IEEE TRANSACTIONS ON
EMERGING TOPICS
IN COMPUTING

Received 5 December 2019; revised 29 March 2020; accepted 26 April 2020.
Date of publication 11 May 2020; date of current version 16 September 2021.

Digital Object Identifier 10.1109/TETC.2020.2993032

Circuit Copyright Blockchain: Blockchain-Based Homomorphic Encryption for IP Circuit Protection

WEI LIANG, (Member, IEEE), DAFANG ZHANG, XIA LEI, MINGDONG TANG, (Member, IEEE), KUAN-CHING LI, (Senior Member, IEEE), AND ALBERT Y. ZOMAYA, (Fellow, IEEE)

W. Liang and D. Zhang are with the College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China
X. Lei is with the Department of Computer Science and Technology, China University of Petroleum, Beijing 100024, China
M. Tang is with the School of Information Science and Technology, Guangdong University of Foreign Studies, Guangzhou 510420, China
K.-C. Li is with the Department of Computer Science and Information Engineering (CSIE), Providence University, Taichung 43301, Taiwan
A.Y. Zomaya is with the School of Computer Science, The University of Sydney, Sydney NSW 2006, Australia
CORRESPONDING AUTHOR: K. LI (kuancli@pu.edu.tw)

ABSTRACT The fast development of Blockchain technology makes it widely applied in several fields of digital transactions, like e-government affairs and the protection of financial transactions. In this article, we propose a homomorphic encryption-based Blockchain for circuit copyright protection that effectively addresses the issues in the protection of circuit copyright transactions, such as low security of private data, low efficiency in transaction data storage, cooperation and supervision. First, we establish a homomorphic encryption-based mathematical model by utilizing Blockchain and intelligent contract, and next, the algorithms that include Blockchain generation, homomorphic chain encryption/decryption, and intelligent contract are designed. As the intelligent contract is correctly executed in Blockchain, a fully homomorphic encryption-based identity authentication protocol is tackled for Blockchain, given that it ensures the change operation of any third-party in Blockchain and realizes real-time verification. The system is apposite for circuit copyright protection in a blockchain network, due to the use of distributed identity authentication and real-time extensible storage improves the security and extensibility of blockchain-based circuit copyright protection. The experimental results show that the proposed algorithm has reduced the transmission cost and improved the efficiency of data storage and supervision. In addition, it is resilient to several common attacks (e.g., double-spending attacks), yet incurs low cost/overhead and has a higher level of security when compared to three other competing algorithms.

INDEX TERMS Blockchain network, homomorphic encryption, IP circuit, consensus mechanism, double-spending

I. INTRODUCTION

With the increasing number of intellectual property (IP) cores being digitalized, it is highly required to have in place mechanisms to protect IP in the digitalized era. There are many challenges associated with the protection of digital IP cores, for example, due to the transient nature of digital goods and the ease in which such goods can be copied across borders.

In this paper, we explore the potential of Blockchain to facilitate the protection of digital IP cores. Before moving further to describing the proposed approach, we first briefly introduce Blockchain, which is a distributed ledger comprising a large number of independent nodes that jointly maintain the integrity and security of data stored in the different blocks. As all nodes jointly maintain and store the data in the chain, data stored in a blockchain is difficult to tamper and forge [1], [2]. There are three types of Blockchain: public / permissionless Blockchain [3], [4], private / permissioned Blockchain, and federated Blockchain. As the name suggests, nodes in a public Blockchain are public, and they can participate in the calculation of Blockchain transaction data and obtain a copy of the complete Blockchain ledger. The public Blockchain is decentralized and is generally associated with high energy consumption and low mining speed, while the private Blockchain is open to only a private group of individuals, where only approved nodes can access the data in the Blockchain and participate in calculation [5]. Some private Blockchain (e.g., Ant Financial)[1] are designed not to be decentralized. Different to former two types, a federated blockchain involves several

[1]https://www.antfin.com

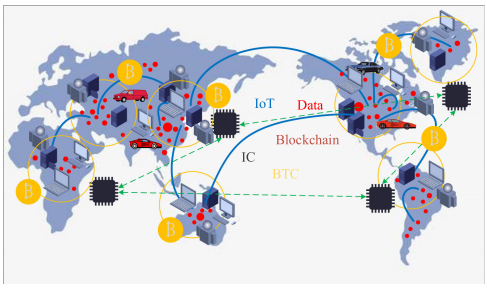

FIGURE 1. Authenticity verification, say in global transaction of electronic chips.

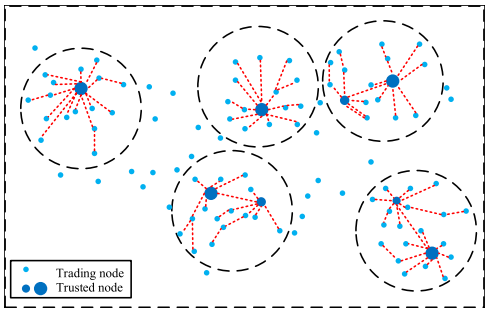

FIGURE 2. Decentralized network transaction.

organizations for joint management. For example, an organization controls a part of the nodes in the federated Blockchain, participates in the data calculation, and jointly records the resultant data. That is, all read and write operations are transmitted between organizations of the federated Blockchain.

One example application of the federated blockchain is in electronic transaction [6], [7], [8] and authenticity verification - say, in global transaction of electronic chips, as depicted in Figure 1. In such a scenario, a Blockchain-based integrated circuit (IC) protection method can rapidly verify the authenticity of various IC components that are traded in different parts of the world [9], [10], [11]. A summary of features that underpin a Blockchain used to facilitate the global transaction of electronic chips is presented as follows:

- The capability to perform a calculation by all nodes in the Blockchain-based network,
- The maintenance and supervision of a distributed system like the Blockchain-based network is spread out and not concentrated at any particular node. For example, by using a proof-of-work (PoW) consensus mechanism, every node in the system participates in the approval process of every transaction. The system also includes a check and balance mechanism to minimize the risk of a cheating node. Censorship and supervision are also performed by the respective algorithms in the network automatically, so that each element in the system is completely transparent. These attributes contribute to decentralization and minimization of cheating, and hence suitable for IC circuit protection,
- As a decentralized point-to-point network, the Blockchain comprises a large number of distributed nodes and servers, where each node stores a copy of the complete ledger. Hence, both high fault-tolerance and security are assured.

The remaining of this paper is organized as follows. We present the proposed approach that integrates homomorphic encryption and Blockchain in Section III, then demonstrate the potential of the proposed approach in Section IV, where we describe both the evaluation setup and discuss the findings, and finally, concluding remarks and future directions in Section V.

II. RELATED WORK

There are a large number of potential applications of blockchain [12], [13], [14], [15], [16], [17], [18], including in service computing[19], [20], digital IC protection[21], among several others.

