MSc Program
Engineering Management

Towards a New Vision of Customer Identity Management in European Banking Using Emerging Distributed Ledger and Cryptographic Approaches: The Case For and Against Blockchain

A Master's Thesis submitted for the degree of
"Master of Science"

supervised by
Dr. Larry Stapleton

Christoph Maurer

00311240

11.01.2018, Vienna, Austria

TU WIEN CONTINUING EDUCATION CENTER

Affidavit

I, **CHRISTOPH MAURER**, hereby declare

1. that I am the sole author of the present Master's Thesis, "TOWARDS A NEW VISION OF CUSTOMER IDENTITY MANAGEMENT IN EUROPEAN BANKING USING EMERGING DISTRIBUTED LEDGER AND CRYPTOGRAPHICN APPROACHES: THE CASE FOR AND AGAINST BLOCKCHAIN", 57 pages, bound, and that I have not used any source or tool other than those referenced or any other illicit aid or tool, and
2. that I have not prior to this date submitted this Master's Thesis as an examination paper in any form in Austria or abroad.

Vienna, 11.01.2018

Signature

MSc Program
Engineering Management

Abstract

Keywords: Blockchain, Identity, Regulatory, Banking, Bitcoin, Technology

This piece of work is aimed at arguing the advantages and disadvantages as well as the challenges of the blockchain technology and if this distributed ledger system, has the potential to replace current regulatory bodies and intermediaries in the financial services sector, specifically in terms of identity management and more generally.

This would seem to have been the vision of the originators of the technology back in 2009/10. To create a self-sustainable, secure environment for transactions of monetary nature.

In this piece of work, it is the intention to follow a specific argument in order to demonstrate that this “original idea” is not something which is likely to survive or become main stream. Rather, arguments will be made to demonstrate that likely there will be a hybrid of “old” and “new” emerging.

The solution suggested to harvest the full potential of those new emerging technologies, amongst others, customer identity management, is to streamline existing processes by involving regulatory bodies in the process of setting up new services for transacting and managing identities, as the need for oversight, due to technological flaws, cannot be argued away completely.

Contents

1 Introduction

1.1 General Background

How distributed ledger technology (DLT) and blockchain basically work is key to this paper and is to be reflected upon in the below introduction.

The concept of blockchain as a distributed database management system was first described in 2008 by Satoshi Nakamoto, likely a fictitious character, in the Bitcoin White Paper. The following year, he published the first bitcoin software implementation and launched the first publicly distributed blockchain (Bitcoin.org, 2008).

A report by the UK Government Chief Scientific Adviser (2015) states that algorithms which enable the development of distributed ledgers are potent and potentially disrupting innovations. Those innovations can very well transform the delivery of public and private services in the long run and potentially increase efficiency through a wide range of uses.

Ledgers in general have been highly important for trade since first being used in ancient times and since have continuously been used to record information, mostly about assets such as money and property.

However, in history, the only really notable innovation in terms of ledgers has been computerization, which initially was merely a transmission from paper to zeros and ones. Nowadays, algorithms allow for the combined formation of digital distributed ledgers with properties and possibilities that have the potential to go past anything we have seen so far, in particular over the last decades.

A distributed ledger, today, basically is an “asset database” that can be shared through a network. All nodes within a network can have their own matching copy of the particular ledger. Any changes to the ledger are mirrored in all reproductions in literally no time (minutes to seconds). With traditional systems, this may well take hours or days.

The assets can be financial, legal, physical or electronic etc. The safety and correctness of those assets are maintained cryptographically through the use of keys and signatures to control the rights within the shared ledger, meaning, who can do what. Records can also be updated by one, some or all of the partakers, according to general guidelines established by the network (gov.uk, 2015).

Fundamental to this technology is the blockchain, which was invented to create the peer-to-peer digital cash Bitcoin in 2008. Blockchain systems enable Bitcoin transactions to be aggregated. These are then added to a “chain” of existing blocks by means of a cryptographic signature.

The Bitcoin ledger is built in a distributed and “permissionless” fashion, so that anybody can add a block of transactions if they can solve a new cryptographic problem to add a new block. The motivation for doing this is that there is a reward in the form of Bitcoins awarded to the solver of the puzzle. Anyone with access to the internet and the computing power to solve the cryptographic puzzles can add to the ledger (Bitcoin mining). The procedure of mining Bitcoin is highly demanding when it comes to matters of energy consumption as it requires very large computing power (gov.uk, 2015). This is the reason why the most successful miners are based in countries where energy is cheap. It has been projected that the energy requirements to run Bitcoin are in excess of 1GW and may be equal to the power usage of Ireland. This basically means that Bitcoin miners provide their computing power to approve transactions and keep the network running and in return get Bitcoins for their work (Tapscott & Tapscott, 2016).

In general, as stated by Geiling (2016), in order to perform a transaction digitally, each user needs an address corresponding to the traditional account number. This is the public key which corresponds cryptographically with a private key. Each transaction is digitally signed using the private key. Other users can check them using their public keys. The problem is that the payment recipient can be sure to complete the transaction with a legitimate partner, but cannot determine whether the digital money, for example, or the item to be transferred is actually in its possession, or whether it has not been issued twice (double spending). This problem is solved by means of a new type of transaction accounting: Instead of holding, checking and approving each individual transaction through a trusted booking center, for example a clearing house in banking, using a "master ledger" (central directory), DLT offers the possibility to transfer assets and/or any other kind of information in a decentralized way. A distributed ledger is a public, decentralized ledger (network of participants/computers/servers). It is the technological foundation of virtual currencies and serves to record transactions from user to user in digital payment and business transactions without the need for a central office that legitimates each individual transaction. Blockchain, for example, is the Distributed Ledger, which is based on the virtual currency bitcoins (Geiling 2016).

With the blockchain technology, all the transactions or exchanges of information in general are ordered in a pool are waiting to be confirmed. The transactions can only be executed after confirmation. For this purpose, all computers operating in the Bitcoin network, ie, those computers that provide computer processing capacity via the bitcoin software for transaction processing, check whether the transactions that are to be checked are contradicting the previous transaction history (McKinsey, 2015). To this end, they are the same as the account books stored on all these computers with the transaction history. If the transactions appear legitimate, because a majority of the computers classify them as non-contradictory, these are confirmed. The computers operating in the network compete for the validation transactions. The operator of the fastest computer receives a bitcoin reward in return for their use. Conclusively, there is an incentive to always provide sufficient computing power for the legitimation check on the network (this is called “mining”) (Geiling, 2016).

In general, the fastest computer stores the validation of transactions in the form of a transaction bundle, a so-called block. The individual transaction information is summarized and coded (hash) by solving a computing task (from the miner). The hash of the newly created block is distributed to all other computers over the entire network (Geiling 2016). The new information is thus not stored centrally but can be accessed locally on any computer in the network. This ensures that other miners can chronologically build on the last block created. This mechanism creates a chain of blocks, the blockchain. If it happens that two miners at the same time create a block of the same transactions, other computers only propagate the chain on one of these blocks. The other becomes an "orphaned block". Transactions that are only part of the orphaned block and do not appear simultaneously in the "sister block" that has become part of the main chain fall into the pool of open and unsettled transactions. A secure confirmation of the transaction therefore always occurs only if several blocks are based on the block that contains the transaction in question, as a security measure, if it has actually become part of the main chain (Geiling, 2016).

The very core of this technology is that in the Bitcoin universe, parties do not have to trust their opponent's blockchain per se. By generating the above-mentioned hash for each block, a backup mechanism exists that must be traversed by each computer involved in the transaction validation (proof of work). Therefore, no access restrictions to the blockchain system are required (permissionless). There are, however, access-restricted DLT systems (permissioned). Instead of a proof of work, a proof-of-stake mechanism is used ("proof of proof"), in which the transferee must demonstrate that he has a special authorization to participate in the system. He receives this from a central legitimation center, that is, from the institution that controls the system. Access to restricted access systems therefore is only given to persons who can be trusted by the opposing party (Geiling, 2016).

In any case though, this piece of work is not about Bitcoin, rather it is to elaborate on the DLT technologies that enable cryptocurrencies and the power of those tools to transform ledgers into useful standards to record, qualify and secure a huge range of trades and a broad variety of other information. Conclusively, the blockchain methodology can be adapted to integrate rules, smart contracts, digital signatures and an array of other existing and new tools and applications.

1.2 The Research Problem

It could be argued that blockchain, as a distributed ledger system, will replace current regulatory bodies and intermediaries in the financial services sector entirely. Indeed, that would seem to have been the vision of the originators of the technology back in 2009/10. In this piece of work, it is the intention to follow a specific argument in order to demonstrate that this "original idea" is not something which is likely to survive or become main stream. Rather, arguments will be prepared to demonstrate that likely there will be a hybrid of "old" and "new" emerging.

Regulators, the financial industry, as well as developers, in any case are very much aware of the issues, threats and opportunities this technological development holds and are acting accordingly. Additionally, parts of the existing framework and system in place today, with much inherent complexities, which have to a large extent been developed organically over time will not that easily be replaced. If change will happen, and we can be comparatively sure that it will, naturally, it will come over time and organically integrate new technological milestones, even if they may be "game changing", such as blockchain.

The solution suggested to harvest the full potential of those new emerging technologies, amongst others, customer identity management, is to streamline existing processes by implicating regulatory bodies in the process of setting up and implementing new services and platforms for transacting and managing identity.

This Thesis will aim to address the potential opportunities and threats the proposed set up of such centralized platforms, based on the distributed ledger and more specifically block chain technology, could hold. It will be aimed at making an argument for incorporating all potentially involved parties, including regulatory bodies when designing and implementing new distributed ledger based services and solutions.

1.3 Motivation of the Research

To work on this issue is of importance, as identity management functions in and amongst banking institutions and corporates take up a large variety of resources to maintain, not only internally, but also on the side of the respective entity and supervising governmental authorities, including central banks.

The resources strained, below the line, are of monetary nature on all sides. More specifically though, the most noteworthy benefits could not only be reduced costs as a result, but convenience, reduced time and reduced structural, organizational and technical complexity for the user and thus may well result in an economic advantage, positively counteracting, partly necessary, regulatory and structural developments of the past years.

Furthermore, it could be argued that it is important to engage all potentially involved parties, including the governmental ones, in order to organically integrate this new technology with an existing framework. On the long run it is an illusion that derivatives of the distributed ledger technology, including cryptocurrencies, will continue to exist without regulators finding a way to intervene accordingly. The question is not if they may decide to do so, but rather when this will be the case.

This topic is of interest to the author personally, as having worked in the financial industry for over ten years and having seen which path the industry took during the years of the last financial crisis towards a completely new regulatory environment, which, to an extent was more than necessary. This development in turn, did lay the seed for the challenges and opportunities faced today more than ever in the past. The most important one as always (at least form an economic perspective) being to keep costs under control and foster efficiency gains at the same time, in order to stay competitive amongst an increasing number of contenders who seized the opportunities of a changing market situation with drastically tightening control mechanisms.

Moreover, there is an increasingly demanding client base (private and corporate), which are confronted with a similar variety of global economic and regulatory challenges broken down to their respective environments.

In order to tackle at least some of the most prominent issues I deem it important to explore the potential of new technologies. Those, such as the distributed ledger technology, are not only a threat to existing structures/technologies, but, as always, and more prominently, an opportunity as well, on an economical, technological, legislative and social scale.

1.4 Research Objectives

The research objective for this piece of work is to demonstrate why it would make sense to develop a broader, permissioned European platform to manage customer identity administration tasks by including existing regulatory bodies in order to benefit banking clients, banks and thus the European economy as a whole. This task will be performed by giving a broad overview of existing technology, own expertise of the author and research in order to be in the position to draw conclusions accordingly.

1.5 Research Questions

1. What are the main features of a digital identity management system infrastructure based upon blockchain for distributed, peer-to-peer financial contracts in European retail banking?

2. What are the benefits of a digital identity management system infrastructure based upon blockchain for customers of European retail banks compared to the traditional identity management system?

3. What are the disadvantages of a digital identity management system infrastructure based upon blockchain for customers of European retail banks compared to the traditional identity management system?

4. In light of the advantages and disadvantages of digital identity management technologies based upon blockchain, can the system be managed effectively on behalf of society without the intervention of central regulatory authorities?

2 “Customer Identity Management in European Financial Services”

2.1 Introduction and Background

The European Financial Services Sector has been paramount for the banking industry with effectively providing banking solutions to EU member states. It has a high number of customers transacting each day across the globe. EU financial services are under pressure to enable customers to conduct their transactions in a safe and secure environment without the need of any intermediaries, which could be facilitated by blockchain applications. The current EU banking systems have a limitation of Customer Identity Management, as all transactions have to undergo manual scrutiny, to an extent, before approval (Rajan, 2008).

