ARTICLES

Integrated Technologies of Blockchain and Biometrics Based on Wireless Sensor Network for Library Management

Meng-Hsuan Fu

ABSTRACT

The Internet of Things (IoT) is built on a strong internet infrastructure and many wireless sensor devices. Presently, Radio Frequency Identification embedded (RFID-embedded) smart cards are ubiquitous, used for many things including student ID cards, transportation cards, bank cards, prepaid cards, and citizenship cards. One example of places that require smart cards is libraries. Each library, such as a university library, city library, local library, or community library, has its own card and the user must bring the appropriate card to enter a library and borrow material. However, it is inconvenient to bring various cards to access different libraries. Wireless infrastructure has been well developed and IoT devices are connected through this infrastructure. Moreover, the development of biometric identification technologies has continued to advance. Blockchain methodologies have been successfully adopted in various fields. This paper proposes the BlockMetrics library based on integrated technologies using blockchain and finger-vein biometrics, which are adopted into a library collection management and access control system. The library collection is managed by image recognition, RFID, and wireless sensor technologies. In addition, a biometric system is connected to a library collection control system, enabling the borrowing procedure to consist of only two steps. First, the user adopts a biometric recognition device for user authentication and then performs a collection scan with the RFID devices. All the records are recorded in a personal borrowing blockchain, which is a peer-to-peer transfer system and permanent data storage. In addition, the user can check the status of his collection across various libraries in his personal borrowing blockchain. The BlockMetrics library is based on an integration of technologies that include blockchain, biometrics, and wireless sensor technologies to improve the smart library.

INTRODUCTION

The Internet of Things (IoT) connects individual objects together through their unique address or tag, which are based on the sensor devices and wireless network infrastructure. Presently, "smart living" (a term that includes concepts such as the smart home, smart city, smart university, smart government, and smart transportation) is based on the IoT, which plays a key role to achieve a convenient and secure living environment.

Gartner, a data analytics company that presents the top ten strategic technology trends for the next year at the end of each year, listed blockchain as one of the top ten in 2017, 2018, 2019, and 2020.[1] The fact that blockchain has been proposed as one of the top strategic technology trends for four consecutive years represents its sustained interest among technology experts and developers. In a blockchain, a block is the basic storage unit where data is saved and protected with cryptography and complex algorithms. The technology of peer-to-peer transfer is adopted

Meng-Hsuan Fu (msfu@mail.shu.edu.tw) is Assistant Professor, Shih Hsin University (Taiwan).

https://doi.org/10.6017/ital.v39i3.11883

when data or information is exchanged without the need for a third party. In other words, data is transferred directly from node to node or user to user thanks to the decentralized nature of the blockchain. In addition, blockchain is authorized and maintained by all nodes in the same blockchain network. Each node has equal right (also known as equal weight) to access the blockchain and authorize new transactions. Thus, all transactions are published and broadcast to all nodes and content cannot be altered by single or minority users or nodes. Additionally, transaction content is secured by cryptography and complex secure algorithms. Therefore, transactions occur and are preserved under a fully secure and private network. In practice, the blockchain has been applied to various fields including finance, medicine, academia, and logistics. The blockchain has also been adopted for personal transaction records for its privacy and security properties and because it offers immutable and permanent data storage. In this research, blockchain technologies are adopted to store the records of collections borrowed from various libraries in a personal borrowing blockchain.

Table 1. Definition of Key Terms of Blockchain

Key Term	Definition
Blockchain	A blockchain comprises many blocks. It has the characteristics of security, decentralized, immutability, distributed ledgers, transparent log, and irreversible data storage.
Block	A block is the basic unit in blockchain. Each block consists of a block header with nonce, previous block hash, timestamp, Merkle root, and many transactions in a block body.
Nonce	The counter of the algorithm, hash value will be changed once the nonce modified.
Merkle root	A secure hash algorithm (SHA) is used in Merkle root to transform data into a meaningless hash value.
Transaction	Each transaction is composed of address, hash, index, and timestamp. All transactions will be stored in blocks permanently.
Hash	Secure hash algorithm (SHA) transforms input data into meaningless output data, called a hash, which consists of English letters and digital numbers, in order to protect data content during transmission.
Biometrics	Using human physical characteristics including finger vein, iris, voice, and facial features for recognition.
Sensor Network	A sensor is a small and portable node with a data record function and power source. A sensor network is composed of many sensors based on a communication infrastructure.
IoT	Internet of Things (IoT) is a system to connect sensors and devices together under an internet environment. Presently, many IoT applications were adopted such as smart home, health care, and smart transportation.