Initial Blockchain is a P2P payment system from which users can directly send bitcoin toward each other for the transaction via Blockchain. The transaction can be controlled by intelligent contract and recorded in Blockchain without the participation of the government. It is pointed out that a Blockchain-based network is an institute to transmit value, and the transaction can be verified in real-time to avoid the deceiving behavior by spending two times of bitcoin [22]. Due to the feature of value transmission, many financial institutes immensely investigated the technical framework of financial Blockchain and proposed several Blockchain about value transmission [23], [24].

In recent years, the control of digital copyright can be regarded as another issue, the way how to make the ecological environment of information resource run healthily by reasonable rules with the participation of illegal users. The Blockchain has features of decentralization, difficulty in tampering, good extensibility, and flexibility, which are suitable for the requirements of digital IC copyright protection [25]. In [26], authors inserted a unique digital digest in a product by using Blockchain technology, making it not be forged nor tampered, while in [27], the design of Blockchain and intelligent contracts can realize automatic copyright transaction in a secure and reliable environment. The cash conversion efficiency and creative motivation are significantly improved. The Blockchain is untampered and traceable that provides natural credibility for tracing the infringement and protection [28], as it can be compelling evidence of enforcing authority. In [29], the Blockchain-based digital copyright protection and the transaction system assist in addressing issues of secure copyright protection and credible transaction.

As shown in Figure 2, the decentralized network transaction has features of fast transaction speed and high efficiency. However, there are severe problems such as low security, data abuse, and dependence on central nodes. Current Blockchain-based IP transactions usually utilized three organization structures for transaction verification, involving linear structure, star structure, and tree structure, as depicted in Figure 3.

In linear structure, the nodes communicate orderly, and a node can communicate after the front one ending communication. If a node is invalid, the sequential nodes cannot receive communication data, causing the bottleneck effect. In

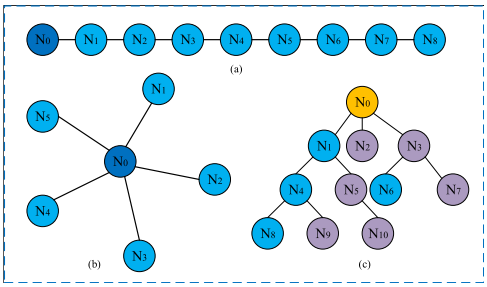

FIGURE 3. The node transaction for different types of Blockchain.

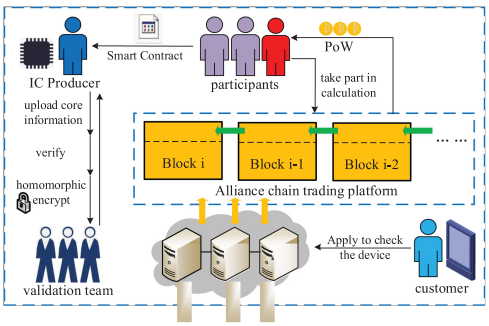

FIGURE 5. IP transaction chart in federated blockchain.

star structure, each node connects with the central node, which is responsible for maintaining the network connectivity, realizing identity authentication, and routing schedule. The star structure has good extensibility, as a new node can be easily added to the network. Besides, network monitoring, security control, and priority control are also convenient. However, the central node may be overloaded, and the network paralysis occurs once the central node is invalid. Lastly, the tree structure is hierarchical, and the layers depend on the node number and communication. Generally, there should not be too many layers, avoiding significant forwarding overhead. In a hierarchical structure, the communication will not depend on a single node. and therefore, there is no bottleneck effect. If the tree structure has two layers, it will be a star structure. If the number of layers in the tree structure is equal to that of the nodes, it is a linear structure, and thus, the hierarchical structure can be regarded as the extension of star structure and linear structure.

At present, there are many privacy leakage events, causing serious security issues. The homomorphic encryption supports various operations on the ciphertext without decryption. After decryption, the operations remain effective for the plain text. In this case, users can fully use the robust calculation and storage ability of Blockchain without worrying about the privacy leakage. The security of Blockchain-based digital copyright is ensured. Notably, the following issues are involved.

In traditional IP transaction, the third party is required to authenticate the credibility of the transaction, since it causes serious effects such as piracy, cheat, and easy loss, as shown in Figure 4 such traditional transaction process. In federated Blockchain, the IP transaction chart is shown in Figure 5.

1) Large communication overhead. The distributed system has no central entity to coordinate other members. Therefore, the coordination and communication can only be performed by the system member, as it requires extra resources and calculation ability. Therefore, not all resources are used for calculation,
2) High complexity. It requires a program or software to make the system normally execute and address various problems in the running process. Extra coordination and communication increase the complexity of the software,
3) Security issue. Network communication means some critical data will be transmitted or shared. However, data transmission via network exists a security issue. Since some incredible entities may monitor the network to capture critical information, any distributed system should first address the security issues. The less limitation of the nodes will cause more security issues.

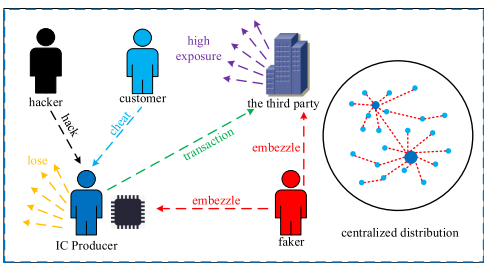

FIGURE 4. Traditional IP transaction chain.

This work utilizes homomorphic encryption to address the abovementioned issues. The homomorphic encryption is that the operations on the ciphertext are equal to that on the decrypted plain text. The service provider can directly deal with the ciphertext and return the result to the users in the form of ciphertext, so the users decrypt the result and obtain the original data.

III. OUR PROPOSAL

In the IP transaction process, we should prove that the chained IP copyright information is legal. First, the credibility of IP should be verified, but not performed by the third central institute. It is conceptualized from distributed multiple centralizations, where the Blockchain-based IP copyright transaction model uses the structure feature of Blockchain without the participation of the third central institute. Therefore, it can compensate for the security drawback due to the existence of a third party. The structure feature of Blockchain can effectively prevent data from being tampered or misappropriated. Besides, the traditional incentive mechanism is to verify a party of IP transaction, which pays for the users. Therefore, as the related benefit party, users may suspect that the quality of IP transaction data is degraded maliciously, so less reward is paid. In the Blockchain-based IP transaction model, the data is verified by the miner who is apart from the benefit. It will effectively avoid the unfair treatment of the users.

This work combines the Blockchain and homomorphic encryption to protect IP copyright in the transaction. Homomorphic encryption can directly decrypt the ciphertext after a

series of operations, and the results are the same as that for the plain text [30]. Due to the high security, homomorphic encryption plays a vital role in the Blockchain environment. The definition of homomorphic encryption is as follows.

