International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7233
***Article Received**: 29 April 2023 **Revised:** 14 June 2023 **Accepted:** 28 June 2023*

Block Chain based Contribute Sequence Tracking System for Secure Data Ascription Management

Low Jin Poo[1], Xu Xiao qi[2]
[1]Graduate School of Management
Management and Science university
University Drive, Off Persiaran Olahraga, 40100 Shah Alam,
Selangor, Malaysia
[1]jasonlow22@gmail.com
[2]Student, School of Management
Universiti Sains Malaysia,Penang, Malaysia,11800
[2]xuxiaoqi@student.usm.my

Abstract: Block chain technique is developed from a distributed, dependable application development platform to an irreversible record of crypto currency transaction history. Block chain technology's emergence has sparked a number of possible changes in how corporate operations are managed across numerous industries. However, to the best of research experience, no prior effort has concentrated on integrating block chain to establish a secure and unchangeable data and evidence attribution maintenance architecture that autonomously checks the origination records. Therefore, the research work proficiently introduces the novel Block Chain based Contribute Sequence Tracking (BCCST) system with amalgamation of Trail based Smart Indenture (TSI) and Release Attribution Model (RAM). The study begins by outlining a practical application of the proposed TSI for the disintermediation of commercial activities utilising a notional, shared information ledger. This ledger not only makes monitoring data exchange easier, but it also encourages supply chain participants to cooperate together on a multilateral network. The novel RAM to create immutable data trails that make it easier to gather, maintain, and verify reliable data provenance.

Keywords: Block chain, smart contract, Distributed systems, Data provenance, supply chain management, distributed ledger

I. INTRODUCTION:

As the volume of data utilised in scientific research skyrockets, it is crucial to guarantee information quality and avoid data manipulation in order to validate study findings. For instance, the National Cancer Institute-funded multi-center cancer clinical trial organisation Cancer and Leukemia Group B discovered that 0.25 percent of the trials it analysed contained signs of fraud. [1].

In order to prevent data frauds, such as data generation, underreporting of the results, and manipulating the results to meet study aims, the provenance of the data must be preserved. Description of data provenance in this context as meta-data that identifies the source of the relevant data, the data owner, and the data modifications that have been made to the data.

Data provenance makes it easier to combine scientific data from several sources and provides source verification. Additionally, it promotes transparency and credibility by serving as a yardstick for gauging how well experiment outcomes support the actual research goals. For instance, the authors of [2] illustrate how data provenance monitoring increases the transparency and dependability of study findings. As a result, information about the data's provenance, from its origination to its modifications to the production of outcomes, must be documented in order to promote openness and reliability. Business operations have changed from manual [3] to with the introduction of process automation[4] framework. The legitimate execution of innovations, for example, electronic information exchange (EDI), esteem added networks (VAN), business insight (BI), and huge information digestion, presents different issues for incorporated tasks. Efficiency, synchronization, and coordination issues impede the interoperability and effectiveness of business actors [5, 6], specifically block chain. In addition, transaction transparency and open cooperation are now possible. Therefore, there is no longer a need for a third, dependable entity like banks or clearing institutions because the movement[7] can now rely solely on the agreement of participating nodes. The activities of business processes are being rearranged to eliminate intermediaries and move toward a global network that is more coordinated, automated, and unreliable [8].

Even though performance of a [10] distributed system can be improved. Handling handoffs like ownership

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7233
***Article Received**: 29 April 2023 **Revised:** 14 June 2023 **Accepted:** 28 June 2023*

transfers or status changes between two parties is made easier by disintermediating supply chain procedures.

Provenance systems face significant challenges due to the gathering and immutable storage of provenance data, as well as their verifiability and privacy preservation. Monitoring the data's origin is just as important as keeping the acquired provenance data private and confidential. Any kind of data used in research can come from a variety of sources and include sensitive information like patient data [13]. The information should be protected from unauthorized access in any system for managing the provenance [14, 15]. An information provenance framework ought to likewise guarantee that the provenance data maintained there may be verified by authorized individuals [16] without endangering their privacy or infringing the data's ownership [17]. From aforementioned concerns, the provenance systems in use today do not make an effort to verify the transaction and modifications prior to storage.

The remaining sections are organized as follows Section 2 covers prior research on the two main topics, namely block chains and smart contracts. The suggested conceptual framework for a tracking and transaction process is presented in Section 3. The possible impact of the suggested framework is thoroughly discussed in Section 4 along with a comparison to the existing model and an analysis of the experimental findings. The final conclusions are provided in Section 5.

II. LITERATURE REVIEW:

Liu et al [18] In order In order to provide a decentralised medicine supply chain traceability solution, this study suggests a comprehensive five-layer Blockchain and Internet of Stuff clever track and tracing platform (BIoT3, for short). A sensible arrangement is presented for the drug business to execute blockchain plan, improvement, application, and assessment, utilizing the five-layer blockchain stage engineering. Key enabling elements include the on-chain and off-chain method, smart contract-enabled drug services, and IoT-based medication identity management. Using real data from cooperating businesses, the Hyperledger Fabric blockchain has confirmed the BIoT3 technology's viability and effectiveness. In addition to gaining useful insights into the tuning, the case study suggests that it provides a viable visibility and traceability.

