complete and the individual that received the money is able to spend it instantly.

Growing Awareness of Blockchain

The first main objective of this thesis is to educate the public, especially public officials about blockchain to encourage dialogue and understanding about the technology before hastily regulating out of fear of the unknown. By understanding the blockchain and its applications, the public sector can be at the forefront, instead of the tail end of innovation. When I decided to research blockchain, I, like many others had heard of bitcoin, but had never heard about blockchain. Many times when talking with individuals at the early stages about blockchain, I would get the response, "What the heck is blockchain?" As a result of this, instead of jumping into the discussion on blockchains, I always asked individuals if they were aware of bitcoin and use this as a reference point to then educate them about the underlying infrastructure of bitcoin: blockchain. I also learned that despite the limited knowledge about blockchain, the excitement for blockchain is evidently gaining momentum.

When I first started researching, limited articles and sources were available, now countless publications are coming out on the topic every day. This trend in growing awareness and understanding of blockchain, even if it's achieved through bitcoin, affirms the ability for this thesis to further bring blockchain to the attention of the public. To showcase the increasing interest in what the blockchain is, *Figure 6: Number of Blockchain Wallet Users* and *Figure 7: Familiarity with Bitcoin* show that people are increasingly not only aware of bitcoin, but are utilizing the distributed ledger. The familiarity with and users of blockchain will only continue to increase. Having the public sector and our public officials at the forefront of this technological evolution will be

paramount to preserve and further established democratic systems. A word of caution is required however regarding bitcoin.

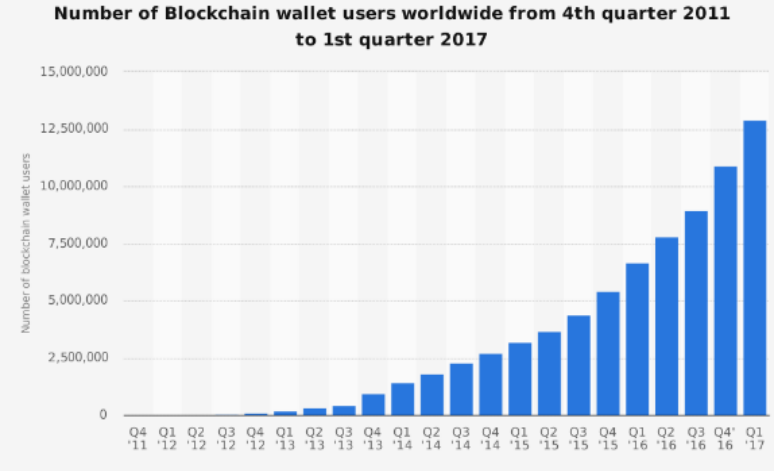

Figure 6: Number of Blockchain Wallet Users (Source: Blockchain, Statista 2017)

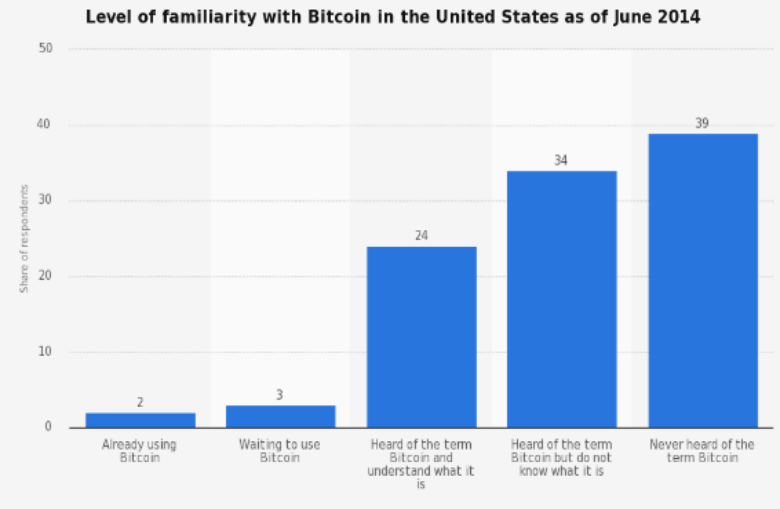

Figure 7: Familiarity with Bitcoin (Source: 451 Group, Statista 2015)

