Blockchain-Based Secure and Efficient Secret Image Sharing with Outsourcing Computation in Wireless Networks

Zhili Zhou, *Member, IEEE*, Yao Wan, Qi Cui, Keping Yu, *Member, IEEE*, Shahid Mumtaz, *Senior Member, IEEE*, Ching-Nung Yang, *Senior Member, IEEE*, and Mohsen Guizani, *Fellow, IEEE*

***Abstract*—Secret Image Sharing (SIS) is the technology that shares any given secret image by generating and distributing n shadow images in the way that any subset of k shadow images can restore the secret image. However, in the existing SIS schemes, the shadow images will be easily tampered and corrupted during the communication, which will pose serious security issues. Recently, blockchain has emerged as a promising paradigm in the field of data communication and information security. To securely communicate and effectively protect the secret image data in wireless networks, we propose a Blockchain-based Secure and Efficient Secret Image Sharing (BC-SESIS) scheme with outsourcing computation in wireless networks. In the proposed BC-SESIS scheme, the shadow images are encrypted and stored in the blockchain to prevent them from being tampered and corrupted. The identity authentication-enabled smart contract is deployed to achieve the (k, n) threshold for secret image restoring. Furthermore, to reduce the computational burden of smart contract and users, an efficient outsourcing computation method is designed to outsource the restoring task, which is securely implemented by agent miners in the encryption domain. Theoretical analysis and extensive experiments demonstrate that the BC-SESIS scheme can achieve desirable communication security and high computational efficiency in the wireless networks.**

***Index Terms*—Blockchain, Secret image sharing, Wireless networks, Outsourcing computation.**

I. Introduction

With the rapid development of wireless communication technology, the broadcast nature of wireless medium makes multimedia information in wireless communication very vulnerable to various security threats such as message modification, tampering, and corruption in wireless networks [1]–[3]. Thus, it is necessary to guarantee the security of any given secret image in the wireless networks. To this end, Secret Image Sharing (SIS) is the technology that shares the secret image by generating n shadow images in the way that any subset of k shadow images can restore the secret image [4]–[13]. The (k, n)-SIS scheme was first proposed by Thien and Lin [4], which is based on the theory of polynomial. In this scheme, every k secret pixels are used as k coefficients of a $(k-1)$-degree polynomial $f(x)$. Then, a dealer can produce n shadow pixels by computing $f(x_i)$, where x_i is an integer and $i \in [1, n]$. After repeating the above process until all pixels of the secret image have been processed, n shadow images are generated and then transmitted to n corresponding participants on networks. By Lagrange's interpolation algorithm, any k shadow images can jointly restore the secret image, but $(k-1)$ or fewer shadow images cannot. Therefore, the (k, n)-SIS scheme can be deemed as a threshold-based cryptography scheme.

Although $(k-1)$ or fewer shadows cannot disclose the information of the secret image, it is very likely that these shadows would be tampered or corrupted in the wireless networks, which will cause the original secret image not to be correctly restored. Thus, it is an urgent demand for SIS schemes to prevent the shadow images from being tampered and/or corrupted in the wireless networks [3], [9]–[13].

To alleviate the above issue, some SIS schemes based on image steganography have been proposed [6], [7], [14]–[16]. Generally, each generated shadow image is hidden into a cover image by imperceptibly modifying the cover image before transmitting in networks. As a result, the risk of tampering and corrupting shadow images can be reduced significantly. It is notable that, although the hidden shadow images are hard to detect by human eyes, it is likely that these shadows can be detected by the powerful steganalysis tools [17]–[19].

As a decentralized data structure, blockchain can effectively address a lot of security issues of the traditional centralized data structures, and thus it has been widely employed in a variety of fields, such as finance [20], [21], healthcare [22]–[24], entertainment [25], [26], supply chain [22], [27], and transportation [28]–[30]. It has become one of promising paradigms in the field of data communication and information security, since it cannot only prevent secret data from being tampered and/or corrupted, but also address the issues of

Zhili Zhou and Qi Cui are with Institute of Artificial Intelligence and Blockchain, Guangzhou University, China. (Email: zhou_zhili@163.com, cuiqischolar@163.com).

Yao Wan is with Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing University of Information Science and Technology, Nanjing 210044, China. (Email: wanyao@nuist.edu.cn).

Keping Yu is with the Graduate School of Science and Engineering, Hosei University, Tokyo 184-8584, Japan. and with the RIKEN Center for Advanced Intelligence Project, RIKEN, Tokyo 103-0027, Japan. (Email: keping.yu@ieee.org).

Shahid Mumtaz s with the Department of Applied Informatics, Silesian University of Technology, Akademicka 16 44-100 Gliwice, Poland and Departement of Engineering, Nottingham Trent University, UK (E-mail: Dr.shahid.mumtaz@ieee.org).

Ching-Nung Yang is with Department of Computer Science and Information Engineering, National Dong Hwa University, Hualien City 97401, Taiwan. (E-mail: cnyang@gms.ndhu.edu.tw).

Mohsen Guizani is with the Machine Learning Department, Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), Abu Dhabi, UAE. (E-mail: mguizani@ieee.org).

Corresponding authors: Zhili Zhou and Qi Cui

malicious codes and behaviors [27], [31]–[35].

Motivated by the great potential of blockchain, to securely communicate and effectively protect the secret image data distributed on the networks, we propose a Blockchain-based Secure and Efficient Secret Image Sharing (BC-SESIS) with outsourcing computation in wireless networks. In the proposed BC-SESIS scheme, the shadow images are first generated from a given secret image, and then they are encrypted by Fully Homomorphic Encryption (FHE) algorithm and stored in the blockchain to prevent them from being tampered and corrupted during the wireless communication. In the stage of secret image restoring, the identity authentication-enabled smart contract is designed and deployed to achieve the (k, n) threshold of SIS for secret image restoring. Furthermore, to reduce the computational burden of smart contract and users, an efficient outsourcing computation method is designed to outsource a considerable part of secret image restoring task, which is securely implemented by agent miners in the encryption domain. Theoretical analyses and extensive experiments demonstrate that the BC-SESIS scheme not only shows strong resistance to data tampering and corruption, but also has high computational efficiency. Our contributions are summarized as follows:

1) The novel SIS scheme is proposed based on the blockchain and FHE algorithm. To the best of our knowledge, this is the first work that employs the blockchain and FHE algorithm in the field of SIS. Since the encrypted information stored on blockchain is hard to tamper, the proposed BC-SESIS scheme not only protects the secret image from leaking, but also prevents the shadow images from being tampered with and corrupted during the wireless communication.

2) The proposed scheme supports the automatic identification of participant identity and triggering of restoring task. To facilitate the secret image restoring stage, by the smart contract, the proposed scheme automatically identifies the participants who apply for the restoring process, and outsources the restoring tasks after receiving enough authorizations. Moreover, the Automatic Identity Authentication (AutoIDAuth)-enabled smart contract is designed to realize the (k, n) threshold of SIS.

3) The FHE-based outsourcing computation method is designed to achieve secret image restoring in the encryption domain. In the BC-SESIS scheme, the shadow images are encrypted with the FHE algorithm before before storing on the blockchain. Owing to the property of the FHE algorithm, the FHE-based outsourcing computation method can outsource the polynomial computation in the encryption domain by miners in the blockchain, which can reduce the computation burden for the smart contract and users significantly.

The remainder of this paper is structured as follows. Section II presents the related work. Section III describes the proposed BC-SESIS scheme. Section IV theoretically analyzes the security of the system. Section V presents and analyzes the experimental results. Conclusions are given in Section VI.

II. Related Work

First, we review the typical SIS schemes. Then, as the proposed BC-SESIS scheme is highly related to the blockchain technologies including Inter Planetary File System (IPFS) and smart contract, we also introduce these blockchain technologies.

A. Secret Image Sharing

Naor and Shamir [36] first proposed the secret sharing scheme in 1979. In essence, instead of directly communicating the original secret data on the network, this secret sharing scheme generates a set of random-like data, called as shares or shadows, from given secret data, and then distributes them to the participants to ensure that each participant has one shadow. In this scheme, the secret data elements are hidden into the constant coefficient of a $(k-1)$-degree polynomial $f(x)$. Then, someone can generate n shadows by computing $f(x_i)$, where x_i is a real number and $x_i \in [0, p-1]$, $i \in [1, n]$. After repeating the above process for every k data elements of the secret image, n shadows are generated and then sent to n corresponding participants on networks. By Lagrange's interpolation algorithm, any k shadows can jointly restore the secret image, but no information of secret image can be revealed by $(k-1)$ or fewer shadow images. Therefore, this scheme can be deemed as a (k, n) threshold SIS scheme. Thien and Lin [4] extended Shamir's scheme for image data, and hided every k secret pixels into all the k coefficients of the polynomial. As a result, the sizes of shadows are decreased to $\frac{1}{k}$ of that of the original secret image.

Subsequently, many SIS schemes were proposed in the past decades. They focus on using different hiding methods to improve the efficiency of sharing [37]–[39], studying the degree of dependence on trusted third-party [40], and the flexibility and robustness of restoring images [38], [41].After carefully reviewing these references, the comprehensive comparison between the proposed scheme and the related SIS schemes are demonstrated in Table I. Note that, although all the above SIS schemes can protect the secret image from being obtained by the others without enough shadows, they cannot prevent the shadow images from being tampered and corrupted in communication networks, which will cause the secret image cannot be exactly restored.

