J Multidisciplinary Scientific Journal

MDPI

Article

Crypto Hash Algorithm-Based Blockchain Technology for Managing Decentralized Ledger Database in Oil and Gas Industry

Lukman Adewale Ajao [1,*], James Agajo [1], Emmanuel Adewale Adedokun [2] and Loveth Karngong [1]

[1] Department of Computer Engineering, Federal University of Technology, Minna 920001, Nigeria
[2] Department of Computer Engineering, Ahamadu Bello University, Zaria 810241, Nigeria
* Correspondence: ajao.wale@futminna.edu.ng; Tel.: +234-70-3735-9128

Received: 16 June 2019; Accepted: 1 August 2019; Published: 8 August 2019

Abstract: This research work proposes a method for the securing and monitoring of petroleum product distribution records in a decentralized ledger database using blockchain technology. The aim of using this technique is to secure the transaction of distributed ledgers in a database and to protect records from tampering, fraudulent activity, and corruption by the chain participants. The blockchain technology approach offers an efficient security measure and novel advantages, such as in the transaction existence and distribution ledger management between the depot, transporter, and retailing filling station. Others advantages are transparency, immunity to fraud, insusceptibility to tampering, and maintaining record order. The technique adopted for this secure distributed ledger database is crypto hash algorithm-1 (SHA-1)-based public permissioned blockchain and telematics, while this telematics approach is an embedded system integrated into an in-vehicle model for remote tracking of geolocation (using Global Positioning System (GPS)), monitoring, and far-off data acquisition in a real-time. The scope of the data in the secure distributed ledger database (using blockchain) developed are identification (ID) of the tanker operator, Depot name, Source station ID, Destination station ID, Petroleum product volume, Transporter ID, and Geographic automobiles location. This system proved to be efficient, secure, and easy to maintain as it does not permit any individual for records tampering, but supports agreement of ~75% of participants in the chain to make changes.

Keywords: blockchain; database; petroleum product; security; telematics

1. Introduction

In the last decades, oil and gas (petroleum product) have been key sources of revenue, liveliness, and industries for the national economy and its development [1]. Nigeria is recognized as one of the highest ranked petroleum product exporting countries in the Organization of the Petroleum Exporting Countries (OPEC) eleven [2]. However, the distribution process of this product in Nigeria has been a great challenge over the years and generally caused fluctuation in the country's economy. These challenges are fuel scarcity, oil and gas hijacking, inflation in price, and many others.

The disruption in the supply of this inflammable resource in Nigeria has been a habitual problem as its distribution has a multitude of problems. Aminu et al. proposed petroleum products (oil and gas), aside from other occupation practices in the marketing supply chain, are generally an imperative source of energy globally, and represent a major part of the economies of most developed nations, including USA, UAE, Saudi Arabia, and so on [3]. One of the reasons for this product scarcity in the nation was due to the transaction's susceptibility to corruption, fraud, and lack of transparency among the parties

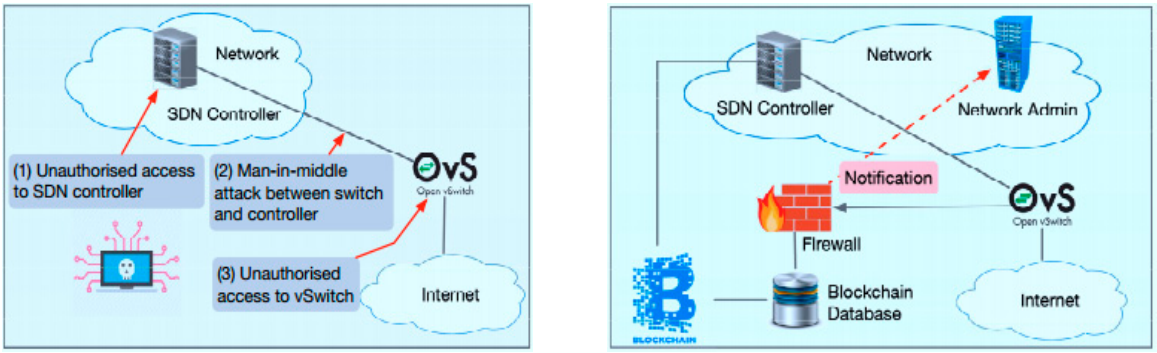
involved in the supply chain and distribution process [4]. Fraud, corruption, and mismanagement in the distribution process is traced back to the usual application of manual transaction, centralized distributed ledgers, and pipeline network distribution vandalism [5].

Although the earlier transaction record is known as a pictographic tablet (3200 BC) ledger, a record of transactions used for keeping information by any business organization in the earlier century [6,7]. The later advanced technology of keeping records in worksheet is known as computerized spreadsheet. This digitized ledger was designed as a centralized ledger that exposes its vulnerability to tampering and susceptibility to corruption and fraud. Others issues are central control and mishandling, which led to the emergence of the crypto-blockchain technology proposed in this research for decentralized ledger system management.

Blockchain is the technology behind bitcoin [8] and has advanced revolutionary services with the ability to influence financial transactions and render advantages of transparency, accurate tracing, permanent ledger, cost reduction, and record management [9]. This blockchain technology provides a solution to the digital confidence of record-keeping and information management with a timestamped, transparent, and decentralized distributed database block [10].

Blockchain is a network of databases that spread across multiple entities, which are kept in sequence and are not peculiar to a single source of control [11,12]. It gives access to information update, but the historical data stored cannot be changed or modified without a broad agreement from the partakers of the network. This means that an administrator from a single unit of the distributed network cannot be allowed to tamper or modify the stored data held on a blockchain without agreement from other participants in the network. Some of the major advantages of blockchain include distributed, efficiency, immutability, security, transparency, and resilience [13].

The blockchain technology has been widely adopted as a security countermeasure against Internet of Things (IoT) and software-defined network (SDN) securities challenges and cyberattacks [14]. Detection of fraudulent rules is proposed by Ferra et al. for security contest and as a countermeasure against man-in-the-middle attack (MITMA) over the SDN using a blockchain technology [15], as illustrated in Figure 1. A lightweight cryptography technique with Open-Flow rules based on the software-defined networks and leveraged on blockchain technology is utilized to achieve accurate detection of fraudulent attempts in the system. The result of the BLOOSTER system proposed demonstrates adequate detection of tampering and fraudulent within short detection time rate of 100%. The blockchain technology demonstrates the possibility and improvement (including immutability, security, and transparency) over the traditional centralized ledger-based database as in the banking industry, national population data management, election voting system management, and e-business transaction.



(**a**) (**b**)

Figure 1. (**a**) Threat model in a network and (**b**) proposed secured blockchain architecture [15].

The authors contributions in this research are centered on the crypto hash blockchain-based database development for securing the decentralized ledger of petroleum distribution records and to safeguard data transaction regarding oil and gas products within the supply chain; also, the

development of an embedded in-vehicle automated tracking system using a global positioning system (GPS) approach for tracking the movement and geographical location of automobile conveyance, as well as volume level of petroleum product in an automobile is inclusive monitored using pairs of ultrasonic sensors in case of leakages, tampering, or other theft activities. The GPS transmission–receiver and its component are integrated and embedded in a strategic location of the automobile conveyance. Consequently, all information acquired is dynamically sent to the crypto-database for update, storage, and safeguarding using a miner algorithm as a distributed ledger principle.

2. Blockchain and Informatics Technology Investigation

Kogias et al. discussed a methodical survey of decentralized digital currencies (Bitcoin) and its limitations as the first implementation of blockchain technology [16,17]. This work discussed how to enhance the performance of Bitcoin security with consistency through collective signing. It was proposed to achieve a high level of secretive consensus and safeguard Bitcoins in open affiliation. The ByzCoin technique utilizes communication trees to augment transaction commitment and authentication by ensuring safety and liveness against deceitful faults; it also provided near-optimal tolerance for the group of membership. Therefore, optimizing the tree-structured communication of Bitcoin further reduces the latency to less than 30 s, which achieved a throughput greater than Paypal's performance with an authorization latency of 15–20 s. Although, this technology (ByzCoin) has a limitation of malicious that can hypothetically exclude nodes from the consensus process.

A Uniform Commercial Code (UCC) is proposed by Chima and Hill, (2007) to improve on the supply chain management problems in the petroleum industry. This industry is involved in a global supply chain product that includes local and international transportation, inventory, ordering, import/export, visibility and control, and information technology. In this supply chain, a company is connected to its upstream suppliers and downstream distributors as materials, data, and capital flow through the supply chain [18].

Kshetri (2017) evaluates the roles of blockchain technology and whether it strengthens the Internet of Things security architecture. It underlies the mechanisms associated with the blockchain-based IoT security node and how blockchain-based resolutions could be implemented in many facets of the IoT ecosystem [19].

Medical record (MedRec) based on blockchain technology is developed as a prototype for securing electronic health archives and medical research data. This system secures logs and provides easy access to their medical data and treatment diary. Using a blockchain technology approach safeguards some sensitive medical records and information and it renders some security services such as authentication, confidentiality, and accountability [20]. The MedRec technology, thus, facilitates the emergence of data economics, delivering big data to empower scholars while appealing patients and providers in the choice to release metadata.

The utilization and development of radio frequency identification (RFID)-based blockchain technology was studied and the merits and disadvantages of using RFID with blockchain technology in creating an agri-food supply chain traceability system were analyzed by Tian (2016). According to this work, food safety has posed serious challenges on the China Nation as a result of traditional agri-food logistics pattern that are no longer matches the demands of the market was described. Therefore, this contest called for the urgent attention in building or developed agri-food supply chain traceability system based blockchain technology. This system can enhance the traceability with trusted information in the entire agri-food supply chain with a consistent guarantee of food safety by gathering, transferring, and allocating reliable data of agri-food to the various production, processing, warehousing, disbursement, and marketing links [21].

Telematics as a French ellipsis (telecommunication and informatics) is utilized as a wireless network technology and communication technique for location tracking, monitoring, and surveillance [22,23]. All the information acquired through this telematics system is remotely transmitted to the crypto hash decentralized database and is dynamically updated with permission of ~75% of the participants

in the chain agreement for any alteration. García et al. developed a service-oriented universal computing model based on decentralized systems for public road transport monitoring. This system is an intelligence-based, service-oriented utility developed to improve highway safety, transportation system management, provide real-time information to travelers, and manage information about public transport systems [24].

An autonomous vehicle in real-time implementation is developed for monitoring path-following of the vehicle using spatial dual global positioning satellite (SDGPS). The system performance is satisfying the trajectory tracking necessities. The block diagram for this proposed method using spatial dual GPS is illustrated [25], and the model in the design is expressed as in Equation (1) using a standard bicycle model [26,27]. A road safety notice and driver assistance smart system based on telematics approach and server-oriented system is developed to provide real-time information assistance to the driver, speed safety information, and data about roads with obstacles, rainfall, or snow [28]. The algorithm and model for these proposed objectives are divided into two parts: a highway-traffic parameter framework and road surface data model for monitoring speed *vj* and distance at time t on the road section j as expressed in Equation (2).

$$\begin{bmatrix} \dot{y} \\ \dot{r} \end{bmatrix} = \begin{bmatrix} -\frac{C_{\propto f}+C_{\propto r}}{mv_x} & -\frac{C_{\propto f}+C_{\propto r}}{mv_x} \\ \frac{l_f C_{\propto r}-l_r C_{\propto f}}{I_z v_x} & \frac{-l_f^2 C_{\propto r}-l_f^2 C_{\propto f}}{I_z v_x} \end{bmatrix} \begin{bmatrix} y \\ r \end{bmatrix} + \begin{bmatrix} \frac{C_{\propto f}}{m} \\ \frac{l_r C_{\propto f}}{I_z} \end{bmatrix} \delta \quad (1)$$

where,

y	is the vehicle longitudinal velocity (m/s)
r	is the yaw rate (%)
δ	the wheel steering angle of the vehicle (rad)
$C_{\propto f}$	is the front wheels stiffness when curve (N/rad)
$C_{\propto r}$	is the rear wheels stiffness when curve (N/rad)
l_f	is the length between CoG to front axle (m)
l_r	is the length between CoG to rear axle (m)
m	the mass of vehicle (kg)
I_z	Inertia moment around the *Z*-axis (kg/m^2)

$$\mu_{vj}(t) = [\text{₮}_{rt} + \sqrt{\text{₮}_{rt^2} + \frac{2 \cdot (\text{₮}_{rt} \cdot v_j(t) + \delta) \cdot \text{₮}_{rt}}{g(f_j(t) + \omega_j(t))}}]_{[g(f_j(t)+\omega_j(t))]} \quad (2)$$

where,

$\mu_{vj}(t)$	the mean speed at time t on the road section j in (m/s)
₮_{rt}	is driver perception and response time (s)
δ	the vehicle distance + gap between vehicle
g	is the acceleration due to gravity rate, 9.8 (m/s)
$f_j(t)$	the frictional-road parameter at time period t on the road section j
$\omega_j(t)$	the level of road section j link during collection period t (%)
t	is collection time period (s)
j	number of road sections.

