Payment Disrupters –
WHATS NOT IN YOUR WALLET?

Koy Stone
SC Telco FCU
Greenville, SC
kstone@sctelcofcu.org

Lewis Smith
Bayport Credit Union
Newport News, VA
lsmith@bayportcu.org

Christine Cooper
Carolina Foothills FCU
Greenville, SC
ccooper@cffcu.org

Michael Poucher
First Commerce Credit Union
Tallahassee, FL
mpoucher@firstcommercecu.org

TABLE OF CONTENTS

I. INTRODUCTION

We live in a very exciting time for consumers. Thanks to technology, there are multiple solutions and options to help us complete any task imaginable. Social media has magnified our voices, we can use the internet to shop for the right car at the best price and we can even watch our favorite sports team play live from our phones. We have these abilities and many more due to the increasing number of technological tools available at our fingertips. Technology has grown at an accelerated rate during the past couple of decades, sparing no industry from its disrupters. A few examples of technology disruption within specific industries includes Uber disrupting the taxicab industry, Netflix disrupting the home entertainment industry and Amazon disrupting the shopping industry.

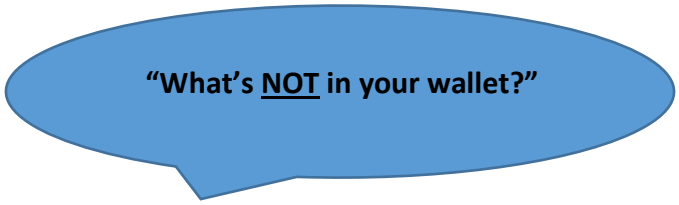
Technology has also proven its ability to break down barriers that once divided industries. In 2007, no one would have predicted the negative impact that the Apple iPhone would have on the digital camera industry. It has been over a decade since the first generation iPhone entered the marketplace, and this device continues to find alternatives for consumers at the detriment of many other industries and companies. Apple is one of many technology companies that has also found a way to disrupt the financial services industry. It has done this both directly through offering Apple Pay, and indirectly by offering a medium for FinTech companies such as Venmo.

Apple is not the only technology disrupter trying to carve out a niche within the financial services industry. Every aspect of our industry is under attack from disrupters of all shapes and sizes. FinTech companies are looking for new ways to attract consumers away from credit unions and banks. These companies typically specialize in one segment of the financial services industry such as Kabbage, who specializes in business loans. Credit unions and banks not only need to compete against these new entrants within the financial services marketplace, but they also need to adopt some of the new technologies offered when it is appropriate to do so. Members have come to expect many of these new technologies as required services from their credit unions. Online Banking is a perfect example of this. At this time, payments are an area within the financial services industry receiving an increasing amount of attention from technology disrupters.

Evolving payment methods is nothing new. Since the beginning of time, humans have relied on various mediums of exchange. During the prehistoric era, bartering was the first medium of exchange used. Later on, humans began to offer coins and paper money as mediums of exchange that are more efficient. In 1950, the Diners Club offered the first credit card that a consumer could use at multiple locations. The first debit cards entered the marketplace in the 1960's. This shows that consumers have adapted with how they conduct payments throughout time. We continue to look for better ways of paying each other, which is even more prevalent in the 21st century by the introduction of three new disruptive forms of technology. These

disrupters are mobile payments, biometric payments and blockchain/ cryptocurrency. The purpose of this study is to investigate and further understand these three payment disrupters.

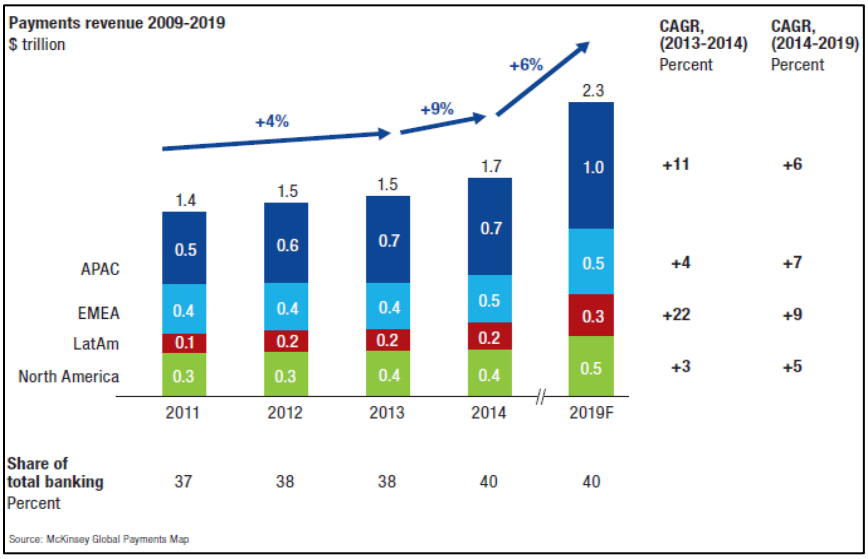
Mobile payments have been around since 1997 when Coca Cola introduced a limited number of vending machines that could accept payments via text message. A company called Pay By Touch first offered biometric payment solutions in 2006. The introduction of Bitcoin in 2009 provided us with the first virtual currency and digital payment system operating through blockchain. All three of these disrupters have been around for an extended time, but continuous technological advances are increasing their impact on the financial services industry and the entire consumer market. In order to survive, credit unions must change with the times by adapting to these emerging payment technologies. The average consumer has become less patient as more technology becomes available to them. We want our payment solutions to be as fast and as easy as possible. Credit unions need to recognize the importance of this consumer mindset and need to invest in the most applicable payment technology advancements for their membership. Successful execution in this area will not only help participating credit unions to survive but it will also enable them to thrive in the future. As leaders in the credit union industry, we should no longer only concern ourselves with the amount of wallet share we have for each of our members. Instead, we need to ask our members:



Credit unions should ask this question, because payments are no longer a stagnant area in the finance world. Most financial institutions only focused on acquiring loans, deposits and member growth in the past. Payments were not a major focus, because they were always a steady source of income that outside competition rarely challenged. Now it is easy for disrupters to challenge the payment revenues that credit unions and banks have taken for granted, and they are also attracted by the valuable data mining opportunities of the transactions themselves. Unfortunately, this new competition comes at the same time as regulations tighten for financial institutions. Tighter regulations will cut into the revenue sourced from payment interchange fees, and new technologies make it easier for financial technical (FinTech) companies to attract consumers with alternative payment channels. Strong global payments revenue over the last few years have attracted these companies to develop payment solutions.

McKinsey & Company conducted a global payments study in October of 2015. This study highlights the healthy growth expected of the Global Payments Industry through 2019, and it describes the challenges that come with this growth. According to the McKinsey Global

Payments Map, payment revenues will experience year-over-year growth of 6% over a five-year period projected to 2019. This study also projects that global payments revenue will reach $2.3 trillion by the end of the same timeframe. The Asian-Pacific (APAC) region will continue to be the leader in payments revenue by accounting for $1 trillion, while North America will account for $0.5 trillion in payments revenue. McKinsey and Company predicts that transaction-related revenues will be the most important driver of growth in the Asian-Pacific, Latin America and North America regions through 2019. Domestic transactions growth, such as credit card volume, will account for 65 percent of overall payments revenue growth for North America during this period. McKinsey & Company claims that increasing regulatory pressure, intensifying competition, rapidly changing consumer behavior and the migration from paper-based to digital payments are trends that provide momentum to domestic transactions growth in North America. This study illustrates the significance of payment trends within the financial industry.



Finding out what is not in our members' wallets will help the credit union movement adapt to the changing landscape of payments. Leveraging the information uncovered from this question will secure a successful future for credit unions as we continue to advance within the Digital Age. Let us not stand by and watch the credit union industry suffer the same fate as the video rental stores. The first step towards using this information is to gain a better understanding on how these currency disrupters benefit our members. Then we need to recognize the business, legal and regulatory risks that comes with each one of these disrupters. In this paper, we will cover the opportunities and threats associated with mobile payments, biometric payments and digital currency. Our goal is that you will be able to use this information to gain a better understanding on the risk of your members distancing themselves from their wallets. Knowing how your members prefer to conduct their business is the most important step in maintaining your credit union's relevance as their financial institution of choice.

II. RESEARCH

Peer Survey

When we started the research for this white paper, our group decided to conduct a study among our credit union peers to gain a better understanding on their view towards these payment disrupters. One hundred participants were included in our study, which we believe to be an adequate sample size for giving us the data we are looking for. The only commonality among our survey participants is that they are all credit union professionals. It is important to note that working in the financial services industry should give our participants a better understanding on these payment disrupters than an ordinary consumer would have. We asked our participants six multiple-choice questions during this survey, and the first three questions focused on our respondents' current use or knowledge level of the highlighted payment disrupters. The first question we asked our participants was how often they used their smartphone to access their credit union accounts. The majority of responses (48%) said that they do this on a daily basis, while only 11% said that they never use their smart phone to access their accounts. These results did not surprise our group, because most of the US population owns a smartphone. However, the responses to our second question did surprise our group. This question asked our participants if they use some form of digital wallet. Only 21% answered 'yes' to this question, while 71% answered 'no'. A small percentage (8%) claimed that they would use a digital wallet if their credit union offered this type of service. The third question asked in our survey was to gauge how familiar our credit union peers are with blockchain and cryptocurrency technologies. It was alarming to see that only 7% of the respondents are comfortable with their knowledge in this area. The majority of responses (54%) claimed that they know what blockchain and cryptocurrency are, but that they do not know them well. Even more concerning is that a large percentage (21%) answered that they know nothing about blockchain and cryptocurrency technologies.

The remaining questions in our survey focused on our participants' opinions regarding the future of these payment disrupters and the possible effects that they can have on credit unions. We asked the respondents if they would use some form of biometric payment as a substitute for debit/credit if their credit union offered it as an alternative. The responses to this question were positive with only 22% saying they would never consider using biometric payments. The majority (53%) of respondents claimed that they would adopt this payment method after their credit union had it in place for at least a year, while 25% said that they would adopt this payment method as soon as their credit union offered it. Biometric payments also had positive results from our next question, which asked the participants which payment option they think is least likely to result in a fraud loss by earning a vote of 70%. Digital wallets were a distant second at 11% followed by plastic cards, checks and cryptocurrencies. The last question that we asked our credit union peers was if they think that any of the new payment technologies will negatively affect the credit union industry. A majority of the respondents (53%) were not

concerned at all, while 33% are worried that credit unions will not be able to adapt and stay relevant. Gathering this information from our peers was extremely valuable, because it gave us an educated consumer's perspective on these payment disrupters and it helped us focus our research efforts.