While talking with individuals and using bitcoin as an opening to find out their level of familiarity, I find many individuals are deeply interested in the investment of cryptocurrencies, such as bitcoin. Bitcoin is outside the scope of this thesis and is used purely as a reference point for an application of the underlying blockchain ledger. A word of caution must be provided however because of the enormous interest expressed. As shown in *Figure 8: Bitcoin Price Index*, the price of bitcoin, because of the continual developmental needs of cryptocurrencies and many uncertainties, fluctuates significantly and are thus are extremely volatile. Further highlighting this note is Bloomberg's report on one of the most troubling days for those involved in bitcoin trading when BITFINEX, a digital currency exchange, lost $65 million in a single day as a result of a vulnerability discovered by hackers (Nakamura and Chen, Bloomberg.com). These examples show that cryptocurrencies as investments carry immense risk and could be an entire senior thesis in and of itself. Despite this word of caution, with the blockchain becoming more readily known and identifiable to the public, we have a unique opportunity to have the public sector at the forefront of this technology and pave the way to remove existing barriers that are already hampering innovation.

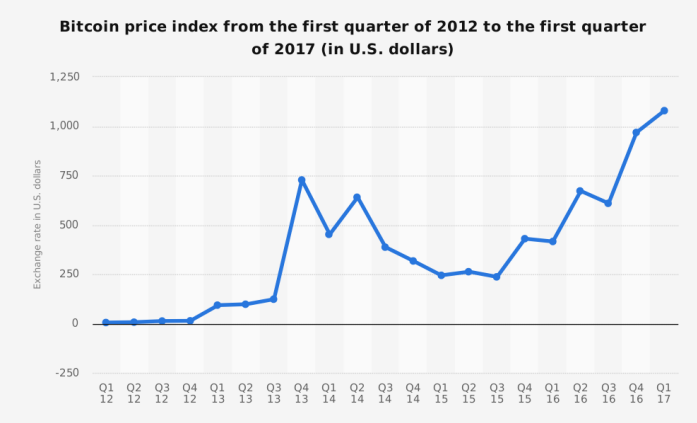

Figure 8: Bitcoin Price Index (Source: Investing.com Statista 2017)

Blockchain and the Public Sector Today: Inhibitors and Trailblazers

The public sector has proved to be both inhibiting and trailblazing in the development and progress of blockchain. Cases that encourage and discourage blockchain development often relate back to bitcoin and crypto based currencies that do not have intermediaries. Although this thesis is focused on applying the underlying technology, blockchain, and not cryptocurrencies to the public sector, efforts at regulating these currencies can project a perception to the business and innovation based communities that might push back blockchain development out of fear of being overregulated or even shut-down. *Figure 9: Reasons for Resistance to Blockchain Adoption* shows that the significant reason (63%) for lack of blockchain adoption is due to regulation. Additionally, *Figure 10: Barriers to Government Adoption to Blockchain* shows that again, the majority reason for limited adoption of blockchain (60%) for the public sector' is regulatory based. Regulatory concerns are a justifiable reason for the slow adoption of blockchain, especially in the public sector. To adopt a new technology, the public sector needs to be certain of not only what it is, but fully reliant upon what it promises to do.

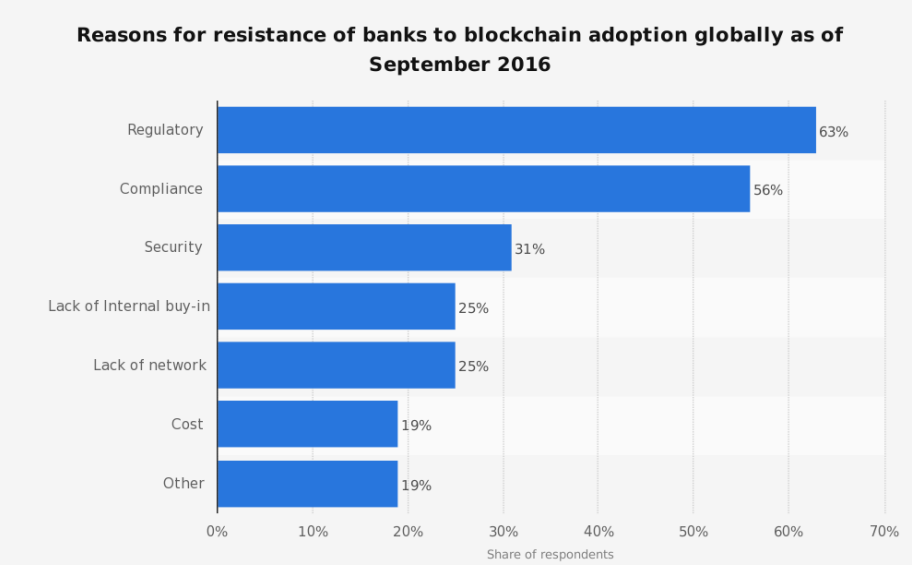

Figure 9: Reasons for Resistance to Blockchain Adoption (Source: Accenture, Statista, 2016)