Therefore, this section of the paper will highlight CIM in European banking. It will provide a detailed analysis of the banking system in Europe and how blockchain technology could be used to improve the banking processes.

Banks have been known to be the biggest financiers of identity management solutions for some time. This may be seen as a reflection of the essential role of identity verification in the financial services industry, where the ability to establish and verify the identities of customers is fundamental to maintaining customer trust, as well as to safeguard the security of transactions and to satisfy regulatory requirements.

Ongoing rapid growth in the area of digitization, new technologies and new user behaviors as well as new regulations are revolutionizing the ways in which banks interact with their clients and, in the process, changing identity management obligations forever. As a result, banks may be starting to re-evaluate their role in the identity supply chain.

At a time when industry convergence and disruptive innovation around payments and commercial services are so intense, this is a high priority. By taking advantage of their investments and experience in this area, banks are aware of the fact that identity is about a lot more than security alone. Remarkably, financial sector organizations in a variety of countries are seizing a broad set of opportunities and benefits by exploiting new identity sources, biometrics and advanced analytics technologies to increase customer insight and service relevance, while reducing fraud, waste and abuse for many years already (Accenture Study, 2013).

Regulatory authorities in almost all countries in Europe (and elsewhere) have been penalizing banks via a huge variety of fines from large to small. This has been an issue due to banks failing to adhere to supervisory standards. In addition to losing much business in order to acceptably fulfill KYC requirements, banks had to pay substantial penalties. Bankers to an extent can blame this on the system and inadequate databases. Hence, some of the banks have moved towards or are thinking about adapting blockchain technology to solve this problematic issue. There have neither been proper databases nor registries in the past, which led to huge complications in the process.

Currently, banks neither meet nor solve Know Your Customer (KYC) requirements and issues together in most cases. This KYC process is the procedure of gathering identity and other client information in the course of the respective onboarding process (Low, 2017). Everybody needs to copy the more or less same set of procedures in order to fulfill the KYC requirements. This is due to lack of an all-encompassing technology. At the same time, if a customer operates multiple accounts in multiple banks, the discrepancies between procedures grow wider as well. Hence, performing KYC processes only once should be the goal. Those should then be published, securely, distributed and shared. It is the above stated issues and challenges that blockchain technology could potentially solve appropriately, which makes it the most promising technology of the near future. Furthermore, many countries, with the exception of a few developed ones, lack any system or technology to provide unique documented identification for each and every individual. Multiple documents issued by multiple authorities do not consolidate into a single verifiable identity. Blockchain technology offers the solution of a digital identity, which may be verifiable by banks and other external agencies. Confirming the unique identity of a customer has been a major challenge for banks (Low, 2017).

As mentioned, financial insituitions face many problems during the process of successfully onboarding, profiling and monitoring clients. Onboarding, is a cost-intensive activity, while performing KYC checks leads to additional unwanted costs (mainly time of ones employess and time to meet deadlines for transactions/deals etc.). This prevents instituions from focusing on their core business. More crucially, stringent KYC norms can even turn away a good and especially a new client.

The challenges faced by banks with regard to KYC compliance have been huge. Lack of proper systems and inefficient and ineffective technologies are to blame. This is where blockchain could play a vital role in overcoming these problems and challenges in KYC processes.

Since most of the banks currently perform KYC checks via centralized external and internal databases, multiple checks have to be performed. Sometimes, each department will have to perform repeated background checks of a customer. This is due to what one calls as a data silo. Similar issues have been the problem for a lot of ventures. With blockchain, the KYC may be completed only once and it then it can be published and shared across all nodes or parties partaking in a transaction of any kind. So, there is no need to perform repetitive checks, which saves time, effort and money.

Conclusively, this is likely to boost the use of blockchain applications as soon as viable options have been developed. There are some around already, naturally, but the one platform that really makes sense on a broader scale with a reduced risk, acceptable stability profile and connected with a large enough number of participants to make it viable still has to emerge. The opinion further developed in the course of this paper is again, that this can only happen if the original idea is abandoned and trust in national regulators, at least in Europe can be reestablished.

2.1.1 Key definitions from bitcoin.org, 2017:

Address

A bitcoin address is similar to a physical address or an email. It is the only information you need to provide for someone to pay you with Bitcoin. An important difference, however, is that each address should only be used for a single transaction.

Bit

Bit is a common unit used to designate a sub-unit of a bitcoin - 1,000,000 bits is equal to 1 bitcoin (BTC or Ƀ). This unit is usually more convenient for pricing tips, goods and services.

Bitcoin

Bitcoin - with capitalization, is used when describing the concept of bitcoin, or the entire network itself. e.g. "I was learning about the bitcoin protocol today."
bitcoin - without capitalization, is used to describe bitcoins as a unit of account. e.g. "I sent ten bitcoins today."; it is also often abbreviated BTC or XBT.

Block

A block is a record in the block chain that contains and confirms many waiting transactions. Roughly every 10 minutes, on average, a new block including transactions is appended to the block chain through mining.

Block Chain

The block chain is a public record of bitcoin transactions in chronological order. The block chain is shared between all bitcoin users. It is used to verify the permanence of Bitcoin transactions and to prevent double spending.

BTC

BTC is a common unit used to designate one bitcoin (Ƀ).

Confirmation

Confirmation means that a transaction has been processed by the network and is highly unlikely to be reversed. Transactions receive a confirmation when they are included in a block and for each subsequent block. Even a single confirmation can be considered secure for low value transactions, although for larger amounts like 1000 US$, it makes sense to wait for 6 confirmations or more. Each confirmation exponentially decreases the risk of a reversed transaction.

Cryptography

Cryptography is the branch of mathematics that lets us create mathematical proofs that provide high levels of security. Online commerce and banking already uses cryptography. In the case of Bitcoin, cryptography is used to make it impossible for anybody to spend funds from another user's wallet or to corrupt the block chain. It can also be used to encrypt a wallet, so that it cannot be used without a password.

Double Spend

If a malicious user tries to spend their bitcoins to two different recipients at the same time, this is double spending. bitcoin mining and the block chain are there to create a consensus on the network about which of the two transactions will confirm and be considered valid.

Hash Rate

The hash rate is the measuring unit of the processing power of the bitcoin network. The bitcoin network must make intensive mathematical operations for security purposes. When the network reached a hash rate of 10 Th/s, it meant it could make 10 trillion calculations per second.

KYC (Know Your Customer)

Know your customer (KYC) is the procedure of banks and other businesses when identifying and verifying the identity of its business partners and clients (Low, 2017). The word is also used to refer to anti-money laundering regulations in banks which govern these procedures. Additionally, know your customer methods are also employed by corporations.

Mining

Bitcoin mining is the process of making computer hardware do mathematical calculations for the bitcoin network to confirm transactions and increase security. As a reward for their services, bitcoin miners can collect transaction fees for the transactions they confirm, along with newly created bitcoins. Mining is a specialized and competitive market where the rewards are divided up according to how much calculation is done. Not all bitcoin users do bitcoin mining, and it is not an easy way to make money.

P2P

Peer-to-peer refers to systems that work like an organized collective by allowing each individual to interact directly with the others. In the case of bitcoin, the network is built in such a way that each user is broadcasting the transactions of other users. And, crucially, no bank is required as a third party.

Private Key

A private key is a secret piece of data that proves your right to spend bitcoins from a specific wallet through a cryptographic signature. Your private key(s) are stored in your computer if you use a software wallet; they are stored on some remote servers if you use a web wallet. Private keys must never be revealed as they allow you to spend bitcoins for their respective Bitcoin wallet.

PoW

A proof of work is data which is difficult (time and costs) to produce but comparatively easy for others to confirm and which fulfils certain requirements. Creating a proof of work can be a random process with low probability. Conclusively, trial and error testing is required before a valid proof of work is generated (bitcoin uses the Hashcash proof of work system).

Signature

A cryptographic signature is a mathematical mechanism that allows someone to prove ownership. In the case of bitcoin, a bitcoin wallet and its private key(s) are linked by some mathematical magic. When your bitcoin software signs a transaction with the appropriate private key, the whole network can see that the signature matches the bitcoins being spent. However, there is no way for the world to guess your private key to steal your hard-earned bitcoins.

Wallet

A Bitcoin wallet is loosely the equivalent of a physical wallet on the bitcoin network. The wallet actually contains your private key(s) which allow you to spend the bitcoins allocated to it in the block chain. Each bitcoin wallet can show you the total balance of all bitcoins it controls and lets you pay a specific amount to a specific person, just like a real wallet. This is different to credit cards where you are charged by the merchant. (bitcoin.org, 2017)

2.1.2 Importance of banking in European commerce

In general, it needs to be stated that of course banking still is a highly important factor in commerce. Banks are and should be enablers of trade in and across countries. To a large extent they are performing this core duty, but this has been changing and countermeasures are not implemented fast or willingly enough due to a variety of reasons.

On the contrary even, banking is in dire need of many more upgrades at a much faster pace. Problem is that those updates of a structural/systemic/technological nature cost a lot of money most banking institutions only seem to have at first glance (Crosby et al., 2016). Since the financial crisis and a regulatory tightening of the surrounding frame, banks rightfully needed to bolster their capital base, watch risk more closely and see that they would not need the taxpayer to bail them out again. This together with a general economic downturn lead to the financial industry being caught up in the mistakes of their past, when they thought that the system was running well enough and most innovations and renovations system wise were often deemed less important than expansion efforts for example. As often in history, in times of need or scarcer resources market participants need to become more innovative in order to still be in the position to serve an increasingly demanding client base. So one could argue that nothing better than the financial crisis ever happened to banking and their clients, which is not entirely true of course as money could not and still does not flow through all parts of the system as it should, because banks need to watch the creditworthiness of their clients more closely to meet regulators demands, even if the regulators basically decided to provide funds to them for free (Özatac & Gökmeoglu, 2017). Those shortcomings, paired with technological developments such as blockchain and cryptocurrencies were niches, which needed to be filled by a new generation of entrepreneurs, leading to a still continuing and likely accelerating cycle of innovation.

The above only starts to describe in a rudimentary way how important banking still is as an integral part of our lives, but it also points in the direction of what the challenges lying ahead are and that the industry, together with client behavior and regulatory endeavors, still has a lot of change to go through along the way on a journey of deep transformation which has only just started (Crosby et al., 2016).

In more detail and as described by Tapscott and Tapscott (2016), new technology has continuously been added to systems which originally stem from the 1970s and thus are in dire need of upgrades. Additionally, this lead to painstaking system complexity and the need for huge data warehouses. A simple card transaction may go through five or more intermediaries until it reaches its destination, takes seconds to clear, but takes days to settle. What this complexity essentially does is that it provides opportunities for financial service providers to charge their customers. Monetary policy makers and regulators often lack many of the facts to make informed decisions thanks to the not necessarily, but often, planned opacity of large financial conglomerates. The main issue with new technologies in banking is that there are so many legacy technologies and thus, same as with the steam engine and electrified engines, most of those systems will likely run in parallel for quite some time, or to an extent for a very long time, before the new technology will be accepted and most of the flaws and shortcomings will be under control (Tapscott and Tapscott, 2016),

2.1.3 Erosion of trust in banks

As shown in EY’s (2016) Global Consumer Banking Survey of over 55ths clients, consumers have comparatively high level of trust in traditional banks to perform their basic duties, such as keeping their money safe etc. 60% of clients agree that banks have a role of importance to play with enabling people to achieve their goals though providing their expertise. Nonetheless, clients have lower levels of trust when it comes to strategic pledges such as providing unbiased advice (48% of customers believe that banks do). Over and above, FinTechs have achieved a parity level of trust with traditional banks already (EY, 2016).

To summarize, banks need to take action against eroding levels of trust. To be honest, who could blame anybody after the crisis years and the economic impact felt by all, as well as the reckless taking advantage of regulatory shortcomings by international financial players.

The good news here is that according to EY (2016), banks do not lag far behind the non-traditional players in the industry, who have to deal with challenging trust situations themselves.

This is the reason why banks should be seeing this as an opportunity to radically transform their front and back line's ability to provide high quality advice and empower them to really make decisions in the client-bank relationship interest, continue to work on operational excellence to eliminate errors, ensure complete transparency with products and pricing, really protect their clients identities/data and reassess the range of services offered to provide a service ecosystem, also encompassing non-financial services (EY, 2016).