An Introduction to Mobile Payments

According to investopedia.com a mobile payment is, "money rendered for a product or service though a portable electronic device such as a cell phone, smart phone or PDA." Mobile payments are one of the most common types of electronic payments, and the payment landscape is changing thanks to their growing popularity. Outside of currency and plastic cards, consumers use electronic payments the most consistently. Currency and plastic have the advantage of being around longer than most electronic payment solutions, including mobile. However, electronic payments are growing thanks to advancements in mobile technology. The '2015 Diary of Consumer Payment Choice' issued by the Federal Reserve Bank of San Francisco illustrates the growth of electronic payments. The results from this study shows that cash usage accounted for approximately 33% of all transactions in 2015. This is down 7% from 2012. This study also shows that debit cards and credit cards combined to account for 48% of all transactions. This is up 6% from 2012. Finally, the study claims that electronic payments accounted for 11% of all transactions, and this is up 7% from the recent study. The takeaway from this information is that electronic payments currently account for a small percentage of all payments made by consumers, but they are growing at a faster rate than the more traditional payment methods. Mobile payment technology contributes to this growth, because consumers are attracted to its ease of use and versatility. A consumer also has many ways they can choose to execute a mobile payment. Everyday payments, POS (point-of-sale) purchases, closed loop, carrier, and mobile card reader are examples of how consumers use mobile payment solutions today.

Several advances in technology have fueled the growing adoption rates for mobile payments. However, the most significant technological advancement for mobile payments is NFC (Near Field Communication). This technology allows two devices to communicate with each other when they are in a close range of one another. The introduction of NFC in the early 2000s provided a means for a consumer to execute contactless payments with their debit and credit cards. Contactless payments allow an individual to complete purchases by 'waving' their card within a close proximity to a POS terminal. NFC is a more advanced form of RFID (radio-frequency identification), which allows devices to identify each other through radio waves. Over the years, RFID has been a common technology that is a consistent presence in our daily lives. For example, a store clerk uses RFID technology to scan an item that a consumer wishes to purchase. Consumers can now make payments more efficiently thanks to the innovative companies, who developed NFC by building off the RFID technology. Mobile payments use NFC technology the same way as contactless card payments. The only difference is the consumer

waives their phone near a POS terminal instead of their card. NFC made mobile payments a reality, and now the introduction of more technological advancements is making mobile payments a preferred purchasing method by a growing contingent of consumers.

The Evolution of Mobile Payments

It is no surprise that the adoption of mobile payment technology is becoming so widespread. The evolution of mobile payments began two decades ago, and it has begun to pick up its pace over the last five years. In 1997, Coca Cola became the first company to accept mobile payments for the purchase of its products. Consumers could buy a soft drink by sending a text message to one of their select vending machines. Coca Cola was the first pioneer in regards to mobile payments, but it did not take banks long to follow the soft drink company's lead. Merita Bank, now called Nordea Bank, was the first financial institution to offer a form of mobile payments. This bank allowed its customers to conduct their transactions via text messages.

Mobile Oil Corp introduced another innovative payment method in 1997 called the Speedpass. At its introduction, the Speedpass was a RFID device in the form of a keychain. Consumers were able to use NFC technology to purchase gas by waving this device near a certain area of the gas pump. In 1999, Mobile Oil Corp merged with Exxon to create the gas company that we know today as Exxon Mobile. This company still offers Speedpass, but it has introduced an enhanced version called Speedpass+. The new version is an app that a person can download to their phone. This app allows the consumer to pay for fuel, earn rewards and even locate an Exxon Mobile gas station.

Companies use NFC technology even more in 2017 as they strive to separate themselves from their competitors. Some of these companies want recognition for introducing the next "big thing" to consumers. However, every company needs to adopt the technologies that consumers require in order to stay relevant. Digital wallets are an example of NFC technology that is trending with consumers. It is becoming the norm for financial institutions to offer some form of a mobile wallet to their members/customers. These digital tools are where a consumer uses their mobile device as a substitute to a traditional wallet. An individual can store their debit and credit cards onto their mobile device, and can make various types of payments through this delivery channel. Apps allow consumers to store their card information onto their phones and to make POS purchases at the store without using cash or a debit/credit card. Many FinTech companies have leveraged digital wallets and NFC technology to disrupt the financial services industry. An example of this is Venmo, which is a company that allows an individual to use their phone for transferring funds to anyone they want. The possibilities for mobile payment technologies appear to be limitless. Thanks to P2P transfers, people no longer need checks to pay back their friends, to pay their child's babysitter or for purchasing an antique at a garage sale. Mobile technology even makes it easier to split the cost of a dinner or

an Uber ride with a friend. In addition, this technology speeds up the checkout process at the store and eliminates cumbersome pocket change.

What is the future of mobile payments? Google tried to get ahead of the curve by offering a hands-free payment solution. Their original goal was to use facial recognition-based shopping to identify shoppers in a retail store as they check out. This would allow the shoppers to walk out of the store without paying with cash, card or a mobile device. The result would be no more checkout lines and prevention of store theft. This was a novel idea of combining NFC and biometric technology to improve the shopping experience by eliminating non-value-added time. The adoption rate for Google's retail experiment was very low, causing the technological giant to put an end to it. Was Google's idea too farfetched for the public to accept? Or did they act five years too soon on this novel venture? The only thing that is certain is that mobile payments are evolving and companies need to be in tune with these advancements if they want to stay relevant in the future.

Mobile Payment Vulnerabilities and Risks

It is crucial for any company to have safeguards in place to protect the consumer whenever they use or store personally identifiable information. This is even more important when the company is utilizing new and emerging technologies, where cyber threats are growing. A company increases their risks and exposure to vulnerabilities when they use a technology that accesses private consumer information. In December of 2016, the European Union Agency of Network and Information Security (ENISA) published a paper, "Security of Mobile Payments and Digital Wallets" which talks about the risks of using mobile payment technology. Some of the identified risks include weak server-side controls, insufficient transport layer protection, improper session handling and poor authorization and authentication.

Weak server-side controls are a significant risk associated with mobile technology. The consumer expects that their confidential information is secure when they use an application as their mobile wallet. Therefore, the mobile platform needs strong controls in place at its server to mitigate the risk of data breaches. If the server has weak controls and security in place, the exposure of consumers' personal data to potential cyber-attacks is possible. Another risk that mobile technology is exposed to is insufficient transport layer protection. A consumer's confidential data is at risk as it moves between one secure platform to another if the transport layer protection is inadequate. A consumer needs this form of security to protect their confidential data as it leaves their mobile device while completing a purchase. Improper session handling also creates security concerns for mobile payments. The mobile payment platform needs to allow the consumer to execute a proper log off after they access their account information. Sessions should also expire after meeting predefined inactivity time limits. Consumers' confidential information is vulnerable if these session handling measures are not in place. Strong authorization and authentication control is the most critical safeguard

to have in place for mobile payment technology. It is important for the mobile platform to identify that the user is who they say there are. Tokens are good tools for identification purposes. However, it is also strongly encouraged to incorporate a heuristic attribute, such as a GPS locator, to the identification requirements.

Biggest Barrier to Break for Mobile Payments: Adoption

Will people like it? This is one of the biggest questions asked when introducing anything new and different into the marketplace. Will people use it? Unfortunately, adoption rates have been slow for the mobile banking industry. This technology is easy to use and provides multiple benefits to the consumer, but many people still fear it. A recent American Banker article stated, "Fear of technology, fear of banks, fear of loss of privacy, fear of complexity and even fear of revealing one's technological ignorance are factors that have slammed the lid on mobile growth". Large banks have seen a decrease in the growth of active mobile banking users since 2012. The main cause for this is the fear of ineffective security. FICO found in a recent study that 44% of U.S consumers recognize bank fraud and identity theft as their biggest fear in life. There is a basis for this fear. Identity thieves have stolen over $107 billion from their victims over the past 6 years.

A lack of usefulness is not the deterrent to mobile banking technology for many consumers. Instead, it is the fear that these people have of making themselves more vulnerable to identity theft. As credit unions, we need to encourage our members' use of this delivery channel. We also need to focus our attention and effort on strengthening the security measures of the mobile banking platforms we promote. These efforts can take many forms such as enhancing cyber security procedures or enhancing vendor due diligence procedures. We will see an increase in mobile payments once we earn our members' confidence in the security of the mobile banking platform that we offer. It would be detrimental to the credit union movement if larger banks and tech companies gain our members' confidence in their mobile payment solutions before we do. Mobile adoption rates are slower than expected, but this technology will eventually have a stronger presence as the preferred method of payment. Will credit unions recognize the importance of investing money, time and effort into the infrastructure and security of their mobile platforms? If not, we will eventually see our membership numbers dwindle as the larger banks and FinTech firms attract the millennial and centennial generations as they get older.

An Introduction to Biometric Payments

Biometric technology has received a lot of publicity over the last couple of years. However, the utilization of biometric data has been around longer than most people realize. Police have been using this data for over 100 years by fingerprinting suspects. Law enforcement even

adopted digital biometric databases in the 1980s to become more effective in fighting crime. Biometrics have evolved from fingerprints to a wide variety of other physical attributes. Some of these attributes include retina, iris, facial, voice, footprint and even body odor analysis. Many industries have adopted biometric technology since the early 2000s. Social Media has been a major driver in this growth due to its ability to easily collect and store biometric data. For example, Facebook has one of the largest facial datasets from its users uploading 350 million photos every day. This social media company utilizes a deep learning facial recognition system called DeepFace for analyzing and storing the biometric information of its users. Even brick-and-mortar stores are using facial recognition to identify repeat customers as well as shoplifters as they enter a store. Like any other industry, financial institutions are no stranger to the recent advancements in biometric technology.

