JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(1), MARCH, 2025
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Veridical Ranking of Inconsistent Responses in Blockchain Consensus Process Using Proof-of-Congruity Consensus Scheme

[1]Omoniyi Wale Salami, [2]Ore-Ofe Ajayi, [3]Emmanuel Adewale Adedokun & [4]Busayo Adebiyi
[1,2&3]*Department of Computer Engineering*
Ahmadu Bello University, Zaria, Nigeria
[4]*Department of Computer Engineering*
Federal University Lokoja

ABSTRACT
Consensus mechanisms provide the security in blockchain for protecting data. The security requirements for a data use case determines the design of consensus mechanism that will be suitable for the blockchain. Forensic investigation requires intact integrity of data and extraction of relevant facts that is adequate for making decisions. Proof-of-Congruity consensus mechanism was proposed for preserving data integrity and fidelity. The Original Proof-of-Congruity consensus mechanism did not review the differences in validators responses when there is no collective consensus. It only award consistency points to validators when all of them agreed on a value. This paper proposed a method for evaluating veridical correlations between different validators' responses for determining the optimal response and rank the validators accordingly. This will provide a means for compensating correct validators and penalizing bad validators appropriately. It will also provide an investigator with a means for determining how reliable a dataset is and the possible veracity of facts that may be extracted from it.

ARTICLE INFO
Article History
Received: September, 2024
Received in revised form: November, 2024
Accepted: February, 2025
Published online: March, 2025

KEYWORDS
Proof-of-Congruity, PoCCS, Collaborative Integrity Mechanism, Consensus Mechanism, Blockchain, Distributed Ledger Technology

INTRODUCTION

Blockchain has become a popular tool in data engineering for securing data. Researchers have proposed several improvements to it to make it suitable for different applications. At the core of blockchain are the consensus mechanisms that are responsible for creating the security provided by blockchain [1]. Blockchain is now applied in wider areas for securing data. Various applications of blockchain demands different security for data. Consensus algorithms have come a long way to become the powerful components of distributed ledgers that provide security for data in the ledger. Thus, suitable consensus algorithm is required for achieving the required security.

Consensus algorithm should ensure correctness and maintain consistent structure of blocks in blockchain [2]. Being the mainstay of blockchain, consensus mechanisms direct transaction execution process, validate transaction and harmonise activities of the replicas to achieve a consistent distributed ledger. They are used by blockchain to achieve reliable overall results from transaction processes [3].

There are different types of distributed ledger technologies (DLTs) that use consensus mechanisms besides blockchain [4]. Each DLT uses consensus mechanism in a way that is determined by the design of the mining protocol used for the ledger. Blockchain uses consensus mechanisms for maintaining chain consistency and immutable blocks protection. Directed Acyclic Graph (DAG) ledger uses consensus to maintain causal relationships between events to prevent biases, maintain transactions order, reduces transaction creation steps and be robust and flexible number of concurrent transactions increases [5]. Hedera Hashgraph ledger is another type of DAG ledger. Its consensus is used

Corresponding author: Omoniyi Wale Salami
✉
Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.

to ensure transaction messages reach all nodes, process transaction faster and store larger data, [6]. Holochain verifies transactions faster with its consensus mechanism and utilises energy efficiently. It is capable processing of very large transaction with its agent-centric consensus protocol [7]. Tempo is another distributed ledger technology that maintains the order of transactions. It uses consensus mechanism to synchronise data stored by each agent in its sub-ledgers (known as sherds) with the data in other agents sherds and maintain uniformity among the agents, [8].

The most common principle used to develop consensus mechanisms is the Byzantine Generals Problem [9]. This principle is considered to be more easily understandable than the Paxos Parliamentary, The Part-Time Parliament [10], Principle [11]. The Byzantine Fault Tolerance (BFT) consensus protocol was based on the [9]. It gained more attention than the Crash Fault Tolerance (CFT) protocol that was developed based on [10]. Many versions of BFT consensus proposed include Probabilistic Byzantine Fault Tolerant [12], Byzantine Fault Tolerant with Non-Determinism [13], Alea-BFT [14], and Dashing and Star [15]. Also, among its variants are Fast-HotStuff [16], Hbft [17], Practical Byzantine Fault Tolerant (PBFT) [18], Zyzzyva [19], among several others. Some CFT based consensus protocols are RMWPaxos [20], Moderately complex paxos made simple [21], Paxos made moderately complex, [22]. There are consensus protocols combined BFT and CFT to develop hybrid solutions that exploit the benefits of both principles like [23].

The BFT and CFT protocols are designed to ensure the system functions in the presence of malicious nodes. Thus, they tolerate some faults in their operations. The other consensus protocols are proof-based mechanisms used for validation of transactions. The proof-based consensus mechanisms use working principles that ensure agreement among the validating nodes. Proof-of-Work (PoW) [24] and Proof-of-Stake (PoS) [25], [26] are popular types of proof-based consensus mechanisms. PoW principle is based on difficulty of computing a certain hash target. PoS is a risk based consensus mechanism where a validator risk its investment to become the primary. Several other proof-based consensus mechanisms are available now. Existing proof-based consensus mechanisms is either based on the working principle of PoW, e.g., [27], [28], or it may be based on the working principle of PoS, e.g., [29], or combine working principles of PoW and PoS, e.g., [30]. It is the proof-based consensus mechanism that provides immutable security to data in distributed ledgers.