To alleviate the above issue, some SIS schemes have been proposed based on image steganography to hide each generated shadow image into a cover image before distribution [6], [7], [14], [15]. Lin *et al.* [6] first combined steganography and SIS technologies to enhance the security of shadow images during the communication. They hided the shadow images into common meaningful cover images imperceptibility. Lin *et al.* [14] proposed a SIS scheme using invertible steganography technology, in which both the cover images and shadow images can be exactly restored. Although these steganography-based SIS schemes can reduce the possibility of shadow images being attacked to some extent, it is very likely that the existence of shadow images hidden in the covers can be exposed by the statistical feature-based steganalysis methods [18], [19], thereby compromising the security of secret communication. Also, some other SIS schemes have proposed based on the integrity verification technology, which can verify the integrity of shadow images to determine whether they have been tampered or not [14], [15].

TABLE I
COMPARISONS BETWEEN THE RELATED SECRET SHARING SCHEMES AND THE PROPOSED SCHEME. (VG: VISUAL CRYPTOGRAPHY, RG: RANDOM GRID, HE: HOMOMORPHIC ENCRYPTION)

	[38]	[39]	[40]	[41]	The proposed method
Security model	N/A	N/A	N/A	Secure	Semi-honest
Pixel expansion	Yes	Minimum	No	No	No
Hiding method	VC	RG	RG	VC	HE
Code book needed	Yes	Yes	No	No	No
Trusted third-part needed	Yes	Yes	No	Yes	Yes
Tamper resistance	No	No	No	No	Yes
Recovery type	Visible	Recognizable	Recognizable	Recognizable	Lossless

In summary, the steganography-based SIS schemes and the integrity verification-based SIS schemes cannot effectively prevent the shadow images from being tampered and corrupted during the wireless communication, which will pose serious security vulnerabilities.

B. Blockchain Technologies

Blockchain: In the literature [27], [31]–[35], [42]–[44], blockchain is usually regarded as a decentralized and distributed data ledger. By using blockchain technology, new information is added to a block and is made available to all the users or nodes in a distributed network. As the maintainers of blockchain, the miners are the network nodes mainly responsible for producing new blocks via the Proof of Work (PoW) mechanism [45]. The PoW mechanism also improves the cost of different malicious attacks and the security level of the blockchain system [46]. Although all the network nodes can observe the data stored on the blockchain, it is very difficult for them to tamper and corrupt the data unless someone breaks 51% network nodes at the same time.

Recently, the blockchain technology has gained increasing attention by integrating its potential benefits into IoT systems [47]–[52]. The researchers explored blockchain technology to improve the security and efficiency of IoT systems. For example, Zuo *et al.* [47]proposed a new cooperative Mobile Edge Computing (MEC) blockchain computation offloading scheme. The cooperative approach can serve for more IoT devices with offloading computations compared with noncooperative schemes. The non-trustworthy MEC verification scheme [49] was proposed for blockchained IoT system, which can allocate computing resources to IoT nodes more reasonably. In [50], the delay-limited mining task based on PoW was formulated as a non-cooperative game, and the Continuous Relaxation and Greedy Rounding (CRGR)-based alternating iterative algorithm was proposed to efficiently achieve optimal delay-limited computation offloading for all users.

The above approaches have demonstrated the security and effectiveness of blockchain techniques in wireless network environment, which inspire us to propose the blockchain-based secure and efficient secret image sharing with outsourcing computation in wireless networks. Compared with the traditional secret sharing schemes without blockchain [41], [53]–[57]], our scheme has the following unique advantages in terms of the security performance. (1) Anti-tampering ability to verify the validity of the data [58]–[60], (2) the transparency of allowing nodes in the network to obtain information [61], [62], and (3) the interactivity of multi-party security cooperation without a third-party organization [63]–[65]. Therefore, this paper proposes a novel secure and efficient SIS scheme based on the blockchain.

IPFS: Motivated by the decentralized characteristic of blockchain, a peer-to-peer distributed file system, *i.e.*, Inter Planetary File System (IPFS), has been proposed [66]–[68]. Different from the traditional distributed file systems that depend on a centralized server for file management and storage, IPFS stores and shares the file data among different network nodes without the need of a central server [68]. The IPFS can offers a high-through storage model by using the Distributed Hash Tables (DHT).

Since the encrypted shadow images files produced by the BC-SESIS scheme usually have large sizes, directly storing these large sized files on the blockchain will cause large storage burden and high latency for the blockchain. Thus, instead of storing these image files directly on the blockchain, in the BC-SESIS scheme, we store the image files in the IPFS, and then sends the hash strings (the file's addresses) returned by the IPFS to the blockchain. If someone is allowed to access an image file, he computes its address at first and then downloads the file from the IPFS according to this address.

Smart Contract: The smart contract has been widely used and studied with the development of blockchain. In 1994, Szabo [69] proposed the concept of "smart contract" and defined a smart contract as a computerized transaction protocol that supports the implementation of the contract's terms. Smart contracts are usually deployed on the blockchain in the form of codes, and they are executed in Ethereum Virtual Machine (EVM) [28], which is a platform of conducting smart contracts on the blockchain. Each smart contract is assigned a unique address on the blockchain, and it can be invoked by being sent transactions. Generally, the smart contract runs on every network node independently and automatically in a predefined manner [28], [70]–[72]. The use of smart contracts can reduce the transaction cost for participants and the occurrence of abnormal and malicious actions on the blockchain. Due to the above advantages of a smart contract, in the proposed BC-SESIS scheme, we design the AutoIDAuth-enabled smart contract to realize the (k, n) threshold of SIS.

III. THE PROPOSED BC-SESIS SCHEME

In this section, we introduce the proposed BC-SESIS scheme in detail. In Section III-A, we introduce the general framework of BC-SESIS scheme. Section III-B describes the

image sharing process. Section III-C elaborates on the image restoring process.

A. The Framework of Proposed BC-SESIS scheme

1) Security model: We considered the semi-honest model throughout the paper. Specifically, any number of participants with fewer than k would conspire with external users in the wireless network to attempt to obtain, tamper or corrupt the image shares of others. Moreover, we assume that attackers cannot compromise the security of the blockchain network. In other words, the attackers do not have the ability to hold most of the computing power and network resources in the blockchain, since most of the nodes in the blockchain network are assumed to be honest and reliable. In addition, we introduce the BFV homomorphic encryption algorithm to ensure the secure outsourcing of secret image restoring. According to the illustration in [72]–[74], this encryption algorithm has superior performances in the efficiency and feasibility, and it is also considered to be secure enough.

2) Roles: To facilitate the introduction of the BC-SESIS scheme, we first list the main roles, which are given as follows.

Dealer: The *Dealer* is the owner of secret image, who takes charge of generating and distributing a set of shadow images and an encryption key to the group of *Participants*.

Participants: In the secret image sharing stage, each *participant* receives one shadow image and the encryption key from the *Dealer*. Then, he encrypts the shadow image by the key, and uploads the encrypted shadow to the blockchain. In the stage of secret image restoring, each *Participant* decides whether to authorize the access of his shadow upon the request of *Applicant*.

Applicant: The *Applicant* is one of the *Participants* who intends to restore the secret image by the designed AutoIDAuth-enabled smart contract.

Agent Miners: The *Agent Miners* are the network nodes on the blockchain. They are responsible for the computation of polynomials in encryption domain for the secret image restoring.

3) Trust setup phase: Assigns a mutual-trust party (the *dealer*), who calculates n secret shares according to the original secret image and distributes them to n *participants* securely, so that any k or more *participants* who share their image shares can easily recover the original secret, but any group that only knows $k-1$ or less shares cannot recover the secret.

4) Framework: Then, we introduce the framework, as shown in 1. It contains the secret image sharing stage and secret image restoring stage. The main notations used in the proposed scheme are listed in TABLE II .

Secret image sharing stage: Given a secret image SI, the *Dealer* first generates n shadow images $\{S_i|1 \le i \le n\}$, and distributes the shadows and the private key of FHE algorithm denoted as (S_i, sk) to n Participants in a secure way. Subsequently, the Participants encrypt their own shadows by the FHE algorithm. Finally, the Participants store the encrypted shadow images S_i' to IPFS, and then upload the address of encrypted file returned from IPFS to the blockchain.

TABLE II
THE NOTATIONS IN THE PROPOSED SCHEME

Notation	Description
k, n	The threshold value of (k, n)-SIS
SI	The original secret image
S_i	The i-th shadow image
sk, pk	The private key and public key of FHE algorithm
S_i'	The i-th encrypted shadow image
$w \times h$	The size of the original secret image
a_i	The i-th coefficient of the polynomial
N	The number of pixels divided into each batch
v_i^j	The j-th vector set segmented from the i-th shadow image
len	The number of vectors in v_i^j
S_i'	The encrypted shadow image
$Ln(x)$	The Lagrange interpolation polynomial
X_i	The encrypted form of the random number x_i
A_{tj}	The encrypted coefficients of polynomial

Secret image restoring stage: First, the *Applicant* sends the request of image restoring with his identity information to the designed AutoIDAuth-enabled smart contract when he intends to restore the secret image. Then, the smart contract verifies the identity, and asks for the authorizations of the access of the *Participants*' shadow images. Once the smart contract collects k authorizations, it outsources a part of secret image restoring task, *i.e.*, the computation of polynomials in encryption domain on the blockchain. Subsequently, some *Agent Miners* compute the polynomials in encryption domain, and then send the coefficients of polynomials to the smart contract. Finally, the smart contract verifies these coefficients and sends them to the *Applicant*, and the *Applicant* computes the secret image by these coefficients.

In the following, we elaborate on the two stages of the framework of proposed BC-SESIS scheme.