In 2006, Pay By Touch was one of the first financial companies to offer biometric payment options to its consumers. Even though this company has dissolved, their idea of a consumer using distinct body attributes to make payments has not. People have become more comfortable with the idea of leveraging biometric technology in an effort to make their day-to-day lives more convenient. The Apple iPhone was a major driver in this mentality shift when it introduced an easy to use home-button fingerprint sensor in 2013. The success that Apple had with bringing a biometric identification tool to the marketplace proved that the public's appetite for biometrics has grown dramatically. Apple even took it a step further by incorporating biometric technology as a security feature in its Apple Pay product. Now an iPhone owner can use their thumbprint to gain access to their phone and to pay for point-of-sale transactions with Apple Pay. The introduction of thumbprint authentication into Apple Pay was a significant step towards a widespread consumer acceptance of biometric payments.

Major credit card companies have taken notice of the consumer appetite for biometric payments, which Apple Pay has helped cultivate. In 2017, MasterCard introduced trials for a new credit card product that incorporates a layer of biometric authentication for executing card payments. MasterCard's new product is a chip and PIN bankcard that uses a fingerprint reader, located on the card, for additional security. The goal of this new product is to increase security and add convenience for consumers. According to MasterCard, future versions of this product will include contactless payment technology. Contactless payments are convenient, because they offer a faster way for a person to make card payments. However, security is a significant trade-off for the added convenience of contactless payments. This is where biometrics can be a game-changer for bankcards by combining a layer of authentication to the speed of a contactless payment. After all, the driver for all the major advancements in payment technology has been convenience and security.

The Benefits of Biometric Payments

There are many ways that companies in the financial services industry can leverage biometric technology to improve convenience for the consumer. MasterCard is leveraging fingerprints as a substitute to the cumbersome and security-flawed method of PIN number authentication during point-of-sale transactions. This increases convenience for the consumer who is "on the go" by speeding up the checkout line at the store. MasterCard also experimented with facial biometrics in October of 2016. The credit card company rolled out a 'selfie pay' app that people can use to make online payments. This technology allows the consumer to complete an online payment by using their phone to take a picture of their face. Many other financial companies are leveraging biometric technology to improve the speed and to add convenience to their processes.

Certain credit unions are taking advantage of biometric technology to improve their member experience. These credit unions use biometrics to authenticate their members in the branch as well as through online delivery channels. Fiserv is a Wisconsin-based company, which offers biometric solutions that can improve the operational efficiency for credit unions. One of Fiserv's products is a palm authentication technology called Verifast, which identifies an individual though the analysis of their palm-vein physical characteristics. Verifast can be used as a member-facing technology by improving efficiencies on the teller line. Gesa Credit Union out of Richmond, Washington is using Verifast to reduce transaction times on their teller line. Their members are using these palm readers to confirm their identities rather than fumbling through their wallets and purses for other forms of identification. This process also reduces non-value-added time by eliminating the need for a credit union employee to analyze and record information off a member's ID. The credit union leverages biometric technology in this scenario by making the transaction process more efficient, and by allowing the branch employee to focus more on member engagement instead of member identification. As an added convenience, this member-facing authentication process allows a member to negotiate a check, make a withdrawal, or receive information from their account without the need of carrying their driver's license.

Not only are biometrics a more convenient method of identification, but it can also be argued that they are a more secure alternative as well. For example, government IDs are easily forged. Fraudsters appear to be one-step ahead of the curve, even with the addition of new security features on identification cards. The enhanced security of biometrics is one of the main reasons that member engagement improves from this technology's use as an authentication method on the teller line. The teller has peace of mind knowing that their member is truly in front of them requesting a withdrawal, because a fraudster cannot forge their members' physical attributes as easily as they can create a counterfeit card. As technology improves, so do the services that credit unions offer to their members. Even the delivery channels for these services are seeing technological advances. Many credit unions are offering online account opening and loan origination as options to their members, and a major concern for these

institutions is security. Fraudsters are attracted to the anonymity of online account and loan origination. Credit unions who use these online delivery channels can protect themselves and their members from fraudulent account and loan origination by leveraging biometric authentication as a security feature. Even though biometrics offer certain security advantages, they also have risks associated with them.

The Risks of Biometric Payments

How safe is biometric technology? According to a survey conducted by OnePoll/Gigya, 80% of consumers agree that biometrics are a more secure form of authentication than traditional passwords. It is true that biometrics offer a more secure alternative to identity authentication than most other options. However, there are significant consequences if biometric data is hacked. A consumer can easily create a new password after a hacker compromises their information, but they do not have the ability to get new hands or new eyes if their biometric data is hacked. This is a major concern for companies that incorporate biometric technology into their processes, because breaches containing biometric information have already occurred.

An example of one of these incidents occurred in December of 2014 when the Office of Personnel Management suffered a massive data breach. 22 million people had their personal information, including their fingerprints, stolen in the breach. What is most concerning about this incident is that the victims of the breach cannot change their fingerprints. In the world of biometrics, there are no second chances. The risks associated with personal privacy will continue to grow as biometrics become more mainstream. Companies that use and store biometric data for authentication purposes will remain under scrutiny as the public becomes more aware of this emerging technology. There are various measures that companies can put in place to mitigate the risk of a biometric data breach. A couple of these mitigation techniques includes encrypting the information and electing not to store it on-site. Another concern with using biometric technology as a primary authentication form is how it may encourage violent robberies. For example, we could see an increase in hostage incidents if biometrics become the common way to withdrawal cash. Desperate criminals will still find ways to commit a robbery even if their victims no longer carry cash or plastic in their wallets. Instead of taking just a wallet, these criminals may escalate the situation by taking their victim. Replacing cash and plastic with biometrics sounds like a far-fetched idea. However, there is momentum of a large nation going cash-less and card-less on the other side of the world.

The Future of Biometric Payments

India has an ambitious goal to eliminate the need for credit cards, debit cards and ATMs by 2021. The country plans to turn every Indian into a 'walking ATM' through the incorporation of biometric payments. A finger or an eye will be all that an Indian needs to complete a transaction in the near

future. A foundation for biometric success is already in place because the Indian government possesses biometric data for 1.1 billion of its citizens. Testing is in progress for India's biometric payments through a payments app and portable fingerprint scanners. In addition, rolling out this point-of-sale technology is significantly less expensive than traditional bankcard terminals. The portable fingerprint scanners cost approximately 2,000 rupees, which is equivalent to $30 in US currency. Eliminating all plastic cards for a country of 1.3 billion people will be a difficult goal to meet, but the data housed by India's unique identification program in conjunction with the inexpensive fingerprint scanners makes the idea possible. India has also made moves to go cashless by instituting a recent note ban. The Indian government hopes that biometric payments will be the solution for eliminating tax evasion and corruption within its borders.

The Reserve Bank of India has recognized the need to enhance security as it moves all its payments to a biometric authentication system. To achieve this, India is making it mandatory for all financial institutions and card networks to move their electronic payment transactions to the Aadhaar-based biometric authentication (ABBA) program. The Central Government of India continues to push ABBA as the only method of payment for its citizens. By June of 2017, this requirement was in effect for 80% of the ration shops across the state of Jharkhand in India. The purpose of this mandate is to enhance security as India transitions into a cash-less society. However, there is concern by some experts that the Aadhaar system will not be able to handle the transaction volume that the large population will demand. India is one of the largest country's in the world. If they have success eliminating cash and plastic cards within their borders by 2021, how will it affect the rest of the world? How will tourists pay for items while visiting India on vacation or business? How long will it take for countries in Europe and North America to follow India's lead in adopting biometric technology as their primary channel for executing payments? These are just a few of many questions that biometric payment technology poses for our future.

An Introduction to Cryptocurrency and Blockchain

'Blockchain and Cryptocurrency and Bitcoin… Oh My!' While these titles do not hold the same feel as Dorothy's "Lions and Tigers and Bears", the terminologies are often intertwined, confusing and can feel threatening. A cryptocurrency is a technological form of verified payments that allows for movement of funds among participants outside of the "rails" provided by traditional financial institutions and payment card providers. Bitcoin is one of the pioneers in the world of cryptocurrency. Therefore, it has received the most publicity and notoriety when the media makes any mention about digital currencies. In fact, Bitcoin is almost synonymous with the word cryptocurrency, like how people may refer to a "Coke" for describing other types of soft drinks. It has also become a popular topic in current events due to recent changes in the marketplace, which enabled more of its trading and speculation. Bitcoin is just one of many cryptocurrencies available and used to conduct transactions in the digital marketplace. What enables and makes cryptocurrencies unique is the underlying

blockchain technology, which has uses beyond the currency markets. It is easiest to learn how cryptocurrency works if you start with its foundation – blockchain.

Blockchain, also known as a distributed ledger, is a shared ledger that incorporates technology to record every transaction. It is not possible to make changes to any of the recorded entries in the ledger. This is similar to writing in a book of transactions with a permanent marker rather than an erasable pencil. Every time a transaction takes place, blockchain adds details of that deal to a block. Miners verify this block by solving a calculation to prove its validity. Miners are tech-savvy individuals who use computer-processing power in a network of machines to solve the calculation. The "chain", which forms a sequential ledger open for anyone to view, accepts the block after the miners prove its validity. One of the ways that blockchain technology prevents fraud is that the ledger is stored in many different locations on the network, and the ledger activity is available for anyone to view at these locations. Therefore, if a hacker gains access to a single computer or local network and makes changes, the hundreds of digital copies of true transactions will expose the fraudulent activity.

Blockchain benefits cryptocurrencies as well as other types of transactions that no longer need a trusted intermediary such as a financial institution. For instance, this technology can establish a verified identification method that people can share to replace the "twenty questions" of verification used by a call center. Blockchain can also verify identities or smart contracts triggered by confirmed actions that occur. An example of this is a rental agreement where one person sends another cryptocurrency in exchange for a key. If the renter does not receive the key, then the cancelled contract automatically issues them a refund of the cryptocurrency. Blockchain records this transaction in the open. This gives all parties, including others, the ability to verify and see the transaction. Kodak recently announced it is working to use blockchain to manage and identify the digital rights of photographs. Many industry experts predict that it will become more common for people to use blockchain technology for transferring a vehicle title or the deed to a home. Many of these examples are of payments between two parties that require a third party (i.e., financial institution, attorney, property manager, etc.) to help facilitate the transaction. These illustrations prove that blockchain is reshaping how individuals pay each other for any type of transaction.

