Design and Research of a Blockchain-based Smart Identity Verification System for Financial Services

Jing-Yuan Ting*

Department of Computer Science and Information Engineering, National Taitung University; john489142@gmail.com

*Corresponding Author: john489142@gmail.com

DOI: https://DOI.org/10.30211/JIC.202402.011

Submitted: Oct. 18, 2024 Accepted: Dec. 15, 2024

ABSTRACT

The goal of this project is to create a smart way for the financial sector to verify identities that uses blockchain technology, mobile devices, and multiple forms of authentication such as passwords, facial recognition, and dynamic electronic signatures. To counter fraud risks from generative AI, it introduces blink detection and analyzes writing speed in signature verification. Additionally, a private blockchain-based verification system ensures cross-border data accuracy, enhancing security and innovation in digital finance.

Keywords: Smart Finance, Facial Recognition, Digital Signature, Blockchain, Identity Verification

1. Introduction

1.1 Research Background and Motivation

In traditional mobile device verification mechanisms, identity verification typically involves the use of an ID and password. To prevent passwords from being cracked, service providers often require the passwords to meet certain complexity standards, such as prohibiting repeated characters and requiring a mix of uppercase and lowercase letters, symbols, etc. However, these requirements often make passwords difficult to remember, and despite such measures, some users still choose high-risk passwords. In addition to an ID and password, service providers commonly send a one-time password (OTP) via SMS or email with a time limit as a form of verification. However, in 2017, the [1] National Institute of Standards and Technology (NIST) in the U.S. pointed out that obtaining OTP codes via mobile devices could be vulnerable to man-in-the-middle attacks by malware, and fraudsters could also impersonate well-known brands or service providers to send fake OTPs. As mobile devices have become widespread, many financial institutions have adopted biometric recognition as a verification method due to its convenience. However, in an age where generative AI can forge biometric data, these verification methods could become compromised at any time. Furthermore, the confidentiality of biometric data is crucial, as any leakage could lead to the misuse of users' personal traits in various contexts. Therefore, preventing biometric data theft has become an important issue for the future.

According to reports [2], as of September 2022, a fraud group in Hong Kong and Macau used

lost identity documents and forged documents to apply for financial services from institutions. By scanning and uploading identity proof documents and taking real-time selfie photos, they employed face-swapping technology to impersonate citizens who had reported lost IDs in facial recognition systems, successfully applying for four loans totaling about HKD 200,000. Although there have not been any successful cases of fraud using forged electronic signatures so far, as early as 2016, [3] researchers from University College London (UCL) developed an algorithm that could analyze font and handwriting styles to generate handwriting that replicated font size, color, texture, and vertical and horizontal spacing. Moreover, [4] at a 2017 Geek Challenge, the team from the China Financial Certification Authority (CFCA) trained a robotic arm to mimic an author's handwriting and generate a text segment. When mixed with original samples, professional handwriting examiners misjudged it at a rate of 50%. These cases warn us that while we enjoy the convenience of technology, we must take high precautions against potential threats. [5] Dr. Cha Shi-Zhao, director of Taiwan Tech's Information Security Center, highlighted that generative AI can produce realistic data, from text, images, and voices to code, significantly lowering the entry barrier for hackers. [5] Trend Micro's senior technology consultant, Jian Sheng-Cai, also pointed out that the development of AI and other new technologies allows hackers to carry out more sophisticated attacks, highlighting the importance of strengthening verification mechanisms.

1.2 Research Objectives and Issues

Combining individual-specific facial feature verification with electronic signature methods can effectively reduce the threat of a single point of attack and avoid the risk of traditional password theft. At the same time, it eliminates the need for users to remember complex password combinations. This method provides both high security and convenience, allowing users to complete verification directly on their mobile phones. Additionally, the use of blockchain to securely store personal characteristics significantly reduces the risk of personal data leakage.

