ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 4, Issue 3, DOI: 10.29027/IJIRASE.v4.i3.2020.669-674, September 2020

KYC Optimization using Blockchain Smart Contract Technology

Ashok Kumar Yadav[1], Ramendra Kumar Bajpai[2]
Department of Information Technology, Rajkiya Engineering College
Azamgarh, UP, India
Email: ashokyadav88.jnu@gmail.com[1], ramendrabajpai21@gmail.com[2]

***Abstract*—** In the present scenario, it is vital for any organization, especially the financial organizations, to understand customers and their financial dealings better. KYC is a process to verify identity and related details of corresponding customers. The current KYC mechanism has a severe concern in financial institutions as it requires separate ledger for the separate financial organizations. Every institution has its KYC process, which sometimes may include third-party, which may cause increased maintenance cost, time and redundancy. There is considerable wastage of costs in the form of opportunity cost, maintenance cost, customer verification cost and many more of around $27 million according to an economic survey. The current KYC process is very time-consuming, and it decreases the user experience. We have proposed an enhanced KYC system using blockchain technology to improve the existing KYC system. An inherent feature of the DLT is used to remove the third-party involvement, and smart contracts are used to build our logic in the mobility of the data. Blockchain technology has various types of cryptographic security which provide a safer place to transact over an unsecured channel. Using the facility of DLT, cryptography and consensus mechanism of blockchain, the proposed model of KYC process can optimize storing, updating, sharing of data and accessing operations along with enhanced security, transparency and privacy. It also enhances customer ownership and improves customer experience. It not only reduces the time duration and document update problem but also saves opportunity cost, aggregation, cost, maintenance cost and many more costs, which can affect the performance of any organization.

***Keywords*— KYC, blockchain, hash, DLT, consensus, Ethereum.**

I. INTRODUCTION

Recent emerging technologies like big data, machine learning and IoT offer an efficient way to handle modern problems of storing, managing and accessing a massive amount of data along with controlling the sensing devices. However, data breaching is a significant issue in big data and IoT systems. Security, transparency and privacy is the significant and primary concern nowadays. The blockchain technology can come into the picture with the embedded functionality of distributed ledger technology as it provides better security, transparency and privacy over an insecure communication channel. Blockchain is an incorruptible, immutable, decentralized replicated digital public ledger with the facility of recording not just only the financial transactions but also almost everything of values [1]. This technology facilitates data decentralization, transparency, the immutability of digital ledger, security and privacy, provenance, trust and finality in peer to peer network. It is the chain of blocks. The blocks are the growing list of records of transactions and connected with the cryptographic hashing technique. Blockchain may be applicable in many challenging fields. However, our primary concern here is to discuss it regarding financial institutions as financial development module can indirectly influence the other fields to get more reliability and profit. KYC is an acronym of 'Know your customer'. KYC is a primary process through which a user needs to go through to acquire all the facilities offered by a particular organization [2]. With the development in the exchange of virtual cash, numerous unethical cases have been accounted for ceaselessly, so every authority has chosen to bring such a framework under which all the potential boundaries of a client can be recognized, and the client can be shielded from any irresponsible utilization of his/her benefits. Some sort of policies which are measured under existing KYC is customer acceptance policy, customer identification policy, monitoring of transactions with risk management [3]. These all can be optimized using blockchain technology. Blockchain was first referenced in the white paper of Satoshi Nakamoto in 2008**.** In straightforward terms, blockchain can be characterized as the chain of blocks with immutable records that can be treated as a public ledger. Blockchain innovation had appeared from the concept of timestamping**.** Timestamping is used to maintain the dignity and integrity of the digital document that is configured for authentication and authorization over an unsecured network **[4]**. "Blockchain Technology can be defined as a platform where people who do not trust each other come together to share their thoughts collaboratively to make rational decision making to achieve the destined goal". In blockchain technology, nodes are located at different locations with their resources of operations and can manage their functioning by using a message-passing system over the network. Blockchain technology works over an unsafe network, so it uses cryptographic algorithms to maintain the integrity and authenticity of the data [5]. Blockchain works on the motto "Visible and verifiable to all within the network, but immutable by nature". Only some set of nodes are authorized to verify the record before the final commitment of a block in the blockchain. These nodes are called miners. Blockchain is a chain of blocks, and a block is a collection of transactions. A block is created in 10 minutes, and priority its size was 1 MB, but it can be

