La Salle University
La Salle University Digital Commons

Economic Crime Forensics Capstones

Economic Crime Forensics Program

Summer 8-31-2016

Using Blockchain Technology to Facilitate Anti-Money Laundering Efforts

Dominick j. Battistini
La Salle University, battistinid1@student.lasalle.edu

Using Blockchain Technology to Facilitate Anti-Money Laundering Efforts

Dominick J. Battistini

La Salle University

Introduction

Money laundering can be defined as any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources (Money Laundering, 2016). It is difficult to determine the magnitude of money laundering because these illicit financial flows remain hidden (Schott, 2006). A report issued by the United Nations Office on Drugs and Crime (UNODC) quoted that the total of all criminal proceeds amounted to $2.1 trillion in 2009. The study also shows that "Less than 1 percent of global illicit financial flows are currently seized and frozen" (Pietschmann & Walker, 2012). This is concerning because money laundering not only enables the operation of criminal organizations such as drug and human traffickers but can also significantly distort the economies in which they enter.

The Financial Action Task Force (FATF) is an inter-governmental policy-making body that has helped to promote anti-money laundering efforts since its formation in 1989. It has issued 40 recommendations to fight money laundering and nine special recommendations to combat terrorist financing which have been adopted by 32 countries (About - Financial Action Task Force, 2016). Unfortunately, implementing these strategies has proved to be difficult for both developed and lesser developed countries. According to a study conducted by PricewaterhouseCoopers in 2016, "over the last few years, in the U.S. alone, nearly a dozen global financial institutions have been assessed fines in the hundreds of millions to billions of dollars for money laundering and/or sanctions violations" (PricewaterhouseCoopers, 2016). It stands to say that if financial institutions are having difficulties implementing frameworks to prevent and detect money laundering, then our enforcement agencies are unable to adequately address the issue as well.

A new hurdle that enforcement agencies have had to face is the emergence of Bitcoin, as well as other cryptocurrencies, that can be described as “a digital currency and online payment system in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank” (Swan, 2015). Being an often unrecognized currency, many banks and financial institutions have not had to worry about modifying their compliance programs. The biggest benefit of cryptocurrencies to money launderers is its decentralized nature. There is no governing authority, as members of the network handle issuances and payments. Once a disruptive technology, Bitcoin is beginning to lose momentum for a number of reasons and some its strongest proponents are now referring to it as nothing more than an experiment. The purpose of this paper is not to examine Bitcoin, but rather its underlying technology that has been found to be the actual value: blockchain. After providing a brief overview of the technology and the hurdles that financial institutions face when implementing anti-money laundering compliance programs, the possible ways in which blockchain can help alleviate these difficulties will be examined.

Understanding Blockchain

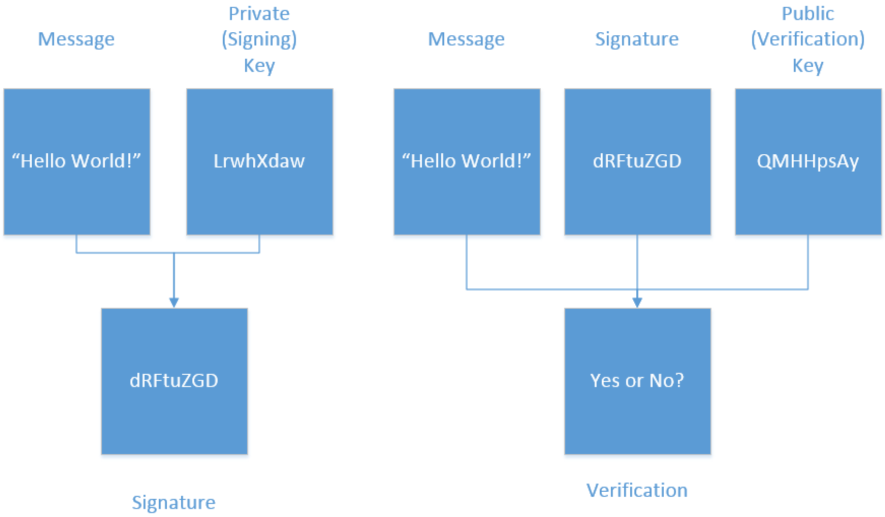
The term blockchain can have several different meanings depending on how it is used. For example, “The blockchain” is used to refer to the specific blockchain that Bitcoin functions on, “blockchain” denotes the underlying technology, and “a blockchain” describes a single implementation of the technology. Blockchain was originally developed for Bitcoin and can be explained by examining it in such terms. Simply put, it is a chain of blocks of data. Within each block are the details of multiple transactions. When transactions are processed, they are placed within a block and added to the end of the chain. Essentially a blockchain is a database where segments of data are stored in time-stamped blocks. The blocks are added to the chain in the order in which they occur. Its decentralization and ability to function without a central authority have led to it being described as a "trustless" protocol.