2.1. Blockchain Technology Types

In general, after the emergence of Bitcoin technology, there are three types of blockchain technologies—public-based permissioned, private-based permissioned and permissionless, or consortium or federated blockchain [29].

1. The public permissioned blockchain is a transparent and open permissioned-based Litecoin system, which allows anyone to update or review anything at a time required. This technology

allows anybody to participate in managing the blockchain as public. It is also known as a permissioned blockchain without any centralized authority required for the verification process as found in the Ethereum, Litecoin, and Bitcoin technology [30]. This type of technology allows complete node running, easy transaction, review, or audit the blockchain by any participant in the Bitcoins/Litecoin (BTC/LTC) chain of blockchain explorer.

2. Private blockchain is an advanced Bitcoin technology that is managed centrally by an individual or organization for adequate security. This permissioned-based blockchain does not allow negotiation of the distributed network management as found in the BankChain practices. This technology does not allow anyone to run a full node and start mining and does not grant transactions access or review/audit by anyone or individual on the blockchain. The private blockchain is a permissioned-based design for central authority and process authentication.
3. The Consortium or Federated Blockchain eliminates the sole autonomy in the private blockchain by making sure there is more than one person in charge of chain management. Different authorities come together to make decisions that are good for the network such as a group of companies or representatives of individuals involved. It is also known as the hybrid blockchain because it combines both the characteristics of a public blockchain and the private blockchain. The R3 companies (New York City, NY, USA) and Energy Web Foundation (EWF) are open source and scalable blockchain platforms.

2.2. Secure Hashing Algorithm (SHA-1)

The most adopted secure algorithms associated with the blockchain technology are (SHA-1, SHA2, and SHA-256) encryption because of their unique quality of hash function that create unique outputs when given different inputs [31,32]. The hash function here is a unique key created to identify a transaction that at the same time identifies an individual in the petroleum supply chain. SHA was originally designed by the United States National Security Agency (NSA) and United States Federal Information Processing Standard. This algorithm is efficient in verifying file and message integrity during transaction, data identification, and password verification. SHA-1 has a message size of $<2^{64}$ bits, 512-bit block size, 32-bit word size, and 160 message digests [33].

Blockchain technology is a combination of blocks in its architecture. Each block is made up of data and the hash of the previous block, except for the origin block that contains no previous hashing as shown in Figure 2.

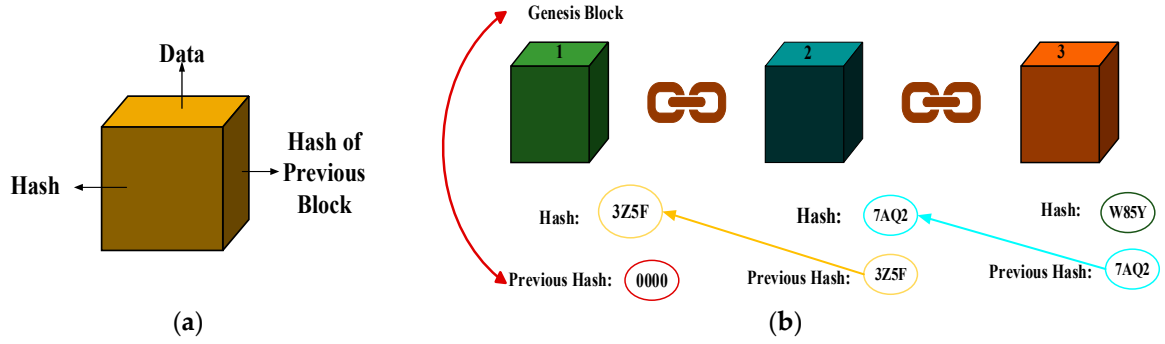


Figure 2. (**a**) Hash block component. (**b**) Blockchain network.

Blockchain technology functions are reliable for use in a hashing crypto method, which helps create an adequate and strong hashing code and convert it from a bit of fixed size data to strings of character. Each transaction proposed in a blockchain are hashed together before shoving in a block, and the hash pointers connect each block to the next block for holding of previous hash data as it is undisputable. Therefore, any changes in the blockchain transaction of hashing function will result in different hash string of character and affect all the involved blocks. The efficient practice of this technology (crypto-blockchain) in the transaction is that any changes propagated by less than 75% of

participants in the chain will result in attack; otherwise, more than 75% from the chain must agree before any alteration. The generation of hash algorithm image using avalanche effect is shown in Figure 3.

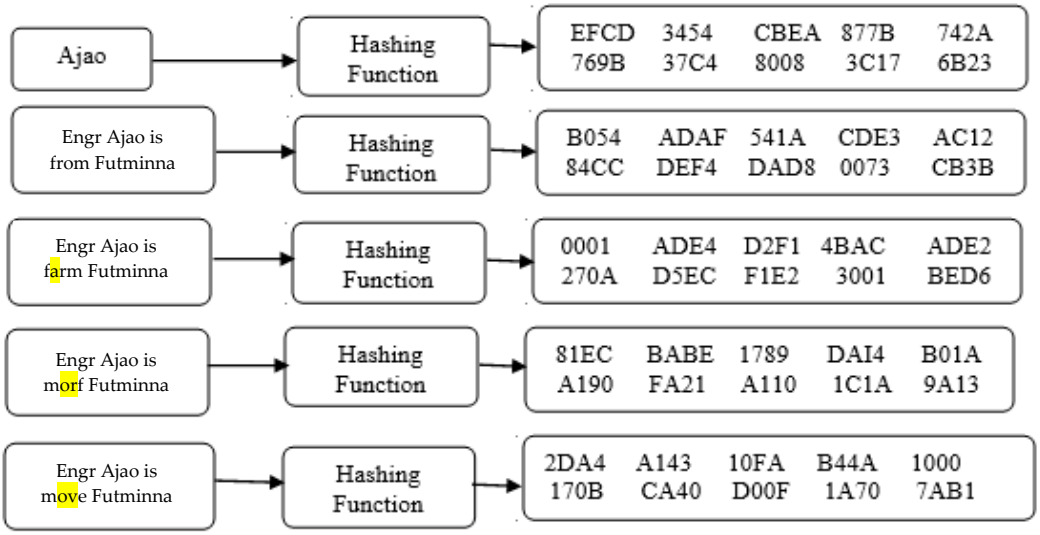


Figure 3. Crypto hash function.

2.3. Problems Statement

Most developed and developing countries, including USA, UAE, Saudi Arabia, Iraq, and Nigeria, among other African countries, are majorly dependent and have economies driven by oil and gas products, serving as the largest means of generating income. The distribution process of these oil and gas products is achieved through the pipeline network from refineries to the depot, to the marketer, and to the final consumers, which are threatened and vulnerable to different attacks, vandalism, and materials expiration (corrosion). However, the road network is another means of conveying oil and gas products from one place to another over long distances, which in the past resulted in serious hazards (accident), product diversification, automobile hijacking, and leakages [34]. Also, some developing countries, like ours (Nigeria), are still utilizing a centralized ledger or manual methods for managing the records of oil and gas product distribution across the states, which is susceptible to fraud, record tampering, and solely autonomy. This shortcoming has become a serious challenge to the oil and gas industries as well as the governments of the nations. Therefore, this sabotage and threat requires maximum attention of the government and industries collaboration for adequate coordination, planning, monitoring, and effective control to achieve maximum level of protection and reduces crisis of fuel scarcity, hijacking, and many others threats.

3. Materials and Methods

The methods adopted in this research are two-fold: the development of secure hash-based blockchain technology for the safeguarding of decentralized distributed ledger (petroleum products distribution data) using consolidation of programming languages and an embedded in-vehicle geotracking and autoremote monitoring system using telematics technique.

The development of a distributed database and web application for the management of petroleum product distribution consists of My Structured Query Language (MySQL), Personal Home Page (PHP) scripting language, JavaScript, and cryptography hashing (SHA-1). The secure blockchain database for this concept was designed using the phpMyAdmin graphical user interface, web application, and public permissioned blockchain-based hashing (SHA-1) was implemented with PHP scripting language and JavaScript. The design of permissioned blockchain approach is classified into four basic nodes, which are the regulator, petroleum depot, filing station, and transporter nodes. These nodes are the

network members in a decentralized ledger network. The method proposed for crypto hash database functions of the decentralized petroleum products is illustrated in Figure 4. The blockchain nodes (users) and the graphic user interface were created using PHP scripting language, HTML scripting language, CSS scripting language, and JavaScript scripting language.

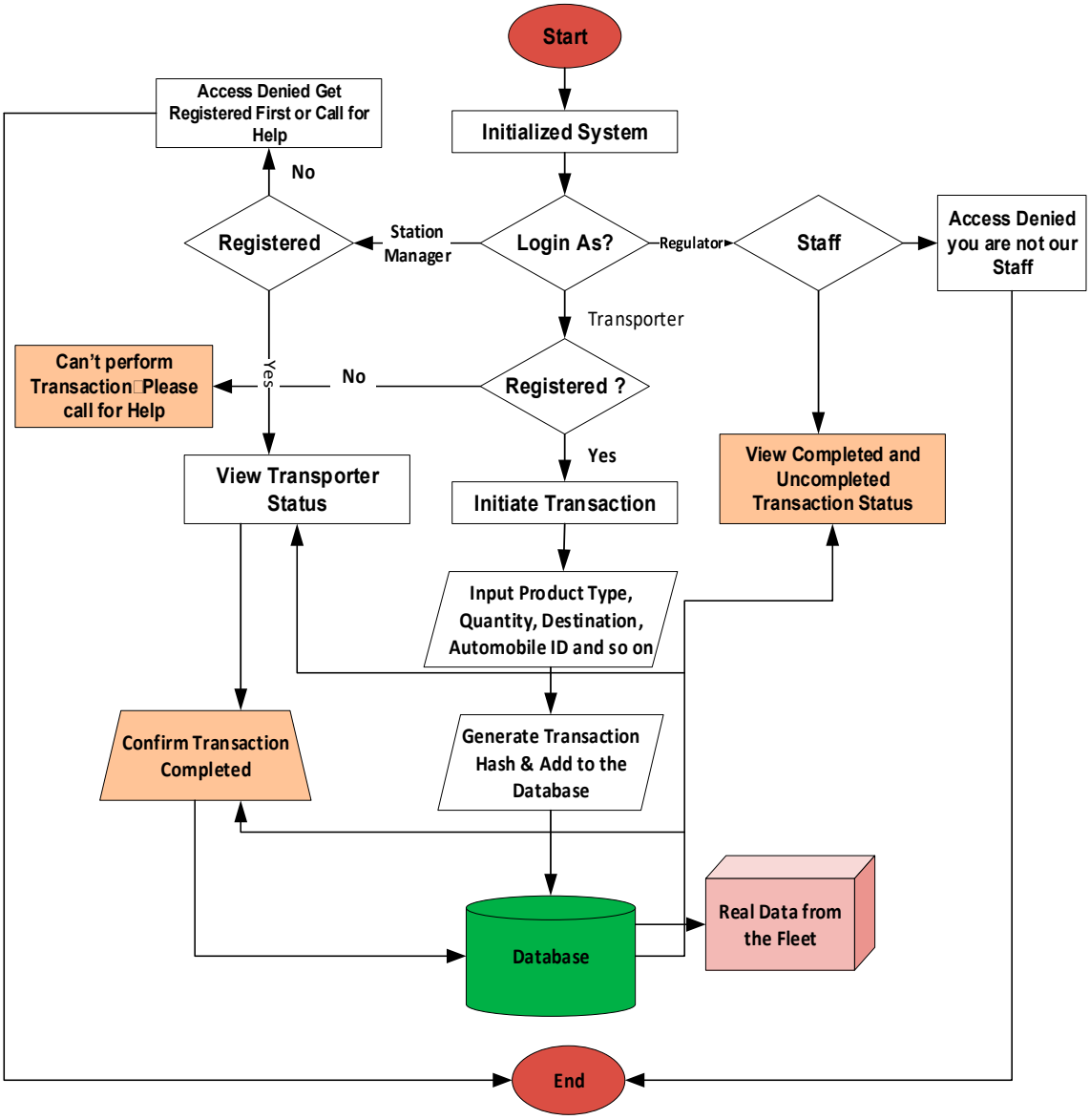


Figure 4. A crypto-database system flow diagram.

3.1. Blockchain Transactions Architecture for Petroleum Product Distribution

A transaction is a copy of transference of assets (digital currency, units of inventory, etc.) between two or more parties in a chain. To carry out a transaction in this system, a tanker fleet drives to the depot and a transaction is initiated by the depot operator/administrator. After the transaction is initiated, a hash of the transaction is generated using the SHA-1 hash function (public key), which is generated based on the previous transactions. This transaction detail is propagated to the participants in the blockchain with generated hash value of that particular transaction and it can be decrypted using (private key). The transaction of oil and gas product architecture is presented in Figure 5, which comprises three major components (the source, third-party (transaction) and agent.

