Hindawi
Mobile Information Systems
Volume 2022, Article ID 9460419, 12 pages
https://doi.org/10.1155/2022/9460419

Research Article

Exploration and Practice of the Acquisition Path of Spoken English for Special Purposes with the Blockchain Technology

Yali Ruan

School of Humanities and International Education, Xi'an Peihua University, Xi'an 710000, Shaanxi, China

Correspondence should be addressed to Yali Ruan; 150832@peihua.edu.cn

Received 10 June 2022; Revised 9 July 2022; Accepted 19 July 2022; Published 16 August 2022

Academic Editor: Chia-Huei Wu

With the increasing trend of globalization, English, as the most widely used language in the world, has become a subject that many people must learn. English for special purposes is mainly applied to some specialized occupations or English in specific professional skill fields. Due to the increasing national demand for professional compound talents, the status of English for special purposes is also getting higher and higher. However, there are still many problems in the curriculum setting of English for special purposes, for example, outdated teaching mode, lack of oral language skills training, lack of students' ability to cope with actual situations, weak teaching awareness of teachers, and lack of analysis of students' needs for English for special purposes, resulting in poor students' enthusiasm for learning and so on. With the support of blockchain technology, combined with consensus algorithm, hash function algorithm, and smart contract, this paper analyzes English for special purposes, establishes an ESP management system and a corpus of spoken English for special purposes, and analyzes the integrity of the corpus data. The test found that when the number of error data blocks is 10, the total number of damaged data blocks and verification accuracy data blocks is about 4% in order to achieve 99% accuracy. Therefore, the integrity of the system is higher when the damage ratio is lower. The system integrity test finds that, with the number of wrong data being larger, when the wrong data block is at 100, 50% of the data blocks of the system integrity are about 1%. The database is complete, which is more helpful for students to study systematically.

1. Introduction

English for special purposes mainly appeared in British and American countries in the 1960s and later developed in China. With the development of global internationalization, people's demand for professional English knowledge in certain fields has also increased year by year. However, in the process of development, there have been a series of problems such as unsystematic learning of professional English vocabulary, weak listening and speaking ability of students, rigid and traditional teaching methods of English for special purposes, and inadequate analysis of students' needs. Combined with consensus algorithm, hash function algorithm, and smart contract in blockchain, this paper analyzed English for special purposes, established an ESP management system and a corpus of spoken English for special purposes, and analyzed the integrity of the corpus data. After verification, the database is completer and more systematic, which effectively improves the efficiency of students' systematic learning of spoken English for special purposes and establishes a professional vocabulary corpus. It meets the needs of students to learn English for professional use and improves students' self-learning awareness. Blockchain technology provides technical support for students to learn spoken English for special purposes.

Based on blockchain technology, this paper analyzes the definition, structure, and classification of blockchain and establishes an ESP management system. Using the core technologies of blockchain, such as consensus algorithm, hash function algorithm, and smart contract, a new exploration of the acquisition path of spoken English for special purposes is carried out. With the support of blockchain technology, the integrity of the database of the English for professional use corpus is higher. Understanding

and improving the curriculum of English for special purposes and analyzing the problems existing in English for special purposes have effectively improved the establishment of the English for special purposes corpus. It provides a good learning tool for students to learn spoken English for special purposes, meets students' learning needs, can effectively allocate teacher resources, and gives full play to students' subjective initiative in learning.

2. Related Work

The advantages of blockchain in dealing with various problems are becoming more and more obvious, and there are more and more researches on blockchain. Miraz and Ali believed that blockchain (BC), the technology behind the Bitcoin cryptocurrency system, was attractive and critical for ensuring enhanced security and privacy for various applications in many other areas, such as the Internet of Things (IoT) ecosystem. Proof of work (PoW) is a cryptographic puzzle that plays a vital role in securing BC by maintaining a digital ledger of transactions. Additionally, BC records the identity of the user using a variable public key (PK), which provides an additional layer of privacy. They surveyed recent research articles and projects/applications to evaluate the implementation of BC enhanced security and identify associated challenges and proposed solutions for BC-enabled enhanced security systems [1]. Yeoh relied on primary data from applicable regulations and secondary data in the public domain to study blockchain and innovative distributed technologies affecting the European Union (EU) and the United States. The findings showed that the smart regulatory hands-off approach adopted by the EU and the US largely boded well for the future innovative contribution of blockchain in financial services and related industries, as well as its contribution to enhancing financial inclusion. His findings provided support for blockchain technology to advance with minimal regulatory brakes for greater value-adding and efficiency gains, expanding accessibility and thus financial inclusion. It helped to draw more attention to the technology underpinning virtual currencies [2]. O'Dair and Beaven found that blockchain technology could have transformative potential for the music industry related to recorded music and the sustainability of the music business. While predictions of widespread disintermediation may be premature, blockchain technology did appear to have the potential to change the role of third parties and make musicians' careers more sustainable. Blockchain can improve the accuracy and availability of copyright data, facilitate near-real-time royalty micropayments, and significantly increase the transparency of the value chain [3]. Ittay saw high potential value in cryptocurrency blockchain protocols or distributed ledger technology (DLT). However, blockchain's requirements and guarantees for cryptocurrencies, from transaction throughput to security primitives and privacy, did not match FinTech's requirements and guarantees. He explored how blockchain research beyond Bitcoin is bridging these gaps and some of the remaining challenges [4].

English for special purposes is mainly used to learn English in a specific field or a specific occupation. This year, the development of English for special purposes is getting faster and faster. Otto P proposed a method for identifying special purpose vocabulary in data-driven learning (DDL) vocabulary activities. He applied his system to the field of civil engineering and found it to be generally effective in recognizing 18 words prevalent in civil engineering writing. In the process, he discussed one disadvantage of the system and discussed two valuable advantages: revealing the role of words in civil engineering discourse and identifying non-engineering words that were easily ignored by lecturers [5]. Gráf reported the results of an empirical study that identified repetition as one of the markers of poor fluency in advanced English learners and contributed to research on *L2* fluency. An analysis of 13 hours of interview recordings of 50 native Czech-speaking advanced English learners found 1905 repetitions, of which the majority (78%) consisted of repetitions of one word appearing at the beginning of clauses and components. Both words were repeated less frequently (19%) but appeared in the same position in the utterance. Longer repetitions were much less frequent (<2.5%). Although there was still a question as to whether this fluency-enhancing strategy should be part of second language teaching, it has been argued that the spoken language learner corpus should also include samples produced by the learner's native language [6]. Chai and Subramaniam found that Computer Media Communication (CMC) has received a great deal of attention in the field of education. They used a mixed approach of case studies to examine the communication strategies of in-service faculty graduate students using the asynchronous WeChat mobile app to solve academic problems and explore their views on the feasibility of using the spoken asynchronous communication program to solve problems. The study found that asynchronous spoken medium triggered "resented speech" patterns that reflected spoken and written characteristics. The problem-solving process in asynchronous spoken language was also mediated using low-frequency communication strategies. The findings provided a rationale for teaching through spoken-language-based asynchronous instructional media in relation to task types and learning objectives [7]. The research is representative of the research on blockchain technology and English for professional use, but the description of the spoken language path is less, and it is still instructive for the writing of the paper.

