Hindawi
Mathematical Problems in Engineering
Volume 2022, Article ID 3429528, 7 pages
https://doi.org/10.1155/2022/3429528

Research Article

Construction and Application of a New Metal Random Matrix-Based Theory in a Numerical Phantom of the Metaverse NFT

Huan wang

College of Art and Design, Shanghai Normal University Tianhua College, Shanghai 201815, China

Correspondence should be addressed to Huan wang; wh2063@sthu.edu.cn

Received 13 June 2022; Revised 28 July 2022; Accepted 8 August 2022; Published 9 September 2022

Academic Editor: Ning Cao

As the metaverse is hot, nonhomogenized tokens (NFT) as digital artwork identifiers present different characteristics and application values from other homogenized tokens, and their use for copyright verification will suffer from the problems of storage space limitation and data verification reliance on database, this study designs an NFT digital copyright authentication model for textual works. To cater for the uncontrollability of conventional Hash algorithms in stream matching due to the high conflict rate, a new random matrix theory is applied to propose a new Hash algorithm, which is used on the block structure of NFT credential authentication, while extending the block structure so that the data within the work is completely stored in the blockchain with NFT as the credential, allowing the database to store the work data in a relatively safe manner. The verification of the work data has the immutability and unique cryptographic solution of NFT. The NFT-based digital model collects TR information and conducts 30 tests, and the average test time for generating blocks is 0.53 s. Through the block query for detection, 248,655 words have exceeded the number of words of an article, and the consumption time is only 0.23s, to meet the customer's real-time query requirements for the system. According to the overhead ratio, the record storage expenditure is about 2-3 times of the text storage expenditure, the work storage expenditure, and the storage expenditure for storing 240,000 words for authentication is about 3720 KB.

1. Introduction

The metaverse [1] is gradually moving from a concept into people's lives, and some technologies or definitions related to it, such as artificial intelligence, VR, and blockchain are gradually gaining attention, and some technologies have started to influence people's lives. Nonhomogeneous tokens (NFT), as a typical representative, are widely used in the blockchain field [2], which can be represented as a unique identifier for digital artworks as commodity entries, that is, digital authentication of artistic goods such as music, videos, and pictures [3]. Blockchain technology led by NFT can achieve traceability, tamper-evident, and distributed storage based on which a blockchain digital model can be established for copyright management and maintenance with NFT technology [4].

In the study of establishing a model for digital authentication of textual copyright, some people combine elliptic curves with cryptography [5] to realise digital authentication of textual works. The digital fingerprint is generated by splicing cryptography, attaching author information and timestamp, and then written into the blocks of the blockchain [6]; copyright information should contain the name of the power owner and the work, which is combined with the registration time as the digital fingerprint and then sealed in the blockchain model to ensure the credibility of the copyright information [7]; to ensure the originality of the text copyright, the digital abstract of the content can be extracted for confirmation on the chain [8]; the hash (Hash) method [9] is used to generate a copyright code in the form of Hash for the main information contained in the original content and store it in the block to ensure that

it cannot be changed, thus ensuring the validity of the copyright of the work [10]. Domestic technology companies introduce MD5 code technology [11] to obtain blockchain IDs, author names, work designations, and timestamps to generate electronic certificates together with MD5 codes [12], and the tangible interests of text creators are maintained.

NFT is heavily used in blockchain technology as a cryptocurrency identifier for artistic digital goods [13]. Digital text copyright is protected by generating feature values (Hash values) to be written to the blockchain, but the Hash function generates conflicts when performing the matching of electronic data streams due to the long bits of each rule, which induce conflicts when mapping them into shorter codes, and the long computation time. Based on this problem, this paper improves the Hash function and introduces a new theory of random matrices to achieve low-conflict Hash features when the numerical model based on the universe NFT is studied.

2. Modifying the Hash Function and Blockchain Authentication Model for Text Works

The digital authentication model needs to ensure that the messages received by both sides are consistent. When the hash function is used to provide message authentication function, the hash function value is usually called message digest. The sender uses this function to calculate a set of Hash values according to the message to be sent and then sends the Hash value and the message together. The receiver performs the same Hash calculation on the message after receiving it and compares the result with the received Hash value. If there is no match, the receiver infers that the message (or Hash value) has been distorted.

