electronics

MDPI

Article

Blockchain Smart Contract to Prevent Forgery of Degree Certificates: Artificial Intelligence Consensus Algorithm

Seong-Kyu Kim [1,2]

[1] Department of Information Security, Joongbu University, Goyang-si 10279, Korea; guitara7@skku.edu or skkim@joongbu.ac.kr
[2] Department of Public Policy and Information Technology, Seoul National University of Science and Technology, Seoul 01811, Korea

Abstract: Certificates are often falsified, such as fake diplomas and forged transcripts. As such, many schools and educational institutions have begun to issue diplomas online. Although diplomas can be issued conveniently anytime, anywhere, there are many cases wherein diplomas are forged through hacking and forgery. This paper deals with the required Blockchain diploma. In addition, we use an automatic translation system, which incorporates natural language processing, to perform verification work that does not require an existing public certificate. The hash algorithm is used to authenticate security. This paper also proposes the use of these security protocols to provide more secure data protection. In addition, each transaction history, whether a diploma is true or not, may be different in length if it is presented in text, but converting it into a hash function means that it is always more than a certain length of SHA-512 or higher. It is then verified using the time stamp values. These chaining codes are designed. This paper also provides the necessary experimental environment. At least 10 nodes are constructed. Blockchain platform development applies and references Blockchain standardization, and a platform test, measurement test, and performance measurement test are conducted to assess the smart contract development and performance measurement. A total of 500 nodes were obtained by averaging 200 times, and a Blockchain-based diploma file was agreed upon at the same time. It shows performance information of about 4100 TPS. In addition, the analysis of artificial intelligence distribution diagram was conducted using a four-point method, and the distribution chart was evenly distributed, confirming the diploma with the highest similarity. The verified values were then analyzed. This paper proposes these natural language processing-based Blockchain algorithms.

Keywords: Blockchain; Diploma Certificates; deep learning; MooC; information security

Citation: Kim, S.-K. Blockchain Smart Contract to Prevent Forgery of Degree Certificates: Artificial Intelligence Consensus Algorithm. *Electronics* **2022**, *11*, 2112. https://doi.org/10.3390/electronics11142112

Academic Editor: Mazdak Zamani

Received: 30 April 2022
Accepted: 22 June 2022
Published: 6 July 2022

1. Introduction

Certificates are often falsified, such as counterfeit diplomas and transcripts. Thus, many schools or educational institutions have begun issuing graduation certificates online. Anyone can obtain a diploma or other documents from anywhere they want. However, there are many cases where such graduation certificates are forged and used. Therefore, we would like to present academic records such as graduation certificates and transcripts using Artificial Intelligence (AI) consensus algorithms [1–3]. Therefore, this paper was written to study the certificate-verifying artificial intelligence block chain. In order to verify for falsification of graduation certificate, we will verify it using the Mask R-Convolutional Neural Networks (R-CNN) Head Architecture. This suggests the necessary verification method using two Faster R-CNN head values. Additionally, we are trying to verify security and authentication using the Mask R-CNN Loss Function algorithm. Block verification is performed using the Fast R-CNN method and Mask R-CNN method. We also want to show fast performance for block verification through the Multi-Layer consensus algorithm. Verification through the Multi-Layer consensus algorithm is a verification of fault-tolerant

distributed protocols, which is an immensely difficult task. Often, in these protocols, thresholds on set cardinalities are used both in the process code and in its correctness proof; a process can perform an action only if it has received an acknowledgment from at least half of its peers. Verification of threshold-based protocols is extremely challenging as it involves two kinds of reasoning. Using this Multi-Layer Artificial Neural Network (ANN) backpropagation and Hidden Markov Model achieves a stable performance for agreed nodes with improved performance. In this research, in the field of artificial intelligence and in the area of Blockchain, the chain design is completed using the certified block node algorithm for diploma verification. Based on a performance evaluation and the limitations of the research experiment, we select and present a target value for measuring performance in order to enhance the variety of functions, the excellence in performance, and the security of the proposed software. We also want to conduct research and development to certify diplomas based on the amount of simultaneously processed trends, the number of chain segments, and the amount of support for consensual algorithms that process simultaneous trends for future verification. Many certificates, including diplomas, are falsified. It can be said that it is used in bad places. Therefore, an artificial intelligence-based Blockchain diploma is a very necessary technology. Additionally, a Blockchain diploma is a technique used to defend the illegal falsification of a diploma with Blockchain technology. In this paper, the AI-based Blockchain diploma is based on a reliability-based architecture, comparing the preregistered real diploma with the forged near diploma by using a Multi-Layer ANN algorithm.

Furthermore, we attempt to conduct first-order verification using artificial intelligence R-CNN Loss Function for algorithms that validate for the mis-design of public documents, certificates, diplomas, etc. We also propose an algorithm that validates blocks in Blockchain for secondary verification and validates them for document consistency.

In addition, Blockchain services for certificates are already being applied in several places and PoC and pilot projects are being conducted. However, we are using Blockchain and artificial intelligence algorithms to verify certificates for an artificial intelligence-based Blockchain certificate system for accurate verification.

Additionally, Section 1 talks about the certificate of the Blockchain diploma. Section 2 looks at the related research, EduTech, Blockchain Agreement Algorithm for Certification, and Deep Learning for Certification. Section 3 discusses the reasons and triggers for the recent Blockchain diploma and shows the architecture of the Artificial Intelligence Blockchain Research Methodology for Diploma Certificate. Section 4 shows Performance Evaluation and Limits of the Research and Section 5 describes the Discussion and Future Application Model. In addition, Section 6 describes the limitations of current research and future studies in the Conclusion and Future Work.

2. Related Research

Academic certificates are now issued online. Still, there are always concerns of falsification in relation to these academic credentials. Thus, we first investigate Edutech, the education market [4–7]. We will also learn about the technologies such as consensus algorithm and shading of the Blockchain. Lastly, we will look into artificial intelligence verification algorithms. Additionally, the related research is a preliminary study to verify a Blockchain diploma based on artificial intelligence. This is a very, very important dictionary study. Through EduTech, we will check certificates relating to all teaching skills. Additionally, we study an important part of the Blockchain agreement algorithm for certification. This paper will also look at the latest technology trends based on artificial intelligence deep learning that is needed in advance.

2.1. Edutech for Cerification

EduTech combines education and technology to develop eLearning from a diverse perspective. This term eLearning means learning by utilizing electronic means, information and communication, and radio and broadcasting technologies, and it has developed into a

means of overcoming the evils of existing offline education, i.e., collectivity and cramming. eLearning includes electronic learning based on the internet, web learning, web-based training, online learning, and remote education and interactive teaching and autonomous learning. Therefore, eLearning is a knowledge service industry that combines Information and Communication Technology (ICT) and education and is evaluated as a new growth engine for high value-added products. Moreover, eLearning provides learners with various learning content, access to information, time-saving, and enjoyment, thereby creating new value for learners [8–12]. With the spread of mobile internet-based smart devices, eLearning learners are enjoying learning on subway trains, buses, cafes, and even restrooms while downloading eLearning applications. In other words, eLearning is an efficient, self-directed learning method that can significantly reduce the time and space constraints and increase the learner's educational effectiveness. In addition, one of the key features of video learning through eLearning is that learners can learn anytime, anywhere. Additionally, because of its strong learner initiative, it can exercise its right to decide on the learning methods and progress. EduTech refers to the interaction between education and technology by combining existing education and technology. There are several features that correspond to self-directedness in eLearning. With the rapid development of Edutech, these technologies are being applied from elementary school to university. After eLearning and regular school courses, however, diplomas and certificates are likely to be forged. Figure 1 shows how Edutech is used to verify diplomas and transcripts.

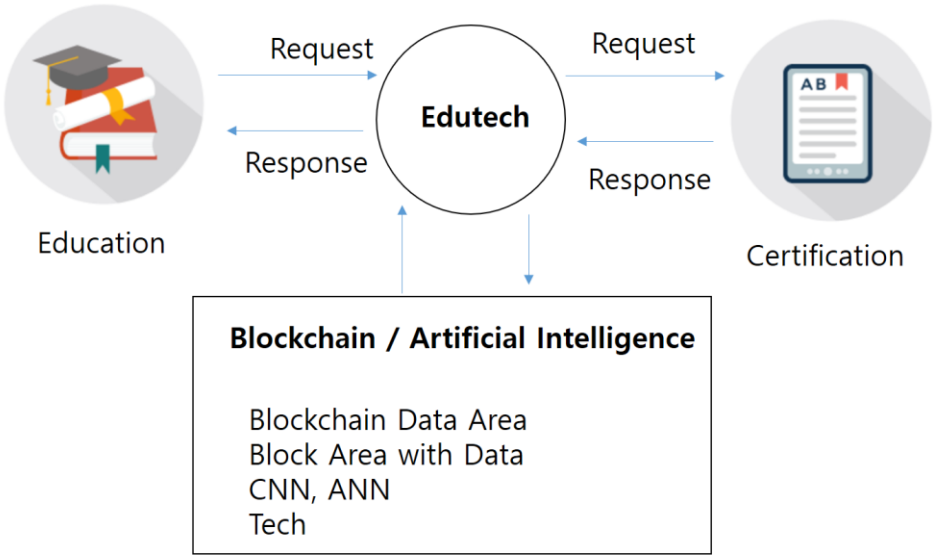

Figure 1. Architecture of Edutech. (Source: https://www.lifentalk.com/1820, accessed on 29 April 2022).

2.2. Blockchain Agreement Algorithm for Certification

For the safe verification of diplomas and transcripts, the process of consensus is needed in the Blockchain node of agreement. The consensus algorithm functions as a double-edged sword in a Blockchain. Without the consensus algorithm, Blockchain nodes in P2P Peer-To-Peer (P2P) networks without servers cannot be guaranteed to have the same data. Thus, the consensus algorithm is necessary in the Blockchain environment, but the scalability and processing speed of the Blockchain are affected by the consensus algorithm [13–17]. Today, research and development of consensus algorithms continue to be carried out to speed up processing without affecting the scalability of the Blockchain in various areas, and new consensus algorithms continue to be released daily. Among the consensus algorithms introduced, the most well-known consensus algorithms include proof of work, proof of equity, and proof of delegated equity. Work verification method is a method that gives authority to create blocks through competition. Work verification uses a method that gives one participant the right to create blocks for the fastest computation of

one-way hash algorithms. In order to speed up the operation of hash algorithms, however, more than a certain level of equipment is required, which consumes a lot of power [18–21].

The equity certification method was developed to address the issue of the highly competitive work certification method, wherein nodes have different interests depending on those defined in the network and they change the difficulty of work certification depending on the interests held by the nodes. In the case of equity verification, however, there is a centralization issue of block creation wherein certain nodes continue to create blocks. The method of proof of delegated shares is similar to the United States (US) electoral college system, wherein nodes elect representatives in the Blockchain network. The number of delegates is fixed in advance, and the elected representatives create blocks through voting among themselves. The method of proving the delegated stake has the disadvantage of having a threat of external attacks, as it can predict who the representative will be (see Figure 2).

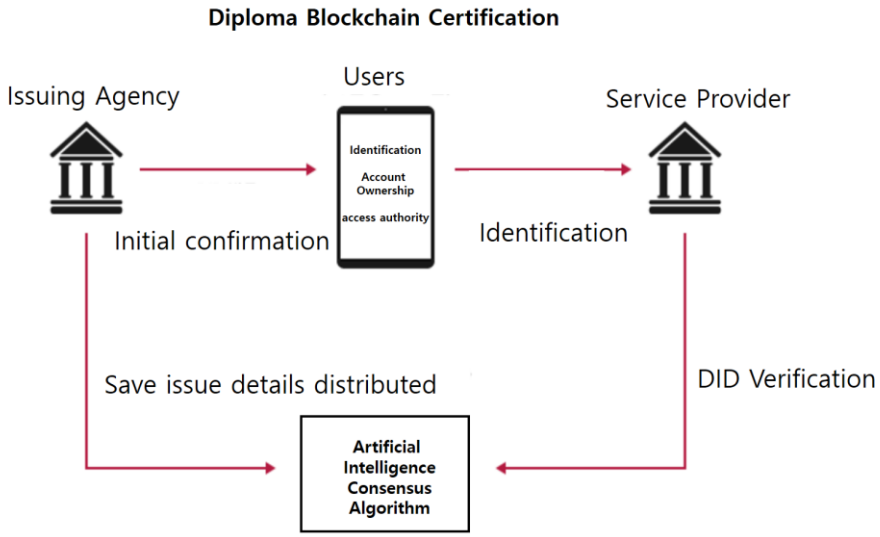

Figure 2. Blockchain architecture for education (source: International Finance, 2017).

Table 1 compares the consensus algorithm of the Blockchain. In addition, the consensus algorithms such as PoW, PoS, DPoS, and PBFT were compared and studied.

Table 1. Consensus Algorithm chain block of comparison.

Algorithm	Contents	Speed
PoW	Bitcoin	Slow
PoS	ADA	Medium
DPoS	EOS	Past
PBFT	Hyperledger	Past

2.2.1. Improved BFT Scalability in Distributed Network Environments

This Blockchain agreement algorithm consists of the Propose, Write, and Accept process, wherein the agreement process is made up of a total of three stages and all nodes participate in voting for each stage to reach an agreement. The biggest characteristic of Byzantine Fault Tolerance (BFT) is that it first identifies the forced termination of a node through the pre-processing process, away from the conventional method of agreement that was in progress without considering the conflicts between nodes or forced shutdown of the system. BFT will reach an agreement with an agreed-upon acceptance rate of 2/3 or more if the number of nodes operating normally is greater than one-half. If the number of nodes operating normally is less than one-half, the non-operating nodes restart the system [22–25].