Using blockchain technology, this paper explores the data integrity of English corpus for professional use. The test finds that when the number of error data blocks is 10, the total number of damaged data blocks and verification accuracy data blocks is about 4% in order to achieve 99% accuracy. Therefore, the integrity of the system is higher when the damage ratio is lower. The system integrity test finds that, with the number of wrong data being larger, when the wrong data block is at 100, 50% of the data blocks of the system integrity are about 1%. With the support of blockchain technology, the integrity of the database of professional English corpus is higher.

3. The Method of Acquiring Spoken English for Special Purposes under the Blockchain Technology

3.1. Definition and Structure of Blockchain

3.1.1. Definition of Blockchain. The essence of blockchain is an anticounterfeiting distributed database, linked from one point to another in the network. Blockchain adopts consensus algorithm to ensure the consistency of data before and after, and usually adopts encryption algorithm to ensure the security of data. Data structures in the blockchain include content records, current block root hashes, previous block root hashes, timestamps, and other pieces of information. At the same time, an end-to-end chain structure is formed in the form of timestamps and hash values, forming a decentralized, transparent, data security, data integrity, and traceable technical system, as shown in Figure 1. Due to different usage scenarios, recorded data types can include asset issuance records, liquidation records, asset transaction records, smart contract records, and even Internet of Things records. The blockchain itself is a scientific and technological means composed of a variety of disciplines. Various disciplines are combined through cryptographic algorithms to form a decentralized distributed data storage structure. These disciplines include computer science, cryptography, mathematics, and finance. Combined with the characteristics of time stamps, the data storage structure has contextual correlation and continuity to establish a data integrity and credible system to ensure data integrity and reliability. For users to trust the blockchain system, the rules for storing, saving, and updating data are formulated accordingly. This system is called an honest distributed storage system. Because of these characteristics of this system, more and more institutions use the blockchain system to promote business activities [8].

3.1.2. Classification of Blockchain

(1) Public blockchain: it has the transparency of information and is a relatively convenient blockchain. Users can access and use without registration and authorization, can freely enter and exit the nodes of the network, and can also participate in the formation process of consensus on the network at any time, that is, decide which block can be added to the blockchain network. All nodes in the public blockchain can participate in information transmission and transactions, which also leads to problems such as data privacy leakage [9]. The public blockchain ensures that transaction information cannot be tampered with through cryptography, and the consensus mechanism provides users with a trusted decentralized operation mode. Consensus mechanisms in public blockchains are typically proof of work (PoW) or proof of stake (PoS). Users choose which consensus mechanism depending on how influential their consensus is. Public blockchains are also often referred to as permissionless chains. There are two mature and successful applications of public blockchains, Bitcoin and Ethereum. Public blockchain is generally applicable to B2C, C2C, or C2B and mass-oriented e-commerce applications such as digital currency and Internet finance.

(2) Community blockchain: the control group forms an alliance, also called the alliance chain. The nodes of the blockchain are preselected so that nodes and nodes can directly maintain a good network connection. Furthermore, data on the blockchain can be public or internally confidential, which can be called "partially decentralized" because it is partially distributed in a sense. The consortium chain needs to control the consensus process and preselected nodes signed by a certain number of members to determine the validity of the new block. Unlike the public blockchain, the consortium chain has some private components, but it also maintains a good degree of decentralization [10]. For example, there is an alliance chain of several financial institutions, each of which will allow one node, and the block must be confirmed by at least 10 of them for it to be effective. The federation chain only allows consensus verification by the validation participants or allows each institution to participate or form a hybrid route, such as exposing the block API and root hash value and allowing other networks to query the blockchain data and block state information. To a certain extent, this can solve the problem of data protection in public chains. Information about the United supermarket chain may be public, or it may only be visible to union members. The alliance chain is suitable for business activities and scenarios that require a high degree of confidentiality. In order to protect the privacy of transactions, all parties in the blockchain have established trust.

(3) Private blockchain: it is aimed at a unique account or a specific institution itself. Data read access has a limited scope, and participants have the right to choose whether to open the permissions. It is also possible to hold a completely private blockchain writing right according to different usage scenarios, and it is also possible to carry out certain restrictions at the same time [11]. Private blockchains by their nature are internally public, so there is no 51% attack by partially verified nodes. A private blockchain can change some of the rules because the owner of the private blockchain can easily make changes to information and data if necessary. However, in many cases, private blockchains do not have public readability, which protects some data that cannot be disclosed. Therefore, the use efficiency of the private blockchain is also greatly reduced, or the information cannot be changed or it is difficult to change. The advantage of the private chain is that the transaction is verified by only a few trusted nodes, and the block generation is faster. Because the verification is carried out by trusted

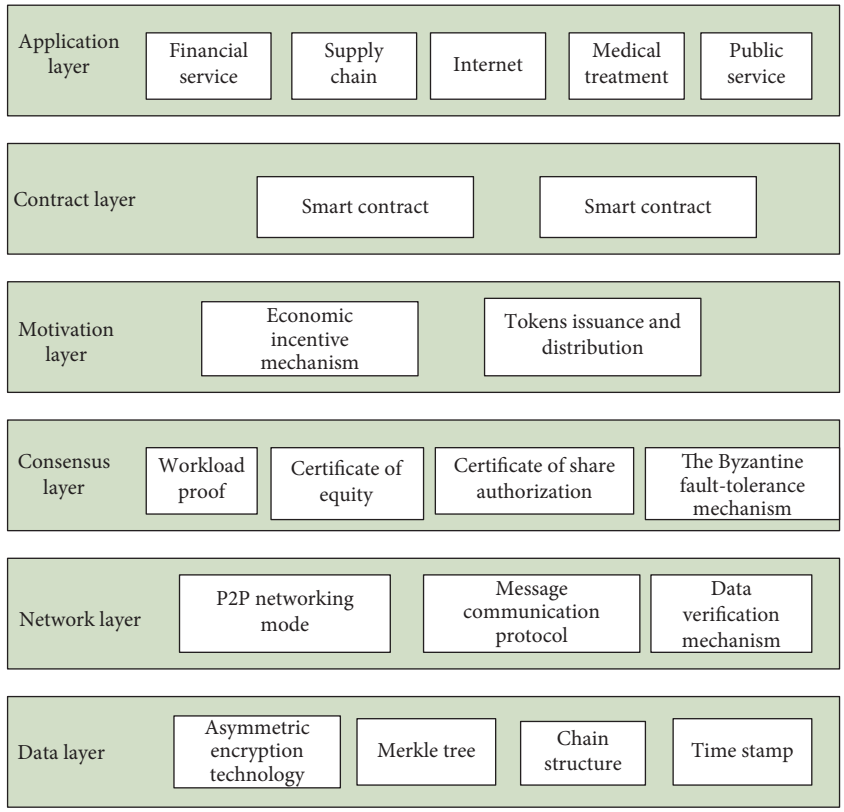

Figure 1: Blockchain technology architecture.

