Acta Scientific COMPUTER SCIENCES

Volume 3 Issue 8 August 2021

Review Article

Smart Contract Using Blockchain Technology: An Experimental Study

Funmilayo Celestina Ayeni, Kofi Sarpong Adu-Manu* and Charles Adjetey

Computer Science Department, Valley View University, Ghana

***Corresponding Author:** Kofi Sarpong Adu-Manu, Computer Science Department, Valley View University, Ghana.

Received: June 14, 2021

Published: July 13, 2021

Abstract

Blockchain technology has seen a massive amount of growth over the years, starting in 2009. The goal of the creation of blockchain technology was to reduce the power of third parties during transactions. However, blockchain technology gained much attention in the use of cryptocurrencies, especially bitcoin. Bitcoin is executed by changing physical cash to electronic cash at stated rates. Digital signatures identify individuals on the platform. The new proposed algorithm is implemented under Python using the SAGEMath library and evaluated. In our approach, only parties involved have copies of transactions that take place between them; however, in doing that, security becomes the most significant problem. This leads to introducing a novel algorithm that uses mathematical modelling to solve problems in other application areas for blockchain. We increased the number of nodes between 10 and 60 and observed that the proposed algorithm's running time remained at 9 seconds for 20 nodes, similar to PoW and PoS, whose running time was around 9 to 10 seconds. However, when the increased the number of nodes was increased to 60 with the exact transaction details, we observed that the running time of the proposed algorithm remained the same as 10 nodes [4 - 9 seconds], and the running-time for PoS and PoW algorithms increased to 42 and 30 seconds, respectively.

Keywords: Smart Contract; Blockchain; Bitcoin; Blockchain Technology

Abbreviations

PoW: Proof-of-Work; PoS: Proof-of-Stake; AI: Artificial Intelligence; IoT: Internet of Things; btc: Bitcoin; p2p: Peer-to-Peer; FCFS: First-Come-First-Serve; ERS: Exchange Rate Services; BT: Blockchain Technology

Introduction

Blockchain technology is gaining more prominence in the financial and healthcare sectors, government agencies, utility companies, and implemented in Internet of things applications. Blockchain is viewed as an open, distributed ledger that is capable of recording transactions that takes place between two parties efficiently and in a permanent and verifiable way. Blockchain is a trustless network because parties can transact even though they may not trust each other [1,2]. The introduction of blockchain technology in the various industries have opened up the field to fully implement smart contracts. Other transactions such as digital assets, remittance, online payment, public services, reputation systems, and security services can take place on the blockchain platform.

Smart contracts are deployed using the blockchain platform in two ways; the actual development and the deployment of the contract terms. Although a number of works have been proposed in literature on smart contracts, the actual development of the contract

is seen mainly in Ethereum which has received little or no attention in academia and industry at large [3,4].

In the traditional blockchain, the network is formed when: 1) transactions are broadcast to all nodes after they have been newly created; 2) each node in the block collects the new transactions; 3) each node provides a difficult Proof-of-Work (PoW) for its block; 4) when the PoW is found and broadcast to all nodes; 5) the block is accepted if the transactions on it are valid; and 6) the nodes present on the network expresses their acceptance by adding the block to the chain on the network and finally uses its hash as the previous hash for the new block [5]. In the proposed blockchain architecture, the network does not opt for the PoW as a solution from a user. Also, all the members on the network do not need to accept the block, the platform will provide the PoW, and only the nodes involved in the transactions will accept it for their operation.

The introduction of blockchain technology removed totally, third parties in transactions. This technology makes users trust in computations rather than third party organizations. Trust in computation on blockchain platform is made possible by the PoW and the Proof-of-Stake (PoS) algorithms [6]. The blockchain technology applied in Artificial Intelligence (AI), Internet of Things (IoT), Medicine has led to the rising of new problems in IoT and AI devices that cannot provide the computational power required to support the PoW and PoS [7].

One key implementation of blockchain is the bitcoin. The bitcoin enables the creation of a peer-to-peer (p2p) version of an electronic cash which allows online payments to be sent directly between two parties without the use of a financial institution [2]. Bitcoin is executed by changing physical cash to electronic cash at stated rates. Digital signatures identify individuals on the platform. Users sign-in on the platform with a public key and a private key. Hash code is used to identify transactions as each block has a unique hash that consists of the hash code of the previous block and the transaction number. This information is added to the chain as more transactions are performed.

In reaching agreements between parties, the information shared during the contract negotiation process has to be confidential. The current blockchain technology does not provide the needed confidentiality because it is a public ledger. The agreement is successfully reached between parties without breaching the laws of financial bodies. Another key challenge in blockchain technology relates to its performance. Blockchain has limited scalability, throughput bottlenecks, latency in transactions, and storage constraints. These challenges greatly impacts the performance of smart contracts. Also, the process of solving a cryptographic puzzle require the computing power of miners. Miners get reward for contributing their computing power for finding a new block. It is a challenge for an individual miner to find a block, hence miners usually join more mining pools to contribute their computing power [8].

In this paper, we took into consideration these problems in the existing blockchain technology by providing a blockchain system that implements a private ledger and does not rely on miners to solve puzzles or computations. In our approach, computations are performed in the blockchain system thereby, passing the needed memory requirement and computational power to manufacturers. This provides trust and solves the issue of high computational power and memory requirements to enable the use of blockchain on IoT/AI devices.

Related works

Blockchain Technology (BT) has seen innovations that have shaken the digital world. BT may be applied in enabling value chains, building closer customer relationships, fostering faster product innovations, and initiating quicker innovations with IoT. BT has gained wide attention from both industry players and academicians. BT is a distributed ledger technology commonly known for its application in cryptocurrencies. Blockchain is defined as a network of computers that most users unanimously accept the transaction before it can be added to a block [9]. Even though the blockchain was first applied in financial operations, its application areas range wide, and potential for research growth is very high. In the digital era, data has an equivalent value to money; the blockchain technology has a future in keeping various forms of data and preventing cyber-attacks [10].