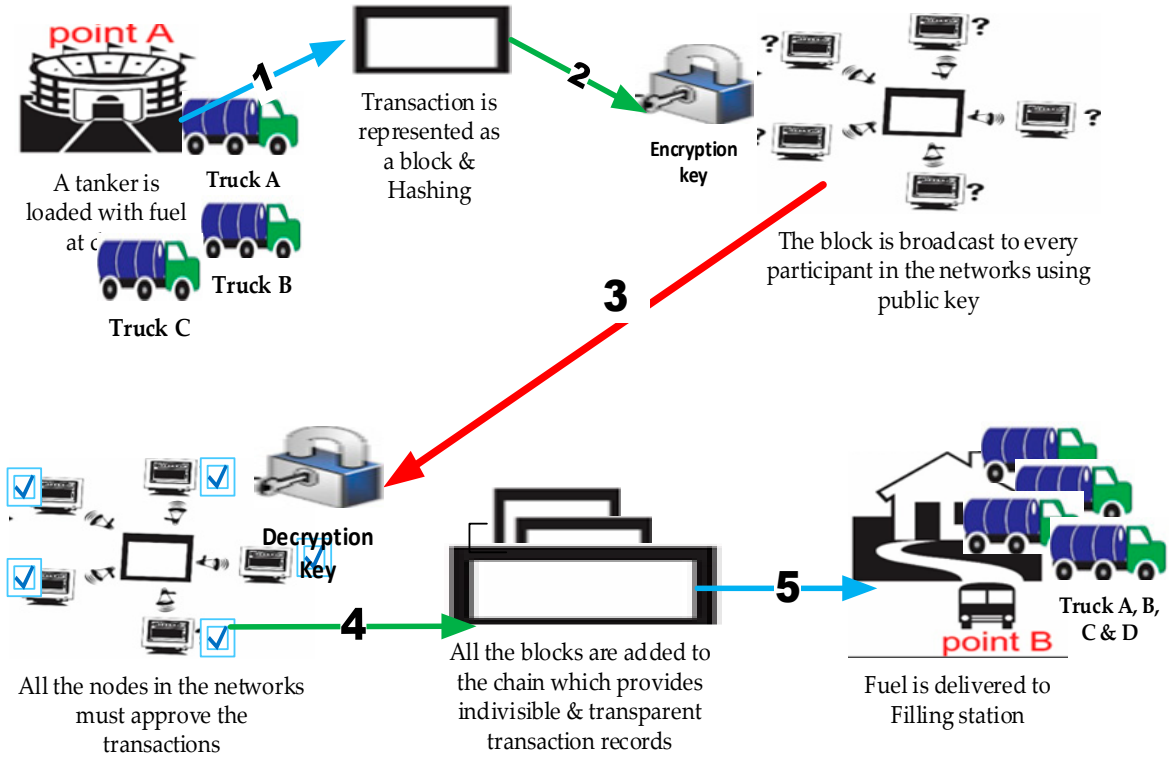


Figure 5. Blockchain transaction model of the developed system.

The source (φ) in this contest refers to the refineries/depot, third-party is the automobile conveyance that is not trusted in the chain and is known as a transaction, and the agent/destination (β) refers to the retailers (Filling station or distributor). Table 1 illustrates the transaction process between the two parties (source A (φ) to different agent or destination B (β_i^n) with many transaction queues in the chain for petroleum distribution using public-permission blockchain.

Table 1. Transaction activities in the blockchain.

S/N	Conveyance ID	Quantity (Liter)	Transaction ID	Destination Area ID	Relation between A→B
1	Ϗ	44,000	$Ϗ_{44,000}$	Minna (M)	$Ϗ_{44,000}$=> φ→ M
2	ϖ	33,000	$ϖ_{33,000}$	Lokoja (λ)	$ϖ_{33,000}$ => φ→ λ
3	μ	11,000	$μ_{11,000}$	Bida (ϐ)	$μ_{11,000}$ => φ→ ϐ
4	ϒ	33,000	$ϒ_{44,000}$	Ilorin (ζ)	$μ_{44,000}$ => φ→ ζ
5	£	44,000	$£_{33,000}$	Okene (ρ)	$μ_{12,000}$ => φ→ ρ

The operation principle of this public-permissioned blockchain used in this designed are divided into two parts which are open ledger belief and decentralized ledger coding.

1. Open Ledger Belief (OLB): This help every participant in this network/chain to see and aware of transaction and its content on the chain and then validate using mining (public key). Here are the procedures.

   i. The oil and gas products are transported between points A and B through the third-party (automobile conveyance).

   ii. The third-party (automobile conveyance) is not trusted with $^{44,000\,L}$ $(Ϗ_{44,000})$ of transaction from point A to point B. The transaction relation between two parties is expressed as $Ϗ_{44,000}$=> φ→ ^{M} and attached with link.

iii. All transactions in the chain are validated using a public key for every participant agreement in the network.

2. Decentralized ledger coding (DLC): This database helps govern the transaction in the chain/network with consensus agreement on the record updates without central authority or third-party negotiation. It has timestamp with unique credentials signature which makes all the transaction history in the chain immutable. These procedures are involved in the operation principle of DLC.

i. Broadcasting and publishing a copy of transaction to the network as follows, $\varpi_{33,000} =>$ $\varphi \rightarrow \lambda$, $\mu_{11,000} => \varphi \rightarrow \mathfrak{b}$, $\mu_{44,000} => \varphi \rightarrow \zeta$, $\mu_{12,000} => \varphi \rightarrow \rho$.

ii. Synchronize the copy to ensure that transaction gets to all participants in the chain/network.

iii. Use a mining algorithm to validate the transaction by computing random hash number generation as a special key used by every participant in the network.

Furthermore, the use of this technology (blockchain) assists in securing the transaction of records (distributed ledger database), avoiding record tampering by sole autonomy or fraudulent participant, making immutable (difficult for an individual participant to tamper or modify), and rendering security. The transaction block diagram of blockchain technology is illustrated in Figure 6.

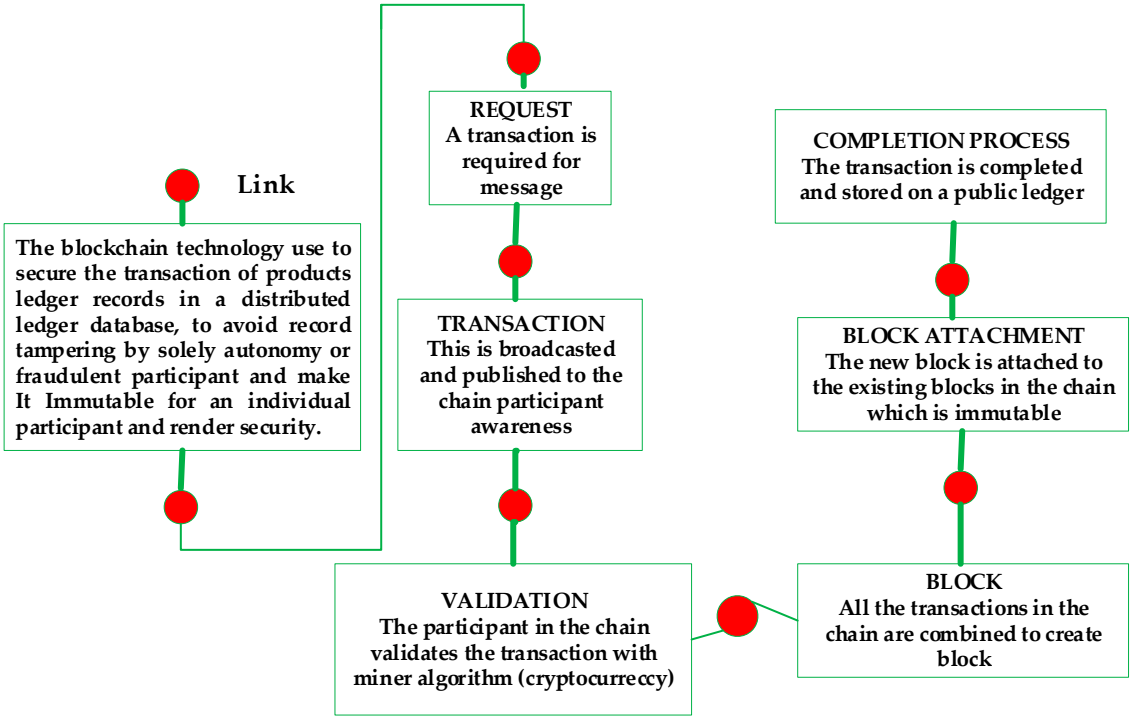


Figure 6. Transaction block diagram in blockchain.

3.2. Crypto Hash Algorithm Functions

In this research, SHA-1 was used to implement the permissioned blockchain for securing the decentralized database of distribution petroleum products. In cryptography, the Secure Hash Algorithm is a cryptographic hash function that takes an input and produces a 160-bit (20-byte) hash value known as a Message Digest (MD), which is rendered as hexadecimal number of 40 digits long (Cryptotrack and cryptotrack). The crypto-blockchain block architecture and secure hash algorithm are outlined.

Cryptotrack: 6BD736F1C2DC0B566812B92B7C47EBA39BCD5222
cryptotrack: 5AA13558D0CCA00C53EDD39427392545046DB597

The processes and implementation of this secure hash algorithm are highlighted here.

1: Takes input text and splits it into an array of the characters' ASCII codes.
2: Converts ASCII codes to binary.
3: Pad zeros to the front of each bit until they are 8 bits long.
4: Join them together and append them to one (1).
5: Pad the binary message with zeros until its length is 512 mod 448.
6: Take binary 8-bit ASCII code array from step 3 and get its length in binary.
7: Pad with zeros until it is 64 characters.
8: Append to your previously created binary message from step 5.
9: Break the message into an array of chunks of 512 characters.
10: Break each chunk into subarray of sixteen 32-bit words.
11: Loop through each chunk array of sixteen 32-bit words and extend each array to 80 words using bitwise operations.
12: Initialize some variables.
13: Looping through each chunk: bitwise operations and variable reassignment.
14: Convert each of the five resulting variables to hexadecimal.
15: Append them together and the result is your hash value or message digest.

3.3. Crypto Hash Computation (SHA-1)

In this type of cryptography hash computation, the modular exponentiation techniques were used [35,36]. This technique (modular exponentiation) computes the remainder of an integer base (b) exponent (e) of nth power, which is divided by a positive integer of modulus (m) as expressed in Equation (3). The crypto hash techniques perform computation randomly in an efficient computable deterministic as given in Equation (4). A given message of "Cryptotrack", with a minor alteration made during transaction to "cryptotrack". The proposed secure algorithm will completely generate an output different as expressed here, and the exchange key architecture of crypto hash function is depicted in Figure 7.

[SHA-1] ("Cryptotrack") denotes 6BD736F1C2DC0B566812B92B7C47EBA39BCD5222
SHA-1("cryptotrack") means 5AA13558D0CCA00C53EDD39427392545046DB597

$$F(x) = Y \tag{3}$$

$$c = b^x \; mod \; p \tag{4}$$

where, F is SHA-1 function, x is transaction or message and Y is the output generated, c is the public key, b is the key generator, x is the private key parties (i or j, or ij), and p is the prime number. From the SHA-1 network, A, B, C, D, and E are 32 bits length; F is a nonlinear iteration function that varies when interchanged; W_t is the message word expanded for round t; K_t is the constant round of t, $\boxplus$ representing an (xor) additional modulo 2^{32}; and $<<<_n$ represents the left bit rotation by numbers of (n). The collision resistance is used during hashing of two different messages to achieve the same value and to prevent a brute force attack as given in Equation (5), and the first iterative function of the message block is expressed in Equation (6).

$$H\{m_1\} = H\{m_2\} \tag{5}$$

$$M_{t+1} = H_{t+1} = h(H_t, \; M_{t+1}) \tag{6}$$

$$H_{t+1} = E(H_t, \; M_{t+1}) \boxplus H_t \tag{7}$$

The expansion of the message block M_t is split into 32 bits of 16 words $\{W_0, W_1, W_2, \ldots, W_{15}\}$ as expressed in Equation (8), the transformation of message input is divided into 32 bits of five words (A_0, B_0, C_0, D_0, and E_0) as given in Equation (9), and the feed forward of input key message M_{t+1} is the sums modulo of 2^{32} that are concatenated to form the variable chaining H_{t+1} as expressed in Equation (10). The copies of each shift rotated message are given in Equation (10).

$$W_i = (W_{i-16} \oplus W_{i-14} \oplus W_{i-8} \oplus W_{i-3}) \lll 1 for\ 16 \le i \le 79 \tag{8}$$

$$Step_{i+1} := \left\{ \begin{array}{c} A_{i+1} = (A_i \ll 5) + f_i(B_i, C_i, D_i) + E_i + K_i + W_i, \\ B_{i+1} = A_i, \\ C_{i+1} = B_i \gg 2, \\ D_{i+1} = C_i, \\ E_{i+1} = D_i. \end{array} \right\} \tag{9}$$

$$H_{t+i} = (A_0 + A_{80}),\ (B_0 + B_{80}),\ (C_0 + C_{80}), (D_0 + D_{80}), (E_0 + E_{80}) \tag{10}$$

$$A_{i+1} = (A_1 \ll + f_i(A_{i-1},\ A_{i-2} \gg 2, A_{i-3} \gg 2) + A_{i-4} \gg 2 + K_i + W_i \tag{11}$$

where, E is the block cipher, H_t is the input message, M_{t+1} is the input key, and K_i is the predetermined constant.

