APPLICATION OF BLOCKCHAIN FOR AUTHENTICATION, VERIFICATION OF IDENTITY AND CLOUD COMPUTING

by

Raymond G. Kuebler

A Capstone Project Submitted to the Faculty of

Utica College

May 2018

In Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Financial Crime and Compliance Management

Abstract

Blockchain has the potential to become a major force within the financial services industry by transforming the way information is secured within our expanding digitalized world. Blockchain provides added security through the authentication of peers that share virtual cash, encryption and the generation of hash values. Blockchain is the foundation on which the popular bitcoin platform is built on and is a technology that efficiently organizes and secures data so that it can ultimately reduce cost, enhance portability of data stored, minimize data duplication, and improve execution and the overall complexity of transactions. For example, one of the greatest obstacles in migrating services online is the ability to secure the data and verifies the identity of the users; for online authentication commonly relies on a password or the use of dual-factor authentication. This presents a problem because passwords are notoriously insecure and sometimes requires sending a code to a third party or a short message service (SMS) to the institution. However, the solution to this problem is blockchain. Blockchain may possibly be the enabling technology that transforms how transactions are recorded and transferred, without the complexity of requiring third-party attestations. Cloud computing has also been adopted within many financial institutions for its efficiency and availability. This capstone project will not only discuss the concept of blockchain technology within a financial institution and its security solutions (i.e., authentication, know-your-customer, anti-money-laundering) but blockchain technology adaption into the security of cloud computing. Keywords: Blockchain Technology, Economic Crime, Compliance Risk Management, Distributed Ledgers, Dr. Kyung-Seok Choo, Electric Wallet, Cloud Computing, Financial Crime and Compliance Management.

Table of Contents

List of Illustrative Materials

Introduction to Blockchain

Statement of Purpose

Operational solutions within the financial industry and banks (collectively, Banks or Institutions) are expanding towards non-physical channels by implementing solutions that are more dynamic in technology to fully reach, engage and retain customers through enhanced customer experiences. Many institutions continue to adopt new solutions to improve storage and simplify operations, which help foster the move away from physical channels and towards an enhanced digital environment. With the expansion or need of digital technology, institutions have been studying the use of blockchain for the secure use of electronic cash by communicating solely between peers to exclude the involvement of any third party (Stanley, 2016). With that said, the use of blockchain to facilitate the exchange of money is well established; for this was the original use of digital currencies such as Bitcoin. However, further opportunities exist for institutions to use blockchain technology to help enhance other services such as compliance functions and cloud computing. In addition, blockchain technology will provide enhanced security compared to storing all data within a central data warehouse (Stanley, 2016).

As the digital world continues to evolve, institutions will implement various anti-corruption measures to help fight against corruption or illicit activity. This project addressed what blockchain technology is, how it works, how it can be used as an effective way to resolve compliance, resolve anti-corruption issues and enhance overall security for cloud computing. This project will also touch on the current challenges of implementing blockchain technology and why it is more secure than dual factor authentication.

Blockchain Technology is Sufficient

As illustrated in Figure 1, blockchain technology is a database of information over a network of computers rather than located on a single, or multiple servers (Stanley, 2016).

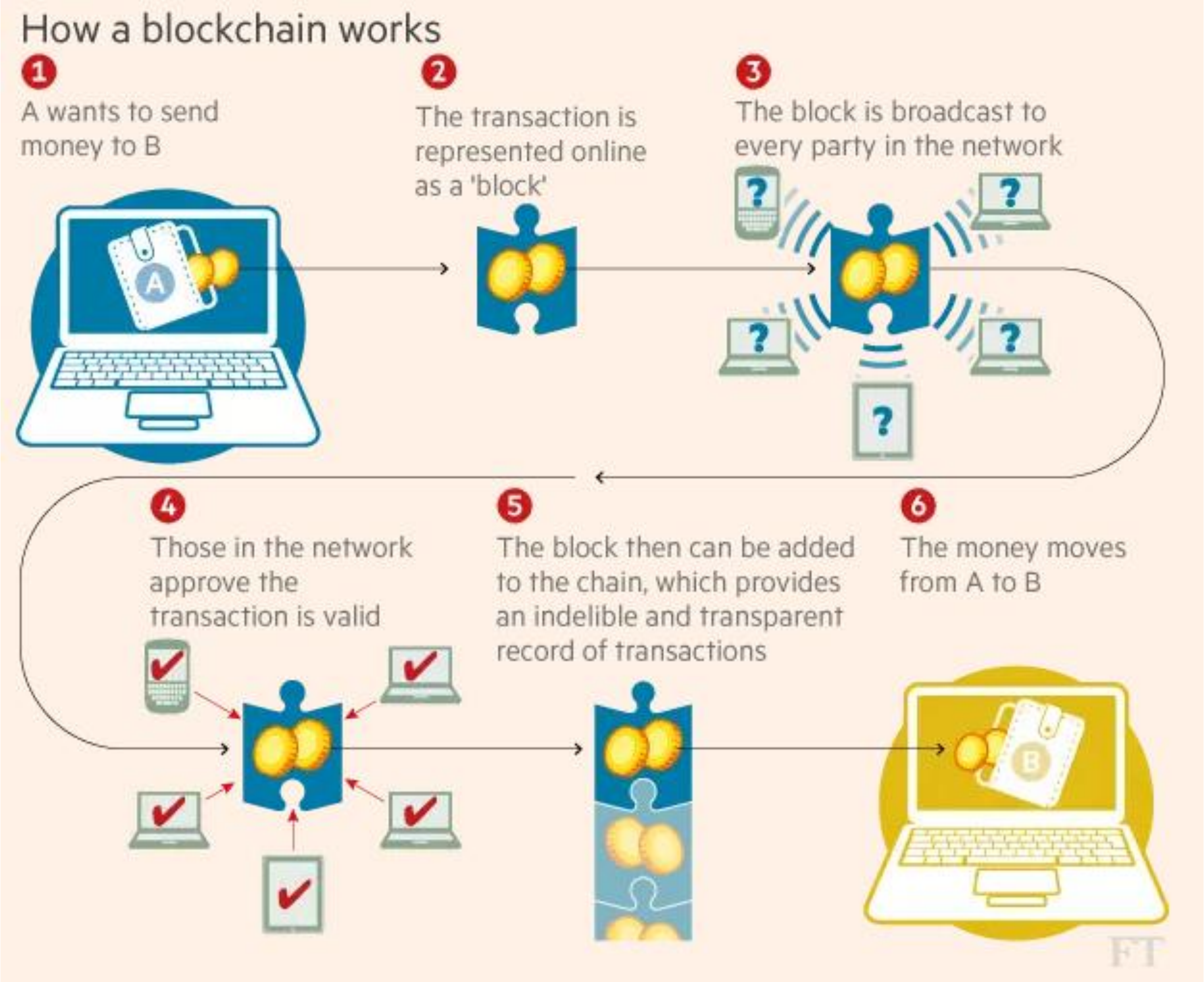

How a blockchain works
1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
A
B
FT

Figure 1. Validation of transaction utilizing blockchain technology (Stanley, Financial Times 2016)

Blockchain was developed as the foundational technology behind the Bitcoin cryptocurrency system. Although the total impact of blockchain is yet to be realized, for the financial market and other sectors are making significant investment into this technology. According to the World Economic Forum, more than 50 big-name banks are exploring the potential of blockchain with more than $1 billion in venture funding (Ulieru, 2016). Blockchain was first described in an October 2008 paper, attributed to Satoshi Nakamoto, which calls for the development of a cryptographically enabled currency that is independent from national monetary systems (Satoshi Nakamoto, 2008). Blockchain technology is an integral part of how cryptocurrencies, including Bitcoin, works. Blockchain is a data structure that makes it possible to create a digital ledger of transactions and share it with a distributed network of computers through cryptography, which allows each participant on the network to manipulate the ledger in a secure way without the need for a central authority (Yermack, 2017). Once a block of data is stored on the ledger, it is difficult to change or remove because it is stored across the blockchain network to ensure the security of the data elements. This makes it a decentralized ledger because it allows the data elements to be transferred from one person to another without any counterparty involvement. Since ownership of the transaction or data elements is through various people, hacking the data is very difficult because each hash stored in the block is affected by the values of the previous blocks (The Four Pillars, 2017). In addition, every record in the distributed ledger has a timestamp and unique cryptographic signature, thus making the ledger an auditable history of all transactions in the network (Wood, 2014). One implementation of distributed ledger technology is the open source Hyperledger Fabric blockchain (IBM Blockchain, 2017).

As illustrated by figure 2, blockchain is a distributed ledger that provides a way for information to be recorded and shared by a community and each member maintains his or her own copy of the information that must be validated for updates collectively (Blockchain, 2016). The information could represent transactions, contracts, assets, identities, or anything else that can be described in digital form. Once entered, they are permanent, transparent, and searchable, which a historical view of the transaction and each update is a new block added to the end of the chain (Blockchain, 2016). Protocols manage how the edits and/or entries are initiated, validated, recorded, and distributed. Figure 2 explains how blockchain works from initiation to completion of a (Blockchain, 2016).