Omar et al. [19] In this study, we present a smart contract-based, blockchain-based strategy for reshaping PPE supply chain operations. We propose a general framework based on decentralized storage systems and Ethereum smart contracts to automate procedures and information exchange. In addition, we provide an in-depth explanation of the algorithms that are used to record the interactions that take place among various players in the supply chain. After being created and tested in the Remix environment, the code for the smart contract is now available to the general public on Github. We carry out comprehensive cost and security analyses for each and every one of the supply chain participants. A blockchain-based solution for PPE supply chains is financially attainable and offers a streamlined, secure, dependable, and transparent method of communication for a variety of stakeholders.

To trace and track the ownership data of spare parts from the original equipment manufacturer to the supplier and end users, we use a block chain-based smart contract that we propose in this study [20]. A trustworthy, secure, traceable, trackable, accessible, immutable, robust, and dependable spare part inventory system has been developed through our use of block chain capabilities. The recommended framework incorporates decentralized IPFS stockpiling to store and share information about spare parts. The entire implementation of algorithms is described. The smart contract is put to the test and evaluated. In addition, we present a cost-and-security analysis and explain how the proposed strategy guarantees precise ownership tracing and tracking of spare parts. On Github, we make the smart contract's source code accessible to everyone.

Utilizing a blockchain-based shrewd agreement that they propose in this review, Hasan et al. [21] keep track of spare parts' ownership information from the original equipment manufacturer all the way to the supplier and end users. A trustworthy, secure, traceable, trackable, accessible, robust, and dependable spare part inventory system is built using the blockchain's capabilities. Data related to spare parts are stored and shared in the proposed system using decentralized IPFS storage. They provide an overview of algorithms as well as complete implementations of those algorithms. The smart contract is put to the test and evaluated. In addition, they demonstrate how the suggested strategy ensures precise ownership tracing and tracking of spare parts and provide a cost- and security-related analysis. We make the source code for the savvy contract accessible to everybody on Github.

In order to implement traceability and shareability of supply chains, track and trace the workflow of agricultural food supply chains, and break down information islands between businesses as much as possible, this paper makes a framework based on consortiums and smart contracts. This framework will improve the reliability, security, and integrity of transaction records, which will reduce the need for centralized institutions and agencies. While collecting information about crop growth and the environment in the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7233
***Article Received**: 29 April 2023 **Revised:** 14 June 2023 **Accepted:** 28 June 2023*

InterPlanetary File System (IPFS), farmers use smart contracts to save file IPFS hashes in the IPFS. This further develops information security as well as lessens the issue brought about by the blast of block chain capacity. Shanwei Lvfengyuan Modern Agricultural Development Co., Ltd. uses this framework. The system has successfully implemented features like disintermediation and traceability of agricultural product information via QR codes, despite numerous flaws. Consequently, businesses can use this article's framework as a guide to maintain product quality and safety traceability.

As indicated by Bright et al. [23], and the final goal of this study is to provide a summary of the various blockchain-based traceability strategies that have been discussed in the existing body of literature. The main focus of this work is to show how blockchain traceability systems can make a supply chain transparent. In addition, it examines how blockchain discernibility arrangements affect various store network circulation network plans and outlines how advancements in the Internet of Things (IoT) and smart contracts enhance blockchain's true capacity. A cold chain Proof of Concept (PoC) demonstrates how blockchain traceability solutions increase supply chain transparency using Microsoft Azure Blockchain Workbench.

The majority of traditional tracking methods [18, 19], 20] rely on manual tasks to synchronize supply chain actors' information. In order to address issues like information synchronization, among others, businesses with more resources invest in the creation of a centralized mechanism like an ERP or EDI system. While these strategies improve productivity, they are unable to reduce the price of the ICT that is required. Changes that are malicious and cyberattacks make it harder to fully adopt the ecosystem. Furthermore, when participants experience system failures as a result of tampering or fraud-related activities, [21] [22] interference from centralized intermediaries, which are intended to increase participant confidence, causes confusion. Additionally, A centralised storage approach is the foundation for many of the existing provenance systems. The drawback of the centralised system design is that, in the event that the central server is attacked, it is feasible to jeopardise all data provenance trails. Another issue with distributed architecture-based provenance systems is the security of the data provenance information. The provenance system's data is editable by any authorised users.

III. BLOCK CHAIN BASED CONTRIBUTE SEQUENCE TRACKING:

A centralized storage approach serves as the foundation for many of the existing provenance systems. The disadvantage of issue with dispersed design provenance technologies. Any authorized users have the ability to tamper with provenance system data.

In this study, the research work proposes a method called BCCST to safely gather scientific provenance data in order to satisfy the aforementioned criteria and obstacles. Thus it comprises two new strategies are Trail based Smart Indenture and Release Attribution Model. The novel Trail based Smart Indenture employs cryptographic methods and the distributed immutability of blockchain technology to securely trace data provenance without disclosing personal information. Additionally, the proposed Release Attribution Model offers an automatic technique for verifying the created provenance data and enables the seamless generation of data attribution by authorized users. Using public key encryption, it also guarantees the confidentiality of the data. The system's access control policies limit authorized users' access to the provenance data.