> The blockchain is seen as the main technological innovation of Bitcoin because it stands as a "trustless" proof mechanism of all the transactions on the network. Users can trust the system of the public ledger stored worldwide on many different decentralized nodes maintained by "miner-accountants," as opposed to having to establish and maintain trust with the transaction counterparty (another person) or a third-party intermediary (like a bank). (Swan, 2015)

Below is an in-depth examination of the technical controls that facilitate this "trustless" nature.

Bitcoin has been termed as a "cryptocurrency" because of its use of cryptographic functions, namely hash functions and private key encryption. As data is added to the chain, a hash function is applied. A hash function is an algorithm that is executed against data to create a unique string of alphanumeric characters. There are several unique characteristics of hash functions that support the role of a blockchain. A hash is a one-way algorithm, meaning that the original data cannot be retrieved from the resulting hash value. Identical data will consistently produce the same hash value. Conversely, the slightest change in the data will create an entirely different hash value. When hash functions are applied to individual transactions and blocks as they are added to the chain, the hash value of the previous transaction or block is included as an input. This creates a chain of hash values that are dependent upon the previous hash values. Any attempt to modify data in a blockchain would create discrepancies between the hash values throughout, making it immutable.

In addition to hash functions, Bitcoin and its blockchain utilize asymmetric cryptography, also known as public-key cryptography. The process begins with the creation of both a public and a private key. A key is nothing more than a string of seemingly random alphanumeric characters, but the public and private keys share a unique mathematical relationship. Data that is encrypted with a private key can only be decrypted by its associated public key. In Bitcoin and the blockchain, a private and public key pair is referred to as a “wallet”. Ownership of a Bitcoin is verified by digital signatures generated by public-key encryption. The private key, or signing key, is applied to a message to generate a signature. Although the public key, or verification key, actually becomes the address of the Bitcoin account after a hash function is applied several times, it can still be used to verify the private key by using the message, the signature, and address as inputs. This is because of the unique mathematical relationship between the signing key and the verification key.



Traditional database infrastructures rely on a central authority to distribute access to the database accordingly to maintain its confidentiality and integrity. In a blockchain, the identity of an account holder is expressed through their address, the hashed public key. The only possible way to determine an accountholder's identity from just the information contained on a blockchain alone is to analyze the pattern of transactions in an attempt to match the behavioral profile. Best practices for securing your identity on a blockchain includes using a separate address and key pair for each transaction, making it impossible to associate multiple transactions to a single behavioral profile. Although the details of each transaction are viewable by members of a blockchain, this data cannot be leveraged in any way as the identity of the account holder is still unknown. These features, in combination with the immutability of a blockchain, make it unnecessary to rely on a central authority to maintain the database as controls to preserve the integrity of the data and the confidentiality of the users are innate to the technology. Because of these factors, a blockchain can function as a "decentralized ledger". This means that a copy of the database is stored on each computer that is a member of a blockchain. The database is distributed using a peer-to-peer network, meaning that each member of the blockchain can speak to each other independently without relying on a central server to manage the communication. Computers that are members of this peer-to-peer network are referred to as "nodes". Because each node maintains its own copy of the ledger, the data will always be available to members of the network. Additionally, the ledger is verified and propagated throughout the network by general consensus. This means that if one member attempts to modify their version of the ledger, it will not be accepted by the rest of the network.