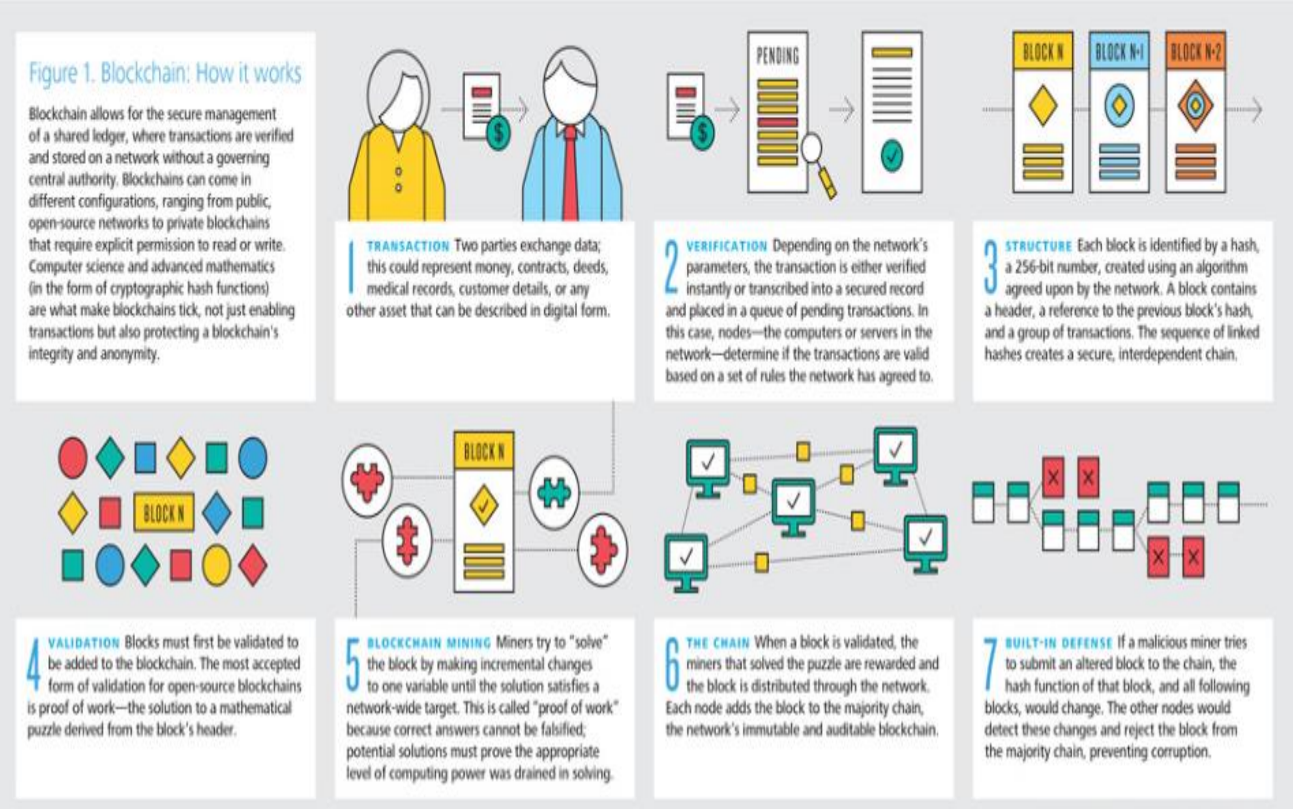


Figure 1. Blockchain: How it works

Blockchain allows for the secure management of a shared ledger, where transactions are verified and stored on a network without a governing central authority. Blockchains can come in different configurations, ranging from public, open-source networks to private blockchains that require explicit permission to read or write. Computer science and advanced mathematics (in the form of cryptographic hash functions) are what make blockchains tick, not just enabling transactions but also protecting a blockchain's integrity and anonymity.

1 TRANSACTION Two parties exchange data; this could represent money, contracts, deeds, medical records, customer details, or any other asset that can be described in digital form.

2 VERIFICATION Depending on the network's parameters, the transaction is either verified instantly or transcribed into a secured record and placed in a queue of pending transactions. In this case, nodes—the computers or servers in the network—determine if the transactions are valid based on a set of rules the network has agreed to.

3 STRUCTURE Each block is identified by a hash, a 256-bit number, created using an algorithm agreed upon by the network. A block contains a header, a reference to the previous block's hash, and a group of transactions. The sequence of linked hashes creates a secure, interdependent chain.

4 VALIDATION Blocks must first be validated to be added to the blockchain. The most accepted form of validation for open-source blockchains is proof of work—the solution to a mathematical puzzle derived from the block's header.

5 BLOCKCHAIN MINING Miners try to "solve" the block by making incremental changes to one variable until the solution satisfies a network-wide target. This is called "proof of work" because correct answers cannot be falsified; potential solutions must prove the appropriate level of computing power was drained in solving.

6 THE CHAIN When a block is validated, the miners that solved the puzzle are rewarded and the block is distributed through the network. Each node adds the block to the majority chain, the network's immutable and auditable blockchain.

7 BUILT-IN DEFENSE If a malicious miner tries to submit an altered block to the chain, the hash function of that block, and all following blocks, would change. The other nodes would detect these changes and reject the block from the majority chain, preventing corruption.

Figure 2. Process flow of the blockchain technology (Blockchain, 2016).

The lifecycle of a transaction using a blockchain is that "Person A" creates a transaction that is digitally signed, which is then sent to a miner who verifies the validity of the transaction and endorses it (Blockchain, 2016). Once validated, the miner will broadcast the transaction as a block to all the connected nodes within that blockchain (Blockchain, 2016). The nodes accept this block only if all transactions are verified as valid transactions and each new block is coupled with the previous transaction (Blockchain, 2016). That is why if something is changed, the blockchain becomes invalid at that point of the change and the error is broadcasted to all the nodes within the established blockchain (Blockchain, 2016). This is what makes blockchain a preferred platform for financial institutions because of its ability to restrict access and reduce the likelihood of cyber attacks.

Challenges of Blockchain Technology

While blockchain is efficient with respect to transactions, concerns do exist over the security of these transactions. Since as early as 2014, cyber criminals have targeted exchanges and companies by utilizing the blockchain and digital currencies which can be hacked like any other platform or protocol (WiecZner, 2017). For example, if the bitcoin and private keys are saved on an internet connected device, they may be stolen. Once these private keys are stolen, it does not matter how secure the architecture is or how encryption features are established. Incidents like this have occurred over the past year, include, the Bitfinex attack in August 2016 in which $65 million was lost and the Ethereum attack in June 2016 in which $150 million was lost (Can the Blockchain, 2016). For example, Fujacks Trojan has successfully proven that it can remotely control infected computers that are nodes in a blockchain, collect information, and install other malware or tools into the blockchain (The fright factor of blockchain, 2017). Another security challenge with blockchain is that fraudulent transactions can be authenticated (The fright factor of blockchain, 2017). For example, a fake bank can approve false Know Your Customer (KYC) documents and create a blockchain that financial institutions start authenticating over time, which ultimately makes the false KYC documents valid (The fright factor of blockchain, 2017). This is also one of the primary reasons a black market for bitcoins exists. This is also why financial institutions have concerns about the confidentiality of transactions, securing private keys and the strength of cryptographic algorithms used in blockchain transactions; for any blockchain transaction is dependent on trust between two or more counterparties. Most people use bitcoins at exchanges and trust the exchange will look after them. However, many money exchange firms are not fully regulated entities and cannot offer assurance on the transfer of digital currencies. However, Bitcoin is set to be given the same financial safeguards as traditional assets. The U.S. Commodity Futures Trading Commission has granted LedgerX, a cryptocurrency trading platform operator, approval to become the first federally regulated digital currency options exchange and clearinghouse in the U.S. (England, 2017).

Concerns with Two-Factor Authentication

There are very few options currently used for two-factor authentication that has relatively wide spread adoption techniques, which posed various other security threats. For example, one of the most common two-factor techniques is sending an SMS message which is notoriously insecure because a potential attacker can sniff these messages and spoof the sender of the message (LedgerX and CBOE, 2017). This poses a problem because if an attacker knows that an account uses text messages as a backup method of authentication and your name, the attacker could intercept the messages and gain access of the codes sent. This option also exposes the issue of a single entity owning the authentication data; for authentication codes can be easily leaked. However as noted above, the decentralized approach offered by blockchain eliminates this problem because the chain is 100% open to the public and no sensitive data is stored in the open on the blockchain (The Four Pillars, 2017).

Criminals targeting Bitcoin services were finding ways around the extra security, either by intercepting software tokens or more elaborate account-recovery schemes (Shanmugam, 2017). In many cases, attackers went after phone carrier accounts directly because of its weak points, by setting up call-forwarding arrangements to intercept codes in transit, which continues to be a real issue for Bitcoin users. Outside of Bitcoin, it’s become clear that most two-factor systems don’t stand up against sophisticated users (Brandom, 2017).

Concerns with Storing Data in a Central Database or Data Warehouse

Another main challenge facing many financial institutions today is the growth of fraud and cyber-attacks. Traditionally, bank ledgers (defined as general ledgers, transaction history and/or audit trail/debits and credits) for accounts have been created within a centralized database. This model has been more susceptible to hackers and cyber-attacks as all the information is located in one place and usually secured behind outdated legacy IT systems. Hackers and cyber-criminals are well aware of evolving digital technology and have been able to bypass these security systems to commit data breaches and fraud.

As blockchain is decentralized, it is less prone to this type of fraud. By using blockchain, there would not only be real-time execution of the transaction, but also complete transparency that would enable real –time fraud analysis and prevention. In addition, for data warehousing, the blockchain has the potential to simplify and even eliminate the process of building history (Devlin, 2017). It is also known that blockchain clients allow for the development of distributed systems which do not rely on what traditional databases call “master-slave” clusters, which drastically increases the resiliency of blockchain networks as a data management solution (Finance, n.d.).