2.1. (一) Hash Function Based on the New Theory of Random Matrices. Suppose the bit length of each element a of a set A is M, and the bit length of each element b of a small set B is m ($M \geq m$), and currently, the bits of each element M of set A are divided into e blocks, denoted as $a_1, a_2, \ldots, a_e$, where the number of bits per block after partition is m, then $e = M/\mathrm{m}$; at this time, the space of the set B is represented as $r = 2^m$, the space of the set A is represented as r^e, and $r \leq r^e$. Suppose there exists a random matrix $\mathbf{R_{re}}$, the individual elements of the matrix are a random number w in the range $[0, r)$, the binary number of w is represented as $w = p_1 p_2 p_3 \ldots p_m$, which satisfies the random distribution $P\{p_i = 0\} = P\{p_i = 1\} = 0.5$ ($i = 1 \ldots m$).

Introducing the new theory of random matrices for Hash (RMhash), the function first sets up a random matrix $\mathbf{R_{re}}$, then divides an element of the set A into e blocks, and each block lends itself to a high matching hash function that transforms it into an element of the $\mathbf{R_{re}}$ matrix and then performs a logical iso-or operation on the e random numbers to obtain a Hash value, then the above assumptions can be expressed as

$$\begin{aligned} b &= g(f(a_i)), \\ f&: a_i -> \{R_{i1}, R_{i2}, \ldots, R_{ie}\}, \\ g&: |f(a_1)||f(a_2)|\ldots|f(a_i)|\ldots|f(a_e)|. \end{aligned} \tag{1}$$

The function f generates an element of the matrix R_{ia} by performing a single high matching hash operation with the input function a_i ($1 \leq i \leq e$). The function g performs a dissimilarity operation on multiple element values transformed by the function f. The generated values of the RMhash satisfy a uniform distribution of $[0, r)$. The individual elements a of a set A are denoted as a_1、a_2....a_e, with a total of e blocks ($0 \leq a_i \leq r, 0 \leq i \leq e$). The $e!$ elements of ai are arbitrarily arranged, and e of the blocks are selected for logical operations, and they generate values with the same Hash value, a phenomenon called proto-conflict. Taking the conventional Mod Hash, XOR Hash, and M-square Hash as examples [14, 15], when block-to-block exchange occurs and thus $a' \neq a$, then there exists $g' = g$, and the chance of original conflict in RMhash is $1/r$.

The conflict rate of RMhash is determinable by first generating a sequence of values satisfying a uniform distribution, that is, a random set of $[0, r)$, with the probability of occurrence of each element being $1/r$. Assuming that C denotes the random probability value and H denotes the parameter value from which k elements are selected, the probability of t conflicts occurring, can be expressed as

$$\left(C_r^k + C_k^2 H_r^{k-1} + C_k^3 H_r^{k-2} + \cdots + C_k^t H_r^{k-t+1} + C_k^{t+1} H_r^{k-t}\right)\left(\frac{1}{r}\right)^k. \tag{2}$$

The designed RMhash generation values satisfy uniform distribution, then the random matrix mapping results satisfy uniform distribution; thus, the RMhash conflict rate obeys Equation (2) and is determinable in terms of conflict probability. Table 1 shows differences of Hash functions before and after improvement.

2.2. (二) Blockchain Authentication Model for Textual Works Based on RMhash/NFT. NFT is used as a digital identity card to be used in the blockchain, where each node stores the complete block information, there is no central node, and the Nonce value is obtained through a proof of workload (POW) in the block [16], with the partition data implicitly kept constant in each node. In designing this digital model, the blockchain is set to be private, introducing the NFT into the POW, thus enabling fast execution of transactions while the block information cannot be changed. The reason why partition points are so stable is that partitions are linked to partitions by RMhash. If you want to modify the information of a block, you need to calculate the RMhash value of the other blocks before that block, and you also need to modify the corresponding information of the corresponding block in each node; thus, the cost is higher, thus further improving the security of the blockchain information storage under this model. Blockchain itself belongs to multinode distributed mapping technology [17, 18]; when a single node fails, other

Table 1: Comparison of Hash functions before and after improvement.

