Covenant Journal of Informatics & Communication Technology. Vol. 12, No. 2, December, 2024
ISSN: *print* 2354 – 3566 *electronics* 2354 – 3507 DOI:

An Open Access Journal Available Online

Improved Blockchain Collaborative Integrity Verification Consensus with Consistent Nuanced Cues for Multicriteria Decision Making

Omoniyi Wale Salami[1], Emmanuel Adewale Adedokun[2], Busayo Adebiyi[3], Risikat Folashade Adebiyi[4]

Department of Computer Engineering, Faculty of Engineering, Ahmadu Bello University, Zaria, Nigeria[1,2,4].
Department of Computer Engineering, Federal University Lokoja, Nigeria[3]
salamiow@gmail.com[1], adewaleadedokun@yahoo.com[2],
busayo.adebiyi@fulokoja.edu.ng[3], rfadebiyi@abu.edu.ng[4]
0000-0003-0589-0535[1], 0000-0002-4220-2562[2], 0000-0002-1917-6896[2], 0000-0002-2555-4777[4]

Received: 10.07.2024 **Accepted: 21.12.2024**

Publication: December 2024

Abstract— Decision making is an essential task that human undertake frequently. Decision is taken before actions. It may catalyze or preclude the success of an action depending on its rightness. Therefore, it is vital to the success of human endeavors. Naturally, making good decisions require personal wisdom or wisdom gotten from advice. Decision is often data driven because the facts on which the decision is based is usually generated from data. Genuine data generates correct facts. Computer is now being used to aid good decision. A computer assisted decision-making process is proposed in this work. The proposed method combined blockchain collaborative integrity verification consensus mechanism (CIVCM) and analytical hierarchy process (AHP) for thorough assessment of available alternatives to achieve a well-informed decision. This solution outperformed other solutions used for evaluating it by returning unambiguous results in the evaluation tests because of its working concept that avoids faults. The results shows that the solution is a better choice for high accuracy demanding applications.

Keywords/Index Terms— Multicriteria Decision Making, Consensus Mechanism, Blockchain, AHP, Gestalt Psychology

1. Introduction

Distributed ledger technology (DLT) comprises of a number of nodes who examine a value individually to find out if it conforms to desired standards. They agree on the most popular view among the examiners (Lashkari & Musilek, 2021). Blockchain is a DLT that has become a popular tool in data engineering because of the immutability it provides for securing data. Genuineness of the data depends on the correctness of the collective consensus of the nodes that examined it. Blockchain consensus protocols basically operates on fault tolerant algorithms. Most of the existing consensus mechanisms were developed using the principle of Byzantine Generals Problem (BGP) (Lamport et al., 1982). Paxos Parliamentary system, also known as The Part-Time Parliament (Lamport & Equipment, 1998), was used to develop crash fault tolerance (CFT) (Ongaro & Ousterhout, 2014). But CFT is not as popular as BFT because of the complexity of Paxos Parliamentary system. The Byzantine Fault Tolerance (BFT) consensus protocol was based on the BGP (Lamport et al., 1982). It gained more attention than CFT protocol because it was found to be more workable. Some of consensus protocols that were developed using BFT are Alea-BFT (Antunes et al., 2024), Byzantine Fault Tolerant with Non-Determinism (Duan & Huang, 2024), Dashing and Star (Duan et al., 2024), and Probabilistic Byzantine Fault Tolerant (Avelãs et al., 2024). Others include Fast-HotStuff (Jalalzai et al., 2023), Hbft (Duan et al., 2015), Practical Byzantine Fault Tolerant (PBFT) (M & B, 2002), and Zyzzyva (Kotla et al., 2009). Those that are based on CFT consensus protocols are RMWPaxos (Skrzypczak et al., 2020), Moderately complex paxos made simple (Y. A. Liu et al., 2019), and Paxos made moderately complex, (Van Renesse & Altinbuken, 2015). There are consensus protocols, like Seemore (Javad et al., 2020), that combined BFT and CFT to develop hybrid solutions. They exploit the benefits of both principles. BFT and CFT protocols ensure that a system functions in the presence of malicious nodes. Thus, they tolerate some faults in their operations. Another type of consensus protocols are proof-based mechanisms used for validation of transactions. The proof-based consensus mechanisms guarantee agreement among the validating nodes. Proof-of-Work (PoW) (Nakamoto, 2008) and Proof-of-Stake (PoS) (G. Wood, 2014; Vasin, 2014) are popular examples of proof-based consensus mechanisms. PoW creates a difficulty hash target that requires great computing efforts to accomplish. The first node to solve the hash target creates the new transaction. On the other hand, PoS is a risk-based consensus mechanism. A validator with largest stakes is elected as primary and creates transactions. It loses it stakes if it creates a wrong transaction. Several other proof-based consensus mechanisms have now been developed. Existing proof-based consensus mechanisms use either the working principle of PoW, e.g., (Lasla et al., 2020; Yazdinejad et al., 2020), or that of PoS, e.g., (Saad et al., 2021). Others combine the principles of PoW and PoS, e.g., (Bentov et al., 2014). Proof-based consensus mechanisms provide immutable security to data in distributed ledgers.

The consensus of nodes that are validating transactions should guaranty a validated value as reliable. It should also maintain correctness and consistent structure of blocks in blockchain (C. Zhang et al., 2020). Coherence of responses of the validators can be a guide for determining reliability of their collective consensus if it conforms with vital metrics that dictate