Bitcoin – A Cryptocurrency

Blockchain technology is responsible for building cryptocurrencies such as Bitcoin. Bitcoin is a digital form of money stored in the owner's online "virtual wallet". It operates independently and is not under the control of any government or financial institution. The introduction of Bitcoin into the market occurred in 2009, and it is still the most popular cryptocurrency. According to an article on Techradar.com, there have been over 3,000 other virtual currencies also introduced since Bitcoin's start. Bitcoins get part of their value from being a limited resource. You can buy them or earn them through "mining". Bitcoin mining programs calculate

an “encryption function” called a “hash” on a set of random numbers. Miners compete against one another by solving these complex calculations to earn Bitcoins. Investment in the process is critical for success. Miners who have the largest and fastest computers have the ability to gain the most coins. As of December 2017, there were approximately 17 million Bitcoins in circulation and the calculations limit the total Bitcoins to no more than 21 million. As the network gets larger, the hash becomes more complicated and miners get fewer Bitcoins for their time. As a result, the miners need better computers, but the rising Bitcoin values make it worth their time and cost. Although Bitcoin is the most common cryptocurrency in the market, other types of digital currencies have experienced similar success. Ethereum is an example of another cryptocurrency that has become popular. Its ability to offer a wider range of benefits to its users has helped Ethereum differentiate itself from other digital currencies.

Ethereum – More Than Just a Cryptocurrency

What is Ethereum? Like Bitcoin, Ethereum is a digital currency. Its introduction as a person-to-person payment platform occurred in 2015. Ether is the name of the Currency Value Exchange Unit or ‘token’ of the Ethereum network. The Ethereum network also uses blockchain as the “rails” for its users to buy or sell Ether. A person can also use this digital currency to trade for goods and services through blockchain. Like other digital currencies, Ether requires either computer hardware or a software program (Ethereum wallet) to interact with blockchain.

What sets Ethereum apart from other cryptocurrencies, is that it leverages blockchain to offer a wider range of solutions. For example, Ethereum is also a platform for applications that run on a peer-to-peer network of computers. Ethereum separates itself from Bitcoin by offering the Ethereum network, where users can build and operate applications. In contrast, Bitcoin is only a digital currency. The Ethereum network has a business functionality, which makes it an attractive resource for corporations. This has led to the creation of a non-profit organization called Enterprise Ethereum Alliance. According to its website, this alliance’s purpose is to connect “Fortune 500 enterprises, startups, academics, and technology vendors with Ethereum subject matter experts”. Three of the founding members for the Enterprise Ethereum Alliance are J.P. Morgan Chase, Microsoft and Intel. Over two hundred companies have joined this alliance as members since its inception. Ethereum is a perfect example on how vast the capabilities of cryptocurrencies and blockchain can be.

Current Usage and Challenges for Cryptocurrencies

Cryptocurrencies are becoming more widely accepted as a payment solution, but they still have many challenges to overcome to sustain long-term success as an option for the everyday consumer. One of their challenges in becoming a widely accepted payment method is their structure as specialized markets with limited uses. Bitcoin has had the most success in

overcoming this hurdle thanks to its increasing value and popularity. At this time, established retailers already accept Bitcoin as a method of payment from their customers. Some of these retailers include Overstock, Expedia, Newegg and Dish Network. Certain ATM locations and vendors allow an individual to exchange their Bitcoin for more traditional forms of currency such as the US dollar. Cryptocurrencies still have a long way to go before the average consumer accepts them as a preferred payment method. As a newer technology, cryptocurrency has many other challenges that it needs to overcome. Some of these challenges include unstable values, high transaction fees, fraud and a lack of regulation.

Cryptocurrency values have soared, and this has created questions surrounding the legitimacy of their worth. Bitcoin is not immune to these fluctuating values. Issues of supply and demand are prevalent with this type of digital currency thanks to its popularity and its finite number of available coins. These factors have led to large swings in Bitcoin's value. In December of 2017, the Chicago Exchange started to allow Bitcoin to trade as a commodity (similar to pork bellies or wheat). Now this cryptocurrency has an established futures market, which allows a trader to enter a contract based on the expected price of the underlying Bitcoin value at a future date. This creates even more speculation and volatility as increased trading can occur on the values of the Bitcoin. This speculation, in conjunction with a less defined transaction market, gives cause for concern that a cryptocurrency bubble is waiting to burst.

Having large swings in value that fluctuate so frequently makes it unreasonable to use many available cryptocurrencies for every day transactions. Originally, several experts believed that Bitcoin would be a great alternative for small purchases or "micropayments", because it would eliminate the credit card interchange fees that are sometimes larger than the purchased item. This has not been the case, and cryptocurrencies, such as Bitcoin, have struggled with large transaction costs. A CNBC article from December of 2017 noted that people are paying $28 on average to complete transactions using this digital currency. One person claimed that he had to pay $16 to send $25 worth of Bitcoin from one address to another. This article also explained that it typically takes around 78 minutes to confirm a Bitcoin transaction, but it took nearly 1,200 minutes on one particular day. High costs at low speeds makes Bitcoin a poor substitute for cash or plastic at this time.

Cryptocurrency technology is set up as a safe substitute for the traditional currencies and payment systems. However, they are unregulated so few protections are in place for consumers. Even though blockchain acts as an open-network, digital currencies still experience fraud, hacking and theft. Fraud has occurred after third-party service wallets used for storing digital funds, such as Coinbase, are victim to scandals involving stolen Bitcoins. Similar to other online financial services, many of these companies require an Account ID and Password for access. These login credentials share the same vulnerabilities as other online accounts for being hacked. After a hacker obtains the credentials, they can steal all a person's Bitcoins. An example of significant Bitcoin theft occurred in December of 2017 when a Bitcoin mining service, called NiceHash, was hacked. This incident resulted in a loss of $64 million in currency,

drawing similarities to the Target hack of 2013. Unlike the Target breach, the NiceHash victims are not likely to recover any losses.

Some breaches have caused the public to question if certain cryptocurrencies are really an open network. For example, the Ethereum network was hacked in 2016, resulting in approximately $50 million of stolen tokens. The Ethereum Foundation, who is the developer behind this platform, reversed some of these fraudulent transactions. This action allowed investors to claim back $40 million of the stolen currency. This goes against the very core concept of being a horizontally layered network in which no single entity would have power over another by undoing what has already transpired. This example shows how the Ethereum network contradicted the culture of an open-network system, which it claims to be. By comparing how the NiceHash and Ethereum network handled their separate breaches, it is evident that the cryptocurrency market suffers from a lack of regulation. This is an issue for the consumer, because it allows the cryptocurrency companies to do as they please without having to answer to any form of oversight agency. A lack of regulation also makes cryptocurrencies, such as Bitcoin, an attractive avenue for nefarious payments and transactions. This allows criminals to use cryptocurrency as a means of anonymity for money laundering or purchasing illegal products and services on the "dark web".

Are Blockchain and Cryptocurrencies a Threat to Credit Unions?

Blockchain and cryptocurrencies are experiencing significant momentum and publicity in the financial industry at this time, but there is still some uncertainty with the long-term potential of these technologies. Volatility may prove to be the largest challenge for cryptocurrencies becoming the average consumer's payment method of choice. However, credit unions still need to pay attention to blockchain and cryptocurrencies, because these technologies allow individuals to conduct certain transactions without using a financial institution. The big question for certain cryptocurrencies is if they can keep up with their current pace. At this time, Bitcoin appears to be the most disruptive cryptocurrency for the payment industry. Even though it is the most popular cryptocurrency, Bitcoin still needs to overcome significant challenges to become a real threat for the credit union industry. This digital currency has many appealing characteristics that can threaten our industry, but it still has serious drawbacks. Bitcoin's high costs and slow transaction speeds are major setbacks for widespread adoption. Its finite number of coins also restricts the size of its market for transactions. Lastly, consumers have concerns over the currency's uninsured status and aforementioned volatility. These identified issues reaffirm that Bitcoin, by itself, is not a significant threat to the credit union industry as a payment alternative now. However, better and more agile products often replace the early leader.

New cryptocurrencies are already taking advantage of Bitcoin's weaknesses. As noted earlier, Bitcoin has high transaction costs and slow transaction speeds. One of its competitors claims

that their XRP currency (the fourth largest by market value) uses a different technology that makes payments in seconds and costs a fraction of a penny. This competitor is implying that they have a better position for making payments and transfers than Bitcoin does, which proves that even the most popular digital currencies are not immune to new competition disrupting their market share. Kik Interactive is another competitor, which launched its own app-based cryptocurrency (Kin) aimed towards the teen demographic. Kik is the first non-blockchain application to develop their own cryptocurrency. These are just a couple of examples that prove how fierce competition is in today's digital marketplace. Not many cryptocurrencies experience significant success due to an over-saturated market containing thousands of digital currencies. In the near future, we may even see an exchange rate to measure cryptocurrencies against one another. This would negatively affect digital currencies, because it creates similar limitations that physical currencies possess now. Competition from other digital currencies can have its benefits, because it influences innovation that can push the cryptocurrency market beyond some of its current challenges. Credit unions need to keep this in mind when discussing their long-term strategic plans.

Credit union leaders also need to be aware that blockchain technology is capable of much more disruption to the financial industry than just the act of buying and selling digital currencies. Etherium's open-network platform enables budding entrepreneurs to create a crowdfund for soliciting monetary contributions though tokenization within the Ethereum network. These entrepreneurs do not need a loan or deposit account to aid in Ethereum crowdfunding. This process eliminates the need for a financial institution to act as the "middle man". Ultimately, the Ethereum platform allows consumers to create nearly any type of project or business that they wish to operate on the Ethereum network. Ethereum's increasing popularity is helping the cryptocurrency market become more commonplace as a method of making payments. This could lead to a further decline of the traditional "brick and mortar" branches used by credit unions and banks. Credit unions should be concerned with the increasing popularity of blockchain technology, because more publicity will help it continue to make inroads within the financial industry. In addition, financial institutions will experience new challenges as consumers identify other ways to leverage blockchain. Credit unions also need to be wary of the growing number of adult millennials, because this generation of potential members is more likely to adopt cryptocurrencies and blockchain for executing their payments in the future. These trends reinforce the importance of credit unions familiarizing themselves with these technologies. Blockchain and cryptocurrencies do not present an immediate threat to credit unions today, but this will change in the future as their momentum continues to build.

