



An End-to-End Bidirectional Authentication System for Pallet Pooling Management Through Blockchain Internet of Things (BloT)

Wen Long, Hunan Modern Logistics College, China

C. H. Wu, The Hang Seng University of Hong Kong, Hong Kong

 <https://orcid.org/0000-0003-1259-4048>

Y. P. Tsang, The Hong Kong Polytechnic University, Hong Kong

 <https://orcid.org/0000-0002-6128-345X>

Qiyang Chen, Montclair State University, USA

ABSTRACT

Pallet pooling is regarded as a sustainable and cost-effective measure for the industry, but it is challenging to advocate due to weak data and pallet authentication. In order to establish trust between end-users and pallet pooling services, the authors propose an end-to-end, bidirectional authentication system for transmitted data and pallets based on blockchain and internet-of-things (IoT) technologies. In addition, secure data authentication fosters the pallet authenticity in the whole supply chain network, which is achieved by considering the tag, location, and object-specific features. To evaluate the object-specific features, the scale invariant feature transform (SIFT) approach is adopted to match key-points and descriptors between two pallet images. According to the case study, it is found that the proposed system provides a low bandwidth blocking rate and a high probability of restoring complete data payloads. Consequently, positive influences on end-user satisfaction, quality of service, operational errors, and pallet traceability are achieved through the deployment of the proposed system.

KEYWORDS

Authentication, Blockchain, Computer Vision, Internet of Things, Pallet Pooling

1. INTRODUCTION

In contemporary logistics and supply chain management, pallet pooling is a novel pallet management strategy to facilitate sustainability, cost-effectiveness, and better pallet quality. Extended from the concept of vendor-managed inventory (VMI) and sharing economy, the pallet pooling strategy is developed to manage the stock and quality of pallets on behalf of the pallet users. In contrast, the pallet pooling service providers (PPSP) are responsible for disseminating, collecting, and repairing the pallets to minimise the logistics operations' industrial wastes. End users in pallet pooling, including supply chain parties and logistics service providers, can order pallets from a shared pool managed

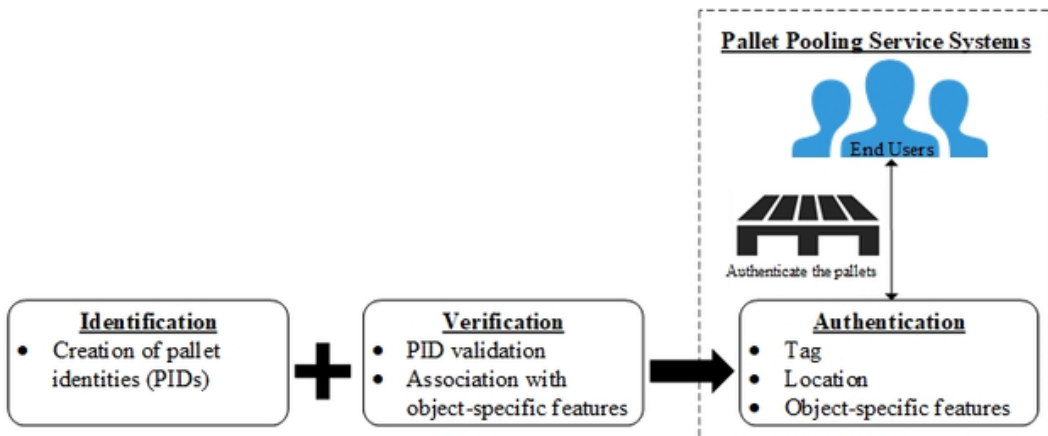
DOI: 10.4018/JOEUC.290349

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

by the pallet pooling company, where the pallets are in good condition, and arrive at the nominated facility just-in-time. In addition, the reverse logistics on pallets throughout the supply chain can be effectively managed to support the reuse and recycling of pallets and reduce corresponding industrial waste. Apart from merely ensuring the pallets are in good condition, some customs regulations, such as pest control, should be fulfilled, in which the pallets are required to be wholly heat-treated or fumigated. Since managing a bulk of pallets by the end-users effectively and sustainably is relatively complicated, the development of pallet pooling in the logistics network has become significant nowadays. Ultimately, the pallet users can get rid of managing the pallets by themselves, and resources on the pallet management can be released to the core business activities of the end-users. Although pallet pooling is regarded as a promising strategy in modern supply chains, effective identification, verification, and authentication of pallets are still under-exploration such that the trustworthiness from the end-users to pallet pooling is questionable. Due to the lack of a secure authentication protocol to manage pallet pools, the trust between end-users and pallet pooling system is difficult to establish, and the problems of fraudulent pallets and malicious nodes in the network are difficult to prevent. The effective implementation of the pallet pooling strategy should be built on secure and reliable data exchange and pallet authentication to eliminate the challenges above and system vulnerability. On the one hand, the access control of the IoT devices representing the pallets should be established to avoid the communication of unauthorised IoT nodes in the blockchain-based system. On the other hand, the pallet authenticity should be guaranteed to circulate the pallets through the identification and verification process between end-users. Consequently, pallet pooling companies are urged to formulate a secure pallet authentication system to create a trustworthy end-user ecosystem.

A typical authentication process using Internet of Things (IoT) requires that objects, including users and products, be identified and verified. As shown in Figure 1, the identification clarifies the identity (ID) information of objects accessed by other users. The verification builds the association between ID and product-specific features to avoid false and fake authentication. The identification and verification information is maintained for the authentication process, which refers to the validation of tag-based and location-based data and the product-specific features. For instance, end-users under the pallet pooling service systems should be able to authenticate their on-hand pallets based on the above identification and verification information. Therefore the pallet quality and specifications are ensured.

Figure 1. Relationship between product identification, verification, and authentication



In view of the contemporary end-user computing environment, the number of enterprise-grade IoT terminals is increasing, and the security policies of enterprise systems can vary and be dependent on the business models and customer requirements. Therefore, object identity information is found in diversified forms, subject to business relationship and user experience (Wu, 2019; Xia et al., 2019). The most critical component of the IoT information processing approach is the host terminal to facilitate information transmission between smart sensors and devices. Under the IoT paradigm, the interconnectivity between physical objects, edge computing, and computing is structured to develop smart applications (Tsang et al., 2021; Wan and Chin, 2021). Apart from the smart system design and development, the requirements for information security and privacy are high, including anti-counterfeiting and system reliability, in order to prevent the collapse of IoT systems and eliminate the system vulnerability. Thus, building an effective authentication protocol for IoT terminal identity information has become the key issue of current research (Trnka et al., 2018; Liang et al., 2019; Chien et al., 2020; Shuai et al., 2021). With the increasing number of terminals, wireless communication networks are facing great pressure on system security and privacy. Since the number of terminals is huge, the security of the equipment itself cannot be comprehensively guaranteed (Beltrán, 2018). Malicious software and programs can attack the IoT systems to obtain and gain access to identity information, resulting in a significant impact on network security. Therefore, an IoT authentication method should be built to ensure the information security of network users, while the effect from malicious attacks can be minimised (Nandy et al., 2019; Dabbagh and Saad, 2019). Although large-scale and interconnected IoT systems bring much convenience to end-users, it also brings many security and privacy risks on the systems. Trusted identity authentication of IoT devices and users is the foundation of solving the related security problems. However, the existing security authentication technology relies on a trusted third party, which incur a high cost for the authentication process, and causes single-point failure and internal tampering attacks (Gill and Shaghghi, 2020).

Due to the emergence of blockchain technology, a new mechanism to solve the aforementioned challenges on network security and product authentication found in existing IoT paradigms can be explored. A safe and reliable authentication protocol is necessary to realise the interconnection of all physical objects in the ubiquitous IoT systems. Since storing a vast amount of data in blockchain may influence the efficiency of the block mining/forging process and corresponding energy consumption, the integration of blockchain and IoT is deemed the promising way to build an effective data and product authentication system. A hybrid approach to interconnect IoT devices, cloud computing, and blockchain is considered for the paradigm shift to blockchain-IoT, in which only the essential data for data and product authentication are recorded in the distributed database under the blockchain technology to synchronise with the nodes and clients in the peer-to-peer network. Other supplementary data collected by IoT devices can be stored in the cloud environment and interacted with the blockchain in real-time. Therefore, the advantages of blockchain and IoT can be revealed and leveraged under the blockchain-IoT paradigm. This study introduces blockchain technology into ubiquitous IoT systems to construct an end-to-end and two-way authentication system for pallet pooling management. The risk of data leakage can be reduced through the decentralised system architecture. From the end-users' perspectives, a high degree of network security and privacy to transmit sensitive business data can be maintained, while pallets offered by the pallet pooling companies can be authenticated. Subsequently, the trust between end-users and pallet pooling service systems can be effectively established to boost the sustainable development of logistics and supply chain management.

The rest of this paper is organised as follows. Section 2 synthesises the state-of-the-art literature from blockchain, IoT technologies, product authentication process, and network security strategies. Section 3 describes the architecture of the proposed authentication system for pallet pooling management. In Section 4, a case study is conducted to assess the feasibility and performance of the proposed system. Section 5 discusses the insights on end-user computing toward ubiquitous pallet pooling service systems, and the conclusion of the study is made in Section 6.

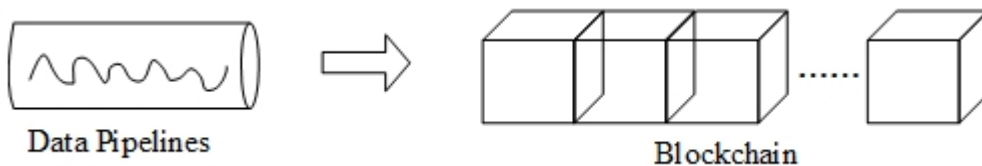
2. MATERIALS AND METHODS

In this section, the literature related to emerging technologies on blockchain and IoT, product authentication approaches, and network security strategies for authentication are reviewed to illustrate the values and motivation of this study.