When it comes to verification, this method is better than rectangular facial recognition methods because it includes blink detection. This makes it harder for generative AI to fake based on partial facial features. As for electronic signatures, with the advancement of generative AI, we can foresee that AI will eventually be able to fully simulate static signature features. Therefore, it is necessary to record multi-dimensional dynamic signature information. The method proposed in this project analyzes the stroke order and writing speed of handwritten signatures to verify the authenticity of the signer. Although the correct stroke order is known, in practice, everyone's signature differs slightly due to personal habits, and these differences may deviate slightly from the examples in the learning data. These subtle variations make it more difficult for generative AI to perfectly imitate, thereby increasing the challenge of forgery.

Regarding the storage of personal data, private chains offer greater privacy and security, where only authorized participants can manage the data. Moreover, due to the structure of blockchain data, once information is written into a block, altering it would require obtaining the private key of the block and modifying more than half of the blocks within a short time, effectively preventing data tampering. Furthermore, the transparency of blockchain transactions allows all authorized

participants to view and verify transaction records, which helps trace the history of user identity verification and further enhances credibility. [6] Xu Wen-Hui, CTO of IBM Taiwan, also pointed out that the characteristics of blockchain not only save time and effort but also provide detailed production and transaction records for government regulation. Additionally, smart contracts can design blockchain with compliance standards, ensuring user privacy and meeting regulatory requirements across different regions.

2. Literature Review

2.1 Blockchain Research: Domestic and International

[7] Compared the security issues of different development frameworks and mentioned that the integration of blockchain and artificial intelligence holds enormous potential in emerging applications across various fields. [8] Highlighted that when blockchain is applied in the financial sector, processing speed becomes the biggest obstacle, leading to the use of private chains with faster consensus algorithms. The author also pointed out that achieving complete decentralization in the financial sector is challenging, as institutional management is still often required. [9] The author proposed a more comprehensive Blockchain as a Service (BaaS) platform, introducing Identity-Chain technology, a blockchain-based identity management system, and smart contract vulnerability detection. The author also noted that while BaaS offers convenience, it may compromise the decentralization and trustless nature of blockchain, suggesting that increased transparency could alleviate the issue of centralization. [10] They suggested a semi-decentralized smart contract system that works in a centralized way off-chain but still has the immutability and verifiability of blockchain, which makes it work better. Smart healthcare systems, involving patients, doctors, nurses, and other healthcare professionals, necessitate secure and efficient data exchange, as noted in [11]. The use of private blockchain combined with identity verification mechanisms can effectively ensure the security of medical data.

To summarize these studies, blockchain and artificial intelligence show enormous potential across various fields. In the financial sector, using a public blockchain can lead to performance limitations, and institutional management is sometimes still necessary. Thus, private blockchains are more suitable in such scenarios. Some studies also emphasize that centralization can lead to inefficiencies, making the balance between security and performance an important issue in different contexts.

2.2 Digital Identity Verification Research: Domestic and International

[12] Proposed a new architecture called MIPGAN for generating morphed facial images (commonly referred to as deepfakes) and evaluated its effectiveness on commercial face recognition systems (FRS) based on deep learning. The study found that without morphing attack detection (MAD), MIPGAN-generated morphed images pose a significant threat to face recognition systems. [13] The study compared three font style transfer models under different training data sizes (handwritten recognition) and evaluated their performance using SSIM, LPIPS, and FID metrics for image similarity. The study showed that models trained with fewer than 400 characters had less than

90% accuracy in handwritten recognition, while a model trained with 1,500 characters reached 92% accuracy. The author also used data from different levels of scribbled handwriting as training material and compared the similarity metrics. The results showed that FID was less correlated compared to SSIM and LPIPS. [14] The author implemented a private blockchain verification system, using multiple cloud servers as nodes through AWS cloud services, and compared the cost differences between cloud and self-hosted servers. The author pointed out that using a private blockchain provides greater security for verification data, in addition to avoiding transaction fees and reducing response times. The author also mentioned that most current authentication systems store data in relational databases, but if tampered with, no trace would be left. In [15], it was mentioned that federated identity management is a method that helps manage identity processes and policies between collaborating entities without the need for centralized control. However, the complexity of federated identity management lies in how different entities interact to provide identity verification mechanisms. In [16], the study discussed how facial morphing attacks aim to bypass facial recognition systems by generating various expressions using facial data and testing whether the system could still verify them. Many systems, to avoid high error rates, intentionally reduce recognition precision, which allows hackers to use generative AI to attack recognition systems. [17] Stated that digital authentication primarily aims for decentralization, with digital identity verification relying on blockchain to achieve decentralized management, thereby avoiding the risk of centralized servers being attacked and causing system failure.