extended to 10 MB. Blockchain technology eliminates almost all the cost that is consumed by the third party to maintain the transaction record. The transactions that have been recorded on the blockchain can be verified by all the user present in the network. But it is almost impossible to change the record because of its immutability nature. The only attack that can affect the blockchain mechanism is 51% attack which is performed by the miners before committing the block finally on blockchain [6]. The digitized information can be utilized by various evolving technologies, i.e. Big data, IoT, but the blockchain have given the new wings to the secured digital information without getting any attack or tampering of information. Its architecture has the inclusion of the DLT (Distributed Ledger Technology) which provides the better execution of decentralized applications with immutable records. There were many consensus protocols have been provided in the blockchain network, i.e. PoW, PBFT, PoB, PoS [7]. Each consensus had been evolved based on the demerit of a previously designed consensus protocol, like PoS was designed to overcome the problem of PoW, similarly to do with PBFT, PoS. PoW consumes a considerable amount of power in the execution of the process and sometimes leads to the monopoly in the mining process [8]. So, to overcome these problems of PoW, PoS consensus protocol was given with the most valuable concept which provided the equality to miners in the execution process. Initially, blockchain was designed to make various operations dependent on cryptocurrency [9]. But later on, consequences which rely on the digital currencies generate innovation in the application of blockchain to the other area like the medical industry, financial institutions, government compliance [10]. Since blockchain has various inbuilt features like decentralization, immutability, secured peer to peer connectivity, digital signatures and cryptography, and each of them mainly focuses on the internal functionality of the blockchain network. The most beautiful feature of the blockchain is transparency in which every peer can observe the transaction record on the block, but cannot change it because the hash value of the existing block is connected with a hash value of the previous block. The security becomes stronger when Merkle tree plays its crucial role in arranging and connecting the hash values in a hierarchical format with the upcoming blocks in the blockchain, which are to be committed [11]. There is always a significant concern of majority voting regarding security which means if any unauthentic task or process absorbs the 51% of majority voting, then consensus can be reached on stated goal in the wrong direction [4].

II. Related Work

In the present scenario, online transactions and digital information are being promoted day by day. This digital transformation has provided the concept of digitized information which has evolved the perspective of transfer of information in very less time and cost. There is one more concept of timestamping in which a stamp is put on every digital document with TS (time of the creation of digital document) before transacting it over a network so that receiver cannot deny further that has not obtained the transaction record [12]. When Bitcoin was proposed first time as application of blockchain, then there were several limitations with the proposed system like it was only designed to increase transaction of digital currency and to remove the third party acting as mediator among countries to change the currency value liable to the corresponding country [13]. Later on, when the blockchain started spreading its arms in other sectors of software development, then it gets more fame all over the world. When one or more organizations come together to work on a defined goal without any trust issue, then this system is called as consortium blockchain which performs the PBFT consensus protocol with state machine replication [14]. There were several problems which were still alive even after the concept of digital information as the KYC process prefers paperwork rather than any digital platform because KYC is getting performed based on the visual appearance of the consumer [3]. It also prefers the offline mode due to some security concern, but Perry Mayo has provided some glimpse to modify the KYC process by using DLT (Distributed ledger technology) for efficient system performance and to reduce various costs involved in the KYC process. He has proposed a blockchain-based KYC system that enhanced efficiency and reduced the cost of the KYC customer-onboarding process **[**15**]**. Rutter illustrates the advantage of decentralizing the KYC process and gives an applied depiction and examination of two diverse, decentralized situations run on Corda – in particular, the self-sovereign model' and the 'bank sharing model'. Norvill et al. [16] proposed a blockchain-based KYC proof-of-concept system which is a tool for managing private blockchain environments. Moyano et al. [17] presented a system that allows automation and permission document sharing to simplify by reducing the Work required by the KYC process.