Research has discussed the main supply chain participants and their roles as a result of the development of global supply chains. Figure 1 shows the movement of information, goods, and money in a typical process. A simplified model outlining the roles of individuals with comparable characteristics is required to gain further understanding of how supply chain participants interact with one another. The foundation of the entire system is formed by supply chain tracking, which also embodies the business rationale that drives each business function

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7233
***Article Received**: 29 April 2023 **Revised:** 14 June 2023 **Accepted:** 28 June 2023*

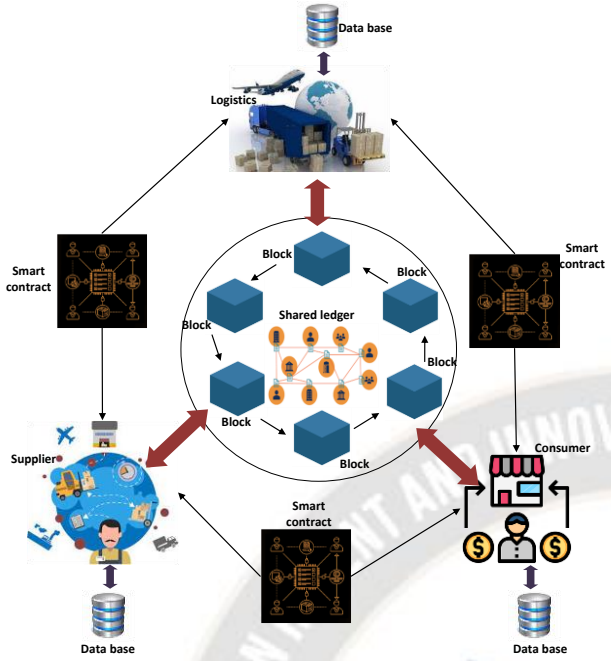

Figure 1: Proposed framework

To lessen inevitable company friction and likely hand-off causes, an integrated framework integrating block chain technology with the present procedure was suggested (see Figure 1). The timely tracking of process status is hampered by obstacles, which lengthens the payment duration. The block chain technology may reduce the inherent restrictions in legacy systems and offer several financial incentives for players to address this scenario. Payments for suppliers and logistics can be paid without worrying about the accuracy of process status as a result of the exemption from extended delivery times and physical inspections. The length of pending cash backlogs could be decreased for purchasers to increase supply chain efficiency. The suggested Trail based Smart Indenture tracking process has a number of design aspects. And off-chain modules as Release Attribution Model, which consist of two components: a cloud-based script for verifying each change made to a data file, and a adjustments and keep track of timings for the voting process. The detailed descriptions about those apprehensions are described as following sections.

3.1. Trail based Smart Indenture tracking process:

At first, Actors throughout the supply chain shared ledgers using the blockchain system. Second, all operational processes data is tracked for updates via smart contracts, which are technically virtual machines. Participants can follow a previous request brought on by an autonomous event device by mutually enrolling two participants on smart contracts, which define the parameters of the partnership. Smart contracts have the potential to instantly activate information push devices, the necessary stakeholders could monitor or respond to the most recent status of the process in a timely manner. Stakeholders who have registered for particular smart contracts are notified whenever the status of their accounts changes using this architecture.

Therefore, Instead of using a pull mechanism, a push mechanism is used to get the most current real-time notice of information changes (related to the trigger event). Our suggested block chain method boosts the effectiveness of the cash flow and logistical procedures. Supply chain partners can avoid the costs of manually verifying traceability and setting up expensive information-sharing platforms like EDI and ERP systems with this integrated architecture.

This paper's work conceptually exemplifies a federal event-obsessed strategy (see Figure 2). Smart contracts enable participants to communicate and connect with one another.

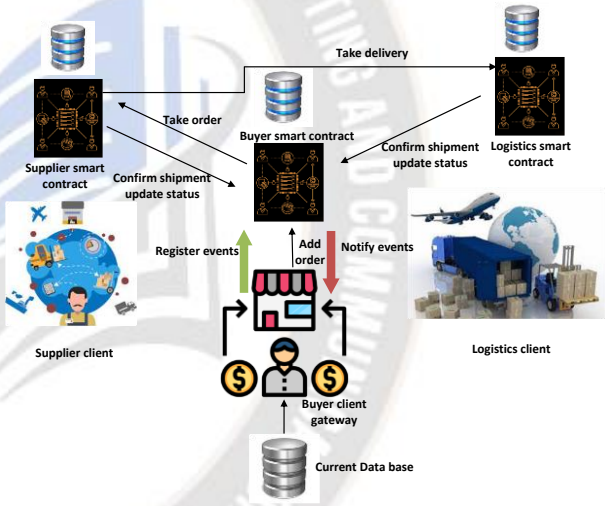

Figure 2: Federal event-obsessed approach

In addition, they send alerts on the procedure's most recent status changes. A single contractual is selected to serve as an administrator for other smart contracts in a government event-obsessed strategy. events triggered by smart contracts, such as changes in vendor or logistics company status are defined by each individual contract. In addition to outlining a variety of methods for updating system parameters, each of these agreements maintains control over the system-level state variables. The status and start events would then be altered by each function in accordance with the transition probability occurrences that were previously defined.