Although the IoT and wireless networks have been well developed, people still own many different RFID-embedded cards, such as public transportation cards, credit cards, student cards, medical cards, identification cards, membership cards, or library cards. An RFID-embedded card is issued for each place or purpose, requiring the user to bring the appropriate cards to access the corresponding functions. In this study, the library is used as the objective to which blockchain technologies are applied because currently each library has its own library card for entering the library and borrowing material. This implies that users may have to carry several library cards to access each of a university library, community library, and district library on the same day. Here, biometrics can be adopted to solve the problem of having to carry many access control cards and managing various borrowing policies.

In this study, the BlockMetrics library is designed based on the technologies of blockchain and biometrics within the environment of a wireless sensor network with IoT devices. Here, borrowing records are transferred and stored through blockchain technologies, automatic library access control is managed by biometric identification and the borrowing and returning of library materials are achieved under a wireless sensor network with IoT devices to create a convenient, efficient, and secure library environment. The key terms of blockchain and its related terms, biometrics, sensor network and IoT applied in this research are defined in table 1.

RELATED WORKS

Blockchain Technology

Nakamoto has presented bitcoin as a peer-to-peer electronic system that uses blockchain technologies, which include smart contracts, cryptography, decentralization, and consensus in proof of work. Because this electronic system is based on cryptography, a trusted third party is not required in the payment mechanism. Additionally, peer-to-peer technology and a timestamp server are adopted and a block is given a hash in serial order. This procedure solves the problem of double-spending during payment.[2] In addition, proof of work is used in a decentralized system for authentication by most nodes in the blockchain network. Each node has equal rights to compete to receive a block and each node can vote to authenticate a new block.[3] Košt'ál et al. define Proof-of-Work (PoW) as an asymmetric method with complex calculations where its difficulty is adjusted by the problem-solving duration.[4] However, PoW has drawbacks, such as high power consumption and the fact that some users can control the blockchain if their shares of users in the same blockchain network reach 51 percent.[5] Despite the possible presence of malicious parties, the information in a blockchain is difficult to modify because of the distributed ledger methodology in which each node has the same copy of ledger, making it difficult for a single or minority node to change or destroy the stored data.[6]

A block is a basic unit in a blockchain. In other words, a blockchain is composed of blocks that are connected. One of the blockchain technologies is the distributed ledger, in which a ledger can be distributed to each node all over the world.[7] Each block is composed of a block body and header, and a block size is 4 bytes. The block header is a combination of the version, previous block hash, Merkle root, timestamp, difficulty target, and nonce. A blockchain is 80 bytes in total and transactions are between 1 to 9 bytes (see table 2).

Table 2. Block Element.

Block size	**4 bytes**	**Size**
Block header (80 bytes)	4 bytes	Version
	32 bytes	Previous block hash
	32 bytes	Merkle root
	4 bytes	Timestamp
	4 bytes	Difficulty target
	4 bytes	Nonce
Block body	1-9 bytes	Transactions

Blockchain technologies have been applied to various fields including finance, art, hygiene, healthcare, and academic certificates. For example, in healthcare, user medical records are stored in a blockchain so users can check their health conditions and share them with their family members in advance. In business, blockchain is adopted into the supply chain management for monitoring activities during goods production. In the academic field, the certificates are permanently saved in a blockchain where users can retrieve them from their mobile devices and show them upon request.[8] Because blockchain is protected by cryptography and offers privacy, reliability, and decentralization, an increasing number of applications are beginning to adopt it. As an application for a library system, a blockchain, in combination with biometrics within a wireless infrastructure, can be adopted for personal borrowing records.

Library Borrowing Management

Each library has its own regulations. For example, the National Central Library (NCL) in Taiwan has created reader service directions in which the general principles and rules for library card application, reader access to library materials, reference services, request for library materials, violations, and supplementary provisions are clearly stated. According to the NCL reader service directions, citizens are required to present their national ID card and foreigners are asked to present their passport to apply for a library card. Users are allowed to access the library when they have a valid library card. Those who have library cards but have forgotten to bring them can apply for a temporary library card to enter the library, but this is limited to three times.[9] This rule is only specific to the NCL. Other libraries in the same country have their own regulations.

Another example is the Taipei Public Library. Citizens can apply for a library card using their citizen's ID card, passport, educational certificate, or residence permit. A Taipei citizen can apply for a family library card using their family certificate. Users can borrow material and return the material to all the libraries in Taipei city. However, these policies are only applicable to users who hold library cards issued by libraries in Taipei city.[10]

As for university libraries, each library also has its own regulations. For instance, Shih Hsin University (SHU) issues its own library card to access its library. Alumni are requested to present their ID cards and photo to apply for a library card in person. The number of items and their loan periods are clearly stated in the rules set by the SHU library.[11] Again, the regulations are individually set by each university library.