Hash function	Number of conflicts	Number of conflicts after rounding off $(100000)_2$
Mod hash	326	6127
XOR hash	832	5587
M-square hash	496	5367
RMhash	16	4177

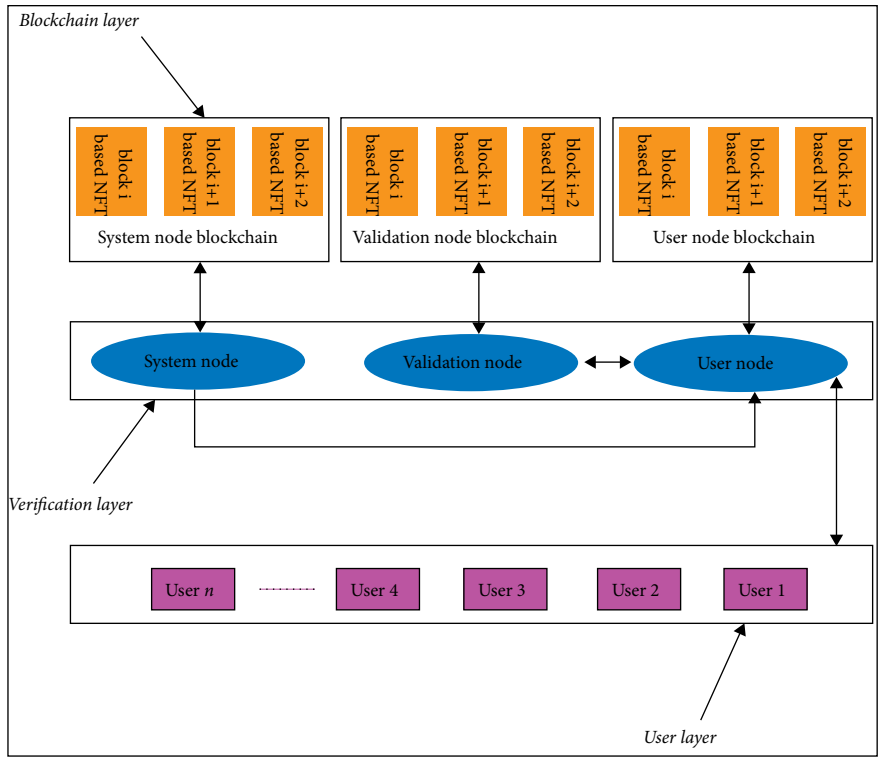

Figure 1: Digital authentication model for text copyright based on NFT blockchain technics.

nodes will not be affected, and at the same time, the node with the obstacle can lend itself to data recovery by other nodes. The adoption of NFT can prompt the digital model under blockchain technology to be data tamper-proof, and the overall model is shown in Figure 1.

The text copyright digital authentication model proposed in this paper consists of three layers, namely, the user layer, the authentication layer, and the blockchain layer, with the blockchain layer serving as the underlying layer of the model. They can be described as follows:

(1) *User Layer.* The user submits the authentication information or personal information required for access through an external interface to the upper layer, i.e., the authentication layer, and the information together with other encrypted information generates an access code, which is matched with the transaction (TR) result of the blockchain, thus realising the complete connection of information of this textual work.

(2) *Verification Layer.* This layer includes multiple nodes and is divided into three categories, namely, user nodes, verification nodes, and system nodes. System nodes can obtain requests from other nodes and classify them and forward them to other nodes for further processing according to the request information; verification nodes extract relevant points, including NFT information, user information, text copyright information and RMhash code according to the transaction information and after verification, to generate new blocks; user requests are submitted to user nodes to generate stored copyright text data to users.