The particular contract must carry out all of the events that have been pre-defined for smart contracts. Through the event mechanism, any event-related information is

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7233
***Article Received**: 29 April 2023 **Revised:** 14 June 2023 **Accepted:** 28 June 2023*

accessible to any client who has registered for the relevant contract events.

The suggested framework, as seen in Figure 3, incorporates six different contract types that are integrated into the three main supply chain procedures outlined below:

1. Contracts between the buyer, logistics, and supplier in the transaction process

2. Payment processes with payment contracts

3. Contracts for query forwarders and dispatchers from external databases used for data access.

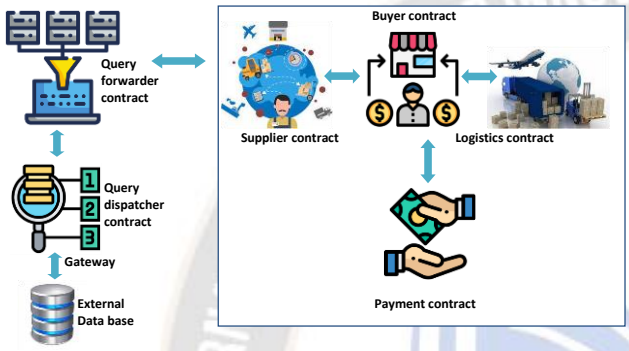

Figure 3: six diverse agreement category

Each of these contracts contributes to one of the three main processes and is deployed on block chain-based platforms like Ethereum or Hyperledger. The following is a description of the communications and connections and the related sub courses.

3.1.1. The contract procedure:

In a business-to-business scenario, To govern overall efficiency and better track the supply chain overview of the system, particular control points are added to the buyer contract's data structure. The order identifier (ID) and ordering time are both recorded on the demand side when an order is placed. Once the suppliers and associated logistics providers opt to accept the order, the shipping process is initiated and the shipment time is documented. When the delivery information is obtained, the checking sub-process is initiated, and the checking time and status (passed or not) are logged. The payment status and the payment time are documented after the buyer has paid the suppliers and logistics providers for the supply function.

From a supply perspective, properly informing customers and confirm shipping, replacing and simulating the work of the centralized administrator, sends the relevant payment information to the suppliers and logistics organizations and updates the most recent status.

3.1.2. The disbursement Procedure:

In order to prevent delinquencies, the transaction agreement was created expressly for the payment procedure. It controls the right to transfer payments to and logistics contracts under the centralized event model. However, because payments have atomic properties, full payment must be made without any things being missed throughout the payment process. We therefore suggest a payment contract to carry out payment activity in order to improve security and guarantee completion of payments. When implementing the holistic payment method, think of the logistics and supplier contracts as one large payment unit. To avoid payment incompletion, we carry out a one-time payment under this payment arrangement.

3.1.3. The statistics admittance procedure:

Some data can be kept on-chain or left in off-chain databases, depending on tracking issues and smart contract structure. This makes block chains more efficient at processing data. By employing two extra smart contracts to connect the block chain to external databases, the suggested technique incorporates both and accounts for the difficulties of accessing an external database's API directly. The query forwarder and dispatcher contracts, which are covered in the next part, were made in order to gather the required data and give input to the designated smart contract.

The query forwarder contract moves information around. Each smart contract's clients have made requests for access to external data in this contract. Outbound requests for event alerts and data feedback are collected through a conduit that is registered on the dispatcher contract by the forwarder contract. Clients of other smart contracts can also receive status change notifications The preceding explanation makes it possible for on-chain and off-chain databases to communicate with one another and clarifies the purposes of the suggested structure. The following section defined the smart contract's storage and retrieval without reducing authentication.

3.2. Model of Release Attribution:

Changes are stored, retrieved, and validated by the client module, which is in charge of interacting with the smart contract. RAM also includes a checking script module operating at the cloud depot where the different instances of the documents are kept, in addition to the client modules in each client. Each say ” that is specific to a particular document is verified by the verification module.

A few of the components that make up the client modules are listed below:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7233
***Article Received**: 29 April 2023 **Revised:** 14 June 2023 **Accepted:** 28 June 2023*

3.2.1. Part that defines the consumer:

The interface module primarily provides a user interface through which smart contracts can be communicated with. The client module provides access to all fundamental system functions, including document change history tracking, creating a new document for tracking, and displaying grant and revocation information. All tasks that a client conducts through the connection point module are certainly carefully endorsed by the module.

3.2.2. Part of the spectator:

The event observer module keeps an eye on the Vote contract's change events. Events that are recorded in the contract and also checks to see if the current client is keeping track of any changes. After decrypting the change event and verifying the anthropogenic climate signing, the watcher contract calls the authentication process to determine whether the compliance modification affects the current user. It educates the client regarding the among doing and, on the off chance that the result is adequate, votes for the client's sake. The consumer does not need to be at the interface because the vote is computerized. Using a database, the observer function monitors the particulars of documents in which the current user is a stakeholder.

3.2.3. Part of control:

The voting stages are under the control of the pic microcontroller. The control module is requested to start the voting interval for the modification whenever a document amendment event takes place. At the conclusion of the voting session, the timer will force the voting process to finish.