Biometrics

RFID-embedded smart cards such as student cards, transportation cards, and bank cards are widely used, however, they can be stolen, lost, or forgotten at home. Biometrics is becoming more widely used in access-control systems for homes, offices, buildings, government facilities, and libraries. For these systems, the fingerprint is one of the most commonly used biometrics. Users place their finger on a read device, usually a touch panel. This method ensures a unique identity, is easy to use and widely accepted, boasts a high scan speed, and is difficult to falsify. However, its effectiveness is influenced by the age of the user and the presence of moisture, wounds, dust, or particles on the finger, in addition to the concern for hygiene because of the use of touch devices. Face recognition has been used in various applications such as unlocking smart devices, performing security checks and community surveillance, and maintaining home security. This method of biometric identification is convenient, widely accepted, difficult to falsify, and can be applied without the awareness of the person. However, limitations to face recognition include errors that can occur due to lighting, facial expression, and cosmetics. Also, privacy is an issue in face recognition because it may take place at a distance without the user's consent. Another form of biometric identification uses the iris as an inner biometric indicator because the iris is unique for each person. Nevertheless, this method is also prone to errors that can be caused by bad lighting and the possible presence of diseases such as diabetes or glaucoma. Devices used for iris recognition are expensive, and thus rarely adopted in biometrics.[12] Speech recognition is used for equipment control such as a smart device switch, however, it can be affected by noise, physical conditions of the user, or weather. Vein recognition using finger or palm veins is becoming more prevalent as a form of biometric identification for banks or access control but can be limited by the possible presence of bruises or a lower temperature. However, vein recognition ensures a unique identity, is easy to use, convenient, accurate, and widely accepted, thus, many businesses are adopting vein recognition for various usages. To summarize, biometric identification is convenient, reduces the error rate in recognition, and is difficult to falsify. Therefore, biometric identification is suitable for access control.

BLOCKMETRICS LIBRARY

The BlockMetrics library is based on the integration of blockchain and biometric technologies in a wireless sensor network with IoT devices. Figure 1 shows the BlockMetrics library architecture with its bottom-up structure consisting of five layers: hardware, software, internet, transfer and security, and application. All components are sequentially described in detail from the bottom to the top layers. In the hardware layer, sensor nodes are physically located on library collection shelves, entrance gates, and relevant equipment to be further connected with the upper layers. RFID tags are attached to each item in the library, including books, audio resources, and videos. Tag information is read and transferred by RFID readers. The biometric devices used in this study include fingerprint readers, palm and finger-vein identifiers, and face or iris recognition devices for biometric authentication when users enter libraries or borrow collections. All images including action images, collection images, and surveillance images are recorded with cameras. The ground surveillance, library collection recognition, image processing, and user identification are manipulated by graphics processing units. Touch panels are used for typing or searching for information and there is a particular process for user registration. For general input and output of information, I/O devices include speakers, microphones, keyboards, and monitors. The entrance gate is connected to biometric devices and recognition systems for automatic access control. Microprocessors and servers, which make up the core of the hardware, handle all the functions that run in the operating system. Data and programs are run and securely saved on a large memory drive. Data transmission occurs through the wireless data collector, and data collection and transfer in the library are based on a wireless environment. In the BlockMetrics library, a library collection database is used to store and maintain all the library material information in a local library for backup usage, and a blockchain is used to record personal borrowing and returning history.

