Journal of Theoretical and Applied Information Technology
15th December 2020. Vol.98. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

BLOCKCHAIN FOR BANKING SYSTEMS: OPPORTUNITIES AND CHALLENGES

[1]AREEJ AL SHORMAN, [2]KHAIR EDDIN SABRI, [3]MOHAMMAD A. M. ABUSHARIAH, [4]MOHAMMAD QAIMARI

[1]Department of Computer Science, King Abdullah II School of Information Technology, The University of Jordan, Amman, Jordan

[2]Department of Computer Science, King Abdullah II School of Information Technology, The University of Jordan, Amman, Jordan

[3]Department of Computer Information Systems, King Abdullah II School of Information Technology, The University of Jordan, Amman, Jordan

[4]Software Architect, Progress Soft, Amman, Jordan

E-mail: [1]ary9160102@ju.edu.jo, [2]k.sabri@ju.edu.jo, [3]m.abushariah@ju.edu.jo, [4]mohammed.qaimari@progressoft.com

ABSTRACT

Blockchain is a promising technology for both academic studies and practical industrial applications. It enables decentralized public ledgers to hold immutable data securely and ensures that the data cannot be altered. Digital identities, social media, supply chain management, luxury goods, and financial assets are among the domains that have widely benefited from this technology. In the literature, we found only a few review papers that target the banking domain, instead of a complete overview of the blockchain-based financial sector. These reviews are limited in reports and articles. Accordingly, the main aim of this study is to present an overview of blockchain-based banking services and discuss the challenges of applying blockchain technologies in the banking domain to give a clear understanding to professionals and researchers in this domain.

Keywords: *Blockchain, Ethereum, Cryptocurrencies, Bank Services, Centralized System, Decentralized System*

1. INTRODUCTION

Blockchain is a decentralized, distributed, shared, and immutable database ledger that records all the transfers of currency in a chain of blocks. This chain has a full history of all transactions and provides a cross-border global distributed trust. Therefore, blockchain can verify the authenticity of assets and prevent fraud [1]. Accordingly, it presents efficient solutions for many domains on a global scale and reshapes the future of monetary systems [2], [3], [4], [5]. This technology is a great innovation that creates decentralized financial infrastructure and secures value networks without the need for centralized trust intermediaries to facilitate the money transfer and purchase processes in a fast, safe, and cheap way [6]. The interesting fact is that tampering or changing the added block inside a blockchain is very difficult and impossible. Moreover, Ethereum, the second generation of a distributed and decentralized blockchain network, executes smart contracts to replace the old conventional paper deeds. A smart contract is an electronic contract that can execute itself once its conditions have been fulfilled [7].

We all witness the impact and growth of digital financial services and their values. The internet opened the door for the development of many fields such as telecommunication, e-commerce, social media, and smart devices. However, the monetary system had not been changed by the internet, where most of its innovations that are adopted nowadays are credit cards, Automated Teller Machine (ATM), online banking, Peer-to-Peer (P2P) lending, and Paypal [8]. On the other hand, blockchain extends the internet to develop a monetary system to refer to the internet of money. It is based on solid math, computer hardware, cryptography, and behavioral

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

economics. In this context, blockchain has the potential to change a wide variety of business and financial models, similar to the internet. To this end, blockchain reshapes the core financial infrastructure and all related business processes, the sustainable development of the global economy, and the current banking system [9].

Considering blockchain's feasibility, financial industries such as the banking domain are starting to adapt themselves to integrate their traditional services with the blockchain technology. According to Gartner's new business value forecast methodology, The business value-add will increase up to $176 billion by 2025 and grow up $3.1 trillion by 2030 [10]. R3, a financial innovation firm that involves over 400 banks and financial institutes using blockchain technology, expects to save $20 billion a year in the banking domain. International Business Machines Corporation (IBM) showed 91% of banks among 200 financial institutions would have fully adopted blockchain [11]. These facts encourage the officials in the legislative and regulatory authorities of banks to integrate blockchain in banking services, but the potential of blockchain has not yet been proven sufficiently succeeding for wide-scale adoption. Nevertheless, blockchain is already being implemented by financial domains [12], [13], [14], [15]. It is now discussed to be utilized in the banking system, a special case of the financial domain, to revolutionize their services. On the other hand, some banking services are not discussed because of the security issues in banks to give details about these services.

In the banking domain, researchers and professionals try to develop banking services on a global scale; whereas people from developing countries are still unbanked and this fact affects productivity, trading within their own country, and transacting with the rest of the world. Approximately, two billions people who form a quarter of the entire global population are unbanked [16]. Also, they try to reduce the time and complicated processes such as correspondent banks, exchange rate losses, counter-party risk, bureaucracy, and paperwork in bank transfers. Moreover, paying fees to a third party for transferring money overseas is costly [17]. All of these make the progressing significantly global economy difficult.

The main advantage of blockchain is that it gives a viable alternative for unbanked people to store and save their money. In addition, countries that are suffering from hyperinflation such as Zimbabwe and Venezuela will high demand for cryptocurrencies. The adoption of blockchain in the banking domains offers efficient solutions for secure, fast, and cheap transactions compared to traditional transactions in the banking system.

The novelty of this paper lies in providing insights to the officials in the legislative and regulatory authorities of banks, the financial and technological institutions, and the relevant authorities in charge to aware of the risks of ignoring blockchain technology in the banking domain. Also, these officials try to integrate banks with blockchain evolution to prevent losing their business in the future. Accordingly, the main focus of this study is to present a deeper understanding of blockchain technology in terms of features and characteristics which may be disrupted traditional banking services in the future. Then, we discuss how blockchain can be integrated into banks to improve their traditional banking services. Finally, the highlighted open challenges of this technology in the banking domain, as presented in this review paper, provide guidance and act as a road map to future research directions.

The rest of the paper is organized as follows: Section 2 provides background information about blockchain with its fundamental features and functions. Section 3 discusses blockchain banking services. Section 4 highlights the open challenges and future research directions. The related works are reviewed in Section 5. Finally, Section 6 concludes the paper.

2. BLOCKCHAIN OVERVIEW

Blockchain is the main technology that is used in cryptocurrencies such as Bitcoin and Ether. It records all the transfers of currency in a chain of blocks that have a full and complete history of all transactions and provides a cross-border global distributed trust [18], [19], [20]. Prior to discussing the use of blockchain technology in banking sector, we will discuss the fundamental principles and strengths of blockchain that are the main enablers of the banking applications that have been surveyed in our paper.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.1 Blockchain Architecture

Blockchain is a database ledger that records all the transfers of currency in a chain of blocks that have a full history of all transactions and provides a cross-border global distributed trust [18]. Therefore, blockchain can greatly verify the authenticity of assets and prevent fraud. Each block contains a ***Block number***, ***Nonce***, ***Txs***, ***Prev***, and ***Hash*** value as shown in Figure 1. The value of ***Nonce*** is obtained by minors who validate the block, and the set of the transactions assembled in a block is listed in ***Txs***. To connect a chain of blocks in a secure way, the SHA-256 algorithm is used to determine the value of ***Prev***, which indicates the hash value of the previous block.