3.2.4. Script for authentication:

The authentication procedure is stored in the system's cloud storage. The validation procedure verifies the data file or document modifications that are uploaded to the BCCST system. The inputs to the authentication process are the links to the most recent version of the file as well as the document's most recent and previous cryptographic hashes from the DataProv updates. First, the authentication code verifies the hashes included with the files. The most recent stable version of the data file is then compared to the current unconfirmed file. If any additional modifications to the file are discovered that are not listed in the change request, the authorization process will notify to prevent future document version manipulation. As a plug-in module, the authentication code can be customized to fit the BCCST system's usage scenario.

3.3. Voting procedures include:

Figure 4 portrays the general image of the democratic system. When the initiator uploads a change to the Vote contract, the voting process begins. The initiator client sets a timer for the beginning of the voting phase for the most recent update. At the beginning of the voting phase for the provided change, the vote contract causes an event to take place. The newly created vote event is read by the client applications' Event listener module. If a client application is a stakeholder in the current document change event, this is confirmed. The cloud-based verification script is then called. in addition to links to the file's most recent and earlier versions and hashes.

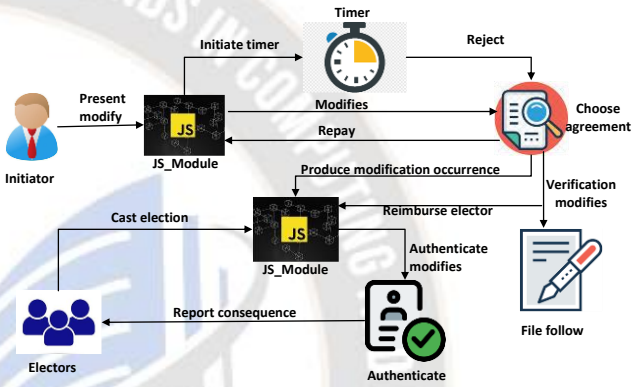

Figure 4: Election procedure for a file change

According to the voting protocol policy, each node calls for verification. alerts the user of the outcome if the verification script returns true. The decision to accept or reject the updates is subsequently decided by the client application. The vote contract records the user decision after obtaining a vote from a client. At the conclusion of the voting session, the timer module will end.

By doing this, we encourage participants to tell the truth while also rewarding them for spotting mistakes.

For systems with a large number of users and changes, voting by every client for each and every update is inefficient. The paper suggest randomised threshold voting in such cases. In randomised threshold voting, the minimum number of votes must be cast in favour of or against the proposed change. Assuming there are o users of the document, the vote contract threshold is u. The contract aims to obtain expectedly v votes for $u > v$ in order to guarantee that each voting phase for a change obtains u votes. The threshold u makes sure that any modification receives the required number of votes for or against it.to decide whether to participate in the change voting phase.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7233
***Article Received**: 29 April 2023 **Revised:** 14 June 2023 **Accepted:** 28 June 2023*

$$L_t = Hash(Bl_n, En_{Txt}, Diff, Addr) \bmod i \quad (1)$$

By hashing Bl_n, En_{Txt}, Dif, the current gas limit, and $Addr$, the initiator's address, the client creates L_t, a random quantity. A comparable random number is generated for each vote after it is cast by the vote contract, which also validates the legitimacy of the cast vote.

3.3.1. Haphazard zed voting investigation:

The work select users at random to vote for or against the modification in the verification method that relies on randomized voting. The paper might want to select a minimum of users at random from the n users who are available for voting for security reasons. Then can set the probability that a user will be randomly selected as $\frac{u}{i}$ where $u > t$ because the process is random. Given this, we may examine the likelihood that a certain voting phase won't receive at least s votes. The work uses the following Chernoff-Hoeffding bound result before performing our analysis.

Theorem a)

Let,

$$Y = \sum_{j=1}^{i} Y_j \; where \quad Y_j, j \in [0,..i] \quad (2)$$

These are separately disseminated in [0,1].

$$Q_e[Y < F[Y] - b] \le e^{\frac{-2b^2}{i}} \quad (3)$$

From theorem a, the work proven the follows theorem:

Theorem b)

For presented the modifications from Known i users could voting, for a haphazard voting procedure with selection of consumer probability $\frac{u}{i}$ where $u > t$, and the probability P_g that owing to malfunction selected consumer cannot vote, the whole number of consumers voted V is lower than t is a probability as:

$$Q_e[V < t] \le e^{\frac{-2(u-t-i-P_g)^2}{i}} \quad (4)$$

Theorem c) If all of the current i users choose has such a probability of $\frac{u}{i}$, then one round of voting will fail at a failure probability of P_g. The predicted voting process cost, $F[C_V]$, can thus be expressed as follows:

$$F[C_V] = \frac{c.u + c_1}{1 - P_g} \le \frac{c.u + c_1}{1 - e - \frac{2*(u-t)^2}{i}} . \quad (5)$$

c and c_1, two system-dependent constants.

Based on the empirical constants c and c_1, the research can apply theorem c) to determine the best value for u given t and i.

Thus, the suggested decentralized system makes use of private-chain to achieve service efficiency at a respectable level in a distributed setting. Second, the high number of human inspections and paper-based transactions required by existing SCM that result in a high number of middlemen and unavoidable business frictions, which reduces service efficiency. As previously said in this article, our block chain- and smart contract-based approach may automate manual and paper-based transaction-based SCM flows, decrease manual intervention, and significantly reduce business friction.