nodes, there is no risk of collusion attack among common associates. In a private chain, nodes can be well connected to each other for centralized management and content audit. In addition, another important feature of private blockchains is the low cost. Private blockchains have many advantages over public blockchains. They are better connected, can be quickly remedied by human intervention in the event of a failure, and can better protect users' privacy while maintaining transaction efficiency.

3.1.3. The Workflow of the Blockchain. Figure 2 is a schematic flowchart of the blockchain, and the specific steps are as follows:

(1) A node wants to initiate a new data record, and the node needs to broadcast this data record to all nodes in the entire network through the P2P network.

(2) Other nodes receive the data and store the received data record in the block.

(3) The node that generates the block broadcasts its block to all nodes in the entire network.

(4) Other nodes verify the broadcasted block. If the block is successfully verified by other nodes, the consensus of the entire network is reached. The block will be added to the main chain and go back to step 1 to wait for a new message to be broadcast.

3.2. English for Specific Purposes (ESP)

(1) Definition: English for specific purposes (ESP) is a diverse teaching philosophy that appears in different forms. ESP is just a branch of LSP, which emerged in the United States in the 1960s.

(2) English for special purposes curriculum

There are many theories about the curriculum setting of English for special purposes. It can be said that there are as many curriculum developers as there are curriculum setting methods. One of the academic courses for English for special purposes is based on spoken language, as shown in Figure 3. The second is a skill-centered curriculum model, as shown in Figure 4, and the last is a learning-centered model.

Combined with the language center and skill center curriculum models, some experts put forward a new view on the acquisition path of oral English for special purposes. As shown in Figure 5, it is a learning-centered curriculum model, which believes that students' curriculum setting for professional purposes needs to be centered on students' needs and formulate learning goals. They are concerned about whether the way students acquire knowledge is effective, whether teachers' teaching methods can arouse students' interest, whether the content, language difficulty, and system of teaching materials meet students' learning standards, and whether the use of oral knowledge corpus has exerted subjective

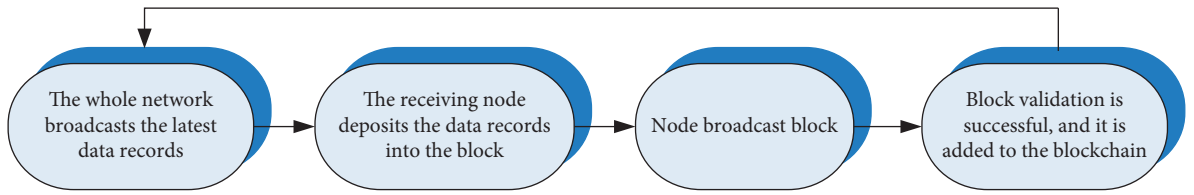

Figure 2: The workflow of the blockchain.

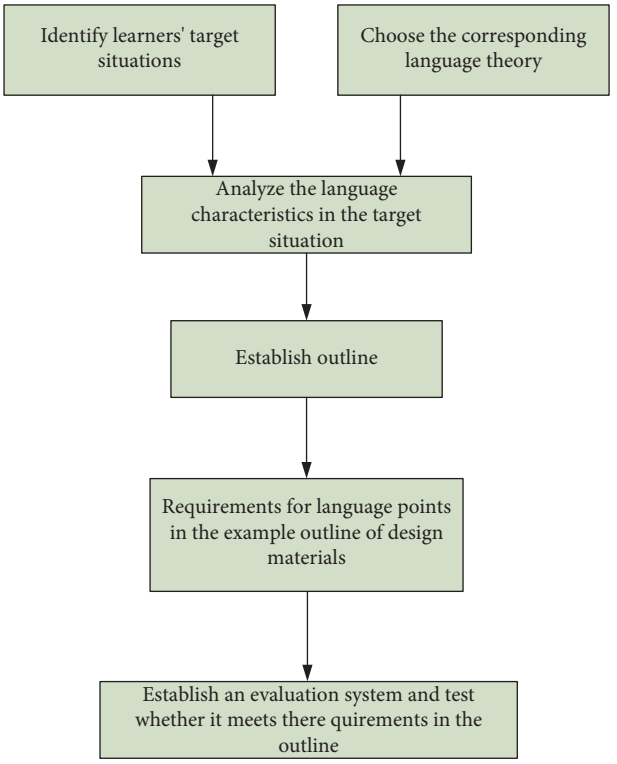

Figure 3: Curriculum centered on spoken language.

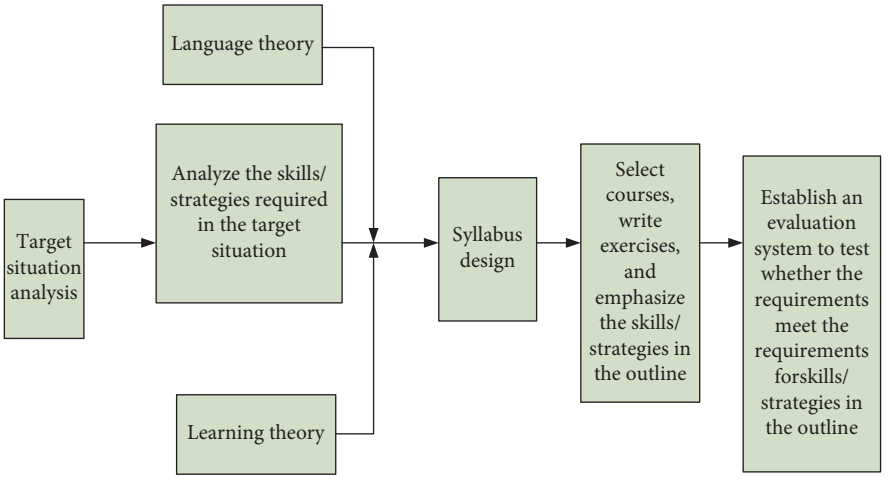

Figure 4: Skills-centric curriculum model.