B. Secret Image Sharing Stage

The stage of a secret image sharing consists of three main steps: shadow image generation, shadow image encryption, and shadow image uploading. Each step is detailed as follows.

Step (1) Shadow image generation: To generate the shadow images from a given secret image SI with the size of $w \times h$, like the existing polynomial-based SIS schemes, we also adopt the polynomial $(k-1)$-degree polynomial, which is defined as follows.

Definition 1. Given two positive integers k and n, where $2 \le k \le n$, and we get a $(k-1)$-degree polynomial as follows:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots\cdots + a_{k-1} x^{k-1} \cdot \mathrm{mod} \cdot p \quad (1)$$

Where, $(a_1, a_2, ..., a_{k-1})$ are the coefficients of the polynomial and p is a prime number.

By using the values of every k secret pixels as the k coefficients of the polynomial, the *Dealer* inputs a set of n random numbers, *i.e.*, $(x_1, x_2, \ldots, x_n)$, no more than p into the $(k-1)$-degree polynomial to compute the corresponding n shadow pixels $\{f(x_i)|1 \le i \le n\}$ by

$$f(x_i) = a_0 + a_1 x_i + a_2 x_i^2 + \cdots\cdots + a_{k-1} x_i^{k-1} \cdot \mathrm{mod} \cdot p \quad (2)$$

Then, the *Dealer* repeats the above process until all the pixels of the secret image have been traversed. Consequently,

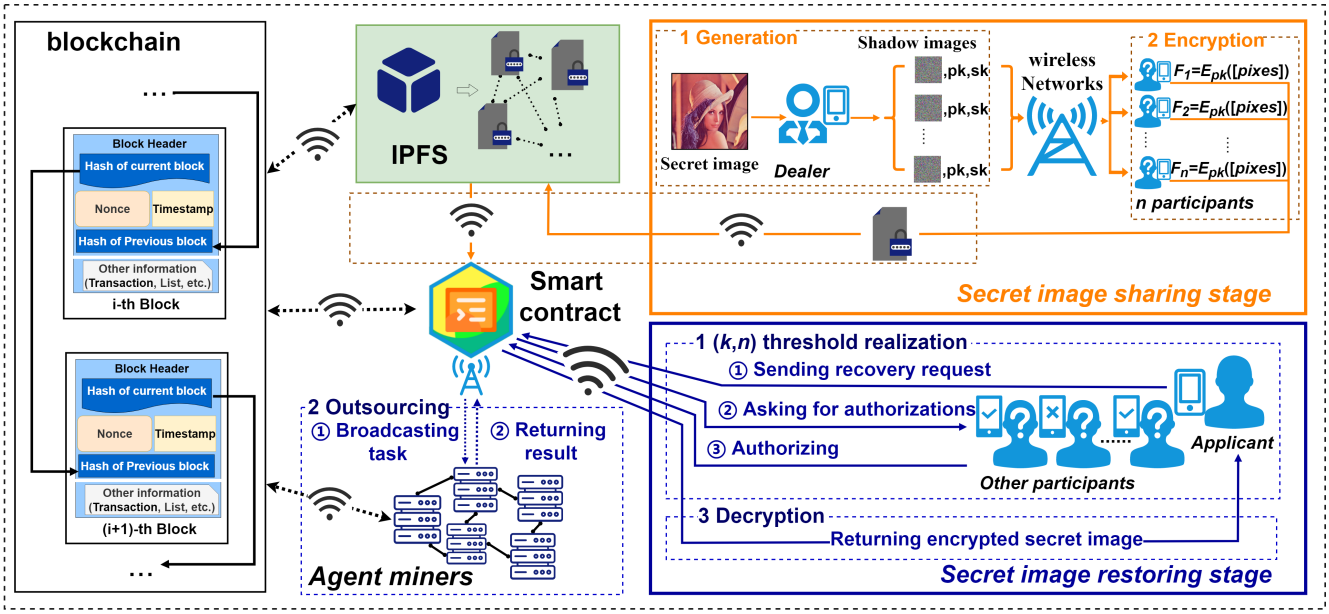

Fig. 1. The framework of proposed BC-SESIS scheme

n shadow images are obtained, and the sizes of shadow images are $\frac{1}{k}$ of that of the original secret one. Note that all the n random numbers $\{x_i | 1 \leq i \leq n\}$ are publicly available.

In the existing polynomial-based SIS schemes, the prime number p is usually set as 251. Thus, for each pixel within the range of $[251, 255]$ in the secret image, it should be truncated to 250 or be expended to two pixels before sharing. Consequently, the secret image will be distorted or be expended significantly. To avoid the above issues, like Yang *et al.* SIS scheme [13], we set the prime number p as 257 to generate the shadow images. If a very few pixels of generated shadow images exceed 255, we only slightly modify these pixels of original secret image to ensure that all pixels of generated shadows are within the range of $[0, 255]$.

Step (2) Shadow image encryption: To enable the outsourcing computation of secret image restoring, we adopt the FHE to encrypt those shadow images before uploading them to the blockchain, since FHE algorithm allows secure computations on encrypted data without decrypting it. Compared with other FHE algorithms [73]–[76], BFV algorithm [77] has superior performances in the aspects of efficiency and feasibility due to its smaller relinearization key [77]–[79]. Thus, we choose BFV as the FHE algorithm in the proposed BC-SESIS scheme for shadow image encryption.

It is notable that, in the restoring stage of the traditional SIS schemes, the *Applicant* generally uses only one pixel from each of k shadow images to compute the coefficients of $(k-1)$-degree polynomial by Lagrange's interpolation algorithm. Those k coefficients are the k pixels of the original secret image. The Applicant repeats the above process until all secret pixels are computed. However, the restoring process is quite time-computing, especially in the encrypted domain. To efficiently encrypt and decrypt the secret image, a batch encryption strategy is designed to encrypt the generated shadow images before uploading to the blockchain.

As shown in 2, instead of encrypting the pixels one by one, the *Participants* first divide the pixels of each shadow image S_i to form a set of vectors $\{v_i^j | 1 \leq j \leq len\}$, represented by

$$\begin{cases} v_i^1 = \{S_i(1), S_i(2), \ldots, S_i(N)\} \\ v_i^2 = \{S_i(N+1), S_i(N+2), \ldots, S_i(2N)\} \\ \cdots\cdots \\ v_i^j = \{S_i(N \times (j-1)+1), S_i(N \times (j-1)+2) \cdots \\ \qquad \cdots, S_i(N \times j)\} \\ \cdots\cdots \\ v_i^{len} = \{S_i(N \times (\ len\ -1)+1), \\ \qquad S_i(N \times (\ len\ -1)+2), \cdots\cdots, S_i(w \times h)\} \end{cases} \tag{3}$$

Where the value of len refers to the number of vectors in this set. Then, those vectors are encrypted sequentially by BFV algorithm as $\{v_i^{j\prime} | 1 \leq j \leq len\}$. Finally, the set of encrypted vectors are packed as an encrypted shadow image file S_i'.

By the above batch encryption strategy, a batch of pixels can be encrypted by one encryption operation, and these encrypted pixels can be also decrypted by a single decryption operation. Consequently, the encryption and decryption can be efficiently implemented, and thus a lot of computing time can be saved. That is also proven by the experimental results given in Sections V-C and V-D.

Step (3) Shadow image uploading: It is worth noting that directly storing these large sized encrypted files on the blockchain will cause large storage burden and high latency for the blockchain. Thus, the *Participants* upload each encrypted file to the IPFS, and the IPFS returns a unique hash string and uses it as the file's address. Then, this address is sent to the blockchain.

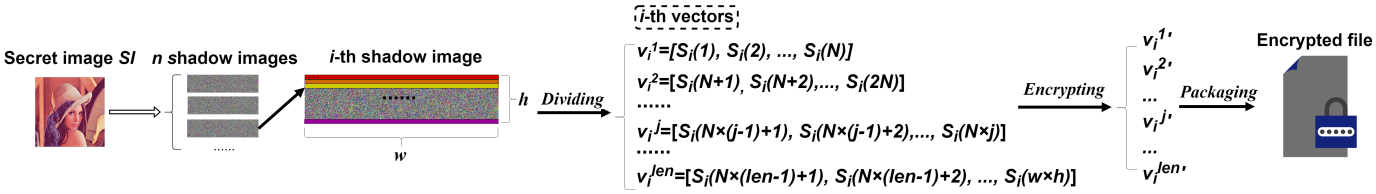

Fig. 2. The process of batch encryption.

C. Secret Image Restoring Stage

In the stage of secret image restoring, there are three main steps:(k, n) threshold realization, encrypted domain polynomial computation, and secret image decryption. To restore the original secret image, we design the AutoIDAuth-enabled smart contract for realizing the (k, n) threshold of SIS and the FHE-based outsourcing computing method for implementing the polynomial computation in encryption domain.

Step (1) (k, n) threshold realization: As introduced in Section II-B, the smart contract is essentially a computing independently and automatically on every node of the network protocol deployed on the blockchain in form of codes. It runs in a predefined manner, thereby decreasing the transaction cost for participants and the occurrence of abnormal and malicious actions on the blockchain. Due to the advantages of the smart contract, we design the AutoIDAuth-enabled smart contract to realize the (k, n) threshold of SIS by authenticating the identities of Participants. To realize the (k, n) threshold of SIS,the AutoIDAuth-enabled smart contract works as follows.

When the *Applicant* intends to restore a secret image, he is required to send the restoring request with his identity and gas reward to the smart contract by the HTTP SSL protocol. Then, the smart contract authenticates the identity of *Applicant*. If the authentication is passed, the smart contract broadcasts the *Applicant*'s restoring request to the n *Participants* to ask for their authorizations for access of the encrypted shadow image files.