The blockchain is a sequence of blocks that stores transactions in the form of a ledger and a linked list since every block contains information that points to the next block [4].

The implementation of blockchain to implement bitcoin (i.e., cryptocurrency) has recorded over 69.5 million transactions since

its inception in 2009 till 2015 [11]. Bitcoin (btc) is an online communication protocol that facilitates the use of virtual currency and electronic payments [12]. On the bitcoin platform, any user can become a miner (that is a transaction verifier). Miners solve mathematical computation attached to a transaction to prove the legitimacy of the transaction before the transaction goes through. The platform makes the computations (puzzle) tougher so that the time taken to add a new block of transaction is exactly 10 minutes [5]. Miners receive 5btc every time they solve a puzzle correctly. Miners post a block that contains PoW to ensure that no illegal transaction is added to the block. In effect, miners vote on the correct transaction, and no transaction is, in turn, complete until it has been added to the chain of blocks [13].

The process provides greater assurance of legitimacy of transactions, but it is also time-consuming considering the time it takes to validate one bitcoin transaction. There are identifiable challenges that come with the implementation and use of Bitcoin. The implementation challenges are: 1) the platform does not provide proof for first-come-first-serve (FCFS) services. For example, if two users request for 50btc from a user having 50btc the first transaction to be validated goes through, that is, the user with the good connectivity and the simplest puzzle attached to their transaction gets the 50btc; 2) the blocks are linked together in the form of a chain making it easier to validate if the user has the needed amount of Bitcoin (btc) required by the other user; 3) the platform does not require additional information from the user when signing up on the platform, therefore, allowing for anonymity [4].

The use of miners poses several challenges in solving puzzles provided by the blockchain platform, miners apart from receiving 50btc for solving the puzzles also receive extra income when buyers or sellers involved in a bitcoin transaction decide to pay a transaction fee. As at March of 2014, 97% of transactions included a transaction fee causing a reduction in the amount miners receive to 25btc. Mining causes addition computational costs. As at 2015, more than 173 megawatts of electricity had been consumed to solve and upload the PoW block on the blockchain platform. Recently, effective mining requires high computing capabilities and access to low-cost electricity. Bitcoin does not provide a way to reverse transactions or cancel unwanted transactions, once a transaction has been validated necessary changes are made to the users' wallet. Another challenge relates to the exchange rate services (ERS). ERSs of blockchain platform do not go through a central body due to the decentralized nature of the technology. This causes breaking of laws of ERSs. The exchange rate prices provided by the bitcoin are computed in real-time by referencing an amount of conventional currency, therefore, making the bitcoin of today resemble a payment system.

Blockchain application areas, models and mining methods

Application areas

Blockchain technology has been applied in so many areas apart from finance. Some of which are.

Artificial intelligence (AI)

Artificial intelligence (AI) and blockchain technologies are gaining traction at an incredible rate. Both technologies are technologically complicated and have multidimensional business ramifications. However, a prevalent misconception regarding the blockchain concept in general is that it is decentralized and not controlled by anyone. The creation of a blockchain system, however, is still assigned to a group of core developers. As an example, a smart contract is a collection of codes (or functions) and data (or states) that are developed and published on a blockchain (say, Ethereum) by various human programmers [14].

Swan advocated using blockchain technology to construct thinking agents, or the brain as a decentralized autonomous company, in the areas of biological science and artificial intelligence in 2015 [15]. Blockchain thinking will be an input-processing-output computational system that will allow for the spread of ideas and potentials through self-mining blockchain models. Data from outside the system, such as sensory data, and data from within the system, such as a memory, will be inputs to the blockchain system. The inputs will be brought into a specific location for processing, and the outputs could include taking action, conducting a transaction, or making a note for a future action. We might also have personal thinking chains, which contain all of a person's thoughts and are gathered utilizing brain-computer inferences, cognitive nanorobots, and other data collection techniques. All of a human's subjective thinking and possibly consciousness might be stored via this method of instantiating and storing, allowing for a more exact definition of consciousness [16,17]. Blockchain could be used to manage electronic medical records. The concept is to use blockchain to store connectomes, which will allow individuals to experience

what it's like to be us at a moment by sharing our thoughts, affect, and valence. It has a memory, storage, and file-serving architecture.

Internet of things (IoT)

Blockchain was introduced as the next security booster. IoT makes use of the current client-server approach which causes implementation issues during synchronization of these devices [5]. Using blockchain on IoT devices makes synchronization easy because it is a distributed system. According to the author, the main drawback to IoT is their dependence on the cloud, and he stated an example of a denial-of-service attack launched on Dyn a US-based DNS provider and most of the Ip address traced back to IoT devices, this was because the devices had been infected with a virus called Mirai [18]. This virus takes control of Internet devices and utilizes them to execute DDoS attacks. Phishing emails were used to infect a computer or home network as part of the infection process. After that, the infection spreads to other computers and devices. The decentralized blockchain approach helps solve the problems caused due to reliance on a centralized cloud account. The anonymity that blockchain supports is good in the implementation of IoT devices because user information needs to be kept private even in the sharing of information.

IBM's use of blockchain to track high-value commodities as they move throughout supply chains is an example of blockchain's integration with IoT devices. This service is provided via their large cloud infrastructure. The data from connected devices are translated into transactions that the blockchain needs. The platform also filters events and guarantees that only the information needed to fulfill contract terms is sent, which is commonly done using an Ethereum smart contract. As long as the data entered is correct, the platform is reliable and the transaction has not been tampered with [19]. Wireless sensors and IoTs have improved technologically, making it easier to connect multiple devices and transport data even from remote locations. Table 1 presents the major differences between cloud-based and blockchain-based architecture for IoT.