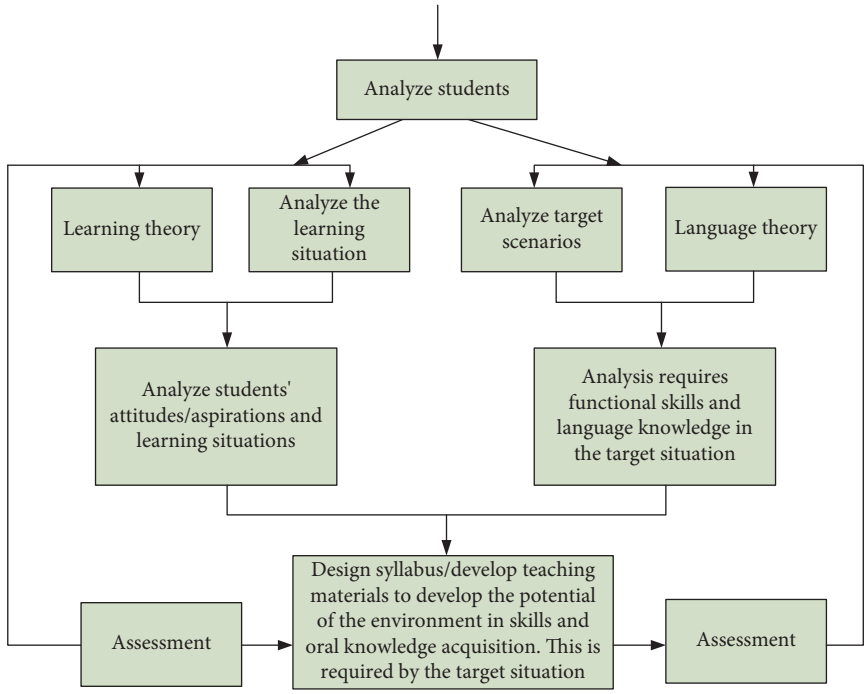

Figure 5: Learning-centered curriculum.

initiative. All influencing factors should be integrated into the process of curriculum design to ensure the maximum effect of the model [12].

(3) Existing problems

The content of ESP teaching materials is outdated and lacks a system, and the language difficulty is high. The teaching methods are outdated and rigid, and the training and development of listening and speaking skills are neglected. The evaluation method is mainly testing, lack of national unified and effective evaluation standards, lack of practical training inspections, and inspections of language application ability in actual situations. The positioning and management of ESP are chaotic. Many colleges and universities deviate from the regulations and make ESP an elective course, and the class hours are far from up to the standard. ESP teachers are short of experience and training opportunities, have a weak willingness to teach, and often teach some experience and general knowledge. The needs analysis is centered on teachers and lacks the analysis of students and society.

3.3. ESP Management System Requirements. According to the analysis, the system summarizes the functions into four functional modules, namely, the user identity establishment function, the user data proxy storage function, the user data access function, and the blockchain management function. The system also designs subfunctions, as shown in Figure 6.

3.3.1. User Identity Establishment Function. The main function of this module is to establish identities for users in the system, and it is necessary to establish a unique identity address so that identities can be differentiated among users. And in order to protect the user's privacy, the user's identity address information cannot relate to the real identity [13]. Secondly, the user identity establishment function needs to realize how the user proves that his identity is real and detects whether the identity of others is real to prevent impostor users.

3.3.2. User Data Proxy Storage Function. The proxy storage function of user data needs to meet the needs of users to securely store data without the need for complex operations. When storing data, the system needs to protect the patient's privacy, and the user's data will not be illegally spread or used without the user's knowledge [14].

3.3.3. User Data Access Function. A huge function of this system is to provide a platform for the sharing of medical data, so it will be a great demand for medical data to be accessed by third parties such as institutions and research institutes [15]. In order to facilitate the safe and convenient access of users' data by third parties, the storage organization needs to confirm the identity of the visitor and the purpose of the visitor's access to the data before accessing and then send the data to the data visitor under the premise of meeting the user's wishes.

3.3.4. Blockchain Management Function. When the system processes data operations, whether it is the data storage record of the storage party or the access record of the visitor to the data, these records are very important to the user. Therefore, how to record effectively and ensure that the record will not be maliciously changed is a big requirement of this system [16]. In addition, in order to support users to query their own historical operation records of data effectively and quickly, the records need to be sorted by time. The

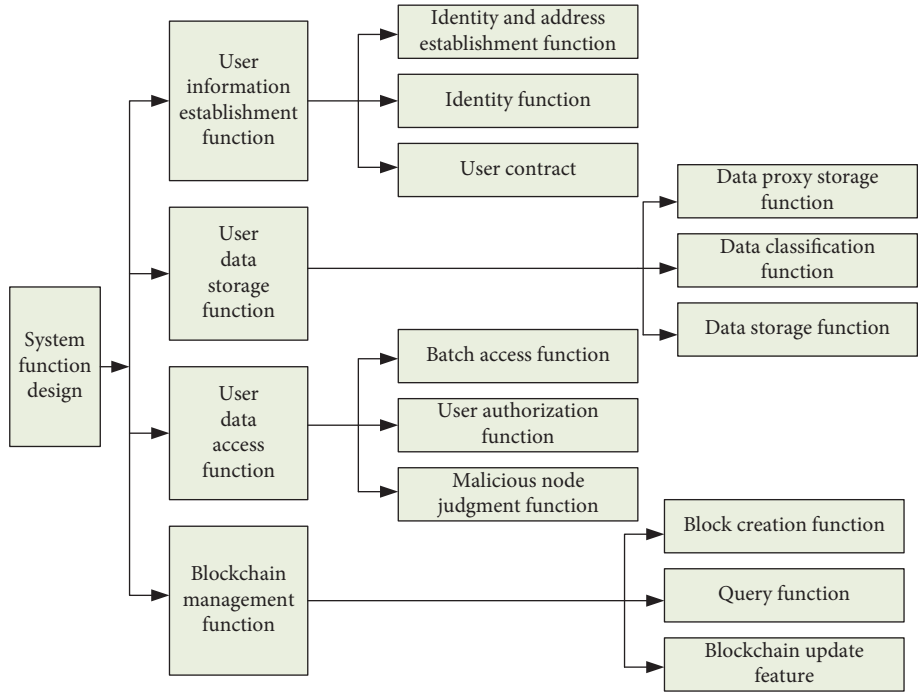

Figure 6: Functional design diagram of the spoken English system for special purposes.

system will use the immutability, traceability, and other characteristics of the blockchain as well as time stamps to manage the records of the entire system.