2.1 Blockchain and Internet of Things

Compared with the previous identity authentication processes used in the IoT, the introduction of blockchain can, to a greater extent, ensure a centralised state of information control, reach a network consensus, and ensure that each user's information is authenticated using cryptography to prevent any leakage of users' private information (Durairaj and Muthuramalingam, 2018; Li et al., 2018; Fachrunnisa and Hussain, 2020). Therefore, the paradigm of blockchain-IoT (BIoT) is now being advocated to boost industrial blockchain development for securely managing IoT data through fully integrating blockchain and IoT technologies (Tsang et al., 2021). Particularly, the service-oriented architecture for IoT was further enhanced to incorporate distributed databases, consensus algorithms, and smart contracts, while novel network security strategies were formulated to provide effective data and product authentication (Yi, 2019). The above BIoT functions are accomplished by restructuring the data managed in the IoT terminal from the data pipelines to a chain of blocked data, as shown in Figure 2.

Figure 2. Transformation from data pipelines to blockchain

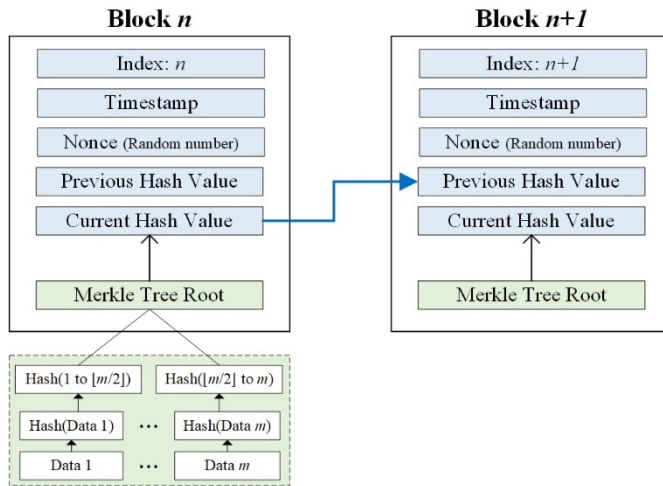


After all the private data are blocked, the data that appear on the blockchain surface are only a small portion of the complete data, while the rest of the data are managed in cloud or edge computing in a hybrid manner (Zheng and Lu, 2021). Under the blockchain framework, the data are segmented into various blocks with the corresponding timestamp. The hash algorithm, such as the secure hash algorithm (SHA), is used for asymmetric encryption, and the consistency and integrity of the data are ensured through the chain structure, solving the Byzantine Generals problem. The data structure following the blockchain paradigm facilitates data tracking and traceability (Li and Wang, 2019; Fang et al., 2020). Ho et al. (2021) showed the power of blockchain technology in access control and product traceability to facilitate inventory control and predictive maintenance. The business operations can be automated through the customisation of smart contracts. Therefore, a secure and reliable data sharing mechanism is established using blockchain. Even if the blockchain-based systems are attacked, it is difficult to tamper with the data blocks and hack the complete data chain. Once a part of the data in the data blocks is changed, the corresponding hash values are changed to break the association between data blocks. The entire blockchain cannot be validated unless malicious nodes tamper and recalculate all the target hash values. Therefore, the blockchain creates a technological improvement for privacy protection and system security.

On the other hand, nodes in the blockchain network, without trust, reach an agreement on the continuously generated blocks by following the specific consensus mechanism, and finally, add new blocks to the end of the chain to complete the blockchain (Norta et al., 2019; Tsang et al., 2019).

The nodes jointly maintain the account book, the so-called distributed ledger, and the whole account book is traceable and tamper-proof, as shown in Figure 3. As there are still problems in data privacy and security in the current IoT paradigm, research on a combination of blockchain technology and IoT is active in building a holistic information security management system (Xu et al., 2021). The public identity information of devices and users are stored in the blockchain, and the users' key private information is effectively protected to prevent information leakage and tampering (Zheng et al., 2019). Using the BIoT paradigm, the secure authentication process of the IoT can be effectively established to protect the product authentication process.

Figure 3. Structure of the blockchain with Merkle tree



The blockchain technology enables a secure and immutable chain of data blocks, effectively decentralised in the peer-to-peer network, compared with the above IoT-based authentication systems. These functionalities can enhance the data management for the authentication process, while each client node has a copy of the authentication record to secure the accuracy of the verification process. In addition, the inclusion of new identification and verification data is required to pass through the customised consensus algorithm, resulting in the mutually agreed authentication process. Therefore, with the aid of blockchain, the trustworthiness of the authentication process can be further improved. The BIoT-based data and product authentication should be explored and exploited in this study.

2.2 Network Security Strategies For Data Authentication

Based on the foundation of BIoT technologies, secure authentication for data transmission between IoT devices can be built to eliminate the system vulnerability (Chen et al., 2019; Wang et al., 2020; Gupta and Narayan, 2021). Zhou et al. (2018) proposed an identity authentication scheme for IoT terminal devices based on an identity-based encryption (IBE) strategy. The strategy realises anonymous mutual authentication between terminal devices and uses an elliptic curve encryption algorithm to ensure the security of information transmission in the authentication process. The security theory and performance analysis showed that the scheme can resist well-known attacks such as a replay attack, a man-in-the-middle attack, and a tamper attack and has a low computational cost. Based on the above IBE strategy, Yan et al. (2019) further explored the access control scheme to prevent over-privileged access behaviour in IoT systems, where the access of unauthorised functions can be avoided. Therefore, the impact on system privacy and security can be reduced, even when there are

many malicious nodes in the IoT network. Furthermore, Liang et al. (2019) proposed an identity authentication protocol for radio frequency identification (RFID) based on the two-stage multiple-choice-arbiter physical unclonable function. The scheme can authenticate the identity of both sides of the communication sensing node. The encryption and decryption need less key information, and there is no key agreement problem. The cluster head node can authenticate the sensing nodes in the same group in the batch to solve the authentication delay and energy consumption problems. Any suspicious nodes can be traced based on the binary search technology to quickly locate the suspicious nodes and identify the untrusted nodes before they can cause damage. Security analysis shows that the mechanism is correct, anonymous, resists known forms of attack, and can effectively prevent malicious nodes from stealing and tampering with the sensing data. Through the experimental studies, the advantages of the bi-directional authentication protocol, namely randomness, stability, and resilience, have been proven in low-cost hardware.

2.3 Product Authentication Approaches

The above network security strategies ensure reliable access control and data authentication to IoT systems, which can be further applied industrial applications to bring positive influence to the product authentication mechanism. Starting from RFID technologies, Lehtonen et al. (2007) elaborated the essential elements in product authentication systems, including tag authentication, location-based authentication, and object-specific features. In addition, seven possibilities on attacking the product authentication were outlined, namely tag cloning, tag removal and reapplying, attack against internal information technology system, manipulation of testing equipment, attack against radio frequency communication, forgery of product history, and manipulation of product history. Due to the presence of blockchain technology in the IoT paradigm, product provenance and authentication can be further strengthened to establish permanent records to help certify products in the market (Choi, 2019; Choi and Ouyang, 2021). Such blockchain-based product provenance and authentication (BPPA) platforms fully leverage the advantages of blockchain technology to build robust product tracking and traceability. However, research on exploring the interaction between blockchain and IoT technologies from data authentication to product authentication is limited, so it is meaningful to create a trustworthy chain of data blocks for specific products in the supply chain perspective.

Overall speaking, this paper proposes an end-to-end and two-way identity security authentication mechanism based on blockchain and IoT technology for data and product authentication. Particular to pallet pooling management, which is the focus of this study, the authentication of users' data and pallets plays an essential role to drive the platform success in order to establish not only security, but also trust, in the pallet pooling network.

3. DESIGN OF AN END-TO-END BIDIRECTIONAL AUTHENTICATION SYSTEM FOR PALLET POOLING

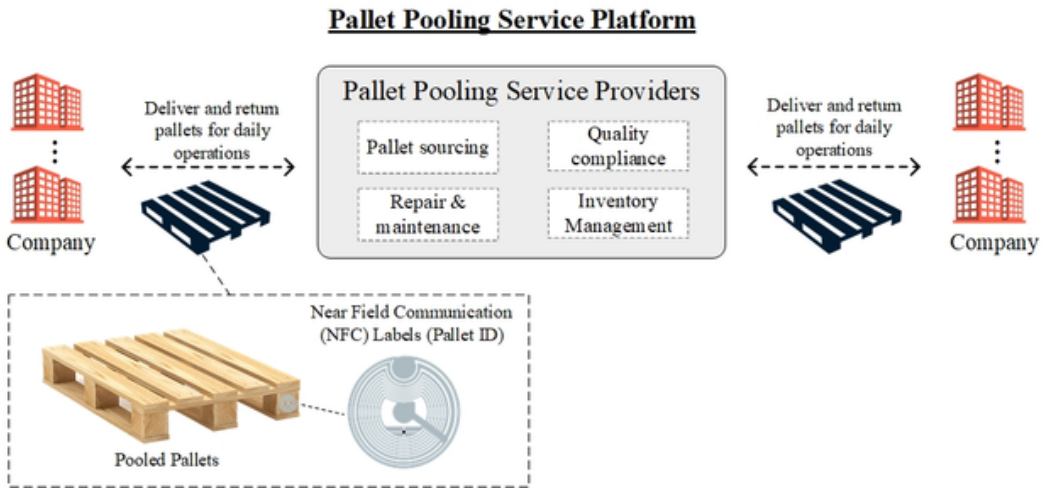
In this section, an end-to-end bidirectional authentication system for pallet pooling is proposed to utilise the values of blockchain and IoT so as to strengthen the trust and security in pallet pooling services. Based on the pallet pooling service platform, two additional sub-tiers in the system, namely (i) data authentication for BIoT and (ii) hybrid pallet authentication, are proposed to ensure the reliability, effectiveness, and security of data transmitted between IoT devices. Subsequently, the collected data from BIoT technologies support pallet authentication throughout the supply chain activities.