Proposed Solution is Blockchain

The use of blockchain-based systems is an indicator of the transparency and usability of blockchain. Though blockchain does have some problems from a security standpoint and other aspects, these problems are expected to be settled over time, especially with the arrival of more stable and secure blockchain platforms. Finally, it is apparent that blockchain technology is gradually becoming a secure platform. It has a cyberattack resilient database architecture supported by cryptography, immutability (resistance to tampering) and consensus principles (meaning there is no need for a central or trusted authority to keep the data or supervise the transaction since each node has a copy of the entire database), which are the key ingredients for the effective implementation of information security in an organization.

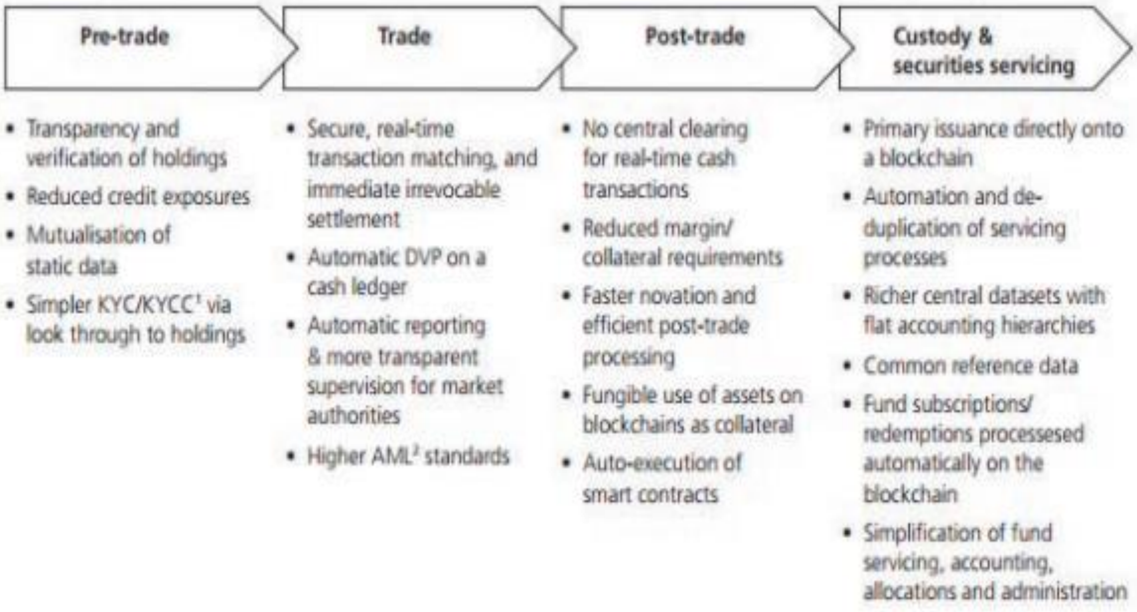
As blockchain has done away with the server to exclude the involvement of the central authority and has facilitated transactions through the participants who jointly store the transaction records and, finally, approve the transactions using peer to peer or P2P (computer systems that communicate to each other through a network without passing through a central server) network technology. The blockchain has a distributed structure and utilizes the peer network and the computing resources of peers. Technical measures such as proof of work and proof of stack (PoS concept states that the person can mine or validate block transactions according to how many coins they hold) have been implemented to improve the security of blockchain. In addition, the anonymity of user information should be ensured when using blockchain in the cloud computing environment and the user information should be completely deleted when removing the service (Liang, 2017).

Again, as the digital world continues to evolve and institutions implement various anti-corruption measures to fight against corruption or illicit activity; blockchain technology will be a key ingredient to resolve compliance concerns, resolve anti-corruption issues and enhance overall security for cloud computing. This project will not only touch on the challenges of implementing blockchain technology, but provide strong support on why it is more secure than dual factor authentication and how it can continue to pave the way for enhanced compliance, improved security and better overall efficiency.

Literature Review

Institutions will continue to implement various anti-corruption measures to help fight against corruption; this project will review what blockchain technology is, how it works, how it can be used as an effective way to resolve compliance and anti-corruption issues as well as enhance overall security for cloud computing. This project will also touch on the current challenges of implementing blockchain technology and why it is more secure than dual factor authentication. As noted earlier, blockchain is a distributed database that maintains a list of records called blocks that are secured from tampering to maintain data integrity. Each block contains a time stamp that is linked to the previous block, and each blockchain consists of blocks that hold batches of valid and approved transactions. These blocks include the hash of prior blocks in the blockchain that link them together. The linked blocks form a chain, which is called a blockchain (The Four Pillars, 2017). This enables institutions or banks to ensure traceability of a given transaction, which enhances security. The architecture of the blockchain even helps to identify error or possible fraud within a given transaction and then corrects it immediately. Once these errors are identified, access is restricted to further reduce the likelihood of a cyberattack. Blockchain technology is a great platform to provide added security to any institution or bank. In addition, the data is not reversible once it is stored within the blockchain, maintains a single source of the truth to further enhance data integrity concerns (The Four Pillars, 2017). As a result, blockchain technology is an asset for institutions to help maintain regulatory compliance by providing readily accessible data and secured information sharing capabilities.

Some of the many economics that enable the development and sustainability of blockchain technology is produced by: (1) the increase in processing speed; and (2) the steep drop in cost of data storage. As noted throughout this project, blockchain can bring various benefits by enabling such things as smart contracts; digital rights management; enhanced business models for the Internet of Things (IoT); enhanced security and protecting personal data; digital content distribution; voting; and/or reputation system enhancement (Trautman, 2016). Blockchain technology has the potential to disrupt the financial industry by facilitating global money remittance, smart contracts, automated banking ledgers and digital assets. In addition, Blockchain technology can even find applications within areas of transaction processing, cash management, ledger administration and even the clearing and settlement of financial assets (Trautman, 2016). For example, Figure 3 clearly illustrates how blockchain technology can bring a positive change to the structure of capital markets because it can bring benefits across the pre-trading/due diligence front, the trade, post-trade and securities servicing (Trautman, 2016).



Pre-trade

- Transparency and verification of holdings
- Reduced credit exposures
- Mutualisation of static data
- Simpler KYC/KYCC[1] via look through to holdings

Trade

- Secure, real-time transaction matching, and immediate irrevocable settlement
- Automatic DVP on a cash ledger
- Automatic reporting & more transparent supervision for market authorities
- Higher AML[2] standards

Post-trade

- No central clearing for real-time cash transactions
- Reduced margin/ collateral requirements
- Faster novation and efficient post-trade processing
- Fungible use of assets on blockchains as collateral
- Auto-execution of smart contracts

Custody & securities servicing

- Primary issuance directly onto a blockchain
- Automation and de-duplication of servicing processes
- Richer central datasets with flat accounting hierarchies
- Common reference data
- Fund subscriptions/ redemptions processesed automatically on the blockchain
- Simplification of fund servicing, accounting, allocations and administration

Figure 3. Benefits of Blockchain Adoption (Trautman, 2016).

Applying the Blockchain for Authentication and Identification

As the pressure continues for financial institutions to reduce costs, the global efforts and expense to prevent money laundering and financial terrorism keep increasing. In addition to the financial burden, KYC requests can further delay the efficiency of transactions (Identity Management on the Blockchain, n.d.). While the use of distributed ledger systems, such as blockchain, could automate processes and further reduce compliance costs and errors. Blockchain would not only remove the duplication of efforts in carrying out KYC efforts, but it would also enable encrypted updates to clients details to be distributed to all financial institutions on a real-time basis. The ledger would even provide a historical record of all documents shared and compliance activities performed for the specific client. This would ultimately provide evidence or an audit trail that the institution has acted in accordance with required regulations. With that said, blockchain can be used to help identify entities attempting to create fraudulent histories (Advertising Trade Group, 2017). Given the current expectations for financial institutions to increase their use of blockchain applications in areas like transaction settlements and payment processing, the use of a common ledger for KYC purposes might offer an even greater opportunity to link institutions to strictly enforce compliance.