(3) *Decentralised Layer.* It chains the execution status of subordinate nodes to a node that acts as a global control, with the number of each functional node meeting the requirement of "N system nodes + N client nodes > N miner nodes." Each node is relatively synchronized in terms of its next state. Assume that the system node and user node are located in the block as A and the newly mined block as B. The NFT in A and B can identify the commodity to be checked as the same commodity, making each local chain partition unbreakable. Assume H to be a synchronized block = 1 + H current blockchain and at the same time, compare the hash of the block before and

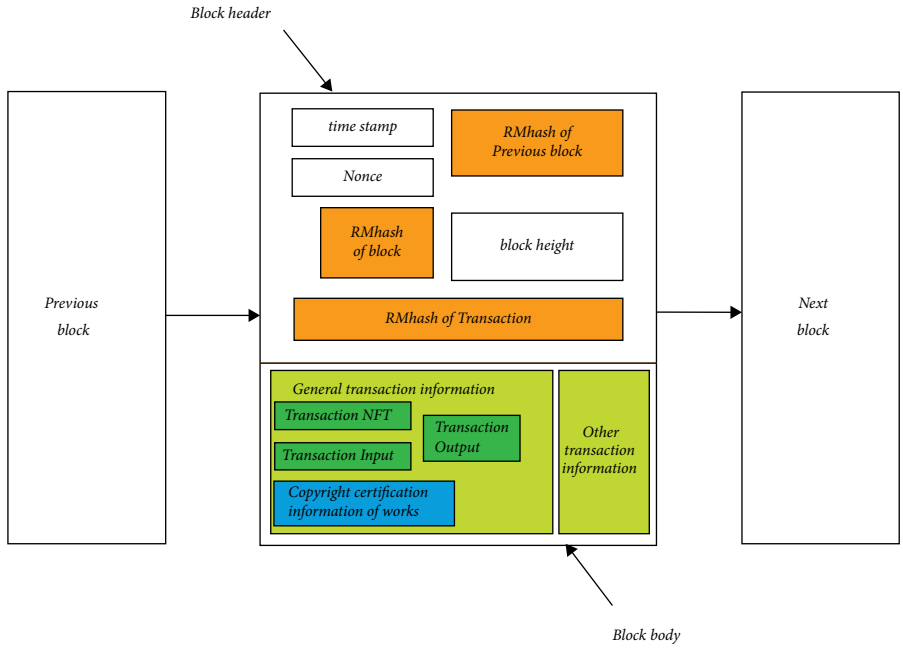

Figure 2: Block body architecture of the NFT/RMhash blockchain model.

after the level, if there exists a hash of the previous block = hash of the local block, then the NFT universe digital model can guarantee the synchronization of the block. Blocks to be intelligent need to lend user nodes and system nodes to meet the above conditions.

The text work is divided into blocks in the blockchain, and each block includes header information, block body, where the header information hash value is calculated using the RMhash method, where the hash value of the previous block and other values of the block are used as input to the RMhash method, and a new RMhash value is calculated. The corresponding hash values in the decentralised individual blocks can be derived via an implicit algorithm, making the distributed and interlinked node architecture a characteristic of the blockchain. The block body mainly holds transaction records, and depending on the specific type of information, different types of transaction data are held; for example, in the case of Bitcoin [19], the block body holds information about the user's transfers, and in the case of Ethernet applications, the block body holds information about the user's electronic contracts [20]. In contrast, in the text copyright authentication of this paper, the block body holds the copyright data of the text work, including author information, work title, NFT entries, and transaction input/output, as shown in Figure 2.

As opposed to the block body structure of most blockchains [21, 22], the random matrix-based improved conflict rate hash is applied to the front and back level blocks, TR, and Nonce, while increasing the height information of the partition to construct the block body. Among them, the Nonce value is calculated by the NFT-based POW algorithm, which solves the previous level of hash, TR hash, Nonce test value, and mining difficulty as input, thus reflecting the complete information of the block, and because of the inclusion of the previous block information, the front and back blocks remain relevant, while more information is involved in the encoding, increasing the degree of immutability of the block information; thus, the reliability of the block data is ensured.