III. Proposed Methodology

As of now, we have discussed such a large number of existing issues in a KYC framework like centralization, traffic force, adaptability and dependability angles and so on. It is an estimation that after utilizing the blockchain framework, we can decrease the expense of around $27 Billion in a year over the globe. Here an inquiry comes as a top priority that, how might we improve or what technique ought to be executed to make this estimation right? We can classify our methodology by some following set of points. We want a system in which some organizations come together to exchange the information among themselves using predefined protocols. In the present scenario, every organization is performing its KYC process. If any user wants to bear the facility offered by that particular organization, then he must pass through the KYC process of that organization. Any organization does not consider the KYC process approved by other organization because they want to have the KYC approval only based on its protocols, rules and regulations. We want to design a system in which, if anyone organization has already performed the KYC process by any person, then it should be accepted by other organizations. Since there may be various issues among the organizations regarding the sharing of information which sometimes become very critical, so we want to provide a system in which organization may resolve the issues regarding the sharing of information (Privacy and Integrity of information). In the current scenario, if a person provides his documents like Aadhar card, pan card, passport and

driving license or any other government-issued document to any organization for KYC, then that organization verifies these details with the corresponding authority (i.e. Aadhar card to UIDAI, pan card from UTITSL). So, all that is needed to bring all the organizations on a common platform using such system which can reduce the time of KYC by maintaining a public ledger inbuilt with immutability in which organizations can easily verify the details. KYC optimization developed using blockchain Smart Contract technology because we have found this innovative platform which suits our requirement with almost uncrackable cryptographic security. In the proposed methodology, every organization which is representing itself as a peer in a consortium network can only verify the details instead to temper it.

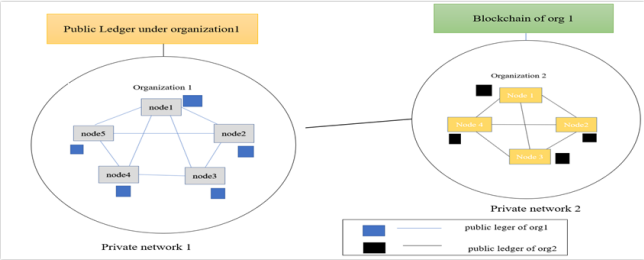


Figure 1: Consortium Blockchain Model

It has developed a consortium blockchain model, as shown in the above figure. The consortium can be defined as a collaborative approach where multiple organizations come together to perform appropriate tasks according to the designed protocols. Such a proposed system comes under permissioned model, and any organization can request the information using their service identity proof. In the proposed system, identity will be provided to every organization to track the record. The immutability and cryptographic feature of blockchain make this system relax from the tempering of data. The maintenance cost of duplicate information will also be removed, and paperwork will be much reduced because data will be stored online on the blockchain. Finally, internal functioning inside every organization will be distributed, but it seems to be a single unit from outside. Blockchain executes such efforts in a very flexible and reliable way.