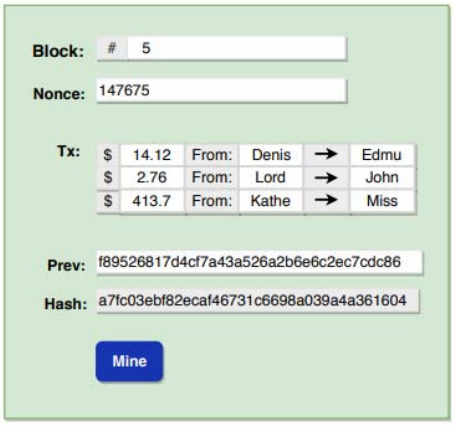

Figure 1: Block structure

Figure 2 explains the mechanism that hashing keeps the blockchain secure through ***Prev***, which indicates the hash value of the previous block using the SHA-256 algorithm [1], [21]. For instance, if a hacker changes something in block 2 as shown in Figure 2 and tampers with it, the hash value calculated by block 2 will be changed accordingly and the ***Hash*** value of block 2 will not be similar to the ***Prev*** value of block 3. In this case, when the whole blockchain is evaluated, the link between blocks 2 and block 3 will be breached and any tampering in the blocks will be detected. In addition, block 1 also referred to as the genesis block, does not have any previous block and the previous hash value is zeroes.

2.2 Consensus Mechanisms

Being decentralized systems, blockchain systems do not need a third party trusted authority to validate a transaction between untrustworthy parties. The distributed consensus mechanism is applied to guarantee a certain state for all the nodes in the blockchain network. In other words, when a new block is added to the blockchain, every node

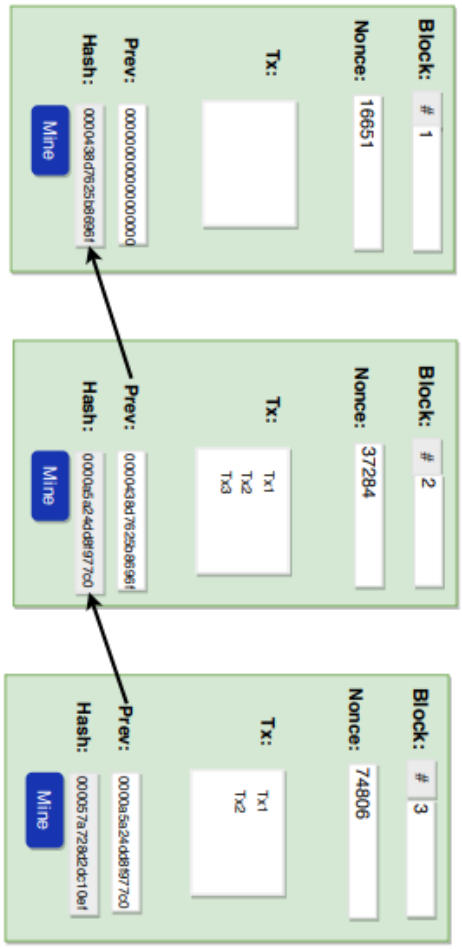

Figure 2: Blockchain structure

in blockchain network has to approve this new block. Therefore, even if a hacker tries to introduce a new block into this network, all nodes in the network need to approve that particular block is valid. Several consensus mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS) are adopted to establish consensus on the blockchain [22].

PoW is the first consensus mechanism used in Bitcoin. It depends on solving complicated mathematical calculations in the authentication process. Figure 3 shows the main steps of these calculations that are involved where each miner calculates a SHA256 based cryptography puzzle of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the constantly changing ***Nonce*** as shown in the following Equation (1) [22].

$$SHA256 (prev \| Tx_1 \| Tx_2 \cdots \| T x_n \| Nonce) < T arget) \quad (1)$$

where ***prev*** is the hash value of the previous block, Tx_1, Tx2 ...., Tx_n are the set of the transactions assembled in a block, ***Nonce*** is a variable which is needed to calculate in this equation for validating the block, and ***Target*** is a variable which is used to tune the difficulty of the PoW puzzle and start with a certain number of zeroes.

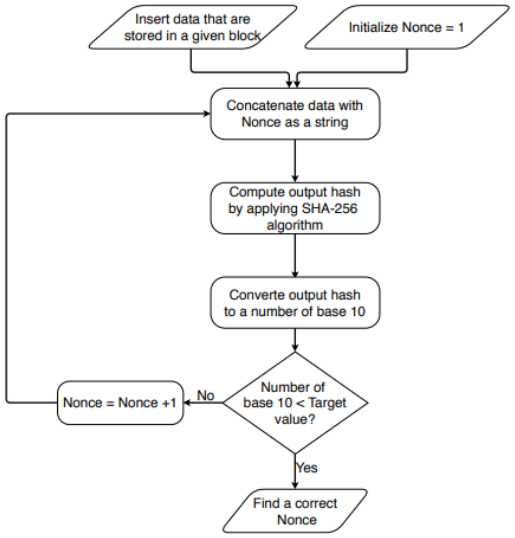

Figure 3: The main steps of PoW algorithm

Figure 4 shows an example of a PoW puzzle. Consider a given block has the amount of data ("***Hi There***") and ***Nonce*** has 1, 2, 3, 4, 5, ..., etc. values like counter variables. The following steps explain how PoW algorithm works:

1) Join data ("***Hi There***") together with the ***Nonce*** in a string.
2) Find a hash of this string to compute ***Output Hash*** (***OH***).
3) Convert ***OH*** to to base 10 notation (***BN***).
4) Increment ***Nonce*** by one if the value of ***BN*** is greater than target value (1000 in this example).
5) Repeat Step 2 until eventually ***BN*** is less than 1000.

When the first node obtains the correct solution of ***Nonce***, it will be rewarded some Ether and broadcast it to other nodes for verification.