Forensic investigation is service that puts a premium on data correctness as much as its immutability [31]. Forensic analysis is basically used to discern ambiguities and deduce genuine convincing facts from events of an incident. Current blockchain consensus protocols that are either tolerate some level of faults could inherently introduce error in forensic data. Those that work based on difficulty of computation may not be too slow for extracting evidence. While those consensus mechanisms requiring risking stakes may not encourage miners to ensure correctness of data but concern to secure their stakes. Thus, they are not suitable for mining forensic evidence. CICM, a blockchain solution for protecting originality of data, was proposed [32]. The authentication algorithm use in [32] was further developed as Proof of Congruity Consensus System (PoCCS) and used to validate a validator's response and confirm the validator as a genuine member of the consensus team in [33] and [34]. PoCCS only record the number of collective consensuses in consensus processes in which the validator was involved.

The solution used PoCCS [33] for validating evidence data in the blocks. The processes that successfully yield a single collective agreement earn the validators involved credit points recorded as consistency history (CH) in PoCCS. But the process where there are different conclusions on a value from the validators was only recorded in auxiliary ledger without credits to the validators involved. This work proposes a veridical ranking method for evaluating correlations between different responses from validators in a consensus team

Corresponding author: Omoniyi Wale Salami
✉
Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(1), MARCH, 2025
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

and the original value they are validating. The method assigns points to validators' responses based on their veridical correlations with the original value. The rest of this paper is arranged as follows; section II contains the review of related works, section III explains the design methodology, implementation of the new method is presented in section IV, while section V contains the discussion of the results of the tests of the new design method, and conclusion presented in section VI.

Related Works

Different distributed ledger technologies use their consensus algorithm in a way that is peculiar to their data security requirements. Anwar (2019) [4] reviewed some DLTs including Hashgraph, Directed Acyclic Graph (DAG), Holochain, and Tempo. Features of some DLTs are provided in Table I.

Table 1: Different Types of Distributed Ledger Technologies and Their Features

DLT	Platform	Storage Structure	Consensus Scheme
Blockchain	Satoshi N.	Continuous Chain of Blocks	Proof-of-Work
Hashgraph	Hedera	Parallel Chains of Events	Mutual Validation
DAG	Hedera	Series of linked Chains	Accumulative Trust
Holochain	Holochain	Contributory transaction ledgers	Node Validity Based
Tempo	Radix	Synchronized Ledger Units	Logical Clock Sequence

The differences in the structures of different DLTs necessitates different consensus mechanisms that are applicable to them. Some consensus mechanisms trust structure rely on the integrity of the state machines. Alea-BFT [14] uses Verifiable consistent broadcast (VCBC) method for ensuring that trusted nodes deliver a message sent by s trusted sender. ProBFT [12] addressed the challenges of security of safety and liveness of data. The solution proposed a method for achieving high probability success of security for realistic adversary attacks. BFT-ND [13] addressed the problem of inconsistencies that do arise from asynchronous order of operations in a consensus process. These solutions did not address peculiar problems that do make data unsuitable for extracting genuine facts because there are many factors that do change data in computer storages [35].

Sometimes of the changes caused are discreet and may be difficult to detect [36]. The process of extracting digital evidence is very importance to ensure the sanctity of the extracted facts [37]. Data and its attributes should be secured from the time of its creation and throughout it span to preserve the integrity and relevance of its information contents [38]. This is necessary to avoid making misleading, counterproductive and/or disputable data-driven decisions [39]. PoCCS [33] was proposed for preserving data integrity and fidelity to ensure data is suitable forensic investigation.

Design Methodology

The cases for concluded process of CICM was expressed in [34] as

$$F(id)\begin{cases}1 \Leftrightarrow \exists\{X_m\} \subset \{X_s\}: \{X_m\} \mapsto \left\{\{O_p\} \cap \{X_s\}\right\} \\ < 1 \Longrightarrow \left\{\{X_m\} \cap \left\{\{O_p\} \cap \{X_s\}\right\}\right\} \subset \{X_m\} \\ 0 \Longrightarrow \forall x \in \{X_m\}: x \notin \left\{\{O_p\} \cap \{X_s\}\right\}\end{cases}$$

1

The Equation (1) [34] defines the policy for CICM operations. Only the topmost and bottom cases, without the middle condition, were included in the equation in [32]. The policy was further expounded in [34] with the addition of the middle case that defines the condition $0<F(id)<1$. Only the case when $F(id) = 1$ for all validators earns the validators credits in both [32] and [34][34]. This

Corresponding author: Omoniyi Wale Salami
✉
Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(1), MARCH, 2025
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

paper designs a CH credit points award system for the case when *F(id)* ∈ [0<*x*<1] for different validators. The award system is based on evaluation of the responses on the scale of their merit relative to the ideal correct response. The design method for awarding the credit points is presented in this section.

Preliminary Setup: Theoretical Basis for the Design of the Deviation Estimation Method

The values for the parameters in 11 are first defined.

$$O_p = \begin{bmatrix} p_{11} & \cdots & p_{1C} \\ \vdots & \cdots & \vdots \\ p_{1R} & \cdots & p_{RC} \end{bmatrix} \quad 2$$

$$X_m = \begin{bmatrix} m_{11} & \cdots & m_{1v} \\ \vdots & \cdots & \vdots \\ m_{1h} & \cdots & m_{hv} \end{bmatrix} \quad 3$$

$$X_s = \begin{bmatrix} s_{11} & \cdots & s_{1V} \\ \vdots & \cdots & \vdots \\ s_{1H} & \cdots & s_{HV} \end{bmatrix} \quad 4$$

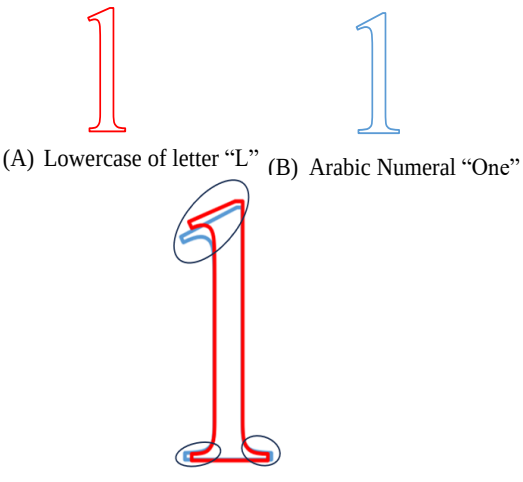
The elements of O_p, X_m, and X_s, in (2), (3), and (4) are the perceptive factors of an observer O, the identity stimuli of an observed object X known to O, and the identity stimuli on X, respectively.