Definition 1 (Homomorphic Encryption): Suppose that the plaintext and ciphertext is $M = \{T_1, T_2, \ldots, T_n\}$ and $C = \{c_1, c_2, \ldots, c_n\}$, the encryption function and decryption function is E and D respectively and the key is $K = k_1, k_2, \ldots, k_n$. If Equation (1) is true for function f, then the encryption operation E is homomorphic for function f.

$$E(f(T_1, T_2, \ldots, T_n)) = f(E(T_1), E(T_2), \ldots, E(T_n)). \tag{1}$$

A complete homomorphic encryption scheme is composed of four parts: key generation function, encryption function, decryption function, and evaluation function. In Section II, a complete IP transaction authentication scheme based on homomorphic encryption in Blockchain and the specific process of homomorphic encryption transaction is proposed. When the transaction initiator initiates a transaction, the miners in the Blockchain verify whether the transaction is reasonable through the IP transaction authentication scheme based on homomorphic encryption. After the verification is passed, the correct execution of the smart contract on the Blockchain will be triggered, and the smart contract automatically updates the ciphertext of the account balance of both parties according to the execution result. After some time, the verified transactions will be confirmed. That is, they enter the Blockchain with the new block. The property of homomorphic encryption allows the miner to directly update the account balance in the ciphertext state without decryption. If the account balance is $\{m_1, m_2, \ldots, m_n\}$, the ciphertext is $(E(m_1), E(m_2), \ldots, E(m_n))$, so the miners can effectively calculate $E(f(T_1, T_2, \ldots, T_n))$ by $f(E(T_1), E(T_2), \ldots, E(T_n))$.

A. HOMOMORPHIC BLOCKCHAIN GENERATION

At present, there are fewer reports of the homomorphic encryption technology in the field of IP circuit protection. To address the robustness and security issues, it is proposed in this work Blockchain-based homomorphic encryption for IP protection, which realizes the transaction protection of the ciphertext in the homomorphic encryption system. The key generation, encryption, and decryption process are illustrated as follows.

When the core purchaser I_1 intends to have access to the IP of the core copyright owner I_2, I_1 initiates a transaction to the Blockchain. Suppose that the account balance of I_1 is W_1 and the transaction amount that I_1 needs to transfer to I_2 is T. Then, an IP transaction authentication scheme based on the Paillier [31] homomorphic cryptosystem in Blockchain is proposed as follows:

1) Key generation: I_1 and I_2 randomly choose two primes p_i and q_i, $i = 1, 2, \ldots$, and compute $Q_i = p_i \cdot q_i$, $\lambda_i = lcm(p_i - 1, q_i - 1)$, $i = 1, 2, \ldots$, where $lcm(\cdot)$ represents the least common multiple. Then I_1 and I_2 randomly choose another integers $r_i = \mathbb{Z}^*_{Q^2}, i = 1, 2, \ldots$, which satisfies formula (2).

$$gcd\left(\frac{r_i^{\lambda_i} \bmod Q_i^2 - 1}{Q_i}, Q_i\right) = 1, \tag{2}$$

where $\mathbb{Z}_{Q^2}$ is the set of integers smaller than Q^2, $\mathbb{Z}^*_{Q^2}$ is the set of integers coprime with Q^2, $gcd(\cdot)$ and represents the most significant common factor.

Let $PK_{I_1} = (Q_1, r_1)$ and $SK_{I_1} = \lambda_1$ be the public key and private key of I_1 and let $PK_{I_2} = (Q_2, r_2)$ and $SK_{I_2} = \lambda_2$ be the public key and private key of I_2 respectively.

2) Encryption stage: I_1 randomly selects an encryption parameter $\tau_{1T} \in \mathbb{Z}^*_Q$ and encrypts T by $PK_{I_1} = (Q_1, r_1)$ to obtain the ciphertext

$$C_{1T} = E_1(T) = r_1^T \cdot \tau_{1T}{}^{Q_1} \bmod {Q_1}^2. \tag{3}$$

In addition, I_1 randomly chooses another encryption parameter $\tau_{2T} \in \mathbb{Z}^*_Q$ and encrypts T by $PK_{I_2} = (Q_2, r_2)$ to obtain the ciphertext

$$C_{2T} = E_2(T) = r_2^T \cdot \tau_{2T}{}^{Q_2} \bmod {Q_2}^2. \tag{4}$$

The randomness of τ results in different ciphertexts of the same transaction amount T, though these different ciphertexts can be decrypted into the same T. Therefore, I_1 needs to evidence to the miner that the plaintext information of the ciphertext C_{1T}, C_{2T} is equal.

3) Decryption and authentication stage: Let $Q_1 = Q_2$, the ciphertext can be decrypted by the private key λ_1, λ_2 of I_1 and I_2 as follows:

$$T_i = D(C_{iT}) = \frac{F(C_{iT}{}^{\lambda_i}) \bmod Q^2}{F(r_i{}^{\lambda_i}) \bmod Q^2} \bmod Q, \tag{5}$$

where $i = 1, 2, \ldots$, $F(x) = \frac{x-1}{Q}$, $T_1 = T_2 = T$. And the following properties are known:

Property 1: $\forall T_1, T_2 \in \mathbb{Z}_Q, k \in \mathbb{N}$,

$$D(E(T_1) \cdot E(T_2) \bmod Q^2) = (T_1 + T_2) \bmod Q. \tag{6}$$

Therefore, the above cryptosystem satisfies the addition of homomorphism.

Property 2: $\forall T \in \mathbb{Z}_Q, k \in \mathbb{N}$,

$$D(E(T)^k \bmod Q^2) = kT \bmod Q. \tag{7}$$

The homomorphism of the above cryptosystem can be applied to prove to the miner that the ciphertexts C_{1T} and C_{2T} contain the same plaintext information, and verify that the transaction is legal while ensuring the transaction security. The specific process is as follows:

Assuming that the safety parameter is N, the core purchaser I_1 generates a uniformly distributed random number $\varepsilon_i, 1 \le i \le N$ and calculates $T + \varepsilon_i, 1 \le i \le N$. Let

$$\eta_{1i} = E_1(\varepsilon_i), \eta_{2i} = E_2(\varepsilon_i), \tag{8}$$

where $1 \leq i \leq N$.

The homomorphic addition is performed by the public key PK_{I_1} of I_1 and let

$$T_{1i} = C_{1T} + \eta_{1i}, 1 \leq i \leq N. \tag{9}$$

Moreover, homomorphic addition is performed by the public key PK_{I_2} of I_2 and let

$$T_{2i} = C_{2T} + \eta_{2i}, 1 \leq i \leq N. \tag{10}$$

I_1 sends the parameters $(C_{1T}, C_{2T}, \eta_{1T}, \eta_{2T}, T_{1i}, T_{2i})$ to the Blockchain. The miners on the Blockchain launch a challenge h to I_1, and send a string $h_i, h_i \in 0, 1$ containing N bits to I_1. When I_1 receives h, if $h_i = 0$, I_1sends the plaintext ε_i of η_{1i}, η_{2i} and the encryption parameters τ_{1i}, τ_{2i} to miners. If $h_i = 1$, I_1 sends the plaintext $T + \varepsilon_i$ of T_{1i}, T_{2i} and the encryption parameters $\tau_{1T} + \tau_{1i}, \tau_{2T} + \tau_{2i}$ to miners. Only when the miner verifies that all ciphertexts have passed, the miners accept the transaction and output T, and the transaction is ignored and outputs F if otherwise. Thus, the following theorem holds.