Figure 10: Barriers to Government Adoption to Blockchain (Source: IBM Institute for Business Value, 2017)

It is because of the fears of the unknowns in blockchain and the negative association's bitcoin and other digital currencies have that I think are stifling the adoption of blockchain in the public sector. Public officials understandably do not want to take the risks with the new technology and they want to protect consumers to the best of their ability from potential risks with the new technology. The issue with this mindset is that if the public sector is not aware of the blockchain and its capabilities, the public sector should not be quick to regulate an unknown. This concern over regulation is highlighted

by Mougayar in his book *The Business Blockchain*, where he outlines what he believes are the three ways in which policy makers respond to new technologies: Policy makers respond in three different ways when faced with a new technology:

1. "Do nothing, let market mature and evolve on its own
2. Control the choke points. For example, these choke points might be the cryptocurrency exchanges or software providers who will be required to get licensed
3. Insert automatic regulation at the point of transaction or somewhere during its journey. Involve making room for the availability of direct data reporting via a backdoor, an information exhaust pipe, or a direct deduction on a transaction" (Mougayar, 77).

These three possibilities are reasonable observations of how the public sector does in fact respond to new technology. With blockchain today, I think the public sector is adopting the second option approach as evidenced in the State of California with AB-1326 Digital Currency.

CA Assembly Bill 1326 Digital Currency, is the first in the state to attempt to regulate cryptocurrencies such as bitcoin. Despite the bill's language of protecting consumers, which is very much needed as we saw with the example of BITFINEX, that lost tens of millions of dollars over night by hackers, the biggest concern stems from the language and push to regulate the still developing and evolving technology. For example, a concerning portion of the bill is when it states, "This bill, until January 1, 2022, would enact the Digital Currency Business Enrollment Program, to be administrated by the Commissioner of Business Oversight, who would be granted authority to make rules and

regulations for this purpose. The bill would prohibit a person from engaging in the digital currency business without enrolling in the program and would prohibit the conduct of digital currency business through an unenrolled agent." (AB 1326) The perceived concern with this language and effort is that California is proposing legislation that would make cryptocurrency based businesses illegal. With Silicon Valley paving the way in global innovation, a bill with such language, with the industry at such an infancy, any possible hard regulations could completely stifle its development. This bill could be an example of some of the reasons for the perceived concerns regarding regulations as exhibited in the prior figures. US Commodity Futures Trading Commissioner, J. Christopher Giancarlo also captures this theme of concern on a difference basis stating, "…investment faces the danger that when regulation does come, it will come from a dozen different directions with different restrictions stifling crucial technological development before it reaches fruition." Despite these concerns with the public sectors embrace of blockchain, there are many cases in which the public sector has been a part of the trailblazers.

Many states such as Arizona, Illinois, Delaware, and California are making trailblazing efforts to foster blockchain innovation. First and foremost, the state of Arizona has had two bills regarding the blockchain in April 2017 and shows an embrace and knack with the technology. Arizona Governor Ducey signed nearly back to back bills regarding blockchain. The first bill (HB 2417) signed by the governor recognized blockchain signatures and smart contracts as being enforceable in a court of law. A week later, a bill (HB 2216) was signed making it illegal to force gun registrations to occur on a distributed ledger technology, such as blockchain (The National Law Review). Both of

these bills show that Arizona is embracing the blockchain technology by upholding the validity of transactions that occur on the ledger in court, thus opening the gates of innovation. Companies that develop smart contracts or utilize digital signatures are assured that their digital contracts and signatures will hold up in a court of law in Arizona. Additionally, even though the bill banning requirements to register firearms on a distributed ledger may appear as an inhibiting instead of trailblazing act, I think this is still trailblazing on the part of Arizona's adoption and acceptance of blockchain in the public sector. By signing this bill, the governor and the government shows that it is not ready to apply blockchain to every possible present issue. This is an important component of blockchain development. During my interview with George Papageorgiou with the University of Nicosia, he said, "blockchain is a way forward, but it is not the way forward for everything". I think his words apply to this decision in Arizona because applying blockchain to everything could dilute its potential and especially applying it to hot button political topics such as gun laws, might cast a negative association onto the technology.