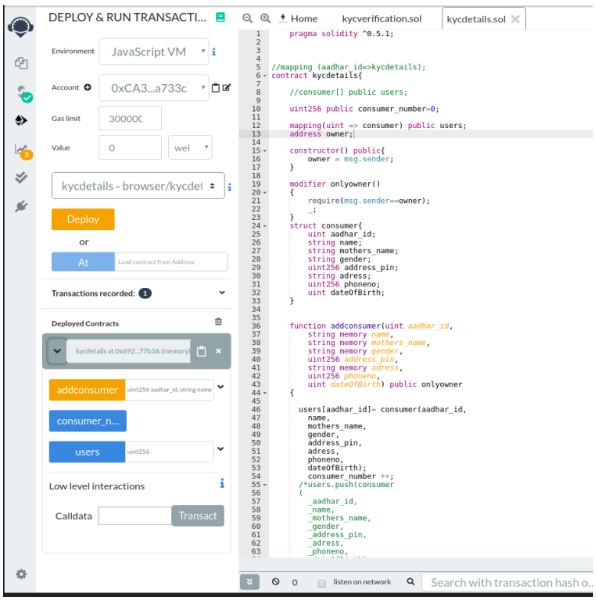
IV. Tools and Implementation

Since blockchain has been provided with many sets of tools, but still we require some specific tools to execute our methodology to enhance or optimize the existing KYC framework. We have picked the Ethereum blockchain development platform to grow such a belief system, so we have to talk about the devices and steady components in a nutshell. We have utilized the instruments referenced beneath. The Remix is an IDE in which smart contracts can be written in the solidity programming language, and it is very smooth functioning IDE which provides many features using which we can connect directly to our blockchain network by enabling injected web3 provider mode of Remix IDE [18]. It provides the feature to check whether our smart contract is working according to our need or not. It provides a better GUI features to understand that what actually is happening in processing. Remix can be accessed via https://remix.ethereum.org/. Metamask is a tool that is injected to our web browser, and that can provide access to the blockchain network from our local browser. Metamask also helps to transact the ether (Ethereum digital currency) to any desired location by providing the receiver's transaction address. Meta mask can be accessed and configured via https://metamask.io/. Ganache is a tool that provides the personal blockchain environment for the Ethereum development used to deploy our smart contracts, develop our applications and run them in our local machine [19]. It can be used by getting GUI (graphic user interface) and also by getting command-line utility. But here in this proposed model, Ganache has been used only to visualize the local blockchain running system. Ganache GUI can be downloaded from https://www.trufflesuite.com/ganache. Ganache CLI (command-line utility) can be installed on a local machine (in Linux terminal) using - npm install -g ganache-cli [20]. In the existing system, data is stored on the central server using some set of parameters of the consumer like Aadhar id or any government-issued id, personal phone number, name, mother's name, father's name, gender, date of birth, address, address pin. The proposed system has also suggested using some of these parameters to proceed with the implementation with the basic architecture of KYC to maintain the integrity of the KYC protocol. The Smart Contract (business logic, which follows some programming paradigm) has been written to utilize such parameters, and all the input details of the consumer will be received under this smart contract. However, Ethereum provides much flexibility to choose the configuration of tools because it has acquired a variety of services, tools and platform, but we choose the remix platform to write the smart contracts in solidity, high-level programming language. After configuring the remix environment, we have used some primary data types needed to store details like unit (i.e. an unsigned integer) to store numeric values according to our bit value, and for high bit value of any particular literal of providing detailed, we can use uint256. Similarly, other formats of uint1 to uint256 can be used as per need of designing protocol, and string data type is used to store literal string values of providing string user input. Following code is the smart contract to store the information of the persons coming with the information on given parameters and attributes given below is based on the design of our protocol.

```
pragma solidity ^0.5.1;
contract kycdetails{
uint256 public consumer_number=0;
mapping(uint => consumer) public users;
address owner;
constructor() public{
owner = msg.sender;
}
modifier onlyowner()
{
require(msg.sender==owner);
_;
}
struct consumer{
uint aadhar_id;
```

```
string name;
string mothers_name;
string gender;
uint256 address_pin;
string adress;
uint256 phoneno;
uint dateOfBirth;
}
function addconsumer (uint _aadhar_id,
string memory _name,
string memory _mothers_name,
string memory _gender,
uint256 _address_pin,
string memory _adress,
uint256 _phoneno,
uint _dateOfBirth) public onlyowner
{
consumer_number ++;
users[_aadhar_id]= consumer(_aadhar_id,
_name,
_mothers_name,
_gender,
_address_pin,
_adress,
_phoneno,
_dateOfBirth);
}
}
```

This smart contract provides the number of blocks in the blockchain and also provides the number of users coming from the KYC process. Record of each person is stored in a separate block in the blockchain. Add consumer function will get the user information and add the information about the user to the blockchain. Its Aadhar id number can search the information. The information retrieved is in encrypted form except for open details. Generally, For Deployment with Metamask undoubtedly injected web3 mode is selected, but to run the smart contract on Remix, it is deployed with the selecting JavaScriptVM mode in the environment module.