The *Participants* who agree to authorize will send their identity information to the smart contract, and the smart contract will authenticate the *Participants*' identities. If the number of *Participants*' authorizations is larger than k, the smart contract will automatically trigger the following process, *i.e.*, the encrypted domain polynomial computation; Otherwise, the *Applicant* will be informed that the original secret image cannot be restored for the lack of enough *Participants*' authorizations.

Step (2) Encrypted domain polynomial computation: As mentioned in the previous step, once the smart contract receives at least k *Participants*' authorizations, it will trigger a part of secret image restoring task, *i.e.*, encrypted domain polynomial computation. Note that it is infeasible for the smart contract to directly implement the computation task, since the computation will cause large computing burden and high latency for the smart contract. Thus, the FHE-based outsourcing computing method is proposed to outsource the polynomial computation task to the *Agent Miners* of blockchain. In this method, BFV [73] is selected as the FHE algorithm to encrypt the generated shadow images, since BFV has superior performances in the aspects of efficiency and feasibility [73], [77], as mentioned in Section III-B. The outsourcing process is described as follows.

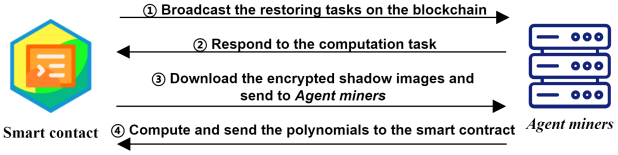

Fig. 3. The illustration of outsourcing process, in which the smart contract outsources the task of secret image computation to the *Agent miners*.

As shown in the 3, after collecting more than k *Participants*' authorizations, the smart contract broadcasts the task of encrypted domain polynomial computation to the *Agent miners* on the blockchain. Then, the *Agent miners* respond to the task. By the k *Participants*' authorizations, the smart contract downloads the corresponding encrypted shadow image files from IPFS, and sends them to m randomly selected *Agent miners* for implementing this task. Afterward, these *Agent miners* compute the polynomials in encrypted domain separately, and send the coefficients of computed polynomials to the smart contract. Finally, the smart contract compares all the computed polynomials to decide whether to keep the computed result. Specifically, if all the computed results are the same, the smart contract will keep the coefficients of computed polynomials and pay the gas reward to the *Agent miners*; Otherwise, it will broadcast the computation task again. That ensures the computation process is implemented correctly and securely. The computation of polynomials in encrypted domain is elaborated as follow.

Suppose an *Agent miner* receives k encrypted shadow images $\{S_i'|1 \leq i \leq n\}$ from the smart contract. According to the FHE and Lagrange Interpolation algorithms, the encrypted secret image SI' can be restored from these shadows by computing a set of $(k-1)$-degree polynomials.

Recall that every N pixels of each shadow image are transformed to a vector, and the vector is encrypted before uploading the shadow image. Consequently, for i-th shadow image, a set of encrypted vectors are generated and packaged $\{v_i^{j'}|1 \leq i \leq k, 1 \leq j \leq len\}$, where len means the number of encrypted vectors. By using all the j-th encrypted vectors $\{v_i^{j'}|1 \leq i \leq k\}$ of the k encrypted shadow images, the corresponding $(k-1)$-degree polynomial $Ln(x)$ can be computed

by using Lagrange Interpolation, represented by

$$Ln(x) = \sum_{i=1}^{k} v_i^{j'} \prod_{t=1, t\neq i}^{k} \frac{(x - X_t)}{(X_i - X_t)} \tag{4}$$

Where, X_i and X_t are the encrypted forms of the two numbers x_i and x_t, which are used in (1) to generate image shadows.

To facilitate the polynomials expression, we take $m_i = \prod_{t=1,t\neq i}^{k}(X_i - X_t)$ and $K = \prod_{i=1}^{k} m_i$. Thus, (13) can be further represented by

$$Ln(x) = \sum_{i=1}^{k} \frac{v_i^{j'}}{m_i} \prod_{t=1, t\neq i}^{k} (x - X_t) \tag{5}$$

For the i-th basic polynomial $\prod_{t=1,t\neq i}^{k}(x - X_t)$, it can be expanded to a $(k-1)$-degree polynomial with the coefficients D_{it}, $1 \leq t < k$, and thus $Ln(x)$ can be expressed by

$$Ln(x) = \sum_{i=1}^{k} \frac{v_i^{j'}}{m_i} \left(D_{i0} + D_{i1}X^1 + \ldots + D_{i,k-1}X^{k-1}\right) \tag{6}$$

In (6), every coefficient is divided by m_i. However, the division operation cannot be supported in BFV algorithm. To handle this issue, we introduce the K's inverse element denoted as $invK$ in the field F_p, and it satisfies:

$$K \cdot \otimes \cdot \operatorname{inv} K \cdot \operatorname{mod} \cdot p = 1 \tag{7}$$

According to Fermat's little theorem, if p is a prime greater than an integer a, $a^{(p-1)} = 1(modp)$ and $invK$ is equal to $K^{(p-2)}$, where the fast exponentiation algorithm is used to calculate the value of $invK$. Then, both sides of (6) are multiplied by $invK * K$ to eliminate the division operation by

$$\begin{aligned} Ln'(x) &= \operatorname{Ln}(x) * K * \operatorname{inv} K \\ &= \sum_{i=1}^{k} \frac{v_i^{j'}}{m_i} * K * \operatorname{inv} K * \sum_{t=0}^{k-1} D_{it} * X^t (\operatorname{mod} \cdot p) \\ &= \sum_{i=1}^{k} v_i^{j'} * K_i * \operatorname{inv} K * \sum_{t=0}^{k-1} D_{it} * X^t (\operatorname{mod} \cdot p) \\ &= \sum_{i=1}^{k} C_{ij} \sum_{t=0}^{k-1} D_{it} * X^t (\operatorname{mod} \cdot p) \end{aligned} \tag{8}$$

Where, $C_{ij} = v_i^{j'} * K_i * invK$, and $K_i = \prod_{t=1,t\neq i}^{k} m_t$, which is the product of all denominators except for m_i. We calculate the coefficient: $A_{tj} = \sum_{i=1}^{k} C_{ij} * D_{it}$, which is the coefficient of X^t when using all the j-th encrypted vectors to compute the polynomial.

Finally, after receiving the coefficient set $\{A_{tj} | 1 \leq k \leq len, 0 \leq t < k\}$, the *Applicant* decrypts the received coefficients as the vectors and transforms them to the pixel values, and then implements modulus operation on these values by p to compute the original secret image *SI*.

Note that, in the stage of secret image restoring, a large amount of computation resources are required in calculating the coefficients of base polynomials like $\prod_{t=1,t\neq i}^{k}(x - X_t)$. If we compute these base polynomials directly, the computational complexity is $O(2^k)$. The time consumption will increase exponentially with the increase of k. To address this issue, based on the idea of recording and reusing the sum of terms of polynomials, we propose an improved computing strategy, called as prefix-sum, to reduce the complexity to $O(k^2)$.

Given a function of continuous multiplication $g(x) = \prod_{i=1)}^{n}(x + a_i)$, by expanding the right side of function completely and merging the congeners, the result is given as follow:

$$\begin{aligned} g(x) =& x^n + \left(\sum_{i_1}^{n} a_{i1}\right) x^{n-1} + \cdots \\ & \cdots + \left(\sum_{i_1=1}^{n-t+1} a_{i1} \sum_{i_2=i_1+1}^{n-t+2} a_{i2} \ldots \sum_{i_t=i_{t-1}+1}^{n} a_{it}\right) x^t \\ & + \cdots + \sum_{i=1}^{n} a_i \end{aligned} \tag{9}$$

We can define the values of D_i as the coefficients. The values of D_i can be represented by:

$$\begin{cases} D_0 =& 1 \\ D_1 =& a_1 + \ldots + a_l + \ldots + a_n (1 \leq l \leq n) \\ D_2 =& a_1 (a_2 + \ldots + a_n) + \cdots + a_l (a_{l+1} + \ldots + a_n) \\ & + \ldots + a_{n-1}a_n (1 \leq l \leq n-1) \\ D_3 =& a_1 (a_2 (a_3 + \ldots + a_n) + \ldots + a_{n-1}a_n) \\ & + a_2 (a_3 (a_4 + \ldots + a_n) + \ldots + a_{n-1}a_n) + \cdots \\ & + a_{n-2}a_{n-1}a_n \\ & \ldots \end{cases} \tag{10}$$

To simplify the expression, we introduce $T_{i,j}$ to represent the sum of the first j terms in D_i's formula. The result is given as follows:

$$\begin{cases} D_0 =& 1 \\ D_1 =& a_1 + \ldots + a_l + \ldots + a_n (1 \leq l \leq n) \\ D_2 =& a_1 (T_{1,n} - T_{1,1}) + \ldots + a_l (T_{1,n} - T_{1,l}) + \ldots + \\ & a_{n-1} (T_{1,n} - T_{1,n-1}) (1 \leq l \leq n-1) \\ D_3 =& a_1 (T_{2,n-1} - T_{2,1}) + \ldots + a_l (T_{2,n-1}T_{2,l}) + \ldots + \\ & a_{n-2} (T_{2,n-1} - T_{2,n-2}) (1 \leq l \leq n-2) \\ & \ldots \\ D_j =& \sum_{t=1}^{n-t+1} a_l (T_{t-1,n-t+2} - T_{t-1,l}) (l \geq 2) \\ & \ldots \end{cases} \tag{11}$$

In the calculation process, recording and reusing $T_{i,j}$ can effectively reduce the computation costs. If we have known the value of $T_{i-1,l}$, the complexity of calculation D_j is only $O(n)$.