Para meters Weights Computation

A set of weighted perceptive factors is computed for each observer O based on the strength of each of its perceptive factors to perceive identity stimuli correctly.

$$O_p^w = \begin{bmatrix} W_{11} & \cdots & W_{1C} \\ \vdots & \cdots & \vdots \\ W_{1R} & \cdots & W_{RC} \end{bmatrix} \quad 5$$

The elements of the matrix in (5) are the weights for the corresponding perspective factor p_{rc} in (2) for an observer O. Each of the W_{rc} for each p_{rc} of an O is determined by considering the uniqueness of the identity stimuli of X for voiding any perspectival similarity of X with another object. In computer vision, the elements of X_s used for an object identification are fixed, e.g., thumbprint minutiae. Each element of X_s in (4) is given a weight, *w*. The weight is computed considering the ambiguous areas on the X that may cause alternations between perceptions and confuse an O to identify X wrongly. Therefore, common areas have lesser weights than areas with the discerning features on X. The lowercase of letter "L" and number "One", both in Times New Roman font-style, in Fig. 1 is used to illustrate such case of ambiguity that can confuse a validator to misconstrue an object as what it is not.



(A) Lowercase of letter "L" (B) Arabic Numeral "One"

(C) Overlapping the two shapes to identify their differencees

Figure 1: Illustration of ambiguous shapes with the lowercase of letter "L" and Arabic Numeral "One" in "Times New Roman" font-style

Corresponding author: Omoniyi Wale Salami
✉
Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(1), MARCH, 2025
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Fig. 1(A) and Fig. 1(B) show the shape of the individual characters on their own alone. In Fig. 1(C) the two characters were overlapped to show their discerning features $\mathfrak{f}$, circled in the figure. The stimuli, $S_{\mathfrak{f}}$, in those circled areas on letter "l" and Arabic numeral "1" have larger weights than common stimuli, *S*, that may not be confused. because they tell the two characters apart and must be properly recognised. If each $S_i \in S$ is assigned weight w_S and the total number of stimuli on X is S_{HV}, the multiplying factor $\delta_{S_{\mathfrak{f}}}$ for calculating the weights for the $S_{\mathfrak{f}}$ will be

$$\delta_{S_{\mathfrak{f}}} = \frac{S_{HV} - |S_{\mathfrak{f}}|}{S_{HV}} \qquad 6$$

In (6), $|S_{\mathfrak{f}}|$ is the total unique stimuli $S_{\mathfrak{f}}$ on X. The weight $w_{S_{\mathfrak{f}i}}$ for each $S_{\mathfrak{f}_i} \in S_{\mathfrak{f}}$, is calculated.

Thus, the fewer the unique stimuli on X the larger their weights will be than weights of other stimuli. Clarity of the viewed object X in terms of illumination and contrast against background also affects perception. This is measured as Visual Saliency [40]. Weights are assigned based on saliency using contrast ratio. The weights are inversely proportional to the contrast ratio. The less illuminated areas are assigned higher weights than better illuminated areas. A validator gets higher credits identifying poorly illuminated object correctly than for properly illuminated ones.

The computation is done as follows;
Let luminosity of a stimulus area be ℓ and the highest illumination on X be $\mathcal{L}$, then the weighing factor based on saliency is computed as;

$$D_{S_{\mathfrak{f}}} = \frac{\mathcal{L}}{\ell} \qquad 7$$

The weighing factors are used to obtained to the weights in (5) as

$$W_{S_{\mathfrak{f}}r,c} = w_S \times \mathrm{e}^{(D_{S_{\mathfrak{f}}r,c} + \delta_{S_{\mathfrak{f}}r,c})} \qquad 8$$

The elements of the matrix in (5) are computed with (8). Thus, if R = 3 and C = 3, (8) will give

$$W_{S_{\mathfrak{f}}r,c} = \begin{bmatrix} W_{11} & W_{12} & W_{13} \\ W_{21} & W_{22} & W_{32} \\ W_{31} & W_{32} & W_{33} \end{bmatrix} \qquad 9$$

Equation (9) gives the relative difficulties of perceiving the stimuli in a region compared to other regions on X.

Apart from uniqueness and saliency of stimuli the usage of the characters also matters to perceiving the characters correctly. Thus, the Contextual and Syntactic usage of the characters are used to award credits or penalize a validator as explained in the following.

Contextual usage here is the situation when the characters are used in a way other than their conventional usage that can make them to be easily understood correctly. As an example, say Fig. 1 has subfigures A, B to M. If after referring to the figure as Fig. 1, the subfigure (L) was referred to as Fig. 1 l, Fig. 1l, Fig. 1(l) or Fig. 1-l, a validator that misconceived the digit '1'or lowercase letter 'l' in either of the cases will not be penalized but corrected. But the validator that that perceived the characters correctly in those cases will earn the equivalent value of the weight of the cryptic stimuli for the character as credits.

Syntactic usage of the characters is used here to refer to the use of letters or digits to form the original spelling of a word or format of a number. The character weight is the same as may be assigned using the weighing system explained earlier. Misconceiving characters in syntactic usage are considered as faults and not as an ambiguity. Thus, the erring validator is penalized for it in the following cases.