genuineness of the value. Blockchain consistency is usually considered based on the uniformity of blocks' structure by maintaining a single chain (Altarawneh & Skjellum, 2020; Alwabel & Kwon, 2021; Kalajdjieski et al., 2023; Kiffer et al., 2018; Zhao et al., 2024). There are situations when accuracy of the contents of the transactions are more important than the structure of the blocks, irrespective of if there are branches on the chain or not. Researchers have identified the limitations of fault tolerant algorithms in different uses of blockchain and proposed improvements to make it suitable for different applications (Altarawneh & Skjellum, 2020). Consensus mechanisms are at the core of blockchain creating the security it provides (Lashkari & Musilek, 2021). Blockchain is now being used for securing data in wider areas beyond the scope of cryptocurrency. The level of strict compliance to desired standards for data required in some applications of blockchain are higher than others. Data accuracy is verified when being captured and mined in blockchain by consensus mechanisms. Fault tolerance systems accept deficiencies that are below set thresholds in data. Forensic investigation is a critical process that puts premium on data correctness as much as its immutability (Costantini et al., 2019). Forensic analysis is basically used to discern ambiguities and deduce genuine convincing facts from events of an incident. Current blockchain consensus protocols that tolerate some level of faults could inherently introduce error in data that may alter investigation results. Those that work based on difficulty of computation may be too slow for extracting evidence. While those consensus mechanisms requiring risking stakes may not encourage miners to ensure correctness of data but to be more concerned with securing their stakes. Thus, they are not suitable for mining forensic evidence. There should be means of evaluating the consistency of consensus reached by the validating nodes. This is to ensure that the consensus truly established the authenticity of the secured data before applying immutability to it.

(Salami et al., 2022a) designed a new consensus solution for ascertaining the accuracy data before mining it in blockchain. The authors proposed a solution called "Collaborative Integrity Checking Blockchain Consensus Mechanism" (CICM) for ensuring that originality of data is correctly preserved in a distributed ledger. CICM was developed on the principles of perception. It uses consistency history (CH) for validating nodes. But CH was created only for nodes that are involved in collective consensus when all validators agreed on a value. When one or more nodes disagree with others the CH for all the nodes that participated will not be updated. CH was used as Proof-of-Congruity Consensus. CH was used to authenticate a validator's response and confirm the validator as a genuine member of the consensus team. The validators in a consensus process that successfully yield a single collective agreement earn credit points recorded as consistency history. But the results of a consensus process where the validators concluded differently on a value will only be recorded in an auxiliary ledger. No credits will be awarded to the validators involved in such process. This work proposes a multicriteria decision making (MCDM) method using Saaty's analytic hierarchy process (AHP) (Saaty, 1987) for gauging hierarchy of different responses from validators in a CICM consensus team. It is expedient for organizing group decision through qualitative and quantitative assessments. While CICM was

used to determine the veridical consistency of the validators' responses to the original value, AHP was used for organising the hierarchy of responses to determine the best among them. This solution harmonises validators' responses based on their consistency with the original value. It was designed for making the best decisions based on available alternatives and choosing the best among available options. The solution was tested with choosing the most efficient optical character recognition (OCR) software for a Court of Law. The software should be able to correctly extract texts from documents wrote out in longhand and save them as electronic files.

The solution proposed in this work uses the principle of perception of a blockchain consensus to determine the parameter for comparing alternatives for achieving optimum decision.

The structure of this paper used the format in (Misra, 2021). The rest of the paper are section II where the design methodology used for this work is explained, section III contains the review of related works, while section IV contains the discussion of the results of the tests carried out on the proposed solution. Conclusion is presented in section V. Future work is in section VI.

2. Design Methodology

The design of the solution proposed in this work is explained in this section. The solution uses the principle of CIVCM protocol expressed in (Salami et al., 2022b)

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

Equation (1) (Salami et al., 2022b) is an improved version of the equation for CICM in (Salami et al., 2022a). Additional case, $0<F(id)<1$, that was not in (Salami et al., 2022a) is added in (1). Only the topmost and bottom cases were defined in (Salami et al., 2022a). This work uses CIVCM (Salami et al., 2022b) for its consensus process. The validators in the blockchain consensus are the six OCR applications tested, Table 1. The validators responses are the texts extracted from the images loaded into the OCR applications. In line with the principle of CIVCM for veridical consistency verification of validators responses, the characters of the original message in the image are the cues. The responses are collated and compared for match with the original texts.

The case study for this work is the selection of an efficient OCR software for extracting texts of very important documents for urgent needs. A court or Police station often require such services. It is important that the software be able to extract the texts accurately without differences between the extracted information and the content of the original document. In this experiment, the proposed solution was used in the process for selecting the best OCR software for a court. The six mobile OCR software in Table I were used in this experiment. The acronyms used for them in the table were adopted here for the purpose of identifications in this work.

Table 1 The Mobile OCR Applications Tested

S/N	Software	Acronym
1	Google Lens	GL
2	OCR Text Scanner	OCRTS
3	OCR-Image to text	OCRX
4	OCR Image to Text Converter	OCRTC
5	Text Scanner	TS
6	Text Extractor	TE

In both (Salami et al., 2022a) and (Salami et al., 2022b) validators earn credits only when $F(id) = 1$ for all for all of them. This paper designs an award system for the case when $0 \leq F(id) < 1$ for different validators and maintain the award system for the case $F(id)=1$. The award system is based on evaluation of consistency of their responses with the original message.

Before using the application for extraction of texts from longhand writings they were first tested with a short message in a pre-experimental test. This is to confirm if the applications have the facilities for recognizing longhand writing texts or only recognize typed texts. The results of the pre-experimental are presented in Figure 1.