Delaware is also a part of the trailblazing public sector groups because as Nasdaq reports, "Delaware is running trials related to using smart contracts to settle financial transactions, particularly those related to stocks". Having direct tests involving blockchain and financial transactions shows a strong effort by Delaware to not only become aware of blockchain, but to make efforts to adopt its potential. Illinois is following a similar embrace as Delaware, "The Illinois Department of Financial and Professional Regulation has joined the blockchain consortium led by startup R3, as financial watchdogs around the world seek to better understand the opportunities and

risks of the emerging technology" (Irrera, y94.com). Illinois' decision to join a leading consortium shows its interest to learn more about the blockchain which is not only a main objective of this thesis, but the way forward for the public sector to ensure any technological innovation, especially blockchain, is not unnecessarily stifled out of regulatory fears of not knowing how it operates. California is also a part of the trailblazer group with its controversial AB-1326 Digital Currency Bill because of the explicit line stating, "At the same time, it is appropriate for the state to nurture, rather than stifle, these ongoing innovations in payment technology" (Dababneh, Feb. 27, 2015 AB-1326). What this shows is that despite earlier text possible over regulating the digital currency environment, lines such as the one highlighted above show California's effort to at least leave the door unlocked to blockchain innovation. All of these states are showing that there is a moderate and slow acceptance of blockchain currently taking place in the public sector if looked closely enough. Governments are starting to experiment and "test the waters" to see what blockchain can do for their public services. In addition to state led efforts to learn about, implement, or cautiously monitor blockchain development, some public officials have been a part of the trailblazing group by accepting bitcoins for campaign contributions.

Candidates in 2014 joined in efforts to showcase the potential embrace of the blockchain by accepting bitcoins a part of campaign contributions. Gov Tech reported that, "This month the Federal Elections Commission [FEC] took its most definitive stand…issuing an advisory opinion that said politicians could accept bitcoin donations - up to $100…" (govtech.com). Having a clearance from the FEC to allow bitcoin donations for campaigns is a significant statement showing that the public sector is

growing to know about and carefully accept the potential applications of blockchain. Beyond this allowance by the FEC, candidates such as Gavin Newsom, mayoral candidate Byan Parker in Oakland, Colorado Representative Jared Polis, Texas Attorney General Greg Abott accepted bitcoins a part of campaign contributions (govtech.com). These trailblazing candidates project an image that they are open to embracing, not stifling technological innovation. These many efforts by states and candidates throughout the public sector provide a glimpse into the potential for the public sector to be at the forefront of this new technology with the right application.

Proposal: Applying Blockchain to Campaign Finance Reform

Following the trailblazers in the public sector today, and to achieve the objective of providing a feasible application of blockchain to the public sector, perhaps the greatest application potential is campaign finance reform. During a conversation with Lea Deesing and Chris Tilden at the City of Riverside, we discussed many components of the blockchain and its operation, but we all seemed to get excited about the application of blockchain to campaign finances because this appeared to be the most feasible method for implementing the blockchain in the public sector. Presently, the State of California has a Form 700 that all elected officials and individuals that have an influence in the public arena, such as appointed Commissioners, are required to fill out to disclose any assets, property holdings, gifts, etc. (FPPC.com). Some municipalities, such as the SF Ethics Commission have developed online filing systems, in San Francisco's case it's known as E-File where candidates file papers electronically (SF Ethics Commission). These existing required forms and efforts at technological application to the candidate process are foundational components to move operations onto a blockchain. However, developments in the ability to donate to candidates is perhaps the greatest cause for needed campaign financing listed on blockchains.

The landscape of campaign finances has blurred as a result of decisions to allow organizations to donate freely to candidates. Sarbanes states, "Citizens United also invalidated the bulk of the Federal Election Campaign Act of 1971, 2 U.S.C. § 441b, which restricted the use of corporate treasury dollars for the purposes of "express advocacy." (Sarbanes, 23&24). The courts decided that based on the first amendment freedom of speech, the government could not restrict how much a group or organization

can contribute, thus these groups and organizations can contribute as they prefer to candidates. As a result of this, having corporate money transacted over a public ledger would not only provide transparency, but would also make such transactions permanent, thus no candidate nor corporation would be able to alter money trails.

Applying the blockchain to campaign finance reform would take place via "sidechains". Sidechains are shown in *Figure 11: Sidechain Process,* for campaign finances. The blockchain ledger for the public sector would be the greater ledger, and a "side chain" would be created to transact and verify immutable records of campaign finances during each election. A sidechain could be used because they would