Step (3) Secret image decryption: After the outsourcing computation, the smart contract receives the coefficients of computed polynomials. Then, the smart contract will transmit the computed polynomials to the *Applicant*. After receiving the computed polynomials, the *Applicant* decrypts the coefficients

as the vectors and transforms them to the pixel values, and then implements the modulus operation on these pixel values by p to restore the original secret image *SI*.

IV. Security Analyses

In this section, the threshold security of the BC-SESIS scheme is analyzed and then its resistance to some common attacks including tampering, corruption, and approximating attacks are discussed.

Theorem 1: Only when k or more *Participants* agree to authorize the access of their shadow images, the original secret image can be restored.

Proof: In the BC-SESIS scheme, the designed AutoIDAuth-enabled smart contract acts as (k, n) threshold function of SIS. The smart contract requires to authenticate the identities of the *Applicant* and *Participants* before sending the encrypted shadows to the *Applicant*. When the number of *Participants* passing the authentication is less than k, the smart contract will not trigger the restoring task. In other words, the original secret image can be restored only when any k or more *Participants* agree to authorize the access of their shadow images. As a result, any $k-1$ or less authorizations cannot restore the secret images in our scheme.

Moreover, to restore the secret image, the BC-SESIS outsources a considerable part of the secret image restoring task, *i.e.*, the polynomial computation in the encryption domain. The polynomial computation algorithm is stored as an executable file deployed on IPFS, and thus it cannot be modified due to the distributed characteristics of IPFS.

In addition, in the BC-SESIS scheme, the original secret image is restored by the Lagrange interpolation algorithm. In the literature [4], [6], [36], the interpolation theorem states that one and only one $(k-1)$-degree polynomial can pass through k given points at the same time in the two-dimensional space (the points refer to the image shadows in our scheme). A corollary is that any number of shadows fewer than k cannot correctly restore the desired $(k-1)$-degree polynomial. In essence, there are countless $(k-1)$-degree polynomials in two-dimensional space that pass through the points fewer than k simultanously. Therefore, in the case of fewer than k shadow image, it is not possible to obtain the secret SI by Lagrange interpolation algorithm.

Theorem 2: Attackers cannot modify or obtain the information of the original images throughout the IPFS and blockchain environment.

Proof: In the semi-honest environment, the possible attacks are given as follows: (1) modifying the image shares before the restoring task, (2) keeping the image shares during the restoring stage and restoring the shadow image after the restoring task is completed. The proof of security against the two attacks is detailed as follows.

(1) By using the blockchain technology, new information is added to a block and can be used by all users or nodes in the distributed network. Due to the distributed and decentralized characteristics of the structure of blockchain data, each node of the network can save the shadow images stored on the blockchain in the encrypted form. However, since most of the nodes in the blockchain network are assumed to be honest and reliable, it is difficult to modify these data, unless 51% of nodes are compromised simultaneously.

(2) The smart contract solves the authentication problem in the secret image sharing. Each participant will be assigned the unique authentication information, which makes the impersonation attack invalid. Even if the miners intercept the information, *i.e.* k encrypted shadow images $\{s_i' | 1 \leq i \leq n\}$, in the restoring calculation and use them for private calculation and restoring task, the miners can only obtain the coefficients of polynomial in the encrypted domain by:

$$Ln(x) = \sum_{i=1}^{k} v_i^{j\prime} \prod_{t=1, t\neq i}^{k} \frac{(x - X_t)}{(X_i - X_t)} \tag{12}$$

To separate the different coefficients, according to the Fermat's little theorem, we introduce the concept of inverse element, so that the formula is deduced to:

$$Ln'(x) = \sum_{i=1}^{k} C_{ij} \sum_{t=0}^{k-1} D_{it} * X^t (\mathrm{mod} \cdot p) \tag{13}$$

By the above formula, the attacker may obtain the set of coefficients that are encrypted during the secret image sharing phase. Hence, without the decryption key *sk*, the attacker cannot obtain any useful information from these encrypted coefficients. Therefore, the attacker cannot restore the original image from these encrypted coefficients. In summary, the attackers cannot modify or obtain the information of the original images in the IPFS and blockchain environment.

Theorem 3: Approximating attack can be resisted effectively.

Proof: Approximating the coefficients is one of the most common attacks on polynomial-based SIS schemes. With the consideration of the correlation of neighboring pixels, someone can assume that $a_0 \approx a_1 \approx a_2 \approx ... \approx a_{(k-1)}$. Hence, $a_0 \approx f(1)/k$, which means one of the coefficients is approximately obtained without any shadows and it will give a clue about the information of secret image SI without encryption. This drawback makes it possible to restore the secret image with the number of image shadows fewer than k.

However, the original secret image is partitioned into a set of parts beforehand, so as to transform the pixels into multi-dimensional vectors. That can not only significantly improve the calculation speed, but also effectively break the relationships between neighboring pixels. Since the relationships between adjacent pixels will not be kept, the approximating attacks can be resisted effectively. Therefore, the proposed scheme is secure against the approximation attack.

V. Experimental Result and Analyses

To test the performance of the BC-SESIS scheme, extensive experiments are implemented and the corresponding analyses are also given. All experiments are conducted on Win10 operating system with i7-9750H CPU @2.60GHz.

TABLE III
IMPACTS OF K AND N ON RESTORING TIME CONSUMPTION ANS ACCURACY

Value of k in the threshold of SIS	Minimum N	Time consumption of computing a polynomial	Restoring accuracy
k=2	16,384	0.697s	100%
k=3	16,384	1.99s	100%
k=4	32,768	19.5s	100%
k=5	32,768	36.4s	100%
k=6	32,768	60.0s	100%

A. Parameter Selection

In the proposed BC-SESIS scheme, there are two key parameters, *i.e.*, k and N. Here, k means the minimum number of shadow images used for restoring the original secret one, and N means the number of pixels divided into each batch during the batch encryption for shadow images. In this section, we measure the impacts of the parameters on the performance of restoring the time consumption and accuracy of the proposed BC-SESIS scheme.

In the BFV algorithm [77], the encryption process is usually accompanied by some noise, and both addition and multiplication will amplify the noise in the decryption result. In the process of computing a single polynomial, encrypting more pixels can lead to more noise in the encryption result. Thus, if N exceeds a certain value, the accuracy of image restoring will be affected. With the increase of N, the computation time of the restoring process increases significantly. Also, the parameter k determines the depth of the multiplication, and has impact on the restoring time consumption and accuracy. To find a good balance between the restoring efficiency and accuracy, it is necessary to test the impacts of the two parameters on the restoring time consumption and accuracy of the proposed BC-SESIS scheme.

TABLE III shows the impacts of k and N on the restoring time consumption and accuracy. Minimum N means the minimum value of N that can ensure the secret image is 100% restored. From this table, to ensure that the restoring accuracy is maintained at a 100%, N is set as 16,384 when k=2 or 3, and N is set as 32,768 when $k \geq 4$. Also, it is clear that the time consumption of computing a single polynomial is only less than 2 seconds when N=16,384. The time consumption increases significantly, when N=32768.

B. Quality of Restored Secret Image

We present the results of secret images restored by the BC-SESIS scheme. 4 shows an experimental result of the original version and the restored version of a 256 × 256 image by the proposed BC-SESIS scheme. In this experiment, a $(4, 6)$-threshold case of our scheme is used. 4(a) shows an image with the size of 256 × 256. 4(b)∼(g) show the generated six shadow images, which are noisy images and their sizes are $\frac{1}{4}$ of the original secret image. Finally, 4(h) is the restored secret image, which is produced from any four shadow ones.

The quality of the restored secret image by the proposed BC-SESIS scheme is tested by different statistical metrics including Root Mean Square Error (RMSE) and Peak Signal to Noise Ratio (PSNR).

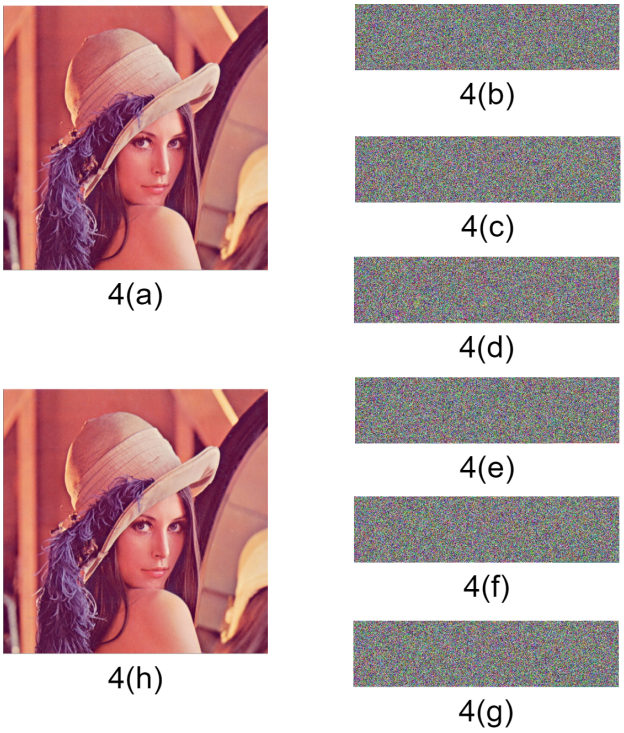

Fig. 4. The comparison between an original secret image and the restored one. (a) the original secret image, (b) (g) the generated shadow images, (h) the restored secret image.