As financial institutions have started to harness the potential of blockchain technology and develop a variety of services using the technology, the center of blockchain authentication would be a blockchain identity verification process for compliance and Know Your Customer (KYC) purposes. For example, this ledger data can essentially provide a block of data on the chain that can be both verified by any third party and display the necessary information such as date of birth. The secret to this verification process is the ECDSA (elliptic curve digital signature algorithm) (The Fundamentals of an ECDSA Authentication System., n.d.). Then, when adding an ID to the blockchain, an identification issuing service binds a public key by default and then transfers ownership of the private key to the user, which allows the user to sign a signature that can be verified against the public key stored within the blockchain (The Fundamentals of an

ECDSA Authentication System., n.d.). This identification process would serve as a decentralized source of authentication and would essentially be a single-sign-on portal that can be accessed by anyone, but not being owned by any single entity. The application would then verify that the signature is valid and that the user's ID verifies who they say they are (The Fundamentals of an ECDSA Authentication System., n.d.). This could ultimately help institutions maintain compliance of current regulatory statutes for customer privacy concerns and support the needs of state and federal law enforcement at the time of an investigation or even prosecution of identity theft. The encrypted data can then be stored locally on an input device for additional security and can only be accessed with the private key of the user on the input device. As institutions are limited in the activity they can view of their consumers, transaction visibility ends with its consumer base and source systems. As financial institutions are not always privileged to information that law enforcement obtains and real time information is not always funneled timely to the financial institutions without execution of a 314(b). Authorities are also unable to see systemic vulnerabilities across institutions on a real-time basis and it is difficult for financial institutions to monitor and respond to systemic vulnerabilities with the lack of information being disseminated to them. Attempts to help facilitate a broader information sharing process, such as through Section 314(b) of the USA Patriot Act, which permits financial institutions to share information under certain criteria, are intended to break these barriers (Whitehead, 2001). Blockchain provides a proactive and real-time response to information sharing and even fraud identification; for many times it is difficult for institutions to respond to law enforcement or take a proactive stance against illicit activity because institutions are not always provided information that law enforcement agencies obtain unless a 314 (b) is executed (Information Sharing-Overview, n.d.). However, this can be solved through the implementation of blockchain, as blockchain is a database of information distributed over a network of computers rather than located on a single or multiple servers. The use of distributed ledger system could provide historical records of all documents shared and compliance activities performed on a specific customer. This means that institutions and law enforcement agencies would then go directly to the blockchain rather than relying on a third party to conduct a KYC or AML analysis of transactional history. As the data stored on the blockchain is irreversible and it would provide a single source of truth that would minimizing the length of the investigation and risk of duplication or even error.

Blockchain technology and identity management are critical as the internet continues to evolve: for institutions face various identity management challenges since the start of the Internet. As the U.S. Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) laws (including customer information requirements) have been established to help distinguish one’s personal identity in the form of a legalized document, such as a driver’s license or even a passport, there is no system for securing online authentication of our personal identities or the identity of digital document. However, blockchain technology can offer a way to correct this problem by delivering a secure solution, without the need for a trust or a centralized authority. Blockchain can be used to create an identity on the blockchain, which can make it easier to manage by giving institutions and/or individual’s greater control over their personal information (PII) and how it can be accessed. Combining the decentralized blockchain principle with an identity verification process, a digital identification can be created to act as a digital watermark that is assigned to each transaction. This enhancement would help institutions check the identity of an individual on every transaction in real time, which would eliminate the overall rate of fraud. The implementation of blockchain technology, institutions and/or individuals would have the ability to login and verify a payment transaction without having to enter any of the traditional username and password information: for the blockchain solution would allow an institution or individual to use a simple application to authentication the transaction. The solution will also store their encrypted identity, allowing them to share their data with other institutions/individuals and manage it on their own terms (Jacobovitz, 2016).

Secure Blockchain Solutions in Cloud Computing

As noted earlier, if a user’s data is disclosed in the cloud computing environment, monetary and emotional damages can occur due to the leak of a user’s sensitive information. The security of saving and transmitting data, such as confidentiality and integrity, in the cloud computing environment is mainly studied and found not to be sufficient (Subashini, 2011). However, as noted throughout, blockchain is a representative technology for ensuring anonymity, and if combined with the cloud computing environment, blockchain can be even more beneficial to financial institutions. An electronic wallet is installed when using the blockchain technology, but if the electronic wallet is not properly deleted the user's information can be left behind (Cooper, 2017). Such as with anything that is built on blockchain technology, digital wallets come with both public and private keys and are essentially the digital address of a client’s wallet and the password to get into it (Cooper, 2017). This is also one of the biggest problems for mainstream adoption because people are used to losing their passwords or their keys. In addition, people sometimes forget their password and ask the financial institutions to supply it back to them; you do not have that option with a private key (Cooper, 2017). If you lose them, you lose your money: for the money will be in that address and you will not have access to it (Cooper, 2017). As our technical environment continues to change, the systems that support it will also need to adapt. Recent data hacks such as Target reveal the dangers of a highly network/capable world in which our data is gathered and held in poorly-secured data warehouses/repositories. The initial intrusion into Target's operating systems was traced back to network credentials that were stolen from a third party vendor contracted by the company. The vendor was a refrigeration, heating and air conditioning (HVAC) subcontractor that worked at a number of Target locations. Target ultimately gave the HVAC vendor external network access, to its payment system network (McMullen, 2016). The credit card information was taken by point-of-sale malware devices that were uploaded to a number of cash registers within the Target stores. Target indicated that the data breach exposed approximately 40 million debit and credit card accounts between November 27 and December 15, 2013 (Weiss, 2015).

Blockchain is a combination of a database and a peer-to-peer network, and the security of a blockchain network can be open or closed/private. Transactions are recorded into the blockchain and attached to the entity in the form of a ledger thereby preserving a complete history for that entity. All participants within the blockchain witness the transaction and everything is replicated across all servers within the network so there are no single points of failure. To hack one server would require a synchronized coordinated attack on the majority of other servers within the network. The data object can be protected at the object level, or at the properties or sub-objects level. This means that for any given object, different actors may have a responsibility for a different aspect of an object throughout its lifecycle. As all records and transactions are replicated to servers throughout the network which avoids single points of failure while also maintaining transparency of activity; further, all other servers within the network are validating the same transactions which can be accepted or rejected to help detect and/or prevent fraud. Second, each transaction receives a hash which is a digital receipt and is used to verify that a transaction record has not been tampered with. Each transaction is linked to the previous transaction using the same hashing technology which means that if any single transaction is modified then the entire ledger is broken. Other methods for security also exist and can be activated to help facilitate credible reviews of transactions by multiple parties to confirm the legitimacy of the transaction. These functions, when combined, ultimately harden the system significantly from hacker attempts and theft. Within blockchain technology, transaction records are permanent and cannot be modified and/or removed. If a mistake is made, it must be corrected by creating a new record to make the correction, which ultimately preserves the complete and full transaction history.

Benefits of Proposed Technology from Central Data Warehouse

As institutions are continuously challenged with maintaining historical data because various systems have limited audit trail capabilities and operate in fire-and-forget mode (Devlin, 2017). As a result, the need to build a historical record remains a key priority for many institutions. The urgency for a truly permanent record of the ever-changing customer environment and to track more aspects of physical, personal, business, and societal activities/ behavior is becoming even more dependent on the computing environment. On the operational front, which drove institutions to build a data warehouse for historical information, blockchain technology is finally bringing institutions the concept of a permanent data record. Being a secure transaction ledger database shared by all parties within the distributed network, a blockchain records and stores every transaction that occurs in that network in a public and unchanging manner (Devlin, 2017). Therefore, blockchain technology can eliminate the use of various third parties in a wide range of industries from finance and legal services to real estate and collateral management. For data warehousing, the blockchain has the potential to simplify and/or eliminate the process of building historical data. It has also done away with the need for a data warehouse server to exclude and/or execute the involvement of the central authority: for it facilitates transactions through the participants who jointly store the transaction records and approves the transactions.

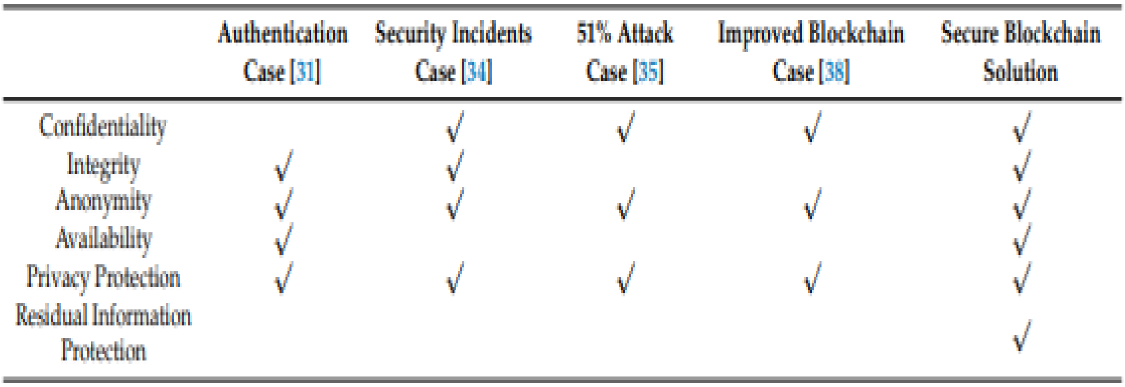
Blockchain records are distributed over the network in a distributed ledger rather than a central database. Consequently, recorded blockchain transactions are simply absolute: for the data of past transactions cannot be changed (only updated) and the data on previous transactions remains permanently available for data integrity and full transparency. The structure makes it vertically impossible to create two conflicting entries into a blockchain. As the blockchain technology provides certainty that every update in the system is valid, the technology ensures that there is an agreement with defined rules to execute the transaction. The reason that makes the use of blockchain revolutionary is simply the lack of a central administrator. For example, if the contents of any given database are stored in the physical memory of a particular system or data warehouse, anyone who has access to it could potentially corrupt the data within. With blockchain, there is no need for a central administrator or a central data warehouse because it was eliminated by cryptography. In addition, each user or institution can be in control of all their information and/or transaction.

One of the biggest problems of bitcoin using blockchain technology is the possibility of a double transaction, which is that act of sending the bitcoin to two or more accounts for malicious purposes. Some of the mechanisms used for preventing fraud from happening are “total currency” and “longest chain wins” (Park, 2017). Park (2017) defines the total currency mechanism as a function that will terminate the transaction if the total currency value exceeds a given value or by double transaction. The article also illustrates that longest chain with the most work will always win (Park, 2017).