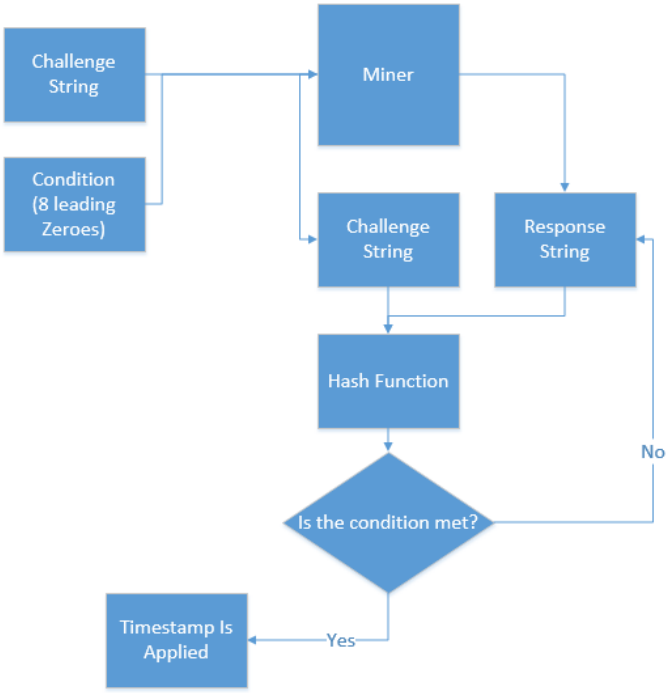
The processing of transactions, referred to as mining, is also decentralized and is completed by nodes called miners. The goal of processing transactions in Bitcoin is to provide verification that the owners did not double spend a coin. This is achieved by implementing a time-stamping server.

> A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it. (Nakamoto, n.d.)

Because the timestamp server is distributed over the peer-to-peer network, a “proof-of-work” is completed to show that the miner did in fact process the transaction. A proof-of-work is a “piece of data that requires significant computation to find” (Antonopoulos, 2015). A proof-of-work is completed by combining a "challenge string" and a "response string" to form a hash value that meets the desired result. The challenge string is provided by the blockchain while the miner’s computer system rapidly calculates hash values with different response strings. In many instances, the goal of a proof-of-work is to generate a hash value that has a specific amount of leading zeroes. Once this is achieved, the block is added to the chain and is propagated throughout the network. The longest chain will always be selected by nodes as the correct one to follow.

> If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one. (Nakamoto, n.d.)

Processing a transaction on the blockchain is essentially the completion of a proof-of-work so that a transaction can be time-stamped.



Another addition to the trustless nature of a blockchain is the concept of smart contracts. The idea of smart contracts existed long before Bitcoin and blockchain. “A smart contract is a computer program that both expresses the contents of a contractual agreement and operates the implementation of that content, on the basis of triggers provided by the users or extracted from the environment” (Idelberger, Governatori, Riveret, & Sartor, 2016). A smart contract lives on the blockchain and is monitored by the nodes of the network. It contains logic that will only execute if certain conditions are met, allowing them to function autonomously. Smart contracts can act as components of actual legal contracts or can be used solely to automate actions on the blockchain. Conditions can be met by monitoring transactional data within the blockchain or a data feed that is provided by a trusted source, known as an oracle. Because smart contracts can only monitor data that exists on the blockchain, oracles feed external data onto the blockchain so that it can be checked by smart contracts. For example, the payment of a sports bet can be automated by way of a smart contract if there is an oracle providing a data feed of the result of the sporting event. Smart contracts eliminate the need for a central authority to enforce an obligation.

Bitcoin functions on a “public blockchain”, meaning that anyone can become a member of the network and the transaction data is readable by everyone. As previously mentioned, the use of public key cryptography helps to hide the identity of the parties involved in the transaction, but other details are still viewable by the public. It is understandable why a financial institution would be hesitant to put data on a public blockchain. Alternatively, a private blockchain has a central organization that has write privileges, processes transactions, and distributes read permissions. This resolves concerns of privacy but eliminates the benefits of decentralizing the database and processing of transactions. A consortium blockchain is a hybrid system, offering the security of a private blockchain and the trustless advantages of a public blockchain. Read permissions can be distributed, limiting access to the data, but the processing of transactions remains decentralized. As opposed to a single organization functioning as a central authority, a group of organizations distributes authority amongst themselves. For example, a collection of financial institutions can establish a consortium blockchain, requiring a consensus of its member institutions to approve and process a transaction (Peters & Panayi, n.d.). This allows data to remain confidential while still being able to establish trustless relationships between members of a blockchain.