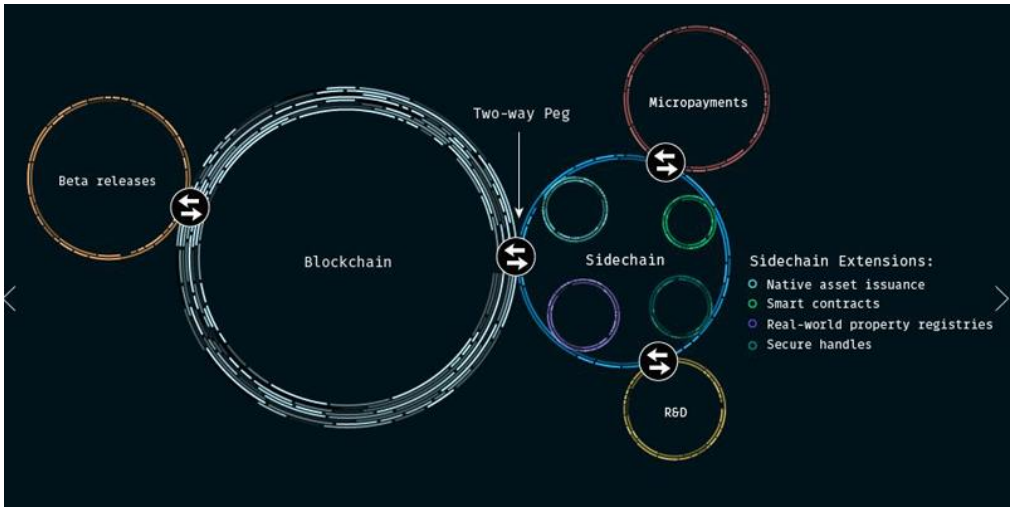

Figure 11: Sidechain Process (Source: blockstream.com)

develop their own smaller distributed ledger. According to the University of Nicosia, "Sidechains will operate in a completely independent and isolated fashion - they are separate systems running in parallel to and taking advantage of the existing Bitcoin blockchain (referred to as "the parent chain"). As such, Sidechains do not introduce any side effects, like the probability of malicious or unintentional damage" (Nicosia). Because of this, smaller municipalities would be able to provide the computing power

necessary to operate a sidechain as opposed to an entire blockchain network. Sidechains would enable the campaign finance disclosures to take advantage of the bigger network while still providing the security and transparency core to the system. Transparency and security would continue to exist past the election and during an official's time in office. This application is also important and critically advanced because, "this system could be augmented with smart contracts prohibiting certain organizations or people from issuing donations after a pre-determined limit is reached (Loop, coindesk.com). In the event courts decide differently regarding campaign limits, such contracts would be initiated, providing an effective check against undue influence.

Proposal: Applying Blockchain to Voting

"For all our technological advances, the mechanics of voting in elections have remained largely unchanged for hundreds of years" (Tapscott, 214). Don and Alex Tapscott have that statement right, voting is a time capsule where citizens must still fill out paper ballots to cast their votes. Gavin Newsom in his book *Citizenville* also highlights this point by describing the 2000 election in Florida where poll workers had to use magnifying glasses to determine which candidates were voted for (Newsom, 157). In areas where electronic voting has been attempted, concerns over security and functionality have been raised. Don and Alex Tapscott highlight the concerns over current electronic voting methods by outlining, "E-voting today suffers from three problems: attacks on the software and hardware, mistakes or bugs in the coding, and human error. In 2004, a voting machine aiding in the general election in North Carolina was accidentally set to store only 3,000 votes. It irrevocably lost 4,438 votes in a race that was decided by a difference of only 2,287" (Tapscott, 215). These three main concerns are very real issues and are significant when one looks at the number of votes lost as a result of the electronic voting system setup. These concerns over digital voting today ultimately arise out of the concern over the third party in charge of supplying the software and hardware to not only capture and store, but to secure cast votes. The possibility of a hacker breaking into an electronic voting system is very real, and if achieved an election could be significantly altered. A public blockchain voting system would be able to overcome the inherent issues and concerns with today's efforts at electronic voting.

Through a public blockchain voting system, the individual votes would be securely encrypted and immutable on the public ledger while the actual tally of votes per candidate would be open and transparent. As a result, if there are any allegations of voter fraud or hacked databases of voting records, the blockchain would be able to provide a readily accessible record of the votes cast. Followmyvote.com had been a leader in the notion of applying the blockchain to voting and provides a comprehensive outline of what voting via blockchain would look like in *Figure 12: Blockchain Voting Example.* This process shows that the voting system would look a lot like that of the bitcoin setup, but instead of trading coins, voters would be casting digital votes for their candidate of their choice.