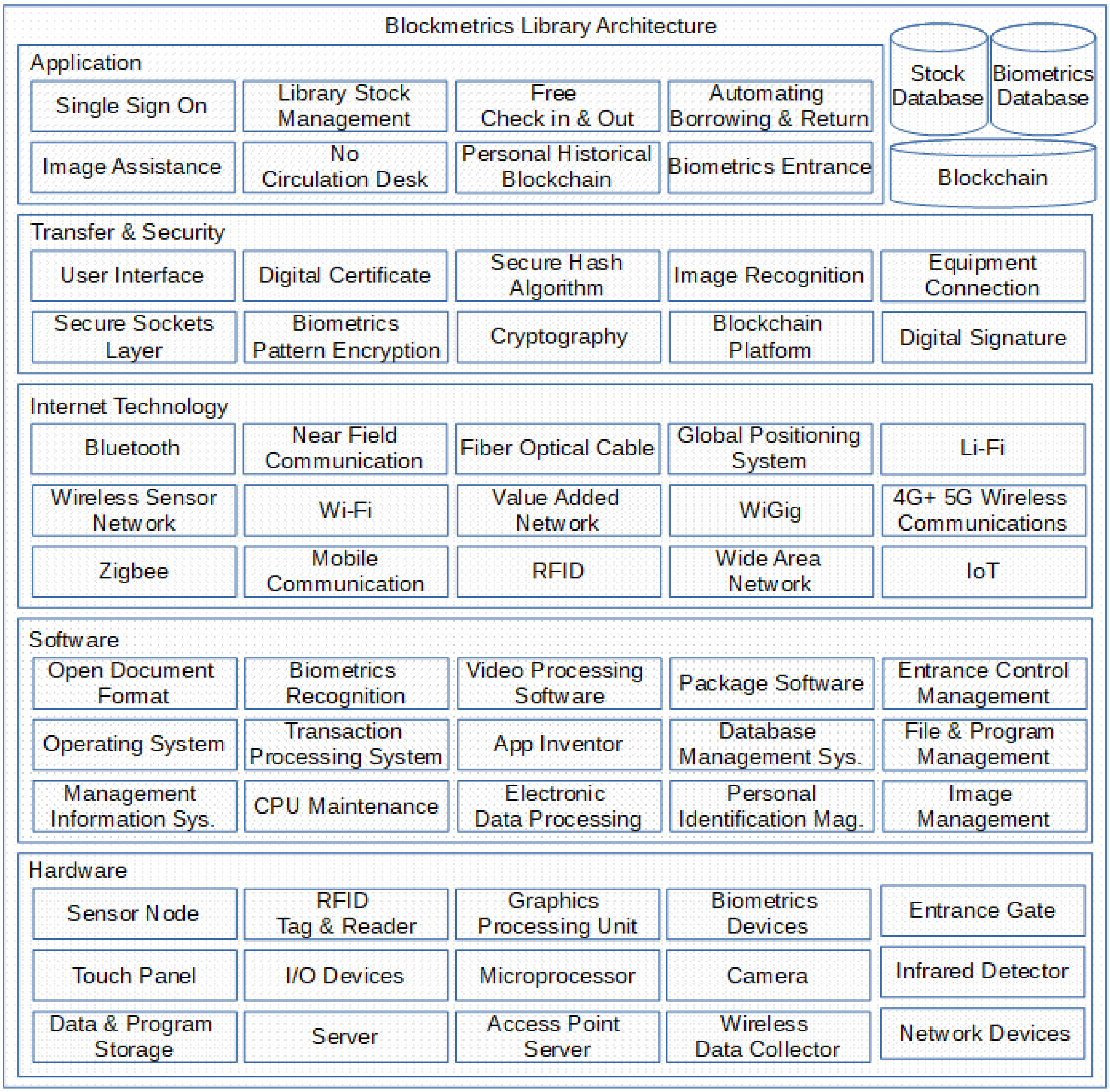

Figure 1. BlockMetrics Library Architecture

In the software layer, an open-source word processor (such as Writer, Impress, or Calc provided by LibreOffice) is used to record library collections and handle library affairs. Biometric recognition identifies a user's biological features collected from biometric devices such as a finger-vein recognition device, which is adopted in this research. All images and videos include ground and entrance surveillance and library material borrowing and returning are recorded by cameras. All images and videos are operated by and processed with video-processing software. The data of the images, videos, personal information, and library collections is managed and saved through an image and file management system as well as a database management system. The software programs associated with creating, modifying, and maintaining library processes are written with open-source programming codes, in particular, Python and R, which were scored as two of the top ten programming languages by IEEE Spectrum in 2019.[13] There are various functions saved as packages that are free to download and can be modified and reproduced into a customized program for specific purposes. The hardware houses the CPU, which runs the general library operations, and software programs are maintained by the operating system and management information system. Library stock management, collection search, personal registration, and other library-related functions can be designed and developed through App Inventor. Each borrow and return record is connected with the personal identification recognized from the finger-vein reader and recognition system and is saved as a transaction. The transactions that take place in a specific period are saved in a block that can be connected to another block to form a personal borrowing blockchain.

The internet technology layer is built upon the hardware and software structure. The main purpose of internet technologies is to connect the equipment and devices with the internet, in which the internet plays the role of an intermediary for all devices communicating and cooperating together in the library. In the internet technology layer, Bluetooth connects devices such as earphones, speakers, and audio guidance within short distances. Files are exchanged between smart devices, including smartphones, tablets, or iPads, through near-field communication, which is a contact-less sensor device. RFID is adopted for collection borrowing and returning services in the library. Because fiber-optic cables have been ubiquitously planted within infrastructure with the development of smart cities, most libraries have also been built with them. Users or vehicles are more easily and more accurately located by the Global Positioning System (GPS), which also assists with image recognition when a material is taken from the shelves. Sensors transfer the sensing data to the relative devices for recording or processing under the infrastructure of the wireless sensor network. The library is currently built with a Wi-Fi environment, but Li-Fi is one of the future trends that involve creating a wireless environment just with light. Mobile devices operate under wireless communications and most countries provide 4G and 4G+ with some supporting even 5G. The internet technology layer is the tools provider for intercommunication among devices.