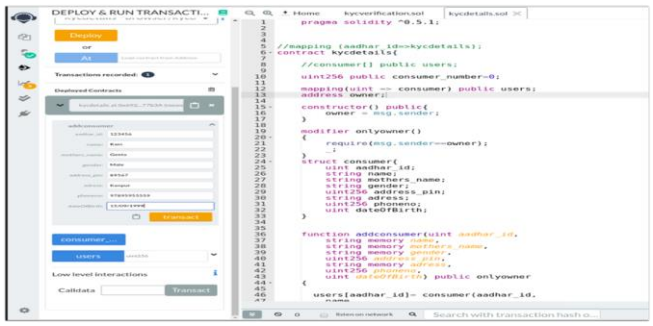


Figure 2: Deployment of Smart Contract on Remix

The smart contract written in the solidity programming language ought to be spared with .sol augmentation. At the point when it will be spared with the .sol expansion, at that point the document will have appeared with the featured worth that is what we call full-scale portrayal of robustness in the Remix. In over two figures of Remix, one speaks to the error, tossed by the solc compiler and other shows the fruitful compilation. When the program is effectively ordered, it will approach to distribute the smart agreement on one of two inbuilt conventions provided in Remix; however, we needn't bother with it because we'll utilize the Metamask to deploy the smart contract instead to use those conventions. After successful compilation, we need the tool Metamask so we'll configure the Metamask to deploy the smart contract.

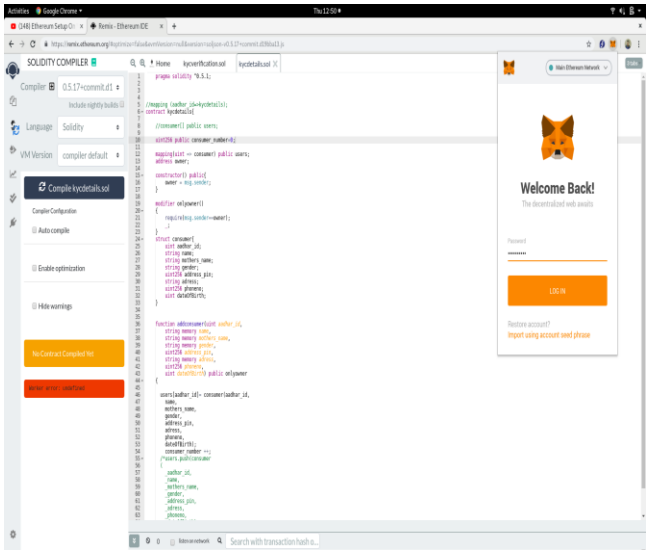


Figure 3: Configuration of Metamas

V. Deployment of Smart Contract with META MASK

Metamask gives us different highlights and distinctive system modes, but we picked the leading Ethereum network to deploy the smart contract. It likewise gives the QRcode of owner account. Ganache has been installed and configured, which can give us a genuine representation of the local running blockchain system. Ganache gives us the best approach to send smart contracts yet here. After setting up the Ethereum environment, we have to deploy the smart contract using Metamask whatever we have structured on the Remix, and that is possible by selecting the injected web 3 transaction module in the Remix. At the point when we attempt to send the smart agreement utilizing injected web

3, then a pop-up screen opens which associates the smart contract module to the transaction address to initiate the contract logic. The smart contract gets associated with a transaction address, but it is initiated when that transaction would be initiated.