In short, generative AI is a very big problem right now when it comes to making fake faces that can't be detected by morphing attack detection (MAD) systems. In text generation, even the better-performing generation models require a substantial amount of data for effective forgery. As for the storage of verification data, private blockchains provide higher security compared to databases. However, the use of centralized private blockchains, which contradicts the decentralized nature of blockchain, remains a debated issue.

3. Research Design

3.1 Design Process

This section describes the project process. The first step is to establish the identity verification mechanism, which involves designing facial recognition and signature stroke verification algorithms, combined with multi-factor authentication, while considering how to counter generative AI. The second step is the development of a decentralized financial system, including the selection of the blockchain platform, type, and technology, as well as defining key components like smart contracts and nodes. The third step is integrating the identity verification system into the blockchain, followed by a preliminary evaluation of the security and performance of the node information. The final step involves testing and optimization, where potential issues are identified from the test results, and optimization opportunities are evaluated. If improvements are needed, the process returns to the integration phase.

3.2 Facial Verification System

In addition to using front-facing facial images as a basis for verification, the system also verifies blinking movements and facial appearance, as current generative AI and deepfake programs struggle with dynamic imagery. This project employs the Google FaceNet pre-trained model to reduce training time.

According to [18], the process first involves using a CNN structure (with Zeiler & Fergus networks and GoogLeNet being tested in the study) to extract features. The data is then L2-normalized to a range between 0 and 1. Next, an embedding layer is applied, where the mapping f(a) of a is positioned on a hypersphere. The final embedding vector output is used with triplet loss as the loss function.

Then, the system uses MTCNN (Multi-Task Cascaded Convolutional Neural Network). Once the facial region is identified, it continuously extracts and preprocesses the facial region, storing it in the database. At this point, the preparation before verification is complete, as shown in Figure 1.

Figure 1. Facial Recognition Preprocessing Flowchart

Source: By authors.

During the verification process, the system similarly scans the face and calculates the Euclidean distance between the scanned feature vectors and those stored in the database. If the distance is within the allowed threshold, the process proceeds to the next stage—blink verification. The system prompts the user to blink. By adopting the blink detection algorithm mentioned in [19], the system calculates the Eye Aspect Ratio (EAR) to determine whether the eyes are open or closed, thereby detecting the blinking action. Both FaceNet and blink verification must be passed for the verification to be considered complete, as shown in Figure 2.

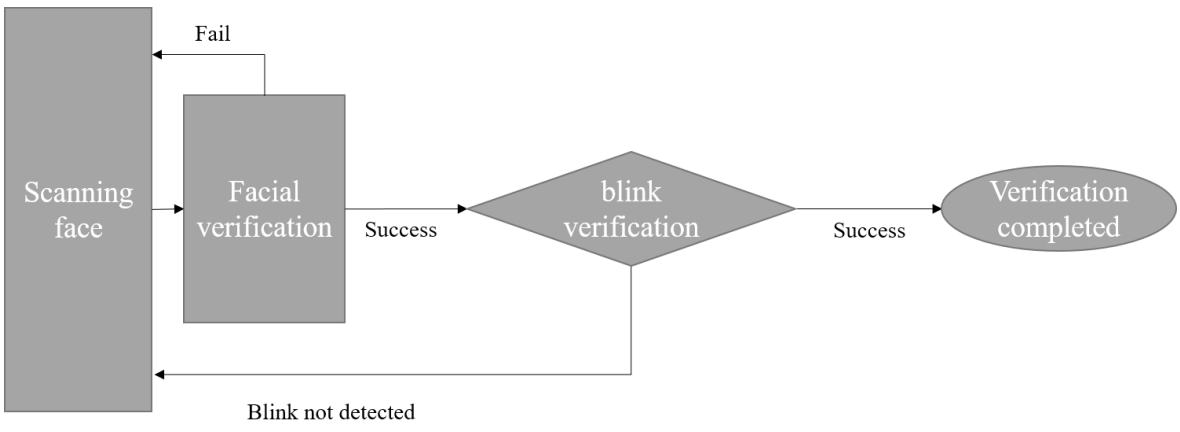

Figure 2. Facial Verification Flowchart

Source: By authors.