In the decentralized network, there might be more than one miner that finds the correct ***Nonce*** simultaneously. Consequently, the blockchain is forked into many branches. Figure 4 shows an example of this case. Suppose that blocks C7

Data	+	Nonce	=	Output hash (OH)	Convert OH to base 10 (BN)	Is BN < 1000
Hi there		0		a23042b2e	178917215	No
Hi there		1		cbc1491	29589283	No
Hi there		2		0ca24258	94869869	No
Hi there		3		d9eed91	13938166	No
Hi there		4		1488baec	419386918	No
Hi there		5		0077bbb	100	Yes

Figure 4: An example of PoW algorithm

and D7 are created at the same time and have the same parent. Miners work on all branches and append a new block on top of them. When new blocks such as (B8, B9, B10, B11, B12, and B13) are added to block B7, the miners working on other forks will switch to the longest branch. Block D9 and C8 in the forks D7-D9, C7-C8 consequentially become orphan blocks, because they no longer increase [1].

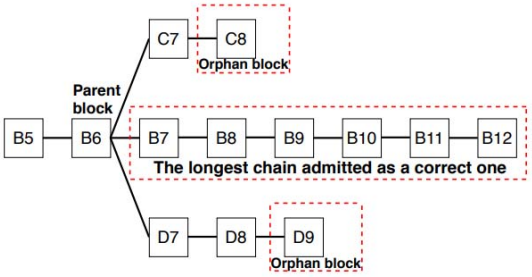

Figure 5: A scenario of the valid blocks are generated simultaneously

The strength of this mechanism appears when the hacker somehow manages to change the data of a specific block, he/she needs to make the whole change valid through recalculating all valid hashes for the next consecutive blocks in this chain. Very complex mathematical calculations will be required for every block in order to succeed in the hacking attempt. In addition, it may take more than ten minutes for the fastest personal computer available nowadays. Therefore, if the hacker wants

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

to make all the consecutive blocks valid, he/she spends considerable time on every block to make it valid. However, miners take millions and billions of times to successfully find the correct ***Nonce*** in PoW. Many resources such as electricity, CPU cycles, and millions of machines, are used in order to guess ***Nonce*** value. In addition, an economic phenomenon is known as the "Tragedy of the Commons", which is a prevalent problem in the study of economics and game theory [23]. As a result, the miner's reward decreases over time causing fewer miners and opening up vulnerability to malicious people who has 51 of the hashing power that may destroy the network.

New blocks are validated by performing a certain amount of computational work in PoW, while the creator of the next block is chosen via various combinations in PoS such as wealth because it is thought that the miners who have a lot of money will be less likely to harm the network. Unfortunately, as the computing power is reduced, the single richest miner is dominated in the entire network and attacks may appear as a consequence. The Ethereum blockchain network uses a specific PoS algorithm called Casper, whereas the validators will actually lose money if they validate a false block that is not correct [24].

2.3 Digital Signature

A digital signature is the other cryptographic concept used in blockchain to provide a layer of verification and security for sent messages through a non-secure channel. It is equivalent to a handwritten signature based on asymmetric cryptography. Asymmetric cryptography that is also called public key infrastructure (PKI) cryptography, uses the private and public keys [1]. In a digital signature, there are two main phases, namely, the signing phase that uses the private key, and the verification phase that uses the public key. Figure 6 shows how the digital signature is signed and verified by two users called ***Alice*** and ***Bob***. When ***Alice*** signs a transaction, she gives proof to anyone that she is the sender through computing a hash value for a transaction and encrypts it by her private key. She then sends both the transaction itself and the encrypted hash to ***Bob***. Any variation on the content on the received transaction or ***Alice's*** private key creates a different signature, so ***Bob*** uses transaction and its digital signature to reverse the process and verify the authenticity of the digital transaction. ***Bob*** generates two hashes, where the first one is generated by decrypting the digital signature using ***Alice***'s public key, and the second one is generated by hashing the content of the received transaction. If both hash values match, it proofs that the transaction was not altered during transit and the transaction is sent by ***Alice***.

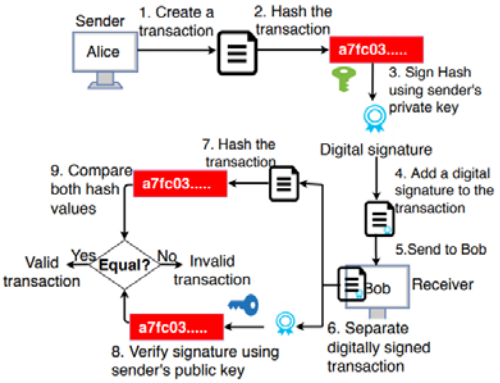

Figure 6: Digital signature used in blockchain

2.4 Key Features of Blockchain

Many features make blockchain the superstar of security in keeping data without the need for trusted intermediaries and create a decentralized financial infrastructure. Blockchain has the following features:

1) ***Decentralization***: A transaction in the decentralized network can be done between any two peers without a central authority. This reduces server costs and prevents the bottlenecks from the central server.

2) ***Persistency***: Since the validation process is done on both transaction and block levels, it detects any tamper where each node of the network has a copy of the blockchain.

3) ***Anonymity***: Blockchain is often described as anonymous, because the user is permitted to send and receive money without giving any personally identifying information, but only generation of one or more address.

4) ***Auditabitity***: Since each block in the blockchain stores a list of transactions, a timestamp for validation and creation, and the hash of the previous block, users can easily verify and trace each transaction that is stored in the blockchain.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Finally, Figure 7 explains the combination mechanism of the previous technologies and features in adopting blockchain in a real network such as Ethereum to hold immutable data in a secure and encrypted manner [25]. Moreover, governments and financial institutions already invested millions of dollars into blockchain development and implementation.

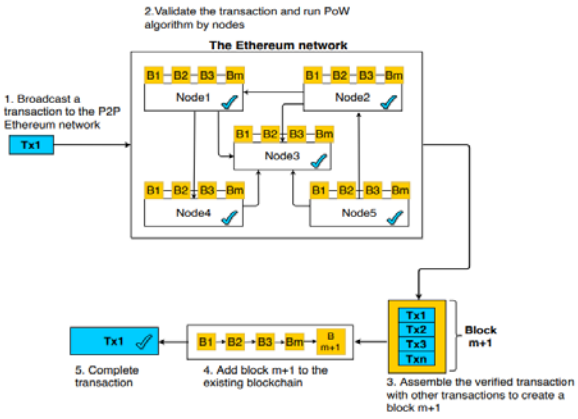

Figure 7: How Ethereum blockchain works

3. BLOCKCHAIN SERVICES IN BANKING SYSTEMS

In this section, we discuss the benefits of adopting blockchain in some of the existing services offered by traditional banks such as payments, post-trade settlements, deposit-taking and credit giving, escrow services, and Know Your Customer (KYC) processes, which are graphically represented in Figure 8.