III. **RECOMMENDATIONS**

Mobile Payments

Most financial institutions, including credit unions, already offer mobile payment solutions to their customers/ members. However, mobile technology continues to improve its payment solutions and many financial institutions do not effectively leverage these enhancements, because they do not understand the drivers behind its demand. Member adoption of mobile payments is still a challenge for most credit unions, but the public's appetite for this delivery channel is building. According to an article written by BI Intelligence in September of 2016, approximately 45% of millennials have made a NFC payment. Mobile payment adoption should continue to increase as younger generations grow to become a larger percentage of the general population. The BI Intelligence article also states that mobile payments will continue to grow at a compound annual growth rate (CAGR) of 80% through 2020. Therefore, the financial institutions who experience the best adoption rates for their mobile payment services will also experience the most success. It is important to understand why these adoption rates are so low now, so your credit union can plan for a strong future. Knowing this information is the best way for your organization to improve the number of mobile payments used by its members. Fear of inadequate security is one of the main reasons many people still stay away from executing mobile payments. Security is a critical feature in the financial services industry, and the growing number of data breaches has made consumers more cautious when conducting their financial transactions. When a credit union offers new mobile payment options to its membership, it should focus on the security of its members' personal information. To do this, the credit union will need to implement proper safeguards and will need to ensure that its vendors do the same as well.

Although effective security is the most critical aspect of a mobile payment platform, your credit union still needs to take other measures for ensuring that its membership adoption rate for mobile payments is successful. As technology continues to change, it is important that your credit union use a mobile platform that is versatile. Selecting the right vendor to partner with for your mobile payment services will help your organization stay relevant as the digital wallet space continues to evolve. By developing your platform with agility in mind, a credit union can adapt to changes more quickly. This allows the credit union to stay competitive by offering the most current mobile product and service offerings. It is also important to make sure that the platform can support multiple mobile touchpoints, because there are several different touchpoints when it comes to mobile services. To be successful with this technology, a credit union needs to offer a platform that is accessible to these touchpoints (i.e., SMS texting, phone apps, mobile websites and tablets). Ensuring that all its members have access to its mobile payment system is essential for achieving a successful usage rate.

The credit union still needs to take several steps to ensure success after it develops a mobile platform for member use. For successful adoption rates, members need to be able to enroll

easily. Some mobile platforms require you to enroll through computer-based systems, which may not be the best option now that most consumers use their mobile device as their computer. Instead, a best practice is for your credit union to adopt a platform that allows users to enroll with their mobile device. The final step to ensuring a successful adoption rate for mobile payment services is effective promotion. It is important to highlight certain functions of the product with a goal of attracting all types of users. Some features of your mobile payment product may be important to certain members, while other features will attract other member segments. Therefore, a credit union should highlight all the different benefits of its mobile payment services for a better chance of attracting more users. If other financial institutions are more successful than your credit union in promoting their mobile payment services, then they will be able to attract more customers, including members from your organization. This makes it critical that your members recognize the value of your mobile services first, before they leave for another financial institution that appears to be more convenient.

Opportunities and Challenges for Mobile Payments

Offering appropriate mobile payment solutions presents a tremendous opportunity for a credit union to attract and retain targeted member groups. The biggest benefit for a member who uses a mobile device for executing payments is convenience. Our members' time is very valuable so it is important to offer them solutions that can save them time while processing payments. For example, why should a member wait to receive a plastic card in the mail before making purchases? They should already have the ability to use the money in their account if it is available, and apps through their mobile devices can help with this. In addition, there is more to convenience than just optimizing the value of time. For example, avid runners can now use Garmin Pay as a payment solution through their watch. Many exercise enthusiasts use Garmin watches to track their time, pace, distance and heart rate while they run, bike or swim. Now a person can stop by a store and use their watch to purchase a sports drink after a long run (without carrying their wallet or cell phone). It is important for your credit union to identify which mobile technology service is most appropriate to offer to its membership. It should also keep in mind specific groups of new members that it hopes to attract when making these decisions.

Member adoption continues to be a major challenge for many credit unions who just introduced a new mobile payment service. On top of that, low adoption rates may prevent some credit unions from investing in new mobile payment services. Other credit unions may stay away from mobile payments all together due to the low industry-wide adoption rates experienced in the market today. Low adoption rates can also occur due to how a credit union presents their mobile payment solutions to its members. Some members may get the negative feeling that a credit union is devaluing them by trying to push them away from traditional branch services. This can occur if your credit union is too strong in its approach with encouraging its members to sign up for mobile services. Rolling out a system that does not

provide the tools and services that your members value can also be a detractor for your organization. It is important for your credit union to take its time when deciding on a mobile payments partner, and when deciding on payment solutions that will put it in position for future success from membership growth. No organization wants to lose market share by not offering mobile payments. However, it is crucial that your credit union fully vets any new services to avoid losing trust as a byproduct of offering a less than par product.

Biometric Payments

Biometric technology can provide a tremendous benefit for credit unions that learn how to leverage it effectively. As mentioned earlier, this technology adds convenience and security for your members as they make payments. Offering this service is like most other strategic decisions. There is not a "one size fits all" approach on deciding how to roll out biometric payments to your membership. Some credit unions may benefit as an early adopter with this newer payment method, while other credit unions may be better off waiting until biometric payments become more widely accepted by society. How your credit union chooses to implement biometric technology depends on several factors. These factors include your credit union's size, technological resources, membership make-up and risk appetite.

Factors That Determine When to Invest in Biometric Technology

Your credit union's size can play a significant role in determining whether it should offer biometric payments now. Smaller credit unions may not have the scale or the financial resources to make this technological investment. In addition, it is in the best interest for credit unions with limited financial resources to allocate any available funds to more pressing needs for their membership. Larger credit unions typically have the financial resources that allow them to introduce new technologies, such as biometrics, to their memberships. Most large credit unions also have strong technological infrastructures, which they can leverage to develop a strategic approach for implementing biometric payments as a service.

The technological resources that a credit union possesses are critical in determining which biometric processes to incorporate. As discussed earlier, biometric technology offers many solutions for financial institutions. Some of these solutions include convenient and secure payment authentication for a member processing a transaction at the teller line, on their mobile device and at a POS terminal. How your credit union chooses to integrate biometrics as a service for its members depends on its technological capabilities. To offer biometric technology, your credit union needs to have sufficient hardware in place and enough personnel to support this hardware. Determining if your credit union has the necessary financial and technological resources is the first step in offering biometric payment solutions to your membership. However, your credit union still needs to decide if offering this technology fits

with its strategic direction before biometric payments become a reality at this time for your organization.

During strategic planning, the first question that your credit union's leadership needs to ask is if biometric payments will benefit the overall membership. To do this, they will need to focus on your institution's membership demographics and its membership appetite for adopting new technologies. Younger generations are likely to be more comfortable in executing payments with their biometric data. On the other hand, a large percentage of the Baby Boomer generation may be slower to adopt this method of making payments. It is important to identify and cater towards the make-up of your credit union's specific membership. Your credit union will not benefit from investing money in biometric technology if no one uses it. You should also be aware that completely replacing traditional payment methods with biometrics might result in attrition within your existing membership if they are slow at adopting new technologies. Many approaches can gather the information needed to understand your membership's make-up and appetite for new technologies. Some of these approaches include focus groups, questionnaires and membership studies conducted by consultants.

If your credit union's leadership is considering biometric payment services, they will also need to ask if the risks associated with offering this technology are in the best interest for the credit union as a whole. If so, they need to determine an acceptable level of risk for investing in this technology. Biometrics have been around for decades in some shape and form. However, the way we use biometrics for processing payments today is a newer iteration of this technology. Various risks are inherit whenever offering a new or enhanced technology, especially in the financial industry. The biggest risk associated with biometric payments is the security of the databases that store biometric identifiers. Biometrics are a great payment solution from a three-factor authentication standpoint because they meet the 'inherence' category within this approach. For example, your fingerprints are a physical characteristic inherent to you, and they enhance your access security when they are presented with what you know (password) and what you possess (card). The risk that needs consideration for these biometric identifiers is when a hacker compromises this information during a data breach. Your members can change their compromised passwords, but they will not be able to change their fingerprints. An option to mitigate some of this risk is to avoid storing sensitive biometric data on a centralized server. Instead, your credit union can rely on a system where this information is stored on a member's device such as their phone or computer. This process verifies their identification through confirmation signals passed between the device and the merchant.

Risk of Ignoring Biometric Technology

It may appear safer to do nothing regarding biometric payments considering the technological investment required, the uncertain adoptions rates and the security risks associated with this new technology. However, there is also a risk of ignoring biometrics or offering them to your

membership too late. As mentioned earlier biometrics can offer a third layer of authentication to enhance security and they can add convenience by speeding up the transaction process. As members become accustomed to these technological efficiencies, their expectations will increase. The average consumer values convenience, ease of use and security for their financial services. Biometrics offer a payment solution that checks all of these boxes. No one wants to remember 20 different passwords that are all 8-12 characters long and include a number and special character. Leveraging the biometric identifiers of your members can eliminate the need to use these cumbersome and inconvenient passwords. Most individuals gravitate towards the path of least resistance. Attrition of existing members and failure to acquire new members may be the result if your credit union never adopts biometric technology as a future method of executing payments. Instead, your credit union leaders need to decide on the best time to introduce biometric payments to your membership, and to decide how this implementation can best meet the risk requirements of your credit union.