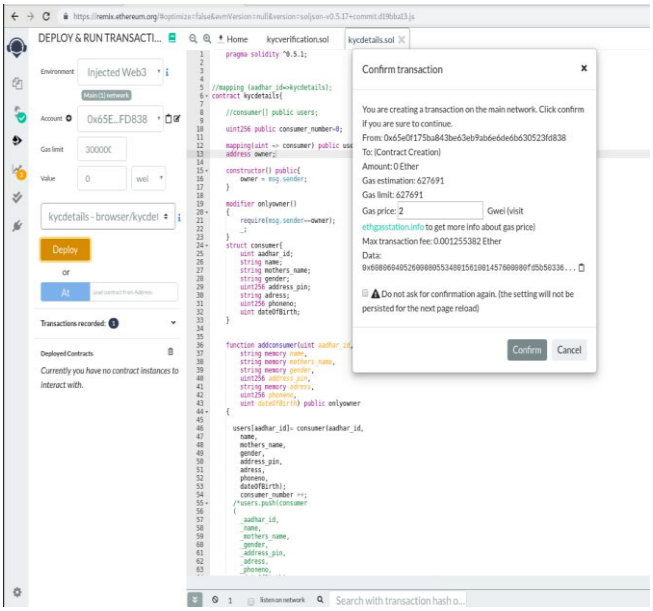
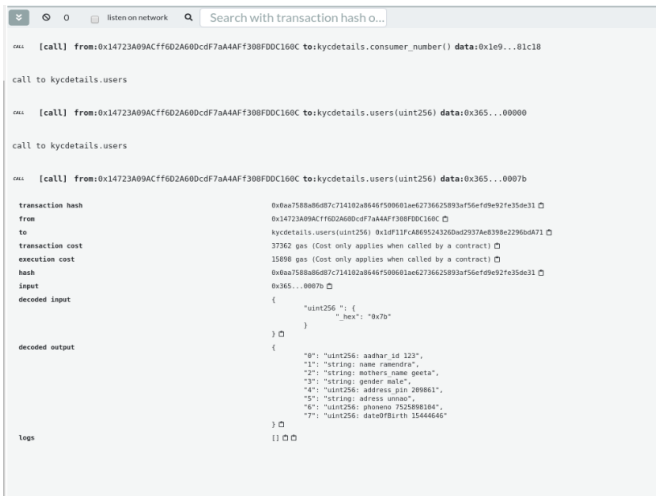


Figure 4: Deployment of Remix Smart Contract with Metamask Account

When the proper connection is established between Metamask and Remix, it will ask for the confirmation on a pop-up window whether the smart contract should be implemented with your account (transaction address) and provides the information about gas consumed, fees in ethers before final contract creation and deployment. Metamask also provides the details of the attached information with a smart contract that is to be transferred through transaction address in hexadecimal format with encryption using Keccak256 so that any outlier cannot guess the real data initiated on transaction address. One primary concern in the proposed system is that we are considering a single transaction address as a transaction address of the whole organization without worrying about the distributed peers working in the organization. They come to participate in this consortium blockchain network



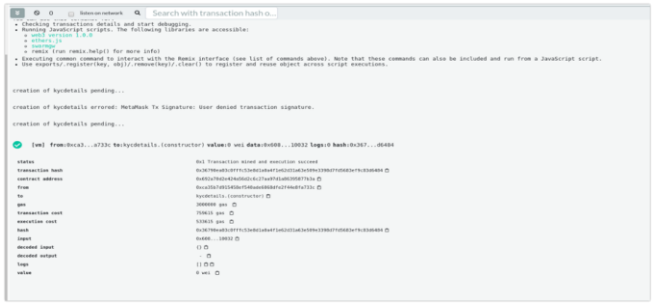


Figure 5: Final Committed Block

VI. Conclusion

In conclusion, it can be stated that many innovative technologies like DLT (distributed ledger technology) and blockchain has collaboratively led the system of KYC optimization using blockchain smart contract technology advancing to the new era. It has been discussed in the perspective on which this system relies, in comparison to the existing system, but the way of handling the events seems to be complicated, sometimes using these technologies. It is because of the simultaneous handling of various modules like web 3, smart contract, network management, message passing system. But finally, this system reduces the aggregation cost, opportunity cost, management cost. These types of minor costs lead to a dynamic change globally. It also reduces the effort of the customer by getting everything online and in a very much secured way over a non-secure channel. This system is also able to reduce the formal regulatory cost, to provide better user experience, reliability among organizations. Finally, there can be more competition further with this approach because of fewer barriers in financial institutions. Further, more optimization may also be possible by integrating the blockchain technique with Big data, artificial intelligence and IoT for smooth execution of over huge population and different paradigms.