> For example, if a user double-spends a bitcoin and the transaction details are sent to two different peers, two blocks will be ultimately be generated and the peers will generate the next blocks using two blocks in competition. As a result, the chain that loses in the competition is naturally eliminated and the longer chain wins addressing the double spending problem. Blockchain is a technology for ensuring anonymity and if combined with a cloud computing environment, blockchain would be a service that provides even stronger security. As the users anonymity will be ensured if the blockchain method is used when saving the users information in the cloud (Park, 2017).

If a user's data is disclosed in a cloud computing environment, monetary damages may occur due to a leak of users' sensitive and/or personal information. Blockchain is a technology for ensuring anonymity and if combined within an adequate cloud computing environment. As a result, blockchain technology will provide enhanced security; for when an electronic wallet is installed. However, the user must ensure that the electronic wallet properly deleted and not left behind (Park, 2017). An electronic wallet is a software program or encrypted storage medium holding financial information that can be used to complete electronic transactions without re-entering the stored data. These private keys are saved in the wallet of the person who owns the balance and the wallet is basically the equivalent of a bank account. The blockchain method is used to remove the information by sending a finished message; for a leak of a user's information can only be prevented when the electronic wallet is completely removed or deleted. This process will also ensure the user's anonymity and overall privacy protection.

In figure 4 noted below, Park further compares the aforementioned method with various other case studies in terms of confidentiality, integrity, anonymity, privacy protection, and residual information protection. The case analysis consists of confidentiality checks if the information is leaked to unauthorized individual, whereas integrity checks are used if the data in the transaction is altered or falsified without authorization during transfer and/or storage. While anonymity will ultimately assure that the individual involved in a transaction is not identifiable. Finally, privacy protection is given to protect the personal information of the parties participating in the transaction, whereas residual information protection checks the safe removal of user data at the time of termination and/or program removal (Park, 2017).



	Authentication Case [31]	Security Incidents Case [34]	51% Attack Case [35]	Improved Blockchain Case [38]	Secure Blockchain Solution
Confidentiality		√	√	√	√
Integrity	√	√			√
Anonymity	√	√	√	√	√
Availability	√				√
Privacy Protection	√	√	√	√	√
Residual Information Protection					√

Figure 4. Comparison of related studies (Park, 2017).

The two-factor authentication case was found to not provide integrity since it has the possibility of leaking the key by hacking the personal key to attack the blockchain. It was also found to not provide residual information protection because it does not verify the complete removal of the electronic wallet. Park also illustrated that the security incidents case did not provide availability since the service became unavailable because of infection by malware and does not provide residual information; for it does not verify the complete removal of the electronic wallet. Next, was the 51% attack case that provided an analysis of two phase proof of work in Bitcoin. This case was found to have problems of infringement of integrity with the transaction ledger and unavailability following an attack that alters 51% of the transaction ledger (Cermeño, 2016). It also did not provide any residual information protection since it does not verify the complete removal of an electronic wallet. The double spending case analysis on improved blockchain was found to neither assure integrity nor provide availability since the vulnerability of double transaction still remained a possibility. In addition, it does not provide residual information protection. However, the aforementioned secure blockchain solution improves security by providing residual information protection since it encrypts the data using a public key and verifies the complete removal of the electronic wallet (Park, 2017).

Revolutionize Regulatory Compliance and Continued Challenges

As stated throughout this project, Blockchain continues to be an ongoing challenge within financial services and the capital markets industry: for the technology has the potential to transform business processes, making the data used in these enhanced processes more available, transparent, immediate and secure. Blockchain technology could also minimize cost, transaction delays and error handling/rework. Some of the many uses include trade reporting; clearing, confirmation, validation and settlement; recordkeeping; monitoring and surveillance; risk management; audit; management and financial accounting; and regulatory compliance, which includes financial crime prevention. The transparency of information captured within a blockchain means that all the necessary data can be recorded in shared ledgers and made available on a real-time basis (Peters, 2016). As a result, stakeholders will no longer be simple recipients of ad-hoc reports, but part of the solution and a real-time process. What makes blockchain unique is its cryptographically assured immutability (Herlihy, 2016). For example, when transactions on the ledger are grouped into blocks and written to the database, they are accompanied by cryptographic verification, which makes it fundamentally impossible to alter the state of the defined ledger. As blockchain is a trusted technology and changes in the data are recorded into the blockchain, then, the transaction can only be completed as all the network participants agree that a transaction is legitimate and in accordance with shared protocols and/or rules. As a result, the interest in blockchain continues to evolve and will only continue to grow as more defined solutions make their way to the marketplace. As noted above, one of the greatest benefits of blockchain from a compliance perspective is its practical immutability; for once the data has been saved into the chain, it cannot be changed, altered and/or deleted. This is the same practice that makes blockchain a great solution for the transfer of digital assets. The immutability of blockchain lends itself as the application of proof-of-process for compliance; for it can also be used to keep track of the steps that are required for specific regulation. Recording actions and their outputs in a blockchain would create the perfect audit trail for any regulatory agency, internal and/or external parties to verify compliance. This would provide the examining parties a real-time view of the blockchain of any given financial organization. This would allow them to play a more proactive role and analyze information in real-time mode. This change would ultimately reduce the time, effort and cost that an institution could spend on regulatory reporting, examinations as well as improving overall data quality and consumer confidence.

As briefly discussed earlier, another field where blockchain could play a pivotal role in enhancing is to know your customer (KYC) and anti-money laundering (AML) requirements. Institutions must complete many rigorous tasks as a part of a client onboarding process, which includes data collection, customer validation, and relationship identification. Many of the needed requirements could ultimately be eliminated if the information existed already in a secure and unchangeable, tamper-resistant database. Also, changes that are needed to a customer's data will automatically be distributed to all participants within the blockchain. As blockchain can play the role of proof-of-process, so all the steps are easily traceable within the network, and the regulators can be confident about the validity of the information. Also, all parties involved would essentially be co-custodians of the information within the blockchain, which would provide additional protection against identity theft. Blockchain technology would eventually build a greater trust amongst institutions as the sharing of sensitive information via blockchain becomes the norm. For example, as the expansion of Society for Worldwide Interbank Financial

Telecommunications (SWIFT) will continue to evolve as a trusted KYC registry the more financial institutions participate. SWIFT technology is a messaging network that financial institutions use to securely transmit information and/or instructions through a standardized system of codes. Its success is attributed to how it continually adds new message codes to transmit different financial transactions. SWIFT is now one of the early steps to a fully trusted digital identity within the financial industry. SWIFT enables banks to use electronic mode to transfer international payments, statements and other banking messages (King, 2010).

While many regulatory agencies have touted the potential benefits of blockchain technology, some have even expressed concerns of the possible impact it would have on financial stability and overall market integrity. An article stated that the Financial Stability Oversight Council (FSOC), a group of U.S. regulators that includes the Securities and Exchange Commission (SEC) and the Treasury Department, warned that blockchain technology poses a great risk and uncertainty to market participants (Kakavand, 2016). However, according to the same article, these and other U.S. regulatory agencies have also individually discussed the benefits of blockchain (nascent) technology (Kakavand, 2016).

The SEC’s Commissioner Stein has also cautioned that as the market embraces blockchain technology, the regulators must be in a position to lead and/or harness its benefits and respond quickly to any potential identified weaknesses (Kakavand, 2016). The SEC has also embraced the early adoption of blockchain as it relates to securities offerings.

Financial Crimes Enforcement Network (FinCEN) is another U.S. regulatory agency that has issued administrative rulings and guidance related to virtual currencies and blockchain technology. In March 2013, FinCEN issued guidance clarifying the applicability of BSA regulations to individuals creating, obtaining, distributing, exchanging, accepting, and/or transmitting virtual currencies (Kakavand, 2016). The ruling requires that an administrator or exchanger of a virtual currency is must register as a money service business (MSB) under FinCEN's regulations (Kakavand, 2016). FinCEN the further elaborated on this guidance in two administrative rulings, which established the BSA's definition of a money transmitter that includes neither users who create virtual currency for their own purposes, nor companies purchasing and selling convertible virtual currency as an investment exclusively for their own benefit (Kakavand, 2016). The Office of the Comptroller of the Currency (OCC) also warned that virtual currencies enable anonymity for cyber criminals, including terrorists and other groups seeking to transfer and launder money globally (Blemus, 2017). This, in turn, can create significant challenges for BSA and antimony laundering compliance (Kakavand, 2016). As financial technology continues to evolve and institutions begin to develop and/or implement smart technologies such as blockchain or smart contracts, the regulators will also need to further enhance the examination approach to ensure transaction security consumer confidence and the reduction in the risk of manipulation.

Establishing and managing the infrastructure to support blockchain technology is another challenge many institutions are experimenting with the advanced technology. As information security, operations, cloud and overall system architecture start to introduce blockchain as a new data or code layer in their institution, the process to implement and/or manage change can be disruptive because there are currently no best practices available to streamline the roll-out process (Kakavand, 2016). This will be a continued challenge for all institutions as the process continues to evolve.

In summary, blockchain technology has the potential to revolutionize and improve many business processes within the financial services industry. Of the many processes that could be improved by blockchain technology, it is regulatory processes such as KYC and financial crime prevention (e.g., AML) that may be early converts. The blockchain solution is continuing to emerge, which is enabled by new technologies and the recognition that the industry needs to establish a sustainable and secure process. Though blockchain does have some problems from a security standpoint, these problems are expected to settle over time, especially as blockchain becomes a more stable, secure and resilient platform. That coupled with a database architecture that is supported by cryptography, immutability and consensus principles, are the key ingredients for the effective implementation of information security in any organization.