The blockchain digital model designed in this study uses NFT as the digital account information, which is written into the TR record as the unique identification information to describe the transfer point information while also achieving the copyright authentication of the work. When a customer is ready to authenticate the copyright of a work, copyright authentication-related content is generated, including the content of the work, NFT, user name, general content of the work, RMhash code, and timestamp'. When the work is facing a copyright dispute, the authentication model will perform a search based on the NFT and display the copyright information associated with the work. When the work is stored, its content can be bundled with the authentication information on the chain instead of being stored in a traditional database, and the integrity and reliability of the work is maintained based on the characteristics of the blockchain. The key algorithm uses the elliptic encryption algorithm so that the private key is used for encryption and the public key for decryption, where the private key signature is verified by the content of the work and the public key, whereas if the database is used for storage, then the content will change and the private key cannot be verified correctly. The private key is used as a digital signature to calculate the true owner of the copyright of the work.

Aiming at the problem of copyright registration and certification of plagiarized works, this model first uses the SimHash algorithm to check and compare the works, screen

out the plagiarized works, and ensure that the registered works are not plagiarized. Although SimHash duplicate checking can be avoided by some means, the copyright authentication record of this model includes work content and timestamp proof; that is, the evidence of copyright authentication of plagiarized works will be permanently stored. It is easy to judge plagiarism through timestamp, which can effectively avoid the problem of copyright authentication of plagiarized works.

3. Pilot Analytics

The simulation of a distributed environment is required. The nodes are installed with a conventional IntelIntel CPU + 4 GB configuration, and seven nodes are screened to achieve a decentralised partitioning effect, with the number of system nodes being one and the other nodes acting as miner nodes and user nodes, respectively. The algorithm code supports multithreaded technology and is programmed in Go language, which can simulate multinode distributed operation. The test data are plain text data, and the simulated block hash is generated using the proposed RMhash algorithm.

The trials were divided into several subgroups. First, it was assumed that the TR information was used for block generation by a sufficient number of TR information, taking text data as an example, and the corresponding time was calculated, and the test results Figure 3.

The NFT-based digital model collected TR information and conducted 30 tests, and the average test time for generating blocks was 0.53 s. In order to simulate the scenario of multiple user nodes participating at the same time during the transaction on the chain, three machines were therefore selected to simulate user nodes, as shown in Figure 3, and the block generation result of less than 1 s met the customer's access requirements.

Changing the number of digits of the work to be copyrighted on different works, the word count of each work was 5386 words, 31252 words, 38477 words, 43659 words, 82,637 words, 166,359 words, and 248,655 words, respectively, Figure 4.

Time of different works on copyright consumption is not proportional to the number of words of works and query text works content through the block query for detection; 248,655 words has exceeded the number of words of an article, and the consumption time is only 0.23 s to meet the customer's real-time query requirements for the system, see Figure 4.

The storage of each block based on different word counts of a number of works and copyright certification for index evaluation based on the storage data can further evaluate the space expenditure of the block, which works on text storage of separate expenditure for Y1, corresponding to the core data of NFT certification storage expenditure which is much less than Y1 and can be expressed as Y2, see Figure 5 and 6 and core storage–text storage expenditure is expressed as Y2/Y1.

According to the overhead ratio, the record storage expenditure is about 2–3 times of the text storage

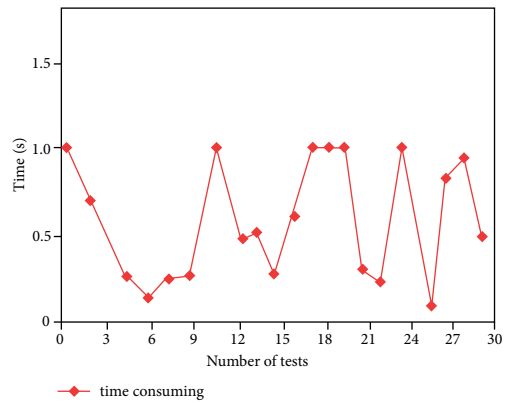

Figure 3: Time-count diagram for generating blocks.