3.1 Pallet Pooling Service Platform

To effectively manage a pallet between service providers and end-users, the pallet pooling service platform plays an important role on pallet sourcing, quality compliance, inventory management, and repair and maintenance. In addition, the pallet pooling service providers are also responsible for allocating and collecting the pallets for the end-users, such as logistics companies and other supply

chain parties, to support their daily operations. Damaged and obsolete pallets are then shipped back to the service providers for repair and disposal. In other words, both forward and reverse logistics for the distribution and return of pallets are managed by the service providers via the pallet pooling service platform. The pallet transaction and quality compliance are consolidated in the platform, where the movement of pallets in the supply chain network can be captured. As shown in Figure 4, the pallet movements between service providers and end-users are graphically illustrated, in which the near field communication (NFC) labels are utilised to identify pallets in the pool. Pallet identities (IDs) are created for all pallets associated with specific transactions and object-specific features to assist the pallet authentication process. Although the pallet pooling strategy has been developed and advocated in recent years, certain resistance is still presented in the supply chain network to hinder the pallet pooling deployment. Firstly, the system vulnerability and reliability are questionable to the end-users. Since the movement of pallets implies a business network and activities between end-users, privacy-preserving and cost-effective security and protection are required to encrypt the data transmission process. Secondly, end-users are concerned whether the received pallets strictly follow quality compliance, and whether the pallets are the same as they ordered in the platform. Pallet quality refers to the pallet conditions and the extent of damage and customs regulations, such as pest control treatments, which may affect the import and export operations of cross-border logistics.

Figure 4. Graphical illustration of pallet pooling service platforms



3.2 Tier 1: Data Authentication For BioT

For identity security authentication, the registration process of the gateway node can be omitted, and the user operation is simplified. The blockchain network node can be represented by the users and the gateway nodes which can authenticate each other. Sensors in the blockchain network have public client information, and the user obtains the information based on the client and verifies its legitimacy (Wan et al., 2018; Fan et al., 2019). The authentication process is safe and efficient in the distributed IoT environment, providing a more secure network environment for wireless sensor network users. When the blockchain function $\varphi^{(1)}(t)$ is taken as the first derivative of the smooth function $\theta(t)$,

$\varphi^{(1)}(t)$ satisfies the block admissibility condition, then the block change of the function $f(t)$ at scale α and coordinate t is formulated as in Equation (1).

$$W_\alpha f(t) = f * \varphi_a^{(1)}(t) = f * \left(a \frac{d\theta}{dt} \right) (t) = a \frac{d}{dt} (f * \theta_a)(t) \quad (1)$$

Since $(f * \theta_a)(t)$ can be described as the result of the smoothing function $f(t)$ at scale α by the low pass smoothing function $\theta(t)$, blockchain transformation $W_\alpha f(t)$ is caused by the first order of data signal in scale α after smoothing, so the local maximum of the modulus $|W_\alpha f(t)|$ corresponds to the inflection point of the smoothed signal $(f * \theta_a)(t)$. If t is in the interval $[t_1, t_2]$, then the block transformation of the function $f(t)$ satisfies:

$$|W_\alpha f(t)| \leq ka^\alpha \quad (2)$$

, where k is a constant, and the Lipchitz exponents of $f(t)$ in the interval $[t_1, t_2]$ are α . As a binary block transformation, $a = 2^j$, and Equation (2) becomes the below Equation (3):

$$|W_{w^j} f(t)| \leq k(2)^{j\alpha} \quad (3)$$

It can be seen that the modulus maxima of the block transformation and α in different scales are as follows: at $\alpha > 0$, the modulus maxima of the block change will increase with the increase of scale j ; at $\alpha < 0$, the modulus maxima of block transformation will decrease with the increase of scale j ; at $\alpha = 0$, the modulus maxima of block change will not change with the change of scale. Therefore, the modulus maxima of the data signal will also increase with the block transformation scale. The maximum modulus value of the data will decrease with the increase of the scale [19–20]. When selecting the appropriate scale, the block changes based on large-scale IoT data, the corresponding security interval of modulus maximum is closed, and the safety period is detected. Suppose the value of attribute B is used to replace the segmentation between initial samples. In that case, the training data D can be regarded as the initial information quantity, and its corresponding characteristic attribute B will contain m outputs and m partition information. Attribute A contains n different values $\{a_1, a_2, \dots, a_n\}$. If the sample set B is divided into S subsets with $\{S_1, S_2, \dots, S_n\}$ subsets by using the feature attribute n , the information gain rate of S is divided by characteristic attribute B as in Equations (4) and (5):

$$GainRatio = \frac{Gain(B)}{SplitInfo(B)} \quad (4)$$

Among them,

$$SplitInfo(B) = -\sum_{j=1}^n B_j \log_2 B_j \quad (5)$$

In the above Equations (4) and (5), $Gain(B)$ is the information gain and $SplitInfo(B)$ is the total information. The best feature attribute subset can generate a good effect on segmentation prediction. The correlation between feature attributes and class attributes is large, and the redundancy between feature attributes is small. Considering the relationship between feature attributes and class attributes, the higher the degree of the relationship between feature attributes, the more redundancy the feature attributes have, and the more effective the subset of feature attributes is.

$$Gain(B_F) = r(i, j) \sum_{f \in F} H(B) - H(B|f) \quad (6)$$

In Equation (6), $Gain(B_F)$ represents the incremental sum of information of other attributes relative to attribute B , proving the correlation degree between feature attribute B and other attributes. F contains the total of class attributes without characteristic attribute B , f represents non-class attributes and $f \in F$. The following formula represents the average information gain of other attributes to the characteristic attribute B :

$$\overline{Gain(B_F)} = \frac{\sum_{f \in F} (H(B) - H(B|f))}{n} \quad (7)$$

On the basis of the current information gain rate, other attributes are introduced to calculate the average information gain of selected feature attributes to shorten the redundant values of other attributes and preselected attributes. After improvement, the increasing rate of information is as follows:

$$GainRatio = \frac{Gain(B)}{SplitInfo(B) + \omega \overline{Gain(B_F)}} \quad (8)$$

, where ω is the weight coefficient. In the improved calculation of the increasing data rate, if the relationship between other attributes and attribute B is quite small, the equilibrium value of other attributes for increasing the information of feature attribute B will decrease. The specific steps of security authentication are as follows:

- a) The specific method is to generate a random number N_r and send $K_{sys} \oplus N_r$ to the label device.
- b) In the process of authentication, the system has K_{sys} tags, N_r can be obtained by XOR operation, and identity information can be transmitted to the server through the label device to obtain server authentication. The tag device generates a random number of N_{d1} , calculates $K_{sys} \oplus TID$, $K_d \oplus N_{d1}$ and $TID \oplus N_r$ respectively, forms the cascaded information and transmits it to the reader (Huang et al., 2018; Liang et al., 2019; Song et al., 2020).
- c) After receiving the message, the server authenticates the reader and tag. First, the server queries whether a device with a dynamic index ID of RID (recognition ID) exists. If it exists, the system key K_{sys} corresponding to RID is used to solve TID (tracking ID) and N_r . Then the server queries whether a device with a dynamic index ID of TID exists. If it exists, the random number N_{d1} generated by the label device is solved using the device key K_d corresponding to the device.

Finally, the server can recalculate $Rot\left[Rot\left(RID + N_r \oplus K_r, K_{sys} + K_d \oplus N_{d1}\right), TID \oplus N_r\right]$ from known messages. If the value obtained is equal to M1, the reader and tag are authenticated by the server.

3.3 Tier 2: Hybrid Pallet Authentication

Provided that a secure data authentication process is built in the pallet pooling service platforms, the pallet authentication mechanism can therefore be formulated by using a tag, location, and object-specific features. Tag-based, location-based, and object-specific authentication are the typical approaches to verify physical objects. To be specific, tag-based authentication refers to the attachment of a tag, such as radio frequency identification (RFID) and barcode, on the object to assign a unique identifier used to verify the item's identity. Location-based authentication denotes object locations collected by the global positioning system or other location-based services to verify the object identity. If the objects (or communication from IoT devices) show up in unexpected regions and locations, the objects can be deemed to be fraudulent. Apart from the tag-based and location-based authentication, the object-specific features can also verify the product authenticity. The object features can be collected by using computer vision and image processing techniques. The collected object-specific features can be used for the verification of the objects along the supply chain. The BIoT-based authentication can be established to support the pallet pooling operations with the identification and verification. Since pallets are tagged with the NFC labels, which provide unique PIDs, such labels can be used to authenticate the pallets, while the details of pallets can be read by using NFC-enabled smart handheld devices. End-users can conveniently confirm the correctness of the pallet types, quality, and quantity. However, it is arguable that merely relying on tag-based authentication is ineffective because fraudulent labels could be made on other anonymous pallets. Subsequently, the location information and object-specific features are included to enrich the pallet authentication mechanism. Since the pallet transaction and ownership transfer are recorded in the service platform, the pallet locations should be fixed in either end-users' storage or transportation facilities. If any abnormalities of pallet location are observed, the particular pallets might be fraudulent and should be excluded from the pallet pool. Furthermore, the pallet-specific features can be captured and analysed to differentiate the real and fake pallets. For every pallet in the specific pool, high-resolution images of pallets taken by the pallet pooling service providers are set as the baseline, which is used to compare with the images taken by the end-users at their facilities. Since the images may be captured with different orientations and backgrounds, the scale-invariant feature transform (SIFT) approach is adopted in this study to perform image feature matching.

