# A Framework for Enhancing Digital Trust of Quranic Text Using Blockchain Technology

Hassan Abubakar[1] and Suhaidi Hassan[2]
[1]*Department of Computer Science, Federal Polytechnic Bauchi, Nigeria.*
[2]*School of Computing, Universiti Utara Malaysia, 06010 UUM Sintok, Kedah, Malaysia.*
*ahassan@fptb.edu.ng*

***Abstract*—The Holy Quran is the fundamental Islamic scripture revealed to the Prophet Muhammad (Peace and Blessings of Allah be upon him) for the past 1400 years. In today's Internet, there exist online sources which provide incomplete or false Quranic text which may either be published deliberately or unintentionally. The research investigates the possibility of developing a digital trust framework that secures the integrity of the Quranic text using blockchain technology. The research uses blockchain technology as the emerging secured distributed ledger to establish digital trust. The Ethereum blockchain platform was used to validate the proposed framework. The proposed digital trust framework was developed in a three-level architecture consisting of participants, digital trust and Quranic text. The key components of the proposed framework were found useful in Ethereum blockchain platform for effective use in distributed ledger, distributed consensus, smart contract, decentralized application development and cryptographic algorithms for database encryption and user authentication in Whisper, Swarm and Ethereum Virtual Machine (EVM). The findings show the effectiveness, efficiency and usability of the proposed digital trust framework on the Ethereum blockchain platform and demonstrate how user of Quran and blockchain miner interact with the system to verify and validate Quranic content. The research has recommended the use of blockchain technology to secure the integrity of the Quranic text. The work facilitates the protection of the Quranic text as well as proving a mean to verify the authenticity of the Quranic content.**

***Index Terms*—Digital Trust; Quranic Text; Blockchain Technology; Distributed Ledger; Ethereum Blockchain**

## I. INTRODUCTION

The research framework remains a process on which knowledge and ideas can be discovered and applied in solving problems. Research questions, hypothesis and objectives are fundamental to the development of any research framework [1]. The increase in the publishing of forge Quranic text which had been experiencing recently in circulation is a great issue to the Muslims Ummah of this generation. There are several online Quranic texts that contain missing letters, words, wrong statements, both deliberate and accidental mistakes [2, 3]. The Holy Quran remains the fundamental guidance for all Muslims in all their actions and daily activities. There are more than one billion Muslims in the world and there is a need for the distribution and maintenance of digital Quranic text. In this generation of the digital and handheld devices, it can be an uncomplicated way for the distribution of the Quran to the hand of every Muslims. The holy Quran was built upon 114 surahs and 6,236 ayat [4]. Muslims have faith, belief and regard to the Quran in high order and a great path for successful life [4, 6].

The digital trust is a mechanism that strengthening believes, confidence and good expectation. Despite that trust is regarded as dynamic, developing a digital trust framework in compliance with blockchain technology provides a way for distributed consensus with secured channels of communication using cryptographic algorithms such as private-public key, secret key and hash functions to implement trustless system. The Blockchain technology can also be described as a shared decentralized ledger system that uses decentralized consensus to verify and validate any record on the ledger and these had been used in various field to solve problems related to trust. The blockchain technology had been implemented on so many applications, that until now no successful attacks was recorded due to the techniques involved in the construction [6, 7, 8, 9].

The research has two objectives, firstly to develop a digital trust framework for the Quranic text using blockchain techniques and secondly to evaluate the validity of the proposed digital trust framework using Ethereum blockchain platform. However, the research was conducted within four months. The previous research depends on the centralized client-server system whereas the current research supported decentralized peer-to-peer system to enhance the digital trust of the Quranic text with the deployment of secured distributed database, distributed consensus and cryptographic algorithms to provide protection and integrity to the digital Quranic text.

## II. RELATED WORKS

The literature discusses the related issues on research framework, digital trust, Quranic text and blockchain technology in an effective and concise way.

The research framework is the development of an understandable demonstration and representation of ideas derived from concepts and theories, by describing the impact and relationships of each component to one another. A concept is a process at which an idea about an issue or thing can be represented in a more understandable way. Therefore, A concept can be defined as a complete or general idea of the topic of discussion. However, a theory is a collection of an understanding that was derived from concepts. The fundamental idea of a research framework is the formulation of concepts and theory which is beneficial to the understanding of knowledge, ideas and wisdom. A conceptual framework is a systematic arrangement of concepts and theories that were coined to produce detailed understanding of knowledge. Whereas, a theoretical framework is a relational literature mapping in the concepts [1]. The theoretical framework is very important in each stage of research and serves as the fundamental on building any

knowledge. The theoretical framework can be referred to as the "blueprint" for the entire research inquiry and provides the structure to define how to deploy philosophy, epistemology, methodology, and analytical approach of the entire research [11].

There are several research frameworks related to digital trust such as policymaker, trust framework model [12], trust models [12, 13], trust builder [15], Marsh's [13], Ad hoc trust framework [15], web of trust, trust policy language, distributed trust model [16], PGP, and Bayesian model [17]. The conceptual framework is specifically focusing on Quranic text validation [2, 3]. Trust is of immense importance when talking about block-chain [18]. The research's conceptual framework has mapped the experimental elements of digital trust in the context of blockchain technology such as distributed consensus, distributed ledger, cryptographic algorithms and smart contract.

## III. Digital Trust

Trust is a concept that can be found in various field of studies such as psychology, sociology and computer science with different approaches, definitions and understanding [11, 12]. There is no unique definition of trust [19]. Generally, trust can be defined as the measure of confidence, expectation, belief, and reliability an entity has for another entity [19, 20, 21, 23]. Trust in the computing is divided into user and system trust [24]. The components of trust are neither static nor objective in nature. However, the key to the successful development of any digital trust system is by understanding digital trust as directed, subjective, context-dependent, measurable, experience, dynamic, transferable, and composite property [19, 20, 22].

The digital systems have been attacks by various intruders and malicious attackers and some of these attacks were done successfully in such a way that a digital trust was being compromised or hacked. The identified types of attacks are divided into masquerading, replay, message modification, and denial-of-service (DoS) [24, 25, 26,27]. The digital trust can be achieved by deploying effective security mechanisms that can be used to encounter any invalid operations on the digital system [29]. Digital trust framework can be implemented by clearly understanding of risks and threats as well as security mechanisms to handle their impact on digital systems [30].

## IV. Quranic Text

The Quran is a book on which all Muslims believe in it as guidance from Allah. Quran is the basic source of Islamic jurisdiction and knowledge. There are about two billion people that are now reading and seeking Quranic knowledge both from Muslims and other faiths. The holy Quran has contained 114 chapters and 6,236 verses. Therefore, The Quranic text throughout the world remains the same for several decades [5], 30, 31]. However, [2, 3, 5,] recently research shows that there are incremental publishing of forge Quranic text, specifically on the Internet. There are several copies of such Quran in the hands and mobile devices of many Muslims [2, 3, 5,]. However, today, there are many Quranic applications and websites that were hosted online for the distribution of Quranic text and other Islamic books. There are some authors that describe the number of Quranic text online to reach about more than twenty- million copies [2, 3, 4, 32].

There are several available techniques that can be used to enhance the Quranic text integrity, availability and confidentiality and at the same time secure distributions. There are some researchers with the view that digital trust is just a good relationship between the interactions entities [34]. Table 1 describes various researches for protecting the integrity of the Quranic content.