Blockchain and Cryptocurrencies

Of the three areas discussed, blockchain and cryptocurrency are the newest payment disrupters that credit unions need to consider. Each credit union will have its own strategic plan to help determine the timing and how much of this technology to adopt. For reasons mentioned earlier, the cryptocurrency payment market is not an immediate threat to credit unions due to problems regarding price fluctuations, high transaction costs, slow transaction speeds and low acceptance rates across the vendor and person-to-person landscapes. However, blockchain technology's ultimate application has the potential to affect a variety of different payments and other processes. During today's strategic planning sessions, credit unions should be actively discussing blockchain and should be considering how to incorporate this technology within their suite of products and services.

Challenges and Possible Strategies for Blockchain and Cryptocurrencies

Blockchain faces similar challenges as most new technologies. The largest of these challenges is trying to converge on a standard that encourages large-scale adoption and allows a large percentage of consumers to benefit from this new system. There are many examples throughout history where different standards and new systems replace the early pioneers. Some of these examples include Beta vs VHS, Microsoft Zune vs Apple's iPod and BlackBerry vs IOS/ Android. Blockchain technology and cryptocurrencies present both opportunities and threats to credit unions. These possible outcomes can influence or inhibit a credit union's mindset regarding digital currencies. Early adopters of these new technologies risk losing on large investments, while those that join the party too late miss several opportunities regarding market share and technical knowledge. Additionally, the largest credit unions are very small compared to the largest banks and other FinTech companies. Their resources, both in dollars

and intellectual capital, are severely limited when compared to these competitors. However, credit unions have the perfect solution to overcome these challenges. Following the credit union blueprint of COOPERATION is the best course to take in regard to navigating through the treacherous waters of blockchain and cryptocurrency. The credit union movement has leveraged cooperation through its current use of shared branch networks and it has given credit union members access to thousands of ATMs free of any surcharge fee. This same cooperative opportunity exists in the credit union space for managing blockchain and cryptocurrency, and it is building momentum. A November 2017 Credit Union Journal article recently highlighted the announcement of two cooperative ventures. The National Association of Federally Insured Credit Unions (NAFCU) announced they were joining Hyperledger. In addition, CU Ledger announced they were partnering with Swirlds, the company that uses the hashgraph distributed consensus platform.

CU Ledger

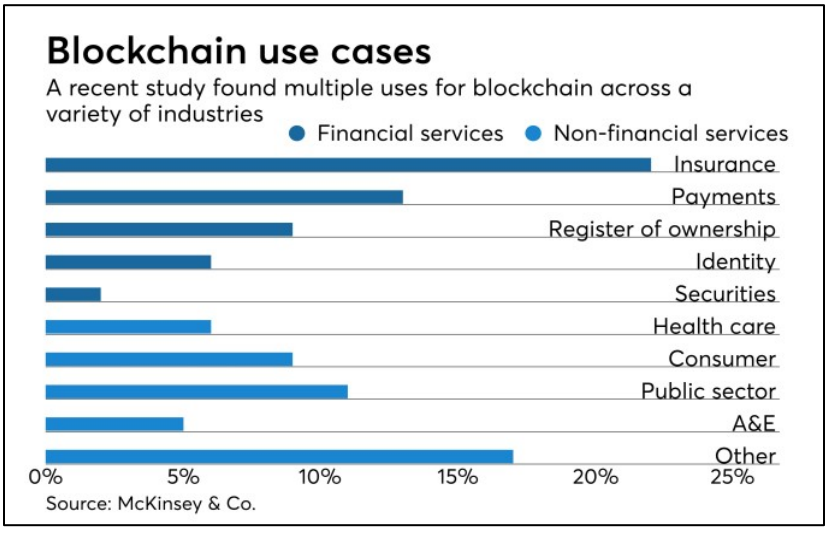
CU Ledger is a perfect example of where credit union cooperation is already at work, and it demonstrates the decisions that credit unions need to consider with their approach towards digital currencies. CU Ledger is a group supported by the Credit Union National Association (CUNA), Mountain West Credit Union association and the Best Innovation Group (BIG). An excellent breakdown of the CU Ledger concepts and practical solutions is available for viewing in a May 2017 update presented by CUNA on Vimeo. The same information regarding this update is also available on the CU Ledger website. The biggest impact that this process has made is with increasing the momentum for the credit union movement to build something that benefits all credit unions and their members. CU Ledger has already made significant decisions and achieved critical milestones. Examples of these decisions include using a private distributed ledger, working to use vendor partnerships and implementing a test case for use.

While Bitcoin is an example of a “permissionless” blockchain located on an open network, CU Ledger uses a “permissioned” blockchain on a private distributed ledger. Most other early testers in the financial institution market are following this same course of action. A private distributed ledger is a closed group of known users that work together while using blockchain. This method reduces “trust” issues, takes less processing power to solve calculations and improves the processing time for transactions. To increase their chances of success, CU Ledger collaborated with industry leaders to lay the foundation for their distributed ledger. An example of this occurred when they announced their partnership with Swirlds, who created the hashgraph distributed consensus platform. The purpose for choosing this path was not only to promote a platform with a banking-grade security level, but also to enable high speeds for processing transactions. Many other distributed ledger platforms only process thousands of transactions per second, while the hashgraph platform processes hundreds of thousands of transactions per second. Lastly, one of CU Ledger’s first applications for their distributed ledger is the creation of an electronic identity. This application allows for credit unions and individuals

to opt-in with creating an electronic identification, which is transportable and usable by any other organization that participates in the network. An example of this useful application may occur when a call center needs to verify the identification of a member. While the member waits on hold, the credit union's call center technology sends a message to the member's phone app that asks for verification in the form of a biometric fingerprint. This allows the call center representative to move forward in confidence when they take the call without asking several questions to confirm the member's identity. In addition, this process is a more secure form of verification, because the traditional "out of wallet" questions are most likely compromised from various breaches (e.g., Equifax Breach of 2017). Distributed ledger technology also incorporates multiple checks throughout its process. These include checking the credentials of the member, checking the credentials of the requesting credit union, verifying the device used in the transaction and using separate biometric confirmations.

Thinking Big and Process Changing Innovation

Like the case with CU Ledger, one of the biggest steps to move forward with implementing blockchain is to determine the possible business cases for its use. A CU Journal article highlights a survey of 200 companies conducted by McKinsey & Company. This study indicates that there are 64 different business cases for utilizing blockchain technology, and approximately half of these cases relate to the financial services industry.



It is important for your credit union to select the correct blockchain business cases for your membership. However, it is just as important to view distributed ledger technology (DLT) in an unrestricted mindset, because DLT is an opportunity to rethink the overall payment process. In addition, your credit union should consider all the possibilities available to it within a distributed ledger system.

Success in accomplishing these large-scale process changes emanates from DLT's ability to allow for "trust" throughout the process and to create an open transaction record.
Each credit union should be cognizant of the opportunities that blockchain/cryptocurrency creates, and should be aware of this technology's ability to influence the future of the financial industry. Therefore, a best practice is for credit unions to make decisions regarding these emerging technologies when developing their strategic plans. A possible strategy is considering ways to collaborate with others in the credit union space. Taking advantage of a cooperative DLT network will create scale that enables credit unions to be successful for offering the best digital member experience in the future.

A Similar Approach for All Payment Disrupters

Each of the payment disrupters identified in this white paper threatens to end how consumers have processed payments for decades. The technological and risk appetite of the average consumer continues to evolve, as millennials get older. Although mobile payments, biometric payments and blockchain/cryptocurrency payments are each unique in their own way, they still share various similarities. These disrupters even fit together on occasion to solve payment and verification pain points. An example of this occurs when a consumer uses their thumbprint for identity verification while executing a mobile payment. Blockchain and cryptocurrency has the potential to become the biggest game changer regarding the payment industry. This disruptor is so significant, because it changes the delivery channel for making payments (blockchain) and it changes the medium of exchange we use to make these payments (cryptocurrency). In addition, blockchain and cryptocurrencies are so new to the market that nobody really knows what type of long-term affects they will have on the financial services industry.

Credit unions should use a similar approach when dealing with these disrupters despite their differences. The worst thing to do would be to ignore these disrupters even if it appears that current adoption rates are low, because outside players are leveraging these new technologies to carve lucrative niches out of the financial services industry. Some of the new competition do not even share the same regulatory burdens as traditional financial institutions, which makes it an even greater challenge for credit unions to compete. Leveraging cooperative resources to offer these new payment solutions will be essential for the credit union movement as it progresses into the digital future. In addition, credit union employees need training that covers the benefits and the risks of payment technologies as they continue to evolve. Ultimately, credit unions need to be open-minded and agile in order to keep up with the changes that these payment disrupters have perpetrated on the financial services industry.

IV. SUMMARY

All three payment disrupters discussed in this paper are very relevant to the current financial market, and this helped our group's research efforts. Mobile payments have already been around for many years so there was plenty of data for this disrupter that we were able to use in our research. Biometric technology and cryptocurrencies are newer forms of payment disrupters, but they have been the subject of many recently published articles and studies. All the material available to us for conducting our research made payment disrupters an ideal topic for our white paper. However, this topic was also a challenge for our group due to the abundance of information that we had to sort through. There is enough information on each of these disrupters, individually, for them to be the sole subjects of their own white papers. Our group recognized that these payment technologies all served the same purpose as disrupters to the financial services industry, so we decided it was pertinent to include them all in our study. Our goal was to produce a white paper that illustrates the similarities between these payment disrupters, and to provide credit union professionals with enough information to make objective strategic decisions regarding how to implement these new payment technologies within their organizations. We had many takeaways from researching and writing about these payment disrupters over the last several months. These takeaways include:

- Previous adoption rates for mobile payments have been slow, but this is quickly changing as technologies and generations of users evolve. In addition, most of today's consumers are never without their mobile phones. Credit unions need to put their focus into mobile payment technologies to offer a secure and efficient solution for their members.

- Credit unions can benefit from effectively introducing each of these payment methods as services to their members. However, there is still a challenge of finding a common framework or "operating system" to use when offering members these payment options. One thing that stands out for mobile payments is that the easiest and most convenient person-to-person payment systems used today operate on the existing infrastructure provided by MasterCard and VISA. This occurs due to almost everyone having this common network connection for executing payments versus the inability to settle on other universal payment systems (i.e., PayPal, Bitcoin, Fiserv's Popmoney, etc.).