Figure 8: Types of banking services that are adopted by blockchain

3.1 Payment

In the legacy banking systems, everyday payments suffer from a set of limitations in terms of cost, security, and time; whereas bank transfers involve multiple intermediate steps such as working with correspondent banks, counter-party risk, bureaucracy, and extensive paperwork [3]. In addition, consumers and businesses pay fees versus the services received. These fees affect customer satisfaction badly. Some of these fees for services are hidden while others are often unclearly shown to customers. For example, global banks like Santander are vastly reliant on fees from international money transfers and these fees form 10% of Santander's revenue in 2016 [26]. Furthermore, the payment process in blockchain takes a few hours instead of at least a few working days.

Blockchain is adopted by many banks in the financial industry to reduce the above limitations through peer to peer network and cut down on the need for verification from third parties. As a result, the process of bank transfers will become cheaper and faster. For example, Santander expects to save about 20 billion dollars a year, and Capgemini, a consultancy, expects that the customers save up to 16 billion dollars in banking and insurance fees a year through blockchain-based applications [2]. Furthermore, some banking officials aware of the potential of implementing blockchain for international money transfers. Developers in ANZ bank, BNP Paribas, BNY Mellon, Wells Fargo, and Hyperledger have applied a proof of concept for cross-border payment that is built on the Hyperledger Fabric blockchain platform. A proof of concept aims to test whether moving member bank accounts to a distributed ledger could help the interbank payments platform Swift Reconcile in real-time. Hyperledger Fabric enables real-time visibility, reconciliation, liquidity, governance, data privacy, standardization, and identity management [27].

Bitcoin, the first cryptocurrency based on blockchain, takes from a few minutes to a few hours to process a payment. Other cryptocurrencies like Litecoin (LTC) provide huge savings in terms of fees and time [4]. Moreover, most of the European Payments Council members expected that blockchain has a huge impact on the industry by 2025 [5].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1.1 Centralized Vs. Decentralized Payment Systems

A centralized payment system bases on a central party that manages money transmitted electronically in the system. Designing its architecture is much easier than a decentralized one. However, the main problem that faces this type of payment system is the bottleneck. In addition, the centralized payment system suffers from security issues such as its attractiveness for attacks. The centralized payment system has many intermediaries who extract disproportionately large value in the form of transaction fees, which would be expensive for customers. Furthermore, the focus market power for a centralized payment system is in the hands of a small group of intermediaries. The centralized payment system also handles a transaction in a slow and more expensive manner.

On the other hand, a decentralized payment network allows online payments to be sent directly from one party to another in a P2P network. In monetary transactions, a financial intermediary is needed to prevent a double-spending problem that occurs when a user tries to spend the same unit of coin twice at the same time. Bitcoin presents the first solution to this problem based on using network timestamps to accept the first attempt and reject any future attempts for the specific user. Also, Bitcoin combines several core technologies such as digital signature, hashing algorithm, and distributed consensus algorithm. All transactions are stored on a chain of blocks called the blockchain and verified in a decentralized manner instead of using a central intermediary [28], [29]. Money is sent and received in a matter of minutes compared to a centralized payment system without the existence of intermediate nodes that charge transaction fees. All network participants maintain consensus on the current state of the transaction ledger at all times. Table 1 summarizes the main differences between a centralized and a decentralized payment system.

The blockchain technology allows payments as well as other types of transactions involving value transfer or record-keeping [30]. This technology can be adapted and used under the supervision of the central authority to serve monetary transactions.

3.2 Post-Trade Settlements

The post-trade settlement system considers as one of the most important financial services. It involves lengthy and costly processes such as bookkeeping, transaction reconciliation, balance reconciliation, payment initiation, and many other processes [28].

Blockchain can significantly improve the efficiency of settlement processes in terms of time, fast, and cost. Trusted by both counter-parties will reduce settlement time because both sides share, control over the same

Table 1: A centralized vs a Decentralized Payment System

Criteria	Centralized	Decentralized
Design	Easier to design	Difficult to design
Cost	Expensive for customers	Affordable for customers
Speed	Slow	Fast
Main Disadvantage	A single point of failure	Double-spending
Control	By a central party	By the user personally
Security	Low	High
Exchange Fees	High	Low

distributed ledger system, and can certainty that the pre-conditions are preserved in smart contracts. In other words, the settlement process can be done directly and almost instantaneously rather than waiting many days and paying fees to the intermediary firms in existing protocols such as SWIFT [31]. Moreover, blockchain reduces mechanical errors as deriving from system failure since it is executed in a distributed network. Also, unnecessary replication of records is removed to guarantee overall consistency. All of these benefits improve the efficiencies of audit and reconciliation.

For example, international stock exchanges save and execute tradings in markets' securities to reduce cost, simplify procedures, and increase the speed of settlement processes in a safe manner. Currently, many applications have been very active in developing blockchain trading

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

platforms. Nasdaq, one of the largest stock exchanges in the world, adopts blockchain for the trading of securities of private companies [32]. In addition, blockchain helps global stock exchanges to save 40 to 50 billion dollars annually in operating expenses [33].

To summarize, banks try to build a leaner, less expensive, and faster back-office structure from traditional structure.

3.3 Deposit Taking and Credit Giving

Banks can either be for commercial or investment purposes. Commercial banks are mainly involved with deposit-taking and credit giving activities, whereas investment banks deal with more sophisticated operations such as assisting businesses in major corporate events as listing their shares on a stock exchange, Initial Public Offering (IPO), and Merger and Acquisitions (M&A) [34].

We focus in this paper on commercial banks because they affect the everyday life of most people. Currently, commercial banks are the main source of collecting deposits from depositors who need to save their money and then lend them to borrowers instead of depositors lend their money directly to borrowers. Also, commercial banks have expertise in recognizing good borrowers and dealing with bad debtors once they stopped servicing paying their debt. These processes are based on the credit reports provided by specialized credit agencies to check some factors such as credit score, homeownership status, or debt to income ratio [35].

The main source of banks' revenues is the difference between the interest they pay to depositors and the interest they charge borrowers [36]. Therefore, the balance between two processes deposit-taking and credit giving is playing a critical role in the success of the entire business model for traditional banks. If people stop depositing money in banks, such banks would not be able to finance the loans that they give to borrowers at a higher rate. Also, commercial banks offer several services such as international money transfers, custody, letters of credit, forex dealing, and escrow accounts [37]. Furthermore, such banks' systems suffer from limitations to satisfy their customers' needs. Some sensitive information that may be focused on a small number of institutions and hacked through exposing them to unauthorized people, which is similar to the case of Equifax [38]. Moreover, high fees are forced by commercial banks.