## V. Blockchain Technology

Blockchain technology was first proposed together with the Bitcoin cryptocurrency, on 31st October 2008 by a person or group of persons Satoshi Nakamoto in a paper entitled "Bitcoin: A Peer-To-Peer Electronic Cash System" [36]. The blockchain is a decentralized database that uses cryptographic techniques in a distributed consensus to verify and validate transaction as well as replicating each transaction and storing it permanently in a chain of blocks. Each node on a blockchain network keeps and update the same content of a ledger. The cryptographic hash function was used to prove the ownership of digital assets or digital events. The blockchain is a technology that was built upon some existing technologies such as distributed ledger, replicated peer to peer, distributed consensus, cryptographic algorithms and smart contracts [ 6, 7, 37, 38, 41].

The blockchain technology allows the automatic execution of terms of agreements between two or more entities without paying for extra party services or legal entity certification. Each transaction has reference to the previous block using hash function to validate the current and future transactions and public-private key system for authentication. Each block on blockchain ledger is recorded base on hashing and timestamp of the transaction. This makes it difficult to reverse or delete a transaction. Each transaction must undergo distributed consensus for it to be considered as valid or invalid. The blockchain uses an open source programming language for software development and must of the blockchain software are free downloadable software which can be operated after the installation on a user node and that make the user as network participant of a blockchain network [6, 7, 34, 35, 49]. The blockchain keeps the records of the transactions in units of blocks. Each block includes a unique ID and the ID of the preceding block. Any miner may add a valid block to the chain by simply publishing it over the network to all other miners that are connected by peer-to-peer network [42]. Miner has their own copy of the blockchain. that solved it. The blockchain itself does not live on any central server. Every blockchain includes the hash value of the previous block, a list of transactions, and the nonce 'blockchain'. The solver of the block is rewarded with some number of Bitcoins [43].

Table 1
Related Quranic text research works [35]

| No. | Approach Used | Findings | Limitations | Evaluations |
|---|---|---|---|---|
| 1. | SQL Query Approach | Algorithm has been proposed for detection of Arabic verse | 1. Not efficient enough as Major user need to know the verse to be verified is from which chapter. The approach is prone to fail if user doesn't know the surah name.<br>2. The algorithm will fail if there is last verse of one surah and first verse of consecutive surah | Two parameters, i.e. "verified and authenticated" and "tampered with" are taken |
| 2. | Hashing | A method based on hashing to authenticate and verify Quranic verse. | 1. Suitable for single verse only.<br>2. Hash Collision can occur.<br>3. Diacritic and non-diacritic Arabic verse will give different hash values. | No performance metric evaluated. Evaluation done based on comparing hash values of different text. |
| 3. | SQL Query approach | A Framework has been proposed to detect and authenticate Quranic text. | 1. Not suitable for non-diacritical text.<br>2. Complexity of the algorithm will increase with more complex diacritical verse. | Accuracy, Precision and recall have been taken as evaluation parameters |
| 4. | Regular Expression approach using SQL queries | A Framework is proposed which can authenticate Quranic verses. | For finding a verse, user need to enter surah- name also which is one of the major limitations of this approach | For Evaluation purposes, accuracy metric has been taken and benchmarked with Ketaballah.net, Muslim-web.com, Holyquran.net |
| 5. | ASP.dot Net platform has been used to develop the system | A new search engine "truth-search-now" has been proposed. | Could not locate the proposed engine online. | Performance of 5 search engines with respect to Islamic contents have been evaluated by measuring search time. |
| 6. | Zero -watermarking | Zero-watermarking approach has been identified as an effective technique to authenticate image-based document | Limited to Image format only. Whole document is hashed like hashing. | Not any evaluation parameter taken. Only encoding time and decoding time mentioned. |
| 7. | Hybrid approach of watermarking and digital signature | Zero-watermarking approach has been used to authenticate image-based document | Limited to Image format. This approach is prone to fail when text input is given. Overhead of storing keys | Not any evaluation parameter taken. Only encoding time and decoding time mentioned |
| 8. | Cryptography and Hashing. | Hybrid approach of AES and RSA is proposed to protect text document from tampering | 1. Lack of proper methodology.<br>2. No pseudo code of hybrid algorithm mentioned. | No experimental results shown |
| 9. | Invisible watermarking and hashing | Invisible watermarking approach based on LSB is proposed | 1. Not valid results due to lack of experiments.<br>2. Limited to Pdf format only | No Experiments done and discussed. |
| 10. | Watermarking | A general framework regarding authentication of website content is proposed | 2. Based on the manual authentication mechanism where RA is assigned to authenticate websites. | Not experimental.<br>General architecture proposed. |
| 1.1. | Fragile Watermarking | Image-based authentication of Quranic images based on fragile watermarking is proposed and proposed algorithm shows significant improvement. | Limited to image only | Top four Quran applications from Android have been taken for experimental purposes. Four evaluation parameters, i.e. Average processing time, Average PSNR value, detection and recovery are taken. |
| 12. | Machine Learning Approach | Machine learning approach has been proposed for classifying Quranic words from Non-Quranic words | Limited to Image format only. | Three parameters, i.e. accuracy, precision and F- measure have been taken for evaluation purposes on 4 different data sets. |
| 13. | Fragile Watermarking | Fragile watermarking approach has been proposed to protect Quran from tampering. | Limited to Image format only | Two metrics, i.e. Bit Error rate and PSNR are taken for evaluation purposes. |
| 14. | Fragile Watermarking | Fragile watermarking approach has been proposed to protect Quran from tampering. | We could not find any major difference between the two approaches proposed by the same author | Two metrics, i.e. Bit Error rate and PSNR are taken for evaluation purposes |
| 15. | Fragile Watermarking | Fragile watermarking approach has been proposed to protect Quran from tampering | Limited to Image format only. No major difference between the previous approaches proposed by the same author | Three parameters, i.e. PSNR, Pearson Correlation Coefficient (PCC) and Normalized Hamming Distance (NHD) are taken for evaluation purposes |
| 16. | Not mentioned | Quran authentication system has been proposed. | This work is just an idea towards developing Quran authentication system. | Simple prototype has been shown, how future Quran authentication system will work. |
| 17. | Steganography | A technique based on steganography has proposed to protect the Quranic document | Limit to Image only. Needs. There is no experimental evidence to prove this technique is prone to various tampering attacks. | There is no specific metric taken for evaluation purposes. |
| 18. | Feature code watermarking | A method based on embedding security bits in Kashida is proposed | 1. Limited to Image only.<br>2. Need to test the proposed approach using different kind of attacks. | There is no specific metric taken for evaluation purposes. |
| 19. | Watermarking | An enhanced approach based on singular value decomposition (SVD) for watermarking the data is proposed | Limited to Image. There are no benchmark results shown from previous work. | For evaluation purposes, 5 parameters have been taken: Peak Signal-to-Noise-Ratio (PSNR), Structural Similarity Index (SSIM), Visual Information Fidelity (VIF), the Universal Quality Index, Noise Quality Measure (NQM) |

Blockchain networks are decentralized in such a way that all participants in an operation or transaction are linked without intermediaries, so that, each transaction is transparent to all the participants in the network. It has been described as a value network, where parties can transfer custody of valued assets in an auditable manner without relying on intermediaries, and it deployed trust and provenance mechanisms in such a way that transactions on the blockchain do not require any authorization, validation or verification by a trusted third party or intermediary. The blockchain provides irrefutable evidence that the data in a block existed at a time, and because each block contains a hash of the header of the preceding block, this creates automatic proof of the history, position and ownership for each block on the chain. Blockchain has resilience and irreversibility operation as blockchains are designed for secure distributed operation in a peer network of public-private cryptographic nodes, or computers, each of which holds a copy of the entire blockchain, thereby making it extremely resilient, much like the internet. Once data or transactions are appended and accepted or confirmed by the nodes on the blockchain, it is nigh impossible to change or alter it [44]. The blockchain is essentially an append-only data store (no deletes or edits allowed), hence its capability and suitability as an unimpeachable record keeper. the blockchain uses cryptography and the power of distributed computing to provide a digital trust mechanism over the Internet [38].