The nodes that restart the system receive data from the nodes that are operating normally to recover the previous data and rejoin the settlement process. BFT improved the scalability of the agreement by proactively identifying conflicts, such as forced shutdown of nodes, to prevent possible obstacles in the settlement process.

2.2.2. Improved Scalability of BFT in a Blockchain Environment

This Blockchain agreement algorithm consists of the Propose, Write, and Accept process, wherein the agreement process is made up of a total of three stages and all nodes participate in the vote for each stage to reach an agreement. The biggest characteristic of Byzantine Fault Tolerance (BFT) is that it first identifies the forced termination of a node through the pre-processing process, away from the conventional method of agreement that was in progress without considering the conflicts between nodes or forced shutdown of the system. BFT will reach an agreement with an agreed-upon acceptance rate of 2/3 or more if the number of nodes operating normally is greater than one-half. If the number of nodes operating normally is less than one-half, the non-operating nodes restart the system.

The nodes that restart the system receive data from the nodes that are operating normally to recover the previous data and rejoin the settlement process. BFT improved the scalability of the agreement by proactively identifying conflicts, such as forced shutdown of nodes, to prevent possible obstacles in the settlement process.

Among Blockchains, the process that several users agree to authenticate transparently, called a consensus algorithm, used a method of converging the existing consensus algorithm, proof of work, and PBFT consensus algorithms, and the preprocessing process improved scalability by limiting the number of nodes participating in the consensus process through grouping nodes. As a pre-processing process, each node performs a proof of work. Nodes are used as a group through nonce values obtained through proof of work. Each group uses Practical Byzantine Fault Tolerance (PBFT) to proceed with the agreement; after the group's agreement is terminated, group results are collected. In the case of SCP, the problem is that the longer the time to create groups through proof of work on each node, the longer the time to aggregate the consensus results of each group; hence the slower processing. For Multi-Agent, the preprocessing, as with the SCP study, limits the number of nodes participating in the consensus process through grouping of nodes. For Multi-Agent, however, unlike SCP, the network topology is adjusted to create a group of nodes. The representatives of each group are described as agents; when the agreement of each group is terminated, the agents collect the results of the agreement [26–28]. Multi-Agent studies, as with SCPs, can also slow down the processing speed if the network topology is adjusted for group creation or if the group's consensus results are longer. This scalability and the recent measurements can be considered below a certain level.

2.3. Deep Learning for Certification

Deep learning has been used in various areas of artificial intelligence. Such deep learning accumulates knowledge of a given task in many useful forms. Learning particular content from a task that performs a task can be seen as a problem of learning by expressing a function in an exact form. Inductive learning is a pattern in which functions are divided into input and output values from scratch. The performance of an inductive learning operation is evaluated as a learning curve. It uses artificial neural networks to verify documents such as diplomas and transcripts using artificial intelligence CNN algorithms. In particular [29–31], Multi-Layer perceptron (MLP) was used to handle more complex systems, which consisted of multiple layers. The MLP is very similar to the RNN, which uses the previous value for the current calculation, but only the current input is used to calculate the current output. Machine learning is described as a kind of artificial intelligence. Machine learning uses artificial neural networks. These artificial neural networks are then linearly computed and subsequently computed via nonlinear functions to use output values. The weights and bias used in linear combinations are determined by learning based on data. After learning, models show high performance not only when the data are

used for learning but also when other data enters the input. This paper seeks to verify better performance through various performance tests using Recurrent Neural Network (RNN) [32–35]. The mathematical model of the basic RNN is described, including how it is applied to self-sensing. It is also used to verify various certificates such as diplomas and transcripts using artificial intelligence techniques. The RNN emerged to model sequence data. What makes RNN different from conventional neural networks is that it has a "hidden state". The memory of the network can be seen as a summary of the input data so far. Every time a new input comes in, the network modifies its memory little by little. Eventually, after processing all the inputs, the memories left to the network become information that summarizes the entire sequence. This is similar to how a person processes a sequence. Because this process is repeated over and over again for each new word, the RNN is named Recurrent, or Circular. RNN can handle any long sequence through this repetition.

3. Blockchain Research Methodology for Diploma Certificate Verification

Many schools and educational institutions offer diplomas, transcripts, academic certificates, etc. to graduates or students. However, the service provided is a civil service that can be falsified and used for malicious purposes. Using a neuron engine and Blockchain, the model of verification service is presented. In addition, research methodology uses artificial intelligence to accurately record the graduates' academic records without falsifying them, so that anyone can be safe and reliable. It also presents improvements in algorithms that are designed and verified based on the existing CNN Intelligent Agent Algorithm and Cloud Architecture. It is also based on the verification of Blockchain Validated Mask R-CNN Head Architecture, Block Verification Mask R-CNN Loss Function, Block Verification Fast R-CNN, and Block Verification R-CNN Loss Function. In addition, it studies diplomas using Blockchain and applies a consensus algorithm to diplomas. This consensus algorithm is designed in consideration of Multi-Layer ANN, Agreements Algorithm Multi-Layer ANN backpropagation, Agreements Algorithm Hidden Markov Model, Agreements Algorithm Hidden Markov Model, and Agreements Algorithm. The design and process of Diploma Verification Blockchain for design is also presented.

3.1. Issue Raising

Nowadays, many students are going abroad to study. This phenomenon is caused by globalization. Still, it is quite difficult to know the school situation in other countries even if a student studies abroad. Currently, many schools are trying to avoid issuing these academic certificates online even though it is possible because the technology has improved. In the past, a student had to go to the school that he/she used to attend in order to obtain a diploma and a transcript [36,37]. Now, however, it is issued through the internet. Still, the number of cases of forgery is increasing when these internet proofs are made. In this study, we try to prevent the falsification of certificates such as these and to ensure that all certificates are safely verified and issued between individuals in the future. The study also uses a methodology that checks the similarity of certificates with the artificial intelligence's Mask CNN and also verifies them in a sucker using a Blockchain. Finally, we will study the block node and deep learning Mask CNN techniques [38–42].

3.2. Research Methodology

The research method for organizing the verification artificial intelligence Blockchain node for diploma identifies nodes and studies the technology of managing the Blockchain network based on the node group through a node grouping protocol and interface [43]. The research involves studying node technology by aggregating node management technology, node grouping technology, node communication protocol, etc. It also provides the ability to manage the list of nodes, establish access to nodes, and set and manage the nodes' connection status and the role of nodes, etc. [44]. Through node grouping technology, nodes are grouped together to provide the ability to set up items for nodes for each corresponding node group or to distribute chains and control roles [45]. By introducing the

design of P2P concurrent communication structure between nodes through multichannel via node communication protocol and design of interchannel communication separation structure, we develop frameworks of internode communication through node grouping and multichannel. These node-based Blockchains decouple artificial intelligence Blockchains Mask pre-diction and class pre-diction [46]. This improves performance by pre-dictating the binary mask without having to consider other classes in the mask presentation Show in Figure 3.

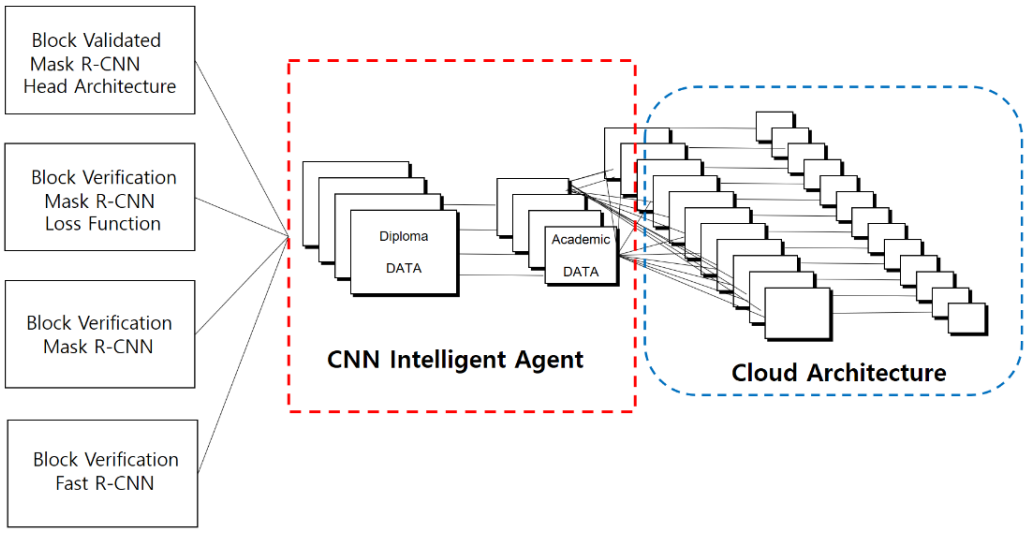

Figure 3. Artificial Intelligence Blockchain research methodology for diploma certificate.

The role of cloud preprocessing is to support CNN Intelligent Agent for the purpose of the proposed research [47]. This is to receive information that is verified and certified through pre-processing in advance [48]. These consensus mechanisms also exist to represent the reliability of the data. In order to use these consensus mechanisms, AI technologies such as consensus algorithms and Fast R-CNN and Multi-Layer need to be modeled. The cloud preprocessing system is a system that helps the CNN Intelligent Agent process. The system helps to decentralize data in processing whether the original graduation certificate is forged or not. It is also responsible for handling data and virtualization that are semi-oxidized [49].

In addition, the difference between this and existing studies is that hybrid Blockchain can be verified in all aspects. All transactions arising from hybrid Blockchain can be conducted privately, and if necessary, the transaction details can be opened for verification [50]. Each transaction can be written only once because it uses a Blockchain. After that, you cannot change the transaction details. However, Blockchain users can fully participate in Blockchain activities once they have been granted access. You can make transactions, view other transaction details, or add or modify transactions [51]. However, to protect the privacy of other users, their identity is kept secret. Additionally, when one user contacts another, his identity is revealed only when the person directly reveals it. Therefore, companies and organizations perform tasks by performing KYC so that the identification process of the hybrid Blockchain is performed correctly [52]. In particular, financial institutions need to respond correctly because they do not have the authority to allow users to make transactions without exposing their personal information to the Blockchain [53]. Even if hybrid Blockchain restricts anonymity to users participating in the network, public anonymity is maintained. No one outside the network can know about the Blockchain user. Hybrid networks provide all the important functions of a public Blockchain, such as security, transparency, immutability, and decentralization. However, they restrict access to transaction details, seeing them, or changing transactions in any way. In addition, it limits the user's permissions to prevent confidential information from leaking out of the network [54].

3.2.1. Blockchain Validated Mask R-CNN Head Architecture

Faster R-CNN box heads have been expanded from Artificial Intelligence ResNet and FPN (Feature Pyramid Network) for block verification. The head of the ResNet C4 backbone includes the fifth stage of the ResNet, which is complex-insensitive. In FPN, the backbone already contains res5, which provides a more efficient head with fewer filters. It also extended two Faster R-CNN heads, which indicates the head extended in ResNet C4 and the head extended in the FPN backbone. The numbers represent the spatial resolution and channels and stand for conv, deconv, or fc layers. The head architecture extends two existing Faster R-CNN heads. The mask Branch is added, and the head for the ResNet C4 and FPN backbone is indicated. The numbers represent spatial resolution and channels. Arrows indicate conv, deconv, or fully connected (fc) layers that can be inferred from the context. All outputs are 3×3, with output values of 1×1 and deconv of 2×2. Strides will also use 2 and the hidden layer will use ReLU. Additionally, 'res5' denotes the order of ResNet. To simplify, the first conv operation was designed. It is used for the algorithm to verify using the Mask R-CNN Head Architecture. The R-CNN algorithm is used to verify the stability of a diploma combined with Blockchain. In addition, the Blockchain network used uses two methods. Convolutional backbone architecture is verified through feature extension in the image and network head: binding-box recognition and classification, and classification and mask prediction work. The Faster R-CNN box heads were expanded from ResNet and FPN to verify whether the diploma was original or not. The head of the ResNet C4 backbone includes the stage of the ResNet, which is complex-insensitive. In FPN, the backbone already contains res5, which provides a more efficient head with fewer filters. For verification purposes, the sliding window is used to calculate the coordinates of the bbox available at each point and the score of the bbox, and the sliding window method uses a method of searching by sliding all the size of the space where the object might be located in the image.

3.2.2. Block Verification Mask R-CNN Loss Function

It is much more difficult to distinguish what objects are in the images than to classify images such as diplomas. The Regions with CNN features (R-CNN) takes several steps to process the task. First, the Selective Search algorithm is used to find the Region Proposal or Binding Box that finds the image area where the object is located. Selective Search combines adjacent pixels with similar colors, strengths, and patterns. Then, to inject the extracted bounding box into CNN's input, the size is force-unified. Moreover, CNN's input size makes it the same. The CNN used here uses a Linear Region model to better align better the bounding box coordinates of the classified final object using the SVM in the final stage of the pre-trained, modified version of AlexNet.

This is the work of transmitting images to pixel values and processing similar patterns and strengths to verify them. Additionally, the image is classified into the final object and processed.