1. If a validator identifies the lowercase of letter "L" in "collocation" as a digit '1', or the digit '1' in number '10' as letter 'l' it is considered as fault and not an ambiguity. The validator will be penalized by deducting a value equivalent to weight of the character from its credits.
2. In a sequential numbering of items, if a validator wrongly identifies a sequential number, say after '9' it takes '10'to be 'L0' or 'lo', it will also be taken as fault and attract penalty.

Corresponding author: Omoniyi Wale Salami
✉
Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(1), MARCH, 2025
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Ranking Validators Using Perception Parameters Weights

The examples described with characters in Fig. 1 illustrate factors that can affect correct perception of values by validators. The factors can manifest in different ways with different objects. The factors will now be used to rank validators and for resolving differences among validators perceptions in the subsequent part of this section.

Based on the psychology principle of perceptual constancy [41], Salami *et al*., [33] proposed PoCCS for recording the number of successful consensus processes a validator has done as a measure of its experience. This will be further improved here for ranking validators as their relative level of trustworthiness. The weights of identity stimuli correctly perceived by an O are used to award credits P to it as follows:

$$P = \frac{\sum_{1,1}^{R,C} W_{S\mathfrak{f}\,r,c}}{|W_{S\mathfrak{f}}|}, P \in \mathbb{N} \quad 10$$

In (10) $\left|W_{S\mathfrak{f}\,r,c}\right|$ is the total number of stimuli in $W_{S\mathfrak{f}\,r,c}$. P is rounded to the nearest integer.

Implementation of the New Solution

PoCCS was implemented in this work for keeping records of a validator's performance in consensus processes that yield collective and non-collective consensus. When the consensus is collective the PoCCS was computed as prescribed in [33]. But in the implementation explained in this section PoCCS was used for awarding credits to validators when there are differences in their responses.

The credits awarded to a validator is an indication of correctness of its response. Two tests, audio transcription and OCR, were conducted in this. The tests designs were based on the fact that, to extract correct facts, multiple nodes examine the same value and give their responses in a blockchain consensus process. In this test 10 laptops were used for transcribing the same audio recording in audio test, they were also used to extract characters from an image scanned with the same scanner using each laptop in turn in OCR test. The results obtained from the tests were used to compute PoCCS.

Experimental Setup: Audio Transcription Test

The validating nodes were arranged at equidistance around the speaker from which the recorded speech was played as shown in Fig. 2. The microphone volume was set at 50% for the validating devices. Other settings were left as default. The speech was recorded and played from a speaker for all the nodes to transcribe.

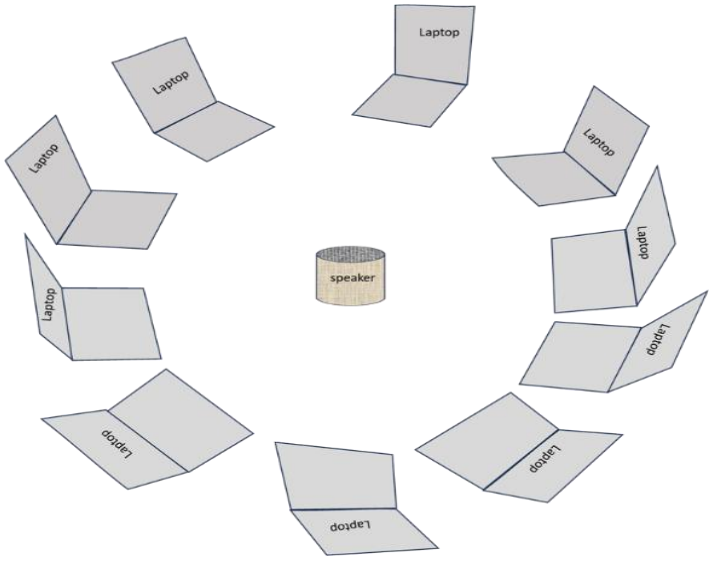


Figure 2: The arrangement of validating nodes around the source of audio sound for transcription

Corresponding author: Omoniyi Wale Salami
✉
Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(1), MARCH, 2025
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

The original texts of the speech played to the nodes was;

These tests only quantify the perception levels of individual validators to be able to ascertain their ability to examine a value correctly. It does not include designing of an application for perception and does not test a particular perception software or an artificial intelligence algorithm.
The validators are labelled Val1, Val2 up to Val10 in this test.
In this transcription test, the following statement is used to assess the ability to transcribe speech correctly under the same conditions by different systems that are using the same software.
The test statement is quoted below:
"He came up with an idea which I did not agree with initially because I wasn't on the same page as him at first. But when he explained further, I keyed in."

The speech text consists of 752 characters, punctuation marks, newline carriages and letters of the words in red are inclusive. There 125 words in the speech. The characters with red colour are considered more important because;

1. Punctuation marks enhance the understanding of the contexts of words and emotion of the speaker.
2. Some words that have similar sounds in singular and plural forms may be easily missed in a dictation.
3. Words that the last letter is pronounced silently may be difficult to get in a dictation.

The characters with more weights were 48 altogether. Saliency was neglected. Thus, the weighing factor was

$$\delta_{s_f} = \frac{752 - 48}{752} = 0.936170213$$

The words are arranged into R X C = 25 X 5 matrix of the words weights W. The base value $w_S = 5$.

$$W_{Sf_{r,c}} = 5 \times e^{(0.936170213)}$$
$$= 12.75097992 \cong 13$$

$W_{Sf_{1,1}}$, $W_{Sf_{1,2}}$, $W_{Sf_{14,2}}$, $W_{Sf_{25,4}}$, and $W_{Sf_{25,5}}$ have weight 13 while others have weight 5. Only words are considered in this test to simplify the illustration of the usage of the method.