*A. How Blockchain Work.*

Several descriptions on how blockchain works were given by many research, specifically by explaining the scenario of digital currency transfer using blockchain technology as described in figure 1 below. The most general scenario is that a user initiates a transaction, the transaction is broadcast to all nodes on the blockchain network in an encapsulated format called "block". The blockchain network verifies and validates the transaction using various replicated ledger within the network. However, the approved and confirmed results of the transaction is broadcast to all the nodes on the network. The confirmed block is added to the ledger in a linear, encrypted and chronological order to the chain. The completed block gives way to the next block in the blockchain. Therefore, the main working processes of blockchain are the sending node that records new data and broadcasting to network. The receiving node checked the message from those data which it received, if the message was correct then it will be stored to a block. All receiving node in the network executes proof of work (PoW) or proof of stake (PoS) algorithm to the block. The block will be stored into the chain after executing consensus algorithm, every node in the network admit this block and will continuously extend the chain base on this block [45].

The above scenario described blockchains as a specific kind of distributed ledger on which the transactions processes involves conversion of data into block, data encryption, transaction ordering and verification and validation of any transactions before recorded and inclusion on blockchain public ledger. The blockchain happens to be the network of computers that maintains and validates a record of consensus of transactions through a cryptographic algorithm with various protections against tempering and revision. The blockchain avoids centralized authority such as clearinghouse. The participants in the blockchain network possess all the records of transactions that took place on the network and it always produces an immutable record [8]. Therefore, if there is need to execute proposed transactions, some or all the nodes on network verifies according to an agreed-upon algorithm called the consensus mechanisms. The records of transactions in block-chains are stored as an encrypted and linked block on the nodes which produce an audit trail [37].

Bitcoin as the first application of blockchain which was launched with the intention to bypass government currency controls and simplify online transactions by getting rid of third-party payment processing intermediaries. Bitcoin transactions are stored and transferred using a distributed ledger on a peer-to-peer network that is open, public and anonymous. Blockchain is the underpinning technology that maintains the Bitcoin transaction ledger. The scenario on how Bitcoin blockchain work is that the database is distributed across a peer-to-peer network and operate without a central authority, network participants must agree on the validity of transactions before they can be recorded. This agreement, which is known as "consensus," is achieved through a process called "mining." After someone uses Bitcoins, miners engage in complex, resource-intense computational equations to verify the legitimacy of the transaction. Through mining, a "proof of work" that meets certain requirements is created. The proof of work is a piece of data that is costly and time-consuming to produce but can easily be verified by others. The transaction can only be valid on the blockchain if an individual record has a proof of work to show that consensus was achieved. By this design, transaction records cannot be tampered with or changed after they have been added to the blockchain. The transaction in the Bitcoin blockchain is verified by consensus of most of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made [46].

*B. Key Components of Blockchain.*

The blockchains networks have been adopting some tools and principles in the successful implementation of the system. However, these tools, principles and techniques work together to form what is known today as the blockchain technology. Basically, there are in any blockchain network tools or components that work together to provide secure communication and distribution of rights and privileges based on terms and conditions of the blockchain network. The common tools on the blockchain networks comprise the following:

*Decentralized application*-There are various blockchain decentralized applications. The most popular one is Bitcoin wallet, Ethereum Wallet and Hyperledger digital wallet to mention few and these applications were developed to satisfy the specific purpose of the application. For instance, in the case of Bitcoin, a Bitcoin wallet keep a secret piece of data called a private key or seed, which is used to sign transactions, providing a mathematical proof that they have come from the owner of the wallet. Bitcoin wallet can be described as something that "stores the digital credentials for your bitcoin holdings" and allows one to access (and spend) them. Bitcoin adopted the use of public-key cryptography to satisfy the means of secured transfer and keeping digital currency in blockchain technology. Therefore, a wallet has a collection of two different keys, one public and one private. Blockchain technology can be applied to contracts, properties, certificates validation, electronic government implementation, voting,

decision making, Government and businesses. The information on blockchain is transparent and authentic and can be trusted by anyone [7].

*Distributed Ledger*-This is a blockchain component that manages data structure based on the decentralized application requirements. The distributed database or ledger was incorporating to work with the distributed or decentralized application to allow the network users to instantly view records and make transactions without trusted third party intervention. The data or information were shared across the nodes on the network. For instance, because of the distributed database, an Ethereum blockchain user can view the Ethereum ledger and interact with the network instantly through smart contract [47]. Blockchain technologies were basically divided into three types by implementation according to the distributed ledger technology (DLT). Public blockchain is the type of blockchain that everyone can check the transaction and verify it, and can also participate in the process of getting consensus. Like Bitcoin and Ethereum are both Public Blockchain. Another type of blockchain called "Consortium blockchains" in this type the node that had authority can be chosen in advance, usually has partnerships like business to business, the data in blockchain can be open or private, is Partly Decentralized. Like Hyperledger and R3CEV are both consortium blockchains. Lastly, Private blockchain, in this kind of blockchain node is restricted, not every node is allowing to participate on the blockchain, has strict authority management on data access [45].

*Cryptographic Algorithms*-A blockchain relies on cryptographic algorithms [48]. Majority of the Blockchain applications and platforms have built-in SHA-256 algorithm which was used to hash chain of digital signatures based upon asymmetric or public key cryptography. Each participant in the P2P network of Blockchain is associated with a matching public key and private key wherein a message signed by private key can be verified by others using the matching public key [42]. Some of the most commonly used hash approaches are Message Digest 2 (MD2) (RFC 1319), MD 4 (RFC 1320), MD 5 (1321), Secure Hash (SHA) and keyed Hash Message authentication code (HMAC). MD 2, MD 4 and MD 5 are also known as message digests suitable for hashing digital signatures into shorter values. Similarly, the SHA family is suitable for making larger message digests [35].

*Distributed Consensus Algorithm*-Consensus function is a mechanism that makes all blockchain nodes have agreement in the same message, can make sure the latest block has been added to the chain correctly, guarantee the message that stored by node was the same one and won't happened "fork attack", even can protect from malicious attacks [45]. The consensus algorithm in the blockchains network varies depending on the required objectives of the decentralized application. However, there are several consensus mechanisms implementation in the blockchain network. Proof-of-Work (PoW) was adopted by blockchain application such as Bitcoin and Ethereum. Proof-of-Stack was proposed by Ethereum to achieve scalability. Other blockchain adopted consensus like Proof of existence, Proof of Authority, Proof of Ownership and so on [7]. The consensus is being used to verify the authentication of a transaction in a blockchain. The Bitcoin blockchain reaches consensus on a global state change every 10 minutes on average whereas the Ethereum blockchain reaches consensus approximately every 15 seconds.