Theorem 1: According to the above IP transaction authentication scheme based on the homomorphic cryptosystem, the probability that I_1 cheats the miner, although they accept the transaction and output T is $1/2^N$. That is, the security of the scheme can be measured with $1 - 1/2^N$.

B. HOMOMORPHIC ENCRYPTION BASED TRADING PROCESS

IC Blockchain is to package the IC transaction information into a block during a period and send it to all the participators of IC transactions. After confirming the IC transaction information is valid, it is chained to an existing IC Blockchain. In the IC Blockchain network, the members who participate in the Blockchain generation is called IC design miner, and the miners repeatedly address issues in the Blockchain. The transaction information is recorded into the newly generated block and then transmitted to the next miner, who will interrupt digging and verify the content of the received block. If there is no problem with the received block, it will be chained to the existing block and pay a reward to the miner. In order to make more bitcoin, the miner requires digging repeatedly. The use of Blockchain is not to store the information into the server, but into the network, and therefore, it is difficult to forge data in the network.

The traditional method is to store information into the central server. If attacked, the security of the stored information is threatened and vulnerable. In the Blockchain, the information is stored in the form of a block. If malicious attackers attack the block, he will attack more than 51 percent stored data in the computer, which is an impossible task for the attackers. Thereafter, this section considers using the homomorphic encryption algorithm to encrypt the transaction information on the Blockchain into ciphertext, and the account balance is stored on the Blockchain in the form of ciphertext. When the transaction information is published on the Blockchain, other verification nodes on the Blockchain validate the rationality of the transaction through the Blockchain authentication scheme based on homomorphic encryption in Section II. If the transaction information is verified, it will trigger the smart contract on the Blockchain to be correctly executed. The smart contract automatically updates the ciphertext of the account balances of both parties to the transaction according to the execution result. The specific process is as follows:

1) User initialization stage: users of the Blockchain-based on homomorphic crypto transaction in this article include core purchaser I_1, the core copyright owner I_2, and other verification nodes V. During the initialization stage, it is utilized the homomorphic encryption algorithm to generate user information during the phase, inputs the public parameters of homomorphic encryption $(Q_j, r_j, \lambda_j, \tau_{jT}), j = 1, 2, \ldots$ and the security parameter N to generate the user's public and private keys $PK_{I_1} = (Q_1, r_1), PK_{I_2} = (Q_2, r_2), SK_{I_1} = \lambda_1, SK_{I_2} = \lambda_2$. And then, the ciphertexts C_{1T} and C_{2T} are generated. The user's public key can be used as the address of the transaction receipt, and the private key can generate a digital signature.

When the core purchaser I_1 initiates a transaction, the public key PK_{I_1}, the private key SK_{I_1} of I_1 and the ciphertext C_{1W_1} of account balance W_1 needs to be generated at this stage and stored on the Blockchain ledger. Also, since the Blockchain transfer authentication based on homomorphic encryption is performed in the subsequent transfer transaction phase, the ciphertext C_{1W_1-T} should be generated by $W_1 - T$ using its own public key PK_{I_1} in this stage.

2) Transfer transaction stage: When a transaction is initiated by I_1, assume that the account balance is W_1 and the transaction amount to be transferred to I_2 is T. According to Section II of the Blockchain authentication scheme based on homomorphic encryption, I_1 generates random $\varepsilon_i, 1 \leq i \leq N$ and $T + \varepsilon_i, \eta_{1i}, \eta_{2i}, T_{1i}, T_{2i}, 1 \leq i \leq N$ can be calculated by formulas (10), (11), (12). I_1 sends the parameters $C_{1T}, C_{2T}, \eta_{1i}, \eta_{2i}, T_{1i}, T_{2i}$ to the Blockchain, and other verification nodes on the Blockchain launch a challenge h to I_1. The miners send a string $h_i, h_i \in 0, 1$ containing N bits to I_1. When I_1 receives h, if $h_i = 0$, I_1 sends ε_i and the encryption parameters τ_{1i} and τ_{2i} to verification nodes. If $h_i = 1$, I_1 sends $T + \varepsilon_i$ and the encryption parameters $\tau_{1T} + \tau_{1i}, \tau_{2T} + \tau_{2i}$ to verification nodes. Solely after the verification nodes are validated with all ciphertexts, the verification nodes accept the transaction and output T; otherwise, the transaction is ignored and outputs F. According to Theorem 1, the probability that cheats the miner though they accept the transaction and output T is $1/2^N$, the security of the scheme can be greatly guaranteed when a larger value of N is taken.

In the transfer transaction stage, I_1 transfers amount T to I_2 and inputs the public parameters $(Q_j, r_j, \lambda_j, \tau_{jT}), j = 1, 2, \ldots$, the transaction amount T, the account balance W_1 of I_1 before the transaction, the public key PK_{I_1}, the ciphertext C_{1W_1} of the account balance W_1 before the transaction, the account balance $W_1 - T$ of I_1 after the transaction, the ciphertext C_{1W_1-T} of the account balance $W_1 - T$ of I_1 after the transaction and

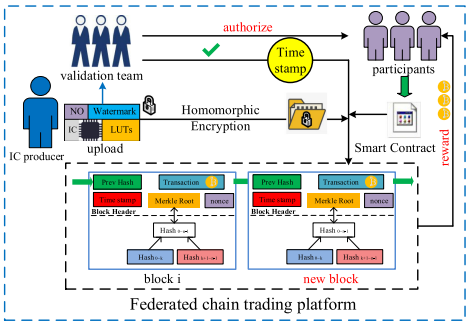

FIGURE 6. **Blockchain-based homomorphic encryption.**

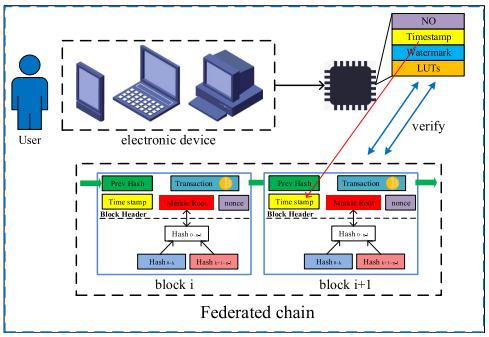

FIGURE 7. **Homomorphic decryption and authentication of federated chain.**

the public key PK_{I_2} of I_2. A transfer statement $(C_{1T}, C_{2T}, T, W_1, PK_{I_1}, PK_{I_2}, C_{1W_1}, C_{1W_1-T}$ is generated and sent to the Blockchain.