2.1.4 Emergence of alternative banking systems

Alternative banking systems and alternative finance, according to Zhang et al. (2016), are mechanisms, channels, or systems of finance arising disconnected from the regulated finance system. Those systems, developing in parallel to the established ones, make use of technological innovations, such as cryptocurrencies, disintermediated business models and lending mechanisms and thus changes the way finance used to work. Other terms, which can be used to refer to alternative finance, include disruptive finance, distributed finance, or disintermediated finance. This new era of financial modernization with its features of transparency, speed, and accessibility has changed the way people, businesses and institutions perform financial transactions, or at least how they think about them, invest in assets, approach potential financing sources and operate in general. Much more thought is flowing into operational excellence and redesigning interfaces etc. The progression of this area is widely covered in the media and is in the process of slowly reaching a broader potential client base, playing a gradually more important role in helping industries and individuals access the capital and resources they need (Zhang et al., 2016).

Alternative finance instruments, or potentially rudimentary “banking systems”, as mentioned, include cryptocurrencies such as Bitcoin, SME mini-bond, social impact bond, community shares, private placement and other “shadow banking” mechanisms. Alternative finance contrasts to more traditional banking or capital market finance through technology-enabled “disintermediation” (Rubinton, 2011).

As stated by Irene Pitter (Global Executive, Banking & Capital Markets Practice Member of the KPMG Fin Tech Leadership Team) in the 2nd European Alternative Finance Industry Report, the European alternative finance market showed respectable growth figures of around 72 percent and thus demonstrated that demand for alternative finance solutions was strong. There are certain factors which are determining this growth accordingly and those are closely connected with the changing regulatory and market environment, as the market grows and matures. Important facts are for example the concern for loans to riskier borrowers and conclusively higher interest rates on potentially less sustainable business models. This, in turn, provides interesting opportunities for alternative banking solutions. Furthermore, a pattern of a pattern of consolidation and development and adaptation of new business models has been identified. Naturally, the strongest players will continue to grow their client base and become standard. This development is leading to partnerships between unconventional banking and finance platforms and banks who do take a stake in those platforms or help develop new ones from the start. Moreover, they may then even reference customers which they could not support on their own through the traditional product line at hand in-house. One example there would be Goldman Sachs, launching an online lending platform (Zhang et al., 2016).

2.2 Customer Identity Management (IM) in European Banking

Customer IM is a very central section of the banking industry that plays a crucial role in enabling daily transaction to be conducted securely and reliably (DiVanna, 2003). The processes involved in IM for European Banking require authorization processes for customer transactions. Authorization of customer transactions requires an intermediary before approval of a transaction. Having intermediaries has increased the costs of transactions for banks which increases the amount paid for each transaction process (Vasiljeva, and Lukanova, 2016).

Customer identity management is a very critical factor in the European and any other Banking system, and it is continuously and increasingly been facing some challenges concerning ensuring that there are no fraud activities such as money laundering (Bhasin, 2016 p60).

Nonetheless, the mechanisms used by European banks are slow and inefficient and at other times vulnerable to irregularities. The challenge for the European Banking Union is that it is faced with a stiff challenge of allowing privacy in personal banking while maintaining a high level of security for user transactions (Elsinger et al., 2006 p80). This problem requires implementation of mechanisms that will ensure that there is no room for vulnerabilities of user transactions by having means of time stamping transactions in real time as well as managing user identity.

To achieve secure transactions for users, the European Banking Union uses intermediaries who have to approve different transactions in the essence of certifying the identity of a customer and the legitimacy of a transaction (Elsinger et al., 2006 p80). Such a process slows down the processing of a transaction. Additionally, the implied costs for the procedure rise accordingly. Further, users are not able to access secure and unmonitored transactions from their accounts. Safe and consistent transactions can only be completed through an appropriate authorization channel. In general, inconsistencies in customer transactions call for specialized and critical identity management processes.

EU banking uses so called micro-prudential supervision for regulation of user transactions which calls for all banking supervisors to enact effective measures that will see to it that there are strict implementation rules and policies to be followed when making transactions (Goodhart, 2011 p140).

As stated by Galati and Moessner (2013), banking systems in the EU have not evolved to using other digitalized mechanisms for IM and secure transactions. Micro-prudential supervision used in the European Banking industry ensures that the risks of failure in individual banking institutions are limited by protecting the customers who make deposits and other transactions in the bank. In this concept, a peer-review analysis is used for monitoring transactions in individual banks and in a network, and unusual behaviors in transactions are viewed as a threat calling for immediate action (Galati and Moessner, 2013 p850). Customers get to transact under strict guidelines and there is a limitation on a global basis, since the IM means are not very efficient and reliable or cross linked.

2.3 Revisiting Customer IM in European Banking

The IM process is initiated the moment a customer opens an account with a specific bank (handing over personal information) after which they are given personalized details for identification such as account number, ATM card, and ATM pin. These are the primary credentials that are used to identify a customer in the bank. Identification processes in European Banks include: Identification, Authentication, and Authorization, as shown in the figure below (de Brisis, 2009).

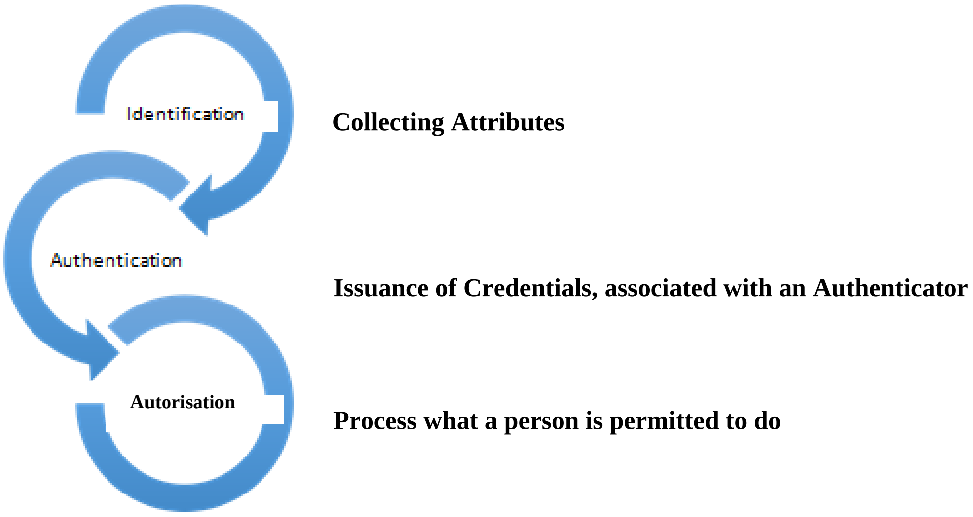

Identification
Collecting Attributes
Authentication
Issuance of Credentials, associated with an Authenticator
Autorisation
Process what a person is permitted to do

Figure 1: Customer Identity Management

i. *Identification*

Customer identification is the process of getting the true identity of a customer through an identity proofing technique that is used in vetting the customer's identity (Acques et al., 2009). The process of customer identification starts by vetting one or more attributes associated with the customer. It involves verification of all the required credentials to assert a customer's identity according to the bank records. The identity is verified electronically through a program used by banks. Processes of customer identification are done in two main dimensions:

- Information collected
- Accuracy of information and reliability

Data collected can be either from an individual with a bank account in the bank who has been given their personalized credentials or parties that have a group account with the bank or a cooperate company. Information is unique to the parties involved according to customized information. In this context, trust is a critical issue when verifying customer identity and it is of the essence that there is always a certain probability of malicious attempt. Therefore, information of a client is treated as wrong until approved. According to Acques et al., (2009), there are four main steps of verification of customer identity in EU banks.

i. The identity information that needs to be verified.
ii. The authorities involved in verifying identity.
iii. The process of identifying the information.
iv. The source of information for verification.

In the course of a transaction, it is necessary for the bank to ascertain that the transaction is being done by the certified parties without breaking any of the transaction procedures. It is essential that when a customer is transferring funds, the sender's details, as well as the receiver's details, have to be certified and matched. All factors considered it is the role of an authenticator to ensure that a transaction has met all its requirements.

ii. Authentication

Banks use authentication mechanisms to verify transactions details. It is aimed at proofing that the identity of a customer is that same as that of a person whose details are recorded with the bank (Acques et al., 2009). Authentication is done when there is a need for a customer to make a considerable sum of a transaction without use of ATM. ATM transactions only require presentation of the Card and the PIN/password which is vulnerable to frauds incase a customer shares their PIN with another person. Authentication during large transactions ensures that all details and requirements of a transaction are true. This process is focused on the behavior of a customer in making transactions. For instance, it becomes suspicious if a customer used to withdraw/deposit an average of $40-$100 and all over sudden a deposit or withdrawal/deposit of $10000 is made in the account. Such factors considered a call for a review of the account which leads to freezing of the account. Therefore, the process can sometimes be termed as biased since a transaction can be completely legitimate. In a nutshell, consistency in banking is the basis of identification and authentication in such cases.

Authentication factors are combined to increase the security of a transaction. Factors that compromise the security banking are eliminated by making it compulsory for customers to pass all the required procedures before a transaction is forwarded for approval. One-time passwords (OTPs) is a pervasive way of authenticating users making transactions online (Tellini and Vargas, 2017). For instance, when a customer needs to withdraw funds from their PayPal account to the local bank account, the authentication process involves entering an OTP sent to a customer's email address to ascertain that they are legitimate users of the account. Such procedures are set to ensure that transactions are only done by verified users.

iii. Authorization

This is the final process of customer IM during a transaction. After all the details of a customer have been verified and authenticated. Authorization is done from the bank where funds are sent to the recipient's account within a given period which is usually 3 to 5 business days in many banks (Acques et al., 2009). Authorization offers grants and privileges to a customer as the recipient or sender of funds. It mainly facilitates a given transaction and decision making depending on the information provided by the customer as well as those available in the banking records. A transaction is complete once the authorization process is over and all details of a transaction have been verified as complete and accurate.

2.4 Synthesis

The customer identification process for European Banking involves a series of processes with significant steps that make it possible to secure a transaction. IM is an essential factor, especially when making large bulks of electronic transactions with the aim of preventing fraud activities. Therefore, EU banking relies on their personalized identity management systems to maintain different user accounts prudently as shown in the figure below.

Banking institutions utilize a third generation identity management process which has a third party or a centralized model for verifying the identity of a customer (Smedinghoff, 2011). Customer data is stored in a central repository system that is used for identification purposes of the system.

To begin with, customer IM systems are federated which is used for the identification processes as a third party. Information regarding a transaction must go through the federated model for verification, authentication, and authorization. A central identity model is used by banks to keep consistent track of customer identity and their personal account information. The federated model provides a source of customer identification for banks and other financial institutions for a secure exchange of funds by customers. Once verification of customer identity is done through the federal entity, a customer will not require further verification, but transaction behavior will be put under monitoring (Smedinghoff, 2009). The customer identity model is illustrated in the figure below.

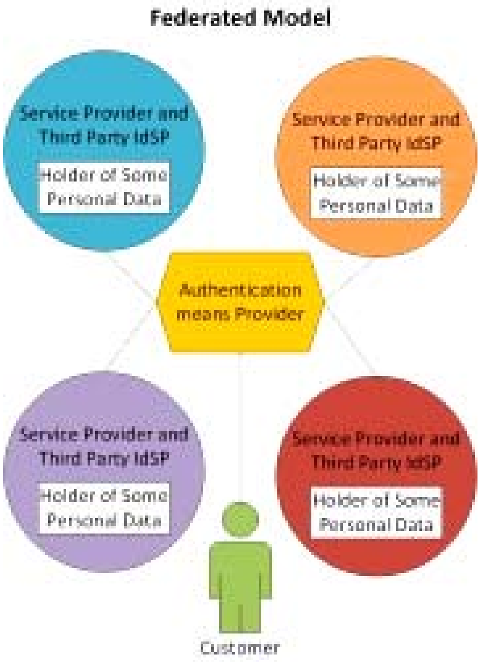

Federated Model
Service Provider and Third Party IdSP
Holder of Some Personal Data
Service Provider and Third Party IdSP
Holder of Some Personal Data
Authentication means Provider
Service Provider and Third Party IdSP
Holder of Some Personal Data
Service Provider and Third Party IdSP
Holder of Some Personal Data
Customer

Figure 2: Federated Model for Customer IM

The risks involved in the European Banking systems for customer IM include vulnerabilities to fraud activity and imposters where one can use another person's ATM card to withdraw funds. It is also important to note that there are issues regarding the amount used for transactions through EU banking sector. The use of a third party to authorize a transaction increases the amount to be paid for a secure transaction to go through. Nevertheless, this method is vulnerable to fraud activities, as intermediaries can potentially make changes to transactions for personal benefits. Individual banks have to implement different policies to ensure that all transactions through the bank are done by certified customers and that the recipient is also verified with a known identity.