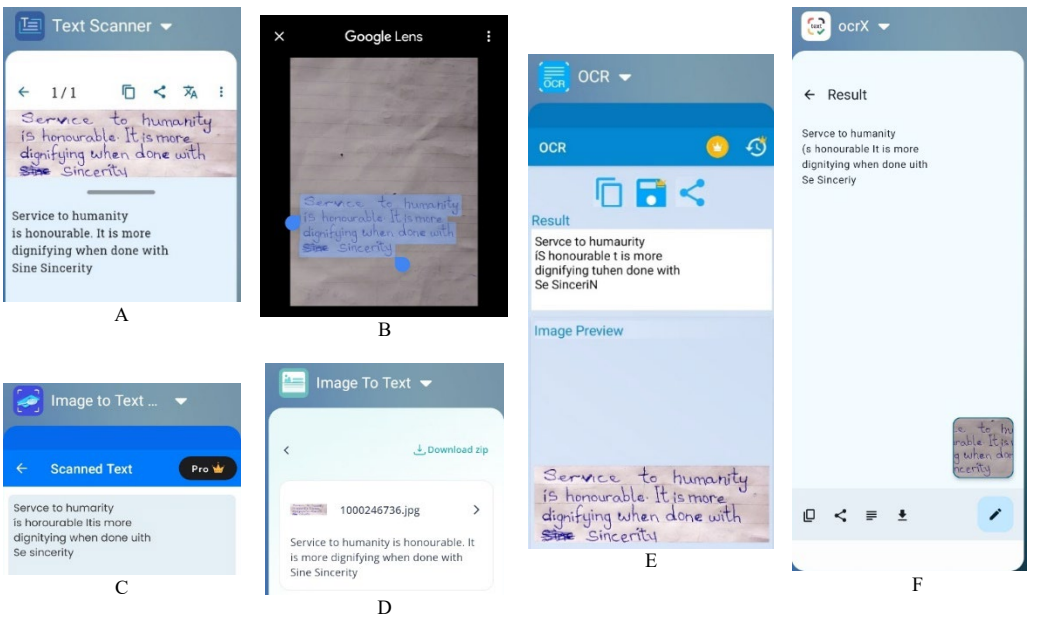


Figure 1: Screenshots of each application interface showing an image and the texts extracted from it by each OCR application

2.1. Experimental Setup

The steps used for testing the performance were as follows.

2.1.1. Texts extraction from images

The software tested were installed on mobile devices, Figure 2. The images of different messages wrote out by longhand writing by different people were taken with a phone AI camera. The images of the handwritten texts were loaded into the applications in the mobile devices. The texts extracted from the images by each application were recorded. The longhand writings in the different images presented different difficulties to the applications in recognising the texts them. Thus, the images were ranked with different points, Table 2.

Points are awarded to each validator based on percentage of the texts of its response that match original texts. Six criteria were set and awarded points that indicate relative importance of a criterion with respect to others. The points for the items; validators, criteria, and alternatives, used for different matrices in AHP were derived based on the correctness of the responses. This is a deviation from the normal method of intuiting on points pairwise comparison matrix (PCM) based on considered relative impact of the items on each other. A pragmatic approach was used in this work for setting up the PCMs.

2.1.2. Topology for blockchain consensus process

The nodes involved in the blockchain collaborative integrity consensus process were arranged as shown in Figure 2A. The topology was developed with Cisco Packet Tracer version 8.2.2.0400 (Salami et al., 2022b). The OCR applications were installed on the smartphones and tablets shown in the figure. The laptop is server and provided collaboration platform for the mobile devices. The laptop and mobile devices were connected through the access point (AP). There were six images each containing different message from others to avoid learning the texts and reproducing it in consequent attempts by an application. Each mobile device picks an image of document containing longhand writing in turns from the laptop and load it to the OCR application installed on it. They submit the extracted texts from the images back to the laptop. The applications pick another image of the messages when they submitted their extracted texts until each of them processes all the six different images as shown in the cycle in Figure 2B.

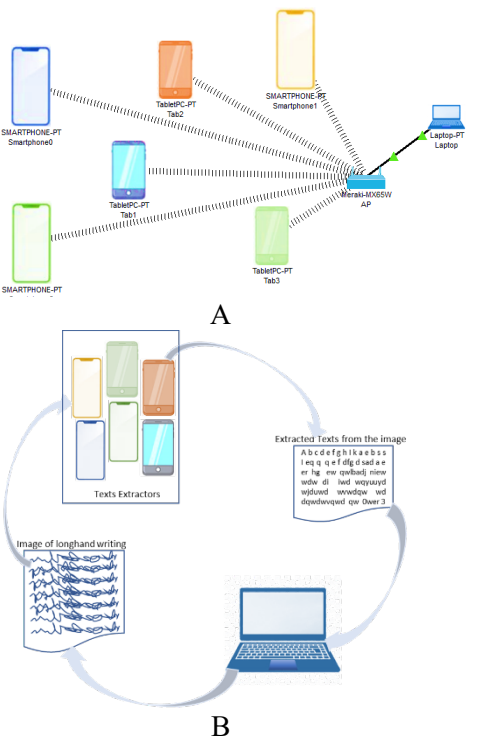


Figure 2: Images of handwritings that were used for testing the mobile OCR applications text extraction capabilities.

2.1.3. Data mining and blocks creation

CIVCM used for the consensus process in this experiment was designed with self-check and collaborative critiquing mechanisms. The nodes use the mechanisms to crosscheck their responses for errors by comparing it with other nodes responses and correct it as may be necessary. But the use case employed in this experiment does not require the applications to compare their responses with other applications results. This is because they were tested for their ability to provide correct results on their own. The corrective mechanisms in CIVCM were not used for this experiment. It could be useful in situations in which achieving accurate results from the collective effort of the nodes is desired. Based on the CIVCM protocol, the laptop mines the texts extracted by each application as transactions in a block for each cycle of the process when an image is processed. The block created on the laptop is shared to the nodes. Each node also computes the hash of its extracted texts and use it confirm that its texts were correctly mined in the blockchain. They used the confirmed blocks to create their local copies of the distributed ledger. The assessment of the responses from each application was carried out on the laptop by comparing the extracted texts from each node with the original texts of the message in the image. The number of texts in the original messages and the number of wrongly captured texts from the images of the messages by each application are compiled in Table 2.

Table 2 Result of the Texts Extraction Tests

Img	Pnt	#Chrs	Error by each app (Wrong|Right)											
			GL		OCRTS		OCRX		OCRTC		TS		TE	
			Wr	Rt	Wr	Rt	Wr	Rt	Wr	Rt	Wr	Rt	Wr	Rt
A	*1*	399	*11*	*388*	*97*	*302*	*174*	*225*	*7*	*392*	*205*	*194*	*273*	*126*
B	2	454	68	386	102	352	218	236	116	338	231	223	186	268
F	3	340	18	322	40	300	180	160	52	288	101	239	116	224
C	4	344	12	332	36	308	153	191	45	299	98	246	112	232
J	5	338	38	300	182	156	267	71	43	295	162	176	167	171
H	6	347	15	332	154	193	159	188	24	323	171	176	173	174
E	7	347	30	317	168	179	161	186	38	309	173	174	169	178
D	8	298	30	268	27	271	32	266	30	268	51	247	48	250
G	8	302	25	277	72	230	260	42	65	237	38	264	70	232
I	9	450	172	278	101	349	272	178	118	332	176	274	120	330

2.2. Evaluating Responses with Analytic Hierachy Process

In Table 2, Img is image, Pnt is the point assigned an image, and #Chrs is the number of letters in the original message. Wr is the number of wrongly captured letters. Rt is number of correctly capture letters. Analytic hierarchy process is a popular method for MCDM used for determining the best option consistency among available alternatives based on index (CI). AHP uses pairwise comparison to establish relations within a data structure. The data for comparison is established in the following according to the AHP computation steps in (Saaty, 1987).