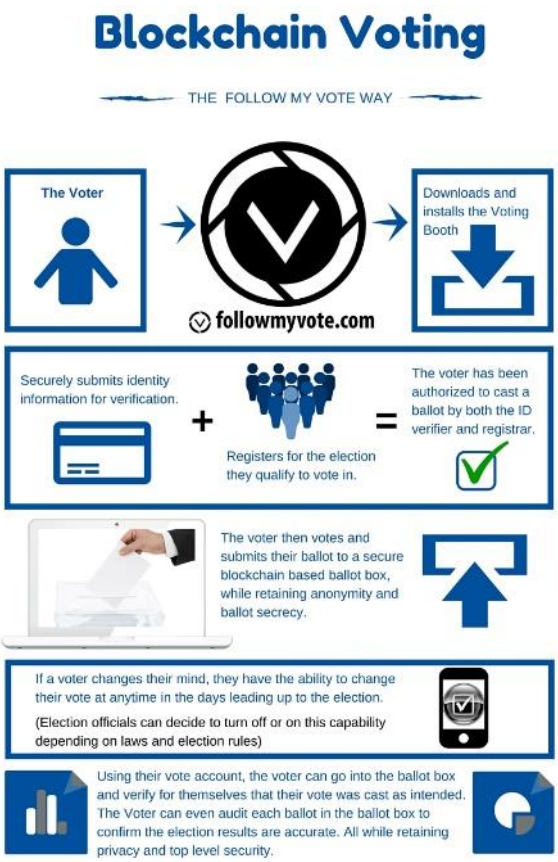

Figure 12: Blockchain Voting Example (Source: followmyvote.com)

Another important benefit of applying blockchain to voting would be the potential to engage with the historically low turnout of younger individuals during elections. *Figure 13: Voter Turnout by Age*, younger individuals historically have extremely week turnout numbers in elections. This lack of participation in the democratic process is only increasing as lives become busier and more interconnected demanding instant abilities, not abilities to drive to a polling place, wait in line and cast a ballot. Or wait for a ballot to arrive in the mail, unfold large pieces of paper, read directions on how to bubble circles, and then place back in the mail. With a blockchain-based voting system in place, all a voter needs to do is cast their digital ballot. As 'blocks', the voter's choices will go directly to their preferred candidate's digital address, the longest address at the end of the election will be the winner. The potential for blockchain voting will provide increased participation, especially among younger voters because citizens can now vote through their phones on mobile wallets, more transparent because anyone could see the distribution of votes cast, reduce concerns about voter fraud, and save money by streamlining the entire process.

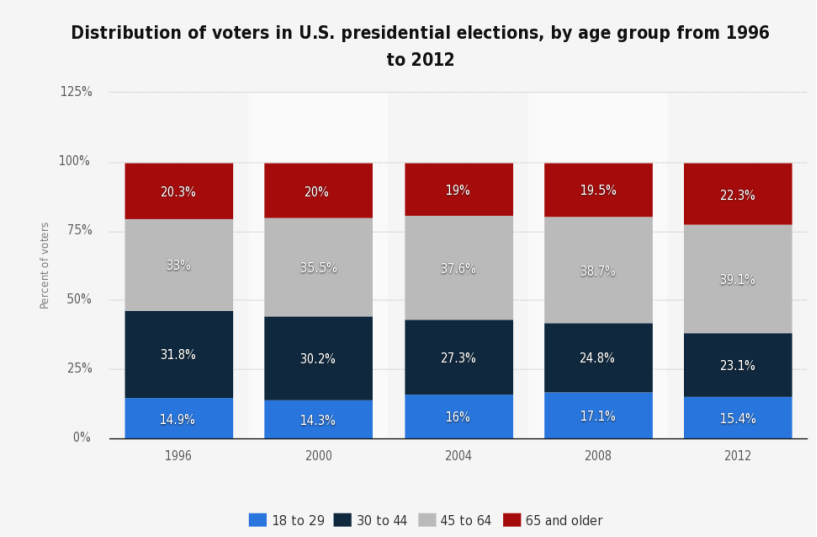

Figure 13: Voter Turnout by Age (Source: US Census, Statista 2016)

Additional Areas for Further Study

The primary opportunity for further study is to gain an even firmer grasp on blockchain and additional public promotion to get it on the radar of public officials. While conducting research and gathering information, the most common response to my question of if they knew of any initiatives using blockchain in the public sector for voting or campaign finance reform, nearly every time I received the same response: What in the world is blockchain. Ethics commissions, public official offices, election groups, and countless others were not aware of the blockchain. However, when explained what the blockchain is and the proposed implementation, great interest was expressed. As a result of the continuing limited knowledge of blockchain, let alone its potential applications, further publication and education of what blockchain is must be developed. Research into academic journals also showcase limited published material on blockchain today, more information needs to become available to provide feasible applications. Additional areas of study stem from underlying issues with the blockchain and with the blockchain's unknowns as it still develops.