3) Execute the transaction phase: the verification node V on the Blockchain verifies that the reduced transaction amount of the account of I_1 and the increasing transaction amount of the account of I_2 is equal, and the account balance before the transaction is greater than the transaction amount. Verification node V takes the public parameters $(Q_j, r_j, \lambda_j, \tau_{jT}), j = 1, 2, \ldots$ and the transfer statements as inputs at this stage. If the verification result is correct, and the verified transaction is announced, the transfer transaction will trigger the smart contract on the Blockchain to automatically perform the transfer operation. The ciphertext of the account balance $C'_{1W_1} = C_{1W_1} - C_{1T}$ of I_1 is updated by the smart contract according to the execution result and the ciphertext of the account balance $C'_{2W_2} = C_{2W_2} - C_{2T}$ of I_2 is updated at the same time. Otherwise, the verification nodes ignore the transaction. After a moment, the verified transaction will be confirmed; that is, the new block will enter the Blockchain. In general, a verification process is deployed on the Blockchain, and transaction verification will trigger a smart contract on the chain that automatically perform the transfer operation.

C. HOMOMORPHIC ENCRYPTION OF BLOCKCHAIN

IP owner can insert the secret information into the encrypted IP core without decryption. Let the copyright information be S. It will first be transformed into a binary stream and then encrypted with the homomorphic encryption algorithm, as shown in Figure 6, and the secret key stored in the key file. The encrypted binary stream is divided into fragments $\{s_1, s_2, \ldots, s_n\}$ with the same length. In the transaction process, the insertion of copyright information may cause suspicion of the attackers, making it be easily attacked. To reduce the randomness and uncontrollability of the inserted information in the transaction process, we design an effective algorithm to make the watermarked positions close to the original functional design. This model can constrain and search for suitable watermark positions, so the watermarks are inserted into the positions around the original design.

The homomorphic encryption algorithm can realize transactions in cases of decryption or non-decryption. The ciphertext of IP or original IP transaction information can be restored, since it can ensure the traceability of the algorithm in IP transaction.

Algorithm 1. Homomorphic Encryption of Federated Chain Transaction Algorithm

Input:

Chip *core*, random number p, *challenge* , difficulty coefficient d , last block $block_{i-1}$;

Output:

New generated block;

1: The chip manufacture uploads *core* and accept authenticity verification;
2: $p = 0$;
3: repeat:
4: $p = p + 1$;
5: until $F(challenge, p) = true$;
6: Broadcast $block_{i-1} = memory - ppol, block_{i-1}, p$;
7: Encrypt the verified chip with homomorphic encryption;
8: Adjust the specific time stamp of the system;
9: The miner competes to perform intelligent contract;
10: The platform pays reward for the miner with POW mechanism;
11: **return** New block $block_i$.

D. DECRYPTION AND AUTHENTICATION

The verifier utilizes the homomorphic encryption to authenticate the copyright information $S = \{s_1, s_2, \ldots, s_n\}$ in encrypted IP core or verifies the original IP circuit by decrypting it with the private key. The homomorphic and authentication of the federated chain is shown in Figure 7. The authentication steps are illustrated as follows.

1) The verifier utilizes the private key λ and the decryption function $Decrypt_\varepsilon(\lambda, C)$ to calculate the plain text of $L' = \{l'_1, l'_2, \ldots, l'_n\}$.

$$l_i = D(l'_i) = \frac{L(l'^{\lambda}_i) mod W^2}{L(r^{\lambda}) mod W^2} mod W. \tag{11}$$

At this point, $L(x) = \frac{x-1}{W}$, $1 \le i \le n$. The decrypted authentication sequence is denoted as $L = \{l_1, l_2, \ldots, l_n\}$.

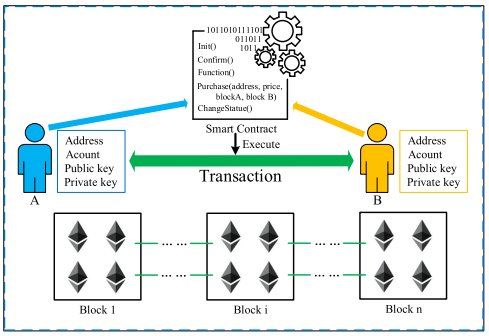

FIGURE 8. Intelligent contract of Blockchain.

2) The authentication sequence $\{s_1, s_2, \ldots, s_n\}$ is used to search the resources of authentication in IP transaction, which are scanned as the programming data stream. The extracted sequence can be parsed with a specific width, and lastly, the encrypted authentication information is generated.

3) The original authentication information is encrypted with the standard homomorphic encryption algorithm. The extracted binary stream should be decrypted to generate the original copyright information S.

4) The decrypted copyright information is compared to that of the IP owner. If the result is consistent, the ownership can be proven.

Algorithm 2. Authentication Algorithm

Input:
Chip $core_n$;
Output:
Authenticity of $core_n$;
User uploads $core_n$ to federated chain;
$p = 0$;
repeat:
$p = p + 1$;
until $F(challenge, p) \rightarrow SHA256(SHA256(challenge|p)) < \frac{2^2 24}{d}$;
Decrypt the stored chip information $core_n$ in the $block_i$ with homomorphic decryption;
if $core_n == Homomorphicdecryption(core_i)$ **then**
return true;
end if
if $core_n! = Homomorphicdecryption(core_i)$ **then**
return false;
end if

chain is used to monitor the check and running of the intelligent contract. The supervision chain can also monitor the transaction chain mutually, thus improving the security of the transaction data. With the requirement of low cost, it can significantly improve the security and management benefit of the IC circuit.

As shown in Figure 8, this work utilizes a Blockchain-based trust encourages mechanism to realize the task of IC circuit authentication. Different users can obtain different rewards. For such, the server gives a reward when a user uploads copyright data, which can be regarded as a transaction, as the generated block of the transaction is verified by a miner and then chained to the Blockchain. In the Blockchain network, the miner verifies a new transaction and records it in the total account book. After a period, a new block will be excavated, and each block contains all transactions during the period of generating the last block and packaging the current block. These transactions are orderly added to the Blockchain. After the transactions are confirmed, the user will get his reward.

The identity authentication of the IC is described as follows. First, the deposit will be paid. The user performs the identification task and uploads data to the miner, who will verify the data quality, quantify the contribution, and the reward calculated. The miner verifies the transaction between the server and the user. The reward standard is transmitted to the server, which will verify and pay the reward to the user.