To achieve the key-point matching between two images by using SIFT approach, four major components, namely (i) scale-space peak selection, (ii) key-point localisation, (iii) orientation assignment, and (iv) key-point descriptor (Cruz-Mota et al., 2012). In the beginning, a scale-space representing meaningful content on digital images is investigated. The scale-space of an image is modelled as $L(x, y, \sigma)$ built from the convolution of a Gaussian kernel (i.e. blurring) at different scales. Particularly, the scale-space is separated into some octaves subject to the size of the original image and the scales. Mathematically, the Gaussian blur operator, namely $G(x, y, \sigma)$, is formulated, where x and y denote the location coordinates, and σ is the scaling parameter for the level of blur, as in Equation (9). By combining with the image $I(x, y)$, the scale-space of the image can be formulated, as in Equation (10).

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-\frac{(x^2+y^2)}{2\sigma^2}} \quad (9)$$

$$L(x, y, \sigma) = G(x, y, \sigma) \times I(x, y) \quad (10)$$

Afterwards, the difference of Gaussians (DoG) is applied to generate another set of images. Two different scaling parameters σ and $k\sigma$ are considered to locate interesting key-points in the set of images following the heat diffusion equation in Equation (11). Therefore, the DoG can be calculated accordingly in the scale-space to evaluate the Laplacian of Gaussian approximations scale-invariant. If the pixel is a local extremum compared with its neighbours in the previous, current, and next scales, it is a potential key-point to represent the scale.

$$G(x, y, k\sigma) - G(x, y, \sigma) \approx (k - 1)\sigma^2 \nabla^2 G, \text{ where } \frac{\partial G}{\partial \sigma} = \sigma \nabla^2 G \quad (11)$$

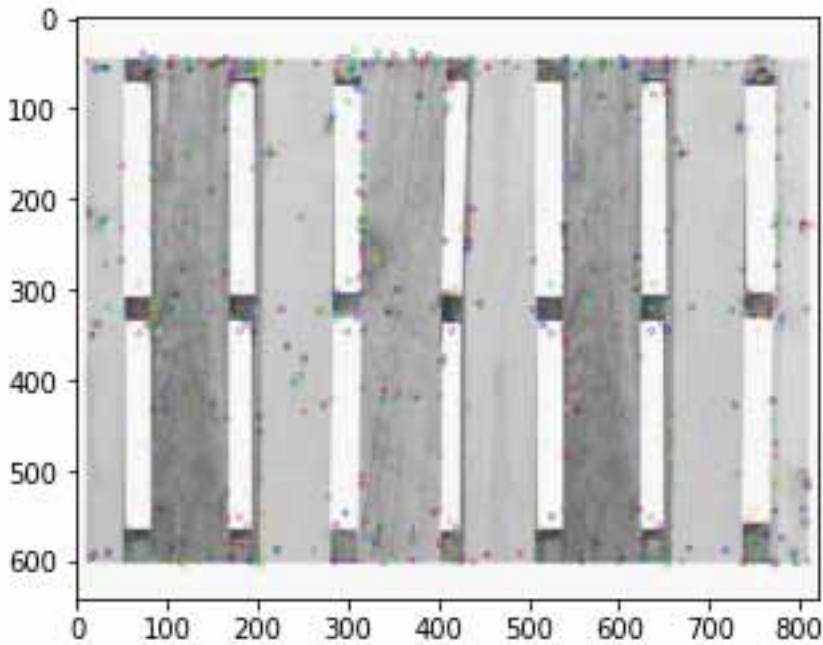
Since many key-points are generated in the above process, the key-point localisation is developed to remove edge features and check the intensities for the low contrast features. For the flats, the intensity at the extremum is set at the threshold, and therefore the flats are rejected when the intensity is less than the expected threshold value as the low contrast point. For the edges, the Hessian matrix is built to evaluate the principal curvature, as in Equation (12) to derive that $\text{Tr}(\mathbf{H}) = D_{xx} + D_{yy} = \lambda_1 + \lambda_2$ and $\text{Det}(\mathbf{H}) = D_{xx}D_{yy} - (D_{xy})^2 = \lambda_1\lambda_2$, where the ratio of the eigenvalues λ_1 and λ_2 are related to the principal curvatures. By comparing the threshold ratio r , the high ratio points are rejected, subject to the condition stated in Equation (13).

$$\mathbf{H} = \begin{bmatrix} D_{xx} & D_{xy} \\ D_{xy} & D_{yy} \end{bmatrix} \quad (12)$$

$$\frac{\text{Tr}^2(\mathbf{H})}{\text{Det}(\mathbf{H})} = \frac{(\lambda_1 + \lambda_2)^2}{\lambda_1\lambda_2} < \frac{(r + 1)^2}{r} \quad (13)$$

Based on the legitimate key-points, the orientation is assigned to each key-points so as to make it rotation invariance in the stage of orientation assignment. In this step, the histogram of oriented gradient (HOG) with 36 bins covering 2π is considered. Weak edges below the threshold gradient magnitude are removed, and the histogram of remaining edge orientations is created. Subsequently, the orientation of the key-points can be calculated effectively. Finally, a 16×16 window for the key-points is taken into consideration for the key-point descriptor, which is then divided into 16 sub-blocks of 4×4 grid of cells. The corresponding orientation histogram for each cell is calculated, and therefore the 128-dimensional descriptor for eight directions is incorporated to build the key-point descriptor. Through the SIFT approach, image key-points can be effectively selected to derive descriptors, like a unique fingerprint, based on neighbouring pixels, orientations, and magnitudes, as shown in Figure 5. Subsequently, the features of the pallet image can be extracted for further comparison with another pallet image. When the features of two pallet images are highly matched, the pallets are deemed to be highly similar such that the risk of receiving fraudulent pallets is reduced. Consequently, the PIDs are associated with basic pallet information, such as types and quality status, and transactions and pallet-specific features to support the pallet validation in real-life operations.

Figure 5. Key-points of a sample pallet image extracted by using SIFT approach



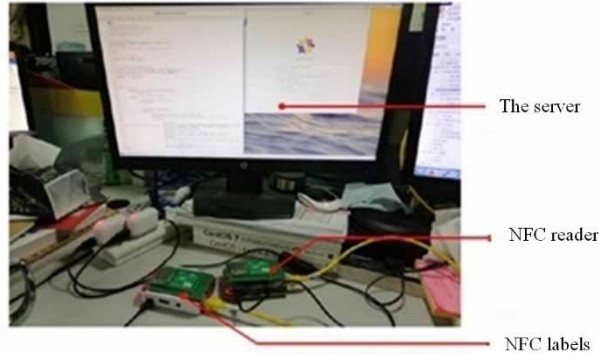
4. CASE STUDY

After elaborating the proposed authentication system, a case study is illustrated in this section to examine the feasibility of the proposed system. In this case study, a company that is actively doing the business on pallet pooling was invited to be the testbed to investigate the effectiveness of data and pallet authentication under the pallet pooling network. The case company manages various types of pallets, such as wooden, plastic, and metal pallets, centralised for its contracted partners in the supply chain network. Through providing pallet pooling services, the case company is responsible for distributing the correct quantity and quality of pallets to customers at the right time. In addition, damaged and excessive pallets are returned to the case company for repair and redistribution in the supply chain network. Thus a closed-loop structure in the pallet management system can be established to enhance the sustainability of the entire supply chain ecosystem. Although the pallet pooling approach may bring certain benefits to various industries, most end-users are concerned about the authenticity of pallets shared in the pool, influencing operational effectiveness and efficiency. Since the end-users, e.g. logistics service providers, may strictly follow the instructions from customers and customs, the types and quality of pallets circulated in the supply chain should meet their standards. Therefore, the case company is eager to revamp its pallet pooling services to enhance the pallet authenticity to end-users by deploying the proposed system described in this study.

4.1 Deployment Of Data Authentication For Biot

A series of simulation analyses are conducted to verify the effectiveness of end-to-end, two-way identity security authentication of the IoT based on blockchain technology. The simulation environment is as follows: a computer operating in Windows 10 (64-bit) with Intel i706770HQ@2.60GHz 2.59GHz and 32GB installed memory. All algorithms used in this study are implemented in C language, and there are 21 links in the authentication network. The frequency gap's capacity of the pipeline support link is 400, the bandwidth of the spectrum slot is 12.5 Hz, and the frequency gap of broadband

Figure 6. Simulation environment for the data authentication



demand distribution is 1 to 10. Based on the Kali Linux platform, an SSH device is selected to log in to a remote Raspberry Pi near-field communication (NFC) device, and the authentication process between devices is investigated.