How can we be certain there is no 'backdoor' into the blockchain? This concern was addressed during an interview with George Papageorgiou a part of the University of Nicosia where he made the important point that, "given the amount of people interested and studying the topic of blockchain and actively trying to find the backdoor or vulnerabilities, the fact nothing has been found since its inception shows the system is extremely secure". This is an excellent response to the concern, however, the question about a backdoor was first brought up by Mr. Steve Reneker during a phone call. I think in order to prove there is no backdoor, additional analysis and specific evidence of the

systems' security must be developed to gain the trust of the public sector. Aside from this concern, there is the concern of the negative association cryptocurrencies carry.

Stories such as the Silk Road, where criminals freely exchanged drugs and weapons via bitcoin payments, shed a negative and questionable association to the decentralized model. How can blockchain distance itself from this image? This will be a hard issue to overcome and is a possible reason for the concerns about over-regulation because the public sector and public officials will have a hard sell to the public implementing a technology if its perceived association is with drugs and crimes. Finally, there is an extremely important issue regarding the environment that must be further explored.

Immense energy is required for adequate computing power to create a block and verify a transaction. That immense computing requires enormous amounts of energy which would cause significant pollution. Presenting a system for the public sector, a key question for further consideration is how the public sector will be able to develop the necessary computing power without negatively impacting the environment? My vision to be able to create the campaign finance reform and voting system outlined in this thesis would take the shape at local, county, and state levels with each level of government being an independent node (or computer base) that would run the verification algorithms for transactions. As a result, it would be extremely dependent on computing power. How can enough clean energy be used to run the transactions must be explored.

Conclusion

As a result of this thesis, it became apparent that the components and application of blockchain are nearly limitless because blockchain is an incredibly powerful distributed ledger that utilizes a network of computers to verify and permanently record transactions publically. As Jim Balistreri told me over one conversation, "When it comes to technology, there is no revolution, there is only evolution". I think this is a perfect quote to capture the next phase of digital development we are entering with blockchain. Blockchain is the next evolution of the internet and digital world. The challenge now with a firm grasp of what blockchain is and what its potential applications are is to not only continue learning about the technology, but to actively create and maintain an open dialogue about blockchain to continue its exploration and development. The public sector can become an innovation and technological leader if the blockchain is fully understood and properly implemented. The future of technology and this next evolution will lie with blockchain, and the fundamental shift in blockchain adoption is upon us as shown in *Figure 14.* Campaign finance reform and voting are just the beginning of possible applications of the blockchain to the public sector. Be aware of and be a part of the development of Blockchain For The Public Sector.

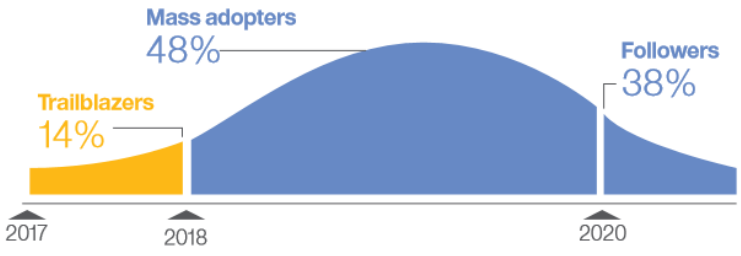

Figure 14: Acceptance of Blockchain Curve (Source: IBM Institute for Business Value, Jan 2017)

Bibliography

Accenture. "Reasons for Resistance of Banks to Blockchain Adoption Globally as of September 2016." *Statista - The Statistics Portal*, Statista, Accessed 8 May 2017.

"Arizona Passes Groundbreaking Blockchain and Smart Contract Law – State Blockchain Laws on the Rise." *The National Law Review*. N.p., 20 Apr. 2017. Web. 1 May 2017.

Assembly 1326, 2015-2016 Regular Session.

Blockchain. "Number of Blockchain Wallet Users Worldwide from 4th Quarter 2011 to 1st Quarter 2017." *Statista - The Statistics Portal,* Statista, Accessed 8 May 2017.

"Blockchain Shared Ledger Could Revolutionize Finance." *ValueWalk*. Goldman Sachs Investment Research, 04 Dec. 2015. Web. 5 Oct. 2016.

"Blockstream." *Blockstream* - Blockstream. N.p., n.d. Web. 19 Mar. 2017.

Building Trust in Government: Exploring the Potential of Blockchains. Rep. IBM Institute for Business Value, 30 Jan. 2017. Web. 17 Mar. 2017.