Algorithm 3. Intelligent Contract Algorithm

Input:
L , key file λ;
Output:
Original copyright information S ;
if (the block is not synchronized)
wait for synchronization;
else
compile specific Solidity contract code;
$Init()$;
$Confirm()$;
$ChangeStatue()$;
if (compiling is successful)
generate binary code of Ethereum virtual machine (EVM);
deploy contract;
launch transaction and wait for entering Blockchain;
return obtained contract address from transaction data;

E. INTELLIGENT CONTRACT DESIGN

An intelligent contract is an executable program in a Blockchain transaction. When a challenge condition is activated, the transaction can be performed according to the preset rules. In this work, it is proposed an intelligent contract for IC circuit transactions to make the transaction secure. The intelligent contract is sold as a product to diversify the contract, as depicted in Figure 8. To ensure the correctness and legality of intelligent contract design, a specific supervision

IV. EXPERIMENT SETUP AND ANALYSIS

The prototype system of the proposed algorithm is implemented in Docker Version 18.03.0-ce, build 0520e24. The experimental environment is a personal computer with Intel I7-4702MQ CPU 2.20 GHz, 16G memory and 64-bit Win10 OS. The performance in terms of time overhead, communication overhead, and security are verified and checked through experiments. This work utilizes Docker to establish the application scene of the IC transaction Blockchain. Docker-compose

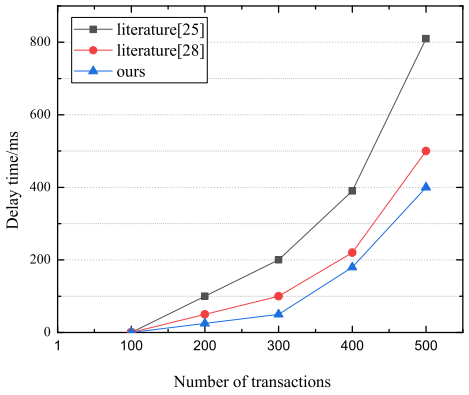

FIGURE 9. Comparison of time consuming performance.

tool can run several docker containers. The Blockchain network can run as a complete service. At the initial stage, several docker-compos.yaml files should be defined. Orderer and blocks organize the configuration, as each organization includes two peer nodes, several of which form a large-scale Blockchain-based transaction network.

A. TIME OVERHEAD

In Blockchain-based homomorphic encryption for IP protection, an empty block is generated by simple POW. The confidence mechanism of transaction nodes in the network is used to determine whether the generated block can be chained. In the generation of a block, hash calculation is used to avoid 51 percent attack. IP transaction will be put into a block and broadcast in the chain, so the chain-based proof-of-stake (POS) is involved. The blocks with higher credibility are easier to be chained than other blocks.

The methods in [25] and [28] mainly depend on calculation ability. By comparing them, this work can significantly improve network throughput and reduce network resource consumption. Besides, this work calls the distributed blocks in parallel to compare the security and management efficiency of the Blockchain-based algorithm and the original algorithm. The transaction certificate is respectively generated by the chain generation algorithm, chain authentication generation algorithm, and chain transaction algorithm. Each data is an average value. The delay time of this proposed work is compared to that of [25] and [28], and the results are depicted in Figure 9. By analyzing this figure, three algorithms have growing time-consuming with the increasing number of transactions. Nevertheless, the proposed algorithm is slower than other algorithms.

B. COMMUNICATION OVERHEAD

In a Blockchain-based IP transaction network, actual topology is a network. The tree structure in this work will not change the actual physical connection. The nodes are organized as a tree logically, so thus the network communication of different tree structures has different performance in reliability.

The node utilization reflects the ratio of nodes participating in data forwarding. The value is expected to be smaller, and

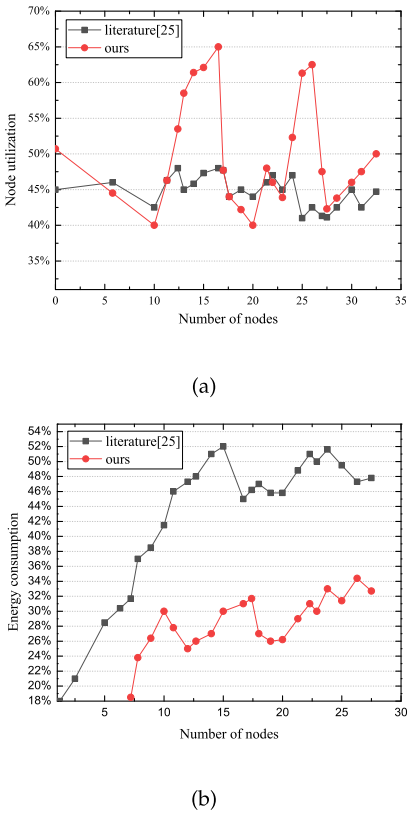

FIGURE 10. Experimental comparison among utilization rate, consumption rate and number of nodes.

thus, the communication performance is achieved by maintaining the stability and reliability of less forwarding nodes in this case. In Figure 10(a), the node utilization, and energy consumption are compared with the increase of the nodes. In [25], the node utilization is stable with the increase of the nodes. In the case of a single connection, the maximum value is less than 50 percent. The proposed algorithm has larger node utilization, and the maximum value achieves 65 percent due to the use of tree structure. In Figure 10(b), the energy consumption of the proposed algorithm is lower with the increase of nodes, when compared to [25]. In a practical Blockchain-based IP transaction environment, the communication of the proposed algorithm is realized by distributing a few high-performance nodes in the entire Blockchain-based transaction network, so the transaction can be verified. It is noted the reduction on the difficulties of management in Blockchain transaction and improvements on the efficiency of transaction verification.

C. SECURITY ANALYSIS

The double-spending attack in data transactions will cause issues of data damage and credit consumption. Credit consumption is set to ensure the participation of nodes. In this work, the trust degree of the node reduces over time. As to ensure data security in Blockchain-based transaction, the nodes should participate in the verification of blocks. After that, the trust degree Tru of the node N_i in the federated Blockchain can be calculated as depicted next.

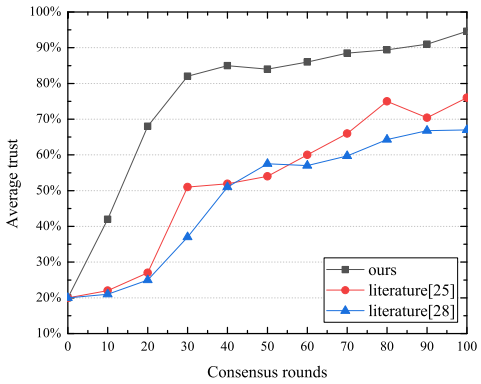

FIGURE 11. Average trust level for different consensus rounds: A comparative summary.

$$Tru_{cur}^{(i)} = \begin{cases} Trust_{last}^{(i)} \times e^{-D\cdot\Delta Inter} \\ e + 0.8 \\ \frac{1}{-\beta[\sum_{j=0}^{m-1}\lambda_x - \theta\times\sum_{j=0}^{m-1}\sigma_x]}, \Delta Inter = 0 \end{cases}. \tag{12}$$