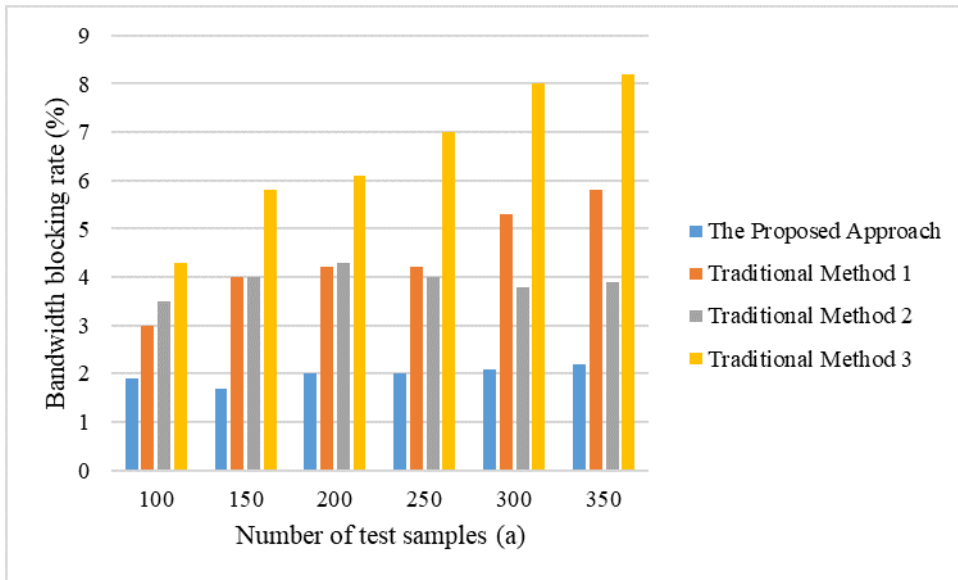
For measuring the effectiveness of the data authentication in blockchain technology, bandwidth blocking rate (%) is introduced. Under the user information identity security authentication service load, the bandwidth blocking rate represents the ratio between rejected services and the total number of services, as in Equation (9). S is the sum of the number of successfully connected services, and S_b is the number of rejected services. Thus, $|S|$ is the number of indirect service requests successfully established, and $|S_b|$ is the number of rejected business requests. When the authentication process reaches a stable state, the blocking rate is inversely proportional to the authentication performance. The smaller the blocking rate is, the better the authentication effect is.

$$BP = \frac{|S_b|}{|S| + |S_b|} \quad (9)$$

In the following experiments, the bandwidth blocking rate is selected as the major evaluation index. The bandwidth blocking rate of the four security authentication methods (the proposed method and three existing methods as benchmarking) is compared in detail. For the three existing methods, traditional methods 1 (Liu et al., 2019), 2 (Zhang et al., 2020) and 3 (Li et al., 2020) are considered. The results of the simulation comparison are shown in the following Figure 6. Analysis of the experimental data in Figure 5 shows that the bandwidth blocking rate of the proposed algorithm is the lowest among the four algorithms. The bandwidth blocking rate of the Traditional Method 3 algorithm is the highest among the four methods. Suppose that the collected data is divided into 100 packages at the source node, and the packet loss rate is set to be 10%. The number of slices received is tested 10,000 times to calculate the probability of restoration.

When considering the relationship between the number of received packets and the data restoration degree, an analysis is conducted and summarised in Figure 7. When the number of received packets are increased to 30, the degree of data restoration is close to 100%, and when the number of received

Figure 7. Comparison of the bandwidth blocking rate between the proposed approach and three existing methods



packets is less than 10, the degree of data restoration is close to 0%. In conclusion, when the number of received packets is guaranteed to be more than 30, the data recovery performance is good.

The main reason for this good performance is that the method proposed in this paper introduces blockchain technology and the gateway into identity security authentication. The node registration process can be omitted, and the user operation for the data authentication is simplified, which can ensure the centralised state of information control to a greater extent. In addition, a network consensus is allowed to be reached and ensures that each user's information is authenticated through cryptography to prevent the leakage of a user's private information. In addition, the storage response time (min) is compared between the proposed approach and three existing methods, where storage response time refers to the time when the system responds to the request, as in Equation (10). The value T represents the total storage time of the file, L represents the data block size of each database submission, n represents the massive big data attribute, and S represents the file size.

$$T = f(S, L) + g(S, L) \quad (10)$$

Similarly, the three existing methods are selected as the comparison methods to verify the effectiveness of the proposed method in the simulation experiment. During the experiment, the number of nodes is set at 3000, and the results of that experimental comparison are shown in Figure 8. It can be seen that with the continuous increase in the number of nodes, the storage methods of various storage times also change. Compared to the other three methods, the storage energy consumption of the proposed approach is significantly lower. The main reason is that this method takes ECC and D-H as the encryption tool of the whole architecture to realise the encrypted communication between the IoT devices and for the encrypted communication between the IoT devices and the Raft service group. At the same time, the proposed method effectively ensures the secrecy of the dynamic data in the IoT, the efficiency of the data communication and reduces the storage time.

Apart from measuring the communication and storage effectiveness, the accuracy of the data storage is evaluated by means of the root mean square error, where the specific calculation is provided

Figure 8. User information data restoration degree in the authentication process

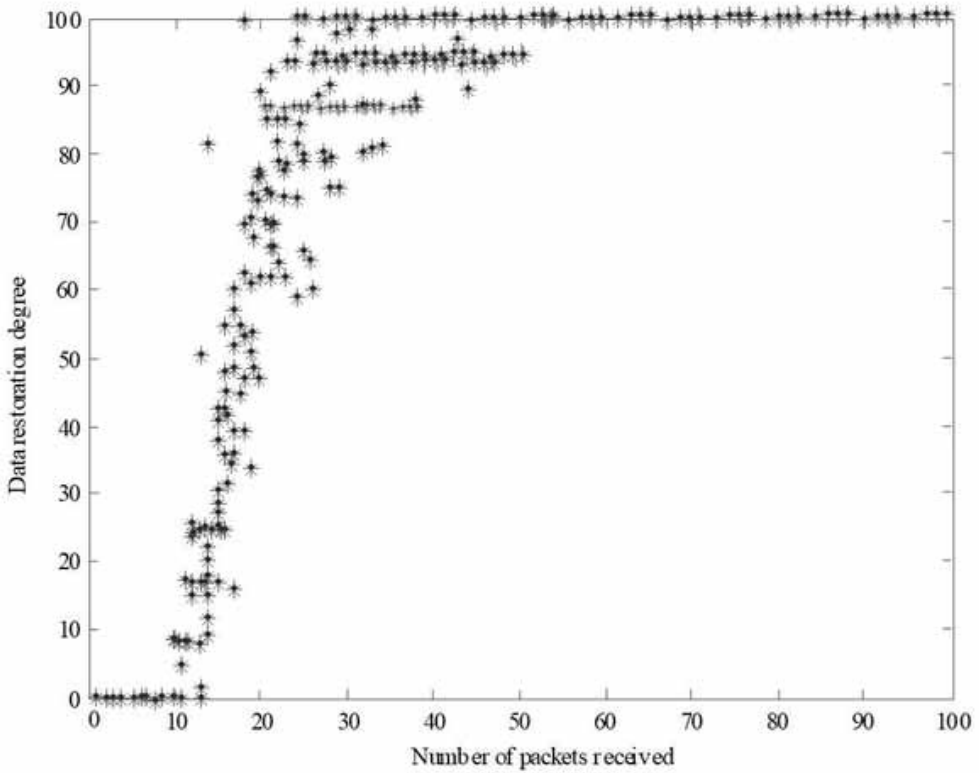


Figure 9. User information data restoration degree in the authentication process between the proposed approach and three existing methods

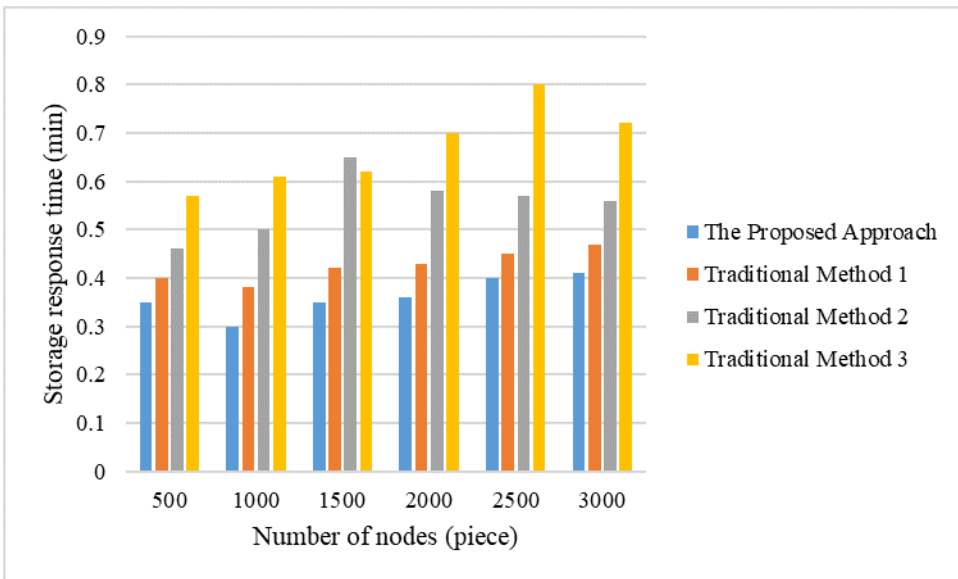


Table 1. Measurement on storage accuracy between the proposed approach and traditional methods

Number of nodes	RMSE error in %			
	Proposed approach	Traditional method 1	Traditional method 2	Traditional method 3
300	0.001	0.003	0.014	0.022
600	0.002	0.002	0.015	0.018
900	0.004	0.007	0.012	0.016
1200	0.003	0.010	0.010	0.019
1500	0.006	0.012	0.014	0.022
1800	0.003	0.008	0.016	0.025
2100	0.005	0.009	0.020	0.028
2400	0.004	0.007	0.015	0.030
2700	0.002	0.011	0.018	0.034
3000	0.001	0.013	0.019	0.037
Average (%)	0.0031	0.0082	0.0153	0.0251

as in Equation (11). In the above equation, (x, y) refers to the feature points in the reference data, (x', y') refers to the corresponding feature points in the data to be registered before and after correction, and m refers to the final feature point logarithm.

$$RMSE = \sqrt{\frac{\sum_{i=1}^m \left[(x_i - x'_i)^2 + (y_i - y'_i)^2 \right]}{m}} \quad (11)$$

The RMSE errors of four different storage methods are compared to verify the effectiveness of the proposed method further. The specific experimental results are shown in Table 1.