2.5 Conclusions

As much as customer IM for EU banks is done through secure channels, it is imperative to note that there is the need to have a system that will eliminate the necessity of any intermediaries for the approval and clearing of transactions. Also, it is worthwhile to understand that banks are mandated with the need to enact a strict and secure policy that will ensure that details of a transaction cannot be changed in any form whatsoever. The vulnerabilities in the current customer IM in EU banks can duly be addressed by emphasizing electronic measures that will allow privatization of transactions as well as eliminating the need for central authorities as intermediaries. The actualization of such a customer IM for banks is done through the implementation of blockchain technology in the European Banking industry. It will likely have numerous advantages which will make transactions more secure and reliable and potentially even centralize KYC management with direct control for a client regarding the sharing of their personal information.

3 “Blockchain as a basis for Customer IM in European Financial Services”

This section sets out the key findings of section 2 and implements it as the basis for Customer IM in European Financial Services with a review of various block chain technologies and using Bitcoin as the case study.

3.1 Introduction

A research report by BIS (2017) indicates that application of blockchain technology in financial institutions could save up to a total of $6-8 billion annually. Furthermore, capital markets in general stand to save $50-$60 billion per annum (BIS, 2017). This is one of the reasons why blockchain technology has a high demand and potential in financial institutions as well as capital markets. Blockchain transformation faces several hurdles in its implementation phase for various financial purposes in different institutions. Organizations use large amounts of resources to research the best ways of implementing blockchain in their institutions. Use of blockchain as a technological advancement may very likely broadly benefit not only financial institutions but also other industries and businesses (McKinsey, 2016).

There is a high rate of “old-fashioned” movements of millions of funds as well as information in different global financial systems in diverse sectors around the globe. Additionally, reliance on paperwork, even if automated to a large extent, will create inefficiencies of systems which are relatively vulnerable to all kinds of fraud (McKinsey, 2016). Therefore, it is worthwhile for financial institutions to test the basic reliability of blockchain technology for their daily transactions in order to be safer from frauds and enhance general system reliability. As a general rule it is a difficult challenge for banks and other financial institutions to develop such an application due to inherent complexities as well as external regulatory issues.

The most pressing issue with developing such applications is the implementation of the technology used. It has proven a hurdle for financial institutions and capital markets as a whole. Thus, it is worthwhile to note that trends in technology are moving towards digitalization of individual assets, depositions, and netting positions (McKinsey, 2016). Therefore, banks are faced with the challenge of meeting the changing needs of their customers for a better service provision. This paper focuses on blockchain as a basis for Customer IM in European Financial Services and aims to provide details regarding challenges that banks face while implementing blockchain to support and further their financial service provision (Crosby et al., 2016).

3.2 The Blockchain Vision and how it works

Blockchain technology is a real-time distributed database that stores records of different transactions in real tim. It maintains the lists of all transactions that take place during specific times, each transaction has its time stamp, and it is stored cryptographically, hence, making it impossible to be tempered with (McKinsey, 2015). The uses of blockchain are diverse, and many institutions like healthcare, media, travel agencies and real estate adopt it. However, the highest rate of adoption is by financial institutions which invest billions of money in implementing different use cases of blockchain ranging from IPO trading platforms to payments (EPC newsletter, April 2015). Banks, in particular, find it very useful to use blockchain technology for delivery of services to their clients. In this context, a critical look at the vision and how blockchain works is essential for a better understanding of its usefulness in the global market as shown in fig 1 below.

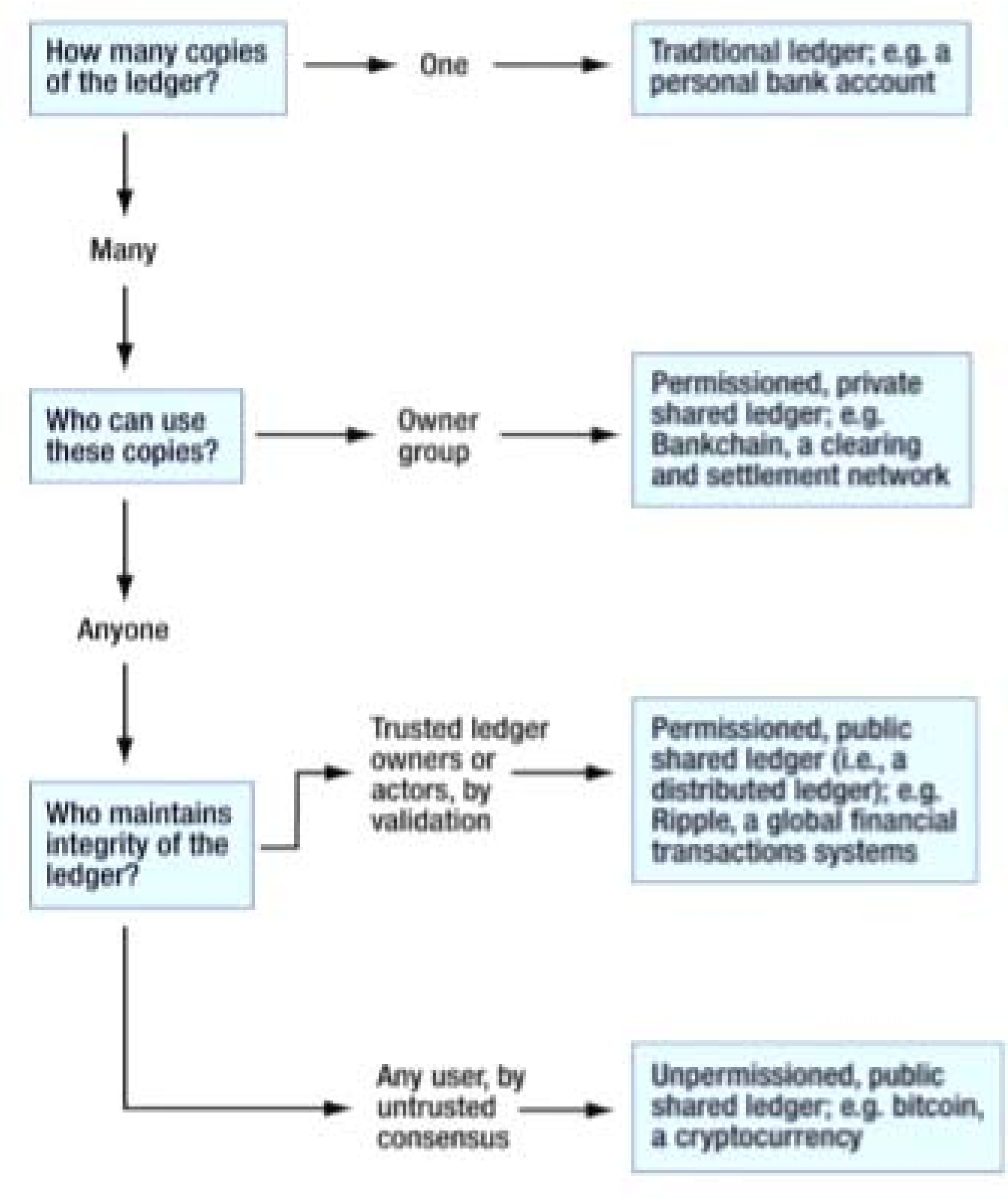

How many copies of the ledger?
One
Traditional ledger; e.g. a personal bank account
Many
Who can use these copies?
Owner group
Permissioned, private shared ledger; e.g. Bankchain, a clearing and settlement network
Anyone
Who maintains integrity of the ledger?
Trusted ledger owners or actors, by validation
Permissioned, public shared ledger (i.e., a distributed ledger); e.g. Ripple, a global financial transactions systems
Any user, by untrusted consensus
Unpermissioned, public shared ledger; e.g. bitcoin, a cryptocurrency

Figure 3: Overview of Blockchain

Source: Consult Hyperion

Blockchain technology works by eliminating intermediaries for purposes of identification, authentication, and the registration of a transaction. It does this through its unique technology with algorithms that authenticate and safeguard transactions, thus, saving an organization the need for a central authority (Una Donovan, 2016). The main vision of blockchain is to increase the saving of financial institutions by approximately 50% by eliminating intermediaries and increasing the efficiency of transaction systems as shown in fig 4 below.

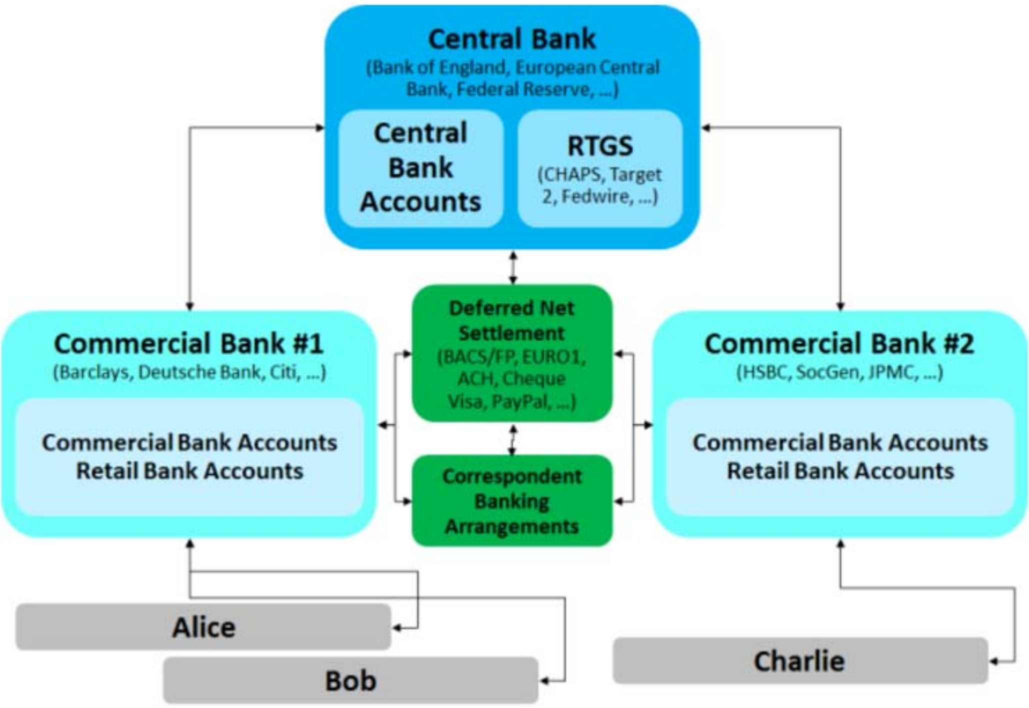

Central Bank
(Bank of England, European Central Bank, Federal Reserve, ...)
Central Bank Accounts
RTGS
(CHAPS, Target 2, Fedwire, ...)
Commercial Bank #1
(Barclays, Deutsche Bank, Citi, ...)
Commercial Bank Accounts
Retail Bank Accounts
Deferred Net Settlement
(BACS/FP, EURO1, ACH, Cheque Visa, PayPal, ...)
Correspondent Banking Arrangements
Commercial Bank #2
(HSBC, SocGen, JPMC, ...)
Commercial Bank Accounts
Retail Bank Accounts
Alice
Bob
Charlie

Figure 4: Blockchain Technology

3.3 A survey of Blockchain-related technologies

Blockchain technology uses a sequence of operational mechanisms to enable it to complete transactions efficiently (EPC newsletter, April 2015). The identification mechanisms use hash functions on values to ensure that it cannot be tempered with since it is close to impossible to interfere with the original data in any form. Therefore, there are six leading blockchain-related technologies used for crypto-currency;

i. Litecoin (LTC)
ii. Ethereum (ETH)
iii. Zcash (ZEC)
iv. Dash
v. Ripple (XRP)
vi. Monero (XMR)

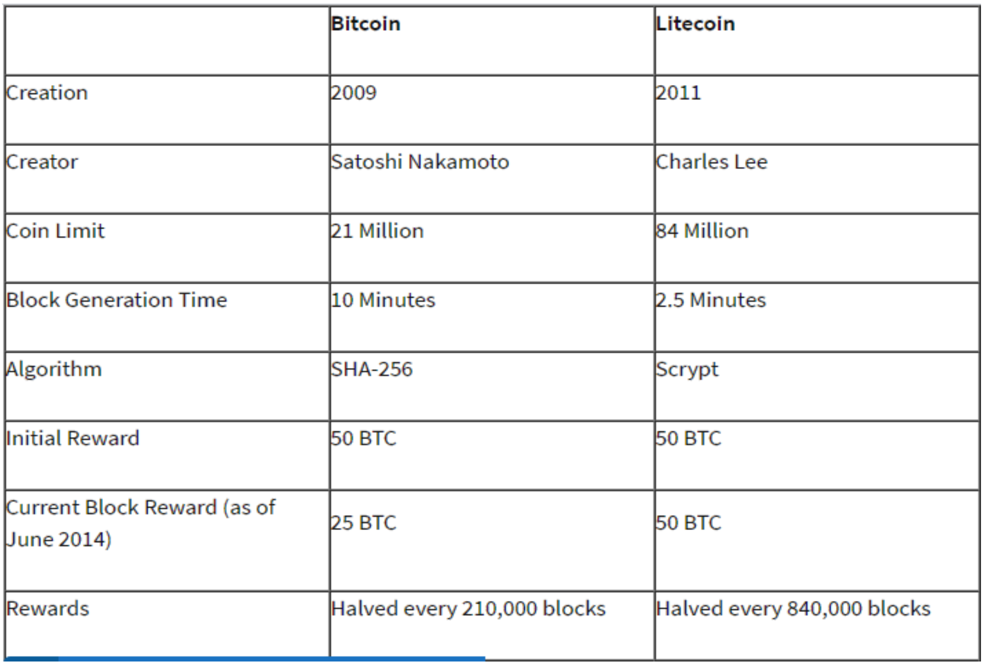
Litecoin

It is an alternative cryptocurrency that is based on the Bitcoin technology model. It was launched in 2011 by Charlie Lee, an MIT graduate. Litecoin is a global open source payment network that is independent of a central authority for control over transactions (Gandal, N. and Halaburda, 2014). The main difference between Litecoin and Bitcoin is its rate of generating blockchain, in essence, Litecoin is faster as it uses a script for Proof of Work (PoW).