3.3 Signature Recognition System

Similarly, to make it more difficult for generative AI to forge, we do not simply use static images of signatures for verification. Instead, we employ biometric signatures that record more detailed information about the signing process. The user's signature is captured through the canvas element on a webpage, as illustrated in Figure 3.

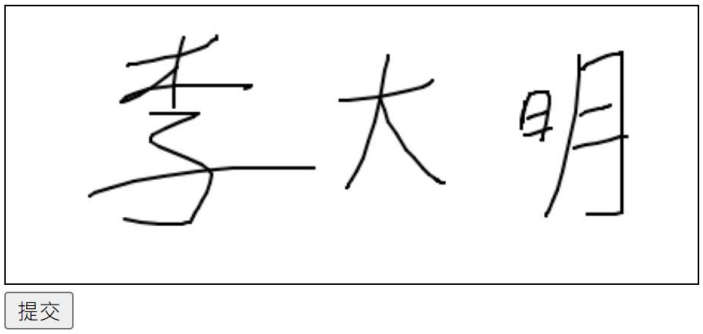

Figure 3. Web-Based Signature Interface

Source: By authors.

At different moments, the X and Y positions of the pen tip are recorded using JavaScript, capturing signature speed and stroke order, along with the overall appearance of the signature. This data is then sent to the backend via API to serve as input for the model, as shown in Figure 4.

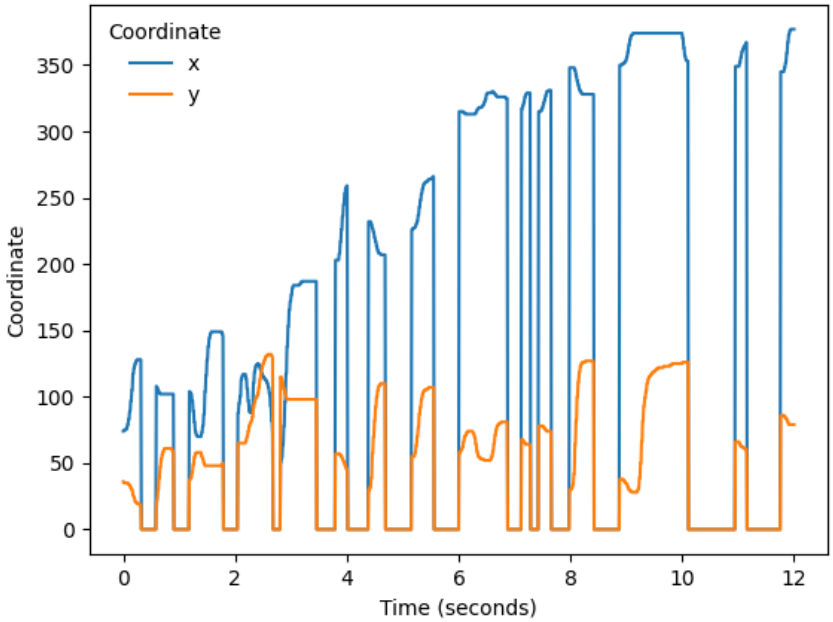

Figure 4. Signature Information

Source: By authors.

Next, a Recurrent Neural Network (RNN), such as Long Short-Term Memory (LSTM), is used to predict whether the handwriting data belongs to the individual, while a Convolutional Neural Network (CNN) extracts overall signature features. The outputs of both models are combined to verify whether the signature falls within a reasonable error range. Finally, hyperparameters such as

learning rate are adjusted, as shown in Figure 5.