3.2.3. Block Verification Fast R-CNN

To verify the block, we propose an algorithm that verifies the image of the diploma and puts it in the block node. The existing R-CNN problem is difficult, with many calculations required, to train three models: CNN for each of the many bounding boxes proposed as Selective Search, classification using SVM, and linear return for the bounding box. Through Fast R-CNN, we want to solve this using necessary ideas. There are many overlapping areas in the bin, and it is wasteful to pass them through CNN separately; the bbox information found in the RoI Pooling Selective Search is maintained through CNN, and the RoI is extracted from the final CNN feature map and pooled. If you extract an image of a diploma and do so, you will see an algorithm that dramatically reduces the amount of time you spend running CNN on each bounding box. In addition, both SVMs and linear regression models are included in one network for training. Softmax can be placed behind CNN instead of SVM and a separate bbox collector can be added after CNN, as with the softmax

layer, instead of linear regression. This is a technology that performs CNN only once to select the features and uses the Feature at the end of CNN to pool ROIs. The core idea of Faster R-CNN is the Region Proposal Network. We removed the original image data of the diploma from the optional search and calculated the ROI over the RPN while inheriting the existing Fast R-CNN structure. With this method, it was possible to calculate the RoI through GPU, and the RoI calculation was also learned to improve accuracy. This allows RPN to have higher accuracy while calculating around 800 RoIs, compared to Selective Search's calculation of 2000 RoIs. Below is the overall structure of the Faster R-CNN.

Therefore, this technique is used to verify whether the original image of the Blockchain diploma is forged or not. This is to process and validate many of the bounding boxes proposed as Pick Selective Search and to process linearly for the bounding box. Thus, it is a verification process for CNN.

3.2.4. Block Verification R-CNN Loss Function

Among the verification methods for block verification, the artificial intelligence image search algorithm is available. We added a network (CNN) to the Faster R-CNN that masks whether or not each pixel corresponds to an object and we stored the mask in a block node called Binary Mask. The Faster R-CNN also designs performance areas that reduce decimal error in the location of the RoI Pool area through bilinear interpolation as RoIign passes through CNN. This block verification has the advantage of extracting more accurate pixel positions than the RoI Pool through the RoI Align.

Therefore, it is used to verify whether the original image of the Blockchain diploma is forged or not. A network is added to the mask whether or not each pixel is an object to verify whether the diploma is forged or not.

3.2.5. Block Verification MD5 and HAS-160

Both the MD5 and HAS-160 hash algorithms consist of four rounds, but the stages of each round are different. Each round of the MD5 consists of 16 stages, while the HAS-160 consists of 20 stages. As mentioned earlier, the two hash algorithms receive input and process in 512-bit increments, but for the final output, MD5 outputs 128 bits and HAS-160 outputs 160 bits. In addition, for the initial value, the number of bits equal to the output bit can be used as the initial value, so MD5 uses 128 bits, whereas HAS-160 uses 160 bits. However, one feature here is that the default initialization constant values of the four 32-bit bits use the same values in the two hash functions. For HAS-160, additional 32-bit initial values are provided only. In addition, 512 bits are represented by 16 32 bits. Additionally, the 16 32-bit values provided as inputs are accessed from the hash function. In this case, the MD5 hash function is randomly accessed while performing step 64 out of 16 input functions. However, in the case of the HAS-160 hash function, four additional input values are generated and used for each round. This reduces the complexity of implementing round functions by pre-generating a total of 16 additional inputs (four rounds $\times$ four = 16 pieces) to be used when receiving 512-bit inputs in the diploma security algorithm, storing them in dual port memory, and providing them when performing round functions. The MD5 and HAS-160 seawater algorithms have FGHI(a) functions. It can be seen that the FGHI(b) function uses different functions for each round, but the MD5 and HAS-160 hash algorithms use similar Boolean functions. The integrated hash algorithm does not require eight Boolean functions, and if you share a common Boolean function, you can provide five Boolean functions. This is a summary of the FGHI(c) Boolean function of the MD5 and HAS-160 hash algorithms and the constant values used in each round. In the case of constant values, MD5 requires 64 because different constant values are used for each step, and in the case of HAS-160, only four constant values are required because the same value is used per round. The following is a summary of the left-hand rotation used in the single-step operation of the two hash algorithms. The left-hand rotation used by the MD5 hash algorithm uses four values in each round, which are repeated. Additionally, in the HAS-160 hash algorithm, 20 values are repeatedly used four times in the case of S1, and in the case for S2 (Figure 4).

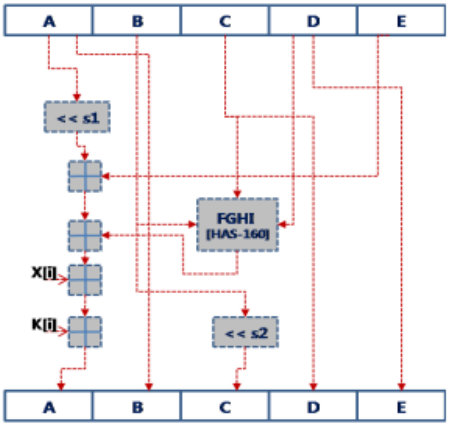

Figure 4. MD5 and HAS-160 hash algorithms for diploma certificate.

3.3. Research Design

Diploma e-document authenticity service refers to the process of registering a document's hash value with a Certificate Authority (CA) agency or a third party company, receiving the result value, and inserting it into the original document. The agency should receive the document's fingerprint value, store it on a highly secure, independent storage, and return the only corresponding value. However, if the document's fingerprint value is entrusted to a CA agency or a third-party company, it becomes dependent on the agency or company. This is because the institution creates a Token value corresponding to the document fingerprint value and uses the value to verify its authenticity. In addition, it is difficult to register documents and verify documents in the future because foreign users must subscribe to the service in Korea to use the service. By providing this service based on Blockchain, any company dependence can be avoided if only the hash function of document fingerprinting can be shared. Furthermore, for document fingerprint registration and document verification, only Blockchain needs to be accessed simply, thus securing internationality. In order to organize this service based on Blockchain, the extracted document fingerprint value is registered on the Blockchain and the Blockchain index (TXID) is submitted as a result, so that it can be inquired on the Blockchain, as shown in Figure 5.

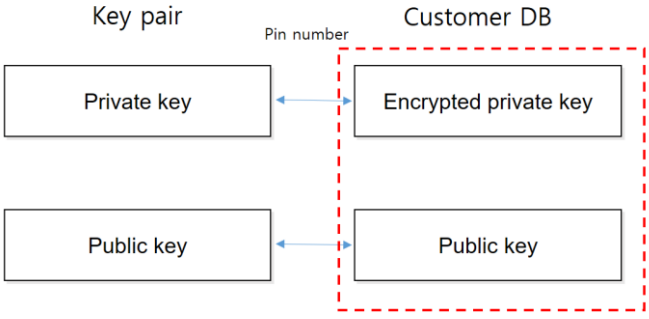

Figure 5. Key management methods.

3.3.1. Based Hash Function

One-way hash functions must be used to extract fingerprint values of documents. A one-way hash function is a function that requires the same string of values to be generated at all times when a document is used as an input value and cannot be inferred from the resultant value. This service uses the SHA-512 function.

3.3.2. Key Management for Blockchain Registration

To register the fingerprint value of a document in the Blockchain, it is necessary to sign a Blockchain transaction using the client's private key. The key management algorithm used by the Blockchain is ECDSA (Evalent Curve Encryption Algorithm) 3, which has the

same principle as the general asymmetric encryption algorithm, but has a relatively small and high security level.

3.4. Diploma Certificate Verification Blockchain Research Architecture

Diploma certificate verification architecture works by dividing structured and unstructured data. In addition, the consensus algorithm Multi-Layer ANN (Artificial Neural Network, ANN) designs data that should be classified with already validated data in order to validate the diploma as a Blockchain. The consensus algorithm Multi-Layer ANN backpropagation can train the output layer in a way that minimizes the process function by defining the same process function as the single-layer ANN's output layer. The consensus algorithm Hidden Markov Model was expanded by adding concealed states and directly identifiable observations to the Markov model. The consensus algorithm Bias-Variance Tradeoff designs the first area as variance on the other side of bias. A large variance and a theoretical background with a small overfit state are designed, as shown in Figure 6.

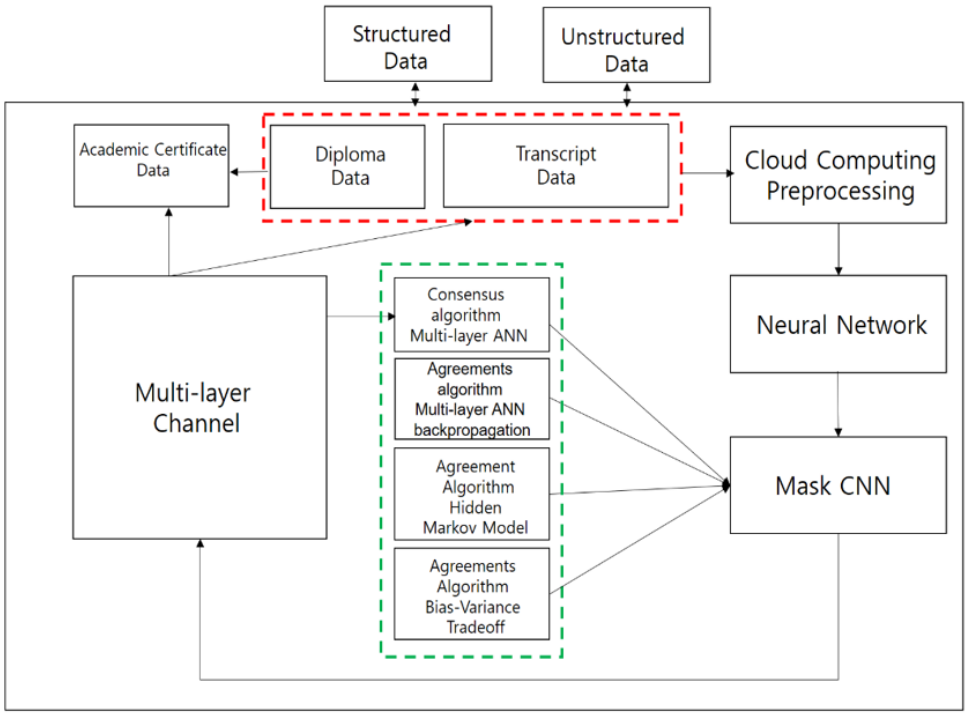

Figure 6. Diploma certificate verification Blockchain architecture.

3.4.1. Consensus Algorithm Multi-Layer ANN

In order to validate the Blockchain diploma, we have designed it by separating the initial data that have already been validated. Categorizing the data perfectly shows a complex form of function. A complex form of function is required, so it may be almost impossible to express with a simple single-layer ANN. A typical example of this problem is the XOR problem. If any transformation is applied, however, it is a model that can fully categorize data with a simple form of linear function. The most important feature of the Multi-Layer ANN for Blockchain Consensus Algorithm is not to form a classifier by using the given data as it is, but to train a transform operation optimized for a given data while forming a classifier by adding a structure called a hidden layer. Depending on the number of neurons in the hidden layer, the function of reducing or increasing the dimensions of the given data can also be performed. Multi-Layer ANN is an ANN that contains two layers of neurons, which can be designed with great refinement. It also represents the structure of the Blockchain consensus algorithm Multi-Layer ANN, and all layers except the output layer and input layer are designed as a hidden layer working with consensus algorithms in the process of agreement.

3.4.2. Agreements Algorithm Multi-Layer ANN Backpropagation

For the Blockchain consensus algorithm, the Multi-Layer ANN's output layer can be trained by defining the process function in the same way as the single-layer ANN's output layer and minimizing it. Therefore, if you use sigmoid function as an activation function and sum of squared error as a cos function, the update rule for parameters making up the output layer is defined by using the lab included in the training date. In addition, training date refers to data that have been pre-treated and machine-trained. In the case of a hidden layer, however, the process function cannot be defined because the label does not exist. The Backpropagation algorithm is designed to solve these problems and train Multi-Layer ANN. The error calculated from the output and the process function of the backpropagation to the hidden layer can be reversed and applied to the consensus algorithm.

3.4.3. Agreement Algorithm Hidden Markov Model

The Markov model for consensus algorithms for block verification expresses any change in phenomena, such as diploma images, image sensors, etc., as probability models. The Hidden Markov model (HMM) is an extension of these Markov models, whereby concealed states and directly identifiable observations are added. HMM is used to solve problems to deduce indirectly concealed states by means of an arrangement. This model represents the concept of concealed state and subsequent observation. HMM is used to infer through an observable sequence to study concealed state work for block verification.

3.4.4. Agreements Algorithm Bias-Variance Tradeoff

This occurs when any classification model or classifier is learned in machine learning for block verification for agreement of the Blockchain. The first area bias is designed on the other-side variance. A model with a large variance and a small overfit state is a model. Although the bias is large, models with small variance include constant function, linear stress, etc. applied to data with complex distributions. When designing a block algorithm such as this, the variance is large, but a model with a small bias is used for high-degree polynomial, deep neural network. When learning these Blockchains, it is important to ensure that both bias and variance are minimized. Bias and variance cannot be minimized at the same time, which applies a bias–variance tradeoff to the Blockchain consensus algorithm.

3.4.5. AI Consensus Algorithm

The artificial intelligence consensus algorithm works automatically. The AI consensus algorithm is basically characterized by the fact that existing AI autonomously judges and selects representatives to give them the authority to create blocks. Through this, the consensus algorithm solves the problems that an alternative to the agreement algorithm, including the work-certification system and the equity-certification system, has. The advantage is that artificial intelligence can automatically apply the Blockchain consensus algorithm to verify it. If the process to construct a "node" to form a "node" for the Blockchain agreement process was generally selected before, in this study, artificial intelligence algorithms set nodes. In addition, other parameters will be used to determine the most operational and efficient nodes, including the reliability of the node itself, and only these nodes will be allowed to agree, thereby eliminating malicious or corrupted nodes to protect the entire Blockchain. Each node is rated by artificial intelligence. The rating creates a reputation for the consensus algorithm to determine which node the system will choose in the future. Node selection depends on four basic factors.