Data security and transmission reliability are extremely important issues when various equipment is linked together and connected to the internet. The user interface is the bridge between the user and the devices. In other words, the user gives commands to the devices or software through a user interface or app. Biometric recognition devices, RFID readers, and entrance control equipment are connected via the internet in this study. The devices send the information to the corresponding devices for specific purposes in a specified order. Collected data such as private user identification are secured by cryptography utilized in blockchain technology. The finger-vein identification used as personal identification is combined with the borrow and return records, stored as transactions, and secured under a secure hash algorithm before being saved into a blockchain. All data and personal identification are transferred under the corresponding secure methodologies.

In the BlockMetrics library, self-check-in and self-checkout rely mostly on RFID technology and finger-vein biometrics. The borrow and return records are stored in a personal borrowing blockchain, where records are saved in the blockchains of user and library, biometrics system, and library servers. Entrance control is automatically managed by finger-vein recognition. Library stock management is particularly based on image assistance and RFID technology. New user registration is performed only through a few identification questions and finger-vein characteristics extraction. The BlockMetrics library is without a circulation desk environment and has an automated borrow and return mechanism through a single sign at the entrance and exit. The five layers in the BlockMetrics library architecture communicate with each other such that operations are inseparably related. The BlockMetrics library scenario is described in the next section.

SCENARIO

In this section, the scenarios for registration, entry, and material borrowing and returning in the BlockMetrics library will be described in detail. In figures 2 and 3, the user side indicates the actual user actions and is represented as solid lines and the background shows mostly background operations and is indicated as dotted lines. In figure 2, when a new user comes into the BlockMetrics library, the registration procedure starts with a biometric pattern extraction and recognition of the user. Finger-vein authentication is selected as the personal biometrics for entrance and material borrowing. On the user side, registration is completed with only two steps. The first is finger-vein extraction and the second is to simply provide personal information. The biometric recognition data is processed and stored in the appropriate database, which is linked to the personal identification management system. Personal information is secured through the cryptography used in blockchain technology, thus, all information is securely stored. The registration procedure is performed only once at the first entry, and afterward all registered users can enter the BlockMetrics library using finger-vein authentication.

Biometric recognition proceeds with a biometrics database that verifies user identity followed by verification results sent to the entrance control management for entrance guarding. The entrance is automatically controlled because the results from the biometric recognition step are sent as the rules for entrance control. Users will be permitted to enter the library when they pass the biometrics recognition step. Users do not have to bring their library cards to enter or borrow material, increasing convenience and decreasing identity infringement when library cards get lost. Figure 3 shows the scenario of library material borrowing and returning.

On the user side, library material borrowing consists of four simple steps performed by the user: 1) retrieving items, 2) authenticating with the finger-vein recognition device, 3) placing items on the RFID reader, and 4) exiting the library. When the user removes a book from the shelf, an infrared detector is triggered, recognizing that a book was removed from the shelf. Then, image recognition identifies the specific book and the book's status is marked as charged to the user in the stock database. If the user wants to leave the library without borrowing anything, the user just scans their finger with the finger-vein device to open the entrance gate. If the user wants to borrow library materials such as books or videos, the borrowing procedure is quickly completed after finger-vein scanning and placing all material including books and videos under the RFID read area. In the background, the user's recognition results from the finger-vein scan are saved in the biometrics database, which is connected to the blockchain. When the library materials are placed together in the RFID read area, all the tags are read at once while the materials' statuses in the database are updated. User information and material borrowing information are linked and saved as transactions that are stored in the personal borrowing blockchain.