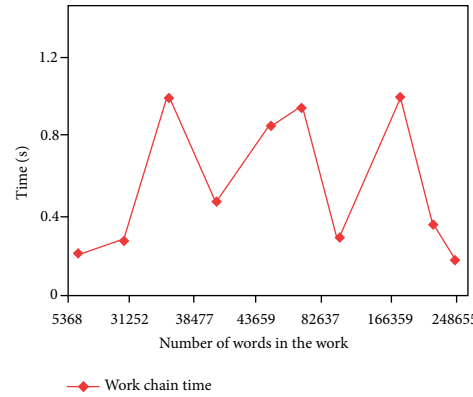

Figure 4: Differential time consumption for certification of works with various word counts.

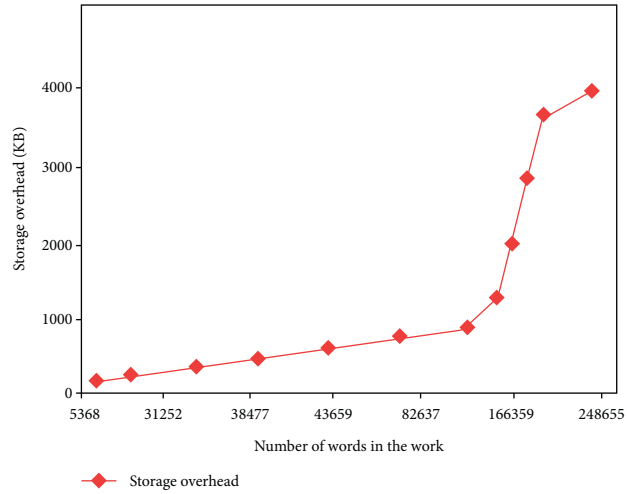

Figure 5: Storage overhead of work text storage.

expenditure, the work storage expenditure, record cognitive expenditure, and expenditure ratio of word count of different works do not vary greatly; according to Figure 5, the storage expenditure for storing 240,000 words for authentication is about 3720 KB; compared

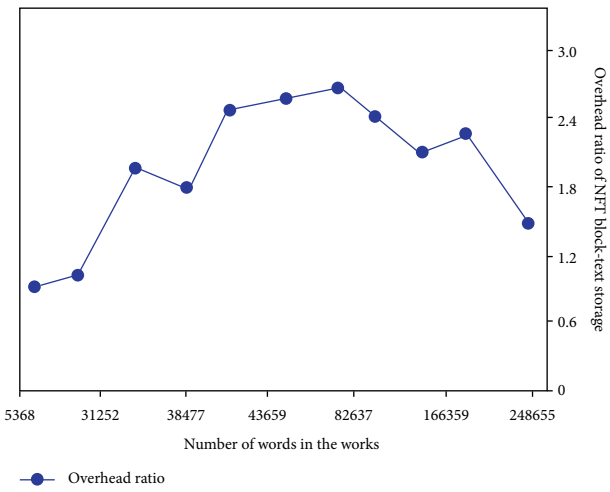

Figure 6: Ratio assessment of work text storage.

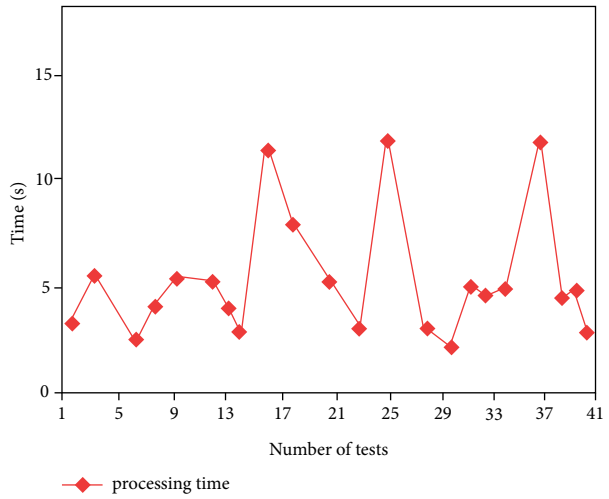

Figure 7: Time consumption for 400 concurrent transactions.

to other text storage models [23, 24], the text digital model with smaller storage space, and the expenditure of block restructuring, record authentication expenditure is removed from the stored information, thus allowing the application of the model's superior storage performance.