2.2.1. Preliminary Setup

The parameters for calculating (1) are first defined.

$$X_s = \begin{bmatrix} f_{11} & \cdots & f_{1C} \\ \vdots & \cdots & \vdots \\ f_{1R} & \cdots & f_{RC} \end{bmatrix} \quad (2)$$

The elements in row R and column C of matrix X_s in □2□ are the identifying parameters on the original value, X, to be validated. They form the criteria to be used for validating a value by a blockchain consensus team. CIVCM accepts the responses that match (2) among responses from the validators (Salami et al., 2022b).

2.2.2. Assign Weights to Validation Criteria

The criteria are compared in pairs. A point indicating the priority of one criterion over the other is assigned to a criterion that it is compared with another. Saaty's criterion (Saaty, 1987) for assigning points is used to assign the priority points to the criteria. The priority points were used to generate the PCM for the criteria.

$$F_{PC} = \begin{bmatrix} 1 & \cdots & f_{CR} \\ \vdots & \cdots & \vdots \\ \frac{1}{f_{RC}} & \cdots & 1 \end{bmatrix} \quad (3)$$

In (3) the reciprocal of the point assigned to an element f_{RC} of the PCM was automatically assigned to its transpose element f_{CR}, ($f_{CR} = \frac{1}{f_{RC}}$). Table 2 was used to calculate points assigned in a PCM matrix in this work based on the working principle of the solution it is prepared for. The CIVCM working principle that match responses to the cues of the original value is used for calculating PCM for the proposed solution. Similarly, the working principles of other solutions used to benchmark the proposed solution in the tests conducted here are used for preparing their PCM.

$$w_f = [w_{f1} \quad \cdots \quad w_{fn}] \quad (4)$$

The matrix in (4) was used in AHP process to compute the weights vector, w_f in (4), for the validation criteria and the validators

responses in the following.

The criteria used for grading the ability of a software to recognize characters efficiently are defined using legibility of the texts (Polat & Kesik, 2023) and saliency (Qian et al., 2022) of the image in the criteria vector cv,

Cv = [brightness, contrast, letter-form, slant, spacing, alinement] (5)

Brightness: proper illumination of the texts-images.

Contrast: the measure distinctive visibility of the letters in the image

Letter form: well-formed letters to represent the alphabet correctly without causing ambiguities

Slant: the state of the letters in the writing been upright on the lines as they should be.

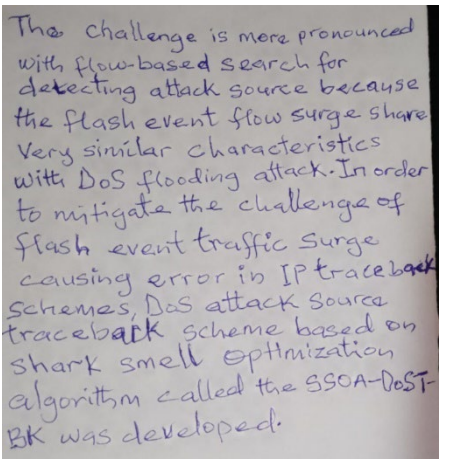
Spacing: the measure of letters and words in the writing having appropriate spacings between them.

Alinement: the state of lines of the writing been horizontally straight and properly arranged.

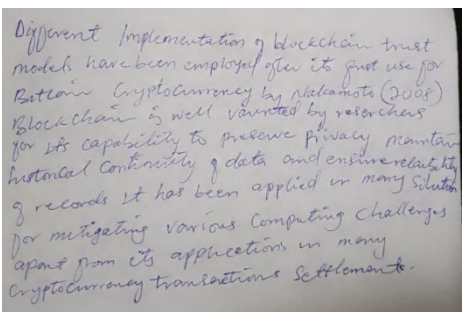
The higher the point assigned to an element of Cv in (5) the more the efforts it is assumed to impose on the viewer to see the letters correctly. In other words, those attributes that could make it more difficult to recognize the letters correctly are assigned higher points. The points are awarded to discriminate those applications that are more robust for extracting texts from wider variations of handwritings than those that can only extract easily recognisable letters from images. Some sample of images used are shown in Figure 3 to illustrate the criteria with the differences between the images. When the points were assigned, it gives the following Cv vectors

Cv = [8, 7, 6, 4, 3, 2] (6)

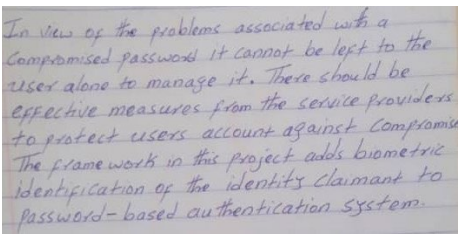
The same criteria were used for all the applications in the tests. This gives the same basis for comparing the applications performances.



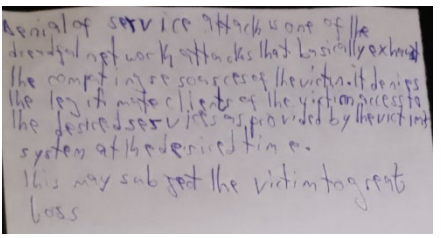
(A) A clear but average contrast image with well-spaced, upright letters and acceptable letter-form and alinement. Adequate for human reading.



(B) A faintly clear image with low contrast containing cursive handwriting. Letter-form, uprightness, spacing, and alinement are not bad. May be more difficult than (A) for human to read.