3.4.6. AI Consensus Blockchain

Artificial intelligence consensus algorithms have been written based on existing Proof of Work (PoW) and Proof of Stake (PoS) algorithms. However, the algorithm we study refers to an algorithm that extends the process of mining or staking the process of consensus on these existing PoW, PoS algorithms to CNN. There are various types of agreements, and

there are also equity-based settlement methods. This is called a proof-of-equity algorithm (PoS). PoS is an algorithm that gives a high probability that a large stakeholder will be selected for transaction validation. There are two reasons for the emergence of PoS. The first is to replace PoW, which wastes real resources because of virtual resources. The second reason is the assumption that the participants who own more shares will verify the transaction in a good way because they have a higher stake in the Blockchain. However, PoS has a winner-take-all problem. The problem has been raised that it will return to those who have a large stake. Therefore, the "DPoS" that delegated shares and participates in verification has emerged. Voting methods have also emerged. The consensus algorithm introduced earlier was a way for selected verifiers to share it to nearby participants. However, there is a problem. Another verification can be selected due to the delay in propagation speed. This is called a fork. Forks are used in spoons, but they also mean pigtails. Of course, this is also designed to be resolved in a consensus manner.

However, these processes result in the cancellation of the approved transaction process. Therefore, the voting method is not to select the verification until the entire verifier participates and approves more than a certain amount. This is called the Byzantine Disability Tolerance (BFT) algorithm. Advantages are definitely stable. The disadvantage is that time can increase indefinitely. This is because a certain percentage of verifiers should wait until they can participate. Thus, the algorithm is implemented as a condition when there is a minority validator. In addition, artificial intelligence delegation certification basically follows the existing delegation stake verification method, but it is a big feature that artificial intelligence autonomously judges and selects a representative to give block creation authority. Through this, we try to solve the problem that alternatives to consensus algorithms, including Bitcoin's traditional work proof system, have. Furthermore, different parameters are used to determine the most operational and efficient nodes, including the reliability of the nodes themselves, and only these nodes allow consensus, resulting in the removal of malicious or corrupted nodes to protect the entire Blockchain Artificial Intelligence.

The rating creates a reputation in which the Bellas system determines which nodes to select in the future. Node selection depends on four fundamental factors: (1) number of transactions, (2) staking points, (3) block generation, and (4) uptime. Artificial intelligence delegation equity proof uses the order of algorithms to distinguish relationships and patterns in a set of data. Neural networks adapt themselves with new inputs and strive to achieve optimal results. Before commercial engagement, neural networks use genetic algorithms to ideally maintain the platform and successfully create a Blockchain. The transaction of Blockchain is demonstrated by the staking process, and the more cryptocurrency an actor has, the more likely it is to be selected to verify Blockchain. Validators receive financial rewards for active participation in the network. Neural networks, part of an artificial intelligence delegation proof system, are used to make accurate decisions about the platform, including compensation for node operators and time calculations required for block formation. The time until a new block is created is determined by the calculated transactions per second. The more transactions are completed, the shorter the time to the next block formation.

3.5. Diploma Verification Blockchain Design and Process

Blocknode design for diploma certification combines chain automatic configuration technology, contract distribution technology and disk virtualization technology to design a chain. Blocknode also means "node" in Blockchain. When this is the end of the chain design, the chain auto-configuration technology takes a way to carry out the distribution of the chain, inject the set values, and secure or approach it. It also provides the function of performing block setting. Additionally, it distributes and manages contracts within the chain at the request of the Contract Services through the Contract Distribution Technology, and loads chain data into virtual paths through the technology of crowd computing, enabling different Blockchain networks or channels to operate without infringing on each other's data. We then present intertransaction data for different channels for parallel

transactions for smart contracts. It also provides for parallel connections such as IPFS for smart control of Blockchain. It is a technique for validating transactions while preserving consistency between data and operations at the transaction verification stage, and also executing and verifying smart contracts in parallel in order to quickly perform the execution and verification of high-volume smart contract transactions on a single channel. To this end, Smart Contract structure that can be parallelized is developed and it is a framework that is needed for parallel execution and verification. The definition of transaction types and model studies for parallel processing of core technical content are based on the flow and processing methods of transactions, which are deeply related to whether transactions only read or write data, the order of transactions, and whether the areas in which transactions read and write data conflict. Methods to support parallel processing are to compare and analyze various verification and diploma data if necessary for block verification, such as how to separate reading and writing, the structure of pre-approval through reliable preprocessing, and how to reduce the processing process by combining transactions through double layers. In addition, in order to verify the diploma, the following process is taken (Figure 7).

(1) The Multi-Layer ANN Blockchain Consensus collects diploma data.
(2) Put subsequent data into the Consensus Algorithm Multi-Layer ANN and Agreements Algorithm.
(3) Put it in Hidden Layer and Process Function.
(4) Insert Block Verification and Deep Neural Network.
(5) Implement the verification block and enter it in the Consensus Algorithm.

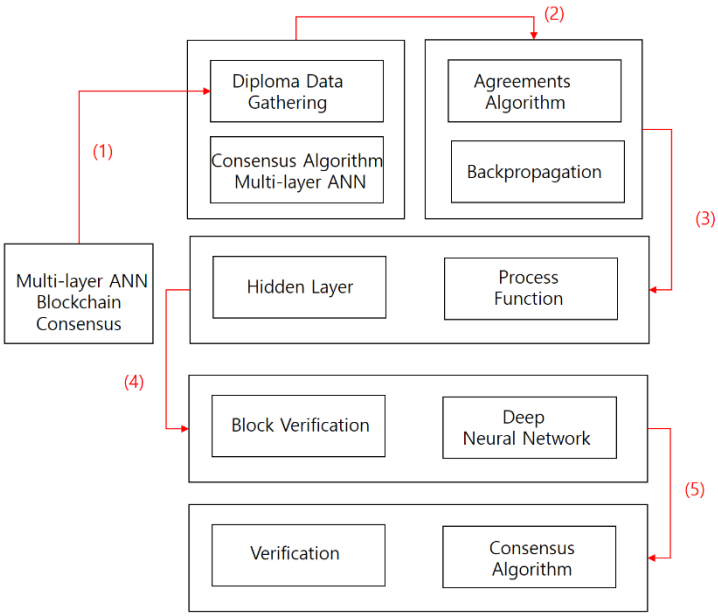

Figure 7. Diploma certificate verification Blockchain architecture.

3.6. Designing a Model for Diploma Verification Authority

Artificial intelligence authorization is the process of identifying entities that have permission to change, view, or access computer resources. Artificial intelligence authorization supports two mechanisms for performing authorization processing. The first mechanism allows us to control authorization using existing Common Language Runtime (CLR) syntax. The second is a claim-based model called the Identification (ID) model. Artificial intelligence authorization uses an ID model to create claims from incoming messages. The ID model class can also be extended to support new claim formats for custom authorization schemes. This topic provides an overview of the key programming concepts of ID model features and a list of very important classes used in them.

Additionally, the ID model is based on the concept of claims. Claims are grouped into sets and aggregated in the authorization context. The authorization context, which includes

a set of claims, is the result of evaluating several authorization policies associated with the authorization manager. Examining these sets of claims ensures that access requirements are met. This is shown in Figure 7, while Figure 8 illustrates the relationship between these different ID model concepts.

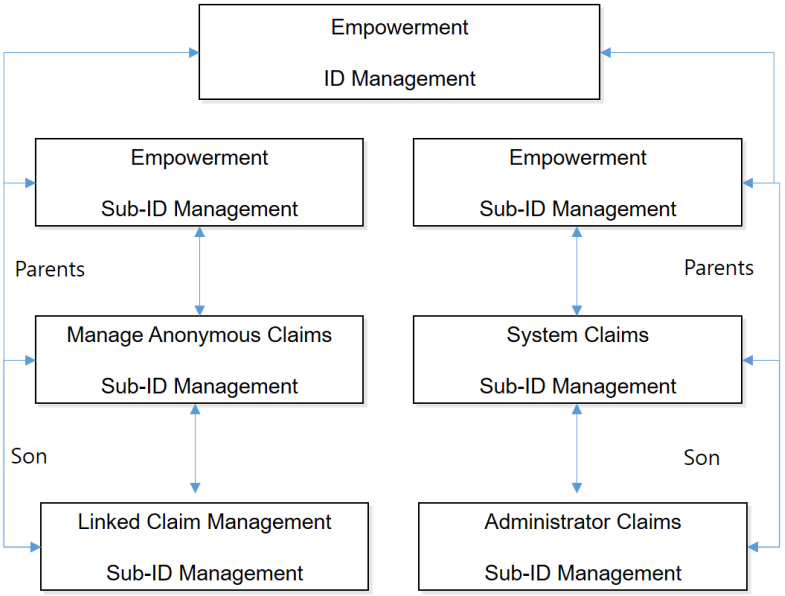

Figure 8. Process of diploma verification Blockchain.

3.7. Diploma Verification Security Plan

Diploma verification security measures include the electronic wallet, which is divided into "Hot Wallet" that is always online and "Cold Wallet" that can be separated from the network and stored separately when not in use.

Electronic wallets in a Blockchain environment are not the concept of Jumoni, where cryptocurrency is stored directly. Blockchain ledger distribution is in the Blockchain system. In other words, an electronic wallet is a place to store certificates that, in a parable, can prove the owner of a cryptocurrency. Therefore, attacking an electronic wallet is not a concept of directly attacking a Blockchain system, but rather a concept of falsifying information through the exploitation of a secret device for personal authentication. It is possible to identify attacks, for example by creating and distributing a Wallet soft operating mainly in a typical computing environment, and moving it to another jigsaw held by the target.

Additionally, by solving the problem of double-payment attacks, the transfer of the original value, i.e., the digital information, once again uses the concept of double payment. When internal protocols are hard-forked, attacks are carried out by using duplicate authentication keys for addresses of existing and new electronic wallets.

Crypto-jacking is a threat to a malicious code distributor's wallet after a certain mining operation by a PC infected with the internet, which can be found in cases due to the recent frequent infection of Chaeguk malware. The attack is not direct financial damage, but it results in the theft of computing power. Computer performance degradation indirectly causes damage such as reduced work efficiency. Recently, web cryptojacking attacks have also occurred frequently. A web cryptojacking blackmailer planted malicious Java Script Code on certain websites. The number of mining infections is increasing, whereby computing power returns normally without installing separate software as soon as the attacker enters the website.

Re-entry attacks are attacks that exploit vulnerabilities caused by recursive functions among the codes that make up Smart Contract. In other words, the term Re-entry Attack applies for transactions such as withdrawals of cryptographic assets and then requests the same new transaction again before the end of the previous transaction. Replay attacks are

also possible in Blockchain environments. Replay attacks in a Blockchain environment are an attack method that exploits the characteristics of a hard-forked basic Blockchain system, which uses the same authentication key of each system when a valid transaction is entered into the Smart Contract of the new Blockchain system. For example, the target of the attack executes unintended transactions by intercepting data in the stage of conducting transactions within the underlying Blockchain system before the target is hard-forked and retransmitted in the newly vivid Blockchain system without performing a separate decoding process. Such attacks can cause unwanted transactions to continue, preventing legitimate transactions and intentionally consuming them.

3.8. Certificate of Diploma Verification

This deals with how authentication takes place inside the Blockchain and user authentication and device authentication using Blockchain. Bitcoin performs signature verification in the process of verifying whether the coin is owned or not, that is, whether the remittance transaction is valid. Ethereum verifies the requestor's signature in all smart track execution as well as coin's remittance and executes the contract using the identified id. Hyperledger performs authentication on all entities based on Public Key Infrastructure (PKI) and provides a separate Certificate Authority (CA) for this. There are four ways to authenticate using Blockchain: a basic authentication information repository, a certification information repository, a verification system for authentication information, and an authentication token platform. It is important to use Blockchain as a shared repository that cannot be falsified, but it is challenging to solve the Oracle problem. Inter-device authentication requires cooperation and a consensus structure of other devices to respond to high-level attacks, such as ghost attacks, which is effective if Blockchain is applied to this end. In addition, the number of nodes was experimental, consisting of 11 nodes.

3.9. Validated UML and Source Code Designs

UML was designed using a class diagram (see Figure 8). Multi-ANN classes were created and Serialize0p (s: stream), GetBlockHeader(): ABlockHeader values were received. This class inherits the Mblock Header, hashHiddenBlock: unit512, hashMakovRoot: unit512, biasTime: unit64, tradeNonce: unit64 and brings it to the value of Ablock Index. AhashBlock: unit512, Aprev: MBlockIndex*, vHeight: int, vTx: int, vTime: unit32. blockConsensus class is set to MultiPros(a: binary), SetM(): ABlockHeader (see Figures 9–11).