A proof of work is a piece of data which was difficult to produce to satisfy certain requirements. The Production of a proof of work is a random process with low probability, so it requires a lot of trial and error on average before a valid proof of work is generated. Bitcoin uses the Hash-cash proof of work. Bitcoin's use of a Proof of Work system is one of the defining and unique characteristics it has as a cryptocurrency. Bitcoin uses the SHA-256 hash function. The network performs hashing on the block sent by the miner and checks if it still fits the pattern for the next block, by doing this the network can easily prove that the new block found by the miner is legitimate. The difficulty for the calculation of the Proof of Work can be adjusted by the network so that a new block is found at approximately every 10 minutes, so it is unpredictable that which worker node in the network will generate the next block [42]. Proof of Work (PoW) generally refers to a mechanism to confirm a person's innocence by doing certain work for easy verification [37]. Proof-of-Work is used to verify the validity of transaction by recording each block of the transaction with reference or hash to the previous block so that any attempt at tampering with the order or the content of any past transaction will always and necessarily result in an apparent discontinuity in the chain of blocks [49]. A Proof of Stake meth-od have no need of electricity consumption as in PoW and might provide increased protection from a malicious attack on the network because the protocol had made it very difficult to an attacker to penetrate or has any effect to the system [45]. Proof-of-Stake was adopted to serve as an alternative to Proof-of-Work [50].

*Virtual Machine*-This is a blockchain component that helps the decentralized application to run on the client computer successfully. A virtual machine was described as the representation of a machine in either real or imaginary form, embedded to communicate directly with the computer system. Therefore, it was usually developed to serve as an abstraction of a computer working inside a computer. Both the Bitcoin and Ethereum implements a virtual machine. The Ethereum virtual machine was embedded in the Ethereum wallet, unlike Bitcoin. Therefore, Ethereum has a wider range of instructions that manage the state of the smart contracts. However, Ethereum virtual machine uses wallet to enforce the terms of the contract. The Ethereum blockchain contract cannot be tempered because of the built-in cryptographic integrity of information.

Ethereum becomes a blockchain platform that has the capability to developed and run all blockchains and protocols just like a unified universal development platform. Each full node in the Ethereum network runs the Ethereum Virtual Machine for seamless smart contract execution. Ethereum is the underlying blockchain-agnostic, protocol-agnostic platform for application development to write smart contracts that can call multiple other blockchains, protocols, and cryptocurrencies. Ethereum has its own distributed ecosystem, which is envisioned to include file serving, messaging, and reputation vouching. The Ethereum component include Swarm as a decentralized file-serving method and Whisper which is a peer-to-peer protocol for secret messaging and digital cryptography [7].

*Smart Contract*-Smart Contract is a digital contract that controls user's digital assets, formulating the participant's right and obligation, will automatically execute by computer system. It's not only just a computer procedure, it is one of a participant, that will respond to message what it receives and store the data, it can also send message or value to outside.

Smart Contract is just like a person can be trusted, can hold the assets temporarily and will follow the order which has already been programmed. Ethereum is an open source blockchain platform combining Smart Contract, offering decentralized virtual machine to handle the contract, by using its digital currency called Ether sometime uses ETH; people can create many different services, applications or contracts on this platform [45].

## VI. Digital Trust for Quranic Text Conceptual Framework

The Blockchain technology as a trustless platform becomes the best technique for preserving integrity of the Quranic text. Therefore, our proposed digital trust for Quranic text conceptual framework was explained in detail below. The proposed framework was developed based on a three-level architecture as described in Figure 1.

*Level 1 Participants*-These are two active members of the Quranic text network or intended to participate in the network. For a participant to possess membership right and privileges, must be an active participant of the network through registration. There are Quran users who use the system to check the validity of a Quranic ayah and other operation of the application. The second participant known as Quran miner, serve as a publisher of the Quran on the application. Both the Quran user and miner network are integrating to perform distributed consensus for Quranic ayah validation, whereas Quran miner network is responsible for publishing the Quranic ayah on the entire network. All active participants on the network have the same right and privileges of read or write on the network based on their registration terms. The rights and privileges of an active participant can be categorized as follows:

*User Computer system*-The participants have right to access, validate and display the Quranic content after been registered and log in to the system. All participant information was cryptographically encrypted, and the Quranic text was hashed on the distributed ledger system. The active participant nodes of the network can be a member of the blockchain consensus which will be used for verification and authentication of participants' Quran as in Figure 1.

*Level 2 Digital Trust*-The blockchain has been involved in various operation to produce reliable, efficient and effective result as it was designed to do. Blockchain provides the mechanisms of keeping and displaying the right information to the right participant at the right time, shared the information at timestamped. Here are some of the blockchain techniques and key characteristics that will be used in this research.

*Smart Contract*-The smart contracts for this study remain one of the fundamental reasons for trustless system as the major concern of blockchain with effort to remove the trusted third party is achieving. The record for contracts legal terms and conditions must be abided by each willing participant in the network. Each participant has a historical record of each operation on application which was recorded on shared ledger of each node of the network. A programming function is used to implement and execute the smart contract legal terms and conditions in accordance with blockchain techniques. Smart contracts execute most of the participants' operation automatically without human intervention, from the participants' computer system such as updating the ledger and directing other functions of the blockchain to be implemented. Smart contracts have deployed the used of the cryptographic algorithms such as public-private, secret key, and hash function to executed the trust less system on peer-to-peer distributed system. The users' information is encrypted and stored in distributed ledger in a real-time, immutable format. The encrypted information can only be decrypted by the authorized individual. The Quranic Ayah data were stored in hash format in the Quran distributed ledger. All the encrypted or hashed records appearing to the users in readable format.

The smart contract has the benefits of controlling participant's identity, operations or transactions, storage management, Quranic text hash management, as well as contracting, enforcement, and compliance of terms and conditions. The risk involved may be the use of the computer system to execute the contract. Therefore, if the source code can't comply with appropriate legal terms of the contract, an error will occur, although most of these problems can be handled using exception handling mechanisms. The functionality of the smart contract on a system as has been described in Figure 1.

*Distributed Consensus*-The verification and validation of a participant operation are being done by other available participants on the network. This is to avoid the unauthorized access to the network as well as check matting the compliance with rights and privileges given to the active participants. The distributed consensus will provide proof of existence and authorization to the operations intended to execute. The verification will be done by various nodes and immediately after the validation, the number of nodes verifies the authenticity of public-private key will be shown together with current operation and timestamp. The distributed consensus is automatically done at the point of opening the content of the Quranic text by comparing the Quranic text hash of the participant time-line with other available nodes on the network if the match will return valid and successfully open, otherwise, return invalid operation. All the participants have equal rights and privileges on the network in terms of verification and validation as well as operations. All the nodes on the network can serve as active validators once online; this is because each node possesses the same hash copy of the Quranic text. If the hash content of the intended participants does not match with the historical Quranic text hash of the network will be considered as invalid operation. The public-private keys remain valid if they are the same in all the available online nodes of the network and otherwise return invalid keys. The Quranic text hash will be published on the blockchain together with the corresponding encrypted public key of each network participant. The application of distributed consensus was described in Figure 1.