References

[1] Vukolić, Marko. "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication." In *International workshop on open problems in network security*, pp. 112-125. Springer, Cham, 2015.

[2] Pilkington, Marc. "Blockchain technology: principles and applications." In *Research handbook on digital transformations*. Edward Elgar Publishing, 2016.

[3] Lopez, David, and Bilal Farooq. "A multi-layered blockchain framework for smart mobility data-markets." *Transportation Research Part C: Emerging Technologies* 111 (2020): 588-615.

[4] Haber, Stuart, and W. Scott Stornetta. "How to time-stamp a digital document." In *Conference on the Theory and Application of Cryptography*, pp. 437-455. Springer, Berlin, Heidelberg, 1990.

[5] Haber, Stuart, and W. Scott Stornetta. "How to time-stamp a digital document." In *Conference on the Theory and Application of Cryptography*, pp. 437-455. Springer, Berlin, Heidelberg, 1990.

[6] Nakamoto, Satoshi. *Bitcoin: A peer-to-peer electronic cash system*. Manubot, 2019.

[7] Yadav, Ashok Kumar, and Karan Singh. "Comparative Analysis of Consensus Algorithms and Issues in Integration of Blockchain with IoT." In *Smart Innovations*

in Communication and Computational Sciences, pp. 25-46. Springer, Singapore.

[8] Bentov, Iddo, Ariel Gabizon, and Alex Mizrahi. "Cryptocurrencies without proof of work." In *International conference on financial cryptography and data security*, pp. 142-157. Springer, Berlin, Heidelberg, 2016.

[9] Jaag, Christian, and Christian Bach. "Blockchain technology and cryptocurrencies: Opportunities for postal financial services." In *The changing postal and delivery sector*, pp. 205-221. Springer, Cham, 2017.

[10] Yadav, Ashok Kumar, and Karan Singh. "Comparative Analysis of Consensus Algorithms of Blockchain Technology." In *Ambient Communications and Computer Systems*, pp. 205-218. Springer, Singapore, 2020.

[11] Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. "Blockchain challenges and opportunities: A survey." *International Journal of Web and Grid Services* 14, no. 4 (2018): 352-375.

[12] Kapsoulis, Nikolaos, Alexandros Psychas, Georgios Palaiokrassas, Achilleas Marinakis, Antonios Litke, and Theodora Varvarigou. "Know Your Customer (KYC) Implementation with Smart Contracts on a Privacy-Oriented Decentralized Architecture." *Future Internet* 12, no. 2 (2020): 41.

[13] Shbair, Wazen, Mathis Steichen, and Jérôme Francois. "Blockchain orchestration and experimentation framework: A case study of KYC." 2018.

[14] Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance and proactive recovery." *ACM Transactions on Computer Systems (TOCS)* 20, no. 4 (2002): 398-461.

[15] Parra-Moyano, José, Tryggvi Thoroddsen, and Omri Ross. "Optimised and dynamic KYC system based on blockchain technology." *International Journal of Blockchains and Cryptocurrencies* 1, no. 1 (2019): 85-106.

[16] Norvill, Robert, Mathis Steichen, Wazen M. Shbair, and Radu State. "Blockchain for the Simplification and Automation of KYC Result Sharing." In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 9-10. IEEE, 2019.

[17] Moyano, José Parra, and Omri Ross. "KYC optimization using distributed ledger technology." *Business & Information Systems Engineering* 59, no. 6 (2017): 411-423.

[18] Dika, Ardit, and Mariusz Nowostawski. "Security vulnerabilities in ethereum smart contracts." In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 955-962. IEEE, 2018.

[19] Mohanty, Debajani. "Deploying smart contracts." In *Ethereum for Architects and Developers*, pp. 105-138. Apress, Berkeley, CA, 2018.

Fridgen, Gilbert, Jannik Lockl, Sven Radszuwill, Alexander Rieger, AndrÃ Schweizer, and Nils Urbach. "A solution in search of a problem: a method for the development of blockchain use cases." (2018).