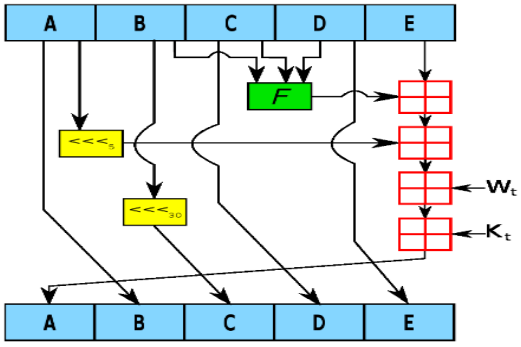


Figure 7. Hash function security key exchange and computation [37].

However, the user authentication nodes permit a user to register instead of storing the passwords as plain text, and subject it through a one-way hash function before being stored in a database, which will be used for the user authentication login password. The user authentication procedure is depicted in Figure 8.

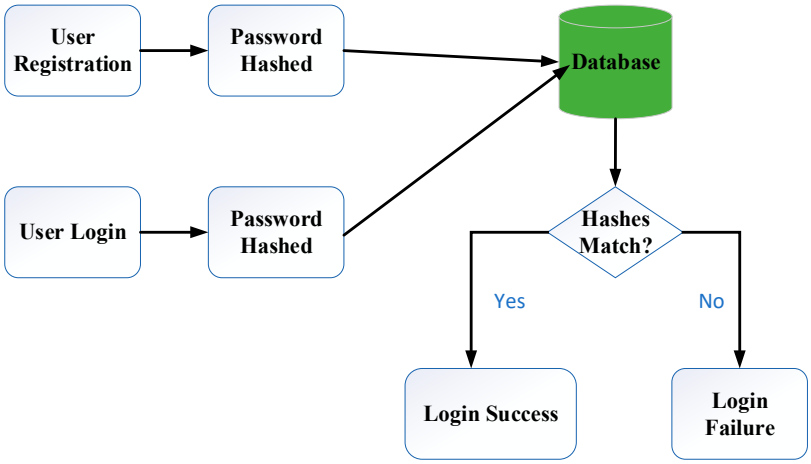


Figure 8. User authentication architecture.

3.4. Mining Algorithm and Pseudocode-Based Blockchain

Mining in the framework of blockchain technology is the process of combining new transactions to the public decentralized ledger database of the previous or existing transactions in the blockchain for recording and validation. This process in the chain is important to set the history of transaction for the mathematical computation (hashing), so that it can achieve an immutable, tamper-resistant consensus and secure any single node participant or third-party in the network. Therefore, the mining algorithm refers to the hashing or cryptographic hash-function that is used for authentication or digital signature in the chain mechanism. This algorithm is used to map arbitrary data size into an equivalent fixed size of hash. The pseudocode, flowchart, and architecture for the mining algorithm are depicted in Figures 9 and 10.

From the process of this mining algorithm, if anyone else is added to the transaction list in the chain from step 1 it will change the random number generated, and there is a tendency for the selection criterion to be met in another round as shown in Figure 11.

```
P := The hash of the previously mined block
B := A block of transactions
H := A hash function
D := Difficulty Level

0 Retreive P
1 Construct/Modify B
2 IF H(P, B, Some Random Number) > D END
3 GOTO 1
```

Figure 9. Pseudocode for the mining algorithm.

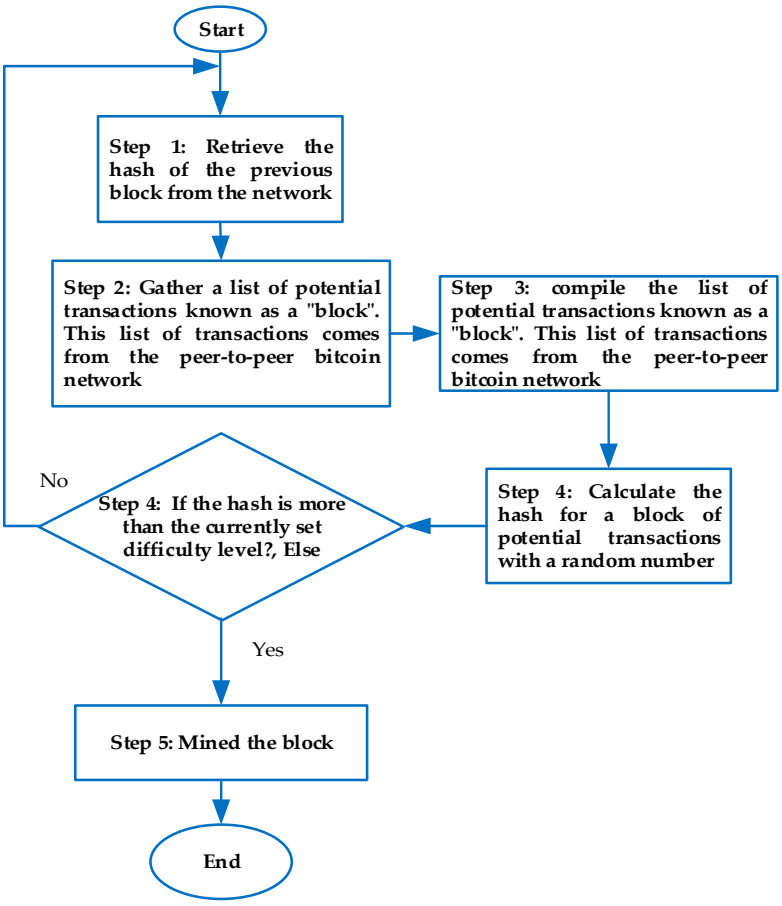


Figure 10. Mining algorithm flow diagram.

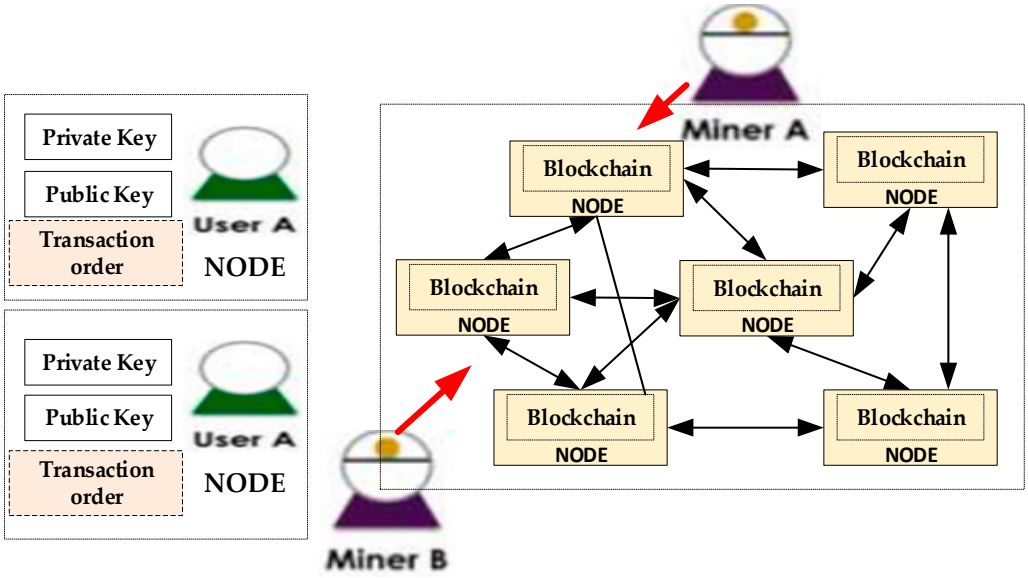


Figure 11. Mining algorithm architecture.

3.5. Cryptographic Algorithm for Key Management in Blockchain Technology

The blockchain protocol is assigning to a single-message (transaction) as an interactive for the establishment of key creation/generation, signing message for randomness of key and verification of public key as illustrated in Figure 12. The algorithm for signature is computed here using digital signature standard (DSS) technique based on SHA-1 [38–40]. The approach for digital signature creation and verification is depicted in Figure 13, the algorithm is outlined, and computation for the key is expressed in Equations (12) and (13).

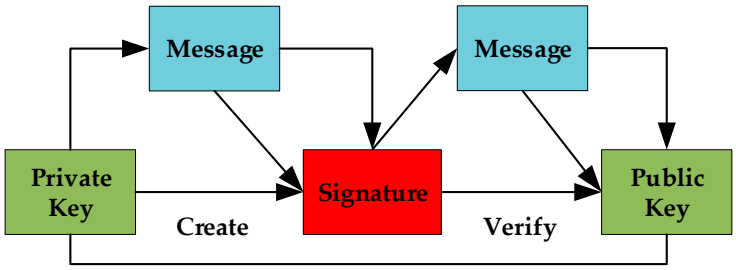
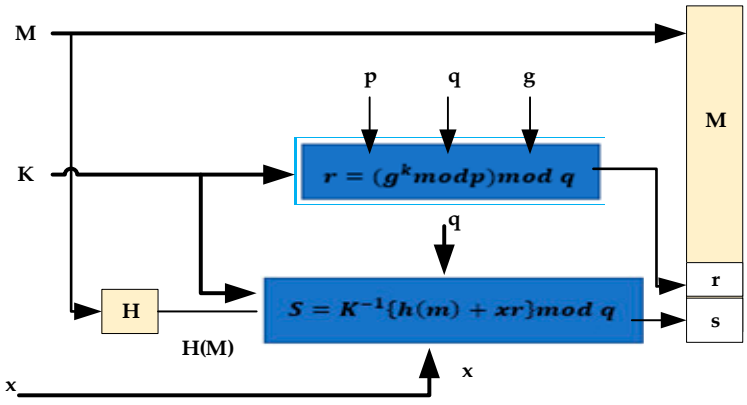
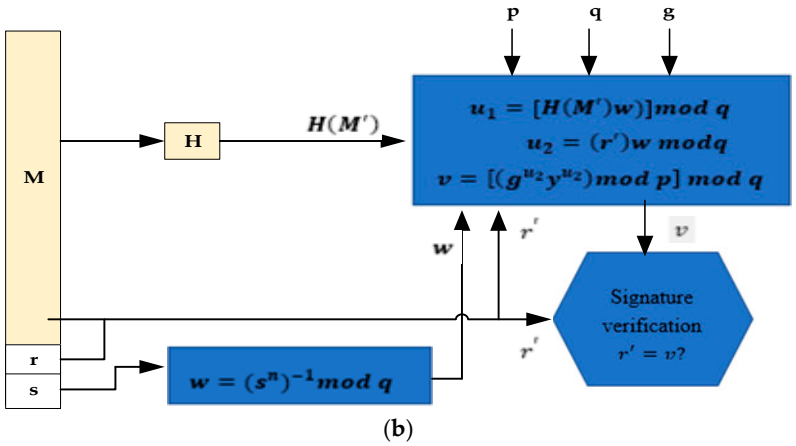


Figure 12. Signature creation and verification.



(**a**)

Figure 13. *Cont.*



(**b**)

Figure 13. (**a**) Verification public; (**b**) Signing message.

1. Key generation procedure/Algorithm

Step 1. **Signing message**

i. Start with shared the global public key values (p, q, g)

ii. Select about 160-bit prime number (q)

iii. Select a large prime number (p) with 2^ (L-1) < p < 2^l, where L will be equal to 512 to 1024 bits and is a multiple of 64 such that q is a 160-bit prime divisor of p-1

iv. Select h, then find g=h^((p-1)/q) mod p, where 1<h<p-1 and h^((p-1)/q) mod p>1

Step 2. Select a private key and compute the public keys

i. Select a random private key such that: x < q

ii. Compute the public key such that: $y = g^x mod p$

2. Creation of Signature

Step1. Signing of a message M, the sender:

i. Creates a random signature key (k), such that k < q

ii. Creation of k must be random, one-time password (OTP) and destroyed after used

Step 2 Computation of signature pair

i. $r = \left(g^k mod\ p\right) mod\ q$

ii. $s = \left[k^{-1}(H(M) + xr)\right] mod\ q$

iii. The signature (r, s) and message M (Transaction) will be send

3. Verification of Signature

i. While receiving message (M) with signature (r, s)

Then, to verify a recipient transaction signature, use the following computation.