Challenges	Cloud-based	Blockchain-based
Cost and capacity constraints	The rapid expansion of IoT devices has resulted in a significant degree of demand from cloud service providers.	Devices can communicate without the assistance of a central server. The platform allows devices to interact, share data, and perform activities.
The architecture	In traditional IoT architecture, each node operates as a single point of failure, causing the entire network to go down. It's subject to DDOS attacks and hacking.	Each transaction is digitally signed with the sender's private key and can only be opened with the user's private key in the blockchain architecture, ensuring that only the sender could have sent it.
Susceptibility to manipulation	There's a good chance that the data was tampered with.	Blockchain is a decentralized system in which adding a new block to the chain requires proof of work, making data manipulation extremely difficult.

Table 1: Differences between cloud-based versus blockchain-based architectures.

Health care

In the health sector a lot of academic scholars have come up with the different areas which the blockchain can help improve health services to humanity such as public health care, medical research, consumer-oriented health care, pharmaceutical sector [20-23]. In the pharmaceutical industry the blockchain can be used in solving the issues of counterfeit drugs entering the supply chain. Most pharmaceutical companies are implementing the blockchain as one of the methods to provide transparency through the supply chain; blockchain can improve transparency in the supply-chain in two ways: 1) by harnessing Internet of Things (IoT) using smart contracts to strengthen security, and 2) by tackling the problem of counterfeit drugs capable of entering the supply chain and reaching patients. In [24], the authors proposed blockchain for keeping health records of patients but in their approached there was the lack of a model on which medical cases can be built. In table 2, some key advantages and disadvantages of using blockchain in healthcare are presented.

The smart contract's terms of the contract will be compliant with rules in order to ensure proper distribution. Sensors are uti-

Advantages	Disadvantages
There is a high level of security since the more nodes in the system are added, the lower the danger of failure.	The deployment of blockchain technology is not well understood by medical professionals.
Because the blockchain is decentralized, it avoids single point failures that can occur in cloud-based or server-based systems.	There are presently no sources for authentication and authentication of data sources.
Because any action may be monetized, hospitals can build brand value without handing away equity.	Because there is no government authority to identify blockchain as a technology, there are no restrictions in place.
The use of blockchain to store health records and data can help to standardize the process.	A blockchain model on which medical practices can be created is currently unavailable.

Table 2: Advantages and disadvantages of using blockchain in medicine.

lized to monitor each drug throughout shipment, and the data is relayed to the platform, where the smart contract assures that the medicine's conditions are consistent with set standards. The system's main feature is that it allows users to track when a product is deficient as well as the consumer who was using it at the time the deficiency was discovered. The distributed platform provided by blockchain allows multiple health practitioners to share information about patients when offering public health services. For example, if a patient had to move out of town and became ill, the doctor would not have had access to the patient's medical records and would have treated the patient based on recent symptoms. Now, thanks to this system, the doctor can access the patient's medical record and treat the patient based on medical records. The application of blockchain in healthcare services is difficult due to a lack of data privacy and effective security. Because doctors are compelled by law to keep their patients' information private, a blockchain that serves as an access control manager for health data is needed.

Blockchain and library management

Information retrieval is considerably easier and faster than it has ever been in our modern digitalized society. Despite the fact that information may be obtained from a variety of sources, it is still necessary to provide a dependable source of knowledge, which libraries give. Libraries have been hesitant to incorporate emerging technologies into their services. When borrowing a book, for example, the method remains unchanged from decades ago: all borrowed books must be returned to the library before being borrowed again. Furthermore, there is sometimes a lack of cooperation between libraries, resulting in consumers registering many times to borrow books from different libraries. A technology that makes such procedures easier and faster can benefit both patrons and libraries. To that end, blockchain technology provides a transparent resource management system that libraries can use to deliver such systems in a safe and convenient manner. For two parties to have a trustworthy transaction, the blockchain eliminates the requirement for a central authority [25].

The use of blockchain in libraries was proposed to keep library records. However, its implications are: 1) allowing for the publishing of authentic journal articles and, 2) digital rights management, allowing readers to access the right articles and writers to earn properly [26]. The authors of [27] suggest a blockchain-based smart library management system. The solution eliminates the risk of data tampering by utilizing blockchain technology's unique workload proof methodology and consensus mechanism, as well as solving the central system's inefficiency and security issues through distributed accounting. The answer to complete proof auditing and stocktaking in today's modern libraries is blockchain-based library management systems, which are transparent and immutable records. The usage of copyright digital content is limited by the blockchain library management system [28,29].

Programming languages

As a primary way of providing accounting of the ?code is law' that specifies agreements between parties, blockchain programming allows stakeholders to still trust the platform to execute the agreed-upon contract (known as smart contract) as planned. In principle, it appears simple, but in practice, it is rarely the case.

Blockchain has been used to create programming languages such as hypertext and Ethereum that allows people to run and build programs that enables them to update the shared state), but programs written on this platform were bug prone and these bugs could not be fixed because programs are irreversible. This programming is known as solidity. Obsidian was introduced as a new programming language for blockchain that provides fixes to

the security bugs issues of solidity. Obsidian is an object-oriented programming language that uses the state first-class, which means that the methods that can be invoked on an object are determined by the object's current state. The blockchain has seen significant advancements and a wide range of applications [30].

Scilla is a mid-level programming language that may be used as a compilation target as well as a standalone programming framework. Scilla provides high safety guarantees through type soundness, using System F as a foundational calculus. It creates a clear distinction between the pure computing, state-manipulating, and communication portions of smart contracts, avoiding many of the known difficulties associated with byzantine execution. Scilla is an explicitly typed functional programming language that encodes common operations for blockchain applications through higher-order functions, an imperative fragment, and explicit effects [31].

The Linux Foundation and IBM created and support Hyperledger Fabric, one of the most popular opensource blockchain permissioned platforms that has already been used in many industrial scenarios. One of the platform's distinguishing features is that it offers a smart contract system that is based on general-purpose languages rather than ad hoc ones. The Hyperledger Fabric network is made up of peers that can play three different roles. Endorser responsible for receiving and executing transactions (transaction proposals) from client applications. The peer in charge of creating transaction blocks is known as the Orderer. Committer that validates all transactions contained in the received block and applies the block to the ledger [32].