(C) A well written message but low brightness image



(D) The most difficult sample in the test score low in all the criteria, except alinement.

Figure 3: Images of handwritings that were used for testing the mobile OCR applications text extraction capabilities.

2.2.3. Comparing the Coherence of Validators Responses to Each Validation Factor

The same procedures used for computing comparison matrix and weights vector for validation criteria were used to prepare similar matrices for validators' responses. The validators responses are the alternatives in the AHP process for this work. Comparison matrix was generated for the validators' responses for each criterion. The number of comparison matrices generated is equal to the number of criteria considered. Weights of each response for each criterion was computed for the corresponding comparison matrix to obtain vectors of weights for all the responses. The weights vectors for the responses were used to calculate their consistency. The details of the method for computing the PCM for the responses is given in the following.

CIVCM principle emphasised on veridical comparison of responses with the original value. The maximum Saaty's point is 9. Thus, from Table 2,

$$P_{pcm} = \frac{Correctly\ captured\ letters\ (W_r)}{Total\ letters\ in\ the\ original\ message\ (\#\text{Chrs})} \times 9 \quad (7)$$

The average of P_{pcm} for the 10 images was calculated and rounded to the nearest integer. The average was used to build the PCM matrix for the responses with the values in Table 3.

Average P_{pcm} values for the responses GL=9, OCRTS=7, OCRX=4, OCRTC=7, TS=6 TE=6.

Table 3 The pairwise comparison matrix for the responses

	GL	OCRTS	OCRX	OCRTC	TS	TE
GL	1	2	5	2	3	3
OCRTS	2	1	5	1	3	3
OCRX	5	5	1	5	5	5
OCRTC	2	1	5	1	2	2
TS	3	3	5	2	1	1
TE	3	3	5	2	1	1

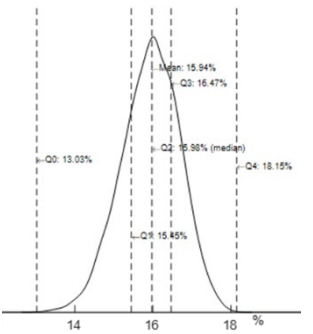
Values in Table 3 were computed by subtracting the smaller average P_{pcm} value among the two alternatives comparing from the larger one. In Saaty's points, 1 indicates two compared alternatives are equally likely, 2 indicates almost equally likely, 3 indicates a slightly higher influence of one alternative over the other, and so on for 4 to 9 (Saaty, 1987). When

the difference between a pair of average P_{pcm} values is zero (0) a Saaty's point 1 is entered in Table 3 for it. If the difference was 1 a Saaty's point 2 is entered for it. For other differences between pairs of average P_{pcm} values corresponding Saaty's points were entered for them. Thus, the comparison matrices were formed based on the values obtained for the alternatives in the tests conducted. The values represent their performance metrics.

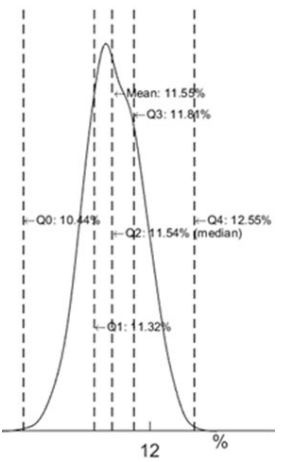
2.2.4. Hierarchical ordering of the Validators' Responses

The AHP generates weights for the alternatives as measures of their relative preferences over others for the choice they are considered for. The products of their weights and their average P_{pcm} values were used to determine their suitability for the intended use. This is reasonable because P_{pcm} was a pragmatically determined measure of relative performance of an alternative compared to others. While the weight is an analytically determined measure of their relevance to the need compared to others. The products of the metrics yield the correct priority of each alternative over the others.

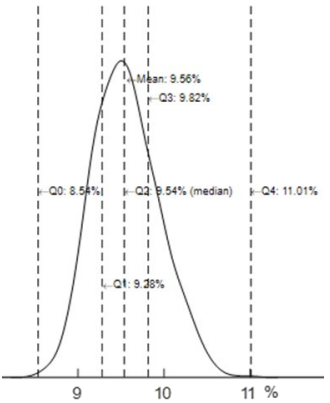
The graph of weight distributions for each software are presented in Figure 4. The plot shows the quartile ranges, the mean and median of the distribution. Weights were calculated for each software under each of the criteria. The weight for a software under a criterion indicates the robustness of the software for that criterion. Figure 4 shows the plot of all the weights of each software for different criteria. For the vector; $P_{pcm} = [9; 7; 4; 7; 6; 6]$, the product of weight matrix and P_{pcm} vector yielded hierarchy vector $H_{vec} = [12.77;\ 8.99;\ 6.83;\ 4.46;\ 3.96;\ 2.30]$. Table 4 contains the relative weights of the responses under each criterion and the overall hierarchical weight for each software. GL, the Google OCR software known as Google Lens, has the highest hierarchical score. The table shows the relative robustness of each software under the conditions of each criterion as compared to other alternatives. It could be seen from the table that Google Lens scaled better than other software in all the conditions.



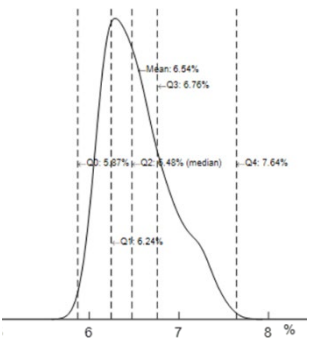
(A) Weight distribution for Google



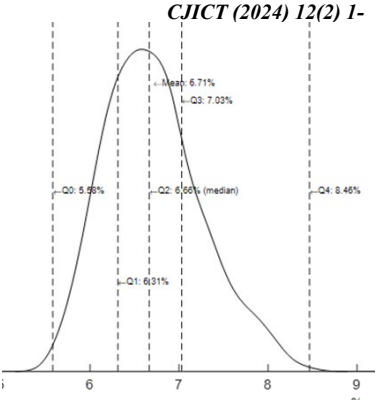
(B) Weight distribution for OCRTS



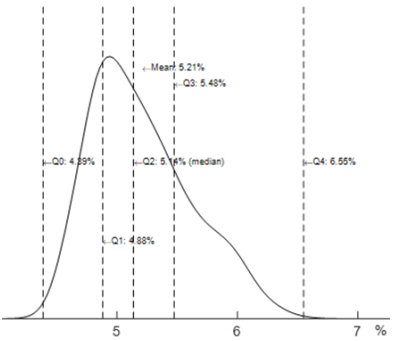
(C) Weight distribution for OCRX



(D) Weight distribution for OCRTC



(E) Weight distribution for TS software



(F) Weight distribution for TE software

Figure 4: The chart of the weight distributions for different OCR software.