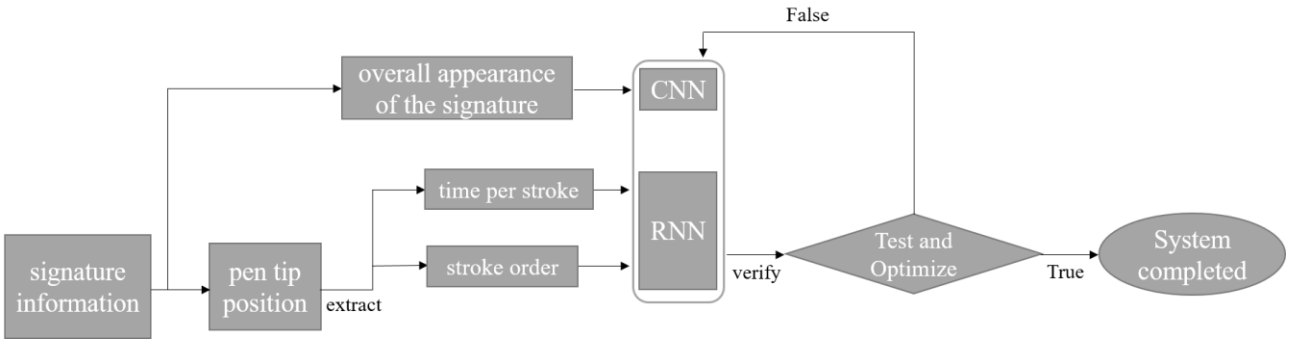

Figure 5. Handwriting Recognition Flowchart

Source: By authors.

3.4 Blockchain System

A private chain is implemented for this project. Since it is used for internal management within organizations and enterprises, the degree of decentralization is lower compared to public chains and consortium chains. However, the number of nodes is controllable, which gives private chains advantages such as faster speeds, stronger security, and lower transaction costs. To achieve the goal of speed, the Proof of Authority (PoA) consensus algorithm is utilized.

4. Results and Discussion

4.1 Facial Verification System

4.1.1. Facial Verification

The program calculates the Euclidean distances between the face embeddings of detected faces and those of known faces stored in the database. It identifies the person by selecting the key corresponding to the smallest distance. However, if this minimum distance exceeds a predefined threshold, the person is labeled as "Undetected."

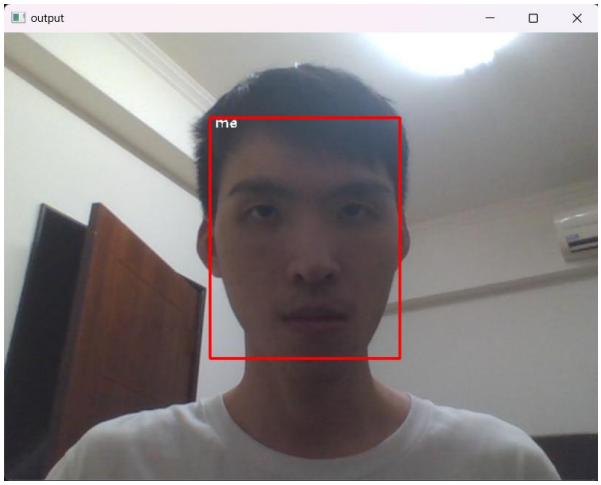

Figure 6. Facial Verification Interface

Source: By authors.

4.1.2. Blink Verification

Experiments revealed that the EAR value for open eyes is mostly between 0.27 and 0.32. The detection process is shown in Figure 7. Therefore, the threshold was set to 0.27. If the EAR value is below the threshold for three consecutive frames, it is considered a blink.