Models

Models have been proposed for the different application areas for blockchain [7]. The most recently used models proposed in literature for blockchain technology are provided in this section. The models include - the Bitcoin Model (A block is a set of transactions. the parent block or genesis block is a block from which other block inherits, it is the starting block in a chain of blocks. It does not have any preceding block. A block contains a block header and the block body):

- **Previous hash**: Is a 256-bit value that points to the previous block in the chain.
- **Nonce:** Is a 4-byte field that increases for every hash calculation.
- **Timestamp: It** uses current time of current transaction as seconds.
- **Merkle tree root:** Contains the hash value of all transactions in a block. The transaction and receipt root are all stored in the Merkle root.
- **nBits:** The current hashing target in compact form.

The blockchain uses digital signatures to determine if a transaction is coming from an expected user or otherwise. When Alice sends a request to Bob for bitcoin, she signs the transaction request using her private key, when the message gets to Bob, Bob uses the available public key for Alice to decrypt the message and sends back the bitcoin to Alice if the bitcoin requested is not greater than the amount of bitcoin Bob has in his wallet [6,18]. The Blockchain-IoT Model has helped visualize the synchronization of various IoT devices for better sharing of data across these devices. However, the IoT models vary for different manufacturers, that is there is no shared platform for IoT devices independent of their manufacturers [15]. The Blockchain-Hypertext Model (i.e., the Hyperledger blockchain) model was built to support the blockchain programming language solidity, it uses the HTML and runs on Ethereum's virtual machine [16]. The Blockchain-Obsidian Model unlike the hypertext which is just applied directly on Ethereum's virtual machine, Obsidian is an object-oriented programming language developed for blockchain it is used like the hypertext language in blockchain [16]. The Blockchain-Health Model so far all the models proposed under for use in health studies are just concepts on what the blockchain can do in the field of health. In the field of pharmacy, the blockchain is said to be used in the supply chain to help reduce selling of counterfeit drugs [33]. Finally, the Blockchain-AI Model is closely related to the field of IoT and both employ the use of sensors [15].

Computational algorithms

Proof-of-work (PoW)

The PoW is a computational algorithm in which nodes compete based on their computational power. The PoW algorithm operates by scanning through a system for a value that when hashed starts with zero bits. The addition of nonce as shown in figure 1 is added to the original value to accomplish the requisite number of zero bits. In PoW, the block cannot be altered when a nonce is found and the PoW has been satisfied by the miners. In a typical blockchain network that applies the PoW, the computations to be solved are

thrown to miners to solve and the solutions to the computations are uploaded to the network, the transaction is only confirmed (that is the block is added to chain) if and only if solutions generated are correct. The PoW algorithm uses an interactional hash back method as proposed by Adam Back. It is interactional in the sense that puzzles are thrown to nodes called miners to solve. The computational cost is borne by the miners. Difficulty of the computational puzzle thrown to miners is increased so as to ensure that the computational results of a block is different for a particular block [34-36]. Since pool operators need to find an effective approach to evaluate the contributions of miners in the pool, the blockchain network require solutions to be submitted by miners. This method of evaluation is challenging due to the level of difficulty in finding a valid block within the system [8].

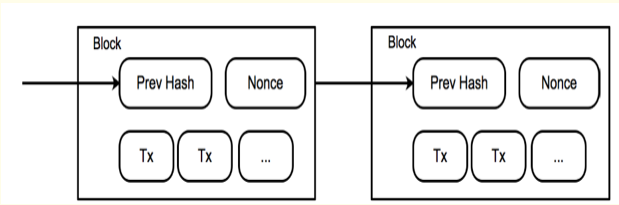

Figure 1: Two blocks within a PoW blockchain system.

Proof-of-stake (PoS)

The PoS was brought about by a need to reduce the computational power required to solve the computational puzzle thrown to miners. Proof-of-Stake also means Proof-of-Ownership. The nodes that want to mine the next block participate in a bid, the node with the highest bid gets the chance to mine the next block. This causes an increase in the number of miners to mine the blocks and reduces the incentives paid to miners [37-41].

Smart contracts

In this section, an overview of smart contract is provided. The popularity of programmable open distributed consensus systems based on blockchain technology has sparked interest in replicated stateful computations, sometimes known as smart contracts. Smart contracts regularly manage millions of dollars' worth of virtual currency, as blockchains are mostly employed in financial applications [31]. Smart contracts was first defined by Nick Szabo as a computerized transaction protocol that executes the terms of contract [42]. Alternatively, smart contract may be defined as a set of promises specified in a digital form, including protocols within which the parties perform on these promises [43]. They are typically deployed and secured on blockchain technology. In smart contract, trust only exists in formal relationships and smart contracts help users to reach a state of trust to transact with one another digitally. Blockchain helped provide a platform on which this idea could be fully implemented because it totally eradicated the use of third parties. So, trust on this system is provided via smart contracts i.e. computational PoW or PoS along with other computational proofs that exist. Smart contracts are very useful for digital transactions because they verify the transactions before it is allowed to go through this verification process is known as mining. Smart contracts are a vital part of blockchain irrespective of the application area in which it is used as data verification is necessary.

Proposed blockchain model

In this section, we provide an overview of the blockchain model proposed in this paper. In existing blockchain models, data is shared on the network when nodes request for a transaction. A new block is formed and before the block is added to the chain the system throws puzzles to be solved to the miners and the miners return the solution which allows the block to be added to the chain only after this transaction is complete.