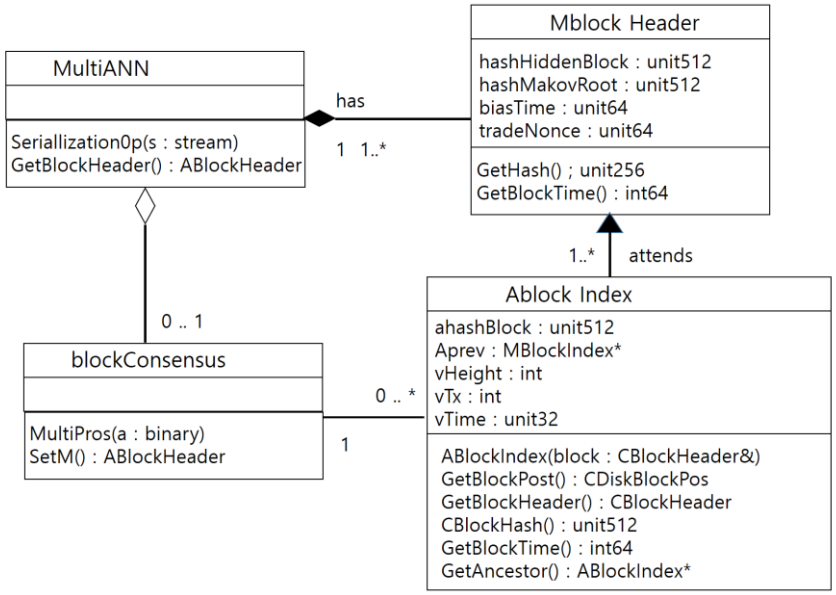

Figure 9. Validated UML of class diagram.

```
public interface multiANN {
    void open();
    void close();
}

public class blockConsensus {
    public void open () {
        System.out.println("open method")

    }
  public void close(){
    System.out.println("open.method")
  }

}
```

Figure 10. Source code multi-ANN.

```
public class Ablock index {
  private Mblock header:

    public Ablock(){
        rank = new Ablock();

    }
  public void AblockHeader(){
    System.out.prinln(Mblock.hashHiddenBlock());
  }
}

public class Mblock {
  privstr int hashMakovRoot ;

  public int biasTime() {
    return hashMakovRoot;
  }
}
```

Figure 11. Source Ccode Ablock.

The source code will also be released to the GITHUB. (https://github.com/erikzhang/leveldb, accessed on 29 April 2022).

A source code should be written with OSS (Open Source Software) so that anyone can be invited.

For the design of the source code, the Class Diagram is designed among UML. First of all, Multi-ANN mainly represents the type of block. Depending on the type of block, various blockheads can be enjoyed. It also belongs to MBlockHeaer. Verification work is being carried out through hash HiddenBlock, hashMakovRoot, baisTime, Trader Nonce, etc. On top of that, we use ashBlock value and Apache, vHeight, vTx, and vTime for verification. The source code also plays a role in creating a blockConsensus algorithm. The ABlockHeader values are passed through MultiPos and SetM(a) values and received as factors.

The source code in Figure 9 has already been set to the value of the agreement. First, we verified the source code. The above source code algorithm specifies the variable in "shape_attributes". In addition, this value is bound to be set as the value of a one-dimensional array with variables. Additionally, the all_points_x value has created an increasingly continuous performance. Here, you can see variable values, such as 588,617,649,673, etc., which are the pointers to the array are stored.

Figure 11 also illustrates logic and algorithms that are verified using repetitive statements. This algorithm specifies the category_id value as a variable using a repeating

statement. After that, the index value of the ablock in the public class is private and the Mblock is the header value. It also creates new products through Ablock. It also inherits for Ablockheader. Then, the hashMakovRoot variable is used to return the biasTime and take it. The values of variables such as fileref, size, and filename are compared and the repeated text is created and compared to try and ease values.

Additionally, this source code brings the actual address value from item2. To begin, an array is placed in the values of scsle, viewpoint, zoom_in, and landmarks. Additionally, it is easy to understand that these array values are memory values in artificial intelligence. At the end, the category_name brings up the value representing "short sleeve top", as show in Figure 12.

```
public class blockConsensus {
  private List comment ;

  public void Ablock(Comment comment){
    coment.add(comment)
  }

  public class comment {

    private Multipro;

    public void SetM(setM) {
      this.SetM = SetM ;
      SetM.addComment(this)
    }
  }
}
```

Figure 12. Source code Ablock.

4. Verification Method of the Study

4.1. Key Management Method

After generating a private key and a public key on the client server, the private key is encrypted and stored as shown above. In principle, pin numbers shall be kept in a place with a high level of security, such as HSM. If a private key or pin number is leaked, the existing number is expired and a new key pair is created and renewed. To maintain a high security level, we continuously and periodically generate new key pairs to replace existing key pairs. The task of registering fingerprint values of electronic documents can be used universally. This document assumes that a financial firm's employee terminal requests fingerprint registration of electronic documents, especially using ODS (outdoor sales). Four tasks with high frequency during financial operations are shown in Figure 13.

(1) Document registration request: Upload the original document for the electronic document authenticity service from the employee terminal.
(2) Request document SHA256 hash: Extract the document's fingerprint value using SHA256 hash from the client's server.
(3) Decode ECDSA private key encrypted by customer: Decode ECDSA private key encrypted in customer's separate storage and bring it to server.
(4) Create transactions using private keys: Create Blockchain transactions using the decrypted customer private keys. The address of the sender and receiver is the address of the customer's Blockchain.
(5) Generated transaction Blockchain registration: Signed transactions with customer's private key are registered on the Blockchain.

Data Payload: {"hash": Document_Finger_Print}

(6) Decryption of Decrypted Private Key: Destroy the Decrypted Private Key used in the transaction signature on memory.
(7) Blockchain registration result: Transaction registration result is received.

(8) Registration results and registered Blockchain index delivery: Transaction registration results are transferred to employee terminals and indexes (addresses) registered on the Blockchain are delivered to customers.

Blockchain index: TXID + VOUT

(9) Insert Blockchain Index: Inserts the received Blockchain index into the original PDF file.

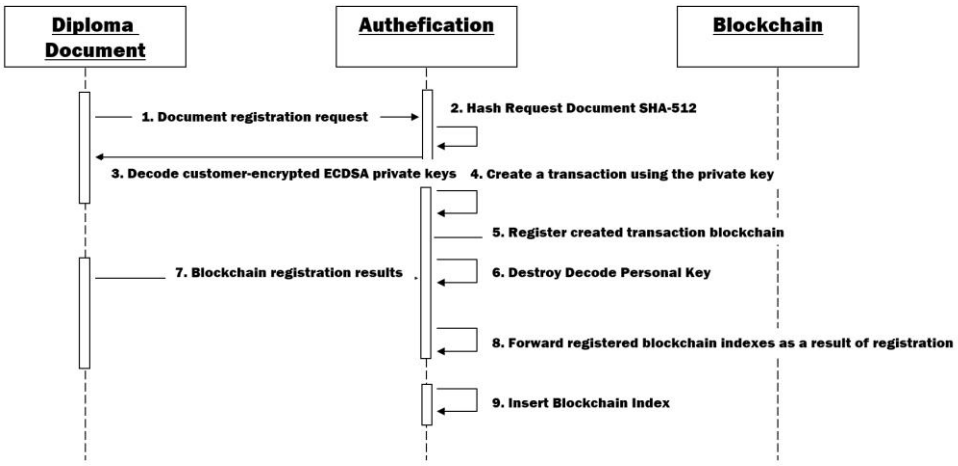

Figure 13. Registration protocol.

4.2. Document Value Verification Protocol

(1) Document verification request: Upload the document requesting verification from the employee's terminal to the client company (see Figure 13).

(2) Blockchain index extraction: The client extracts the Blockchain index value that was inserted when the document fingerprint value was registered in the requested document.

(3) Request document SHA256 hash: Hash the customer's requested verification document using SHA256 to extract hash values.

(4) Hash value lookup request: Using the Blockchain index value extracted from No. 2, the original hash value of the document registered in the Blockchain is requested by the Get method.

(5) Registered hash value transfer: Return the hash value of the registered document on the Blockchain using the TXID and Vout offset of the Blockchain in Figure 14.

Data Payload
{
"tx": Registration Blockchain Transaction ID,
"vout": Registration Transaction vout,
"confirmations": confirmation Count,
"timestamp": stamp date,
"Hash": the document fingerprint value,
}

---

(6) Hash value comparison: Determine the authenticity of the document by comparing the hash value of the document requested for verification three times with the original hash value registered on the Blockchain five times.

(7) Return Result: Return whether the document has registered or authentic fingerprint values.

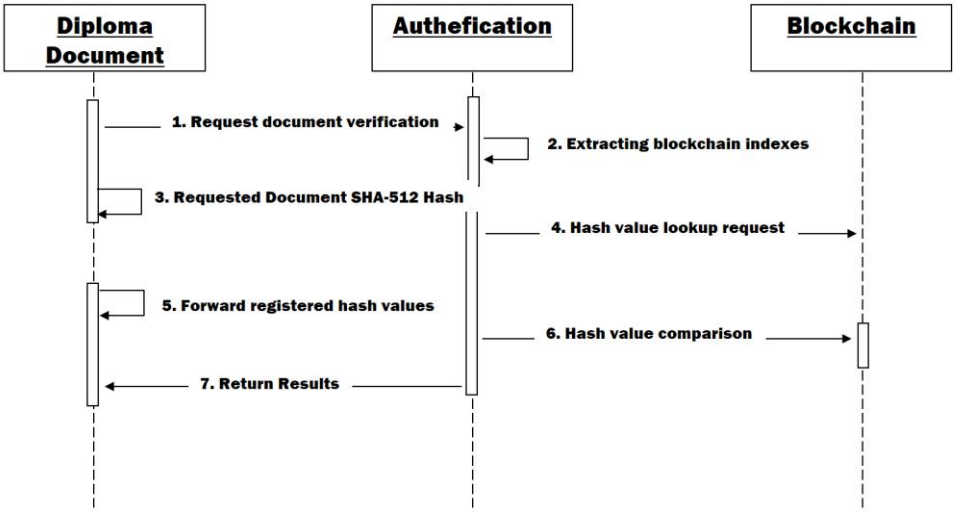

Figure 14. Verification protocol.

4.3. Verification Plan

Due to the nature of the service, the electronic document verification service must be entrusted to a third party to keep and verify data. Therefore, services become institution-dependent and neither the permanence of data or the internationality can be guaranteed. Providing this service based on Blockchain not only allows data to be stored permanently, but also does not have any company dependence, thus securing internationality.

5. Performance Evaluation and Limitations of the Research

5.1. Experimental Environment

In order to conduct a block chain test that can measure the quantitative performance of the block chain for proper evaluation of the quantitative target items, the original data of the graduation certificate is verified in advance using artificial intelligence. Objective and fair performance measurements are made according to the verification of the graduation certificate image stored on the Blockchain node in the early stages. Among the quantitative goals, the test classification details provided by the block chain test are achieved through the block chain test tube. In addition, servers of the right size for the node are built in advance for performance testing. Additionally, the test server was tested using 30 servers. The Central Processing Unit (CPU) used a 16 Core server and Read Access Memory (RAM) used 64 GB of memory. Storage is also load-balanced with four Solid-State Drive (SSD) 500 GBs. Additionally, node specifications may change depending on the results of the operating environment analysis. Therefore, we experimented with a test environment.

In addition, Blockchain testing refers to writing and reading items such as block fixing performance, block reference performance, and block capacity expansion performance, as well as testing the entire Blockchain for node failure response, data integrity and secure key management. The experimental environment is presented to produce results. Additionally, we experimented with 200 rounds using many Graphics Processing Unit (GPU) servers.

(a) Use servers of the right size for the node;
(b) Enable CPU/RAM in range for common nodes;
(c) Use popular SSD storage;
(d) Use a single network considering the actual operating environment;
(e) Node specification;
(f) Number of servers: 30;
(g) CPU: 16 Core;
(h) RAM: 64 GB;
(i) Storage: SSD 500 GB $\times$ 4 EA;

(j) Node specifications may change depending on the results of the operating environment analysis;
(k) Depending on the test environment, NVMe may be used instead of SSD;
(l) Network AWS Cloud System.

Table 2 shows the results of an experiment with software and hardware such as Bandwidth and Geekbench 5.0 for LINUX.

Table 2. Experimental Condition for Performance Evaluation.

Infomation	Spec	Core
Bandwidth	5 TB	TeraByte
Geekbench 5.0 for LINUX	5.324	Version
Hardware	Depends on user enviroment	S/W
Software	HTML5	Chrome

5.2. Experimental Condition

Measure the total number of transactions processed per second per channel, the maximum value of a multichannel that can be generated, and the time it takes for transactions to be processed that cause a change in the state of two or more channels being managed (see Table 3).

Table 3. Experimental Condition for Performance Evaluation.

Major Performance	Spec Unit	Evaluation Measuring Technique
Concurrent Transaction Processing Count	Unit	Create multiple channels and propagate transactions to the transaction generator
Number of Concurrent Transaction Types	TPS	Create a multi-channel and check the operation of the channel
Number of Chain Splits	EA	The platform creates a chain to check the chains
Number of Agreement Algorithm Supports	EA	Select consensus algorithms via platform to ensure chain behavior after deployment
Concurrent Transaction Processing Count	TPS	Create multiple channels and propagate transactions to the transaction generator
Number of Concurrent Transaction Types	EA	Create a multi-channel and check the operation of the channel
Number of Chain Splits	EA	The platform creates a chain to check the chain's
Number of Agreement Algorithm Supports	EA	Select consensus algorithms via platform to ensure chain behavior after deployment

5.3. Classification of Motions

The high-performance multi-Blockchain platform, which is applied with multi-chain division and channel acceleration for the certificate of graduation, develops core technology and a Blockchain platform to test. The development of core technology is divided into high-performance channel technology, multi-agreement support technology, and multi-channel technology, and the development of the Blockchain platform is applied to Blockchain standardization and referenced; the Platform test and measurement test are conducted to evaluate smart contract development and performance measurement (see Figure 15). A total of 500 nodes were obtained with an average of 200 times, although the results of the one-time simulation were about 4000 Transaction Per Second (TPS), while at the same time, a diploma file based on the Blockchain was agreed upon (see Figure 15). The average value of 200 averages also shows performance information of approximately 4100 TPS (see Figure 16).