Concurrent processing of 400 TR messages and text data are synchronously hashed in each node to obtain the time consumption and then to obtain the average TR processing velocity, and the number of tests is 41 times the concurrent test outcomes of digital text data, see Figure 7.

In multiple tests of 40 times, the concurrent processing of 400 text records took an average of 6.87 s, with an average processing speed of 58.22 articles/s. A processing speed of 268 articles/s can be achieved in the best case and 15 articles/s in the worst case, and the data concurrency of the model supports high frequency transactions in a real production environment.

4. Conclusion

Aiming at the current problems of blockchain copyright storage [25, 26], this manuscript introduces the NFT digital ledger tag, proposes an RMhash algorithm for the problems of the hash function in the block, and introduces a new theory of random matrix to achieve the key values satisfying uniform distribution and reducing originality conflicts. The block structure is extended with the introduction of NFT, and the actual core information of the copyright of the work is used as the data source to design the storage structure, realising the chain storage of the actual content and copyright information of the work. The semiprivate key authentication of the information unlocking function is within the scope of the authentication needs of the work copyright and helps to record the creator's full work creation process. Experimenting with the Go language as a development tool for a distributed multinode layout, the designed digital model of the NFT universe was tested and the results showed that the model has good performance in the field of authentication of text type data. NFT has a wide range of applications in the field of representing real world assets, and the next step could be to enhance its research in the asset management scenario, where the trusted information of the blockchain is provided by individual block bodies, and an area research could contribute to future research in computer model formulation.

Data Availability

The dataset used in this paper are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding this work.

References

[1] A. Siyaev and G. S. Jo, "Towards aircraft maintenance metaverse using speech interactions with virtual objects in mixed reality," *Sensors*, vol. 21, no. 6, 2021.

[2] S. N. Suzuki, H. Kanematsu, D. M. Barry et al., "Virtual emetaverse and their applications to collaborative projects: the framework and its significance," *Procedia Computer Science*, vol. 176, pp. 2125–2132, 2020.

[3] W. Chen, L. Dai, K. B. Letaief, and Z. Cao, "A unified cross-layer framework for resource allocation in cooperative networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 8, pp. 3000–3012, 2008.

[4] G. Jun, "Virtual reality church as a new mission frontier in the metaverse: exploring theological controversies and missional potential of virtual reality church," *Transformation An International Journal of Holistic Mission Studies*, vol. 37, no. 3, pp. 1–9, 2020.

[5] J. Kim and J. D. Park, "The non-homogeneous flow of a thixotropic fluid around a sphere," *Applied Mathematical Modelling*, vol. 82, pp. 848–866, 2020.

[6] M. Fazilati, N. Maleki-Jirsaraei, S. Rouhani, and B. Daniel, "Quasi-periodic and irregular motion of a solid sphere falling

through a thixotropic yield-stress fluid," *Applied Physics Express*, vol. 10, no. 11, pp. 117301.1–117301.4, 2017.

[7] N. Ganikhodjaev and H. H. b. Ibrahim, "Two-dimensional ising model with non-homogenous interactions," *AIP Conference Proceedings*, vol. 1830, no. 1, pp. 1–6, 2017.

[8] Z. Xiang, "Applications of homogenous balanced principle on investigating exact solutions to a series of time fractional nonlinear PDEs," *Communications in Nonlinear Science and Numerical Simulation*, vol. 59, no. 6, pp. 606-607, 2017.

[9] D. Cao, Y. Gao, J. Wang, M. Yao, and W Zhang, "Analytical analysis of free vibration of non-uniform and non-homogenous beams: a," *Applied Mathematical Modelling*, vol. 65, pp. 526–534, 2019.