In the proposed approach, the system solves the puzzle and uploads the computational results; the only entity that interacts with the system is the node that request the transaction and checked the block. The addition of codes to identify individuals took into consideration the need for privacy on the healthcare model and the change of the PoW model took into consideration the requirement of a PoW model that does not require as much computational work as current proof of work and state. Figure 2 shows the manner in which chain of blocks are connected in our model. The blocks are connected together in the form of a chain and every new block added contains information about the previous block which is the hash. When nodes connect to the platform, the nodes are assigned the codes along with their digital keys. Transactions are stored on every node on the network but the transaction may be stored with or without encryption. Encrypting the transactions or not depends on whether the assigned codes match with the codes of the generating nodes as illustrated in figure 3.

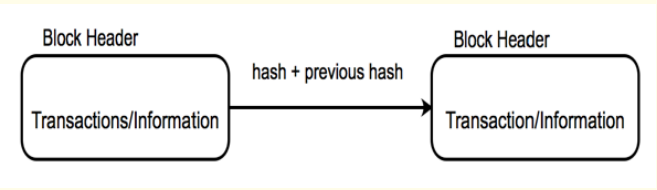

Figure 2: The proposed blockchain model.

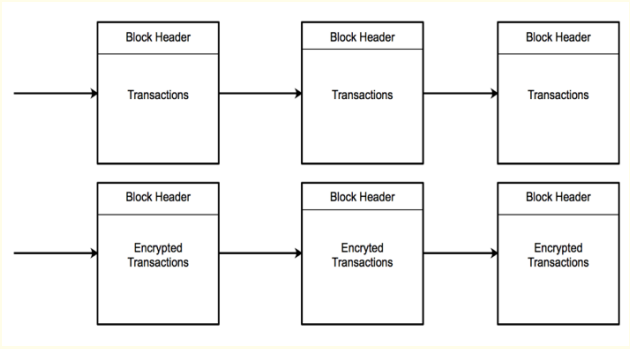

Figure 3: Transactions with or without encryption.

Algorithmic-based solution

In this paper, in generating the mathematical equation, the first form was a homogeneous differential equation: $\frac{dy}{dx}$.

A homogeneous equation was used because the process of checking for homogeneity can be used to determine the validity of a block. The adopted homogeneous equation (See equation 1) was such that:

$$\frac{dy}{dx} = x + y \quad \text{----------(1)}$$

From Equation (5), x represents the dependent variables and y the independent variable. x- represents the number of nodes and y represents the server token and the amount to be transferred during the transaction.

To evaluate the equation, we set the number nodes to 5 and the servers to 4 to obtain Equation 2.

$$\frac{dy}{dx} = 5x + 6y \quad \text{---------- (2)}$$

The level of difficulty *d*, was determined as the squared of $\frac{dy}{dx}$ because the complexity of the equation should increase in sequence if the equation is to the power of three, then the puzzle will immediately become a polynomial, i.e. an equation raised to three, then the time required to solve increases as shown in Equation 3.

$$d = \frac{dy^2}{dx} \quad \text{---------- (3)}$$

The first differential when *d* is made $\frac{dy^2}{dx}$ is 25 - 40xy + 16 using the perfect square trinomial. The differential when d is made is $\frac{dy^3}{dx} = 125x^2 + 300x^2y + 240xy^2 + 64y^3$. The differential equation method makes it challenging to determine the number of coins held by the node sending bitcoins, but it defines the number of coins to be sent. The verification for the number of tokens in a user wallet is not made. We compared the server tokens (i.e., the amount available on the server) and the tokens available in user wallet to determine the effect of the independent variable (that is, the server token) and the dependent (i.e., the number of nodes). The problems described above were solved from an algorithmic point of view. A brief description for the process are discussed based on code assignment, mining and computation of token.

Algorithm for assigning codes

The algorithm for assigning codes is used in defining the components of the hash for a block on the network. The hash is assigned when a new block is added to the chain. This algorithm is represented as follows:

Algorithm 1 Algorithm for Code Assignment to a New Block

Step 1: Start

Step 2: Declare method H (bool s||x)

Step 3: Then declare variables int code, int nonce, timestamp, int previous_hash, int no_of_block, int T

Step 4: Check for genesis block no_of_block = 1 + no_of_block

Step 5: If (no_of_block ==1)

Then initialize int hash = code + nonce + timestamp +T Else hash = previous_hash + hash.

Mining algorithm

The mining algorithm is implemented using the following parameters.

X: Is a random 128-bits number to make it impossible for two blocks to have the same computation starting point when two transaction requests are sent at the same time. k: is the work factor, i.e. the first bits of the hash function.

S: Is the string of bits generated in the transaction. i.e., the number of bitcoins being transferred during the transaction. It is used based on the service name to prevent mints on a server being used on another server.

T: Is the number of bitcoins available in the user's wallet. i.e., tokens

If (v ≥ s)

Then compute ();

For every new transaction request.

To model the behaviour of the nodes in the network, we represented the server tokens and the number of tokens the node owns to the actual number of tokens being sent. The algorithm mathematical represented as $s = \{0,1,...\}^*$, where s is the set of tokens or coins to be transferred during a transaction, s_i is the leftmost and rightmost bit, $s_{i...j}$ is the bit substring between i and j. This is also tied with a service term making it impossible to transport a server to a user over another server.

$$s = s_i||...||s_j \quad \text{-------(4)}$$

Algorithm 2 algorithm for mining:

Step 1: Start after hash is determined

Step 2: Declare the method to compute the puzzle if (H==h)

Then public compute ()

Else Discard block.

Algorithm to perform computations

This algorithm is for performing the actual proof-of-work or mining to add the block to the chain of blocks, and this is done when all required pre-conditions are met, i.e., the number of tokens the node is attempting to send is not higher than the number of tokens in the node's wallet.

Algorithm 3 algorithm for mining

Step 1: Start.

Step 2: Declare variable double compute, int s, int w; (Where s represents the number of bitcoins involved in the transaction and w represents the hash code for the transaction).

Step 3: Declare method public Compute () PUBLIC: hash function hash () with output size k bits V: value(T): it evaluates the token.