At this point, the interval between the current block and the last generated block is denoted by $\Delta Inter$, as follows.

$$Inter_{cur} - Inter_{pre} = \Delta Inter. \tag{13}$$

This section simulates double-spending attack and compare to algorithms presented in [25] and [28], as shown in Figure 11. With the increase of consensus rounds, the proposed algorithm can maintain a higher level of trust degree than other algorithms. In the homomorphic hash calculation, the consensus mechanisms depend on calculation ability or stake value to maintain network stability and security, which tends to centralization [25], [28]. The security of blocks mainly depends on the organization of nodes in each block and the similarity of organizations. Larger similarity means the aggregated data has lower information loss. When the number of nodes achieves the maximum value, the information loss is minimum and higher than the anonymous degree. Besides, the Blockchain-based homomorphic encryption can protect the data privacy of users and prevent network attacks from malicious nodes. From the experiments, the malicious node that performs a double-spending attack can be rapidly identified by detecting the nodes with such homomorphic encryption. After multiple consensus rounds, the trust degree of nodes in the Blockchain network will attain a high level in the proposed algorithm, yet the centralization problem is avoided. Thereafter, the proposed algorithm has better performance and ability against a double-spending attack than researches presented in [25] and [28].

TABLE 1. The complexity comparison of various algorithms.

Algorithm	*time(ms)*	*Storage space(bit)*	*Time complexity*
Literature [25]	81983*15	256	O(log2n)
Literature [27]	33644*15	128	O(log2n)
Literature [28]	81983*8	256*8	O(n)
The proposed algorithm	33644*8	128*8	O(n)

TABLE 2. Comparison of key strength and traceability of various algorithms.

Algorithm	*Multiple identity*	*Key strength*	*Traceability*
Literature [25]	NO	NO	YES
Literature [27]	YES	YES	NO
Literature [28]	NO	YES	YES
The proposed algorithm	YES	YES	YES

D. COMPLEXITY ANALYSIS

As there is data transmission in an IP transaction, the complexity of transactions should be analyzed. Table 1 lists the comparison result of storage space and time complexity on search. In [25], the time complexity of encryption and decryption in transaction is O(log2n), whilst [28] shows the same time complexity with the proposed algorithm despite it requires a larger storage space. This proposed research does not perform the hash calculation of the tree structure, so thus the time complexity is O(n).

E. TRACEABILITY ANALYSIS

From the analysis above given, the proposed algorithm is suitable for electronic data transactions. In [28], the security of the hash function depends on the attribute of the function itself and resistance against collision due to the structure of the hash function, and the length of the hash value is the main factor to resist collision. As shown in Table 2, both algorithms [25] and [28] can achieve traceability, but [28] has better performance of key strength than that of [25]. In [27], the traceability is not ensured. The proposed algorithm realizes the listed performance since it utilized the homomorphic encryption with many distributed central identities and strengthened key. Besides, the use of Blockchain realizes strong traceability. Together, both make the system achieving higher rates of security.

V. CONCLUDING REMARKS AND FUTURE WORK

In this paper, We propose a Blockchain-based IP copyright protection algorithm that utilizes homomorphic encryption, by changing the traditional decentralized authentication model. First, the homomorphic encryption is utilized to encrypt the IP circuit and the intelligent contract in Blockchain, where the homomorphic encryption-based mathematical model is also established. A transaction protocol for circuit copyright protection is designed by combining distributed Blockchain and intelligent contract, in which it realizes homomorphic computation before the intelligent contract executes. The computation does not leak any copyright information. Besides, real-time identity authentication and extensible data storage are designed to improve security and extensibility. Experimental results show that the proposed scheme has good security and stability, which can be applied for real-time

circuit copyright authentication. As future directions, investigations on the reliable storage technology for private data in the blockchain-based network will be tackled, due to the secure storage and consistency of data cooperation in high-frequent data transactions.

ACKNOWLEDGMENTS

This work was supported in part by the National Natural Science Foundation of China under Grant 61572188 and Grant 61976087, in part by the Scientific Research Program of the New Century Excellent Talents in Fujian Province University, in part by the Fujian Provincial Natural Science Foundation of China under Grant 2018J01570, and in part by the Hunan Provincial Science and Technology Project Foundation under Grant 2018TP1018.

REFERENCES

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congress Big Data*, 2017, pp. 557–564.

[2] G. Zyskind and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security Privacy Workshops*, 2015, pp. 180–184.

[3] X. Li *et al.*, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, 2020.

[4] Z. Zheng *et al.*,"Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Serv.*, vol. 14, pp. 352–375, 2018.

[5] W. Liang, Y. Fan, K. Li, D. Zhang, and J. Gaudiot, "Secure data storage and recovery in industrial blockchain network environments," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2020.2966069.

[6] J. L. Caton, "Cryptoliquidity: The blockchain and monetary stability," *J. Entrepreneurship Public Policy*, to be published, doi: 10.1108/JEPP-03-2019-0011.

[7] Z. Zheng *et al.*, "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, 2020.

[8] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, and L. Xie, "A decentralized solution for IoT data trusted exchange based-on blockchain," in *Proc. 3rd IEEE Int. Conf. Comput. Commun.*, 2017, pp. 1180–1184.

[9] A. Savelyev, "Copyright in the blockchain era: Promises and challenges," *Comput. Law Secur. Rev.*, vol. 34, pp. 550–561, 2018.

[10] S. Qi, Y. Zheng, M. Li, L. Lu, and Y. Liu, "Secure and private RFID-enabled third-party supply chain systems," *IEEE Trans. Comput.*, vol. 65, no. 11, pp. 3413–3426, Nov. 2016.

[11] W. Liang, W. Huang, J. Long, K. Zhang, K. Li, and D. Zhang, "Deep reinforcement learning for resource protection and real-time detection in IoT environment," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2020.2974281.

[12] K.-C. Li, X. Chen, H. Jiang, and E. Bertino, *Essentials of Blockchain Technology*. Boca Raton, FL, USA: /New York, NY, USA: CRC Press/Taylor & Francis, 2019.

[13] H. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[14] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, and K.-C. Li, "A secure FaBric blockchain-based data transmission technique for industrial Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3582–3592, Jun. 2019.

[15] K. Zhang, S. Leng, X. Peng, L. Pan, S. Maharjan, and Y. Zhang, "Artificial intelligence inspired transmission scheduling in cognitive vehicular communications and networks," *IEEE Internet Things*, vol. 6, no. 2, pp. 1987–1997, Apr. 2019.

[16] W. Liang, K.-C. Li, J. Long, X. Kui, and A. Y. Zomaya, "An industrial network intrusion detection algorithm based on multi-characteristic data clustering optimization model," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2063–2071, Mar. 2020. doi: 10.1109/TII.2019.2946791.