The findings of the study offer theoretical contributions to scholarly work on the design of block chain-based applications, particularly with the BPR approach that has been successfully used to transform established The transition of commercial services and corporate applications from centralized to distributed peer-to-peer architecture is one feature of cutting-edge block chain technology. To accommodate the advancing block chain technology into a practical distributed architecture with applications, the study theoretically broadens the conceptual framework rather than fundamentally altering it. The exploration has effectively shown that the proposed BPR strategy might be used to re-engineer the important and material piece of a business interaction rather than modifying the cycle completely, taking into consideration the redesign of existing administrations and applications.

IV. RESULT ANALYSIS:

The paper utilized the python based experimental setup for proven the proficiency of the research. And the work has been analyzed parameters such as Success Rate, Average Latency, Throughput, and resource consumption. The

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7233
***Article Received**: 29 April 2023 **Revised:** 14 June 2023 **Accepted:** 28 June 2023*

capacity to enable smart contracts is among the most important elements for any Block chain system. Consequently, we will use Ethereum's smart contract and chain code with this experiment.

As previously noted, we evaluated performance using four metrics: success rate, Average Latency, throughput, and resource usage. These four measures are defined as follows to avoid ambiguity.

4.1. Experimental performances based on parameters analysis:

4.1.1. Success rate:

100 transactions are carried out via the smart contract used in this experiment. As a result, the number of successful transactions carried out of 100 transactions is what determines a block chain's success rate. The following figure 6 described the success rate of the proposed work in an effectual manner.

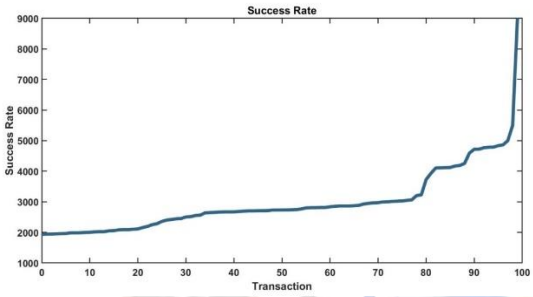

Figure 6: Success rate of the research work

The proportion of transactions has been successful out of 100 that are started by various smart contract functionalities. For the Transfer function, only Ethereum has a 100% success rate, making a more trustworthy system whenever it relates to sending money to various accounts. All Block chain systems examined here have a 100% success rate.

4.1.2. Average Latency:

The median amount of time for each transaction in the data set between the initialization of the code and its considered relevant is referred to as average latency.

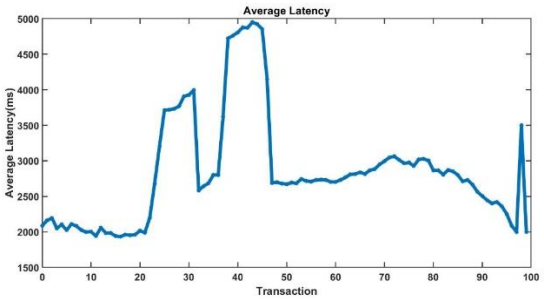

Figure 7: Average latency of the proposed work

From figure 7 illustrated the average latency of the proposed work, hence it shown the reduction value defined the efficiency of the proposed work.

4.2.2. Throughput:

The quantity of transactions that are completed each second is referred to as throughput. Figure 8 shows the function execution throughput across all Block chain platforms. Because the throughput range increases with each traction level relative to the one before it, it can be stated that the suggested blockchain-based transaction outperformed the parameter analysis.

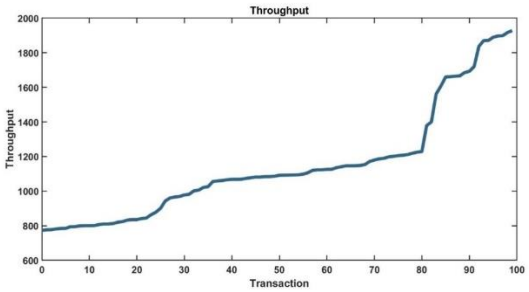

Figure 8: Throughput of the research

4.2.3. Memory usage:

Here, the research analyzes the variations in memory and CPU use among different Block chain platforms investigated in this experiment for the same three functions. The average memory, measured in kilobytes ("KB"), utilized by each block chain platform to execute functions is shown in the figure 9. This means that Ethereum uses a lot of RAM when being tested against benchmarks.