Definition 2 The value of RMSE describes the distinction between the original secret image and the restored one. RMSE is defined by

$$RMSE = \sqrt{\frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (S[i,j] - RI[i,j])^2} \quad (14)$$

where $SI[i,j]$ and $RI[i,j]$ are the (i,j)-th pixels of secret image and the restored image with the sizes of $M \times N$, respectively. Smaller RMSE value means higher quality of the restored secret image.

Definition 3. PSNR measures the similarity between the original secret image and the restored one. PSNR is defined by

$$PSNR(db) = 10 \times \log_{10}\left(\frac{255 \times 255}{RMSE}\right) \quad (15)$$

Where, a higher PSNR value means a higher quality of the restored secret images.

In the experiment, when 65536 pixels were restored, the RMSE value is only 0.0771 and the PSNR value reaches up to 59.2611, as shown TABLE IV. Thus, it is clear that there is

TABLE IV
RMSE AND PSNR VALUES OF SECRET AND RESTORED IMAGES OF BC-SESIS SCHEME

Number of pixels	RMSE	PSNR
65536	0.0771	59.2611

almost no difference between the original secret image and the restored image. Thus, the quality of the secret image restored by the BC-SESIS is desirable.

C. Validity of Batch Encryption Strategy on Efficiency

To improve the efficiency of generating shadow images, the batch encryption strategy is designed and adopted in Section III-B. The process of secret image restoring consists of multiple operation of computing polynomials by Lagrange's interpolation algorithm. In the traditional scheme, each coefficient of the polynomial is used to hide one pixel and each polynomial computation can restore k pixels. In the proposed BC-SESIS scheme, batch encryption strategy can greatly enhance the restoring efficiency of secret image. It can hide N pixels into each coefficient and each polynomial computation can restore $N \times k$ pixels simultaneously. In this section, we will conduct the experiments to compare the time consumption and the number of restored pixels per each polynomial computation by traditional encryption strategy and batch encryption strategy. In addition, we will finally compare the efficiency of the two strategies by observing the time consumption of restoring an image with the size of 512×512.

According to TABLE V, the restore efficiency of the batch encryption strategy is much higher than that of the traditional one, in which the pixels are encrypted one by one. For different values of k, different values of N are selected to keep the restoring accuracy at 100%. When $k = 6$, the restoring time per pixel consumed by the batch encryption scheme is nearly 800 times faster than that of the traditional encryption strategy. Since each polynomial computation can restore $N \times k$ pixels, the time for restoring the whole image by using the batch encryption strategy is much less than that by the traditional strategy. It is obvious that the batch encryption strategy can greatly improve the efficiency of our scheme, especially when k equals to a large value.

D. Validity of Prefix-Sum Strategy on Efficiency

As described in Section III, we introduce a *Prefix-Sum* strategy to efficiently compute the coefficients of continuous multiplication polynomials $\prod_{(t=1,t\neq i)}^{k}(x - X_t)$. The proposed *Prefix-Sum* strategy significantly reduce the computational complexity of our scheme from $O(2^k)$ to $O(k^2)$. In the following part, we will compare the time consumption of each polynomial computation between the standard computation strategy and the proposed *Prefix-Sum* computation strategy.

As shown in 5, by comparing the efficiency of the two computation strategies, it is clear that the time consumption of the the standard computation strategy is slightly lower than that of *Prefix-Sum* computation strategy when k is 2 or 3. When k is greater than 3, it is obvious that the time consumption of the standard computation strategy grows much faster than that of the Prefix-Sum computation strategy. In summary, the proposed *Prefix-Sum* computation strategy can efficiently improve the efficiency of the proposed scheme, especially when k is equal to a large value.

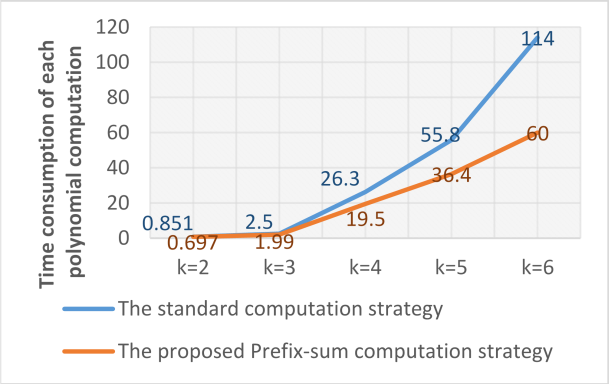

Fig. 5. Efficiency comparison between the standard computation strategy and the proposed *Prefix-Sum* computation strategy.

E. Time Saved in Users' Side

As described in Section III-C, the *Applicant* outsources the task of computing polynomials in the encrypted domain to the *Agent miners*. Then, the *Applicant* also should decrypt the computed polynomial coefficients as vectors and transforms them to the pixel values, and implement a modulus operation by p on the pixel values to restore the original secret image. Thus, we analyze the time saved at the users' side by the outsourcing computation.

In the following part, we will test the users' time consumption T_1 with outsourcing computation, the time consumption T_2 of restoring the secret image, and the saving rate of time consumption $\alpha = \frac{(T_2 - T_1)}{T_2}$. The time consumption is shown in TABLE VI. From this table, since the *Applicant* outsources the complex polynomial computation process, the saving rate of users' side can reach 62.7% to 74.9%, when the value of k ranges from 2 to 6; The outsourcing computing can effectively save rate of time consumption at the users' side at least 62.7%; In addition, with the increasing the value of k, the polynomial computation process becomes more complex, and the proportion of the modular operation in the total restoring task is reduced. Thus, the saving rate of the time consumption increases with the increase of k. In summary, it is proven that the outsourcing computing method can significantly saves users' computing resources.

F. The probability of cracking the secret image

In this subsection, we text the probability of successfully cracking the secret image via random guess. Suppose an attacker cannot obtain the decryption key sk, which is protected well by the participants. According to (1) and (3) in Section III-B, the probabilities of successfully cracking the secret

TABLE V
EFFICIENCY COMPARISON BETWEEN BATCH ENCRYPTION STRATEGY AND TRADITIONAL ENCRYPTION STRATEGY IN RESTORING STAGE

Schemes		Number of restored pixels	Consuming time	Restoring 512×512 picture
k=2	Traditional	2	0.678s	24.7h
	Batch	16384	0.697s	11.5s
k=3	Traditional	3	1.98s	48.1h
	Batch	24576	1.99s	21.9s
k=4	Traditional	4	19.6s	357h
	Batch	65536	19.5s	78s
k=5	Traditional	5	36.1s	526h
	Batch	81920	36.4s	116s
k=6	Traditional	6	59.6s	723h
	Batch	98304	60.0s	160s

TABLE VI
TIME SAVED BY THE PROPOSED BC-SESIS SCHEME IN THE USERS' SIDE WITH DIFFERENT VALUES OF K

	T_1(ms)	T_2(ms)	$\alpha(\%)$	the size of *SI*
k=2	0.081	0.217	62.7	128 × 256
k=3	0.081	0.233	65.2	128 × 256
k=4	0.163	0.502	67.5	256 × 256
k=5	0.163	0.573	71.6	256 × 256
k=6	0.163	0.649	74.9	256 × 256

image hidden into the encrypted coefficients of polynomials can be computed by

$$P_c = \frac{1}{256^{k^2 \times len}} \tag{16}$$

Where k means the threshold value and len means the number of polynomials of the proposed BC-SESIS scheme. The computed P_c values with different values of k are listed in Table VII. It is clear that the probabilities of successfully cracking the secret image are quite small, which indicates the proposed scheme is secure enough.

VI. CONCLUSION

In this paper, to securely communicate and effectively protect secret image data in wireless communication, we have presented the BC-SESIS scheme with outsourcing computation in wireless networks. In this scheme, the generated shadows are encrypted and stored in the blockchain to prevent them from being tampered and/or corrupted. The identity authentication-enabled smart contract is deployed on the blockchain to achieve the (k, n) threshold of SIS for secret image restoring. The FHE-based outsourcing computation method is designed to outsource the task of secret image restoring to reduce the computational burden of smart contract and users. The theoretical analyses and extensive experiments prove that the BC-SESIS scheme not only achieves desirable security, but also has high computational efficiency.

The proposed BC-SESIS scheme has been proven that it can effectively manage and protect the images distributed on the networks. Thus, it has great significance in practical applications. In the days and future of digital world, we plan to further reduce the computational burden of smart contract and users, and also attempt to improve the outsourcing computation method to completely outsource all the verification and computation operations of the SIS task in the wireless networks.

ACKNOWLEDGMENT

This work is supported in part by the National Natural Science Foundation of China under Grant 61972205 and Grant U1936218, in part by the Guangdong Natural Science Funds for Distinguished Young Scholar under Grant 2023B1515020041, in part by Ministry of Science and Technology under Grant MOST 110-2221-E-259-005-MY2, in part by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) fund, China, and in part by the Japan Society for the Promotion of Science (JSPS) Grants-in-Aid for Scientific Research (KAKENHI) under Grant JP21K17736.

Zhili Zhou (M'19) received his MS and PhD degrees in Computer Application at the School of Information Science and Engineering from Hunan University, in 2010 and 2014, respectively. He is currently a professor with Institute of Artificial Intelligence and Blockchain, Guangzhou University. Also, he was a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Windsor, Canada. His current research interests include Multimedia Security, Artificial Intelligence Security, Information Hiding, Digital Forensics, Blockchain, and Secret Sharing. He has authored or coauthored more than 100 refereed papers. He is serving as an Associate Editor of Journal of Real-Time Image Processing, Security and Communication Networks, and International Journal on Semantic Web and Information Systems. He received ACM Rising Star Award and got Guangdong Natural Science Funds for Distinguished Young Scholar.