In the future, smart contracts based on blockchain technology play a critical role in facilitating deposit-taking and credit giving processes and make them more transparent. The clarity deriving from the blockchain reduces Informational asymmetries between borrowers and lenders. Pre-agreed terms will be respected and sorted on a public database that allows people to trace the history of the borrower in the past and then decide to lend him/her money or not. For example, the success of the online marketplace depends on a rating. In the blockchain platform, the borrowers' reputation and their previous transactions will be registered on the blockchain. This would certainly reduce informational asymmetries between borrowers and lenders, validate transactions, and perform routine account administration tasks in a faster and less expensive manner [28]. On the other hand, lenders would have more information regarding the type of borrower that is wanted to lend money to. Moreover, this information would be immutable and easily accessible. As a result, blockchain would create a competitive market for borrowers without geographical constraints i.e., borrowers from all over the world can bid to provide the loan.

Banks are burdened by heavy administrative costs that inflate the final interest rate they charge borrowers. In a p2p lending market adopted by blockchain and smart contracts technology. The lender would not have to cover any admin cost and would be happy to receive a fraction of the interest rates charged by banks.

3.4 Escrow Services

In escrow services, trust is an important issue when many parties trade with each other. Therefore, banks play the role of a middleman to increase trust by providing letters of credit and escrow services. For example, suppose a retailer in Europe wants to import clothes from China. The problem is that the retailer has not worked with the supplier before and does not have a guarantee that the Chinese manufacturer will deliver the clothes once the money is paid. Also, the Chinese manufacturer does not have a guarantee the European retailer will pay the money once the goods are shipped. This problem is solved using the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

escrow account in a trusted bank where the European retailer will deposit the funds in a bank that releases the funds when the producer will ship the goods. In this case, the bank's reputation and regulatory license removes informational asymmetries on both parties, facilitates the trade and making it more legitimate as possible [39]. However, the bank forces fees depending on the total transaction value to check and track this trading process.

Smart contract-based blockchain transforms this line of business through designing mechanism that transfers the title of goodes and funds automatically between involved parties in transparent way. The conditions that are related on how to execute this type of trade are held into a smart contract. The parties in a business transaction would be able to write code that is immutable and executes automatically when the predefined conditions are met [40].

3.5 KYC Processes

Banks require to know some essential information about their customers, verify their identity, and monitor their account movement. The collecting of this information aims to validate that their customers have not been involved in illegal activities such as fraud, money laundering, or funding of terrorist organizations. KYC processes are lengthy processes for banks, where banks work with millions of clients, use tons of forms, and investigate suspicious cases. In addition, banks should go through these processes for every new customer and their cost can be covered by large banks, but small banks cannot cover the cost [41].

Blockchain facilitates sharing a unique distributed database among banks and regulators to reduce KYC processes in traditional banks. The history of client transactions is stored in a secure, unbiased, immutable way by all banks shared in the blockchain platform. Furthermore, blockchain increases transparency for participants who have private permission.

Many case studies are developed and tested by the solution of blockchain. For example, although the economic growth in the Philippines is quickly increasing, 44% of Filipinos were utilizing bank account in 2017, it is still hampering by inefficient ways of checking the identity and tracking the history of new account applicants [42]. Additionally, KYC laws require asking for the same information more than once time which is not available in digital or verifiable form. To solve this issue, Hyperledger Indy is built based on a set of libraries, tools, and other components for digital identity on blockchains [43]. The platform undertook a proof of concept exercise to streamline the onboarding of new accounts by allowing customers to enter information only once in a privacy-preserving way and reuse this information for a new account opening. Banks can trust that the history of this information is correct. Based on the successful of this platform, it could serve as a test for the national identity system in the future.

A similar example presents by a consortium of Singapore regulator and several banks such as HSBC and Mitsubishi Financial Group (MUFG). A proof of concept prototype for a KYC blockchain is built and tested between February and May 2017 in terms of functionality, scalability, and security. Results show that blockchain functionality can deal with a high volume of information flow. It is also proved the immutability to third party interference and only allowing access by participants who have legitimate authentication [44].

4. BLOCKCHAIN OPPORTUNITIES IN BANKING SYSTEMS

In this section, we identify some of the potential challenges and critical issues that can be taken into consideration for future research by the research community. Figure 9 presents the most open challenges and future research directions for integrating blockchain into the banking sector.

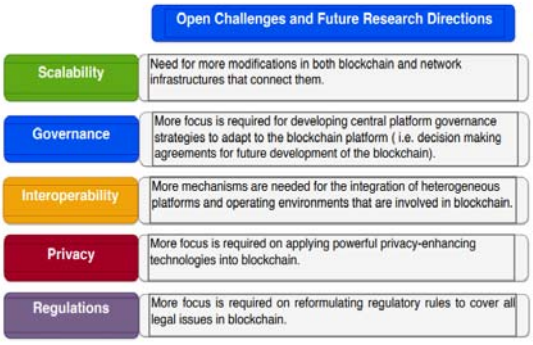

Figure 9: Open Challenges And Future Research Directions For Integrating Blockchain Into The Banking Sector

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.1 Scalability

To achieve consistency between the untrustworthy networks, the blockchain platform applies the consensus mechanism such as PoW among all nodes on the network. This mechanism is complex and takes too much time and energy compared with the central server model that would run faster. However, the central server model has a single point of failure. Therefore, two issues have surfaced, which are the scalability and performance on one hand, and security on the other hand.

The security of blockchain protocols such as Bitcoin and Ethereum requires processing and replicating every transaction by every single full node in the network. Accordingly, blockchain is slower than centralized payment processing networks such as Visa, MasterCard, and PayPal. The average of transactions that will be executed plays a critical role in the performance of banking systems; Visa and MasterCard can handle about 50000 transactions/second and PayPal can handle 450 transactions/second. On another side, Bitcoin can process up to 7 transactions/second and Ethereum can process up to approximately 30 transactions/second [45].

Current architectures need some modifications to scale up the number of transactions that can be handled by the banking system. In addition, the global community of developers always present proposals to improve blockchain protocols and solutions to reduce the technical complexity in the blockchain.

For solving the scalability issue in Ethereum, two layers of solutions are presented, namely: On-chain and off the chain. The first layer focuses on modifying the underlying blockchain infrastructure, while the second one focuses on developing additional network infrastructure that connects to the main blockchain network but operates separately from it. In more detail, an on-chain solution adopts the Proof-of-Stake consensus algorithm instead of the Pow algorithm. Another solution implements a technique called sharding, which is the process for scaling existing distributed database such as MySQL and MongoDB. Based on this technology, the state and tasks of the blockchain are divided into multiple nodes called shared rather than being done by everyone, where each shared processes transaction in different parts of the blockchain state in parallel. Thus, the throughput is improved and the storage requirements are reduced.