Blockchain facilitated the rise of “Bitcoin" but can be applied to much more than cryptocurrencies. Its components allow for transactions to occur without the need for a central authority to facilitate trust. Its use of public key cryptography allows for verification of ownership and conceals the identity of the account holder. The decentralized ledger, the completion of a "proof-of-work", and consensus-based propagation eliminate the need for a central data source and processor. Hash functions ensure that the ledger is immutable and preserves the integrity of the data. All transactions are recorded in the decentralized ledger which creates a full audit trail that supports transparency. While privacy is a concern of public blockchains, consortium blockchains allow members to distribute read permissions as necessary while still functioning in a decentralized environment. All of these characteristics make trust inherent to the blockchain and create many opportunities to increase efficiency in various sectors, including the financial services industry.

An Overview of Money Laundering

Money laundering is a financial transaction with the property that "represents the proceeds of some form of unlawful activity" (“18 U.S.C. 1956 - laundering of monetary instruments,” n.d.). A money launderer "conceals the existence, illegal source, or illegal application of income, and then disguises that income to make it appear legitimate" (Schroeder, 2001).

> Regardless of the crime, money laundering typically involves a three-step process when converting illicit proceeds into apparently legal monies or goods: (i) placement: the criminally derived money is placed into a legitimate enterprise; (ii) layering: the funds are layered through various transactions to obscure the original source; and (iii) integration: the newly laundered funds are integrated into the legitimate financial world in the form of bank notes, loans, letters of credit, or any number of recognizable financial instruments. (Hart, 2014)

These basic rules of money laundering summarize the overall strategies of some common techniques: anonymity, speed, complexity, and secrecy (Nedelcu, n.d.). First and foremost, the source of the funds must remain anonymous because it derived from illegal activity. During the placement phase, illicit funds are placed in the name of a legitimate entity to conceal their true nature. The funds are often distributed amongst entities so that they can enter financial institutions in smaller, less noticeable amounts. The desire for anonymity also carries over to the financing of terrorism, but is often achieved during the layering phase as the source funds may be from a legitimate entity. In the layering phase, a series of transactions is rapidly completed to create a complex paper trail, obscuring the parties involved in the placement process. By layering these rapid transactions and choosing different countries of destination, the movement of illicit funds becomes increasingly complex and challenging for investigators to follow. For these reasons, international movement of funds and cross-currency transactions are common amongst money launderers.

As money laundering has come to light as a growing economic issue and facilitator of criminal and terrorist organizations, it has gained attention from both national and international regulatory bodies such as the Financial Action Task Force (FATF). The FATF plays an integral role in establishing and maintaining anti-money laundering efforts on an international level.

> The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a 'policy-making body' which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas”. (About - Financial Action Task Force, 2016)

As cross-currency transactions are standard in the layering phase of the laundering process, these collaborative relationships between nations are crucial.

Although this progress has been a significant step forward in establishing regulatory frameworks for countries to combat money laundering, the FATF is purely a regulatory body. The enforcement of anti-money laundering controls is the responsibility of the financial institutions and local law enforcement agencies.

> Prevention is a regulatory tool and focuses mostly on sanctions, regulatory and supervisory rules and standards, reporting and customer due diligence. Enforcement is a legal tool, concentrating on investigation, confiscation, prosecution and punishment. Despite the criminalization of money laundering and the increasingly prominent and public role of enforcement agencies in the AML regime, the process is in practice overwhelmingly a preventative regulatory one. (Tsingou, 2010)

The enforcement of anti-money laundering regulations has been challenging for many financial institutions as it carries a broad set of responsibilities with it. As previously mentioned, international movement of funds is a very common strategy during the layering phase. Money launderers not only target countries that have strict bank secrecy policies, but they also take advantage of lesser developed countries (LDC's) that do not have the proper resources to detect or prevent money laundering.