3.4. Blockchain ESP Management System Database. The characteristics of multitenancy are used to form a blockchain network, and the characteristics of the blockchain are used to prevent user data from being illegally tampered with. This section uses elliptic bilinear mapping to design the integrity verification scheme. When the user is concerned about whether the data is completely stored in the corpus, the integrity verification scheme is used to challenge the verification of the CSP [17].

By deploying distributed virtual machine agents in the cloud, the multitenant in the cloud is used to form a blockchain network, and the algorithm process of data integrity is carried out by designing a cloud-oriented data integrity verification scheme BPDP.

How to judge whether the data in the corpus has been tampered with or destroyed, this only needs to send challenge information to the server. According to the data information returned by the system, it can be judged whether the information inside the system has been tampered with or destroyed to judge the integrity of the professional corpus. By executing the mobile agent task on the storage node, the corresponding data block is obtained and returned to the VMA node to calculate the total data block. The calculation formula is as follows:

$$W = \sum_{j=1}^{n} \sum_{i \in I\ DX} d\left(w_{ij}\right). \tag{1}$$

According to the stored in the VMA node, the total data block label value is calculated as follows:

$$F = \prod_{j=1}^{n} f_j^{d(W)}. \tag{2}$$

In the process of outputting the result, VMA reads the tag value of the challenge data block from its own database to calculate R and at the same time calculates the hash value E of the corresponding challenge block number and obtains the formula:

$$R = \prod_{i \in IDX} \partial_i^{k_i}, E = \prod_{i \in IDX} D\left(g_i \| r_i\right)^{k_i}. \tag{3}$$

Generate evidence proof = $\{F, E, R\}$, and perform the calculation based on the generated evidence:

$$\lambda(E, u) \cdot \lambda(F, u) = \lambda\left(R, l_2\right). \tag{4}$$

If the formula holds, the proof file is complete.

The user will receive the verification result sent by the VMA, and at the same time, according to the obtained file MHT root hash value, the two match at the same time; that is, the verification result is credible.

The formula for calculating the nontampering possibility data block is follows:

$$\begin{aligned} U &= 1 - \frac{x-t}{x} \cdot \frac{x-1-t}{x-1} \cdot \ldots \cdot \frac{x-n \cdot x-t}{x-n \cdot x} \geq 1 - \left(\frac{x-t}{x}\right)^{n \cdot x} \\ &= 1 - \left(1-u_b\right)^{n \cdot x}. \end{aligned} \tag{5}$$

The system integrity verification stage is shown in Figure 7. The user randomly selects a data block and challenges

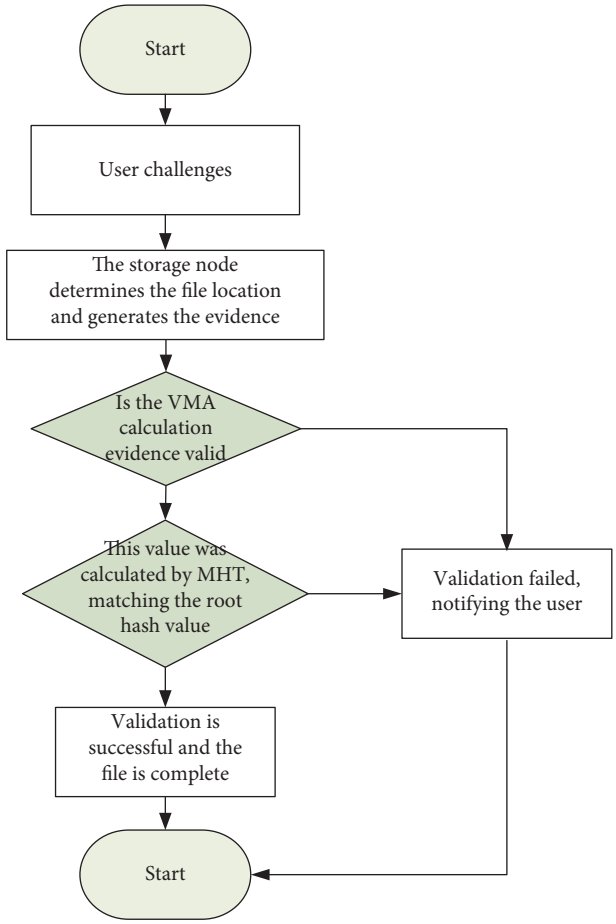

Figure 7: Database integrity verification flow.

the storage node of the CSP through the VMA node. According to the IPFS cluster challenge block, the file position can be obtained, and the evidence is generated and returned to the VMA. VMA calculates whether the evidence is valid through the verification formula. If it is valid, the second step of verification is performed, and the MHT is used to calculate whether the challenge block exists and whether it is consistent with the root hash value. If it is consistent, the proof file is complete; otherwise, the file is destroyed.

3.5. Hash Function Algorithm. The hash algorithm also is the hash function. The function of the hash algorithm is to map arbitrary length of data to shorter and fixed length of data. The mapped data is the hash value. The two characteristics of hash functions are noncollision and irreversibility. Noncollision means that it is impossible to find two identical pieces of data, such that the two pieces of data have the same hash value. Irreversibility means that it is very easy to obtain the hash result from the original data, but it is difficult to obtain the original data from the hash result [18]. Hash in cryptography is a one-way cryptosystem from plaintext to ciphertext. There is no decryption, only encryption, and it is irreversible. The ciphertext corresponding to a little difference in the plaintext will be different.

User access to the database is also very clever for the design of user access. When the visitor needs to enter this special purpose block, the system data agent will verify the visiting user. The hash value of the user generated based on the user's id address is as follows:

$$W = \text{hash}\left(\text{address} \| m \| n \| k_G \| l_G \| k \| l\right), \tag{6}$$

where address represents the user's address, m and n represent the parameters in the ellipse, and new information is generated by combining the message to be signed with the user's hash value:

$$\overline{R} = W \| R_s. \tag{7}$$

The new information generated is processed, and f is contained in $[1, n-1]$:

$$\overline{K} = \text{hash}\left(\overline{R}\right). \tag{8}$$

According to the random number, the curve points of the ellipse are calculated, which can be obtained:

$$\left(m_1, n_1\right) = [f] \cdot G. \tag{9}$$

When the value of m_1 is an integer, the value of h can be calculated:

$$h = \left(k + m_1\right) \bmod n. \tag{10}$$

If the calculation result is $h = 0$, then the generated b value needs to be recalculated. If not, the calculated value of the private key is as follows:

$$p = (1 + k)^{-1} \cdot (r - h \cdot k) \bmod n. \tag{11}$$

If the value of p is 0, the value of b needs to be recalculated to generate the final message and signature.