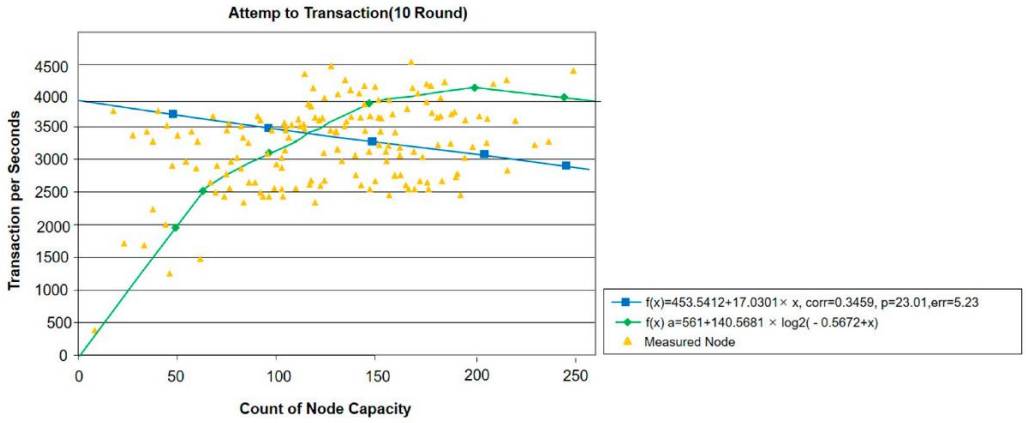

Figure 15. Blockchain Validation Results (1 round).

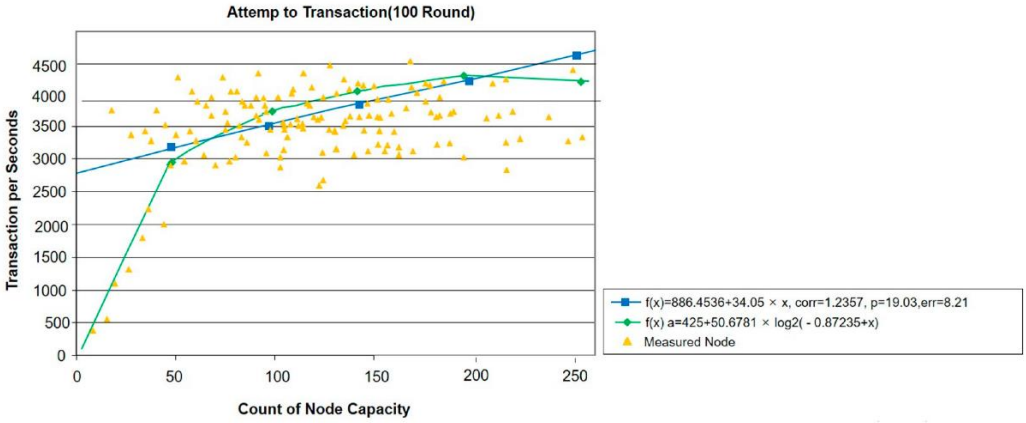

Figure 16. Blockchain validation results (200 rounds).

The result also shows performance data of 4000 TPS per second for the simulation of 1 round. This was designed by the GPU Server considering its characteristics. Additionally, when simulating 200 rounds, the average value is 4100 TPS, which shows higher performance data. The results of this experiment were derived by constructing the experimental environment by constructing 11 paddles. Simulations were also derived from a number of experiments in these experimental environments.

The Blockchain system evaluation criteria consist of quality, repair operation, and cost, and are secured to the characteristics of Blockchain technology based on the quality evaluation criteria (SQuaRE) of centralized systems and software. Quality measurement items are classified as efficiency, compatibility, extension, reliability, security, and portability, and the evaluation criteria are constructed with a total of 20 sub-items. Repair and operability were classified as modular, reusable, interpretable, modifiable and testable. Finally, the costs were classified into research and development (R&D), implementation, repair and operation, and the evaluation criteria were organized, with a total of seven sub-items.

After conducting 200 experiments by dividing Atemp to translation into nodes, we found the average value. A variety of performance results were present in the similarity test of artificial intelligence. In this distribution chart, the count of node performance information is obtained and the distribution is considered to be the best in about 300. The Measure Node value is also an algorithm that affects various results. In addition, we performed 1 round on Blockchain Validation Results and repeatedly tested 200 rounds on Blockchain Validation Results, and the resulting values for the test were approximately 4000 TPS. This value is the result pack. It also shows performance data.

We compared the Blocknode value with four experimental values. The consistency, performance, and analysis results are shown. Additionally, Figure 17 shows the distribution

plot using distribution degree value. The distribution plot shows that the scatterplot is high. As you can see, the scatterplot is evenly distributed to improve the quality (Figure 17).

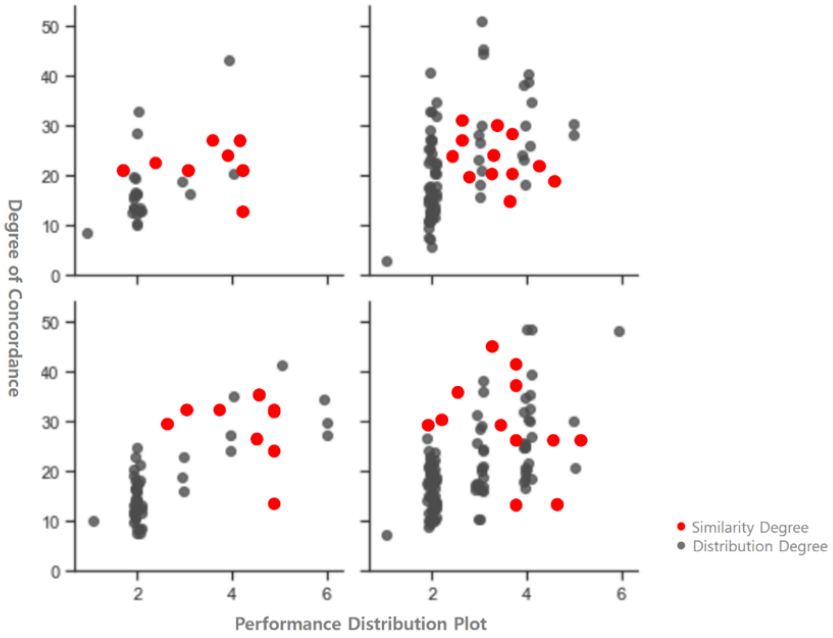

Figure 17. Analysis results of the degree of concordance, performance distribution plot.

In addition, the analysis of artificial intelligence distribution diagram was conducted using a four-point method, and the distribution chart was evenly distributed, thus confirming the diploma with the highest similarity.

First, the game was designed and developed to write all the data in the game on the Blockchain so that the transaction can be performed excessively as much as the commercial service on the Blockchain. It is not necessary for ordinary Blockchain DApp to list all transactions on the chain. However, this test needs to overestimate the number of these transactions in securing test results that are expected to be huge services through limited users. Accordingly, all transactions are designed to be described on the chain.

Secondly, games developed to create a test environment were distributed and installed on cloud servers in six global regions. The test was also performed for about 15 days.

Thirdly, based on the number of transactions collected through tests and Transaction Per Second (TPS), improved performance and scalability were verified through comparison with the existing Blockchain platform or DApp's Transaction Issue and TPS.

In addition, based on this, this study aimed to measure chain performance in a test environment similar to a commercial environment that could not be measured with the existing methodology. The Blockchain records all the history of transactions in the distributed ledger. In the case of a general public Blockchain, the distributed ledger is open to all, and through this, the user can trust the transaction history recorded in the ledger without a third party or a trust agency that guarantees the history. Based on this technical understanding, distributed applications (DApps) have emerged, and the computational history of these DApps is also disclosed to everyone through the portal site. In general, in the Blockchain industry, such portal sites are called Block Explorer. Block Explorer lets users know the content and history of transaction, the number, and success/failure. Accordingly, this paper selected one type of Blockchain platform to verify performance by implementing the game, and developed one type of block explorer that can view diploma data and maximum TPS, transaction, and block history. In addition, the goal is to secure data for use equivalent to the actual environment through the overuse of transaction records recorded on the distributed ledger of the Blockchain, so all data generated in the game are designed to be recorded in the distributed ledger.

5.4. Comparison with Previous Studies

Table 4 compares the performance between VISA and the existing Blockchain platform and expresses it as a percentage. Based on this, it can be seen that the maximum acceptance TPS of the Ethereum platform used by the majority of DApps is about 30 TPS, which shows 0.125% performance compared to the most representative VISA among financial services, and only 15% performance compared to PayPal. Considering that PayPal is a single fintech service, the performance of Ethereum, a driving platform for various DApps, will be further evaluated. On the other hand, the maximum TPS of DApp, the system presented in this study, was 4000. It was verified that the platform under evaluation showed at least 50 times more performance than the maximum TPS of Ethereum's entire chain based on the maximum TPS of a single DApp in a commercial service environment.

Table 4. Comparison with previous studies.

Blockchain Project Name	Year of Release	Maximum TPS (Internal Test)	Performance Versus VISA
Bitcoin	2009	10	0.0417%
Ethereum	2015	30	0.125%
Eos	2018	3000	12.5%
Our Blockchain	2022	4000	17.8%

5.5. Performance Attacker Analysis

This is a meta-model for Blockchain-based smart contract design. It consists of contracts and components, such as Attribute and Function, to provide the functionality of smart contracts, which are included within the block along with translation, which provides transaction history. Proof of work relationships are formed between blocks and are referenced by an account within the Blockchain. Between accounts, Nerutooks are constructed. This is the design notation of the contract property. It uses the grammar of Unified Model Language (UML) and defines an option in the field of visibility. The data type uses the type provided by Solidity. It is a method of designing a function of the contract. We specify OPTION before the function, including visibility, and include additional approaches provided by the solidity language. The conversion type designs additional data types, such as the basic data types Boolean, int, uint, and address corresponding to the account address value. This is the relationship between contract function design and solidity code. It should also be implemented with OPTION and function names changed, and OPTION should be preceded by a returns reservation term. The dynamic design of the contract utilizes an ordered diagram of object-oriented design techniques. The dynamic design is designed based on the context defined by the static design, and includes the accounts and block instances within the Blockchain. Instances in the Blockchain are defined using stereotypes, and the definition of service flow is also defined using stereotypes. There is also an instance and service flow stereotype within a Blockchain.

As with contract distribution, dynamic design for synchronization is also possible. Deployment and synchronization are performed within the Blockchain platform, so the design is similar, but dynamic design of the features within the contract must be designed differently each time. This is a detailed design for the contract distribution. The distribution must be distributed between blocks connected within the Blockchain, and is created by distribution through repetitive statements and distribution to blocks in other accounts. At this time, the creation is confirmed within the Blockchain by proof of work. The distribution is mainly carried out by the Blockchain platform, and it is applied to the Blockchain platform after designing through the action design which accounts should be distributed.

6. Discussion and Future Application Model

6.1. Discussion

Recently, with the development of eLearning, various types of education are being provided. In particular, the number of institutions that provide education online is increasing, and universities and middle and high schools are following suit. All over the world, universities integrate into the MOOC system and provide education. Nonetheless, cases of forgery occur in receiving academic certificates, such as graduation certificates, and at the time of being hired for a job or returning to school after finishing education. This study attempted to investigate the transparent academic management system by using the Blockchain to prevent forgery of academic records such as diplomas. This research will be meaningful only if all universities join in the future. Nonetheless, we want to perform verification through the design of the agreement node between CNN and Blockchain of artificial intelligence. Although it is still meaningful for all educational institutions to participate and join the node, we hope to expand it based on these studies in the future.

Additionally, many basic Blockchain-based graduation certificate systems are also being tried. MIT Engineering, Malaysia's Ministry of Education and Korea's Ministry of Education are trying. The reason for this is that there are expectations that Blockchain technology can solve the problem of academic forgery. The argument is that it should be applied to various fields such as degree management, real estate, and distribution network management by using the principle of Blockchain that cannot modify or delete data. In fact, in 2017, Massachusetts Institute of Technology (MIT) issued a Blockchain diploma to 111 graduates. BlockSuits, a Blockchain-based academic document certification platform developed by MIT Media Lab, allows degree recipients to use digital certificates without recertification in the future if they receive an official certification from their alma mater once using the BlockSuits application. If a Blockchain diploma is issued, the applicant can submit to the company a digital certificate of the degree recorded on the Blockchain through an app instead of a paper certificate during the recruitment process. The entity may view this certificate at no additional cost. Both the creation and modification of copies are recorded, so manipulation itself is impossible. As such, the Blockchain-based degree management system can secure trust in degrees without having to go through the existing complicated verification process. Furthermore, it can address social costs in all areas that require certification, such as administration, education and finance. However, the graduation certificate of this study has the advantage of adding algorithms by adding the existing Blockchain consensus algorithm method and Mask-CNN and Fast-CNN method soul. The objection to this is that it hands over the reliability of the verification process to the agreement on the encryption algorithm of the Blockchain. It also has the advantage of using deep learning algorithms to verify the original existence of the diploma image stored in the block at the beginning of the actual Blockchain data. This is a different study from the existing diploma Blockchain (see Table 5).