It is the second largest cryptocurrency after Bitcoin, and it has significantly gained popularity in the long run as a peer-to-peer currency (Haferkorn and Diaz, 2014 p110). Litecoin is a decentralized, open source payment network that was developed with a primary objective of improving the various shortcomings associated with Bitcoin technology.

The technology has received adequate support from the industry for trade volumes and liquidity (Ahamad et al., 2013 p45). The table below shows the in detailed difference between the two cryptocurrencies.

Table 1: Differences between Bitcoin and Litecoin



	Bitcoin	Litecoin
Creation	2009	2011
Creator	Satoshi Nakamoto	Charles Lee
Coin Limit	21 Million	84 Million
Block Generation Time	10 Minutes	2.5 Minutes
Algorithm	SHA-256	Scrypt
Initial Reward	50 BTC	50 BTC
Current Block Reward (as of June 2014)	25 BTC	50 BTC
Rewards	Halved every 210,000 blocks	Halved every 840,000 blocks

Source: Haferkorn and Diaz, 2014, p110

Ethereum

It is a blockchain platform that is decentralized with the capability of presenting and maintaining the integrity of ownership of property and other valuables (Sunnarborg, 2017). Ethereum (ETH) can store contracts as a way of allowing people to move funds, create markets, store information relating to the registry or debt promises, and complete different business transactions without the need of intermediaries. It has a smart wallet that allows people to secure their funds and other assets in the form of cryptocurrency.

ETH was launched in 2015 as a decentralized software with smart contract capabilities as well as Distributed Applications (DApps) that can efficiently run with no downtime or third-party interference (Sunnaborg, 2017). In 2014, it launched its first ether that was received with adequate support in the market with an overwhelmingly positive response from users. ETH runs its applications on aether, a cryptographic token. Ethers are small segments of applications that move around the ETH platform to carry out different transactions (Buterin, 2014). Developers use ethers to execute applications inside the ETH. Etherum platform has the capabilities to *"codify, decentralize, secure and trade just about anything"* (ETH, 2015). For the security of data and other transactions, ETH is split into two main platforms; Ethereum (ETH) and Ethereum Classic (ETC) where each one is independent on its own but can share data for backup and security. Currently, ETH has a capitalization market of almost $4.46 billion which comes second after the leader, Bitcoin (Teutsch et al., 2016 p505).

Zcash

Zcash is another cryptocurrency that was ushered by Bitcoin in 2008. It is a form of alternative currency just like altcoin and 700 other alternative coins (Gupta et al., 2017). Therefore, Zcash is viewed as one of the most growing technologies in the alternative versions. They are versions of bitcoins that increase the competitive advantage of the currency in the market. Most of its operations are in the form of small market capitalization with low volume and circulations (Greenberg, 2016).

Zcash, like many other cryptocurrencies, is decentralized and open-sourced software which is very promising in cryptocurrency. Zcash itself offers a high level of privacy as well as a selective transparency of different transactions by allowing the user to choose their level of transparency. It can provide high security and privacy for all its transactions by recording and publishing them on a blockchain while keeping all the personal details of the sender and the recipient as private as well as the amount in a transaction (Greenberg, 2016).

Also, it has an advanced capability for 'shielded' transactions that encrypt content with zk-SNARK technique which is an advanced level of cryptography (Eswara, 2017). The method ensures that there is the validity of transactions with secure ledgers containing balances without disclosing any information pertaining the amount or the parties involved in the transaction. It ensures that there is no chance for anyone to steal or cheat during a transaction. In 2017, Zcash was able to raise $2 million for equity of the company from a total of 17 investors as listed below;

- Aaron Grieshaber
- Branson Bollinger
- Maple Ventures (Amir Chetrit and Steven Nerayoff)
- Brian Cartmell,
- VladZamfir
- Roger Ver
- Digital Currency Group
- Barry Silbert
- Charles Songhurst
- Fenbushi
- Shapeshift
- Erik Voorhees
- David Lee KuoChuen
- Fred Ehrsam
- Sebastian Serrano
- Li Xiaolai.

16.4% of the company is currently owned by investors who are part of the management board. Zcash offers only 10% of $21 from the total monetary base, and the remaining 90% is offered to the miners. It sells its coins to investors at around $15.24 per coin, Zcash has managed to distribute a total of 131,250 coins to its investors. On October 28, 2016, Zcash was launched, and up to now, it has hovered $226 mio (Greenberg, 2016).

Dash

It is regarded as the most secretive version of Bitcoin, and it was originally known as 'Darkcoin' since it has a high level of anonymity. Dash works on a decentralized "*master code network"* which makes all of its transactions untraceable (Eswara, 2017). It was launched in January 2014, and since then, it has experienced a massive increase of users in a significantly short span of time. Its developer, Evan Duffield, designed it with the capabilities of using CPU and GPU in mining. Up-to-date, Dash uses advanced technology such as Darksend and InstantX for sending and receiving transactions in a secretive manner.

Ripple (XRP)

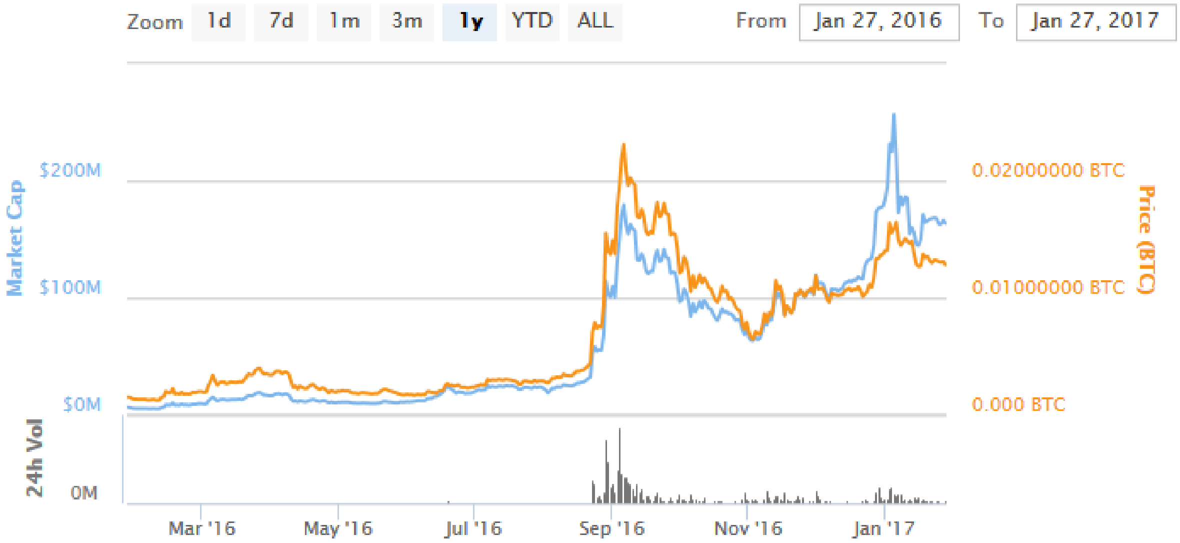
Ripple is a term that was used by the author of "The Dow Theory," Robert Rhea in describing the daily fluctuations in the stock market prices (Eswara, 2017). According to Rhea (1932), there exist three simultaneous fluctuations in stock market prices that can be compared to tides, waves, and ripples. Rhea (1932) also points out that there are investors who find their success from the existing fluctuations in the stock market.

Ripple has originated from the idea of the Dow Theory by simulating the simultaneous movements in prices. From the simulations, traders can see the trends in the stock market prices and make investments that will attract profits. Most profits are obtained from short-term price fluctuations rather than the long-term price movements. Ripple allows investors to make their fortune through trading.

Monero

It is a technology that is based on the "dark-web", where most black markets are outside the reach of the law. Most of the marketplaces on the "dark-web" require digital currencies to enable them to avoid detection and allow them to exchange their illegal goods and services without being detected monetarily (Miller, et al., 2017). In this context, Bitcoin has been greatly used for such transactions. However, concerns about the total anonymity of ripple have constantly been put in question. It is worthwhile to note that, a dark market, Silk Road, used Bitcoins for its transactions but it was shut down by the FBI after a transaction through Bitcoin was traced back to the website. Therefore, Monero has come as a replacement of Bitcoin in the black market due to its ability to prevent the traceability of transactions (Miller, et al., 2017).

Monero is one of the best performing cryptocurrencies in 2016 regarding its market price. The term ‘monero” means coin in Esperanto, hence, its coins are referred to as moneros. One monero is currently trading at $12 in the dark market, and its use is constantly growing in size since there is a high rate of black market business online. The figure below shows the performance of Monero from March 2016 to January 2017.



Source: CoinMarketCap, 2017

The anonymity in Monero's transactions is achieved by addressing the various vulnerabilities associated with Bitcoin (Noether, 2015 p1098). The protocols in Monero are more disguised and untraceable. For instance, "stealth addresses" are used to obscure the wallet balances of Monero. Also, it mixes up the different transactions of many users together using a mechanism called "ring signatures" which makes it utterly impossible for one to make any conclusive analysis of the flow of money during forensics (Noether, 2015 p1098). Also, users transacting over monero, can easily change the funds into any currency in the market without facing any unnecessary inconveniences, thus, attracting a large number of users periodically.

3.4 Case Study: Bitcoin as an Application of Blockchain IM capability, with particular focus upon Customer IM

Bitcoins are virtual currencies that are distributed across the globe without the need of external management like banks, and it uses the software technology to discover its value. Satoshi Nakamoto (2008) observed bitcoin as a "*A Peer-to-Peer Electronic Cash System*" with the following characteristics:

- It allows individuals to do a direct transaction of money without third parties.
- It prevents reversing of transactions
- It reduces the charges for making small transactions.
- It prevents double-spending

The use of bitcoin officially commenced in 2009, and it has greatly increased its number of users. It is a very efficient system with no downtime and can be used anywhere in the world which makes it even more efficient and theoretically reliable (to a large extent). Transactions through bitcoin are traceable which gives it a unique feature that being increased security and speed of funds in transactions.

Bitcoin uses different technologies to create new functions for application and security (Andreessen, 2014). It has put in place some measures that will prevent falsification of information and duplication of payments by users. Also, there are measures to prevent attacks by hackers. Therefore, it has employed different technologies (such as; public key cryptography, hash, P2P, and proof of work) to ensure the safety of data in the system (Back, et al., 2014). It is important to look at the blockchain mechanism used in the proof of work technology to understand the use of blockchains in customer IM.

Proof of work is a form of identification mechanism that ascertains that a particular transaction is genuine. It is a form of verification that is done on transactions to prevent falsification and duplication of payments. PoW uses the hash function to compare values of transactions for verification and correctness. Data mining is also used to extract valuable data for different transactions to use as reference points. Bitcoin technology is highly suitable for customer IM by using mining operations. Mining allows users to secure their transactions by using sidechains which is an alternative to blockchains. Therefore, application of bitcoins in customer IM comes into realization when blockchains are used in financial sectors to provide customer services in a trusted platform where customers can securely do their transactions without the need of intermediaries (Back et al., 2014).