When verifying the signature, the user data is detected, and new information is generated based on the information received by the system:

$$\overline{R} = W \| R_a. \tag{12}$$

The hash value is recalculated:

$$\overline{R} = \text{hash}\left(\overline{E}\right). \tag{13}$$

When the data of h and p are converted to integers, their values are calculated and obtained:

$$x = \left(h' + p'\right) \bmod n. \tag{14}$$

When the verification fails, the value of the curve point of the ellipse is recalculated:

$$\left(m_1', n_1'\right) = \left[p'\right] \cdot G + \left[x'\right] \cdot Q. \tag{15}$$

After generating the new data from the data of m_1', its value is converted to an integer, and it can be gotten:

$$B = \left(d' + m_1'\right) \bmod n. \tag{16}$$

The last $B = h'$ is checked to see if it can be established. If it is established, the verification is passed; otherwise, the verification is not passed.

3.6. Blockchain Consensus Protocol. Blockchain is a decentralized mechanism for maintaining system ledger and consistency according to nodes. Blockchain is a distributed and decentralized system derived from Bitcoin, which stores the internal content of the system in a distributed manner and is not controlled by the central system. Consistent content exists on each node, which is the consensus mechanism of the blockchain [19]. At present, the consensus mechanism of blockchain mainly includes 4 types: PoW, PoS, DPoS, and distributed consistency algorithm.

PoW (proof of work) is equivalent to the mining principle of Bitcoin. The miner packs a new block without the network accounting and then keeps calculating to find a random number that conforms to the rules of hash cryptography. The purpose is to find a new block that can contain such a rule of random numbers [20]. After such a random number is found, the new block of the blockchain is confirmed, and the miner thus obtains the accounting right of this round of hash calculation competition. After the miner finds such a random number and broadcasts it, the nearby nodes verify the random number. If the verification is successful, the new block will be added to the old block, which is the consensus of the whole network [21].

Today Bitcoin utilizes a proof-of-work mechanism to achieve distributed consistency. However, it will consume a lot of resources, resulting in a waste of computing resources, and there are mining pools that concentrate computing power together on a large scale, which violates the essence of decentralization. One of the biggest problems is that it takes a lot of time for PoW to reach consensus, and it can only process up to 7 transactions per second, which is not suitable for large-scale commercial applications. On the premise of trust verification, nodes can enter and exit the network freely, avoiding the cost of maintaining the centralized credit intermediary and realizing complete decentralization. If the computing power of the whole network does not exceed 50%, the data on the blockchain is safe and can be distributed uniformly.

PoS (proof of stake) is to require a node to have a certain amount of digital currency to prove that it has computing power for distributed consistency confirmation to achieve a consensus mechanism for all nodes [22]. Proof of stake has a serious disadvantage; that is, if a node owns a large amount of digital currency, it is very likely to launch an attack on the entire network. This is a system instability caused by a large gap between the rich and the poor, which is unfair and will lead to the centralization of power [23]. Therefore, on the basis of proof of stake, certain restrictions need to be added to ensure the fairness of the entire network verification. PoS can greatly reduce the time it takes to reach a distributed consensus and reduce the waste of computing resources caused by the PoW consensus mechanism. Network saboteurs can launch an attack on the entire network at a low cost, and the security of the network will have to be verified. The network nodes with more coins will have more billing power, which will destroy the fairness and security of the network and make the gap between the rich and the poor bigger and bigger.

The distributed consensus algorithm is a traditional blockchain algorithm, the most prominent of which is the Byzantine fault-tolerant algorithm. It is very common in systems with a small number of nodes, and a little failure of a node will not affect the Byzantine fault-tolerant algorithm. There is also a distributed consensus algorithm to solve the non-Byzantine problem in the system to ensure the consistency of the data results in the system. This algorithm often appears in the alliance chain to solve some problems in the consensus mechanism. Based on ensuring consistency, a second-level fast consensus mechanism is realized. However, the distributed consistency algorithm does not have a certain decentralized distributed structure and lacks the consensus mechanism of the public chain, so it is more suitable for the multi-centralized business model in which many parties participate.

3.7. Smart Contract Management. The smart contract blockchain ledger database is divided for the acquisition path of spoken English for special purposes, and the key management is strengthened. The function of the key management module is to realize key generation, group key update, key file storage, key file reading, the signing, revocation, and deletion of keys by invoking smart contract, and so on. The state data of the English for special purpose corpus is changed. The state data includes personal data information, user information, student demand information public key, and group key information. In the blockchain, the code chain is designed for the data structure in the system [24].

The personal public key information stored in the blockchain includes public key ID, public key owner ID, public key content, public key issuer ID, issuer's digital signature on the public key, public key creation time, public key revocation time, and the identification of whether the public key is revoked. Table 1 shows the key data structure.

By calling the smart contract on various parameters in the system, the operation of entering, modifying, reading, revoking, and deleting the user's public key is realized. Whether there is a corresponding chain value in the code chain will affect the change of the state data of the English corpus.

4. Experiment on the Acquisition Path of Spoken English for Special Purposes under the Blockchain Technology

4.1. Experiment of Database Integrity of ESP Management System under Blockchain Technology. This section tests the performance of the system according to the functional design of spoken English for special purposes system and the problems existing in the acquisition path of spoken English for special purposes. By building a blockchain network and dividing the placement and management of ESP, the system realizes the functions of system login, ESP management, key management, and user management in the ESP management system.

Table 1: Key data structure.

Variable	Type	Describe
Depth	int	The depth of the extension key
Parent	int	Summary of the extension key parent key
Sequence	int	The sequence used to generate the extension key
Chaincode	byte	The MAC key used to generate the subkey
Masterkey	Key	Key information in the extension key

This paper analyzes the accuracy of the integrity verification protocol of the ESP management system, assuming that there are n data blocks in the professional vocabulary corpus in the ESP management system and nontampered data can be obtained. Then there are damaged data blocks, the proportion of challenge data blocks to total data in the data blocks, and the database integrity of the ESP management system which is determined according to the ratio of nontampered data blocks to damaged data blocks.

Figure 8 shows the data integrity in the professional vocabulary corpus when the number of error data blocks in the system is 10 and 100. When the number of error data blocks is 10, the total number of damaged data blocks and verification accuracy data blocks should reach 99% accuracy, and then the proportion should be about 4%. Therefore, the integrity of the system is higher when the damage ratio is lower. When the number of incorrect data found in the system integrity test is greater, the integrity of 50% of the data blocks of the system is around 1%. With the support of blockchain technology, the integrity of the database of professional English corpus is higher.