Discussion of Findings

This section of the capstone project will critically reflect on the goals of blockchain, compare these goals with the results of the work performed throughout this project and discuss any implications or challenges identified as a result of this project. First, this projected reviewed some of the proposed theories/applications, core concepts and principles of maintaining the enhanced security of blockchain technology. Afterwards, we will discuss some of the downsides and/or weaknesses of the technology and some of the lessons-learned throughout this capstone project.

As discussed earlier, operational solutions within the financial sector and/or banks have been expanding in an effort implement more dynamic channels to further drive efficiency, security and improve the overall customer experience to become fully engaged. Institutions also continuously look to move away from manual processes to further improve data storage capabilities and simplify processes geared at fostering a new digital environment. With this drive for expansion, institutions will continue to studying and/or implement the use of blockchain for a secure use of electronic cash by communicating solely between peers to exclude the involvement of any third parties (Stanley, 2016). With that said, the use of blockchain to facilitate the exchange of money is well established; for this was the original use of digital currencies such as Bitcoin. However, further opportunities exist for institutions to use blockchain technology to help enhance other services such as compliance functions, cloud computing and the future vision of the internet to enhance overall business intelligence. In addition, blockchain technology will provide advanced security compared to typical data warehouse functionalities (Stanley, 2016).

As discussed within this project, blockchain technology is no longer just a hypothetical process, but it is an implemented and proven enhancement. As the implementation of blockchain continues to evolve, it will continue to move from an institution's expectation to an actual reality. However, there will always be some degree of inefficiencies and challenges along the way as the human element will continue to exist in some way. As this digital world continues to evolve, institutions must look to enhance anti-corruption measures to fight against corruption and illicit activity. As discussed throughout this project, blockchain technology is an effective answer to resolve anti-corruption issues and improve overall security for cloud computing.

Institutions can no longer just rely on their reputation and continue with business as in the past. Consumer demands and the need to continuously improve a customer's experience must be at the forefront of every institution. To enable sustained growth, institutions must adapt quickly and change through the implementation of enhanced technologies. This puts institutions in a hard situation because the pace of change is rapid and the digitalization or interconnection of the world is evolving like never before. To be relevant, institutions can no longer wait for the technology to prove its capabilities or net worth. Institutions must stay at the forefront of technology and continue to make strategic investments to be relevant. As noted through this project, collaboration has been noted amongst many of the world's largest financial institutions.

This collaboration has been focused on creating a standardization of a blockchain based system. However, one of the challenges of enhanced digitalization is the cost for development and implementation. Another obstacle of implementing blockchain is earning the trust of the general public to truly expand and change the financial market in a fundamental way, which stems from the unwillingness of the institutions to invest, train and lead positive change.

The Concept of Blockchain

Blockchain is the foundation on which the popular bitcoin platform is built on and is a technology that efficiently organizes and secures data so that it can ultimately reduce cost, enhance portability of data stored, minimize data duplication, and improve execution and the overall complexity of transactions. This project also briefly explained a peer-to-peer version of electronic cash, one that allows online payments to be sent directly from one party to another without going through a financial institution or independent third party. Blockchain is the name of the technology that makes this possible. A blockchain is essentially a distributed database of records and/or a public ledger of all transactions or executed digital events that are shared among all related parties across peer network.

This project explains that blockchain has the following fundamental features: 1) blockchain is a public ledger; it is encrypted and it is trusted. Given blockchain resides on a network, it is public and anyone can view or access it at any given time. As a result, it is a distributed ledger with no single institution being charged with maintaining the records. 2) Blockchain technology enables a complete bypass of third-party actors in transactional relationships, thus creating advantages in cost and efficiency. 3) Blockchain also guarantees security through the use of encryption that involves both public and private keys. This allows individuals who do not know or even have trust in each other to form a trustworthy ledger. All information such as property rights and virtual currency transactions can be stored within the blockchain. Given the information is available to everyone and tamperproof, it allows the blockchain to be a transparent and preserves the truth. These blocks are linked to each other (like a chain) in linear, chronological order, with every block containing the hash of the previous block. The participants together enhance and continue the blockchain by complying strict rules and a general agreement, which means that the participants agree on how the chain should be updated. Integrity is encoded into every step of the process and distributed, not vested.

As noted earlier within this project, the technology functions via a peer-to-peer network that is based on specific logic or thousands of nodes, which can come and go as they please. New blocks are created by a process called mining, which takes several steps to accomplish and ultimately confirm. In currency transactions, these miners verify and supervise the transaction to ensure its integrity and that everything is in order. Each accepted transaction is maintained in order, which ultimately forms the chain. Every transaction has an identifying code, as a hash which contains the original piece of information of the transaction. The timestamp of each transaction then proves that the data existed at origination. The hash at each header is the identifying string of the newly mined blocks, which is ultimately part of the blockchain. We also learned that transactions could be postponed until a given amount of blocks have been mined. As blockchain continues to establish the new era of a digitalized economy, there are several principles that help create the business models and/or governance of blockchain, which include network integrity, distributed networks, incentives for alignment, added security, enhanced privacy and inclusion.

Challenges of Blockchain Technology

Even though blockchain technology is believed to pave the way and revolutionize the way of doing business, it will take time to fully implement this change as a standard business practice. It is also possible if blockchain technology is implemented worldwide, it may be challenging to support all services securely. Research also found that the creation of new blocks or the need for a transaction to be verified within a given blockchain may result in a negative impact to the work environment because the mining process will consume a vast majority of the energy. The more blockchain technology is used; the more energy is consumed. Therefore, a secondary use for the wasted energy and a more environmentally friendly mining process may be required as blockchain technology expands (The Economist, 2015).

This project has clearly expressed the excitement surrounding blockchain and the vast opportunities it offers for both financial and non-financial services. However, blockchain also has some drawbacks and work still must be done on the applications and implications of blockchain. Some of the challenges that commonly arise in relation to public blockchains are as follows:

First, is geared towards performance. When transactions are being processed a blockchain must perform the same tasks that a regular database could. However, it would also require three additional steps related to signature verification, consensus mechanisms and redundancy because every node in the network must be processed independently.

The second challenge that developers try to minimize is related to scalability, which is often raised in technical discussions of the bitcoin protocol because it is capped. The main obstacle with blockchain is scalability because it has a tendency toward centralization. As the blockchain continues to grow, the larger the requirement becomes for storage, bandwidth, and computational power that is spent by the nodes. This leads to a risk of higher centralization if the blockchain becomes too large and only a few of the nodes are able to process a block.

The last challenge is related to privacy. This project has illustrated that blockchain can preserve privacy through a public key, but it cannot guarantee transactional privacy since each value and/or balance of a transaction is publicly visible. This means that private data will be fully exposed through the flow of every node. However, the HD wallet fixed this concern because it allows users to protect their data by sending their payment in multiple transactions without requiring any coordination between the sender and the recipient. This gives users the option to control the data they are sharing with the system. Most Web services do not request the user's ID copy, but in order to do registration on the platform and become a member, one needs to share the name, email and other confidential data. Moreover, there is an absence of trust to the platforms, as there are no tools to trace on how the information is used. Privacy concerns can also be settled into the system architecture by changing the way of user's data is verified and was is required to do so.

In free and democratic societies, it is distilled into us that an individual's privacy is a basic human right, which should be respected. However, the internet is based on centralized solutions, which are collecting, analyzing and shared amongst users without notifying them of it. Additionally, information is stored on a centralized server, which has a greater probability to be hacked. In summary, this project identified two major privacy issues in collecting and using personal data without proper permission and inability of services to provide adequate security measures against centralized hacks.

The use of blockchain is going to fix the problems discussed above because it does not require confidential data to operate. Also, no email, name or any other personal information is collected. Hence, due to the blockchain structure, it allows and ensures privacy and anonymity of users. In addition, the identification and verification layers are completely divided from the transactional layer. During the process of transaction, there is no reference to a given identity, but there is a reference to authorization of the address and verification of the given transaction. The blockchain principle of privacy provides a new way of organizing the systems and reorganizes the way a personal identity is shared over the internet. Users receive the tools to realize their rights and the application of this principle is going to change the usage of data significantly in a way of enhanced transparency and integrity. It is a switch from big data to private data.

An important lesson learned throughout this project was that designing the blockchain is one of the first steps, but designing the interfaces to the real world is probably the most important. For example, if a blockchain is used and every single document is stored and validated, no one is able to manipulate the document. However, if one individual prints out the document, signs it and sends it back via mail, the second individual cannot trust the integrity of the document as it was possible to manipulate between exporting it from the blockchain and printing it. As a result, the security goal of data integrity was not fulfilled. The integrity of the blockchain was not violated, but it was circumvented by making the document mutual between two parties. This is a central problem discussed above, as one cannot prove the overall integrity of information which is not completely stored in a blockchain and retrieved directly from it. For that reason, one must carefully review the interfaces between the real world and the blockchain, as tampering may be possible. This project clearly illustrates that technical risks occurring throughout the life-cycle of a blockchain.