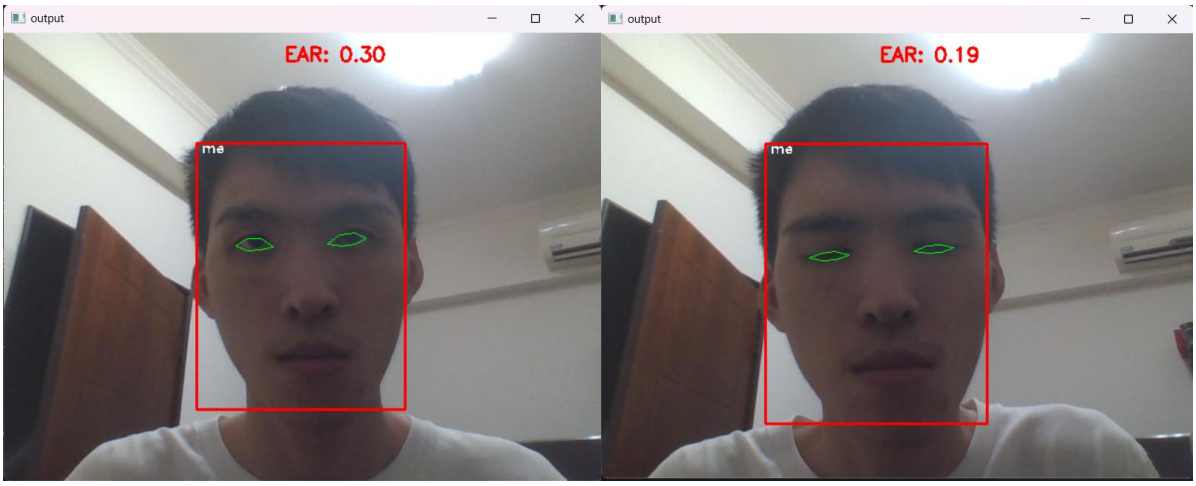

Figure 7. Blink Verification Interface and the difference in EAR between open and closed eyes. Source: By authors.

4.2 Signature Recognition System

When using 200 signature samples as the training set and 40 as the testing set. In the training set's 100 negative samples, half are signatures by the same person as the positive samples but with incorrect strokes, while the other half are forged signatures by a different person. the model performance on the test set is shown in Figure 8. The model achieved a performance of Precision: 0.8, Recall: 0.6957, and F1-Score: 0.7435.

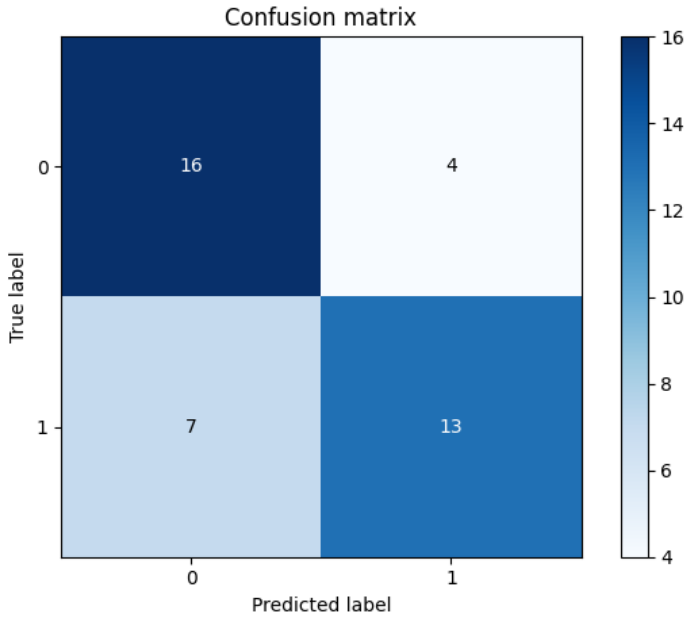

Figure 8. Confusion Matrix.

Source: By authors.

5. Conclusions

This study successfully integrates facial feature verification and blink detection technology, offering an enhanced security authentication method. In terms of facial verification, incorporating blink detection effectively reduces the risk of spoofing attacks that may arise when relying solely on static images for identity authentication. Furthermore, the dynamic electronic signature verification mechanism demonstrates exceptional potential. It can tell the difference between real signatures and fakes by looking at the writing speed and stroke dynamics of signatures. This stops hackers from using static signature images to try to break in.

However, this study also faces certain challenges and areas for improvement. We need more precise metrics for facial verification to assess the system's robustness and accuracy, particularly in diverse usage scenarios. Additionally, the accuracy of signature recognition needs further enhancement to counter potentially sophisticated forgery techniques. Future research could focus on introducing a broader range of feature parameters and deep learning models to improve overall system performance. Moreover, further exploration of the applicability and scalability of the technology in real-world scenarios is warranted.

References

[1] Chou, C.Y. SMS-based two-factor authentication is no longer secure and advises against using it. Available online: https://www.ithome.com.tw/news/112845.