The Tests Materials

Hardware

The list of the hardware devices used for the tests are listed in Table II.

Table II: Hardware Components used for the Experiment

Item	Quantity
Laptop PCs	10
MP3 Player	1

Val1 was a HP Zbook 15 G5 Core i7, 32 GB RAM with Nvidia GPU Graphics 4 GB Video memory, Val4 was a Dell Latitude E7450 Core i5, 16 GB RAM with Intel GPU graphics 4 GB Video memory. Val2, val3, Val5, and Val6 were HP 2000 Core i3 notebook PC with Intel HD Graphics. The remaining Val7, Val8, and Val9 were Dell latitude 3340 Core i3 G5, and val10 was a HP Elitebook 840 G3, Core i5 with Intel HD Graphics. Val1 have windows 11 Pro, others systems have Windows 10 Pro. They are all 64-bit operating system, x64-based processor

Software

Table III contains the list of the application software used for executing the desired tasks in the tests.

Table III: Software Components used for the Experiment

Item	Type
Browser	Chrome
Google Speech-to-Text App	Online

Tests Methodology

The Google online speech-to-text app was opened on the devices using the same Google account, Fig. 3. Speech recording in the speech-to-text was started on the devices just before the recorded speech was start on the MP3 player. The speech recording was stopped and submitted for transcription immediately the speech playing completed.

Corresponding author: Omoniyi Wale Salami
✉
Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(1), MARCH, 2025
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

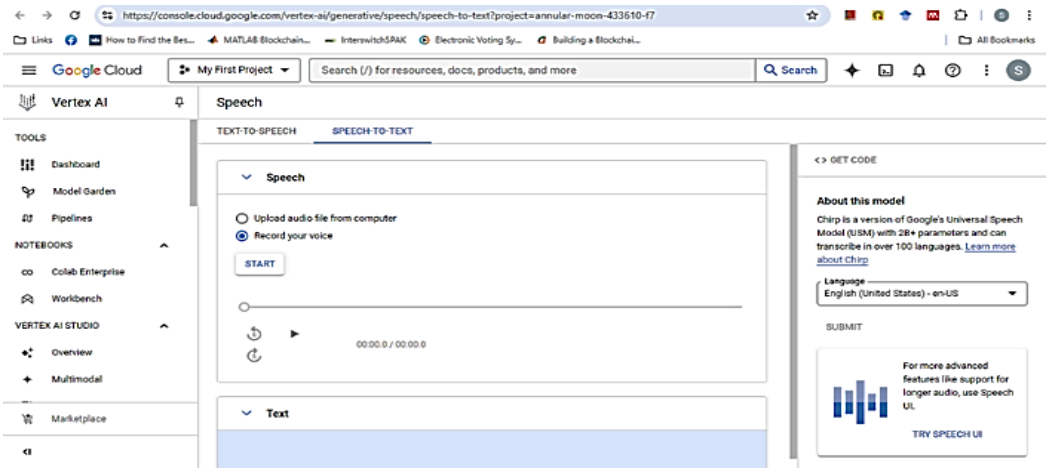


Figure 3: The Google speech-to-text app used for capturing texts of the recorded speech played to validators

RESULTS AND DISCUSSION

The results obtained from tests conducted on PoCCS and on other two other similar literature, Green-PoW [27] and e-PoS [29], used to compare PoCCS performances are presented in this section. The results are first presented and then the implications of using the solutions for forensic investigations are discussed.

The Tests Results

PoCCS

The details of each validator's response including the hash digest of the actual speech and that of the validator's response, the errors in each response, and points scored by each validator are recorded in Table IV for PoCCS.

Table IV: PoCCS Mining Tests Results

Validator	Original Message Hash	Response Hash	Wrongly Captured	Score Points (752)
Val1	ec4acfa8770ebd91d9405b2b61d026ad1b3e389ae7a58b4243ad59220fbc569d	653707e765464ddb6bb7f7a7eb85b64a18c5c736269e3a76218a45f4b7a92ea4	These tests only: this test only same conditions: same condition **I keyed in: i came in**	708
Val2	ec4acfa8770ebd91d9405b2b61d026ad1b3e389ae7a58b4243ad59220fbc569d	13a24942f4e4d3136e69c08bb9a04ebd6125785bb2ce46f63d17df251d040def	These tests: this test in this test: in this text i keyedin: i keyedin	708
Val3	ec4acfa8770ebd91d9405b2b61d026ad1b3e389ae7a58b4243ad59220fbc569d	7bc07d2ffcabb1911f43c11e021ad84ffd61a95cc159736e5bd533a603151d88	These tests: this test Perception levels of: perceprion level of i keyedin: i keel in	695
Val4	ec4acfa8770ebd91d9405b2b61d026ad1b3e389ae7a58b4243ad59220fbc569d	64cea58b34c7ce28a3b3686ffd5c599e9c2f98b4143396937b7992f6b09e32c0	Perception levels of: persuasion levels of	747

Corresponding author: Omoniyi Wale Salami
✉
Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.