Table 5. Comparing the existing Blockchain diploma with the AI Blockchain diploma of this study.

Item	Existing Blockchain Diploma	AI Blockchain Diploma of This Study
Initial Data Verification	No	Artificial Intelligence Utilization Verification
Graduation Certificate Image Verification Method	Human Verification	Mask-CNN, Fast-CNN
Consensus Mechanism	Dependence on Consensus Algorithm	Verification of Early Image of Consensus Algorithm and Artificial Intelligence Technology
Reilability	High	Very-High

6.2. Application Model

An empirical model has been implemented for applications to certify diplomas. Figure 18 shows the main screen for validating and certifying a diploma. The main screen

proves the diploma. Additionally, the cross-chain using the mainnet as shown in the picture. It also shows a screen that allows you to use dApp. Additionally, the screen is the main screen to verify the diploma and provides UI/UX for use in both mobile and PC versions.

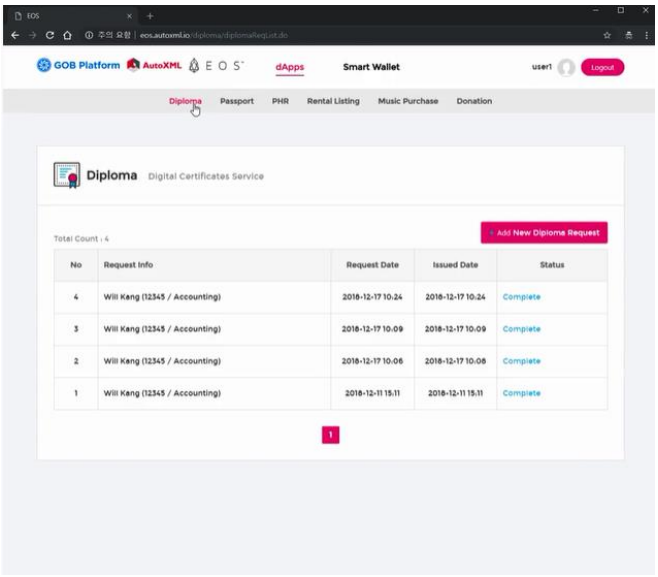

Figure 18. Initial screen for ceritificate of diploma certification.

As shown in Figure 19, the main screen is designed to be cross-browsing for PC and mobile devices. Figure 19 shows that the user must select their year of graduation, search for their diploma, and then be verified with a Blockchain. In addition, we have accessed the school's website and certified it with my ID and PWD, and even if such authentication information is hacked, the Blockchain has the authentication information, so we can protect it from hacking based on this authentication information. Additionally, the screen requires personal authentication after logging in and comparing the actual date of graduation with the original one. In addition, information about the date is initially entered and the date value entered is stored in the Blockchain code. In addition, the date and time are stored in Blockchain blocks, making forgery impossible.

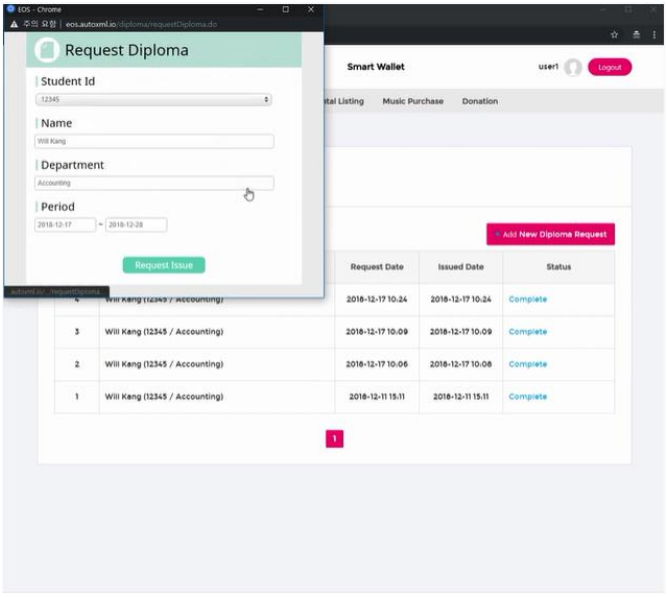

Figure 19. Diploma selection screen.

In addition, we are carrying out similarity test with artificial intelligence. Figure 20 shows a screen that is verified by requesting the original diploma and the Blockchain diploma that has been verified. First of all, student ID refers to the class number. Additionally, the name value is called. Additionally, the figure shows the detailed screen where users can obtain a graduation certificate with safe certification information. Additionally, the picture is a system that can be safely certified as a smart country through smart wallets. In this way, users will obtain a safe and verified graduation certificate. Additionally, the screen updates personal ID, name, search period, and verification time by searching based on actual artificial intelligence-based Blockchain Request ID.

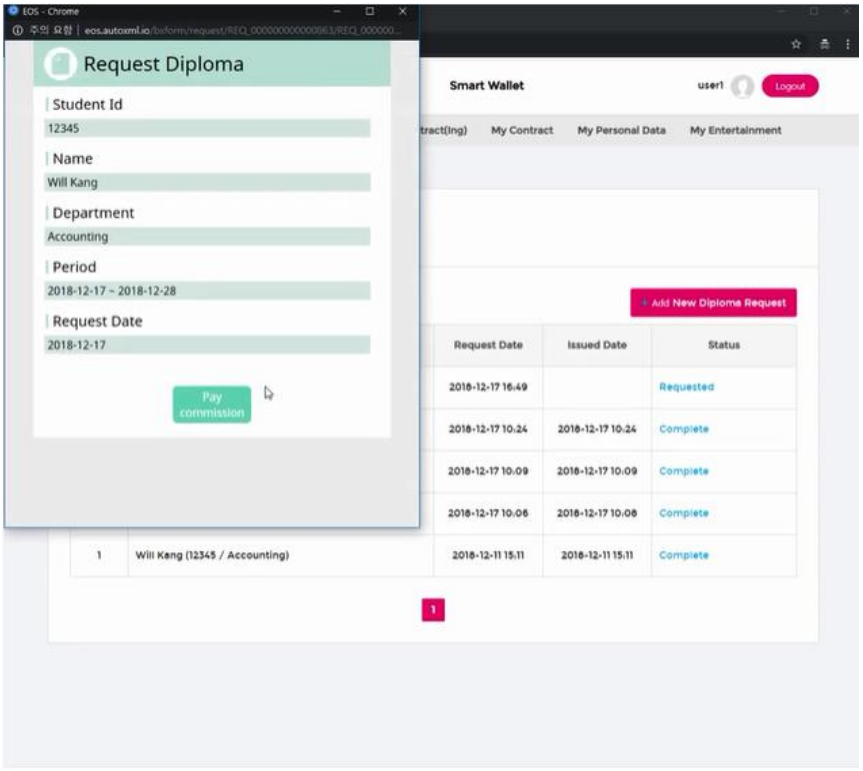

Figure 20. Diploma request screen.

Figure 21 shows a proven diploma is saved to a block node on a smart country screen. Additionally, BlockNum has the block number of graduation certificate. It then calls up the value of the data name of the Extensible Markup Language (XML). The Server Info Show then calls the data from the server. Transaction How also brings up the transactionable data code. It also brings up these data values. Block Number contains the value of the user's Node ID to verify that it cannot be falsified. Additionally, transaction refers to the actual transmitted value. The xmlName transfers the values of the existing eXtensible Stylesheet Language (XSL), and the Transaction Show can see the source code of the actual verified diploma).

Appendix (Screen) refers to the process, results, and performance information of proof of graduation certificates using actual Blockchain.

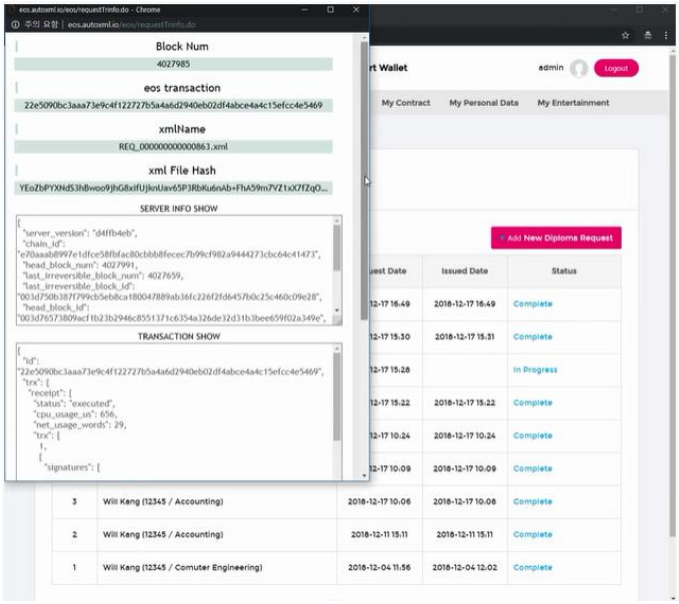

Figure 21. Graduation transactions storage screen.

7. Conclusions and Future Work

Certificates are often falsified such as fake diplomas and forged transcripts. Thus, many schools or educational institutions have begun to issue diplomas online. Although diplomas can be issued conveniently anytime, anywhere, many counterfeit diplomas are often found through hacking and forgery. As such, a Blockchain diploma that can verify academic records such as graduation certificates through Blockchain and artificial intelligence is presented. In addition, an automatic translation system, which involves natural language processing, is used to perform verification work that does not require an existing public certificate. This study also proposed algorithms that encrypt using hash functions and map data with different lengths of hash functions into data with fixed lengths. In addition, the methodologies and models for research on artificial intelligence Blockchain verification are set. Blocknode technology aggregates node management technology, node grouping technology, node communication protocol, and so on.

It also provides the ability to manage the list of nodes, establish access to nodes, and set and manage the node's connection status and role of nodes, etc. Through node grouping technology, nodes are grouped together to provide the ability to set up items for nodes for each corresponding node group or to distribute chains and control roles. In Block-validated Mask R-CNN Head Architecture at PN, the backbone already contains res5, providing a more efficient head with fewer filters. For block verification Mask R-CNN Loss Function, R-CNN processes the task in several steps. First, the Selective Search algorithm is used to find the Region Proposal or Binding Box that finds the image area where the object is located. Selective Search combines adjacent pixels with similar colors, strengths, and patterns. Block verification Mask R-CNN adds a network (CNN) to the Faster R-CNN that masks whether or not each pixel corresponds to an object and stores the mask in a block node called Binary Mask. After designing the algorithm, the consensus algorithm Multi-Layer ANN is presented. The agreement algorithm Multi-Layer ANN backpropagation and the agreement algorithm Hidden Markov Model as well as the agreement algorithm Bias-Variance Tradeoff are proposed. The verification UML and source code required for research were designed. The high-performance multi-Blockchain platform, which sets the environment for the experiment and applies multi-chain division and channel acceleration for certificate of graduation, develops core technology as well as the Blockchain platform to conduct the test. The development of core technology is divided into high-performance channel technology, multi-agreement support technology, and multi-channel technology, and the development of the Blockchain platform is applied to Blockchain standardization

and referenced. The platform test and measurement test are conducted to test smart contract development and performance measurement. A total of 500 nodes were obtained by averaging 200 times, and a Blockchain-based diploma file was agreed upon at the same time. It shows performance information of about 4100 TPS.

In addition, the analysis of artificial intelligence distribution diagram was conducted using a four-point method, and the distribution chart was evenly distributed, confirming the diploma with the highest similarity. In addition, each transaction history, whether a diploma is true or not, may be different in length if it is presented in text, but converting it into a hash function always suggests more than a certain length of SHA-512 or higher. It is then verified using the time stamp values. These chaining codes are designed. It also provides the necessary experimental environment and constructs at least 10 nodes. The verified values are then analyzed. This paper proposes these natural language processing-based Blockchain algorithms.

However, these Blockchain certificates are bifurcated using the existing public certificate method. Additionally, in the future, the existing document issuance system will have to invest a lot of money to prevent forgery and alteration, and protect against hacking, and users will have to install numerous security programs to obtain the documents issued. In addition, since each public institution uses different security programs, there are dozens of programs that must be installed on computers. Although it can be installed on a PC, it is often not supported in mobile or smart pad environments. However, there is a limit to how the Blockchain platform solves these problems. This is because the Blockchain platform itself has a strong advantage in security, and it is easy to manage issuance details and change the history. Even if you submit a copy, you can use the Blockchain to prevent denial in the event of a problem later. However, the total size of the block chain, including transaction data, is very small, so it is virtually impossible for ordinary mobile devices to participate as full nodes that can be verified on their own. In other words, participating in a Blockchain network as a complete node that can directly verify transactions on its own without a third trust agency requires high computing power. Artificial intelligence technology is also needed because it allows selective management of the necessary data.

Additionally, performance of VISA and the existing Blockchain platform is compared and and expressed as a percentage. Based on this, it can be seen that the maximum acceptance TPS of the Ethereum platform used by the majority of DApps is about 30 TPS, which shows 0.125% performance compared to the most representative VISA among financial services, and only 15% performance compared to PayPal. Considering that PayPal is a single fintech service, the performance of Ethereum, a driving platform for various DApps, will be further evaluated. On the other hand, the maximum TPS of DApp, the system presented in this study, was 4000. It was verified that the platform under evaluation showed at least 50 times more performance than the maximum TPS of Ethereum's entire chain based on the maximum TPS of a single DApp in a commercial service environment.