The technology used in Bitcoin is based on some blockchains interoperated together to allow easy movement of assets between different chains. In PoW, side chains are used to ensure that there is the security of user transactions by isolating different transactions for the security of payments (Back et al., 2014). For verification of customer identity, and security of transactions, side chains are used to handle only a certain amount of funds while the rest is left in a blockchain. Therefore, not all the available funds are exposed to risks of loss or malicious attacks. The internet plays a significant role in implementing the use of bitcoin technology for customer IM. It is a system innovation that uses no regulatory or permissions in both the public and private sector. Adoption of the technology has become relevant in the current business trends to enhance service delivery with minimum or no expenses on the middle authorization.

According to Hanseth and Lyytinen, (2010), Bitcoin as an information structure that meets the definition of *"a shared, open and unbounded, heterogeneous, and evolving socio-technical system consisting of a set of IT capabilities and their user, operations, and design communities."* With its diverse characteristics, it can be highly placed in a position for customer IM in financial institutions. Some of the unique features that make bitcoin suitable for customer IM are illustrated in the table below.

Table 2: Description of Bitcoin

Feature	***Description***
It can be shared	The technology is universal across all platforms in IT with many capabilities. It is universally shared among users regardless of geological location as long as there is the internet connection.
open source	Bitcoin allows unlimited connections by all users with multiple capabilities; any user is allowed to use bitcoin.
It is a heterogeneous technology	It increases/or expands technically and socially with some applications being generated across different platforms such as; altcoins, side chains, and Ethereum (wood, 2014)
Evolves	It is not limited to time or the users; it keeps on evolving where technology is continuously adopted in other systems with more functionalities and applications.
It has different organizing principles	Bitcoin is recursive with a composition of different IT capabilities, operating on different platforms, and having the different infrastructure, a good example is the different wallets, altcoins, and other platforms like Ethereum respectively (Poon and Dryja, 2015).
It has different controls	Since it is a distributed system, it requires dynamic negotiations among users to make it acceptable in the community.

The operation of bitcoin as a digital platform forms the basis of this research with the aim of understanding the applicability of the blockchain technology in improving customer IM in banks and other financial institutions across Europe. As defined by Kazlan et et al., (2014), bitcoin is highly reliable as a digital platform with the interplay of governance reliability of safe transactions which makes it suitable for use in customer IM. Adoption of the technology by European banks will ultimately reduce the cases of fraud activity as well as safe time and administrative costs, hence, maximize savings.

3.5 Summary of key points

From the discussions in this paper, a summary of the main points highlighted from different topics above can be done.

i. Blockchain vision is to eliminate the use of intermediaries in processing transactions by providing a platform where users can transfer assets from different regions safely and efficiently.

ii. The main competitive block-chain related technologies include ICOs and Ethereum which have evolved from the bitcoin technology.

iii. Bitcoin has taken the financial world by storm through making it possible for people to do their transactions safely from anywhere, anytime without the need of intermediaries.

3.6 Comparative Review Synthesis

Blockchain technology is a concept that has greatly received attention in the financial technology (FinTech) area and is a tool to be used to coordinate efficient transactions across different platforms. It is a combination of various technologies which include a distributed storage system, point-to-point transmission, and different encryption algorithms (Guo & Liang, 2016). It has come out as a fundamental breakthrough in the storage and transmission of data in different business platforms. According to Mu Qi-Guo (2016), blockchain technology is the point of transformation in the corporate finance and economic sector by implementing new methods in the existing models that will push towards the achievement of secure and reliable transactions.

There have been various breakthroughs in implementing blockchain technology in international institutions such as the United Nations and the International Monetary Fund (IMF), using digital currency (Guo & Liang, 2016). Countries like the US, UK, and Japan have greatly explored different blockchain technologies and their applicability in different fields such as banking and capital markets. Initiation of the technology has also been done in countries like China, India, Russia, and South Africa. Report findings indicated that in February 2016, China's leading bank; The People's Bank of China announced the possibilities of adoption of digital currency using blockchain technology, pointing to its efficiency in making unlimited transactions across the globe (Guo & Liang, 2016).

There is a high rate of optimism regarding the use of blockchain technology in banking (Pilkington, M., 2015).There has been positive feedback from major financial institutions towards the different application of blockchain technology with significant emphasis being placed on its use to reduce operational costs in making large transactions (Pilkington, M., 2015). Therefore, it is worth noting that the banking industry stands on high ground as a beneficiary of blockchain technology. The European banking sector can greatly benefit from blockchain technology in customer IM and processing large transactions.

3.6.1 Summary key points Literature Review

- Blockchain is a breakthrough in storage and transmission of data across financial institutions
- Blockchain brings a transformation of the existing models in the finance sector

- Blockchain is very suitable for financial institutions such as banks since it increases the security of transactions while reducing operational costs during transactions.
- European banks stand a high chance of benefiting from a regulated blockchain technology for customer identity management and completion of different transactions.

3.6.1.1 Advantages

- Blockchain technology will reduce operational costs by making transactions
- Adoption of Blockchains by the European banks will allow easier and efficient identity management for customers, hence, enhance the security of doing transactions.
- Blockchains are efficient and reliable in doing transactions across the globe.
- It results in limitless financial innovations and diversification of different investment opportunities and financing.

3.6.1.2 Gaps/disadvantages

- It does not cater for IT illiterate customers yet
- When there is insufficient information on customers, it leads to challenges when processing credits.

3.6.3 Answer to RQ 2 & 3

Advantages	**Disadvantages**
Efficient and reliable in doing transactions	Does not cater for IT illiterate customers
Limitless financial innovations and diversification of different investments	Insufficient information on customers, it leads to challenges when processing credits
Allow easier and efficient identity management for customers for data security.	
Reduce operational costs in making transactions	

3.6.4 Revisiting the diagrammatic overview of section 2

Fig 2 should be changed by having an identity management mechanism to allow users to verify their identity through a proof of work (PoW) system to ensure that transactions are done in a secure manner as shown in fig 3 below.

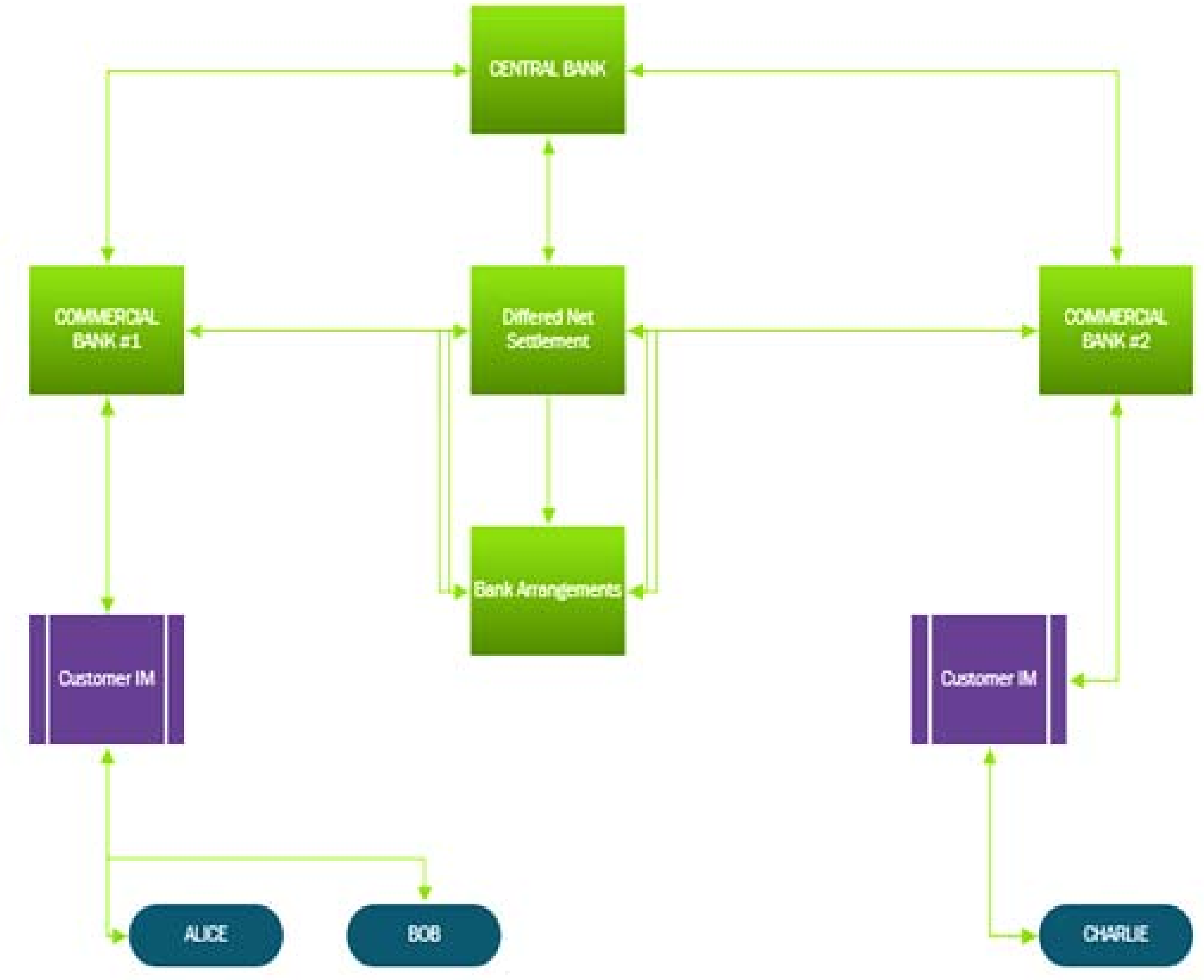


Fig 3: Blockchain with customer IM system

4 “Regulating a Blockchain Customer IM Infrastructure”

Blockchain in customer IM has played a significant role in enhancing the efficiency of processing transactions through a secure platform. The IM infrastructure in financial institutions uses blockchain technology in different dimensions. It has optimized the potential profits of financial institutions by eliminating the need for having a centralized body to manage customer IM. However, there are cases of irregularities in blockchain technology, involving the legalization of transactions. Meaning, ensuring that all transactions are legal, compliant with the respective countries laws and that the customers or users are protected from potential systemic or legal deficiencies.

It is, therefore, a necessity to ensure that all transactions through any blockchain based IM infrastructure are regulated and have met all legal requirements. All financial institutions and other entities (such as blockchain platform and/or solution providers) have to make sure those legal requirements are then introduced into the respective platforms.

In the United States for example, the Financial Crimes Enforcement Network (FinCEN) has enacted certain guidance, rulings, enforcements that provide a basis of regulations for banks and other institutions (Kiviat, 2015 p569). The Bank Secrecy Act (BSA), for example, mandates banks and other financial institutions to have registrations and recordkeeping requirements for customer IM. These regulations mandate banks to have the records of customers registered in the Department of Treasury for effective countering of money laundering and other fraud activities (Linn, 2010 p407).

Customer IM programs are initiated by different financial bodies with the aim of enhancing the security of customer transactions in different platforms. In March, 2013 FinCEN regulations mandated that the regulatory rules and procedures to be applied to all participants including the ones who make transactions that are "virtually convertible" (Kiviat, 2015 p569). The virtual currencies imply the ones that do not have any legal jurisdiction in any environment and only acts as a substitute to the actual currency in given environment or one that has the same value to a given currency. Regulations mandate that these currencies must meet the IM requirements for prevention of money laundering (Linn, 2010 p407) and thus it is of importance that existing laws and regulations are and can be streamlined to blockchain IM platforms as the security of the technical least well versed citizen can still be guaranteed to an extent.

FinCEN regulations mandate all money exchangers and administrators to be subjected to all the regulatory requirements for secure transactions. For instance, in Bitcoin, there are "Exchangers" who exchange their real money for virtual currencies while "Administrators" who are the people who have the virtual money and put virtual money into circulation in Bitcoin (Hamburger, 2015 p207). Additionally, exchangers and Administrators are subjected to recordkeeping and registration through the departments of treasury.

Further, it is important to mention that, in 2014, FinCEN enacted laws governing blockchain transactions (Network, 2014). It requires all financial institutions to have proper measures that will protect end users from any additional fraud activities.