The experimental data in Table 1 shows that the root mean square error of the proposed method is significantly lower than that of the three traditional methods. The most important reason is that the proposed method made a series of improvements in the traditional methods that have greatly reduced the root mean square error of the proposed method. The proposed method combines the blockchain technology to store the dynamic data in the IoT and the access of IoT nodes, which stores the dynamic data between IoT nodes in the storage structure under the chain and reduces the root mean square error of the data storage.

4.3 Deployment Of Hybrid Pallet Authentication

Once the data authenticity in the IoT network is guaranteed by deploying the blockchain technology, the authenticity can be further extended to the pallets circulated in the supply chain network. Similar to virtual currency transactions, the ownership transfer of pallets can be recorded in the blockchain to manage the pallet movements in the network. The pallets are authenticated at each pallet transfer between users by considering the tags, locations, and pallet-specific features. Using the Hyperledger fabric blockchain framework, the Raft consensus algorithm is applied to achieve consensus in the supply chain network using crash fault tolerance. The validators to forge the blocks are selected by voting. Subsequently, the permissioned blockchain application for pallet pooling is established in a

Figure 10. Matching two pallet images by using SIFT approach

highly-efficient and cost-effective manner. The minimum network size should be $2N+1$, where N refers to the number of crashed/disappeared nodes.

Once the pallet transfer transactions are proposed, a smart contract mechanism is activated to check the pallet authenticity. Firstly, the pallet IDs are the first wall of defence to ensure that the pallet IDs listed in the transactions match the IDs stored in the NFC labels. Secondly, the pallet locations should be recorded within a reasonable range of movements. Since the pallet transfer operations should occur in specific premises, such as warehouses, retail stores, and other logistics facilities under the end-users, alerts to end-users and pallet pooling service providers are sent to resolve such abnormalities. In addition to tag-based and location-based authentication, the pallet-specific features extracted by pallet photos are analysed using the SIFT approach as elaborated in Section 3.3. After identifying the key-points from the pallet image at pallet registration, the matching process between the original image and the image captured by the end-users is conducted. To validate the image similarity, a threshold of the number of matches between the two images should be defined in advance. In this case study, the threshold ratio is set at 0.5, which implies that the pallet image captured by the end-users should contain at least half of the key-points identified from the original image. A stricter threshold can be set to enhance the reliability of the authentication process in terms of pallet-specific features. By using OpenCV (i.e. cv2) in the Python environment, the SIFT approach can be implemented effectively to inspect the similarity of the two images. For example, the pallet image depicted in Section 3.3 is used to compare with the pallet image captured at the warehouse. Figure 9 shows the matched key-points between the two images, where it is found that there are 411 matched key-points out of 800 key-points identified from the original image. Under the defined threshold, the pallets at the users' premises can be authenticated so that the pallet ownership transfer can also be validated in the blockchain network. With the aid of three defence walls, the pallet authentication process becomes trustworthy and reliable, and the sensitive data transmitted in the supply chain network for pallet management can be more secure.

5. RESULTS AND DISCUSSION

After the proposed system is successfully implemented in the case company, the data and pallet authenticity are improved in the pallet pooling services such that end-users can safely transmit their transactions to the platform for pallet ownership transfer. Regarding the advantages and values of developing pallet pooling, supply chain stakeholders, such as logistics companies, are no longer required to manage the pallets by themselves for daily operations. The pallet pooling service providers are particularly responsible for assuring the pallet quality and complying with import and export regulations, namely heat treatment, fumigation and pest control. Also, the concept of vendor-managed inventory (VMI) can be further extended to the pallet management under the pallet pooling services. The stock level of pallets can be controlled by the service providers, resulting in the minimisation of the corresponding storage spaces. Lastly, the industry's rise of pallet pooling services may lead to the process standardisation in the trusted supply chain network, while only standardised and authenticated pallets are circulated. Beyond the system implementation, the impact of the proposed system is shown in this section, while the managerial insights are then discussed.

5.1 Impact Of The Proposed System

In order to measure the impact of the proposed system implemented in the case company, a simple survey on the end-users and system perspectives was conducted with the five dimensions as shown

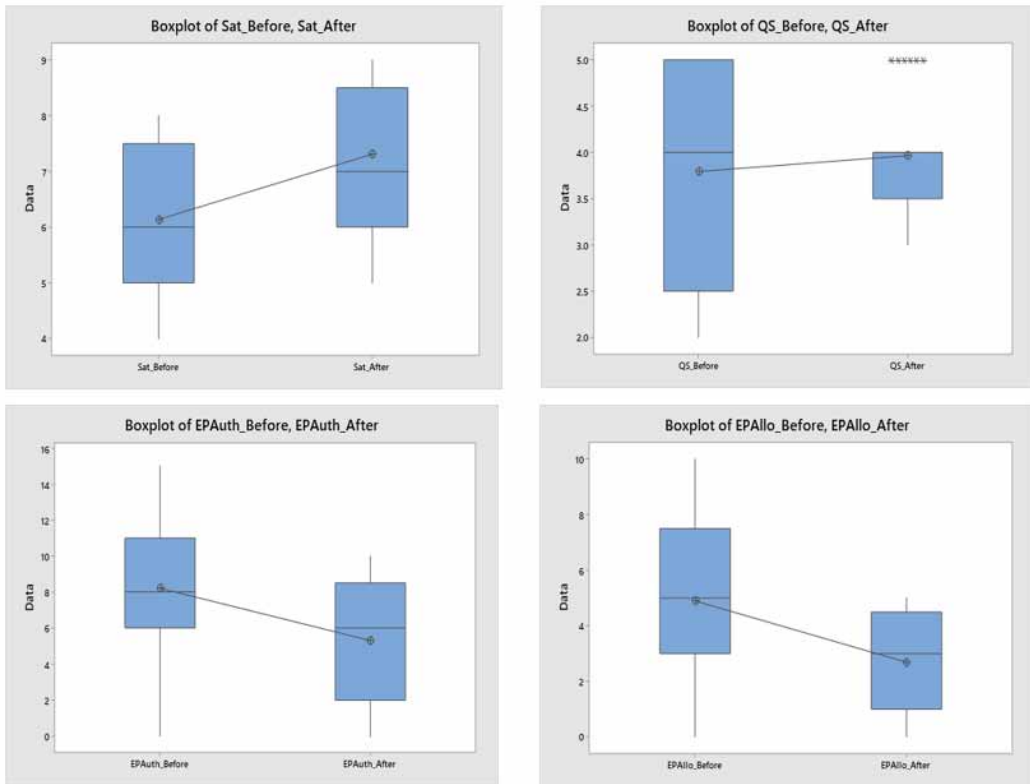
in Table 2. The five dimensions were: (i) end-user satisfaction (in scale 1 to 10), (ii) quality of services (in scale 1 to 5) referring to users' mean opinion score on system quality, (iii) error of pallet authentication (in times), (iv) error of pallet allocation (in times), and (v) time for pallet traceability (in hours). In this measurement with a two-month timeframe, 30 customers of the case company using the pallet pooling services were invited to investigate the percentage change before and after implementing the proposed system. Table 2 also shows the summary of the survey results in the aforementioned five dimensions. It was found that a positive impact on end-user satisfaction and quality of services was observed at +19.10% and +4.55%, respectively. When applying the two-sample *t* test, the difference on end-user satisfaction before and after implementing the proposed system was statistically significant in the 95% confidence level (p -value = 0.001 \leq 0.05). However, the difference in service quality was not statistically significant. In addition, the use of the proposed system also brought positive effects on the pallet authentication and allocation with improvements of 35.29% and 45.07%, respectively. In using the two-sample *t* test, differences in pallet authentication and allocation errors were statistically significant in the 95% confidence level, where their p -values were 0.001 and 0.002, respectively. Lastly, the integration of blockchain technology in the pallet pooling service platform generated a constructive influence on pallet traceability. Under the distributed and append-only ledger database, the time for pallet traceability was greatly reduced by 87.5% from 2 hours to 0.25 hours. To visualise the results of the above two-sample *t* tests, the corresponding boxplots are presented for the dimensions of end-user satisfaction, service quality, errors of pallet authentication and pallet allocation, as shown in Figure 10.

Table 2. /Impact of the proposed system in the case company

Dimension (unit)	Before	After	% Change
End-user satisfaction (scale 1-10)	6.14	7.31	+19.10%
Service quality (scale 1-5)	3.79	3.97	+4.55%
Error of pallet authentication (times)	8.21	5.31	-35.29%
Error of pallet allocation (times)	4.90	2.69	-45.07%
Time for pallet traceability (hours)	2	0.25	-87.50%

Compared with existing pallet pooling studies (Li et al., 2018; Accorsi et al., 2019), the information platform for pallet pooling is further enhanced using BIoT technologies, resulting in a reduced number of errors and better end-user satisfaction. Apart from the cloud computing environments and resources described in the previous work (Li et al., 2018; Sathiyamoorthi et al., 2021), BIoT technologies leverage the features of decentralisation and immutability so as to facilitate data and pallet authentication reliably. In order to elaborate the impact of the proposed system on the pallet operations, the impact is classified into (i) performance-aspect, (ii) efficiency-aspect, and (iii) service innovativeness. With the aid of the proposed system, the system performance for pallet pooling is enhanced with enhanced information flow to authenticate pallets by end-users, while the data authentication between IoT devices and blockchain strengthens the access control, resulting in between system reliability and security. Regarding operational efficiency, the pallet pooling services can be further smoothed by automated data and pallet authentication, while the errors for sharing pallets are reduced to enhance the service quality. In addition, the efficiency of pallet traceability is enhanced to drive the effective control and monitoring of the pallets circulated in the logistics network. For the service innovativeness, pallet pooling services are emerging in the logistics industry, which enhances the environmental sustainability and operational resilience of pallet users. In order

Figure 11a. Boxplots of the two sample t tests for (a) end-user satisfaction, (b) service quality, (c) error of pallet authentication, and (d) error of pallet allocation



to effectively circulate the pallets in the logistics network, reliable data and pallet authentication are ensured through this study so as to establish a decentralised pallet pooling service in the industry.