Based on this project, the two most common risks are related to scalability and missing regulations. The missing scalability is important because it prevents the platform from growing with a higher user demand that may lead to possible delays when interacting with the system. Missing regulations is also important because many legal questions still remain unanswered that could be preventing businesses from developing advanced solutions with blockchain technology. Meeting these challenges requires an agreement with the whole community involved. Only then can a thorough adoption of blockchain technology can be implemented. As this project specifies that a decentralized system based on a distributed ledger may be as trustworthy or even more trustworthy than a centralized. It was also clearly illustrated that blockchain technology could be successfully applied to information storage. There is still little knowledge of what blockchain technology will exactly enable, but it has great potential to transform how the economy works and how to disrupt industries that rely on trust. This project provided strong insight on how this new and disruptive technology can revolutionize and reshape the financial sector.

Blockchain technology can also create faith in the financial system. This is an important aspect especially from the perspective of financial institutions. When people trust in the financial markets, financial institutions can more efficiently concentrate on their main assignments, such as transferring resources from lenders to borrowers. This new technology has the ability to enhance overall efficiency and cut down on expenses. From an economic perspective, blockchain technology is all about minimizing waste and increasing assets within a company. In addition to reducing risks and expenses, blockchain technology can minimize errors along with fraud. In blockchain, fraud is not accepted and could enable a more trusted and secure system than the traditional banking system of today.

Blockchain has done away with the involvement of the central authority and has facilitated transactions through the participants who jointly store the transaction records and, finally, approve the transactions using P2P network technology. The blockchain has a distributed structure and utilizes the peer network and the computing resources of peers. Technical measures such as proof of work and proof of stack have been implemented to improve the security of blockchain. In addition, the anonymity of user information should be ensured when using blockchain in the cloud computing environment, and the user information should be completely deleted when removing the service.

Again, as the digital world continues to evolve and institutions implement various anti-corruption measures to fight against corruption or illicit activity; blockchain technology will be a key ingredient to resolve compliance concerns, resolve anti-corruption issues and enhance overall security for cloud computing. This project not only touched on the challenges of implementing blockchain technology, but provided strong support on why it is more secure than dual-factor authentication and how it can continue to pave the way for enhanced compliance, improved security and better overall efficiency.

Future Research

At first blockchain technology is commonly seen as the main technological innovation of bitcoin. Today, this technology has more advanced practical implementations than bitcoin, which ranges from financial application, including digital payment systems, smart contracts, insurance, and capital markets, to non-financial applications, such as governmental services, decentralized storage, and decentralized IoT. This project focused mainly on the potential of implementing blockchain technology within the financial sector. Given the continued focus on regulatory expectations and that the regulatory environment may not be up to speed with the advancement of blockchain technology, which may cause a problem within the various markets, especially the financial industry. The regulatory environment and current expectations will prove to be an interesting research topic to further examine how the regulators adapt to a fast-changing environment and if there are any regulatory obstacles with the implementation of blockchain. It is important for institutions to receive continued guidance in order to apply adequate rigor to related policies and procedures to ensure compliance with regulatory expectations and the continuous change in the controls of virtual currencies. Furthermore, a need for further research on developing better evaluation frameworks for blockchain implementations within different industries has also been identified as a good research topic to expand on.

Recommendations and Conclusion

To allow an industry or society to move in a new direction within our digitalized world, it must first understand how the environment evolved to its present state and provide trust within these new developments to promote further expansion. This project provided a strong foundation of what blockchain technology is, how it works, how it can be used as an effective way to help resolve compliance concerns, anti-corruption issues and help promote a stable environment for enhanced cloud computing. This project also touched on the current challenges of implementing blockchain technology and why it still remains a technology with the potential to exceed strategic initiatives as further enhancements are made within our digitalized world. Blockchain technology is a promising development that can support both further digitalization and enhanced efficiency of control processes. However, a number of questions and/or concerns became apparent during this project and will need to be settled and researched before any type of blockchain architecture is fully implemented within an institution on a large scale. First, institutions as a whole must clearly understand the benefits (pros and cons) of blockchain technology and how blockchain principles can help them meet strategic initiatives in an efficient manner. Second, a blockchain IT system should be fully understood and trusted; as one of the main challenges an institution will face is transforming the current business landscape to fully trust in blockchain technology. The mindset of all key stakeholders is critical and must learn to accept blockchain technology. The next challenge is to implement an effective change model to help foster change. The change could be met with resistance, and it is important to make sure everyone is on the same page. Additionally, institutions must trust that data sharing is an opportunity for advancement and not a threat to system security. The last major challenge is to invest within the correct blockchain architecture best suited for your institution, one that would promote sustained growth, technology expansion and consistent compliance with regulatory expectations; for these expectations/requirements will also continue to evolve as regulatory agencies become more educated on blockchain technology.   As blockchain technology offers the opportunity to conduct financial transactions across various regulatory systems, products, national borders and regions (i.e., sending Bitcoins), regulatory agencies need to come together and further analyze blockchain capabilities on an international level to better understand these pros and cons of the technology.

Blockchain technology can help any institution provide resilient communications in a highly contested environment. As blockchain provides an efficient and reliable way of confirming the party submitting a record to the blockchain, the times submitted, and the date of its submission. It also confirms the contents of the record at the time of submission by eliminating the need for any third-party. However, it is equally as important to understand that blockchain technology does not verify or address the reliability and/or the accuracy of the content and blockchain technology does not provide any storage for records. Instead, it provides the hashes thereof.

This project also illustrates blockchain technology as a product that provides a distributed consensus, anonymity, cryptography and numerous other attack prevention capabilities. Blockchain technology is trustless because it can be compromised by both internal and external threats. At the same time, blockchains are secure and transparent because they do not rely on failure-prone secrets, but rather on a cryptographic data structure that provides a secure foundation on which to add additional security protocols. Finally, blockchains are fault tolerant; for they use algorithmic consensus mechanisms to align the efforts of honest nodes and reject those that are dishonest. Together, these distinct principals allow institutions and information system designers to rethink the fundamental architectures of cyber systems and network design, which must be reviewed and analyzed before implementation. Understand that blockchain technology is not completely immune to fraud, hacking and/or other malicious activities, but it continues to evolve and mature as more institutions are continuing to experiment with it and accept it.

The aforementioned principles clearly illustrate some key benefits of implementing blockchain technology; therefore these benefits along with strong architectural roadblocks could be a beneficial research project to determine what the best long-term solution is while maintaining operational efficiency and regulatory compliance. Future research should also be conducted on effective change models and training tools to help promote a sustainable IT infrastructure of blockchain technology. The following also illustrates additional recommendations for advanced research that can further promote sustainable and consistent anti-fraud capabilities. The absence of a central regulating authority and the autonomy enabled by its distributed consensus allows blockchain technology to aid in the administrative burden of government agencies to ensure compliance. Government agencies, regulators and law enforcement agencies must continue to further examine and understand the impacts of blockchain technology to close the gap and implement well-defined requirements. Once the technology and its uses are clearly understood, they should collectively come together and develop policies, procedures and regulations to govern the use of blockchain technology. Doing so will ensure consistency, promote consumer confidence, further stabilize system security capabilities and enhanced the overall functionality of emerging products within the blockchain environment (i.e. peer-to-peer economy). It is critical that regulatory agencies must work with state agencies to collectively understand the best way to regulate blockchain technology and ensure it is presented as a balanced approach across all regions, products and services.

As blockchain technology is clearly a model that breaks the mold of the many flawed assumptions of a traditional security network. Blockchain operates on a cryptographic data structure that provides a secure foundation on which allows the network to add additional security protocols. It simply uses established algorithmic consensus to align the efforts of honest nodes to simply reject those that are dishonest or do not match the defined protocols. Together, these protocols allow system designers to adjust the fundamental architectures of cyber systems and/or networks.

Conclusion

Distinguished by high transparency and a decentralized system, blockchain technology is one of the most innovative developments in recent years. While blockchain's best-known, most used and highest-impact application is Bitcoin, the potential impact of the technology is much greater and wider than virtual currencies. As we see a growing trend towards less trust in the financial sector and the overall governance of institutions, we see greater social expectations of accountability and responsibility within our new digitalized world. As the popularity of blockchain technology continues, it reflects an emerging social trend in our economy to prioritize transparency over anonymity.

Operational solutions within the financial industry and banks are expanding towards non-physical channels by implementing solutions that are more dynamic in technology to fully reach, engage and retain customers through enhanced customer experiences. Many institutions continue to adopt new solutions to improve storage and simplify operations, which help foster the move away from physical channels and towards an enhanced digital environment. With the expansion or need of digital technology, institutions have been studying the use of blockchain for the secure use of electronic cash by communicating solely between peers to exclude the involvement of any third party (Stanley, 2016). With that said, the use of blockchain to facilitate the exchange of money is well established; for this was the original use of digital currencies such as Bitcoin. However, further opportunities exist for institutions to use blockchain technology to help enhance other services such as compliance functions and cloud computing. In addition, blockchain technology will provide enhanced security compared to storing all data within a central data warehouse (Stanley, 2016).

As the digital world continues to evolve, institutions will implement various anti-corruption measures to help fight against corruption or illicit activity. This project addressed what blockchain technology is, how it works, how it can be used as an effective way to resolve compliance, resolve anti-corruption issues and enhance overall security for cloud computing. This project also touched on the current challenges of implementing blockchain technology and why it is more secure than dual factor authentication.

The use of blockchain-based systems is an indicator of the transparency and usability of the blockchain. Though blockchain does have some problems from a security standpoint and other aspects, these problems are expected to be settled over time, especially with the arrival of more stable and secure blockchain platforms. Finally, it is apparent that blockchain technology is gradually becoming a secure platform. It has a cyberattack resilient database architecture supported by cryptography, immutability and consensus principles, which are the key ingredients for the effective implementation of information security in an organization.