Performance evaluation and discussions

In this section, we use SageMath mathematics software system (version 9.0) to design the experiment and run the data analysis in Matlab. The implementation and testing was done in SageMath library under the Python 3 programming modules using machine (Lenovo Thinkpad L480) with the following computing specifications - CPU (Intel Core (TM) i5-8250U 1.60 GHz -1.80 GHz), and memory (16.0 GB) and evaluated. In the simulation, the number of nodes employed in the system ranged between 2 to 70 nodes. We performed sensitivity analysis to determine how the different values of an impacted the entire network under the following assumptions: 1) every set of nodes on the network is a 'correct' node (that is no transaction is, in turn, complete until it has been added to the chain of blocks) and 2) every account is an 'accurate' account (that is the transaction has not been tampered with). Figure 4 shows the complexity of the three algorithms studied in this paper. The complexity of the proposed algorithm increases in contrast with the proof-of-stake and proof-of-work algorithms. The complexity for the proposed algorithm increases at that speed at first because computations are generated for the first time on the setup test network, and the cost of mining is borne by the network increasing calculation complexity to set up the first puzzles for the network, so complexity for proposed algorithm is approaching 20 for the first 10 nodes. The proof-of-stake performs better than the other two algorithms because mining on the proof-of-stake was done with bidding for the right to compute taking place only ones on the testing server. The proof-of-work performed better because mining on the node took place at a constant pace and difficulty levels increased.

In figure 7, the proposed algorithms' complexity performs relatively better, and the complexity increases at a fair pace with an increase in the number of nodes and transactions performed by

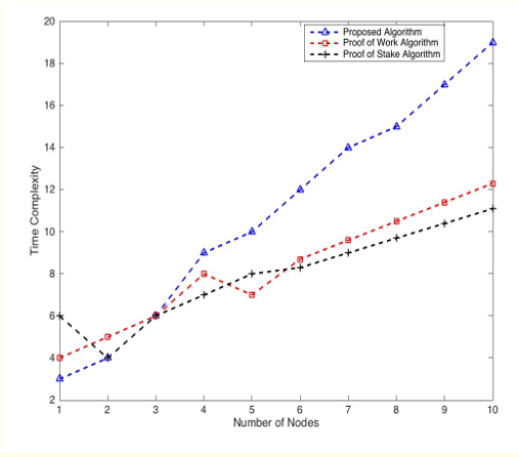

Figure 4: Time complexity for 10 nodes.

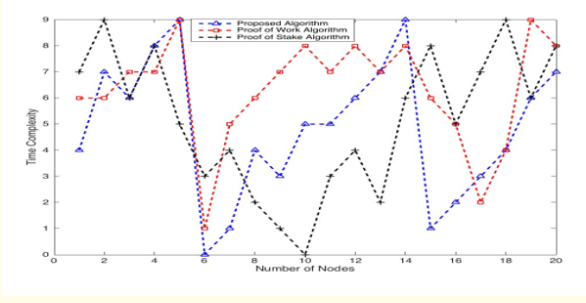

Figure 5: Time complexity for 20 nodes.

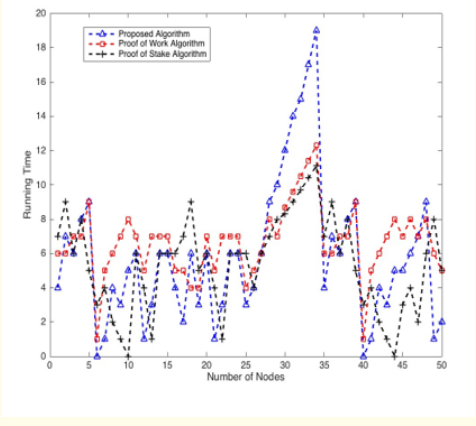

Figure 6: Time complexity for 50 nodes.

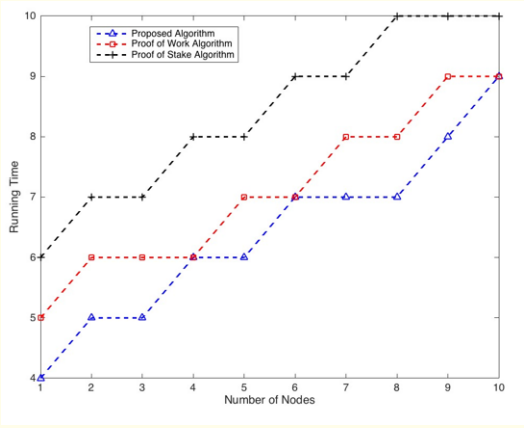

Figure 7: Running time for 10 nodes.

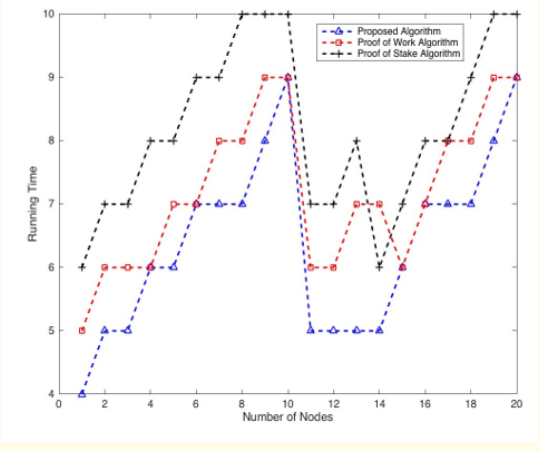

Figure 8: Running for 20 nodes.

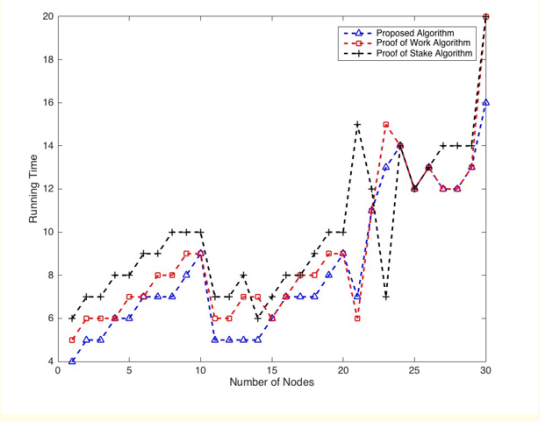

Figure 9: Running for 20 nodes. runtime to increase to 20.