*Level 3 Quranic Text*-The blockchain has been designed to store information on a shared ledger of the network of participating nodes. Therefore, each active node on the system will be storing participants records on the shared ledger of it computing system and updating accordingly. The blockchain has best known as a decentralized system that store and share information. However, every information about participants and Quranic text will be stored on blockchain and can be accessed based on predefined terms.

*Quran Distributed Ledger*-The network system of the Quranic text protection, validation and distributed consensus are processed in a shared decentralized way. This means that each participating computer is acting as both client and server on the network. The record in each node remains the same and keep growing and updating based on the increment in the blockchain. A shared ledger is attached to each node to keep

a record of each participant's operations. The benefits behind this system are that, if an attacker successfully attacks a node, the peer-to-peer system will continue working and cannot affect other nodes, unlike server-based database management system. This shows that the system has deployed a guaranteed fault tolerance resistant, in such a way that, information is easily recovered for the affected node. Each peer can testify, verify and validate the operation of other peers from an irrefutable ledger record. Each participant can display or print up to date records of all the participants in the blockchain Quranic text. Each active participant must possess both public and private keys of the Quranic text blockchain. Basically, the content of the Quranic text is kept and replicated in hash format. Each participant on the network possesses the same hash Quranic text on the participating node which will be decrypted once certified by the distributed consensus. Each participant can replicate Quranic text hash and share with other willing participating parties. The Proposed Digital Trust for Quranic Text Conceptual Framework was developed in Figure 1.

## VII. Data Collection Procedure

Ethereum blockchain was used to explain the proposed framework data collection procedure. Ethereum blockchain was described as global transaction ledgers that operate remotely to validate distributed data using a Proof-of-Work (PoW) protocol. Ethereum application which is called wallet has a built-in virtual machine that helps to verify a search such as a Quranic ayah within a brief time using either a user or miner computer system. Ethereum system consists of swarm distributed database system, Whisper instant messaging, and Ethereum virtual machine.

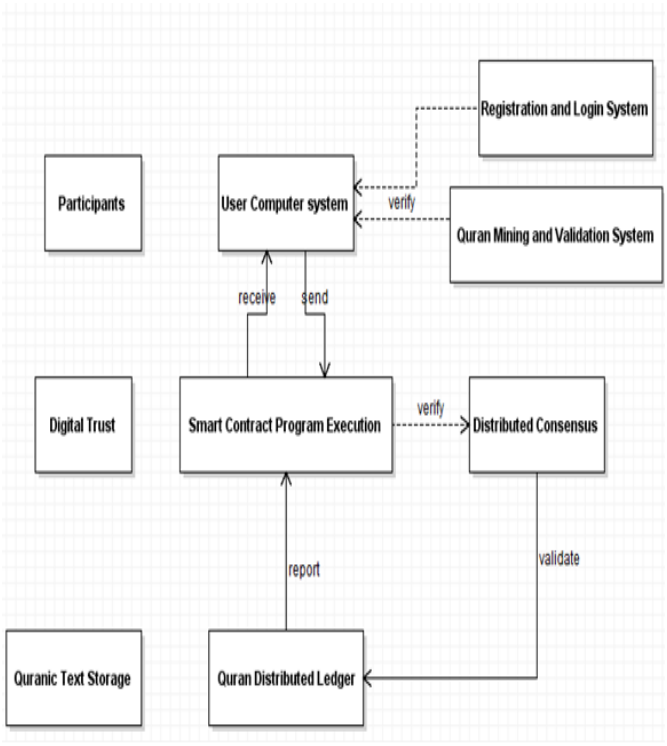


Figure 1: Proposed Digital Trust for Quranic Text Conceptual Framework

Proposed digital trust framework described the deployment of smart contract, distributed consensus and distributed database. These can be implemented using the following tools and platforms:

*Whisper*-This is a network protocol used for instant messaging. Whisper is used for implementing real-time distributed consensus by instantly receiving feedback from other computers on the network. Distributed consensus was implemented in various protocol, in this research we are using proof of work for both Quranic miners and Quranic users to reach consensus in Quranic ayah verification and validation.

*Swarm*-This is a distributed storage platform and content distribution service, a native base layer service of the ethereum web 3 stack. Swarm is used to store information in a distributed way in such a way that the copy of the information can never be deleted or change. The primary objective of Swarm is to provide a sufficiently decentralized and redundant store of Ethereum's public record, store and distribute decentralized application (dapp) code and data as well as blockchain data.

*Ethereum Virtual Machine (EVM)*-Ethereum is a decentralized virtual machine, which can execute programs, called contracts, written in a Turing-complete bytecode language. Every contract has permanent storage where to keep data, and a set of functions which can be invoked either by users or by other contracts. Ethereum is an open blockchain platform that allows developing and using any decentralized applications that runs on blockchain technology. Therefore, this shows that Ethereum is a programming based blockchain platform. However, Ethereum Virtual Machine allows other programming languages such as JavaScript, Java and Python to be executed.

*Mist Browser*-This is a browser that incorporates all parts of Ethereum and displays the decentralized applications. However, decentralized applications can be used in combination with normal browsers as well. A javascript library is available which is an interface to Ethereum and all the parts like Whisper and Swarm to be able to use the Dapps in other browsers.

*Computer System*-The use of computer system in the establishment of digital trust, digital Quranic text, and blockchain technology is necessary. In Theory, blockchain technology can be deployed on any digital computer system such as Desktop, Laptop, and Handheld devices. There is no restriction in the operating system, blockchain technology supported by all operating systems, such as Windows, Linux, and Unix. Despite that until now, Ethereum's Swarm is not fully supported by Windows.

*Internet*-This is a global communication network that allows almost all computers worldwide to connect and exchange information. The blockchain technology adopted the use of Internet to connect all computers together on its network to share resources and maintaining information.

## VIII. Data Analysis Techniques

The capability of the proposed digital trust framework of the Quranic text was demonstrated extensively in diagrams using StarUML and Violet UML editor. The functionality of some important user view or interface for the proposed digital trust framework was clearly illustrated using hypertext transfer markup language (HTML), cascading style sheet (CSS) language design.

## IX. Result and Analysis

The framework was designed and developed in such a way that digital trust, Quranic text and blockchain technology had been studied and applied in the architecture. The research framework considers the deployment of digital trust adopted by blockchain technology to describe security, privacy, trust and reliable usability of the system. In this research, blockchain techniques had been described with the effort to prevent and protect the digital Quranic text from been forged, misspelled, system failure, hacked or compromised by using cryptographic algorithms, distributed ledger, distributed consensus and smart contract in system development. The research adopts ethereum blockchain platform to validate the proposed digital trust framework, in a situation whereby a user is checking the authenticity of a Quran ayah as described in Figure 2.

*Registration and Login*-The research framework shows that all the network participants should be either registered miner or user as in Figure 1. Once registered the system will automatically send their public-private key which is called "Username and Password". The public key is used to identify the user node while the private key will be used by user to get access to the network as valid user. This is the same for all the network participants. The only difference is that miner participate in the Quranic ayah publishing. Therefore, Quran miner uses this opportunity to validate Quran Ayah whenever the need arises through a protocol called "Proof-of-Work" while the Quran user participates in the validation through a protocol called "Proof-of-Stake" as adopted by Ethereum Blockchain [51].