$w = s^{-1} mod\ q = k(H(m) + xr)^{-1} mod\ q$

ii. $u1 = [H(M)w] mod\ q$

$u2 = (rw) mod\ q$

$v = \left[\left(g^{u1} y^{u2}\right) mod\ p\right] mod\ q$

iii. If v = r, then transaction signature is confirmed

End the process.

$$S = K^{-1}\{h(m) + xr\} mod\ q \tag{12}$$

$$Z_p = \{1,\ 2,\ \ldots, p-1\} \tag{13}$$

where,

p	is prime number where $2^{L-1} < p < 2^{L}$, for 512 $\leq L \leq 1024$ and L a multiple of 64 , i.e., ., a bit length between 512 and 1024 bits in increments of 64 bits
q	prime divisor of $(p-1)$, where $2^{159} < q < 2^{160}$i.e .... a bit length of 160 bits
s	$h^{(p-1)/q} \bmod p$, where h is any integer with $1 < h < (p-1)$, such that $h^{(p-1)/q} \bmod p > 1$
x	random or pseudorandom integer with $0 < x < q$ used as a ***private key***
y	is given as $g^{x} \bmod p$ used as ***public key***
k	used to generate random or pseudo – random integer with $0 < k <$ q per message sec ret number
r, s	is the **signature for *signing,*** where $r = \left(g^{k} \bmod p\right) \bmod q$, and $\mathbf{s} = [k^{-1}(H(M) + xr)] \bmod q$
v, r	v = r is the ***verification***, $w = (s^{-})^{-1} \bmod q$ $u_1 = [H(M')w] \bmod q$ $u_2 = \left(\mathbf{r}'\right) w \bmod q$ $v = \left[\left(g^{u1} y^{u2}\right) \bmod p\right] \bmod q$
M	Message to be signed
H(M)	Hash of M using SHA-1
M′, r, s′	the received varieties or copy of M, r, s.

3.6. Implementation of (Telematics) an In-Vehicle Tracking System Prototype

The telematics system was developed and programmed in Arduino integrated development environment (IDE) for monitoring the petroleum volume of automobiles using some hardware components. The telematics method is shown in Figure 14. The automobile tracking system prototype was designed and integrated into the oil and gas tankers for monitoring and tracking the geolocation of automobiles. The hardware system consists of GPS, which is capable of transmitting and receiving remote information through satellite and compute the geographic position (longitude, latitude and altitude) for the location-dependent. The ultrasonic sensor (HC-SR04, is a distance measuring sensor that capable of providing 2 cm–400 cm measurement with accuracy of about 3mm ranging. The transmitter, receiver and control circuit are embedded with four pins connection namely are power (VCC), trigger (Trig), Receive (Echo) and ground (GND). It is manufactured by Hc Sr04 company in China. (Arduino Uno development board (ATmega 328P, it is an 8-bit reduced instructional set computer manufactured by the Microchip in Padova, Italy) for system activities control and coordination. A lithium battery of 9v is used for the system power using DC–DC converter.

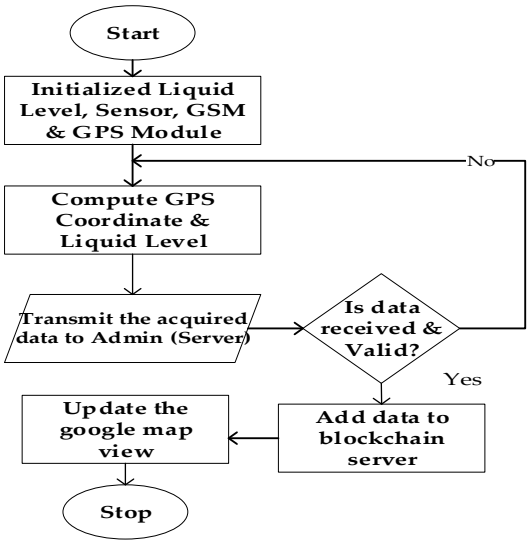


Figure 14. Hardware system flow diagram.

The HC-SR04 ultrasonic sensor has two phases for the signal transmit (Tx) and receiver (Rx), which both cover a distance of 4 m. Each phase of the sensor uses the distance between itself and the petroleum product surface to calculate the liquid level in a tank as expressed in Equation (14).

$$Distance\ (\mathrm{d}) = \frac{Speed\ of\ sound\ (\mathrm{u}) \ * \ time\ delay\ (t)}{2} \tag{14}$$

The time of flight of the HC-SR04 sensor between the levels of the liquid to the receiver is computed as 2dx. Therefore, the speed (u) of the wave is expressed as in Equation (15), where changes in distance (dx) of the liquid level are calculated in Equations (16) and (17).

$$\mathrm{u} = \frac{2\mathrm{d}x}{\mathrm{d}t} \tag{15}$$

$$\mathrm{d}x = \frac{\mathrm{u}\mathrm{d}t}{2} \tag{16}$$

$$\int \mathrm{d}x = \frac{\mathrm{u}}{2} \int \mathrm{d}t \tag{17}$$

The speed (u) of sound in air is ~340 m/s, the instantaneous distance (dx) between the liquid level and sensor with respect to time of flight (t) is calculated as in Equation (16), the maximum height of tank is H and the volume of the liquid in the tank is v, which are expressed as in Equations (18)–(20), where k is a constant of proportionality.

$$x = \frac{340ms^{-1} \times \mathrm{d}t}{2} = 170m/s \tag{18}$$

$$\mathrm{d}l = \mathrm{h} - \mathrm{d}\mathrm{x} \tag{19}$$

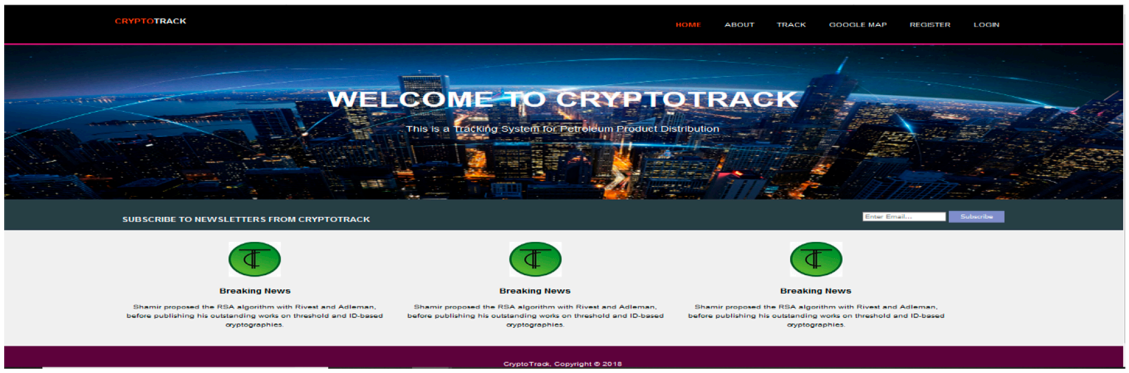
$$\upsilon = \mathrm{k}\mathrm{d}\mathrm{l} \tag{20}$$

4. Results and Discussion

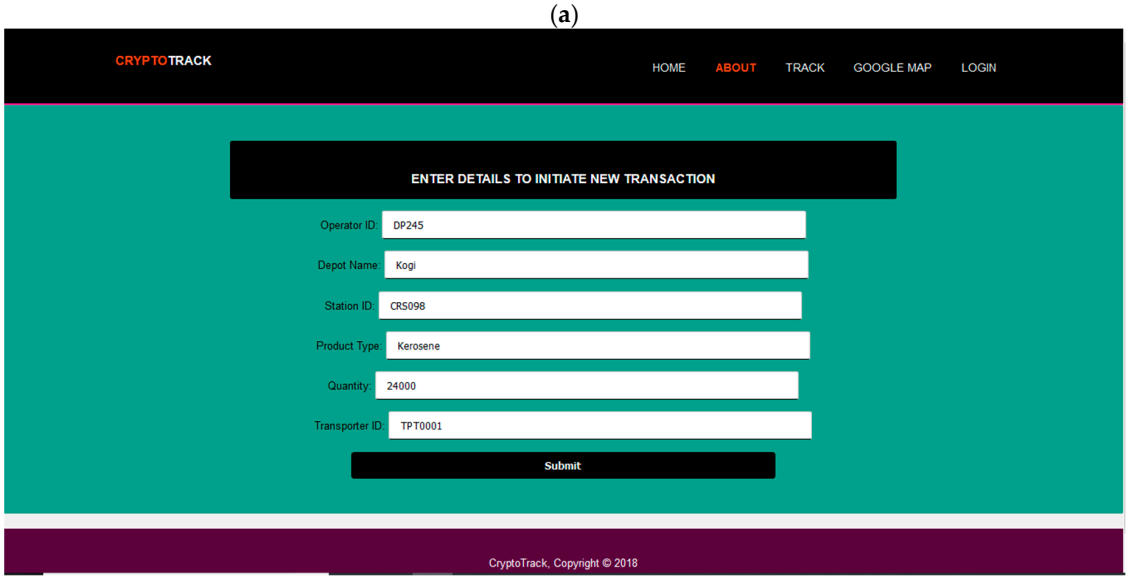
4.1. Development of Crypto Hash Decentralized Ledger

This section illustrates the implementation of the developed crypto hash decentralized ledger for managing the transaction of petroleum products distribution. The crypto-system was design for managing transactions data that occur in oil and gas distribution depot and the data received information from the tanker fleet while in transit to the destination is remotely transferred to the secure database and updated immediately. Table 2 contains detailed analysis of tracking information sent to the secure database during testing and some other related data.

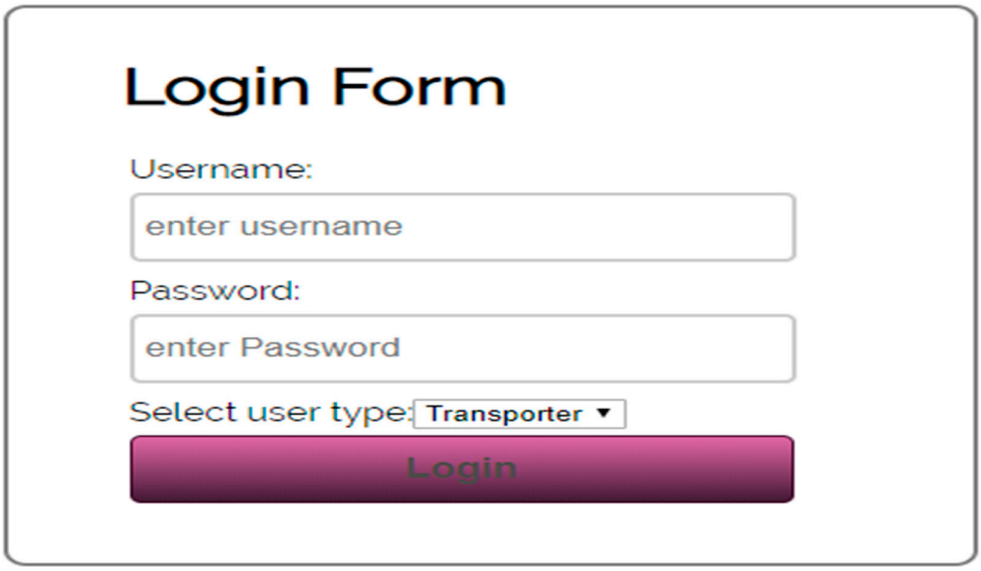
Figure 15 illustrates the results of the developed secure blockchain database for oil and gas distributions: (a) Homepage GUI, it is a login interface for transaction registration. (b) Users registration page, this is the registration page that contained general information concerning third-party in the transaction. (c) First layer login interface, this is a login form for the transporter. (d) Admin section for user confirmation, this contains details information about new transaction and authentication. (e) Admin section for managing transporter geolocation, this stored a remote tracking information about the transaction for admin monitoring in a real-time. (f) GUI for new transaction details, this page stored all the transaction records details include crypto-hash code.