Additionally, the limitation of the paper is that if the original file stored on the block chain server node is falsified or hacked for verification in the first place, it can cause problems. This is also a threshold for all Blockchains. However, it is necessary to study mechanisms to verify the first Genesis block, and also to study the artificial intelligence block chain-based graduation certificate system from the perspective of OSI 7 Layer, including network security, server security, and intercept security until the original image was registered in the original node.

In addition, this study proposed and developed a meaningful tool model to verify the scalability and performance of the Blockchain platform, but it also had the following limitations. It cannot be said that the maximum TPS is absolutely higher than the amount of activity in general IT commercial services. Therefore, there is a limitation in concluding that both the performance and scalability of the general IT commercial service level of the platform to be verified based on the data from this study. However, considering that a large amount of usage has been collected and compared to the existing DApp, it can be supplemented by conducting tests on more users in the future. Second, the results of this

study were validated only in a virtual environment. Usually, services using Blockchain platforms generally use Bitcoin's finance as it covers various services such as logistics, medical care, and the environment in Lohae, and it is necessary to verify them through development and testing in other environments in the future.

Funding: This research received no external funding.

Acknowledgments: This paper was supported by Joongbu University Research & Development Fund, in 2021.

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

References

1. Corea, F. AI and Blockchain. In *An Introduction to Data; Studies in Big Data*; Springer: Cham, Switzerland, 2019; Volume 50, pp. 69–76.
2. Huh, J.H. An efficient solitary senior citizens care algorithm and application: Considering emotional care for big data collection. *Processes* **2018**, *6*, 244. [CrossRef]
3. Jirgensons, M.; Kapenieks, J. Blockchain and the Future of Digital Learning Credential Assessment and Management. *J. Teach. Educ. Sustain.* **2018**, *20*, 145–156. [CrossRef]
4. Chen, Y. Blockchain tokens and the potential democratization of entrepreneurship and innovation. *Bus. Horiz.* **2017**, *61*, 567–575. [CrossRef]
5. Kshetri, N. Blockchain's roles in meeting key supply chain management objectives. *Int. J. Inform. Manag.* **2018**, *39*, 80–82. [CrossRef]
6. Wang, W.C.; Chang, Y.J.; Wang, H.C. An Application of the Spatial Autocorrelation Method on the Change of Real Estate Prices in Taitung City. *ISPRS* **2019**, *8*, 249. [CrossRef]
7. Watkins, T. Cosmology of artificial intelligence project: Libraries, makerspaces, community and AI literacy. *AI Matters* **2020**, *4*, 134–140. [CrossRef]
8. Dima, G.A.; Jitariu, A.G.; Pisa, C.; Bianchi, G. Scholarium: Supporting Identity Claims Through a Permissioned Blockchain. In Proceedings of the 2018 IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI), Palermo, Italy, 10–13 September 2018.
9. Löbbe, S.; Hackbarth, A. *The Transformation of the German Electricity Sector and the Emergence of New Business Models in Distributed Energy Systems*; Elsevier: Amsterdam, The Netherlands, 2017; Chapter 15; pp. 287–318.
10. Hong, S.; Park, T.; Choi, J. Analyzing Research Trends in University Student Experience Based on Topic Modeling. *Sustainability* **2020**, *12*, 3570. [CrossRef]
11. Radanović, I.; Likić, R. Opportunities for Use of Blockchain Technology in Medicine. *Appl. Health Econ. Health Policy* **2018**, *16*, 583–590. [CrossRef]
12. Sayed, R.H. Potential of Blockchain Technology to Solve Fake Diploma Problem. Master's Thesis, University of Jyväskylä, Jyväskylä, Finland, 2019.
13. Huh, J.-H.; Kim, S.-K. The blockchain consensus algorithm for viable management of new and renewable energies. *Sustainability* **2019**, *11*, 3184. [CrossRef]
14. Drungilas, V.; Vaičiukynas, E.; Jurgelaitis, M.; Butkienė, R.; Čeponienė, L. Towards Blockchain-Based Federated Machine Learning: Smart Contract for Model Inference. *Appl. Sci.* **2021**, *11*, 1010. [CrossRef]
15. Kim, J.-H.; Lee, S.; Hong, S. Autonomous Operation Control of IoT Blockchain Networks. *Electronics* **2021**, *10*, 204. [CrossRef]
16. Alkahtani, M.; Khalid, Q.S.; Jalees, M.; Omair, M.; Hussain, G.; Pruncu, C.I. E-Agricultural Supply Chain Management Coupled with Blockchain Effect and Cooperative Strategies. *Sustainability* **2021**, *13*, 816. [CrossRef]
17. Sladić, G.; Milosavljević, B.; Nikolić, S.; Sladić, D.; Radulović, A. A Blockchain Solution for Securing Real Property Transactions: A Case Study for Serbia. *ISPRS Int. J. Geo-Inf.* **2021**, *10*, 35. [CrossRef]
18. Jiang, Y.; Shen, X.; Zheng, S. An Effective Data Sharing Scheme Based on Blockchain in Vehicular Social Networks. *Electronics* **2021**, *10*, 114. [CrossRef]
19. Mosteanu, N.R.; Faccia, A. Fintech Frontiers in Quantum Computing, Fractals, and Blockchain Distributed Ledger: Paradigm Shifts and Open Innovation. *J. Open Innov. Technol. Mark. Complex.* **2021**, *7*, 19. [CrossRef]
20. Sabri-Laghaie, K.; Ghoushchi, S.J.; Elhambakhsh, F.; Mardani, A. Monitoring Blockchain Cryptocurrency Transactions to Improve the Trustworthiness of the Fourth Industrial Revolution (Industry 4.0). *Algorithms* **2020**, *13*, 312. [CrossRef]
21. Ma, X.; Zhou, J.; Yang, X.; Liu, G. A Blockchain Voting System Based on the Feedback Mechanism and Wilson Score. *Information* **2020**, *11*, 552. [CrossRef]
22. Pajooh, H.H.; Rashid, M.; Alam, F.; Demidenko, S. Multi-Layer Blockchain-Based Security Architecture for Internet of Things. *Sensors* **2021**, *21*, 772. [CrossRef]
23. Yang, B.; Garcia-Molina, H. PPay, Micropayments for peer-to-peer systems. In Proceedings of the 10th ACM Conference on Computer and Communications Security, Washington, DC, USA, 27–31 October 2003; ACM: New York, NY, USA, 2003; pp. 300–310.

24. Savelyev, A. Copyright in the Blockchain era: Promises and Challenges. *Comput. Law Secur. Rev.* **2018**, *34*, 550–561. [CrossRef]
25. Hajer, M.; Nilsson, M.; Raworth, K.; Bakker, P.; Berkhout, F.; De Boer, Y.; Rockström, J.; Ludwig, K.; Kok, M. Beyond cockpit-ism: Four insights to enhance the transformative potential of the sustainable development goals. *Sustainability* **2015**, *7*, 1651–1660. [CrossRef]
26. Lee, S.; Woo, H.; Shin, Y. Study on Personal Information Leak Detection Based on Machine Learning. *Adv. Sci. Lett.* **2017**, *23*, 12818–12821. [CrossRef]
27. Mnih, V.; Kavukcuoglu, K.; Silver, D.; Rusu, A.A.; Veness, J.; Bellemare, M.G.; Grave, A.; Riedmiller, M.; Fidjeland, A.K.; Ostrovski, G.; et al. Human-level control through deep reinforcement learning. *Nature* **2015**, *518*, 529–533. [CrossRef] [PubMed]
28. Wang, Z.; Peterson, J.L.; Rea, C.; Humphreys, D. Special Issue on Machine Learning, Data Science, and Artificial Intelligence in Plasma Research. *IEEE Trans. Plasma Sci.* **2020**, *48*, 1–2. [CrossRef]
29. Wang, Y.; Kwong, S.; Leung, H.; Lu, J.; Smith, M.H.; Trajkovic, L.; Tunstel, E.; Plataniotis, K.N.; Yen, G.G.; Kinsner, W. Brain-Inspired Systems: A Transdisciplinary Exploration on Cognitive Cybernetics, Humanity, and Systems Science Toward Autonomous Artificial Intelligence. *IEEE Syst. Man Cybern. Mag.* **2020**, *6*, 6–13. [CrossRef]
30. Hák, T.; Janoušková, S.; Moldan, B. Sustainable Development Goals: A need for relevant indicators. *Ecol. Indic.* **2016**, *60*, 565–573. [CrossRef]
31. Chowdhury, M.J.M.; Ferdous, S.; Biswas, K.; Chowdhury, N.; Kayes, A.S.M.; Alazab, M.; Watters, P. A Comparative Analysis of Distributed Ledger Technology Platforms. *IEEE Access* **2019**, *7*, 167930–167943. [CrossRef]
32. Silver, D.; Schrittwieser, J.; Simonyan, K.; Antonoglou, I.; Huang, A.; Guez, A.; Hubert, T.; Baker, L.; Lai, M.; Bolton, A.; et al. Mastering the game of go without human knowledge. *Nature* **2017**, *550*, 354–359. [CrossRef]
33. DeepMind. AlphaGo Zero: Learning from the Scratch. Available online: https://deepmind.com/blog/alphago-zero-learning-scratch/ (accessed on 27 March 2020).
34. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerComWorkshops), Kona, HI, USA, 13–17 March 2017.
35. Imbault, F.; Swiatek, M.; De Beaufort, R.; Plana, R. The green blockchain: Managing decentralized energy production and consumption. In Proceedings of the 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Milan, Italy, 6–9 June 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–5.
36. Underwood, S. Blockchain beyond Bitcoin. In *Communications of the ACM*; ACM: New York, NY, USA, 2016; Volume 59, pp. 15–17.
37. Duan, B.; Zhong, Y.; Liu, D. Education application of blockchain technology: Learning outcome and meta-diploma. In Proceedings of the2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS), Shenzhen, China, 15–17 December 2017; pp. 814–817.
38. Vidal, F.; Gouveia, F.; Soares, C. Analysis of Blockchain Technology for Higher Education. In Proceedings of the 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Guilin, China, 17–19 October 2019; pp. 28–33.
39. BSTProv: Blockchain-Based Secure and Trustworthy Data Provenance Sharing. *Electronics* **2022**, *11*, 1489. [CrossRef]
40. Zhang, L.; Wang, J.; Wang, W.; Jin, Z.; Zhao, C.; Cai, Z.; Chen, H. A Novel Smart Contract Vulnerability Detection Method Based on Information Graph and Ensemble Learning. *Sensors* **2022**, *22*, 3581. [CrossRef]
41. Jung, S.H.; Huh, J.H. A novel on transmission line tower big data analysis model using altered K-means and ADQL. *Sustainability* **2019**, *11*, 3499. [CrossRef]
42. Huh, J.H.; Seo, K. Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing. *J. Supercomput.* **2019**, *75*, 31233139. [CrossRef]
43. Cocco, L.; Mannaro, K.; Tonelli, R.; Mariani, L.; Lodi, M.B.; Melis, A.; Simone, M.; Fanti, A. A Blockchain-Based Traceability System in Agri-Food SME: Case Study of a Traditional Bakery. *IEEE Access* **2021**, *9*, 62899–62915. [CrossRef]
44. Prodanović, R.; Rančić, D.; Vulić, I.; Zorić, N.; Bogićević, D.; Ostojić, G.; Sarang, S.; Stankovski, S. Wireless Sensor Network in Agriculture: Model of Cyber Security. *Sensors* **2020**, *20*, 6747. [CrossRef] [PubMed]
45. Oad, A.; Razaque, A.; Tolemyssov, A.; Alotaibi, M.; Alotaibi, B.; Zhao, C. Blockchain-Enabled Transaction Scanning Method for Money Laundering Detection. *Electronics* **2021**, *10*, 1766. [CrossRef]
46. Wong, S.; Yeung, J.-K.-W.; Lau, Y.-Y.; So, J. Technical Sustainability of Cloud-Based Blockchain Integrated with Machine Learning for Supply Chain Management. *Sustainability* **2021**, *13*, 8270. [CrossRef]
47. Chen, G.; Xu, B.; Lu, M.; Chen, N.-S. Exploring blockchain technology and its potential applications for education. *Smart Learn. Environ.* **2018**, *5*, 1. [CrossRef]
48. Stefanini, A.; Aloini, D.; Gloor, P.; Pochiero, F. Patient Satisfaction in Emergency Department: Unveiling Complex Interactions by Wearable Sensors. *J. Bus. Res.* **2020**, *129*, 600–611. [CrossRef]
49. Stefanini, A.; Aloini, D.; Gloor, P. Silence is golden: The role of team coordination in health operations. *Int. J. Oper. Prod. Manag.* **2020**, *40*, 1421–1447. [CrossRef]
50. Garrido, I.; Erazo-Aux, J.; Lagüela, S.; Sfarra, S.; Ibarra-Castanedo, C.; Pivarčiová, E.; Gargiulo, G.; Maldague, X.; Arias, P. Introduction of Deep Learning in Thermographic Monitoring of Cultural Heritage and Improvement by Automatic Thermogram Pre-Processing Algorithms. *Sensors* **2021**, *21*, 750. [CrossRef]

51. Bolos, M.-I.; Bradea, I.-A.; Delcea, C. Modeling the Performance Indicators of Financial Assets with Neutrosophic Fuzzy Numbers. *Symmetry* **2019**, *11*, 1021. [CrossRef]
52. Aslam, M.; Albassam, M. Inspection Plan Based on the Process Capability Index Using the Neutrosophic Statistical Method. *Mathematics* **2019**, *7*, 631. [CrossRef]
53. Available online: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4329 (accessed on 30 April 2022).
54. Available online: https://dl.acm.org/doi/abs/10.1145/3467019 (accessed on 30 April 2022).