Table 4 Weights of responses under each criteria

	brightness	contrast	letter-form	slant	spacing	alinement	H_{vec}
GL	*0.34*	*0.33*	*0.40*	*0.34*	*0.37*	*0.20*	*12.77*
OCRTS	*0.29*	*0.21*	*0.20*	*0.21*	*0.24*	*0.20*	*8.99*
OCRX	*0.17*	*0.20*	*0.13*	*0.20*	*0.15*	*0.18*	*6.83*
OCRTC	*0.10*	*0.09*	*0.2*	*0.09*	*0.09*	*0.16*	*4.46*
TS	*0.06*	*0.13*	*0.10*	*0.13*	*0.06*	*0.14*	*3.96*
TE	*0.04*	*0.04*	*0.03*	*0.04*	*0.09*	*0.12*	*2.30*

Similar tests were conducted with ProBFT (Avelãs et al., 2024) and CF-BFT (Z. Zhang et al., 2023). The two works are BFT solutions. They work on assumptions that majority of trusted nodes will always produce correct results. Thus, the formular for calculating the PCM element for them was formulated as follows;

$$E_{pcm} = \frac{Correct\ Chrs\ returned\ by\ majority}{Total\ Chrs\ returned\ by\ a\ node\ (R_t+W_r)} \times 9 \quad (8)$$

In (6) the "Correct Chrs returned by majority" are the correctly captured letters that are common in the responses from the majority. Equation (6) was used for each of the responses from ProBFT nodes. CF-BFT does its consensus in two stages; Check_BFT and Fast_BFT. In the Check_BFT, (6) was used for individual node reponses. While Fast_BFT it was used for the responses from the primary on behalf of all nodes. The results obtained from the two solutions in comparison with the results of the proposed solution are presented in Table 5.

3. Related Works

The nodes in a distributed ledger technology (DLT) consensus team confirm the authenticity of value to be stored in the ledger. Consensus protocols are used in different DLTs, including Hashgraph, Directed Acyclic Graph (DAG), Holochain, and Tempo, to achieve needed security for data (Anwar, 2019). The required security would be peculiar to the type of use case for which the DLT is employed. (Çolak et al., 2020) used blockchain as a multicriteria decision making technology for determining appropriate supply chain management for business sectors. They used Hesitant Fuzzy Analytic Hierarchy Process (HF-AHP) and Hesitant Fuzzy Technique for Order Preference by Similarity to Ideal Solution (HF-TOPSIS) methods with 5 main criteria and 17 sub-criteria for hierarchical organization of different sectors considered as alternatives. (Erol et al., 2022) used Fuzzy SWARA-COPRAS-EDAS and COPELAND-based framework for determining the feasible function of sustainable supply chain for employing blockchain in industry. They were able to determine the best and the areas where blockchain may be useful for

implementation in supply chain. (Tavana et al., 2023) noted the challenge faced when deciding to select appropriate platform for blockchain technology and Internet-of-Things implementation in supply chain network. They proposed a method for approaching this challenge using appropriate criteria in Weighted Influence Non-linear Gauge System (WINGS) and VIseKriterijumska Optimizacija I Kompromisno Resenje (VIKOR) technique for determining the suitable platform. The challenge of deciding a suitable blockchain technology for a particular was addressed in (J. Liu et al., 2024) using heterogeneous multi-criteria Decision-Making. Criteria for deciding suitable blockchain were chosen from analysis of popular blockchain technologies.

Table 5 Results of the tested solutions.

Solutions	**Result**		**Remark**
Proposed Solution	GL	12.77	Google Lens was distinctively returned as the most suitable software of choice
	OCRTS	8.99	
	OCRX	6.83	
	OCRTC	4.46	
	TS	3.96	
	TE	2.30	
ProBFT	GL	7.80	Three software; GL, OCRTS and OCRX were returned to be chosen. But OCRTS and OCRX were second and third runner up after the GL in the proposed solutions results. This software uses majority view for decision rather than actual critique of the value. Majority view may lack specificity.
	OCRTS	7.80	
	OCRX	7.80	
	OCRTC	5.31	
	TS	4.51	
	TE	1.62	
CF-BFT	GL	7.64	Three software; GL, OCRTC, and TE were also returned here. OCRTS took second position but TE performed worst in the proposed solution results. This software uses majority view for decision rather than actual critique of
	OCRTS	4.23	
	OCRX	3.71	
	OCRTC	7.64	
	TS	3.77	
	TE	7.64	

			the value. Majority view may lack specificity.

They then used closeness degree metric from AHP-EWM for ranking blockchain alternatives in their order of suitability. Similarly, (Lai & Liao, 2021) developed solution for evaluation of blockchain platforms to enhance decision on choosing a suitable one. Their solution used linguistic D numbers (LDNs), double normalization-based multiple aggregation (DNMA), and Criteria Importance Through Inter-criteria Correlation (CRITIC) methods. Computer aided decision-making solutions were also developed by (Filatovas et al., 2022; Moghaddasi & Masdari, 2024) to aid selection of suitable consensus mechanism for blockchain systems, and IoT task offloading respectively. The paradigm shift in application of blockchain technology is growing wider. It is now becoming popular in multicriteria decision making. The solution proposed in this work contributes to the growing application of blockchain technology in multicriteria decision making by extending its uses to the choice of the best application for taking very vital records.