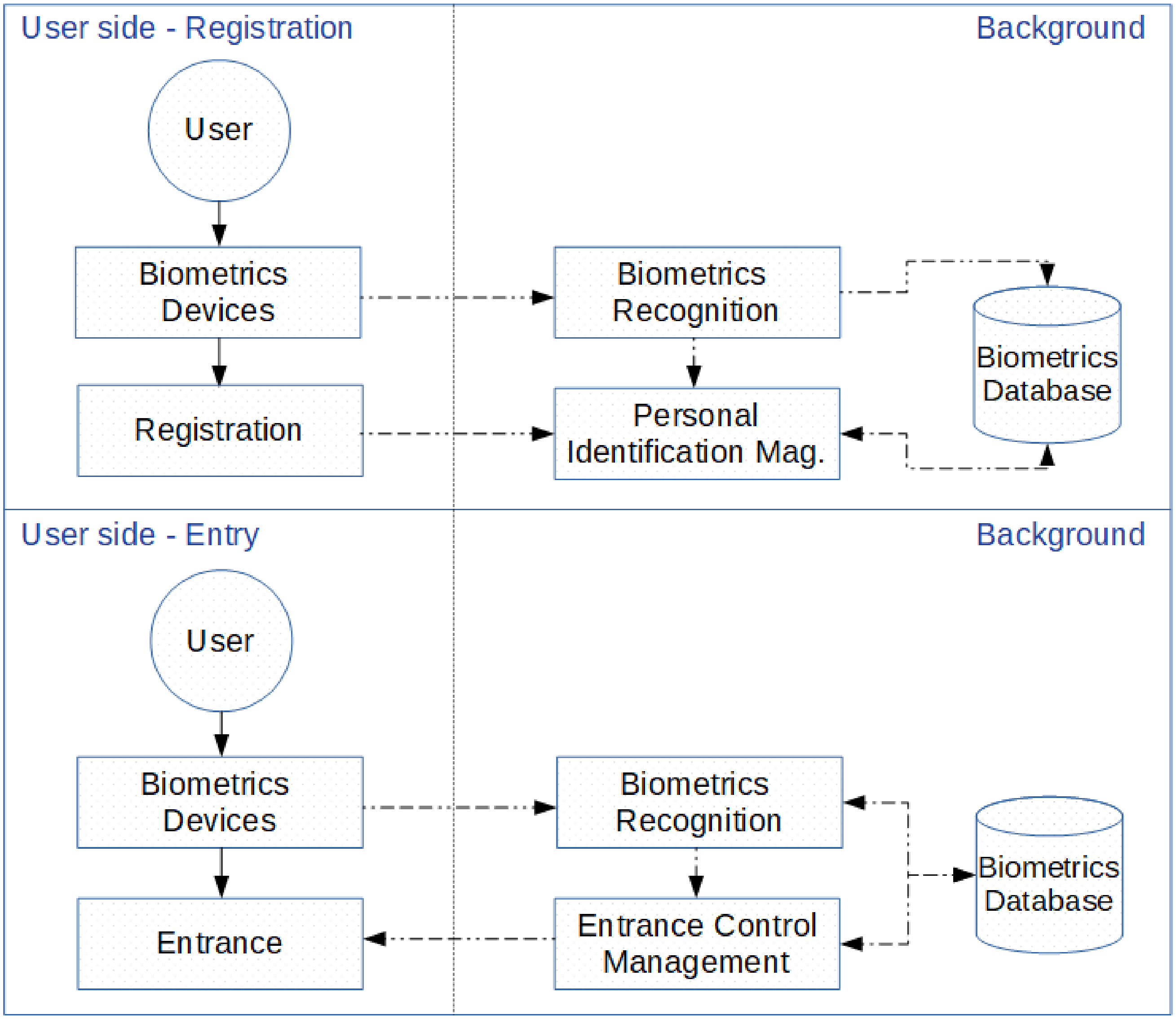

Figure 2. BlockMetrics Library Scenario—Registration and Entry

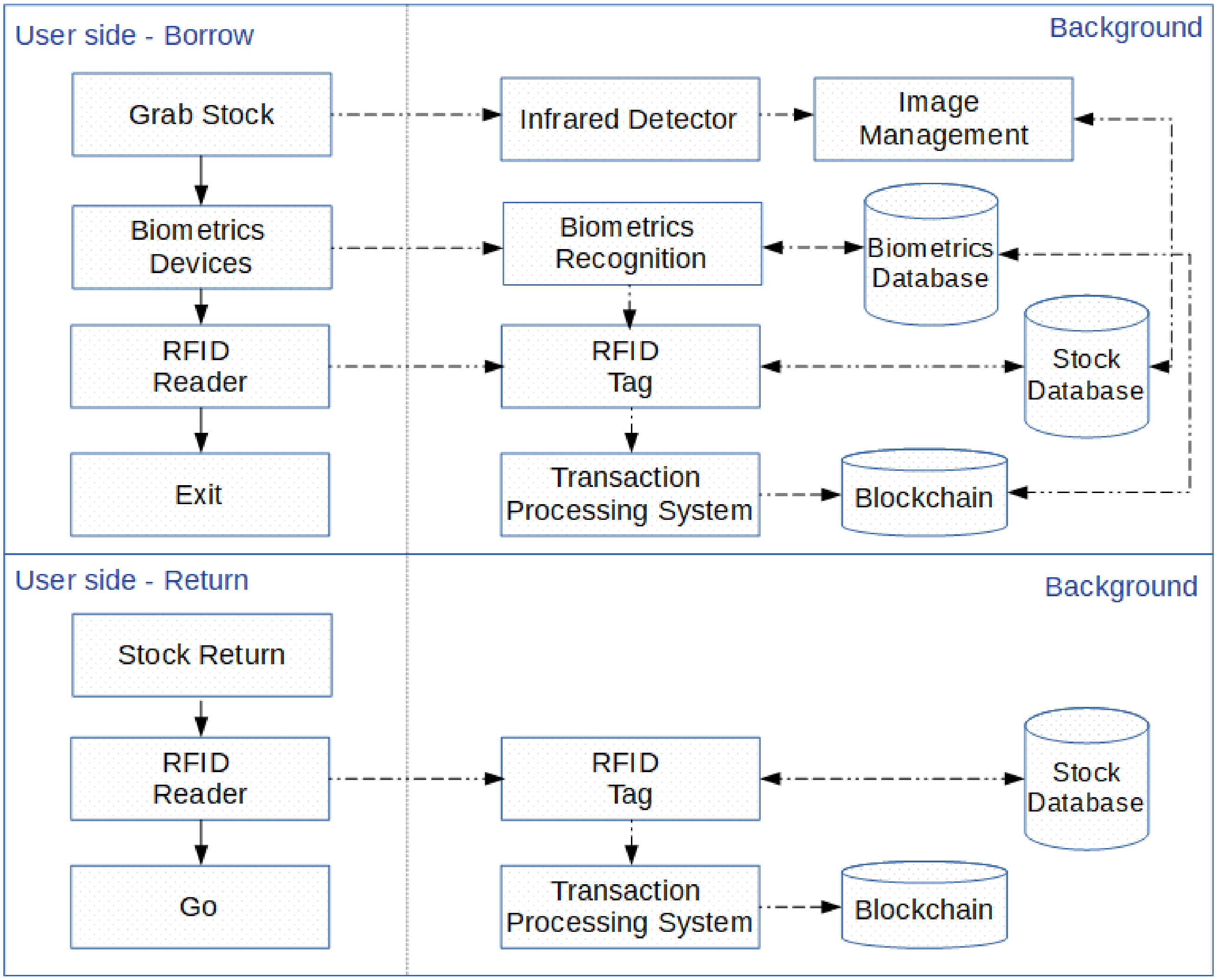

Figure 3. BlockMetrics Library Scenario – Borrowing and Returning

To return library material, the user only needs to put the library materials in the specific area with the RFID reader and the return procedure is completed. The RFID tags of returned materials are read and recorded and their status in the stock database is updated. Personal borrow and return records are saved as transactions and stored in the personal borrowing blockchain as well.

LIMITATIONS

Partial biometric technologies such as facial recognition or fingerprint recognition systems have been adopted by some libraries. These tools have increased the efficiency of accessing and borrowing procedures. However, all the records include some personal information (e.g., fingerprint, historical borrowing records, log of library access, etc.) that is still stored in the individual libraries' database. The blockchain model may not suitable for all current libraries system due to the unknown database design of each library. At present, library classification systems are by each library individually. Therefore, integrating library information among national or international libraries will be a huge task. Thus, how to establish the general regulations for all libraries to develop and manage the library information will need additional research. After that, the information management system should be designed and built by collecting diverse comments from all library managers. The works should be completed by interdisciplinary experts including library management, information engineering, biometrics system design, and data management. The cost may include manager committees, collection coding design, system development, hardware layout, and related training plans. Also, there may exist unpredictable privacy issues which could be known until practical system operation. Lastly, some users need an adaptation period while new technologies are implemented, the duration of which can depend on how smooth the interface design is, if the system manipulation is easy and clear to use, and what benefits the technologies bring to users' life. The limitations are concluded as: 1) integrating library information such as stock data and serial numbers, 2) establishing general regulations, 3) creating a consistent library management system, 4) the cost for this system, 5) potential for privacy breaches, and 6) library patron resistance or reluctance to use the technology.