> Owing to antiquated systems in countries like Uganda, record keeping is manual and of poor quality. In most financial institutions in less developed economies, there are no records at all that can help in monitoring transactions or tracking cases of money laundering because records are poorly kept. (Mugarura, 2013)

Having the proper infrastructure in place to be able to track and monitor the flow of illicit fund requires a significant amount of both human and technical resources. It can become difficult to trace illicit financial flows as funds are transferred in between banks, on both a national and international level, because of the inconsistencies of institutional infrastructures in not only LDC's but developed countries as well. This is in part due to the competitive and confidential nature of banking but also becomes an issue when dealing with the compatibility amongst different technologies that financial institutions are using. These are some of the many challenges standing in the way of an effective global anti-money laundering strategy.

Compliance Requirements

When examining how blockchain can assist financial institutions combat money laundering, it helps to understand the applicable regulations. Two of the most important regulations are "Know Your Customer (KYC)" and "Anti-Money Laundering (AML)". Additionally, sanction lists contain information regarding entities for which financial institutions should not process transactions. Because all of these are used to prevent and detect money laundering, AML can be utilized as an umbrella term. Below is a brief overview of each and what they mean for financial institutions.

The Bank Secrecy Act of 1970 signaled the beginning of AML controls and the first formal efforts against money laundering. Its purpose was, and still is, to identify the source and movement of currency and other monetary instruments by establishing recording keeping and reporting requirements for financial institutions. These first reporting requirements mandated that banks "(1) report cash transactions over $10,000 using the Currency Transaction Report; (2) properly identify persons conducting transactions; and (3) maintain a paper trail by keeping appropriate records of financial transactions" (History of Anti-Money Laundering Laws, n.d.). The Annunzio-Wylie Anti-Money Laundering Act of 1992 introduced Suspicious Activity Reports (SAR's) and expanded recordkeeping requirements to include wire transfers. In 2001, the USA PATRIOT Act was passed in the aftermath of the terrorist attacks of September 11th. Title III addresses money laundering as well as the funding of terrorist organizations and is known as the International Money Laundering Abatement and Financial Anti-Terrorism Act. This improved information sharing between financial institutions and the U.S. government by requiring government-institution information sharing, voluntary information sharing among financial institutions, and required banks to respond to regulatory requests for information within 120 hours. According to a manual created by The Federal Financial Institutions Examination Council, suspicious activity monitoring should include the following reports:

- Suspicious activity monitoring reports.
- Large currency aggregation reports.
- Monetary instrument records.
- Funds transfer records.
- Nonsufficient funds (NSF) reports.
- Large balance fluctuation reports.
- Account relationship reports. (BSA/AML Compliance Program, n.d.)

Requiring recordkeeping, the above reports, and government-institution information sharing increased the efficiency of money laundering investigations.

KYC is often viewed as a component of AML, both being commonly referred to as AML/KYC. “KYC generally refers to the steps taken by a financial institution to establish the identity of a customer and be satisfied that the source of the customer funds is legitimate” (“Guide to US AML Requirements,” 2012). This includes a customer identification program (CIP) and collecting relevant information, known as Customer due diligence (CDD) for all customers. In circumstances when a customer is deemed to be a higher risk, additional information will be collected known as enhanced due diligence (EDD). This allows the financial institution to create a profile for the customer based on the expected pattern of activity of the account in terms of transaction types, dollar volume, and frequency, in addition to the expected origination and destination of funds.

Whereas AML/KYC refers to specific regulations, sanction lists identify entities for which a bank should not process transactions. One of the most notable collections of sanction lists is maintained by The Office of Foreign Assets Control (OFAC). These sanctions can be based on geographical location or nature of the transaction, such as Counter Terrorism Sanctions and Nonproliferation Sanctions.

> The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. ("Office of foreign assets control (OFAC)," 2016)

By adhering to sanctions, institutions can ensure that they are not facilitating transactions associated with particular criminal or terrorist activity.

AML compliance can be seen as encompassing KYC and sanction lists, but it helps to understand them by separating them by function. AML requires financial institutions to keep accurate records of transactions, file suspicious activity reports when necessary, and share this information with government agencies promptly upon request. KYC requires that financial institutions perform due diligence when engaging in business with new customers and that a profile is created based on expected transactions, destinations, and origins of funds. Sanctions ensure that financial institutions are aware of and do not conduct business with entities and countries that may be deemed as a high risk. Although all of these may seem similar in nature, each provides a specific function to facilitate the detection and prevention of money laundering.