In order to verify the integrity of the professional vocabulary corpus established in this paper, the hash value data in the corpus is saved to the blockchain by constructing the MHT structure. Finally, the results of the hash sampling data are used to complete the secondary verification of the system integrity to ensure the security integrity of the system database. After verification, the database is completer and more systematic, which can improve the efficiency of students' systematic learning of spoken English for special purposes. The establishment of professional vocabulary corpus can also meet the learning needs of students to learn professional English, realize self-learning awareness, and become an effective tool for students to learn professional English.

To check whether the professional vocabulary corpus is complete, the time cost analysis of the corpus can also be performed, as shown in Figure 9, which is a comparison chart of the time cost of preprocessing and generating evidence.

It can be seen from Figure 9 that when the blocks are too small, the number of blocks increases sharply, and the preprocessing time is long. When the block size is large, the number of data segments increases sharply when the data block is divided into data segments, which leads to an increase in the time for generating evidence. Setting the file to 1 GB and, with proper block size, a series of integrity verification will be completed in 12 s.

4.2. ESP Management System Key Performance Test. The key of the ESP management system is designed to be updated, and the system performance is determined by calculating the

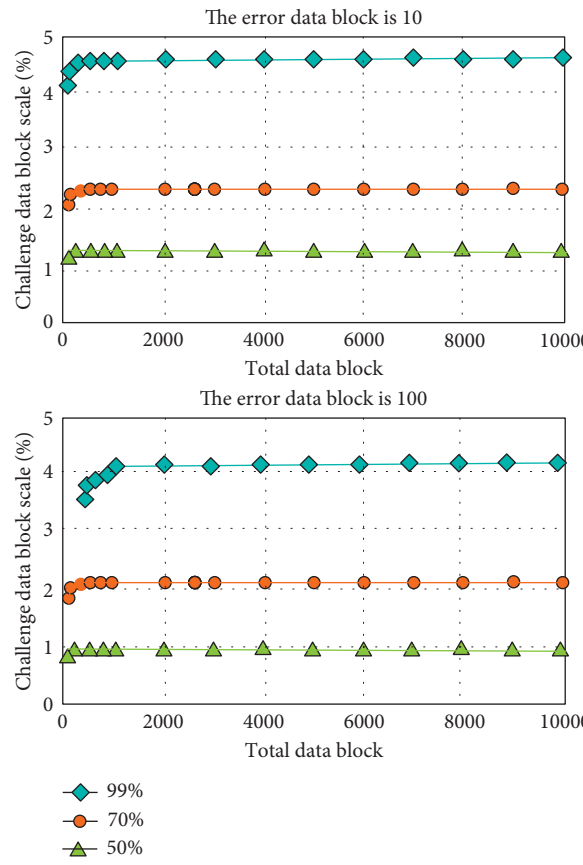

Figure 8: Challenge data block scale diagram.

number of keys and the time used. The generated test code is as follows. The time taken to generate 5, 10, 20, 50, 100, 200, and 500 subkeys in succession was tested.

The key generation test results are shown in Table 2. When the number of subkey generation times is less than 50, the key generation time can be within 100 ms, which has a faster generation speed. The length of the group key update parameter is the maximum number of computations required to obtain the latest group key. Therefore, the group key update scheme can be optimized as follows:

(1) When the length of the group key update parameter is large, the group key is saved locally every 50 versions.

(2) The latest group key is also stored locally and is updated every time when logging in.

The optimized group key management scheme updates the parameter length of the group key of length L and

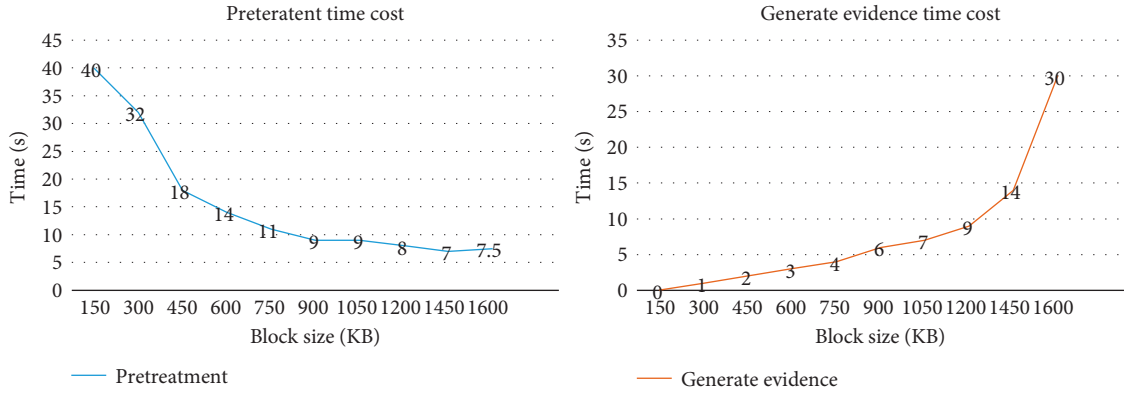

Figure 9: Comparison of preprocessing and proof generation time overhead.

Table 2: Key generation test results.

Number of subkey generation times	Time spent (ms)
5	14
10	25
20	32
50	72
100	157
200	415
500	1092

Table 3: Social network security comparison.

Name	Consensus algorithm	Blockchain mode	Safety proportion	Token transmission efficiency
Ryu	PoT	Self-built private chain	7	37
Synereo	DPoS	Self-built private chain	6	60
Steemit	DPoS	Self-built private chain	5	53
Yours	PoW	Public chain	4	41
ONO	PoS	Self-built private chain	8	78
RRCoin	PoS	Self-built private chain	9	28

calculates the maximum key storage overhead, and the calculation amount of each historical group key is less than 100 ms.

4.3. Consensus Algorithm Comparison Experiment of ESP System. The number of users in the English for special purpose corpus is fed into the security scheduling algorithm and filtered, all nodes are traversed, and the result is a measurable degree of security.

The next part is the coin attribute proportions of the security of the six special purpose English corpora. The security proportions range from 0 to 9 from small to large, and the token transmission efficiency from small to large ranges from 10 to 99. The comparison chart after the experiment is described as follows.

As can be seen from Table 3, PoS has the best transmission efficiency, reaching 78%, and the security coin attribute is 8. Compared with the security performance in other public chains, the transmission effect and security of PoS have achieved excellent results. The security and transmission effect of the only private chain in the test did not play a good role. It proved that, in the blockchain, the proof of stake can effectively improve the security of the system.