(**a**)

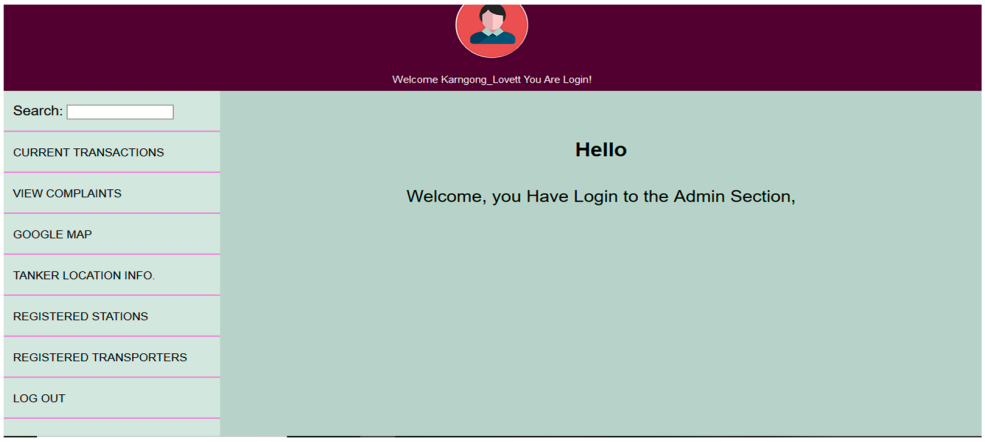


(**b**)

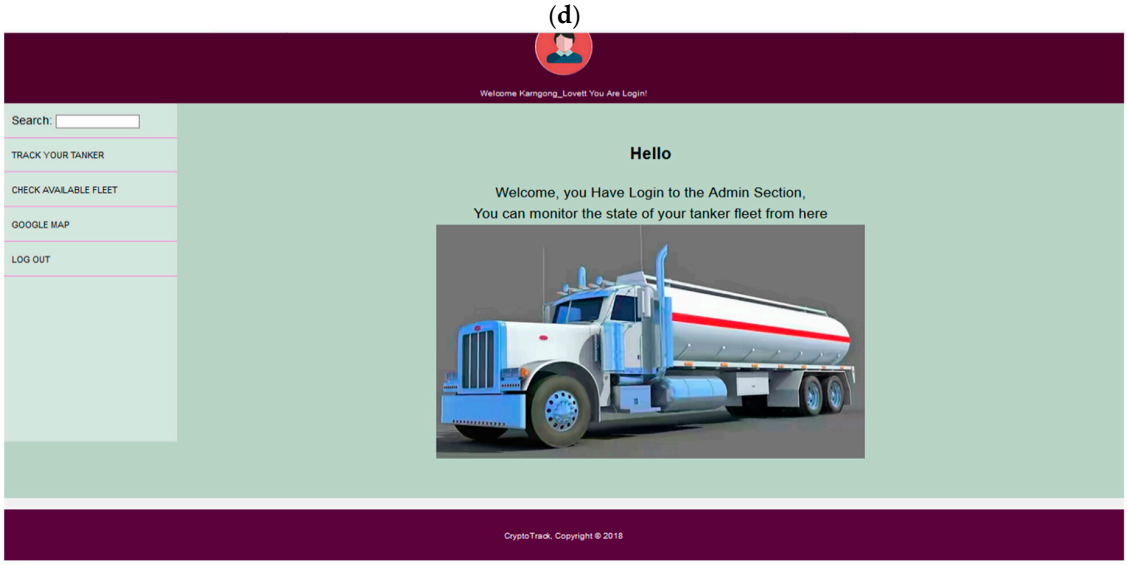


(**c**)

Figure 15. *Cont.*



(**d**)



(**e**)

TRANSACTION ID	OPERATOR ID	DEPOT	STATION ID	PRODUCT TYPE	QUANTITY	TRANSPORTER ID	DATE	TIME	HASH
8	OPT34	Kogi	ABJ0007	Petroleum	44000	TPT0004	25-09-2018	11:45:57am	f0bb8c34c72f13a5b723aeabddfdc720f6cfd970
9	OPT34	Minna Depot	TRB0002	Motor Oil	24000	TPT0056	25-09-2018	11:45:57am	fab17df2fe7535550284b7d6c114d02785f15c04
10	OPT34	Yenagoa	ABJ0007	Kerosene	24000	TPT089	25-09-2018	12:40:34pm	0dc1dba8635696354b80378a2f90ba91e4a9628c
11	OPT07	Minna Depot	ABJ0007	Diesel Fuel	24000	TPT1000	25-09-2018	12:41:41pm	b951c300b30b17f3379e7d55194d1ad20d0f5121
12	OPT07	Minna Depot	NCS0002	Asphailt	24000	TPT089	26-09-2018	01:55:33am	74de5ffd55d4ca8e1a5a3f735cad72b91bf281d7
13	OPT07	Kogi	CRS098	Asphalt	24000	TPT0001	2-10-2018	03:03:13am	65518675d31d8e9d95dbd0a58a55b048a7dc3098
14	DP199	Bauchi Depot	ST098		30000	TPT2000	3-10-2018	07:52:53am	4f81c10c60bc2cfe44bdd02f13c7a9fa532f98ab

(**f**)

Figure 15. Crypto-track blockchain database login interface and detail transaction records. (**a**) Homepage GUI; (**b**) Users registration page; (**c**) First layer login interface; (**d**) Admin section for user confirmation; (**e**) Admin section for managing transporter geolocation; (**f**) GUI for new transaction details.

Table 2. Detailed analysis of tracking information sent to the secure database during testing.

Id	Tanker_ID	Time	Date	Satellite Number	HDOP	Liquid Level	Speed	Latitude	Longitude
1	865210031078669	06:15:44	08/10/2018	5	2.19	66	0.35	9.531407	6.451446
2	865210031078669	06:16:17	08/10/2018	6	1.92	89	0.37	9.531438	6.451479
3	865210031078669	06:16:50	08/10/2018	5	1.98	89	0.59	9.531368	6.451441
4	865210031078669	06:17:23	08/10/2018	6	2.03	89	0.44	9.531471	6.451372
5	865210031078669	06:17:56	08/10/2018	5	1.6	97	1.19	9.531489	6.451346
6	865210031078669	07:55:25	08/10/2018	5	2.56	100	1.2	9.530928	6.451571
7	865210031078669	07:55:58	08/10/2018	4	9.51	100	1.81	9.531051	6.451568
8	865210031078669	07:56:32	08/10/2018	5	2.5	100	1.04	9.530858	6.451453
9	865210031078669	07:57:05	08/10/2018	8	2.5	100	1.5	9.530884	6.45146
10	865210031078669	07:57:38	08/10/2018	6	4.99	100	1.98	9.531068	6.451518
11	865210031078669	07:58:11	08/10/2018	5	4.94	100	2.85	9.530917	6.451497
12	865210031078669	07:58:44	08/10/2018	6	2.48	100	1.87	9.530988	6.45146
13	865210031078669	18:20:29	08/10/2018	9	0.81	48	0.2	9.531387	6.451231
14	865210031078669	18:21:02	08/10/2018	9	0.88	0	0.15	9.531398	6.451261
15	865210031078669	18:21:35	08/10/2018	10	0.82	0	1.11	9.53142	6.451247
16	865210031078669	18:22:08	08/10/2018	10	0.78	0	0.2	9.531483	6.451261
17	865210031078669	18:22:41	08/10/2018	9	0.87	0	0.74	9.531522	6.451264
18	865210031078669	18:23:14	08/10/2018	10	0.87	0	2.63	9.531484	6.451257
19	865210031078669	18:23:47	08/10/2018	10	0.98	0	2.57	9.531505	6.451173
20	865210031078669	18:24:20	08/10/2018	10	0.78	0	0.44	9.531486	6.451322
21	865210031078669	18:24:53	08/10/2018	9	0.85	0	0.61	9.531514	6.451376
22	865210031078669	18:25:26	08/10/2018	9	0.85	0	0.61	9.531542	6.451425
23	865210031078669	18:25:59	08/10/2018	5	1.82	0	14.26	9.531661	6.451532
24	865210031078669	18:26:32	08/10/2018	7	2.88	0	8.72	9.531518	6.451762
25	865210031078669	18:27:06	08/10/2018	0	99.99	0	14.93	9.531453	6.452001
26	865210031078669	18:27:40	08/10/2018	9	1.01	0	4.63	9.531857	6.451674
27	865210031078669	18:28:13	08/10/2018	8	0.9	0	0.24	9.531544	6.451401
28	865210031078669	00:37:47	09/12/2018	9	0.98	0	0.74	9.531361	6.451714
29	865210031078669	00:38:34	09/12/2018	9	0.85	0	0.11	9.531422	6.451569
30	865210031078669	00:39:21	09/12/2018	9	0.88	0	0.06	9.531407	6.451598
31	865210031078669	00:40:08	09/12/2018	9	0.8	0	0.33	9.53139	6.451566
32	865210031078669	00:40:55	09/12/2018	11	0.76	0	0.17	9.531413	6.451585
33	865210031078669	00:41:42	09/12/2018	9	0.99	0	0.48	9.531431	6.45158
34	865210031078669	00:42:29	09/12/2018	10	0.88	0	1	9.531427	6.4516
35	865210031078669	00:43:16	09/12/2018	10	0.92	0	0.63	9.531411	6.45163
36	865210031078669	00:44:03	09/12/2018	9	0.92	0	1.98	9.531393	6.451665

4.2. Encryption and Decryption Algorithm Testing and Results Using WAVE

A Waveform Audio File Format (WAVE) is an application of Resource Interchange File Format (RIFF) that stores audio bit streams of signal in "chunks". This application (WAVE) encodes the sound in Linear Pulse Code Modulation (LPCM). To test for the encryption and decryption processes of the proposed secure hash algorithm-based blockchain technology in the WAVE bitstream format is depicted in Figure 16. The application interface program was developed using C-Sharp, which is capable of converting the data stream into the audio signal wave and performing the encryption and decryption algorithms. The stream of Waveform Audio File Format (WAVE) file was used to encrypt and decrypt the data. MATLAB software (2015a, The MathWorks, Inc., Natick, MA, USA) is used to perform matrix manipulation for the encryption and decryption of sound files into and from image files. This method is known as data compression technique. The novel method uses encryption and decryption in 'drum.wav', which is a sound file in image formats such as PNG, TIF, and JPEG. The

sound file is fetched and the values corresponding to the sample range are put in a column matrix, which is arranged in a two-dimensional matrix having "double" as the data type. The "imwrite" function of MATLAB is used and defined in the matrix class as double, which inserts a graphic file having a dynamic range from 0 to 1.

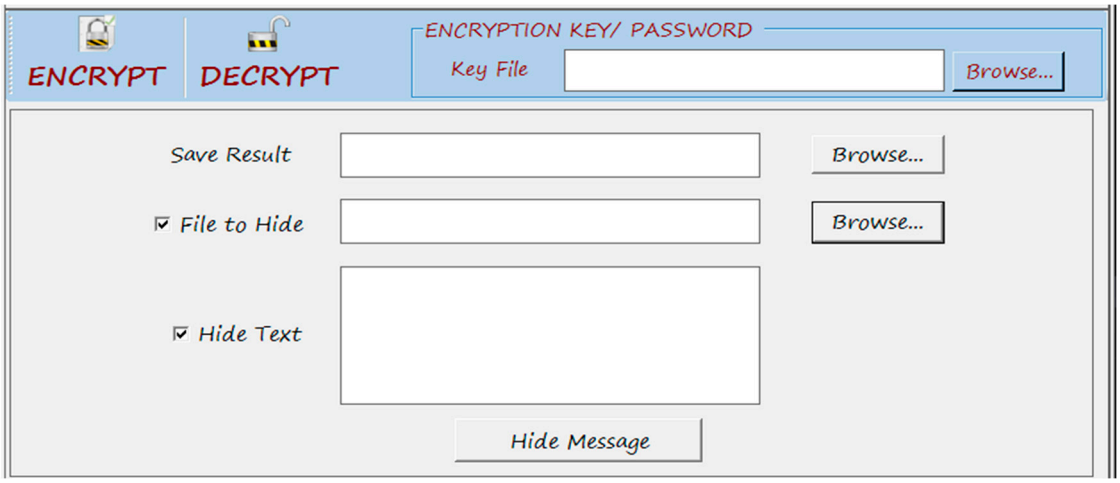


Figure 16. Graphic user interface of cryptography algorithm.

Encryption algorithm
Phase 1: Encryption of algorithm
Step 1: Generate the ASCII value of each plaintext.
Step 2: Sum the ASCII value of all character.
Step 3: Mod the value of 128 for the total number of keys consider as ASCII value.
Step 4: Corresponding ASCII value is considered as a key.
Step 5: Apply this expression in Equations (8) and (9) to generate cipher text.
where, E is encryption, P is plaintext and K is key.

$$K = (C_1 + C_2 + \ldots\ C_n)\%256 \tag{21}$$

$$E = ((P + K)\%256) \tag{22}$$

Step 6: The cipher text value is used to perform the transposition.
Phase 2: Encryption of auto key
Step 7: Use the cipher text value of the substitution method as input of the auto text key
Step 8: Here we considered key value as 3.
Step 9: Perform Auto text key to generate the final cipher text.
Decryption algorithm
Decryption of wave cipher
Step 1: Perform Rail Fence Cipher decryption process using the key value of 3.
Step 2: Generate .wav cipher text by substitution.
Step 3: Perform step2 as input value of the .wav cipher method.
Step 4: Here the same encryption key used.
Step 5: Use this expression in Equation (10)

$$D = ((P - K)\%256) \tag{23}$$

Step 6: Generate the ASCII character of the corresponding decimal value as your original text

It is interesting to note that the purpose of encryption is to distort the original signal as illustrated from the behavior of the graph, where more noise is introduced to the system. The result of the

(plaintext)t stream character is converted into a .wav audio signal as shown in Figure 17, and for hashing, a noise signal was introduced, which is added to the original plaintext as depicted in Figure 18. After encryption algorithm, the data is retrieved from the image file and compared with the original wave file to show the variation in encrypted string character as shown in Figure 19.