Combating Money Laundering With Blockchain

As previously noted, the four basic rules of money laundering are anonymity, speed, complexity, and secrecy. While organizations like the FATF have pushed countries and institutions to implement compliance programs, a gap remains between prevention and enforcement.   Financial institutions must comply with AML/KYC and sanction lists, but inconsistencies of institutional setup and barriers for LDC’s have made these strategies difficult to adopt. By implementing a consortium blockchain, financial institutions are able to address rules of money laundering, simplify information sharing with enforcement agencies, and ease the difficulties of implementing a compliance program. The proposed solution would utilize a blockchain to facilitate communications between institutions as opposed to functioning as a cryptocurrency. It would ideally be implemented as a payment rail, although adoption may be difficult to facilitate. At the very least, a blockchain could be implemented as a record keeping tool spanning across financial institutions.

Unlike traditional infrastructure, implementing a blockchain is not resource intensive. Servers and networking technology are the backbone of traditional infrastructure. The technology itself can be costly and require a team of professionals to maintain. To join a blockchain, an institution only has to have one node on the peer-to-peer network. Instead of constructing an entire data center, an institution can utilize a single computer to become part of a secure network to store data and comply with regulatory frameworks. In some instances, cost may not be a barrier but inconsistencies of institutional setup make it difficult for enforcement agencies to examine the flow of funds between institutions. They must often submit separate requests for different institutions and piece together the information. An institution can easily integrate a blockchain into their existing infrastructure and become a member of a consistent network where a record of all transactions is stored on all nodes. Enforcement agencies are able to see a full audit trail of conducted transactions by accessing a single database instead of submitting requests to multiple institutions that must allocate resources to comply within 120 hours. Access to the data can be distributed to parties by the consortium as necessary, each bank being responsible for their accountholder’s privacy. Additionally, "Section 314(b) of the USA PATRIOT Act provides financial institutions with the ability to share information with one another, under a safe harbor that offers protections from liability, in order to better identify and report potential money laundering or terrorist activities"("Section 314(b) Fact Sheet," 2013).

With traditional infrastructures, money launderers achieve anonymity by conducting a series of rapid transactions in order to build a complex paper trail. Because of the separate infrastructures that financial institutions maintain, a single bank is unaware of the transactions that an accountholder previously conducted with other financial institutions. This makes it difficult to recognize the overall behavior as suspicious. Additionally, analysis by enforcement agencies becomes difficult because they have to acquire data from many different sources. A blockchain’s decentralized ledger compiles all data into one database. Behavioral analysis can then be conducted on the ledger in both real time and during the investigative process.

KYC is often the first applicable regulation that financial institutions must comply with as it is part of the client on-boarding process. “While institutions can rely on third parties to provide needed information in certain cases, the ultimate compliance responsibility rests with the financial institutions themselves” (Ryan, 2016). From this manner of thinking, it can be derived that the best verification of KYC information would be from another financial institution. Institutions should indeed remain responsible for their own KYC compliance, but can at least verify the legitimacy of the new customer's claims by comparing the data with that of other financial institutions that already do business with this customer. The identifiable information can be converted to hash-values and compared so that the verification process does not provide the financial institutions with any more data than what is needed. This blockchain would be used solely for the Customer Identification program with banking activity recorded on another. Reporting, tracking, and monitoring of account behavior in accordance with AML/KYC can be automated by the use of smart contracts. To review, smart contracts function autonomously and execute when a set of conditions is found to be true. Similarly, AML regulations dictate that reports, such as Suspicious Activity Reports and Large Balance Fluctuation Reports, be filed when particular behaviors occur. If these behaviors can be translated into computational logic, a smart contract can be created to autonomously submit the required report in real time to enforcement agencies. It is common for banks to submit a SAR if a party conducts frequent transactions just under $10,000; as it is usually seen as an attempt to avoid reporting requirements. Logic could be embedded into a smart contract to file a SAR if the number of transactions involving funds in the range of $8,000-$9,999 exceeds a specified amount within an allotted period of time for a specific account. In the case of Large Balance Fluctuation Reports, a conditional expression can be used to automate the submission of a report if an account exceeds a daily threshold. As previously noted, KYC profiles are created per customer based upon transaction types, dollar volume, and frequency, in addition to the expected origination and destination of funds. These values can be embedded into a smart contract so that a report is filed if the account holder deviates from his expected pattern of behavior. Integrating smart contracts and AML/KYC reporting is based on data that exists on a blockchain, making the implementation seamless.