CONCLUSION

In this research, the BlockMetrics library is designed under a wireless sensor network infrastructure combined with blockchain, biometric, IoT, and RFID technologies. The library access control system is based on finger-vein biometric recognition, in which users can register with their finger-vein information through biometric devices and input personal information via various I/O devices. Thus, automatic and secure library access control is achieved through biometric recognition. Additionally, image recognition, GPS, and RFID are adopted in the library collection management, providing a simplified way to borrow and return library material. Blockchain technologies are utilized to record personal borrowing history of collections from various libraries into a personal borrowing blockchain where records are permanently stored. Users can clearly understand their borrowing status through their own blockchain and manage their borrowing information through an application. To summarize, users can enter the library with finger-vein recognition instead of a specific library card. Then, if they would like to check out library material, the user can retrieve the items, pass them through the RFID reader, scan their finger vein, and go. The BlockMetrics library is designed for convenience and security, which are achieved by combining a wireless sensor network with the integration of blockchain and biometric technologies. This method eliminates the inconvenience of having to bring many library cards, increases the efficiency of collection borrowing procedures, and simplifies the management of collection borrowing from different libraries. Adoption of these biometric technologies is still in its early stages. Some libraries have begun using different tools, but few libraries have adopted all of them. It simplifies both accessing and borrowing procedures, and all the records are still stored in a particular library's database for private access only. The development of the BlockMetrics library will help to integrate biometric technologies and blockchain under the infrastructure of wireless sensor network to maintain library-accessing recognition, library collections, library users, borrowing records crossing libraries to raise the user convenience and satisfactions, library management efficiency, and library security. In the near future, the library transaction formula in a blockchain will be developed for collection borrowing storage. The library collection serial numbers will be considered in information management system as well.