5.2 Managerial Implications

With the aid of the proposed system, the advantages of blockchain and IoT technologies are leveraged on improving pallet pooling services such that pallets circulated in the supply chain network are considered trustworthy. Compared with typical pallet pooling management, integrating blockchain and IoT technologies enhances the system reliability and performance. The transformation of the current pallet management practice can be further facilitated in the industry. Currently, most logistics service providers and supply chain parties purchase single-use expendable pallets with high flexibility and cost-effectiveness, but the industry’s sustainability is relatively weak. Moving towards the era of Industry 5.0, intelligent systems should be sustainable, human-centric, and resilient to the industry beyond the improvements in productivity and operational efficiency. The proposed system promotes a closed-loop business model in managing pallets throughout the whole industry, and therefore the business and environmental sustainability are greatly improved. Therefore, advanced information and communication technology applications are derived to drive the maturity and practical adoption in the business environment (Peng et al., 2020; Gholami et al., 2021).

Regarding the organisation and end-user computing, the proposed system tackles the challenges on the platform itself. It strengthens the interaction and secure data transmission between end-users and the platform. Instead of merely pooling all the pallets for users, the design of the proposed

system considers the data and pallet authenticity from the end-users' perspectives. Together with user-centric thinking, end-users can safely and conveniently upload their business data to the platform, and effectively authenticate the pallets circulating in the network. The above features of the proposed system can establish trust between the end-users and the platform so that end-users are confident to participating and promoting the use of pallet pooling. Consequently, the proposed system can be deemed a vital contribution to organisational and end-user computing (Mondal and Chakrabarti, 2021).

5.3 Academic Implications

Apart from the managerial implications in logistics and supply chain management, this study also contributes to the research of organisational and end-user computing in two-facets. Instead of leveraging the benefits of emerging technologies, ways to motivate user engagement are essential to lead to innovative systems and services (Fedushko et al., 2020). Firstly, the proposed system is designed and developed in an end-user-centric manner to enhance the reliability and practicality of the pallet pooling services. Most of the existing pallet pooling services focus on the pallet distribution and return in the logistics operations, regardless of the end-user perspectives for the data and pallet authentication. The BIoT technologies are exploited to verify the data and pallet authenticity to address the end-user concerns in the proposed system. The end-users are effective to exchange the operational data and verify the pallets. Secondly, the proposed system is built on the pallet pooling service platform, which involves multiple organisations in the supply chain network. Subsequently, the proposed system can be regarded as one of the BIoT use cases in the context of organisational and end-user computing to structure the organisational behaviour on managing pallets in their premises. Consequently, this study can be contributed to the future development of BIoT-driven organisational and end-user computing.

6. CONCLUSIONS

In view of existing pallet management approaches, pallet pooling is deemed to be sustainable and resilient in circulating the right pallets with the right quantity at the right time, while industrial waste caused by pallet management can be eliminated. To align with the direction of industry 5.0 in near future, the current pallet pooling approach should be further enhanced to be human-centric, instead of merely improving operational efficiency and productivity. In this study, intelligent data and pallet authentication are proposed on the basis of the existing pallet pooling service platform by means of blockchain and IoT technologies. End-users in the service platform can safely and securely upload sensitive business information, such as pallet movements and transactions, while the pallets used in the supply chain operations are effectively authenticated. From the end-users' viewpoints, the proposed system can establish trust between the end-users and the service platform so that the use of pallet pooling can be adopted. To examine the feasibility, a case study on a local pallet pooling service provider was conducted to illustrate the deployment of BIoT data authentication and intelligent pallet authentication based on tag, location and pallet-specific features. Therefore, improvements on data and pallet authenticity, as the core objective in the study, has been achieved. The proposed system contributes to the research and development of BIoT technologies and pallet management in logistics and supply chain management. A secure, reliable, and mutually-agreed authentication protocol is exploited to consolidate the effective identification, verification and authentication process as a whole. For an industrial perspective, the proposed system, which ensures the data and pallet authenticity, gets rid of the system vulnerability and poor-quality pallets circulated in the logistics network, resulting in smoothening the material and information flows. Since the benefits of blockchain and IoT technologies are leveraged in pallet management, the proposed system can be further extended to other pooling strategies in supply chain management, such as cold chain technology. Besides, the proposed system for the pallet authentication is limited to the SIFT approach to measuring the similarity between two pallet images, while the proposed system is only examined by a case company selected in this study.

In future studies, detailed case studies can be conducted to comprehensively inspect the benefits, acceptance, and resistance of using blockchain and IoT technologies. Also, different computer vision approaches should be considered and compared to evaluate the system performance.

ACKNOWLEDGMENT

The work described in this paper was partially supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region, China (UGC/FDS14/E06/20); and a matching grant from the University Grants Committee of the Hong Kong Special Administrative Region, China (RMGS Project No. 700005). The authors would like to thank Big Data Intelligence Centre and Department of SCM, The Hang Seng University of Hong Kong, and Department of ISE, Hong Kong Polytechnic University for supporting the research.

REFERENCES

- Accorsi, R., Baruffaldi, G., Manzini, R., & Pini, C. (2019). Environmental impacts of reusable transport items: A case study of pallet pooling in a retailer supply chain. *Sustainability, 11*(11), 3147. doi:10.3390/su11113147
- Beltrán, M. (2018). Identifying, authenticating and authorising smart objects and end users to cloud services in Internet of Things. *Computers & Security, 77*, 595–611. doi:10.1016/j.cose.2018.05.011
- Chen, X., Liu, Z., Wan, J., & Li, Z. (2019). Aggregated handover authentication for machine type communication. *Journal of Organizational and End User Computing, 31*(3), 83–96. doi:10.4018/JOEUC.2019070105
- Chien, W. C., Chang, Y. C., Tsou, Y. T., Kuo, S. Y., & Chang, C. R. (2020). STT-DPSA: Digital PUF-Based Secure Authentication Using STT-MRAM for the Internet of Things. *Micromachines, 11*(5), 502. doi:10.3390/mi11050502 PMID:32429169
- Choi, T. M. (2019). Blockchain-technology-supported platforms for diamond authentication and certification in luxury supply chains. *Transportation Research Part E, Logistics and Transportation Review, 128*, 17–29. doi:10.1016/j.tre.2019.05.011
- Choi, T. M., & Ouyang, X. (2021). Initial coin offerings for blockchain based product provenance authentication platforms. *International Journal of Production Economics, 233*, 107995. doi:10.1016/j.ijpe.2020.107995
- Cruz-Mota, J., Bogdanova, I., Paquier, B., Bierlaire, M., & Thiran, J. P. (2012). Scale invariant feature transform on the sphere: Theory and applications. *International Journal of Computer Vision, 98*(2), 217–241. doi:10.1007/s11263-011-0505-4
- Dabbagh, Y. S., & Saad, W. (2019). Authentication of wireless devices in the Internet of Things: Learning and environmental effects. *IEEE Internet of Things Journal, 6*(4), 6692–6705. doi:10.1109/JIOT.2019.2910233
- Durairaj, M., & Muthuramalingam, K. (2018). User authentication and key agreement scheme for internet of thing-a study. *International Journal of Computer Aided Engineering and Technology, 10*(5), 589–598. doi:10.1504/IJCAET.2018.094338
- Fachrunnisa, O., & Hussain, F. K. (2020). Blockchain-based human resource management practices for mitigating skills and competencies gap in workforce. *International Journal of Engineering Business Management, 12*. Advance online publication. doi:10.1177/1847979020966400
- Fan, P., Liu, Y., Zhu, J., Fan, X., & Wen, L. (2019). Identity Management Security Authentication Based on Blockchain Technologies. *International Journal of Network Security, 21*(6), 912–917.
- Fang, H., Qi, A., & Wang, X. (2020). Fast authentication and progressive authorisation in large-scale IoT: How to leverage ai for security enhancement. *IEEE Network, 34*(3), 24–29. doi:10.1109/MNET.011.1900276
- Fedushko, S., Ustyianovych, T., Syerov, Y., & Peracek, T. (2020). User-Engagement Score and SLIs/SLOs/SLAs Measurements Correlation of E-Business Projects Through Big Data Analysis. *Applied Sciences (Basel, Switzerland), 10*(24), 9112. doi:10.3390/app10249112
- Gholami, R., Singh, N., Agrawal, P., Espinosa, K., & Bamufleh, D. (2021). Information Technology/Systems Adoption in the Public Sector: Evidence From the Illinois Department of Transportation. *Journal of Global Information Management, 29*(4), 172–194. doi:10.4018/JGIM.20210701.oa8
- Gill, S. S., & Shaghghi, A. (2020). Security-aware autonomic allocation of cloud resources: A model, research trends, and future directions. *Journal of Organizational and End User Computing, 32*(3), 15–22. doi:10.4018/JOEUC.2020070102
- Gupta, B. B., & Narayan, S. (2021). A Key-Based Mutual Authentication Framework for Mobile Contactless Payment System Using Authentication Server. *Journal of Organizational and End User Computing, 33*(2), 1–16. doi:10.4018/JOEUC.20210301.oa1
- Ho, G. T. S., Tang, Y. M., Tsang, K. Y., Tang, V., & Chau, K. Y. (2021). A blockchain-based system to enhance aircraft parts traceability and trackability for inventory management. *Expert Systems with Applications, 179*, 115101. doi:10.1016/j.eswa.2021.115101