- Using a member's thumbprint as a method of authentication is a biometric payment solution that credit unions may want to explore on a limited basis. However, further biometric solutions may not be viable for the majority of credit unions now.

- It is interesting to see how biometric identification technologies have evolved over time. Even more interesting, are the possibilities of using this technology for identity verification and payment solutions in the future. India is a major nation that has made a bold claim of removing all plastic cards and ATMs from their country's payment infrastructure by the year 2021. They plan to achieve this goal by relying on biometric technology as their primary payment method. If India is successful in removing all plastic cards from their payment infrastructure, how will this impact international business conducted within its borders? Will other major nations follow India's lead? These are just a couple of questions that will arise if India successfully meets their objective.

- Smart contracts have some very useful applications that can offer long-term cost savings to credit unions by eliminating intermediaries for payments and by sharing independent BSA verifications. Credit unions will benefit from using smart contracts to share BSA verifications through eliminating redundancies and reducing fraud with higher security thresholds. Unfortunately, the expense of adding qualified programmers, the loss of privacy for financial transactions and legal jurisdiction concerns currently outweighs any potential benefits. Credit Unions would likely require joint efforts from a cooperative, such as CU Ledger, to make the integration of smart contracts cost beneficial.

- Blockchain, or Distributed Ledger technologies, is very interesting due to its wide-ranging possibilities of driving improvements in member experiences and process changes. One of our team members commented that learning of these possibilities and learning that CUNA already has an existing cooperative startup called CU Ledger, makes him want to inquire what his credit union is willing to do to help this project move forward.

This white paper was particularly challenging due to the scope of its topic. Selecting the most relevant and influential material from numerous articles and case studies on these payment disrupters was a difficult task for our group, because so much interesting information was at our disposal for this assignment. We had to be cautious of scope creep while creating this paper in an effort to keep our message focused. Biometrics and blockchain technology both have uses outside of executing payments, and we highlighted some of these uses to give our reader a better understanding of how influential these technologies can be for the financial services industry. However, it was important to get quickly back in line with the central theme of our white paper, which is analyzing these technologies as payment disrupters. To help us stay focused, we consistently asked the same question; "What is not in our members' wallets?" Discovering the answer to this question is so important, because understanding your members' payment preferences is the only way to stay relevant as their financial institution of choice.

V. REFERENCES

(ICFAI), Prableen Bajpai CFA. "The 6 Most Important Cryptocurrencies Other Than Bitcoin." Investopedia. N.p., 09 Aug. 2017. Web. 14 Aug. 2017. http://www.investopedia.com/tech/6-most-important-cryptocurrencies-other-bitcoin.com

10 Best BitCoin Alternatives - Profitable Cryptocurrencies Mining With Home Computers." GeckoandFly. N.p., 07 July 2017. Web. 14 Aug. 2017. https://www.geckoandfly.com/23517/best-bitcoin-alternatives-cryptocurrencies-mining

12 Cryptocurrency Alternatives To Bitcoin." Google. Google, n.d. Web. 14 Aug. 2017. https://www.google.com/amp/www.bankrate.com/investing/12-cryptocurrency-alternatives-to-bitcoin/%3Famp%3D1

20% Of Smartphone Users Use Proximity Mobile Payments." Mobile Payments World, 9 Nov. 2016, www.mobilepaymentsworld.com/20-smartphone-users-use-proximity-mobile-payments/?v=7516fd43adaa.

A solution for your industry & your size of business." Bevel Payment Solutions Home Comments. N.p., n.d. Web. 14 Aug. 2017. https://www.bevelpayment.com

Arnold, Martin. "Financial Industry Faces Extreme Disruption in Payments." Financial Times, Financial Times, 26 Sept. 2016, www.ft.com/content/1b82a0e6-4f67-11e6-8172-e39ecd3b86fc.

Aurus: Cutting-Edge Retail Payment Solutions. N.p., n.d. Web. 14 Aug. 2017. http://www.siliconindiamagazine.com/vendor/aurus-cuttingedge-retail-payment-solutions-cid-1023.html

BI Intelligence. "Nearly Half of Millennials Have Used a Mobile Wallet." Business Insider, Business Insider, 6 Sept. 2016, www.businessinsider.com/nearly-half-of-millennials-have-used-a-mobile-wallet-2016-9

Bitcoin 2.0: The Rise of Ethereum." Strategic Tech Investor. N.p., n.d. Web. 14 Aug. 2017. http://strategictechinvestor.com/acq/ether/bitcoin-2-0-rise-ethereum/?src=adwords

Browne, Ryan. "Big Transaction Fees Are a Problem for Bitcoin - but There Could Be a Solution." CNBC, CNBC, 21 Dec. 2017, www.cnbc.com/2017/12/19/big-transactions-fees-are-a-problem-for-bitcoin.html.

Carter, Jamie. "Bitcoin vs Distributed Ledger vs Ethereum vs Blockchain." TechRadar, TechRadar pro IT Insights for Business, 13 Sept. 2016, www.techradar.com/news/internet/bitcoin-vs-distributed-ledger-vs-ethereum-vs-blockchain-1328432

China Mobile Proximity Payments Market Growth | PYMNTS.com.” Google, Google, www.google.com/amp/www.pymnts.com/news/mobile-payments/2016/china-mobile-proximity-payments/amp/.

Coin-on-a-String Trick." TV Tropes. N.p., n.d. Web. 14 Aug. 2017. http://tvtropes.org/pmwiki/pmwiki.php/Main/CoinOnAStringTrick.com

Cooper, Luke. “Blockchain Explained: What You Need To Know About The Future Of Money.” Huffington Post Australia, Huffington Post Australia, 3 Aug. 2017, www.huffingtonpost.com.au/2017/08/02/blockchain-explained-what-you-need-to-know_a_23025848/.

Drèze, Jean. “Aadhaar or Else.” The Indian Express, 20 Nov. 2017, indianexpress.com/article/opinion/columns/aadhaar-biometric-authentication-abba-public-distribution-system-pds-jharkhand-4946834/.

ENISA. “Security of Mobile Payments and Digital Wallets.” Security of Mobile Payments and Digital Wallets - ENISA, 13 Jan. 2017, www.enisa.europa.eu/publications/mobile-payments-security/.

e-Security, Richard Moulds Thales. “Why Mobile Payments Adoption Has Been Slow – And Why That's About to Change.” Wired, Conde Nast, 7 Aug. 2015, www.wired.com/insights/2015/01/mobile-payments-adoption/.

Ethereum: the competitor to Bitcoin which could transform entire industries." Google. Google, n.d. Web. 14 Aug. 2017. https://www.google.com/amp/www.newstatesman.com/culture/observations/2016/04/ethereum-competitor-bitcoin-which-could-transform-entire-industries%3Famp

Gartenberg, Chaim. “Google Is Killing Its Experimental Hands Free Payment App.” The Verge, The Verge, 2 Feb. 2017, www.theverge.com/2017/2/2/14483758/google-hands-free-payment-app-shut-down-android-pay.
Gillespie, Patrick. “Cash Is Still King in the Digital Era.” CNNMoney, Cable News Network, 20 Nov. 2017, money.cnn.com/2017/11/20/news/economy/cash-circulation-payment/index.html.

Glaser, April. "Biometrics Are Coming, Along With Serious Security Concerns." Wired. Conde Nast, 03 June 2017. Web. 14 Aug. 2017. https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/

History of Mobile & Contactless Payment Systems.” History of Mobile and Contactless Payment Systems – NearFieldCommunication.org, nearfieldcommunication.org/payment-systems.html.

India's Banks Must Move to Aadhaar-Based Biometric Authentication." Bank Information Security. N.p., n.d. Web. 14 Aug. 2017. http://www.bankinfosecurity.com/indias-banks-must-move-to-aadhaar-based-biometric-authentication-a-9785

Iyengar, Rishi. “India Could Switch to Biometric Payments by 2020.” CNNMoney, Cable News Network, 19 Jan. 2017, money.cnn.com/2017/01/19/technology/india-cash-biometric-payments-davos/index.html.

Kanvaty, Vishal, and Sudhir Kesavan. “Blockchain Adoption by the Banking Industry.” MEDICI, MEDICI, 23 Nov. 2016, gomedici.com/blockchain-adoption-by-the-banking-industry/.

King, W.B. “Are Credit Unions Ready to Do More than Dip a Toe into Distributed Ledger?” Credit Union Journal, 14 Nov. 2017, www.cujournal.com/news/are-credit-unions-ready-to-do-more-than-dip-a-toe-into-distributed-ledger.

Lomas, Natasha. "MasterCard trials biometric bankcard with embedded fingerprint reader." TechCrunch. TechCrunch, 20 Apr. 2017. Web. 14 Aug. 2017. https://techcrunch.com/2017/04/20/mastercard-trials-biometric-bankcard-with-embedded-fingerprint-reader/

Looking for a Bitcoin Alternative? Here are 6 Coins to Consider." Google. Google, n.d. Web. 14 Aug. 2017. https://www.google.com/amp/s/99bitcoins.com/bitcoin-alternative-6-coins/amp/

McKinsey & Company. Global Payments 2015: A Healthy Industry Confronts Disruption . Oct. 2015, www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/how%20the%20payments%20industry%20is%20being%20disrupted/global_payments_2015_a_healthy_industry_confronts_disruption.ashx.

New Ways to Pay." InComm. N.p., n.d. Web. 14 Aug. 2017. http://www.incomm.com/our-solutions/Pages/New-Ways-to-Pay.aspx

NFC Guide: All You Need to Know About Near Field Communication.” Square, squareup.com/guides/nfc.

OMNICHANNEL PAYMENT SOLUTIONS." Financial Technology Leader - Global Payments. N.p., n.d. Web. 14 Aug. 2017. https://www.globalpaymentsinc.com/en-us

Orem, Tina. “Visa Launches Fingerprint-Enabled Credit Cards.” Credit Union Times, 22 Jan. 2018, www.cutimes.com/2018/01/22/visa-launches-fingerprint-enabled-credit-cards?eNL=5a669a5b160ba09a060a900b&utm_source=CUT_Daily&utm_medium=EMC-Email_editorial&utm_campaign=01232018.