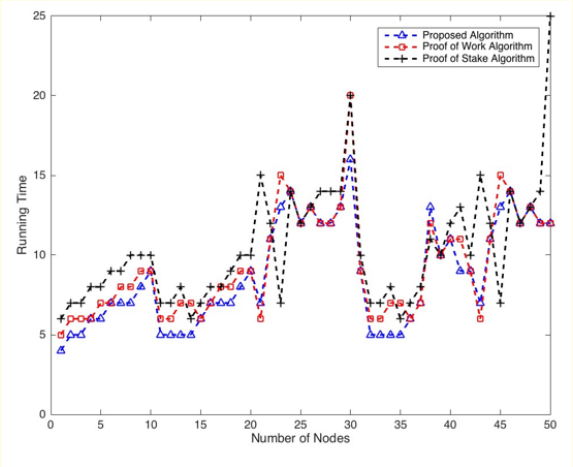

Figure 10: Running time for 50 nodes.

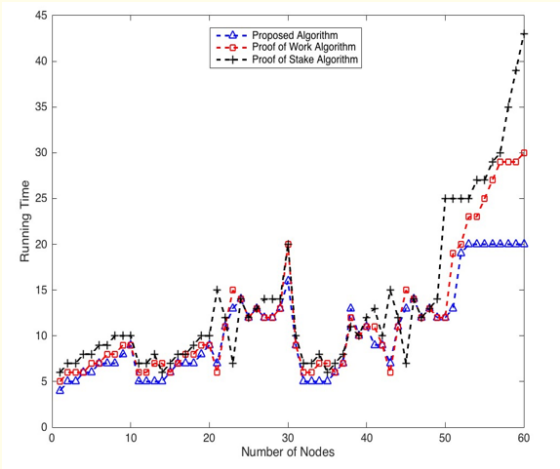

Figure 11: Running time for 60 nodes.

the nodes. The reason being that the system no longer formulates new puzzles with the addition of blocks and only increases the difficulty level of already existing puzzle, and, the proof of stake algorithm complexity increases because the experiment was performed with new bidding taking place every time a transaction request occurred. In figure 6, the proposed algorithm was tested by placing two trans- action requests from different nodes to different nodes at the same time to check for complexity and delays. The results shown in figure 6 indicates a spike in the complexity of the proposed algorithm with the running time approaching 20, similar to the result in figure 4. The proof-of-stake and proof-of-work algorithms were also tested under the same circumstances. The spikes are as a result of calculating the delay caused by the other transactions.

In figure 7, the algorithms were checked to determine their runtime with an increase in the number of nodes. The proposed algorithm runtime is seen to increase from 4-9 seconds for 10 nodes. This is because the puzzle was already generated from the very first experiment performed on the network. The proof of stake algorithm runtime is higher than that of the proof of work and proposed algorithm because bidding took place each time a new block was formed during the experiment. Proof-of-stake the data was collected with the same variables in place for the first experiment. In figure 8, the number of nodes was increased to 20, and the runtime for the proposed algorithm remained at 9 seconds for 20 nodes, and the runtime for the proof of stake and proof of work remained at 9 and 10 seconds respectively. This is because the experiment was performed under the same conditions similar to that of figure 7. The only difference was the increase in the number of nodes. So, it is assumed that the nodes requested transaction at the same rate as when the network was running with 10 nodes.

In figure 9, the nodes were increased to 30, and the algorithms were tested for their runtimes. This time around the number of transactions requested and the frequency of transactions request was increased in the experiment. This caused a spike in the time required to mine a block on the network using the various algorithms.

The proof of stake and proof of work saw the highest increase because the cost of mining is borne by the nodes and the network, causing their seconds each. The runtime for the proposed algorithm also increased to 16 seconds when 30 nodes were placed on the network.

In Figure 10, the rate of transaction request was maintained, and the number of nodes placed on the network was increased to 50 nodes. We observed a sharp decline in running time for all three algorithms. There was an increase in the running time to 25 for the proof-of-stake. The running time for the proof-of- work and

the proposed algorithm was reduced. The proof of stake runtime was 25 seconds, and the runtime for the proof of work and the proposed algorithm was 12 seconds each. In figure 11, we maintained the rate of transactions but increased the number of nodes to 60. The running time of the proposed algorithm was the same as in figure 10, and the runtime for proof of stake and proof of work algorithms increased to 42 and 30 seconds, respectively.

Conclusion

The algorithm was designed to assist in blockchain implementation in other areas apart from finance. In our new approach, nodes that access ledger information and help IoT devices perform computations are verified. Based on the experimental results, our algorithm performed better at 50 nodes. Smart contracts may be applied in several applications, for example, insurance, transportation, and smart cities. Hence, future blockchain technologies implementing smart contracts should be designed to accommodate an increased number of nodes. Smart contracts require a great deal of security if implemented in sensitive areas such as financial institutions. Hence, researchers should provide new mechanisms to validate transactions to prevent theft and spoofing. A new area where these could be implemented is product sorting where the implementation of blockchain could be used in sorting systems. The major limitation and advantage of blockchain is that when transactions have been recorded further changes cannot be made, so in sensitive application areas like IoT faulty nodes must be checked and repaired to prevent the recording of incorrect data.

Acknowledgements

We appreciate colleagues who supported us in diverse ways especially encouraging us to get to this point of publication.

Conflict of Interest

There is no conflict of interest of any kind.

Bibliography

1. Christidis Konstantinos and Michael Devetsikiotis. "Blockchains and smart contracts for the internet of things". *IEEE Access* 4 (2016): 2292-2303.