Validator	Original Message Hash	Response Hash	Wrongly Captured	Score Points (752)
Val1	ec4acfa8770ebd91d9405b2b61d026ad1b3e389ae7a58b4243ad59220fbc569d	653707e765464ddb6bb7f7a7eb85b64a18c5c736269e3a76218a45f4b7a92ea4	These tests only: this test only same conditions: same condition **I keyed in: i came in**	708
Val5	ec4acfa8770ebd91d9405b2b61d026ad1b3e389ae7a58b4243ad59220fbc569d	31c7ca960e3985b0a148329f0d950dbb6f75e98432e76f555902b85b89911250	Assess: ascesis Designing: disiring	734
Val6	ec4acfa8770ebd91d9405b2b61d026ad1b3e389ae7a58b4243ad59220fbc569d	bf9645d88ae1cf8dbf434297b9ee8eb3f568a3c06866ce26598edf1a4caa30c6	These tests only: this test	734
Val7	ec4acfa8770ebd91d9405b2b61d026ad1b3e389ae7a58b4243ad59220fbc569d	44a8f87a41fea080f906f729db1ac9c3053bcefbdad39a5983fc8cb79e7683a8	I keyed in: i came in	739
Val8	ec4acfa8770ebd91d9405b2b61d026ad1b3e389ae7a58b4243ad59220fbc569d	4093f9671726255f387c80d607f2419667e54a72a82c3d21b7d2dd1d3db15a51	These tests only: this test only Used to assess: used to access I keyed in: i killed him	703
Val9	ec4acfa8770ebd91d9405b2b61d026ad1b3e389ae7a58b4243ad59220fbc569d	87a0f0b1f042735f8bafeaf1435df091806aeec8a007b926936783e004339ec8	These tests only: this test only I keyed in: i came in	713
Val10	ec4acfa8770ebd91d9405b2b61d026ad1b3e389ae7a58b4243ad59220fbc569d	acc64f1508c61fadd78f550e189ae27194cb85069ae1910b70fe7a09d583ef65	For Perception: for persuasion I keyed in: i came in	726

Green-PoW and e-PoS results

The same experimental setup was used to test Green-PoW [27], a Proof-of-Work based consensus, and e-PoS [29], a Proof-of-Stake based consensus. The same speech was played and captured by the same set of validating nodes. These consensus solutions were used to mine the extracted texts in turns. The results of obtained for Green-PoW and e-PoS and that of the validator with the highest points in PoCCS tests are presented in Table V.

Corresponding author: Omoniyi Wale Salami
✉
Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(1), MARCH, 2025
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Table V. Green-PoW and E-PoS Mining Tests Results

Original Message Hash	Green-PoW Mined Block	e-PoW Mined Block	PoCCS Mined Block
	Miner: Val1	**Miner: Consensus of majority**	**Miner:** Val4
Original Message Hash ec4acfa8770ebd91d9405b2b61d026ad1b3e389ae7a58b4243ad59220fbc569d	**Block Hash** 00000019d8186226e7f0f73cc8592b9a7270b32e410614f03a1fcf220ba99dc9	**Block Hash** 0eb35950a1458a238ab4329893342e96cbe371c2682b6daaa728af753d6e3707	**Block Hash** f4f2b52baaf3a9fc74d3daf625686011c7b8a422d8e2dd8d1e92f761fabfc672
	Nonce 461854		**Nonce** 2911
Original Value These tests only quantify the perception levels of individual validators to be able to ascertain their ability to examine a value correctly. It does not include designing of an application for perception and does not test a particular perception software or an artificial intelligence algorithm. The validators are labelled Val1, Val2 up to Val10 in this test. In this transcription test, the following statement is used to assess the ability to transcribe speech correctly under the same conditions by different systems that are using the same software. The test statement is quoted below: "He came up with an idea which I did not agree with initially because I wasn't on the same page as him at first. But when he explained further, I keyed in."	**Mined Value** this test only quantify the perception levels of individual validators to be able to ascertain their ability to examine a value correctly it does not include designing of an application for persuasion and does not test a particular perception software or an artificial intelligence algorithm the validators are labelled value one value two up to value ten in this test in this transcription test the following statement is used to assess the ability to transcribe speech correctly under the same conditions by different systems that are using the same software the test statement is quoted below he came up with an idea which i did not agree with initially because i wasn't on the same pace as him at first but when he explained further i came in	**Consensus Value** this test only quantify the perception levels of individual validators to be able to ascertain their ability to examine a value correctly it does not include designing of an application for persuasion and does not test a particular perception software or an artificial intelligence algorithm the validators are labelled value one value two up to value ten in this test in this transcription test the following statement is used to assess the ability to transcribe speech correctly under the same conditions by different systems that are using the same software the test statement is quoted below he came up with an idea which i did not agree with initially because i wasn't on the same pace as him at first but when he explained further i came in	**Consensus Value** these tests only quantify the persuasion levels of individual validators to be able to ascertain their ability to examine a value correctly it does not include designing of an application for persuasion and does not test a particular perception software or an artificial intelligence algorithm the validators are labelled value one value two up to value ten in this test in this transcription test the following statement is used to assess the ability to transcribe speech correctly under the same condition by different systems that are using the same software the test statement is quoted below he came up with an idea which i did not agree with initially because i wasn't on the same pace as him at first but when he explained further i keyed in[747]

Corresponding author: Omoniyi Wale Salami
✉
Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.

The Discussion of the Results

The free version of Google speech-to-text used in the tests produced transcribed texts in lowercase letters. Also, it did not assigned punctuation or quotation marks. No new line was inserted in the transcribed texts. Therefore, only words spellings, the use of words, or mis-captured words were considered in the transcribed texts. The words that were misspelled or mis-captured are shown with red font-colour in the transcribed texts. Those in blue font-colour are numbers or abbreviated words that were spelled in full.

In the mining process the words are the transactions in the block. In Green-PoW the responses of validators that find the target hash before others formed the block. Val1 returned the target hash with prefix '00000' faster than others. The block it mined contains more errors than the block produced by PoCCS. The e-PoS block was made up of words that were returned by most validators, i.e., majority consensus. The e-PoS mined block is similar to that of Green-PoS and contained similar errors. The mined block by PoCCS contained the least errors because its transactions were selected to be the closest match to the actual value based on veridical evaluation method.