Blockchain has done away with the server to exclude the involvement of the central authority and has facilitated transactions through the participants who jointly store the transaction records and, finally, approve the transactions using P2P network technology. The blockchain has a distributed structure and utilizes the peer network and the computing resources of peers. Technical measures such as proof of work and proof of stack have been implemented to improve the security of blockchain. In addition, the anonymity of user information should be ensured when using blockchain in the cloud computing environment, and the user information should be completely deleted when removing the service.

Again, as the digital world continues to evolve and institutions implement various anti-corruption measures to fight against corruption or illicit activity; blockchain technology will be a key ingredient to resolve compliance concerns, resolve anti-corruption issues and enhance overall security for cloud computing. This project not only touched on the challenges of implementing blockchain technology, but provided strong support on why it is more secure than dual factor authentication and how it can continue to pave the way for enhanced compliance, improved security and better overall efficiency.

As illustrated throughout this project, blockchain technology enables various different types of applications and will enable even more as our digitalized world continues to evolve. As a result, it is difficult to tell what sorts of applications will be applied and to what extent, since the blockchain technology continues to expand. Given its expansion capabilities, there still remains plenty of additional research needed to fully understand the vast capabilities of blockchain technology. This project focused on the effects of blockchain technology in the financial industry and what sorts of applications it could enable (i.e. authentication, verification, cloud computing, etc.). As noted earlier within this project, there are many interesting topics regarding the use of blockchain technology. One thing for sure is that within the banking industry, services will become more efficient, faster and cheaper. There are still various technical and legislative barriers to overcome, but it is certain that blockchain technology will play a significant role in our future.

References

Blemus, S. (2017, December 11). Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide. Retrieved February 15, 2018, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080639

Blockchain: Democratized trust. (2016, February). Retrieved October 20, 2017, from https://dupress.deloitte.com/dup-us-en/focus/tech-trends/2016/blockchain-applications-and-trust-in-a-global-economy.html

Brandom, R. (2017, July 10). Two-factor authentication is a mess. Retrieved October 20, 2017, from https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess

B. Shanmugam, S. Azam, K. C. Yeo, J. Jose and K. Kannoorpatti, "A critical review of Bitcoins usage by cybercriminals," 2017 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, 2017, pp. 1-7., from doi: 10.1109/ICCCI.2017.8117693

Can the Blockchain Deliver Security to Banks Against Cyber Attacks? (2016, September 12). Retrieved October 20, 2017, from https://www.cryptocoinsnews.com/can-blockchain-deliver-security-banks-cyber-attacks/

Cermeño, J. S. (2016). Blockchain in financial services: Regulatory landscape and future challenges for its commercial application. BBVA Research, Madrid, Spain.

Cooper, L. (2017, October 09). What Is A Digital Wallet? Retrieved October 20, 2017, from http://www.huffingtonpost.com.au/2017/10/09/what-is-a-digital-wallet_a_23234568/

Devlin. B. (2017, March 14). Historical Data: From Data Warehouse to Immutable Blockchain. Retrieved October 20, 2017, from https://tdwi.org/articles/2016/03/14/historical-data.aspx

England, R. (2017, July 26). Bitcoin grows up and gets its first federally regulated exchange. Retrieved October 20, 2017, from https://www.engadget.com/2017/07/26/bitcoin-federal-regulation-exchange-ledgex-protection/

Finance, D. B. (n.d.). Blockchains and Data Management. Retrieved October 20, 2017, from http://www.finyear.com/Blockchains-and-Data-Management_a36228.html

Guo, Y., & Liang, C. (2016, December 09). Blockchain application and outlook in the banking industry. Retrieved February 18, 2018, from https://link.springer.com/article/10.1186/s40854-016-0034-9

Herlihy, M., & Moir, M. (2016, June 23). Enhancing Accountability and Trust in Distributed Ledgers. Retrieved February 15, 2018, from https://arxiv.org/abs/1606.07490

IBM Blockchain basics: Introduction to distributed ledgers. (2017, August 21). Retrieved October 20, 2017, from https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html

Identity Management on the Blockchain. (n.d.). Retrieved October 20, 2017, from https://shocard.com/cpt_news/identity-management-on-the-blockchain/

Information Sharing-Overview. (n.d.). Retrieved February 25, 2018, from https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_021.htm

Jacobovitz, O. (2016). Blockchain for Identity Management. *Blockchain for Identity Management, Technical Report #16-02*. Retrieved February 11, 2018.

Kakavand, H., & Kost De Sevres, N. (2016). The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies.

King, B. (2010). Bank 2.0: How customer behavior and technology will change the future of financial services. Marshall Cavendish International Asia Pte Ltd.

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017, May). Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (pp. 468-477). IEEE Press.

LedgerX and CBOE: The CFTC's Trojan Horse in an SEC Turf War. (2017, August 14). Retrieved October 20, 2017, from https://www.coindesk.com/ledgerx-cboe-cftcs-trojan-horse-sec-turf-war/

McMullen, Dorothy A. and Sanchez, Maria H. and Reilly-Allen, Margaret O', Target Security: A Case Study of How Hackers Hit the Jackpot at the Expense of Customers (2016). Review of Business & Finance Studies, Vol. 7, No. 2, pp. 41-50, 2016. Available at SSRN: https://ssrn.com/abstract=2801762

McNamara, S. (2016, June 01). BlockChain Applications in banking. Retrieved January 5 2018, from https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-deloitte-blockchain-app-in-banking.pdf

Park, J. H., & Park, J. H. (2017). Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. *Symmetry*, *9*(8), 164.

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In Banking Beyond Banks and Money (pp. 239-278). Springer, Cham.

Satoshi Nakamoto (Ft. Coinbase) – Bitcoin: A Peer-to-Peer Electronic Cash System. (2008, October). Retrieved October 20, 2017, from https://genius.com/Satoshi-nakamoto-bitcoin-a-peer-to-peer-electronic-cash-system-annotated

Stanley, M. (2016, April 14). Banking on the Blockchain. Retrieved March 3, 2017, from http://www.morganstanley.com/ideas/big-banks-try-to-harness-blockchain

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11., from doi:10.1016/j.jnca.2010.07.006

Swan, M. (n.d.). Blockchain: Blueprint for a New Economy. Retrieved February 18, 2018, from https://books.google.com/books?hl=en&lr=&id=RHJmBgAAQBAJ&oi=fnd&pg=PR3&dq=BLOCKCHAIN%2BFOR%2BAUTHENTICATION%2C%2BVERIFICATION%2B&ots=XQrJAY2Nc3&sig=NM48cALpVHfGxHjmaaC_ut-w200#v=onepage&q=BLOCKCHAIN%20FOR%20AUTHENTICATION%2C%20VERIFICATION&f=falsehttps://books.google.com/books?hl=en&lr=&id=RHJmBgAAQBAJ&oi=fnd&pg=PR3&dq=BLOCKCHAIN%2BFOR%2BAUTHENTICATION%2C%2BVERIFICATION%2B&ots=XQrJAY2Nc3&sig=NM48cALpVHfGxHjmaaC_ut-

w200#v=onepage&q=BLOCKCHAIN%20FOR%20AUTHENTICATION%2C%20VERIFICATION&f=false

The Economist - The great chain of being sure about things. (2015, October 31). Retrieved March 20, 2018, from https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

The Four Pillars of Blockchain Technology (Part 1). (2017, January 25). Retrieved October 7, 2017, from https://richtopia.com/emerging-technologies/four-pillars-blockchain-technology-part-1

The fright factor of blockchain. (2017, October 19). Retrieved October 20, 2017, from http://www.crainscleveland.com/article/20171018/blogs05/139231/fright-factor-blockchain

The Fundamentals of an ECDSA Authentication System. (n.d.). Retrieved October 20, 2017, from https://www.maximintegrated.com/en/app-notes/index.mvp/id/5767

Trautman, L. J. (2016). Is disruptive blockchain technology the future of financial services? Is disruptive blockchain technology the future of financial services, SSRN-id2786186. doi:10.1075/ps.5.3.02chi.audio.2f

Ulieru, Mihaela; "Bitcoin: what it is, how it really can change the world," World Economic Forum, 23 June 2016, from www.weforum.org/agenda/2016/06/the-blockchain/

Weiss, N. E., & Miller, R. S. (2015, February). The target and other financial data breaches: Frequently asked questions. In Congressional Research Service, Prepared for Members and Committees of Congress February (Vol. 4, p. 2015).

Whitehead, J. W., & Aden, S. H. (2001). Forfeiting enduring freedom for homeland security: A constitutional analysis of the USA Patriot Act and the Justice Department's anti-terrorism initiatives. Am. UL Rev., 51, 1081.

WiecZner, J. (2017, August 22). Hacking Coinbase: The Great Bitcoin Bank Robbery. Retrieved February 11, 2018, from http://fortune.com/2017/08/22/bitcoin-coinbase-hack/

Wood, G. (2014). Ethereum: A secure decentralized generalized transaction ledger. *Ethereum Project Yellow Paper*, *151*, 1-32.

Yermack, D. (2017, January 10). Corporate Governance and Blockchains. *Review of Finance*, 21(1), 7-31. Oxford Academic. Retrieved February 15, 2018, from https://doi.org/10.1093/rof/rfw074