*Proposed Framework Validation*-The research second objective is to validate the proposed digital trust framework using Ethereum blockchain platform. However, the Figures 2 and 3 below, demonstrated the efficiency, effectiveness, usability and trust of the proposed framework in the checking of the validity of a Quranic ayah content by a Quran user as in Figure 2. In this research, our assumption is that a miner creates or publish Quran ayah by ayah and a user check the Quranic ayah validity ayah by ayah. Now, in the scenario given in this research for the proposed digital framework validation, we emphasize on that, a miner creates Quran based on certain criteria as in Table 3. This serves as the basis for smart contract on Quranic ayah creation. As in the scenario in Figure 2 where a miner uses original Quran and mine an ayah. Then broadcast the Quran ayah copy to the miners' network using Ethereum blockchain platform. All the miners' computers online reach agreement known as "Consensus" based on the agreed criteria as stated in the smart contract source code implementation. The newly created Quran ayah then broadcast to be added on the Ethereum swarm of the system called "Quran Distributed ledger" as in Figure 1 and Ethereum blockchain platform (that is Figure 2). The stored record is synchronized to update all the databases on the network including Quran users' databases.

The scenario of the transaction or operation is that a user wants to check the validity of an ayah of the Quran. Therefore, the ayah was uploaded to the system through the Quran decentralized application called "QURAN VALIDATION APPLICATION" installed on the Ethereum blockchain platform as in Figure 2. The ayah was encapsulated as a "block" and broadcast to the network using whisper instant messaging protocol. The Quran ayah content instantly received by all the participants nodes (both Quran users and Miners) for checking the authenticity of the ayah by comparing the ayah content with the Quranic ayah content in their various database called "Swarm" and return the validity of the Quran ayah content, using Ethereum virtual machine (EVM) which work on that, if and only if the Quran ayah content is the same in all the nodes or majority of the nodes, based on the available nodes online at the time of checking. However, the Quran ayah information automatically displays to the user as well as storing the result to various swarm on the network as shown in Figure 2 and 3. Otherwise, return the Quran ayah information as invalid or unconfirmed according to the smart contract implementation as in Figure 1.

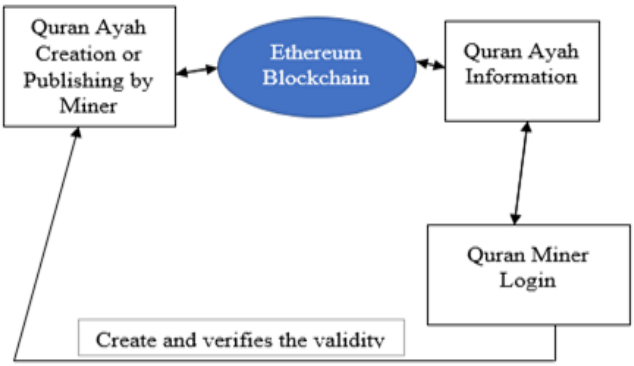


Figure 2: Quran Mining and Validation

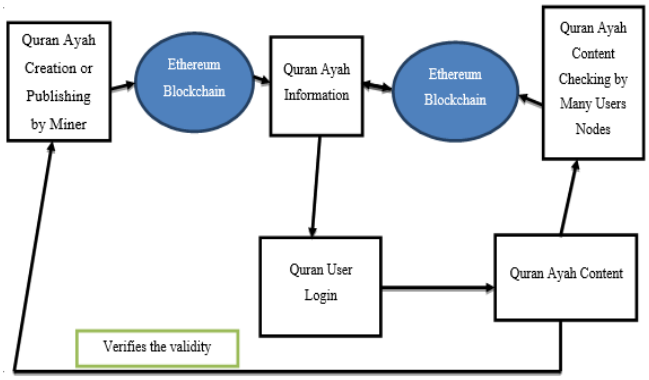


Figure 3: Proposed Digital Trust Framework Validation diagram

*Ethereum Blockchain Platform*-The research adopted ethereum blockchain platform as the validation platform as in Figure 2. The detail of the ethereum blockchain in Figure 4. The Ethereum block-chain platform consist of some series of integrated and dedicated software and hardware that make up of the platform and these are what make the Ethereum blockchain platform universal for any decentralized application as in [52]. Ethereum is an open source platform which enables the creation and distribution of decentralized applications. Therefore, in relation to Figure 2, the system has completed Quran distributed ledger resided in the swarm database, which was initially created by miners' network after reaching consensus based on the smart contract of their privileges to do so. The swarm database stored data and information in an encrypted format as in [53].

*Data Description, Specification and Analysis*-The proposed framework as in Figure 1 deploy the participant's registration criteria. The registration process requested for some information that can be used to the authenticated user and assign right and privileges in the participation and

accessibility to the network. However, we proposed some the record of some information as in Table 2.

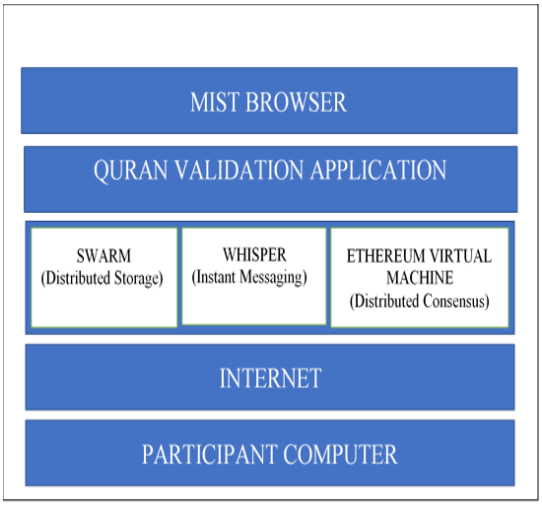


Figure 4: Ethereum Blockchain Platform

*Participant Data Description, Specification and Analysis*-The Ethereum blockchain like any other blockchain implementation, because block-chain is a peer-to-peer communication and has no trusted third party as mentioned in various literature. One of the criteria to achieve this is through generating participants information at the point of joining the network and storing in a cryptographic format as supported by Ethereum swarm as in Figure 4. Therefore, the user's privileges to participate in the use of the system depend on the registration. As described in the literature, that Ethereum blockchain is a public ledger blockchain. However, the operation and accessibility are corresponding to the registration to use the system. The participant can be either a miner (publisher and validator) or user (in our research a Quran ayah validator). In this research, we suggested that participants data or information should be or include the data in Table 2.

Table 2
Participants Registration Information

| Field | Data Value | Description | Size(Byte) |
|---|---|---|---|
| Username | Encrypted | Stand for Public Key | 32 |
| Password | 256-bit Hash | Stands for Private Key | 32 |
| Email Address | Encrypted | To verify Users | 32 |
| Mobile No | Encrypted | To verify Users | 32 |

*Quran Data Description, Specification and Analysis*-The research use Ethereum blockchain platform to describe the Quranic text information as in Figure 1 and Ethereum swarm in Figure 4. These extensively use to emphasizes on the effective and efficient study of the Quranic data and information as well as the Ethereum blockchain platform capability. The Ethereum swarm records are crypto-graphically by default. In hashing, strings of characters are transformed into a specific key representing the original string. To check the integrity of that same string, the hash value is calculated and compared. If the hash values are the same for both the documents, the data are correct and accurate. In case the hash values do not meet the signified string, they have been modified and are not authentic [35]. The proposed framework has adapted Ethereum blockchain implementation for applying to protect Quranic text and help users to check for the validity of their Quranic text or ayah. The research focuses on providing protection to the integrity of the Quranic text as in Table 3.