[17] K. Zhang, Y. Zhu, S. Maharjan, and Y. Zhang, "Edge intelligence and blockchain empowered 5G beyond for industrial Internet of Things," *IEEE Netw. Mag.*, vol. 33, no. 5, pp. 12–19, Sep./Oct. 2019.

[18] K. Zhang, Y. Zhu, S. Leng, Y. He, S. Maharjan, and Y. Zhang, "Deep learning empowered task offloading for mobile edge computing in urban informatics," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7635–7647, Oct. 2019.

[19] Y. Zhang, G. Cui, S. Deng, F. Chen, Y. Wang, and Q. He, "Efficient query of quality correlation for service composition," *IEEE Trans. Services Comput.*, to be published, doi: 10.1109/TSC.018.2830773.

[20] Y. Zhang, C. Yin, Q. Wu, Q. He, and H. Zhu, "Location-aware deep collaborative filtering for service recommendation," *IEEE Trans. Syst., Man, Cybern. Syst.*, to be published, doi: 10.1109/TSMC.2019.2931723.

[21] J. Long, W. Liang, K.-C. Li, D. Zhang, M. Tang, and H. Luo, "PUF-based anonymous authentication scheme for hardware devices and IPS in edge computing environment," *IEEE Access*, vol. 7, no. 1, pp. 124 785–124 796, 2019.

[22] T. I. Kiviat, "Beyond bitcoin: Issues in regulating blockchain tranactions," *Duke L.J.*, vol. 65, 2015, Art. no. 569.

[23] S. Davidson, P. De Filippi, and J. Potts , "Economics of blockchain," 2016. [Online]. Available: https://ssrn.com/abstract=2744751

[24] L. Cocco, A. Pinna, and M. Marchesi, "Banking on blockchain: Costs savings thanks to the blockchain technology," *Future Internet*, vol. 9, 2017, Art. no. 25.

[25] M. N. Islam, V. C. Patii, and S. Kundu, "On IC traceability via blockchain," in *Proc. Int. Symp. VLSI Des. Autom. Test*, 2018, pp. 1–4.

[26] A. Beikverdi and J. S. Song, "Trend of centralization in bitcoin's distributed network," in *Proc. IEEE/ACIS 16th Int. Conf. Softw. Eng. Artif. Intell. Netw. Parallel/Distrib. Comput.*, 2015, pp. 1–6.

[27] F. Idelberger *et al.*, "Evaluation of logic-based smart contracts for blockchain systems," in *Proc. Int. Symp. Rules Rule Markup Lang. Semantic Web*, 2016, pp. 167–183.

[28] Q. Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability," *IEEE Softw.*, vol. 34, no. 6, pp. 21–27, Nov./Dec. 2017.

[29] A. Savelyev, "Copyright in the blockchain era: Promises and challenges," *Comput. Law Secur. Rev.*, vol. 34, pp. 550–561, 2018.

[30] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," *SIAM J. Comput.*, vol. 43, pp. 831–871, 2014.

[31] H. T. Wu, Y. Cheung, and J. Huang, "Reversible data hiding in paillier cryptosystem," *J. Vis. Commun. Image Representation*, vol. 40, pp. 765–771, 2016.

WEI LIANG (Member, IEEE) received the PhD degree from Hunan University, China, in 2013 and was a postdoctoral scholar at Lehigh University, Bethlehem, Pennsylvania, during 2014–2016. He is currently an associate professor with the College of Computer Science and Electronic Engineering, Hunan University, China. He served as application track chair of IEEE Trustcom 2015, a workshop chair of IEEE Trustcom WSN 2015 and IEEE Trustcom WSN 2016. He has published more than 110 journal/conference papers such as the *IEEE Transactions on Industrial Informatics*, *IEEE Transactions on Emerging Topics in Computing*, *IEEE Transactions on Computational Biology and Bioinformatics*, and *IEEE Internet of Things Journal*. His research interests include blockchain security technology, networks security protection, embedded system and hardware IP protection, fog computing, and security management in WSN.

DAFANG ZHANG received the PhD degree in applied mathematics from Hunan University, China, in 1997. He is a professor with the College of Computer Science and Electronic Engineering, Hunan University, China. He was a visiting fellow at Regina University, Canada during 2002–2003, and senior visiting fellow at Michigan State University, East Lansing, Michigan, in 2013. He has published more than 230 journal/conference papers and PI for more than 30 large scale scientific projects. His research interests include dependable systems/networks, network security, network measurement, hardware security, and IP protection.

XIA LEI received the BS degree in mathematics and applied mathematics from Jimei University, China, in 2012, and the MS degree in basic mathematics from Fuzhou University, China, in 2015. She is currently working toward the PhD degree in computer science and technology at the China University of Petroleum, Beijing, China. Her current research interests include theories of blockchain, software security, and explainable AI.

MINGDONG TANG (Member, IEEE) received the BS degree in electrical engineering from Tianjin University, China, in 2000, the MS degree in control engineering from Shanghai University, Shanghai, China, in 2003, and the PhD degree in computer science from the Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China, in 2010. He is currently a professor with the School of Information Science and Technology, Guangdong University of Foreign Studies, China. He has published more than 100 peer-reviewed scientific research papers in various journals and conferences. His research interests include service computing, blockchain, privacy, and trust. He is a member of the China Computer Federation and ACM.

KUAN-CHING LI (Senior Member, IEEE) is currently a distinguished professor at Providence University, Taiwan, where he also serves as the director of the High Performance Computing and Networking Lab. He is a recipient of awards and funding support from several agencies and industrial companies, as he also received distinguished chair professorships from universities in several countries. He is the editor-in-chief of the Connection Science (Taylor & Francis), and serves as associate editor, editorial board member and guest editor for several leading journals. He published more than 250 scientific papers and articles and is co-author or co-editor of more than 20 books published by Taylor & Francis, Springer, and McGraw-Hill. His research interests include parallel and distributed computing, big data, and emerging technologies. He is a fellow of the IET.

ALBERT Y. ZOMAYA (Fellow, IEEE) is the chair professor of High Performance Computing and Networking in the School of Information Technologies, University of Sydney, Australia, and he also serves as the director of the Centre for Distributed and High Performance Computing. He published more than 550 scientific papers and articles and is author, co-author or editor of more than 20 books. He is the founding editor in chief of the *IEEE Transactions on Sustainable Computing* and serves as an associate editor for more than 20 leading journals. He served as an editor in chief for the *IEEE Transactions on Computers* (2011–2014). He is the recipient of the IEEE Technical Committee on Parallel Processing Outstanding Service Award (2011), the IEEE Technical Committee on Scalable Computing Medal for Excellence in Scalable Computing (2011), and the IEEE Computer Society Technical Achievement Award (2014), and the ACM MSWIM Reginald A. Fessenden Award (2017). He is a chartered engineer, a fellow of AAAS and IET. His research interests are in the areas of parallel and distributed computing and complex systems.