Yao Wan is a graduate student. He is currently pursuing the M.S. degree in the Nanjing University of Information Science and Technology, China, in 2020. His research interest includes blockchain and information security.

TABLE VII
THE PROBABILITIES OF SUCCESSFUL CRACKING SECRET IMAGE PROTECTED BY BC-SESIS SCHEME

	k=2	k=3	k=4	k=5	k=6
P_c	1.84×10^{-19}	7.92×10^{-28}	1.84×10^{-19}	1.21×10^{-24}	7.92×10^{-28}

Qi Cui received his B.S. degree in Software Engineering and Ph.D. degree in Information and Communication Engineering at Nanjing University of Information Science and Technology, China in 2017 and 2022. Now he is a research fellow at the Institute of Artificial Intelligence and Blockchain, Guangzhou University, China. He was a visiting scholar at the Centre for Computer Vision and Deep Learning, University of Windsor, Canada. His research interests include information hiding, adversarial learning, and multi-media security.

Keping YU (S'11-M'17) received the M.E. and Ph.D. degrees from the Graduate School of Global Information and Telecommunication Studies, Waseda University, Tokyo, Japan, in 2012 and 2016, respectively. Currently, he is with the Graduate School of Science and Engineering, Hosei University, Tokyo 184-8584, Japan. He is also a Visiting Professor with the College of Computer Science, Sichuan Normal University, Chengdu, China. His research interests include smart grids, information-centric networking, the Internet of Things, blockchain, and information security.

Shahid Mumtaz (M'13–SM'16) is with the Department of Applied Informatics, Silesian University of Technology, Akademicka 16 44-100 Gliwice, Poland and Departement of Engineering, Nottingham Trent University, UK, and an IET Fellow, an IEEE ComSoc and ACM Distinguished Lecturer, a recipient of the IEEE ComSoc Young Researcher Award, founder and Editor-in-Chief of IET's Journal of Quantum Communication, Editor-in-Chief of the Alex-andria Engineering Journal (Elsevier), Vice-Chair, Europe/Africa Region - IEEE ComSoc Green Communications Computing Society, and Vice-Chair for IEEE Standard P1932.1, "Standard for Licensed/Unlicensed Spectrum Interoperability in Wireless Mobile Networks." His work has resulted in technology transfer to companies and patented technology. His expertise lies in 5G/6G wireless technologies using AI/ML and digital twin (VR/XR) tools and innovation paths in industry and academia. Moreover, he worked as a senior 5G consultant at Huawei and InterDigital, where he contributed to RAN1 /RAN2 and looked after the university-industrial collaborative projects.

Ching-Nung Yang (Senior Member, IEEE) received the B.S. and M.S. degrees in telecommunication engineering from National Chiao Tung University, Hsinchu, Taiwan, in 1983 and 1985, respectively, and the Ph.D. degree in electrical engineering from National Cheng Kung University, Tainan City, Taiwan, in 1997. He is currently a Full Professor with the Department of Computer Science and Information Engineering, National Dong Hwa University, Hualien, Taiwan. His research interests include coding theory, information security, and cryptography. He is a fellow of IET.

MOHSEN GUIZANI (Fellow, IEEE) received the BS (with distinction), MS and PhD degrees in Electrical and Computer engineering from Syracuse University, Syracuse, NY, USA in 1985, 1987 and 1990, respectively. He is currently a Professor of Machine Learning and the Associate Provost at Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), Abu Dhabi, UAE. Previously, he worked in different institutions in the USA. His research interests include applied machine learning and artificial intelligence, Internet of Things (IoT), intelligent autonomous systems, smart city, and cybersecurity. He was elevated to the IEEE Fellow in 2009 and was listed as a Clarivate Analytics Highly Cited Researcher in Computer Science in 2019, 2020, 2021 and 2022. Dr. Guizani has won several research awards including the "2015 IEEE Communications Society Best Survey Paper Award", the Best ComSoc Journal Paper Award in 2021 as well five Best Paper Awards from ICC and Globecom Conferences. He is the author of ten books and more than 800 publications. He is also the recipient of the 2017 IEEE Communications Society Wireless Technical Committee (WTC) Recognition Award, the 2018 AdHoc Technical Committee Recognition Award, and the 2019 IEEE Communications and Information Security Technical Recognition (CISTC) Award. He served as the Editor-in-Chief of IEEE Network and is currently serving on the Editorial Boards of many IEEE Transactions and Magazines. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of the TAOS Technical Committee. He served as the IEEE Computer Society Distinguished Speaker and is currently the IEEE ComSoc Distinguished Lecturer.

REFERENCES

[1] F. Zhan, N. Yao, Z. Gao, and H. Yu, "Efficient key generation leveraging wireless channel reciprocity for manets," *Journal of Network and Computer Applications*, vol. 103, pp. 18–28, 2018.

[2] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Networks*, vol. 21, no. 6, pp. 1835–1846, 2015.

[3] T. Karygiannis and L. Owens, *Wireless Network Security:*. US Department of Commerce, Technology Administration, National Institute of . . . , 2002.

[4] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Computers & Graphics*, vol. 26, no. 5, pp. 765–770, 2002.

[5] ——, "An image-sharing method with user-friendly shadow images," *IEEE Transactions on circuits and systems for video technology*, vol. 13, no. 12, pp. 1161–1169, 2003.

[6] C.-C. Lin and W.-H. Tsai, "Secret image sharing with steganography and authentication," *Journal of Systems and software*, vol. 73, no. 3, pp. 405–414, 2004.

[7] C.-N. Yang, T.-S. Chen, K. H. Yu, and C.-C. Wang, "Improvements of image sharing with steganography and authentication," *Journal of Systems and software*, vol. 80, no. 7, pp. 1070–1076, 2007.

[8] A. Beimel, "Secret-sharing schemes: A survey," in *International conference on coding and cryptology*. Springer, 2011, pp. 11–46.

[9] X. Yan, L. Liu, L. Li, and Y. Lu, "Robust secret image sharing resistant to noise in shares," *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, vol. 17, no. 1, pp. 1–22, 2021.

[10] Y. Sun, Y. Lu, X. Yan, L. Liu, and L. Li, "Robust secret image sharing scheme against noise in shadow images," *IEEE Access*, vol. 9, pp. 23 284–23 300, 2021.

[11] M. K. Sardar and A. Adhikari, "A new lossless secret image sharing scheme for grayscale images with small shadow size," in *Proceedings of International Conference on Frontiers in Computing and Systems*. Springer, 2021, pp. 701–709.

[12] S. Charoghchi and S. Mashhadi, "Three (t, n)-secret image sharing schemes based on homogeneous linear recursion," *Information Sciences*, vol. 552, pp. 220–243, 2021.

[13] X. Wu, C.-N. Yang, and Y.-Y. Yang, "A hybrid scheme for enhancing recovered image quality in polynomial based secret image sharing by modify-and-recalculate strategy," *Journal of Information Security and Applications*, vol. 51, p. 102452, 2020.

[14] P.-Y. Lin and C.-S. Chan, "Invertible secret image sharing with steganography," *Pattern Recognition Letters*, vol. 31, no. 13, pp. 1887–1893, 2010.

[15] X. Wu, D. Ou, Q. Liang, and W. Sun, "A user-friendly secret image sharing scheme with reversible steganography based on cellular automata," *Journal of Systems and Software*, vol. 85, no. 8, pp. 1852–1863, 2012.

[16] G. Prema and S. Natarajan, "Steganography using genetic algorithm along with visual cryptography for wireless network application," in *2013 International Conference on Information Communication and Embedded Systems (ICICES)*. IEEE, 2013, pp. 727–730.

[17] N. F. Johnson and S. Jajodia, "Steganalysis: The investigation of hidden information," in *1998 IEEE Information Technology Conference, Information Environment for the Future (Cat. No. 98EX228)*. IEEE, 1998, pp. 113–116.

[18] J. Fridrich and M. Goljan, "Practical steganalysis of digital images: state of the art," *security and Watermarking of Multimedia Contents IV*, vol. 4675, pp. 1–13, 2002.

[19] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," *IEEE Transactions on information Forensics and Security*, vol. 7, no. 3, pp. 868–882, 2012.

[20] M. Poongodi, A. Sharma, V. Vijayakumar, V. Bhardwaj, A. P. Sharma, R. Iqbal, and R. Kumar, "Prediction of the price of ethereum blockchain cryptocurrency in an industrial finance system," *Computers & Electrical Engineering*, vol. 81, p. 106527, 2020.

[21] P. Treleaven, R. G. Brown, and D. Yang, "Blockchain technology in finance," *Computer*, vol. 50, no. 9, pp. 14–17, 2017.

[22] K. A. Clauson, E. A. Breeden, C. Davidson, and T. K. Mackey, "Leveraging blockchain technology to enhance supply chain management in healthcare:: An exploration of challenges and opportunities in the health supply chain," *Blockchain in healthcare today*, 2018.

[23] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom)*. IEEE, 2016, pp. 1–3.

[24] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare:"medrec" prototype for electronic health records and medical research data," in *Proceedings of IEEE open & big data conference*, vol. 13, 2016, p. 13.

[25] D.-Y. Liao and X. Wang, "Applications of blockchain technology to logistics management in integrated casinos and entertainment," in *Informatics*, vol. 5, no. 4. MDPI, 2018, p. 44.