However, the data contained on sanction lists exists outside of public view and requires a different approach. As previously noted, oracles are trusted sources that feed data onto the blockchain. Sanction lists regulate the movement of funds based on a broader set of criteria such as country or nature of the transaction and are maintained by an external source. Oracles can be established for each sanction list, such as those provided by OFAC, so that smart contracts can use the data in their conditional operations. In addition to enabling the autonomous enforcement of sanctions, this allows the lists to be updated in real time, as opposed to the previously mentioned AML/KYC regulations that require reporting based on specific accounts and transactional behaviors.

One of the purposes of the investigation process is to prepare evidence for the prosecution so that a case can be presented in court. A major challenge of working with digital evidence is maintaining the chain of custody and proving that the integrity of the data has been preserved. This is commonly achieved by applying a hash function to the data and generating the same value at a later date to prove that the evidence has not been tampered with. Blockchain implements hash functions directly into its operations. In addition to making the data immutable during business operations, it also reinforces the validity of the data if and when it needs to be presented as evidence. As with any new technology, there are definitely hurdles that blockchain must overcome in order to be deemed admissible in court. Because Bitcoin has become widely used by criminal organizations, there has been pressure placed on legislative bodies to deem evidence found on the blockchain as admissible so that it can aid in prosecution. Because Bitcoin is based on blockchain technology, any precedent would apply to the admissibility of evidence found on any blockchain.

The integration of a blockchain into the operations of banks and financial institutions can provide a strong support system for AML/KYC compliance. For starters, it eliminates the ability for money launderers to achieve anonymity through the use of speed and complexity during the layering phase by providing an easily accessible ledger of all transactions that can be audited and traced with data analytics. The use of decentralized ledgers and peer-to-peer networks eliminates inconsistencies of institutional setup and barriers that LDC's may face when attempting to implement an adequate infrastructure, making compliance achievable by all financial institutions. The decentralized ledger also gives enforcement agencies the ability to have direct access to the data as opposed to obtaining data separately from each financial institution involved. Smart contracts not only allow reporting requirements and the monitoring of expected activity to be automated but can also enforce standards set forth by sanctions by querying a data feed provided by an oracle. As one of the main purposes of the investigation process is to prepare evidence for use in court, the immutability of the data and use of hash functions can ease some of the challenges of maintaining its integrity. These benefits can greatly decrease the amount of resources necessary to maintain an AML/KYC compliance program and increase its efficiency.

Conclusion

The impact of money laundering is significant, allowing criminal enterprises to convert illicit funds to licit and significantly distort legitimate economies. Policy making bodies such as the FATF have done well in promoting the use of AML/KYC compliance programs. The difficulty has arisen in the actual implementation in both developed and lesser developed countries. Although it functions as the foundation for Bitcoin, a cryptocurrency that has greatly enabled money launderers, blockchain technology has many specific functions and features that can help financial institutions to overcome the challenges being faced in the AML/KYC regulatory space.

By utilizing a decentralized ledger, institutions are able to avoid inconsistencies in their setup. It also allows lesser developed countries to implement an infrastructure without having to heavily invest in technical or human resources. Additionally, enforcement agencies are able to access a single source of data for all financial institutions in real-time. A consortium blockchain functioning via a peer-to-peer network allows financial institutions to work together without placing their trust or data in a single authority or source. The nature of the decentralized ledger is to record every transaction, creating a full audit trail for every account. Because the blockchain is immutable, all data maintains its integrity. If deemed admissible in court, evidence stored on the blockchain would be easily preserved. Smart contracts can fulfill AML/KYC reporting and monitoring requirements of suspicious and expected activity, while sanction lists can also be autonomously enforced once they are entered onto a blockchain by a trusted data feed known as an oracle.