- Huang, Y., Liang, W., Long, J., Xu, J., & Li, K. C. (2018, August). A Novel Identity Authentication for FPGA Based IP Designs. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 1531-1536). IEEE. doi:10.1109/TrustCom/BigDataSE.2018.00218
- Lehtonen, M. O., Michahelles, F., & Fleisch, E. (2007). Trust and security in RFID-based product authentication systems. *IEEE Systems Journal, 1*(2), 129–144. doi:10.1109/JSYST.2007.909820
- Li, C. T., Lee, C. C., & Weng, C. Y. (2018). A secure three party node authentication and key establishment scheme for the Internet of things environment. *Journal of Internet Technology, 19*(1), 147–155.
- Li, J. B., He, S. W., & Yin, W. C. (2018). The study of pallet pooling information platform based on cloud computing. *Scientific Programming, 2018*, 1–5. Advance online publication. doi:10.1155/2018/5106392
- Li, Q., Zhao, Y., Li, S., Yu, J., & Gao, S. (2020). Identity authentication scheme between terminal devices of Internet of things based on IBE strategy. *Information Technology and Network Security, 39*(3), 10-13.
- Li, W., & Wang, P. (2019). Two-factor authentication in industrial Internet-of-Things: Attacks, evaluation and new construction. *Future Generation Computer Systems, 101*, 694–708. doi:10.1016/j.future.2019.06.020
- Liang, W., Xie, S., Long, J., Li, K. C., Zhang, D., & Li, K. (2019). A double PUF-based RFID identity authentication protocol in service-centric internet of things environments. *Information Sciences, 503*, 129–147. doi:10.1016/j.ins.2019.06.047
- Liu, T., Zhou, P., & Li, J. (2019). Research on SG-eIoT Identity Authentication Technology based on Blockchain. *Cyberspace Security, 10*(7), 48–54.
- Mondal, A., & Chakrabarti, A. B. (2021). Information and Communication Technology Adoption Strategies of Emerging Multinationals From India. *Journal of Global Information Management, 29*(5), 161–175. doi:10.4018/JGIM.20210901.0a9
- Nandy, T., Idris, M. Y. I. B., Noor, R. M., Kiah, L. M., Lun, L. S., Juma'at, N. B. A., & Bhattacharyya, S. et al. (2019). Review on security of Internet of Things authentication mechanism. *IEEE Access: Practical Innovations, Open Solutions, 7*, 151054–151089. doi:10.1109/ACCESS.2019.2947723
- Norta, A., Matulevičius, R., & Leiding, B. (2019). Safeguarding a formalised blockchain-enabled identity-authentication protocol by applying security risk-oriented patterns. *Computers & Security, 86*, 253–269. doi:10.1016/j.cose.2019.05.017
- Peng, J., Guo, P., Guo, M., & Zhang, G. (2020). IT application maturity in china: How do you manage it? *Journal of Global Information Management, 28*(3), 99–122. doi:10.4018/JGIM.2020070106
- Sathiyamoorthi, V., Keerthika, P., & Suresh, P. (2021). Adaptive Fault Tolerant Resource Allocation Scheme for Cloud Computing Environments. *Journal of Organizational and End User Computing, 33*(5), 135–152. doi:10.4018/JOEUC.20210901.0a7
- Shuai, M., Yu, N., Wang, H., Xiong, L., & Li, Y. (2021). A Lightweight Three-Factor Anonymous Authentication Scheme With Privacy Protection for Personalized Healthcare Applications. *Journal of Organizational and End User Computing, 33*(3), 1–18. doi:10.4018/JOEUC.20210501.0a1
- Song, L., Sun, G., Yu, H., Du, X., & Guizani, M. (2020). Fbia: A fog-based identity authentication scheme for privacy preservation in internet of vehicles. *IEEE Transactions on Vehicular Technology, 69*(5), 5403–5415. doi:10.1109/TVT.2020.2977829
- Trnka, M., Cerny, T., & Stickney, N. (2018). Survey of Authentication and Authorization for the Internet of Things. *Security and Communication Networks, 2018*, 1–17. Advance online publication. doi:10.1155/2018/4351603
- Tsang, Y. P., Choy, K. L., Wu, C. H., Ho, G. T. S., & Lam, H. Y. (2019). Blockchain-driven IoT for food traceability with an integrated consensus mechanism. *IEEE Access: Practical Innovations, Open Solutions, 7*, 129000–129017. doi:10.1109/ACCESS.2019.2940227
- Tsang, Y. P., Wu, C. H., Ip, W. H., & Shiau, W. L. (2021). Exploring the intellectual cores of the blockchain-Internet of Things (BIoT). *Journal of Enterprise Information Management*. Advance online publication. doi:10.1108/JEIM-10-2020-0395

- Tsang, Y. P., Wu, C. H., Lam, H. Y., Choy, K. L., & Ho, G. T. (2021). Integrating Internet of Things and multi-temperature delivery planning for perishable food E-commerce logistics: A model and application. *International Journal of Production Research*, 59(5), 1534–1556. doi:10.1080/00207543.2020.1841315
- Wan, H. C., & Chin, K. S. (2021). Exploring internet of healthcare things for establishing an integrated care link system in the healthcare industry. *International Journal of Engineering Business Management*, 13. doi:10.1177/18479790211019526
- Wan, R., Da, B., Li, R., Wang, C., & Li, H. (2018, January). Identity based security for authentication and mobility in future ID oriented networks. In *2018 International Conference on Information Networking (ICOIN)* (pp. 402-407). IEEE. doi:10.1109/ICOIN.2018.8343149
- Wang, F., Shan, G. B., Chen, Y., Zheng, X., Wang, H., Mingwei, S., & Haihua, L. (2020). Identity authentication security management in mobile payment systems. *Journal of Global Information Management*, 28(1), 189–203. doi:10.4018/JGIM.2020010110
- Wu, Z. Y. (2019). An radio-frequency identification security authentication mechanism for Internet of things applications. *International Journal of Distributed Sensor Networks*, 15(7). doi:10.1177/1550147719862223
- Xia, T., Qin, H., & Li, Z. (2019). Application and Research of Trusted Identity Authentication Cloud Service in Ubiquitous Power Internet of Things. *Electric Power Information and Communication Technology*, 17(07), 11–15.
- Xu, B., Xu, L. D., Wang, Y., & Cai, H. (2021). A distributed dynamic authorisation method for Internet+ medical & healthcare data access based on consortium blockchain. *Enterprise Information Systems*, 1–19. Advance online publication. doi:10.1080/17517575.2021.1922757
- Yan, H., Wang, Y., Jia, C., Li, J., Xiang, Y., & Pedrycz, W. (2019). IoT-FBAC: Function-based access control scheme using identity-based encryption in IoT. *Future Generation Computer Systems*, 95, 344–353. doi:10.1016/j.future.2018.12.061
- Yi, H. (2019). A secure logistics model based on blockchain. *Enterprise Information Systems*. Advance online publication. doi:10.1080/17517575.2019.1696988
- Zhang, X., Song, J., & Du, Y. (2020). A Bi-directional Identity Authentication Protocol of Internet of Things Based on Elliptic Curve. *Software Guide*, 19(10), 233–237.
- Zheng, K., Zhang, Z., Chen, Y., & Wu, J. (2019). Blockchain adoption for information sharing: Risk decision-making in spacecraft supply chain. *Enterprise Information Systems*. Advance online publication. doi:10.1080/17517575.2019.1669831
- Zheng, X. R., & Lu, Y. (2021). Blockchain technology—recent research and future trend. *Enterprise Information Systems*, 1–23. Advance online publication. doi:10.1080/17517575.2021.1939895
- Zhou, B., Li, H., & Xu, L. (2018, June). An authentication scheme using identity-based encryption & blockchain. In *2018 IEEE Symposium on Computers and Communications (ISCC)* (pp. 00556-00561). IEEE.

Wen Long is an associate professor and works in the party and government office of Hunan Modern Logistics College. She graduated from the Law School of Hunan University, and got Master's degree (2007) and Doctoral degree (2012). Her research interests include legal theory, economic law, logistics law theory, legal practice and legal teaching. In recent years, Wen Long has published 45 papers, 4 articles are indexed by CSSCI, 2 articles are indexed by CPCI and 1 article is indexed by EI. So far, Wen Long has presided over and participated in 10 projects, including 7 provincial projects and 3 national projects.

C. H. Wu excels in his role with PolyU as a researcher with more than a decade of professional experience. Having held numerous roles with the university previously, his expertise precedes him. Over the years, Dr Wu worked closely with many industrial partners to support and contribute to the formulation of their business strategies, operations improvement, and new product development. As he looks to the future, Dr Wu intends to continue researching in the fields of Industrial Internet of Things (IIoT), Industry 4.0 and healthcare technology in HSUHK.

Y. P. Tsang is currently a Research Assistant Professor at the Department of Industrial and Systems Engineering of The Hong Kong Polytechnic University. He received his BSc (Hons) in Logistics Engineering Management and PhD in the Department of Industrial and Systems Engineering from The Hong Kong Polytechnic University in 2015 and 2020, respectively. His current research areas cover industrial blockchain with applications, internet of things and industry 4.0 technologies, and artificial intelligence for decision-making. He is also a member and council associate of Hong Kong Logistics Association.

Qiyang Chen is a full professor in the Department of Information Management & Business Analytics, teaching courses in information systems, database, and applications development in business. His research interests and publications are in the areas of information resource management, interactive systems, and knowledge engineering. Dr. Chen received a PhD in Information Systems from the University of Maryland, an MS in Computer Science from the China Academy of Space, and a BS in Applied Math and Information Systems from the National University of Defense Technology (China).