Pinola, Melanie. “Lose the Wallet and Pick Up a Mobile Payment App.” Lifewire, 13 Mar. 2018, www.lifewire.com/mobile-payments-4103869.

POS Payment Technology, Mobile & Clover Payment | Silveredge." Silver Edge. N.p., n.d. Web. 14 Aug. 2017. http://gosilveredge.com

Proximity and Remote Mobile Wallets: What's the Difference?” Mobile Business Insights, 2 Dec. 2016, http://mobilebusinessinsights.com/2016/08/proximity-remote-mobile-wallets-whats-difference/

Proximity Payments, equensworldline.com/emergingservices/mobile_financial_services/proximity_payments.jsp.

Rampton, John. "10 cutting-edge companies changing the way payments are made." Mashable. Mashable, 16 Apr. 2016. Web. 14 Aug. 2017. http://mashable.com/2016/04/16/10-companies-changing-payments/#IaVewCWIa8qm

Rampton, John. "The evolution of the mobile payment." TechCrunch. TechCrunch, 17 June 2016. Web. 14 Aug. 2017. https://techcrunch.com/2016/06/17/the-evolution-of-the-mobile-payment

Redirect Notice." Google. Google, n.d. Web. 14 Aug. 2017. https://www.google.com/amp/www.cnbc.com/amp/2017/05/23/bigger-than-bitcoin-enterprise-ethereum-alliance-grows-in-size.html

Roberts, Jeff John. "What if Your Fingerprint Gets Hacked? Biometrics Pose New Security Risk." Biometrics Pose New Risk to Consumer Security | Fortune.com. Fortune, 12 May 2016. Web. 14 Aug. 2017. http://fortune.com/2016/05/12/biometrics-passwords/

Rosic, Ameer. “What Are Smart Contracts? A Beginner's Guide to Smart Contracts.” Blockgeeks, Jan. 2017, blockgeeks.com/guides/smart-contracts/.

Services, Total Merchant. "Total Merchant Services Offers Free, Cutting-Edge Payment Processing Solutions for Businesses of All Types." PR Newswire: news distribution, targeting and monitoring. N.p., 26 Jan. 2017. Web. 14 Aug. 2017. http://www.prnewswire.com/news-releases/total-merchant-services-offers-free-cutting-edge-payment-processing-solutions-for-businesses-of-all-types-300397133.html

Sottile, Chiara A. "As Biometric Scanning Use Grows, So Does Security Risk." NBCNews.com. NBCUniversal News Group, 24 July 2016. Web. 14 Aug. 2017. http://www.nbcnews.com/tech/tech-news/biometric-scanning-use-grows-so-do-security-risks-n593161

Swirlds and CULedger Collaborate to Deliver High Performance, Secure, Distributed Applications to Credit Unions." CUNA News RSS, 27 Oct. 2017, news.cuna.org/articles/113192-swirlds-and-culedger-collaborate-to-deliver-high-performance-secure-distributed-applications-to-credit-unions.

The 1 Reason Why These Entrepreneurs Are All In on Ethereum (ETH), Bitcoin's Competitor." Influencive. N.p., 22 Mar. 2017. Web. 14 Aug. 2017. http://www.influencive.com/1-reason-entrepreneurs-ethereum-eth-bitcoins-competitor/

The Future of Payments." ACI Worldwide. N.p., n.d. Web. 14 Aug. 2017. https://www.aciworldwide.com/lp/future-payments

The head of a government-run policy institute said on Thursday that the country could completely eliminate the need for credit cards. "India could switch to biometric payments by 2020." CNNMoney. Cable News Network, n.d. Web. 14 Aug. 2017. http://money.cnn.com/2017/01/19/technology/india-cash-biometric-payments-davos/index.html

The Rise And Fall Of Bitcoin (And The New Kid On The Blockchain)." Google. Google, n.d. Web. 14 Aug. 2017. https://www.google.com/amp/s/www.forbes.com/sites/forbestechcouncil/2017/04/20/the-rise-and-fall-of-bitcoin-and-the-new-kid-on-the-blockchain/amp/

Thompson, Collin. "How Does the Blockchain Work? (Part 1) – The Blockchain Review – Medium." Medium, The Blockchain Review, 2 Oct. 2016, http://medium.com/the-intrepid-review/how-does-the-blockchain-work-for-dummies-explained-simply-9f94d386e093

Urrico, Roy. "Biometrics Catching on With Credit Unions." Credit Union Times. N.p., 16 June 2017. Web. 14 Aug. 2017. http://www.cutimes.com/2017/06/16/biometrics-catching-on-with-creditunions?eNL=5968f0c0150ba0fe4cd817e7&utm_source=CUT_CuttingEdge&utm_medium=EMC-Email_editorial&utm_campaign=07172017

Urrico, Roy. "U.S. Biometric Payment Card Market Trial, Secure Tech Alliance Agenda Announced." CUTimes.com, CreditUnionTimes, 16 Jan. 2018 www.cutimes.com/sites/credituniontimes/2018/01/16/u-s-biometric-payment-card-market-trial-secure-tech-alliance-agenda-announced/.

Virtual Merchant Services | Cutting Edge Bank Card Services." Cutting Edge Bank Card Services, Inc. N.p., n.d. Web. 14 Aug. 2017. http://ce411.com

What's the biggest competitor to bitcoins?" What's the biggest competitor to bitcoins? - Quora. N.p., n.d. Web. 14 Aug. 2017. https://www.quora.com/Whats-the-biggest-competitor-to-bitcoins

Why Ethereum is outpacing Bitcoin." Google. Google, n.d. Web. 14 Aug. 2017. https://www.google.com/amp/s/venturebeat.com/2017/06/11/why-ethereum-is-outpacing-bitcoin/amp

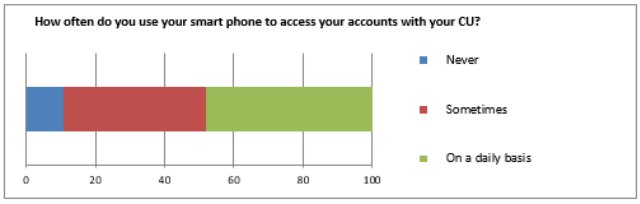
Why Ethereum is outpacing Bitcoin." VentureBeat. N.p., 09 June 2017. Web. 14 Aug. 2017. https://venturebeat.com/2017/06/11/why-ethereum-is-outpacing-bitcoin/
Written by Hwan Kim, Manager, Monitor Deloitte. "5 predictions for the future of payments."

World Economic Forum. N.p., n.d. Web. 14 Aug. 2017. https://www.weforum.org/agenda/2015/08/5-predictions-for-the-future-of-payments/

VI. APPENDIX – SURVEY RESULTS

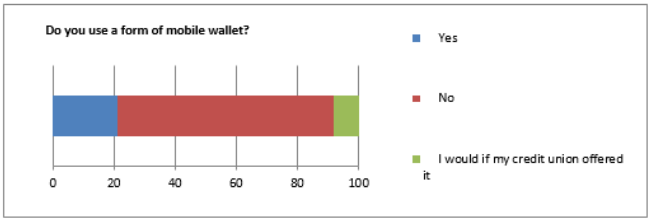
1.) **How often do you use your smart phone to access accounts with your credit union?**

Never	11
Sometimes	41
On a daily basis	48
	100



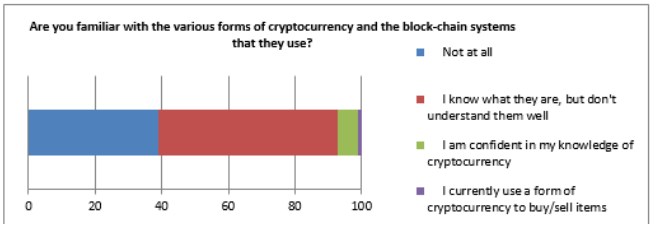
2.) **Do you use a form of mobile wallet (i.e. Apple Pay)?**

Yes	21
No	71
I would if my credit union offered it	8
	100



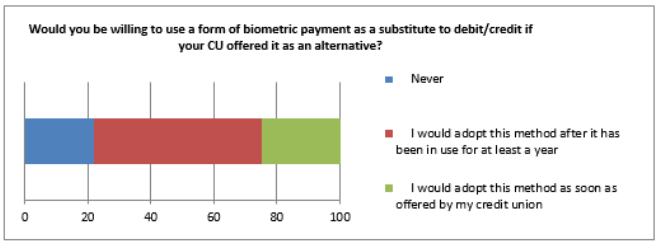
3.) **Are you familiar with the various forms of cryptocurrency (i.e. Bitcoin), and the block-chain systems that they use?**

Not at all	39
I know what they are, but don't understand them well	54
I am confident in my knowledge of cryptocurrency	6
I currently use a form of cryptocurrency to buy/sell items	1
	100



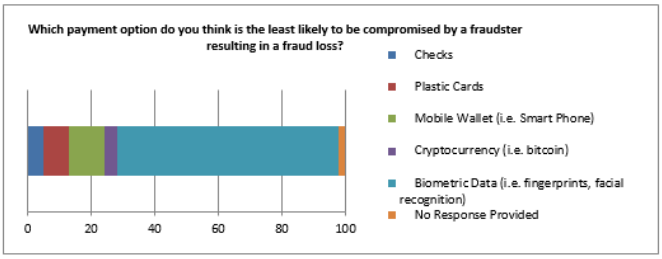
4.) **Would you be willing to use a form of biometric payment (i.e. fingerprints, eye scans, etc.) as a substitute to debit/credit if your credit union offered it as an alternative?**

Never	22
I would adopt this method after it has been in use for at least a year	53
I would adopt this method as soon as offered by my credit union	25
	100



5.) **Which payment option do you think is the least likely to be compromised by a fraudster resulting in a fraud loss?**

Checks	5
Plastic Cards	8
Mobile Wallet (i.e. Smart Phone)	11
Cryptocurrency (i.e. bitcoin)	4
Biometric Data (i.e. fingerprints, facial recognition)	70
No Response Provided	2
	100



6.) **Do you think any of the new payment technologies will negatively affect the credit union industry?**

Worried that credit unions will go away in the near future	4
Concerned that credit unions will be able to remain adapt and remain releva	33
Not concerned at all!	53
Other	10
	100