In the European Union the above mentioned is taken care of by the European Banking Authority (EBA), in close cooperation with FinCEN and other agencies around the globe. One of the EBA's main and most important oversight responsibilities is to detect and analyze trends, possible risks and weaknesses stemming from the micro-prudential level, across borders and segments with the goal of safeguarding the systematic functioning and integrity of financial markets and the stability of the financial system in the EU (EBA, 2017).

Decentralization of blockchain as a public key that will be used to provide users with a secure digital identity which again can be used for all types of transactions has a long way to go until it could be established in such an open way, as originally intended, and regulators are well aware of the costs and hurdles for law giving entities to make that experience comparatively safe for all kinds of end users. At the moment those functions, with integrated systems, in banking networks and such, are still taken care of by those institutions in the respective legal frameworks. If, as mentioned above, those blockchain based technologies become more open and system relevant in terms of transaction sizes etc., regulators will have much work and costs to deal with in order to adapt the structures.

Today, regulations mandate that all financial institutions have to ensure that all users have been registered with the various bodies of the respective federal governments to ensure that criminal activities are not promoted through blockchain technology. Thus, the IM process forms the basis of identifying wanted criminals and criminal organizations and their funders as well as prevents unlawful conduct. Such transactions are frozen to eliminate the promotion of criminal acts (Claxton, 2011). It is essential for banks to have crucial knowledge of their customers as well as all their transactions.

4.1 Role of regulatory authorities in Customer IM systems (traditional)

Regulatory bodies have an important role in Customer IM systems to ensure that all transactions are done by certified parties. One of the mandates of conventional regulatory agencies in European Banking is to ensure that customer identity is established in every part of a transaction through the network (Casu, 2003). Customer IM is used as the foundation for regulating transactions in European banks. The various regulatory authorities have important roles in ensuring that transactions meet all the legal mandates from both the sender and recipient. Organizations and other bodies are subjected to several rules and procedures that have to be achieved accordingly, resulting in the protection of all participants in the system.

Main Roles of Regulatory Authorities:

Legislation

The European Banking Authority (EBA) provides a legal background for a conducive personal and business environment for customers. It is important that all transactions in the EU banking industry meet all the legal entities in financial banking. An essential factor is customer identity; it has to be verified and authenticated. For users to make any transactions through the bank, they have to be fully validated as customers (EBA, 2016). The legal requirements of a transaction include making sure that funds are not sent with an aim to support criminal bodies or organizations and other illegal activities.

Account Auditing

It is the role of regulatory bodies to do auditing of various accounts for transparency in transactions and promoting high security standards in banking. Every account in the bank is subjected to auditing by the regulating bodies for verification of details of an account holder. Part of auditing processes includes identification and verification of user details, cross-checking transactions, and identification of recipient accounts. The auditing procedures are mandatory for all accounts; it is meant to track transaction behaviors of a customer for easy identification of suspicious activities (Casu, 2003).

Prevent Money Laundering and Curb Financial Terrorism

One of the major objectives of the European Banking Authorities is to ensure that there is integrity, transparency, and an orderly functioning in the financial market. Regulatory bodies have a mandate to ensure that institutions that offer banking and other financial services are competent, credible, and legitimate (Casu, 2003). It is the role of regulatory bodies to curb cases of money laundering through fraud activities. The legislation is effectively applied under the European Anti-Money laundering and countering the Financing of Terrorism (AML/CFT) directives. To enact the different set of laws, regulatory authorities like the EBA can discharge functions through:

- Fostering and facilitation of co-operation within different AML/CFT bodies of EU member states.
- Promoting the development of common goals and understanding among regulatory bodies by having close working relations with ESMA and EIOPA bodies to ensure that potential risks associated with banking are curbed.
- Working with other regulatory bodies through a joint committee to facilitate delivering of its mandate as per the (EU) 2015/849 and (EU) 2015/847 directives, which are policies to safeguard the financial system.

Consumer protection

Banking is a very sensitive matter in general which requires control, integrity, fairness, and transparency for all consumers when making financial transactions and using other services in the same contextual framework. Regularity authorities play a significant role in fostering consumer protection when making transactions for products and services. They ensure that the various detriments and potential risks faced by consumers are duly addressed in order to ensure that every transaction is done with a certified party to prevent cases of loss of frauds. According to EBA (2016), regulatory authorities carry out their activities by collecting, analyzing, and reporting on consumer trends to easily detect and prevent fraud activities that might compromise consumer protection rights. Also, it is the role of various regulatory bodies to facilitate "*reviewing and coordinating financial literacy and education initiatives; developing training standards for the industry; contributing to the development of common disclosure rules; monitoring existing and new financial activities; issuing warnings if a financial activity poses a serious threat to consumers and obstruction of laid down regulations" (EBA, 2016).* To enhance consumer protection, EBA goes ahead to confine various transactions that pose a threat to consumers through violation of the regulations and acts enforced by the regulatory bodies.

4.2 Relevance in Blockchain based systems

Blockchain as a distributed ledger system will replace current regulatory bodies in the financial services sector entirely. Indeed, that would seem to have been the vision of the originators of the technology back in 2009/10.

Currently, different financial systems have only just started adopting the blockchain technology as a fractional replacement for the existing regulatory bodies for efficient and secure transacting.

Additionally, there is an increase in businesses using the Internet of Things (IoT) in different financial sectors like; banking, insurance and reinsurance, therefore, blockchain technology has been adopted by such institutions as an efficient regulatory body instead of the more traditional systems (Peters and Panayi, 2016 p240). With reference to the replacement of traditional regulatory bodies with blockchain technology for faster, easier, secure, and efficient transactions, fraud management is also an essential factor that can be supported and controlled by blockchain technology. Many banks have implemented the blockchain technology for digital identity as far as cases of transactions, payments, and contracts are concerned, not so however for customer KYC data management per se (Peters and Panayi, 2016 p240). Furthermore, information management is another significant aspect of implementation of blockchain technology especially in other aspects of the industry. Fundamental factors regarding replacement of regulatory bodies by blockchain technology are a milestone towards improvement of financial services across the globe with minimum worry of the safety and security of funds.

The systems have greatly transformed the financial industry by eliminating the need for third parties as intermediaries in various transactions. The verification, authentication, and authorization of customer transactions can be done through a distributed ledger. Customer identity management is done through unique proofing mechanisms such as Proof of Work (POW) which ensures that transactions are done by verified customers.

The relevance of blockchain financial institutions is huge, and the advantages that come with it are enormous (Guo & Liang, 2016).

Increased Efficiency in Business

Blockchain technology has significantly increased the efficiency in the financial market by an elimination of central channels of authorities in business (Pilkington, 2015). The blockchain framework eliminates issues in the existing financial institutions which experience high verification costs for transactions (Guo & Liang, 2016). Below the the line, in the experience of the author, we did not yet arrive at the point of severe efficiency gains, as the new technology still needs to be fully integrated and all parties need to do so on various levels. Nonetheless, the potential certainly is in the process of being proven and use cases become more and more.

Creation of New Markets

Blockchain technology has opened up a spectrum of new market opportunities by creating room for reengineering of different economic models that were in existence in order to promote or enhance the sale of previously unprofitable goods or services (Pilkington, 2015). It has the capabilities of establishing digital identity in an efficient and cost-effective manner which creates room for inclusion of previous consumer segments that remained underserved with minimum attention or priority (Lee, 2017). Implementation of blockchain technology has boosted business processes by providing opportunities for new markets that expand existing and provide a testing ground for new business models which will expedite the processes of adopting new technologies in the financial sector (Lee, 2017).

Anti-money laundering and customer identification programs

In 2011, banks and other financial institutions were faced with an increased cost of 53% in the enforced regulatory compliance that safeguards money laundering which saw many banks pulling out from other markets (McKinsey, 2016). Such activities have a significant effect on the economy and need to be addressed with great measures. In this context, blockchain technology has the potential to completely transform the banking industry by providing an automated way of storing financial information and eliminating the errors associated with manual storage and auditing procedures, thus, increasing efficiency, reduce identification and reporting costs, and enhance advanced regulatory oversight for future transactions.

Blockchain likely has the potential to help many banks and financial institutions to reduce money laundering by having all information relating to specific transactions stored in distributed ledgers with time stamps which eliminate the possibility of counterfeiting a transaction. Making transactions through blockchains has become more secure, transparent and, cost-effective for consumers by having professionalized validation of transactions. Customer IM has also been greatly boosted by blockchain through having various mechanized frameworks that work together to verify, validate, and authorize a customer to make a transaction (Smedinghoff, 2011). Through various regulations, it is mandated that all information of a customer to be kept in an accessible database. It has allowed all end users to have complete control of personal identity, reputation, and assets in a secure environment.

4.3 New problems in the Blockchain system

Use of distributed ledger technology is a new concept that is still in the process of evolution and naturally it is bound to face some significant challenges during its implementation.

Challenges faced by blockchain technology can be put into three categories: technical, regulatory, and institutional, according to the context of a problem (Guo & Liang, 2016). The original idea of blockchain technology does not really have high chances of survival in the financial sector. There are a lot of challenges that compromise the safety and soundness of transactions, this being a fundamental aspect here. The financial sector is presumably faced with uncertainties on whether to fully adapt the technology for daily business transactions. Many aspects of the technology in customer identity management are suitable for adoption especially by retail banks (Guo & Liang, 2016). However, there are regulating issues, threats, and vulnerabilities that compromise the safety of using blockchain technology. Many argue that the full adoption of the technology is a highly difficult issue due to technological integration and uncertainty issues.

Technical

This brings out the issues of complexity of the technology. Blockchain uses an entirely new language and mechanisms for operation. Thus, not many are able to understand it effectively which normally leads to rejection, slow implementation, and mostly occurrence of collateral errors (Kiviat, 2015 p.569). Despite the existence of several efforts of making glossaries for use, the level of complexity is still a challenge to many.

Blockchain technology is faced with various technical problems that have slowed down its adoption processes in the industry. To begin with, the scalability f transaction speeds in a distributed ledger cannot be ascertained in permission fewer systems such as Bitcoin (Kiviat, 2015 p.569). Secondly, there is no sure way of ascertaining the interoperability of blockchain technology with other existing systems for efficient transactions as well as knowledge of the costs for making a transition from one distributed ledger to another. Thirdly, it is worthwhile to note that the blockchain technology can be prone to cyber-attacks which have great implications for the integrity and security of transactions, funds, and user data (Kiviat, 2015 p.569). Lastly, the privacy customer data is very essential in financial institutions which call for adequate measures to protect it from loss or access by unauthorized people.

Regulatory

The legal framework behind use of blockchain technology has not been well stated. This is due to the jurisdiction behind the technology in the essence that there is no clear definition of territorial boundaries and liability in case anything goes wrong during a transaction. The fact that there is no central administration for a distributed ledger makes it clear of any applicable laws or jurisdiction (Kiviat, 2015 p.569). Therefore, the fact that it is not under any jurisdiction makes the technology very unsuitable for important business transactions which minimizes the likelihood of being adopted by financial institutions.

The technology suffers from a clear framework that will ensure that it meets all the statutory requirements of transactions. For instance, a report by the Cambridge Center of Alternative Finance (2017) indicates that more than half of the transactions through Asia-Pacific, Europe, and Latin America did not have any official government authorization. Therefore, the need to set up a clear and consistent framework for formal approval of transactions. It is complicated to design a blockchain that is relevant globally and can be adopted by all governing bodies.

4.4 Summary: Can regulators support with integrating 2 and 3

It is possible for regulators to promote the integration of relevance of blockchain technology and the problems faced with and by blockchain. It has the potential for a future Joint regulatory body between consumers, regulators and financial institutions to be structured. The aim of integrating is to provide a clear and concise means of transacting through a secure and transparent platform.

4.5 Answer to RQ 4 and discussion

Clearly, considering the inefficiencies of the existing system and the potential of the new, blockchain based system with its variety of possibilities, it is comparatively certain that the system inherent deficiencies of blockchain based systems can only be counterbalanced by regulatory bodies being involved on behalf an for the best of society. Conclusively, the inclusion of regulators would result in an efficient, secure, and reliable digital IM body (McKinsey, 2016).

The regulatory issues that affect blockchain technology can be integrated with Anti-money laundering and customer identification programs. The core principle here is to ensure that all transactions done through blockchains are transparent and orderly. In the context of making a transaction orderly, it is fundamental that the governing bodies authorize transactions to be done by the parties involved (McKinsey, 2016). With the support of governments, it is possible to have a consistent way of identifying customers from different continents of the world as well as preventing money laundering. Further, the technological challenges of the system can be integrated with the creation of new markets. By exploration of the various challenges faced by the technology, it is possible to reengineer different technologies that will provide increased technical aspects of the system. Many systems can be adopted to provide improved services to consumers. Moreover, evolution in technology is a crucial factor in developing a system, and it usually explores the challenges faced by one system to establish a better system that will cater for the various needs of the existing one. Therefore, new market products can be introduced through the existing one.