Table 3
Quranic Text Information

| Field | Fixed Hash Value | Description | Size (Bytes) |
|---|---|---|---|
| hashPrev Block | 256-bit hash of previous ayah block | This is used for easy verification to validate the ayah requested for validation | 32 |
| hashCurre ntBlock | 256-bit hash of the current block | New and present ayah to be hash by miner or check by both user and miner | 32 |
| hashSurah Block | 256-bit hash of the chapter header | Surah header, content name of the surah | 32 |
| hashBasm alaBlock | 256-bit 256 hash of the Basmala block | Basmala as it's at the beginning of each surah. Basmala at the beginning of Surah Fatiha counted as ayah while surah taubah do not start with Basmala | 32 |
| SurahNu m | 32-bit surah number from the beginning of Quran (start at 1) | Number of surah from the beginning of the Quran | 4 |
| surahAya hNum | 32-bit number of ayah in each chapter | Number of ayah content in each surah. They are varying. | 4 |
| ayahNum | 32-bit number of ayah starting from the beginning of surah (start at 1) | Ayah counter for each surah | 4 |
| quranAya hNum | 32-bit number of ayah from the beginning of the Quran | Ayah counter for all the Quran, starting from first ayah (that is 1 to 6236) | 4 |

## X. DISCUSSION

Building a conceptual framework by linking the relationship of each component to one another is highly important. The digital trust had been built in various structures specifically centralized client-server system. According to the literature, there is no digital trust framework that was built using blockchain technology. The research covered all the important aspect of building research frameworks, digital trust, and Quranic text, and Blockchain techniques based on the time constraint of the research. Blockchain technology was built to serve users in a secure distributed or decentralized system, where each user own control over data and information on the network. Therefore, the proposed digital trust was designed to comply with the blockchain operation procedures. The problems related to missing of some Quranic verses in some Quranic web application make it necessary for the Muslims ummah to look for the mechanisms that can be used to secure the digital content of the Quran. The trust mechanisms should be deployed on the Quranic text to provide belief, confidence and reliability for the digital Quranic text applications. The application of Blockchain digital trust happens to be a satisfactory solution for these issues. The blockchain keep copies in duplicate through its network and no alteration will be granted access, instead will be considered invalid or unconfirmed accessibility [38]. Blockchain has experienced several attacks since its inception, but no record for compromise or hacked for the network had been recorded. So far, there is no any significant problem found with the blockchain. Blockchain technology

can be applied to legal services, government administration, software applications, health services, copyrights, and any other communication services. Blockchain technology is excelling beyond imaginations and there are uncountable opportunities in this disruptive technology [7]

The related literature based on the research topic was reviewed and for each definition, benefits and applications were described. The formation of the literature review was based on research framework, digital trust, Quranic text, and blockchain techniques respectively.

## XI. CONCLUSION

The objectives of the research have been achieved. We use blockchain technology to develop our proposed digital trust framework as in Figure 1. We use Ethereum block-chain platform to validate our proposed digital trust framework as in Figure 2, 3 and 4. The UML diagrams in Figures 5,6,7,8 and 9 and web interface in Figure 10,11,12 and 13 were used to analyse the validity of the operations in Figure 2, and 3. The Table 2 and Table 3 were used to describe the nature of participants and Quranic information according to blockchain technology as in Figure 1 and Ethereum swarm as in Figure 4.

Throughout this research, we adhere to our objectives, related literature, data collection and analysis techniques for our finding and conclusion. The results of our findings show that the proposed digital trust framework is effective and efficient to be used when applied to the Ethereum blockchain platform. Secondly, the Quranic text information is secured and protected. Thirdly, the validation process of Ethereum blockchain platform is transparent and unique to all parties on the networks.

## XII. IMPLICATION AND RECOMMENDATION

This research had been the first of its kind in both digital trust and blockchain technology, where no research had been conducted for developing digital trust framework using blockchain technology and there is no research that uses blockchain in the Quranic text. The research has several benefits. The benefits of the research can be categorized into three; the first benefit is that a digital trust framework was build which can be adopted by in any digital communication. Secondly, the research was an effort to provide secured system for Quranic applications. Thirdly, the important aspect of block-chain technology and digital trust was discovered. Finally, the ethereum blockchain platform had been identified. However, the future research should be focusing on the application implementation and related applications such as Islamic texts, Certificates ownership, Identity Management, Copyrights, Assets Management, Government services, Public and Private Sector Management.

## REFERENCES


[1] A. A. Aliyu and A. A. Abdu, "Research Framework Development on the Effect of Intangible Location Attributes on the Values of Residential Properties in Jos, Nigeria," *Dev. Ctry. Stud. www.iiste.org Res.*, vol. 5, no. 16, pp. 8–31, 2015.

[2] M. G. M. Mostafa and I. M. Ibrahim, "Securing the Digital Script of the Holy Quran on the Internet," *in 2013 Taibah Univ. Int. Conf. Adv. Inf. Technol. Holy Quran Its Sci.*, 2013, pp. 57–60.

[3] M. S. Khalil, F. Kurniawan, M. K. Khan, and Y. M. Alginahi, "Two-layer fragile watermarking method secured with chaotic map for authentication of digital holy Quran," *Sci. World J.*, vol. 2014, 2014.

[4] A. Alqurneh, A. Mustapha, M. A. A. Murad, and N. M. Sharef, "Stylometric model for detecting oath expressions: A case study for Quranic texts," *Lit. Linguist Computing 2016*; vol. 31, pp. 1-20, 2014.

[5] A. M. Iqbal, Rizwan, "An experience of developing Quran ontology with contextual information support," *Multicult. Educ. Technol. J.*, vol. 7.4, pp. 333–343, 2013.

[6] N. Nawaz and S. F. Jahangir, "Effects of memorizing Quran by heart (Hifz) on later academic achievement," *J. Islam. Stud.*, vol. 3, no. 1, pp. 58–64, 2015.

[7] M. Swan. *Blockchain: Blueprint for a New Economy, February 2*. The United States of America: O'Reilly Media, 2015.

[8] L. Howard, "Whitepaper on Distributed Ledger Technology" [Online]. Available: http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf

[9] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts, (SoK)" in *Proc. International Conference on Principles of Security and Trust*. Springer, Berlin, Heidelberg, 2017, pp. 1–22.

[10] R. E. Samuel, "A Layered Architectural Approach To Understanding Distributed Cryptographic Ledgers," *Issues Inf. Syst.*, vol. 17, no. IV, pp. 222–226, 2016.

[11] C. Grant and A. Osanloo, "Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for Your 'House,'" *Adm. Issues J. Educ. Pract. Res.*, pp. 12–26, 2014.

[12] C. D. Schultz, "A trust framework model for situational contexts," in *Proc. 2006 Int. Conf. Privacy, Secur. Trust Bridg. Gap Between PST Technol. Bus. Serv. - PST '06*, 2006, p. 1.

[13] F. Moyano, C. Fernandez-Gago, and J. Lopez, "A conceptual framework for trust models," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7449 LNCS, no. 256980, pp. 93–104, 2012.

[14] T. Judgi and P. Varalakshmi, "A Survey on Trust Management in Cloud Computing," *Adv. Nat. Appl. Sci.*, vol. 20, pp. 416–420, 2015.