Deesing, Lea, and Chris Tilden. "Senior Thesis: Blockchain UC Riverside." Personal interview. 20 Oct. 2016.

eMarketer. "Level of Familiarity with Bitcoin in The United States as of June 2014." *Statista - The Statistics Portal*, Statista, Accessed 8 May 2017.

GAO. "Number of Cyber Security Incident Reports by Federal Agencies in The United States from Fy 2006 to 2015." *Statista - The Statistics Portal*, Statista, Accessed 9 May 2017.

Garofoli, Joe. "California Lt. Gov. Gavin Newsom Among First Politicians Opening Coffers to Bitcoin." *Government Technology: State & Local Government News Articles*. N.p., 20 May 2014. Web. 1 May 2017.

Goodman, Marc. *Future crimes: everything is connected, everyone is vulnerable and what we can do about it.* London: Gorgi , 2016. Print.

"How MasterCard Processes 74B Transactions a Year." Blog post. *UniBul's Money Blog*. N.p., n.d. Web.

Investing.com. "Bitcoin Price Index from The First Quarter of 2012 to The First Quarter of 2017 (in U.S. Dollars)." *Statista - The Statistics Portal*, Statista, Accessed 8 May 2017.

Irrera, Anna. "Illinois Watchdog First U.S. Regulator to Join Blockchain Consortium R3." *Y94*. Midwest Communications Inc., 16 Mar. 2017. Web. 8 May 2017.

Loop, Peter. "4 Ways Blockchain Can Disrupt Civic Traditions." *CoinDesk*. N.p., 17 Mar. 2017. Web. 8 May 2017.

Marquit, Due.com Miranda. "What Do Delaware And Japan Have In Common? Blockchain Trials." *NASDAQ.com*. Nasdaq, 20 Apr. 2017. Web. 10 May 2017.

Mougayar, William. *The business blockchain: Promise, practice, and application of the next Internet technology*. Hoboken, NJ: John Wiley & Sons, Inc., 2016. Print.

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. Web. 17 Oct. 2016.

Nakamura, Yuji, and Lulu Yilun Chen. "Bitcoin Traders Made 700% Returns Before Losing Millions in Hack Attack." *Bloomberg.com*. Bloomberg Technology, 11 Aug. 2016. Web. 1 May 2017.

Nath, Trevir. "How Safe Is Venmo And Why Is It Free?" *Investopedia*. Investopedia, 31 Oct. 2016. Web. 25 Apr. 2017.

Newsom, Gavin Christopher, and Lisa Dickey. *Citizenville: how to take the town square digital and reinvent government.* NY, NY: Penguin , 2014. Print.

Papageorgiou, George. "Senior Thesis: Blockchain UC Riverside." Online interview. 8 Mar. 2017.

Reneker, Steve. "Senior Thesis: Blockchain UC Riverside." Telephone interview. 6 Mar. 2017.

SARBANES, REPRESENTATIVE JOHN P. and RAYMOND O'MARA III. "Power & Opportunity: Campaign Finance Reform for the 21St Century." *Harvard Journal on Legislation*, vol. 53, no. 1, Jan. 2016, pp. 1-38. EBSCOhost.

Tapscott, Don, and Alex Tapscott. *Blockchain revolution how the technology behind bitcoin is changing money, business and the world*. New York: Portfolio Penguin, 2016. Print.

Tapscott, Alex. "Blockchain Is Eating Wall Street." TEDxSanFrancisco. San Francisco. 10 Dec. 2016. *YouTube*. Web.

The Future of Financial Infrastructure: An Ambitious Look at How Blockchain Can Reshape Financial Services. Rep. Word Economic Forum, 12 Aug. 2016. Web. 5 Oct. 2016.

Tsukerman, Misha. "The Block Is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future." *Berkeley Technology Law Journal*, vol. 30, 2015 Special Issue, pp. 1127-1169. EBSCOhost.

Underwood, Sarah. "Blockchain beyond Bitcoin." *Communications of the ACM*, vol. 59, no. 11, Nov. 2016, pp. 15-17. EBSCOhost.

University of Nicosia MSc in Digital Currency DFIN-511 (Nicosia) Wednesday March 22nd, 2017 Andreas (Antonopouos, 3/22/17).

US Census Bureau. "Distribution of Voters in U.S. Presidential Elections, by Age Group from 1996 to 2012." *Statista - The Statistics Portal*, Statista, Accessed 9 May 2017.

"Venmo." *Venmo.com*. Venmo, 2017. Web. 25 Apr. 2017.

Yang, Jia Lynn, and Amrita Jayakumar. "Target Says up to 70 Million More Customers Were Hit by December Data Breach." *The Washington Post*. WP Company, 10 Jan. 2014. Web. 5 May 2017.