5. Discussion

Through the analysis of blockchain and English for special purposes, this paper established a corpus of English for special purposes in view of the existing problems of English for special purposes. The hash function was used to verify the rigor of the system key, and the comparison experiment of the ESP system consensus algorithm was carried out, which proved that, in the blockchain, the proof of rights could effectively improve the security of the system. The smart contract blockchain ledger database was divided for the acquisition path of spoken English for special purposes, and the key management was strengthened. In all respects, blockchain is beneficial to the learning and development of spoken English for special purposes.

6. Conclusions

This paper focused on the consensus algorithm, hash function algorithm, and smart contract. Through the analysis of English for special purposes, the ESP management system and spoken English for special purpose corpus were established, and the integrity of the corpus data was analyzed. The paper firstly talked about the concept and basic structure of the blockchain so that people had a preliminary understanding of the blockchain. The definition and course modules of English for specific purposes (ESP) were described, and then combined with the algorithm of the blockchain, a corpus of spoken English for special purposes (ESP) was constructed. The paper used the knowledge of blockchain to discuss the integrity of the corpus data and found that the integrity of the system is higher when the database damage ratio is relatively low. Although the paper proposes some blockchain algorithms that are beneficial to the acquisition path of spoken English for specific purposes, the practical operation remains to be considered.

Data Availability

Data sharing is not applicable to this paper as no new data were created or analyzed in this study.

Conflicts of Interest

The author states that this paper has no conflicts of interest.

Acknowledgments

This work was supported by the General Special Scientific Research Projects of Education Department of Shaanxi Province (no. 21JK0275).

References

[1] M. H. Miraz and M. Ali, "Applications of blockchain technology beyond cryptocurrency," *Annals of Emerging Technologies in Computing*, vol. 2, no. 1, pp. 1–6, 2018.

[2] P. Yeoh, "Regulatory issues in blockchain technology," *Journal of Financial Regulation and Compliance*, vol. 25, no. 2, pp. 196–208, 2017.

[3] M. O'Dair and Z. Beaven, "The networked record industry: how blockchain technology could transform the record industry," *Strategic Change*, vol. 26, no. 5, pp. 471–480, 2017.

[4] I. Eyal, "Blockchain technology: transforming libertarian cryptocurrency dreams to finance and banking realities," *Computer*, vol. 50, no. 9, pp. 38–49, 2017.

[5] P. Otto, "Choosing specialized vocabulary to teach with data-driven learning: an example from civil engineering," *English for Specific Purposes*, vol. 61, no. 5, pp. 32–46, 2021.

[6] T. Gráf, "Repeats in advanced spoken English of learners with Czech as L1," *AUC PHILOLOGICA*, vol. 2017, no. 3, pp. 65–78, 2017.

[7] X. Y. Chai and G. Subramaniam, "The use of communication strategies in mobile asynchronous chat," *International Journal of Computer-Assisted Language Learning and Teaching*, vol. 11, no. 2, pp. 33–50, 2021.

[8] R. Beck, M. Avital, M. Rossi, and J. B. Thatcher, "Blockchain technology in business and information systems research," *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 381–384, 2017.

[9] Y. Yuan, T. Zhou, and A. Y. Zhou, "Blockchain technology: from data intelligence to knowledge automation," *Zidonghua Xuebao/Acta Automatica Sinica*, vol. 43, no. 9, pp. 1485–1490, 2017.

[10] S. Mansfield-Devine, "Beyond Bitcoin: using blockchain technology to provide assurance in the commercial world," *Computer Fraud & Security*, vol. 2017, no. 5, pp. 14–18, 2017.

[11] A. Prashanth Joshi, M. Han, and Y. Wang, "A survey on security and privacy issues of blockchain technology," *Mathematical Foundations of Computing*, vol. 1, no. 2, pp. 121–147, 2018.

[12] S. Shackelford, "J. Block-by-Block: leveraging the power of blockchain technology to build trust and promote cyber peace," *Yale Journal of Law and Technology*, vol. 19, no. 1, p. 7, 2018.

[13] S. Nakamura, H. Reinders, and P. Darasawang, "A classroom-based study on the antecedents of epistemic curiosity in L2 learning," *Journal of Psycholinguistic Research*, vol. 51, no. 2, pp. 293–308, 2022.

[14] H. Liang, "An empirical study on the effects of computer-corpus-based formulaic sequences on college students' oral English learning," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 12, no. 08, pp. 67–76, 2017.

[15] M. A. Zarco-Tejada, "L2 English learning books under analysis: a computational study of conjunctions in oral English," *Journal of Research Design and Statistics in Linguistics and Communication Science*, vol. 4, no. 1, pp. 50–72, 2017.

[16] P. Eze, T. Eziokwu, and C. Okpara, "A triplicate smart contract model using blockchain technology," *Circulation in Computer Science*, vol. 2017, no. 01, pp. 1–10, 2017.

[17] M. R. Biktimirov, A. V. Domashev, P. A. Cherkashin, and A. Y. Shcherbakov, "Blockchain technology: universal structure and requirements," *Automatic Documentation and Mathematical Linguistics*, vol. 51, no. 6, pp. 235–238, 2017.

[18] S. P. Stawicki, M. Firstenberg, and T. J. Papadimos, "What's new in academic medicine? Blockchain technology in healthcare: bigger, better, fairer, faster, and leaner," *International Journal of Academic Medicine*, vol. 4, no. 1, pp. 1–11, 2018.

[19] D. Xing and B. Bolden, "Exploring oral English learning motivation in Chinese international students with low oral English proficiency," *Journal of International Students*, vol. 9, no. 3, pp. 834–855, 2019.

[20] Q. Meng, "A study on cultivating college students' oral English ability based on computer assisted language learning environment," *Boletin Tecnico/technical Bulletin*, vol. 55, no. 4, pp. 80–85, 2017.

[21] X. Wei, "Simulation of English intelligent system based on CA-IAFSA algorithm and artificial intelligence," *Journal of Intelligent and Fuzzy Systems*, vol. 2, pp. 1–11, 2021.

[22] S. J. Supalla, J. H. Cripps, and A. P. J. Byrne, "Why American sign language gloss must matter," *American Annals of the Deaf*, vol. 161, no. 5, pp. 540–551, 2017.

[23] O. P. Adelana, O. P. Adelana, and O. D. Atolagbe, "Teaching oral English through technology: perceptions of teachers in Nigerian secondary schools," *International Journal of Learning and Teaching*, vol. 14, no. 1, pp. 55–68, 2022.

[24] Z. Meng and N. Li, "Design and application path of online college English learning system based on the B/S structure," *Revista de la Facultad de Ingenieria*, vol. 32, no. 13, pp. 579–584, 2017.