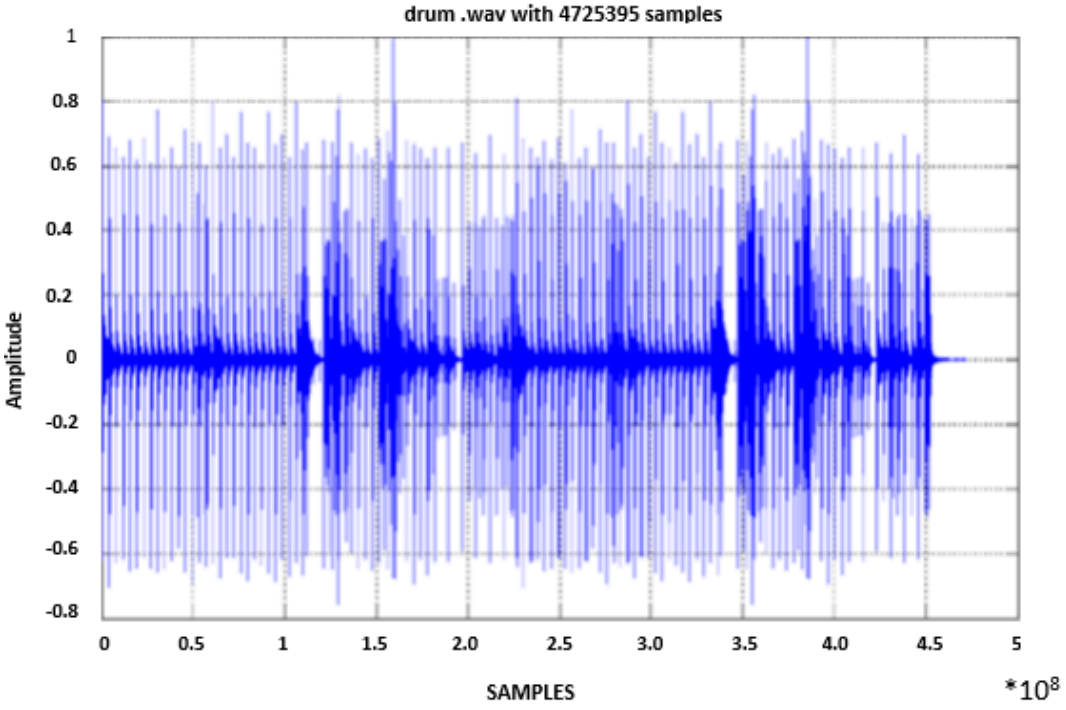


Figure 17. Encipher .wav audio signal.

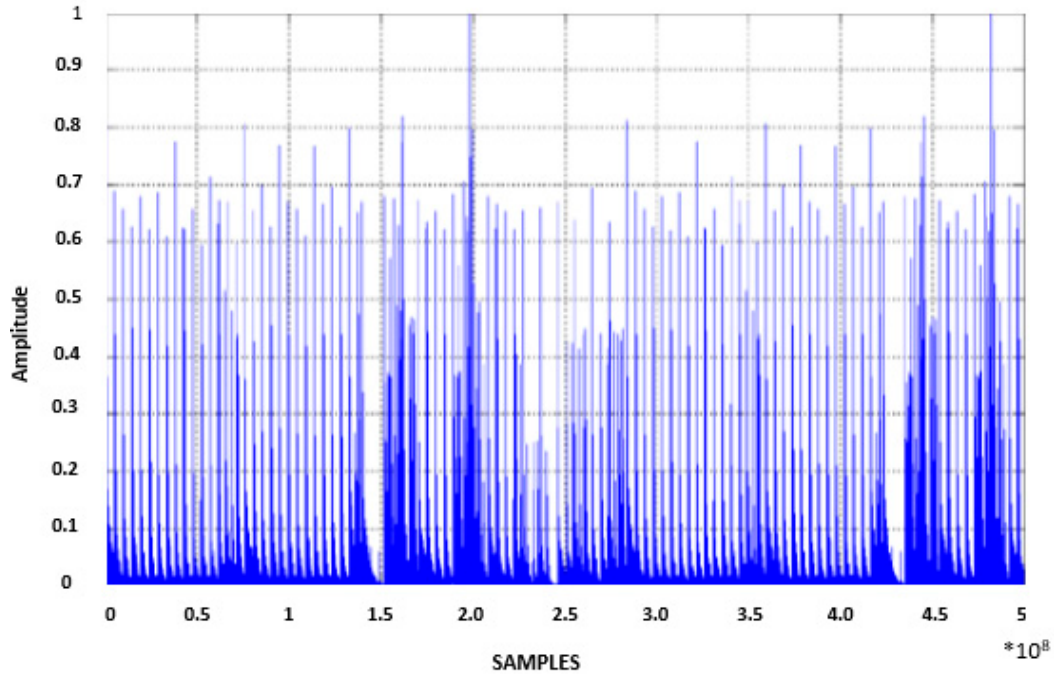


Figure 18. Noise audio signal generation for encoding (salt).

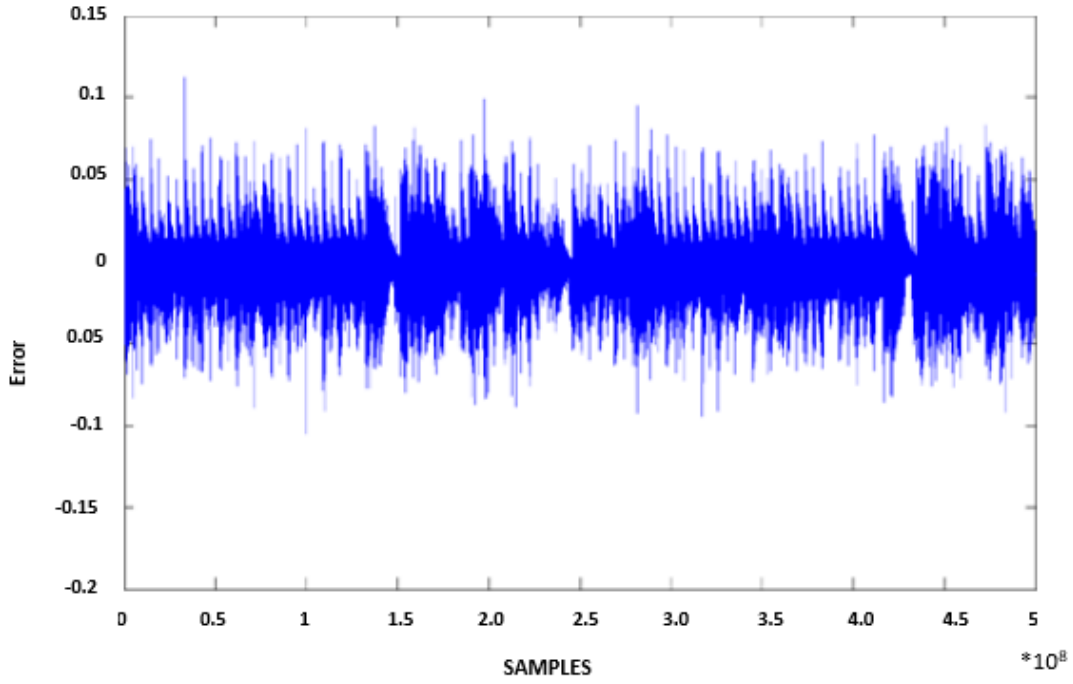


Figure 19. Encryption .wav audio generation signal.

4.3. *Testing and Results of Implemented Automobile Based Telematics*

The automobile tracking system-based telematics approach for the petroleum distribution is developed, implemented, and tested within the Federal University of Technology, Minna. This system is configured and connected logically with the secure hash blockchain database for remote information storage. The Google Maps result of the telematics-based automobile tracking system is illustrated in Figure 20, and the results of automobile geolocation tracking based on the longitude and latitude are evaluated by comparing the actual geolocation results with the GPS-based telematics device presented in Table 3.

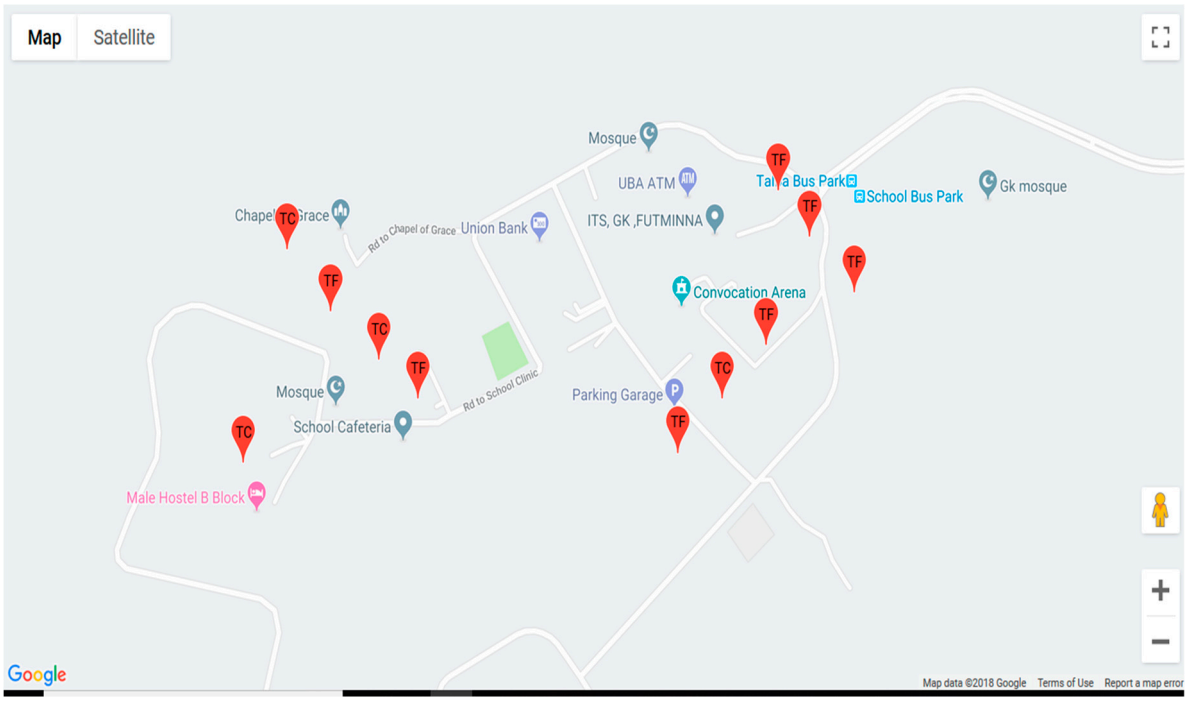


Figure 20. Google Maps geolocation tracking.

Table 3. Performance evaluation of geolocation tracking in FUTMinna.

Actual Coordinate Values			GPS Coordinate Values		
Location (Address)	**Latitudinal Coordinate**	**Longitudinal Coordinate**	**Latitudinal Coordinate**	**Longitudinal Coordinate**	**No of Satellite Captured**
ICT Complex	6.451576	9.531347	6.451829	9.531222	4
Engineering Complex	6.449162	9.533510	6.449241	9.533539	8
E-exam Center	6.449688	9.536088	6.449667	9.536154	9
ITS Center	6.452325	9.535278	6.452507	9.535301	5
Agric Complex	6.451862	9.533240	6.451966	9.533134	7
Senate Building	6.452790	9.534655	6.452748	9.52748	6

4.4. Performance Evaluation Testing of the Crypto Hash System

The crypto hash database system was developed and performance evaluation was carried out in the Mozilla web developer tool. The system performance metrics was evaluated base on the speed of the web application developed which includes file type, size, time, and the transfer speed as illustrated in Figure 21. The file transmission rate is a function of the type of file being transferred in the system, which generates the result given of the primed and empty cache. The empty cache scenario occurs when the browser makes the first request to the page using a HTTP request, and the Primed cache instance is when the browser has a cached version of the page. In a Primed Cache instance, the components are already in the cache, thereby decreasing the number of HTTP requests and the weight of the page. The data files considered in this platform are CSS, HTML, JS, XHR HTTP Request, and images.