The PoCCS attached each validator's score at the end of its response insides square brackets. Also, the validator's consistency history is inserted in the hash of its response. The val4 score that was 747 points out of 752 was attached to the end of its response. Its consistency is was 693_{10}, which is $2b5_{16}$, was inserted in the hash of its response at index 4, which was Val4's serial number in consensus members list. This information can give an investigator the level of confidence to put in the data. The Collaborative Integrity Verification Consensus Mechanism (CIVCM) [34] that PoCCS works with normal keep the copies of the validators' responses to make them accessible to the investigator when needed. The investigator may review the errors in the PoCCS results by comparing what other PoCCS validators returned for the value and be able to deduce correct value.

The severity of the consequences of the wrongly captured words by Green-PoW and e-PoW is very high. When "I keyed in" was changed to "I came in" the meaning changed from "I concurred" to "I interjected" which are almost opposite to each other. The situation is worse when there is no other means to verify it.

CONCLUSION

A response scoring method in Proof-of-Congruity Consensus Scheme was proposed in this work to give the level of confidence of the response at a glance. It makes PoCCS to be more suitable for use for forensic investigation than other consensus mechanism.

Future Work

Further improvements will be made to PoCCS ranking method so that it can also show the degree of deviation of the response from the original value.

REFERENCES

[1] B. Lashkari and P. Musilek, "A Comprehensive Review of Blockchain Consensus Mechanisms," in *IEEE Access*, 2021, vol. 9, pp. 43620–43652. doi: 10.1109/ACCESS.2021.3065880.

[2] C. Zhang, C. Wu, and X. Wang, "Overview of blockchain consensus mechanism," *ACM Int. Conf. Proceeding Ser.*, pp. 7–12, 2020, doi: 10.1145/3404512.3404522.

[3] F. Ma *et al.*, "LOKI: State-Aware Fuzzing Framework for the Implementation of Blockchain Consensus Protocols," *30th Annu. Netw. Distrib. Syst. Secur. Symp. NDSS 2023*, no. March, 2023, doi: 10.14722/ndss.2023.24078.

[4] H. Anwar, "Distributed Ledger Technology: Where Technological Revolution Starts," *101blockchains.com*, 2019. https://101blockchains.com/distributed-ledger-technology-dlt/#3 (accessed Aug. 02, 2024).

[5] F. Kahmann, F. Honecker, J. Dreyer, M. Fischer, and R. Tönjes, "Performance Comparison of Directed Acyclic Graph-Based Distributed Ledgers and Blockchain Platforms," *Computers*, vol. 12, no. 257, 2023, doi: 10.3390/computers12120257.

[6] L. Amherd, S.-N. Li, and C. J. Tessone, "Centralised or Decentralised? Data Analysis of Transaction Network of Hedera Hashgraph,"

Corresponding author: Omoniyi Wale Salami
✉
Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.

arXiv e-print, vol. arXiv:2311, no. 1, pp. 1–15, 2023, doi: 10.5195/LEDGER.20XX.XXX.
[7] R. T. Frahat, M. M. Monowar, and S. M. Buhari, "Secure and Scalable Trust Management Model for IoT P2P Network," in *2nd International Conference on Computer Applications and Information Security, ICCAIS 2019*, 2019, pp. 1–6. doi: 10.1109/CAIS.2019.8769467.
[8] D. G. Bundi, S. M. Mutua, and S. M. Karume, "Underlying Consensus Algorithms, Architectures and Data Structures in Distributed Ledger Technologies Applications," *ICONIC Res. Eng. JOURNALS*, vol. 7, no. 7, pp. 449–460, 2024.
[9] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 1982, doi: 10.1145/357172.357176.
[10] L. Lamport and D. Equipment, "The Part-Time Parliament," *ACM Trans. Comput. Syst.*, vol. 16, no. 2, pp. 133–169, 1998.
[11] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *Proceedings of the 2014 USENIX Annual Technical Conference, USENIX ATC 2014*, 2014, pp. 305–319.
[12] D. Avelãs, H. Heydari, E. Alchieri, T. Distler, and A. Bessani, "Probabilistic Byzantine Fault Tolerance (Extended Version)," in *ACM Symposium on Principles of Distributed Computing (PODC '24)*, 2024, vol. 1, no. 1, pp. 1–29. doi: 10.1145/3662158.3662810.
[13] S. Duan and Y. Huang, "Byzantine Fault Tolerance with Non-Determinism, Revisited," *Cryptol. ePrint Arch.*, vol. 2024, no. 134, pp. 1–16, 2024.
[14] D. S. Antunes *et al.*, "Alea-BFT : Practical Asynchronous Byzantine Fault Tolerance," in *Proceedings of the 21st USENIX Symposium on Networked Systems Design and Implementation*, 2024, pp. 313–328.
[15] S. Duan *et al.*, "Dashing and Star: Byzantine Fault Tolerance with Weak Certificates," in *EuroSys '24: Proceedings of the Nineteenth European Conference on Computer Systems*, 2024, pp. 250–264. doi: 10.1145/3627703.3650073.
[16] M. M. Jalalzai, J. Niu, C. Feng, and F. Gai, "Fast-HotStuff: A Fast and Robust BFT Protocol for Blockchains," *IEEE Trans. Dependable Secur. Comput.*, vol. 20, no. 4, pp. 1–17, 2023, doi: 10.1109/TDSC.2023.3308848.
[17] S. Duan, S. Peisert, and K. N. Levitt, "Hbft: Speculative Byzantine fault tolerance with minimum cost," *IEEE Trans. Dependable Secur. Comput.*, vol. 12, no. 1, pp. 58–70, Jan. 2015, doi: 10.1109/TDSC.2014.2312331.
[18] C. M and L. B, "Practical byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, 2002.
[19] R. Kotla, L. Alvisi, M. Dahlin, A. Clement, and E. Wong, "Zyzzyva: Speculative Byzantine Fault Tolerance," *ACM Trans. Comput. Syst.*, vol. 27, no. 4, pp. 7:1-7:39, Jan. 2009, doi: 10.1145/1658357.1658358.
[20] J. Skrzypczak, … F. S.-I. T. on, and U. 2020, "RMWPaxos: fault-tolerant in-place consensus sequences," *IEEE Trans. PARALLEL Distrib. Syst.*, vol. 31, no. 10, pp. 2392–2405, 2020.
[21] Y. A. Liu, S. Chand, and S. D. Stoller, "Moderately complex paxos made simple: High-level executable specification of distributed algorithms," *PervasiveHealth Pervasive Comput. Technol. Healthc.*, no. March, 2019, doi: 10.1145/3354166.3354180.
[22] R. Van Renesse and D. Altinbuken, "Paxos made moderately complex," *ACM Comput. Surv.*, vol. 47, no. 3, pp. 1–36, 2015, doi: 10.1145/2673577.
[23] M. Javad, A. Sujaya, M. Divyakant, A. Amr, and E. Abbadi, "Seemore: A fault-tolerant protocol for hybrid cloud environments," in *IEEE 36th International Conference on Data Engineering (ICDE)*, 2020, pp. 1345–1356.
[24] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Decentralized Bus. Rev.*, vol. 21260, pp. 1–9, 2008.
[25] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger," *Ethereum Proj. yellow Pap.*, vol. 151, pp. 1–32, 2014.
[26] P. Vasin, "BlackCoin ' s Proof-of-Stake Protocol v2," *whitpaper*, 2014. https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf (accessed Apr. 07, 2022).
[27] N. Lasla, L. Al-Sahan, M. Abdallah, and M. Younis, "Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm," *Comput. Networks*, vol. 214, no. 109118, pp. 1–11, 2020, doi: 10.1016/j.comnet.2022.109118.