2. Bach Leo Maxim., *et al*. "Comparative analysis of blockchain consensus algorithms". 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE (2018).

3. Antonopoulos Andreas M and Gavin Wood. "Mastering ethereum: building smart contracts and dapps". O'reilly Media (2018).

4. Zheng Zibin., *et al*. "Blockchain challenges and opportunities: A survey". *International Journal of Web and Grid Services* 14.4 (2018): 352-375.

5. Nakamoto Satoshi. "Bitcoin: A peer-to-peer electronic cash system". Manubot (2019).

6. Michael J., *et al*. "Blockchain technology". *The Journal* 1.7 (2018).

7. Underwood Sarah. "Blockchain beyond bitcoin". *Communications of the ACM* 59.11 (2016): 15-17.

8. Qin Rui., *et al*. "Research on the selection strategies of blockchain mining pools". *IEEE Transactions on Computational Social Systems* 5.3 (2018): 748-757.

9. Nguyen Quoc Khanh. "Blockchain-a financial technology for future sustainable development". 2016 3rd International conference on green technology and sustainable development (GTSD). IEEE (2016).

10. Ahram Tareq., *et al*. "Blockchain technology innovations". 2017 IEEE Technology and Engineering Management Conference (TEMSCON). IEEE, (2017).

11. Houben Robby and Alexander Snyers. "Cryptocurrencies and blockchain". *Bruxelles: European Parliament* (2018).

12. Böhme Rainer., *et al*. "Bitcoin: Economics, technology, and governance". *Journal of economic Perspectives* 29.2 (2015): 213-238.

13. Atzori Marcella. "Blockchain technology and decentralized governance: Is the state still necessary?". *Available at SSRN 2709713* (2015).

14. Marwala Tshilidzi and Bo Xing. "Blockchain and artificial intelligence". *arXiv preprint arXiv:1802.04451* (2018).

15. Swan M. "Blockchain AI: Consensus as the mechanism to foster 'friendly'AI". *Institute for Ethics and Emerging Technologies* (2014).

16. e Koronkevich Paule. "Obsidian in the Rough: A Case Study Evaluation of a New Blockchain Programming Language". *SPLASH Student Research Companion* (2018).

17. Walch Angela. "The bitcoin blockchain as financial market infrastructure: A consideration of operational risk". *NYUJ Legis. and Pub. Pol'y* 18 (2015): 837.

18. Huh Seyoung., *et al*. "Managing IoT devices using blockchain platform". 2017 19th international conference on advanced communication technology (ICACT). IEEE (2017).

19. Kshetri Nir. "Can blockchain strengthen the internet of things?". *IT Professional* 19.4 (2017): 68-72.

20. Linn Laure A and Martha B Koo. "Blockchain for health data and its potential use in health it and health care related research". ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST (2016).

21. Azaria Asaph., *et al*. "Medrec: Using blockchain for medical data access and permission management". 2016 2nd International Conference on Open and Big Data (OBD). IEEE (2016).

22. Shae Zonyin and Jeffrey Tsai. "Transform blockchain into distributed parallel computing architecture for precision medicine". 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS) IEEE (2018).

23. Aves Alex. "The application of blockchain in the pharmaceutical sector". (2018).

24. Hegadekatti Kartik and Yatish SG. "Kibbutz Economy Interactions with Blockchains and Cryptocurrency Networks". *Available at SSRN 2916278* (2017).

25. Cabello Juan., *et al*. "Distributed library management system based on the blockchain technology". *Atos IT Challenge* (2017).

26. Hoy Matthew B. "An introduction to the blockchain and its implications for libraries and medicine". *Medical Reference Services Quarterly* 36.3 (2017): 273-279.

27. Liu Xidong. "A smart book management system based on Blockchain platform". 2019 International Conference on Communications, Information System and Computer Engineering (CISCE). IEEE (2019).

28. Verma Manish. "Amalgamation of Blockchain Technology and Knowledge Management System to fetch an enhanced system in Library". (2021): 474-477.

29. Coblenz Michael. "Obsidian: a safer blockchain programming language". 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C). IEEE (2017).

30. Sergey Ilya., *et al*. "Safer smart contract programming with Scilla". *Proceedings of the ACM on Programming Languages* 3. OOPSLA (2019): 1-30.

31. Foschini Luca., *et al*. "Hyperledger Fabric Blockchain: Chaincode Performance Analysis". ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE (2020).

32. Li Bo. "Blockchain and smart contracts in health-related My Data scenario". (2017).

33. Vasin Pavel. "Blackcoin's proof-of-stake protocol v2". 71 (2014).

34. Li Wenting., *et al*. "Securing proof-of-stake blockchain protocols". *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, Cham (2017): 297-315.

35. Saleh Fahad. "Blockchain without waste: Proof-of-stake". *The Review of Financial Studies* 34.3 (2021): 1156-1190.

36. King Sunny and Scott Nadal. "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake". Self-Published Paper, August 19 (2012): 1.

37. Poelstra Andrew. "Distributed consensus from proof of stake is impossible". Self-published Paper (2014).

38. Milutinovic Mitar., *et al*. "Proof of luck: An efficient blockchain consensus protocol". Proceedings of the 1st Workshop on System Software for Trusted Execution (2016).

39. Gaži Peter., *et al*. "Stake-bleeding attacks on proof-of-stake blockchains". 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE (2018).

40. Cao Bin., *et al*. "When Internet of Things meets blockchain: Challenges in distributed consensus". *IEEE Network* 33.6 (2019): 133-139.

41. Szabo Nick. "Smart contracts: building blocks for digital markets". *EXTROPY: The Journal of Transhumanist Thought* 18.2 (1996).

42. Wang Shuai., *et al*. "Blockchain-enabled smart contracts: architecture, applications, and future trends". *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 49.11 (2019): 2266-2277.

43. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Volume 3 Issue 8 August 2021