The off-chain layer involves many solutions such as state channels, a payment channel network called Raiden [46], a new concept layer for improving scalability in smart contracts called Plasma [47], and Truebit solution for processing complex computations [48].

4.2 Governance

Integrating blockchain into banking services needs dealing and communicating with broad communities of stakeholders such as founding teams, developers, miners, and others, to reach an agreement on the future development of the blockchain. Moreover, the relationships between various participants are quit complex and unclear compared to firms, where the operation of ownership power and control among different stakeholders are clear.

From an economic perspective, the greater the number of nodes with the network, the more valuable the service becomes to the community through their mutual involvement in the system (positive network effect principle). However, the decision making becomes more complex and some issues have appeared when everybody needs to agree to a course of action. For example, after the DAO attack has occurred the Ethereum network is split into Ethereum and Ethereum classic in 2016. Another example on 15 November 2016, Segregated Witness, Bitcoin Core version 0.13.1, is released to increase the block size limit [6].

The decentralization is the main feature of blockchain that makes governance a complicated matter. Also, when a transaction is deployed on the blockchain, it is impossible to change it. This poses a challenge to the ways that can be used to correct potential errors from technological and governance perspectives. For example, who would announce mistakes, which suitable methods would then be applied to correct these mistakes, and how much time is needed to correct them. In clearing and settlement processing, the mistakes have to be solved quickly [35].

The adoption of blockchain in financial markets affects several aspects that represent our understanding of the working mechanism of financial markets and how to govern them. Therefore, governance strategies used in the central

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

platform must be adapted to the blockchain platform.

4.3 Interoperability

Blockchain is designed for multiple distributed applications to support future applications especially banking services. Therefore, interoperability is a key issue for blockchain to integrate different blockchain networks. On the other hand, there are many difficulties in fetching data from the internet, which need Oracles software patterns as intermediaries between smart contracts that are stored on the blockchain and external information that may play a critical role in smart contracts correct execution [49]. However, this solution is not suitable for blockchain technology, which tries to remove middlemen and encourage a decentralized environment.

There are many cases illustrating interoperability, the first case occurs when integrating the blockchain with existing systems including legacy applications. Sometimes this integration is not an easy task and suffers from security issues. The second case is related to heterogeneous platforms and operating environments that are involved in blockchain technology. Finally, blockchain is dealing with different vendors using different environments, development mechanisms, and programming languages [35].

Thus, there are some research and development efforts to solve this issue. Most solutions are presented as building bridges between different blockchain protocols such as atomic swaps, decentralized exchanges, and inter-chain communication protocols. Atomic swaps represent a directed trade to exchange different cryptocurrencies between customers and guarantee that either the coins are swapped or the balances are untouched. This process is done on-chain compared to the majority of popular cryptocurrencies exchange which match and settle transaction off-chain like standard financial exchanges. Both on-chain and off-chain are deployed on the blockchain to become the main trading venues in the future [46].

A platform is presented to achieve interoperability between the Bitcoin and the Etherum networks called Rootstock (RSK). This platform is a sidechain that is based on a 2-Way peg mechanism. The 2-Way peg is a method to connect the original Bitcoin into Smart Bitcoin Currency (SBTC), which is introduced by RSK platform. The compatibility of this platform with the Ethereum in terms of programing language and Ethereum virtual machine (EVM). RSK also builds a layer of the Lightning network called Lumino network which can increase its transaction throughput to thousands of transactions per second [50].

In the future, blockchain needs to be able to maintain the correctness and reliability of the existing applications' functions and the consistency of the sharing mechanism among all integrated systems. In addition, it should maintain data security and privacy challenges in the current ways of data storing and sharing to achieve global success. Thus in the future, blockchain needs to be able to maintain the correctness and reliability of the existing applications' functions and the consistency of the sharing mechanism among all integrated systems. In addition, it should maintain data security and privacy challenges in the current ways of data storing and sharing in order to achieve global success.

4.4 Privacy

Preserving customer privacy and sensitive information is an important feature for both businesses and individuals. In traditional banking systems, the efforts of preserving customer information require a costly process, and can only be shared with others based on regulations on a need to know basis. On the other hand, the customer information is broadcasted to all the participants of the blockchain network, which may help in tracing the history of the transactions, the balance of cash, and assets held on accounts. For example, many corporations don't prefer to deploy their internal processes and business secrets on a transparent and immutable blockchain. Also many high profiles or high net worth individuals prefer to hide their private financial dealing.

One of the most powerful privacy-enhancing technologies is zero-knowledge proofs that are used in many projects like Polkadot and T3 to include privacy features [51], [52]. Ethereum integrated this technology into its environments to create a privacy layer and enhance its functionality. Thus, it can enable many decentralized applications that inherently require privacy [53].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

This challenge combines the public nature of blockchain and preserves the anonymity and privacy of critical information recorded. In this technology, customers can create many encryption identifiers such as private keys instead of the name to provide an additional level of privacy but the management and control processes of these keys are difficult tasks [54]. Blockchain has three types with different properties, namely: public, consortium, and private. Privacy is an important issue that affects the adoption of blockchain technology.

4.5 Regulations

As blockchain is a real groundbreaking technology that is still in the development stage, the regulatory rules are not being fully formulated yet in order to cover all legal issues that might occur. Furthermore, these regulations are among the most significant factors that will be studied, especially when the blockchain platform is adopted into a full-fledged financial-services industry [12].

Although smart contracts are agreements between the contractors, which are self-executed when certain conditions are met. They need to be supported by rules, laws, and specific regulations to address legal issues and disagreements between the contractors. For example, in the case where both parties agree on material purchases and they use an approved smart contract, the payment process is done by digital currency, and the order is delivered within the agreed time. The synchronization between payment and delivery is a critical issue that must be controlled by the legal system. In addition, an issue might occur when the parties are from different countries and they need to decide on the country's law that should be applied. Although smart contracts are agreements between the contractors, which are self-executed when certain conditions are met. They need to be supported by rules, laws, and specific regulations to address legal issues and disagreements between the contractors. For example, in the case where both parties agree on material purchases and they use an approved smart contract, the payment process is done by digital currency, and the order is delivered within the agreed time. The synchronization between payment and delivery is a critical issue that must be controlled by the legal system. In addition, an issue might occur when the parties are from different countries and they need to decide on the country's law that should be applied.

5. RELATED WORKS

The huge potential of blockchain technology in providing a great infrastructure for the monetary system has sparked growing research interest in many financial domains, similar to the internet. However, since this technology is still in an early stage, there is a limited number of surveys in the literature discussing blockchain technology in the banking domain. Also, these studies are limited to reports and articles.