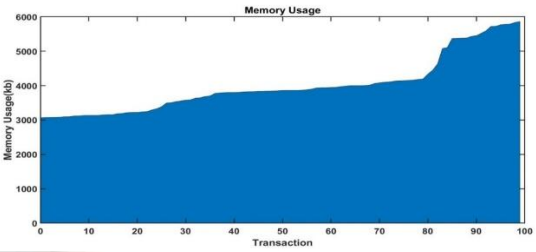

Figure 9: Memory consumption of the work

4.2.4. CPU usage:

As an alternative, figure 10 shows the average CPU utilization in terms of the share of each Block chain platform. Ethereum uses higher CPU processing power, which is consistent with the experimental memory use statistics.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7233
***Article Received**: 29 April 2023 **Revised:** 14 June 2023 **Accepted:** 28 June 2023*

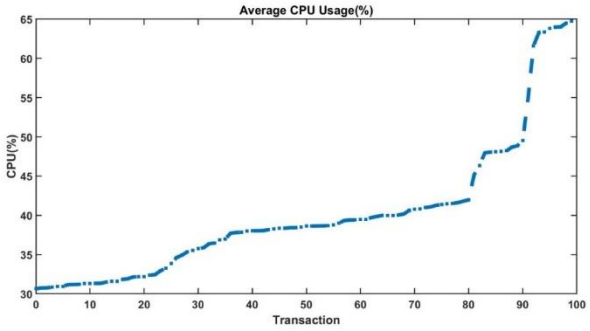

Figure 10: CPU utilization

In this study, 100 transactions are carried out to compare the performance of Block chain platforms in terms of throughput and average delay. The research work discovered that Ethereum uses less hardware resources by comparing the resource usage of Block chain systems. However, research findings revealed that when using the Transfer function, Ethereum performs better in terms of the number of successful transactions. Overall, the performance evaluation results show that research work is superior across all four criteria, including success rate, average latency, throughput, and resource usage. The next section described the comparative analysis based on different tools has been used in block chain transaction.

4.3. Comparative analysis based on different tools:

The security tools that have been published in peer-reviewed journals, articles, and conference papers are the basis for the comparative analysis of the research work. Although this step does not add any new comparative results, it does take into account and analyze the security tool findings provided by their creators and other independent researchers. The research work has been utilized the porosity tool for 100 effectual block chain transaction. And the figure 11 illustrated the FDR of porosity, oyente, remix, securify, and smartcheck is 100%, 99%, 96%, 99%, and 68% respectively. Also FNR is 100%, 99%, 92%, 99%, and 47% respectively. Hence it defined the porosity has been attains more effectual performances.

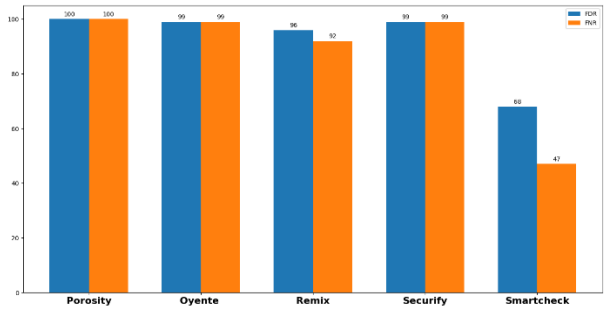

Figure 11: Comparative analysis based on FDR and FNR

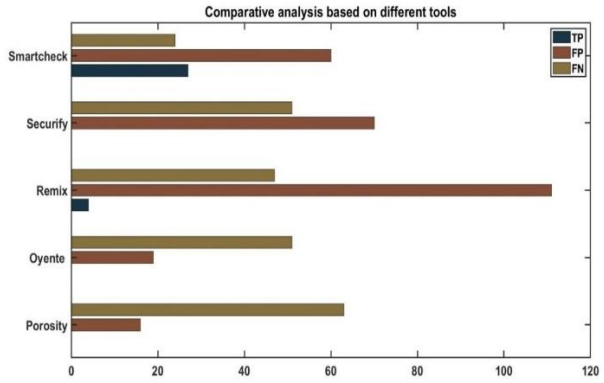

Figure 12: Comparative analysis based on TP, FP, FN

In figure 12 described the comparative analysis based on different tools with the performances of TP, FP, and FN. The tools used for comparison such as porosity, oyente, remix, securify, and smart check with their corresponding TP values are 0, 0, 4, 0, and 27. FP values are 16, 19, 111, 70, and 60. FN values are 63, 51, 47, 51, 47, 51, and 24.

V. CONCLUSION:

The research work concluded that adopting digital currency as an alternative payment option is possible and could shorten the payment lead time. The successful outcomes of the research that provide provenance trails for data access control-based privacy protection. By integrating randomized voting with tracking for the change trails recorded/captured and leveraging smart contracts to punish any deviation, the BCCST system significantly improves the reliability of the data trails. Additionally, this study gives company managers a better model for evaluating events from a smart contract perspective as well as improved operations management efficiency. Supply chain managers can monitor the status of cash flows and logistics using the suggested blockchain-based architecture with smart contracts. In conclusion, the supply chain's transparent tracking and prompt controls might be advantageous to the process's participants. Additionally, a quick enhanced help lower the costs of keeping a cash reserve. Future research into the enhancement of supply chain performance may benefit from looking at how the suggested blockchain-based process may be used to follow the supply chain process promptly and increase the level of supply chain process automation.

REFERENCES:

[1]. Ahl, A., Yarime, M., Tanaka, K. & Sagawa, D. (2019). Review of blockchain-based distributed energy: Implications for institutional development. Renewable and Sustainable Energy Reviews. 107: 200-211. https://doi.org/10.1016/j.rser.2019.03.002.