The benefits of using a blockchain to facilitate AML/KYC compliance are numerous. Although ideally the solution would be implemented as a payment rail, it is understandable that financial institutions would be hesitant of its adoption. In an effort to introduce the concept slowly and gain acceptance, it could begin its implementation as purely a tool for recordkeeping and function alongside existing payment rails. This would give financial institutions the ability to reap the rewards of using a blockchain without immediately exposing themselves to the risks of using a new technology to facilitate the transfer of funds. Establishing and maintaining an effective AML/KYC compliance program is a unique and demanding challenge that blockchain can simplify. The benefits of using a blockchain in the financial services sector for AML/KYC compliance are too great to go unnoticed simply because of hesitation of adoption.

References

18 U.S.C. 1956 - laundering of monetary instruments. Retrieved July 27, 2016, from https://www.gpo.gov/fdsys/granule/USCODE-2011-title18/USCODE-2011-title18-partI-chap95-sec1956

About - Financial Action Task Force (FATF). (2016). Retrieved July 18, 2016, from http://www.fatf-gafi.org/about/

Antonopoulos, A. (2015). *Mastering Bitcoin: Unlocking digital Crypto-Currencies*. United States: O'Reilly Media, Inc, USA.

BSA/AML Compliance Program—Overview. Retrieved July 18, 2016, from Bank Secrecy Act Anti-Money Laundering Examination Manual, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_007.htm

Guide to US AML Requirements (2012). (5th ed.). Retrieved from https://www.protiviti.com/en-US/Documents/Resource-Guides/Guide-to-US-AML-Requirements-5thEdition-Protiviti.pdf

Hart, C. (2014). Money Laundering. *American Criminal Law Review, 51*(4), 1449.

History of anti-money laundering laws. Retrieved July 18, 2016, from https://www.fincen.gov/news_room/aml_history.html

Idelberger, F., Governatori, G., Riveret, R., & Sartor, G. (2016). *Evaluation of Logic-Based Smart Contracts for Blockchain Systems*. Retrieved from https://www.researchgate.net/profile/Guido_Governatori/publication/303679677_Evaluation_of_Logic-Based_Smart_Contracts_for_Blockchain_Systems/links/574cb84308ae8bc5d15a5a3a.pdf

Money laundering. (2016, June 20). Retrieved July 18, 2016, from http://www.interpol.int/Crime-areas/Financial-crime/Money-laundering

Mugarura, N. (2013). Scoping the regulatory environment for harnessing normative anti-money laundering laws in LDCs. *Journal of Money Laundering Control*, *16*(4), 333–352. doi:10.1108/jmlc-04-2013-0009

Nakamoto, S. *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from https://Bitcoin.org/Bitcoin.pdf

Nedelcu, C. (n.d.). Money Laundering Techniques Commonly Used. *Challenges of the Knowledge Society*. Retrieved from http://www.oalib.com/paper/2953592#.V4yZFvkrJD8

Office of foreign assets control (OFAC). (2016, April 29). Retrieved July 18, 2016, from https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx

Peters, G. W., & Panayi, E. (n.d.). Understanding modern banking ledgers through Blockchain technologies: Future of transaction processing and smart contracts on the Internet of money. *SSRN Electronic Journal*. doi:10.2139/ssrn.2692487

Pietschmann, T., & Walker, J. (2012). *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes: Research report*. Retrieved from https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf

PricewaterhouseCoopers. (2016, February 25). *Anti-money laundering*. Retrieved July 18, 2016, from http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/anti-money-laundering.html

Ryan, D. (2016, February 7). *FinCEN: Know your customer requirements*. Retrieved July 18, 2016, from https://corpgov.law.harvard.edu/2016/02/07/fincen-know-your-customer-requirements/

Schott, P. A. (2006). *Reference guide to anti-money laundering and combating the financing of terrorism* (2nd ed.). Retrieved from http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/Reference_Guide_AMLCFT_2ndSupplement.pdf

Schroeder, W. (2001). Money Laundering: A Global Threat and the International Community's Response. *FBI Law Enforcement Bulletin*, *70*(5), 1–9.

Section 314(b) Fact Sheet. (2013, October). Retrieved from https://www.fincen.gov/statutes_regs/patriot/pdf/314bfactsheet.pdf

Swan, M. (2015). Blockchain: Blueprint for a new economy. United States: O'Reilly Media, Inc, USA.

Tsingou, E. (2010). Global financial governance and the developing anti-money laundering regime: What lessons for international political economy? *International Politics*, *47*(6), 617–637. doi:10.1057/ip.2010.32