The most studies [12], [13], [14], [15] present the applicability of applying blockchain in many financial services from a different point of views. The study of Geber [13] explains the role of blockchain in succeeding crowdfunding of the European Union (EU). Another study, Mills et al. [14], presents an analytical framework for central banks to identify the opportunities and challenges associated with payment, clearing, and settlement activities. Permissions, data integrity, data security, and data authenticity are the main characteristics of blockchain technology to integrate into central bank treasury ledgers, retail and investment bank ledgers, trading, settlement and clearing processes, and multi-signature escrow services [12]. A case study is presented in the German-speaking area in Europe to explain the advantages and disadvantages of adoption blockchain into online payment and sales transaction systems through literature review and conduct a questionnaire survey among experts in this area [15]. Financial markets are another case study that discusses the strength and weakness points in the adoption of blockchain in them [55]. Beck et al. [56] develop a proof of concept prototype that has the potential to offer a distributed trust-free coffee shop payment solution instead of a traditional solution based on a trust-based. On the other hand, Zarpala and Casino [57] focus on developing the laws and regulations to support fast-moving industries based on blockchain. Also, it presents a forensic-by-design methodology for embezzlement detection.

Another important contribution of blockchain technologies in firms and organizations such as R3, Sand Hill Road, and Coinbase is reducing the time and cost of settling a syndicated loan trade, where this process can take a nanosecond instead of 20 days and save at least $20 billion annually in the regulatory, settlement, and cross-border payment costs [58]. The recent study

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of Linn and Koo [11] points out that there are many famous banks such as Barclays, Goldman Sachs, LohmusRain, and LHV bank trying to build a framework to utilize the benefits of blockchain in their traditional services and save 15-20bn USD by 2022 [59]. Recently, many banks try to promote global economic growth and develop green technologies using blockchain technology and focus on how blockchain achieves the sustainable development of the global economy by giving freedom and transparency for participants to manage their interests [8], [60].

To sum up, there are a limited number of studies in the literature that integrates blockchain technology with the banking domain. These studies primarily focus on integrating blockchain with generic financial services. Therefore, they mainly lack providing a comprehensive investigation of blockchain technologies to be applied in the banking domain. In this study, we discuss how to integrate blockchain in many banking system services as well as analyze the challenges to provide a comprehensive picture.

6. CONCLUSION

With the recent advancements in internet and network technologies, there is a clear need for improving the quality of banking services. There are many issues in the traditional banking system that need solutions based on decentralized platforms. In this context, blockchain technology can play a critical role in the security and integrity of customer information. Therefore, the main focus of this paper was to provide an overview of blockchain technology in the banking domain. This paper presented an overview of blockchain technologies including main characteristics and functions. It also highlighted the benefits of a decentralized payment system over the centralized payment system. Moreover, this work identified several services in the banking domain such as payment, post-trade settlements, deposit-taking and credit giving, escrow services, and KYC processes, where blockchain technology can be useful and make noticeable improvements to them. In addition, this paper identified potential open challenges and drew a road-map for future research directions for blockchain-based banking systems. Scalability, governance, interoperability, privacy, and regulations, were among the open challenges and future research directions that were discussed in this paper. Therefore, future research works in the banking system are required to address these challenges and bridge the gap for more efficient, scalable, and secure banking services based on blockchain technology.

This study can have some potential limitations. Expected limitations are restricted to related studies that are not discovered by the authors. To reduce this limitation, we interview some software architects in Progress Soft, a Jordanian corporation focuses to provide real-time payment solutions that simplify daily tasks in business and in life. Also, this study focuses only on banking services and what the challenges may appear in them.

REFERENCES

[1] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.

[2] A. Tapscott and D. Tapscott, "How blockchain is changing finance," Harvard Business Review, vol. 1, no. 9, pp. 2–5, 2017.

[3] M. Buitenhek, "Understanding and applying blockchain technology in banking: Evolution or revolution?" Journal of Digital Banking, vol. 1, no. 2, pp. 111–119, 2016.

[4] S. Ahamad, M. Nair, and B. Varghese, "A survey on crypto currencies," in 4th International Conference on Advances in Computer Science, AETACS. Citeseer, 2013, pp. 42–48.

[5] S. Kesharwani, M. P. Sarkar et al., "Blockchain bringing paradigm shift in indian governmental society functioning," CYBERNOMICS, vol. 1, no. 2, pp. 38–42, 2019.

[6] L. Cocco, A. Pinna, and M. Marchesi, "Banking on blockchain: Costs savings thanks to the blockchain technology," Future internet, vol. 9, no. 3, p. 25, 2017.

[7] V. Buterin et al., "Ethereum white paper," GitHub repository, pp. 22–23, 2013.

[8] Q. K. Nguyen, "Blockchain-a financial technology for future sustainable development," in 2016 3rd International Conference on Green Technology and Sustainable Development (GTSD). IEEE, 2016, pp. 51–54.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[9] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the internet of things: A systematic literature review," in 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA). IEEE, 2016, pp. 1–6.

[10] B. Granetto, R. Kandaswamy, J. Lovelock, and M. Reynolds, "Forecast: Blockchain business value, worldwide, 2017–2030," Gartner Research, Technical Report, Tech. Rep., 2017.

[11] T. A. Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, "A comparative analysis of blockchain architecture and its applications: Problems and recommendations," IEEE Access, vol. 7, pp. 176 838–176 869, 2019.

[12] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in Banking beyond banks and money. Springer, 2016, pp. 239–278.

[13] M. Gebert, "Application of blockchain technology in crowdfunding," New European, vol. 18, 2017.

[14] D. C. Mills, K. Wang, B. Malone, A. Ravi, J. Marquardt, A. I. Badev, T. Brezinski, L. Fahy, K. Liao, V. Kargenian et al., "Distributed ledger technology in payments, clearing, and settlement," 2016.

[15] H. Peter and A. Moser, "Blockchain-applications in banking & payment transactions: Results of a survey," European financial systems, vol. 141, p. 141, 2017.

[16] G. J. Larios-Hernandez, "Blockchain entrepreneurship opportunity in ´ the practices of the unbanked," Business Horizons, vol. 60, no. 6, pp. 865–874, 2017.

[17] M. Orozco, "Attracting remittances: Market, money and reduced costs," Inter-American Development Bank, Tech. Rep., 2010.

[18] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (sok)," in International Conference on Principles of Security and Trust. Springer, 2017, pp. 164–186.

[19] X. Lin, R. Xu, Y. Chen, and J. K. Lum, "A blockchain-enabled decentralized time banking for a new social value system," in 2019 IEEE Conference on Communications and Network Security (CNS). IEEE, 2019, pp. 1–5.