[10] J. N. Zhu, X. C. Liu, and C. Liu, "Non-equidistant non-homogenous grey prediction model with fractional accumulation and its application," *Journal of Intelligent and Fuzzy Systems*, vol. 40, no. 4, pp. 1–14, 2021.

[11] M. G. Jassam and S. S. Abdulrazzaq, "Theoretical Analysis of Seepage through Homogeneous and Non-homogeneous Saturated-Unsaturated Soil," *University of Baghdad Engineering Journal*, vol. 25, no. 5, pp. 52–67, 2019.

[12] W. Rui, "Applications of homogenous balanced principle on investigating exact solutions to a series of time fractional nonlinear PDEs," *Communications in Nonlinear Science and Numerical Simulation*, vol. 47, pp. 253–266, 2017.

[13] F. Yzquierdo, "The Malta case: distributed ledger technologies (dlts) and Islamic commercial law in the European Union. A European controversy," *Journal of the Sociology and Theory of Religion*, vol. 9, no. 1, pp. 99–109, 2020.

[14] K. Alabi, "Digital blockchain networks appear to be following Metcalfe's Law," *Electronic Commerce Research and Applications*, vol. 24, pp. 23–29, 2017.

[15] R. Almuttalibi, "Blockchain hash function for secure biometric system," *Journal of Engineering and Applied Sciences*, vol. 14, no. 11, pp. 3797–3805, 2019.

[16] R. Wei, A. Jh, D. Tza, Y. Ren, and K. K. R. Choo, "A flexible method to defend against computationally resourceful miners in blockchain proof of work," *Information Sciences*, vol. 507, pp. 161–171, 2020.

[17] S. Huckle and M. White, "Fake news: a technological approach to proving the origins of content, using blockchains," *Big Data*, vol. 5, no. 4, pp. 356–371, 2017.

[18] K. Fan, L. I. Fei, Y. U. Haiyang, and Y. Zhen, "A blockchain-based flexible data auditing scheme for the cloud service," *Chinese Journal of Electronics*, vol. 30, no. 6, pp. 1159–1166, 2021.

[19] J. Fu, S. Qiao, Y. Huang, X. Si, B. Li, and C. Yuan, "A study on the optimization of blockchain hashing algorithm based on PRCA," *Security and Communication Networks*, vol. 2020, no. 8, pp. 1–12, 2020.

[20] C. Komalavalli, D. Saxena, and C. Laroiya, "Overview of Blockchain Technology Concepts," *Handbook of Research on Blockchain Technology*, pp. 349–371, agan Institute of Management Studies, Rohini, New Delhi India, 2020.

[21] A. N. Saleh and M. A. Al-Ahmad, "Security of a new cryptographic hash function - titanium," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 10, no. 2, pp. 827–832, 2018.

[22] V. Manuceau, "About a fast cryptographic hash function using cellular automata ruled by far-off neighbours," *International Journal of Engineering Trends and Technology*, vol. 69, no. 2, pp. 39–41, 2021.

[23] F. Tao and W. Qian, "Image hash authentication algorithm for orthogonal moments of fractional order chaotic scrambling coupling hyper-complex number," *Measurement*, vol. 134, pp. 866–873, 2019.

[24] M. M. D. Priyadharshini and C. Ananth, "A secure hash message authentication code to avoid certificate revocation list checking in vehicular adhoc networks," *Social Science Electronic Publishing*, vol. 10, no. 2, pp. 1250–1254, 2017.

[25] K. Benzekki, A. E. Fergougui, and E. B. Elalaoui, "DePass: A Secure Hash-Based Authentication scheme," in *Procedings of the Intelligent Systems & Computer Vision*, pp. 1–8, IEEE, Fez, Morocco, April 2017.

[26] H. Tohidi and V. T. Vakili, "Lightweight authentication scheme for smart grid using Merkle hash tree and lossless compression hybrid method," *IET Communications*, vol. 12, no. 19, pp. 2478–2484, 2018.