4. Results and Discussion

The solution proposed in this work performed holistic analysis of the value considered and reported a clear result. The process of determining the correct result by the proposed solution include thorough examination of the value in consideration. All relevant attributes that were necessary for correct view of the value were considered during the assessment of the value. The results returned were consistent. The chart of the weights of the considered alternatives showed that the returned option, Google Lens, was the most consistent in all the tests. Its weights distribution was the most symmetrical and closest to perfect binomial distribution among the weight distribution charts of the alternatives. Other solution tested together with the proposed solution returned three out of six options as the correct results. This could be confusing. Thus, the proposed solution performed better than the other solutions in the tests.

5. Conclusion

This work proposed the use of CIVCM (Salami et al., 2022b) for use with the AHP method of MCDM for making correct decision when faced with the challenge of making choice among multiple options. The solution proposed in this work was tested with the challenge of choosing the best software for use as OCR for extracting texts from handwritten texts. Six software were tested with 10 different handwritings of various degree of difficulties for recognition. Two other similar solution were tested together with the solution proposed in this work. This solution was able to return a single software that was most suitable for the intended tasks. Other two solutions returned multiple results that could confuse the user.

6. Future Work

Collaborative integrity verification consensus mechanism is a new blockchain consensus solution that is suitable for wide application areas. Further work will explore the use of CIVCM in other areas requiring highly accurate results. The improvement that may be required to make it suitable for other applications will also be observed and applied.

References

Altarawneh, A., & Skjellum, A. (2020). The security ingredients for correct and byzantine fault-tolerant blockchain consensus algorithms. *2020 International Symposium on Networks, Computers and Communications (ISNCC 2020)*, 1–9. https://doi.org/10.1109/ISNCC49221.2020.9297326

Alwabel, M., & Kwon, Y. (2021). Blockchain Consistency Check Protocol for Improved Reliability. *Computer Systems Science and Engineering*, *36*(2), 281–292. https://doi.org/10.32604/csse.2021.014630

Antunes, D. S., Oliveira, A. N., Breda, A., Franco, M. G., Moniz, H., Rodrigues, R., Superior, I., Ulisboa, T., & Clara, S. (2024). Alea-BFT : Practical Asynchronous Byzantine Fault Tolerance. In L. Vanbever & I. Zhang (Eds.), *Proceedings of the 21st USENIX Symposium on Networked Systems Design and Implementation* (pp. 313–328). USENIX Association.

Anwar, H. (2019). *Distributed Ledger Technology: Where Technological Revolution Starts*. 101blockchains.Com. https://101blockchains.com/distributed-ledger-technology-dlt/#3

Avelãs, D., Heydari, H., Alchieri, E., Distler, T., & Bessani, A. (2024). Probabilistic Byzantine Fault Tolerance (Extended Version). *ACM Symposium on Principles of Distributed Computing (PODC '24)*, *1*(1), 1–29. https://doi.org/10.1145/3662158.3662810

Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. *ACM SIGMETRICS Performance Evaluation Review*, *42*(3), 34–37. https://doi.org/10.1145/2695533.2695545

Çolak, M., Kaya, I., Özkan, B., Budak, A., & Karaşan, A. (2020). A multi-criteria evaluation model based on hesitant fuzzy sets for blockchain technology in supply chain management. *Journal of Intelligent & Fuzzy Systems*, *38*(1), 935–946. https://doi.org/10.3233/JIFS-179460

Costantini, S., De Gasperis, G., & Olivieri, R. (2019). Digital forensics and investigations meet artificial intelligence. In *Annals of Mathematics and Artificial Intelligence* (Mathematic). Springer Nature Switzerland AG. https://doi.org/10.1007/s10472-019-09632-y

Duan, S., & Huang, Y. (2024). Byzantine Fault Tolerance with Non-Determinism, Revisited. *Cryptology EPrint Archive*, *2024*(134), 1–16.

Duan, S., Peisert, S., & Levitt, K. N. (2015). Hbft: Speculative Byzantine fault tolerance with minimum cost. *IEEE Transactions on Dependable and Secure Computing*, *12*(1), 58–70. https://doi.org/10.1109/TDSC.2014.2312331

Duan, S., Zhang, H., Sui, X., Huang, B., Mu, C., Di, G., & Wang, X. (2024). Dashing and Star: Byzantine Fault Tolerance with Weak Certificates. *EuroSys '24: Proceedings of the Nineteenth European Conference on Computer Systems*, 250–264. https://doi.org/10.1145/3627703.365

0073

Erol, I., Ar, I. M., & Peker, I. (2022). Scrutinizing blockchain applicability in sustainable supply chains through an integrated fuzzy multi-criteria decision making framework. *Applied Soft Computing*, *116*, 108331. https://doi.org/10.1016/J.ASOC.2021.108331

Filatovas, E., Marcozzi, M., Mostarda, L., & Paulavičius, R. (2022). A MCDM-based framework for blockchain consensus protocol selection. *Expert Systems with Applications*, *204*, 117609. https://doi.org/10.1016/J.ESWA.2022.117609

G. Wood. (2014). Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, *151*, 1–32.

Jalalzai, M. M., Niu, J., Feng, C., & Gai, F. (2023). Fast-HotStuff: A Fast and Robust BFT Protocol for Blockchains. *IEEE Transactions on Dependable and Secure Computing*, *20*(4), 1–17. https://doi.org/10.1109/TDSC.2023.3308848

Javad, M., Sujaya, A., Divyakant, M., Amr, A., & Abbadi, E. (2020). Seemore: A fault-tolerant protocol for hybrid cloud environments. *IEEE 36th International Conference on Data Engineering (ICDE)*, 1345–1356.

Kalajdjieski, J., Raikwar, M., Arsov, N., Velinov, G., & Gligoroski, D. (2023). Databases fit for blockchain technology: A complete overview. *Blockchain: Research and Applications*, *4*(1), 1–18. https://doi.org/10.1016/j.bcra.2022.100116

Kiffer, L., Rajaraman, R., & Shelat, A. (2018). A Better Method to Analyze Blockchain Consistency∗. *Proceedings of the ACM Conference on Computer and Communications Security*, 729–744. https://doi.org/10.1145/3243734.3243814

Kotla, R., Alvisi, L., Dahlin, M., Clement, A., & Wong, E. (2009). Zyzzyva: Speculative Byzantine Fault Tolerance. *ACM Transactions on Computer Systems (TOCS)*, *27*(4), 7:1-7:39. https://doi.org/10.1145/1658357.1658358

Lai, H., & Liao, H. (2021). A multi-criteria decision making method based on DNMA and CRITIC with linguistic D numbers for blockchain platform evaluation. *Engineering Applications of Artificial Intelligence*, *101*, 104200. https://doi.org/10.1016/J.ENGAPPAI.2021.104200

Lamport, L., & Equipment, D. (1998). The Part-Time Parliament. *ACM Transactions on Computer Systems*, *16*(2), 133–169.