[2]. Banalieva, E. R., Cuervo-Cazzura, A. &Sarathy, R (2018). Dynamics of pro-market institutions and firm performance. Journal of International Business Studies. 49: 858- 880. https://doi.org/10.1057/s41267-018-0155-7.

[3]. Bohme, R., Christin, N., Edelman, B. & Moore, T. (2015). Bitcoin: Economics, technology and governance. Journal of Economic Perspectives. 29(2): 213-238. DOI: 10.1257/jep.29.2.213.

[4]. Gadde, S. ., & Chakravarthy, A. S. N. . (2023). Novel and Heuristic MolDoc Scoring Procedure for Identification of Staphylococcus Aureus. International Journal of Intelligent Systems and Applications in Engineering, 11(2s), 125 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2516

[5]. Cruz Jason, Paul and Kaji Yuichi. 2015. The Bitcoin Network as Platform for Trans-Organizational Attribute Authentication. IPSJ SIG Notes 2015, 12 (feb 2015), 1–6. http://ci.nii.ac.jp/naid/110009877764/en/

[6]. The Economist. 2016. Better with bitcoin. (2016). http://www.economist.com/news/science-and-technology/21699099- blockchain-technology-could-improve-reliability-medical-trials-better.

[7]. Brophy, R. (2020). Blockchain and insurance: A review of operations and regulation. Journal of Financial Regulation and Compliance. 28(2): 215-234. https://doi.org/10.1108/JFRC-09-2018-0127.

[8]. Bruton, G. D., Lau, C.-M. &Oboj, K. (2014). Institutions, resources and firm strategies: A comparative analysis of entrepreneurial firms in three transition economies. European Journal of International Management. 8(6): 697-719. https://doi.org/10.1504/EJIM.2014.064905.

[9]. Cai, L., Sun, Y., Zheng, Z., Xiao, J. &Qiu, W. (2021). Blockchain in China. Communications of the ACM, November 2021, 64(11): 88-93

[10]. Carter, N. (2021). How much energy does bitcoin actually consumer? Harvard Business Review. Retrieved from https://hbr.org/2021/05/how-much-energy-doesbitcoin-actually-consume.

[11]. Albeshr, S. &Nobanee, H. (2020). Blockchain applications in banking industry: A minireview. SSRN working paper. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3539152.

[12]. Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J. &Arami, M. (2020). How blockchain can impact financial services – the overview, challenges, and recommendations from expert interviewees. Technological Forecasting and Social Change. 158. 1- 10. https://doi.org/10.1016/j.techfore.2020.120166.

[13]. Chen, Y. &Bellavitis, C. (2020). Blockchain disruption and decentralized finance; The rise of decentralized business models. Journal of Business Venturing Insights. 13. E00151. https://doi.org/10.1016/j.jbvi.2019.e00151.

[14]. Chen, Y. &Bellavitis, C. (2019). Decentralized finance: Blockchain technology and the quest for an open financial system. SSRN. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3418557.

[15]. Chen, L. & Yang, W. (2019). R&D tax credits and firm innovation: Evidence from China. Technological Forecasting and Social Change. 146: 233-241. https://doi.org/10.1016/j.techfore.2019.05.018.

[16]. Chiu, J. &Koeppl, T. (2017). The economics of cryptocurrencies – bitcoin and beyond. SSRN working paper. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048124.

[17]. Carney, M., Gedajilovic, E. & Yang, X. (2009). Varieties of Asian capitalism: Toward an institutional theory of Asian enterprise. Asia Pacific Journal of Management. 26: 361-380. https://doi.org/10.1007/s10490-009-9139-2.

[18]. Choi, T.-M. (2020). Creating all-win by blockchain technology in supply chains: Impacts of agents' risk attitudes towards cryptocurrency. Journal of Operational Research Society. 2020, 1-9. https://doi.org/10.1080/01605682.2020.1800419.

[19]. Liu, X., Barenji, A.V., Li, Z., Montreuil, B. and Huang, G.Q., 2021. Blockchain-based smart tracking and tracing platform for drug supply chain. Computers & Industrial Engineering, 161, p.107669.

[20]. Omar, I.A., Debe, M., Jayaraman, R., Salah, K., Omar, M. and Arshad, J., 2022. Blockchain-based Supply Chain Traceability for COVID-19 personal protective equipment. Computers & Industrial Engineering, 167, p.107995.

[21]. Musamih, A., Salah, K., Jayaraman, R., Arshad, J., Debe, M., Al-Hammadi, Y. and Ellahham, S., 2021. A blockchain-based approach for drug traceability in healthcare supply chain. IEEE access, 9, pp.9728-9743.

[22]. Hasan, H.R., Salah, K., Jayaraman, R., Ahmad, R.W., Yaqoob, I. and Omar, M., 2020. Blockchain-based solution for the traceability of spare parts in manufacturing. IEEE Access, 8, pp.100308-100322.

[23]. Wang, L., Xu, L., Zheng, Z., Liu, S., Li, X., Cao, L., Li, J. and Sun, C., 2021. Smart contract-based agricultural food supply chain traceability. IEEE Access, 9, pp.9296-9307.

[24]. Sunny, J., Undralla, N. and Pillai, V.M., 2020. Supply chain transparency through blockchain-based traceability: An overview with demonstration. Computers & Industrial Engineering, 150, p.106895.