[26] A. Dutra, A. Tumasjan, and I. M. Welpe, "Blockchain is changing how media and entertainment companies compete," *MIT Sloan Management Review*, vol. 60, no. 1, pp. 39–45, 2018.

[27] B. Yong, J. Shen, X. Liu, F. Li, H. Chen, and Q. Zhou, "An intelligent blockchain-based system for safe vaccine supply and supervision," *International Journal of Information Management*, vol. 52, p. 102024, 2020.

[28] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[29] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *2016 IEEE 19th international conference on intelligent transportation systems (ITSC)*. IEEE, 2016, pp. 2663–2668.

[30] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, 2017.

[31] T. N. Dinh and M. T. Thai, "Ai and blockchain: A disruptive integration," *Computer*, vol. 51, no. 9, pp. 48–53, 2018.

[32] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International journal of web and grid services*, vol. 14, no. 4, pp. 352–375, 2018.

[33] S. Rathore, Y. Pan, and J. H. Park, "Blockdeepnet: a blockchain-based secure deep learning for iot network," *Sustainability*, vol. 11, no. 14, p. 3974, 2019.

[34] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, "A comprehensive review of the covid-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact," *Ieee access*, vol. 8, pp. 90 225–90 265, 2020.

[35] Z. Zhou, M. Wang, C.-N. Yang, Z. Fu, X. Sun, and Q. J. Wu, "Blockchain-based decentralized reputation system in e-commerce environment," *Future Generation Computer Systems*, vol. 124, pp. 155–167, 2021.

[36] M. Naor and A. Shamir, "Visual cryptography," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1994, pp. 1–12.

[37] X. Yan, S. Wang, A. A. Abd El-Latif, and X. Niu, "New approaches for efficient information hiding-based secret image sharing schemes," *Signal, Image and Video Processing*, vol. 9, no. 3, pp. 499–510, 2015.

[38] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology—EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia, Italy, May 9–12, 1994 Proceedings 13*. Springer, 1995, pp. 1–12.

[39] X. Jia, D. Wang, D. Nie, and C. Zhang, "Collaborative visual cryptography schemes," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 5, pp. 1056–1070, 2016.

[40] T.-H. Chen and K.-H. Tsao, "Visual secret sharing by random grids revisited," *Pattern recognition*, vol. 42, no. 9, pp. 2203–2217, 2009.

[41] K.-S. Lin, C.-H. Lin, and T.-H. Chen, "Distortionless visual multi-secret sharing based on random grid," *Information Sciences*, vol. 288, pp. 330–346, 2014.

[42] Y. Zhang, J. Zhang, W. Gao, X. Zheng, L. Yang, J. Hao, and X. Dai, "Distributed electrical energy systems: Needs, concepts, approaches and vision," *Acta Automatica Sinica*, vol. 43, no. NREL/JA-5D00-70646, 2017.

[43] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for ai: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10 127–10 149, 2019.

[44] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 3–16.

[45] ——, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 3–16.

[46] Y. Zuo, S. Jin, and S. Zhang, "Blockchain storage, computation offloading, and user association for heterogeneous cellular networks," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8191–8204, 2021.

[47] Y. Zuo, S. Jin, S. Zhang, and Y. Zhang, "Blockchain storage and computation offloading for cooperative mobile-edge computing," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 9084–9098, 2021.

[48] Y. Zuo, S. Jin, and S. Zhang, "Blockchain storage, computation offloading, and user association for heterogeneous cellular networks," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8191–8204, 2021.

[49] ——, "Computation offloading in untrusted mec-aided mobile blockchain iot systems," *IEEE Transactions on Wireless Communications*, vol. 20, no. 12, pp. 8333–8347, 2021.

[50] Y. Zuo, S. Jin, S. Zhang, Y. Han, and K.-K. Wong, "Delay-limited computation offloading for mec-assisted mobile blockchain networks," *IEEE Transactions on Communications*, vol. 69, no. 12, pp. 8569–8584, 2021.

[51] Y. Zuo, S. Jin, and S. Zhang, "Computation offloading and user association for blockchain-enabled heterogeneous cellular networks," in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*. IEEE, 2021, pp. 01–06.

[52] J. Guo, Y. Zuo, C.-K. Wen, and S. Jin, "User-centric online gossip training for autoencoder-based csi feedback," *IEEE Journal of Selected Topics in Signal Processing*, vol. 16, no. 3, pp. 559–572, 2022.

[53] Y.-X. Liu, C.-N. Yang, C.-M. Wu, Q.-D. Sun, and W. Bi, "Threshold changeable secret image sharing scheme based on interpolation polynomial," *Multimedia Tools and Applications*, vol. 78, pp. 18 653–18 667, 2019.

[54] Z. Wu, Y. Liu, and X. Jia, "A novel hierarchical secret image sharing scheme with multi-group joint management," *Mathematics*, vol. 8, no. 3, p. 448, 2020.

[55] X. Yan, Y. Lu, and L. Liu, "A general progressive secret image sharing construction method," *Signal Processing: Image Communication*, vol. 71, pp. 66–75, 2019.

[56] C. Guo, C.-C. Chang, and C. Qin, "A hierarchical threshold secret image sharing," *Pattern Recognition Letters*, vol. 33, no. 1, pp. 83–91, 2012.

[57] T.-H. Chen and C.-S. Wu, "Efficient multi-secret image sharing based on boolean operations," *Signal Processing*, vol. 91, no. 1, pp. 90–97, 2011.

[58] A. Iftekhar and X. Cui, "Anti-tamper protection for internet of things system using hyperledger fabric blockchain technology," *arXiv preprint arXiv:2109.07074*, 2021.

[59] R. Huo, S. Zeng, Z. Wang, J. Shang, W. Chen, T. Huang, S. Wang, F. R. Yu, and Y. Liu, "A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges," *IEEE Communications Surveys & Tutorials*, 2022.

[60] B. Zhang, "Research on the judicial expertise of electronic evidence based on blockchain," in *MATEC Web of Conferences*, vol. 359. EDP Sciences, 2022, p. 01022.

[61] M. Yoo and Y. Won, "A study on the transparent price tracing system in supply chain management based on blockchain," *Sustainability*, vol. 10, no. 11, p. 4037, 2018.

[62] P. Centobelli, R. Cerchione, P. Del Vecchio, E. Oropallo, and G. Secundo, "Blockchain technology for bridging trust, traceability and transparency in circular supply chain," *Information & Management*, vol. 59, no. 7, p. 103508, 2022.

[63] H. Gao, Z. Ma, S. Luo, and Z. Wang, "Bfr-mpc: a blockchain-based fair and robust multi-party computation scheme," *IEEE access*, vol. 7, pp. 110 439–110 450, 2019.

[64] S. Wu, J. Li, F. Duan, Y. Lu, X. Zhang, and J. Gan, "The survey on the development of secure multi-party computing in the blockchain," in *2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC)*. IEEE, 2021, pp. 1–7.

[65] Y. Wei, "Blockchain-based data traceability platform architecture for supply chain management," in *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*. IEEE, 2020, pp. 77–85.

[66] J. Benet, "Ipfs-content addressed, versioned, p2p file system," *arXiv preprint arXiv:1407.3561*, 2014.

[67] Y. Chen, H. Li, K. Li, and J. Zhang, "An improved p2p file system scheme based on ipfs and blockchain," in *2017 IEEE International Conference on Big Data (Big Data)*. IEEE, 2017, pp. 2652–2657.

[68] Q. Zheng, Y. Li, P. Chen, and X. Dong, "An innovative ipfs-based storage model for blockchain," in *2018 IEEE/WIC/ACM international conference on web intelligence (WI)*. IEEE, 2018, pp. 704–708.

[69] N. Szabo, "Formalizing and securing relationships on public networks," *First monday*, 1997.

[70] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, pp. 2–1, 2014.

[71] C. D. Clack, V. A. Bakshi, and L. Braine, "Smart contract templates: foundations, design landscape and research directions," *arXiv preprint arXiv:1608.00771*, 2016.

[72] W. Zou, D. Lo, P. S. Kochhar, X.-B. D. Le, X. Xia, Y. Feng, Z. Chen, and B. Xu, "Smart contract development: Challenges and opportunities," *IEEE Transactions on Software Engineering*, vol. 47, no. 10, pp. 2084–2106, 2019.

[73] M. Ibtihal, N. Hassan *et al.*, "Homomorphic encryption as a service for outsourced images in mobile cloud computing environment," in *Cryptography: Breakthroughs in Research and Practice*. IGI Global, 2020, pp. 316–330.

[74] Z. Brakerski and V. Vaikuntanathan, "Fully homomorphic encryption from ring-lwe and security for key dependent messages," in *Annual cryptology conference*. Springer, 2011, pp. 505–524.

[75] C. Gentry, *A fully homomorphic encryption scheme*. Stanford university, 2009.

[76] C. Gentry, S. Halevi, C. Peikert, and N. P. Smart, "Ring switching in bgv-style homomorphic encryption," in *International Conference on Security and Cryptography for Networks*. Springer, 2012, pp. 19–37.

[77] S. Halevi, Y. Polyakov, and V. Shoup, "An improved rns variant of the bfv homomorphic encryption scheme," in *Cryptographers' Track at the RSA Conference*. Springer, 2019, pp. 83–105.

[78] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) lwe," *SIAM Journal on computing*, vol. 43, no. 2, pp. 831–871, 2014.

[79] C. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based," in *Annual Cryptology Conference*. Springer, 2013, pp. 75–92.