5 Conclusions and future work

5.1 Main answers to RQs

1. What are the main features of a digital identity management system infrastructure based upon blockchain for distributed, peer-to-peer financial contracts in European retail banking?

The main features identified for identity management infrastructures are: security, privacy, and usability.

Blockchain technology would strengthen security in the long run, as it would allow parties to transact with each other, without having to completely trust each other, if there is a permissioned blockchain system in place. In terms of privacy, why do we have to register again and again with all kinds of financial institutions and cannot share information selectively. Moreover, in terms of usability it is to mention that the complexity in existing systems may very often be overwhelming for the client in terms of his personal data being unmanageable for the average user. All of those issues could potentially be solved, at least to an extent, by establishing an identity management infrastructure based on blockchain with a core entity or core entities that are permissioned in order to control system inherent flaws.

2. What are the benefits of a digital identity management system infrastructure based upon blockchain for customers of European retail banks compared to the traditional identity management system?

3. What are the disadvantages of a digital identity management system infrastructure based upon blockchain for customers of European retail banks compared to the traditional identity management system?

Advantages	**Disadvantages**
Efficient and reliable in doing transactions	Does not cater for IT illiterate customers
Limitless financial innovations and diversification of different investments	Insufficient information on customers, it may lead to challenges when processing credits
Allow easier and efficient identity management for customers for data security.	
Reduce operational costs in making transactions	

4. In light of the advantages and disadvantages of digital identity management technologies based upon blockchain, can the system be managed effectively on behalf of society without the intervention of central regulatory authorities?

Clearly, considering the inefficiencies of the existing system and the potential of the new, blockchain based, system with its variety of possibilities, it is comparatively certain that the system inherent deficiencies of blockchain based systems can only be counterbalanced by regulatory bodies being involved on behalf of and for the best of society.

5.2 Limitations

The suggested solution concentrates on a permissioned core system in order to be transparent and forego system flaws as much as possible.

It does not supplement existing validation processes to an extent, as for example Customer Due Diligence (KYC) would not have to be repeated over and over again. Additionally, there would be a regulatory entity involved, which will lead to swifter and more secure technology adaptability. The suggested solutions however cannot completely foresee technological developments and the research integrated could not keep up with publications and new use cases coming out in the course of writing this paper.

5.3 Future research

Due the potential for new players in the system and the exchange of highly sensitive data being in the core of blockchain usability in finance, questions about legislative issues arose, in connection with the involved costs of adapting existing reporting and regulatory standards on the one side as well as the cost of making the technical and technological infrastructure available and secure.

Furthermore, the attempt of setting up central bank owned cryptocurrencies is made and the question of what is to happen/what the implications are to/for retail banks is a question which may be of great interest to theorize about.

Moreover, there is a large potential for future research being done about the variety of applications or potentially new application of blockchain popping up each week.

5.4 Summary

To summarize the above written, it is important to mention that the blockchain in the financial sector, certainly is here to stay and that the author deems it proven that at the end regulatory entities will have an important say about which direction further technological developments will take. This may, as stated, contradict the original idea, but at the end the challenge is integrating a new technological path, around 8 years old, with an organically developed, highly complex banking system which dictates our daily lives to an extent which can hardly be underestimated over at least the last 100 years.

This can hardly happen without a regulatory supervised system to counterbalance inefficiencies and flaws of a new technology in its integration phase as our identities and digital identities for that matter certainly are the most precious wares we have on offer and thus those should be protected accordingly and at the end should be under our full control. This certainly is a promise held by blockchain and we will see fast if this technology can be turned into something serving the client as well as coporations and state equally.

6 Bibliography

Accenture Study (2013). The future of identity in banking. Retrieved 06.10.2017 from: https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_9/Accenture-Future-Identity-Banking.pdf

Ahamad, S., Nair, M. and Varghese, B., 2013. A survey on crypto currencies. In 4th International Conference on Advances in Computer Science, AETACS (pp. 42-48)

Andreessen, M., 2014. Why Bitcoin Matters. Retrieved 05.09.2017 from: https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/

Antonopoulos, A.M., 2014. Mastering Bitcoin - Unlocking Digital Cryptocurrencies. O'Reilley Media Inc.

Back, A., 2001. Hash cash: A partial hash collision based postage scheme. Retrieved 06.09.2017 from: http://www. hashcash.org

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., Wuille, P., 2014. Enabling blockchain innovations with pegged sidechains. URL: http://opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains

Bank of International Settlements, 2017. Distributed ledger technology in payment, clearing, and settlement: an Analytical framework. ISBN 978-92-9259-031-4

Bhasin, M.L., 2016. The Fight Against Bank Frauds: Current Scenario and Future Challenges. Ciencia e Tecnica Vitivinicola Journal, 31(2), pp.56-85

Bitcoin: A Peer-to-Peer Electronic Cash System. bitcoin.org (2008). Retrieved 01.09.2017 from: https://bitcoin.org/bitcoin.pdf

Bitcoin Vocabulary. bitcoin.org (2017). Retrieved 06.09.2017 from: https://bitcoin.org/en/vocabulary

Casu, B. and Molyneux, P., 2003. A comparative study of efficiency in European banking. Applied Economics, 35(17), pp.1865-187

Claxton, N., 2011. Progress, Privacy, and Preemption: A Study of the Regulatory History of Stored-Value Cards in the United States and the European Union. Ariz. J. Int'l & Comp. L., 28, p.501

Crosby, M., Pattanayak, P., Verma, S., and Kalyanaraman, V., 2016. Blockchain technology: Beyond bitcoin. Applied Innovation, 2, pp.6-10.

de Brisis, K., 2009. The role of digital identity management in the internet economy: A primer for policy makers. OECD, 2009. Retrieved 20.11.2017 from: https://core.ac.uk/download/pdf/30684947.pdf

DiVanna, J.A., 2004. The future of retail banking. Palgrave Macmillan, New York.

Easton, C., 2017. European Union information law and the sharing economy. In EU Internet Law (pp. 163-181). Springer, Cham

European Banking Authority (2017). Retrieved 18.09.2017 from https://www.eba.europa.eu/about-us

Elsinger, H., Lehar, A. and Summer, M., 2006. Systemically important banks: an analysis for the European banking system. International Economics and Economic Policy, 3(1), pp.73-89

Ernst and Young (EY) Study (2016): The relevance challenge: What retail banks must do to remain in the game. Retrieved 06.10.2017 from: http://www.ey.com/Publication/vwLUAssets/ey-the-relevance-challenge/$FILE/ey-the-relevance-challenge-2016.pdf

Eswara, M., 2017. Cryptocurrency Gyration and Bitcoin Volatility. Retrieved 06.11.2017 from: http://www.ijbarr.com/downloads/1908201732.pdf

Galati, G. and Moessner, R., 2013. Macroprudential policy–a literature review. Journal of Economic Surveys, 27(5), pp.846-878

Gandal, N. and Halaburda, H., 2014. Competition in the Cryptocurrency Market. Retrieved 10.11.2017 from: http://www.banqueducanada.ca/wp-content/uploads/2014/08/wp2014-33.pdf

Geiling, L. (2016). Distributed Ledger: Die Technologie hinter den virtuellen Währungen am Beispiel der Blockchain. Retrieved 06.09.2017 from: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2016/fa_bj_1602_blockchain.html

Goodhart, C.A.E., 2011. The changing role of central banks. Financial History Review, 18(2), pp.135-154

Government Office for Science ‘FinTech Futures: The UK as a World Leader in Financial Technologies’ (2015). Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf

Greenberg, A., 2016. Zcash, an untraceable bitcoin alternative, launches in alpha. Retrieved 30.11.2017 from: https://www.wired.com/2016/01/zcash-an-untraceable-bitcoin-alternative-launches-in-alpha/

Guo, Y. and Liang, C., 2016. Blockchain application and outlook in the banking industry. Financial Innovation, 2(1), p.24

Gupta, S., Lauppe, P. and Ravishankar, S., 2017. A Blockchain-Backed Central Bank Cryptocurrency. Retrieved 10.10.2017 from: https://law.yale.edu/system/files/area/center/global/document/411_final_paper_-_fedcoin.pdf

Haferkorn, M. and Diaz, J.M.Q., 2014, December. Seasonality and Interconnectivity Within Cryptocurrencies-An Analysis on the Basis of Bitcoin, Litecoin and Namecoin. In International Workshop on Enterprise Applications and Services in the Finance Industry (pp. 106-120). Springer, Cham

Hamburger, J., 2015. Bitcoins vs. State Money Transmission Laws: Protecting Consumers or Hindering Innovation. JL Econ. & Pol'y, 11, p.229

Kazan, E., Tan, C.-W., Lim, E.T., 2014. Towards a Framework of Digital Platform Disruption: A Comparative Study of Centralized & Decentralized Payment Providers. 25th Australasian Conference on Information Systems 8th – 10th Dec 2014, Auckland, New Zealand

Kiviat, T.I., 2015. Beyond Bitcoin: Issues in Regulating Blockchain Tranactions. Duke LJ, 65, p.569

Lee, E., 2017. Financial Inclusion: A Challenge to the New Paradigm of Financial Technology, Regulatory Technology and Anti-Money Laundering Law

Linn, C.J., 2010. Redefining the bank secrecy act: Currency reporting and the crime of structuring. Santa Clara L. Rev., 50, p.407

Low, J.X. (2017). "How to conduct proper customer due diligence (CDD) — AML-CFT". Retrieved 10.11.2017 from: https://aml-cft.net/conduct-proper-customer-due-diligence-cdd/

Marinelli, M. and Smith, M., 2015. Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology). The Journal of Financial Perspectives, 3(3), pp.38-69

McKinsey, 2016. How blockchains could change the world. Retrieved 08.11.2017 from: https://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world

Miller, A., Möser, M., Lee, K. and Narayanan, A., 2017. An Empirical Analysis of Linkability in the Monero Blockchain. arXiv preprint arXiv:1704.04299

Mu Qi-Guo., 2016. First Report on Survey of Blockchain Technology: Potential to Disrupt All Industries [J]. Report by Chuancai Securities Co. Ltd

Network, F.C.E., 2014. Application of FinCEN's regulations to virtual currency software development and certain investment activity. Retrieved 30.11.2017 from: https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R002.pdf

Noether, S., 2015. Ring Signature Confidential Transactions for Monero. IACR Cryptology ePrint Archive, 2015, p.1098

Özatak N. and Gökmeoglu K., 2017. New Challenges in Banking and Finance. Springer, New York

Pilkington, M., 2015. Blockchain Technology: Principles and Applications. Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar, 2016. Available at SSRN: https://ssrn.com/abstract=2662660

Poon, J., Dryja, T., 2015. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Technical Report (draft). Retrieved 10.11.2017 from: https://lightning.network/lightning-network-paper.pdf

Rajan, R.G., 1998. The past and future of commercial banking viewed through an incomplete contract lens. Journal of Money, Credit and Banking, pp.524-550.

Rubinton, B. (2011). Crowdfunding: Disintermediated Investment Banking. Retrieved 11.09.2017 from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1807204

Smedinghoff, T.J., 2009. Federated identity management: balancing privacy rights, liability risks, and the duty to authenticate. Retrieved 10.11.2017 from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1471599

Smedinghoff, T.J., 2011. Introduction to Online Identity Management. Retrieved 10.11.2017:

http://www.uncitral.org/pdf/english/colloquia/EC/Smedinghoff_Paper_-_Introduction_to_Identity_Management.pdf

Tapscott, D. and Tapscott, A. (2016). Blockchain Revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin Random House LLC, New York

Tellini, N. and Vargas, F., 2017. Two-Factor Authentication: Selecting and implementing a two-factor authentication method for a digital assessment platform

Teutsch, J. et al., 2016, February. When cryptocurrencies mine their own business. In International Conference on Financial Cryptography and Data Security (pp. 499-514). Springer, Berlin, Heidelberg

Vasiljeva, T. and Lukanova, K., 2016. COMMERCIAL BANKS AND FINTECH COMPANIES IN THE DIGITAL TRANSFORMATION: CHALLENGES FOR THE FUTURE. Journal of Business Management, (11)

Wood, D.G., 2014. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum. Retrieved 09.10.2017 from: http://gavwood.com/paper.pdf

Zhang, B. et al. (2016). 2nd European Alternative Finance Industry Report. Cambridge, UK. University of Cambridge, Cambridge Center of Alternative Finance, Cambridge

List of Figures

List of Tables