ENDNOTES

1 Gartner, "Smart With Gartner, Gartner Top 10 Strategic Technology Trends for 2020," https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020/; Gartner, "Smart With Gartner, Gartner Top 10 Strategic Technology Trends for 2019," https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/; Gartner, "Smart With Gartner, Gartner Top 10 Strategic Technology Trends for 2018," https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/; Gartner, "Smart With Gartner, Gartner Top 10 Strategic Technology Trends for 2017," https://www.gartner.com/smarterwithgartner/gartners-top-10-technology-trends-2017/.

2 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2009), https://bitcoin.org/bitcoin.pdf.

3 David Shrier, Weige Wu, and Alex Pentland, "Blockchain & infrastructure (identity, data security)," Connection Science & Engineering, Massachusetts Institute of Technology, 2016.

4 Kristián Košt'ál et al., "On Transition between PoW and PoS," International Symposium ELMAR (2018).

5 Thomas P. Keenan, "Alice in Blockchains: Surprising Security Pitfalls in PoW and PoS Blockchain Systems," 15th Annual Conference on Privacy, Security and Trust (2017); Takeshi Ogawa, Hayato Kima, and Noriharu Miyaho, "Proposal of Proof-of-Lucky-ID (PoL) to Solve the Problems of PoW and PoS," IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data (2018).

6 Quoc Khanh Nguyen, Quang Vang Dang, "Blockchain Technology for the Advancement of the Future," 4th International Conference on Green Technology and Sustainable Development, (2018); Nir Kshetri and Jeffrey Voas, "Blockchain in Developing Countries," *IT Professional,* 20, no.2 (2018): 11-14.

7 Shangping Wang, Yinglong Zhang, and Yaling Zhang, "A Blockchain-Based Framework for Data Sharing with Fine-Grained Access Control in Decentralized Storage Systems," 2018 IEEE Access, 6 (2018):38437-38450.

8 Pinyaphat Tasatanattakool and Chian Techapanupreeda, "Blockchain: Challenges and applications," 2018 International Conference on Information Networking (ICOIN), (2018), https://doi.org/10.1109/ICOIN.2018.8343163; Abderahman Rejeb, John G. Keogh and Horst Treiblmaier, "Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management," *Future Internet*, 11, no. 7 (2019): 161; Stanislaw P. Stawicki, Michael S. Firstenberg, and Thomas J. Papadimos, "What's new in academic medicine? blockchain technology in health-care: bigger, better, fairer, faster, and leaner," *International Journal of Academic Medicine,* 4, no. 1 (2018): 1-11; Guang Chen et al., "Exploring blockchain technology and its potential applications for education," *Smart Learning Environments,* 5, no. 1 (2018), https://doi.org/10.1186/s40561-017-0050-x; Asma Khatoon, "A Blockchain-Based Smart Contract System for Healthcare Management," *Electronics,* 9, no. 1 (2020): 94.

9 National Central Library, "National Central Library Reader Service Directions," November 11, 2016, https://enwww.ncl.edu.tw/content_26.html.

10 Taipei Public Library, "Regulation of Circulation Services," June 13, 2018, https://english.tpml.gov.taipei/cp.aspx?n=AF5CCA6FC258864E.

11 Shih Hsin University Library, "Library Regulations, Access to SHU Libraries," http://lib.shu.edu.tw/e_orders_enter.htm; Shih Hsin University Library, "Library Regulations, Borrowing Policies," accessed September 25, 2019, http://lib.shu.edu.tw/e_orders_borrows.htm.

12 Sudhinder Singh Chowhan and Ganeshchandra Shinde, "Iris Biometrics Recognition Application in Security Management," 2008 Congress on Image and Signal Processing.

13 Stephen Cass, "The Top Programming Languages 2019," IEEE Spectrum (2019), https://spectrum.ieee.org/computing/software/the-top-programming-languages-2019.