[15] G. F. Marias, K. Papapanagiotou, V. Tsetsos, O. Sekkas, and P. Georgiadis, "Integrating a trust framework with a distributed certificate validation scheme for MANETs," *Eurasip J. Wirel. Commun. Netw.*, vol. 2006, pp. 1–18, 2006.

[16] K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–317, 2006.

[17] R. Dennis and G. Owenson, "Rep on the Roll: A Peer to Peer Reputation System Based on a Rolling Blockchain," *International Journal of Digital Society (IJDS)*, vol. 7, no. 1, pp. 1123–1134, March 2016.

[18] J. A. Seppälä, "The role of trust in understanding the effects of blockchain on business models" [Online]. Available: https://aaltodoc.aalto.fi/bitstream/handle/123456789/23302/master_Sepp%C3%A4l%C3%A4_Jane_2016.pdf?sequence=1&isAllowed=y

[19] Y. L. Sun, Z. Han, W. Yu, and K. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in *Proc. IEEE INFOCOM 2006. 25TH IEEE Int. Conf. Comput. Commun.*, vol. 6, no. c, pp. 1–13, 2006.

[20] Z. Y. and S. Holtmanns. *Trust Modeling and Management: from Social Trust to Digital Trust*. IGI Global, 2008, pp. 290-323.

[21] W. Sherchan and C. Paris, "A Survey of Trust in Social Networks," *ACM Computing Surveys (CSUR)*, vol. 45, no. 4, pp. 1–33, 2013.

[22] W. K. Wong, S. O. Cheung, T. W. Yiu, and H. Y. Pang, "A framework for trust in construction contracting," *Int. J. Proj. Manag.*, vol. 26, no. 8, pp. 821–829, 2008.

[23] H. Li and M. Singhal, "Trust management in distributed systems," Computer vol. 40, pp. 45–53, 2007.

[24] T. W. Um, G. M. Lee, and J. K. Choi, "Strengthening trust in the future ICT infrastructure," *in Proceedings of the 2015 ITU Kaleidoscope: Trust in the Information Society, K-2015 - Academic Conference.* 2016.

[25] A. H. Networks, J. Cho, A. Swami, and I. Chen, "A Survey on Trust Management for Mobile Ad hoc Network," *IEEE Communications Surveys & Tutorials*, vol. 13, pp. 562-583, 2011.

[26] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Communications Surveys & Tutorials*, vol, 18, pp. 2084-2123, 2015.

[27] D. Quercia, S. Hailes, and L. Capra, "B-trust: Bayesian trust framework for pervasive computing," in *International Conference on Trust Management. Springer Berlin Heidelberg*, vol. 3986 LNCS, no. vii, pp. 298–312, 2006.

[28] E. Wustrow and B. VanderSloot, "DDoSCoin: Cryptocurrency with a Malicious Proof-of-Work," *in Proceedings of the 10th USENIX*

*Conference on Offensive Technologies. USENIX Association, (WOOT 16)*, 2016.

[29] L. Kagal, S. Cost, T. Finin, Y. Peng, and C. Science, "A framework for distributed trust management," *in Proc. IJCAI-01 Work*, 2001.

[30] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, 2012.

[31] A., Neuwirth, N. Sinai, and M. Marx (eds). *The Qurʾān in context: historical and literary investigations into the Qurʾānic milieu*. Brill, 2009.

[32] S. Ghafouri-Fard and S. M. Akrami, "Man evolution an Islamic point of view," *Eur. J. Sci. Theol.*, vol. 7, no. 3, pp. 17–28, 2011.

[33] A. M. Sharaf, "The Qur'an Annotation for Text Mining," [Online]. Available: http://textminingthequran.com/papers/firstyear.pdf

[34] I. C. Gaps,"The State of Cybersecurity and Digital Trust 2016 to Rethink State of the Art" [Online]. Available: https://www.accenture.com/t20160704T014005__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf

[35] S. Hakak, A. Kamsin, M. Y. Idna Idris, A. Gani, T. Herawan, and S. Zerdoumi, "Preserving Content Integrity of Digital Holy Quran: Survey and Open Challenges," *IEEE Access*, vol. 3536, p. 1, 2017.

[36] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" [Online]. Available: https://bitcoin.org/bitcoin.pdf

[37] METI, "Survey on Blockchain Technologies and Related Services FY2015 Report" [Online]. Available: www.meti.go.jp/english/press/2016/pdf/0531_01e.pdf

[38] R. Beck, J. Stenum Czepluch, N. Lollike, and S. Malone, "Blockchain - The Gateway to trust-free cryptographic Transactions," *in Twenty-Fourth European Conference on Information Systems (ECIS), 2016*, pp. 1–14.

[39] J. Condos, W. Sorrell and S. Donegan, "Blockchain Technology: Opportunities and Risks" [Online]. Available: http://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf

[40] U. K. Government and C. Scientific (2016), "Distributed Ledger Technology: beyond block chain," [Online]. Available: https://www.gov.uk/government/distributed-ledger-technology-beyond-block-chain

[41] J. Mattila, "The Blockchain Phenomenon the Disruptive Potential of Distributed Consensus Architectures," *The Research Institute of the Finnish Economy*, vol. 2420, no. 38, 2016.

[42] C. A. Vyas and M. Lunagaria, "Security Concerns and Issues for Bitcoin," *Int. J. Comput. Appl.*, pp. 10–12, 2014.

[43] P. Barton, "Bitcoin and the Politics of Distributed Trust (Senior Thesis)" [Online]. Available: https://scholarship.tricolib.brynmawr.edu/handle/10066/16548

[44] N. Zhumabekuly Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams," *IEEE Trans. Dependable Secur. Comput.*, vol. 5971, no. c, p. 1, 2016.

[45] I. Lin and T. Liao, "A Survey of Blockchain Security Issues and Challenges," *IJ Network Security*, vol. 19, no. 5, pp. 653–659, 2017.

[46] A. Beikverdi and J. Song, "Trend of centralization in Bitcoin's distributed network," *in Proc 2015 IEEE/ACIS 16th Int. Conf. Softw. Eng. Artif. Intell. Netw. Parallel/Distributed Comput. SNPD 2015*, vol. 16, pp. 1–6., 2015.

[47] M. O. Dair, D. Neilson, and P. Pacifico (2016), "Music on The Blockchain Lead Researcher" [Online]. Available: https://www.mdx.ac.uk/__data/assets/pdf_file/0026/Music-On-The-Blockchain.pdf

[48] P. De Filippi, "The interplay between decentralization and privacy: the case of blockchain technologies" [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852689

[49] P. De Filippi, "The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure," *Internet Policy Rev.*, vol. 5, no. 3, pp. 1–28, 2016.

[50] A. Baliga, "The Blockchain Landscape" [Online]. Available: https://www.persistent.com/wp-content/uploads/2016/03/The-Blockchain-Landscape-.pdf

[51] M. Mwale, "Modelling the Dynamics of the Bitcoin Blockchain" [Online]. Available: http://scholar.sun.ac.za/bitstream/handle/10019.1/98844/mwale_modelling_2016.pdf?sequence=2.

[52] J. Dienelt , "'Understanding Ethereum.' New York, NY: CoinDesk." [Online]. Available: https://forum.daohub.org/uploads/default/original/2X/b/b583e2bb2e6998bfec40d488b1709deb53abdc4a.pdf

[53] Ethereum, "Solidity Documentation" [Online]. Available: https://media.readthedocs.org/pdf/solidity/develop/solidity.pdf