Corresponding author: Omoniyi Wale Salami
✉
Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.

[28] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, H. Karimipour, and S. R. Karizno, "SLPoW: Secure and Low Latency Proof of Work Protocol for Blockchain in Green IoT Networks," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020, pp. 1–5. doi: 10.1109/VTC2020-Spring48590.2020.9129462.

[29] M. Saad, Z. Qin, K. Ren, D. H. Nyang, and D. Mohaisen, "E-PoS: Making Proof-of-Stake Decentralized and Fair," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 8, pp. 1961–1973, 2021, doi: 10.1109/TPDS.2020.3048853.

[30] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, 2014, doi: 10.1145/2695533.2695545.

[31] S. Costantini, G. De Gasperis, and R. Olivieri, *Digital forensics and investigations meet artificial intelligence*, Mathematic. Springer Nature Switzerland AG, 2019. doi: 10.1007/s10472-019-09632-y.

[32] O. W. Salami, M. B. Abdulrazaq, E. A. Adedokun, and B. Yahaya, "CICM: A Collaborative Integrity Checking Blockchain Consensus Mechanism for Preserving the Originality of Data the Cloud for Forensic Investigation," *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 7, no. 1, pp. 55–68, Feb. 2022, doi: 10.22219/KINETIK.V7I1.1378.

[33] O. W. Salami, M. B. Abdulrazaq, Y. Basira, and B. Adebiyi, "Proof-of-Congruity Consensus Scheme: A Blockchain Consensus Mechanism for Mining Potential Data for Forensic Analysis," *Covenant J. Informatics Commun. Technol.*, vol. 12, no. 1, pp. 1–15, 2024.

[34] W. Salami, Omoniyi, B. Abdulrazaq, Muhammad, A. Adedokun, Emmanuel, B. Yahaya, and A. Umar, "Blockchain Collaborative Integrity Verification Consensus Mechanism for Avoiding Repudiation in E-Voting System."

[35] F. Daryabar, A. Dehghantanha, and K.-K. R. Choo, "Cloud storage forensics: MEGA as a case study," *Aust. J. Forensic Sci.*, vol. 49, no. 3, pp. 344–357, May 2017, doi: 10.1080/00450618.2016.1153714.

[36] J. Schneider, J. Wolf, and F. Freiling, "Tampering with Digital Evidence is Hard: The Case of Main Memory Images," *Digit. Investig.*, vol. 32, no. (2020) 300924, pp. S1–S9, 2020, doi: 10.1016/j.fsidi.2020.300924.

[37] L. Pasquale, D. Alrajeh, C. Peersman, T. Tun, B. Nuseibeh, and A. Rashid, "Towards forensic-ready software systems," in *ICSE-NIER'18: 2018 ACM/IEEE 40th International Conference on Software Engineering: New Ideas and Emerging Results Towards*, 2018, pp. 9–12. doi: 10.1145/3183399.3183426.

[38] L. Floridi, "Artificial Intelligence, Deepfakes and a Future of Ectypes," *Philos. Technol.*, vol. 31, no. 3, pp. 317–321, 2018, doi: 10.1007/s13347-018-0325-3.

[39] C. B. Mueller, L. C. Kirkpatrick, and L. Richter, "§7.7 Reliability Standard (Daubert, Frye)," Washington, DC, 2018–71, 2018. doi: 10.2139/ssrn.3277067.

[40] S. Qian, Y. Shi, H. Wu, J. Liu, and W. Zhang, "An adaptive enhancement algorithm based on visual saliency for low illumination images," *Appl. Intell.*, vol. 52, no. 2, pp. 1770–1792, 2022, doi: 10.1007/s10489-021-02466-4.

[41] A. Buccella and A. Chemero, "Reconsidering perceptual constancy," *Philos. Psychol.*, vol. 35, no. 7, pp. 1057–1071, 2022, doi: 10.1080/09515089.2022.2038122.

Corresponding author: Omoniyi Wale Salami
✉
Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.