[2] Meng, Y.J. Hong Kong police cracked their first AI deepfake loan fraud case, arresting six individuals involved in a scheme worth 200,000 HKD. Available online: http://www.hkcna.hk/docDetail.jsp?id=100451430&channel=4371.

[3] Haines, T.S.F., Mac Aodha, O. and Brostow, G.J. My text in your handwriting. ACM Transactions on Graphics, 2015, Article XXXX, 28 pages.

[4] Han, X. CFCA Machine Learning Laboratory made its debut at the GeekPwn International Security Geek Competition. Available online: https://www.cebnet.com.cn/20171025/102437122.html.

[5] Xu, Z. The misuse of generative AI has led to a surge in cyberattacks and online fraud. Available online: https://ec.ltn.com.tw/article/paper/1602505.

[6] Mia. IBM Blockchain Lab Director, optimistic about the Greater China region, emphasized that governments need to understand the technology and establish regulatory sandboxes to balance oversight and innovation. Available online: https://www.inside.com.tw/article/6678-ibm-blockchain.

[7] Bhutta, M.N.M., Khwaja, A.A., Nadeem, A., Ahmad, H.F., Khan, M.K., Hanif, M.A., Song, H., Alshamari, M. and Cao, Y. A survey on blockchain technology: Evolution, architecture, and security. IEEE Access, 2021. doi: 10.1109/ACCESS.2021.3072849.

[8] Wang, Y.C. A study on the application of blockchain in the financial industry. [Master's thesis, National Taiwan University] National Digital Library of Theses and Dissertations in Taiwan. Available online: https://hdl.handle.net/11296/whehp2.

[9] Zheng, W., Zheng, Z., Chen, X., Dai, K., Li, P. and Chen, R. NutBaaS: A blockchain-as-a-service platform. IEEE Access, 2019, 7, 134422-134433. doi: 10.1109/ACCESS.2019.2941905.

[10] Lin, H.P. Semi-centralized blockchain smart contract: Smart contract of centralized verification and off-chain execution on Ethereum blockchain. [Master's thesis, National Taiwan University] National Digital Library of Theses and Dissertations in Taiwan. Available online: https://hdl.handle.net/11296/j2w3tk.

[11] Yazdinejad, A., Srivastava, G., Parizi, R.M., Dehghantanha, A., Choo, K.K.R. and Aledhari, M. Decentralized authentication of distributed patients in hospital networks using blockchain. IEEE Journal of Biomedical and Health Informatics, 2020, 24(8), 2146-2156. doi: 10.1109/JBHI.2020.2969648.

[12] Zhang, H., Venkatesh, S., Ramachandra, R., Raja, K., Damer, N. and Busch, C. MIPGAN-Generating strong and high-quality morphing attacks using identity prior driven GAN. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2021, 3(3), 365-383. doi: 10.1109/TBIOM.2021.3072349.

[13] Huang, J.X. Analysis and comparison of handwriting style font generation based on generative adversarial network. [Master's thesis, National Cheng Kung University] National Digital Library of Theses and Dissertations in Taiwan. Available online: https://hdl.handle.net/11296/eu3cbj.

[14] Liu, J.T. A study on the private-blockchain-based smart contract using certification as an example. [Master's thesis, Shih Chien University] National Digital Library of Theses and Dissertations in Taiwan. Available online: https://hdl.handle.net/11296/h8rp5d.

[15] Carretero, J., Izquierdo-Moreno, G., Vasile-Cabezas, M. and Garcia-Blas, J. Federated identity architecture of the European eID system. IEEE Access, 2018, 6, 75302-75326. doi: 10.1109/ACCESS.2018.2882870.

[16] Kersic, V., Vidovic, U., Vrecko, A., Domajnko, M. and Turkanovic, M. Orchestrating digital wallets for on- and off-chain decentralized identity management. IEEE Access, 2023, 11, 78135-78151. doi: 10.1109/ACCESS.2023.3299047.

[17] Schroff, F., Kalenichenko, D. and Philbin, J. FaceNet: A unified embedding for face recognition and clustering. 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015, 815-823. doi: 10.1109/CVPR.2015.7298682.

[18] Soukupová, T. and Cech, J. Real-time eye blink detection using facial landmarks. 2016.