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, *4*(3), 382–401. https://doi.org/10.1145/357172.357176

Lashkari, B., & Musilek, P. (2021). A Comprehensive Review of Blockchain Consensus Mechanisms. *IEEE Access*, *9*, 43620–43652. https://doi.org/10.1109/ACCESS.2021.3065880

Lasla, N., Al-Sahan, L., Abdallah, M., & Younis, M. (2020). Green-PoW: An

energy-efficient blockchain Proof-of-Work consensus algorithm. *Computer Networks*, *214*(109118), 1–11. https://doi.org/10.1016/j.comnet.2022.109118

Liu, J., Zhang, Q., Xie, M., Lin, M., & Xu, Z. (2024). A blockchain platform selection method with heterogeneous multi-criteria Decision-Making based on hybrid distance measures and an AHP-EWM weight method. *Expert Systems with Applications*, *256*, 124910. https://doi.org/10.1016/J.ESWA.2024.124910

Liu, Y. A., Chand, S., & Stoller, S. D. (2019). Moderately complex paxos made simple: High-level executable specification of distributed algorithms. *PervasiveHealth: Pervasive Computing Technologies for Healthcare*, *March*. https://doi.org/10.1145/3354166.3354180

M, C., & B, L. (2002). Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems*, *20*(4), 398–461.

Misra, S. (2021). A Step by Step Guide for Choosing Project Topics and Writing Research Papers in ICT Related Disciplines. *Communications in Computer and Information Science*, *1350*, 727–744. https://doi.org/10.1007/978-3-030-69143-1

Moghaddasi, K., & Masdari, M. (2024). Blockchain-driven optimization of IoT in mobile edge computing environment with deep reinforcement learning and multi-criteria decision-making techniques. *Cluster Computing*, *27*(4), 4385–4413. https://doi.org/10.1007/S10586-023-04195-4/METRICS

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Decentralized Business Review*, *21260*, 1–9.

Ongaro, D., & Ousterhout, J. (2014). In search of an understandable consensus algorithm. *Proceedings of the 2014 USENIX Annual Technical Conference, USENIX ATC 2014*, 305–319.

Polat, İ., & Kesik, C. (2023). An Analysis of Handwriting Legibility of First Grade Students by School Starting Age. *International Journal of Progressive Education*, *19*(5). https://doi.org/10.29329/ijpe.2023.603.13

Qian, S., Shi, Y., Wu, H., Liu, J., & Zhang, W. (2022). An adaptive enhancement algorithm based on visual saliency for low illumination images. *Applied Intelligence*, *52*(2), 1770–1792. https://doi.org/10.1007/s10489-021-02466-4

Saad, M., Qin, Z., Ren, K., Nyang, D. H., & Mohaisen, D. (2021). E-PoS: Making Proof-of-Stake Decentralized and Fair. *IEEE Transactions on Parallel and Distributed Systems*, *32*(8), 1961–1973. https://doi.org/10.1109/TPDS.2020.3048853

Saaty, R. W. (1987). The analytic hierarchy process-what it is and how it is used. *Mathematical Modelling*, *9*(3–5), 161–176. https://doi.org/10.1016/0270-0255(87)90473-8

Salami, O. W., Abdulrazaq, M. B., Adedokun, E. A., & Yahaya, B. (2022a). CICM: A Collaborative Integrity Checking Blockchain Consensus Mechanism for Preserving the Originality of Data the Cloud for Forensic Investigation. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, *7*(1), 55–68. https://doi.org/10.22219/KINETIK.V7I1.1378

Salami, O. W., Abdulrazaq, M. B., Adedokun, E. A., & Yahaya, B. (2022b). Collaborative Integrity Verification for Blockchain-Based Cloud Forensic Readiness Data Protection. *Communications in Computer and Information Science*, *1547 CCIS*, 138–152. https://doi.org/10.1007/978-3-030-95630-1_10

Skrzypczak, J., … F. S.-I. T. on, & 2020, U. (2020). RMWPaxos: fault-tolerant in-place consensus sequences. *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, *31*(10), 2392–2405.

Tavana, M., Khalili Nasr, A., Ahmadabadi, A. B., Amiri, A. S., & Mina, H. (2023). An interval multi-criteria decision-making model for evaluating blockchain-IoT technology in supply chain networks. *Internet of Things*, *22*, 100786. https://doi.org/10.1016/J.IOT.2023.100786

Van Renesse, R., & Altinbuken, D. (2015). Paxos made moderately complex. *ACM Computing Surveys*, *47*(3), 1–36. https://doi.org/10.1145/2673577

Vasin, P. (2014). *BlackCoin ' s Proof-of-Stake Protocol v2*. Whitpaper. https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf

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

Zhang, C., Wu, C., & Wang, X. (2020). Overview of blockchain consensus mechanism. *ACM International Conference Proceeding Series*, 7–12. https://doi.org/10.1145/3404512.3404522

Zhang, Z., Wang, F., Liu, Y., Lu, Y., & Liu, X. (2023). CF-BFT: A Dual-Mode Byzantine Fault-Tolerant Protocol Based on Node Authentication. *Computers, Materials and Continua*, *76*(3), 3113–3129. https://doi.org/10.32604/cmc.2023.040600

Zhao, J., Zhang, Y., Jiang, J., Hua, Z., & Xiang, Y. (2024). A secure dynamic cross-chain decentralized data consistency verification model. *Journal of King Saud University - Computer and Information Sciences*, *36*(1), 1–13. https://doi.org/10.1016/j.jksuci.2023.101897