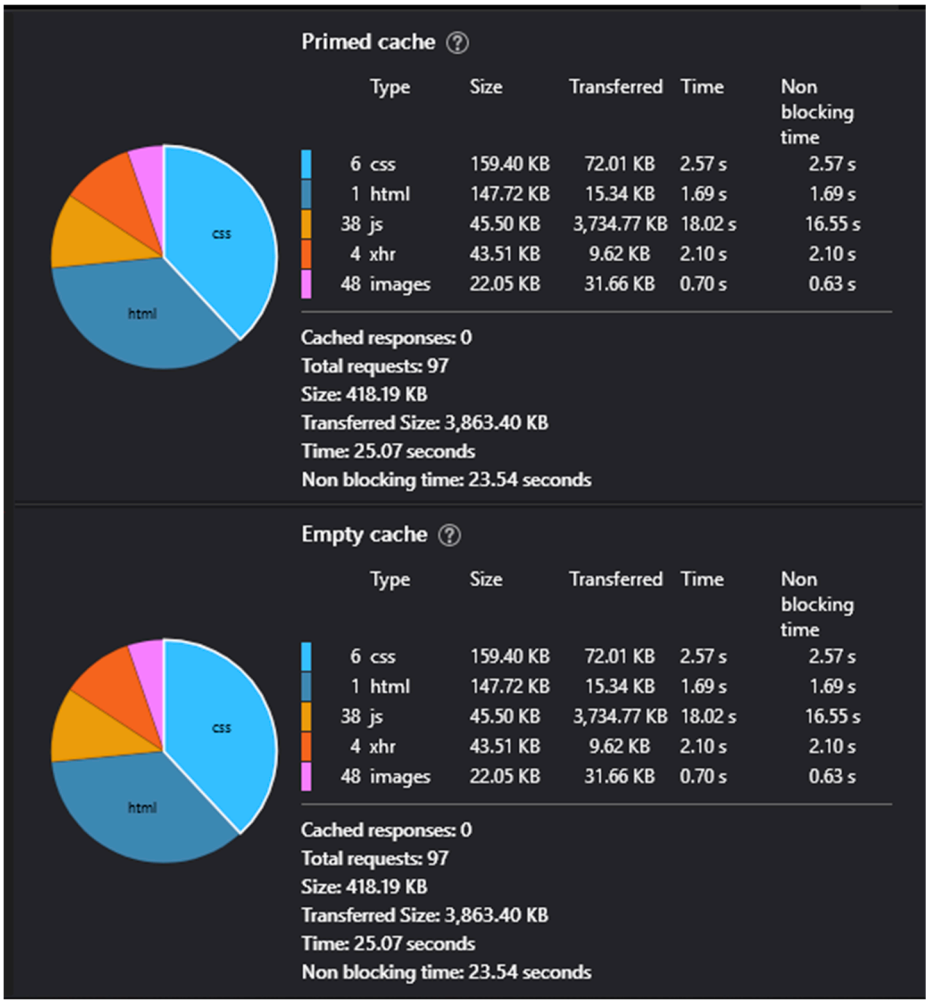


Figure 21. Performance evaluation results of both backend and frontend system.

5. Conclusions

This research work presents a novel secured decentralized ledger in a database that manages petroleum product distribution records using a secure hash algorithm-based blockchain. Also, a telematics approach for the geolocation tracking and monitoring of petroleum volume level was proposed, which is connected to the remote database and updated with real-time information dynamically. The implementation of this permissioned blockchain technique using SHA-1 computation techniques ensures hashing of every transaction generated based on the previous transaction and has proven efficiency, since it is not vulnerable to individual tampering of the record, but it gives access to any changes or updates when participants in the chain have over 75% agreement; otherwise permission is denied. The details of this transaction are stored on the distributed ledger where every participant in the chain can access the data or information transparently and provide security with immune to tampering. Further research can be focused on securing military information, banking systems, and ballot voting systems (BVS) using decentralized distributed ledger and crypto hashing blockchain technology for data management and unified security. Also, the future work will consider the analysis based on the quality of oil and gas product information acquired from molecular markers (fuel marker program).

Author Contributions: Investigation, L.A.A.; Methodology, L.A.A., J.A., and L.K.; Software, L.A.A. and L.K.; Supervision, J.A. and E.A.A.; Writing—original draft, L.A.A. and L.K.; Writing—review & editing, L.A.A., J.A., and E.A.A.

Funding: This research received no external funding.

Acknowledgments: The authors are grateful to the management of Federal University of Technology Minna Nigeria, School of Engineering, and Engineering Technology, Department of Computer Engineering, for their technical and financial support.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Nwoba, O.E.; Abah, E.O. Impact of crude oil revenue (cor) on economic growth in nigeria (1960–2010). *IOSR J. Hum. Soc. Sci.* **2017**, *22*, 85–99.
2. Özturkoglu, Ö.; Lawal, O. The integrated network model of pipeline, sea and road distribution of petroleum product. *Int. J. Optim. Control Theor. Appl.* **2016**, *6*, 151–165. [CrossRef]
3. Aminu, S.A.; Olawore, O.P. Empirical investigation of challenges of distribution of premium motor spirit (PMS) in federal capital territory (Fct), abuja and environs, Nigeria. *Int. J. Manag. Sci. Humanit.* **2014**, *2*, 17–59.
4. Ajao, L.A.; Adedokun, E.A.; Nwishieyi, C.P.; Adegboye, M.A.; Agajo, J.; Kolo, J.G. An anti-theft oil pipeline vandalism detection. *Int. J. Eng. Sci. Appl.* **2018**, *2*, 41–46.
5. Adegboye, M.A.; Fung, W.-K.; Karnik, A. Recent advances in pipeline monitoring and oil leakage detection technologies: principles and approaches. *Sensors* **2019**, *19*, 2548. [CrossRef] [PubMed]
6. Basu, S.; Waymire, G.B. Record-keeping and human evolution. *Account. Horiz.* **2006**, *20*, 201–229. [CrossRef]
7. Bacina, M.; Partner, P.; Alderman, P. The Era of Digital Trust. Available online: https://www.legaler.com/.../Blockchain-for-Lawyers-eBook.pdf (accessed on 10 December 2018).
8. Diego, R.; Giovanni, S. Beyond bitcoin: A critical look at blockchain-based systems. *Cryptography* **2017**, *1*, 15.
9. Lavanya, B.M. Blockchain technology beyond bitcoin: An overview. *Int. J. Comput. Sci. Mob. Appl.* **2018**, *6*, 76–80.
10. Ajao, L.A.; Agajo, J.; Olaniyi, O.M.; Jibril, I.Z.; Sebiotimo, A.E. A Secure Tracking Automobile System for Oil and Gas Distribution using Telematics and Blockchain Techniques. *J. Electr. Comput. Eng. Innov.* **2019**, *7*, 171–177.
11. Marr, B. *A Very Brief History of Blockchain Technology Everyone Should Read*; Forbes: New York, NY, USA, 2018.
12. Vestergaard, C. Better than a floppy the potential of distributed ledger technology for nuclear safeguards information management, innovative approaches to peace and security from the stanley foundation. *Anal. Brief.* **2018**, *1*, 1–8.

13. Hardjono, T.; Lipton, A.; Pentland, A. *Towards a Design Philosophy for Interoperable Blockchain System*; Springer: Berlin, Germany, 2018; pp. 1–27.
14. Derhab, A.; Guerroumi, M.; Maglaras, L.; Ferrag, M.A.; Mukherjee, M.; Khan, F.A. BLOSTER: Blockchain-based system for detection of fraudulent rules in software-defined networks. In Proceedings of the 6th International Symposium for ICS & SCADA Cyber Security Research 2019, Athens, Greece, 10–12 September 2019; pp. 1–3.
15. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Int. Things J.* **2019**, *6*, 2188–2204. [CrossRef]
16. Kogias, E.K.; Jovanovic, P.; Gailly, N.; Khoffi, L.; Gasser, L.; Ford, B. Enhancing bitcoin security and performance with strong consistency via collective signing. In Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, USA, 10–12 August 2016; pp. 279–296.
17. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2084–2123. [CrossRef]
18. Chima, C.M.; Hills, D. Supply-chain management issues in the oil and gas industry. *J. Bus. Econ. Res.* **2007**, *5*, 27–36. [CrossRef]
19. Kshetri, N. Can blockchain strengthen the internet of things. *IT Prof.* **2017**, *19*, 68–72. [CrossRef]
20. Ekblaw, A.; Azaria, A.; Halamka, J.D.; Lippman, A. A case study for blockchain in healthcare: Medrec prototype for electronic health records and medical research data. *Proc. IEEE Open Big Data Conf.* **2016**, *13*, 1–13.
21. Tian, F. An agri-food supply chain traceability system for China based on RFID & blockchain technology, In Service Systems and Service Management (ICSSSM). In Proceedings of the 13th IEEE International Conference, Kunming, China, 24–26 June 2016; pp. 1–6.
22. Micheal, C. What is Telematics, Geotab Inc., 2018. Available online: https://www.geotab.com/blog/what-is-telematics/ (accessed on 8 January 2018).
23. Handel, P.; Skog, I.; Wahlstrom, J.; Bonawiede, F.; Welch, R.; Ohlsson, J.; Ohlsson, M. Insurance telematics: Opportunities and challenges with the smartphone solution. *Int. Trans. Syst. Manag. IEEE* **2014**, *6*, 57–70. [CrossRef]
24. García, C.R.; Quesada-Arencibia, A.; Cristóbal, T.; Padrón, G.; Alayón, F. Systematic development of intelligent systems for public road transport. *Sensors* **2016**, *16*, 1104. [CrossRef]
25. Winter, A.; Baldi, S. Real-Life implementation of a GPS-Based path-following system for an autonomous vehicle. *Sensors* **2018**, *18*, 3940. [CrossRef]
26. Awan, M. Compensation of Low Performance Steering System Using Torque Vectoring. Ph.D. Thesis, Cranfield University, Bedfordshire, UK, 2012.
27. Isermann, R. Diagnosis methods for electronic controlled vehicles. *Veh. Syst. Dyn.* **2001**, *36*, 77–117. [CrossRef]
28. Jang, J.A.; Kim, H.S.; Cho, H.B. Smart roadside system for driver assistance and safety warnings: Framework and applications. *Sensors* **2011**, *11*, 7420–7436. [CrossRef]
29. Khatwani, S. Different Types of Blockchains in the Market and Why We Need Them. Available online: https://coinsutra.com/different-types-blockchains/ (accessed on 15 September 2018).
30. DataFlair Team, Blockchain Tutorial. 2018. Available online: https://data-flair.training/blogs/bitcoin-and-cryptocurrency-technologies (accessed on 14 September 2018).
31. Kumar, S.; Gupta, P. A comparative analysis of sha and MD5 algorithm. *Int. J. Comput. Sci. Inf. Technol.* **2014**, *5*, 4492–4495.
32. Gligoroski, D.; Markovski, S.; Knapskog, S.J. A secure hash algorithm with only 8 folded sha-1 steps. *Int. J. 194 Comput. Sci. Netw. Secur.* **2006**, *6*, 194–205.
33. Manuel, S. Classification and generation of disturbance vectors for collision attacks against SHA-1. *Des. Codes Cryptogr.* **2011**, *59*, 247–263. [CrossRef]
34. White, B.; Kreuz, T.; Simons, S. Midstream. In *Compression Machinery for Oil and Gas*; Klaus, B., Rainer, K., Eds.; Gulf Professional Publishing: Houston, TX, USA, 2019; pp. 387–400.
35. Adrian, A.; Cendana, M.; Dian, S.; Permana, H. Diffie-Hellman Key Exchange Modification using Blowfish Algorithm to Prevent Logjam Attack. *J. Telecommun. Electron. Comput. Eng.* **2018**, *10*, 1–7.

36. Oluwade, O.R.; Olaniyi, O.M.; Abdulsalam, Y.S.; Ajao, L.A. Entropy management technique in lightweight cryptographically secured smart home. In Proceedings of the 12th International Multi-Conference on ICT Applications (AICTTRA, 2018), Ile-Ife, Nigeria, 15 September 2018; pp. 258–265.
37. Hulsing, A. Digital signature schemes and the random oracle model. Technische Universiteit Eindhoven. Available online: https://www.win.tue.nl/applied_crypto/2016/20161115_ROM_Signatures.pdf (accessed on 23 September 2016).
38. Sene, I.; Ciss, A.A.; Niang, O. I2PA: An Efficient ABC for IoT. *Cryptography* **2019**, *3*, 16. [CrossRef]
39. Hülsing, A. Digital Signature Schemes and the Random Oracle Model. Available online: https://www.win.tue.nl/applied_crypto/2016/20161115_ROM_Signatures.pdf. (accessed on 23 September 2016).
40. Liu, J.K.; Baek, J.; Zhou, J.; Yang, Y.; Wong, J.W. Efficient online/offline identity-based signature for wireless sensor network. *Int. J. Inf. Secur.* **2010**, *9*, 287–296. [CrossRef]