[20] S. Yaqoob, M. M. Khan, R. Talib, A. D. Butt, S. Saleem, F. Arif, and A. Nadeem, "Use of blockchain in healthcare: A systematic literature review," Int. J. Adv. Comput. Sci. Appl, vol. 10, pp. 644–653, 2019.

[21] L. Luu, Y. Velner, J. Teutsch, and P. Saxena, "Smartpool: Practical decentralized pooled mining," in 26th {USENIX} Security Symposium ({USENIX} Security 17), 2017, pp. 1409–1426.

[22] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," Future Generation Computer Systems, 2017.

[23] M. J. Casey and P. Vigna, "In blockchain we trust," Technol. Rev, vol. 121, pp. 10–16, 2018.

[24] T. Duong, L. Fan, and H.-S. Zhou, "2-hop blockchain: Combining proof-of-work and proof-of-stake securely," 2016.

[25] M. Pilkington, "11 blockchain technology: principles and applications," Research handbook on digital transformations, vol. 225, 2016.

[26] J. Oh and I. Shong, "A case study on business model innovations using blockchain: focusing on financial institutions," Asia Pacific Journal of Innovation and Entrepreneurship, vol. 11, no. 3, pp. 335–344, 2017.

[27] V. Ramachandran and T. Rehermann, "Can blockchain technology address de-risking in emerging markets?" 2017.

[28] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," Financial Innovation, vol. 2, no. 1, p. 24, 2016.

[29] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.

[30] J. L. Zhao, S. Fan, and J. Yan, "Overview of business innovations and research opportunities in blockchain and introduction to the special issue," 2016.

[31] D. Gozman, J. Liebenau, and J. Mangan, "The innovation mechanisms of fintech start-ups: insights from swift's innotribe competition," Journal of Management Information Systems, vol. 35, no. 1, pp. 145–179, 2018.

[32] M. Geranio, "Fintech in the exchange industry: Potential for disruption," Masaryk UJL & Tech., vol. 11, p. 245, 2017.

[33] BISsearch, "Blockchain technology in financial services market - analysis and forecast: 2017 to

2026 (focus on opportunity and use case analysis," Tech. Rep., 2017.

[34] M. Jensen, "The role of network resources in market entry: Commercial banks' entry into investment banking, 1991–1997," Administrative Science Quarterly, vol. 48, no. 3, pp. 466–497, 2003.

[35] J. S. Cermeno, "Blockchain in financial services: Regulatory landscape ˜ and future challenges for its commercial application," BBVA Research Paper, no. 16/20, 2016.

[36] P. L. Brock and L. R. Suarez, "Understanding the behavior of bank spreads in latin america," Journal of development Economics, vol. 63, no. 1, pp. 113–134, 2000.

[37] L. J. Radecki, "Banks' payments-driven revenues," Economic Policy Review, vol. 5, no. 2, 1999.

[38] C. Kenny, "The equifax data breach and the resulting legal recourse," Brook. J. Corp. Fin. & Com. L., vol. 13, p. 215, 2018.

[39] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, "Untrusted business process monitoring and execution using blockchain," in International Conference on Business Process Management. Springer, 2016, pp. 329–347.

[40] C. K. Frantz and M. Nowostawski, "From institutions to code: Towards automated generation of smart contracts," in 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W). IEEE, 2016, pp. 210–215.

[41] R. Arasa, "Determinants of know your customer (kyc) compliance among commercial banks in kenya," Journal of Economics and Behavioral Studies, vol. 7, no. 2, pp. 162–175, 2015.

[42] P. Lipovyanov, Blockchain for Business 2019: A user-friendly introduction to blockchain technology and its business applications. Packt Publishing Ltd, 2019.

[43] I. N. S. Cunha, "Beyond the hype: embracing blockchain for social change," 2019.

[44] H. Hassani, X. Huang, and E. Silva, "Banking with blockchain-ed big data," Journal of Management Analytics, vol. 5, no. 4, pp. 256–275, 2018.

[45] G. Karame, "On the security and scalability of bitcoin's blockchain," in Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. ACM, 2016, pp. 1861–1862.

[46] G. Malavolta, P. Moreno-Sanchez, C. Schneidewind, A. Kate, and M. Maffei, "Anonymous multi-hop locks for blockchain scalability and interoperability." in NDSS, 2019.

[47] S. Dziembowski, G. Fabianski, S. Faust, and S. Riahi, "Lower bounds for off-chain protocols: Exploring the limits of plasma." IACR Cryptol. ePrint Arch., vol. 2020, p. 175, 2020.

[48] J. Teutsch and C. Reitwießner, "A scalable verification solution for blockchains," arXiv preprint arXiv:1908.04756, 2019.

[49] M. Bartoletti and L. Pompianu, "An empirical analysis of smart contracts: platforms, applications, and design patterns," in International conference on financial cryptography and data security. Springer, 2017, pp. 494–509.

[50] K. Wilkerson and S. Daley, "Ascension project," 2017.

[51] G. Kaur and C. Gandhi, "Scalability in blockchain: Challenges and solutions," in Handbook of Research on Blockchain Technology. Elsevier, 2020, pp. 373–406.

[52] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," IEEE Access, vol. 7, pp. 36 500–36 515, 2019.

[53] E. Morais, T. Koens, C. Van Wijk, and A. Koren, "A survey on zero knowledge range proofs and applications," SN Applied Sciences, vol. 1, no. 8, p. 946, 2019.

[54] H. Halpin and M. Piekarska, "Introduction to security and privacy on the blockchain," in 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2017, pp. 1–3.

[55] R. Lewis, J. McPartland, R. Ranjan et al., "Blockchain and financial market innovation," Economic Perspectives, vol. 41, no. 7, pp. 1–17, 2017.

[56] R. Beck, J. Stenum Czepluch, N. Lollike, and S. Malone, "Blockchain– the gateway to trust-free cryptographic transactions," 2016.

[57] L. Zarpala and F. Casino, "A blockchain-based forensic model for financial crime investigation: The embezzlement scenario," arXiv preprint arXiv:2008.07958, 2020.

[58] K. Fanning and D. P. Centers, "Blockchain and its coming impact on financial services,"

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Journal of Corporate Accounting & Finance, vol. 27, no. 5, pp. 53–57, 2016.

[59] P. Paech, "The governance of blockchain financial networks," The Modern Law Review, vol. 80, no. 6, pp. 1073–1110, 2017.

[60] H. M. Gazali, R. Hassan, R. M. Nor, and H. M. Rahman, "Re-inventing ptptn study loan with blockchain and smart contracts," in 2017 8th International Conference on Information Technology (ICIT). IEEE, 2017, pp. 751–754.